Avaya Contact Recorder

VMware Guide

Release 12.0

Issue 1
July 2014

Contents

Chapter 1

VMware Requirements

The following sections describe the requirements for an Avaya Contact Recorder Recorder deployment with VMware:

Overview

Avaya Contact Recorder is a real-time media application, and as such requires low-latency access to resources in order to perform according to specification and to sizing guidelines. This document provides an overview of the requirements for provisioning Avaya Contact Recorder in a VMware environment. Failure to follow the configuration guidelines herein may result in the loss of recording, application functionality, and data loss.

Requirements

The requirements in this document apply to Avaya Contact Recorder servers.

To configure a Recorder virtual machine (VM), the VM host must:

- have the **VMWare Tools** application installed on the VM guest machine.
- meet the requirements for each of the following as set out in the *Planning, Installation & Administration (PIA) Guide*:
  - **Central Processing Unit (CPU) Reservations** set with the appropriate amount of MHz (according to server type).
  - **Memory Reservations** set with the appropriate GB amount (according to server type) defined in the PIA Guide.
  - **Dedicated Physical Network Interface Care (NIC)** per VM guest hosting ACR. Refer to the PIA Guide for details regarding appropriate sizing and quantity of NICs. Configure the NIC TX/RX buffer as described on VM Guest NIC Configuration, page 7.
- The VMXNET3 driver must be used for any NICs that are being used for recording, unless the NIC is configured as a passthrough mechanism (such as SR-IOV) to bypass the network virtualization layer, in which case the native driver is required.

CPU and Memory Reservations

Recorder VMs require CPU and memory reservations equivalent to the physical hardware on which they are run.

Hyper-threading is supported for virtual CPUs [vCPUs]. If hyper-threading is not provided, then double the number of physical cores are required to meet the vCPU requirement.

NOTE ESX 5.0 and above is supported for Avaya Contact Recorder servers.

The following are the CPU and memory reservation requirements for the different recorder server types. Failure to meet the requirements will trigger alarms in systems running on VMware.

Server Type	Minimum # CPU Cores	Minimum CPU Reservation†	Minimum Memory Reservation	Media IOPS*	DB IOPS	System IOPS‡
Recording Server	16 vCPUs	24000 MHz	8 GB	Up to 1000 IOPS	N/A	200

* Media IOPS Requirements are 1 IOPS per recording channel. Media IOPS refers here to the storage IOPS requirement from the media partition of the Recorder.

† CPU with Intel Supplemental SSE3 (SSSE3) support.

‡ System IOPS includes the operating system, software install and log partitions.

To Reserve CPU Resources

When reserving CPU resources, keep in mind that the number of physical CPUs (pCPUs) required is the as that same as that defined for virtual CPUs (vCPUs) in the table above.

1. In the VMware vSphere Client, right-click the virtual machine for the Recorder server and select **Edit Settings**.
2. On the **Resources** tab, click **CPU**.
3. Under **Resource Allocation**, set **Shares** to **Normal**.
4. Adjust the **Reservation** to a minimum level as stipulated in the table above.
5. Select the **Unlimited** check box.
6. Click **OK**.

To Reserve Memory

The memory allocated to an Avaya Contact Recorder can be larger than the indicated minimum memory reservation indicated in the table on page 6. In such a case, the reservation allocated to the corresponding virtual machine must match that of the Recorder. For example, if a machine is allocated 12 GB of RAM, the memory reservation must be 8 GB of RAM. This is because memory given to Windows can be reclaimed from VMware at any time if it is not reserved.

As an example, with a 8 GB allocation of RAM to a virtual machine, if only 4 GB were reserved, VMWare could take the additional 4 GB of RAM from the machine that is being used. If that memory happens to contain critical information for processing, it can cause the Recorders to pause, resulting in a loss of recording.

1. In the VMware vSphere Client, right-click the virtual machine for the Recorder server and select **Edit Settings**.
2. On the **Resources** tab, click **Memory**.
3. Under **Resource Allocation**, de-select **Reserve all guest memory**.
4. Set **Shares** to **Normal**.
5. Adjust the **Reservation** to a minimum level as stipulated in the table on page 6.
6. Select the **Unlimited** check box.
7. Click **OK**.

VM Guest NIC Configuration

For Delivery, no changes to the VM Guest NIC Configuration are required.

When using a dedicated NIC for Passive IP recording, the TX buffers must be set to the minimal number available and the record buffers must be increased to the maximum available. If using a passthrough NIC, these minimum/maximum numbers will vary depending on the driver/manufacturer.

When using a virtual NIC, the VMware VMXNET3 driver should have the following settings for Interception- (span-) based recordings or High Capacity Delivery recording:

- Large Rx buffers: 8192
- Rx Ring # 1 size: 4096
- Rx Ring #2 size: 4096
- Small Rx Buffers: 8192
- Enable adaptive Rx ring sizing: Disable this setting.

Host Requirements

All requirements provided by Avaya assume the use of Intel CPUs. Please consult Avaya if you are using AMD CPUs, as the requirements for these are different.

The Host machine CPUs must match the minimum CPU types outlined in the PIA Guide.

In addition to the requirements above concerning the Recorder's CPU reservation, the physical host must have additional processing available for scheduling, network handling, device interrupt handling and other related tasks. To prevent any loss of recording, the CPUs on a host should not be overcommitted, and the equivalent of two physical CPU cores must be available to handle these tasks.

NIC Requirements

When used as an IP Recorder, VMs have the same physical NIC requirements as a physical machine. Refer to the Server Platform Sizing section of the PIA Guide.

Please note the following requirements:

- The VMXNET3 virtual NIC driver must be used for all virtual NICs used for recording.
- For Passive IP, you must configure the vSwitch for Promiscuous Mode (see below for instructions).

To Configure a vSwitch in Promiscuous Mode

This applies to Passive IP recording (therefore, complete the following steps for the NIC used to acquire audio through Passive IP).

1. In the VMware vSphere Client, on the configuration tab select the networking page, and then access the properties of the vSwitch.
2. On the **Ports** tab, click **Edit**.
3. Click the **Security** tab.
4. Under **Policy Exceptions**, set **Promiscuous Mode** to **Accept**. This allows the detection of all frames passed on the standard switch that are allowed under the VLAN policy for the associated port group.
5. Click **OK**.

VMware Suite Features

The following features are not supported in conjunction with Avaya Contact Recorder (and as such should be disabled where applicable):

- Snapshotting — The Avaya Contact Recorders do not support virtual machine snapshotting while the machine is running, as this can lead to pauses in the virtual machine and a loss of recording.
- Ballooning — Ballooning causes RAM to be randomly swapped out of a host, resulting in pauses and a loss of recording.
- High Availability (HA), including vMotion.
- Direct Resource Services (DRS).

Both HA and DRS are not supported for a number of reasons, among them the fact that the Avaya Contact Recorder requires a dedicated NIC for recording.

Chapter 2

Best Practices and Troubleshooting

This chapter outlines some best practices and troubleshooting guidelines to aid the performance of Avaya Contact Recorder on VMware.

VMware Best Practices

Avaya Contact Recorder servers perform real-time processing, making them latency-sensitive. VMware recommends the use of its latency-sensitivity features in such an environment, thereby virtualizing the Recorder and associated applications. To this end, please observe the following guidelines:

- Set 100% memory reservation.
- Reserve 100% of the CPU. This guarantees exclusive pCPU access, which in turn helps to reduce vCPU halt/wake-up cost.
- Over provision pCPUs. This reduces the impact of sharing the last-level cache (LLC), and also helps to improve the performance of latency-sensitive VMs that use virtual NICs (vNICs) for network I/O.
- Use a passthrough mechanism such as SR-IOV to bypass the network virtualization layer, if the hardware supports it.
- Use a separate physical NIC (pNIC) for latency-sensitive VMs in order to avoid contention for network bandwidth.
- If you don't use a passthrough mechanism and there is contention for network bandwidth, use Network I/O Control (NetIOC).
- Disable all power management in both the Basic Input/Output System (BIOS) and vSphere.

Resources

The following documents from VMware discuss how to virtualize latency-sensitive applications:

http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf

http://www.vmware.com/files/pdf/techpaper/latency-sensitive-perf-vsphere55.pdf

Troubleshooting VMware Issues

Missed Packets

If there are missed packets at the guest, host, or physical hardware level:

- Ensure that you have followed the guidelines under VMware Best Practices, page 11.

If you are using a vSwitch, increase the Rx buffers. On the physical NIC through the VMware host, use the **`ethtool`** command to modify the rc.local or local.sh file to make the settings persistent across reboots (these are settings specific to your environment and the particular physical NIC involved).

General Alarms

If you encounter high CPU utilization, Recorder disconnects, or a high number of alarms:

- Verify that the system meets the minimum CPU/memory reservations outlined in this document.
- Verify that the system CPU of the host is of the minimum version or higher stipulated in the PIA Guide.
- Verify that the host is not under resource contention or being oversubscribed. Check the CPU ready time.
- Verify that the disk subsystem latency is healthy (that is, always below 20 ms latency).

Memory Swapped Alarm

Memory swapping should not occur on the Recorder server. If you encounter an alarm that indicates this has occurred, check the configuration of the virtual machine and its host, and ensure that you have met the requirements stipulated in this document.

CPU Time Stolen Alarm

CPU stolen time should be lower than 3% at all times; anything higher than this will generate an alarm.

Such an alarm indicates that the VMware host is having an issue allocating enough CPU resources to the Recorder guest VMware instance. Work with the VMware administrator to resolve this, either by adding more CPU resources to the machine, or removing some of the VMware guests running on the same VMware host (and therefore competing with the Recorder for resources).