



Oracleテクニカル・ホワイト・ペーパー
2014年1月、バージョン2.1

Microsoft Serverと Oracle ZFS Storage Applianceの統合

SMB展開の実装ガイド

概要	3
概要	エラー! ブックマークが定義されていません。
前提条件	5
オペレーティング・システムの前提条件	5
ストレージ・システムの前提条件	5
Oracle ZFS Storage Applianceを使用したシステム構成の ベスト・プラクティスと原則 ...	7
ネットワーク	7
Oracle ZFS Storage Applianceのクラスタ	7
Microsoft Cluster Service (MSCS)	7
ユーザー	7
構成全体への原則の実装	8
システムの構成	8
Network Time Protocol (NTP) サーバーに同期させる	8
ワークグループ・アクセス用のローカル・ユーザーを作成する	12
Active Directoryで使用されているDomain Name Service (DNS) サーバーに接続する	13
Active Directoryで認証するように構成する	15
サービスの構成	18
SMBサービス・プロトコルを選択する	18
シェアを作成する - プロジェクトとファイル・システム	19
シェアの構成	23
シェアのACLをワークグループ・モードで構成する	30
シェアのACLをドメイン・モードで構成する	31
Windows Server 2008 R2でのシェア管理	36
Active Directoryへのシェアの公開	38
データの移行	40
DFSターゲット	40
スナップショット	43
Analytics	46
結論	50
参考資料	51

概要

Oracle ZFS Storage Applianceは、Microsoft Serverの主要なツールおよびユーティリティと統合された環境で動作するように設計されています。このドキュメントでは、既存のWindows Server環境で使用するための推奨項目を構築方法について説明します。

Active Directoryドメイン・コントローラでの最初の登録操作から、シェアをActive Directoryに公開して分散ファイル・システム (DFS) ターゲットとして構成する操作まで、一般的な構成とタスクについて例を示しながら説明します。

ここで説明している情報を理解するためには、Windows Server環境の基礎知識を持っており、またIP、ネットマスク、ゲートウェイなどのネットワーク設定でOracle ZFS Storage Applianceの初期設定が済み、ストレージ・プールが構成され、アプライアンスとクライアント・マシン (NTP) の間で時刻が同期される必要があります。

はじめに

Oracle ZFS Storage Applianceシリーズでは、Active Directoryデータベースやワークグループモードのアプライアンスのローカル・ユーザーを使用してサーバー・メッセージ・ブロック (SMB) (または、コモン・インターネット・ファイル・システム (CIFS)) の認証を行います。このActive Directoryサービスを使用して、ユーザー、グループ、シェア、その他の共有オブジェクトの情報が格納されているMicrosoft Active Directoryデータベースにアクセスします。これに対して、LDAPではWindowsユーザーを格納することはできません。

リソースをActive Directoryにメンバーとして追加したら、このリリースをドメイン内で検出できるようになります。Active Directoryはコンテナ単位または組織単位 (OU) で動作します。管理上の目的で、リソースを複数の異なるOUに分けることができます。管理タスクはOU内で実行できます。

Oracle ZFS Storage Applianceをドメインに参加させると、参加プロセスで、このアプライアンスの名前が付いたコンピュータ・アカウント・オブジェクトがAD内に作成されます。

このドキュメントでは、ファイル・システムをドメイン・モードとワークグループ・モードの両方で作成および共有し、ドメインに参加し、ドメイン内にSMB共有をマウントし、オブジェクトの権限を管理するプロセスについて説明します。

このドキュメントに目を通すと、次のことを行えるようになります。

- Active Directoryメンバーシップを取得するための前提条件をリストアップする
- ローカル・ユーザーをSMB共有に使用する
- Oracle ZFS Storage ApplianceをActive Directoryドメインに参加させる
- ローカル・ユーザーとActive Directoryユーザーの両方にシェアのアクセス許可を設定する
- DFSターゲットを設定する
- シェアをActive Directoryに公開する
- 提供されている基本的な分析機能を理解する

注：Sun ZFS Storage Appliance、Sun ZFS Storage 7000、ZFS Storage Applianceへの参照はすべて同じOracle ZFS Storage Appliance製品を参照します。引用した画面のコードやドキュメントの中には、従来の命名規則を使用しているものがあります。

前提条件

このドキュメントで説明されている手順を適切に実行するためには、次の前提条件を満たしている必要があります。

オペレーティング・システムの前提条件

次のドメイン・コントローラが現在サポートされています。

- Microsoft Windows Server 2000 SP4
- Windows Server 2003 (または2003 R2)
- Windows Server 2008 (または2008 R2)

Windows NT 4.0ドメイン・コントローラは現在サポートされていません。

このドキュメントの手順は、Microsoft Windows Server 2003以降を使ってActive Directoryドメインを実装するためのものです。

クライアント、サーバー、ドメイン・コントローラ、およびアプライアンスの時刻がすべて同期されていることが重要です (“構成全体への原則の実装”の“Network Time Protocol (NTP) サーバーに同期させる”を参照してください)。

ストレージ・システムの前提条件

最新バージョンのOracle ZFS Storage Applianceソフトウェアがインストールされていることを確認します。最新バージョンのソフトウェアをダウンロードするには、オラクルのWebサイト“My Oracle Support”にアクセスして、“Patches & Updates”セクションに移動します。検索文字列“Sun ZFS Storage Appliance”を使用して、ドロップダウン・ボックスから最新リリースを選択し、図1に示すように「Search」をクリックします。

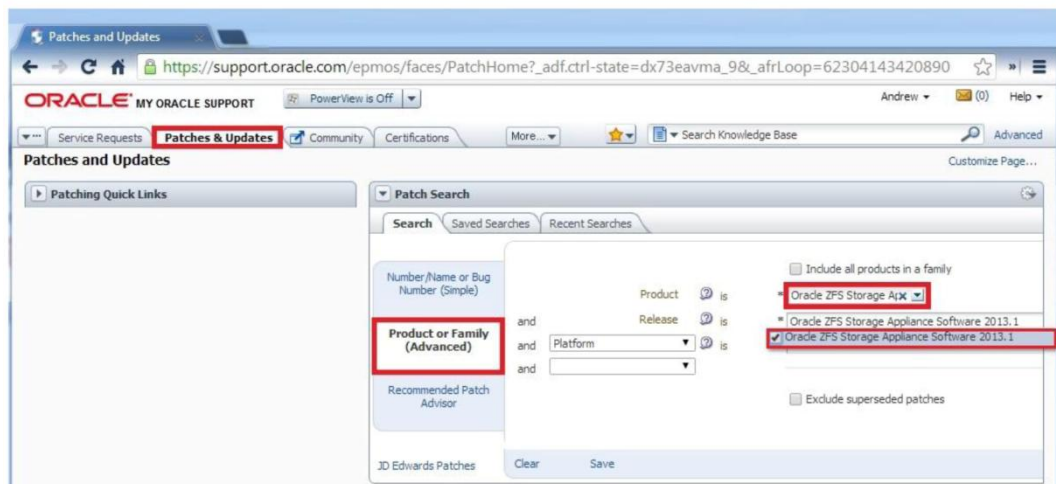


図1: Oracle My SupportのPatches & Updates画面

SMB、NTPクライアント、およびActive DirectoryがOracle ZFS Storage Applianceソフトウェアで提供されているデフォルト機能です。

- 手動またはNTPを使用して時刻を同期する必要があります。SMBを使用してファイル・システムを共有する場合、ユーザー認証エラーを避けるため、クライアントの時刻はアプライアンスの時刻の5分以内になるように同期させる必要があります。時刻を確実に同期させる方法として、同じNTPサーバー（可能であればドメイン・コントローラ自体）を使用するようにアプライアンスとSMBクライアントを構成する方法があります。
- リンク・アグリゲーションまたはVLANのデータリンクを使用する場合、接続しているスイッチ・ポートをそれに応じて構成する必要があります。
- 機能の多くは、構成するのにストレージ・プールは必要ありませんが、ファイル・システム、LUN、またはシェアを作成するためには、利用可能な領域が含まれた基盤となるストレージ・プールが必要です。

Active Directoryドメインに参加する前に、Oracle ZFS Storage ApplianceをDNSサービス用に構成します。DNSを設定するには、名前解決が行われるように、WindowsのDNS管理プラグインを使用してホスト（“A”）レコードを作成します。アプライアンスによって、ドメイン・コントローラ（DC）のDNS SRVレコードが取得されて、指定のドメインのDCが自動的に検出されます。

注：Active Directory DCではないDNSサーバーを使用するようにアプライアンスを構成する場合、適切なDNS SRVレコードでこのDNSサーバーを構成する必要があります。Windows以外の別のDNSサーバーを使用できますが、その場合は、Active Directoryドメインと相互運用するのに必要なすべてのDNS SRVレコードをこのDNSに手動で追加する必要があります。ただし、Active DirectoryをDNSサーバーとして使用する場合は、すべてがデフォルトで構成されます。

Oracle ZFS Storage Applianceを使用したシステム構成の ベスト・プラクティスと原則

構成プロセスで、示されている機能について以下の原則と推奨事項を考慮してください。

ネットワーク

Active DirectoryまたはSMB共有では、特定のネットワーク設定タスクは必要ありません。デバイス、データリンク、インタフェース、LACPリンク・アグリゲーション、およびIPマルチパス（IPMP）のグループはすべてサポートされています。パブリックLANまたは管理LANに含まれないデータ・トラフィックには、プライベート・ネットワーク接続を作成します。さらに広い帯域幅が必要な場合は、10Gbインタフェースやリンク・アグリゲーションを実装します。

Oracle ZFS Storage Applianceのクラスタ

Oracle ZFS Storage Applianceのクラスタ化は、CIFS共有またはNFS共有が含まれたActive Directory環境で完全にサポートされています。フェイルオーバーが発生した場合、すべてのシェアが代替のヘッドに自動的に移動されます。

このドキュメントでは、クラスタ化については説明していません。Oracle ZFS Storage Applianceのクラスタ化の詳細については、『Sun ZFS Storage 7000システム管理ガイド』（http://docs.oracle.com/cd/E25769_01/PDF/E23718-01.pdf）を参照してください。

Microsoft Cluster Service (MSCS)

MSCSクラスタに共有可能なクラスタ・リソースを作成するには、iSCSIを使ってLUNをマウントしてから、クラスタ全体でLUNをSMB共有として共有します。Microsoft Cluster Serviceの詳細については、このドキュメントの対象範囲外となります。

ユーザー

ユーザー画面は、アプライアンスの管理委譲と制御を行ったり、アプライアンスをワークグループ・モードで使用する場合にローカル・ユーザーのアクセス許可を設定するために使用します。アプライアンスをワークグループ・モードに設定する場合、アクセス権を付与するローカル・ユーザーを作成する必要があります。アプライアンスをActive Directoryドメインに参加させる場合は、共有のアクセス許可用のこのセクションは必要ありません。

このドキュメントでは、管理委譲については説明していません。

UNIXユーザーとWindowsユーザーが混在しており、Windowsユーザーと、対応するOracle Solarisユーザー、UNIXユーザー、またはLinuxユーザーの間でマッピングを行う必要がある環境では、アイデンティティ・マッピング・サービスを使用できます。この機能については、このドキュメントでは説明していませんが、Sun NAS Storageドキュメンテーションのページ

（<http://www.oracle.com/technetwork/jp/server-storage/sun-unified-storage/documentation/index.html>）のホワイト・ペーパー・コレクションで提供されているOracle Technical Network (OTN)のドキュメント『*Configuring the Oracle ZFS Storage Appliance to Use IDMU to Map Identities*』および『*Oracle ZFS Storage Appliance Rule-Based Identity Mapping*』で説明しています。

構成全体への原則の実装

以下に、システムとサービスを連携して機能するように構成し、Oracle ZFS Storage ApplianceをWindowsサーバー環境と統合するための、ステップ・バイ・ステップのガイダンスと例を示します。

システムの構成

Oracle ZFS Storage ApplianceをWindows環境と統合するためには、次のシステムレベルの機能を設定する必要があります。

Network Time Protocol

サーバーアクセスに使用するユーザアカウント

Domain Name Service (DNS) サーバー

Active Directory

Network Time Protocol (NTP) サーバーに同期させる

NTPサーバーのサービスを使用するようにOracle ZFS Storage Applianceを構成するには、Webブラウザを使用し、セキュアな接続のポート215 (<https://sunzfssa.example.com:215>) でOracle ZFS Storage Applianceのブラウザ・ユーザー・インターフェースに接続します。

次の図に、ブラウザのログイン画面を示します。



図2: ブラウザのログイン画面

ログインすると、図3に示すように、Oracle ZFS Storage Applianceのメイン・メニュー画面が表示されます。

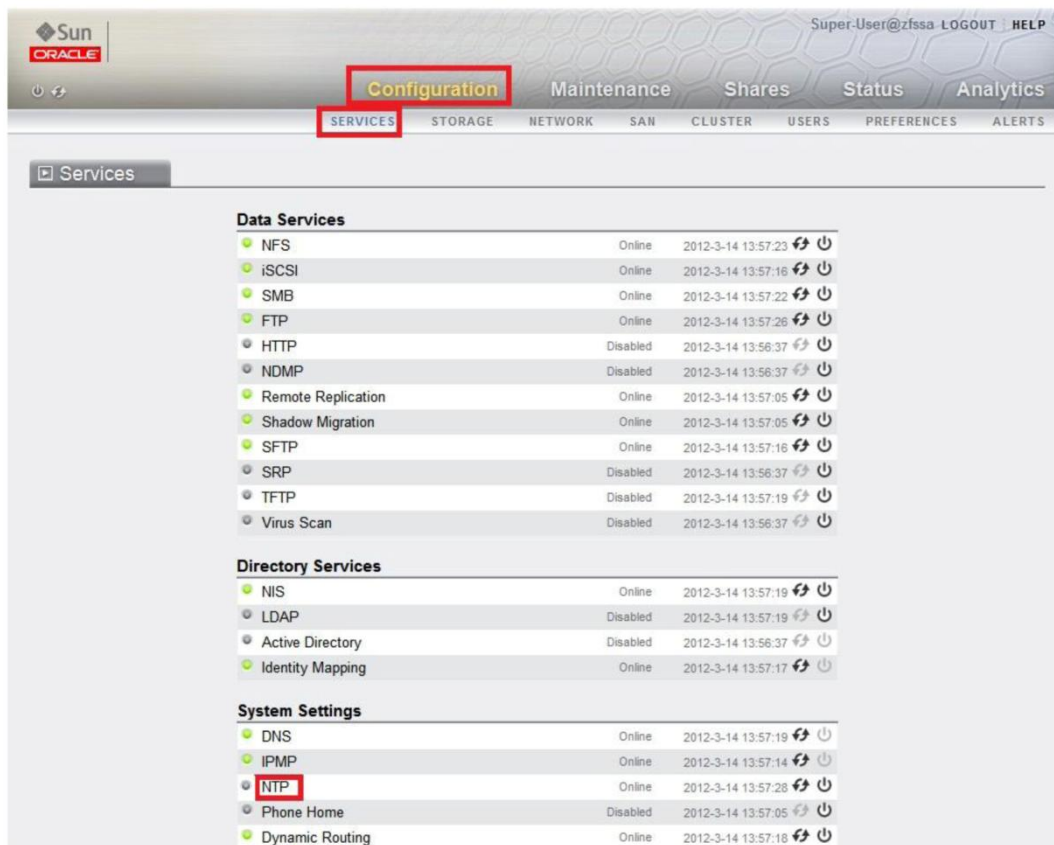


図3: Oracle ZFS Storage Applianceの構成画面

図3に示すように、画面の上側にある「Configuration」タブをクリックし、その下にある「SERVICES」サブタブをクリックし、System Settingsの「NTP」エントリをクリックすると、図4に示すようにNTP構成パネルが表示されます。



図4：NTPサーバーの情報の入力

共通のNTPサーバーの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。この手順は、Active Directoryドメインに参加する前および参加した後は必要ありませんが、ドメイン・コントローラとOracle ZFS Storage Applianceの時刻が5分以上異なる場合は、ドメインへの参加プロセスとユーザー認証が失敗する可能性があります。NTPサーバーがActive Directoryドメイン・コントローラである必要はありません。

NTPに対応するようにWindows サーバーを構成する手順については、<http://support.microsoft.com/kb/816042>を参照してください。必要に応じて、このドキュメントの手順に従ってNTP認証キーを追加します（NTP認証キーの横にある+記号を使用）。NTPキーは、認可されているサーバーとクライアント間で時刻を確実に同期するために使用され、認証などのタイム・クリティカルなアプリケーションで特に重要です。

「apply」をクリックすると、サービスがまだ有効になっていない場合は、サービスを有効にするかどうかを確認するダイアログ・ボックスが表示されます。「enable」をクリックします。有効になると、NTPサービスのボタンが緑色になり、アプライアンスの時刻がクライアントおよびドメイン・コントローラと同期されます。

ワークグループ・アクセス用のローカル・ユーザーを作成する

ワークグループ・アクセス専用の場合は、シェアをクライアント・システムにマウントするために、Oracle ZFS Storage Applianceにローカル・ユーザーを作成する必要があります（図1を参照）。図5に示すように、「Configuration」をクリックし、「Users」をクリックし、Usersの左にある「+」アイコンをクリックします。

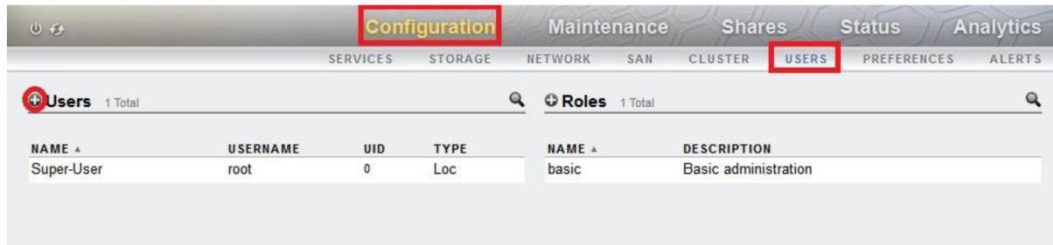


図5：ユーザーの追加

図6に示すように、Add Userダイアログ・ウィンドウが表示されます。

図6：Add Userダイアログ・ウィンドウ

「Local Only」ラジオ・ボタンを選択してから、Username、Full Name、Password、およびConfirm（パスワード確認）の各エントリに情報を入力します。ユーザーに管理権限が必要ない場合は、「Require session annotation」と「Kiosk user」をオフのままにします。このユーザーがアプリケーションにログインするのを防ぐには、下部に示されているすべてのロールもオフにする必要があります。

可能であれば、アプライアンスのローカル・ユーザーをワークグループ・メンバーのマシンに定義されているWindowsローカル・ユーザーとミラー化します。

アプライアンス全体でユーザー名とパスワードを同じにすると、ワークグループ・モードのクライアントで、シェアをワークグループ・モードでマップするたびに明示的に認証する必要がなくなります。このユーザーにシェアのアクセス許可が割り当てられて、ネットワーク・コンピュータやネットワーク・ドライブの割当てインターフェースを使用して、このユーザーがアプライアンスに接続したりシェアをマップしたりできるようになります。

「Add」ボタンをクリックすると操作が完了し、図7に示すように、確認用に、追加したユーザーの名前がユーザーの一覧に表示されます。



Users 2 Total				Roles 1 Total	
NAME ▲	USERNAME	UID	TYPE	NAME ▲	DESCRIPTION
John Doe	John	2000000000	Loc	basic	Basic administration
Super-User	root	0	Loc		

図7：ユーザーの追加の確認

Active Directoryで使用されているDomain Name Service (DNS) サーバーに接続する

DNSベースのActive Directoryサービスを使用するためには、Active Directoryドメイン・コントローラと同じDNSサーバーを使用するようにOracle ZFS Storage Applianceを構成します。そのためには、図8に示すように、上部のタブ・セットから「Configuration」を選択し、サブタブ・セットから「Services」を選択し、構成サービスのSystems Settingsセクションから「DNS」を選択します。

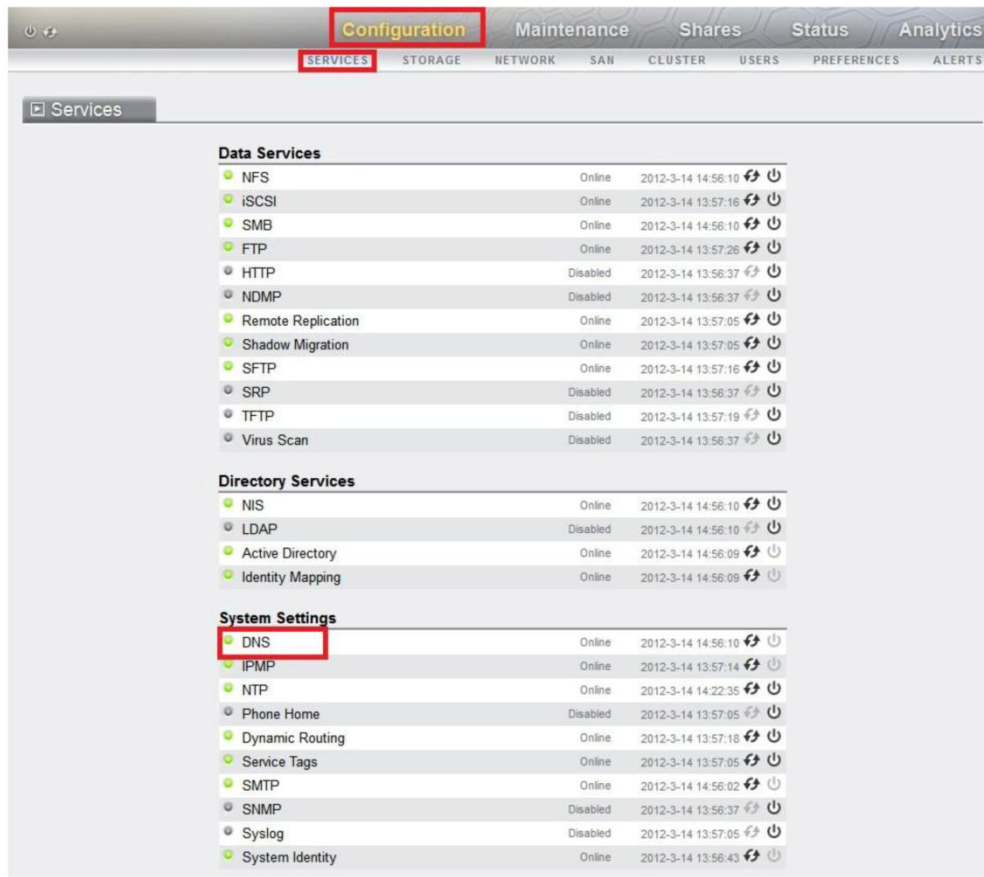


図8 : System SettingsでのDNSサービスの選択

図9に示すDNS構成パネルが表示されます。関連するボックスにDNSドメイン名とDNSサーバーのIPアドレスを入力します。DNSサーバーの追加のIPアドレスを指定するには「DNS Server(s)」の右側にある「+」アイコンをクリックします。「Apply」をクリックしてDNS構成を完了します。



図9 : DNS設定ウィンドウ

Active Directoryで認証するように構成する

ドメイン・モードでは、Oracle ZFS Storage ApplianceはSMB/CIFSファイル・サービスをMicrosoft Active Directoryドメインのメンバー・サーバーとして提供します。Oracle ZFS Storage Applianceがメンバーになれるのは1つのドメインですが、Windows名前空間全体に機能を拡張できるように、推移的な信頼、ドメイン間の信頼、およびフォレスト間の信頼が完全にサポートされています。

Active Directoryサービスを直接有効または無効にするのではなく、ドメインまたはワークグループに参加してサービスを変更できます。ドメインに参加すると、指定のActive Directoryドメインにアプライアンスのコンピュータ・アカウントが自動的に作成されます。コンピュータ・アカウントが作成されたら、アプライアンスによって、データベースに対してユーザー、グループ、および共有の情報を安全に問合せできるようになります。

Active Directoryでは、すべてのリソースにアカウントを設定する必要があります。これには、Active Directoryドメインに参加するユーザー、ワークステーション、サーバー、およびその他のデバイスが含まれます。Oracle ZFS Storage Applianceをドメインに参加させると、コンピュータ・アカウントが自動的に作成されます。

Active DirectoryにIDが設定されているWindowsユーザーは、アプライアンスがドメインに参加するとすぐに、このアプライアンスで許可されているシェアをマップできるようになります。Windowsドメイン・ユーザーがシェアをマップしようとする時、Oracle ZFS Storage Applianceがドメイン・コントローラでユーザーのIDを認証し、ユーザーの資格情報とアクセス許可を取得して、Windowsユーザーの名前を検証します。Active Directoryの信頼ルールに従って、Active Directoryフォレスト内の信頼されたドメイン内のユーザーは、十分な権限が付与されていればアプライアンスにアクセスできます。同様に、信頼されたフォレスト内のユーザーもアプライアンスのリソースにアクセスできます。

Oracle ZFS Storage Applianceでディレクトリ・サービスの認証構成をActive Directoryサービスからワークグループに変更すると、暗黙的にActive Directoryドメインから抜けることになります。そのため、Active Directoryデータベースに格納されているすべてのSMBクライアントがシェアに接続できなくなります。

Active Directory構成パネルを表示するには、図10に示すように、最上部の「Configuration」タブをクリックしてから「Services」サブタブをクリックし、Directory Servicesセクションから「Active Directory」を選択します。

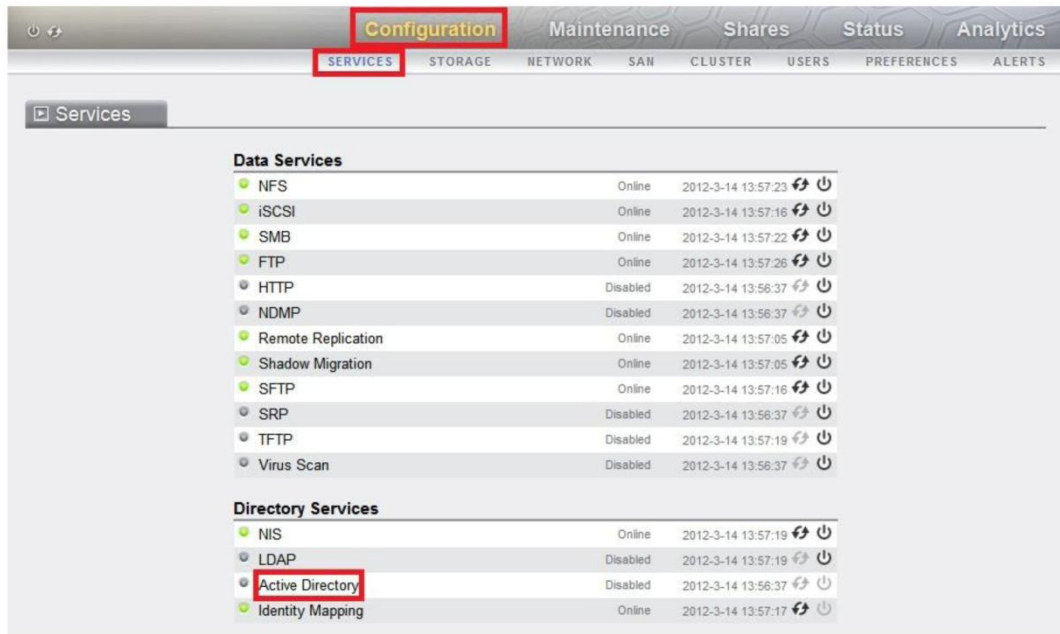


図10 : Active Directoryに対応するディレクトリ・サービスの構成

「Active Directory」を選択すると、次のサービス画面が表示されます。この表示からドメインに参加できます。



図11 : Active Directoryの状態が構成されていない場合

「Join Domain」ボタン（図11を参照）をクリックすると、図12に示すようにActive Directory構成パネルが表示されます。

図12：Active Directory構成パネル

Active Directoryドメインに参加するには、Active Directoryドメイン・ウィンドウに完全修飾ドメイン名（FQDN）、ドメイン管理者の資格情報を持つユーザー、および管理者のパスワードを入力します。「Apply」をクリックして参加要求を開始します。この手順は通常、30秒ほどかかります。アプライアンスがドメインに参加すると、Active Directoryサービスが起動してオンラインに表示されます。図13に示すように、ドメインの最新情報が表示されます。

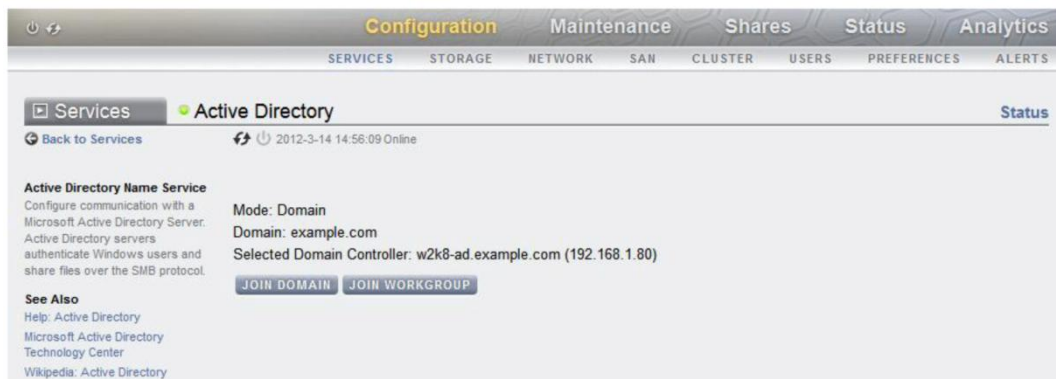


図13：Active Directoryのドメイン・メンバーシップ

図14に示すようなエラー・メッセージが表示されて操作が失敗した場合、Oracle ZFS Storage ApplianceのDNS構成を確認して、Active Directoryドメイン・コントローラのDNS構成と同じ情報が含まれていることを確認します。

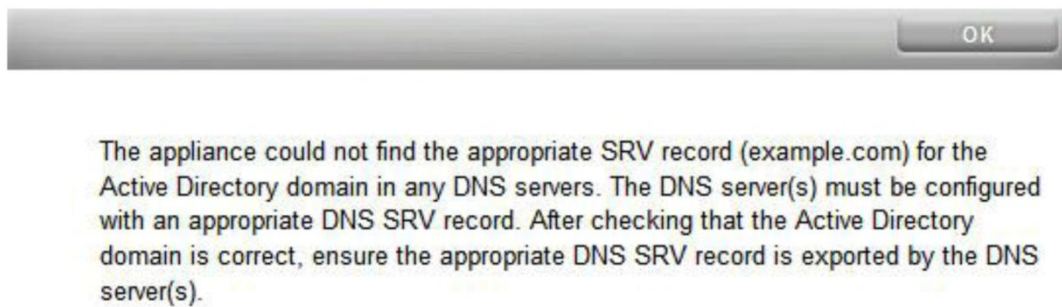


図14 : DNS構成の問題のためにActive Directoryの参加要求が失敗

アプライアンスのコンピュータ・アカウントを表示するには、ドメイン・コントローラにログオンして、Active Directoryユーザーとコンピュータにアクセスします。アプライアンスのコンピュータ・アカウントは、図15に示すように標準の“コンピュータ”コンテナに作成されています。

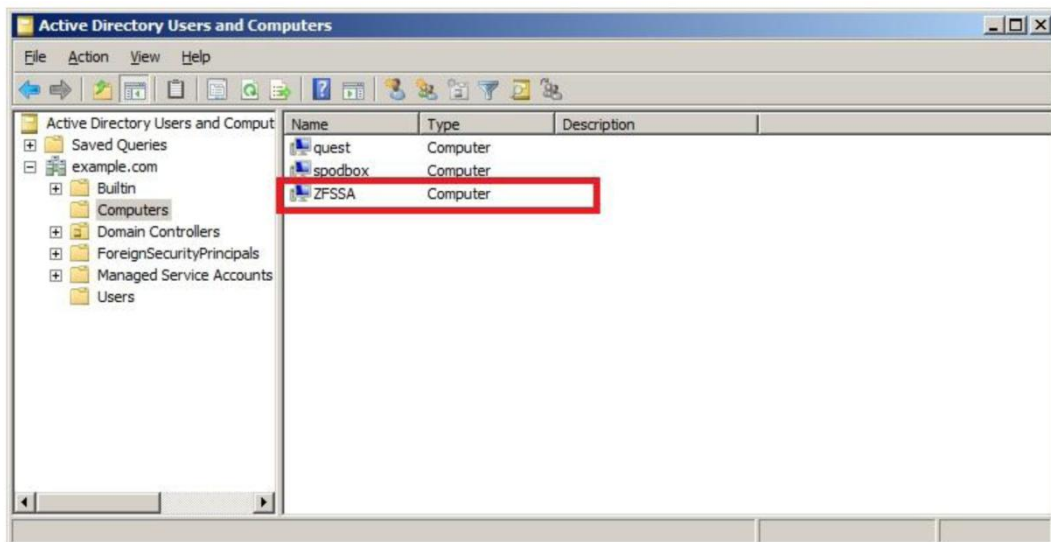


図15 : Active Directoryユーザーとコンピュータの表示

サービスの構成

以降の手順で、データ・アクセス・プロトコルSMB/CIFSを使用し、シェアを作成および構成して、Oracle ZFS Storage ApplianceとWindows環境の間でファイル・システムの共有とアクセスを確立します。

SMBサービス・プロトコルを選択する

SMBサービスでは、SMB/CIFSプロトコルを使用してファイル・システムにアクセスします。シェア構成でSMBを使用して共有するように、ファイル・システムを構成する必要があります。最初の手順として、図16に示すように、「Configuration」、「Services」タブの順に選択してサービスを有効にし、SMBエントリがDisabledと表示される場合は、このエントリの右側にある電源ボタン・アイコンをクリックします。SMBエントリがOnlineと表示される場合は、設定を変更しないでください。

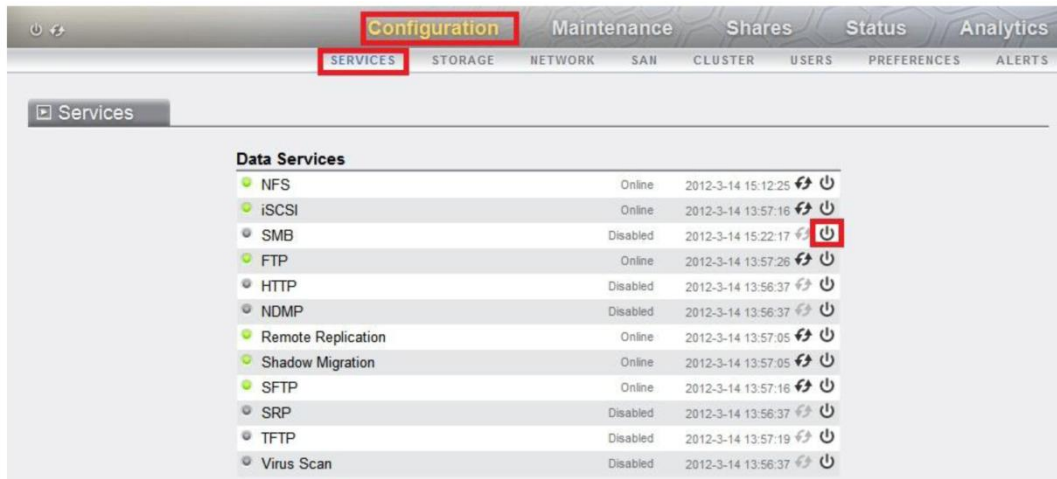


図16 : Oracle ZFS Storage ApplianceでのSMB/CIFSの有効化

シェアを作成する - プロジェクトとファイル・システム

すべてのファイル・システムとLUNがプロジェクトにグループ化されます。プロジェクトでは、シェアを管理する共通の管理制御ポイントが定義されています。同じプロジェクト内のすべてのシェアで共通の設定を使用でき、シェアレベルだけでなくプロジェクト・レベルでも割当て制限を適用できます。また、プロジェクトを使用して、論理的に関連付けられたシェアを単にグループ化し、プロジェクトの共通属性（蓄積領域など）に1箇所からアクセスすることもできます。

プロジェクトにプレフィックスを追加すると、リソースでプロジェクト名を識別できます（たとえば、dev_codeの場合、devはプロジェクト名Developmentに割り当てられたプレフィックスで、codeは共有名です）。

プロジェクトを構成するには、プロジェクトのProtocolsのSMBセクションを変更し、Resource Nameを“on”に設定します。これにより、別の方法で構成されている場合を除き、このプロジェクトで作成されたすべてのシェアにproject_share名前付けスキームを使ってアクセスできるようになります。図17にこの例を示します。

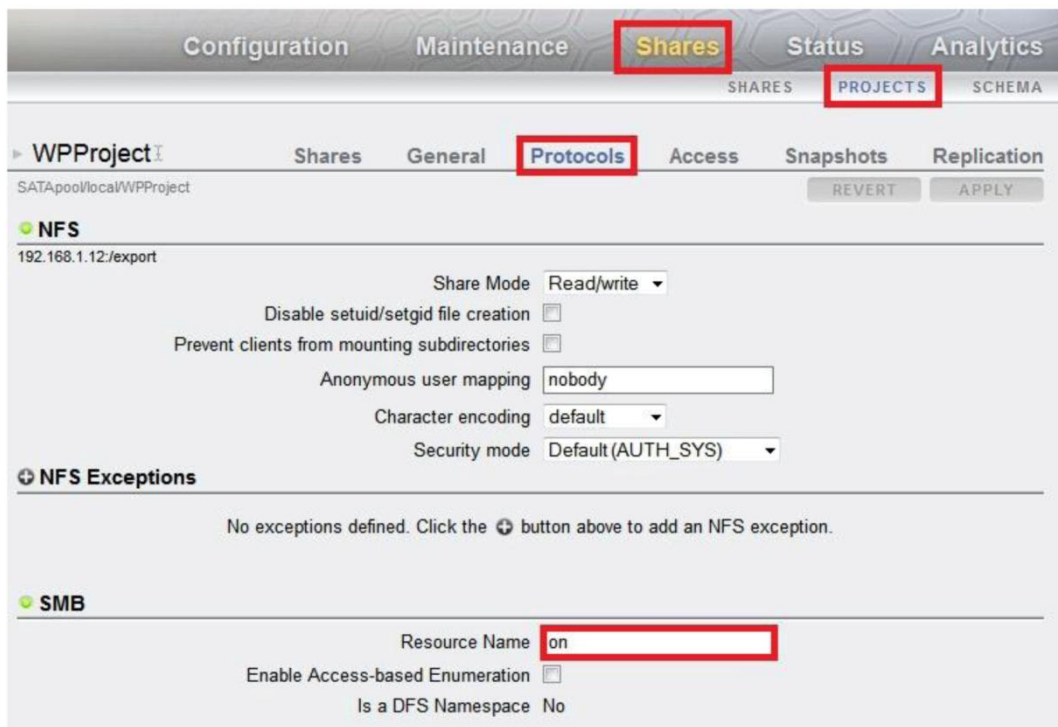


図17：自動のシェア名前付けの有効化

デフォルトでは、ストレージ・プールを初めて構成したときに、Oracle ZFS Storage Applianceによってデフォルトのプロジェクトが1つ作成されます。デフォルトのプロジェクト内にすべてのシェアを作成できますが、大規模な環境では、整理の目的で追加のプロジェクトを作成することを強く推奨します。

Windows環境には、シェアのアクセス許可と基盤となるファイル・システムのアクセス許可の、2層のアクセス許可があります。この2つのアクセス許可には、もっとも制限の多いアクセス許可のみ適用されます。この2層のアクセス許可のいずれかを選択して、一貫して使用することを推奨します。

ファイル・システムのアクセス許可、ファイルのアクセス許可、フォルダのアクセス許可、およびNTFSのアクセス許可の命名体系は多くの場合、区別せずに使用されます。Oracle ZFS Storage Applianceでは、これらのアクセス許可はルート・ディレクトリのアクセス権と呼ばれています。これらのアクセス許可をBUIのfilesystemタブのAccessタブに表示し、変更できます。

シェアは、ファイル・システムでもブロック・プロトコルのLUN (iSCSIまたはファイバ・チャネル)でも構いません。ファイル・システムは、作成されるとSMB共有としてエクスポートされます。

領域の管理、共通の設定、レプリケーションの制御などの共通の管理の目的で、シェアをプロジェクトにグループ化できます。シェアはデフォルトでシン・プロビジョニングされるため、シェアに固定サイズのファイル・システムは必要ありません。固定サイズの予約済み領域が必要な場合は、割当て制限と予約を使用して予約済み領域を設定できます。

ファイル・システム作成のデフォルト設定では、所有者には読み込み、書き込み、および実行のアクセス許可が付与され、所有者以外にはアクセス許可は付与されません。この慎重なアプローチによって、アクセス許可が誤って広く適用されるのを防いでいます。図18に示すように、Projects表示のGeneralタブで、このデフォルト設定をプロジェクト・レベルで変更できます。

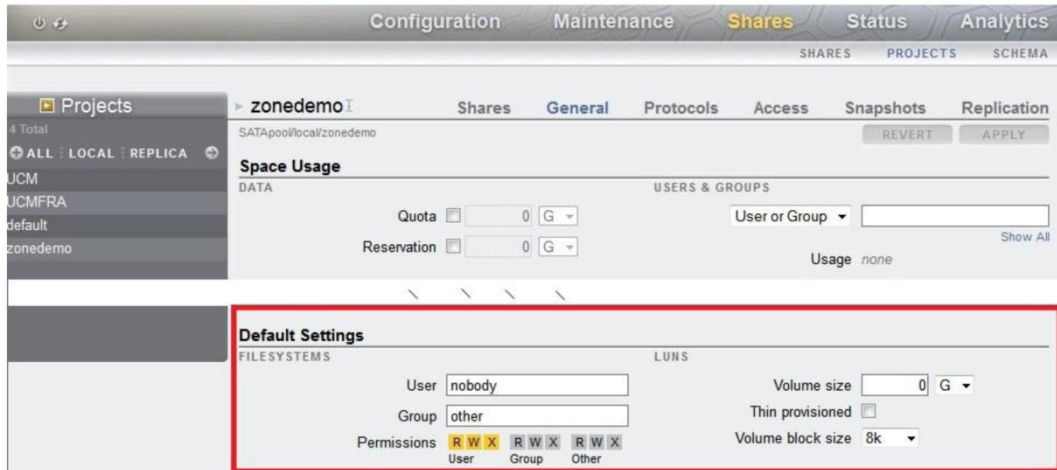


図18：プロジェクトのファイル・システムのデフォルト設定

Windowsではアクセス制御リスト（ACL）のみ参照されて、図18に示すUser/Group/Otherのアクセス許可のボックスは参照されないため、新しいファイル・システムの作成時にデフォルトのアクセス許可は変更しないままにします。

シェアレベルのデフォルトのACL設定では、すべてのユーザーが自由にアクセスできるようになります。図18の強調表示したボックスで示すように、ファイル・システムのデフォルトのACL設定では、User（所有者）が“nobody”でGroupが“other”となり、User（所有者）のみ読み込み、書き込み、および実行のアクセス許可が付与されます。Windowsでは、ACLの制御は共有シェアレベルではなくファイル・システム・レベルで行うことが推奨されています。前述したように、両方を保持するのは難しいため、両方ではなくいずれか1つのレベルを選択します。Windowsのみの環境でアプライアンスの管理を簡素化するため、すべてのユーザーにシェアレベルとファイル・システム・レベルの両方でフル・コントロールのアクセス許可を設定してから、Windowsクライアントの個々のアクセス許可を管理します。以下の3つの図に、これを行うための画面を示します。図19に、シェアレベルのACL構成パネルを表示する方法を示します。



図19：シェアの構成パネル

図20に、“すべてのユーザー”に“フル・コントロール”を許可するシェアレベルのACLパネルを示します。

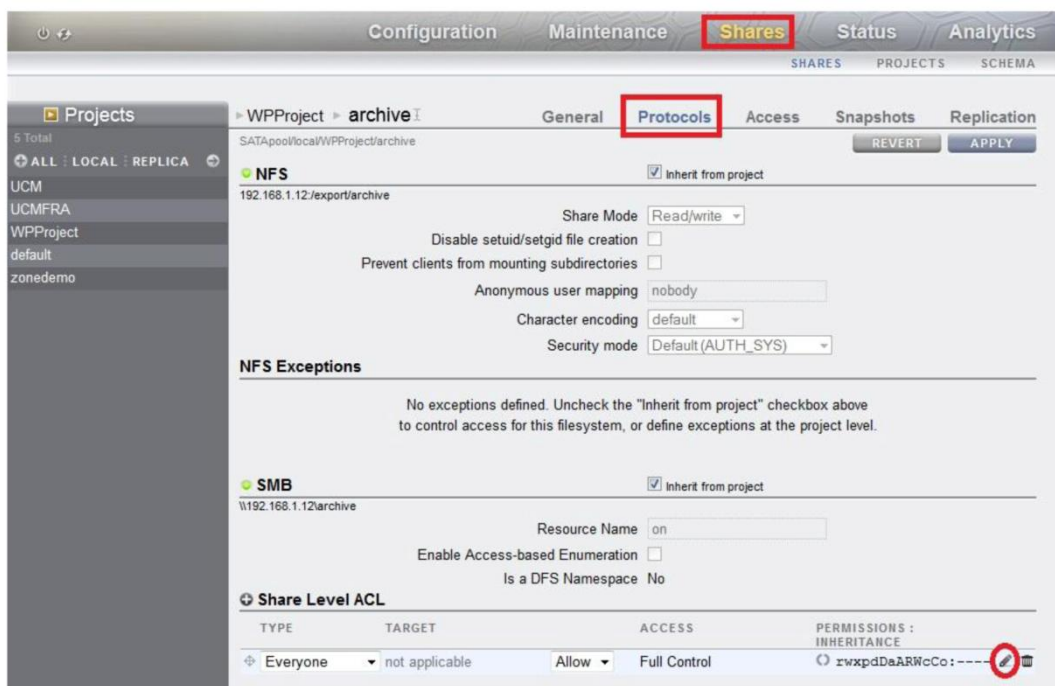
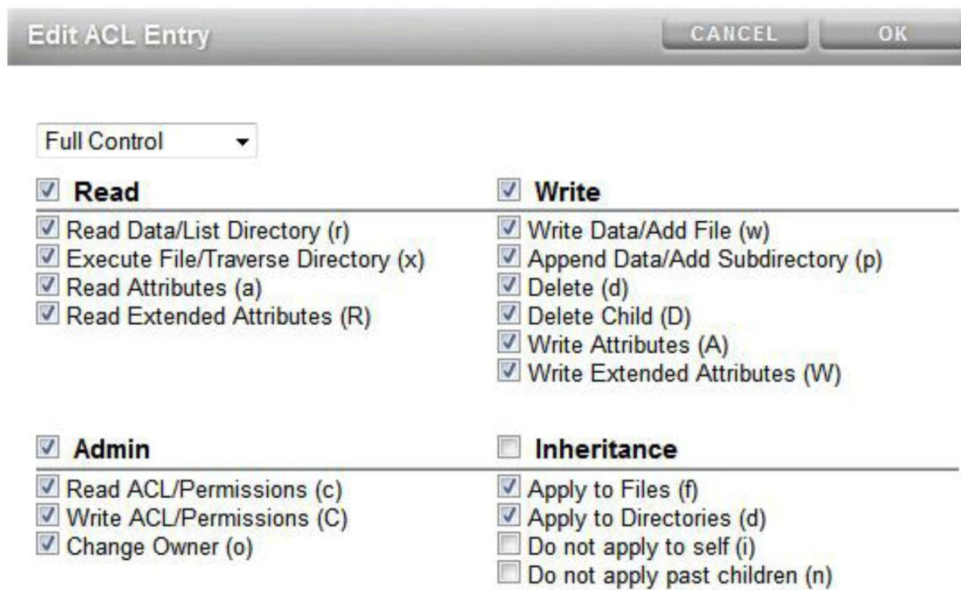


図20：シェアレベルのACL設定の変更

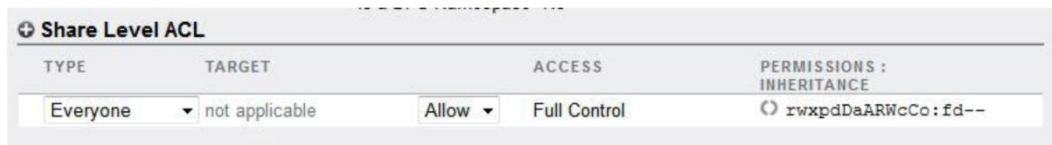
図21に、すべてのユーザーにフル・コントロールが付与されている場合の、個別のアクセス許可の例を示します。



<<

図21: 'すべてのユーザー'にフル・アクセスが付与されている場合の関連する設定

「OK」ボタンを押して選択を確定すると、図22に示すように、“Share Level ACL”セクションに更新されたACLが表示されます。



TYPE	TARGET	ACCESS	PERMISSIONS : INHERITANCE
Everyone	not applicable	Allow	Full Control rwxpdDaARWcCo:fd--

図22: 'すべてのユーザー'にフル・コントロールのACLが付与されていることを示す画面

シェアの構成

プロジェクトのProtocolsタブで、SMBサービスのライトが緑になっており、Resource Nameがoffに設定されていることを確認します。SMBサービスがオンになっている場合でも、シェアが公開されるように、SMBのResource Nameを文字列に変更する必要があります。Resource Nameをonに設定すると、各ファイル・システムが`¥¥servername¥filesystem`の形式のファイル・システム名で表示されます。または、プロジェクト・レベルでプレフィックスを割り当てることもできます。その場合、各プロジェクトのシェアを相互に区別するため、プレフィックスをファイル・システム名の前に配置します (`¥¥servername¥prefix_filesystem`など)。この表記規則は、ProtocolタブのSMBセクションの“inherit from project”チェックボックスをオンにしてそのプロジェクトに作成した、すべてのファイル・システムに適用されます。図23と図24に示すように、図23でSMBセクションのResource Nameを“on”に設定し、図24のファイル・システム設定で“inherit from project”を許可すると、SMB共有のデフォルトの名前付けスキームがファイル・システム名に設定されます。

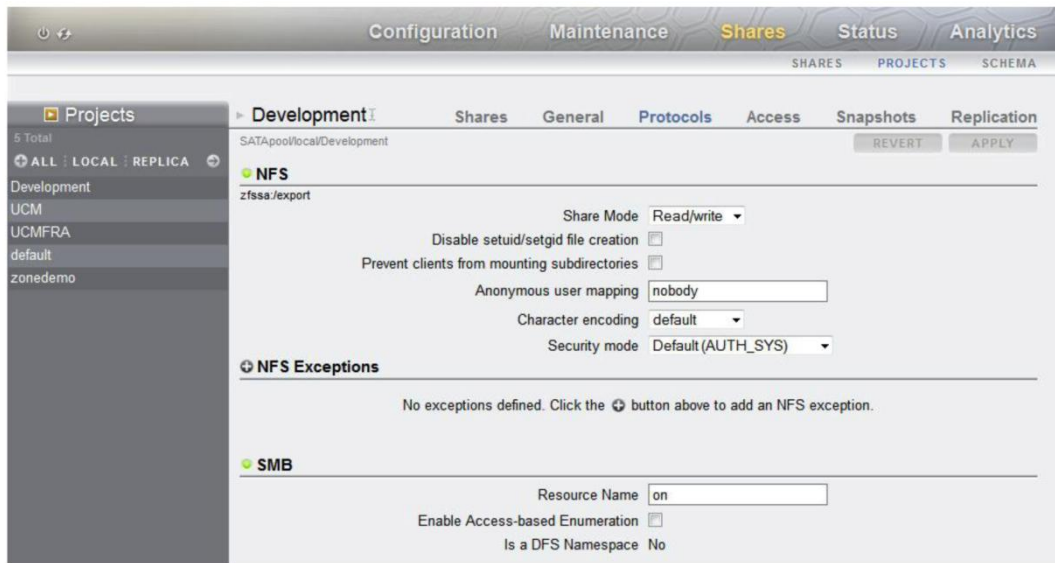


図23：プロジェクト・レベルのプロトコルの表示

図24に、ファイル・システム・レベルのプロトコルを示します。codeという名前のファイル・システムがDevelopmentプロジェクトに作成されています。

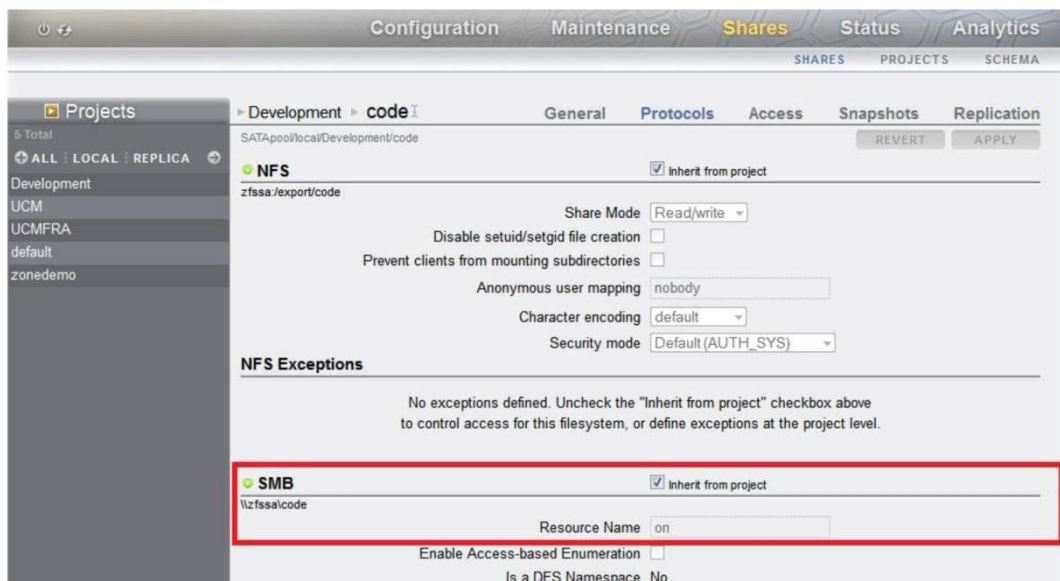


図24：ファイル・システム・レベルのProtocolsタブ

Windowsクライアントのエクスプローラー・ウィンドウでは、シェアのファイル・システムは図25に示すように表示されます。

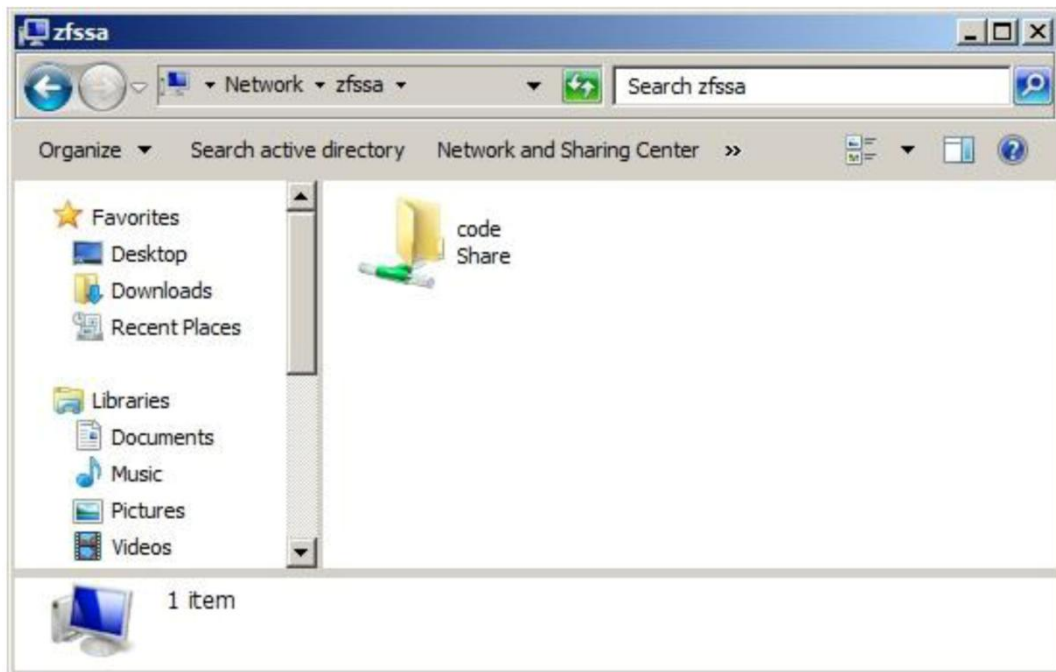


図25: クライアントのエクスプローラー・ウィンドウでのcodeという名前のファイル・システムの表示

図26と図27に示すように、プロジェクト・レベルでResource Nameに一意のID(この例では“deptSMB”)を設定すると、外部クライアント(図28)で表示されるように、ファイル・システムでそのプレフィックス、アンダースコア、およびシェア名が継承されます。

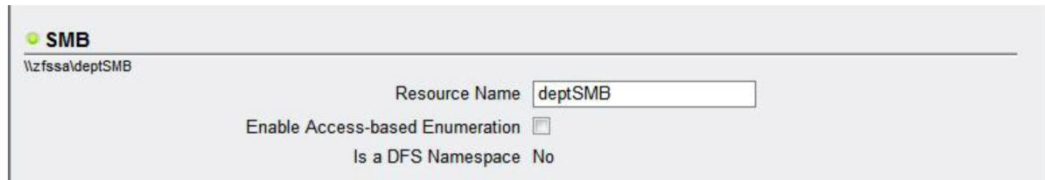


図26: プロジェクト・レベルのプロトコルでのResource Nameの設定

図27に、SMBで継承された完全なファイル・システム名deptSMB_codeを示します。

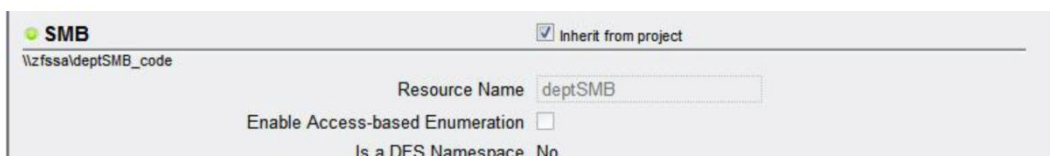


図27: ファイル・システム・レベルのプロトコルで表示される継承された名前

図28に示すように、Windowsクライアントのエクスプローラー画面には完全なファイル・システム名が表示されます。

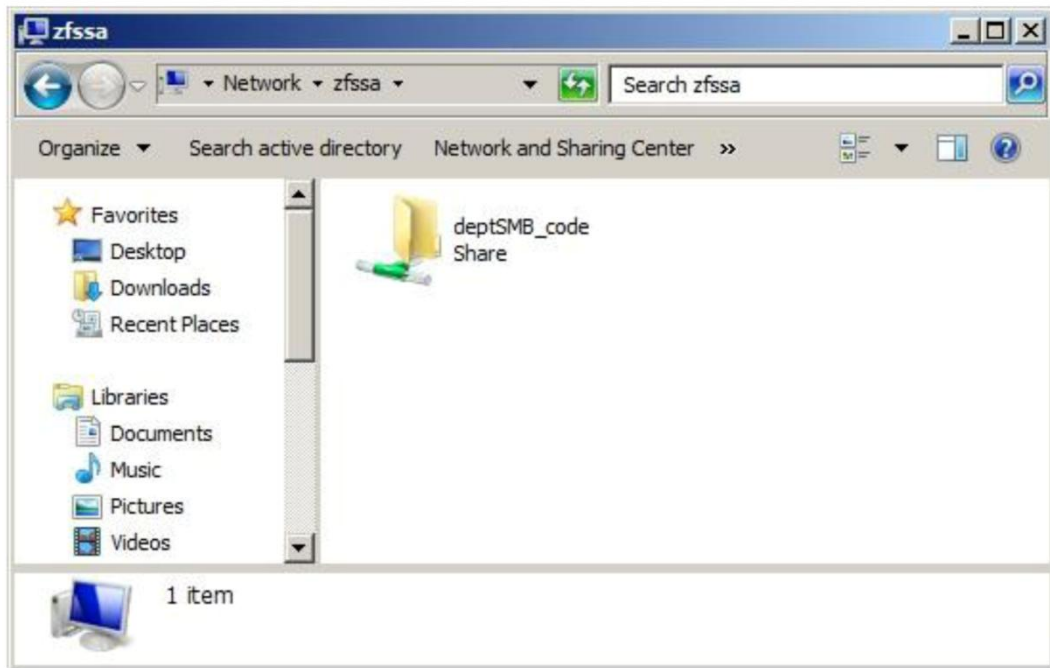


図28 : Windowsクライアントで表示される継承された名前

また、“Inherit from project”をオンにしない場合は、SMBのResource Nameを“on”に設定して、ファイル・システム名を共有レベルまたはファイル・システム・レベルの一意のIDとして指定することもできます。図29にこの設定を示します。

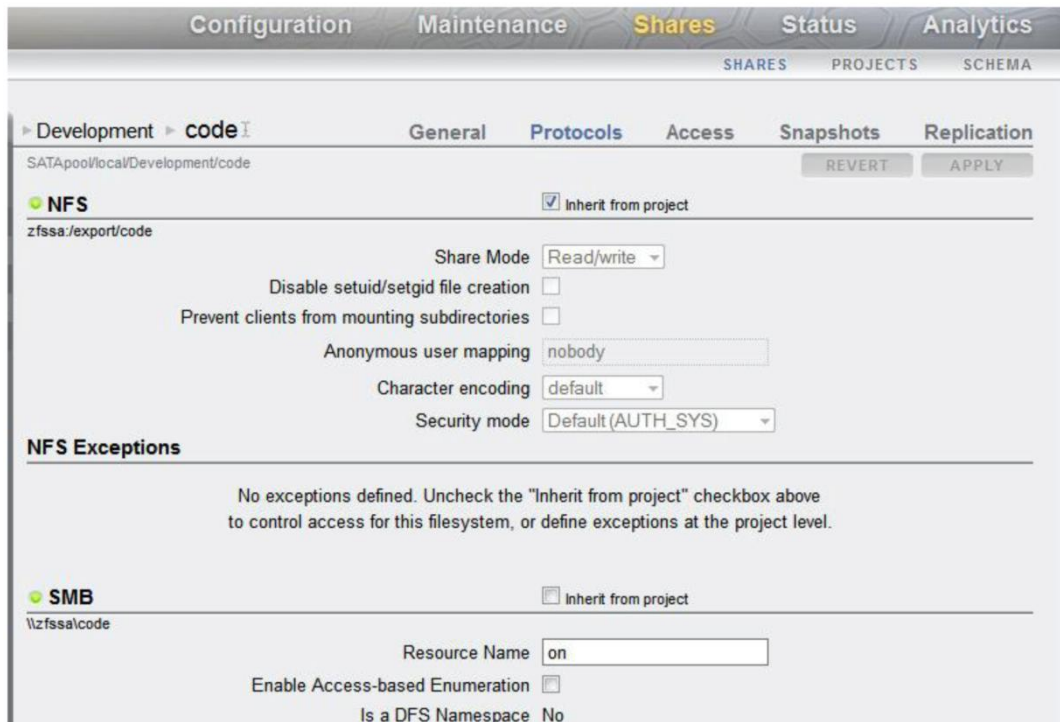


図29：ファイル・システム・レベルのProtocolsタブでResource Nameを“on”に設定したもの

図30に、Windowsエクスプローラー画面でのこの設定の結果を示します。

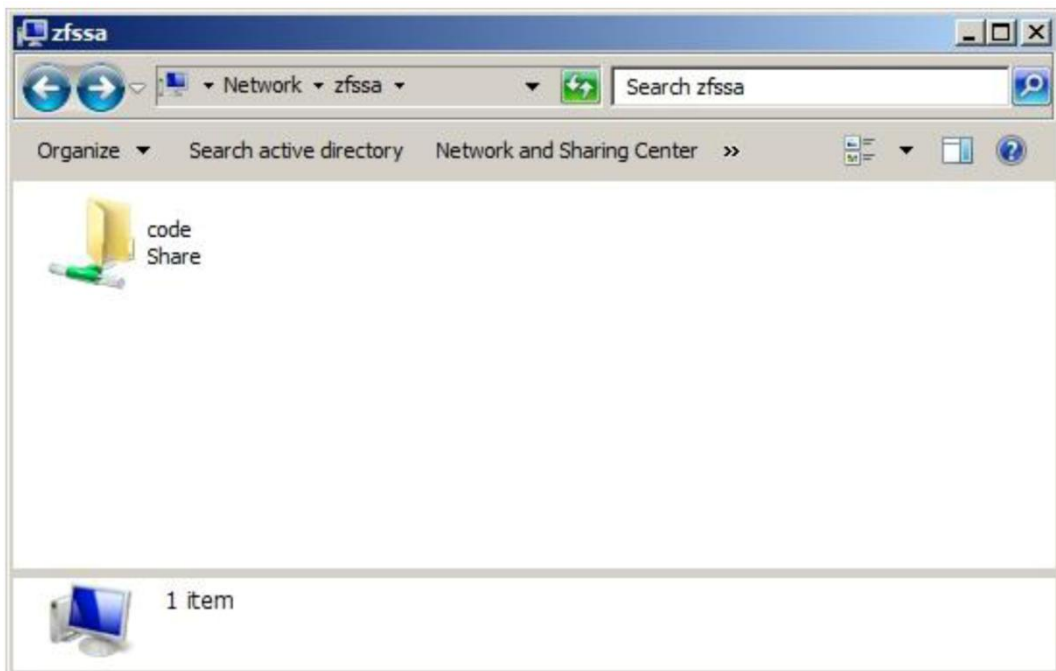


図30：Resource Nameを“on”に設定した場合の、クライアントのエクスプローラー・ウィンドウ

図31と図32に示すように、ファイル・システム名とは異なるシェア名を割り当てるのはサポートされていますが、混乱が生じる可能性があるため、推奨されません。この例では、リソース名を“dept1”に設定しています。

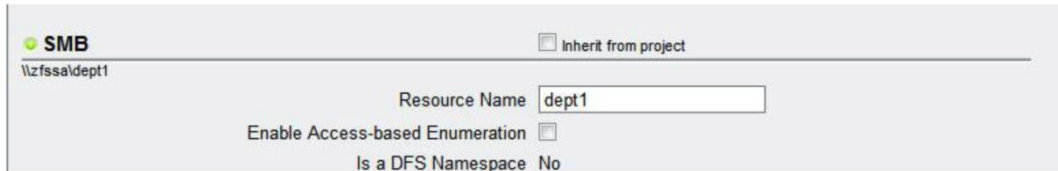


図31：ファイル・システム・プロトコル・レベルでの明示的な共有名の割当て

図32に、Windowsクライアントのエクスプローラー画面での、明示的に名前を指定したシェアを示します。

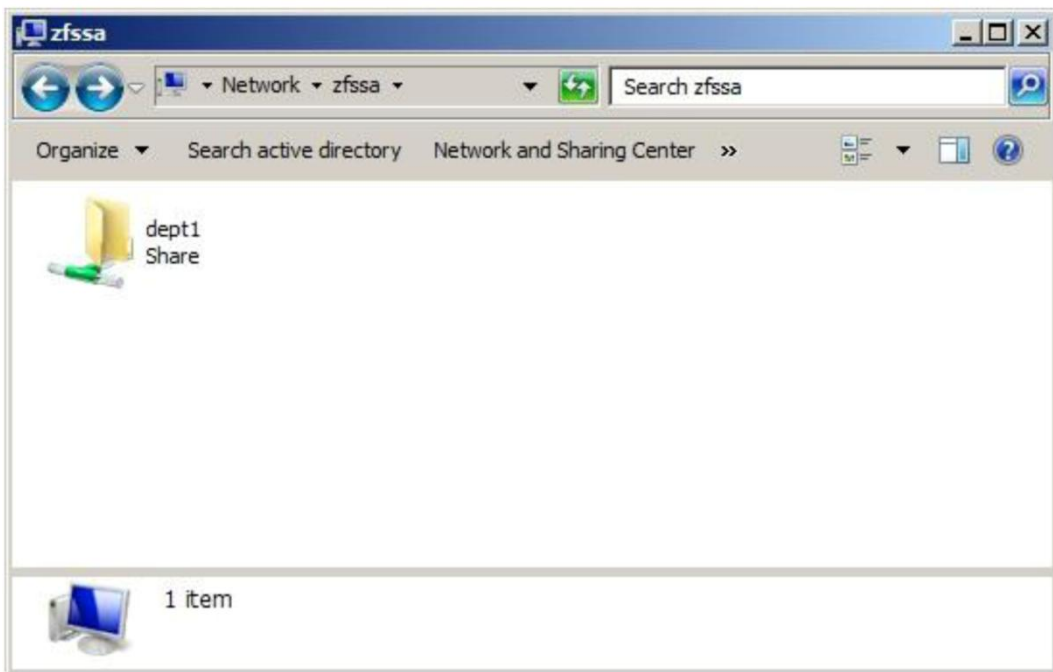


図32：Windowsクライアントに表示される明示的な名前

次の例では、DevelopmentとProductionの2つのプロジェクトを示します。Developmentには“code”という名前のシェアがあり、Productionには“data”という名前のシェアがあります。クライアント・マシンには、Oracle ZFS Storage Applianceに接続されている両方のシェアが表示されます。Developmentプロジェクトにプレフィックス“dev”を追加し、Productionプロジェクトにプレフィックス“prod”を追加すると、この2つのプロジェクトを簡単に区別できます。

図33に、特定のプロジェクトに名前を関連付ける前の、この2つのシェアを示します。

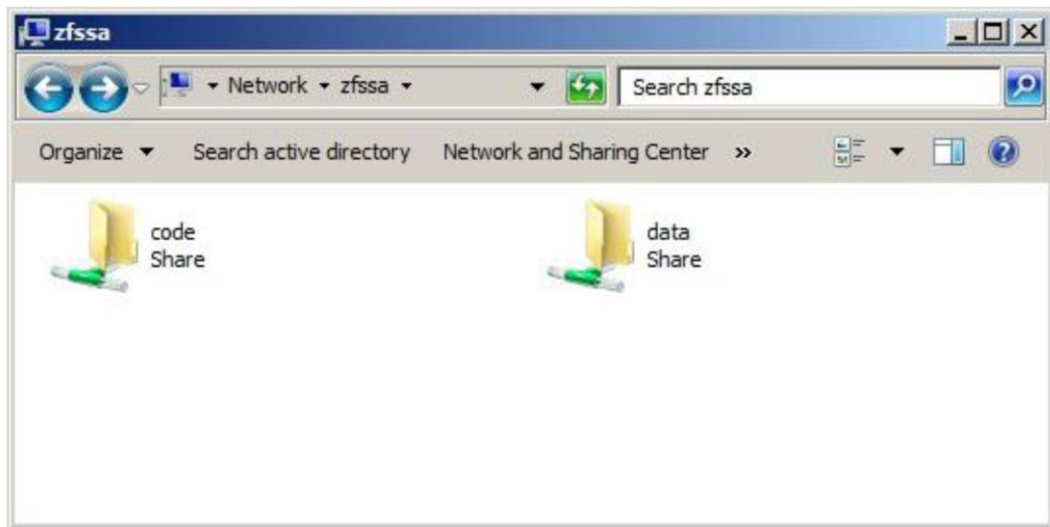


図33 : プロジェクト・レベルの名前付きリソースがないことを示す画面

図34に、Windowsクライアントでの、名前が変更されたシェアを示します。それぞれのプレフィックスを使って、プロジェクトに簡単に関連付けできるようになりました。

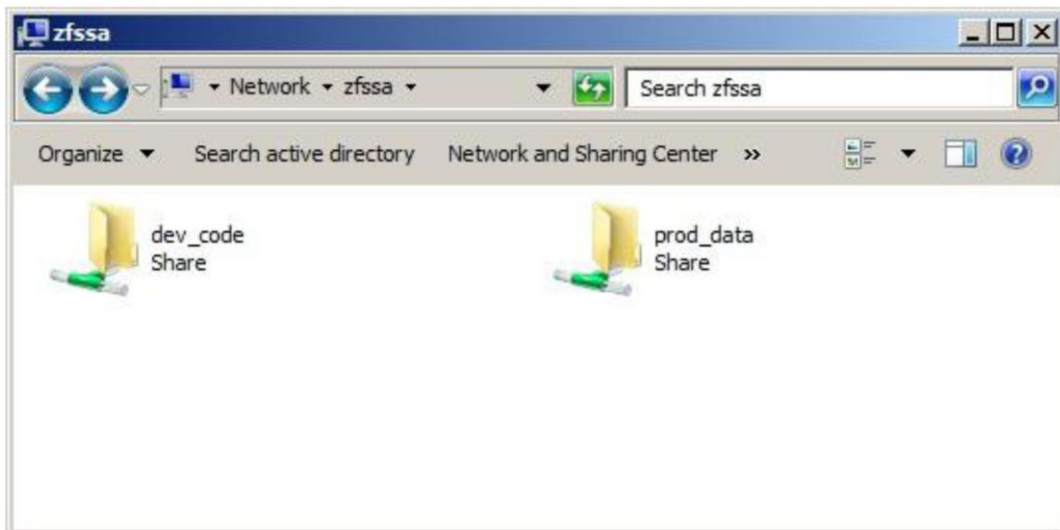


図34 : プロジェクト・レベルの名前付きリソースを示す画面

シェアのACLをワークグループ・モードで構成する

次の例で、Oracle ZFS Storage ApplianceでACLを設定する手順を示します。

注：ドキュメントのこのセクションは、ローカル・ユーザーを伴うワークグループ・モードに対応するもので、Active Directoryユーザーには適用されません（Active Directoryユーザーについては、のちほど説明します）。

図35に示すように、クライアント・システムからシェアcodeを表示できるようになりましたが、codeフォルダを開こうとするとアクセス許可が拒否されます。各ローカル・ユーザーに特定のアクセス許可を割り当てできます。

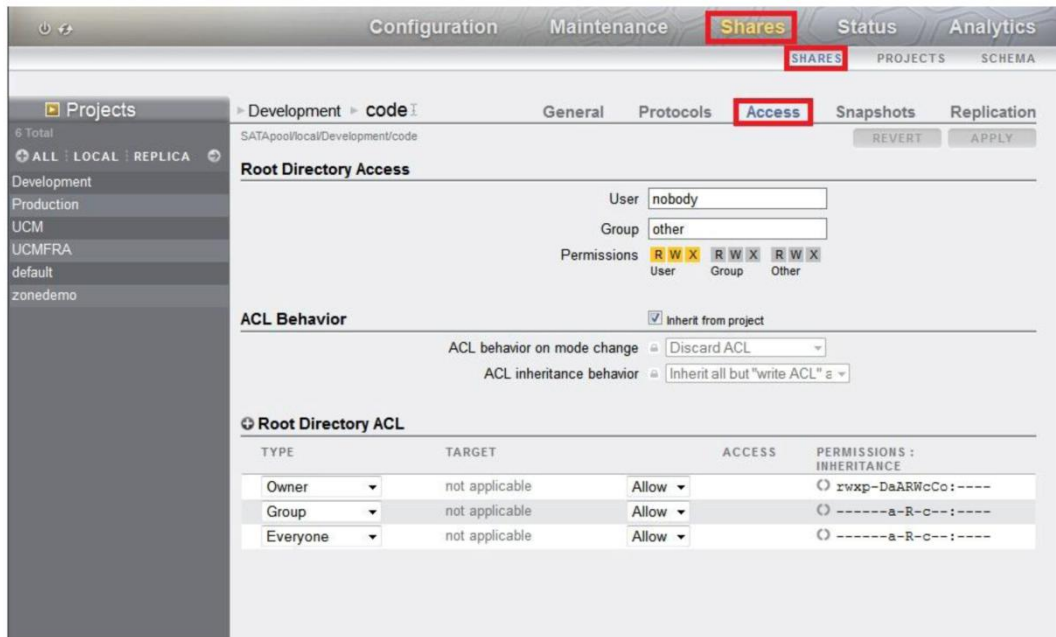


図35：デフォルトのACLアクセス許可の表示

図36に示すように、現在、読み込み、書き込みと実行（rwx）のアクセス許可がBobに割り当てられ、読み込みと実行（rx）のアクセス許可がTimに割り当てられ、所有者（User）がJackに変更されています。これらの各ユーザーは、Usersタブでアプライアンスに設定されたパスワードを持っています。アプライアンスのユーザー名およびパスワードがクライアント・マシンのクライアント・ログインのユーザー名およびパスワードと一致し、そのユーザーに少なくともシェアの読み込みアクセス許可がある場合、そのユーザーにパススルーを使用してアクセスが許可されます。ユーザーのパスワードがクライアントとアプライアンスで異なる場合、パスワードのダイアログ・ボックスが表示されます。

JackとBobは、codeの下に自身のフォルダとファイルを作成できます。相手のファイルとフォルダには、書き込みや読み込みを行うことはできません。Timは、codeの内容を表示できますが、それ以外の操作は実行できません。

The screenshot displays the 'Access' configuration page for a share named 'code'. The 'Root Directory Access' section is configured with User: Jack, Group: other, and Permissions: RWX for User, RWX for Group, and RWX for Other. The 'ACL Behavior' section has 'inherit from project' checked, 'ACL behavior on mode change' set to 'Discard ACL', and 'ACL inheritance behavior' set to 'Inherit all but "write ACL"'. The 'Root Directory ACL' table is as follows:

TYPE	TARGET	ACCESS	PERMISSIONS : INHERITANCE
Named User	Bob	Allow	rwxp--aAR----:----
Named User	Tim	Allow	r-xp--a-R----:----
Owner	not applicable	Allow	rwxp-DaARWcCo:----
Group	not applicable	Allow	-----a-R-c--:----
Everyone	not applicable	Allow	-----a-R-c--:----

図36 : 更新後のアクセス許可が表示されたRoot directory ACL

注 : ローカルのシェアとユーザーを構成してからアプライアンスをドメインに参加させた場合、これらのユーザーとアクセス許可は有効なままになります。

シェアのACLをドメイン・モードで構成する

ドメイン・ユーザーにアクセス許可を割り当てるプロセスは、ワークグループ・モードでローカル・ユーザーに割り当てるプロセスとやや異なります。Oracle ZFS Storage Applianceをドメインに参加させたら、ユーザー名にもusername@FQDNの形式で完全修飾ドメイン名を含める必要があります。図37に示すように、Joe (Joe@example.com) がReportsという名前の新しいファイル・システムを作成しています。Joeがこのファイル・システムの所有者になりますが、読み込みと実行 (rx) のアクセス許可をaccounting_users (accounting_users@example.com) ドメイン・グループに付与します。

Create Filesystem

CANCEL APPLY

Project Accounting

Name Reports

Data migration source None

User joe@example.com

Group accounting_users@example.com

Permissions Use Windows default permissions

Inherit mountpoint

Mountpoint

Reject non UTF-8

Case sensitivity Mixed

Normalization None

R W X R W X R W X
User Group Other

図37: ドメイン内のActive Directoryユーザーへのアクセス許可の割当て

accounting_usersドメイン・グループのメンバーであるJoeは、このシェアを表示してアクセスできます。ファイル・システムReportsはプロジェクト・リソース名“acct”で共有されており、セキュリティ情報は図38に示すようになります。

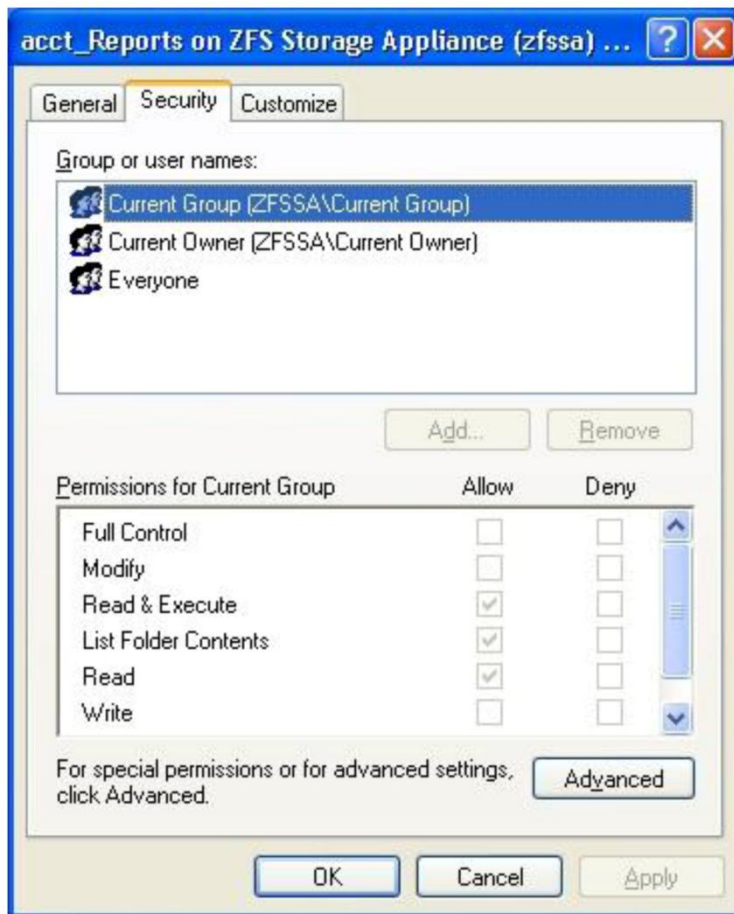


図38 : Windowsクライアントのセキュリティ・タブに表示された、ドメインベースのファイル・システムacct_Reportsの情報

個々のユーザーまたはユーザーのグループにアクセス許可を付与するには、「Named User」または「Named Group」を選択します。図39に示すように、ドメインのユーザーまたはグループにアクセス許可を割り当てる際、完全修飾ドメイン名（FQDN）を使用する必要があります。

Accounting > Reports General Protocols Access Snapshots Replication

SATApool/local/Accounting/Reports REVERT APPLY

Root Directory Access

User:

Group:

Permissions: R W X R W X R W X

User Group Other

ACL Behavior

Inherit from project

ACL behavior on mode change:

ACL inheritance behavior:

Root Directory ACL

TYPE	TARGET	ACCESS	PERMISSIONS : INHERITANCE
Named User	<input type="text" value="brian@example.com"/>	Allow	Full Control <input type="text" value="rwxpdDaARWcCo:fd--"/>
Named Group	<input type="text" value="finance_analysts@example.com"/>	Allow	Read & Execute <input type="text" value="r-x---a-R-c--:----"/>
Owner	not applicable	Allow	<input type="text" value="rwxp-DaARWcCo:----"/>
Group	not applicable	Allow	Read & Execute <input type="text" value="r-x---a-R-c--:----"/>
Everyone	not applicable	Allow	<input type="text" value="-----a-R-c--:----"/>

図39 : Brianとfinance_analystsのユーザーとグループの明示的な追加

ZFSのACLは特殊なアクセス許可セクションに保持されます。このセクションには、Windows XPのWindowsエクスプローラーの詳細設定ボタン（図40）からアクセスするか、Windows Server 2003以降では「プロパティ」→「セキュリティ」タブの順に選択してアクセスします。

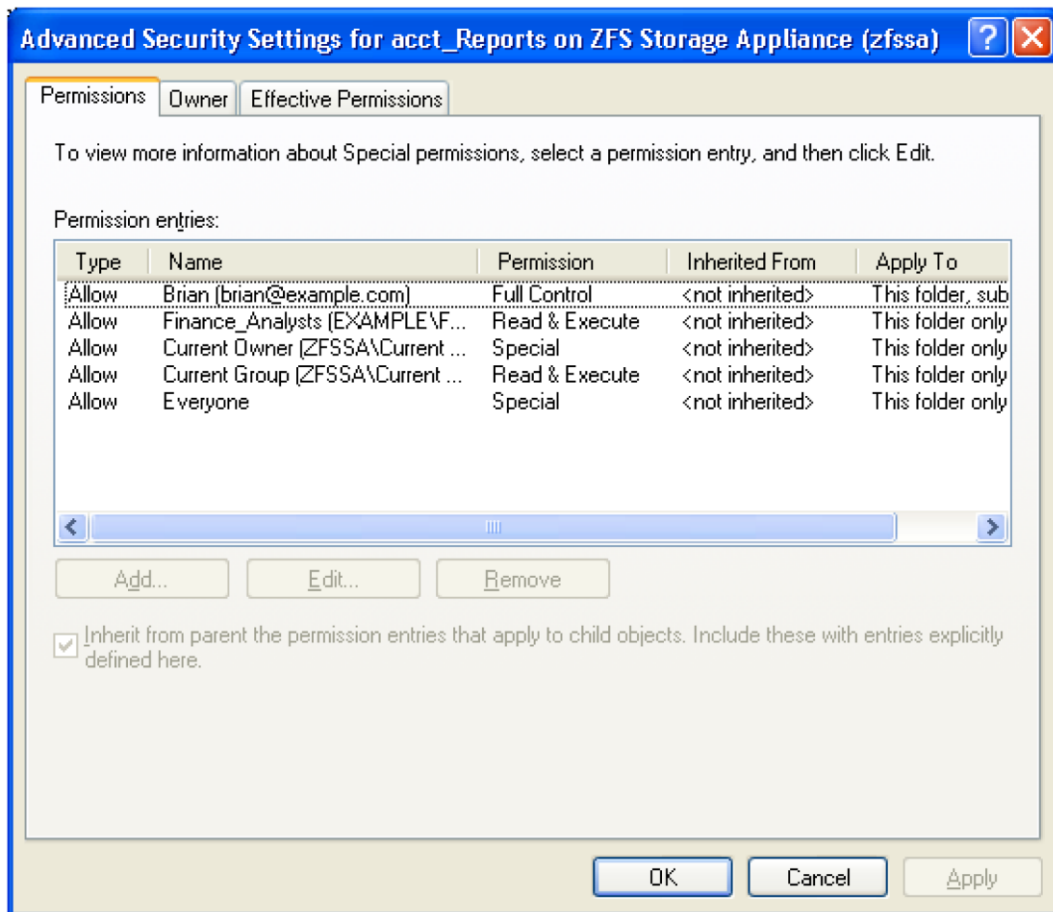


図40 : Windows XPのエクスプローラーの特殊なアクセス許可

次の図に、Windows 2003以降の特殊なアクセス許可の場所を示します。

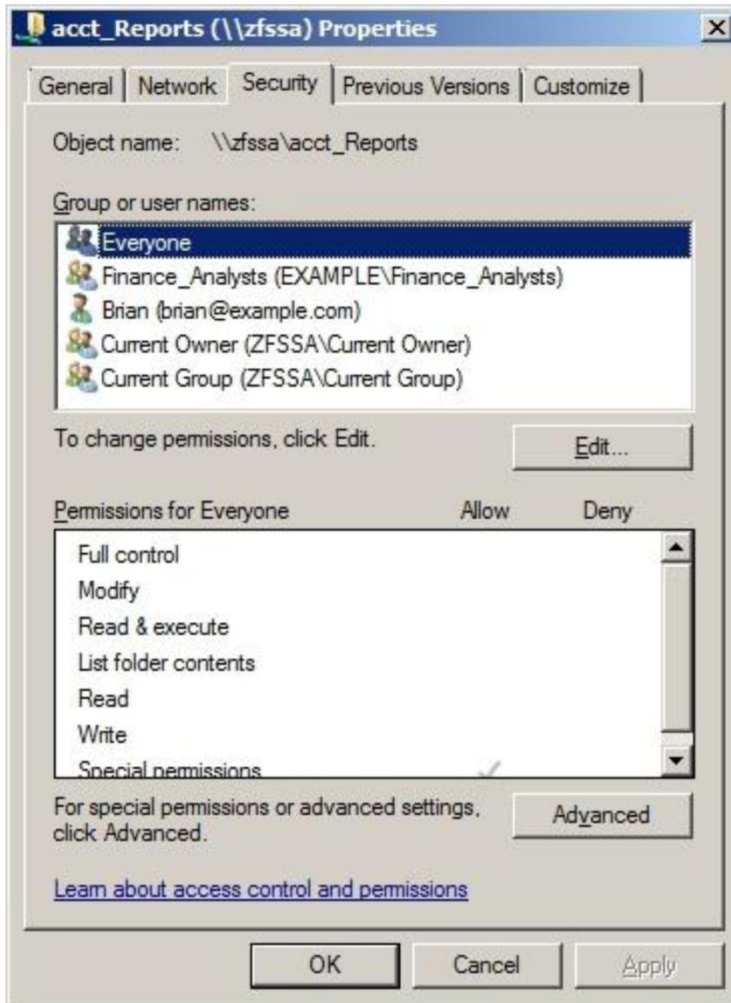


図41 : Windows Server 2003以降の特殊なアクセス許可とプロパティの表示

ルート・フォルダのアクセス許可の変更は、Windowsサーバーとアプライアンスのいずれからでも実行できます。Windows側でアクセス許可を変更した場合は、アクセス許可を上書きしないように注意してください。

Windows Server 2008 R2でのシェア管理

図42に示すように、Windows Server 2008 R2は、シェアのルート・ディレクトリを管理するための、コンピュータの管理スナップインを備えています。コンピュータの管理ユーティリティの制限のために、1度に管理できるサーバーは1つだけです。



図42：コンピュータの管理コンソール

Oracle ZFS Storage Applianceを管理するには、「コンピュータの管理（ローカル）」ツリー項目を右クリックし、「別のコンピュータへ接続」を選択すると、図43に示す選択のダイアログ・ボックスが表示されます。



図43：Oracle ZFS Storage Applianceの接続

登録されているOracle ZFS Storage Applianceの名前を入力し、「OK」をクリックします。

図44に示すように、「システムツール」→「共有フォルダ」ツリーを展開して「共有」を選択すると、Oracle ZFS Storage Applianceの構成済みの共有が表示されます。

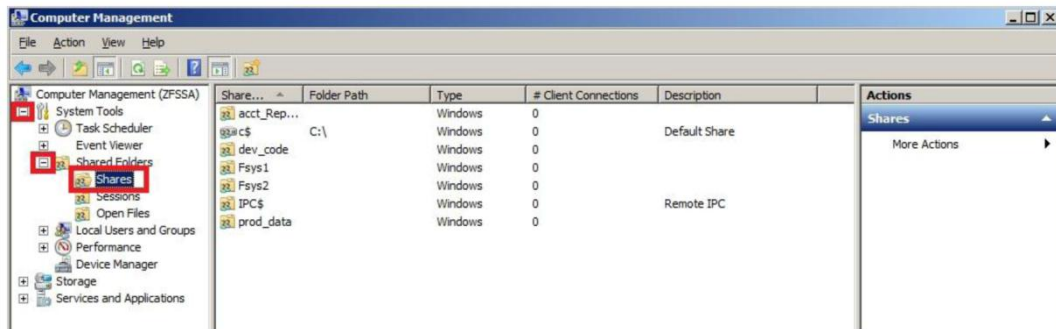


図44：コンピュータの管理ウィンドウのアプライアンスの共有の表示

図45に示すように、コンピュータの管理コンソールで現在のセッションも表示できます。

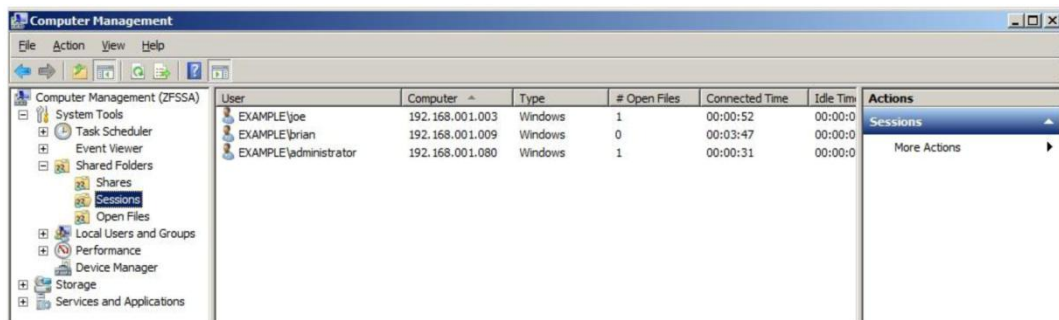


図45：コンピュータの管理ウィンドウでの現在のSMBセッションの表示

Active Directoryへのシェアの公開

シェアを公開すると、大規模なAD環境でリソースを簡単に見つけることができます。Active Directoryにシェアを公開すると、ユーザーは、Windowsデスクトップのスタート・メニューの検索機能を使用し、IDまたは説明に基づいてリモートシェアを見つけることができます。Active Directoryにシェアを公開するには、ファイル・サーバーの管理コンソールを開いて「共有」をクリックし、公開するシェアの名前を右クリックします。「プロパティ」をクリックしてから、「公開」タブを選択し、図46に示すように、「Active Directoryでこの共有を公開する」をオンにします。

検索可能な説明とキーワードを指定すると、このリソースを検索するのにさらに役立ちます。

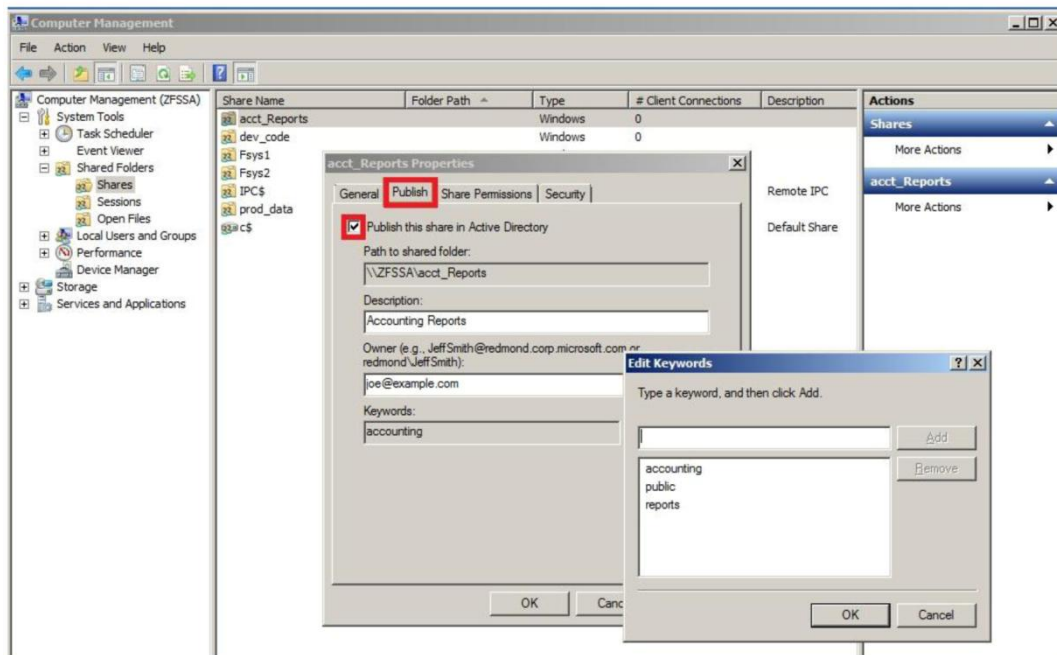


図46：検索可能な説明とキーワードを指定した、Active Directoryでのシェアの公開

データの移行

他のデバイスでホストされている別のSMB共有からデータを移行する場合、ZFSで使用されているACLによってNTのACLが完全にサポートされます。そのため、移行時にACLの構成が失われたり一部の構成が欠けることはありません。

DFSターゲット

Windows Server 2003 R2以降で分散ファイル・システム (DFS) ソリューションを使用すると、管理者はネットワーク全体のシェアフォルダを名前空間と呼ばれる仮想ツリー・フォルダにグループ化できます。Oracle ZFS Storage Applianceソフトウェアの最新リリース (最小ソフトウェア・バージョン要件は2010. Q3. 4. 1) では、アプライアンスのSMB共有をDFSターゲットとして機能させることができます。名前空間のルートが、Active Directory内の別のオブジェクトですでにアクティブになっている必要があります。Oracle ZFS Storage ApplianceのSMB共有をターゲットとして任意のDFSルートに追加できます。

Oracle ZFS Storage ApplianceのSMB共有をターゲットまたはDFS紹介として追加するには、既存のDFSルート共有で「フォルダの追加」をクリックします。図47の例に、ドメイン全体の共有 `\\example\HR` を示します。ルート共有の下で共有するSMB共有のパスを入力し、フォルダに一意的な名前を指定します。この例では、あるOracle ZFS Storage ApplianceのシェアFormsを別のOracle ZFS Storage ApplianceのシェアReportsとともに追加しています。

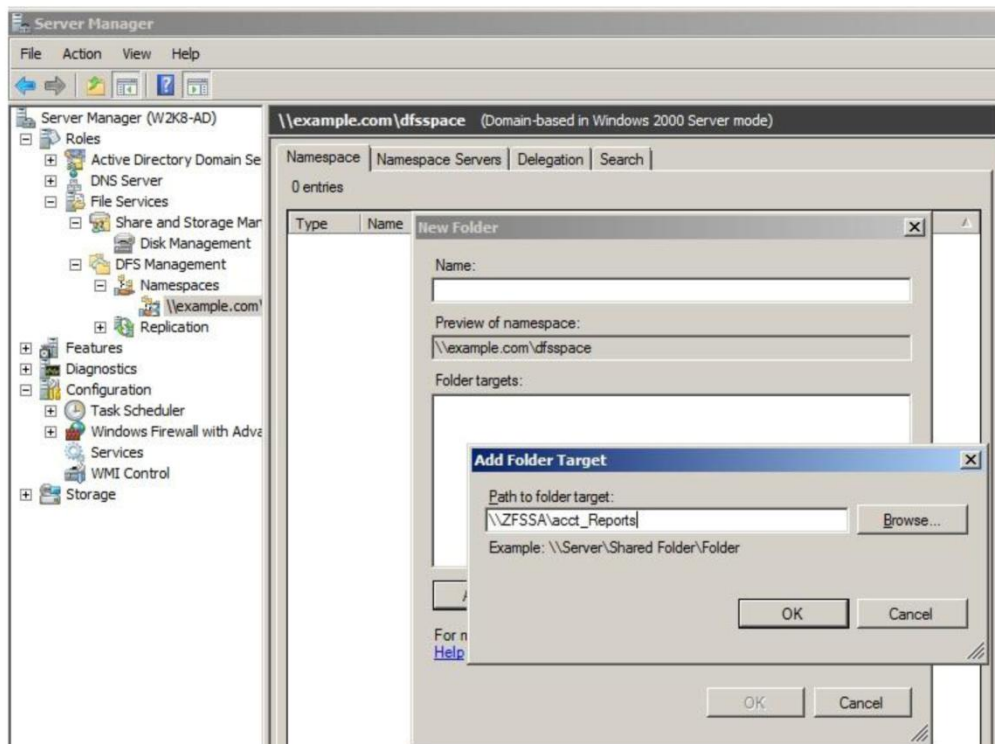


図47：DFSターゲットの作成

図48に示すように、両方のシェアがルート\\example.com\dfsspaceに配置されています。

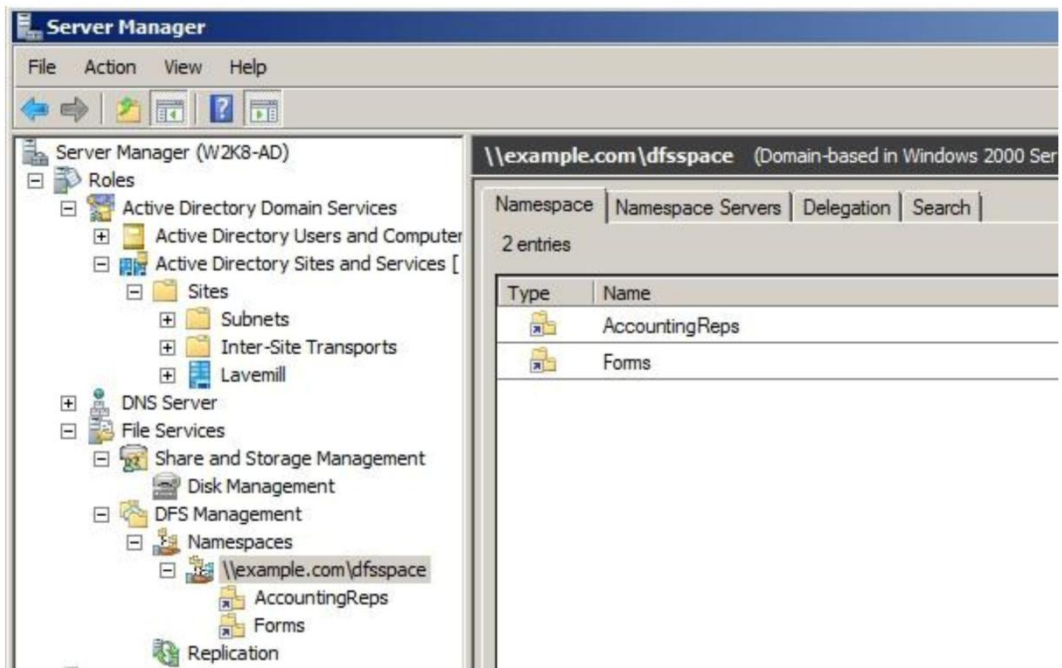


図48：作成したDFS共有の表示

クライアントで表示した場合、\\example.com\dfsspaceを参照すると、図49に示すように、FormsとAccountingRepsは別々のOracle ZFS Storage Applianceから提供されていますが、この両方が同じディレクトリ・ツリーに表示されます。

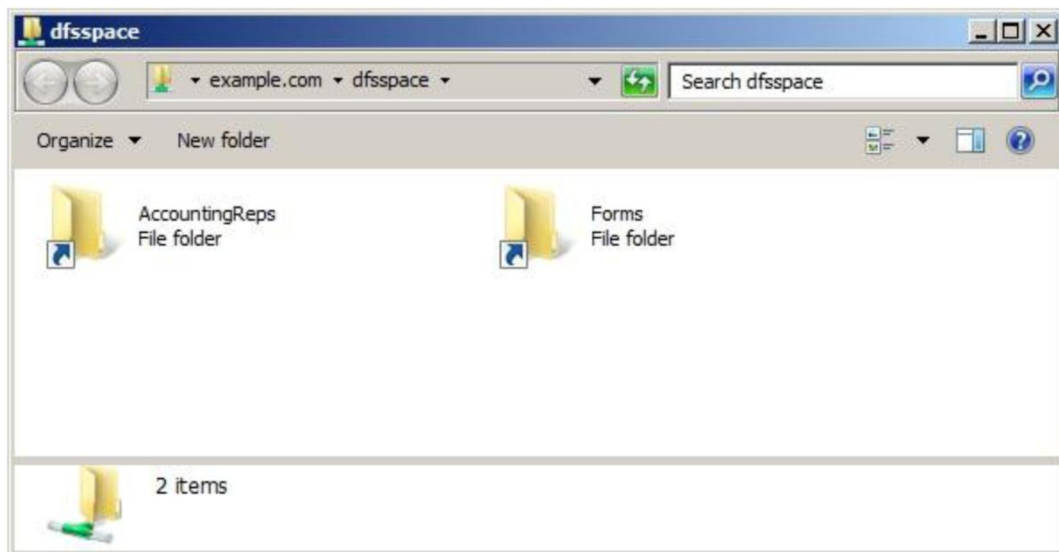


図49：Windowsクライアントで表示したDFS共有

スナップショット

プロジェクトとシェアでスナップショットを有効にできます。シェアには、プロジェクトからスナップショット・ポリシーを継承するか、独自のスケジュールを設定できます。スナップショットを有効にすると、ファイルの一貫性を保つとともに、ファイルのバージョン管理を実行できます。`.zfs`フォルダ内でスナップショットを参照し、ファイルをすばやく簡単にリカバリできます。デフォルトでは、プロジェクトの`.zfs/snapshot visibility`プロパティは“Hidden”に設定されます。クライアント・システムから`.zfs`フォルダを参照するためには、「Visible」を選択している必要があります。

スナップショットを作成するには、プロジェクトまたはシェアにスナップショットを手動で実行するか、スナップショットを実行するスケジュールを作成する必要があります。図50に、デフォルトのスナップショット・スケジュールのページを示します。

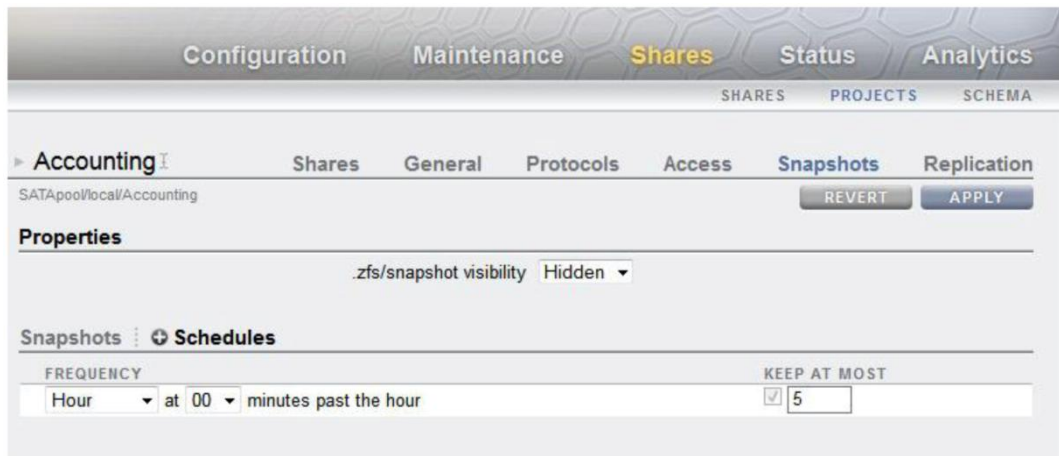


図50：デフォルトのスナップショット・スケジュール

図51に示すように、「Snapshot」オプションを選択すると、既存のスナップショットをプロジェクト・レベルまたは個々のシェアレベルで表示できます。

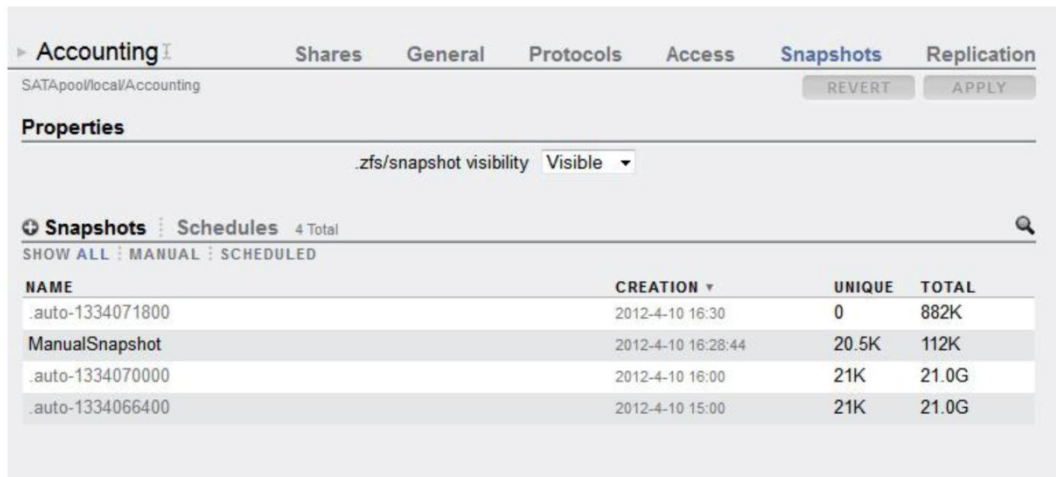


図51：既存のスナップショット

.zfs/snapshot visibilityを“Visible”に設定している場合、コピーする個々のファイルを.zfsフォルダで参照して、すばやくリストアできます。図52に、Windowsエクスプローラーのフォルダを示します。

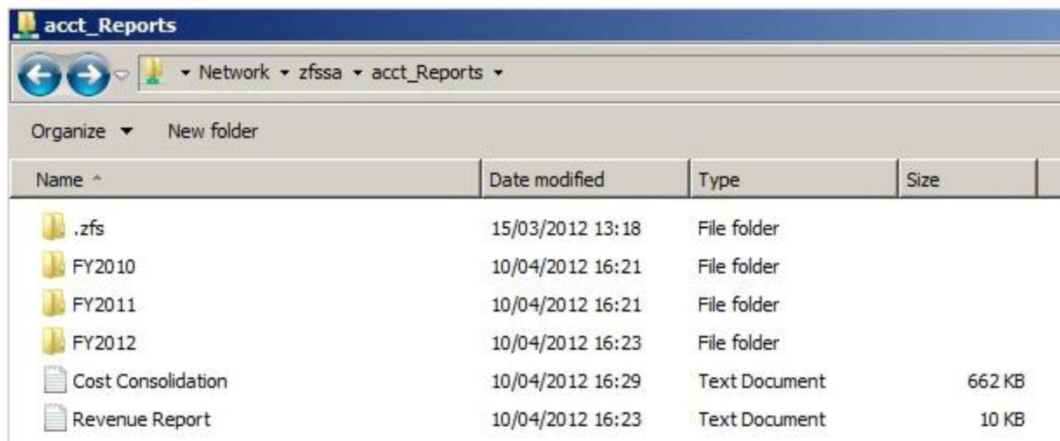


図52：Windowsエクスプローラーのスナップショットの表示

図53に、.zfsという名前のディレクトリに含まれているスナップショット・ファイルを示します。

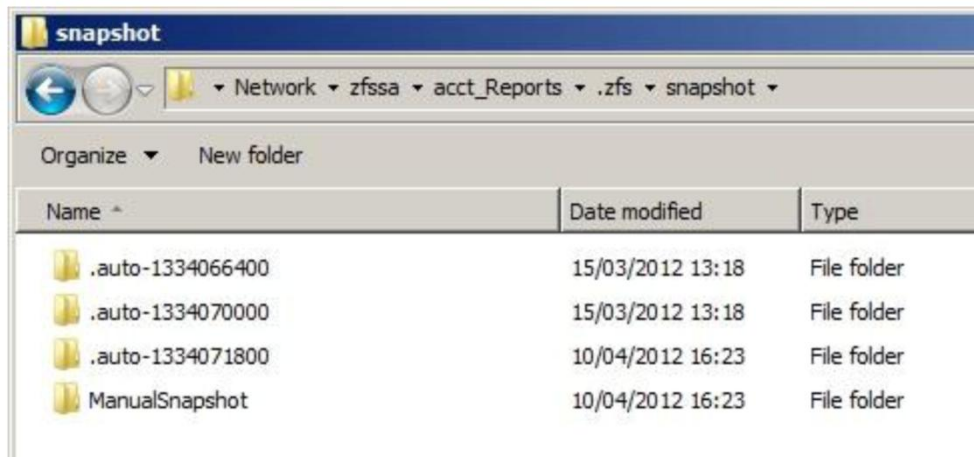


図53 : zfsスナップショット・フォルダを展開したもの

Analytics

Analyticsは、アプライアンスで送受信したデータの量に加えて、関連したファイルとクライアント、レイテンシなどのさらに詳細な情報を測定できる便利なツールです。

Analyticsを使用すると、SMBを表示した次の9種類の情報を取得できます。

- 操作のタイプで分類したSMB操作
- クライアントで分類したSMB操作
- ファイル名で分類したSMB操作
- シェアで分類したSMB操作
- プロジェクトで分類したSMB操作
- レイテンシで分類したSMB操作
- サイズで分類したSMB操作
- オフセットで分類したSMB操作
- SMB操作の生の統計情報（1秒あたりの操作数）

Analyticsでは、図54に示すように、SMBプロトコルのパフォーマンス統計情報をさまざまなタイプの操作で分類できます。

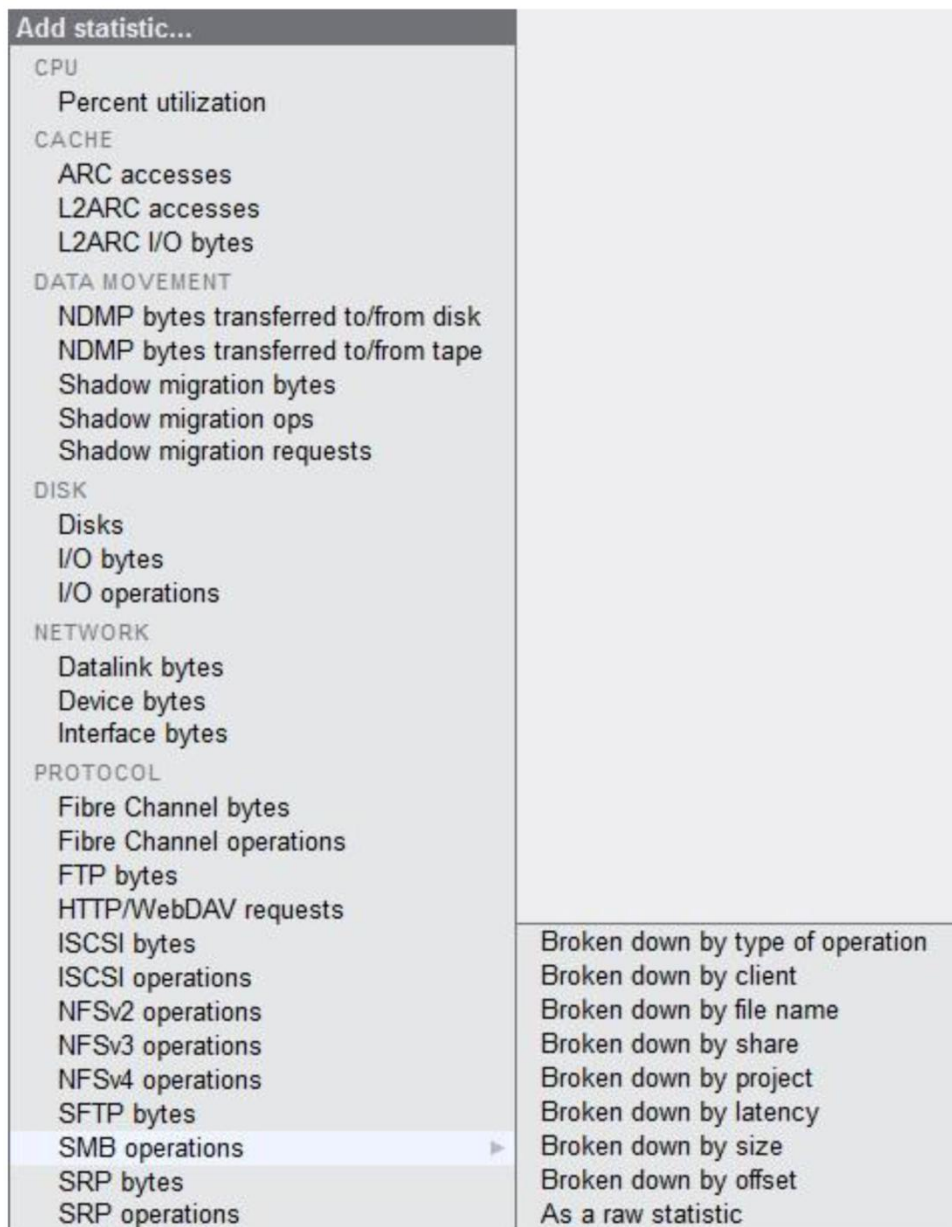


図54 : SMB操作の分析の選択

図55に示すように、クライアント別に1秒あたりでSMB操作を表示して、アクティビティのおおまかな概要を確認できます。

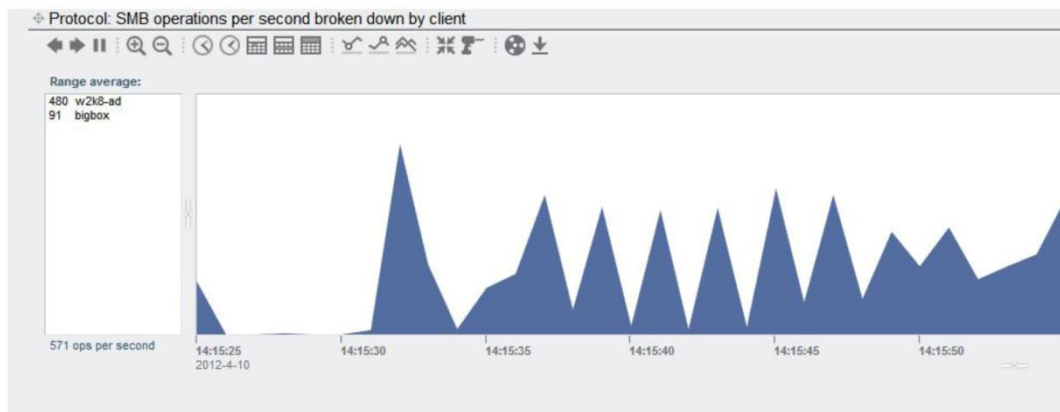


図55：クライアント別のSMB操作の分析

特定のクライアントのアクティビティが他のクライアントよりも多い場合、そのクライアントをドリルダウンして、図44に示すようにさらに詳しいデータを表示できます。この例では、w2k8-adでbigboxよりも多くのI/Oが開始されています。強調表示されているアクセスを図で表示するには、図56に示すように、“Range Average”ボックスでホスト名をクリックすると、選択したホストが別の色で表示されます。

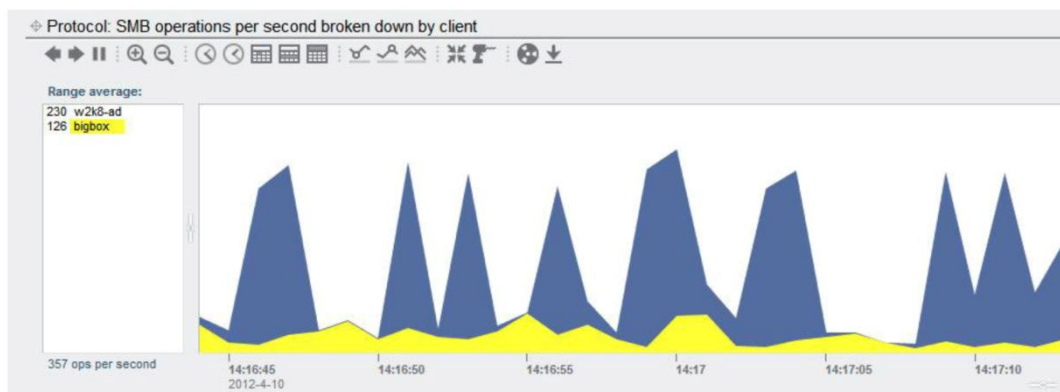


図56：詳しいデータを表示する特定のクライアントの選択

w2k8-adで実行されていることを正確に表示するために、特定のホストをドリルダウンしてさらに詳しい情報を表示できます。もっともアクセスの多いファイルを表示するのに役立ちます。ファイルを表示するには、w2k8-adを選択し、ドリル・アイコンをクリックして、ファイル名別に分類されたSMB処理を選択します。

図57の表示には、ファイル名、シェア、およびプロジェクト別のSMB操作が含まれており、もっとも要求の多いリソースを判別するのに役立ちます。これらの分析は、ストレージの問題のトラブルシューティング、ロードバランシング、および容量計画に役立ちます。

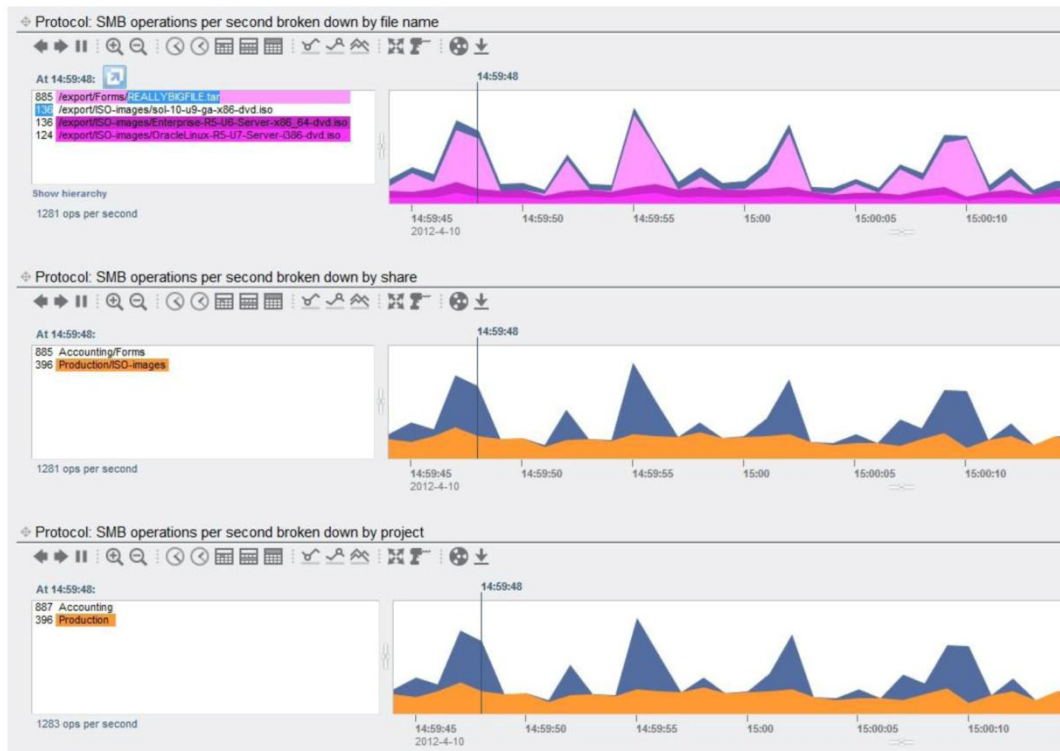


図57: SMBのファイル名、シェア、プロジェクトの分析

操作のレイテンシをグラフ化すると、問題の診断に非常に役立ちます。図58の例は、253の操作が131マイクロ秒未満で完了しており、197の操作が131マイクロ秒で完了していることを示しています。Y軸はレイテンシを表し、X軸は時刻を表しています。下部付近の濃い帯は、より多くのデータが短い応答時間で処理されていることを示し、薄い帯は長い応答時間がかかっていることを示しています。

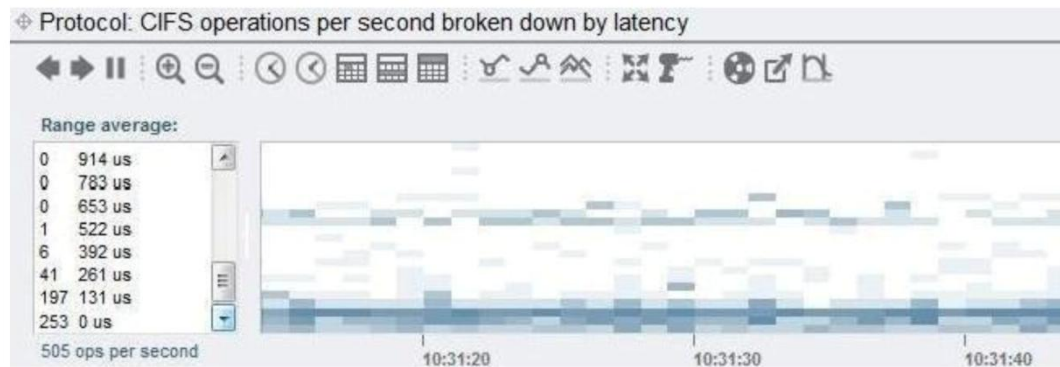


図58: SMBの分析による操作のレイテンシの表示

図59に、処理されたI/O要求のサイズと要求のレイテンシを示します。この例の大部分の転送は32K（サイズのグラフの上部の濃い帯）で、マイクロ秒のタイミング（レイテンシのグラフの下部の濃い帯）で処理されています。



図59：SMBの分析による操作のサイズとレイテンシの表示

結論

Oracle ZFS Storage Applianceは、Windows Serverのツールセットおよび概念と非常に緊密に統合できるため、Windows Server管理者が使い慣れた形式でストレージ・リソースを直感的に制御および管理できます。

ネイティブのパフォーマンス管理ツール、アイデンティティ・マッピング機能、およびデータ保護機能とともに、Oracle ZFS Storage ApplianceはWindows Server環境に適合するとともに、これを補強します。

参考資料

『Sun ZFS Storage 7000システム管理ガイド』	docs.oracle.com/cd/E22471_01/pdf/820-4167.pdf
『Configuring the Sun ZFS Storage Appliance to Use IDMU to Map Identities Between Active Directory and NIS』	Sun NAS Storageドキュメンテーションのホワイト・ペーパー (http://www.oracle.com/technetwork/jp/server-storage/sun-unified-storage/documentation/index.html)
『Oracle ZFS Storage Appliance Rule-based Identity Mapping』	
『Windows Serverで権限のあるタイム・サーバーを構成する方法』	http://support.microsoft.com/kb/816042
Oracle ZFS Storage Applianceの情報	www.oracle.com/jp/products/servers-storage/storage/nas/overview/index.html
Microsoft Server 2012 R2	www.microsoft.com/en-us/server-cloud/windows-server/default.aspx
Microsoft Server Active Directoryの概要	www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx
Microsoft分散ファイル・システムの概要	technet.microsoft.com/en-us/library/cc738688%28v=ws.10%29.aspx



Microsoft ServerとOracle ZFS

Storage Applianceの統合

2012年7月、バージョン2.0

2014年1月、バージョン2.1

著者：Ryan H PrattおよびAndrew Ness



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

Copyright © 2012, 2014, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

IntelおよびIntel XeonはIntel Corporationの商標または登録商標です。すべてのSPARC商標はライセンスに基づいて使用されるSPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴおよびAMD Opteronロゴは、Advanced Micro Devicesの商標または登録商標です。UNIXはX/Open Company, Ltd.によってライセンス提供された登録商標です。0611

Hardware and Software, Engineered to Work Together