Novell
資格情報プロビジョニングポリシー

3.5.1

www.novell.com

資格情報プロビジョニングポリシー

September 28, 2007

Novell®

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っていません。また文書の商品性、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、本書の内容は予告なく変更されることがあります。

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いません。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。

本契約の下で提供される製品または技術情報はすべて、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出については、「Novell International Trade Services (http://www.novell.com/info/exports/)」の Web ページをご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

米国 Novell, Inc. は、本文書に記載されている製品に統合されている技術に関する知的所有権を保有します。これらの知的所有権は、「Novell Legal Patents (http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります .

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

オンラインヘルプ: 本製品とその他の Novell 製品の最新のオンラインヘルプにアクセスする場合は、「Novell Documentation (http://www.novell.com/documentation)」の Web ページをご覧ください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に属します。

目次

このガイドについて **3**

1 概要 **5**

2 Novell SecureLogin による Novell 資格情報プロビジョニングポリシー **7**

3 Novell SecureLogin による Novell 資格情報プロビジョニングポリシーの実装 **11**

3.1 Novell SecureLogin による資格情報プロビジョニングポリシーの要件 11
3.2 Novell SecureLogin の LDAP スキーマの拡張 12
3.3 Novell SecureLogin の展開環境設定パラメータの決定 13
3.3.1 プロビジョニング環境設定データの例 14
3.4 Novell SecureLogin のリポジトリオブジェクトの作成 15
3.4.1 Designer での Novell SecureLogin のリポジトリオブジェクトの作成 16
3.4.2 iManager での Novell SecureLogin のリポジトリオブジェクトの作成 19
3.5 Novell SecureLogin のアプリケーションオブジェクトの作成 22
3.5.1 Designer での Novell SecureLogin のアプリケーションオブジェクトの作成 . . . 22
3.5.2 iManager での Novell SecureLogin のアプリケーションオブジェクトの作成 . . . 25
3.6 Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定 28
3.6.1 Designer での Novell SecureLogin の資格情報プロビジョニングポリシーの作成 . 28
3.6.2 iManager での Novell SecureLogin の資格情報プロビジョニングポリシーの作成 . 30
3.7 資格情報プロビジョニングポリシーの例 31
3.8 操作データキャッシング 32
3.9 SecureLogin のプロビジョニング 33
3.10 SecureLogin のプロビジョニング解除 33

4 Novell SecretStore による Novell 資格情報プロビジョニングポリシー **35**

5 Novell SecretStore による Novell 資格情報プロビジョニングポリシーの実装 **39**

5.1 Novell SecretStore による資格情報プロビジョニングポリシーの要件 39
5.2 Novell SecretStore の展開環境設定パラメータの決定 40
5.2.1 プロビジョニング環境設定データの例 41
5.3 Novell SecretStore のリポジトリオブジェクトの作成 43
5.3.1 Designer での Novell SecretStore のリポジトリオブジェクトの作成 43
5.3.2 iManager での Novell SecretStore のリポジトリオブジェクトの作成. 46
5.4 Novell SecretStore のアプリケーションオブジェクトの作成 50
5.4.1 Designer での Novell SecretStore のアプリケーションオブジェクトの作成 50
5.4.2 iManager での Novell SecretStore のアプリケーションオブジェクトの作成. . . . 53
5.5 Novell SecretStore の資格情報プロビジョニングポリシーの作成 57
5.5.1 Designer での Novell SecretStore の資格情報プロビジョニングポリシーの作成 . . 57
5.5.2 iManager での Novell Se cretStore の資格情報プロビジョニングポリシーの環境設定 59
5.6 資格情報プロビジョニングポリシーの例 60
5.7 操作データキャッシング 60
5.8 SecretStore のプロビジョニング 61
5.9 SecretStore のプロビジョニング解除 61

6 Novell 資格情報プロビジョニングポリシーの管理 63

6.1 リポジトリおよびアプリケーションオブジェクトの管理 63
6.2 資格情報プロビジョニングポリシーの管理 63

このガイドについて

Identity Manager 3.5.1 用 Novell® 資格情報プロビジョニングポリシーは、アプリケーション資格情報を Novell SecretStore® および Novell SecureLogin の資格情報リポジトリに同時にプロビジョニングする機能を実現することにより、すべての Identity Manager ドライバのユーザプロビジョニング機能を拡張します。加えて、否認防止が必要な環境で SecureLogin パスフレーズの質問と回答をプロビジョニングできます。

このガイドは、資格情報プロビジョニングポリシーを SecureLogin および SecretStore と共に実装する方法について、詳しいリファレンスを提供します。このガイドでは、Identity Manager、SecureLogin、または SecretStore の設定情報については取り上げません。

- 5 ページの第 1 章「概要」
- 7 ページの第 2 章「Novell SecureLogin による Novell 資格情報プロビジョニングポリシー」
- 11 ページの第 3 章「Novell SecureLogin による Novell 資格情報プロビジョニングポリシーの実装」
- 35 ページの第 4 章「Novell SecretStore による Novell 資格情報プロビジョニングポリシー」
- 39 ページの第 5 章「Novell SecretStore による Novell 資格情報プロビジョニングポリシーの実装」

対象読者

このガイドは、Identity Manager の管理者を対象にしています。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか www.novell.com/documentation/feedback.html にアクセスしてコメントを記入してください。

マニュアルの更新

『*資格情報プロビジョニングポリシー*』の最新バージョンについては、Identity Manager Web サイト (http://www.novell.com/documentation/idm) にアクセスしてください。

追加のマニュアル

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

Identity Manager ドライバのマニュアルについては、Identity Manager マニュアル Web サイト (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) を参照してください。

SecureLogin のマニュアルについては、Novell SecureLogin マニュアル Web サイト (http://www.novell.com/documentation/secretstore33/index.html) を参照してください。

SecretStore のマニュアルについては、Novell SecretStore マニュアル Web サイト (http://www.novell.com/documentation/securelogin60/index.html) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します。

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。

プラットフォームによっては、シングルパス名に円記号 (\) を使用できる場合とスラッシュ (/) を使用できる場合がありますが、パス名は円記号で表記されます。Linux*、UNIX* など、スラッシュを使う必要があるプラットフォームを使用しているユーザは、必要に応じてスラッシュを使用してください。

概要

1

Identity Manager 用 Novell® 資格情報プロビジョニングポリシーは、アプリケーション資格情報を Novell SecureLogin® および Novell SecretStore® の資格情報リポジトリに同時にプロビジョニングする機能を実現することにより、すべての Identity Manager ドライバのユーザプロビジョニング機能を拡張します。加えて、この製品では、否認防止が必要な環境で SecureLogin パスフレーズの質問と回答をプロビジョニングできます。

これらの機能によりユーザの Single Sign-On (SSO) の操作性を向上させ、SSO 技術への投資に対する見返りを増やすには、SecureLogin アカウント情報の初期設定をなくし、アプリケーション資格情報のセキュリティを高め、ユーザの SSO 資格情報ストアのプロビジョニングに通常関連する作業の反復を減らします。また、資格情報プロビジョニングポリシーで Identity Manager ポリシーを使用することで、アプリケーション資格情報を自動的にプロビジョニング解除し、アプリケーションデータへのアクセスを防ぐことができます。

- 7 ページの第 2 章「Novell SecureLogin による Novell 資格情報プロビジョニングポリシー」
- 11 ページの第 3 章「Novell SecureLogin による Novell 資格情報プロビジョニングポリシーの実装」
  - 11 ページのセクション 3.1「Novell SecureLogin による資格情報プロビジョニングポリシーの要件」
  - 12 ページのセクション 3.2「Novell SecureLogin の LDAP スキーマの拡張」
  - 13 ページのセクション 3.3「Novell SecureLogin の展開環境設定パラメータの決定」
  - 15 ページのセクション 3.4「Novell SecureLogin のリポジトリオブジェクトの作成」
  - 22 ページのセクション 3.5「Novell SecureLogin のアプリケーションオブジェクトの作成」
  - 28 ページのセクション 3.6「Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定」
- 35 ページの第 4 章「Novell SecretStore による Novell 資格情報プロビジョニングポリシー」
- 39 ページの第 5 章「Novell SecretStore による Novell 資格情報プロビジョニングポリシーの実装」
  - 39 ページのセクション 5.1「Novell SecretStore による資格情報プロビジョニングポリシーの要件」
  - 40 ページのセクション 5.2「Novell SecretStore の展開環境設定パラメータの決定」
  - 43 ページのセクション 5.3「Novell SecretStore のリポジトリオブジェクトの作成」
  - 50 ページのセクション 5.4「Novell SecretStore のアプリケーションオブジェクトの作成」
  - 57 ページのセクション 5.5「Novell SecretStore の資格情報プロビジョニングポリシーの作成」
- 63 ページの第 6 章「Novell 資格情報プロビジョニングポリシーの管理」

2 Novell SecureLoginによるNovell資格情報プロビジョニングポリシー

Novell® 資格情報プロビジョニングポリシーを使用することで、SecureLogin® がサポートするアプリケーション資格情報を自動的にプロビジョニングできます。この項では、Identity Manager 内のオブジェクトとポリシーを設定するために必要な手順について記載しています。SecureLogin コンポーネントの展開および設定についての情報は含まれていません。SecureLogin のマニュアルについては、Novell SecureLogin 6.0 マニュアル Web サイト (http://www.novell.com/documentation/securelogin60/index.html) を参照してください。

SecureLogin を用いて資格情報プロビジョニングを実装するには、リポジトリオブジェクト、アプリケーションオブジェクト、およびポリシーが必要です。リポジトリとアプリケーションのオブジェクトには、Identity Manager が使用できるように SecureLogin の情報が格納されます。ポリシーは、ドライバで資格情報プロビジョニングを使用できるようにするために使用されます。詳細については、11 ページの第 3 章「Novell SecureLogin による Novell 資格情報プロビジョニングポリシーの実装」を参照してください。

次のオプションも設定できます。

- 資格情報プロビジョニングは、発行者チャネル、購読者チャネル、または両方のチャネルで設定できます。
- SecureLogin の同期は、アプリケーションのパスワード同期の一部として実行したり、他のイベントにトリガさせたりすることができます。
- Web サービスの資格情報は、アプリケーションのアカウントをプロビジョニングしなくてもプロビジョニングできます。
- SecureLogin パスフレーズの初期の質問と回答をプロビジョニングできます。

パスワードのランダム生成機能を使用して、接続システム上のユーザアカウントのパスワードを設定し、識別情報管理環境のセキュリティをさらに高めることができます。詳細については、『*Novell Identity Manager 3.5.1 管理ガイド*』でパスワードのランダム生成機能の使い方を参照してください。

8 ページの 図 2-1 は、一般的なシナリオを簡略に示しています。このシナリオでは、財務部の SAP* 財務アプリケーションの新規ユーザに対し、SecureLogin 資格情報をプロビジョニングしています。SAP アプリケーションでは、通常のアプリケーションで指定する一般的なユーザ名とパスワードのほかにもログインパラメータが必要です。そのため、この例では、SAP ユーザのプロビジョニングを使用しています。

この部署では、SAP HR システムと Identity Manager を使用して、識別ボールト内に新しいユーザをプロビジョニングします。組織の情報に基づき、ユーザオブジェクトは Active Directory* 内に実装された部署の認証ツリー内にプロビジョニングされます。ここが新しいユーザがネットワークに対して認証される場所であり、SecureLogin 資格情報のリポジトリの場所になります。続いて、Identity Manager によって、ユーザはさまざまな Finance アプリケーションに対しプロビジョニングされ、それらのシステムの資格情報は、Active Directory 内の SecureLogin ストアに同期されます。

図 2-1 は、ユーザ Glen の認証資格情報がプロビジョニングされているところを示しています。Glen が自分の部署の Active Directory 認証ドメインに対して認証を実行し、

SecureLogin クライアントを起動すると、SAP の財務アカウントへ Single Sign-On できます。このとき、システムのパスワードを入力したり、記憶している必要さえありません。

図 2-1 *SecureLogin による資格情報プロビジョニング*

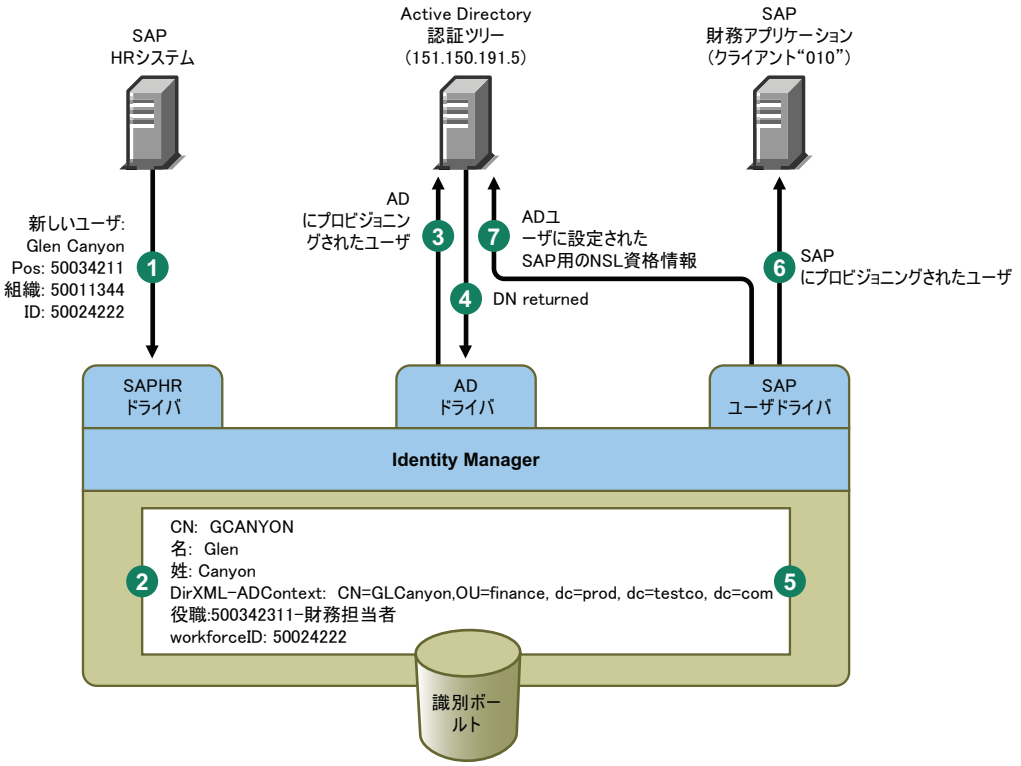


図 2-1 は、以下の手順を示しています。

1. SAP HR システムが、新入社員 Glen Canyon のデータを発行します。Identity Manager の SAP HP ドライバが、このデータを処理します。
2. Cn 値「GCANYON」および workforceID 値「50024222」を持つ新しいユーザオブジェクトが、識別ボールト内に作成されます。このユーザは、会社の財務組織に割り当てられているため、finance.prod.testco.com ドメインにある財務部の Active Directory サーバで認証を受ける必要があります。ドメインを同期する Identity Manager の Active Directory ドライバは、識別ボールトの情報を使用するようになりました。
3. Glen は、Finance 部の Active Directory サーバにプロビジョニングされます。
4. このドライバは、Glen の完全識別 LDAP 名「CN=GLCanyon,OU=finace,dc=prod,dc=testco,dc=com」を取得するように設定されます。
5. ドライバは、この名前を識別ボールト内の GCANYON ユーザの DirXML-ADContext 属性に配置します。

   これで、識別ボールト内で必要な属性が使用できるようになったので、SAP ユーザ管理ドライバによって、GCANYON オブジェクトの属性が処理されます。
6. Glen は Finance 組織に所属するため、ドライバは SAP Finance サーバ上ある SAP ユーザアカウントの GCANYON に対してプロビジョニングを行います。
7. アカウントの作成が成功すると、SAP ユーザ管理ドライバのポリシーによって、Glen の SAP 認証資格情報がこのユーザの AD ユーザアカウントにプロビジョニング

されます。コマンドが「追加」操作であるため、ポリシーは SecureLogin パスフレーズの質問と回答もプロビジョニングします。

3 Novell SecureLoginによるNovell資格情報プロビジョニングポリシーの実装

Novell* SecureLogin による Novell 資格情報プロビジョニングポリシーの実装は、柔軟にカスタマイズできます。実装手順は、SecureLogin がインストールされているプラットフォーム、プロビジョニング対象のアプリケーション、使用する Identity Manager ドライバによって異なります。

SecureLogin による資格情報プロビジョニングポリシーを実装するには、次のトピックを参照してください。

- 11 ページのセクション 3.1「Novell SecureLogin による資格情報プロビジョニングポリシーの要件」
- 12 ページのセクション 3.2「Novell SecureLogin の LDAP スキーマの拡張」
- 13 ページのセクション 3.3「Novell SecureLogin の展開環境設定パラメータの決定」
- 15 ページのセクション 3.4「Novell SecureLogin のリポジトリオブジェクトの作成」
- 22 ページのセクション 3.5「Novell SecureLogin のアプリケーションオブジェクトの作成」
- 28 ページのセクション 3.6「Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定」
- 31 ページのセクション 3.7「資格情報プロビジョニングポリシーの例」
- 32 ページのセクション 3.8「操作データキャッシング」
- 33 ページのセクション 3.9「SecureLogin のプロビジョニング」
- 33 ページのセクション 3.10「SecureLogin のプロビジョニング解除」

3.1 Novell SecureLogin による資格情報プロビジョニングポリシーの要件

SecureLogin による資格情報プロビジョニングポリシーを使用するには、次の要件を満たす必要があります。

- Identity Manager 3.0.1 以降
- eDirectory™ 8.7x または eDirectory 8.8.1 以降。eDirectory 8.8 はサポートされていません。
- jsso.jar、idmcp.jar、および jnet.jar が Identity Manager Java ライブラリの標準の場所にあることを確認します。
- Novell SecureLogin 6.0 以降

要件が満たされていることを確認したら、12 ページのセクション 3.2「Novell SecureLogin の LDAP スキーマの拡張」に進んでください。

3.2 Novell SecureLogin の LDAP スキーマの拡張

SecureLogin を eDirectory サーバ上に展開する場合、ndsschema.exe というツールを使用して、SecureLogin の属性セットで eDirectory スキーマを拡張します。これらの属性は、暗号化された資格情報、ポリシーなどをユーザおよびコンテナのオブジェクトに保存するために使用されます。属性を次に示します。

- Prot:SSO Auth
- Prot:SSO Entry
- Prot:SSO Entry Checksum
- Prot:SSO Profile
- Prot:SSO Security Prefs
- Prot:SSO Security Prefs Checksum

これらの属性は eDirectory に特有のもので、SecureLogin 製品を機能させるために必要です。Identity Manager 3.0 Support Pack 1 に付属しているプロビジョニング API では、LDAP ネームスペースを使用してその機能を実行することで、あらゆる SecureLogin 資格情報ストアと連動できるようにします。

上記の属性への LDAP マッピングを行うには、SecureLogin 製品に付属している 2 つめのツールを使用します。このツールの名前は ldapschema.exe で、eDirectory 属性へ LDAP ネームスペースをマッピングするため、eDirectory 環境で使用されます。

『*Novell SecureLogin 6.0 インストールガイド*』の「LDAP ディレクトリの準備 (http://www.novell.com/documentation/securelogin60/index.html?page=/documentation/securelogin60/nslinst/data/b1tnxsu.html#b1tnxsu)」を参照してください。

ldapschema.exe を実行したら、iManager で LDAP グループ属性を確認することで、マッピングを確認します。

1. iManager で、*［LDAP］>［LDAP Options (LDAP オプション)］の順にクリックします。*
2. SecureLogin をホストする eDirectory サーバに関連付けられた LDAP グループを選択します。
3. ［LDAP グループのプロパティ］ページから、［*属性マップ*］オプションを選択して、eDirectory 属性が正しくマップされていることを確認します。

eDirectory 属性	LDAP 属性
Prot:SSO Auth	protocom-SSO-Auth-Data
Prot:SSO Entry	protocom-SSO-Entries
Prot:SSO Entry Checksum	protocom-SSO-Entries-Checksum
Prot:SSO Profile	protocom-SSO-Profile
Prot:SSO Security Prefs	protocom-SSO-Security-Prefs
Prot:SSO Security Prefs Checksum	protocom-SSO-Security-Prefs-Checksum

4. スキーマを拡張したら、13 ページのセクション 3.3「Novell SecureLogin の展開環境設定パラメータの決定」に進んでください。

3.3 Novell SecureLogin の展開環境設定パラメータの決定

図 2-1 の展開シナリオで説明されている同期機能を提供するには、まず、Identity Manager および SecureLogin 環境に関連したすべてのビジネスプロセス情報を収集します。13 ページの ï 3-1§ 「SecureLogin の資格情報プロビジョニングポリシーワークシート」を印刷して、情報を記録するためのワークシートとして使用してください。

表 3-1 *SecureLogin の資格情報プロビジョニングポリシーワークシート*

必要な環境設定情報	情報
1) SecureLogin シングルサインオンのプロビジョニング用に設定するアプリケーション。	
2) SecureLogin アプリケーションの定義が認証サーバであらかじめ設定されていて、その内容をこれらのシステムにプロビジョニングされる新規ユーザが継承可能であることを確認する。	
3) SecureLogin リポジトリサーバの DNS 名または IP アドレス。	
4) SecureLogin リポジトリサーバの SSL LDAP ポート。	
5) SecureLogin リポジトリサーバ管理者の完全修飾された LDAP 識別名。	
6) SecureLogin リポジトリサーバの管理者のパスワード。	
7) SecureLogin サーバからエクスポートされる SSL 証明書へのフルパスおよび証明書名。証明書は、Identity Manager サーバのローカルに配置する必要があります。	
8) 1 つの SecureLogin リポジトリを複数のドライバで使用するか、または各ドライバで専用のリポジトリを使用するかを決定する。	
9) SecureLogin アプリケーションごとのアプリケーション ID。	
10) 各アプリケーションに必要な認証キー (ユーザ名、パスワード、クライアント、言語など) をすべて一覧にする。これらはアプリケーションごとに異なる場合があります。	
11) 認証キーの値をスタティックな値に設定するかどうかを決定する。	
12) ユーザごとに異なる値である (または異なる値にできる) スタティックでない値の場合は、そのスタティックでない情報のソースを書き留める (イベント情報または識別ボールトの属性値)。	

必要な環境設定情報	情報
13) ターゲットアプリケーションへのパスワードも同期しているドライバに SecureLogin のプロビジョニングを実装する場合、SecureLogin のプロビジョニングを、ターゲットアプリケーションのサーバにパスワードが設定される前と後のどちらで開始するかを決定する。	
14) リポジトリおよびアプリケーションのオブジェクトが格納されるドライバオブジェクトの名前 (格納先ドライバは別々に指定可能)。	
15) ターゲットアプリケーションのユーザオブジェクトの DN を決定する。	
16) SecureLogin パスフレーズを実装する場合、パスフレーズの質問と回答を決定する。	質問 : 回答 :

3.3.1 プロビジョニング環境設定データの例

8 ページの 図 2-1 のプロビジョニングシナリオを使用したサンプルデータを次に示します。ここでは、財務部の Active Directory 認証ツリー内のユーザに、SAP 財務サーバの SecureLogin 資格情報をプロビジョニングします。

表 3-2 *SecureLogin の資格情報プロビジョニングポリシーワークシートの例*

必要な環境設定情報	情報
1) SecureLogin シングルサインオンのプロビジョニング用に設定するアプリケーション。	SAP Finance アプリケーション
2) SecureLogin アプリケーションの定義が認証サーバであらかじめ設定されていて、その内容をこれらのシステムにプロビジョニングされる新規ユーザが継承可能であることを確認する。	確認済み
3) SecureLogin リポジトリサーバの DNS 名または IP アドレス。	151.150.191.5
4) SecureLogin リポジトリサーバの SSL LDAP ポート。	636
5) SecureLogin リポジトリサーバ管理者の完全修飾された LDAP 識別名。	cn=admin,ou=prod,dc=testco,dc=.com
6) SecureLogin リポジトリサーバの管理者のパスワード。	dixml
7) SecureLogin サーバからエクスポートされる SSL 証明書へのフルパスおよび証明書名。証明書は、Identity Manager サーバのローカルに配置する必要があります。	c:\novell\nds\FinanceAD.cer
8) 1 つの SecureLogin リポジトリを複数のドライバで使用するか、または各ドライバで専用のリポジトリを使用するかを決定する。	この例では、リポジトリは 1 つだけにします。

必要な環境設定情報	情報
9) SecureLogin アプリケーションごとのアプリケーション ID。	SAP - 151.150.191.27
10) 各アプリケーションに必要な認証キー (ユーザ名、パスワード、クライアント、言語など) をすべて一覧にする。これらはアプリケーションごとに異なる場合があります。	SAP Client 010 ログインパラメータクライアント SAP Client 010 ログインパラメータ言語 SAP Client 010 ログインパラメータユーザ名 SAP Client 010 ログインパラメータパスワード
11) 認証キーの値をスタティックな値に設定するかどうかを決定する。	SAP Client 010 ログインパラメータクライアント : 「010」SAP Client 010 ログインパラメータ言語 : 「EN」
12) ユーザごとに異なる値である (または異なる値にできる) スタティックでない値の場合は、そのスタティックでない情報のソースを書き留める (イベント情報または識別ボールトの属性値)。	SAP Client 010 ログインパラメータユーザ名 : 識別ボールト属性「sapUsername」SAP Client 010 ログインパラメータパスワード : イベント <password>
13) ターゲットアプリケーションへのパスワードも同期しているドライバに SecureLogin のプロビジョニングを実装する場合、SecureLogin のプロビジョニングを、ターゲットアプリケーションのサーバにパスワードが設定される前と後のどちらで開始するかを決定する。	After
14) リポジトリおよびアプリケーションのオブジェクトが格納されるドライバオブジェクトの名前 (格納先ドライバは別々に指定可能)。	SAP ドライバ
15) ターゲットアプリケーションのユーザオブジェクトの DN を決定する。	識別ボールト属性の「DirXML-ADContext」
16) SecureLogin パスフレーズをプロビジョニングする場合、パスフレーズの質問と回答を決定する。	質問 : 「従業員コードは ?」回答 : 識別ボールト属性の「workforceID」

その他の環境設定情報 :

- 財務部の AD ツリーは、すべての財務アプリケーションの SecureLogin リポジトリとして動作します。
- Finance 部関連のプロビジョニングドライバは、すべて「Finance Drivers」という名前のドライバセット内に設定されます。
- 識別ボールトの属性「employeeStatus」の値が「I」に設定された場合、SAP ユーザアカウントを削除して、その SAP ユーザアカウントの SecureLogin 資格情報も Active Directory ユーザから削除する必要があります。

すべての環境設定データを決定したら、15 ページのセクション 3.4「Novell SecureLogin のリポジトリオブジェクトの作成」に進んでください。

3.4 Novell SecureLogin のリポジトリオブジェクトの作成

リポジトリオブジェクトには、SecureLogin のスタティックな環境設定情報が保存されます。リポジトリの情報は、アプリケーション資格情報を使用するアプリケーションからは独立しています。この情報は、接続システム (SAP、PeopleSoft*、Notes* など) に関係な

く、すべてのプロビジョニングイベントに適用されます。リポジトリオブジェクトは、Designer または iManager で作成できます。

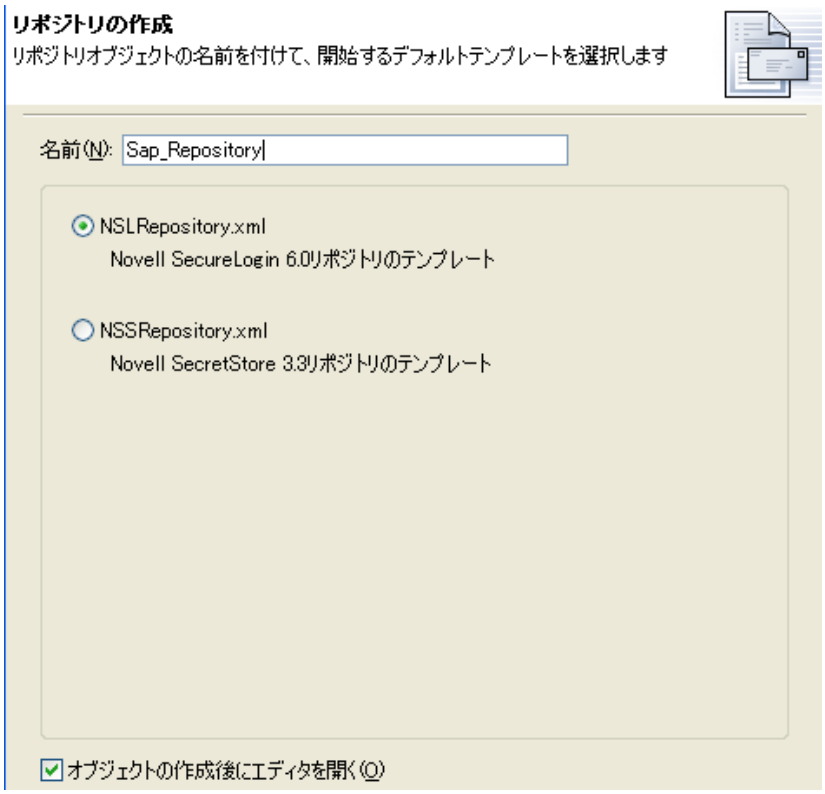
- 16 ページのセクション 3.4.1「Designer での Novell SecureLogin のリポジトリオブジェクトの作成」
- 19 ページのセクション 3.4.2「iManager での Novell SecureLogin のリポジトリオブジェクトの作成」

3.4.1 Designer での Novell SecureLogin のリポジトリオブジェクトの作成

次に示すのは、Designer でリポジトリオブジェクトを作成する方法のうちの 1 つです。

1. アウトラインビューで、リポジトリオブジェクトを格納するドライバオブジェクトを右クリックします。
2. *［新規］>［資格情報リポジトリ］*の順にクリックします。

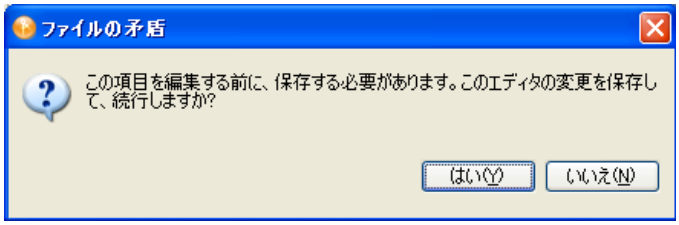
3. リポジトリオブジェクトの名前を指定します。
4. SecureLogin テンプレートを使用するため、［*NSLRepository.xml*］を選択します。



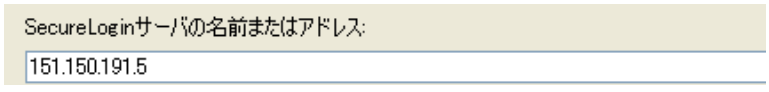
［*オブジェクトの作成後にエディタを開く*］チェックボックスがオンになっていることを確認します。

5 ［*OK*］をクリックします。

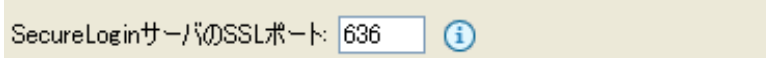
6 ［*はい*］をクリックして、新しいリポジトリオブジェクトを保存します。



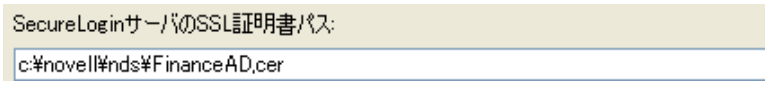
7 SecureLogin サーバの DNS 名または IP アドレスを指定します (ワークシート項目の 3 を参照してください)。



8 SecureLogin サーバの SSL ポートを指定します (ワークシート項目の 4 を参照してください)。

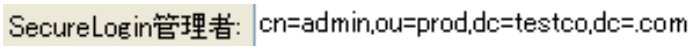


9 SecureLogin サーバからエクスポートされる SSL 証明書へのフルパスを指定します。このパスには証明書名を含め、Identity Manager サーバのローカルに配置する必要があります (ワークシート項目の 7 を参照してください)。

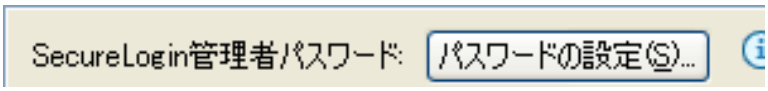


SecureLogin サーバは、複数のタイプのプラットフォーム上で実行できます。SSL 証明書のエクスポート方法については、プラットフォームごとのマニュアルを参照してください。

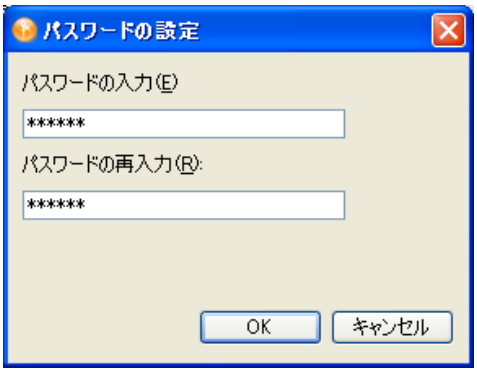
10 SecureLogin 管理者の完全修飾 LDAP 識別名を指定します (ワークシート項目の 5 を参照してください)。



11 [*パスワードの設定*] をクリックします。



12 SecureLogin 管理者のパスワードを 2 回入力し、[*OK*] をクリックします (ワークシート項目の 6 を参照してください)。



13 情報を確認し、[*保存*] アイコンをクリックして情報を保存します。

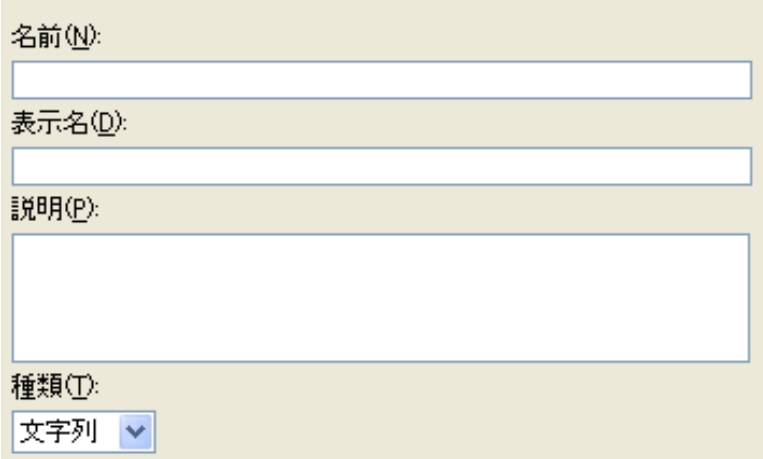
14 (オプション) リポジトリオブジェクトに対する他の環境設定パラメータを作成する場合は、[*新しい項目の追加*アイコン] をクリックします。

14a パラメータの名前を指定します。

14b パラメータの表示名を指定します。

14c 参照情報として、パラメータの説明を入力します。

パラメータは文字列で保存されます。



14d *[OK]* をクリックします。

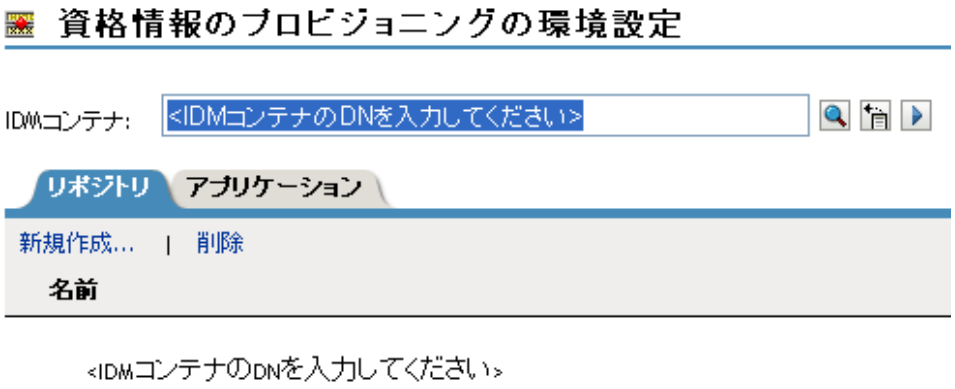
14e [*保存*] アイコンをクリックして、リポジトリオブジェクトを保存します。

リポジトリオブジェクトが作成されたら、22 ページの 「Novell SecureLogin のアプリケーションオブジェクトの作成」に進んでください。

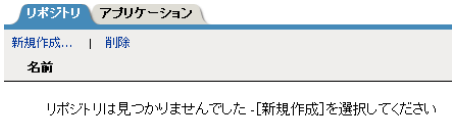
3.4.2 iManager での Novell SecureLogin のリポジトリオブジェクトの作成

1 iManager で、*[資格情報のプロビジョニング]* > *[環境設定]* の順に選択します。

2 リポジトリオブジェクトを保存するドライバオブジェクトを参照して選択します。



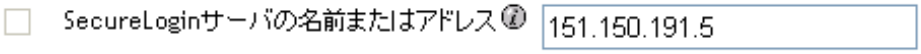
3 [*新規作成*] をクリックしてリポジトリを作成します。



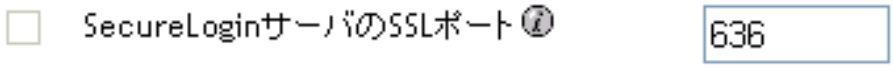
4 リポジトリオブジェクトの名前を指定したら、SecureLogin テンプレートを使用してリポジトリを作成するため、［*NSLRepository.xml*］を選択します。

5 ［*OK*］をクリックします。

6 SecureLogin サーバの DNS 名または IP アドレスを指定します (ワークシート項目の 3 を参照してください)。



7 SecureLogin サーバの SSL ポートを指定します (ワークシート項目の 4 を参照してください)。

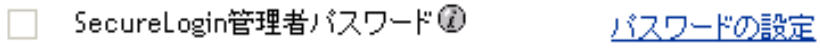


8 SecureLogin サーバからエクスポートされる SSL 証明書へのフルパスを指定します。このパスには証明書名を含め、Identity Manager サーバのローカルに配置する必要があります (ワークシート項目の 7 を参照してください)。

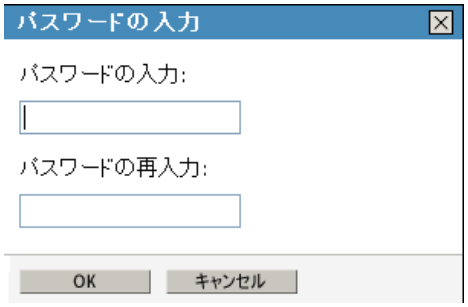
SecureLogin サーバは、複数のタイプのプラットフォーム上で実行できます。SSL 証明書のエクスポート方法については、プラットフォームごとのマニュアルを参照してください。

9 SecureLogin 管理者の完全修飾 LDAP 識別名を指定します (ワークシート項目の 5 を参照してください)。

10 ［*パスワードの設定*］をクリックします。

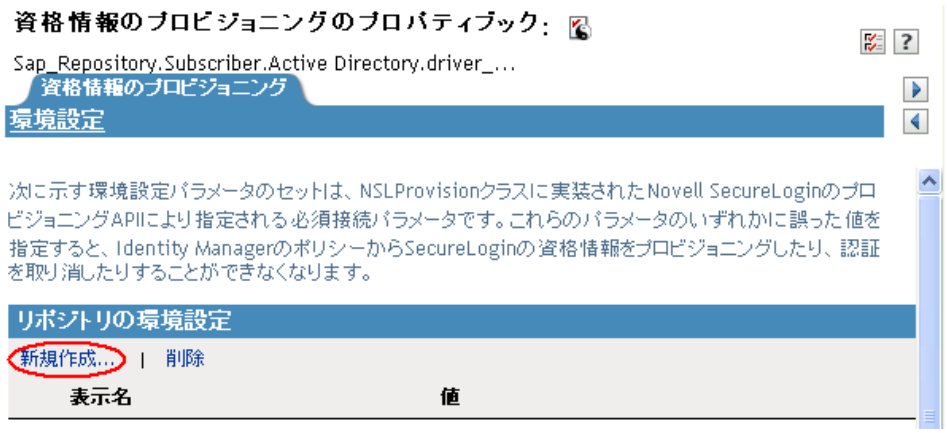


11 SecureLogin 管理者のパスワードを 2 回入力し、［*OK*］をクリックします (ワークシート項目の 6 を参照してください)。



12 指定した値を確認し、［*OK*］をクリックします。

13 (オプション) リポジトリに対する他の環境設定パラメータを作成する必要がある場合は、［*新規作成*］をクリックします。



13a パラメータの名前を指定します。

13b パラメータの表示名を指定します。

13c 参照情報として、パラメータの説明を入力します。

パラメータは文字列で保存されます。

13d ［*OK*］をクリックします。

リポジトリオブジェクトが作成されたら、22 ページの 「Novell SecureLogin のアプリケーションオブジェクトの作成」に進んでください。

3.5 Novell SecureLogin のアプリケーションオブジェクトの作成

アプリケーションオブジェクトには、SecureLogin のアプリケーション認証パラメータ値が保存されます。アプリケーション情報は、そのアプリケーションの資格情報を使用しているアプリケーションに特有のものです (GroupWise® クライアントの情報または SAP データベースクライアントの情報など)。アプリケーションオブジェクトは、Designer または iManager で作成できます。

- 22 ページのセクション 3.5.1「Designer での Novell SecureLogin のアプリケーションオブジェクトの作成」
- 25 ページのセクション 3.5.2「iManager での Novell SecureLogin のアプリケーションオブジェクトの作成」

3.5.1 Designer での Novell SecureLogin のアプリケーションオブジェクトの作成

次に示すのは、Designer でアプリケーションオブジェクトを作成する方法のうちの 1 つです。

1. アウトラインビューで、アプリケーションオブジェクトを格納するドライバオブジェクトを右クリックします。
2. *［新規作成］>［資格情報アプリケーション］*の順にクリックします。

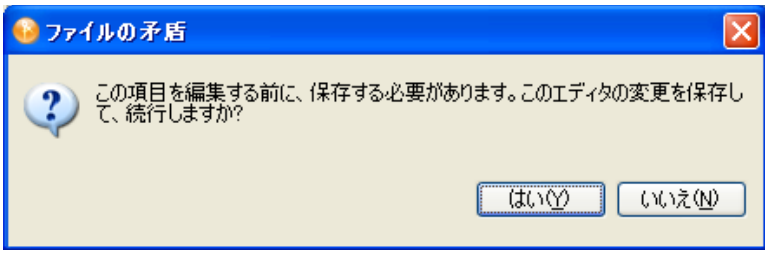
3 アプリケーションオブジェクトの名前を指定します。

4 SecureLogin テンプレートを使用するため、［*NSLApplication.xml*］を選択します。

［*オブジェクトの作成後にエディタを開く*］チェックボックスがオンになっていることを確認します。

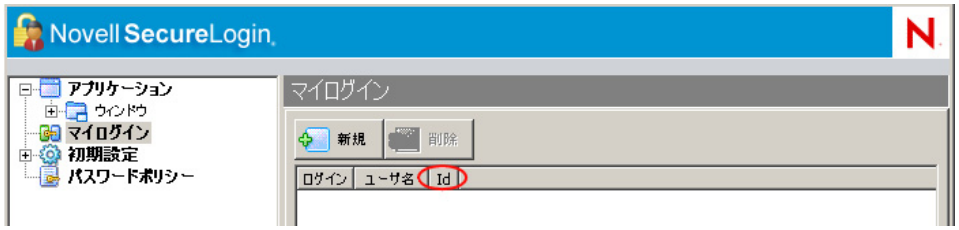
5 ［*OK*］をクリックします。

6 ［*はい*］をクリックして、新しいアプリケーションオブジェクトを保存します。



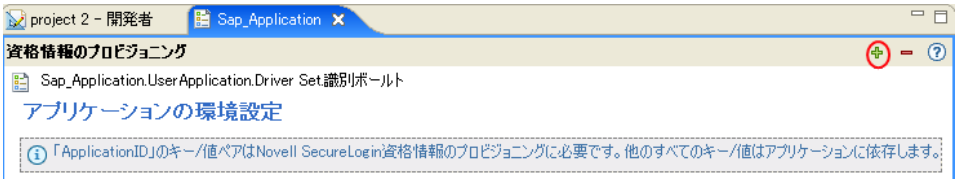
7 ［SecureLogin アプリケーション ID］を指定します (ワークシート項目の 9 を参照してください)。

SecureLogin のアプリケーション ID を見つけるには、［*マイログイン*］をクリックします。アプリケーション ID は、［*ID*］フィールドに保存されています。



8 ［*保存*］アイコンをクリックして、アプリケーションを保存します。

9 アプリケーションに必要な認証キーを追加するため、［*新しい項目の追加*］アイコンをクリックします。

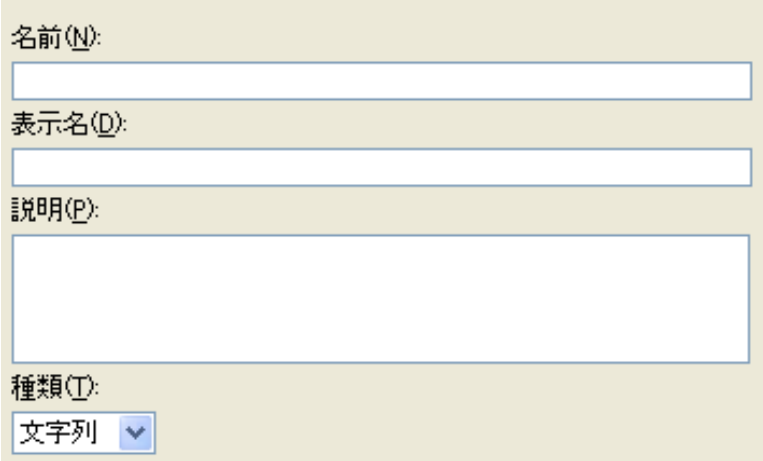


9a 認証キーの名前を指定します。

9b 認証キーの表示名を指定します。

9c 参照情報として、認証キーの説明を入力します。

認証キーは文字列で保存されます。



9d ［*OK*］をクリックします。

9e 入力が必要な新規認証キーごとに、ステップ 9 を繰り返します。

アプリケーションの認証キーを見つけるには、そのアプリケーションのユーザに対し、SecureLogin 資格情報を手動作成し、そのユーザでログインします。ユーザがログインすると、SecureLogin の管理ウィンドウ内の［My Logins (マイログイン)］に、認証キー情報が表示されます。

10 認証キーがすべてのユーザ資格情報で共有するスタティックな値である場合、その値を指定します。

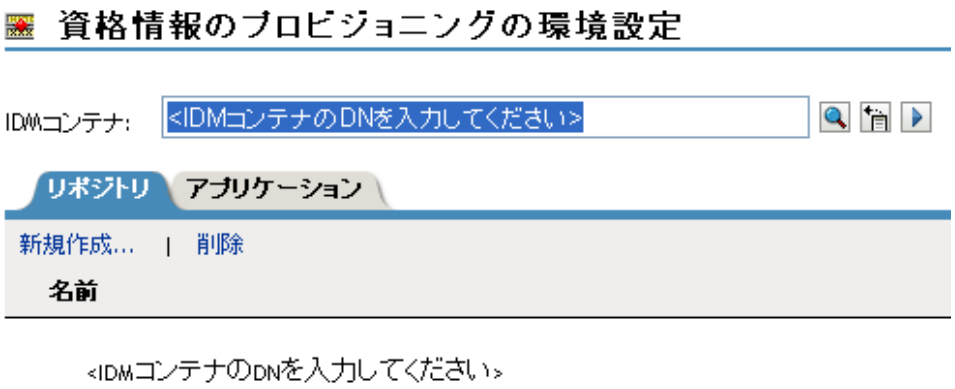
11 ［保存］アイコンをクリックして、アプリケーションを保存します。

アプリケーションオブジェクトが作成されたら、28 ページの 「Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定」に進んでください。

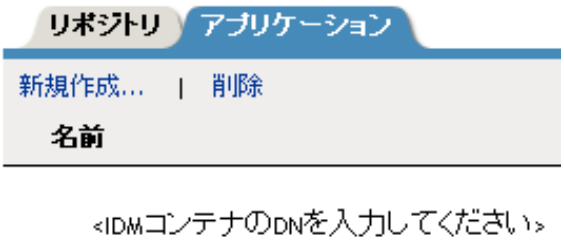
3.5.2 iManager での Novell SecureLogin のアプリケーションオブジェクトの作成

1 iManager で、*［資格情報のプロビジョニング］*>*［環境設定］*の順に選択します。

2 アプリケーションオブジェクトを保存するドライバオブジェクトを参照して選択します。

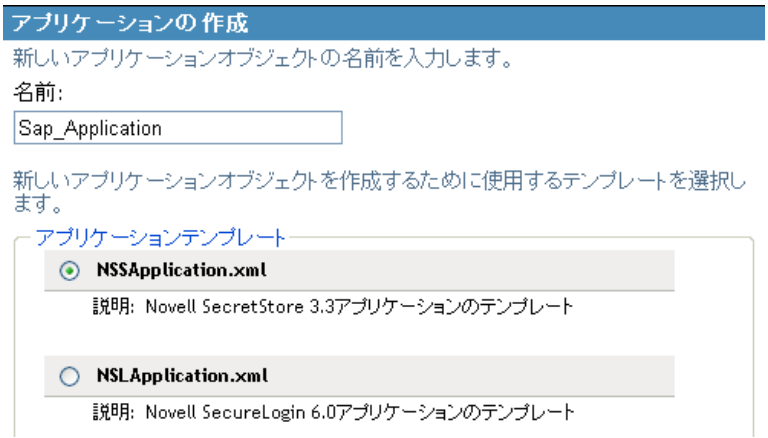


3 ［*アプリケーション*］タブを選択し、［*新規作成*］をクリックします。



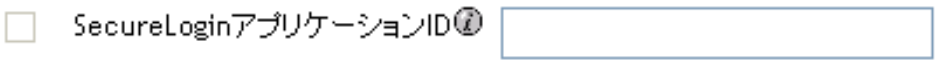
4 アプリケーションオブジェクトの名前を指定します。

5 SecureLogin テンプレートを使用してアプリケーションを作成するため、［*NSLApplication.xml*］を選択します。

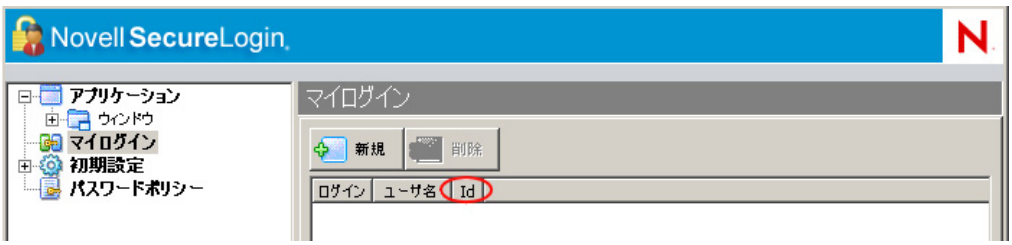


6 ［*OK*］をクリックします。

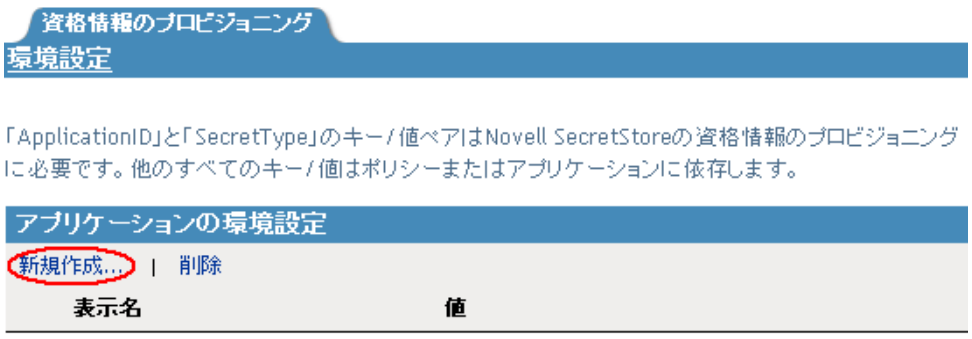
7 ［*SecureLogin アプリケーション ID*］を指定します (ワークシート項目の 9 を参照してください)。



SecureLogin のアプリケーション ID を見つけるには、［*マイログイン*］をクリックします。アプリケーション ID は、［*ID*］フィールドに保存されています。



8 認証キーパラメータを作成するため、［*新規作成*］をクリックします (ワークシート項目の 10 を参照してください)。



8a 認証キーの名前を指定します。

8b 認証キーの表示名を指定します。

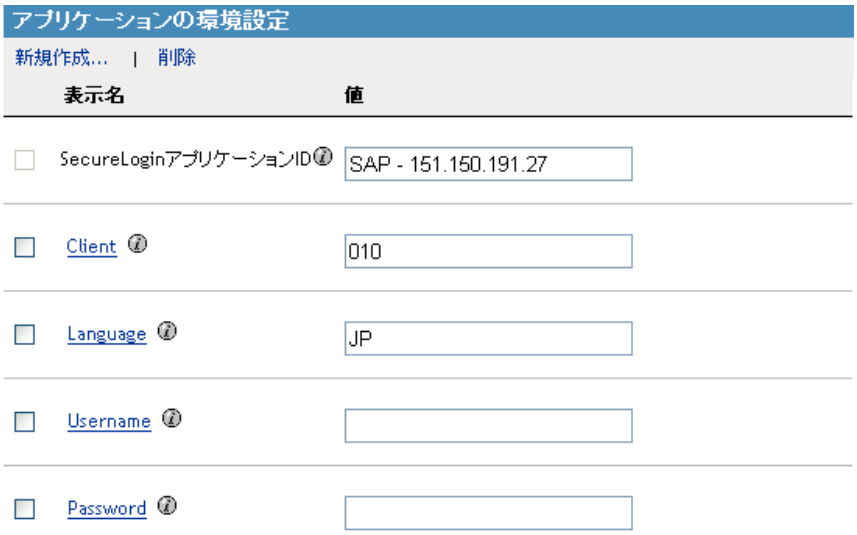
8c 参照情報として、認証キーの説明を入力します。

認証キーは文字列で保存されます。

アプリケーションの認証キーを見つけるには、そのアプリケーションのユーザに対し、SecureLogin 資格情報を手動作成し、そのユーザでログインします。ユーザがログインすると、SecureLogin の管理ウィンドウ内の［*マイログイン*］に、認証キー情報が表示されます。

8d ［*OK*］をクリックします。

8e 認証キー値を指定し、その値がスタティックである場合は、続いて［*OK*］をクリックします。



アプリケーションオブジェクトが作成されたら、28 ページの 「Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定」に進んでください。

3.6 Novell SecureLogin の資格情報プロビジョニングポリシーの環境設定

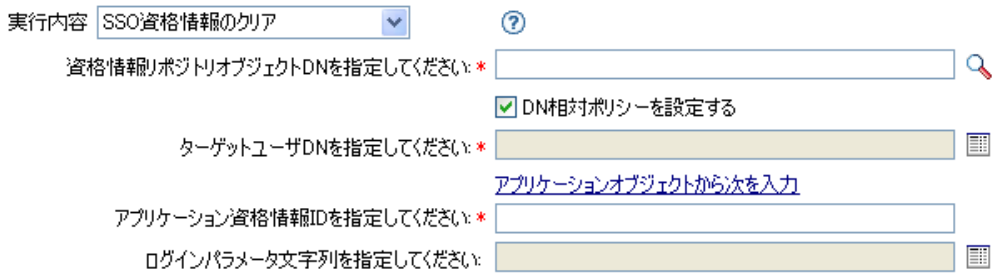
リポジトリとアプリケーションのオブジェクトを作成したら、ポリシーを作成して SecureLogin 情報をプロビジョニングする必要があります。ポリシーは、Designer または iManager で作成できます。

- 28 ページのセクション 3.6.1「Designer での Novell SecureLogin の資格情報プロビジョニングポリシーの作成」
- 30 ページのセクション 3.6.2「iManager での Novell SecureLogin の資格情報プロビジョニングポリシーの作成」

3.6.1 Designer での Novell SecureLogin の資格情報プロビジョニングポリシーの作成

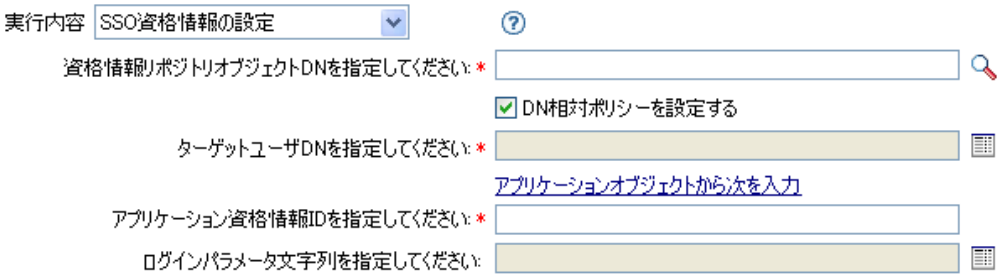
ポリシーは、リポジトリとアプリケーションのオブジェクトに格納された情報を使用します。

1. ポリシービルダで、新しいポリシーを作成します。
2. (オプション) オブジェクトをプロビジョニング解除できるように SSO 資格情報を消去するには、[*SSO 資格情報のクリア*] アクションを選択して、以下のフィールドに入力します。



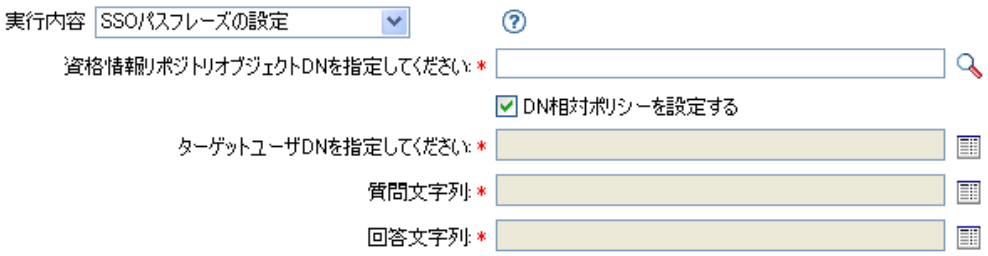
- **資格情報リポジトリオブジェクト DN を指定してください：**リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザ DN を指定してください：**引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーション資格情報 ID を指定してください：**アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータ文字列を指定してください：**文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

3 (オプション) ユーザオブジェクトの作成時またはパスワードの変更時に SSO 資格情報を設定するには、[*SSO 資格情報の設定*] アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を指定してください：**リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザ DN を指定してください：**引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーション資格情報 ID を指定してください：**アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータ文字列を指定してください：**文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

4 (オプション) ユーザオブジェクトのプロビジョニング時にユーザオブジェクトに対して SecureLogin のパスフレーズと回答を作成するには、[*SSO パスフレーズの設定*] アクションを選択して、以下のフィールドに入力します。

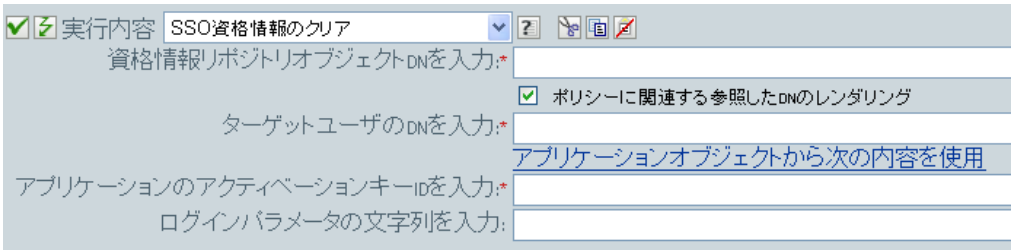


- **資格情報リポジトリオブジェクト DN を指定してください :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザ DN を指定してください :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **質問文字列 :** パスフレーズの質問を指定します (ワークシート項目の 16 を参照してください)。
- **回答文字列 :** パスフレーズの回答を指定します (ワークシート項目の 16 を参照してください)。

3.6.2 iManager での Novell SecureLogin の資格情報プロビジョニングポリシーの作成

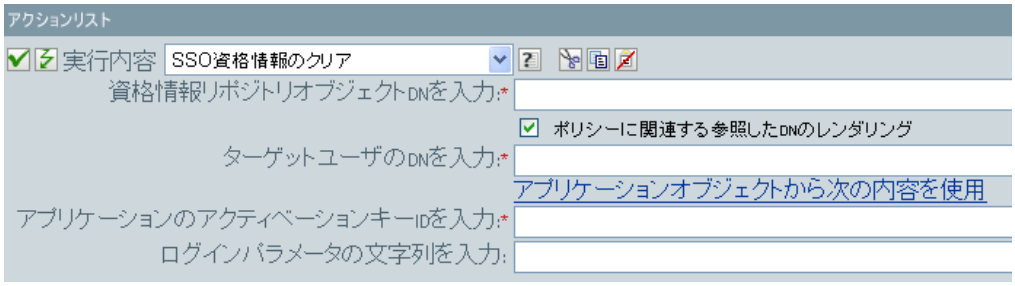
ポリシーは、リポジトリとアプリケーションのオブジェクトに格納された情報を使用します。

1. ポリシービルダで、新しいポリシーを作成します。
2. (オプション) オブジェクトをプロビジョニング解除できるように SSO 資格情報を消去するには、[*SSO 資格情報のクリア*] アクションを選択して、以下のフィールドに入力します。



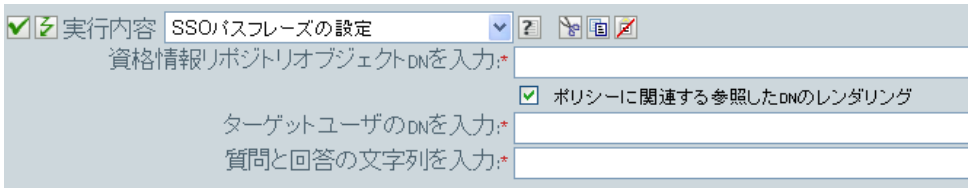
- **資格情報リポジトリオブジェクト DN を入力 :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザの DN を入力 :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーションのアクティベーションキー ID を入力 :** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータの文字列を入力 :** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

3 (オプション) ユーザオブジェクトの作成時またはパスワードの変更時に SSO 資格情報を設定するには、[*SSO 資格情報の設定*] アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を入力 :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザの DN を入力 :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーションのアクティベーションキー ID を入力 :** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータの文字列を入力 :** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

4 (オプション) ユーザオブジェクトのプロビジョニング時にユーザオブジェクトに対して SecureLogin のパスフレーズと回答を作成するには、[*SSO パスフレーズの設定*] アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を入力 :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザの DN を入力 :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **質問と回答の文字列を入力 :** 文字列ビルダを起動して、パスフレーズの質問と回答を入力します (ワークシート項目の 16 を参照してください)。

3.7 資格情報プロビジョニングポリシーの例

プロビジョニングポリシーは、各自の環境の要件を満たすように実装およびカスタマイズできます。次の例では、8 ページの 図 2-1 で示したシナリオのポリシーの設定方法について説明します。

財務部のシナリオでは、SecureLogin のプロビジョニングは、SAP 内にパスワードが設定された後に実行されます。必要なパラメータの多くはスタティックに設定されており、リポジトリやアプリケーションのオブジェクトを介してすべてのポリシーで使用可能です。ただし、スタティックでないデータパラメータ (sapUsername、password、DirXML-

ADContext および workforceID) もあります。これらのパラメータは、SAP ユーザ管理ドライバの <add> または <modify-password> コマンドが実行され、<output> ステータスドキュメントが SAP ユーザ管理ドライバシムから返された後にのみ使用可能です。<ouput> ドキュメントには、購読者チャネルの操作属性が含まれていないため、コマンドのユーザコンテキストは失われ、その結果、オブジェクトへのクエリが阻まれます。そのため、次のことを実行する必要があります。

- SAP ユーザドライバの購読者作成ポリシーによって、スタティックでないデータパラメータの存在を強制するようにします。
- 購読者コマンドを SAP ユーザドライバシムへ発行する前に、プロビジョニング操作に必要なスタティックでないパラメータをキャッシュします。
- コマンドが正常に実行された後は、SecureLogin のプロビジョニングで使用するため、キャッシュされたデータを取得します。

注 : Identity Manager 3.0 Support Pack 1 のメディアには、XML 形式で使用可能なサンプルポリシーがあります。ファイル名は、SampleInputTransform.xml、SampleSubCommandTransform.xml、および SampleSubEventTransform.xml です。これらのファイルは、次のディレクトリにあります (プラットフォーム別に示します)。

- linux\setup\utilities\cred_prov
- nt\dirxml\utilities\cred_prov
- nw\dirxml\utilities\cred_prov

これらのファイルは、ユーティリティのインストール時に資格情報プロビジョニングのサンプルポリシーを選択すると、Identity Manager サーバにインストールされます。サンプルポリシーは、次の場所にインストールされます (プラットフォーム別に示します)。

- Windows: C:\Novell\NDS\DirXMLUtilities (デフォルト。インストール時にユーザが変更可能。)
- NetWare®: SYS:\System\DirXmlUtilities
- Linux (eDir 8.7): /usr/lib/dirxml/rules/credprov
- Linux (eDir 8.8.1): /opt/novell/eDirectory/lib/dirxml/rules/credprov (デフォルト。インストール時にユーザが変更可能。)

サンプルポリシーは、各自の環境で機能するポリシーを開発するための開始ポイントとして使用できます。

3.8 操作データキャッシング

必須の操作データキャッシングに使用できるメカニズムは、<operation-data> 要素です。SecureLogin アカウントは <add> または <modify-password> コマンドのいずれかからプロビジョニングする必要があるため、スタティックでないデータキャッシングポリシーを実装する論理的な場所は、購読者コマンド変換ポリシー内になります。次の例に、一般的な SecureLogin のプロビジョニングにおける <operation-data> 要素を示します。

```
<operation-data> <nsl-sync-data> <nsl-target-user-dn>
cn=GLCANYON,ou=finance,dc=prod,dc=testco,dc=com </nsl-target-user-dn> <nsl-app-
username>GCANYON</nsl-app-username> <password><!-- コンテンツは非表示 --></
password> <nsl-passphrase-answer>50024222</nsl-passphrase-answer> </nsl-sync-data> </
operation-data>
```

8 ページの 図 2-1 で示したサンプルの財務部のシナリオでは、操作データのペイロードを入力するのに以下の値が必要です。

- <nsl-target-user-dn> 要素は、識別ボールトの DirXML-ADContext 属性を使用して入力されます。この属性は、Active Directory ドライバによって設定されたものです。AD ドライバによって値が設定されたときに SAP ユーザドライバに通知されるようにするには、DirXML-ADContext を購読者フィルタに通知属性として追加してください。
- <nsl-app-username> 要素は、sapUsername 属性によって入力されます。<add> コマンドは、SAP ユーザドライバの作成ポリシーによって生成されるため、操作属性として使用できます。SAP ユーザドライバを使用すると、SAP ユーザ名の値が関連付けの値の一部になります。このことは、パスワード変更イベントの場合、関連付けから名前が解析されるということ意味します。
- パスワード要素には、<add> または <modify-password> コマンド内の <password> 要素の値が入力されます。
- <nsl-passphrase-answer> 要素には、識別ボールトから workforceID 属性の値が入力されます。この属性は、SAP HR ドライバによって設定されたものです。この値は、識別ボールトへの初めてのプロビジョニングで設定されますが、workforceID を通知属性として購読者フィルタに追加することを推奨します。

3.9 SecureLogin のプロビジョニング

このプロビジョニングシナリオでは、SecureLogin 資格情報プロビジョニング用に操作データが取得され、使用される最初の場所は、ドライバの入力変換ポリシー内に指定されています。サンプルのシナリオでは、次の 3 つのポリシーが実装されています。

- パスワードが正常に同期された後の SecureLogin 資格情報の設定
- SecureLogin パスフレーズと回答の設定
- アプリケーションユーザが削除された場合の SecureLogin 資格情報の削除 (識別ボールトのオブジェクトは削除されない)

注 : SampleInputTransform.xml ファイルには、SecureLogin 資格情報をパスワード同期が成功した後に設定するためのサンプルポリシーがあります。このファイルは、Identity Manager 3.0 Support Pack 1 メディアの「Credential Provisioning」フォルダにあります。

SecureLogin 資格情報の設定ポリシーでは、プロビジョニングが実行されるのは、返されたコマンドステータスが「成功」で、以前に設定した <operation-data> が存在する場合のみに限定してください。

3.10 SecureLogin のプロビジョニング解除

「接続システムのユーザアカウントは削除し、識別ボールトのアカウントは残す」というポリシーを使用する状況は数多く考えられます。財務のシナリオでは、ユーザの識別ボールトの employeeStatus 属性値が「I」に設定された場合に、SAP ユーザのアカウントを削除して、SecureLogin 資格情報のプロビジョニングを解除します。この状況を処理するため、SAP ユーザドライバの購読者イベント変換に、変更属性値をオブジェクトの削除に変換するポリシーが含まれています。Active Directory アカウントの名前は、<delete> コマンドが実行された後も必要なため、<operation-data> イベントを <delete> コマンドに設定

して、入力変換ポリシー内の SecureLogin のプロビジョニング解除ポリシーで使用できるようにする必要があります。

<operation-data> <nsl-sync-data> <nsl-target-user-dn> cn=GLCANYON,ou=finance,dc=prod,dc=testco,dc=com </nsl-targer-user-dn> </nsl-sync-data> </operation-data>

<modify> イベントを <delete> に変換してこの要素を作成するポリシーは、SampleSubEventTransform.xml ファイル内のサンプル資格情報プロビジョニングポリシーにあります。

ポリシーが作成されたら、63 ページの第 6 章「Novell 資格情報プロビジョニングポリシーの管理」に進んでください。

Novell SecretStore による Novell 資格情報プロビジョニングポリシー

4

Novell® 資格情報プロビジョニングポリシーにより、アプリケーション資格情報を Novell SecretStore 内のユーザオブジェクトにプロビジョニングできます。アプリケーションサーバおよびユーザ資格情報を、通常の Identity Manager プロビジョニングシナリオの一部としてプロビジョニングできるため、より安全で同期された Web シングルサインオン機能をユーザに提供できます。

この項では、Identity Manager 内のオブジェクトとポリシーを設定するために必要な手順について記載しています。SecretStore コンポーネントの展開および設定についての情報は含まれていません。SecretStore のマニュアルは、「Novell SecretStore 3.3.3 のマニュアル (http://www.novell.com/documentation/secretstore33/index.html)」を参照してください。

SecretStore で資格情報のプロビジョニングを実装するには、リポジトリオブジェクト、アプリケーションオブジェクト、およびポリシーの作成が必要です。リポジトリとアプリケーションのオブジェクトには、Identity Manager が使用できるように SecretStore の情報が格納されます。ポリシーは、ドライバが資格情報プロビジョニングを使用できるようにするために使用されます。次のオプションも設定できます。

- 資格情報プロビジョニングは、発行者チャネル、購読者チャネル、または両方のチャネルで設定できます。
- SecretStore の同期は、アプリケーションのパスワード同期の一部として発生させたり、他のイベントによってトリガすることができます。
- Web サービスの資格情報は、アプリケーションのアカウントをプロビジョニングしなくてもプロビジョニングできます。

パスワードのランダム生成機能を使用して、接続システム上のユーザアカウントのパスワードを設定し、識別情報管理環境のセキュリティをさらに高めることができます。詳細については、『*Novell Identity Manager 3.5.1 管理ガイド*』でパスワードのランダム生成機能の使い方を参照してください。

図 4-1 は、一般的なシナリオを簡略に示したものです。このシナリオでは、Single Sign-On の資格情報を GroupWise® の新規ユーザにプロビジョニングしています。この部署では、SAP HR システムと Identity Manager を使用して、識別ボールト内に新しいユーザをプロビジョニングします。組織の情報に基づき、ユーザは、eDirectory™ 内に実装された部署の認証ツリー内にプロビジョニングされます。ここが新しいユーザがネットワークに対して認証される場所であり、会社のファイアウォールの外から安全な Single Sign-On 機能を提供するために、Novell iChain® または Novell Access Manager™ によって使用される GroupWise セキュリティの資格情報リポジトリになります。ユーザは続いて、Identity Manager によって GroupWise にプロビジョニングされ、それらのシステムの資格情報は、認証ツリー内の SecretStore 属性に同期されます。

図 4-1 SecretStore による資格情報プロビジョニング

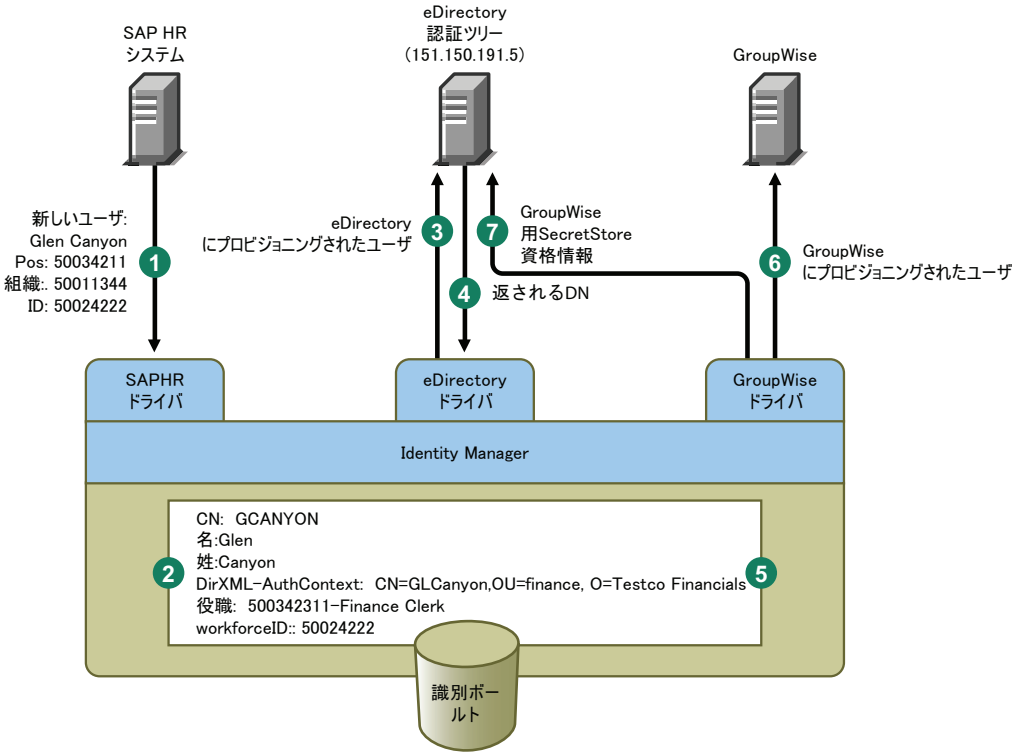


図 4-1 は、以下のプロビジョニング手順を示しています。

1. SAP HR システムが、新入社員 Glen Canyon のデータを発行します。Identity Manager の SAP HP ドライバが、このデータを処理します。
2. 新しいユーザオブジェクトが、CN 値「GCANYON」および workforceID 値「50024222」を使用して、識別ボールト内に作成されます。このユーザは、会社の財務組織に割り当てられているため、財務部の eDirectory サーバに認証される必要があります。Identity Manager の eDirectory ドライバがドメインを同期すると、識別ボールトの情報を使用できるようになります。
3. Glen は、Finance 部の eDirectory サーバにプロビジョニングされます。
4. このドライバは、Glen の完全識別 LDAP 名「 CN=GLCanyon,OU=finance,O=Testco Financials」を取得するように設定されます。
5. この LDAP 名は、識別ボールト内の GCANYON ユーザの DirXML-AuthContext (ユーザオブジェクトの拡張属性、DirXML-ADContext のコピー) 属性に配置されます。

   これで、識別ボールト内で必要な属性が使用できるようになったので、GroupWise ドライバによって、GCANYON オブジェクトの属性が処理されます。
6. Glen は Finance 組織に所属するため、ドライバは GCANYON の GroupWise アカウントを Finance 部の GroupWise ドメインサーバ上にプロビジョニングします。
7. アカウントの作成が成功すると、GroupWise ドライバのポリシーによって、Glen の GroupWise 認証資格情報がこのユーザの eDirectory ユーザアカウントの SecretStore にプロビジョニングされます。

Glen がインターネットから会社の Web サイトに認証される場合、iChain サーバが SecretStore 資格情報を使用して、このユーザの安全な GroupWise 電子メールアカウントへ

の認証情報を入力するので、GroupWise 資格情報を自分で入力する必要も、会社のリソースにセキュリティを追加設定する必要もありません。

5 Novell SecretStore による Novell 資格情報プロビジョニングポリシーの実装

Novell SecretStore® による Novell® 資格情報プロビジョニングポリシーの実装は、柔軟にカスタマイズできます。実装手順は、SecretStore がインストールされているプラットフォーム、プロビジョニング対象のアプリケーション、使用する Identity Manager ドライバによって異なります。

SecretStore による資格情報プロビジョニングポリシーを実装するには ,、次の手順に従います。

- 39 ページのセクション 5.1「Novell SecretStore による資格情報プロビジョニングポリシーの要件」
- 40 ページのセクション 5.2「Novell SecretStore の展開環境設定パラメータの決定」
- 43 ページのセクション 5.3「Novell SecretStore のリポジトリオブジェクトの作成」
- 50 ページのセクション 5.4「Novell SecretStore のアプリケーションオブジェクトの作成」
- 57 ページのセクション 5.5「Novell SecretStore の資格情報プロビジョニングポリシーの作成」
- 60 ページのセクション 5.6「資格情報プロビジョニングポリシーの例」
- 60 ページのセクション 5.7「操作データキャッシング」
- 61 ページのセクション 5.8「SecretStore のプロビジョニング」
- 61 ページのセクション 5.9「SecretStore のプロビジョニング解除」

5.1 Novell SecretStore による資格情報プロビジョニングポリシーの要件

SecretStore による資格情報プロビジョニングポリシーを使用するには、次の要件を満たす必要があります。

- Identity Manager 3.0.1 以降
- eDirectory™ 8.7x または eDirectory 8.8.1 以降。eDirectory 8.8 はサポートされていません。
- jsso.jar、idmcp.jar、および jnet.jar が Identity Manager Java ライブラリの標準の場所にあることを確認します。
- Novell SecretStore 3.3 以降

要件が満たされていることを確認したら、40 ページのセクション 5.2「Novell SecretStore の展開環境設定パラメータの決定」に進んでください。

5.2 Novell SecretStore の展開環境設定パラメータの決定

図 4-1 の展開シナリオで説明されている同期機能を提供するには、まず、Identity Manager および SecretStore 環境に関連したすべてのビジネスプロセス情報を収集します。40 ページの ï 5-1§ 「SecretStore の資格情報プロビジョニングポリシーワークシート」を印刷して、情報を記録するためのワークシートとして使用してください。

表 5-1 *SecretStore の資格情報プロビジョニングポリシーワークシート*

必要な環境設定情報	情報
1) Web シングルサインオンのプロビジョニング用に設定するアプリケーション。	
2) SecretStore リポジトリサーバの DNS 名または IP アドレス。	
3) SecretStore リポジトリサーバの SSL LDAP ポート。	
4) SecretStore リポジトリサーバ管理者の完全修飾された LDAP 識別名。	
5) SecretStore リポジトリサーバの管理者のパスワード。	
6) SecretStore サーバからエクスポートされる、SSL 証明書へのフルパスおよび証明書名。証明書は、Identity Manager サーバのローカルに配置する必要があります。	
7) 1 つの SecretStore リポジトリを複数のドライバで使用するか、または各ドライバで専用のリポジトリを使用するかを決定する。	
8) 使用される SecretStore のシークレットタイプを記録する。 サポートされるシークレットタイプには次に示す 2 つの種類があります。 ◆ A: アプリケーションシークレット (SS_App: プレフィックス) ◆ C: 資格情報セットシークレット (SS_CredSet: プレフィックス)	
9) プロビジョニング対象アプリケーションごとのアプリケーション ID または資格情報セット。	
10) 各アプリケーションに必要な認証キー (ユーザ名やパスワードなど) をすべて一覧にする。これらはアプリケーションごとに異なる場合があります。	
11) 認証キーの値をスタティックな値に設定するかどうかを決定する。	

必要な環境設定情報	情報
12) ユーザごとに異なる値である (または異なる値にできる) スタティックでない値の場合は、そのスタティックでない情報のソースを書き留める (イベント情報または識別ボールトの属性値)。	
13) ターゲットアプリケーションへのパスワードも同期しているドライバに SecretStore のプロビジョニングを実装する場合、SecretStore のプロビジョニングを、ターゲットアプリケーションのサーバにパスワードが設定される前と後のどちらで開始するかを決定する。	
14) リポジトリおよびアプリケーションのオブジェクトが格納されるドライバオブジェクトの名前 (格納先ドライバは別々に指定可能)。	
15) ターゲットアプリケーションのユーザオブジェクトの DN を決定する。	

5.2.1 プロビジョニング環境設定データの例

36 ページの 図 4-1 のプロビジョニングシナリオを使用したサンプルデータを次に示します。ここでは、財務 eDirectory 認証ツリー内のユーザに、財務部の GroupWise® ドメインサーバの SecretStore 資格情報をプロビジョニングします。

表 5-2 *SecretStore の資格情報プロビジョニングポリシーワークシートの例*

必要な環境設定情報	情報
1) Web シングルサインオンのプロビジョニング用に設定するアプリケーション。	GroupWise
2) SecretStore リポジトリサーバの DNS 名または IP アドレス。	151.150.191.5
3) SecretStore リポジトリサーバの SSL LDAP ポート。	636
4) SecretStore リポジトリサーバ管理者の完全修飾された LDAP 識別名。	cn=admin,ou=finance,o=Tesetco Financials
5) SecretStore リポジトリサーバの管理者のパスワード。	dixml
6) SecretStore サーバからエクスポートされる、SSL 証明書へのフルパスおよび証明書名。証明書は、Identity Manager サーバのローカルに配置する必要があります。	c:\novell\nds\FinanceAD.cer
7) 1 つの SecretStore リポジトリを複数のドライバで使用するか、または各ドライバで専用のリポジトリを使用するかを決定する。	この例では、リポジトリは 1 つだけにします。

必要な環境設定情報	情報
8) 使用される SecretStore のシークレットタイプを記録する。 サポートされるシークレットタイプには次に示す 2 つの種類があります。 ◆ A: アプリケーションシークレット (SS_App: プレフィックス) ◆ C: 資格情報セットシークレット (SS_CredSet: プレフィックス)	
9) プロビジョニング対象アプリケーションごとのアプリケーション ID または資格情報セット。	GroupWise_Credentials
10) 各アプリケーションに必要な認証キー (ユーザ名やパスワードなど) をすべて一覧にする。これらはアプリケーションごとに異なる場合があります。	ユーザ名 パスワード
11) 認証キーの値をスタティックな値に設定するかどうかを決定する。	このシナリオではスタティックな情報は使用しません。
12) ユーザごとに異なる値である (または異なる値にできる) スタティックでない値の場合は、そのスタティックでない情報のソースを書き留める (イベント情報または識別ボールトの属性値)。	ユーザ名 : 識別ボールトの属性「CN」パスワード : イベント <password>
13) ターゲットアプリケーションへのパスワードも同期しているドライバに SecretStore のプロビジョニングを実装する場合、SecretStore のプロビジョニングを、ターゲットアプリケーションのサーバにパスワードが設定される前と後のどちらで開始するかを決定する。	After
14) リポジトリおよびアプリケーションのオブジェクトが格納されるドライバオブジェクトの名前 (格納先ドライバは別々に指定可能)。	GroupWise-Finance ドライバ
15) ターゲットアプリケーションのユーザオブジェクトの DN を決定する。	識別ボールト属性の「DirXML-ADContext」

その他の環境設定情報 :

- 財務部の eDirectory ツリーは、すべての財務アプリケーションの SecretStore リポジトリとして動作します。
- Finance 部関連のプロビジョニングドライバは、すべて「Finance Drivers」という名前のドライバセット内に設定されます。
- 識別ボールトの属性 employeeStatus の値が「I」に設定された場合、GroupWise ユーザアカウントを削除して、その GroupWise ユーザアカウントの SecretStore 資格情報も eDirectory ユーザから削除する必要があります。

収集したデータから見ると、SecretStore リポジトリの情報は、財務部のアプリケーションをプロビジョニングするすべてのドライバに対してグローバルです。また、すべてのプロビジョニング情報は、GroupWise のログインパラメータであるユーザ名、パスワードおよびターゲットユーザの DN を除き、スタティックに設定されています。

すべての環境設定データを決定したら、43 ページのセクション 5.3「Novell SecretStore のリポジトリオブジェクトの作成」に進んでください。

5.3 Novell SecretStore のリポジトリオブジェクトの作成

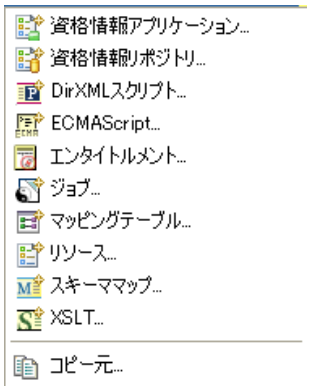
リポジトリオブジェクトには、SecretStore のスタティックな環境設定情報が保存されます。リポジトリの情報は、アプリケーション資格情報を使用するアプリケーションからは独立しています。この情報は、接続システム (SAP、PeopleSoft、Notes など) に関係なく、すべてのプロビジョニングイベントに適用されます。リポジトリオブジェクトは、Designer または iManager で作成できます。

- 43 ページのセクション 5.3.1「Designer での Novell SecretStore のリポジトリオブジェクトの作成」
- 46 ページのセクション 5.3.2「iManager での Novell SecretStore のリポジトリオブジェクトの作成」

5.3.1 Designer での Novell SecretStore のリポジトリオブジェクトの作成

次に示すのは、Designer でリポジトリオブジェクトを作成する方法のうちの 1 つです。

1. アウトラインビューで、リポジトリオブジェクトを格納するドライバオブジェクトを右クリックします。
2. *［新規］>［資格情報リポジトリ］*の順にクリックします。

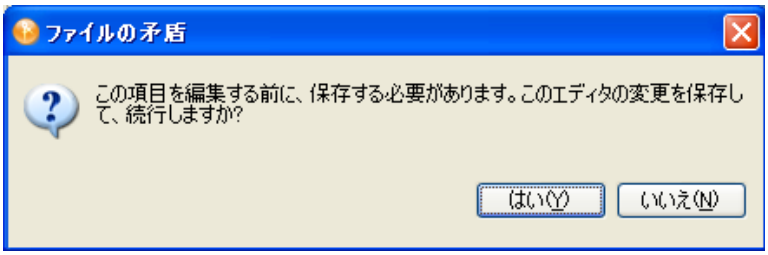


3. リポジトリオブジェクトの名前を指定します。
4. SecretStore テンプレートを使用するため、［*NSSRepository.xml*］を選択します。

［*オブジェクトの作成後にエディタを開く*］チェックボックスがオンになっていることを確認します。

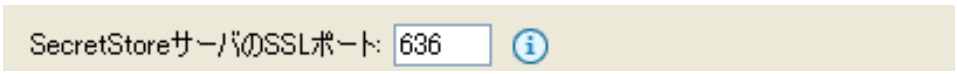
5 ［*OK*］をクリックします。

6 ［*はい*］をクリックして、新しいリポジトリオブジェクトを保存します。



7 SecretStore サーバの DNS 名または IP アドレスを指定します (ワークシート項目の 2 を参照してください)。

8 SecretStore サーバの SSL ポートを指定します (ワークシート項目の 3 を参照してください)。



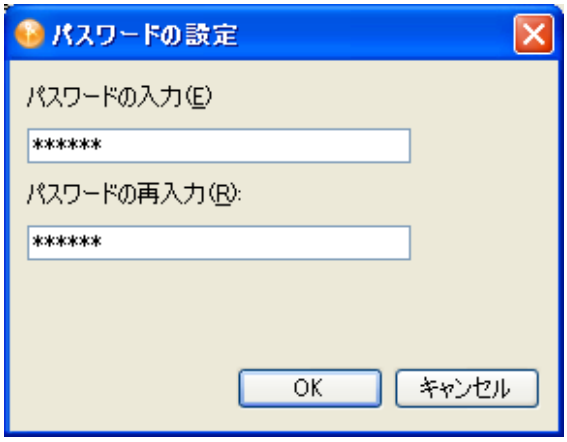
9 SecretStore サーバからエクスポートされる SSL 証明書へのフルパスを指定します。このパスには証明書名を含め、Identity Manager サーバのローカルに配置する必要があります (ワークシート項目の 6 を参照してください)。

SSL 証明書のエクスポート方法については、証明書サーバ (http://www.novell.com/documentation/crt32/index.html) のマニュアルを参照してください。

10 SecretStore 管理者の完全修飾 LDAP 識別名を指定します (ワークシート項目の 4 を参照してください)。

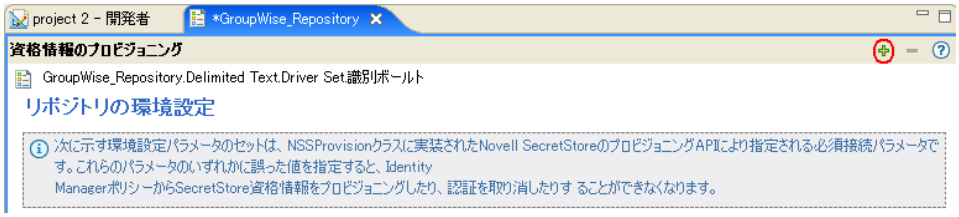
11 [*パスワードの設定*] をクリックします。

12 SecretStore 管理者のパスワードを 2 回入力し、[OK] をクリックします (ワークシート項目の 5 を参照してください)。



13 情報を確認し、[*保存*] アイコンをクリックして情報を保存します。

14 (オプション) リポジトリオブジェクトに対する他の環境設定パラメータを作成する場合は、[*新しい項目の追加*] アイコンをクリックします。

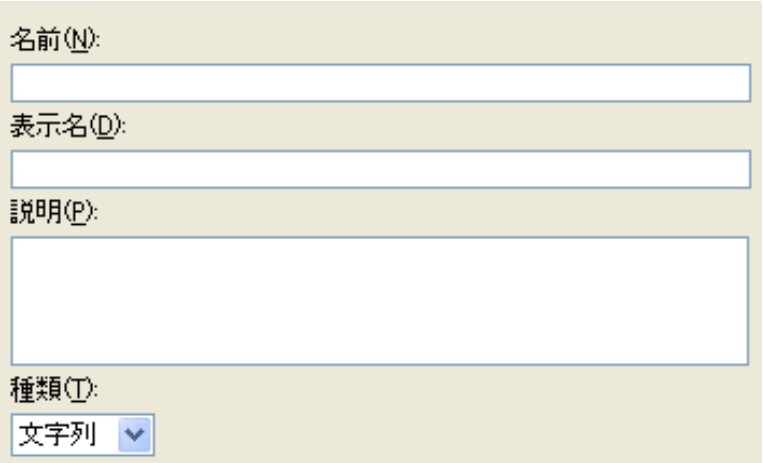


14a パラメータの名前を指定します。

14b パラメータの表示名を指定します。

14c 参照情報として、パラメータの説明を入力します。

パラメータは文字列で保存されます。



14d ［*OK*］をクリックします。

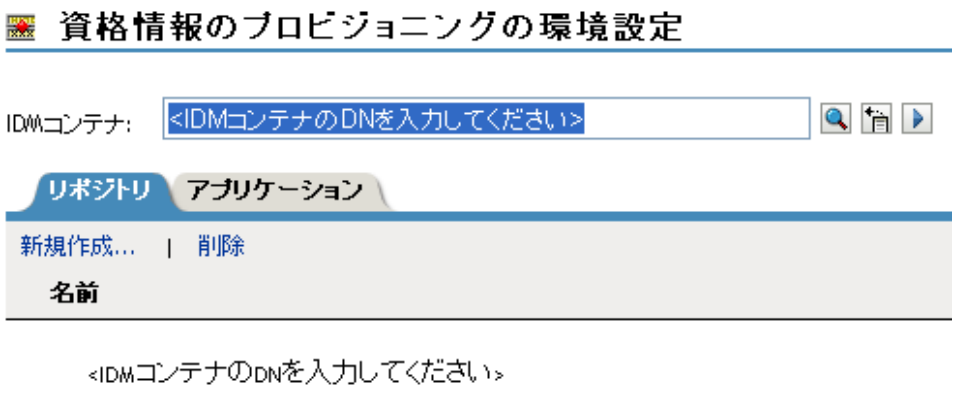
14e ［*保存*］アイコンをクリックして、リポジトリオブジェクトを保存します。

リポジトリオブジェクトが作成されたら、22 ページの 「Novell SecureLogin のアプリケーションオブジェクトの作成」に進んでください。

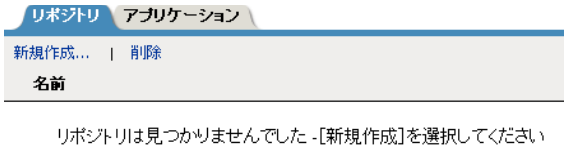
5.3.2 iManager での Novell SecretStore のリポジトリオブジェクトの作成

1 iManager で、［*資格情報のプロビジョニング*］>［*環境設定*］の順に選択します。

2 リポジトリオブジェクトを保存するドライバオブジェクトを参照して選択します。



3 ［*新規作成*］をクリックしてリポジトリを作成します。



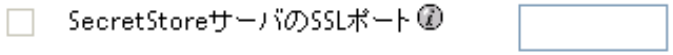
4 リポジトリオブジェクトの名前を指定します。

5 SecretStore テンプレートを使用してリポジトリを作成するため、［*NSSRepository.xml*］を選択します。

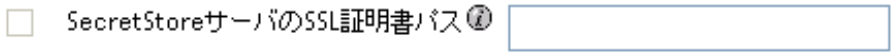
6 ［*OK*］をクリックします。

7 SecretStore サーバの DNS 名または IP アドレスを指定します (ワークシート項目の 2 を参照してください)。

8 SecretStore サーバの SSL ポートを指定します (ワークシート項目の 3 を参照してください)。



9 SecretStore サーバからエクスポートされる SSL 証明書へのフルパスを指定します。このパスには証明書名を含め、Identity Manager サーバのローカルに配置する必要があります (ワークシート項目の 6 を参照してください)。

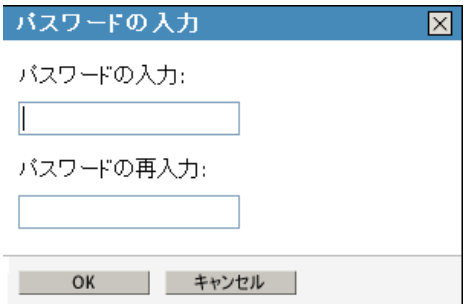


SSL 証明書のエクスポート方法については、証明書サーバ (http://www.novell.com/documentation/crt32/index.html) のマニュアルを参照してください。

10 SecretStore 管理者の完全修飾 LDAP 識別名を指定します (ワークシート項目の 4 を参照してください)。

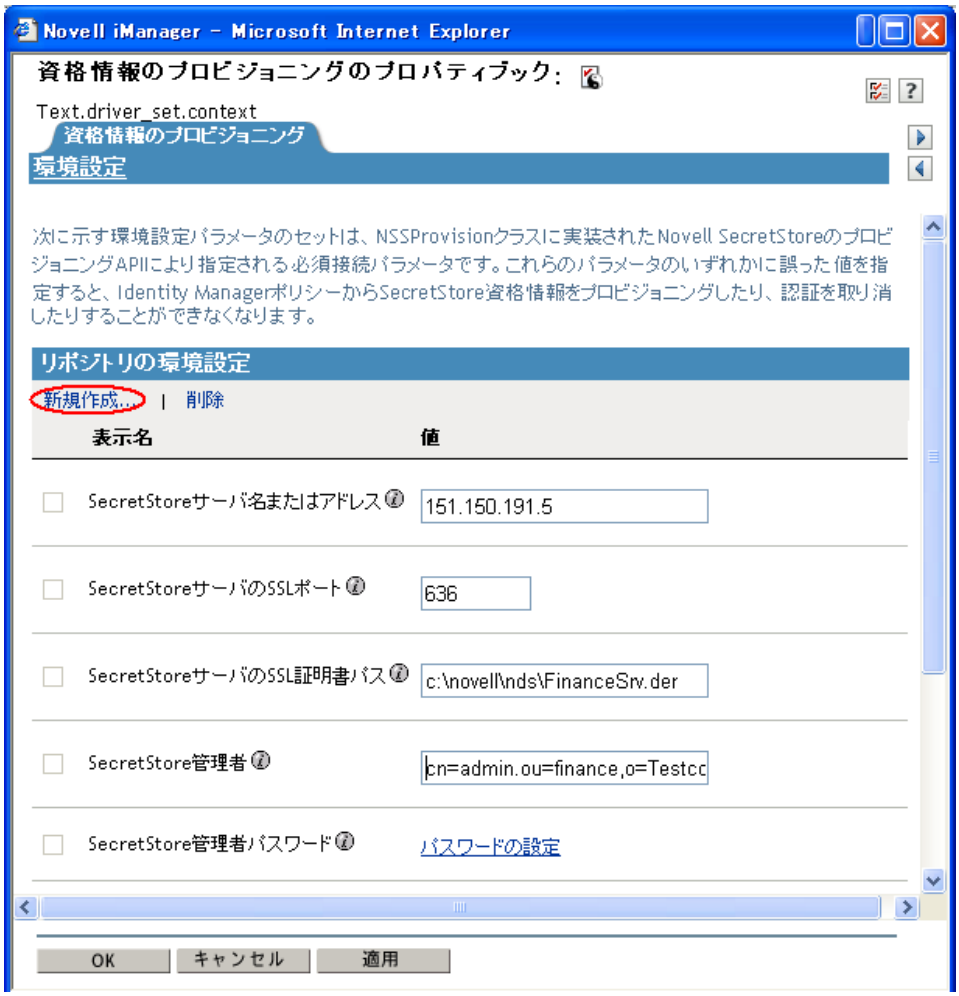
11 ［*パスワードの設定*］をクリックします。

12 SecretStore 管理者のパスワードを 2 回入力し、［*OK*］をクリックします (ワークシート項目の 5 を参照してください)。



13 指定した値を確認し、［*OK*］をクリックします。

14 (オプション) リポジトリオブジェクトに対する他の環境設定パラメータを作成する場合は、［*新規作成*］をクリックします。



この例は、36 ページの 図 4-1 のシナリオに記載されています。

14a パラメータの名前を指定します。

14b パラメータの表示名を指定します。

14c 参照情報として、パラメータの説明を入力します。

パラメータは文字列で保存されます。

14d ［*OK*］をクリックします。

リポジトリオブジェクトが作成されたら、22 ページの 「Novell SecureLogin のアプリケーションオブジェクトの作成」に進んでください。

5.4 Novell SecretStore のアプリケーションオブジェクトの作成

アプリケーションには、SecretStore のスタティックな環境設定パラメータ値が保存されます。アプリケーション情報は、そのアプリケーションの資格情報を使用しているアプリケーションに特有のものです (GroupWise クライアントの情報、SAP データベースクライアントの情報など)。アプリケーションオブジェクトは、Designer または iManager で作成できます。

- 50 ページのセクション 5.4.1「Designer での Novell SecretStore のアプリケーションオブジェクトの作成」
- 53 ページのセクション 5.4.2「iManager での Novell SecretStore のアプリケーションオブジェクトの作成」

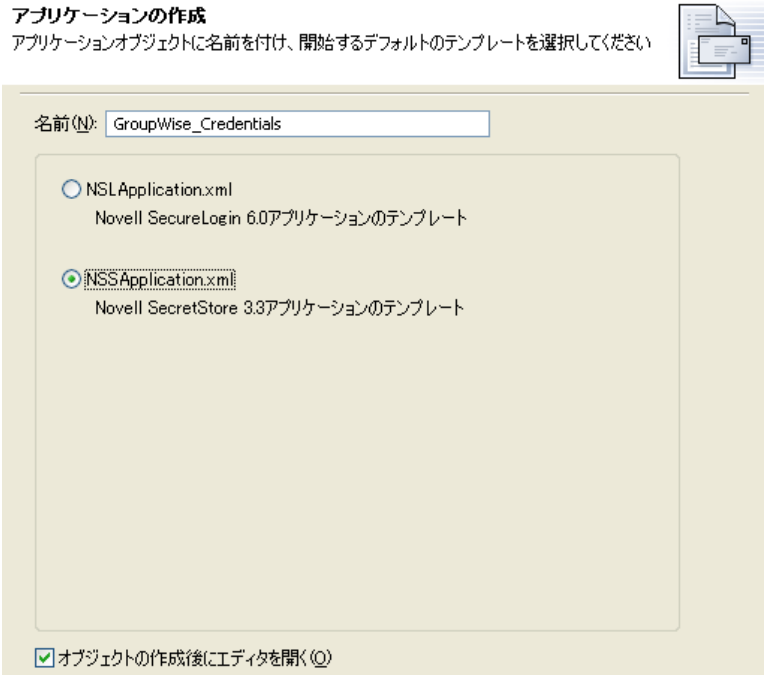
5.4.1 Designer での Novell SecretStore のアプリケーションオブジェクトの作成

次に示すのは、Designer でアプリケーションを作成する方法のうちの 1 つです。

1. アウトラインビューで、アプリケーションオブジェクトを格納するドライバオブジェクトを右クリックします。
2. *［新規作成］>［資格情報アプリケーション］*の順にクリックします。

3 アプリケーションオブジェクトの名前を指定します。

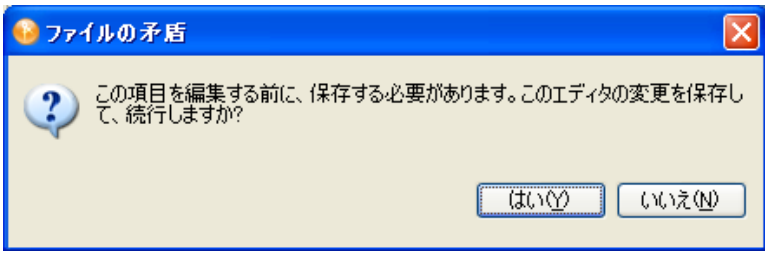
4 SecretStore テンプレートを使用するため、［*NSSApplication.xml*］を選択します。



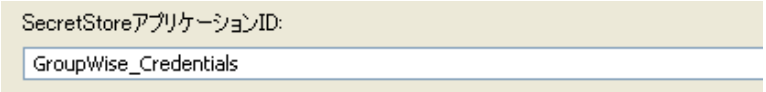
［*オブジェクトの作成後にエディタを開く*］チェックボックスがオンになっていることを確認します。

5 ［*OK*］をクリックします。

6 ［*はい*］をクリックして、新しいアプリケーションオブジェクトを保存します。

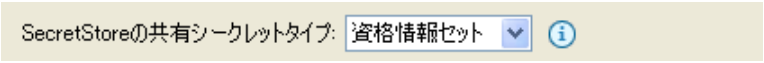


7 ［SecretStore アプリケーション ID］を指定します (ワークシート項目の 9 を参照してください)。

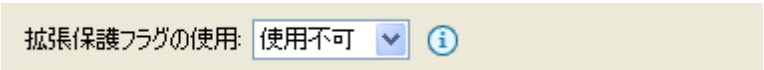


8 ［*SecretStore のシークレットタイプ*］を選択します (ワークシート項目の 8 を参照してください)。

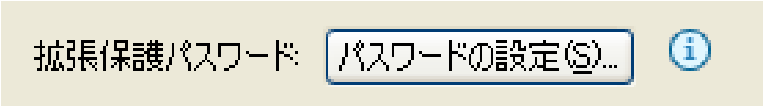
9 ［*SecretStore の共有シークレットタイプ*］を選択します (ワークシート項目の 8 を参照してください)。



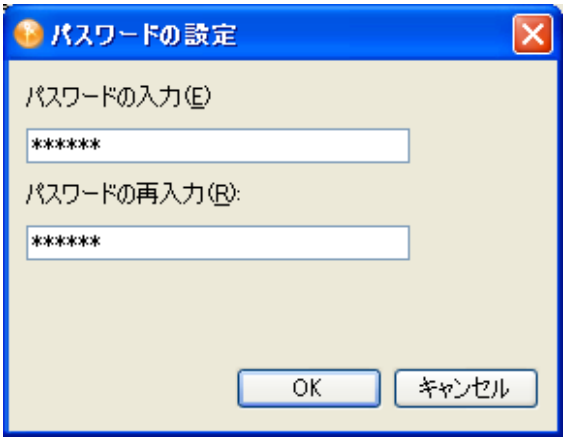
10 SecretStore の［*拡張保護フラグの使用*］で、［*使用不可*］または［*使用可能*］を選選択します。



11 有効である場合、［*パスワードの設定*］をクリックして、［*拡張保護パスワード*］を設定します。



12 パスワードを 2 回入力し、［*OK*］をクリックします。



13 ［*保存*］アイコンをクリックして、アプリケーションを保存します。

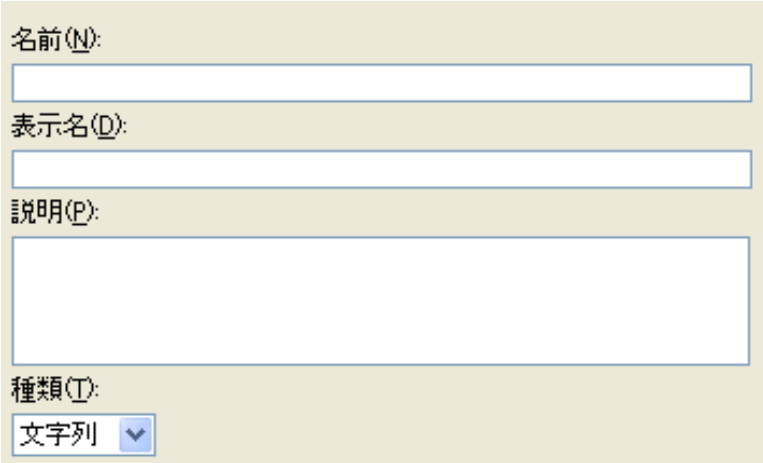
14 アプリケーションに必要な認証キーを追加するため、［*新しい項目の追加*］アイコンをクリックします。

14a 認証キーの名前を指定します。

14b 認証キーの表示名を指定します。

14c 参照情報として、認証キーの説明を入力します。

認証キーは文字列で保存されます。



14d ［*OK*］をクリックします。

14e 入力が必要な新規認証キーごとに、ステップ 14 を繰り返します。

15 認証キーがすべてのユーザ資格情報で共有するスタティックな値である場合、その値を指定します。

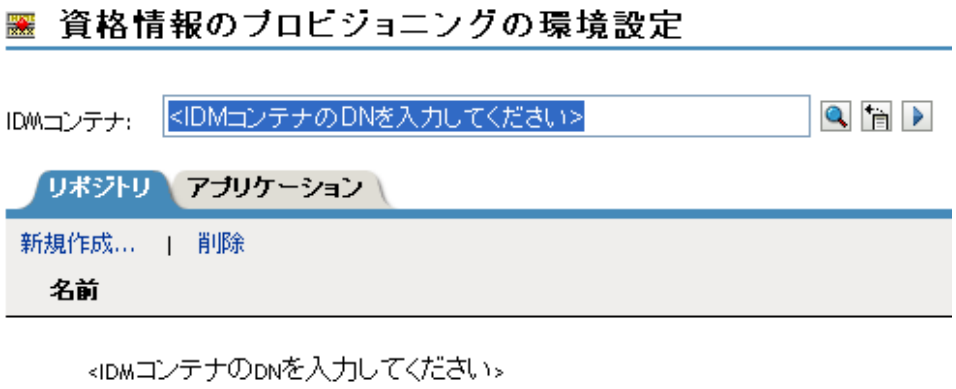
16 ［*保存*］アイコンをクリックして、アプリケーションを保存します。

アプリケーションオブジェクトが作成されたら、57 ページのセクション 5.5「Novell SecretStore の資格情報プロビジョニングポリシーの作成」に進んでください。

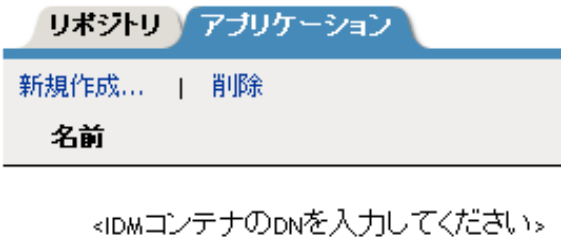
5.4.2 iManager での Novell SecretStore のアプリケーションオブジェクトの作成

1 iManager で、*［資格情報のプロビジョニング］*>*［環境設定］*の順に選択します。

2 アプリケーションオブジェクトを保存するドライバオブジェクトを参照して選択し、［*OK*］をクリックします。

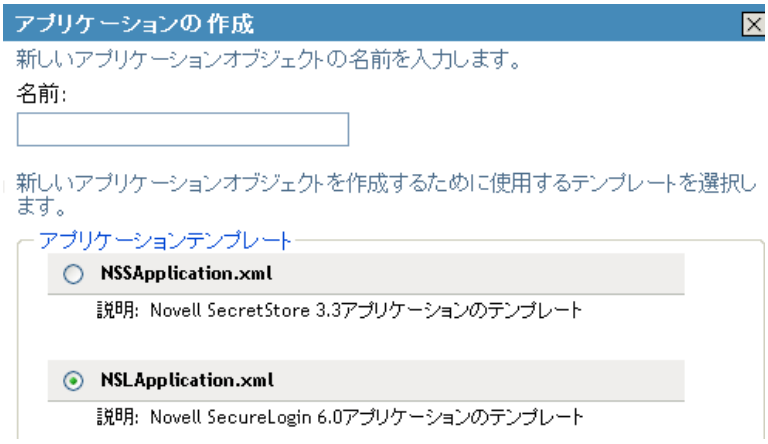


3 ［*アプリケーション*］タブを選択し、［*新規作成*］をクリックします。



4 アプリケーションオブジェクトの名前を指定します。

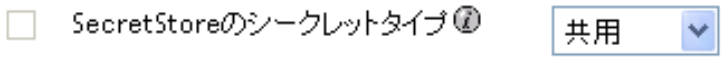
5 SecretStore テンプレートを使用してアプリケーションを作成するため、［*NSSApplication.xml*］を選択します。



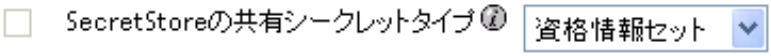
6 ［*OK*］をクリックします。

7 ［*SecretStore アプリケーション ID*］を指定します (ワークシート項目の 9 を参照してください)。

8 [*SecretStore のシークレットタイプ*] を選択します (ワークシート項目の 7 を参照してください)。SecretStore のタイプは [*共用*] または [*共用なし*] です。



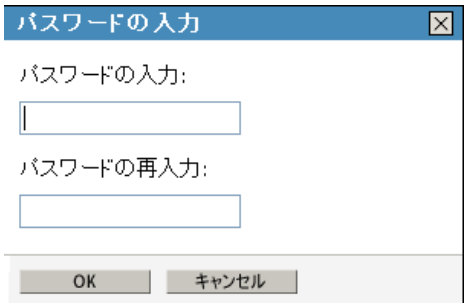
9 [*SecretStore の共有シークレットタイプ*] を選択します (ワークシート項目の 8 を参照してください)。共有される場合の SecretStore のタイプは、[*資格情報セット*] または [*アプリケーション*] です。



10 SecretStore の [*拡張保護フラグの使用*] で、[*無効*] または [*有効*] を選選択します。

11 有効である場合、[*パスワードの設定*] をクリックして、[*拡張保護パスワード*] を設定します。

12 パスワードを 2 回入力し、[*OK*] をクリックします。



13 アプリケーションで必要な認証キーを作成するため、[*新規作成*] をクリックします (ワークシート項目の 10 を参照してください)。

13a 認証キーの名前を指定します。

13b 認証キーの表示名を指定します。

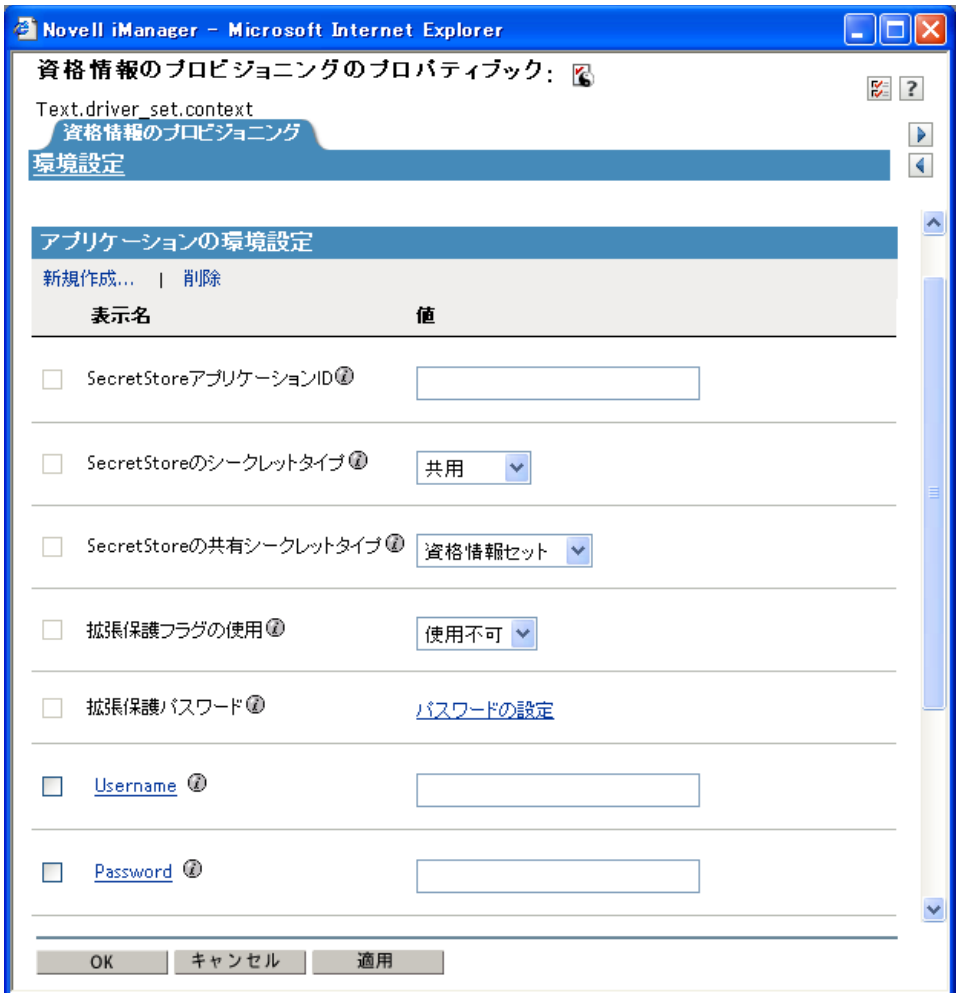
13c 参照情報として、認証キーの説明を入力します。

認証キーは文字列で保存されます。

13d ［*OK*］をクリックします。

13e アプリケーションが必要とする認証キーごとに、ステップ 13 を繰り返します。

14 認証キー値を指定し、その値がスタティックである場合は、続いて［*OK*］をクリックします。



アプリケーションオブジェクトが作成されたら、57 ページのセクション 5.5「Novell SecretStore の資格情報プロビジョニングポリシーの作成」に進んでください。

5.5 Novell SecretStore の資格情報プロビジョニングポリシーの作成

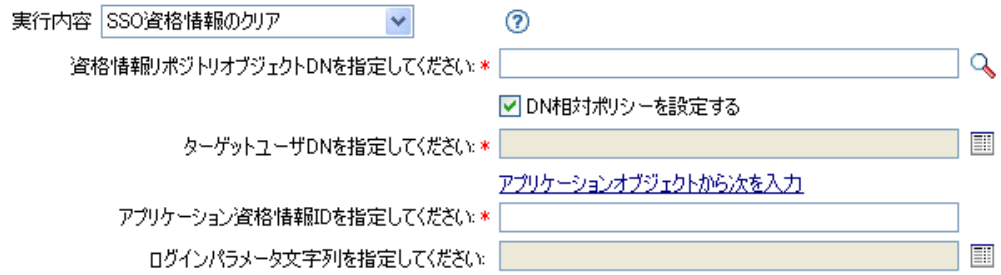
リポジトリとアプリケーションのオブジェクトを作成したら、ポリシーを作成して SecretStore 情報をプロビジョニングする必要があります。ポリシーは、Designer または iManager で作成できます。

5.5.1 Designer での Novell SecretStore の資格情報プロビジョニングポリシーの作成

ポリシーは、リポジトリとアプリケーションのオブジェクトに格納された情報を使用します。

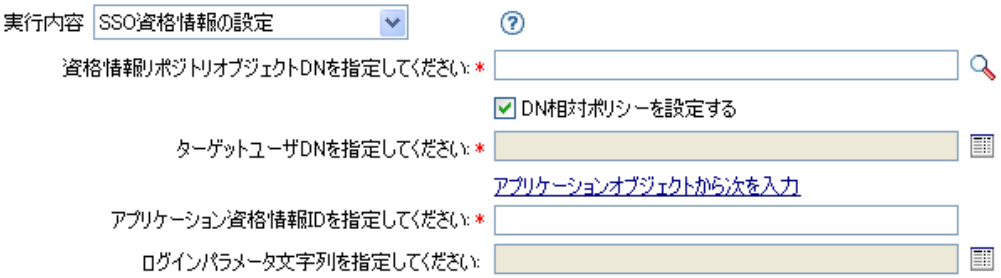
1 ポリシービルダで、新しいポリシーを作成します。

2 (オプション) オブジェクトをプロビジョニング解除できるように SSO 資格情報を消去するには、［*SSO 資格情報のクリア*］アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を指定してください：** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザ DN を指定してください：** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーション資格情報 ID を指定してください：** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータ文字列を指定してください：** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

3 (オプション) ユーザオブジェクトの作成時またはパスワードの変更時に SSO 資格情報を設定するには、［*SSO 資格情報の設定*］アクションを選択して、以下のフィールドに入力します。



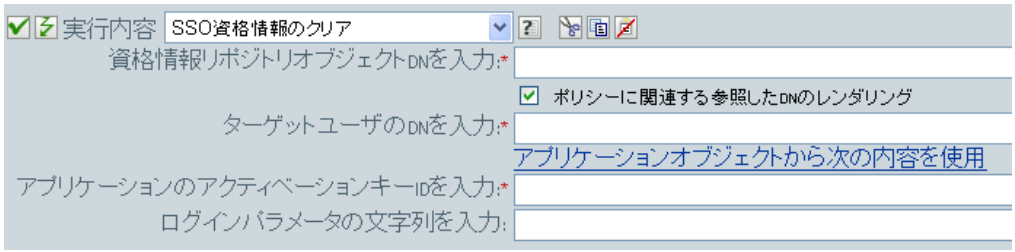
- **資格情報リポジトリオブジェクト DN を指定してください：** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザ DN を指定してください：** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーション資格情報 ID を指定してください：** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータ文字列を指定してください：** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

5.5.2 iManager での Novell SecretStore の資格情報プロビジョニングポリシーの環境設定

ポリシーは、リポジトリとアプリケーションのオブジェクトに格納された情報を使用します。

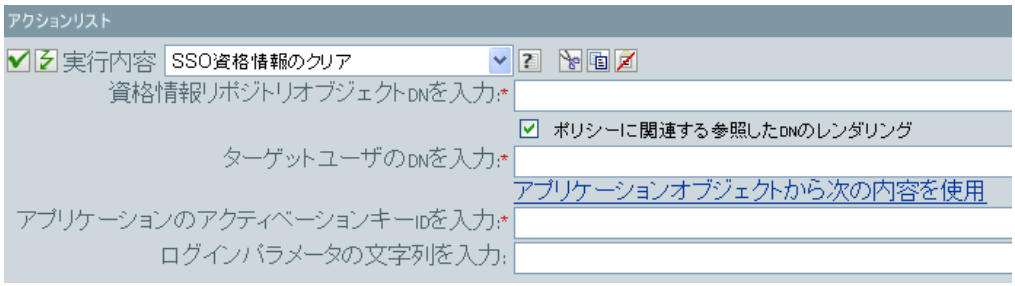
1 ポリシービルダで、新しいポリシーを作成します。

2 (オプション) オブジェクトをプロビジョニング解除できるように SSO 資格情報を消去するには、[*SSO 資格情報のクリア*] アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を入力 :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザの DN を入力 :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーションのアクティベーションキー ID を入力 :** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータの文字列を入力 :** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

3 (オプション) ユーザオブジェクトの作成時またはパスワードの変更時に SSO 資格情報を設定するには、[*SSO 資格情報の設定*] アクションを選択して、以下のフィールドに入力します。



- **資格情報リポジトリオブジェクト DN を入力 :** リポジトリオブジェクトを参照して選択します (ワークシート項目の 8 を参照してください)。
- **ターゲットユーザの DN を入力 :** 引数ビルダを使用してターゲットユーザの DN を作成します (ワークシート項目の 15 を参照してください)。
- **アプリケーションのアクティベーションキー ID を入力 :** アプリケーション ID を指定します (ワークシート項目の 9 を参照してください)。
- **ログインパラメータの文字列を入力 :** 文字列ビルダを起動して、アプリケーションの認証キーを入力します (ワークシート項目の 10 を参照してください)。

5.6 資格情報プロビジョニングポリシーの例

資格情報プロビジョニングポリシーは、各自の環境の要件を満たすように実装およびカスタマイズできます。次の例では、36 ページの 図 4-1 で示したシナリオのポリシーの設定方法について説明します。

財務部のシナリオでは、SecretStore のプロビジョニングは、GroupWise 内にパスワードが設定された後に実行されます。必要なパラメータの多くはスタティックに設定されており、リポジトリやアプリケーションのオブジェクトを介してすべてのポリシーで使用可能です。ただし、スタティックでないデータパラメータ (CN、password、および DirXML-ADContext) もあります。これらのパラメータは、GroupWise ユーザの <add> または <modify-password> コマンドが実行され、<output> ドキュメントが GroupWise ドライバシムから返された後にのみ使用可能です。<ouput> ドキュメントには、購読者の操作属性が含まれていないため、コマンドのユーザコンテキストは失われ、その結果、オブジェクトへのクエリが阻まれます。そのため、次のことを実行する必要があります。

- GroupWise ドライバの購読者作成ポリシーによって、スタティックでないデータパラメータの存在を強制するようにします。
- 購読者コマンドを GroupWise ドライバシムへ発行する前に、プロビジョニング操作に必要なスタティックでないパラメータをキャッシュします。
- コマンドが正常に実行された後は、SecretStore のプロビジョニングで使用するため、キャッシュされたデータを取得します。

注 : Identity Manager 3.0 Support Pack 1 のメディアには、XML 形式で使用可能なサンプルポリシーがあります。ファイル名は、SampleInputTransform.xml、SampleSubCommandTransform.xml、および SampleSubEventTransform.xml です。これらのファイルは、次のディレクトリにあります。

- linux\setup\utilities\cred_prov
- nt\dirxml\utilities\cred_prov
- nw\dirxml\utilities\cred_prov

これらのファイルは、ユーティリティのインストール時に資格情報プロビジョニングのサンプルポリシーを選択すると、Identity Manager サーバにインストールされます。サンプルポリシーは、次の場所にインストールされます (プラットフォーム別に示します)。

- Windows: C:\Novell\NDS\DirXMLUtilities (デフォルト。インストール時にユーザが変更可能。)
- NetWare®: SYS:\System\DirXmlUtilities
- Linux (eDir 8.7): /usr/lib/dirxml/rules/credprov
- Linux (eDir 8.8.1): /opt/novell/eDirectory/lib/dirxml/rules/credprov (デフォルト。インストール時にユーザが変更可能。)

サンプルポリシーは、各自の環境で機能するポリシーを開発するための開始ポイントとして使用できます。

5.7 操作データキャッシング

必須の操作データキャッシングに使用できるメカニズムは、<operation-data> 要素です。SecretStore アカウントは <add> または <modify-password> コマンドのいずれかからプロビ

ジョニングする必要があるため、スタティックでないデータキャッシングポリシーを実装する論理的な場所は、購読者コマンド変換ポリシー内になります。次の例に、一般的な SecretStore のプロビジョニングにおける要素を示します。

<operation-data> <nss-sync-data> <nss-target-user-dn> cn=GLCANYON,ou=finance,o=Testco Financials </nss-target-user-dn> <nss-app-username>GCANYON</nss-app-username> <password><!-- コンテンツは非表示 --></password> <nss-passphrase-answer>50024222</nss-passphrase-answer> </nss-sync-data> </operation-data>

36 ページの 図 4-1 で示したサンプルの財務部のシナリオでは、操作データのペイロードを入力するのに以下の値が必要です。

- <nss-target-user-dn> 要素は、識別ボールトの DirXML-ADContext 属性を使用して入力されます。この属性は、eDirectory ドライバによって設定されたものです。eDirectory ドライバによって値が設定されたときに GroupWise ドライバに通知されるようにするには、DirXML-ADContext を購読者フィルタに通知属性として追加してください。
- <nss-app-username> 要素は、識別ボールト内の CN 属性値によって入力されます。
- パスワード要素には、<add> または <modify-password> コマンド内の <password> 要素の値が入力されます。

5.8 SecretStore のプロビジョニング

サンプルのシナリオでは、SecretStore 資格情報プロビジョニング用の操作データが取得され、使用される最初の場所は、ドライバの入力変換ポリシー内にあります。サンプルのシナリオでは、2 つのポリシーが実装されています。

- パスワードが正常に同期された後の SecretStore 資格情報の設定。
- アプリケーションユーザが削除された場合のSecretStore資格情報の削除(識別ボールトのオブジェクトは削除されない)

注 : SampleInputTransform.xml ファイルには、SecretStore 資格情報をパスワード同期が成功した後に設定するためのサンプルポリシーがあります。このファイルは、Identity Manager 3.0 Support Pack 1 メディアの utilities ディレクトリの cred_prov フォルダにあります。

SecretStore 資格情報の設定ポリシーでは、プロビジョニングが実行されるのは、返されたコマンドステータスが「成功」で、以前に設定した <operation-data> が存在する場合のみに限定してください。

5.9 SecretStore のプロビジョニング解除

「接続システムのユーザアカウントは削除し、識別ボールトのアカウントは残す」というポリシーを使用する状況は数多く考えられます。財務のシナリオでは、ユーザの識別ボールトの employeeStatus 属性値が「I」に設定された場合に、GroupWise アカウントを削除して、SecretStore 資格情報のプロビジョニングを解除します。この状況を処理するため、GroupWise ドライバの購読者イベント変換に、変更属性値をオブジェクトの削除に変換するポリシーが含まれています。eDirectory アカウントの名前は、<delete> コマンドが実行された後も必要なため、<operation-data> イベントを <delete> コマンドに設定して、入力変換ポリシー内の SecretStore のプロビジョニング解除ポリシーで使用できるようにする必要があります。

<operation-data> <nss-sync-data> <nss-target-user-dn> cn=GLCANYON,ou=finance,o=Testco Financials </nss-targer-user-dn> </nss-sync-data> </operation-data>

<modify> イベントを <delete> に変換してこの要素を作成するポリシーは、Identity Manager 3.0 Support Pack 1 メディア上の utilities ディレクトリの cred_prov フォルダにある SampleSubEventTransform.xml という名前のファイルに XML 形式で入っています。

ポリシーが作成されたら、63 ページの第 6 章「Novell 資格情報プロビジョニングポリシーの管理」に進んでください。

Novell 資格情報プロビジョニングポリシーの管理

6

Novell® 資格情報プロビジョニングポリシーの実装後に、ポリシーを管理するために追加のタスクを実行できます。

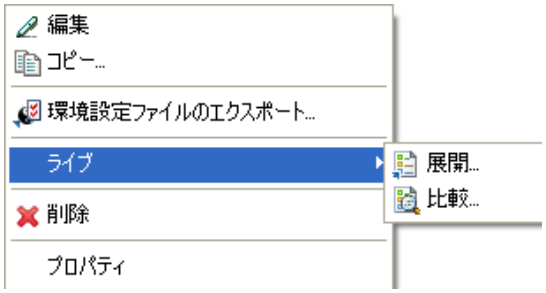
- 63 ページのセクション 6.1「リポジトリおよびアプリケーションオブジェクトの管理」
- 63 ページのセクション 6.2「資格情報プロビジョニングポリシーの管理」

6.1 リポジトリおよびアプリケーションオブジェクトの管理

リポジトリおよびアプリケーションオブジェクト (リソースオブジェクト) を管理する

1 アウトラインビューで、リソースオブジェクトを右クリックします。

2 目的のタスクを選択します。

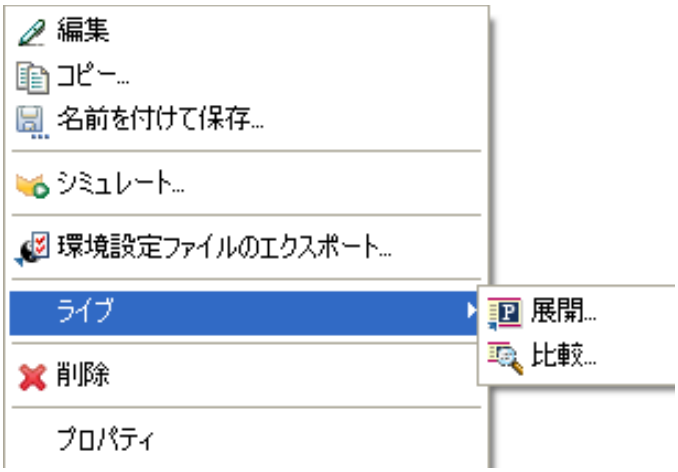


- **編集 :** リソースオブジェクトを編集できます。
- **コピー :** リソースオブジェクトをコピーします。
- **環境設定ファイルのエクスポート :** リソースオブジェクトを XML ファイルとして保存します。このオプションは、リソースオブジェクトのバックアップを作成する場合に使用します。
- **［ライブ］>［展開］:** 識別ボールトにリソースオブジェクトを展開します。
- **［ライブ］>［比較］:** リソースオブジェクトを、識別ボールトで対応するオブジェクトと比較します。
- **削除 :** リソースオブジェクトを削除します。
- **プロパティ :** リソースオブジェクトの名前を変更できます。

6.2 資格情報プロビジョニングポリシーの管理

1 アウトラインビューで、ポリシーを右クリックします。

2 目的のタスクを選択します。



- **編集：**ポリシーを編集できます。
- **コピー：**ポリシーをコピーします。
- **名前を付けて保存：**ポリシーのコピーを別の名前で保存します。
- **シミュレート：**ポリシーを識別ボールトに展開する前に、Designer でポリシーをテストすることができます。
- **環境設定ファイルのエクスポート：**ポリシーを XML ファイルとして保存します。このオプションは、ポリシーのバックアップを作成する場合に使用します。
- **［ライブ］>［展開］：**識別ボールトにポリシーを展開します。
- **［ライブ］>［比較］：**ポリシーを、識別ボールトで対応するオブジェクトと比較します。
- **削除：**ポリシーを削除します。
- **プロパティ：**ポリシーの名前を変更できます。