Sun | SUN ZFS STORAGE APPLIANCE

Oracle ホワイトペーパー
2011 年 2 月

Sun ZFS Storage Appliance の Active Directory とネットワーク情報サービス間ルールベースアイデンティティマッピング実装ガイド

はじめに

Sun ZFS Storage Appliance アイデンティティマッピングサービスでは、それぞれのユーザーの Windows および UNIX アイデンティティを関連付けて、Active Directory サービスとネットワーク情報サービス (NIS) の両方のユーザーを管理します。このマッピングサービスを使用すると、パスワードによってアクセスが制御されるディレクトリやファイルなどの共有を、クライアントから共通インターネットファイルシステム (CIFS)/サーバーメッセージブロック (SMB) またはネットワークファイルシステム (NFS) プロトコルを介してエクスポートおよびアクセスできるようになります。

本書、アイデンティティと名前のマッピング用にルールが作成されるルールベースのマッピングアプローチについて説明します。これらのルールによって、Windows アイデンティティと UNIX アイデンティティ間の相関関係が確立されます。本書では、UNIX アイデンティティ用のディレクトリサービスとして NIS が使用されていますが、軽量ディレクトリアクセスプロトコル (LDAP) サーバーでも同じ機能を実行できます。

概要と前提条件

本書では、ルールベースのアイデンティティマッピングを正しく動作させるための Sun ZFS Storage Appliance アイデンティティマッピングサービスと関連アプライアンスの設定の構成方法について説明します。また、アプライアンス上で実行されるアクティビティについて説明し、Windows クライアントと Solaris クライアントの両方に対しどのようにマッピングが動作するかを示します。

本書の内容は、Sun ZFS Storage Appliance Software Release 2010.Q3 に基づいています。以前のバージョンの Sun ZFS Storage Appliance ソフトウェアでは、SMB が CIFS と呼ばれていましたが、このホワイトペーパーの目的に合わせて、CIFS サービスを SMB と呼びます。

本書では、読者が Windows Active Directory および Solaris NIS 環境について実際に役立つ知識を備えていることを前提にします。

本書内の手順では、次のことが想定されます。

- Sun ZFS Storage Appliance が、IP アドレス、ネットマスク、ゲートウェイなどのネットワーク設定とともに初期構成されている
- アプライアンスクロックが時刻情報プロトコル (NTP) タイムサーバーと同期している
- ストレージプールが構成されている
- それぞれのドメインに、マップするユーザーとグループが配置されている

ユーザーとグループのアクセス権設定は、デフォルト値とともに表示されていますが、これは推奨設定を示すものではありません。

Sun ZFS Storage Appliance アイデンティティマッピングサービスの、概念、機能、動作などの詳細については、このホワイトペーパーの終りにあるセクション「関連資料」を参照してください。

次の内容は本書の対象外です。

- ドメインコントローラ上のドメイン名システム (DNS)/NTP 設定
- ディレクトリベースのアイデンティティマッピング
- UNIX (IDMU) 統合用のアイデンティティ管理
- マッピングの拒否
- Active Directory から UNIX または UNIX から Active Directory への単一方向マッピング
- 自動ホーム機能

Sun ZFS Storage Appliance の準備

アイデンティティマッピングサービスを正しく動作させるには、ネットワークおよびネームサービスを適切に構成する必要があります。このセクションでは、Active Directory と NIS 間のルールベースアイデンティティマッピングを構成するためのデフォルト以外のアプライアンス設定について説明します。

DNS サービスの設定

Sun ZFS Storage アプライアンスを Active Directory ドメインに参加させるには、事前に DNS サービス設定を適切に行う必要があります。「DNS サービス」ページで、次の手順を実行します。

- DNS サーバーのドメイン名を、「**DNS ドメイン**」ボックスに入力します。
- DNS サーバーの IP アドレスを、「**DNS サーバー**」ボックスに入力します。
- 「**適用**」ボタンをクリックします。

さらに DNS サーバーを追加するには、「+」アイコンをクリックします。

NTP サーバーの指定

必須ではありませんが、Active Directory サーバーを NTP サーバーとして使用すると、アプライアンスクロックが確実に Active Directory ドメインクロックと同期します。ドメインコントローラとアプライアンス間の時間差が 5 分を超えていると、アプライアンスを Active Directory ドメインに参加させようとしても失敗する場合があります。

- 「NTP サービス」ページで、次の手順を実行します。
- 「Manually specify NTP servers(s)」オプションを選択します。
- 「サーバー」ボックスに、NTP サーバー名を入力します。
- 「**適用**」ボタンをクリックします。

さらに NTP サーバーを追加するには、「+」アイコンをクリックします。

注:「Sync」ボタンを選択すると、アプライアンスの時間とブラウザの時間が同期しますが、NTP サーバー時間とは同期しません。

アプライアンスを Active Directory ドメインに参加させる

アプライアンスを Active Directory ドメインに参加させるには、「Active Directory サービス」ページで、次の手順に従います。

- 「**JOIN DOMAIN**」ボタンをクリックします。
- Active Directory Domain、管理ユーザー名およびパスワードを入力します。
- 「**適用**」ボタンをクリックします。

ドメインに参加させようとすると認証エラーが発生する場合は、以下のセクション「SMB サービスのトラブルシューティング」でトラブルシューティング情報を参照してください。

アプライアンスを NIS ドメインに参加させる

アプライアンスを NIS ドメインに参加させる前に、NIS サーバー用のレコードが DNS に存在することを確認してください。

これは、正しい名前解決がアプライアンスで行われるようにするための必須手順です。「NIS サービス」ページで、次の手順を実行します。

- 「**ドメイン**」ボックスに、NIS ドメイン名を入力します。
- 「**Use listed servers**」オプションを選択して、オプションの下に表示されるボックスにサーバー名を入力します。
- 「**適用**」ボタンをクリックします。

さらに NIS スレーブを追加するには、「+」アイコンをクリックします。

SMB サービスのトラブルシューティング

正しいユーザー名とパスワードを入力しても、アクセスが拒否されているか、オペレーティングシステムがユーザーのログオンを実行できない状態を示すエラーメッセージが表示される場合は、「**LAN Manager Compatibility Level**」設定の変更が必要になる場合があります。Sun ZFS Storage Appliance 上でサポートされる認証モードは、LAN Manager (LM)、NT LAN Manager (NTLM)、LMv2、NTLMv2 です。

SMB サービスの構成に関するヘルプ情報については、アプライアンスインタフェースの右上隅にある「ヘルプ」ボタンをクリックしてください。左のサイドバーで、「サービス」を選択します。右の「目次」ボックスで、「**データ**」を選択します。表示されるテーブルで、「**SMB**」を選択します。

Windows Server 2003 および 2008 上での Active Directory サービスの構成

異なるバージョンの Windows Server で動作するように Active Directory サービスを構成する方法の最新情報については、アプライアンスインタフェースの右上隅にある「ヘルプ」をクリックしてください。左のサイドバーで、「**サービス**」を選択します。右の「目次」ボックスで、「**ディレクトリ**」を選択します。表示されるテーブルで、「**Active Directory**」を選択します。右の「目次」ボックスで、「**Windows Server 2008 Support**」を選択します。

SMB のトラブルシューティング情報については、Genunix OpenSolaris wiki の「CIFS サービストラブルシューティング」ページで「Cannot Join a Windows Domain」トピックを参照してください。

NFS サービスのトラブルシューティング

以前のバージョンの Sun ZFS Storage ソフトウェアによっては、アプライアンスを Active Directory ドメインに参加させると、Active Directory ドメインが、NFS サービスの「検索」フィールドの最初のオプションになります。その結果、NFSv4 アイデンティティドメインがデフォルトにより Active Directory ドメインになります。

この動作をオーバーライドするには、「NFS サービス」ページで次の手順に従います。

- 「**Use DNS domain as NFSv4 identity domain**」オプションの選択を解除します。

- 優先 NFSv4 アイデンティティドメイン名を、「**Use custom NFSv4 identity domain**」ボックスに入力します。
- 「**適用**」ボタンをクリックします。

注:アイデンティティドメインが、NFSv4 クライアントとサーバー間で一致していないと、クライアントは正しく認証できなくなります。

ルールベースのアイデンティティマッピングの定義

このセクションでは、双方向マッピングを使用して、Active Directory アイデンティティと UNIX アイデンティティをマップできるようにするマッピングルールの設定について説明します。これらのルールは、アイデンティティマッピングの最も一般的な配備を表し、ルールベースのアイデンティティマッピングのみに依存するほとんどの顧客環境の要件を満たします。

注:アイデンティティマッピングルールを変更しても、すぐに反映されない場合があります。したがって、アクティブなファイル共有セッションに影響しない可能性があります。混乱を避けるため、マッピングを構成してから共有をエクスポートしてください。クライアントが共有にアクセスしているときに変更が必要になった場合は、「マッピング」タブに移動し、マッピングのキャッシュをフラッシュして、すべてのクライアントでマッピングの再確立を実行します。

マッピングモードの選択

マッピングモードを選択するには、「サービス」ページで次の手順に従います。

- 図 1 のように、「**マッピングモード**」ドロップダウンボックスから「**ルールベース**」を選択します。
- 「**適用**」ボタンをクリックします。

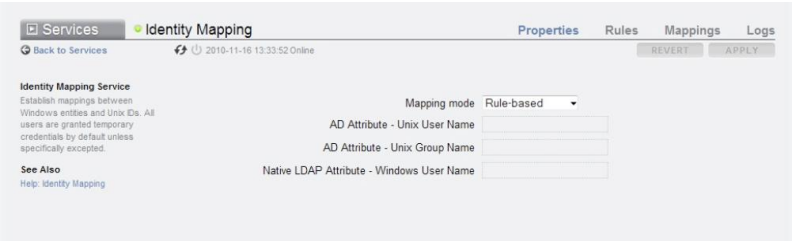

図 1:アイデンティティマッピングプロパティー

ドメイン全体ルールを使用したルールベースマッピングの追加

ドメイン全体マッピングルールは、Windows ドメインから UNIX 名にマップする場合、一部またはすべての名前に適合します。

注:Windows ドメインごとに、Windows ドメイン内のすべてのユーザーをすべての UNIX ユーザーにマップする双方向マッピングを 1 回のみ行えます。

Windows から UNIX へのマッピングでは、大文字と小文字と区別します。たとえば、Windows ユーザー名の jsmith は UNIX ユーザー名の jsmith に一致しますが、Windows

ユーザー名の Jsmith は一致しません。ただし、ワイルドカード文字 (*) を使用して、複数のユーザー名をマップできます。

ドメイン全体マッピングルールをユーザー用に作成するには、次の手順に従います。

- Rules という語の隣にある「**ルール**」タブで、「**+**」**アイコン**をクリックします。
- 図 2 のように、オプションを選択します。

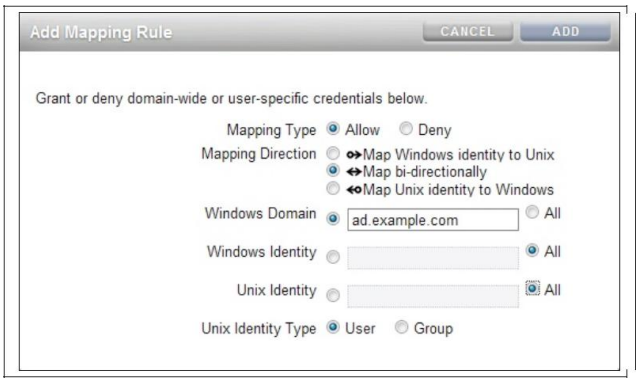

図 2: ドメイン全体ユーザーマッピングの追加

ドメイン全体マッピングルールをグループ用に作成するには、次の手順に従います。

- Rules という語の隣にある「**ルール**」タブで、「**+**」**アイコン**をクリックします。
- 図 3 のように、オプションを選択します。

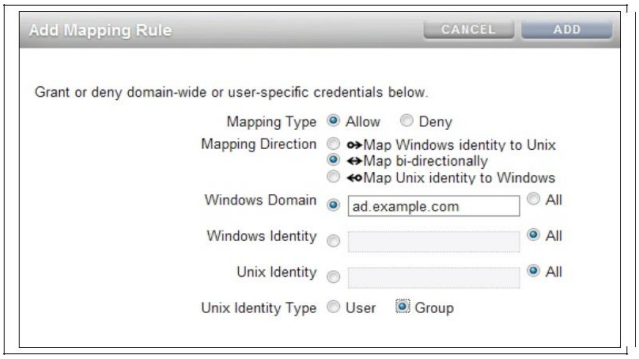

図 3: ドメイン全体グループマッピングルールの追加

図 4 は、図 2 と図 3 で作成された 2 つのマッピングルールの結果を示しています。

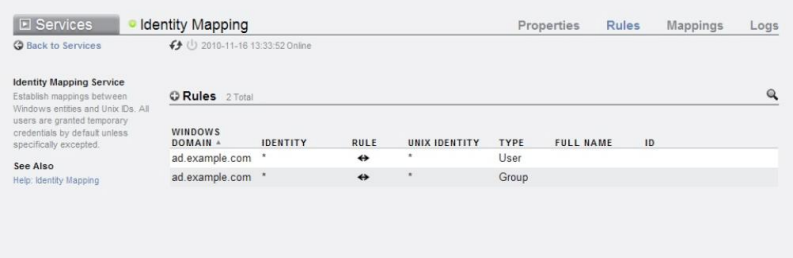

図 4: ドメイン全体ルールの要約

図 5 と図 6 は、上で作成したドメイン全体ルールに基づいて、ユーザーとグループをマップする方法を示しています。Windows ユーザー名またはグループ名を「アイデンティティ」フィールドに入力したときにマッピングが定義されていると、対応する UNIX ユーザー名またはグループ名と ID が「ユーザープロパティ」の下に表示されます。同じように、UNIX ユーザー名またはグループ名を「アイデンティティ」フィールドに入力したときにマッピングが定義されていると、対応する Windows ユーザー名またはグループ名と ID が「ユーザープロパティ」の下に表示されます。

図 5 は、UNIX ユーザー *user01* にマップされた Windows ユーザー *user01* を示しています。

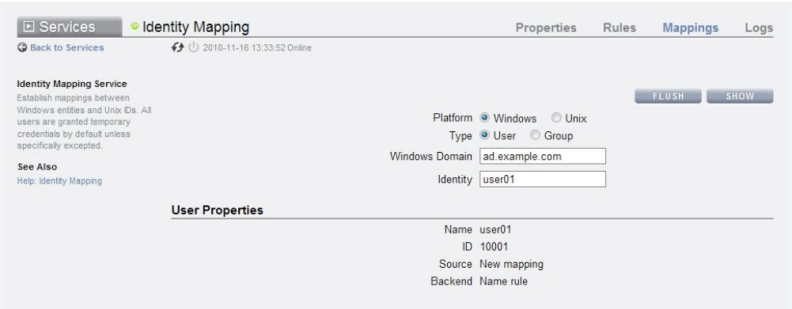

図 5:Windows ユーザー user01 の場合のドメイン全体マッピングの結果

図 6 は、Windows グループ *group01@ad.example.com* にマップされた UNIX グループ *group01* を示しています。

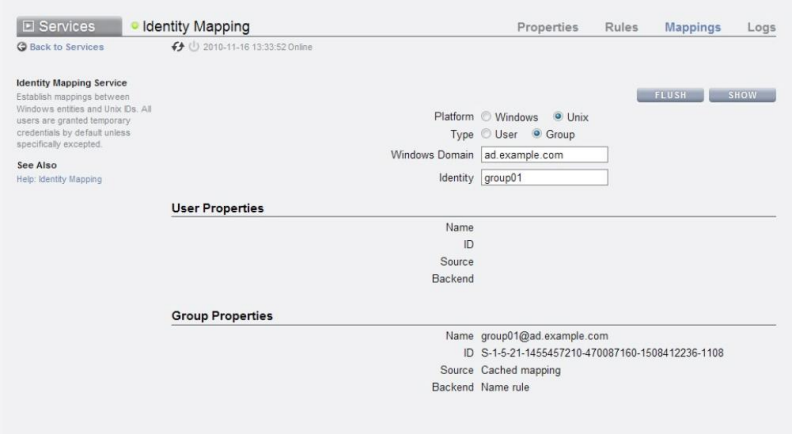

図 6:UNIX グループ group01 の場合のドメイン全体マッピングの結果

個々のユーザーまたはグループごとのルールベースマッピングの追加

Windows ユーザー ad-user と UNIX ユーザー nis-user 間のマッピングルールを作成するには、次の手順に従います。

- Rules という語の隣にある「**ルール**」タブで、「**+**」**アイコン**をクリックします。
- 図 7 のように、オプションを選択します。

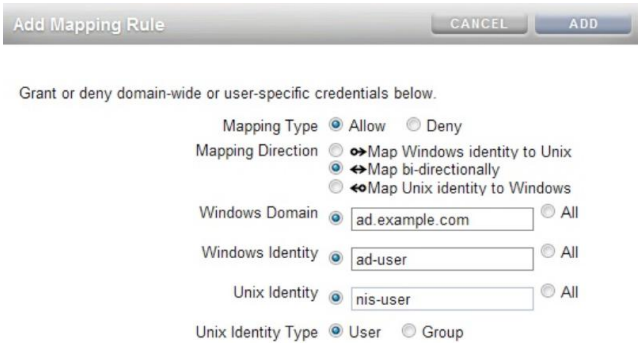

図 7:個々のユーザールールの追加

Windows グループ *ad-group* と UNIX グループ *nis-group* 間のマッピングルールを作成するには、次の手順に従います。

- Work Rules の隣にある「**ルール**」タブで、「**+**」**アイコン**をクリックします。
- 図 8 のように、オプションを選択します。

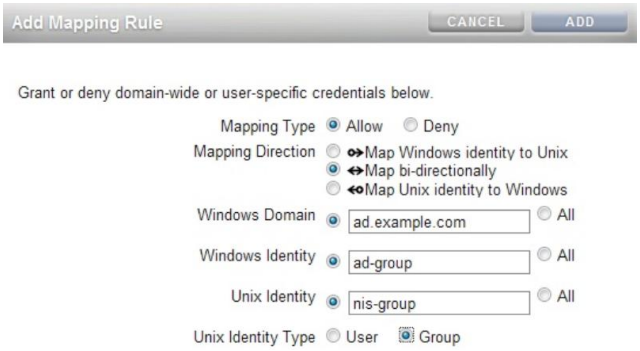

図 8:個々のグループルールの追加

Active Directory のデフォルトグループ *Domain Users* を NIS デフォルトグループ *staff* にマップするマッピングルールを作成するには、次の手順に従います。

- Rules という語の隣にある「**ルール**」タブで、「**+**」**アイコン**を選択します。
- 図 9 のように、オプションを選択します。

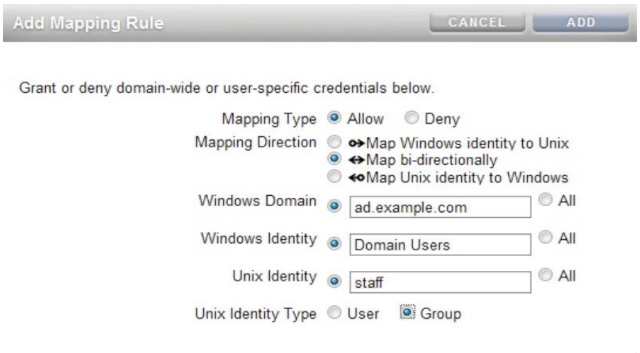

図 9:デフォルトグループルールの追加

図 10 に示す「ルール」ページには、図 7、図 8、図 9 で定義したユーザーおよびグループマッピングルールが一覧表示されます。

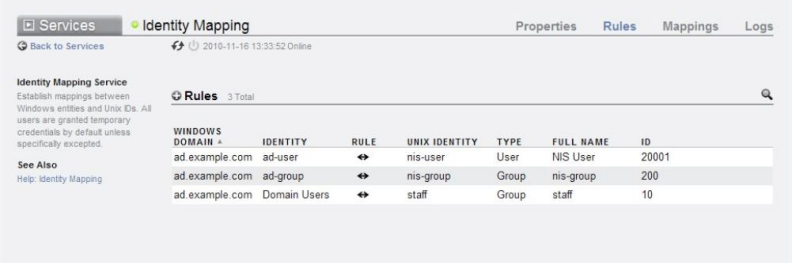

図 10:個々のユーザーおよびグループルールの要約

図 11 は、図 7 で定義した個々のユーザールールの結果として UNIX ユーザー nis-user にマップされた Windows ユーザー ad-user を示しています。

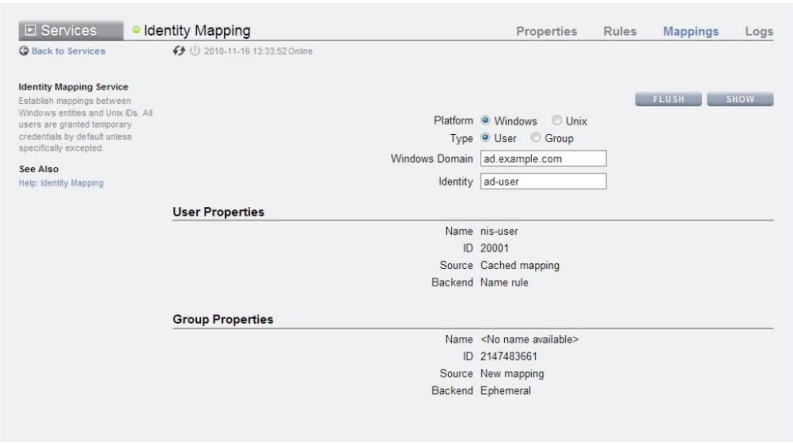

図 11:個々のユーザーマッピングの結果

図 12 は、図 8 で定義したグループルールの結果として Windows グループ *ad-group@ad.example.com* にマップされた UNIX グループ *nis-group* を示しています。

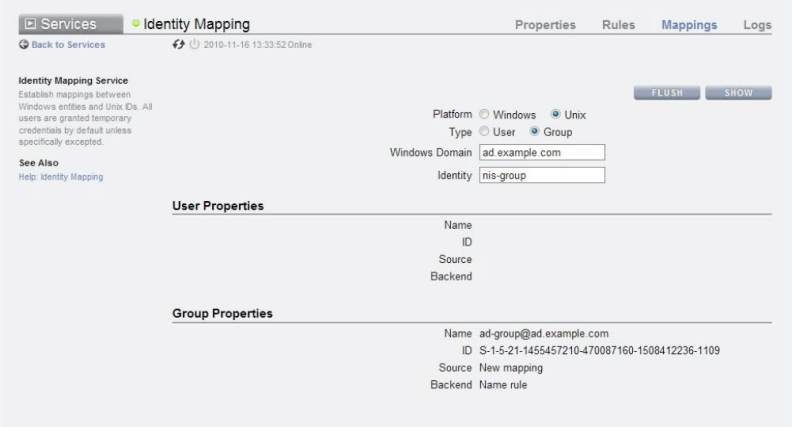

図 12:個々のグループマッピングの結果

図 13 は、図 9 で定義したデフォルトグループルールの結果として Windows グループ *Domain Users@ad.example.com* にマップされた UNIX グループ *staff* を示しています。

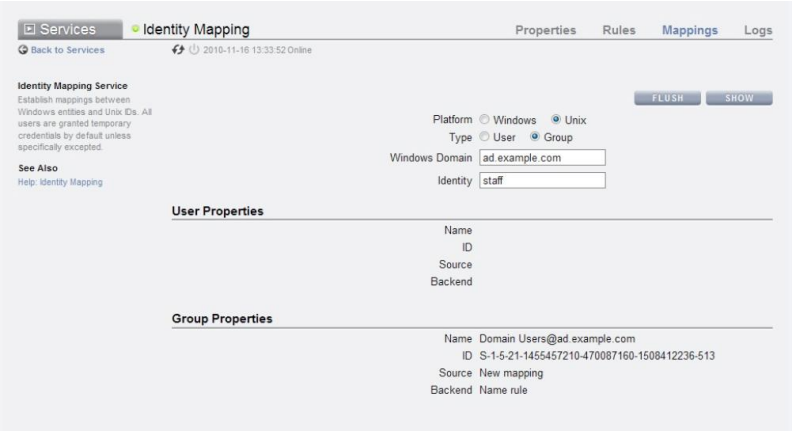

図 13:デフォルトのグループマッピングの結果

ドメイン全体ルールと個々のルールベースマッピングの併用

Active Directory ドメイン内のユーザーまたはグループが NIS ドメインで同じ名前にならない場合は、ドメイン全体ルールでは不十分な可能性があります。たとえば、Active Directory の *Domain Users* グループを NIS *staff* グループにマップすることが必要な場合があります。

図 14 に示すルールには、ドメイン全体マッピングと個々のマッピングの両方が含まれています。Windows アイデンティティを UNIX アイデンティティにマップする要求が行われると、要求は最初に個々のすべてのルールのコンテキストで評価され (図 14 の 3 番目、4 番目、5 番目のルール)、次にドメイン全体ルールのコンテキストで評価されます (図 14 の最初の 2 つのルール)。この例では、アイデンティティマッピングサービスで Windows ユーザー *ad-user* に対する UNIX アイデンティティを提供するように要求されると、サービスで *ad-user* という名前の UNIX ユーザーを解決できる場合でも、UNIX ユーザー *nis-user* が提供されます。

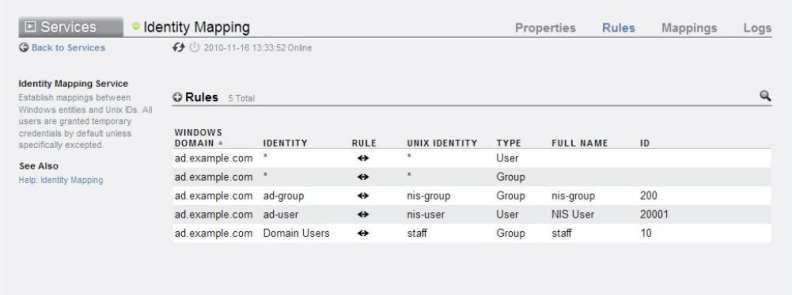

図 14:ドメイン全体ルールと個々のルールの要約

共有の構成と割り当て

ルールベースのアイデンティティマッピングを正しく動作させるには、以下で説明するとおりに特定のプロパティを指定して共有を構成する必要があります。共有は、ユーザーレベルまたはグループレベルで作成して構成できます。

ユーザー共有の設定

このセクションでは、ユーザー共有の作成、共有へのユーザーの割り当て、共有レベルのプロトコル設定、アクセス設定の方法について説明します。

ユーザー共有の作成

user01_share という名前の共有をユーザー *user01* に対して作成するには、次の手順に従います。

- 「共有」タブで、デフォルトプロジェクトを選択します。
- 「**ファイルシステム**」を選択して、「**+**」**アイコン**をクリックします。図 15 のような「**Create Filesystem**」ページが表示されます。
- 共有名 *user01_share* を「**名前**」ボックス、ユーザー名 *user01* を「**ユーザー**」ボックス、グループ名 *staff* を「**グループ**」ボックスに入力します。
- 「Permissions」で、「**Use Windows default permissions**」オプションを選択します。
- 「**適用**」ボタンをクリックします。

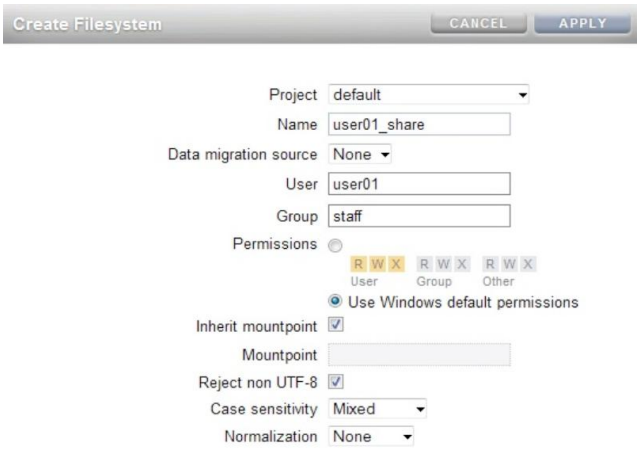

図 15:ユーザー共有の作成

ユーザー共有レベルのプロトコル設定の構成

共有をエクスポートするために SMB プロトコルをユーザーレベルで設定するには、次の手順を実行します（図 16 を参照）。

共有の「プロトコル」タブで、次の手順に従います。

- 「**Inherit from project**」チェックボックスをオフにします。
- 「**リソース名**」ボックスで、エントリ **off** をエントリ **on** に置き換えます。
- 「**適用**」ボタンをクリックします。

リソース名は、この共有を SMB クライアントで参照するときに使用される名前です。off に設定されたリソース名は、SMB クライアントで共有にアクセスできないことを示します。on に設定されたリソース名は、共有が `¥¥server¥<filesystem_name>` としてエクスポートされることを示します。共有名を手動で指定するには、***on*** または ***off*** でなく、カスタムリソース名を入力します。

アクセスベースの列挙が必要な場合は、「**Enable Access-based Enumeration**」オプションを選択して列挙を有効にします。アクセスベースの列挙では、クライアントの資格に基づいてディレクトリエントリをフィルタリングします。クライアントに、ファイルまたはディレクトリへのアクセス権がないと、そのファイルは、クライアントに戻されるエントリの一覧から除外されます。このオプションは、デフォルトでは有効になりません。

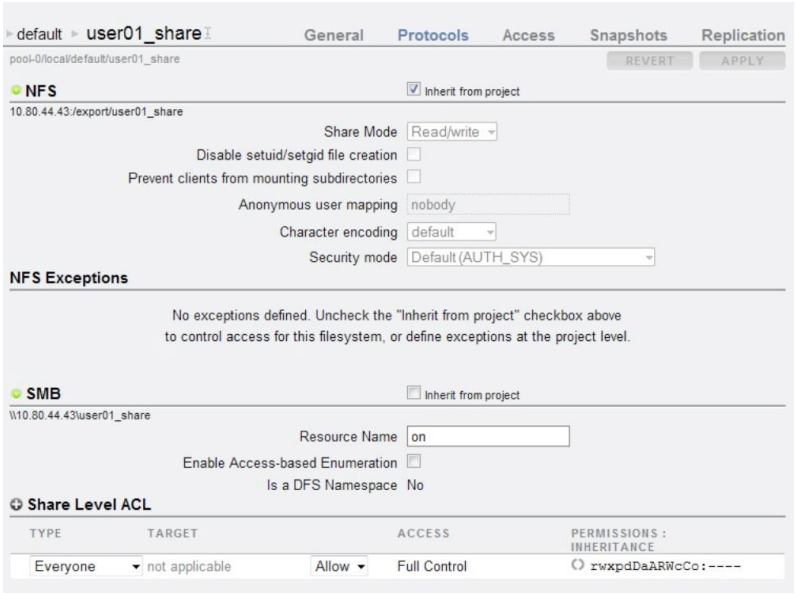

図 16:ユーザー共有レベル SMB プロトコル設定

ユーザー共有レベルのアクセス設定の構成

ルートディレクトリへのアクセス権は、その時点のアクセス許可に基づいて共有が作成されるときに (「ユーザー共有の作成」を参照)、設定されます。このセクションでは、Sun ZFS Storage Appliance Software Release 2010.Q3 および Software Release 2010.Q1 でのアクセス制御リスト (ACL) の継承動作について説明します。

このセクションで示す例は、ドメイン全体ルールを使用してマップされたユーザー *user01* に割り当てられている共有 *user01_share* に基づいています (「ドメイン全体ルールを使用したルールベースマッピングの追加」セクションを参照)。

Sun ZFS Storage Appliance Software Release 2010.Q3 での ACL 動作

Software Release 2010.Q3 で ACL 動作を設定するには、次の手順に従います。

- 「**Inherit from project**」チェックボックスをオフにします。
- 「**ACL inheritance behavior**」ドロップダウンボックスで、図 17 のように「**Inherit all entries**」を選択します。「**Inherit all entries**」オプションを選択すると、継承可能なすべての ACL エントリが継承されます。このオプションは、ユーザーが新しいファイルを作成したときに、ファイルによって作成元のディレクトリツリーのアクセス権が継承されるように、ACL *passthrough* モードを設定します。管理者は、0664 や 0666 などの ACL 継承に使用されるアクセス権を設定します。
- 「**適用**」ボタンをクリックします。

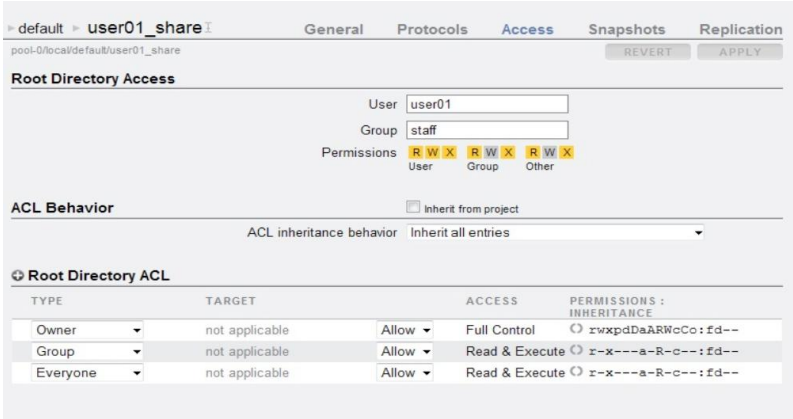

図 17:Sun ZFS Storage Appliance Software Release 2010.Q3 に対応する ACL 継承動作

ルートディレクトリ ACL は、選択された「**Use Windows default permissions**」オプションに基づいて共有が作成されるときに設定されます (図 15 を参照)。図 17 は、「所有者」、「グループ」、「Everyone」ごとに作成された 3 つの**許可**モードエントリを示しています。

エントリを削除するには、エントリにマウスを合わせてゴミ箱アイコンを選択します。

エントリを編集するには、エントリにマウスを合わせて編集用の鉛筆アイコンを選択します。

エントリを追加するには、「**+**」**アイコン**をクリックします。

変更後に「**適用**」ボタンをクリックします。

Sun ZFS Storage Appliance Software Release 2010.Q1 での ACL 動作

Software Release 2010.Q1 で ACL 動作を設定するには、次の手順に従います。

- 図 18 のように、「**Inherit from project**」チェックボックスをオフにします。
- 「**ACL behavior on mode change**」ドロップダウンボックスで、「**Do not change ACL**」を選択して、アクセス権の変更操作が適用されるときに ACL エントリを保持します。
- 「**ACL inheritance behavior**」ドロップダウンボックスで、「**Inherit all entries**」を選択して、継承可能なすべての ACL エントリが継承されることを指定します。
- 「***適用***」ボタンをクリックします。

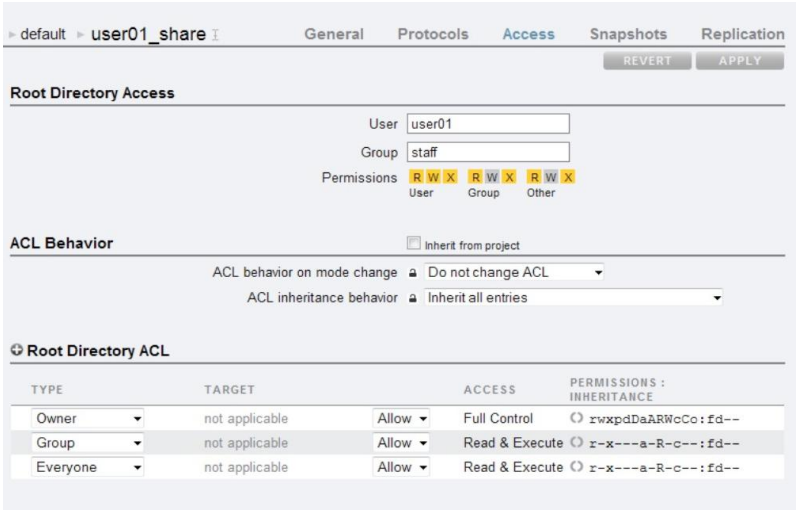

図 18:Sun ZFS Storage Appliance Software Release 2010.Q1 に対応する ACL 継承動作

ルートディレクトリ ACL は、選択された「**Use Windows default permissions**」オプションに基づいて共有が作成されるときに設定されます (図 15 を参照)。図 18 は、「所有者」、「グループ」、「Everyone」ごとに作成された 3 つの**許可**モードエントリを示しています。

エントリを削除するには、エントリにマウスを合わせてゴミ箱アイコンを選択します。

エントリを編集するには、エントリにマウスを合わせて編集用の鉛筆アイコンを選択します。

エントリを追加するには、「+」**アイコン**をクリックします。

変更後に「**適用**」ボタンをクリックします。

グループ共有の設定

このセクションでは、グループ共有の作成、共有へのグループの割り当て、共有レベルのプロトコル設定、アクセス設定の方法について説明します。

グループ共有の作成

group01_share という名前の共有をグループ *group01* に対して作成するには、次の手順に従います。

- 「共有」タブで、デフォルトプロジェクトを選択します。
- 「**ファイルシステム**」を選択して、「**+**」**アイコン**をクリックします。「Create Filesystem」ページが表示されます(図 19 を参照)。
- 共有名 *group01_share* を「**名前**」ボックス、root などのユーザー名を「**ユーザー**」ボックス、グループ名 *group01* を「**グループ**」ボックスに入力します。
- 「Permissions」で、「**Use Windows default permissions**」オプションを選択します。
- 「**適用**」ボタンをクリックします。

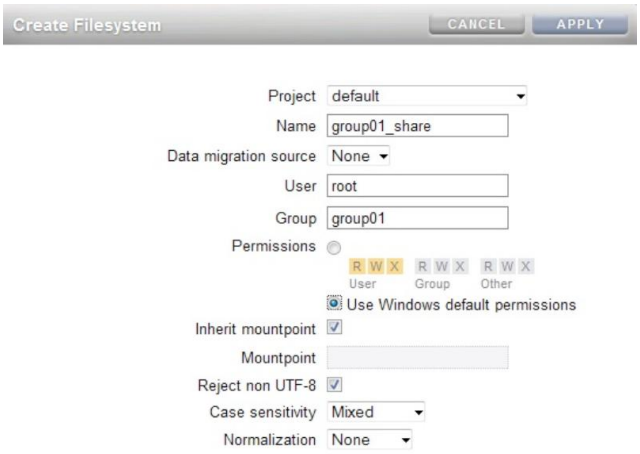

図 19:グループ共有の作成

グループ共有レベルのプロトコル設定の構成

共有をエクスポートするために SMB プロトコルをグループレベルで設定するには、次の手順を実行します（図 20 を参照）。

共有の「プロトコル」タブで、次の手順に従います。

- 「**Inherit from project**」チェックボックスをオフにします。
- 「**リソース名**」ボックスで、エントリ **off** をエントリ **on** に置き換えます。
- 「**適用**」ボタンをクリックします。

リソース名は、この共有を SMB クライアントで参照するときに使用される名前です。off に設定されたリソース名は、SMB クライアントで共有にアクセスできないことを示します。on に設定されたリソース名は、共有が `¥¥server¥<filesystem_name>` としてエクスポートされることを示します。共有名を手動で指定するには、***on*** または ***off*** でなく、カスタムリソース名を入力します。

アクセスベースの列挙が必要な場合は、「**Enable Access-based Enumeration**」オプションを選択して列挙を有効にします。アクセスベースの列挙では、クライアントの資格に基づいてディレクトリエントリをフィルタリングします。

クライアントに、ファイルまたはディレクトリへのアクセス権がないと、そのファイルは、クライアントに戻されるエントリの一覧から除外されます。このオプションは、デフォルトでは有効になりません。

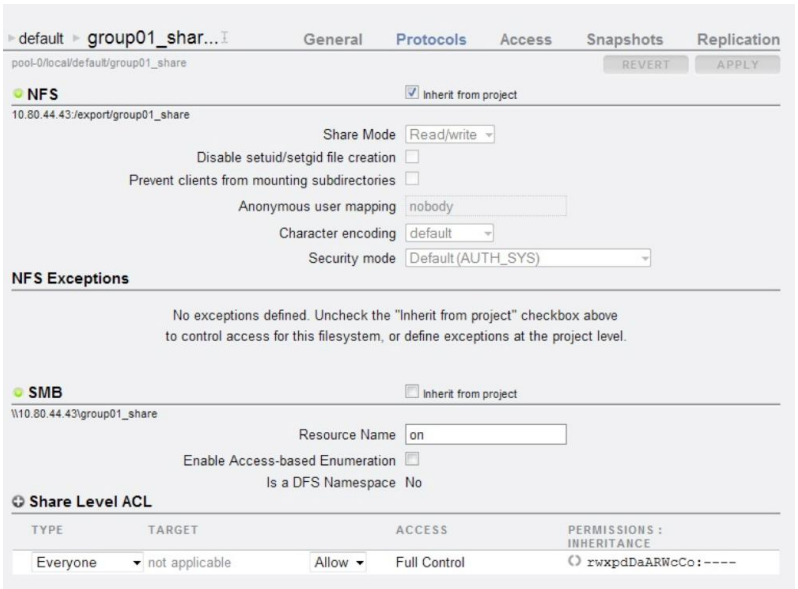

図 20:グループ共有レベル SMB プロトコル設定

グループ共有レベルのアクセス設定の構成

このセクションでは、共有の作成、共有へのグループの割り当て、共有レベルのプロトコル設定、アクセス設定の方法について説明します。

ルートディレクトリへのアクセス権は、その時点のアクセス許可に基づいて共有が作成されるときに (「ユーザー共有の作成」を参照)、設定されます。このセクションでは、Sun ZFS Storage Appliance Software Release 2010.Q3 および Software Release 2010.Q1 でのアクセス制御リスト (ACL) の継承動作について説明します。このセクションで示す例は、ドメイン全体ルールを使用してマップされたグループ *group01* に割り当てられている共有 *group01_share* に基づいています。

Software Release 2010.Q3 での ACL 動作

Software Release 2010.Q3 で ACL 動作を設定するには、次の手順に従います。

- 「**Inherit from project**」チェックボックスをオフにします。
- 「**ACL inheritance behavior**」ドロップダウンボックスで、図 21 のように「**Inherit all entries**」を選択します。「**Inherit all entries**」オプションを選択すると、継承可能なすべての ACL エントリが継承されます。このオプションは、ユーザーが新しいファイルを作成したときに、ファイルによって作成元のディレクトリツリーのアクセス権が継承されるように、ACL *passthrough* モードを設定します。管理者は、0664 や 0666 などの ACL 継承に使用されるアクセス権を設定します。
- 「**適用**」ボタンをクリックします。

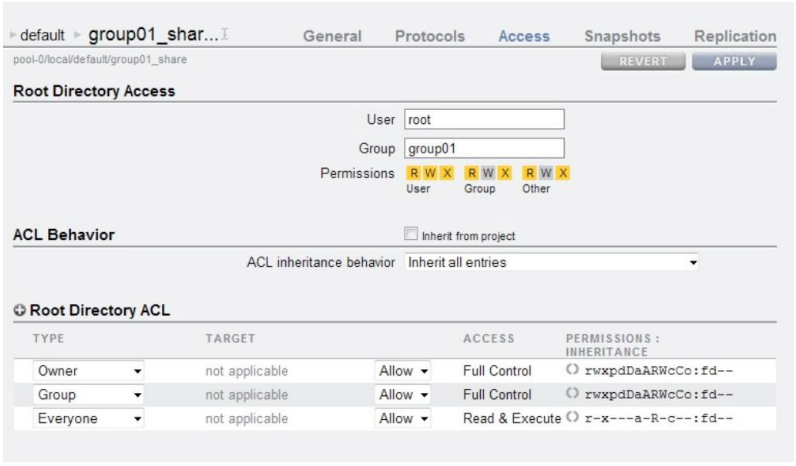

図 21:Software Release 2010.Q3 でのグループ共有レベルアクセス設定

ルートディレクトリ ACL は、選択された「**Use Windows default permissions**」オプションに基づいて共有が作成されるときに設定されます (図 19 を参照)。図 21 は、「所有者」、「グループ」、「Everyone」ごとに作成された 3 つの**許可**モードエントリを示しています。

エントリを削除するには、エントリにマウスを合わせてゴミ箱アイコンを選択します。

エントリを編集するには、エントリにマウスを合わせて編集用の鉛筆アイコンを選択します。

エントリを追加するには、「+」**アイコン**をクリックします。

変更後に「**適用**」ボタンをクリックします。

これはグループ共有なので、フルアクセス権をグループに付与できます。グループの**ルートディレクトリ ACL** を変更するには、次の手順に従います。

- マウスを ACL エントリに移動して、編集用の鉛筆アイコンを選択します。
- ACL エントリを**フル制御**に設定するには、図 22 のように「Edit ACL Entry」ページの上部にあるドロップダウンボックスから「Full Control」を選択します。
- 「**OK**」ボタンをクリックします。

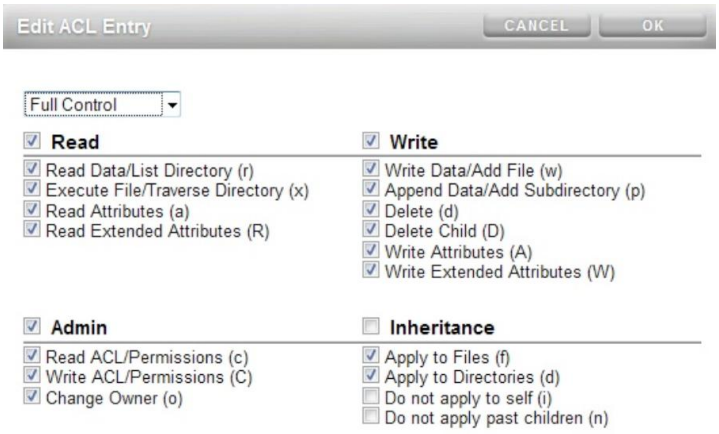

図 22:グループ ACL エントリの編集

Software Release 2010.Q1 での ACL 動作

Software Release 2010.Q1 で ACL 動作を設定するには、次の手順に従います。

- 図 23 のように、「**Inherit from project**」チェックボックスをオフにします。
- 「**ACL behavior on mode change**」ドロップダウンボックスで、「**Do not change ACL**」を選択して、アクセス権の変更操作が適用されるときに ACL エントリを保持します。
- 「**ACL inheritance behavior**」ドロップダウンボックスで、「**Inherit all entries**」を選択して、継承可能なすべての ACL エントリが継承されることを指定します。
- 「***適用***」ボタンをクリックします。

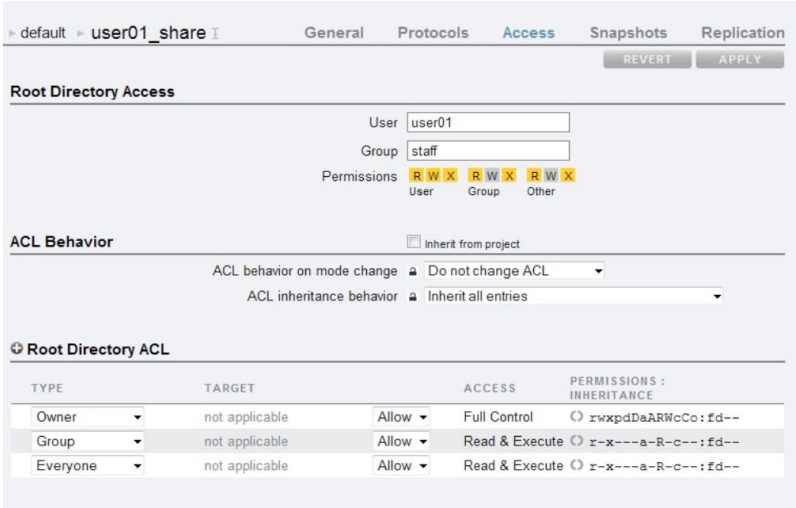

図 23:Software Release 2010.Q1 でのグループ共有レベルアクセス設定

ルートディレクトリ ACL は、選択された「**Use Windows default permissions**」オプションに基づいて共有が作成されるときに設定されます (図 19 を参照)。図 23 は、「所有者」、「グループ」、「Everyone」ごとに作成された 3 つの**許可**モードエントリを示しています。

エントリを削除するには、エントリにマウスを合わせてゴミ箱アイコンを選択します。

エントリを編集するには、エントリにマウスを合わせて編集用の鉛筆アイコンを選択します。

エントリを追加するには、「**+**」**アイコン**をクリックします。

変更後に「**適用**」ボタンをクリックします。

これはグループ共有なので、フルアクセス権をグループに付与できます。グループの**ルートディレクトリ ACL** を変更するには、次の手順に従います。

- マウスを ACL エントリに移動して、編集用の鉛筆アイコンを選択します。
- ACL エントリをフル制御に設定するには、図 24 のように「Edit ACL Entry」ページの上部にあるドロップダウンボックスから「**Full Control**」を選択します。
- 「**OK**」ボタンをクリックします。

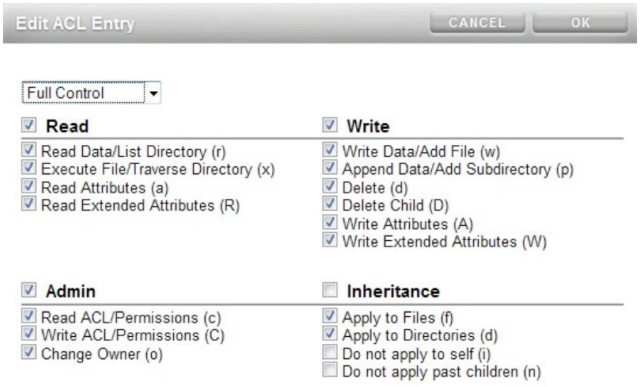

図 24:グループのルートディレクトリ ACL の編集

マップされたユーザーとグループの例

ユーザーマッピング

図 25 と図 26 は、2 人のユーザー、*ad-user*、*nis-user* による SMB および NFS を介した同じ共有へのシームレスなアクセスを示しています。この 2 人のユーザーは、「個々のユーザーまたはグループごとのルールベースマッピングの追加」セクションで説明したように相互にマップされています。

この例では、*ad-nis-user* 共有が Sun ZFS Storage Appliance 上に存在し、Windows クライアントと Solaris クライアントの両方にマップされるかその両方によってマウントされています。異なるプラットフォームに基づき、ユーザー *ad-user* は、`Windows` と呼ばれるディレクトリ、ユーザー *nis-user* は、`Solaris` と呼ばれるディレクトリを ad-nis-user 共有で作成しています。図 25 は、「セキュリティー」タブと「所有者」タブの詳細が両方のディレクトリで同一になることを示しています。

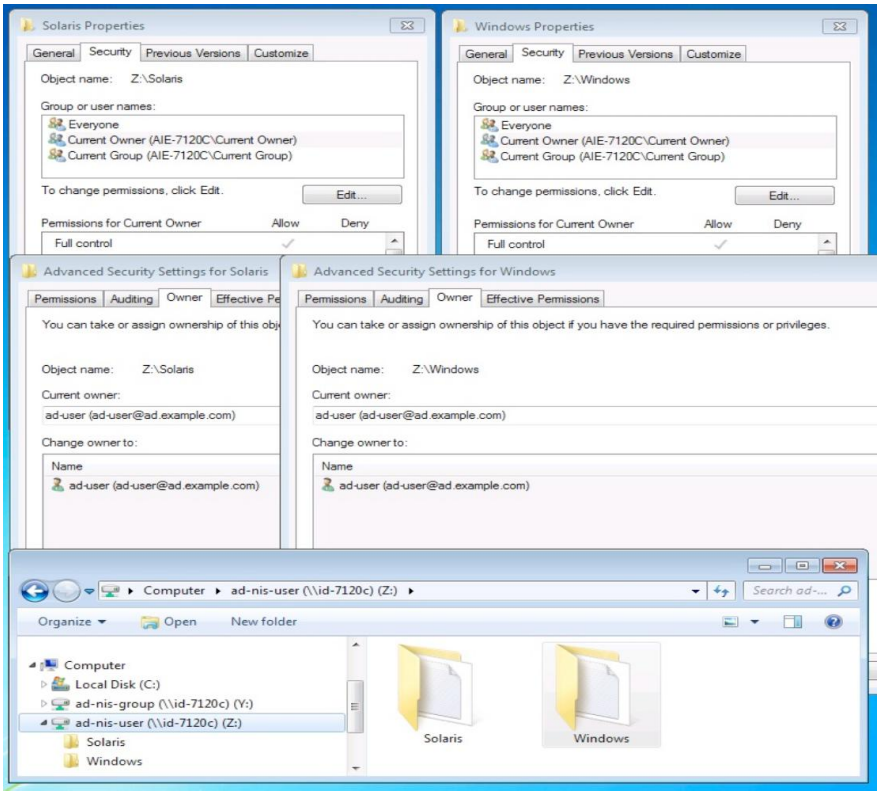

図 25:Windows でマップされたユーザーの例

図 26 には、Solaris クライアント用の *ad-nis-user* ディレクトリの端末出力が表示されています。この Solaris システムは、`nis.example.com` ドメインに属していて、ディレクトリ *ad-nis-user* は、ユーザー *nis-user* のホームディレクトリ (`/home/nis-user`) にマウントされています。`ls -lV` コマンドの出力には、このディレクトリリストのコンパクトな ACL 出力が表示され、両方のディレクトリが同一で、しかも 2 つの異なるプラットフォームから作成されたことがわかります。

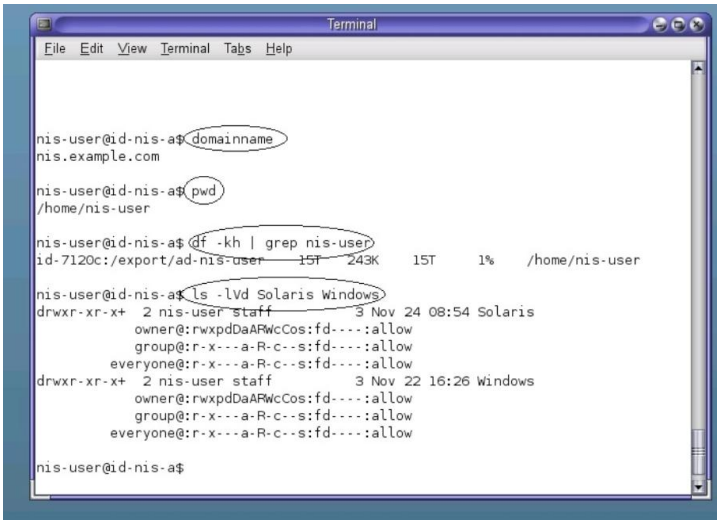

図 26:Solaris でマップされたユーザーの例

グループマッピング

図 27 と図 28 は、Windows システム上のグループ *ad-group* と Solaris システム上のグループ *nis-group* による、同じグループ共有へのシームレスなアクセスを示しています。この 2 つのグループは、「個々のユーザーまたはグループごとのルールベースマッピングの追加」セクションで説明したように相互にマップされています。この場合、Windows ディレクトリと Solaris ディレクトリは、*ad-nis-group* という名前のグループ共有で作成され、Windows システム上の *ad-group* および Solaris システム上の *nis-group* によってマウントされています。図 27 は、フルアクセス権 (フル制御) がこれらのグループ用の *ad-nis-group* グループ共有に付与されていることを示しています (「グループ共有レベルのアクセス設定の構成」セクションを参照)。

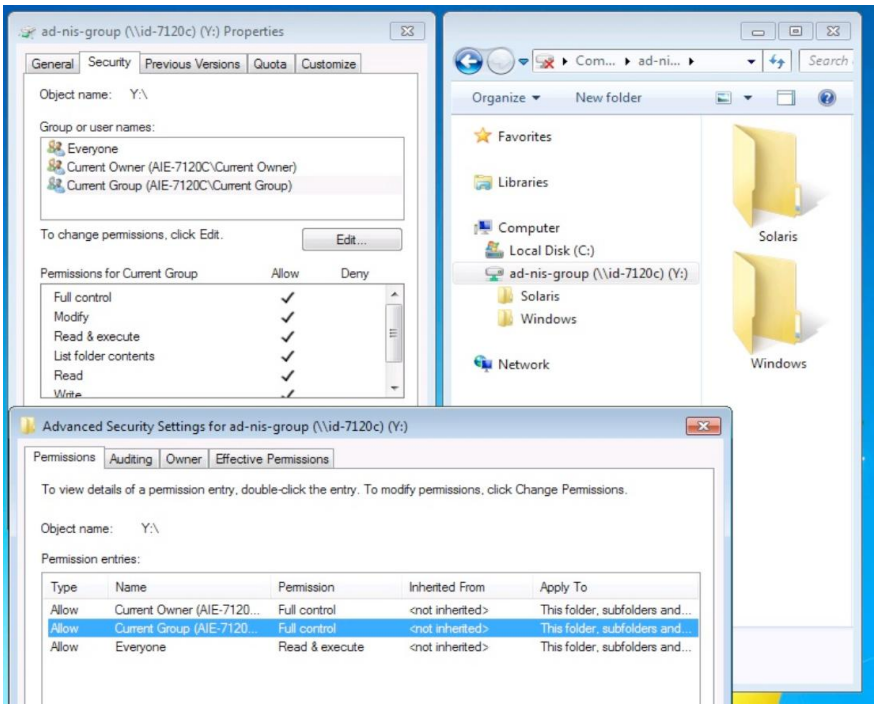

図 27:Windows でマップされたグループの例

図 28 には、Solaris クライアント用の *ad-nis-group* ディレクトリの端末出力が表示されています。この Solaris システムは `nis.example.com` ドメインに属し、ユーザー *nis-user* は、グループ *nis-users* に属しています。ディレクトリ `ad-nis-group` は、クライアントシステム上の Sun ZFS Storage Appliance から、`/mnt/ad-nis-group` にマウントされています。

`ls -lV` コマンドの出力には、`ad-nis-group` ディレクトリのコンパクトな ACL 出力が表示され、所有者が *ad-nis-group:* `root` で、nis-group がフル制御権を持つグループであることがわかります。`ls -lV` コマンドの出力には、`ad-nis-group` ディレクトリで Windows および Solaris クライアントによって作成された 2 つのディレクトリのコンパクトな ACL 出力が表示され、ここでも両方のディレクトリが同一で、マッピングがシームレスに行われていることがわかります。

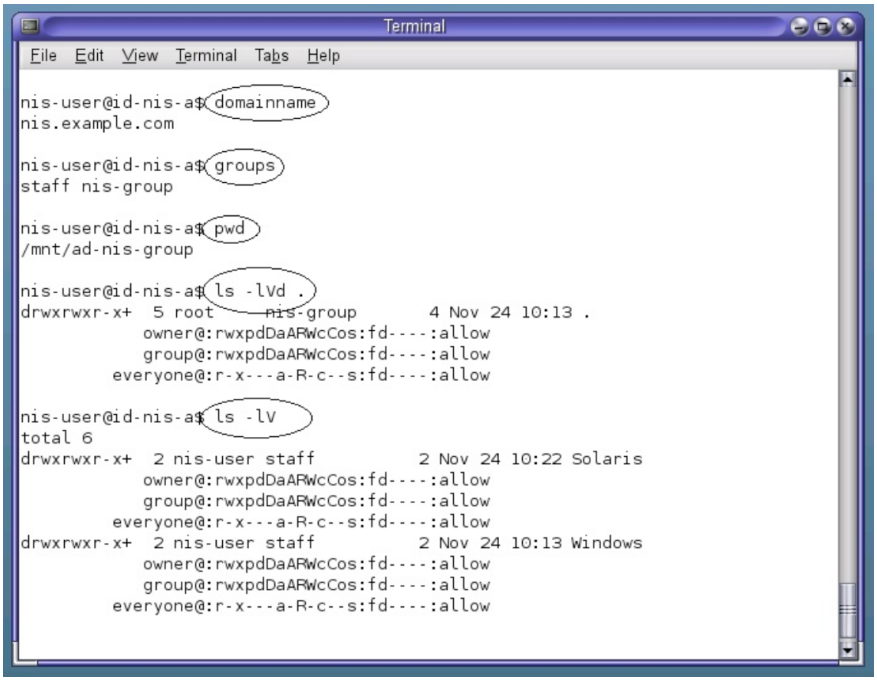

図 28:Solaris でマップされたグループの例

クイックトラブルシューティング Q&A

Q:アプライアンスを Active Directory ドメインに参加させることができない。

A1:アプライアンスの DNS 設定が適切で、DNS にアプライアンス用の DNS レコードが存在することを確認してください。

A2:Active Directory ドメインへの参加を試行しているユーザーにドメインの管理権限があることを確認してください。

A3:アプライアンスクロックがドメインコントローラクロックと同期していることを確認してください。

A4:「SMB サービスのトラブルシューティング」セクションで説明されている「LAN Manager Compatibility Level」設定が適切であることを確認してください。

A5:「NIS サービス」ページで NIS ドメインに指定したサーバーの IP アドレスを使用してください (「アプライアンスを NIS ドメインに参加させる」を参照)。

A6:Active Directory に参加させるアプライアンスでジャンボフレームを使用している場合は、Active Directory サーバーでも使用する必要があります。

Q:使用している SMB サービスはグリーン対応だが、クライアントから共有を表示できない。

A:プロジェクトまたは共有レベルで、ファイルシステム用の SMB リソース名が off に設定されていないことを確認してください。

「共有の構成と割り当て」セクションを参照してください。

Q:Solaris クライアント上に NFS 共有が表示されない。またはアプライアンスから削除した NFS 共有が表示される。

A1:Solaris オートマウンタまたは AutoFS サービスが更新されるまでに時間がかかる場合があります。

A2:クライアントとサーバーの NFSv4 アイデンティティドメインが同じであることを確認してください。

結論

Sun ZFS Storage Appliance 上のルールベースアイデンティティマッピングでは、Windows Active Directory と Solaris NIS ディレクトリサービス間で、ユーザーおよびグループアイデンティティを簡単にすばやくマップできます。Sun ZFS Storage Appliance の初期設定を完了し、Windows ドメインと NIS ドメインにユーザーおよびグループを配置したあとは、ワイルドカードを使用して、ドメイン全体マッピングルールを作成できます。またはアプライアンスインタフェースを使用してユーザーごとまたはグループごとのベースで行うこともできます。

関連資料

- Sun Unified Storage
- Solaris SMB/CIFS サービストラブルシューティング
- アラン・ライトの SMB/CIFS Solaris ブログ
- Sun ZFS Storage Appliance ソフトウェア
- Unified Storage For Dummies, Oracle Special Edition
- ZFS Storage Appliance リソースキット
- オラクルの Sun Unified Storage Simulator

Sun ZFS Storage Appliance Rule-based Identity Mapping Between Active Directory and NIS Implementation Guide
2011 年 2 月、バージョン 1.1
著者:Art Larkin

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

海外からのお問い合わせ窓口:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together