# HP Serviceguard for Linux with VMware virtual machines

## Table of contents

- About this paper .......................................................................................................................................................... 2
- Terminologies and symbols used in this document ........................................................................................................ 2
- Introduction .................................................................................................................................................................... 3
- Supported cluster deployment models with VMware virtual machines ........................................................................ 4
  - Cluster with VMs only from one host .......................................................................................................................... 5
  - Cluster with one or more VMs each from multiple hosts ............................................................................................ 5
  - Cluster with one VM each from multiple hosts ............................................................................................................. 6
  - Clusters with VMs and physical machines ..................................................................................................................... 6
- Disaster recovery clusters using VMware virtual machines ............................................................................................ 8
  - Extended Distance Cluster deployment models ........................................................................................................... 8
  - Metrocluster deployment models ................................................................................................................................. 8
  - Continental clusters deployment models .................................................................................................................... 10
- Configuring a VMware virtual machine ........................................................................................................................ 10
- Configuration requirements for a Serviceguard cluster with VMware guests ................................................................ 11
  - Network configurations ............................................................................................................................................... 11
  - Shared storage configurations ................................................................................................................................... 12
- Prerequisites for VMware guests used as cluster nodes ................................................................................................ 26
  - VMware tools ............................................................................................................................................................. 26
  - SCSI persistent reservation (sg_persist) ....................................................................................................................... 26
- Serviceguard support for VMware vMotion .................................................................................................................... 27
  - Prerequisites ............................................................................................................................................................... 27
  - Migrating virtual machines that are Serviceguard nodes .......................................................................................... 27
- Summary of requirements ................................................................................................................................................ 29
- Summary of recommendations ......................................................................................................................................... 29
- Support information ........................................................................................................................................................ 29
- Summary ........................................................................................................................................................................... 29
- References ....................................................................................................................................................................... 30

Click here to verify the latest version of this document
About this paper

Virtual machine (VM) technology is a powerful capability that can reduce costs and power usage, while also improving resource utilization. HP applies virtualization to various aspects of the data center—uniting virtual and physical resources to create an environment suitable for deploying mission-critical applications.

HP Serviceguard for Linux® is certified for deployment on VMware® VMs created on VMware ESX/ESXi Server running on industry-standard HP ProLiant servers.¹ This white paper discusses the various ways a VMware VM can be deployed in a Serviceguard for Linux cluster, Extended Distance Cluster, Continentalclusters and a Metrocluster. The paper describes how you can configure a cluster using VMs from single host and multiple hosts, as well as a combination of VMs and physical machines, to provide high availability (HA) for your applications. Reasonable expertise in the installation and configuration of HP Serviceguard for Linux and ESX/ESXi Server, as well as familiarity with their capabilities and limitations, is assumed.

This white paper provides details on recommended network and storage configurations for VMs used as Serviceguard cluster nodes. In addition, this paper recommends how to eliminate single point of failures and provides pointers to other useful, relevant documents as appropriate.

For the complete list of supported operating systems, certified configurations, ESX/ESXi Server, and storage with the listed version of HP Serviceguard for Linux release, please refer to the “HP Serviceguard for Linux Certification Matrix” document at hp.com/go/linux-serviceguard-docs.

Note

Except as noted in this technical white paper, all HP Serviceguard configuration options documented in the “Managing HP Serviceguard for Linux manual” are supported for VMware guests, and all the documented requirements apply.

Terminologies and symbols used in this document

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware host, host</td>
<td>Physical server on which the VMware hypervisor is installed</td>
</tr>
<tr>
<td>VM guest, guest VM</td>
<td>VMware virtual machine carved out of the hypervisor</td>
</tr>
<tr>
<td>Physical machine</td>
<td>Physical server configured as a Serviceguard cluster node</td>
</tr>
<tr>
<td>NIC</td>
<td>Network interface card</td>
</tr>
<tr>
<td>Cluster, Serviceguard cluster</td>
<td>HP Serviceguard for Linux cluster</td>
</tr>
<tr>
<td>HA</td>
<td>High availability</td>
</tr>
<tr>
<td>OS</td>
<td>Operating system</td>
</tr>
<tr>
<td>SPOF</td>
<td>Single point of failure</td>
</tr>
<tr>
<td>NPIV</td>
<td>N_Port ID Virtualization</td>
</tr>
<tr>
<td>RDM</td>
<td>Raw device mapping</td>
</tr>
</tbody>
</table>

¹ For the latest details concerning alliances and partnership, visit hp.com/go/vmware and vmware.com/en/partners/global-alliances/hp/overview.html.
Table 2. Symbols used in this document

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Virtual Machine guest which is a Serviceguard cluster node" /></td>
<td>Virtual Machine guest which is a Serviceguard cluster node</td>
</tr>
<tr>
<td><img src="image2" alt="Hypervisor/Virtual Machine Host" /></td>
<td>Hypervisor/Virtual Machine Host</td>
</tr>
<tr>
<td><img src="image3" alt="Physical machine which is a Serviceguard cluster node" /></td>
<td>Physical machine which is a Serviceguard cluster node</td>
</tr>
<tr>
<td><img src="image4" alt="HP Serviceguard" /></td>
<td>HP Serviceguard</td>
</tr>
<tr>
<td><img src="image5" alt="Serviceguard Package" /></td>
<td>Serviceguard Package</td>
</tr>
<tr>
<td><img src="image6" alt="Shared storage" /></td>
<td>Shared storage</td>
</tr>
</tbody>
</table>

**Introduction**

VMware VMs are increasingly deployed for server consolidation and flexibility. VM technology allows one physical server to simulate multiple servers, each concurrently running its own OS. In virtual machine technology, the virtualization layer (also known as the hypervisor) abstracts the physical resources so each instance of an OS appears to have its own NIC, processor, disk, and memory, when in fact they are virtual instances. This abstraction allows you to replace numerous existing physical servers with just one, but at the cost of greater exposure to single point of failure.

HP Serviceguard for Linux software is designed to protect applications and services from planned and unplanned downtime. By packaging an application or service with its associated resources, and moving that package to other servers as needed, Serviceguard for Linux ensures 24x7 application availability. Packages can be moved automatically when Serviceguard detects a failure in a resource, or manually to perform system maintenance or upgrades. By monitoring the health of each server (node) within a cluster, Serviceguard for Linux can quickly respond to failures such as those that affect processes, memory, LAN media and adapters, disk, operating environments, and more.

HP Serviceguard for Linux running on VMs provides a significant level of protection. Specifically, it fails over an application when any of a large number of failures occurs, including:

- Application failure
- Failure of any of the components in the underlying network infrastructure that can cause failure of the application network
- Failure of storage
- An OS “hang” or failure of the virtual machine itself
- Failure of the physical machine

In addition, HP Serviceguard for Linux provides a framework for integrating custom user-defined monitors, using the generic resource monitoring service.

---

2 A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware, or hardware that creates and runs virtual machines.
Beyond increased failure protection, HP Serviceguard for Linux also offers other advantages, such as:

- Faster failover of monitored applications
- Rolling upgrades, allowing for less planned downtime
  - With HP Serviceguard for Linux, an application (package) can be moved off a virtual machine and restarted on another node in the cluster. The "empty" server can then have its OS or applications upgraded while those applications remain available to users, since they are running on other nodes.
- HP Serviceguard for Linux with the VMware vMotion feature enables you to move an entire running virtual machine from one physical server to another with no downtime. The virtual machine retains its network identity and connections, ensuring a seamless migration process with no perceivable impact to the end user.

HP Serviceguard for Linux, combined with VMware software solutions, can protect your applications, while also optimizing the cost, with no compromises on application availability and reliability.

## Supported cluster deployment models with VMware virtual machines

An HP Serviceguard for Linux cluster that includes virtual machines as cluster nodes have multiple deployment model.

The following table provides a summary of the supported models with Fibre Channel (FC) and iSCSI as shared storage in a Serviceguard cluster. Please refer to the appropriate sections in this document to find out more about each supported model.

<table>
<thead>
<tr>
<th>Supported cluster models</th>
<th>Shared storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FC (RDM)</td>
</tr>
<tr>
<td>Cluster with VMs from a single host as cluster nodes</td>
<td>✗</td>
</tr>
<tr>
<td>Cluster with one or more VMs each from multiple hosts as cluster nodes</td>
<td>✗</td>
</tr>
<tr>
<td>Cluster with only one VM each from multiple hosts</td>
<td>✓</td>
</tr>
<tr>
<td>Cluster with VMs and physical machine as cluster nodes</td>
<td>✓</td>
</tr>
<tr>
<td>Extended Distance Cluster (XDC) deployment models</td>
<td>✓</td>
</tr>
<tr>
<td>Metrocluster deployment models</td>
<td>✓</td>
</tr>
<tr>
<td>Continental clusters deployment models</td>
<td>✓</td>
</tr>
</tbody>
</table>

* With HP 3PAR as shared storage NPIV is not yet supported.
Cluster with VMs only from one host

In this configuration, a cluster is formed with VMware guests all of which are carved out of a single host (cluster-in-a-box), as shown in figure 1. Even though this configuration provides consolidation of resources, it is not an ideal solution. A failure of the host would bring down all the nodes in the cluster thus making the host a single point of failure (SPOF). Hence, the configuration is not recommended. In this configuration as more than one VM from the same host is participating in a single cluster, the use of the NPIV enabled storage infrastructure is mandatory when using FC devices as shared storage. iSCSI devices exposed using software initiator can also be used as shared storage in this model.

Figure 1. Cluster-in-a-box

Cluster with one or more VMs each from multiple hosts

In this deployment model, a cluster can be formed with a collection of VMs that are hosted on multiple hosts and with more than one VM coming from all or some of the hosts as shown in figure 2.

In such a model when using FC devices as shared storage the use of NPIV enabled storage infrastructure becomes mandatory. iSCSI devices exposed using software initiator can also be used as shared storage.

One must also ensure that the VM nodes are so distributed across the hosts; that the failure of any one of the hosts should not result in more than half of the cluster nodes going down. As shown in figure 2 the correct distribution would be, two VMs each on two hosts configured as cluster nodes, rather than three VMs from Host1 and one VM from the Host2. In the latter case, the failure of the host with three VM cluster nodes would bring down the entire cluster.

Serviceguard is installed on the VM cluster nodes and it provides high availability to the applications running as packages in these VMs. In case of failures, Serviceguard fails over the application packages to other adoptive cluster nodes.

Figure 2. Cluster with one or more VMs each from multiple hosts
Cluster with one VM each from multiple hosts

In this model, a cluster can be formed with multiple guests hosted on multiple hosts, where only one guest from each host is used as a node in a cluster as shown in figure 3. In other words, one host can have multiple guests all of which can be part of different clusters, but no two guests from the same host can belong to the same cluster. This configuration does not mandate the use of NPIV enable storage infrastructure when using FC devices as shared storage. iSCSI devices exposed using software initiator can also be used as shared storage in this model.

Serviceguard is installed on the VM cluster nodes and it provides high availability to the applications running as packages in these VMs. In case of failures, Serviceguard fails over the application packages to other adoptive cluster nodes.

Clusters with VMs and physical machines

In this deployment model, a combination of VMware guests and physical machines can be used as nodes in a Serviceguard cluster, as shown in figures 4 and 5. Serviceguard is installed on the VMware guests and physical machines, and a cluster is formed among them. Serviceguard provides high availability to the applications running as packages in the VMs and physical machines. In case of failures, Serviceguard fails over the application to other adoptive cluster nodes. The application can be failed over from a VM to a physical machine and vice versa.

As mentioned above, the cluster nodes must be equally distributed to ensure that a host does not become a single point of failure (SPOF). If more than one guest from a given host needs to be used in the cluster (as shown in figure 5), and FC devices are used as shared storage then using NPIV enabled storage infrastructure becomes mandatory. If NPIV is not used, then only one guest from a given host can be used in a given cluster (as shown in figure 4). iSCSI devices exposed using software initiator can also be used as shared storage in both these models as shown in figure 4 and figure 5.

This is a very powerful model where the application can primarily run on the physical machine and in case of failures can fail over to an adoptive VM. Thus enabling users to take advantage of the performance of a physical machine, and at the same time allowing for consolidation of standby resources.
Figure 4. Hybrid cluster—Mix of Physical machines and one VM each from multiple hosts as cluster node

Figure 5 shows how you can configure a cluster that combines all of above-mentioned models. The diagram includes two guests from a host participating in a cluster, which means NPIV is mandatory.

Figure 5. Hybrid cluster—Mix of Physical machines and one or more VMs each from multiple hosts
Disaster recovery clusters using VMware virtual machines

Extended Distance Cluster deployment models

VMware guests can also be used as cluster nodes in an Extended Distance Cluster (XDC). You can form an XDC with guests spanning across two different sites, where each guest is carved out of a different host, as shown in figure 6. Currently, multiple guests from a host cannot be used in one Extended Distance Cluster using FC shared storage as this mandates the use of NPIV enabled storage infrastructure, which is currently not certified for use in an XDC environment. However, a host can have multiple guests all belonging to different XDCs. When using iSCSI devices as shared storage the above-mentioned restriction does not apply and one or more VMs from a host can belong to one XDC. An XDC can also have a mix of Physical machines and VMs.

Figure 6. Extended Distance Cluster with one VM each from multiple hosts

Metrocluster deployment models

VMware guests can also be used as cluster nodes in a Metrocluster where the VMs are spanning across two different sites. There are two models of deployment possible when using VMs in a Metrocluster.

In the first model, a cluster is formed with a collection of VMs where each VM cluster node is hosted on a different host as shown in figure 7. As discussed in section “Cluster with one VM each from multiple hosts” multiple guest from a hosts can all be part of different clusters, however, no two guests from the same host can be part of one cluster. This model does not mandate the use of NPIV enabled storage infrastructure when using FC devices as shared storage.

In the second model, a cluster can be formed with a collection of VMs that are hosted on multiple hosts and with more than one VM coming from all or some of the hosts as shown in figure 8. This model mandates the use of NPIV enabled storage infrastructure when using FC devices as shared storage.

A Metrocluster can also have a mix of Physical machines and VMs, where the VMs are deployed as per the two models discussed above.
Figure 7. Metrocluster with one VM each from multiple hosts

Figure 8. Metrocluster with one or more VMs each from multiple hosts

Note
As of writing of this document, VMware NPIV is not certified for use with HP 3PAR StoreServ arrays. Thus when using HP 3PAR arrays as shared storage in a Metrocluster the model described in figure 7 alone is supported.
For more information about Metrocluster, please see the document entitled, “Understanding and Designing Serviceguard Disaster Recovery Architectures” at hp.com/go/linux-serviceguard-docs.

**Continentalclusters deployment models**

VMware VMs can be used as Serviceguard cluster nodes in Continentalclusters. In Continentalclusters, distinct clusters are separated by large distances, with a wide area network (WAN) used to connect them. Continentalclusters are configured using two or more Serviceguard clusters. The individual clusters can be created as per the models described in the above sections. All the requirements and restrictions listed in the above section for configuration, deployment of a cluster, Metrocluster are all applicable when configuring a cluster and/or array based replication in a Continentalcluster.

For more information about Continentalclusters, please refer to the document entitled, “Understanding and Designing Serviceguard Disaster Recovery Architectures” at hp.com/go/linux-serviceguard-docs.

*Figure 9. Continental clusters with VMs*

---

**Configuring a VMware virtual machine**

For detailed steps and instructions on how to configure, manage, and administer a virtual machine using VMware ESX/ESXi Server, please refer to the VMware document entitled, “Server Configuration Guide” (in References section). The resources allocated to the VMs depend on the requirements of the applications deployed on the VMs, as well as the resources available to the host. For configuration limitations, rules and restrictions, sizing, and capacity planning, please refer to the document entitled, “Configuration Maximums for VMware vSphere 5” (in References section).

HP Serviceguard for Linux places no limits on the number of guests that you can provision on one host. For all provisioning guidelines, please refer to the VMware documentation. For resource planning, please follow the recommendation specified by the OS or application.
Configuration requirements for a Serviceguard cluster with VMware guests

Network configurations

To avoid single point of failure, HP Serviceguard for Linux recommends you deploy a highly available network configuration with redundant heartbeats and data networks. The following section describes how to achieve network redundancy using a VMware NIC teaming configuration.

Use VMware NIC teaming at the host level for all networks used by the applications that run on VMware guests. Do not use NIC teaming at the guest level.

The HP Serviceguard configuration requires at least two heartbeat links; so if the applications need multiple data networks, you might need to share the logical NICs for data and heartbeats. Practical difficulties might arise when allocating more than a certain number of logical NICs in a virtual machine. This number varies, depending on the VMware ESX/ESXi version. For more information, please refer to the document entitled, “Configuration Maximums for VMware vSphere 5 or later,” (in References section).

Use VMware NIC teaming to avoid single point of failure

VMware virtual machines use virtual network interfaces. As HP Serviceguard does not support channel bonding of virtual NICs, you should use VMware NIC teaming instead.

VMware NIC teaming at the host level provides the same functionality as Linux channel bonding—enabling you to group two or more physical NICs into a single logical network device called a bond. After a logical NIC is configured, the virtual machine no longer knows about the underlying physical NICs. Packets sent to the logical NIC are dispatched to one of the physical NICs in the bond interfaces; packets arriving at any of the physical NICs are automatically directed to the appropriate logical interface.

You can configure VMware NIC teaming in load-balancing or fault-tolerant mode. You should use fault-tolerant mode to get the benefit of HA.

When VMware NIC teaming is configured in fault-tolerant mode, and one of the underlying physical NICs fails or its cable is unplugged, ESX/ESXi Server detects the fault condition and automatically moves traffic to another NIC in the bond interfaces. Doing so eliminates any physical NIC as a single point of failure, and makes the overall network connection fault tolerant. This feature requires the beacon monitoring feature (see the “VMware Server Configuration Guide” in References section) of both the physical switch and ESX/ESXi Server NIC team to be enabled. (Beacon monitoring allows ESX/ESXi Server to test the links in a bond by sending a packet from one adapter to the other adapters within a virtual switch across the physical links.)

While using VMware NIC teaming, the networking requirements of a Serviceguard cluster might not be met. In such situations, you will see a warning message while applying the cluster configurations.

WARNING: Minimum network configuration requirements for the cluster have not been met. Minimum network configuration requirements are:

- Two (2) or more heartbeat networks OR
- One (1) heartbeat network with local switch (HP-UX Only) OR
- One (1) heartbeat network using APA with two (2) trunk members (HP-UX Only) OR
- One (1) heartbeat network using bonding (mode 1) with two (2) slaves (Linux Only)

You can safely ignore the message and continue with the cluster configuration.

---

3 At the time of this writing, vSphere 5 allows up to 10 NICs to be configured per virtual machine.
4 Bonds generated by VMware NIC teaming are different from bonds created by channel bonding.
Shared storage configurations

HP Serviceguard for Linux is a high-availability cluster that requires application data to be in shared storage, which is accessible from all adoptive cluster nodes. When using VMware guests as cluster nodes, iSCSI and Fibre Channel devices can be used as shared storage.

Shared storage configuration for VMware guest nodes using Fibre Channel devices
You can configure Fibre Channel devices as shared storage using raw device mapping (RDM) or RDM with NPIV.

Shared storage configurations using raw device mapping (RDM)
To accommodate scenarios where external physical machines must share block-level data with a virtual machine, ESX/ESXi server allows raw LUNs to be presented to the virtual machine by means of RDM. When using VMware guests as cluster nodes, you must use RDM to configure the FC disk as shared storage.

Creating and exposing a new RDM-mapped disk to a VM
To modify the configuration of a virtual machine, you must first power it down. To add a LUN to a virtual machine in RDM mode, invoke the Add Hardware wizard. On a VMware vSphere client, right-click the node to which you want to add the disk, and then select Edit Settings to start the wizard.

Figure 10. Start the wizard by selecting Edit Settings

5 In this paper, we used vSphere Client 5.0. The screens might look different on other versions of vSphere.
To add the device, click the Add button above the hardware listing, as shown in figure 11.

**Figure 11.** Select Add from the Hardware list

From Add Hardware, select Hard Disk from the Device Type menu.

**Figure 12.** Select Hard Disk
Click the Raw Device Mappings radio button, as shown in figure 13. If the RDM option is disabled, the system indicates that there is no free LUN available for mapping. If the LUNs are exposed to the ESX/ESXi server, and if the system indicates that no LUNs are available for mapping, you might need to reboot the ESX/ESXi server. Make sure all VMs are powered down when you reboot the ESX/ESXi server.

**Figure 13.** Select Raw Device Mappings

Select the Target LUN from the list of available LUNs, as shown in figure 14.

**Figure 14.** Select Target LUN
Select a Datastore to store the LUN mapping file, as shown in figure 15.

**Figure 15.** Select a Datastore

Next, you need to select the Compatibility Mode. Select Physical, as shown in figure 16. This option allows the guest OS to access the LUN directly.

**Figure 16.** Selecting the Compatibility Mode
Specifying Advanced Options for the selected virtual disk is the next step. In the screen shown in figure 17, the drop-down list shows SCSI (1:0), SCSI (1:1) SCSI (1:15). The first number identifies the SCSI controller, and the second number is the sequence of the LUN or disk. Select a separate SCSI controller, for example SCSI (1:x), for the newly added LUNs. VMware reserves SCSI (0:x) for the non-shared disks and SCSI (1:x) for the shared LUNs.

**Figure 17.** Select Advanced Options

Click Next to verify the selections, as shown in figure 18.

**Figure 18.** Ready to Complete menu
After you verify your selections, click Finish. This advances you to the Virtual Machine Properties screen, shown in figure 19. For the newly added hard disk, you can see Physical is selected under Compatibility mode. This selection allows virtual disks to be shared between virtual machines on any server.

**Figure 19. Virtual Machine Properties**

![Virtual Machine Properties](image)

For more details on SAN configuration options, please refer to the following documents:

- “VMware Infrastructure 3.x, HP Storage best practices” (in References section)
- “SAN System Design and Deployment Guide” (in References section)

If the previous steps are successful, the RDM-mapped disks will be visible in the VMs once they are booted up. To expose the same disk to the other cluster nodes that need to access it, follow the instructions in the section entitled, “Exposing an existing RDM-mapped disk to a VM.” Once the disks are exposed to all cluster nodes, then you can proceed with storage preparation, such as creating virtual groups and disk groups.

Exposing an existing RDM-mapped disk to a VM

To expose an existing RDM-mapped disk to a VM, follow these steps:

1. Right-click the VM and click Edit Settings.
2. From Virtual Machine Properties, choose Add from the Hardware list.
3. Select Hard Disk as the Device Type menu from the Add Hardware Wizard, and then click Next.
4. Click the Use an existing virtual disk radio button from the Select Disk menu, and then click Next (as shown in figure 20).
Figure 20. Select Use an existing virtual disk option

Select the disk file path from the Select Existing Disk menu, and then browse the path from Datastores or copy the vmdk path from the VM hard disk you configured earlier.

Figure 21. Select the Disk File Path
In the Advanced Options menu, choose the Virtual Device Node SCSI controller number, as shown in figure 22. Select the same SCSI controller number sequence that you selected earlier when configuring the VM, and then click Next.

**Figure 22.** Choose from the SCSI Virtual Device Node menu

Review the selected options for Hard Disk from the Ready to Complete tab, and then click Finish.

**Figure 23.** Ready to Complete menu
From the Virtual Machine Properties tab, verify the virtual device node and vmdk path, and then click OK.

**Figure 24.** Adding RDM in the Virtual Machine Properties menu

![Virtual Machine Properties](image)

**Note**

If the VMware setup is planned for vMotion, then the NPIV configuration (as explained in the following section) is mandatory. Additional required configuration changes are listed in the section entitled, "Shared storage configuration for vMotion when using RDM and NPIV".

*Shared storage configurations using RDM and NPIV*

When multiple guests from a single host need to be configured as cluster nodes in the same cluster, then you must use Fibre Channel NPIV in addition to RDM. NPIV configuration is mandatory if you plan to use the vMotion feature on guests configured as Serviceguard cluster nodes.
To modify the configuration of a virtual machine, you must first power it down. To configure NPIV to a virtual machine, invoke the Add Hardware wizard. On a vSphere client, right-click the node you need to configure with Fibre Channel NPIV, and then select Edit Settings to start the wizard (see figure 25).

**Figure 25.** Start the wizard by selecting Edit Settings

Next, select Fibre Channel NPIV in the Options tab under Advanced, as shown in figure 26.

**Figure 26.** Selecting Fibre Channel NPIV
Next, enable the NPIV by deselecting Temporarily Disable NPIV for this virtual machine, clicking the Generate new WWNs radio button, and selecting the Number of WWNs from the drop-down menu as required. Click OK.

**Figure 27.** Enable the Fibre Channel NPIV
NPIV is now enabled for the virtual machine. Verify that NPIV is enabled by navigating to Fibre Channel NPIV in the Options tab under Advanced. You should see the Node WWNs and Port WWNs in the WWN Assignments section (as shown in figure 28).

Figure 28. Verify Fibre Channel NPIV

Once the Node and Port WWNs have been generated (as shown in figure 28), you need to add them to the zoning configuration of the underlying FC infrastructure (SAN switch, storage, etc.). For more information on NPIV configuration with VMware, please refer to the document entitled, “Configuring and Troubleshooting N-Port ID Virtualization” (in References section). For information on NPIV zoning configuration, please refer to the appropriate document for your storage infrastructure.

Shared storage configuration for vMotion when using RDM and NPIV

If you need to use VMware vMotion with the guests configured as Serviceguard cluster nodes, you must use the following storage configurations on all cluster nodes.

1. Shared disks should be presented to guests in RDM mode with NPIV, as described above.
2. SCSI Bus Sharing Mode should be set to None for all RDM disk SCSI controllers.
   A. Right-click the VM and click Edit Settings.
   B. From the Hardware list, choose SCSI controller <n> (where <n> is the SCSI controller number).
   C. Click the None radio button for SCSI Bus Sharing policy, as shown in figure 29.
3. You must enable the “multi-writer” flag for all the RDM disks in the VM. You can do this by adding one entry per SCSI controller in the corresponding .vmx file, or by adding an entry to the RDM configuration of the disk.

- To add the previous configuration in the corresponding .vmx file of the VM, add one “scsiX:Y.sharing = multi-writer” entry for every SCSI controller in the VM, where “X” is the controller ID and “Y” is the disk ID on that controller.
- To add the configuration changes in the RDM configuration on the VM, follow these steps to enable the multi-writer flag:
  - Power off the VM.
  - Right-click the VM and click Edit Settings.
  - From the Advanced options, choose General.
  - Click the Configurations Parameters button.
  - Click the Add Row button.

Add rows for each of the shared disks, and set their values to multi-writer. For example, to share four disks, the configuration file entries look like this:

```plaintext
scsi1:0.sharing = “multi-writer”
scsi1:1.sharing = “multi-writer”
scsi1:2.sharing = “multi-writer”
scsi1:3.sharing = “multi-writer”
```
**Figure 30.** Set Configuration Parameters for multi-writer

![Configuration Parameters](image)

For more information on the vMotion feature, please refer to the Serviceguard Support for VMware vMotion section of this document.

**VMware multipathing when using RDM/RDM and NPIV**

Serviceguard currently does not support multipathing at host level. If there are multiple paths available for a LUN, only one path should be active. Rest of the other paths should be disabled as shown in figure below.

**Figure 31.** Disable all but one paths for a LUN

![Disable all but one paths for a LUN](image)
Shared storage configuration using VMDirectPath I/O
You can also use VMDirectPath I/O to configure shared storage. When using VMDirectPath I/O, you must exclusively assign a host bus adapter (HBA) device on the ESX host to one virtual machine, and then configure the shared storage. This solution is not scalable, as a dedicated HBA port is required for each virtual machine. For more details on VMDirectPath I/O, please refer to the document entitled, “Configuration Examples and Troubleshooting for VMDirectPath” (in References section).

Note
With the VMDirectPath I/O configuration, vMotion and several other features are not supported.

Shared storage configuration for VMware guest nodes using iSCSI devices
You can use iSCSI devices as shared storage when using VMware guests as Serviceguard cluster nodes.

Note
Only iSCSI devices exposed using iSCSI software initiator are supported.

Please refer to the appropriate operating system’s “Storage Administration Guide” (in References section) for steps on installing and configuring the software initiator for iSCSI. The VMware vMotion feature is also supported when using iSCSI as shared storage.

Prerequisites for VMware guests used as cluster nodes

VMware tools
VMware recommends you use VMware tools—a suite of utilities that enhances the performance of the VMs guest operating system. VMware tools also improve VM management by enabling some important functionality. For more information on the benefits of using VMware tools and installation instructions, please refer VMware documentation for installation and configuration of VMware tools. You can find the latest edition of the document at vmware.com/support/ws55/doc/ws_newguest_tools_linux.html.

SCSI persistent reservation (sg_persist)
Serviceguard requires the use of persistent reservation (PR) on all cluster nodes in all its cluster configurations. The PR functionality is provided by the sg3_utils rpm, which is part of the OS distribution.

While creating modular packages, the PR functionality is provided by the "sg/pr_cntl" module, which was introduced in Serviceguard for Linux A.11.19.00. You must add this module when creating the packages by using the following command:

```bash
# cmmakepkg –m sg/all -m sg/pr_cntl <new_pkg.conf>
```

From Serviceguard A.11.20.20 onward, this is a mandatory module; it is automatically added to the packages. If your existing packages do not include this module, you can add it manually by using the following command:

```bash
# cmmakepkg -i <existing_pkg.conf> -m sg/pr_cntl <new_pkg.conf>
```

If you are using legacy packages, please refer to the white paper entitled, “Migrating packages from legacy to modular style.” You can find this white paper at hp.com/go/linux-serviceguard-docs -> White papers.
Serviceguard support for VMware vMotion

The VMware vMotion feature enables the live migration of running virtual machines from one physical server to another with zero downtime—ensuring continuous service availability and complete transaction integrity. vMotion is supported in the VMs used as Serviceguard cluster nodes when you use the following configurations.

Prerequisites

Serviceguard supports vMotion with the following configurations:

• The VM nodes must be created using ESXi Server 5.1 or later and HP Serviceguard version must be A.11.20.xx onwards.
• The boot image/boot disk for the guests should reside on shared disks; they must be accessible from both source and destination hosts.
• The source and destination hosts should be accessible by a common VMware vCenter Server instance.
• The shared storage should be configured with Fibre Channel or iSCSI; all the configurations must be complete as described in the “Shared Storage Configuration for vMotion when using RDM and NPIV” section of this document.

Migrating virtual machines that are Serviceguard nodes

Serviceguard uses Live Application Detach (LAD) to support vMotion of VMs that are cluster nodes. To migrate a node, you must first detach it from the cluster, and then you can initiate vMotion for the node. Once the migration is complete, you can reattach the node to the cluster. If vMotion is performed without first detaching the node, the other Serviceguard cluster nodes might not be able to exchange heartbeat messages with the node that is being migrated. If this happens, the remaining cluster nodes would reform the cluster without the node that was migrated. This can lead to undesirable scenarios/results.

When LAD detaches a node from a Serviceguard cluster, the cluster services stop running on the node. As a result, there is no heartbeat exchange, and the other nodes in the cluster do not see the migration as a node failure. In addition, the packages continue to run in the detached state. For more details on LAD, please refer to the latest version of the user manual, located at hp.com/go/linux-serviceguard-docs -> User guide -> Managing HP Serviceguard A.12.00.00 for Linux.

To perform vMotion on a VM that is a Serviceguard cluster node, follow these steps:

1. Ensure that all prerequisites are met.
2. Detach the node that needs to be migrated using the cmhaltnode –d command.
3. Choose the host, where you will migrate the guest.
4. From VMware vCenter Server, move the node using the Migrate option, as shown in figure 32.  

**Figure 32.** Perform vMotion with the Migrate option

5. After the migration is complete, reattach the node using the `cmrunnode` command.

**Note**  
When migrating a VM cluster node for any maintenance activities, you might find that more than half of the cluster nodes are running on one host. In this situation, the host becomes a single point of failure, because failure of the host would cause the entire cluster to go down. To resolve this problem, you should reset the configuration to equal node distribution across the hosts as soon as possible.

For example, consider a four-node Serviceguard cluster where Guest 1 and Guest 2 are two nodes running on Host1, and Guest 3 and Guest 4 are two more nodes running on Host2, as show in figure 33.  

**Figure 33.** A four-node Serviceguard cluster configuration before migration
Next, we will migrate Guest 2 to Host2 by completing these steps:

1. `cmhaltnode -d <VM2_Node_Name>`
2. Migrate Guest2 from Host1 to Host2
3. `cmrunnode <VM2_Node_Name>`

**Figure 34.** Serviceguard cluster configuration after migration of Guest 2

### Summary of requirements

- Persistent Reservation is required in all Serviceguard for Linux configurations.
- Serviceguard requires you to use NIC teaming at the host level to achieve network redundancy for heartbeats and applications.
- You must use RDM to attach shared LUNs to virtual machines when using FC as shared storage.
- Use software initiator to expose the shared LUNs when using iSCSI as shared storage.
- NPIV over RDM is mandatory when multiple VMs from a single host must be configured in the same cluster or when vMotion is used in the cluster.

### Summary of recommendations

- Install VMware guest tools on all VMs, and select the Time Synchronization option.
- Enable beacon monitoring for teamed NICs.

### Support information

- Co-existence of VMware HA and HP Serviceguard for Linux is not supported.
- HP Serviceguard running on ESX/ESXi Server versions other than those mentioned in the support matrix are not supported.
- vMotion is supported on HP Serviceguard for Linux clusters with the above-mentioned configuration requirements.

### Summary

This guide describes best practices for deploying HP Serviceguard in a typical VMware ESX/ESXi Server environment. This guide is not intended to duplicate the strategies and best practices of other HP or VMware technical white papers.

The strategies and best practices offered here are presented at a very high level to provide general knowledge. Where appropriate, links are provided for additional documents that offer more detailed information.
References

2. VMware vSphere documentation: vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

Learn more at hp.com/go/sglx