ORACLE

ZFS STORAGE APPLIANCE

Oracleホワイト・ペーパー
2014年11月

Oracle ZFS Storage ApplianceでLDAPソースとしてMicrosoft Active Directoryを使用する方法

ORACLE

目次

はじめに

Oracle ZFS Storage Applianceは、高度なハードウェアおよびソフトウェア・アーキテクチャを統合し、もっとも要求の厳しいワークロードを実行できる使いやすいマルチプロトコル・ストレージ・システムを提供します。これらのワークロードには、同時に実行されるさまざまなアプリケーションや高度なデータ・サービスが含まれます。SPC-1、SPC-2、SPECsfsといった業界標準ベンチマークの結果により、最高クラスのパフォーマンス特性が明らかにされています。

ユニファイド・ストレージ・プラットフォームとして、Oracle ZFS Storage Applianceは複数の環境で同時に稼働するように構成できます。これらの環境に完全に統合するには、その環境に適合したネーミング・システムに登録する必要があります。

Microsoft Windowsでは、通常、Active Directoryが使用されます。また、UNIX環境ではLDAPがもっとも一般的に利用されているディレクトリ・システムです。状況によっては、Active Directoryのみをディレクトリ・サービスとして展開して、Microsoft WindowsとUNIX環境の両方にサービスを提供することが望ましい場合があります。

このドキュメントでは、Active Directoryサービスを使用してLDAPサービスを提供し、IDマッピングで異なる環境の橋渡しをする方法を説明します。

ここでは、架空の'example.org'というActive Directoryドメインを使って説明します。

Active Directory LDAPサービス

Microsoft Active Directoryは、Microsoft Windows環境向けの業界標準のディレクトリ・サービスです。Active Directory（AD）は、認証で使用するKerberos、認可で使用するLightweight Directory Access Protocol（LDAP）、ホスト名の解決とサービスの検索で使用するディレクトリ・サービスとDomain Name System（DNS）を組み合わせて緊密に統合されています。ADを使用すると、ユーザー、グループ、共有、およびさまざまな種類の共有オブジェクトに関する情報を格納できます。

Oracle ZFS Storage Applianceは、直接ADと統合し、Microsoft Windows環境全体に一貫したセキュリティと所有権の詳細情報を提供します。ただし、ADは、標準のままではUNIX環境のIDを表現することはできません。UNIX環境では、IDは正の整数で表現されるユーザーID（UID）とグループID（GID）によって定義されます。ホーム・ディレクトリ、グループ・メンバーシップ、デフォルトのシェル、および暗号化されたパスワードなどの詳細情報も、デフォルトではADにはありません。一部の詳細情報（GECOSフィールドなど）は、標準のADの属性を利用できます。

設計上、ADはスキーマ変更によって拡張可能です。つまり、アプリケーションで必要な場合に、UIDやGIDの追加など、オブジェクトに属性を追加することにより、Windows ADドメイン・コントローラでUNIX環境のディレクトリ・アクセスを管理できます。

Windows Server 2012 R2までのWindows Serverのバージョンには、Microsoft Identity Mapping for UNIXをインストールすることで、UNIXホストへのNISディレクトリ・アクセスが可能となる機能があります。

UNIX LDAPディレクトリ・アクセスの標準は、RFC 2307にカプセル化されており、Microsoft Identity Mapping for UNIXをインストールすることで、ADスキーマを変更し、RFC 2307に準拠することができます。商用パッケージにも、RFC 2307準拠の機能を提供しているものが数多くあります。

Active DirectoryのLDAPサービスは、未加工のLDAPディレクトリへのアクセスを可能とするADSI Editのような標準のADツールを介する以外には、通常、その構造を明確には把握できません。AD構成が単純な標準設定とは異なる場合には、このようなツールを使用することで、ディレクトリ構造を確認できます。図1は、新しく作成したアクティブ・ドメインを"Active Directory Users and Computers"アプリケーションで表示した例を示しており、図2は、より構造化した"ADSI Edit"で表示しています。

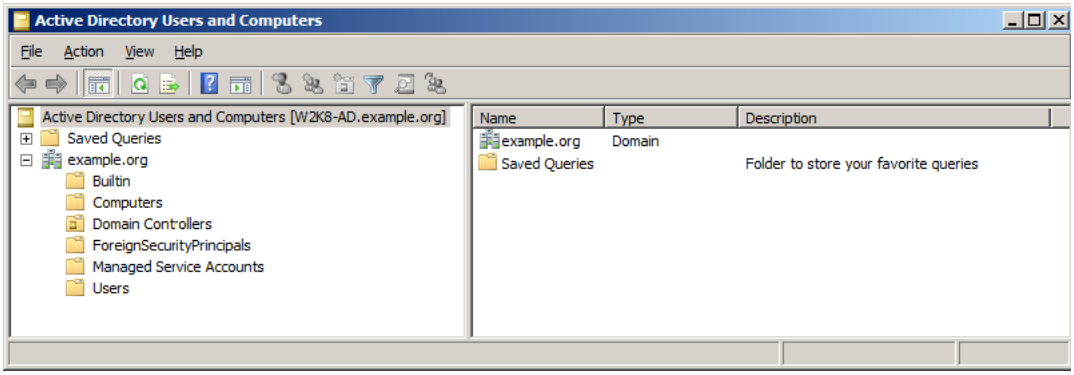


図1.新しく作成したドメインのActive Directory Users and Computersビュー

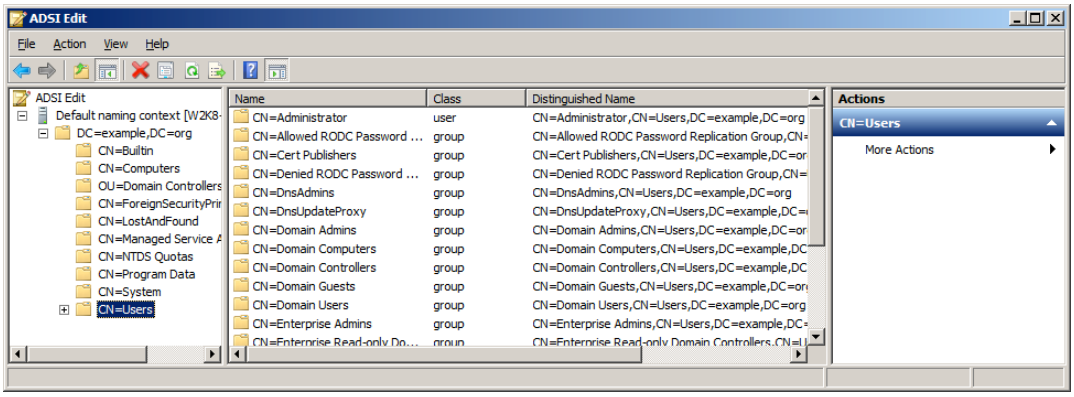


図2.新しく作成したドメインのADSI Editビュー

ADSI Editのビューでは、さらに多くのLDAP構造をADスキーマに表示します。

この他にも、商用、フリーウェアを問わずLDAPブラウザはありますが、ADSI EditはWindows Server AD Serverデプロイメントにデフォルトでインストールされるため、この例で使用しています。

Active Directoryユーザーとコンピューター内でUNIX属性を有効にするには、IDMU NIS移行ウィザードで空のテキスト・ファイルをインポートして、空白のNIS構成を作成する必要があります。Oracle ZFS Storage ApplianceでのMicrosoft IDMUの使用方法を説明したチュートリアルは、以下で入手できます。

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-051-zffsa-idmu-mapping-405716.pdf

ADへのアクセスのためのOracle ZFS Storage Applianceの構成

適切な認証オブジェクトとアクセス権を作成するには、ADにアクセスするようOracle ZFS Storage Applianceを構成する必要があります。前述のとおり、DNSサービスはADで大きな役割を果たします。したがって、Windows DNSサービスを使用するようOracle ZFS Storage Applianceを構成する必要があります。

時刻の同期も、ADを正しく操作するために重要です。Oracle ZFS Storage ApplianceとADドメイン・コントローラの時刻の差は、ADへの参加を正常に行うために15分未満にする必要があります。Network Time Protocol（NTP）サービスをインストールし、Oracle ZFS Storage ApplianceとADドメイン・コントローラがNTPサービスのクライアントになるよう構成することを強く推奨します。

1. Oracle ZFS Storage Applianceのブラウザ・ユーザー・インタフェース（BUI）を使用して、DNS構成がActive Directoryサーバーと同じDNSサーバーを参照していることを確認します。次の図のように、「**Configuration**」→「**Services**」→「**DNS**」を選択してDNS構成画面にアクセスします。

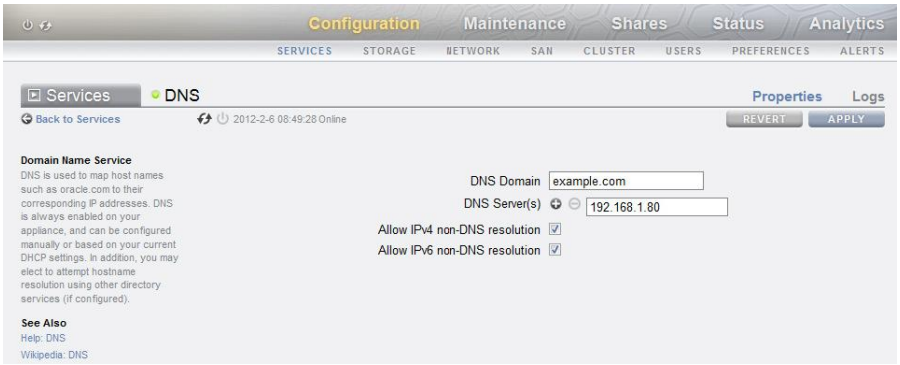


図3. DNS構成の確認

2. Oracle ZFS Storage ApplianceとWindows ADドメイン・コントローラの時計が同期していることを確認します。

   BUIで、「**Configuration**」→「**Services**」→「**NTP**」を選択します。NTP Serverのアドレスの詳細情報に適切な値を入力します。

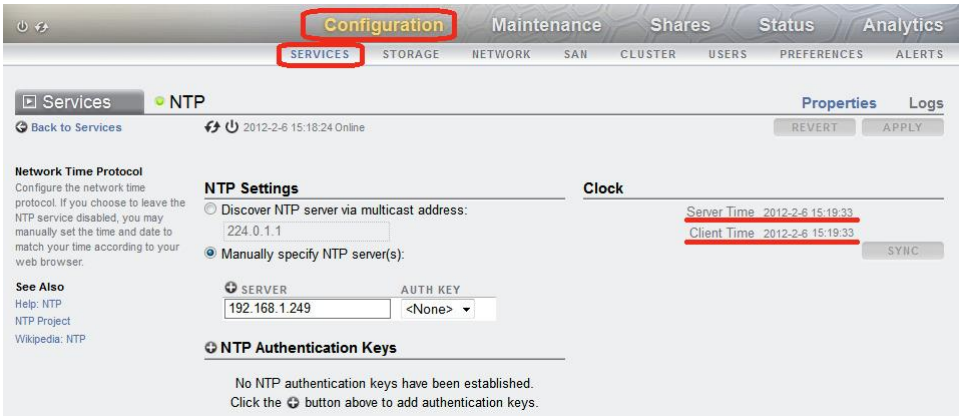


図4. 時計の同期の確認

3. 次の図のように、「Configuration」→「Services」→「Active Directory」ページで、「Join Domain」ボタンをクリックします。

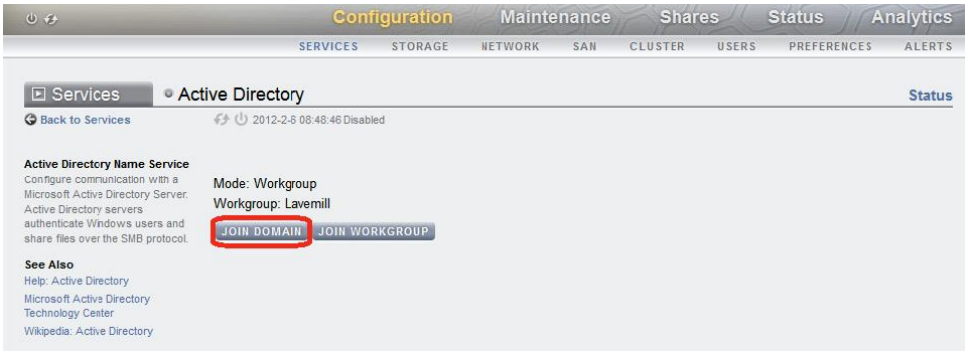


図5. Active Directoryサービス・ページ

4. 図6のように、Oracle ZFS Storage ApplianceをADに参加させる権限を持つドメイン管理者の詳細情報を入力します。「APPLY」をクリックして続行します。

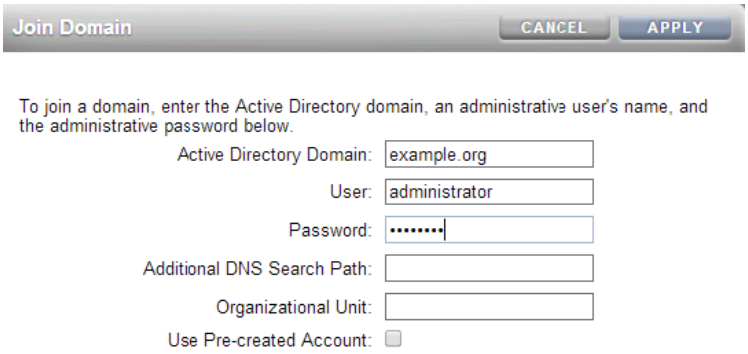


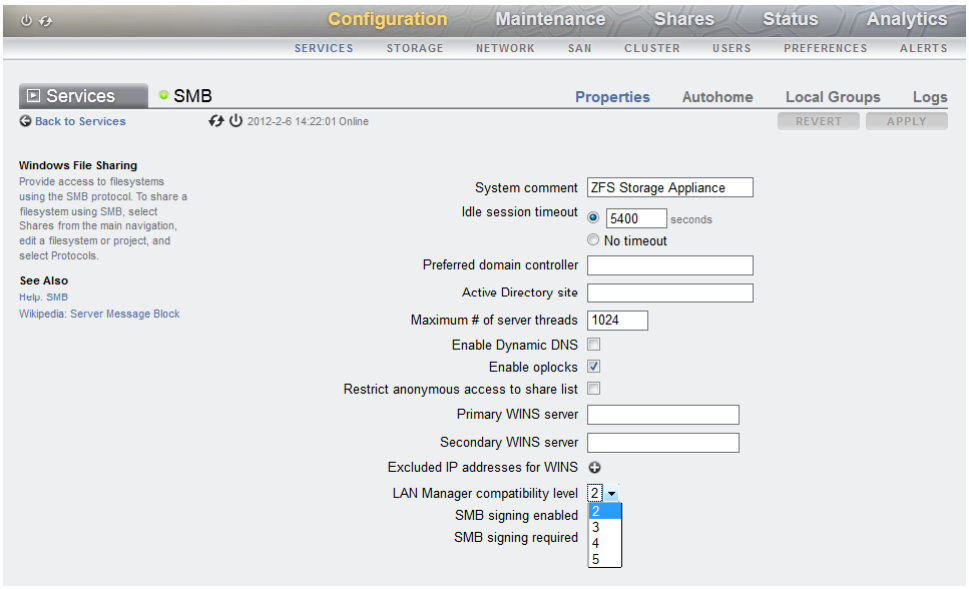
図6. AD管理者の詳細情報を入力します

5. 参加の操作が正常に行われると、次のような承認が表示されます。

図7. ADへの正常な参加

ADドメイン管理者のユーザー名とパスワードが正しいのに'アクセスが拒否された'ことを示すメッセージが表示される場合は、LAN Managerの互換性レベルをレベル2に変更する必要があります。

これを行うには、「Configuration」→「Services」→「SMB」を選択し、図8に示すように、プロパティの一番下にあるドロップダウンからレベルを選択します。次に、手順3に戻って、ドメインへの参加プロセスを繰り返すことができます。



これで、Oracle ZFS Storage Applianceでは、Active DirectoryからWindows環境のユーザーとグループを解決できるようになりました。さらに、Oracle ZFS Storage Applianceから、LDAPインタフェースを介してADにアクセスするために必要なアクセス権が設定されました。

LDAPへのアクセスのためのOracle ZFS Storage Applianceの構成

例として使用するADドメイン`example.com`は、LDAPインタフェース内では、識別名（DN）`DC=example,DC=org`で表されています。このDNは、検索ベースとして使用されます。

Oracle ZFS Storage Appliance LDAPクライアントを構成するには、**「Configuration」→「Services」→「LDAP」**に移動します。Base search DNに、次の形式で入力します（この例では、`DC=example,DC=org`）。

サブツリー（再帰的）検索を有効にして、LDAPクライアントにより、ADに構築されている適切なツリー構造を下に移動して検索できるようにします。

ADにプロキシ・ユーザーを作成し、Oracle ZFS Storage ApplianceからLDAPへのアクセスを可能にします。ただし、LDAPへのアクセスを可能にするようADを構成した前のセクションの例のように、バインド資格証明レベルを'Self'にすることができます。これにより、プロキシ・ユーザーのDNとパスワードの格納が不要になります。

次に、ADドメイン・コントローラをサーバーとして追加する必要があります。次の例では、w2k8-adおよびw2k8-ad2という2つのADドメイン・コントローラが指定されています。

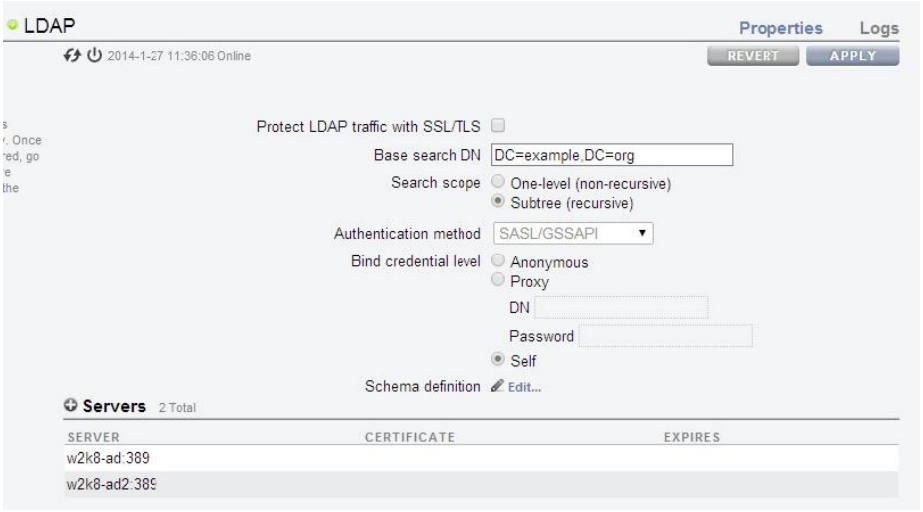


図9.LDAPクライアント・インタフェースの構成

次の手順では、スキーマ定義を行います。

設計上、Windowsユーザーとグループは同じネームスペースを共有します。したがって、同じ名前のユーザーやグループを持つことはできません。デフォルトでは、これらのオブジェクトは'Users'コンテナに存在します。このコンテナは、ADでは`CN=Users,<BASE-DN>`で表されます。この例では、コンテナは`CN=Users,DC=example,DC=org`です。このDNは、スキーマ定義でユーザー検索記述子として使用されます。

ただし、UNIX環境では、ユーザーとグループの定義には別のネームスペースがあるため、ユーザーと同じ名前でグループを作成できます。この違いに対応するため、グループ検索記述子はユーザー検索記述子と同じに設定する必要があります。

いったんIDMUがドメイン・コントローラにインストールされると、uidNumber属性およびgidNumber属性がADに定義されて、マッピングを行う必要はありません。その他の属性には、UNIX環境に必要な名前とは少し異なる名前が付けられます。

次に、推奨するマッピングの一覧を示します。

ユーザー属性	対応するADのユーザー属性
gecos	CN
homeDirectory	unixHomeDirectory
userPassword	unixUserPassword
uid	sAMAccountName

これらのマッピングを行うには、UNIXオブジェクト・クラスposixAccountをADオブジェクト・クラスUserにマップする必要があります。グループへのアクセスの場合も同様に、UNIXオブジェクト・クラスposixGroupは、ADオブジェクト・クラス'group'に、検索記述子にユーザー記述子と同じものを設定してマップする必要があります（ADが共有ネームスペースを利用するためです）。

Oracle ZFS Storage Appliance BUIでこれらの変更を実行するには、**「Configuration」→「Services」→「LDAP」**（図9を参照）に移動して、Schema definition行の右にある「Edit…」を選択します。これにより、図10に示す'Edit LDAP Schema Definition'ダイアログ・ウィンドウが表示されます。

以下を入力します。

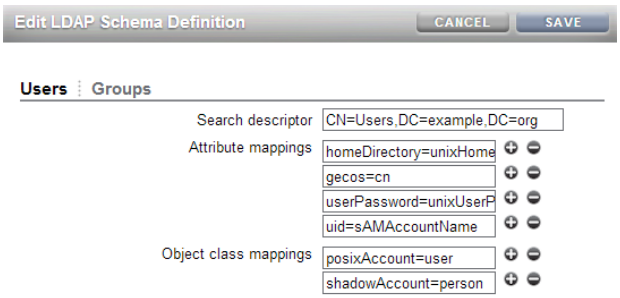


図10.Edit LDAP Schema Definition - Users

1. 適切な検索記述子を入力します。例で示しているのは、

   CN=Users,DC=example,DC=orgです。

   推奨するマッピングを使用するか、使用している独自のADスキーマで決定したマッピングからgecos、homeDirectory、userPasswordおよびuidの属性マッピングを追加します。「+」アイコンをクリックして、追加の属性マッピングがあれば追加します。

2. posixAccountおよびshadowAccountのオブジェクト・クラス・マッピングを入力します。スキーマ・マップは一意にする必要があるため、後者はposixAccountとは異なる必要があります。最終的には、人へのマッピングでも同様です。

3. 「Group」タブをダイアログ・ボックスの左上から選択し、手順1と同じ検索記述子を入力します。

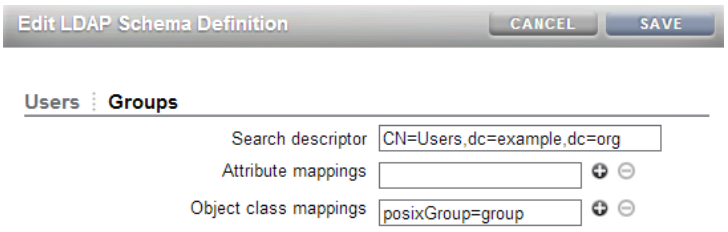


図11.Edit LDAP Schema Definition - Groups

4. posixGroupのオブジェクト・クラス・マッピングを入力し、「**Save**」をクリックします。

想定される動作の確認

これらのスキーマ定義の変更を行ったら、WindowsとUNIX環境との間で所有権とアクセス権の整合性が保たれるよう、想定したとおりにマッピングが行われることを確認します。

注：正しいマッピングをテストするには、UNIX属性を構成したユーザーを1つ以上ADに定義する必要があります。同様に、ユーザーのUNIX属性を定義する前に、UNIX属性を構成したセキュリティ・グループをADに定義しておく必要があります。

たとえば、ADにunixusersと定義したグループには、gid10000を割り当てておきます。ADにandrewと定義したユーザーには、uid70592を割り当て、そのプライマリ・グループにunixusersを定義します。

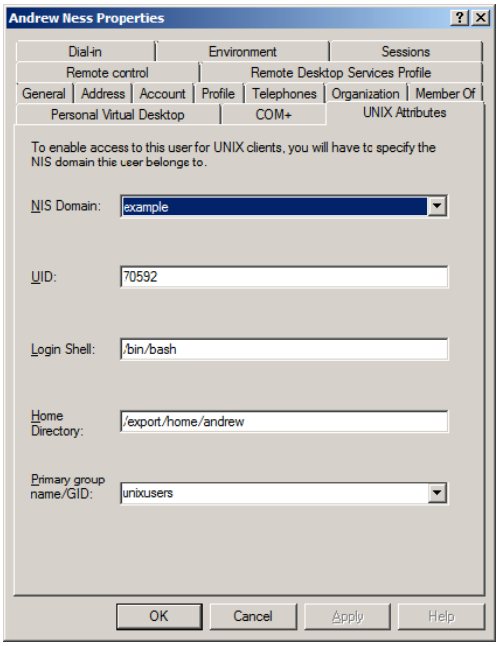


図12.'andrew'のUNIX属性

ADには、sharonという名前の別のユーザーも定義しました。このユーザーにはUNIX属性は定義されていません。

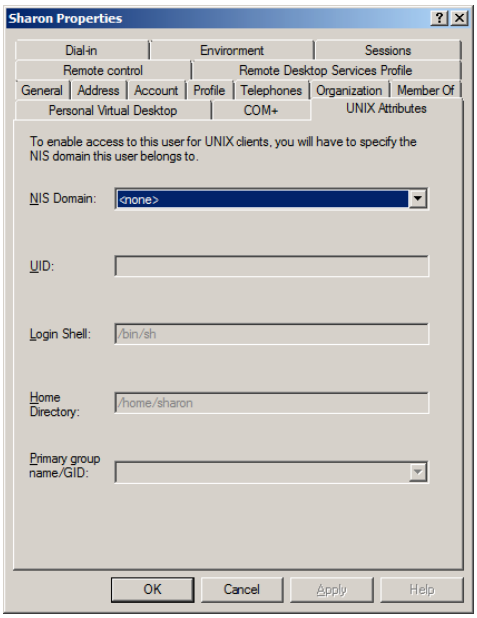


図13. sharonに対するUNIX属性は定義されていない

Oracle ZFS Storage Appliance BUIから、「**Configuration**」→「**Services**」→「**Identity Mapping**」に移動します。マッピング・モードが**IDMU**に設定されていることを確認します。必要に応じて変更し、変更を「**APPLY**」します。

「**Mappings**」を選択します。Mappings画面で、Identityにandrewと入力して、Windows Domainはデフォルトのままにします。「**SHOW**」ボタンをクリックします。

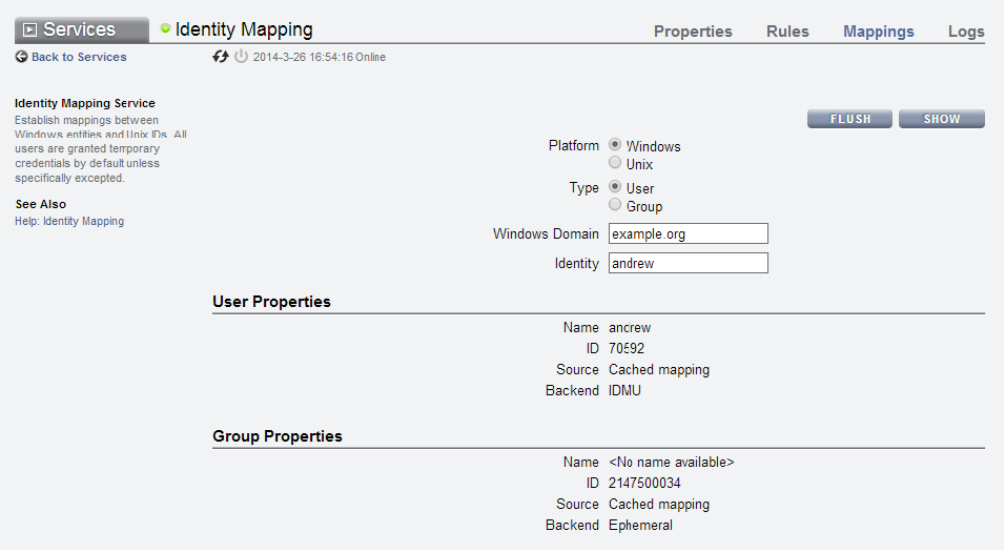


図14. andrewのマッピング詳細情報の確認 – 1

図14で確認できるとおり、ユーザーandrewには正しいユーザーID（70592）が設定されています。ここでは、andrewというグループがないので一時IDが生成されますが、そのIDは使用されないため、グループのプロパティは無視できます。

Platformで「Unix」を選択すると、Windows IDが正しく表示されます。ここでは、グループは表示されません。

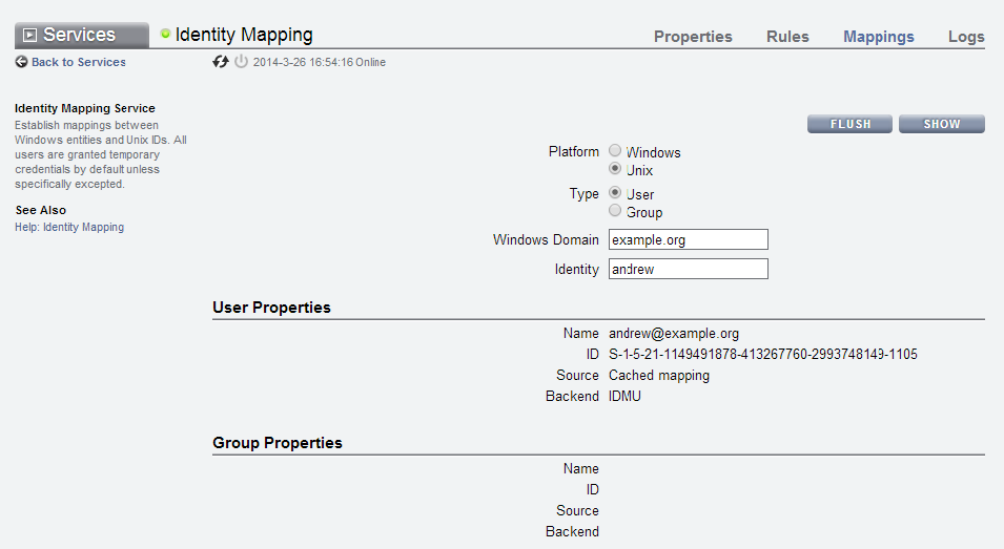


図15. andrewのマッピング詳細情報の確認 – 2

Typeで「Group」を選択し、`unixusers`を入力した場合も同様の結果が表示されます。

`sharon`の詳細情報を検索すると、Windowsの詳細情報は表示されません。これは、一時UIDが自動的に生成されても、WindowsユーザーIDを一時UNIXユーザーIDと永続的にマップする方法がないためです（図16および17）。

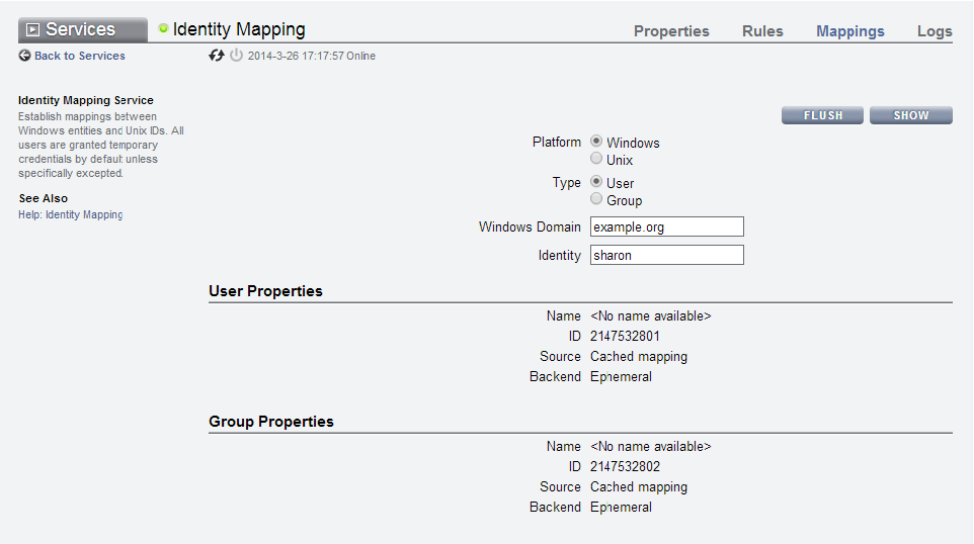


図16. sharonに対して作成された一時ID

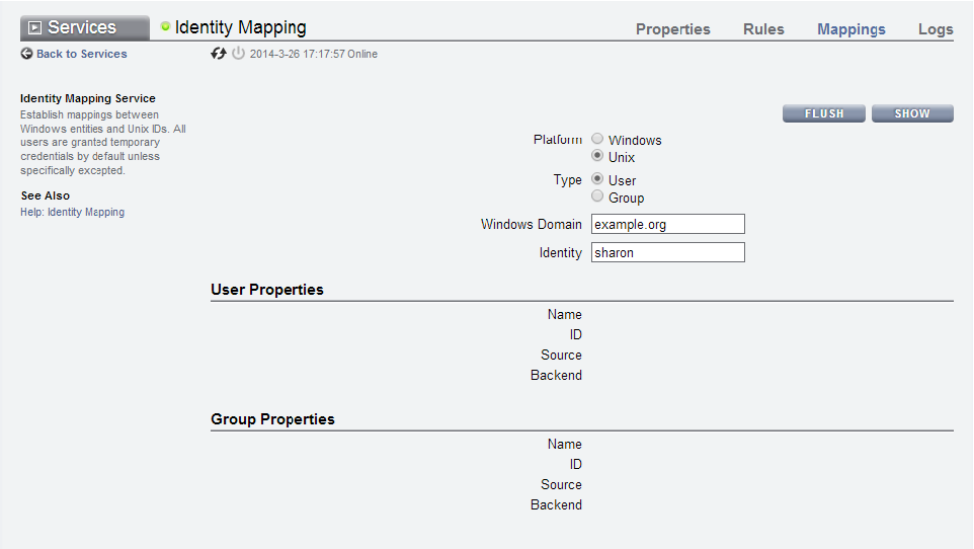


図17. sharonのWindowsユーザーIDは表示されない

ユーザーsharonに対してUNIXとWindows環境の間のマッピングを指定するには、Active Directory Users and Computersウィザードで、UNIX属性を入力する必要があります。この例では、sharonのUNIX UIDは70593で、グループunixusersに割り当てられています。

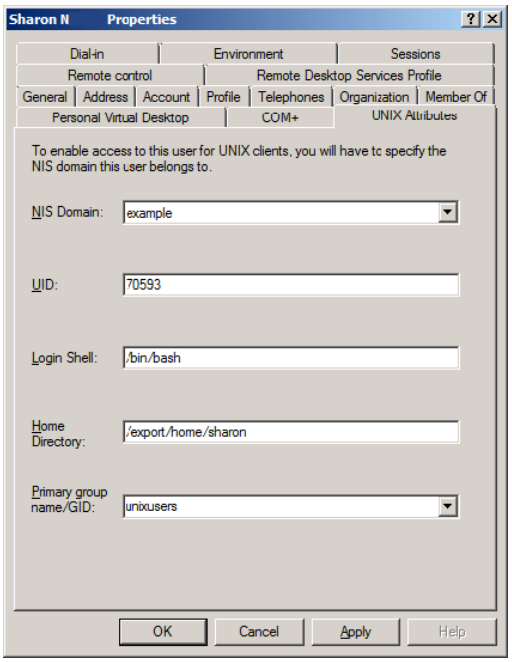


図18. UNIX環境へのsharonの追加

変更を適用した後、マッピング・テストを再実行すると、図19と図20のように、想定した結果が表示されます。

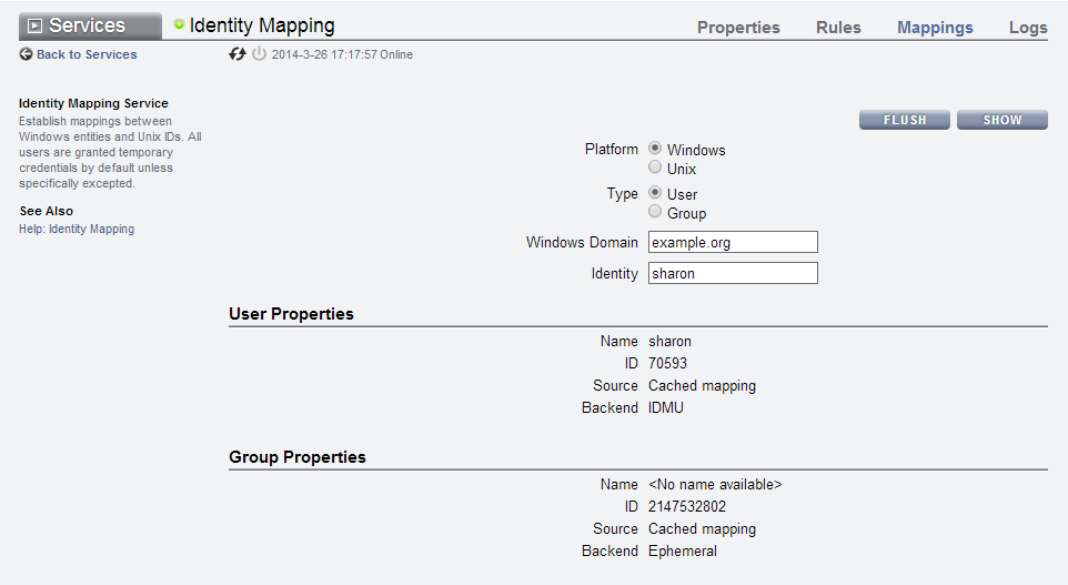


図19. sharonに新しく適用されたUID

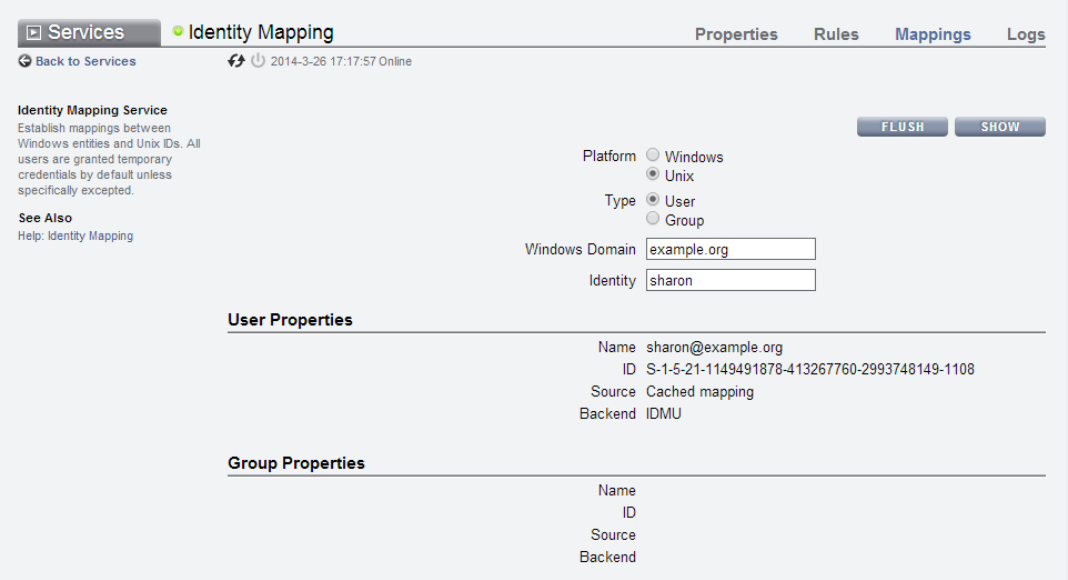


図20. sharonに新しく適用されたWindows ID

複雑なADのディレクトリ構造

大規模で複雑なADスキーマが展開されている場合、Windows AD管理者は、地域や職務、またはその両方で分割したユーザー階層を採用しなければならないことがあります。状況によっては検索を1つまたはいくつかのサブツリーに制限して、最適なID解決スピードを実現するために検索範囲を制限することが望ましい場合もあります。

説明のために、仮に、example.orgに20,000を超えるアクティブADユーザーが定義されていて、複数の国に分布しているとします。階層を管理しやすくするために、AD管理者は地域別にツリーを配置しています。ユーザーに焦点を当てたこのツリーのサブセットを、図21に示します。

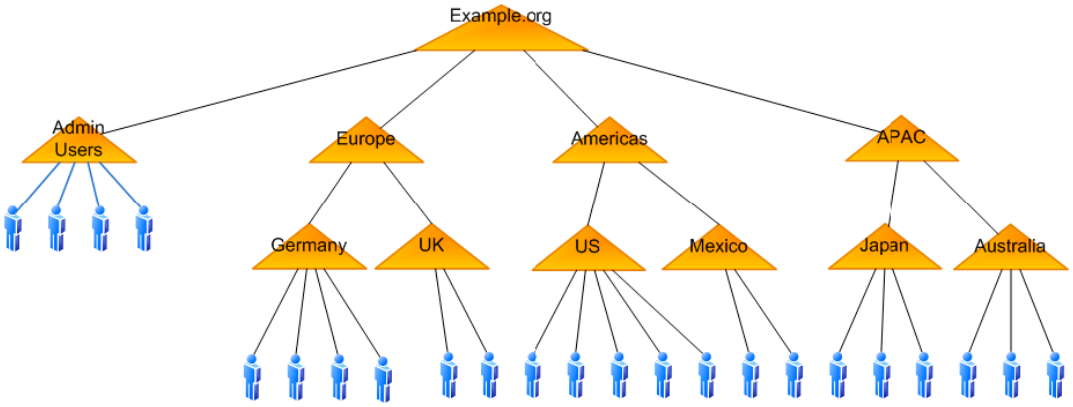


図21. Example.ORGの階層

検索パフォーマンスを最大化するために、ストレージ管理者は、検索を地域と管理者ユーザーのサブツリーだけに制限することにしました。

ユーザーはその国の組織単位（OU:Organizational Units）に存在し、ユーザーが属する国は地域のOUに含まれています。個別にAdminUsers OUも作成して、地域のユーザーに対する影響、または地域のユーザーからの影響を発生させることなく、所属するユーザーにグループ・ポリシーを適用可能にしました。

ルート・ドメイン以外に共通のノードがなく、パフォーマンス上の理由からユーザーがツリー全体を検索することは推奨できないため、Oracle ZFS Storage Applianceでは、代替の手法を用意しています。その手法では、DNをセミコロンで区切ることで、複数のサブツリーを指定して検索することができます。

"単純な"例では、ユーザー検索記述子は、CN=Users,DC=example,DC=orgでした。追加の検索機能を使用すると、この複雑な構成におけるユーザー検索記述子は次のようになります。

```
OU=AdminUsers,DC=example,DC=org; OU=Americas,DC=example,DC=org;      ¥
OU=APAC,DC=example,DC=org; OU=Europe,DC=example,DC=org
```

Oracle ZFS Storage Applianceにより、参照が解決されるよう、これらのサブツリーが1つずつ順番に検索されます。よって、Oracle ZFS Storage Applianceが配置されている拠点、およびOracle ZFS Storage Applianceが提供するサービスをもっとも利用しているユーザー・ベースに従ってOUの順序を変更するのが適切な場合があります。

さらに、グループが同じような方法で配置されている場合、グループ検索記述子も変更する必要があります。つまり、各地域のOUで管理している場合、または個別のOUを作成してADにセキュリティ・グループを保持している場合には、職務単位の割当ては、地域ではなくグローバルな視点で定義されている可能性があります。

`example.org`ドメインでは、図22と23にそれぞれ示すように、3つのユーザーがUS OUに、5つのユーザーがUK OUに存在しています。

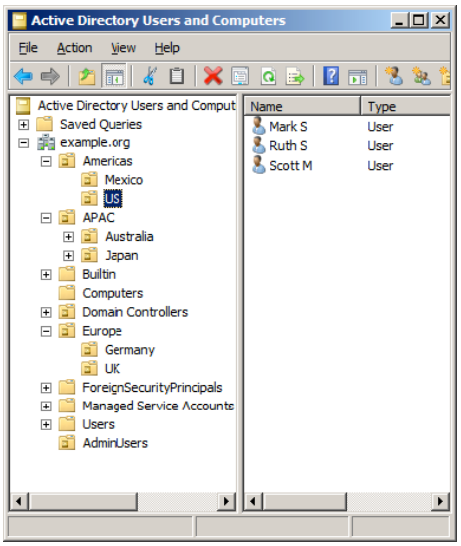


図22. US OUのユーザー

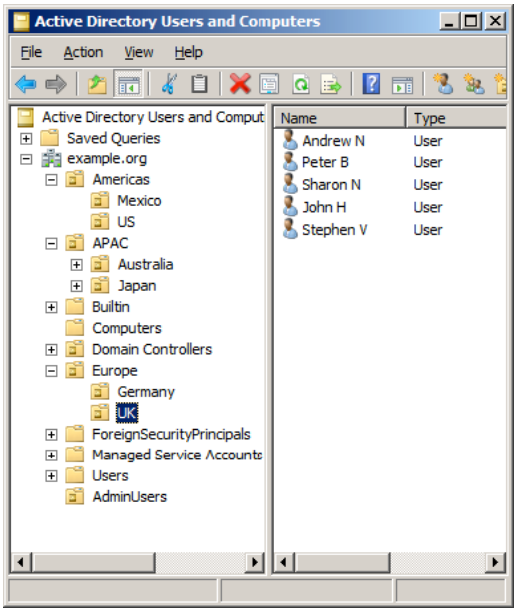


図23. UK OUのユーザー

この構成のADSI Editのビューを図24に示します。

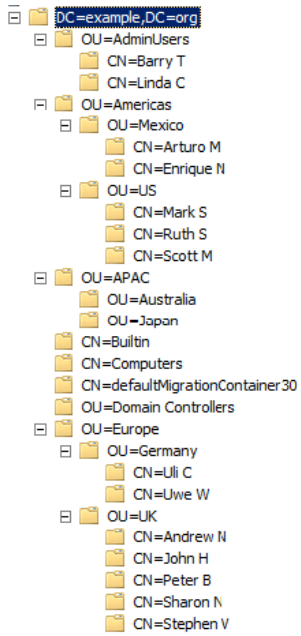


図24. ADSI Editのビュー

地域の単位と管理者ユーザーを取得するよう、ユーザー検索記述子を適切に設定しておくと、IMDUによって、指定したいずれかのサブツリーから解決とマッピングを行うことができます。

以下の図で、この例をいくつか示します。

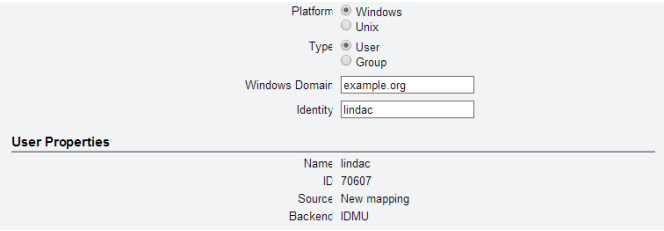


図25. AdminUsersからの解決

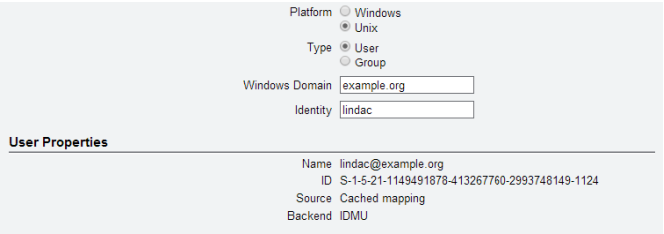


図26. AdminUsersからの解決

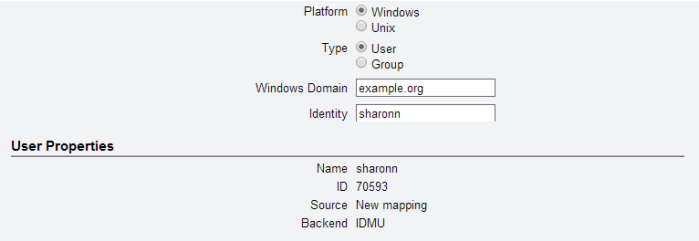


図27. UKからの解決

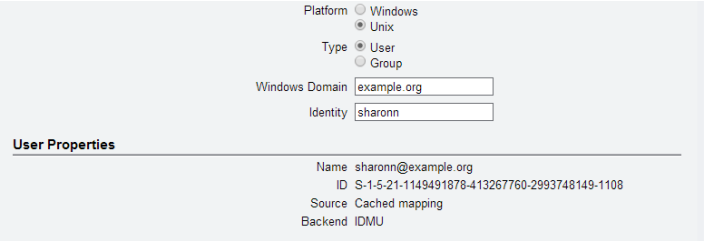


図28. UKからの解決

結論

Oracle ZFS Storage Applianceは、整合性を保ちながら安全にWindowsとUNIX環境の橋渡しをするプラットフォームを提供します。一方の環境で許可されたアクセス認可は、適切なマッピングが利用できるもう一方の環境にミラー化されます。

検索記述子を調整できる柔軟性を実現することで、単純な、または極めて複雑なActive Directoryスキーマを、整合性を保ちながら容易に処理できます。

LDAPインタフェースを提供するIDマッピング機能により、まったく異なる2つの環境を統合し、データの共有と、他の環境では使用できない余剰ストレージを含むストレージ・アイランドの削減が可能となります。

ORACLE

Oracle ZFS Storage Appliance で
LDAP ソースとして Microsoft Active
Directory を使用する方法

2014年11月、バージョン1.0
著者：Andrew Ness

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

Hardware and Software, Engineered to Work Together