



What's inside:

- 2 Configuration example
- 3 Configuring the ARX
- 10 Mapping a network drive on the SharePoint server
- 10 Configuring AvePoint DocAve to use the mapped drive
- 12 Importing the ARX Virtual Service hosted file contents
- 13 Synchronization Operations
- 14 Appendix: Verifying ARX Client access

Deploying ARX File Virtualization with AvePoint DocAve File Share Connector for SharePoint

Welcome to the F5 ARX deployment guide for AvePoint® DocAve® File Share Connector for SharePoint for use with Microsoft® SharePoint®. This guide provides step-by-step instructions on configuring ARX file virtualization with the DocAve File Share Connector for SharePoint.

The DocAve File Share Connector for Microsoft SharePoint is an application that allows file system content to be imported into a SharePoint site collection. Once the file contents have been imported, periodic synchronizations occur between SharePoint and the file system. These synchronizations pick up new files from the file system and update the files that have been modified by users accessing the content from SharePoint.

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

For more information on DocAve, see <http://www.avepoint.com/SharePoint-management-of-file-share-content/>

Products and versions tested

Product	Version
Microsoft SharePoint	2010
F5 ARX	5.2.0
AvePoint DocAve	v5.6.1.0

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- SharePoint 2010 is installed, configured, and a site collection exists
- ARX Managed volume with two tiers is configured with an AD authenticated CIFS virtual service.
- File content exists, or is copied into the CIFS Virtual service.

- AvePoint and the File Share connector have been installed with basic connector settings. For more information see the AvePoint DocAve File Share Connector How to Guide. http://www.avepoint.com/assets/pdf/SharePoint_user_guides/How_to_Install_and_Configure_DocAve_File_Share_Connector.pdf

To leave feedback for this or other F5 solution documents, email us at solutionsfeedback@f5.com

Configuration example

SharePoint clients access the site with a web browser over http or https. In turn, the AvePoint File Share Connector communicates with the ARX virtual services over CIFS. The network consists of two windows 2008 storage servers with iScsi SAN attached storage.

In this guide the file system contents will be accessed through the ARX CIFS Virtual Service. The ARX will tier files based on last modified times and ensure the most recently modified content is on the tier 1 file systems. As files are migrated between the back end file systems, the SharePoint site does not change. The files are still visible and accessible through the SharePoint site collections.

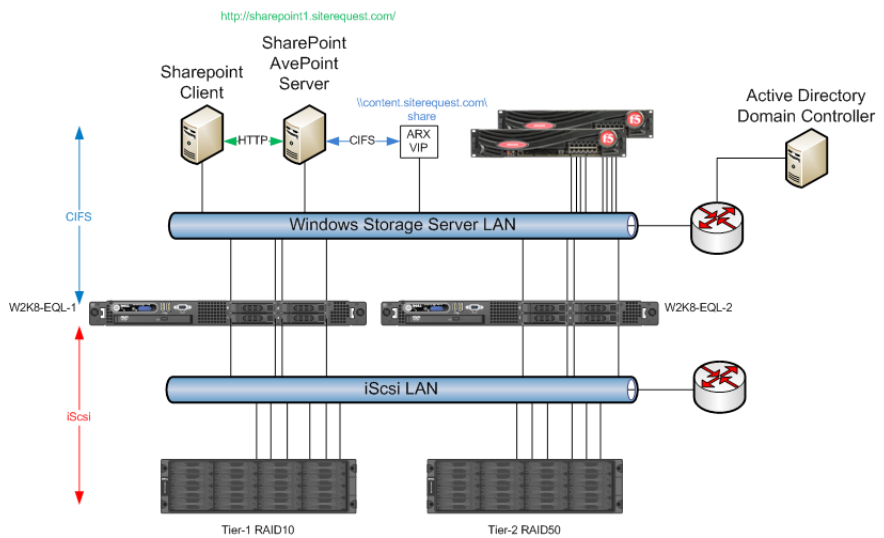


Figure 1: Logical configuration example

Configuring the ARX

In this section, we show you how to configure the ARX series. In this guide, we detail how to configure a Managed volume with two tiers, including an AD authenticated CIFS virtual service.

Note



If you have an existing ARX configuration, you do not need to perform this configuration. Continue with *Mapping a network drive on the SharePoint server on page 10*.

Creating an Authentication Server

The first task in the ARX configuration is to create an Authentication server. In this example, we show how to configure an Active Directory Authentication server.

To create the Active Directory Authentication server

1. From the navigation pane, expand **Authentication**, and then click **NTLM Auth. Servers**. The server summary opens.
2. Click the **Add** button. The Add NTLM Authentication server page opens.
3. In the **NTLM Auth. Server Name** box, type a name for the server. In our example, we type **siterequest**.
4. In the **IP Address** box, type the IP address of the server. We type **10.60.112.10**.
5. In the **Windows Domain Name** box, type the Windows domain. In our example, we type **siterequest.com**.
6. In the **Secure Agent Password** box, type the password. This is the password assigned on the domain controller for the secure agent application. Confirm the password in the next box.
7. Leave the **Agent Port** box at the default.
8. Click **OK**.

Creating a Proxy User

The next task in configuring NTLM authentication is to create a proxy user.

To create a proxy user

1. From the navigation pane, expand **Authentication**, and then click **CIFS Proxy Users**.
2. Click the **Add** button. The Add CIFS proxy user page opens.
3. In the **Proxy Username** box, type the username. This is the Active Directory user that was assigned as the Backup Operator. These user credentials are used to access the backend filer CIFS shares.
4. In the **Proxy User Account** box, type the Proxy User Account.
5. In the **Proxy User Account Password** box, type the associated password. Confirm the password in the next box.
6. In the **Windows Domain** box, type the domain. In our example, we type **siterequest.com**.
7. In the **Pre Win2k Domain** box, type the domain. In our example, we type **siterequest**.
8. Click **OK**.

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.

The active Directory authentication configuration is complete.

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. This is the AD domain user that is a member of the backup operator group for each Windows file server. In our example, we type **acmeuser001**. Click the **Next** button.
7. Click the **Finished** button.

Creating a Volume

The backend filer CIFS shares will be incorporated into an ARX Managed Volume. File placement policy is managed at the volume level. In this example, we place the Volume Metadata onto the incumbent 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 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 the appropriate protocol. In our example, we 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. If you are using a file server for which the ARX supports snapshots (such as NetApp), make sure there is a check in the **This file server supports snapshots** box. For more information on snapshot support, see the ARX documentation.
 - f. From the **File Server Type** list, select the appropriate server type. In our example, we 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 snapshot directories the ARX should ignore, and then click the **Add** button. In our example, we type **.snapshot, ~snapshot**.
 - k. Click the **Save** button. You return to the managed volume wizard.
7. In the **Metadata CIFS share/ NFS** path box, type the path. In our example, we type **/metadata**.
8. Click **Next**. 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. Configure the Performance Tuning section as applicable for your configuration.
11. *Optional:* Click the **Files and directories can be renamed during import and re-import** button.
12. Check the **Enable the volume when finished** box, and then click **Next**.
13. Review the summary, and then click **Finish**.

Adding the External Filers

The next task is to add the external filer entries to the ARX. These entries are referenced later when we add the filer shares to the managed volume.

To add the External Filers

1. From the navigation pane, click **File Servers**.
2. Click the **Add** button. The Add File Server screen opens.
3. In the **Name** box, type a name for this File Server. In our example, we type **filer1**.
4. In the **Primary IP Address** box, type the primary IP address. In our example, we type **10.10.10.2**.
5. In the **Secondary IP Address** box, type any secondary IP addresses, and then click the **Add** button. In our example, we do not include any secondary IP addresses.
6. In the **Description** box, you can optionally type a description.
7. In the **Ignore Directories (optional)** box, type any snapshot directories the ARX should ignore on the backend file shares, and then click the **Add** button.
8. Click the **OK** button.
9. Repeat this entire procedure for additional filers.

Adding the root level share

First file share we will add is the root level share. This is the incumbent legacy storage volumes with file content. The subsequent shares to be added 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 **Share0**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace on page 4*. In our example, we select **Content**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Volume on page 4*. 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 *Adding the External Filers on page 5*. In our example, we select **netapp**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share0**.
8. *Optional:* In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes. By checking this box, in the case a collision, directories and files are renamed.
9. Click the **Next** button.
10. Review the summary, and click the **Finish** button.
11. **Important:** Repeat this procedure to add additional shares to the managed volume.
These are the shares from the filers you created in Adding the External Filers, on page 14. These shares are used in a share farm. A share farm is a way to add storage to an existing managed volume and is often used to build a load balanced environment for storage access.

Give the shares a unique name, and from the File Server list, select the appropriate file server (filer1, filer2 and so on).

In Step 8, also check **Synchronize directory attributes between shares on import**. This ensures the new volume inherits the root share attributes.

Creating the Share farm

A share farm is a load balancing feature. When files are migrated to the share farm the files are stripped between the share farm members. If a managed volume needs more capacity the user can add more shares to the share farm and dynamically redistribute files across all shares.

In this example we group the three previously added shares together.

To create the Share farm

1. From the left navigation pane, click **Common Operations**.
2. Click the **Load Balancing** button. The Load Balancing Wizard opens.
3. In the **Policy name** box, type a name for this policy. In our example, we type **Sharefarm**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace on page 4*. In our example, we select **Content**.
5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume on page 4*. In our example, we select **/data**.
Click the **Next** button.
6. Click the boxes of the file shares to be included in the share farm.
Click the **Next** button.
7. From the **Load Balancing Algorithm** list, select an appropriate load balancing method. In our example, we select **Round-Robin**.
8. In the Constraint Options section, click the **Place new files in the same shares as their parent directories** box.
9. In the **Enable** section, ensure the **Enable this load balancing policy when finished** box is checked.
10. Click the **Next** button.
11. Review the summary and then click the **Finish** button.

Creating a Tiered Storage policy

The next task is to create a tiered storage policy. This policy enumerates the file contents of the Tier-1 (share0) platform and if any files have not been modified for more than 90 days they are migrated to the Tier-2 (Share Farm) storage pool.

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 **Tiering**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace on page 4*. In our example, we select **Content**.

5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Volume on page 4*. In our example, we select **/data**.
6. From the **Number of tiers** list, select a number of tiers. In our example we select **2**. Click the **Next** button.
7. For Tier 1, select the root-level share you created in *Adding the root level share on page 6*. In our example, we select **share0**. Click the **Next** button.
8. For Tier 2, select the second Share farm you created in *Creating the Share farm on page 7*. In our example, we select **Sharefarm**. Click the **Next** button.
9. The next step is to specify the criteria for moving files and the schedule. Click the **Add** button to the right of Schedule to define the schedule to be associated with the policy.
 - a. In the **Schedule Name** box, type a name for this schedule. In our example, we type **Tiering_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 Interval section, configure an appropriate interval. In our example, we click the **Hours** button, from the **Hour** list, select **1**, and then click the **Add** button. In a production environment, you may want to run the schedule once a day.
 - d. The other fields are optional, configure as applicable for your deployment.
 - e. Click the **Save** button. You return to the Tiered Storage Wizard.
10. From the **Move files not** list, select **Modified**. In the **In the last** box, type a number and select a time period. In our example, we type **90** and select **days** from the list.
11. From the **Schedule** list, select the schedule you just created if it is not already selected.
12. In the **Enable** box, ensure the **Enable this policy when finished** box is checked.
13. Click the **Next** button.
14. 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 proxies these requests to the appropriate backend filer.

The ARX Client nodes connect to the Virtual service FQDN or IP address and map the share to an unused drive letter. The Virtual Service is created within the IP address scope of the Client LAN.

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 4*. 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 **172.30.72.102**.
 - c. In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.192**.
 - d. From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **302**.
 - e. Ensure the **Enable the virtual service when finished** box is checked.
5. Click the **Next** button.
 6. From the **Windows Domain Name** box, select the Windows domain name. In our example, we select **siterequest.com**.
 7. In the **Pre Win2k Domain** box, type the Pre Win2k Windows domain name. In our example, we type **siterequest**.
 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 New Export section, from the **Volume** list, select the Volume you created in *Creating a Volume on page 4*. In our example, we select **/data**.
 11. In the **Volume Path** box, type the Volume Path. In our example, we type **/**.
 12. In the **Export Name** box, type a name for the **Export**. In our example, we type **share**.
 13. Configure the other options as applicable for your configuration, and then click the **Add Export** button.
 14. Click the **Next** button.
 15. Review the summary and then click **Finish**.

The virtual service also needs to be incorporated into the Active Directory domain as a domain computer. For Kerberos authentication:

16. Check the box for the Virtual Service you just created and then click the **Join Domain** button.
17. Type the **Username**, User **Password**, and the **Organizational Unit**, and then click **OK**.

You can now review the Virtual Service by clicking **Virtual Services** from the navigation pane. Notice the Domain Join is Joined, Admin State is enabled and the Status is ready.

To verify ARX client access, see *Appendix: Verifying ARX Client access on page 14*.

This completes the ARX configuration.

Mapping a network drive on the SharePoint server

In this procedure, we map a network drive on the SharePoint server that is used by the File Share Connector.

To map a network drive

1. Open Windows Explorer, and from the **Tools** menu, select **Map Network Drive**. The Map Network Drive wizard opens.
2. From the **Drive** list, select an unused drive letter. We select **W**.
3. In the **Folder** box, type the network folder. The folder is comprised of the Virtual Service FQDN and export path.
4. Click the Connect using a different user name link. In the **User name** and **Password** boxes, type a domain user with the proper access rights. In our example, we use the Proxy User credentials. Click **OK**.
5. Click **Finish**. Windows explorer opens the new network drive and displays the contents. This drive is used by the File Share Connector.

Configuring the AvePoint DocAve File Share Connector for SharePoint to use the mapped drive

The next task is to configure AvePoint DocAve to use the network drive you just mapped.

To configure DocAve to use the mapped drive

1. Log onto the AvePoint web-based Manager Application. The interface is available at port 8080 on the SharePoint server. <http://<SharePoint Address or FQDN>:8080>
2. Type the Administrative login name and password. The DocAve home page opens.
3. On the Menu bar, click **Storage Optimization, Connector, Content Library**, and then **Settings**.
 - a. From the Navigation pane, click **Function Settings**.
 - b. In the **Profile Name** box, type a name for this profile. In our example, we type **ARX_Function**.
 - c. Click **Save**.

Net Share Settings | Cloud Storage Settings | Third Party Storage Settings

Settings Profile: **New** Profile Name: ARX_Function

Function Settings Profiles: Default, ARX_Function

Action	User Permissions	Configure
Load data from storage device	Full Control, Site Admin	Configure
Synchronize between storage device and SharePoint	Full Control, Site Admin	Configure
Store to SharePoint	Site Admin	Configure

Other Settings:

Prevent loading when the number of files exceeds: [input]

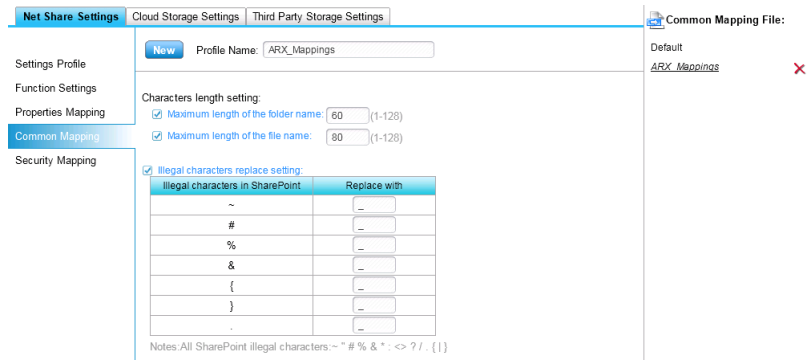
When loading a folder to SharePoint, the folder permission will be:

Unchanged

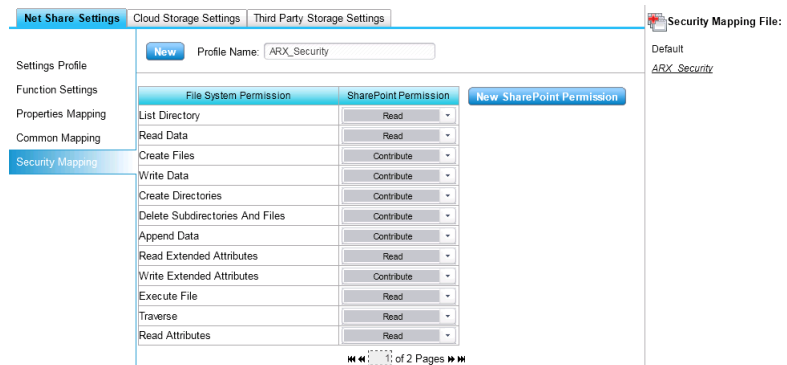
Set read-write to the DocAve account, none to other users.

Set read-write to the DocAve account, read right to the users who have rights on the folder now.

- d. From the Navigation pane, click **Properties Mapping**.
- e. In the **Profile Name** box, type a name. In our example, we use **ARX_Properties**.
- f. We recommend leaving the default settings. Click **Save**.
- g. From the Navigation pane, click **Common Mapping**.
- h. In the **Profile Name** box, type a name. In our example, we type **ARX_Mapping**.
- i. We recommend leaving the default settings. Click **Save**.

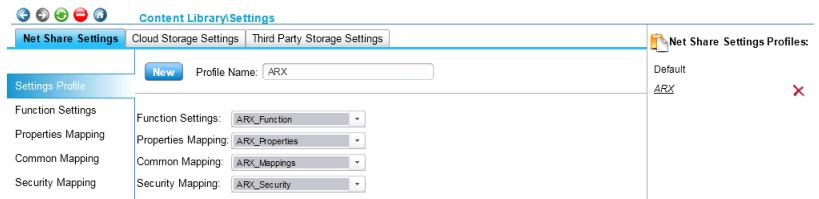


- j. From the Navigation pane, click **Security Mapping**.
- k. In the **Profile Name** box, type a name. In our example, we type **ARX_Security**.
- l. We recommend leaving the default settings. Click **Save**.

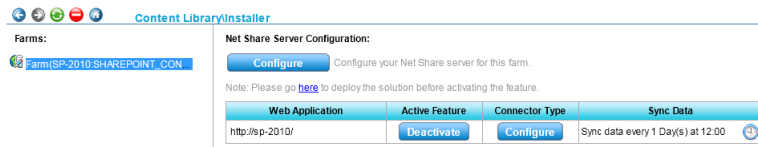


- m. From the Navigation pane, click **Settings Profile**.
- n. In the **Profile Name** box, type a name. In our example, we type **ARX**.
- o. From the **Function Settings** list, select the name of the Function Settings profile you created.
- p. From the **Properties Mapping** list, select the name of the Function Settings profile you created.
- q. From the **Common Mapping** list, select the name of the Function Settings profile you created.

- r. From the **Security Mapping** list, select the name of the Function Settings profile you created.
- s. Click the **Save** button. When you are finished, the screen should look like the following example.



4. From the Menu bar select **Storage Optimization, Connector, Content Library**, and then **Installer**.
 - a. Verify the **Content Library** is installed and configured.
 - b. From the Navigation pane, select the SharePoint Farm.
 - c. Ensure the **Web Application** is correct. If it is not, you need to start debugging your SharePoint implementation. We recommend making sure both SQL and SharePoint services are started. For more information, see the SharePoint documentation.

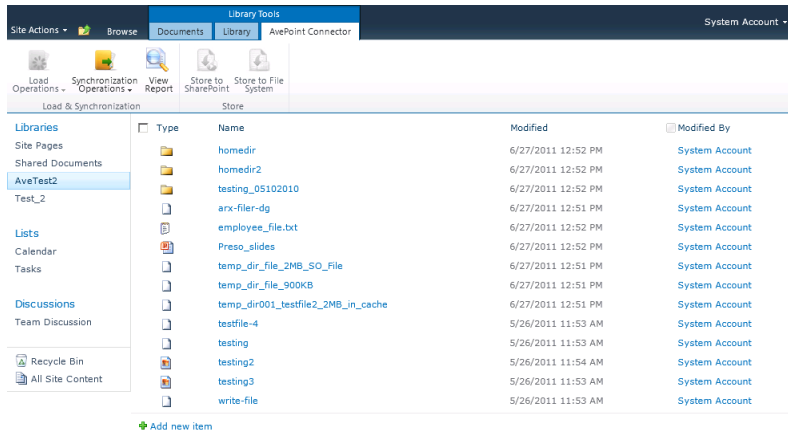


Importing the ARX Virtual Service hosted file contents

The next task is to import the ARX virtual service hosted file contents.

To import the ARX hosted file contents

1. Open a Web browser and navigate to the SharePoint Site.
2. In the Menu Ribbon click the Library Tool for AvePoint Connector. The list of menu items for AvePoint Connector open.
3. Select the Load Operations menu, and then click **Load**.
4. Specify the drive you mapped in *Mapping a network drive on the SharePoint server on page 10*. Pointers to the mapped drive file contents will be imported into the SharePoint site.
5. Now the site is populated with pointers to the file contents stored on the ARX Virtual Service Share.

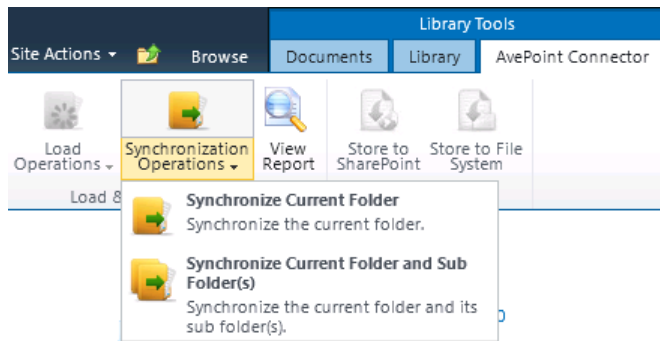


Synchronization Operations

The AvePoint File Share Connector periodically will synchronize the SharePoint content with the file system content. In the screen shot below the schedule will occur at 12:00 every day. Optionally the user can choose to force the synchronization to occur.

To force synchronization

1. Click the AvePoint Connector tab in Library Tools.
2. Click Synchronization Operations. The options are Current Folder or Current and sub-folders. Selecting either of these will cause a synchronization to occur and a progress status bar to be displayed.
3. The folders and sub folders will synchronize and update any changes.



This completes the configuration.

Appendix: Verifying ARX Client access

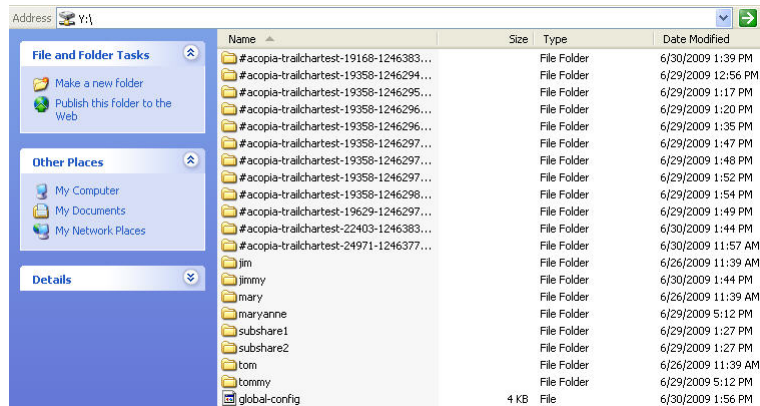
In this Appendix, we show how to verify the Test Client can access the ARX Virtual Service and the managed volume CIFS share. The ARX adds flexibility with the Managed Volume and Virtual Services that create a robust virtual machine environment providing continuous client access to data.

Mounting the Virtual Server CIFS share

To confirm the Virtual Service is operating properly, we map a network drive to the Virtual Service Export from a Windows Client. The export shows that files and directories exist. The user cannot determine on which backend file share the files reside. The ARX has merged the files and directories into one common virtual path.

To map the Virtual Service CIFS Share to drive letter

1. From a Windows client, open Windows Explorer, and, from the Tools menu, select Map Network Drive.
2. Select an unused Drive Letter and the network folder. The folder is comprised of the Virtual Service FQDN and export path.
3. From the Drive list, select an unused Drive Letter.
4. In the Folder box, type the network folder. The folder is comprised of the Virtual Service FQDN and export path. In our example, we type `\\share.siterequest.com\share`.
5. Select Connect using a different user name and specify the Domain User with the proper access rights. In our example, we use the Proxy User credentials.
6. Click Finish. Microsoft Windows mounts the drive. The drive can be explored and the following screen displays the file contents of the virtual service export.



In our example, there are multiple root level directories. Under these directories there is various test content. The content is stripped across the backend servers and presented as a unified volume to the client.

The volume statistics can be viewed from the ARX by clicking the Managed Volume in the left pane and then clicking the volume (`/data` in our example).

Generating an ARX Metadata Report

File placement can be determined by creating 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 generate an ARX Metadata report

1. From the navigation pane, click **Managed Volumes** and then click the volume (**/data** in our example).
2. From the Managed Volume Details screen, click **Report**.
3. On the Report Volume page, complete the following:
 - a. In the **Path** box, type the path. In our example, we type **/**.
 - b. In the **Report type** row, click **Metadata**.
 - c. In the **Output Report Name** box, type a name. In our example, we type **metadata_report**.
 - d. Click **OK**.

The ARX generates the report, which is accessible from the navigation pane by clicking **Reports**, and then clicking the name of the report you just created.

Add files to the Virtual Service CIFS share and rerun the report. Wait for the Tiering Policy to be invoked and compare the results of a metadata report from before versus after the policy is executed.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

