An Oracle Technical White Paper

January 2014, v2.1

Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Implementation Guide for SMB Deployment
# Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

## Executive Overview

```
3
```

## Introduction

```
3
```

## Prerequisites

```
5

Operating System Prerequisites
5
Storage System Prerequisites
5
```

## Best Practices and Principles for System Configuration with the Oracle ZFS Storage Appliance

```
7

Network
7
Oracle ZFS Storage Appliance Clusters
7
Microsoft Cluster Service (MSCS)
7
Users
7
```

## Implementing the Principles Through the Configuration

```
8

Configuring the System
8
Synching to the Network Time Protocol (NTP) Server
8
Creating Local Users for Workgroup Access
12
Connecting to Domain Name Service (DNS) Servers Used by Active Directory
13
Configuring to Authenticate with Active Directory
15
```

## Configuring Services

```
18

Selecting SMB Services Protocol
18
Creating Shares – Projects and Filesystems
19
```

## Configuring a Share

```
23

Configuring Share ACLs in Workgroup Mode
30
Configuring Share ACLs in Domain Mode
31
```

## Share Management from Windows Server 2008 R2

```
36
Publishing Shares to Active Directory
38
```

## Data Migration

```
40
```
Executive Overview

The Oracle ZFS Storage Appliance is designed to integrate with core Microsoft Server tools and utilities. This document discusses the best practices and deployment procedures to complete the integration with an existing Windows Server infrastructure.

From initial registration with an Active Directory Domain Controller to publishing shares in Active Directory and configuring as a Distributed File System (DFS) target, the most common configurations and tasks are explained with examples.

To understand the information presented here, readers should already have a basic knowledge of Windows Server environments and an initially configured Oracle ZFS Storage Appliance with a network setup that includes an IP, netmask and gateway, a configured storage pool, and clocks synchronized between the appliance and client machines (NTP).

Introduction

The Oracle ZFS Storage Appliance series allows for Server Message Block (SMB) (also called Common Internet File System or CIFS) authentication with an Active Directory database or using local users on the appliance in workgroup mode. The Active Directory service provides access to a Microsoft Active Directory database, which stores information about users, groups, shares, and other shared objects. There is no facility to store Windows users in LDAP.

When a resource is added as a member to Active Directory, it is discoverable within the domain. Active Directory works on a container basis or Organization Unit (OU) basis. Resources can be separated into different OUs for administrative purposes. Administrative tasks can be accomplished within an OU.

When the Oracle ZFS Storage Appliance is joined to a domain, a computer account object with the appliance's name is created within AD by the joining process.
This document focuses on the process of creating and sharing filesystems in both domain and workgroup mode, joining a domain, mounting SMB shares within the domain, and managing object rights.

After reading this document, you should be able to:

- List the prerequisites for a successful Active Directory membership
- Use local users for SMB shares
- Join the Oracle ZFS Storage Appliance to an Active Directory domain
- Set permissions for a share with both local and Active Directory users
- Set up a DFS target
- Publish shares in Active Directory
- Understand basic analytics that are available

NOTE: References to Sun ZFS Storage Appliance, Sun ZFS Storage 7000, and ZFS Storage Appliance all refer to the same family of Oracle ZFS Storage Appliance products. Some cited screen code or documentation may still carry these legacy naming conventions.
Prerequisites

The following prerequisites must be met in order to successfully implement the procedures outlined in this document.

Operating System Prerequisites

The following domain controllers are currently supported:

- Microsoft Windows Server 2000 SP4
- Windows Server 2003 (or 2003 R2)
- Windows Server 2008 (or 2008 R2)

Windows NT 4.0 domain controllers are not currently supported.

This document’s instructions are based on the use of Microsoft Windows Server 2003 or later for implementing Active Directory domains.

It is important that the client, server, domain controller and appliance clocks are all synchronized (see the “Synching to the Network Time Protocol (NTP) Server” section under "Integrating the Principles Through the Configuration Steps").

Storage System Prerequisites

Make sure you have installed the latest version of the Oracle ZFS Storage Appliance software. To download it, go to Oracle’s “My Oracle Support” web site, “Patches & Updates” section. Using the search string “Sun ZFS Storage Appliance”, select the latest release from the dropdown box and click “Search” as shown in Figure 1.

![Figure 1. Oracle My Support Patches and Updates screen](image)
SMB, NTP client and Active Directory are default features provided by the Oracle ZFS Storage Appliance software.

- Clocks must be synchronized manually or via NTP. When a filesystem is shared using SMB, the client clocks must be synchronized to within five minutes of the appliance clock to avoid user authentication errors. One way to ensure clock synchronization is to configure the appliance and the SMB clients to use the same NTP server, preferably the Domain Controller itself.

- If link aggregation or VLAN datalinks will be used, the connected switch ports must be configured accordingly.

- Although a storage pool is not required to configure many of the features, you must have an underlying storage pool with available space in order to create a filesystem, LUN, or share.

Before attempting to join an Active Directory domain, configure the Oracle ZFS Storage Appliance for DNS service. To set up DNS, use the DNS management plug-in for Windows to create a host ("A") record so that name resolution may occur. The appliance will automatically find the Domain Controller (DC) for the specified domain by retrieving the DNS SRV record for a DC.

Note: If the appliance is configured to use a DNS server that is not the Active Directory DC, then the DNS server(s) must be configured with an appropriate DNS SRV record. You can use a separate non-Windows DNS server, but it will require that you manually add to that DNS all the DNS SRV records needed to inter-operate with the Active Directory domain. However, if you use Active Directory as your DNS server, everything is configured by default.
Best Practices and Principles for System Configuration with the Oracle ZFS Storage Appliance

Consider the following principles and suggestions for the listed features during the configuration process.

Network

Active Directory or SMB shares do not require any specific networking setup tasks. Devices, datalinks, interfaces, LACP link aggregations, and IP multipathing (IPMP) groups are all supported. For data traffic that is not part of a public or management LAN, create a private network connection. For greater bandwidth needs, implement 10Gb interfaces and/or link aggregations.

Oracle ZFS Storage Appliance Clusters

Oracle ZFS Storage Appliance clustering is fully supported in an Active Directory environment with CIFS or NFS shares. In the event of a failover, any shares are automatically moved to the alternate head.

This document does not cover clustering. For more information regarding Oracle ZFS Storage Appliance clustering, refer to the Sun ZFS Storage 7000 System Administration Guide available at http://docs.oracle.com/cd/E22471_01/pdf/820-4167.pdf.

Microsoft Cluster Service (MSCS)

To create shareable cluster resources on an MSCS cluster, mount a LUN using iSCSI and then share it through the cluster as a SMB share. Further information on Microsoft Cluster Service is outside of the scope of this document.

Users

The Users screen is used both for appliance administration delegation and control, as well as setting local user permissions when using the appliance in workgroup mode. If the appliance is set to workgroup mode, local users must be created for access rights. If the appliance is joined to an Active Directory domain, this section is not required for share permissions. Administration delegation is not covered in this document.

For environments where there is a mix of UNIX and Windows users and there is a desire to have a mapping between Windows user and a corresponding Solaris, UNIX, or Linux users, an identity mapping service is provided. This feature will not be discussed in this document but is discussed in the Oracle Technical Network (OTN) document “Configuring the Oracle ZFS Storage Appliance to Use IDMU to Map Identities” as well as “Oracle ZFS Storage Appliance Rule-Based Identity Mapping” available in the white paper collection of the Sun

Implementing the Principles Through the Configuration

The following instructions provide step-by-step guidance and examples for configuring systems and services to function together, integrating the Oracle ZFS Storage Appliance with the Windows server environment.

Configuring the System

The Oracle ZFS Storage Appliance requires settings for the following system-level features and/or functions to integrate it with the Windows environment:

- Network Time Protocol Server
- User account for access
- Domain Name Service (DNS) Server
- Active Directory

Synching to the Network Time Protocol (NTP) Server

To configure the Oracle ZFS Storage Appliance to use the services of an NTP server, use a web browser to connect to the Oracle ZFS Storage Appliance browser user interface at port 215 with a secured connection: https://sunzfssa.example.com:215.

The following figure shows the browser login screen.
Once you are logged in, you should see the main Oracle ZFS Storage Appliance menu screen, shown in Figure 3.
By clicking on the Configuration tab at the top of the screen, then the SERVICES subtab underneath it and, finally, on the NTP entry under System Settings as shown in Figure 3, you will see the NTP configuration panel, shown in Figure 4.
Enter the fully qualified domain name (FQDN) or IP address of the common NTP server. Though this step is not required before or after joining an Active Directory domain, the process of joining the domain, as well as user authentication, may fail if there is greater than a five-minute time difference between the domain controller and the Oracle ZFS Storage Appliance. It is not required that the NTP server be the Active Directory domain controller.

For instructions on how to configure a Windows server for NTP, see [http://support.microsoft.com/kb/816042](http://support.microsoft.com/kb/816042). If required, add NTP authentication keys (using the + sign next to NTP Authentication Keys) according to the instructions in the document. The NTP keys are used to ensure secure time synchronization among authorized servers and clients, which is particularly important for time-critical applications such as authentication.

Once you click apply, a dialog box asking whether to enable the service if it is not already enabled will appear. Click enable. Once enabled, the NTP service button should be green and the appliance time should sync with the clients and domain controller.
Creating Local Users for Workgroup Access

For workgroup access only, you must create a local user on the Oracle ZFS Storage Appliance in order for a share to be mounted on a client system (as shown in Figure 1). Under Configuration, then Users, click the + icon to the left of the Users title as shown in Figure 5.

![Figure 5. Adding a user](image)

The Add User dialog window, as shown in Figure 6, displays.

![Figure 6. Add User dialog window](image)

Select the Local Only radio button, then fill in the information for the Username, Full Name, Password, and Confirm (password confirmation) entries. If this user does not need the right to administer the box, leave ‘Require session annotation’ and ‘Kiosk user’ unchecked. To prevent this user from logging into the appliance, you also must uncheck any role that is specified at the bottom.
If possible, mirror the appliance local user with the Windows local user defined on the workgroup member machines.

Matching the usernames/passwords across the appliance and the workgroup-mode client eliminates the need to explicitly authenticate each time a share is mapped in workgroup mode. This user may now be assigned share permissions and can now connect to the appliance and map shares by navigating through the Network Neighborhood or the Map Network Drive interface.

Clicking the Add button completes the operation, which is confirmed as the added user’s name displays in the list of users as shown in Figure 7.

![Figure 7. Confirming the user addition](image)

Connecting to Domain Name Service (DNS) Servers Used by Active Directory

In order to use the DNS-based Active Directory services, configure the Oracle ZFS Storage Appliance to use the same DNS servers as the Active Directory domain controllers. To do so, select Configuration from the top tab set, Services from the subtab set, and DNS from the Systems Settings section of the configuration services displayed as shown in Figure 8.
The DNS configuration panel shown in Figure 9 displays. Enter the DNS domain name and the IP address of the DNS server in the relevant boxes. You can specify additional DNS server IP addresses by clicking on the + icon to the right of the “DNS Server(s)” title. Clicking Apply will complete the DNS configuration.
Configuring to Authenticate with Active Directory

In Domain mode, the Oracle ZFS Storage Appliance offers SMB/CIFS file services as a member server in a Microsoft Active Directory domain. The Oracle ZFS Storage Appliance may only be a member of a single domain, but transitive, interdomain and cross forest trusts are fully supported to extend functionality across the Windows namespace.

Instead of enabling and disabling the Active Directory service directly, you can modify the service by joining a domain or a workgroup. Joining a domain involves automatically creating a computer account for the appliance in the given Active Directory domain. Once you establish the computer account, the appliance can securely query the database for information about users, groups, and shares.

In Active Directory, every resource must have an account. This includes users, workstations, servers and other devices that participate in an Active Directory domain. Joining the Oracle ZFS Storage Appliance into the domain automatically creates a computer account.

Windows users who have an identity established in Active Directory can map allowed shares on the appliance as soon as the appliance has successfully joined the domain. When a Windows domain user attempts to map a share, the Oracle ZFS Storage Appliance will validate the Windows user's name by authenticating the user's identity with the domain controller and obtaining the user's credentials and access permissions. According to the trust rules of Active Directory, users in any trusted domain in the Active Directory forest can access the appliance if they have been granted sufficient privileges. Similarly, users in trusted forests may also access appliance resources.

Modifying the Oracle ZFS Storage Appliance configuration for Directory Services authentication from Active Directory service to a workgroup implicitly means exiting an Active Directory domain. This results in all SMB clients who are stored in the Active Directory database being unable to connect to shares.

Locate the Active Directory configuration panel by clicking the top-level Configuration tab, then the Services subtab, and selecting Active Directory from the Directory Services section as shown in Figure 10.
Figure 10. Configuring Directory Services for Active Directory

After selecting Active Directory, the following service screen appears. From this display, you can join a domain.

Figure 11. Unconfigured Active Directory state
Clicking on the Join Domain button (seen in Figure 11) will display the Active Directory configuration panel as shown in Figure 12.

![Join Domain button](image)

To join a domain, enter the Active Directory domain, an administrative user's name, and the administrative password below.

- **Active Directory Domain**: example.com
- **Administrative User**: administrator
- **Administrative Password**: ********
- **Additional DNS Search Path**: 

![Active Directory configuration panel](image)

Figure 12. Active Directory configuration panel

To join an Active Directory domain, enter the fully qualified domain name (FQDN) in the Active Directory Domain window, a user with domain administrator credentials, and the administrator's password. Clicking Apply initiates the join request. This step commonly takes approximately 30 seconds. Once the appliance has been joined to the domain, the Active Directory service will start and show online. Current details of the domain will display, as shown in Figure 13.

![Domain membership of Active Directory](image)

Figure 13. Domain membership of Active Directory

If the operation fails with the error message as shown in Figure 14, check the DNS configuration of the Oracle ZFS Storage Appliance to ensure that it contains the same details as the Active Directory domain controller DNS configuration.
The appliance could not find the appropriate SRV record (example.com) for the Active Directory domain in any DNS servers. The DNS server(s) must be configured with an appropriate DNS SRV record. After checking that the Active Directory domain is correct, ensure the appropriate DNS SRV record is exported by the DNS server(s).

Figure 14. Active Directory join request fails due to DNS configuration issues

To display the computer account for the appliance, log on to the domain controller and access the Active Directory Users and Computers console. A computer account for the appliance has been created in the generic “Computers” container, as shown in Figure 15.

Figure 15. Active Directory Users and Computers display

Configuring Services

The following steps establish the sharing and accessibility of filesystems between the Oracle ZFS Storage Appliance and the Windows environment, through the data access protocol SMB/CIFS and through share creation and configuration.

Selecting SMB Services Protocol

The SMB service provides access to the filesystems using the SMB/CIFS protocol. Filesystems must be configured to share using SMB from the Shares configuration. The first
step is to enable the service from the Configuration, Services tab and click on the power button icon to the right of the SMB entry as shown in Figure 16 if it is shown as Disabled. If the SMB entry is shown as Online, do not change the setting.

Figure 16. Enabling SMB/CIFS on the Oracle ZFS Storage Appliance

Creating Shares – Projects and Filesystems

All filesystems and LUNs are grouped into projects. A project defines a common administrative control point for managing shares. All shares within a project can share common settings, and quotas can be enforced at the project level in addition to the share level. You can also use projects solely for grouping logically related shares together, so their common attributes (such as accumulated space) can be accessed from a single point. Adding a prefix to the project helps identify the project name with the resource (for example, dev_code, where dev is the prefix assigned to the Development project name and code is the share name).

Configure the project by modifying the SMB section of the Project Protocols and setting the Resource Name to “on” – after which all shares created from this project, unless otherwise configured, will be accessible with the project_share naming scheme. An example of this is shown in Figure 17.
By default, the Oracle ZFS Storage Appliance creates a single default project when a storage pool is first configured. It is possible to create all shares within this default project, although for larger-sized environments, creating additional projects is strongly recommended, if only for organizational purposes.

Windows environments have two layers of permissions in shared folders: permissions on the share and permissions on the underlying filesystem. Between two permissions, only the most restrictive permission is enforced. The recommended practice is to choose and consistently use one layer of permissions.

Often the nomenclature of filesystem permissions, file permissions, folder permissions and NTFS permissions are used interchangeably. On the Oracle ZFS Storage Appliance, these permissions are referred to as root directory access permission. You can view and modify them under the Access tab of the filesystem tab in the BUI.

Shares can be filesystems or block-protocol LUNs (iSCSI or Fibre Channel). Filesystems are created and then exported as SMB shares.

Shares can be grouped into projects for common administrative purposes, including space management, common settings and replication control. A share does not require a static size for the filesystems, as they are thin provisioned by default. If a certain amount of reserved space is required, you can use quotas and reservations to set it.
The default permissions on a filesystem creation are set to read, write and execute for the owner, with no permissions for everyone else. This conservative approach protects against unintentionally opening permissions up too broadly. You can change this default setting at the project level under the General tab of the Projects display, as shown in Figure 18.

In creating a new filesystem, leave the default permissions unchanged, as Windows only refers to the access control list (ACL) and not the 3x3 permission boxes seen in Figure 18.

The default Share Level ACL setting provides wide access to Everyone. The default filesystem ACL settings are "nobody" as User (owner), "other" as Group, and only the User (owner) with permission to read, write and execute, as seen in the highlighted boxes in Figure 18. A Windows best practice is to control ACLs from the filesystem level rather than the share level. As mentioned earlier, maintaining both may be difficult, so choose one level but not both. In order to simplify management of the appliance in a pure Windows environment, set both the share level and filesystem level permissions to full control for everyone and then manage the individual permissions from a Windows client. The following three figures show the screen sequence for achieving. Figure 19 shows how to reach the Share Level ACL configuration panel.
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Figure 19. Shares configuration panel

Figure 20 shows the Share Level ACL panel, with “Everyone” allowed “Full Control.”

Figure 20. Modifying the Share Level ACL setting

Figure 21 shows an example of the specific permissions that accompany everyone having full control.
Figure 21. Settings associated with full access for 'everyone'

Once you affirm the selections by pressing the OK button, the updated ACL displays in the “Share Level ACL” section as shown in Figure 22.

Figure 22. Display showing full control ACL for 'everyone'

Configuring a Share

Under the Protocols tab in the project, make sure that the SMB service light is green and that the Resource Name is not set to off. Even if the SMB service is turned on, you must change the SMB Resource Name to a string so that the share will be published. Setting the Resource Name to on will present each filesystem as its filesystem name as follows \servername\filesystem. Alternatively, you may assign a prefix in the project level that will place that prefix prior to the filesystem name in order to differentiate each project’s shares from one another (such as \servername\prefix_filesystem). This convention will apply to all filesystems that are created in that project with the “inherit from project” checkbox in the SMB section of the Protocol tab marked. As shown in Figures 23 and 24, the default naming scheme for the SMB shares is set to their filesystem names by setting the
Resource Name to “on” (under the SMB section) in Figure 23 and allowing the filesystem setting to “Inherit from project” as seen in Figure 24.

Figure 23. Projects level Protocols display

Figure 24 shows the protocols at the filesystem level. A filesystem named code was created under the Development project.

Figure 24. Filesystem level Protocols tab

In a Windows client Explorer window, the shared filesystem displays as seen in Figure 25.
As shown in Figures 26 and 27, by setting a unique identifier in the Resource Name at the project level (in this example, “deptSMB”), the filesystem will inherit that prefix, an underscore and the share name as seen by any external clients (Figure 28.)

![Figure 25. Client Explorer window showing the filesystem called code](image1)

Figure 25. Client Explorer window showing the filesystem called code

A Windows client Explorer screen displays the full filesystem name, as shown in Figure 28.
Alternatively, if “Inherit from project” is not checked, you can set the Resource Name under SMB to “on” to specify the filesystem name as the share or filesystem-level unique identifier. Figure 29 shows this setting.
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Figure 29. Resource Name set to “on” in the filesystem-level Protocols tab

Figure 30 shows the results of this setting in a Windows Explorer screen.

Figure 30. Client Explorer window with Resource Name “on”
Assigning a different share name from the filesystem name, as shown in Figures 31 and 32, is supported but not recommended due to its potential for confusion. In the example, the resource name has been set to “dept1.”

Figure 31. Assigning an explicit share name at the filesystem-protocol level

Figure 32 shows the explicitly named share in a Windows client Explorer screen.

The following example shows two projects, Development and Production. Development has a share named “code” and Production has a share named “data.” A client machine would see both shares once connected to the Oracle ZFS Storage Appliance. By adding the “dev” prefix to the Development project and the “prod” prefix to the Production project, the two projects are easily distinguished.

Figure 33 shows the two shares before their naming association with their particular projects.
Figure 33. Display showing no named resource at the project level

Figure 34 shows the renamed shares, now readily associated with their projects through their respective prefixes, in the Windows client.

Figure 34. Display showing a project-level named resource
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Configuring Share ACLs in Workgroup Mode

The following examples show the steps to set ACLs on the Oracle ZFS Storage Appliance. Note: This section of the document is for workgroup mode with local users and does not apply to Active Directory users, who will be discussed later.

As shown in Figure 35, you can now see the share code from a client system, but if there is an attempt to open the code folder, permission is denied. Specific permissions may now be assigned to each local user.

![Figure 35. Default ACL permissions displayed](image)

As shown in Figure 36, read, write and execute permissions (rwx) are now given to Bob, read and execute (rx) permissions are assigned to Tim, and the owner (User) is changed to Jack. Each of these users have a password set on the appliance in the Users tab. If the appliance's user name and password match the client login user name and password on the client machine and that user has permission to at least read the share, the user will be granted access using passthru. If the user’s password is different on the client compared to the appliance, a password dialog box will display.

Jack and Bob can now create their own folders and files under code. They cannot write to or read each other's files or folders. Tim can now view the contents of code, but can do nothing else.
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Figure 36. Root directory ACL with updated permissions

Note: If the appliance is then joined to a domain after local shares and users are configured, these users and permissions will remain valid.

Configuring Share ACLs in Domain Mode

Assigning permissions for domain users is slightly different from the process for local users in workgroup mode. Once the Oracle ZFS Storage Appliance is joined to the domain, usernames must also contain the fully qualified domain name with the form username@FQDN. As shown in Figure 37, a new filesystem named Reports is being created by Joe (Joe@example.com), who will own the filesystem, but gives read and execute (rx) permissions to the accounting_users (accounting_users@example.com) domain group.
Joe, who is in the `accounting_users` domain group, can now view and traverse this share. The filesystem `Reports` has been shared with a project resource name of “acct” and the security details are shown in Figure 38.
Figure 38. Windows client’s Security tab detail for the domain-based filesystem `acct_Reports`

To grant permissions to individual users or groups of users, select “Named User” or “Named Group.” You must use a fully qualified domain name (FQDN) when assigning domain user or group permissions, as shown in Figure 39.
Figure 39. Explicit user and group addition for Brian and finance_analysts

The ZFS ACLs are held in the Special Permissions section, which you can access from the Advanced button in Windows XP's Windows Explorer (Figure 40) or from the Properties > Security tab in Windows Server 2003 and later.
Figure 40. Windows XP Explorer special permissions

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Permission</th>
<th>Inherited From</th>
<th>Apply To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Brian [<a href="mailto:brian@example.com">brian@example.com</a>]</td>
<td>Full Control</td>
<td>&lt;not inherited&gt;</td>
<td>This folder, subfolders</td>
</tr>
<tr>
<td>Allow</td>
<td>Finance_Analysts [EXAMPLE\Finance]</td>
<td>Read &amp; Execute</td>
<td>&lt;not inherited&gt;</td>
<td>This folder only</td>
</tr>
<tr>
<td>Allow</td>
<td>Current Owner (ZFSSA\Current Owner)</td>
<td>Special</td>
<td>&lt;not inherited&gt;</td>
<td>This folder only</td>
</tr>
<tr>
<td>Allow</td>
<td>Current Group (ZFSSA\Current Group)</td>
<td>Read &amp; Execute</td>
<td>&lt;not inherited&gt;</td>
<td>This folder only</td>
</tr>
<tr>
<td>Allow</td>
<td>Everyone</td>
<td>Special</td>
<td>&lt;not inherited&gt;</td>
<td>This folder only</td>
</tr>
</tbody>
</table>

To view more information about Special permissions, select a permission entry, and then click Edit.

Inherit from parent the permission entries that apply to child objects. Include those with entries explicitly defined here.
The following figure shows the location of special permissions for Windows 2003 and later.

![Figure 41. Windows Server 2003 and later special permissions and properties display](image)

You can change permissions for the root folder from the Windows server or from the appliance. Be careful not to override permissions when changing permissions on the Windows side.

**Share Management from Windows Server 2008 R2**

As shown in Figure 42, Windows Server 2008 R2 has a Computer Management snap-in which allows the management of the root directories of shares. Due to a limitation of the Computer Management utility, you can manage only one server at a time.
To manage the Oracle ZFS Storage Appliance, Right Click on the “Computer Management (Local)” tree item and select “Connect to another computer …” which will then display the selection dialog box shown in Figure 43.

Enter the registered Oracle ZFS Storage Appliance name and select “OK.”

Expanding the “System Tools > Shared Folders” tree and selecting “Shares” as shown in Figure 44 will then display the configured shares from the Oracle ZFS Storage Appliance.
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Figure 44. Viewing the Appliance shares through the Computer Management window

You can also view the current sessions through the Computer Management console as shown in Figure 45.

Figure 45. Viewing current SMB sessions in the Computer Management window

Publishing Shares to Active Directory

Publishing shares makes it easier for a resource to be found in large AD environments. By publishing shares to Active Directory, users can use the Find feature on the Start menu on their Windows desktops to find remote shares based on their identifier or description. In order to publish shares to Active Directory, open the File Server Management console, click on Shares, right click on the share name to be published, click on properties, then choose the Publish tab and check the “Publish this share in Active Directory” box as shown in Figure 46.

A searchable Description and Keywords may also be specified to further assist in finding this resource.
Figure 46. Publishing the share in Active Directory with a searchable description and keywords
Data Migration

When migrating data from an alternate SMB share hosted on any other device, the ACLs used by ZFS fully support NT ACLs. Therefore, no ACL configuration will be lost or truncated during migration.

DFS Target

The Distributed File System (DFS) solution in Windows Server 2003 R2 and later allows administrators to group shared folders across the network into a virtual tree of folders called a namespace. The current Oracle ZFS Storage Appliance software release (the minimum required software version is 2010.Q3.4.1) allows for an appliance SMB share to act as a DFS target. A namespace root must already be active on an alternate object in Active Directory. You can add SMB shares from the Oracle ZFS Storage Appliance as targets to any DFS root.

To add a SMB share from the Oracle ZFS Storage Appliance as a target or DFS referral, click Add Folder from an existing DFS root share; the Figure 47 example shows a domain-wide share of \example\HR. Enter the path to the SMB share that should be shared underneath the root share and give the folder a unique name. In this example, a Forms share from one Oracle ZFS Storage Appliance is added along with a Reports share from an alternate Oracle ZFS Storage Appliance.
Figure 47. Creating a DFS target

As shown in Figure 48, both shares are now placed in the \example.com\dfsspace root.
When viewed from a client’s perspective, browsing to `\example.com\dfsspace` will show both Forms and AccountingReps in the same directory tree, although they are presented by separate Oracle ZFS Storage Appliances as can be seen in Figure 49.
Snapshots

Projects and/or shares may have snapshots enabled. The shares may inherit the snapshot policies from the project or have their own schedule. Enabling snapshots is a way to enable file consistency as well as file versioning. Snapshot browsing in the .zfs folder is a quick and easy way to recover files. By default, the project's .zfs/snapshot visibility property is set to “Hidden.” In order to browse the .zfs folder from a client system, “Visible” must be selected.

In order to create a snapshot, you must either execute it manually for the project or share or create a schedule for the snapshots to execute. Figure 50 shows the default snapshot schedule page.

Figure 50. Default snapshot schedule

As shown in Figure 51, you can view any existing snapshots either on a project level or on an individual share level by selecting the “Snapshot” option.
Integrating Microsoft Servers and the Oracle ZFS Storage Appliance

Figure 51. Existing snapshots

With the .zfs/snapshot visibility feature set to “Visible,” you can browse a .zfs folder for individual files to copy from for a quick restore. Figures 52 shows the folder in Windows Explorer.

Figure 52. Snapshot view in Windows Explorer

Figure 53 shows the snapshot files contained in the .zfs directory name.
Figure 53. Expanded zfs snapshot folder

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>.auto-1334066400</td>
<td>15/03/2012 13:18</td>
<td>File folder</td>
</tr>
<tr>
<td>.auto-1334070000</td>
<td>15/03/2012 13:18</td>
<td>File folder</td>
</tr>
<tr>
<td>.auto-1334071800</td>
<td>10/04/2012 15:23</td>
<td>File folder</td>
</tr>
<tr>
<td>ManualSnapshot</td>
<td>10/04/2012 15:23</td>
<td>File folder</td>
</tr>
</tbody>
</table>
Analytics

Analytics is a useful tool for gauging how much data is being sent in and out of an appliance, as well as more specific details; for example, what files and clients are involved, or the latency.

Analytics can provide the following nine categories of listings for viewing SMB:

- SMB operations broken down by type of operation
- SMB operations broken down by client
- SMB operations broken down by file name
- SMB operations broken down by share
- SMB operations broken down by project
- SMB operations broken down by latency
- SMB operations broken down by size
- SMB operations broken down by offset
- SMB operations as a raw statistic (operations per second)

Analytics allows for the breakdown of performance statistics for the SMB protocol by several different type of operations, as shown in Figure 54.
Adding statistics...

<table>
<thead>
<tr>
<th>Category</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Percent utilization</td>
</tr>
<tr>
<td>CACHE</td>
<td>ARC accesses</td>
</tr>
<tr>
<td></td>
<td>L2ARC accesses</td>
</tr>
<tr>
<td></td>
<td>L2ARC I/O bytes</td>
</tr>
<tr>
<td>DATA MOVEMENT</td>
<td>NDMP bytes transferred to/from disk</td>
</tr>
<tr>
<td></td>
<td>NDMP bytes transferred to/from tape</td>
</tr>
<tr>
<td></td>
<td>Shadow migration bytes</td>
</tr>
<tr>
<td></td>
<td>Shadow migration ops</td>
</tr>
<tr>
<td></td>
<td>Shadow migration requests</td>
</tr>
<tr>
<td>DISK</td>
<td>Disks</td>
</tr>
<tr>
<td></td>
<td>I/O bytes</td>
</tr>
<tr>
<td></td>
<td>I/O operations</td>
</tr>
<tr>
<td>NETWORK</td>
<td>DataLink bytes</td>
</tr>
<tr>
<td></td>
<td>Device bytes</td>
</tr>
<tr>
<td></td>
<td>Interface bytes</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>Fibre Channel bytes</td>
</tr>
<tr>
<td></td>
<td>Fibre Channel operations</td>
</tr>
<tr>
<td></td>
<td>FTP bytes</td>
</tr>
<tr>
<td></td>
<td>HTTP/WebDAV requests</td>
</tr>
<tr>
<td></td>
<td>iSCSI bytes</td>
</tr>
<tr>
<td></td>
<td>iSCSI operations</td>
</tr>
<tr>
<td></td>
<td>NFSv2 operations</td>
</tr>
<tr>
<td></td>
<td>NFSv3 operations</td>
</tr>
<tr>
<td></td>
<td>NFSv4 operations</td>
</tr>
<tr>
<td></td>
<td>SFTP bytes</td>
</tr>
<tr>
<td></td>
<td>SMB operations</td>
</tr>
<tr>
<td></td>
<td>SRP bytes</td>
</tr>
<tr>
<td></td>
<td>SRP operations</td>
</tr>
</tbody>
</table>

Figure 54. Selecting analytics for SMB operations

You can see a high-level picture of activity viewing SMB operations per second broken down by client, as shown in Figure 55.
If a particular client has more activity than another, you can drill down on that client to view more granular data as shown in Illustration 44. In this example, w2k8-ad is initiating I/O more than bigbox. In order to get a pictorial representation of the access highlighted, click on the host name in the “Range Average” box and the selected host will display in a contrasting color as shown in Figure 56.

To view exactly what w2k8-ad is doing, you can drill down on a specific host for more details. It may be helpful to view which files are being accessed most often. To view files, select w2k8-ad, click on the drill icon, and choose SMB Operations broken down by filename.

The following views in Figure 57 include SMB operations by file name, share, and project, which can be useful to determine the highest requested resource. These analytics are a valuable tool in troubleshooting storage problems, load balancing, or for planning capacity.
Graphing operation latency can be very useful for problem diagnosis. The example in Figure 58 shows that 253 operations completed in less than 131 microseconds and 197 operations complete in 131 microseconds. The Y-axis represents latency and the X-axis represents time. The darker bands near the bottom represent that more data is being serviced in short response times compared to the lighter bands representing longer response times.

Figure 58. SMB analytics showing operation latency

Figure 59 shows the size of the I/O request being serviced and the latency of the request. Most of the transfers in this example are 32K (represented by the darker band at the top of...
the size graph) and are being serviced in usecond timings (represented by the dark band at the bottom of the latency graph).

![Protocol: SMB operations per second broken down by size](image)

![Protocol: SMB operations per second broken down by latency](image)

Figure 59. SMB analytics for operation size and latency

**Conclusion**

The Oracle ZFS Storage Appliance allows very close integration with Windows server toolsets and concepts, allowing intuitive control and management of the storage resources in a form familiar to Windows Server administrators.

Along with the native performance management tools, identity mapping features and data protection facilities, the Oracle ZFS Storage Appliance fits into and augments Windows Server environments.
## References

<table>
<thead>
<tr>
<th>Sun ZFS Storage Appliance Administration Guide</th>
<th>docs.oracle.com/cd/E22471_01/pdf/820-4167.pdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Oracle ZFS Storage Appliance to Use IDMU to Map Identities Between Active Directory and NIS</td>
<td>Sun NAS Storage Documentation white papers at: <a href="http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html">http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html</a></td>
</tr>
<tr>
<td>Oracle ZFS Storage Appliance Rule-based Identity Mapping</td>
<td></td>
</tr>
<tr>
<td>How to Configure an Authoritative Time Server in Windows Server</td>
<td><a href="http://support.microsoft.com/kb/816042">http://support.microsoft.com/kb/816042</a></td>
</tr>
<tr>
<td>Microsoft Distributed File System Overview</td>
<td>technet.microsoft.com/en-us/library/cc738688%28v=ws.10%29.aspx</td>
</tr>
</tbody>
</table>
Integrating Microsoft Server and the Oracle ZFS Storage Appliance

July 2012, Version 2.0
January 2014, Version 2.1

Authors: Ryan H Pratt & Andrew Ness

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

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com