



Deploying the F5 ARX with the ARX Cloud Extender

Table of Contents

| | |
|---|----|
| Deploying the F5 ARX with F5 ARX Cloud Extender | |
| Prerequisites and configuration notes | 1 |
| Product versions and revision history | 2 |
| Configuration example | 3 |
| Configuring the F5 ARX Cloud Extender | 5 |
| Creating the source CIFS share | 5 |
| Configuring the ARX Cloud Extender Backup Operator user | 6 |
| Configuring the ARX Cloud Extender Connectors | 7 |
| Defining the Source Location | 11 |
| Configuring the ARX Cloud Extender storage destination | 12 |
| Creating a Rule | 15 |
| Creating a Policy | 16 |
| Creating a Task | 17 |
| Configuring the F5 ARX | 18 |
| Prerequisites | 18 |
| Disabling Sparse File Support | 18 |
| Adding the External Filer | 19 |
| Adding the Cloud Extender Share to the volume | 19 |
| Creating the File Placement Policy | 21 |
| Connecting to the Virtual Service | 25 |
| Storage Integration Verification | 28 |
| Generating an F5 ARX Metadata Report | 28 |
| Viewing the status of the F5 ARX Cloud Extender | 30 |
| Viewing Cloud Provider Status | 31 |
| Conclusion | 33 |

Deploying the F5 ARX with F5 ARX Cloud Extender

Welcome to the F5 ARX Cloud Extender deployment guide. This guide provides step by step procedures on deploying the Adaptive Resource Switch (ARX) with the ARX Cloud Extender for file based tiering to Cloud Storage Providers.

F5 ARX Cloud Extender works with the automated storage tiering capabilities of F5 ARX file virtualization devices to seamlessly extend the file storage infrastructure from the data center to the cloud. Customizable tiering policies automate the process of identifying and moving appropriate data to the cloud, which minimizes IT overhead and cost of access. And, data stored in the cloud is presented as if it resides locally in the data center, so users and applications can access information as they always have.

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

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:

◆ *Network Configuration*

- F5 ARX is configured for network access and the initial switch interview has been completed. If this has not been completed refer to the F5 ARX Hardware Installation guide for specific details.
- F5 ARX managed volume and Virtual Service for CIFS is configured and available.
An NFS Export with root access is available as an F5 ARX Metadata store.

◆ *Storage and ARX Configuration*

- Windows Storage Server is installed and configured for tier 1.
- This document is based on the fact that the Microsoft Active Directory Domain is preconfigured and the F5 Secure Agent is installed if necessary.
- The F5 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 F5 ARX platform. Redundant switch configuration steps within the product documentation should be followed in order to deploy a high available configuration.

◆ *F5 ARX Cloud Extender*

- The Cloud Extender hardware and software is installed with an initial network configuration for system management access has been applied.

- If you are using the F5 ARX Cloud Extender with Amazon S3, you must install and configure the plugin to use the Cloud Storage account. This requires an Amazon S3 account and Encryption keys. Follow the instructions provided in Chapter 5 of the F5 ARX Cloud Extender Administration Guide, available on Ask F5: http://support.f5.com/kb/en-us/products/arx_cloud_extender.html
 - If you are using the Cloud Extender with EMC Atmos, you must follow the instructions provided in Chapter 5 of the F5 ARX Cloud Extender product documentation to install the EMC Atmos Cloud Connector plugin.
 - The F5 ARX Cloud Extender does not support IPv6. Be sure not to have IPv6 Installed or Configured on the Windows Servers running the F5 ARX Cloud Extender Services.
- ◆ The F5 ARX does not support the Sparse file feature with F5 ARX Cloud Extender. Be sure to disable Sparse within the managed volume configuration.
 - ◆ The ARX Snapshot feature is not supported. Configure Sparse Snapshots so that the other filers within the managed volume can perform Snapshots.

Product versions and revision history

Product and versions tested for this deployment guide:

| Product Tested | Version Tested |
|---------------------------------------|-----------------|
| Microsoft Windows 2008 Storage Server | v6.0.6001 |
| F5 ARX Switch Firmware | 5.1.9 and 5.2.2 |
| F5 ARX Cloud Extender | v1.8.1.19 |

| Document Version | Description |
|------------------|---|
| 1.0 | New deployment guide |
| 2.0 | Added support for EMC Atmos and AT&T Synaptic (based on Atmos). Added NFS as a Destination Location. |

Configuration example

In the following diagram, we show basic connectivity between clients, F5 ARX, F5 ARX Cloud Extender and the Cloud Storage Managed Service Provider.

In this guide, we configure a policy on the ARX that checks the last time files were modified, and migrates the file to the appropriate filer if the conditions of the policy are met. In our example, the ARX policy is checking for a last modified time of less than (or more than) 30 days. If the policy matches, the F5 ARX moves the file between the backend filers according to policy. Files that meet the policy attributes are moved to the Cloud Extender cache and migrated to the Cloud Storage Provider. Migrated files are replaced with stub files. When these files are accessed, the Cloud Extender retrieves the file contents from the cloud storage provider.

The network configuration defined in the lab used an F5 ARX with 4 Gigabit Ethernet links configured into a LACP bundle between the F5 ARX and the core switch. The server Gig-E connections were bundled into two 4 Gig-E Smart Load Balancing connections. One bundle was dedicated to client traffic, another bundle dedicated for iSCSI storage array access. The Active Directory (AD) Primary Domain Controller was on a different subnet than the Windows storage servers. The Proxy User was assigned local Administrator group privileges for each Windows Servers.

The F5 ARX Cloud Extender has two server components: the first is the Web Server and is used as the Graphical User Interface for provisioning the F5 ARX Cloud Extender components. The second component is another server that performs the function of providing a CIFS Share for clients and migrates the files to the Cloud Storage Provider. The CIFS share is a source for the policy. Files placed in this share are migrated to the cloud storage provider.

This deployment guide is a demonstration of our example configuration. The example is simplified to include just two storage tiers. For production deployments, the ARX tiering policy will most likely be 3 or more storage tiers where the Cloud Extender is the last tier for files that have the oldest last modified times.

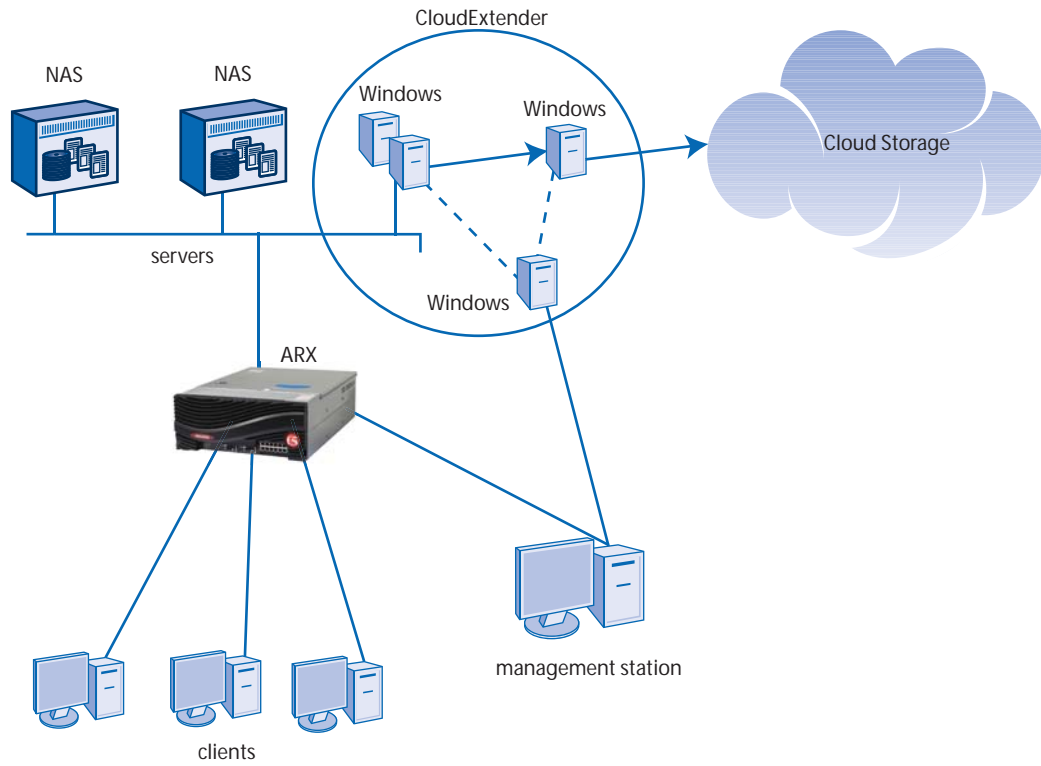


Figure 1 Logical configuration example

Configuring the F5 ARX Cloud Extender

First we configure the F5 ARX Cloud Extender. This section requires that the F5 ARX Cloud Extender has been properly installed and configured for Web Management access. There must be IP connectivity between the F5 ARX and the F5 ARX Cloud Extender. If there is not, repair the network configuration prior to proceeding with these procedures.

◆ Important

If Anti-Virus or Search and Indexing applications are in use or you plan to use them, be sure to configure these applications to ignore offline files. Otherwise these applications will invoke mass recalls of files stored within the cloud storage provider. For more details refer to Chapter 8 of the F5 ARX Cloud Extender Administration Guide.

Creating the source CIFS share

The first task is to create a CIFS Share on the F5 ARX Cloud Extender. This CIFS share is defined as the source location for files intended to be migrated to the Cloud Storage Provider. We also create a sub directory and define a new share for this location.

This procedure is performed from a MS Windows command prompt. In the following procedure, our example uses a directory in the root **E:** drive partition called **Cloud_Source**.

To create the source CIFS Share

1. Open a Windows Command Prompt.
2. Use the following command syntax, followed by pressing Enter:

```
mkdir <partition>:\<directory name>
```

in our example, we type

```
mkdir e:\Cloud_Source
```

3. Share the subdirectory with the following **Net Share** command, followed by pressing Enter:

```
net share Cloud_Source=e:\Cloud_Source /GRANT:Everyone,Full
```

Be sure to change the partition and directory name if you modified them from our example.

The command prompt reports that Cloud_Source was shared successfully.

4. To view the new share, type **net share**. You should see results similar to the following:

```

C:\>mkdir e:\Cloud_Source
C:\>net share Cloud_Source=e:\Cloud_Source /GRANT:Everyone,Full
sharename was shared successfully.
C:\>net share

```

| Share name | Resource | Remark |
|---------------------|------------------------|---------------|
| C\$ | C:\ | Default share |
| ADMIN\$ | C:\WINDOWS | Remote Admin |
| IPC\$ | | Remote IPC |
| E\$ | E:\ | Default share |
| share | E:\ | |
| Cloud_Source | e:\Cloud_Source | |
| tmp | E:\tmp | |

```

The command completed successfully.

```

The share has been created and is available for use.

Next the F5 ARX Cloud Extender Windows Server needs to grant access for the ARX Proxy user to have Local Backup Operator privileges.

◆ Note

Some advanced configurations may require Local Administrative rights. Refer to the F5 ARX product documentation for further details. Complete product documentation is available within the ARX GUI.

Configuring the ARX Cloud Extender Backup Operator user

The next task is to assign the F5 ARX proxy user to the **Local Backup Operator** group. This procedure is performed on the Windows Server GUI on which the F5 ARX Cloud Extender is installed.

To configure the backup operator user

1. From the Windows Server interface on which the Cloud Extender is installed, run the Computer Management application: From the **Start** menu, select **Administrative Tools** and then click **Computer Management**.
2. From the left navigation pane, expand **System Tools**, then **Local Users and Groups**, and then click **Groups**.
3. In the right pane, double-click **Backup Operators**. The Backup Operators Properties box opens.
4. Click the **Add** button.

-
5. In the **Enter Object names to select** section, type the user name of the F5 ARX Proxy User, and then click **Check Names**.
In our example, we type the Domain User **proxyuser**.
Domain Control user credentials may be required.
 6. If prompted, type the Domain Control user name with permissions to browse the user lists, and then Click **OK**. Select the user from the list and then click **OK**.
The Backup operator properties dialog opens with the user we just added in the list.
 7. Click **OK** to continue.

Configuring the ARX Cloud Extender Connectors

The Cloud Extender Connectors are software components that allow the F5 ARX Cloud Extender to store files in the storage provider cloud. The currently supported public cloud storage providers are Amazon S3, EMC Atmos, and AT&T Synaptic. For private cloud on premise deployments an NFS export can be used as a secondary storage target.

- For Amazon S3, see *Configuring the Cloud Extender for Amazon S3*
- For EMC Atmos, see *Configuring the Cloud Extender for EMC Atmos*, on page 9

Configuring the Cloud Extender for Amazon S3

The Amazon S3 cloud storage is managed in a concept of Buckets. Each Bucket represents a file space that is much like a file server shared folder. In this section the F5 ARX Cloud Extender S3 Configuration tool is used to create a new storage bucket within the Amazon S3 cloud storage account.

◆ Important

Do not create the Amazon S3 bucket with the Amazon Web access. The ARX Cloud extender does not support certain character types that the Amazon S3 Web portal would allow the user to improperly define.

To configure the Cloud Extender S3 plugin for bucket management

1. Launch the Cloud Extender S3 Plugin Configuration utility (from the **Start** menu, select **All Programs-->F5 ARX Cloud Extender--> ARX CE Connector Configurator--> F5 S3 Config**).
The Configuration box opens.
2. From the **File** menu, click **Open**, and navigate to the **S3.cfg** file location.
Note: This file was generated when the F5 ARX Cloud Extender was

installed and configured. The file should exist in the C:\Program Files\F5 ARX CE Agent directory path.

The Amazon Web Services Access Key ID and Secret Key loads.

3. Click **Manage Buckets** to manage the S3 Buckets.
The list of S3 Buckets is presented.

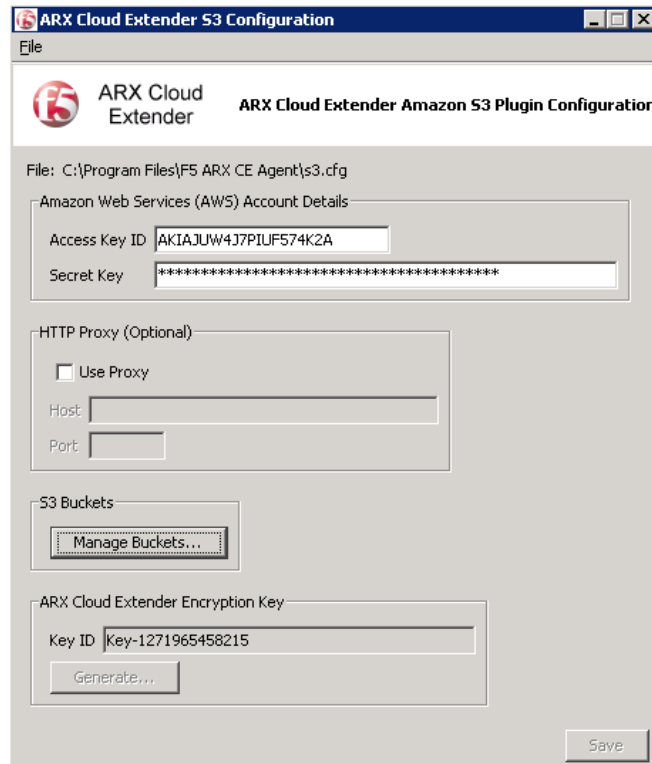


Figure 2 ARX Cloud Extender S3 configuration utility

4. Click the **New** button to create a new bucket.
5. In the box, type a bucket name and then click **OK**. In our example, we type **cloud-extender-bucket1**.
6. Select a Bucket Location appropriate for your location. In our example, we select **US Standard**. Make sure you select a location in which you can legally tier your files, there may be compliance issues in some locations.
7. Click **OK** to complete the creation. The Bucket appears in the list. This bucket data is used in *Configuring the ARX Cloud Extender storage destination*, on page 12.

Configuring the Cloud Extender for EMC Atmos

The EMC Atmos and AT&T Synaptic cloud storage access is managed by the Cloud Connector Configurator. The Configuration parameters are specific to each cloud provider. This section will cover the steps to utilize an AT&T Synaptic cloud storage implementation. AT&T Synaptic is built with EMC Atmos technology.

◆ Note

Follow the instructions provided in Chapter 5 of the F5 ARX Cloud Extender product documentation to install the EMC Atmos Cloud Connector plugin prior to attempting these steps.

To configure the Cloud Extender for Atmos

1. Launch the Cloud Extender Atmos Configuration utility (from the **Start** menu, select **All Programs-->F5 ARX Cloud Extender-->ARX CE Connector Configurator--> F5 ARX CE Atmos Connector Configuration**).

The Configuration box opens.

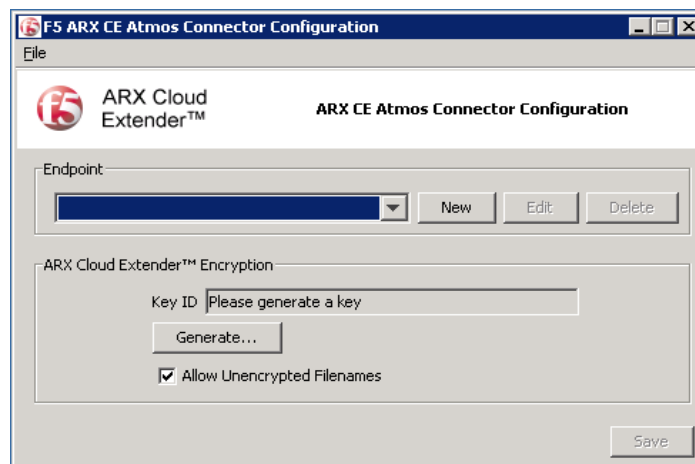


Figure 3 Cloud Extender Atmos Connector Configuration

2. In the Endpoint section, click the **New** button. The Endpoint is the HTTPS server at the cloud provider.
3. In the box for the Endpoint URI, type the URI in the format **http://<hostname>/rest**. In our example, we configure AT&T Synaptic Cloud Service, so we type **https://storage.synaptic.att.com/rest**

Click **OK**. The Atmos Authentication Details dialog displays.

4. *Optional:* If your configuration requires an HTTPS proxy, check the **Use Proxy** box, and then type the **Host** and **Port** in the boxes.

5. In the Credentials section, next to **Subtenant ID**, click the **New** button to create a new Subtenant ID. In the box, type the Subtenant ID. This ID is a unique integer, and for some providers is also the Customer ID. Click **OK**.
6. Click the **New** button next to **Application IDs** to create a new Application ID. The Shared Secret box opens.
7. In the **Secret Key** box, type the Secret Key for the Application ID and then click **OK**. You return to the Atmos Authentication Details page.

Tip: The **Get URI** button in the Application ID section is a convenient way to get an example of the URI for this storage location. This URI is referenced when you define the Destination Location for Atmos on page 13.

Figure 4 Atmos Authentication Details

8. On the Atmos Authentication Details page, click **OK** to return to the Connector Configurator main page.
9. On the Atmos Configurator main page, in the ARX Cloud Extender Encryption section, click the **Generate** button to generate an encryption key.
10. Type a valid passphrase and then click **OK**.

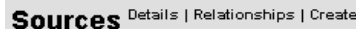
-
11. The Configurator requires the details are physically printed (this can be printed from a printer, as a PDF, MS XPS driver and so on). Click **OK** to continue. The printout contains a validation code.
 12. In the Validation Code box, type the validation code found on the printout. Click **OK**.
 13. From the File tab, click **Save** to save the **atmos.cfg** file. This file is saved to the **C:\Program Files\F5 ARX CE Agent** subdirectory

Defining the Source Location

The F5 ARX Cloud Extender needs a CIFS share defined to which F5 ARX connects. This CIFS share is defined as the source location for files intended to be migrated to the Cloud Storage Provider. Sources are locations (folders) on the network from where Operations may be performed. When describing the Source location, the server and starting folder is a URI location.

To define the Source Location

1. Log onto the ARX Cloud Extender user interface. This can be found using the following path: *Start->All Programs-> F5 ARX Cloud Extender->ARX CE Admin Tools->F5 ARX CE Control Panel*
The home page of the Cloud Extender opens.
2. Next to **Sources**, click **Create** to create a new Source definition.



Sources Details | Relationships | Create

Figure 5 Create Source Hyper link

3. In the **Name** box, type a name. In our example, we type **Source_Dir**. You can optionally type a **Description** for this source definition. In our example the source directory location is on the server named **w2k3-7**. The subdirectory created and shared in section *Creating the source CIFS share*, on page 5 is the source location.
4. In the URI section, perform the following:
 - a) Click **win**. win appears in the URI box.
 - b) Type the Server Name (do not use the IP address alone) and then click **Go**.
A list of Drive letters opens.
 - c) Click a Drive letter, and then click **Go**. In our example, we select **E:**. The URI box updates, and a list of directories opens.
 - d) Select the directory you created in *Creating the source CIFS share*, on page 5. In our example, we select **Cloud_Source**.

e) Click **Save**.

◆ Important

Only refer to the Server Names as their DNS resolvable names. ARX Cloud Extender does not support IP Addresses to be used as the server name.

Figure 6 Source location configuration.

5. Click **Save** to continue. You have now defined the Source location which appears below Sources.

Configuring the ARX Cloud Extender storage destination

The storage destination configuration defines the cloud storage configuration for storing files and directories. This can be an on premise deployment for a private cloud via NFS, or a public cloud provider as in Amazon S3 and EMC Atmos. This section describes how to configure Amazon S3, EMC Atmos, or NFS as a destination storage location.

Defining the Destination Location for Amazon S3

ARX Destinations are locations on the network to where files are copied, moved or migrated. A Destination is a single folder on a single server. When describing the Destination location, the server and folder is a URI.

To create a new destination entry for Amazon S3

1. From the Cloud Extender user interface, click **Create** next to **Destinations**.
2. In the **Name** box, type a name. In our example, we type **Cloud_Storage_Provider-s3**. You can optionally type a description.

-
3. In the URI section, complete the following:
 - a) select **s3** for the Amazon S3 Destination.

Destination only schemes:


 s3 Amazon S3 (via ARX CE Gateway)

Figure 7 Destination provider

- b) Type the appropriate URI. The URI is comprised of the IP address or FQDN of the server where the S3 Plugin was configured (*Configuring the Cloud Extender for Amazon S3*, on page 7). In our example, the Plugin was installed on the server named **w2k3-7** and the S3 Bucket created was **cloud-extender-bucket-1**, so we type **s3://w2k3-7/cloud-extender-bucket-1**
 - c) Click **Go**.

◆ WARNING

Do not install or configure IPv6 on the Servers executing the F5 ARX Cloud Extender Services. Task Log messages will report that the Plugin is not reachable by the gateway agent.

4. Click **Save** to continue. The new Destination appears under the word **Destinations**.

Defining the Destination Location for EMC Atmos

In this section, we configure the Destination to be EMC Atmos. ARX Destinations are locations on the network to which files are migrated and demigrated. A Destination is a single folder on a single server. When describing the Destination location, the server and folder is a URI

To create a new destination entry for EMC Atmos

1. From the Cloud Extender user interface, click **Create** next to **Destinations**.
2. In the **Name** box, type a name. In our example, we type **Cloud_Storage_Provider-atmos**. You can optionally type a description.
3. In the URI section, complete the following:
 - a) select **atmos** for the Atmos Destination.

Destination only schemes:


 atmos EMC² Atmos™ (via ARX CE Gateway)

Figure 8 Destination provider

- b) Type the appropriate URI. The URI is comprised of the IP address or FQDN of the server where the EMC Atmos cloud extender connector was configured (*Configuring the Cloud Extender for EMC Atmos*, on page 9).

The URI Format is:

```
atmos://{gateway}/[{{subtenant ID}@}{host}[:{port}]/{App ID}/{pool}
```

Where:

gateway is the name of the system running the ARX CE Connector agent/gateway.

Subtenant ID is the Atmos subtenant ID supplied by the cloud provider.

Host is the hostname serving the cloud provider.

Port is an optional protocol port value the service is listening on (default 443).

App ID is provided by the storage provider and is also known as a User ID and is supplied by the cloud provider.

Pool is the storage pool created within the Application ID context and stores the data (default pool is named DEFAULTPOOL).

For more information see Chapter 5 of the ARX CE product documentation.

In our example, the Plugin was installed on the server named **w2k3-4**, so we type `atmos://w2k3-4/<Subtenant ID>@storage.synaptic.att.com/test/DEFAULTPOOL`

◆ WARNING

Do not install or configure IPv6 on the Servers executing the F5 ARX Cloud Extender Services. Task Log messages will report that the Plugin is not reachable by the gateway agent.

4. Click **Go**.
5. Click **Save** to continue. The new Destination appears under the word **Destinations**.

Defining the Destination Location for NFS

Use the procedure in this section if you are using NFS as the provider for the cloud storage destination.

ARX Destinations are locations on the network to where files are copied, moved or migrated. A Destination is a single folder on a single server. When describing the Destination location, the server and folder is a URI.

To create a new destination entry for NFS

1. From the Cloud Extender user interface, click **Create** next to **Destinations**.

-
2. In the **Name** box, type a name. In our example, we type **Cloud_Storage_Provider-nfs**. You can optionally type a description.
 3. In the URI section, complete the following:
 - a) select **nfs** for the Destination.



Figure 9 Destination provider

- b) Type the appropriate URI. The URI is comprised of the FQDN of the server where an NFS export is present. Support for NFS destinations is native to the Cloud Extender. Unlike Public Cloud support, NFS support does not require a plugin to be installed. For this example we type **nfs://nfs-server1/vol/vol0** as FQDN of the NFS Server.
 - c) Click **Go**.
 4. Click **Save** to continue. The new Destination appears under the word **Destinations**.

Creating a Rule

Rules are collections of criteria that determine if a file is part of a copy, move or migrate operation, and are applied to each file located in the Source. If the Rules match, the operation is performed on the file.

Rules can be Simple or Compound, which are a combination of many simple rules. In this section, we create a simple rule which will match all files from the source definition.

To create a new rule

1. From the Cloud Extender user interface, click **Create** next to **Rules**.
2. Click **Simple Rule**.
3. In the **Name** box, type a name. We type **All-Files**. You can optionally type a Description.
4. Leave the **Combine Logic** list at default, **Filter (AND)**.
5. From the File Matching section, in the **Patterns** box, type *. This will match all files in the directory.
6. For this rule, we leave the **Date Matching** settings at the default. Note that it is possible to restrict the file matching criteria to a set of files that span a period of time or by age.
7. For this rule, we leave the **Owner Matching** settings at the default. Note that you can base file matching criteria on file ownership.

8. For this rule, we leave the **Attribute State Matching** settings at the default. You can base file matching criteria on file attribute state.
9. Click **Save**. The rule is created and appears on the main configuration page.

Creating a Policy

Policies are management plans for files on your network. A Policy contains the Rules to apply to a Source, the operation to perform on these files (such as Copy, Move, Migrate, and so on), and the Destination location for the files that match the Rules. In this guide we create a Migrate Operation. The Migration policy copies the files that match the rule to the Cloud Provider (Destination). Once the file is copied to the cloud, the local file is replaced with a stub file and the file attributes are marked to set the Offline bit.

To create a new policy

1. From the Cloud Extender UI, click **Create** next to **Policies**.
2. In the **Name** box, type a name. We type **Migrate_Policy**. You can optionally type a Description.
3. From the **Operation** list, select **Migrate**.

◆ Important

Only the Migration or DeMigrate Operations are qualified and supported by the F5 ARX.

The next section is split into two sections. The list of available Rules versus selected rules.

4. Double-click the name of the rule you created in *Creating a Rule*, on page 15 to move it to the **Selected** list. We double-click **All-Files**.
5. In the Sources section, double-click the Source Location you created in *Defining the Source Location*, on page 11 to move it to the **Selected** list. In our example we click **Source_Dir**. This is where the files are migrated from. The source directory is moved to the **Selected** list.
6. In the Destination section, from the **Root** list, select either the Amazon S3, EMC Atmos or NFS destination you defined in *Configuring the ARX Cloud Extender storage destination*, on page 12. In our example, we select **Amazon**.
7. Click **Save**.

Creating a Task

Tasks are the jobs that execute the Policies. You can schedule them to run at a specific time, use a Run Now feature to execute them immediately, or you can use a Run Now (Simulate) feature to simulate the running of the Task. In the following procedure, we create a task that invokes the **Migrate Policy** and is allowed to run anytime of the day.

To create a new task

1. From the Cloud Extender user interface, click **Create** next to **Tasks**.
2. In the **Name** box, type a name. We type **Migrate_Task**. You can optionally type a Description.
3. Double-click the Policy you created in *Creating a Policy*, on page 16 to move it to the Selected list. In our example, we select **Migrate_Policy**.
4. In the Schedule section, click to check the **Enable** box, and then configure a schedule. In our example, we allow the task to run anytime of the day, so in the **Time Spec** box, we type ********* (see Figure 10, on page 17).
5. Click **Save**.

Schedule

Enable:

| Min | Hour | Day | Month | DoW |
|-----|------|-----|-----------|-----------|
| 00 | 11 | 19 | January | Sunday |
| 05 | 12 | 20 | February | Monday |
| 10 | 13 | 21 | March | Tuesday |
| 15 | 14 | 22 | April | Wednesday |
| 20 | 15 | 23 | May | Thursday |
| 25 | 16 | 24 | June | Friday |
| 30 | 17 | 25 | July | Saturday |
| 35 | 18 | 26 | August | |
| 40 | 19 | 27 | September | |
| 45 | 20 | 28 | October | |
| 50 | 21 | 29 | November | |
| 55 | 22 | 30 | December | |
| | 23 | 31 | | |

Hint: use shift/ctrl for multiple selection

Time Spec:

Hint: press Tab to update graphical display

Figure 10 Task schedule

You return to the main configuration page. Notice the **Migrate_Task** is displayed under the Tasks keyword. This schedule has the F5 ARX Cloud Extender evaluate files in the source directory approximately every five minutes.

This completes the Cloud Extender configuration. Continue with the next section to configure the ARX.

Configuring the F5 ARX

In this section, we configure the F5 ARX to access the F5 ARX Cloud Extender for a tiering configuration that migrates files to the cloud service provider. A CIFS namespace has already been configured with a managed volume and at least one CIFS share used as Tier 1 storage. The shares are incorporated into a managed volume with a file placement policy. As files age and are not modified for more than 30 days, they are moved between these shares depending upon the file last modified time.

In this section we configure the following:

1. *Disabling Sparse File Support*, on page 18
2. *Adding the External Filer*, on page 19
3. *Adding the Cloud Extender Share to the volume*, on page 19
4. *Creating the File Placement Policy*, on page 21
5. *Connecting to the Virtual Service*, on page 25

Prerequisites

The F5 ARX in this example has an existing configuration. Our configuration contains the following objects:

- CIFS only Namespace: **Cloud**
- Managed Volume: **/vol**
- Tiered Storage (created and added to the Volume): **Tier1**
- Root Level Share: **\\server1\cloud1**
- Virtual Service: **\\clouddemo.siterequest.com\cloud_demo**
- ARX Proxy User: **proxyuser**

If you have not already configured these objects on the ARX, see the ARX documentation on creating them before continuing the remainder of this guide.

Disabling Sparse File Support

The F5 ARX and F5 ARX Cloud Extender do not support the *Sparse File* feature in the F5 ARX Managed Volume.

To disable Sparse File support

1. From the left navigation pane, expand **Managed Volumes**.
2. Click the appropriate volume. In our example, we click **/vol**.
3. Click the **Edit** button.

-
4. Click to uncheck the **Sparse Files** box.
 5. Click **OK**. Sparse files are now disabled.

Adding the External Filer

The next task is to add the F5 ARX Cloud Extender as an external filer. This entry is referenced later when we add the filer share 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 **F5-ARX-Cloud-Extender**.
4. In the **Primary IP Address** box, type the primary IP address of the ARX Cloud Extender.
5. In the **Description** box, you can optionally type a description.
6. The rest of the settings are optional. You can, for example, configure the ARX to limit the total number of simultaneous CIFS Connections to the external filer.
7. Click the **Save** button. The File Server Summary page displays.

Adding the Cloud Extender Share to the volume

Next, we add the F5 ARX Cloud Extender share to the volume.

To add the 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 **Cloud_Storage**.
4. From the **Namespace** list, select the name of the namespace that you had already configured. In our example, we select **Cloud**.
5. From the **Volume** list, select the name of the Volume that you had already configured. In our example, we select **/vol**.
6. Click the **Next** button.

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

Share name:


Replica Snapshot: Replica snapshot share.

Namespace:

Volume:

Figure 11 Share Name definition

7. From the **File Server** list, select the External Filer you added in *Adding the External Filer*, on page 19. In our example, we select **F5-ARX-Cloud-Extender**.
8. In the **CIFS Share** box, type the name of the CIFS share. In our example, the server is the F5 ARX Cloud Extender and the CIFS Share is **Cloud_Source**.
9. Click **Next** to continue.
10. On the Share options page, check the **Rename files with naming collisions on import** and **Synchronize directory attributes between shares on import** boxes.
If this share had previously been apart of another F5 ARX Managed Volume, also select **Allow this switch to import this share, even if it is owned by another ARX** (see Figure 12).
11. Click the **Next** button.
12. Review the summary, and click the **Finish** button.

Select the options you would like this share to have. 

Share name: Cloud_Storage
Import Priority:

Import Conflict Resolution

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

Local Groups

Share contains local groups
 Ignore SID errors

Enable Share

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

Figure 12 Share Options

Once the Cloud Extender share has been added to the Volume, verify the share status. The Managed Volume Details reports the share status. Figure 13 shows the root level share is **online** and the newly added share is **Importing**.

Managed Volume Details

Namespace: Cloud Volume: /vol

Volume Shares

Add... Remove... Edit... Enable Disable Sync...

| Share | File Server | File Server Path | Free Space | Import Priority | Transitions | Status |
|--|-------------------------------------|------------------|------------|-----------------|-------------|----------|
| <input type="checkbox"/> Cloud Storage | F5-ARX-Cloud-Extender 10.10.10.2 | Cloud_Source | 1.9 G | 65535 (Lowest) | 1 | ● Online |
| <input type="checkbox"/> Tier1 | Server1 10.10.10.1 | cloud1 | 95 G | 65535 (Lowest) | 1 | ● Online |

Figure 13 Manage Volume Details: Share list

Creating the File Placement Policy


A file placement policy rule is assigned to a managed volume. It facilitates file movement between backend file shares based on file attributes. The files can be placed based on modified time, last access time, file name, and applied as a scheduled event. The ARX periodically (on schedule) will scan the metadata store and check for policy matches. If a match is located the ARX will process the rule and move 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 F5 ARX Cloud Extender which sends the files to the Cloud Storage Provider. The policy is enumerated every day at 1AM.

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 **Cloud_Tier**.
4. From the **Namespace** list, select the name of the namespace you created previously. In our example, we select **Cloud**.
5. From the **Managed volume** list, select the name of the Volume you created previously. In our example, we select **/vol**.
6. From the **Number of tiers** list, select a number of tiers. In our example, we select **2**.

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.



Policy name prefix:

Namespace:

Managed volume:

Number of tiers:

Figure 14 Creating a new 2 Tier Storage Policy

7. Click the **Next** button.
8. For Tier 1, select the Tier 1 file share. In our example, we select **Tier1**. Click the **Next** button.
9. For Tier 2, select the Tier 2 file share that you created in *Adding the Cloud Extender Share to the volume*, on page 19. In our example, we select **Cloud_Storage**.
10. Click the **Next** button.
11. The next step is to specify the criteria for moving files between the Tiers, and to define the schedule. Click the **Add** button to the right of Schedule to define the schedule to associate with the policy.
 - a) In the **Schedule Name** box, type a name for this schedule. In our example, we type **At_1AM**.
 - b) In the **Start Time** fields, you can specify a specific start time.
 - 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 (see Figure 15, on page 23). You return to the Tiered Storage Wizard.

| | |
|----------------------|---|
| Schedule Name | At_1AM |
| Description | Everyday at 1AM |
| Start Time | <input checked="" type="checkbox"/> Specify start time. <input type="text" value="13"/> / <input type="text" value="10"/> / <input type="text" value="2010"/> - <input type="text" value="01"/> : <input type="text" value="00"/> <small>Day Month Year Hour Minute</small> |
| Stop Time | <input type="checkbox"/> Specify stop time. <input type="text" value="18"/> / <input type="text" value="10"/> / <input type="text" value="2010"/> - <input type="text" value="14"/> : <input type="text" value="53"/> <small>Day Month Year Hour Minute</small> |
| Interval | <input checked="" type="radio"/> Every <input type="text" value="1"/> days <input type="radio"/> Weekdays Frequency <input type="text" value="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 <input type="text" value="00"/> <input type="button" value="Add"/> 01:00 Minute <input type="text" value="00"/> <input type="button" value="Remove"/> |
| Run Duration | <input type="checkbox"/> Specify run duration. <input type="text" value="0"/> : <input type="text" value="0"/> <small>Hour Minute</small> |

Figure 15 Policy Schedule

12. Optionally a fileset can be defined. A fileset restricts this policy to certain file types. In our example, we create a fileset by performing the following:
 - a) Click the **Add** button to create a fileset. In this example, we want to match all files.
 - b) In the **Name** box, type a name. In our example, we type **All_Files**.
 - c) From the Fileset type, select a type. We select **filename**.
 - d) In the Filename Matching Criteria section, we click **Wildcard Expression**, and then type * in the box.
 - e) Click Save to return to the Tiered Storage Wizard (see Figure 16, on page 24).

Create a new fileset.

Fileset Name:

Fileset Type:

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:

Exclude Path:

Ignore Case for Path:

Recurse Subdirectories:

Figure 16 Fileset Definition

13. On the Criteria for moving files between tiers page, from the Schedule list, select the Schedule you created. In our example, we select **At_1AM**.
14. From the **Move files not** list, select **modified**. In the **in the last** box, type a number, and from the list, select an option. In our example, we type **30** and select **Days**.
15. In the Options box, from the **Fileset** list, select the fileset you just created. In our example, we select **All_Files**.
16. Within the Tiered Storage Wizard select the Schedule **At_1AM** and the fileset to be **All_Files**.
17. Click **Next** to continue (see Figure 17, on page 25).

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

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

Move files not in the last days

Schedule:

Options

Fileset (optional):

Generate reports

Enable

Enable this policy when finished
 Enable tentative

Figure 17 Policy Criteria

18. Review the Summary and then click **Finish**.
19. On the left Navigation pane of the GUI, expand the **Policy** and then click **Place Rules**.
 The two policies that were created using the wizard display. The first policy is for migrating files to Tier-2 and the second policy is for moving files back to Tier-1 if they have a last modified time less than 30 days.

Place Rule Summary

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

Namespace: Volume:

| <input type="checkbox"/> | Rule | Volume | Namespace | Precedence | From | To | Admin State | Status |
|--------------------------|---|--------|-----------|------------|---|---------------------------------------|-------------|-------------------------------------|
| <input type="checkbox"/> | Cloud_Tier_tier-1-Tier1 | /vol | Cloud | 1 | Cloud_Tier_tier-1 (fileset) | Tier1 (share) | Enabled | Scan: Complete Migrate: Complete |
| <input type="checkbox"/> | Cloud_Tier_tier-2-Cloud Storage | /vol | Cloud | 2 | Cloud_Tier_tier-2 (fileset) | Cloud Storage (share) | Enabled | Scan: Complete Migrate: Complete |

Figure 18 Placerule Summary

Connecting to 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 backend filer. The Virtual

service was already configured on the F5 ARX as a prerequisite. To review the Virtual Service settings click **Virtual Services** in the left navigation pane.

Virtual Service Summary

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

| | Domain Name | Virtual IP | VLAN | Exports | Domain Join | Admin State | Status |
|--------------------------|---|------------------------------|------|---------|--|---------------|-------------|
| <input type="checkbox"/> | clouddemo.siterequest.com | 10.10.10.10 255.255.255.0 | 301 | | 1 Joined to siterequest.com Delegation: Unconstrained, Kerberos Only | CIFS: Enabled | CIFS: Ready |

Figure 19 Virtual Service Summary

In our example, the FQDN is **clouddemo.siterequest.com** at IP address **10.10.10.10** and it is joined to the domain.

The next task is to map a network drive.

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 **X**.
3. 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 **\\clouddemo.siterequest.com\cloud_demo**.
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. Click OK.
5. Click **Finish**. Windows explorer opens the new network drive and displays the contents. In the F5 ARX managed volume there are several files that reside in both the Tier 1 and the Tier 2 shares.

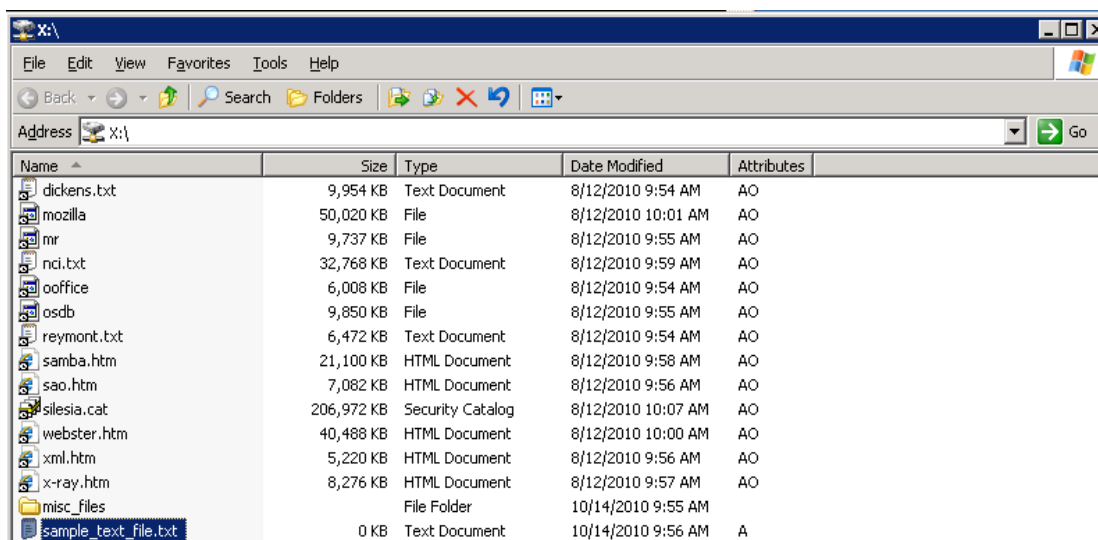


Figure 20 F5 ARX Virtual Service Managed Volume file contents

Within the list of files notice the attributes column. These files are marked with the Archive bit and some are also marked with the offline bit. The files marked as offline have been migrated to the Cloud Storage provider. When these files are accessed, the F5 ARX will proxy the file access request to the correct backend file share. When the files that are offline are accessed the F5 ARX Cloud Extender retrieves the files from the Cloud Storage Provider and serves the content to the requesting client. The file is not marked as offline after it has been recalled.



Figure 21 Recalled file attributes

The F5 ARX Cloud Extender and Cloud Storage Provider has been successfully integrated into a Managed Volume.

Storage Integration Verification

In this section, we verify that the configuration is operating properly. We use the device's management interfaces and cloud storage web portal to check on the operational status of the solution

Generating an F5 ARX Metadata Report

The F5 ARX can generate a report on the MetaData for the files that the F5 ARX is storing. This report identifies which back end file shares files and folders are located.

To create an ARX Report

1. From the left navigation pane, click **Managed Volumes**.
2. Click on the Managed Volume **/vol**.
3. Click the **Report** button.
The Report Volume screen opens.
4. In the **Path** box, you can type a path.
In our example, we leave the path 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 **Test_Report**.
7. From the **Share** list, select the **Cloud_Storage** share.
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 **Test_Report**. The Report opens in a new browser window or tab.
In our example, the report looks like the following:

```
**** Metadata-Only Report: Started at Thu Oct 14 11:22:12 2010 ****
**** Software Version: 5.02.000.12635 (Oct 8 2010 22:09:29) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: Cloud
**** Volume: /vol
**** Path: /vol
**** Share: Cloud_Storage
```

```
Share                Physical Filer
-----
[Cloud_Storage      ] 10.10.10.2:Cloud_Source
```

```
**** 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.
**** IA = Inconsistent attributes between this directory's master and stripes
(recorded).
**** IS = Inconsistent attributes on this specific directory stripe (recorded).

```

| Type | Share | Path |
|------|------------------|----------------|
| [FL |] [Cloud_Storage |] /mozilla |
| [FL |] [Cloud_Storage |] /dickens.txt |
| [FL |] [Cloud_Storage |] /nci.txt |
| [FL |] [Cloud_Storage |] /x-ray.htm |
| [FL |] [Cloud_Storage |] /ooffice |
| [FL |] [Cloud_Storage |] /samba.htm |
| [FL |] [Cloud_Storage |] /webster.htm |
| [FL |] [Cloud_Storage |] /mr |
| [FL |] [Cloud_Storage |] /reymont.txt |
| [FL |] [Cloud_Storage |] /silesia.cat |
| [FL |] [Cloud_Storage |] /osdb |
| [FL |] [Cloud_Storage |] /xml.htm |
| [FL |] [Cloud_Storage |] /sao.htm |

```

**** Total Files: 13
**** Total Directories: 0
**** Total Hard Links (nlink>1): 0
**** Total Symlinks: 0
**** Total Locking Errors: 0

**** Total items: 13
**** Elapsed time: 00:00:00
**** Metadata-Only Report: DONE at Thu Oct 14 11:22:12 2010 ****

```

Figure 22 F5 ARX Cloud Extender Tier Metadata report

Repeat this procedure, but this time, in Step 7 select the Tier 1 share.
For the Tier 1 share, our report looks like the following:

```

**** Metadata-Only Report: Started at Thu Oct 14 11:33:08 2010 ****
**** Software Version: 5.02.000.12635 (Oct 8 2010 22:09:29) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: Cloud
**** Volume: /vol
**** Path: /vol
**** Share: Tier1

```

| Share | Physical Filer |
|--------|---------------------|
| [Tier1 |] 10.10.10.1:cloud1 |

```

**** 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.
**** IA = Inconsistent attributes between this directory's master and stripes
(recorded).
**** IS = Inconsistent attributes on this specific directory stripe (recorded).

```

| Type | Share | Path |
|------|----------|-------------------------|
| [FL |] [Tier1 |] /sample_text_file.txt |
| [DR |] [Tier1 |] /misc_files |

```

**** Total Files: 1
**** Total Directories: 1
**** Total Hard Links (nlink>1): 0
**** Total Symlinks: 0
**** Total Locking Errors: 0

**** Total items: 2
**** Elapsed time: 00:00:00
**** Metadata-Only Report: DONE at Thu Oct 14 11:33:08 2010 ****

```

Figure 23 Tier-1 Metadata report

Reviewing these two reports shows that files exist in both tiers of storage. Most of the files are residing within the F5 ARX Cloud Extender external filer.

Viewing the status of the F5 ARX Cloud Extender

The web interface of the F5 ARX Cloud Extender has a section for Running Tasks and Recent Task History. The running tasks area reports tasks that are actively running. The Recent Task History has log files for previous tasks that were run.

Click **Details** next to one of the tasks.

Running Tasks [Details](#) | [Suspend Scheduler](#)
(live update)

Recent Task History [Details](#) | [Clear](#) | [Hide Successful](#)

Migrate_Task: Source_Dir
 Ended: 2010-10-14 12:15:59 (EDT) (time elapsed: 0h 0m 0s)
 State: Finished
 Files examined: 16 (2 dirs)
 Operations succeeded: 1 (37 bytes)
[Migrate_Task log](#) | [Task log](#)

Figure 24 Migrate Task History

The log entry for the **Migrate_Task** task is listed. The details show how long the task took to run, number of files examined, and successful operations. Click the **Migrate_Task log** link to open the log. Our log looks like the following:

```
2010-10-14 11:25:59.668 (EDT) --- LOG STARTED ---
2010-10-14 11:25:59.668 (EDT) Rule: (Filename MATCHES "**")
2010-10-14 11:26:00.121 (EDT) Migrate succeeded win://w2k3-7/E/Cloud_Source/x-ray.htm
(8474240) to s3://w2k3-7/cloud-extender-bucket-1/
2010-10-14 11:26:00.278 (EDT) Migrate succeeded win://w2k3-7/E/Cloud_Source/xml.htm
(5345280) to s3://w2k3-7/cloud-extender-bucket-1/
2010-10-14 11:26:00.449 (EDT) Migrate succeeded
win://w2k3-7/E/Cloud_Source/.acopia/.pinturaazul (37) to
s3://w2k3-7/cloud-extender-bucket-1/
2010-10-14 11:26:00.449 (EDT) --- Policy 'Migrate_Policy' completed. (13819557)
2010-10-14 11:26:00.449 (EDT) Summary: Files examined: 16, dirs examined: 2, max. dir
depth: 1, operations succeeded: 3, operations failed: 0, operations skipped: 0, operations
locked: 0
```

Figure 25 Task Log example

This log entry is a simple task log that ran and migrated a few files. Each file that was migrated is reported in the log and marked as Succeeded. Failures are also reported when they exist.

Viewing Cloud Provider Status

In our example, we chose to use Amazon S3 as the Cloud Storage Provider. Amazon's web services portal has the ability to browse to the file stored in the S3 cloud as well as generate usage reports.

In this section, we generate a usage report to ensure the migrated files are accounted for in the S3 cloud storage bucket.

For other cloud providers, follow the vendor specific instructions to query account details.

To view the Amazon S3 status

1. Login into the Amazon S3 web services portal.
2. Click the **Account** link to bring up the account details.
3. Click **Usage Reports**.
4. From the **Service** list, select the service **Amazon Simple Storage Service**.
5. From the **Usage Type** list, select **APS-1 Data Transfer in Bytes** or **All Operations**.
6. Click the **Download Report** button. The .CSV file is downloaded and can be viewed in Microsoft Excel or in a text editor.

Service: Amazon Simple Storage Service

Usage Types: AFS1-DataTransfer-In-Bytes (What's this?)

Operation: All Operations

Time Period: Current billing period

Report Granularity: Hours

Download report (XML) Download report (CSV)

Figure 26 Usage Report generation screen

In our example, the following snippet of data was taken from the usage report for **All Operations**.

| | A | B | C | D | E | F | G |
|-----|----------|-----------|------------------------|-------------------------|-----------------|------------------|------------|
| 1 | Service | Operation | UsageType | Resource | StartTime | EndTime | UsageValue |
| 227 | AmazonS3 | GetObject | Requests-Tier2 | cloud-extender-bucket-1 | 10/14/2010 5:00 | 10/14/2010 6:00 | 18 |
| 228 | AmazonS3 | PutObject | Requests-Tier1 | cloud-extender-bucket-1 | 10/14/2010 5:00 | 10/14/2010 6:00 | 12 |
| 229 | AmazonS3 | GetObject | DataTransfer-Out-Bytes | cloud-extender-bucket-1 | 10/14/2010 5:00 | 10/14/2010 6:00 | 3744 |
| 230 | AmazonS3 | PutObject | DataTransfer-In-Bytes | cloud-extender-bucket-1 | 10/14/2010 5:00 | 10/14/2010 6:00 | 3456 |
| 231 | AmazonS3 | GetObject | Requests-Tier2 | cloud-extender-bucket-1 | 10/14/2010 6:00 | 10/14/2010 7:00 | 18 |
| 232 | AmazonS3 | PutObject | Requests-Tier1 | cloud-extender-bucket-1 | 10/14/2010 6:00 | 10/14/2010 7:00 | 12 |
| 233 | AmazonS3 | GetObject | DataTransfer-Out-Bytes | cloud-extender-bucket-1 | 10/14/2010 6:00 | 10/14/2010 7:00 | 3744 |
| 234 | AmazonS3 | PutObject | DataTransfer-In-Bytes | cloud-extender-bucket-1 | 10/14/2010 6:00 | 10/14/2010 7:00 | 3456 |
| 235 | AmazonS3 | PutObject | DataTransfer-In-Bytes | cloud-extender-bucket-1 | 10/14/2010 7:00 | 10/14/2010 8:00 | 3456 |
| 236 | AmazonS3 | GetObject | Requests-Tier2 | cloud-extender-bucket-1 | 10/14/2010 7:00 | 10/14/2010 8:00 | 18 |
| 237 | AmazonS3 | PutObject | Requests-Tier1 | cloud-extender-bucket-1 | 10/14/2010 7:00 | 10/14/2010 8:00 | 12 |
| 238 | AmazonS3 | GetObject | DataTransfer-Out-Bytes | cloud-extender-bucket-1 | 10/14/2010 7:00 | 10/14/2010 8:00 | 3744 |
| 239 | AmazonS3 | GetObject | DataTransfer-Out-Bytes | cloud-extender-bucket-1 | 10/14/2010 8:00 | 10/14/2010 9:00 | 3744 |
| 240 | AmazonS3 | PutObject | DataTransfer-In-Bytes | cloud-extender-bucket-1 | 10/14/2010 8:00 | 10/14/2010 9:00 | 3456 |
| 241 | AmazonS3 | GetObject | Requests-Tier2 | cloud-extender-bucket-1 | 10/14/2010 8:00 | 10/14/2010 9:00 | 18 |
| 242 | AmazonS3 | PutObject | Requests-Tier1 | cloud-extender-bucket-1 | 10/14/2010 8:00 | 10/14/2010 9:00 | 12 |
| 243 | AmazonS3 | GetObject | Requests-Tier2 | cloud-extender-bucket-1 | 10/14/2010 9:00 | 10/14/2010 10:00 | 18 |
| 244 | AmazonS3 | PutObject | Requests-Tier1 | cloud-extender-bucket-1 | 10/14/2010 9:00 | 10/14/2010 10:00 | 12 |
| 245 | AmazonS3 | GetObject | DataTransfer-Out-Bytes | cloud-extender-bucket-1 | 10/14/2010 9:00 | 10/14/2010 10:00 | 3744 |
| 246 | AmazonS3 | PutObject | DataTransfer-In-Bytes | cloud-extender-bucket-1 | 10/14/2010 9:00 | 10/14/2010 10:00 | 3456 |

Figure 27 Usage Report data

Filtering on the **cloud-extender-bucket-1** resource the report shows **PutObject** and **GetObject** traffic. This shows data is being read and written to this storage bucket.

Amazon Web Services Management Console also allows you to browse the stored data files and directory entries. To browse these files, launch the **AWS Management Console** and then click the bucket being used. In our example, we click the **cloud-extender-bucket-1** bucket (see Figure 28, on page 33).

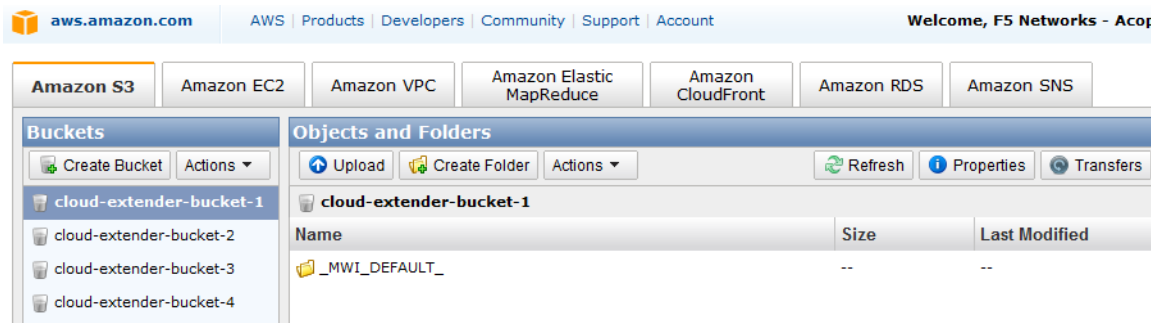


Figure 28 AWS Management Console

The F5 ARX Cloud Extender created a default directory to organize and store the files migrated to the cloud service provider.

◆ WARNING

DO NOT directly modify these files through the AWS Management Console. Only view the files. Use the F5 ARX Cloud Extender to manipulate the files. Always access the file contents managed by the F5 ARX through the virtual service interface.

Conclusion

This deployment guide demonstrated the way to integrate F5 ARX and F5 ARX Cloud Extender with Windows Storage Servers for tiering to a Cloud Storage Managed Service Provider.

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