Top Ten Tips for Using Integrity Virtual Machines

Introduction

For most people, the first time they use a new technology it is not used to its maximum potential. The same is true for Integrity Virtual Machines (Integrity VM). There are several things in a virtual machine (VM) environment that can, and often do, cause problems in three general areas:

- Performance – Poor performance of applications running on a VM
- Functionality – The OS running on the VM (guest OS) or virtual hardware functionality is missing or inoperable
- Reliability – The guest OS is sluggish or unstable.

This white paper outlines the ten most common issues in Integrity VM configurations that can lead to problems in the above categories. For each issue, the most likely symptoms will be listed using these categories (Performance, Functionality, Reliability).

The term 'VM Host' is used to refer to the physical Integrity server which has the Integrity VM software installed on it. A virtual machine (VM) runs on the 'VM Host.' A virtual machine, along with its OS is referred to as a 'guest.' Accordingly, the 'guest OS' is the operating system running on the VM.

#1 – Do Not Install OS using Golden Image of a VM Host

The Integrity VM Host system has the bundles T2767AC and VMKernelSW installed by definition. The presence of these bundles on a VM is not supported and may render the VM inoperable. Installation of these bundles on a VM is prevented by SD-UX, but they may still be present whenever the OS was installed using a golden image created with Ignite-UX tools.

Symptoms: Performance, Reliability

Applications running in the VM, especially those that are I/O intensive, perform very poorly. The guest OS may crash or appear to be sluggish.

Prevention and Treatment

It is very rare that a golden image of your Integrity VM Host will be useful. If this is the only Integrity system you have and you need or want to create a golden image with it, then create the golden image before the Integrity VM software (bundles T2767AC and VMKernelSW) is installed.

In the event you already have several guests created using a VM Host golden image then those systems can be repaired. On each virtual machine, do the following:

1. Remove the Integrity VM software entirely:
   `swremove –x autoreboot=true T2767AC VMKernelSW`
2. After the system reboots, reset the following tunables (see kctune(1m)) to their defaults or the settings appropriate for the applications that will run in that VM: `dbc_min_pct, dbc_max_pct, swapmem_on`

#2 – Install VM Kit in the Guests

Symptoms: Performance, Functionality

Applications in the VM, especially those that are disk I/O intensive, perform poorly. This is especially pertinent when virtual disks are mapped to logical volumes on the VM Host.

The command line interfaces `hpvminfo` and `hpvmcollect` are delivered with guest kits.

Prevention and Treatment

HP-UX Guests

The HPVM-Guest bundle is provided in an SD (tape format) depot file,

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

on the VM Host system.

When creating a golden image to use for OS installation on virtual machines, install the HPVM-Guest bundle on the golden system.

Once the OS installed on a VM, install the bundle directly from the VM Host (or it may be copied to an SD depot with swcopy). For example, if the VM Host's hostname is vmhost.lab.hp.com, then the bundle may be installed on the VM with

```
swinstall –x autoreboot=true \
-s vmhost.lab.hp.com:/opt/hpvm/guest-images/hpux/hpvm_guest_depot.sd \
HPVM-Guest
```

For the newer Integrity servers (with Montecito processors), the guests and VM Host will need to install the Hardware Enablement (HWE) bundle available with the September 2006 (0609) OE media.

Windows® Guests

Installation of HP's SmartSetup media, version 4.5 or later, provides the guest kit for Windows, including the WBEM providers for virtual machines and utilization that are used by VSE tools. Note that you may need to create an exception in the Windows Firewall by adding a port with name `wbem-https` and number `5989`.

Linux® Guests

The Integrity VM guest kit for Linux as well as HP's Utilization WBEM provider is available from the Management CD, version 3.63 or later, in HP's Integrity Essentials Foundation Pack for Linux. VSE tools require the installation and configuration of WBEM functionality. Consult VSE documentation for more details.

For more information on the SmartSetup media for Windows, visit the website http://www.hp.com/go/integrityessentials. Similarly, details regarding the Management CD and HP Integrity Essentials Foundation Pack for Linux are available from http://www.hp.com/go/integritylinuxessentials.

#3 – Use Multipath or RAID Technology on the VM Host, Not the Guest

Symptoms: Functionality

Multipathing or RAID technology doesn't work as expected. For example, mirroring on the VM didn't help whenever one of the virtual hard drives was 'lost.'

Prevention and Treatment

Multipath technologies address physical connections to storage and are not applicable to virtual machines. Similarly RAID functionality applies to physical storage units.

Use multipathing and RAID technologies on the VM Host and use only the 'primary' path as a virtual hard drive. The multipathing or RAID technology on the VM Host will protect against link failures and the virtual machines benefit indirectly. See the white paper "Best Practices for Integrity VM" for more information.

#4 – Install the Required Patches on the VM Host

Symptoms: Performance, Reliability

The guest OS or its applications perform poorly. CPU resource allocation to the virtual machines may not correctly correspond to entitlements for those virtual machines.

Prevention and Treatment

Consult the Integrity VM release notes (always available on docs.hp.com) for the set of patches required by Integrity VM.

As noted above, newer Integrity servers with Montecito processors will need the HWE bundle installed on the VM Host and guests.

#5 – Configure Sufficient Swap Space on the VM Host

Symptoms: Functionality

A virtual machine won't start, the failure usually accompanied by the message:

```
     Warning 1: Insufficient swap resource for guest.
These problems may prevent HPVM guest vm-name from booting.
hpvmstart: Unable to continue.
```

Prevention and Treatment

This is typically due to the VM Host having insufficient swap space. An Integrity VM Host system must have swap space that is at least 4GB larger than the total physical memory on the VM Host. For example, if the VM Host has 64GB of physical memory then you should have a minimum of 68GB of swap space on the VM Host.

#6 – Do Not Exceed the Maximum Supported Number of Virtual Storage Devices

Symptoms: Functionality

Virtual storage devices (disk or DVD) do not respond to I/O transactions or are otherwise inoperable.

Prevention and Treatment

Version 2.0 of Integrity VM supports up to 30 virtual storage devices per virtual machine. In the event that your virtual machine needs capacity provided by more than 30 LUNs, then you may have to consider combining some of LUNs into logical volumes on the VM Host and then using these logical volumes to define your virtual disks.

In previous versions, the limit is 15 virtual storage devices per virtual machine. Note that in these releases the limit was not enforced, resulting in inadvertently creating configurations which exceeded the limit. Version 2.0 enforces this limit.

#7 – Do Not Share Disks Between Guests and the VM Host

Symptoms: Functionality, Reliability

Both the VM Host and its guests may experience widespread data corruption and severe system reliability problems.

Prevention and Treatment

Take care in what storage is used to define virtual machine devices. Integrity VM will, by default, prevent sharing amongst virtual machines, but cannot protect the VM Host's storage from being shared with guests. Use the `hpvmdevmgmt` CLI to designate storage used by the VM Host as restricted devices. This should include all disks and logical volumes used by the VM Host (e.g., its file systems and root volumes).

#8 – Do Not Use Hardware Monitoring Tools in a VM

Symptoms: Functionality

Hardware monitoring applications running in the guest will provide information about virtual devices – at best. Such tools may not be used to measure physical hardware utilization due to the virtualization of hardware by Integrity VM.

Prevention and Treatment

Monitor actual hardware on the VM Host. Tools such as top, glance and others will report actual hardware information when executed on the VM Host. For examples of how to monitor the utilization of hardware by individual virtual machines, see the white paper "Best Practices for Using Integrity Virtual Machines."

Hardware utilization tools such as top and glance may be useful to run in a virtual machine to monitor virtual CPU utilization. Keep in mind that the utilization of virtual hardware – i.e., the virtual machine's share of the physical resource – will be reported by such tools. The virtual machine's share of a given hardware resource may change rapidly, especially in the case of virtual CPUs. Use hardware monitoring tools – including those provided with Integrity VM – on the VM Host system to measure a virtual machine's share of a given hardware resource.

#9 –Set Entitlements Conservatively

Symptoms: Functionality, Performance

Virtual machines may not start, displaying the message:

```
      Warning 1: Insufficient cpu resource for guest.
These problems may prevent HPVM guest vm-name from booting.
hpvmstart: Unable to continue.
```

Otherwise, virtual machines may not perform as well as expected due to inadequate resource allocation.

Prevention and Treatment

Such problems often result when using multi-CPU virtual machines (virtual SMPs). The virtual CPUs of a virtual SMP must run on separate physical CPUs. As a result, the entitlement for the virtual SMP with N virtual CPUs must be available on N different physical CPUs. For example, consider a single-CPU VM with entitlement of 70% running on an Integrity server with 2 physical CPUs. A second VM with 2 virtual CPUs is defined with entitlement of 50%. This second VM will not start, even though the aggregate available CPU entitlement is 130% (100% of one physical CPU and 30% of the other). This is because only 30% entitlement is available on one of the physical CPUs and the virtual SMP needs 50% on both physical CPUs.

In general, you should use the minimum or default entitlements until one or more of the VMs are not receiving adequate CPU resources for their workloads.

Note that the default entitlement settings for a VM are different depending on whether it was created by the CLI (hpvmcreate) or the GUI (VM Manager).

#10 – Install Versions of VMProvider and gWLM Appropriate for Your Version of Integrity VM

Symptoms: Functionality

On the VM Host system, Integrity VM 2.0 is not compatible with older versions of HP's Global Workload Manager (gWLM) and Virtual Machine WBEM Provider (VMProvider). You will need version 2.5 or later of gWLM and version 2.0 or later of VMProvider.

Prevention and Treatment

Replace older versions of gWLM with version 2.5. When installing Integrity VM (bundle T2767AC), simultaneously install the VMProvider bundle from the Integrity VM media.

For more information

http://docs.hp.com/en/vse.html provides most of the HP documentation for Integrity Virtual Machines, including

- Integrity VM Installation, Configuration, and Administration Guide
- Best Practices for Using Integrity Virtual Machines and other white papers

http://www.hp.com/go/virtualization

4AA1-1169ENW Rev 3.0, 8/2007

invent