



Deploying the F5 ARX with Oracle's Sun ZFS Storage Appliance 7000 Series for CIFS

Table of Contents

Deploying the F5 ARX with Oracle's Sun ZFS Storage Appliance 7000 Series for CIFS

Prerequisites and configuration notes	1
Product versions and revision history	2
Configuration example	3
Configuring the Oracle's Sun ZFS Storage Appliance 7000 Series	4
Configuring the initial settings on Oracle's Sun ZFS Storage Appliance	4
Performing the system setup for Oracle's Sun ZFS Storage Appliance	7
Configuring the ARX device	14
Creating the CIFS Namespace	14
Adding the External Filers	16
Creating a Volume	17
Adding the root level share	18
Adding Oracle's Sun ZFS Storage Appliance 7000 Series CIFS Share	20
Creating the File Placement Policy	21
Creating the Virtual Service	23
Storage Integration Verification	26
Mount the Virtual Server CIFS share	26
Verifying the Virtual Service Directory Contents	27
Conclusion	27

Deploying the F5 ARX with Oracle's Sun ZFS Storage Appliance 7000 Series for CIFS

Welcome to the F5 - Oracle's Sun ZFS Storage Appliance 7000 Series deployment guide. This guide provides step by step procedures on deploying the Adaptive Resource Switch (ARX) with Oracle's Sun ZFS Storage Appliance 7000 Series.

The F5 ARX file virtualization platform decouples file access from physical file location within Network Attached Storage (NAS) environments. The ARX platform automates file migration to the appropriate tier of storage without affecting data access, thus minimizing backup and recovery windows.

For more information on the ARX system, see <http://www.f5.com/products/arx-series/>

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this deployment:

- ◆ This document is based on the fact that the Tier 1 external filer legacy storage is pre-configured and available as a network resource.
- ◆ This document is based on the fact that the Microsoft Active Directory Domain is preconfigured and the F5 Secure Agent is installed.
- ◆ The ARX initial switch interview has been completed.
- ◆ The ARX has is configued for network access and has an active license.
- ◆ The following CIFS attributes are supported:
 - Named Streams
A named stream (or Alternate Data Stream) is a hidden file with meta-information about the main file, such as a summary description or a thumb-nail graphic.
 - Unicode-on-Disk
A volume that supports unicode on disk can support file names with any of the multi-byte characters (such as Korean or Japanese characters) supported by the Unicode character set.
 - Persistent ACLs
A volume with persistent Access-Control Lists (ACLs) can display the ACLs of its files and directories to its clients.
- ◆ The following features are **NOT** supported:
 - *Kerberos Authentication*
You can configure the namespace to authenticate clients with Kerberos instead of (or in addition to) NTLM. The Sun ZFS Storage Appliance does not support Kerberos authentication. The user must configure NTLM authentication.

- *Multiprotocol Access (NFS & CIFS)*
 If all the back-end shares support both NFS and CIFS, you can configure a *multi-protocol namespace*. Clients can access the same files from either a CIFS or an NFS client. The namespace can be backed by a heterogeneous mix of multi-protocol filers, possibly from multiple vendors. The switch passes client requests to these filers, and passes filer responses back to the clients. File attributes, such as file ownership and permission settings, are managed by each filer. Each filer also manages its file and directory naming; if a name is legal in NFS but illegal in CIFS, each filer creates a filer-generated name (FGN) for its CIFS clients. Different vendors use different conventions for attribute conversions and FGNs, so that a CIFS-side name and/or ACLs at one filer may be different at another filer.
- *ARX Virtual snapshot support*
 A *snapshot* is an exact copy of a managed volume at a single point-in-time. You can create regularly-scheduled snapshots in a managed volume, and you can limit the CIFS clients who can access those snapshots.
- *CIFS filer subshares*
 A managed volume that supports CIFS can optionally support subshares and their share-level ACLs. A subshare is a CIFS share below the root of the volume

◆ **Note**

The screen shots depicted in this guide may differ depending on the version of software installed on F5 ARX and Oracle's Sun ZFS Storage Appliance.

Product versions and revision history

Product Tested	Version Tested
Oracle's Sun ZFS Storage Appliance 7000 Series	S7310c
Oracle's Sun ZFS Storage Appliance 7000 Series Software release	2010.08.17.4.0,1-1.31
F5 ARX	6.1.0 HFRU1

Revision History

Document Version	Description
1.0	New deployment guide

Configuration example

In the following diagram, we show basic connectivity between clients, ARX and Sun ZFS Storage Appliance. In this configuration, a client attempts to retrieve a file from a file share. The ARX proxies the request and transparently retrieves the file from the server storing the file. We configure a policy on the ARX that periodically checks the last time files were modified, and then migrates the file to the appropriate filer if the conditions of the policy are met. In our example, the ARX policy is checking for a last modified time of less than (or more than) 30 days. If the policy matches, then the ARX moves the file between the backend filers according to policy.

The network configuration in our test lab used an ARX2000 with 4 Gigabit Ethernet links configured into a LACP bundle between the ARX and the core switch. The ARX, Sun ZFS Storage Appliance, Incumbent Legacy Storage, and Test client are all on the same subnet. The Active Directory (AD) Primary Domain Controller was on a different subnet than the Sun ZFS Storage Appliance. The Sun ZFS Storage Appliance has joined the Microsoft Windows Active Directory domain. The ARX Proxy User is assigned backup operator privileges for the Sun ZFS Storage Appliance Storage system as a local Backup Operator, as described in this guide.

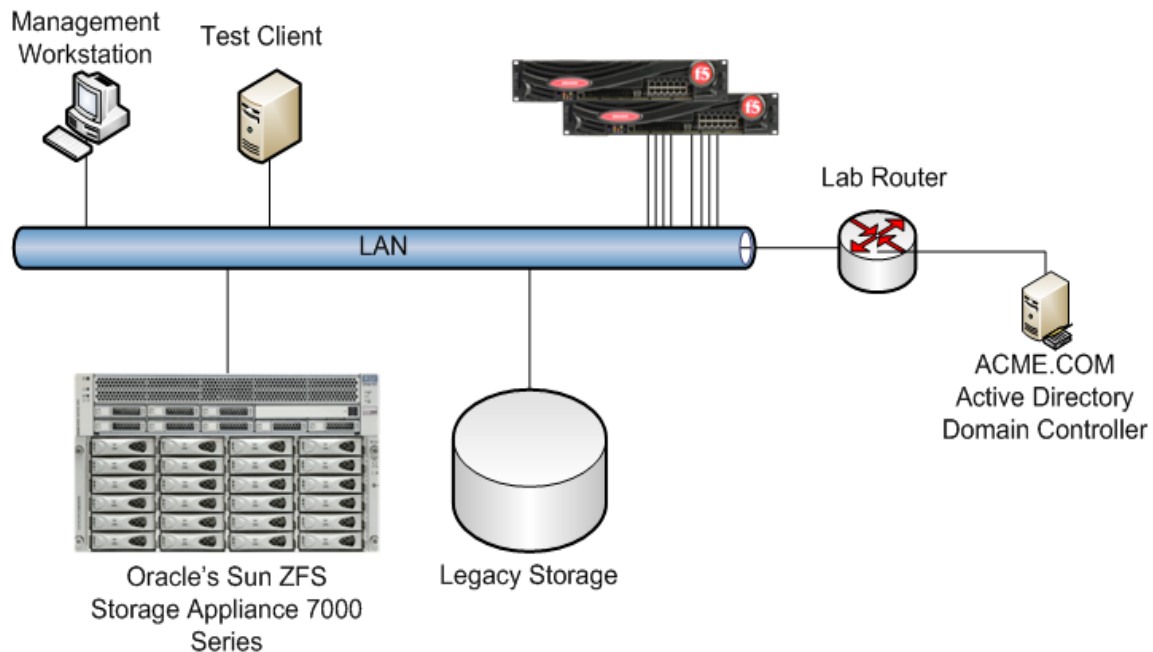


Figure 1 Logical configuration example

Configuring the Oracle's Sun ZFS Storage Appliance 7000 Series

Oracle's Sun ZFS Storage Appliance 7000 Series is shipped with preinstalled system software; initial setup is performed on the console port and complete configuration is performed with a Web browser. This section addresses the configuration of the Sun ZFS Storage Appliance including initial setup. The array is configured for RAID volumes. The Sun ZFS Storage Appliance is added to the Active Directory Domain, and the volume is shared to the network.

There are several levels of authentication and access control that are available to the system administrator. This guide describes configuration for highly permissive access control settings that are intended for demonstration purposes only. The access rights for a live deployment most likely would not leverage such relaxed security policies.

This section contains the following procedures:

- *Configuring the initial settings on Oracle's Sun ZFS Storage Appliance 7000 Series*, on page 4
- *Performing the system setup for Oracle's Sun ZFS Storage Appliance 7000 Series*, on page 7
- *Joining the Active Directory Domain*, on page 7
- *Defining the Local Backup Operator*, on page 8
- *Creating a project*, on page 9
- *Creating the CIFS shares for Oracle's Sun ZFS Storage Appliance 7000 Series*, on page 11

Configuring the initial settings on Oracle's Sun ZFS Storage Appliance 7000 Series

The initial configuration of the Sun ZFS Storage Appliance is accomplished through the console port on the array controller. Use the Null Modem cable provided with the array and a terminal emulation application.

The initial configuration defines the IP network interfaces. An IP address, Mask, Default gateway (router), DNS Server, and root password are defined in these steps.

To configure the Sun ZFS Storage Appliance

1. Using a terminal application connect to the console port. Using the following parameters: **9600 Baud, N,8,1, no flow control**.
2. Enter the host name as **S7110**
3. The network interface is **NET-0**
4. IP address **10.51.105.20**
5. Network Mask **255.255.255.0**

6. Default Router **10.51.105.1**
7. DNS Server IP **192.168.1.5**
8. Type a password for the administration account.
9. Press the **F1** or **ESC 1** key to apply the settings and exit.

In the next procedure, we continue the initial configuration, but in this case, we use the Sun Storage 7000 user interface.

To configure the Sun User Interface

1. Using a web browser, log into the Sun ZFS Storage Appliance as root. By default the web interface is listening on port **215**. Use the following URL syntax:
http://<ip address>:215
If this is your first time configuring the Sun device, the initial setup wizard opens.
If you need to restart the wizard, it is available from the **Maintenance** menu by clicking **System**. Refer to the Sun documentation for more information on re-running this wizard.
2. In the first 5 steps of the wizard, verify the appropriate settings (and edit if necessary), such as the network setup, DNS, and NTP.
3. In Step 6 of 6, click the **Configure** button to configure the storage pool. In this example, we create a single storage pool named **pool-0**. This pool consists of all the disks with a RAID data profile. The Storage wizard opens.
4. On the **Verify Storage** page (Step 1 of 2), click the **Commit** button.



Figure 2 Verifying Storage

5. On the **Configure Storage** page (Step 2 of 2), you select the Data Profile to apply to the storage pool. In our example, we click **Double Parity RAID**, and then click **Commit**. This creates the storage pool.

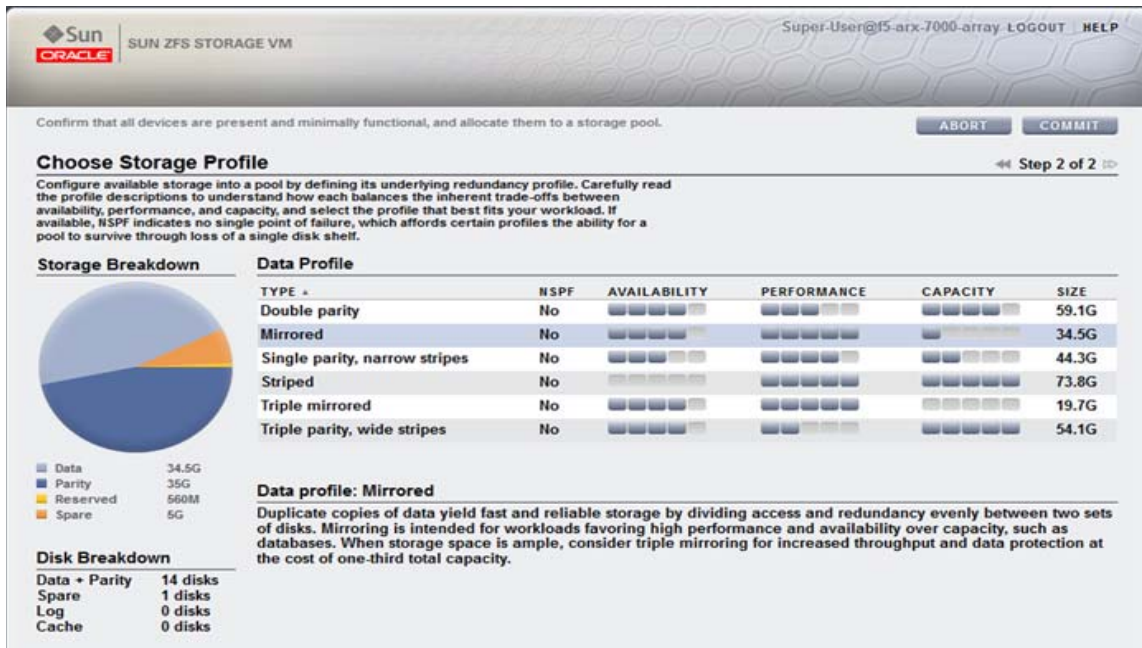


Figure 3 Configure Storage Data Profile

- You return to Step 6 of the Configure Storage wizard. Click **Commit** to complete Step 6 of 6.

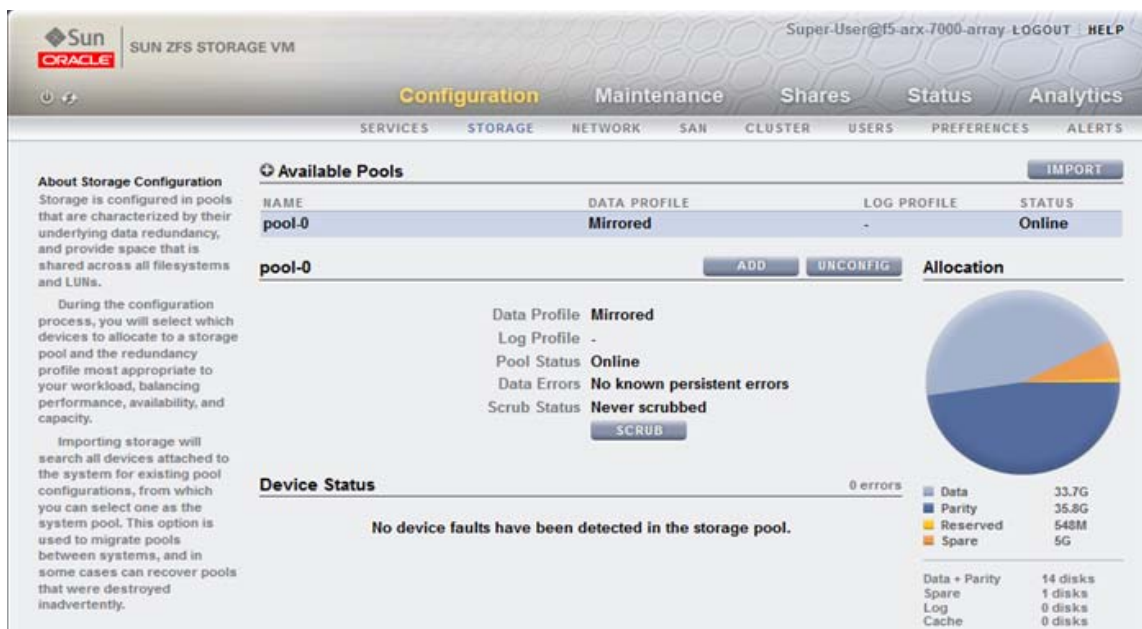


Figure 4 Configure Storage Step 6 complete

Performing the system setup for Oracle's Sun ZFS Storage Appliance 7000 Series

In this section, we perform the Sun system setup. In our configuration example the storage pools are already created. This deployment guide demonstrates how to configure new CIFS shares with Microsoft Active Directory User authentication.

Joining the Active Directory Domain

The Sun ZFS Storage Appliance needs to join the Microsoft Active Directory Domain Computer.

To join the Active Directory Domain

1. Log into the Sun ZFS Storage Appliance as root (the internal web server is listening on port 215). Use the following URL syntax: **http://<ip address>:215**.
The initial status page opens.
2. Click the Configuration tab, and then click **Active Directory** in the Directory Services section.
The Active Directory configuration screen opens.
3. Click the **Join Domain** button. The Join Domain dialog opens.
4. In the **Active Directory Domain** box, type the appropriate Domain Name.
5. In the **Administrative User** box, type the appropriate administrative user.
6. In the **Administrative Password** box, type the appropriate administrator password.
7. Click the **Apply** button.

Join Domain

CANCEL APPLY

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

Active Directory Domain:

Administrative User:

Administrative Password:

Additional DNS Search Path:

Figure 5 The Join Domain dialog

If the Join request is successful, the Active Directory status shows **Online** (see Figure 6). If it does not, verify that NTP is configured, the Domain Administrator access credentials are correct, and that the Domain Controller is network reachable.



Figure 6 Successful Joined the Domain and Online

Defining the Local Backup Operator

Next, you need to define a backup operator for the Sun ZFS Storage Appliance. This operator is the Proxy User the ARX uses to authenticate to the CIFS Shares. This is a special operator for non-interactive user sessions.

To add the Proxy User as a backup operator

1. Click the **Configuration** tab, and then click **CMB**.
2. Click the Local Groups tab, and then click the Add (+) button symbol to add a new member.
3. In the **User** box, type the user name for the member. Be sure to include the domain name. In this example we used the ACME Domain user **acmeuser001**. The Sun ZFS Storage Appliance has to be actively joined to the Domain in order to retrieve the SID for this user.
4. From the **Local group** box, select **Backup Operators**.



Figure 7 Add Member to the local Backup Operator group

5. Click the **Add** button. The Sun ZFS Storage Appliance attempts to retrieve the SID from the Active Primary Domain Controller. If successful, the SID appears in the list.

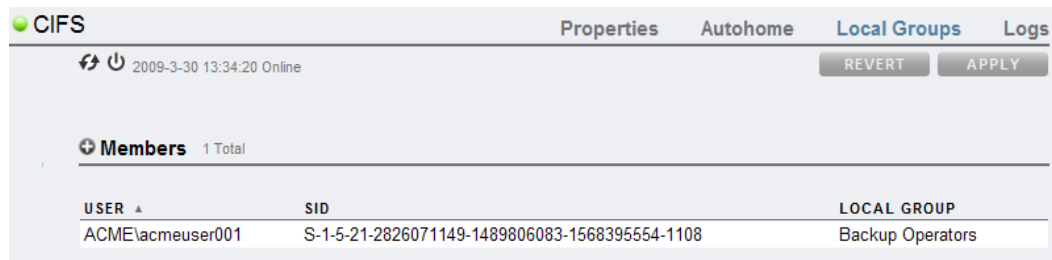


Figure 8 Local Group members list

Creating a project

Best practices suggest that you create a new Project to manage the shares in a collection of common values.

To create a new project

1. From the top menu, click **Shares**.
2. From the left pane, click the arrow next to **Projects**. The Projects List opens.
3. Click the Add (+) button. The Create Project dialog opens.
4. In the **Name** box, type a name for this project. In our example, we type **ARX**.
5. Click the **Apply** button.

Once you have created the Project, you need to set the default settings for the project.

To set the default settings for the project

1. From the top menu, click **Shares**, and then click **Projects** in the sub menu.
2. From the **Project** list, point your mouse at the project you just created; a small pencil and trash can icon appear on the right. Click the pencil to edit the project (see Figure 9).
A list of submenu options appear

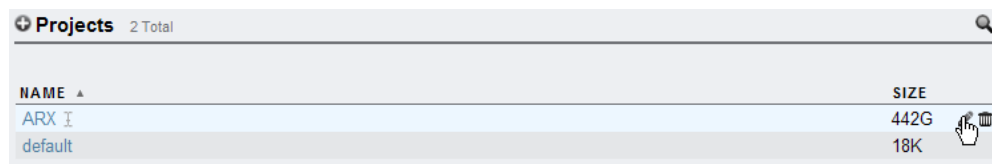


Figure 9 List of Projects

3. From the submenu bar, click **General**.
4. From the Inherited Properties section, in the **Mountpoint** box, type the directory name. In our example, we type `/export/arf`.
5. Click **Apply** to commit the changes.

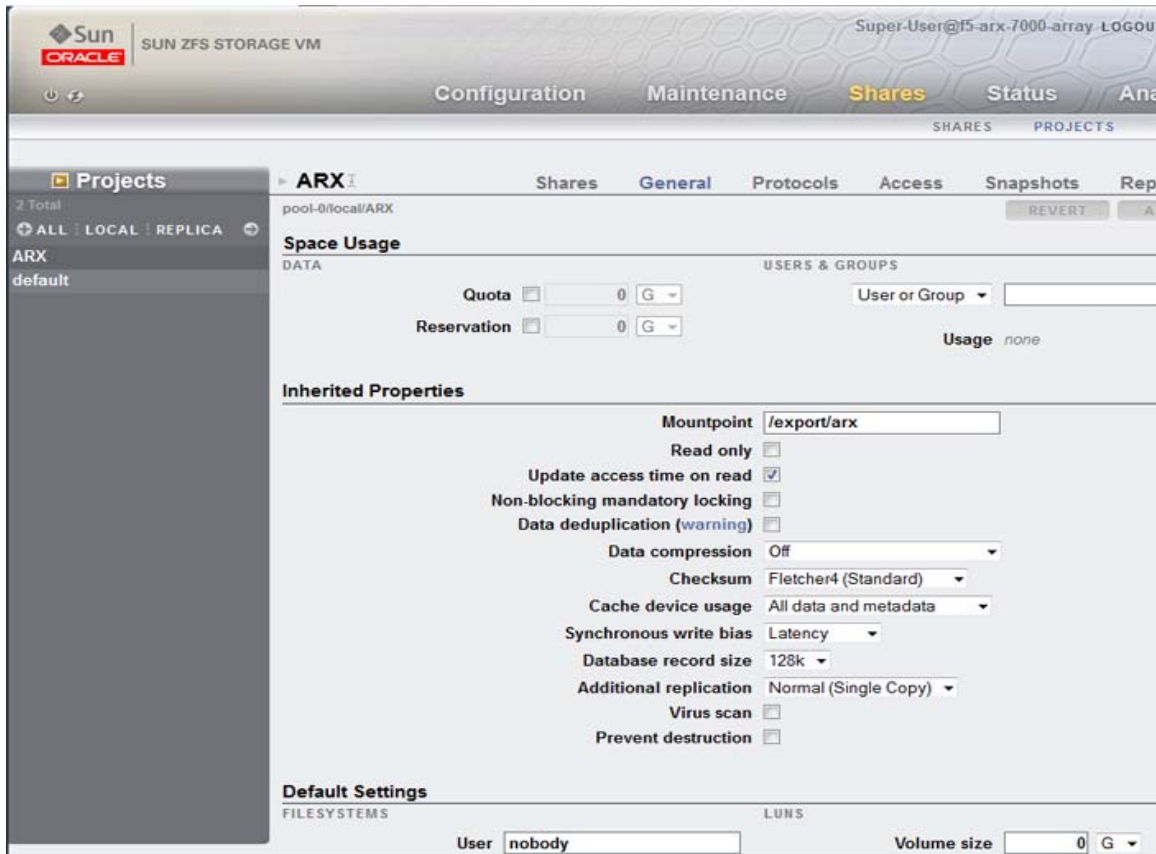


Figure 10 Project Inherited Properties

6. From the submenu bar, click **Protocols**.
7. From the SMB section, in the **Resource Name** box, type a resource name. This is the base name the SMB shares inherit. Notice under the word SMB the URL is displayed.
8. If applicable, check the **Enable Access-based Enumeration** box.
9. Click **Apply** to commit the changes.
10. From the submenu bar, click **Access** to define the ACL behaviors. In our example, from the **ACL inheritance behavior** list, we select **Do not inherit entries**.
11. Click **Apply** to commit the changes.

You have now specified the Project default values. These values are inherited by each share created as a part of this project. These attributes can be overridden within each share as needed.

Creating the CIFS shares for Oracle's Sun ZFS Storage Appliance 7000 Series

The next step is to create the CIFS shares for the Sun ZFS Storage Appliance. These shares are imported into the ARX managed volume later in this guide. The shares are created within the context of the project we just created.

To create the CIFS shares

1. From the top menu, click **Shares**.
2. From the left pane, click the arrow next to **Projects**. From the Projects list, click the name of the project you created. In our example, we click **ARX**.
Once selected the ARX project menu bar appears. The first item is the list of shares. Initially this list is empty. The list reports the Share name, Size is the amount of space used, and the actual mount point within the Sun ZFS Storage Appliance internal file system.
3. Click the Add (+) button next to **File Systems** to add a new share. The Create File System box opens.
4. In the **Name** box, type a name for this share. In our example, we type **share**. Leave the rest of the values at the default setting.
5. Click the **Apply** button. The new share appears in the list.

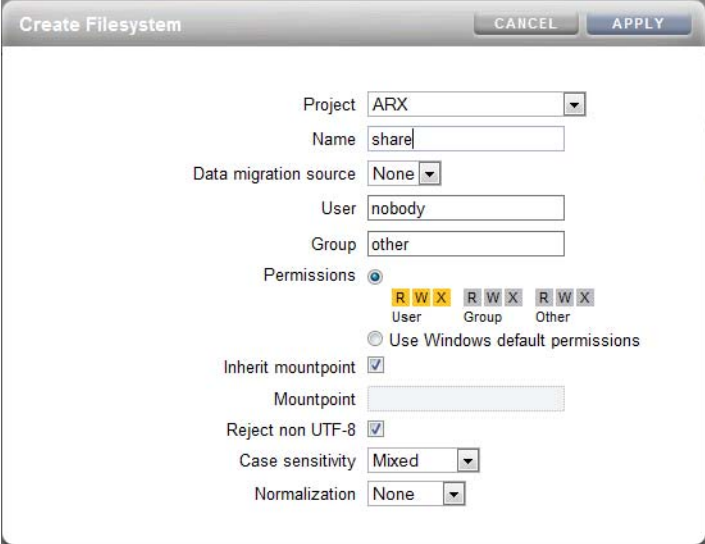


Figure 11 Creating the File system

The next step is to edit the root directory ACL.

To edit the root directory ACL

1. Point your mouse at the Share you just created; a small pencil appears on the right. Click the pencil to edit the share properties.
2. Click **Protocols** on the submenu bar.
3. In the root directory ACL section, point your mouse at the ACL with the Type of **Everyone**; a small pencil appears. Click the pencil to edit the ACL properties. The Edit ACL Entry dialog box opens.
4. In the Inheritance section, click a check in the **Apply to Files** and **Apply to Directories** boxes.

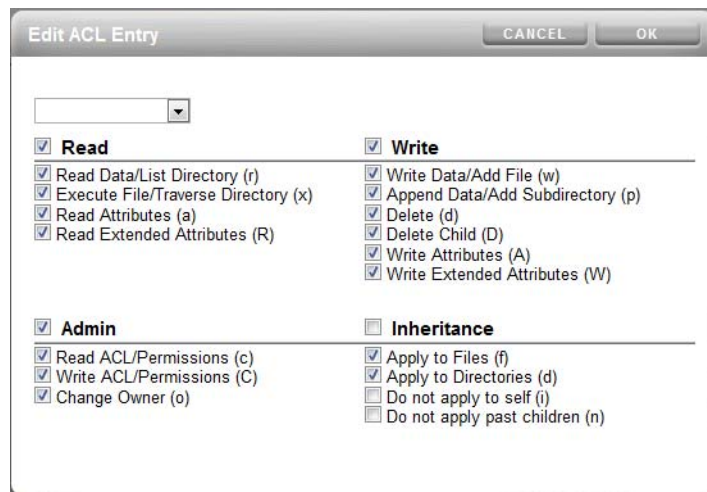


Figure 12 Permissions and Inheritance settings

5. Click the **OK** button.
The next step is to define the access to this share.
6. Click the **Access** submenu
7. In the **Root Directory ACL** section, leave the ACL type **Everyone** entry, and delete any other ACLs by hovering over the appropriate row, clicking the Trashcan icon when it appears.
8. Make sure the **Mode** of the Everyone ACL is set to **Allow**.
The ACL should now look exactly like Figure 13.
9. Edit the ACL entry as in step 4 above, however, in this case, in the Inheritance section, also check the **Do Not Apply to self (i)** box.

Root Directory ACL				
TYPE	TARGET	ACCESS	PERMISSIONS : INHERITANCE	
Everyone	not applicable	Allow	Full Control	rwxpdaARWcCo:fdi-

Figure 13 Root Directory ACL Permissions and Inheritance settings

10. Click the **Apply** button.

Repeat these settings to create a **/metadata** share to be used by the ARX as its metadata repository. Also repeat these steps for any other share you may want to virtualize with the ARX.

Configuring the ARX device

In this section, we configure the ARX to access the Incumbent Storage, and the Sun ZFS Storage Appliance. We create a CIFS namespace and add two shares. We then incorporate the shares into a managed volume with a file placement policy. As files age and are not modified for more than 30 days, they are moved between the shares, depending upon the file last modified time.

To configure the ARX, perform the following procedures:

- *Creating the CIFS Namespace*, on page 14
- *Creating a Volume*, on page 17
- *Adding the root level share*, on page 18
- *Adding the root level share*, on page 18
- *Adding Oracle's Sun ZFS Storage Appliance 7000 Series CIFS Share*, on page 20
- *Creating the File Placement Policy*, on page 21
- *Creating the Virtual Service*, on page 23


The main page of the ARX user interface is the Common Operations page. Much of the following steps start from this page.

Creating the CIFS Namespace

The first task in configuring the ARX is to create the CIFS namespace.

To create the CIFS namespace

1. Open the ARX web-based Configuration utility, and in the left navigation pane, click **Common Operations**.
2. Click the **Create Namespace** button. The Create Namespace wizard opens.
3. In the **Namespace name** box, type a name. In our example, we type **Oracle_CIFS**.
You can optionally type a description.
4. From the **Protocol** list, click the **CIFS** box, and then click **Next**.

This wizard creates a namespace that is a container for client access protocol(s) and authentication configuration. It is also a container for one or more volume(s). Enter the namespace name and select the protocol(s) for the namespace to use. 

Namespace name:

Description (optional):

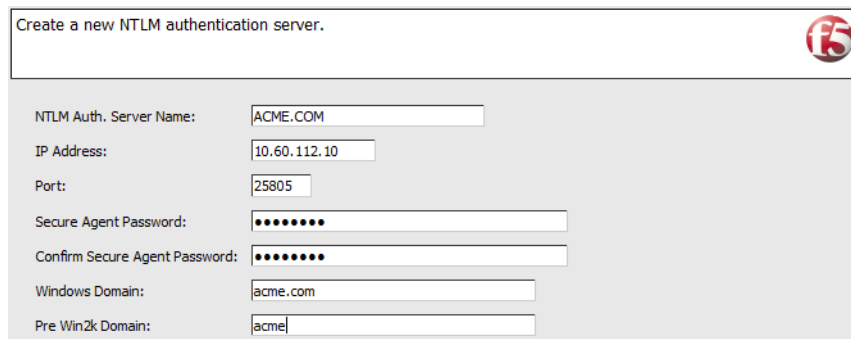
Protocol(s): NFSv2 NFSv3-UDP NFSv3-TCP CIFS

Figure 14 Configuring the Namespace

-
5. From the CIFS authentication information screen, click the **Use NTLM** box. Click the **Add** button to add an NTLM server.

Note: The Sun ZFS Storage Appliance does not support Kerberos, do not select the Kerberos option.

- a) In the **NTLM Auth. Server Name** box, type the Fully Qualified Domain Name (FQDN) of the server.
- b) In the **IP address** box, type the IP address of the server.
- c) In the **Port** box, type the appropriate port, or leave it at the default setting: **25805**.
- d) In the **Secure Agent password** box, type the password. This is the password assigned on the Domain Controller for the Secure Agent application. Retype the password.
- e) In the **Windows Domain** box, type the appropriate Windows Domain.
- f) Click **Save**. You return to the CIFS authentication page.



The screenshot shows a web form titled "Create a new NTLM authentication server." with a red "15" icon in the top right corner. The form contains the following fields and values:

NTLM Auth. Server Name:	ACME.COM
IP Address:	10.60.112.10
Port:	25805
Secure Agent Password:	••••••••
Confirm Secure Agent Password:	••••••••
Windows Domain:	acme.com
Pre Win2k Domain:	acme

Figure 15 Configuring an NTLM server

6. In the Proxy User section, click **Add** to add a proxy user. The ARX uses the proxy user credentials in order to access the filer and perform policy actions. This is the Active Directory user that was assigned as the Backup Operator in the previous section.
 - a) In the **Proxy User Name** box, type the name. In our example, we type **acmeuser**.
 - b) In the **Proxy User Account** box, type the proxy user account. In our example, we type **acmeuser001**.
 - c) In the **Proxy User Account Password**, type the password. Retype the password in the **Confirm Proxy User Account Password** box.
 - d) In the **Windows Domain** and **Pre Win2k Domain** boxes, type the appropriate Windows Domain. In our example, we type **acme.com** and **acme** in the boxes (see Figure 16).

- e) Click the **Save** button. You return to the CIFS authentication page.

Proxy Username	arx_proxy_user
Description:	
Proxy User Account	acmeuser001
Proxy User Account Password	●●●●●●
Confirm Proxy User Account Password	●●●●●●
Windows Domain	acme.com
Pre Win2k Domain	acme

Figure 16 Creating a new proxy user

7. On the CIFS authentication page, click the **Next** button.
8. Review the summary, and click the **Finish** button.
The namespace is created.

The CIFS Authentication details are complete.

Adding the External Filers

In this section we add the Sun ZFS Storage Appliance as an external filer entry in the ARX. This entry is referenced later when we add the filer shares to the managed volume.

To add the External Filers

1. From the navigation pane, click **File Servers**.
2. Click the **Add** button. The Add File Server screen opens.
3. In the **Name** box, type a name for this File Server. In our example, we type **Oracle**.
4. In the **Primary IP Address** box, type the primary IP address.
5. In the **Secondary IP Address** box, optionally type any secondary IP addresses, and click the **Add** button. In our example, we do not include any secondary IP addresses.
6. In the **Description** box, you can optionally type a description.
7. In the **Ignore Directories (optional)** box, type any snapshot directories the ARX should ignore on the backend file shares, and click the **Add** button.
8. Click the **OK** button.
9. Repeat this procedure for the Legacy storage platform. In our example, we name this filer **LegacyStorage**.

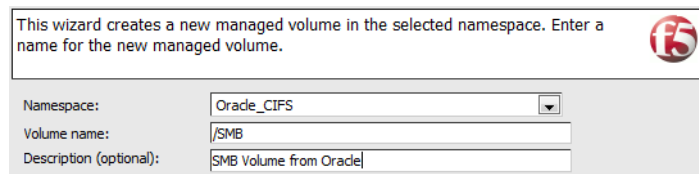
Creating a Volume

The backend filer CIFS shares are incorporated into an ARX Managed Volume. File placement policy is managed at the volume level. The volume attributes to be defined are namespace, volume name, description, CIFS parameters, and the metadata store mount point.

In our example, we place the Volume Metadata onto the incumbent legacy storage platform. F5 recommends Metadata should be created on an NFS export if one is available. Alternatively, a CIFS share could be used.

To create a volume on the ARX

1. From the left navigation pane, click **Common Operations**.
2. Click the **Create Volume** button. The Create Volume wizard opens.
3. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 14. In our example, we select **Oracle_CIFS**.
4. In the **Volume name** box, type the volume name. In our example, we type **/SMB**. You can optionally add a description. See Figure 17.
5. Click the **Next** button.



This wizard creates a new managed volume in the selected namespace. Enter a name for the new managed volume.

Namespace: Oracle_CIFS

Volume name: /SMB

Description (optional): SMB Volume from Oracle

Figure 17 Creating a new Volume

6. From the **Metadata file server protocol** list, select an appropriate protocol. In our example, we select **CIFS**.
7. From the **Metadata file server** list, select the file server you created in *Adding the External Filers*, on page 16. In our example, we select **Oracle**.
8. In the **Metadata CIFS share/NFS path** box, type the path. In our example, we type **/metadata**. Click the **Next** button.
9. From the CIFS Parameters page, in the Auto-synchronization section, click the **Auto-synchronize** box.
10. In the CIFS Attributes section, click the **Auto-detect CIFS attributes** box. Click the **Next** button.
11. From the Volume Parameters page, in the Performance Tuning section, from the **VPU ID** list, select **Dynamic**. Ensure the **Auto Reserve files** box is checked.

12. In the Import Conflict Resolution section, click the **Files and directories can be renamed during import and re-import. makes the volume read write** button.
13. In the Enable Volume section, click the **Enable the volume when finished** button (see Figure 18).
14. Click the **Next** button.
15. Review the summary, and click **Finish**.

Set the volume parameters or accept the defaults. Set the maximum file count to the approximate number of files that will be in the volume.

Performance Tuning

Volume Group:

Auto reserve files

Maximum files:

Import Conflict Resolution

Files and directories are not renamed during import. Makes the volume read only.

Files and directories can be renamed during import and a re-import. Makes the volume read write.
(Rename files and rename directories should also be set when adding shares to this volume.)

By default volumes are created Read-Only.

Shadow Target

Make this volume a shadow-copy target.

Enable Volume

Enable the volume when finished.

Figure 18 Configuring the volume parameters

Adding the root level share

The first file share we add is the root level share. This is the incumbent legacy storage volumes with file content. The subsequent shares adapt to the root volume permissions.

To add a root level share

1. From the left navigation pane, click **Common Operations**.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **Legacy Share**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 14. In our example, we select **Oracle_CIFS**.

-
- From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 17. In our example, we select **/CIFS**. Click the **Next** button.

This wizard adds a share to a volume. Files and directories on the share will be imported into the volume. Enter the name of the share to add to the selected the namespace and volume.

Share name: Legacy Share

Replica Snapshot: Replica snapshot share.

Namespace: Orade_CIFS

Volume: /SMB

Figure 19 Configuring the initial properties of the root level share.

- From the **File Server** list, select the name of the file server you created in step 9 of *Adding the External Filers*, on page 16. In our example, we select **LegacyStorage**.
- In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **Content2**.
- In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes (see Figure 20).
- Optional: You can select the ability for the ARX to take ownership if the share is owned by another ARX by clicking the **Allow this switch to import this share, even if it's owned by another Acopia switch box**.
- Click the **Next** button.
- Review the summary, and click the **Finish** button.

Select the options you would like this share to have.

Share name: Legacy Share
Import Priority: 65535

Import Conflict Resolution

- Rename files with naming collisions on import.
- Rename directories with naming collisions on import.
- Synchronize directory attributes between shares on import.
- Disable the managed file system check on import.

Local Groups

- Share contains local groups
- Ignore SID errors

Enable Share

- Enable this share when finished.
- Allow this switch to import this share, even if it is owned by another ARX.

Figure 20 File Server and Share name

Adding Oracle's Sun ZFS Storage Appliance 7000 Series CIFS Share

In this procedure, we add the Sun ZFS Storage Appliance share to the volume.

To add the CIFS Shares to the volume

1. From the left navigation pane, click Common Operations.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **Oracle_Share**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 14. In our example, we select **Oracle_CIFS**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 17. In our example, we select **/SMB**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in step 3 of *Adding the root level share*, on page 18. In our example, we select **Oracle**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share**.

8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import**, **Rename directories with naming collisions on import**, and **Synchronize directory attributes between shares on import** boxes.
9. Optional: You can select the ability for the ARX to take ownership if the share is owned by another ARX by clicking the **Allow this switch to import this share, even if it's owned by another Acopia switch box**.
10. Click the **Next** button.
11. Review the summary, and click the **Finish** button.

Select the options you would like this share to have.

Share name: Oracle Share
 Import Priority:

Import Conflict Resolution

- Rename files with naming collisions on import.
- Rename directories with naming collisions on import.
- Synchronize directory attributes between shares on import.
- Disable the managed file system check on import.

Local Groups

- Share contains local groups
- Ignore SID errors

Enable Share

- Enable this share when finished.
- Allow this switch to import this share, even if it is owned by another ARX.

Figure 21 File Server and share name

Creating the File Placement Policy

A placement policy rule is a policy assigned to a managed volume. It facilitates file movement between backend file shares based on file attributes. The files can be placed based on modified time, last access time, file name, and applied as a scheduled event. The ARX periodically (on schedule) scans the metadata store and checks for policy matches. If a match is located, the ARX processes the rule and moves the file according to the policy definition. Policy rule enumeration can be limited by a time of day rule, and it can also restrict the total time a policy is allowed to process files.

In this example, we create a Policy rule to move files that have not been modified for more than 30 days onto the Sun ZFS Storage Appliance. The files are copied to the SMB share named *share*. The policy is enumerated every 30 minutes.

To create the file placement policy

1. From the left navigation pane, click **Common Operations**.
2. Click the **Tiered Storage** button. The Tiered Storage Wizard opens.
3. In the **Policy name prefix** box, type a prefix. In our example, we type **2-Tiers**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 14. In our example, we select **Oracle_CIFS**.
5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume*, on page 17. In our example, we select **/SMB**.
6. From the **Number of tiers** list, select a number of tiers. In our example we select **2**.
Click the **Next** button.
7. For Tier 1, select the incumbent legacy storage file share you created in *Adding the root level share*, on page 18. In our example, we select **Legacy Share**. Click the **Next** button.

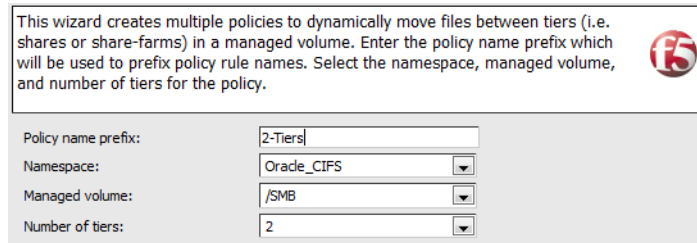


Figure 22 *Selecting the incumbent legacy storage file share*

8. For Tier 2, select the name of the Sun ZFS Storage Appliance Storage Share you created in *Adding Oracle's Sun ZFS Storage Appliance 7000 Series CIFS Share*, on page 20. In our example, we select **Oracle_Share**.
Click the **Next** button.
9. The next step is to specify the criteria for moving files and the schedule. Click the **Add** button to the right of Schedule to define the schedule to be associated with the policy.
 - a) In the **Schedule Name** box, type a name for this schedule. In our example, we type **Oracle Schedule**.
 - b) In the **Start Time** fields, you can specify a specific start time. In our example, we leave the fields at the default.
 - c) In the **Every** box, type a number, and select a time period from the list. In our example, we type **30**, and select **minutes** from the list.

-
- d) The other fields are optional, configure as applicable for your deployment.
 - e) Click the **Save** button. You return to the Tiered Storage Wizard.
 10. From the **Move files not** list, select **Modified**. In the **In the last** box, type a number and select a time period. In our example, we type **30** and select **days** from the list. So files are moved if they have not been modified for 30 days with the schedule defined in the previous step.
 11. From the **Schedule** list, select the name of the Schedule you just created. In our example, we select **Oracle Schedule**.
 12. In the Enable box, ensure the **Enable this policy when finished** box is checked (see Figure 23).
 13. Click the **Next** button.
 14. Review the summary and then click the **Finish** button.

Select the criteria for moving files between tiers. Optionally select a fileset and/or schedule for the policy. If an optional fileset is not selected, the default is to evaluate all files.

Specify the criteria for moving files between **Tier 1 and Tier 2:**

Move files not in the last

Schedule:

Options

Fileset (optional):

Generate reports

Enable

Enable this policy when finished

Enable tentative

Figure 23 File movement criteria

Creating the Virtual Service

The Virtual Service is how the ARX presents CIFS Shares to the network clients. Clients send file requests through the Virtual Service and the ARX proxies these requests to the appropriate backend filer.

To create the virtual service

1. From the navigation pane, click **Virtual Services**.
The Virtual Service Summary page opens.

2. Click the **Add** button. The Add Virtual Service Wizard opens.
3. Click the **Create a new virtual service** button.
 - a) In the **Supported Protocols** section, check the **CIFS** box.
 - a) In the **Virtual service DNS name** box, type the DNS name for the virtual service. In our example, we type **oracle_smb.acme.com**.
 - b) Ensure the **Enable the virtual service when finished** box is checked.
 - c) In the **Active Directory Domain Name** box, type the AD domain name. In our example, we type **acme.com**.
 - d) In the **Pre Win2k Domain (optional)** box, type the domain. In our example, we type **acme**.
 - e) Click **Next**.
4. In the **IP Address** box, type the IP address of the VIP. In our example, we type **10.10.10.1**.
5. In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.0**.
6. From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **1**.
7. Click the **Next** button. The Virtual Service Exports screen opens.
8. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 14. In our example, we select **Oracle_CIFS**.
9. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 17. In our example, we select **/SMB**. Click the **Next** button.
10. In the Volume Path box, type the path. In our example, we type **/**.
11. In the **Export Name** box, type a name for the Export. In our example, we type **Oracle_Vip**.
12. Configure the other options as applicable for your configuration, and then click the **Add Export** button.
13. Click the **Next** button.
14. Review the attributes and confirm the creation of the Virtual Service by clicking **Finish**.

You can review the Virtual Service by clicking **Virtual Services** from the navigation pane. You should see the Admin state is enabled and the status is Ready.

Virtual Service Summary

Click on a virtual service to view its details, or select a virtual service and click on an action button.

<input type="checkbox"/>	Domain Name	Virtual IP	VLAN	Exports	Domain Join	Admin State	Status
<input type="checkbox"/>	orade_smb.acme.com	10.10.10.1 255.255.255.0	1		Not Joined Delegation: Unknown	CIFS: Enabled	CIFS: Ready

Figure 24 Virtual Service Summary

You can also drill into the Virtual Service by clicking on the Domain Name. The Export Summary displays. Notice the status is Online:

Export Summary

Select an export and click on an action button.

Virtual Service:

<input type="checkbox"/>	Export	Domain Name	Protocol	Namespace	Volume	Virtual Vol Path
<input type="checkbox"/>	Orade_Vip	orade_smb.acme.com 10.10.10.1	CIFS	Orade_CIFS	/SMB	/SMB

Figure 25 Viewing the Export Summary

Storage Integration Verification

In this section, we verify the configuration is operating properly. We use a test client to mount the Virtualized Volume as a drive letter. The incumbent storage content will be visible.

Mount the Virtual Server CIFS share

The first step is to confirm the Virtual Service is operating properly. To do this, from a Windows client, we map a network drive to the Virtual Service Export. The export shows where files and directories reside on the backend shares. Users cannot determine which of the three backend file shares the files reside on because ARX has merged the files and directories into one common virtual path.

To map a drive for Virtual Service CIFS share

1. From the XP client, open **My Computer**.
2. From the **Tools** menu, click **Map Network Drive**. The Map Network Drive wizard opens.
3. From the **Drive** list, select an unused Drive letter.
4. In the **Folder** box, type the Virtual Service FQDN and export path. In our example, we type **oracle_smb.acme.com\Oracle_Vip**.
5. If the client's current user name is different than the Active Directory user name, click the **Connect using a different user name link**. Specify the user credentials, and then click **OK**. In our example, we use the Proxy User we created in *Defining the Local Backup Operator*, on page 8.
6. Click the **Finish** button. The drive is now mapped.

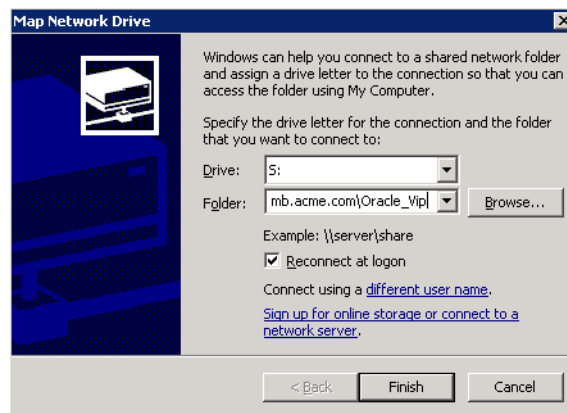


Figure 26 Mapping the Network Drive

Verifying the Virtual Service Directory Contents

Microsoft Windows mounts the drive. The drive can be explored and the following screen displays the file contents of the virtual service export. The files and directories of all the External Filer shares within the Managed volume are available through the Virtual Service CIFS share.

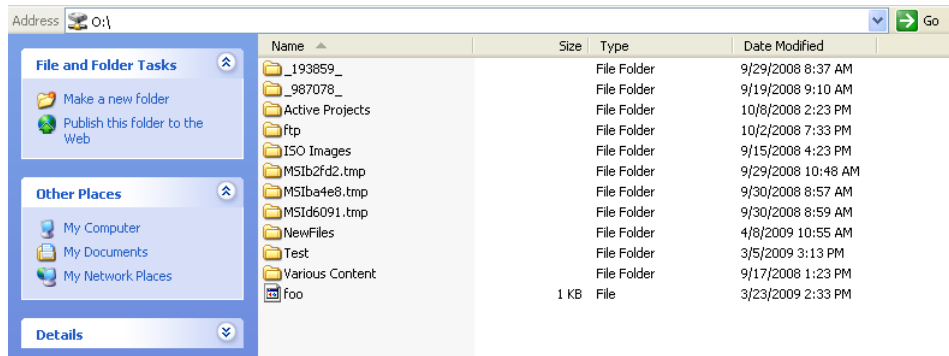


Figure 27 Network Drive Mapping to the Virtual Service CIFS Share

Conclusion

This deployment guide demonstrated the way to integrate F5 ARX platform with the Sun ZFS Storage Appliance. The deployment enables the migration of files from legacy storage platforms onto the Sun ZFS Storage Appliance.

For more information on configuring the F5 ARX, refer to the documentation, available on [Ask F5](#).