

Novell Nsure™ Identity Manager

2

www.novell.com

管理者ガイド

June 30, 2004

N

Novell®

法的通知

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っておりません。また、本書の商品性、および特定の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。また、米国 Novell, Inc. およびノベル株式会社は、予告なくこの出版物を改訂またはその内容を変更する権利を有します。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っておりません。またノベル製ソフトウェアの商品性、および特定の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。

米国輸出規制や居住国の法律など、適用される法律または規制に違反して当製品を輸出または再輸出することはできません。

Copyright © 2004 Novell, Inc. All rights reserved. 本書のいかなる部分についても、発行者の書面による明示的同意なしに、複製、コピー、検索システムへの保存、伝送を行ってはなりません。

U. S. Patent Nos. 5, 349, 642; 5, 608, 903; 5, 671, 414; 5, 677, 851; 5, 758, 344; 5, 784, 560; 5, 818, 936; 5, 828, 882; 5, 832, 275; 5, 832, 483; 5, 832, 487; 5, 870, 561; 5, 870, 739; 5, 873, 079; 5, 878, 415; 5, 884, 304; 5, 919, 257; 5, 933, 503; 5, 933, 826; 5, 946, 467; 5, 956, 718; 6, 016, 499; 6, 065, 017; 6, 105, 062; 6, 105, 132; 6, 108, 649; 6, 167, 393; 6, 286, 010; 6, 308, 181; 6, 345, 266; 6, 424, 976; 6, 516, 325; 6, 519, 610; 6, 539, 381; 6, 578, 035; 6, 615, 350; 6, 629, 132. 特許出願中。

米国 Novell, Inc.
1800 South Novell Place
Provo, UT 84606
米国

www.novell.com

Novell Nsure Identity Manager 2 管理ガイド

[June 30, 2004](#)

オンラインドキュメント： この製品およびその他の Novell 製品のオンラインマニュアルや更新情報については、www.novell.com/documentation を参照してください。

Novell の商標

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

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

eDirectory は、米国 Novell, Inc. の商標です。

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、Novell, Inc. の商標です。

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

Nsure は米国 Novell, Inc. の商標です。

SUSE は、米国 Novell, Inc. の事業部である SUSE LINUX AG の登録商標です。

Third-Party Materials

すべてのサードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて	11
1 概要	13
Identity Manager 2 の新機能	15
ポリシーを作成するための Policy Builder のインタフェースと DirXML Script	15
パスワードの管理	16
Role-Based Entitlement (役割ベースのエンタイトルメント)	16
Novell Nsure Audit を使用したレポーティングと通知	17
グローバル設定値	17
ドライバのハートビート	18
ドライバ設定をインポートする際の柔軟なプロンプト	18
Identity Manager のアーキテクチャの概要	18
DirXML エンジン	19
DirXML ドライバシム	20
ドライバ設定ファイル	20
Identity Manager のイベントキャッシュ	20
Identity Manager のコンポーネント	20
ドライバセット	20
ドライバオブジェクト	21
ドライバシム	22
発行者チャンネルと加入者チャンネル	23
イベントとコマンド	23
ポリシーとフィルタ	23
関連付け	23
2 計画	25
一般的なインストールシナリオ	25
Identity Manager の新しいインストール	25
同一環境での Identity Manager と DirXML 1.1a の使用	27
Starter Pack から Identity Manager へのアップグレード	29
Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード	31
Identity Manager 実装のプロジェクト管理面の計画	33
Novell Identity Manager の展開	33
Identity Manager 実装の技術面の計画	39
Identity Manager がサーバ上で必要とするオブジェクトの複製	39
スコープフィルタ処理を使用した別のサーバ上のユーザの管理	41
3 アップグレード	45
パスワード同期のアップグレード	45
RNS から Nsure Audit へのアップグレード	45
ドライバ設定のアップグレード	45
4 インストール	47
インストールの前に	47
Identity Manager のコンポーネントとシステム要件	48
Identity Manager の NetWare へのインストール	50

Identity Manager の Windows へのインストール	51
Identity Manager の UNIX プラットフォームへのインストール	52
インストール後の作業	53
リモートローダ	53
概要	53
リモートローダのインストール	54
リモートローダの設定	57
リモートローダで使用する DirXML ドライバの設定	67
リモートローダの実行	72
Identity Manager 製品のアクティベーション	76
カスタムドライバのインストール	76
5 DirXML ドライバの管理	77
ドライバの作成と設定	77
ドライバオブジェクトの作成	78
複数のドライバの作成	78
Identity Manager 環境での DirXML 1.x ドライバの管理	78
DirXML 1.x から Identity Manager 形式へのドライバ設定のアップグレード	79
ドライバの起動、停止、または再起動	79
グローバル設定値の使用	80
DirXML コマンドラインユーティリティの使用	80
バージョン情報の表示	80
階層構造でのバージョン情報の表示	81
テキストファイルの表示	83
バージョン情報の保存	84
名前付きパスワードの使用	85
iManager を使用した名前付きパスワードの設定	85
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	87
ドライバポリシーでの名前付きパスワードの使用	90
ドライバオブジェクトとサーバの再関連付け	90
ドライバハートビートの追加	91
6 ポリシーの作成	93
7 Password Policy (パスワードポリシー) を使用したパスワードの管理	95
Password Policy (パスワードポリシー) 機能の概要	95
ユニバーサルパスワードの有効化	96
Advanced Password Rule (詳細パスワードルール) の設定	97
Password Policy (パスワードポリシー) への独自のパスワード変更メッセージの追加	99
ユーザへのパスワードを忘れた場合のセルフサービスの提供	99
ユーザへのパスワードのリセットセルフサービスの提供	99
eDirectory ユーザへのポリシーの割り当て	99
eDirectory 内でのポリシーの適用	100
接続システムへのポリシーの適用	101
ユーザに対して有効な Password Policy (パスワードポリシー) の表示	102
ユーザのユニバーサルパスワードの設定	102
Password Policy (パスワードポリシー) の計画	102
Password Policy (パスワードポリシー) をツリー内に割り当てる方法の計画	103
Password Policy (パスワードポリシー) のルールの計画	103
ユーザのログインおよびパスワード変更方法の計画	103
Password Policy (パスワードポリシー) の使用に関する前提条件	107
ユニバーサルパスワードなしでの Password Policy (パスワードポリシー) の展開	108
(NetWare 6.5 のみ) ユニバーサルパスワード割り当ての再作成	108
Password Policy (パスワードポリシー) の作成	110
ユーザへの Password Policy (パスワードポリシー) の割り当て	111
ユーザに割り当てられているポリシーの確認	112

ユーザのパスワードの設定	112
チャレンジセットの作成または変更	112
パスワード通知機能の設定	112
Password Policy (パスワードポリシー) のトラブルシューティング	113
8 パスワードセルフサービス	115
セルフサービス機能の概要	115
ユーザへのパスワードを忘れた場合のセルフサービスの提供	116
ユーザへのパスワードのリセットセルフサービスの提供	117
セルフサービスの使用に関する前提条件	118
パスワードセルフサービスのログイン方法の計画	118
エンドユーザへのパスワードを忘れた場合のセルフサービスの提供	118
チャレンジセット	119
[Forgotten Password] のアクション	120
パスワードヒント	121
エンドユーザへの [Forgotten Password] の設定の要求	122
パスワードを忘れた場合のセルフサービスのエンドユーザ設定	123
エンドユーザがパスワードを忘れた場合に表示される機能	132
[Forgot Your Password?] リンクのオフ	135
Hint ガジェットの削除によるパスワードヒントの無効化	137
ユーザへのパスワードのリセットセルフサービスの提供	138
Password Policy (パスワードポリシー) への独自の Password Change Message (パスワード変更メッセージ) の追加	139
チャレンジセットの作成または変更	140
パスワードセルフサービスの通知の設定	140
パスワードセルフサービスのテスト	140
企業ポータルへのパスワードセルフサービスの追加	141
パスワードセルフサービスの exteNd Director 4.1 との統合	142
パスワードセルフサービスと Virtual Office との統合	144
企業ポータルからパスワードセルフサービスへのリンク	145
ユーザによるパスワード機能設定の確認	148
パスワードセルフサービスのトラブルシューティング	149
9 接続システム間のパスワード同期	151
概要	151
パスワードの概要	152
Password Synchronization 1.0 と Identity Manager パスワード同期の比較	153
双方向パスワード同期とは	154
Identity Manager パスワード同期の機能	155
パスワード同期フローの図	158
パスワード同期をサポートする接続システム	159
パスワード同期の前提条件	161
ユニバーサルパスワードのサポート	162
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	162
グローバル設定値を使用して作成するパスワード同期設定	162
ドライバ設定で必要なポリシー	166
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	167
ユーザ用に作成する Password Policy (パスワードポリシー)	168
NMASS ログインメソッド	168
機密情報の処理	168
SSL の使用	169
セキュリティで保護された eDirectory および Identity Manager オブジェクトへのアクセス	169
パスワード管理機能のセキュリティ上の考慮事項の確認	169
強力な Password Policy (パスワードポリシー) の作成	170
パスワード同期に参加する接続システムのセキュリティ保護	171
セキュリティの業界ベストプラクティスへの準拠	171

Nsure Audit を使用した機密情報の変更の追跡	171
Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業	173
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	173
iManager セルフサービスコンソールまたは Novell Client によるパスワードの変更	174
ユニバーサルパスワードを使用するための準備作業	175
レプリカの計画と Password Policy (パスワードポリシー)	176
電子メール通知の設定	176
新しいドライバ設定と Identity Manager パスワード同期	176
Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード	178
Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード	178
パスワード同期の実装	184
Identity Manager と NMAS の関係の概要	184
シナリオ 1 - NDS パスワードを使用した eDirectory 間でのパスワード同期化	185
シナリオ 2 - ユニバーサルパスワードの同期	188
シナリオ 3 - Identity Manager での配布パスワードのアップデートによる、 eDirectory および接続システムの同期化	197
シナリオ 4 - トンネリングと Identity Manager での配布パスワードのアップデートによる、 eDirectory ではなく接続システムの同期化	207
シナリオ 5 - アプリケーションのパスワードの通常パスワードへの同期化	213
パスワードフィルタの設定	216
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	216
NIS のためのパスワード同期のフィルタの設定	216
パスワード同期の管理	217
システム間のパスワードフローの設定	217
接続システムへの Password Policy (パスワードポリシー) の適用	220
eDirectory パスワードを同期化されたパスワードとは別にそのままにしておく方法	220
ユーザのパスワード同期ステータスのチェック	220
電子メール通知の設定	220
前提条件	221
電子メール通知を送信するための SMTP サーバの設定	222
通知のための電子メールテンプレートの設定	223
ドライバポリシーでの SMTP 認証情報の提供	224
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	225
電子メール通知の管理者への送信	233
電子メール通知テンプレートのローカライズ	233
パスワード同期のトラブルシューティング	234
10 Role-Based Entitlement (役割ベースのエンタイトルメント)	237
概要	237
Role-Based Entitlement (役割ベースのエンタイトルメント) の仕組み	239
前提条件	240
エンタイトルメントサービスドライバの作成と接続システムのドライバの設定	241
エンタイトルメントドライバのためのドライバオブジェクトの作成	241
Entitlement Policy (エンタイトルメントポリシー) を使用するためのドライバの設定	242
Entitlement Policy (エンタイトルメントポリシー) の作成	242
Entitlement Policy (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	243
Entitlement Policy (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	245
アカウントの安全の保持	250
エンタイトルメントの追加または削除の意味の制御	250
Entitlement Policy (エンタイトルメントポリシー) 間の衝突の解決	251
概要	251
各エンタイトルメントの衝突の解決方法の変更	253
Entitlement Policy (エンタイトルメントポリシー) の優先度の設定	254
パスワード同期と Role-Based Entitlement (役割ベースのエンタイトルメント)	255
Role-Based Entitlement (役割ベースのエンタイトルメント) のトラブルシューティング	256

11	エンジンサービスの管理	257
	エンタイトルメントサービスドライバ	257
	ループバックサービスドライバ: 移動プロキシサービスによるオブジェクトの移動	257
	移動プロキシサービスの概要	258
	移動プロキシサービスの設定	258
	移動プロキシサーバに移動を委任するための他のドライバの設定	260
	Manual Task Service Driver (Workflow Service Request Driver)	261
12	高可用性	263
	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	263
	eDirectory のインストール	264
	Identity Manager のインストール	264
	NICI データの共有	265
	eDirectory および Identity Manager のデータの共有	265
	DirXML ドライバについての考慮事項	267
	SuSE Linux についてのケーススタディ	267
13	Nsure Audit によるログとレポート	269
	概要	269
	Nsure Audit の設定	270
	プラットフォームエージェントの設定	270
	セキュアログサーバの設定	271
	ログの設定	271
	ログするイベントの選択	272
	ユーザ定義イベント	275
	eDirectory オブジェクト	277
	クエリおよびレポート	278
	Identity Manager のレポート	278
	Identity Manager のイベントの表示	278
	イベントに基づく通知の送信	279
	ステータスログの使用	279
	最大ログサイズの設定	279
	ステータスログの表示	280
A	Novell Identity Manager 製品のアクティベーション	281
	Identity Manager 製品ライセンスの購入	281
	ジェネリックキーによる Identity Manager のアクティベーション	282
	プロダクトアクティベーション要求の作成	283
	プロダクトアクティベーション要求の送信	284
	プロダクトアクティベーションキーのインストール	286
	Identity Manager および DirXML ドライバのプロダクトアクティベーションの表示	288
B	eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート	289
C	更新履歴	293
	2004 年 3 月	293
	2004 年 4 月 1 日	293
	2004 年 4 月 13 日	293
	2004 年 6 月 30 日	294

このガイドについて

Novell® Nsure™ Identity Manager 2 (以前の名称はDirXML®) 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の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、シングルサインオン、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 サービスの基盤となります。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配布できます。

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

追加のドキュメント

DirXML ドライバの使用に関するマニュアルについては、[Identity Manager オンラインマニュアルの Web サイト \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](http://www.novell.com/documentation/lg/dirxmldrivers/index.html) を参照してください。

最新のマニュアル

このマニュアルの最新版については、[Identity Manager オンラインマニュアルの Web サイト \(http://www.novell.com/documentation/lg/dirxml20/index.html\)](http://www.novell.com/documentation/lg/dirxml20/index.html) を参照してください。

マニュアル表記規則

このマニュアルでは、手順に含まれる複数の操作および相互参照パス内の項目を分けるために、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 (*) はサードパーティの商標を示します。

ユーザコメント

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コメントと提案をお聞かせください。proddoc@novell.com まで電子メールにてご連絡ください。

1

概要

Novell® Nsure™ Identity Manager 2（以前の名称は DirXML®）は、データの管理方法を根本的に改革する評価の高いデータ共有および同期ソリューションです。このサービスでは、識別ボールドを利用して、アプリケーション、データベース、およびディレクトリ全体で情報を同期化、変換、および配布します。

あるシステムのデータが変更されると、DirXML エンジンはいくつかの変更を検出し、ユーザが定義したビジネスルールに基づいて、接続されているその他のエンティティにこれらの変更を伝えます。このソリューションにより、ユーザは特定のデータ（たとえば、ユーザの ID は人事アプリケーションで所有するユーザ ID および、メッセージングシステムで所有するユーザの電子メールアカウント情報）に対してデータソースの信頼性を強化することができます。

Identity Manager によって、SAP*、PeopleSoft*、Lotus Notes*、Microsoft* Exchange、Active Directory* などのアプリケーションから次の処理を実行することができます。

- ◆ 識別ボールド (Novell eDirectory™) とデータを共有する。
- ◆ アプリケーションデータベース内で共有データが変更された場合、そのデータを識別ボールドと同期化して変換する。
- ◆ 識別ボールド内で共有データが変更された場合、そのデータをアプリケーションデータベースと同期化して変換する。

Identity Manager は、双方向のフレームワークを提供することでこれを実現しています。このフレームワークにより、管理者は、どのデータを識別ボールドからアプリケーションに適用し、どのデータをアプリケーションから識別ボールドに適用するかを指定できます。このフレームワークは、XML を使用してデータとイベントの変換機能を備えており、これによって識別ボールドのデータとイベントを指定されたアプリケーション固有の形式に変換します。さらに、アプリケーション固有の形式を識別ボールドが解釈できる形式に変換する処理も行います。アプリケーションとの対話はすべてアプリケーションのネイティブ API を使用して実行されます。

Identity Manager では、関連するアプリケーション固有のレコードとフィールドに対応した eDirectory の属性とクラスのみを選択できます。たとえば、eDirectory データベースでユーザタイプのオブジェクトを人事データベースと共有し、サーバ、プリンタ、ボリュームタイプなどのネットワークリソースオブジェクトは共有しないように選択できます。同様に、人事データベースではユーザの名前、名刺、イニシャル、電話番号、および勤務地を eDirectory と共有できますが、ユーザの家族情報と職歴は共有できません。

他のアプリケーションと共有するデータのクラスまたは属性が eDirectory にない場合は、eDirectory のスキーマを拡張してこれらを含めることができます。この場合、eDirectory は、eDirectory では必要なくても他のアプリケーションからは使用できる情報のリポジトリとなります。アプリケーションだけが必要とする情報のリポジトリは、アプリケーション固有のデータベースで維持されます。

Identity Manager が実行するタスクは次のとおりです。

- ◆ イベントを使用して識別ボールド内の変更を取得する。
- ◆ すべてのデータを一括して取得するハブとして機能することによって、データを集中管理または分散管理する。
- ◆ ディレクトリデータを XML 形式で開示し、XML アプリケーション、または Identity Manager で統合されたアプリケーション間でデータの使用 / 共有を可能にする。
- ◆ システムで定義されたデータ要素を管理する固有のフィルタを使ってデータフローを制御する。
- ◆ 許可とフィルタを使って承認されたデータソースを使用する。
- ◆ XML 形式のディレクトリデータにルールを適用する。これらのルールは、Identity Manager エンジン経由でデータ変更が反映される際のデータの変換を制御しています。
- ◆ データを XML 形式から任意のデータ形式に変換する。これによって、Identity Manager はあらゆるアプリケーションとデータを共有することができます。
- ◆ 識別ボールドのオブジェクトと他の統合システム内のオブジェクトの関連付けを厳密に管理し、データの変更がすべての統合システムに適切に反映されるようにする。

Identity Manager を使用すると、人事プロセスの簡素化、データ管理コストの削減、高度にカスタマイズされたサービスによる顧客関係の構築、および成功の妨げとなる相互運用性上の障害の排除を実現できます。次に、Identity Manager が実現するアクティビティの例を示します。

アクティビティ	Identity Manager によるソリューション
ユーザアカウントの管理	1 回の操作で次の処理を実行できます。 Identity Manager は即時に従業員のリソースへのアクセスを許可または削除します。 Identity Manager が備える自動従業員プロビジョニング機能により、新しい従業員に、ネットワーク、電子メール、アプリケーション、リソースなどへのアクセスが付与されます。 Identity Manager は、退職時または休暇時にアクセスを制限または無効化することもできます。
備品インベントリの追跡と統合	Identity Manager は、すべての備品インベントリ項目（コンピュータ、モニター、電話、ライブラリリソース、椅子、机など）のプロファイルを eDirectory に追加し、これらを個人、部門、組織などのユーザプロファイルと統合できます。
ホワイト / イエローページディレクトリの自動化	Identity Manager は、社内用と社外用に異なるレベルの情報を持つ統合ディレクトリを作成できます。社外ディレクトリには電子メールアドレスのみを含め、社内ディレクトリには勤務地、電話番号、Fax 番号、携帯番号、自宅住所などを含めることができます。
ユーザプロファイルの拡張	Identity Manager は、電子メールアドレス、電話番号、自宅住所、初期設定、社内の所属組織、ハードウェア備品、電話、キー、インベントリなどの情報を追加または同期化することによって、ユーザプロファイルを強化します。

アクティビティ	Identity Manager によるソリューション
通信アクセスの統合	Identity Manager は、個々のユーザまたはグループのネットワーク、電話、ポケットベル、またはワイヤレスアクセスのディレクトリを共通管理インタフェースと同期化することによって、これらのアクセスを簡素化します。
パートナー関係の強化	Identity Manager は、ファイアウォールの外部にパートナーシステムにプロファイル（従業員や顧客など）を作成して、パートナーが必要に応じて即座にサービスを提供できるようにすることにより、パートナーシップを強化します。
サプライチェーンの強化	Identity Manager は、顧客ごとに複数あるアカウントを認識して統合することによって、顧客サービスを向上させます。
顧客ロイヤルティの構築	Identity Manager では、これまで使用されることなく孤立して保存されていたデータをまとめて表示できるため、顧客ニーズを認識して新しいサービスを提供できます。
サービスのカスタマイズ	Identity Manager は、関係、ステータス、サービスレコードなど、同期化された情報をすべて備えたプロファイルユーザ（従業員、顧客、パートナーなど）に提供します。 これらのプロファイルを使用して、サービスと情報へのさまざまなレベルのアクセスを設定したり、顧客の立場に基づいて、カスタマイズされたサービスをリアルタイムに提供したりできます。

Identity Manager 2 の新機能

この節では、次の項目について説明します。

- ◆ 15 ページの「ポリシーを作成するための Policy Builder のインタフェースと DirXML Script」
- ◆ 16 ページの「パスワードの管理」
- ◆ 16 ページの「Role-Based Entitlement（役割ベースのエンタイトルメント）」
- ◆ 17 ページの「Novell Nsure Audit を使用したレポートिंगと通知」
- ◆ 17 ページの「グローバル設定値」
- ◆ 18 ページの「ドライバのハートビート」
- ◆ 18 ページの「ドライバ設定をインポートする際の柔軟なプロンプト」

ポリシーを作成するための Policy Builder のインタフェースと DirXML Script

DirXML の以前のリリースでは、ドライバ設定で 사용되는ポリシーは、ルールオブジェクトおよびスタイルシートオブジェクトと呼ばれていました。Identity Manager 2 では、ドライバ設定の各部分をポリシーオブジェクトと呼び、個々のルールはこれらのポリシーに含まれます。

一般的なタスクでは、新しい Policy Builder インタフェースを使用することで、XSLT コードを記述せずにドライバのポリシーを作成できるようになりました。Policy Builder では、新しい DirXML Script を使用して 25 個の一般的なルールを設定できます。詳細については、93 ページの「ポリシーの作成」を参照してください。

このリリースには、新しい条件、アクション、および値を持つ Policy Builder の拡張機能を含みます。統合されたクリップボード、XML ポリシーをインポート、エクスポート、および参照する機能など多くの新機能が Policy Builder に追加されています。詳細については、『*Policy Builder とドライバカスタマイズガイド* (<http://www.novell.com/documentation/dirxml20/policies/data/front.html#bktitle>)』を参照してください。

パスワードの管理

Identity Manager 2 は、次のような新しい強化されたパスワード管理機能を備えています。

- ◆ 新しい Password Policy (パスワードポリシー) では、パスワードのルールを作成して、ユーザ、コンテナ、または eDirectory ツリー全体に割り当てることができます。ユニバーサルパスワードを有効にすると、パスワードに詳細な条件を設定したり、特殊文字を使用できるように設定したりできます。
- ◆ Identity Manager パスワード同期はクロスプラットフォーム対応になり、接続システム全体に Password Policy (パスワードポリシー) を適用できるようになりました。新しい通知テンプレートを使用すると、パスワード同期ステータスに関するメッセージをユーザに自動的に送信できます。
- ◆ Password Policy (パスワードポリシー) を使用して、パスワードを忘れた場合のセルフサービスおよびパスワードのリセットセルフサービスをユーザに提供することもできます。これらの新しい機能により、ヘルプデスクへの問い合わせを削減できます。また、忘れたパスワードやパスワードのヒントを記載したメッセージをユーザに自動送信する通知テンプレートも追加されています。

詳細については、7 章 95 ページの、「Password Policy (パスワードポリシー) を使用したパスワードの管理」および 9 章 151 ページの、「接続システム間のパスワード同期」を参照してください。

Role-Based Entitlement (役割ベースのエンタイトルメント)

Role-Based Entitlement (役割ベースのエンタイトルメント) により、Novell eDirectory ユーザのグループに、接続システムへのエンタイトルメントを付与できます。Entitlement Policy (エンタイトルメントポリシー) を使用して、ビジネスポリシーの管理を簡素化し、DirXML ドライバを設定する必要性を低減できます。

Role-Based Entitlement (役割ベースのエンタイトルメント) は、Identity Manager を管理するもう 1 つの方法です。この方法は、集中型の Identity Manager 管理モデルが必要な場合に使用できます。

Entitlement Policy (エンタイトルメントポリシー) は、接続システムに対する機能が追加された eDirectory ダイナミックグループオブジェクトです。Entitlement Policy (エンタイトルメントポリシー) を作成する場合は、ポリシーのメンバーシップと、Entitlement (エンタイトルメント) のメンバーに付与するエンタイトルメントを定義してください。

Role-Based Entitlement (役割ベースのエンタイトルメント) により、接続システムへのエンタイトルメント、および eDirectory 内の権利を付与できます。接続システムへのエンタイトルメントには、次のいずれにも設定できます。

- ◆ 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
- ◆ カスタマイズする接続システムに対するその他のエンタイトルメント

Role-Based Entitlement (役割ベースのエンタイトルメント) 機能は Identity Manager に基づくため、接続システムを管理できるようにするには、DirXML ドライバをインストールして適切に設定する必要があります。さらに、Entitlement Policy (エンタイトルメントポリシー) の割り当てと DirXML ドライバ設定の衝突を避けるために、ビジネスポリシーと、Identity Manager でビジネスポリシーを管理する方法も理解しておく必要があります。

Novell Nsure Audit を使用したレポーティングと通知

Identity Manager 2 では、レポーティングおよび通知のサービスに Novell Nsure Audit を使用できるようになりました。Novell Nsure Audit はクロスプラットフォーム環境に対応した集中監査サービスです。このサービスは、複数のプラットフォームにおいて複数のアプリケーションからイベントデータを収集し、単一の否認防止データストアに書き込みます。また、Nsure Audit では、フィルタ処理されたデータストアを作成することもできます。Nsure Audit は、ユーザの定義した条件に基づいて特定タイプのイベントを取得して、2 次データストアに書き込みます。

Nsure Audit コンポーネントがバージョン 1.0.2 にアップデートされています。このバージョンには、クエリとレポーティングを強化する追加イベントフィールド、および大容量の XML ドキュメントを格納するための拡張データフィールドがあります。詳細については、[13 章 269 ページの「Nsure Audit によるログとレポート」](#)を参照してください。

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、エンジンは引き続き RNS 機能を処理します。Nsure 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 Identity Manager の今後のリリースではサポートされなくなるため、Nsure Audit への移行を計画することをお勧めします。RNS のドキュメントについては、『[DirXML 1.1a Administration Guide \(DirXML 1.1a 管理ガイド\)](#) (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html>)』を参照してください。

グローバル設定値

グローバル設定値 (GCV) は、ドライバパラメータに似た新しい設定です。グローバル設定値は、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。ドライバが特定の GCV の値を持たない場合、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、パスワード同期などの新しい機能の設定や、個々のドライバ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、ドライバ設定を容易にカスタマイズできます。

詳細については、[80 ページの「グローバル設定値の使用」](#)を参照してください。

ドライバのハートビート

DirXML エンジンにはドライバからドライバハートビートドキュメントを受け付けるようになり、ハートビートを送信するようにドライバを設定できます。

詳細については、91 ページの「[ドライバハートビートの追加](#)」を参照してください。

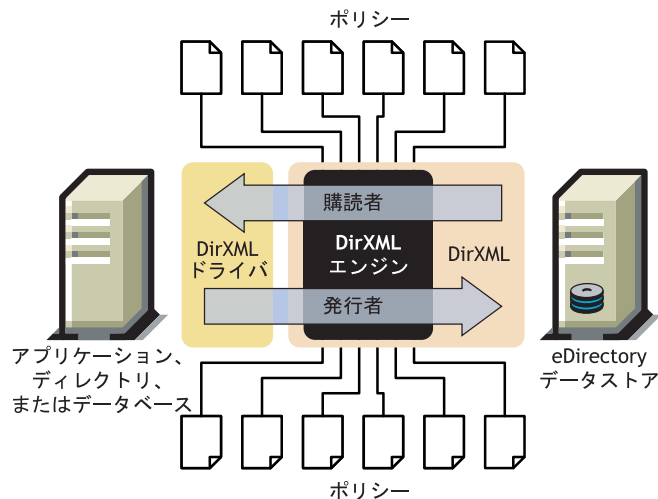
ドライバ設定をインポートする際の柔軟なプロンプト

多くのサンプルドライバ設定では新しい機能である柔軟なプロンプトが採用され、設定をインポートする際の複雑さが軽減されています。たとえば、インポートの初期画面でプロンプトを表示して、リモートローダや Role-Based Entitlement（役割ベースのエンタイトルメント）などの機能を使用するかどうかを選択できます。[yes] を選択した場合は、ウィザードにインポートプロンプトの別のページを表示して、選択した機能に関する追加の情報を提供できます。

Identity Manager のアーキテクチャの概要

Identity Manager テクノロジーは複数の異なるコンポーネントで構成されています。その主な目的は、識別ポータルと任意のアプリケーション、ディレクトリ、またはデータベース間でデータを適切に移動できるようにすることです。このために、Identity Manager にはディレクトリデータとイベントを XML 形式に変換する洗練されたインタフェースが用意されています。このインタフェースによって、eDirectory との間でデータを双方向にやり取りできます。

次の図は、Identity Manager の基本コンポーネントとそれらの関係を示します。



DirXML エンジンには 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、DirXML ドライバが eDirectory と情報を同期化できるインタフェースを提供し、異なるデータシステムを接続してデータを共有できるようにします。

DirXML エンジンには XML 形式を使って eDirectory データや eDirectory イベントを開示します。DirXML エンジンにはルールプロセッサとデータ変換エンジンを採用し、2つのシステム間のデータフローを操作しています。

eDirectory は、初期化時に次の処理を実行します。

1. すべての DirXML ドライバのフィルタを読み込みます。
2. 適切な eDirectory 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 eDirectory イベントのキャッシュを設定します。

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 eDirectory 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 DirXML エンジンに送信します。エンジンはアプリケーションドライバに設定されたポリシー (Mapping (マッピング)、Matching (一致)、Placement (配置)、Create (作成)、Transformation (変換)、Style Sheets (スタイルシート) など) を確認し、それによって XML 形式のデータを作成し、アプリケーションドライバに送信します。次に変換したデータをアプリケーションに送信し、その後正常に完了した旨のコードを受け取るまでの間データ更新を監視します。

ドライバの発行者部は、外部アプリケーションデータベースの更新情報の収集と、それらの情報の識別ポルトへの送信を担当しています。2つのデータベース間で共有している情報の変更がアプリケーションドライバに通知されると、ドライバはそれらの情報を収集し、フィルタに適合したデータ群かどうかを確認した後 DirXML 形式に変換してエンジンに送信します。

DirXML エンジン

DirXML エンジンは、Join エンジンと呼ばれることもあり、NDS[®] インタフェースと Join エンジンという2つのコンポーネントに分けることができます。

NDS インタフェース

DirXML エンジンに組み込まれた NDS 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。NDS インタフェースでは複数のドライバをロードできるため、Identity Manager のインスタンスが1つしか実行されていなくても複数のアプリケーションと通信できます。eDirectory とアプリケーション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、個々のアプリケーション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。

Join エンジン

Join エンジンは、Identity Manager に提供される各イベントに XML ベースのルール (XDS) を適用します。Identity Manager ルールは XSLT (Extensible Stylesheet Language Transformation) 形式でも記述できます。XSLT は、XML ドキュメントを操作して変換するために定義された、より強力な XML ボキャブラリです。

Join エンジンは各タイプのルール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。データは eDirectory と個々のアプリケーション間で共有されているため、リアルタイムで変換されます。

DirXML ドライバシム

DirXML ドライバシムは、通常はドライバと呼ばれ、eDirectory とアプリケーション、ディレクトリ、またはデータベースの間で情報を転送するルートのことです。DirXML 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 ドキュメントを使用して処理されます。

シムは Java* または C++ のいずれかで記述されます。

ドライバ設定ファイル

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

これらのドライバ設定にはサンプルポリシーが含まれます。これらは運用環境での使用を目的としたものではなく、ユーザが変更するテンプレートとして提供されています。

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ないようにしています。

Identity Manager のコンポーネント

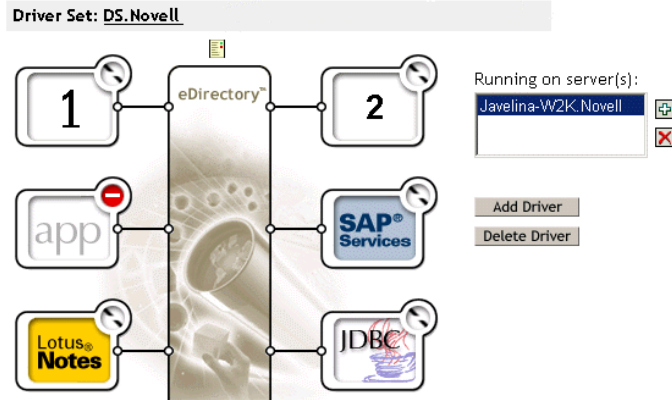
この節では、Identity Manager の概念と、Identity Manager を構成する各コンポーネントについて説明します。

ドライバセット

ドライバセットは DirXML ドライバを保持するコンテナです。1 つのサーバで同時にアクティブにできるドライバセットは 1 つだけです。このため、アクティブな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。ドライバセットを使用しているすべてのサーバで、ドライバセット内のドライバすべてを有効にする必要はありません。

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いずれかの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。これは、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が移動されないようにするためです。

次のイメージは、iManager 内のドライバセットを表します。



iManager の [Overview] ページ（上記）から、次の操作を実行できます。

- ◆ 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

ドライバオブジェクト

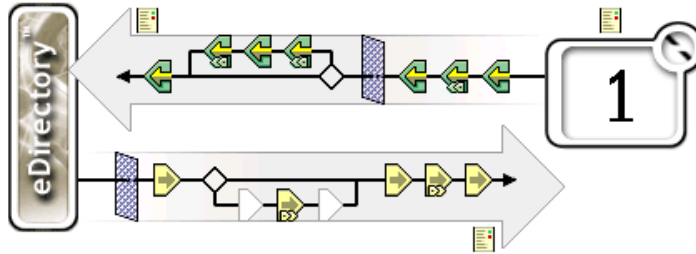
ドライバオブジェクトは、eDirectory に統合されるアプリケーションに接続するドライバを表します。次のコンポーネントは、ドライバオブジェクトとその設定パラメータを構成しています。

- ◆ 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加入者チャンネルオブジェクト。
- ◆ 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、加入者オブジェクト、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。シムはこれを使用してシムのリモート部分を認証できます。
- ◆ サポートされているディレクトリまたはアプリケーションに接続し、これを認証するために使用される認証パラメータ。
- ◆ 次を含む、ドライバの起動オプション。
 - ◆ Disabled - ドライバは実行されません。
 - ◆ Manual - ドライバは iManager を介して手動で起動する必要があります。
 - ◆ Auto start - ドライバは eDirectory の起動時に自動的に起動します。

- ◆ Schema Mapping Policy (スキーママッピングポリシー) の参照
- ◆ サポートされているアプリケーションまたはディレクトリのスキーマの XML 表現。
通常、これはシムによってアプリケーションまたはディレクトリから自動的に取得されます。

iManager では、[DirXML Driver Overview] を表示し、既存のドライバパラメータ、ルール、およびスタイルシートを変更できます。[DirXML Driver Overview] を次に示します。

Driver: 1.D5.Novell



また、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する、eDirectory の十分な権利を付与する必要があります。このためには、ドライバオブジェクトを、ドライバが同期化する eDirectory オブジェクトのトラステイにするか、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。

権利の割り当てについては、『*Novell eDirectory 8.7.3 管理ガイド*』の「[eDirectory 権利 \(http://www.novell.com/documentation/lg/edir87/edir87/data/fbachifb.html\)](http://www.novell.com/documentation/lg/edir87/edir87/data/fbachifb.html)」を参照してください。

ドライバシム

ドライバシムは、アプリケーション、ディレクトリ、またはデータベースと eDirectory 間における情報のルートとして機能します。シムは Java*、C、または C++ のいずれかで記述されます。

DirXML エンジンとドライバシムは、イベント、クエリ、および結果を記述する XML ドキュメントの形式で通信します。

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

また、Identity Manager が同期化されたアプリケーション、ディレクトリ、またはデータベース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する必要があります。

eDirectory で、同期化されたアプリケーションまたはディレクトリでアクションを引き起こすイベントが発生すると、Identity Manager は、その eDirectory イベントを記述する XML ドキュメントを作成し、加入者チャネルを介してドライバシムに送信します。

同期化されたアプリケーション、ディレクトリ、またはデータベースにイベントが発生すると、イベントシムはそのアプリケーションイベントを記述する XML ドキュメントを生成します。続いて、ドライバシムがその XML ドキュメントを発行者チャネルを介して Identity Manager に送信します。Identity Manager は、アプリケーションルール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 eDirectory に指示します。

発行者チャネルと加入者チャネル

DirXML 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加入者チャネルという 2 つのチャネルがあります。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。

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。要素がドライバに送信される場合、その要素はコマンドです。要素が Identity Manager に送信される場合、その要素はイベント通知です。ドライバは、Identity Manager にイベント通知を送信する際に、アプリケーションで発生した変更を Identity Manager に通知します。Identity Manager は、設定可能なルールに基づいて、どのコマンドを eDirectory に送信する必要があるかを決定します（コマンドが必要な場合）。

Identity Manager は、ドライバにコマンドを送信する場合、すでに eDirectory 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、コマンドが表すアプリケーション内の変更が必要であると判断しています。

ポリシーとフィルタ

ポリシーとフィルタによって、ユーザはシステム間のデータフローを制御できます。ポリシーとフィルタの詳細については、『*Policy Builder とドライバカスタマイズガイド* (<http://www.novell.com/documentation/lg/dirxml20/policies/data/boswupw.html>)』を参照してください。

関連付け

他のほとんどの識別情報管理製品では、アプリケーションからディレクトリにオブジェクトをマップするために、接続されたアプリケーションに何らかの識別子を格納する必要があります。Identity Manager では、アプリケーションの変更は必要ありません。eDirectory の各オブジェクトには、接続されているディレクトリおよびアプリケーション内で固有の識別子を eDirectory オブジェクトにマップする関連付けテーブルが含まれています。この表はリバースインデックス形式なので、接続されたアプリケーションは、eDirectory の更新時に eDirectory 識別子（識別名など）を統合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、ネットワーク内の別のオブジェクトにまだ関連付けられていないオブジェクトに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ルールを作成できます。

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、Matching Policy（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。このためには、最低限の作成条件すべてに一致していないければなりません。これらの条件はCreate Policy（作成ポリシー）によって定義されます。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Placement Policy（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として
- ◆ 特定場所内のオブジェクトの新しい作成として

形成されたオブジェクト間の関連付けは、eDirectory 管理者がオブジェクトを作成するか、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 を初めてインストールすると、NetWare[®] および Windows* NT*/2000 では eDirectory スキーマが拡張されます。Solaris* または Linux* を使用している場合、スキーマは自動的に拡張されません。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ています。この属性が関連付けテーブルです。関連付けテーブルは、eDirectory オブジェクトがリンクされているすべての外部アプリケーション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維持されるため、この情報を手動で編集する必要はほとんどありません。

2 計画

この節では、次の項目について説明します。

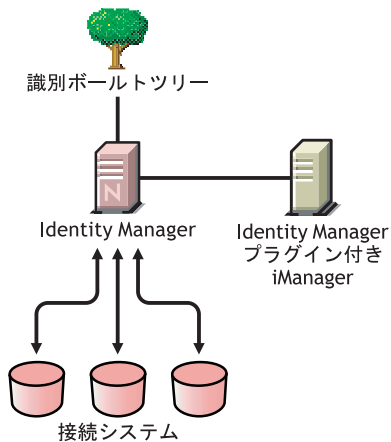
- ◆ 25 ページの「一般的なインストールシナリオ」
- ◆ 33 ページの「Identity Manager 実装のプロジェクト管理面の計画」
- ◆ 39 ページの「Identity Manager 実装の技術面の計画」

一般的なインストールシナリオ

次のシナリオは、Identity Manager の使用環境の例です。各シナリオに対して、実装に役立つガイドラインをいくつか示します。

- ◆ 25 ページの「Identity Manager の新しいインストール」
- ◆ 27 ページの「同一環境での Identity Manager と DirXML 1.1a の使用」
- ◆ 29 ページの「Starter Pack から Identity Manager へのアップグレード」
- ◆ 31 ページの「Password Synchronization 1.0からIdentity Managerパスワード同期へのアップグレード」

Identity Manager の新しいインストール



Nsure™ Identity Manager は、識別ポールドツリーを利用して、アプリケーション、データベース、およびディレクトリ全体で情報を自動的に同期化、変換、配布するデータ共有ソリューションです。

Identity Manager ソリューションには次のコンポーネントが含まれます。

Identity Manager の識別ポータルツリー

識別ポータルツリーには、接続された他のシステムと共有または同期化するユーザーデータやオブジェクトデータが格納されます。Identity Manager を独自のツリーにインストールし、これを識別ポータルとして使用することをお勧めします。

iManager サーバと Identity Manager プラグイン

Identity Manager ソリューションを管理するには、Novell® iManager と Identity Manager プラグインを使用します。

接続システム

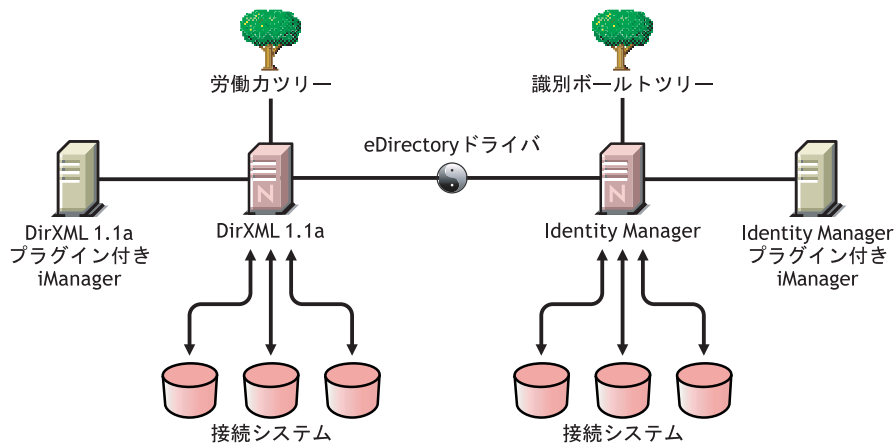
接続システムには、識別ポータルとデータを共有または同期化する他のアプリケーション、ディレクトリ、およびデータベースなどを含めることができます。識別ポータルから接続システムへの接続を確立するには、接続システムに適切なドライバをインストールします。詳細な手順については、[ドライバ実装に関するガイド \(http://www.novell.com/documentation/dirxmldrivers/index.html\)](http://www.novell.com/documentation/dirxmldrivers/index.html) を参照してください。

Identity Manager の一般的なタスク

- ◆ **システムコンポーネントのインストール** - Identity Manager ソリューションは複数のコンピュータ、サーバ、またはプラットフォームに分散される場合があるため、インストールプログラムを実行して、各システムに対して適切なコンポーネントをインストールする必要があります。詳細については、[48 ページの「Identity Manager のコンポーネントとシステム要件」](#)を参照してください。
- ◆ **接続システムの設定** - 詳細な手順については、[48 ページの「Identity Manager のコンポーネントとシステム要件」](#)および『[ドライバ実装に関するガイド \(http://www.novell.com/documentation/dirxmldrivers/index.html\)](#)』を参照してください。
- ◆ **製品のアクティベート** - Identity Manager 製品 (Professional または Server Edition、およびドライバグループ) は、インストール後 90 日以内にアクティベートする必要があります。[281 ページの付録 A、「Novell Identity Manager 製品のアクティベーション」](#)を参照してください。
- ◆ **ビジネスポリシーの定義** - ビジネスポリシーにより、Novell eDirectory™ との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。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の多くのタスクも実行できます。ポリシーの詳細な説明については『[Policy Builder とドライバカスタマイズガイド](#)』を参照してください。
- ◆ **パスワードの管理の設定** - Password Policy (パスワードポリシー) を使用すると、ユーザーのパスワード作成方法にルールを設定してセキュリティを強化できます。また、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスのオプションをユーザーに提供して、ヘルプデスクのコストを削減することもできます。パスワードの管理の詳細については、[7 章 95 ページの、「Password Policy \(パスワードポリシー\) を使用したパスワードの管理」](#)を参照してください。

- ◆ **Role-Based Entitlement (役割ベースのエンタイトルメント)の設定** - Role-Based Entitlement (役割ベースのエンタイトルメント)により、接続システムへのエンタイトルメントを Novell eDirectory ユーザのグループに付与できます。Entitlement Policy (エンタイトルメントポリシー)の使用により、ビジネスポリシーの管理を簡素化し、DirXML ドライバを設定する必要性を低減できます。詳細については、10 章 237 ページの、「**Role-Based Entitlement (役割ベースのエンタイトルメント)**」を参照してください。
- ◆ **Nsure Audit によるイベントのロギング** - Nsure Identity Manager は、監査とレポートに Novell Nsure を使用するように用意されています。Nsure Audit は、監視、ログ、レポート、および通知の機能を実行するテクノロジーを1つにまとめたものです。Identity Manager を Nsure Audit と統合すると、ドライバとエンジンアクティビティについて現在および過去のステータスに関する詳細な情報が提供されます。この情報は、事前設定済みのレポート、標準通知サービス、およびユーザ定義ログのセットによって提供されます。13 章 269 ページの、「**Nsure Audit によるログとレポート**」を参照してください。

同一環境での Identity Manager と DirXML 1.1a の使用



Identity Manager と DirXML[®] 1.1a の両方を同じ環境で実行する場合は、次の点に注意してください。

識別ポールの作成

- ◆ Identity Manager を別のツリーにインストールし、これを識別ポータルとして使用することをお勧めします。

管理ツール

- ◆ ConsoleOne[®] は、DirXML 1.1a ではサポートされていますが、Identity Manager ではサポートされていません。
- ◆ DirXML 1.1a プラグインと Identity Manager プラグインに1つずつ、2つの iManager サーバが必要です。これは、プラグインが強化されていることと、Identity Manager ドライバは DirXML Script を使用しているためです。
- ◆ DirXML 1.1a 用の iManager プラグインは、ほとんどの Identity Manager ドライバのサンプルドライバ設定で使用されている DirXML Script を読み込むことができません。

後方互換性

- ◆ Identity Manager サーバ上で DirXML 1.1a ドライバシムと設定を実行し、ドライバセットの DirXML Overview で iManager 内のドライバを表示できます。ただし、Identity Manager プラグインでは、Identity Manager の形式に変換しない限り、ドライバ設定は表示または編集できません。

Identity Manager プラグインでは、1.1a 形式のドライバをクリックすると、変換を求めるメッセージが表示されます。このプロセスはウィザードを使用して簡単に実行でき、ドライバ設定の機能は変更されません。このプロセスの一部として、DirXML 1.1a バージョンのバックアップコピーが保存されます。

- ◆ DirXML 1.x ドライバのアクティベーションは、Identity Manager エンジンでドライバを実行する場合には引き続き有効です。ただし、ドライバシムを Identity Manager バージョンにアップグレードした場合は、新しいアクティベーションが必要です。
- ◆ ほとんどの場合、Identity Manager ドライバシムは DirXML 1.1a 設定で実行できます。アップグレードの情報については、個々の [ドライバ実装に関するガイド](http://www.novell.com/documentation/dirxml/drivers/index.html) (<http://www.novell.com/documentation/dirxml/drivers/index.html>) を参照してください。

ただし、AD と NT は例外で、ドライバシムをアップグレードすると、追加ドライバポリシーをいくつか追加しない限り Password Synchronization 1.0 は正しく動作しないので注意してください。手順については、Active Directory および NT ドメイン用 DirXML ドライバの [ドライバ実装に関するガイド](http://www.novell.com/documentation/dirxml/drivers/index.html) (<http://www.novell.com/documentation/dirxml/drivers/index.html>) のパスワード同期に関する節を参照してください。

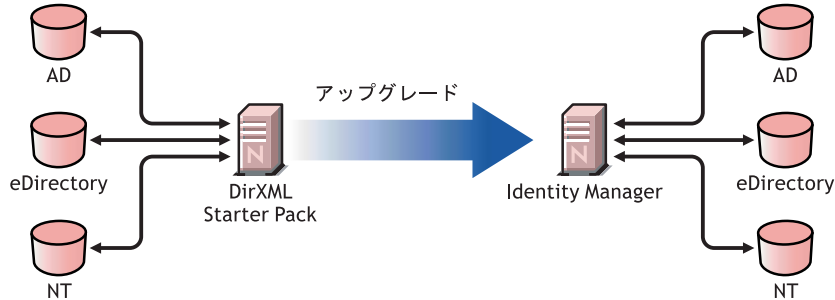
- ◆ Identity Manager ドライバシムとドライバ設定を DirXML 1.1a エンジンで実行することはできません。
- ◆ Identity Manager ドライバ設定を DirXML 1.1a ドライバシムで実行することはできません。
- ◆ 複数のサーバで同じ DirXML ドライバ設定を実行する場合は、これらのサーバで同じバージョンの DirXML または Identity Manager、および同じバージョンの eDirectory が実行されていることを確認してください。

パスワードの管理

- ◆ より強固なパスワードを要求する Advanced Password Rules (詳細パスワードルール)、パスワードを忘れた場合のセルフサービス、パスワードのリセットセルフサービスなどの機能をユーザに提供する Password Policy (パスワードポリシー) を作成できます。7 章 95 ページの、「[Password Policy \(パスワードポリシー\) を使用したパスワードの管理](#)」と 8 章 115 ページの、「[パスワードセルフサービス](#)」を参照してください。
- ◆ NetWare 6.5 の初期リリースでユニバーサルパスワードの使用を開始する場合は、新しい Password Policy (パスワードポリシー) 機能を使用する前に、いくつかのアップグレード手順が必要です。108 ページの「[\(NetWare 6.5 のみ\) ユニバーサルパスワード割り当ての再作成](#)」を参照してください。この手順は、NetWare 6.5 SP2 でユニバーサルパスワードの使用を開始する場合には必要ありません。
- ◆ Identity Manager パスワード同期では、双方向パスワード同期が提供されており、Password Synchronization 1.0 よりも多くのプラットフォームがサポートされています。

- ◆ ADまたはNTでPassword Synchronization 1.0を使用している場合は、新しいドライバシムをインストールする前にアップグレード手順を確認してください。31 ページの「Password Synchronization 1.0からIdentity Managerパスワード同期へのアップグレード」を参照してください。
- ◆ 既存のドライバに双方向パスワード同期機能を追加するのに役立つドライバポリシー「オーバーレイ」が用意されています。178 ページの「Identity Managerパスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。

Starter Pack から Identity Manager へのアップグレード



その他の Novell 製品に付属する DirXML Starter Pack ソリューションでは、NT ドメイン、Active Directory、および eDirectory に格納されている情報のライセンス同期が提供されています。さらに、PeopleSoft*、GroupWise®、Lotus Notes* などのシステムについては評価版ドライバが付属しており、システムのデータ同期化を調査できます。

また、このソリューションには、ユーザパスワードを同期化する機能も用意されています。PasswordSync では、1つのパスワードを覚えておけばどのシステムにもログインできます。管理者はどのシステムからでもパスワードを管理できます。いずれかの環境でパスワードを変更すると、すべての環境でそのパスワードが更新されます。

NetWare 6.5 および Nenterprise Linux Services 1.0 に付属していた DirXML Starter Pack は、DirXML 1.1a テクノロジーに基づいています。Starter Pack を Identity Manager の最新バージョンにアップグレードする場合は、次の点に注意してください。

管理ツール

- ◆ ConsoleOne は、DirXML 1.1a ではサポートされていますが、Identity Manager ではサポートされていません。

後方互換性

- ◆ Identity Manager サーバ上で DirXML 1.1a ドライバシムと設定を実行し、ドライバセットの DirXML Overview で iManager 内のドライバを表示できます。ただし、Identity Manager プラグインでは、Identity Manager の形式に変換しない限り、ドライバ設定は表示または編集できません。

Identity Manager プラグインでは、1.1a 形式のドライバをクリックすると、変換を求めるメッセージが表示されます。このプロセスはウィザードを使用して簡単に実行でき、ドライバ設定の機能は変更されません。このプロセスの一部として、DirXML 1.1a バージョンのバックアップコピーが保存されます。

- ◆ DirXML 1. x ドライバのアクティベーションは、Identity Manager エンジンでドライバを実行する場合には引き続き有効です。ただし、ドライバシムを Identity Manager バージョンにアップグレードした場合は、新しいアクティベーションが必要です。
 - ◆ ほとんどの場合、Identity Manager ドライバシムは DirXML 1. 1a 設定で実行できません。アップグレードの情報については、個々の **ドライバ実装に関するガイド** (<http://www.novell.com/documentation/dirxmldrivers/index.html>) を参照してください。
- ただし、AD と NT は例外で、ドライバシムをアップグレードすると、追加ドライバポリシーをいくつか追加しない限り Password Synchronization 1. 0 は正しく動作しないので注意してください。手順については、Active Directory および NT ドメイン用 DirXML ドライバの **ドライバ実装に関するガイド** (<http://www.novell.com/documentation/dirxmldrivers/index.html>) のパスワード同期に関する節を参照してください。
- ◆ Identity Manager ドライバシムとドライバ設定を DirXML 1. 1a エンジンで実行することはできません。
 - ◆ Identity Manager ドライバ設定を DirXML 1. 1a ドライバシムで実行することはできません。
 - ◆ 複数のサーバで同じ DirXML ドライバ設定を実行する場合は、これらのサーバで同じバージョンの DirXML または Identity Manager、および同じバージョンの eDirectory が実行されていることを確認してください。

パスワードの管理

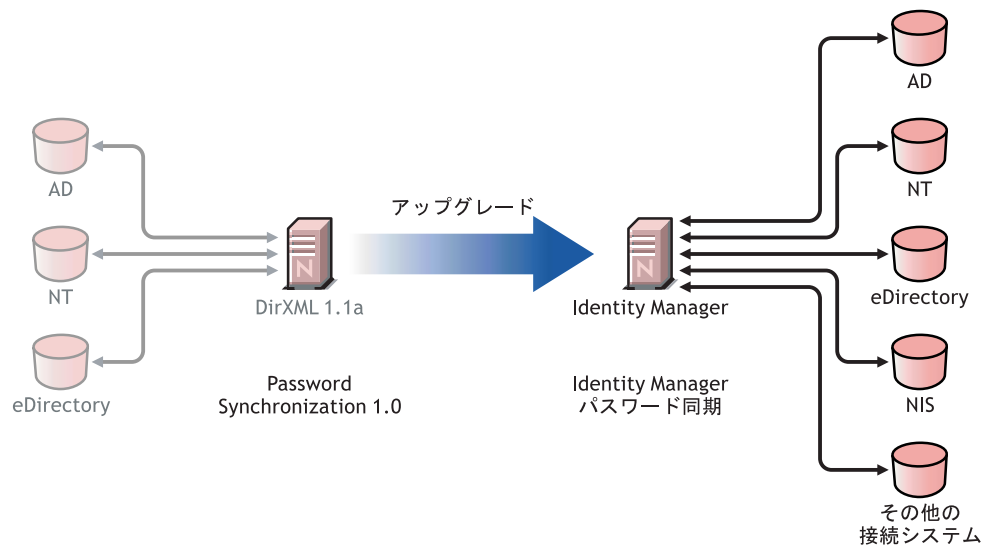
- ◆ ドライバをアップグレードすると、Starter Packs (DirXML 1. 1a) に付属する Password Synchronization 1. 0 は、追加ドライバポリシーをいくつか追加しない限り、AD と NT に対しては正しく動作しません。手順については、Active Directory および NT ドメイン用 DirXML ドライバの **ドライバ実装に関するガイド** (<http://www.novell.com/documentation/dirxmldrivers/index.html>) のパスワード同期に関する節を参照してください。
- ◆ このアップグレードプロセスに関する詳細な手順については、**31 ページの「Password Synchronization 1. 0 から Identity Manager パスワード同期へのアップグレード」**を参照してください。

アクティベーション

- ◆ Identity Manager と DirXML 製品はすべて 90 日以内にアクティベートする必要があります。その他の Novell ソフトウェアを購入した場合、DirXML 1. 1a エンジンと、NT、AD、および eDirectory 用ドライバのアクティベーションは、DirXML Starter Pack に含まれています。DirXML Starter Pack からアップグレードした場合は、これらのドライバにアクティベーション認証を再適用しなければならないことがあります。

アクティベーションの詳細については、**281 ページの付録 A、「Novell Identity Manager 製品のアクティベーション」**を参照してください。

Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード



Identity Manager パスワード同期には、双方向パスワード同期、追加プラットフォーム、パスワードの同期に失敗した場合の電子メール通知など、多くの機能が用意されています。

Active Directory または NT ドメインで Password Synchronization 1.0 を使用する場合、新しいドライバシムをインストールする前にアップグレード手順を確認することが非常に重要です。

Identity Manager パスワード同期の一般的な情報については、[9 章 151 ページの「接続システム間のパスワード同期」](#)を参照してください。新旧機能の比較、前提条件、各接続システムでサポートされている機能のリスト、既存のドライバにサポートを追加する手順、新機能を使用する方法を示したいくつかのシナリオなどの概念が記載されています。

この節では、次の項目について説明します。

- ◆ [31 ページの「AD または NT 用のパスワード同期のアップグレード」](#)
- ◆ [32 ページの「eDirectory 用のパスワード同期のアップグレード」](#)
- ◆ [32 ページの「その他の接続システムのドライバのアップグレード」](#)
- ◆ [33 ページの「機密情報の処理」](#)

AD または NT 用のパスワード同期のアップグレード

新しいパスワード同期機能は、別個のエージェントではなくドライバポリシーによって実行されます。つまり、ドライバ設定をアップグレードせずに新しいドライバシムをインストールした場合、Password Synchronization 1.0 は既存のユーザに対してのみ動作します。ドライバ設定のアップグレードを完了するまで、新しいユーザ、移動したユーザ、または名前変更されたユーザはパスワード同期に参加しません。

次の一般的な手順に従ってアップグレードしてください。

1. ユニバーサルパスワードをサポートするように現在の環境をアップグレードします。Novell Client を使用している場合は、そのアップグレードも行います。
2. Identity Manager ドライバシムをインストールして、AD または NT 用の DirXML 1. x ドライバシムを置換します。
3. 新しいポリシーをドライバ設定に追加して、ただちに Password Synchronization 1.0 との後方互換性を設定します。

この手順によって、Identity Manager パスワード同期に切り替えるまで、Password Synchronization 1.0 を引き続き正常に機能させることができます。

4. ドライバポリシーを使用して、新しい Identity Manager パスワード同期のサポートを追加します。
5. 新しいパスワード同期のフィルタをインストールして設定します。
6. 必要に応じて SSL を設定します。
7. 必要に応じて、Password Policy (パスワードポリシー) を使用してユニバーサルパスワードをオンにします。
8. 使用する Identity Manager パスワード同期のシナリオを設定します。

『*Novell Nsure Identity Manager 2 管理ガイド*』の「パスワード同期の実装」を参照してください。

9. Password Synchronization 1.0 を削除します。

Active Directory および NT ドメイン用 DirXML ドライバの詳細な手順については、[ドライバ実装に関するガイド \(http://www.novell.com/documentation/dirxmldrivers/index.html\)](http://www.novell.com/documentation/dirxmldrivers/index.html) を参照してください。

eDirectory 用のパスワード同期のアップグレード

eDirectory のアップグレードは簡単です。ドライバシムと設定に最新のパッチが適用されていれば、新しいドライバシムは、変更なしに既存のドライバ設定で動作します。アップグレード方法については、『*DirXML Driver for eDirectory Implementation Guide (eDirectory の DirXML ドライバ実装ガイド)* (<http://www.novell.com/documentation/dirxmldrivers/index.html>)』を参照してください。

その他の接続システムのドライバのアップグレード

Identity Manager パスワード同期は、Password Synchronization 1.0 よりも多くの接続システムをサポートします。

その他のシステムについてサポートされている機能のリストは、[159 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。

以前にサポートされていなかった接続システムに対しては、既存のドライバに双方向パスワード同期機能を追加するのに役立つドライバポリシー「オーバーレイ」が用意されています。[178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」](#)を参照してください。

機密情報の処理

ユニバーサルパスワードは、eDirectory 内では4層の暗号化によって保護されているため、非常に安全です。双方向パスワード同期を使用してユニバーサルパスワードを配布パスワードと同期化する場合は、eDirectory のパスワードを抽出して他の接続システムに送信することになります。パスワードの転送と同期先の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。168 ページの「機密情報の処理」を参照してください。

Identity Manager 実装のプロジェクト管理面の計画

この節では、Identity Manager の実装における計画およびプロジェクト管理上の高レベルな側面の概要について説明します（技術面については、39 ページの「Identity Manager 実装の技術面の計画」を参照してください）。

この計画用ドキュメントには、通常は Identity Manager プロジェクトの開始から完全な運用環境への展開までに行われるアクティビティのタイプが記載されています。識別情報管理戦略を実装するには、現在の環境におけるニーズと利害関係者を特定し、ソリューションを設計し、利害関係者の参画を得て、ソリューションをテストして導入する必要があります。この節は、このプロセスに関する十分な情報を読者に提供して、Identity Manager を使用することで最大限の利点が得られるようにすることを目的としています。

ソリューション展開の各フェーズを支援するために、Identity Manager のエキスパートを参加させることを強くお勧めします。パートナーシップのオプションの詳細については、Novell® Nsure™ ソリューションパートナーの Web サイト (<http://www.novell.com/solutions/nsure/partners>) を参照してください。Novell Education では、Identity Manager の実装に対応したコースも提供しています。

この節はすべての情報を網羅するものではありません。また、考えられる設定すべてを取り上げているわけではなく、その実行に限定したものでもありません。環境はそれぞれ異なるため、使用するアクティビティのタイプに応じた柔軟性が求められます。

Novell Identity Manager の展開

Identity Manager の展開時のベストプラクティスとしてお勧めするアクティビティはいくつかあります。

- ◆ 34 ページの「検出」
- ◆ 34 ページの「要件と設計の分析」
- ◆ 37 ページの「POC (Proof of Concept)」
- ◆ 38 ページの「データの検証と準備」
- ◆ 38 ページの「運用試験」
- ◆ 38 ページの「運用投入計画」
- ◆ 39 ページの「運用環境への展開」

検出

Identity Manager の実装は検出プロセスから開始でき、この検出プロセスによって次のことが可能になります。

- ◆ 識別情報を管理する主な目的を識別する
- ◆ 対処するビジネス上の問題を定義または明確化する
- ◆ 未解決の問題に対処するために必要なイニシアティブを決定する
- ◆ これらのイニシアティブの1つ以上を遂行するために何が必要かを決定する
- ◆ 高レベルな戦略または「ソリューションロードマップ」と、承認された実行パスを策定する

検出プロセスにより、すべての利害関係者が問題とソリューションに関して共通の理解を得ることができます。分析フェーズでは、利害関係者がディレクトリ、Novell eDirectory™、Novell Nsure Identity Manager、および XML 統合の基本知識を持っている必要があります。検出プロセスは、この分析フェーズに対する優れた手引きとなります。

- ◆ すべての利害関係者が基礎的なレベルの理解を得ることができる
- ◆ 利害関係者からビジネスおよびシステムに関する重要な情報を取得できる
- ◆ ソリューションロードマップの作成が可能になる

検出により、次のような直後の手順も特定されます。

- ◆ 要件および設計フェーズに備えて計画アクティビティを特定する
- ◆ 利害関係者に対する追加の教育を定義する

主な成果物

- ◆ ビジネスおよび技術上の主な利害関係者との構造化インタビュー
- ◆ ビジネスおよび技術上の課題に関する高レベルな概要レポート
- ◆ 次の手順についての推奨事項
- ◆ 検出の成果の概要を説明したエグゼクティブプレゼンテーション

要件と設計の分析

この分析フェーズでは、プロジェクトの技術的側面とビジネス的側面の両方を詳細に捉え、データモデルと高レベルな Identity Manager アーキテクチャ設計を生成します。このアクティビティは、ソリューションを実装する最初の重要な手順です。

設計の焦点は特に識別情報管理に置きますが、ファイルや印刷など、従来はリソース管理ディレクトリに関連付けられていたさまざまな要素に焦点を置くこともできます。次に、評価できる項目のサンプルを示します。

- ◆ 使用するシステムソフトウェアのバージョンは何か？
- ◆ ディレクトリの設計は適切か？
- ◆ すべてのシステムのデータの品質は適切か？（データが使用できる品質ではない場合、ビジネスポリシーが希望どおりに実装されない場合があります）

要件の分析が完了したら、実装の範囲とプロジェクト計画を設定し、前提条件アクティビティが必要かどうかを判断できます。大きなミスを防ぐために、情報の収集と要件の文書化をできるだけ徹底的に行ってください。

要件評価中に次のタスクを完了できます。

- ◆ 35 ページの「ビジネス要件の定義」
- ◆ 36 ページの「ビジネスプロセスの分析」
- ◆ 36 ページの「企業のデータモデルの設計」

ビジネス要件の定義

組織のビジネスプロセスと、これらのビジネスプロセスを定義する要件を収集します。

たとえば、従業員の退職に関するビジネス要件は、従業員のネットワークと電子メールアクセスを従業員の退職当日に削除するというものです。

次のタスクはビジネス要件の定義に役立ちます。

- ◆ プロセスフロー、プロセストリガ、およびデータマッピングの関係を確立する。
たとえば、あるプロセスで何かが発生した場合、そのプロセスが原因で何が発生しますか？ その他のどのようなプロセスがトリガされますか？
- ◆ アプリケーション間のデータフローをマップする。
- ◆ 2/25/2002 から 25 Feb 2002 への変換など、ある形式から別の形式にデータを変換するために必要な作業を特定する。
- ◆ 存在するデータ従属関係を文書化する。

特定の値を変更する場合、その値に対する従属関係があるかどうかを理解することが重要です。特定のプロセスを変更する場合は、そのプロセスに対する従属関係があるかどうかを理解することが重要です。

たとえば、人事システムで「臨時採用」という従業員ステータス値を選択した場合、IT 部門では、制限付き権利を持ち特定の時間帯にネットワークにアクセスできるユーザオブジェクトを eDirectory 内に作成しなければならないことがあります。

- ◆ 優先度をリストアップする。

すべての関係者のすべての要件、要求、および希望をすぐに満たすことができるとは限りません。プロビジョニングシステムの設計と展開の優先度は、ロードマップの計画に役立ちます。

展開を複数のフェーズに分割すると、展開の一部は前倒しで実装し、その他の部分は後で実装することもできるため、効果的な場合があります。

- ◆ 前提条件を定義する。

展開の特定フェーズの実装に必要な前提条件を文書化する必要があります。

- ◆ 認証されたデータソースを特定する。

システム管理者やマネージャが自身に属すると考えている情報を早い段階で把握しておく、すべての関係者から参画を得て維持するのに役立ちます。

たとえば、アカウント管理者には、特定のファイルとディレクトリに対する権利を従業員に付与する権利が必要となります。これは、アカウントシステムにローカルなトラスティ割り当てを実装することによって対応できます。

ビジネスプロセスの分析

多くの場合、ビジネスプロセスの分析は、マネージャ、管理者、従業員など、アプリケーションやシステムを実際に使用する個々の人物と話し合うことから始まります。対処すべき主な課題は次のとおりです。

- ◆ データが生成されるのはどこか？
- ◆ そのデータが送られるのはどこか？
- ◆ データに対する責任者はだれか？
- ◆ データを所有するビジネス機能の所有権を持っているのはだれか？
- ◆ データを変更する場合の連絡先はだれか？
- ◆ データの変更によってどのような影響があるか？
- ◆ データ処理（収集または編集、あるいはその両方）についてどのような作業手順があるか？
- ◆ どのような種類の操作を行うか？
- ◆ データの品質と整合性を確保するためにどのような方法を使用しているか？
- ◆ システムはどこにあるか（どの部署のどのサーバ）？
- ◆ 自動処理に適さないプロセスはどのようなものか？

たとえば、人事部の PeopleSoft システムの管理者には次のような質問を尋ねることができます。

- ◆ PeopleSoft データベースにはどのようなデータが格納されているか？
- ◆ 従業員のアカウントの各種パネルに何が表示されるか？
- ◆ プロビジョニングシステムに反映する必要があるアクションは何か（追加、変更、削除など）？
- ◆ これらのうち、どれが必須で、どれが必須でないか？
- ◆ PeopleSoft で実行されるアクションに基づいてトリガする必要があるアクションは何か？
- ◆ どの操作 / イベント / アクションを無視する必要があるか？

重要な人々へのインタビューによって、組織のどの部門であればプロセスの全体像を明確化できるかがわかります。

企業のデータモデルの設計

ビジネスプロセスを定義したら、現在のビジネスプロセスを反映したデータモデルの設計を開始できます。

このモデルには、データがどこで生成され、どこに送られるか、およびデータを移動できない場所を示す必要があります。また、重要なイベントがデータフローにどのように影響するかを考慮する必要もあります。

提案されたビジネスプロセスと、そのプロセスに自動プロビジョニングを実装することの利点を示した図を作成することもできます。

このモデルの開発は次のような質問に答えることから始めます。

- ◆ どのような種類のオブジェクト（ユーザやグループなど）を移動するか？
- ◆ どのイベントが重要か？
- ◆ どの属性を同期化する必要があるか？

- ◆ 管理するさまざまなオブジェクトのタイプについて、ビジネス全体でどのようなデータを保存するか？
- ◆ 同期化は一方向か、それとも双方向か？
- ◆ どのシステムがどの属性の認証されたソースか？

システム間のさまざまな値の相関関係を考慮することも重要です。

たとえば、PeopleSoft の「従業員ステータス」フィールドには、「従業員」、「契約社員」、および「研修社員」の 3 つの設定値があります。しかし、Active Directory システムには、「正社員」と「アルバイト」の 2 つの値しかありません。この状況では、PeopleSoft の「契約」ステータスと、Active Directory の「正社員」と「アルバイト」の値の関係を決定する必要があります。

この作業の焦点は、各ディレクトリシステムとこれらの相関関係、およびどのオブジェクトと属性をシステム間で同期化する必要があるかを理解することです。

主な成果物

- ◆ すべてのシステム、承認されたデータソース、イベント、情報フロー、およびデータ形式の標準を示すデータモデル
- ◆ ソリューションに適した Identity Manager アーキテクチャ
- ◆ 追加のシステム接続要件の詳細
- ◆ データ検証とレコード一致のための戦略
- ◆ Identity Manager インフラストラクチャをサポートするディレクトリ設計

従属関係

- ◆ すべての外部システムに精通したスタッフ（人事データベース管理者、ネットワークおよびメッセージングシステム管理者）
- ◆ システムスキーマとサンプルデータの提供
- ◆ 分析および設計フェーズからのデータモデル
- ◆ 組織図、WAN、サービインフラストラクチャなどの基本情報の提供

POC (Proof of Concept)

このアクティビティの成果とは、会社のビジネスポリシーとデータフローが反映された研究室環境にサンプル実装を実現することです。これは、要件分析と設計の際に作成されるデータモデルの設計に基づいており、運用試験前の最終手順です。

注：多くの場合、この手順は、経営陣から最終的な実装作業のためのサポートと資金を得るために有益です。

主な成果物

- ◆ すべてのシステム接続が動作可能な状態における Identity Manager の有効な POC

従属関係

- ◆ ハードウェアプラットフォーム
- ◆ 必要なソフトウェア
- ◆ 必要な接続を識別する分析および設計のフェーズ
- ◆ テスト目的での他のシステムの利用とアクセス
- ◆ 分析および設計のフェーズからのデータモデル

データの検証と準備

運用システムのデータは、品質と整合性にばらつきがある可能性があるため、システムを同期化すると不整合を生じることがあります。このフェーズは、Nsure Resourcesの実装チームと、統合されるシステム内のデータを「所有」または管理する業務単位またはグループを明確に分離するポイントになります。場合によっては、関連付けられているリスクとコストの要因は、プロビジョニングプロジェクトには属さないことがあります。

主な成果物

- ◆ eDirectory へのロードに適した運用データセット（分析および設計のアクティビティで識別）。これには、ロード方法（バルクロードか、コネクタ経由）も含まれます。検証されるデータの要件、または他の方法でフォーマットされているデータの要件も識別されます。

従属関係

- ◆ 分析および設計のフェーズからのデータモデル（提案されたレコード一致とデータ形式の戦略）
- ◆ 運用データセットへのアクセス

運用試験

このアクティビティの目的は、運用環境への移行を開始することです。このフェーズ中に、追加のカスタマイズが必要になることがあります。この限定的な導入では、前のアクティビティが目的どおりの成果を達成しているかどうかを確認し、運用投入のための同意を得ることができます。

注： このフェーズは、ソリューションの受け入れ基準、または本格運用までに必要なマイルストーン、あるいはその両方になる場合があります。

主な成果物

- ◆ データモデルおよびプロセスに求める結果に関する実際の POC と検証を提供する試験ソリューション

従属関係

- ◆ それ以前のすべてのアクティビティ（分析と設計、Identity Manager テクノロジプラットフォーム）。

運用投入計画

このフェーズでは運用展開を計画します。計画では次の作業を行う必要があります。

- ◆ サーバプラットフォーム、ソフトウェアの改定、およびサービスパックを確認する
- ◆ 全般的な環境を確認する
- ◆ eDirectory の導入、および異なるツリーの共存を確認する
- ◆ パーティションと複製の戦略を確認する
- ◆ Identity Manager の実装を確認する
- ◆ レガシープロセスのカットオーバーを計画する
- ◆ ロールバックコンティンジェンシ戦略を計画する

主な成果物

- ◆ 運用投入計画
- ◆ レガシープロセスのカットオーバー計画
- ◆ ロールバックコンティンジェンシ計画

従属関係

- ◆ 以前のすべてのアクティビティ

運用環境への展開

このフェーズでは、運用環境の実際のデータすべてが対象になるように試験ソリューションを拡張します。一般的には、運用試験が技術上およびビジネス上の要件をすべて満たしていることに同意が得られた後で実施されます。

主な成果物

- ◆ 移行準備の整った運用ソリューション

従属関係

- ◆ 以前のすべてのアクティビティ

Identity Manager 実装の技術面の計画

Identity Manager がサーバ上で必要とするオブジェクトの複製

計画の一部として、DirXML ドライバを実行するサーバに特定の eDirectory オブジェクトが複製されていることを確認する必要があります。

フィルタ済みレプリカを使用できます。ただし、ドライバが読み込むか同期化する必要があるすべてのオブジェクトと属性がフィルタ済みレプリカに含まれていることが条件です。

DirXML ドライバオブジェクトには、同期化するあらゆるオブジェクトに対する十分な eDirectory 権限を与える必要があります。これは、明示的に権限を付与するか、ドライバオブジェクトのセキュリティを、必要な権限を持つオブジェクトと同等にすることによって行います。

DirXML ドライバが実行されている eDirectory サーバ（または、リモートローダを使用している場合はドライバが参照する eDirectory サーバ）は、次のマスタレプリカまたは読み書き可能レプリカを保持している必要があります。

- ◆ 該当するサーバのドライバセットオブジェクト。

Identity Manager を実行している各サーバに 1 つのドライバセットオブジェクトが必要です。特に必要でない限り、同じドライバセットオブジェクトに複数のサーバを関連付けないでください。

注：ドライバセットオブジェクトを作成する場合、デフォルトでは別々のパーティションが作成されるよう設定されていますが、これは必須ではありません。

- ◆ 該当するサーバのサーバオブジェクト。

サーバオブジェクトによってドライバはオブジェクトのキーペアを生成できるため、サーバオブジェクトが必要です。また、リモートローダ認証にも重要です。

- ◆ ドライバのこのインスタンスと同期化するオブジェクト。

これらのドライバのレプリカがドライバと同じサーバ上にない限り、ドライバはオブジェクトを同期化できません。実際に、DirXML ドライバは、ユーザがルール（「スコープフィルタ処理」のルール）を作成して別の方法を指定している場合を除き、サーバ上で複製された「すべて」のコンテナに含まれるオブジェクトを同期化します。

たとえば、特定のドライバですべてのユーザオブジェクトを同期化する場合、最も簡単な方法は、ユーザ全員のマスタレプリカまたは読み書き可能レプリカを保持するサーバ上で、そのドライバの1つのインスタンスを使用する方法です。

ただし、多くの環境では、1つのサーバにユーザ全員のレプリカが含まれるのではなく、ユーザの完全なセットが複数のサーバに分散されています。この場合、次の2つの方法があります。

- ◆ **ユーザを1つのサーバに集約する。** 既存のサーバにレプリカを追加することによって、すべてのユーザを保持する1つのサーバを作成できます。必要なユーザオブジェクトと属性がフィルタ済みレプリカの一部である限り、フィルタ済みレプリカを使用すると、eDirectory データベースのサイズを削減できます。
- ◆ **スコープフィルタ処理によって複数のサーバ上でドライバの複数のインスタンスを使用する。** 1つのサーバにユーザを集約「しない」場合は、どのサーバセットにすべてのユーザを保持するかを決定し、これらの各サーバに DirXML ドライバの1つのインスタンスを設定する必要があります。

ドライバの別個のインスタンスが同じユーザを同期化しないようにするために、「スコープフィルタ処理」を使用して、ドライバの各インスタンスでどのユーザを同期化するかを定義する必要があります。スコープフィルタ処理とは、各ドライバにルールを追加して、ドライバの管理の範囲を特定のコンテナに制限することです。41 ページの「**スコープフィルタ処理を使用した別のサーバ上のユーザの管理**」を参照してください。

- ◆ テンプレートを使用するよう選択した場合に、ユーザの作成時にドライバが使用するテンプレートオブジェクト。

DirXML ドライバでは、ユーザを作成するための eDirectory テンプレートオブジェクトを指定する必要はありません。ただし、eDirectory 内にユーザを作成する際にドライバがテンプレートを使用するように指定した場合は、ドライバを実行しているサーバ上にテンプレートオブジェクトを複製する必要があります。

- ◆ DirXML ドライバがユーザの管理に使用するコンテナ。

たとえば、Inactive User というコンテナを作成して、無効になっているユーザアカウントを保持する場合、ドライバを実行しているサーバ上に、そのコンテナのマスタレプリカまたは読み書き可能レプリカ（可能であればマスタレプリカ）が必要です。

- ◆ ドライバが参照する必要のあるその他のオブジェクト (Avaya PBX ドライバの作業オーダオブジェクトなど)。

その他のオブジェクトがドライバによって読み込まれるだけで変更されない場合は、サーバ上のこれらのオブジェクトのレプリカには読み込み専用レプリカを使用できます。

スコープフィルタ処理を使用した別のサーバ上のユーザの管理

スコープフィルタ処理とは、各ドライバにルールを追加して、ドライバのアクションの範囲を特定のコンテナに制限することです。次に、スコープフィルタ処理が必要になる2つの状況を示します。

- ◆ 特定のコンテナに含まれるユーザのみをドライバで同期化する場合。

DirXML ドライバは、デフォルトで、DirXML ドライバが実行されているサーバ上に複製されているすべてのコンテナ内のオブジェクトを同期化します。この範囲を絞り込むには、スコープフィルタ処理ルールを作成する必要があります。

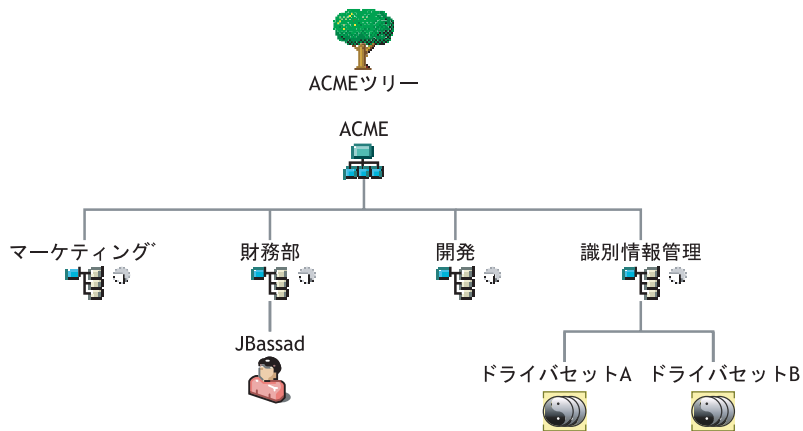
- ◆ DirXML ドライバですべてのユーザを同期化しつつ、すべてのユーザを同じサーバ上に複製しない場合。

1つのサーバ上でユーザを複製することなくユーザ全員を同期化するには、すべてのユーザを保持するサーバセットを決定し、これらの各サーバ上にDirXML ドライバのインスタンスを作成する必要があります。ドライバの2つのインスタンスが同じユーザを同期化しないようにするために、スコープフィルタ処理を使用して、ドライバの各インスタンスがどのユーザを同期化するかを定義する必要があります。

注：現在、サーバのレプリカが重複していても、スコープフィルタ処理を使用することをお勧めします。今後サーバにレプリカを追加すると、意図せずレプリカが重複してしまうことがあります。スコープフィルタ処理を使用すると、サーバにレプリカを追加しても、DirXML ドライバが同じサーバを同期化することはありません。

次に、スコープフィルタ処理の使用例を示します。

次の図は、ユーザが格納された3つのコンテナである Marketing、Finance、および Development を持つツリーを示します。各コンテナは別個のパーティションです。



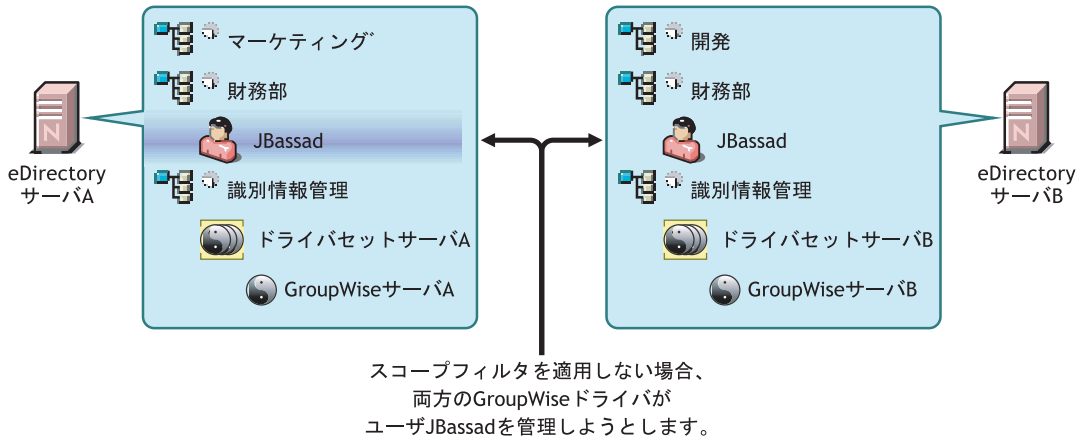
この例では、次の図に示すように、eDirectory 管理者は Server A と Server B という2台の eDirectory サーバを管理しています。どちらのサーバにもすべてのユーザのコピーは含まれません。各サーバには3つのパーティションのうち2つが含まれるため、サーバが保持する範囲が重複しています。

管理者は、ツリー内のすべてのユーザを GroupWise ドライバで同期化したいと考えていますが、ユーザのレプリカを1つのサーバに集約しようとは考えていません。このため、GroupWise ドライバの2つのインスタンスを各サーバで1つずつ使用することにしました。管理者は Identity Manager をインストールし、各 eDirectory サーバに GroupWise ドライバを設定します。

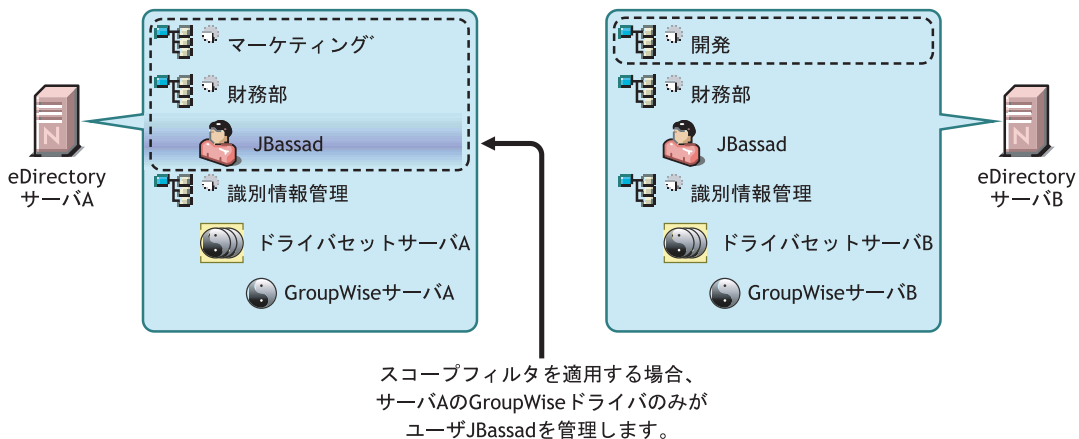
Server AはMarketing コンテナと Finance コンテナのレプリカを保持しています。また、このサーバには Identity Manager コンテナのレプリカもあり、このレプリカに Server A のドライバセットと Server A の GroupWise ドライバオブジェクトが保持されています。

Server Bには、Development コンテナと Finance コンテナのレプリカ、および Server B のドライバセットと Server B の GroupWise ドライバオブジェクトを格納する Identity Manager コンテナが保持されています。

Server A と Server B の両方に Finance コンテナのレプリカが保持されているため、Finance コンテナ内に存在するユーザ JBassad は、両方のサーバに保持されています。スコープフィルタ処理を使用しない場合、GroupWise ドライバ A と GroupWise ドライバ B の両方が JBassad を同期化します。



次の図は、スコープフィルタ処理を使用して、ドライバの2つのインスタンスが同じユーザを管理しないようにしていることを示します。これは、スコープフィルタ処理によって、各コンテナを同期化するドライバを定義しているためです。



次に、スコープフィルタ処理のルールを作成する方法のサンプルを示します。このルールは、Subscriber Event Transformation スタイルシートに記述します。

```
<xsl:transform version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:jstring="http://www.novell.com/nxsl/java/java.lang.String"
  exclude-result-prefixes="jstring">

  <!--
  To select different containers for scoping, add/delete/modify the <value>
  elements in the body of the variable "in-scope-containers-rtf"

  Note that if the container is not in the root of the tree, then the DN
  (minus the tree name) of the container must be specified, e.g.,
  Corporate\Executives

  Note: THESE MUST BE ENTERED IN THE TABLE AS ALL UPPERCASE
  -->

  <xsl:variable name="in-scope-containers-rtf">
    <value>CORPORATE\USERS\ACTIVE</value>
    <value>CORPORATE\USERS\INACTIVE</value>
  </xsl:variable>
  <xsl:variable name="in-scope-containers" select="document('')/xsl:transform/
  xsl:variable[@name='in-scope-containers-rtf']/value"/>

  <!--
  "identity" transformation - copies unchanged everything not explicitly
  matched by other templates
  -->

  <xsl:template match="node()|@*">
    <xsl:copy>
      <xsl:apply-templates select="@*|node()"/>
    </xsl:copy>
  </xsl:template>

  <!-- throw away events that are out of scope -->

  <xsl:template match="input/*[@src-dn]">
    <xsl:variable name="in-scope">
      <xsl:call-template name="in-scope"/>
    </xsl:variable>
    <xsl:choose>
      <xsl:when test="$in-scope = '1'">
        <xsl:copy>
          <xsl:apply-templates select="@*|node()"/>
        </xsl:copy>
      </xsl:when>
      <xsl:otherwise>
        <xsl:message>
          <status level="warning">Operation vetoed by Event Transformation
            Rule - out of scope</status>
        </xsl:message>
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>

  <!--
  check to see if an object is in the scope defined by the variable
  "in-scope-containers"
  -->
```

```

-->

<xsl:template name="in-scope">
  <!-- validate that the container is in scope -->
  <xsl:variable name="src-dn" select="substring-after(substring-after(@src-dn, '\'), '\')"/>
  <xsl:variable name="src-dn-i" select="jstring:lastIndexOf($src-dn, '\')"/>
  <xsl:if test="$src-dn-i != -1">
    <xsl:variable name="src-dn-container" select="jstring:substring($src-dn, 0, $src-dn-
i)"/>

    <!--
    the following test takes advantage of the XPath existential
    quantification semantics:
    basically, if one node in the node-set has a string value that matches
    the string, then the statement is true
    -->

    <xsl:if test="jstring:toUpperCase($src-dn-container) = $in-scope-containers">
      <xsl:value-of select="'1'"/>
    </xsl:if>
  </xsl:if>
</xsl:template>
</xsl:transform>

```

3

アップグレード

この節では、次の項目について説明します。

- ◆ 45 ページの「パスワード同期のアップグレード」
- ◆ 45 ページの「RNS から Nsure Audit へのアップグレード」
- ◆ 45 ページの「ドライバ設定のアップグレード」

一部のシナリオについては、25 ページの「一般的なインストールシナリオ」で説明しています。

パスワード同期のアップグレード

178 ページの「Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード」を参照してください。

RNS から Nsure Audit へのアップグレード

レポートिंग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、エンジンは引き続き RNS 機能进行处理します。Nsure 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くなるため、Nsure Audit への移行を計画することをお勧めします。

詳細については、13 章 269 ページの、「Nsure Audit によるログとレポート」を参照してください。

ドライバ設定のアップグレード

ドライバ設定のアップグレードでは次の 2 つの点に注意してください。

- ◆ ルールを Identity Manager ポリシーに変換する。これは変換ツールで実行され、ドライバの機能は強化されません。レガシードライバはこの変換なしでも動作しますが、変換を行うことで DirXML iManager プラグインに既存のドライバ設定を表示できます。
- ◆ ドライバポリシーをアップグレードして新しい機能を追加する。これは Identity Manager のエキスパートが実行するのが適切です。

79 ページの「DirXML 1.x から Identity Manager 形式へのドライバ設定のアップグレード」と 78 ページの「Identity Manager 環境での DirXML 1.x ドライバの管理」を参照してください。

また、Identity Manager ドライバの設定から始めて、これらを DirXML 1.x 設定と同じ処理を実行するようにカスタマイズする方法もあります。

4 インストール

この節では、Nsure™ Identity Manager および DirXML® ドライバの要件とインストール手順について説明します。

- ◆ 47 ページの「インストールの前に」
- ◆ 48 ページの「Identity Manager のコンポーネントとシステム要件」
- ◆ 50 ページの「Identity Manager の NetWare へのインストール」
- ◆ 51 ページの「Identity Manager の Windows へのインストール」
- ◆ 52 ページの「Identity Manager の UNIX プラットフォームへのインストール」
- ◆ 53 ページの「インストール後の作業」
- ◆ 53 ページの「リモートローダ」
- ◆ 76 ページの「Identity Manager 製品のアクティベーション」
- ◆ 76 ページの「カスタムドライバのインストール」

インストールの前に

Identity Manager をインストールする前に、次の情報を確認してください。

- ◆ 25 ページの「一般的なインストールシナリオ」
- ◆ 33 ページの「Identity Manager 実装のプロジェクト管理面の計画」および 39 ページの「Identity Manager 実装の技術面の計画」で説明した計画情報を確認します。
- ◆ すべてのシステム要件を満たすことを確認します。48 ページの「Identity Manager のコンポーネントとシステム要件」を参照してください。
- ◆ Novell® eDirectory™ サーバをバックアップすることをお勧めします。Novell マニュアルの「[Backing Up and Restoring eDirectory \(eDirectory のバックアップと復元\)](http://www.novell.com/documentation/lg/edir871/edir871/data/a2n4mb6.html) (<http://www.novell.com/documentation/lg/edir871/edir871/data/a2n4mb6.html>)」を参照してください。
- ◆ サーバに Identity Manager をインストールすると、ホスト eDirectory サーバのパーティションレプリカに物理的に含まれる情報のみが同期化されます。特定の同期化アプリケーションに対して eDirectory データのツリー全体のビューが必要な場合、1 台のサーバに複数のパーティションを集約する必要があります。詳細については、39 ページの「Identity Manager がサーバ上で必要とするオブジェクトの複製」を参照してください。
- ◆ ドライバのホストになるサーバのフル読み書き可能レプリカに、ドライバセットオブジェクトが存在する必要があります。
- ◆ ドライバオブジェクトには、同期先のオブジェクトに対する十分な eDirectory 権限を付与するか、ドライバオブジェクトに任意の権限を持つオブジェクトと同等のセキュリティを設定する必要があります。

Identity Manager のコンポーネントとシステム要件

Nsure Identity Manager は、複数のシステムとプラットフォーム上の環境内にインストールできるコンポーネントを含みます。システム設定によっては、Identity Manager インストールプログラムを数回実行して、適切なシステムに Identity Manager コンポーネントをインストールする必要があります。

次の表は、Identity Manager の 4 つのインストールコンポーネントと各システムの要件を一覧しています。

システムコンポーネント	システム要件	メモ
DirXML サーバ <ul style="list-style-type: none">◆ DirXML エンジン◆ Nsure Auditエージェント◆ DirXML サービスドライバ◆ DirXML ドライバ◆ NMAS (Novell Modular Authentication Services) コンポーネント	<p>次のオペレーティングシステムのうちいずれか 1 つ</p> <ul style="list-style-type: none">◆ 最新の Support Pack が導入されている NetWare[®] 6 または 6.5◆ 最新のサービスパックが導入されている Windows NT*、2000、または 2003◆ Linux Red Hat* AS または ES 2.1◆ SUSE[®] LINUX Enterprise Server 8◆ Solaris 8 または 9◆ AIX 5.2L <p>次の eDirectory のバージョンのうちの 1 つ。</p> <ul style="list-style-type: none">◆ 最新の Support Pack が導入されている eDirectory 8.6.2◆ 最新の Support Pack が導入されている eDirectory 8.7.3	<ul style="list-style-type: none">◆ 一部の機能は eDirectory 8.6.2 ではサポートされていません。eDirectory の特定の機能とバージョンについては、289 ページの「eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート」を参照してください。
接続システムサーバ <ul style="list-style-type: none">◆ DirXML リモートローダ◆ リモートローダ設定ツール (Windows のみ)◆ Nsure Auditエージェント◆ 接続システムのドライバシム◆ 接続システムのツール	<p>各システムに固有のオペレーティングシステムと接続システムの要件については、『Identity Manager Driver documentation (Identity Manager ドライバマニュアル) (http://www.novell.com/documentation/lg/dirxmldrivers)』を参照してください。</p>	

システムコンポーネント	システム要件	メモ
Web ベースの管理サーバ <ul style="list-style-type: none"> ◆ DirXML とパスワード管理 iManager プラグイン ◆ ドライバ設定 ◆ エンドユーザパスワードセルフサービス ◆ EGuide 	<p>次のオペレーティングシステムのうちいずれか1つ</p> <ul style="list-style-type: none"> ◆ 最新の Support Pack が導入されている NetWare 6 または 6.5 ◆ 最新のサービスパックが導入されている Windows 2000、XP、または 2003 ◆ Linux Red Hat AS または ES 2.1 (Glibc バージョン 2.1.1 以降、および Kernel バージョン 2.2. x x 以降)。 ◆ Solaris 8 または 9 <p>次のソフトウェア</p> <ul style="list-style-type: none"> ◆ Novell iManager 2.0.2 (Apache 2.0.44 以降および Tomcat 4.1.18 以降を含む) 	<ul style="list-style-type: none"> ◆ ブラウザのサポートは iManager 2.0.2 によって決定されます。詳細および既知の問題については、『Novell iManager 2.0.2 管理ガイド』を参照してください。(http://www.novell.com/documentation/ig/imanager20/imanager20/data/bobxl9n.html) ◆ iManager Configuration Wizard に従ってポータルコンテンツを eDirectory にインストールする必要があります。これは、パスワードのセルフサービスやパスワードを忘れた場合の機能を、Identity Manager をすぐに使用できるようにするために必要です。 これは iManager のインストール中に実行でき、ここで実行するのがデフォルトです。インストール中にこの作業を実行しない場合は、インストール後に実行する必要があります。 ◆ eGuide をインストールする場合は、インストールプログラムを実行する前に Web サーバとアプリケーションサーバをインストールしておく必要があります。 ◆ eDirectory がインストールされている同じサーバに iManager 2.0.2 をインストールする場合は、eDirectory のバージョンが 8.7.3 でなければなりません。 ◆ (Netware) Novell eGuide 2.1.2 をインストールするには、有効な JVM をサーバにインストールする必要があります。 ◆ (Windows) Novell Client™ 4.83 は、Novell Software Downloads (http://www.novell.com/download/index.html) から入手できます。 ◆ iManager で他のツリーにログインしてリモートの Identity Manager サーバを管理する場合、リモートサーバの IP アドレスの代わりにサーバ名を使用すると、エラーが発生することがあります。さらに、NDS 内の LDAP サーバグループオブジェクトは、単純なバインドに TLS を必要とするように設定する必要があり、リモートツリーのルート認証局の証明書を認証局証明書として Web サーバにインポートする必要があります。
DirXML ユーティリティ <ul style="list-style-type: none"> ◆ DirXML ライセンス監査ツール ◆ アプリケーションツール (AD、Notes、SAP、PeopleSoft、および JDBC) ◆ Nsure Audit 設定ツール 	<p>各システムに固有の要件については、『Identity Manager Driver documentation (Identity Manager ドライバマニュアル)』(http://www.novell.com/documentation/ig/dirxmldrivers)』を参照してください。</p>	

Identity Manager の NetWare へのインストール

インストールを開始する前に、システムが 48 ページの「Identity Manager のコンポーネントとシステム要件」に一覧されている要件を満たすことを確認してください。

- 1 サーバコンソールで、「nwconfig.nlm」と入力します。
- 2 [Product Options] > [Install a Product Not Listed] の順に選択します。
- 3 <F3> キー (RCONSOLE で接続している場合には <F4> キー) を押し、Identity Manager NetWare インストールファイルへのパスを指定します。
しばらくすると、グラフィックインストールユーティリティが起動します。
- 4 [Next] をクリックします。
ファイルのコピーが終了すると、DirXML の初期画面が表示されます。[Next] をクリックすると、インストールが開始されます。
- 5 システムの種類を説明する概要ページを確認し、[Next] をクリックして続行します。
- 6 使用許諾書を読んで、[I Accept] をクリックします。
- 7 インストールするコンポーネントを選択します。次のオプションを使用できます。
 - ◆ **[DirXML Server]** - DirXML エンジンとサービスドライバ、eDirectory、LDAP、JDBC*、GroupWise[®]、Delimited Text、および SIF ドライバ用の DirXML ドライバ、NMASTM コンポーネント、Nsure Audit エージェントをインストールし、eDirectory スキーマを拡張します。
このオプションをインストールするには、Novell eDirectory をインストールしている必要があります。
 - ◆ **[Connected System]** - リモートローダをインストールし、LDAP、JDBC、eDirectory、GroupWise、SIF、および Delimited Text のドライバをインストールします。
 - ◆ **[DirXML Web Components]** - DirXML プラグイン、DirXML ドライバ設定、および Novell eGuide をインストールします。
このオプションをインストールするには、Novell iManager をインストールしている必要があります。
 - ◆ **[Utilities]** - JDBC ドライバの追加スクリプトをインストールします。
- 8 [Next] をクリックします。
- 9 [Schema Extension] ページで次を指定します。
 - ◆ **[User Name]** - スキーマを拡張する権限を持つユーザのユーザ名 (LDAP 形式) を指定します。
 - ◆ **[User Password]** - ユーザのパスワードを指定します。
- 10 [Next] をクリックします。
- 11 [Summary] ページで選択した内容を確認し、[Finish] をクリックします。
- 12 インストールが完了し、[Installation Complete] ダイアログボックスが表示されたら、[Close] を押します。

Identity Manager の Windows へのインストール

インストールを開始する前に、システムが [48 ページの「Identity Manager のコンポーネントとシステム要件」](#)に一覧されている要件を満たすことを確認してください。

- 1 Identity Manager インストールファイルをダウンロードし、解凍します。
- 2 NT ディレクトリから install.exe を実行します。
- 3 初期画面の説明を読み、[Next] をクリックします。
- 4 使用許諾書を読んで、[I Accept] をクリックします。
- 5 各種システムとコンポーネントの概要ページを確認し、[Next] をクリックしてインストールを開始します。
- 6 インストールするコンポーネントを選択します。
 - ◆ **[DirXML Server]**- DirXML エンジンとサービスドライバ、DirXML ドライバ、NMASS コンポーネント、および Nsure Audit エージェントをインストールし、eDirectory スキーマを拡張します。

このオプションをインストールするには、Novell eDirectory をインストールしている必要があります。
 - ◆ **[Connected System]**- リモートローダと任意の DirXML ドライバをインストールします。
 - ◆ **[DirXML Web Components]**- DirXML プラグイン、DirXML ドライバ設定、および Novell eGuide をインストールします。

このオプションをインストールするには、Novell iManager をインストールしている必要があります。
 - ◆ **[Utilities]**- 任意のアプリケーションユーティリティをインストールします。

JMS (Driver for Java Message Service) と WebSphere MQ は別々にインストールする必要があります。[ドライバ実装に関するガイド \(http://www.novell.com/documentation/dirxml/drivers\)](http://www.novell.com/documentation/dirxml/drivers) を参照してください。
- 7 [Schema Extension] ページで次を指定します。
 - ◆ **[User Name]**- スキーマを拡張する権限を持つユーザのユーザ名 (LDAP 形式) を指定します。
 - ◆ **[User Password]** - ユーザのパスワードを指定します。
- 8 インストールする Web コンポーネントを選択し、[Next] をクリックします。
- 9 インストールするユーティリティを選択し、[Next] をクリックします。インストールプログラムによってインストールパスが表示されます。デフォルトの場所を変更する場合は、任意の場所を入力 (またはその場所を参照し)、[Next] をクリックします。
- 10 インストールするシステムコンポーネント (JDBC、PeopleSoft、DirXML ライセンス監査ユーティリティ、Active Directory Discovery Tool、Lotus Notes Discovery Tool) を選択し、[Next] をクリックします。
- 11 [Summary] ページに一覧されている項目を確認します。承認する場合は、[Finish] をクリックしてコンポーネントをインストールします。
- 12 インストールプログラムを終了するには、[Close] をクリックします。

Identity Manager の UNIX プラットフォームへのインストール

インストールを開始する前に、システムが 48 ページの「Identity Manager のコンポーネントとシステム要件」に一覧されている要件を満たすことを確認してください。

- 1 tar ファイルを任意の場所にダウンロードし、解凍します。
- 2 ホストコンピュータから、root としてログインします。
- 3 tar ファイルを解凍したディレクトリから、次のコマンドのいずれかを入力してインストールプログラムを実行します。

Linux の場合： /unix/Linux/setup/dirxml_linux.bin

Solaris の場合： /unix/Solaris/setup/dirxml_solaris.bin

AIX の場合： /unix/AIX/setup/dirxml_aix.bin

- 4 初期画面の情報を確認し、〈Enter〉キーを押してインストールを続行します。
- 5 使用許諾契約を読み、使用条件に同意する場合は「Y」を入力します。同意しない場合は、「N」を入力してインストールプログラムを終了します。
- 6 インストールするインストールセットの適切な番号 (1 ~ 4) を指定します。インストールセットには次のコンポーネントが含まれます。

- ◆ **[DirXML Server]**– DirXML エンジンとサービスドライバ、DirXML ドライバ、NMAS コンポーネント、および Nsure Audit エージェントをインストールし、eDirectory スキーマを拡張します。

このオプションをインストールするには、Novell eDirectory をインストールしている必要があります。

注：高可用性を確保するために共有ストレージを設定する場合は、12 章 263 ページの、「高可用性」の情報を参照してください。

- ◆ **[Connected System Server]**– リモートローダをインストールし、LDAP、JDBC、eDirectory、SAP、Delimited Text、GroupWise (Linux SUSE 8 の場合のみ)、および Lotus Notes のドライバをインストールします。
- ◆ **[Web-Based Administration Server]**– DirXML プラグイン、DirXML ドライバ設定、および Novell eGuide をインストールします。

このオプションをインストールするには、Novell iManager をインストールしている必要があります。

- ◆ **[Customize]** – コンポーネントの一覧から任意のコンポーネントをインストールします。

注：直前のメニューに戻ってインストールオプションを変更するには「prev」と入力します。

- 7 (オプション) 入力したオプションによっては、LDAP ユーザ名とパスワードを指定するか、Web Server Secure ポートを指定するように要求するメッセージが表示されることがあります。

重要：(Solaris へのインストールの場合のみ) Web ベースの管理サーバを eDirectory と同じサーバにインストールする場合は、Web Server Secure ポートを要求するメッセージが表示された後で、デフォルト値を 8443 に変更します。

- 8 eDirectory が一時的にシャットダウンされるため (DirXML エンジンとスキーマファイルのインストール時)、サマリに含まれる情報が正しいことを検証します。[Install Summary] の情報が正しい場合は、〈Enter〉キーを押してパッケージのインストールを開始します。
- 9 終了したら、「OK」と入力してインストールプログラムを閉じます。

インストール後の作業

eDirectory が実行されている場合、Identity Manager モジュールは自動的に起動します。Identity Manager を手動でロードまたはアンロードする必要はありません。Identity Manager がインストールされたら、Identity Manager（およびインストールしたドライバ）を、ビジネスプロセスによって定義されたポリシーと要件を満たすように設定する必要があります。通常、インストール後には、主に次のような作業を行います。

- ◆ アプリケーションシステムの設定（特定のドライバ設定方法については、『[Identity Manager Driver Documentation \(Identity Manager ドライバマニュアル\)](http://www.novell.com/documentation/lg/dirxmldrivers)』（<http://www.novell.com/documentation/lg/dirxmldrivers>）を参照してください）。
- ◆ 77 ページの「ドライバの作成と設定」
- ◆ 93 ページの「ポリシーの作成」
- ◆ 79 ページの「ドライバの起動、停止、または再起動」
- ◆ 76 ページの「Identity Manager 製品のアクティベーション」

リモートローダ

この章では、次の各項目について説明します。

- ◆ 53 ページの「概要」
- ◆ 54 ページの「リモートローダのインストール」
- ◆ 57 ページの「リモートローダの設定」
- ◆ 72 ページの「Java リモートローダで使用する新しいドライバの設定」
- ◆ 72 ページの「リモートローダの実行」

概要

リモートローダは、異なるプロセスとして異なる場所で実行されている DirXML ドライバと DirXML エンジンがデータを交換できるようにするサービスです。リモートローダの動作形態には次のようなものがあります。

- ◆ DirXML エンジンが実行されているサーバ上の別のプロセスとして実行する
DirXML エンジン は eDirectory プロセスの一部として実行されます。一部の DirXML ドライバは、DirXML エンジンが実行されているサーバ上で実行できます。実際に、これらは DirXML エンジンと同じプロセスの一部として実行できます。
戦略上の理由から、DirXML ドライバをサーバ上で別のプロセスとして実行できませんが、通常は別のサーバ上で実行します。
- ◆ DirXML エンジンが実行されているサーバ以外のサーバ上で実行する
一部の DirXML ドライバは、DirXML エンジンが実行されているサーバ上では実行できません。リモートローダを使用すると、DirXML エンジンを特定の環境で実行しつつ、DirXML ドライバは別の環境のサーバ上で実行できます。

シナリオ - 別のサーバ。 DirXML エンジンは NewWare サーバ上で実行されています。Active Directory 用の DirXML 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 DirXML エンジン間の通信チャンネルになります。

シナリオ - ホスト以外。 DirXML エンジンは Solaris 上で実行されています。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 DirXML エンジンを実行しません。NIS システム上にリモートローダと NIS 用の DirXML 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ダが NIS ドライバを実行し、DirXML 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。

リモートローダによって、DirXML エンジンは次の環境で実行されている DirXML ドライバと通信できます。

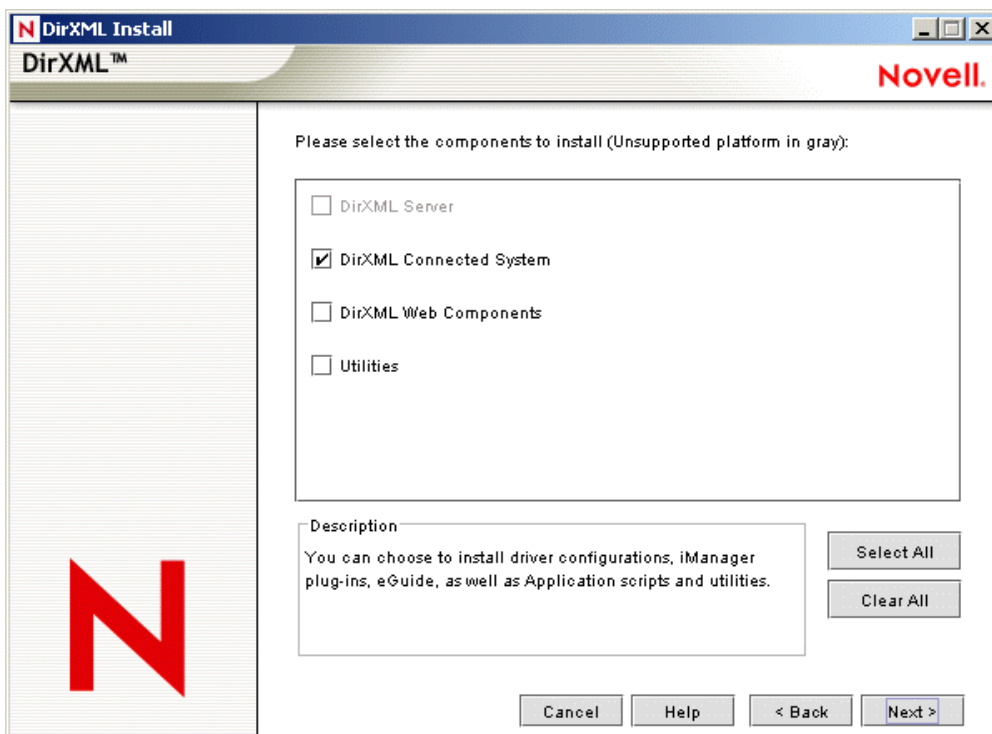
- ◆ Windows
- ◆ Solaris、Linux、または AIX

DirXML Java リモートローダは純粋な Java アプリケーションです。これは、あるサーバ上で実行中の DirXML エンジンと、rdxml が実行されていない別の場所で実行中の DirXML ドライバの間でデータを交換するために使用されます。互換性のある JRE (1.4.0 以上、1.4.2 以上を推奨) と Java Socket がインストールされたシステムであれば動作しますが、公式にサポートされているのは、HP-UX、AS/400、OS/390、または z/OS 上のみです。

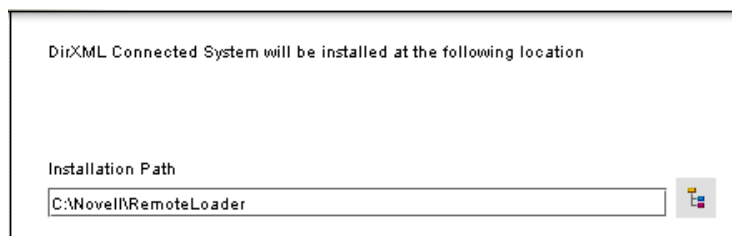
リモートローダのインストール

リモートローダの Windows サーバへのインストール

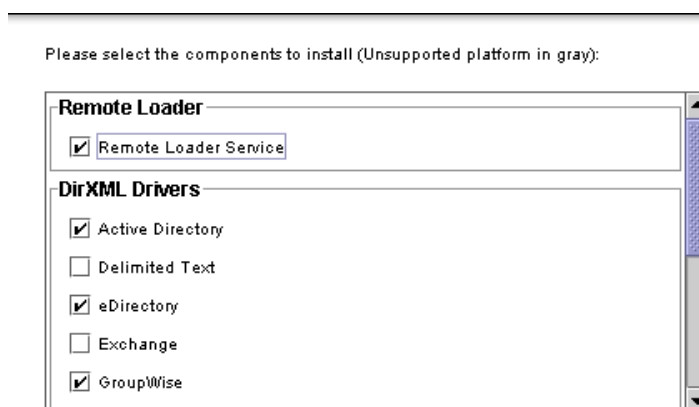
- 1 Identity Manager 2 インストールプログラムを実行します (¥nt¥install.exe など)。
- 2 最初の画面を確認して、使用許諾契約に同意し、2つの概要ページを表示します。
- 3 [DirXML Install] ダイアログボックスで、[DirXML Connected System] 以外のすべてのコンポーネントを選択解除して、[Next] をクリックします。



- 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、[Next] をクリックします。



- 5 [DirXML Remote Loader Service] とリモートドライバシムを選択し、[Next] 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、[Finish] をクリックします。
- 7 デスクトップに [Remote Loader Console] 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

Novell Web サイトからダウンロードした Identity Manager 2 ファイルを展開した後で、次の手順を実行します。

- 1 プラットフォームに合わせ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 [Choose Install Set] ページを表示します。

```

=====
Choose Install Set
=====
Please choose the Install Set to be installed by this installer.
|
|  ->1- DirXML Server
|     2- DirXML Connected System Server
|     3- Web-based Administrative Server
|
|     4- Customize...
|
ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: 2

```

- 3 「2」と入力して [DirXML Connected System Server] を選択し、〈Enter〉キーを押します。
- 4 [Pre-Installation Summary] 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:
Product Name:
  dirXML
Install Set
  DirXML Connected System Server
Product Components:
  LDAP Driver,
  SAP Driver,
  JDBC Driver,
  Delimited Text Driver,
  Notes Driver,
  Remote Loader,
  NIS Driver,
  Groupwise Driver

```


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

- 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 手順 1 で作成したディレクトリに、Identity Manager 2 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 z/OS	dirxml_jremote.tar.gz
OS/390	dirxml_jremote_mvs.tar

- 3 HP-UX、AS/400、または z/OS については、dirxml_jremote ファイルを解凍します。
- 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。この tar ファイルはドライバを含まないため、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。

MVS の情報については、dirxml_jremote_mvs.tar ファイルを解凍 (untar) して、usage.html ドキュメントを参照してください。

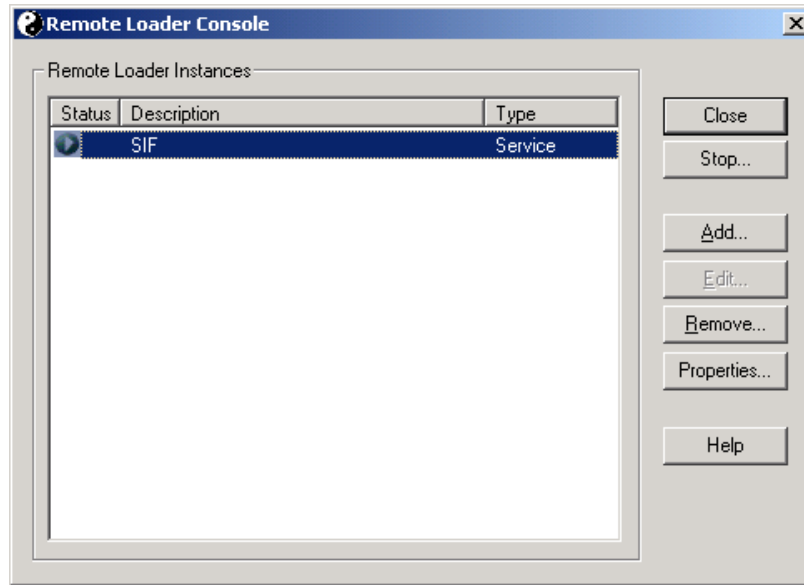
リモートローダの設定

DirXML リモートローダは、.dll、.nlm、.so、または .jar ファイルに含まれる DirXML 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。

Windows でのリモートローダの設定

Dirxml_remote.exe は、Windows プラットフォーム上でリモートローダを実行します。DirXML リモートローダは、パラメータを指定せずに dirxml_remote.exe を実行することで設定できます。この実行可能ファイルは、リモートローダを設定できる設定ウィザードを起動します。

リモートローダコンソールは、Identity Manager 2 の新しい機能です。dirxml_remote.exe によって起動されるウィザードの代わりにリモートローダコンソールを使用することをお勧めします。デスクトップの [Remote Loader Console] アイコンをクリックすると、次のリモートローダコンソールが表示されます。



コンソールを使用して、コンピュータのリモートローダ下で実行されているすべて DirXML ドライバ（またはこれらのドライバのインスタンス）を管理できます。

- ◆ ローカルコンピュータにリモートローダの新しいインスタンスを追加し、設定する。
- ◆ 設定を編集する。
- ◆ リモートローダのインスタンスを開始および停止する。
- ◆ 各ドライバのインスタンスのトレースを開始および停止する。

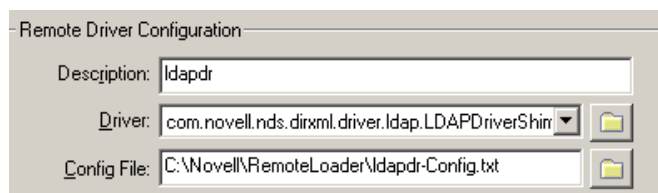
注：Identity Manager 2 にアップグレードすると、コンソールはリモートロードの既存のインスタンスを検出し、インポートします（自動的にインポートするには、ドライバ設定を remoteloader ディレクトリ（通常は c:\Novell\remoteloader）に保存する必要があります）。これでコンソールを使用してリモートドライバを管理できます。

ウィザードとコンソールを併用すると、予期しない動作が生じることがあります。実行中の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情報の提供

リモートローダのインスタンスを追加または編集すると、次の情報を求めるメッセージが表示されます。

Remote Driver Configuration

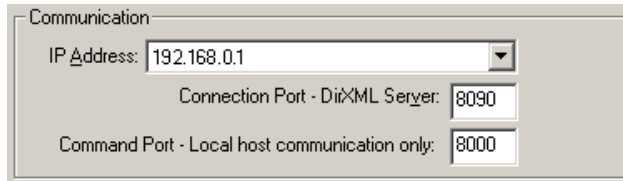


- ◆ Description
リモートローダのインスタンスを識別する説明を指定します。
- ◆ Driver
ドライバに適したシムを参照して選択します。

- ◆ Config File

設定ファイルの名前を指定します。リモートローダのコンソールは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。

Communication



- ◆ IP Address

リモートローダが DirXML 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 - DirXML Server

リモートローダが DirXML 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。作成する新しいインスタンスごとに、デフォルトのポート番号が自動的に 1 つずつ増えます。

- ◆ Command Port - Local Host Communication Only

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。作成する新しいインスタンスごとに、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：異なる接続ポートとコマンドポートを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。

Remote Loader Password



- ◆ Password

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。リモート接続するためのドライバの設定時に (Novell iManager の [Driver Parameters] のページで) 指定したパスワードと同じパスワードを指定する必要があります。

- ◆ Confirm

パスワードを再入力します。

Driver Object Password



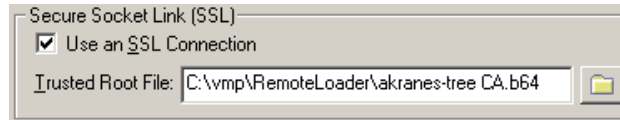
- ◆ Password

リモートローダはこのパスワードを使用して DirXML サーバで自身を認証します。このパスワードには、ドライバをリモートで接続するように設定する際に (Novell iManager の [Driver Parameters] のページで) 指定したパスワードと同じパスワードを指定する必要があります。

- ◆ Confirm

パスワードを再入力します。

Secure Socket Link (SSL)



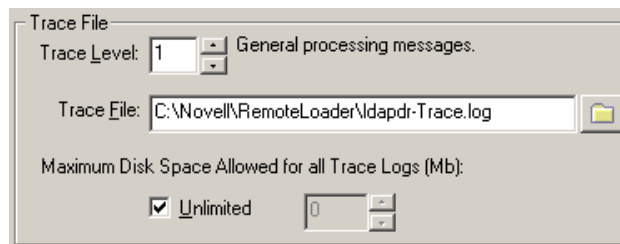
- ◆ Use an SSL Connection

SSL 接続を指定する場合は、このオプションを選択します。

- ◆ Trusted Root File

適切なルート認証局証明書を含む証明書ファイルを参照し、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。証明書は Base64 形式 (たとえば、akranes-tree CA.b64) でエクスポートする必要があります。

Trace File



- ◆ Trace Level

リモートローダインスタンスが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。

- ◆ Trace File

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。特定のマシン上で実行されているリモートローダの各インスタンスは、別々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。

- ◆ Maximum Disk Space Allowed for all Trace Logs (MB)

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。[Unlimited] を選択しないと、デフォルト値は 4096MB (4 ギガバイト) に設定されます。

リモートローダサービスの設定

Establish a Remote Loader service for this driver instance.

- ◆ リモートローダの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。

リモートローダの設定ファイルの作成

Rdxml は Solaris、Linux、または AIX プラットフォーム上でリモートローダを実行する実行可能ファイルです。Rdxml は、ネイティブドライバまたは Java ドライバのいずれかをホストできます。rdxml を使用してリモートローダの環境を設定できます。rdxml はコマンドラインから実行します。

Rdxml は、ネイティブインタフェースを使用する Java ドライバをサポートするために、JVM をロードします。また、ネイティブドライバもロードします。

次の表に示されたコマンドを使用して次の作業を実行できます。

- ◆ 設定ファイルにコマンドラインのオプションとパラメータを指定する。
テキストエディタを使用して、テキストエディタで設定ファイルを開くか、作成します。続いて、コマンドを追加します。
- ◆ 環境設定ファイルを起動する。
- ◆ リモートローダの実行中に一部の設定を変更する。

オプション	2 次名	パラメータ	説明
-class	-cl	Java クラス名	管理する DirXML アプリケーションシムの Java クラス名を指定します。クラスオプションとモジュールオプションは排他的で、どちらか一方を使用することができます。 例： -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim

オプション	2 次名	パラメータ	説明
-commandport	-cp	ポート番号	<p>リモートローダの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。リモートローダの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のインスタンスが、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。リモートローダのインスタンスが、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。</p> <p>例：</p> <pre>-commandport 8001 -cp 8001</pre>
-config	なし	ファイル名	<p>環境設定ファイルを指定します。環境設定ファイルには、<i>config</i> 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。</p> <p>例：</p> <pre>-config config.txt</pre>
-connection	-conn	接続設定文字列	<p>DirXML リモートインタフェースシムを実行している DirXML 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 DirXML 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。</p> <p>例：</p> <pre>-connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"</pre>
-description	-desc	短い説明	<p>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を指定します。</p> <p>例：</p> <pre>-description SAP -desc SAP</pre>

オプション	2 次名	パラメータ	説明
-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のインスタンスがデバッグを有効にするよう指定します。これは DirXML アプリケーションシムの開発者向けです。 例： -javadebugport 8080 -jdp 8080
-module	-m	モジュール名	ホストされる DirXML アプリケーションシムを含むモジュールを指定します。モジュールオプションとクラスオプションは排他的で、どちらか一方を使用することができます。 例： -module c:\drivers\exchanges\exdrivr.dll -m c:\drivers\exchanges\exdrivr.dll
-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 <i>setpasswords</i> 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、 <i>password</i> 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要求するメッセージが表示されます。 例： -password novell4 -p novell4

オプション	2 次名	パラメータ	説明
-service	-serv	なし、または install/uninstall	<p>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。</p> <p>このオプションを指定すると、Wind32 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。</p> <p>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。</p> <p>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。</p> <p>例：</p> <pre>-service install</pre> <pre>-serv uninstall</pre> <p>このオプションは Java リモートローダでは使用できません。</p>
-setpasswords	-sp	パスワード パス ワード	<p>リモートローダの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 DirXML 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、DirXML 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 DirXML 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。ただし、このオプションを指定しても、DirXML 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。</p> <p>例：</p> <pre>-setpasswords novell4 staccato3</pre> <pre>-sp novell4 staccato3</pre>
-trace	-t	整数	<p>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 DirXML サーバで使用されているレベルと同じです。</p> <p>例：</p> <pre>-trace 3</pre> <pre>-t 3</pre>

オプション	2 次名	パラメータ	説明
-tracechange	-tc	整数	<p>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 DirXML サーバで使用されているレベルと同じです。</p> <p>例：</p> <pre>-tracechange 1 -tc 1</pre>
-tracefile	-tf	ファイル名	<p>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。</p> <p>例：</p> <pre>-tracefile c:\temp\trace.txt -tf c:\temp\trace.txt</pre>
-tracefilechange	-tfc	なし、またはファイル名	<p>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。</p> <p>例：</p> <pre>-tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt</pre>
-tracefilemax	-tfm	サイズ	<p>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「roll-over」ファイルが生成されます。roll-over 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。</p> <p>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。</p> <p>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ーが完了するまで、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となります。</p> <p>例：</p> <pre>-tracefilemax 25M -tfm 25M</pre>

オプション	2 次名	パラメータ	説明
-unload	-u	なし	<p>リモートローダの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。</p> <p>例：</p> <pre>-unload</pre> <pre>-u</pre>
-window	-w	On/Off	<p>リモートローダの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。</p> <p>例：</p> <pre>-window on</pre> <pre>-w off</pre> <p>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。</p>
-wizard	-wiz	なし	<p>Configuration Wizard 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なしで <code>dirxml_remote.exe</code> を実行しても起動します。このオプションは、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、ウィザードは設定ファイルの値を使用して起動するので、このウィザードを使用して、設定ファイルを直接編集せずに設定を変更できます。</p> <p>例：</p> <pre>-wizard</pre> <pre>-wiz</pre> <p>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。</p>

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`

SSL で実行するリモートローダの設定

- 1 (オプション) DirXML サーバと Java リモートローダとの通信に SSL を使用する場合は、次の手順を実行します。
 - 1a DirXML サーバが表示されているツリーの組織 CA から自己署名証明書をエクスポートします。

証明書とともにプライベートキーをエクスポートする必要はありません。証明書をバイナリ (DER) 形式で保存します。
 - 1b create_keystore スクリプトを実行して、リモートローダで使用する Java キーストアファイルを作成します。

たとえば、次のように入力します。

```
create_keystore tree-root.der my.keystore
```

設定ファイルで使用できるように、create_keystore スクリプトによって表示される設定パラメータを書き留めます。create_keystore スクリプトは、キーストアのパスワードに、ハードコードされたパスワード「dirxml」を指定します。キーストアに保存されるのはパブリック証明書とパブリックキーのみなので、セキュリティリスクはありません。
- 2 サンプルの設定ファイル (config8000.txt) を編集し、任意のプロパティを指定します。

特に、実行されるドライバのクラス名、接続パラメータ、およびコマンドポートを指定します。
- 3 (オプション) DirXML サーバと Java リモートローダとの通信に SSL を使用する場合は、create_keystore スクリプトによって報告されるキーストア値とストアパス値を接続文字列に追加します。

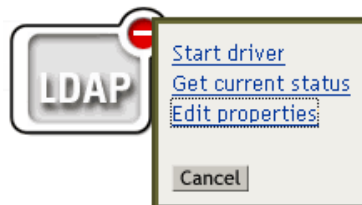
リモートローダで使用する DirXML ドライバの設定

ドライバシムのインストールと同じ手順を実行します。iManager で、[DirXML Management] > [Overview] の順に選択し、ドライバシムを既存のドライバセットまたは新しいドライバセットに追加します。

ドライバオブジェクトのプロパティの設定

リモートローダと DirXML ドライバをインストールした後、ドライバオブジェクトに、リモートローダに接続するためのパラメータを指定する必要があります。

- 1 Novell iManager で、[DirXML Management] > [Overview] の順にクリックします。
- 2 設定するドライバオブジェクト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、[Edit Properties] をクリックします。



4 リモートローダのパラメータを入力します。

- ◆ Communication

- ◆ IP Address

- この通信パラメータを指定しないと、値はデフォルトで localhost に設定されます。

- ◆ Connection port

- これは、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付けるポートです。この通信パラメータを指定しないと、値はデフォルトで 8090 に設定されます。

- ◆ Application Password

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、ドライバがアプリケーションと接続するために、ドライバシムはこのパスワードを必要とします。

- ◆ Remote Loader Password

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は、このパスワードを使用してリモートローダで自身を認証します。

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。

- ◆ Secure Socket Link

この通信パラメータを指定しないと、値は保存されません。つまり、SSL は使用されません。

5 [OK] をクリックします。

コマンドラインオプションとパラメータの使用

DirXML リモートローダでコマンドラインオプションを使用すると、次の操作を実行できます。

- ◆ DirXML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の各種パラメータを指定する。

これらのオプションには、シムクラス名の指定、DirXML サーバ上のリモートインタフェースシムとの通信に使用される接続パラメータの指定、またはトレースレベルの設定などがあります。

- ◆ DirXML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コマンドを送信する。

これらのオプションには、トレースウィンドウの開閉やリモートローダのアンロードなどがあります。

- ◆ リモートローダを設定する。

これらのオプションには、パスワードの設定や、リモートローダインスタンスの Win32 サービスとしてのインストールおよびアンインストールなどがあります。

オプションリストについては、61 ページの「リモートローダの設定ファイルの作成」の表を参照してください。

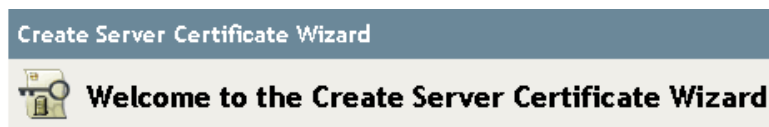
セキュリティで保護されたデータ転送の提供

SSL を使用してセキュリティで保護されたデータ転送を提供する場合は、次に示す作業を完了します。

- ◆ サーバ証明書を作成する。
- ◆ 自己署名証明書をエクスポートする。
- ◆ DirXML エンジンとリモートローダ間の SSL 接続を設定する。

サーバ証明書の作成

- 1 Novell iManager で、[Novell Certificate Server] > [Create Server Certificate] 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。



Select the server which will own the certificate.

Server:

RDDev31 

Certificate nickname:

remotecert

Creation method

- Standard
(Default parameters)
- Custom
(User specifies parameters)
- Import
(Allows a PKCS12 file to provide the keys and certificates)

重要: 証明書のニックネーム (remotecert など) は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 KM0 名に使用します。

- 3 [Creation method] は [Standard] のままにし、[Next] をクリックします。
- 4 [Summary] の画面を確認し、[Finish] をクリックして [Close] 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。69 ページの「自己署名証明書のエクスポート」に進みます。

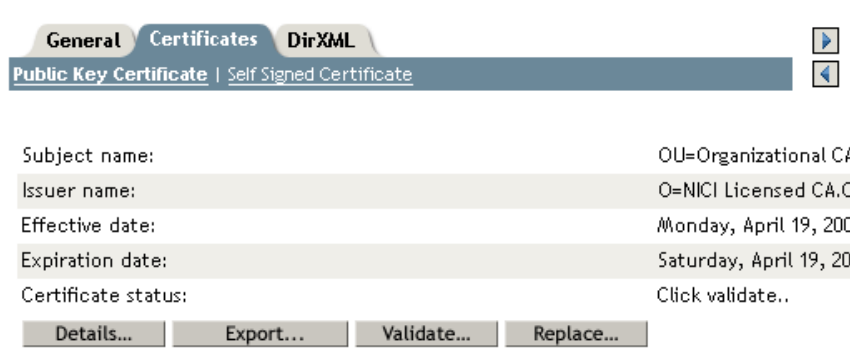
自己署名証明書のエクスポート

- 1 [eDirectory Administration] > [Modify Object] の順にクリックします。
- 2 [Security] コンテナの [Certificate Authority] を参照して選択し、[OK] をクリックします。



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

- 3 [Certificates] タブをクリックして [Self-Signed Certificate] をクリックし、[Export] をクリックします。



- 4 Export Certificate Wizard で、[No] を選択して [Next] をクリックします。
プライベートキーは証明書と一緒にエクスポートしません。
- 5 ファイルを Base64 形式でエクスポートすることを選択し、[Next] をクリックします。



Select an output format.

- File in binary DER format
- File in Base64 format

- 6 [Save the Exported Certificate to a File] へのリンクをクリックし、場所を指定して [Save] をクリックします。
- 7 [Save As] 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。

SSL 接続を使用するドライバの設定

SSL 接続を設定する前に、自己署名証明書をエクスポート済みで、リモートローダが、エクスポートしたファイルへのアクセス権を持っていることを確認してください。69 ページの「サーバ証明書の作成」を参照してください。

ここで、この証明書を使用するようにドライバのパラメータを変更する必要があります。

- 1 Novell iManager で、[DirXML Management] > [Overview] の順にクリックします。
- 2 SSL 接続を設定するドライバオブジェクトを参照して選択します。
- 3 リモートローダの接続パラメータを指定します。

たとえば、次のように入力します。

```
192.168.0.1 port=8090 remotecert
```

BFIO11-NDS.vmp

Authentication ID:	cn=Directory Manager
Authentication context:	122.0.0.1:389
Remote loader connection parameters:	192.168.0.1. port=8090 remotecert
Driver cache limit (kilobytes):	0

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、69 ページの「サーバ証明書の作成」の手順 2 で指定したニックネーム値です。

キーストアスクリプトの作成

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 DirXML エンジンの間で SSL を使用する必要があります、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。

Windows でのキーストア

Windows では Keytool ユーティリティを実行します。このツールは、通常は 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、%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。

コマンドラインで次を入力します。

```
create_keystore self-signed_certificate_name keystorename
```

Keystorename には任意の名前を指定できます (rdev_keystore など)。

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 には任意の名前を指定できます (rdev_keystore など)。

Java リモートローダで使用する新しいドライバの設定

- 1 [Overview] から [DirXML Driver] オブジェクトをクリックします。
- 2 [Driver Configuration] ページで [Connect to Remote Loader] を選択します。
- 3 [Driver Object] 編集ボックスにパスワードを入力します。
リモートローダは、このパスワードを使用してリモートインタフェースシムで自身を認証します。
- 4 [Authentication] ページでアプリケーションのパスワードを入力します。
リモートローダは、このパスワードを使用してリモートインタフェースシムで自身を認証します。
- 5 リモートローダのパスワードを入力します。
リモートローダは、このパスワードを使用してリモートインタフェースシムで自身を認証します。
- 6 リモートローダの通信パラメータを入力します。
パラメータはキーと値のペアです。
 - ◆ hostname
ホスト名または IP アドレス (190. 162.0. 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。
 - ◆ port
TCP ポート番号 (8090 など)。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付けるポートを指定します。
 - ◆ kmo
SSL に使用するキーと証明書を含む暗号化キーオブジェクトのキー名 (kmo=remotecert など) を指定します。
たとえば、通信パラメータは、hostname=192.168.0.1 port=8090 kmo=remotecert のようになります。

リモートローダの実行

Windows でのリモートローダコンソールからのリモートローダの実行

Windows でリモートローダを実行するには、デスクトップの [Remote Loader Console] アイコンをクリックします。

コマンドラインからのリモートローダの実行

Solaris、Linux、または AIX では、バイナリコンポーネント rdxml がリモートローダの機能を提供します。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	<code>dirxml_remote -config path_to_config_file -sp password password</code>
Solaris Linux AIX	<code>rdxml -config path_to_config_file -sp password password</code>
HP-UX AS/400 OS/390 z/OS	<code>dirxml_jremote -config path_to_config_file -sp password password</code>

- 2 設定ファイルを起動するコマンドを入力して、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	<code>dirxml_remote -config path_to_config_file</code>
Solaris Linux AIX	<code>rdxml -config path_to_config_file</code>
HP-UX AS/400 OS/390 z/OS	<code>dirxml_jremote -config path_to_config_file</code>

- 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。

ps コマンドまたはトレースファイルを使用して、コマンドと接続ポートがリッスンしているかどうかを確認します。

Java リモートローダが実行されている間は、トレースファイルで次の tail コマンドを使用して、その進捗を監視できます。

```
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されていて、DirXML 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()
```

リモートローダは、リモートローダが DirXML 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、DirXML アプリケーションシムをロードします。つまり、たとえば、リモートローダが DirXML サーバとの通信を失うと、アプリケーションシムはシャットダウンされます。

リモートローダを停止するには、コマンドラインで次を入力します。

プラットフォーム	コマンド
Windows	<code>dirxml_remote -config path_to_config_file -U</code>
Solaris Linux AIX	<code>rdxml -config path_to_config_file -U</code>
HP-UX AS/400 OS/390 z/OS	<code>dirxml_jremote -config path_to_config_file -U</code>

コンピュータ上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。

接続パラメータの設定

接続パラメータは、接続コマンドラインのオプションを使用して指定します。

DirXML リモートローダでは、リモートローダと、DirXML サーバ上でホストされているリモートインタフェースシムの間でカスタム接続方法を使用できます。デフォルトの接続方法は、SSL を使用した TCP/IP です。カスタム接続の接続文字列の要件と設定可能な項目の詳細については、カスタム接続モジュールに付属のマニュアルを参照してください。

リモートローダはサーバソケットを開き、リモートインタフェースシムからの接続をリッスンします。リモートインタフェースシムがリモートローダに接続すると、SSL ハンドシェイクが実行され、セキュリティで保護されたチャンネルが確立されます。セキュリティで保護されたチャンネルが確立された後、リモートインタフェースシムはリモートローダの認証を受けます。

リモートインタフェースシムが正常に認証されると、リモートローダがリモートインタフェースシムの認証を受けます。同期トラフィックは、両側が認証されたエンティティと通信していることを確認した後でのみ発生します。

この節では、TCP/IP 接続方法の引数名とパラメータについて説明します。

- 1 テキストエディタで設定ファイルを開くか、または作成します。
- 2 次の表を使用して TCP/IP 接続を設定します。

オプション	パラメータ	説明
address	IP アドレス	<p>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。アドレスを指定しないと、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。</p> <p>例：</p> <pre>address=137.65.134.83</pre>
keypass	キーパス	<p>.jar ファイルに含まれる DirXML 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。</p> <p>例：</p> <pre>keypass=mypassword</pre> <p>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。</p>
keystore	キーストア	<p>.jar ファイルに含まれる DirXML アプリケーションシムにのみ使用します。</p> <p>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。</p> <p>例：</p> <pre>keystore=my.keystore</pre>
port	10 進数のポート番号	<p>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。</p> <p>例：</p> <pre>port=8090</pre>
rootfile	ファイル名	<p>.dll ファイルに含まれる DirXML 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が使用する証明書の発行者のルート認証局証明書を含むファイルを指定します。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。証明書ファイルは Base64 形式 (PEM) でなければなりません。</p> <p>このオプションは Java リモートローダでは使用できません。</p>

Identity Manager 製品のアクティベーション

Identity Manager 製品はアクティベーションが必要です。詳細については、281 ページの付録 A、「Novell Identity Manager 製品のアクティベーション」を参照してください。

カスタムドライバのインストール

カスタムドライバは次で構成されています。

- ◆ .jar ファイルまたはネイティブファイル (.dll や .nlm など) のセット
- ◆ ドライバを設定するための XML ルールファイル
- ◆ マニュアル

カスタムドライバの作成またはインストールについては、『Novell Developer Kit (<http://developer.novell.com/ndk/dirxml-index.htm>)』を参照してください。

5

DirXML ドライバの管理

この節では、DirXML[®] 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。

- ◆ 77 ページの「ドライバの作成と設定」
- ◆ 78 ページの「Identity Manager 環境での DirXML 1.x ドライバの管理」
- ◆ 79 ページの「DirXML 1.x から Identity Manager 形式へのドライバ設定のアップグレード」
- ◆ 79 ページの「ドライバの起動、停止、または再起動」
- ◆ 80 ページの「グローバル設定値の使用」
- ◆ 80 ページの「DirXML コマンドラインユーティリティの使用」
- ◆ 80 ページの「バージョン情報の表示」
- ◆ 85 ページの「名前付きパスワードの使用」
- ◆ 90 ページの「ドライバオブジェクトとサーバの再関連付け」
- ◆ 91 ページの「ドライバハートビートの追加」

ドライバの作成と設定

使用する各 DirXML 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は設定パラメータとそのドライバのポリシーを含みます。ドライバオブジェクトの作成時に、ドライバ固有の設定ファイルをインポートします。ドライバ設定はデフォルトのポリシーセットを含みます。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。

- ◆ [Create Driver] タスク - 1 つのドライバを作成して、ドライバ設定にインポートできます。詳細については、78 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。
- ◆ [Import Driver] タスク - 複数のドライバを同時に作成して、それらの設定をインポートできます。詳細については、78 ページの「[複数のドライバの作成](#)」を参照してください。

ドライバオブジェクトの作成

ドライバ設定 (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、ドライバ設定ファイルには、実装に合わせて変更できる基本ポリシーも含まれています。

- 1 iManager で、[DirXML Utilities] > [Create Driver] 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、[Next] 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 [Import a Driver Configuration from the Server] を選択し、.xml ファイルを選択します。
ドライバ設定ファイルは、iManager の設定時に Web サーバにインストールされます。
- 4 プロンプトに従ってドライバ設定のインポートを完了します。

必要な Nsure™ 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を定義しなかったり、管理ユーザを除外したりした場合、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。

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必要なオブジェクトをドライバ設定 (XML) ファイルで作成および設定するという点では、単一のオブジェクト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、[DirXML Utilities] > [Import Drivers] 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、[Next] 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ドライバを選択し、[Next] をクリックします。
- 4 プロンプトに従って要求されたデータを指定し、[Next] をクリックします。

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を定義しなかったり、管理ユーザを除外したりした場合、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。

Identity Manager 環境での DirXML 1.x ドライバの管理

DirXML 1.x 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。

Nsure Identity Manager 2 に付属の DirXML エンジンには、旧ドライバとの後方互換性を備えています (旧ドライバシムと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)。後方互換性を確保するために、DirXML エンジンには、ドライバ設定をその場で Identity Manager 形式に変換しています。この変換は、エンジンを使用するためだけのもので、既存の DirXML 1.x ドライバ設定が恒常的に変更されることはありません。このエンジンは後方互換性を備えているため、必要に応じて、変更を加えずに Identity Manager サーバ上で DirXML 1.x 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 [Overview] に表示できますが、ドライバ設定を表示または編集することはできません。ドライバセットの [Overview] で DirXML 1.x ドライバをクリックすると、DirXML プラグインはそのドライバが 1.x 形式であることを検出し、ウィザードを使用してドライバを 2.0 形式に変換するようメッセージを表示します。

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.x ドライバを 1.x 形式で編集するには、DirXML 1.x 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.x 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 DirXML プラグインを使用してドライバ設定を編集するには、ドライバを Identity Manager 2 形式に変換する必要があります。

DirXML 1.x から Identity Manager 形式へのドライバ設定のアップグレード

Identity Manager をインストールすると、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設定は変更されません。

DirXML.x 用に作成された既存のドライバ設定は、Identity Manager でも引き続き動作します。ただし、Identity Manager の iManager DirXML 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： DirXML 1.x エンジンを使用して Identity Manager DirXML ドライバシムまたはドライバ設定を実行することはできません。

DirXML 1.x 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、[DirXML Management] > [Overview] の順にクリックします。変換するドライバを含むドライバセットを選択します。
- 2 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。
- 3 ウィザードの手順に従って変換を完了します。

ドライバの起動、停止、または再起動

- 1 iManager で、[DirXML Management] > [Overview] 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ます。
- 3 ステータスを変更するドライバをクリックし、適切なオプション（起動、停止、再起動）を選択します。

グローバル設定値の使用

グローバル設定値 (GCV) は、ドライバパラメータに似た新しい設定です。グローバル設定値は、ドライバセットおよび個々のドライバに対して指定できます。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新しい Identity Manager 機能の設定、および個々のドライバ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] ページではなく、ドライバの [Server Variables] ページで利用できるグラフィカルインター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 [Server Variables] 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、[Password Management] > [Password Synchronization] 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。このページは、パスワード同期の各設定のオンラインヘルプを含みます。

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、[DirXML Management] > [Overview] 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、[Global Config Value] タブをクリックします。
- 3 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。

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を使用すると、DirXML のすべての副動詞にアクセスでき、ドライバの起動や停止などの一般的なドライバ管理作業をコマンドラインから実行できます。DirXML コマンドラインユーティリティは Identity Manager とともにインストールされますが、DirXML 1. x 実装でも動作します。

Identity Manager の管理には iManager を使用することをお勧めしますが、一般的な操作は DirXML コマンドラインユーティリティでも実行できます。このユーティリティはインタラクティブモードでも、純粋なコマンドラインモードでも使用できます。

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。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

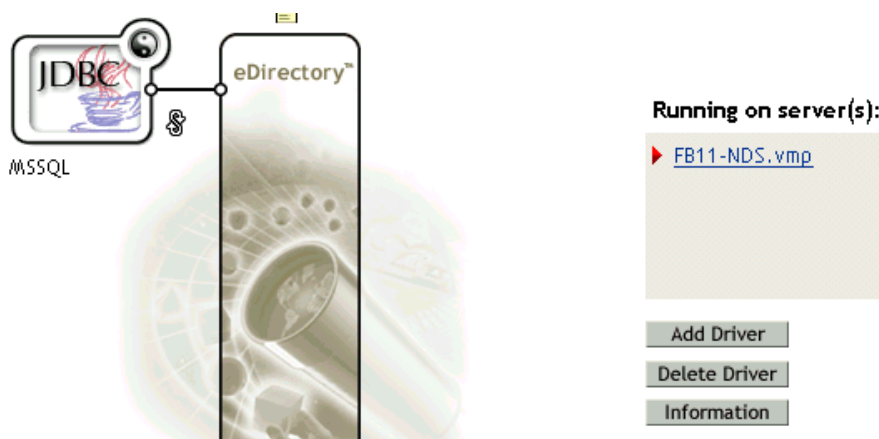
バージョン情報の表示

Versioning Discovery Tool で実行できる作業は、次のとおりです。

- ◆ DirXML 設定に関するバージョン情報を階層構造で表示する。
- ◆ 使用可能な同じ情報のテキストファイルを階層構造で表示する。
- ◆ ローカルドライブまたはネットワークドライブにバージョン情報を保存する。

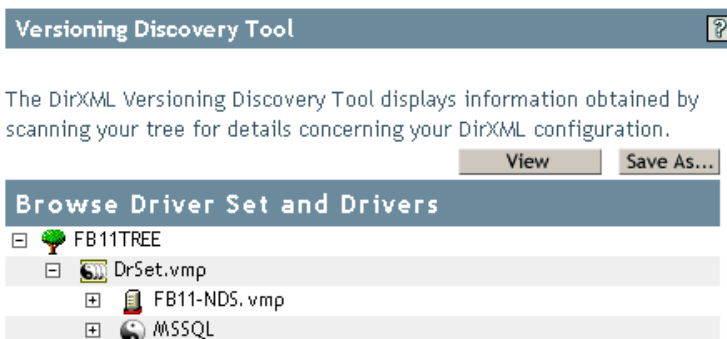
階層構造でのバージョン情報の表示

- 1 ドライバセットの [DirXML Overview] ダイアログボックスで、[Information] をクリックします。



[DirXML Utilities] > [Versioning Discovery Tool] の順に選択し、ドライバセットを参照して選択し、[Information] をクリックすることもできます。

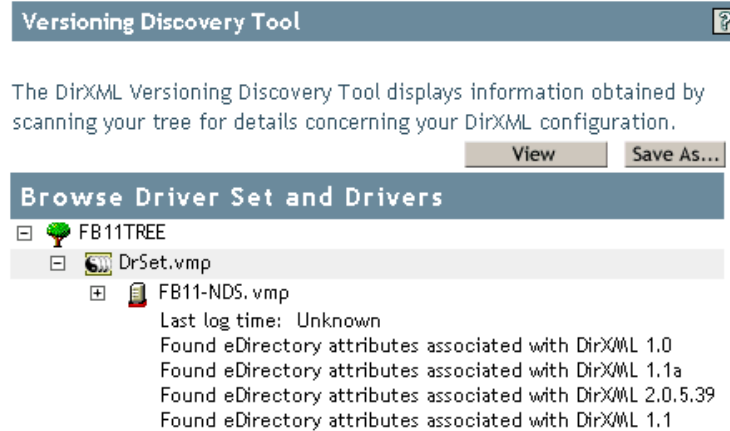
- 2 トップレベルのバージョン情報を表示します（未展開の状態）。



未展開の階層ビューでは、次が表示されます。

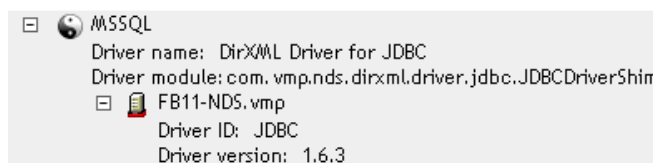
- ◆ 認証されているツリー
- ◆ 選択したドライバセット
- ◆ ドライバセットに関連付けられているサーバ
ドライバセットが2つ以上のサーバに関連付けられている場合、各サーバのDirXML情報を表示できます。
- ◆ ドライバ

- 3 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
 - ◆ サーバ上で実行されているか、または実行されていた DirXML のバージョン
- Versioning Discovery Tool では、Identity Manager 2 は DirXML 2. x. x. x として表示されます。この例では、[Found eDirectory Attributes Associated with DirXML 2.0.5.39] が、サーバ上で実行されている DirXML のバージョンです。
2. x. x. x より前の DirXML では、バージョン番号は保存されていませんでした。DirXML の以前のバージョンがサーバ上で実行されていた場合、Versioning Discovery Tool では、ディレクトリにマークが表示されます。この例では、3つの「Found」行によって、DirXML の以前のバージョン (1.0、1.1a、および 1.1) のマークが識別されます。
- 4 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。



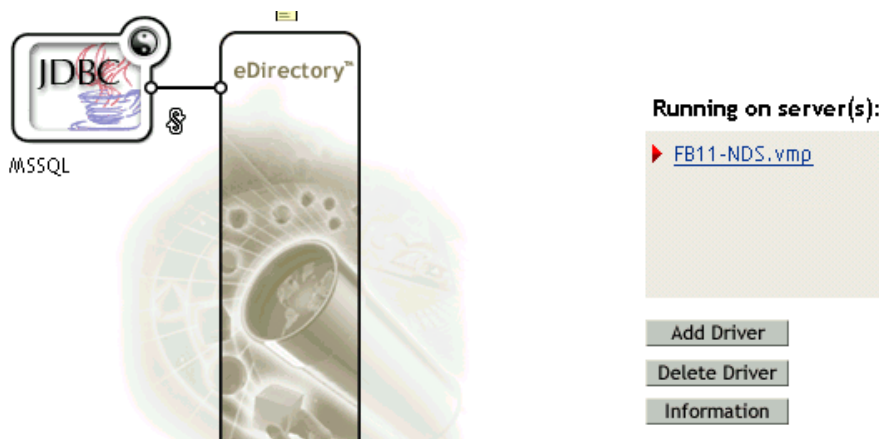
トップレベルのドライバアイコンの展開ビューには、次が表示されます。

- ◆ ドライバ名
 - ◆ ドライバモジュール (com.vmp.nds.dirxml.driver.jdbc.JDBCDriverShim 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

テキストファイルの表示

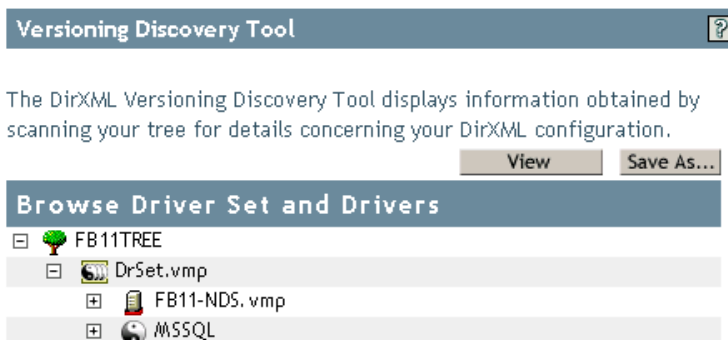
DirXML はバージョン情報をファイルに発行します。テキスト形式で保存されたこの情報を表示できます。テキスト形式に含まれる情報は、階層ビューと同じです。

- 1 ドライバセットの [DirXML Overview] ダイアログボックスで、[Information] をクリックします。



[DirXML Utilities] > [Versioning Discovery Tool] の順に選択し、ドライバセットを参照して選択し、[Information] をクリックすることもできます。

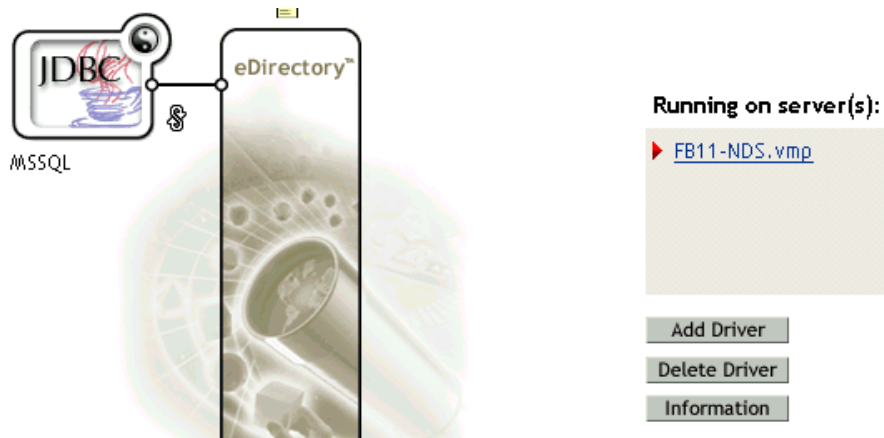
- 2 [Versioning Discovery Tool] ダイアログボックスで、[View] をクリックします。



バージョン情報の保存

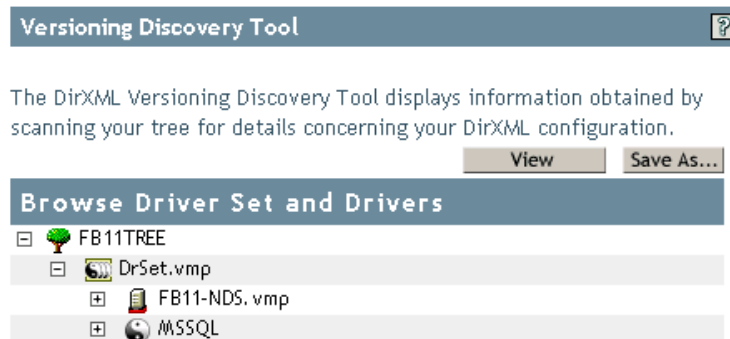
バージョン情報は、ローカルドライブまたはネットワークドライブにテキストファイルとして保存できます。

- 1 ドライバセットの [DirXML Overview] ダイアログボックスの [Information] をクリックします。



[DirXML Utilities] > [Versioning Discovery Tool] の順に選択し、ドライバセットを参照して選択し、[Information] をクリックすることもできます。

- 2 [Versioning Discovery Tool] ダイアログボックスで、[Save As] をクリックします。



- 3 [File Download] ダイアログボックスで、[Save] をクリックします。
- 4 目的のディレクトリに移動し、ファイル名を入力して [Save] 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。

名前付きパスワードの使用

DirXML 1. *x*には、1つのパスワードを安全に保存する機能があり、これにより、ドライバポリシーにパスワードをクリアテキストでハードコードせずにパスワードを使用できるようになっていました。

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。この新しい機能は、「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、DirXML 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復元の方法は、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： DirXML Driver for Lotus Notes 用に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、『*DirXML Driver for Lotus Notes Implementation Guide (DirXML Driver for Lotus Notes 実装ガイド)* (<http://www.novell.com/documentation/lg/dirxmldrivers>)』の名前付きパスワードに関する節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。

- ◆ 85 ページの「iManager を使用した名前付きパスワードの設定」
- ◆ 87 ページの「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」
- ◆ 90 ページの「ドライバポリシーでの名前付きパスワードの使用」

iManager を使用した名前付きパスワードの設定

- 1 iManager で、[DirXML Management] > [Overview] の順にクリックします。ドライバセットを検索するか、またはドライバセットを保持するコンテナを参照して選択します。

ドライバセットのグラフィック画面が表示されます。

- 2 [DirXML Overview] で、ドライバのアイコンをクリックします。

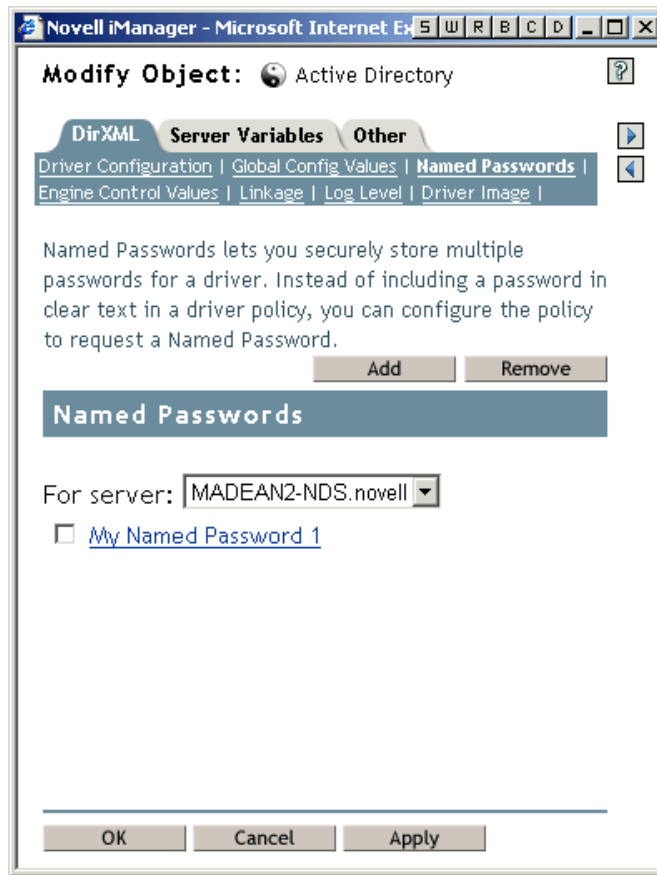
ドライバ設定のグラフィック画面が表示されます。

- 3 [DirXML Driver Overview] で、ドライバのアイコンをクリックします。

[Modify Object] ページが表示されます。

- 4 [DirXML] タブの [Modify Object] ページで、[Named Passwords] をクリックします。

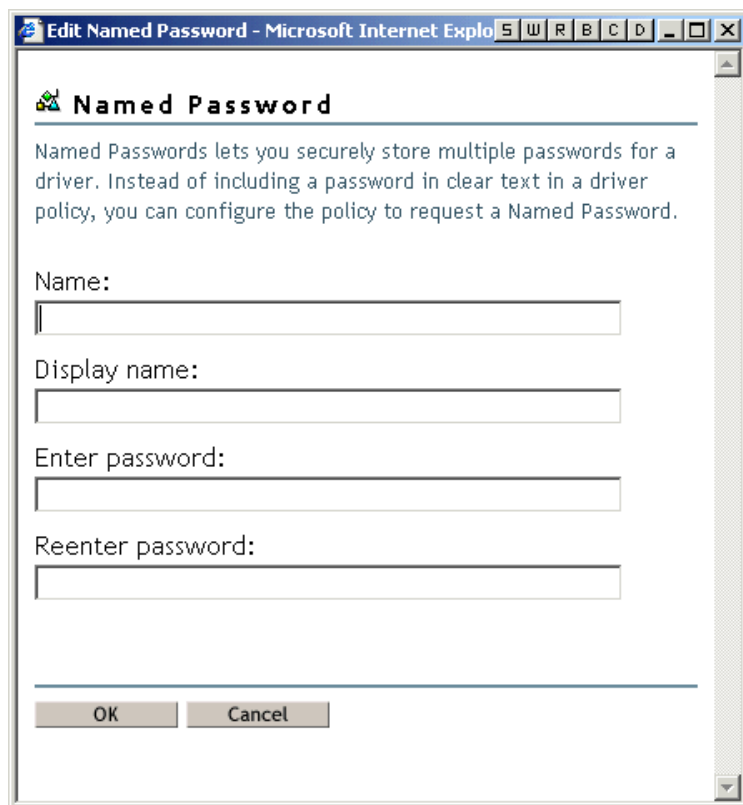
このドライバの現在の名前付きパスワードを一覧表示する [Named Passwords] ページが表示されます。名前付きパスワードを設定していない場合、このリストは空です。



- 5 名前付きパスワードを追加するには、[Add] 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。

名前、表示名、およびパスワードを指定できるページが表示されます。

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。



- 6 名前付きパスワードを削除するには、[Remove] 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。

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

- ◆ [87 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」](#)
- ◆ [89 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、[80 ページの「DirXML コマンドラインユーティリティの使用」](#)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。

この手順が終わったら、オプション 99 を 2 回使用してメニューを終了し、DXCommand 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なくなっただけの場合に便利です。

- 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、80 ページの「DirXML コマンドラインユーティリティの使用」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
```

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 (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。
この手順によって、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。
この手順によって、削除したパスワードが正しいことを確認できます。
この手順が終わったら、オプション99を2回使用してメニューを終了し、DXCommandユーティリティを終了します。

ドライバポリシーでの名前付きパスワードの使用

次のサンプルは、名前付きパスワードを加入者チャンネルのドライバポリシーでXSLTによって参照す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/>
```

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。

- ◆ DirXML (Identity Manager 2) 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。
- ◆ [DirXML Overview] のドライバの横にサーバのリストが表示されない。
- ◆ [DirXML Overview] 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、[DirXML Overview] のドライバオブジェクトに進みます。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。

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 に付属する DirXML ドライバの新しい機能で、使用するかどうかはオプションです。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ンネル上で通信が行われていない場合、ドライバはハートビートドキュメントを DirXML エンジンに送信します。

ドライバハートビートの目的は、ドライバが、アクションの実行頻度と同程度には発行者チャンネル上で通信していない場合に、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。DirXML エンジンには、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、次の手順を実行します。

- 1 iManager で、[DirXML Management] > [Overview] の順にクリックします。ドライバを検索し、ドライバのアイコンをクリックします。
- 2 ドライバ設定のグラフィック画面で、ドライバアイコンをクリックします。
- 3 [DirXML] ページで、[Drive Parameter] までスクロールし、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、設定は完了です。

間隔の値は 1 未満には設定できません。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。

- 4 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、[Edit XML] をクリックします。
- 5 次の例のようなドライバパラメータのエントリを、<publisher-options> の子として追加します (AD ドライバでは、これを <driver-options> の子にします)。

```
<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。

- 6 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、グラフィック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、間隔のグローバル設定値 (GCV) への参照を作成する方法です。他のグローバル設定値と同様に、ドライバハードビートは、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設定値がなく、ドライバセットにグローバル設定値がある場合、ドライバはドライバセットの値を継承します。

次の例は、Notes ドライバによって送信されたハートビートステータスドキュメントです。

```
<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>
```

6

ポリシーの作成

ポリシーにより、Novell® eDirectory™ 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 DirXML 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、Nsure™ 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の多くのタスクも実行できます。

ポリシーの詳細な説明については、『*Policy Builder とドライバカスタマイズガイド*』を参照してください。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、Policy Builder 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 とドライバカスタマイズガイド*』を参照してください。

7

Password Policy（パスワードポリシー）を使用したパスワードの管理

Password Policy（パスワードポリシー）を使用すると、ユーザのパスワード作成方法にルールを設定してセキュリティを強化できます。また、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスのオプションをユーザに提供して、ヘルプデスクのコストを削減することもできます。

このセクションでは、次の項目について説明します。

- ◆ [95 ページの「Password Policy（パスワードポリシー）機能の概要」](#)
- ◆ [102 ページの「Password Policy（パスワードポリシー）の計画」](#)
- ◆ [107 ページの「Password Policy（パスワードポリシー）の使用に関する前提条件」](#)
- ◆ [110 ページの「Password Policy（パスワードポリシー）の作成」](#)
- ◆ [111 ページの「ユーザへの Password Policy（パスワードポリシー）の割り当て」](#)
- ◆ [112 ページの「ユーザに割り当てられているポリシーの確認」](#)
- ◆ [112 ページの「ユーザのパスワードの設定」](#)
- ◆ [112 ページの「チャレンジセットの作成または変更」](#)
- ◆ [112 ページの「パスワード通知機能の設定」](#)
- ◆ [106 ページの「レガシー Novell Client によるパスワード変更の防止」](#)
- ◆ [113 ページの「Password Policy（パスワードポリシー）のトラブルシューティング」](#)

パスワードを忘れた場合のセルフサービスおよびパスワードのリセットセルフサービスの詳細については、[8 章 115 ページの「パスワードセルフサービス」](#)を参照してください。

Password Policy（パスワードポリシー）機能の概要

Password Policy（パスワードポリシー）は、エンドユーザパスワードの作成および交換に関する基準を指定した管理者定義ルールの集まりです。Nsure™ Identity Manager は、NMASTM を利用して、Novell™ eDirectory™ でユーザに割り当てた Password Policy（パスワードポリシー）を適用します。また、パスワード同期を使用して、接続システムで Password Policy（パスワードポリシー）を適用することもできます。[9 章 151 ページの「接続システム間のパスワード同期」](#)を参照してください。

Password Policy（パスワードポリシー）には、パスワードを忘れた場合のセルフサービス機能も含まれており、パスワードを忘れた場合のヘルプデスクへの問い合わせを減らすことができます。もう1つのセルフサービス機能は、パスワードのリセットセルフサービスです。このサービスにより、ユーザは、管理者がPassword Policy（パスワードポリシー）で指定したルールを参照しながら、自分のパスワードを変更できます。これらの機能には、iManagerのセルフサービスコンソールを介してアクセスします。

パスワード管理のほとんどの機能では、ユニバーサルパスワードを有効にする必要があります。会社にポータルがある場合は、iManagerセルフサービスコンソールを既存のポータルに統合し、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスにユーザが簡単にアクセスできるようにするのが理想的です。

Password Policy（パスワードポリシー）は、ウィザードを使用して作成します。これには、iManagerで、[Password Management] > [Manage Password Policies] > [Nex]の順に選択します。

新しいパスワード管理機能では、次の操作を実行できます。

- ◆ 96 ページの「ユニバーサルパスワードの有効化」
- ◆ 97 ページの「Advanced Password Rule（詳細パスワードルール）の設定」
- ◆ 99 ページの「Password Policy（パスワードポリシー）への独自のパスワード変更メッセージの追加」
- ◆ 116 ページの「ユーザへのパスワードを忘れた場合のセルフサービスの提供」
- ◆ 117 ページの「ユーザへのパスワードのリセットセルフサービスの提供」
- ◆ 99 ページの「eDirectory ユーザへのポリシーの割り当て」
- ◆ 100 ページの「eDirectory 内でのポリシーの適用」
- ◆ 101 ページの「接続システムへのポリシーの適用」
- ◆ 102 ページの「ユーザに対して有効な Password Policy（パスワードポリシー）の表示」
- ◆ 102 ページの「ユーザのユニバーサルパスワードの設定」

ユニバーサルパスワードの有効化

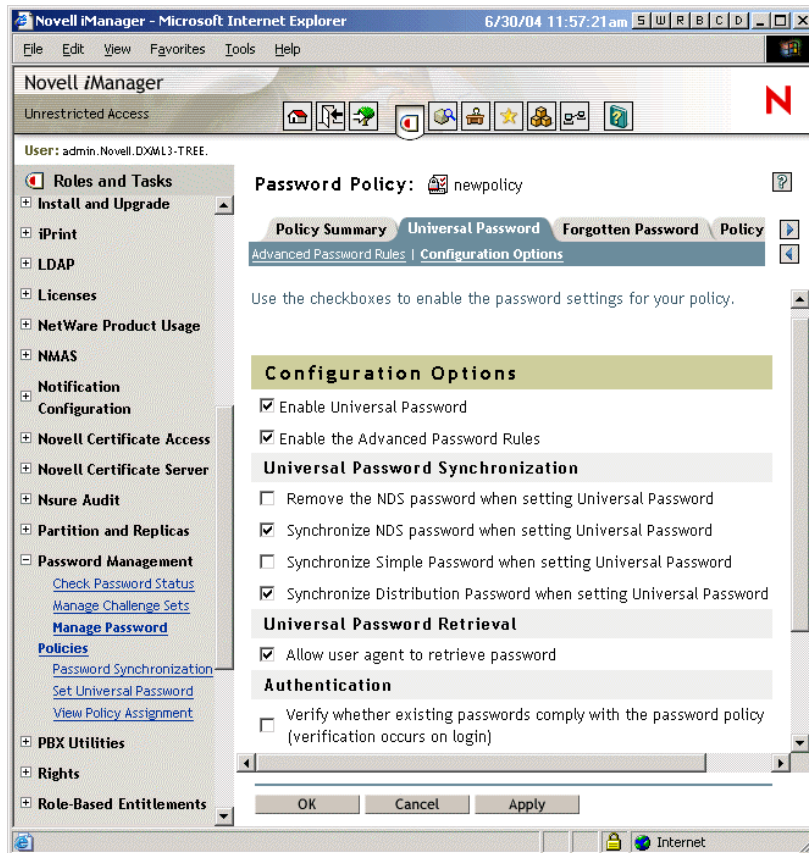
ユニバーサルパスワードは、eDirectory 8.9.1の新しいパスワード機能です。Advanced Password Rule（詳細パスワードルール）、パスワード同期、およびパスワードを忘れた場合のセルフサービスに関する多くの機能を使用する場合は、ユーザに対してユニバーサルパスワードを有効にする必要があります。

Password Policy（パスワードポリシー）を使用して、ユニバーサルパスワードを有効にするかどうかを指定できます。次に、Password Policy（パスワードポリシー）をユーザ（ツリー全体、コンテナまたはパーティション、あるいは特定のユーザ）に割り当てることができます。ツリー全体に対してユニバーサルパスワードをオンにする必要はありません。異なる Password Policy（パスワードポリシー）を使用すると、ユニバーサルパスワードの使用方法をニーズに合わせて変更できます。管理を簡素化するために、Password Policy（パスワードポリシー）はできるだけツリーの上位に割り当てておくことをお勧めします。

Novell Client™ や eDirectory のアップグレードなど、ユニバーサルパスワード用の環境を準備するための追加計画が必要になります。

また、NDS または通常パスワードのどちらをユニバーサルパスワードと同期化するかなど、Password Policy（パスワードポリシー）内で、ユニバーサルパスワードと NMAS の他の設定を編集することもできます。

次の図は、Password Policy（パスワードポリシー）のユニバーサルパスワード設定オプションを指定するプロパティページの例を示します。



Advanced Password Rule（詳細パスワードルール）の設定

Advanced Password Rule（詳細パスワードルール）では、次のように、許容できるパスワードの条件を定義できます。

- ◆ パスワードの構文
- ◆ パスワードのプロパティ
- ◆ パスワードの使用期限
- ◆ 特殊文字の使用
- ◆ パスワードの除外

重要：パスワードの除外は、セキュリティリスクになると考えられるいくつかの単語に対して使用すると便利です。除外リストを使用することもできますが、辞書などの長い単語リストに使用するためのものではありません。大量の除外単語を記述したリストを使用すると、サーバーのパフォーマンスに影響することがあります。パスワードに対する「辞書攻撃」から保護するには、長い除外リストを使用する代わりに、パスワードに数字を含めることを要求する Advanced Password Rule（詳細パスワードルール）を使用することをお勧めします。

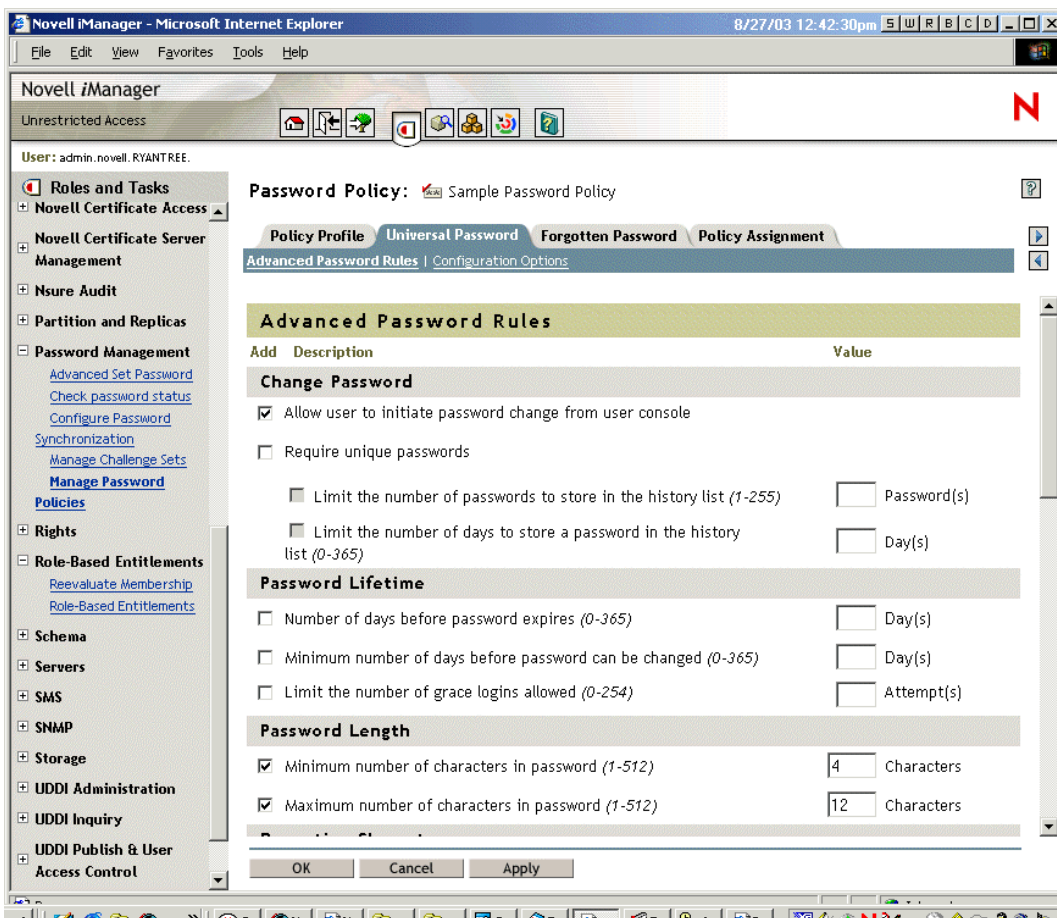
Password Policy (パスワードポリシー) で Advanced Password Rule (詳細パスワードルール) を使用するには、ユニバーサルパスワードを有効にする必要があります。ポリシーに対してユニバーサルパスワードを有効にしない場合、代わりに、NDS のパスワードに設定されているパスワード制限が適用されます。

注: Password Policy (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有効にすると、NDS パスワードの既存のパスワード設定ではなく、Advanced Password Rule (詳細パスワードルール) が適用されます。レガシーパスワード設定は無視されます。Password Policy (パスワードポリシー) の作成時に、以前の設定が自動的にマージまたはコピーされることはありません。

たとえば、NDS パスワードで使用する猶予ログイン回数の設定がある場合、ユニバーサルパスワードを有効にすると、Password Policy (パスワードポリシー) で Advanced Password Rule (詳細パスワードルール) に猶予ログイン設定を再作成する必要があります。

その後、Password Policy (パスワードポリシー) でユニバーサルパスワードを無効にした場合は、以前に設定していた既存のパスワード設定が有効になります。これらの設定は、NDS パスワードに対して適用されます。

次の図は、Password Policy (パスワードポリシー) の Advance Password Rule (Advanced Password Rule (詳細パスワードルール)) を指定するプロパティページの例を示します。



Password Policy（パスワードポリシー）への独自のパスワード変更メッセージの追加

[139 ページの「Password Policy（パスワードポリシー）への独自の Password Change Message（パスワード変更メッセージ）の追加」](#)を参照してください。

ユーザへのパスワードを忘れた場合のセルフサービスの提供

[116 ページの「ユーザへのパスワードを忘れた場合のセルフサービスの提供」](#)を参照してください。

ユーザへのパスワードのリセットセルフサービスの提供

[117 ページの「ユーザへのパスワードのリセットセルフサービスの提供」](#)を参照してください。

eDirectory ユーザへのポリシーの割り当て

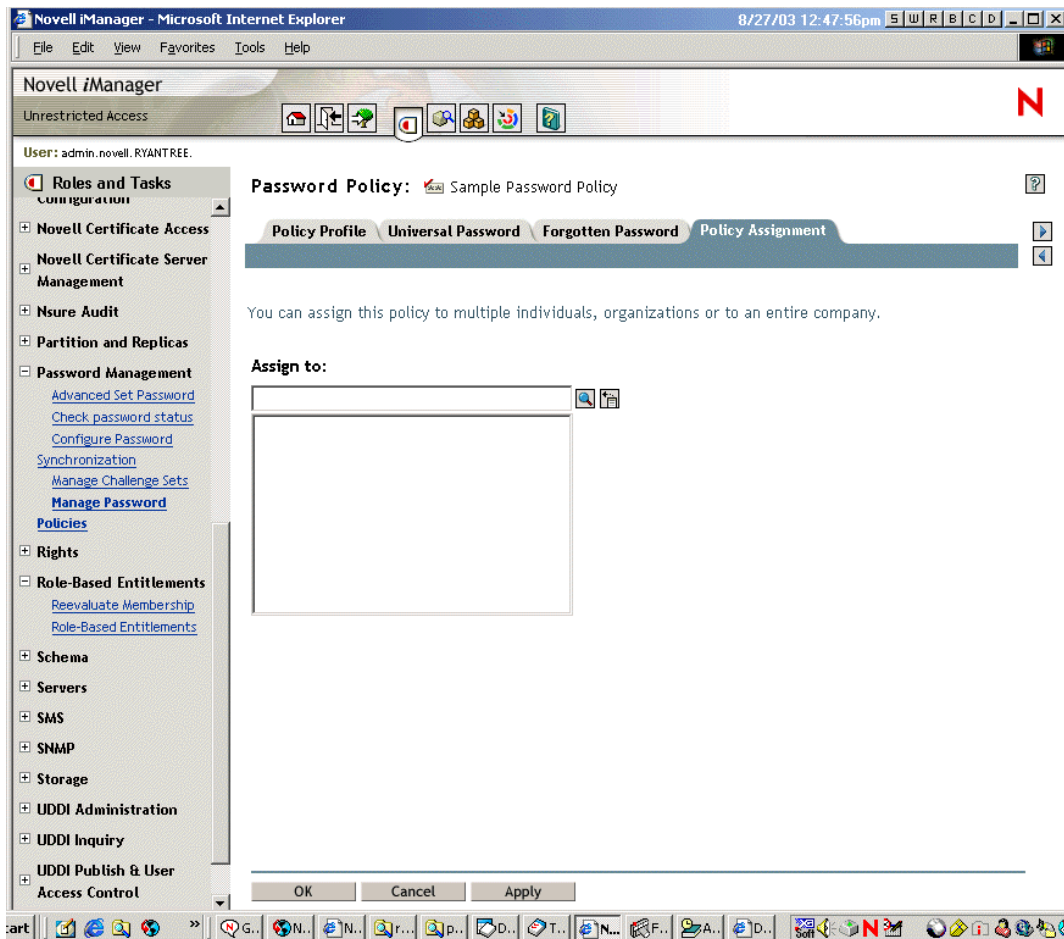
Password Policy（パスワードポリシー）を eDirectory 内のユーザに割り当てるには、ポリシーをツリー全体（ログインポリシーオブジェクトを使用）、特定のパーティションまたはコンテナ、または特定のユーザに割り当てます。

管理を簡素化するため、デフォルトのポリシーはツリー全体に割り当て、使用するその他のポリシーはできるだけツリーの上位に割り当てることをお勧めします。

NMAS は、ユーザに対してどの Password Policy（パスワードポリシー）が有効かを決定します。Password Policy（パスワードポリシー）をユーザに割り当てる方法については、[111 ページの「ユーザへの Password Policy（パスワードポリシー）の割り当て」](#)を参照してください。

パスワード同期を使用する場合は、Password Policy（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。Password Policy（パスワードポリシー）はツリー中心で割り当てられます。対照的に、パスワード同期はサーバベースでドライバごとに設定されます。パスワード同期から期待どおりの結果を得るには、パスワード同期のドライバを実行し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存在するユーザが、Password Policy（パスワードポリシー）を割り当ててユニバーサルパスワードを有効にしているコンテナと一致していることを確認してください。パーティションルートコンテナに Password Policy（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 Password Policy（パスワードポリシー）が割り当てられます。

次の図は、どのオブジェクトに Password Policy（パスワードポリシー）を割り当てるかを指定するプロパティページの例を示します。



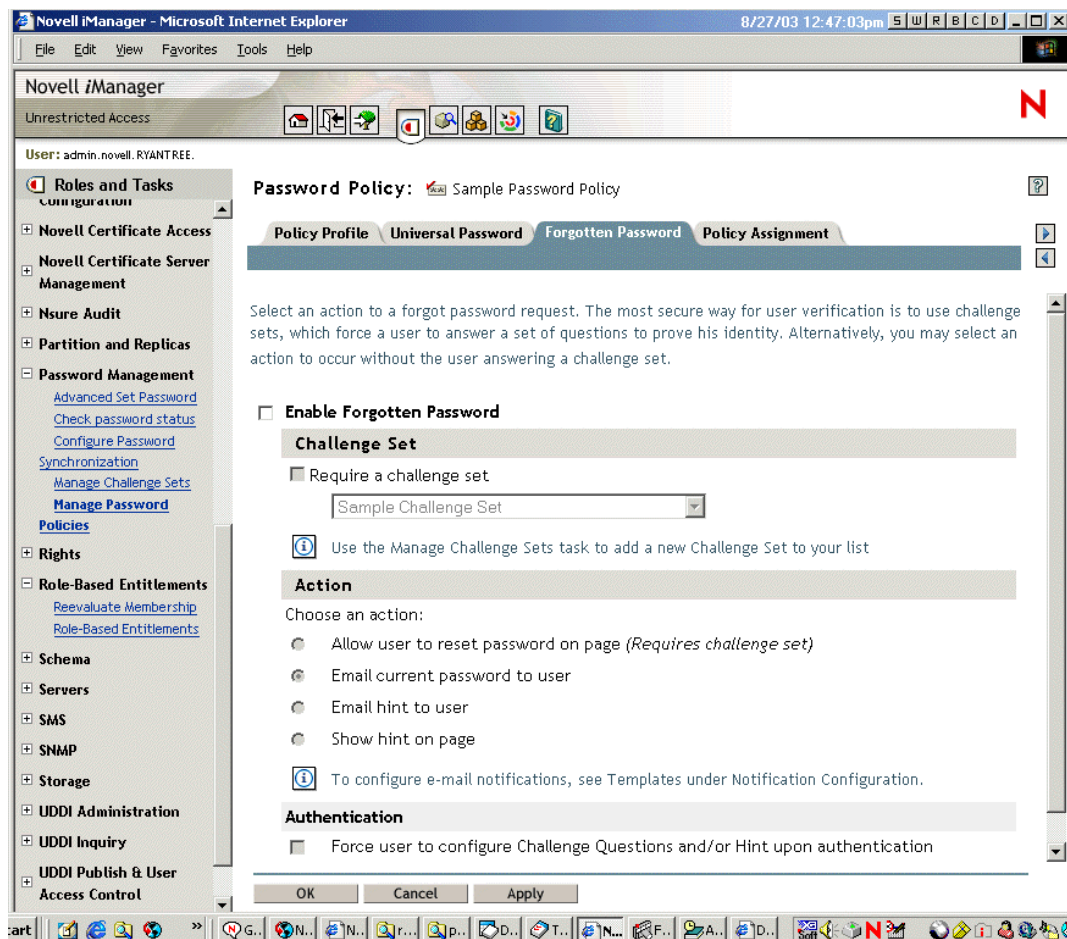
eDirectory 内でのポリシーの適用

ツリー内のユーザに Password Policy（パスワードポリシー）を割り当てる場合、以降のパスワード変更は、そのポリシーの Advanced Password Rule（詳細パスワードルール）に準拠している必要があります。ブラウザでは、パスワードルールは、ユーザがパスワードを変更するページに表示されます。Novell Client 4.9 SP2 以降では、ルールも表示されます。どちらの方法でも、準拠しないパスワードは拒否されます。NMAS は、これらのルールを適用するアプリケーションです。

既存のパスワードがルールに準拠しているかを確認し、準拠していない既存のパスワードは変更しなければならないように指定できます。

また、ユーザが iManager または iManager セルフサービスコンソールを介して認証する場合に、有効にした、パスワードを忘れた場合の機能の設定を求めるメッセージを表示するように指定することもできます。これは、認証後のサービスと呼ばれます。たとえば、ユーザがパスワードを忘れた場合、電子メールでパスワードヒントをユーザに送信できます。このパスワードヒントをユーザに作成させる場合は、認証後サービスを使用して、ログイン時にパスワードヒントを作成するようユーザに要求するメッセージを表示できます。

次の図が示すように、認証後設定は、[Forgotten Password] プロパティページの最後のオプションです。



接続システムへのポリシーの適用

パスワード同期を使用している場合、各ドライブに設定が提供され、Password Policy（パスワードポリシー）の Advanced Password Rule（詳細パスワードルール）を適用できます。

このポリシーを設定するには、次の手順を実行します。

- ◆ 一般に、Identity Manager が接続システムによって発行されたパスワードを受け付けるかどうかを決定します。
- ◆ 接続システムから受信するパスワードに対してポリシーを適用します。パスワードが準拠しない場合、Identity Manager はそのパスワードを受け付けません。
- ◆ 準拠していないパスワードをリセットすることによって、接続システムにポリシーを適用します。Identity Manager に入るパスワードが準拠していない場合、Identity Manager は識別ポータルへのパスワード変更を拒否できます。また、既存の Identity Manager 配布パスワードを使用して、接続システム上のパスワードをリセットすることもできます。
- ◆ パスワード同期が成功しなかった場合、ユーザに通知します。たとえば、ユーザが接続システム上で準拠していないパスワードを作成し、Identity Manager がそのパスワードを受け付けなかった場合、パスワード変更が同期化されなかったことをユーザに電子メールで通知できます。

Advanced Password Rule（詳細パスワードルール）と Identity Manager 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 Password Policy（パスワードポリシー）を調査して、eDirectory Password Policy（パスワードポリシー）の Advanced Password Rule（詳細パスワードルール）に互換性があることを確認し、パスワードを正常に同期化できるようにすることをお勧めします。

Password Policy（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。

Password Policy（パスワードポリシー）はツリー中心で割り当てられます。対照的に、パスワード同期はドライバごとに設定されます。ドライバはサーバベースでインストールされ、マスタレプリカまたは読み書き可能レプリカ内に存在するユーザのみを管理できます。パスワード同期から期待どおりの結果を得るには、パスワード同期のドライバを実行し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存在するユーザが、Password Policy（パスワードポリシー）を割り当ててユニバーサルパスワードを有効にしているコンテナと一致していることを確認してください。パーティションルートコンテナに Password Policy（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 Password Policy（パスワードポリシー）が割り当てられます。

パスワードフローを指定する方法については、[162 ページの「グローバル設定値を使用して作成するパスワード同期設定」](#)を参照してください。

ユーザに対して有効な Password Policy（パスワードポリシー）の表示

iManager では、ユーザに対して有効なポリシーを確認できます。[112 ページの「ユーザに割り当てられているポリシーの確認」](#)を参照してください。

ユーザのユニバーサルパスワードの設定

管理者、またはヘルプデスクの担当者がユーザのユニバーサルパスワードを設定できるように、新しい iManager プラグインが用意されています。このプラグインでは、ユーザの Password Policy（パスワードポリシー）の Advanced Password Rule（詳細パスワードルール）が表示されます。これにより、管理者またはヘルプデスクユーザは、準拠したユニバーサルパスワードを作成できます。[Set Universal Password] タスクは、パスワード管理役割にあります。

Password Policy（パスワードポリシー）の計画

このセクションでは、次の項目について説明します。

- ◆ [103 ページの「Password Policy（パスワードポリシー）をツリー内に割り当てる方法の計画」](#)
- ◆ [103 ページの「Password Policy（パスワードポリシー）のルールの計画」](#)
- ◆ [103 ページの「ユーザのログインおよびパスワード変更方法の計画」](#)

Password Policy（パスワードポリシー）をツリー内に割り当てる方法の計画

管理を簡素化するため、デフォルトのポリシーはツリー全体に割り当て、使用するその他のポリシーはできるだけツリーの上位に割り当てることをお勧めします。

NMAS は、ユーザに対してどの Password Policy（パスワードポリシー）が有効かを決定します。Password Policy（パスワードポリシー）をユーザに割り当てる方法については、[111 ページの「ユーザへの Password Policy（パスワードポリシー）の割り当て」](#)を参照してください。

Password Policy（パスワードポリシー）のルールの計画

Password Policy（パスワードポリシー）で Advanced Password Rule（詳細パスワードルール）を使用すると、パスワードのビジネスポリシーを適用できます。

Password Policy（パスワードポリシー）のパスワードルールが表示されるのは、Novell Client（4.9 SP2）と iManager セルフサービスコンソールのみです。ユーザが LDAP サーバを介してパスワードを変更する場合や、接続システム上でパスワードを変更する場合、準拠したパスワードの作成に役立つパスワードルールをユーザがすぐに参照できるようにする必要があります。

パスワード同期を使用する場合は、Password Policy（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。Password Policy（パスワードポリシー）はツリー中心で割り当てられます。対照的に、パスワード同期はサーバベースでドライブごとに設定されます。パスワード同期から期待どおりの結果を得るには、パスワード同期のドライブを実行し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存在するユーザが、Password Policy（パスワードポリシー）を割り当ててユニバーサルパスワードを有効にしているコンテナと一致していることを確認してください。パーティションルートコンテナに Password Policy（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 Password Policy（パスワードポリシー）が割り当てられます。

ユーザのログインおよびパスワード変更方法の計画

ユーザは、複数の方法でログインまたはパスワード変更を実行できます。

どの方法であっても、関連付けられた LDAP サーバ、NMAS 2.3、および iManager 2.0.2 以降を使用して、eDirectory 8.7.1 以降に環境をアップグレードする必要があります。ユニバーサルパスワードをサポートするためのアップグレードの詳細については、『[Novell Modular Authentication Services \(NMAS\) 2.3 Administration Guide \(Novell Modular Authentication Services \(NMAS\) 2.3 管理ガイド\)](#) (<http://www.novell.com/documentation/nmas23/index.html>)』を参照してください。

この節では、各状況でユニバーサルパスワードをサポートするための追加要件について説明します。

- ◆ [104 ページの「Novell Client」](#)
- ◆ [105 ページの「iManager と iManager セルフサービスコンソール」](#)
- ◆ [105 ページの「LDAP などのプロトコル」](#)
- ◆ [105 ページの「接続システム」](#)

Novell Client を使用している場合は、バージョン 4.9 SP2 以降にアップグレードします。

環境によっては、ユーザは、iManager セルフサービスコンソールまたは他の企業ポータルからログインできるため、Novell Client の使用は必須ではありません。また、AD または NT 上のパスワード同期にも Novell Client は必要ありません。

次の表は、ユニバーサルパスワードに関する Novell Client バージョン間の違いを説明し、レガシークライアントの推奨処理方法を示します。

Novell Client バージョン	ログイン	パスワード変更
4.9 より前	NMAS を経由しないため、ユニバーサルパスワードをサポートしません。 代わりに、NDS パスワードを使用して直接ログインします。	NMAS を経由せず、NDS パスワードを直接変更します。 ユニバーサルパスワードを使用している場合、NDS パスワードとユニバーサルパスワードの同期が維持されない「パスワードドリフト」という問題が発生することがあります。これを防ぐには、次の3つの方法があります。 <ul style="list-style-type: none"> すべてのクライアントをバージョン 4.9 以降にアップグレードする。 コンテナの属性値を使用して、レガシークライアントがパスワードを変更できないようにする。この解決方法では、レガシークライアントはこれまでどおりログインできますが、パスワードは変更できません。パスワードの変更は、最新クライアントまたは iManager を使用して実行する必要があります。106 ページの「レガシー Novell Client によるパスワード変更の防止」を参照してください。 Password Policy (パスワードポリシー) 設定を使用して、ユニバーサルパスワードの設定時に NDS パスワードを削除する。NDS パスワードを使用してログインすることも、パスワードを変更することもできなくなるため、かなり思い切った方法です。
4.9	ユニバーサルパスワードをサポートします。	ユニバーサルパスワードの Password Policy (パスワードポリシー) ルールを適用します。 ユーザが準拠しないパスワードを作成しようとした場合、パスワード変更は拒否されます。ただし、ルールのリストはユーザに表示されません。
4.9 SP2	ユニバーサルパスワードをサポートします。	ユニバーサルパスワードの Password Policy (パスワードポリシー) ルールを適用します。 さらに、準拠したパスワードの作成に役立つルールも表示されます。

iManager と iManager セルフサービスコンソール

iManager セルフサービスコンソールはパスワードセルフサービスを備えているため、ユーザはパスワードをリセットしたり、Password Policy（パスワードポリシー）で提供されていれば、パスワードを忘れた場合のセルフサービスを設定したりできます。iManager サーバ上のユーザは、<https://www.servername.com/nps> などの URL を使用して、iManager セルフサービスコンソールにアクセスできます。たとえば、<https://www.myiManager.com/nps> などです。

- ◆ ユーザが iManager 2.0.2 以降をサポートするブラウザを使用していることを確認します。
- ◆ Password Policy（パスワードポリシー）で [Synchronize NDS password When Setting Universal Password] を選択することをお勧めします。これはデフォルト設定です。
- ◆ NMAS 通常パスワードのログイン方法がインストールされていることを確認します。これは、eDirectory のインストール時にインストールするか、後で手動でインストールできます。

LDAP などのプロトコル

すでに説明したように、eDirectory、LDAP サーバ、NMAS、および iManager がユニバーサルパスワードをサポートするようにアップグレードされていることを確認します。

AFP、CIFS などのプロトコルでユニバーサルパスワードを使用する方法の詳細については、『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Novell Modular Authentication Services (NMAS) 2.3 管理ガイド)* (<http://www.novell.com/documentation/nmas23/index.html>)』の「Deploying Universal Password（ユニバーサルパスワードの展開）」を参照してください。

接続システム

Identity Manager パスワード同期を使用する場合は、ユーザパスワードを正常に変更できるように、次の要件を満たしていることを確認します。

- ◆ システムの DirXML ドライバが Identity Manager 形式にアップグレードされている。
- ◆ [176 ページの「新しいドライバ設定と Identity Manager パスワード同期」](#) および [178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」](#) の説明に従って、DirXML ドライバ設定に新しい Password Synchronization Policy（パスワード同期ポリシー）が含まれている。
- ◆ パスワード同期設定で、ユニバーサルパスワードを使用すること、および双方向のパスワード同期が必要な場合は配布パスワードも使用することが指定されている。
- ◆ 必要に応じて、パスワードを取得するために、接続システムにパスワードフィルタが展開されている。

詳細については、[9 章 151 ページの「接続システム間のパスワード同期」](#) を参照してください。

レガシー Novell Client によるパスワード変更の防止

Novell Client の 4.9 以前のバージョンについては、ログインとパスワードの変更は、NMAS を経由せずに NDS パスワードに直接送られるため、ユニバーサルパスワードはサポートされていません。

ユニバーサルパスワードを使用している場合、レガシー Client を使用してパスワードを変更すると、NDS パスワードとユニバーサルパスワードの同期が維持されない「パスワードドリフト」という問題が発生することがあります。

この問題を防ぐ 1 つの方法は、バージョン 4.9 より以前の Client がパスワードを変更できないようにすることです。これは、特定のルートコンテナ、クラス、またはオブジェクトで eDirectory 属性を使用して行います。属性は eDirectory 8.7.1 以降のスキーマの一部であり、eDirectory 8.7.0 以前ではサポートされていません。

レガシー Client で使用される NDS パスワードの変更方法は、NDAP パスワード管理と呼ばれます。次のリストは、属性を使用してパーティションレベルで NDAP パスワード管理を無効にする方法を説明しています。必要に応じて、他の属性を使用して、パスワード管理をクラスごとまたはオブジェクトごとに有効できます。

- ◆ **ndapPartitionPasswordMgmt** - パーティションレベルのコンテナ用。属性が存在しない場合、または値がパーティションレベルで設定されていない場合、NDAP パスワード管理は有効になります。

NDAP パスワード管理を無効にするには、この属性をパーティションに追加して 0 に設定します。もう一度有効にするには、1 に設定します。

次に示す他の属性を使用すると、NDAP パスワード管理がパーティションレベルで無効になっていても、クラスまたはオブジェクトで NDAP パスワード管理を使用できます。ただし、NDAP パスワード管理がパーティションレベルで有効になっている場合、NDAP パスワード管理は、クラスおよびエントリレベルのポリシーには関係なく、そのパーティション内のすべてのオブジェクトに対して有効になります。

- ◆ **ndapClassPasswordMgmt** - クラス用。この属性をクラス定義に追加すると、パーティションレベルのポリシーで NDAP パスワード管理が無効に指定されていても、クラスで NDAP パスワード管理を使用できます（この属性が存在すれば NDAP パスワード管理は有効になります。値は重要ではありません）。
- ◆ **ndapPasswordMgmt** - 特定のオブジェクト用。この属性を特定のオブジェクトに追加して値を 1 に設定すると、パーティションまたはクラスで NDAP パスワード管理が無効に指定されていても、オブジェクトで NDAP パスワード管理を使用できます。

0 に設定すると、NDAP パスワード管理は無効になります。ただし、パーティションレベルでも NDAP パスワード管理が無効になっている場合に限りです。

重要： eDirectory 8.7.0 以前はこの機能をサポートしていません。ツリーに eDirectory 8.7.1 サーバ以降と eDirectory 8.7.0 サーバ以前が存在する場合、2 つのサーバが 1 つのパーティションを共有するため、そのパーティション上で NDAP パスワード管理を無効にすると、不安定な結果になります。8.7.1 サーバでは設定が適用され、レガシークライアントは NDS パスワードを変更できなくなります。一方、8.7.0 サーバでは設定が適用されないため、ユーザが 8.7.0 サーバを介して NDS パスワードを変更しようとする、変更が成功します。

Password Policy（パスワードポリシー）の使用に関する前提条件

Password Policy（パスワードポリシー）のすべての機能を利用する場合は、いくつかの手順を完了して環境を用意する必要があります。

- 1 ユニバーサルパスワードをサポートするように環境をアップグレードします。

詳細については、『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Novell Modular Authentication Services (NMAS) 2.3 管理ガイド)* (<http://www.novell.com/documentation/nmas23/index.html>)』を参照してください。

ユニバーサルパスワードを展開する準備が整っていない場合、または eDirectory 8.6.2 を使用している場合は、[289 ページの「eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート」](#)で、ユニバーサルパスワードで使用できる Password Policy（パスワードポリシー）機能を確認してください。

- 2 ユニバーサルパスワードをサポートするようにクライアント環境をアップグレードします。

詳細については、[103 ページの「ユーザのログインおよびパスワード変更方法の計画」](#)および、『*Novell Modular Authentication Services (NMAS) 2.3 管理ガイド* (<http://www.novell.com/documentation/nmas23/index.html>)』の「Deploying Universal Password（ユニバーサルパスワードの展開）」を参照してください。

- 3 iManager の設定時（iManager のインストール時またはインストール後）に iManager Configuration Wizard を実行していない場合は、実行する必要があります。

重要： iManager Configuration Wizard を実行すると、iManager は RBS モードで実行されます。つまり、管理者が自分自身に特定の役割を割り当てていない限り、タスクを参照できなくなります。管理者に役割を割り当てて、iManager のすべてのタスクへのアクセスを付与してください。

- 4 [4 章 47 ページの「インストール」](#)の説明に従って、Identity Manager をインストールします。

パスワード管理のプラグインは、このインストールの一部として iManager Web サーバにインストールされます。

Password Policy（パスワードポリシー）については、Identity Manager と接続システムの間でパスワードを同期化するときパスワード同期を使用して Password Policy（パスワードポリシー）を適用しない限り、ドライバ設定を変更する必要はありません。

- 5 iManager Web サーバと eDirectory が同じマシン上で実行されている場合でも、これらの間に SSL が設定されていることを確認します。

これは、NMAS 2.3 以降、および[ステップ 6](#)の要件です。

- 6 eDirectory の LDAP グループオブジェクトとサーバオブジェクトが、簡単なバインドのために TLS を要求するように設定されていることを確認します。

これは iManager の設定時のデフォルト設定です。パスワードのセルフサービス機能に対しては、単純なバインドのために TLS を要求することをお勧めします。また、iManager タスクの使用（[Password Management] > [Set Universal Password]）にも必要です。

単純なバインドのために TLS を要求する場合、LDAP SSL ポートの追加設定は必要ありません。

重要： 単純なバインドを要求しないように選択した場合、ユーザはクリアテキストパスワードを使用して iManager セルフサービスコンソールにログインできます。

このオプションを使用することはできますが、別の手順が必要です。

デフォルトでは、パスワードのセルフサービス機能は、LDAP SSL ポートが、PortalServlet.properties ファイルの System.DirectoryAddress 設定で指定されているポートであると想定します。異なる LDAP SSL ポートの場合、PortalServlet.properties ファイルに次のキーペアを追加することによって、正しいポートを指定する必要があります。

```
LDAPSSLPort=your_port_number
```

たとえば、Tomcat を実行している場合は、tomcat¥webapps¥nps¥WEB_INF ディレクトリ内の PortalServlet.properties ファイルにこのキーペアを追加します。

- 7 パスワードを忘れた場合の機能の電子メール通知を有効にするには、[220 ページの「電子メール通知の設定」](#)の手順を完了します。

SMTP サーバを設定し、電子メールテンプレートをカスタマイズする必要があります。

- 8 (NetWare 6.5 ユーザのみ) NetWare 6.5 で使用できるようにユニバーサルパスワードを設定済みの場合は、[108 ページの「\(NetWare 6.5 のみ\) ユニバーサルパスワード割り当ての再作成」](#)の手順を完了します。

これで、Password Policy (パスワードポリシー) のすべての機能を使用できます。[110 ページの「Password Policy \(パスワードポリシー\) の作成」](#)に説明されている手順に従って、ポリシーを作成してください。

ユニバーサルパスワードなしでの Password Policy (パスワードポリシー) の展開

Password Policy (パスワードポリシー) とパスワード同期のすべての機能を使用できるように、環境を準備してユニバーサルパスワードをオンにすることをお勧めします。ただし、このための準備が整っていなくても、一部の機能は、ユニバーサルパスワードを展開せずに使用できます。

リストについては、[289 ページの「eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート」](#)を参照してください。このリストでは、ユニバーサルパスワードが無効な場合に eDirectory 8.6.2 または eDirectory 8.7.3 で使用できる機能について説明しています。

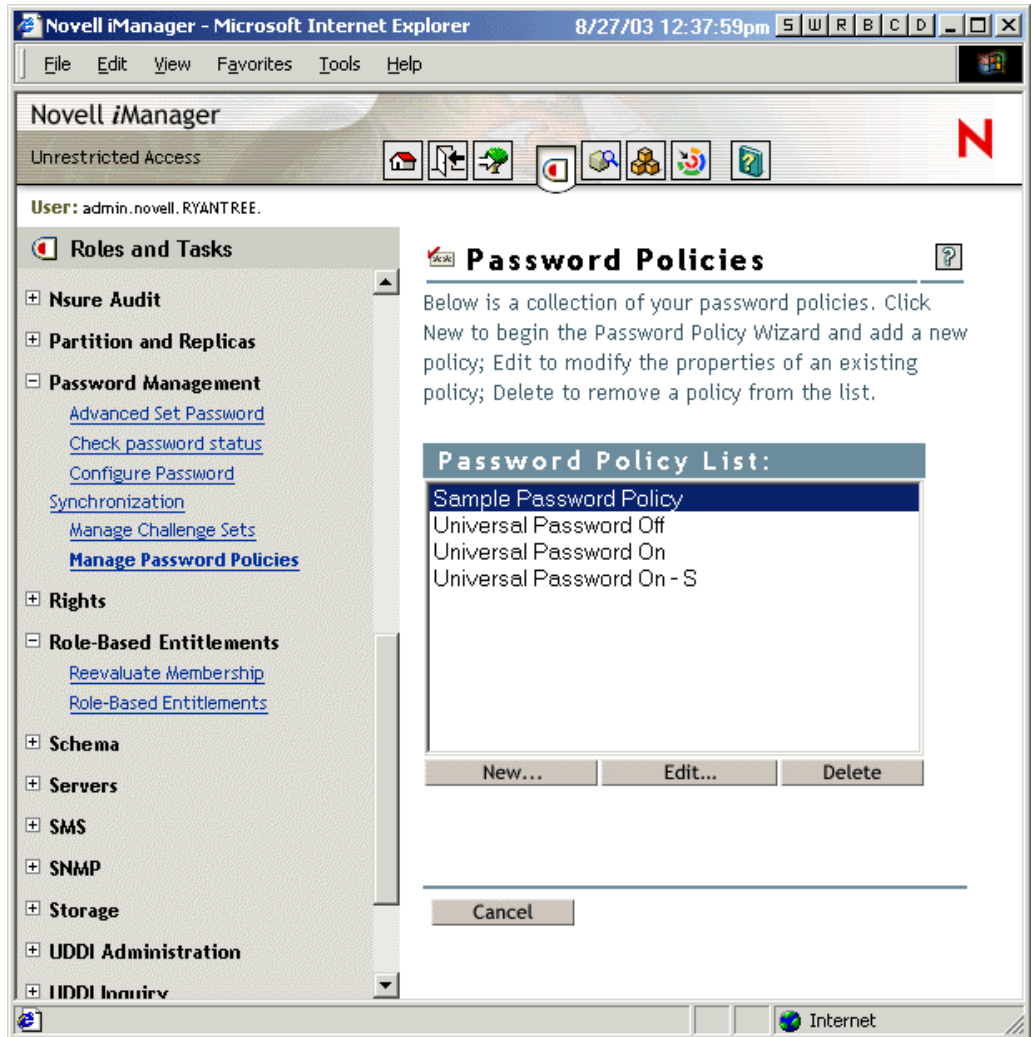
(NetWare 6.5 のみ) ユニバーサルパスワード割り当ての再作成

NetWare 6.5 で使用できるようにユニバーサルパスワードを設定済みの場合は、古い Password Policy (パスワードポリシー) を削除し、新しいプラグインと Password Policy (パスワードポリシー) を使用する必要があります。

- ◆ Identity Manager をインストールすると、NetWare 6.5 でユニバーサルパスワード用に使用されていた NMAS プラグインは使用できなくなります。代わりに、[Password Management] > [Manage Password Policies] の順に選択すると、より多くの機能を利用できます。
- ◆ 新しいプラグインで初めて [Manage Password Policies] を使用すると、次の編集できないリストに 3 つのポリシーオブジェクトが表示されます。
 - ◆ Universal Password On
 - ◆ Universal Password Off
 - ◆ Universal Password On - S

これらのオブジェクトは、NetWare 6.5 でのユニバーサルパスワードの実装に使用されていました。Identity Manager で提供されている Password Policy (パスワードポリシー) の追加の利点を活用するには、これらを削除する必要があります。

次の図に例を示します。



古いポリシーオブジェクトを削除して、Password Policy（パスワードポリシー）を使用してポリシーを再作成する

- 1 ユニバーサルパスワードをツリーのどこで有効にするかを決定します。
 - ◆ NetWare 6.5 プラグインで初めてユニバーサルパスワードを設定したときと同じコンテナをオンにする場合は、**ステップ 2**に進みます。
 - ◆ ツリーのすべての場所でオンにする場合は、ユニバーサルパスワードを有効にして新しい Password Policy（パスワードポリシー）を作成し、ログインポリシーオブジェクトに割り当てます。続いて、**ステップ 4**に進み、古いポリシーを削除します。
- 2 NetWare 6.5 に付属のプラグインを使用してユニバーサルパスワードを設定したときにユニバーサルパスワードを有効にしたツリーを検索します。

古いプラグインを使用して割り当てが実行された場所はプラグインによって表示されないため、この手順が必要です。代わりに、ツリーを検索して、該当する割り当てを見つけます。

- 2a 次のいずれかの値が入力された nspmPasswordPolicyDN 属性を持つオブジェクトをツリーで検索します。
 - ◆ Universal Password On
 - ◆ Universal Password On - S
- 2b 検索結果であるすべてのコンテナを書き留めておきます。これらが、ユニバーサルパスワードがオンになっているコンテナです。
- 3 以前にユニバーサルパスワードを割り当てた同じコンテナにユニバーサルパスワードを割り当てる場合は、ユニバーサルパスワードを有効にし、1つまたは複数の新しい Password Policy (パスワードポリシー) を作成して同じコンテナに割り当てます。

ステップ 2 のコンテナリストを参照し、割り当てが一致していることを確認してください。
- 4 [Password Management] > [Manage Password Policies] の順に進み、最初の NetWare 6.5 実装から残っている次のポリシーオブジェクトを削除します。
 - ◆ Universal Password Off
 - ◆ Universal Password On
 - ◆ Universal Password On - S

古いポリシーオブジェクトを削除したら、パスワードのニーズを満たす新しい Password Policy (パスワードポリシー) を使用できます。

Password Policy (パスワードポリシー) の作成

- 1 107 ページの「Password Policy (パスワードポリシー) の使用に関する前提条件」の手順を完了していることを確認します。これらの手順によって、Password Policy (パスワードポリシー) のすべての機能を使用できます。
- 2 iManager で、[Password Management] > [Manage Password Policies] の順に選択します。
- 3 [New] をクリックして新しい Password Policy (パスワードポリシー) を作成します。
- 4 ウィザードの手順に従って、ポリシーの Advanced Password Rule (詳細パスワードルール)、ユニバーサルパスワードの設定オプション、およびパスワードを忘れた場合の機能を設定します。

各手順の詳細については、オンラインヘルプ、および 7 章 95 ページの、「Password Policy (パスワードポリシー) を使用したパスワードの管理」と 8 章 115 ページの、「パスワードセルフサービス」の情報を参照してください。

ユーザへの Password Policy（パスワードポリシー）の割り当て

管理を簡素化するために、Password Policy（パスワードポリシー）はできるだけツリーの上位に設定することをお勧めします。

ポリシーは、1つまたは複数のオブジェクトに割り当てるとは有効になりません。Password Policy（パスワードポリシー）は次のオブジェクトに割り当てることができます。

- ◆ ログインポリシーオブジェクト

ツリー内のすべてのユーザに対してデフォルトの Password Policy（パスワードポリシー）を作成することをお勧めします。このためには、ポリシーを作成して、ログインポリシーオブジェクトに割り当てます。ログインポリシーオブジェクトは、ツリーのルートの直下にあるセキュリティコンテナにあります。

- ◆ パーティションルートであるコンテナ

パーティションのルートであるコンテナにポリシーを割り当てると、ポリシーの割り当ては、サブコンテナ内のユーザを含む、そのパーティション内のすべてのユーザに継承されます。コンテナがパーティションルートかどうかを判断するには、コンテナを参照し、その横に表示されているパーティションアイコンが次の例のように表示されているかどうかを確認します。

- ◆ パーティションルートではないコンテナ

パーティションのルートではないコンテナにポリシーを割り当てると、ポリシーの割り当ては、そのパーティション内に保持されているユーザにのみ継承されません。サブコンテナ内に保持されているユーザには継承されません。パーティションルートではないコンテナ下のすべてのユーザにポリシーを適用する場合は、ポリシーを各サブコンテナに個々に割り当てする必要があります。

- ◆ 特定のユーザ

注： ドライバセットオブジェクトに対しては、特別な Password Policy（パスワードポリシー）が自動的に作成されます。

1人のユーザに対して同時に1つのポリシーのみが有効です。NMAS（Novell Modular Authentication Services）は、この順番でポリシーを検索し、見つかった最初のポリシーを適用することによって、ユーザに対して有効なポリシーを判断します。

1. 特定のユーザ割り当て - Password Policy（パスワードポリシー）が特定のユーザに割り当てられている場合、そのポリシーが適用されます。
2. コンテナ - ユーザに特定の割り当てが設定されていない場合、NMAS は、ユーザを保持するコンテナに割り当てられているポリシーを適用します。
3. パーティションルートコンテナ - ユーザまたはユーザの真上のコンテナにポリシーが割り当てられていない場合は、パーティションルートコンテナに割り当てられているポリシーが適用されます。
4. ログインポリシーオブジェクト - ユーザまたはその他のコンテナにポリシーが割り当てられていない場合は、ログインポリシーオブジェクトに割り当てられているポリシーが適用されます。これはツリー内のすべてのユーザのデフォルトポリシーです。

ユーザに割り当てられているポリシーの確認

1人のユーザに対して同時に1つのポリシーのみが有効です。特定のユーザまたはコンテナに対して有効なポリシーを確認するには、[iManager] > [Password Manager] > [View Policy Assignment] の順に進みます。

ツリー内に複数のポリシーがある場合、NMAは、111 ページの「ユーザへの Password Policy (パスワードポリシー) の割り当て」の説明に従って、どのポリシーをユーザに適用するかを決定します。

ユーザのパスワードの設定

管理者またはヘルプデスクの担当者は、iManager 内の新しいタスクを使用して、ユーザのユニバーサルパスワードを設定できます。このタスクでは、ユーザに対して有効な Password Policy (パスワードポリシー) のパスワードルールが表示されます。

- 1 iManager で、[Password Management] > [Set Universal Password] の順にクリックします。

ユーザに Password Policy (パスワードポリシー) が割り当てられていて、ユニバーサルパスワードが有効な場合、このタスクを使用してパスワードを変更できます。

ポリシーで Advanced Password Rule (詳細パスワードルール) が有効な場合は、従う必要のあるルールのリストが表示されます。

注: ユーザに対してユニバーサルパスワードが有効でない場合、[Advanced Password Set] タスクを実行するとエラーが表示され、パスワードは変更されません。ユーザにポリシーを割り当ててからもう一度このタスクを実行するか、[eDirectory Administration] > [Modify Object] の順に選択し、[Modify Object] タスクを使用してユーザの NDS パスワードを変更する必要があります。

- 2 ユーザのパスワードを作成し、表示されているすべてのパスワードルールに準拠していることを確認します。

ユーザのユニバーサルパスワードが変更されます。

現在の環境でパスワード同期が設定されている場合、ユーザの新しいパスワードは、それを受け付けるように設定されている接続システムに配布されます。

注: NMA 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回答する場合などに、管理者がユーザのパスワードを変更する場合、Password Policy (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、セキュリティ上の理由からパスワードは自動的に期限切れになります。Password Policy (パスワードポリシー) のこの設定は、Advanced Password Rule (詳細パスワードルール) にあり、[Number of days before password expires (0-365)] という名前が付けられています。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。

チャレンジセットの作成または変更

140 ページの「チャレンジセットの作成または変更」を参照してください。

パスワード通知機能の設定

220 ページの「電子メール通知の設定」の指示に従ってください。

Password Policy (パスワードポリシー) のトラブルシューティング

- ◆ iManager セルフサービスログイン時における完全な DN の要求 - ログインプロンプトで完全な DN を入力する必要がある場合、該当するユーザオブジェクトは、iManager/Portal 設定中に指定されたコンテナの下層には存在しない可能性があります。Portal Servlet Configuration Wizard (http://your_iManager_server/nps/servlet/) を実行して、コンテキストレスログイン用に追加のログインコンテナを指定する必要があります。パスワードを忘れた場合の機能も、この設定を使用してユーザの DN を解決します。
- ◆ ユーザに Password Policy (パスワードポリシー) が割り当てられていないことを示すエラー - [Set Universal Password] タスクから、ユーザに Password Policy (パスワードポリシー) が割り当てられていないことを知らせるエラーメッセージが表示される場合、そのユーザに Password Policy (パスワードポリシー) が割り当てられていることがわかっているときは、SSL に問題があると考えられます。
 - ◆ SSL 設定に問題があることを確認するには、[View Policy Assignment] タスクを使用して、そのユーザのポリシーを確認します。[View Policy Assignment] タスクで NMAS トランスポートエラーが表示される場合も、SSL が適切に設定されていないことを示している可能性があります。
 - ◆ iManager を実行している Web サーバと eDirectory の主ツリーの間で SSL が正しく設定されていることを確認します。Web サーバと eDirectory の間に証明書が設定されていることを確認します。

Windows 2000 マシン上で IIS を Web サーバとして iManager を実行している場合、iManager のインストール時に適切に証明書が自動的に設定されないため、これが問題になる可能性があります。

- ◆ 単純なバインドのために TLS を要求しない場合は、[ステップ 6 の注記および 107 ページの「Password Policy \(パスワードポリシー\) の使用に関する前提条件」](#)で説明されているように、正しい LDAP SSL ポートを指定していることを確認する必要があります。
- ◆ チャレンジ / レスポンス方式の質問の使用 - iManager 2.02 がサポートするブラウザを使用していることを確認します。
- ◆ 新しいコンテナ内のユーザへのアクセス権の付与 - iManager または Novell ポータル製品 (exteNd™ Director™ Standard Edition など) の 1 つを設定する場合は、ポータルユーザコンテナを指定してください。通常、ツリー内のすべてのユーザがポータル機能にアクセスできるように、ツリーの高レベルにあるコンテナを指定します。すべてのユーザがそのコンテナの下層に存在していれば、すべてのユーザに、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスへのアクセスが付与されます。

後でユーザが含まれるコンテナをポータルユーザコンテナ外に作成し、これらのユーザが、パスワードを忘れた場合の機能およびパスワードリセットの機能にアクセスできない場合は、その新しいコンテナの Challenge Response Setup、Change Universal Password、および Hint Setup というガジェットに明示的に権限を割り当てる必要があります。

新しいユーザをポータルユーザコンテナに追加する方法については、『[Novell exteNd Director Platform Edition Installation and Configuration Guide \(Novell exteNd Director Platform Edition のイントールと設定ガイド\)](http://www.novell.com/documentation/lg/nedpe41/configure/data/ajhotzv.html#ajhotzv) (<http://www.novell.com/documentation/lg/nedpe41/configure/data/ajhotzv.html#ajhotzv>)』の「Portal User (ポータルユーザ)」を参照してください。

- ◆ NMAS LDAP トランSPORTエラー – マルチサーバ環境に Identity Manager をインストールし、iManager で特定のパスワード管理プラグインを使用した場合、「NMAS LDAP Transport Error」から始まるエラーが表示されることがあります。

このエラーの一般的な原因の1つは、PortalServlet.properties ファイルが、Identity Manager に必要な NMAS™ 拡張機能を持たない LDAP サーバを指していることにあります。PortalServlet.properties ファイルを開き、LDAP サーバのアドレスが Identity Manager をインストールしたサーバと同じサーバであることを確認してください。

考えられるその他の原因：

- ◆ LDAP サーバが実行されていない。
- ◆ LDAP 用に、プラグインを実行する iManager サーバと LDAP サーバの間で SSL が設定されていない。
- ◆ iManager で他のツリーにログインしてリモートの Identity Manager DirXML サーバを管理する場合、リモートサーバの IP アドレスの代わりにサーバ名を使用すると、エラーが発生することがある。
- ◆ 認証するツリーのルート認証局証明書は、認証局証明書として Web サーバにインポートする必要があります。keytool.exe を使用して証明書を Web サーバにエクスポートできます (eGuide をインストールする場合、この証明書は設定処理中に Web サーバにエクスポートされます)。
- ◆ eDirectory 内の LDAP サーバグループオブジェクトは、単純なバインドに TLS を要求するように設定する必要があります。このオプションは、iManager の LDAP サーバオブジェクトプロパティを編集することで設定します。
- ◆ Identity Manager パスワード同期を使用する場合は、次の節も参照してください。
 - ◆ [234 ページの「パスワード同期のトラブルシューティング」](#)
 - ◆ [184 ページの「パスワード同期の実装」](#)に記載されている各シナリオのトラブルシューティングに関する節
 - ◆ [ドライバマニュアルの Web サイト \(http://www.novell.com/documentation/lg/dirxmldrivers\)](http://www.novell.com/documentation/lg/dirxmldrivers) に掲載されている、関連する特定のドライブのマニュアル

8

パスワードセルフサービス

Password Policy（パスワードポリシー）を使用すると、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスに関するオプションをユーザーに提供することによって、ヘルプデスクのコストを削減することができます。

パスワードセルフサービスを使用する前に、7章 95 ページの、「[Password Policy（パスワードポリシー）を使用したパスワードの管理](#)」で Password Policy（パスワードポリシー）の詳細を確認してください。

この節では、次の項目について説明します。

- ◆ [115 ページの「セルフサービス機能の概要](#)」
- ◆ [118 ページの「セルフサービスの使用に関する前提条件](#)」
- ◆ [118 ページの「パスワードセルフサービスのログイン方法の計画](#)」
- ◆ [118 ページの「エンドユーザーへのパスワードを忘れた場合のセルフサービスの提供](#)」
- ◆ [138 ページの「ユーザーへのパスワードのリセットセルフサービスの提供](#)」
- ◆ [139 ページの「Password Policy（パスワードポリシー）への独自の Password Change Message（パスワード変更メッセージ）の追加](#)」
- ◆ [140 ページの「チャレンジセットの作成または変更](#)」
- ◆ [140 ページの「パスワードセルフサービスの通知の設定](#)」
- ◆ [140 ページの「パスワードセルフサービスのテスト](#)」
- ◆ [141 ページの「企業ポータルへのパスワードセルフサービスの追加](#)」
- ◆ [149 ページの「パスワードセルフサービスのトラブルシューティング](#)」

セルフサービス機能の概要

Password Policy（パスワードポリシー）には、パスワードを忘れた場合のヘルプデスクへの問い合わせを減らすための、パスワードを忘れた場合のセルフサービス、および管理者が Password Policy（パスワードポリシー）内に指定したルールを表示しながらユーザーが自らのパスワード変更できるパスワードのリセットセルフサービスが含まれます。これらの機能には、iManager のセルフサービスコンソールを介してアクセスします。

パスワード管理のほとんどの機能では、ユニバーサルパスワードを有効にする必要があります。iManager セルフサービスコンソールを既存の企業ポータルに統合し、パスワードを忘れた場合のセルフサービスとパスワードのリセットセルフサービスにユーザーが簡単にアクセスできるようにするのが理想的です。

新しいパスワードセルフサービス機能では、次の操作を実行できます。

- ◆ 99 ページの「ユーザへのパスワードを忘れた場合のセルフサービスの提供」
- ◆ 99 ページの「ユーザへのパスワードのリセットセルフサービスの提供」

ユーザへのパスワードを忘れた場合のセルフサービスの提供

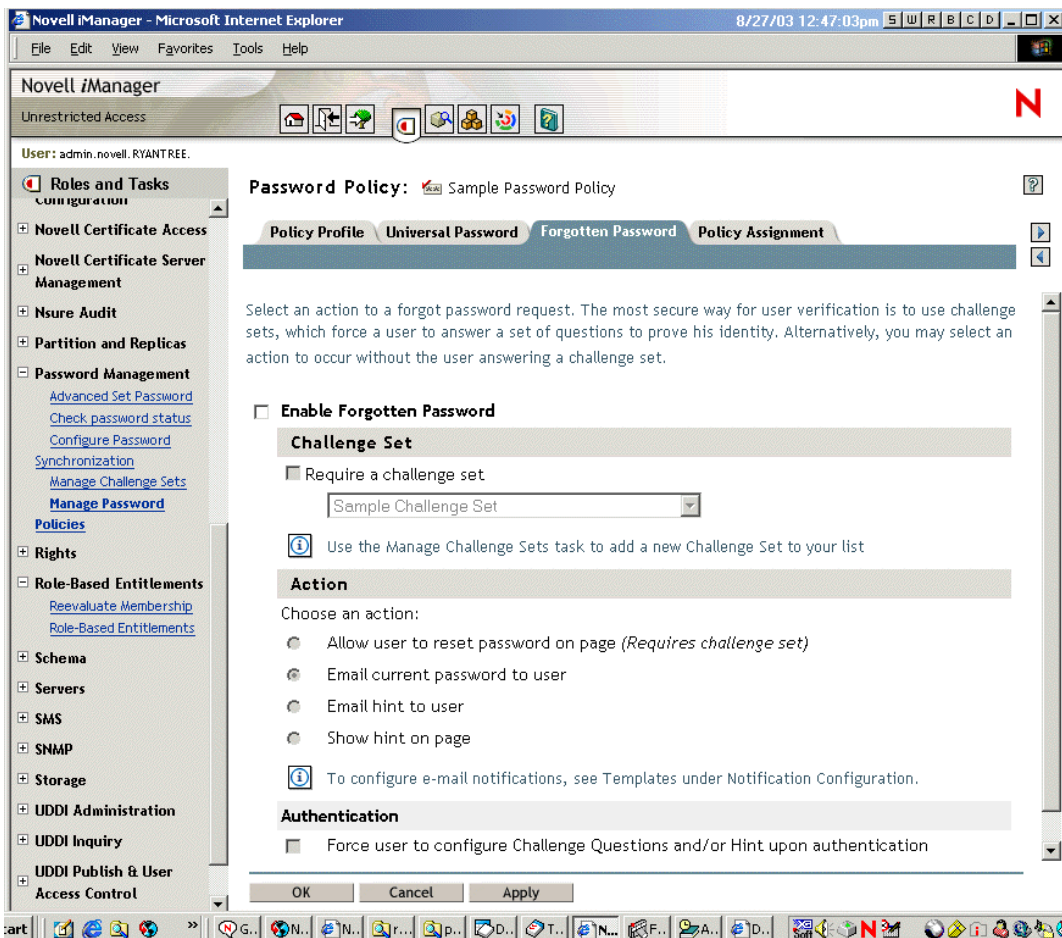
Password Policy（パスワードポリシー）を使用すると、ヘルプデスクに問い合わせずに忘れたパスワードを復元する機能をユーザに提供できます。[Forgot your password?] リンクは、ユーザが iManager のセルフサービスコンソールにログインするときに利用できます。

パスワードを忘れた場合のセルフサービス機能は次の機能を含みます。

- ◆ ユーザが質問に回答し、ID を提供できるチャレンジセット
- ◆ ユーザにパスワードヒントまたは忘れたパスワードを電子メールで知らせる機能
- ◆ ユーザが忘れたパスワードを要求中にブラウザでパスワードをリセットできる機能

ユーザが [Forgot your password?] リンクを使用して実行できる操作の例を確認するには、118 ページの「エンドユーザへのパスワードを忘れた場合のセルフサービスの提供」を参照してください。

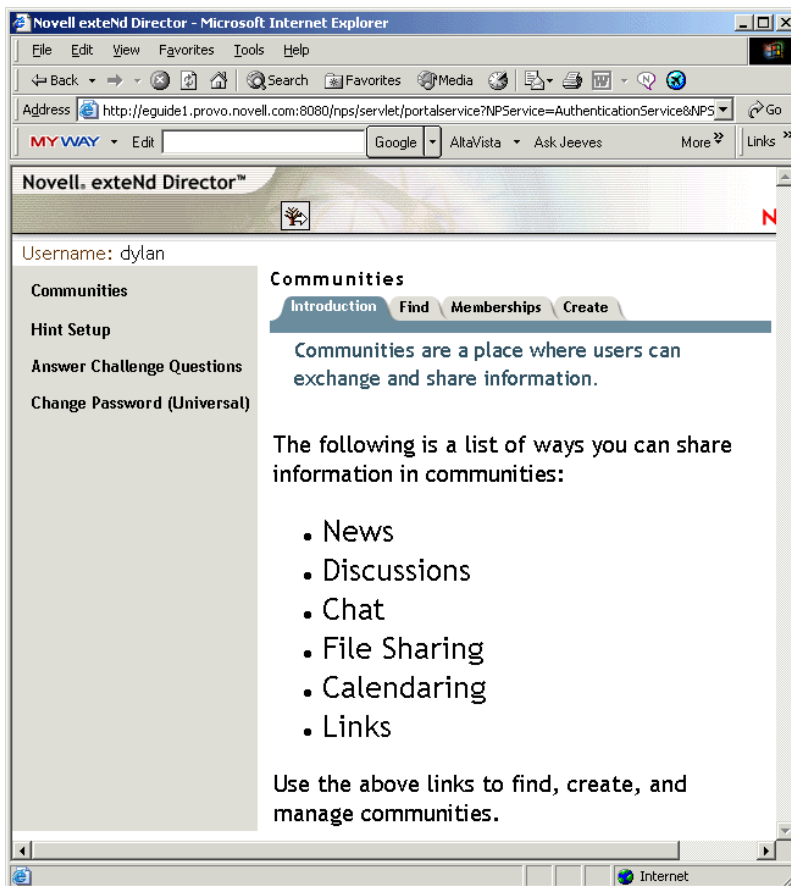
次の図は、Password Policy（パスワードポリシー）の忘れたパスワードの設定を指定するプロパティページの例を示します。



ユーザへのパスワードのリセットセルフサービスの提供

iManager セルフサービスコンソールを使用すると、ユーザは Advanced Password Rule（詳細パスワードルール）を参照しながらパスワードをリセットできます。これは、Change Password (Universal) ガジェットを使用して実行します。

iManager Web サーバ上の iManager セルフサービスコンソールに URL (<https://www.servername.com/nps> など) を使用してログインしたときにユーザに表示される画面の例は、次のとおりです。



ユーザが ChangePassword（ユニバーサル）リンクを使用して実行できる操作の例を確認するには、118 ページの「エンドユーザへのパスワードを忘れた場合のセルフサービスの提供」を参照してください。

セルフサービスの使用に関する前提条件

7 章 95 ページの、「Password Policy (パスワードポリシー) を使用したパスワードの管理」の情報を確認し、107 ページの「Password Policy (パスワードポリシー) の使用に関する前提条件」の前提条件を満たします。

Password Policy (パスワードポリシー) のすべての機能を使用できるように、環境を準備してユニバーサルパスワードをオンにすることをお勧めします。ただし、このための準備が整っていなくても、一部の機能は、ユニバーサルパスワードを展開せずに使用できます。

リストについては、289 ページの「eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート」を参照してください。このリストでは、ユニバーサルパスワードが無効な場合に Novell® eDirectory™ 8.6.2 または eDirectory 8.7.3 で使用できる機能について説明しています。

パスワードセルフサービスのログイン方法の計画

iManager サーバ上のユーザは、https://www.my_iManager_server.com/nps などの URL を使用して、iManager セルフサービスコンソールにアクセスできます。

103 ページの「ユーザのログインおよびパスワード変更方法の計画」の説明に従って、ユニバーサルパスワードをサポートするようにクライアント環境をアップグレードします。

詳細については、『*Novell Modular Authentication Services (NMAS) 2.3 管理ガイド* (<http://www.novell.com/documentation/nmas23/index.html>)』の「Deploying Universal Password (ユニバーサルパスワードの展開)」を参照してください。

エンドユーザへのパスワードを忘れた場合のセルフサービスの提供

New Password Policy Wizard を使用して Password Policy (パスワードポリシー) を作成すると、エンドユーザに提供する、パスワードを忘れた場合の機能を決定するよう求めるメッセージが表示されます。

この節では、オプションの詳細について説明し、[Forgot your password?] リンクを使用してエンドユーザが実行できる操作の例を示します。

この節では、次の項目について説明します。

- ◆ 119 ページの「チャレンジセット」
- ◆ 120 ページの「 [Forgotten Password] のアクション」
- ◆ 121 ページの「パスワードヒント」
- ◆ 122 ページの「エンドユーザへの [Forgotten Password] の設定の要求」
- ◆ 123 ページの「パスワードを忘れた場合のセルフサービスのエンドユーザ設定」
- ◆ 132 ページの「エンドユーザがパスワードを忘れた場合に表示される機能」
- ◆ 135 ページの「 [Forgot Your Password?] リンクのオフ」
- ◆ 137 ページの「Hint ガジェットの削除によるパスワードヒントの無効化」

チャレンジセット

チャレンジセットはユーザが回答できる一連の質問で、ユーザはパスワードを使用する代わりに自らの識別情報を提供します。チャレンジセットは、Password Policy（パスワードポリシー）に割り当てられ、Password Policy（パスワードポリシー）の認証方法の一部として使用されます。チャレンジセットは、パスワードを忘れた場合のセルフサービスをユーザに提供する際に、その一部として使用できます。ユーザに対し、忘れたパスワードに関するヘルプを受け取るためにチャレンジセットの質問に答えるよう要求することで、さらにセキュリティが高まります。チャレンジセットを使用するには、[Manage Password Policies] タスクを使用して Password Policy（パスワードポリシー）を作成し、パスワードを忘れた場合の機能を設定します。

Password Policy（パスワードポリシー）の作成時に、ユーザがヘルプデスクに問い合わせることなくヘルプを利用できるように、パスワードを忘れた場合のセルフサービスを有効にできます。セルフサービスのセキュリティを高めるために、チャレンジセットを作成して、忘れたパスワードに関するヘルプを利用するにはユーザがチャレンジセットの質問に答えなければならないように指定できます。また、ユーザにパスワードヒントを表示するなど、ユーザが質問に回答した後でユーザを支援するために実行するアクションも指定します。ユーザは、Novell iManager セルフサービスコンソールを介してこれらのセルフサービス機能を利用できます。選択できるアクションは、[120 ページの「\[Forgotten Password\] のアクション」](#)で説明しています。

チャレンジセットの質問の構造は、次の選択肢を使用して定義します。

[Admin-Defined] - 管理者は、各ユーザに提示する質問を作成できます。ただし、各ユーザの回答は固有です。

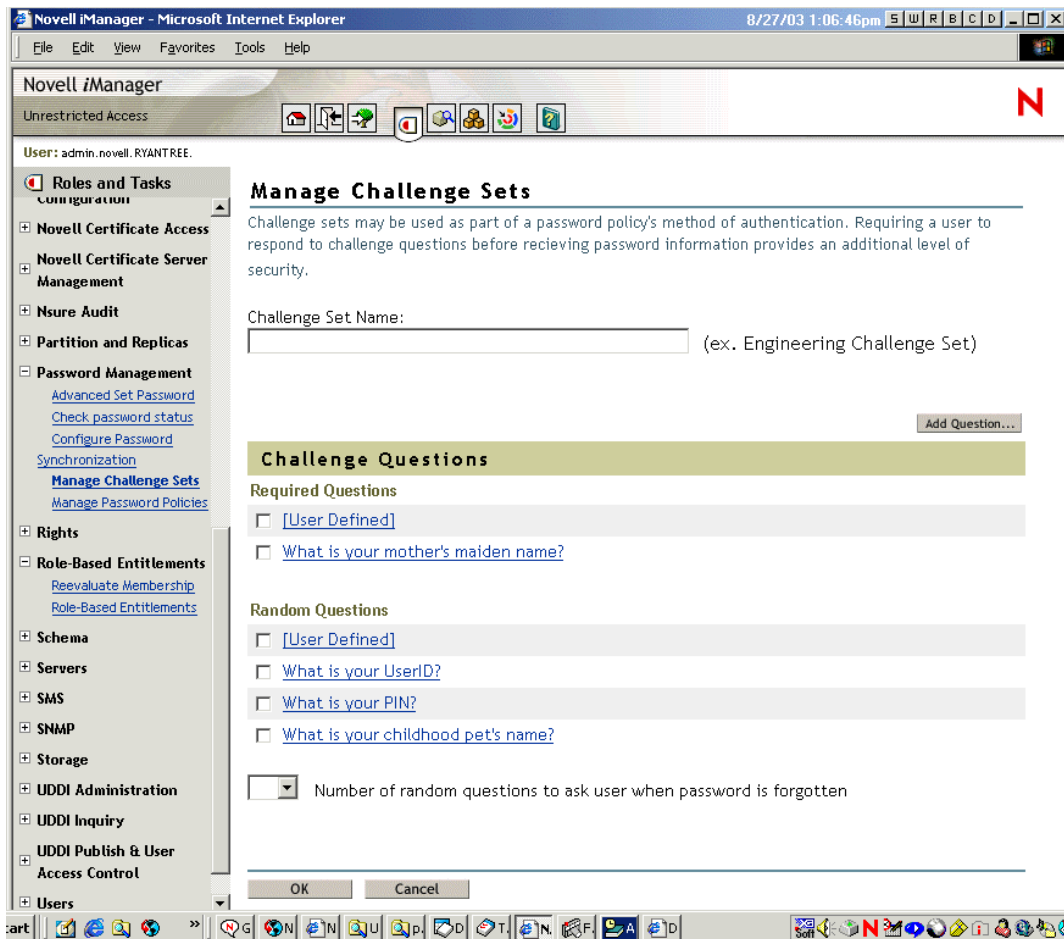
[User-Defined] - 管理者は、ユーザが1つまたは複数の質問を作成するように指定できます。この場合、各ユーザの質問と回答の両方が固有です。

[Required] - このリスト内の質問は、ユーザがパスワードを忘れた場合のセルフサービス機能を使用するときは、必ずユーザに提示されます。

[Random] - このリスト内の質問は、チャレンジセットの質問に最初に答えることによって、ユーザがパスワードを忘れた場合の機能を設定するときに、完全なセットとして一度だけユーザに提示されます。ユーザがパスワードを忘れた場合の機能にアクセスする必要がある場合は、いくつかの質問だけがユーザに示されます。ランダムに表示される質問の数は、管理者によって決定されます。

ユーザの回答とユーザ定義の質問は、NMAS (Novell Modular Authentication Services) によって Novell eDirectory に保存されます。

新しいチャレンジセットを作成する画面例は、次のとおりです。デフォルトで提供されるサンプルの質問から選択することも、独自の質問を追加することもできます。



[Forgotten Password] のアクション

[Enable Forgotten Password] が有効な場合、[Password Policy] には、次のような [Forgotten Password] のアクションが示されます。

- ◆ **[Allow user to reset password on page]** - ユーザは、チャレンジセットの質問に回答して識別情報を提供すると、新しいパスワードに変更できます。ユーザはチャレンジ質問に回答することですでに認証されているため、旧パスワードを入力しなくてもパスワードを変更できます。このオプションを使用するには、管理者がチャレンジセットを要求するよう設定しており、ユーザは、チャレンジセットの質問に答えることによって、iManager セルフサービスコンソールでパスワードを忘れた場合の機能を設定済みでなければなりません。
- ◆ **[E-mail current password to user]** - ユーザは、チャレンジセットの質問に回答して識別情報を提供すると、現在のパスワードを電子メールで受け取ることができます。このオプションを使用するには、管理者は、ポリシーのユニバーサルパスワードと [Allow user to retrieve password] を有効にする必要があります（これらはいずれも [Universal Password] > [Configuration Options] にあります）。また、220 ページの「電子メール通知の設定」の説明に従って電子メール通知を設定する必要があります。さらに、ユーザは、チャレンジセットの質問に回答することによって、iManager セルフサービスコンソールでパスワードを忘れた場合の機能を設定済みである必要があります。

- ◆ **[E-mail hint to user]** - ユーザはパスワードヒントを電子メールで受け取ります。このオプションを使用するには、管理者が [220 ページの「電子メール通知の設定」](#) の説明に従って電子メール通知を設定する必要があります。また、ユーザは、パスワードヒントを指定して、iManager セルフサービスコンソールでパスワードを忘れた場合の機能を設定している必要があります。
- ◆ **[Show hint on page]** - iManager セルフサービスコンソールで、ユーザに対してパスワードヒントを表示します。このオプションを使用するには、ユーザは、パスワードヒントを指定することによって、iManager セルフサービスコンソールでパスワードを忘れた場合の機能を設定済みである必要があります。

パスワードヒント

パスワードヒントが必要な [Forgotten Password] のアクションを指定すると、ユーザはパスワードを思い出すヒントを入力できます。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。

パスワードヒント属性 (nsimHint) は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。パスワードヒントは、ヘルプデスクへの問い合わせ削減に大きな効果があります。

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せん。

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チャレンジ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。[\[Password Policy\] の \[Password Change Message\]](#) は、これを実行する1つの方法です。[139 ページの「Password Policy \(パスワードポリシー\) への独自の Password Change Message \(パスワード変更メッセージ\) の追加」](#)を参照してください。

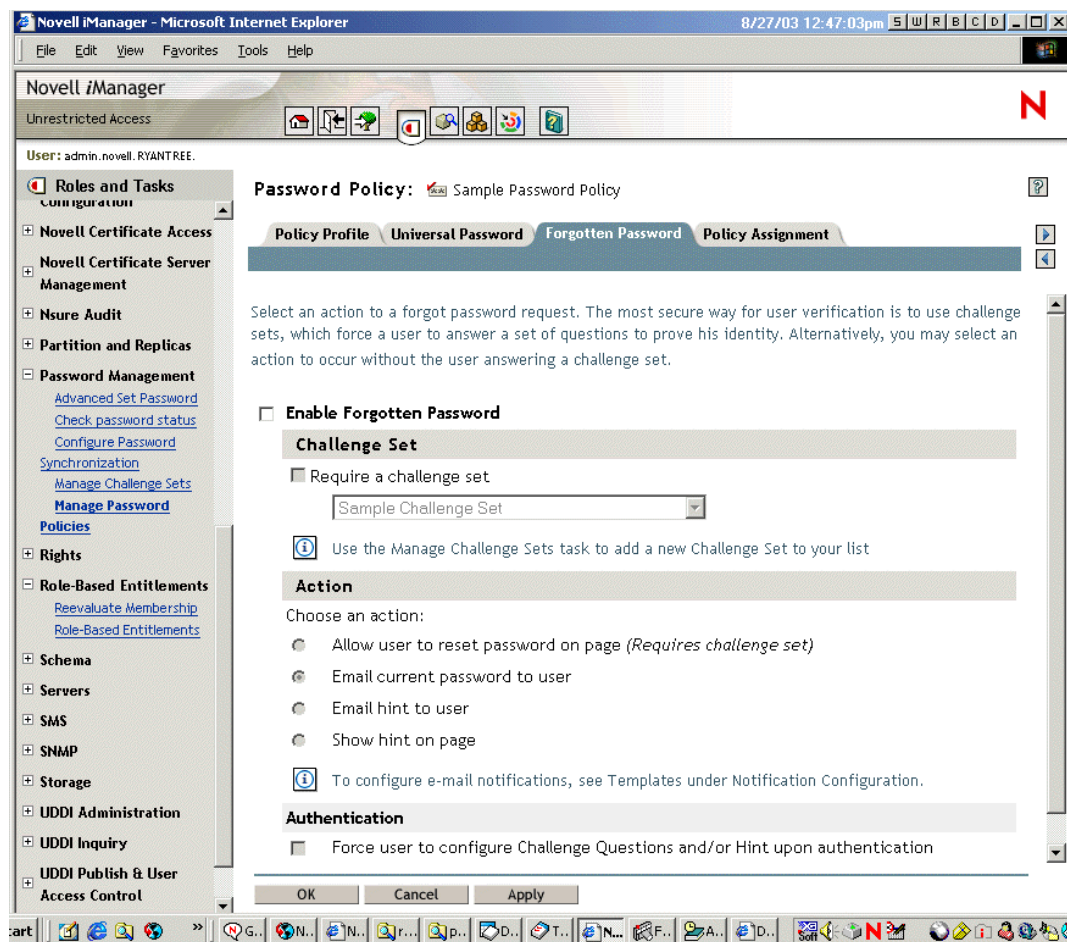
パスワードヒントをまったく使用しないよう選択した場合は、どの Password Policy (パスワードポリシー) でもパスワードヒントを使用していないことを確認します。パスワードヒントが設定されないようにするには、さらに高度な設定として、Hint Setup ガジェットを完全に削除します。[137 ページの「Hint ガジェットの削除によるパスワードヒントの無効化」](#)を参照してください。

エンドユーザへの [Forgotten Password] の設定の要求

一部の [Forgotten Password] のアクションでは、エンドユーザがパスワードを忘れた場合のセルフサービスを使用する前に、いくつかの設定を実行する必要があります。たとえば、[Password Policy] で、チャレンジセットを使用してユーザが識別情報を提供できるように指定している場合や、[Forgotten Password] のアクションが、ユーザに電子メールでパスワードヒントを知らせる設定の場合、ユーザは、パスワードを忘れた場合のセルフサービスを使用するには、まずチャレンジセットの質問に答え、パスワードヒントを作成する必要があります。

これらの機能の設定は、iManager セルフサービスコンソールで開始できます。または、認証後サービス（ユーザが iManager セルフサービスコンソールにログインするときに表示されるページ）を使用して、ユーザに設定を要求できます。

これらの機能をログイン時に設定するように要求するメッセージをユーザに表示するには、[Forgotten Password] ページの最下部にある Password Policy インタフェースのオプション（[Force users to configure Challenge Questions and/or Hint upon authentication]）を選択します。これはポリシーの作成時にデフォルトで選択されています。



ユーザが好きなきに [Forgotten Password] を設定できるようにするには、https://www.my_iManager_server.com/nps などの iManager セルフサービスコンソールの URL をユーザに伝える必要があります。

パスワードを忘れた場合のセルフサービスのエンドユーザ設定

iManager セルフサービスコンソール (<https://www.servername.com/nps>) へのログイン時に [Forgot your password?] をクリックしても、ユーザが次の条件を満たしていない限り、アクションは実行されません。

- ◆ 管理者がパスワードを忘れた場合の機能が有効な Password Policy (パスワードポリシー) を設定している。
- ◆ [Forgotton Password] の設定でチャレンジ質問またはパスワードヒントのいずれかが指定されている場合、ユーザがこれらのいずれかを設定済みである。

ユーザが設定可能な部分は、次の 2 つの方法で設定できます。

- ◆ [123 ページの「忘れたパスワード、認証後のユーザ設定」](#)
- ◆ [126 ページの「iManager セルフサービスコンソールでのパスワードを忘れた場合の機能のユーザ設定」](#)

忘れたパスワード、認証後のユーザ設定

管理者は、ユーザが [Enable Forgotton Password] オプションをオンにすることによって正常にログインした後で、パスワードを忘れた場合の機能を設定し、ユーザがチャレンジ質問またはヒント、あるいはその両方を認証時に設定するように要求できます。このオプションをオンにしている、ユーザが質問またはヒントを設定していない場合、ユーザが iManager セルフサービスコンソール (<https://www.servername.com/nps>) を介して次にログインすると、Forgotton Password 設定ガジェットが表示されます。これを認証後設定と呼びます。

次の画面はチャレンジセット設定 - 認証後を示しています。

Answer Challenge Questions

Notice: Password policy requires that you set up your Challenge Questions before authentication.

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: What is your mother's maiden name?
Challenge Response:

Challenge Question: What is your childhood pet's name?
Challenge Response:

User-Defined Questions

Challenge Question: ?
Challenge Response:

Challenge Question: ?
Challenge Response:

次の画面はパスワードヒント設定 - 認証後を示しています。

HintSetup - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Copy Paste Links »

Define Password Hint

Notice: Password policy requires that you set up your Password Hint before authentication.

Please enter a password hint to help you remember your password.

Create a Password Hint

Username: dylan

Password Hint:

Done Local intranet

iManager セルフサービスコンソールでのパスワードを忘れた場合の機能のユーザ設定

ユーザがポータルを介してログインすると、iManager セルフサービスコンソールが表示されます。このコンソールから、パスワードを忘れた場合のセルフサービスのチャレンジセットとパスワードヒントを設定または変更するためのガジェットにアクセスできます。これは、ユーザがパスワードの変更を開始できる場所と同じ場所です。ここでユーザがアクセスできるガジェットの名前は次のとおりです。

- ◆ Hint Setup
- ◆ Answer Challenge Questions
- ◆ Change Password (Universal)

ユーザはこれらの変更をいつでも開始できます。ヒントまたはチャレンジセットがユーザの Password Policy（パスワードポリシー）で必要ない場合、ユーザはこれらを設定できません。ページにはそのオプションにアクセスできないこと示すメッセージが表示されます。

次の図は、[Hint Setup] ページを示します。



次の図は、[Answer Challenge Questions] ページを示します。

Novell exteNd Director - Microsoft Internet Explorer 9/25/03 6:44:49pm

File Edit View Favorites Tools Help

Novell. exteNd Director™ Novell.

Username: dylan

Communities

Hint Setup

Answer Challenge Questions

Change Password (Universal)

Answer Challenge Questions

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: What is your mother's maiden name?
Challenge Response:

Challenge Question: What is your childhood pet's name?
Challenge Response:

User-Defined Questions

Challenge Question: ?
Challenge Response:

Challenge Question: ?
Challenge Response:

Done Internet

この例にリストされている最初の質問は、管理者が定義し、その他の質問はユーザが定義します。ユーザは管理者の質問に答え、次の例に示すとおり、ユーザ定義質問の質問と回答の両方を作成します。

The screenshot shows a web browser window titled "Novell exteNd Director - Microsoft Internet Explorer" with the address bar displaying "9/25/03 6:46:56pm". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The page header features the "Novell. exteNd Director™" logo and the "Novell." logo. Below the header, the user's "Username: dylan" is displayed. A left-hand navigation menu contains the following items: "Communities", "Hint Setup", "Answer Challenge Questions" (which is highlighted), and "Change Password (Universal)". The main content area is titled "Answer Challenge Questions" and includes an introductory paragraph: "These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response." The page is divided into two sections: "Admin-Defined Questions" and "User-Defined Questions".

Admin-Defined Questions

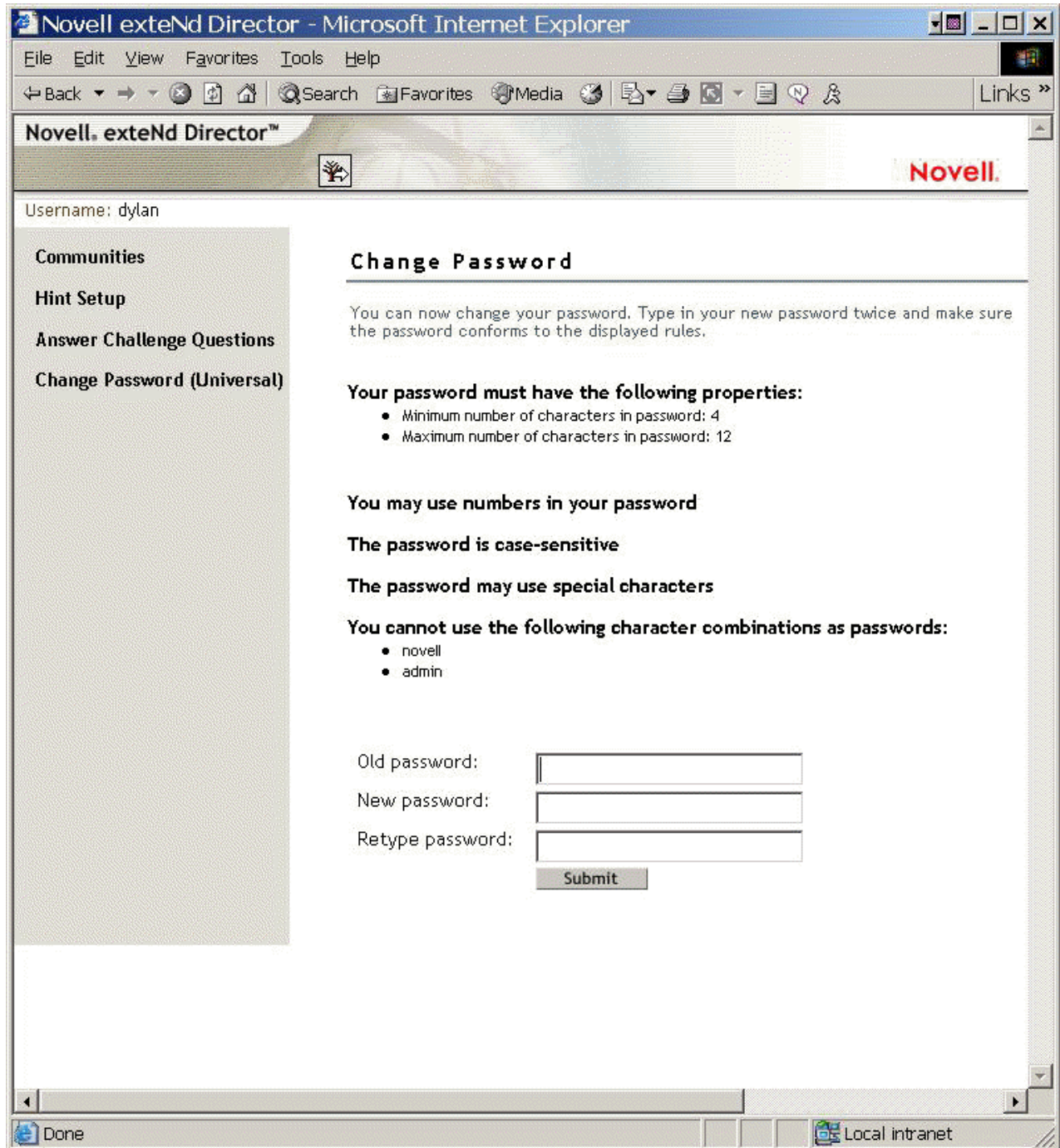
Challenge Question:	What is your mother's maiden name?
Challenge Response:	<input type="text" value="Ranadive"/>
Challenge Question:	What is your childhood pet's name?
Challenge Response:	<input type="text" value="Cocoa"/>

User-Defined Questions

Challenge Question:	<input type="text" value="What street did you grow up on?"/>
Challenge Response:	<input type="text" value="Van Dorn Street"/>
Challenge Question:	<input type="text" value="What is your favorite food?"/>
Challenge Response:	<input type="text" value="rice"/>

At the bottom of the form is a "Submit" button. The browser's status bar at the bottom shows "Internet".

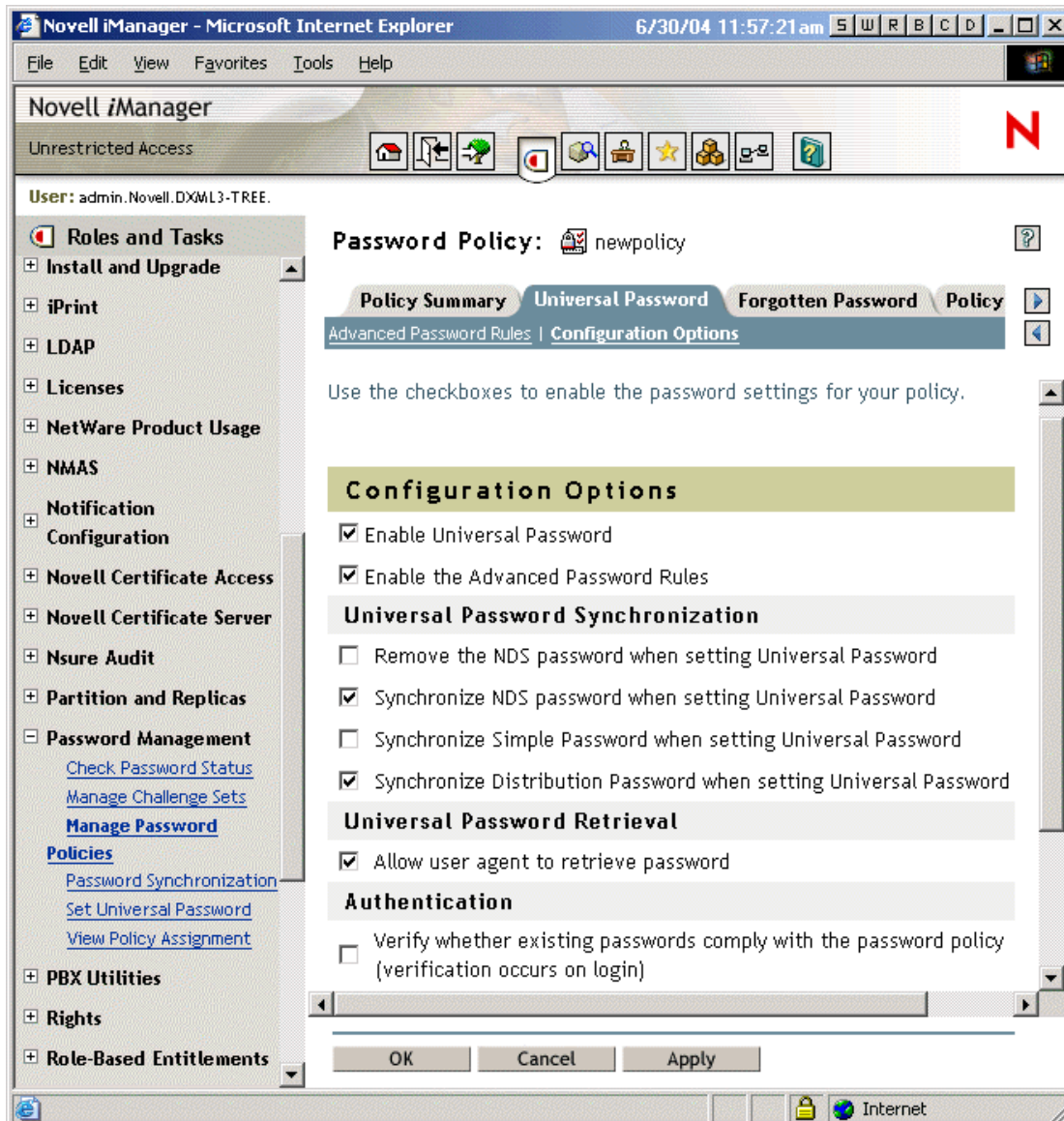
次の図は、[Change Password (Universal)] ページを示します。



既存のパスワードの準拠の要求

管理者が Password Policy（パスワードポリシー）を作成または変更する場合、管理者はユーザに対し、ポータルを介して次回ログインする際に、準拠しない既存のパスワードを変更するように要求できます。

これは、[Configuration Options] にある [Universal Password] タブで [Password Policy] のオプションを設定することによって実行されます。このオプションは、[Verify whether existing passwords comply with the password policy (verification occurs on login)] という名前です。デフォルトでは、このオプションは、新しい Password Policy（パスワードポリシー）の作成時にはオフになっています。次の図は、このオプションを設定するページを示します。



このオプションが設定されている場合、ユーザがポータルを介して次にログインすると、ユーザのパスワードが Password Policy（パスワードポリシー）に準拠しているかどうか確認されます。準拠していない場合、次のようなページが表示され、ユーザはパスワードを変更しないとログインできません。

Change Password

Notice: Password policy requires password to conform to displayed rules.

You can now change your password. Type in your new password twice and make sure the password conforms to the displayed rules.

Your password must have the following properties:

- Minimum number of characters in password: 4
- Maximum number of characters in password: 12

You may use numbers in your password

The password is case-sensitive

The password may use special characters

You cannot use the following character combinations as passwords:

- novell
- admin

Old password:

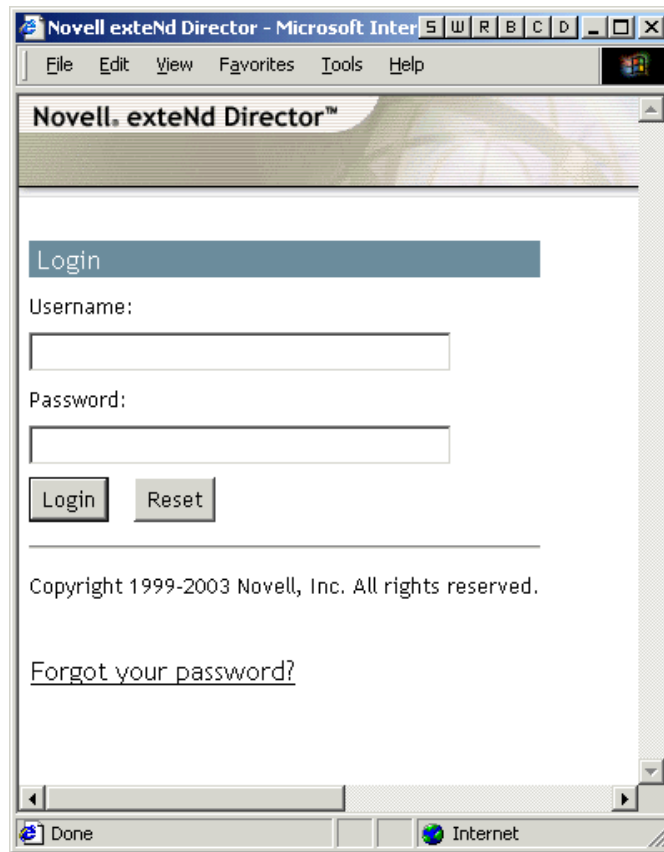
New password:

Retype password:

エンドユーザがパスワードを忘れた場合に表示される機能

この節では、パスワードを忘れた場合のセルフサービスを使用してユーザが実行できる操作を説明します。

Identity Manager に付属の iManager プラグインをインストールすると、次の図に示す iManager セルフサービスコンソール (<https://www.servername.com/nps> など) に [Forgotten Password] リンクが表示されます。

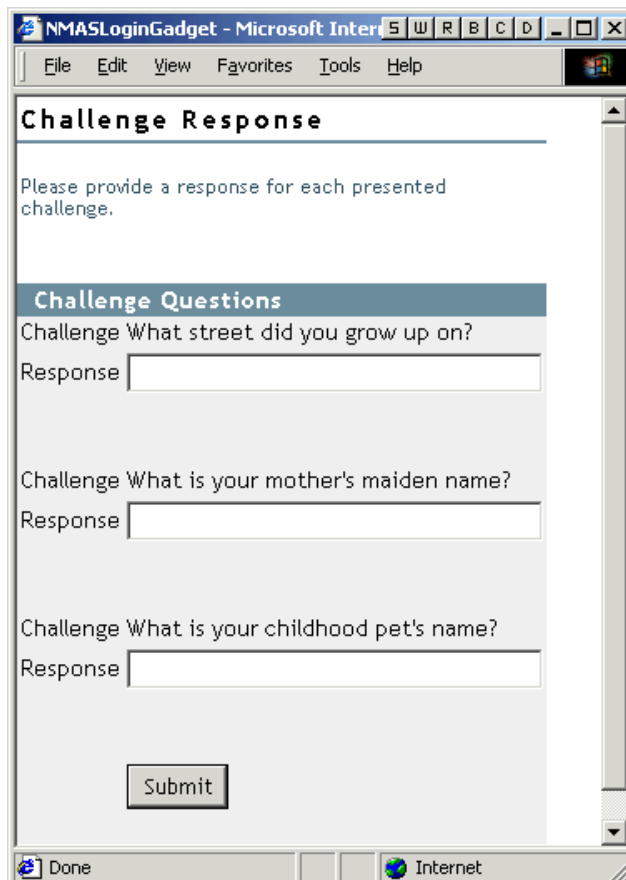


ユーザがこのリンクをクリックすると、次のページが表示され、ユーザ名の入力を求めるプロンプトが表示されます。



ユーザ名が入力されると、[Forgotten Password] 設定によってユーザに表示する内容が決定されます。

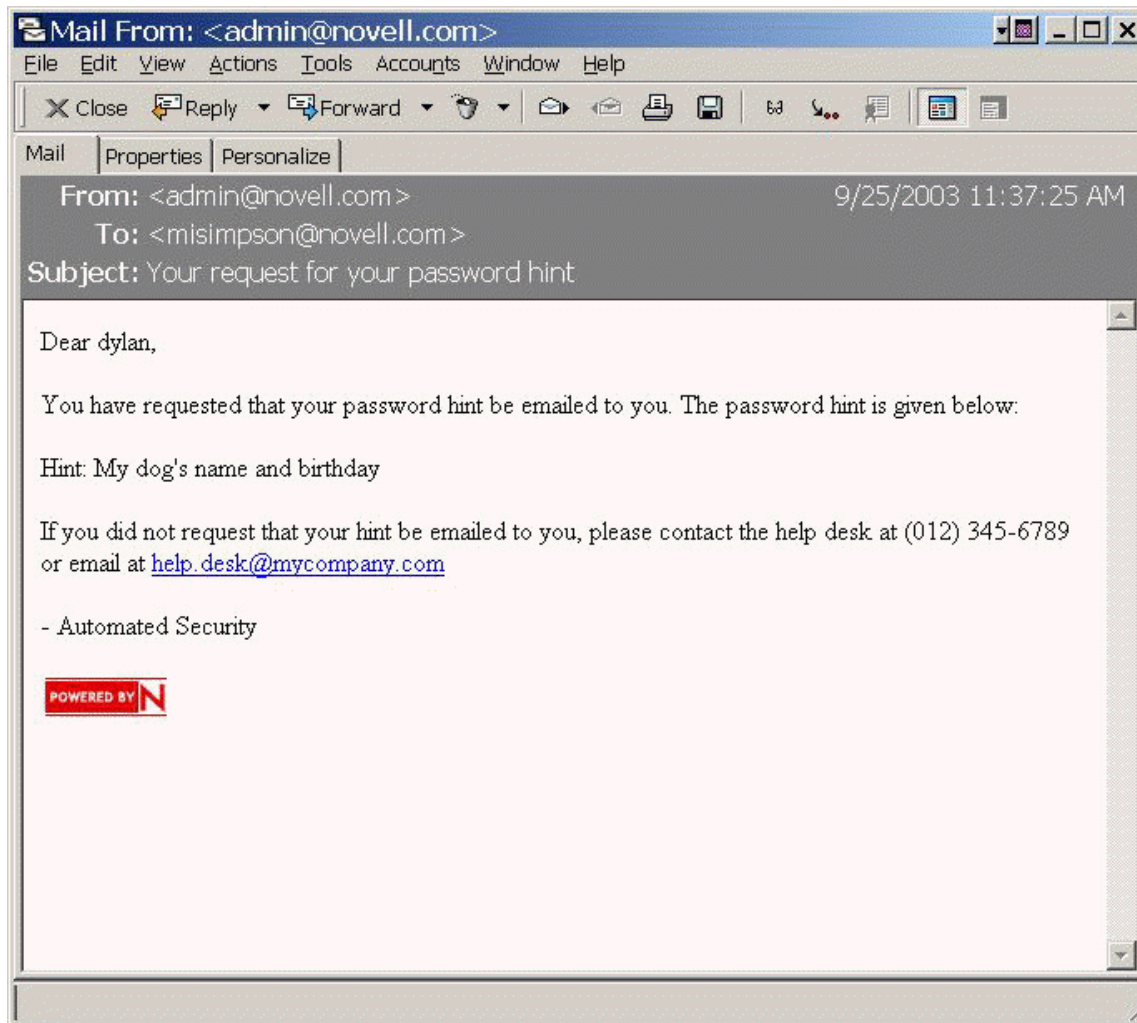
たとえば、管理者が [Password Policy] で、チャレンジセットを使用するように指定している場合、次のようなページが表示され、ユーザはチャレンジセットの質問に回答してユーザの識別情報を提供する必要があります。



管理者が、[Forgotten Password] のアクションを [Show hint on page] に指定した場合、次のようなページが表示されます。




管理者が、[Forgotten Password] のアクションを [E-mail current password to user] または [E-mail hint to user] に指定した場合、このページには、パスワードまたはヒントが電子メールで送信されたことを知らせるメッセージが表示されます。ユーザは次のような電子メールを受け取ります。



[Forgot Your Password?] リンクのオフ

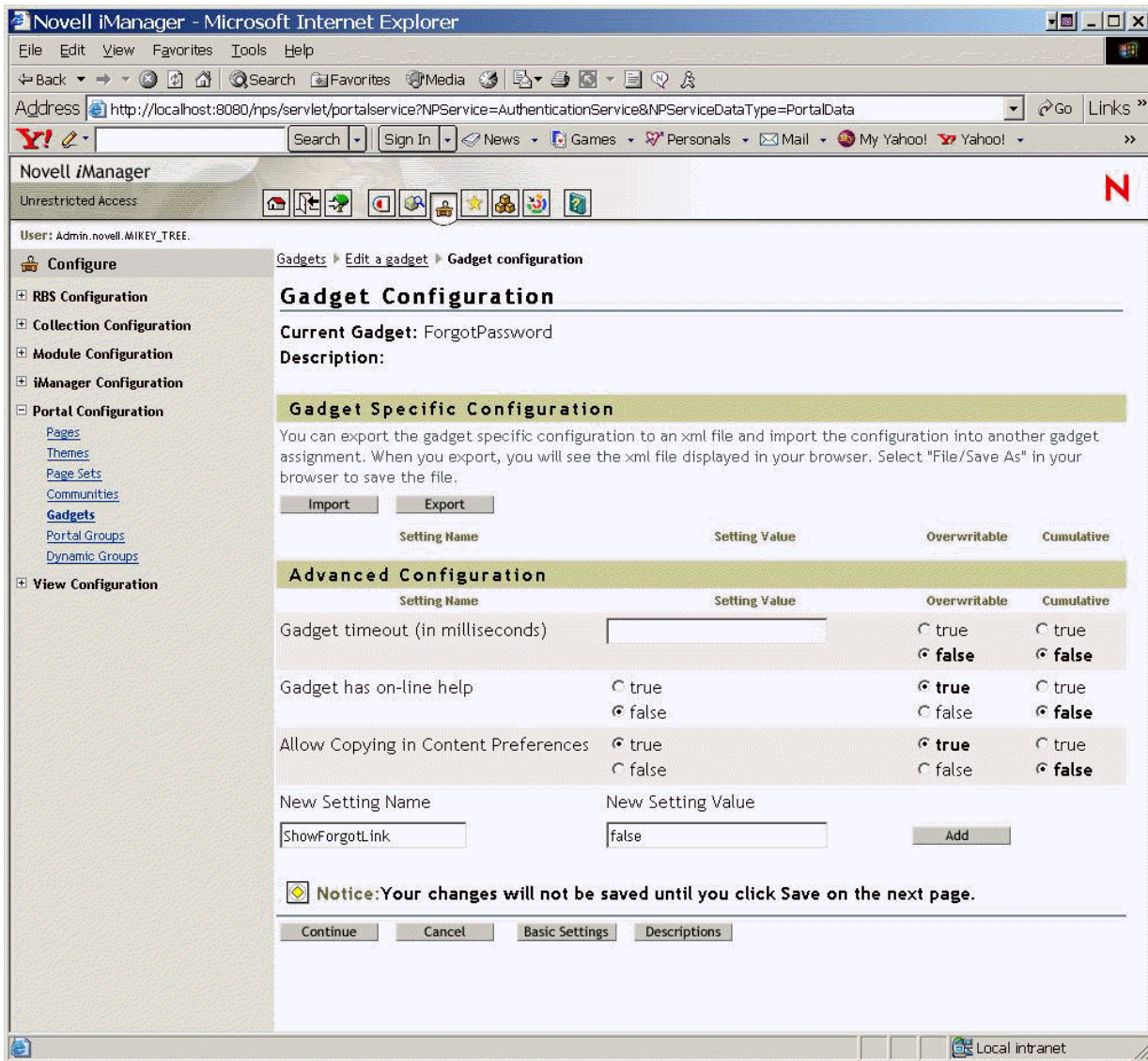
[Forgot your password?] リンクをポータルに表示しない場合は、次の手順に従ってこれをオフにできます。

- 1 iManager から、設定アイコン  をクリックして、Administration ガジェットを起動します。
- 2 [Portal Platform Configuration] > [Gadgets] の順にクリックします。
- 3 ガジェットのリストから [Forgot Password] ガジェットを選択します。
- 4 [Edit] ボタンをクリックし、[Configuration] をクリックします。[All Settings] ボタンをクリックします。

5 次の図に示すように、ガジェット設定でキーペアを追加します。

ShowForgotLink=false

このキーペアがガジェット設定にまったく存在しない場合、デフォルトの動作は「true」です。



6 [Continue] をクリックし、次のページで [Save] をクリックして変更を保存します。

7 Web サーバを再起動して、変更を有効にします。

Hint ガジェットの削除によるパスワードヒントの無効化


パスワードヒントは、パスワードを忘れた場合のセルフサービスの一部として、ユーザがパスワードを思い出せるようにする 1 つの方法です。[Password Policy] では、パスワードヒントを使用する、[Forgotten Password] のアクションは、[E-mail hint to user] または [Show hint on page] という名前です。

パスワードを忘れたユーザにとってパスワードヒントが有益となるためには、認証されていないユーザがパスワードヒント属性 (nsimHint) へのパブリックアクセスを持つ必要があります。ヒントの作成時にユーザが実際のパスワードをパスワードヒントに含めていないかがチェックされますが、このパブリックアクセスはセキュリティを脅かす問題になると思われるかもしれません。

パスワードヒントを使用しない場合は、[Password Policy] で、[Forgotten Password] アクションに別のオプションを選択します。

また、必要に応じて Hint Setup ガジェットを完全に削除できます。

iManager の Identity Manager プラグインをインストールした後、[Configure] 画面を使用して Hint Setup ガジェットを削除します。

- 1 iManager の設定アイコン  をクリックします。
- 2 [Portal Platform Configuration] > [Gadgets] の順にクリックします。
- 3 ガジェットのリストから [Hint Setup] を選択します。
- 4 [Delete] をクリックします。

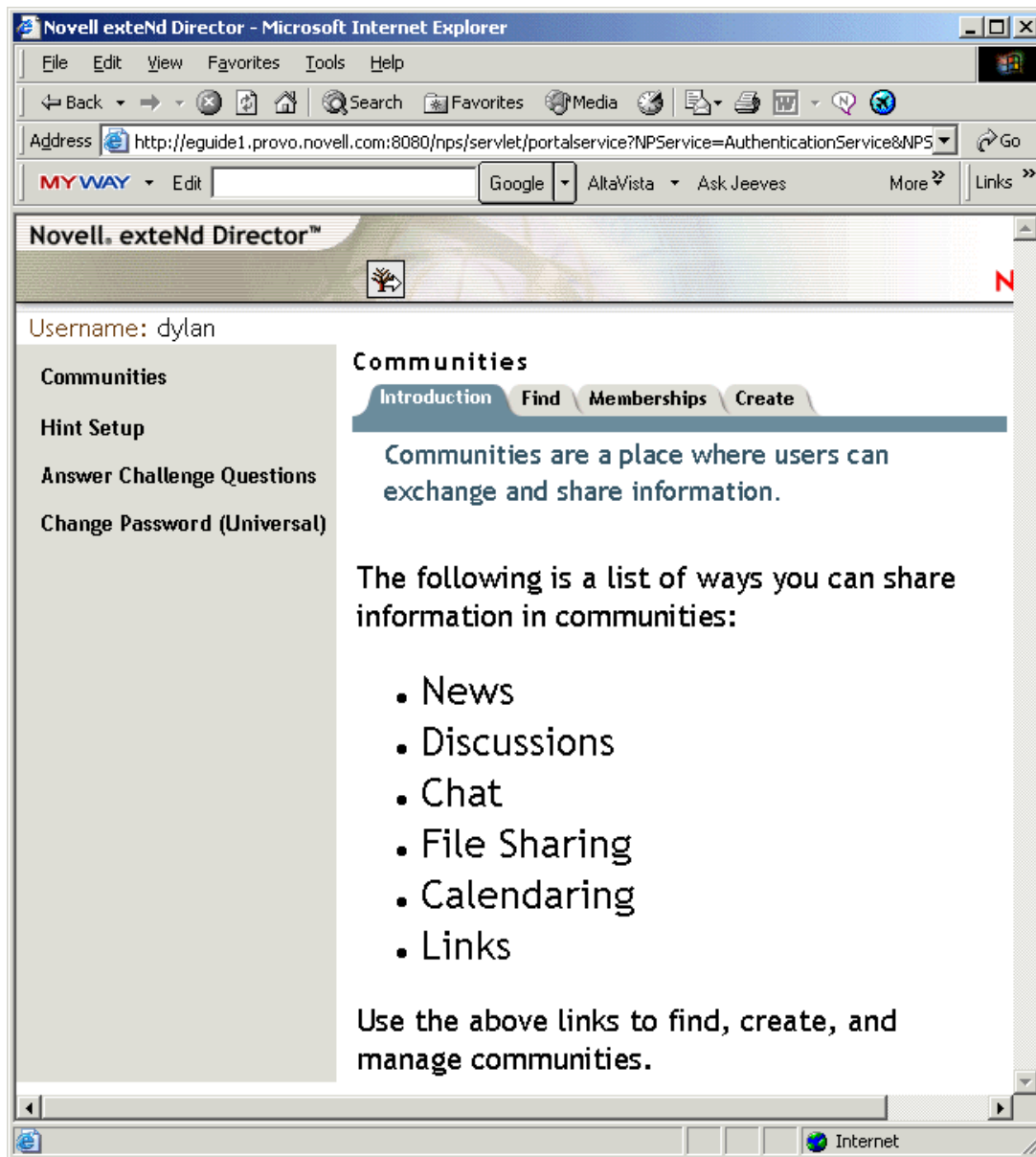
ガジェットを削除すると、ユーザは Hint Setup を利用できなくなります。認証後サービスは、既存のガジェットを委任リストに追加する前にこれらを検索します。認証後サービスに対してポリシーで何が設定されているかに関わらず、ガジェットが存在しなければ、認証後サービスによって、または iManager セルフサービスコンソール内でサービスはユーザに表示されません。

Hint ガジェットを削除した後は、[Password Policy] で、[Forgotten Password] のアクションとして [E-mail Hint] または [Display Hint] を選択していないことを確認します。

ユーザへのパスワードのリセットセルフサービスの提供

ユーザは iManager セルフサービスコンソールで自分のパスワードをリセットできます。コンソールには、<https://www.servername.com/nps> などの URL を使用してアクセスします。たとえば、<https://www.myiManager.com/nps> などです。

次に、ログイン後の iManager セルフサービスコンソールの例を示します。

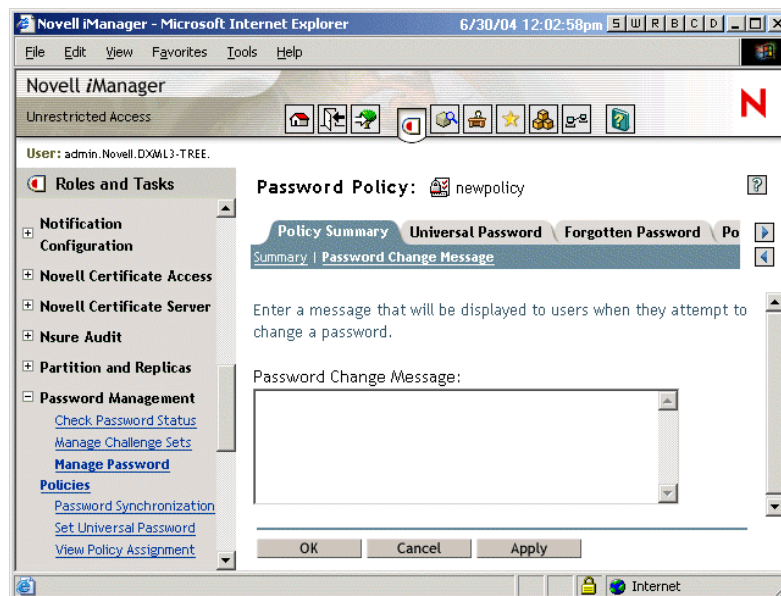


Password Policy（パスワードポリシー）への独自の Password Change Message（パスワード変更メッセージ）の追加

[Password Policy] では、ポリシーで指定したパスワードルールとともにユーザに表示する Password Change Message（パスワード変更メッセージ）を作成できます。ユーザがパスワードの変更を開始するか、またはパスワードの変更を行うように要求されるたびに、メッセージとパスワードルールが表示されます。

このメッセージを作成するには、Password Policy（パスワードポリシー）を次のように編集します。

- 1 iManager で、[Password Management] > [Manage Password Policies] の順に選択します。
- 2 メッセージに追加する Password Policy（パスワードポリシー）をクリックし、[Edit] をクリックします。
- 3 [Policy Summary] タブの [Password Change Message] をクリックします。
次のページが表示されます。



- 4 パスワードルールとともにユーザに表示するメッセージを入力し、[OK] をクリックします。

チャレンジセットの作成または変更

チャレンジセットは、ユーザに対してパスワードを忘れた場合のセルフサービスを設定する場合に役立つ Password Policy（パスワードポリシー）の機能です。チャレンジセットはユーザが回答できる一連の質問で、ユーザはパスワードを使用する代わりに自らの識別情報を提供します。

Password Policy（パスワードポリシー）の作成時に、ユーザがヘルプデスクに問い合わせることなくヘルプを利用できるように、パスワードを忘れた場合のセルフサービスを有効にできます。セルフサービスのセキュリティを高めるために、チャレンジセットを作成して、忘れたパスワードに関するヘルプを利用するにはユーザがチャレンジセットの質問に答えなければならないように指定できます。

チャレンジセットは、Password Policy（パスワードポリシー）の作成時に作成できます。iManager で、[Password Management] > [Manage Password Policies] > [New] の順に選択します。

また、チャレンジセットを別のタスクとして管理することもできます。iManager で、[Password Management] > [Manage Challenge Sets] の順に選択します。

チャレンジセットを使用するには、ユーザは質問と回答を設定する必要があります。[Forgotten Password] タブの [Password Policy] のオプションを使用して、ユーザが iManager または iManager セルフサービスコンソールに次にログインしたときにチャレンジセットを設定するように要求できます。このオプションは、[Force user to configure Challenge Questions and/or Hint upon authentication] という名前です。ユーザはこの設定を開始することも、iManager セルフサービスコンソールで変更することもできます。

チャレンジセットの質問の構造を定義します。ユーザの回答とユーザ定義の質問は、NMAS (Novell Modular Authentication Services) によって Novell eDirectory に保存されます。

パスワードセルフサービスの通知の設定

220 ページの「[電子メール通知の設定](#)」の指示に従ってください。

パスワードセルフサービスのテスト

機能が正しく設定されていることを確認するには、次のタスクをパスワードセルフサービスのテストの一部として完了します。

- 1 次の特性を持つポリシーを作成します。
 - ◆ パスワードを忘れた場合の機能を有効にする
 - ◆ チャレンジセットを要求する
 - ◆ チャレンジ / レスポンスとヒントがログイン時に設定されることを確認するオプションを選択する
 - ◆ テストに使用できる少なくとも 1 人のユーザ (Internet EMail Address 属性のユーザオブジェクトで指定された電子メールアドレスを持つユーザ) が含まれるコンテナに、Password Policy（パスワードポリシー）を割り当てる
- 2 Password Policy（パスワードポリシー）が割り当てられていない別のテスト対象ユーザが存在することを確認します。

- 3 Password Policy (パスワードポリシー) が割り当てられているユーザとして Virtual Office にログインし、チャレンジ質問への回答およびヒントの設定という認証後手順を受けることを確認します。
- 4 iManager セルフサービスコンソールのログインページに戻り、[Forgot your password?] をクリックします。同じユーザのユーザ ID で、チャレンジ質問が正しく表示されていること、これらの質問に正しく回答することによって正しいアクション (ヒントの表示や、ユーザへのパスワードリセットの許可など) が実行されることを確認します。
- 5 iManager セルフサービスコンソールのログインページに戻り、[Forgot your password?] をクリックします。Password Policy (パスワードポリシー) が割り当てられていないユーザのユーザ ID を入力します。適切なエラーが表示され、パスワードを忘れた場合の機能を利用できないことが通知されることを確認します。

企業ポータルへのパスワードセルフサービスの追加

「パスワードセルフサービス」の手順のほとんどは、iManager 2.0.2 サーバを使用することを想定しています。

iManager 以外の製品を含め、ポータル製品でパスワードセルフサービス機能を使用する方法については、次の表を参照してください。

製品	パスワードセルフサービスのサポート	使用する設定方法
iManager 2.0.2	機能を統合できます。 パスワード管理プラグインをインストールしている場合、この製品はパスワードセルフサービス機能をサポートします。これらのプラグインは、DirXML 2 プラグインに含まれ、download.novell.com から個別にダウンロードすることもできます。	次の手順に従います。 <ul style="list-style-type: none"> ◆ 107 ページの「Password Policy (パスワードポリシー) の使用に関する前提条件」。これらの手順については、7 章 95 ページの、「Password Policy (パスワードポリシー) を使用したパスワードの管理」を参照してください。 ◆ その他の手順については、パスワードセルフサービスを参照してください。141 ページの「企業ポータルへのパスワードセルフサービスの追加」に記載されている情報は、iManager 2.0.2 には不要です。
exteNd™ Director™ Standard Edition 4.1 Support Pack 1	機能を統合できます。 このバージョンの exteNd Director は、必要な Novell ポータルモジュール (.npm ファイル) をインストールしている場合、パスワードセルフサービス機能をサポートします。 機能をサポートするには、Support Pack 1 以降を適用する必要があります。	142 ページの「パスワードセルフサービスの exteNd Director 4.1 との統合」
iManager サーバ上で実行されている、NetWare 6.5 Support Pack 2 に付属の Virtual Office	機能を統合できます。 プラグインをインストールし、いくつかの追加手順を完了することによって、Virtual Office と iManager に使用するものと同じ NetWare サーバ上でパスワードセルフサービス機能を使用することができます。	144 ページの「パスワードセルフサービスと Virtual Office との統合」

製品	パスワードセルフサービスのサポート	使用する設定方法
exteNd Director 5	<p>機能にリンクする必要があります。</p> <p>exteNd Director 5はポートレットに基づき、パスワードセルフサービスはNPM (Novell Portal Module) に基づくため、別の製品ではパスワードセルフサービス機能を直接使用することはできません。</p> <p>この製品でパスワードセルフサービス機能を使用するには、企業ポータルから iManager サーバのエンドユーザパスワード機能へのリンクを作成します。</p>	145 ページの「企業ポータルからパスワードセルフサービスへのリンク」
Novell Portal Services (NPS) 4.1 以前のバージョン	<p>機能にリンクする必要があります。</p> <p>これらのレガシーNPS 製品では、Novell Portal Module (NPM) が実行されますが、ForgottenPassword.npm のパスワードセルフサービス機能に必要な一部の強化機能がありません。</p> <p>この製品でパスワードセルフサービス機能を使用するには、企業ポータルから iManager サーバのエンドユーザパスワード機能へのリンクを作成します。</p>	145 ページの「企業ポータルからパスワードセルフサービスへのリンク」
サードパーティの製品	<p>機能にリンクする必要があります。</p> <p>サードパーティの製品では Novell Portal Module (NPM) が実行されないため、別の製品でパスワードセルフサービス機能を直接使用することはできません。</p> <p>サードパーティ製品でパスワードセルフサービス機能を使用するには、企業ポータルから iManager サーバのエンドユーザパスワード機能へのリンクを作成します。</p>	145 ページの「企業ポータルからパスワードセルフサービスへのリンク」

パスワードセルフサービスの exteNd Director 4.1 との統合

企業ポータルに exteNd Director Standard Edition 4.1 Support Pack 1 を使用している場合は、その他の NPM (Novell Portal Module) と同様に、Forgotten Password モジュールをポータルに追加できます。このモジュールによって、iManager 2.0.2 上で使用した場合と同じように次の機能を利用することができます。

- ◆ パスワードセルフサービスの新しいポータルユーザタスク
 - ◆ Hint Setup
 - ◆ Answer Challenge Questions
 - ◆ Change Password (Universal)
- ◆ ポータルログインページ上の [Forgot your password?] リンクからアクセスする、パスワードを忘れた場合のセルフサービス
- ◆ 準拠しないパスワードを変更したり、ヒントやチャレンジ質問など、パスワードを忘れた場合の機能の項目を更新したりするようユーザに要求するメッセージを表示する認証後機能

これらの機能を追加する

- 1 Support Pack 1 をインストール済みであることを確認します。

これは ForgottenPassword.npm に必要な強化機能を含みます。

- 2 exteNd Director Web サーバと eDirectory が同じマシン上で実行されている場合でも、これらの間に SSL が設定されていることを確認します。

これは NMAS 2.3 以降の要件です。

- 3 Forgotten Password ガジェットのセキュリティを確保するため、LDAP SSL ポート番号を確認します。

636 以外の LDAP SSL ポートを使用している場合、次の設定手順を完了する必要があります。

PortalServlet.properties ファイルに次のキーペアを追加します。

```
LDAPSSLPort=your_port_number
```

たとえば、Web サーバで Active Directory が実行されている場合、Active Directory はポート 636 を使用するため、この変更が必要です。Tomcat を実行している場合は、tomcat¥webapps¥nps¥WEB_INF ディレクトリにある PortalServlet.properties ファイルの設定を変更してください。

該当するファイルに値が記述されている場合、デフォルト値の 636 よりも優先されます。

- 4 設定を変更したら、Web サーバを再起動します。

- 5 ポータルユーザコンテナ内のすべての eDirectory ユーザが、Hint 属性 (nsimHint) に対して自己権利を持っていることを確認します。

DirXML プラグインを iManager Web サーバにインストールする場合、この手順は、iManager が設定されるツリーに対しては自動的に完了されます。

ただし、異なるツリーをポイントする場合は、この手順を手動で完了する必要があります。

これを実行するのに役立つユーティリティが用意されています。このユーティリティは、次の手順に従ってダウンロードして実行できます。

5a <http://download.novell.com> にアクセスします。

5b 次のフィールドに値を入力します。

- ◆ [Search by] - Product
- ◆ [Choose a Product] - Nsure Identity Manager

5c 「2.0 Password Management Plug-in for iManager 2.0.x」という項目をダウンロードします。

5d nsimhintreadme.txt ファイルに記載された指示に従います。

ユーザが nsimHint 属性についての自己権利を持たない場合、ユーザがヒントを作成しようとするときのようなエラーメッセージが表示されます。

"Could not write user hint" (Task could not be completed).

- 6 (オプション) eDirectory と NMAS を保持するサーバ上に Identity Manager をインストールしていない場合は、Challenge Response Login Method for NMAS をインストールします。

このログインメソッドは Identity Manager によって自動的にインストールされ、eDirectory 8.7.3 の一部として提供されます。

次に、Method Installer を使用して Windows 上にログインメソッドをインストールする 1 つの方法を示します。

- 6a eDirectory CD の `\nmas\NmasMethods` ディレクトリから `MethodInstaller.exe` ファイルを検索します。
- 6b ワークステーションで実行可能ファイルを実行し、チャレンジ / レスポンス方法を確認します。
- 6c 使用許諾契約に同意し、ログインシーケンスのデフォルト値をそのまま使用します。

このメソッドは、Authorized Login Methods.Security. `tree_name` コンテナに追加されます。

UNIX へのインストールを含め、ログインメソッドのインストールの詳細については、『*MAS 2.3 Administration Guide (MAS 2.3 管理ガイド)* (<http://www.novell.com/documentation/lg/nmas23>)』の「Installing a Login Method (ログインメソッドのインストール) (<http://www.novell.com/documentation/lg/nmas23/admin/data/a49tuwk.html#a49tuwk>)」を参照してください。

7 次のモジュールを `exteNd Director` に追加します。

- ◆ `ForgottenPassword.npm`
- ◆ `nmasclient.npm`

これらは DirXML 製品のディストリビューションに付属しています。

モジュールの追加方法については、『*Novell exteNd Director Standard Edition Installation and Configuration Guide (Novell exteNd Director Standard Edition のインストールと設定ガイド)* (<http://www.novell.com/documentation/lg/nedse41/configure/data/ajhotzv.html>)』を参照してください。

パスワードセルフサービスと Virtual Office との統合

NetWare 6.5 Support Pack 2 では、Virtual Office は、パスワードセルフサービスのすべての機能をサポートしています。これらの機能を使用するには、いくつかの手順を実行する必要がありますが、一部の手順は eDirectory ツリー内に Identity Manager をインストールして、iManager サーバ上に Identity Manager プラグインをインストールするときに自動的に実行されます。

手順の詳細については、『*Novell Virtual Office for NetWare 6.5 Configuration Guide (Novell Virtual Office for NetWare 6.5 設定ガイド)* (<http://www.novell.com/documentation/nw65/virtualoffice/data/ac6spye.html>)』を参照してください。Identity Manager をインストールしている場合、すでに完了している項目は次のとおりです。

- ◆ パスワード管理のスキーマの拡張
- ◆ パスワード管理プラグインのインストール
- ◆ Challenge Response Login Method のインストール
- ◆ パスワードヒントへのユーザ権限の付与

注：DirXML プラグインを iManager サーバにインストールする場合、パスワードヒントへのユーザ権限の付与は、iManager が設定されるツリーに対して自動的に完了されます。異なるツリーをポイントする場合は、この手順を手動で完了する必要があります。

企業ポータルからパスワードセルフサービスへのリンク

ForgottenPassword.npm を実行することによってパスワードセルフサービス機能を提供できない製品 (141 ページの「企業ポータルへのパスワードセルフサービスの追加」の表の記述を参照) では、パスワード管理プラグインがインストールされている別の iManager サーバを作成し、ポータルホームページからそのサーバ上の iManager セルフサービスコンソールにリンク (https://iManager_server_IP_address/nps など) することによって、パスワードセルフサービス機能を使用できます。

パスワード管理プラグインは、DirXML 2 プラグインに付属しています。また、<http://download.novell.com> から 2.0 Password Management Plug-in for iManager 2.0.x をダウンロードすることで、個別に入手できます。

簡単に組み込むことができない機能は認証後サービスです。このサービスは、パスワードを更新して Password Policy (パスワードポリシー) に準拠するようユーザに要求し、パスワードヒントの作成など、Password Policy (パスワードポリシー) に従って、パスワードを忘れた場合のセルフサービス機能を設定するように要求します。ユーザのパスワードが準拠しており、パスワードを忘れた場合のセルフサービスを使用するように設定されていることを確認するには、Password Policy (パスワードポリシー) に変更を加えるたびに、ユーザが少なくとも 1 回は iManager セルフサービスコンソールにログインし、準拠するパスワードを作成して、パスワード管理設定を完了していることを確認する必要があります。

次の節の項目を完了します。

- ◆ 145 ページの「前提条件」
- ◆ 145 ページの「パスワードを忘れた場合のセルフサービスへのリンク」
- ◆ 146 ページの「エンドユーザパスワード管理タスクへのリンク」
- ◆ 147 ページの「企業ポータルへのセルフサービスユーザの移動」
- ◆ 148 ページの「ユーザによるパスワード機能設定の確認」

前提条件

使用している iManager サーバとツリーを次のように準備する必要があります。

- ◆ 4 章 47 ページの、「インストール」に記載されている要件を満たす
- ◆ 107 ページの「Password Policy (パスワードポリシー) の使用に関する前提条件」に説明されている前提条件を満たす
- ◆ eDirectory ユーザに対して Password Policy (パスワードポリシー) を設定していることを確認する

パスワードを忘れた場合のセルフサービスへのリンク

ユーザに、企業ポータルからパスワードを忘れた場合のセルフサービスへのアクセスを付与するには、別の iManager Web サーバ上のサービスにリンクします。

- 1 企業ポータルのログインページに [Forgot your password?] のようなリンクを作成し、iManager Web サーバ上の次の URL をポイントします。

```
http://iManager_server_IP_address/nps/servlet/  
fullpageservice?NPSservice=ForgotPassword&nextState=getUserID
```

この URL にアクセスすると次のページがユーザに表示され、パスワードを忘れた場合のプロセスを開始できます。このプロセスの他のページ例については、[118 ページの「エンドユーザへのパスワードを忘れた場合のセルフサービスの提供」](#)を参照してください。



- 2 [147 ページの「企業ポータルへのセルフサービスユーザの移動」](#)の手順をすべて実行します。

エンドユーザパスワード管理タスクへのリンク

- 1 ポータルユーザコンテナ内のすべての eDirectory ユーザが、nsimHint という名前の Hint 属性に対して自己権利を持つことを確認します。

DirXML プラグインを iManager Web サーバにインストールする場合、この手順は iManager が設定されるツリーに対しては自動的に完了されます。

異なるツリーをポイントする場合は、この手順を手動で完了する必要があります。

これを実行するのに役立つユーティリティが用意されています。このユーティリティは、次の手順に従ってダウンロードして実行できます。

1a <http://download.novell.com> にアクセスします。

1b 次のフィールドに値を入力します。

- ◆ [Search by] - Product
- ◆ [Choose a Product] - Nsure Identity Manager

1c 「2.0 Password Management Plug-in for iManager 2.0.x」という項目をダウンロードします。

1d nsimhintreadme.txt ファイルに記載された指示に従います。

ユーザが nsimHint 属性についての自己権利を持たない場合、ユーザがヒントを作成しようとするときのようなエラーメッセージが表示されます。

"Could not write user hint" (Task could not be completed).

2 ユーザに企業ポータルからパスワード管理タスクへのリンクを提供します。

会社ポータルからの [Manage Passwords] リンクを作成して、https://other_iManager_server/nps にリンクできます。このリンクによって、次のパスワード管理エンドユーザタスクにアクセスできるようになります。

- ◆ Hint Setup
- ◆ Answer Challenge Questions
- ◆ Change Password (Universal)

リンクをクリックするユーザは、まずログインする必要があります。ログイン後、次のようなページが表示されます。



3 147 ページの「企業ポータルへのセルフサービスユーザの移動」の手順をすべて実行します。

企業ポータルへのセルフサービスユーザの移動

パスワードセルフサービス機能には、ログインページに戻ることでリンクをユーザに提供するシナリオが含まれます。たとえば、ユーザがパスワードを忘れた場合のセルフサービスを使用してパスワードを変更すると、「Your password has been successfully changed. Click here to return to login page」というメッセージを示したページが表示されます。

企業ポータルから別の iManager サーバ上のパスワードセルフサービスをポイントする場合、デフォルトのリターンページをカスタマイズして、パスワードタスクの完了時に企業ポータルのログインページに戻るようにできます。デフォルトでは、ボタンをクリックすると、ユーザは iManager Web サーバ上のページに戻ります。

ログインページに戻るリンクは、次の3つの場所に用意されています。

- ◆ ユーザが新しいパスワードを設定できるページ
- ◆ ユーザがパスワードを正常に変更した後で表示されるページ
- ◆ ユーザがヒントを表示するページ

リターンページをカスタマイズするには、次の手順に従って企業ポータルログインページに進みます。

- 1 パスワードを忘れた場合のセルフサービスに使用している iManager Web サービスから、次のディレクトリを検索します。

```
¥tomcat¥webapps¥nps¥portal¥modules¥ForgottenPassword¥skins¥default¥devices¥default
```

- 2 そのディレクトリで次のファイルを検索します。

```
forgottenpassword.xml
```

- 3 forgottenpassword.xml ファイルを編集して、デフォルトのリターンページをカスタマイズします。

次のコードを、ハードコードした URL に置き換えます。

```
href="{LoginURL}"
```

たとえば、次のような URL に置き換えます。

```
href="(http:\\www.your_company_portal_home_page.com)"
```

この変更はファイル内の3つの場所で行う必要があります。

- 4 iManager サーバ上の Tomcat を停止し、再起動します。

これで、[Return to Login Page] リンクをクリックすると、ユーザは企業ポータルログインページにリダイレクトされます。

ユーザによるパスワード機能設定の確認

ユーザが `https://iManager_server_IP_address/nps` で iManager セルフサービスコンソールにログインすると、次のような条件を満たす場合、一連の認証後ページを介して操作するように要求するメッセージが表示されます。

- ◆ ユーザのパスワードが Password Policy (パスワードポリシー) 内の Advanced Password Rule (詳細パスワードルール) に準拠しない
- ◆ Password Policy (パスワードポリシー) で、パスワードを忘れた場合のセルフサービス使用時のチャレンジ質問が要求されていて、ユーザがこれらを設定していない
- ◆ Password Policy (パスワードポリシー) で、パスワードを忘れた場合の機能を、[Display Password Hint] をアクションとして使用していて、ユーザがヒントを作成していない

たとえば、これらの要求メッセージは、パスワードを忘れた場合のセルフサービスをユーザが確実に使用できるようにするために必要です。Password Policy (パスワードポリシー) で、ユーザがチャレンジ質問に回答するよう要求されていて、ユーザがこれらを最初に設定していない場合、ユーザはパスワードを忘れた場合のセルフサービスにアクセスできません。ユーザがパスワードヒントを作成していない場合、ユーザはパスワードヒントを取得して、パスワードを思い出すために利用できません。

その他のポータル製品では、認証後機能は自動的に提供されないため、Password Policy（パスワードポリシー）を変更するたびに、ユーザが少なくとも1回は iManager セルフサービスコンソールにログインし、**準拠したパスワードを作成し、パスワード管理設定を完了する**ようにする必要があります。

このためには、**146 ページの「エンドユーザパスワード管理タスクへのリンク」**の説明に従って、ユーザが提供された [Manage Passwords] リンクにアクセスするようにします。これにより、ユーザが iManager セルフサービスコンソールにログインしなければなりません。

パスワードセルフサービスのトラブルシューティング

- ◆ チャレンジ回答の質問を使用するには、iManager 2.02 がサポートするブラウザを使用していることを確認します。
- ◆ SSL を適切に設定していない場合は、iManager またはセルフサービスコンソールにログインできません。ただし、iManager に問題なくログインでき、単純なバインドのために TLS を要求している場合、SSL は適切に設定されており、パスワードセルフサービスをトラブルシューティングする際に、SSL 関連の問題は除外できます。
- ◆ 次の節も参照してください。
 - ◆ **113 ページの「Password Policy（パスワードポリシー）のトラブルシューティング」**
 - ◆ Identity Manager パスワード同期を使用している場合は、**234 ページの「パスワード同期のトラブルシューティング」**、**184 ページの「パスワード同期の実装」**の各シナリオのトラブルシューティングに関する節、および**ドライバマニュアルの Web サイト** (<http://www.novell.com/documentation/lg/dirxmldrivers>) に掲載されている、関連する特定のドライバのマニュアルを参照してください。

9

接続システム間のパスワード同期

Nsure™ Identity Manager パスワード同期は、次のような新しい利点をいくつか備えています。

- ◆ 双方向のパスワード同期
- ◆ 接続システムへの Password Policy（パスワードポリシー）の適用
- ◆ 同期失敗時の電子メールによる通知
- ◆ ユーザのパスワードの同期化ステータスを確認する機能

オプションの理解に役立つよう、184 ページの「パスワード同期の実装」で、いくつかのシナリオが説明されています。

この節では、次の項目について説明します。

- ◆ 151 ページの「概要」
- ◆ 159 ページの「パスワード同期をサポートする接続システム」
- ◆ 161 ページの「パスワード同期の前提条件」
- ◆ 173 ページの「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」
- ◆ 184 ページの「パスワード同期の実装」
- ◆ 168 ページの「機密情報の処理」
- ◆ 176 ページの「新しいドライバ設定と Identity Manager パスワード同期」
- ◆ 178 ページの「Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード」
- ◆ 178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」
- ◆ 216 ページの「パスワードフィルタの設定」
- ◆ 217 ページの「パスワード同期の管理」
- ◆ 220 ページの「ユーザのパスワード同期ステータスのチェック」
- ◆ 220 ページの「電子メール通知の設定」
- ◆ 234 ページの「パスワード同期のトラブルシューティング」

概要

Identity Manager では、パスワードの発行と加入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を導入しています。

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

- ◆ 152 ページの「パスワードの概要」
- ◆ 153 ページの「Password Synchronization 1.0 と Identity Manager パスワード同期の比較」
- ◆ 154 ページの「双方向パスワード同期とは」
- ◆ 155 ページの「Identity Manager パスワード同期の機能」
- ◆ 158 ページの「パスワード同期フローの図」

パスワードの概要

eDirectory には、さまざまな目的に使用される複数のパスワードがあります。eDirectory と DirXML 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、これは一方向の同期でした。

eDirectory 8.7.1 で導入されたユニバーサルパスワードは、必要に応じてその他の eDirectory パスワードと同期化できる逆方向パスワードです。ユニバーサルパスワードは、4 つの暗号化層で保護されています。

NMAS は、ユニバーサルパスワードとその他の eDirectory パスワードとの関係を制御します。たとえば、ユニバーサルパスワードが NDS パスワード、通常パスワード、または配布パスワードとの同期が維持されているかどうかを確認します。NMAS は、パスワード変更を要求する着信リクエストを傍受し、Password Policy (パスワードポリシー) の設定に従って処理します (一部のレガシーメソッドを除く。103 ページの「ユーザのログインおよびパスワード変更方法の計画」を参照してください)。

eDirectory パスワード間の関係を制御する Password Policy インタフェースの例については、96 ページの「ユニバーサルパスワードの有効化」の図を参照してください。

Identity Manager は、eDirectory 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 eDirectory 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 4 つの暗号化層で保護されていて、逆方向で同期化できます。

[Password Policy] で、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 (この設定は [Synchronize Distribution Password when setting Universal Password] 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よう選択する場合は、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できます。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 (168 ページの「機密情報の処理」を参照)。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 ([Password Policy] 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て接続システム間でパスワードを「トンネル」することはできません。

eDirectory のさまざまなパスワードについては、『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Novell Modular Authentication Services (NMAS) 2.3 管理ガイド)* (<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、184 ページの「パスワード同期の実装」を参照してください。

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

	Password Synchronization 1.0	Identity Manager 2 パスワード同期
製品の提供	DirXML とは別の製品	Identity Manager に含まれる機能。単体の製品としては販売されません。
プラットフォーム	<ul style="list-style-type: none"> ◆ Active Directory ◆ NT ドメイン ◆ eDirectory 	<ul style="list-style-type: none"> ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT ドメイン <p>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。</p> <p>加入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。</p> <p>『<i>Novell Nsure Identity Manager 2 管理ガイド</i>』の「パスワード同期の接続システムのサポート」を参照してください。</p>
eDirectory で使用されるパスワード	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、『 <i>Novell Nsure Identity Manager 2 管理ガイド</i> 』の「パスワード同期の実装」を参照してください。
Windows 接続システムの主な機能	eDirectory パスワードが Windows パスワードと同期されるようにパスワードを DirXML に送信。NDS パスワードは逆方向に同期化できないため、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。ユニバーサルパスワード（および配布パスワード）は逆方向に同期化できるため、パスワードは両方のディレクトリで同期化できます。
LDAP 変更	サポートなし	サポートあり
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。

	Password Synchronization 1.0	Identity Manager 2 パスワード同期
パスワード同期機能を含むコンポーネント	nadLoginName を更新するための機能は DirXML ドライバに含まれていました。	<p>ドライバ設定の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、DirXML エンジンによって与えられるタスクを実行します。</p> <p>ドライバマニフェスト、グローバル設定値、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、サンプルドライバ設定に含まれており、既存のドライバに追加できます。178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。</p>
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。

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取る Identity Manager と、指定した接続にパスワードを配布する Identity Manager 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信し、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。これらのシステムを次に示します。

- ◆ Active Directory
- ◆ Novell® eDirectory™
- ◆ 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化できます。ただし、Password Policy（パスワードポリシー）で Advanced Password Rule（詳細パスワードルール）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信できる場合があります。

159 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。

Identity Manager パスワード同期の機能

Identity Manager パスワード同期によって提供される機能を説明するために、双方向のパスワード同期の対象を2つに分けることができます。それは、接続システムから送信されて Identity Manager によって受信されるパスワードと、Identity Manager によって配布されて接続システムによって受信されるパスワードです。

次の節では、Identity Manager のパスワード同期の機能について説明します。

- ◆ 155 ページの「Identity Manager が接続システムからパスワードを受信する機能」
- ◆ 156 ページの「Identity Manager から接続システムにパスワードを配布する機能」
- ◆ 156 ページの「Identity Manager がデータストアおよび接続システムで Password Policy（パスワードポリシー）を適用する機能」
- ◆ 157 ページの「Identity Manager が提供する同期パスワード用の複数のシナリオ」
- ◆ 157 ページの「Identity Manager からユーザにパスワード同期の失敗を通知する機能」
- ◆ 158 ページの「Identity Manager がユーザのパスワード同期ステータスを確認する機能」

Identity Manager が接続システムからパスワードを受信する機能

DirXML[®] 以前のバージョンと同様に、接続システムは識別ボールドにパスワードを発行できます。

Identity Manager がパスワードを受信す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 eDirectory ツリー内でユーザのパスワードを更新するかどうか、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ルートまたは「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、eDirectory 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 eDirectory ツリー、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 と同期化して、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。

Identity Manager から接続システムにパスワードを配布する機能

Identity Manager パスワード同期には、共通のパスワードを接続システムに配布する機能が導入されています。

DirXML 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 DirXML 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、逆方向に同期化できないため、中央の Identity Manager 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ありませんでした。

eDirectory 8.7.3 が提供する新しいユニバーサルパスワードは逆方向に同期化できるため、配布できます。

Identity Manager は接続システムからパスワードを受け取ります。ユニバーサルパスワードは逆方向に同期化できるため、Identity Manager は、そのパスワードを識別ボールトから、新しいアカウントの初期パスワードの設定とパスワードの変更をサポートする接続システムに配布できます。

パスワードの発行元に関係なく、Identity Manager は配布パスワードを、接続システムにパスワードを配布する場所であるレポジトリとして使用します。ユニバーサルパスワードと同様に、配布パスワードでも、Password Policy（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、[184 ページの「パスワード同期の実装」](#)を参照してください。

ユーザのその他の属性と同様に、どのシステムをパスワードの承認されたソースにするかを決定でき、Identity Manager は承認されたソースからその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。

Identity Manager がデータストアおよび接続システムで Password Policy（パスワードポリシー）を適用する機能

Identity Manager では、NMASTM を呼び出すことによって、着信パスワードに Password Policy（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準拠していない場合は、Identity Manager がその識別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 Password Policy（パスワードポリシー）を適用することもできます。Identity Manager に発行されたパスワードが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、識別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、少なくとも 1 つの数字を含むパスワードを要求している場合に、接続システム自体にそのようなポリシーを適用する機能がない場合、準拠しない接続システムからのパスワードを Identity Manager がリセットするように指定できます。

Advanced Password Rule（詳細パスワードルール）と Identity Manager パスワード同期を使用している場合、パスワードが確実に同期されるように、接続システムすべての Password Policy（パスワードポリシー）を調査し、eDirectory パスワードポリシー内の Advanced Password Rule（詳細パスワードルール）に互換性があることを確認することをお勧めします。

Password Policy（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。

Password Policy（パスワードポリシー）はツリー中心で割り当てられます。対照的に、パスワード同期はドライブごとに設定されます。ドライブはサーバーベースでインストールされ、マスタレプリカまたは読み書き可能レプリカ内に存在するユーザのみを管理できます。パスワードの同期化により期待される結果を取得するには、パスワードの同期化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 Password Policy（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 Password Policy（パスワードポリシー）が割り当てられます。

Password Policy（パスワードポリシー）をユーザに割り当てる方法については、[111 ページの「ユーザへの Password Policy（パスワードポリシー）の割り当て」](#)を参照してください。

Identity Manager が提供する同期パスワード用の複数のシナリオ

その他の属性と同様に、Identity Manager ではどのシステムをパスワードの承認されたソースにするかを決定できます。Identity Manager では、パスワードが移動する方法を柔軟に決定できます。

Identity Manager パスワード同期の新しい機能のほとんどは、eDirectory が提供する、逆方向に同期化できる新しい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。

ただし、ユニバーサルパスワードを展開する必要のないシナリオもあります。

さらに、Identity Manager パスワード同期は、Identity Manager が接続システムにパスワードを配布する元のレポジトリである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、[184 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ると、各環境のニーズを満たすことができます。

Identity Manager で Novell Client なしで Windows 上でパスワードを同期化する機能

Active Directory と 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。

Identity Manager からユーザにパスワード同期の失敗を通知する機能

[156 ページの「Identity Manager がデータストアおよび接続システムで Password Policy（パスワードポリシー）を適用する機能」](#)では、Identity Manager は準拠しないパスワードを接続システムから受け取らないことによって Password Policy（パスワードポリシー）を適用できることを説明しました。

新しい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。

たとえば、NT ドメインからの着信パスワードが Password Policy（パスワードポリシー）に準拠しない場合、Identity Manager でこれを受け入れないように設定していて、電子メールの通知を有効にしているとします。Password Policy（パスワードポリシー）のあるルールでは、会社名をパスワードとして使用できないことを示していて、あるユーザが NT ドメイン接続システム上でパスワードを会社名に変更します。この場合、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化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。Identity Manager が送信するメッセージテキストはカスタマイズできます。また、通知をカスタマイズして、管理者にコピーを送信できます。詳細については、[220 ページの「電子メール通知の設定」](#)を参照してください。

Identity Manager がユーザのパスワード同期ステータスを確認する機能

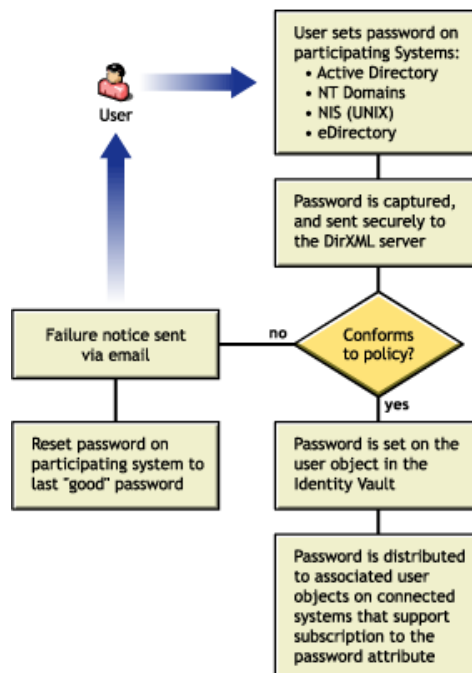
Identity Manager は、接続システムに問い合わせて、ユーザのパスワード同期ステータスを確認します。接続システムがパスワードの確認機能をサポートしている場合、パスワードが正常に同期化されているかどうかを確認できます。

パスワードを確認する方法については、[220 ページの「ユーザのパスワード同期ステータスのチェック」](#)を参照してください。

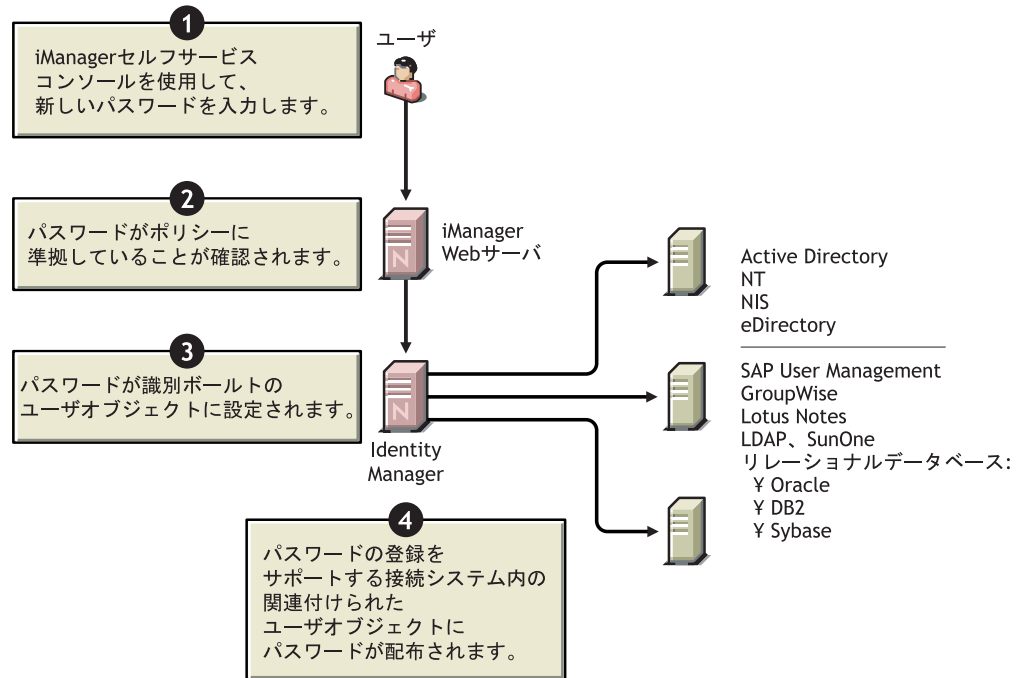
パスワードの確認をサポートしているシステムのリストについては、[159 ページの「パスワード同期をサポートする接続システム」](#)を参照してください。

パスワード同期フローの図

Identity Manager にパスワードを発行する接続システムの概要を次に示します。



接続システムにパスワードを配布する Identity Manager の概要を次に示します。



パスワード同期をサポートする接続システム

Identity Manager は常に接続システムからパスワードを受信できます。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、eDir、およびNISはIdentity Managerからパスワードを受信でき、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。

その他のシステムは、発行者チャネルのドライバ設定内にポリシーを定義することによって、パスワードを作成するために使用できるデータを提供できます。この例については、ほとんどのドライバのサンプルドライバ設定で示されています。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。

この節では、接続システムのリスト、およびサンプルドライバ設定でサポートされている機能を示します。

サンプルドライバ設定の機能は、ドライバマニフェストに記載されています。この表は、ドライバマニフェストにない次の追加情報を示します。

- ◆ アプリケーションがパスワードを受け入れることができるかどうかについては、この表は、アプリケーションが新しいアカウントに設定された初期パスワードを受け取るかどうかと、既存のパスワードへの変更を受け取ることができるかどうかを示します。

マニフェストでは、接続システムがパスワードを受け取ることができ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。

- ◆ ドライバをグループ化することで、様の機能を持つサンプルドライバ設定を確認できます。

接続システムのドライバ	加入者チャンネル	加入者チャンネル	加入者チャンネル	発行者チャンネル
	アプリケーションが初期パスワードの設定を受け取ることができる	アプリケーションがパスワードの変更を受け取ることができる	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	Identity Manager がパスワードを提供（同期化）できる

次の接続システムは、双方向パスワード同期をサポートします。

これらは、接続システム上でユーザの実際のパスワードを提供し、Identity Manager からのパスワードを受け取ることができます。

Active Directory	はい	はい	はい	はい
eDirectory ¹	はい	はい	はい	はい
NT ドメイン	はい	はい	いいえ	はい
NIS	はい	はい	はい	はい
SIF	はい	はい	いいえ	はい

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取ることができます。これらのシステムは、接続システム上でユーザの実際のパスワードを Identity Manager に提供できません。ユーザの実際のパスワードは提供できませんが、接続システム内のその他のユーザデータに基づき、発行者チャン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（サンプルドライバ設定には、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）。

Groupwise [®]	はい	はい	いいえ	いいえ ²
JDBC	はい ³	いいえ ⁴	いいえ	いいえ ⁵
LDAP	はい ⁶	はい ⁶	はい	いいえ
Notes	はい	はい ⁷	はい ⁷	いいえ
SAP User Management	はい	はい	いいえ	いいえ

次の接続システムは、サンプルドライバ設定を使用してパスワードを受け取ったり、接続システム上でユーザのパスワードを提供したりできません。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、接続システム内のその他のユーザデータに基づき、発行者チャン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（サンプルドライバ設定には、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）。

区切りテキスト	いいえ ⁸	いいえ ⁸	いいえ ⁸	いいえ ⁸
Exchange 5.5	いいえ	いいえ	いいえ	いいえ
PeopleSoft 3.6	いいえ	いいえ	いいえ	いいえ
PeopleSoft 4.0	いいえ	いいえ	いいえ	いいえ
SAP HR	いいえ	いいえ	いいえ	いいえ

次の接続システムは、パスワード同期での使用向けではありません。

Avaya* PBX	いいえ	いいえ	いいえ	いいえ
エンタイトルメントサービスドライバ	いいえ	いいえ	いいえ	いいえ
LoopBack サービスドライバ	いいえ	いいえ	いいえ	いいえ

接続システムのドライバ	加入者チャンネル	加入者チャンネル	加入者チャンネル	発行者チャンネル
	アプリケーションが初期パスワードの設定を受け取ることができる	アプリケーションがパスワードの変更を受け取ることができる	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	Identity Manager がパスワードを提供（同期化）できる
手動タスクサービスドライバ	いいえ	いいえ	いいえ	いいえ

¹eDirectory 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。185 ページの「シナリオ 1 - NDS パスワードを使用した eDirectory 間でのパスワード同期化」を参照してください。

²GroupWise は 2 つの認証方法をサポートします。1) GroupWise は独自の認証を提供し、ユーザパスワードを維持します。2) GroupWise は 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。オプション 2 を使用すると、GroupWise はドライバ同期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*OS など、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。

⁴JDBC の DirXML 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、サンプルドライバ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化できます。

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

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

⁸DirXML Driver for Delimited Text 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を持ちません。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。

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。

- ◆ 162 ページの「ユニバーサルパスワードのサポート」
- ◆ 162 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」
- ◆ 162 ページの「グローバル設定値を使用して作成するパスワード同期設定」
- ◆ 166 ページの「ドライバ設定で必要なポリシー」
- ◆ 167 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」
- ◆ 168 ページの「ユーザ用に作成する Password Policy（パスワードポリシー）」
- ◆ 168 ページの「NMASS ログインメソッド」

ユニバーサルパスワードのサポート

175 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」を参照してください。

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 からパスワードを受け取る（マニフェストは初期パスワードの作成の受け取りと、パスワード変更の受け取りを区別しません）
- ◆ 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できる

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。これは、ドライバシムと設定の真の機能を表すものであるため、マニフェストだけ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、またはドライバ設定を強化する必要があります。

Identity Manager に付属するドライバ設定はドライバマニフェストエントリを含みません。既存のドライバにこれらを追加するには、178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。

グローバル設定値を使用して作成するパスワード同期設定

グローバル設定値は Identity Manager の新機能で、これにより、ポリシー内で参照できる定数値を設定できます（これらは、サーバ変数と呼ばれることもあります。レプリカごとの属性に保持されるためです）。

パスワード同期では、これらの設定値を使用して、Identity Manager に対するパスワードフローの設定を作成できます。

ドライバ設定内のパスワード同期ポリシーはグローバル設定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のフローを簡単に変更できます。

グローバル設定値を使用して、各接続システムの次の設定を制御できます。インタフェースでは、Identity Manager は DirXML と呼ばれます。

- ◆ 接続システムから Identity Manager がパスワードを受け取るかどうか。
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、および発行者チャンネルのドライバ設定内の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。
- ◆ ユニバーサルパスワードの直接更新、または配布パスワードの直接更新のどちらの同期方法を Identity Manager が使用するか。Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager が更新するかを制御します。NMAS は、Password Policy（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。この設定を行うには、[Universal Password] > [Configuration Options] の順に選択します。

これらの方法を使用したシナリオ例については、184 ページの「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 Password Policy (パスワードポリシー) を適用するかどうか。
適用した場合、着信パスワードは、準拠しない場合は Identity Manager データストアに書き込まれないことになります。
- ◆ Identity Manager が Identity Manager パスワードを使用して、準拠しないパスワードをリセットすることによって接続システムに Password Policy (パスワードポリシー) を適用するかどうか。
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)。
- ◆ 接続システムがパスワードを受け取るかどうか。
この設定は Identity Manager によって配布されるパスワードと、加入者チャンネルのドライバ設定内の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。

Identity Manager に付属するドライバ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、[178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」](#)を参照してください。

これらの GCV は、iManager の [Password Synchronization] タスク ([Password Management] > [Password Synchronization]) で編集します。このグラフィカルインタフェースを使用して、接続システムと Identity Manager の間のパスワードフローを指定できます。

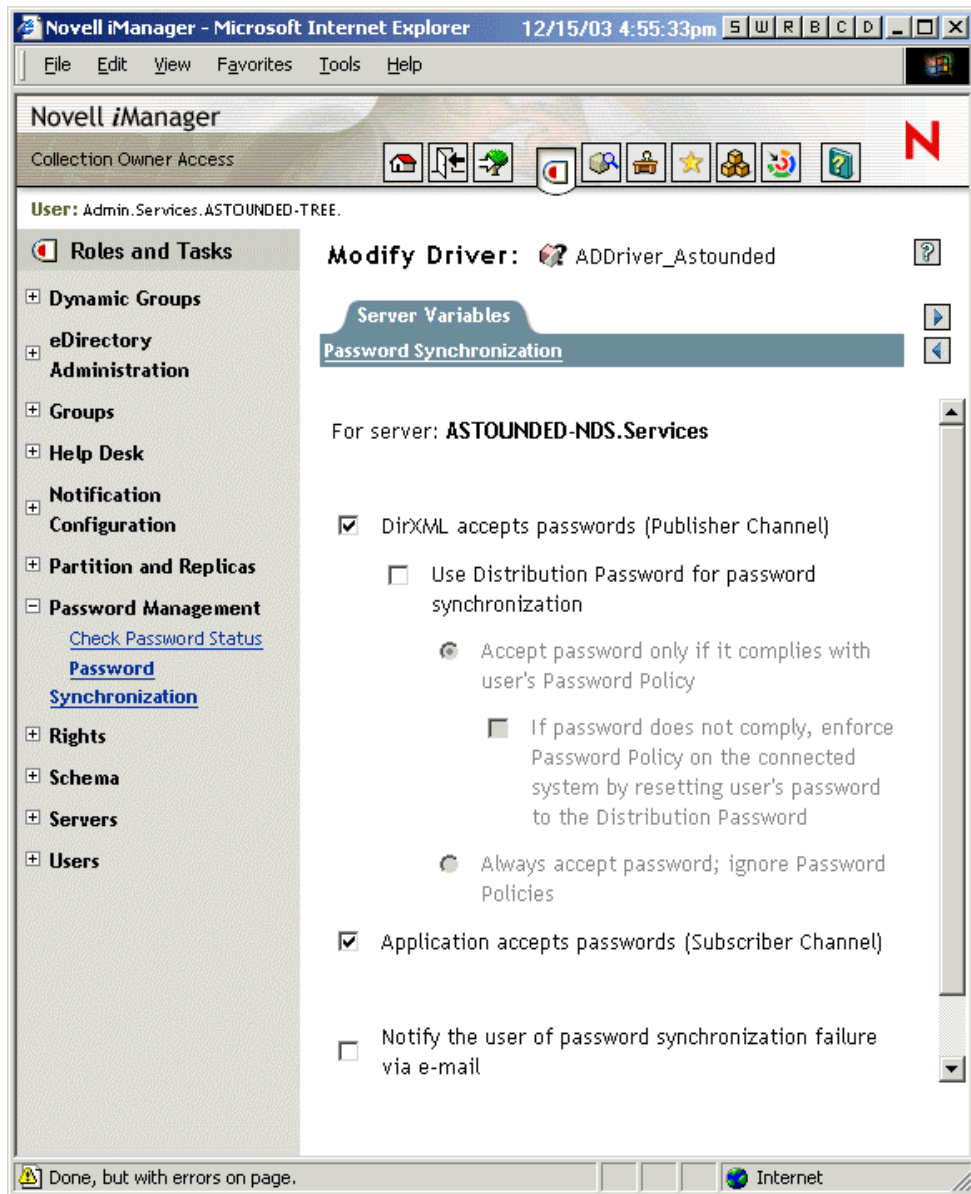
接続システムドライバを検索する場所を指定すると、インタフェースによって検索されたすべての接続システムに対するパスワードフロー設定の概要が表示されます。概要ページの一例を次に示します。

The screenshot shows the Novell iManager web interface in a Microsoft Internet Explorer browser window. The page title is "Novell iManager" and the user is identified as "admin.Novell.DXML3-TREE". The main content area is titled "Password Synchronization" and contains a table of "Connected Systems: .DXML3-TREE.".

Name	Server	DirXML Accepts Passwords	Application Accepts Passwords
ADDriver	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
DB2	DXML3	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Not Available
eDirectory Driver99	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Entitlement Services Driver	DXML3	<input type="checkbox"/> Not Available	<input type="checkbox"/> Not Available
NT Domains	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

このページでは、ドライバ名をクリックすると、制御するすべての設定をドリルダウンして表示できます。

次の図は、表示されるページを示します。これは、パスワード同期のグローバル設定値を設定するためのグラフィカルインターフェースです。



このページのオプションが淡色表示されている場合は、ドライバマニフェストによって、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が示されています。

注：このインタフェースによって、各ドライバのグローバル設定値を設定できます。ドライバのグローバル設定値は、ドライバセットの値よりも優先され、特定のドライバにグローバル設定値を設定することで、より細分化された制御が可能です。このページは、個々のドライバに存在するグローバル設定値だけを表示できます。

グローバル設定値は、ドライバ設定オブジェクトに設定でき、ドライバセット内のドライバが自身の値を持たない場合はそのドライバがグローバル設定値を継承します。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設定値を継承する場合、このインタフェースは表示されません。このインタフェースには継承されているグローバル設定値は表示されませんが、グローバル設定値はパスワード同期ポリシーによって適用されます。

ドライバ設定で必要なポリシー

各ドライバの発行者チャンネルと加入者チャンネルのポリシーは、前述のグローバル設定値内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 のドライバ設定に含まれます。

既存のドライバ設定を置き換えるのではなく更新する場合は、これらのポリシーを設定に追加する必要があります (178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照)。

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設定の正しい場所に指定する必要があります。

ドライバ設定内の場所	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) これらのポリシーはこの順番で表示され、Publisher Command Transformation (発行者コマンド変換) ポリシーセット内の最後のポリシーである必要があります。	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(加入者)-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を適切に動作させるには、その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 のチェック)	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取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 [DirXML accepts passwords from application] 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、publish-password-to-dp、および enforce-password-policy です。
	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、パスワード要素を除去します。 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、エンジン内で閲覧されるペイロードデータを挿入します。

ドライバ設定内の場所	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) 入力変換に複数のポリシーがある場合、このポリシーは最後に記述することをお勧めします。	Password(Pub)-Sub Email Notifications (パスワード(発行者)-加入者の電子メール通知)	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、ユーザーに電子メールを送信します。電子メールは、eDirectory内のInternet EMail Address 属性に示されているユーザー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。
Subscriber Command Transformation (加入者コマンド変換) これらのポリシーはこの順番で表示され、Subscriber Command Transformation (加入者コマンド変換) ポリシーセット内の最後のポリシーである必要があります。	Password(Sub)-Transform Distribution Password (パスワード(加入者)-配布パスワードの変換) Password(Sub)-Default Password Policy (パスワード(加入者)-デフォルトパスワードポリシー)	ユニバーサルパスワードを <password> 要素に変換します。 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を適切に動作させるには、その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(加入者)-パスワード GCV のチェック)	GCV を確認し、接続システムがパスワードを受け取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 [Application accepts passwords from DirXML data store] です。
	Password(Sub)-Add Password Payload (パスワード(加入者)-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。
Subscriber Output Transformation (加入者出力変換) 出力変換に複数のポリシーがある場合、このポリシーは最後にリストすることをお勧めします。	Password(Sub)-Pub Email Notifications (パスワード(加入者)-発行者の電子メール通知)	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、ユーザー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。

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、ユーザー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。

[216 ページの「パスワードフィルタの設定」](#)を参照してください。

ユーザ用に作成する Password Policy（パスワードポリシー）

Password Policy（パスワードポリシー）を使用してユーザ用のユニバーサルパスワードを有効にする必要があります（ただし、ユニバーサルパスワードなしでもパスワード同期の一部の機能は使用できます）。また、Password Policy（パスワードポリシー）によって、Advanced Password Rule（詳細パスワードルール）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 パスワード同期を使用するには、Password Policy（パスワードポリシー）を理解する必要があります。

Password Policy（パスワードポリシー）については、7 章 95 ページの、「[Password Policy（パスワードポリシー）を使用したパスワードの管理](#)」で説明しています。

NMAS ログインメソッド

状況によっては、NMAS Simple Password Login Method 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。

ログインメソッドについては、『[Novell Modular Authentication Services \(NMAS\) 2.3 Administration Guide \(Novell Modular Authentication Services \(NMAS\) 2.3 管理ガイド\)](http://www.novell.com/documentation/nmas23/index.html) (<http://www.novell.com/documentation/nmas23/index.html>)』を参照してください。

機密情報の処理

Identity Manager パスワード同期は、ユーザパスワードを簡素化し、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。その新機能の 1 つが双方向パスワード同期です。これにより、184 ページの「[パスワード同期の実装](#)」のシナリオで説明されているように、eDirectory と接続システムの間で、複数の方法でパスワードを共有できます。

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。

Identity Manager とパスワード同期を使用するための計画の一部として、次のセキュリティ上の推奨事項を確認することをお勧めします。

- ◆ 169 ページの「[SSL の使用](#)」
- ◆ 169 ページの「[セキュリティで保護された eDirectory および Identity Manager オブジェクトへのアクセス](#)」
- ◆ 169 ページの「[パスワード管理機能のセキュリティ上の考慮事項の確認](#)」
- ◆ 170 ページの「[強力な Password Policy（パスワードポリシー）の作成](#)」
- ◆ 171 ページの「[パスワード同期に参加する接続システムのセキュリティ保護](#)」
- ◆ 171 ページの「[セキュリティの業界ベストプラクティスへの準拠](#)」
- ◆ 171 ページの「[Nsure Audit を使用した機密情報の変更の追跡](#)」

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にする必要があります。SSL は、DirXML エンジンとリモートローダ (69 ページの「[セキュリティで保護されたデータ転送の提供](#)」を参照) の間、DirXML 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。

セキュリティで保護された eDirectory および Identity Manager オブジェクトへのアクセス

物理的なセキュリティ - Novell eDirectory 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。

- ◆ DirXML ドライバセット。
- ◆ DirXML 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。
- ◆ Password Policy (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。

パスワード管理機能のセキュリティ上の考慮事項の確認

- ◆ Password Policy (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、eDirectory に問い合わせ、どの Password Policy (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。Password Policy (パスワードポリシー) で、強力なパスワードを作成するようユーザに要求する場合、170 ページの「[強力な Password Policy \(パスワードポリシー\) の作成](#)」に説明されているように、これがリスクになることは避ける必要があります。
- ◆ 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。パスワードヒントは、ヘルプデスクへの問い合わせ削減に大きな効果があります。

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せん。

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チャレンジ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。Password Policy (パスワードポリシー) 内の [Password Change Message] は、これを実行する 1 つの方法です。139 ページの「Password Policy (パスワードポリシー) への独自の Password Change Message (パスワード変更メッセージ) の追加」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 Password Policy (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。パスワードヒントが設定されないようにするには、さらに高度な設定として、Hint Setup ガジェットを完全に削除します。137 ページの「Hint ガジェットの削除によるパスワードヒントの無効化」を参照してください。

- ◆ チャレンジ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。チャレンジ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。

チャレンジ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チャレンジ質問を作成できます。本人だけが理解できるチャレンジ質問と回答を作成するように徹底してください。[Password Policy] の [Password Change Message] は、これを実行する 1 つの方法です。139 ページの「Password Policy (パスワードポリシー) への独自の Password Change Message (パスワード変更メッセージ) の追加」を参照してください。

- ◆ セキュリティのため、[Forgotten Password] のアクション [E-mail password to user] および [Allow user to reset password] は、チャレンジ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回答する場合などに、管理者がユーザのパスワードを変更する場合、Password Policy (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、セキュリティ上の理由からパスワードは自動的に期限切れになります。Password Policy (パスワードポリシー) のこの設定は、Advanced Password Rule (詳細パスワードルール) にあり、[Number of days before password expires (0-365)] という名前が付けられています。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。

強力な Password Policy (パスワードポリシー) の作成

ユニバーサルパスワードと Password Policy (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。[Password Policy] の [Advanced Password Rule] 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 Password Policy (パスワードポリシー) を作成できます。Password Policy (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 (管理を簡素化するために、Password Policy (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ておく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 [Password Policy] の設定ではなく、親コンテナの設定です。『*Novell eDirectory 8.7.3 管理ガイド* (<http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv>)』の「ユーザアカウントの管理」を参照してください。

パスワード同期に参加する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 Windows 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。

セキュリティの業界ベストプラクティスへの準拠

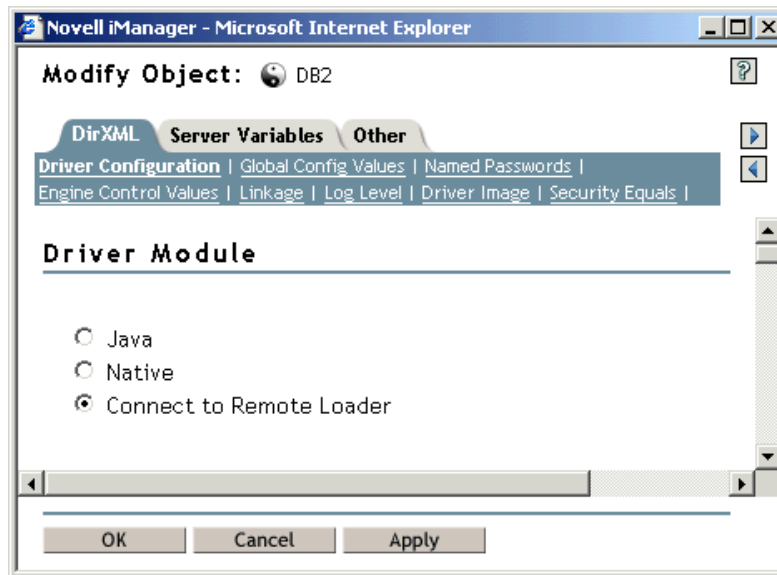
サーバ上の未使用ポートをブロックするなど、セキュリティ対策に関する業界ベストプラクティスに従っていることを確認します。

Nsure Audit を使用した機密情報の変更の追跡

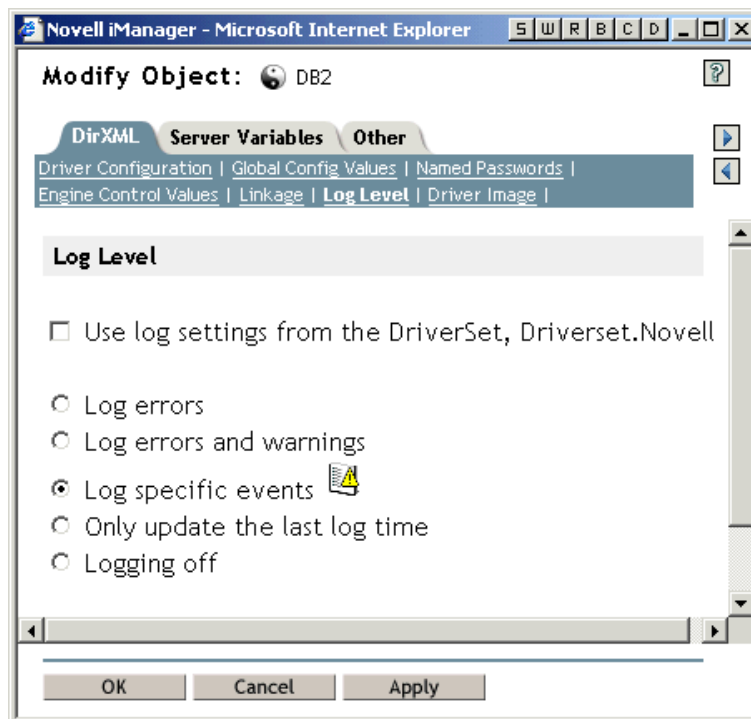
Nsure Audit を使用すると、セキュリティにとって重要と思われるイベントのログを記録できます。Nsure Audit の詳細については、[13 章 269 ページの「Nsure Audit によるログとレポート」](#)を参照してください。


たとえば、特定の DirXML 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 ドライバ (またはドライバセット) のプロパティの [DirXML] タブで、[Log Level] をクリックします。



- 2 [Log Level] ページが表示されたら、[Log Specific Events] をクリックします。これは、ドライバに対して独自の設定を行うか、ドライバセットの設定を使用するかを指定するページです。



- 3 具体的なイベントを選択するには、[log events] アイコン  をクリックします。
- 4 [Events] ページが表示されたら、次のチェックボックスをオンにします。
- ◆ [Operation Events] で、[Change Password] 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。

- ◆ [Transformation Events] で、[Password Set] および [Password Sync] 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。

Operation Events

- | | | |
|--|--|---|
| <input type="checkbox"/> Search | <input type="checkbox"/> Add | <input type="checkbox"/> Remove |
| <input type="checkbox"/> Modify | <input type="checkbox"/> Rename | <input type="checkbox"/> Move |
| <input type="checkbox"/> Add Association | <input type="checkbox"/> Remove Association | <input type="checkbox"/> Query Schema |
| <input type="checkbox"/> Check Password | <input type="checkbox"/> Check Object Password | <input checked="" type="checkbox"/> Change Password |
| <input type="checkbox"/> Sync | <input type="checkbox"/> Clear Attribute | <input type="checkbox"/> Add Value |
| <input type="checkbox"/> Remove Value | <input type="checkbox"/> Merge Entry | |

Transformation Events

- | | | |
|--|--|---|
| <input type="checkbox"/> Initial Document | <input type="checkbox"/> Input | <input type="checkbox"/> Output |
| <input type="checkbox"/> Event | <input type="checkbox"/> Placement | <input type="checkbox"/> Create |
| <input type="checkbox"/> Input Mapping | <input type="checkbox"/> Output Mapping | <input type="checkbox"/> Matching |
| <input type="checkbox"/> Command | <input type="checkbox"/> Driver Filter | <input type="checkbox"/> User Agent Request |
| <input type="checkbox"/> Resync Request | <input type="checkbox"/> Migrate Request | <input checked="" type="checkbox"/> Password Sync |
| <input checked="" type="checkbox"/> Password Set | | |

5 [Events] ページおよび [Log Level] ページの [OK] をクリックします。

Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業

この節では、次の項目について説明します。

- ◆ [173 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」](#)
- ◆ [174 ページの「iManager セルフサービスコンソールまたは Novell Client によるパスワードの変更」](#)
- ◆ [175 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」](#)
- ◆ [176 ページの「レプリカの計画と Password Policy \(パスワードポリシー\)」](#)
- ◆ [176 ページの「電子メール通知の設定」](#)

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

Password Policy (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れる必要があります。

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 (Identity Manager パスワード同期に必要です) を使用している場合は、ユニバーサルパスワードをサポートする新しい Novell Client を配布します。次にユーザが新しい Novell Client を使用してログインすると、クライアントは NDS パスワードがハッシュされる前にキャプチャし、ユニバーサルパスワードへの値の入力に使用します (103 ページの「ユーザのログインおよびパスワード変更方法の計画」を参照)。
- ◆ 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、企業ポータルです。

iManager セルフサービスコンソールまたは Novell Client によるパスワードの変更

ユーザが iManager、iManager のセルフサービスコンソール、および Novell Client でパスワードを変更する場合、Password Policy (パスワードポリシー) の Advanced Password Rule (詳細パスワードルール) が表示されます。このため、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、その変更が Identity Manager および他の接続システムと同期化されます。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、Advanced Password Rule (詳細パスワードルール) が表示されません。

Advanced Password Rule (詳細パスワードルール) 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 の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、Advanced Password Rule (詳細パスワードルール) をユーザに周知徹底させます。

接続システムでは、ユーザは Password Policy (パスワードポリシー) のルールを参照せずにパスワードを変更できるので、ルールを正しく思い出せ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 Password Policy (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 eDirectory に同期化されません。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化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、接続システムで選択した新しいパスワードで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。

ユニバーサルパスワードを使用するための準備作業

必要な情報のほとんどは、『[Novell Modular Authentication Services \(NMAS\) 2.3 Administration Guide \(Novell Modular Authentication Services \(NMAS\) 2.3 管理ガイド\)](http://www.novell.com/documentation/nmas23/index.html) (<http://www.novell.com/documentation/nmas23/index.html>)』の「Deploying Universal Password (ユニバーサルパスワードの展開)」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。NetWare のマニュアルではこの点が更新されています。
- ◆ Identity Manager パスワード同期は、ユニバーサルパスワードと、別の種類のパスワードである配布パスワードの両方に基づきます。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ときに使用するリポジトリです。ユニバーサルパスワードと同様、ポリシーは配布パスワードにも適用できます。
- ◆ Identity Manager に付属の DirXML iManager プラグインには、Password Policy (パスワードポリシー) を作成するための新しい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により、ユニバーサルパスワードを NDS パスワード、通常パスワード、および配布パスワードに同期化する方法が決定されます。

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。7 章 95 ページの、「[Password Policy \(パスワードポリシー\) を使用したパスワードの管理](#)」を参照してください。

- ◆ 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。ただし、パスワード同期化機能のサブセットでは eDirectory 8.6.2 がサポートされているので、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には、他のツリーとして使用できます。
- ◆ 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識別ボールドとして作成することです。多くの環境ではすでに DirXML およびドライバのために、識別ボールドを使用しています。
- ◆ ユニバーサルパスワードは、Password Policy (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なかった新し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。103 ページの「[ユーザのログインおよびパスワード変更方法の計画](#)」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 Password Policy (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、Password Policy (パスワードポリシー) で作成した Advanced Password Rule (詳細パスワードルール) は表示されません。現時点では、Novell Client でも Advanced Password Rule は表示されませんが、Novell Client では Advanced Password Rule は適用されます。

代わりに、パスワードの変更は iManager の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、Password Policy (パスワードポリシー) 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のユーザに徹底します。
- ◆ 管理者およびヘルプデスクのユーザが、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を理解するようにしてください。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。それにより、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、すなわち「パスワードドリフト」が回避されます。

『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Novell Modular Authentication Services (NMAS) 2.3 管理ガイド)* (<http://www.novell.com/documentation/nmas23/index.html>)』には、ユーティリティとそのユニバーサルパスワードのサポート状況のリストが表示されている TID (Technical Information Document) が記載されています。

レプリカの計画と Password Policy (パスワードポリシー)

Password Policy (パスワードポリシー) はツリー中心で割り当てられます。対照的に、パスワード同期はドライブごとに設定されます。ドライブはサーバベースでインストールされ、マスタレプリカまたは読み書き可能レプリカ内に存在するユーザのみを管理できます。パスワードの同期化により期待される結果を取得するには、パスワードの同期化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 Password Policy (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 Password Policy (パスワードポリシー) が割り当てられます。

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] タスク作業を使用し、電子メールサーバを設定する
- ◆ 必要に応じて、iManager の [Notification Configuration] 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
- ◆ eDirectory ユーザが Internet EMail Address 属性に入力済みであることを確認する

220 ページの「電子メール通知の設定」の指示に従います。

新しいドライブ設定と Identity Manager パスワード同期

現在の環境で Password Synchronization 1.0 を使用しておらず、新しいドライブを作成するか、または既存の設定を新しい Identity Manager の設定に置き換える場合は、次の指示に従い、Identity Manager パスワード同期の機能を設定します。

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

- 2 新しいドライバを作成するか、既存のドライバの設定を Identity Manager 2 の設定に置き換えます。

Identity Manager の設定には、ポリシーおよび Identity Manager パスワード同期に必要なその他の項目が含まれます。新しいドライバ設定のサンプルのインポートについては、個々の [rXML ドライバガイド \(http://www.novell.com/documentation/beta/dirxmldrivers\)](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 Password Policy (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。

110 ページの「Password Policy (パスワードポリシー) の作成」を参照してください。以前に NetWare 6.5 でユニバーサルパスワードを使用していた場合は、**108 ページの「(NetWare 6.5 のみ) ユニバーサルパスワード割り当ての再作成」**に説明されているいくつかの手順が追加が必要です。

Password Policy (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。

[Password Policy] の [Universal Password] > [Configuration Options] では、NMAS で異なる種類のパスワードの同期を保つ方法のオプションを指定できます。

パスワード同期を使用シナリオの例、および Password Policy (パスワードポリシー) の一致の方法については、**184 ページの「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、[DirXML Drivers \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](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 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。

5a iManager で、[Password Management] > [Password Synchronization] 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、グローバル設定値 (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。
- ◆ Identity Manager が直接アップデートするパスワードは、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であるか。Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager が更新するかを制御します。NMAS は、Password Policy (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。この設定を行うには、[Universal Password] > [Configuration Options] の順に選択します。
- ◆ Identity Manager に入力されるパスワードの変更に、ユーザの Password Policy (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。

これらのオプションの画面表示については、[184 ページの「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。

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 にパスワードを発行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、[184 ページの「パスワード同期の実装」](#)を参照してください。

Password Synchronization 1.0 から Identity Manager パスワード同期へのアップグレード

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 DirXML 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、[DirXML Drivers \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](http://www.novell.com/documentation/lg/dirxmldrivers/index.html)にある Active Directory および NT ドメイン用 DirXML ドライバのドライバ実装ガイドを参照してください。

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

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

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 DirXML ドライバをアップグレードする場合は、[DirXML Drivers \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](http://www.novell.com/documentation/lg/dirxmldrivers/index.html)にある、Active Directory および NT ドメイン用 DirXML 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う必要があります。

注： 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化するために eDirectory ドライバを使用している場合には、これらのポリシーは eDirectory ドライバの設定に使用できません。[185 ページの「シナリオ 1 - NDS パスワードを使用した eDirectory 間でのパスワード同期化」](#)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、Public Key および Private Key の属性を使用して、同期化されます。

ここで説明する手順を使用して実行する作業の概要を次に示します。

- ◆ Identity Manager 2 の形式に、ドライバを変換します。
- ◆ ドライバマニフェスト、GCV、およびパスワード同期のポリシーをドライバ設定に追加します。追加するポリシーのリストについては、[166 ページの「ドライバ設定に必要なポリシー」](#)を参照してください。
- ◆ nspmDistributionPassword 属性のフィルタ設定を変更します。
- ◆ パスワード同期のフローを設定します。

前提条件

- ❑ Export Drivers Wizard 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。[Check Password Status] 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 DirXML 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。DirXML Drivers (<http://www.novell.com/documentation/lg/dirxmldrivers/index.html>) にある Active Directory および NT ドメイン用 DirXML 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。

手順

- 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。173 ページの「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。
- 2 ウィザードに従い、Identity Manager の形式にドライバを変換します。79 ページの「DirXML 1.x から Identity Manager 形式へのドライバ設定のアップグレード」を参照してください。
- 3 iManager で、[DirXML Utilities] > [Import Drivers] の順にクリックします。
「オーバーレイ」設定ファイルをインポートしてポリシー、ドライバマニフェスト、および GCV を一度に追加することで、パスワード同期の対象とする各ドライバに Identity Manager パスワード同期のサポートを追加します。

サポートを追加した後、nspmDistributionPassword 属性もフィルタに追加する必要があります。

これらの作業については、後の手順で説明します。
- 4 既存のドライバの存在するドライバセットを選択します。
- 5 表示されるドライバ設定のリストから、[Password Synchronization 2.0 Policies] というラベルの付いた項目のみを選択します。このリストは [Additional Policies] の下にあります。[Next] をクリックします。

インポートプロンプトのリストが表示されます。
- 6 アップデートする既存のドライバを選択します。
- 7 ドロップダウンリストからドライバのタイプを選択します。

ドライバのタイプに基づき、Import Driver Wizard は、ドライバ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 DirXML ドライバシム、およびドライバ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 [Next] をクリックします。ドライバについてのすべてをアップデートするよう選択します。

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、およびポリシーを指定します。

ドライバマニフェストおよび GCV は、既存の値を上書きしますが、これらのドライバパラメータは Identity Manager 2 の新しいパラメータです。このため、DirXML 1.x ドライバについては、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： 保存したいドライバマニフェストまたは GCV がいない場合、ドライバの [Update Only Selected Policies] という名前のオプションを選択し、ポリシーすべてのチェックボックスをオンにします。このオプションは、Password Policy (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。



- 9 [Next] をクリックし、[Finish] 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、ドライバ設定の一部にはなっていません。設定にリンクさせるには、発行者および加入者チャンネルのドライバ設定右側のポイントに、各ポリシーを手動で挿入する必要があります。

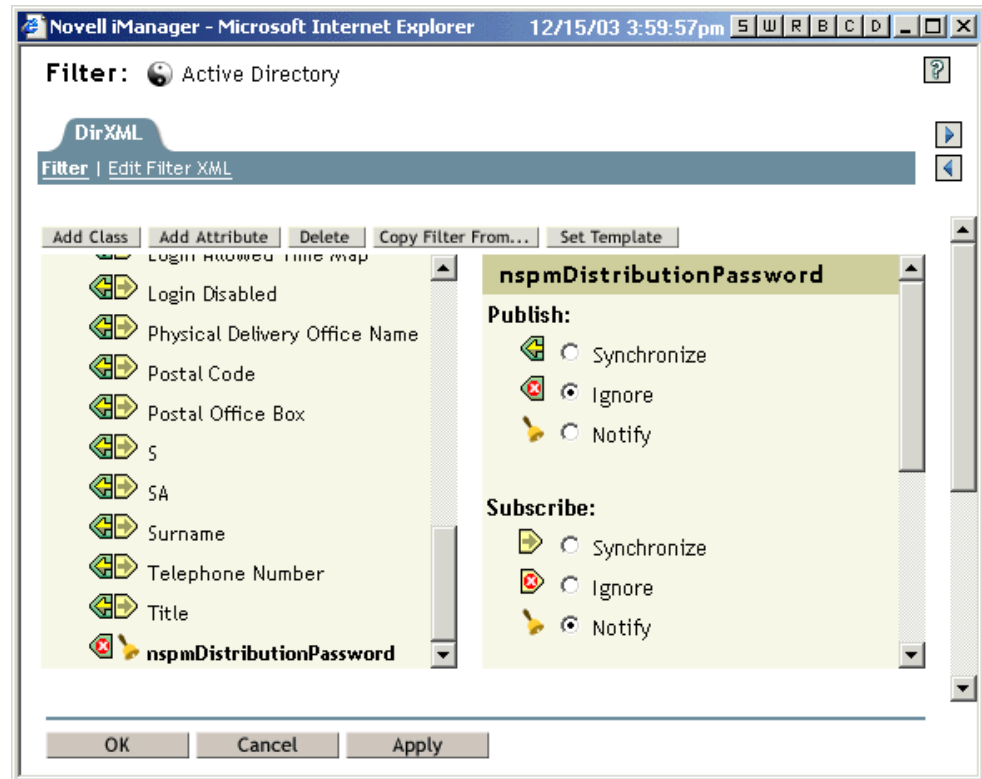
- 10 新しい各ポリシーを既存のドライバ設定の正しい場所に挿入します。ポリシーセットに複数のポリシーがある場合には、パスワード同期のポリシーが最後のリストとなるように挿入します。

ポリシーのリストおよび挿入する場所については、[166 ページの「ドライバ設定で必要なポリシー」](#)を参照してください。

ポリシーごとに、次の手順を繰り返します。

- 10a [DirXML Management] > [Overview] の順にクリックします。アップデートするドライバのドライバセットを選択します。
- 10b アップデートしたドライバをクリックします。ドライバ設定のグラフィック画面のページが開きます。
- 10c 新しいポリシーのいずれかを追加する必要がある場所のアイコンをクリックします。
- 10d [Insert] をクリックし、新しいポリシーを追加します。表示される [Insert] ページで、[Use an Existing Policy] をクリックし、新しいポリシーオブジェクトを参照します。[OK] をクリックします。
- 10e 新しいポリシーのどれかに対応するポリシーがリスト内に複数ある場合は、矢印ボタン  を使用し、新しいポリシーをリストの正しい位置に移動します。[166 ページの「ドライバ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。

- 11 パスワードを同期化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。
- ◆ 発行者チャンネルについては、フィルタが nspmDistributionPassword 属性を無視するよう設定します。
 - ◆ 加入者チャンネルについては、フィルタが nspmDistributionPassword 属性を通知するよう設定します。



- 12 nspmDistributionPassword 属性の [Notify] が設定されているすべてのオブジェクトに対しては、ドライバフィルタの Public Key および Private Key の属性は無視します。



- 13 パスワード同期の対象とするためにアップデートするドライバすべてに対して、**ステップ 2** から**ステップ 12** 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。

- 14 Identity Manager パスワード同期の設定に必要な追加の手順または情報がないか、ドライバ実装ガイドを [DirXML Drivers \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](http://www.novell.com/documentation/lg/dirxmldrivers/index.html) で確認します。
- 15 ユニバーサルパスワードが有効な Password Policy (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。

110 ページの「**Password Policy (パスワードポリシー) の作成**」を参照してください。以前に NetWare 6.5 でユニバーサルパスワードを使用していた場合は、**108 ページ**の「**(NetWare 6.5 のみ) ユニバーサルパスワード割り当ての再作成**」に説明されているいくつかの手順が追加が必要です。

Password Policy (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。

[Password Policy] の [Universal Password] > [Configuration Options] では、NMAS で異なる種類のパスワードの同期を保つ方法のオプションを指定できます。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、該当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シナリオの例、および Password Policy（パスワードポリシー）の一致の方法については、[184 ページの「パスワード同期の実装」](#)を参照してください。

Password Policy（パスワードポリシー）はツリー中心で割り当てられます。対照的に、パスワード同期はドライバごとに設定されます。ドライバはサーバベースでインストールされ、マスタレプリカまたは読み書き可能レプリカ内に存在するユーザのみを管理できます。パスワードの同期化により期待される結果を取得するには、パスワードの同期化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 Password Policy（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 Password Policy（パスワードポリシー）が割り当てられます。

16 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。

16a iManager で、[Password Management] > [Password Synchronization] 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。

16b パスワードフローの現在の設定を表示します。これは、グローバル設定値 (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。
- ◆ Identity Manager が直接アップデートするパスワードは、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であるか。Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager が更新するかを制御します。NMAS は、Password Policy（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。この設定を行うには、[Universal Password] > [Configuration Options] の順に選択します。
- ◆ Identity Manager に入力されるパスワードの変更に、ユーザの Password Policy（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 Password Policy（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。

これらのオプションの画面表示については、[184 ページの「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。

17 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、[184 ページの「パスワード同期の実装」](#)を参照してください。

パスワード同期の実装

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、いくつかの基本シナリオについて説明し、パスワード同期と Password Policy（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。

この節では、次の項目について説明します。

- ◆ 184 ページの「Identity Manager と NMAS の関係の概要」
- ◆ 185 ページの「シナリオ1 - NDSパスワードを使用したeDirectory間でのパスワード同期化」
- ◆ 188 ページの「シナリオ2 - ユニバーサルパスワードの同期」
- ◆ 197 ページの「シナリオ3 - Identity Manager での配布パスワードのアップデートによる、eDirectory および接続システムの同期化」
- ◆ 207 ページの「シナリオ4 - トンネリング & Identity Manager での配布パスワードのアップデートによる、eDirectory ではなく接続システムの同期化」
- ◆ 213 ページの「シナリオ5 - アプリケーションのパスワードの通常パスワードへの同期化」

Identity Manager と NMAS の関係の概要

この節では、次の項目について説明します。

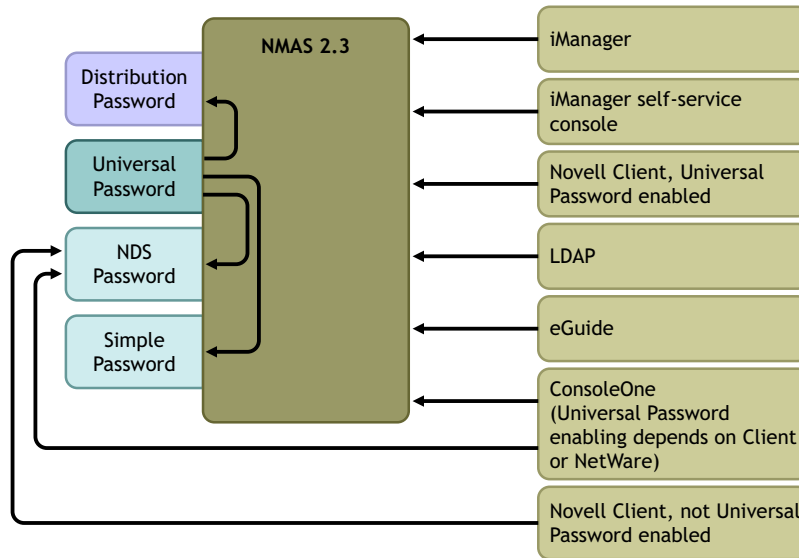
- ◆ 184 ページの「ユーティリティと NMAS」
- ◆ 185 ページの「Identity Manager と NMAS」

ユーティリティと NMAS

iManager、Novell Client などの最新のユーティリティは、特定のパスワードを直接アップデートするのではなく、NMAS と通信し、NMAS がどのパスワードをアップデートするかを決定するエンティティになります。

NMAS は Password Policy（パスワードポリシー）の設定に基づき、パスワードを eDirectory 内で同期化します。

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 パスワードを直接アップデートします。NMAS と通信し、NMAS がどのパスワードをアップデートするかを決定するではありません。現在の環境で、ユーザおよびヘルプデスクがどのようにレガシーユーティリティを使用しているかに注意してください。レガシーユーティリティは NMAS と通信するのではなく NDS パスワードを直接アップデートするため、ユニバーサルパスワードおよび 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 パスワードの同期がずれる問題）が発生することがあります。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。



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アップデートします）。NMAS は、eDirectory 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 DirXML ドライバを使用して、NDS パスワードを直接アップデートできます。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。

この節の後の方で説明する、**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どちらかがアップデートされ、Identity Manager は NMAS と通信してパスワードの変更を行います。これにより、NMAS は Password Policy（パスワードポリシー）の設定の決定に基づき他の eDirectory パスワードをアップデートし、パスワードが接続システムと同期化できるように、Password Policy（パスワードポリシー）から Advanced Password Rule（詳細パスワードルール）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。各シナリオ間の相違は、NMAS の Password Policy（パスワードポリシー）の設定、および接続システムの各ドライバについての Identity Manager パスワード同期の設定の組み合わせです。

シナリオ 1 - NDS パスワードを使用した eDirectory 間でのパスワード同期化

Password Synchronization 1.0 と同様に、eDirectory ドライバを使用して 2 つの eDirectory ツリー間で NDS パスワードを同期化できます。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なく、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化とも呼ばれます。

この方法は、eDirectory 間でパスワードを同期化する場合にのみ使用してください。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。

この節では、次の項目について説明します。

- ◆ [186 ページの「シナリオ 1 の長所と短所」](#)
- ◆ [186 ページの「シナリオ 1 の図」](#)

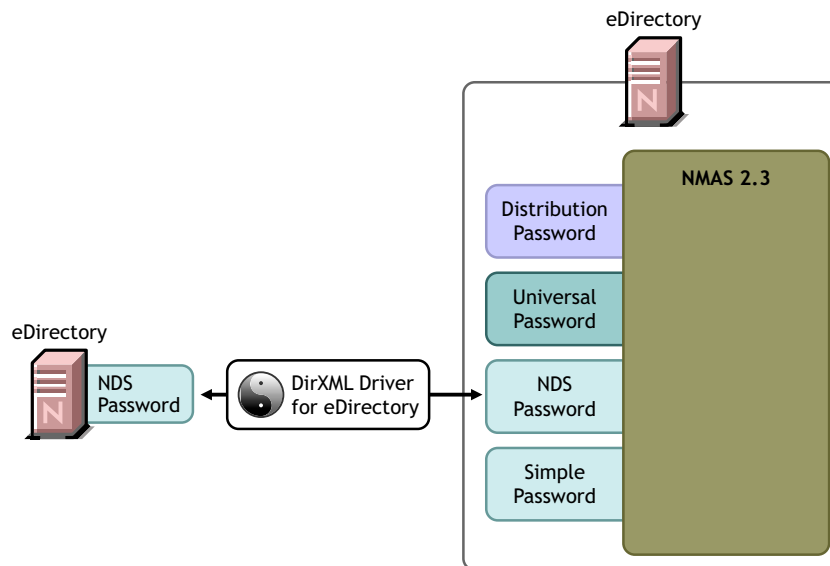
- ◆ 187 ページの「シナリオ 1 の設定」
- ◆ 188 ページの「シナリオ 1 のトラブルシューティング」

シナリオ 1 の長所と短所

長所	短所
<p>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。</p> <p>各ステージで Identity Manager 2 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。</p> <ul style="list-style-type: none"> ◆ 新しいパスワード同期のポリシーをドライバ設定に追加する必要がない。 ◆ ユニバーサルパスワードを Identity Manager 2 ツリー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ツリーで使用できる。 ◆ NMAS 2.3 は必要ない。 <p>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。</p>	<p>この方法は、eDirectory ツリー間でパスワードを同期化しません。他の接続システムとパスワードを同期化することはできません。</p> <p>ユニバーサルパスワードまたは配布パスワードはアップデートされません。</p> <p>NMAS を使用しないので、別のツリーからのパスワードに対して設定した Password Policy (パスワードポリシー) の Advanced Password Rule (詳細パスワードルール) との照合によってパスワードを検証できません。</p> <p>NMAS を使用しないので、パスワードが Password Policy (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 eDirectory ツリーでパスワードをリセットできません。</p> <p>パスワード同期化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。</p> <p>iManager のタスクからの [Check Password Status] 操作はサポートされません (この機能には配布パスワードが必要です)。</p>

シナリオ 1 の図

次の図は、DirXML 1.x と同様、eDirectory の DirXML ドライバを使用して 2 つの eDirectory ツリー間で NDS パスワードを同期化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。



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

ユニバーサルパスワードの展開

必要ありません。

Password Policy（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 [Password Synchronization] 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。

ドライバ設定

166 ページの「ドライバ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、Public Key および Private Key の属性を使用して、同期化されます。

両方の eDirectory ドライバのフィルタによって、パスワードを同期化するすべてのオブジェクトクラスの Public Key および Private Key の属性が同期化されていることを確認します。次の図は、例を示します。



シナリオ1のトラブルシューティング

- ◆ [DXML 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、Public Key と Private Key の属性が同期化されており、無視されていないことを確認します。
- ◆ [234 ページの「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 - ユニバーサルパスワードの同期

Identity Manager では、接続システムのパスワードを eDirectory のユニバーサルパスワードに同期化できます。

ユニバーサルパスワードがアップデートされると、Password Policy (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、または通常パスワードもアップデートできます。

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 からのパスワードの変更を購読できるわけではありません。[159 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。

この節では、次の項目について説明します。

- ◆ [189 ページの「シナリオ2の長所と短所」](#)
- ◆ [189 ページの「シナリオ2の図」](#)
- ◆ [190 ページの「シナリオ2の設定」](#)
- ◆ [195 ページの「シナリオ2のトラブルシューティング」](#)

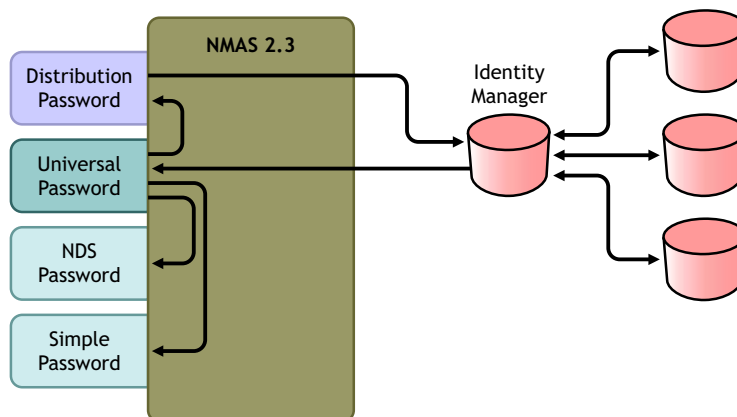
シナリオ 2 の長所と短所

長所	短所
<p>eDirectory および接続システム間でパスワードを同期化できます。</p> <p>パスワードを NMAS Password Policy（パスワードポリシー）と照合して検証できます。</p> <p>接続システムから受信したパスワードが Password Policy（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。</p> <p>ユニバーサルパスワードが配布パスワードと同期化され、接続システムがパスワードのチェックをサポートする場合、iManager の [Check Password Status] タスクをサポートします。</p> <p>NMAS は、ルールが有効な場合、Password Policy（パスワードポリシー）の Advanced Password Rule（詳細パスワードルール）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。</p> <p>Password Policy（パスワードポリシー）のルールを適用しない場合は、[Enable Advanced Password Rules in the Password Policy] チェックボックスをオフにできます。</p>	<p>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。Password Policy（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。</p>

シナリオ 2 の図

次の図は、Identity Manager を通じてパスワードが送られ、Identity Manager がユニバーサルパスワードを直接アップデートするために NMAS と通信することを示します。NMAS は、ユニバーサルパスワードを、配布パスワードおよび Password Policy（パスワードポリシー）設定に従って、その他のパスワードに同期化します。最後に、Identity Manager は配布パスワードを取得し、パスワードを受け入れるよう設定されている接続システムに配布します。

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、設定は接続システムのドライバごとに作成することに注意してください。



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

- ◆ 190 ページの「ユニバーサルパスワードの展開」
- ◆ 190 ページの「Password Policy（パスワードポリシー）の設定」
- ◆ 192 ページの「パスワード同期の設定」
- ◆ 193 ページの「ドライバ設定」

ユニバーサルパスワードの展開

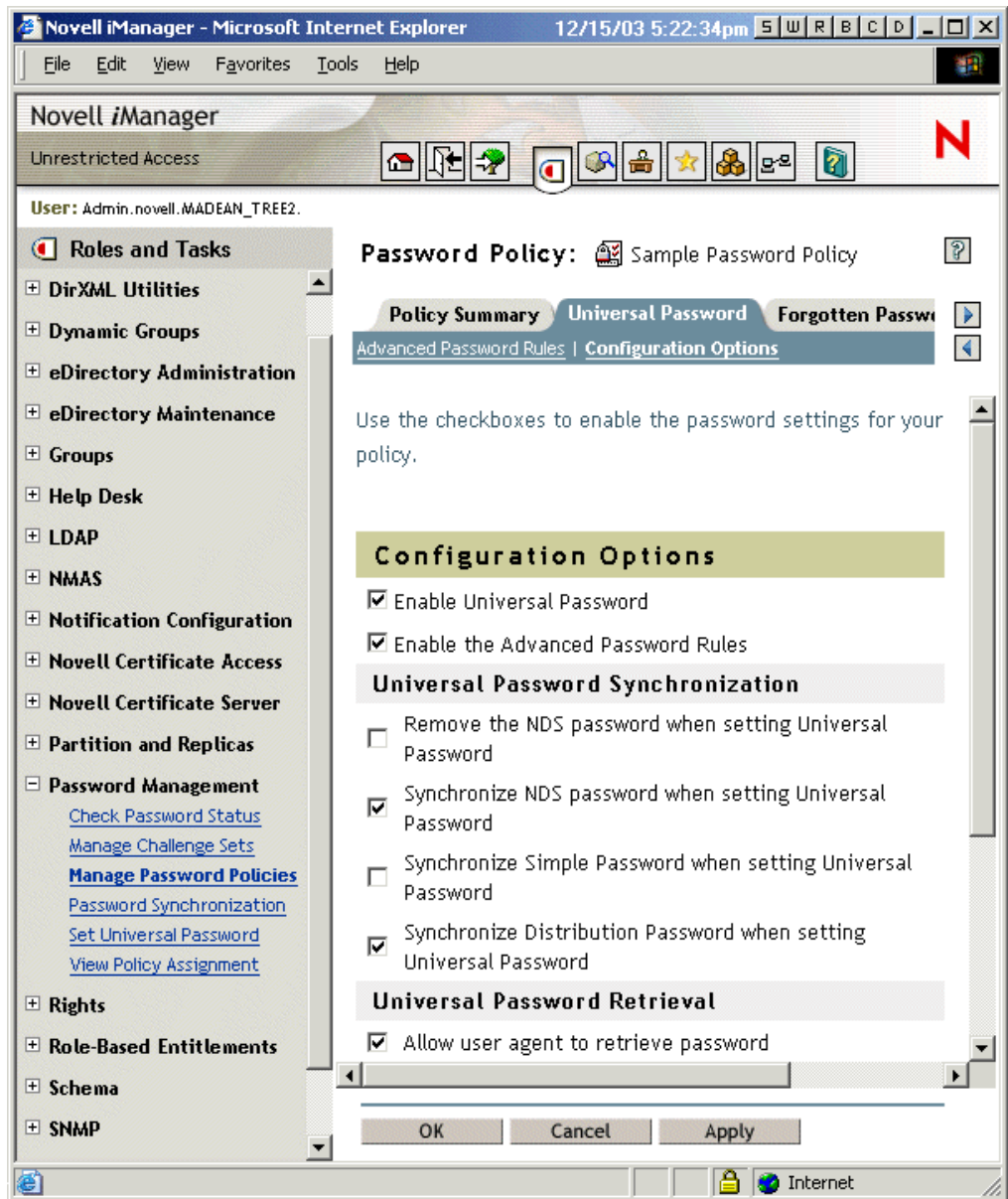
現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。[173 ページの「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」](#)を参照してください。

Password Policy（パスワードポリシー）の設定

[Password Management] > [Manage Password Policies] の順に選択して、次を実行します。

- 1 この種類のパスワード同期を行う eDirectory ツリーの一部に Password Policy（パスワードポリシー）が割り当てられていることを確認します。Password Policy（パスワードポリシー）は、ツリー全体（ログインポリシーオブジェクトを使用）、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。管理を簡素化するために、Password Policy（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ておくことをお勧めします。
- 2 [Password Policy] で、次のオプションが選択されていることを確認します。
 - ◆ Enable Universal Password
 - ◆ Synchronize NDS Password when Setting Universal Password
 - ◆ Synchronize Distribution Password when Setting Universal Password

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。



3 必要に応じ、[Password Policy] 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、Password Policy（パスワードポリシー）の Advanced Password Rule（詳細パスワードルール）を適用します。Password Policy（パスワードポリシー）のルールを適用しない場合は、[Enable Advanced Password Rules] チェックボックスをオフにします。

4 Advanced Password Rule（詳細パスワードルール）を使用している場合、パスワードを購読している接続システムの Password Policy（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

[Password Management] > [Password Synchronization] の順に選択し、接続システムのドライバの設定を行います。

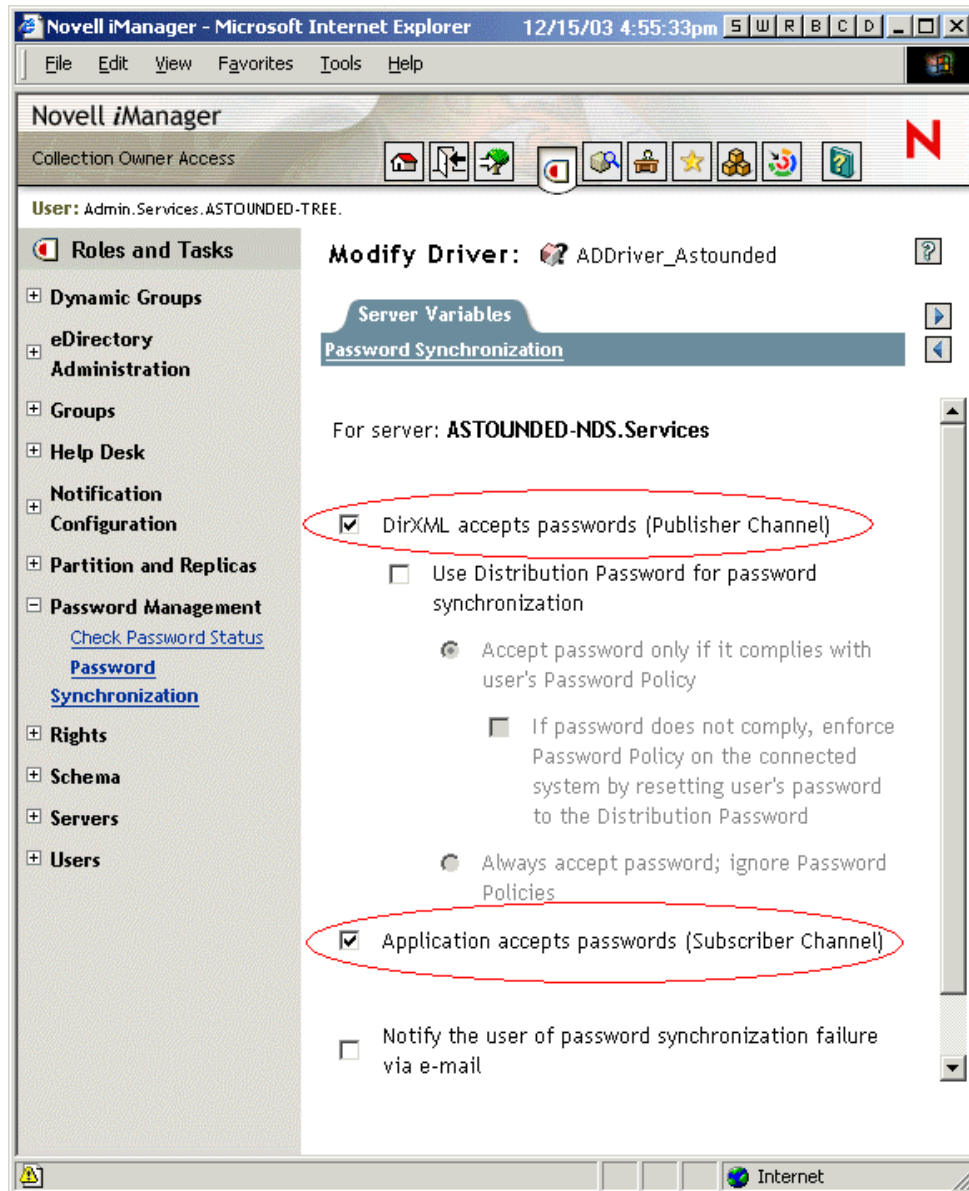
1 次のオプションが選択されていることを確認します。

- ◆ DirXML accepts passwords (Publisher Channel)

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。

- ◆ Application accepts passwords (Subscriber Channel)

接続システム j 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。

パスワードの承認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購読するが発行しないようにする場合は、[Application accepts passwords (Subscriber Channel)]のみを選択します。

2 次のオプションがオフになっていることを確認します。

- ◆ Use Distribution Password for Password Synchronization

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アップデートします。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アップデートされます。

3 (オプション) 必要に応じ、次のオプションを選択します。

- ◆ Notify the User of Password Synchronization Failure via E-mail

電子メール通知には、eDirectory ユーザオブジェクトの Internet EMail Address 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。電子メール通知は、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を与えず、失敗した場合でも、操作自体が再試行されない限り、電子メール通知が再試行されることはありません。

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。

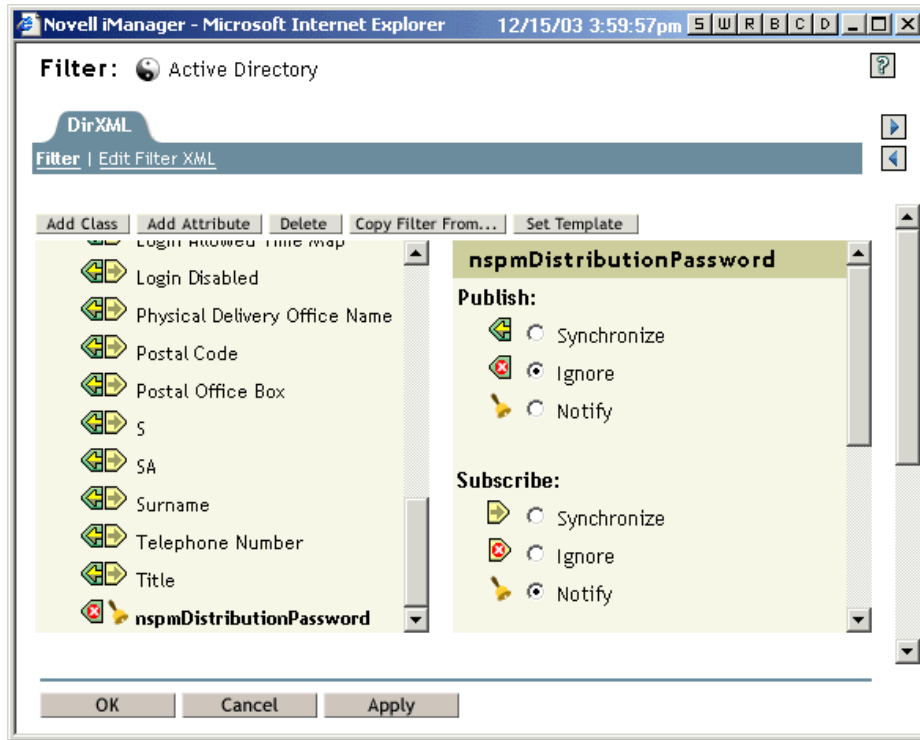
ドライバ設定

1 必要な Identity Manager スクリプトパスワード同期化ポリシーが、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、166 ページの「ドライバ設定に必要なポリシー」を参照してください。

Identity Manager のサンプル設定には、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デートする場合は、178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」の手順を使用してポリシーを追加できます。

2 nspmDistributionPassword 属性のために、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、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。
- ◆ 加入者チャネルについては、フィルタが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 属性について [Notify] と設定したすべてのオブジェクトの、ドライバフィルタの Public Key および Private Key の属性は無視します。



- 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

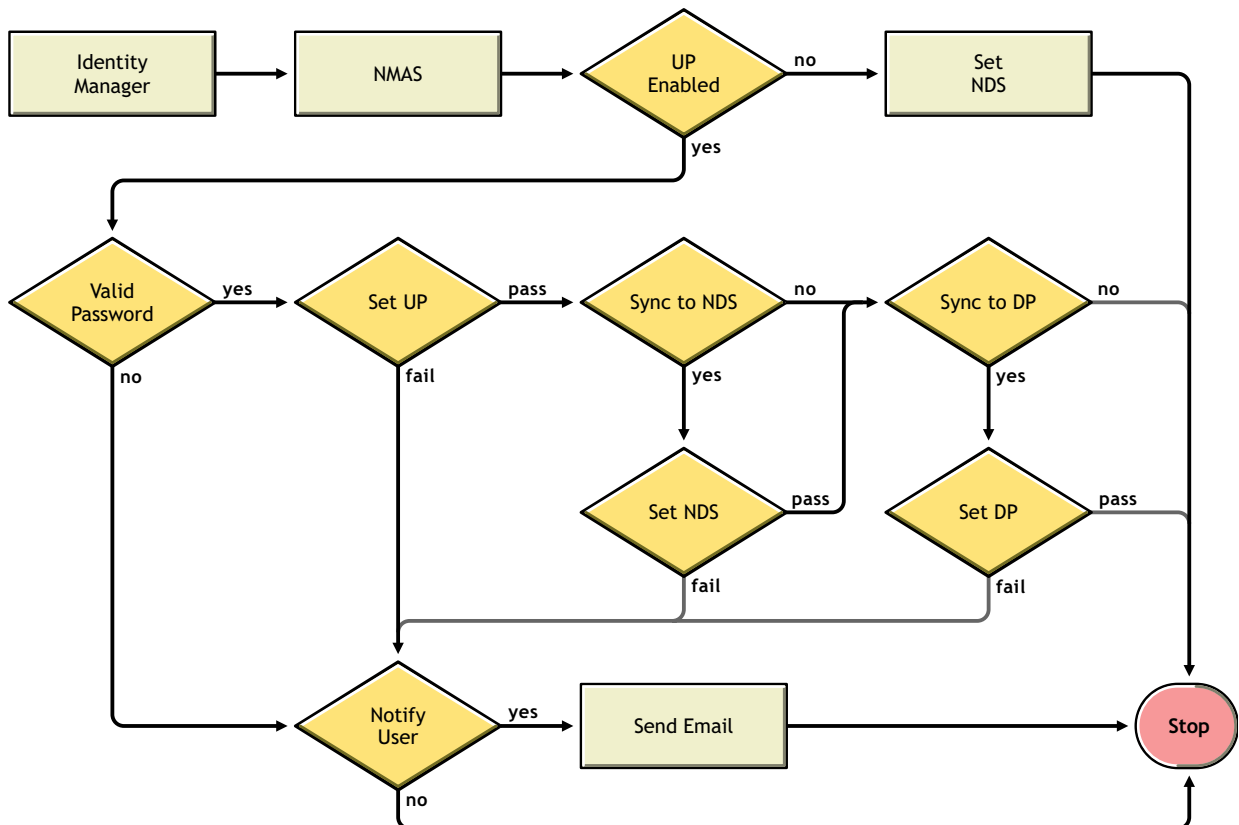
この節では、次の項目について説明します。

- ◆ 195 ページの「シナリオ2のフローチャート」
- ◆ 196 ページの「eDirectoryへのログインのトラブルシューティング」
- ◆ 196 ページの「パスワードを購読する別の接続システムへのログインに関するトラブルシューティング」
- ◆ 196 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」
- ◆ 197 ページの「[Check the Object Password]を使用した場合のエラー」
- ◆ 197 ページの「DSTraceの便利なコマンド」

234 ページの「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ます。このシナリオでは、パスワードはユニバーサルパスワードに同期化されます。ユニバーサルパスワードがPassword Policy（パスワードポリシー）で有効になっているか、送られるパスワードがAdvanced Password Rule（詳細パスワードルール）に準拠することが有効になっているか、およびPassword Policy（パスワードポリシー）にユニバーサルパスワードと他のパスワード同期のためのその他の設定があるかに基づき、パスワードの処理の方法をNMASが決定します。



eDirectory へのログインのトラブルシューティング

- ◆ [DSTrace] の [+AUTH]、[+DCLN]、[+DXML]、および [+DVRS] の設定をオンにします。
- ◆ <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。
- ◆ Password Policy (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 Password Policy (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 [Password Synchronization] ページで、[DirXML accepts passwords] が選択されていることを確認します。
- ◆ [Password Policy] で、[Synchronize Distribution Password when Setting Universal Password] が選択されていることを確認します。

パスワードを購読する別の接続システムへのログインに関する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、そのパスワードを購読するもう 1 つの接続システムが発行するシステムからの変更を購読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受信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 DirXML のトレースレベルを 3 に設定します。
- ◆ [Password Synchronization] の [DirXML accepts passwords] 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、[193 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> (追加の場合) 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。
- ◆ DirXML Script の Password Policy (パスワードポリシー) が、[166 ページの「ドライバ設定で必要なポリシー」](#) で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。
- ◆ eDirectory の Password Policy (パスワードポリシー) と、接続システムにより適用される Password Policy (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、DirXML のルール処理を確認します。
- ◆ ドライバの DirXML 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。
- ◆ eDirectory オ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 Internet EMail Address 属性に含まれていることを確認します。
- ◆ [Notification Configuration] 作業で、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。[220 ページの「電子メール通知の設定」](#) を参照してください。

[Check the Object Password] を使用した場合のエラー

iManager の [Check Password Status] タスクにより、実行する [Check Object Password] アクションがドライバに与えられます。問題が発生した場合は、次を確認します。

- ◆ [Check Object Password] が -603 を返す場合、eDirectory オブジェクトに nspmDistributionPassword 属性が含まれていません。ドライバフィルタの nspmDistributionPassword 属性が正しく設定されていることを確認し、[Password Policy has Synchronize Distribution Password when Setting Universal Password] が選択されていることを確認します。
- ◆ [Check Object Password] が 「Not Synchronized」 を返す場合、ドライバ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。
- ◆ eDirectory の Password Policy (パスワードポリシー) と、接続システムにより適用される Password Policy (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。
- ◆ [Check Object Password] は、配布パスワードから操作します。配布パスワードがアップデートされていない場合、[Check Object Password] によって、パスワードが同期化されていることがレポートされないことがあります。
- ◆ eDirectory ドライバのみについては、[Check Password Status] は、配布パスワードではなく NDS パスワードをチェックすることに注意してください。

DSTrace の便利なコマンド

+DXML - DirXML 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 - DirXML ドライバ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

シナリオ 3 - Identity Manager での配布パスワードのアップデートによる、eDirectory および接続システムの同期化

この方法では、Identity Manager は配布パスワードを直接アップデートし、他の eDirectory パスワードをどのように同期化するかは 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 からのパスワードの変更を購読できるわけではありません。[159 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。

この節では、次の項目について説明します。

- ◆ [198 ページの「シナリオ 3 の長所と短所」](#)
- ◆ [198 ページの「シナリオ 3 の図」](#)
- ◆ [198 ページの「シナリオ 3 の設定」](#)
- ◆ [204 ページの「シナリオ 3 のトラブルシューティング」](#)

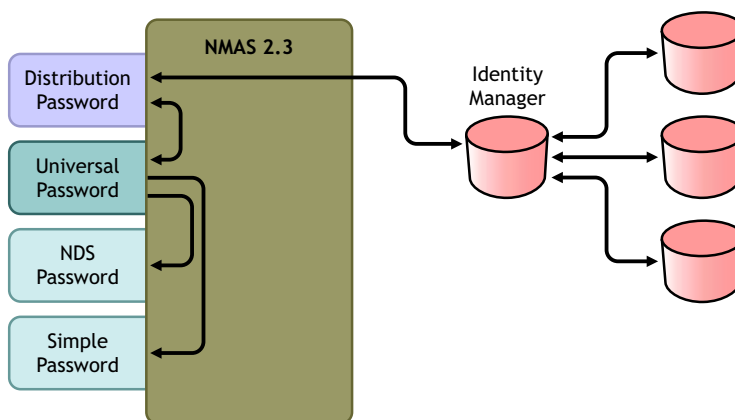
シナリオ 3 の長所と短所

長所	短所
eDirectory および接続システム間でパスワードを同期化できます。	
接続システムから受信したパスワードに対して、Password Policy（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。	
Password Policy（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 Password Policy 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。	

シナリオ 3 の図

次の図は、Identity Manager を通じてパスワードが送られ、Identity Manager が配布パスワードを直接アップデートするために NMAS と通信することを示します。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。NMAS は、ユニバーサルパスワードを、配布パスワード、および Password Policy（パスワードポリシー）設定に基づいてその他のパスワードに同期化します。

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、設定は接続システムのドライバごとに作成することに注意してください。



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

- ◆ 199 ページの「ユニバーサルパスワードの展開」
- ◆ 199 ページの「Password Policy（パスワードポリシー）の設定」
- ◆ 201 ページの「パスワード同期の設定」
- ◆ 202 ページの「ドライバ設定」

ユニバーサルパスワードの展開

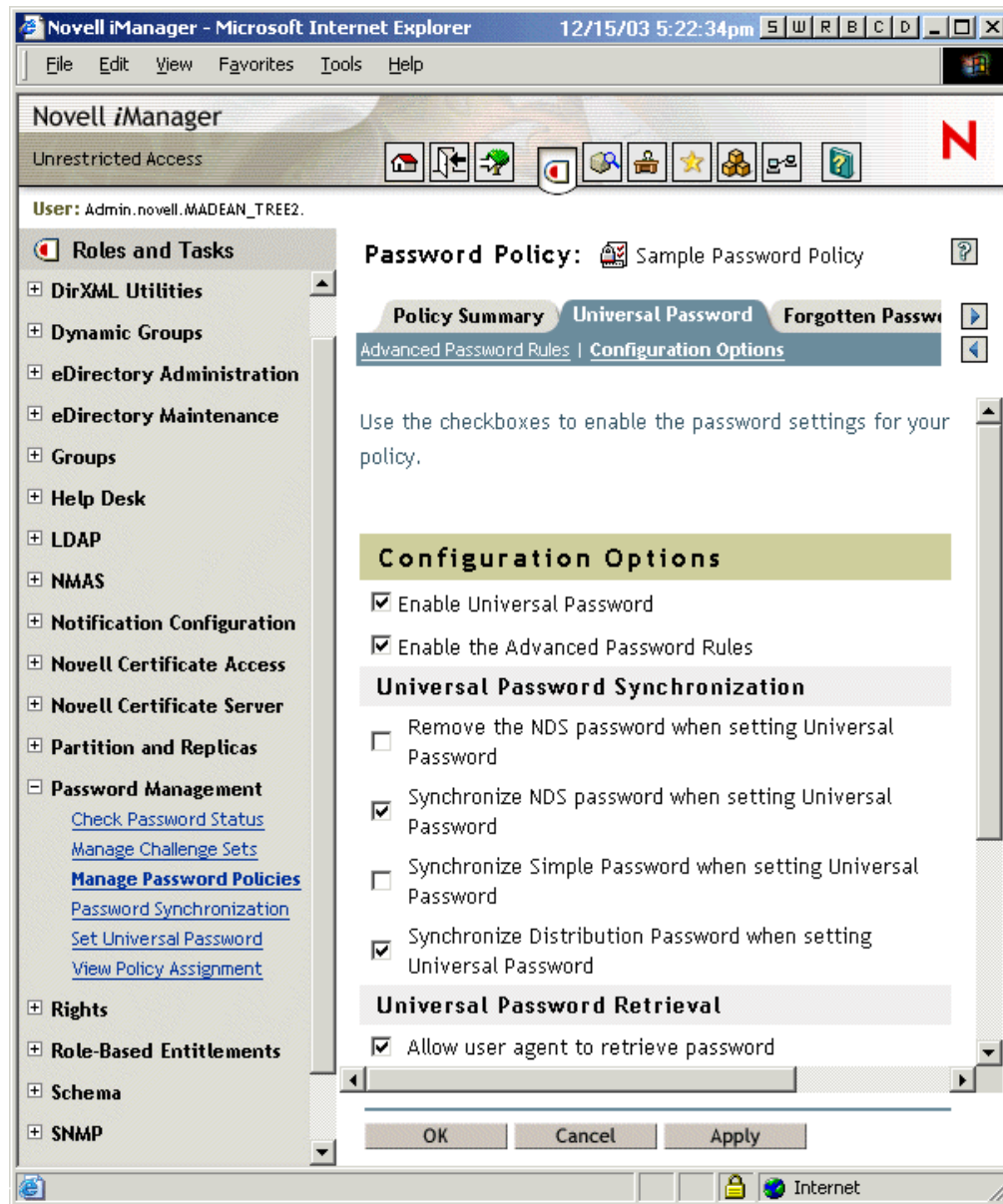
現在の環境でユニバーサルパスワードを使用する準備ができていないことを確認します。[173 ページの「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」](#)を参照してください。

Password Policy（パスワードポリシー）の設定

[Password Management] > [Manage Password Policies] で、次を実行します。

- 1 この種類のパスワード同期を行う eDirectory ツリーの一部に Password Policy（パスワードポリシー）が割り当てられていることを確認します。Password Policy（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、または特定のユーザに割り当てることができます。管理を簡素化するために、Password Policy（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ておくことをお勧めします。
- 2 [Password Policy] で、次のオプションが選択されていることを確認します。
 - ◆ Enable Universal Password
 - ◆ Synchronize NDS Password When Setting Universal Password
 - ◆ Synchronize Distribution Password When Setting Universal Password

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。



- 3 Advanced Password Rule（詳細パスワードルール）を使用している場合、パスワードを受信している接続システムの Password Policy（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

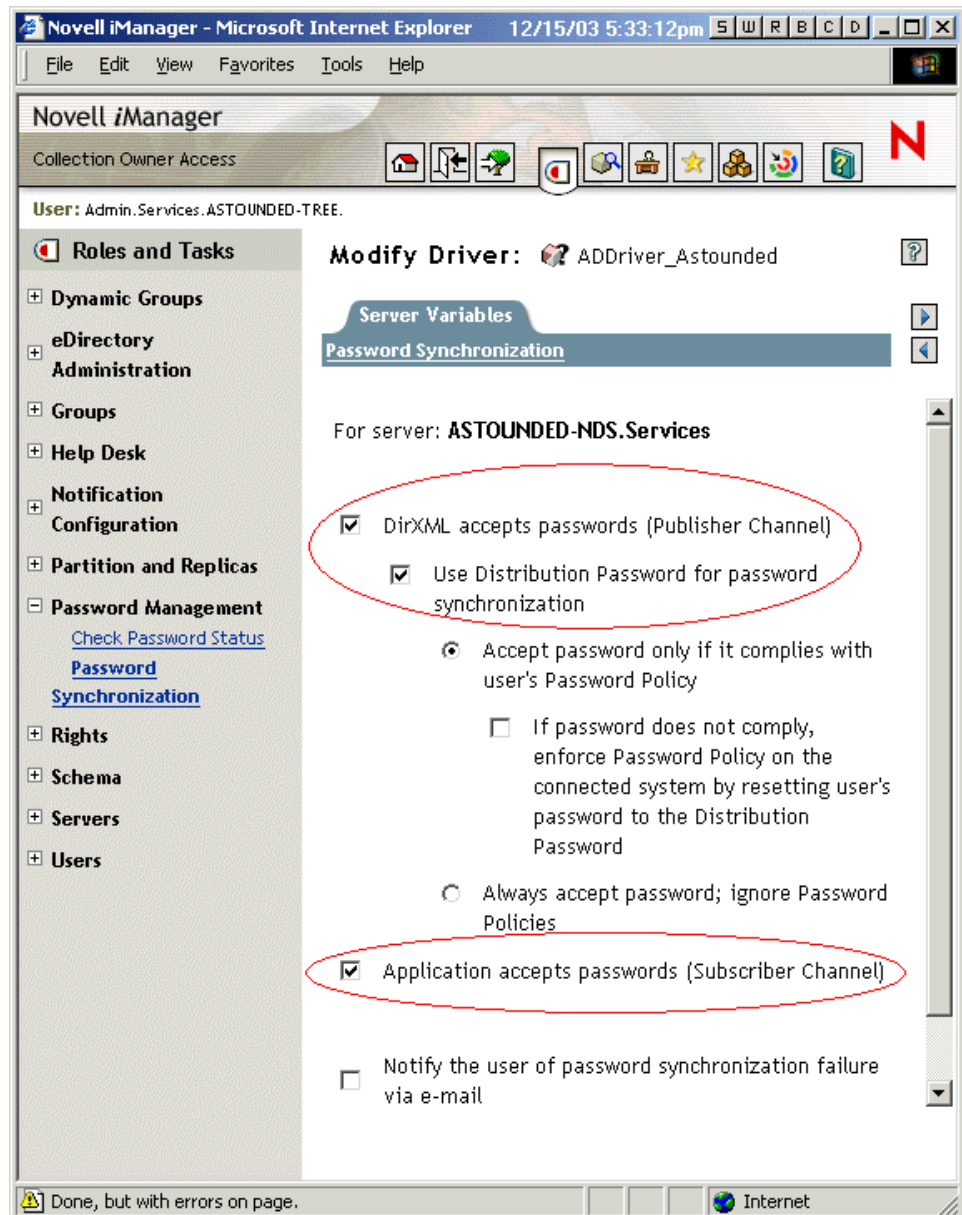
[Password Management] > [Password Synchronization] で、次の設定を使用します。

1 次のオプションが選択されていることを確認します。

- ◆ DirXML accepts Passwords (Publisher Channel)
 - ◆ Use Distribution Password for Password Synchronization

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。

- ◆ Application accepts passwords (Subscriber Channel)



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。

パスワードの承認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購読するが発行しないようにする場合は、[Application accepts passwords (Subscriber Channel)]のみを選択します。

- 2 [Use Distribution Password for password synchronization]のオプションを使用し、パスワード同期の Password Policy (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。
- 3 (オプション) Password Policy (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。
- 4 (オプション) 必要に応じ、次のオプションを選択します。

- ◆ Notify the User of Password Synchronization Failure via E-mail

電子メール通知には、eDirectory ユーザオブジェクトの Internet EMail Address 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。電子メール通知は、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を与えず、失敗した場合でも、操作自体が再試行されない限り、電子メール通知が再試行されることはありません。

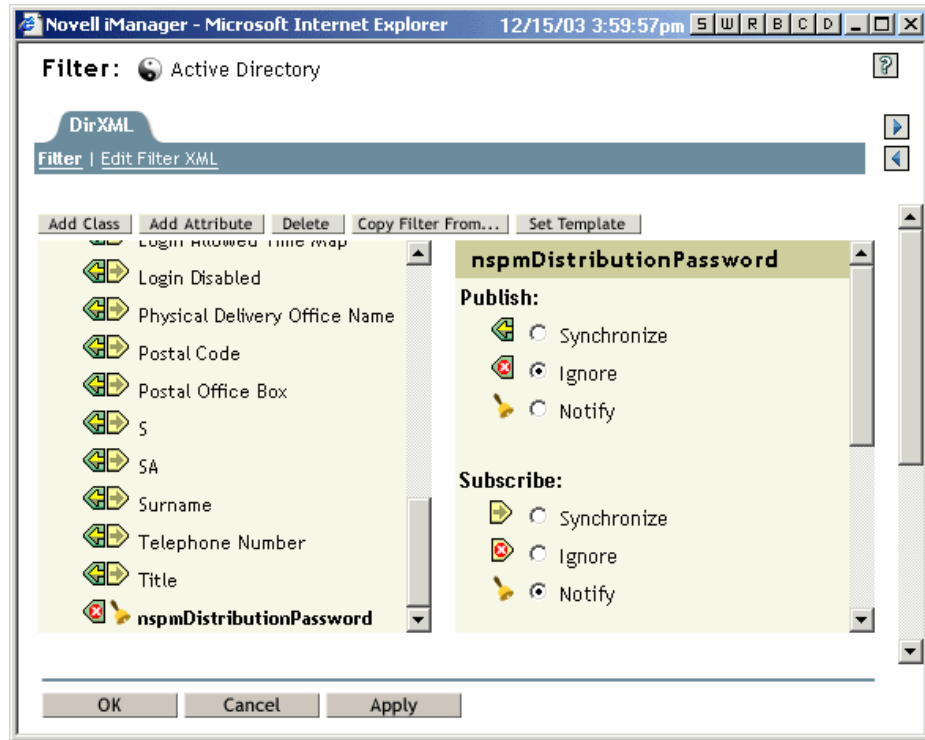
ただし、電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

ドライバ設定

- 1 必要な DirXML スクリプトパスワード同期化ポリシーが、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、[166 ページの「ドライバ設定に必要なポリシー」](#)を参照してください。

Identity Manager のサンプル設定には、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デートする場合は、[178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」](#)の手順を使用してポリシーを追加できます。

- 2 nspmDistributionPassword 属性のために、フィルタを正しく設定します。
 - ◆ 発行者チャンネルについては、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。
 - ◆ 加入者チャンネルについては、ドライバフィルタがすべてのオブジェクトクラスの nspmDistributionPassword 属性を通知するよう設定します。



- 3 nspmDistributionPassword 属性について [Notify] と設定したすべてのオブジェクトの、ドライバフィルタの Public Key および Private Key の属性は無視します。



- 4 パスワードのセキュリティを確保するには、DirXML 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

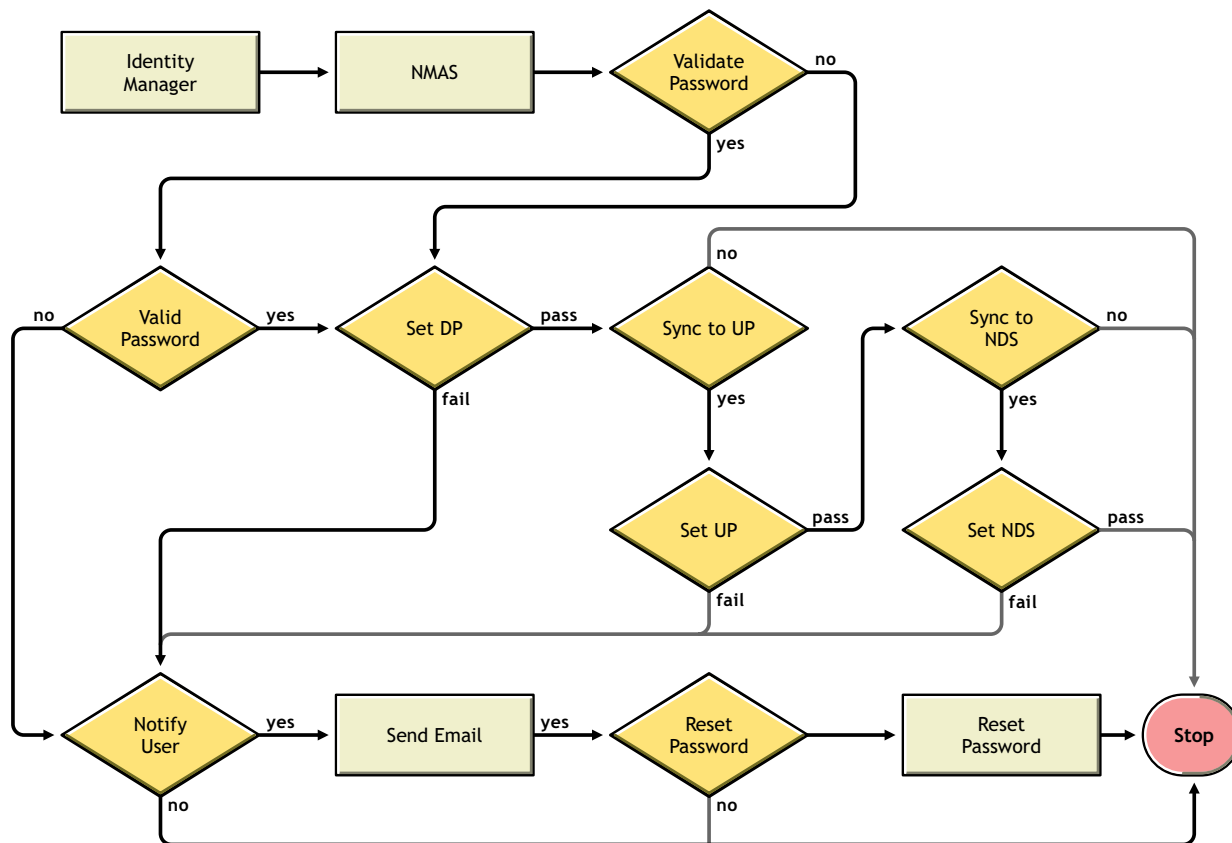
この節では、次の項目について説明します。

- ◆ 204 ページの「シナリオ3のフローチャート」
- ◆ 205 ページの「eDirectoryへのログインのトラブルシューティング」
- ◆ 205 ページの「パスワードを購読する別の接続システムへのログインに関するトラブルシューティング」
- ◆ 206 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」
- ◆ 206 ページの「[Check Password Status]を使用した場合のエラー」
- ◆ 207 ページの「DSTraceの便利なコマンド」

234 ページの「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ます。このシナリオでは、パスワードは配布パスワードに同期化されます。送られるパスワードをPassword Policy（パスワードポリシー）ルールと照合して検証するよう指定したかどうか（ユニバーサルパスワードおよびAdvanced Password Rule（詳細パスワードルール）が有効になっている場合）、およびPassword Policy（パスワードポリシー）にユニバーサルパスワードと他のパスワード同期のためのその他の設定があるかに基づき、パスワードの処理の方法をNMASが決定します。



eDirectory へのログインのトラブルシューティング

- ◆ [DSTrace] の [+AUTH]、[+DCLN]、[+DXML]、および [+DVRS] の設定をオンにします。
- ◆ <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。
- ◆ Password Policy (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。
- ◆ Password Policy (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 [Password Synchronization] ページで、[DirXML accepts passwords (Publisher Channel)] が選択されていることを確認します。
- ◆ [Password Policy] で、[Synchronize Distribution Password when Setting Universal Password] が選択されていることを確認します。
- ◆ [Password Policy] で、必要に応じ、[Synchronize NDS Password when Setting Universal Password] 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 パスワードに同期化されていない場合、レガシーな Novell Clients および ConsoleOne からは、eDirectory 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可能です。『[MAS 2.3 Administration Guide \(MAS 2.3 管理ガイド\)](http://www.novell.com/documentation/lg/nmas23)』(<http://www.novell.com/documentation/lg/nmas23>) 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 パスワードに同期化されていない場合には、それらも eDirectory 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 Password Policy (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化のオプションを指定できるようにします。

パスワードを購読する別の接続システムへのログインに関する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、そのパスワードを購読するもう 1 つの接続システムが発行するシステムからの変更を購読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受信することを意味します。

- ◆ [+DXML] および [+DVRS] の設定をオンにし、DirXML 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 DirXML のトレースレベルを 3 に設定します。
- ◆ [Password Synchronization] ページの [DirXML accepts passwords (Publisher Channel)] オプションが選択されていることを確認します。
- ◆ [Password Policy] で、[Synchronize Distribution Password when Setting Universal Password] が選択され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化します。ユニバーサルパスワードは、この同期化方法の配布パスワードに同期化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 属性の追加または変更の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 Password Policy（パスワードポリシー）が、[166 ページの「ドライバ設定に必要なポリシー」](#)で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。
- ◆ eDirectory の Password Policy（パスワードポリシー）と、接続システムにより適用される Password Policy（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、DirXML のルール処理を確認します。
- ◆ ドライバの DirXML 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。
- ◆ eDirectory オブジェクトを検証し、Internet EMail Address 属性に正しい値が含まれていることを確認します。
- ◆ [Notification Configuration] 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。[220 ページの「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。電子メール通知は、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を与えず、失敗した場合でも、操作自体が再試行されない限り、電子メール通知が再試行されることはありません。

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。

[Check Password Status] を使用した場合のエラー

iManager の [Check Password Status] タスクにより、実行する [Check Object Password] アクションがドライバに与えられます。

- ◆ 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。[159 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。

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いない場合は、iManager からこの機能を使用することはできません。

- ◆ [Check Object Password] が -603 を返す場合、eDirectory オブジェクトに nspmDistributionPassword 属性が含まれていません。ドライバフィルタ、および [Password Policy] の [Synchronize Universal to Distribution] オプションを確認します。
- ◆ [Check Object Password] が [Not Synchronized] を返す場合、ドライバ設定に 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。

- ◆ eDirectory の Password Policy (パスワードポリシー) と、接続システムにより適用される Password Policy (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。
- ◆ [Check Object Password] は、配布パスワードをチェックします。配布パスワードがアップデートされていない場合、[Check Object Password] によって、パスワードが同期化されていることがレポートされないことがあります。
- ◆ eDirectory ドライバについては、[Check Password Status] は、ユニバーサルパスワードではなく NDS パスワードをチェックすることに注意してください。つまり、ユーザの Password Policy (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化するように指定されていない場合は、必ず、パスワードが同期化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化されないことがあります。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化されない限り、[Check Password Status] は正確とは限りません。

DSTrace の便利なコマンド

- +DXML - DirXML 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 - DirXML ドライバ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

シナリオ 4 - トンネリングと Identity Manager での配布パスワードのアップデートによる、eDirectory ではなく接続システムの同期化

Identity Manager では、eDirectory 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化できます。このマニュアルでは、これを「トンネリング」と呼びます。

この方法では、Identity Manager が配布パスワードを直接アップデートします。この方法は、前の 197 ページの「シナリオ 3 - Identity Manager での配布パスワードのアップデートによる、eDirectory および接続システムの同期化」とほぼ同じです。相違点は、ユニバーサルパスワードおよび配布パスワードは同期化されないことです。これは、Password Policy (パスワードポリシー) を使用しないか、[Synchronize Distribution Password When Setting Universal Password] のオプションを無効にした Password Policy (パスワードポリシー) を使用するかのどちらかで行います。

この節では、次の項目について説明します。

- ◆ 208 ページの「シナリオ 4 の長所と短所」
- ◆ 208 ページの「シナリオ 4 の図」
- ◆ 209 ページの「シナリオ 4 の設定」
- ◆ 211 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

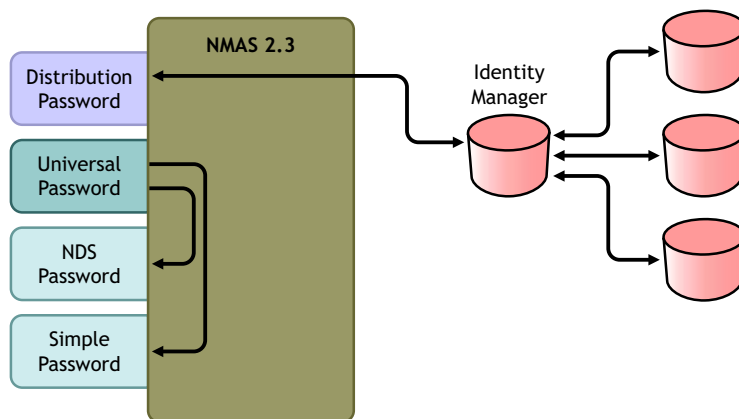
長所	短所
<p>eDirectory のパスワードはそのままにしながら、接続システム間でパスワードを同期化できます。</p> <p>Password Policy (パスワードポリシー) は必要ありません。</p> <p>Password Policy (パスワードポリシー) を使用している場合、ユニバーサルパスワードを有効にする必要はありません。ただし、使用する環境はユニバーサルパスワードをサポートする必要があります。</p> <p>接続システムが iManager の [Check Password Status] タスクをサポートする場合、このシナリオも [Check Password Status] タスクをサポートします。</p> <p>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。</p> <p>接続システムのパスワードが Password Policy (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。</p> <p>ユニバーサルパスワードおよび Advanced Password Rule (詳細パスワードルール) が有効になっている場合、Password Policy (パスワードポリシー) を適用するよう指定した際は Password Policy (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。</p>	<p>ユニバーサルパスワードおよび Advanced Password Rule (詳細パスワードルール) が無効になっている場合、Password Policy (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。</p>

シナリオ 4 の図

次の図は、Identity Manager を通じてパスワードが送られ、Identity Manager が配布パスワードを直接アップデートするために NMAS と通信することを示します。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。

このシナリオの重要な点は、Password Policy (パスワードポリシー) で、ユニバーサルパスワードと配布パスワードとの同期化が無効に設定されていることです。配布パスワードとユニバーサルパスワードは同期化されないため、Identity Manager は、eDirectory 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化します。

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。



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

- ◆ 209 ページの「ユニバーサルパスワードの展開」
- ◆ 209 ページの「Password Policy (パスワードポリシー) の設定」
- ◆ 210 ページの「パスワード同期の設定」
- ◆ 211 ページの「ドライバ設定」

ユニバーサルパスワードの展開

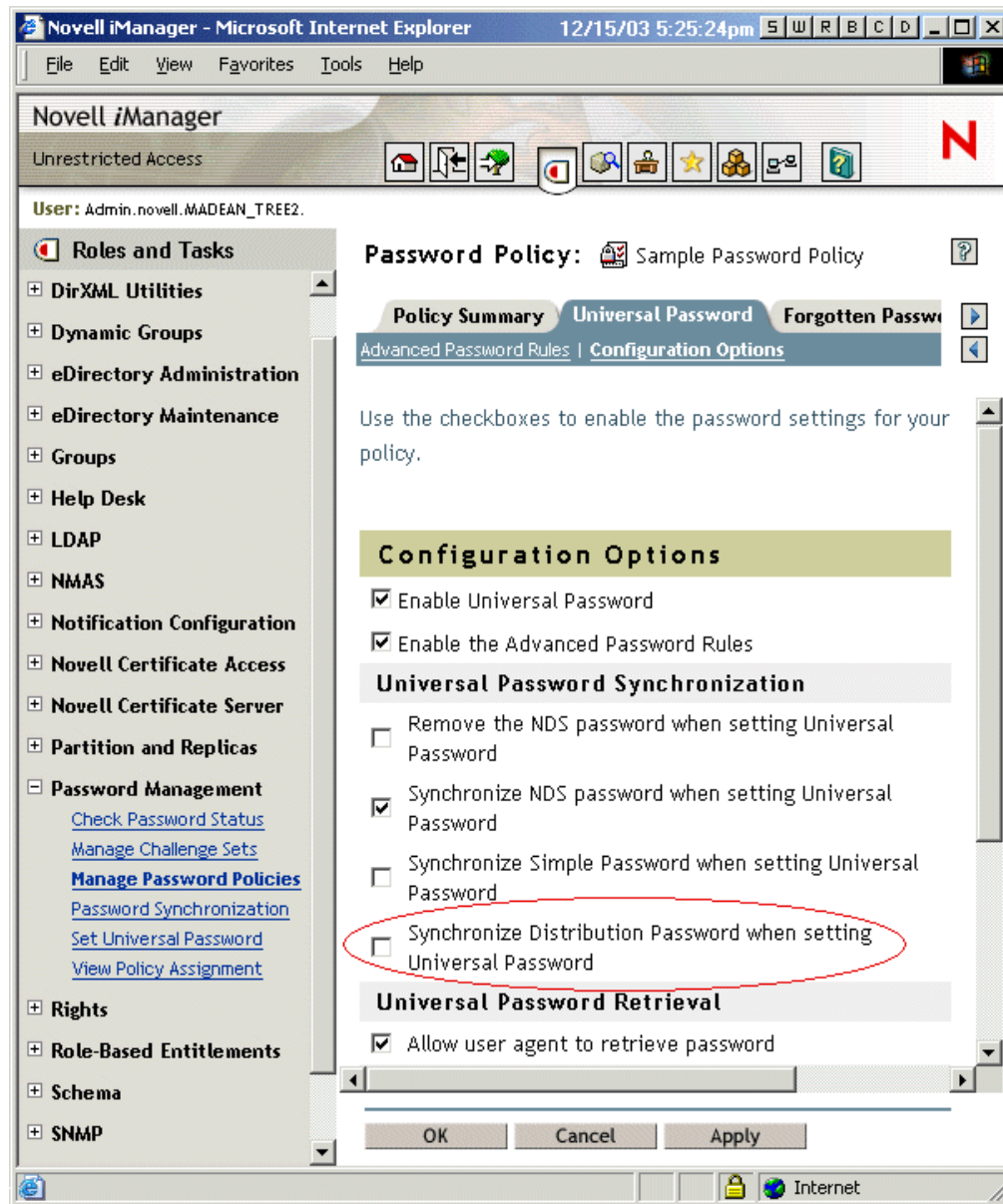
Password Policy (パスワードポリシー) でユニバーサルパスワードを有効にする必要はありません。ただし、現在の環境で、ユニバーサルパスワードをサポートする eDirectory 8.7.3 を使用していることが必要です。173 ページの「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

Password Policy (パスワードポリシー) の設定

この方法では、eDirectory ユーザに対する Password Policy (パスワードポリシー) の設定は必要ありません。

ただし、Password Policy (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。
 - ◆ Synchronize Distribution Password when Setting Universal Password
eDirectory 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化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、eDirectory 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 Password Policy (パスワードポリシー) のその他の設定を行います。
Password Policy (パスワードポリシー) のその他のパスワードの設定は、任意です。

パスワード同期の設定

197 ページの「シナリオ 3 - Identity Manager」での配布パスワードのアップデートによる、eDirectory および接続システムの同期化の「パスワード同期の設定」と同じ設定を使用します。

ドライバ設定

197 ページの「シナリオ 3 - Identity Manager での配布パスワードのアップデートによる、eDirectory および接続システムの同期化」の「ドライバ設定」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。

この節では、次の項目について説明します。

- ◆ 211 ページの「パスワードを購読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」
- ◆ 212 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」
- ◆ 212 ページの「 [Check Password Status] を使用した場合のエラー」
- ◆ 212 ページの「DSTrace の便利なコマンド」

234 ページの「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。

パスワードを購読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、そのパスワードを購読するもう 1 つの接続システムが発行するシステムからの変更を購読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受信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、DirXML 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 DirXML のトレースレベルを 3 に設定します。
- ◆ [Password Synchronization] ページの [DirXML accepts passwords (Publisher Channel)] オプションが選択されていることを確認します。
- ◆ [Password Policy] で、[Synchronize Distribution Password when Setting Universal Password] が選択され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化します。ユニバーサルパスワードは、この同期化方法の配布パスワードに同期化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）または <modify-password> 要素が、nspmDistributionPassword 属性の追加または変更の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。
- ◆ DirXML Script の Password Policy（パスワードポリシー）が、166 ページの「**ドライバ設定で必要なポリシー**」で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。

- ◆ eDirectory の Password Policy (パスワードポリシー) と、接続システムにより適用される Password Policy (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、DirXML のルール処理を確認します。
- ◆ ドライバの DirXML 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。
- ◆ eDirectory オブジェクトを検証し、Internet EMail Address 属性に正しい値が含まれていることを確認します。
- ◆ [Notification Configuration] で、SMTP サーバと電子メールテンプレートを確認します。[220 ページの「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。電子メール通知は、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を与えず、失敗した場合でも、操作自体が再試行されない限り、電子メール通知が再試行されることはありません。

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。

[Check Password Status] を使用した場合のエラー

iManager の [Check Password Status] タスクにより、実行する [Check Object Password] アクションがドライバに与えられます。

- ◆ 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。[159 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。

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いない場合は、iManager からこの機能を使用することはできません。

- ◆ [Check Object Password] が -603 を返す場合、eDirectory オブジェクトに nspmDistributionPassword 属性が含まれていません。DirXML 属性フィルタ、および [Password Policy] の [Synchronize Universal to Distribution] オプションを確認します。
- ◆ [Check Object Password] が「Not Synchronized」を返す場合、ドライバ設定に適切な DirXML 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。
- ◆ eDirectory の Password Policy (パスワードポリシー) と、接続システムにより適用される Password Policy (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。
- ◆ [Check Object Password] は、配布パスワードをチェックします。配布パスワードがアップデートされていない場合、[Check Object Password] によって、パスワードが同期化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 - DirXML 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 - DirXML ドライバ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

シナリオ5 - アプリケーションのパスワードの通常パスワードへの同期化

このシナリオは、パスワード同期化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、直接、eDirectory の通常パスワードに同期化できます。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、通常パスワードに同期化できます。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、eDirectory に対して認証できます。NMAS コンポーネントは、通常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 eDirectory の通常パスワードの場所に発行できます。

接続システムがハッシュされたパスワード (MD5、SHA、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通常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 を使用して通常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、通常パスワードの値を比較します。通常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通常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。

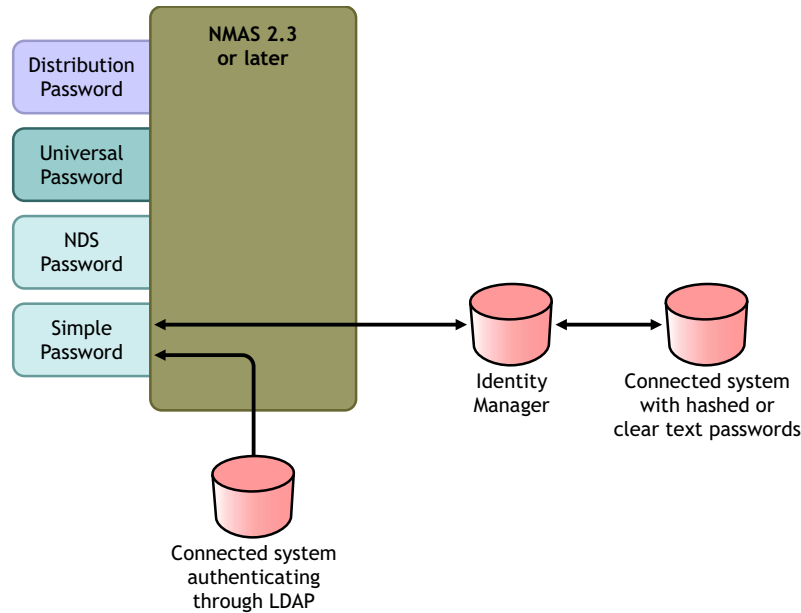
この節では、次の項目について説明します。

- ◆ [213 ページの「シナリオ5の長所と短所」](#)
- ◆ [214 ページの「シナリオ5の図」](#)
- ◆ [214 ページの「シナリオ5の設定」](#)

シナリオ5の長所と短所

長所	短所
<ul style="list-style-type: none">◆ 通常パスワードを直接アップデートできます。◆ ハッシュされたパスワードを同期化し、ハッシュに戻さずに、複数のアプリケーションでの認証に使用できます。	<ul style="list-style-type: none">◆ 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せんが、通常パスワードについては使用できません。◆ [Password Management] > [Set Universal Password] タスクはユニバーサルパスワードに依存するため、管理者はこのタスクを使用して eDirectory 内のユーザのパスワードを設定することはできません。

シナリオ 5 の図



シナリオ 5 の設定

- ◆ 214 ページの「Password Policy（パスワードポリシー）の設定」
- ◆ 214 ページの「パスワード同期の設定」
- ◆ 214 ページの「ドライバ設定」

Password Policy（パスワードポリシー）の設定

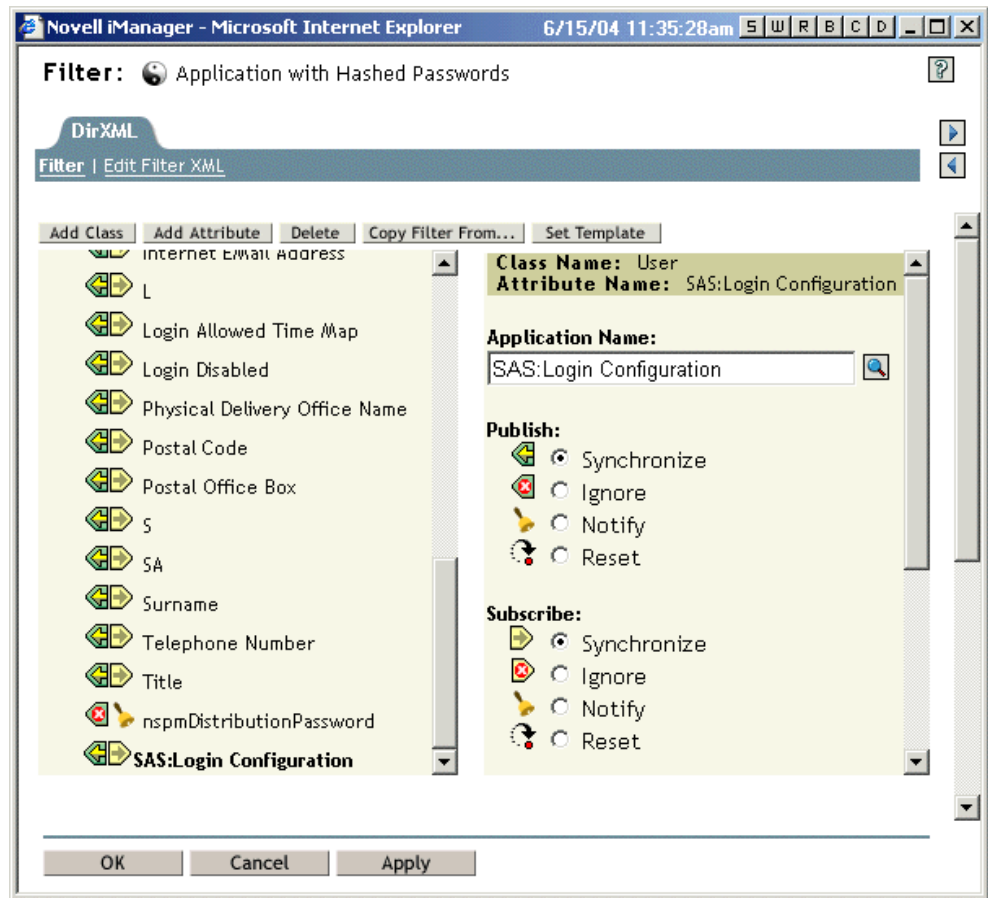
このシナリオでは、ユーザに対する Password Policy（パスワードポリシー）の設定は必要ありません。ユニバーサルパスワードは使用できません。

パスワード同期の設定

このシナリオでは、DirXML 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 [Password Management] > [Password Synchronization] タスクを使用して設定される、パスワード同期のグローバル設定値 (GCV) に効果はありません。

ドライバ設定

- 1 フィルタの、発行者および加入者の両方のチャンネルの SAS:Login Configuration 属性について、同期化するよう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末尾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 パスワードを通常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。

たとえば、変更操作内で modify-attr 要素を使用して、通常パスワードを MD5 でハッシュされたパスワードに変更する方法を次に示します。

```
<modify-attr attr-name="SAS:Login Configuration">
  <add-value>
    <value>{MD5}2tEgXrIHtAnGH0zH3ENslg==</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}2tEgXrIHtAnGH0zH3ENslg==</value>
</add-attr>
```

または、

```
<add-attr attr-name="SAS:Login Configuration">
  <value>clearpwd</value>
</add-attr>
```

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。

- ◆ 216 ページの「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」
- ◆ 216 ページの「NIS のためのパスワード同期のフィルタの設定」

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

この情報については、DirXML Drivers (<http://www.novell.com/documentation/lg/dirxmldrivers/index.html>) にある Active Directory および NT ドメイン用 DirXML ドライバのドライバ実装ガイドの「Password Synchronization (パスワード同期)」の節で説明しています。

Active Directory および NT ドメイン用 DirXML 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。

NIS のためのパスワード同期のフィルタの設定

NIS 2.0 対応の DirXML ドライバは、ファイル、NIS、および NIS+ の 3 つの UNIX 認証データを使用して動作します。パスワードをキャプチャし NIS 対応の DirXML 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、DirXML ドライバ (<http://www.novell.com/documentation/lg/dirxmldrivers/index.html>) にある『DirXML Driver for NIS Implementation Guide (NIS 用 DirXML ドライバの実装ガイド)』で説明しています。

パスワード同期の管理

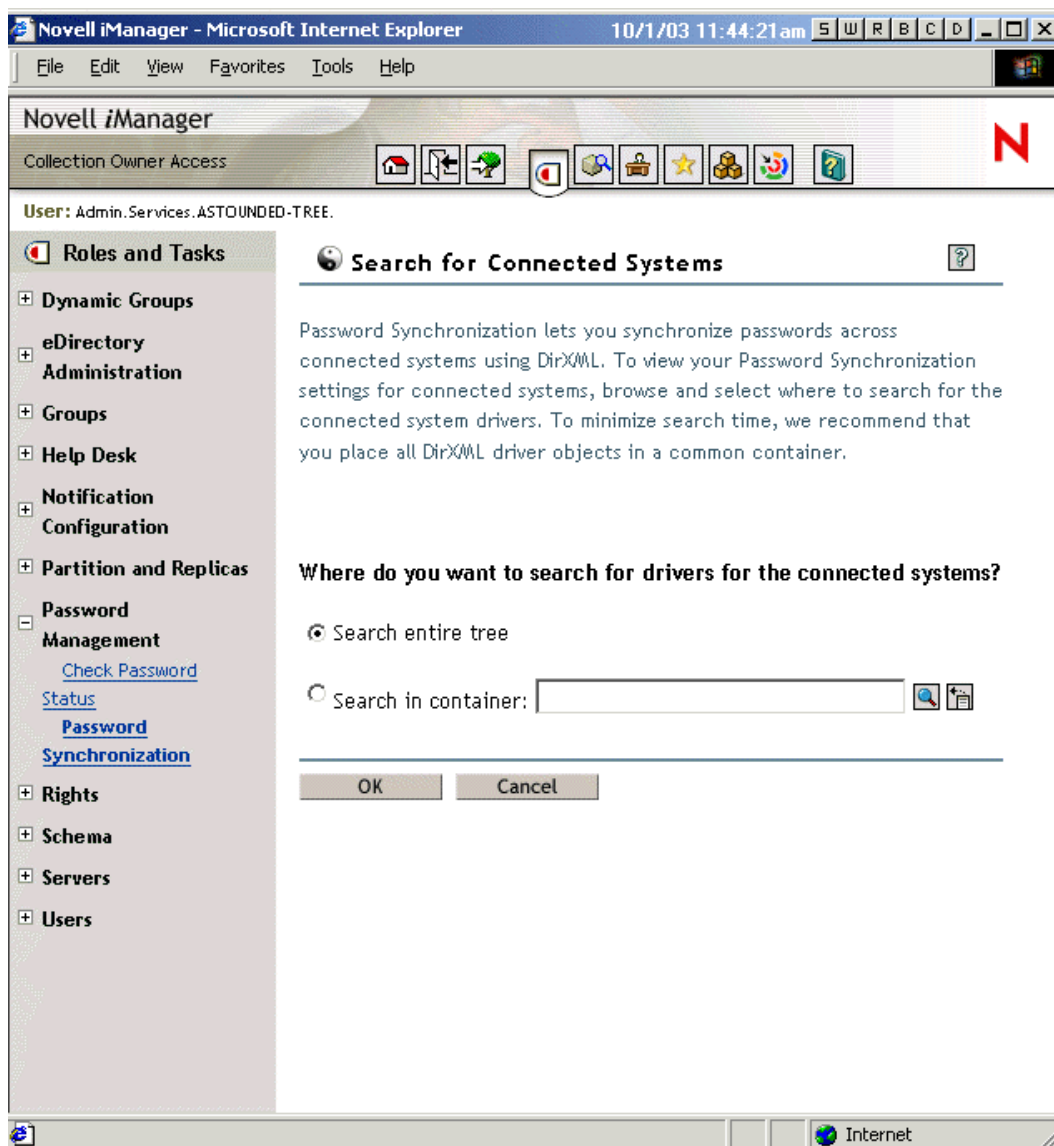
この節では、次の項目について説明します。

- ◆ 217 ページの「システム間のパスワードフローの設定」
- ◆ 220 ページの「接続システムへの Password Policy (パスワードポリシー) の適用」
- ◆ 220 ページの「eDirectoryパスワードを同期化されたパスワードとは別にそのまましておく方法」

システム間のパスワードフローの設定

次のインタフェースでは、パスワードの受け入れまたは発行のためのシステムの設定方法を参照できます。この画面は、[Password Management] 役割の下の [Password Synchronization] タスクからアクセスできます。

最初のページでは、接続システムのドライバを検索できます。



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。

The screenshot shows the Novell iManager web interface in Microsoft Internet Explorer. The browser's address bar displays the URL: <https://dxml3.provo.novell.com/nps/servlet/portalservice?NPService=AuthenticationService&NPServiceDataType>. The page title is "Novell iManager" and the user is identified as "admin.Novell.DXML3-TREE".

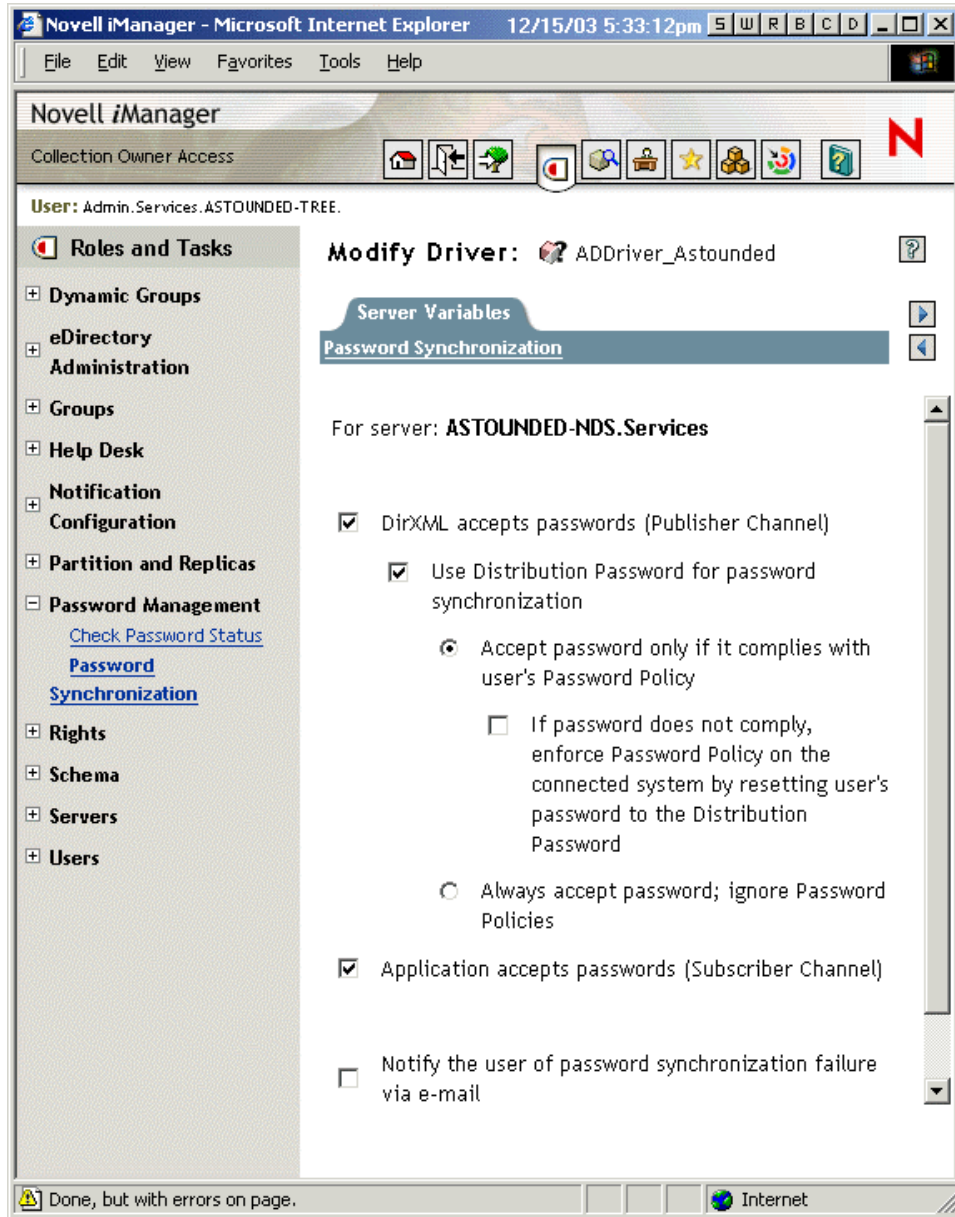
The main content area is titled "Password Synchronization" and includes a help icon. Below the title, a paragraph states: "This list shows drivers for connected systems and their current settings for Password Synchronization. Click on the Name link to change the settings. Note that making changes will cause the associated driver to be restarted."

A section titled "Connected Systems: .DXML3-TREE." contains a table with the following data:

Name	Server	DirXML Accepts Passwords	Application Accepts Passwords
ADDriver	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
DB2	DXML3	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Not Available
eDirectory Driver99	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Entitlement Services Driver	DXML3	<input type="checkbox"/> Not Available	<input type="checkbox"/> Not Available
NT Domains	DXML3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

The left sidebar contains a navigation menu with the following items: Roles and Tasks, Notification Configuration, Novell Certificate Access, Novell Certificate Server, Partition and Replicas, Password Management (with sub-links: Check Password Status, Manage Challenge Sets, Manage Password Policies, Password, Synchronization, Set Universal Password, View Policy Assignment), Rights, Role-Based Entitlements, Schema, SNMP, UNIX Profile Management, Users, and WAN Traffic.

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。詳細を確認して設定を変更するための、次のページが表示されます。



このページでは、Identity Manager が受信するパスワードに Password Policy（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 Password Policy（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。162 ページの「グローバル設定値を使用して作成するパスワード同期設定」を参照してください。

接続システムへの Password Policy（パスワードポリシー）の適用

Advanced Password Rule（詳細パスワードルール）と Identity Manager 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 Password Policy（パスワードポリシー）を検索し、Advanced Password Rule（詳細パスワードルール）が互換性があることを確認することをお勧めします。

eDirectory パスワードを同期化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、207 ページの「シナリオ 4 - トンネリング & Identity Manager での配布パスワードのアップデートによる、eDirectory ではなく接続システムの同期化」で説明しています。

ユーザのパスワード同期ステータスのチェック

iManager では、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確認するためのタスクが提供されています。

iManager で、[Password Management] > [Check Password Status] をクリックします。

iManager の [Check Password Status] タスクにより、実行する [Check Object Password] アクションがドライバに与えられます。

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しないドライバは、ドライバのマニフェストにパスワードチェック機能を含める必要があります。iManager では、マニフェストにこの機能を含まないドライバに、パスワードチェック操作を送信することできません。

[Check Object Password] は、配布パスワードをチェックします。配布パスワードがアップデートされていない場合、[Check Object Password] によって、パスワードが同期化されていないとレポートされることがあります。

次の場合、配布パスワードはアップデートされません。

- ◆ 185 ページの「シナリオ 1 - NDSパスワードを使用した eDirectory 間でのパスワード同期化」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化している (188 ページの「シナリオ 2 - ユニバーサルパスワードの同期」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化する Password Policy（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：eDirectory ドライバについては、[Check Password Status] は、ユニバーサルパスワードではなく NDS パスワードをチェックすることに注意してください。つまり、ユーザの Password Policy（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化するように指定されていない場合は、必ず、パスワードが同期化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化されませんが、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化されない限り、[Check Password Status] は正確とは限りません。

電子メール通知の設定

[Notification Configuration] という iManager の役割を使用すると、電子メールサーバを指定し、電子メール通知のテンプレートをカスタマイズできます。

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。

テンプレートを作成する必要はありません。テンプレートは、それらを使用するアプリケーションにより提供されます。電子メールテンプレートは、eDirectory 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。これらは eDirectory オブジェクトですが、iManager インタフェースからのみ編集することをお勧めします。

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。

Identity Manager では、パスワード同期およびパスワードを忘れた場合の通知のためのテンプレートが提供されています。iManager インタフェースでの選択に基づき、電子メールを送信するかどうかは制御されます。

パスワードを忘れた場合は、電子メールを送信する [Forgotten Password] のいずれかのアクションについてパスワードをユーザに電子メールで送信するか、パスワードヒントをユーザに電子メールで送信するかのどちらか 1 つを選択した場合にのみ電子メール通知が送信されます。このオプションの設定に使用するページについては、[99 ページの「ユーザへのパスワードを忘れた場合のセルフサービスの提供」](#)を参照してください。

パスワード同期は、パスワード同期処理の失敗についてのみ、および指定するドライバについてのみ電子メールを送信するよう設定されます。このオプションの設定に使用するページについては、[162 ページの「グローバル設定値を使用して作成するパスワード同期設定」](#)の最後の図を参照してください。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。

この節では、次の項目について説明します。

- ◆ [221 ページの「前提条件」](#)
- ◆ [222 ページの「電子メール通知を送信するための SMTP サーバの設定」](#)
- ◆ [223 ページの「通知のための電子メールテンプレートの設定」](#)
- ◆ [224 ページの「ドライバポリシーでの SMTP 認証情報の提供」](#)
- ◆ [225 ページの「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」](#)
- ◆ [233 ページの「電子メール通知の管理者への送信」](#)
- ◆ [233 ページの「電子メール通知テンプレートのローカライズ」](#)

前提条件

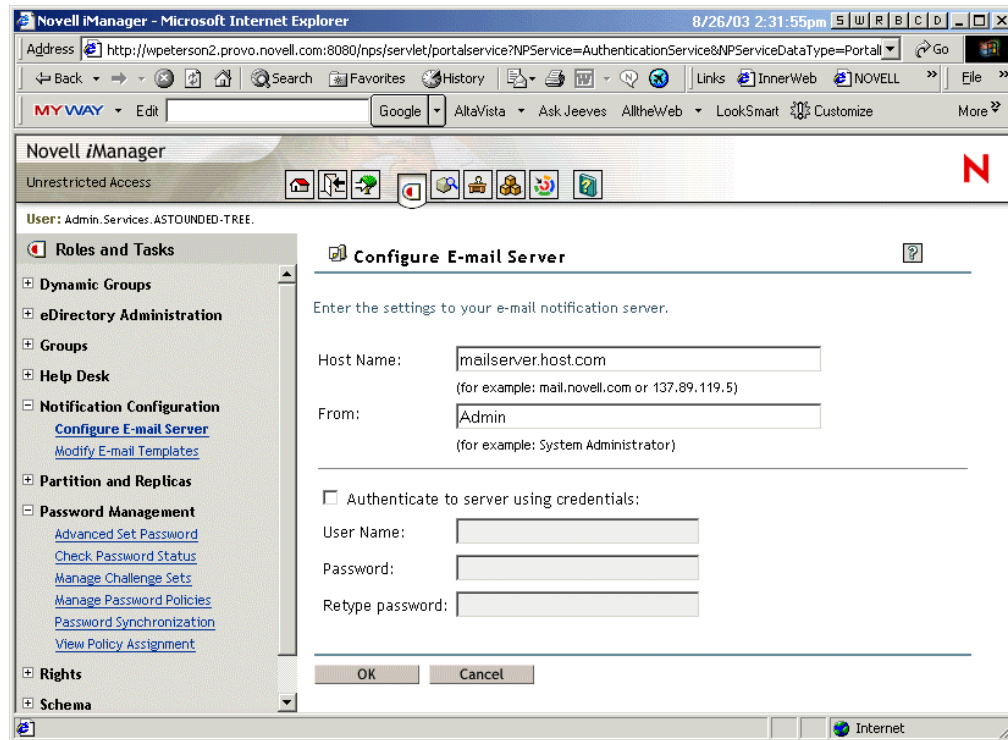
- ❑ eDirectory ユーザが Internet EMail Address 属性に入力済みであることを確認します。
- ❑ パスワード同期の電子メール通知を使用する場合は、パスワード同期化のドライバポリシーに SMTP サーバのパスワードが含まれていることを確認します。[224 ページの「ドライバポリシーでの SMTP 認証情報の提供」](#)を参照してください。
- ❑ 電子メールアドレスを入力していないユーザがいる可能性がある場合や、すべての失敗操作の通知の電子メールレコードが必要な場合は、ユーザだけではなく、パスワード管理者アカウントにも電子メール通知を送信するよう選択することを検討します。この電子メールアドレスは、DirXML Script 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、[233 ページの「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。レプリカは、ルートにあるセキュリティコンテナに格納されるため、サーバにはルートパーティションのレプリカも必要です。

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、[Notification Configuration] > [Configure E-mail Server] の順にクリックします。

次のページが表示されます。



- 2 次の情報を入力します。

- ◆ ホスト名
- ◆ 管理者など、電子メールメッセージの [From] フィールドに表示する名前
- ◆ 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 [Close] をクリックします。

- 4 DirXML 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、[224 ページの「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 [Configure E-Mail Server] 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 変更に伴いアップデートする必要がある DirXML 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。

- 5 223 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。

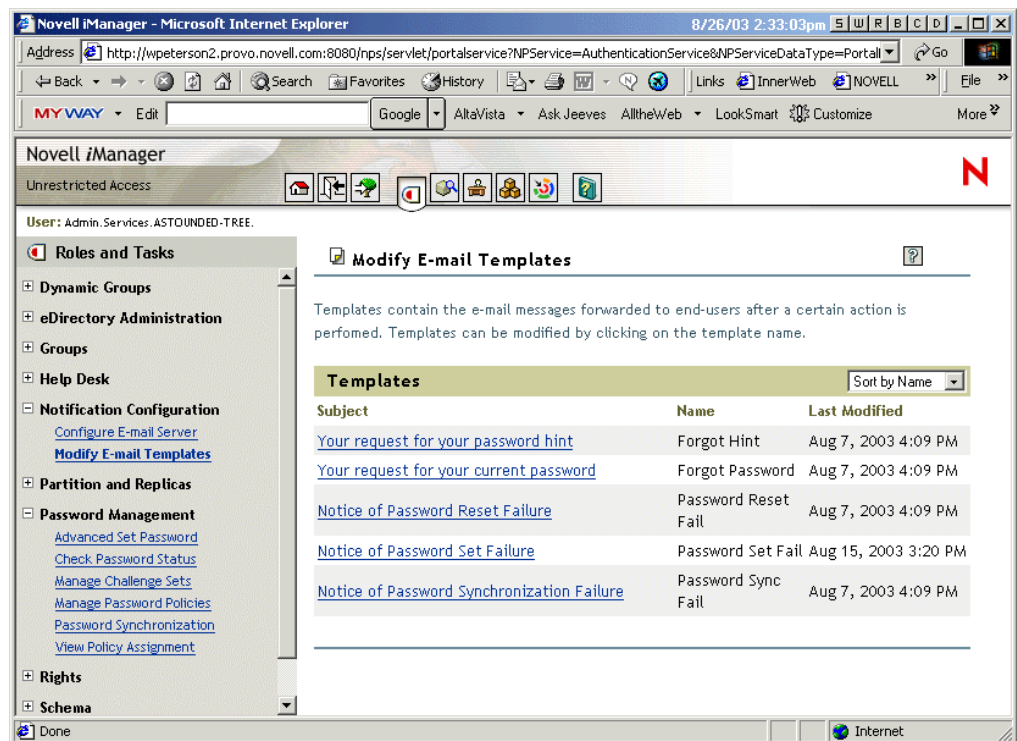
メッセージを送信する機能を使用する場合は、電子メールサーバの設定後、電子メールテンプレートを使用するアプリケーションから電子メールメッセージを送信できます。

通知のための電子メールテンプレートの設定

テンプレートをカスタマイズして独自のテキストを使用できます。テンプレートの名前は、使用目的を示します。

- 1 iManager で、[Notification Configuration] > [Modify E-mail Templates] の順にクリックします。

次の例のような、テンプレートのリストが表示されます。



Subject	Name	Last Modified
Your request for your password hint	Forgot Hint	Aug 7, 2003 4:09 PM
Your request for your current password	Forgot Password	Aug 7, 2003 4:09 PM
Notice of Password Reset Failure	Password Reset Fail	Aug 7, 2003 4:09 PM
Notice of Password Set Failure	Password Set Fail	Aug 15, 2003 3:20 PM
Notice of Password Synchronization Failure	Password Sync Fail	Aug 7, 2003 4:09 PM

- 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。225 ページの「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 変更に伴いアップデートする必要がある DirXML 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。

ドライバポリシーでの SMTP 認証情報の提供

222 ページの「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。DirXML エンジンに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 パスワード同期を DirXML 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、[Notify the user of password synchronization failure via e-mail] 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、サンプルドライバ設定で提供されています。また、178 ページの「Identity Manager パスワード同期をサポートするための、既存のドライバ設定のアップグレード」に従い、追加することもできます。

- 2 iManager で、[DirXML Management] > [Overview] の順にクリックします。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。

ドライバセットのグラフィック画面が表示されます。

- 3 [DirXML Overview] で、ドライバのアイコンをクリックします。

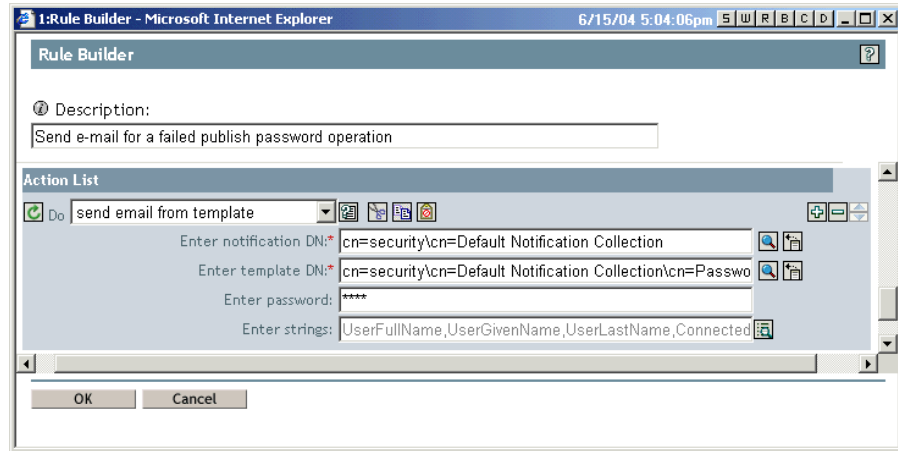
ドライバ設定のグラフィック画面が表示されます。

- 4 [Do Send E-mail from Template] 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、サンプルドライバ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
Input Transformation (入力変換)	Password(Pub)-Sub Email Notifications (パスワード(発行者)-加入者の電子メール通知)	<ul style="list-style-type: none">◆ パスワード購読時のエラーを電子メールで送信する◆ DirXML データストアのパスワードを使用して接続システムのパスワードをリセットする際のエラーを電子メールで送信する
Output Transformation (出力変換)	Password(Sub)-Pub Email Notifications (パスワード(加入者)-発行者の電子メール通知)	<ul style="list-style-type: none">◆ パスワード発行操作のエラーを電子メールで送信する

次の図は、パスワードを必要とする [Do Send E-mail from Template] アクションの例を示します。



eDirectory に保存されている場合、パスワードは不明です。

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。

この節では、次の項目について説明します。

- ◆ [225 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」](#)
- ◆ [233 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化ポリシールールに定義しないと使用できません。[Do Send Email From Template] 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化ポリシーも、ドライバ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の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。[Send e-mail on a failure when subscribing to passwords] という名前のポリシールールは、[Do Send Email From Template] アクションの電子メールテンプレートを参照します。このルールは、パスワード同期化のエラーの通知をユーザに送信するために、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、DirXML 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 DirXML ドライバ設定にあるタグを参照できます。

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、Policy Builder 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、Policy Builder 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 Source または Destination の属性

パスワードを忘れた場合の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、eDirectory 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。パスワード同期化の電子メール通知テンプレートと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。

- ◆ グローバル設定値 (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、Policy Builder を使用してそれらにタグを追加します。

- 1 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検索します。

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。

- 2 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。iManager で、[DirXML Management] > [Overview] の順にクリックします。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。

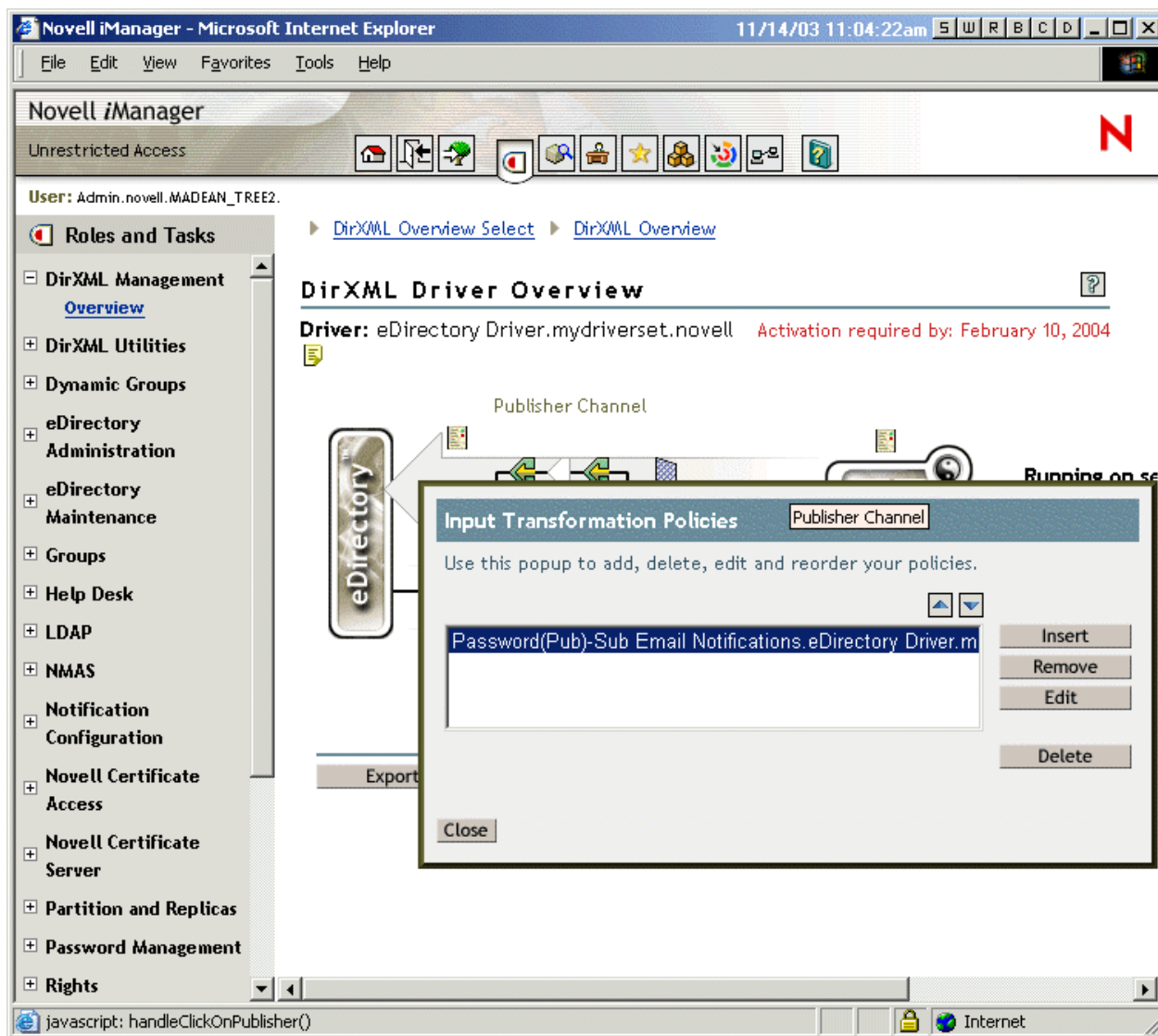
3 編集するポリシーが設定されているドライバのアイコンをクリックします。

4 編集するポリシーを含むポリシーのセットをクリックします。

たとえば、Identity Manager に付属する eDirectory ドライバ用のドライバ設定には、パスワード同期化の両方の電子メール通知テンプレートを参照する Input Transformation（入力変換）ポリシーセットのポリシーが含まれます。

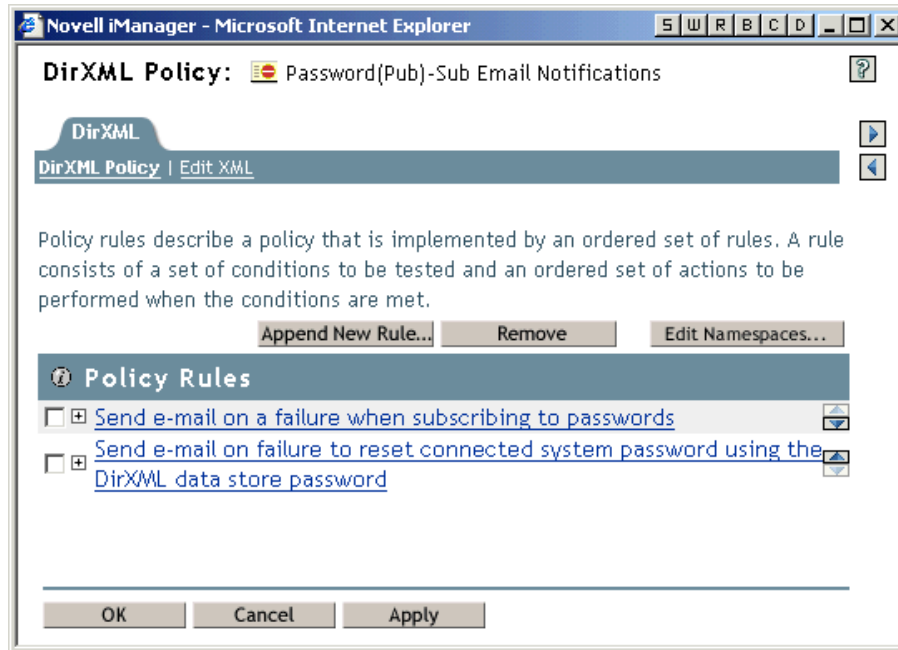
5 ポリシーをクリックした後、[Edit] をクリックします。

たとえば、Password(Pub)-Sub Email Notifications（パスワード（発行者）-加入者の電子メール通知）ポリシーを編集していた場合は、次のページで [Edit] をクリックします。



- 6 開かれたルールの一覧から、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)-加入者の電子メール通知)ポリシーでは、このようなルールの一覧が表示されます。これらのルールは両方とも、パスワード同期化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。

Policy Builder - Rule Builder FrameSet - Microsoft Internet Explorer 11/14/03 11:16:51 am

Rule Builder

Description:
Send e-mail on a failure when subscribing to passwords

Conditions
Select condition structure:
 OR Conditions, AND Groups
 AND Conditions, OR Groups

Append Condition Group * Required

Condition Group 1 ✖

If global variable 🔍

Enter name:* notify-user-on-password-dist-failure 🔍

Select operator:* equal

Compare mode: case insensitive

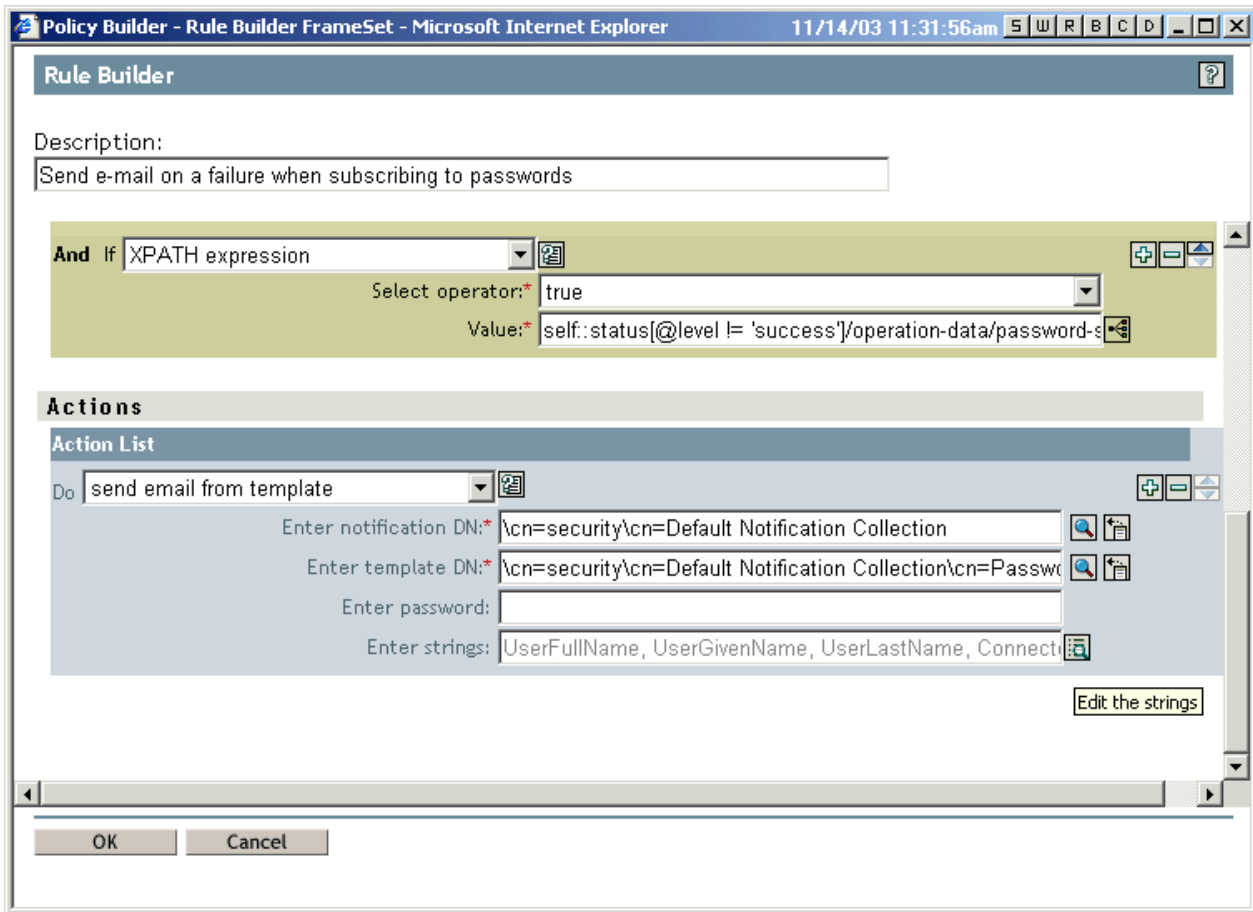
Value: true


And If operation 🔍

Select operator:* equal

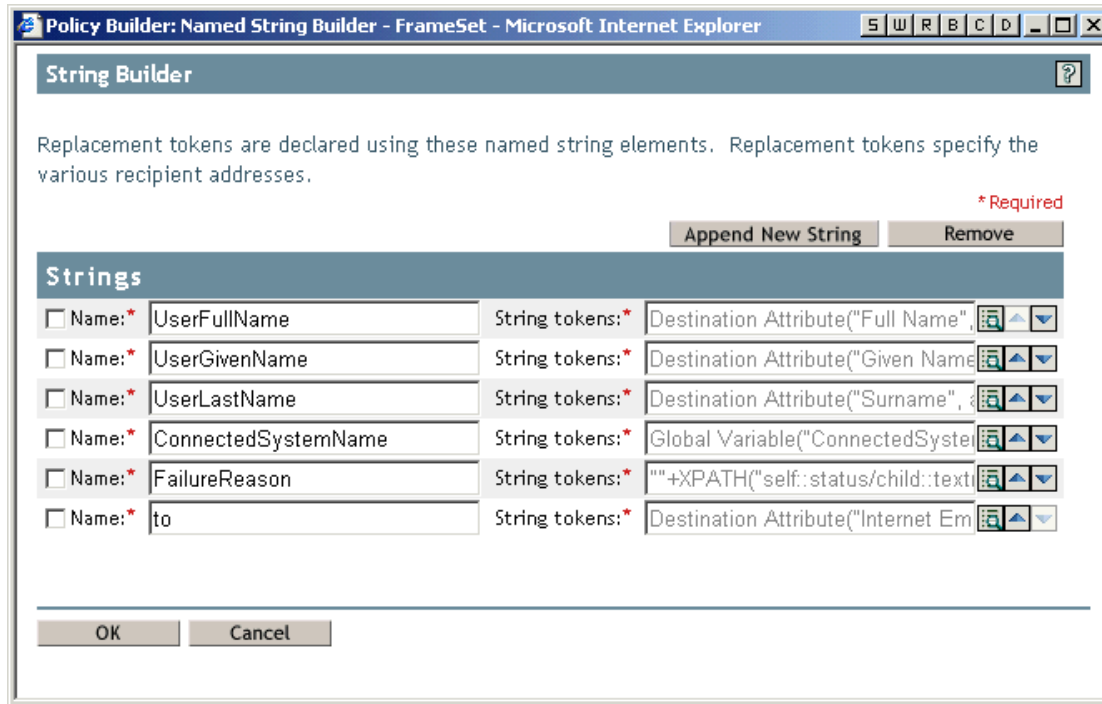
OK Cancel


- 7 アクションが表示されるルールセクションまで、スクロールします。
たとえば、次のセクションが表示されるまでスクロールします。



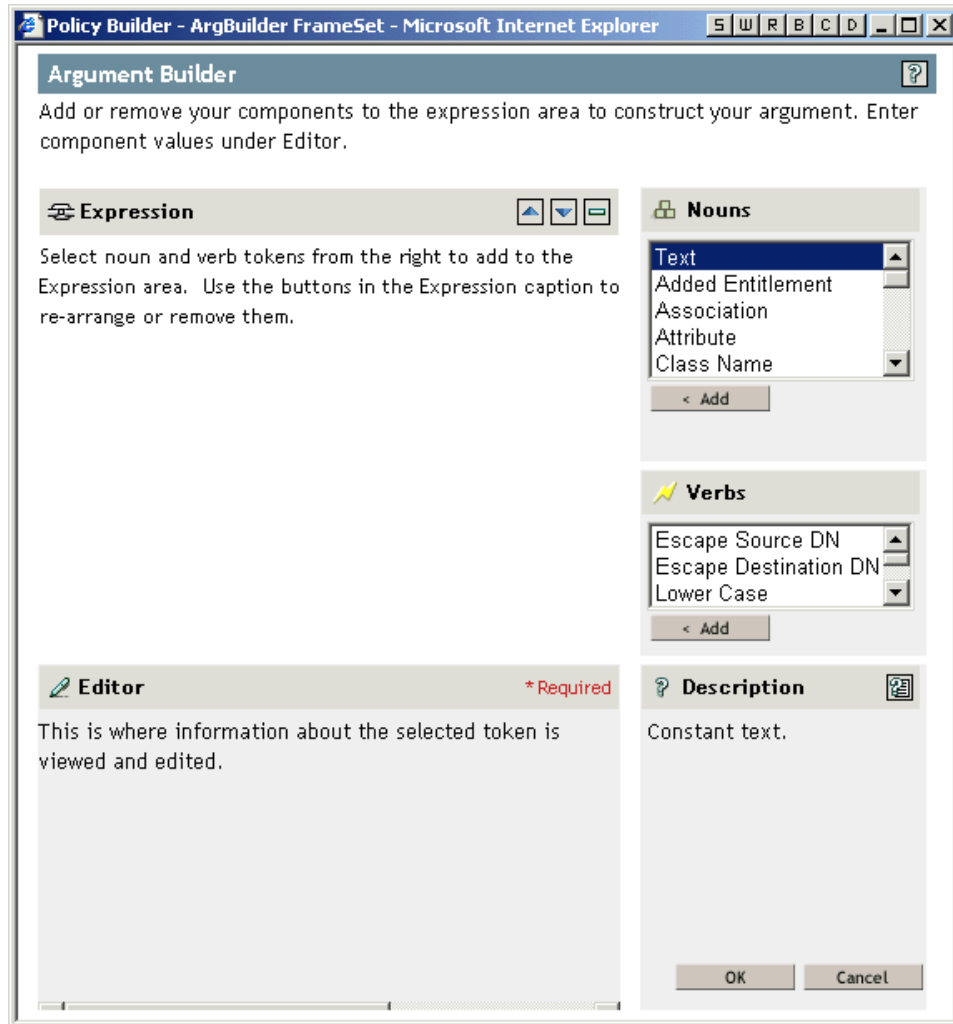
- 8 [Do Send Email from Template] ルールでは、[Enter strings] フィールドの参照ボタンをクリックします。[String Builder] が開きます。

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、DirXML ドライバ設定の一部である、パスワード同期化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] をクリックします。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完全に同じ名前を入力してください。
- 10 [String tokens] フィールドで、参照ボタンをクリックし、タグを定義します。[Argument Builder] ページが開きます。このページでは、電子メール通知テンプレートでこのタグを使用した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。
- ◆ ユーザの送信元または送信先の属性
パスワードを忘れた場合の電子メールテンプレートにタグを追加する場合は異なり、eDirectory 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。パスワード同期化の電子メール通知テンプレートと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。
 - ◆ グローバル設定値 (GCV)
 - ◆ XPATH 式

次の図は、タグの定義に使用するページの例を示します。



タグの定義が終了したら [OK] をクリックします。タグが [String Builder] ページに文字列の 1 つとして表示されます。

- 11 [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。
- 12 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。
- 13 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。
- 14 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必要があります。

LDAP 属性と eDirectory 属性の名前の対応については、LDAP の DirXML ドライバのスキーママッピングルールを参照してください。

- ◆ その他の設定は必要ありません。

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 eDirectory オブジェクトの電子メールアドレスを使用します。

ただし、パスワード同期化のポリシーでは、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、ポリシーの 1 つの DirXML 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する必要があります。次に、追加する arg-string 要素の例を示します。

```
<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。

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あればなりません。
- ◆ 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。

- ◆ パスワードを忘れた場合の電子メールメッセージについては、<mail>、<message>、および<attachment>各要素に 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。

パスワード同期のトラブルシューティング

- ◆ 184 ページの「パスワード同期の実装」のヒントを参照してください。
- ◆ NMAS に通常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 により同期化する接続システムのパスワードに NMAS で Password Policy (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。
- ◆ パスワード同期化の対象のユーザが、パスワードを同期化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 サーバおよび Directory 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 eDirectory に正しく設定されている場合は、ドライバのデフォルトのパスワードが、ユーザに適用される Password Policy (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。

次に、Active Directory ドライバを使用し、同じ問題が別のドライバについて発生する可能性のある例を示します。

例：Active Directory のユーザに一致するような新しいユーザオブジェクトを eDirectory に作成する際に、Active Directory ドライバがユーザの初期パスワードを提供すると想定します。Active Directory ドライバのサンプル設定は、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々に実行されるので、このケースでは新しいユーザは、一時的ではあるにしても、必ずデフォルトパスワードを受け取ります。ユーザの追加後すぐにパスワードを Active Directory ドライバが送信するので、パスワードはすぐにアップデートされます。デフォルトパスワードがユーザの eDirectory の Password Policy (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 Password Policy (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 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、初期パスワードがイベントの追加に付属するのではなく、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。

- ◆ eDirectory で組織のものとして定義されている Password Policy (パスワードポリシー) ([Password Management] > [Manage Password Policies] で作成) にデフォルトパスワードが準拠するよう、デフォルトパスワードを作成する発行者チャンネルのポリシーを変更します。初期パスワードが認証された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 Password Policy (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。

または、

- ◆ デフォルトパスワードを作成する加入者チャンネルのポリシーを削除します。サンプル設定では、このポリシーは Command Transformation (コマンド変換) ポリシーセットにより提供されます。eDirectory では、パスワードのないユーザも追加できます。このオプションは、新しく作成されたユーザオブジェクトについてのパスワードが最終的に加入者チャン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。
- ◆ Password Policy (パスワードポリシー) はツリー中心で割り当てられます。対照的に、パスワード同期はドライバごとに設定されます。ドライバはサーバベースでインストールされ、マスタレプリカまたは読み書き可能レプリカ内に存在するユーザのみを管理できます。パスワードの同期化により期待される結果を取得するには、パスワードの同期化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 Password Policy (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 Password Policy (パスワードポリシー) が割り当てられます。
- ◆ DTrace の便利なコマンド
 - +DXML - DirXML 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 - DirXML ドライバ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

10

Role-Based Entitlement（役割ベースのエンタイトルメント）

Role-Based Entitlement（役割ベースのエンタイトルメント）を使用すると、接続システムのエンタイトルメントを Novell® eDirectory™ ユーザに付与できます。Entitlement Policy（エンタイトルメントポリシー）の使用により、ビジネスポリシーの管理を効率化し、DirXML® ドライバの設定を簡略化できます。

この節では、次の項目について説明します。

- ◆ 237 ページの「概要」
- ◆ 239 ページの「Role-Based Entitlement（役割ベースのエンタイトルメント）の仕組み」
- ◆ 240 ページの「前提条件」
- ◆ 242 ページの「Entitlement Policy（エンタイトルメントポリシー）の作成」
- ◆ 250 ページの「アカウントの安全の保持」
- ◆ 250 ページの「エンタイトルメントの追加または削除の意味の制御」
- ◆ 251 ページの「Entitlement Policy（エンタイトルメントポリシー）間の衝突の解決」
- ◆ 255 ページの「パスワード同期と Role-Based Entitlement（役割ベースのエンタイトルメント）」
- ◆ 256 ページの「Role-Based Entitlement（役割ベースのエンタイトルメント）のトラブルシューティング」

概要

Role-Based Entitlement（役割ベースのエンタイトルメント）により、現在の環境でだれにエンタイトルメントを付与するかというビジネスポリシーを定義できます。Entitlement Policy（エンタイトルメントポリシー）（強化された eDirectory ダイナミックグループ）の使用により、「テスト」という役職名など、ダイナミックな検索条件に基づき、エンタイトルメントをどのユーザに付与するかを定義します。ポリシーに対してスタティックな包含および除外のリストを使用して、例外を管理できます。

ポリシーを適用するユーザを定義したら、接続システムでそのユーザに付与するエンタイトルメントを指定します。ダイナミックグループに対してと同様、eDirectoryでの権利を付与することもできます。

接続システムのエンタイトルメントは、Role-Based Entitlement（役割ベースのエンタイトルメント）をサポートするよう設定された DirXML ドライバにより付与されます。

このビジネスポリシー管理モデルは、DirXML ドライバ設定からビジネスポリシーアップストリームを指定する点で、Identity Manager による従来型のプロビジョニング方法とは異なります。

従来型では、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、Policy Builder 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す。この従来型の分散モデルでは、別の管理者が各 DirXML 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。

Role-Based Entitlement（役割ベースの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ビジネスポリシーを制御する権限を持つ環境に適しています。このような管理者は、Identity Manager 全体を理解する必要がありますが、Role-Based Entitlement インタフェースを使用するために Identity Manager または XSLT に関する十分な専門知識はなくてもかまいません。

Role-Based Entitlement（役割ベースのエンタイトルメント）と従来型の Identity Manager 管理のもう1つの相違点は、Entitlement Policy（エンタイトルメントポリシー）は運用環境で直接変更できることです。従来型では、ドライバ設定の変更は、まず研究室環境でテストされます。Entitlement Policy（エンタイトルメントポリシー）ではビジネスポリシーの変更が簡単になりますが、運用環境での変更は十分に注意して行う必要があります（詳細については、[250 ページの「アカウントの安全の保持」](#)を参照してください）。

違いをよく理解するために、次のシナリオを考えてみます。

ビジネスポリシーの例

次の2つの付与により、新しい従業員に「テスト」という役職名を自動的にプロビジョニングすることを想定します。

- ◆ GroupWise® の電子メールアカウント
- ◆ エラーをトラックするために使用する Oracle データベースのアカウント

ビジネスポリシーの設定

従来型 - 従来型モデルを使用する場合、Identity Manager の開発者は Policy Builder またはスタイルシートを使用し、ドライバ設定のビジネスポリシーを JDBC 用の DirXML ドライバおよび GroupWise 用の DirXML ドライバに「ハードコード」します。

Role-Based Entitlement（役割ベースのエンタイトルメント） - この例では、Role-Based Entitlement（役割ベースのエンタイトルメント）を使用して、Entitlement Policy（エンタイトルメントポリシー）を作成し、「テスト」という役職名のダイナミックメンバーシップを定義します。Identity Manager の開発者は、JDBC 用の DirXML ドライバおよび GroupWise 用の DirXML ドライバを、Role-Based Entitlement（役割ベースのエンタイトルメント）をサポートするよう設定する必要もあります。ダイナミックメンバーシップ条件に合致したユーザには、ドライバによってアカウントが付与されます。

この例では、ここまでは結果は同じです。どちらの方法を使用しても、「テスト」という役職名のユーザに対してアカウントが自動的に付与されます。

ただし、Role-Based Entitlement（役割ベースのエンタイトルメント）を使用する場合の方が、このビジネスポリシーを変更する際に必要な Identity Manager の専門知識が少なく済みます。

ビジネスポリシーの変更

ビジネスポリシーの設定後、「テストマネージャ」という役職名のユーザにも同じ種類のアカウントを付与する必要があるとわかったと想定します。

従来型 - 従来型モデルを使用する場合、Identity Manager の開発者は Policy Builder を使用し、ビジネスポリシーに次の 2 つの変更を「ハードコード」します。

- ◆ GroupWise 用のドライバ設定
- ◆ JDBC 用のドライバ設定

Role-Based Entitlement (役割ベースのエンタイトルメント) - Role-Based Entitlement (役割ベースのエンタイトルメント) モデルを使用する場合、LDAP フィルタの知識を持つネットワーク管理者であれば、Entitlement Policy (エンタイトルメントポリシー) のダイナミックメンバーシップに追加のユーザ条件を簡単に追加できます。DirXML Script を編集する必要はありません。JDBC ドライバおよび GroupWise ドライバにより、ドライバ設定を変更せずに、正しいユーザにアカウントが付与されます。

Role-Based Entitlement (役割ベースのエンタイトルメント) の仕組み

Role-Based Entitlement (役割ベースのエンタイトルメント) 機能は、ユーザが Entitlement Policy (エンタイトルメントポリシー) にメンバーシップがあるかどうかを監視するエンジンサービスであるエンタイトルメントサービスドライバに依存します。ユーザが Entitlement Policy (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、ユーザの DirXML-SPEntitlements 属性に情報を追加します。ユーザに付与されるエンタイトルメントは、属性に書き込まれます。

242 ページの「[Entitlement Policy \(エンタイトルメントポリシー\) を使用するためのドライバの設定](#)」のリストに表示されているシステムについては、Identity Manager サンプルドライバ設定をインポートする際に、Role-Based Entitlement (役割ベースのエンタイトルメント) のオプションを選択できます。その後、DirXML-SPEntitlements 属性を監視してエンタイトルメントを付与または取り消すことによって、Role-Based Entitlement (役割ベースのエンタイトルメント) 機能をサポートするポリシーを確認できます。

次のどれかが発生した場合にのみ、DirXML-SPEntitlements 属性はエンタイトルメントサービスドライバによりアップデートされます。

- ◆ [Reevaluate Membership] タスクの使用
ツリーのどの部分でユーザを再評価するかを指定できます。
- ◆ ユーザの削除
- ◆ ユーザの名前変更
- ◆ Entitlement Policy (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の変更

Entitlement Policy（エンタイトルメントポリシー）により、接続システムのエンタイトルメントおよび eDirectory の権利を付与できます。接続システムのエンタイトルメントは、次のとおりです。

- ◆ 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
- ◆ 接続システムにある対応オブジェクトの属性（指定する値に更新）
- ◆ 配置
- ◆ その他のカスタマイズ可能なエンタイトルメント

オプションの中には、サンプルドライバ設定で説明されているものもあります。

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、Entitlement Policy（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。

Role-Based Entitlement（役割ベースのエンタイトルメント）機能は Identity Manager に基づいているため、接続システムを管理できるようにするには、DirXML ドライバのインストールおよび設定を正しく行う必要があります。

Entitlement Policy（エンタイトルメントポリシー）の割り当てと DirXML 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。DirXMLEntitlement Policy（エンタイトルメントポリシー）とドライバ設定のポリシーが重複または衝突するような方法で属性を管理しないでください。

前提条件

- eDirectory 8.7.3（この機能は、eDirectory 8.7.1をサポートしません）。
- Identity Manager。
- エンタイトルメントサービスドライバ。Role-Based Entitlement（役割ベースのエンタイトルメント）を使用するドライバセットごとに、エンタイトルメントサービスドライバが必要です。エンタイトルメントサービスドライバを使用するには、各ドライバセットについて、簡単な設定が一度だけ必要です。[241 ページの「エンタイトルメントドライバのためのドライバオブジェクトの作成」](#)を参照してください。
- Role-Based Entitlement（役割ベースの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 Role-Based Entitlement を使用する前に、Identity Manager サンプルドライバ設定をドライバにインポートして、ドライバを Role-Based Entitlement を使用するように指定するか、または役割ベースのエンタイトルメントをサポートする独自のドライバ設定を作成する必要があります。[242 ページの「Entitlement Policy（エンタイトルメントポリシー）を使用するためのドライバの設定」](#)を参照してください。

エンタイトルメントサービスドライバの作成と接続システムのドライバの設定

この節では、次の項目について説明します。

- ◆ 241 ページの「エンタイトルメントドライバのためのドライバオブジェクトの作成」
- ◆ 242 ページの「Entitlement Policy (エンタイトルメントポリシー) を使用するためのドライバの設定」

エンタイトルメントドライバのためのドライバオブジェクトの作成

Entitlement Policy (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。

エンタイトルメントサービスドライバオブジェクトがない場合は、[Role-Based Entitlement] 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るために、iManager で、[Role-Based Entitlements] > [Role-Based Entitlements] の順にクリックします。ドライバセットを選択します。
 - ◆ [No Entitlements Driver] 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。
 - ◆ Entitlement Policy (エンタイトルメントポリシー) のリストを示す [Role-Based Entitlements] 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。この手順を実行する必要はありません。
- 2 [No Entitlements Driver] ページで、[OK] をクリックします。Import Driver Wizard が開きます ([DirXML Utilities] > [Import Drivers] をクリックしても開きます)。
- 3 手順に従ってドライバのリストからエンタイトルメントサービスを選択し、ドライバオブジェクトを作成します。

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選択するだけです。追加の設定または情報の入力はありません。

エンタイトルメントドライバのドライバシムは、DirXML インストール時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設定ファイルは、iManager サーバに DirXML 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。

- 4 ウィザード完了後、Role-Based Entitlement (役割ベースの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 Entitlement Policy (エンタイトルメントポリシー) の作成を開始できます。

Entitlement Policy（エンタイトルメントポリシー）を使用するためのドライバの設定

Role-Based Entitlement（役割ベースのエンタイトルメント）を接続システムで使用するには、Identity Manager のドライバシムをインストールする必要があります。

ドライバは、Role-Based Entitlement（役割ベースのエンタイトルメント）をサポートするよう設定する必要があります。ドライバマニフェストの正しいエントリの設定も含まれます。

Identity Manager サンプルドライバ設定をドライバにインポートして Role-Based Entitlement（役割ベースのエンタイトルメント）を使用するようオプションを選択するか、サンプルドライバ設定の例に従ってドライバ設定を独自にカスタマイズできます。

次のサンプルドライバ設定には、Role-Based Entitlement（役割ベースのエンタイトルメント）のサポートがオプションとして含まれています。

- ◆ Active Directory
- ◆ Exchange
- ◆ GroupWise
- ◆ LDAP
- ◆ NIS
- ◆ Notes
- ◆ NT ドメイン

これらのドライバ設定は、Role-Based Entitlement（役割ベースのエンタイトルメント）で何ができるかの例を示します。その他の接続システムのドライバ、およびその他の種類のエンタイトルメントおよび説明変数も設定できます。

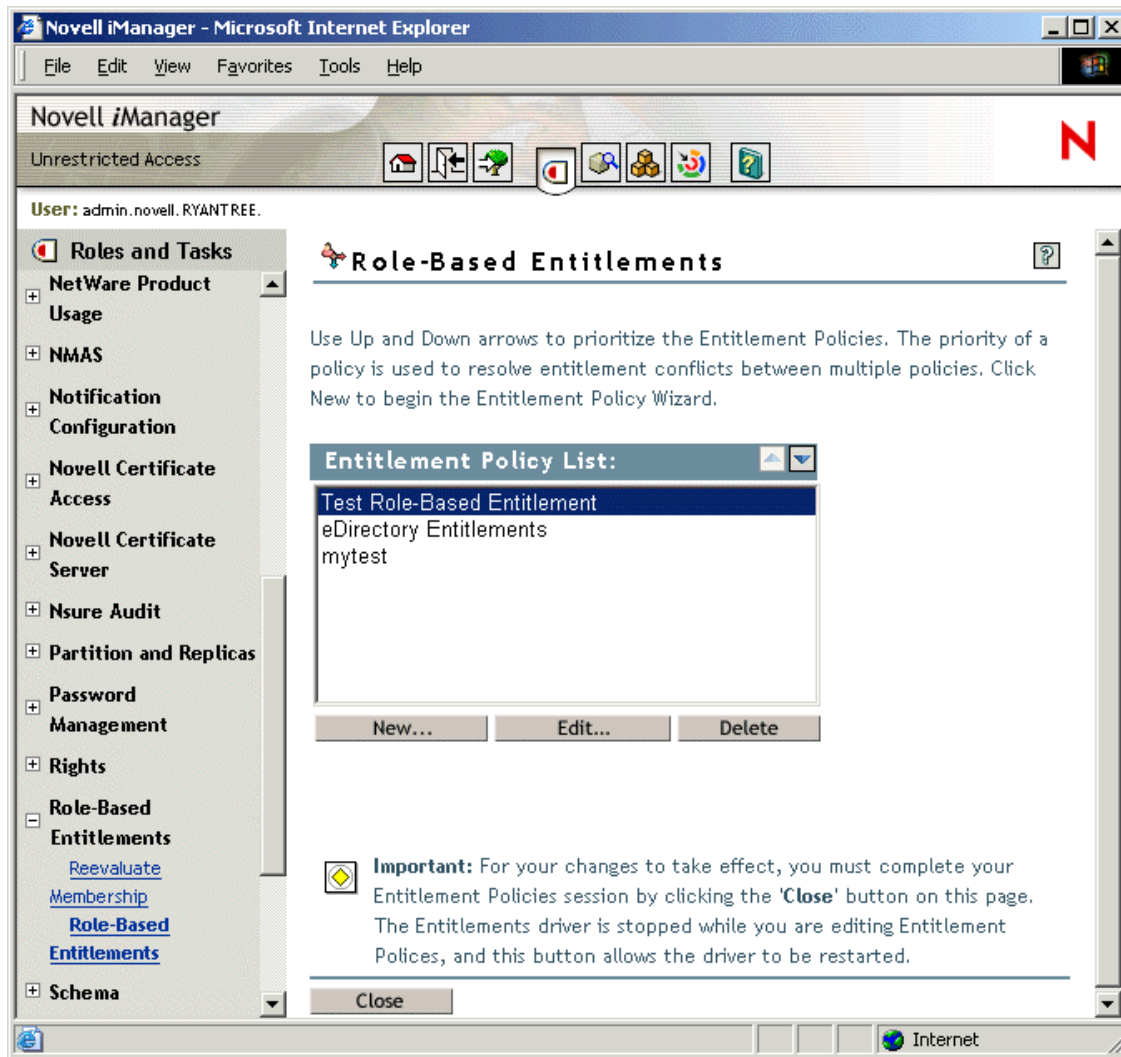
Entitlement Policy（エンタイトルメントポリシー）の作成

Entitlement Policy（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、[Role-Based Entitlements] 役割 > [Role-Based Entitlements] タスクの順にクリックします。
- 3 ドライバセットを選択します。

Entitlement Policy（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 Entitlement Policy（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 Role-Based Entitlement（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 [New] をクリックします。

Create New Entitlement Policy Wizardが開きます。

5 ウィザードの指示に従い、新しいポリシーを作成します。

ウィザードの各手順については、オンラインヘルプを参照してください。

Entitlement Policy（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

DirXML ドライバと同様、各 Entitlement Policy（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 Entitlement Policy（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。

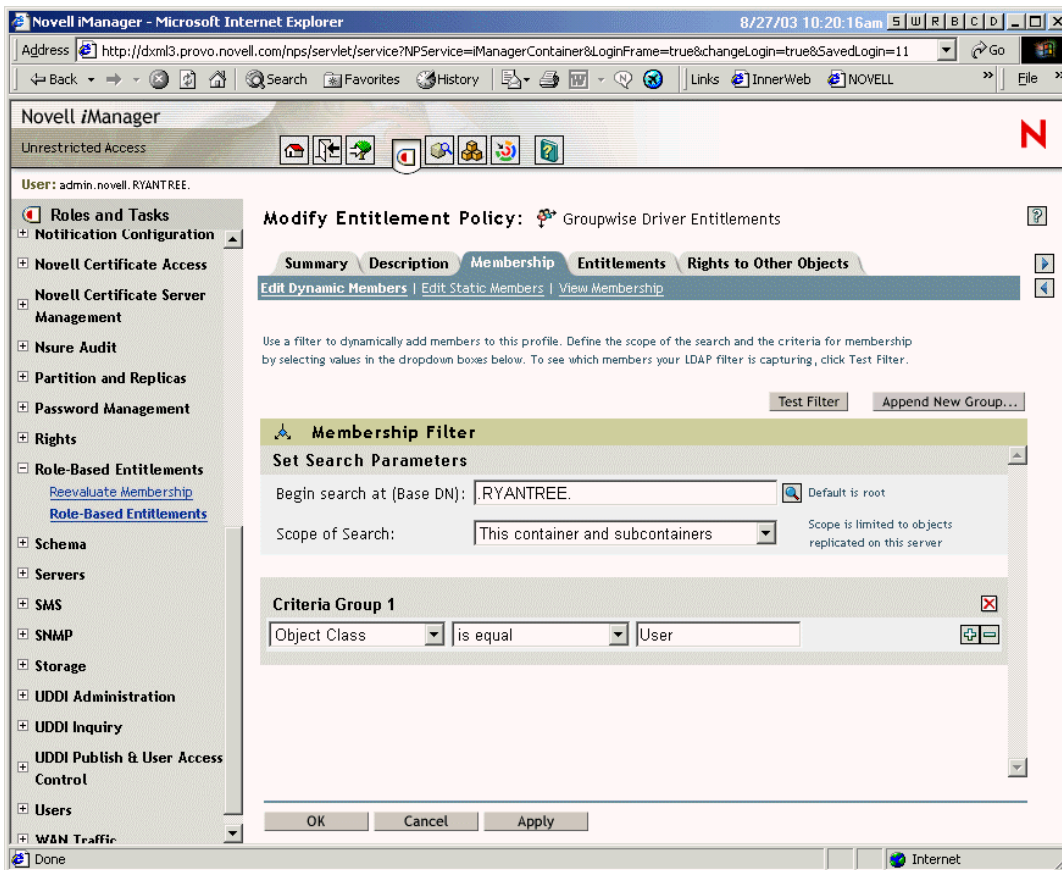
Entitlement Policy（エンタイトルメントポリシー）のメンバーになることができるのは、ユーザオブジェクト（およびユーザのクラスに基づく他のオブジェクトタイプ）だけです。

Entitlement Policy (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。Entitlement Policy (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 Entitlement Policy (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 Entitlement Policy (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。



- ◆ **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、Entitlement Policy (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。

Entitlement Policy（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

Role-Based Entitlement（役割ベースのエンタイトルメント）により、接続システムのエンタイトルメントおよび eDirectory の権利を付与できます。

Role-Based Entitlement（役割ベースのエンタイトルメント）をサポートするドライバは、Entitlement Policy（エンタイトルメントポリシー）を使用して割り当てられるエンタイトルメントのリストを提供します。ドライバが提供できるエンタイトルメントは、ドライバマニフェストにリスト表示されます。ドライバマニフェストは、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（Identity Manager 管理者は、ドライバマニフェストを編集しないでください）。

eDirectory 内のオブジェクトに対するトラスティ権は、Entitlement Policy（エンタイトルメントポリシー）のメンバーにただちに付与されます。デフォルトでは、次に Entitlement Policy（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 Entitlement Policy（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は、次のとおりです。

- ◆ 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

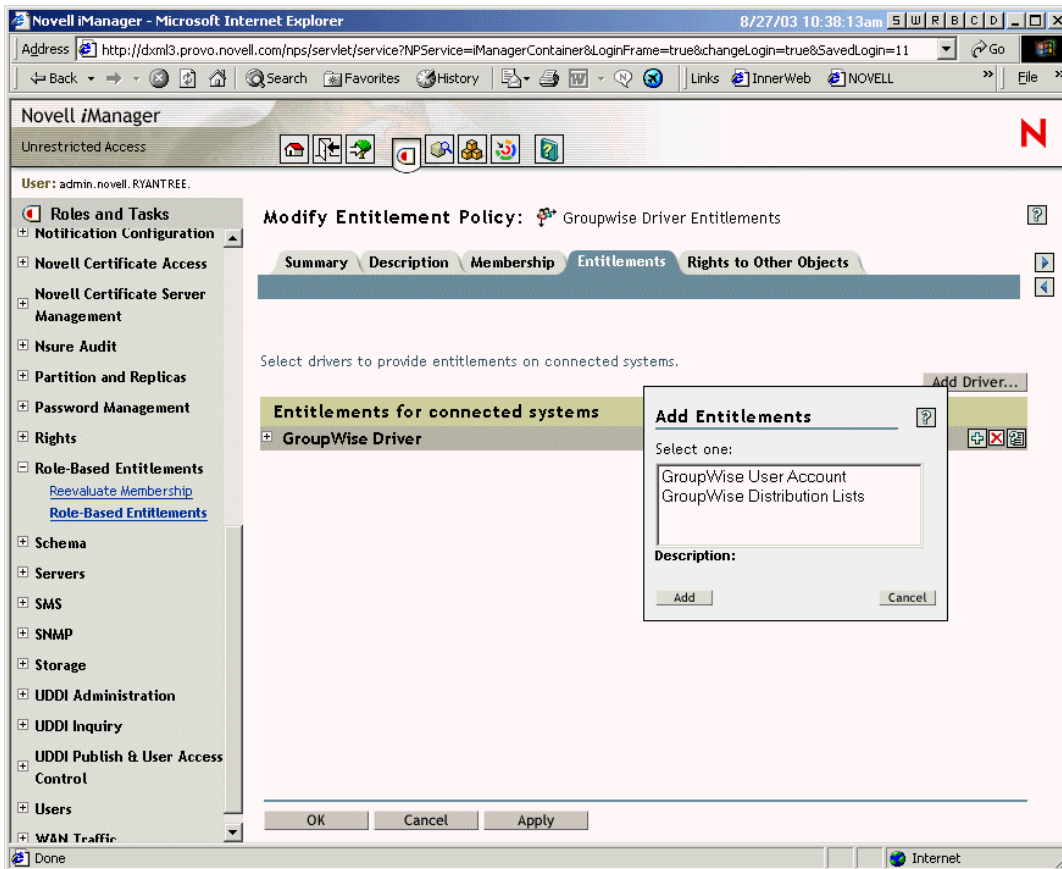
この節では、次の項目について説明します。

- ◆ [246 ページの「接続システムのアカウント」](#)
- ◆ [247 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」](#)
- ◆ [249 ページの「接続システムの属性値」](#)

接続システムのアカウント

Entitlement Policy（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、[Entitlements] 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。

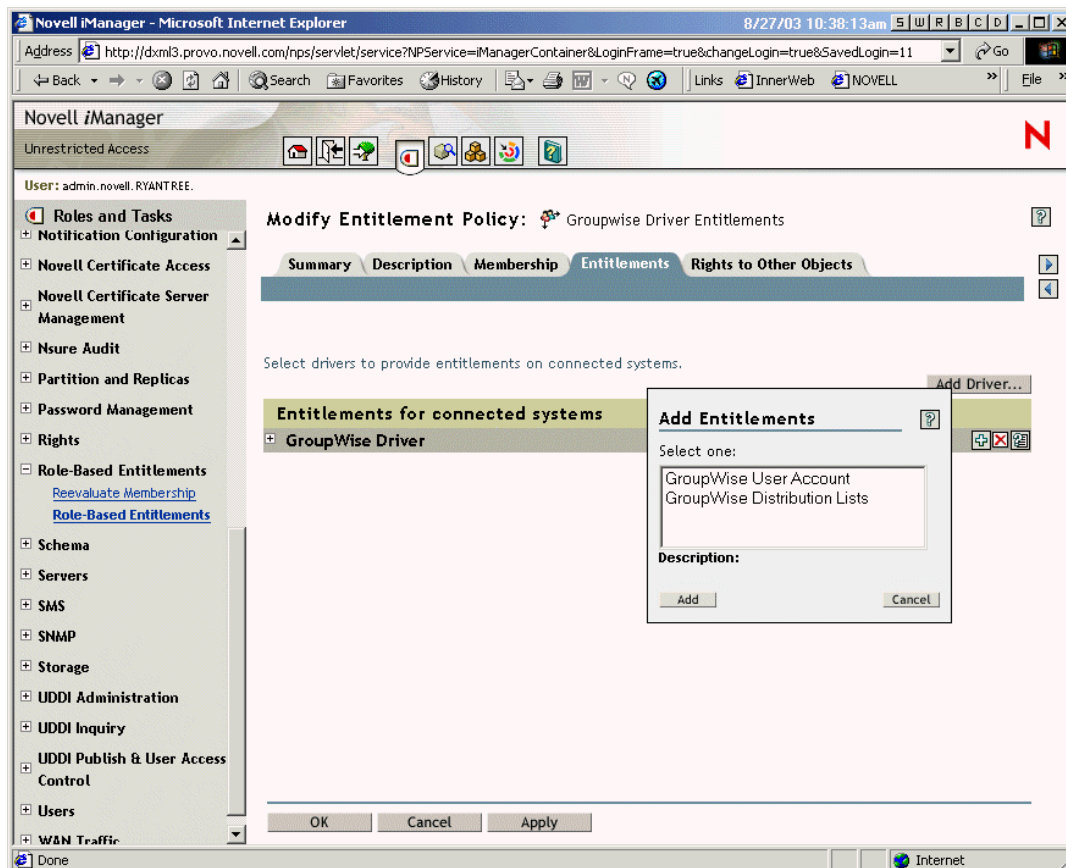
たとえば、次の図は、GroupWise ドライバにより 2 種類のエンタイトルメントが提供され、リストの先頭に [GroupWise User Account] が表示されていることを示します。



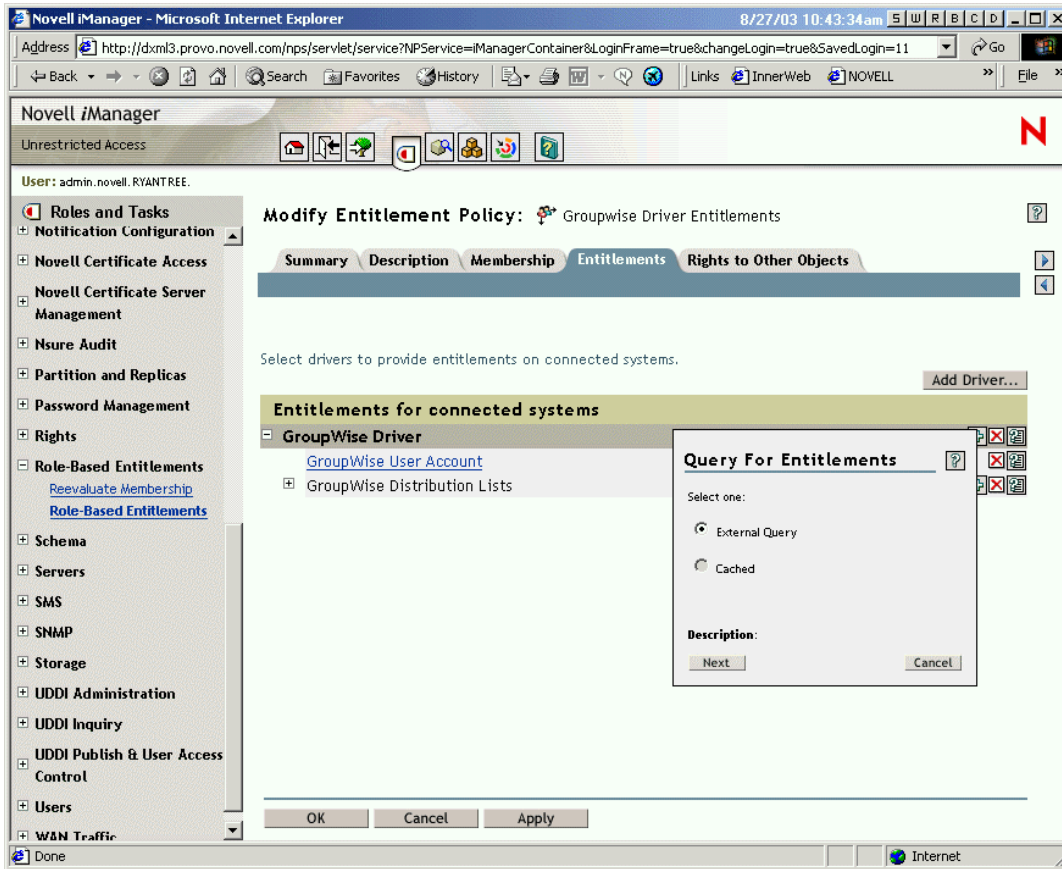
電子メール配布リストおよびNOS リストのメンバーシップ

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 Distribution Lists] がリストの 2 番目に表示されている例を示します。



この例で [GroupWise Distribution Lists] 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。



Entitlement Policy 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。

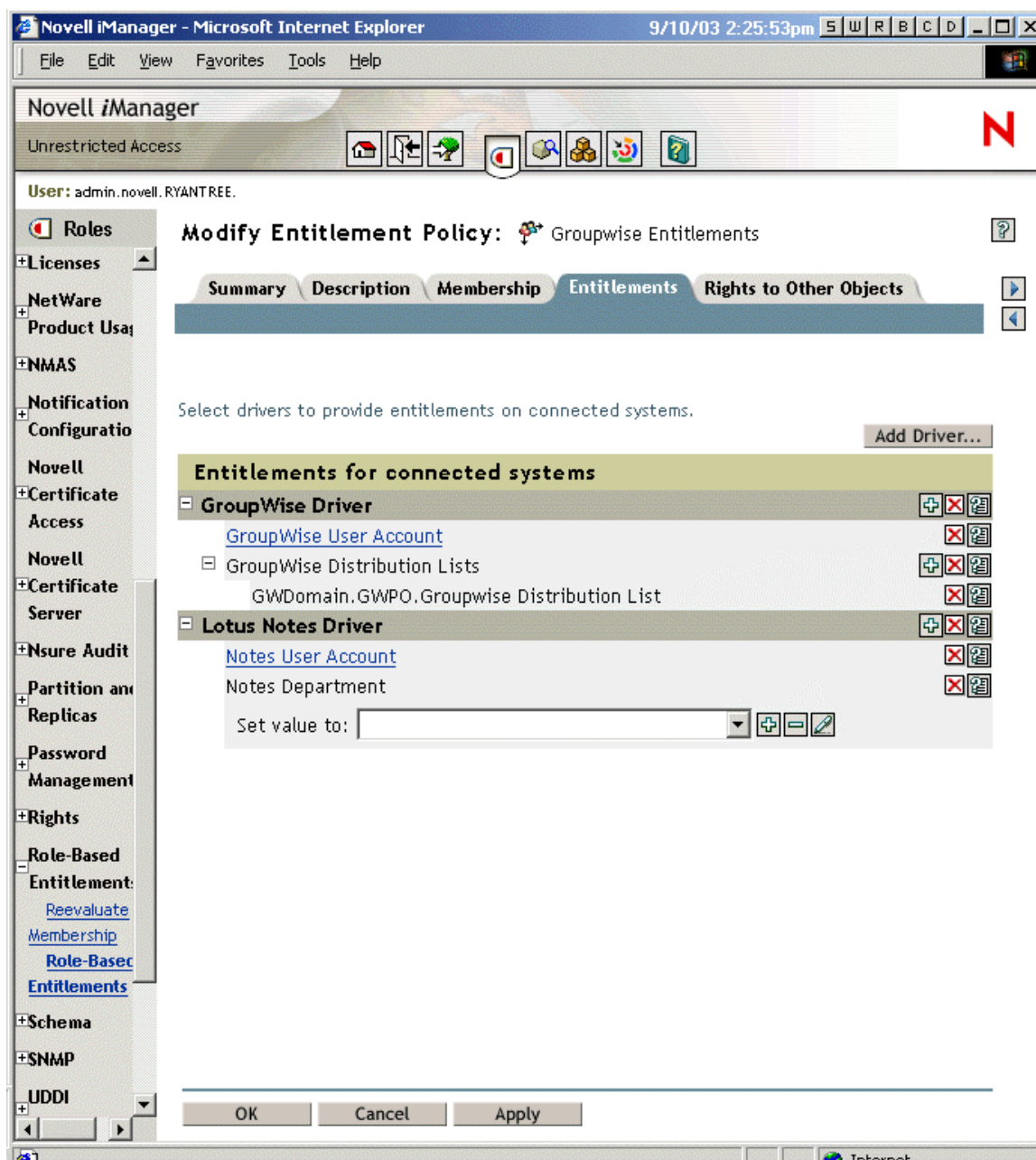
ドライバは完全なリストを返すように設定されているので、接続システムに存在するリストから選択できます。

注：完全なリストを返すクエリではなく、入力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。提供される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。



アカウントの安全の保持

Role-Based Entitlement（役割ベースの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。データの損失を防ぐには、どの設定が有効かを理解する必要があります。

2つの設定方法の最も大きな違いは、説明変数および衝突の解決です。[250 ページの「エンタイトルメントの追加または削除の意味の制御」](#)と [251 ページの「Entitlement Policy（エンタイトルメントポリシー）間の衝突の解決」](#)を参照してください。

たとえば、削除は、アカウントを削除するための説明変数に対する値として使用しないことをお勧めします。Role-Based Entitlement（役割ベースのエンタイトルメント）により、テスト期間を経ずに運用環境で大きな変更を加えることができます。また、いずれかのユーザから意図せずアカウントエンタイトルメントを削除するという誤りが発生する可能性があります。

管理者は、アカウントを取り消すための説明変数を削除ではなく無効に設定することで、データを保護できます。

新しい Entitlement Policy（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、[Entitlement Policies] インタフェースの [Restart] 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 Entitlement Policy（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、[Restart] ボタンを使用してドライバを再起動しようとする、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。

エンタイトルメントの追加または削除の意味の制御

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、「追加」または「削除」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、追加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に、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、DirXML 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を持つエンタイトルメントを削除しません。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 Entitlement Policy（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削除の解釈は特に重要です。Role-Based Entitlement（役割ベースの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。

追加または削除を解釈するための設定を変更するには、Entitlement Policy（エンタイトルメントポリシー）の [Entitlements] ページでアカウントエンタイトルメントをクリックします。表示されるページで、ドライバパラメータの一部である GCV を編集できます。個々の Entitlement Policy（エンタイトルメントポリシー）の [Entitlement] ページで解釈の設定を編集できますが、その変更は、変更時に編集していた Entitlement Policy（エンタイトルメントポリシー）だけではなく、特定の DirXML ドライバおよび接続システムから特定のエンタイトルメントを付与するすべての Entitlement Policy（エンタイトルメントポリシー）に影響を与えることに注意してください。設定は、Entitlement Policy（エンタイトルメントポリシー）ごとではなく、エンタイトルメントおよびドライバごとに行います。

[251 ページの「Entitlement Policy（エンタイトルメントポリシー）間の衝突の解決」](#)も参照してください。

Identity Manager 2 のドライバ設定では、説明変数は、アカウントエンタイトルメントでのみ使用されます。ただし、他のタイプのエンタイトルメントの説明変数も持つよう、ドライバを設定できます。

注：ドライバがサポートするアクションは、ドライバマニフェストで宣言されます。マニフェストは、ドライバの機能を示すために、ドライバ開発者が作成します。ネットワーク管理者は、これらのオプションを編集しないでください。ドライバマニフェストを変更するだけでは、ドライバは新しい解釈をサポートしません。ドライバまたは接続システムも同様に強化する必要があります。

Entitlement Policy（エンタイトルメントポリシー）間の衝突の解決

この節では、次の項目について説明します。

- ◆ [251 ページの「概要」](#)
- ◆ [253 ページの「各エンタイトルメントの衝突の解決方法の変更」](#)
- ◆ [254 ページの「Entitlement Policy（エンタイトルメントポリシー）の優先度の設定」](#)

概要

Entitlement Policy（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** - ほとんどの場合、アカウントは、値のないエンタイトルメントです。ユーザが接続システムでのアカウントを Entitlement Policy（エンタイトルメントポリシー）により付与される場合、ユーザはシステム上でアカウントを受け取ります。別の Entitlement Policy（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** - これらは、グループメンバーシップなどのエンタイトルメントと、値、または値のある属性のグループ名のリストです。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。

必要に応じて、この種類のエンタイトルメントの衝突の解決を変更できます。

各エンタイトルメントタイプの衝突の解決を制御する設定は、ドライバのドライバマニフェストにあります。ドライバが提供する各種別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。デフォルトの設定は、`conflict-resolution="union"` です。他に設定できる値は、`conflict-resolution="priority"` です。

- ◆ **`conflict-resolution="union"`** 4 「union」という値は、エンタイトルメントが付加でき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単に追加され、ユーザはそれらすべてを取得します。

たとえば、Jameel 氏が、「トレードショーメンバーリングリスト」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ーポリシー」のメンバーであり、「トレードショーメンバーリングリスト」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 Entitlement Policy (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"`** 4 反対に、「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、Entitlement Policy (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 Entitlement Policy (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ーポリシー」より上位にリスト表示される場合、「トレードショーメンバーリングリスト」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、Role-Based Entitlement（役割ベースの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は、この機能が役立ちます。ユーザは任意の1ヶ所に配置でき、同時に2ヶ所に配置することはできません。

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とは関係ありません。

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。広いメンバーシップを持つグループは、狭いメンバーシップを持つグループより上位に配置することをお勧めします。

各エンタイトルメントの衝突の解決方法の変更

- 1 iManager で、[DirXML Management] > [Overview] 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。
- 2 ドライバを停止します。
- 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。
- 4 ドライバアイコンをクリックし、ドライバのパラメータのページを開きます。
- 5 [Driver Manifest] をクリックします。
ドライバマニフェストが XML で表示されますが、編集可能モードではないので淡色表示されます。
- 6 [Enable XML editing] チェックボックスをオンにします。
- 7 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">
```
- 8 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、251 ページの「Entitlement Policy（エンタイトルメントポリシー）間の衝突の解決」を参照してください。
- 9 エンタイトルメントサービスドライバを再起動します。

Entitlement Policy (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、Entitlement Policy (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 2 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、Entitlement Policy (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、[251 ページの「Entitlement Policy \(エンタイトルメントポリシー\) 間の衝突の解決」](#)を参照してください。

Entitlement Policy (エンタイトルメントポリシー) の順序を変更するには、Entitlement Policy (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、[Role-Based Entitlements] > [Role-Based Entitlements] 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。

Entitlement Policy (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。

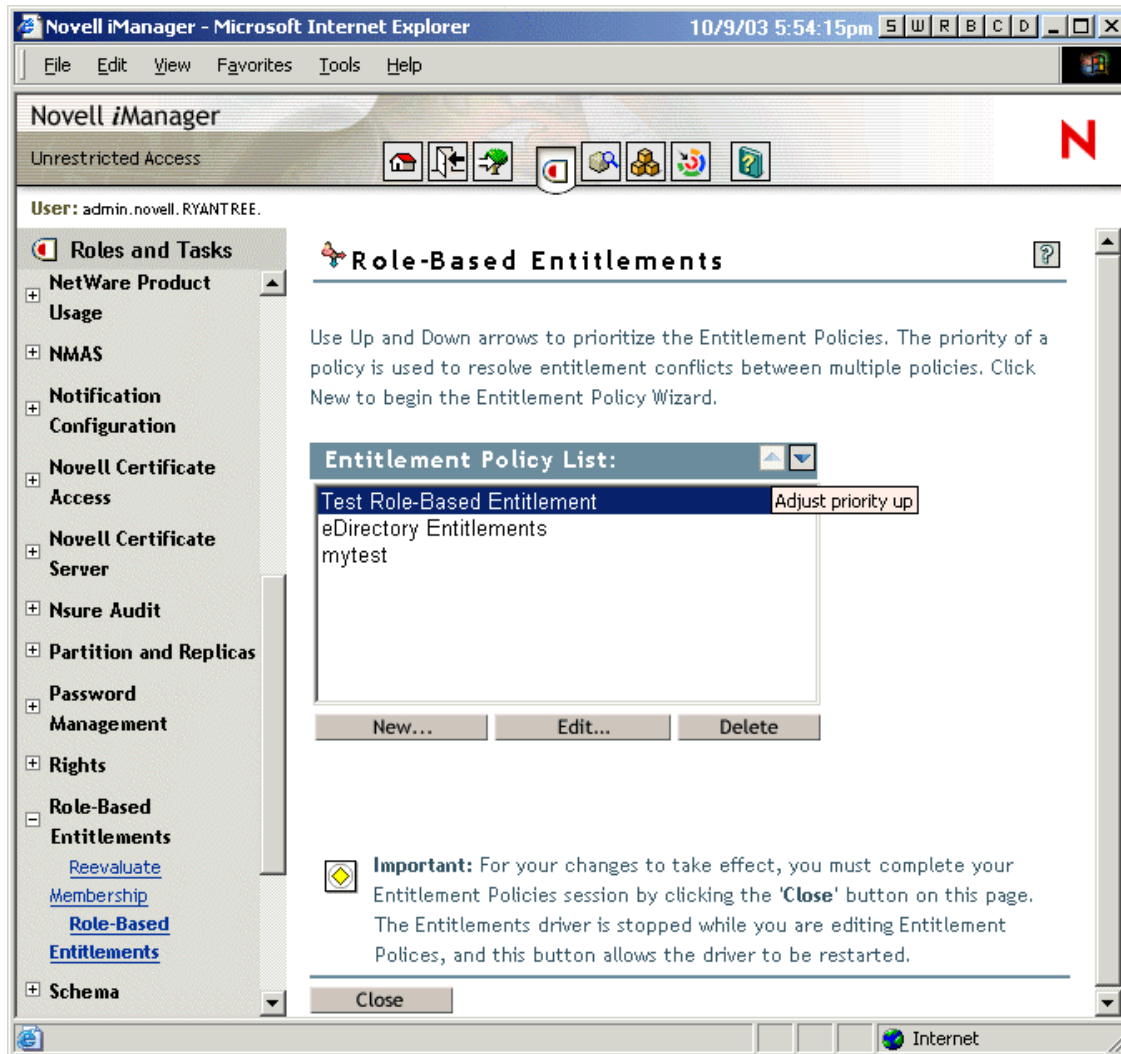
- 3 矢印ボタンを使用してポリシーをリスト内で上下に移動し、Entitlement Policy (エンタイトルメントポリシー) の優先度を変更します。

Entitlement Policy (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 [Close] ボタンをクリックし、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。

矢印ボタンが表示されたポリシーリストのページの例については、次の図を参照してください。



パスワード同期と Role-Based Entitlement（役割ベースのエンタイトルメント）

9 章 151 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、Role-Based Entitlement（役割ベースの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。

Role-Based Entitlement（役割ベースの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 [New]、[Edit]、または [Remove] 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 [Close] ボタン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 Entitlement Policy（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。
- ◆ エンタイトルメントサービスドライバは、ドライバオブジェクトが複数のサーバに関連付けられている場合は、起動しません。この設定はサポートされません。
- ◆ Entitlement Policy（エンタイトルメントポリシー）は、接続システム上のエンタイトルメントを DirXML ドライバを通じて付与します。ドライバは、オブジェクトの名前ではなく、eDirectory 内のドライバオブジェクトの GUID により識別されます。つまり、ドライバオブジェクトを、同じ名前を持つ別のドライバオブジェクトで置き換える場合、オブジェクトは新しい GUID を持つため、Entitlement Policy（エンタイトルメントポリシー）は、当該ドライバ上のエンタイトルメントに対して有効ではなくなります。
- ◆ 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、Entitlement Policy（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ーレプリカに含まれるユーザだけです。

11

エンジンサービスの管理

ドライバの中には、外部の接続システム用ではなく、DirXML[®] エンジンサービス専用のものもあります。

この節では、次の項目について説明します。

- ◆ [257 ページの「エンタイトルメントサービスドライバ」](#)
- ◆ [257 ページの「ループバックサービスドライバ：移動プロキシサービスによるオブジェクトの移動」](#)
- ◆ [261 ページの「Manual Task Service Driver \(Workflow Service Request Driver\)」](#)

エンタイトルメントサービスドライバ

[10 章 237 ページの「Role-Based Entitlement \(役割ベースのエンタイトルメント\)」](#)を参照してください。

ループバックサービスドライバ：移動プロキシサービスによるオブジェクトの移動

DirXML ドライバは、同じ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のどちらかに複製されたオブジェクトを同期化できます。ドライバが実行できる処理の1つは、コンテナ間でのオブジェクトの移動です。たとえば、人事アプリケーションで割り当てられている組織に基づき、Novell[®] eDirectory[™] にユーザを配置するようドライバを設定できます。人事アプリケーションでユーザの組織が変更された場合には、ドライバは、対応するコンテナに eDirectory ユーザオブジェクトを移動できます。

コンテナ間でオブジェクトを移動できるようドライバを設定するには、次のいずれかを実行する必要があります。

- ◆ すべての移動元または移動先のコンテナのマスタレプリカを保存するサーバ上に、ドライバを配置します。
- ◆ 読み書き可能レプリカのあるサーバ上にドライバを配置し、マスタレプリカのあるサーバ上で移動プロキシサービスを設定して、オブジェクトを移動できるようにします。次に、移動プロキシサービスに移動を委任するようドライバを設定します。

移動プロキシサービスは、ループバックサービスドライバシムで実行できる特別な設定です。この節では、移動プロキシサービスと設定方法、および他の接続システムのドライバがこのサービスを使用できるようにするための設定について説明します。

この節では、次の項目について説明します。

- ◆ [258 ページの「移動プロキシサービスの概要」](#)
- ◆ [258 ページの「移動プロキシサービスの設定」](#)
- ◆ [260 ページの「移動プロキシサーバに移動を委任するための他のドライバの設定」](#)

移動プロキシサービスの概要

Nsure™ Identity Manager および eDirectory では、特に同時に他の変更がオブジェクトに対して行われている場合、オブジェクトの移動はマスタレプリカで行うのが最適です。

コンテナ間でオブジェクトを移動できるようドライバを設定するには、次のいずれかを実行する必要があります。

- ◆ すべての移動元または移動先のコンテナのマスタレプリカを保存するサーバ上に、ドライバを配置します。
- ◆ 読み書き可能レプリカのあるサーバ上にドライバを配置し、マスタレプリカのあるサーバ上で移動プロキシサービスを設定して、オブジェクトを移動できるようにします。次に、移動プロキシサービスに移動を委任するようドライバを設定します。

移動プロキシサービスは、マスタレプリカのあるサーバ上で実行する特別な設定を持つドライバオブジェクトです。移動プロキシサービスの目的は、読み書き可能レプリカを保存するサーバで実行されている DirXML ドライバの代わりにオブジェクトを移動することです。移動の委任により、委任元のドライバによって実行されたオブジェクトの変更を、移動前にマスタサーバに複製できます。

ドライバから移動プロキシサービスに移動を委任した場合の処理手順は次のとおりです。

1. 移動する必要があるオブジェクトの `moveProxyTrigger` 属性の値を設定することにより、ドライバは移動を委任します。ドライバは、`moveProxyTrigger` 属性を、オブジェクトの移動先のコンテナの DN に設定します。
2. 移動プロキシサービスは、`moveProxyTrigger` 属性の「値の追加」イベントを監視し、移動するオブジェクトの移動元の DN および移動先のコンテナの DN を指定するカスタムコマンドに、イベントを変換します。

カスタムコマンドは、移動プロキシサービスドライバの Subscriber Event Transformation Rule（加入者イベント変換ルール）により作成されます。

3. 移動プロキシサービスドライバは、発行者チャンネルで実際のオブジェクトの移動を開始します。次に、移動プロキシサービスドライバは、移動先 DN の値をオブジェクトの `moveProxyTrigger` 属性から削除します。

移動が「再実行」ステータスとなり失敗した場合は（通常は、同じオブジェクトの前の移動がまだ完了していないためです）、加入者チャンネルを通じてステータスが Identity Manager に返されます。Identity Manager は、移動が成功するか、他の理由で失敗するまで、元のイベントを 30 秒ごとに再送信します。

移動プロキシサービスの設定

移動プロキシサービスの設定は、マスタレプリカを保存するサーバ上で実行します。このサービスが必要になる状況の概要については、[258 ページの「移動プロキシサービスの概要」](#)を参照してください。

この手順を終了後、サーバ上で実行されているドライバを、移動プロキシドライバに移動を委任するよう設定し、マスタレプリカで移動を実行できるようにします。

- 1 マスタレプリカのあるサーバに Identity Manager がまだインストールされていない場合は、インストールします。

2 移動プロキシサービスの次のファイルが Identity Manager とともにインストールされていることを確認します。インストールされていない場合は、製品のディストリビューションまたは **Novell サポート** (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm>) から入手します。

- ◆ loopback.jar

これは、移動プロキシサービスを実行するために必要なループバックシムファイルです。このドライバシムファイルは、各 OS の /lib ディレクトリに配置する必要があります。

- ◆ moveproxy.xml

これは、ドライバ設定ファイルです。他のドライバ設定ファイルが保存されているデフォルトの場所に配置されていない場合は、**ステップ 4** でドライバオブジェクトを作成する際に、その場所を参照する必要があります。

- ◆ moveproxy.xlf

このファイルは、ドライバ設定 moveproxy.xml をインポートする場合に表示されるプロンプトを作成します。

- ◆ mvproxy_client_publisher_command_transformation.xsl

このファイルは、移動プロキシサービスに移動を委任する各ドライバに追加する Command Transformation (コマンド変換) スタイルシートを提供します。**260 ページの「移動プロキシサーバに移動を委任するための他のドライバの設定」**を参照してください。

3 eDirectory のスキーマに DirXML-moveProxyTrigger という名前の属性が含まれていることを確認します。含まれていない場合は、mvproxy.sch ファイルおよびプラットフォームに適したユーティリティ (NetWare では nwconfig、Win32 では install.dlm、および UNIX では ndssch) を使用し、eDirectory スキーマを拡張します。

Novell サポート (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm>) にアクセスし、mvproxy.sch ファイルを入手します。

注:すでにスキーマに DirXML-moveProxyTrigger 属性が含まれている場合は、**ステップ 2** のリストに表示されているファイルも製品のディストリビューションに含まれています。スキーマにこの属性が含まれておらず、mvproxy.sch スキーマ拡張ファイル、および**ステップ 2** のリストに表示されているその他のファイルを Novell サポートから入手する場合、Novell サポートから入手したファイルでは、DirXML-moveProxyTrigger ではなく moveProxyTrigger という名前の属性が使用されていることに注意してください。設定方法は同じですが、属性の名前が多少異なります。

4 マスタレプリカを保存するサーバの新しい DirXML ドライバオブジェクトを作成し、moveproxy.xml をインポートしてドライバ設定を作成します。

DirXML エンジン、ループバックドライバシムを使用し、ドライバオブジェクトを実行します。

5 作成した新しいドライバオブジェクトについて、加入者および発行者のフィルタを編集し、移動を代わりに実行するオブジェクトクラスが含まれるようにします。これらの各クラスのフィルタに DirXML-moveProxyTrigger (または moveProxyTrigger) 属性を追加します。

フィルタに含まれるクラスの他の属性は追加しないでください。

- 6 目的の [Driver Startup] オプションを [Driver object] に設定し、ドライバを再起動します。
ドライバの設定が完了し、正しく動作した後は、[Driver Startup] オプションは [Automatic] にすることをお勧めします。
- 7 260 ページの「移動プロキシサーバに移動を委任するための他のドライバの設定」に説明されているとおり、他のサーバのドライバが移動プロキシサービスを使用するよう設定されていることを確認します。

移動プロキシサーバに移動を委任するための他のドライバの設定

このサービスが必要になる状況の概要については、258 ページの「移動プロキシサービスの概要」を参照してください。

- 1 258 ページの「移動プロキシサービスの設定」の作業を完了していることを確認します。
- 2 ドライバの DirXML-Publisher オブジェクトに、DirXML-Stylesheet オブジェクトを作成します。
- 3 mvproxy_client_publisher_command_transformation.xml という名前のファイルが Identity Manager にインストールされていることを確認します。
このスタイルシートは、259 ページのステップ 2 で確認した移動プロキシのファイルの 1 つです。インストールされていない場合は、製品のディストリビューションまたは [Novell サポート \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm) から入手します。
- 4 作成した新しいスタイルシートオブジェクトで、[Edit XML property] ページに移動し、mvproxy_client_publisher_command_transformation.xml という名前のファイルの内容を貼り付けます。
- 5 次のいずれかを実行し、スタイルシートが Command Transformation Rule (コマンド変換ルール) の一部となるようにします。
 - ◆ DirXML-PublisherオブジェクトにCommand Transformation Rule (コマンド変換ルール) が含まれていない場合は、新しいスタイルシートをコマンド変換ルールにします。
 - ◆ DirXML-PublisherオブジェクトにCommand Transformation Rule (コマンド変換ルール) がすでに含まれている場合は、ルールチェーンを使用し、既存のコマンド変換ルールの次の情報を新しいスタイルシートに設定します。
- 6 加入者または発行者のどちらかのチャンネルで使用されるスタイルシートが srcCommandProcessor または destCommandProcessor を通じて eDirectory に移動を生成および送信している場合は、ステップ 5 で作成した新しい Command Transformation Rule (コマンド変換ルール) で生成されるものと同様の変更イベントを送信するように、スタイルシートを変更します。

Manual Task Service Driver (Workflow Service Request Driver)

ドライバの用途がわかりやすいように、Identity Manager の Workflow Request Service Driver は、Manual Task Service Driver という名前に変更されています。

Manual Task Service Driver 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、Novell 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、Manual Task Service Driver 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、加入者チャンネルのルールと電子メールテンプレート、および発行者チャンネルの Web サーバテンプレートとルールです。

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。

詳細については、『*Manual Task Service Driver Implementation Guide (Manual Task Server Driver 実装ガイド)* (<http://www.novell.com/documentation/lg/dirxmldrivers/index.html>)』を参照してください。

12 高可用性

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 eDirectory および Identity Manager を使用するには、いくつかの手順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。

- ◆ 263 ページの「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」
- ◆ 267 ページの「SuSE Linux についてのケーススタディ」

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 を設定する手順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りますということです。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/dib 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。共有ストレージに存在する必要のある eDirectory 設定データは、他にもあります。

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。

- ◆ [264 ページの「eDirectory のインストール」](#)
- ◆ [264 ページの「Identity Manager のインストール」](#)
- ◆ [265 ページの「NICI データの共有」](#)
- ◆ [265 ページの「eDirectory および Identity Manager のデータの共有」](#)
- ◆ [267 ページの「DirXML ドライバについての考慮事項」](#)

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。
セカンダリノードには個別のツリーはありません。
- 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。

Identity Manager のインストール

- 1 [DirXML Server] オプションを使用し、プライマリクラスタノードに Identity Manager 2.0.1 (DR1) 以降をインストールします。
インストールプロセスにより、DirXML 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、[DirXML Server] 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、DirXML 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。

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

- 1 セカンダリクラスタノード上の `/var/novell/nici` を別の名前（たとえば `/var/novell/nici.sav`）に名前変更します。
- 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。

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 のデフォルトの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。これらの手順は、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。

- ◆ [265 ページの「プライマリノード上の手順」](#)
- ◆ [267 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` to `/shared/var/nds` からの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
/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の上書きします）。

- ◆ 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 への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上の手順が終了したら、クラスタサービスを起動します。eDirectory および Identity Manager がプライマリノード上で起動します。

DirXML ドライバについての考慮事項

DirXML 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、Manual Task Driver のテンプレートディレクトリなどです。

SuSE Linux についてのケーススタディ

SuSE LINUX Enterprise Server 8 を使用した場合の共有ストレージ上の Identity Manager の実行については、TID 番号 [NOVL97459](http://support.novell.com/cgi-bin/search/searchtid.cgi?NOVL97459.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?NOVL97459.htm>) の説明を参照してください。

13

Nsure Audit によるログとレポート

Nsure™ Identity Manager では、Novell® Nsure Audit を使用して監査とレポートを実行する機能が装備されています。

Nsure 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。Nsure Audit、および Identity Manager 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細な情報が提供されます。この情報は、事前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、Nsure 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。

Nsure Audit に送信されるメッセージのタイプは、レポートと通知サービス (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追加レベルを追加します。

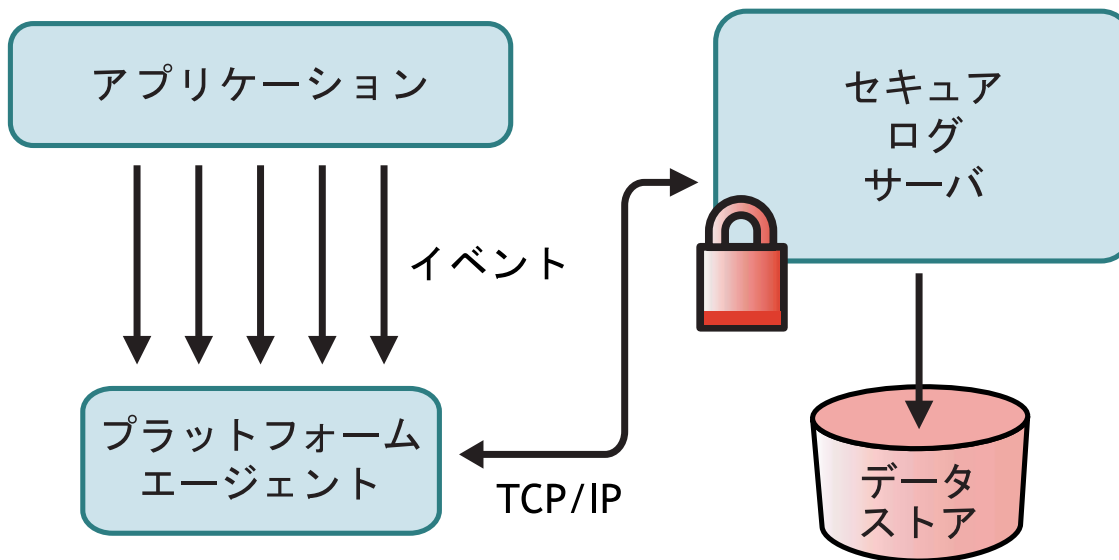
レポートと通知サービス (RNS)

レポートと通知サービス (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、エンジンは引き続き RNS 機能を実行します。Nsure 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くなるため、Nsure 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 (DirXML 1.1a 管理ガイド)* (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html>)』を参照してください。

概要

Nsure 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ログできます。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、Nsure Audit の上位レベルのアーキテクチャを示します。



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 Nsure 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。

Nsure Audit の設定

「概要」で説明したように、Nsure 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 Nsure Audit 1.0.2 の一部としてインストールされます。

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 Nsure Audit System Components for DirXML] オプションを選択すると、インストールされます。Identity Manager と同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： DirXML[®] エンジンのインストール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、プラットフォームエージェントと Identity Manager がリンクされる前に、Identity Manager を再起動する必要があります。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がインストールされた後、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 Nsure 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。

セキュアログサーバの設定

注： Nsure Audit のセキュアログサーバは、DirXML には含まれていません。セキュアログサーバは、Nsure Audit 1.0.2 の一部です。Nsure Audit 1.0.2 のダウンロードの詳細については、[Nsure Audit の製品ページ \(http://www.novell.com/products/nsureaudit\)](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 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ログできます。Nsure Audit には、Nsure 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。この高度なレポートツールを使用するには、ODBC コネクタを持つデータベースが必要です。

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、Nsure Audit 1.0.2 のインストールにも含まれています。また、[Novell Nsure Audit マニュアルの Web サイト \(http://www.novell.com/documentation/lg/nsureaudit\)](http://www.novell.com/documentation/lg/nsureaudit) にある『*Nsure Audit 1.0.2 Administration Guide (Nsure Audit 1.0.2 管理ガイド)*』で参照することもできます。

ログの設定

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、またはログする各イベントを個別に選択し、ログするイベントを設定できます。設定の変更もログされます。

275 ページの「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ログされ、DirXML 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、**277 ページの「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されます。

ログするイベントの選択

ドライバセットで実行する手順：

- 1 iManager で、[DirXML Driver Management] 役割を開き、[Overview] タスクを選択します。
- 2 [Driver Set] の名前のリンクをクリックします。[Modify Object] ウィンドウが表示されます。
- 3 [DirXML] タブで [Log Level] リンクをクリックします。次のログオプションを指定できます。

オプション	説明
Log Errors	<p>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します。</p> <p>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。</p>
Log Errors and Warnings	<p>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します。</p> <p>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。</p>
Log Specific Events	<p>このオプションでは、ログ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、常にログされます。</p> <p>エラーまたは警告以外のイベントをログするには、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するときは、エラーおよび警告を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、274 ページの「DirXML イベント」を参照してください。</p>
Only Update the Last Log Time	<p>ユーザ定義イベントのみをログします。イベントが発生した場合、最終ログ時刻がアップデートされるため、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。</p>
Logging Off	<p>ユーザ定義イベントのみをログします。</p>
Maximum Number of Entries in the Log	<p>この設定では、ステータスログにログするエントリの最大数を指定します。詳細については、280 ページの「ステータスログの表示」を参照してください。</p>

- 4 ログするイベントをすべて選択したら、[OK] をクリックします。

ドライバで実行する手順：

- 1 iManager で、[DirXML Driver Management] 役割を開き、[Overview] タスクを選択します。
- 2 ドライバのステータスアイコンをクリックして、[Edit Properties] を選択します。
- 3 [DirXML] タブで [Log Level] リンクをクリックします。デフォルトでは、ドライバは、ドライバセットのログ設定を継承するよう設定されています。このドライバについてのみログするイベントを選択するには、次の選択を解除します。

Use log settings from the DriverSet, DS.Novell

The following log settings are from the DriverSet and cannot be changed on this page. To modify the DriverSet's settings, [click here](#).

- 4 次のログオプションを指定できます。

オプション	説明
Log Errors	<p>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します。</p> <p>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。</p>
Log Errors and Warnings	<p>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します。</p> <p>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。</p>
Log Specific Events	<p>このオプションでは、ログ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、常にログされます。</p> <p>エラーまたは警告以外のイベントをログするには、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するときは、エラーおよび警告を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、274 ページの「DirXML イベント」を参照してください。</p>
Only Update the Last Log Time	<p>ユーザ定義イベントのみをログします。イベントが発生した場合、最終ログ時刻がアップデートされるため、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。</p>
Logging Off	<p>ユーザ定義イベントのみをログします。</p>
Maximum Number of Entries in the Log	<p>この設定では、ステータスログにログするエントリの最大数を指定します。詳細については、280 ページの「ステータスログの表示」を参照してください。</p>

- 5 ログするイベントをすべて選択したら、[OK] をクリックします。

DirXML イベント

DirXML によりログされるすべてのイベントのリストは、別の HTML ファイル [DirXML Events \(dirxml_events.html\)](#) にあります。

ドライバの起動および停止のイベント

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。次の表は、このようなイベントについて詳しく示します。

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するには、[Log Specific Events] 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するには、[Log Errors and Warnings] を選択するか、[Log Specific Events] 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 Nsure Audit の通知を作成する方法の詳細については、[279 ページの「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。次の表は、このようなイベントについて詳しく示します。

イベント	ログレベル	情報
DirXML_Error	LOG_ERROR	すべての DirXML エラーがこのイベントをログします。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。 エラーをログするには、[Log Errors]、[Log Errors and Warnings] を選択するか、[Log Specific Events] 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	すべての DirXML 警告がこのイベントをログします。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。 ドライバの停止をログするには、[Log Errors and Warnings] を選択するか、[Log Specific Events] 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 Nsure Audit の通知を作成する方法の詳細については、[279 ページの「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されます。

イベント	ログレベル	情報
Remote Loader Start	LOG_INFO	<p>すべての DirXML エラーがこのイベントをログします。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。</p> <p>エラーをログするには、[Log Errors]、[Log Errors and Warnings] を選択するか、[Log Specific Events] オプションを使用してこのイベントを選択します。</p>
Remote Loader Stop	LOG_INFO	<p>すべての DirXML 警告がこのイベントをログします。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。</p> <p>ドライバの停止をログするには、[Log Errors and Warnings] を選択するか、[Log Specific Events] オプションを使用してこのイベントを選択します。</p>
Remote Loader Connection Established	LOG_INFO	<p>すべての DirXML 警告がこのイベントをログします。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。</p> <p>ドライバの停止をログするには、[Log Errors and Warnings] を選択するか、[Log Specific Events] オプションを使用してこのイベントを選択します。</p>
Remote Loader Connection Dropped	LOG_INFO	<p>すべての DirXML 警告がこのイベントをログします。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。</p> <p>ドライバの停止をログするには、[Log Errors and Warnings] を選択するか、[Log Specific Events] オプションを使用してこのイベントを選択します。</p>

これらのイベントに基づいて Nsure Audit の通知を作成する方法の詳細については、[279 ページの「イベントに基づく通知の送信」](#)を参照してください。

ユーザ定義イベント

Identity Manager では、独自のイベントログを Nsure Audit に設定できます。イベントをログするには、Policy Builder 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ログできます。

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。Nsure Audit では、この ID は、DirXML 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、ログ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。

ログレベル	説明
log-emergency	DirXML 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	DirXML の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	DirXML またはドライバによって処理できるエラーを説明するイベント。
log-warning	問題を表さ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	いずれかの重要度を持つポジティブイベント。
log-debug	サポートまたはエンジニアが DirXML 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。

Policy Builder を使用したイベントの生成

Policy Builder では、[Generate Event] アクションを選択してイベントをログします。

- 1 イベントを生成するために満たす必要がある条件を選択し、[Generate Event] 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 [Enter Strings] フィールドの横の  アイコンをクリックし、Named String Builder を起動します。
- 5 Named String Builder 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。

Strings			
<input type="checkbox"/> Name:	text1	String tokens:	Operation Attribute("Given Name") 
<input type="checkbox"/> Name:	text2	String tokens:	Operation() 
<input type="checkbox"/> Name:	value	String tokens:	"1000" 

- 6 [OK] をクリックして Policy Builder に戻り、ポリシーの続きを作成します。

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、Nsure Audit に送信されます。

ステータスレベル	ステータスイベント ID
Success (成功)	EV_LOG_STATUS_SUCCESS (1)
Retry (再試行)	EV_LOG_STATUS_RETRY (2)
Warning (警告)	EV_LOG_STATUS_WARNING (3)
Error (エラー)	EV_LOG_STATUS_ERROR (4)
Fatal (致命的)	EV_LOG_STATUS_FATAL (5)
User Defined (ユーザ定義)	EV_LOG_STATUS_OTHER (6)

次の例では、Nsure Audit イベント 0x004、value=7777、およびレベル EV_LOG_STATUS_ERROR のイベントが生成されます。

```
<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、Nsure Audit イベント 0x004、value1=7778、およびレベル EV_LOG_STATUS_ERROR のイベントが生成されます。

```
<xsl:message>
  <status level="error" text1="This would be text1" text2="This would be
text2" value="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>
```

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。属性は複数值整数で、各値はログされるイベント ID を識別します。

イベントをログする前に、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 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。

クエリおよびレポート

Nsure Audit では、Nsure 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の 2 つのツールを用意しています。Nsure Audit iManager プラグイン、および Nsure Audit Report (LReport) です。

Nsure 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。

Nsure Audit Report は、Windows ベースの ODBC 準拠アプリケーションで、SQL クエリ構文または 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。

Nsure Audit iManager プラグインへのアクセス、または Nsure Audit Report の設定を行うには、『*Nsure Audit 1.0.2 Administration Guide (Nsure Audit 1.0.2 管理ガイド)*』の手順に従います。このガイドは、[Novell Nsure Audit のマニュアルの Web サイト \(http://www.novell.com/documentation/lg/nsureaudit\)](http://www.novell.com/documentation/lg/nsureaudit) から入手できます。

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) を提供しています。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。

Nsure 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。Nsure Audit Report でレポートを使用する方法の詳細については、『*Nsure Audit 1.0.2 Administration Guide (Nsure Audit 1.0.2 管理ガイド)*』の「[Working with Reports in Nsure Audit Report \(Nsure Audit Report でのレポートの操作\)](http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html) (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html)」を参照してください。

Identity Manager のイベントの表示

- 1 [Nsure Audit Report Workspace] で [Events] 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 DirXML 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、イベントの属性を表示します。
- 2 DirXML イベントのクエリを実行するには、[Workspace] でイベントを右クリックし、[Define Query] を選択します。
- 3 [Query Expert] が表示されたら、間隔を指定し、イベントを確認します。
- 4 このクエリを実行するには、[Workspace] の [Query] タブを選択した後、クエリ名を右クリックして [Run] を選択します。

クエリは、SQL 構文を使用しても作成できます。すべての DirXML 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。

イベントに基づく通知の送信

Nsure 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、ログチャンネルに送信できます。また、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できます。

通知の作成の詳細については、『*Nsure Audit 1.0.2 Administration Guide (Nsure Audit 1.0.2 管理ガイド)*』の「Configuring Filters and Event Notifications (フィルタとイベント通知の設定) (<http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/a10lg08.html#a10lg08>)」を参照してください。

ステータスログの使用

Nsure Audit で提供される機能に加え、Identity Manager では指定した数のイベントをドライバセットオブジェクトまたはドライバセットにログします。これらのステータスログは、Identity Manager の最新のアクティビティを示します。ログが設定サイズに達すると、最新のイベントを記録するための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、長期間トラックするイベントは、Nsure Audit またはレポートと通知サービス (RNS) にログすることをお勧めします。

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。これは、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、ログ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。

ドライバセットへのログサイズの設定：

- 1 iManager で、[DirXML Driver Management] 役割を開き、[Overview] タスクを選択します。
- 2 [Driver Set] の名前のリンクをクリックします。[Modify Object] ウィンドウが表示されます。
- 3 [DirXML] タブで [Log Level] リンクをクリックします。[Maximum number of entries in the log] フィールドで、最大ログサイズを指定します。

Maximum number of entries in the log (50 - 500):

- 4 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、[DirXML Driver Management] 役割を開き、[Overview] タスクを選択します。
- 2 ドライバのステータスアイコンをクリックして、[Edit Properties] を選択します。
- 3 [DirXML] タブで [Log Level] リンクをクリックします。[Maximum number of entries in the log] フィールドで、最大ログサイズを指定します。

Maximum number of entries in the log (50 - 500):

- 4 最大値を指定したら、[OK] をクリックします。

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 [status log] 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ンネル
- ◆ セット内の各ドライバの加入者チャンネル

発行者および加入者のチャン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ン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含まれるのは、ドライバセット内の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です。エンジンメッセージはすべてログされます。

A

Novell Identity Manager 製品のアクティベーション

ここでは、Novell® Nsure™ Identity Manager に基づく製品のアクティベーションの仕組みについて説明します。Identity Manager Professional または Server edition およびドライバグループは、インストール後 90 日以内にアクティベートする必要があります。実行しない場合は、シャットダウンされます。90 日間はいつでも、または後に、Identity Manager 製品をアクティベートするよう選択できます。

注： ドライバをアクティベートすることで、現在の設定が変更されたり、新バージョンのドライバシムがインストールされたりすることはありません。単にドライバがアクティベート済みの状態になります。

Identity Manager およびドライバグループをアクティベートするには、次の 2 つの方法のどちらかを使用します。1 番目の方法には、次の作業が含まれます。

- ◆ Identity Manager 製品ライセンスの購入
- ◆ ジェネリックキーによる Identity Manager のアクティベーション
- ◆ プロダクトアクティベーションキーのインストール

2 番目の方法には、次の作業が含まれます。

- ◆ Identity Manager 製品ライセンスの購入
- ◆ プロダクトアクティベーション要求の作成
- ◆ プロダクトアクティベーション要求の送信
- ◆ プロダクトアクティベーションキーのインストール

この節では、次のトピックについて説明します。

- ◆ 288 ページの「Identity Manager および DirXML ドライバのプロダクトアクティベーションの表示」

Identity Manager 製品ライセンスの購入

Identity Manager 製品ライセンスを購入するには、Novell Nsure Identity Manager: ご購入の Web ページ (<http://www.novell.com/products/nsureidentitymanager/howtobuy.html>) を参照してください。

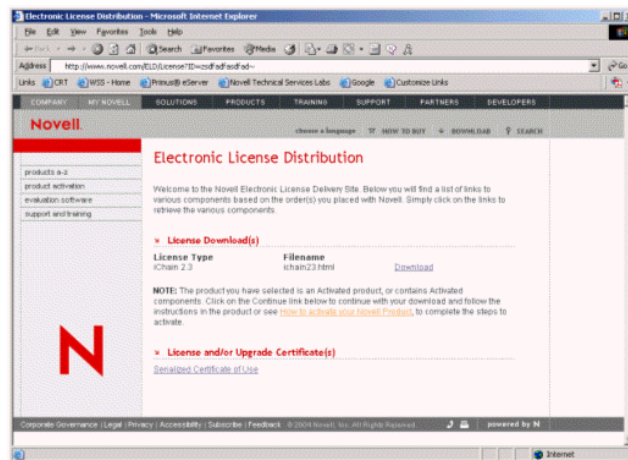
製品ライセンスを購入すると、Novell より電子メールでお客様 ID が送信されます。電子メールには、ジェネリックキーを取得できる Novell サイトの URL も記載されています。お客様 ID がわからない場合、またはお客様 ID を受け取っていない場合は、Novell アクティベーションセンターに連絡してください。米国の電話番号は 1-800-418-8373 です。その他の地域では、1-801-861-8373 です (801 市外局番を使用した通話には料金がかかります)。

ジェネリックキーによる Identity Manager のアクティベーション

- 1 ライセンスを購入すると、Novell より電子メールでお客様 ID が送信されます。電子メールの「Order Detail」セクションの下には、ジェネリックキーを取得するためのサイトへのリンクも記載されています。リンクをクリックしてサイトに移動します。

重要：ジェネリックキーを取得するリンクにアクセスするために使用できる電子メールアドレスは、3種類だけです。3つを超える電子メールアドレスを使用してリンクにアクセスしようとすると、セキュリティリスクとみなされ、アクセスが拒否されます。また、ジェネリックライセンスの取得情報が記載された「Order Detail」セクションを含む電子メールを受信するのは、お客様 ID の所有者 / 契約として指定された電子メールアドレスのみです。受信した電子メールに「Order Detail」セクションが含まれていない場合は、組織内でお客様 ID を持つユーザーに問い合わせ、ジェネリックキーを取得する必要があります。

リンクをクリックすると、次の図と同じようなページが表示されます。：



- 2 [license download] リンクをクリックし、保存 ([download]) するか、.html ファイルを開きます。

ファイルが開くと、次の図に示したものと同様の内容が表示されます。:



- 3 Identity Manager およびドライバのアクティベーションの方法については、[286 ページの「プロダクトアクティベーションキーのインストール」](#)に進んでください。

プロダクトアクティベーション要求の作成

プロダクトアクティベーション要求を作成するには、お客様 ID を使用します。Identity Manager 製品を購入すると、お客様 ID が記載された電子メールが Novell より会社の主要担当者（製品ライセンスを購入した担当者）に送信されます。

お客様 ID がわからない場合またはお客様 ID を受け取っていない場合は、Novell アクティベーションセンターに連絡してください。米国の電話番号は 1-800-418-8373 です。その他の地域では、1-801-861-8373 です（場合によっては、801 市外局番を使用した通話には長距離通話料金がかかります）。

注： 製品ライセンスを購入する個人は、お客様 ID が記載された電子メールを受信します。会社が購入エージェントを通じてこの取引を処理する場合は、この個人に確認してお客様 ID を取得しなければならないことがあります。

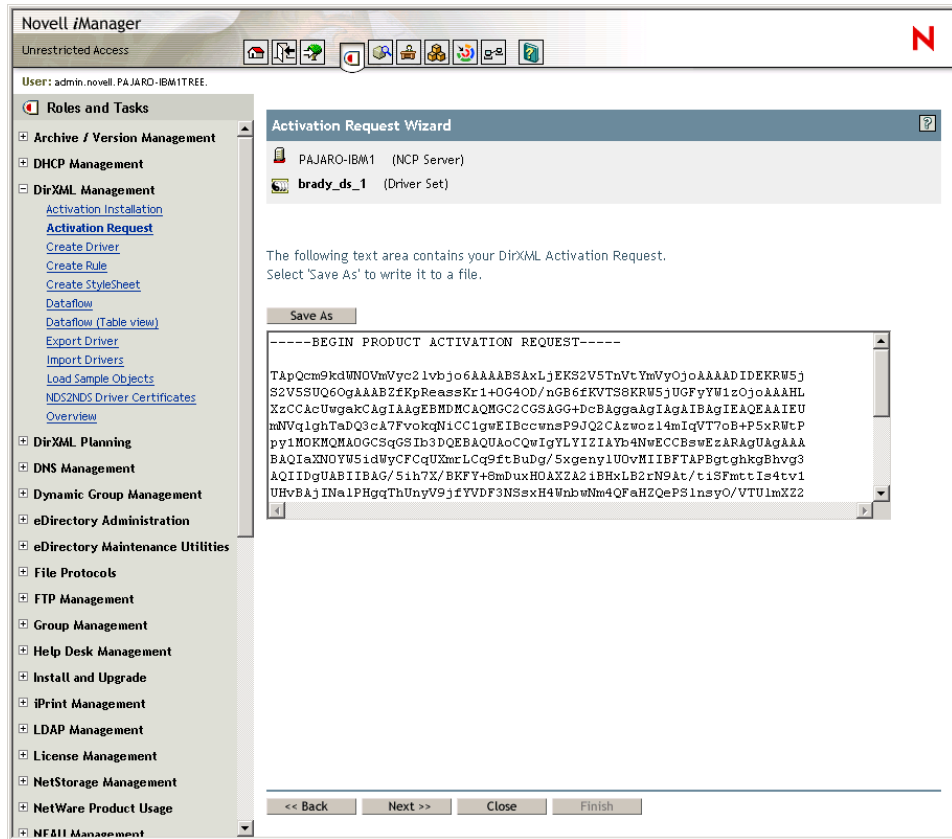
Identity Manager をアクティベートするためのプロダクトアクティベーション要求を作成する前に、ドライバセットオブジェクトを作成する必要があります。

- 1 <http://serveripaddress/nps/iManager.html> に移動し、iManager を起動します。
- 2 [DirXML Management] > [Activation Request] の順にクリックします。
- 3 アクティベートするドライバセットを参照し、[Next] をクリックします。

注： ドライバセットがサーバに関連付けられていない場合、または複数のサーバに関連付けられている場合は、ドライバセットに関連付けるサーバを選択するよう、プロンプトが表示されます。

- 4 Novell お客様 ID を入力し、[Next] をクリックしてアクティベーション要求ファイルを作成します。

お客様 ID およびサーバのツリーについての識別情報は、プロダクトアクティベーション要求に格納されます。



- 5 テキスト領域に表示されるプロダクトアクティベーション要求をクリップボードにコピーするか、要求を直接ファイルに保存し、[Next] をクリックします。

この情報は、後に Novell Product Activation (Novell プロダクトアクティベーション) の Web サイトで必要になります。

重要： プロダクトアクティベーション要求の内容は編集しないでください。

- 6 ハイパーリンクをクリックし、Novell Product Activation (Novell プロダクトアクティベーション) の Web サイト (<http://www.novell.com/products/activation>) にアクセスします。

または、

[Finish] をクリックし、iManager のメインメニューに戻ります。

注： アクティベーションプロセスを続行するには、Novell Product Activation (Novell プロダクトアクティベーション) の Web サイト (<http://www.novell.com/products/activation>) で、このプロダクトアクティベーション要求を Novell に送信する必要があります。詳細については、284 ページの「[プロダクトアクティベーション要求の送信](#)」を参照してください。

プロダクトアクティベーション要求の送信

プロダクトアクティベーション要求を作成したら、Novell Product Activation (Novell プロダクトアクティベーション) の Web サイト (<http://www.novell.com/products/activation>) から Novell に送信します。すると、プロダクトアクティベーションキーが記載された電子メールが、Novell より送信されます。スイートまたはドライバグループのアクティベーションには、このキーを使用します。

1 [Product Activation \(プロダクトアクティベーション\) の Web サイト \(http://www.novell.com/products/activation\)](http://www.novell.com/products/activation) に移動し、[Identity Manager product(s)] をクリックします。

2 概要画面に従い、プロンプトが表示されたら、MyNovell アカウントにログインします。

Product Activation (プロダクトアクティベーション) の Web サイトにアクセスするには、MyNovell アカウントが必要です。まだアカウントを持っていない場合には、プロダクトアクティベーションサイトにアクセスするときに無償アカウントを作成できます。

3 [Browse] をクリックし、プロダクトアクティベーション要求ファイルへのパスを指定するか、プロダクトアクティベーション要求のテキストをテキスト領域に貼り付けます。

プロダクトアクティベーション要求をフロッピーディスクにコピーした場合は、作業しているコンピュータでその要求が使用できることを確認してください。

重要: プロダクトアクティベーション要求の内容は編集しないでください。

4 [Submit] をクリックします。

アクティベートできる購入製品が表示されます。

The screenshot shows the Novell Product Activator web interface. At the top, there is a navigation menu with links for COMPANY, MY NOVELL, SOLUTIONS, PRODUCTS, TRAINING, SUPPORT, PARTNERS, and DEVELOPERS. Below the menu is the Novell logo and a search bar. The main content area is titled "Novell Product Activator" and includes a "Company Information" section with details for ACME Design, including address and contact email. Below this is a "New Activation Request" section with explanatory text. A table lists product licenses with columns for Product Description, Date Purchased, Quantity Purchased, Licensed Units, and Previous Activations. A "Submit" button is located at the bottom of the table. A large red "N" logo is positioned in the bottom left corner of the page content.

Product Description	Date Purchased	Quantity Purchased	Licensed Units	Previous Activations
<input checked="" type="checkbox"/> DirXML Starter Pack -DirXML Engine -DirXML Driver for eDirectory -DirXML Driver for Active Directory and Exchange 2000 -DirXML Driver for NT Domain	05/06/2003	1	1	5 (details)

5 アクティベートする購入製品をマークします。

一度に1つの購入製品のみをアクティベートできます。現在アクティベートしている購入製品をマークします。リストに表示された他の製品をアクティベートする必要があり、それらが同じツリーで使用される場合は、プロダクトアクティベーション要求を再度送信します。異なるツリーで使用される場合は、新しいプロダクトアクティベーション要求を作成し、要求を送信してキーを取得します。

6 [Submit] をクリックします。

Novell は、送信されたプロダクトアクティベーション要求に基づいてプロダクトアクティベーションキーを作成し、電子メールでキーを送信します。キーのコピーは、主要担当者にも送信されます。

注：会社によっては、キーを受信できる権限がある従業員を制限している場合もあります。お客様 ID を使用する権利をユーザ自身を持っていないこともあります。この場合は、[Submit] をクリックすると、通知が主要担当者に送信されます。主要担当者は、ユーザがキーを電子メールで受信する前に、該当するユーザがお客様 ID を使用することを承認する必要があります。

プロダクトアクティベーションキーのインストール

プロダクトアクティベーションキーは、iManager でインストールします。次に、プロダクトアクティベーションキーのインストール手順を説明します。

1 プロダクトアクティベーションキーが記載されている Novell からの電子メールを開きます。

2 次のいずれかの手順を実行します。

- ◆ プロダクトアクティベーションキーファイルを保存します。

または、

- ◆ プロダクトアクティベーションキーファイルを開き、プロダクトアクティベーションキーの内容をクリップボードにコピーします。

重要：プロダクトアクティベーションキーの内容は編集しないでください。

3 iManager を開きます。

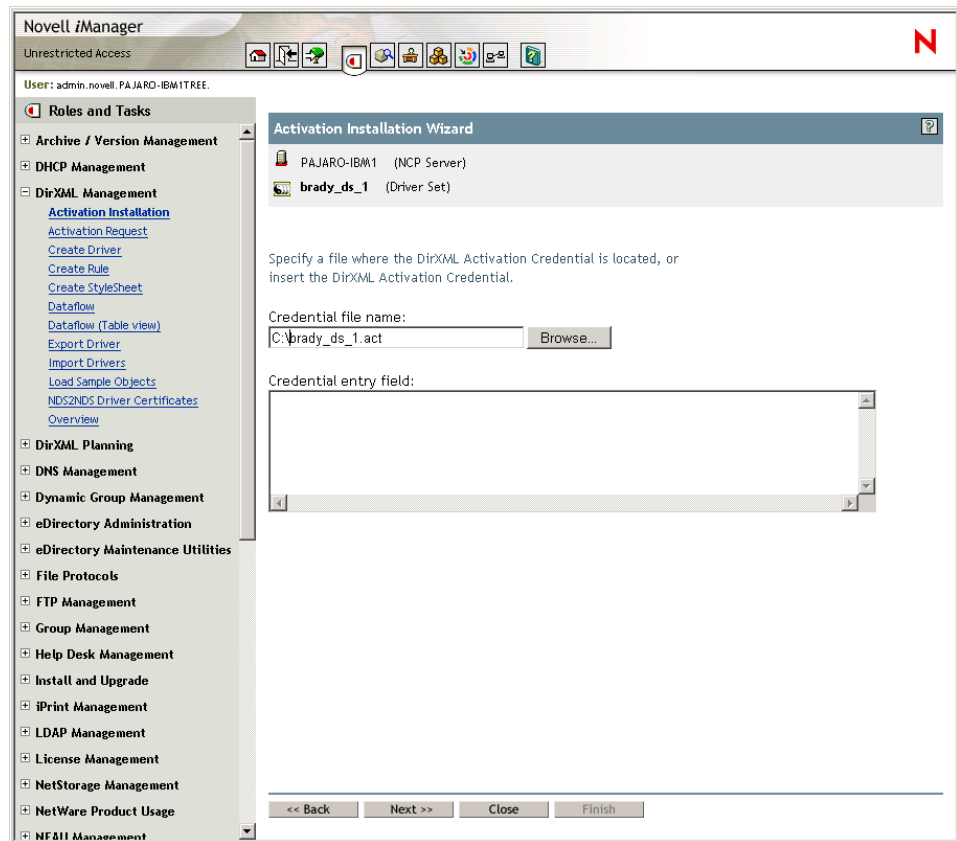
4 [DirXML Utilities] > [Activation Installation] の順に選択します。

5 ドライバセットを選択または参照して、[Next] をクリックします。

重要：最初にプロダクトアクティベーション要求を作成したツリーと同じツリーにあるドライバセットを選択してください。

6 ドライバセットがサーバに関連付けられていない場合、または複数のサーバに関連付けられている場合は、ドライバセットに関連付けるサーバを選択してから [Next] をクリックします。

インストールを行うダイアログボックスが表示されます。



7 次のいずれかの手順を実行します。

- ◆ DirXML アクティベーションキーを保存した場所を指定し、[Next] をクリックします。
- または、
- ◆ DirXML アクティベーションキーの内容をテキスト領域に貼り付け、[Next] をクリックします。

8 [Finish] をクリックします。

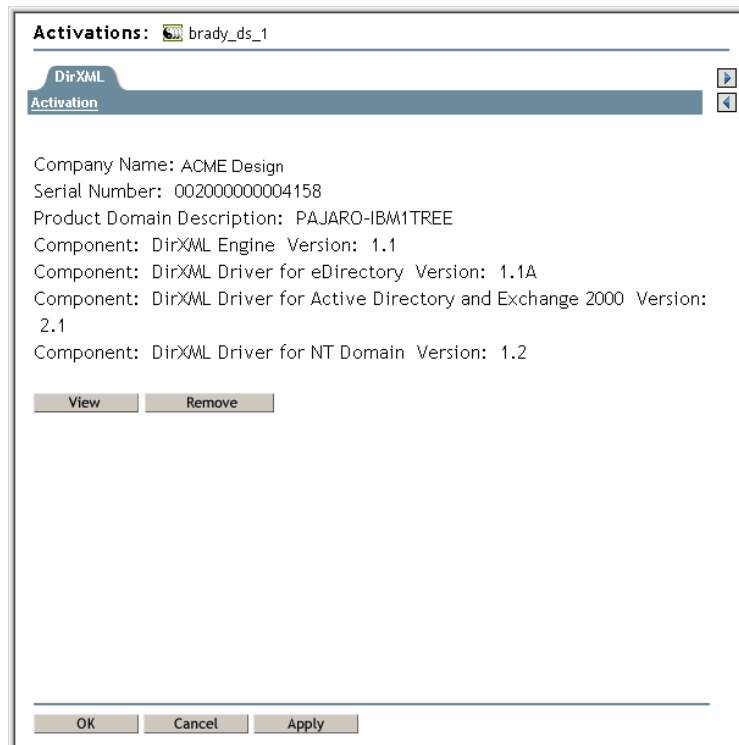
注： アクティベーションは、ドライバを含むドライバセットごとに実行する必要があります。ドライバセットが同じツリーにある限り、同じプロダクトアクティベーションキーを使用して他のドライバセットもアクティベートできます。プロダクトアクティベーションキーは、プロダクトアクティベーション要求が作成されたツリーでのみ使用できます。

Identity Manager および DirXML ドライバのプロダクトアクティベーションの表示

ドライバセットごとに、DirXML エンジンおよびドライバにインストールしたプロダクトアクティベーションキーを表示できます。プロダクトアクティベーションキーを表示する

- 1 iManager を開きます。
- 2 [eDirectory Administration] > [Modify Object] の順にクリックします。
- 3 アクティベーション情報を表示するドライバセットまたはドライバを、[object name] フィールドに入力します。
または、
アクティベーション情報を表示するドライバセットまたはドライバを参照します。
- 4 [DirXML] タブから [Activation] を選択します。

DirXML および DirXML ドライバのアクティベーションキーが、このページに表示されます。



アクティベーションキーのテキストを表示できます。エラーがレポートされた場合は、アクティベーションキーを削除できます。

注：プロダクトアクティベーションキーをドライバセットにインストールした後も、ドライバ名の横に [Activation Required] と表示されることがあります。この場合、ドライバを再起動すると、このメッセージは表示されなくなります。

B

eDirectory 8.6.2 および eDirectory 8.7.3 の機能サポート

次の表は、eDirectory 8.6.2 を実行している場合にサポートされない機能と、eDirectory 8.7.3 に関するいくつかの考慮事項を示します。

注： eDirectory 8.6.2 より前のバージョンをレガシー NDS® と呼びます。Identity Manager に付属の DirXML エンジンも、レガシー NDS では実行できません。

Identity Manager は eDirectory 8.7 ではテストされていないため、eDirectory 8.7 はサポートされません。eDirectory 8.7.3 はサポートされており、eDirectory 8.7 から無償でアップグレードできます。

機能	eDirectory 8.6.2	eDirectory 8.7.3
Policy Builder	サポートされます。	サポートされます。
DirXML Script	サポートされます。	サポートされます。
Password Policy (パスワードポリシー): Advanced Password Rules (詳細パスワードルール)	<p>パスワードルールにはユニバーサルパスワードが必要なため、eDirectory 8.6.2 上の Identity Manager ではサポートされません。</p> <p>ただし、混在環境では、2つのツリーを同期化し、一方が eDirectory 8.7.3 の場合、8.6.2 ツリーには Advanced Password Rule (詳細パスワードルール) を適用できます。たとえば、8.7.3 が実行されている識別ポールドがあり、そのツリー内でパスワードの変更のみをユーザに許可している場合は、識別ポールドのユニバーサルパスワードをオンにして、eDirectory 8.6.2 ツリーに一方方向で同期化できます。ユニバーサルパスワードを NDS パスワードに同期化し、パスワードルールを適用できます。</p> <p>eDirectory 8.6.2 を使用する場合、使用できるパスワード制限は、NDS パスワードについて使用できる制限となります。</p>	<p>Password Policy (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場合、サポートされます。</p> <p>接続システムで Password Policy (パスワードポリシー) を適用することもできます。</p>

機能	eDirectory 8.6.2	eDirectory 8.7.3
Password Policy (パスワードポリシー): パスワードを忘れた場合のセルフサービス	<p>次を除くすべての機能がサポートされます。</p> <ul style="list-style-type: none"> ◆ ページ上でのパスワードのリセットをユーザに許可する ◆ 現在のパスワードをユーザに電子メールで送信する <p>この機能には、逆方向パスワードが必要です。eDirectory 8.6.2 はユニバーサルパスワードをサポートしないため、この機能は使用できません。</p>	<p>Password Policy (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場合は、すべての機能がサポートされます。</p> <p>Password Policy (パスワードポリシー) でユニバーサルパスワードが無効になっている場合、管理者は、次のオプションをポリシーのユーザに提供することはできません。</p> <ul style="list-style-type: none"> ◆ ページ上でのパスワードのリセットをユーザに許可する ◆ 現在のパスワードをユーザに電子メールで送信する <p>この機能には逆方向パスワードが必要なため、ユニバーサルパスワードが有効になっていない場合は使用できません。</p>
Password Policy (パスワードポリシー): チャレンジセット	サポートされます。	サポートされます。
Password Policy (パスワードポリシー): パスワードのリセットのセルフサービス	<p>サポートされます。</p> <p>ユニバーサルパスワードが使用できない場合、Reset Password ガジェットはNDS パスワードを変更するので、eDirectory 8.6.2 で使用できます。</p>	<p>サポートされます。</p> <p>ユニバーサルパスワードが使用できない場合、Reset Password ガジェットはNDS パスワードを変更するので、ユーザの Password Policy (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ない場合でも使用できます。</p>
Password Policy (パスワードポリシー): [Set Universal Password] タスク	NDS パスワードの変更はサポートされません。代わりに、[Modify Object] タスクまたは他のヘルプデスクタスクを使用して、ユーザのNDS パスワードを変更できます。	<p>ユニバーサルパスワードが有効になっている場合はサポートされます。</p> <p>[Reset Password] タスクと異なり、[Set Universal Password] タスクは、ユニバーサルパスワードがユーザの Password Policy (パスワードポリシー) で有効になっている場合にのみ使用できます。</p>
パスワード同期	<p>Identity Manager に発行するパスワードのみがサポートされます。</p> <p>8.6.2 を使用し、新しいプラットフォームに対するサポートを追加すると、Password Synchronization 1.0 で提供される機能と同じ機能を模倣するようドライバを設定できます。</p> <p>Identity Manager は、接続システムからのパスワードを受け入れ、NDS パスワードをアップデートできます。ただしユニバーサルパスワードがない場合、接続システムが別の eDirectory ツリーでない限り、Identity Manager は接続システムにパスワードを配布できません。</p>	<p>サポートされます。</p> <p>ただし、Password Policy (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ない場合は、パスワードを接続システムに配布できません。この場合、受信したパスワードに対しては Password Policy (パスワードポリシー) を適用できますが、接続システムに対しては適用できません。</p>

機能	eDirectory 8.6.2	eDirectory 8.7.3
Role-Based Entitlement (役割ベースのエンタイトルメント)	サポートされていません。Entitlement Policy (エンタイトルメントポリシー) はダイナミックグループです。ダイナミックグループの機能の一部は eDirectory 8.6.2 ではサポートされていません。	サポートされます。
レポーティングと通知	Novell Nsure Audit をサポートします。 アップグレードのお客様のみが利用できます。レガシーのレポーティングと通知サービスである RNS もサポートされます。RNS は Identity Manager に含まれますが、DirXML エンジン用の RNS コンポーネントは含まれません。	Novell Nsure Audit をサポートします。 アップグレードのお客様のみが利用できます。レガシーのレポーティングと通知サービスである RNS もサポートします。RNS は Identity Manager に含まれますが、DirXML エンジン用の RNS コンポーネントは含まれません。
eGuide	サポートされます。	サポートされます。

C

更新履歴

- ◆ 293 ページの「2004年3月」
- ◆ 293 ページの「2004年4月1日」
- ◆ 293 ページの「2004年4月13日」
- ◆ 294 ページの「2004年6月30日」

2004年3月

- ◆ 次の新しい節が追加されました。
 - ◆ 80 ページの「DirXML コマンドラインユーティリティの使用」
 - ◆ 85 ページの「名前付きパスワードの使用」
 - ◆ 新機能に関する節、17 ページの「グローバル設定値」および 18 ページの「ドライバのハートビート」
- ◆ 新しいパスワード同期機能が別の製品ではなく、Identity Manager の機能であることを示すために、Password Synchronization 2.0 の呼称が Identity Manager パスワード同期に変更されています。
- ◆ DirXML[®] 2.0 の呼称が Nsure[™] Identity Manager 2 に変更されました。エンジンおよびドライバについては、以前と同様に DirXML エンジンおよび DirXML ドライバと呼びます。

2004年4月1日

- ◆ 参照しやすくするため、パスワードのセルフサービスの説明が独立した章として取り扱われています。NMA[™] Password Policy (パスワードポリシー) についての説明が次の2つの章に分かれました。
 - ◆ 7章 95 ページの、「Password Policy (パスワードポリシー) を使用したパスワードの管理」
 - ◆ 8章 115 ページの、「パスワードセルフサービス」

2004年4月13日

編集上の細かい変更が行われました。

2004年6月30日

Identity Manager 2.0.1 のブックをアップデートするための変更が行われました。

- ◆ 次の新しい節が追加されました。
 - ◆ 53 ページの「リモートローダ」
 - ◆ 152 ページの「パスワードの概要」
 - ◆ 168 ページの「機密情報の処理」
 - ◆ 12 章 263 ページの、「高可用性」
 - ◆ 139 ページの「Password Policy (パスワードポリシー) への独自の Password Change Message (パスワード変更メッセージ) の追加」
 - ◆ 137 ページの「Hint ガジェットの削除によるパスワードヒントの無効化」
 - ◆ 85 ページの「iManager を使用した名前付きパスワードの設定」
 - ◆ 213 ページの「シナリオ 5 - アプリケーションのパスワードの通常パスワードへの同期化」
 - ◆ 224 ページの「ドライバポリシーでの SMTP 認証情報の提供」
- ◆ 「パスワードの管理」で、「Making Sure Password Policies Are Correct for Identity Manager」という名前の節が削除されました。ポリシーは自動的に作成されるようになったため、Password Policy (パスワードポリシー) を特に手動で作成する必要はなくなりました。
- ◆ 144 ページの「パスワードセルフサービスと Virtual Office との統合」という名前の節は、『*Novell Virtual Office for NetWare 6.5 Configuration Guide (Novell Virtual Office for NetWare 6.5 設定ガイド)* (<http://www.novell.com/documentation/nw65/virtualoffice/data/ac6spye.html>)』に移動されました。
- ◆ 103 ページの「ユーザのログインおよびパスワード変更方法の計画」に説明が追加されました。古いクライアントが NDS パスワードを直接変更できないようブロックする方法についても、106 ページの「レガシー Novell Client によるパスワード変更の防止」に説明が追加されました。
- ◆ 233 ページの「電子メール通知テンプレートのローカライズ」に説明が追加されました。