



Deploying the F5 ARX with Isilon Systems OneFS

Table of Contents

Deploying the F5 ARX with the Isilon Systems OneFS	
Prerequisites and configuration notes	1
Product versions and revision history	2
Configuration example	3
Configuring the Isilon Cluster	5
Installing and configuring the Isilon cluster	5
Configuring the Secondary and Tertiary Cluster nodes	7
Completing the cluster configuration	8
Creating a local user	11
Configuring Domain user share permissions	12
Modifying a global parameter: Unmappable SIDs	13
Configuring the ARX for Isilon Systems OneFS	14
Configuring Active Directory authentication	14
Creating the CIFS Namespace	16
Adding the external filers	17
Verifying ARX access with command line utilities	17
Creating a Volume	20
Adding root level share	21
Adding the Isilon CIFS share	22
Create the Virtual Service	22
Confirming the Virtual Service is functional	25
Creating an ARX Metadata report	27
Creating the File Migration policy	29
Removing the Legacy Storage CIFS share	32
Conclusion	33

Deploying the F5 ARX with the Isilon Systems OneFS

Welcome to the F5 ARX deployment guide for Isilon® Systems OneFS®. This guide provides step-by-step procedures on how to configure the F5 ARX with the Isilon OneFS Clustered file system.

OneFS is Isilon's sixth-generation operating system that provides the intelligence behind all Isilon scale-out storage systems. It combines the three layers of traditional storage architectures—file system, volume manager and RAID—into one unified software layer, creating a single intelligent file system that spans all nodes within a cluster.

For more information on Isilon OneFS, see <http://www.isilon.com/onefs-operating-system>

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:

- ◆ Equipment physically racked and powered on, with ethernet interfaces cabled properly, VLANs provisioned, and the initial ARX switch interview completed.
- ◆ For NTLM Authentication, the F5 Secure Agent must be on the Active Directory Domain Controller. An AD Domain User must be preconfigured and assigned to be the ARX Proxy User.
- ◆ The ARX platform is deployed in redundant pairs. The secondary switch is a Hot Standby switch. Redundant switch configuration steps within the product documentation should be followed in order to deploy a high available configuration.
- ◆ The screenshots and command line examples in this guide may differ slightly from your device. The configuration procedures are valid.

The following features of the ARX are not supported:

- *Access Based Enumeration*
A file server CIFS share with Access Based Enumeration provides customized directory listing to its clients. This is a directory listing that only contains files and folders where the client has Read access. The intent of this feature is to reduce client curiosity about files and directories that they are prohibited from reading.
- *Compression*
A volume that supports compressed files allows its clients to compress its files and preserves the file compression for policy migrations and shadow copies. If any back-end CIFS filer does not support compressed files, you must disable the feature for its namespace volume.

- *Sparse Files*
Some applications create “holes” in files with no data (that is, all zeros); a volume that supports sparse files like these does not use any disk space for those holes. If any back-end CIFS filer does not support sparse files, you must disable the feature for its namespace volume.
- *Multi protocol 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.
- *ARX CIFS Multiplexing*
The ARX CIFS Multiplexing feature is not supported.

Product versions and revision history

Product Tested	Version Tested
F5 ARX	6.1.0 HFRU#1
Isilon Systems OneFS	6.5.1.8

Document Version	Description
1.0	New guide
1.1	Updated versions supported and removed support for previous versions. Removed Filer Subshares from the Not Supported list. Corrected example IP address in ARX external filer configuration.

Configuration example

In the following diagram, we show basic connectivity between clients, ARX, legacy storage and Isilon. The ARX accesses the Isilon CIFS shares through a Virtual CIFS Server (floating IP address). The IP address is active only on one of the nodes at a time. In case of failure, the IP address ownership transitions to another node.

Isilon also supports multiple IP addresses that are configured to access the file storage in an Active-Active cluster configuration. The F5 ARX does not support Active-Active cluster access to the same storage resources. This deployment guide is written to address an Isilon Smart Connect configuration containing only one Smart Connect Service IP address.

The ARX imports the Isilon Shares into a managed volume. The managed volume is presented to the network clients as an ARX Virtual Service. A fileset Migration policy is defined to migrate the file contents of the Legacy Storage to the Isilon storage system. See Figure 1, on page 4.

Isilon Clustering Information

The minimum size of any Isilon cluster is three nodes, while the required minimum protection level depends on the type of Isilon node. For most Isilon node types, the minimum cluster size of three nodes ensures the minimum protection level of N+1. However, for 4U Isilon IQ x-Series and NL-Series nodes, and IQ 12000x/EX 12000 combination platforms, the minimum cluster size of three nodes requires a minimum protection level of N+2:1. All Isilon IQ clusters use high-speed, low-latency InfiniBand fabric for intra-cluster communication. A cluster can grow to a maximum of 144 nodes.

Two types of networks are associated with a cluster: internal and external.

- ◆ *Internal*

Communication occurs using Gigabit Ethernet or Infiniband, with the option to configure an additional failover network for redundancy. Essentially, the back-end network acts as the backplane of the cluster, enabling each node to act as a contributor to the whole. We recommend you avoid using the back-end network for any other purpose.

- ◆ *External*

Clients connect to the cluster using the external Gigabit Ethernet connections. The Isilon cluster supports standard network communication protocols, including UNIX file sharing (NFS), Windows file sharing (CIFS), HTTP, and FTP. The cluster includes various front-end Ethernet connections, providing flexibility for a wide variety of network configurations. Front-end speeds vary from 100 megabits to 10 gigabits across various products.

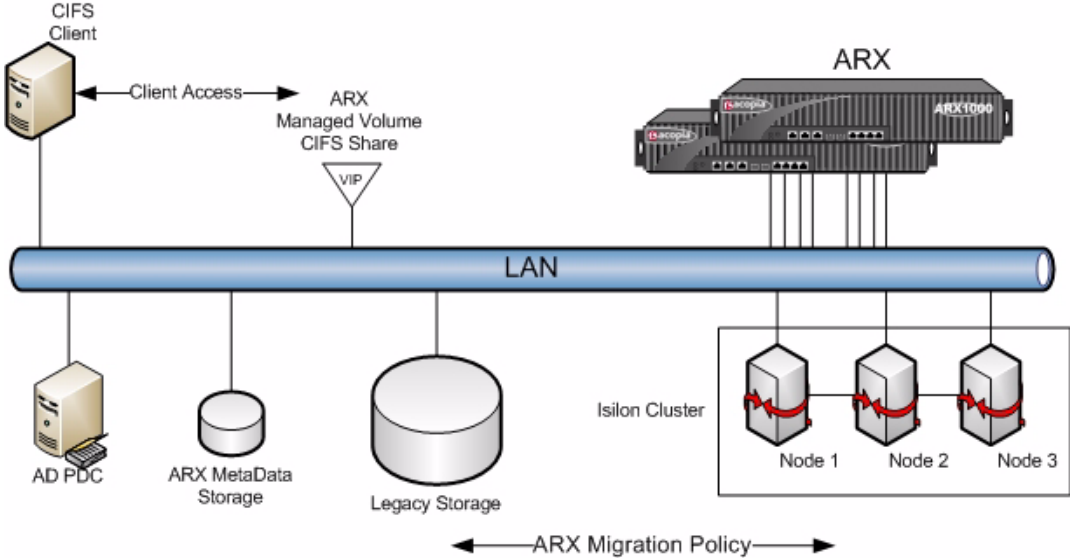


Figure 1 Logical configuration example

Configuring the Isilon Cluster

This section contains the detailed procedures to build an Isilon Systems Cluster configuration. Before beginning this section, the cluster nodes should be unpacked, racked, and powered on with network connectivity configured on the access switch.

Installing and configuring the Isilon cluster

With the cluster nodes powered on and the physical network connections installed, we begin installation and configuration of the cluster.

To install and configure the Isilon cluster

1. Connect to the console interface of the first node using a terminal emulation program.
The serial console parameters are **115,200 bps, N-8-1** with **hardware flow control**.
2. When prompted to format the drives, type **Yes**.
The Isilon cluster configuration wizard automatically starts.
3. From the *Select an option* prompt, type **1** to create a new cluster.

```
Welcome to the Isilon IQ configuration wizard.
Copyright (c) 2001-2009 Isilon Systems, Inc. All rights reserved.
Enter 'help' at any prompt for additional information on that step.
Enter 'back' at any prompt to return to previous step.
Enter 'quit' at any prompt to discard all changes.
Enter 'manual' at any prompt to switch to manual mode (console).

Node build: Isilon OneFS v5.5.3.8 B_5_5_3_8(RELEASE)
Node serial number: None

Select an option:
[ 1] Create a new cluster
[ 2] Join an existing cluster
[ 3] Exit wizard and configure manually
Wizard >>> █
```

Figure 2 Cluster Configuration Wizard creation options

4. From the *change the root password* prompt, type a new password.
When prompted, re-enter the password.
5. From the *change the admin password* prompt, type a new password.
When prompted, re-enter the password.
6. From the *send critical alerts back to Isilon* prompt, type **yes** or **no**.
In our example, we type **no**.
7. At the *name* prompt, type a name for this cluster.
8. From the *encoding* prompt, leave the default, **UTF-8**. Do not select any other encoding type.

The cluster has at least two network interfaces. They are named *int-a* and *ext-1*. The next step is to assign each interface an IP addresses. This range of IP addresses are assigned to the secondary and tertiary nodes automatically.

9. From the *configure interface int-a* prompt, Type **1** to define the Network Mask. Select **3** to define the list of IP addresses. Follow the prompts.

```
Configure interface int-a:
[ 1] Configure netmask
[ 2] Configure MTU
[ 3] Configure int-a IP ranges
[Enter] Keep the current configuration:
      Netmask: 255.255.255.0
           MTU: 1500 (shared)
      IP ranges: 10.1.1.10-10.1.1.12
Configure interface int-a >>> █
```

Figure 3 Internal IP address pool settings

10. From the *external network interface* prompt, type **1** and then press **Enter**. Type **1** to define the Network Mask. Select **3** to define the list of IP addresses. Follow the prompts.
11. From the *default gateway* prompt, type the IP address of the default gateway and then press **Enter**.
12. From the *configure SmartConnect settings* prompt, type **1** to configure a zone name. Type a name, and then press Enter. In our example we type **F5-Isilon**. Type **2** to configure the service IP address. Type the IP address and then press Enter. In our example, we type **10.2.2.13**.

◆ **Note**

F5 ARX only supports an Isilon SmartConnect configuration with a single floating IP address.

13. From the DNS settings prompt, type **1** and then type the DNS server IP address. If you have more than one DNS server, type the IP addresses in a comma separated list. In our example the single DNS server is at **10.2.2.254**. Type **2** and then type the search domain. In our example, the search domain is **siterequest.com**. Press **Enter** to continue.
The configuration of the External Subnet is complete.
14. Press **Enter** to continue.

15. At the *time zone* prompt, type **1** and then type the time zone. Type **2** and then configure the day and time. Press **Enter** to continue.
16. From the *cluster join mode* prompt, type **1** or **2**. This is the method for other nodes to join this cluster. In our example, we type **1** for manual (the default).
17. Press Enter, and the cluster configuration is printed to the console. Review the settings. If they are correct for your environment type **Yes** to continue. Otherwise type **No** and correct the settings.

```

You have made the following configuration changes:
Cluster name       : (not set) -> F5-Isilon
Encoding           : (not set) -> utf-8
int-a netmask     : (not set) -> 255.255.255.0
int-a IP ranges   : (not set) -> { 10.1.1.10-10.1.1.12 }
External netmask  : (not set) -> 255.255.255.0
External IP range : (not set) -> { 10.2.2.10-10.2.2.12 }
External gateway  : (not set) -> 10.2.2.1
SmartConnect zone name : (not set) -> F5-Isilon
SmartConnect service IP: (not set) -> 10.2.2.13
DNS servers       : (not set) -> { 10.2.2.254 }
Search domains    : (not set) -> { siterequest.com }
Time zone         : Greenwich Mean Time -> Eastern Time Zone
Current date/time  : 2010/07/28 12:42:50 GMT -> 2010/07/28 15:42:05 EDT

Do you wish to commit these changes? [yes]
Commit changes? >>> █

```

Figure 4 Cluster configuration settings

The primary cluster node boots and applies the settings. Wait for the Login prompt to appear on the console.

Configuring the Secondary and Tertiary Cluster nodes

The next task is to configure the secondary and tertiary cluster nodes. These are much simpler to configure than the primary. As long as network connectivity is properly configured so all the nodes can receive each other's traffic, the nodes automatically select IP settings from the IP Pools defined on the primary node and configure themselves. However, there are some initial settings to configure.

To configure the secondary and tertiary cluster nodes

1. Disconnect the console cable from the first node and connect it to the next cluster node. The node boots up.
2. From the *format drives* prompt, type **Yes** and then press **Enter** to format the drives.
3. From the *cluster* prompt, type **2** to join an existing cluster. The node broadcasts on the network and discovers the local cluster names.

- From the *cluster* list, type the number of the cluster you created in the preceding procedure, and then press Enter. In our example, we select 1 for F5-Isilon.

```
Select the cluster you want to join
Index  Name      Version  Status
-----
1      F5-Isilon  B_5_5_3_8R  available
[Enter] Refresh the list
Join cluster >>> 1
```

Figure 5 Select the cluster to join

The node joins the cluster and automatically configures the IP addresses, netmasks, and DNS attributes from the Primary node's pool configuration. The node boots and becomes an active cluster member.

- Repeat this entire procedure for each tertiary cluster node member.

Completing the cluster configuration

In this section, we configure the cluster to join the Active directory domain, assign the backup operator to run with root privileges, and create the CIFS shares created.

Logging on to the Isilon Administration utility

The first task is to log on to the Isilon Administration utility.

To complete the cluster configuration

- Open a web browser, and in the Address box, type the IP address of the Smart Connect interface. In our example, we type **http://10.2.2.13**.
The Isilon Administration utility opens.
- Login as **root**, with the password you created in step 4 of *Installing and configuring the Isilon cluster*, on page 5.
The Cluster Status page opens.

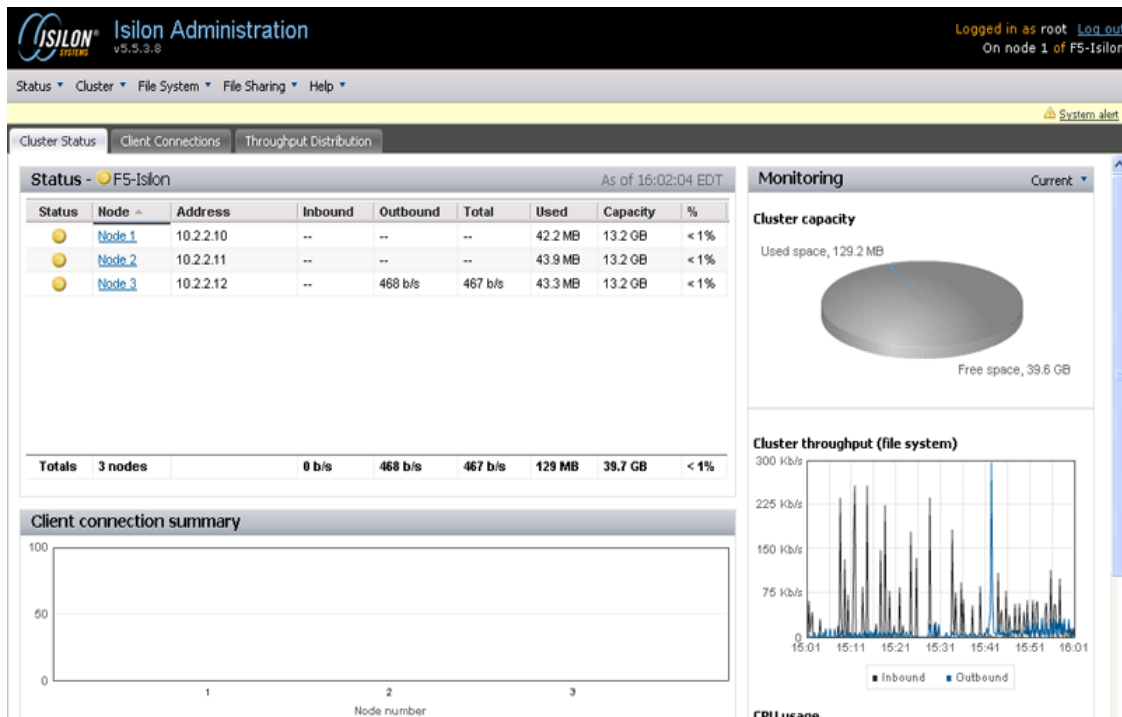


Figure 6 Cluster Status

In our example, there are three cluster nodes configured.

Joining the Active Directory domain

The next task is to join this cluster configuration with the Microsoft Active Directory domain.

To join the Active Directory domain

1. From the **File Sharing** menu, select **CIFS Windows File Sharing** and then click **Domain And Authentication Mode**.
The Domain and Authentication mode page opens.
2. Click the **Enable domain mode** link to join the domain.
The Configure Domain Mode screen opens.
3. In the Configure Domain Mode section, complete the following
 - a) In the **Domain** box, type the domain. In our example, we type **siterequest.com**. You can optionally type a description.
 - b) From the **Domain Account Username** box, type the user name (we type **Administrator**). In the **Domain Account Password** box, type the associated password.
 - c) Click **Submit**

Once the cluster completes the join process, the Domain and Authentication mode screen is displayed. The status should show *Enabled*, the Mode shows *Active Directory Domain*, and the proper *domain* is listed.

Creating the Isilon CIFS share

The next task is to create a CIFS share from the Administration utility.

To create the CIFS share

1. In the Isilon Administration utility, from the **File Sharing** menu, select **CIFS - Windows File Shares**, and then click **Shares**. The list of existing shares opens.
2. Click the **Add Share** link. The Add Share screen opens.
3. On the Add Share page, complete the following:
 - a) In the **Share Name** box, type a name. In our example, we type **share1**.
 - b) *Optional*: In the **Description** box, type a description.
 - c) In the **Directory to share** box, type the directory, or click **Browse** to locate the directory manually.
 - d) Click **Submit**.

[Shares](#) | [Domain and Authentication Mode](#) | [Global Parameters](#) | Add Share

CIFS - Windows File Sharing > Add Share

Basic Settings

Share name: *	<input type="text" value="share1"/>
Description:	<input type="text" value="Isilon Share : F5 ARX"/>
Directory to share:	<input type="text" value="/ifs/share1"/> <input type="button" value="Browse..."/>
Directory ACLs:	<input checked="" type="radio"/> Apply Windows default ACLs <input type="radio"/> Do not change existing permissions

Figure 7 Add Share Parameters

4. If the file directory does not exist, you are prompted to create the it. Click **Create Directory** and then **Submit** to continue. The Share listing displays.
5. Repeat this entire procedure to create additional shares. In our example, we create two more CIFS shares, named **share2** and **share3**.

Creating a local user

The ARX requires a user with privileged access to the cluster in order to migrate and synchronize file attributes. This is normally an Active Directory user with Backup Operator group privileges. For the Isilon filer, this user needs to be created as a **local user** with administrator privileges. The user name and password need to match the same user name and password you will provision on the ARX later in this document.

To add a new local user

1. From the Administration utility, next to *Local Users*, click **Add user**. The New User screen opens.
2. On the New User page, complete the following
 - a) In the **User name** box, type a user name. In our example, we type **acmeuser001**.
 - b) In the **Full name** box, type the full name. In our example, we type **ARX Proxy User**.
 - c) In the **Password** and **Confirm password** boxes, type the associated password.
 - d) From the **Primary Group** list, select **Administrators**.
 - e) From the **Shell** list, select a shell.
 - f) Any additional groups are optional.
 - g) Click **Submit** to continue.
 - h) Because the Home Directory does not yet exist, the you are prompted to create it. Click **Yes** at the prompt and then click **Submit**.

Status ▾ Cluster ▾ File System ▾ File Sharing ▾ Help ▾

Local Users > Edit User

User name: *

Full name: *

Password: *

Confirm password: *

Home directory: *

Primary group: *

Shell: *

Enabled

Figure 8 New user settings

Configuring Domain user share permissions

The Active Directory Domain User assigned to be the ARX Proxy user must be allowed to *Run as Root*. This is a share parameter in the Windows File Sharing configuration, and must be configured on each share.

To configure the share permissions

1. From the **File Sharing** menu, select **CIFS - Windows File Share** and then click **Shares**. The share listing displays.

Shares | [Domain and Authentication Mode](#) | [Global Parameters](#) | [Add Share](#)

CIFS - Windows File Sharing > Shares

Number of shares: 4

Name	Directory	Description		
ifs	/ifs	ifs	Edit	Delete
share1	/ifs/share1	Isilon Share: F5 ARX	Edit	Delete
share2	/ifs/share2	Isilon Share2 : F5 ARX	Edit	Delete
share3	/ifs/share3	Isilon Share3 : F5 ARX	Edit	Delete

Figure 9 Share listing

2. Click the **Edit** link next to one of the shares. The Users and Groups page opens.
3. Click the **Add** button to add the ARX Proxy user domain user to the share. The Add Users or Groups box opens.
4. In the **Name** box, type the Domain User name and then click **Search**. In our example, we type **acmeuser001**.
5. From the list of users, select the Domain User and then click **Add**. The User appears in the list.
6. Click **Edit permissions** next to the user. The Edit Permissions box opens.
7. Click the **Run as Root** box, and then click **OK**.
8. Repeat steps 2-7 for each of the shares in your implementation.

With these values set the Active Directory Domain User assigned to be the ARX Proxy user now has the appropriate share permissions to modify file ACLs as necessary.

Modifying a global parameter: Unmappable SIDs

The next task is to modify a global parameter on the Isilon cluster. This parameter change allows the cluster to ignore SIDs that are unmappable.

To modify the global parameter

1. From the **File Sharing** menu, select **CIFS - Windows File Share** and then click **Global Parameters**.
2. In the Security Parameters section, click the box to the left of **Onefs: ignore unmappable SIDs**.
3. From the **ignore unmappable SIDs** list, select **Yes**.
4. Click **Submit**.

The screenshot shows the Isilon Administration interface for version v5.5.4.2.1. The navigation menu includes Status, Cluster, File System, File Sharing, and Help. The breadcrumb trail is Shares > Domain and Authentication Mode > Global Parameters > Add Share. The main heading is CIFS - Windows File Sharing > Global Parameters. A warning message states: "Uninformed changes to the following parameters may result in an operation failure." The General Parameters section includes: Log level (0), SMB ports (445 139), and VFS objects (onefs_shadow_copy onefs). The Security Parameters section includes: Encrypt passwords (yes), Guest account (nobody), Map to guest (never), Force username map (yes), Onefs: ignore SACLs (no), Onefs: ignore unmappable SIDs (checked, yes), and SMB server signing (never).

Figure 10 Onefs: ignore unmappable SIDs

This completes the Isilon configuration section.

Configuring the ARX for Isilon Systems OneFS

In this section, we detail the procedures necessary to configure the ARX for virtualizing the Legacy Storage and the new Isilon Clustered storage into a Managed Volume. The ARX is configured to access the Legacy Storage and the Isilon cluster.

This guide demonstrates how to configure the solution for a fileset migration policy. Legacy storage is decommissioned and the file contents are migrated to the Isilon Cluster. Network clients continue to have access to the Legacy Storage file contents through the ARX Virtual Service during file migration.

Configuring Active Directory authentication

The first task in configuring the ARX is to configure Active Directory authentication. To configure Active Directory authentication, you must create an NTLM server, create a proxy user, and then add the Active Directory Forest details.

Creating the NTLM Auth server

The first step in configuring Active Directory Authentication is to create an NTLM Auth. Server on the ARX device.

To configure Active Directory authentication

1. On the ARX user interface, from navigation pane, expand **Authentication** and then click **NTLM Auth. servers**.
2. Click the **Add** button.
3. In the **NTLM Auth. Server Name** box, type the FQDN name of this server. In our example, we type **siterequest**.
4. In the **IP address** box, type the IP address.
5. In the **Windows Domain** and **Pre Win2k Domain** boxes, type the Windows Domain. In our example, we type **siterequest.com**.
6. In the **Secure Agent Password** and confirmation boxes, type the Secure Agent Password. The Secure Agent password is the password assigned on the Domain Controller for the Secure Agent application.
7. Click the **Ok** button.

Add NTLM Authentication Server	
NTLM Auth. Server Name	Siterequest
IP Address	10.16.112.10
Windows Domain	siterequest.com
Secure Agent Password	••••••••••
Confirm Secure Agent Password	••••••••••
Agent Port	25805

Figure 11 Create a new Authentication Server

Creating the proxy user

The next task is to create proxy user. This is the same user that was configured as a local user within the administrators group in *Creating a local user*, on page 11. These user credentials are used to access the backend filer CIFS shares.

To create the proxy user

1. From navigation pane, expand **Authentication**, click **CIFS Proxy Users**, and then click the **Add** button.
2. In the **Proxy User Name** box, type the name. In our example, we type **proxy_user**.
3. In the **Proxy User Account** box, type the proxy user account. In our example, we type **acmeuser001**.
4. In the **Proxy User Account Password**, type the password. Retype the password in the **Confirm** box.
5. In the **Windows Domain** and **Pre Win2k Domain** boxes, type the appropriate Windows Domain. In our example, we type **siterequest.com** and **siterequest** respectively.
6. Click the **OK** button. You return to the CIFS authentication page.

Add CIFS Proxy User	
Proxy Username	proxy_user
Proxy User Account	acmeuser001
Proxy User Account Password	•••••
Confirm Proxy User Account Password	•••••
Windows Domain	siterequest.com
Pre Win2k Domain	siterequest

Figure 12 CIFS Proxy User

Adding the Active Directory Forest details

The next task is to add the Active Directory Forest details to the ARX.

To add the Active Directory Forest details

1. From navigation pane, expand **Authentication**, click **Active Dir. Forests**, and then click the **Add** button.
2. From the **Domain Type** list, select **forest-root**.
3. In the **Domain Name** box, type the Domain name. In our example, we type **siterequest.com**.
4. In the **Domain Controller IP** box, type the Controller IP.
5. Check the **Preferred**, **KDC**, and **DNS** boxes, and then click the **Add** button.
6. Click **OK**.

Verifying Active Directory Authentication

Next, we verify the ARX is properly joined to the Active Directory domain.

Log into the ARX command line interface using SSH. Type the following:
show active-directory status

```
arx500-1# show active-directory status

Offline timeout is set to 2000 milliseconds.

PROCESSOR 1.1:

Domain Name                               Domain Controller   Status   Preferred
-----
SITEREQUEST.COM                           10.60.112.10        Active   Yes
```

Verify that the Status state is **Active**.

The Active Directory authentication configuration is complete.

Creating the CIFS Namespace

Next, we create the CIFS Namespace.

To create the CIFS namespace

1. From 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 **Isilon**. You can optionally type a description.
 4. From the **Protocol** list, click the **CIFS** box, and then click **Next**
 5. In the CIFS authentication protocol section, check the **Use Kerberos** and **Use NTLM** boxes.
 6. In the Proxy User section, select the user you created in *Creating the proxy user*, on page 15. In our example, we select **proxy user**.
 7. Click **Next**.
 8. Review the summary and then click **Finished**.

Adding the external filers

In this section, we add the Legacy Server and the Isilon Cluster as external filer entries in the ARX. These entries are 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 **Legacy**.
4. In the **Primary IP Address** box, type the primary IP address. In our example, we type **10.2.2.13**.
5. In the **Secondary IP Address** box, 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 back end file shares, and click the **Add** button.
8. Click the **OK** button.
9. **Repeat** this entire procedure to add the Isilon cluster as a Filer. Name the entry **Isilon** and use the IP address of the cluster.

Verifying ARX access using the command line

With the external filers and the ARX proxy user defined, the shares can be tested to verify the ARX and filers have the proper credentials.

Log onto the ARX from the command line, and type the command **show exports**. Review the list of exports and compare with the server.

In our example, it shows the following:

```
arx1000-2# show exports external-filer Isilon proxy-user proxy_user
Export probe of filer "Isilon" at 10.2.2.13
```

Connectivity:

Slot.Proc	Proxy Address	Ping (size: result)
1.2	10.2.2.21	64: Success 2000: Success 8820: Success
1.3	10.2.2.22	64: Success 2000: Success 8820: Success
1.4	10.2.2.23	64: Success 2000: Success 8820: Success
1.5	10.2.2.24	64: Success 2000: Success 8820: Success

CIFS Credentials:

```
User          acmeuser001
Windows Domain siterequest.com
Pre-Win2k     SITEREQUEST
```

Capabilities:

```
CIFS
Security Mode      User level, Challenge/response, Signatures optional
Extended Security Kerberos, NTLMSSP
Server             TCP/445, TCP/139
Max Request       16644 bytes
IPC$ Share        Access OK
Auth Method       NTLMv2
Discovered SPN    Isilon@SITEREQUEST.COM
```

Shares:

Share	Storage Space		Serial Num
	Total (MB)	Free (MB)	
share1	76795	76746	06f1-698a
share2	76795	76746	06f1-698b
share3	76795	76746	06f1-698c

Time:

```
CIFS
Filer's time is ahead of the switch's time: 00:00:19
```

The ARX command probe exports is useful to check that the ARX and the proxy user settings have the proper credentials. If the **Write** and the **Privs** columns report **OK** then the ARX is properly credentialed. For example:

```
arx1000-2# probe exports external-filer Isilon proxy-user proxy_user
Export probe of filer "Isilon" at 10.2.2.13
```

```
CIFS Credentials:
```

```
User          acmeuser001
Windows Domain siterequest.com
Pre-Win2k     SITEREQUEST
```

```
Security:
```

```
CIFS
```

```
Description Key: OK (success) NO (failure) -- (not applicable)
```

Share	Write	Privs
-----	-----	-----
share1	OK	OK
share2	OK	OK
share3	OK	OK

The ARX can also show the CIFS attributes of the CIFS shares. This is useful to verify the CIFS features the filer can support. These CIFS features are applied to the ARX configuration in the next section *Creating a Volume*, on page 20.

```
aarx1000-2# show exports external-filer Isilon attributes proxy-user proxy_user
Export probe of filer "Isilon" at 10.2.2.13
```

```
CIFS Credentials:
```

```
User          acmeuser001
Windows Domain siterequest.com
Pre-Win2k     SITEREQUEST
```

```
Attributes:
```

```
CIFS
```

```
Codes: AE=Access-based Enum, CF=Compressed Files, NS=Named Streams,
        PA=Persistent ACLs, SF=Sparse Files, UD=Unicode On Disk
```

Share	Attributes						
	AE	CF	NS	PA	SF	UD	
-----	--	--	--	--	--	--	
share1	-	-	X	X	-	X	
share2	-	-	X	X	-	X	
share3	-	-	X	X	-	X	

The Isilon cluster supports Named Streams, Persistent ACLs, and Unicode on Disk.

Creating a Volume

The backend filer CIFS shares will be incorporated into an ARX Managed Volume. In this example, we place the Volume Metadata onto the new Isilon Cluster. One of the new CIFS shares is used to store the ARX metadata database. Because the Isilon Cluster is the target for the legacy storage to be migrated to it, the MetaData database is provisioned onto it.

To create the managed volume

1. From the navigation pane, click **Managed Volumes**, and then click the **Add** button.
2. From the **Namespace** list, select the name of the Isilon namespace you created. In our example, we select **Isilon**.
3. In the **Volume Name** box, type the name for the volume. In our example, we type **/data**. You can optionally type a description.
4. Click **Next**.
5. From the **Metadata file server protocol** list, select **NFS**.
6. From the **Metadata file server** row, click the **Add** button to create an external filer. The new file server wizard opens. Complete the following:
 - a) In the **Name** box, type a name for this File Server. In our example, we type **Metadata-Server**.
 - b) In the **Primary IP Address** box, type the primary IP address.
 - c) In the **Secondary IP Address** box, type any secondary IP addresses, and click the **Add** button. In our example, we do not include any secondary IP addresses.
 - d) In the **Description** box, you can optionally type a description.
 - e) Click the **Save** button. You return to the wizard.
7. In the **Metadata CIFS share/ NFS path** box, type the path. In our example, we type **/metadata**.
8. Click the **Next** button. The CIFS parameter option page opens.
9. Check the box in the **Auto-synchronization** section.
10. In the CIFS Attributes section, uncheck the **Auto detect CIFS Attributes** box. Click to check the **Named Streams, Unicode on Disk, and Persistent ACLs** and then click **Next**. The Volume parameters page opens.

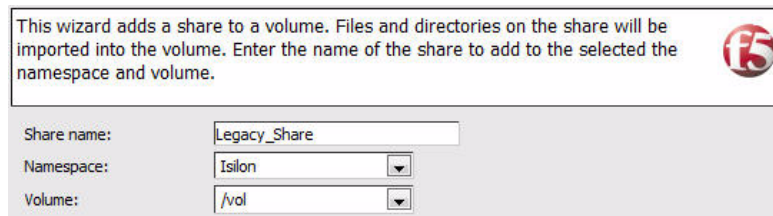
Note: The values for these attributes were learned in the previous section from the output of the `show exports` command.
11. Click the **Files and directories can be renamed during import and re-import** button.
12. Check the **Enable the volume when finished** box. Click **Next**.
13. Review the summary, and then click **Finish**.

Adding root level share

First file share we add is the root level share. This is the incumbent legacy storage volume with file content. The subsequent shares to be added 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 16. In our example, we select **Isilon**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 20. In our example, we select **/vol**. 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

Namespace: Isilon

Volume: /vol

Figure 13 Share name definition

6. From the **File Server** list, select the name of the file server you created in step 3 of *Adding the external filers*, on page 17. In our example, we select **Legacy**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **vol4**.
8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes.
9. In the Enable Share section, check to enable the share, and also click **Allow the switch to import this share even if owned by another ARX**.
10. Click the **Next** button.
11. Review the summary, and click the **Finish** button.

Adding the Isilon CIFS share

In this task, we add the Isilon Cluster CIFS share named *share2* to the managed volume. This share synchronizes its attributes with the root level share. This share also becomes the root share after the Legacy file contents have been migrated.

To add the Isilon 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 **Isilon_Share2**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 16. In our example, we select **Isilon**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 20. In our example, we select **/vol**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in step 9 of *Adding the external filers*, on page 17. In our example, we select **Isilon**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share2**.
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** boxes.
9. In the Enable Share section, check to enable the share, and also click **Allow the switch to import this share even if owned by another ARX**.
10. Click the **Next** button.
11. Review the summary, and click the **Finish** button.

With the two external filer CIFS shares added to a managed volume a virtual service can be defined to allow network clients access to the volume contents.

Create the Virtual Service

The Virtual Service is how the ARX presents the 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 is opens.
3. From the **Namespace** list, select the namespace you created in *Creating the CIFS Namespace*, on page 16. In our example, we select **Isilon**.
4. Click the **Create a new virtual service (VIP) button**.
 - a) In the **Virtual service DNS name** box, type the DNS name for the virtual service. In our example, we type **isilon.siterequest.com**.
 - b) In the **IP Address** box, type the IP address of the VIP. In our example, we type **10.2.2.20**.
 - c) In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.0**.
 - d) From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **1**.
 - e) Ensure the **Enable the virtual service when finished** box is checked.
5. Click **Next**.

This wizard creates either a new virtual service (virtual IP address) or adds a new export to an existing virtual service. Select a namespace and whether to add a new service or add an export to an existing service.

Namespace: Isilon

Add export(s) to an existing virtual service (VIP)

Virtual Service Name & IP Address: -- No VIPs are defined --

Create a new virtual service

Virtual service DNS name: isilon.siterequest.com

IP Address: 10.2.2.20

Subnet Mask: 255.255.255.0

VLAN ID: 1

[Enable Virtual Service](#)

Enable the virtual service when finished

Figure 14 Create new Virtual Service Wizard

6. In the **Windows Domain Name** and **Pre Win2k Domain** boxes, type the Windows domain name. In our example, we type **siterequest.com**.

7. The other settings on this screen are optional, configure as appropriate for your deployment. In our example, we leave the rest of the settings at the default level.
8. Click the **Next** button. The Virtual Service Exports screen opens.
9. From the **Volume** list, select the appropriate volume. In our example, we select **/vol**.
10. In the **Volume Path** list, type the path to the volume. In our example, we type **/**.
11. In the **Export Name** box, type a name for the Export. In our example, we type **virtual_Isilon**. You can optionally type a description.
12. Configure the other options as applicable for your configuration, and then click the **Add Export** button.
13. Confirm the creation of the Virtual Service and click **Finish** to continue. Review the Virtual Service by selecting Virtual Services from the left pane. Notice the admin state is **enabled** and the status is **ready**.

◆ **Note**

*Notice that the virtual service is reporting **Join Required**. This is required for Kerberos authentication.*

Adding the virtual service to the Active Directory domain

The next task is to incorporate the virtual service into the Active Directory Domain as a Domain Computer.

To add the virtual service to the Active Directory domain

1. From the navigation pane, click **Virtual Services**, check the box next to the virtual service you just created, and then click the **Join Domain** button.
2. In the **Username** box, type the appropriate user name.
3. In the **User Password** box, type the associated password.
4. In the **Organizational Unit** box, type the organizational unit.
5. Click **OK**.

Join Active Directory Domain

When a namespace is configured with kerberos authentication, associated virtual services must be joined to an Active Directory domain. This adds the virtual service as a computer in Active Directory.

Domain Name	siterequest.com
Username	administrator
User Password	••••••••
Organizational Unit	Computers

Figure 15 Join Active Directory Domain

The *Virtual Service Summary* page opens. Notice the *Domain Join* column is reporting **Joined**. Click the Domain Name entry. Select the *CIFS Exports* tab. The Export Summary will be displayed. Notice the status is **Online** and the ARX managed volume is **/vol/**.

A network client can now connect to the ARX virtual service and begin accessing the CIFS share.

Confirming the Virtual Service is functional

The next task is to confirm the Virtual Service is operating properly. In this procedure, you map a network drive to the Virtual Service Export using the test Windows Client. The export shows files and directories exist. The user at first cannot determine on which of the backend file shares the files reside. The ARX has merged the files and directories into one common virtual path.

To map the virtual service CIFS Share to a drive letter

1. From the Windows 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 `\\silon.siterequest.com\virtual_Isilon`.
5. Click the **Connect using a different user name link**. Specify the Domain user with the proper access rights. In our example, we use the Proxy User credentials, and then click **OK**.
6. Click the **Finish** button. The drive is now mapped. The drive can be explored and the following screen displays the file contents of the virtual service export.

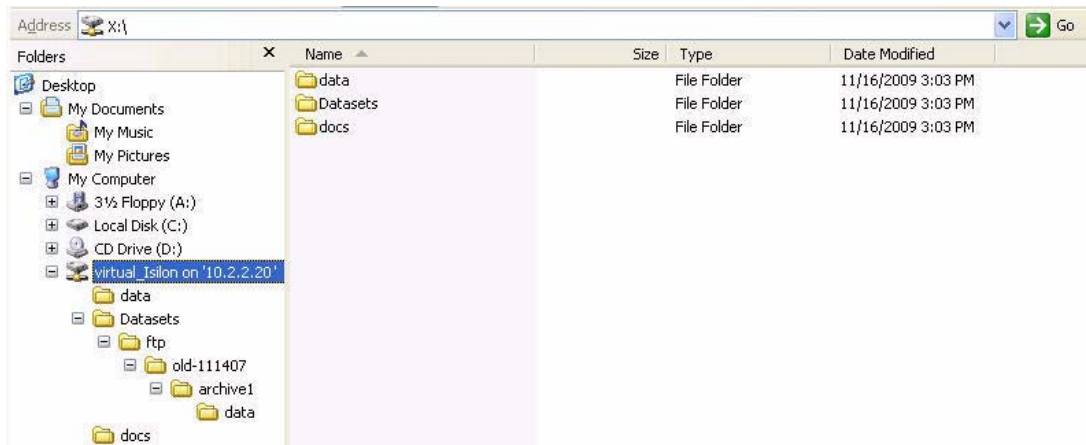


Figure 16 Virtual service shared drive contents

In this example there are multiple root level directories. Under these directories there is various test content. The content is currently stored on the Legacy Storage platform. It's unclear from this point of view where the content resides with regards to the ARX External Filers. In the next section a metadata report will be generated to show the actual file placement.

The volume statistics can be viewed from the ARX GUI by selecting the **Managed Volume** menu item in the left pane. Select the hyperlink **/vol** volume. In our example the volume contains 1200 files distributed within 8 directories requiring 3.9 MB of disk space.

Volume Name	/vol
Admin State	Enabled
Status	Normal
Description	Isilon Cluster Managed Volume
Protocols	CIFS
Metadata Size	548 kB
Metadata Free Space	74 GB
Free Space	74 GB
Shares	2 of 2 enabled
Files	1.2 k (8 dirs) of 3.9 M
VPU	1 (domain 1)
Processor	1.1
Auto Reserve Files	Enabled
Shadow Target	No
Snapshots	Not Enabled
Snapshot Timeout	50 seconds
Snapshot Directory	~snapshot
Free Space Calculation	Automatic
Import Conflict	Files and directories can be renamed during import and a re-import. (per share setting)
Auto Synchronize	On
Filer Subshares	Disabled
Oplock Support	Enabled
Access Based Enumeration	Disabled
CIFS Characteristics	Named streams, Persistent ACLs, Sparse files, Unicode on disk

Figure 17 Managed volume /vol Details

In order to determine which backend filers the file contents reside on a metadata report can be generated on the ARX.

Creating an ARX Metadata report

The file placement can be determined by executing an ARX report. The administrator can also view the directory contents on the backend servers and see how the files are placed. In this procedure we demonstrate how to create an ARX Report.

To create an ARX Report

1. From the left navigation pane, click **Managed Volumes**.
2. Click on the Managed Volume **/vol**
3. Click the **Report** button.
The Report Volume screen opens.
4. In the **Path** box, you can type a path.
In our example, we leave it at the default: /
5. From the **Report Type** row, click **Metadata**.

6. In the **Output Report Name** box, type a name for the report. In our example, we type **Verification_Report**.
7. Click the **OK** button. The report is generated.

The report lists the ARX attributes including Software version, Platform, time the report was run. And most importantly the Namespace, Volume, Path and external filers shares. In this example nearly all the files reside on the **Legacy_Share**.

```

**** Metadata-Only Report: Started at Wed Aug  4 11:12:51 2010 ****
**** Software Version: 5.01.005.11965 (Mar  9 2010 17:25:04) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: Isilon
**** Volume: /vol
**** Path: /vol

Share                Physical Filer
-----
[Legacy_Share        ] 10.2.2.40:vol4
[Isilon_Share2       ] 10.2.2.13:share2

**** Legend:
****  FL = File: The reported entry is a file.
****  DR = Directory: The reported entry is a directory.
****  LN = Link: The reported entry has a link count greater than one.
****  NL = No Lock: Was unable to lock parent directory during report.
****  CC = NFS case-blind name collision.
****  IC = Name contains invalid CIFS characters.
****  FN = Name may conflict with a filer-generated name.
****  SP = A persistent split is registered in the metadata, due to a FGN.
****  NF = Name is only accessible to NFS clients.

Type                Share                Path
-----
[FL                 ] [Isilon_Share2       ] /psfs.probe
[ DR                ] [Legacy_Share        ] /data
[ DR                ] [Legacy_Share        ] /docs
[ DR                ] [Legacy_Share        ] /Datasets
[FL                 ] [Legacy_Share        ] /docs/psfonts.zip
[FL                 ] [Legacy_Share        ] /data/update_dr_v5g.exp

```

After the migration policy is defined and invoked. Another Metadata report can be generated to verify the files have completely migrated.


Creating the File Migration policy

A fileset migration policy is assigned to a managed volume. It facilitates file movement between backend file shares based on file attributes. The fileset matching attributes include exact match, wildcard expressions, and regular expressions.

In this example, we create a Fileset Migration Policy to move files from the Legacy Storage to the Isilon Cluster. The files are copied to the CIFS Share `/share2`.

To create the fileset migration policy

1. From the left navigation pane, click **Common Operations**.
2. Click the **Fileset Migration** button. The Fileset Migration Wizard opens.
3. In the **Policy name prefix** box, type a prefix. In our example, we type **Migrate_to_Isilon**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 16. In our example, we select **Isilon**.
5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume*, on page 20. In our example, we select **/vol**.
6. Click **Next**.
7. In the **Select Fileset** Box, choose a fileset. In our example we will create a new fileset. Select the **Add** button next to the right of Fileset to create a new fileset to be assigned to the policy.
 - a) In the **Fileset Name** box, type a name for this fileset. In our example, we type **Migrate_All**.
 - b) In the **Fileset Type** box, select a type for this fileset. In our example, we chose **filename**.
 - c) In the **Filename Matching Criteria** radio button selection, select the matching criteria. In our example we chose **Wildcard Expressions**. In the box, we type *****.
 - d) In the **Path Matching Criteria** selection, select the criteria. In our example we chose **Exact Match**, and in the box, typed a directory name of **/**.
 - e) The other fields are optional, configure as applicable for your deployment.
 - f) Click the **Save** button (see Figure 12). You return to the Fileset Migration Wizard.

Create a new fileset. 

Fileset Name:

Fileset Type:

Filename Matching Criteria: Exact Match Wildcard Expression (i.e. shell style) Regular Expression

Filename Matching Criteria:

Exclude Name:

Ignore Case for Name:

Path Matching Criteria: Exact Match Wildcard Expression (i.e. shell style) Regular Expression

Path Matching Criteria:

Exclude Path:

Ignore Case for Path:

Recurse Subdirectories:

Figure 18 New Fileset criteria

8. The next step is to define the **Match Criteria** for the fileset policy. In our example we chose **Files and Directories**.
9. For **Source**, select the Source file share you created in *Adding root level share*, on page 21. In our example, we select **Legacy_Share**.
10. For **Target**, select the appropriate share. In our example, we select **Isilon_Share2**. Click the **Next** button.
11. The next step is to define the **Optional Parameters**. In our example we leave the defaults.
12. Click the **Next** button.
13. Review the summary and then click the **Finish** button.

By default a report is generated for this policy. Select the **Report** menu item from the left pane. A list of reports is displayed. The topmost is the report that was just created for the fileset migration.

Select the report by clicking on the **Report Name** link. A new browser window or tab opens and the report can be reviewed. The following is an example.

```
**** File Placement Report: Started at Wed Aug  4 11:32:51 2010 ****
**** Software Version: 5.01.005.11965 (Mar  9 2010 17:25:04) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:

Place Rule:      Migrate_to_Isilon
```

```

Configuration:
  From fileset:           Migrate_All (files and directories)
  Source share:           Legacy_Share
  Target share:           Isilon_Share2
  Report:                 Migrate_to_Isilon, Verbose, Delete Empty
Reports
  Migrate limit:         0
  Volume Scan:           Enabled
  Inline Notifications:  Enabled
  Promote Directories:   Disabled
  Auto-Close Files:     Disabled

  Tentative:             No
  State:                 Enabled

```

Date	Source Share	Target Share
File		
Result		

Tue Nov 17 13:20:03 2009	Legacy_Share	Isilon_Share2
/vol/data/eula.1041.txt		
Complete		
Tue Nov 17 13:20:03 2009	Legacy_Share	Isilon_Share2
/vol/data/fm-72.txt		
Complete		
Tue Nov 17 13:20:03 2009	Legacy_Share	Isilon_Share2
/vol/data/VC_RED.MSI		
Complete		

The rest of the report output is a listing of all files that were migrated. All the files have been moved from the Legacy Storage to the Isilon Cluster. A metadata report can confirm this.

To generate a metadata report, see *Creating an ARX Metadata report*, on page 27. In this example we named the report **Metadata_Post_Migration**.

The report is generated and is available in the **Reports** menu item. Open the report and review the *Share* column. For each file the Share that is its physically present is reported. Notice all the files report they are residing on the share named **Isilon_Share2**. It may also show directories still exist on the **Legacy_Storage** share. This is normal behavior for the ARX. The Legacy Storage export may now be removed from the managed volume.

Removing the Legacy Storage CIFS share

The legacy storage CIFS share can be removed from the managed volume.

To remove the legacy storage CIFS share

1. From the navigation pane, click **Managed Volumes**.
2. Click the appropriate volume (**/vol** in our example) box, and then click the *Shares* tab.
3. Click a check in the box for the legacy share. In our example, we click **Legacy_Share**.

Managed Volume Details

Namespace: Isilon Volume: /vol

Volume Shares

Buttons: Add... Remove... Edit... Enable Disable Sync...

<input type="checkbox"/>	Share	File Server	File Server Path	Free Space	Transitions	Status
<input type="checkbox"/>	Isilon_Share2	Isilon 10.2.2.13	share2	74 G	1	Online
<input checked="" type="checkbox"/>	Legacy_Share	Legacy 10.2.2.40	vol4	21 M	1	Online

Figure 19 Managed Volume Details

4. Click the **Remove** button. The Remove Share Wizard is opens.
5. Click **Next** to continue.
The removal process ensures any files that may exist on the old share are migrated prior to removal. This is important since users may have added files to the managed volume.
6. Click **Remove and Migrate the contents to another target** and then specify the destination (**Isilon_Share2** in our example).
7. Click **Next** to continue.
8. Click **Finish**. You return to the Managed Volume Details screen. Refresh the browser window and the volume reports that the Legacy Storage is removed and only the Isilon Cluster share exists.

The Legacy Storage platform can now be decommissioned or re-purposed safely. The remaining CIFS Share from the Isilon Cluster could be added to the managed volume either as secondary storage or in a share farm.

Conclusion

This deployment guide demonstrated how to integrate F5 ARX platform with Isilon OneFS cluster file system. This configuration in this deployment enables the virtualization and migration of files from legacy storage platforms to a new Isilon Storage cluster.

For more information on configuring the F5 ARX, refer to the documentation, available on Ask F5

[\(http://support.f5.com/kb/en-us/products/arx.html\)](http://support.f5.com/kb/en-us/products/arx.html)