Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see https://f5.com/solutions/deployment-guides.
# Table of Contents

## Deploying F5 with VMware ESX Server
- **Prerequisites and configuration notes** ........................................... 1-1
- **Revision history** .................................................................................. 1-2

## Configuring the BIG-IP LTM system for VMware ESX
- **Load Balancing of Virtual Machine Guest Applications** .................. 1-3
- **Load balancing behavior with DRS** .................................................. 1-6
- **Load Balancing behavior with VMware HA** ...................................... 1-7
- **Using LTM to improve hardware capacity in a virtual environment** .... 1-8

## Configuring the F5 WebAccelerator module with applications running on VMware
- **Prerequisites and configuration notes** ............................................. 2-1
- **Configuration example** ..................................................................... 2-1

## Configuring the WebAccelerator module
- **Connecting to the BIG-IP LTM device** ............................................. 2-2
- **Creating an HTTP Class profile** ....................................................... 2-2
- **Modifying the Virtual Server to use the Class profile** ..................... 2-3
- **Creating an Application** ................................................................... 2-4

## Using BIG-IP GTM to provide global site redirection to a secondary data center
- **Configuring a self IP address on the BIG-IP LTM** ............................. 3-2
- **Creating a Listener on the GTM** ....................................................... 3-2
- **Creating data centers on the GTM system** ...................................... 3-3
- **Creating the monitor** ....................................................................... 3-4
- **Creating Servers for the data center** .............................................. 3-5
- **Creating a GTM pool** ....................................................................... 3-6
- **Creating a wide IP on the GTM** ....................................................... 3-8
- **Configuring the Wide IP as an MX record using ZoneRunner** .......... 3-9

## Deploying the ARX with Windows XP VMware VMs for accessing Content Shares
- **Prerequisites and configuration notes** ............................................. 4-1
- **Configuration example** ..................................................................... 4-1

## Integrating ARX and VMware Virtual machines
- **Configuring the ARX** ....................................................................... 4-3
- **Configuring Active Directory Authentication** .................................. 4-3
- **Verifying the Active Directory Authentication** ................................. 4-8
- **Creating the CIFS Namespace** .......................................................... 4-9
- **Creating a Managed Volume** ............................................................ 4-10
- **Adding the External Filers** ............................................................... 4-13
- **Adding root level share** .................................................................. 4-14
- **Adding a second CIFS Share** .......................................................... 4-16
- **Creating the Share farm** ................................................................. 4-17
- **Creating the Virtual Service** ............................................................ 4-19

## Integrating the VMware Guest operating system
- **Mounting the Virtual Server CIFS share** ......................................... 4-22
- **Generating an ARX Metadata Report** ............................................. 4-25

## Deploying the ARX for VMware ESX virtualized Windows 2008 in a Managed Volume
- **Prerequisites and configuration notes** ............................................. 5-1
- **Product versions and revision history** .............................................. 5-2
- **Configuration example** ..................................................................... 5-2
Configuring Windows Server 2008 for the ARX .......................................................... 5-3
  Joining the Active Directory Domain ...................................................................... 5-3
  Initializing a new VMware storage device ............................................................ 5-4
  Initializing the Windows Server 2008 Disk ............................................................ 5-5
  Creating a CIFS File Share ..................................................................................... 5-7
  Assigning the Local Backup Operator ................................................................. 5-8
Configuring the ARX ................................................................................................. 5-10
  Configuring the Active Directory Authentication .................................................. 5-10
  Verifying Active Directory Authentication ............................................................. 5-11
  Creating the CIFS Namespace ............................................................................... 5-12
  Creating a volume .................................................................................................. 5-13
  Adding the External Filers ..................................................................................... 5-14
  Adding the root level share ................................................................................... 5-15
  Creating the Share farm ........................................................................................ 5-16
  Creating a Tiered Storage policy ........................................................................... 5-17
  Creating the Virtual Service .................................................................................. 5-20
Verifying Client access ............................................................................................... 5-23
  Mounting the Virtual Server CIFS share ............................................................... 5-23
  Generating an ARX Metadata Report ................................................................... 5-24
  Conclusion .............................................................................................................. 5-25
Deploying F5 with VMware ESX Server

• Configuring the BIG-IP LTM system for VMware ESX

• Load Balancing of Virtual Machine Guest Applications

• Load balancing behavior with DRS

• Load Balancing behavior with VMware HA

• Using LTM to improve hardware capacity in a virtual environment
Deploying F5 with VMware ESX Server

Welcome to the F5 Deployment Guide on VMware ESX Server. This document provides guidance and configuration procedures for deploying the BIG-IP Local Traffic Manager (LTM), BIG-IP Global Traffic Manager (GTM), WebAccelerator, and ARX series with VMware ESX server and the applications running on those devices.

VMware ESX Server, particularly when deployed as part of VMware Virtual Infrastructure, permits a high degree of flexibility for guest operating systems and applications within a datacenter, or between remote data centers. By using BIG-IP LTM and GTM in conjunction with ESX Server, administrators and application architects can improve scalability, ease administrative overhead, and improve end-user experience for applications hosted within a virtualized environment. For additional resources on F5 and VMware, see the VMware forum on DevCentral.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Important

This guide is different than F5’s typical Deployment Guides, as the F5 configuration is highly dependent on which applications that are running on the VMware ESX devices. Therefore, most of this document provides general guidance for deploying F5 devices with VMware, as opposed to specific configuration procedures. Refer to the Deployment Guide specific to your application for specific configuration procedures.

This Deployment Guide is broken up into the following chapters:
• Configuring the BIG-IP LTM system for VMware ESX, on page 1-3
• Configuring the F5 WebAccelerator module with applications running on VMware, on page 2-1
• Using BIG-IP GTM to provide global site redirection to a secondary data center, on page 3-1
• Deploying the F5 ARX with Windows XP VMware Virtual machines for accessing Content Shares, on page 4-1
• Deploying the F5 ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume, on page 5-1

Prerequisites and configuration notes

The following are prerequisites for this solution:
• This Deployment Guide was tested using VMware Virtual Infrastructure 3. Although many of the basic practices outlined in the Load Balancing of Virtual Machine Guest Applications, on page 1-3 section of this document are also valid for VMware Server or other VMware virtualization products, most other sections depend on enterprise-level features only found in the Virtual Infrastructure suite.
We recommend running BIG-IP LTM version 9.4 or later.

Within the context of this deployment guide, virtual server will be used to refer to an IP address and port on a BIG-IP LTM which accepts network traffic. On ESX Server, virtualized operating systems will be referred to as guests.

Revision history

Product and versions tested for this deployment guide:

<table>
<thead>
<tr>
<th>Product Tested</th>
<th>Version Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG-IP LTM, GTM, WebAccelerator</td>
<td>v9.4.2</td>
</tr>
<tr>
<td>F5 ARX</td>
<td>5.0.1</td>
</tr>
<tr>
<td>VMware ESX</td>
<td>ESX Server 3, 3.5</td>
</tr>
</tbody>
</table>

Revision history:

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>New deployment guide</td>
</tr>
<tr>
<td>1.1</td>
<td>Added Chapter 4, Deploying the ARX with VMware ESX Servers for Shared Content Access, for deploying the F5 ARX with VMware. No updates to other sections of the guide.</td>
</tr>
<tr>
<td>1.2</td>
<td>Added Chapter 5, Configuring the ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume. No updates to other sections of the guide.</td>
</tr>
<tr>
<td>1.3</td>
<td>Removed the WANJet chapter. For guidance on long distance VMware deployments, see the VMware Long-Distance VMotion deployment guides, available at <a href="http://www.f5.com/solutions/resources/deployment-guides/#letterV">www.f5.com/solutions/resources/deployment-guides/#letterV</a></td>
</tr>
</tbody>
</table>
Configuring the BIG-IP LTM system for VMware ESX

This section provides general guidance for deploying the BIG-IP LTM system with VMware ESX devices. This section contains the following topics:

- Load Balancing of Virtual Machine Guest Applications
- Load balancing behavior with DRS, on page 1-6
- Load Balancing behavior with VMware HA, on page 1-7
- Using LTM to improve hardware capacity in a virtual environment, on page 1-8

Load Balancing of Virtual Machine Guest Applications

In most ways, an application within an ESX guest behaves much like an application running outside of a virtualized environment. Because a BIG-IP LTM directs traffic to a network address, guests that are defined as members in an LTM pool can be located on any number of ESX servers, and distributed among multiple host servers in any manner.

![Diagram of BIG-IP LTM and ESX deployments]

Figure 1.1 Using the BIG-IP LTM to direct traffic to ESX deployments
Considerations for load balancing method

When configuring a BIG-IP LTM system, the IP addresses and Service Ports of the target device or application are added to a load balancing pool. For each BIG-IP LTM pool that contains an ESX device, we recommend choosing one of the following load balancing methods:

- **Observed (member)**
  The Observed load balancing method allows the BIG-IP LTM to use a combination of logic based on the Least Connections and Fastest load balancing methods to determine the optimal ESX guest to which new traffic should be directed. Since virtualized guests usually co-exist with other applications on the same hardware, this ensures that new traffic is sent to the pool member most able to handle the traffic. For instance, if an ESX server is engaged in heavy disk activity due to events occurring within other guests, and the target guest is therefore unable to process requests in as timely a manner as during normal situations, LTM will dynamically adjust traffic levels to target those guests on other hosts that are better able to process the traffic. The Observed method is particularly useful when ESX hosts may be of dissimilar hardware profiles, or when applications are not evenly distributed throughout an environment.

- **Predictive (member)**
  The Predictive load balancing method is similar to Observed, except that it also takes into account trending of each pool member. In a highly-dynamic ESX environment, or one that is subject to extreme traffic fluctuations, the Predictive algorithm may help decrease the number of VMotion migrations triggered by VMware DRS technology by directing traffic to guests that not only have the least connections and fastest response times, but those that are likely to remain that way.

**To modify the load balancing method of a BIG-IP LTM pool**

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. From the Pool list, click the name of the applicable pool. The Pool Properties screen opens.
3. On the menu bar, click **Members**.
4. From the **Load Balancing Method** list, select **Observed (member)** or **Predictive (member)** based on the preceding descriptions.
5. Click the **Update** button.

![Figure 1.2 Changing the load balancing method of the pool](image)
VMware ESX Server makes it easy to clone existing guests, to suspend guests and resume their operation quickly at a later time, and to fully boot guests that have been shut down. As a result, administrators have the option of quickly adding guests at either predictable intervals, or to meet unexpected traffic spikes. You may want to pre-allocate IP addresses for guests and pre-configure those as nodes and pool members within BIG-IP LTM. No traffic will be sent to those guests unless and until such time as they are brought online, but in that scenario no further configuration of the LTM is required once you make the decision to activate the guests.

Considerations for the health monitor

Health monitors for applications running on ESX should be based on application behavior, not simple methods such as icmp or tcp. For example, we recommend an advanced health monitor based on the http parent that checks for a specific response string from the guest application. This ensures that newly-provisioned, newly-unsuspended, or newly-migrated guests are truly ready to process application traffic correctly.

You can modify an existing health monitor, or create a new one based on the following procedure.

To create an advanced health monitor

1. On the Main tab, expand Local Traffic, and then click Monitors.
2. Click the Create button. The New Monitor screen opens.
3. In the Name box, type a name for the Monitor.
   In our example, we type advhttp-monitor.
4. From the Type list, select http.
5. In the Configuration section, in the Interval and Timeout boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of 5 and an timeout of 16). In our example, we use a Interval of 30 and a Timeout of 91. In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.
6. In the Send String box, type a string that you expect the target device to return. In our example, we use a Send String of GET/iisstart.htm.
   If the page you are requesting in the Send String requires authentication, type a user name and password in the appropriate boxes.
7. In the Receive Rule box, type what you expect to receive from the Send String. In our example, we expect the Under Construction page to be returned, so we type [Uu]nder [Cc]onstruction (see Figure 1.3).
8. Click the **Finished** button.
The new monitor is added to the Monitor list.

![Image](image.png)

**Figure 1.3 Creating an advanced HTTP monitor**

**Load balancing behavior with DRS**

VMware DRS is a technology for resource balancing, allocation, and management among hosts. Using DRS, an administrator can define threshold limits on each host. When an ESX guest encounters the CPU or memory threshold, DRS moves that guest to a host with more resources. VMware's VMotion technology allows this to occur while the guest is still running.

BIG-IP LTM continues to direct traffic to the guest on the new host; to LTM, this is still the same pool member. By using **Predictive** or **Observed** load balancing methods, traffic is automatically sent to the guest at a level appropriate to new capacities of guest, which is now running on a host that is less constrained.

The BIG-IP LTM offers the additional benefit of mitigating the very brief time in which VMotioned guests are not on the network. A busy web server, for instance, may have several requests interrupted mid-stream. Although many clients will be able to gracefully re-request the data, it's also possible that an application may mis-behave or that content may be delivered...
incompletely. By using BIG-IP LTM, which will manage the direct connectivity to the servers on behalf of the clients, you ensure that only valid, correct, and complete data is returned to the client.

Figure 1.4 Using a BIG-IP LTM to transparently direct appropriate traffic to a VMotioned guest

Load Balancing behavior with VMware HA

VMware HA (High Availability) will restart ESX guests on different hosts, if their original hardware hosts fail. Unlike with VMware DRS, which moves guests to hosts that have more resources available, in a hardware failure situation the total resources available to the resource pool will decrease. As a result, it’s likely that guests will restart on hosts with more-constrained capabilities.

BIG-IP LTM will direct traffic to the newly-restartet guests regardless of which host they are assigned. Also, by using Predictive or Observed load balancing methods, the guests will receive the proportional amount of traffic appropriate to their new hosts.
Using LTM to improve hardware capacity in a virtual environment

ESX guests share the CPU, disk, and RAM resources of their hosts. By decreasing the per-transaction resources required by each guest, you can dramatically increase the number of virtual machines that can run effectively on any host, while also increasing the effective work that each virtual machine can accomplish.

As an example, BIG-IP’s TCP Express feature set ensures optimal network performance for all clients and servers, regardless of operating system and version.

The F5 WebAccelerator (available as a module on the BIG-IP system) can also significantly improve hardware capacity in a virtual environment. See Configuring the F5 WebAccelerator module with applications running on VMware, on page 2-1.

Offloading SSL transactions

One of the strengths of the BIG-IP LTM is the ability to terminate HTTPS or other SSL connections, and send traffic to the guests unencrypted. This reduces CPU and memory load on ESX guests by using the dedicated
decryption hardware on the LTM. By terminating SSL/TLS connections at the BIG-IP LTM, you also simplify certificate management, and allow new guest to come online quickly and inexpensively.

To configure the BIG-IP LTM system to offload SSL you need to install a SSL certificate on the BIG-IP LTM and add the certificate and key to a Client SSL profile which is added to the appropriate virtual server. The following procedures describe how to import an SSL certificate into the BIG-IP LTM, how to add the certificate to a profile, and how to modify the virtual server to include the profile.

For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the Configuration Guide for Local Traffic Management.

Importing keys and certificates

Once you have obtained a certificate from a certificate authority, you can import this certificate into the BIG-IP LTM system using the Configuration utility.

**To import a key or certificate**

1. On the Main tab, expand Local Traffic.
2. Click SSL Certificates. The list of existing certificates displays.
3. In the upper right corner of the screen, click Import.
4. From the Import Type list, select the type of import (Certificate or Key).
5. In the Certificate (or Key) Name box, type a unique name for the certificate or key.
6. In the Certificate (or Key) Source box, choose to either upload the file or paste the text.
7. Click Import.

If you imported the certificate, repeat this procedure for the key.

Creating a Client SSL profile

The next step is to create a Client SSL profile. This profile contains the SSL certificate and Key information for decrypting the SSL traffic on behalf of the servers.

**To create a new Client SSL profile**

1. On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
2. On the Menu bar, from the SSL menu, select Client. The Client SSL Profiles screen opens.
3. In the upper right portion of the screen, click the Create button. The New Client SSL Profile screen opens.

4. In the Name box, type a name for this profile. In our example, we type clientssl-profile.

5. In the Configuration section, check the Certificate and Key Custom boxes.

6. From the Certificate list, select the name of the Certificate you imported in the Importing keys and certificates section.

7. From the Key list, select the key you imported in the Importing keys and certificates section.

8. Click the Finished button.

Modifying the virtual server to include the Client SSL profile

The final task to enable the BIG-IP LTM to offload SSL is to modify the appropriate virtual server to include the Client SSL profile you just created.

To modify an existing virtual server to use the Client SSL profile

1. On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.

2. From the Virtual Server list, click the virtual server that will be offloading SSL traffic.

3. In the Configuration section, from the SSL Profile (Client) list, select the name of the profile you created in Creating a Client SSL profile, on page 1-9. In our example, we select clientssl-profile.

4. Click the Update button.

![Figure 1.6 Adding the Client SSL profile to the virtual server](image)

**Figure 1.6** Adding the Client SSL profile to the virtual server
Creating BIG-IP LTM profiles to optimize application transactions

The BIG-IP LTM system uses profiles to enhance your control over managing network traffic, and makes traffic-management tasks easier and more efficient. For applications running on VMware, we recommend using custom HTTP and TCP profiles to optimize the BIG-IP LTM to Guest connections. This allows each guest to perform as efficiently as possible. The optimized HTTP profile makes use of F5’s RAM cache and compression engine which speed application transactions.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to the application, and ensures you do not accidentally overwrite the default profile.

Creating an HTTP profile

The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In the following example, we leave all settings at their default levels. You can modify any of the profile settings to tune the profile to your application. Although you can use the default profiles, we strongly recommend creating new profiles based off of the parent profile to make

To create a new HTTP profile

1. On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the Create button. The New HTTP Profile screen opens.
3. In the Name box, type a name for this profile. In our example, we type http-optimized.
4. From the Parent Profile list, select http-wan-optimized-compression-caching.
5. Check the Custom box for Content Compression, and leave Content List selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the Finished button.

Creating the WAN optimized TCP profile

The next profile we create is a LAN optimized profile.

To create a new TCP profile

1. On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
2. On the Menu bar, from the Protocol menu, click tcp.
3. In the upper right portion of the screen, click the Create button. The New TCP Profile screen opens.

4. In the Name box, type a name for this profile. In our example, we type optimized-tcp-wan.

5. From the Parent Profile list, select tcp-wan-optimized.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the Finished button.

Creating the LAN optimized TCP profile

The next profile we create is a LAN optimized profile.

To create a new TCP profile

1. On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.

2. On the Menu bar, from the Protocol menu, click tcp.

3. In the upper right portion of the screen, click the Create button. The New TCP Profile screen opens.

4. In the Name box, type a name for this profile. In our example, we type optimized-tcp-lan.

5. From the Parent Profile list, select tcp-lan-optimized.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the Finished button.

Modifying the virtual server to use the new profiles

The next task is to modify the virtual server to use the new profiles you just created.

1. On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.

2. From the Virtual Server list, click the virtual server that will use the new profiles.

3. From the Configuration list, select Advanced. The Advanced configuration options appear.

4. From the Protocol Profile (Client) list, select the name of the profile you created in the Creating the WAN optimized TCP profile section. In our example, we select optimized-tcp-wan.

5. From the Protocol Profile (Server) list, select the name of the profile you created in the Creating the LAN optimized TCP profile section. In our example, we select optimized-tcp-lan.
6. From the HTTP Profile list, select the name of the profile you created in the Creating an HTTP profile section. In our example, we select http-optimized.

7. Click the Update button.

This concludes the BIG-IP LTM system guidance for VMware devices.
Deploying the WebAccelerator module with VMware ESX Servers

- Configuring the WebAccelerator module
- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application
Configuring the F5 WebAccelerator module with applications running on VMware

In this chapter, we configure the WebAccelerator module for the VMware devices to improve hardware capacity in a virtual environment. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

For more information on the F5 WebAccelerator, see www.f5.com/products/big-ip/product-modules/webaccelerator.html.

Prerequisites and configuration notes

The following are prerequisites for this section:

- We assume that you have already configured the BIG-IP LTM system for directing traffic to the ESX deployment as described in this Deployment Guide.
- You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later.
- If you are using the BIG-IP LTM version 9.4.2 or later, you must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (we recommend HTTP Acceleration) and associate it with the virtual server. This is only required for BIG-IP LTM version 9.4.2 and later.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to improve hardware capacity for the VMware devices. The BIG-IP LTM with WebAccelerator module both offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency accesses an ESX device via the WebAccelerator. The user’s request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.
Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the WebAccelerator Administrator Guide for more information.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP LTM system’s web-based Configuration utility using a web browser.

To connect to the BIG-IP LTM system using the Configuration utility

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click Yes.
   The authorization dialog box appears.
2. Type your user name and password, and click OK.
   The Welcome screen opens.

Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

To create a new HTTP class profile

1. On the Main tab, expand WebAccelerator, and then click Classes.
   The HTTP Class Profiles screen opens.
2. In the upper right portion of the screen, click the Create button.
   The New HTTP Class Profile screen opens.
3. In the Name box, type a name for this Class. In our example, we type example-class.
4. From the Parent Profile list, make sure httpclass is selected.
5. In the Configuration section, from the WebAccelerator row, make sure Enabled is selected.
6. In the Hosts row, from the list select Match Only. The Host List options appear.
   a) In the Host box, type the host name that your end users use to access the application on the ESX devices. In our example, we type http://example-application.f5.com/.
b) Leave the Entry Type at **Pattern String**.

c) Click the **Add** button.

d) Repeat these sub-steps for any other host names users might use to access the SAP deployment.

7. The rest of the settings are optional, configure them as applicable for your deployment.

8. Click the **Finished** button. The new HTTP class is added to the list.

### Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server on the BIG-IP LTM system to use the HTTP Class profile you just created.

**To modify the Virtual Server to use the Class profile**

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.

2. From the **Virtual Server** list, click the name of the virtual server you created for the application on the VMware devices. In our example, we click **example-http-vs**. The General Properties screen for the Virtual Server opens.

3. On the Menu bar, click **Resources**. The Resources screen for the Virtual Server opens.

4. In the HTTP Class Profiles section, click the **Manage** button.

5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (<<) button to move it to the Enabled box. In our example, we select **example-class**.

6. Click the **Update** button. The HTTP Class Profile is now associated with the Virtual Server.

**Important**

*If you are using the BIG-IP LTM version 9.4.2 or later, you must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example, we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile. This is only required for BIG-IP LTM version 9.4.2 and later.*

*To create the HTTP profile, use Creating an HTTP profile, on page 1-11, selecting the HTTP Acceleration parent profile. You must leave RAM Cache enabled; all other settings are optional. To modify the virtual server, follow*
Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click **Update**.

Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

**To create a new Application**

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**.
   The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **New Application** button.
3. In the Application Name box, type a name for your application. In our example, we type **Example Application**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select the Policy that best matches the application you are running on the VMware devices. If there is not a predefined policy for your application, you can create a new WebAccelerator policy for your application.
6. In the **Requested Host** box, type the host name that your end users use to access the application. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we type **http://example-application.f5.com/**.
   If you have additional host names, click the **Add Host** button and enter the host name(s).
7. Click the **Save** button.

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice a marked improvement in performance after their first visit.
Deploying the BIG-IP GTM for VMware ESX Server multi-data center deployments

- Configuring a self IP address on the BIG-IP LTM
- Creating a Listener on the GTM
- Creating data centers on the GTM system
- Creating the monitor
- Creating Servers for the data center
- Creating a GTM pool
- Creating a wide IP on the GTM
- Configuring the Wide IP as an MX record using ZoneRunner
Using BIG-IP GTM to provide global site redirection to a secondary data center

In this chapter, we configure the BIG-IP Global Traffic Manager for multi-data center deployments of VMware. VMware Infrastructure makes hosting duplicate sites or applications in remote data centers an easier and more-manageable task. Because of that, it’s even more important than ever to have a global traffic management solution that can direct clients to the correct, functional site in a timely manner.

The BIG-IP Global Traffic Manager module (GTM) can perform all required functions to make this possible. If for instance Site 1 becomes unavailable because its Internet connection is severed, BIG-IP-GTM modifies DNS to direct clients to Site 2 when appropriate -- when replication of VMware images is complete, guests are running, and the application is accepting traffic.

The BIG-IP GTM is available as a module on the BIG-IP system.

For more information on the BIG-IP GTM, see www.f5.com/products/big-ip/product-modules/global-traffic-manager.html

Figure 3.1 Logical configuration example using BIG-IP Local and Global Traffic Managers
Configuring a self IP address on the BIG-IP LTM

The first task in this configuration is to create a unique self IP address on the BIG-IP LTM system for use by the GTM. You need a unique self IP address for each redundant pair of BIG-IP LTM devices in this configuration, so if you have multiple pairs of BIG-IP LTMs you need a unique self IP for each one.

The IP address you choose, and the VLAN to which you assign it, must be accessible by any clients that will be performing DNS queries against the GTM. It may be a private IP address if a Network Address Translation (NAT) device, such as a BIG-IP LTM, a firewall, or a router, is providing a public address and forwarding DNS traffic to the listener.

To create a self IP address
1. On the Main tab, expand Network, and then click Self IPs. The Self IP screen opens.
2. Click the Create button. The new Self IP screen opens.
3. In the IP Address box, type an IP address in the appropriate VLAN (the VLAN you choose in step 5). In our example, we type 10.133.20.70.
4. In the Netmask box, type the corresponding subnet mask. In our example, we type 255.255.255.0.
5. From the VLAN list, select the appropriate VLAN.
6. Click the Finished button. The new self IP address appears in the list.

Creating a Listener on the GTM

The next task is to create a listener on the BIG-IP GTM system. A listener instructs the Global Traffic Manager to listen for network traffic destined for a specific IP address. In our case, this specific IP address is the self IP address on the LTM system we just created.

To create a listener on the GTM system
1. On the Main tab of the navigation pane, expand Global Traffic and then click Listeners. The main listeners screen opens.
2. Click the Create button.
3. In the Destination box, type the self IP address you created in Configuring a self IP address on the BIG-IP LTM, on page 3-2. In our example, we type 10.133.20.70 (see Figure 3.2).
4. Leave the VLAN Traffic list set to All VLANs.
5. Click the Finished button.
6. Repeat this procedure for any additional self IP addresses you configured in the Configuring a self IP address on the BIG-IP LTM section.

![Figure 3.2 Creating a new listener](image)

Creating data centers on the GTM system

The next step is to create data centers on the GTM system for each real-world location that will host globally load balanced ESX devices servers. A data center defines the group of Global Traffic Managers, Local Traffic Managers, host systems, and links that share the same subnet on the network. In our example, we created a Seattle data center and a New York data center.

To create a new Datacenter on the GTM system

1. On the Main tab of the navigation pane, expand Global Traffic and click Data Centers. The main screen for data centers opens.
2. Click the Create button. The New Data Center screen opens.
3. In the Name box, type a name for this datacenter. In our example, we type Seattle DC.
4. In the Location box, type a location that describes the physical location of the data center. In our example, we type Seattle, Washington.
5. In the Contact box, type the name of the person responsible for managing the network at the data center. In our example, we type admin@f5seattledatacenter.com.
6. Make sure the State list remains at Enabled (see Figure 3.3).
7. Click the Finished button.
8. Repeat this procedure for each of your data centers. In our example, we repeat the procedure once for our New York data center.
Creating the monitor

The next task is to create a monitor on the GTM system. Monitors verify connections on pools and virtual servers and are designed to check the status of a pool or virtual server on an ongoing basis, at a set interval. If a pool or virtual server being checked does not respond within a specified timeout period, or the status of a pool or virtual server indicates that performance is degraded, then the Global Traffic Manager can redirect the traffic to another resource.

In our example, the application running on our VMware devices is an email application, so we create an SMTP monitor. The SMTP monitor issues standard Simple Mail Transport Protocol (SMTP) commands to ensure that the BIG-IP LTM virtual server is available. You can configure a monitor most appropriate for your configuration.

Although it is possible to use the default monitor, we recommend creating a new monitor based off the default monitor, which enables you to configure specific options.

To create a BIG-IP GTM health monitor

1. On the Main tab of the navigation pane, expand Global Traffic and then click Monitors.
2. Click the Create button. The New Monitor screen opens.
3. In the Name box, type a name for the monitor. In our example, we type gtm_smtp.
4. From the Type list, select SMTP.
5. Configure the options as applicable for your deployment. In our example, we leave the options at their default levels.
6. Click the Finished button. The new monitor is added to the list.
Creating Servers for the data center

The next task is to create a GTM Server for the data centers. A server defines a specific system on the network. In this deployment, the GTM servers are the BIG-IP LTM systems we configured earlier in this guide.

To create a GTM server

1. On the Main tab of the navigation pane, expand Global Traffic and click Servers. The main screen for servers opens.
2. Click the Create button. The New Server screen opens.
3. In the Name box, type a name that identifies the Local Traffic Manager. In our example, we type Seattle_BIG-IP.
4. From the Product list, select either BIG-IP System (Single) or BIG-IP System (Redundant) depending on your configuration. In our example, we select BIG-IP System (Redundant).
5. From the Address List section, in the Address box, type the self IP address of the BIG-IP LTM device, and then click the Add button. In our example, we type 10.133.20.227.
6. If you selected BIG-IP System (Redundant) in Step 4, from the Peer Address List section, in the Address box, type the self IP address of the redundant BIG-IP LTM device, and then click the Add button.

   Note: Do not use a floating IP address of the redundant pair. Do not use the administrative interface of the either member of a redundant pair.

7. From the Data Center list, select the name of the data center you created in the Creating data centers on the GTM system section. In our example, we select Seattle DC.
8. In the Health Monitors section, from the Available list, select the name of the monitor you created in the Creating the monitor section, and click the Add (<<) button. In our example, we select gtm_smtp.
9. In the Resources section, from the Virtual Server Discovery list, choose an option. We recommend Enabled (No Delete). With this option, the GTM will discover all the virtual servers you have configured on the LTM(s) via iControl, and will update, but not delete them.
10. Click the Finished button.
Creating a GTM pool

The next task is to create a pool on the GTM device that contains the BIG-IP LTM virtual server.

**To create a pool on the GTM**

1. On the Main tab of the navigation pane, expand Global Traffic and click Pools (located under Wide IPs).
2. Click the **Create** button. The New Pool screen opens.

3. In the **Name** box, type a name for the pool. In our example, we type **Seattle_pool**.

4. In the Health Monitors section, from the Available list, select the name of the monitor you created in the *Creating the monitor* section, and click the Add (<<) button. In our example, we select **gtm_smtp**.

5. In the Load Balancing Method section, choose the load balancing methods from the lists appropriate for your configuration. In our example, we select **Global Availability, Round Robin, and Return to DNS**, in that order.

6. In the Member List section, from the Virtual Server list, select the virtual server you created for the ESX devices, and click the Add button. You must select the virtual server by IP Address and port number combination. In our example, we select **10.133.20.200:25**. If you have additional virtual servers for the ESX devices configured on the BIG-IP LTM system, repeat this step.

7. Click the **Finished** button.

---

**Figure 3.5 Creating a pool on the BIG-IP GTM**
Creating a wide IP on the GTM

The next task is to create a wide IP on the GTM system. A **wide IP** is a mapping of a fully-qualified domain name (FQDN) to a set of virtual servers that host the domain’s content.

**To create a wide IP on the GTM system**

1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Wide IPs**.
2. Click the **Create** button. The New Wide IP screen opens.
3. In the **Name** box, type a name for the Wide IP. In our example, we type **mail.example.com**.
4. In our example, we are not using any iRules, so we skip the iRule section. Configure as appropriate for your deployment.
5. In the Pools section, from the **Load Balancing Method** list, select a load balancing method. In our example, we select **Global Availability**. Global Availability instructs the GTM to select the first pool in the wide IP until it becomes unavailable, at which point it selects the next pool until the first pool becomes available again.

   In our example, the GTM sends all incoming email to the first-listed pool, **Seattle_pool**. If that pool is unavailable, all incoming email is sent to the next-listed pool, **NewYork_pool**. If you wish to distribute incoming email among multiple pools, select another method, such as Ratio. Consult the online documentation or the product manual for more details about load balancing methods.
6. From the Pool List section, from the **Pool** list, select the name of the pool you created in the **Creating a GTM pool** section, and then click the **Add** button.
   In our example, we select **Seattle_pool**.
   Repeat this step for any additional pools. In our example, we repeat one time for the **NewYork_pool**.
7. All other settings are optional, configure as appropriate for your deployment.
8. Click the **Finished** button (see Figure 3.6).
Figure 3.6 Creating a new Wide IP on the GTM system

The next task is to add the newly-created Wide IP as an MX record in your DNS system. If using the GTM as your primary DNS system, this is done through the ZoneRunner utility.

Configuring the Wide IP as an MX record using ZoneRunner

The final task in this configuration is to configure the Wide IP as an MX record in a DNS system. In our example, we are using the GTM system as our primary DNS, and use ZoneRunner to add the Wide IP as an MX record.

The ZoneRunner utility is an advanced feature of the Global Traffic Manager. We highly recommend that you become familiar with the various aspects of BIND and DNS before you use this feature. For in-depth information, we recommend the following resources:

- DNS and BIND, 4th edition, Paul Albitz and Cricket Liu
- The IETF DNS documents, RFC 1034 and RFC 1035

For information on adding the required MX record to other DNS servers, for instance BIND or Microsoft Windows 2007 DNS Service, consult the appropriate product documentation.

**To add the Wide IP as an MX record using ZoneRunner**

1. On the Main tab of the navigation pane, expand Global Traffic and click ZoneRunner.
2. Click the Create button. The New Resource Record screen opens.
3. From the View list, select a view. In our example, we select external.
4. From the Zone list, select the appropriate zone. In our example, we select example.com
5. In the Name box, type a name for the Resource Record. Make sure the domain for which you are creating an MX record is shown, and note that it must end with a period.
6. In the TTL box, type a number of seconds. In our example, we type 500 (which is the default TTL for our zone).
7. From the Type list, select MX.
8. In the Preference box, type 10. Preference is a numeric value for the preference of this mail exchange host relevant to all other mail exchange hosts for the domain. Lower numbers indicate a higher preference, or priority. In a traditional DNS configuration, you would create multiple MX records with different priorities; however, since you're using GTM to provide true wide-area load balancing, it is only necessary to create a single record in this case.
9. In the Mail Server, enter the name of the Wide IP that you created in Creating a wide IP on the GTM. Make sure that this name also ends with a period. In our example, we type mail.example.com.
10. Click the Finished button (see Figure 3.7).
Figure 3.7 Creating a new Resource Record using ZoneRunner

This concludes the BIG-IP GTM configuration. For more information on the BIG-IP GTM, see the GTM documentation.
4

Deploying the ARX with VMware ESX Servers for Shared Content Access

- Integrating ARX and VMware Virtual machines
- Configuring the ARX
- Integrating the VMware Guest operating system
Deploying the F5 ARX with Windows XP VMware Virtual machines for accessing Content Shares

This chapter illustrates how the F5 ARX can interoperate with VMware Virtual machines running Microsoft Windows XP. The Windows Virtual machines will boot from the VMware VMDK datastore and mount ARX Virtual volumes as content drives.

The benefit of this type of configuration is Virtual Machines can migrate from one VMware server to the next and still maintain consistent access to the shared content available from the ARX Virtualized storage shares.

The shared content is kept in sync between data centers by leveraging the external filer’s replication/mirroring technology. The filers simultaneously mirror the main data center’s content to distant data center filers. When a failover between data centers is invoked, the read-only copies in the far end data center are changed to read/write access and the guest systems can mount the local replicas. This guide demonstrates how to access the replicated data after the read/write access has been granted.

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

Prerequisites and configuration notes

The following are additional prerequisites and configuration notes for this chapter:

- In our configuration, the VMware Guest operating system was Microsoft Windows XP.

Configuration example

In the following diagram, we show basic connectivity between clients, ARX and Virtual Machines accessing content shares. The VMware virtual machines operate within the ESX hypervisor. These VMs will attach to the ARX virtualized volumes via the LAN.
Figure 4.1 Logical configuration example
Integrating ARX and VMware Virtual machines

To configure the ARX and the VMware Virtual machines, you must complete the following procedures:

- **Configuring the ARX**, on page 4-3
  - **Configuring Active Directory Authentication**, on page 4-3
  - **Verifying the Active Directory Authentication**, on page 4-8
  - **Creating the CIFS Namespace**, on page 4-9
  - **Creating a Managed Volume**, on page 4-10
  - **Adding the External Filers**, on page 4-13
  - **Adding root level share**, on page 4-14
  - **Adding a second CIFS Share**, on page 4-16
  - **Creating the Share farm**, on page 4-17
  - **Creating the Virtual Service**, on page 4-19

- **Integrating the VMware Guest operating system**, on page 4-22
  - **Mounting the Virtual Server CIFS share**, on page 4-22
  - **Generating an ARX Metadata Report**, on page 4-25

Configuring the ARX

In this section, we configure the ARX to access the external storage devices. We create a CIFS namespace with two shares added to it. The shares are incorporated into a managed volume. The storage volumes are organized into an ARX Share Farm.

**Tip**

Familiarize yourself with the ARX Common Operations page on the ARX configuration utility. Most of the following procedures start from the Common Operations page.

Configuring Active Directory Authentication

The first task in configuring the ARX device is to add an Active Directory Authentication Server. There are three procedures required to add an Active Directory Authentication device: Adding an NTLM Authentication Server, adding a Proxy user, and adding the ARX device to the Active Directory Forest.

Adding the NTLM Authentication Server

The first procedure is to add the NTLM authentication server.
To add the NTLM authentication server

1. In a web browser, open the ARX Manager user interface.
2. From the navigation pane, expand Authentication, and then click NTLM Auth. Servers.
3. Click the Add button.
4. In the NTLM Auth. Server Name box, type the Fully Qualified Domain Name (FQDN) name of the server.
5. In the IP address box, type the IP address of the server.
6. In the Windows Domain box, type the Windows Domain. In our example, we type acme.com.
7. In the Secure Agent password box, type the Secure Agent Password. The Secure Agent password is the password assigned on the Domain Controller for the Secure Agent application. Repeat the password in the Confirm Secure Agent Password box.
8. Click OK.

Figure 4.2 Adding a new Authentication Server

Assigning Backup Operator Privileges

The Proxy User as defined on the ARX is an Active Directory User that is used to access the backend filer shared volumes. This user must be assigned a special privilege in order to access the files. The Backup Operator is a special operator allowed to access all files and directories of a volume in a non-interactive manner.

This privilege should be applied to the local group within each external filer the ARX will manage.

The ARX CLI Storage-Management Guide is available on the ARX. The ARX GUI has a Documentation link facilitating access to the pre-installed manuals on each switch. See https://<ARX IP Address>/acopia/docs/cliStorage/cliStorage.pdf

◆ Note

If you have already assigned a Backup Operator, continue with Adding the Proxy user, on page 4-7.
There are multiple ways to configure Backup Operator Privileges. If the filer is a Microsoft Windows server, you can use the server’s computer management interface. The Microsoft Management Console (MMC) is another option. Note that not all filers support MMC. For those filers use the filer’s user interface to configure the equivalent privilege.

Using the MMC, the Local User groups can be configured on the filer remotely. In the following example we manage the local groups of a Windows Server acting as an external filer to the ARX.

**To assign the backup operator using MMC**

1. From a remote client, launch MMC (for example, from the Windows Start menu, click **Run**, and then type **mmc**, and click **Ok**.
   The MMC Console opens.
2. From the **File** menu, click **Add/Remove Snap-in**.
3. Click the **Add...** button. The Add Standalone Snap-in dialog box opens.
4. From the Snap-in list, click **Computer Management**, and then click the **Add** button. The Computer Management dialog box opens.
5. Click the **Another Computer** option button, and then type the IP address or host name of the remote filer. In our example, we type `\10.10.10.1`.
6. Click the **Finish** button, and then click the **Ok** button on the Add/Remove Snap-in page.
   You return to the MMC console.
7. From the MMC navigation pane, expand Computer Management for the server you just added. Under Computer Management, expand **Local Users and Groups**, and then click **Groups**.
The local groups for the server appear on the right.

![MMC Console to the Local Users Groups.](image)

8. Double click **Backup Operator**. The Backup Operator Properties open. The list will most likely be empty.

9. Click **Add** to add the domain user to the list of Local Backup Operators. The select user dialog box opens.

10. Type the ARX Active Directory (AD) Proxy User user name and click **Check Names**. Be sure to provide an accurate Active Directory user name. In our example, **acmeuser001** is our Proxy User. Click **OK**. The Enter Network Password dialog box opens.

11. In the **User name** and **Password** boxes, type the AD Administrative credentials, and then click **OK** (in order to add an AD user to the local groups, Administrative privileges are required).
The select users dialog box opens with the fully qualified name of the domain user.

12. Click **OK**. The backup operator properties screen opens with the AD user successfully added to the Backup Operator Local Group.

13. Click the **OK**.

The backup operator configuration is complete. We recommend you save this Console session for future use.
Adding the Proxy user

The next task is to create a Proxy User on the ARX system. This is the Active Directory user that was assigned as the Backup Operator. These user credentials are used to access the backend filer CIFS shares.

**To create a proxy user**

1. From the navigation pane, expand Authentication, and then click CIFS Proxy users.
2. Click the Add button.
3. In the Proxy User name box, type the name. In our example, we type acmeuser.
4. In the Proxy User Account box, type the proxy user account. In our example, we type acmeuser001.
5. In the Proxy User Account Password, type the password. Retype the password in the Confirm Proxy User Account Password box.
6. In the Windows Domain and Pre Win2k Domain boxes, type the appropriate Windows Domain. In our example, we type acme.com and acme in the boxes.
7. Click the Save button.

![Add CIFS Proxy User](image)

*Figure 4.5 Adding a CIFS Proxy User*

Adding the ARX device to the Active Directory Forest

The final procedure in this section is to add the ARX Switch to the Active Directory Forest.

**To add the ARX device to the Active Directory Forest**

1. From the navigation pane, expand Authentication, and then click Active Dir. Forests.
2. Click the Add button.
3. In the Forest Name box, type a name for this forest. In our example, we type acme.
4. From the **Domain Type** list, select **forest-root**.

5. In the **Domain Name** box, type a name for this domain. In our example, we type **acme.com**.

6. In the **Domain Controller IP** box, type the Domain Controller IP address. In our example, we type **10.60.112.10**.

7. Check the **Preferred**, **KDC** and **DNS** boxes.

8. Click the **OK** button.

**Figure 4.6 Adding an Active Directory Forest**

The Active Directory authentication configuration is complete. Use the following procedure to verify the ARX has joined the Active Directory domain.

**Verifying the Active Directory Authentication**

To verify that the ARX is properly joined to the Active Directory domain, log into the ARX using the SSH command line management interface, and type the following command:

```
show active-directory status
```

The output should look similar to the following. Verify the **Status** state is Active:

```
arx500-1# show active-directory status
Offline timeout is set to 2000 milliseconds.

PROCESSOR 1.1:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Domain Controller IP</th>
<th>Status</th>
<th>Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME.COM</td>
<td>10.60.112.10</td>
<td>Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

If the Status state is not active, try the following troubleshooting steps:

1. Verify the user admin user credentials are correct.
2. Review the syslog output. GUI: maintenance tab->Logs->syslog and/or traplog. Review for error statements.

3. From the CLI: `show logs syslog` and `show logs traplog`

4. From the CLI: `show active-directory domain acme.com` and double check IP address of the Domain Controller

**Creating the CIFS Namespace**

The next task to create the CIFS Namespace.

**To create the CIFS Namespace**

1. From the left navigation pane, click **Common Operations**.

2. Click the **Create Namespace** button. The Create Namespace wizard opens.

3. In the **Namespace name** box, type a name. In our example, we type **Content**.
   You can optionally type a description.

4. From the **Protocol** options, click the **CIFS** box, and then click **Next**.

![Namespace creation dialog](image)

5. From the CIFS authentication information screen, click the **Use Kerberos** and **Use NTLM** boxes.

6. Click the **Next** button.
Creating a Managed Volume

The backend filer CIFS shares will be incorporated into an ARX Managed Volume. File placement policy is managed at the volume level. The volume attributes to be defined are namespace, volume name, description, CIFS parameters, and the metadata store mount point. In this example, we place the Volume Metadata onto the incumbent legacy storage platform. ARX best practices state Metadata should be created on an NFS export if one is available. Alternatively, a CIFS share could be used.

To create a managed volume

1. From the left navigation pane, click **Common Operations**.
2. Click the **Create Volume** button. The Create Volume wizard opens.
3. From the **Namespace** list, select the name of the namespace you created in **Creating the CIFS Namespace**, on page 9.
   In our example, we select **Content**.
4. In the **Volume name** box, type the volume name. In our example, we type /data. You can optionally add a description. See Figure 4.9.
5. Click the **Next** button.
6. From the Metadata file server protocol list, select an appropriate protocol. In our example, we select NFSv3-UDP.

7. From the Metadata file server list, select the file server if it has already been configured. In our example, the external filer has not yet been configured, so we click the Add button.

   a) In the Name box, type a name for the file server. In our example, we type netapp.

   b) In the Primary IP address box, type the IP address of the filer.

   c) Configure the other options as applicable for your configuration. In our example, we leave the defaults.

   d) Click the Save button. You return to the Volume metadata page.

Figure 4.9  Creating a Volume

Figure 4.10  New External filer for the MetaData database
8. On the Metadata page, click **Next**.

9. From the CIFS Parameters page, in the Auto-synchronization section, click the **Auto-synchronize** box.

10. In the CIFS Attributes section, click the **Auto-detect CIFS attributes** box. Click the **Next** button.

11. From the Volume Parameters page, in the Performance Tuning section, from the **VPU ID** list, select **Dynamic**. Ensure the **Auto Reserve files** box is checked.

12. In the Enable Volume section, click the **Enable the volume when finished** button (see Figure 4.12).

13. Click the **Next** button.

14. Review the summary, and click **Finish**.
Adding the External Filers

In this section we will add the external filer entries to the ARX. This entry is referenced later when we add the filer shares to the managed volume.

To add the External Filers

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

First file share we will add is the root level share. This is the incumbent legacy storage volumes with file content. The subsequent shares to be added will adapt to the root volume permissions.

To add a root level share

1. From the left navigation pane, click Common Operations.
2. Click the Add Share button. The Add Share Wizard opens.
3. In the Share Name box, type a name for this Share. In our example, we type share1.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 4-9. In our example, we select **Content**.

5. From the **Volume** list, select the name of the Volume you created in *Creating a Managed Volume*, on page 4-10. In our example, we select **/data**. Click the **Next** button.

6. From the **File Server** list, select the name of the file server you created in *Adding the External Filers*, on page 13. In our example, we select **filer1**.

7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share1**.

8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes (see Figure 4.15).

9. Optional: You can select the ability for the ARX to take ownership if the share is owned by another ARX by clicking the **Allow this switch to import this share, even if it's owned by another Acopia switch box**.

10. Make sure the **Enable this Share when finished** box is checked.

11. Click the **Next** button.

12. Review the summary, and click the **Finish** button.
Adding a second CIFS Share

Now add as second share to the managed volume. This share will be used in a share farm. A share farm is a way to add storage to an existing manage volume and is often used to build a load balanced environment for storage access. This new share will be on a second external filer named filer2.

**To add a root level share**

1. From the left navigation pane, click **Common Operations**.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **share1**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 4-9. In our example, we select **Content**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a Managed Volume*, on page 4-10. In our example, we select **/data**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in *Adding the External Filers*, on page 4-13. In our example, we select **filer2**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share2**.
8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes. Also, click **Synchronize directory attributes between shares on import** so the new volume inherits the root share attributes. (see Figure 4.16).

9. Make sure the **Enable this Share when finished** box is checked.

10. Click the **Next** button.

11. Review the summary, and click the **Finish** button.

---

**Figure 4.16** Specify the external filer, share name, and attributes.

---

**Creating the Share farm**

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

In this example we will group the two previous added shares together.

**To create a share farm**

1. From the left navigation pane, click **Common Operations**.

2. Click the **Load Balancing** button.
   The Load Balancing Wizard opens.

3. In the **Policy Name** box, type a name. In our example, we type **ShareFarm**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 4-9. In our example, we select **Content**.

5. From the **Managed volume** list, select the name of the Volume you created in *Creating a Managed Volume*, on page 4-10. In our example, we select **/data**. Click the **Next** button.

![Create Share Farm wizard](image1)

*Figure 4.17 Create Share Farm wizard*

6. On the Shares page, click the boxes for the file shares to be included in the share farm. In our example, we click the boxes for **share1** and **share2**.

![Select the shares to include](image2)

*Figure 4.18 Select the shares to include*

7. On the Load Balancing page, select a load balancing algorithm and choose one of the constraint options. In our example, we leave these settings at the default levels.

![Configuring the load balancing algorithm and options](image3)

*Figure 4.19 Configuring the load balancing algorithm and options*
8. Make sure the **Enable this load balancing policy when finished** box is checked.

9. Click the **Next** button.

10. Review the summary, and click the **Finish** button.

---

### Creating the Virtual Service

The Virtual Service is how the ARX presents CIFS Shares to the network clients. Clients send file requests through the Virtual Service and the ARX proxies these requests to the appropriate backend filer.

The VMware guest operating system nodes connect to the Virtual service IP and map the share to an unused drive letter.

**To create the virtual service**

1. From the left navigation pane, click **Common Operations**.

2. Click the **Create Virtual Services** button. The Add Virtual Service Wizard opens.

3. From the **Namespace** list, select the namespace you created in *Creating the CIFS Namespace*, on page 4-9. In our example, we select **Content**.

4. Click the **Create a new virtual service (VIP)** button.
   a) In the **Virtual service DNS name** box, type the DNS name for the virtual service. In our example, we type **share.acme.com**.
   b) In the **IP Address** box, type the IP address of the VIP. In our example, we type **172.30.72.102**.
   c) In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.192**.
   d) From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **302**.

5. Ensure the **Enable the virtual service when finished** box is checked.

6. Click the **Next** button.
Deploying the ARX with VMware ESX Servers for Shared Content Access

Figure 4.20 Virtual Service creation

7. On the Windows Domain page, from the Windows Domain Name list, select the appropriate domain. In our example, we select acme.com.

8. In the Pre Win2k Domain box, type the Pre Win2k domain. In our example, we type acme. Click Next.

9. On the Export page, from the Volume list, select the Volume you created in Creating a Managed Volume, on page 10. In our example, we select /data.

10. In the Volume Path box, type the path. In our example, we type /. 

11. In the Export Name box, type a name for the export. In our example, we type share. You can optionally type a description (see Figure 4.21).

12. Click the Add Export button.

13. Click the Next button.

14. Review the summary, and click the Finish button.
You can review the Virtual Service by clicking Virtual Services in the navigation pane. The admin state shows enabled and the status shows ready.

**Figure 4.21 Virtual Service file share export**

**Figure 4.22 Virtual Service Summary**
Integrating the VMware Guest operating system

In this section, we show how the Windows Guests can access the ARX Virtual Service and the managed volume CIFS share. This process is the same process to follow if the client is a virtual machine or a physical machine. One of the many benefits of virtual machines is their ability to be mobile. The ARX adds flexibility with the Managed Volume and Virtual Services that creates a robust virtual machine environment providing continuous access to data content as VMs migrate from one data center to the next.

The following list of items will be configured in order to integrate and verify client access to the ARX Virtual Service.

- Mounting the Virtual Server CIFS share, on page 4-22
- Generating an ARX Metadata Report, on page 4-25

Mounting the Virtual Server CIFS share

In this section, we confirm that the Virtual Service is operating properly by mapping a network drive to the Virtual Service Export from a VMware Guest Windows Client. You can either start a Remote Desktop Session to the guest, or access the guest console through the VMware vSphere client and clicking the console tab.

The next step is to map the 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 Y.
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 \share.acme.com\share.
4. Click the **Connect using a different user name** link. In the **User name** and **Password** boxes, type a domain user with the proper access rights. In our example, we use the Proxy User credentials.

**Figure 4.25 Connect As the Acmeuser001 user credentials**

Microsoft Windows mounts the drive. The drive can be explored and the following screen displays the file contents of the virtual service export.
Deploying the ARX with VMware ESX Servers for Shared Content Access

The export shows the files and directories that exist. The user cannot determine which of the two backend file shares the files reside on. The ARX has merged the files and directories into one common virtual path.

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

The volume statistics can be viewed from the ARX GUI by clicking the Managed Volume tab in the left pane. Select the /data volume. In our example the volume contains 60 file distributed within 41 directories (see Figure 4.27).
Generating an ARX Metadata Report

The file placement can be determined by executing an ARX report. The administrator can also view the directory contents on the backend servers and see how the files are placed. In this section, we demonstrate how to create an ARX Report.

To generate an ARX Metadata Report

1. From the navigation pane, click Managed Volumes.
2. From the Volume column, click the name of the appropriate volume. In our example, we click /data.
3. Click the Report button.
4. In the Path box, type /.
5. In the Report Type row, click Metadata.
6. In the **Output Report Name** box, type a name for the report.

7. Click the **OK** button.

![Figure 4.28 Volume Report](image)

The report is generated and is accessible by clicking Reports in the navigation pane, then clicking the name of the report you just created. The following snippet of the report displays filenames and the file shares they are located on.

```
**** Software Version: 5.00.001.11704 (Jun 24 2009 22:25:14) [nbuids]
**** Hardware Platform: ARX-1000
**** Report Destination: Content
**** Volume: /data
**** Path: /

<table>
<thead>
<tr>
<th>Share</th>
<th>Physical Filer</th>
</tr>
</thead>
<tbody>
<tr>
<td>[share1]</td>
<td>10.10.10.2:share1</td>
</tr>
<tr>
<td>[share2]</td>
<td>10.10.10.3:share2</td>
</tr>
</tbody>
</table>

**** Legend:
**** FL = File: The reported entry is a file.
**** DR = Directory: The reported entry is a directory.
**** 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.
```
Conclusion

This chapter of the deployment guide demonstrated the way to integrate F5 ARX platform with VMware Guest operating systems. The deployment enables the virtualized servers to mount a common content share. This facilitates a site to site failover of both Virtual Servers as well as the data content they need access too. The ARX external filers can replicate the content between data centers and when a failover is initiated these replication peers can present the same content to the virtual servers that was presented in the primary site.

For more information on configuring the F5 ARX, refer to the documentation, available on Ask F5.
Configuring the ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume

- Configuring Windows Server 2008 for the ARX
- Configuring the ARX
- Verifying Client access
Deploying the F5 ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume

This chapter illustrates how the F5 ARX can interoperate with VMware® Virtual Machines running Microsoft® Windows® Server 2008. The Windows Virtual machines boot from the VMware Virtual Machine Disk Format (VMDK) datastore and present CIFS shares to the ARX to be managed as Tier-2 external filers.

When the performance of one virtualized windows server is exceeded, the system administrator can add additional virtualized servers and incorporate them into the managed volume to meet the performance and storage capacity needs.

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

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this deployment:

- This document is based on ARX version 5.0.1

- We assume the ARX is configured for network access and the initial switch interview has been completed. If not, refer to the ARX Hardware Installation guide for specific details.

- The example scenario in this deployment guide is based on the following:
  
  - The Tier 1 external filer storage is pre-configured and available as a network resource.
  
  - Three Windows Server 2008 VMware Guest OS systems are installed and available as a network resource.
  
  - Microsoft Active Directory Domain is preconfigured and the F5 Secure Agent is installed.

- The ARX is deployed in production environments in a high availability pair. This guide demonstrates how to configure the first of the two clustered ARX switches.
Configuring the ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume

Product versions and revision history

Products and versions tested for this deployment guide:

<table>
<thead>
<tr>
<th>Product Tested</th>
<th>Version Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5 Acopia ARX</td>
<td>5.0.1</td>
</tr>
<tr>
<td>VMware ESX</td>
<td>3.5.0 or later</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008</td>
<td>2008</td>
</tr>
<tr>
<td>Microsoft XP Client</td>
<td>XP SP3</td>
</tr>
</tbody>
</table>

Configuration example

In the following diagram, we show basic connectivity between clients, the ARX, and Virtual Machines accessing content shares. The VMware virtual machines operate within the ESX provisory. These VMs share network storage to be managed by the ARX.

The ARX manages the CIFS shares from the data center LAN into a single managed volume. This volume is shared to the client LAN with an ARX Virtual Service. Clients do not have direct access to the data center LAN.

Figure 5.1 Logical configuration example
Configuring Windows Server 2008 for the ARX

In this section, we configure the Windows 2008 Servers. You must complete the following tasks on the each Windows Server:

- **Joining the Active Directory Domain**, on page 5-3
- **Initializing a new VMware storage device**, on page 5-4
- **Initializing the Windows Server 2008 Disk**, on page 5-5
- **Creating a CIFS File Share**, on page 5-7
- **Assigning the Local Backup Operator**, on page 5-8

◆ Note

You must complete the following procedures for each of the Windows 2008 Servers to be included in the ARX Managed Volume. In our example, we repeat the procedures for the three Windows 2008 Servers in our implementation.

Joining the Active Directory Domain

The first task is to authenticate the file servers to the Active Directory (AD) Domain Controller. This adds the file servers into the Domain as Domain Computers and registers the IP addresses with DNS.

**To join the Active Directory domain**

1. Use RDP to connect to the server, or open the server console with the VMware vSphere client.
2. From the Windows **Start** menu, click **Control Panel**.
3. On the Control Panel screen, click **System**. The System Properties screen opens.
4. Under **Computer name, domain, and workgroup settings**, click **Change Settings**.
5. Click the Computer Name tab, and then click the **Change** button.
6. In the Member of section, click the **Domain** button, and type the appropriate domain in the box.
7. Click the **OK** button.
8. When prompted, type the **User Name** and **Password** of an account with domain administrator permissions.
9. Click the **OK** button. You see a Welcome to the domain message. If you do not, double-check your DNS server settings, administrator credentials, or basic network connectivity to the domain controllers.
10. You must restart the computer to apply the changes. We recommend shutting down the Windows Server 2008 device instead of rebooting.
Configuring the ARX for VMware ESX virtualized Windows Server 2008 in a Managed Volume

### Initializing a new VMware storage device

The next task is to configure a new storage device. In this section, we create a new Hard Drive using the VMware VSphere Client which is subsequently initialized by the Windows Server. Note that this process needs to occur with the VM shutdown.

**To initialize a new VMware storage device**

1. Launch the VMware vSphere client.
2. From the navigation pane, select the appropriate virtual machine. In the main pane, click *Edit virtual machine settings*. The properties box opens.
3. On the Hardware tab, click the *Add* button. The Add Hardware wizard opens.
4. Click *Hard Disk*, and then click *Next*.

![Add Hardware Wizard](image)

*Figure 5.2 Add Hardware Wizard*

5. In the Disk box, ensure *Create a new virtual disk* is selected. Click *Next*.
6. From the *Disk* list, select or type a number for the virtual disk size. In our example, we type *10* and select *GB* for the disk size (see Figure 5.3). Click *Next*.
7. On the Advanced Options page, configure as applicable. In our example, the Windows 2008 Virtual Machine is installed with a Virtual SCSI controller. VMware selects the next available LUN by default. We leave all settings at the default, and then click *Next*. 
8. Review the options and then click **Finish**. The system creates the disk and the virtual machine properties page opens with the new disk highlighted with a status of Adding.

9. Click **OK** to close the properties box.

10. Click **Play** to power on the virtual machine.

### Initializing the Windows Server 2008 Disk

The next task is to use the Windows Disk Manager to initialize and format the new virtual disk.

**To initialize the new virtual disk**

1. From the **Start** menu, select **Administrative Tools**, and then click **Computer Management**. Expand the **Storage** menu and then click **Disk Management**.
   
The Computer Management screen opens, and you see the disk you just created in the list.

2. If the new disk has a status of Offline, right-click the disk and then select **Online**.
To initialize the disk, right-click the disk and click Initialize Disk.

Leave the partition style at MBR (Master Boot Record). Click OK. The disk state should now show Basic and online.

Next, we create and format a simple volume.

Right-click the disk you just initialized, and select New Simple Volume. The New Simple Volume Wizard opens.

Click the Next button to start the wizard.

In the Simple Volume Size in MB box, type the maximum disk space, as we want the volume to be the entire disk. Click Next.

Make sure Assign the following drive letter is selected, and choose a letter from the list. In our example, we select F. Click Next.
9. On the Format Partition page, click Format this volume with the following settings button, and complete the following:
   
a) From the **File System** list, select **NTFS**.
   
b) From the **Allocation unit size** list, you can select a unit size. We leave this setting at the **Default**.
   
c) In the **Volume label** box, type a name. In our example, we type **Share Volume**.
   
d) Check the **Perform a quick format** box.
   
e) Click **Next**.

![Format Partition page](image)

**Figure 5.6** Format Partition page

10. Review the new volume parameters, and then click **Finish**. The disk reports the status of **Healthy (Primary partition)**.

    Keep the Disk Management utility open and proceed to the next section to share the new drive.

**Creating a CIFS File Share**

The disk is ready to be shared on the network as a CIFS network device file share. The drive sharing is a simple task. The CIFS share name is what the ARX imports into a managed volume.

**To create the CIFS file share**

1. From the Disk Management utility, right-click the drive (Share Volume (F:) in our example) and select **Properties**. The drive properties window opens.
2. Click the Sharing tab, and then click the Advanced Sharing button.
3. On the Advanced Sharing page, click the Share this folder box.
4. In the Share name box, type a name, and then click the Add button. In our example, we type share1.

![Advanced Sharing](image)

Figure 5.7 Advanced Sharing

5. You can optionally limit the number of simultaneous users. We recommend not limiting the number of users.
6. Click the Permissions to set the Share Level permissions. The permissions box opens.
7. Check the Allow boxes for Full Control and Change.
8. Click OK.
9. Click OK again on the Advanced Sharing settings page, and then click Close to complete the creation of the CIFS share.
10. **Important:** Repeat this procedure for each Windows 2008 server to be included in the ARX Managed Volume. For simplicity name each share sequentially (for example share1, share2, share3).

Assigning the Local Backup Operator

The next task is to assign Local Backup Operator rights to the Windows Servers for the Active Directory Domain User. This is the ARX Proxy User and is required in order to allow the ARX to perform various directory and file transactions.
◆ Tip

For the following advanced features the ARX proxy user should be assigned to the Local Administrators group: Access based Enumeration (import and priv-exec), Filer subshares (Export and replicate), Share enable replicate / export subshares, and snapshot creations. These features are not a part of this deployment guide.

To assign a local backup operator

1. Use RDP to connect to the server, or open the server console with the VMware vSphere client.
2. From the Windows Start menu, navigate to Administrative Tools, and then select Computer Management.
3. From the navigation pane, expand System Tools, expand Local Users and Groups, and then click Groups.
4. Double-click the Backup Operator group. The Backup Operators Properties page opens. Click the Add button.
5. In the Enter object names to select box, type the domain user with administrative credentials and then click Check Names. If multiple names return, select the correct user and then click OK.
6. Type the network password, and then click OK. You return to the Select Users, Computer, or Groups box.
7. Click OK. You return to the Backup Operator Properties box, and the new user is now a Member of the local backup operators group.
8. Click OK to finish.

This completes the Windows Server 2008 configuration. Be sure to repeat these procedures for each of the Windows 2008 Servers to be included in the ARX Managed Volume.
Configuring the ARX

This section we configure the ARX to access the external storage devices. We create a CIFS namespace with 4 shares added to it. The first share is the Root Level share and is the Tier-1 filer. The remaining 3 shares are the Virtualized Windows Servers. The shares are incorporated into a managed volume. The storage volumes are organized into an ARX Share Farm.

Configuring the Active Directory Authentication

The first task in configuring the ARX device is to create a new Active Directory (AD) Authentication server.

To create the active directory authentication server

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

Figure 5.8 Create a new Authentication Server
Creating a Proxy User

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

**To create a proxy user**

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

Adding the Active Directory Forest details

The next task is to add the Active Directory Forest details to the ARX.

**To add the Active Directory Forest details**

1. From navigation pane, expand **Authentication**, click **Active Dir. Forests**, and then click the **Add** button.
2. From the **Domain Type** list, select **forest-root**.
3. In the **Domain Name** box, type the Domain name. In our example, we type **siterequest.com**.
4. In the **Domain Controller IP** box, type the Controller IP.
5. Check the **Preferred**, **KDC**, and **DNS** boxes, and then click the **Add** button.

   The active Directory authentication configuration is complete.

Verifying Active Directory Authentication

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

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


```
arx500-1# show active-directory status

Offline timeout is set to 2000 milliseconds.
```

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Domain Controller</th>
<th>Status</th>
<th>Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>SITEREQUEST.COM</td>
<td>10.60.112.10</td>
<td>Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Verify that the Status state is Active.

**Creating the CIFS Namespace**

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

**To create the CIFS namespace**

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

![CIFS namespace wizard](image)

**Figure 5.9 CIFS namespace wizard**

5. In the CIFS authentication protocol section, check the **Use Kerberos** and **Use NTLM** boxes.
6. In the Proxy User section, type the name of the proxy user. In our example, we type **acmeuser001**. Click the **Next** button.
7. Click the **Finished** button.
Creating a volume

The backend filer CIFS shares will be incorporated into an ARX Managed Volume. File placement policy is managed at the volume level. In this example, we place the Volume Metadata onto the incumbent legacy storage platform. ARX best practices state Metadata should be created on an NFS export if one is available. Alternatively, a CIFS share could be used.

To create the managed volume

1. From the navigation pane, click Managed Volumes, and then click the Add button.
2. From the Namespace list, select the name of the namespace you created. In our example, we select Content.
3. In the Volume Name box, type the name for the volume. In our example, we type /data. You can optionally type a description.
4. Click Next.
5. From the Metadata file server protocol list, select NFSv3-UDP.
6. From the Metadata file server row, click the Add button to create an external filer. The new file server wizard opens. Complete the following:
   a) In the Name box, type a name for this File Server. In our example, we type netapp.
   b) In the Primary IP Address box, type the primary IP address.
   c) In the Secondary IP Address box, type any secondary IP addresses, and click the Add button. In our example, we do not include any secondary IP addresses.
   d) In the Description box, you can optionally type a description.
   e) Make sure there is a check in the This file server supports snapshots box.
   f) From the File Server Type list, select NetApp.
      In order to allow the ARX access to these filers (EMC, NetApp, Windows) management access is required.
   g) In the Management IP Address box, type the management IP address.
   h) From the Management Protocol list, select the appropriate protocol. In our example, we select SSH.
   i) In the Management Proxy User box, type the proxy user. In our example, we type root.
   j) In the Ignore Directories (optional) box, type any snapshot directories the ARX should ignore, and click the Add button. In our example, we type .snapshot, ~snapshot.
k) Click the **Save** button. You return to the managed volume wizard.

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

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

9. Check the box in the **Auto-synchronization** section, and then check the **Auto detect CIFS Attributes** box. Click **Next**. The Volume parameters page opens.

10. Configure the Performance Tuning section as applicable for your configuration.

11. Click the **Files and directories can be renamed during import and re-import** button.

12. Check the **Enable the volume when finished** box, and then click **Next**.

13. Review the summary, and then click **Finish**.

---

### Adding the External Filers

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

**To add the External Filers**

1. From the navigation pane, click **File Servers**.

2. Click the **Add** button. The Add File Server screen opens.

3. In the **Name** box, type a name for this File Server. In our example, we type **filer1**.

4. In the **Primary IP Address** box, type the primary IP address. In our example, we type **10.10.10.2**.

5. In the **Secondary IP Address** box, type any secondary IP addresses, and click the **Add** button. In our example, we do not include any secondary IP addresses.

6. In the **Description** box, you can optionally type a description.

7. In the **Ignore Directories (optional)** box, type any snapshot directories the ARX should ignore on the backend file shares, and click the **Add** button.

8. Click the **OK** button.

9. Repeat this entire procedure for additional filers. In our example, we repeat this procedure twice and name the filers **filer2** and **filer3**. We add the additional files to facilitate building a share farm that consists of a share from three separate filers for concatenating and load balancing access to the storage devices.
Adding the root level share

First file share we will add is the root level share. This is the incumbent legacy storage volumes with file content. The subsequent shares to be added will adapt to the root volume permissions.

To add a root level share

1. From the left navigation pane, click **Common Operations**.
2. Click the **Add Share** button. The Add Share Wizard opens.
3. In the **Share Name** box, type a name for this Share. In our example, we type **Share0**.
4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 5-12. In our example, we select **Content**.
5. From the **Volume** list, select the name of the Volume you created in *Creating a volume*, on page 5-13. In our example, we select **/data**. Click the **Next** button.
6. From the **File Server** list, select the name of the file server you created in step 6a of *Adding the External Filers*, on page 5-14. In our example, we select **netapp**.
7. In the **CIFS Share** box, type the name of the CIFS share. In our example, we type **share0**.
8. In the Import Conflict Resolution section, check the **Rename files with naming collisions on import** and **Rename directories with naming collisions on import** boxes (see Figure 5.10).
9. Click the **Next** button.
10. Review the summary, and click the **Finish** button.
11. **Important**: Repeat this procedure to add the virtualized Windows 2008 shares to the managed volume. These are the shares from the filers you created in *Adding the External Filers*, on page 14 (Filer1, Filer2, and Filer3 in our example). These shares are used in a share farm. A share farm is a way to add storage to an existing manage volume and is often used to build a load balanced environment for storage access.
    Give the shares a unique name, and from the **File Server** list, select the appropriate file server (filer1, filer2 and so on).

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

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

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

**To create the Share farm**

1. From the left navigation pane, click Common Operations.
2. Click the Load Balancing button. The Load Balancing Wizard opens.
3. In the Policy name box, type a name for this policy. In our example, we type Sharefarm.
4. From the Namespace list, select the name of the namespace you created in Creating the CIFS Namespace, on page 5-12. In our example, we select Content.
5. From the Managed volume list, select the name of the Volume you created in Creating a volume, on page 5-13. In our example, we select /data. Click the Next button.
6. Click the boxes of the file shares to be included in the share farm. In our example we select the **share1**, **share2**, and **share3** file shares. Click the **Next** button.

![Select the shares to include](image.png)

*Figure 5.11* Select the shares to include

7. From the **Load Balancing Algorithm** list, select an appropriate load balancing method. In our example, we select **Round-Robin**.

8. In the Constraint Options section, click the **Place new files in the same shares as their parent directories** box.

9. In the Enable section, ensure the **Enable this load balancing policy when finished** box is checked.

10. Click the **Next** button.

11. Review the summary and then click the **Finish** button.

### Creating a Tiered Storage policy

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

#### To create the file placement policy

1. From the left navigation pane, click **Common Operations**.

2. Click the **Tiered Storage** button. The Tiered Storage Wizard opens.

3. In the **Policy name prefix** box, type a prefix. In our example, we type **Tiering**.

4. From the **Namespace** list, select the name of the namespace you created in *Creating the CIFS Namespace*, on page 5-12. In our example, we select **Content**.

5. From the **Managed volume** list, select the name of the Volume you created in *Creating a volume*, on page 5-13. In our example, we select **/data**.
6. From the **Number of tiers** list, select a number of tiers. In our example we select 2. Click the **Next** button.

![Figure 5.12 Tiering Policy Wizard](image)

7. For Tier 1, select the root-level share you created in *Adding the root level share*, on page 5-15. In our example, we select `share0`. Click the **Next** button.

8. For Tier 2, select the second Share farm you created in *Creating the Share farm*, on page 5-16. In our example, we select `Sharefarm`. Click the **Next** button.

9. The next step is to specify the criteria for moving files and the schedule. Click the **Add** button to the right of Schedule to define the schedule to be associated with the policy.

   a) In the **Schedule Name** box, type a name for this schedule. In our example, we type **Tiering Schedule**.

   b) In the **Start Time** fields, you can specify a specific start time. In our example, we leave the fields at the default.

   c) In the Interval section, click the **Hours** button, from the **Hour** list, select 1, and then click the Add button.

   d) The other fields are optional, configure as applicable for your deployment.

   e) Click the **Save** button (see Figure 5.13). You return to the Tiered Storage Wizard.
10. From the **Move files not** list, select **Modified**. In the **In the last** box, type a number and select a time period. In our example, we type **90** and select **days** from the list.

11. From the **Schedule** list, select the schedule you just created if it is not already selected.

12. In the **Enable** box, ensure the **Enable this policy when finished** box is checked.

13. Click the **Next** button.

14. Review the summary and then click the **Finish** button.
Figure 5.14 Specify the Tiering Policy attributes

The Tiered Storage policy is created and migrates files that have not been modified for 90 days or longer to be moved from Tier-1 to Tier-2. This frees up space on the Tier-1 filer by moving inactive data files to lower cost storage filers.

Creating the Virtual Service

The Virtual Service is how the ARX presents CIFS Shares to the network clients. Clients send file requests through the Virtual Service and the ARX proxies these requests to the appropriate backend filer.

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

To create the virtual service

1. From the navigation pane, click Virtual Services.
2. Click the Add button. The Add Virtual Service Wizard opens.
3. From the Namespace list, select the namespace you created in Creating the CIFS Namespace, on page 5-12. In our example, we select Content.
4. Click the Create a new virtual service (VIP) button.
   a) In the Virtual service DNS name box, type the DNS name for the virtual service. In our example, we type share.siterequest.com.
b) In the **IP Address** box, type the IP address of the VIP. In our example, we type **172.30.72.102**.

c) In the **Subnet Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.192**.

d) From the **VLAN ID** list, select the appropriate VLAN ID. In our example, we select **302**.

e) Ensure the **Enable the virtual service when finished** box is checked.

![New Virtual Service Wizard](image)

**Figure 5.15 New Virtual Service Wizard**

5. Click the **Next** button.

6. From the **Windows Domain Name** box, select the Windows domain name. In our example, we select **siterequest.com**.

7. In the **Pre Win2k Domain** box, type the Pre Win2k Windows domain name. In our example, we type **siterequest**.

8. The other settings on this screen are optional, configure as appropriate for your deployment. In our example, we leave the rest of the settings at the default level.

9. Click the **Next** button. The Virtual Service Exports screen opens.

10. In the New Export section, from the **Volume** list, select the Volume you created in *Creating a volume*, on page 5-13. In our example, we select **/data**.

11. In the **Volume Path** box, type the Volume Path. In our example, we type **/**.

12. In the **Export Name** box, type a name for the Export. In our example, we type **share**.
13. Configure the other options as applicable for your configuration, and then click the Add Export button.

14. Click the Next button.

15. Review the summary and then click Finish.

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

16. Check the box for the Virtual Service you just created and then click the Join Domain button.

17. Type the Username, User Password, and the Organizational Unit, and then click OK.

![Figure 5.16 Join Active Directory Domain](image)

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

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

The following list of items will be configured in order to integrate and verify client access to the ARX Virtual Service.

- Mounting the Virtual Server CIFS share, following
- Generating an ARX Metadata Report, on page 5-24

Mounting the Virtual Server CIFS share

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

To map the Virtual Service CIFS Share to drive letter

1. From a Windows client, open Windows Explorer, and, from the Tools menu, select Map Network Drive.
2. Select an unused Drive Letter and the network folder. The folder is comprised of the Virtual Service FQDN and export path.
3. From the Drive list, select an unused Drive Letter.
4. In the Folder box, type the network folder. The folder is comprised of the Virtual Service FQDN and export path. In our example, we type \share.siterequest.com\share.
5. Select Connect using a different user name and specify the Domain User with the proper access rights. In our example, we use the Proxy User credentials.
6. Click Finish. Microsoft Windows mounts the drive. The drive can be explored and the following screen displays the file contents of the virtual service export.
In this example, there are multiple root level directories. Under these directories there is various test content. The content is striped across the backend servers and presented as a unified volume to the client.

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

### Generating an ARX Metadata Report

File placement can be determined by creating an ARX report. The administrator can also view the directory contents on the backend servers and see how the files are placed. In this section, we demonstrate how to create an ARX Report.

**To generate an ARX Metadata report**

1. From the navigation pane, click the **Managed Volumes** and then click the volume (/data in our example).
2. From the Managed Volume Details screen, click **Report**.
3. On the Report Volume page, complete the following:
   a) In the **Path** box, type the path. In our example, we type `/`.
   b) In the Report type row, click **Metadata**.
   c) In the **Output Report Name** box, type a name. In our example, we type `metadata_report`.
   d) Click **OK**.
The ARX generates the report, which is accessible from the navigation pane by clicking Reports, and then clicking the name of the report you just created. Add files to the Virtual Service CIFS share and rerun the report. Wait for the Tiering Policy to be invoked and compare the results of a metadata report from before versus after the policy is executed.

<table>
<thead>
<tr>
<th>Report Volume:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This operation generates a report about the metadata associated with this volume.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>share</td>
</tr>
<tr>
<td>Path</td>
<td>/</td>
</tr>
<tr>
<td>Report Type</td>
<td>Inconsistencies, Metadata</td>
</tr>
<tr>
<td>Output Report Name</td>
<td>metadata_report</td>
</tr>
<tr>
<td>Recurse Subdirectories</td>
<td>Include Subdirectories</td>
</tr>
<tr>
<td>Share</td>
<td>All</td>
</tr>
<tr>
<td>Include File Handles</td>
<td>Include File Handles</td>
</tr>
</tbody>
</table>

Figure 5.18 Volume Report

Conclusion

This deployment guide demonstrated the way to integrate F5 ARX platform with VMware Guest operating systems. The deployment enables the virtualized servers file shares to be used as ARX External Filers. This creates a multi-tiered storage solution for load balancing across multiple virtualized Windows 2008 servers.

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