



Deploying the F5 ARX with the NetApp StorageGRID Gateway

Table of Contents

Deploying the F5 ARX with the NetApp StorageGRID Gateway

Prerequisites and configuration notes	1
Product versions and revision history	3
Theory of operation	3
Configuration example	4
Installing the NetApp StorageGRID Gateway hardware	5
Initial Configuration of the NetApp StorageGRID Gateways	5
Configuring the ARX	7
Creating the CIFS Namespace	7
Creating a Volume	9
Adding the External Filers	11
Adding the root level share	12
Adding the Tier 2 CIFS Shares	13
Adding the NetApp StorageGRID Gateway Share	14
Creating the File Placement Policies	15
Creating a fileset migration policy	18
Creating the Virtual Service	21
Verifying the Storage Integration	23
Mounting the Virtual Server CIFS share	23
Generating an ARX Metadata Report	23
Conclusion	25

Deploying the F5 ARX with the NetApp StorageGRID Gateway

Welcome to the F5 - NetApp deployment guide. This guide provides step by step procedures on deploying the Adaptive Resource Switch (ARX) with the NetApp StorageGRID Gateway.

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

The NetApp StorageGRID - Gateway hardware is deployed onsite by NetApp's engineers. F5, NetApp and the customer must work in tandem in order to deploy the solution.

NetApp StorageGRID helps deliver boundless scalability, intelligent data management, and secure content retention, as well as always-on global data availability for enterprises and service providers that need to manage petabyte-scale globally distributed repositories of data.

NetApp StorageGRID is a tiering to the cloud solution. The ARX tiers files onto the StorageGRID by policy. Once the files are present on the gateway they are replicated to the NetApp cloud storage data centers.

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

For more information on NetApp StorageGRID, see <http://www.netapp.com/us/products/storage-software/storagegrid/>
<http://media.netapp.com/documents/ds-3038.pdf>

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this deployment:

- ◆ This deployment guide assumes a Microsoft Active Directory (AD) environment is properly configured and the Secure Agent Software installed. This agent has a password which will be needed during NTLM Authentication Server configuration. The AD must have an ARX proxy user defined that is assigned Backup Operator Privileges. This guides uses the AD User name **arx_proxy_user** in the **siterequest.com** AD domain.
- ◆ This deployment guide assumes an NFS Export is available on the network to act as the ARX Metadata Server. This external filer will be referenced in this guide as **MetaDataServer**. The export name is **/Metadata**.
- ◆ The ARX must be deployed in a High Availability pair. The HA configuration details are well documented in the ARX Configuration Manual. Refer to **The CLI Network Management Guide** and the

section *Adding a Redundant Switch* for more details. ARX Documentation is installed on the ARX switch and accessible within the Web User Interface.

- ◆ DOS file attribute bits for System and Hidden files are not preserved on files residing within the NetApp StorageGRID.
- ◆ When files are migrated to the NetApp CIFS share the File Access time becomes the time the file was migrated to the NetApp StorageGRID gateway.

The following features of the ARX are not supported:

- *Filer Subshares*
A managed volume that supports CIFS can optionally support subshares and their share-level ACLs. A subshare is a CIFS share below the root of the volume. Through a volume that supports subshares, a properly-configured cifs service can pass its clients from a front-end subshare to the corresponding back-end subshare. The back-end filer can then apply the subshare's ACL to the client's actions. The NetApp StorageGRID storage solution does not support this capability.
- *Access Based Enumeration*
A file server CIFS share with ABE 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.
- *Named Streams*
A named stream (or Alternate Data Stream) is a hidden file with meta-information about the main file, such as a summary description or a thumb-nail graphic. If any back-end-CIFS filer does not support named streams, you must disable the feature for its namespace volume.
- *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.
- *NFS or 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.

Product versions and revision history

Product Tested	Version Tested
NetApp StorageGRID	v8.1.2.0
F5 Acopia ARX	5.1.5

Document Version	Description
1.0	New deployment guide

Theory of operation

User access to NetApp StorageGRID is via CIFS protocol to the gateway nodes (NetApp StorageGRID supports CIFS, NFS and HTTP/Rest access protocols, however for the purpose of this document we are looking at accessing content through CIFS only). When the ARX copies a file to one of the CIFS shares it is stored locally in the gateway cache. In the background, the file is uploaded across a secure VPN connection into two geographically separated NetApp data centers. As files are committed to the Data Center StorageGRID, the local copies residing in cache may be freed up. This process occurs autonomously. The directory entries from the user's point of view will still show the files as available through the same virtual service regardless of the file's physical location.

When a user accesses a file stored on the grid, the gateway nodes attempt to retrieve it from local cache if its still available. Otherwise the local gateways request the file from the data center and send it to the user. During this time, the user's file is copied from the data center grid and cached locally within the StorageGRID Gateway. File retrieval rates depend on the customer environment and available WAN bandwidth.

If the files are modified and saved, the files will be eligible to be promoted to higher level tiers.

Configuration example

In the following diagram, we show basic connectivity between clients, ARX Tier 1 and Tier 2 storage, and the NetApp StorageGRID Gateways. In this configuration, a client attempts to retrieve a file from a file share. The ARX proxies the request, and transparently retrieves the file from the server storing the file. We configure a policy on the ARX that periodically checks the last time files were modified, and migrate the file to the appropriate filer if the conditions of the policy are met. In our example, the ARX policy is checking for a last modified time of less than (or more than) 30 days. If the policy matches, then the ARX moves the file between the back end filers according to policy. If the file has not been modified in more than 180 Days it will be moved to the NetApp StorageGRID gateway to be stored off site in NetApp data centers.

The network configuration defined in the lab utilized an ARX with 4 Gigabit Ethernet links configured into a LACP bundle between the ARX and the core switch. The ARX, Tier 1 Storage, Tier 2 Storage, Active Directory Primary Controller, and Test client are all on the same subnet. The StorageGRID Gateways were deployed in a DMZ network. The ARX Proxy User is assigned backup operator privileges for the StorageGRID Gateways.

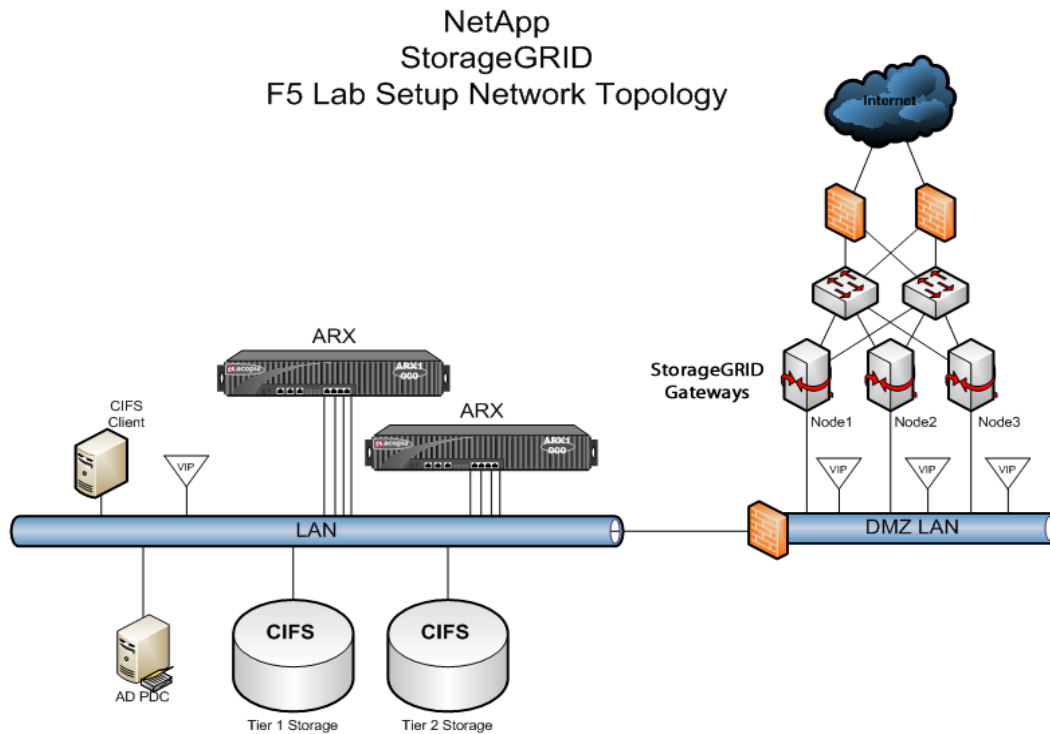


Figure 1 Logical configuration example

Installing the NetApp StorageGRID Gateway hardware

The NetApp StorageGRID Gateway hardware is deployed and installed by NetApp engineers. During the installation, the hardware is physically installed at the customer premise. The customer provides IP addresses, Windows Domain Controller Login Credentials, and Internet access.

NetApp Engineers take the details provided by the customer and provisions the gateway hardware accordingly. Many of these attributes are also needed in order to configure the ARX.

The following details are needed in order to configure the solution:

1. Customer Facing IP Network settings
 - StorageGRID Gateway Node IP addresses: one per node
 - StorageGRID Gateway Virtual IP address: one per node
 - IP Mask and Gateway for internal IP networks not reachable via the Internet Default Gateway
2. Internet Facing IP Network settings
 - Three Externally routable IP addresses and mask
 - External IP address of the Internet Default Gateway
 - Primary and Secondary DNS addresses
3. Microsoft Windows Server details
 - Windows Active Directory Domain Name
 - Primary Domain Controller IP address
 - CIFS Share names
 - ARX Proxy User
 - Active Directory Join Domain Authentication Credentials

These configuration attributes are applied by the NetApp Deployment Engineers.

Initial Configuration of the NetApp StorageGRID Gateways

The initial configuration of the NetApp StorageGRID Gateway is also performed by the NetApp Engineer on site and the network operations center staff. The results of this configuration have the gateway nodes

provisioned on the customer networks. The gateways are authenticated to the Primary Domain Controller, and the CIFS Shares are accessible to the ARX.

◆ Note

The Domain Controller login credentials are required in order to properly join the AD Domain.

Configuring the ARX

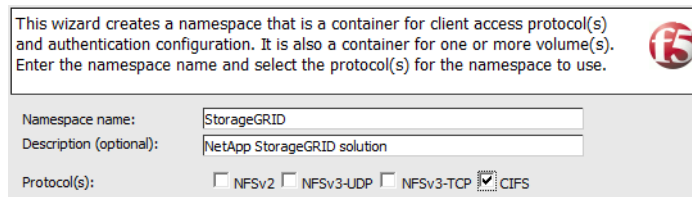
This section we configure the ARX to access the Tier 1 and Tier 2 Storage, and the StorageGRID Gateways. A CIFS namespace is created with 3 shares added to it. The shares are incorporated into a managed volume with a file placement policy. As files age and are not modified for more than 60 days they are moved between these shares depending upon the file last modified time. As the files last modified time is longer than 180 days these files are placed on the StorageGRID Gateways for off site backup.

Creating the CIFS Namespace

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

To create the CIFS namespace

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



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

Namespace name:

Description (optional):

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

Figure 2 Configuring the Namespace

5. From the CIFS authentication information screen, click the **Use NTLM** box. Click the **Add** button to add an NTLM server.
 - a) In the **NTLM Auth. Server Name** box, type the Fully Qualified Domain Name (FQDN) of the server.
 - b) In the **IP address** box, type the IP address of the server
 - c) In the **Port** box, type the appropriate port, or leave it at the default setting: **25805**.
 - d) In the **Secure Agent password** box, type the password. This is the password assigned on the Domain Controller for the Secure Agent application. Retype the password.

- e) In the **Windows Domain** box, type the appropriate Windows Domain.
- f) Click **Save**. You return to the CIFS authentication page.

Create a new NTLM authentication server.

NTLM Auth. Server Name:	<input type="text" value="Auth_Server"/>
IP Address:	<input type="text" value="1.2.3.4"/>
Port:	<input type="text" value="25805"/>
Secure Agent Password:	<input type="password" value="••••••"/>
Confirm Secure Agent Password:	<input type="password" value="••••••"/>
Windows Domain:	<input type="text" value="siterequest.com"/>
Pre Win2k Domain:	<input type="text"/>

Figure 3 Configuring an NTLM server

6. In the Proxy User section, click **Add** to add a proxy user. This is the Active Directory user that was assigned as the Backup Operator in the previous section. This user is used by the ARX to access the back end filer CIFS shares.
 - a) In the **Proxy User Name** box, type the name. In our example, we type **proxy_user**.
 - b) Optionally provide a description for the user.
 - c) In the **Proxy User Account** box, type the proxy user account. In our example, we type **arx_proxy_user**.
 - d) In the **Proxy User Account Password**, type the password. Retype the password in the confirm box.
 - e) In the **Windows Domain** and **Pre Win2k Domain** boxes, type the appropriate Windows Domain. In our example, we type **siterequest.com** in both boxes.
 - f) Click the **Save** button. You return to the CIFS authentication page.

Create a new proxy user.

Proxy User Name:	<input type="text" value="proxy_user"/>
Description:	<input type="text" value="The ARX Proxy User with Backup Operator Privs"/>
Proxy User Account:	<input type="text" value="arx_proxy_user"/>
Proxy User Account Password:	<input type="password" value="••••••"/>
Confirm Proxy User Account Password:	<input type="password" value="••••••"/>
Windows Domain:	<input type="text" value="siterequest.com"/>
Pre Win2k Domain:	<input type="text"/>

Figure 4 Creating a new proxy user

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


Creating a Volume

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

In our example we place the Volume Metadata onto the legacy storage platform. 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 a volume on the ARX

1. From the left navigation pane, click **Common Operations**.
2. Click the **Create Volume** button. The Create Volume wizard opens.
3. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7.
In our example, we select **StorageGRID**.
4. In the Volume name box, type the volume name. In our example, we type **/NetApp_vol**. You can optionally add a description. See Figure 5.
5. Click the **Next** button.

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

Namespace:	StorageGRID
Volume name:	/NetApp_vol
Description (optional):	NetApp StorageGRID

Figure 5 Creating a new Volume

6. From the **Metadata file server protocol** list, select an appropriate protocol. In our example, we select **NFSv3-UDP**.
7. From the **Metadata file server** list, select the file server if configured. In our example, the external filer has not yet been configured, so we click the **Add** button.
 - a) In the **Name** box, type a name for the file server. In our example, we type **MetaDataServer**.
 - b) In the **Primary IP address** box, type the IP address of the filer. In our example, we type **10.2.3.7**.
 - c) Configure the other options as applicable for your configuration. In our example, we leave the defaults.
 - d) Click the **Save** button. You return to the Volume metadata page.
8. In the **Metadata CIFS share/NFS path** box, type the path. In our example, we type **/metadata**. Click the **Next** button.
9. From the CIFS Parameters page, in the Auto-synchronization section, click the **Auto-synchronize** box.

Note

The StorageGRID Gateway does not support all the CIFS Attributes the ARX can support. The Volume CIFS Attributes is the intersection of all external shares CIFS capabilities.

10. In the CIFS Attributes section, uncheck the **Auto-detect CIFS attributes** box. Click the **Persistent ACLs** and **Unicode on disk** check boxes. Click the **Next** button.
11. From the Volume Parameters page, in the Performance Tuning section, from the **VPU ID** list, select **Dynamic**. Ensure the **Auto Reserve files** box is checked.
12. In the Share Import Modifications section, click the **Allow modifications to files or directories on import (per share settings)** button.
13. In the Enable Volume section, click the **Enable the volume when finished** button (see Figure 6).

14. Click the **Next** button.
15. Review the summary, and click **Finish**.

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

Performance Tuning

VPU ID:

Auto reserve files

Maximum files:

Import Conflict Resolution

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

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

By default volumes are created Read-Only.

Shadow Target

Make this volume a shadow-copy target.

Enable Volume

Enable the volume when finished.

Figure 6 Configuring the volume parameters

Adding the External Filers

In this section we add the Tier 1, Tier 2, and the NetApp StorageGRID Gateway as an external filer of the ARX. These values 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 **Tier1**.
4. In the **Primary IP Address** box, type the primary IP address. In our example, we type **10.2.3.8**.
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 for Tier 2 Filer. Name the entry **Tier2**. Add the NetApp StorageGRID Gateway node and name the entry **StorageGRID Gateway**. Chose one of the StorageGRID Gateway node virtual IP address as defined in section *Initial Configuration of the NetApp StorageGRID Gateways*, on page 5 as configured by the NetApp Engineer.

Adding the root level share

First file share we add is the root level share. This is the Tier 1 storage volumes with file content. The subsequent shares to be added adapt to the root volume permissions. As stated in the prerequisites section, we assume the Legacy storage is installed and the root level share is known. In our example, the root share on the Tier 1 External Filer is named **Tier1**.

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 **Tier1**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7. In our example, we select **StorageGRID**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 9. In our example, we select **/NetApp_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 namespace and volume. 

Share name:

Namespace:

Volume:

Figure 7 Configuring the initial properties of the root level share.

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 11. In our example, we select **Tier1**.

-
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **Tier1**.
 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. Click the **Next** button.
 10. Review the summary, and click the **Finish** button.

Adding the Tier 2 CIFS Shares

Next, we add the Tier 2 CIFS share to the volume.

To add the CIFS Share to the volume

1. From the left navigation pane, click **Common Operations**.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **Tier2**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7. In our example, we select **StorageGRID**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 9. In our example, we select **/NetApp_vol**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in the repeated step 3 of *Adding the External Filers*, on page 11. In our example, we select **Tier2**.
7. In the **CIFS Share** box, type the name of the CIFS for the Tier2 server. In our example, we type **Tier2**.
8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import**, **Rename directories with naming collisions on import**, and **Synchronize directory attributes between shares on import** boxes. See Figure 8.
9. Click the **Next** button.
10. Review the summary, and click the **Finish** button.

Select the file server and file server share to add to the volume. If the volume is a managed volume, select any import options and indicate whether the share contains access control lists with local groups.

Share name: Tier2

File Server: Tier2

CIFS Share: Tier2

Import Priority: 65535

Import Conflict Resolution

Rename files with naming collisions on import.

Rename directories with naming collisions on import.

Synchronize directory attributes between shares on import.

Disable the managed file system check on import.

Local Groups

Share contains local groups

Ignore SID errors

Enable Share

Enable this share when finished.

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

Figure 8 Configuring the CIFS Share

Adding the NetApp StorageGRID Gateway Share

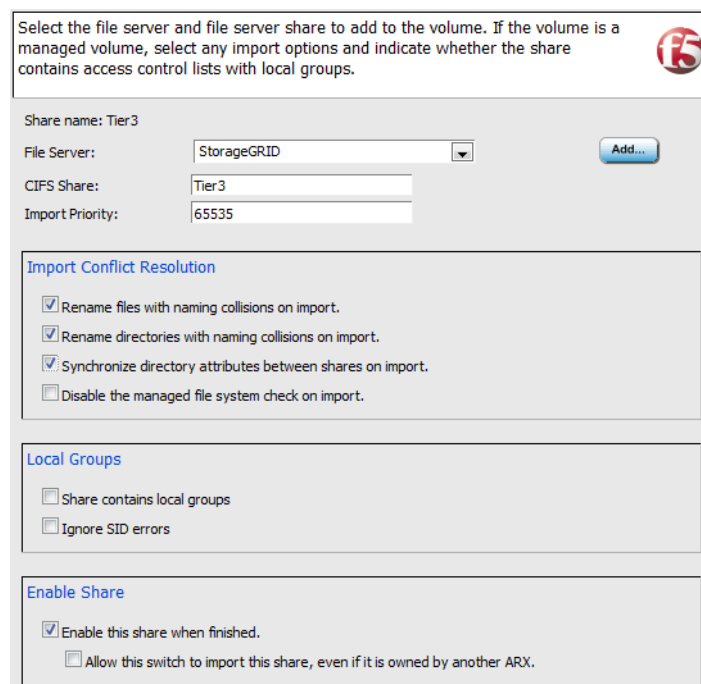
The StorageGRID Gateway Share needs to be added to the volume. This share is the gateway to the NetApp Data Center. Any files or directories copied to this filer are uploaded to the NetApp Data centers.

This share is referenced as Tier 3 storage.

To add the CIFS Share to the volume

1. From the left navigation pane, click **Common Operations**.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **StorageGRID Gateway**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7. In our example, we select **StorageGRID**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume*, on page 9. In our example, we select **/NetApp_vol**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in the repeated step 3 of *Adding the External Filers*, on page 11. In our example, we select **StorageGRID Gateway**.

7. In the **CIFS Share** box, type the name of the CIFS for the NetApp StorageGRID Gateway. In our example, we type **Tier3**.
8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import**, **Rename directories with naming collisions on import**, and **Synchronize directory attributes between shares on import** boxes. See Figure 8.
9. Click the **Next** button.
10. Review the summary, and click the **Finish** button.



Select the file server and file server share to add to the volume. If the volume is a managed volume, select any import options and indicate whether the share contains access control lists with local groups.

Share name: Tier3

File Server: StorageGRID

CIFS Share: Tier3

Import Priority: 65535

Import Conflict Resolution

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

Local Groups

- Share contains local groups
- Ignore SID errors

Enable Share

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

Figure 9 Configuring the CIFS Share

Creating the File Placement Policies

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

In this example we create a Policy rule to move files that have not been modified for more than 30 days onto the Tier 2 Storage device. The policy is enumerated every 30 minutes.

We also define a second Policy that places files that have not been modified for more than 180 days to the NetApp StorageGRID gateway for off site archiving via the internet. The second policy is scheduled to enumerate the external filers once a day.

To create the file placement policy

1. From the left navigation pane, click **Common Operations**.
2. Click the **Tiered Storage** button. The Tiered Storage Wizard opens.
3. In the **Policy name prefix** box, type a prefix. In our example, we type **Migrate_1**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7. In our example, we select **StorageGRID**.
5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume*, on page 9. In our example, we select **/NetApp_vol**.
6. From the **Number of tiers** list, select a number of tiers. In our example we select **3**.

This wizard creates multiple policies to dynamically move files between tiers (i.e. shares or share-farms) in a managed volume. Enter the policy name prefix which will be used to prefix policy rule names. Select the namespace, managed volume, and number of tiers for the policy.

f5

Policy name prefix:	<input type="text" value="Migrate_1"/>
Namespace:	<input type="text" value="StorageGRID"/>
Managed volume:	<input type="text" value="/NetApp_vol"/>
Number of tiers:	<input type="text" value="3"/>

Figure 10 Creating a new 3 Tier Storage Policy

7. Click the **Next** button.
8. For Tier 1, select the Tier 1 file share you created in *Adding the root level share*, on page 12. In our example, we select **Tier1**. Click the **Next** button.
9. For Tier 2, select the Tier 2 file share you created in *Adding the Tier 2 CIFS Shares*, on page 13. In our example, we select **Tier2**. Repeat for any additional Tiers. Click the **Next** button.
10. For Tier 3, select the Tier 3 file share you created in *Adding the NetApp StorageGRID Gateway Share*, on page 14. In our example, we select **Tier3**. Click the **Next** button.

11. The next step is to specify the criteria for moving files between Tier 1 and Tier 2 and the schedule. Click the **Add** button to the right of Schedule to define the schedule to be associated with the policy.
 - a) In the **Schedule Name** box, type a name for this schedule. In our example, we type **Tier2_Schedule**.
 - b) In the **Start Time** fields, you can specify a specific start time. In our example, the start time will be **1 A.M.**
 - c) In the **Every** box, type a number, and select a time period from the list. In our example, we type **1**, and select **days** from the list.
 - d) The other fields are optional, configure as applicable for your deployment.
 - e) Click the **Save** button. You return to the Tiered Storage Wizard.

Create a policy schedule

Schedule Name	Tier2_Schedule
Description	
Start Time	<input checked="" type="checkbox"/> Specify start time. 11 / 11 / 2010 - 01 : 00 <small>Day Month Year Hour Minute</small>
Stop Time	<input type="checkbox"/> Specify stop time. 11 / 11 / 2010 - 20 : 00 <small>Day Month Year Hour Minute</small>
Interval	<input checked="" type="radio"/> Every 1 days <input type="radio"/> Weekdays Frequency: Every <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday <input type="radio"/> Days Day of Month: <input type="text"/> <input type="radio"/> Hours Hour: 00 <input type="button" value="Add"/> <input type="text"/> Minute: 00 <input type="button" value="Remove"/> <input type="text"/>
Run Duration	<input type="checkbox"/> Specify run duration. 0 : 0 <small>Hour Minute</small>

Figure 11 Creating a new policy schedule

12. From the **Move files not** list, select **Modified**. In the **In the last** box, type a number and select a time period. In our example, we type **30** and select **days** from the list. So files are moved if they have not been modified for 30 Days with the schedule defined in the previous step.
13. In the Enable box, ensure the **Enable this policy when finished** box is checked.

14. The Fileset option allows the policy to restrict its operation to files that match a Fileset criteria. In this example we left the fileset un set at the default value.
15. Click the **Next** button.
16. The next step is to specify the criteria for moving files between Tier 2 and Tier 3 and the schedule. Click the **Add** button to the right of Schedule to define the schedule to be associated with the policy.
 - a) In the **Schedule Name** box, type a name for this schedule. In our example, we type **Tier3_Schedule**.
 - b) In the **Start Time** fields, you can specify a specific start time. In our example, we leave the fields at the default.
 - c) In the **Every** box, type a number, and select a time period from the list. In our example, we type **1**, and select **day** from the list.
 - d) The other fields are optional, configure as applicable for your deployment.
 - e) Click the **Save** button (see Figure 11). You return to the Tiered Storage Wizard.
17. From the **Move files not** list, select **Modified**. In the **In the last** box, type a number and select a time period. In our example, we type **180** and select **days** from the list. So files are moved if they have not been modified for 180 Days with the schedule defined in the previous step.
18. In the Enable box, ensure the **Enable this policy when finished** box is checked.
19. Click the **Next** button.
20. Review the summary and then click the **Finish** button.

Creating a fileset migration policy

A *fileset* is a group of files and/or directories to which you can apply replication and migration policies. You can configure filesets based on filename, directory path, size, and/or age. You can create complex filesets by joining multiple filesets in a union or taking the intersection of two or more filesets.

In this section we create a fileset migration policy. This policy enumerates files in a directory and the files that have not been modified are copied to the StorageGRID Gateway to be stored in the Cloud Storage.

This functionality allows for a manual override of the last Modified rules and forces a fileset to be written to the NetApp data center via the StorageGRID Gateway.

As an example this same fileset operation could be used to migrate project directories in their entirety to the backup Tier3 regardless of the last modified date.

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 **Backup_Files**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 7. In our example, we select **StorageGRID**.
5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume*, on page 9. In our example, we select **/NetApp_vol**.
6. 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 **Backup_files**.
 - 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**. And applied a ***.*** wildcard setting.
 - d) In the **Path Matching Criteria** selection, select the criteria. In our example we chose **Exact Match**. And applied a directory name of **/backup**.
 - 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: Backup_files

Fileset Type: filename

Filename Matching Criteria:

 Exact Match
 Wildcard Expression (i.e. shell style)
 Regular Expression

 Criteria: *.*

Exclude Name:

Ignore Case for Name:

Path Matching Criteria:

 Exact Match
 Wildcard Expression (i.e. shell style)
 Regular Expression

 Criteria: /backup/

Exclude Path:

Ignore Case for Path:

Recurse Subdirectories:

Figure 12 Creating a new Fileset

7. The next step is to define the **Match Criteria** for the fileset policy. In our example we chose **Files and Directories**.
8. For Source, select the Source file share you created in *Adding the root level share*, on page 12. In our example, we select **Tier1**.
9. For Target, select the Tier 3 file share you created in *Adding the NetApp StorageGRID Gateway Share*, on page 14. In our example, we select **Tier3**. Click the **Next** button.

Select the fileset to use for matching files and the target where they will be placed. The target can be a share or a share farm.

Fileset: Backup_Files

Match Criteria: Files and Directories

 Promote Directories

Source: Tier1 [share]

Target: Tier3 [share]

Figure 13 Creating a new Fileset matching criteria

10. The next step is to define the **Optional Parameters**. In our example we selected a Schedule. Select the Tier3_schedule you created in Step 15 of *Creating the File Placement Policies*, on page 15.
11. Click the **Next** button.
12. Review the summary and then click the **Finish** button.

Creating the Virtual Service

The Virtual Service is how the ARX presents CIFS Shares to the network clients. Clients send file requests through the Virtual Service and the ARX will proxy these requests to the appropriate back end 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 7. In our example, we select **StorageGRID**.
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 **NetApp_StorageGRID.siterequest.com**.
 - b) In the **IP Address** box, type the IP address of the VIP. In our example, we type **10.2.3.9**.
 - 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 **311**.
5. Ensure the **Enable the virtual service when finished** box is checked.


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:	StorageGRID
<input type="radio"/> Add export(s) to an existing virtual service (VIP)	
Virtual Service Name & IP Address:	-- No VIPs are defined --
<input checked="" type="radio"/> Create a new virtual service	
Virtual service DNS name:	NetApp_StorageGRID
IP Address:	10.2.3.9
Subnet Mask:	255.255.255.0
VLAN ID:	311
Enable Virtual Service	
<input checked="" type="checkbox"/> Enable the virtual service when finished	

Figure 14 *Creating a new Virtual Service*

6. Click the **Next** button.

7. In the **Windows Domain Name** and **Pre Win2k Domain** boxes, type the Windows domain name. In our example, we type **siterequest.com**.
8. 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.
9. Click the **Next** button. The Virtual Service Exports screen opens.
10. In the Export Name box, type a name for the Export. In our example, we type **NetApp_StorageGRID_GW**.
11. Configure the other options as applicable for your configuration, and then click the **Add Export** button.

Optionally export one or more volumes from the virtual service. The volume path is the path within the volume to export (the default is to export the root). The export name is the name that clients will mount. 

Volume	Volume Path	Export Name	Filer Subshare (optional):	
/NetApp_vol	/	NetApp_StorageGRID_GW	No	Remove

New Export

Protocol: CIFS

Volume: /NetApp_vol

Volume Path: /

Export Name:

Description (optional):

[Filer Subshares](#)

Filer Subshare (optional):

Filer Subshare Hidden (optional):

[Add Export](#)

Figure 15 Configuring the Export for the virtual service

12. Click the **Next** button.
13. Review the attributes and confirm the creation of the Virtual Service by clicking **Finish**.

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

Verifying the Storage Integration

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

An ARX report is generated to show where the files were placed on the back end storage arrays (see *Generating an ARX Metadata Report*, on page 23).

Mounting the Virtual Server CIFS share

The first step is to confirm the Virtual Service is operating properly. To do this, from a Windows client, we map a network drive to the Virtual Service Export. The export shows files and directories exist. The user is unable to determine which of the three back end file shares host the files. The ARX has merged the files and directories into one common virtual path.

To map a drive for Virtual Service CIFS share

1. From the XP client, open **My Computer**.
2. From the **Tools** menu, click **Map Network Drive**.
The Map Network Drive wizard opens.
3. From the **Drive** list, select an unused Drive letter.
4. In the **Folder** box, type the Virtual Service FQDN and export path.
In our example, we type
NetApp_StorageGRID.siterequest.com\NetApp_StorageGRID_GW.
5. If the client's current user name is different than the Active Directory user name, click the **Connect using a different user name link**. Specify the user credentials, and then click **OK**. In our example, we use a qualified domain user.
6. Click the **Finish** button. The drive is now mapped.

The drive can now be explored. The content is stripped across the back end servers and presented as a unified volume to the client.

The volume statistics can be viewed from the ARX GUI by clicking **Managed Volumes** in the left pane, and selecting the Volume name.

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 back end 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 on the Managed Volume **/NetApp_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.
8. 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 **Verification_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	StorageGRID
Volume	/NetApp_vol
Path	/
Report Type	<input type="radio"/> Inconsistencies <input checked="" type="radio"/> Metadata <input type="radio"/> Symlinks
Output Report Name	Verification_Report
Recurse Subdirectories	<input checked="" type="checkbox"/> Recurse Subdirectories
Share	All
Include File Handles	<input checked="" type="checkbox"/> Include File Handles

Figure 16 Generating a Report

Highlighted below are the report attributes, file and directory information. The share that each file is currently stored in is listed in the *Share* column. The paths are stripped across all the shares within the managed volume and contain different files depending upon the files last modified time.

```

**** Metadata-Only Report: Started at Tue Jun 15 15:05:57 2010 ****
**** Software Version: 5.01.005.11965 (Mar 9 2010 17:25:04) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: StorageGRID
**** Volume: /NetApp_vol
**** Path: /NetApp_vol

```

Share	Physical Filer
[Tier1] 10.2.3.8:Tier1
[Tier2] 10.2.3.10:Tier2
[Tier3] 10.2.3.11:Tier3

**** Legend:

**** FL = File: The reported entry is a file.
 **** DR = Directory: The reported entry is a directory.
 **** SL = Symlink: The reported entry is a symbolic link.
 **** 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
[DR] [Tier1] /System Volume Information
[DR] [Tier1] /._nfs
[DR] [Legacy_Storage] /ISO
[DR] [Tier3] /traces
[DR] [Tier3] /VMWare
[DR] [Tier3] /docs
[DR] [Tier3] /tools
[DR] [Tier3] /Deployment_Guides
[FL] [Tier3] /System Volume Information/tracking.log
[DR] [Tier3] /Deployment_Guides/NetApp
[FL] [Tier3] /Deployment_Guides/NetApp/NetApp.vss
[FL] [Tier2] /Deployment_Guides/NetApp/NetApp.pdf
[FL] [Tier3] /Deployment_Guides/Dell/Dell-PowerEdge-Servers.vss
[FL] [Tier2] /Deployment_Guides/NetApp/NetApp-dg.pdf
[FL] [Tier1] /Deployment_Guides/NetApp/Old PowerVault.RDP
[FL] [Tier1] /Deployment_Guides/NetApp/pvnx1950_smb.pdf

◆ **Note**

The full report was edited to reduce the size of this document for demonstration purposes.

Conclusion

This deployment guide demonstrated one way to integrate F5 ARX platform with the NetApp StorageGRID Gateway. The deployment enables the migration of files from Tiered storage platforms into NetApp data centers via a secure VPN tunnel.

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