

## Technical Overview

---

### 本文書の内容

- ユーザーの認証
- ユーザーおよびグループの認可
- ユーザーおよびグループの管理
- グループ・ポリシーの適用
- ソフトウェアのコンポーネントおよびアーキテクチャ

### 要約

本概要文書では、Likewise が、Active Directory への非 Windows コンピュータ統合、ユーザー認証、リソースへアクセスするためのユーザーおよびグループの認可、Active Directory への UNIX/Linux ユーザー情報格納、グループ・ポリシーを用いた Linux/UNIX コンピュータ管理をどのように行うかについて解説する。また、Likewise の 2 つのオペレーティング・モード、セルの利用、ソフトウェアのコンポーネントおよびプロセスについても概説する。

The information contained in this document represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKewise SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software  
15395 SE 30th Place, Suite #140  
Bellevue, WA 98007  
USA

## 目次

ドメインの追加 .....	5
ユーザーの認証.....	7
Likewise を用いた認証 .....	7
ユーザーとグループの認可 .....	9
スキーマ・モードと非スキーマ・モード.....	9
主な違い .....	12
ユーザーとグループの管理 .....	14
セルの作成.....	14
デフォルト・セル.....	15
セルのリンク .....	15
Cell Manager.....	16
NIS ドメインの移行 .....	16
複数セルの利用.....	17
移行ツール.....	18
孤立オブジェクト・ツール .....	18
グループ・ポリシーの適用 .....	19
ユーザー・ポリシー .....	21
ソフトウェア・コンポーネントの概要.....	23
Likewise Agent.....	23
Likewise Console .....	24
Integrated Management Tool.....	26
標準とプロトコル .....	28
まとめ .....	29

## はじめに

混在型のネットワークを構築していたとしよう。Web サーバとネットワーク・アプリケーションは Linux コンピュータ上で動作している。データベース・サーバは UNIX、電子メール・サーバは Windows である。デスクトップ・ユーザーの大半は Windows 環境にあるが、美術部門では Mac OS X が採用されている。

この混在型ネットワークは、さまざまなオペレーティング・システムによって異なる ID 管理システムで企業に負担をかけている。Windows ユーザーは Active Directory で、UNIX ユーザーは NIS で認証を行う。Linux ユーザーは /etc/passwd ファイルを使ってローカル認証を行うだけである。一方、Mac OS X ユーザーは各自任意の Kerberos キー配布センター経由で認証を行う。この Kerberos キー配布センターの維持やトラブルシューティングを行うには専門知識が必要である。ユーザーが入退社するたびに毎回、これらの各 ID 管理システムを別々にアップデートする必要がある。時間がかかるこうしたプロセスでは、セキュリティ・ホールが放置されがちになる。

しかし、かかる負荷はユーザー認証、ID のアップデート、リソースにおけるセキュリティの確保だけにとどまらない。つまり、システムの管理、構成、維持、監査も行わなければならないのである。かなり困難な仕事である。混在型ネットワークには多くの業務が積みまとう。

さらに、自社の Windows コンピュータを Active Directory のグループ・ポリシーを適用して集中管理していても、Linux、UNIX、Mac OS X コンピュータは別物で、各コンピュータ上の.conf ファイルでコントロールされる独立したコンポーネントで管理される。Linux/UNIX コンピュータのグローバルな構成変更は困難で効率が悪く、エラーが発生しやすい。

Likewise は、全ユーザーID の集中管理、全システム共通のユーザー認証、グループ・ポリシーを用いた Linux/UNIX コンピュータの集中アドミニストレーションを実現できるよう、Linux、UNIX、Mac OS X コンピュータを Active Directory にシームレスに統合することによって、混在型ネットワークの管理にまつわる負荷を軽減する。

本概要文書では、Likewise が、Active Directory への非 Windows コンピュータ統合、ユーザー認証、リソースへアクセスするためのユーザーおよびグループの認可、Active Directory への UNIX/Linux ユーザー情報格納、グループ・ポリシーを用いた Linux/UNIX コンピュータ管理をどのように行うかについて解説する。また、Likewise の 2 つのオペレーティング・モード、セルの利用、ソフトウェアのコンポーネントおよびプロセスについても概説する。

## ドメインの追加

Likewise は、Linux/UNIX コンピュータを Active Directory ドメインへ迅速かつ簡単に組み込む機能を提供することにより、相互運用性を確保するための基盤を提供する。下表は Likewise の主要コンポーネントをまとめたものである。これらのコンポーネントは連携しており、基本レベルの相互運用性を確立する。

Likewise コンポーネント	ロケーション	機能
エージェント	ドメイン用の各 Linux、UNIX、Mac OS X コンピュータにインストールされている。	Linux、UNIX、Mac OS X コンピュータをドメインに追加するために Active Directory とやりとりする。
Domain Join Tool	Linux、UNIX、Mac OS X コンピュータ上のエージェントを用いてインストールされている。	コンピュータをドメインに追加するためのグラフィカル・ユーザー・インタフェースとコマンドライン・インタフェースを提供する。
コンソール	Active Directory Domain Controller に接続されている Windows 管理ワークステーション上にインストールされている。	コンソール・インストール・プロセスでは最初に、UNIX、Linux、Mac OS X コンピュータを統合するために Active Directory の設定を行い、また、Active Directory Users and Computers MMC スナップイン内で UNIX/Linux コンピュータを管理するツールを組み込む。

Linux、UNIX、Mac OS X コンピュータ上にエージェントがインストールされ、Active Directory Domain Controller に接続されている管理ワークステーション上にコンソールがインストールされていれば、Domain Join Tool を使って UNIX/Linux コンピュータをドメインに追加できる。

ドメインを追加するために、エージェントは CIFS RPC、LDAP、Kerberos プロトコルを用いて Active Directory とやりとりする。Domain Join Tool によってコンピュータがドメインに追加されると Active Directory にマシン・アカウントが作成される。そしてこのマシン・アカウントは、Active Directory に対する認証済み LDAP/RPC コールの生成に用いることができる。



追加された時点で、エージェントはドメイン、マシン・アカウント名、パスワードに関する情報を保存する。Active Directory に組み込まれたユーザーは、個々の Active Directory 証明書を用いて UNIX/Linux コンピュータにログオン可能になり、認証される。

## ユーザーの認証

認証は、コンピュータやアプリケーションへのアクセスを望むユーザーの身元を確認するシステムによって行われるプロセスである。Likewise を使わない場合、UNIX/Linux コンピュータ上では通常、`/etc/passwd` ファイルと `/etc/group` ファイルに照らしたユーザー名 / パスワード認証を行うための Pluggable Authentication Modules (PAM) と、ユーザー名をユーザー ID (UID) およびグループ ID (GID) に関連付ける `nsswitch` を用いて認証が行われる。各コンピュータ上の `/etc/passwd` ファイルには、認可済みのユーザー名一覧が保存され、`nsswitch` には、UID や GID などのユーザー関連情報が格納される。

`/etc/passwd` ファイルを用いてユーザー認証を行うということは、各 UNIX/Linux コンピュータが実際にはそれぞれの ID 管理システムとして稼働していることを意味する。つまり、複数のコンピュータへアクセスするユーザーは各コンピュータに各自のパスワードを設定する必要があり、また、パスワードを変更しなければならない場合、すべてのコンピュータ上のパスワードを変更する必要がある。こうしたプロセスは時間がかかる上にエラーが発生しやすい。`/etc/passwd` ファイルを管理しないようにするために、一部の企業は管理者に root アカウントを単純に利用させているが、これは一般的なセキュリティ標準 / 規則に反する危険な方法である。

また、クライアント-サーバ間のディレクトリ・サービス・プロトコルである Network Information Service (NIS) を利用して、複数の UNIX マシンが単一の `/etc/passwd` ファイルを共有できるようにしている企業も存在する。NIS の場合、全ユーザーは NIS ドメインにつながるすべてのマシンに共通する UID と GID マッピングを設定している。しかし、NIS は、規模の調整が難しく、複数のオペレーティング・システムに対応した実装が煩雑で、LDAP や Kerberos よりもかなり安全性が低い。

こうした企業内では、同期化された `/etc/passwd` ファイルの展開や、LDAP の実装が行われている可能性がある。合併を経た企業であれば、複数の方式や実装を利用しているかもしれない。

### Likewise を用いた認証

Active Directory へ非 Windows コンピュータを統合する Likewise の機能は、UNIX、Linux、Mac OS X コンピュータが Active Directory の認証プロセスを利用できるようにするというメリットをすぐにもたらす。Active Directory は Kerberos キー配布センターとして機能するため、Likewise は Kerberos 5 ネットワーク認証プロトコルを用いて UNIX と Linux のユーザー名とパスワードを認証できる。Kerberos は、セキュリティ・レベルの低いネットワーク上でやりとりを

行うユーザーやコンピュータに安全な方式で ID を相互検証させる。Likewise の場合、以下ようになる。

1. ユーザーは Linux/UNIX クライアントにログオンし、ログイン・プログラムがユーザー名とパスワードを受け取る。
2. ユーザー名とパスワードが PAM に送信される。
3. pam\_lwidentity.so ライブラリが lwiauth デーモンとやりとりする。
4. ユーザー名とパスワードから、lwiauth デーモンが秘密鍵を生成する。
5. lwiauth はこの秘密鍵を使って、Active Directory の Kerberos キー配布センター (KDC) が発行するチケット認可チケット (TGT) を要求する。
6. KDC が秘密鍵を検証し、クライアントに TGT を発行する。
7. クライアントと KDC はメッセージ交換を行ってクライアントを認証する。
8. lwiauth デーモンは TGT を用いて、SSH といったほかのサービス向けのサービス・チケットを要求できるようになる。

## ユーザーとグループの認可

課題: AD ユーザーが UNIX/Linux ホスト上のリソースにアクセスできるようにする。この課題はなぜ難しいのか。なぜなら、UNIX/Linux の場合、UID と GID によって定義されるユーザー / グループ用の許可設定は単純な整数型で、一般的に 32 ビットの整数である一方、Active Directory の場合、セキュリティ識別子 (SID) はドメイン特有のユニバーサルに固有の ID を含んでいるからである。Active Directory において、1 つの SID はフォレスト内で 1 つのユーザー、グループ、コンピュータを一意的に識別する。相互運用性を確保するにはこのように、SID を UID と GID にマッピングするためのメソッドが必要である。

Likewise は、SID と UID / プライマリ GID のマッピングおよび Active Directory における情報格納を実現することによってこの不整合を解決している。

以下の情報も格納される。

- セカンダリ・グループ・メンバーシップ用の GID
- ユーザーのホーム・ディレクトリ・パス
- ユーザーのシステム・シェル
- ユーザーのフルネーム
- ユーザーごとの記述的文字列

この情報を Active Directory に格納する方法は、ユーザーが Active Directory に対応するために Likewise を設定する際に選択するモードによって異なる。

### スキーマ・モードと非スキーマ・モード

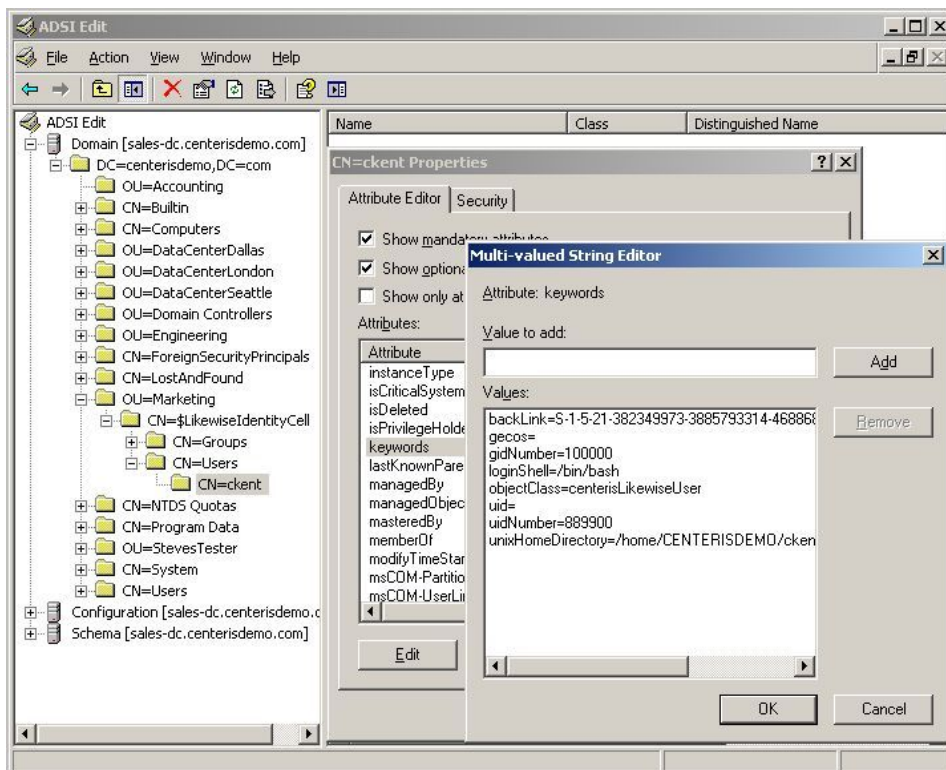
Likewise は、スキーマ・モードと非スキーマ・モードという 2 つのオペレーティング・モードを実装している。非スキーマ・モードでは、RFC 2307 オブジェクト・クラス / 属性の要求や既存のスキーマの変更を行うことなく Linux/UNIX データを保存できる。その代わりに、既存のオブジェクト・クラス / 属性を用いてデータを格納する。セル関連情報を格納するために、Likewise は container オブジェクトを作成し、その description 属性にデータを格納する。グループやユーザーに関する情報については、serviceConnectionPoint オブジェクトを作成してその keywords 属性にデータを格納する。keywords と description は両方とも多値属性であり、複数の値を保持できる一方で固有値の AD サーチも可能である。

具体的には、非スキーマ・モードにおいて Likewise は RFC 2307 の属性名を用いて値を name=value の形で keywords 属性と description 属性に格納する。ここで、name は属性名で、value はその値である。keywords 属性名と値のペアが AD ユーザー用の UNIX/Linux 情報をどのように含むことが可能なのかについて一例を示す。

```
uid=  
uidNumber=1016  
gidNumber=100000  
loginShell=/bin/bash  
unixHomeDirectory=/home/joe  
gecos=  
backlink=[securityIdentifierOfUser]  
objectClass=CenterisLikewiseUser
```

本例において uid 属性は空白である。uid 属性は、AD ユーザーが各自の AD アカウント名以外の何らかを使ってコンピュータにログオンできるようにするためにネーム・エイリアスを指定したい場合にのみ必要である。

ADSI Edit において、ユーザー用のプロパティは以下ようになる。

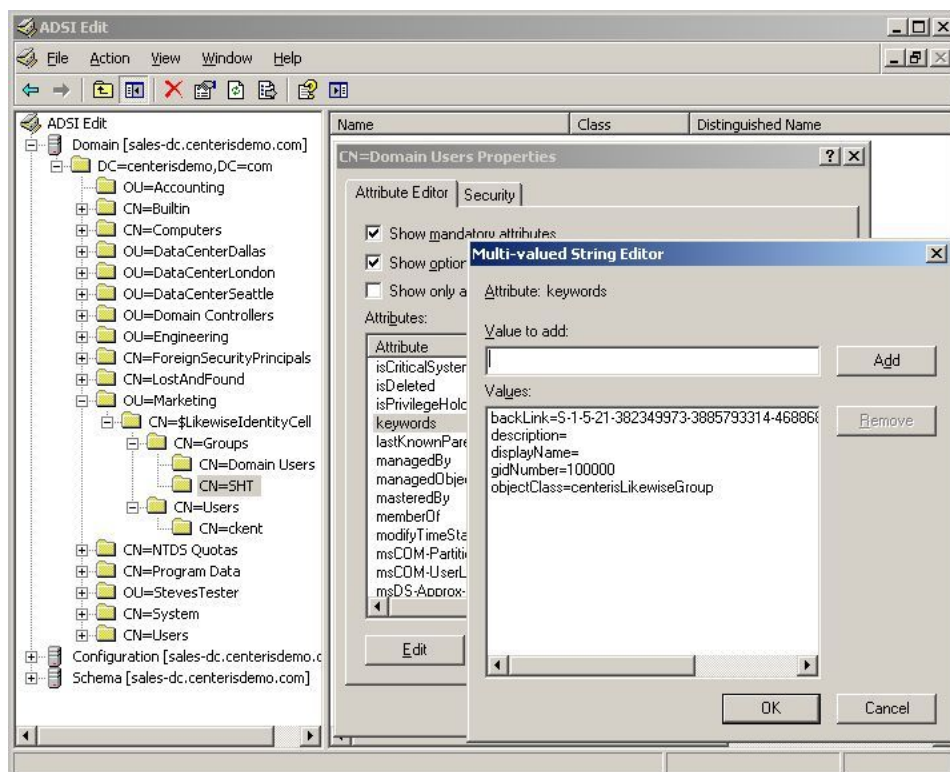


keywords 属性も UNIX/Linux グループ情報の格納に使われる。属性名と値のペアがグループ用の UNIX/Linux 情報をどのように含むことが可能なのかについて一例を示す。

```
backLink=[securityIdentifierOfGroup]
description=
displayName=
gidNumber=100000
objectClass=centerisLikewiseGroup
```

グループ用のエイリアスを設定すると、それは `displayName` 属性に格納される (前出の例におけるグループの場合、エイリアスは設定されていないため、`displayName` は空白である)。

ADSI Edit において、`keywords` 属性の値は以下ようになる。



スキーマ・モードのアプローチは若干異なる。このモードの場合、UNIX/Linux のユーザー / グループ情報を格納するために UNIX および Linux 固有の RFC 2307 オブジェクト・クラス / 属性、すなわち `posixAccount` と `posixGroup` のオブジェクト・クラスを利用する。たとえば、`posixAccount` と `posixGroup` のオブジェクト・クラスには `uidNumber` と `gidNumber` という属性が含まれている。Likewise はこれを利用して UID と GID のマッピングを行う。さらに Likewise は、`keywords` 属性を用いることによって非スキーマ・モードと同一の情報を格納するために `serviceConnectionPoint` オブジェクトを利用する。

スキーマ・モードの採用を決定したもののスキーマが RFC 2307 に適合していない場合、スキーマを変更する必要がある。コンソール内にあるツールである Likewise Domain Extension Wizard を使うと、RFC 2307 に適合するようスキーマを自動的にアップグレードできる。(Windows Server 2003 R2 は RFC 2307 適合)。RFC 2307 に適合したスキーマでスキーマ・モードを実行する場合、Likewise はスキーマの変更を行わないが、グローバル・カタログ内の RFC 2307 属性の反映およびサーチ高速化に向けた調整を行うために Domain Extension Wizard をやはり実行させる必要がある。

#### 主な違い

スキーマ・モードと非スキーマ・モードの違いを下表にまとめた。

モード	適用ケース	格納メソッド
非スキーマ・モード	最新の AD スキーマへ移行していない AD 実装である。管理者がスキーマの変更に消極的である。	Likewise は container の description 属性と keywords 属性、serviceConnectionPoint オブジェクトを用いて、ユーザー、グループ、セル向けの UNIX/Linux 情報を格納する。
スキーマ・モード	Windows Server 2003 R2 など、RFC 2307 に適合した AD 実装である。管理者が、RFC 2307 に適合するスキーマへの変更に積極的であり、フォレストの機能レベルを Windows Server 2003 へ引き上げたいと考えている。 注: Windows Server 2003 へのフォレストの機能レベル引き上げについて、Windows 2000 のドメインのドメイン・コントローラは除外される。	Likewise は、RFC 2307 スキーマに組み込まれた UNIX/Linux 固有の属性、container オブジェクト、keywords 属性を利用する。

スキーマ・モードと非スキーマ・モードはどちらも、Likewise が SID と UID/GID 相互のマッピングを行えるよう、Active Directory に (UID や GID などの) UNIX/Linux 情報を格納するメソッドを提供する。このマッピングによって、Likewise は Active Directory のユーザー・アカウントを用いて、UID-GID スキームで管理される UNIX/Linux リソースへのユーザー・アクセスを許可すること

ができる。AD ユーザーが UNIX/Linux コンピュータへログオンすると、Likewise Agent は標準の LDAP プロトコルを用いて Active Directory Domain Controller とやりとりし、以下の認可データを受け取る。

- UID
- プライマリ GID
- セカンダリ GID
- ホーム・ディレクトリ
- ログイン・シェル

Likewise はこの情報を用いて、UNIX/Linux リソースに対するユーザー・アクセスをコントロールする。

## ユーザーとグループの管理

Active Directory は、オブジェクトを一貫性と整合性の高い方法で管理できるよう、組織単位を利用して共通のコンテナに関連オブジェクトを分類する。Active Directory ユーザーを Linux/UNIX ユーザー ID (UID) とグループ ID (GID) にマッピングするためには、Likewise セルを組織単位に関連付ける。セルを組織単位 (OU) に関連付けると、そのセルは UID と GID に対する Active Directory ユーザーのカスタム・マッピングになる。

セルを使って、異なるコンピュータ用のさまざまな UID と GID にユーザーをマッピングできる。OU (またはそれにネスト化された OU) 内の Linux/UNIX コンピュータは、このセルを使って AD ユーザーを UID と GID にマッピングする。次の画面は、Clark Kent という名のユーザーが、選択された Likewise セル内の Linux/UNIX コンピュータへのアクセスを許可されている例を示す。

Clark Kent Properties

Published Certificates | Member Of | Dial-in | Object  
Security | Environment | Sessions | Remote control  
General | Address | Account | Profile | Telephones | Organization  
Terminal Services Profile | COM+ | Likewise Settings

UNIX/Linux User Information

To allow this user to logon to UNIX/Linux computers joined to Active Directory, you must specify which Centeris Likewise cell(s) the user is allowed to access. If you have not created any cells, specify the Default cell.

Centeris Cells  Use Distinguished Names

- (Default) - Default cell
- Accounting - OU=Accounting,DC=centerisdemo,DC=com
- Engineering - OU=Engineering,DC=centerisdemo,DC=com
- Marketing - OU=Marketing,DC=centerisdemo,DC=com
- StevesTester - OU=StevesTester,DC=centerisdemo,DC=com

User info for cell: (Default)

Specify UID 100000  
GID 100000 Domain Users  
Login Name  
Home Directory /home/CENTERISDEMO/ckent  
Login Shell /bin/bash  
Comment (GECOS)

OK Cancel Apply

### セルの作成

Likewise は、OU 用に関連付けられたセルを作成してそれを UID-GID 番号の管理に使えるようにするために、Active Directory Users and Computers MMC スナップインを変更する。セルを作成する場合、Active Directory Users and Computers を用いて希望する OU を選択し、Likewise Settings プロパティシートを表示させ、チェックボックスを選択してセルを OU に関連付ける。その結果、UID-GID 番号のアサインは手動で、あるいは Likewise で自動的に行えるようになる。

UNIX/Linux コンピュータは Active Directory に接続されると、OU がどのメンバーに属するかを確認し、また Likewise セルが関連付けられているかどうかをチェックする。セルが OU に関連付けられていなければ、UNIX コンピュータ上の Likewise Agent は、Likewise に関連付けられたセルを持つ OU を検出するまでペアレント/グランドペアレントの OU を検索する。関連付けられたセルを持つ OU が検出されなかった場合、Likewise Agent はデフォルト・セルを使ってそのユーザー名を UID/GID 情報にマッピングする。

セルを組織単位に関連付ける前に、選択したいスキーマ・モードを見極めておく必要がある。デフォルト・セルを使った場合も含め、セル作成後はスキーマ・モードを変更できない。

#### デフォルト・セル

Likewise の場合、ユーザーはデフォルト・セルを指定できる。デフォルト・セルは、関連付けられたセルを持つ OU や関連付けられたセルにリンクされたセル内に存在しないコンピュータのマッピングを行う。デフォルト・セルには、全 Linux/UNIX コンピュータのマッピング情報を格納できる。

Linux/UNIX コンピュータは、任意の OU のメンバーになることができる。その OU に関連付けられたセルを持たなくても、である。このような場合、その OU に関連付けられたグループ・ポリシーが Linux/UNIX コンピュータに適用されるが、ユーザーの UID-GID マッピングは直近のペアレント・セルかデフォルト・セルのポリシーに従う。

#### セルのリンク

継承メカニズムを提供し、システム管理負荷を軽減させるために、Likewise はセルをリンクさせることができる。リンクさせると、同一セル内のユーザーとグループはリンク先のセル内のリソースにアクセスできる。たとえば、デフォルト・セルに 100 システム管理者が含まれ、これらの管理者を別のセル「Engineering」にアクセスさせたい場合、Engineering セル内でこれらのユーザーにプロビジョニングを行う必要はない。ただ単に Engineering セルをデフォルト・セルにリンクさせるだけで、Engineering セルはデフォルト・セルの設定を継

承する。そして、管理をさらに楽にするために、Engineering セルでデフォルト・セルから逸脱したマッピング情報を指定することができる。

リンクによって実質的にセルの階層を設定できるが、リンクは再帰性が低い。たとえば、「Civil」というセルが「Engineering」セルにリンクされ、その「Engineering」セルがデフォルト・セルにリンクされている場合、デフォルト・セルの設定は「Civil」セルに継承されない。

複数のセルにリンクする際、設定する命令が重要である。なぜなら、それが検索命令をコントロールするからである。システム管理者である Steve がデフォルト・セルに 100 万セット、Engineering セルに 15 万セットの UID を保有していたとする。しかし、Civil セルにおいては、Engineering セルの UID を用いて Civil コンピュータにログオンしなければならない。Civil セルがデフォルト・セルと Engineering セルの両方にリンクされている場合、その命令が重要になる。Engineering が検索命令においてデフォルト・セルに優先されていないならば、Steve には誤った UID がアサインされ、彼は Civil セルのコンピュータにログオンできなくなる。

### Cell Manager

Likewise Cell Manager は MMC スナップインであり、Active Directory Organizational Units に関連付けたセルの管理に利用できる。Cell Manager を使うと、自分に関係するすべてのセルを一覧できる。Cell Manager は、セルの管理権限 (ユーザーやグループをセルに追加する機能) を移譲する、つまり、(ユーザーかグループのいずれかの) 他者に与えることによって Active Directory Users and Computers を補完する。Cell Manager は Likewise Console と同時に自動的にインストールされる。

### NIS ドメインの移行

Likewise を用いてすべての UNIX/Linux ユーザーを Active Directory に移行させる場合、たいいていは、Active Directory に組み込まれたすべての UNIX/Linux コンピュータに一貫した UID と GID をユーザーにアサインする。これは、管理上の諸経費を削減するシンプルな方法である。

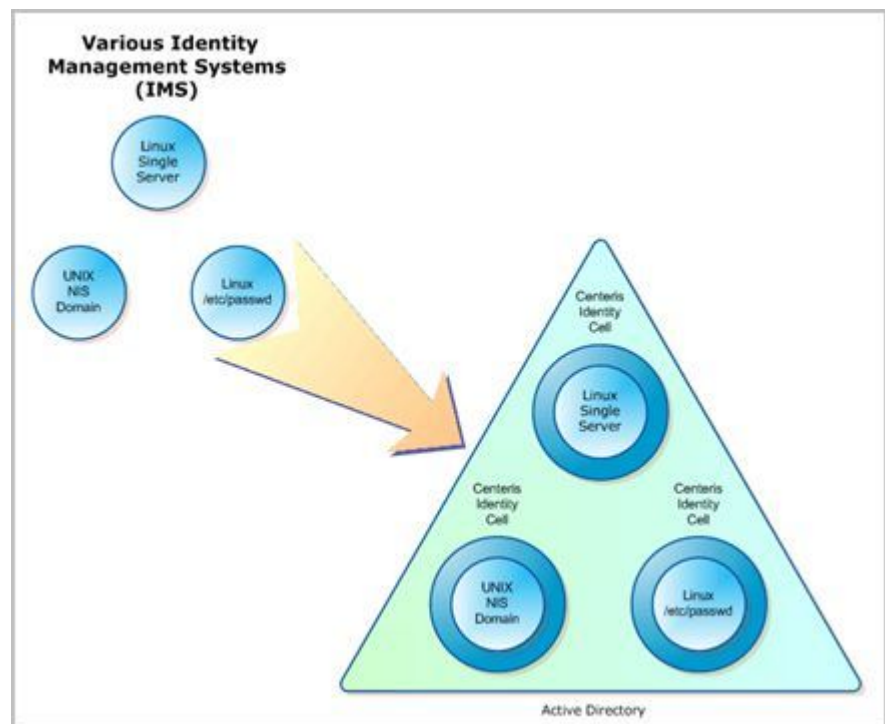
複数の NIS ドメインが利用されており、それらをやがては削除して全ユーザー / コンピュータを Active Directory に移行させたい場合、Active Directory ユーザーを単一の UID と GID にマッピングさせることは極めて困難かもしれない。複数の NIS ドメインが定義されていると、ユーザーは一般的に各 NIS ドメイン

にさまざまな UID-GID マップを保持している。Likewise を使うと、こうした NIS ドメインを削除できるが、Active Directory の異なる NIS マッピング情報は維持される。なぜなら Likewise はセルを利用して、アクセス中の UNIX/Linux コンピュータに応じてユーザーを異なる UID や GID にマッピングさせるからである。

複数 NIS サーバの保有時に Active Directory へ移行する場合、OU を作成 (または既存の OU を選択) し、NIS サーバに接続されているすべての UNIX コンピュータを OU に追加することができる。その結果、旧 ID 管理システムが作成した、ユーザーの UID-GID マッピングに相当するセルを利用できる。

### 複数セルの利用

複数の UNIX/Linux ホストを保有しているが、UID や GID の管理に集中スキームを採用していなければ、各ホストに固有の UID-GID マッピングが設定されている可能性が高い。また、複数の NIS ドメインといった、2 つ以上の集中 IMS が実装されている可能性もある。ここで、NIS ドメインによって提供された UID-GID の関連付け設定に代わり、複数のセルを利用することが可能である。この方式によって、UNIX/Linux ユーザーは引き続き、各自の既存の UID-GID 情報だけでなく Active Directory 証明書も利用できる。下図は、この方式について図示したものである。



複数のセルを利用している場合、セルが代理する UNIX/Linux オブジェクトを見極めておくに役に立つ。例を以下に挙げる。

- 個々の UNIX、Linux、Mac OS X コンピュータ
- 単一の NIS ドメイン
- 複数の NIS ドメイン (複数セルを要求)

### 移行ツール

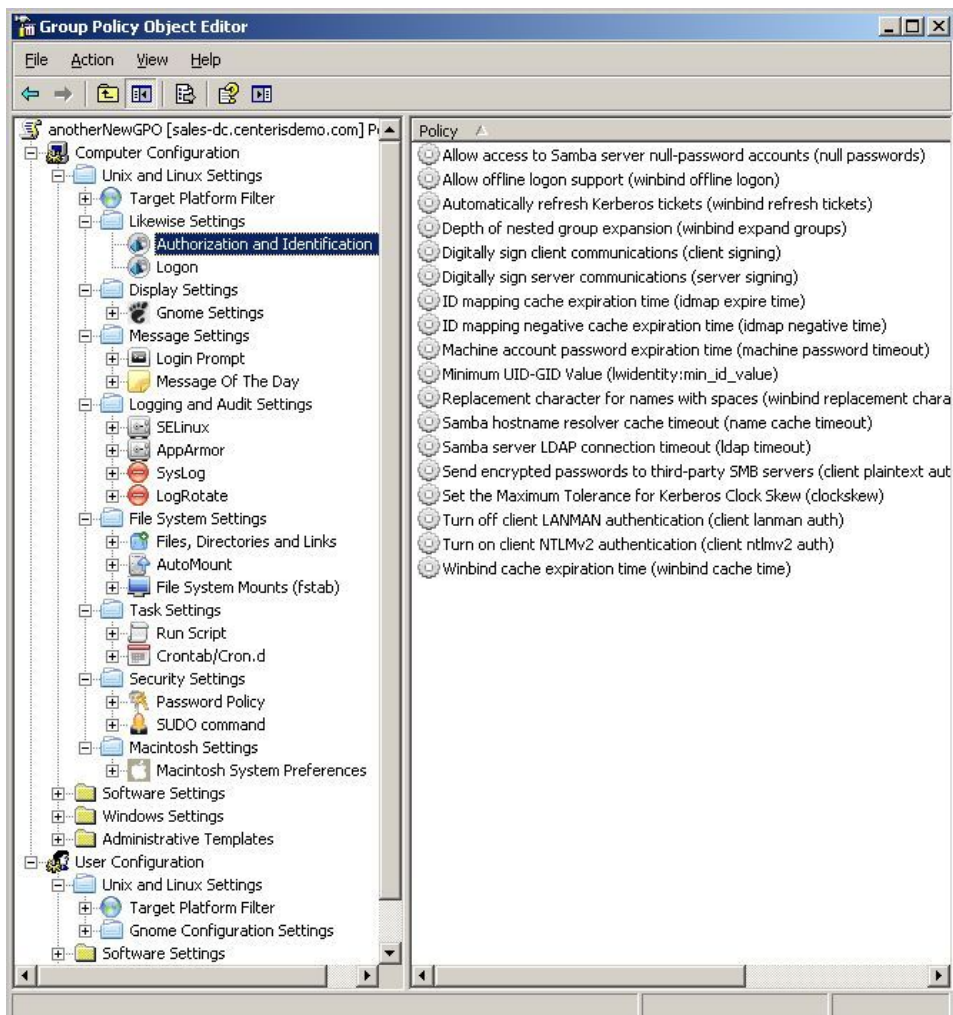
Likewise Console は、Linux、UNIX、Mac OS X のパスワード・ファイルとグループ・ファイル (通常、/etc/passwd および/etc/group) をインポートし、その UID と GID を、Active Directory において定義されたユーザーやグループに自動的にマッピングする移行ツールを提供している。このツールは、UNIX と Linux の UID および GID を Active Directory のユーザーやグループに関連付ける Windows 自動スクリプトも作成する。

### 孤立オブジェクト・ツール

Likewise Console は、孤立オブジェクトを検出して削除するツールを提供している。孤立オブジェクトは、UNIX や Linux のユーザー ID やグループ ID などのリンク済みオブジェクトであり、Active Directory ドメインからグループやユーザーのセキュリティ ID (SID) を削除した後に Likewise セルに残っている。Active Directory の孤立オブジェクトを削除することは、手動でアサインされたユーザー ID の整理と検索スピードの向上につながる。

## グループ・ポリシーの適用

Active Directory と、UNIX、Linux、Mac OS X コンピュータ間の相互運用性の確保における究極の課題は、グループ・ポリシーの適用である。Likewise の場合、Group Policy Object Editor と Group Policy Management Console を使って 100 を超える Likewise グループ・ポリシーと何千ものユーザー・ポリシーを作成して、それらを Linux、UNIX、Mac OS X 環境のコンピュータに適用でき、非 Windows システムの集中管理を行える。



たとえば、ドメイン内の目的のコンピュータ用の共通 sudoers ファイルを定義することによって、ルート・レベル・コマンドへ sudo でアクセス可能なユーザーをコントロールするグループ・ポリシーを設定できる。sudo 用のグループ・ポリシーを用いると、一貫性の高い監査をリモートで行い、UNIX/Linux リソースへのアクセスをコントロールする強力なメソッドを得られる。

Likewise は、セキュリティ、認可、監査、その他の課題の解決に役立つグループ・ポリシー・カテゴリを提供している。下表を参照されたい。これは、100 を超える Likewise のグループ・ポリシーのほんの一部を例として挙げたものである。

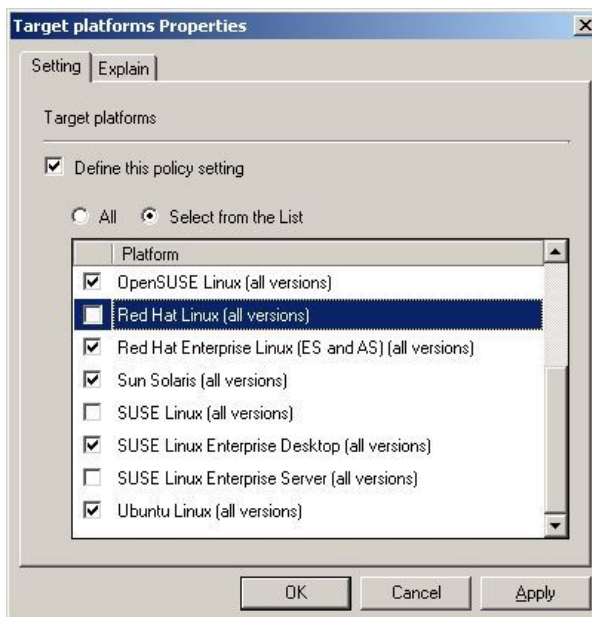
グループ・ポリシー・カテゴリ	ポリシー例
認可と ID	Kerberos チケットの自動更新 lwiauthd 用の winbind のキャッシュ有効期限を設定 マシン・アカウント・パスワードの有効期限を設定
ログオン	キャッシュされたログオンの許可 ログオン権限の許可 デバッグ情報のログ ログオン時における Kerberos チケットの取得 ログオン段階でユーザー・アカウント用のホーム・ディレクトリを作成
ディスプレイ設定	スクリーン・セーバーでシステムをロック スクリーン・セーバーのアイドル遅延の設定
メッセージ設定	特定日のメッセージの設定 ログイン・プロンプト・メッセージの設定
設定のロギングと監査	SysLog ポリシーの作成 SELinux ポリシーの定義 AppArmor ポリシーの設定
ファイル・システム設定	ファイル・システム・マウントの設定 ファイル・システムの自動マウント
タスク設定	スクリプトの実行 crontab や cron.d を用いた cron ジョブのスケジューリング
セキュリティ設定	sudoer ファイルの定義 パスワードの最短長、最長/最短有効期間の設定 複雑なパスワードの要求
Mac OS X	UDP トラフィックの阻止 自動ユーザー・ログインの無効化 ファイアウォール・アクティビティのログ システム優先権をパスワードで保護

Likewise は、Windows のシステム・ボリューム (sysvol) 共有ディレクトリのデフォルトのグループ・ポリシーと同じフォーマットで UNIX/Linux グループ・ポリシーを格納する。ロケーションも同じである。Active Directory のドメインに追加さ

れる UNIX/Linux コンピュータは、Windows システムと同じ方式で個々のグループ・ポリシーを受け取る。

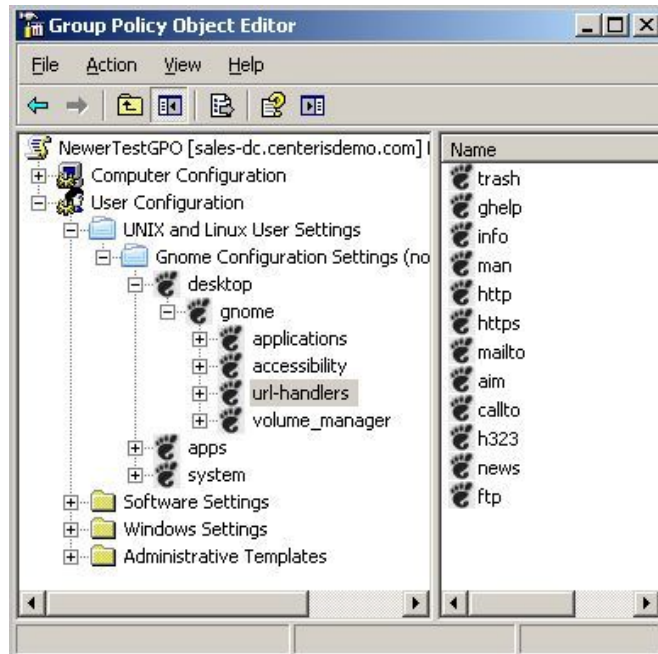
グループ・ポリシーを用意してコンピュータに適用するために、Likewise Group Policy Agent は、ドメインに追加されている Linux、UNIX、Mac OS X コンピュータ上でデーモンとして常時起動している。このエージェントは、コンピュータが属するドメインや組織単位用に設定されたポリシーの変更についてドメイン・コントローラを調べる。Group Policy Agent は、コンピュータのマシン・アカウント証明書を利用して、ネットワーク上でドメインの保護システム・ボリューム共有ディレクトリからポリシー・テンプレート・ファイルをセキュアに取り込む。Group Policy Agent は Active Directory に接続し、30 分おきに変更を取り込んで適用し、コンピュータはブートあるいは再起動される。GPO リフレッシュ・ツールがブートや再起動を要求することもある。

ポリシーを適用する Linux/UNIX プラットフォームは選択できる。たとえば、ある sudo ポリシーを UNIX プラットフォーム用に、そして別の sudo ポリシーを Linux プラットフォーム用に定義することが可能である。



### ユーザー・ポリシー

Likewise ではまた、Linux のユーザー設定に適したグループ・ポリシーを設定できる。このポリシーは、Gnome GConf プロジェクト・ベースで、デフォルトの Web ブラウザなど、デスクトップおよびアプリケーションの優先度について定義する。Linux プラットフォーム用に Gnome スキーマを追加すれば、Group Policy Object Editor の User Configuration の下にある Unix and Linux User Settings フォルダにポリシーが格納される。



Gnome ベースのグループ・ポリシーは数千種存在しており、ブラウザ、ヘルプ・ビューワ、メイン・メニューなどのアプリケーション用ユーザー設定を含んでいる。また、アクセス性を確保するためのキーボード調整、URL ハンドラの定義、ボリューム・マネージャの構成用の設定も組み込まれている。たとえば、リムーバブル記憶装置ドライブをコンピュータに挿入したときに Gnome ボリューム・マネージャが自動的にそれをマウントしたか否かを見極めるためのユーザー・ポリシーを設定できる。

## ソフトウェア・コンポーネントの概要

Likewise は、いくつかのソフトウェア・コンポーネントを構成している。各コンポーネントは Linux/UNIX コンピュータを Active Directory で管理するために必要な機能部分を提供している。

コンポーネント	機能
Agent	Linux/UNIX コンピュータを Active Directory に追加する (Domain Join Tool を使用)。 Active Directory Domain Controller とやりとりしてユーザーやグループを認証 / 認可する。 グループ・ポリシーの用意と更新。
Console	Active Directory Domain Controller に接続されている Windows 管理ワークステーション上で実行され、Active Directory 上の Linux、UNIX、Mac OS X コンピュータを管理しやすくする。 ユーザーの移行、ステータス・チェック、ライセンスのアサイン、孤立オブジェクトの検出と削除、レポート作成を行う。
Integrated Management Tools	UNIX/Linux ユーザーを統合するために Active Directory Users and Computers を拡張する。 Linux、UNIX、Mac OS X のグループ・ポリシーと、特定プラットフォームにおいてそれらを対象にする方法を盛り込むために Group Policy Object Editor を拡張する。
Cell Manager	Active Directory Organizational Units に関連付けられたセルを管理する MMC スナップイン。

### Likewise Agent

このエージェントは、Linux/UNIX コンピュータに展開されており、ネーム・サービス・スイッチ (NSS) あるいは Pluggable Authentication Module (PAM) を用いたようなアプリケーションにもマッピングを実装できるようコア・オペレーティング・システムに統合されている。PAM 対応アプリケーションの例として、ログイン・プロセス (/bin/login) が挙げられる。

このエージェントは、認証用の Kerberos 5 クライアントとして、また、認可用の LDAP クライアントとして機能する。さらに、Active Directory ドメインがローカル・ソフトウェア設定を更新する間に作成されたセキュリティ証明書 (例: sudo 構成ファイル) を用いて、グループ・ポリシーを実施するサービスとして機能する。

エージェント・デーモン	説明
/etc/init.d/centeris.com-lwiauthd	Likewise の認証デーモン。認証、認可、キャッシング、idmap 検索を行う。
/etc/init.d/centeris.com-gpagent	Group Policy Agent。Active Directory から Group Policy Objects を検索し、それをコンピュータに適用する機能をバックグラウンド・サービスとして実行する。

このエージェントも 2 つのライブラリを備えている。

1. NSS ライブラリ: `lwidentity.so`
2. PAM ライブラリ: `pam_lwidentity.so`

このエージェントは、アウトバウンド・トラフィックに以下のポートを使用する。また、クライアント専用であり、どのようなポートにおいても反応しない。

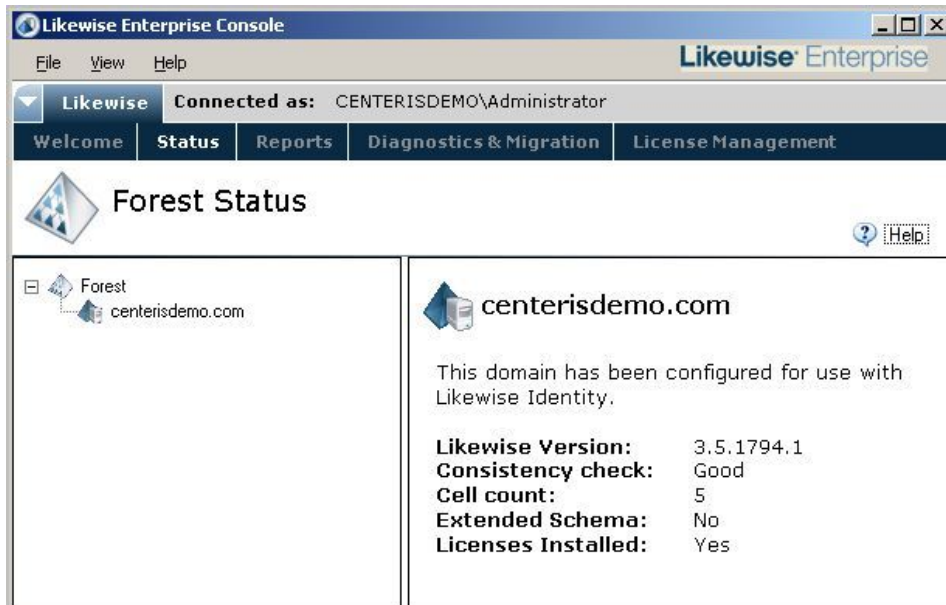
ポート	プロトコル	用途
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP

### Likewise Console

Likewise Console は、Active Directory 内で Linux、UNIX、Mac OS X コンピュータを管理する上で役に立つ。このコンソールは、Active Directory Domain Controller に接続されている Windows 管理ワークステーション上で実行される。コンソールに含まれる複数のインスタンスを実行でき、また、それらを別のドメインに振り向けることもできる。さらに、異なるユーザー・アカウントを用いて実行することも可能である。

コンソール・コンポーネント	機能
Domain Extension Wizard	スキーマ・モード/非スキーマ・モードの選択、Schema Master ドメイン・コントローラにおけるスキーマの拡張のインストール、RFC 2307 属性のグローバル・カタログへの追加を行う。
Status	Active Directory のフォレストおよびドメインに関するステータス情報を獲得する。
Migration Tool	passwd ファイルとグループ・ファイルをインポートし、情報を Active Directory のユーザーとグループにマッピングすることによって UNIX/Linux ユーザー/グループを移行させる。
Orphaned Objects Tool	孤立オブジェクトを検出して削除する。孤立オブジェクトは、UNIX や Linux のユーザーID やグループ ID などのリンク済みオブジェクトであり、Active Directory ドメインからグループやユーザーのセキュリティ ID (SID) を削除した後に Likewise セルに残っている。
Reports	ユーザー、グループ、コンピュータに関するレポートを作成する。
License Management	Likewise ライセンスを UNIX/Linux コンピュータにインポート、アサインする。

以下に、コンソールの Status ページの例を示す。

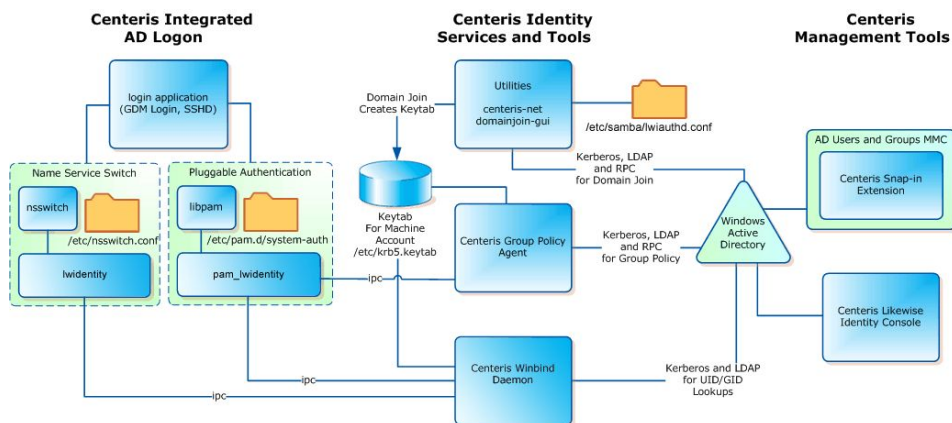


### Integrated Management Tool

コンソールをインストールする際、UNIX/Linux コンピュータ、ユーザー、グループを管理できるようにするために Likewise の設定が Active Directory Users and Computers に追加される。設定はさらに、Linux/UNIX 固有のグループ・ポリシーを作成、編集できるようにするために Group Policy Object Editor に追加される。Group Policy Management Console でグループ・ポリシー関連情報を閲覧することもできる。

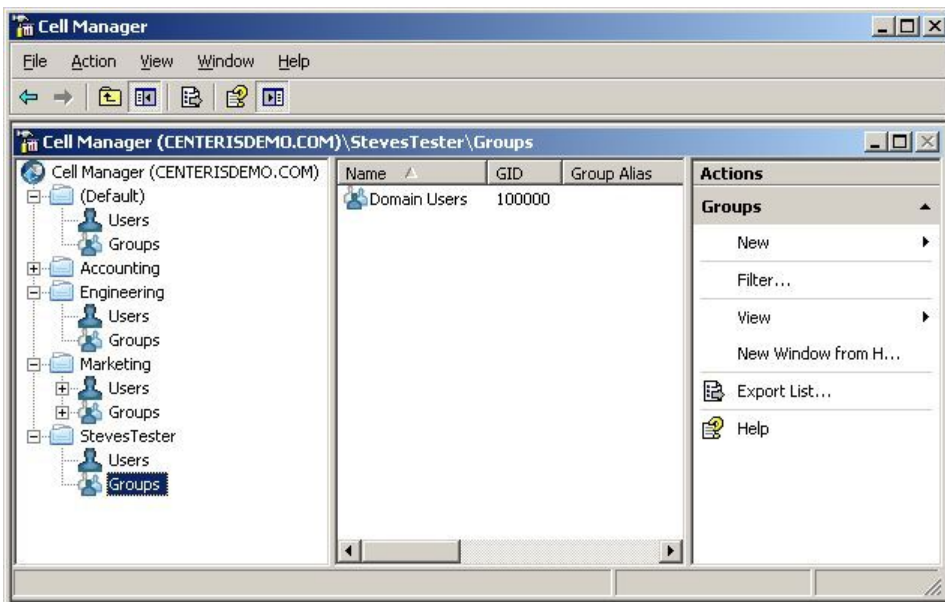
修正済み AD コンポーネント	UI の追加と機能
Active Directory Users and Computers	OU をセル、管理コンピュータ、ユーザー、グループ、UID/GID、ホーム・ディレクトリ、シェルなどの情報に関連付けるための設定 (Properties シートの Likewise Settings タブ上に格納)。
Group Policy Object Editor	各ポリシーを設定するためのコンソール・ツリーとユーザー・インタフェースにおける Linux、UNIX、Mac OS X のグループ・ポリシー。 異なる UNIX/Linux プラットフォームにおけるグループ・ポリシーを目的としたユーザー・インタフェース。
Group Policy Management Console	Linux、UNIX、Mac OS X グループ・ポリシー向けの総括レポート。

下図は、管理ツール、コンソール、グループ・ポリシー・エージェント、Likewise winbind デーモンが PAM、NSS、Kerberos とどのようにやりとりし、Active Directory で相互運用性を確保するのを示したものである。



## Cell Manager

Likewise Cell Manager は MMC スナップインであり、Active Directory Organizational Units に関連付けたセルの管理に利用できる。Cell Manager を用いると、セルのフィルタと閲覧、管理権限の移譲、セル向け認可の変更、セルの追加を行え、ユーザーとグループは Linux/UNIX にアクセスできるようになる。たとえば、Cell Manager を使ってアクセス・コントロール・リスト (ACL) を作成できる。ACL によって、ユーザーは特別な権限がなくても、指定した操作を実行できる。Cell Manager は、Likewise Console と同時に自動的にインストールされるが、その画面は以下のようなものである。



## 標準とプロトコル

Likewise ソフトウェアは以下の標準、プロトコル、RFC に対応している。

- Kerberos 5 (RFC 4120)
- LDAP (RFC 4511 および 2307)
- DNS (RFC 1035 および 3645)
- SMB/CIFS
- MSRPC

## まとめ

UNIX/Linux コンピュータを Active Directory に統合する場合、いくつかの重要な障壁がある。

1. Linux/UNIX コンピュータを Active Directory ドメインへ追加する。
2. Active Directory を用いてユーザーを認証する。
3. UNIX/Linux コンピュータ上のリソースへアクセスするために Active Directory ユーザーを認可する。
4. Linux と UNIX の UID/GID 情報を Active Directory 対応オブジェクトにマッピングする。
5. Active Directory を用いてグループ・ポリシーを Linux/UNIX コンピュータに適用する。

Likewise は、集中管理と ID 管理を実現するソリューションを提供することによって、下表に示すとおり、相互運用性にまつわるこれらの課題を解決する。

相互運用性上の障壁	Likewise ソリューション
UNIX コンピュータには NIS、Linux コンピュータにはローカル認証、Windows コンピュータには Active Directory といった具合に、システムによってまったく異なる ID 管理システムが採用されている。	Linux、UNIX、Mac OS X、Windows コンピュータの ID 管理を Active Directory 内で集中化させる。
認証	Kerberos を用いて、Windows、Linux、UNIX、Mac OS X コンピュータ上で個々の Active Directory 証明書を持つユーザーを認証する。
認可	UNIX/Linux ユーザーとグループ ID を Active Directory オブジェクトにマッピングする。
集中管理: UNIX/Linux コンピュータは.conf ファイルに、Windows コンピュータはグループ・ポリシーにマッピングされている。	100 を超えるグループ・ポリシーを Active Directory 内で Linux、UNIX、Mac OS X コンピュータ向けに提供することによって集中メンテナンス / 管理を行う。