

HP Integrity Virtual Machines A.03.00 Release Notes

HP Part Number: T2767-90076
Published: April 2007, Edition 4.0



© Copyright 2007 Hewlett-Packard Development Company, L.P.

Legal Notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

UNIX is a registered trademark of The Open Group.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Oracle® is a registered trademark of Oracle Corporation.

VERITAS® is a registered trademark of VERITAS Software Corporation in the US and other countries.

Table of Contents

About This Document.....	9
1 Intended Audience.....	9
2 New and Changed Information in This Edition.....	9
3 Typographic Conventions.....	9
4 Document Organization.....	9
5 Related Information.....	10
6 Publishing History.....	10
7 HP Encourages Your Comments.....	10
1 Introduction.....	13
1.1 New Features and Enhancements in This Version of Integrity VM.....	13
1.2 Using Linux Guests.....	14
1.3 Dynamic Memory.....	14
1.4 Creating Virtual Machine Administrator and Operator Accounts.....	14
1.5 Using P2V Workload Migration.....	14
1.6 Integrity VM Command Changes.....	14
1.7 Guest Management Software.....	16
2 Installation Notes.....	17
2.1 Installing Integrity VM.....	17
2.1.1 Integrity VM Includes the Foundation Operating Environment.....	17
2.1.2 Upgrade HP WBEM Services.....	17
2.1.3 Installing the hpvmmigrate Command.....	17
2.1.4 Installing VM Provider.....	17
2.1.5 Upgrade the VM Host to 0609 or Later.....	18
2.1.6 HP-UX Patches Required in the VM Host.....	18
2.1.7 Patches Required in the HP-UX Guest.....	19
2.1.8 Patches Required for Ignite/UX Servers.....	20
2.1.9 Patches Required for Windows Guests.....	20
2.2 Upgrading from Earlier Versions of Integrity VM.....	21
2.3 Installing the HP Integrity Virtual Machines Product Over the Evaluation Software.....	22
2.4 Do Not Install Applications on the VM Host System.....	22
2.5 Do Not Install Integrity VM on a Virtual Partition.....	23
2.6 Do Not Install Windows as Alternate Boot on a VM Host System.....	23
3 Creating Virtual Machines.....	25
3.1 Default Guest Settings for HP-UX, Windows, and Linux.....	25
3.2 Autoboot Causes Virtual Machines to Start.....	25
3.3 Reserving Swap Space for Guests.....	25
3.4 Do Not Create Golden Images of the VM Host for Guest Installation.....	26
4 Installing Guests.....	27
4.1 Windows Guests.....	27
4.1.1 Removing Media During Installation Hangs Guest.....	27
4.1.2 HP Insight Manager Automatic Server Recovery Does Not Work.....	27
4.1.3 Running Windows Guests on a Dual Core Intel Itanium2 Processor (Montecito) System.....	27
4.1.4 Installing Windows with Virtual NullDVD is Not Recommended.....	27
4.1.5 Enabling MP Services on Windows Guest Logs telnetd Errors.....	28

4.1.6	Using Windows Firewall Requires ICMP to Allow Echo.....	28
4.1.7	Poor Console Screen Formatting.....	28
4.1.8	The hpvmstop Command Does Not Shut Down Windows Guests Gracefully.....	28
4.1.9	Do Not Delete EFI Shell Boot Option.....	28
4.2	HP-UX Guests.....	28
4.2.1	HP-UX 11.31 Guests May Fail to Configure More than Two MPT Interfaces.....	29
4.2.2	Patches for HP-UX 11.31 Guests.....	29
4.2.3	Do Not Run Live Kernel Debuggers Inside a Guest.....	29
4.2.4	Do Not Use the iomap(7) Command on HP-UX Guests.....	29
4.2.5	iCAP Commands Fail on HP-UX Guests.....	29
4.3	Linux Guests.....	29
4.3.1	Linux Guest Installation Errors.....	30
4.3.2	Linux Guests with FC Tapes Display Errors.....	30
4.3.3	Disable IPv6 on Linux Guests.....	30
4.3.4	Preparing Linux Guests for VM Manager.....	30
4.3.5	IPv6 Dynamic Address Resolution is Broken in Linux.....	31
4.3.6	Infrequent Ooops: timer ticks before it is due Errors.....	31
4.3.7	Infrequent e1000: eth1: e1000_clean_tx_irq: Detected Tx Unit Hang Errors.....	31
4.3.8	Inconsistent “Bogomips” Values between Virtual CPU0 and Other Virtual CPUs.....	31
4.3.9	Incorrect Display of Special Characters when Displayed Using HP-UX Terminal.....	31
4.3.10	Occasional Floating-Point Assist Fault Messages.....	31
5	Using Integrity VM Commands.....	33
5.1	Using hpvmmodify -N -s Options Together Causes Guest to Be Inaccessible.....	33
5.2	The hpvmmodify Command Reevaluates Guest Configurations.....	33
5.3	The hpvmdevmgmt Command Truncates File Sizes.....	33
5.4	Setting Devices to Sharable Can Lead to Device Conflicts.....	33
5.5	Errors on Displaying Guest or Vswitch Information While that Information is Being Modified...33	33
5.6	Do Not Attempt to Remove Busy Virtual Devices.....	33
5.7	Missing uuid or .vmid Files.....	34
5.8	Maintain Minimum Entitlement.....	34
5.9	Guest Memory Must Be a Multiple of 64 MB.....	34
5.10	Actual Running Entitlement May Differ from Configured Entitlement.....	34
5.11	Duplicate Messages when Modifying Running Guests.....	34
5.12	Manpages Display on Linux Guests.....	34
6	Guest Administration.....	37
6.1	Administrator Account Names.....	37
6.2	Guest User Accounts.....	37
6.3	Creating Virtual Machine Administrator and Operator Accounts.....	37
6.4	Modifying Guests.....	38
6.5	Do Not Add User Accounts to the hpvmsys Group.....	38
6.6	Do Not Enter Ctrl/B after Starting Guest with Virtual Console.....	38
6.7	Restoring the NVRAM for Windows Guests.....	39
6.8	How to Stop Guests.....	39
6.9	The hpvmconsole pc -cycle Command Occasionally Doesn’t Complete.....	39
6.10	How to Recover from a Guest Hang.....	39
6.11	Using HP Serviceguard to Manage Guests.....	39
6.11.1	Required HP Serviceguard Patches.....	40
6.11.2	Reenter Command to Start Packages.....	40
6.11.3	Do not Use Integrity VM Commands to Manage Distributed Guests.....	40
6.11.4	Different Cluster Nodes Report Virtual Machine Status Differently.....	40
6.11.5	Syslog Entries for cmcld Can Be Ignored.....	40

6.11.6 Using Virtual Machines Manager (VM Manager) to Manage Distributed Guests.....	40
6.11.7 Polling Interval for Virtual Machine Serviceguard Nodes.....	40
6.12 Managing Guests using gWLM.....	41
7 Networking Information.....	43
7.1 Vswitches Are Always in SHARED Mode.....	43
7.2 Do Not Use the HP A5506B PCI 10/100Base-TX 4 Port Interface for Virtual Networking.....	43
7.3 MAC Address Validation Can Be Enhanced.....	43
7.4 Auto Port Aggregation (APA) is Supported on the VM Host, Not on the Guest.....	43
7.5 Do Not Run Applications that Set Network Devices into Promiscuous Mode.....	43
7.6 Do not Turn on Checksum Offloading (CKO) on the Physical Network Interface Backing the Vswitch.....	43
7.7 Do Not Turn on TSO on the VM Host and on HP-UX Guests.....	44
7.8 Do Not Configure VLAN Vswitches on HP-UX VLANs.....	44
7.9 For VLANs Between VM Host and Guests, Turn Off CKO.....	44
7.10 Restarting Vswitches.....	44
8 Storage Information.....	47
8.1 DMP Files Not Supported as Backing Stores	47
8.2 Using Database Management Products on Virtual Machines.....	47
8.3 Integrity VM Does Not Honor File Permissions on Backing Stores.....	47
8.4 Using USB CD/DVD Devices.....	47
8.5 The hpvmmodify Command Fails to Change a DVD.....	47
8.6 Virtual FileDVD Reverts to Original Resource Statement.....	47
8.7 Physical Device null Assigned to Nonexistent Path.....	47
8.8 Using sam on Guest Cannot Initialize Disk.....	48
8.9 Extending a Logical Volume Backing Store Corrupts the Guest.....	48
8.10 Management Limitations of Virtual SCSI Devices.....	48
8.11 Installing Integrity VM Clears SecurePath 3.0F SP1 Settings.....	48
9 Migrating Virtual Machines.....	49
9.1 Do Not Migrate Distributed Guests.....	49
9.2 Collect CapAd Data before Migrating.....	49
10 Error Logging.....	51
10.1 Guest Log Can Grow Unbounded.....	51
10.2 Log Messages Written to Old Log File.....	51
10.3 Saved MCA or INIT Register State Can Be Inaccurate.....	51
10.4 Modifying the Size of the Monitor Log File.....	51
10.5 Virtual Console Event Logs Different from Physical Machine Logs.....	51

List of Tables

1-1	Option Keywords for Virtual Machine MAC Address and Serial Number.....	15
1-2	Guest Management Software Kit Locations.....	16
2-1	VM Host Patches.....	18
2-2	HP-UX Guest Patches.....	19
2-3	Do Not Install Products or Patches on HP-UX Guests.....	20
2-4	Ignite/UX Patches.....	20
2-5	Windows Patches.....	20
2-6	Do Not Install Products or Patches on Windows Guests.....	21
3-1	Guest Default Settings.....	25

About This Document

The *HP Integrity Virtual Machines Release Notes* document describes the latest enhancements and changes to the HP Integrity Virtual Machines product (Integrity VM), including limitations and guidelines for using the Integrity VM software. Always read the release notes before installing and using the product. For the most current information, obtain the latest version of this document from docs.hp.com.

1 Intended Audience

This document is intended for system and network administrators responsible for installing, configuring, and managing Integrity VM. Administrators are expected to have an in-depth knowledge of HP-UX operating system concepts, commands, and configuration. In addition, administrators must be familiar with the HP Integrity machine console and how to install the operating systems and applications running on their virtual machines.

2 New and Changed Information in This Edition

This document supersedes the HP Integrity Virtual Machines Release Notes for Integrity VM A.20.00.

3 Typographic Conventions

<i>find</i> (1)	HP-UX manpage. In this example, “find” is the manpage name and “1” is the manpage section.
<i>Book Title</i>	Title of a book or other document.
Linked Title	Title that is a hyperlink to a book or other document.
http://www.hp.com	A Web site address that is a hyperlink to the site.
Command	Command name or qualified command phrase.
user input	Commands and other text that you type.
computer output	Text displayed by the computer.
Enter	The name of a keyboard key. Note that Return and Enter both refer to the same key. A sequence such as Ctrl+A indicates that you must hold down the key labeled Ctrl while pressing the A key.
term	Defined use of an important word or phrase.
variable	The name of an environment variable, for example <code>PATH</code> or <code>errno</code> .
value	A value that you may replace in a command or function, or information in a display that represents several possible values.
<element>	An element used in a markup language.
attrib=	An attribute used in a markup language.

4 Document Organization

This document contains information that supplements the information in the *Integrity Virtual Machines Installation, Configuration, and Administration* and includes the following chapters:

- “Introduction” (page 13) describes some of the enhancements and quality improvements in the current release of the HP Integrity Virtual Machines product.
- “Installation Notes” (page 17) contains information about installing and upgrading Integrity VM and associated products.
- “Creating Virtual Machines” (page 25) contains information about creating virtual machines.

- “Installing Guests” (page 27) contains information about installing guest operating system and management software.
- “Using Integrity VM Commands” (page 33) contains information about using Integrity VM commands.
- “Guest Administration” (page 37) contains information about guest system administration.
- “Networking Information” (page 43) contains information about virtual networking resources.
- “Storage Information” (page 47) contains information about virtual data storage for guests.
- “Migrating Virtual Machines” (page 49) contains information about migrating virtual machines from one system to another.
- “Error Logging” (page 51) contains information about the message logging provided by Integrity VM.

5 Related Information

The following documents, which are found at the HP Technical Documentation Web site at <http://docs.hp.com/>, may be useful to the reader of this document:

- *Integrity Virtual Machines Installation, Configuration, and Administration*
- *Ignite-UX Reference*
- *HP-UX Installation and Update Guide*
- *HP-UX Reference*
- *Managing Serviceguard*
- *Windows on Integrity: Smart Setup Guide*

6 Publishing History

Publication Number	Supported VM Host Operating System	Supported Integrity VM Version	Edition Number	Publication Date
T2767 - 90005	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.01.00	1.0	October 2005
T2767-90010	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.01.20	2.0	February 2006
T2767 - 90010	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.01.20	2.2	February 2006
T2767-90014	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.01.20	2.3	April 2006
T2767-90043	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.01.20	2.4	June 2006
T2767-90033	HP-UX 11i V2 May 2005 and later	HP Integrity Virtual Machines A.02.00	3.0	October 2006
T2767-90076	HP-UX 11i V2 September 2006 and later	HP Integrity Virtual Machines A.03.00	4.0	April 2007

7 HP Encourages Your Comments

HP encourages your comments concerning this document. We are truly committed to providing documentation that meets your needs.

Please submit comments to:

<http://docs.hp.com/assistance/feedback.html>

Please include the document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document.

1 Introduction

Thank you for installing HP Integrity Virtual Machines (also called Integrity VM). This *Release Notes* document describes the changes in this version of the Integrity VM product.

HP Integrity Virtual Machines A.03.00 is installed on HP Integrity servers or nPartitions running HP-UX 11i V2 (September 2006 [0609] or later). For complete information about the requirements for installing Integrity VM, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

This chapter contains the following sections:

- “New Features and Enhancements in This Version of Integrity VM” (page 13)
- “Using Linux Guests” (page 14)
- “Dynamic Memory” (page 14)
- “Creating Virtual Machine Administrator and Operator Accounts” (page 14)
- “Using P2V Workload Migration” (page 14)
- “Integrity VM Command Changes” (page 14)
- “Guest Management Software” (page 16)

1.1 New Features and Enhancements in This Version of Integrity VM

This section describes how the current version of Integrity VM has been enhanced over previous versions. For more information about these enhancements, refer to the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

- Guests can run any of the following operating systems:
 - HP-UX 11.23 (May 2005 [0505] or later)
 - HP-UX 11.31
 - Windows 2003 (Enterprise or Datacenter edition)
 - RedHat Linux Enterprise Edition Advanced Server Release 4 update 4.
- Administrators can dynamically change the size of memory allocated to the HP-UX guest. This feature includes:
 - Changes to the `hpvmcreate`, `hpvmmodify`, and `hpvmclone` commands to configure the guest.
 - Changes to the `hpvmstatus` command to view dynamic memory data for a configured guest.
 - A new guest-only utility (`hpvmgmt`) to view guest dynamic memory data.
- Networking enhancements include:
 - Administrators can change the physical network interface card (pNIC) for a vswitch using the `-C` option to the `hpvmnet` command.
 - Administrators can clone the selected vswitch to a newly named vswitch using the `-N` option to the `hpvmnet` command. The cloned vswitch will have the same VLAN port information configuration data as the parent vswitch.
- Multiple virtual machine administrator and operator accounts can be created to manage virtual machines remotely.
- Workloads can be migrated from a physical Integrity system or nPar to a virtual machine using the P2V (physical to virtual) assistant.
- Attached I/O (tape, changer, CD/DVD burner) can be used as backing storage by all types of guests.

1.2 Using Linux Guests

This version of Integrity VM introduces support for Linux guests. You can install the RedHat Linux Enterprise Edition Advanced Server Release 4 update 4 on a virtual machine.

For information about this Linux operating system, see www.redhat.com. Specifically:

- *Red Hat Enterprise Linux 4 Installation Guide for x86, Itanium, AMD64*
- *Intel Extended Memory 64 Technology (Intel EM64T)*
- *Red Hat Linux Customization Guide*

The guest parameter settings for Linux guests are listed in Table 3-1 (page 25).

For information about installing Linux guests, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

1.3 Dynamic Memory

With this version of Integrity VM, system administrators can set memory parameters that allow guest memory allocation to be changed dynamically; that is, without rebooting the guest.

Normally, guests use a fixed amount of memory. That memory is allocated when the virtual machine is started and locked down so it cannot be paged or swapped. Once the memory is locked down, the VM Host cannot make it available to other virtual machines. The VM Host supports a fixed number of running virtual machines based on the amount of memory in the VM Host system and the number and size of the virtual machines.

Dynamic memory allows you to change the amount of physical memory in use by a virtual machine without rebooting the virtual machine. In this release of Integrity VM, the dynamic memory feature is available on HP-UX guests only. In order to use dynamic memory, the guest must have the guest management software installed.

For example, this feature allows a guest that is a Serviceguard node to be used as a standby server for multiple Serviceguard packages. When a package fails over to the guest, the guest memory can be changed to suit the requirements of the package before, during, and after the failover process.

For information about enabling and using dynamic memory, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

1.4 Creating Virtual Machine Administrator and Operator Accounts

In versions of Integrity VM prior to A.03.00, only Admin console access is available, and only one such account per guest is allowed. The administrator account name must match the guest name. The new version of Integrity VM provides proper access controls and individual accountability for these accounts. For more information, see Section 6.3 (page 37).

1.5 Using P2V Workload Migration

The P2V assistant allows you to migrate an application from a discrete physical system or nPar to a virtual machine. The P2V assistant consists of a set of scripts and tools that aid in this migration. For more information, see *p2vassist(1M)*.

1.6 Integrity VM Command Changes

The Integrity VM commands have changed in the following ways:

- The *hpvmresources* manpage, which describes the syntax for specifying storage and network devices when creating or modifying a guest, has been moved from the (1M) volume to the (5) volume.
- The new *p2vassist(1M)* manpage describes how to use the physical-to-virtual assistant toolkit to migrate a workload from a discrete system (server or partition) to a virtual machine.

- To support various types of guest operating systems, the `-O` option to the `hpvmcreate`, `hpvmclone`, and `hpvmmodify` commands accepts the following keywords:
 - HPUX
 - WINDOWS
 - LINUX

The keyword is not case-sensitive.

- Some Integrity VM commands now use the new `-x` option, which accepts name and value pairs (for example, `name=value`) to set guest configuration options. The commands that use the new `-x` option are:
 - `hpvmcreate` (runs on VM Host)
 - `hpvmclone` (runs on VM Host)
 - `hpvmmodify` (runs on VM Host)
 - `hpvmmgmt` (runs on guest)
- The `hpvmcreate`, `hpvmclone`, and `hpvmmodify` commands allow you specify the virtual machine MAC address and serial number. To specify this information, include the `-x` option with the following keywords:

Table 1-1 Option Keywords for Virtual Machine MAC Address and Serial Number

<code>-x mac_address={new same}</code>	Specifies the MAC address of the virtual machine.
<code>-x serial_number={new same}</code>	Specifies the serial number of the virtual machine.

- The new `hpvmmgmt` command is used on the Integrity VM guest to view and change dynamic memory settings.
- The `hpvmstatus` command has been enhanced to show information about dynamic memory settings. The dynamic memory output is only displayed if the guest is configured to use dynamic memory. When configured as such, if the guest is not running or is running without having a dynamic memory driver installed on the guest, then only configuration values are displayed. Otherwise, on a running guest with dynamic memory configured and the dynamic memory driver installed, the `hpvmstatus` command displays actual values.
- The `hpvmclone` command allows you to use the `-b` option to specify the boot disk for the new virtual machine.

The following example shows how to use the `hpvmclone` command to create a new Linux guest named `linux2` based on the existing guest named `linux1`. The boot disk for the guest named `linux2` is specified.

```
# hpvmclone -P linux1 -N linux2 -b disk:scsi:0,0,0:disk:
```

- The `hpvmcollect` command allows you to use the `-g` option to clean up a guest debug memory dump directory after a memory dump has been collected in the `hpvmcollect` archive.
- The `hpvmstop` command allows you stop all the running guests at the same time with the new `-a` option.
- The `hpvmnet` command allows you to change the virtual switch characteristics (using the `-C` option) and to clone the virtual switch (using the `-N` option).
- The `-Q` option has been added to `hpvmstart`, `hpvmstop`, and `hpvmremove` commands. The `-Q` option suppresses the confirmation dialog. The command function is performed without requiring user input.
- The `hpvmmigrate` command is enhanced to accept options to specify guest characteristics, as with the `hpvmcreate`, `hpvmclone`, and `hpvmmodify` commands. Specifically, the following options have been added to the `hpvmmigrate` command synopsis:

- `-N new_vm_name` specifies the new name for the virtual machine being migrated.
- `-l vm_label` specifies a descriptive label for the virtual machine.
- `-e percent` specifies the percentage of CPU resources to which the guest's virtual CPUs are entitled.
- `-E cycles` specifies the virtual machine's CPU entitlement in CPU cycles.
- `-m resource` modifies the existing I/O resource for the virtual machine.
- `-C` physically copies the storage device specified with the `-m` option to the target host during the migration process.

For more information, refer to `hpvmigrate(1M)`.

- Commands that prompt for confirmation display the confirmation prompt in a consistent manner. The `hpvmstart`, `hpvmcreate`, `hpvmclone`, `hpvmmodify`, and `hpvmnet` commands present the same prompt with the same default. For example, the `hpvmstop` command displays the following confirmation prompt:

```
# hpvmstop -P guest1
hpvmstop: Stop the virtual machine 'guest1'? [n/y]:<Enter>
hpvmstop: Virtual machine was not stopped.
```

The default action is to not perform the action.

1.7 Guest Management Software

Integrity VM provides specific software for each type of guest operating system. This guest management software enhances guest performance, enables Integrity VM commands, and includes providers for virtual management software, such as VM Manager. The locations and contents of the guest management kits are modified in this version of Integrity VM. The guest management software is required on each guest.

Guest management software is installed on the guest either remotely, from a software depot, or locally, after being copied to the guest. The guest management software is located in the `/opt/hpvm/guest-images` directory. Table 1-2 lists the location of the guest management software kit for each type of guest operating system. The instructions for installing the guest management software are provided in `README.txt` files in these directories.

Table 1-2 Guest Management Software Kit Locations

Guest Operating System	Guest Management Software Location
HP-UX 11i v2	<code>/opt/hpvm/guest-images/hpux/11iv2</code>
HP-UX 11i v3	<code>/opt/hpvm/guest-images/hpux/11iv3</code>
Linux	<code>/opt/hpvm/guest-images/linux</code>
Windows	<code>/opt/hpvm/guest-images/windows</code>

Installing the guest management software kit causes the guest to reboot.

Whenever you upgrade Integrity VM, reinstall the guest kit on all the guests. This ensures that guests run well and continue to be manageable and supportable. Failure to install and upgrade the guest management software on each guest can cause problems that are difficult to diagnose and solve.

2 Installation Notes

This chapter contains notes about installing and upgrading Integrity VM and associated software on the VM Host system.

2.1 Installing Integrity VM

This section describes information about installing the HP Integrity Virtual Machines product and associated software on the VM Host system.

HP Integrity Virtual Machines A.03.00 is installed on HP Integrity servers or nPartitions running HP-UX 11i V2 (September 2006 [0609] or later). For complete information about the requirements for installing Integrity VM, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

When you upgrade or reinstall Integrity VM, guests are stopped, but they are not removed. When the new version of Integrity VM starts, the virtual machines may also start, depending on the setting of the guest boot attribute.

2.1.1 Integrity VM Includes the Foundation Operating Environment

The HP-UX Foundation Operating Environment (FOE) is included with Integrity VM. Install the FOE on the VM Host on which you install Integrity VM. The license for the FOE (used in the VM Host only) is included with the purchase of Integrity VM. (Licenses for OEs that run inside the individual virtual machines must be purchased separately.)

For VM Hosts that will support guests as Serviceguard packages, the Mission Critical Operating Environment (MCOE) can also be used.

2.1.2 Upgrade HP WBEM Services

Integrity VM fails to install if the version of WBEM Services on your VM Host is old. The VM Host system must be running HP WBEM Services A.02.00.10 or later. The HP WBEM Services for HP-UX software bundle (B8465BA) is available as part of the HP-UX operating system, or download the software from www.hp.com. This version of HP WBEM Services is also required in order to install VM Provider and VM Manager.

2.1.3 Installing the hpvmmigrate Command

The `hpvmmigrate` command is included in the HP Integrity Virtual Machines product, but it is packaged in the separate VMMigrate bundle and must be explicitly specified. You must install the T2767AC bundle before or with the VMMigrate bundle, to make sure the versions of the bundles are compatible.

To install the VM Migrate bundle with the Integrity VM software, enter the following command:

```
# swinstall -x autoreboot=true -s my.server.foo.com:/depot/path T2767AC VMMigrate
```

2.1.4 Installing VM Provider

To install the VM Provider bundle with the Integrity VM software on the VM Host, enter the following command:

```
# swinstall -x autoreboot=true -s my.server.foo.com:/depot/path T2767AC VMProvider
```

To install the VM Provider bundle with the Integrity VM software on the HP-UX guest, enter the following command:

```
# swinstall -x autoreboot=true -s my.server.foo.com:/depot/path VMProvider
```

If you install the VM Provider on either the VM Host or a guest, make sure that the system is using HP WBEM Services A.02.00.10 or higher. For example:

```

# swlist WBEMServices
# Initializing...
# Contacting target "alien2"...
#
# Target:  alien2:/
#

# WBEMServices                A.02.00.11      WBEM Services CORE
Product
  WBEMServices.WBEM-CORE      A.02.00.11      WBEM Services CORE
Fileset for hp Integrity servers
  WBEMServices.WBEM-CORE-COM  A.02.00.11      WBEM Services COM
Fileset for hp Integrity servers and hp 9000 servers
  WBEMServices.WBEM-MAN      A.02.00.11      WBEM Services MAN
Fileset
  WBEMServices.WBEM-MX      A.02.00.11      WBEM Services MX
fileset

```

2.1.5 Upgrade the VM Host to 0609 or Later

This version of Integrity VM does not run on HP-UX 11.23 versions released before September 2006 (0609). If the VM Host system is running an older versions of HP-UX 11.23, you must upgrade to 0609 or later before you upgrade to the current version of Integrity VM.

2.1.6 HP-UX Patches Required in the VM Host

Table 2-1 lists the patches that are required in the VM Host system running Integrity VM A.03.00 and later. For patches required for earlier versions of Integrity VM, consult the *Release Notes* document for that version.

Table 2-1 VM Host Patches

Affected HP-UX (VM Host) Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11.23 0512 or later	A.02.00 or later	PHNE_33724	Bug Fix	Fixes a problem of a panic on the VM Host.
11.23 0505 or later	A.02.00 or later	PHNE_34474	Bug Fix	Required when using linkloop over VLANs between guest and VM Host VLAN.
11.23 0505	A.01.00 or later	Cimserver 02.00.011 PHSS_34429	Bug Fix	Resolves potential corruption of guest configuration, cimserver, or other WBEM files when under extreme load. Download HP WBEM Services for HP-UX Product Bundle B8465BA from the HP software depot.
11.23 0505 or later	A.01.00 or later	PHNE_34278	Bug Fix	Resolves panic and system hang symptoms

Table 2-1 VM Host Patches (continued)

Affected HP-UX (VM Host) Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11.23 0505 or later	A.01.00 or later	PHNE_35182	Bug Fix	Cumulative ARPA transport patch, resolves panic. Requires prerequisite PHNE_33732
11.23 Montecito	A.01.20	HPVM A.02.00 11.23.0609 HWE	Montecito HW support	HPVM V2.0 is strongly recommended for use with Montecito-based systems.

2.1.7 Patches Required in the HP-UX Guest

Table 2-2 lists the patches that are required in HP-UX guests:

Table 2-2 HP-UX Guest Patches

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
HP-UX 11.23 0505	A.01.00 or later	U320 SCSI MPT driver version B.11.23.03, bundle A7173A	Includes fixes for performance and stability.	MPT driver update. This patch is included in the 0512 update.
HP-UX 11.23 0505 or later	A.01.00 or later	PHKL_34278	Bug fix	Resolves panic and system hang symptoms.
HP-UX 11.23 0505 or later	A.01.00 or later	PHKL_34589	Bug fix	Resolves panic on guest.
11.23 0606 or later	A.01.20 or later	PHKL_34540 PHKL_34336 PHKL_34928	Fix to allow sharing of idle CPU cycles between guests.	Ensure loaded when using 0606 and later. Must be manually installed if feature 11i is not installed. Without this patch, Integrity VM may not detect guest is idle and not share resources, heavily impacting performance.
11.23 0505 or later	A.01.00 or later	PHKL_33823	Bug Fix	Resolves panic on guest.
11.23 0505 or later	A.02.00 or later	PHSS_34760	Serviceguard Monitor fix	Required for running in Serviceguard 11.16 environment.
11.23 0505 or later	A.02.00 or later	PHSS_34337	Serviceguard Monitor fix	Required for running in Serviceguard 11.17 environment.
11.23 0505 or later	A.01.00 or later	Cimserver 02.00.09 (PHSS_34429)	Bug fix	Resolves potential corruption of guest configuration, cimserver, or other WBEM Services files when under extreme load.

11.23 0505 or later	A.01.00 or later	PHNE_35182	Bug fix	Cumulative ARPA transport patch, resolves panic. Requires prerequisite PHNE_33732
11.23 Montecito	A.01.20 or later	HPVM A.02.00 11.23.0609 HWE	Montecito hardware support	Integrity VM V2.0 or later is strongly recommended for use with Montecito-based systems.

For more information about updates to HP-UX software, contact your HP representative or support specialist.

Table 2-3 lists patches and products that you should not install on HP-UX guests. In guests where these patches are installed, degradations and regressions have been observed.

Table 2-3 Do Not Install Products or Patches on HP-UX Guests

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
HP-UX 11.23 0505 or later	A.01.00A.01.20	PHKL_33361	Cumulative kernel SCSI patch	Resolved in Integrity VM A.02.00 and later.
HP-UX 11.23 0505 or later	A.01.00A.01.20A.02.00	PHKL_35739	VxVM 4.1 Kernel Patch 04	Resolved in Integrity VM A.03.00 and later.

2.1.8 Patches Required for Ignite/UX Servers

Table 2-4 lists the patches that are required in the guests:

Table 2-4 Ignite/UX Patches

Affected OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
HP-UX 11.00	A.01.00 or later	PHKL_25355	tftpd	
HP-UX 11.11	A.01.00 or later	PHKL_32825	tftpd	

2.1.9 Patches Required for Windows Guests

Table 2-5 lists the patches that are required in the guests.

Table 2-5 Windows Patches

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
Windows Server 2003	A.02.00 or later	SSM 4.6	Bug Fix`	Microsoft patches correct a compiler issue that can affect Windows guests in various ways.

Table 2-6 lists patches and products that you should not install on Windows guests.

Table 2-6 Do Not Install Products or Patches on Windows Guests

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
SSM 4.5 SSM 4.6 Montecito	A.02.00 or later	PalHaltLightRegEdit component	Idle detection	See Section 4.1.3: "Running Windows Guests on a Dual Core Intel Itanium2 Processor (Montecito) System" (page 27)

2.2 Upgrading from Earlier Versions of Integrity VM

If the HP Integrity Virtual Machines software is already installed, you can install the new version on the VM Host system without removing the existing software. Guests and guest applications are shut down but they are not otherwise affected when you upgrade Integrity VM. This procedure reboots the VM Host system.

- If you have previously installed the Integrity VM product:
 1. Back up the `/var/opt/hpvm` directory to retain existing Integrity VM configuration files. When you install Integrity VM, the guest and virtual switch configuration files are modified in a way that makes them incompatible with the previous version. This step allows you to drop back to a previous version of Integrity VM, if desired.
 2. Log in to each guest on the VM Host and shut down its operating system. The installation procedure will stop any running guests, but it is preferable to shut them down manually before you start the installation procedure.
 3. Identify the media from which you are installing the software.
 - If you have installation media, mount it.
 - If you are installing from the network, identify the system and path name corresponding to the HP-UX software depot that contains the Integrity VM software. (For example, `my.server.example.com:/depot/path`.)
- Use the `swinstall` command to install the software.
 - If you are using the command line interface, specify the path to the software depot. For example, the following command installs only the Integrity VM software:


```
# swinstall -x autoreboot=true -s my.server.example.com:/depot/path T2767AC
```
 - If you are using the installation graphical interface (GUI), perform the following steps:
 1. Enter the following command:


```
# swinstall
```
 2. Select the T2767AC bundle from the list presented by the GUI.

This command installs the latest version of Integrity VM from the software depot.
- If the `VMMigrate` and `VMProvider` bundles are to be installed or upgraded, specify them when you install the new version of Integrity VM, or install them separately.

For example, if `VMProvider` is in the list, you can include it in the command to install the current version of Integrity VM:

```
# swinstall -x autoreboot=true -s my.server.foo.com:/depot/path T2767AC VMProvider
```

Installation of the current version of Integrity VM fails on systems that have older versions of the `VMProvider` bundle. The `swinstall` session fails and logs messages to `/etc/rc.log` indicating that a new version of `VMProvider` must be installed before or at the same time as Integrity VM. The `VMProvider` bundle is available on the Integrity VM installation media. If you do not wish to install the new version of the `VMProvider`, you must remove the `VM Provider` before you install the current version of Integrity VM.

To see which bundles are installed, enter the following command:

```
# swlist | grep -i "integrity vm"
```

T2767AC	A.03.00.00	Integrity VM
VMGuestLib	A.03.00.00.76	Integrity VM Guest Support Libraries
VMKernelSW	A.02.00.00	Integrity VM Kernel Software
VMMigrate	A.03.00.00	Integrity VM Migration Bundle
VMProvider	A.03.00.00.76	WBEM Provider for Integrity VM

The VMGuestLib guest support libraries and the VMKernelSW kernel software are included with the HP-UX operating system installation.

- Reinstall the guest management software on each existing guest, as described in the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

2.3 Installing the HP Integrity Virtual Machines Product Over the Evaluation Software

If you installed the evaluation version of Integrity VM, you must remove the evaluation software before you install the current version of the product. For example, to remove the evaluation version of Integrity VM, enter the following commands:

```
# swremove -x autoreboot=true T2801AA VMProvider VMMigrate
# rm -rf /opt/hpvm
# rm -rf /opt/hpvmprovider
```

Do not remove the directory `/var/opt/hpvm`. This directory contains all the virtual machine configurations that were created with the evaluation software.

2.4 Do Not Install Applications on the VM Host System

When you install Integrity VM, HP-UX kernel parameters are changed to accommodate the virtual machine environment. This makes the system unsuitable for running any other applications. Regardless of whether guests are configured and running, the VM Host system is not configured to allow applications to share system resources. You can run system management utilities and Serviceguard, as documented in the *HP Integrity VM Installation, Configuration, and Administration* manual.

- **Using HP Storage Data Protector for guest backup**

You can use Data Protector to back up the guest OS image. Install the Data Protector agent on the VM Host, not on the guests. For more information, refer to the *HP-UX 11i V2 Installation and Upgrade Guide*.

- **Using HP GlancePlus/iX to monitor guests**

You can use Glance on the VM Host to monitor guest data, but recorded measurements can be misleading. Glance receives the CPU accounting information from the guest kernel. Because the VM Host can take the processor away (for example, when a hardware interrupt occurs), the time spent running other guests is reported for the state that the guest was in at the time the CPU was taken away. For more information about using Glance, refer to *glance(1M)*.

- **Using HP Integrity Essentials Global Workload Manager (gWLM)**

If you use gWLM within VSE to manage virtual machines, when you upgrade the VM Host, make sure the gWLM agent on that host is running gWLM A.02.50 or greater. Also, the managing VSE Central Management Station (CMS) must be running A.02.50 or greater, as described in the *VSE Management Software Installation and Update Guide*. To upgrade the VM Host, use the following procedure:

1. Remove the gWLM agent using the following command:

```
# swremove gWLM-Agent
```

2. Upgrade Integrity VM as described in “Upgrading from Earlier Versions of Integrity VM” (page 21).
3. Upgrade the gWLM agent, as described in the *VSE Management Software Installation and Update Guide*.

If you install the current version of Integrity VM without upgrading to gWLM A.02.50 or later, and then attempt to use gWLM within VSE to manage virtual machines, the following error is reported:

```
Error acquiring workload management lock. Look in the the file  
/var/opt/gwlm/gwlmagent.log.0 on hostname for more details.
```

- **Using the HP Integrity Virtual Machines Manager (VM Manager)**

The HP VM Manager product provides a graphical user interface (GUI) for Integrity VM. It is available from either of the following management interfaces:

- HP System Management Homepage (SMH).
For more information about using VM Manager under SMH, see the *Getting Started with VM Manager* guide.

- HP Virtual Server Environment (VSE) Management Software environment in the HP Systems Insight Manager (SIM) on the Central Management Server (CMS).

For more information about VSE, see the *VSE Management Software Quick Start Guide*

If you have installed the HP VM Manager software, you must upgrade it to a version that supports this version of Integrity VM.

To use VM Manager, you must install the VMProvider bundle that is provided with Integrity VM. If you upgrade Integrity VM, be sure to keep the VMProvider up to date also. If the VMProvider version does not match the Integrity VM version, the VM Manager will not work properly.

For Windows guests, you must also install the UtilProvider software (provided with the HP Integrity Support Pack for Windows). Follow the instructions for installing Windows guests in the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

- **Using HP Instant Capacity with Integrity VM**

You can use HP Instant Capacity solutions on the VM Host system as you would on any other HP-UX system.

2.5 Do Not Install Integrity VM on a Virtual Partition

HP does not support running Integrity VM in a vPar. If you override the Integrity VM installation warnings and force this installation, you receive errors during the start of Integrity VM.

2.6 Do Not Install Windows as Alternate Boot on a VM Host System

Guest boot disks may become unbootable if the VM Host is restarted as a Windows system.

3 Creating Virtual Machines

This section contains notes about creating and configuring virtual machines on the VM Host system.

3.1 Default Guest Settings for HP-UX, Windows, and Linux

Table 3-1 lists the default guest settings for HP-UX, Windows, Linux, and Unknown guests. An Unknown guest is a virtual machine that has not booted with any operating system. When an Unknown guest type boots, the appropriate operating system type is applied to the guest configuration.

The following guest OS specific settings are applied if you specify the operating system type with the `-o` option to the `hpvmcreate` command.

Table 3-1 Guest Default Settings

	HP-UX Guest Default Settings	Windows Guest Default Settings	Linux Guest Default Settings	Unknown Guest Operating System Default Settings
Maximum CPUs	4	4	4	4
Default CPUs	1	1	1	1
Default memory	2 GB	2 GB	2 GB	2 GB
Minimum memory	512 MB	32 MB	512 MB	32 MB
Maximum memory	64 GB	64 GB	64 GB	128 GB
Default reserved memory	64 MB	64 MB	64 MB	64 MB
Minimum reserved memory	32 MB	64 MB	32 MB	32 MB
Maximum reserved memory	64 GB	64 GB	64GB	128 GB



NOTE: The amount of memory you should allocate to the guest must be sufficient to allow the guest operating system to boot. This amount may differ from the defaults documented here. Refer to the product documentation for the operating system and applications on the guest for specific memory requirements.

3.2 Autoboot Causes Virtual Machines to Start

The virtual machine `start_attr` attribute can be set to `auto` or `manual` using the `-b` option to the `hpvmcreate`, `hpvmmodify`, and `hpvmclone` commands. When this attribute is set to `auto`, the virtual machine starts whenever Integrity VM starts running. This also occurs after you install or upgrade Integrity VM.

3.3 Reserving Swap Space for Guests

Integrity VM installation requirements includes swap space for guests. Swap space on the VM Host must be configured as device swap (not file system swap). The amount of swap space must be no less than the total size of physical memory plus 4 Gb.

The VM Host uses this space to start up guests, but guests are never swapped out. (A guest's physical memory is locked down.) By turning off the `swapmemon` feature on the VM Host, Integrity VM conserves RAM for guest use.

3.4 Do Not Create Golden Images of the VM Host for Guest Installation

Do not use the VM Host to create golden images to be used for guest OS installations using Ignite-UX.

An Integrity system may be used to create a golden image suitable for OS installation on a virtual machine, provided it has all of the VM Host software completely removed. To do so, remove both the Integrity VM bundle (T2767AC) and the VMKernelSW bundle:

```
# swremove -x autoreboot=true T2767AC VMKernelSW
```

Before using the system to create a golden image, verify that neither of these bundles are installed. That is, errors should result when querying the system with `swlist`:

```
# swlist T2767AC VMKernelSW
# Initializing...
# Contacting target "foo"...
ERROR:   Software "T2767AC" was not found on host "foo:".
ERROR:   Software "VMKernelSW" was not found on host "foo:".
```

For more information about using Ignite-UX golden images, refer to the *Ignite-UX Administration Guide*.

4 Installing Guests

This section describes notes pertaining to installing guest software on the virtual machines. The following sections are included:

- “Windows Guests” (page 27)
- “HP-UX Guests” (page 28)
- “Linux Guests” (page 29)

4.1 Windows Guests

This section lists the release notes specific to installing Windows guests.

4.1.1 Removing Media During Installation Hangs Guest

If you begin the installation of the Windows operating system and then eject the media from the virtual console, the guest hangs. To recover from the problem, restart the guest from the virtual console.

4.1.2 HP Insight Manager Automatic Server Recovery Does Not Work

On Windows guests, the HP Insight Manager product supports Automatic Server Recovery: if a system does not send out a heartbeat within a specified interval, a user-specified action takes place (for example, automatic reboot). Integrity VM takes no action if a heartbeat is not detected; instead, a message is logged on the console and the VM Host System Event Log. You should monitor these log files and manually perform the reboot if the guest does not respond.

4.1.3 Running Windows Guests on a Dual Core Intel Itanium2 Processor (Montecito) System

If you use a version of the OPK Smart Setup Media released prior to Version 5.0, and wish to run a Windows guest on a Montecito server, you must disable the PalHaltLightRegEdit patch. To do this, go to **Add/Remove Programs** and remove the PalHaltLightRegEdit component.

4.1.4 Installing Windows with Virtual NullDVD is Not Recommended

To use a Virtual NullDVD as installation media, define the device as a file or as the physical drive. For example, use one of the following commands:

```
# hpvmmodify -P guest-name -a dvd:scsi::file:/InstallMedia/Windows.iso
```

```
# hpvmmodify -P guest-name -a dvd:scsi::disk:/dev/rdisk/c0t0d0
```

Insert and remove media (for software installation using multiple CDs) using the `hpvmmodify` command (effectively ejecting and inserting files) or, in the case of a physical drive, actually eject and insert the media in the drive. For example, to change the media in an existing virtual DVD defined in the above example, enter the following command:

```
# hpvmmodify -m dvd:scsi:0,0,1:file:/InstallMedia/SmartSetup.iso
```

Where the path name `/InstallMedia/SmartSetup.iso` indicates the new media to use.

Defining the virtual DVD as a null type (for example: `hpvmmodify -a dvd:scsi:null:/path/to/media/`) is not recommended for software installation.

Software installation from virtual DVDs defined with the null storage type (also referred to as *removable media* functionality) often results in installation failures because the removable media is automatically ejected when the virtual machine is stopped and started during software installation.

To complete Windows installation from removable media, follow these steps:

- After the automatic reboot, Windows controls the console. When you see the SAC> prompt, use **Esc-Tab** to change the channel to the product key prompt.
- Stop and start the virtual machine and interrupt the automatic boot sequence.
- Before the system is allowed to continue, from the virtual console, execute the necessary insert (IN) command to reload the media.
- After the media is reloaded into the virtual DVD, select the Windows Media install (the first boot option) and allow the system to boot.
- When prompted, enter the product key. The installation process proceeds normally from this point.

For more information about using removable media, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

4.1.5 Enabling MP Services on Windows Guest Logs telnetd Errors

If you enable MP Services on a guest, the following telnetd errors might be written to the VM Host's log file (/var/adm/syslog/syslog.log). You can safely ignore these messages:

```
Jun 13 11:41:41 AGTVM telnetd[21551]: getmsg error:no data
Jun 14 20:38:00 AGTVM telnetd[29216]: getmsg error:no data
Jun 14 21:52:07 AGTVM telnetd[29504]: getmsg error:no data
```

To prevent this problem, disable MP Services.

4.1.6 Using Windows Firewall Requires ICMP to Allow Echo

When the Microsoft firewall is on, ICMP must be enabled so that you can ping the guest (echo). This setting can be found in the network properties applet, as follows: Control Panel => Network Connections => Local Area Connection/Properties Advanced => Windows Firewall => Settings ICMP. Check the **Allow Incoming Echo Requests** box.

4.1.7 Poor Console Screen Formatting

The Windows guest console may not format the virtual console display properly. Manage the guest using the Remote Desktop or make a network connection to the Windows guest.

4.1.8 The hpvmstop Command Does Not Shut Down Windows Guests Gracefully

Do not use the following commands to shut down Windows guests:

```
# hpvmstop -P winguest
# hpvmconsole -P winguest -c "pc -off"
```

These commands do not stop the Windows operating system gracefully. To shut down a Windows guest, use the standard Windows operating system commands.

4.1.9 Do Not Delete EFI Shell Boot Option

Do not delete the EFI Shell [Built-in] EFI Boot Manager option. Deleting this option may interfere with the subsequent installation of the guest operating system. To recover if there are no options present on the EFI Boot Manager menu screen:

1. Enter the Boot option maintenance menu.
2. Select Add a Boot Option.
3. Select Load File [EFI Shell [Built-in]].
4. Save the setting to NVRAM.

4.2 HP-UX Guests

This section lists release notes specific to installing HP-UX guests.

4.2.1 HP-UX 11.31 Guests May Fail to Configure More than Two MPT Interfaces

If an HP-UX 11.31 system is configured with less than 2112 MB of memory, no more than two MPT interfaces are successfully configured. If more than two interfaces are desired, allocate at least 2.5 GB of memory to the guest.

4.2.2 Patches for HP-UX 11.31 Guests

Customers running HP-UX 11.31 guests should install the following patches (or their superseding patches) in each guest running HP-UX 11.31:

- PHKL_36261
- PHKL_36242

These patches prevent performance problems in environments where applications spawn large numbers of short-lived processes (such as development environments). To obtain these patches, contact your support specialist or HP representative.

4.2.3 Do Not Run Live Kernel Debuggers Inside a Guest

Do not run tools that write kernel text, such as live kernel debuggers and performance tools such as `kgmon` and `kttracer` inside a guest. Under rare circumstances, these tools cause the guest to panic.

4.2.4 Do Not Use the `iomap(7)` Command on HP-UX Guests

The `iomap(7)` command allows you to map physical I/O addresses into the user process address space. Do not use this command on HP-UX guests.

4.2.5 iCAP Commands Fail on HP-UX Guests

iCAP is installed as part of the HP-UX OS installation. Install-time configuration of iCAP reports failure with messages similar to the following:

```
NOTE:      Checking for partitionable system.
ERROR:     Software configuration has failed. After addressing the issues
           in the following output, configure this software with
           'swconfig B9073BA'.

ERROR:     Command not allowed to run on a Virtual Machine Guest.
ERROR:     The "configure" script for "iCOD.ICOD-RUN" failed (exit code
           "1"). The script location was
           "/var/adm/sw/products/iCOD/ICOD-RUN/configure".
* This script had errors and the execution of this fileset
  cannot proceed until the problem is fixed. Check the above
  output from the script for further details.
* Running config clean command /usr/lbin/sw/config_clean.

* Summary of Execution Phase:
ERROR:     Installed      iCOD.ICOD-RUN,l=/,r=B.11.23.08.00.00.95
ERROR:     1 of 882 filesets had Errors.
* 881 of 882 filesets had no Errors or Warnings.
ERROR:     The Execution Phase had errors. See the above output for
           details.
```

These startup messages in `/etc/rc.log` may be disregarded.

iCAP commands cannot be used on virtual machines. iCAP commands are designed to work on the VM Host system.

This problem is resolved in guests running HP-UX 11i V2 0706 and later.

4.3 Linux Guests

The following sections describe release notes for Linux guests.

4.3.1 Linux Guest Installation Errors

The first time you install the Linux guest management software, the following error may occur:

```
=== from /var/log/messages file ===  
Jan 18 22:45:00 lsn0000 kernel: ipmi_si: Error clearing flags: c1
```

```
=== from "dmesg" command ===  
ipmi_si: Error clearing flags: c1
```

You can ignore this error message.

4.3.2 Linux Guests with FC Tapes Display Errors

MPT errors may appear while booting a Linux guest if FC tapes are attached to it. FC tape devices return EIO on device reset, which causes timeout of the MPT reset. The boot proceeds after the reset timeouts; these errors can be ignored. For example:

```
Use ^ and v to change option(s). Use Enter to select an option  
Loading.: Red Hat Enterprise Linux AS  
Starting: Red Hat Enterprise Linux AS- - - - -  
  
ELILO boot: Uncompressing Linux... done  
Loading initrd initrd-2.6.9-42.EL.img...done  
i8042.c: i8042 controller self test timeout.  
Red Hat nash version 4.2.1.8 starting  
mptbase: ioc0: ERROR - Doorbell ACK timeout (count=4999), IntStatus=80000000!  
mptbase: ioc0: ERROR - Doorbell ACK timeout (count=4999), IntStatus=80000000!  
  Reading all physical volumes. This may take a while..  
  Found volume group "VolGroup00" using metadata type lvm2  
  2 logical volume(s) in volume group "VolGroup00" now active  
INIT: version 2.85 booting  
      Welcome to Red Hat Enterprise Linux AS
```

4.3.3 Disable IPv6 on Linux Guests

Integrity VM does not support IPv6 on guests. Linux Redhat enables IPv6 by default. When the Linux guest boots, the following message is displayed:

```
printk: 1 message suppressed
```

This message indicates an issue in the IPv6 DAD (Duplicate Address Detect) mechanism and is harmless. You can ignore this message, or you can disable it by including the following line in the `/etc/modprobe.conf` file:

```
alias net-pf-10 off
```

4.3.4 Preparing Linux Guests for VM Manager

If Linux guests are to be managed by VM Manager:

1. Install the `tog-pegasus` package.
2. On Red Hat Enterprise Linux, modify the file `/etc/Pegasus/access.conf` to allow WBEM access using your designated WBEM user name and password. Follow the steps below to configure this file. In this example, your designated WBEM user name is assumed to be `wbemuser`.
 - a. Look for the following line in this file:

```
-: ALL EXCEPT pegasus:wbemNetwork
```
 - b. Change this line to either of the following options:
 - # Allow access only from user 'wbemuser':

```
-: ALL EXCEPT wbemuser pegasus:wbemNetwork
```
 - # Allow access by all users:

```
+: ALL EXCEPT :wbemNetwork
```
3. Start the `tog-pegasus` package by executing the following command:

```
# /etc/init.d/tog-pegasus start
```

For information on where to download the Utilization Provider for the Linux guest, see the *VSE Management Software Installation and Update Guide*.

4.3.5 IPv6 Dynamic Address Resolution is Broken in Linux

Linux guests report messages such as `printk: 1 message suppressed` on a regular basis on the console. To prevent these messages, add the following line to the file `/etc/modprobe.conf`:

```
alias net-pf-10 off
```

4.3.6 Infrequent “Ooops: timer ticks before it is due” Errors

Infrequent `Ooops: timer ticks before it is due` messages appear on the console. You can safely ignore this message, because it is harmless.

4.3.7 Infrequent “e1000: eth1: e1000_clean_tx_irq: Detected Tx Unit Hang” Errors

Infrequent `e1000: eth1: e1000_clean_tx_irq: Detected Tx Unit Hang` messages appear on the console. You can safely ignore this message, because it is harmless.

4.3.8 Inconsistent “Bogomips” Values between Virtual CPU0 and Other Virtual CPUs

“Bogomips” values can be inconsistent between virtual CPU0 and other virtual CPUs. This condition is harmless. To prevent this problem, add the `lpj=4000000` boot option in `/boot/efi/efi/redhat/elilo.conf`. For example:

```
# cat elilo.conf
prompt
timeout=20
default=linux
relocatable

image=vmlinuz-2.6.9-42.EL.img
    label=linux
    initrd=initrd-2.6.9-42.EL.img
    read-only
    root=/dev/VolGroup00/LogVol100
    append="console=tty0 console=ttyS0 rhgb quiet lpj=4000000
```

4.3.9 Incorrect Display of Special Characters when Displayed Using HP-UX Terminal

The Linux Red Hat installation program does not display correctly when run within `hpvmconsole` on an HP-UX terminal. It displays accented A characters instead of boxes.

4.3.10 Occasional Floating-Point Assist Fault Messages.

Occasional floating-point assist fault messages appear when running Mozilla. This problem also occurs on native Integrity servers running Linux. For more information, see the “Developer & Solution Partner Program (DSPP)” web page on <http://www.hp.com>, and search for “floating-point assist fault”.

5 Using Integrity VM Commands

This section contains notes about the Integrity VM commands.

5.1 Using `hpvmmodify -N -s` Options Together Causes Guest to Be Inaccessible

Using the `hpvmmodify -N` and `-s` options together can cause the guest to disappear from the `hpvmstatus` output and become inaccessible. The guest directory name is erroneously changed, but the guest configuration files still have the original guest names.

To correct this problem, change the guest name back to the original guest name using the following command:

```
# mv /var/opt/hpvm/guest/guest_new_name /var/opt/hpvm/guest/guest_original_name
```

5.2 The `hpvmmodify` Command Reevaluates Guest Configurations

When you use the `hpvmmodify` command to modify a guest, the entire guest configuration is reevaluated. Any problems that might prevent the guest from starting are reported. For example, if a guest has a reference to a host device that no longer exists, and you enter an `hpvmmodify` command that modifies the guest but does not fix the bad reference, a warning message is generated.

5.3 The `hpvmdevgmt` Command Truncates File Sizes

When you use the `-S` option on the `hpvmdevgmt` command to create a file to be used as a virtual device, you can specify the file size. The file size must be specified in whole integers. Anything after the initial whole integer is ignored. For instance, both the `hpvmdevgmt -S 1G` command and the `hpvmdevgmt -S 1.5G` command create a 1 GB file.

5.4 Setting Devices to Sharable Can Lead to Device Conflicts

Integrity VM allows Virtual FileDVDs to be shared by guests. With HP Serviceguard, you can share Virtual Disks. Other types of storage devices are not supported for sharing and cannot be allocated to multiple guests. Be careful when you set a virtual device to sharable using the `hpvmdevgmt` command. Incorrectly marking a virtual device as sharable can lead to device conflicts and data corruption if multiple guests access it concurrently. In particular, attached devices (tape, burner, or changer) should not be made sharable.

5.5 Errors on Displaying Guest or Vswitch Information While that Information is Being Modified

The `hpvmstatus`, `hpvmmodify`, `hpvmcreate`, `hpvmclone`, and `hpvmremove` commands might return the following error when another command accesses the same guest's configuration files at the same time:

```
hpvm_guest_get_state:103:No Guest by that name or number
```

If you receive this error when you try to display a guest or vswitch configuration, enter the command again.

5.6 Do Not Attempt to Remove Busy Virtual Devices

Before removing virtual devices with the `hpvmmodify` command, make sure that the guest operating system is no longer directing I/O to the device. Unmount the device if it is mounted. If you attempt to remove a device that has I/O in progress, the `hpvmmodify` command incorrectly removes the device from the guest configuration file. The `hpvmstatus` command no longer

displays the device, and the `hpvmmodify` command does not retry the device removal, but the guest operating system sees the device as available. To remove the device, restart the guest.

5.7 Missing `uuid` or `.vmid` Files

If you use Integrity VM commands while guests are being removed, you may receive errors about missing `uuid` or `.vmid` files. Enter the command after the guest removal has completed.

5.8 Maintain Minimum Entitlement

The `hpvmcreate` and `hpvmmodify` commands do not allow the minimum CPU entitlement to be set below 5%. If you force the entitlements below 5%, boot time and potential runtime failures occur.

Set entitlement percentages in integers, not fractions. Fractions are ignored.

5.9 Guest Memory Must Be a Multiple of 64 MB

When you specify the guest memory, use a multiple of 64 MB. When a guest is created, Integrity VM rounds the guest memory up to the nearest multiple of 64 MB. However, if you specify a value that is not a multiple of 64 MB, the actual value can be rounded down, which may prevent the guest from booting.

5.10 Actual Running Entitlement May Differ from Configured Entitlement

Displayed and reported guest entitlement settings can differ from values that are specified. This occurs when entitlement settings have a granularity of one percent of the VM Host CPU capacity. An entitlement specified in cycles can be rounded to an integral percentage of VM Host cycles. For example, if you specify the guest entitlement as `-E 100` on a 900 MHz host system, it is rounded to 108 MHz (12%).

5.11 Duplicate Messages when Modifying Running Guests

Using the `hpvmmodify` command to add zero-length files to file-backed virtual disks can result in duplicate warning messages. For example:

```
# hpvmmodify -P test_duperr -a disk:scsi::file:/tmp/zero.size.1 \  
-a disk:scsi::file:/tmp/zero.size.2  
hpvmmodify: WARNING (test_duperr): File size of: 0 (bytes) for disk backing file:  
/tmp/zero.size.1 must be equal to or greater than: 512 (bytes),  
or the device may not show up in the guest when booted.  
hpvmmodify: WARNING (test_duperr): File size of: 0 (bytes) for disk backing file:  
/tmp/zero.size.2 must be equal to or greater than: 512 (bytes),  
or the device may not show up in the guest when booted.  
hpvmmodify: WARNING (test_duperr): File size of: 0 (bytes) for disk backing file:  
/tmp/zero.size.1 must be equal to or greater than: 512 (bytes),  
or the device may not show up in the guest when booted.  
hpvmmodify: WARNING (test_duperr): File size of: 0 (bytes) for disk backing file:  
/tmp/zero.size.2 must be equal to or greater than: 512 (bytes),  
or the device may not show up in the guest when booted.
```

Remove the failing device from the guest configuration using the `hpvmmodify` command.

5.12 Manpages Display on Linux Guests

The `hpvmcollect` and `hpvminfo` commands are available on Linux guests after installing the Linux guest management software kit, as described in the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual. To view the command displays properly, enter the following commands on the Linux guest:

```
# export LANG=en_US.iso88591  
# export TERM=vt200
```

Exporting these environment variables allows you to display the manpage content from a Linux guest console. Some minor differences in the appearance of the manpages as displayed on HP-UX and as displayed on Linux are expected.

6 Guest Administration

This chapter contains information about managing Integrity VM guests.

6.1 Administrator Account Names

This version of Integrity VM lifts the restriction that the virtual console administrator account names must be the same as the guest name. As a result, the virtual console administrator name can be any valid HP-UX login name. To continue accessing the virtual console, existing guest console accounts must be added to the authorization list for the associated guest with the `usermod` command. This allows multiple accounts to map to the guest, and requires the account names to be valid HP-UX login strings.

Authorization of access to the virtual console is determined by the guest configuration file (set using the `-u` and `-g` options to the `hpvmcreate`, `hpvmmodify`, and `hpvmclone` commands). This controlled access allows you to temporarily block access by using the `hpvmmodify` command to change the virtual console administrator account name.

6.2 Guest User Accounts

The configuration for captive `hpvmconsole` guest user accounts has changed in this release to support additional access controls and configurations. This change requires that the guest user accounts have the correct home directory. It is also necessary to list the console access account in the guest configuration file.

For example, using a guest named `compass1` (and therefore a user account named `compass1`), the home directory for user `compass1` must be `/var/opt/hpvm/guests/compass1`. To ensure that the user continues to have administrative console access, use the following command:

```
# hpvmmodify -P compass1 -u compass1:admin
```

6.3 Creating Virtual Machine Administrator and Operator Accounts

In prior versions of Integrity VM, only `admin` console access is available, and only one such account per guest is allowed. The administrator account name must match the guest name. The new version of Integrity VM provides proper access controls and individual accountability for these accounts.

A captive virtual console account is a special-purpose user account created on the VM Host for each guest administrator. These types of user accounts use `/opt/hpvm/bin/hpvmconsole` for a shell, and the desired guest's per-guest directory for a home directory. For virtual console access, the account also requires a password, and access to its associated guest. You create this account with the `hpvmcreate`, `hpvmclone`, or `hpvmmodify` command. You can establish group membership of the account using the `-g` option to those commands, or user membership, using the `-u` option to those commands.



NOTE: Do not use the `hpvmsys` group for user accounts. This group is used for security isolation between components of Integrity VM.

The HP-UX `useradd` command may not work as expected. To create user accounts for virtual console access, use the `useradd` command before you create the virtual machine. Alternatively, specify the user account directory completely in the `/etc/passwd` file, ensuring the entry is unique.

In the following example, the `useradd` command is used to create three user accounts on the VM Host system (`testme1`, `testme2`, and `testme3`):

```
# useradd -r no -g users -s /opt/hpvm/bin/hpvmconsole \  
-c "Console access to guest 'testme'" \  
testme1
```

```

-d /var/opt/hpvm/guests/testme \
testme1
# useradd -r no -g users -s /opt/hpvm/bin/hpvmconsole \
-c "Console access to guest 'testme'" \> -d /var/opt/hpvm/guests/testme \
testme2
# useradd -r no -g users -s /opt/hpvm/bin/hpvmconsole \
-c "Console access to guest 'testme'" \
-d /var/opt/hpvm/guests/testme \
testme3

```

The following command creates the virtual machine named `testme`:

```
# hpvmcreate -P testme -u testme1:admin -u testme2 -u testme3:oper
```

At this point, users `testme2` and `testme3` both have `oper` level access to the virtual console, and user `testme1` has `admin` level access. In order to make these accounts usable, set passwords for them, as follows:

```

# passwd testme1
...
# passwd testme2
...
# passwd testme3
...

```

Because of the way the `useradd` command works, an attempt to create an additional account may result in an error. For example, the following command attempts and fails to add the `testme4` user account:

```

# useradd -r no -g users -s /opt/hpvm/bin/hpvmconsole \
> -c "Console access to guest 'testme'" \
> -d /var/opt/hpvm/guests/testme \
> testme4
'/var/opt/hpvm/guests/testme' is not a valid directory

```

To enter the command correctly, include the entire directory path. For example:

```

# useradd -r no -g users -s /opt/hpvm/bin/hpvmconsole \
> -c "Console access to guest 'testme'" \
> -d /var/opt/hpvm/guests/testme/. \
> testme4
# hpvmmodify -P testme -u testme4
# passwd testme4

```

Note the addition of the `/.` to the end of the argument to the `-d` option, which ensures there is no confusion with HP-UX shared home directories.

6.4 Modifying Guests

Do not reduce the physical CPU count below the virtual CPU (vCPU) count of any guest. No running guest should be allocated more vCPUs than the VM Host system has physical processors.

6.5 Do Not Add User Accounts to the `hpvmsys` Group

The `hpvmsys` group implements the security model for the VM Host and guests. The `hpvmsys` group is automatically added to `/etc/group` when Integrity VM is installed. Do not add user accounts to this group.

6.6 Do Not Enter `Ctrl/B` after Starting Guest with Virtual Console

When you use the `pc -on` command inside the Integrity VM virtual console to start the guest, do not enter **Ctrl/B**; this will interrupt the guest boot process. Wait for the guest boot to complete and the virtual console prompt to return. Then enter **Ctrl/B**.

6.7 Restoring the NVRAM for Windows Guests

When a guest has been terminated unexpectedly due to a panic or another critical condition, the guest's boot settings (which are stored in a per-guest NVRAM file on the VM Host) can become corrupted. This can cause problems with subsequent reboots of that guest. To correct the problem, copy the file `/opt/hpvm/guest-images/common/nvram` to `/var/opt/hpvm/guests/vm_name/nvram` on the VM Host system. This procedure restores the copy of the NVRAM that was used when the guest was created. Then you can use the EFI Boot Manager to recreate the guest's boot path and other data. (The installed guest's operating system should be intact and unaffected by the corruption.)

To build the EFI Boot Menu Entry for Windows Enterprise:

1. From the Boot Maintenance options, select the boot device and enter the following command:

```
fs0> ls \EFI\Microsoft\WINNT50
```

Look for the `Bootxxxx` filename.

2. Change to the `MSUtil` directory. For example:

```
fs0> cd \MSUtil
```

3. Enter the following command:

```
fs0:> nvrboot
```

4. Enter the `I` command to import the Windows boot entry. Then enter the correct location of the boot entry. For example:

```
\EFI\Microsoft\WINNT50\Bootxxxx
```

6.8 How to Stop Guests

To stop a guest, HP recommends that you perform an operating system shutdown from a privileged account on the guest. If the guest is not responding, use the `hpvmstop -g` command on the VM Host. Do not stop a guest by killing the `hpvmapp` process.

6.9 The `hpvmconsole pc -cycle` Command Occasionally Doesn't Complete

If the guest `hpvmconsole pc -cycle` command doesn't complete and restart the guest, enter **Ctrl/B** to interrupt the command and then press **Enter** to return to the virtual console. Exit the virtual console by entering the `X` command. At the VM Host command prompt, enter the following command to start the guest:

```
# hpvmstart -P guestname
```

6.10 How to Recover from a Guest Hang

If a guest hangs, use **Ctrl/B** to enter the virtual console. Enter the `tc` command to reset the guest. The guest captures a memory dump of the machine state, which can be used later for offline diagnosis. Do not kill the guest from the VM Host or use the virtual console to power down a hung guest. Doing so can corrupt the guest file system.

6.11 Using HP Serviceguard to Manage Guests

This section lists release notes specific to using Serviceguard in the Integrity VM environment.

Do not attempt to use guests as Serviceguard packages and guests as Serviceguard nodes at the same time on the same VM Host system.

You can install HP Serviceguard A.11.16 or 11.17 on the VM Host or on the HP-UX guest. You can install HP Serviceguard 11.18 only on guests running HP-UX 11i v3.

6.11.1 Required HP Serviceguard Patches

To use Serviceguard to manage HP-UX guests, make sure the required patches are installed. For more information, see [Section 2.1.6 \(page 18\)](#).

6.11.2 Reenter Command to Start Packages

The procedure for configuring and starting guest packages includes the `cmrunpkg` command. This command does not always work the first time you enter it. If the command does not start the package, re-enter the command.

6.11.3 Do not Use Integrity VM Commands to Manage Distributed Guests

Guests configured as Serviceguard packages should only be stopped and started using Serviceguard package control commands. Do not use the Integrity VM commands (`hpvmstart`, `hpvmstop`, and `hpvmconsole`) to start and stop these types of guests. For more information about using Serviceguard to manage virtual machines, see the *Integrity Virtual Machines Installation, Configuration, and Administration* manual.

6.11.4 Different Cluster Nodes Report Virtual Machine Status Differently

Integrity VM commands can receive different warnings and errors from guests running on different Serviceguard nodes. For example, the Serviceguard node that is starting a guest as part of a package knows that the guest is running before any other nodes know. (The delay is usually less than 10 seconds.) Commands that are run on different servers report different errors or warnings depending on whether the guest is running or not.

6.11.5 Syslog Entries for `cmclld` Can Be Ignored

With Serviceguard and Integrity VM running, you may see the following types of message in the `syslog` file:

```
Syslog entries - cmclld[XXXX]: Warning: cmclld process was unable to run for the last X.XX seconds
```

These messages can be ignored.

6.11.6 Using Virtual Machines Manager (VM Manager) to Manage Distributed Guests

The following situations might occur when you are using VSE to manage distributed guests (guests that are configured as Serviceguard packages):

- There is a guest configuration file for each guest on each VM Host. Therefore, when you modify a distributed guest you must modify the guest on each VM Host that is a cluster node.
- Do not start and stop distributed guests using VM Manager menu items. Use Serviceguard commands to start and stop distributed virtual machines. For more information, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.
- The **VM Hosts** field on the VM Properties page sometimes shows an incorrect list of hosts in the cluster. If VM Manager is running on the VM Host that is actively managing the virtual machine that is being viewed, the list is correct. In all other cases, the list is incorrect.

6.11.7 Polling Interval for Virtual Machine Serviceguard Nodes

Serviceguard failover in Integrity VM can take longer than expected with the default 5-second network polling interval. To reduce the failover time, reduce the value of the `HPVMNETINTVL` tunable to 2.

If your system has Serviceguard installed and you want to make sure that failover of their `vswitches` used for Serviceguard fail over in less than 5 seconds, use a text editor to add or change the following line in the `/etc/rc.config.d/hpvmconf` file:

HPVMNETINTVL=*n*

Where *n* is an integer between 1 and 10 that specifies the number of seconds.

The default value is 5. That is, if the HPVMNETINTVL tunable is not set in the file, the value is 5 seconds. For Serviceguard in Integrity VM configurations, the recommended value is 2.

For more information, see the following manuals:

- *HP Integrity Virtual Machines Installation, Configuration, and Administration*: Chapter 11, “Using HP Serviceguard with Integrity VM”
- *Managing Serviceguard*: Chapter 4, “Planning and Documenting an HA Cluster”

6.12 Managing Guests using gWLM

Guests configured with processing power specified in cycles instead of percentage are incompatible with gWLM A.02.50 and earlier versions.

If gWLM/VSE produces an error message similar to the following, a guest is configured with the processing power specified in cycles:

```
A VM encountered with no size
```

This is apparent when using gWLM A.02.50 with Integrity VM A.03.00. You can correct the problem by modifying the guest and specifying processing power in percentage rather than CPU cycles. For example, to modify the guest named `compass1` to use 10% of the CPU processing power, enter the following command

```
# hpvmmmodify -P compass1 -e 10
```

You must boot the guest to initiate this setting for gWLM.

Alternatively, upgrade gWLM to A.03.00 for use with Integrity VM A.03.00.

7 Networking Information

This section contains notes about configuring networks for virtual machines.

7.1 Vswitches Are Always in SHARED Mode

The `hpvmnet` command displays the status of the vswitches, including the mode. The vswitches are always in SHARED mode. No other modes are supported at this time.

7.2 Do Not Use the HP A5506B PCI 10/100Base-TX 4 Port Interface for Virtual Networking

Host to guest connectivity may not be reliable when using the HP A5506B PCI 10/100Base-TX 4 Port interface for guest networking.

7.3 MAC Address Validation Can Be Enhanced

When you add a virtual NIC to your guest, Integrity VM checks to make sure the MAC address is unique.

By default, Integrity VM makes three attempts (each with a one-second timeout) to determine the validity of the MAC address for the virtual NIC. This process can result in up to ten seconds of delay for each defined virtual NIC. To speed up this processing, add the following tunable to the `/etc/rc.config.d/hpvmconf` configuration file:

```
HPVMMACADDRFRAMES=n
```

Where *n* is the number of attempts (1 to 30). The default is 3. A value of 1 or 2 increases performance at the risk of missing a response from a slow NIC.

Do not set the HPVMMACADDRFRAMES tunable to 0. Setting this tunable to 0 results in a virtual NIC with a MAC address that is the same as another virtual or physical NIC. The first guest to boot obtains the MAC address; the guest with the duplicate MAC address fails to boot.

To boost virtual network performance, create additional vswitches and allocate them across guests.

7.4 Auto Port Aggregation (APA) is Supported on the VM Host, Not on the Guest

Integrity VM does not support running APA on a guest. You can run APA on the VM Host.

APA can be configured on the VM Host to provide a highly available LAN for the vswitch (APA in active/passive mode) or to increase the bandwidth of the vswitch LAN (APA active/active mode). Before you stop APA, use the `hpvmnet -h` command to halt the vswitch. If you do not halt the vswitch first, the `hpvmnet` command reports an incorrect MAC address for the vswitch.

7.5 Do Not Run Applications that Set Network Devices into Promiscuous Mode

Vswitches must not be connected to network devices that are set to promiscuous mode. Do not run applications like `tcpdump` on the VM Host on interfaces that are used for virtual switches.

7.6 Do not Turn on Checksum Offloading (CKO) on the Physical Network Interface Backing the Vswitch

Checksum offloading (CKO) is turned off by default on physical network interfaces used as backing for the vswitch. Do not turn on CKO on from the guest using a remote command, such as `remsh`. The operation hangs and interrupts the guest network.

7.7 Do Not Turn on TSO on the VM Host and on HP-UX Guests

TCP Segmentation Offload (TSO) is turned off by default in HP-UX. HP recommends that you leave it turned off on both the VM Host system and on HP-UX guests. This applies to both the virtual network interface cards in the guest and any physical network interface cards in the VM Host that are used by vswitches. When TSO is enabled, guest networks are interrupted.

To verify whether TSO is turned on, enter the following command:

```
# lanadmin -x vmtu n
```

Where *n* is the VM Host interface, as displayed by the `hpvmnet` command. For example, to verify that TSO is on for `lan0`, enter the following command:

```
# lanadmin -x vmtu 0
```

```
Driver/Hardware supports TCP Segmentation Offload, Current VMTU = 32160
```

To turn TSO off on `lan0`, use the following command:

```
# lanadmin -X vmtu 0 0
```

```
Virtual MTU is set to 0
```

7.8 Do Not Configure VLAN Vswitches on HP-UX VLANs

Do not use the `hpvmnet` command to create a virtual switch that is associated with a VLAN port on the VM Host (that is, a LAN created with `lanadmin -v`). This “nested VLAN” configuration is not supported.

7.9 For VLANs Between VM Host and Guests, Turn Off CKO

Checksum offload (CKO) on the network interface used by the vswitch is turned off by default during vswitch creation. When you use a VLAN vswitch for communication between guests and the VM Host, turn off transmit checksum offload (CKO) on the network interface used by the vswitch. On the VM Host, identify the PPA of the network interface for the vswitch using the `hpvmnet` command. For example:

```
# hpvmnet
```

Name	Number	State	Mode	PPA	MAC Address	IP Address
localnet	21	Up	Shared		N/A	N/A
vmlan0	22	Up	Shared	lan0	0x00306ea72c0d	15.13.114.205
vmlan4	23	Up	Shared	lan4	0x00127942fce3	192.1.2.205
vmlan900	24	Up	Shared	lan900	0x00306e39815a	192.1.4.205

Check the status of the transmit CKO using the following command:

```
# lanadmin -x cko 4
```

```
Hardware TCP/UDP (IPv4) transmit checksum offload is currently enabled.  
Hardware TCP/UDP (IPv4) receive checksum offload is currently disabled.
```

In this example, the VLANs are configured over the vswitch `vmlan4`. This vswitch is created on PPA 4 on the VM Host. To turn off CKO on PPA 4, enter the following command on the VM Host:

```
# lanadmin -X send_cko_off 4
```

```
Hardware TCP/UDP (IPv4) transmit checksum offload is currently disabled.
```

7.10 Restarting Vswitches

It is necessary to restart the vswitch when:

- You replace the physical network card associated with the vswitch.
- You change a VM Host IP address associated with the vswitch's network interface card.
- You change the network interface characteristics on the VM Host; for example, by using the `lanadmin` command to change checksum offloading (CKO).

For information about how to restart vswitches, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

When you restart a vswitch, it is not necessary to restart the guests using the vswitch.

8 Storage Information

This section contains information about storage devices used as backing stores for guest virtual devices.

8.1 DMP Files Not Supported as Backing Stores

Veritas VxVM DMP device files (files under `/dev/vx/rdmp/`) is not supported by Symantec for whole disk backing stores for virtual machines.

8.2 Using Database Management Products on Virtual Machines

For optimal performance with storage intensive applications such as Oracle®, HP strongly recommends using whole disk backing stores. Virtual disks that use logical volumes or files as backing storage do not provide optimal performance for this type of application. For more information about the Integrity VM storage subsystem, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

8.3 Integrity VM Does Not Honor File Permissions on Backing Stores

File permission settings do not affect the way Integrity VM accesses backing stores. Backing stores provided as virtual disks can be written to regardless of the file permission settings on the backing store. A backing store provided as a virtual DVD is always read-only. Attached devices do not consider file permissions when backing up data.

8.4 Using USB CD/DVD Devices

USB CD/DVD devices are not supported for use as attachable media, and perform slowly when used as virtual devices. HP Integrity blade, rx3600, and rx6600 servers with such devices should use Virtual FileDVDs or Ignite-UX for guest operating system installations. Hardware supportability requirements for Integrity VM are described in the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

To identify USB CD/DVD devices, use the `ioscan -fun` command.

8.5 The `hpvmmodify` Command Fails to Change a DVD

The `hpvmmodify` command might fail to change a Virtual FileDVD if the device has already been modified by the virtual console. The `hpvmstatus` command displays the current status of the Virtual FileDVD, which may not be in its original resource state. To see the original resource statement, which is required by the `hpvmmodify` command to change a Virtual FileDVD, use the `hpvmstatus -D` command.

8.6 Virtual FileDVD Reverts to Original Resource Statement

A Virtual FileDVD reverts to its original resource statement when the guest shuts down or reboots. Therefore, after you install a guest from multiple CDs or DVDs, you must reload the Virtual FileDVD when the guest reboots to complete the installation. Stop the automatic EFI reboot and insert the CD/DVD using the appropriate `IN` and `EJ` commands. When the media is loaded, proceed with the installation.

8.7 Physical Device `null` Assigned to Nonexistent Path

Devices with physical storage type `null` may be given device path specifiers that do not exist. This problem does not prevent guests from starting. In previous versions of Integrity VM, the guest does not start if the device path for a `null` physical storage type device does not exist as a real device, file, or directory.

8.8 Using sam on Guest Cannot Initialize Disk

When you create a file system using the `sam` command on an HP-UX guest, do not initialize the disk. This option returns an error and the file system is not created.

8.9 Extending a Logical Volume Backing Store Corrupts the Guest

On the VM Host, do not extend a logical volume (LVM or VxVM) used as a backing store for a guest root disk. If you do this, the guest panics on its next reboot with the following error:

```
System panic: all VFS_MOUNTROOTs failed: Need DRIVERS.
```

In this case, the guest root device has been corrupted. You must reinstall the guest operating system.

For a logical volume used as a backing store for a guest data disk, you can extend the volume after removing it from the guest using the `hpvmmodify` command. After extending the volume, use the `hpvmmodify` command to add the volume to the guest. Do not modify a logical volume used as a backing store without first removing it from the guest.

After you extend the logical volume, use operating system commands on the guest to extend its file system.

8.10 Management Limitations of Virtual SCSI Devices

Although SCSI devices appear to a guest as Ultra320 SCSI controllers claimed by the MPT driver, this is an emulation. There are several differences from using a real device. Specifically:

- You cannot upload or download firmware for emulated devices.
- Although HP-UX commands such as `mptutil(1M)` and `mptconfig(1M)` do not fail when run in a guest, they do not always return the same information as they would when referencing a physical device.
- The EFI `drvcfg` command does not fail when run in a guest, but it returns no useful data.

8.11 Installing Integrity VM Clears SecurePath 3.0F SP1 Settings

If you are using SecurePath for a storage array configured as active-active, update to SecurePath 3.0F SP2 before installing Integrity VM. With earlier versions of Securepath, you must manually restore your SecurePath configuration after installing Integrity VM.

9 Migrating Virtual Machines

This section contains information about migrating virtual machines.

9.1 Do Not Migrate Distributed Guests

Guests that are configured as Serviceguard packages cannot be migrated.

9.2 Collect CapAd Data before Migrating

If you migrate a virtual machine that is being managed by VSE, use Capacity Advisor to collect utilization data before you migrate the virtual machine. Otherwise, the utilization information for the VM Host prior to the migration is lost.

10 Error Logging

This section contains information about the way Integrity VM logs messages.

10.1 Guest Log Can Grow Unbounded

The guest monitor log file (`/var/opt/hpvm/guests/vm_name/log`) records guest start and stop information. These log files can grow very large. Use the `hpvmconsole` command `rec -rotate` to close the current log file, rename it, and open a new one.

10.2 Log Messages Written to Old Log File

Log messages might be written to the `command.log.old` file instead of the `command.log` file. If this is a problem, reboot the VM Host system. This reinitializes the log file for applications that generate Integrity VM log messages to write to the current `command.log` file.

10.3 Saved MCA or INIT Register State Can Be Inaccurate

Virtual machines do not support standard management processor console `errdump` commands. The virtual console's Virtual Machine menu provides the `ed` command for this purpose. The options for a virtual machine are `-mca` and `-init`. When you examine the saved guest state using the `ed -mca` or `ed -init` command, the preserved branch registers (B1-B5) do not always contain accurate data.

10.4 Modifying the Size of the Monitor Log File

Integrity VM includes a monitor log (`/var/opt/hpvm/common/hpvm_mon_log`), which captures the state of the VM Host. The size of the log file is determined by the `VMMLOGSIZE` tunable, stored in the `/etc/rc.config.d/hpvmconf` file.

When the log file reaches `VMMLOGSIZE`, the current timestamp is appended to the name of the log file and a new log file is opened. If you see many such files, increase the value of the `VMMLOGSIZE` tunable. Do not set the value of the `VMMLOGSIZE` tunable below its 1024 KB default.

10.5 Virtual Console Event Logs Different from Physical Machine Logs

The virtual console allows you to use the `s1` command to list the System Event log and the Forward Progress log. The displays from the virtual console differ from those generated on a physical machine in the following ways:

- Event numbering is inconsistent for different lines.
- Although the command menu allows you to specify a cell number, virtual machines are not cellular. Therefore, this option is not functional.