



NIS ベースの認証から Microsoft Active Directory™ への Linux/UNIX システムの移行

アプリケーション ノート

要約

この文書は、Likewise Enterprise によって Linux/UNIX コンピュータの認証方式を NIS ベースから Microsoft Active Directory ベースに容易に移行する方法について説明しています。Likewise Enterprise Migration Tool を使用してこの移行プロセスを自動化する方法、また移行プロセスによって影響を受ける可能性があるシステムの更新方法についても説明しています。

この文書の内容は予告なしに変更されることがあります。

目次

はじめに.....	1
NIS の基本.....	2
LIKEWISE ENTERPRISE のセル.....	4
LIKEWISE ENTERPRISE MIGRATION TOOL.....	5
NIS の移行の完了	10

,

はじめに

Likewise Enterprise を利用すると、Linux および UNIX コンピュータは Microsoft Active Directory™を通じてユーザーの認証と許可を行うことができるようになります。Microsoft Active Directory で行う認証には、次のような多くのメリットがあります。

- Microsoft Windows™システム、非 Windows システムのいずれを使用する場合でも、ユーザーは単一のユーザー名とパスワードでシステムを使うことができます。
- ユーザー アカウント管理の大幅な簡略化。システム管理者は、単一のアイデンティティ管理システムを使用してユーザーのプロビジョニング、パスワードの管理、ユーザーのプロビジョニング解除を実行することができます。
- セキュリティの向上。Likewise Enterprise は、Active Directory の多数のアカウント ポリシーを Linux および UNIX システムに拡張します。管理者は、Windows システムおよび非 Windows システム両方に適用するパスワードの最小長、複雑なパスワードの要件、パスワードの失効などのポリシーやその他の設定を構成することができます。
- 職務の分離をサポートするきめ細かい許可。Likewise Enterprise は、Active Directory のグループ ポリシー機能を Linux および UNIX システムに拡張し、標準化された SUDOer 設定ファイルのプロビジョニングをコントロールするためのポリシー設定を提供します。

ただし、Linux/UNIX コンピュータで Likewise Enterprise を活用するには、まずすべての既存の認証データを Active Directory に移行する必要があります。現在 *Network Information Service* (NIS) を使用して重要な認証データベース (Linux/UNIX の *passwd* および *group* ファイル) を共有している組織には、これらのデータベース内の情報を Likewise Enterprise 内に保持できるというメリットがあります。この NIS データを Likewise Enterprise に正しく移行できないと、孤立ファイル (所有者もグループも不明なファイル) が発生したり、最悪の場合にはセキュリティが低下したりすることがあります。

以降のセクションでは、*Likewise Enterprise Migration Tool* を使用して NIS から *Active Directory* にデータをインポートする方法について説明していきます。

NIS の基本

Linux/UNIX コンピュータは、NIS によって、複数の重要なシステム ファイルの共通情報ストアを共有することができます。これらのシステム ファイルのマスター バージョンは NIS サーバー上に保持され、さまざまな NIS クライアントがアクセスします。NIS は、パフォーマンスの向上と冗長化のためにスレーブサーバーの使用をサポートしています。

NIS では、共有システム ファイルはマップと呼ばれます。これは、NIS クライアントおよび NIS サーバーが使用する基盤プロトコルにより、これらのファイルをきめ細かく読み出せる（「ユーザー「root」のアカウント情報を読み込む」など）ためです。

NIS はさまざまなシステム ファイルの共有をサポートしていますが、認証を行う際に最も重要なシステム ファイルは、*passwd* ファイルと *group* ファイルです。これらのファイルには、有効なユーザー アカウントおよびグループ定義のリストが保持されています。NIS を使用するように構成されている Linux/UNIX コンピュータは、ユーザーの認証時とユーザーに関する情報の問い合わせ時にこれらの共有ファイルを使用します。ユーザーに関する情報を必要とするアプリケーションも、NIS を通じてユーザー情報を取得します。

NIS を使用する主なメリットは、複数のマシン上で単一のユーザー名とパスワードの使用が可能なことです。数百、あるいは数千にのぼる可能性があるすべての NIS クライアント上で *passwd* ファイルを管理するよりも、1 台の NIS サーバー上で 1 つの *passwd* ファイルを管理するほうがはるかに簡単です。

組織が共有ファイル サーバーを活用する場合は、一貫性のある ID が重要です。

ユーザー アカウント情報の管理に NIS を使用する 2 つ目のメリットは、すべての NIS クライアント間でユーザーが一貫性あるユーザー ID (UID) と一次グループ ID (GID) を持つことが保証される点です。ID の一貫性は、組織がネットワーク ファイル システム (NFS) などの共有ファイル サーバーを使用している場合に特に重要です。ID に一貫性がないと、NFS で適切なアクセス制御を継続していくことは困難になります。Linux/UNIX ファイルシステムは、すべてのファイルに所有者の UID とグループの GID を付与します。これらの属性は、Linux/UNIX のアクセス制御チェック方法の基盤です。

NIS は、UID と GID の一貫性の面でユーザーにメリットを提供しますが、安全な認証方式であるとは認められていません。NIS が使用する暗号化技術 (DES ハッシュなど) は、現在の基準では安全性が不十分と考えられています。また、NIS クライアントが共有パスワード ファイルを利用できるため、不正な NIS クライアントがブルートフォース攻撃を使ってこのファイルに保管されている暗号化されたパスワード ハッシュの解読を試みる可能性もあります。NIS を使用している企業は、概して法規制の遵守に必要な監査に合格していません。

NIS の後継である NIS+は、NIS のセキュリティ上の欠点の一部を補いましたが、あまり普及していません。NIS+の初期バージョンには問題が多く、使用できるプラットフォームも限られていました。また、NIS+サーバーの構成と管理は複雑で、このプロトコルを開発者した Sun Microsystems でさ

えも、NIS+よりも望ましいソリューションとしてLDAPベースのソリューションを推奨しています。

このようなセキュリティ上の懸念から、NISを使用する多くの組織は、（Likewise Enterpriseを通じて）認証のためにActive Directoryへの移行を進めています。移行の際には、既存のユーザー設定をActive Directoryに反映させるために、既存のNISマップをインポートできると便利です。また、ユーザーの既存のUIDおよびGID値を維持できることが非常に重要です。これらの値が維持されなければ、ADへの移行後、Linux/UNIXシステムはそれまでのようなファイルシステムアクセス制御を行うことができなくなってしまいます。移行後にユーザーIDが変更されると、たとえば移行前に「joe」というユーザーに所有されていたファイルの所有者が他のユーザーになってしまいます。

Likewise Enterprise Migration Toolを使用すれば、システムをADベースの認証に移行する際に、既存のNISマップを容易に維持することができます。ただし、IDを維持できるかどうかはLikewise Enterpriseセルの使用 방법에影響されます。このため、セルについて、またセルがID割り当てにどのように影響するかについて理解することが非常に重要です。

LIKEWISE ENTERPRISE のセル

Likewise Enterprise のセルにより、ユーザーがログインしているコンピュータに応じて、カスタマイズされた UID/GID マッピングを使用することができます。

NIS マップの移行を最も容易に行うには、組織単位を作成し、すべての NIS クライアントをこの組織単位に配置します。

Likewise Enterprise を使用すると、ユーザーがログオンしているコンピュータの種類に応じて、ユーザーを異なる UID および GID にマッピングすることができます。皆さんの組織の環境とは異なるかもしれませんが、例として複数の NIS サーバーを使用している組織のシナリオを考えてみましょう。この例では、便宜上エンジニアリング部門用のすべての Linux および Unix コンピュータ名を映画「スターウォーズ」の登場人物名とし、これらのコンピュータが *Jabba*（やはり「スターウォーズ」の登場人物）という名前の NIS サーバーに接続するとします。一方、製造部門内のすべての Linux および Unix コンピュータ名をテレビ番組「セサミストリート」のキャラクター名とし、「*BigBird*」（やはり「セサミストリート」のキャラクター）という名前の NIS サーバーに接続するとします。ユーザー「*joe*」は、コンピュータ「*Skywalker*」（「スターウォーズ」の登場人物）にログオンするときには UID 200 にマッピングされますが、「*Elmo*」（「セサミストリート」のキャラクター）にログオンするときには UID 314 にマッピングされます。Likewise Enterprise を導入後もこのようなマッピングを維持できれば非常に有益です。Likewise Enterprise は、セルを活用してこのマッピングの維持を実現します。

NIS ベースのシステムから Likewise Enterprise に移行する際、移行を最も容易に行う方法として、リプレースする NIS サーバーごとに Active Directory の組織単位 (OU) を作成します。この例では、「*Jabba*」NIS サーバー、「*BigBird*」NIS サーバーそれぞれに対応する OU を作成します。次に、Likewise Enterprise Management Tools を使用して[Active Directory ユーザーとコンピュータ] (ADUC) コンソールを起動し、作成した OU を選択します。OU の *Likewise Settings* プロパティ ページを開き、Linux/UNIX との使用を有効化します。OU の Linux/Unix との使用を有効化すると、Likewise Enterprise はこの OU に対してセルを作成します。セルは、カスタマイズされた UID/GID マッピングで、この OU 内のコンピュータに適用されます。セルが作成されたら、エンジニアリング部門のすべてのコンピュータを Active Directory に参加させ、作成した OU に移動することによって、「*Jabba*」NIS サーバーの移行を行います。製造部門のコンピュータに対しても同様の手順を実行し、「*BigBird*」NIS サーバーのために作成された OU にコンピュータを移動します。このような作業が終了したら、Likewise Management Tools を使用して、2 つのセルに異なる UID/GID マッピングを指定することができます。

既存の NIS サーバーがないケースでは、独立した複数のセルの作成を望む場合と望まない場合が考えられます。セルの管理に懸念があるときは、すべての Linux/UNIX コンピュータを単純にデフォルトセルの一部に追加することができます。デフォルトセルは、「フォレスト全体」に対応するセルです。つまりデフォルトセルは、他の OU と関連づけられたセルには含まれていない AD フォレスト内の任意の場所の Linux/UNIX コンピュータに適用されます。デフォルトセル内のすべての Linux/UNIX コンピュータは、同一の UID/GID マッピングを共有します。デフォルトセルでの ID の自動割り当て（他のセルでは行われません）を円滑に行うために、Likewise Enterprise は AD フォレスト内の異なるドメインに異なる ID 範囲を割り当てます。デフォ

Likewise Enterprise のデフォルトセルでは、利用可能な ID 値が制限されるため、デフォルトセルの使用は避ける必要があります。

ルトでは、フォレスト内の 1 つ目の Likewise Enterprise 設定ドメインには 100,000 ~ 199,999 までの範囲が、2 つ目のドメインには 200,000 ~ 299,999 の範囲が割り当てられます。それ以降のドメインにも範囲が割り当てられません。

ID がこのように割り当てられるため、**デフォルトセルでは UID および GID を自由に設定することができません**。この割り当ては、Migration Tool にも影響を及ぼします。NIS サーバーからデフォルトセルに ID マッピングをインポートすると、既存の ID を維持することができなくなります。したがって、NIS サーバーから情報をインポートする場合には、デフォルトセル以外のセルに情報をインポートするのが最善の策です。こうすることで、これまでのマッピングを維持することが可能になり、所有者およびグループ情報の補正のためにファイルシステムを修正する必要がなくなります。

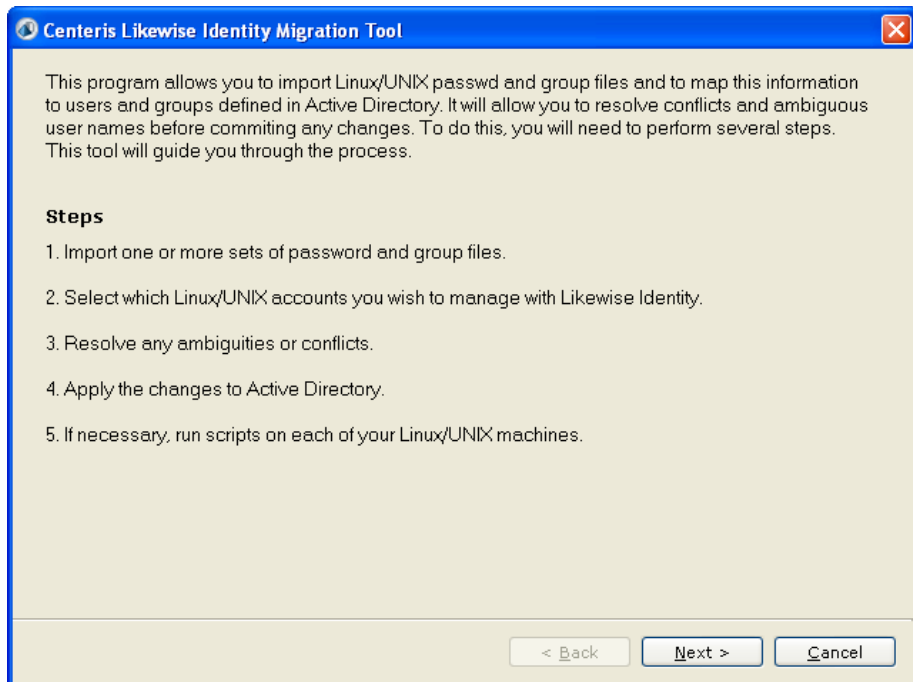
Likewise Enterprise Migration Tool は、Linux/UNIX のアカウント情報を特定のセル/OU にインポートすることに注目してください。このツールは、ドメインとその子組織単位のツリーを表示し、ユーザーに Linux/UNIX アカウント情報のインポート先のノードの選択を求めます。そのノードにセルが存在しない場合は、Migration Tool がユーザーに代わってセルを 1 つ作成します。ドメインのトップノードを選択すると、このフォレストのデフォルトセルを指定することになります。

すでに説明したように、Migration Tool を使用して Linux/UNIX アカウント情報をインポートする場合、デフォルトセルの使用を回避するのが得策です。デフォルトセルを使用すると、既存のユーザーに新しい UID および GID が割り当てられるため、ファイルの所有権とグループ設定を適切に更新するために、Linux/UNIX マシン上で修正スクリプトを実行する必要性が生じます。

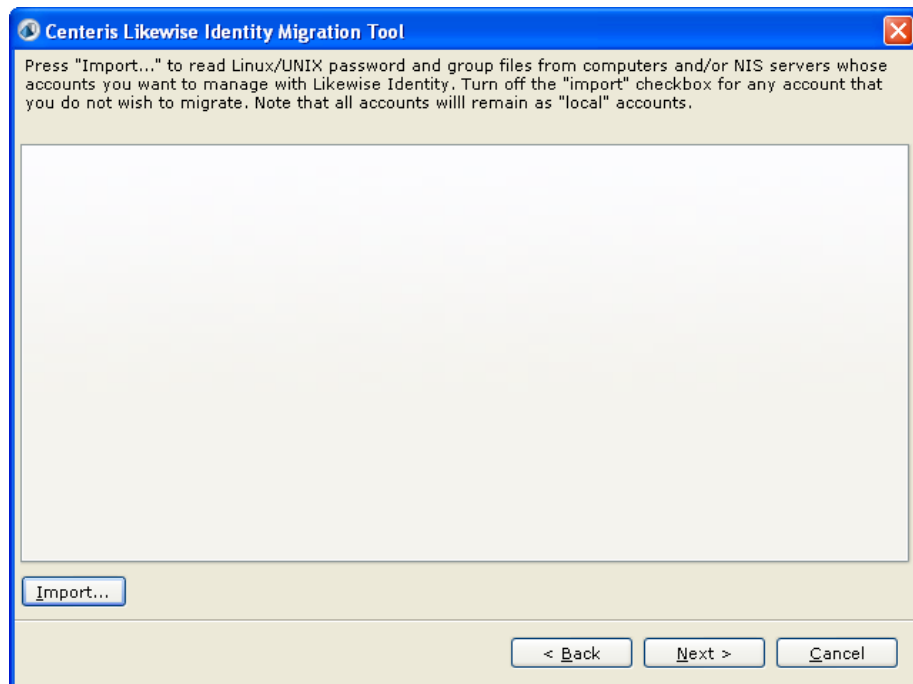
Likewise Enterprise Migration Tool (IMT) は、NIS の passwd ファイルおよび group ファイルを読み込み、そのデータを Active Directory にインポートすることができます。また、このツールを使用するとインポートするユーザーとグループを選択できるほか、インポートしたユーザーとグループを Active Directory の既存のエントリにマッピングすることができます。IMT は、Likewise Enterprise のセルとグループの容易な自動作成をサポートし、以前の UID/GID 設定を維持するために AD オブジェクトを構成します。IMT では、AD を直接修正することも、適切な移行のために個別に実行可能なスクリプトを作成することもできます。

NIS の passwd ファイルおよび group ファイルをインポートするには、まず *scp*、*ftp*、*smbclient*、またはその他のメカニズムを使用して、Likewise Enterprise Management Tools および Likewise Enterprise Migration Tool をインストール済みの Windows コンピュータにこれらのファイルを NIS サーバーからコピーする必要があります。次に Migration Tool (*lwimigrate.exe*) を実行します。最初に簡単な説明のページが表示されます。

LIKewise ENTERPRISE MIGRATION TOOL



[Next]をクリックし、質問に回答していくと、次のようなウィザードページが表示されます。



[Import]ボタンをクリックし、次のフォームを使用して *passwd* ファイルと *group* ファイルの場所を指定します。

Specify a Linux/UNIX-style passwd file and its corresponding group file. These files will be imported to a "map" that will then be matched to existing Active Directory user and group names. This migration tool will also generate a Linux/UNIX script to properly reset the ownership of any files that might be affected by the migration. Specify a name for the map that corresponds to the computer where the map originated.

Map name:

Passwd file:

Group file:

Limit standard Linux/UNIX user accounts

[Map Name]は特に重要ではありませんが、後で生成されるファイル名の一部にこの名前が使用される場合があります。標準の Linux/UNIX アカウント（root、mail、ftp など）を省略するように Migration Tool に指示するボックスがチェックされている（デフォルトでオンに設定されている）ことに注目してください。 *passwd* ファイルと *group* ファイルの場所を指定し（[Browse]ボタンを使用して場所を探すことができます）、[Import]をクリックしてこれらのファイルを Migration Tool にロードします。

Press "Import..." to read Linux/UNIX password and group files from computers and/or NIS servers whose accounts you want to manage with Likewise Identity. Turn off the "import" checkbox for any account that you do not wish to migrate. Note that all accounts will remain as "local" accounts.

Jabba

Users

Import	UID	Login Name	GID	Full Name	Home Directory	Shell
<input checked="" type="checkbox"/>	1011	mporwit	100		/home/mporwit	/bin/zsh
<input checked="" type="checkbox"/>	1012	jslider	100		/home/srv3/jsli...	/bin/bash
<input checked="" type="checkbox"/>	780	jerry	100		/home/srv3/jerry	/bin/bash

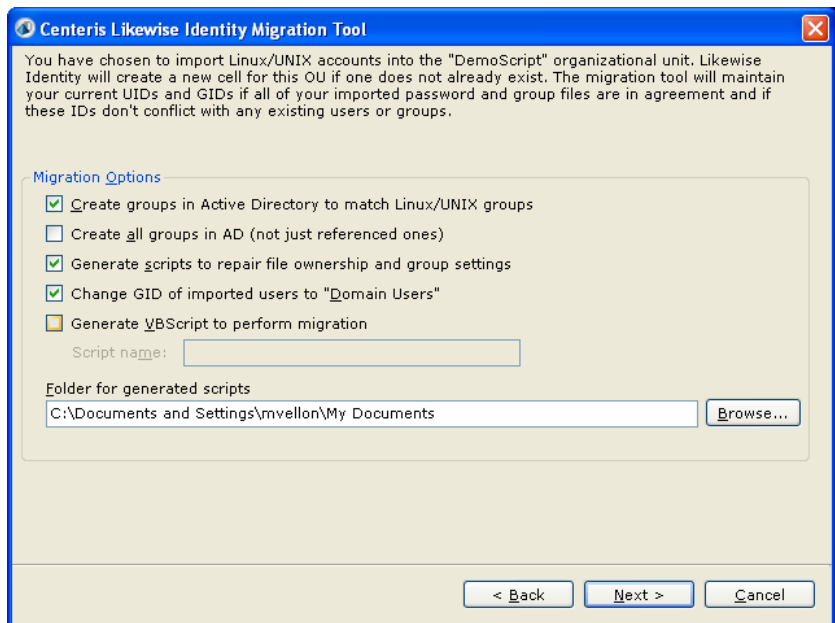
Groups

GID	Name	Users
0	root	root,caroot
1	bin	root,bin,daemon
2	daemon	root,bin,daemon
3	sys	root,bin,adm

このページには、インポートしたマップファイルの情報が表示されます。
[Import]列のチェックボックスのチェックを外すと、インポート プロセスから特定のユーザーを除外することができます。

[Next]をクリックし、NIS データのインポート先となる組織単位を選択します。すでに説明したように、ドメイン ノードを選択すると、Migration Tool はデータをデフォルト セルにインポートするため、既存の ID マッピングを維持できなくなります。それより低レベルの OU を選択すると、Migration Tool は必要に応じてユーザーに代わってセルを作成します。

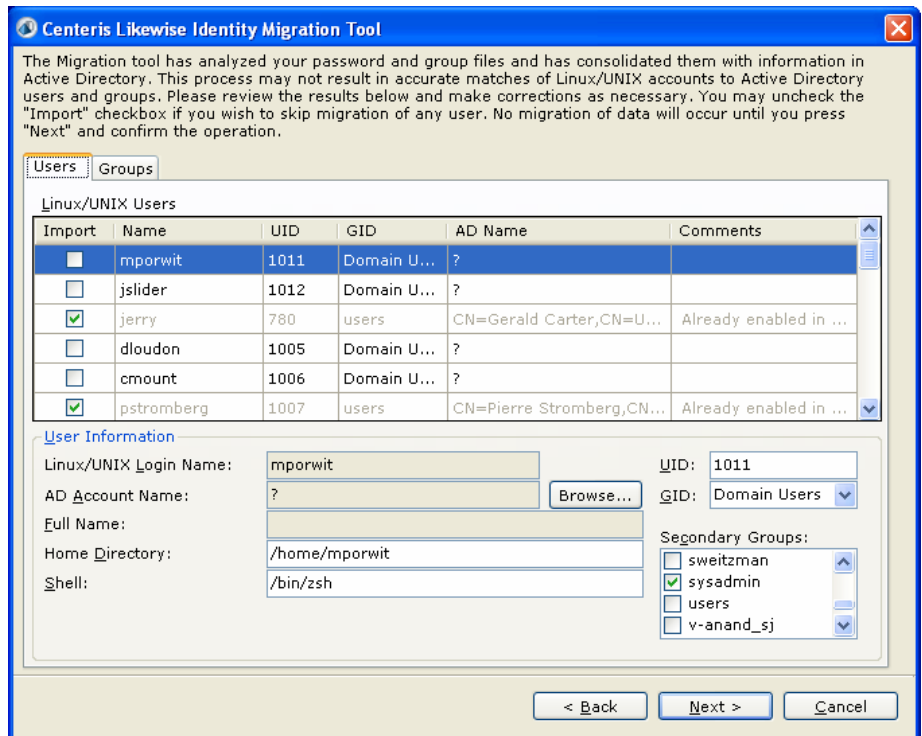
移行ノードを選択すると、移行オプションのリストが表示されます。



NIS マップの移行が成功した場合は、ファイルシステムの所有権とグループ設定を修正する必要はありません。

このページでは、複数のオプションを設定することができます。ファイルの所有権とグループ設定を修復するスクリプトの生成 (Generate scripts to repair file ownership and group settings) を可能にするオプションに注目してください。**NIS の移行が成功した場合、生成されたスクリプトの修正を行う必要はありません。**このオプションを有効化し、生成されたスクリプトを検証してファイルの所有権やグループ設定が誤って変更されていないことを確認してください。その他の移行オプションの詳細情報については、Likewise Enterprise Migration Tool のドキュメンテーションを参照してください。

必要な移行オプションを指定し、[Next]をクリックします。



この画面には、インポート済みのマップとユーザー指定の移行ポイント（組織単位）を Migration Tool が比較して調整した内容が表示されます。[Users] タブには、インポートされたユーザーが既存の AD ユーザーにどのようにマッピングされているかが表示されます。[Group] タブには、インポートされたグループの同様のデータが表示されます。いずれのタブでも、表の行を選択すると、その行に関する詳細情報が画面下部に表示されます。各表の各アイテムを検証し、Migration Tool によって適切にデータがインポートされていることを確認してください。特に[AD Name]列に注意します。Migration Tool は、インポートされた名前と AD の既存名の照合を試みます。インポートされた名前と完全に一致する名前が見つからない場合は、[AD Name]列に疑問符（？）が表示されます。画面下部の[Browse]ボタンを使用すると、AD ピッカーを起動し、アイテムを手動で照合することができます。

UID および GID 設定と 2 次グループ設定にも注目してください。必要な修正を加え、移行プロセスを完了する準備が整ったら[Next]をクリックします。生成されたすべてのスクリプトを見直し、移行が適切に実行されたことを確認します。

NIS の移行の完了

Migration Tool の使用が終了したら、いくつかの作業を行う必要があります。まず、NIS の使用を停止し、Likewise Enterprise の使用を開始する必要があります。これは次の手順で操作します。

- NIS サーバーに接続されているすべての NIS クライアント マシンに Likewise Enterprise エージェントをインストールします。
- Likewise Enterprise Domain Join Tool を使用して、これらすべてのマシンを Active Directory に参加させます。
- [Active Directory ユーザーとコンピュータ] (ADUC) ツールを使用して、Domain Join Tool によって (AD のコンピュータ ノードに) 作成されたコンピュータ アカウントを、NIS マップのインポート時に作成したセル/OU に移動します。
- Linux/UNIX マシンを再起動します (または、少なくとも `/etc/init.d/centeris.com-lwiauthd restart` を使用して各マシン上の Likewise Enterprise エージェントを再起動します)。
- 各 Linux/UNIX マシンで `edit /etc/nsswitch.conf` を実行し、NIS への (少なくとも `passwd` および `group` 行への) 参照を削除します。

なんらかの理由で既存の NIS の UID および GID を維持できなかった場合は、Migration Tool によって、既存の Linux/UNIX ファイルシステムを修正して新しい ID マッピングを反映させるための修正スクリプトを生成します。修正が必要なすべての Linux/UNIX マシンでこれらのスクリプトを実行してください。

修正スクリプトを実行しない場合は、スクリプトの次のような重要な行に注目してください。

```
#
# File user ownership changes
find . -user 1019 -exec chown 100005 {} \;
...
#
# File group changes
find . -group 502 -exec chgrp 100020 ( ) \;
...
```

所有者やグループの特定には、Linux/UNIX の `find` コマンドが使用され、これらの値の修正には `chown` および `chgrp` コマンドが使用されます (新しい AD ベースのマッピングに従ってこれらの値を設定します)。修正スクリプトには、新旧の値のリストも (コメントとして) 含まれます。これらのスクリプトを実行しない場合には、このスクリプトに含まれている情報を使用して手作業で修正を行うことができます。