



Single Root I/O Virtualization (SR-IOV)

- [Configuring BIOS and Cisco UCS Manager Parameters](#) , on page 1
- [Configuring SR-IOV VFs on the ESXi Host Server](#) , on page 6

Configuring BIOS and Cisco UCS Manager Parameters

Enabling SR-IOV BIOS Parameters

Before you begin

- You must have a BIOS policy that is already created with the following options enabled:
 - For Intel based servers, **Intel VT for directed IO** under **Intel Directed IO** tab.
 - For AMD based servers, **IOMMU** and **SVM Mode** under **Processor** tab.

To update BIOS options, see, [Cisco UCS Manager Server Management Guide](#).

- You must have a service profile already created for SR-IOV configuration. To create a Service Profile see [Cisco UCS Manager Server Management Guide](#). Once the Service Profile is created, follow the steps in this procedure to enable SR-IOV in the BIOS policy.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization that includes the service profile for which you want to enable SR-IOV BIOS parameters.

If the system does not include multi-tenancy, expand the root node.

Step 4 Click the service profile for which you want to enable SR-IOV BIOS parameters.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 On the **Policies** tab, expand **BIOS Policy**.

Step 7 From the **BIOS Policy** drop-down list, select the BIOS policy that you have created for SR-IOV configuration.

Ensure that the BIOS policy selected satisfies the per-requisites for this procedure.

Step 8 Save changes and click **Yes** to reboot the server.

Enabling SR-IOV VFs using Cisco UCS Manager GUI

To enable SR-IOV from Cisco UCS Manager, you must

- Create an SRIOV HPN Connection Policy with desired number of VFs.
- Assign the SRIOV HPN Connection Policy to a Service Profile.

Before you begin

- Ensure that the required BIOS options are enabled before performing this procedure.

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **Policies > root**.

Step 3 To create SRIOV HPN Connection Policy, right click **SRIOV HPN Connection Policies**.

Step 4 You can view and modify the created **SRIOV HPN Connection Policy** properties.

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	Brief description of the policy.
Number of SRIOV HPN vnics field	Enter an integer between 1 and 64.
Transmit Queues field	The number of descriptors in each transmit queue. Enter an integer between 1 and 8.
Receive Queues field	The number of receive queue resources to allocate. Enter an integer between 1 and 8.
Completion Queues field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 16.

Name	Description
Interrupt Count field	<p>The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.</p> <p>Enter an integer between 1 and 16.</p>

- Step 5** Provide the policy name with the desired number of SRIOV HPN vNICs and click **OK** to create **SRIOV HPN Connection Policy**.
- Step 6** In the **Navigation** pane, click **Servers**.
- Step 7** Expand **Servers > Service Profiles**.
- Step 8** Expand the node and service profile for the organization that contains the service profile for SR-IOV configuration.
- Step 9** Click the desired service profile for which you wish to apply the SR-IOV VFs.
- Step 10** Expand **vNIC** and select the vNIC for which you wish to apply the SR-IOV VFs.
- Step 11** In the work pane, select the **General** tab.
- Step 12** At the **Adapter Policy** drop-down list, select **SRIOV-HPN**.
- Step 13** Under the **Connection Policies** radio buttons, select **SRIOV-HPN**.
- Step 14** From the **SRIOV HPN Connection Policy** drop-down list, select the policy you have already created for SR-IOV configuration.
- Step 15** Save changes and click **Yes** to reboot the server.

Disabling SR-IOV VFs Using Cisco UCS Manager GUI

- Step 1** In the **Navigation** pane, click **Servers**.
- Step 2** Expand **Servers > Service Profiles**.
Expand the node and service profile for the organization that contains the service profile for SR-IOV configuration.
- Step 3** Click the service profile from which you wish to remove the SR-IOV VFs.
- Step 4** Expand **vNIC** and select the vNIC for which you wish to disable the SR-IOV VFs.
- Step 5** In the work pane, select the **General** tab.
- Step 6** Under the **Connection Policies** radio button options, select **SRIOV-HPN**.
- Step 7** From the **SRIOV HPN Connection Policy** drop-down list, select **not set** to remove the SR-IOV connection policy.
- Step 8** Save changes and click **Yes** to reboot the server.

Enabling SR-IOV VFs using Cisco UCS Manager CLI

To enable SR-IOV from Cisco UCS Manager, you must

- Create an SRIOV HPN Connection Policy with desired number of VFs.
- Assign the SRIOV HPN Connection Policy to a Service Profile.

Before you begin

- Ensure that the required BIOS options are enabled before performing this procedure.

SUMMARY STEPS

1. UCS-A # **scope org** *org-name*
2. UCS-A /org # **create sriov-hpn-conn-policy** *policy-name*
3. UCS-A /org/sriov-hpn-conn-policy* # **set sriov-hpn-count** *sriov hpn count*
4. UCS-A /org/sriov-hpn-conn-policy* # **set transmit-queue-count** *transmit queue count*
5. UCS-A /org/sriov-hpn-conn-policy* # **set receive-queue-count** *receive queue count*
6. UCS-A /org/sriov-hpn-conn-policy* # **set completion-queue-count** *completion-queue count*
7. UCS-A /org/sriov-hpn-conn-policy* # **set interrupt-queue-count** *interrupt queue count*
8. UCS-A /org/sriov-hpn-conn-policy* # **commit-buffer**
9. UCS-A /org/sriov-hpn-conn-policy* # **exit**
10. UCS-A /org # **scope service-profile** *profile-name-for-sriov-config*
11. UCS-A# scope /org/service-profile # **scope vnic** *eth0/eth1*
12. UCS-A /org/service-profile/vnic # **set adapter-policy SRIOV-HPN**
13. UCS-A /org/service-profile/vnic # **enter sriov-hpn-conn-policy-ref** *sriov_hpn_connection_policy_name*
14. UCS-A /org/service-profile/vnic/sriov-hpn-conn-policy-ref* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A # scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name.
Step 2	UCS-A /org # create sriov-hpn-conn-policy <i>policy-name</i>	Specifies the name for the SRIOV HPN connection policy.
Step 3	UCS-A /org/sriov-hpn-conn-policy* # set sriov-hpn-count <i>sriov hpn count</i>	Specifies the SRIOV HPN vNICs count for the SRIOV HPN connection policy. Enter an integer between 1 and 64.
Step 4	UCS-A /org/sriov-hpn-conn-policy* # set transmit-queue-count <i>transmit queue count</i>	Specifies the transmit queue count for the SRIOV HPN connection policy. Enter an integer between 1 and 8.
Step 5	UCS-A /org/sriov-hpn-conn-policy* # set receive-queue-count <i>receive queue count</i>	Specifies the receive queue count for the SRIOV HPN connection policy. Enter an integer between 1 and 8.
Step 6	UCS-A /org/sriov-hpn-conn-policy* # set completion-queue-count <i>completion-queue count</i>	Specifies the completion queue count for the SRIOV HPN connection policy. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 16.
Step 7	UCS-A /org/sriov-hpn-conn-policy* # set interrupt-queue-count <i>interrupt queue count</i>	Specifies the interrupt count for the SRIOV HPN connection policy. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 16.

	Command or Action	Purpose
Step 8	UCS-A /org/sriov-hpn-conn-policy* # commit-buffer	Commits the transaction to the system.
Step 9	UCS-A /org/sriov-hpn-conn-policy* # exit	
Step 10	UCS-A /org # scope service-profile <i>profile-name-for-sriov-config</i>	Enters the service profile for the organization that contains the service profile for SR-IOV configuration.
Step 11	UCS-A# scope /org/service-profile # scope vnic <i>eth0/eth1</i>	Select a vNIC for which you wish to apply the SR-IOV VFs.
Step 12	UCS-A /org/service-profile/vnic # set adapter-policy SRIOV-HPN	Sets the adapter policy as SRIOV HPN
Step 13	UCS-A /org/service-profile/vnic # enter sriov-hpn-conn-policy-ref <i>sriov_hpn_connection_policy_name</i>	Assigns the SRIOV HPN connection policy created previously to the vNIC.
Step 14	UCS-A /org/service-profile/vnic/sriov-hpn-conn-policy-ref* # commit-buffer	Commits the transaction to the system.

Disabling SR-IOV VFs using Cisco UCS Manager CLI

To disable the SRIOV VFs, you must delete the associated SRIOV HPN connection policy.

SUMMARY STEPS

1. UCS-A # **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *service_profile_name*
3. UCS-A /org/service-profile # **scope vnic** *eth0/eth1*
4. UCS-A /org/service-profile/vnic # **delete sriov-hpn-conn-policy-ref** *sriov_hpn_connection_policy_name*
5. UCS-A /org/service-profile/vnic* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A # scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name.
Step 2	UCS-A /org # scope service-profile <i>service_profile_name</i>	Enter the service profile withing which you wish to disable the SRIOV VFs.
Step 3	UCS-A /org/service-profile # scope vnic <i>eth0/eth1</i>	Select a vNIC for which you wish to apply the SR-IOV VFs.
Step 4	UCS-A /org/service-profile/vnic # delete sriov-hpn-conn-policy-ref <i>sriov_hpn_connection_policy_name</i>	Deletes the SRIOV HPN Connection policy. This disables the SRIOV VFs.
Step 5	UCS-A /org/service-profile/vnic* # commit-buffer	Commits the transaction to the system.

Configuring SR-IOV VFs on the ESXi Host Server

Installing Cisco eNIC Driver

Before you begin

Ensure that the SR-IOV BIOS parameters and SR-IOV VFs configurations are completed.

Step 1 Install the enic driver on the host.

The following example shows the installation of eNIC driver on EXSi:

```
[root@localhost:/vmfs/volumes/645c8bdd-c655e553-8ba0-e8d32272f6c0] esxcli software vib install -v
/vmfs/volumes/C240M7-Standalone/nenic-2.0.10.0-1OEM.800.1.0.20143090.x86_64.vib --no-sig-check
Installation Result
Message: The update completed successfully, but the system needs to be rebooted for the changes to
be effective.
VIBs Installed: CIS_bootbank_nenic_2.0.10.0-1OEM.800.1.0.20143090
VIBs Removed: CIS_bootbank_nenic_2.0.11.0-1OEM.800.1.0.20143090
VIBs Skipped:
Reboot Required: true
DPU Results:
[root@localhost:/vmfs/volumes/645c8bdd-c655e553-8ba0-e8d32272f6c0]
```

Step 2 Reboot the server to load the enic driver into the running kernel.

Step 3 After reboot, execute the **esxcli software vib list | grep nenic** command to check the driver version.

Verifying the Total Number of SR-IOV VFs Per Ports on the Host

You can verify the total number of SR-IOV VFs in the following two ways:

Step 1 Verify by logging into the VMware ESXi Host Client.:

- Login to the VMware ESXi Host Client.
- Execute the following command to check the vNIC with SR-IOV capability:

```
root@localhost:~] esxcli network sriovnic list
Name      PCI Device      Driver  Link  Speed  Duplex  MAC Address      MTU  Description
-----
vmmnic0  0000:1b:00.0  nenic  Up    50000  Full    f4:ee:31:30:80:40  1500 Cisco Systems Inc
Cisco VIC Ethernet NIC
```

The following output shows the number of VF configured on vNIC:

```
[root@localhost:~] esxcli network sriovnic vf list -n vmmnic0
VF ID  Active  PCI Address  Owner World ID
0      false  00000:027:00.1  -
1      false  00000:027:00.2  -
2      false  00000:027:00.3  -
3      false  00000:027:00.4  -
4      false  00000:027:00.5  -
5      false  00000:027:00.6  -
```

```
6 false 00000:027:00.7 -
7 false 00000:027:01.0 -
```

Step 2 Alternatively, you can also access your host from vSphere vCenter Client.

For more information on configuring SR-IOV VFs on the host, see [Creating SR-IOV VFs on the Host](#).

After you reboot the host server, do the following:

- Login to the ESXi Host Client, and choose **Networking > Virtual Switches**.
- Click **Add Standard Virtual Switch**.
- Add a switch name in the **vSwitch Name** field, select the vmnic with SR-IOV capability, and click **Add**.
- In the **Port Groups** tab, click **Add Port Group**.
- In the **Add Port Group** dialog-box, add a new port group and select the switch from the **Virtual Switch** drop-down.

Creating SR-IOV VFs on the Host

Step 1 Login to your VMware ESXi Host Client.

Alternatively, you can also access your host from vSphere vCenter Client and browse to **Configure > Networking > Physical adapters**.

Step 2 Go to **Host > Manage** and select the **Hardware** tab.

Step 3 Select **PCI Devices** from the list.

Step 4 From the drop-down list, select **SR-IOV Capable**.

The list shows all the SR-IOV capable devices.

Step 5 Select the vNIC for which you wish to create the VFs.

Step 6 Click **Configure SR-IOV**.

Configure SR-IOV for Cisco VIC Ethernet NIC window is displayed.

Step 7 Perform the following:

Field	Description
Enabled radio button	Select Yes to enable the configuration.
Virtual functions field	Number of VFs as configured on SRIOV connection policy that are available for the configuration. Enter an integer between 1 and 64.

Step 8 Click **Save** and then reboot the host server.

Configuring the Switch

Before you begin

Ensure that the SR-IOV VFs are configured.

- Step 1** Login to your VMware ESXi Host Client.
- Step 2** Navigate to **Host > Networking** and select the **Virtual switches** tab.
- Step 3** Click **Add Standard Virtual Switch**.
- Step 4** Enter the name for the switch.
- Step 5** Select a SR-IOV Capable Vmnic from the list.
- Step 6** Click **Add**.
- Step 7** Complete the following:

Field	Description
vSwitch Name field	Enter a suitable name for the virtual switch.
MTU field	Enter the maximum transmission unit. The default is 1500 bytes.
Uplink 1 drop-down list	From the drop-down list, select the PCIe devices for which you created the SR-IOVs.
Link Discovery	From the drop-down list, select the Mode and the Protocol . Note These fields remain as default.
Security	Choose from the following options: <ul style="list-style-type: none"> • Promiscuous mode—Accept, Reject, or Inherit from vSwitch. • MAC address changes—Accept, Reject, or Inherit from vSwitch. • Forged trasmits—Accept, Reject, or Inherit from vSwitch.

Field	Description
NIC teaming	<p>Choose from the following:</p> <ul style="list-style-type: none"> • Load balancing—From the drop-down list choose the Load balancing. Values are: Inherit from vSwitch, • Network failover detection—From the drop-down list choose the network failover detection. Values are: Inherit from vSwitch, • Notify switches—Choose the notify switches. Values are Yes, No, Inherit from vSwitch. • Fallback—Choose the fallback. Values are Yes, No, Inherit from vSwitch. • Override failover order—From the drop-down list choose the override failover order. Values are Yes or No, • Failover order—Choose the failover order.
Traffic Shaping	<p>Perform the following:</p> <ul style="list-style-type: none"> • Status—Choose the status. Values are Enabled, Disabled, Inherit from vSwitch. • Average bandwidth—Enter the average bandwidth. • Peek bandwidth—Enter the peek bandwidth. • Burst size—Enter the burst size. <p>Note Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.</p>

What to do next

[Creating a Virtual Port, on page 9](#)

Creating a Virtual Port

Before you begin

Ensure that the SR-IOV VFs are configured.

- Step 1** Login to your VMware ESXi Host Client.
- Step 2** Go to **Host > Networking** and select the **Port Groups** tab.
- Step 3** Click **Add port group**.
- Add port group-New port group** window is displayed

Step 4 Complete the following:

Field	Description
Name field	Enter a suitable name for the virtual port.
VLAN ID field	Enter the VLAN ID.
Virtual Switch drop-down list	From the drop-down list, select the virtual switch.
Security	Choose from the following options: <ul style="list-style-type: none"> • Promiscuous mode—Accept, Reject, or Inherit from vSwitch. • MAC address changes—Accept, Reject, or Inherit from vSwitch. • Forged trasmits—Accept, Reject, or Inherit from vSwitch.

Step 5 Click **Add**.

Creating a New Virtual Machine (VM)

Before you begin

- Host with Desktop Environment
- sudo user with admin rights
- Virtualization packages are installed
- OS ISO image is copied to the host server

Refer [Installing OS on Guest VM on ESXi, on page 11](#).

Adding SR-IOV VF on the Virtual Machine

Before you begin

The Virtual Machine is powered off.

Step 1 Select a Virtual Machine Manager from the host, and choose **Edit Settings**.

Step 2 Choose **Memory** and set the **Reservation** for the memory to **4 GB**.

Step 3 Check the **Reserve all guest memory (All locked)** check box.

Step 4 On the right, click **Add New Device** and choose **Network Adapter**.

Step 5 In the **New Network** dialog-box, click **Browse** to select the vNIC with SR-IOV capable from the **Select Network** window, and click **OK**.

Table 1: Network Adapter Dialog Box

Field	Description
Status	The status of the network adapter.
Adapter Type	Choose the adapter type from the drop-down list.
Physical Function	The physical function of the network adapter.
MAC Address	The MAC address of the network adapter.
Allow Guest MTU Change	Choose to allow the guest MTU.

Step 6 Choose **PCI Device passthrough** from the **Adapter Type** drop-down.

Step 7 Select the device from the **Device Selection** window, and choose vNIC.

Step 8 Click **OK**.

What to do next

You can now log into the virtual machine, install Cisco eNIC driver 4.5.0.23 with Linux VMs on ESXi, reboot the virtual machine, and then use the `ip link` command to verify the added SR-IOV VF.

Installing OS on Guest VM on ESXi

Before you begin

Upload the Linux operating system ISO on the datastore.

Step 1 Right-click the host node and navigate to **vCenter > New Virtual machine**.

Step 2 Select a **Creation Type > Create New Virtual Machine**, and click **Next**.

Step 3 Enter a name for the folder, and click **Next**.

Step 4 Select a compute resource, choose a node and click **Next**.

Step 5 Select Storage and check the datastore radio-button, and click **Next**.

Step 6 Select the compatibility ESXi 8.0 or later and click **Next**.

Step 7 Select a guest OS version as **RHEL Linux9 (64-bit)**, and click **Next**.

Step 8 Customize the hardware set **CPU** to 2, and **Memory values** to 4 GB.

Step 9 Expand the **Memory** tab, and check **Reserve all guest memory (All lockset)** check box.

Step 10 Select **New CD/DVD Drive (Datastore ISO file)**, and check the **Connect At Power On** check box.

Step 11 Under **CD/DVD Media**, browse and select the Linux ISO image and click **Next**.

Step 12 Click **Finish**.
