2

Working with the Virtual Services Platform

This chapter describes the Virtual Services Platform (VSP) feature. It includes the following sections:

Overview of VSP

With VSP, you can consolidate basic services in the branch (such as print, DNS, and DHCP services) to run in a dedicated partition on SteelHead EX systems.

VSP offers the following benefits:

- A VMware-based virtualization platform with the benefits of the most commonly deployed and advanced virtualization tool set. VSP uses ESXi 6.0 Express Patch 4 as the virtualization platform.
- Support for up to five virtual machines on a single SteelHead, depending on the service and SteelHead model.
- A simplified ESXi configuration through an installation wizard in the management console, as well as access by using the standard VMware administration tools, such as vSphere Client and vCenter.

VSP is included in the SteelHead EX functionality and does not require a separate download or license. You set up and manage VSP through the management console; you set up and configure virtual machines through vSphere.

Supported features

VSP on the SteelHead EX supports the basic features of VMware virtual machines, including the following:

- Virtual machine configuration through vSphere
- Stopping, starting, and restarting virtual machines through vSphere
- vSphere High Availability
- Reporting

VSP and virtual machines hosted on an SteelHead EX do not support advanced VMware features, including the following:

- vSphere vMotion
- vSphere Storage vMotion
- vSphere Fault Tolerance
- Backup/Restore

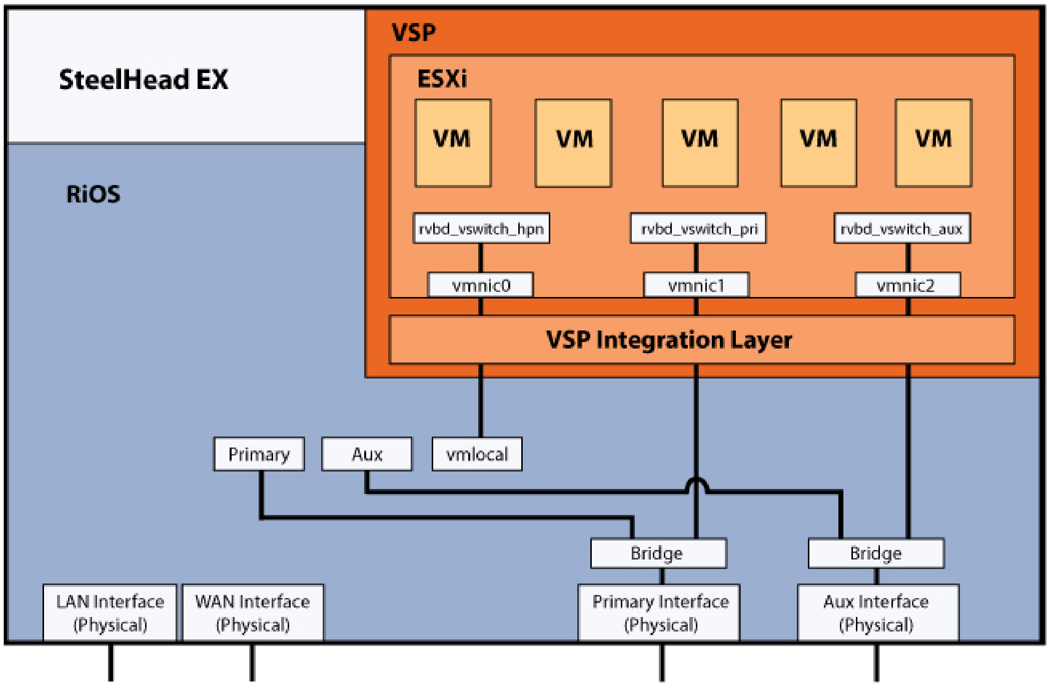
VSP architecture

VSP runs in a dedicated partition on the SteelHead EX. This partition is separate from the RiOS and traffic for the RiOS optimization is separate from VSP traffic.

Note: Starting in 3.1, Virtual Machines deployed in VSP can read traffic from AUX and Primary interfaces. This enables traffic monitoring programs that require promiscuous mode, such as NetShark-v, to run on VSP. You configure this feature through the Riverbed command-line interface using the **interface <interface-name> traffic-mode** command. For more information, see the *Riverbed Command-Line Interface Reference Manual*. You can also configure the AUX and Primary interface without an IP address if they are only monitoring VSP traffic.

You manage VSP and ESXi through the primary and auxiliary interfaces using VMware tools, such as the vSphere Client and vCenter.

Figure 2-1. VSP Architecture



Setting up the Virtual Services Platform

This section describes how to configure VSP and ESXi for the SteelHead EX. It includes the following topics:

- “Before you begin” on page 30
- “Configuring VSP” on page 30
- “Using the ESXi installation wizard” on page 33

Before you begin

Before you launch the installation wizard, configure the disk layout for VSP. To use VSP, ensure that you have allocated disk space to VSP. For details, see “Configuring disk management” on page 507.

Configuring VSP

You can configure VSP and ESXi from the EX Features > Virtualization: Virtual Services Platform page.

A configuration wizard guides you through the initial configuration of ESXi. After you run the wizard, you can customize additional settings on this page, such as the ESXi password and VNC access. You can also monitor the VSP current status and resource allocation from this page.

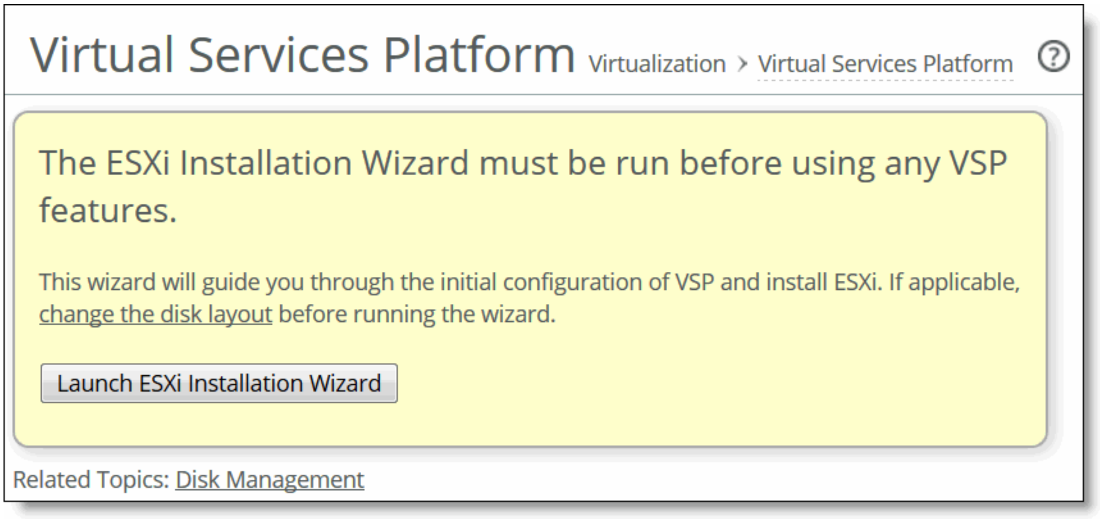
Note: During the ESXi installation, an HPN virtual switch on vnic0 is created. The switch has a kernel port and a virtual machine port. This switch is used for communication within the appliance. Do not modify or delete this virtual switch.

To configure VSP

1. Choose EX Features > Virtualization: Virtual Services Platform to display the Virtual Services Platform page.

2. If you have not configured ESXi for VSP, the Virtual Services Platform page displays an information message with a **Launch ESXi Installation Wizard** button.

Figure 2-2. Initial Launch of Configuration Wizard


Virtual Services Platform
Virtualization > Virtual Services Platform
?
Launch ESXi Installation Wizard

The ESXi Installation Wizard must be run before using any VSP features.

This wizard will guide you through the initial configuration of VSP and install ESXi. If applicable, change the disk layout before running the wizard.

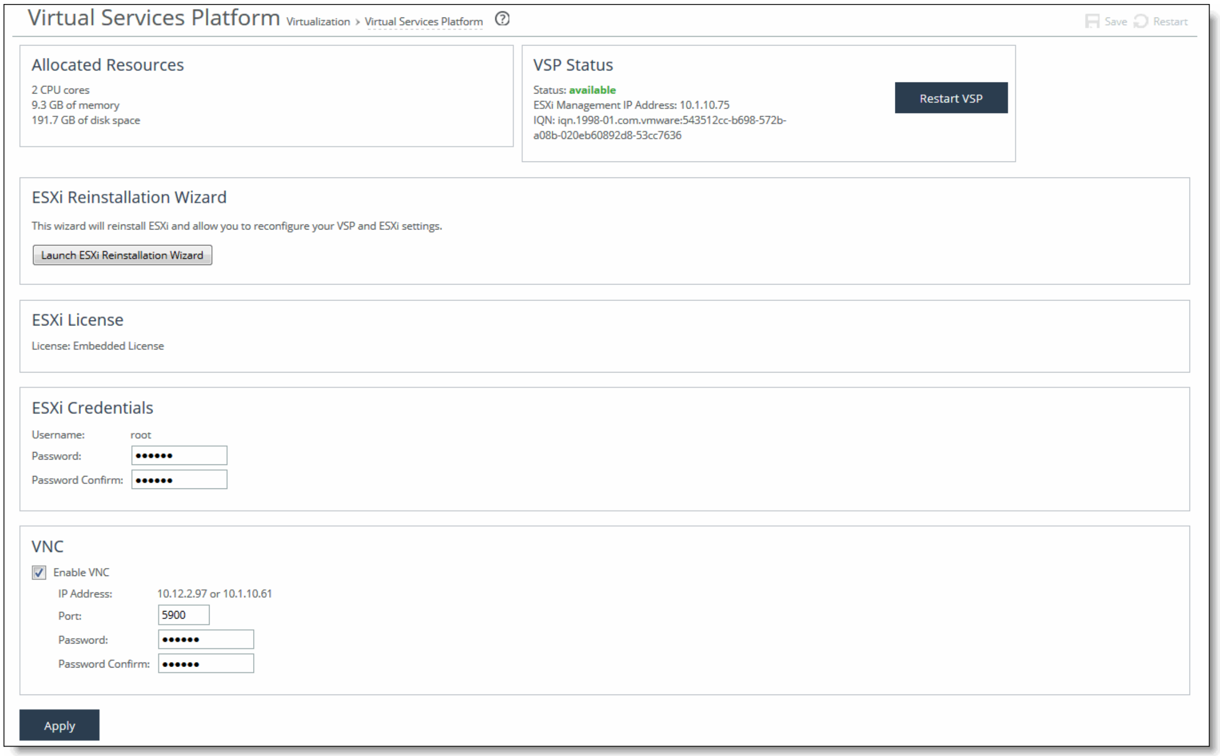
Related Topics: Disk Management

3. If necessary, run the Installation wizard.

   For details, see "Using the ESXi installation wizard" on page 33.

   After you have configured ESXi, the page displays a section for the ESXi wizard, displays the current status and resources, and provides access to additional settings.

Figure 2-3. Virtual Services Platform Configuration Page


Virtual Services Platform
Virtualization > Virtual Services Platform
?
Save
Restart
Restart VSP
Launch ESXi Reinstallation Wizard
Apply

Allocated Resources

2 CPU cores
9.3 GB of memory
191.7 GB of disk space

VSP Status

Status: available
ESXi Management IP Address: 10.1.10.75
IQN: iqn.1998-01.com.vmware:543512cc-b698-572b-a08b-020eb60892d8-53cc7636

ESXi Reinstallation Wizard

This wizard will reinstall ESXi and allow you to reconfigure your VSP and ESXi settings.

ESXi License

License: Embedded License

ESXi Credentials

Username: root
Password: ••••••
Password Confirm: ••••••

VNC

☑ Enable VNC
IP Address: 10.12.2.97 or 10.1.10.61
Port: 5900
Password: ••••••
Password Confirm: ••••••

4. To make additional changes after you run the Installation wizard, modify the VSP as described in this table.

Control	Description
ESXi Reinstallation Wizard	Launches a wizard that steps you through reinstalling ESXi with new settings. When you reinstall ESXi using this wizard, the new configuration overwrites any previous configuration changes made through vSphere and vCenter with the new settings from the wizard. The reinstallation wizard includes a Local Datastore page that asks if you want to erase and then re-create the local datastore. Use caution when selecting this option, as it deletes all data from the local datastore, including existing VMs, after you confirm. Riverbed recommends that you back up ESXi data before proceeding.
ESXi License	Click **Restore Default ESXi License** to replace the existing ESXi license with the default ESXi license, which does not have vCenter functionality.
ESXi Credentials	**Username** - Specifies the ESXi user name. **Password/Confirm Password** - Specify a password. The password must meet the default ESXi password complexity requirements. Confirm the password in the Password Confirm text box. **Important:** If you change the ESXi password in VNC or vSphere, you must also change it on this page. Changing the ESXi password using VNC or vSphere triggers the ESXi Communication Failed alarm in RiOS. When the passwords are not synchronized, RiOS cannot communicate with ESXi.
VNC	**Enable VNC** - Enables the use of a VNC (virtual network computing) client to connect to the direct console user interface (DCUI) of the ESXi server. **Port** - Specify a port. By default, a VNC client uses port 5900. **Password/Confirm Password** - Specify a password. The password must have a maximum of eight characters. Confirm the password in the Password Confirm text box. For details about using VNC, see "Managing virtual machines using VNC" on page 38.

5. Click **Apply**.

   The system copies the settings to the ESXi configuration.

6. Click **Restart VSP** to restart VSP.

   If you receive a warning that VSP is not in a safe state to restart, click **Cancel** to cancel the restart or **Continue** to proceed.

If you have installed a network card in slot 1 of the appliance and configured the card to use data interfaces, the VSP NIC Status table displays vmnic details. You can click an interface to view additional configuration details. For more details, see "Modifying data interfaces" on page 78.

Using the ESXi installation wizard

The VSP and ESXi installation wizard guides you through setting up your network settings, your local datastore, and your vCenter license (if applicable) and pushes these settings to the ESXi configuration.

Before running the installation wizard, configure the VSP disk space allocation, if necessary. For details, see “Configuring disk management” on page 507.

To set up ESXi using the installation wizard

1. Choose EX Features > Virtualization: Virtual Services Platform to display the Virtual Services Platform page.

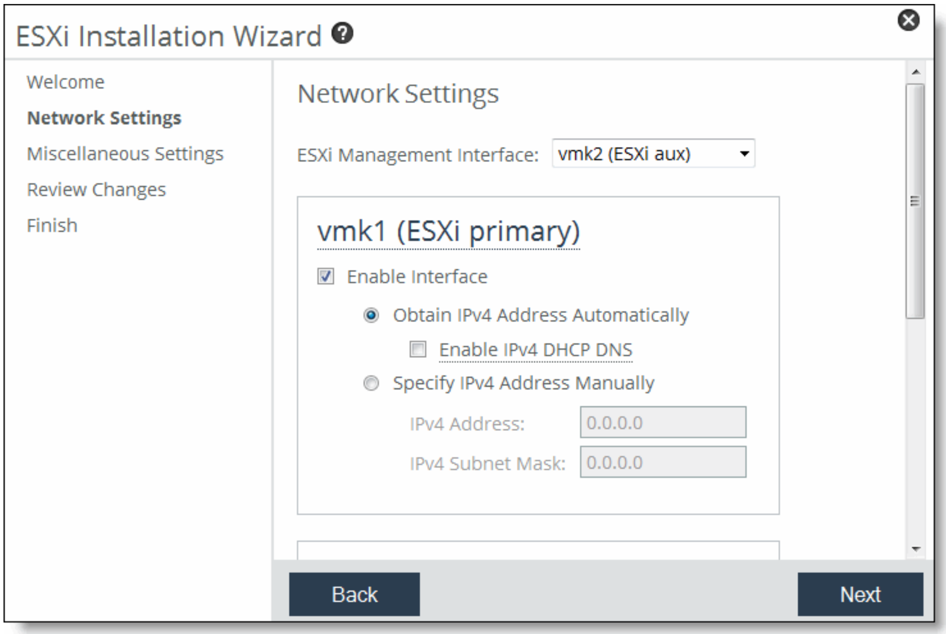
2. Click the button to launch the ESXi Installation Wizard.

   The ESXi Installation Wizard opens and displays the Welcome page.

3. Click **Next**.

   The Network Settings page appears.

Figure 2-4. Network Settings Page



ESXi Installation Wizard

Network Settings

ESXi Management Interface: vmk2 (ESXi aux)

vmk1 (ESXi primary)

☑ Enable Interface

● Obtain IPv4 Address Automatically

□ Enable IPv4 DHCP DNS

○ Specify IPv4 Address Manually

IPv4 Address: 0.0.0.0

IPv4 Subnet Mask: 0.0.0.0

4. Under Network Settings, complete the network configuration as described in this table.

Note: During the ESXi installation, an HPN virtual switch on vnic0 is created. The switch has a kernel port and a virtual machine port. This is used for communication within the appliance. Do not modify or delete this virtual switch.

You must specify IP address settings for the ESXi management interface.

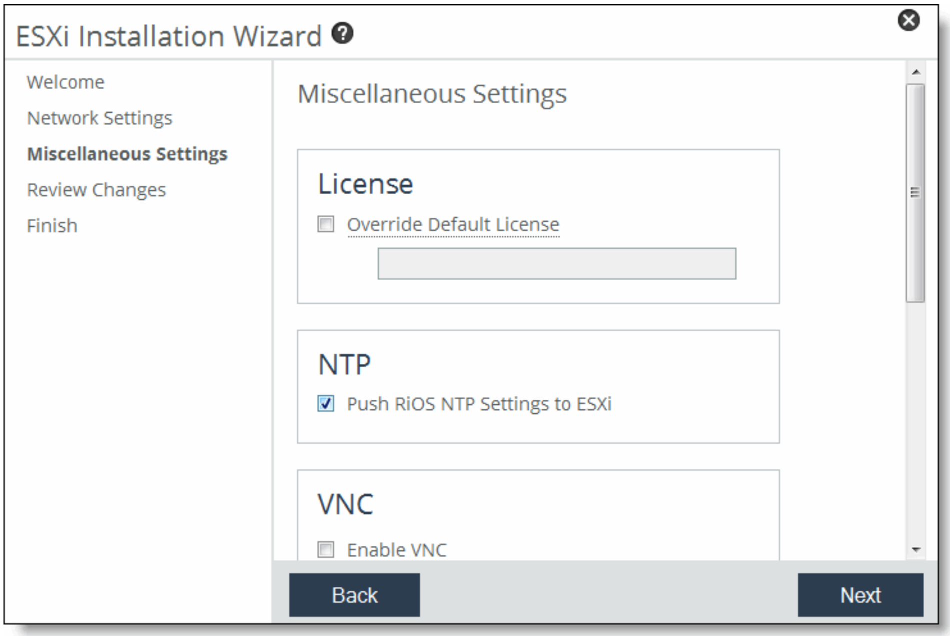
Control	Description
ESXi Management Interface	Select which interface (vmk1 for primary or vmk2 for auxiliary) you want to use for vSphere management access. The default is vmk1. When only one vmk interface is enabled, the wizard selects it automatically. If you disable a vmk interface and later decide to enable it, you must either manually create the vmk interface through vSphere or reinstall VSP.
Obtain IPv4 Address Automatically	Specify this option to automatically obtain the ESXi IPv4 address from a DHCP server. A DHCP server must be available so that the system can request the IP address from it. ▪ **Enable IPv4 DHCP DNS** - Select this option to enable IPv4 dynamic DNS. Dynamic DNS is a method, protocol, or network service that enables a network device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information.
Specify IPv4 Address Manually	Specify this option if you do not use a DHCP server to set the ESXi IP address. Specify the following: ▪ **IPv4 Address -** Specify an ESXi IPv4 address. Do not enter a RiOS IPv4 address. ▪ **IPv4 Subnet Mask -** Specify an IPv4 subnet mask. ▪ **IPv4 Gateway** - Specify an IPv4 gateway. The gateway field is available only for the interface that is currently selected as the ESXi management interface.

5. Click **Next.**

   The wizard validates the network settings, and the Miscellaneous Settings page appears.

If there is an error in the configuration, an error message appears and you must dismiss the message, correct your network settings, and click **Next** again to proceed to the Miscellaneous Settings page.

Figure 2-5. Miscellaneous Settings Page



Miscellaneous Settings

License

☐ Override Default License

NTP

☑ Push RiOS NTP Settings to ESXi

VNC

☐ Enable VNC

6. Complete the configuration as described in this table.

Control	Description
Override Default License	Specify a vCenter license to override the default ESXi license. The EX software includes a base ESXi license for you to manage your virtual machines, but this license does not include vCenter support. If you want to use vCenter for management, you must purchase a vCenter license from VMware and enter it here.
Push RiOS NTP Settings to ESXi	Select to use the NTP settings from RiOS for ESXi. By default, this is enabled.

Control	Description
VNC	**Enable VNC** - Enables the use of a VNC (Virtual Network Computing) client to connect directly to an ESXi host that is running on a SteelHead EX. **Port** - Specify a port. By default, a VNC client uses port 5900. **Password/Confirm Password** - Specify a password. The password must be a maximum of eight characters. Confirm the password in the Password Confirm text box. For details about using VNC, see "Managing virtual machines using VNC" on page 38.
ESXi Credentials	Specify and confirm the ESXi password. The password must meet the password requirements currently set in ESXi. **Important:** If you change the ESXi password using VNC or vSphere, you must change it in the Management Console. Changing the ESXi password using VNC or vSphere triggers the ESXi Communication Failed alarm in RiOS. When the passwords are not synchronized, RiOS cannot communicate with ESXi. To synchronize the passwords, enter the new password in the EX Features > Virtualization: Virtual Services Platform page.

7. Click **Next.**

   The confirmation page appears and displays the configuration settings for ESXi. The settings include both the values you specified in the wizard as well as default configuration settings optimized for ESXi with the SteelHead EX.

8. Review the changes.

9. Click **Install ESXi.**

   The system copies the settings to the ESXi configuration. This is a one-time, one-way transfer. The changes overwrite any changes that were made directly in ESXi outside of the wizard. You can make future changes to the ESXi configuration through vSphere and vCenter, but if you run the Installation Wizard again, it overwrites all the changes in ESXi with the new values from the wizard.

   The wizard places a green check mark next to each item as the installation completes, which takes approximately 10 minutes.

10. Click **Close** to close the wizard and return to the Management Console page.

    VSP and ESXi restart with the new values. VSP is now available and the page displays the current resource allocations and a VSP status of Available.

Managing ESXi and virtual machines with vSphere

The vSphere Client is a downloadable interface for administering ESXi and vCenter Server.

The vSphere Client user interface changes, depending on the server:

- When the server is an ESXi host, the vSphere Client displays only the options appropriate to single host management. SteelHead EX provides this capability without the need for a separate license.
- When the server is a vCenter Server system, the vSphere Client displays all the options available to the vSphere environment, according to the licensing configuration and the user permissions. To use vCenter, you need a separate license from VMware.

To manage the host with the vSphere Client and vCenter Server, you must install the applications on a computer with network access to the ESXi host. The ESXi host must be powered on and the VSP status must be available.

You can download the vSphere applications from the VMware website, or download the vSphere Client from the ESXi host.

To download the vSphere Client from the ESXi host

1. Connect to the ESXi host using the IP address for the vSphere management interface.

   This is the address used for ESXi management. The IP address appears in the VSP Status section of the EX Features > Virtualization: Virtual Services Platform page of the SteelHead Management Console.

   The VMware ESXi welcome page appears.

2. Click the link to download the vSphere Client.

To log in to the VSP ESXi host using vSphere

1. Start the vSphere Client.

2. In the IP Address / Name field, type the management IP address that appears in the VSP Status section of the EX Features > Virtualization: Virtual Services Platform page of the SteelHead Management Console.

3. For the user name, log in as **root**.

4. Enter the password you set up when you configured ESXi in the SteelHead Management Console.

5. Click **Login**.

   Security warning messages appear because the vSphere Client detects certificates signed by the ESXi host or vCenter Server system (default setting).

6. To ignore the security warnings that appear, click **Ignore**.

   The vSphere Client opens and displays information about the ESXi host.

To manage ESXi using vCenter

1. Start the vSphere Client.

2. In the vSphere Client login window, type the vCenter Server IP address or host name.

3. Type your user name and password.

4. Click **Login**.

   Security warning messages appear because the vSphere Client detects certificates signed by the ESXi host or vCenter Server system (default setting).

5. To ignore the security warnings that appear, click **Ignore.**

6. Add the ESXi host.

   vCenter discovers any virtual machines running on the host, as well as the server details.

Consult the VMware vSphere documentation for complete details about working with vSphere.

Creating and configuring virtual machines

After you have configured VSP and ESXi, you can add virtual machines using VMware tools. You can add a virtual machine to the SteelHead EX host by creating a new virtual machine or by deploying a virtual appliance. (A virtual appliance is a prebuilt virtual machine with an operating system installed.)

To learn how to add a virtual machine using VMware tools, go to the vSphere 6.0 Documentation Center at http://pubs.vmware.com/vsphere-60/index.jsp.

Helpful topics include:

- **Creating a Virtual Machine in vSphere Client**
  http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.hostclient.doc/GUID-7834894B-DD17-4D59-A9BF-A33D02478521.html

- **Deploying OVF Templates**
  http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vm_admin.doc/GUID-AFEDC48B-C96F-4088-9C1F-4F0A30E965DE.html

- **Configuring Virtual Machines**
  http://pubs.vmware.com/vsphere-60/topic/com.vmware.wssdk.pg.doc/PG_VM_Config.12.4.html

Managing virtual machines using VNC

You can use a VNC (virtual network computing) client to connect to the direct console user interface (DCUI) of the ESXi server. You can use a client such as TightVNC on a Windows or Linux host or client system.

VSP must be running and indicate an active status before you can connect to the ESXi host on the SteelHead EX with a VNC client.

To use a VNC client, configure VNC for VSP in the Management Console.

To enable VNC access

1. Choose EX Features > Virtualization: Virtual Services Platform.
2. Select Enable VNC.
3. Accept the default port of 5900 or specify another port.
4. Provide a password for VNC and confirm the password.
5. Click **Apply**.
6. Click **Restart.**

To connect to the ESXi host with a VNC client, start the VNC client application and specify the hostname or the IP address of the RiOS interface associated with the EXSi management interface, along with the VNC port number. For example, if you chose vmk1 (ESXi primary) as the ESXi management interface, enter the RiOS primary IP address to get VNC access to ESXi.

After you connect to the ESXi host, you must log in. Log in as **root** and use the password specified in the Management Console.

If you do not see the ESXi console after connecting with the VNC client, check your VNC display settings or try another VNC client.

Using the VNC client

From the VNC, you have the following options:

- **Configure Password** - Set the password.

  Changing the ESXi password using VNC or vSphere Management triggers the ESXi Communication Failed alarm in RiOS. When the passwords are not synchronized, RiOS cannot communicate with ESXi. To synchronize the passwords, enter the new password in the EX Features > Virtualization: Virtual Services Platform page.
- **Configure Management Network** - View or modify the host's network management settings.
- **Restart Management Network** - Restart the management interface and obtain or renew the DHCP lease.
- **Test Management Network** - Perform a brief network test.
- **Restore Network Setting** - Revert all network configuration values to their default values.
- **Configure Keyboard** - Select the layout type of the keyboard.
- **Troubleshooting Options** - View or change the state of ESXi troubleshooting options, such as ESXi Shell, SSH, and Restart Agents.
- **View System Logs** - View log files for the system, such as Syslog, Vmkernel, Config, Management Agent, VirtualCenter Agent, and VMware ESXi Observation.
- **View Support Information** - View information such as serial number, license serial number, SSL thumbprint, and SSH DSA key fingerprint.

- **Reset System Configuration** - Revert all system parameters to their software defaults, including resetting the root password.
- **Shut down/Restart** - Shut down or restart the ESXi platform.

Adding SteelFusion Edge as an ESXi datastore

This section describes how to configure ESXi to connect to and use a SteelFusion LUN as a VM datastore. If you use the VSP standalone storage mode without SteelFusion, you do not need to follow this procedure. The local VSP datastore configuration is complete, and you can begin deploying VMs to that datastore. For details about storage modes, see "Configuring disk management" on page 507.

The VM datastores provide storage locations for VM files. You can store and host VMs in a local datastore, and you can store and host VMs in a datastore on the projected SteelFusion LUN at the data center location.

The VM datastores are not related to the RiOS data stores that the SteelHead uses for SDR optimization.

Before you begin

Before you configure SteelFusion Edge as an ESXi datastore, complete the following configuration tasks:

- **Configure SteelFusion Core** - Make sure that the SteelFusion Core communicates with the backend storage, the SteelFusion Edge communicates with the SteelFusion Core, and the system optimizes SteelFusion traffic.
- **Provision the Logical Unit Numbers (LUNs)** - On the Core, provision at least one LUN to the Edge and allow the ESXi iSCSI initiator access to connect to this LUN.

For details, see the *SteelFusion Core Management Console User's Guide*.

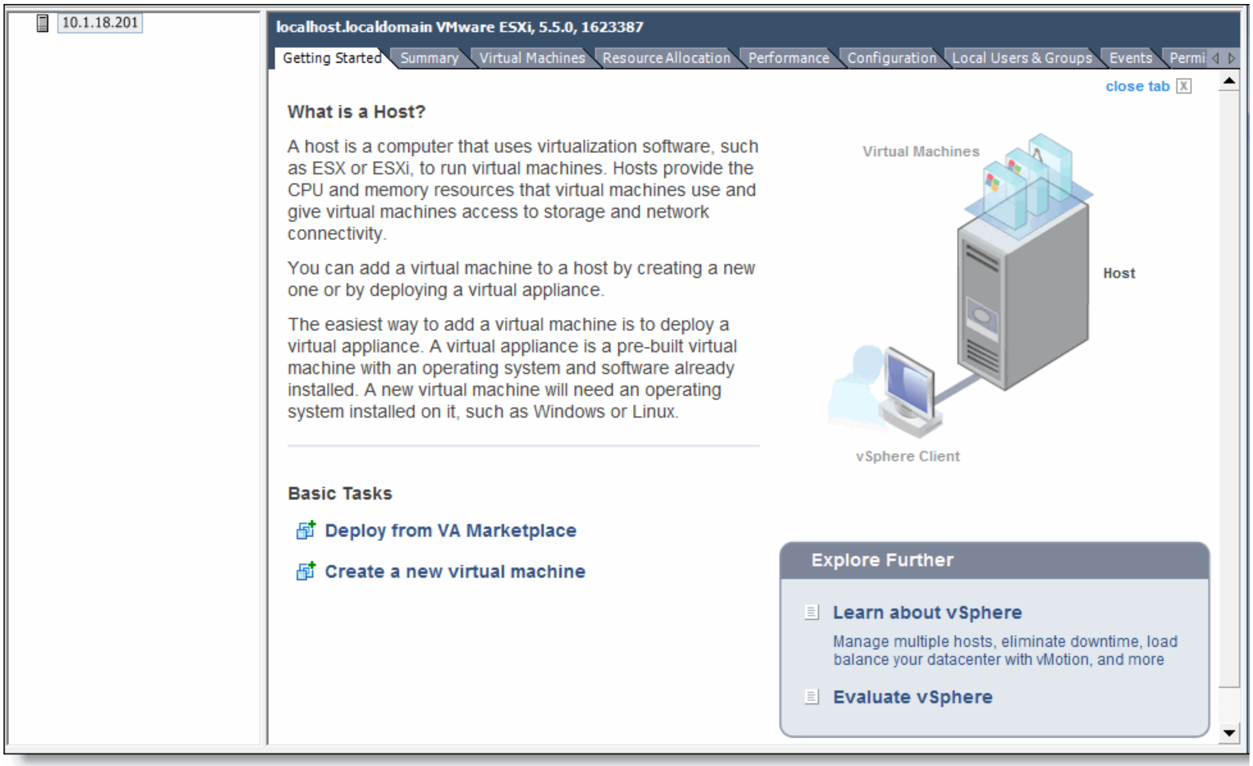
Provisioning a LUN from remote storage

You can provision a LUN from remote storage accessible through iSCSI, or provision a LUN from local storage on the appliance. This section provides the steps for provisioning a LUN projected by the SteelFusion Core and accessed through iSCSI.

To provision a LUN from remote storage using iSCSI

1. On the ESXi VSP host, start the vSphere Client.

Figure 2-6. vSphere Client Getting Started Page



What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

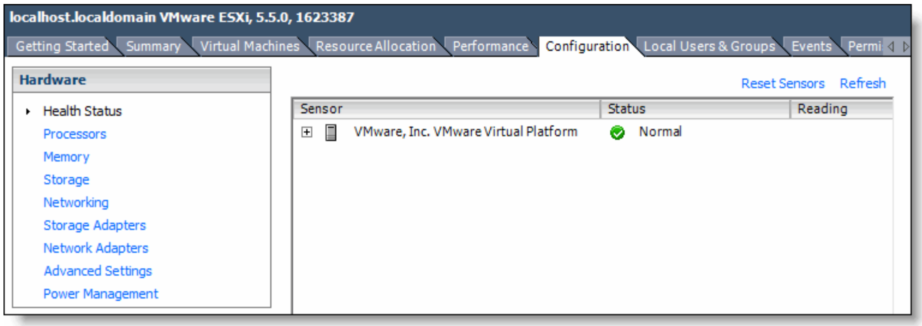
The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

2. Select the Configuration tab.

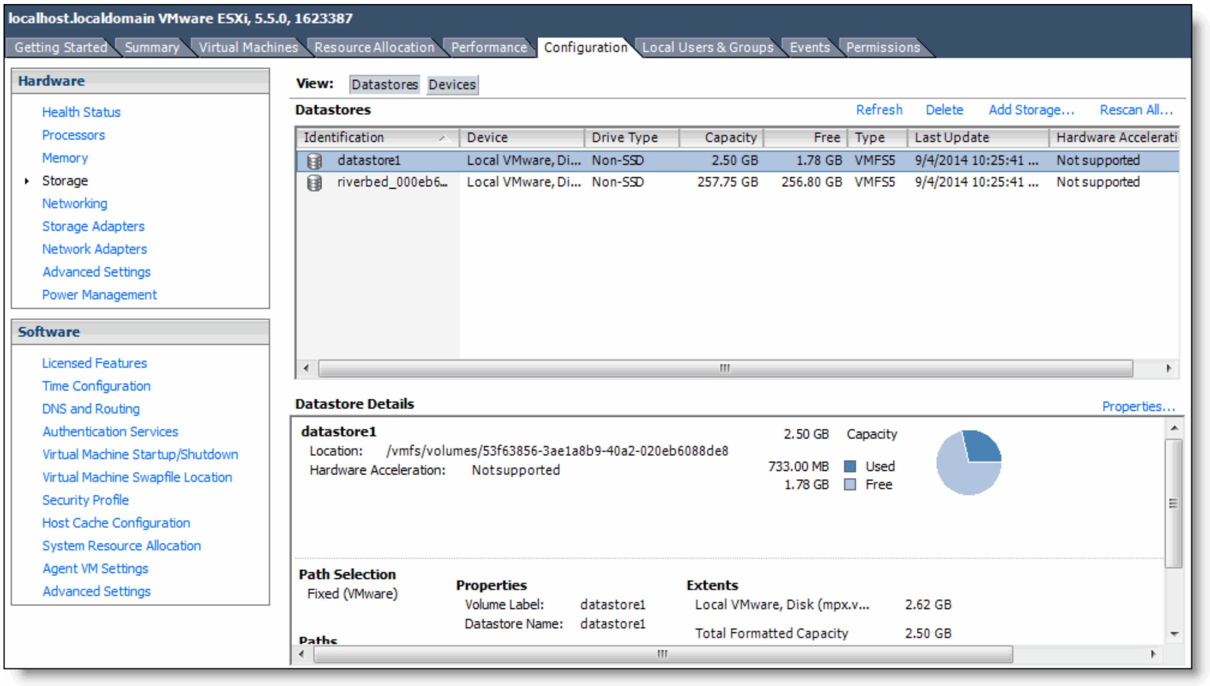
Figure 2-7. vSphere Client Configuration Tab



Sensor	Status	Reading
VMware, Inc. VMware Virtual Platform	Normal	

3. Under Hardware, select Storage.

Figure 2-8. vSphere Client Storage Display



Datastores

Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Accelerati
datastore1	Local VMware, Di...	Non-SSD	2.50 GB	1.78 GB	VMFS5	9/4/2014 10:25:41 ...	Not supported
riverbed_000eb6...	Local VMware, Di...	Non-SSD	257.75 GB	256.80 GB	VMFS5	9/4/2014 10:25:41 ...	Not supported

Datastore Details

datastore1
Location: /vmfs/volumes/53f63856-3ae1a8b9-40a2-020eb6088de8
Hardware Acceleration: Not supported

2.50 GB Capacity
733.00 MB ■ Used
1.78 GB □ Free

Path Selection
Fixed (VMware)

Properties
Volume Label: datastore1
Datastore Name: datastore1

Extents
Local VMware, Disk (mpx.v... 2.62 GB
Total Formatted Capacity 2.50 GB

Paths

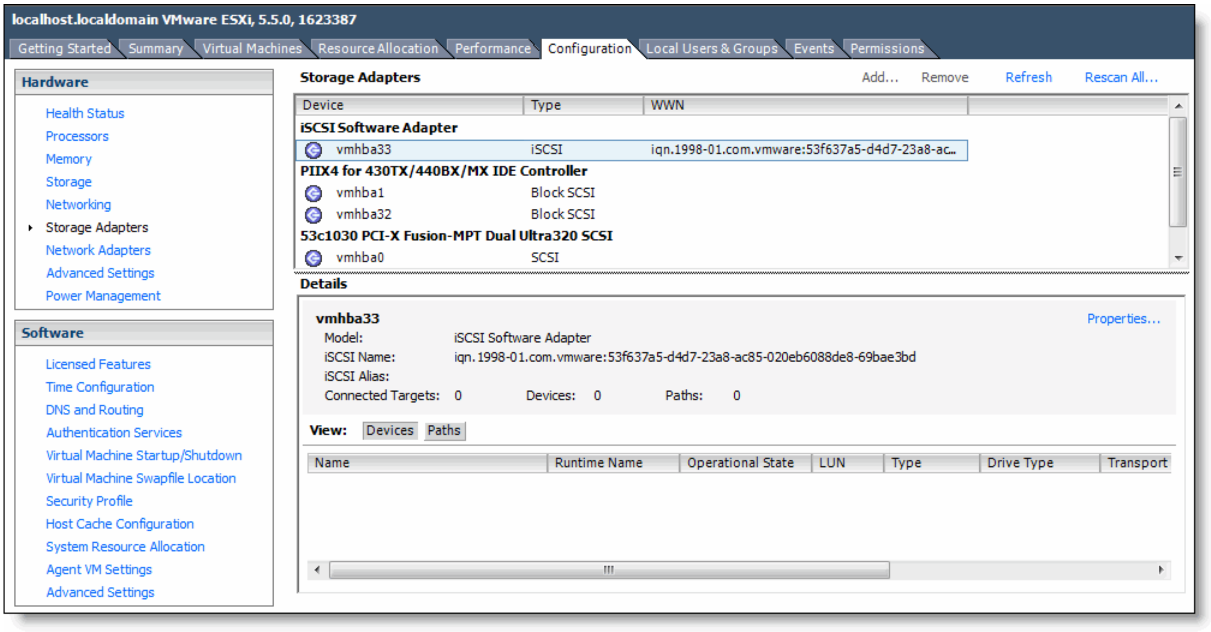
The page displays any VM datastores configured for the ESXi server, along with details such as the amount of used and available storage. The amount of storage varies depending on the disk layout configuration. For example, if you are using the VSP standalone storage mode, there is more storage available than if you are using the SteelFusion only storage mode.

SteelFusion LUNs do not appear by default, because ESXi does not yet know which LUNs to mount as a VM datastore. You configure the LUNs in SteelFusion Core. For details, see the *SteelFusion Core Management Console User's Guide*.

When the LUN is ready to go through iSCSI, you configure the ESXi host to add storage. To view the SteelFusion LUNs that you can configure to communicate with the iSCSI target, log in to the SteelFusion Core appliance and choose Configure > Manage: SteelFusion Edges. Click the Edge device name and select the LUNs tab to view the LUNs. The LUN you use as the VM datastore target must allow iSCSI initiator access.

4. Under Hardware, select Storage Adapters.

Figure 2-9. vSphere Client Storage Adapters



Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:53f637a5-d4d7-23a8-ac...
PIIX4 for 430TX/440BX/MX IDE Controller		
vmhba1	Block SCSI	
vmhba32	Block SCSI	
53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI		
vmhba0	SCSI	

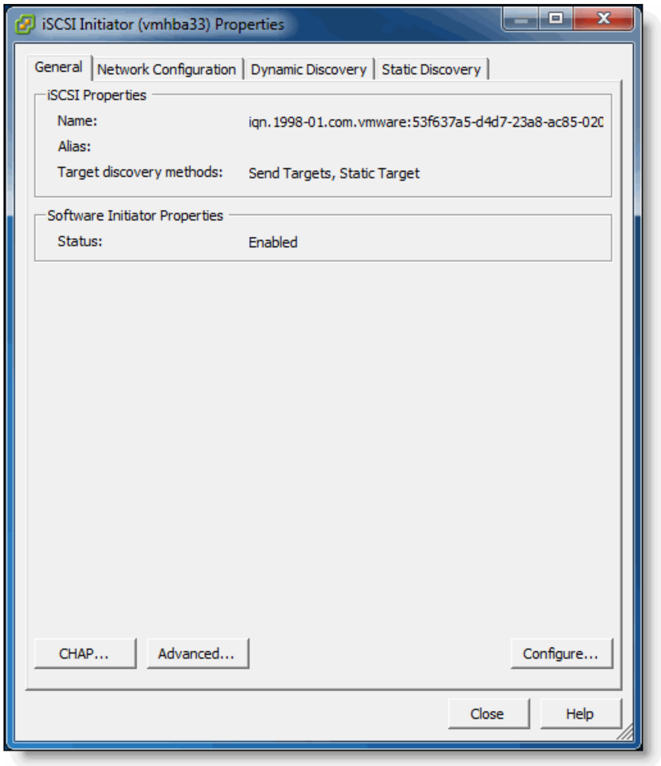
vmhba33
Model: iSCSI Software Adapter
iSCSI Name: iqn.1998-01.com.vmware:53f637a5-d4d7-23a8-ac85-020eb6088de8-69bae3bd
iSCSI Alias:
Connected Targets: 0 Devices: 0 Paths: 0

Name	Runtime Name	Operational State	LUN	Type	Drive Type	Transport

5. Select the iSCSI software adapter to configure.

6. Select Properties.

Figure 2-10. iSCSI Software Adapter Properties

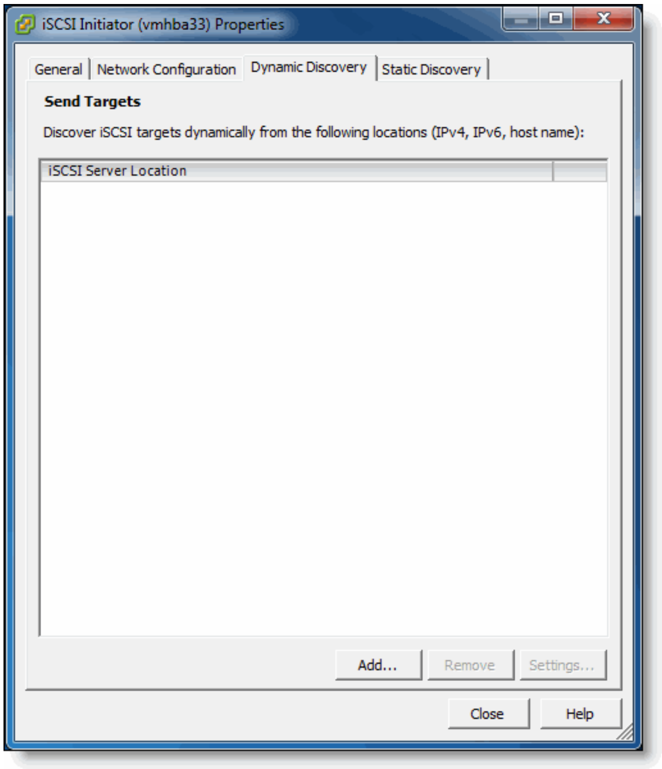


iSCSI Properties
Name: iqn.1998-01.com.vmware:53f637a5-d4d7-23a8-ac85-02C
Alias:
Target discovery methods: Send Targets, Static Target

Software Initiator Properties
Status: Enabled

7. Select the Dynamic Discovery tab.

Figure 2-11. iSCSI Dynamic Discovery tab



Send Targets

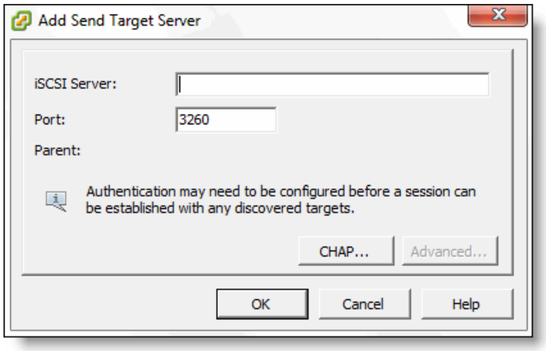
Discover iSCSI targets dynamically from the following locations (IPv4, IPv6, host name):

8. Click **Add**.

9. Enter the IP address of the SteelFusion Edge iSCSI network portal. The SteelFusion Edge is listening on all of the interfaces that have been added as multi-path I/O (MPIO) interfaces. Riverbed recommends that you enter the IP address of the primary interface, as this is the default MPIO interface. The iSCSI target on the SteelFusion Edge automatically exposes the relevant network portals to ESXi to ensure the closest and most optimal path for the I/O.

   For details about enabling MPIO interfaces, see the *SteelFusion Core Management Console User's Guide*.

Figure 2-12. Add Send Target Server



iSCSI Server:

Port: 3260

Parent:

Authentication may need to be configured before a session can be established with any discovered targets.

10. Click **OK** and then **Close**.

11. When asked to rescan the adapter, click **Yes**.

    The LUNs from SteelFusion Core appear under iSCSI software adapter. The ESXi server is targeting the SteelFusion Edge as an iSCSI target.

Provisioning a LUN from local storage

You can provision a LUN from remote storage accessible through iSCSI, or provision a LUN from local storage on the SteelFusion Edge appliance. This section provides the steps for provisioning an LUN from available space on the SteelFusion Edge appliance local disk storage.

To provision a LUN from local storage

- Launch the SteelFusion Core management console and provision a local LUN, ensuring that the initiator on the ESXi host is granted access to the LUN. For details, see the *SteelFusion Core Management Console User's Guide*.

Creating a datastore on the LUN

After provisioning a LUN to your ESXi server, you can create a datastore on the LUN for running virtual machines and storing virtual machine data.

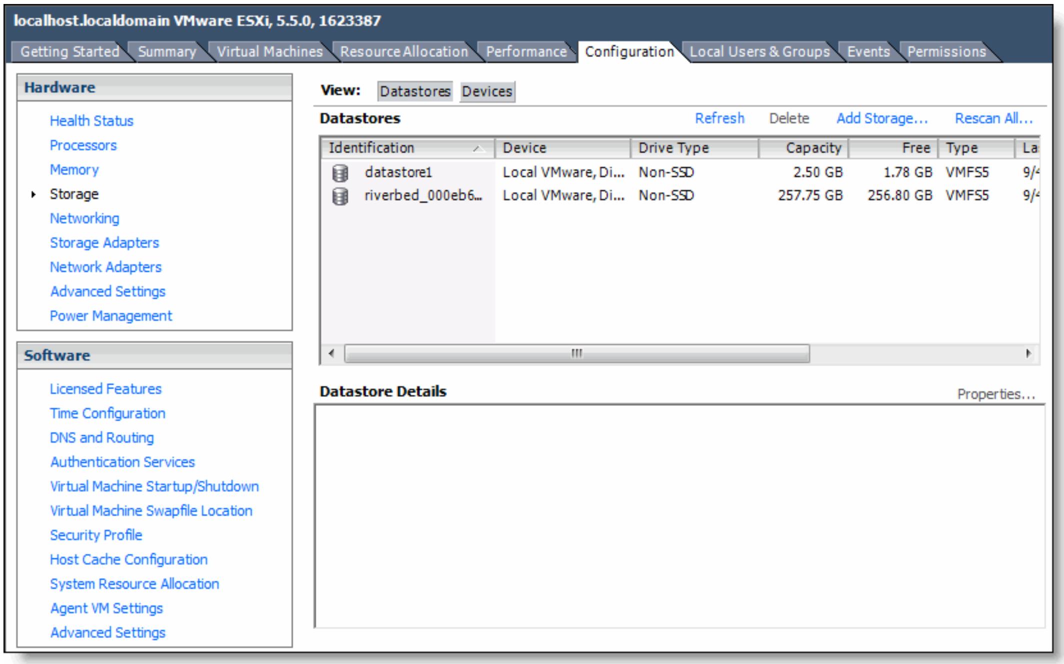
To create a new datastore on the LUN

1. Launch a vSphere Client and connect to your ESXi host.

2. Navigate to the Configuration tab.

3. Under Hardware, select Storage and then click the Datastores view.

Figure 2-13. Datastore List



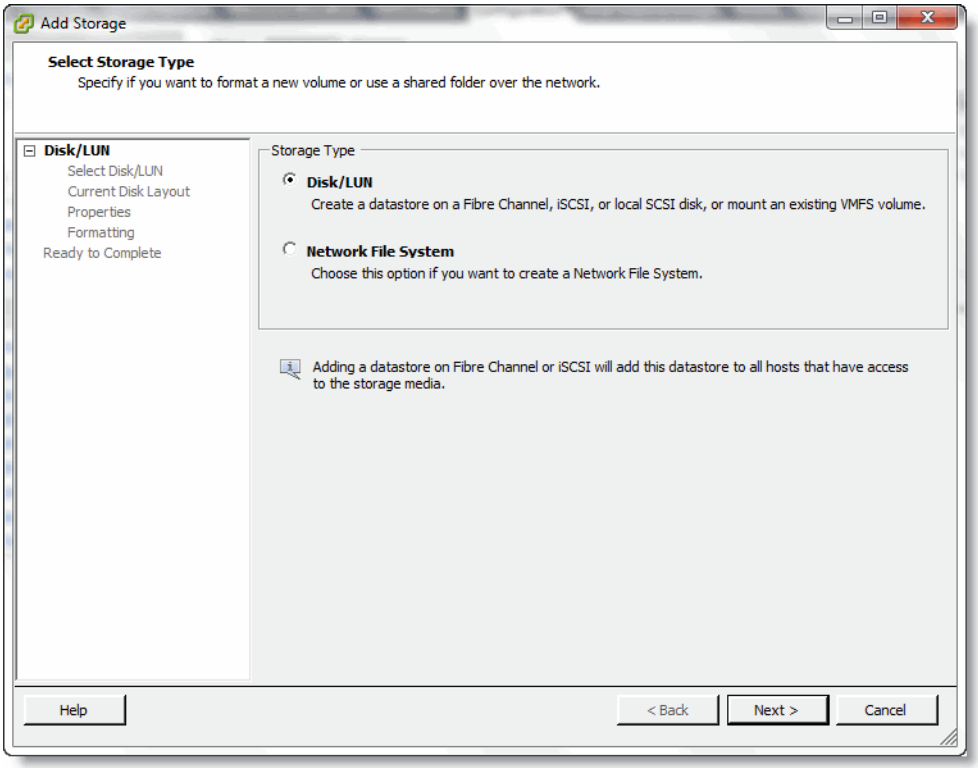
Identification	Device	Drive Type	Capacity	Free	Type	La
datastore1	Local VMware, Di...	Non-SSD	2.50 GB	1.78 GB	VMFS5	9/
riverbed_000eb6...	Local VMware, Di...	Non-SSD	257.75 GB	256.80 GB	VMFS5	9/

4. Click **Rescan All.**

5. Click **Add Storage**.

6. Select Disk/LUN and click **Next**.

Figure 2-14. Selecting a Storage Type



Add Storage

Select Storage Type

Specify if you want to format a new volume or use a shared folder over the network.

Storage Type

● **Disk/LUN**

Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume.

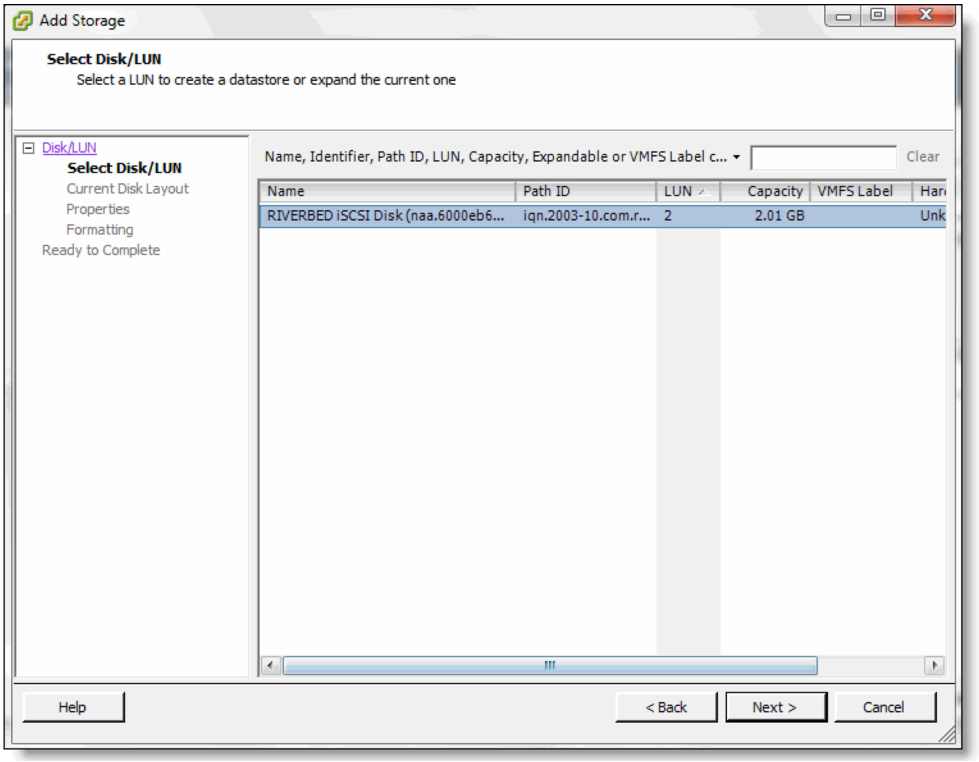
○ **Network File System**

Choose this option if you want to create a Network File System.

Adding a datastore on Fibre Channel or iSCSI will add this datastore to all hosts that have access to the storage media.

7. Select the LUN and click **Next**.

Figure 2-15. LUN Selection



Add Storage

Select Disk/LUN

Select a LUN to create a datastore or expand the current one

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c...

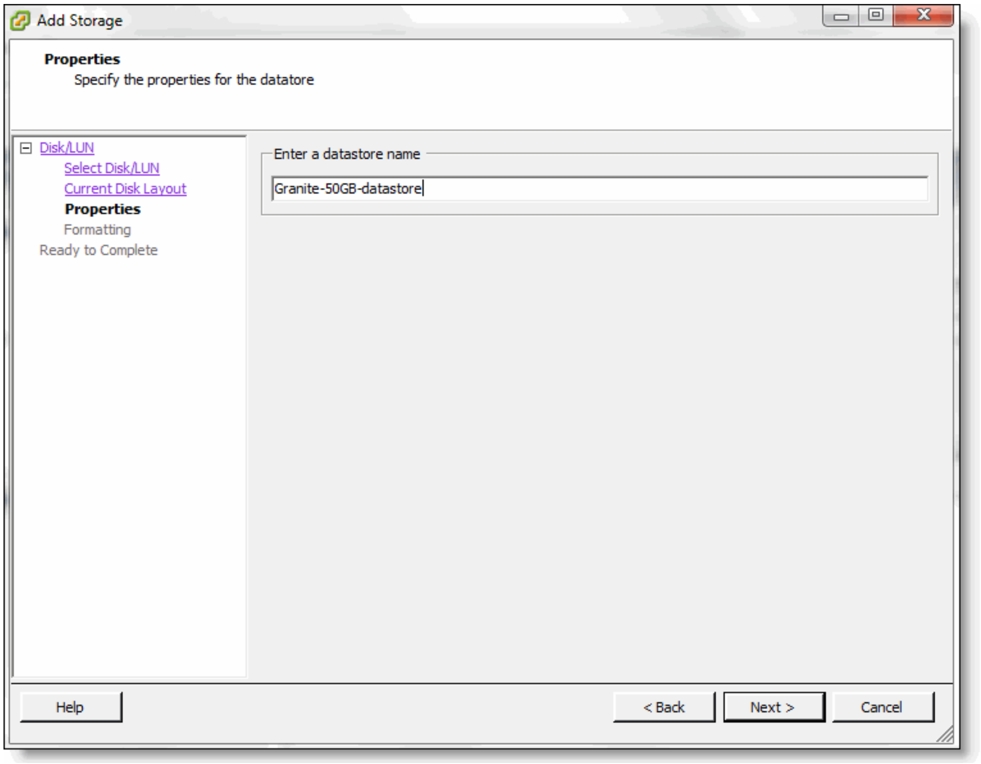
Name	Path ID	LUN	Capacity	VMFS Label	Har
RIVERBED iSCSI Disk (naa.6000eb6...	iqn.2003-10.com.r...	2	2.01 GB		Unk

8. Select VMFS-5 as the file system version and click **Next**.

   If the LUN is already formatted, this screen does not appear.

9. Type a name for the datastore (for example, SteelFusion-50GB-datastore) and click **Next.**

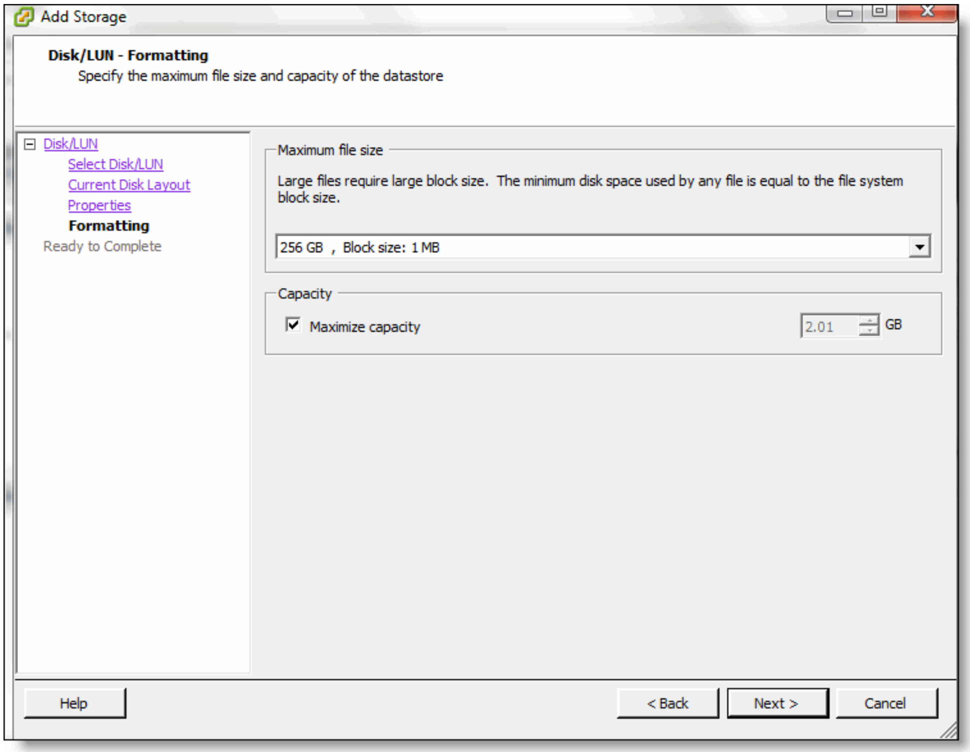
Figure 2-16. LUN Selection



10. Specify the maximum file size and datastore capacity and click **Next.**

If the LUN is already formatted, this screen does not appear.

Figure 2-17. Formatting options



Add Storage

Disk/LUN - Formatting

Specify the maximum file size and capacity of the datastore

Maximum file size

Large files require large block size. The minimum disk space used by any file is equal to the file system block size.

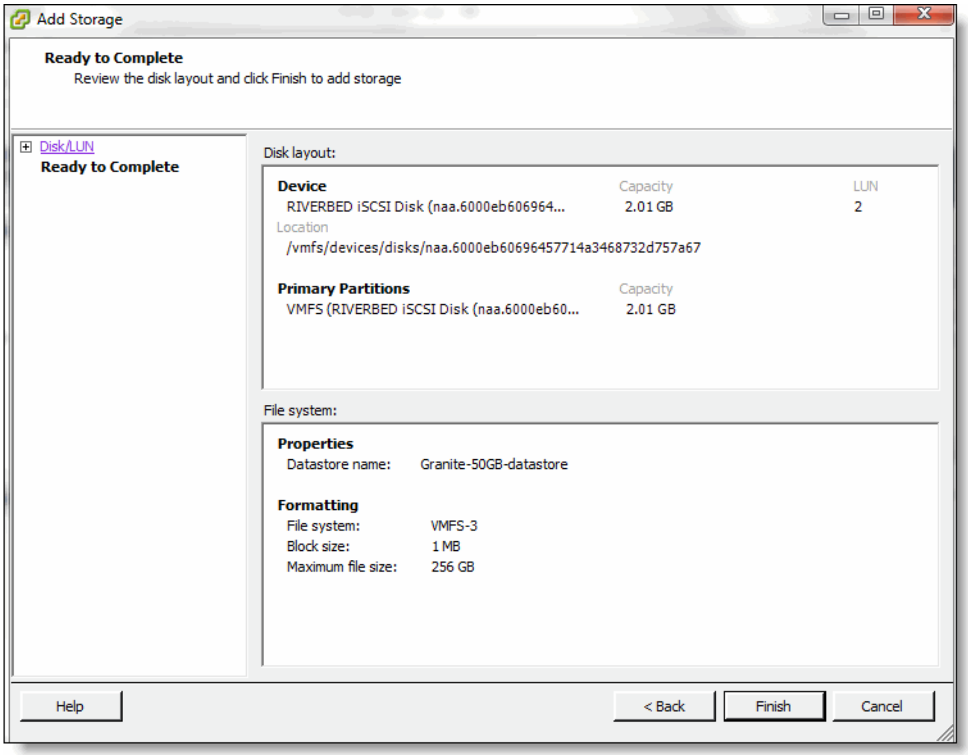
256 GB , Block size: 1 MB

Capacity

☑ Maximize capacity 2.01 GB

11. Click **Finish.**

Figure 2-18. Final step to add the data store



Add Storage

Ready to Complete

Review the disk layout and click Finish to add storage

Disk layout:

Device	Capacity	LUN
RIVERBED iSCSI Disk (naa.6000eb606964...	2.01 GB	2

Location

/vmfs/devices/disks/naa.6000eb60696457714a3468732d757a67

Primary Partitions	Capacity
VMFS (RIVERBED iSCSI Disk (naa.6000eb60...	2.01 GB

File system:

Properties

Datastore name: Granite-50GB-datastore

Formatting

File system: VMFS-3

Block size: 1 MB

Maximum file size: 256 GB

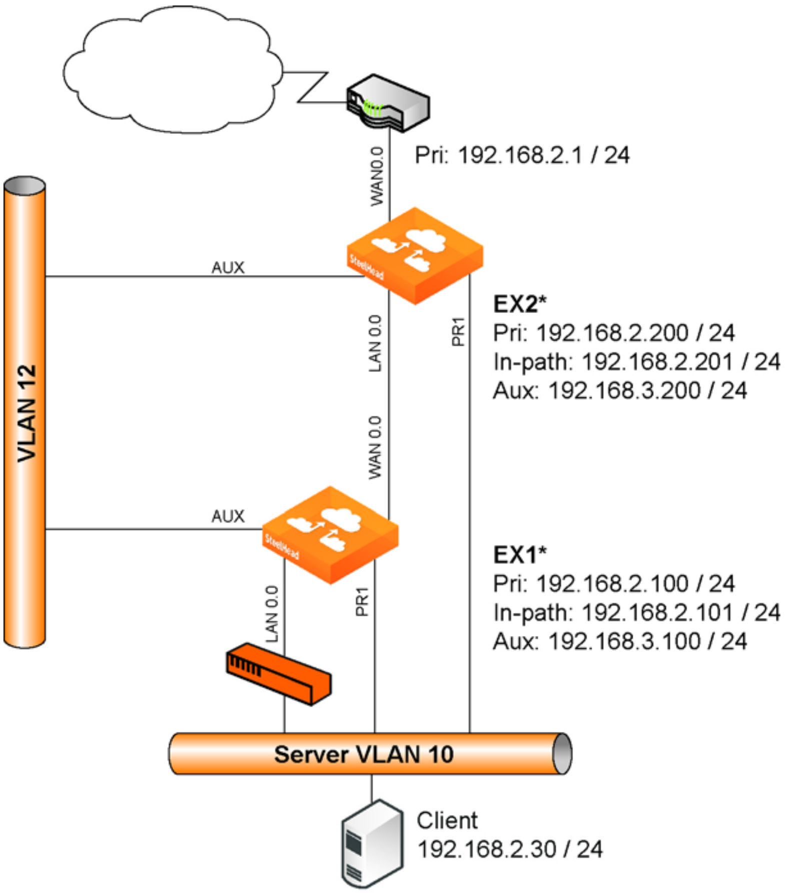
The SteelFusion LUN now hosts the new VM datastore.

VSP high availability overview

SteelHead EX provides high availability for VSP and SteelFusion. High availability can be deployed in any of the following modes:

- **Integrated mode** - SteelFusion, VSP, and virtual machines operate on a single SteelHead EX, which acts as the active device. A second, passive, SteelHead EX acts as the failover device.

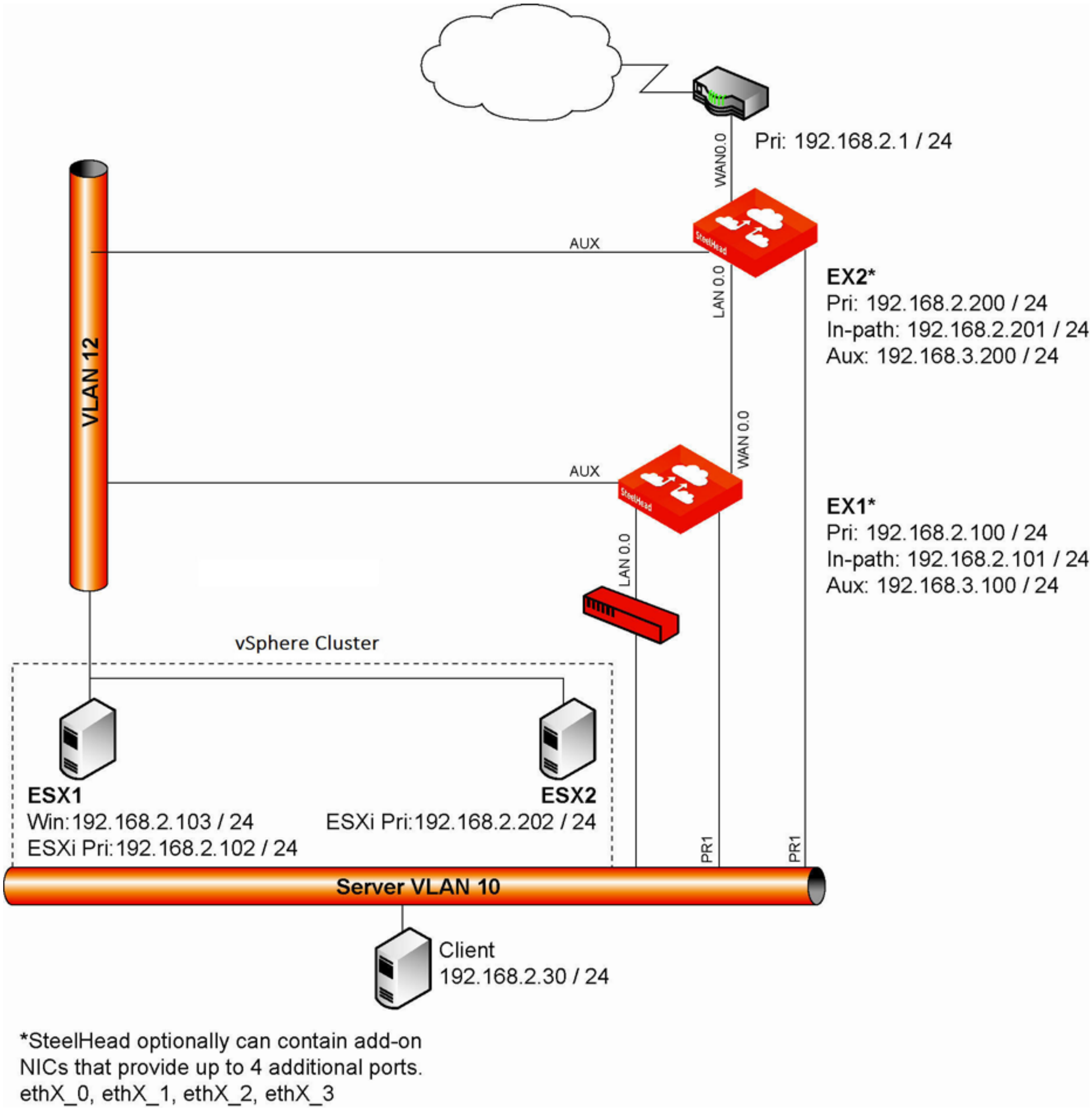
Figure 2-19. Integrated mode



*SteelHead optionally can contain add-on NICs that provide up to 4 additional ports. ethX_0, ethX_1, ethX_2, ethX_3

- **Dedicated mode -** One active SteelHead EX hosts SteelFusion while a separate active ESXi server hosts virtual machines and connects to the SteelHead EX. A passive SteelHead EX and a passive ESXi server are also deployed and act as failover devices for SteelFusion and virtual machines, respectively.

Figure 2-20. Dedicated mode



VSP HA deployment considerations

Consider the following restrictions when planning a high availability deployment:

- High availability is supported between SteelHead EXs of the same model and series.
- High availability is supported between SteelHead EXs, not in SteelHead EX-to-ESX configurations.
- The primary interfaces and the in-path interfaces of the HA pair of SteelHead EXs must be on the same subnet.
- The aux interfaces of the HA pair of SteelHead EXs must be on separate subnets.
- SteelFusion must be licensed on the SteelHead EXs.
- vSphere must be licensed at the Standard level or later.

VSP HA supported port configurations

The following tables list supported uses for ports on the appliance. Supported uses vary slightly depending on deployment (integrated, dedicated) and on whether an add-on NIC is installed on the appliance. For recommended configurations, see "VSP HA recommended port configurations" on page 55.

Supported port uses for integrated mode deployments

The following table lists supported uses for ports on the appliance when deployed in integrated mode:

Primary	Auxiliary
▪ CIFS ▪ Datastore synchronization ▪ vSphere HA heartbeat ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration) ▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration) ▪ SteelFusion HA traffic (Depends on configuration)	▪ vSphere HA heartbeats ▪ SteelFusion heartbeat ▪ Blockstore synchronization ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration) ▪ SteelFusion HA traffic (Depends on configuration)

The following table lists supported uses for ports on the appliance when deployed in integrated mode with add-on NIC:

Primary	Auxiliary	ethX_0	ethX_1	ethX_2	ethX_3
▪ CIFS ▪ Datastore synchronization ▪ vSphere HA heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration) ▪ SteelFusion Edge appliance to SteelFusion Edge appliance (Depends on user configuration)	▪ vSphere HA heartbeats ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration)	▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration)	▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX.) ▪ Blockstore synchronization (Primary path)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX.) ▪ Blockstore synchroniz ation (Secondary path)

Supported port uses for dedicated mode deployments

The following table lists supported uses for ports on the appliance when deployed in dedicated mode:

Primary	Auxiliary
▪ CIFS ▪ Datastore synchronization ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration) ▪ SteelFusion HA traffic (Depends on configuration)	▪ SteelFusion heartbeat ▪ Blockstore synchronization ▪ RiOS management (Depends on user configuration) ▪ SteelFusion HA traffic (Depends on configuration)

The following table lists supported uses for ports on the appliance when deployed in dedicated mode with add-on NIC:

Primary	Auxiliary	ethX_0	ethX_1	ethX_2	ethX_3
▪ CIFS ▪ Datastore synchronization ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration) ▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration) ▪ iSCSI Traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ RiOS management (Depends on user configuration)	▪ iSCSI Traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ iSCSI Traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Primary path)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Secondary path)

VSP HA recommended port configurations

The following tables list recommended uses for ports on the appliance. Recommended uses vary slightly depending on deployment (integrated, dedicated) and on whether an add-on NIC is installed on the appliance. For a list of all supported configurations, see “VSP HA supported port configurations” on page 53.

Recommended port uses for integrated mode deployments

The following table lists recommended uses for ports on the appliance when deployed in integrated mode:

Primary	Auxiliary
▪ CIFS ▪ Datastore synchronization ▪ vSphere HA heartbeat ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration)	▪ vSphere HA heartbeat ▪ SteelFusion heartbeat ▪ Blockstore synchronization ▪ SteelFusion HA traffic

The following table lists recommended uses for ports on the appliance when deployed in integrated mode with add-on NIC:

Primary	Auxiliary	ethX_0	ethX_1	ethX_2	ethX_3
▪ CIFS ▪ Datastore synchronization ▪ vSphere HA ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration)	▪ vSphere HA heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration)	▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration)	▪ SteelFusion Edge appliance to SteelFusion Core appliance (Depends on user configuration)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Primary path)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Secondary path)

Recommended port uses for dedicated mode deployments

The following table lists recommended uses for ports on the appliance when deployed in dedicated mode:

Primary	Auxiliary
▪ CIFS ▪ Datastore synchronization ▪ vSphere HA heartbeat ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ ESXi management (Depends on user configuration)	▪ vSphere HA heartbeat ▪ SteelFusion heartbeat ▪ Blockstore synchronization ▪ SteelFusion HA traffic

The following table lists recommended uses for ports on the appliance when deployed in dedicated mode with add-on NIC:

Primary	Auxiliary	ethX_0	ethX_1	ethX_2	ethX_3
▪ CIFS ▪ Datastore synchronization ▪ SteelFusion heartbeat ▪ RiOS management (Depends on user configuration) ▪ iSCSI traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ RiOS management (Depends on user configuration)	▪ iSCSI traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ iSCSI traffic between SteelFusion Edge and External ESXi/ Windows Server	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Primary path)	▪ SteelFusion heartbeat (Direct cross connected with secondary EX) ▪ Blockstore Synchronization (Secondary path)

Deploying VSP HA in integrated mode

This section describes how to deploy SteelHead EXs in an *integrated mode* high availability configuration. In integrated mode, SteelFusion services and virtual machines operate on the same SteelHead EX; the failover target for both is a secondary SteelHead EX.

To deploy SteelHeads in an integrated mode high availability configuration

1. Deploy an active SteelHead EX and a passive, failover SteelHead EX as indicated in Figure 2-19.

2. Ensure that SteelFusion is properly licensed on the active appliance and on the passive appliance.

3. Enable multi-path I/O (MPIO) interfaces on each appliance. For details about enabling MPIO interfaces, see the *SteelFusion Core Management Console User's Guide*.

4. Provision a LUN to host virtual machine datastores. The LUN must be accessible to both the active and passive SteelHead EXs. The LUN can be sourced from the active appliance's local disk, or it can be sourced and projected from a SteelFusion Core appliance. See "Adding SteelFusion Edge as an ESXi datastore" on page 40.

5. Establish datastores on the LUN. See "Creating a datastore on the LUN" on page 45.

6. Ensure that the VMware vSphere licenses on each appliance are sufficient to enable native vSphere high availability. (*Standard*, *Enterprise*, and *Enterprise Plus* licenses enable high availability.)

7. Launch a vSphere Client and connect to your vCenter Server that manages ESXi on the SteelHead EXs.

8. Using the vSphere Client, place the active SteelHead EX and the passive one into the same HA cluster.

9. Deploy your virtual machines to ESXi on the active SteelHead EX.

Deploying VSP HA in dedicated mode

This section describes how to deploy SteelHead EXs in an *dedicated mode* high availability configuration. Dedicated mode is when SteelFusion services operate on the SteelHead EX and virtual machines are hosted on a separate ESXi system; the failover target for SteelFusion is the secondary SteelHead EX, while the failover target for virtual machines is a secondary ESXi system.

To deploy SteelHead EXs in a dedicated mode high availability configuration

1. Deploy an active SteelHead EX and a passive, failover SteelHead EX as indicated in Figure 2-19.

2. Ensure that SteelFusion functionality is properly licensed on both the active and the passive appliances.

3. Enable MPIO interfaces on each appliance. For details about enabling MPIO interfaces, see the *SteelFusion Core Management Console User's Guide*.

4. Provision a LUN to host virtual machine datastores. The LUN must be accessible to both the active and passive SteelHead EXs. The LUN can be sourced from the active appliance's local disk, or it can be sourced and projected from a SteelFusion Core appliance. See "Adding SteelFusion Edge as an ESXi datastore" on page 40.

5. Establish datastores on the LUN. See "Creating a datastore on the LUN" on page 45.

6. Ensure that the VMware vSphere licenses on each appliance are sufficient to enable native vSphere high availability. (*Standard*, *Enterprise*, and *Enterprise Plus* licenses enable high availability.)

7. Launch a vSphere Client and connect to your vCenter Server that manages the ESXi systems.

8. Using the vSphere Client, place both the active and the passive ESXi systems into the same HA cluster.

9. Deploy your virtual machines to the active ESXi system.