HP Integrity Virtual Machines Release Notes Version A.03.50

HP Part Number: T2767-90170
Published: November 2008, Edition 7.1

Legal Notices

Acknowledgments

Table of Contents

About This Document....9
Intended Audience....9
New and Changed Information in This Edition....9
Typographic Conventions....9
Document Organization....9
Related Information....10
Publishing History....10
HP Encourages Your Comments....11

1 Introduction....13
1.1 New Features and Enhancements in This Version of Integrity VM....13
1.2 Using Linux Guests....15
1.3 Creating Virtual Machine Administrator and Operator Accounts....16
1.4 Integrity VM Command Changes....16
1.5 Using the IGNOREWWID=YES Attribute....17
1.6 Specifying Memory Type....17
1.7 Guest Management Software....17

2 Installation Notes....19
2.1 Installing Integrity VM....19
2.1.1 Install these Patches....19
2.1.2 Do not install Integrity VM V3.5 Kit on a Host Prior to HP–UX 0712....19
2.1.3 Integrity VM Includes the Foundation Operating Environment....19
2.1.4 Upgrade HP WBEM Services....20
2.1.5 Installing the Migration Tools Including `hpvmmigrate` and Physical-to-Virtual Assist Tools....20
2.1.6 Installing VM Provider....20
2.1.7 VMMGR V3.0 Does Not Support Integrity VM V3.5 AVIO Functionality....21
2.1.8 VxVM Device Path Not Valid Error on HP-UX 0803....21
2.1.9 HP-UX Patches Required in the VM Host....21
2.1.10 Patches Required in the HP-UX Guest....23
2.1.11 Patches Required for Ignite/UX Servers....26
2.1.12 Patches Required for Windows Guests....26
2.1.13 Patches Required for Red Hat Linux Guests....26
2.1.14 Patches Required for SUSE Enterprise Linux Guests....27
2.2 Upgrading from Earlier Versions of Integrity VM....27
2.3 Installing the HP Integrity Virtual Machines Product Over the Evaluation Software....28
2.4 Do Not Install Applications on the VM Host System....28
2.5 Do Not Install Integrity VM on a Virtual Partition....29
2.6 Do Not Install Windows as Alternate Boot on a VM Host System....30
2.7 Trunking Software....30
2.8 Using EMC PowerPath with AVIO and VIO....30

3 Creating Virtual Machines....31
3.1 Default Guest Settings for HP-UX, Windows, and Linux....31
3.2 Autoboot Causes Virtual Machines to Start....31
3.3 Reserving Swap Space for Guests....31
3.4 Do Not Create Golden Images of the VM Host for Guest Installation....32

3.5 Golden Images of Systems with HPVM-Guest Installed Must have HPVM Device Drivers Configured....32
3.6 Numbers Reported by Glance 4.6 or above Running on VM Host Might be Incorrect....32
3.7 Interleaved Memory on Cellular Hosts....32
3.8 hpvmcreate Manpage Incorrect....32
3.9 hpvmstop Manpage Incorrect....33
3.10 New option for hpvmstatus Command....33
3.11 The `hpvmstatus` Display Can Lag in a Serviceguard Cluster....33

4 Installing Guests....35
4.1 Windows Guests....35
4.1.1 Removing Media During Installation Hangs Guest....35
4.1.2 Network Driver for Some Windows Guests Not Behaving Correctly....35
4.1.3 Virtual DVD Misconfiguration can Lead to Windows Slow Down....35
4.1.4 HP Insight Manager Automatic Server Recovery Does Not Work....35
4.1.5 PalHalLight RegEdit Patch Should Not be Installed....35
4.1.6 Installing Windows with Virtual NullDVD is Not Recommended....35
4.1.7 Enabling MP Services on Windows Guest Logs telnetd Errors....36
4.1.8 Using Windows Firewall Requires ICMP to Allow Echo....36
4.1.9 Poor Console Screen Formatting....36
4.1.10 The hpvmstop Command Does Not Shut Down Windows Guests Gracefully....36
4.1.11 Do Not Delete EFI Shell Boot Option....37
4.1.12 Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL — 1....37
4.1.13 Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL — 12....37
4.1.14 Restoring the NVRAM for Windows Guests....37
4.2 HP-UX Guests....38
4.2.1 Installing the Guest Management Software....38
4.2.2 HP-UX 11i v3 Guests Might Fail to Configure Interface Cards Due to Lack of Memory Resources....39
4.2.3 Patches for HP-UX 11i v3 Guests....39
4.2.4 Do Not Run Live Kernel Debuggers Inside a Guest....39
4.2.5 Do Not Use the `iomap(7)` Mechanism on HP-UX Guests....39
4.2.6 iCAP Commands Fail on HP-UX Guests....39
4.3 Linux Guests....40
4.3.1 SLES10 SP1 Guests Supported on Integrity Servers....40
4.3.2 Before Installing the SUSE Linux Guest....40
4.3.3 Installing Linux Guest Management Software for the First Time....40
4.3.4 ACPI Warnings, Errors, and Exceptions Displayed when SUSE Guest Booted....41
4.3.5 HP SIM CMS Cannot Connect to SLES10 over SSH....41
4.3.6 Preparing Linux Guests for VM Manager....41
4.3.7 Linux Guests with FC Tapes Display Errors....42
4.3.8 Disable IPv6 on Linux Guests....42
4.3.9 Infrequent “Ooops: timer ticks before it is due” Errors....42
4.3.10 Infrequent “e1000: eth1: e1000_clean_tx_irq: Detected Tx Unit Hang” Errors....42
4.3.11 Inconsistent “Bogomips” Values between Virtual CPU0 and Other Virtual CPUs....43
4.3.12 Incorrect Display of Special Characters when Displayed Using HP-UX Terminal....43
4.3.13 Occasional Floating-Point Assist Fault Messages....43
4.3.14 TC INIT Dump Messages Do Not Appear on the SUSE Linux Guest Console....43

5 Using Integrity VM Commands....45
5.1 Accidental Use of `-R` Option with `hpvmmodify` Instead of `-r`....45
5.2 Changing Guest LAN from AVIO to VIO....45
5.3 The `hpvmmodify` Command Reevaluates Guest Configurations....45

5.4 The hpvmdevmgmt Command Truncates File Sizes....45
5.5 Setting Devices to Sharable Can Lead to Device Conflicts....45
5.6 Errors on Displaying Guest or Vswitch Information While that Information is Being Modified...45
5.7 Do Not Attempt to Remove Busy Virtual Devices....46
5.8 Missing uuid or .vmid Files....46
5.9 Maintain Minimum Entitlement....46
5.10 Guest Memory Must Be a Multiple of 64 MB....46
5.11 Actual Running Entitlement Might Differ from Configured Entitlement....46
5.12 Duplicate Messages when Modifying Running Guests....46
5.13 Manpages Display on Linux Guests....46
5.14 hpvmpubapi Manpage on Linux Guests....47
5.15 Integrity VM Check Might Fail Because of Bad Switch....47

6 Guest Administration....49
6.1 Administrator Account Names....49
6.2 Guest User Accounts....49
6.3 Creating Virtual Machine Administrator and Operator Accounts....49
6.4 Modifying Guests....50
6.5 Do Not Add User Accounts to the hpvmsys Group....50
6.6 Do Not Enter Ctrl/B after Starting Guest with Virtual Console....50
6.7 HP-UX 11i v3 Guests Might Panic with a NaT_hndler: kernel NaT Consumption Fault....51
6.8 How to Stop Guests....51
6.9 The hpvmconsole pc –cycle Command Occasionally Doesn't Complete....51
6.10 How to Recover from a Guest Hang....51
6.11 Using HP Serviceguard to Manage Guests....51
6.11.1 The hpvmsg_package Does Not Add Appropriate Entries....51
6.11.2 Using AVIO lan Device in a Serviceguard Configured Guest....51
6.11.3 Required HP Serviceguard Patches....52
6.11.4 Reenter Command to Start Packages....52
6.11.5 Do not Use Integrity VM Commands to Manage Distributed Guests....52
6.11.6 Different Cluster Nodes Report Virtual Machine Status Differently....52
6.11.7 Syslog Entries for cmcld Can Be Ignored....52
6.11.8 Using Virtual Machines Manager (VM Manager) to Manage Distributed Guests....52
6.12 Managing Guests using gWLM....52

7 Networking Information....55
7.1 Supported Adapters....55
7.2 Sufficient Memory for Guests with Virtual LAN Devices....55
7.3 Vswitches Are Always in SHARED Mode....55
7.4 Do Not Use the HP A5506B PCI 10/100Base-TX 4 Port Interface for Virtual Networking....55
7.5 MAC Address Validation Can Be Enhanced....55
7.6 Auto Port Aggregation (APA) is Supported on the VM Host, Not on the Guest....55
7.7 VM Manager Does Not Display APA Link Aggregate LAN Device....56
7.8 Do Not Run Applications that Set Network Devices into Promiscuous Mode....56
7.9 Guest and Host Communication....56
7.10 Configuring vswitches to be Backed by a VLAN Interface on the VM Host is Not Supported....56
7.11 Do Not Turn on TSO on the VM Host and on HP-UX Guests....56
7.12 Restarting Vswitches....57
7.13 Guest AVIO Interface Behavior....57
7.14 AVIO LAN Devices Not Claimed by Guest with DOWN Vswitch at Boot Time....57
7.15 Do Not Use TCP Software Packet Reassembly in IGSSN Driver....58
7.16 HP-UX 11i v3 Guest Might Fail to Configure AVIO Network Interfaces Due to Lack of Memory Resources....58

7.17 Other Issues and Notes....58

8 Storage Information....61
8.1 Critical Issue Fixed in HostAVIOStor B.11.23.0803....61
8.2 USB 2.0 Now Supported....61
8.3 The sam Command might Display Incorrect Number of Disks and Paths on an HP-UX 11i v2 Guest....61
8.4 AVIO Current Limitations....62
8.4.1 Modifying the Storage Adapter from `scsi` to `avio_stor`....62
8.4.2 Virtual Device Types and Backing Store Support....62
8.4.3 GuestAVIO Bundle not Installed but AVIO Storage Device is Configured....62
8.4.4 Access of Disk Configured Under an AVIO Storage Adapter Might Take Longer than Expected....62
8.4.5 I/O Resource Delete Using `hpvmmodify` Fails When Guest is at EFI....63
8.4.6 Mapping AVIO Storage Devices....63
8.5 Crash Dump Collection Might Fail for HP-UX Guests with Attached I/O Devices....64
8.6 DMP Files Not Supported as Backing Stores....64
8.7 Assigning a Null Device to a Resource....65
8.8 Using Database Management Products on Virtual Machines....65
8.9 Integrity VM Does Not Honor File Permissions on Backing Stores....65
8.10 Using USB CD/DVD Devices....65
8.11 The hpvmmodify Command Fails to Change a DVD....65
8.12 Virtual FileDVD Reverts to Original Resource Statement....65
8.13 Physical Device `null` Assigned to Nonexistent Path....65
8.14 Using sam on Guest Cannot Initialize Disk....66
8.15 Extending a Logical Volume Backing Store Corrupts the Guest....66
8.16 Management Limitations of Virtual SCSI Devices....66
8.17 Installing Integrity VM Clears Secure Path 3.0F SP1 Settings....66
8.18 Secure Path and LVM Configurations....66
8.19 AVIO Multipathing Support....67
8.20 The gvsdmgr Utility....67
8.21 Storage Driver not Listed in Installation Manual....69

9 Migrating Virtual Machines....71
9.1 Do Not Migrate Distributed Guests....71
9.2 Collect CapAd Data before Migrating....71

10 Error Logging....73
10.1 Guest Log Can Grow Unbounded....73
10.2 Log Messages Written to Old Log File....73
10.3 Saved MCA or INIT Register State Can Be Inaccurate....73
10.4 Modifying the Size of the Monitor Log File....73
10.5 Virtual Console Event Logs Different from Physical Machine Logs....73

List of Tables

1-1 Guest Management Software Kit Locations....18
2-1 VM Host Patches....21
2-2 Do Not Install Product or Patch....23
2-3 HP-UX Guest Patches....24
2-4 Do Not Install Products or Patches on HP-UX Guests....26
2-5 Ignite/UX Patches....26
2-6 Windows Patches....26
2-7 Do Not Install Products or Patches on Windows Guests....26
2-8 Red Hat Linux Patches....27
2-9 SUSE Enterprise Linux Guests....27
3-1 Guest Default Settings....31

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.

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.

New and Changed Information in This Edition

This document supersedes the HP Integrity Virtual Machines Release Notes for Integrity VM A.03.50, T2767–90150.

Typographic Conventions

find(1)	HP-UX manpage. In this example, "find" is the manpage name and "1" is the manpage section.
Book Title	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 `PATH` or `errno`.
`value`	A value that you might 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.

Document Organization

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

- Chapter 1: "Introduction" (page 13) describes some of the enhancements and quality improvements in the current release of the HP Integrity Virtual Machines product.
- Chapter 2: "Installation Notes" (page 19) contains information about installing and upgrading Integrity VM and associated products.

- Chapter 3: "Creating Virtual Machines" (page 31) contains information about creating virtual machines.
- Chapter 4: "Installing Guests" (page 35) contains information about installing guest operating system and management software.
- Chapter 5: "Using Integrity VM Commands" (page 45) contains information about using Integrity VM commands.
- Chapter 6: "Guest Administration" (page 49) contains information about guest system administration.
- Chapter 7: "Networking Information" (page 55) contains information about virtual networking resources.
- Chapter 8: "Storage Information" (page 61) contains information about virtual data storage for guests.
- Chapter 9: "Migrating Virtual Machines" (page 71) contains information about migrating virtual machines from one system to another.
- Chapter 10: "Error Logging" (page 73) contains information about the message logging provided by Integrity VM.

Related Information

The following documents, which are found at the HP Technical Documentation website at http://docs.hp.com/, might be useful to the reader of this document:

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

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
T2767–90094	HP-UX 11i v2 December 2007 and later	HP Integrity Virtual Machines A.03.50	5.0	December 2007
T2767–90114	HP-UX 11i v2 December 2007 and later	HP Integrity Virtual Machines A.03.50	6.0	December 2007

Publication Number	Supported VM Host Operating System	Supported Integrity VM Version	Edition Number	Publication Date
T2767–90150	HP-UX 11i v2 March 2008 and later	HP Integrity Virtual Machines A.03.50	7.0	March 2008
T2767–90170	HP-UX 11i v2 July 2008 and later	HP Integrity Virtual Machines A.03.50	7.1	November 2008

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.

The Integrity VM Version 3.5 release introduces new accelerated storage and networking products to improve the overall I/O performance for Integrity VM. These new Accelerated Virtual I/O (AVIO) products provide up to a 60% reduction in service demand and as much as a twofold improvement in throughput over the existing fully-virtualized storage and networking Integrity VM solutions. Performance depends on the application workload, and in general, is better with larger message sizes.

HP Integrity Virtual Machines A.03.50 is supported as a host on HP Integrity servers or nPartitions running HP-UX 11i v2 December 2007 0712 or later. For complete information about the requirements for installing Integrity VM, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

NOTE: Integrity VM patches for fixes developed subsequent to the Integrity VM V3.5 release are available at the HP IT Resource Center (ITRC) website. Go to this website http://www.itrc.hp.com and download the following patches:

- PHSS_37312 (Integrity VM)
- PHSS_37306 (VMagent)

HP highly recommends that you install these patches. Make sure you install them after installing Integrity VM V3.5. In addition, update AVIO with the WEB0803 version.

HP highly recommends that you always install the latest AVIO components on both the VM Host and guests. For the latest version of the AVIO software, check the software depot website, http://software.hp.com and search for the keywords HPVM AVIO.

For the latest patch kits, see the HP IT Resource Center (ITRC) website: http://www.itrc.hp.com.

For the most up-to-date information about HP Integrity Virtual Machines, see the documentation on the HP Technical Documentation website, http://www.docs.hp.com.

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, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

- Guests can run any of the following operating systems:
  - HP-UX 11i v2 (May 2005 [0505] or later), including HP–UX 11i v2 0712
  - HP-UX 11i v3 0803.
  - Windows 2003 Server (Enterprise or Datacenter edition) SP1 and SP2
  - Red Hat® Linux Enterprise Edition Advanced Server Release 4 update 4, update 5, and update 6. (Support provided for update 6 in the Q1 Patch.)
  - SUSE® Linux Enterprise Server (SLES) for HP Integrity servers SLES 10 update 1.
- Integrity VM now includes the capability of Accelerated Virtual I/O (AVIO), which improves the performance of both storage and network access for virtual machines. With Integrity VM V3.5, AVIO supports on the VM Host on the HP-UX 11i v2 operating system and both HP-UX 11i v2 and HP-UX 11i v3 on virtual machines (guests). (AVIO support for 11i v3 guests was provided in the Q1 patch.)

  The AVIO feature includes:

  - Changes to the `hpvmnet` command. The changes include displaying the adapter type for each port defined on the vswitch and getting port specific statistics.
  - Changes to the *hpvmresources* and *hpvmstatus* manpages to include the new AVIO names for guest creation: `avio_lan`, and `avio_stor`.
  - Change to the `hpvmcollect` command to add values for AVIO LANs and storage.
  - Changes to the `hpvmcreate`, `hpvmclone`, and `hpvmmodify` commands to add the designation for an AVIO network adapter and an AVIO storage adapter on a guest. The network adapter designator is `avio_lan` or `aviolan`, and the storage adapter designator is `avio_stor` or `aviostor`. For more information about AVIO, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration Version A.03.50* manual.
  - Support for the AD386A 10GBe adapter.
  - Changes to the `hpvmclone` command to clone guests with additional AVIO network or storage devices.

  For information about installing AVIO drivers, see *HP Integrity Virtual Machines Installation, Configuration, and Administration Version A.03.50* manual.

- AVIO storage support for Logical Volume backing storage devices (virtual LvDisk) on HostAVIOStor B.11.23.0712.01 and later.
- AVIO now supports Active-Passive configuration on EVA GL series (3000/5000) starting with HostAVIOStor B.11.23.0712.01. This is in addition to the already supported Active-Active configuration on EVA GL and EVA XL series (4000/6000/8000). SecurePath Active-Passive is now supported in addition to Active-Active on AVIO. For more information, see Section 8.17.
- Hierarchy checking

  The `hpvmdevmgmt` command has been changed to provide hierarchy checking by adding a host-file-system directory to the device database as a restricted device. All files, devices, and subdirectories under a restricted directory are also restricted. A directory might not be restricted if a file, device, or subdirectory is already in use by a guest. Note that the `/etc` and the `/stand` directories are added by default.

- New public APIs defined in `/opt/hpvm/include/hpvm_api_public.h` for host and guests:

  The following APIs have been added to Integrity VM:

  - `hpvm_api_server_check` — Checks if running on an Integrity VM server system.
  - `hpvm_api_virtmach_check` — Checks if running on an Integrity VM virtual machine.
  - `hpvm_api_version_get` — Gets the version string of an Integrity VM server or virtual machine.
  - `hpvm_api_my_uuid_get` — Gets the uuid for this running Integrity VM server or virtual machine.
  - `hpvm_api_server_uuid_get` — Gets the uuid for the Integrity VM server of the virtual machine running this API.
  - `hpvm_api_server_hostname_get` — Gets the host name for the Integrity VM server of the virtual machine running this API.

  For information about the new public APIs, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration A.03.50* manual.

- The EFI direct tape boot functionality has been added to Integrity VM. If you use the Ignite make_tape_recovery utility on the HP-UX guest to make a backup tape of that guest system, you can use the backup tape to boot from EFI to perform the restore and reinstallation from the backup tape.

- Change to the `hpvminfo` command to display the information returned by the supported public interfaces defined in `/opt/hpvm/include/hpvm_api_public.h`. For example, when running on a VM host:

  ```
  hpvminfo -S
  HPVM Server information
  VERSION: HPVM A.03.50 BL10 clearcase opt Wed Aug 01 2007 12h20m34s EDT
  MY UUID: 58d03f5d-79ed-11d9-b720-17c097e9e0d0
  ```

  When running on a guest:

  ```
  hpvminfo -S
  HPVM Guest information
  VERSION: HPVM A.03.50 BL06 clearcase opt Mon Jun 11 2007 13h32m14s
  SERVER HOSTNAME: test.case.com
  ```

- Storage used by the VM Host system is now better protected in this release. The new `hpvmhostrdev` command identifies disks, LUNs, and logical volumes used by the VM Host for its operating system, file system, and swap storage as "restricted devices" in the Integrity VM device database. This prevents their use by virtual machines as storage, avoiding inadvertent corruption or destruction of the VM Host's environment. When Integrity VM starts on the VM Host system, it invokes the `hpvmhostrdev` command, automatically adding these restricted devices to the Integrity VM device database. The `hpvmhostrdev` command is based on the same storage analysis tools used by HP System Management Homepage (HP SMH) and other Virtual Server Environment (VSE) management tools, maintaining consistency across HP management products.

  The `hpvmhostrdev` command can also be used by privileged users on the VM Host system to update the Integrity VM device database. By default, the command forces a full hardware scan on the VM Host system. Depending on storage and network configuration, the scan might take several minutes to complete. This use might be prudent whenever new hardware is added to the VM Host system. The `hpvmhostrdev` command also accepts the `-u` option, which does not force a new HW scan, using the latest HW configuration information to update the device database. The only other option accepted by `hpvmhostrdev` is `-h,`, which provides a brief summary of the available options and their use.

  Existing virtual machines using deprecated storage for virtual disks, partitions created with `idisk`(1M) in particular, might not start after installing the latest release of Integrity VM. You can alleviate this condition by removing the restricted device entry corresponding to the base path of the disk that has been partitioned from the Integrity VM device database. For example, if the disk `/dev/rdsk/c2d3t4` has one or more partitions being used as virtual storage, execute the command `hpvmdevmgmt -d rdev:/dev/rdsk/c2t3d4` to delete the device from being used as virtual storage. Note that the use of such partitions for Integrity VM storage has been deprecated.

1.2 Using Linux Guests

This version of Integrity VM introduces support for SUSE Linux SLES 10 update 1 guests and Red Hat Linux Enterprise Edition Advanced Server Release 4 update 5 and update 6. You can install the SUSE Linux or the Red Hat Linux on a virtual machine.

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

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

NOTE: To use Red Hat Linux 4 update 6, you must install a patch on the guest. See Table 2-8 (page 27).

For information about the SUSE Linux operating system for HP Integrity servers, see http://h20341.www2.hp.com/integrity/cache/342574–0–0–0–121.html

The guest parameter settings for Linux guests are listed in Table 3-1 (page 31).

For information about installing Linux guests, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration A.03.50* manual.

1.3 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 49).

1.4 Integrity VM Command Changes

The Integrity VM commands have changed in the following ways:

- The `hpvminfo` command has been enhanced to print information that is accessible through the public APIs.
- The `hpvmnet` command now displays the adapter type for each port defined on the vswitch and provides the new option `-A`, which displays the AVIO port specific statistics. For example, if you have a guest with AVIO port, you can use the `hpvmnet` command as follows:

```
# hpvmnet -S myswitch -p 11 -A
Vswitch Name            :  myswitch
Max Number of Ports     :  100
Port Number             :  11
  Port State            :  Active
  Active VM             :  avio_vm
  Untagged VlanId       :  none
  Reserved VMs          :  avio_vm
  Adaptor               :  avio_lan
    Inbound Octets                      : 32714
    Inbound Unicast Pkts (wire)         : 197
    Inbound Unicast Pkts (local)        : 0
    Inbound Non-Unicast Pkts (wire)     : 0
    Inbound Non-Unicast Pkts (local)    : 0
    Inbound Discards                    : 0
    Outbound Octets                     : 19580
    Outbound Unicast Pkts (wire)        : 241
    Outbound Unicast Pkts (local)       : 0
    Outbound Non-Unicast Pkts           : 11
    Outbound Discards                   : 0
```

  There is no distinction between “Outbound Non-Unicast Pkts” sent locally or on the wire, because all outbound non-unicast packets are always sent to both the other local interfaces and also to the wire.

  To clear the AVIO statistics, use the `-Z` command option.

- The `hpvmcreate`, `hpvmclone`, and `hpvmmodify` commands have been changed to support the addition, modification, and deletion of AVIO LAN and storage devices.
- The `hpvmstatus` command now displays the new AVIO adapter types.
- The *hpvmresources* manpage, which describes the syntax for specifying storage and network devices when creating or modifying a guest, has been updated to include a description of the `avio_lan` and `avio_stor` options.
- The `hpvmmodify`, `hpvmcreate`, and `hpvmclone` commands now include the `-x sched_preference` option for specifying either Cell Local Memory (CLM), Interleaved Memory (ILM), or None.

NOTE: The use of cell local memory on Integrity Virtual Machine hosts is an experimental feature for this release. In general, you should see performance improvement by using cell local memory when running on cell based systems. If you encounter performance issues with this feature, you should revert back to using 100% interleaved memory.

1.5 Using the IGNOREWWID=YES Attribute

Use the IGNOREWWID=Yes attribute as a work-around if you have a disk that produces Wordwide-ID (WWID) values with which Integrity VM device management has a problem (for example, it causes an Integrity VM device database corruption.). The device WWID is the last field stored and displayed for a device entry in the device database.

Specifying this attribute sets the WWID to WWID_NUL and forces the Integrity VM device management utilities to ignore the WWID field and not do WWID field checking. For example:

```
# hpvmdevmgmt -m gdev:/someguestdevice:attr:IGNOREWWID=YES
```

NOTE: If you specify IGNOREWWID=YES, use only one path of a multipath device; otherwise, serious device and guest conflicts might occur.

1.6 Specifying Memory Type

For those sites that must configure the host with CLM, Integrity VM selects the best available pool at boot time. If your application performance benefits from ILM or CLM, you can make note of that preference. If cell is chosen, the cell with the most CPU and memory space is selected. When the guest is active, the scheduler optimizes where the guest runs, so that it can be closest to its memory.

Databases with high I/O can benefit from this model. Guests that are larger than any single cell, and some highly threaded applications, should be placed in *ilm*. If your application is predominantly CPU bound, either model should perform the same. Therefore, you can leave it as the default preference of *none*. The selection is called a preference, because if there is only one type of memory left, Integrity VM determines the type of memory that will enable your guest to boot. If you do not know which model is better for your application; boot with one setting, measure performance, reboot with the opposite setting, and re-measure with the same test. If there is no difference, then set the preference back to *none*.

The `hpvmstatus` command shows the general preference you selected for guests that are down, and the actual cell number selection for booted guests.

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 1-1 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 1-1 Guest Management Software Kit Locations

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

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.03.50 is supported on HP Integrity servers or nPartitions running HP-UX 11i v2 (December 2007 0712 or later). 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 might also start, depending on the setting of the guest boot attribute.

NOTE: Version 3.5 of Integrity Virtual Machines requires the installation of both the HostAVIOStor and HostAvioLan bundles. Other Integrity Virtual Machines documentation may state this requirement is optional, but it is not.

For complete information about the requirements for installing Integrity VM, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration* manual.

2.1.1 Install these Patches

Install the following patches, from the ITRC website (http://www.itrc.hp.com), after installing Integrity VM:

- PHSS_37312 (Integrity VM)
- PHSS_37306 (VMagent)

Go to the http://software.hp.com and search for the keywords HPVM AVIO, to download and install any AVIO web release bundles.

NOTE: Although the installation order does not matter, Integrity VM patches and AVIO web release bundles cannot be installed using a single `swinstall` command.

2.1.2 Do not install Integrity VM V3.5 Kit on a Host Prior to HP–UX 0712

The HP Integrity VM Version 3.5 kit can be installed only onto an HP–UX 11i v2 0712 host. You must upgrade to 0712 before you upgrade to the current version of Integrity VM. Any attempt to install the Integrity VM Version 3.5 kit onto a host running any HP-UX system prior to 0712 does the following:

- Leaves the host in an unknown state.
- Installs the Integrity VM Version 3.5 T2767AC.VMCONVERT product, VMGuestLib, and VMKernelSW bundles onto the host.
- Reboots the host.

The `swlist` command also shows the Integrity VM Version 3.5 bundles T2767AC, VMGuestLib and VMKernelSW as installed after the host reboot. However, the Integrity VM Version 3.5 product does not install completely and can leave the host in an unknown state.

2.1.3 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.

2.1.4 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 to install VM Provider and VM Manager.

2.1.5 Installing the Migration Tools Including `hpvmmigrate` and Physical-to-Virtual Assist Tools

The VMMigrate SD-UX bundle no longer exists. The functionality delivered with this bundle is now delivered with installation of the Integrity VM bundle T2767AC. Installation of T2767AC causes the old VMMigrate bundle to be automatically removed. The functionality previously delivered with the VMMigrate bundle has been replaced by the contents of two SD-UX products within the T2767AC bundle, VMMIGRATE and VMCONVERT. The VMMIGRATE product contains the `hpvmmigrate` command along with its supporting tools and manual. The physical-to-virtual tools and documentation are delivered in the VMCONVERT product. These SD-UX products and others can be seen with the swlist command:

```
swlist -R T2767AC
```

The repackaging of the physical-to-virtual tools in the T2767AC.VMCONVERT product, allows them to be installed on any Integrity HP-UX 11i v2 system, not just on a VM Host or a virtual machine. This results in more practical use of the physical-to-virtual tooks enabling them on physical Integrity servers, vPars, nPars, and so on.

To install the physical-to-virtual tools on an Integrity HP-UX 11i v2 system, enter the following command:

```
# swinstall -s path to Integrity VM install media T2767AC.VMCONVERT
```

This installs only the physical-to-virtual tools without any of the other Integrity VM functionality.

NOTE: Be sure to completely specify T2767AC.VMCONVERT, so that you do not accidentally transform your host to a VM Host that is left in an unknown state.

2.1.6 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, see Section 4.2.1 (page 38):

If you install the VMProvider 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
```

2.1.7 VMMGR V3.0 Does Not Support Integrity VM V3.5 AVIO Functionality

Integrity Virtual Machine Manager Version 3.0 and earlier versions do not support AVIO functionality. You can use Integrity VM Manager to view and manage virtual machines with the following restrictions:

- When creating or modifying a virtual machine, you can add only VIO storage or network devices from Integrity VM Manager. To add an AVIO device or change an existing device from VIO to AVIO, use the hpvmmodify(1M) command after the VM has been created.
- There is no indication on any screen whether a particular virtual I/O device, virtual switch, or physical device supports AVIO, with one exception. On the VM Host and VM properties network tabs, AVIO virtual network interfaces appear with the numeral "14" replacing the word "LAN" in the first line of the box representing the virtual network interface.
- If a virtual machine contains an AVIO storage device, displaying the VM Host or VM Properties storage tab results in a stack trace. If you want to use AVIO storage devices with Integrity VM Manager Version 3.0, consult HP technical support for a fix for this issue. After the issue has been fixed, AVIO virtual storage devices will appear with the annotation "Unknown Storage Adapter" instead of "SCSI".

2.1.8 VxVM Device Path Not Valid Error on HP-UX 0803

Installing or updating HP-UX 0803 might result in the following VxVM error:

```
NOTICE: VxVM vxdmp V-5-0-34 added disk array OTHER_DISKS, datype = OTHER_DISKS

VxVM vxdisk ERROR V-5-1-5433 Device disk1_p2: init failed:
        Device path not valid
       * smapi listener returned "ACTION_FAILURE" for message "CREATE_GROUP"
        The configuration process has incurred an error, would you like
        to push a shell for debugging purposes? (y/[n]):
```

This error is caused by a 32–byte VxVM length limitation on disk device ID information. Integrity VM virtual disks report back a standard T10 device ID created with the 8–byte T10 HP identifier followed by a null terminated string of the backing store name. For example, the resource statement, `"disk:scsi::lv:/dev/vx/rdsk/lvrackA/disk1"`, results in the T10 device ID, `"HP /dev/vx/rdsk/lvrackA/disk1"`. Therefore, to avoid this error, the length of the backing store name must not exceed 23 characters.

2.1.9 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.01.00 and later. For patches required for earlier versions of Integrity VM, consult the *Release Notes* document for that version. For the most up-to-date patch list, see the HP ITRC website: http://www.itrc.hp.com.

Table 2-1 VM Host Patches

Affected HP-UX (VM Host) Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11i v2 0505 through 0509	A.01.20 or later	PHKL_33052 (11.23.0512)	FSS	This patch incorporated into 0512 update.
11i v2 0505 through 0606	A.01.20 or later	PHKL_34082 (11.23.0609)	Bug fix	Resolves panic on host.

Table 2-1 VM Host Patches *(continued)*

Affected HP-UX (VM Host) Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11i v2 0512 or later	A.02.00 or later	PHNE_33724 (11.23.0706)	Bug fix	Fixes a problem of a panic on the VM Host. Likely only on Integrity VM V2.0 as HP-UX guests in V1.0 do not do what the Windows guests do in V2.0 (ping the guest).
11i v2 0505 or later	A.02.00 or later	PHNE_34474	Bug fix	Required when using linkloop over VLANs between guest and VM Host VLAN.
11i v2 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 files when under extreme load. Download HP WBEM Services for HP-UX Product Bundle B8465BA from the HP software depot.
11i v2 0505 thru 0606	A.02.00 or later	PHKL_33604 (11.23.0609) PHKL_33605 (11.23.0609)	FSS	Must install PHKL_33605 before PHKL_33604.
11i v2 0512 thru 0606	A.01.00 or later	PHKL_33827 (11.23.0609)	Bug fix	Resolves panic on guest. Specific to EVA8000 environment. (corrected to be Host patch, not guest)
11i v2 0505 or later	A.01.00 or later	PHKL_34278	Bug fix	Resolves panic and system hang symptoms
11i v2 0505 or later	A.01.00 or later	PHNE_35182	Bug fix	Cumulative ARPA transport patch, resolves panic. Requires prerequisite PHNE_32277.
11i v2 Intel Itanium 9000 (Montecito)	A.01.20 or later	HPVM A.02.00 11.23.0609 HWE	Montecito HW support	HPVM V2.0 or later is strongly recommended for use with Intel Itanium 9000-based systems. See the support statement at: http://wtec.cup.hp.com.

Table 2-1 VM Host Patches *(continued)*

Affected HP-UX (VM Host) Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11i v2 0505 or later	A.01.20 or later	PHSS_35863 (Serviceguard A.11.16) PHSS_35427 (Serviceguard A.11.17)	Bug fix	Specific to Serviceguard. If Serviceguard is running on a node with only one CPU, threads can get blocked, and the node will TOC. This happens only on nodes with a single CPU and pthreads patch installed (PHCO_34944, or later). Nodes with more than 1 CPU will not see this problem.
11i v2 0706 or later	A.03.00	PHSS_36737	Bug fix	Dynamic memory expansion might fail on guest running on 11.23.0706 host.
11i v2 0505 to 0706	A.03.50	PHNE_36839	Bug fix	DLPI is modified to pre-enable network performance enhancements.
11i v2 0712	A.03.50	PHSS_37312	Bug fix	Mandatory Integrity VM patch
11i v2 0712	A.03.50	PHSS_37306	Bug fix	Mandatory Integrity VM patch
11i v2 0505 or later	A.03.00 or later	PHSS_36997 (Serviceguard A.11.18)	Bug fix	Serviceguard support for 11i v2.
11i v2 0712	A.03.50	PHSS_37845	Bug fix	Enables users to create Red Hat 4.6 guests.

Table 2-2 Do Not Install Product or Patch

Affected HP-UX Host Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11i v2 0505 or later	A.02.00 or later	PHNE_35793	igelan patch	An Integrity VM guest that uses a virtual interface that belongs to an IGELAN interface configured on the Integrity VM host can experience hangs with network services like ping, NFS, rcp, ftp for data transfers that use full-sized frames.

2.1.10 Patches Required in the HP-UX Guest

Table 2-3 lists the patches that are required in HP-UX guests:

Table 2-3 HP-UX Guest Patches

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
11i v2 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.
11i v2 0505 or later	A.01.00 or later	PHKL_34278	Bug fix	Resolves panic and system hang symptoms.
11i v2 0505 through 0606	A.01.00 or later	PHKL_34589 (11.23.0609)	Bug fix	Resolves panic on guest.
11i v2 0505 or later	A.01.20 or later	PHKL_34540 (11.23.0609 HWE) PHKL_34336 (11.23.0606) PHKL_34928 (11.23.0609)	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 might not detect guest is idle and not share resources, heavily impacting performance.
11i v2 0505 through 0606	A.01.00 or later	PHKL_33823 (11.23.0609)	Bug fix	Resolves panic on guest.
11i v2 0505 or later	A.02.00 or later	PHSS_34760	Serviceguard Monitor fix	Required for running in Serviceguard 11.16 environment.
11i v2 0505 or later	A.02.00 or later	PHSS_34337	Serviceguard Monitor fix	Required for running in Serviceguard 11.17 environment.
11i v2 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.
11i v2 0505 or later	A.01.00 or later	PHNE_35182	Bug fix	Cumulative ARPA transport patch, resolves panic. Requires prerequisite PHNE_32277.

11i v2 Intel Itanium 9000 (Montecito)	A.01.20 or later	HPVM A.02.00 11.23.0609 HWE	Intel Itanium 9000 hardware support	Integrity VM V2.0 or later is strongly recommended for use with Intel Itanium 9000-based systems. See the support statement at http://wtec.cup.hp.com/
11i v2 0505 or later	A.01.20 or later	PHSS_35863 (Serviceguard A.11.16) PHSS_35427 (Serviceguard A.11.17)	Bug fix	Specific to Serviceguard. If Serviceguard is running on a node with only one CPU, threads can get blocked, and the node will TOC. This happens only on nodes with a single CPU and pthreads patch installed (PHCO_34944, or later). Nodes with more than 1 CPU will not see this problem.
11i v3	A.03.00	PHKL_36261 PHKL_36242	Bug fix performance	Without these patches, 11i v3 guest performance is severely impacted when running applications that continually spawn a large number of short-lived processes (that is, a software build environment).
11i v2 0505 or later	A.03.00	PHSS_36997 (Serviceguard A.11.18)	Bug fix	Serviceguard 11.18 support for 11i v2.
11i v3	A.03.00	PHSS_36998 (Serviceguard A.11.18)	Bug fix	Serviceguard 11.18 support for 11i v3.
11i v2 0505 or later	A.03.50	PHNE_35765	Bug fix	Fixes NAT consumption panic.
11i v2 0505 through 0706	A.03.50	PHCO_37038 (11.23.0712)	Bug fix	Fixes `mkboot` command with AVIO.
11i v2 0505 or later	A.03.50	PHCO_36563	Bug fix	SAM-NNC support in the guest for Integrity VM V3.5 AVIO support.
11i v3 0703	A.03.50	PHKL_36009 (11.31.0709)	Bug fix	Fixes panic caused by failure to allocate alias page table entry.
11i v2 0505 through 0706	A.03.50	PHKL_37091 (11.23.0712)	Bug fix	Fixes EFI bootpath with AVIO.
11i v3	A.03.50	PHSS_37843	Bug fix	

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

Table 2-4 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 2-4 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 11i v2 0505 or later	A.01.00 A.01.20	PHKL_33361	Cumulative kernel SCSI patch	Resolved in Integrity VM A.02.00 and later.
HP–UX 11i v2 0505 or later	A.01.00 A.01.20 A.02.00	PHKL_35739 PHKL_35891	VxVM 4.1 Kernel Patch 04 or 05	Installing VxVM 4.1 Kernel Patch 04 onto HP-UX 11i v2 guest with VxVM boot disk results in an unbootable system. Resolved in Integrity VM V3.0.

2.1.11 Patches Required for Ignite/UX Servers

Table 2-5 lists the patches that are required in the Ignite/UX server:

Table 2-5 Ignite/UX Patches

Affected OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
HP-UX 11.00	A.01.00 or later	PHNE_25355	tftpd	
HP-UX 11.11	A.01.00 or later	PHNE_32825	tftpd	

2.1.12 Patches Required for Windows Guests

Table 2-6 lists the patches that are required in the guests.

Table 2-6 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 2-7 lists patches and products that you should not install on Windows guests.

Table 2-7 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 Intel Itanium 9000 (Montecito)	A.02.00 or later	PalHalLightRegEdit component	Idle detection	See Section 4.1.5: "PalHalLight RegEdit Patch Should Not be Installed" (page 35)

2.1.13 Patches Required for Red Hat Linux Guests

Table 2-8 lists the patches that are required in the guests.

Table 2-8 Red Hat Linux Patches

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
RHEL4U4 through U5	A.03.00 or later	SGLX_00190 (Serviceguard or Linux A.11.18.02)	Bug fix	Serviceguard on Linux SG A.11.18.02

2.1.14 Patches Required for SUSE Enterprise Linux Guests

Table 2-9 lists the patches that are required in the guests.

Table 2-9 SUSE Enterprise Linux Guests

Affected Guest OS and Version	Affected Integrity VM Version	Fix	Description/Impact	Comment
SLES10U1	A.03.50	SGLX_00196 (Serviceguard or Linux A.11.18)	Bug fix	Serviceguard on Linux SG A.11.18.02

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 vmProvider
    ```

  - 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 VMProvider bundle is to be installed or upgraded, specify it when you install the new version of Integrity VM, or install it 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.03.50     Integrity VM
  VMGuestLib            A.03.50     Integrity VM Guest Support Libraries
  VMKernelSW            A.02.50     Integrity VM Kernel Software
  VMProvider            A.03.50     WBEM Provider for Integrity VM
```

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

- The VMMigrate bundle shipped in earlier versions of Integrity VM has been merged into the T2767AC bundle and is installed or upgraded when T2767AC is installed.
- 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
# 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 backup solutions for VM Host and guest backups**

  Backup solutions such as HP Data Protector or Veritas NetBackup can be used on both the VM Host system and the guest systems. Consult the support matrix of such products for supported versions. Install the backup (client) agents on the VM Host and the guests. HP highly recommends that the /var and /opt directories, in addition to the standard locations, be backed up regularly on the VM Host system. Do not use the VM Host system as a backup server. For more information, see the *HP-UX 11i Installation and Update Guide* corresponding to the target operating system.

- **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, see *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 27).
  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.
  ```

NOTE: You can use WLM on the VM Host, but only to manage iCAP resources. gWLM is the workload management solution for managing resource allocation to virtual machines.

- **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 might become unbootable if the VM Host is restarted as a Windows system.

2.7 Trunking Software

Trunking software such as HP Auto Port Aggregation (APA) is supported only on the VM Host and not on the guest.

2.8 Using EMC PowerPath with AVIO and VIO

AVIO and VIO have been tested with the EMC PowerPath product. Note, direct support-related questions on the use of EMC PowerPath with Integrity VM to the EMC Corporation.

3 Creating Virtual Machines

This chapter 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[1]	1 GB	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

1 The minimum memory requirement for HP-UX 11i v2 is 512 MB. The minimum memory requirement for HP-UX 11i v3 is 1 GB (see "System Requirements" section in the *HP-UX 11i v3 Installation and Update Guide*); however, the *HP-UX 11i v3 Installation and Update Guide* warns that cold installations with 1 GB or less memory might fail or take a long time to complete. Therefore, 2 GB is recommended for cold installations of HP-UX 11i v3.

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

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 can 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, see the *Ignite-UX Administration Guide*.

3.5 Golden Images of Systems with HPVM-Guest Installed Must have HPVM Device Drivers Configured

Golden images of systems with HPVM-Guest bundle installed must explicitly configure the dynamic memory device driver. If your golden system has the HPVM-Guest bundle installed, be sure the dynamic memory device driver is configured correctly in the associated golden image's configuration file. To achieve this, add the line

```
set_kernel += “module hpvmdynmem loaded”
```

after the “init_sw_sel” stanza in the golden image's configuration file. Failure to do so might render the dynamic memory control inoperable when the golden image is installed on a virtual machine.

3.6 Numbers Reported by Glance 4.6 or above Running on VM Host Might be Incorrect

Glance 4.6 or above running on a VM Host might report incorrect values (for example, vCPU utilization is distorted and guest memory size is reported as being zero.). This is a warning, not a performance problem.

3.7 Interleaved Memory on Cellular Hosts

HP recommends that you use only interleaved memory (ILM) on cellular hosts instead of using cell local memory (CLM). When ILM is set too low on a CLM system, guests can fail to start. Furthermore, a guest is not guaranteed to be placed on the same cell where its memory was allocated, thereby, degrading performance. If your site requires CLM, contact HP Field Support for possible alternatives.

3.8 hpvmcreate Manpage Incorrect

The `hpvmcreate` manpage incorrectly states that the default behavior for the `-B` *`start-attr`* option is `auto`. This is incorrect. The default behavior is `manual`.

3.9 hpvmstop Manpage Incorrect

The `hpvmstop` manpage incorrectly states that the `-g` option is the default behavior when in fact the `-h` option is the default.

3.10 New option for hpvmstatus Command

The user can now determine whether the VM Host and guests use Cell Local Memory (CLM) interleaved Memory (ILM) with the `hpvmstatus -C` option. The `hpvmstatus -C` command provides a list of guests with their memory type.

If you do not use CLM at all, then all the guests use Interleaved Memory (ILM). If however, CLM is set, every hpvmstart command checks whether Integrity VM chooses cell or interleaved for this particular guest, and if cell is chosen, which cell it is. For example, you have an 8 GB VM Host configured with 75 percent CLM and 25 percent ILM. With two cells, each contributes 3 GB to cell local and 1 GB to interleaved. On boot, the operating system takes 1 GB of the interleaved memory. If each guest takes 1 GB to start, the breakdown looks like this:

- guest 1: cell 0 (2 GB CLM left)
- guest 2: cell 1 (2 GB CLM left)
- guest 3: cell 0 (1 GB CLM left)
- guest 4: cell 1 (1 GB CLM left)
- guest 5: cell 0 (no CLM left)
- guest 6: cell 1 (no CLM left)
- guest 7: interleaved (no memory left at all)

3.11 The `hpvmstatus` Display Can Lag in a Serviceguard Cluster

When Integrity VM guests are configured as packages in a Serviceguard (SG) cluster, the `hpvmstatus` command displays which VM Host is running the distributed guest as an SG package. This information comes from SG and can be delayed by as much as 10 seconds. This delay does not cause any risk of starting the same guest on two different Integrity VM Hosts, because SG is controlling the start of these guests and will allow only a single instance to run at any time.

4 Installing Guests

This chapter describes notes pertaining to installing guest software on the virtual machines.

4.1 Windows Guests

The following sections contain 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 Network Driver for Some Windows Guests Not Behaving Correctly

The network driver for some Windows guests is not behaving correctly if the network device is configured at PCI bus 0, device 3, function 1, because of an interaction with the console device at PCI bus 0, device 3, function 0. To avoid this issue, do not specify PCI bus 0, device 3 as an address when adding network devices to a Windows virtual machine.

There is no issue if `hpvmcreate` or `hpvmmodify` automatically assign PCI addresses. This problem can be corrected by removing any network devices at PCI bus 0, device 3 and adding them at any other free PCI address.

4.1.3 Virtual DVD Misconfiguration can Lead to Windows Slow Down

Windows 2003 Server constantly polls the status of a DVD. If you configure the virtual DVD incorrectly, such as inserting a blank DVD as a backing store, the virtual DVD disappears from the Guest. However, the Windows 2003 Server Guest continues to scan for the DVD to come back. This scanning activity can cause a slow down in Windows performance. Bad DVD configurations are reported in the /var/opt/hpvm/common/hpvm_mon_log, like the following:

```
9   ScsiDiskOpen: block open failed dev=1f000000 cdev=bc000000 errno=16
9   DVD dev 0xbc000000 may be empty
```

You can correct this error by first placing the virtual DVD into ejection state (vMP> ej) and then replacing the media in the VM Host CD or DVD drive with a readable disc.

4.1.4 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.

4.1.5 PalHalLight RegEdit Patch Should Not be Installed

Do not install the PalHalLightRegEdit patch, and if you have already installed it, remove it from Integrity VM Windows 2003 guests. To remove the `PalHalLightRegEdit` patch, go to **Add/Remove Programs** and remove the `PalHalLightRegEdit` component. You must reboot the system for the change to take effect.

4.1.6 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/rdsk/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.

4.1.7 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.

4.1.8 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.

4.1.9 Poor Console Screen Formatting

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

4.1.10 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.

4.1.11 Do Not Delete EFI Shell Boot Option

Do not delete the `EFI Shell [Built-in]` EFI Boot Manager option. Deleting this option might 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.

4.1.12 Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL — 1

If the footprint on the guest console looks like the following text, then this is a known problem with the Microsoft Windows 2003 Server SPx code base.

```
*** STOP: 0x0000000A
  (0x00000000000003E8, 0x000000000000000C, 0x0000000000000000, 0xXXXXXXXXXXXXX)
```

We are investigating possible workarounds for this problem. If this bug check continues to occur, try reducing or adding virtual CPUs or changing another configuration parameter temporarily.

4.1.13 Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL — 12

If the footprint on the guest console looks like the following text, then this is a known problem with the Microsoft Windows 2003 Server SPx code base.

```
*** STOP: 0x0000000A
  (0x0000000000000010, 0x0000000000000002, 0x0000000000000000, 0xXXXXXXXXXXXXX)
```

There is a patch available from Microsoft (4.6 QFE) to resolve this issue.

4.1.14 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 used 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 `Boot`*`xxxx`* 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\Boot*xxxx*

4.2 HP-UX Guests

The following sections contain release notes specific to installing HP-UX guests.

4.2.1 Installing the Guest Management Software

The guest management software is required on each guest. The guest management software ensures that guests have the required patches for optimum performance and manageability. It enables the `hpvmcollect` and `hpvminfo` commands on the guest.

The guest management software is stored on the VM Host system in the `/opt/hpvm/guest-images` directory. A subdirectory contains the guest management software for each type of guest operating system, as shown in the following example:

```
# cd /opt/hpvm/guest-images
# ls
common   hpux    linux   windows
```

To install guest management software on an HP-UX guest, select the appropriate version of HP-UX:

- 11iv2 indicates HP-UX 11.23.

  For HP-UX 11i v2 guests, the guest depot file:

  `/opt/hpvm/guest-images/hp-ux/11iv2/hpvm_guest_depot.11iv2.sd`

- 11iv3 indicates HP-UX 11.31.

  For HP-UX 11i v3 guests, the guest depot file is:

  `/opt/hpvm/guest-images/hpux/11iv3/hpvm_guest_depot.11iv3.sd`

Before installing the guest kit (bundle HPVM-Guest), preview the install task allowing the installation analysis. This provides the opportunity to identify and address any warnings that might result from this preview before proceeding with the installation. For example, the analysis phase includes checks for installation of the appropriate AVIO drivers on the guest. To preview the installation, use the `-p` option of `swinstall` as shown in the following example:

`swinstall -p -x autoreboot=true -s` *`path to hpvm_guest_depot.11iv#.sd`* `HPVM-Guest vmProvider`

You might see the following warning on an Integrity VM guest installed on an HP-UX 11i v2 prior to December 2007:

```
WARNING: Recommended bundle GUESTAVIOLAN not installed on guest.
WARNING: Recommended bundle GUESTAVIOSTOR not installed on guest.
WARNING: The "checkinstall" script for "vmTools.VMTOOLS-RUN" had a
         warning (exit code "2"0. The script location was
         "/var/tmp/BAAa05960/catalog/vmTools/VMTOOLS-RUN/chekinstall".
       * This script had warnings but the execution of this fileset
         will still proceed.  Check the above output from the script
         for further details.
```

If the HPVM-Guest bundle is not installed in the guest, the `/etc/rc.log` file will record:

```
"/sbin/rc3.d/S829hpvmguestlib start" FAILED
```

Depending on the version of VMGuestLib installed on the guest, the text of the failure will be one of the following:

- ```
  Start HP Virtual Machine Guest Libraries
  Output from "/sbin/rc3.d/S829hpvmguestlib start":
  WARNING: The HPVM-Guest software is not installed on this VM.
     Overall system performance may not be optimal.
  "/sbin/rc3.d/S829hpvmguestlib start" FAILED
  ```

- ```
  Start HP Virtual Machine Guest Libraries
  Output from "/sbin/rc3.d/S829hpvmguestlib start":
  WARNING: The software is not installed on this VM.
  ```

```
      Overall system performance may not be optimal.
   "/sbin/rc3.d/S829hpvmguestlib start" FAILED
```

This issue can be corrected by installing the HPVM-Guest bundle.

4.2.2 HP-UX 11i v3 Guests Might Fail to Configure Interface Cards Due to Lack of Memory Resources

HP-UX 11i v3 guests with small memory resources (less or equal to 2 GB RAM) might fail to configure one or more virtual interface cards. Messages like the following might be seen on the guest console:

```
wsio_claim init failed isc=0xe000000109c41400 name=mpt or
igssn: The device at hardware path 0/0/1/0 failed initialization (3309).
```

The problem might occur during installation, in which case it results in some devices not being seen by the guest.

To resolve this problem, temporarily increase memory assigned to the guest to more than 2 GB (for example 2.5 GB). Then reduce memory back to the intended size after you reboot the guest.

4.2.3 Patches for HP-UX 11i v3 Guests

Customers running HP-UX 11i v3 guests should install the following patches (or their superseding patches) in each guest running HP-UX 11i v3 :

- 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.

4.2.4 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 `ktracer` inside a guest. Under rare circumstances, these tools cause the guest to panic.

4.2.5 Do Not Use the `iomap(7)` Mechanism on HP-UX Guests

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

4.2.6 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` can 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 SLES10 SP1 Guests Supported on Integrity Servers

SLES10 SP1 guests are supported on all Integrity servers except the following:

- HP Integrity rx1600 server
- HP Integrity rx2600 server
- HP Integrity rx5600 server

4.3.2 Before Installing the SUSE Linux Guest

You must install the tog-pegasus RPM kit prior to installing the SUSE Linux RPM guest; however, the SUSE Linux installation media does not contain the tog-pegasus RPM kit. This RPM kit is available in the "HP Integrity Essentials Foundation Pack for Linux" (also known as HPIEFL for Linux).

The SUSE Linux RPM guest kit is actually two parts, a guest kit and a provider kit. The Hpvm.*.rpm kit contains:

- Tuning scripts
- hpvminfo
- hpvmcollect
- Guest library

The Hpvmprovider.*.rpm kit contains the VMprovider and related files. This RPM requires that both the hpvm and tog-pegasus kits must be installed.

http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T2387AA

The information you need is provided in Chapter 5 of the *HP Integrity Essentials Foundation Pack for Linux User's Guide*.

To download the HPIEFL for Linux kit, click the link http://www.hp.com/go/integritylinuxessentials listed in Chapter 5, then click *Download for HP Integrity Essentials Foundation Pack for Linux* link on this website.

4.3.3 Installing Linux Guest Management Software for the First Time

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

```
=== from /var/log/messages file ===
Jan 18 22:45:00 1sn000 kernel: ipmi_si: Error clearing flags: cl

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

You can ignore this error message.

4.3.4 ACPI Warnings, Errors, and Exceptions Displayed when SUSE Guest Booted

When an installed SUSE guest is booted, messages similar to the following are displayed on the guest's console:

```
Loading processor
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI idfor the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
  ACPI Error (acpi_processor-0500): Invalid PBLK length [0] [20060127]
  .
  .
  .
  ACPI Warning (acpi_processor-0555): BIOS reporting wrong ACPI id for the processor [20060127]
  ACPI Exception (evxface-0538): AE_BAD_PARAMETER, Removing notify handler [20060127]
```

These warnings, errors, and exceptions occur because some optional elements are not provided by the Integrity VM ACPI table. These messages are printed because the SUSE startup/initialization code is trying to reference these optional elements, particularly for configured guest CPUs.

The messages do not impede the SUSE boot process; the boot/startup process completes. The only known side-effect of these messages is that there is an extra CPU created in the `/proc/acpi/processor` file system, which might lead to confusion as to the actual number of CPUs configured in the guest.

4.3.5 HP SIM CMS Cannot Connect to SLES10 over SSH

SSH password authentication is turned off by default in SLES10. In this default setting, HP SIM CMS cannot connect to the SUSE guest.

To enable password authentication for SSH, do the following:

1. Login to SUSE.
2. Edit the `/etc/ssh/sshd_config` file.
3. Set *passwordauthentication* value to yes.
4. Restart *sshd*.

For more information, see Secure Shell (SSH) in HP SIM 5.x, Troubleshooting section (page 31).

4.3.6 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 Red Hat Linux guest, see the *VSE Management Software Installation and Update Guide*.

NOTE: If using SUSE Linux SLES10 SP1 guests, install need the HP Integrity Essentials Foundation Pack for Linux (HPIEFPL) Version 2.1 kit or later to get an appropriate version of the Utilization Provider. To get the VMProvider for the SLES10 guest, install the HPIEFPL Version 2.2 kit or later or make sure you install the Integrity VM V3.5 guest kit. For more information about obtaining the Utilization Provider, see the HPIEFPL 2.2 Release Notes.

4.3.7 Linux Guests with FC Tapes Display Errors

MPT errors might 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
```

4.3.8 Disable IPv6 on Linux Guests

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

```
printk: 1 message suppressed
```

The `dmesg` command reports numerous `duplicate address detected!` messages on every IPv6 configured interface. These messages indicates an issue in the IPv6 DAD (Duplicate Address Detect) mechanism and are harmless. You can ignore them, or you can disable them by including the following line in the `/etc/modprobe.conf` file:

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

4.3.9 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.

4.3.10 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.

4.3.11 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/LogVo100
        append="console=tty0 console=ttyS0 rhgb quiet lpj=4000000
```

4.3.12 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.

4.3.13 Occasional Floating-Point Assist Fault Messages.

Occasional floating-point assist fault messages appear when running Mozilla. This problem also occurs o 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”.

4.3.14 TC INIT Dump Messages Do Not Appear on the SUSE Linux Guest Console

TC INIT dump messages do not appear in the SUSE Linux guest console running multi-CPUs. The `hpvmconsole` TC command normally causes INIT dump message to be displayed on the guest console. These messages do appear with the one-way SUSE Linux guest. However, these messages fail to appear with multi-CPUs SUSE Linux guest.

5 Using Integrity VM Commands

This chapter contains notes about the Integrity VM commands.

5.1 Accidental Use of `-R` Option with `hpvmmodify` Instead of `-r`

The `hpvmmodify` command supports two options related to guest memory configuration, `-r` and `-R`. Accidental confusion of one for the other might create undesired results with your guest configuration. For an explanation of these command options, see the hpvmmodify manpage.

The `-R` option, with the same meaning, is accepted by the `hpvmcreate` and `hpvmclone` commands, but use of the `-R` option with those commands is currently unsupported. Nevertheless, similar undesired results might occur with a similar mistaken use of `-R` for `-r` with those commands.

5.2 Changing Guest LAN from AVIO to VIO

When changing a guest LAN from AVIO to VIO, you must restart the vswitch that the LAN is on. Use the following commands:

```
hpvmnet -h -S switchname // for the vswitch associated with the LAN change
hpvmnet -b -S switchname
```

5.3 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.

5.4 The `hpvmdevmgmt` Command Truncates File Sizes

When you use the `-S` option on the `hpvmdevmgmt` 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 `hpvmdevmgmt -S 1G` command and the `hpvmdevmgmt -S 1.5G` command create a 1 GB file.

5.5 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 `hpvmdevmgmt` 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.

5.6 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.

5.7 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.

5.8 Missing `uuid` or `.vmid` Files

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

5.9 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.

5.10 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 might prevent the guest from booting.

5.11 Actual Running Entitlement Might 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%).

5.12 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.

5.13 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.

5.14 hpvmpubapi Manpage on Linux Guests

The `hpvmpubapi` manpage on Linux guests is missing the synopsis section. Go to the `hpvmpubapi` manpage on the VM Host to view the complete manpage.

5.15 Integrity VM Check Might Fail Because of Bad Switch

The Cisco switch for HP BladeSystem c-Class Server Blades has a protocol error that causes it to respond to every MAC address. Because MAC addresses are unique, Integrity VM checks that the generated guest virtual MAC address is unique. If one of these bad switches is on your network, Integrity VM's check will fail.

The `hpvmcreate` command might fail with messages like the following:

```
hpvmcreate:  WARNING (host): Failed after 3 attempts.
hpvmcreate:  WARNING (host): Unable to create Ethernet MAC Address.
```

Similarly, the `hpvmstart` command might fail with messages like the following:

```
# hpvmstart -P vm2
HPVM guest vm2 configuration problems:
Warning 1 on itme nic1: Guest MAC address for switch nic1 is in use.
```

Cisco Systems, Inc. released a fix for the Cisco Catalyst Blade Switch 3020 in December 2006, which is available from the Cisco Systems website:

http://cco.cisco.com

It is also available from the HP website:

http://www.hp.com

From the HP website, select Software & Driver downloads and search for switch cisco 3020. The minimum required firmware version is 12.2(35) SE.

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 might 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'" \
```

```
 -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 might 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 HP-UX 11i v3 Guests Might Panic with a NaT_hndler: kernel NaT Consumption Fault

Under certain situations, an HP-UX 11i v3 guest might panic with a `NaT_hndler: kernel NaT Consumption fault` when using Logical Volume Manager (LVM) software.

To avoid this situation, install the BaseLVM (B.11.31.0712) software from the HP-UX 11i v3 0712 AR media.

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, attach to the guest's virtual console using the `hpvmconsole` command, then 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 The hpvmsg_package Does Not Add Appropriate Entries

The `hpvmsg_package` does not add appropriate entries to the package configuration and control script files. After running the `/opt/cmcluster/toolkit/hpvmsg_package` script to package a guest that contains CVM or CFS backing stores, review and modify the package configuration and control scripts for each cluster member. As part of this process, add CVM and/or CFS backing store entries to these files.

The package configuration and control scripts can be found at: `/etc/cluster/`*`guest-name`*`/`

6.11.2 Using AVIO lan Device in a Serviceguard Configured Guest

When using AVIO networking devices for guests that are configured as Serviceguard Packages, be sure that all Serviceguard standby `lans` are configured using PPA devices supported by AVIO. Failure to do so causes network connectivity to be lost even if the standby link is up.

6.11.3 Required HP Serviceguard Patches

To use Serviceguard to manage HP-UX guests, make sure the required patches are installed. For more information, see Section 2.1.9 (page 21).

6.11.4 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.

6.11.5 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.

6.11.6 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.

6.11.7 Syslog Entries for `cmcld` Can Be Ignored

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

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

These messages can be ignored.

6.11.8 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.

6.12 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

```
# hpvmmodify -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 chapter contains notes about configuring networks for virtual machines.

7.1 Supported Adapters

Integrity VM supports only those adapters that are of Ethernet or the IEEE 802.3 CSMA/CD network. Note that AVIO interfaces are supported by a select set of Ethernet host NICs. For a list of the specific AVIO supported NICs, see the *HP Integrity Virtual Machines Installation, Configuration, and Administration A.03.50* manual.

7.2 Sufficient Memory for Guests with Virtual LAN Devices

If the guest is configured with a number of virtual LAN devices and the guest does not have sufficient memory, some of the devices could be missing after the guest is booted. To resolve this issue, increase the size of guest memory with the `hpvmmodify -r` command.

7.3 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.

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

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

7.5 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.

You can set the `HPVMMACADDRFRAMES` tunable to zero (0), which completely eliminates the MAC address verification. However, HP recommends that you do so only after you configure all of your guests and confirm that there are no conflicts with MAC addresses in your network environment.

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

7.6 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.

7.7 VM Manager Does Not Display APA Link Aggregate LAN Device

If a VM host system has an APA link aggregate LAN device that is composed of one or more APA link aggregate LAN devices, the VM Manager does not display this APA link aggregate as a possible backing LAN device in the VM dialog. To create a vswitch with this APA link aggregate, use `hpvmnet` CLI.

7.8 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.

7.9 Guest and Host Communication

Checksum offloading (CKO) is not supported. On most of the physical interfaces that are not of 10 Gigabyte type, CKO is turned off by default. Consult your interface card documentation for details.

Turning on CKO can cause host-to-guest connections as well as guest-to-host communication over a VLAN to fail. If you are receiving failures with host-to-guest connections or guest-to-host communication using a VLAN, ensure that the CKO is turned off in the host interface driver. If that does not fix the problem, reboot the vswitch.

To turn off the CKO 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 send_cko_off 4

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

7.10 Configuring vswitches to be Backed by a VLAN Interface on the VM Host is Not Supported

Do not use the `hpvmnet` command to create a virtual switch backed by a VLAN port on the VM Host. This configuration is not supported.

7.11 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
```

Note that this restriction applies to VIO interfaces.

7.12 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).
- You notice that there is no communication from an `avio_lan` interface to a `lan` interface after booting the guest(s) while the vswitch is down.

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.

7.13 Guest AVIO Interface Behavior

The following list describes the guest AVIO interface behavior when guest boots while vswitch is down or resetting:

- If you boot a guest while the vswitch is not up, AVIO interfaces associated with the vswitch might not be claimed in the guest. For example, this might occur if the guest is booted prior to booting the vswitch or if the corresponding network interface on the VM Host is not cabled. If you encounter this problem, first fix the vswitch state (that is, ensure that `hpvmnet` displays its state as Up), and then execute the `ioscan` command in the guest. These actions will claim the AVIO interfaces.
- After `ioscan` claims the AVIO devices in the guest, you might notice that the AVIO devices cannot communicate with another VIO guest interface configured on the same vswitch. When this occurs, invoke the `hpvmnet -r` option on the vswitch to restore connectivity.
- If the vswitch is in an unstable state while the guest is booting, guest AVIO interfaces might fail initialization and move to the DOWN state (as displayed by the`lanscan` command). When this occurs, first ensure that the vswitch enters a stable state , then reset the guest interface using `lanadmin`.

7.14 AVIO LAN Devices Not Claimed by Guest with DOWN Vswitch at Boot Time

In addition to running `ioscan`, you must re-run the necessary network startup scripts, so that IP addresses can be reconfigured on the network interface cards (NICs). For example:

```
/sbin/rc2.d/S340net start
/sbin/rc2.d/S340net-ipv6 start
```

7.15 Do Not Use TCP Software Packet Reassembly in IGSSN Driver

There have been problems with TCP Software Packet reassembly in the igssn driver in a guest HP-UX image. For this release, do not enable it on a guest. By default, software packet reassembly (known with acronyms as drv_pr for driver packet reassembly) is enabled in igssn in the guest.

To determine if drv_pr is enabled, an administrator can execute the following command:

```
lanadmin -x drv_pr ppa
```

where *ppa* is the Card instance # (Crd in#) from `lanscan`.

To manually disable drv_pr, and administrator can execute the following command:

```
lanadmin -X drv_pr_off ppa
```

To manually enable `drv_pr`, an administrator can execute the following command:

```
lanadmin -X drv_pr_on ppa
```

NOTE: These change are not carried over to subsequent reboots of the system. To maintain the configuration over reboots of the guest, the administrator must edit the guest file, `/etc/rc.config.d/hpigssnconf`.

For each igssn device that must have `drv_pr` disabled, you must construct a block of information in the `hpigssnconf` file. For example, if your guest needed to have both lan0 and lan3 disable `drv_pr`, you might have:

```
HP_IGSSN_INTERFACE_NAME[0]=lan0
HP_IGSSN_STATION_ADDRESS[0]=
HP_IGSSN_MTU[0]=
HP_IGSSN_DRV_PR[0]=0

HP_IGSSN_INTERFACE_NAME[3]=lan3
HP_IGSSN_STATION_ADDRESS[3]=
HP_IGSSN_MTU[3]=
HP_IGSSN_DRV_PR[3]=0
```

7.16 HP-UX 11i v3 Guest Might Fail to Configure AVIO Network Interfaces Due to Lack of Memory Resources

If any HP-UX 11i v3 guest AVIO network interfaces are not claimed when the guest boots, you can resolve this issue by giving the guest more memory, then rebooting it. If you encounter this issue and need all the AVIO interfaces, use this kernel tunable command to work around this issue:

```
kctune -B dma32_pool_size=8388608
```

Then reboot the guest.

7.17 Other Issues and Notes

The following list provides additional issues with the Integrity VM V3.5 release of which you should be aware :

- If you modify the MAC address of an interface in the guest, the hpvmstatus command in the VM Host does not display the current MAC address correctly. There is no fix or workaround for this problem at this time.
- Just as with physical devices on a network, for communication to occur uninterrupted between all stations on a LAN segment, the MTUs of all the systems on the LAN segment

or VLAN must match, whether they are physical systems or guests. The VM Host does not check for MTU mismatches for its guests.

- The `lanadmin` card specific options that are supported on igssn on the guest are:
  - `-x:speed,fctrl,cko,type,card_info,stats drv,vmtu,and drv_pr.`
  - `-X:drv_pr_on,drv_pr_off,stats clear`

8 Storage Information

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

8.1 Critical Issue Fixed in HostAVIOStor B.11.23.0803

A critical issue with AVIO DVD devices that caused guest installation failure on platforms that have USB DVD devices (for example, rx2660, rx3600, rx6600 and so forth), has been fixed.

8.2 USB 2.0 Now Supported

Integrity VM now supports the USB 2.0 driver on an HP-UX 11i v2 VM Host.

8.3 The sam Command might Display Incorrect Number of Disks and Paths on an HP-UX 11i v2 Guest

The number of disks display by the `sam` command using "Sam Areas->Disks and File Systems->Disk Devices" might be incorrect. The number of paths displayed for a device might also be incorrect. This problem exists on disks configured under both SCSI and AVIO storage adapters. `ioscan` displays all the disks correctly.

For example, the following are the `sam` output and the`ioscan` output on the same HP-UX 11i v2 guest:

```
"Disk Devices" window in sam(1M) shows the following disks and number of paths:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xDisk Devices                                                     0 of 8 selectedx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
x  Hardware      Number                 Volume      Total                        x
x  Path          of Paths   Use         Group      Mbytes   Description          x
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xx 0/0/2/0.0.0   2          VxFS/Swap   --          70007   HP      Virtual    x
xx 0/0/5/0.0.0   1          Unused      --          69504   HP      Virtual    x
xx 0/0/5/0.1.0   2          Unused      --          70007   HP      Virtual    x
xx 0/0/5/0.2.0   2          Unused      --          70007   HP      Virtual    x
xx 0/0/6/0.3.0   1          Unused      --          70007   HP      Virtual    x
xx 0/0/6/0.4.0   1          Unused      --          70007   HP      Virtual    x

 "ioscan -kfnC disk" shows the following disks:

Class     I  H/W Path     Driver  S/W State   H/W Type     Description
=====================================================================
disk     15  0/0/2/0.0.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c0t0d0     /dev/rdsk/c0t0d0
                         /dev/dsk/c0t0d0s1   /dev/rdsk/c0t0d0s1
                         /dev/dsk/c0t0d0s2   /dev/rdsk/c0t0d0s2
                         /dev/dsk/c0t0d0s3   /dev/rdsk/c0t0d0s3
disk     16  0/0/5/0.0.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c3t0d0     /dev/rdsk/c3t0d0
disk     18  0/0/5/0.1.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c3t1d0     /dev/rdsk/c3t1d0
disk     20  0/0/5/0.2.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c3t2d0     /dev/rdsk/c3t2d0
disk     17  0/0/6/0.0.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c4t0d0   /dev/rdsk/c4t0d0
disk     19  0/0/6/0.1.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c4t1d0   /dev/rdsk/c4t1d0
disk     21  0/0/6/0.2.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c4t2d0   /dev/rdsk/c4t2d0
disk     23  0/0/6/0.3.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c4t3d0   /dev/rdsk/c4t3d0
```

```
disk      25  0/0/6/0.4.0  sdisk   CLAIMED     DEVICE       HP      Virtual Disk
                         /dev/dsk/c4t4d0   /dev/rdsk/c4t4d0
```

Workaround: Use the System Management Homepage (SMH) to configure the devices.

8.4 AVIO Current Limitations

The following sections describe the current limitations using AVIO.

8.4.1 Modifying the Storage Adapter from `scsi` to `avio_stor`

If you attempt to modify a storage adapter from `scsi` to `avio_stor` on a port for a running guest, the `hpvmmodify` command allows the change, but the change lasts only until the next guest startup. In addition, the `hpvmnet` command displays incorrect port information for the currently running guest until the guest is stopped and restarted.

8.4.2 Virtual Device Types and Backing Store Support

The current release of the AVIO storage driver does not have support for all of the physical backing stores or virtual device types supported by the virtual SCSI adapter.

The following physical backing stores are not supported by the AVIO driver:

- Attach
- Disk Partitions

AVIO storage supports lv backing store devices (Virtual LvDisk) on HostAVIOStor B.11.23.0712.01 and later. VmVM logical volumes are not supported.

The following virtual device types are not supported by the AVIO driver:

- Tape
- Changer
- Burner

NOTE: The `hpvmstatus -V` command does not display ioscan format for AVIO devices.

A virtual machine can have up to 30 VIO devices or up to 128 AVIO devices total (the number of virtual and attached devices).

8.4.3 GuestAVIO Bundle not Installed but AVIO Storage Device is Configured

If the GuestAVIO bundle is not installed on the guest but you've configured an AVIO storage device, the AVIO Stor HBAs will not be claimed in the guest and the LUNs configured under the AVIO Stor HBAs will not be accessible. If the LUN is a boot disk, boot will fail with a panic indicating missing drivers.

8.4.4 Access of Disk Configured Under an AVIO Storage Adapter Might Take Longer than Expected

Access of a disk configured under an AVIO storage adapter might take up to 30 seconds on an HP-UX guest if there are errors on the backing store in the host. For example, when the backing store device is removed or not responding, an open of the disk device, configured under an AVIO storage adapter, from the Integrity VM guest might take up to 30 seconds. An application that tries to open an AVIO disk device might see a delay because of this. For example, the `diskinfo` command might fail after 30 seconds:

```
# time diskinfo /dev/rsdk/c1t14d0:
diskinfo: can't open /dev/rdsk/c1tl4d0: No such device or address
    real     0m30.26s
    user     0m0.00s
    sys      0m0.01s
```

This delay is caused by the retry of failed commands from the nonresponding backing store. There is currently no workaround.

8.4.5 I/O Resource Delete Using `hpvmmodify` Fails When Guest is at EFI

Devices configured under AVIO Stor HBA for a guest cannot be deleted (using the `hpvmmodify` command) if the guest is at EFI.

Workaround: Stop the guest using the `hpvmstop` command and retry the command.

8.4.6 Mapping AVIO Storage Devices

This section explains how to map an AVIO storage device on an HP-UX guest to an `hpvmstatus` display on the Integrity VM Host either at the EFI console or at the HP-UX operating system.

The following example shows the output of `hpvmstatus` from the Integrity VM Host:

```
# hpvmstatus -P aviotest
[Storage Interface Details]
Guest                                    Physical
Device  Adaptor    Bus Dev Ftn Tgt Lun Storage   Device
======= ========== === === === === === ========= ========================
disk    avio_stor    0   2   0  22   0 disk      /dev/rdsk/c82t15d3
```

The following statistics are displayed in this example:

- PciBus = 0
- PciDev = 2
- PciFtn = 0
- Addr (Target Id) = 22 (0x16)
- Lun = 0

Note that Addr (Target Id) is decimal in the `hpvmstatus` display, and PciFtn and Lun are always zero (0).

The Integrity VM guest EFI device path encodes PciBus, PciDev, and Addr (Target Id) from the `hpvmstatus` display:

```
                          PciDev
                             |
                             | PCIFtn
                  PciBus     | |       Addr(Target Id)
                     |       | |         |
                     V       V V         V
blk16 : Acpi(PNP0A03,0)/Pci(2|0)/Scsi(Pun16,Lun0)
```

PciFtn (PCI function) and Lun# are always zero (0). Addr (Target Id) becomes EFI Pun# and is displayed as a hexidecimal number.

The two methods for mapping an Integrity VM HP-UX guest hardware path or HP-UX Device Specific File (DSF) to an Integrity VM Host `hpvmstatus` display:

1. `-e` option of the `ioscan` utility

   `ioscan -fne` displays the HP-UX hardware path/DSF and the EFI device path for the device. The HP-UX hardware path encodes the following from the `hpvmstatus` display:

   - PciBus
   - PciDev
   - Addr (Target Id)

   Addr (Target Id) is encoded as an HP-UX tgt ID and an HP-UX lun ID in the HP-UX hardware path.

   HP-UX tgt ID and HP-UX lun ID are calculated from Addr (Target Id) in the `hpvmstatus` display using the following equations:

   ```
   HP-UX tgt ID = Addr(Target Id) % 16
   HP-UX lun ID = Addr(Target Id) / 16
   ```

Note the following example:

```
# ioscan -fne
                 PciDev
                    | PCIFtn
                    | |(Addr(Target Id) % 16) <-> HP-UX tgt ID
             PciBus | | |(Addr(Target Id) / 16) <-> HP-UX lun ID
                  | | | | |
                  V V V V V
disk       49  0/0/2/0.6.1   sdisk     CLAIMED     DEVICE       HP      Virtual Disk
                           /dev/dsk/c0t6d1   /dev/rdsk/c0t6d1
        Acpi(PNP0A03,0)/Pci(2|0)/Scsi(Pun16,Lun0)
                        ^      ^ ^          ^
                        |      | |          |
                     PciBus    | PCIFtn   Addr(Target Id)
                               |
                            PciDev
```

In this example, exp1 / exp2 represents the quotient from exp1 divided by exp2 (integer division), and exp1 % exp2 finds modulo of exp1 divided by exp2 (that is, finds the remainder of an integer division).

2. `get_info` option of the `gvsdmgr` utility

If you are using the HP-UX DSF, the following `gvsdmgr` option can be used to get the VSD LUN ID, which is the same as the Addr (Target Id) in the `hpvmstatus` display. The `gvsdmgr` utility displays VSD LUN Id as a hexidecimal number. The first nibble of VSD LUN Id becomes HP-UX lun ID, and the second nibble becomes HP-UX tgt ID. The following example shows the `get_info` option with the `gvdsmgr` utility:

```
# gvsdmgr get_info -D /dev/gvsd0 -q lun=/dev/rdsk/c0t6d1
Tue Oct  2 13:35:32 2007

Lun DSF                                                 : /dev/rdsk/c0t6d1
VSD LUN Id                                              : 0x16
Lun  Hardware path                                      : 0/0/2/0.6.1
LUN State                                               : UNOPENED
```

8.5 Crash Dump Collection Might Fail for HP-UX Guests with Attached I/O Devices

HP-UX guest OS crash might fail to save a crash dump with the following console message:

```
Error: can't open first dump device /dev/dsk/c0t0d0. Dump aborted.
INIT[0]: OS_INIT ends. Resetting the system
```

This problem is caused by the HP-UX MPT dump driver in the guest waiting only 1 second for a bus reset to finish. If there is an attached tape or changer sharing the same virtual MPT adapter as the guest boot disk, the reset time of that attached tape or changer might exceed the 1 second timeout, resulting in the error message above.

To avoid this problem on HP-UX 11i v2 0505–0706 or HP-UX 11i v3 guests, make sure the guest boot disk and any attached tape or changer do not share the same virtual MPT adapter. For information about how to specify bus and device numbers to place the tapes or changers on a separate MPT adapter than the guest boot disk, see the *hpvmresources* manpage or the *HP Integrity Virtual Machines Installation, Configuration, and Administration*.

For HP-UX 11i v2 0712, HP-UX 11i v3 0803, and all later supported HP-UX guest releases, make sure the HPVM-Guest depot is installed. The HPVM-Guest depot adjusts the MPT dump reset timeout allowing for tape and changers to be placed on the same virtual MPT adapter as the boot disk.

8.6 DMP Files Not Supported as Backing Stores

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

8.7 Assigning a Null Device to a Resource

When assigning a null device to a resource on a virtual machine, the file name serves as a placeholder. Therefore, if the file does not exist, you will not receive an error message. For example, the following command string will not produce an error message if the file XXXX.iso does not exist:

```
hpvmmodify -P vm1 -a "disk:scsi::null:/opt/XXXX.iso
```

8.8 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.

8.9 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.

8.10 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.

8.11 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 might 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.

8.12 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.

8.13 Physical Device `null` Assigned to Nonexistent Path

Devices with physical storage type `null` might 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.

8.14 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.

8.15 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.

8.16 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.

8.17 Installing Integrity VM Clears Secure Path 3.0F SP1 Settings

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

8.18 Secure Path and LVM Configurations

When using HP StorageWorks Secure Path 3.0F Service Pack 2 for HP-UX 11i v2, Integrity Virtual Machines Manager (VMMgr) versions 3.0 and earlier do not recognize the virtual device special files introduced in this version of Secure Path for use with Active-Active configurations. These virtual device special files are located in directory `/hpap`. While these virtual device special files can be used as backing devices for virtual disks in virtual machines, they are not displayed in the list of candidate backing devices by VMMgr when creating or adding storage to a VM.

When a VM contains a virtual disk backed by an `/hpap` device, the virtual disk will be displayed on the host view and VM view storage tabs. However, VMMgr is not able to map this device special file to the corresponding physical storage LUNs and, therefore, will display a question mark (?) icon inside the box representing the backing device for the virtual disk. It will also not be able to display any disk utilization data for the virtual disk backed by the `/hpap` device.

To add a virtual disk backed by a virtual device special file to a VM, use the `hpvmcreate` or `hpvmmodify` command line utility. You can also use the methods available in earlier versions of Secure Path, for example, use a path-dependent device special file name or use LVM to configure a logical volume, which can then be used as a backing device.

For more information about how to configure LVM with Secure Path, see the release notes and user documentation for HP StorageWorks Secure Path 3.0F Service Pack 2 for HP-UX.

8.19 AVIO Multipathing Support

The AVIO storage driver supports both Active-Active and Active-Passive firmware on EVA GL series (3000/5000) starting with HostAVIOStor B.11.23.0712.01. AVIO is now compatible with SCSI with respect to EVA support. The minimum Active-Passive firmware version recommended is VCS v3.110. The EVA XL series (4000/6000/8000) continues to support the Active-Active configuration. SecurePath Active-Passive is now supported in addition to Active-Active on AVIO. SecurePath can be used on both EVA XL and EVA GL.

8.20 The gvsdmgr Utility

The following pages contain the manpage description of the HP-UX `gvsdmgr` utility, which manages AVIO HBAs and provide `replace_dsk` functionality to guard against backing store changes in use by the guest.

gvsdmgr(1M)

NAME

gvsdmgr - A utility to manage HP-UX Mass Storage Core I/O cards or HBAs claimed by Integrity VM Guest AVIO Storage driver (gvsdmgr).

SYNOPSIS

```
Path: /opt/gvsd/bin
gvsdmgr [-h] [-f] bdr -D device_file -q lun={all | lun_def}
gvsdmgr [-h] clear_stat -D device_file
gvsdmgr [-h] clear_stat -D device_file -q all
gvsdmgr [-h] clear_stat -D device_file -q lun={all | lun_def}
gvsdmgr [-h] get_info -D device_file
gvsdmgr [-h] get_info -D device_file -q lun={all | lun_def}
gvsdmgr [-h] get_stat -D device_file
gvsdmgr [-h] get_stat -D device_file -q lun={all | lun_def}
gvsdmgr [-h] [-f] replace_dsk -D device_file -q lun=lun_def
```

DESCRIPTION

gvsdmgr is a diagnostic utility to be used for managing controllers claimed by the GVSD driver. This command provides the ability to retrieve various configuration information, issue Task Management commands, and read accumulated statistics of the controller and connected LUN devices.

gvsdmgr requires the use of a device file to indicate the interface over which the requested command needs to be performed

OPTIONS

gvsdmgr recognizes the following command-line options:

`-f` Displays a warning message before continuing the command.

`-h` Provides a brief description of what the command does.

`-q` Describes the command's qualifiers. A command is defined by a set of qualifiers that must be specified after the command name. Each qualifier is preceded by the `-q` option. Some qualifiers can take one or more values and are given as `-q qualifier_name`={x | y} where *`qualifier_name`* can take either the value x or y.

`-v` Provides verbose information.

COMMANDS

gvsdmgr recognizes the following commands. A command is defined by a set of qualifiers. Attributes are specified with the `-q` option. All keywords are case-sensitive.

- `bdr`

  The following qualifier must be specified with the `bdr` command:

  — `lun` — Resets the specified target device. This is a destructive operation. If the `-f` option is not specified with this command, gvsdmgr displays a warning message before continuing. Otherwise, it suppresses the warning message and executes the command.

- `clear_stat`

  The following qualifiers can be specified with the `clear_stat` command:

  — `all` — Clears all statistics for the Core I/O card / HBA and all LUNs.

  — `lun` — Clears statistics for a specific LUN or all LUNs.

  When the *`clear_stat`* command is run without qualifiers, it clears statistics of the Core I/O card / HBA represented by *`device_file`*.

- `get_info`

  The following qualifier can be specified with the get_info command:

  — `lun` — Shows lun information for a specific LUN or all LUNs.

  When the `get_info` command is run without qualifiers, it returns information about the Core I/O card / HBA represented by *`device_file`*.

- `get_stat`

  The following qualifier can be specified with the get_stat command:

  — `lun` — Shows statistics for a specific LUN or all LUNs.

  When the `get_stat` command is run without qualifiers, it shows statistics about the Core I/O card / HBA represented by *`device_file`*.

- `replace_disk`

  The following qualifier must be specified with the `replace_disk` command:

  — *`lun_def`* — Replaces the backing store device for a LUN with the backing store device found during last open. If the `-f` option is not specified, gvsdmgr displays a warning message before proceeding. Otherwise, it suppresses the warning message and executes the command.

The gvsdmgr utility requires superuser privilege for execution. For information about privileged access on systems that support fine-grained privileges, see the *privileges* manpage.

EXAMPLES

Display adapter information of the Core I/O card / HBA whose device file is `/dev/gvsd0`:

```
gvsdmgr get_info -D /dev/gvsd0
```

Display all LUN information of the Core I/O card / HBA whose device file is `/dev/gvsdo`:

```
gvsdmgr get_info -D /dev/gvsdo -q lun=all
```

Clear statistics for a LUN with device special file `/dev/rdsk/c0t2d2` of the Core I/O / HBA whose device file is `/dev/gvsd0`:

```
gvsdmgr clear_stat -D /dev/gvsd0 -q lun=/dev/rdsk/c0t2d2
```

AUTHOR

gvsdmgr was developed by HP.

8.21 Storage Driver not Listed in Installation Manual

Section 7.2.1.1 VM Storage Supportability, in the *HP Integrity VM Installation, Configuration, and Administration* manual is missing the FibrChanl-02 (Driver Name FCLP) driver in the list of supported drivers.

This driver will be added to the list the next time the manual is revised.

9 Migrating Virtual Machines

This chapter 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 chapter 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 `sl` 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.