# SteelCentral™ NetShark
# Quick Start Guide

Virtual Edition for Microsoft Hyper-V

Version 10.9

October 2015

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

This manual is for informational purposes only. Addresses shown in screen captures were generated by simulation software and are for illustrative purposes only. They are not intended to represent any real traffic or any registered IP or MAC addresses.

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com

712-00241-02

# Contents

# About this guide

The Riverbed® SteelCentral™ NetShark virtual edition is a virtualized implementation of the SteelCentral NetShark. NetShark provides visibility into virtual environments by monitoring virtual machine (VM) ingress and egress traffic on virtual switches in a Hyper-V host.

If you are acquainted with the physical NetShark, you will find the NetShark virtual edition similar in structure and function.

The installation instructions assume you are familiar with the Microsoft Hyper-V hypervisor, Hyper-V Manager and the use of Microsoft PowerShell to manage VMs in a Microsoft Hyper-V host.

This guide details the steps to deploy NetShark on a Hyper-V host. When you have completed the initial installation and configuration, refer to the *SteelCentral NetShark User's Guide* for further instructions on operational configuration and use.

The instructions in this guide covers version 10.8 or later of the NetShark software.

# Preparing to deploy the NetShark

## Gathering the software components

Have these software components available or installed, as appropriate.

- Microsoft Hyper-V R3 installed on one of the following hardware servers:
  - Windows Server 2012 R2
  - Hyper-V Server 2012 R2
- A Hyper-V host requires the capacity for a virtual machine with 2 virtual CPUs, 2 GB of RAM, 30 GB of storage for the system, plus up to 2 TB for packet storage
- A local connection or a Remote Desktop Connection to the Hyper-V server
- Windows PowerShell 4.0 (or later) with Hyper-V Module for Windows PowerShell
- Hyper-V Manager client software that connects to the Hyper-V host
- NetShark HyperV.zip file containing the NetShark virtual edition virtual hard disk (VHD), an installation PowerShell script and a network configuration PowerShell script
- SteelCentral™ Packet Analyzer (formerly Cascade® Pilot) 9.6 (or later) software, installed on your local system

## Preparing to Install the NetShark Virtual Machine

NetShark captures packets using port monitoring in a Hyper-V host. A NetShark monitor port is configured as a destination port for mirrored ingress and egress traffic from virtual machine (VM) source ports (network interfaces) in a Hyper-V host virtual switch.

When deploying NetShark on a Hyper-V host, consider the following:

- A NetShark supports up to four monitor ports, enabling packet capture on up to four virtual switches in a Hyper-V host.
- All mirror destination ports in a virtual switch receive the same traffic, so one NetShark monitor port is sufficient for a Hyper-V host virtual switch. There is no benefit in placing two monitor ports from the same NetShark in a virtual switch.
- Other VMs may be running applications that also use port monitoring, for example, a security application. The traffic from source ports configured by such an application also is mirrored to a NetShark monitoring port on that virtual switch.
- Hyper-V performs packet deduplication on mirrored traffic in a virtual switch.

The installation and configuration of a NetShark VM on a Hyper-V host requires a NetShark VHD and two PowerShell scripts, downloaded as a.zip file from the Riverbed Support Web site.

A NetShark VM is preconfigured with these components:

| | |
|---|---|
| • `primary` (network adapter) | primary management port |
| • `aux` (network adapter) | secondary management port |
| • `mon0` (network adapter) | monitor port for packet capture |
| • `Hard Drive` (IDE Controller 0) | 30 GB NetShark VHD |

You can add more components to a NetShark VM, depending on your requirements:

- an additional hard disk for up to 2 TB of packet storage (mandatory for most installations)
- up to three more monitor ports (optional, as required by your Hyper-V host configuration)

## Access to network

If you lock down your network on a port-by-port basis, check that the following ports are open between the NetShark and other devices it must communicate with:

- **TCP/22** – (ssh) Command line interface
- **TCP/443** – (https) Web interface and control from Riverbed® SteelCentral Packet Analyzer, also used by concurrent license server for Packet Analyzer
- **TCP or UDP/514** – Default port for external Syslog use, configured in NetShark Web UI
- **TCP/41017** – Traffic data to Riverbed® SteelCentral™ NetProfiler
- **UDP/123** – (ntp) Time synchronization
- **UDP/319 and 320** – (ptp) Time synchronization

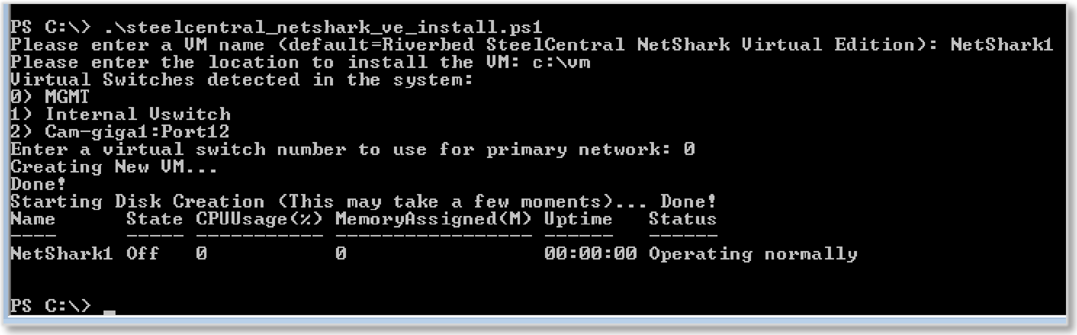
# Deploying the NetShark

## Deploying a NetShark to a Hyper-V host

Install the NetShark on a Hyper-V host, as follows:

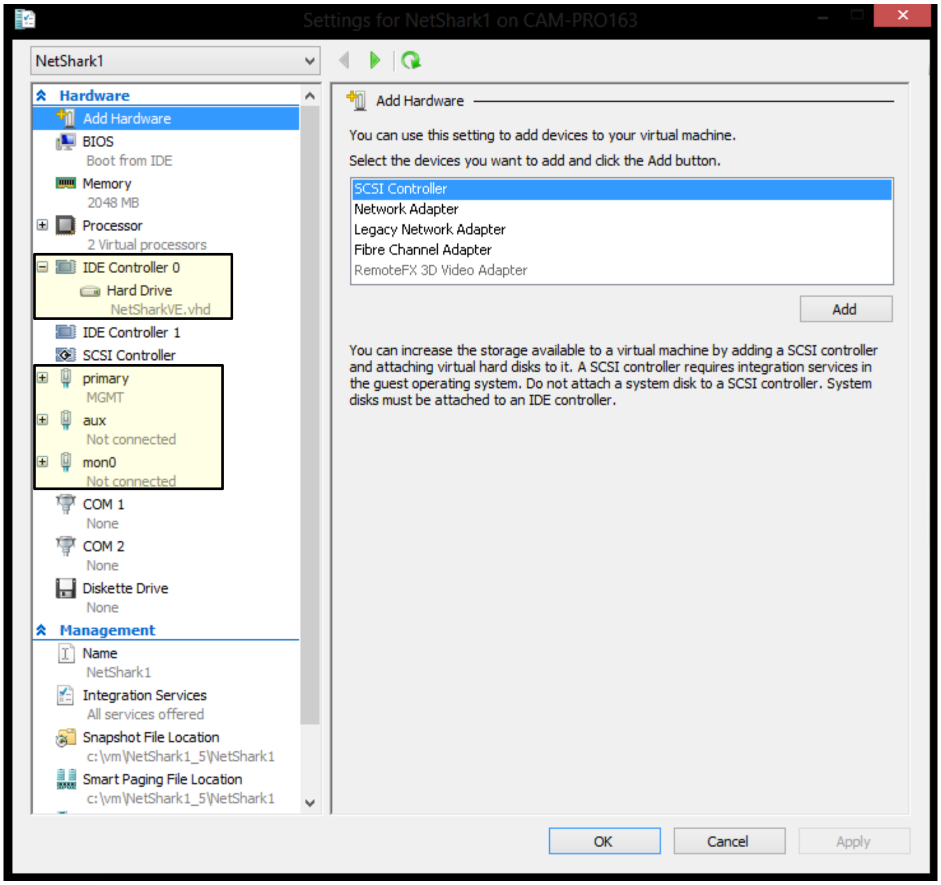
1. Confirm that PowerShell is installed and that scripts are enabled on the Hyper-V hypervisor host computer. To enable scripting, execute the command **`Set-ExecutionPolicy unrestricted`** from the PowerShell command line.
2. Download the zip package from the Riverbed Support Web site. Go to https://support.riverbed.com. Access to software downloads requires registration.
3. Copy the zip package to the Hyper-V host computer and unzip it.
4. Open Windows PowerShell on the Hyper-V host and run the STEELCENTRAL_NETSHARK_VE_INSTALL.ps1 script.
    - **Enter the VM name** – Choose a name that identifies the VM as a NetShark. This simplifies configuring the NetShark VM, as you select a NetShark VM to configure from a list of VMs running on the Hyper-V host.
    - **Enter the VM location** – Enter the path for installing the virtual hard drive (VHD) where all information about the VM is stored. This VHD also contains the NetShark system software, pcap trace files, View metrics, and Microflow Indexing data for Job Traces.
    - **Select a virtual switch to be used for the primary network** - At installation, the script configures two network interfaces for the NetShark management ports, `primary` and `aux` along with a network interface for a monitor port (`mon0`). By default, the `primary` port is enabled on the virtual switch you select. **Note:** the management port network interface must be accessible from an external network. If you plan to use DHCP to assign an IP address to the management port, access to a DHCP server also is needed.

An example installation of a NetShark VM named `NetShark1` using the installation script STEELCENTRAL_NETSHARK_VE_INSTALL.ps1 appears below. When the script completes, the NetShark VM is off, ready to be configured.



```
PS C:\> .\steelcentral_netshark_ve_install.ps1
Please enter a VM name (default=Riverbed SteelCentral NetShark Virtual Edition): NetShark1
Please enter the location to install the VM: c:\vm
Virtual Switches detected in the system:
0) MGMT
1) Internal Vswitch
2) Cam-giga1:Port12
Enter a virtual switch number to use for primary network: 0
Creating New VM...
Done!
Starting Disk Creation (This may take a few moments)... Done!
Name      State CPUUsage(%) MemoryAssigned(M) Uptime   Status
----      ----- ----------- ----------------- ------   ------
NetShark1 Off   0           0                 00:00:00 Operating normally


PS C:\> _
```

The settings in Hyper-V Manager for the NetShark1 VM appear below. The interfaces and devices added by the STEELCENTRAL_NETSHARK_VE_INSTALL.ps1 script are highlighted.



Settings for NetShark1 on CAM-PRO163

NetShark1

Hardware

- Add Hardware
- BIOS
  Boot from IDE
- Memory
  2048 MB
- Processor
  2 Virtual processors
- IDE Controller 0
  - Hard Drive
    NetSharkVE.vhd
- IDE Controller 1
- SCSI Controller
- primary
  MGMT
- aux
  Not connected
- mon0
  Not connected
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management

- Name
  NetShark1
- Integration Services
  All services offered
- Snapshot File Location
  c:\vm\NetShark1_5\NetShark1
- Smart Paging File Location
  c:\vm\NetShark1_5\NetShark1

Add Hardware

You can use this setting to add devices to your virtual machine.

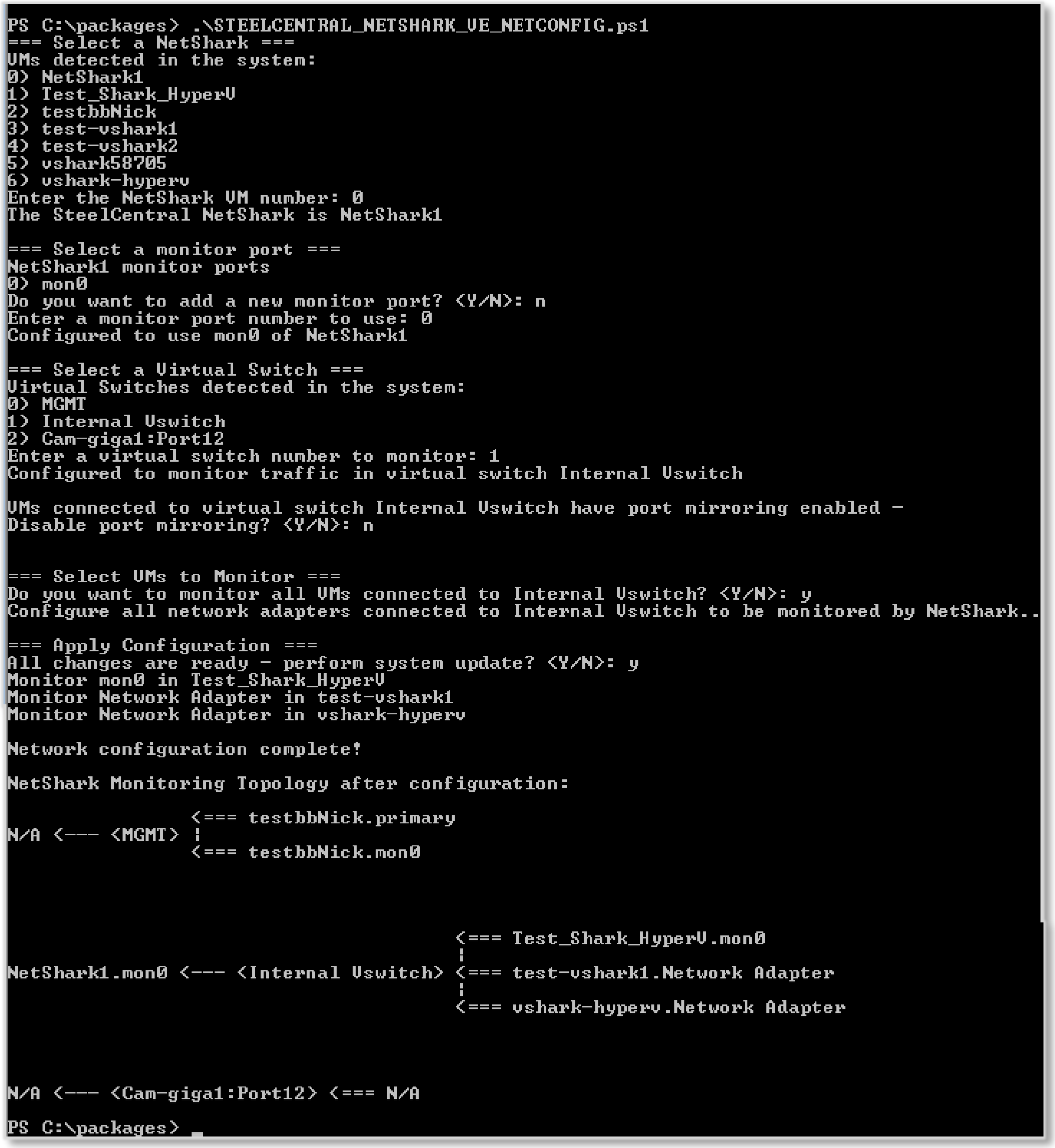
Select the devices you want to add and click the Add button.

- SCSI Controller
- Network Adapter
- Legacy Network Adapter
- Fibre Channel Adapter
- RemoteFX 3D Video Adapter

You can increase the storage available to a virtual machine by adding a SCSI controller and attaching virtual hard disks to it. A SCSI controller requires integration services in the guest operating system. Do not attach a system disk to a SCSI controller. System disks must be attached to an IDE controller.

Run the PowerShell script STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1 to configure a NetShark monitor port for a virtual switch and connected VM interfaces.

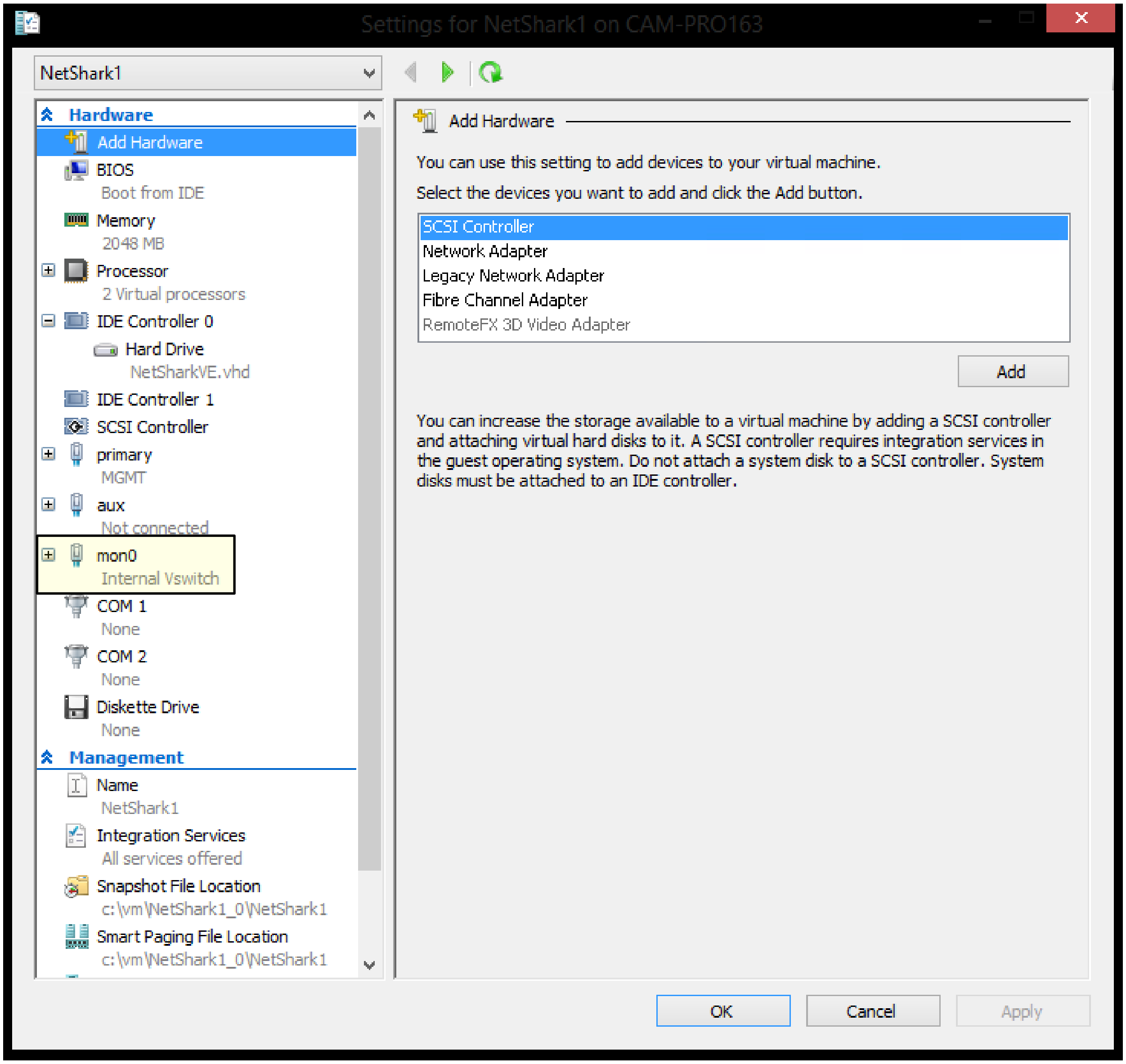
1. Select a NetShark. Select from the list of VMs presented.
2. Select a monitor port. The selected monitor port is the destination for traffic mirrored from all or the selected VM network interfaces. Enter "N" and select monitor port mon0.
3. Select a Virtual Switch to monitor. As all mirrored traffic is sent to all mirror destination ports, if mirroring is currently enabled on a VM, determine if this mirrored traffic must continue. Select "Y" to disable or "N" to continue existing mirrored traffic from VMs.
4. Select VMs to monitor. You can monitor ingress and egress traffic for all VMs connected to a virtual switch by entering "Y" or select only specific VMs by entering "N." Enter "Y."
5. Apply Configuration. Enter "Y" to agree to make the configuration changes. A list of VM interfaces to be monitored is displayed. Enter "N" to exit the script without making any configuration changes.



```
PS C:\packages> .\STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1
=== Select a NetShark ===
VMs detected in the system:
0) NetShark1
1) Test_Shark_HyperV
2) testbbNick
3) test-vshark1
4) test-vshark2
5) vshark58705
6) vshark-hyperv
Enter the NetShark VM number: 0
The SteelCentral NetShark is NetShark1

=== Select a monitor port ===
NetShark1 monitor ports
0) mon0
Do you want to add a new monitor port? <Y/N>: n
Enter a monitor port number to use: 0
Configured to use mon0 of NetShark1

=== Select a Virtual Switch ===
Virtual Switches detected in the system:
0) MGMT
1) Internal Vswitch
2) Cam-giga1:Port12
Enter a virtual switch number to monitor: 1
Configured to monitor traffic in virtual switch Internal Vswitch

VMs connected to virtual switch Internal Vswitch have port mirroring enabled -
Disable port mirroring? <Y/N>: n


=== Select VMs to Monitor ===
Do you want to monitor all VMs connected to Internal Vswitch? <Y/N>: y
Configure all network adapters connected to Internal Vswitch to be monitored by NetShark..

=== Apply Configuration ===
All changes are ready - perform system update? <Y/N>: y
Monitor mon0 in Test_Shark_HyperV
Monitor Network Adapter in test-vshark1
Monitor Network Adapter in vshark-hyperv

Network configuration complete!

NetShark Monitoring Topology after configuration:

                <=== testbbNick.primary
N/A <--- <MGMT> |
                <=== testbbNick.mon0




                                       <=== Test_Shark_HyperV.mon0
                                       |
NetShark1.mon0 <--- <Internal Vswitch> <=== test-vshark1.Network Adapter
                                       |
                                       <=== vshark-hyperv.Network Adapter




N/A <--- <Cam-giga1:Port12> <=== N/A

PS C:\packages> _
```

When the configuration is finished, the script displays a Network Topology of the NetShark monitoring ports, Hyper-V host virtual switches and monitored VM network interfaces. In the above example, the virtual switch `Internal Vswitch` is being monitored by NetShark `mon0`. The network adapters from the `Test_Shark_HyperV, test-vshark1` and `vshark-hyperv` VMs are mirrored traffic sources to the NetShark `mon0` port. The other two virtual switches, `MGMT` and `cam-giga1:Port12`, in the Hyper-V host are not presently being monitored by NetShark.

The settings for the NetShark1 VM in Hyper-V Manager after the configuration appear below. The change made by running the STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1 script is highlighted.



BIOS
Boot from IDE
Memory
2048 MB
Processor
2 Virtual processors
IDE Controller 0
Hard Drive
NetSharkVE.vhd
IDE Controller 1
SCSI Controller
primary
MGMT
aux
Not connected
mon0
Internal Vswitch
COM 1
None
COM 2
None
Diskette Drive
None

Name
NetShark1
Integration Services
All services offered
Snapshot File Location
c:\vm\NetShark1_0\NetShark1
Smart Paging File Location
c:\vm\NetShark1_0\NetShark1

Add Hardware

You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

SCSI Controller
Network Adapter
Legacy Network Adapter
Fibre Channel Adapter
RemoteFX 3D Video Adapter

You can increase the storage available to a virtual machine by adding a SCSI controller and attaching virtual hard disks to it. A SCSI controller requires integration services in the guest operating system. Do not attach a system disk to a SCSI controller. System disks must be attached to an IDE controller.

## Adding a hard disk for packet storage

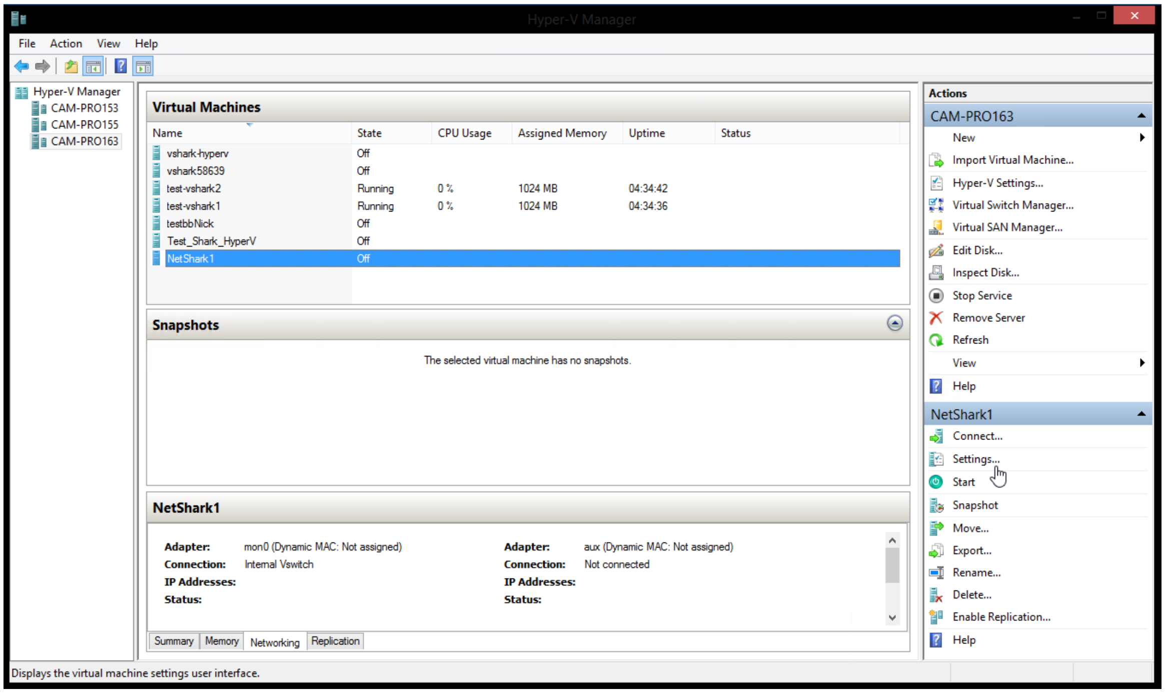
The preconfigured NetShark VM has one virtual hard disk, `NetSharkVE.vhd`, the system disk. For NetShark packet storage, a second virtual hard disk must be configured. Packet storage is not enabled until a license is installed on NetShark.

Packet storage summary:

- Packet storage may require high levels of disk activity. For best performance, Riverbed recommends using a VHD format drive of a fixed size. VHDX disks also are supported.
- If you specify a large amount of packet storage, say 1TB or 2TB, you might want to locate the hard disk on a path separate from the NetShark VM VHD.
- The maximum size of a packet storage hard disk is 2 TB.

The NetShark VM must be off to perform this procedure.

1. Open Hyper-V Manager and select the NetShark VM. Under **Actions**, click S***ettings*** under the NetShark VM.



Virtual Machines

| Name | State | CPU Usage | Assigned Memory | Uptime | Status |
|---|---|---|---|---|---|
| vshark-hyperv | Off | | | | |
| vshark58639 | Off | | | | |
| test-vshark2 | Running | 0 % | 1024 MB | 04:34:42 | |
| test-vshark1 | Running | 0 % | 1024 MB | 04:34:36 | |
| testbbNick | Off | | | | |
| Test_Shark_HyperV | Off | | | | |
| NetShark1 | Off | | | | |

Snapshots

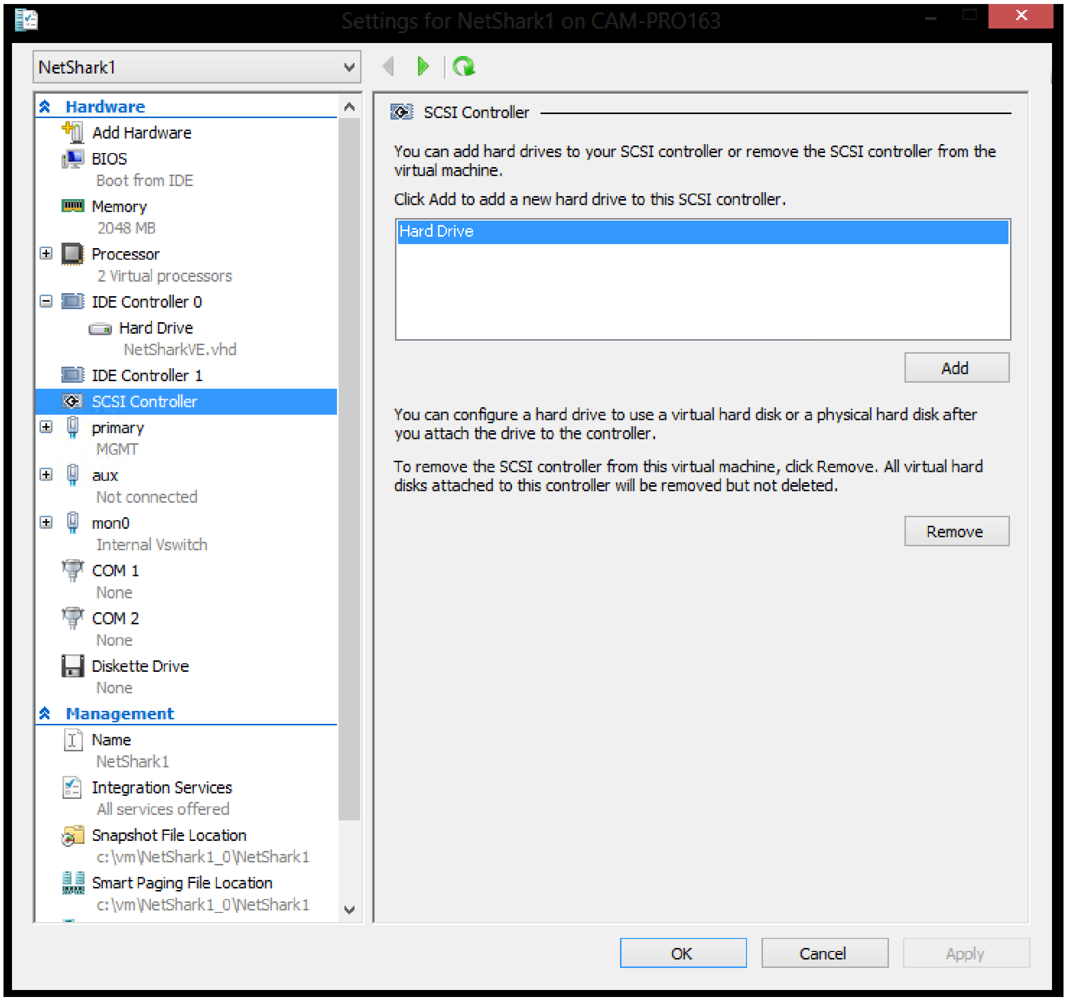
The selected virtual machine has no snapshots.

NetShark1

| | | | |
|---|---|---|---|
| **Adapter:** | mon0 (Dynamic MAC: Not assigned) | **Adapter:** | aux (Dynamic MAC: Not assigned) |
| **Connection:** | Internal Vswitch | **Connection:** | Not connected |
| **IP Addresses:** | | **IP Addresses:** | |
| **Status:** | | **Status:** | |

Displays the virtual machine settings user interface.

2. Click on an available SCSI Controller, select **Hard Drive** and then click **Add**.



Settings for NetShark1 on CAM-PRO163

NetShark1

**Hardware**

Add Hardware

BIOS
Boot from IDE

Memory
2048 MB

Processor
2 Virtual processors

IDE Controller 0

Hard Drive
NetSharkVE.vhd

IDE Controller 1

SCSI Controller

primary
MGMT

aux
Not connected

mon0
Internal Vswitch

COM 1
None

COM 2
None

Diskette Drive
None

**Management**

Name
NetShark1

Integration Services
All services offered

Snapshot File Location
c:\vm\NetShark1_0\NetShark1

Smart Paging File Location
c:\vm\NetShark1_0\NetShark1

SCSI Controller

You can add hard drives to your SCSI controller or remove the SCSI controller from the virtual machine.

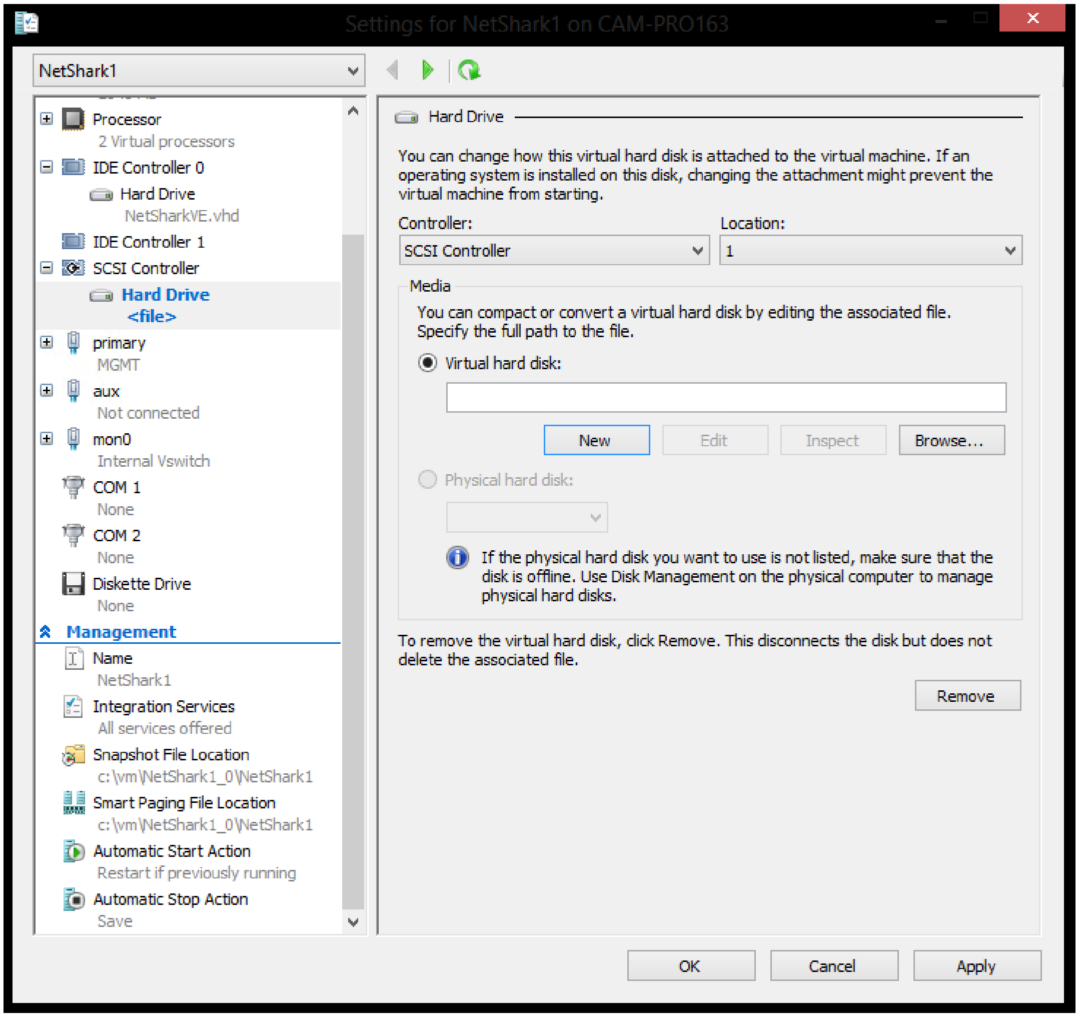
Click Add to add a new hard drive to this SCSI controller.

Hard Drive

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

To remove the SCSI controller from this virtual machine, click Remove. All virtual hard disks attached to this controller will be removed but not deleted.

3. On the ***Hard Drive*** page:
   - select the SCSI controller and location to use to connect to your NetShark VM
   - click **New** to create a new virtual hard disk



Settings for NetShark1 on CAM-PRO163

NetShark1

- Processor
  2 Virtual processors
- IDE Controller 0
  - Hard Drive
    NetSharkVE.vhd
- IDE Controller 1
- SCSI Controller
  - **Hard Drive**
    **<file>**
- primary
  MGMT
- aux
  Not connected
- mon0
  Internal Vswitch
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

**Management**

- Name
  NetShark1
- Integration Services
  All services offered
- Snapshot File Location
  c:\vm\NetShark1_0\NetShark1
- Smart Paging File Location
  c:\vm\NetShark1_0\NetShark1
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller

Location: 1

Media

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

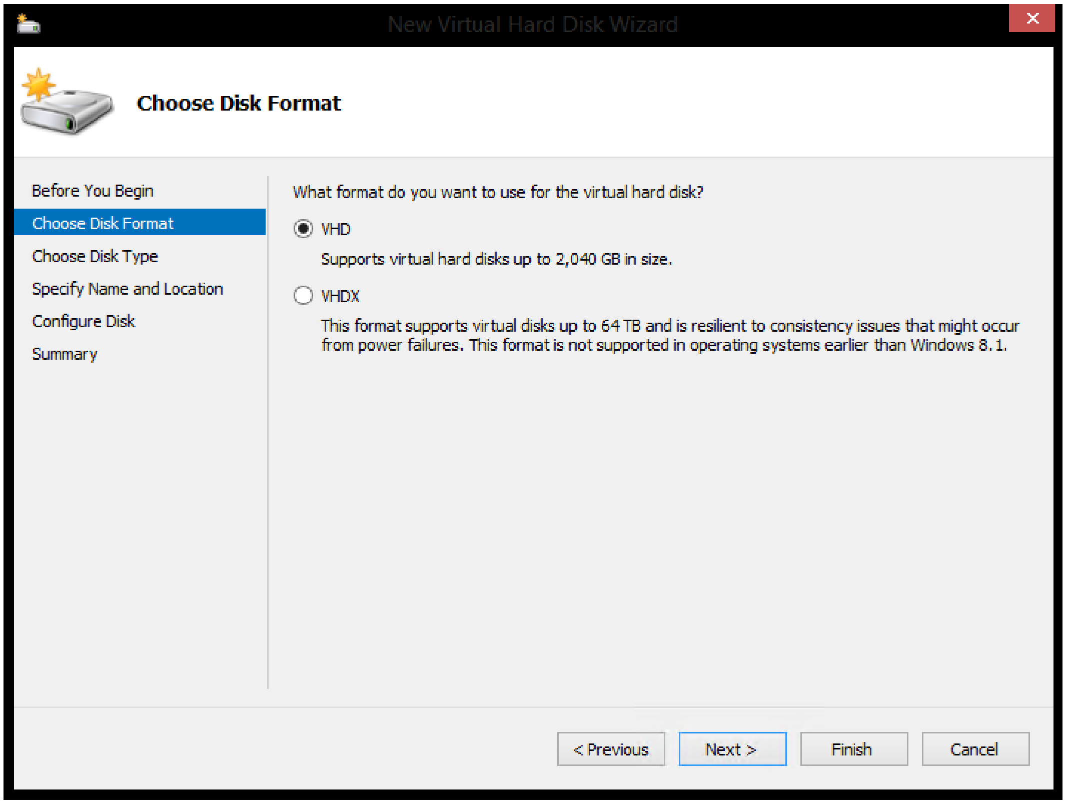
● Virtual hard disk:

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

4. On the ***Choose Disk Format*** page select V***HD***.



What format do you want to use for the virtual hard disk?

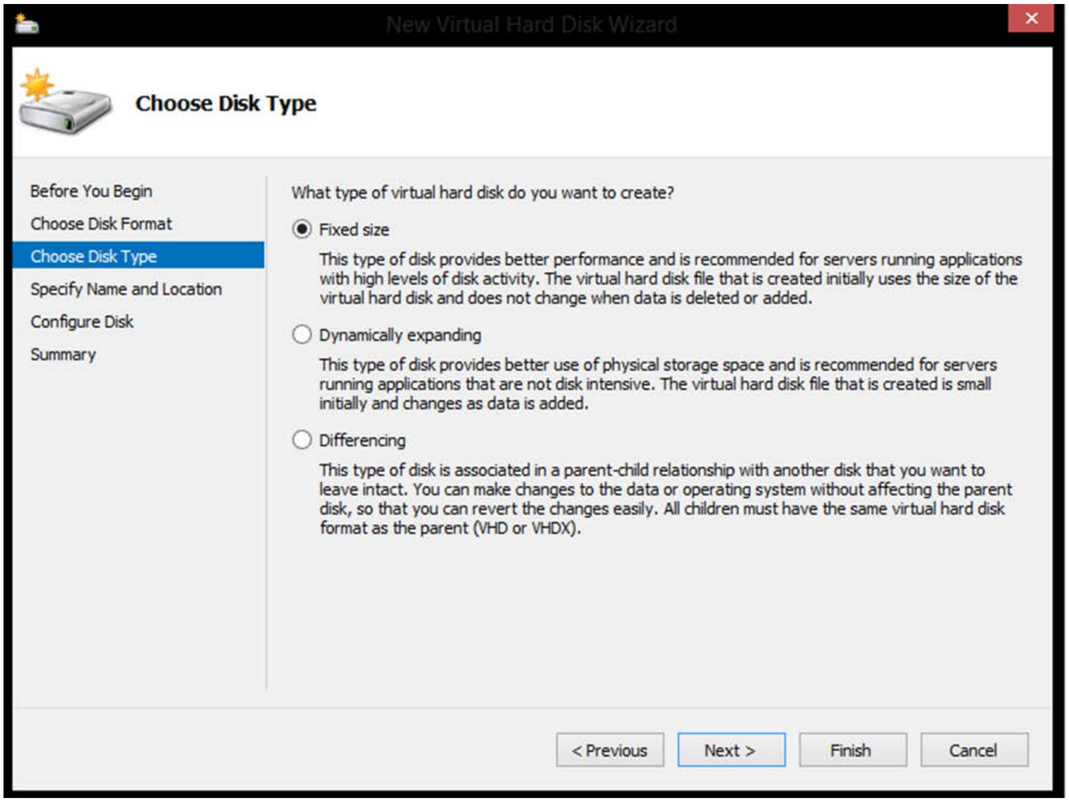
● VHD

Supports virtual hard disks up to 2,040 GB in size.

○ VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows 8.1.

5. On the ***Choose Disk Type*** page select ***Fixed size***.



Choose Disk Type

What type of virtual hard disk do you want to create?

● Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

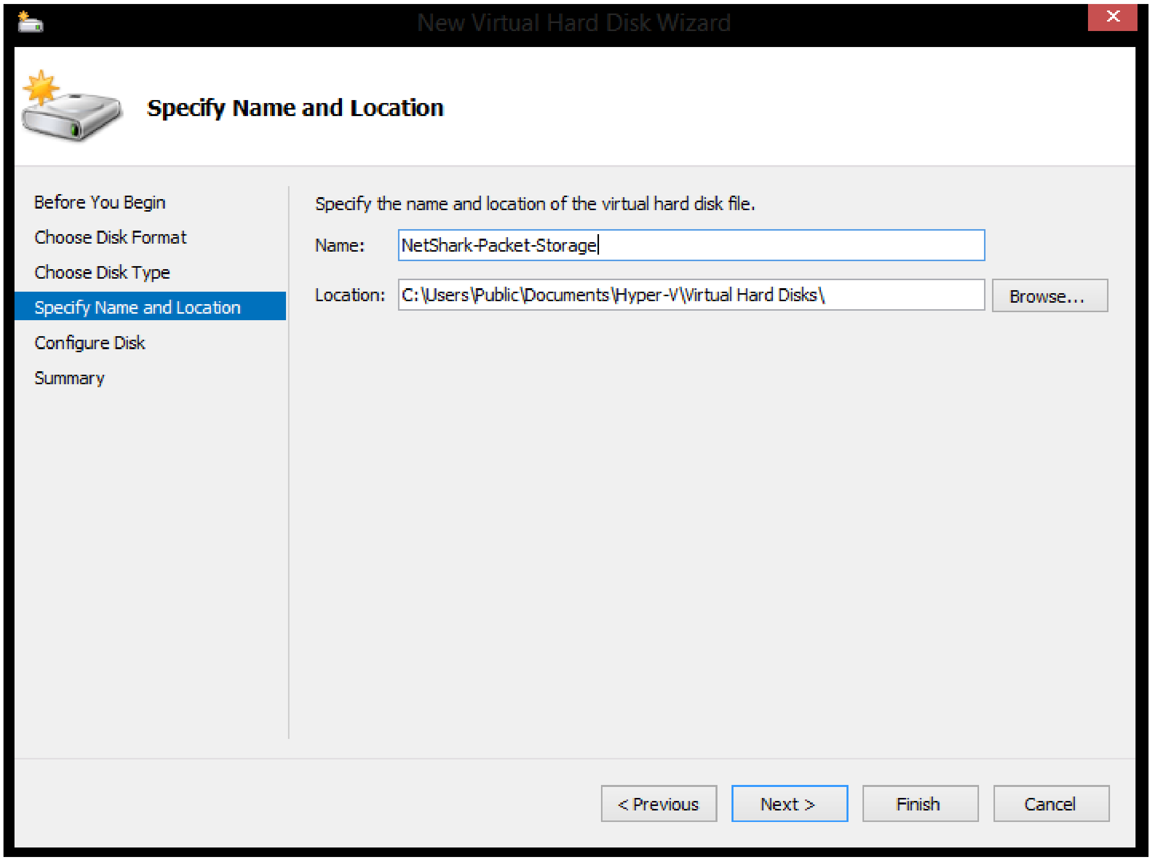
○ Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

○ Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

6. Specify the hard disk **Name** and **Location**.

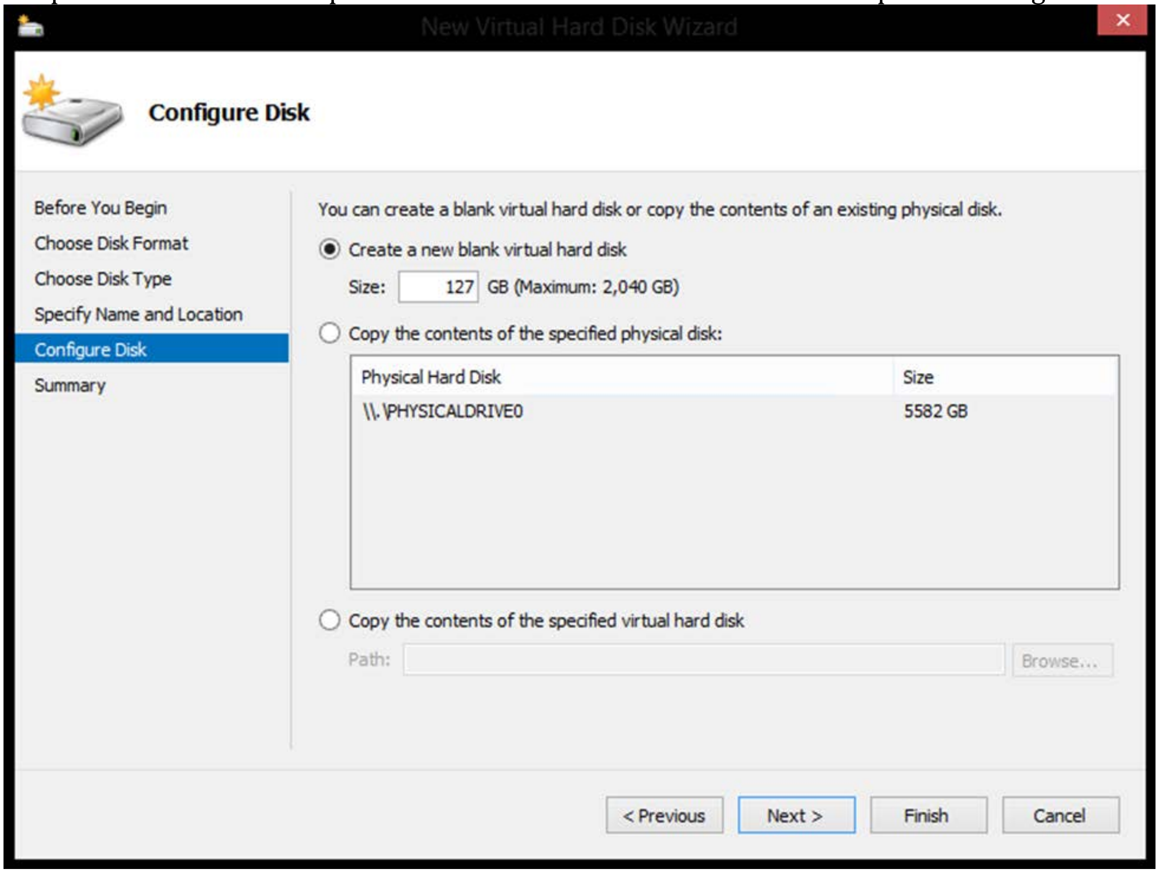


Specify the name and location of the virtual hard disk file.

Name: NetShark-Packet-Storage

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

7. Select **Create a new blank virtual hard disk** and specify a virtual hard disk size of up to 2 TB. In this example a 127 GB virtual hard disk is created for packet storage.



You can create a blank virtual hard disk or copy the contents of an existing physical disk.

● Create a new blank virtual hard disk

Size: 127 GB (Maximum: 2,040 GB)

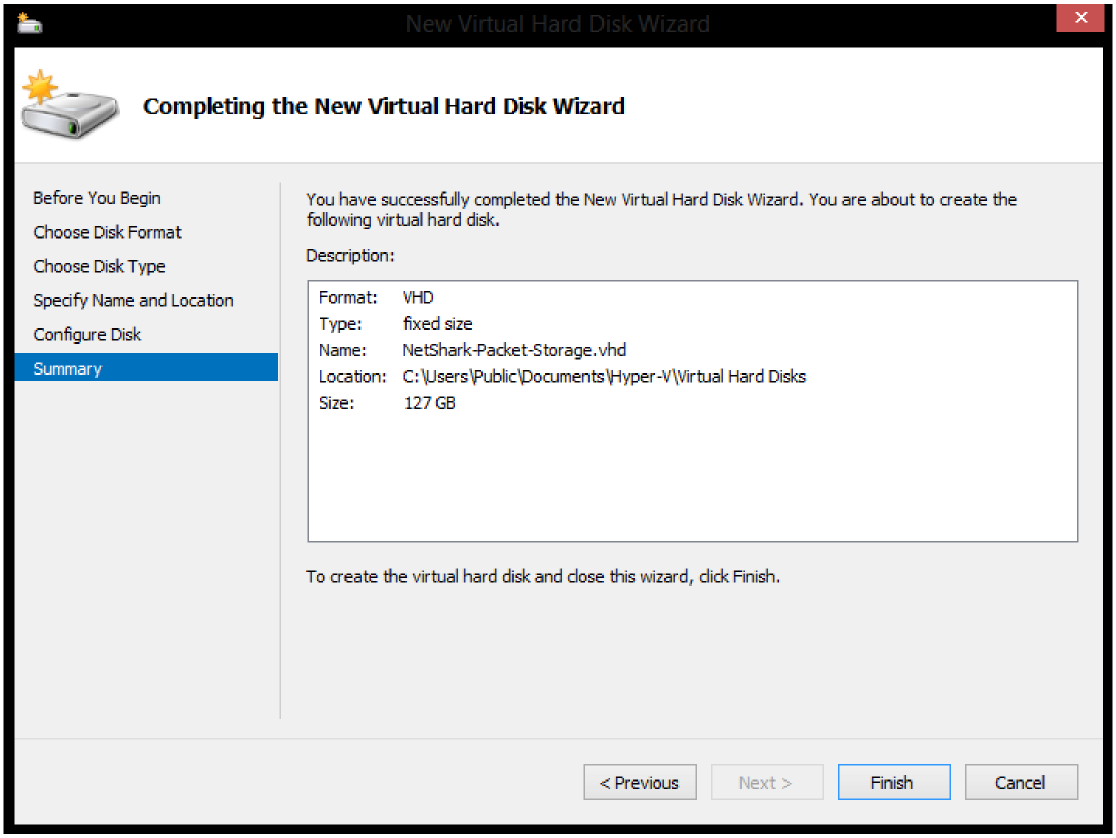
○ Copy the contents of the specified physical disk:

| Physical Hard Disk | Size |
|---|---|
| \\.\PHYSICALDRIVE0 | 5582 GB |

○ Copy the contents of the specified virtual hard disk

Path:

8. Review your choices; click **Finish** to create the virtual hard disk.



Completing the New Virtual Hard Disk Wizard

You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

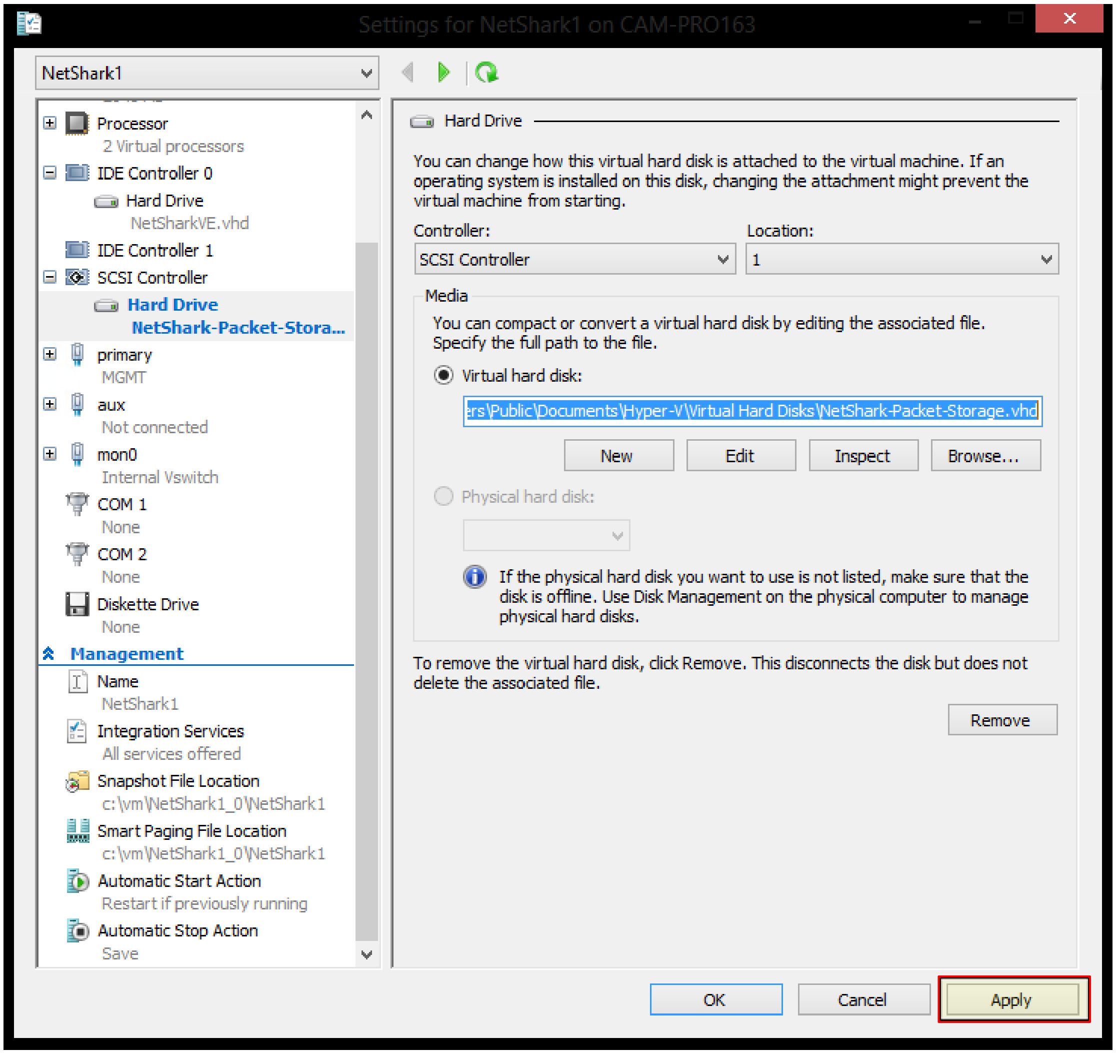
Description:

Format: VHD
Type: fixed size
Name: NetShark-Packet-Storage.vhd
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Size: 127 GB

To create the virtual hard disk and close this wizard, click Finish.

In this example a 127 GB virtual hard disk is specified for packet storage. NetShark supports a packet storage disk of up to 2 TB.

9. The Hard disk has been created. Click **Apply** to configure the NetShark VM.



You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller

Location: 1

Media

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk: ers\Public\Documents\Hyper-V\Virtual Hard Disks\NetShark-Packet-Storage.vhd

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

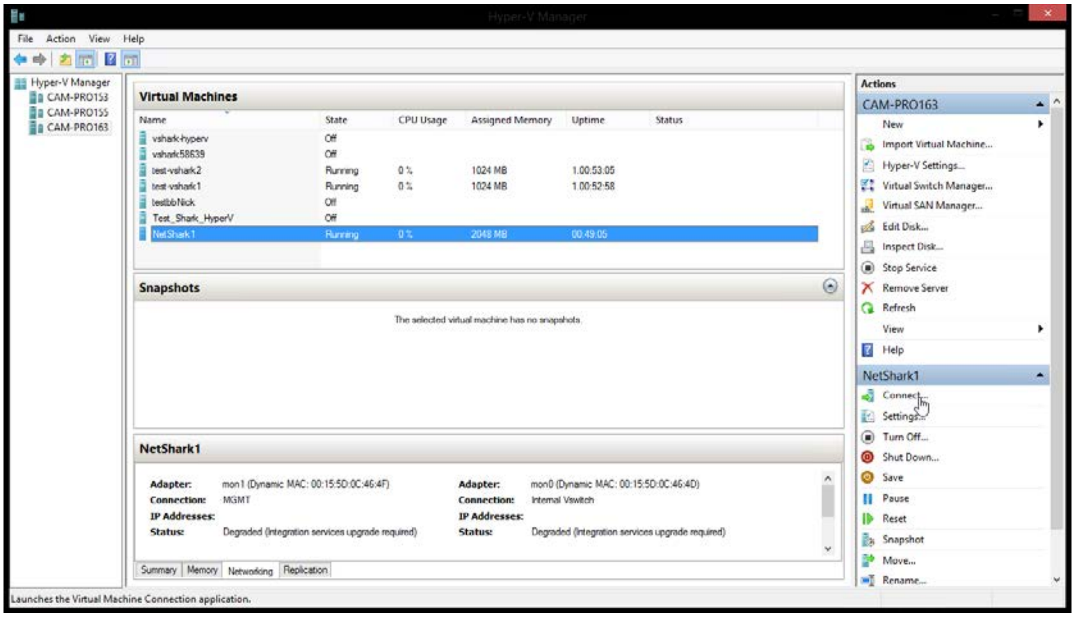
# Configuring the NetShark

## Setting up the initial configuration

The initial configuration sets up the IP address, password, time configuration, and other basic settings for the NetShark. You perform this configuration through the NetShark console port.

1. Start the NetShark. Open Hyper-V Manager and select the NetShark from the list of virtual machines. Under ***Actions***, click ***Start*** under your NetShark VM.

2. Click ***Connect*** to launch the NetShark console.



Virtual Machines

| Name | State | CPU Usage | Assigned Memory | Uptime | Status |
|---|---|---|---|---|---|
| vshark-hyperv | Off | | | | |
| vshark58639 | Off | | | | |
| test-vshark2 | Running | 0 % | 1024 MB | 1.00:53:05 | |
| test-vshark1 | Running | 0 % | 1024 MB | 1.00:52:58 | |
| testbbNick | Off | | | | |
| Test_Shark_HyperV | Off | | | | |
| NetShark1 | Running | 0 % | 2048 MB | 00:49:05 | |

Snapshots

The selected virtual machine has no snapshots.

NetShark1

**Adapter:** mon1 (Dynamic MAC: 00:15:5D:0C:46:4F)
**Connection:** MGMT
**IP Addresses:**
**Status:** Degraded (Integration services upgrade required)

**Adapter:** mon0 (Dynamic MAC: 00:15:5D:0C:46:4D)
**Connection:** Internal Vswitch
**IP Addresses:**
**Status:** Degraded (Integration services upgrade required)

Launches the Virtual Machine Connection application.

3. At the **`login:`** prompt, enter the default username and password.
   `login:` **`admin`**
   `password:` **`admin`**
   **Note:** Always keep a record of the login password.

4. At the console prompt, enter **wizard** to start the initial configuration wizard and then answer the questions presented.

   ```
   shark> wizard
   ```

   The setup wizard guides you through the initial configuration of the NetShark. Press **Enter** at any step to accept the current setting and move to the next step. A typical configuration dialog might look like this:

   ```
   Step 0: Hostname [shark]? NetShark1
   Step 1: Use DHCP for primary [yes]?
   Step 5: Enable aux [no]?
   Step 12: Timezone (type * for list) [America/Los_Angeles]? *
   Africa/            America/           Antarctica/        Arctic/
   Asia/              Atlantic/          Australia/         Etc/
   Europe/            Indian/            Pacific/
   Step 12: Timezone (type * for list) [America/Los_Angeles]? Australia/*
   Adelaide           Brisbane           Broken_Hill        Currie
   Darwin             Eucla              Hobart             Lindeman
   Lord_Howe          Melbourne          Perth              Sydney
   Step 12: Timezone (type * for list) [America/Los_Angeles]? Australia/Perth
   Step 13: Enable SSH [yes]? yes
   Step 14: Enable PTP [no]?
   Step 15: PTP Interface [primary]?
   Step 16: NTP server names [0.riverbed.pool.ntp.org,1.riverbed.pool.ntp.org,
   2.riverbed.pool.ntp.org,3.riverbed.pool.ntp.org]?
   ```

   The purposes of the steps in the setup wizard are as follows:

   Step 0 sets the hostname (without the domain). This name is used as the console prompt, and identifies the appliance in the NetShark Web user interface.

   Steps 1 through 4 configure the IP management network. Enter **yes** in Step 1 to use DHCP for the **primary** management port or **no** to use a static IP configuration, and press Enter. For a static IP configuration, use Step 2 to specify the IP address, Step 3 to specify the IP net mask, and Step 4 to specify the default gateway.

   Step 5 selects whether to use the second management port (**aux**). Note that in a standard installation **aux** is not needed. Enter **yes** to enable **aux**. If **aux** is enabled, Steps 6 through 9 configure **aux** for either DHCP or a static IP configuration.

   Steps 10 and 11 configure the DNS servers (as a comma- or space-separated list) and the domain name of the NetShark. If DHCP is used for the **primary** management network configuration, these steps are skipped (because they are configured by the DHCP server).

   Step 12 sets the time zone of the NetShark. Entering an asterisk ***** lists the available time zone areas. To list the specific time zones within an area (for example, Europe), enter the area followed by **/***. To specify a particular time zone, enter the full time zone including the area (for example, **Europe/Rome**). Use **Etc/*** to specify GMT time.

Step 13 enables or disables the remote shell (SSH). It is enabled by default.

Steps 14 and 15 select and configure the use of Precision Time Protocol (PTP) for clock synchronization (in version 10.6 or later of the software).

Step 16 defines the NTP server(s) used for clock synchronization. Enter one or more NTP server names or IP addresses, separated by commas or spaces.

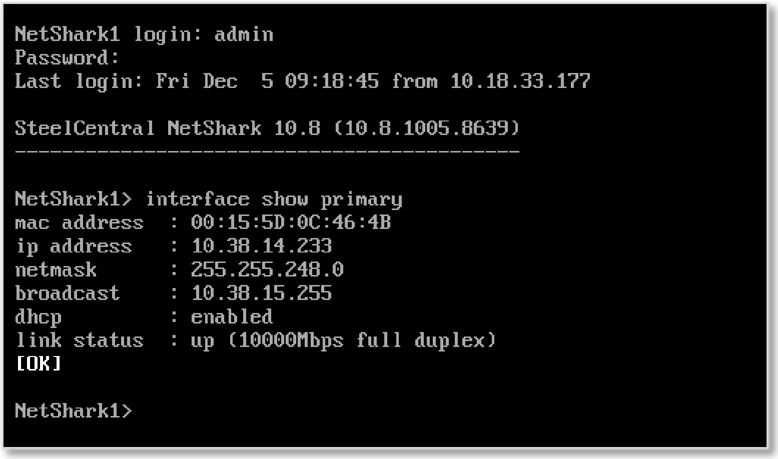
At the end of the configuration, the wizard prints out a summary of the parameters. Each step can be revisited by entering the step number. Entering an “s” saves the configuration, and entering a “c” cancels it.

```
To change an answer, enter the step number to return to.

Type 's' to save changes and exit

Type 'c' to exit without saving changes
```

5. Once the configuration is complete, enter `s` to save the configuration and exit.

   **Note:** A change to the host name, IP address, or time zone requires a reboot in order to take effect. The wizard asks for confirmation before rebooting NetShark. If you changed the name (the hostname entry in step 0) the new name will appear in the console prompt.

6. If you have used DHCP to provision an IP address for NetShark, at the console prompt enter **`interface show primary`** to find the IP address.



```
NetShark1 login: admin
Password:
Last login: Fri Dec  5 09:18:45 from 10.18.33.177

SteelCentral NetShark 10.8 (10.8.1005.8639)
-------------------------------------------

NetShark1> interface show primary
mac address  : 00:15:5D:0C:46:4B
ip address   : 10.38.14.233
netmask      : 255.255.248.0
broadcast    : 10.38.15.255
dhcp         : enabled
link status  : up (10000Mbps full duplex)
[OK]

NetShark1>
```

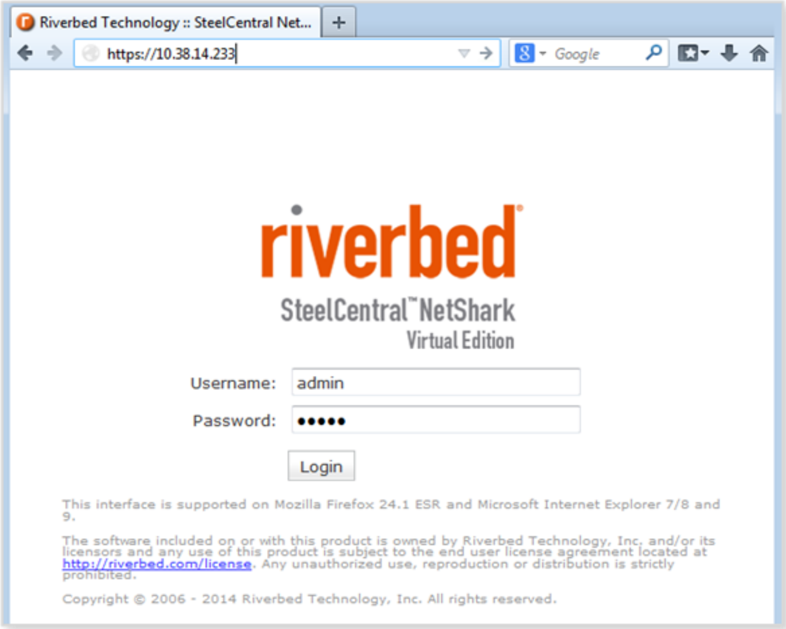
You use this address (or the DNS name of the NetShark) to connect to the NetShark Web user interface for subsequent NetShark configuration and operation.

# Logging in to the Web user interface

The Web user interface is a primary means of access to the NetShark. You use it for further configuration of the NetShark, as well as for normal operation.

Connect to the NetShark through its Web user interface. You can do this using your Web browser. The NetShark Web interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9. Make sure that SSL, cookies, and JavaScript are enabled in your browser.

Point your browser at https://<NetShark> where <NetShark> is the IP address or DNS name of the NetShark. Enter username and password, then click the Login button. (Default value is “admin” for both username  and password.)



Username: admin

Password: ●●●●●

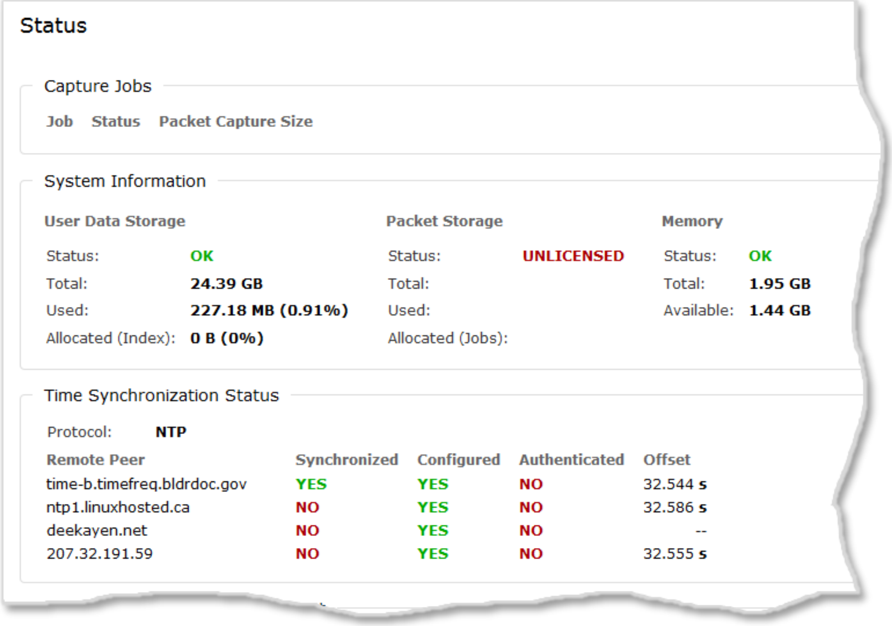
Login

This interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9.

The software included on or with this product is owned by Riverbed Technology, Inc. and/or its licensors and any use of this product is subject to the end user license agreement located at http://riverbed.com/license. Any unauthorized use, reproduction or distribution is strictly prohibited.

Copyright © 2006 - 2014 Riverbed Technology, Inc. All rights reserved.

When you have logged in to the Web user interface, you will see the **Status** page.



Status

Capture Jobs

| Job | Status | Packet Capture Size |
|---|---|---|

System Information

| User Data Storage | | Packet Storage | | Memory | |
|---|---|---|---|---|---|
| Status: | OK | Status: | UNLICENSED | Status: | OK |
| Total: | 24.39 GB | Total: | | Total: | 1.95 GB |
| Used: | 227.18 MB (0.91%) | Used: | | Available: | 1.44 GB |
| Allocated (Index): | 0 B (0%) | Allocated (Jobs): | | | |

Time Synchronization Status

Protocol: NTP

| Remote Peer | Synchronized | Configured | Authenticated | Offset |
|---|---|---|---|---|
| time-b.timefreq.bldrdoc.gov | YES | YES | NO | 32.544 s |
| ntp1.linuxhosted.ca | NO | YES | NO | 32.586 s |
| deekayen.net | NO | YES | NO | -- |
| 207.32.191.59 | NO | YES | NO | 32.555 s |

## Applying licenses

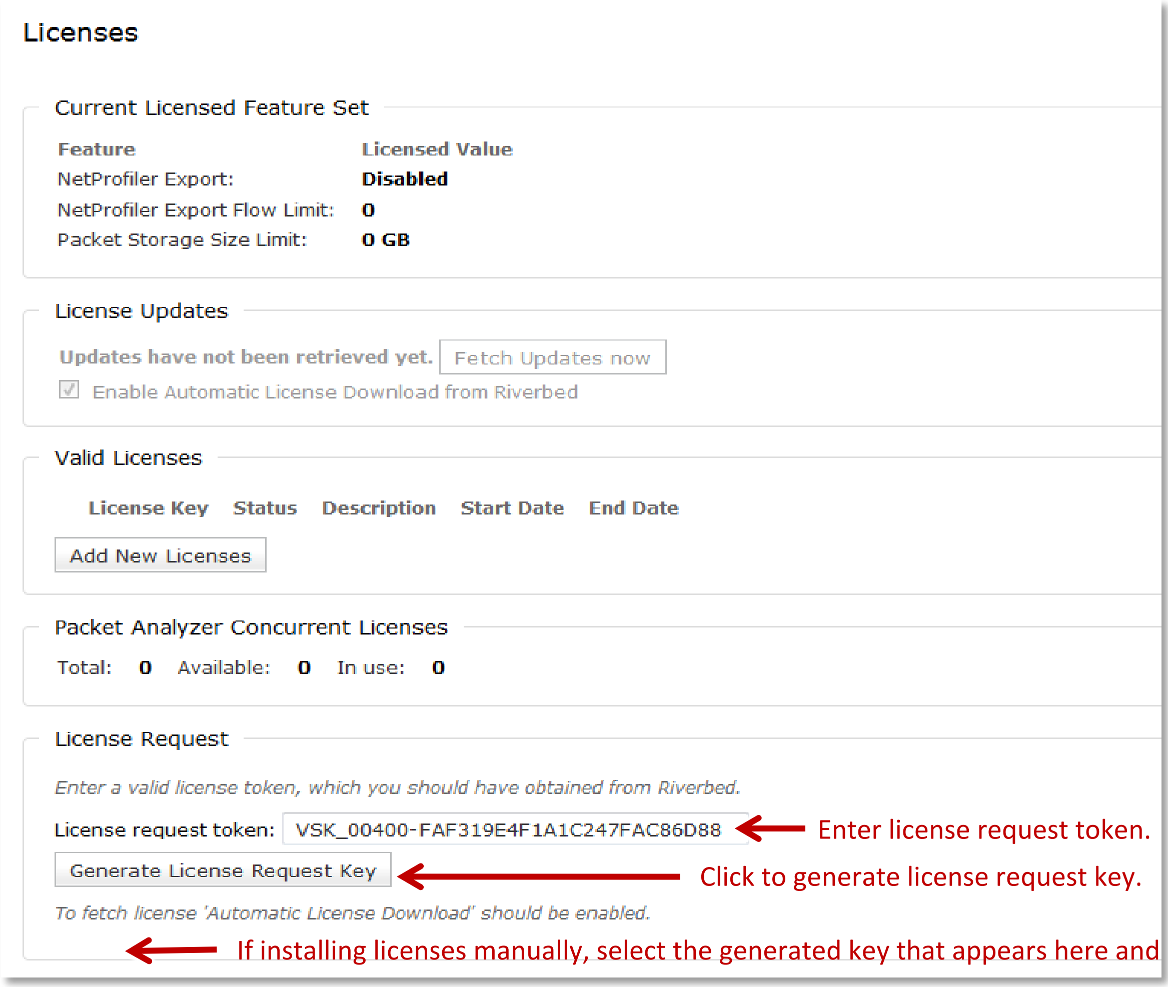
To use packet storage and other NetShark features on a NetShark you must apply licenses. You received a license request token when you purchased your NetShark. NetShark uses this token to obtain license keys from the Riverbed licensing Web site.

If the NetShark has been configured to be accessible on the network and if it has access to the Internet, auto-licensing is used to automatically download and update the license key(s). Otherwise, you can manually license your NetShark using the Riverbed licensing Web site.

1. Log in to the NetShark Web user interface.

2. Navigate to the System->Licenses page.

3. Paste or enter your license request token in the License Request section and click **Generate License Request Key**. The NetShark generates a license request key and displays it at the bottom of the page.



Licenses

Current Licensed Feature Set

| Feature | Licensed Value |
|---|---|
| NetProfiler Export: | **Disabled** |
| NetProfiler Export Flow Limit: | **0** |
| Packet Storage Size Limit: | **0 GB** |

License Updates

Updates have not been retrieved yet. Fetch Updates now

☑ Enable Automatic License Download from Riverbed

Valid Licenses

| License Key | Status | Description | Start Date | End Date |
|---|---|---|---|---|

Add New Licenses

Packet Analyzer Concurrent Licenses

Total: **0** Available: **0** In use: **0**

License Request

*Enter a valid license token, which you should have obtained from Riverbed.*

License request token: VSK_00400-FAF319E4F1A1C247FAC86D88

Generate License Request Key

*To fetch license 'Automatic License Download' should be enabled.*

Enter license request token.

Click to generate license request key.

If installing licenses manually, select the generated key that appears here and copy it.

If the NetShark has access to the Internet, licenses are automatically downloaded and installed.

The NetShark must be restarted to activate a license. A message in the upper right corner of the Licenses page allows you to restart or delay the restart of the NetShark to install licenses. Installed licenses are listed in the Valid Licenses section of the Licensing page.

If **Enable Automatic License Download from Riverbed** is enabled (the default after the first license is applied), the NetShark automatically connects to the Riverbed licensing Web site every 12 hours and downloads licenses that you have purchased. Uncheck the box to disable automatic retrieval of license updates.

The **Fetch Updates Now** button causes the NetShark to immediately connect to the Riverbed licensing Web site and download any new licenses that you have purchased.

If the NetExpress does not have Internet connectivity, you can install licenses manually.

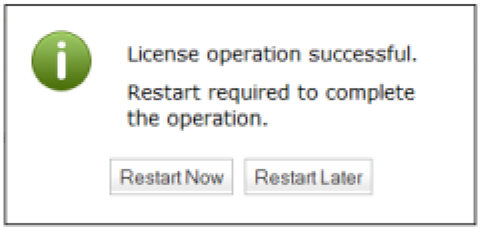
1. Copy the license request key displayed it at the bottom of the page.

2. Point your browser at the Riverbed licensing Web site, https://licensing.riverbed.com, and follow the process found there.

3. The licensing portal returns several license keys. You copy those license keys to the NetShark Licenses page.

4. On the **`Licenses`** page, click **`Add Licenses`**, then copy and paste the license keys into the window, one line per key. Click **`Add`** to add the keys to the NetShark**.**

5. When the keys have been added, the NetShark returns a completion message. Click ***Restart Now*** to restart the NetShark probe service.



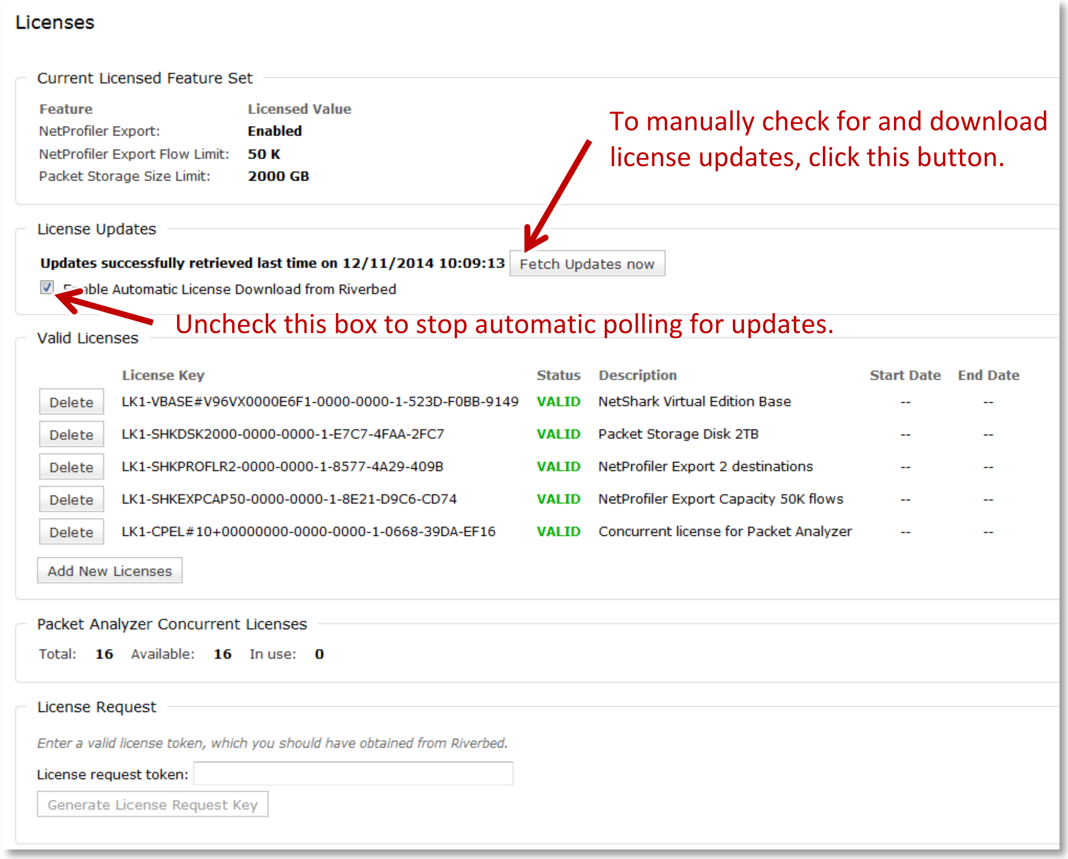
License operation successful.

Restart required to complete the operation.

6. After the NetShark probe service is restarted, the NetShark is fully licensed.

**Note:** If you purchase and download a license for a higher capacity than a current license, the NetShark uses the license with the higher capacity.

When licensing is completed all installed licenses are listed under Valid Licenses. Remove a license by clicking the **Delete** button next to its licensing key. If a NetShark is connected to the Web it can automatically or manually check for license updates



Licenses

Current Licensed Feature Set

| Feature | Licensed Value |
|---|---|
| NetProfiler Export: | **Enabled** |
| NetProfiler Export Flow Limit: | **50 K** |
| Packet Storage Size Limit: | **2000 GB** |

To manually check for and download license updates, click this button.

License Updates

**Updates successfully retrieved last time on 12/11/2014 10:09:13** Fetch Updates now

☑ Enable Automatic License Download from Riverbed

Uncheck this box to stop automatic polling for updates.

Valid Licenses

| | License Key | Status | Description | Start Date | End Date |
|---|---|---|---|---|---|
| Delete | LK1-VBASE#V96VX0000E6F1-0000-0000-1-523D-F0BB-9149 | VALID | NetShark Virtual Edition Base | -- | -- |
| Delete | LK1-SHKDSK2000-0000-0000-1-E7C7-4FAA-2FC7 | VALID | Packet Storage Disk 2TB | -- | -- |
| Delete | LK1-SHKPROFLR2-0000-0000-1-8577-4A29-409B | VALID | NetProfiler Export 2 destinations | -- | -- |
| Delete | LK1-SHKEXPCAP50-0000-0000-1-8E21-D9C6-CD74 | VALID | NetProfiler Export Capacity 50K flows | -- | -- |
| Delete | LK1-CPEL#10+00000000-0000-0000-1-0668-39DA-EF16 | VALID | Concurrent license for Packet Analyzer | -- | -- |

Add New Licenses

Packet Analyzer Concurrent Licenses

Total: **16** Available: **16** In use: **0**

License Request

*Enter a valid license token, which you should have obtained from Riverbed.*

License request token:

Generate License Request Key

## Additional Configuration

For operational configuration and use, including setting up capture jobs and setting up communication with NetProfiler appliances, refer to the *SteelCentral NetShark User's Guide* or the *SteelCentral Packet Analyzer Reference Manual*.

# Beyond the basics

## Adding or changing a monitor port

You can have up to four monitor ports in a NetShark virtual edition. The first monitor port, `mon0`, is configured as part of the initial deployment of the NetShark. You can configure additional monitor ports or reconfigure an existing monitor port by following the procedure below.

In general, the procedure for adding or changing a monitor port includes the following:

- Stopping the NetShark VM.
- Running the STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1 script.
- Selecting a new virtual switch to be monitored by a new monitor port, or selecting an already monitored virtual switch to change the VMs monitored by an existing monitor port.
- Selecting the VMs to monitor.

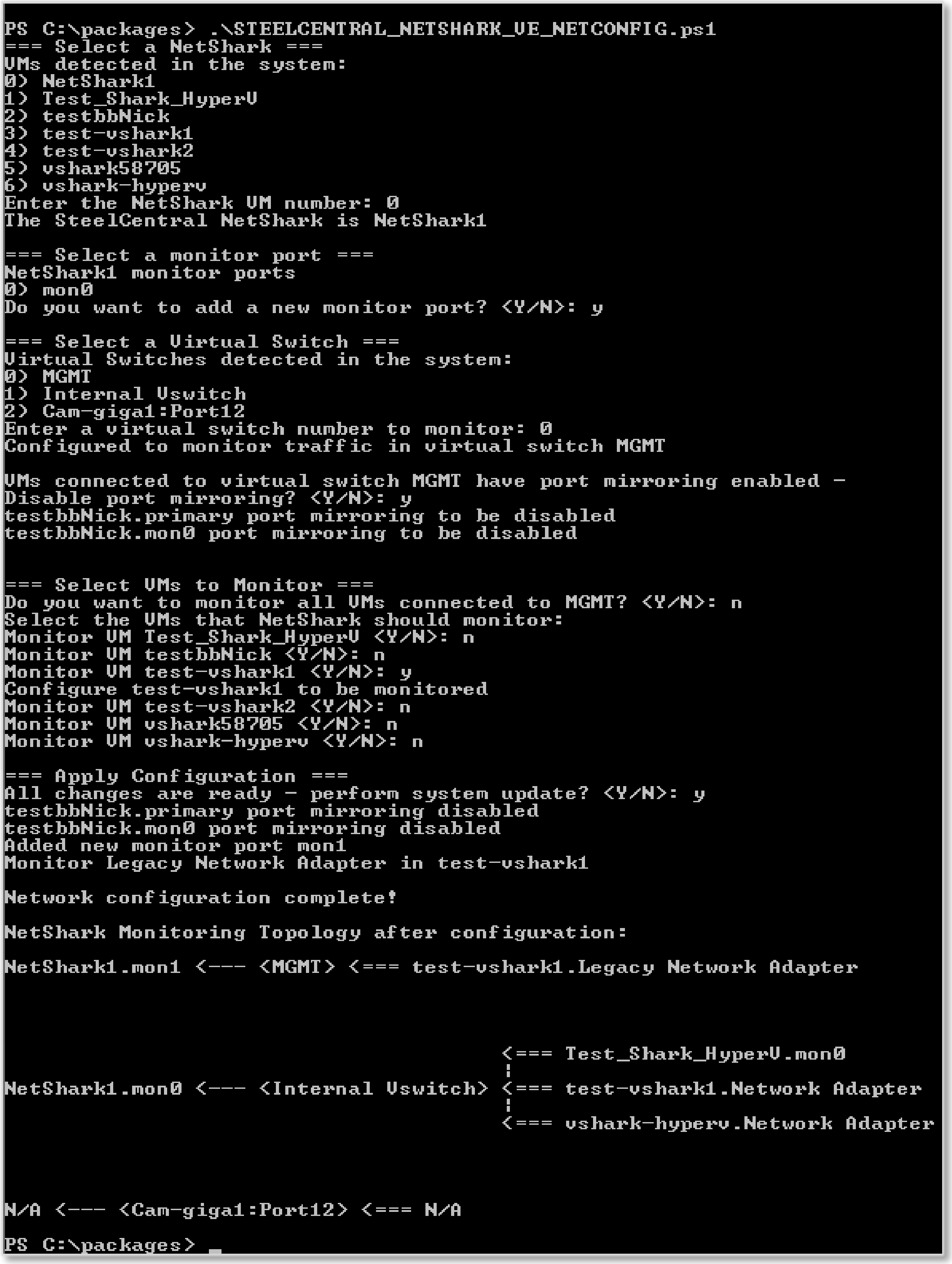
The rest of this section provides the detailed steps for adding or changing a monitor port.

### Adding a monitor port

The NetShark VM should be turned off before starting this procedure.

1. Run the PowerShell script STEELCENTRAL_NETSHA RK_VE_NETCONFIG.ps1 to configure a NetShark monitor port for a virtual switch and connected VM interfaces.
2. Select the NetShark. Choose the NetShark where you want to add the monitor port.
3. Select a monitor port. At **Add a new monitor port?**, enter “Y”. NetShark assigns monitor port names starting from `mon1` through `mon3`.
4. Select a Virtual Switch to monitor. As all mirrored traffic is sent to all mirror destination ports, if mirroring is currently enabled on a VM, determine if this mirrored traffic must continue. Select “Y” to disable or “N” to continue existing mirrored traffic from VMs.
5. Select VMs to monitor. You can monitor ingress and egress traffic for all VMs connected to a virtual switch by entering “Y” or select only specific VMs by entering “N.” Enter “N.”
6. Apply configuration. Enter “Y” to agree to make the configuration changes. A list of VMs to be monitored is displayed. Enter “N” to exit the script with no changes made.

   If you make a mistake or want to start over, enter **Ctrl-c** to exit the script without making any configuration changes.



```
PS C:\packages> .\STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1
=== Select a NetShark ===
VMs detected in the system:
0) NetShark1
1) Test_Shark_HyperV
2) testbbNick
3) test-vshark1
4) test-vshark2
5) vshark58705
6) vshark-hyperv
Enter the NetShark VM number: 0
The SteelCentral NetShark is NetShark1

=== Select a monitor port ===
NetShark1 monitor ports
0) mon0
Do you want to add a new monitor port? (Y/N): y

=== Select a Virtual Switch ===
Virtual Switches detected in the system:
0) MGMT
1) Internal Vswitch
2) Cam-giga1:Port12
Enter a virtual switch number to monitor: 0
Configured to monitor traffic in virtual switch MGMT

VMs connected to virtual switch MGMT have port mirroring enabled -
Disable port mirroring? (Y/N): y
testbbNick.primary port mirroring to be disabled
testbbNick.mon0 port mirroring to be disabled


=== Select VMs to Monitor ===
Do you want to monitor all VMs connected to MGMT? (Y/N): n
Select the VMs that NetShark should monitor:
Monitor VM Test_Shark_HyperV (Y/N): n
Monitor VM testbbNick (Y/N): n
Monitor VM test-vshark1 (Y/N): y
Configure test-vshark1 to be monitored
Monitor VM test-vshark2 (Y/N): n
Monitor VM vshark58705 (Y/N): n
Monitor VM vshark-hyperv (Y/N): n

=== Apply Configuration ===
All changes are ready - perform system update? (Y/N): y
testbbNick.primary port mirroring disabled
testbbNick.mon0 port mirroring disabled
Added new monitor port mon1
Monitor Legacy Network Adapter in test-vshark1

Network configuration complete!

NetShark Monitoring Topology after configuration:

NetShark1.mon1 <--- (MGMT) <=== test-vshark1.Legacy Network Adapter



                                       <=== Test_Shark_HyperV.mon0
                                       ¦
NetShark1.mon0 <--- (Internal Vswitch) <=== test-vshark1.Network Adapter
                                       ¦
                                       <=== vshark-hyperv.Network Adapter



N/A <--- (Cam-giga1:Port12) <=== N/A

PS C:\packages> _
```

In this example, a new NetShark1monitoring port, mon1, has been added to the MGMT virtual switch. One VM, test-vshark1, was selected to be monitored. The network interfaces on test-vshark1 mirror traffic to mon1.

## Changing a monitor port

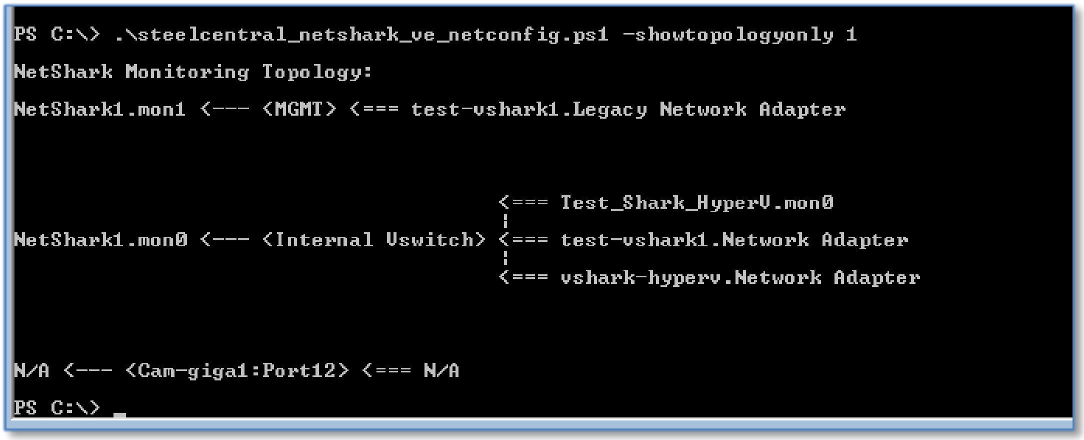
Run the STEELCENTRAL_NETSHA RK_VE_NETCONFIG.ps1 to add or remove VMs on a virtual switch being monitored by a NetShark monitor port. The script detects VMs with port mirroring enabled on the selected virtual switch and asks if you want to disable any existing port mirroring.

You can:

- Enter “Y” and disable any existing port mirroring on VM network interfaces. You can restore port mirroring on a VM when you configure the new or existing monitor port you have selected.
- Enter “N” and keep the existing port mirroring. Any new VMs you select to monitor are added to the existing VMs with port mirroring.
- Enter Ctrl c to close the script without making any changes.

The NetShark VM should be turned off before starting this procedure.

1. Review the currently configured NetShark monitor ports in the Hyper-V host network topology. Enter **`STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1 -ShowTopologyOnly 1`** on a PowerShell command line.



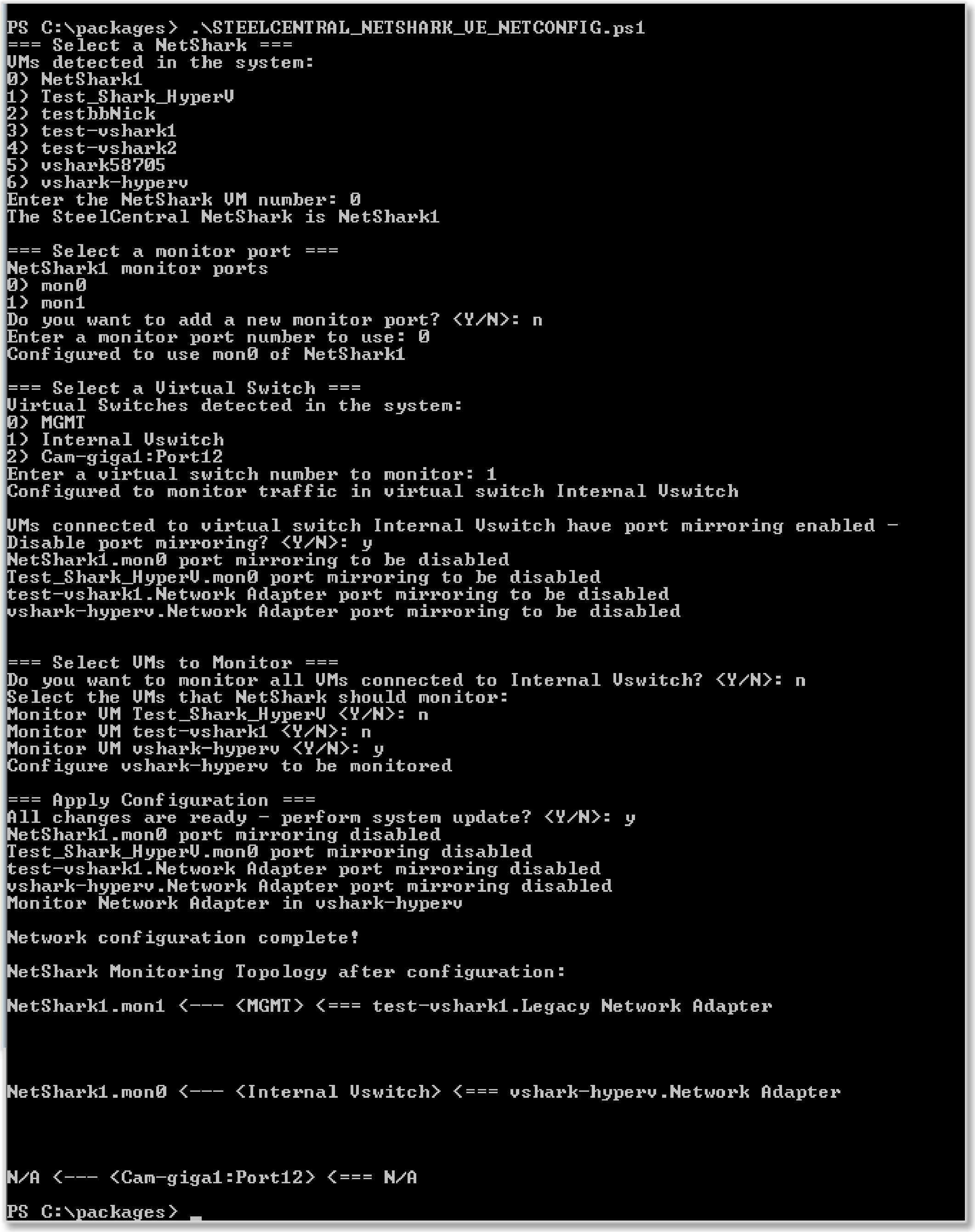
```
PS C:\> .\steelcentral_netshark_ve_netconfig.ps1 -showtopologyonly 1
NetShark Monitoring Topology:
NetShark1.mon1 <--- <MGMT> <=== test-vshark1.Legacy Network Adapter



                                       <=== Test_Shark_HyperV.mon0
                                       ¦
NetShark1.mon0 <--- <Internal Vswitch> <=== test-vshark1.Network Adapter
                                       ¦
                                       <=== vshark-hyperv.Network Adapter



N/A <--- <Cam-giga1:Port12> <=== N/A
PS C:\> _
```

   The example above shows the current NetShark1 monitor ports and their mapping to virtual switches and VMs on the switch. Virtual switches on the Hyper-V host without a monitor port, for example, `Cam-giga1:Port12`, are also shown in the topology.

2. Run the script again without the **`-ShowTopologyOnly 1`** parameter.
   In this example the monitor port `mon0` on virtual switch `Internal Vswitch` is changed to only monitor the network interfaces of the `vshark-hyperv` VM.
3. Select the NetShark. Select the NetShark with the monitor port you want to change.
4. Select a monitor port. At **Add a new monitor port?**, enter “N”.
5. Select the Virtual Switch.
6. Disable or keep existing VM port mirroring. For this example port mirroring is disabled on all VMs and then restored on `vshark-hyperv`. Enter “Y.”
7. Configure VM monitoring
   - If port mirroring was disabled, enter a new configuration for port monitoring on the virtual switch.
   - If port mirroring was kept, add new VMs to the current configuration.

8. Accept the changes and apply the configuration.

   The Network Topology shows the new configuration.



```
PS C:\packages> .\STEELCENTRAL_NETSHARK_VE_NETCONFIG.ps1
=== Select a NetShark ===
VMs detected in the system:
0> NetShark1
1> Test_Shark_HyperV
2> testbbNick
3> test-vshark1
4> test-vshark2
5> vshark58705
6> vshark-hyperv
Enter the NetShark VM number: 0
The SteelCentral NetShark is NetShark1

=== Select a monitor port ===
NetShark1 monitor ports
0> mon0
1> mon1
Do you want to add a new monitor port? <Y/N>: n
Enter a monitor port number to use: 0
Configured to use mon0 of NetShark1

=== Select a Virtual Switch ===
Virtual Switches detected in the system:
0> MGMT
1> Internal Vswitch
2> Cam-giga1:Port12
Enter a virtual switch number to monitor: 1
Configured to monitor traffic in virtual switch Internal Vswitch

VMs connected to virtual switch Internal Vswitch have port mirroring enabled -
Disable port mirroring? <Y/N>: y
NetShark1.mon0 port mirroring to be disabled
Test_Shark_HyperV.mon0 port mirroring to be disabled
test-vshark1.Network Adapter port mirroring to be disabled
vshark-hyperv.Network Adapter port mirroring to be disabled


=== Select VMs to Monitor ===
Do you want to monitor all VMs connected to Internal Vswitch? <Y/N>: n
Select the VMs that NetShark should monitor:
Monitor VM Test_Shark_HyperV <Y/N>: n
Monitor VM test-vshark1 <Y/N>: n
Monitor VM vshark-hyperv <Y/N>: y
Configure vshark-hyperv to be monitored

=== Apply Configuration ===
All changes are ready - perform system update? <Y/N>: y
NetShark1.mon0 port mirroring disabled
Test_Shark_HyperV.mon0 port mirroring disabled
test-vshark1.Network Adapter port mirroring disabled
vshark-hyperv.Network Adapter port mirroring disabled
Monitor Network Adapter in vshark-hyperv

Network configuration complete!

NetShark Monitoring Topology after configuration:

NetShark1.mon1 <--- <MGMT> <=== test-vshark1.Legacy Network Adapter



NetShark1.mon0 <--- <Internal Vswitch> <=== vshark-hyperv.Network Adapter



N/A <--- <Cam-giga1:Port12> <=== N/A

PS C:\packages> _
```

**Note:** If you disable port mirroring on all VMs being monitored on a virtual switch, the monitor port remains connected to the virtual switch and appears in the topology. You can reuse the monitor port by reconfiguring it to a new virtual switch.

## Contacting Riverbed

Options for contacting Riverbed include:

- Internet - Find out about Riverbed products at http://www.riverbed.com.
- Support - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Technical Support or your channel partner who provides support. To contact Riverbed Technical Support, please open a trouble ticket at https://support.riverbed.com or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.
- Professional Services - Riverbed has a staff of engineers who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom-coded solutions. To contact Riverbed Professional Services, go to http://www.riverbed.com or email proserve@riverbed.com.
- Documentation - Riverbed continually strives to improve the quality and usability of its documentation. We appreciate any suggestions you may have about our on line documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com