



Deploying the F5 ARX and BIG-IP WOM for CIFS Remote File Tiering

What's inside:

- 4 Configuring the BIG-IP WOM
- 5 Configuring the WOM networking objects
- 6 Configuring the BIG-IP WOM
- 9 Configuring the ARX
- 14 Storage Integration Verification
- 18 Viewing the BIG-IP WOM Dashboard Statistics

Welcome to the F5 ARX - and BIG-IP WAN Optimization Module (WOM) deployment guide. This guide provides step by step procedures on deploying the Adaptive Resource Switch (ARX) with F5 WOM for tiering to remote file servers.

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.

See *Configuration example on page 2* for detailed information about this solution.

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

For more information on the F5 BIG-IP WOM, see <http://www.f5.com/products/big-ip/wan-optimization-module.html>

Products and versions tested

Product	Version
Microsoft Windows 2008 Storage Server	v6.0.6.001
F5 ARX	5.2.0
BIG-IP WOM	10.2.1

Prerequisites and configuration notes

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

➤ ARX prerequisites

- » The ARX is configured for network access and the initial switch interview has been completed. If this has not been completed refer to the ARX Hardware Installation guide for specific details.
- » Windows Storage Server is installed and configured for tier 1.
- » Microsoft Active Directory Domain is preconfigured.
- » An NFS Export with root access is available as an ARX Metadata store.
- » The ARX platform is deployed in redundant pairs. The secondary switch is a

Hot Standby switch. This guide addresses the configuration steps in order to integrate the Network Appliance platform with the ARX platform. Redundant switch configuration steps within the product documentation should be followed in order to deploy a high available configuration.

- » ARX managed volume and Virtual Service for CIFS is configured and available. Several F5 ARX Deployment Guides are available to assist with the initial ARX Tier 1 storage virtualization configuration details. Refer to <http://www.f5.com/solutions/resources/deployment-guides.view.products.arx.html>
- **BIG-IP WOM prerequisites:**
 - » One BIG-IP system with the WAN Optimization Module for each end of the WAN network you wish to use for WAN optimization.
 - » BIG-IP WOM hardware is installed with an initial network configuration applied. You must have two BIG-IP WOM devices that are running on one of the following platforms: 3600, 3900, 6900, 8900, or 11000.
 - » You must be running BIG-IP version 10.2.1 or later (with the same version running on each unit), and the WOM license enabled on both devices. This can be either the WOM Add-on license with the BIG-IP LTM, or the Edge Gateway license which includes WOM.
 - » You must have administrative access to both the Web management and SSH command line interfaces on the BIG-IP system.
 - » You must have an existing routed IP network between the two locations where the BIG-IP WOMs will be installed.
 - » If there are firewalls, you must have TCP port 443 open in both directions. Optionally, you can allow TCP port 22 for SSH access to the command line interface for configuration verification, but not for actual BIG-IP WOM traffic (this verification can also be performed from the Configuration utility: (Quick Start-->Diagnostics).
 - » For more configuration options on the BIG-IP WAN Optimization Module, see the Configuration Guide for BIG-IP WAN Optimization Module, available on Ask F5.

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

Configuration example

In the following diagram, we show basic connectivity between clients, ARX BIG-IP WOM and the remote file server.

We will configure a policy on the ARX that on a daily schedule 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 backend filers according to policy.

The network configuration defined in the lab used an ARX1000 with 4 Gigabit Ethernet links configured into a LACP bundle between the ARX and the core switch. The server Gig-E connections are bundled into two 4 Gig-E Smart Load Balancing connections. One bundle dedicated to client traffic, and 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 remote CIFS server is another Windows Server with a CIFS share. The access to the server is across BIG-IP WAN Optimized iSession. File Server access to the remote site is all proxied through the ARX. The Proxy IP addresses of the ARX facilitate file access and file migrations.

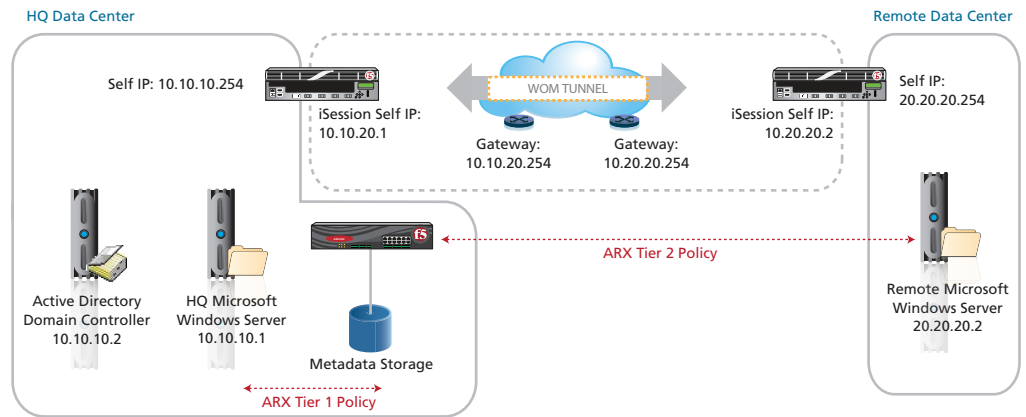


Figure 1: Logical configuration example

The examples in this guide use the IP addresses in Figure 1. Figure 2 on the next page shows the order of operations for configuring the BIG-IP WOM.

Configuring the BIG-IP WOM

The following diagram visually represents the order in which the WOM devices must be configured. You should have access to the BIG-IP WOM devices in both data centers.

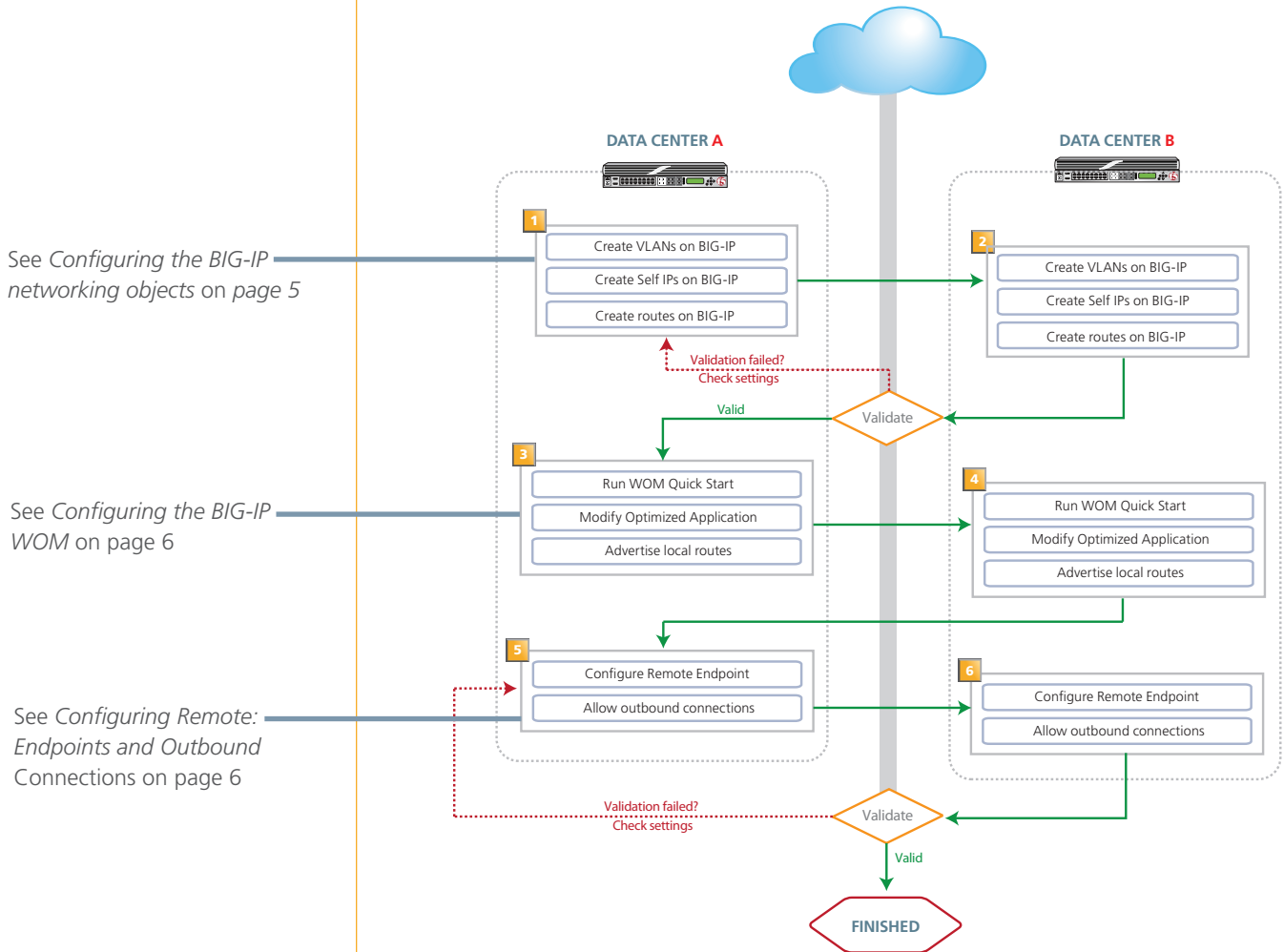


Figure 2: Order of operations

➡ **Tip** If you have enabled Auto Discovery during the Quick Start configuration, the remote endpoints and advertised routes can be discovered and populated.

Configuring the WOM networking objects

In this section, we create the networking objects on the BIG-IP systems in both data centers. Use the following table for guidance on each object. For specific information on how to configure individual objects, see the online help or product documentation.

WOM Object	Description/Notes
VLANs (Main tab--> Network-->VLANs)	We recommend at least two VLANs for WOM: a LAN VLAN and a WAN VLAN. The LAN VLAN is configured for access from the ARX Proxy IP addresses as well as the windows servers. Give each VLAN a descriptive name. Note: We find using VLAN tags makes management easier. However, tagging is not mandatory if your configuration can support individual interfaces instead of VLANs.
Self IPs (Main tab--> Network-->Self IPs)	Assign an otherwise-unused static IP address that resides on the VLAN you created. The LAN-side Self IP is used as a gateway on that network. The WAN-side Self IP is used for the WOM iSession; (we also refer to this as the Local Endpoint Self IP). Important: For the iSession VLAN only : From the Port Lockdown list, select Allow None . For all other VLANs, Port Lockdown is set to Allow Default .
Routes (Main tab--> Network-->Routes)	Create a route on BIG-IP in the primary data center to route to the BIG-IP in the secondary data center. You also need a route for the remote network where application services reside. For example, in Figure 1 the BIG-IP WOM in the HQ data center would need a route to the address 20.20.20.2 (the self IP of the remote BIG-IP) and 10.20.20.0/24 (the remote network), both using the gateway 10.10.20.254. The BIG IP in the remote data center B needs corresponding routes back to the BIG-IP and the network in the HQ data center.

Repeat the WOM networking objects in the secondary data center

Next, repeat the VLAN, Self IP and Route configuration on the BIG-IP WOM in the remote data center.

Checkpoint

Use the checkpoints to ensure the configuration thus far is working properly.

Checkpoint

At this point, you should be able to ping the local endpoint, the router, and the BIG-IP system in the secondary data center. The following requires command line or SSH access to the BIG-IP system. Consult the product documentation for instructions on how to use SSH.

- Log into the BIG-IP in the primary data center from the command line.
- Use the ping command to check the following. You should receive successful responses from each:
 - » Local endpoint - In our example, we use **ping 10.10.20.1**
 - » The router - In our example, we use **ping 10.10.20.254**
 - » The BIG-IP in the secondary data center - In our example, we use **ping 10.20.20.2**.
- Repeat this procedure in the remote data center using the appropriate IPs.

If you do not receive successful responses, check the IP addresses and VLAN configuration.

Configuring the BIG-IP WOM

The next task is to configure the BIG-IP WOM. Use the following table for guidance on any setting that is not to be left at the default for each object. For specific information on how to configure individual objects, see the online help or product documentation.

WOM Object	Description/Notes
WOM Quickstart (Main tab--> WAN Optimization-->Quick Start)	<p>WAN Self IP Address: Self IP address for the Local Endpoint (iSession)</p> <p>Discovery: Enabled</p> <p>LAN VLAN: Select the VLAN that corresponds to the local network</p> <p>WAN VLAN: Select the VLAN that corresponds to the WAN side of the network.</p> <p>Authentication and Encryption section: Leave the defaults.</p> <p>Application Security section: Configure as applicable.</p> <p>Create Optimized Applications: Check the box for Microsoft Office and Windows File Sharing.</p>
Optimized Applications (Main tab--> WAN Optimization--> Optimized Applications)	<p>Click cifs-optimized-client:</p> <ul style="list-style-type: none"> - In the Destination section, click Network. - In the Address box, type the IP address of the remote file server. - In the Netmask box, type the corresponding subnet mask.
Advertised Routes (Main tab--> WAN Optimization--> Advertised Routes)	<p>The Local subnet associated with the Internal VLAN needs to be advertised to the other WOM device</p> <p>Address: This is the IP address that specifies the local subnet. We enter the network address for the Internal VLAN: 10.10.10.0</p> <p>Netmask: The corresponding subnet mask (255.255.255.0 in our example).</p>

Repeat the WOM configuration in the secondary data center

Next, repeat the WOM Quickstart, Optimized Application and Advertised Routes configuration on the BIG-IP WOM in the secondary data center.

 **Tip**

There are a number of settings on the iSession Profile and the Application Profile that you can optionally change depending on the installation and WAN characteristics. For example, on the Application Profile, you can modify the CIFS specific optimizations for Write Behind, Read Ahead, Record and Replay, Office 2003 Extended, Fast Close, and Fast Set File Information (all enabled by default). On the iSession Profile, you can change the Deduplication, Adaptive Compression, LZ0, Deflate and Null compression settings (all enabled by default).

To access the iSession or Application profile, under WAN Optimization click **Optimized Applications**. Locate the row for the optimized application created by the quick start. The two columns at the far right are for the iSession Profile and the Application profile. Click **isession-cifs** to modify the iSession profile. Click **cifs** to modify the application profile. The online help tab contains detailed information on each setting.

You can also modify the Deduplication mode to use **Disk** or **Memory** depending on your environment (click **Symmetric Deduplication** under WAN Optimization).

Configuring remote endpoints and outbound connections

The final tasks in the WOM configuration are configuring the remote endpoints and confirming that outbound connections are allowed.

WOM Object	Description/Notes
Remote Endpoint (Main tab--> WAN Optimization-->Remote Endpoints)	IP address: The Self IP address for the BIG-IP WOM module in the remote data center (this is the iSession Self IP on the remote WOM, 10.20.20.2 in our example).
Confirming Outbound Connections are allowed (Main tab--> WAN Optimization-->Remote Endpoints)	From the Remote Endpoints section of the GUI, click the IP address of the Endpoint you created above. - Make sure there is a green circle in the left column. If it is red, there is a connectivity problem; recheck connectivity between data centers. - In the <i>Outbound iSession to WAN</i> section, make sure there is a check in the Outbound Connections box. If there is not, check the box and then click Update .

Checkpoint

Use the checkpoints to ensure the configuration thus far is working properly.

Checkpoint: Testing the configuration

At this checkpoint, we make sure that BIG-IP WOM connectivity between the primary and secondary data center is enabled. As this is a critical point in this configuration, we use two different procedures to make sure the WOM tunnel is properly configured.

To test WOM connectivity

1. From the Main tab of the BIG-IP configuration utility, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. From the list of Remote Endpoints, make sure the Status Indicator is green for the endpoint in the secondary data center.
3. If the status indicator is a color other than green, on the Main tab under WAN Optimization, and then click Diagnostics. Run through all of the troubleshooting diagnostics.

Use the following procedure to ensure that the WOM tunnel endpoints are up and running properly. For the procedure you will need SSH access to the BIG-IP.

To verify the WOM tunnel

1. Using an SSH client, like Putty, establish a connection to each BIG-IP.
2. After logging in, at the command prompt, type **b endpoint remote show all**. You should see an output similar to the following, however your host name and IP addresses will be different. Make sure you see the tunnel state as **ready, ready**.
b endpoint remote show all

```
ENDPOINT REMOTE 20.20.20.20
| HOSTNAME PRIMARYDC.example.com
| MGMT ADDR 10.1.102.61 VERSION 10.2.0
| UUID c1f3:68d6:f697:6834:108:5668:1e16:3fce
| enable STATE ready (incoming, outgoing)=(ready, ready)
```

```
| BEHIND NAT disable  
| CONFIG STATUS "none"  
| DEDUP CACHE 62380 REFRESH (count) = (0)  
| ALLOW ROUTING enable  
+--> ENDPOINT REMOTE 20.20.20.20 ROUTE 20.20.20.0/24  
| | INCLUDE enable LABEL West
```

3. SSH to the second BIG-IP and verify the tunnel status shows ready/ready.

➡ **Note:** *Only proceed with configuration after the status of the tunnel shows **ready/ready**.*

 **Tip**



When you have finished configuring the ARX in the following section, be sure to see *Viewing the BIG-IP WOM Dashboard Statistics* on page 18.

Configuring the ARX

In this section, we show you how to configure the ARX to add the Remote server Windows Storage Server CIFS Share to the existing ARX Managed Volume.

For this configuration, we assume a CIFS namespace has already been configured with a managed volume and at least one CIFS share used as Tier 1 storage. The shares will be 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.

Prerequisites

The configuration presented in this guide is based on the fact that you have the following ARX objects already configured on the ARX (the names are used in our examples):

- CIFS only Namespace: **WOM**
- Managed Volume: **/vol**
- Root Level Share: **\\primary.siterequest.com\Tier1**
- Virtual Service: **\\arxwom.siterequest.com\demo**
- ARX Proxy User: **proxyuser**

If you have not already configured these objects on the ARX, see the ARX documentation.

In case the ARX is not preconfigured with a Tier 1 filer and managed volume refer to one of the existing deployment guides for ARX available at <http://www.f5.com/solutions/resources/deployment-guides.view.products.arx.html> for more information and example ARX configurations.

Adding the External Filer

In this section we add the Remote Windows File Server 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 **Remote**.
4. In the **Primary IP Address** box, type the primary IP address. We type **20.20.20.2**.
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 ignore Snapshot directories on EMC or NetApp filers, or have the ARX 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 Remote Windows File Server Share to the volume

The Remote Windows File Server share needs to be added 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 **Remote**.
4. From the **Namespace** list, select the name of the namespace that you had previously configured. In our example, we select **WOM**.
5. From the **Volume** list, select the name of the Volume that you had previously 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 3: Share Name definition

7. From the **File Server** list, select the External Filer you added in *Adding the External Filer on page 9*. In our example, we select **Remote**.
8. In the **CIFS Share** box, type the name of the CIFS share. In our example, the server is the remote Windows File Server (Remote) and the CIFS Share is **Tier2**.
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.
11. If this share had previously been a part of another F5 ARX Managed Volume, also select **Allow this switch to import this share, even if it is owned by another ARX**.
12. Click the **Next** button.

Select the options you would like this share to have.

Share name: foo

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 4: Share Options

Once the has been added to the Volume, verify the share status. The Managed Volume Details will report the share status and should show the root level share is online and the newly added share is Importing.

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) 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 Remote Windows File Server. These files will traverse the F5 BIG-IP WOM tunnel. 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 **rem_Tier**.
4. From the **Namespace** list, select the name of the namespace you created previously. In our example, we select **WOM**.
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:	<input type="text" value="Rem_Tier"/>
Namespace:	<input type="text" value="WOM"/>
Managed volume:	<input type="text" value="/vol"/>
Number of tiers:	<input type="text" value="2"/>

Figure 5: 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 **HQ**.
9. Click the **Next** button.
10. For **Tier 2**, select the Tier 2 file share. In our example, we select **Tier2**.
11. Click the **Next** button.
The next task is to specify the criteria for moving files between the Tiers, and to define the schedule.
12. Click the **Add** button to the right of Schedule to define the schedule to associate with the policy.

13. In the **Schedule Name** box, type a name for this schedule. In our example, we type **At_1AM**.
14. In the **Start Time** fields, you can specify a specific start time.
15. 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.
16. The other fields are optional. Configure as applicable for your deployment.
17. Click the **Save** button. 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="0"/> <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 6: Policy Schedule

Next, we create a fileset. A fileset restricts this policy to certain file types. However, for this implementation, we want to select all files. In our example, we create a fileset by performing the following:

18. Click the **Add** button to create a fileset. In this example, we want to match all files.
19. In the **Name** box, type a name. In our example, we type **All_Files**.
20. From the **Fileset type** list, select a type. We select **filename**.
21. In the *Filename Matching Criteria* section, we click **Wildcard Expression**, and then type ***** in the box.
22. Click **Save** to return to the Tiered Storage Wizard (see Figure 7 on the next page).

Figure 7: Fileset Definition

23. 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**.
24. From the **Move files not** list, select **modified**. In the **Last** box, type a number, and then from the list, select an option. In our example, we type **30** and select **Days**.
25. In the **Options** box, from the **Fileset** list, select the fileset you just created. In our example, we select **All_Files**.
26. From the Tiered Storage Wizard, select the Schedule **At_1AM** and the fileset **All_Files**.
27. Click **Next** to continue.

Figure 8: Policy Criteria

28. Review the Summary and then click **Finish**.

To view the Policies, from the left Navigation pane, expand the **Policy** and then click **Place Rules**. The two policies that were created using the wizard display. The first policy (which is precedence order 1) is for migrating files to Tier-1 (Headquarters server) and the second policy is for moving files to Tier-2 (Remote server) if they have a last modified time greater 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: All Volume: All

Fileset Migration... Tiered Storage... Remove... Edit... Enable Disable

<input type="checkbox"/>	Rule	Volume	Namespace	Precedence	From	To	Admin State	Status
<input type="checkbox"/>	Rem_Tier_tier-1-HQ	/vol	WOM	1	Rem_Tier_tier-1 (fileset)	HQ (share)	Enabled	Scan: Complete Migrate: Complete
<input type="checkbox"/>	Rem_Tier_tier-2-Tier2	/vol	WOM	2	Rem_Tier_tier-2 (fileset)	Tier2 (share)	Enabled	Scan: Complete Migrate: Migrating

Figure 9: Placerule Summary

The F5 ARX and F5 BIG-IP WOM have been configured for CIFS WAN optimized traffic. Both the HQ and the Remote filer servers have successfully been integrated into a Managed Volume.

Storage Integration Verification

In this section, we verify the configuration is operating properly. We use a test client to access the ARX Managed Volume.

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 proxies 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.

Add... Remove... Edit... Enable Disable Join Domain... Sync...

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

Figure 10: Virtual Service Summary

In the Virtual Services summary is the FQDN is arxwom.siterequest.com at the IP address 10.10.10.10 which is joined to the Active Directory 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 **W**.
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 **\\arxwom.siterequest.com\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**.

- 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.

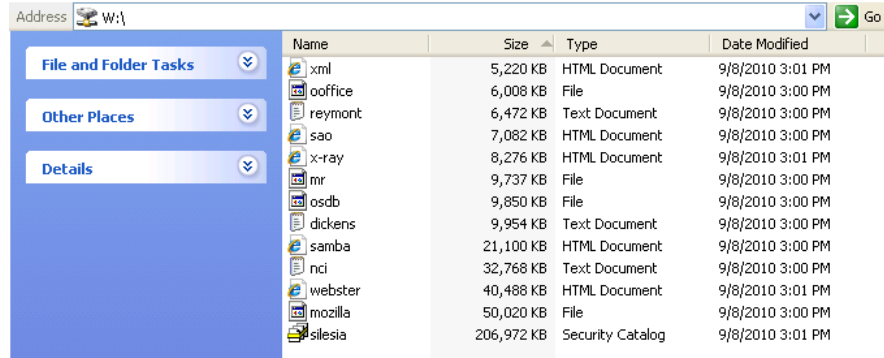


Figure 11: F5 ARX Virtual Service Managed Volume file contents

Generating an F5 ARX Metadata Report

The F5 ARX can generate a report to identify on which back end file shares files and folders are currently located.

To create an ARX Report

- From the left navigation pane, click **Managed Volumes**.
- Click on the Managed Volume **/vol**.
- Click the **Report** button. The Report Volume screen opens.
- In the **Path** box, you can type a path. In our example, we leave the default: **/**
- From the **Report Type** row, click **Metadata**.
- In the **Output Report Name** box, type a name for the report. In our example, we type **HQ_based_files**.
- From the **Share** list, select the **HQ** share.
- Click the **OK** button. The report is generated.
- Repeat this procedure, but in step 6, type a unique name, and in Step 7, select the Tier2 share.
- 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 **HQ_based_files.rpt**. The Report opens in a new browser window or tab.

Notice that only one file is newer than 30 days and this file is located on the HQ File Server.

In our example, the Metadata report for HQ looks like the following:

```
**** Metadata-Only Report: Started at Mon Mar 14 15:01:18 2011 ****
**** Software Version: 5.02.000.12637 (Oct 14 2010 23:24:00) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: WOM
```

```
**** Volume: /vol
**** Path: /vol
**** Share: HQ
```

Share	Physical Filer
[HQ] 10.10.10.1:Tier1

**** 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] [HQ] /HQ_filers.txt

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

```
**** Total items: 1
**** Elapsed time: 00:00:00
**** Metadata-Only Report: DONE at Mon Mar 14 15:01:18 2011 ****
```

Metadata Report for Tier 2

Select the report named **Tier2_based_files.rpt**. A new web browser window is launched and the report is displayed. Notice that 13 files are older than 30 days and these files are located on the Remote File Server.

```
**** Metadata-Only Report: Started at Mon Mar 14 15:03:32 2011 ****
**** Software Version: 5.02.000.12637 (Oct 14 2010 23:24:00) [nbuilds]
**** Hardware Platform: ARX-2000
**** Report Destination:
**** Namespace: WOM
**** Volume: /vol
```

**** Path: /vol
**** Share: Tier2

Share	Physical Filer
-------	----------------

[Tier2] 20.20.20.2:Tier2
--------	--------------------

**** 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] [Tier2] /mozilla
[FL] [Tier2] /dickens.txt
[FL] [Tier2] /nci.txt
[FL] [Tier2] /x-ray.htm
[FL] [Tier2] /ooffice
[FL] [Tier2] /samba.htm
[FL] [Tier2] /webster.htm
[FL] [Tier2] /mr
[FL] [Tier2] /reymont.txt
[FL] [Tier2] /silesia.cat
[FL] [Tier2] /osdb
[FL] [Tier2] /xml.htm
[FL] [Tier2] /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 Mon Mar 14 15:03:32 2011 ****

Viewing the BIG-IP WOM Dashboard Statistics

The BIG-IP WOM module has a Dashboard feature as a part of the Configuration utility. You can customize the dashboard to show different statistic values and graphs. While an ARX policy is operating or users are accessing files across the WOM tunnel, the charts reflect the overall performance and optimization statistics.

To access the WOM Dashboard

1. On the Main tab of the BIG-IP system, expand WAN Optimization, and then click Dashboard. The Dashboard opens in a new window.
2. View the statistics. See the following examples from our BIG-IP WOM of the values recorded while tiering files to and from the Remote file server.

The bandwidth Gain chart reports the raw versus Optimized bits / second and the current ratio meter:

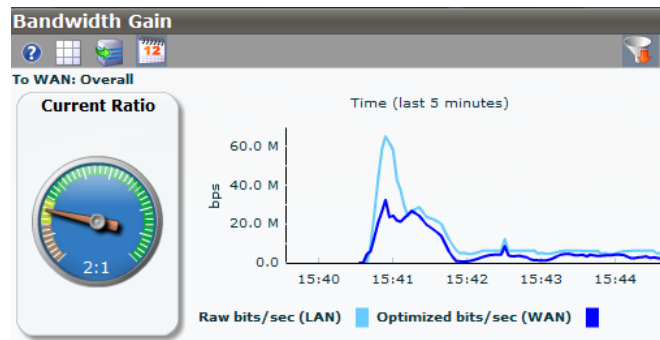


Figure 12: Bandwidth Gain chart

The Top Virtual Servers chart lists the configured virtual servers, percentage of traffic, raw and optimized megabytes transferred:

Top Virtual Servers				
To WAN				
Virtual Server	Percentage of Total WAN Traffic	%	Raw	Opt
CIFS_optimized_F		100.0	439.9 MB	264.8 MB
isession-virtual		0.0	7.4 KB	27.5 KB

Figure 13: Top Virtual Servers chart

The deduplication bucket distribution reports the Hit Bucket is being used for deduplicated data bytes.

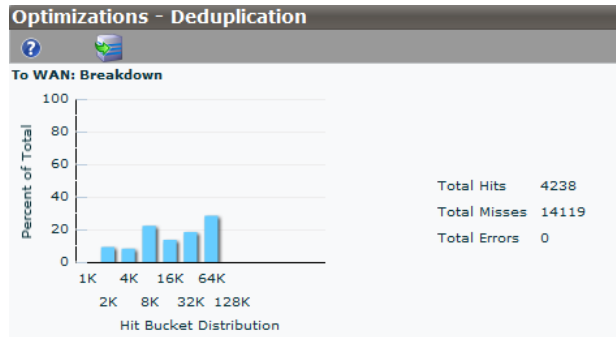


Figure 14: Deduplication breakdown chart

The CIFS Optimization breakdown chart reports the amount of reads or writes that were performed locally versus remote read or writes.

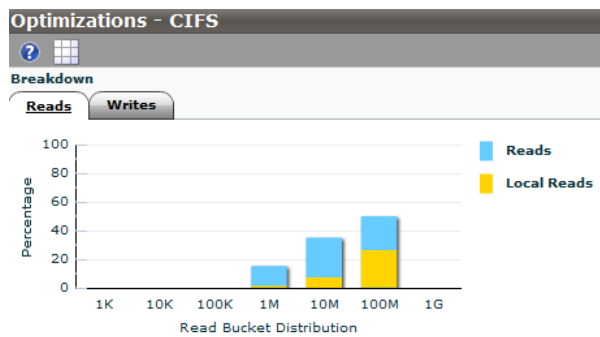


Figure 15: CIFS Optimizations breakdown chart

Conclusion

This deployment guide demonstrated the way to integrate the F5 ARX and BIG-IP WOM with Windows Storage Servers for tiering to a remote file server leveraging WAN Optimization.

For more information on configuring the F5 ARX or BIG-IP WOM, refer to the documentation, available on Ask F5.

