



Deploying the F5 ARX with NetApp Filers

Table of Contents

Deploying the F5 ARX with Network Appliance filers	1
Prerequisites and configuration notes	1
Product versions and revision history	2
Configuration example	2
Configuring NetApp Filer	3
Initial NetApp configuration	3
Managing Licenses	6
Setting the Date and Time	6
Configuring DNS resolution	7
Reviewing the Disk Aggregate settings	8
Resizing the Volume	9
Creating Volumes	10
Configuring the NFS Export	12
Running the CIFS Setup Wizard	14
Creating the CIFS Share	17
Configuring the ARX	21
Configuring Active Directory Authentication	21
Creating the CIFS Namespace	24
Creating a Managed Volume	24
Modifying the Volume Snapshot attributes	27
Adding root level share	28
Creating Snapshot Support	29
Create the Virtual Service	33
Accessing the CIFS Virtual Service from an XP Client	36
Accessing Snapshots through the Virtual Service	36
Generating an ARX Metadata Report	38
Conclusion	39

Table of Contents



Deploying the F5 ARX with NetApp Filers

Deploying the F5 ARX with Network Appliance filers

This ARX deployment guide illustrates how the F5 ARX interoperates with Network Appliance (NetApp) filers. NetApp filers can be incorporated into ARX managed volumes as Tier-1 Filers. This guide explains the details for configuring a NetApp filer from its initial power up to the point that the NAS storage access is operational. The ARX configuration includes all the necessary steps in order to virtualize the NetApp CIFS Share.

In this configuration, the NetApp is configured for both NFS and CIFS. The NFS Export services the ARX as a metadata store. The CIFS Share are added to the managed volume.

◆ Note

*This is **NOT** a Multiprotocol deployment. The configuration will be a CIFS only namespace. ARX Training covers in depth the NetApp features and how the ARX may or may not support those other configurations.*

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:

- ◆ The F5 ARX must be configured for network access and the initial switch interview must be complete. If you have not performed these tasks, refer to the ARX Hardware Installation guide for specific details.
- ◆ NetApp filer must be physically installed and powered on.
- ◆ This document is based on ARX version 5.0.1 and NetApp ONTap 7.3.1
- ◆ This document is based on the fact that the Microsoft Active Directory Domain is preconfigured and the F5 Secure Agent is installed. You also need to create (or already have) a domain user that is assigned to the Backup Operator Group.
- ◆ The ARX platform is deployed in redundant pairs. The secondary switch is a Hot Standby switch. This guide will address the configuration steps in order to integrate the Network Appliance platform with the ARX platform. Redundant switch configuration steps within the product documentation should be followed in order to deploy a high available configuration.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
F5 Acopia ARX	5.0.1
Network Appliance ONTap Software	v7.3.1 or later

Document Version	Description
1.0	New guide

Configuration example

In the following diagram, we show basic connectivity between clients, ARX and NetApp tier-1 filers. The ARX uses the NetApp File NFS export and CIFS share into a managed volume. The managed volume is shared on the LAN as a CIFS share via the ARX Virtual Interface. The XP Client connects to the share by accessing the network resource `\\share.siterequest.com\share` and in turn the ARX proxies the access to the NetApp CIFS share `\share1`.

NetApp Tier-1 Filer Lab Network Topology

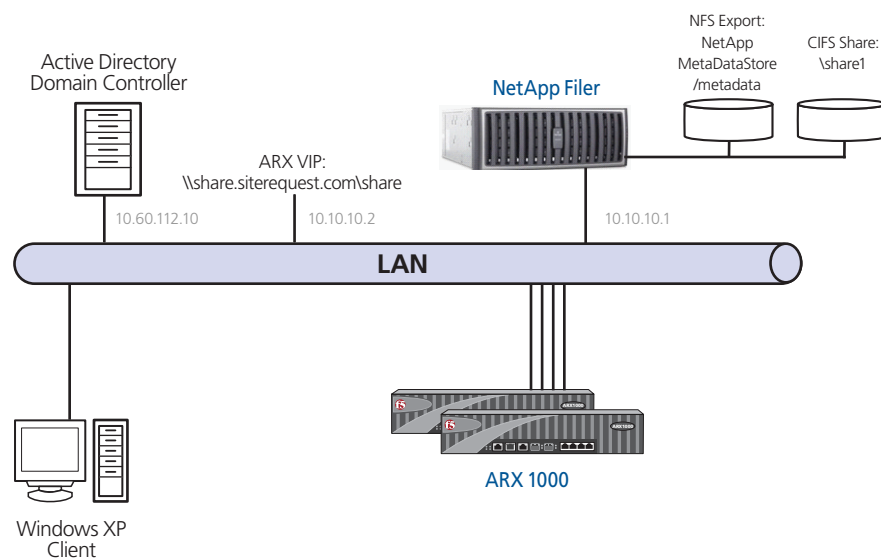


Figure 1 Logical configuration example

Configuring NetApp Filer

In this section we provide the minimum configuration steps required to install and deploy the NetApp filer as a tier-1 storage product. The Network Appliance filers have a broad set of configurable items. This section addresses the configuration steps needed for a basic configuration to support a CIFS file sharing deployment scenario.

The appliance also hosts the ARX metadata database on an NFS export. A NetApp CIFS share is configured as an ARX External Filer share and incorporated into a Managed Volume.

The following steps are covered in this section.

- *Initial NetApp configuration*, on page 3
- *Managing Licenses*, on page 6
- *Setting the Date and Time*, on page 6
- *Setting the Date and Time*, on page 6
- *Configuring DNS resolution*, on page 7
- *Reviewing the Disk Aggregate settings*, on page 8
- *Resizing the Volume*, on page 9
- *Creating Volumes*, on page 10
- *Configuring the NFS Export*, on page 12
- *Running the CIFS Setup Wizard*, on page 14
- *Creating the CIFS Share*, on page 17

Initial NetApp configuration

The NetApp filer ships with no configuration for network and disk partitioning. In this section we show how to perform the initial NetApp configuration. This configuration is performed on the NetApp Serial Console interface.

To perform the NetApp initial configuration

1. Log onto the NetApp via the serial interface. Using Putty and a serial cable connect to the appliance with **19,200 Baud, No Parity, 8 bit, and 1 stop bit**. Default username is **root** and **no password**.
2. Run the NetApp Setup wizard from the command line by typing **setup**.
3. When prompted to continue, type **yes**.
4. Type a new host name at the prompt. In our example, we type **NETAPPVM12**.
5. At the enable IPv6 prompt, type **n**.
6. At the configure virtual network interfaces prompt, type **y**.

7. Type the number of virtual interfaces to configure at the prompt. In our example, we type **1**.
8. Type a name for the virtual interface. In our example, we type **Storage1**.
9. Type **I** for lacp at the virtual interface type prompt.
10. Type **i** for IP-based load balancing at the prompt.
11. Type the number of links for the virtual interface. In our example, we type 2.
12. Type a name for each of the links when prompted. In our example, we name our two links **e0a** and **e0b**.
13. Type the IP address for the Network Interface. In our example, we type **10.10.10.1**.
14. Type the appropriate netmask. In our example, we type **255.0.0.0**.
15. Type the media type for the network interface. In our example, we type **auto**.
16. Type **n** when prompted to continue setup through the web interface.
17. Type the name or IP address of the IPv4 default gateway. In our example, we type **10.10.10.254**.
18. When prompted to type the IP address of the administration host, press return to allow /etc root access to all NFS clients.
19. Type the appropriate timezone. In our example, we type **US/Eastern**.
20. Type the location of the filer. In our example, we type **VMRack3**.
21. Type **n** when prompted to run DNS resolver.
22. Type **n** when prompted to run NIS client.
23. Type **n** when prompted to configure the BMC.
24. Type **reboot** for the changes to take effect.

See the example on the following page.

```

The setup command will rewrite the /etc/rc, /etc/exports,
/etc/hosts, /etc/hosts.equiv, /etc/dgateways, /etc/nsswitch.conf,
and /etc/resolv.conf files, saving the original contents of
these files in .bak files (e.g. /etc/exports.bak).
Are you sure you want to continue? [yes]YES
Please enter the new hostname []: NETAPPVM12
Do you want to enable IPv6? [n]: n
Do you want to configure virtual network interfaces? [y]: y
Number of virtual interfaces to configure? [1] 1
Name of virtual interface #1 []: Storage1
Is Storage1 a single [s], multi [m] or a lacp [l] virtual interface? [1] 1
Is Storage1 to support IP-based [i] or MAC-based [m] load balancing? [i] i
Number of links for Storage1? [2] 2
Name of link #1 for Storage1 []: e0b
Name of link #2 for Storage1 []: e0a
Please enter the IP address for Network Interface Storage1 [0.0.0.0]: 10.10.10.1
Please enter the netmask for Network Interface Storage1 [0.0.0.0]: 255.0.0.0
Please enter media type for Storage1 {100tx-fd, tp-fd, 100tx, tp, auto (10/100/1000)} []: auto
Would you like to continue setup through the web interface? [n]: n
Please enter the name or IP address of the IPv4 default gateway [0.0.0.0]: 10.10.10.254
    The administration host is given root access to the filer's
    /etc files for system administration. To allow /etc root access
    to all NFS clients enter RETURN below.
Please enter the name or IP address of the administration host: <Carriage Return>
Please enter timezone []: ? US/Eastern
Where is the filer located? []: VM Rack3
Do you want to run DNS resolver? [n]: N
Do you want to run NIS client? [n]: n
    The Baseboard Management Controller (BMC) provides remote management capabilities
    including console redirection, logging and power control.
    It also extends autosupport by sending down filer event alerts.

Would you like to configure the BMC [y]: n
Now type 'reboot' for changes to take effect.
reboot

```

Figure 2 NetApp CLI Setup Procedure

The CLI output shows how the NetApp was configured with a LACP group of two Gigabit Ethernet interfaces. A single IP address was assigned to the LACP group. The filer allows all hosts to manage it. The remaining configuration is performed using the Web management interface.

Managing Licenses

You must perform several other configuration details to NetApp, including NTP, DNS, Active Directory, and Feature licensing. In this procedure, we log on to the NetApp Web Interface, and enter the NFS and CIFS license keys. The features of the NetApp are enabled with license keys. The required keys for this configuration are NFS and CIFS license keys.

To log on to the NetApp Web Interface

1. Launch a Web Browser and go to the following address:
http://<ip address or FQDN of NetApp>/na_admin
2. Type the user name and password. The Data ONTAP landing page opens.
3. Click the **FilerView** icon. The System Status page opens with multiple panes. The left pane is a menu tree of features that can be configured. The right hand pane displays the attributes of the features.
4. From the left navigation, click to expand the **Filer** menu, and then click **Manage Licenses**.
5. In the CIFS and NFS boxes, type the appropriate license keys.
6. Click the **Apply** button at the bottom of the screen.

Setting the Date and Time

For this deployment, accurate and synchronized time is required. The filers, ARX, and clients need their clocks synchronized to within five minutes of each other. We configure the NetApp for the **Rdate** protocol and to receive system time from an external time server.

To set the date and time

1. From the **Filer** menu, click **Set Date/Time**. The Date/Time attributes open.
2. Click **Modify Date/Time**. The Date/Time wizard opens and the current timezone is displayed.
3. If necessary, change the time zone and then click **Next**.
4. On the System Time Update Method screen, click **Automatic**. We use automatic because time skew can occur. Click the **Next** button.

-
5. On the Time Daemon Options page, configure the following options (The time daemon is the process that runs on the NetApp and performs the time synchronization. The protocol needs to match the time server environment. In our example we will use rdate protocol for time synchronization):
 - a) In the **Maximum Skew** box, type a time interval. In our example, we type **5** and select **minutes** from the list.
 - b) From the Protocol list, select the appropriate protocol. In our example, we select **rdate**.
 - c) From the **Schedule** list, select how often you want the system to contact the time daemon server. In our example, we select **hourly**.
 - d) Click the **Next** button. The Time Daemon Servers page opens.

Date/Time Wizard- Time Daemon Options

Time Daemon Log Enable ?
Select the check box if you want changes initiated by the time daemon to be logged to the console.

Maximum Skew ?
Specify the maximum amount of difference allowed between the system's time and the time server's time. 5 minutes

Protocol ?
Select the protocol to synchronize time. rdate

Schedule ?
Indicate how frequently you want the system to contact the time daemon server. Hourly means once an hour, multihourly means every 6 hours, and daily means once a day. hourly

Figure 3 Time Daemon Options

6. In the **Servers** box, type the IP address or host name of the time server. You can optionally enter up to five time servers. Also optional is checking the **Validate** box to make sure the names resolve. Click the **Next** button.
7. On the Execute Rdate page, you can optionally check the **Execute** box to synchronize the time immediately. Click **Next**.
8. Review the summary and click the **Commit** button. The Set Date/Time status is displayed and should represent an accurate local time.

Configuring DNS resolution

The next task is to configure DNS name resolution on the NetApp filer.

To configure DNS name resolution

1. From the left navigation, click to expand **Network** and then click **Configure Host Name Resolution (DNS & NIS)**. The Host Name Resolution Policy Wizard opens. Click **Next**.
2. On the Enable Policies page, check the **Enabled** box to enable DNS, and then click the **Next** button.
3. In the DNS Domain Name box, type the Domain name. In our example, type **siterequest.com**. Configure the other DNS Domain Parameter options as applicable. In our example, we leave the rest of the values at the defaults. Click the **Next** button.

Host Name Resolution Policy Wizard - DNS Domain Parameters

DNS Domain Name
Enter the DNS Domain Name

DNS Dynamic Update Interval
Specify the validity period for the DNS entry related to the filer on the DNS Server. This specifies the time interval after which DNS entries are updated dynamically.

Dynamic DNS Updates Enabled

Select the check box if you want DNS entries to be updated dynamically after the update interval.

Use DNS Cache Enabled

Select the check box to use the DNS cache when looking up names. Clearing the check box will have the effect of flushing the DNS cache.

Figure 4 Configuring the DNS Domain Parameters

4. In the **DNS Servers** box, type the IP address of up to three DNS Servers in priority order.
5. In the Domain Search list box, type the appropriate domain(s) to search in priority order, and then click the **Next** button.
6. On the Name Service Configuration page, configure these settings as applicable for your implementation. In our example, we leave the settings at the default levels. Click the **Next** button.
7. Review the configuration changes and click the **Commit** button.

Reviewing the Disk Aggregate settings

An Aggregate is a NetApp term that represents a logical grouping of physical disks with a RAID profile defined. Depending on the NetApp configuration, multiple aggregates can be created and managed

independently. For simplicity, we use a single aggregate. For more complex configurations, consult the NetApp documentation or the F5 Data Solutions training and professional services.

The first Aggregate, **aggr0**, is created automatically.

To review the disk aggregate

1. In the left navigation, click to expand **Aggregate**, and then click **Manage**.
2. Click the aggregate **aggr0** to see the properties.
3. If changes are necessary for your configuration needs click **Modify** to change the aggregate settings.

The screenshot shows the 'Aggregate Properties' page for 'aggr0'. At the top, there is a breadcrumb 'Aggregates → Aggregate Properties' and a title 'Aggregate Properties' with a help icon. Below the title, there is a dropdown menu for 'Aggregate:' set to 'aggr0' and a 'View' button. A table displays the following properties:

Name:	aggr0	Root Aggregate?	✓
Type:	Aggregate	Raid Size:	14
Status:	online_raid_dp	Checksums:	block
Used Capacity:	41.9 GB	Number of Disks:	4
% Used:	6%	Double Parity?	✓
Total Capacity:	707 GB		
Number of Files:	107		
Max Files:	31.1 k		

Below the table, there are several buttons: 'Modify', 'Show Volumes', 'Show RAID', 'Add Disks', 'Rename', 'Mirror', and 'Refresh'.

Figure 5 Aggregate aggr0 properties

Resizing the Volume

By default, a pre-existing volume (**vol0**) is present on the NetApp filer. This is the root volume and contains the NetApp application code and cannot be removed. However it can be resized, and must be in this case.

To resize the volume

1. From the left navigation, click to expand **Volumes**, and then click **Manage**.
2. On the Manage Volumes screen, click **vol0**. The volume properties open.
3. Click the **Resize Storage** button. The Volume wizard opens.
4. On the Welcome page, click **Next**.

5. On the Flexible Volume Parameters page, from the Space Guarantee list, select **Volume**. This guarantees space for the entire volume within the disk aggregate. Click **Next**.
6. On the Flexible Volume Size page, set the following options:
 - a) In the **Volume Size Type** section, click the **Total Size** button.
 - b) In the **Volume Size** box, type **40** and make sure **GB** is selected.
 - c) In the **Snapshot Reserve** box, type **0**.
 - d) Click the **Next** button.

Volume Wizard - Flexible Volume Size

Volume Size Type:
Select **Total Size** to enter the total volume size (including snap reserve) and **Usable Size** to enter the usable volume size (excluding snap reserve).

Total Size [?]
 Usable Size

Volume Size:
Enter the desired volume size. The volume is using a total of 1.27 GB out of its current 40 GB total volume size. The containing aggregate, **aggr0** has a maximum of 665 GB space available. The new total volume size cannot exceed 705 GB with the Space Guarantee set to volume.

40 GB [?]
705 GB (Max)

Snapshot Reserve :
Enter the snapshot reserve for volume 'vol0'. The range is between 0% and 100%. The default is 20%.

0 % [?]

Figure 6 Setting the Flexible Volume Size options

7. Review the Volume setting changes and click **Commit**.

Creating Volumes

The next task is to create two new volumes. The first is a small volume to be associated to an NFS Export. This volume is the Metadata Store for the ARX. The second volume is for user content and is a CIFS share for the user's file content and incorporated into an ARX Managed Volume.

NetApp has 3 volume implementations. For our example we create a Flexible Volume (FlexVol). FlexVols are an advantage of NetApp storage. The FlexVol is not tied directly to the physical storage. Each FlexVol can be sized as appropriately fits within the aggregate. FlexVols span all disks (Except Hot Spare disks) within an aggregate this implementation provides a higher utilization of the raw disks than can be achieved with classic environments. FlexVols can be resized on-line while serving data.

To create a new volume

1. In the left navigation, click to expand **Volumes**, and then click **Add**. The Volume wizard opens.
2. On the Volume Type Selection page, click the **Flexible** button, and then click **Next**.

3. On the Volume Parameters page, configure the following options:
 - a) In the **Volume Name** box, type a name for this volume. In our example, we leave it as **vol1**.
 - b) From the Language list, select the appropriate language. In our example, we select **POSIX**.
 - c) Check the **UTF-8** box, if appropriate.
 - d) Click the **Next** button.

4. On the Flexible Volume Parameters page, configure the following options:
 - a) From the **Containing Aggregate** list, select the appropriate aggregate. Volumes are assigned to NetApp Aggregates to store the file contents.
 - b) From the **Space Guarantee** list, select **volume**.
 - c) Click the **Next** button.

5. On the Flexible Volume Size page, configure the following options:
 - a) In the **Volume Size Type** section, click the **Total Size** button.
 - b) In the **Volume Size** box, type **40** and make sure **GB** is selected.
 - c) In the **Snapshot Reserve** box, type **10**. This number can be higher or lower, but must not be 0.
 - d) Click the **Next** button.

Volume Wizard - Flexible Volume Size

Volume Size Type:
 Select **Total Size** to enter the total volume size (including snap reserve) and **Usable Size** to enter the usable volume size (excluding snap reserve).

Total Size ?
 Usable Size

Volume Size:
 Enter the desired volume size. The volume is using a total of 104 KB out of its current 40 MB total volume size. The containing aggregate, **aggr0** has a maximum of 463 GB space available. The new total volume size cannot exceed 464 GB with the Space Guarantee set to volume.

40 GB ?
 464 GB (Max)

Snapshot Reserve :
 Enter the snapshot reserve for volume 'vol1'. The range is between 0% and 100%. The default is 20%.

10 % ?

Figure 7 Flexible Volume Size

6. Review the volume parameters and then click **Commit**.

Changing the volume security style

By default, the volume you just created uses NTFS security style. Because this volume is designated for an NFS Export to serve as the ARX Metadata Store the security style needs to be changed to Unix.

To change the volume security

1. From the left navigation, expand **Volumes**, and then expand **Qtree**. Click **Manage** under Qtree.
2. Click the volume you just created. In our example, we click **vol1**. The Modify Qtree page opens.
3. From the **Security Style** list, select **Unix**.
4. Click the **Apply** button.

Important

*Do not select the security style **Mixed**. The ARX does not support a Mixed Mode security style.*

Creating the second volume

The second volume to be created is used as a file content volume and incorporated into an ARX managed volume. The configuration for this volume is largely the same as the previous volume.

To configure this volume, follow the procedure *To create a new volume*, on page 10 with the following exceptions:

- In Step 3a, give this volume a unique name. We use **vol2**.
- In Step 5b, type 200 and select GB for the Volume Size. This volume is created for the CIFS Share that the ARX will incorporate into a Managed Volume.
- In Step 5c, type 20 for the Snapshot Reserve.

Configuring the NFS Export

In this section, we configure the NFS Export to be used by the ARX as the Metadata store. This export is referenced in the ARX Configuration section later in this guide. The ARX needs to have root access to the NFS share. Normally NFS Exports will restrict access. The **NO_ROOT_SQUASH** feature of NFS must be defined in order to fulfill this requirement. When the volume was created a default NFS export was also created, we modify that export in this procedure.

To configure the NFS Export

1. From the left navigation, click to expand **NFS**, and then click **Manage Exports**.

2. From the list, click the /vol/<name of first volume you created> to edit the export. In our example, we click **/vol/vol1**. The NFS Export wizard opens.
3. Check the **Actual Path**, **Anonymous User ID**, **Read-Write Access**, **Root Access**, and **Security** boxes. Click **Next**. The Export Path page opens.



Figure 8 NFS Export Options

4. In the **Export Path** box, type **/metadata**. This is the name the NFS Client references for mounting. The ARX mounts this path to be used as the MetaData Store. Click **Next**. The Actual Path page opens.
5. Type the actual path to the volume. In our example, we type **/vol/vol1**. Click **Next**. The Anonymous User ID page opens.
6. In the Anonymous User Id box, type **0** and then click **Next**. The Read-Write Access page opens.
7. On the Read-Write Access page, check the **All Hosts** box. NFS protocol can restrict Read-Write access by hostname. Only hosts entered into the list are granted Read-Write access. In our example we want all hosts to have Read-Write access. Click **Next**. The Root Access page opens.
8. On the Root Hosts page, click the **Add** button. A host box opens. In the **Hosts to Add** box, type the keyword **NO_ROOT_SQUASH**, and then click **OK**. Root access is a restricted access right. The keyword **NO_ROOT_SQUASH** is used to allow Root users to mount the NFS export.
9. Click the **Next** button.



Figure 9 No Root Squash Root Access

10. In the **Security** list, leave Security as **Unix Style**. Click **Next**.
11. Review the configuration changes and then click **Commit**.
12. Click **Close** to return to the Manage NFS Exports page.
13. Click the **Refresh** button to update the page. The new export **/metadata** displays.
14. Click the **Export All** link to apply the changes. This is a way to validate the NFS Export configuration. If an error exists it is reported when you click this link. Because there are two entries for **/vol/vol1** a duplicate entry error is displayed.
15. To resolve this error, click the volume (in our example **/vol/vol1**) and click the **Delete** button. A confirmation warning is displayed. Click **Ok**, and then click the **Export All** link again. No error should be displayed.

The NFS Export **/metadata** is now ready for use.

Running the CIFS Setup Wizard

The NetApp has a CIFS Setup wizard to assist with joining the Windows Active Directory Domain.

To run the CIFS Setup Wizard

1. From the left navigation, click to expand **Wizards**, and then click **CIFS Setup Wizard**. The Setup Wizard opens.
2. On the Welcome page, click **Next**.

-
3. On the Filer Name page, configure the following options:
 - a) In the **Filer Name** box, type a name for this filer. In our example, we type **netapp**.
 - b) In the **Description** box, type a description of the filer.
 - c) In the **WINS Servers** box, type the IP addresses of up to four WINS servers that clients may use.
 - d) Click **Next**.

CIFS Setup Wizard - Filer Name

Filer Name:
Enter the name of the filer as known to CIFS. ?

Description:
Enter a description of the filer, which appears in Server Manager and network properties. ?

WINS Servers:
Enter up to four WINS servers that your clients might use. ?

Figure 10 Filer Name and description

4. On the Authentication page, select the appropriate authentication. Authentication can be workgroup or domain authentication. In our example we are joining a Windows 2000 domain, so we select **Windows 2000**. Click **Next**.
5. On the Domain page, configure the following options:
 - a) In the **Domain name** box, type a domain name. In our example, we type **siterequest.com**.
 - b) In the **Windows 2000 Administrator Name** box, type the administrator name. In our example, we type **administrator**.
 - c) In the **Windows 2000 Administrator Password** box, type the administrator password.
 - d) Click **Next**.
6. On the Security Style page, click the **NTFS Only** button, and then click **Next**.
7. Review the summary and then click **Commit**.

The CIFS Services are restarted and the NetApp attempts to join the domain. If it is successful, you see a Success page. If it fails, check the administrative credentials, domain name, DNS resolution, and WINS server values.

Testing the Domain Controller

The Domain Controller can be tested directly from the NetApp filer. To test the domain controller, complete the following procedure.

To test the domain controller

1. From the left navigation, click to expand CIFS, and then click **Test Domain Controller**.

The NetApp initiates a request to the Domain Controller and reports status on each controller found.

CIFS Test Domain Controller ?

CIFS → Test Domain Controller

```
Using Established configuration
Current Mode of NBT is H Mode

Netbios scope ""
Registered names...
      NETAPP      < 0> WINS
      NETAPP      < 3> WINS
      NETAPP      <20> WINS
      ACME        < 0> WINS

Testing all Primary Domain Controllers
found 3 unique addresses

found PDC ACMEADS01 at 10.60.112.10
found PDC VM-DCACME2K8-01 at 10.63.132.14
found PDC ACMEADS02 at 10.60.112.11

Testing all Domain Controllers
found 3 unique addresses

found DC ACMEADS01 at 10.60.112.10
found DC VM-DCACME2K8-01 at 10.63.132.14
found DC ACMEADS02 at 10.60.112.11
```

Figure 11 CIFS Domain Controller test

Looking up a user name and Security ID from the Domain Controller

The NetApp can also lookup a Username and Security ID from the Domain Controller. This is useful to test the Proxy User and to verify it exists within the domain.

To look up a user name and SID

1. From the left navigation, click to expand CIFS, and then click **Look Up Name/SID**.
2. In the **Name or SID** box, type the domain user that is assigned to the backup operator. In our example, we type **acmeuser001** and then click **Lookup**. The user's SID is returned. If it does not return a SID, verify the user is created in the active directory domain and is spelled correctly.

Name/SID Look Up ?

CIFS → Look Up Name/SID

i **Success**

SID = S-1-5-21-2826071149-1489806083-1568395554-1108

Name or SID: ?

Enter a Windows user or group name, or a Security ID (SID).

Figure 12 Looking up a Name/SID

Creating the CIFS Share

In this section we create a CIFS file share to be used by the ARX as the Tier-1 file space. This share is referenced in the ARX Configuration section later in this guide.

To create the CIFS share

1. From the left navigation, click to Expand **CIFS**, click **Shares**, and then click **Add**. The Add a CIFS Share page opens.
2. In the **Share Name** box, type a name for this share. In our example, we type **share1**.
3. In the **Mount Point** box, type the volume mount point for this share. In our example, we type **/vol/vol2**.
4. In the Share Description box, you can optionally type a description.
5. In the **Max. Users** box, you can optionally type the maximum number of simultaneous users. In our example, we leave this blank.
6. In the **Force Group** box, you can optionally type a UNIX group that will be automatically assigned to the files in this share. In our example, we leave this blank.
7. Click the **Add** button (see Figure 13).
If the share is valid, it is created and the status is displays, and the new share appears in the share list. The share is now ready for use.

Add a CIFS Share ?

CIFS → Shares → Add

Share Name: ?
Enter the share name.

Mount Point: ?
Enter the volume mount point for this share, for example, /vol/vol0 /home.

Share Description: ?
Enter the description (double quotes will be stripped out).

Max. Users: ?
Enter the maximum number of simultaneous connections allowed. If left blank, the maximum is limited only by the amount of filer memory.

Force Group: ?
Enter the UNIX group that will be automatically assigned to files in this share.

Figure 13 Add a CIFS Share

You can test this filer share for compatibility using the ARX command line. From the ARX command line, type the **show exports** command to enumerate the filers file systems shares. In our example we type the following command:

```
show exports external-filer NetApp proxy-user acmeuser001
```

The following page shows the output in our example.

```
arx500-1# show exports external-filer NetApp proxy-user acmeuser001
Export probe of filer "NetApp" at 10.10.10.1
Connectivity:

Slot.Proc Proxy Address Ping (size: result)
-----
1,2      10.10.10.10    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 disabled
  Extended Security Kerberos, NTLMSSP
  Server             TCP/445, TCP/139
  Max Request        33028 bytes
  IPC$ Share         Access OK
  Auth Method Used   Kerberos
  SPN Used           netapp$@SITEREQUEST.COM
  Discovered SPN    netapp$@SITEREQUEST.COM

Shares:

CIFS
  Share                               Storage Space
  Total (MB) Free (MB) Serial Num
-----
HOME                                40960    39653    0001-ba13
share1                              163840   163832   0201-45b0

Time:

CIFS
Filer's time is the same as the switch's time.
```

The share **/share1** exists, the ARX proxy user has access, and the filer time matches the ARX time. The share can be probed to see if it is supportable. Issue the ARX **probe exports** command to verify proper access is granted by the filer. In our example, we type:

```
probe exports external-filer NetApp proxy-user acmeuser001
```

```
arx500-1# probe exports external-filer NetApp proxy-user acmeuser001
Export probe of filer "NetApp" at 10.10.10.10

CIFS Credentials:
  User           acmeuser001
  Windows Domain siterequest.com
  Pre-Win2k      ACME

Security:

CIFS

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

Share           Write  Privs
-----
HOME            OK    OK
share1          OK    OK
```

Figure 14 ARX probe exports command output

The Write and Privs columns report **OK** for the **share1** share. This validates the proxy user is properly authenticated to manage the share contents. The NetApp configuration is complete. The CIFS Share may now be configured into an ARX managed volume.

Configuring the ARX

This section we configure the ARX to access the external storage devices. We create a CIFS namespace with a single share added to it. The share is incorporated into a managed volume.

This section contains the following procedures:

- *Configuring Active Directory Authentication*, on page 21
- *Verify Active Directory Authentication*, on page 23
- *Creating the CIFS Namespace*, on page 24
- *Creating a Managed Volume*, on page 24
- *Adding root level share*, on page 28
- *Creating Snapshot Support*, on page 29
- *Create the Virtual Service*, on page 33
- *Accessing the CIFS Virtual Service from an XP Client*, on page 36
- *Accessing Snapshots through the Virtual Service*, on page 36
- *Generating an ARX Metadata Report*, on page 38

The main Web GUI Page is the Common Operations page. Much of the following steps will start from this page.

Configuring Active Directory Authentication

The first task in configuring the ARX is to configure Active Directory authentication.

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.
7. Click the **Ok** button.

Add NTLM Authentication Server

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

OK Cancel

Figure 15 Create a new Authentication Server

Creating the Proxy users

The next task is to create proxy users. This is the Active Directory user that was assigned as the Backup Operator. This user is used to access the backend filer CIFS shares.

To create the proxy user

1. On the ARX user interface, 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 **acmeuser**.
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** in both boxes.
6. Click the **Save** button. You return to the CIFS authentication page.

The ARX can support the snapshot feature on the NetApp filers. This feature requires the ARX is capable of logging into the NetApp command line interface to perform snapshot maintenance. The next step is to create a second proxy user that has the login credentials for the NetApp. In our example the NetApp allows a username of **root** to access the command line of the NetApp. This user reference will be used when the NetApp filer is added to the ARX configuration.

Repeat the preceding procedure, creating a CIFS user that has the login credentials for the NetApp device.

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.

Verify Active Directory Authentication

In this section, we verify that the ARX is properly joined to the Active Directory domain.

Log into the ARX via SSH to access the command line interface. Enter the **show active-directory status** command.

```
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**.

Creating the CIFS Namespace

The next task is to create a CIFS namespace on the ARX.

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 **Content**. 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, type the name of the proxy user. In our example, we type **acmeuser001**. Click the **Next** button.
7. Click the **Finished** button.

Figure 17 CIFS Authentication settings

Creating a Managed 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 this example, we place

the Volume Metadata onto the NFS Export on the NetApp Filer. ARX best practices state Metadata should be created on an NFS export if one is available. Alternatively, a CIFS share could be used.

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 namespace you created. In our example, we select **Content**.
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 **NFSv3-UDP**.
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 **netapp**.
 - 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) Make sure there is a check in the **This file server supports snapshots** box.
 - f) From the **File Server Type** list, select **NetApp**.

In order to allow the ARX access to these filers (EMC, NetApp, Windows) management access is required.

- g) In the **Management IP Address** box, type the management IP address.
 - h) From the **Management Protocol** list, select the appropriate protocol. In our example, we select **SSH**.
 - i) In the **Management Proxy User** box, type the proxy user. In our example, we type **root**.
 - j) In the **Ignore Directories (optional)** box, type any Network Appliance snapshot directories the ARX should ignore, and click the **Add** button. In our example, we type **.snapshot, ~snapshot**. See Figure 18.
 - k) Click the **Save** button. You return to the managed volume wizard.
- For more information refer to the ARX CLI Storage guide,

Chapter 6 section *Preparing the Filer for ARX-Snapshot Support*

<https://<arx IP address>/acopia/docs/cliStorage/cliStorage.pdf>).

To configure a new file server, enter its name and primary IP address. Optionally add a secondary IP address for a multi-homed file server. Optionally enter any directories or files to (always) ignore when importing data from this file server (e.g. '.snapshot').

Name: netapp
 Primary IP address: 10.10.10.1
 Secondary IP Address:
 CIFS Port: 445
 Supports Snapshots: This file server supports snapshots.
 File Server Type: NetApp
 Management IP Address: 10.10.10.1
 Management Protocol: SSH
 Management Proxy User: root
 Kerberos Service Principle Name (optional):
 Description (optional):
 Ignore names (optional): .snapshot, ~snapshot

Common examples:
 EMC: .etc, lost+found, .ckpt*
 Network Appliance: .snapshot, ~snapshot

Buttons: Remove, Add, Back, Save, Cancel

Figure 18 Configuring a new file server

7. In the Metadata CIFS share/ NFS path box, type the path. In our example, we type **/metadata**.

A managed volume requires metadata that should be located on a highly available file server (i.e. clustered). Select the file server and enter the file server path where the metadata will be stored.

Metadata file server protocol: NFSv3-UDP
 Metadata file server: netapp
 Metadata CIFS share / NFS path: /metadata

NFS e.g. /vol/vol1/meta1
 CIFS e.g. metadata1

Buttons: Add..., Edit...

Figure 19 Define the Metadata datastore location

8. Click the **Next** button. The CIFS parameter option page opens.

9. Check the box in the **Auto-synchronization** section, and then check the **Auto detect CIFS Attributes** box. Click **Next**. The Volume parameters page opens.
10. Click the **Files and directories can be renamed during import and re-import** button.
11. Check the **Enable the volume when finished** box, and then click **Next**.
12. Review the summary, and then click **Finish**.

Modifying the Volume Snapshot attributes

The next task is to change the default settings for the Volume Snapshot attributes. We modify the settings to present the snapshot contents in a hidden directory named **~snapshot** as apart of the Virtual Service CIFS Share.

To create the modify the volume snapshot

1. From the navigation pane, click **Managed Volumes**, and then click the name of the volume you just created. The volume details page opens.
2. Click the **Edit** button.
3. In the Snapshot Directory Name box, type **~snapshot**.
4. From the **Snapshot Directory Display** list, select **All Exports**, and then check the **Mark snapshot directory as hidden** box.
5. Click the **OK** button.

Edit Managed Volume	
Enable Volume	<input checked="" type="checkbox"/> Enable Volume
Volume Name	/data
Volume Description	<input type="text"/>
Metadata File Server	netapp <input type="text"/>
Metadata Protocol	NFSv3-UDP <input type="text"/>
Metadata Path	/metadata <input type="text"/>
Shadow Volume	<input type="checkbox"/> Shadow Volume
Snapshot Directory Name	~snapshot <input type="text"/>
Snapshot Directory Display	All Exports <input type="text"/> <input checked="" type="checkbox"/> Mark snapshot directory as hidden.
Privileged Snapshot Access	<input type="checkbox"/> Allow access to snapshots by privileged users only.
Snapshot Consistency	<input type="checkbox"/> Make snapshots consistent.
Snapshot Timeout	50 seconds <input type="text"/>
VSS Mode	Windows XP <input type="text"/>

Figure 20 Edit Volume dialog

Adding root level share

The first file share added to the ARX managed volume is the root level share. This is the CIFS Share created on the NetApp Filer. When more shares are added they will 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 Storage**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 24. In our example, we select **Content**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Managed Volume*, on page 24. In our example, we select **/data**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in step 6a of *Creating a Managed Volume*, on page 24. In our example, we select **netapp**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share1**.
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 (see Figure 21).
9. Click the **Next** button.
10. Review the summary, and click the **Finish** button.

Figure 21 Add Share Wizard

Creating 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. While we have already configured the volume parameters for the ARX to support NetApp snapshots, you need to create a snapshot policy and schedule.

To create a snapshot policy

1. From the left navigation pane, click to expand **Policy**, and then click **Snapshots**.
2. Click the **Add** button. The Snapshot wizard opens.
3. In the **Policy Name** box, type a name for the policy. In our example, we type **Snapshot_Support**.
4. From the **Namespace** list, make sure the namespace you created in *Creating the CIFS Namespace*, on page 24 is selected. If it is not, select it from the list.
5. From the **Volume** list, make sure the volume you created in *Creating a Managed Volume*, on page 24 is selected. If it is not, select it from the list.
6. Click **Next**.

7. In the Options section, click the **Add** button to add a Schedule, and complete the following:
 - a) In the Schedule Name box, type a name for the schedule. In our example, we type SnapShot_Schedule.
 - b) In the **Start Time** box, type a start time or leave the default (the current time and date).
 - c) In the Interval section, specify an interval. In our example, we type **30** in the **Every** box and select **minutes** from the list to schedule a snapshot to occur every 30 minutes.
 - d) Click the **Save** button to return to the Snapshot wizard.

Figure 22 Policy Schedule

8. In Retention Count box, type a number of previous snapshots the ARX device maintains. Older snapshots are deleted by the ARX for maintenance purposes. You can check the **Generate reports** box to generate reports.
In our example, we maintain **5** snapshots total, and generate a report each time a snapshot is performed.

◆ **Note**

The frequency and retention depth for snapshots is deployment specific. Tune these parameters to fit the customer retention policy.

9. Click the **Next** button.
10. Review the Summary and then click **Finish**.

The snapshot policy can be manually invoked. This is a good way to test the snapshot configuration. Select the policy you just created and click the **Snap** button.

You can also define a custom report name *<name?>*. After testing the snapshot configuration, return to the snapshot summary screen. To review the report, from the left navigation, click **Reports**. A list of reports will be listed in reverse chronological order. Click the report to review it.

A new browser tab opens and the report is displayed. The following example is the report we just created.

Snapshot Summary

Namespace Name:	Content
Volume Name:	/data
Snapshot Rule Name:	SnapShot_Support

Snapshot Properties

Snapshots Enabled:	Yes
Snapshot Timeout Selector:	50 seconds
Guarantee Consistency:	Disabled
Retain Count:	5
Schedule:	SnapShot_Schedule
Directory Name:	~snapshot
Directory Display:	All Exports
Hidden File Attribute:	Set
Restricted Access Configured:	No
VSS Mode:	Windows XP
Contents:	
Metadata:	No
Volume Configuration:	No
User Snapshots:	Yes
Archive:	
Total Archive Operations:	0
Total Successful Operations:	0
Total Failed Operations:	0
Total Saved Metadata:	0
Total Saved Volume Config:	0
Average Copy Rate:	0 b/s

Snapshot Summary - SnapShot_Support_0

Snapshot Name:	SnapShot_Support_0
Snapshot Operation:	Create
Result:	Success
Time Requested:	Fri Oct 23 14:14:24 2009
Time Created:	Fri Oct 23 14:14:24 2009
Last Time Verified:	
Request:	Create
Snapshot State:	Complete

```

Snapshot Origin:          Manual
Report Name:              SnapShot_Support_0_create_20091023141424626.rpt

Included Shares
-----
Share Name:              share1 (user data)
Filer:
  Name:                  netapp
  CIFS Share:            share1
  Volume:                vol2
Filer Snapshot:
acopia_38_200910231414_10259b50-5c86-11dc-978c-b9d1a5320bdc_vol2

```

Figure 23 Snapshot Report

Take notice of the *Snapshot Name* field, this is the ARX reference to the snapshot. Subsequent snapshots are named *SnapShot_Support_1*, *SnapShot_Support_2*, and so on. The ARX appends the instance to the end of the Snapshot Policy Name. Also review the last report field *Filer Snapshot*. This is the actual name the ARX used when it invoked the snapshot on the NetApp filer.

The NetApp command line has a **snap list** command that can be used to display the snapshots that have been taken and currently maintained. The NetApp CIFS share that the ARX is managing is the NetApp Volume named *vol2*. SSH into the NetApp console and type the following command: **snap list vol2**.

The NetApp lists all the snapshots. The following is an example.

◆ **Note**

The Snapshot name matches the name in the ARX report.

```

NETAPPVM12> snap list vol2
Volume vol2
working...

  %/used    %/total    date          name
-----
5% ( 3%)   0% ( 0%)   Oct 23 10:14  acopia_38_200910231414_10259b50-5c86-11dc-978c-b9d1a5320bdc_vol2

```

Figure 24 NetApp Snapshot listing

To exit the NetApp CLI press CTRL-D (^d). In the section *Accessing Snapshots through the Virtual Service*, on page 36 we demonstrate how the client can access the snapshot file contents.

Create the Virtual Service

The Virtual Service is how the ARX presents CIFS Shares to the network clients. The client will send file requests through the Virtual Service and the ARX will proxy these requests to the appropriate backend filer. The Virtual Service requires a Namespace, FQDN, IP address, IP Mask, VLAN ID, ARX Volume, and an Export name.

The XP Client will connect to the Virtual service FQDN and map the share to an unused drive letter.

To create the virtual service

1. From the navigation pane, click **Virtual Services**.
2. Click the **Add** button. The Add Virtual Service Wizard opens.
3. From the **Namespace** list, select the namespace you created in *Creating the CIFS Namespace*, on page 24. In our example, we select **Content**.
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 **share.siterequest.com**.
 - b) In the **IP Address** box, type the IP address of the VIP. In our example, we type **10.10.10.2**.
 - c) In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.0.0.0**.
 - d) From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **1** (see Figure 25).
5. Ensure the **Enable the virtual service when finished** box is checked.
6. Click the **Next** button.
7. From the **Windows Domain Name** box, select the Windows domain name. In our example, we select **siterequest.com**.
8. In the **Pre Win2k Domain** box, type the Pre Win2k Windows domain name. In our example, we type **siterequest**.
9. 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.
10. Click the **Next** button. The Virtual Service Exports screen opens.

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:

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

Virtual Service Name & IP Address:

Create a new virtual service

Virtual service DNS name:

IP Address:

Subnet Mask:

VLAN ID:

[Enable Virtual Service](#)

Enable the virtual service when finished

Figure 25 Virtual Service creation

11. In the New Export section, from the **Volume** list, select the Volume you created in *Creating a Managed Volume*, on page 24. In our example, we select **/data**.
12. In the **Volume Path** box, type the Volume Path. In our example, we type **/**.
13. In the **Export Name** box, type a name for the Export. In our example, we type **share**.
14. Configure the other options as applicable for your configuration, and then click the **Add Export** button.
15. Click the **Next** button.
16. Review the summary and then click **Finish**.

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**.

Review the Virtual Service by clicking Virtual Services from the left pane. Notice 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"/>	share.siterequest.com	10.10.10.2 255.0.0.0	1	<u>1</u>	Joined	CIFS: Enabled	CIFS: Ready

Figure 26 Virtual Service Summary

Accessing the CIFS Virtual Service from an XP Client

In this section, the Virtual Service CIFS Share is mapped to a drive letter on the XP Client. The client authenticates and has read/write access to the managed volume. To verify read/write access, file data is copied to the share location.

To map the CIFS share to a drive letter

1. Logon to the Windows XP Client as a domain user.
2. Open Windows Explorer, and then from the **Tools** menu, select **Map Network Drive**. The Map Network Drive wizard opens.
3. From the **Drive** list, select a letter. We use **Z** in our example.
4. In the Folder box, type the ARX Virtual Service CIFS Share. In our example, we type `\\share.siterequest.com\share`.
5. Click the **Finish** button.

The network resource is mapped as the drive letter on the XP Client. To test user access: create a folder and copy test data files into the folder. This content is useful in the next sections for accessing snapshot files and for the Metadata report generation.

Accessing Snapshots through the Virtual Service

The NetApp filers support snapshots. Snapshots are point in time copies of the file system. Snapshots get triggered on a timely basis within the NetApp filer. These copies assist users in self restoring backup copies of their data. The ARX supports this feature and can present the snapshots to the user via the virtual service in a user friendly manor through the Windows Previous Versions feature.

Microsoft's Previous Versions feature is an intuitive interface designed for the vast majority of CIFS clients. It simplifies the file restore process by binding a list of previous file versions to the file properties option. Where as the ~snapshot directory is designed for well-informed CIFS administrators.

Recall in section *Creating Snapshot Support*, on page 29 the ARX was configured to perform a snapshot every half hour and retain 5 copies.

◆ Note

The files need to change in order to show up with Previous Version History. Microsoft Explorer filters the same versions and does not present them in the list of previous versions.

For this example, we made a top level **\Test** directory, and added a couple files to it. These files are used to demonstrate how a user can self restore previous versions of their own files.

First, we navigate into the **Z:\Test** directory. There are two files that exist in this directory. We have edited these files over a long enough period of time that the versions of files span multiple snapshot copies (that were created from our previously defined schedule). To review the list of previous files, we right-click a file and click **Properties**, and then click the **Previous Versions** tab. In our example, two previous versions exist for this test file. The user has the option to View, Copy, or Restore the file.

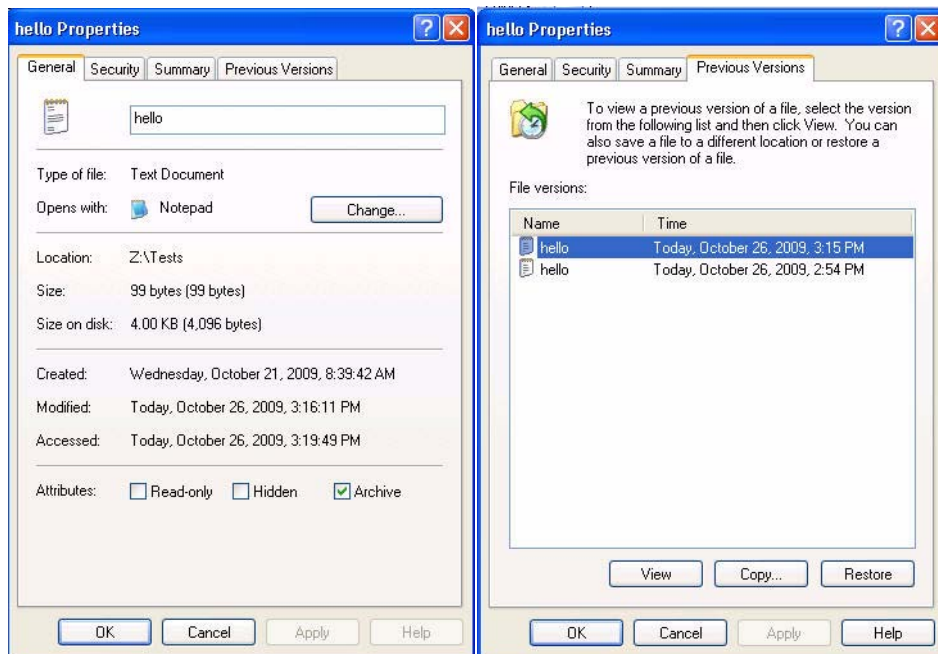


Figure 27 File Properties

Network Appliance snapshots

A snapshot is a point in time copy of the file system. Snapshots are taken instantaneously and do not impact system performance. Snapshots can be browsed in a directory which is similar to the original. A snapshot directory is a read-only image of the file system encapsulated in time to when it was taken. Majority of file restore requests are for individual files. NetApp snapshots are simple and end user friendly. End users can self restore their own files. This alleviates the reliance on the IT staff to perform the file restores.

Using the XP Client, make sure that the Windows option **Show Hidden files** is enabled, and navigate to the root level directory on the Z drive. You see the hidden **~snapshot** directory is visible. In typical deployments this

directory is not presented. For demonstration purposes, in section *Creating a Managed Volume*, on page 24 we modified the volume to expose the hidden directory.

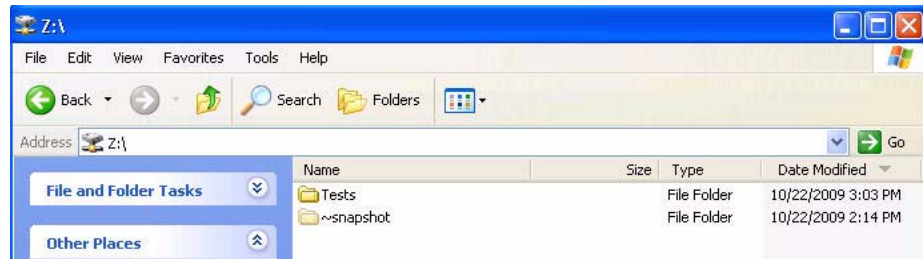


Figure 28 Top Level share directory

Within the ~snapshot directory are the five retained snapshot copies. The directory names reflect the ARX Snapshot Policy Name. These directories are normally hidden and not presented.

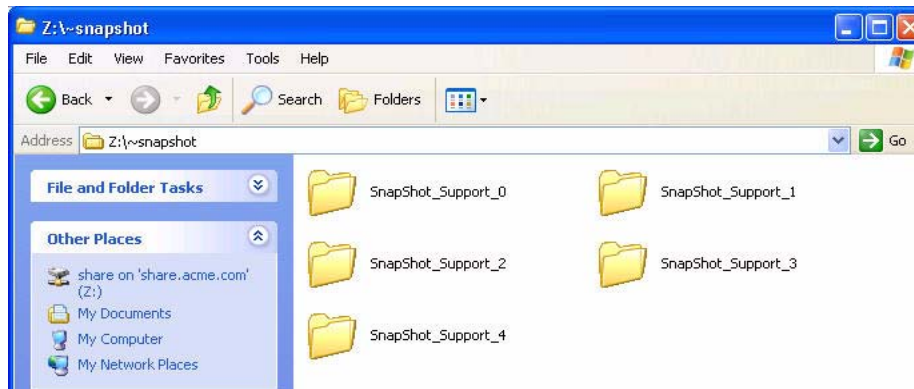


Figure 29 Top Level share directory

Generating 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 section, we demonstrate how to create an ARX Report.

To create an ARX Report

1. From the left navigation pane, click **Managed Volumes**.
2. Click one of the available Managed Volumes. In our example, we click **/data**.

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 **metadata_report**.
7. All other settings are optional.
8. Click the **OK** button. The report is generated.
9. To view the report, from the left navigation pane, click **Reports**.
From the **Report** list, select the name of the report you just created.
In our example, we click **metadata_report**. The Report opens in a new browser window or tab.

Report Volume

This operation generates a report about the metadata associated with this volume.

Namespace	Content
Volume	/data
Path	/
Report Type	<input type="radio"/> Inconsistencies <input checked="" type="radio"/> Metadata
Output Report Name	metadata_report
Recurse Subdirectories	<input checked="" type="checkbox"/> Recurse Subdirectories
Share	All
Include File Handles	<input checked="" type="checkbox"/> Include File Handles

Figure 30 Volume Report

Conclusion

This deployment guide demonstrated an effective way to integrate the F5 ARX platform with Network Appliance filers for a Tier-1 filer deployment. The deployment enables the ARX to virtualize the NetApp share within a Managed Volume. This allows the Namespace to grow over time without interrupting access to the file contents.

There are several other deployment guides written for ARX solutions. These include using Tier-2 class NAS filers for information lifecycle management. In those guides the prerequisite for an incumbent legacy storage platform is already available to the network is stated. The NetApp filer in this guide is the incumbent storage device.

For more information on configuring the F5 ARX, refer to the documentation, available on the ARX switch or Ask F5 (<https://support.f5.com/kb/en-us/products/arx.html?product=arx>).