



Optimizing VMware vMotion and NetApp FlexCache Replication for Long Distance Live Migration with F5

What's inside:

- 4 Configuration table for BIG-IP objects
- 6 Configuration table for ESX, NetApp, and Servers
- 8 Performing the BIG-IP system initial configuration tasks
- 12 Configuring NetApp FlexCache
- 17 Configuring VMware ESX servers
- 18 Configuring VMware VMkernel for vMotion
- 22 Configuring the BIG-IP WAN Optimization Module
- 33 Managing VM hosts, VM storage and client traffic
- 36 Configuring the BIG-IP GTM
- 39 Appendix A: Configuration worksheets
- 41 Appendix B: Frequently Asked Questions

F5® BIG-IP® WAN Optimization Module™ (WOM) enables VMware® vMotion® long distance live migration and optimizes NetApp® FlexCache® replication. BIG-IP WOM creates opportunities to architect virtual data center solutions and allows administrators to move entire pools of virtual machines from one data center to another. In this guide, we describe how to use BIG-IP WOM to optimize vMotion for ESX, how to optimize storage vMotion using NetApp FlexCache and how to maintain user connections between data centers during the virtual machine moves.

The key benefits of using BIG-IP WOM include:

- Increase Performance - Improves vMotion and FlexCache transfer times.
- Increase Efficiency - Maximizes bandwidth use.
- Cost Savings - Reduces WAN costs and offloads CPU-intensive processes from the servers.
- Improve Security - Encrypts vMotion transfers over the WAN.

In this guide, we provide step-by-step instructions on how to configure the BIG-IP system, VMware ESX and NetApp FlexCache devices for long distance live migration. Because long distance live migration is a two data center solution, we advise that you have access to BIG-IP systems, NetApp devices, and ESX servers in both data centers before starting. In this guide we alternate configuration between the primary and secondary data center in order to make configuration as simple as possible.

For more information on the F5 devices in this guide, see <http://www.f5.com/products/big-ip/>

Products and versions tested

Product	Version
BIG-IP WOM	10.2
VMware vMotion	ESX vSphere 4.0 and 4.1
NetApp FlexCache	Data ONTAP Release 7.3.4

See *Document Revision History* on page 46 for a list of modifications to this guide.

Prerequisites and configuration notes

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

- You must have the WAN Optimization module licensed and provisioned on your BIG-IP systems.

In this document, we typically refer to the *primary* and *secondary* data centers on the BIG-IP systems. The WAN optimization module user interface and documentation uses the terms *local* and *remote*.

- The BIG-IP system must be running version 10.2 or later.
- You must have ESX vMotion and Storage vMotion licenses.
- You must have NetApp FlexCache licensed on your NetApp device.
- VMware vMotion uses TCP port 8000. This port must be allowed to be initiated between the two data centers and between the two ESX servers.
- BIG-IP iSessions use TCP port 443. This port must be allowed to be initiated between the two data centers.
- NFS traffic uses TCP port 2049. This port must be allowed to be initiated between the two data centers. See NetApp FlexCache documentation for further information.
- VMware vMotion preserves all network settings of a virtual machine. While moving a machine between two data centers, the IP and network configuration for the migrated hosts between the two data centers must be identical. However, the infrastructure does not need to be part of the same layer 2 broadcast domain.
- For verification and troubleshooting purposes, we assume you are able to issue ICMP **ping** commands and that they are allowed in your network.

ICMP ping is being used only for verification and troubleshooting in configuration checkpoints in this document and is not part of the solution.

- We assume that there is a private connection between the primary and secondary data center. For example, an IPSec tunnel, a point-to-point fibre connection, an MPLS connection, and so on.
- The use of EtherIP tunnels as described in this document adds 2 bytes of IP overhead, and in conjunction with IPSec tunnels may result in packet fragmentation. We recommend tuning the MTU values in your network to prevent fragmentation. The specific amount of tuning depends on your topology and data center-to-data center transport technology.
- vCenter in your primary data center must be able to initiate connections to ESX hosts in both the primary and secondary data centers from the VMkernel service console. TCP ports 443 and UDP ports 902 are used (UDP 902 for heartbeat and error checking).

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

Configuration example

In our configuration example for this document, we modify a primary and secondary data center to be able to participate in long distance live migration for memory and storage. Our use case in this scenario is for disaster avoidance, a preemptive move of VMware guests to mitigate an issue in the primary data center.

The components of our architecture include:

- ESX Servers in the primary and secondary data center
- NetApp devices used for ESX storage in both data centers
- BIG-IP devices with the LTM and WOM modules in both data centers. Our BIG-IP devices serve two purposes, first to handle Application Delivery for users on the Internet (e.g., Load Balancing) and second, the BIG-IP WAN Optimization Module (WOM) enables long distance live migration.
- BIG-IP GTM, a separate physical device in our example, provides traffic direction based on where the ESX Virtual Servers are located.

Between the two data centers we establish two connections handled by the BIG-IP devices and carried over transport technologies such as IPSec or MPLS. First, BIG-IP iSessions connect and accelerate the two data centers to enable vMotion traffic. Second, a BIG-IP EtherIP tunnel connects the two data centers to carry established connections until the connections are complete.

In summary, iSessions enable and accelerate vMotion traffic while EtherIP provides an uninterrupted user experience during vMotion.

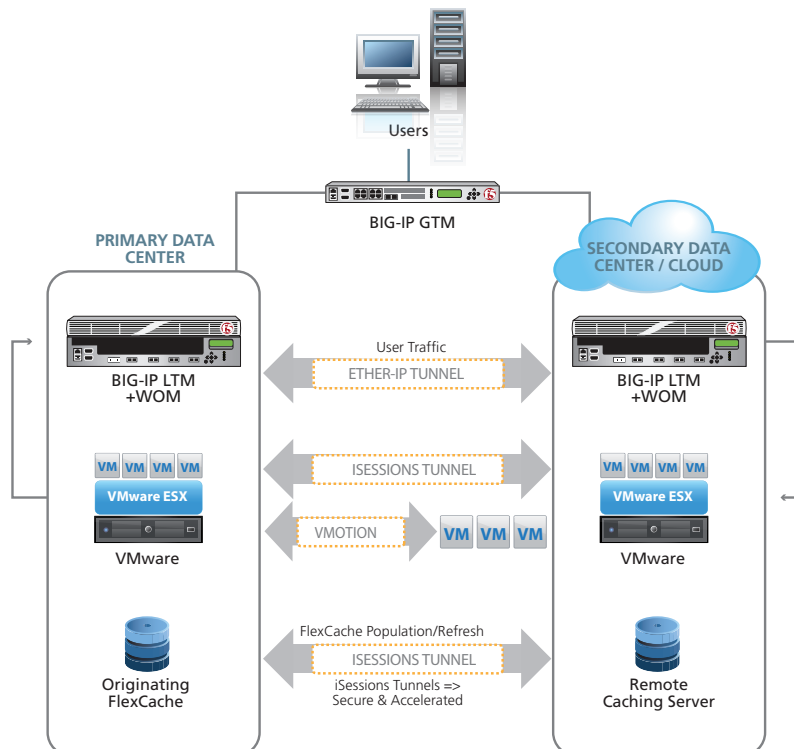


Figure 1: Logical configuration example

Configuration table for BIG-IP objects

The following is a description of the networks in the table on the following page

➤ **Private-WAN**

This is the network that enables BIG-IP iSessions and EtherIP. iSessions are used for deduplication, encryption and compression. The iSession network transfers Storage vMotion as well as Active State (memory) vMotion.

This network also enables the EtherIP network, that also runs only between the two BIG-IPs in the primary and secondary data center. EtherIP and iSessions are two distinct and separate technologies but in our example they traverse the same Private-WAN.

The Private-WAN network runs only between the two BIG-IP devices in the primary and secondary data center and needs to be routed properly to reach the destination each way.

➤ **Internal-LAN**

This is the network on the LAN side that terminates the vMotion traffic on either side. This Self IP will be the default gateway for both the VMware vMotion VMkernel and NetApp FlexCache's EOB interface.

In our example, we use a separate physical interface on the BIG-IP for this network and do not use VLAN tags for this network.

➤ **Servers**

This network is where the VM servers are hosted by ESX. Notice the network has to be the same IP Address space in both primary and secondary data center in order to pass VMware validation and to work with EtherIP (see FAQ section for additional details of VMware networking during vMotion).

➤ **Client**

This is the incoming client request traffic network. In this diagram, we are using private address space because there is upstream Network Address Translation (NAT) converting public IPs to our private space. In your scenario your client traffic network may be publicly routable IP space.

Because this implementation has four distinct areas to setup, the following configuration tables show the different VLAN, self IP and route settings in our example configuration.

Appendix A: Configuration worksheets on page 42 contains a blank worksheet that you can fill out before beginning the BIG-IP configuration to streamline your deployment process.

➡ **Note** *For simplicity, the chart below consists of all /24 subnet masks. In your deployment it is only important to be consistent in your subnets, the actual size is not relevant.*

Network	Primary Data Center	Secondary Data Center	Notes
Private-WAN	10.133.64.0/24 Network	192.168.64.0/24 Network	This network is used to transport WOM and EtherIP traffic.
VLAN	vlan-private-WAN1 Our tag is 1064	vlan-private-WAN2 Our tag is 1064	Although the tags are the same in our example, each data center may have different tags.
Self IP for WOM	10.133.64.245	192.168.64.245	Port Lockdown set to Allow None
Self IP for EtherIP	10.133.64.246	192.168.64.246	Port Lockdown set to Allow Default
Route	A route to the secondary data center is required	A route to the primary data center is required	Long distance live migration is a routed solution.
Internal-LAN	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp connectivity.
VLAN	vlan-internal1	vlan-internal2	This is used as the default gateway for ESX and NetApp. This is an untagged VLAN
Self IP	10.133.65.245	192.168.65.245	Port Lockdown set to Allow Default
Route	This is a local network, and routing is optional	This is a local network, and routing is optional	Routing is only necessary if local ESX and NetApp require it.
Servers (pool members)	10.133.66.0/24 Network	10.133.66.0/24 Network	This network is used for pool members and they are the same in both data centers
VLAN	vlan-servers Our tag is 1066	vlan-servers Our tag is 1066	Although tags are the same in our example, each data center may have different tags.
Self IP	10.133.66.245	10.133.66.245	Port Lockdown set to Allow Default
Route	This is a local network and routing is optional	This is a local network and routing is optional	Routing is only necessary if local pool members require it.
Client (virtual servers)	10.133.67.0/24 Network	192.168.67.0/24 Network	This network is used for external traffic and is usually publicly routable
VLAN	vlan-client1 Our tag is 1067	vlan-client2 Our tag is 1067	Although tags are the same in our example, each data center may have different tags.
Self IP	10.133.67.245	192.168.67.246	Port Lockdown set to Allow Default
Route	This external network needs appropriate routes	This external network needs appropriate routes	

Table 1: Configuration table for BIG-IP Objects

Configuration table for ESX, NetApp, and Servers

The following is a description of the networks in the following table:

➤ **Storage Origin**

This is a private network for storage mounts between ESX Servers and the NetApp devices. To pass vMotion validation between data centers, we assign the same name volume names and IP address to this network on the NetApp devices. In our example, we configure the Storage Origin on the E0A interface of the NetApp and assign an IP address of 10.30.30.60 in both data centers. This is an untagged network and routing is typically not needed as the NetApps are in the same broadcast domain as the ESX servers.

➡ **NOTE:** *The local storage network does not pass through the BIG-IP devices in either data center; only the FlexCache volumes pass through the BIG-IP systems.*

➤ **Storage Cache**

This is a routed network that traverses the BIG-IP and takes advantage of iSession acceleration, using deduplication and compression and iSession encryption using SSL. NetApp Flexcache volumes handle all of the communication between the Primary and Secondary network. In our example we assign an IP address in the 10.133.65.0/24 network in the Primary data center and 192.168.65.0/24 network in the Secondary data center. We add a route on the NetApp server so that the traffic traverses the BIG-IP and the WOM module.

➤ **vMotion**

The vMotion network is used for memory and storage vMotion when vMotion migration events are started. To enable Long distance live migration, the ESX server's VMkernel for vMotion is configured to be in the vMotion network and a default gateway is assigned for the VMkernel to point to the BIG-IP with the WOM module. In our example, the Primary data center VMkernel is configured with an IP address 10.133.65.20/24 and a default route of 10.133.65.245 which is the BIG-IP Self-IP address. In the Secondary data center, the VMkernel is configured with an IP address 192.168.65.20/24 and a default route of 192.168.65.245 which is the BIG-IP Self-IP address.

Optimization policies specific to vMotion capture and transmit all vMotion traffic over BIG-IP's iSession technology once these steps have been completed.

➤ **Pool Members (servers)**

The server network is where the pool members reside. In order to pass validation for vMotion and preserve networking (either when BIG-IP EtherIP technology is used or not), the IP address space is the same in both data centers for servers (pool members). In our example, we have provisioned 10.133.66.0/24 for servers in both the Primary and Secondary data center.

Because this implementation has four distinct areas to setup, the following configuration tables show the different VLAN, self IP and route settings in our example configuration.

Appendix A: Configuration worksheets on page 42 contains a blank worksheet that you can fill out before beginning the BIG-IP configuration to streamline your deployment process.

➡ **Note** *For simplicity, the chart below consists of all /24 subnet masks. In your deployment it is only important to be consistent in your subnets, the actual size is not relevant.*

Network	Primary Data Center	Secondary Data Center	Notes
Storage Origin	10.30.30.0/24 Network	10.30.30.0/24 Network	This is a local only network between NetApp and ESX.
VLAN	Not applicable Our tag is: untagged	Not applicable Our tag is: untagged	This is a local only network and VLANs tags are not required.
IP address	10.30.30.60	10.30.30.60	This is the E0A interface.
Default Gateway	Not applicable	Not applicable	This is a local only network and default gateways are not required.
Storage Cache	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp FlexCache connectivity.
VLAN	vlan-internal1	vlan-internal2	This is an untagged network (no VLAN tags on NetApp)
IP address	10.133.65.10	192.168.65.10	This is the E0B interface.
Default Gateway	10.133.65.245 Our tag is 1065	192.168.65.245 Our tag is 1065	The default gateway is the Self IP address of the local BIG-IP.
vMotion	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp FlexCache connectivity.
VLAN	vlan-internal1	vlan-internal2	ESX VMkernel for vMotion. In our example, we do not use tags for this network.
IP address	10.133.65.20	192.168.65.20	
Default Gateway	10.133.65.245	192.168.65.245	The default gateway is the Self IP address of the local BIG-IP.
Pool members (servers)	10.133.66.0/24 Network	10.133.66.0/24 Network	This network is used for pool members and they are the same in both data centers
VLAN	vlan-servers Tagging on ESX only	vlan-servers Tagging on ESX only	Tagging on the servers themselves is not necessary as ESX handles this function. The name of this VLAN MUST be identical on both ESX servers to pass vMotion validation but the VLAN tags (if any) may be different.
IP address	10.133.66.x	10.133.66.x	Assign IP addresses for your servers as you normally would.
Default Gateway	10.133.66.245	192.168.66.245	The default gateway is the Self IP address of the local BIG-IP.

Table 2: Configuration table for ESX, NetApp and Servers

Performing the BIG-IP system initial configuration tasks

In this section, we configure the networking objects on the BIG-IP system. This includes the appropriate VLANs, Self IP addresses and Routes.

Configuring the primary data center BIG-IP

First, we configure the BIG-IP system in the primary data center.

Creating the VLANs on the primary data center BIG-IP

The first task is creating the VLANs on the BIG-IP system. For this configuration, you need to create the four VLANs outlined in the *Configuration table for BIG-IP objects on page 4*.

To create a VLAN

1. On the Main tab, expand **Network**, and then click **VLANs**.
2. Click the **Create** button.
3. In the **Name** box, type a unique name for the VLAN. This is the network that will carry iSession and EtherIP traffic. In our example, for the iSession WAN VLAN we use **vlan-private-WAN1**.
4. In the **Tag** box, we assign a tag. In our example, we find that using VLAN tags make management easier. However, tagging is not mandatory if your configuration can support individual interfaces instead of VLANs. In our example, we use tag **1064**.
5. In the Resources section, from the **Available** list, select the interface that will have access to tagged traffic, and add it to the Tagged box by clicking the Add (>>) button. In our example, we select **1.1**.
6. Click the **Repeat** button for the other three VLANs. In our example, we create:
 - **vlan-internal1:**
This is the internal network that will be used as the default gateway for ESX and NetApp FlexCache volumes. In our example, we assign tag **1065**.

For this VLAN only: Add the interface to the **Untagged** box. So in step 5, select the interface that will have access to untagged traffic and add it to the **Untagged** box by clicking the Add (<<) button. In our example, we select **1.2**.
 - **vlan-servers:**
This is the network VMware guests (servers) will reside in and this network will have the same IP Address in both data centers. In our example, we assign tag **1066**.
 - **vlan-client1:**
This is the external facing network which hosts BIG-IP Virtual Servers and accepts client traffic from the Internet. In our example, we assign tag **1067**.
7. Click the **Finished** button.

Creating self IP addresses on the primary data center BIG-IP

Self IP addresses are the IP addresses owned by the BIG-IP LTM system that you use to access the VLANs. The next task in this configuration is to create the five self IP addresses outlined in the *Configuration table for BIG-IP objects on page 4*.

To create the self IP addresses

1. On the Main tab, expand **Network**, and then click **Self IPs**.
2. Click the **Create** button.

Important

This step is only for the WOM Self IP in the private WAN.

3. In the **IP Address** box, type a static IP address that resides on the VLAN you created in the preceding procedure. In our example, we start with **vlan-private-WAN1**, so we use an IP address of **10.133.64.245**.
4. In the **Netmask** box, type the corresponding subnet mask. In our example, **255.255.255.0**.
5. From the **VLAN** list, select the appropriate VLAN you created in *Creating the VLANs on the primary data center BIG-IP on page 8*. In our example, this is the WOM self IP in **vlan-private-wan1**.
6. *For the Self IP for WOM in the Private WAN only:* From the **Port Lockdown** list, select **Allow None**. In our example, this is **vlan-private-WAN1**.
7. Click the **Repeat** button, and repeat this procedure for the other self IP address (making sure you set **Port Lockdown** to **Allow Default** for all but the Self IP for WOM in the private WAN network).
In our example, we create the following additional self IP addresses shown in <vlan: self IP, Netmask> format:
 - **vlan-private-WAN1:** 10.133.64.246 Netmask: 255.255.255.0 (for EtherIP)
 - **vlan-internal1:** 10.133.65.245 Netmask: 255.255.255.0
 - **vlan-servers:** 10.133.66.245 Netmask: 255.255.255.0
 - **vlan-client1:** 10.133.67.245 Netmask: 255.255.255.0
8. Click **Finished**.

Creating Routes on the primary data center BIG-IP

The next task is to create the Routes on the BIG-IP system. The BIG-IP in the primary data center needs to be able to route to the BIG-IP in the secondary data center. You also need a route for the remote network where application services reside. .

In our example, for the primary data center we add a route for 192.168.64.0/24 via the local router in the 10.133.64.0/24 network.

To create the routes

1. On the Main tab, expand **Network**, and then click **Routes**.
2. Click the **Create** button.
3. From the **Type** list, select **Route**.
4. In the **Destination** box, type the IP network address of the remote network you wish to reach. In our example, **192.168.64.0**.
5. In the **Netmask** box, type the associated netmask. In our example **255.255.255.0**.
6. From the **Resource** list, make sure **Use Gateway** is selected.
7. From the **Gateway Address** list, select **IP Address**, and then type the IP address of the remote internal network via the next hop gateway. In our example, we use **10.133.64.200** because this is the internal router that connects our primary and secondary data centers.
8. Click **Finished**.

Configuring the initial tasks on secondary data center BIG-IP

In this section, we configure the BIG-IP system in the secondary data center. The procedures are the same, but the settings are different.

Creating the VLANs on the secondary data center BIG-IP

First we create the VLANs on the BIG-IP system in the secondary data center. For this configuration, you need to create the four VLANs outlined in the *Configuration table for BIG-IP objects* on page 4.

To create a VLAN

1. On the Main tab, expand **Network**, and then click **VLANs**.
2. Click the **Create** button.
3. In the **Name** box, type a unique name for the VLAN. In our example, for the iSession WAN VLAN we use **vlan-private-WAN2**.
4. In the **Tag** box, we assign a tag. In our example we find that using VLAN tags make management easier. However, tagging is not mandatory if your configuration can support individual interfaces instead of VLANs. In our example, we use **1064**.
5. In the Resources section, from the **Available** list, select the interface that will have access to tagged traffic, and add it to the Tagged box by clicking the Add (>>) button. In our example, we select **1.1**.
6. Click the **Repeat** button for the other three VLANs:
 - **vlan-internal2**: In our example, we assign tag **1065**.
*For this VLAN only: Add the interface to the **Untagged** box. So in step 5, select the interface that will have access to untagged traffic and add it to the **Untagged** box by clicking the Add (<<) button. In our example, we select **1.2**.*
 - **vlan-servers**: In our example, we assign tag **1066**.
 - **vlan-client2**: In our example, we assign tag **1067**.
7. Click the **Finished** button.

Creating self IP addresses on the secondary data center BIG-IP

Self IP addresses are the IP addresses owned by the BIG-IP LTM system that you use to access the VLANs. The next task in this configuration is to create the five self IP addresses outlined in the *Configuration table for BIG-IP objects* on page 4.

To create the self IP addresses

1. On the Main tab, expand **Network**, and then click **Self IPs**.
2. Click the **Create** button.
3. In the **IP Address** box, type a static IP address that resides on the VLAN you created in the preceding procedure. In our example, we start with **vlan-private-WAN2**, so we use an IP address of **192.168.64.245**.
4. In the **Netmask** box, type the corresponding subnet mask. In our example, **255.255.255.0**.

Important

This step is only for the WOM Self IP in the private WAN.

- From the **VLAN** list, select the appropriate VLAN you created in *Creating the VLANs on the secondary data center BIG-IP on page 10*. In our example, this is **vlan-private-WAN2**.
- For the Self IP for WOM in the Private WAN only: From the **Port Lockdown** list, select **Allow None**. In our example, this is for the WOM self IP in **vlan-private-WAN2**.
- Click the **Repeat** button. (making sure you set **Port Lockdown** to **Allow Default** for all but the Self IP for WOM in the private WAN network).

In our example, we create the following self IP addresses shown in `<vlan: self IP, Netmask>` format:

- **vlan-private-WAN2:** 192.168.64.246 Netmask: 255.255.255.0 (for EtherIP)
- **vlan-internal2:** 192.168.65.245 Netmask: 255.255.255.0
- **vlan-servers:** 192.168.66.245 Netmask: 255.255.255.0
- **vlan-client2:** 192.168.67.246 Netmask: 255.255.255.0

- Repeat steps 3-6 for each self IP address, and then click **Finished**.

Creating Routes on the secondary data center BIG-IP

The next task is to create the Routes on the BIG-IP system. The BIG-IP in the secondary data center needs to be able to route to the BIG-IP in the primary data center. You also need a route for the remote network where application services reside. .

In our example, for the secondary data center we add a route for 10.133.64.0/24 via the local router in the 192.168.64.0/24 network.

To create the routes

- On the Main tab, expand **Network**, and then click **Routes**.
- Click the **Create** button.
- From the **Type** list, select **Route**.
- In the **Destination** box, type the IP network address of the remote network you wish to reach. In our example, we type **10.133.64.0**.
- In the **Netmask** box, type the associated netmask. In our example, we type **255.255.255.0**.
- From the **Resource** list, make sure **Use Gateway** is selected.
- From the **Gateway Address** list, select **IP Address**, and then type the IP address of the remote internal network via the next hop gateway.
In our example, we type **192.168.64.200** because this is the internal router that connects our primary and secondary data centers.
- Click **Finished**.

 **Checkpoint**

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

Checkpoint

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

- Log into the BIG-IP in the primary data center from the command line.
- Use the ping command to check the following. You should receive successful responses from each:
 - » Local endpoint - In our example, we use **ping 10.133.64.245**,
 - » The router - In our example, we use **ping 10.133.64.200**
 - » The BIG-IP in the secondary data center - In our example, we use **ping 192.168.64.245**.
- Repeat this procedure in the other data center.

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

Configuring NetApp FlexCache

For this deployment guide, we assume you have completed the base installation of NetApp and FlexCache. Refer to the NetApp documentation for specific instructions.

In this section, we set up four volumes: two storage volumes, one in each data center; and two FlexCache volumes, one in each data center.

In both data centers, we configure a primary storage volume on NetApp as the primary storage for ESX Virtual Machines. This storage volume is connected to ESX on a local, non-routed subnet on a RFC 1918 address space. This address space must be identical in both data centers. This is critical for vMotion operations to pass validation.

We then setup a second storage volume which is the FlexCache volume pointed to the opposite data center. This storage volume is connected to NetApp on a routable, internal address.

Performing the NetApp initial configuration

In this section we show how to setup NetApp IP configuration to participate in Long Distance Live Migration.

Physical configuration

In our example, we have two physical network interfaces on our NetApp chassis, the first one (E0A) is connected through a Layer 2 switch directly to the ESX servers. The second one (E0B) is connected through a Layer 2 switch directly to the BIG-IP network.

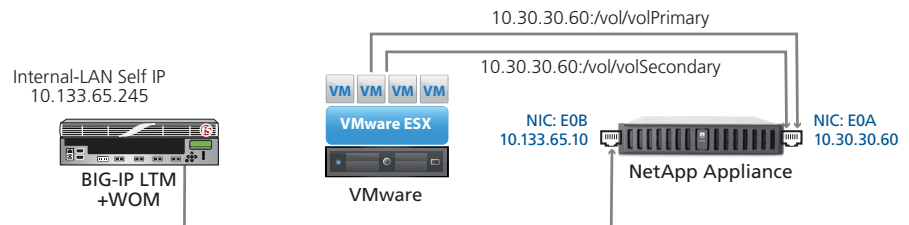


Figure 2: FlexCache storage configuration example (primary data center)

In this initial configuration, we configure the following in the Primary data center:

- **E0A**
IP address: 10.30.30.60
Netmask: 255.255.255.0
Default Gateway: In our example, E0A is on the same Layer 2 broadcast domain as the ESX server and therefore the default gateway is not applicable. However we have configured a default gateway of 10.30.30.1.
- **E0B**
IP address: 10.133.65.10
Netmask: 255.255.255.0
Default Gateway: This must be the BIG-IP self IP address for Internal-LAN. In our example, this is 10.133.65.245.

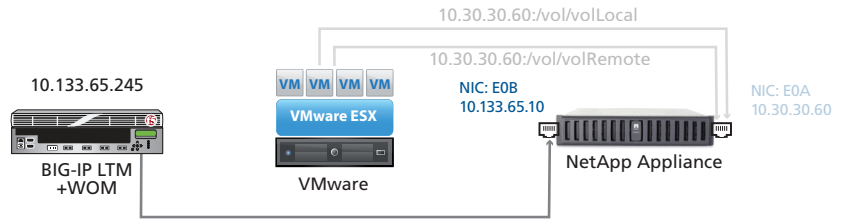


Figure 3: EOB configuration

In the Secondary data center, EOA is the same, but EOB is unique:

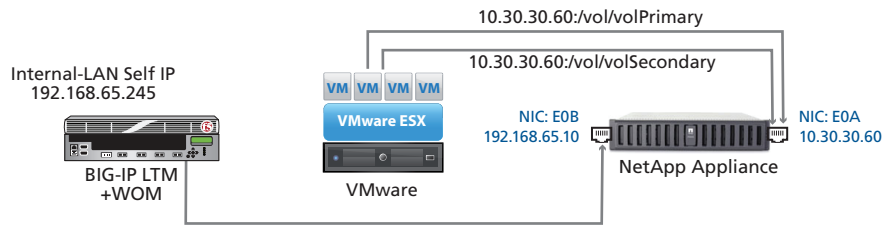


Figure 4: FlexCache storage configuration example (secondary data center)

- **EOA**

IP address: 10.30.30.60

Netmask: 255.255.255.0

Default Gateway: In our example, EOA is on the same Layer 2 broadcast domain as the ESX server and therefore the default gateway is not applicable. However we have configured a default gateway of 10.30.30.1.



Figure 5: Secondary data center configuration

- **EOB**

IP address: 192.168.65.10

Netmask: 255.255.255.0

Default Gateway: This must be the BIG-IP self IP address for Internal-LAN. In our example, this is 192.168.65.245 (see Figure 4)

➔ **Note:** The network configuration for EOA is identical in both the primary and secondary data centers.

Creating manual routes

In this section, we create the manual routes on the NetApp devices so that the EOB interface will route traffic over BIG-IP to the opposite data center. We do not provide step-by-step procedures in this section. For specific instructions on editing configuration files on the command line, consult your NetApp documentation.

- **Tip:** *NetApp recommends using Wordpad instead of Notepad to avoid incorrect line end characters if editing the file using a mount from Microsoft Windows. If editing from the NetApp command line, the `rdfile` command should be used to read and make a backup copy of the file and then the `wfile` command used to append the route to the end of the existing `/etc/rc.local`.*

We add one static route for the NetApp for each data center. First, add the route manually, and then you must edit your `/etc/rc.local` file so that the route persists through reboots. The command syntax is

```
route add <destination> <gateway> <metric>
```

In our example, we enter the following based on our entries in the *Configuration table for ESX, NetApp, and Servers* on page 6

- From the primary site, we use
route add 192.168.65.10 10.133.65.245 1
- From the secondary site, we use:
route add 10.133.65.10 192.168.65.245 1

Configuring primary storage volumes for VMware ESX servers

In this section, we configure the primary storage volumes on the NetApp device for VMware ESX servers.

Configuring the primary storage volume in the Primary data center

Use the following procedure to create the primary storage volume in the primary data center.

To create a new volume

1. In the left navigation, click to expand **Volumes**, and then click **Add**. The Volume wizard opens.
2. On the Volume Type Selection page, click the **Flexible** button, and then click **Next**.
3. On the Volume Parameters page, configure the following options:
 - a. In the **Volume Name** box, type a name for this volume. In our example, we type **volPrimary**.
 - b. From the **Language** list, select the appropriate language. In our example, we select POSIX.
 - c. Check the UTF-8 box, if appropriate.
 - d. Click the **Next** button.
4. On the Flexible Volume Parameters page, configure the following options:
 - a. From the **Containing Aggregate** list, select the appropriate aggregate. Volumes are assigned to NetApp Aggregates to store the file contents.
 - b. From the **Space Guarantee** list, select **Volume**.
 - c. Click the **Next** button.
5. On the Flexible Volume Size page, configure the following options as applicable:
 - a. In **Volume Size Type**, select an option. We click the **Total Size** button.
 - b. In the **Volume Size** box, type a number and select a size from the list.
 - c. In the **Snapshot Reserve** box, type a number. This number must not be 0.

- d. Click the **Next** button.
6. Review the volume parameters and then click **Commit**.

Configuring the primary storage volume in the Secondary data center

Repeat the preceding procedure to create the primary storage volume in the secondary data center, keeping in mind the following

- Step 3a: Use a unique name. In our example, we use **volSecondary**.
- We address this volume on a subnet that is not routed outside this datacenter and is identical to the address chosen in the primary datacenter. We use **10.30.30.60** in our example, with a netmask of **255.255.255.0**.

Configuring FlexCache volumes for VMware ESX servers

In this section, we configure the FlexCache storage volumes on the NetApp device for VMware ESX servers.

Configuring the FlexCache storage volume in the Primary data center

First we create the FlexCache volume in the Primary data center, which will be the cache for the secondary data center.

To create a new Cache volume

1. In the left navigation, click to expand **Volumes**, and then click **Add**. The Volume wizard opens.
2. On the Volume Type Selection page, click the **Cache** button, and then click **Next**.
3. In the **Volume Name** box, type a name for this volume, and then click **Next**. In our example, we type **volFlexCachePrimary**.
4. On the Flexible Volume Parameters page, configure the following options:
 - a. From the **Containing Aggregate** list, select the appropriate aggregate. Volumes are assigned to NetApp Aggregates to store the file contents.
 - b. In the **Remote Host Name** box, type the IP address of the E0B interface of the NetApp in the Secondary data center. In our example, type **192.168.65.10**.
 - c. In the **Remote Volume Name** box, type the name of the volume you created on the secondary data center. In our example, we type **volPrimary**.
 - d. Click the **Next** button.
5. In the **Volume Size** box, type a number and select a size from the list.
6. Review the volume parameters and then click **Commit**.

Configuring the FlexCache storage volume in the Secondary data center

Use the following procedure to create the FlexCache storage volume in the Secondary data center.

To create a new Cache volume

1. In the left navigation, click to expand **Volumes**, and then click **Add**. The Volume wizard opens.

2. On the Volume Type Selection page, click the **Cache** button, and then click **Next**.
3. In the **Volume Name** box, type a name for this volume, and then click **Next**. In our example, we type **volFlexCacheSecondary**.
4. On the Flexible Volume Parameters page, configure the following options:
 - a. From the **Containing Aggregate** list, select the appropriate aggregate. Volumes are assigned to NetApp Aggregates to store the file contents.
 - b. In the **Remote Host Name** box, type the IP address of the E0B interface of the NetApp in the Primary data center. In our example, type **10.133.65.10**.
 - c. In the **Remote Volume Name** box, type the name of the volume you created on the secondary data center. In our example, we type **volSecondary**.
 - d. Click the **Next** button.
5. In the **Volume Size** box, type a number and select a size from the list.
6. Review the volume parameters and then click **Commit**.

This completes the NetApp configuration.

Configuring VMware ESX servers

In this section, we configure the VMware ESX devices.

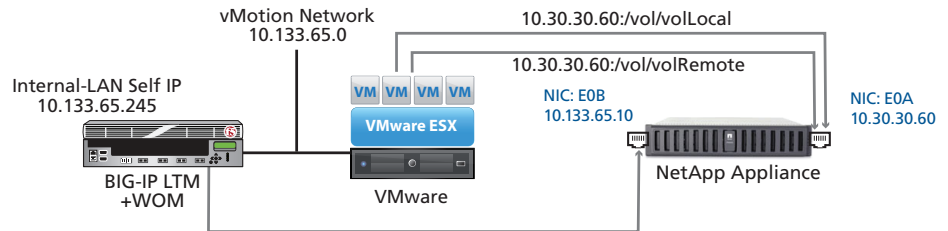


Figure 6: Configuration example for the vMotion network in the Primary data center

Configuring the ESX servers in the Primary data center

In this section, we configure the ESX servers in the Primary data center.

Creating a network

The first task is to create a network. In the network configuration section of the vSphere client, create a network that will communicate on a subnet in the Storage Origin network (**10.30.30.0/24** subnet in our example). You may have to create an appropriate vSwitch or Virtual Machine for this network. See VMware documentation for more information or specific instructions on creating a network.

➔ **Note:** As a reminder, this network connects directly to the NetApp chassis and will mount both a NetApp origin volume and a NetApp FlexCache volume.

Creating the storage volumes

The next task is to create a connection to new storage volumes that represent the logical and remote storage.

To create a storage volume

1. Open the VMware vSphere client, and navigate to the Configuration tab of the applicable ESX server.
2. In the *Hardware* box, click **Storage**, and then click the **Add Storage** link.
3. Click the **Network File System** option button and then click **Next**.
4. In the **Properties** box, type the IP address from the Storage Origin network. In our example, we type **10.30.30.60**.
5. In the **Folder** box, type the appropriate folder. In our example, we type **/vol/volPrimary**.
6. In the **Datastore name** box, type an appropriate datastore name. In our example, we type **Primary DC**.
7. Review the Summary, and then click **Finished**.
8. Repeat this entire procedure to create a new storage volume that represents the remote storage. In our example, we use the folder **/vol/volSecondary** and a Datastore name of **SecondaryDC**. As noted in the side bar, the IP address is the same in both volumes.

Configuring the ESX servers in the Secondary data center

In this section, we configure the ESX servers in the secondary data center. To configure the ESX servers in the secondary data center, return to *Configuring the ESX servers in the Primary data center on page 18* and repeat procedures *Creating the network* and *Creating the storage volume*.

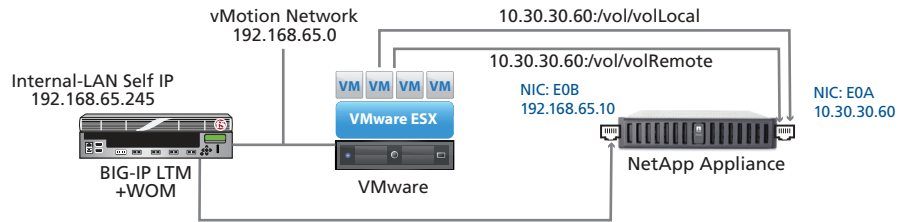


Figure 7: Configuration example for the vMotion network in the Secondary data center

Configuring VMware VMkernel for vMotion

In this deployment guide, we assume you already have your VMware vMotion implementation up and running. However, there are some modifications you need to make to the VMware configuration for the configuration in this guide to work properly.

Creating a network

The first task is to create a network. In the network configuration section of the vSphere client, create a network that will communicate on a subnet in the Internal-LAN network (10.133.65.0/24 in our example). You may have to create an appropriate vSwitch or Virtual Machine for this network. See VMware documentation for more information or specific instructions on creating a network.

Modifying the VMware ESX configuration

The ESX servers should be configured to have a VMkernel Port for vMotion. This VMkernel port, on an ESX virtual switch should be bound to a unique physical adapter.

Configuring the VMkernel networking on the primary data center

In this procedure, we configure networking for VMkernel for vMotion. We assign an IP address in the internal-LAN network and then set the default gateway to the internal-LAN self IP address you created in *Creating self IP addresses on the primary data center BIG-IP on page 8*.

To configure the VMkernel networking

1. Open the VMware vSphere client, and select the appropriate ESX server host.
2. Click the Configuration tab.
3. In the **Hardware** box, click **Networking**.
4. From the **Networking** list, locate the Virtual Switch that contains the vMotion kernel.
5. Click the **Properties** link.
6. Click to highlight **VMkernel** and then click the **Edit** button. The VMkernel properties box opens.
7. Click the IP Settings tab.

8. In the **IP address** box, type the vMotion IP address you provisioned in the configuration table. In our example we type **10.133.65.20**.
9. In the **Subnet mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.0**.
10. Click the **Edit** button next to VMkernel Default Gateway. The DNS and Routing Configuration box opens.
11. In the **Default Gateway** box, type the Internal-LAN self IP address on the BIG-IP device. In our example, this is **10.133.65.245**.
12. Click the **OK** button, and then click **OK** and **Close** to close all the open windows.

Binding the ESX devices to a specific vmknic

The final task is to bind the ESX machine to a specific vmknic.

To bind VMKernel to a specific vmknic

1. Open the VMware vSphere client, and select the appropriate ESX host.
2. Click the Configuration tab.
3. In the Software box, click **Advanced Settings**. The Advanced Settings window opens.
4. From the left navigation tree, click **Migrate**.
5. In the **Migrate.BindToVmknic** row, type **1** in the box.
6. Click the **OK** button.

Configuring the VMkernel networking on the secondary data center

In this procedure, we create a network, and then configure networking for VMkernel for vMotion. We assign an IP address in the internal-LAN network and then set the default gateway to the internal-LAN self IP address you created in *Creating self IP addresses on the primary data center BIG-IP on page 8*.

Creating a network

In the network configuration section of the vSphere client, create a network that will communicate on a subnet in the Internal-LAN network (192.168.65.0/24 in our example). You may have to create an appropriate vSwitch or Virtual Machine for this network. See VMware documentation for more information or specific instructions on creating a network.

Configuring VMkernel networking

Now we configure the VMkernel networking.

To configure the VMkernel networking

1. Open the VMware vSphere client, and select the appropriate ESX server host.
2. Click the Configuration tab.
3. In the **Hardware** box, click **Networking**.
4. From the **Networking** list, locate the Virtual Switch that contains the vMotion kernel.
5. Click the **Properties** link.
6. Click to highlight **VMkernel** and then click the **Edit** button. The VMkernel properties box opens.
7. Click the IP Settings tab.

8. In the **IP address** box, type the vMotion IP address you provisioned in the configuration table. In our example we type **192.168.65.20**.
9. In the **Subnet mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.0**.
10. Click the **Edit** button next to VMkernel Default Gateway. The DNS and Routing Configuration box opens.
11. In the **Default Gateway** box, type the Internal-LAN self IP address on the BIG-IP device. In our example, this is **192.168.65.245**.
12. Click the **OK** button, and then click **OK** and **Close** to close all the open windows.

Binding the ESX devices to a specific vmknic

The final task is to bind the ESX machine to a specific vmknic.

To bind VMKernel to a specific vmknic

1. Open the VMware vSphere client, and select the appropriate ESX host.
2. Click the Configuration tab.
3. In the Software box, click **Advanced Settings**. The Advanced Settings window opens.
4. From the left navigation tree, click **Migrate**.
5. In the **Migrate.BindToVmknic** row, type **1** in the box.
6. Click the **OK** button.

Checkpoint

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

Checkpoint

At this point, you should be able to ping from your ESX hosts to the BIG-IP Internal-LAN self IP address. The following commands require SSH access to the BIG-IP or ESX servers. Consult the product documentation for instructions on how to use SSH.

- Log in to either your BIG-IP or ESX server via SSH and execute a ping command to test network connectivity.

For example, in the primary data center:

- » From BIG-IP, issue the command: **ping 10.133.65.20**.
You should see a successful response.
- » From the ESX server, issue the command: **vmkping 10.133.65.245**.
You should see a successful response.

For example, in the secondary data center:

- » From BIG-IP, issue the command: **ping 192.168.65.20**.
You should see a successful response.
- » From the ESX server, issue the command: **vmkping 192.168.65.245**.
You should see a successful response.

If any of the pings are not successful, we recommend checking the following:

- **For the BIG-IP**
Return to Performing the BIG-IP system initial configuration tasks on page 8 and double check the Initial configuration, paying close attention to the IP address and VLANs.
- **For ESX,**
Return to Modifying the VMware ESX configuration on page 19 and check the IP address for in step 8.

Configuring the BIG-IP WAN Optimization Module

In this section, we configure the BIG-IP WAN Optimization Module (WOM). The WAN optimization module allows you to encrypt and accelerate data between BIG-IP devices, accelerate applications across the WAN.



Figure 8: WAN optimization configuration

Performing the WOM initial configuration in the primary data center

In this section, we set up the WAN optimization module initial configuration.

Running the BIG-IP WOM quick start

The first task in this section is to configure the BIG-IP WOM using the Quick Start Wizard.

To configure the WOM module using the Quick Start

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Quick Start**. The Quick Start configuration screen opens.
2. In the **WAN Self IP Address** box, type the BIG-IP self IP address you provisioned for the WAN Endpoint. In our example, we use **10.133.64.245**.
3. From the **Discovery** list, select **Enabled**.
4. In the LAN VLANs section, from the **Available** list, select the Internal-LAN VLAN you created in *Creating the VLANs on the primary data center BIG-IP on page 8* and then click the Add (<) button. In our example, we click **vlan-internal1**.
5. In the WAN VLANs section, from the **Available** list, select the Private WAN VLAN you created and then click the Add (<<) button. In our example, we click **vlan-private-WAN1**.
6. In the *Authentication and Encryption* section, leave the defaults.
7. From the **Application Data Encryption** list, we strongly recommend selecting **Enabled** from the list because VMware does not encrypt vMotion data.
8. In the Create Optimized Applications section, check the box for **VMware vMotion**.
9. Click the **Apply** button.
You will see a green checkmark next to VMware vMotion and Data Encryption should be set to **Enabled**.

Creating the iSession profile for Storage vMotion with NetApp FlexCache

In this section, we create an iSession profile for Storage vMotion with FlexCache. The iSession profile tells the system how to optimize traffic; encryption, deduplication and compression are controlled in the iSession profile. This profile is only used for the Storage vMotion.

To create the iSession profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, select **iSession**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **isession-storage**.
5. In the Outbound iSession to WAN section, click the **Custom** box for **Application Data Encryption**, and then select **Enabled** from the list.
6. Leave the other settings at the default levels.
7. Click the **Finished** button.

Creating the Optimized Application for Storage vMotion

In this section, we create an Optimized Application object for FlexCache that uses the iSession profile you just created.

To create the Optimized Application

1. On the Main tab, expand **WAN Optimization**, mouse over **Optimized Applications**, and then click **Create Outbound**.
2. In the **Name** box, type a name for this application. In our example, we type **flexcache**.
3. In the **Port** box, type **2049**.
4. From the Enabled LAN VLANs section, from the **Available** list, click the VLAN you created for the storage network and then click the Add (<<) button. In our example, we move **vlan-internal1** to the Selected list.
5. From the **iSession Profile** list, select the profile you created in the preceding procedure. In our example, we click **isession-storage**.
6. Click the **Finished** button.

Advertising local networks

The next task is to advertise the local networks. In this procedure, we configure the BIG-IP WOM module to apply WAN optimization to only the appropriate networks. In our example, the vMotion-specific network vlan-internal1.

To advertise the local networks

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Advertised Routes**.
2. Click the **Create** button.
3. In the **Address** box, type the IP Address of the Internal-LAN. In our example, this is the **vlan-internal1** VLAN, so we type **10.133.65.0**.
4. In the **Netmask** box, type the corresponding subnet netmask. In our example, we type **255.255.255.0**.
5. Click the **Finished** button.

Repeating the WOM configuration on the secondary data center BIG-IP

Now we log on to the BIG-IP system in the secondary data center and configure WOM for the secondary data center using the appropriate secondary data center values from the *Configuration table for BIG-IP objects* on page 4.

Running the BIG-IP WOM quick start

The first task in this section is to configure the BIG-IP WOM using the Quick Start Wizard.

To configure the WOM module using the Quick Start

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Quick Start**. The Quick Start configuration screen opens.
2. In the **WAN Self IP Address** box, type the BIG-IP self IP address you provisioned for the WAN Endpoint. In our example, we use **192.168.64.245**.
3. From the **Discovery** list, select **Enabled**.
4. In the LAN VLANs section, from the **Available** list, select the Internal-LAN VLAN you created in *Creating the VLANs on the secondary data center BIG-IP* on page 10 and then click the Add (<<) button. In our example, we click **vlan-internal2**.
5. In the WAN VLANs section, from the **Available** list, select the Private WAN VLAN you created and then click the Add (<<) button. In our example, we click **vlan-private-WAN2**.
6. In the *Authentication and Encryption* section, leave the defaults.
7. From the **Application Data Encryption** list, we strongly recommend selecting **Enabled** from the list because VMware does not encrypt vMotion data.
8. In the Create Optimized Applications section, check the box for **VMware vMotion**.
9. Click the **Apply** button.
You will see a green checkmark next to VMware vMotion and Data Encryption should be set to **Enabled**.

Creating the iSession profile for Storage vMotion with NetApp FlexCache

In this section, we create an iSession profile for Storage vMotion with FlexCache. The iSession profile tells the system how to optimize traffic; encryption, deduplication and compression are controlled in the iSession profile. This profile is only used for the Storage vMotion.

To create the iSession profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, select **iSession**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **isession-storage-secondary**.
5. In the Outbound iSession to WAN section, click the **Custom** box for **Application Data Encryption**, and then select **Enabled** from the list.
6. Leave the other settings at the default levels.
7. Click the **Finished** button.

Creating the Optimized Application for Storage vMotion

In this section, we create an Optimized Application object for FlexCache that uses the iSession profile you just created.

To create the Optimized Application

1. On the Main tab, expand **WAN Optimization**, mouse over **Optimized Applications**, and then click **Create Outbound**.
2. In the **Name** box, type a name for this application. In our example, we type **flexcache-secondary**.
3. In the **Port** box, type **2049**.
4. From the Enabled LAN VLANs section, from the **Available** list, click the VLAN you created for the storage network and then click the Add (<<) button. In our example, we move **vlan-internal2** to the Selected list.
5. From the **iSession Profile** list, select the profile you created in the preceding procedure. In our example, we click **isession-storage-secondary**.
6. Click the **Finished** button.

Advertising local networks

The next task is to advertise the local networks. In this procedure, we configure the BIG-IP WOM module to apply WAN optimization to only the appropriate networks. In our example, the vMotion-specific network vlan-internal2.

To advertise the local networks

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Advertised Routes**.
2. Click the **Create** button.
3. In the **Address** box, type the IP Address of the Client Network. In our example, this is the **vlan-internal2** VLAN, so we type **192.168.65.0**.
4. In the **Netmask** box, type the corresponding subnet netmask. In our example, we type **255.255.255.0**.
5. Click the **Finished** button.

Configuring the BIG-IP WOM Remote Endpoints

The next task is to configure the Remote Endpoints on the BIG-IP WAN optimization module.

Configuring the remote endpoints in the primary data center BIG-IP

First, we configure the remote endpoint in the primary data center.

To configure the remote endpoints

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. Click the **Create** button.
3. In the **IP Address** box, type the Self IP address for the BIG-IP WOM module in the secondary data center (this is also called the *local endpoint*). In our example, we type **192.168.64.245**.
4. Leave all other settings at the defaults.
5. Click the **Finished** button. The remote endpoint is added to the list.

Configuring remote endpoints in the secondary data center BIG-IP

Now we log into the secondary data center BIG-IP system to configure the remote end point.

To configure the remote endpoints

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. Click the **Create** button.
3. In the **IP Address** box, type the Self IP address for the BIG-IP WOM module in the primary data center (this is also called the *remote endpoint*). In our example, we type **10.133.64.245**.
4. Leave all other settings at the defaults.
5. Click the **Finished** button. The remote endpoint is added to the list.

Confirming outbound connections are allowed

The next task is to confirm that outbound connections are allowed.

Confirming outbound connections from the primary data center

First we confirm the outbound connections from the primary data center BIG-IP.

To confirm outbound connections are allowed

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. In the table, click the IP address for the remote Endpoint you just created. In our example, we click **192.168.64.245**.
Check to make sure there is a green circle in the left column for this Endpoint. If it's red, there is a connectivity problem. Recheck connectivity between data centers.

3. In the *Outbound iSession to WAN* section, make sure there is a check in the **Outbound Connections** box. If there is not, check the box.
4. Click **Update**. You return to the Remote Endpoints list.
5. In the *Remote Endpoints* table, click a check in the box next to the IP address of the Remote Endpoint you modified, and then click the **Manual Save** button.

Confirming outbound connections from the secondary data center

Now we confirm the outbound connections from the secondary data center BIG-IP.

To confirm outbound connections are allowed

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. In the table, click the IP address for the remote Endpoint you just created. In our example, we click **10.133.64.245**.
Check to make sure there is a green circle in the left column for this Endpoint. If it's red, there is a connectivity problem. Recheck connectivity between data centers
3. In the *Outbound iSession to WAN* section, make sure there is a check in the **Outbound Connections** box. If there is not, check the box.
4. Click **Update**. You return to the Remote Endpoints list.
5. In the *Remote Endpoints* table, click a check in the box next to the IP address of the Remote Endpoint you modified, and then click the **Manual Save** button.

Checkpoint

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

Checkpoint: Testing the configuration

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

To test WOM connectivity

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

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

To verify the WOM tunnel

1. Using an SSH client, like Putty, establish a connection to each BIG-IP.
2. After logging in, at the command prompt, type **b endpoint remote show all**

You should see an output similar to the following, however your host name and IP addresses will be different. Make sure you see the tunnel state as **ready, ready**.

```
b endpoint remote show all
```

```
ENDPOINT REMOTE 20.20.20.20
| HOSTNAME PRIMARYDC.example.com
| MGMT ADDR 10.1.102.61 VERSION 10.2.0
| UUID c1f3:68d6:f697:6834:108:5668:1e16:3fce
| enable STATE ready (incoming, outgoing)=(ready, ready)
| BEHIND NAT disable
| CONFIG STATUS "none"
| DEDUP CACHE 62380 REFRESH (count) = (0)
| ALLOW ROUTING enable
+--> ENDPOINT REMOTE 20.20.20.20 ROUTE 20.20.20.0/24
| | INCLUDE enable LABEL West
```

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

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

For more information and product documentation/troubleshooting, see our technical support site AskF5 (http://support.f5.com/kb/en-us/products/wan_optimization/versions.10_2_0.html).

Configuring EtherIP

In this section, we configure EtherIP on the BIG-IP system. The EtherIP configuration must be carried out using the command line. There are two procedures for configuring EtherIP: configuring the EtherIP tunnel and configuring a VLAN group.



Figure 9: EtherIP configuration

Creating the EtherIP tunnel

The first procedure in configuring EtherIP is to create the EtherIP tunnel on the BIG-IP system. This must be done using the command line.

To configure the EtherIP tunnel

1. On the BIG-IP system, start a console session.
2. Type a user name and password, and then press Enter.
3. At the system prompt, type **tmsh** and then press Enter. This opens the Traffic Management shell.
4. Type **net tunnel**, and press Enter.
5. Use the following syntax to create the tunnel:
create tunnel <tunnel name> profile etherip local-address <local_self_ip_address> remote-address <remote_self_ip_address>

The self IP addresses that you specify are those you created for specifically for EtherIP in the Private WAN network on both the local and the remote BIG-IP system.

In our example, we type:

```
create tunnel eip profile etherip local-address 10.133.64.246  
remote-address 192.168.64.246
```

6. Type **save / sys config**, and press Enter.
7. To exit the shell, type **quit**, and press Enter.

Creating the VLAN group

To complete the EtherIP tunnel configuration, you must create a VLAN group. This VLAN group associates the EtherIP traffic with the BIG-IP virtual server traffic. This allows the BIG-IP system to recognize where servers are located, either “locally” or “remotely” (via the EtherIP interface). To create the VLAN group, you must use the command line, however once it is created, it can be edited using the BIG-IP Configuration utility (GUI).

To create the VLAN group

1. On the BIG-IP system, start a console session.
2. Type a user name and password and then press Enter.

3. At the system prompt, type **tmsh** and then press Enter. This opens the Traffic Management shell.
4. Type **net vlan-group**, and then press Enter.
5. Use the following syntax to create the VLAN group:

```
create <vlangroup-name> mode <mode> members add { <EtherIP tunnel> }
members add <vlan-name> }
```

In our example, we associate the EtherIP tunnel named eip, and the VLAN vlan-servers with the VLAN group vg-eip, so we type:

```
create vg-eip mode transparent members add { eip } members add {
vlan-servers }
```

6. Type **save / sys config**, and press Enter.
7. To exit the shell, type **quit**, and press Enter.
8. Open the BIG-IP Configuration utility using a web browser. In the following steps, we verify that the VLAN group was successfully added.
9. On the Main tab of the navigation pane, expand **Network** and then click **VLANS**.
10. From the menu bar, click **VLAN Groups**, and then click **List**.
11. Click the name of the VLAN group you just created. Verify it has two members: the EtherIP tunnel and the VLAN for your servers.

Configuring the VLAN group for failover BIG-IP pairs

When setting up BIG-IP in a failover pair, the Media Access Control (MAC) Masquerade feature should be used to insure seamless traffic failover between the Active and Standby BIG-IP devices. In order to configure MAC Masquerade, you need to create a unique MAC address for this VLAN Group. When there is a failover event between the BIG-IP devices, while EtherIP is in use, traffic will not be disrupted.

You must select two unique MAC address to be shared between your active and standby BIG-IP devices (One per data center; the standby BIG-IP device uses its own MAC address when it is not active). Selecting a unique and locally administered Media Access Control (MAC) address is important to insure there are no overlaps with any other MAC address on your networks. F5 solution 3523:

<https://support.f5.com/kb/en-us/solutions/public/3000/500/sol3523.html> describes this process. The convention to designate an address as locally administered, recommended by F5, is to flip the second to last bit of the first byte of the MAC address to one. The following table from SOL3523 illustrates how to do this. See the solution for more information.

Pre-assigned MAC address	First byte	Local bit	Flipped local bit	New first byte	Locally administered MAC address
00:01:D7:01:02:03	00	00000000	00000010	02	02:01:D7:01:02:03
01:01:D7:01:02:03	01	00000001	00000011	03	03:01:D7:01:02:03
08:01:D7:01:02:03	08	00001000	00001010	0A	0A:01:D7:01:02:03

Table 3: MAC address conversion table from Ask F5

To determine your own unique, locally administered MAC address

1. On the Main tab of the navigation pane, expand **Network** and then click **Interfaces**.
2. In the fourth column, note the physical MAC address associated with the physical interface used for EtherIP traffic. In our case it is: **0:1:d7:92:c0:c4**.

In this case, the first byte is **00** (listed as a single zero in the display).

The local bit in this case is **00000000** (eight zeros), we flip the second to last bit and we now have **00000010**. Our new first byte is now **02**.

3. In our example, we replace our new first byte and end up with: **02:01:d7:92:c0:c4**. We use this in step 5 of the following procedure.

This scheme guarantees the MAC address is always unique.

To configure MAC Masquerade

1. On the Main tab of the navigation pane, expand **Network** and then click **VLANs**.
2. From the menu bar, click **VLAN Groups**, and then click **List**.
3. Click the name of the VLAN group you created in *Creating the VLAN group on page 30*.
4. Make sure the **Bridge in Standby** box is *not* checked.
5. In the **MAC Masquerade** box, type the unique MAC address you calculated in the preceding procedure.
6. Click **Update**.

Repeat this MAC Masquerade section for your secondary site, ensuring that you create a brand new and unique locally administered MAC address using the instructions here.

This concludes the EtherIP configuration for the primary data center.

Repeating the EtherIP configuration on the secondary data center BIG-IP

The final task in this section is to log on to the BIG-IP system in the secondary data center and repeat this entire section using the appropriate values for the secondary data center from the *Configuration table for BIG-IP objects on page 4*.

Be sure to repeat the following procedures on the BIG-IP system in the secondary data center:

- *Creating the EtherIP tunnel on page 30*
 - » Step 5: use the following syntax to create the tunnel (keeping in mind the local address is now in the secondary data center):

```
create tunnel <tunnel name> profile etherip local-address <local_  
self_ip_address> remote-address <remote_self_ip_address>
```

The self IP addresses you specify are those you created for EtherIP on both the local and the remote BIG-IP system.

In our example, we type:

```
create tunnel eip profile etherip local-address 192.168.64.246  
remote-address 10.133.64.246
```

- *Creating the VLAN group on page 30*
 - » Step 5: We use the following as our example:
create vg-eip mode transparent members add { eip } members add { vlan-servers }

Checkpoint

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

Checkpoint

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

- Log into the BIG-IP in the both data centers from the command line. Use the **ping** command to check the following. You should receive successful responses from each:
 - » From the primary data center BIG-IP - we use **ping 192.168.64.246**
 - » From the secondary data center BIG-IP - we use **ping 10.133.64.246**

You can check tunnel traffic from the **tmsh** shell, by performing the following procedure.

To check tunnel traffic from tmsh

1. On the BIG-IP system, start a console session.
2. Type a user name and password, and then press Enter.
3. At the system prompt, type **tmsh** and then press Enter. This opens the Traffic Management shell.
4. Type **net tunnel**, and then press Enter.
5. Type **show tunnel**, and then press Enter.
You will see tunnel traffic.

Managing VM hosts, VM storage and client traffic between data centers during vMotion events

This section contains information about the management of VM hosts (memory and storage) and client traffic between data centers while the vMotion events are occurring.

Components to be managed by automation

The following three components can be scripted to more effectively manage long distance live migration:

- Migrating Storage
- Migrating the virtual machine
- Using ratios to switch data center traffic with GTM

For best results with long distance live migration using vMotion, we recommend the following order for vacating the one data center for the other: first, Storage vMotion; second, memory vMotion; third, GTM, allowing EtherIP to handle already established connections.

Migrating Storage

In our example, the movement of a 40 Gigabyte disk takes the longest amount of time (many minutes or hours) to complete. After this storage migration is completed, the memory portion of vMotion could be completed in a matter of seconds. This order of operation results in the least amount of time when disk I/O operations would be subjected to higher latency.

In this document we have demonstrated how using NetApp FlexCache allows for NetApp to handle the network communication between the primary and secondary data center for storage vMotion events. By using NetApp FlexCache in conjunction with BIG-IP WOM, storage vMotion is accelerated while ESX servers in both data centers preserve their stability by always communicating with their local NetApp devices.

In a storage vMotion event, NetApp first consults its cache volume and populates the origin volume, thus greatly improving storage vMotion times.

Configuring the application-specific objects on the BIG-IP system

Because this guide is not specific to any particular application, this document does not include configuration procedures for a specific application objects on the BIG-IP system (such as application specific health monitors, pools, profiles and virtual servers). There are a number of deployment guides for specific applications found on our web site:

<http://www.f5.com/solutions/resources/deployment-guides/>

However, there are some guidelines you must follow when configuring the application-specific pools and virtual servers on the BIG-IP when using this deployment guide to enable long distance live migration:

BIG-IP Pool Members

Pool members involved in Long Distance live migration should be the same in both the primary and secondary data centers.

In our example, we have pool members in the 10.133.66.0/24 network (10.133.66.50, 10.133.66.51, and 10.133.66.52) in the primary data center. We use these exact same IP addresses when configuring the BIG-IP pool in the secondary data center.

Using the Virtual Location monitor to track the location of BIG-IP Pool members

Because pool members may be located in either the Primary or Secondary data center, we configure an advanced BIG-IP health monitor called *Virtual Location* that tracks the location of a particular pool.

This monitor is designed to be used in conjunction with standard monitors for your pools, and is often the second or third monitor associated with a particular pool. The Virtual Location monitor serves two functions: it polls and tracks where ARP requests are coming for each particular pool member; and it reports a Virtual Server (VS) score to BIG-IP GTM. The VS score can be used by GTM to make decisions about how and where to distribute traffic as vMotion events take place.

➤ **Note:** *The Virtual Location monitor works in conjunction with other monitors which track up/down status and information for high availability of pools. Therefore, standard monitors will be combined with a Virtual Location Monitor for pool members.*

To create the Virtual Location Monitor

1. On the Main tab of the BIG-IP system navigation pane, expand **Local Traffic** and then click **Pools**.
2. From the Pool list, find and make note of the exact name of the pool that will participate in Long Distance live migration. In our example, this is the pool **ApacheServers-HTTP**.
No changes are required to this pool yet, but you do need to record the exact name with all spaces, punctuation, etc.
3. On the Main tab of the navigation pane, under **Local Traffic**, click **Monitors**.
4. Click the **Create** button.
5. In the **Name** box, type a name. In our example, we use **Apache-HTTP-Pool-Location**.
6. From the Type list, select Virtual Location.
7. In the **Pool Name** box, type the exact name of the pool you recorded in step 2. In our example, we type **ApacheServers-HTTP** because this is the pool we will be tracking with the Virtual Location monitor.
8. Leave all other settings at the default levels.
9. Click **Finished**.

BIG-IP Virtual Servers

The BIG-IP virtual servers can be any public or private address space the infrastructure needs. Note that in our example the client network users 10.133.67.0/24 and 192.168.67.0/24 in the primary secondary data center respectively.

➤ **Important:** *Enable SNAT Automap in order to ensure the pool member routes back to the Virtual Server from which it received traffic. The SNAT Automap setting is found on the BIG-IP virtual server configuration page.*

For more information on SNAT, see the product documentation.

In both the primary and secondary data center provision nodes that participate in long distance live migration, for example, 10.133.66.50, 10.133.66.51, 10.133.66.52 will be our application servers. Do this on BOTH DATACENTERS with the identical IP Addresses.

- In both data centers configure pools of this servers, in our example we create identically named pools called "ApplicationServers" on port 8080. Note that while we use identical pool names in our example, only identical IP address space is mandatory, not names.
- In the primary data center create a virtual server using this pool and address it on the externally facing network, in our case, the 10.133.67.0/24 network.

In the secondary data center create a virtual server using the application pool and address it on the externally facing network, in our case, the 192.168.67.0/24 network.

EtherIP will maintain already established connections that originate from the Virtual Servers during and after vMotion events.

Migrating the virtual machine

In order to manage hosts during vMotion events, the use of scripting and orchestration is recommended. The basic components for orchestration that can be used without additional expenditure are listed below. VMware also provides VMware Orchestrator, part of the vCenter Server Suite, which may be licensed for advanced automation.

- VMware's vSphere Web Services API
<http://www.vmware.com/support/developer/vc-sdk/>
- F5 BIG-IP's iControl API
<http://devcentral.f5.com/Default.aspx?tabid=76>

Using ratios to switch data center traffic with GTM

We recommend the use of F5 iControl to dynamically manage the ratio or the cutover point for global traffic. This ensures traffic destined for one data center does not overwhelm an increasingly smaller number of hosts. To illustrate this, the following sections examine some typical long distance live migration scenarios.

➡ **Note:** *Because the final implementation depends on the automation or orchestration solution used by your implementation, we do not provide detailed procedures for configuring ratios. See the product documentation or DevCentral for more information.*

Migrating a group of vMotion servers (2 or more)

For the migration of a group of hosts, management through scripting or orchestration is recommended to minimize client traffic disruption. A video showing this type of orchestration is located on YouTube: http://www.youtube.com/watch?v=9-c_iB10Wqk

As an example, these are some of the tasks that the orchestration scenario implements:

Administrative or automated decision is made to move the pool,

- Scripting or orchestration initiates the migration of storage from the primary data center to the secondary data center for the first host.
- Once storage is completed, the memory portion of the host is moved to the secondary data center.

- This process is repeated until 50% of the hosts are migrated at which point, GTM is instructed to direct traffic to the secondary data center,
- Host migration is completed, at which point, any traffic still arriving at the primary data center because of DNS or browser cache are retransmitted to the secondary data center through the use of Priority Pool Activation.

Configuring the BIG-IP GTM

F5's Global Traffic Manager must be configured to direct traffic to the correct LTM virtual server. In our example, we send all traffic to the primary data center, unless the utilization alarms we configure are triggered.

There are multiple ways to configure the BIG-IP GTM with Long Distance Live Migration. The most common methods are active/standby, where the GTM fails over an entire data center once all migrations are complete, or active/active, where the GTM sends traffic go to both data centers. In this section, we provide guidance on active/standby and active/active configurations.

In this guide, the GTM monitors traffic at the Wide IP level regardless of whether you are using an active/standby or active/active configuration. Specifically, every Long Distance Live Migration event with vMotion which requires global traffic management (I.e, vMotion events that are associated with incoming Virtual IP Addresses) should use the BIG-IP GTM to control the Wide IP. If your virtual machines do not have Internet virtual IP addresses, the BIG-IP GTM may not be necessary. In the following procedures, while we provide instructions on how to configure the GTM for basic functionality, we focus on the configuration of the Wide IP.

For example, this configuration focuses on an HTTP virtual server that has pool members which will be migrated with vMotion from a primary data center to a secondary data center. During the move process, it is likely that some virtual machines will be in the primary data center and some will be in the secondary. In the active/standby configuration, the GTM will update the Wide IP corresponding to the active data center when all of the machines have moved. In the active/active configuration, the GTM can provide addresses in a ratio based on how many machines are in each data center.

Ultimately, the choice of how GTM distributes IPs is one that depends on the nature of your application, the strategy option used for hosting your applications, and the ability of your virtual machines to service the load required to service all requests.

BIG-IP GTM initial configuration

In this section, we configure communication between the BIG-IP GTM and the LTM devices in this configuration. After this has been completed, we configure the Long Distance Live Migration components.

Creating the data centers

In this task you need to create two data centers, called Primary and Secondary respectively, that correspond to your physical data centers.

To create the data centers

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. In our example, we type **Primary**.
4. Complete the rest of the configuration as applicable for your deployment.
5. Click the **Finished** button.
6. Repeat this procedure for the Secondary data center.

Creating the GTM Server objects

Next, we create the GTM Servers. A server defines a specific system on the network.

Important

*You must add a Server object for the BIG-IP GTM you are currently configuring and every GTM that is a part of the sync group. For more information on GTM sync groups, see the online help or GTM documentation.
You must also add a Server object for each BIG-IP LTM in this configuration.*

To create the GTM servers

1. On the Main tab, expand **Global Traffic** and then click **Servers**.
2. Click the **Create** button. The New Server screen opens.
3. In the **Name** box, type a name that identifies this GTM. In our example, we type **GTM-1**.
4. From the **Product** list, select the either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.
5. In the **Address List** section, type the self IP of this GTM, and then click the **Add** button.

Important

Be sure to use a Self IP address and not the Management address of the BIG-IP.

If you selected *BIG-IP System (Redundant)* in step 4, type the appropriate IP address in the Peer Address List section.

6. From the **Data Center** list, select the appropriate Data Center you created. In our example, we select **Primary**.
7. *Optional - recommended:* In the **Health Monitors** section, from the **Available** list, select the monitor type **bigip** and then click the Add (<<) button.
8. From the **Virtual Server Discovery** list, select **Enabled**. (We strongly recommend Enabling Discovery, however you can leave this set to Disabled and manually configure the virtual server information).
9. Click **Finished**.
10. Repeat this entire procedure if there are other GTM devices in your configuration.
11. Repeat this entire procedure for each **BIG-IP LTM** in your configuration.

Important

Enabling trust between BIG-IP LTM and GTM

The next task is to enable trust between the GTM and the LTM devices. The following tasks must be performed from the command line.

On the BIG-IP GTM

To add a BIG-IP LTM to the GTM, you must make sure the **big3d** agent is on the same version on the BIG-IP LTM and GTM.

From the GTM device command line, use the following command syntax:

big3d_install <IP address of target LTM>

where the target system is the LTM that you want to add as a server on the GTM. This pushes out the newest version of big3d.

Repeat for each BIG-IP LTM in this configuration.

Next, type

bigip_add

to exchange keys with the LTM. Type the password at the prompt.

If the boxes are communicating over iQuery, you see a list of configuration information from the remote BIG-IP.

You must run the **bigip_add** command for every BIG-IP LTM in the configuration.

On the BIG-IP LTM devices

To complete the trust relationship, you must add the GTM device from the LTM devices.

From the LTM command line, use the following command syntax:

/usr/local/bin/bigip_add <self IP address of target GTM>

Type Yes if you get an authenticity message. Type the password for the GTM device when prompted.

Repeat this command on each BIG-IP LTM system.

 **Checkpoint**

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

Checkpoint: Testing the configuration

To test the configuration, from the BIG-IP GTM command line, use the following syntax:

iqdump <ip address of remote LTM>

You should see a list of virtual server information, including virtual server score, if you have configured the virtual score monitor.

Configuring the BIG-IP GTM for Long Distance Live Migration

Use the following procedures to configure the GTM for Long Distance Live Migration.

Creating the monitor

The next step is to create a health monitor. In our example, we are showing how to do Long Distance Live Migration with an HTTP virtual server, so we configure a HTTP monitor.

To create the 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. In our example, we type **VM-http-monitor**.
4. From the **Type** list, select **HTTP**.
5. Configure the options as applicable for your deployment.
6. Click the **Finished** button. The new monitor is added to the list.

Creating the GTM pool

The next task is to create a pool on the BIG-IP GTM system that includes the LTM virtual server in the primary data center, and one that includes the LTM virtual server in the secondary data center. The secondary data center pool should be Disabled after creation

To create a GTM pool

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 **Primary_pool**.
4. In the Health Monitors section, from the **Available** list, select the name of the monitor you created above, and then click the Add (<<) button. In our example, we select **VM-http-monitor**.
5. In the Load Balancing Method section, choose the load balancing methods from each list as appropriate for your configuration.

The two primary methods we recommend are either Global Availability or VS Score. As described in the introduction to this section, the Global Availability monitor is used in active/standby scenarios and VS Score is used in active/active scenarios.

In our example, from the **Preferred** list, we select **VS Score** to dynamically direct traffic between data centers based on the virtual location monitor on the LTM.

6. In the Member List section, from the **Virtual Server** list, select the virtual server you created for the application, and click the **Add** button. Note that you must select the virtual server by IP Address and port number combination. In our example, we select **10.133.39.51:80**.
7. Configure the other settings as applicable for your deployment.
8. Click the **Finished** button.

Creating a wide IP on the GTM

The final step in the GTM configuration is to create a wide IP that includes both newly-created pools, and uses the fully qualified domain name (FQDN) you wish to use for the application. In our example, we use `vmhttp.siterequest.com`.

To create a wide IP

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. In our example, we type **vmhttp.example.com**.
4. From the **State** list, ensure that **Enabled** is selected.
5. From the Pools section, from the **Load Balancing Method** list, select a load balancing method appropriate for your configuration.
6. In the Pool List section, from the **Pool** list, select the name of the pool you created above, and then click the **Add** button. In our example, we select **Primary_pool**.
7. Repeat this step for the remote pool.
8. All other settings are optional, configure as appropriate for your deployment.
9. Click the **Finished** button.

Note that you should make the Wide IP authoritative so that Local DNS's on the Internet resolve to the correct GTM pool.

This completes the basic GTM configuration. For more advanced GTM configuration options, see the BIG-IP GTM documentation.

Appendix A: Configuration worksheets

In this section, we provide mostly blank configuration worksheets you can use to assist with the implementation in this guide. We have left our network names and IP address in the grey column for reference.

Configuration table for BIG-IP objects

Network	Primary Data Center	Secondary Data Center	Notes
Private-WAN	10.133.64.0/24 Network	192.168.64.0/24 Network	This network is used to transport WOM and EtherIP traffic.
VLAN			Although the tags are the same in our example, each data center may have different tags.
Self IP for WOM			Port Lockdown set to Allow None
Self IP for EtherIP			Port Lockdown set to Allow Default
Route			Long distance live migration is a routed solution.
Internal-LAN	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp connectivity.
VLAN			This is used as the default gateway for ESX and NetApp. This is an untagged VLAN
Self IP			Port Lockdown set to Allow Default
Route			Routing is only necessary if local ESX and NetApp require it.
Servers (pool members)	10.133.66.0/24 Network	10.133.66.0/24 Network	This network is used for pool members and they are the same in both data centers
VLAN			Although tags are the same in our example, each data center may have different tags.
Self IP			Port Lockdown set to Allow Default
Route			Routing is only necessary if local pool members require it.
Client (virtual servers)	10.133.67.0/24 Network	192.168.67.0/24 Network	This network is used for external traffic and is usually publicly routable
VLAN			Although tags are the same in our example, each data center may have different tags.
Self IP			Port Lockdown set to Allow Default
Route			

Configuration worksheet for ESX, NetApp, and Servers

Network	Primary Data Center	Secondary Data Center	Notes
Storage Origin	10.30.30.0/24 Network	10.30.30.0/24 Network	This is a local only network between NetApp and ESX.
VLAN			This is a local only network and VLANs are not required.
IP address			This is the E0A interface.
Default Gateway			This is a local only network and default gateways are not required.
Storage Cache	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp FlexCache connectivity.
VLAN			This is an untagged network (no VLAN tags on NetApp)
IP address			This is the E0B interface.
Default Gateway			The default gateway is the Self IP address of the local BIG-IP.
vMotion	10.133.65.0/24 Network	192.168.65.0/24 Network	This network is used for local ESX and NetApp FlexCache connectivity.
VLAN			ESX VMkernel for vMotion must be tagged appropriately.
IP address			
Default Gateway			The default gateway is the Self IP address of the local BIG-IP.
Pool members (servers)	10.133.66.0/24 Network	10.133.66.0/24 Network	This network is used for pool members and they are the same in both data centers
VLAN			Tagging is not necessary as ESX handles this function.
IP address			Assign IP addresses for your servers as you normally would.
Default Gateway			The default gateway is the Self IP address of the local BIG-IP.

Appendix B: Frequently Asked Questions

Q: Doesn't vMotion require ESX hosts to share a layer 2 bridge? How does this work over a traditional WAN, like the Internet?

A: A common misconception is that vMotion requires a layer 2 bridge to work across a WAN. However, the only technical requirement from a network standpoint for vMotion to succeed is that the network from the guest VM perspective remain identical. This means the guest IP address remains unchanged, and all port groups which touch the guest exist in the source and target ESX hosts. The vMotion traffic itself uses the VMkernel port of ESX, and this does not have to be identical on each host. It is through the VMkernel port and default gateway (which is not shared by the guest VM) that we route traffic across the iSession tunnel.

Q: Can you summarize what IP addresses are different, and why?

A: The following tables summarize the key network IP addresses.

IP Address	Description	Different for each data center?
LTM virtual server	Public IP which is used for client connections between clients and the LTM. The GTM determines which LTM virtual server to direct clients to when they initialize new application connections.	Yes
VM guest IP	The IP address the guest uses to receive and respond to client requests.	No
ESX VMkernel IP	Used for vMotion and Storage vMotion traffic.	Yes
ESX VMkernel default gateway	The gateway used to route vMotion traffic between hosts.	Yes. Specifically, this value will be a self IP on the local LTM of each data center

Q: The guide mentions use of a dedicated migration host in each data center to transition from one vCenter to another. Can you elaborate?

A: An alternative deployment scenario would leverage a dedicated host in each data center to be used for long distance live migration, analogous to a dedicated host in VMware Fault Tolerant deployments. This host would not be a member of any DRS or HA resource pools, nor would it use any Distributed Virtual Switches you may have in your cluster. In this scenario, the dedicated hosts in each data center would only have to be able talk to the other hosts on the Service Console network (or Management Network on ESXi), and have the same port groups which are accessed by the VM configured on the standard switch(es) of that host (as required by vMotion).

The work flow of migrating a virtual machine from, for example, a DRS cluster from one data center into a DRS cluster in the other data center would work as follows:

1. Both transition hosts would be initially managed by the vCenter in the primary data center.
2. Configure the hosts with access to a datastore in both the primary and secondary data centers.
3. vMotion the VM from the DRS resource pool to this dedicated host.
4. Storage vMotion, then vMotion the VM from the primary dedicated host/datastore to the secondary dedicated host/datastore.

5. De-register the secondary host from vCenter in the primary site.
6. Register this host with the vCenter in the secondary site.
7. vMotion the VM from this host into the secondary DRS resource pool in the target data center.

Q: Do any MAC addresses change during vMotion? What about ARPs and reverse ARPs?

A: No. A key principle of vMotion is that the networking stack from the guest perspective remains exactly the same before and after a vMotion. In a typical LAN scenario, a reverse ARP is issued at the completion of the vMotion in order to tell the local router that traffic bound for the VM has moved guests, and to direct that traffic to the new MAC address of the destination host. This is necessary because in a non-F5 enhanced vMotion event, both hosts are on the same broadcast domain.

However, in this solution, the guest has moved from a host in one physical data center to another. The task of routing traffic bound for the guest is managed not by a single local router, but by GTM and LTM. When the guest arrives in the secondary data center, inbound connections continue to reach the guest VM, because GTM and the LTMs are aware of the guest's location dynamically, and will route those inbound connections to the correct data center where the guest lives at that moment in time. MAC addresses do not change on the guest nor the hosts.

Q: What are the optimal use cases for F5's long distance live migration solution?

A: A key element of this solution is the transparent redirection of inbound connections between clients and application VMs. Migrating web applications between data centers is the ideal use case for this type of solution, as web applications have many short lived connections between clients and servers. Web applications are almost always session based, meaning once a user begins using a web application, it is important that all requests from that user persist to the same VM. Should that VM migrate from one data center to another, requests from an existing user session must continue to reach the same VM. The F5 solution meets these requirements transparently and effectively, making it an ideal use case.

Applications that have long-lived persistent connections, such as SSH, telnet, or streaming media, are not good use cases. Similarly, any applications that are highly transactional, such as database applications, are not good use cases for the solution. Attempting to perform a Storage vMotion (whether local or over long distance) of a database is not recommended and such use cases are better addressed using database replication solutions from storage vendors, which are purpose built for moving and synchronizing highly transactional data between sites.

Q: What are some suggested strategies for automating this solution?

A: One of the key benefits of both VMware and F5 solutions is the ability to automate complex tasks through published APIs. Automation decreases the risk of human error, simplifies complexity, and reduces operating costs associated with a task by streamlining workflow.

Fortunately, this solution lends itself quite well to automation. Many organizations already have workflow engines in their environment to automate tasks. Others develop scripts in-house for common functions. In either scenario, the discreet steps of executing a long

distance live migration can be programmatically executed using the VMware vSphere Web Services

API:

1. Execute the Storage vMotion
2. Execute the vMotion
3. (optionally) De-register host with vCenter in the primary data center
4. (optionally) Register host with vCenter in secondary data center.

For further discussion on VMware or vMotion, visit the VMware forums on DevCentral:

<http://devcentral.f5.com/Default.aspx?tabid=53&view=topics&forumid=46>

Document Revision History

Version	Description
1.0	New Version
1.1	Inserted the correct configuration worksheet for BIG-IP objects on <i>page 42</i>
1.2	Changed "long distance vMotion" to "long distance live migration"
1.3	- Corrected VLAN names and IP addresses in our examples for the Advertised routes on pages 24 and 26. - Moved Revision history to the end of the document
1.4	Clarified and enhanced BIG-IP GTM configuration

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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

