ESXi Driver Install Handbook

ESXi 7.0.3

Publication Number: 58426 v1.0

Date: October 2023

AMD

Contents

AMD

List of Figures

Chapter 1 BIOS Settings to Support Virtualization

The following are the BIOS settings required to support virtualization.

- Intel VT-d is enabled.
- SRIOV is enabled.
- MMIO Base and MMIO Size is set to maximum.
- MMCFG Base and MMCFG Size is set to maximum.

Chapter 2 ESXi Driver Installation

ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware® for deploying and serving virtual computers.

Follow the instruction in the following sections for ESXi installation.

2.1 Software Needed for Setup

Following software is required for the setup.

- ISO file of ESXi.
- Host driver: Vib driver provided.
- Guest driver: Standard AMD ROCm™ package provided.

2.2 Install Host Driver

Method 1

In the VMware vSphere™ client, either have the system go into maintenance mode or directly use the command:

In host (ssh terminal):

```
# vim-cmd /hostsvc/maintenance_mode_enter
# esxcli software vib install --no-sig-check -v /vmfs/volumes/datastore2/amdgpuv-*.vib
# vim-cmd /hostsvc/maintenance_mode_exit
# esxcli system module set -m amdgpuv -e true (This is required only for first instance of driver installation)
# reboot
```

Method 2

Manually load the driver every time the system boots up.

In CentOS dev machine:

```
# scp amdgpuv/build/amdgpuv root@(host's ip):/usr/lib/vmware/vmkmod/
# scp amdgpuv/build/amdgpuv.map root@(host's ip):/etc/vmware/default.map.d/
```

In host (ssh terminal):

```
# vmkload_mod amdgpuv // To enable amdgpuv driver
```

Note: If you encounter issues with copying, it may be due to a conflict with vib. Uninstall vib by doing the following.

```
# esxcli software vib remove --maintenance-mode -n amdgpuv
```

Then unload the driver.

```
# esxcfg-module -u amdgpuv
```

2.2.1 Uninstall Host Driver (When Applicable)

Method 1

In host (ssh terminal):

```
# esxcli software vib remove --maintenance-mode -n amdgpuv
# reboot
```

Method 2

Manually unload the driver.

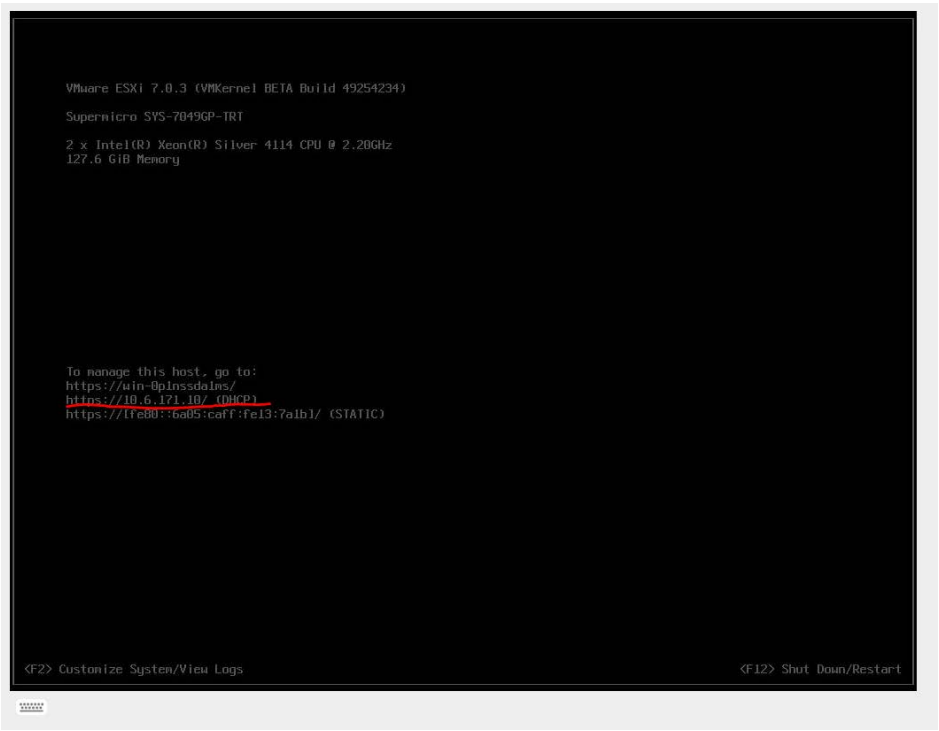
In host (ssh terminal):

```
# vmkload_mod -u amdgpuv // To disable amdgpuv driver
```

2.3 Configure VFs via Host Web Client

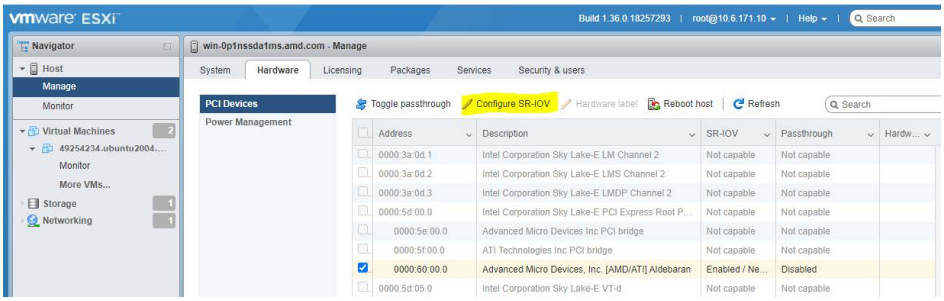
1. Log in to your host web client by following the IP.

   Figure 2.1: How to Find Your Host Web Client



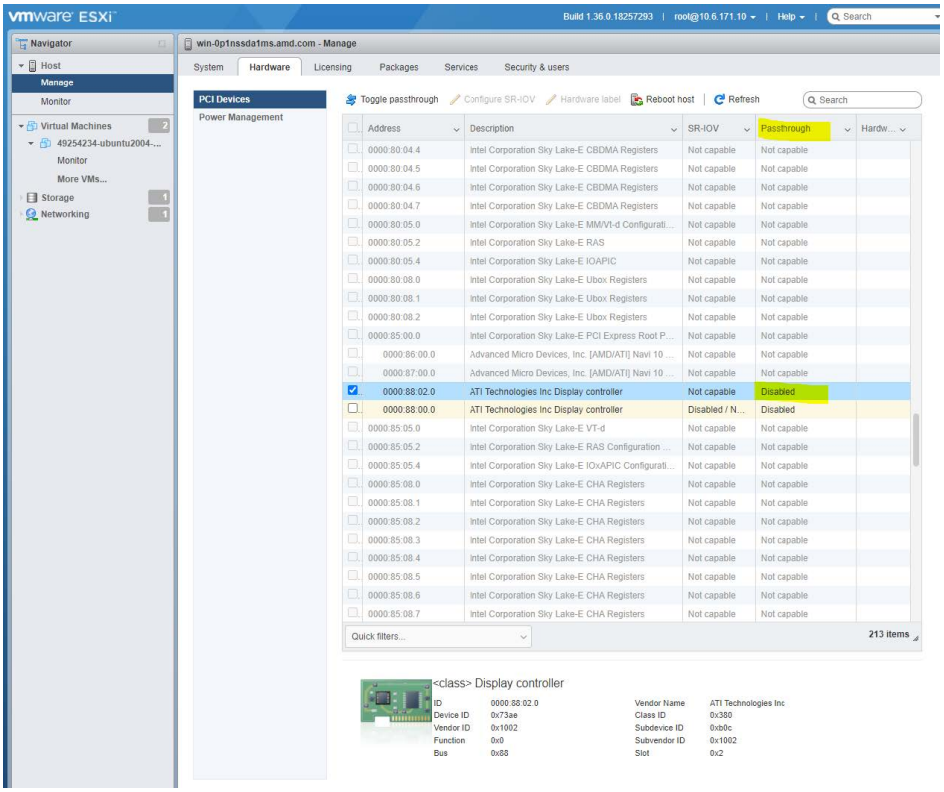
2. Locate the correct PF device by doing the following: **Host** > **Manage** > **Hardware** > **PCI Devices**. Then click **Configure SR_IOV** to enable the required amount o VFs.

Figure 2.2: Locating PF Device



3. After the VFs are enabled, make sure they are passthrough enabled. If not, select the VF and toggle passthrough.

Figure 2.3: VF Passthrough



2.4 Guest VM Setup

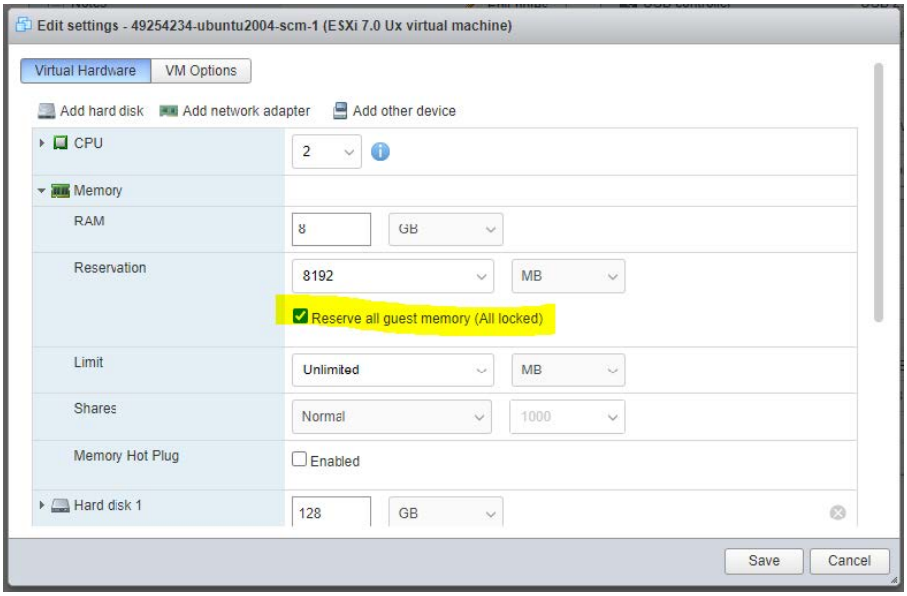
There are a couple of different methods for setting up guest VMs:

- Create from an ISO image.
- Clone from an existing VM.

2.4.1 Create a VM from Scratch

1. In the host web UI, do the following: select **Virtual Machines** > **Create/Register VM**, and follow the on-screen instruction to create an VM with the ISO for your guest mapped as CD/ DVD device.
2. In the VM settings, check the option **Reserve all guest memory**.

Figure 2.4: VM Settings



3. Assign the previous enabled VF to this VM by doing the following: select **VM setting** > **Edit** > **Add other device** > **PCI device**. Select the VF (with BDF) that enabled for passthrough, and click **save** to continue.
4. Edit the VM configure file */vmfs/volumes/datastore*/[VM name]/[VM name].vmx* by adding the following lines:

```
firmware = "efi"
pciPassthru.use64bitMMIO = "TRUE"
pciPassthru.64bitMMIOSizeGB = "128"
```

Note: These settings can also be added from the host web client under **VM Options** > **Advanced Settings**

5. Power on the VM to go through normal ISO installation procedure.
6. After installation is complete, remove the installation method (E.g. ISO image) to reboot the guest.

2.4.2 Clone VM from vCenter

1. Register your host to vCenter by doing the following:
   a. Log in vCenter server on web using IP.

b. Right-click on the server, select **IP** > **New Datacenter**, enter a name.

c. Right-click on the newly named datacenter tab, select **Add Host** and follow the on-screen instructions.

d. After the host is added, refresh/re-login your host web client until vCenter shows that your server is connected.

2. Once your ESXi server is connected to vCenter, follow steps below to clone the VM:

a. In vCenter UI, go to the VM's page that you are cloning and do the following:

a. Select **Action** > **Clone** > **Clone to Virtual Machine**.

b. Follow the on-screen instruction to perform the following:

1) Enter new VM's name.

2) Select the location for the new VM.

3) Select the correct host resource and storage location.

4) Select advanced clone options (customize guest OS or hardware options) if necessary.

a. If there are no error prompts, then the cloning is complete.

2.4.3 Clone to VM Template and Deploy (Link Clone)

1. Register your host to vCenter, and make sure there's a VM template for the clone to exist.

a. In vCenter UI, navigate to the VM's page, left-click on **ACTIONS** > **Clone** > **Clone to Template or Clone as Template to Library**.

b. Follow the instructions on screen.

2. In vCenter UI, right-click on your host and select **New Virtual Machine**. Follow the instruction on screen.

a. In Select a creation type, select **Deploy from template**.

b. In Select a template, select **corresponding template location**.

c. Follow the steps in Clone VM from vCenter to complete the cloning.

Appendix A Additional Resources and Legal Notices

A.1 Revision History

The following table shows the revision history for this document.

Section	Revision Summary
October 2023 Version 1.0	
Initial release.	

Appendix B Notices

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED "AS IS." AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.1 Trademarks

AMD, the AMD Arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc.

Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

VMware is a registered trademark of VMware in the US or other countries.

VMware vSPHERE is a registered trademark of VMware in the US or other countries.