SteelFusion Best Practices Guide

Solution Guide

Riverbed Technical Marketing

June 2016

Table of Contents

Introduction

The Riverbed® SteelFusion™ solution is a dual-ended system that enables complete consolidation of storage at the data center by providing local disk performance at the remote/branch office. The following best practices guide will help you deploy and configure SteelFusion appliances in your distributed organization.

Audience

This paper is written for storage and network administrators familiar with administering and managing distributed office environments using common network and storage protocols such as iSCSI, SCSI, TCP, CIFS, HTTP, FTP, and NFS.

You must also be familiar with:

- Riverbed Steelhead® appliance installation and configuration process.
- Riverbed Steelhead management interface.

Additional Resources

For a complete list and the most current version of Riverbed documentation log in to the Riverbed support website located at https://support.riverbed.com.

The Riverbed Knowledge Base is a database of known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for key words and strings. To access the Riverbed Knowledge Base, log in to the Riverbed Support site located at https://support.riverbed.com.

SteelFusion Overview

SteelFusion products enable users and applications in branch office locations to write to and access centrally managed storage maintaining local disk performance. By accelerating branch access to data center deployed storage infrastructure, IT organizations no longer need to provision and maintain dedicated storage resources in branch offices.

The SteelFusion solution is deployed in conjunction with Steelhead appliances and consists of two components:

- SteelFusion Core – a physical or virtual appliance that resides in the data center alongside a Steelhead appliance and the storage system
- SteelFusion Edge – a software module that runs on a physical appliance in the branch office

SteelFusion Core mounts the LUNs provisioned in the data center and shares the storage resources with branch offices running the SteelFusion Edge module. SteelFusion Edge virtually presents one or more iSCSI targets in the branch which can be utilized by services and systems running both within the VSP as well as externally to the SteelFusion Edge appliance. SteelFusion Core inspects mounted file systems and is able to proactively stream data to the branch locations utilizing innovative block-level prediction algorithms. This industry-first capability allows data from centralized storage to be available wherever and whenever it is needed. Through asynchronous block-based write acceleration SteelFusion Edge ensures that data created in branch office locations is securely stored in the data center.

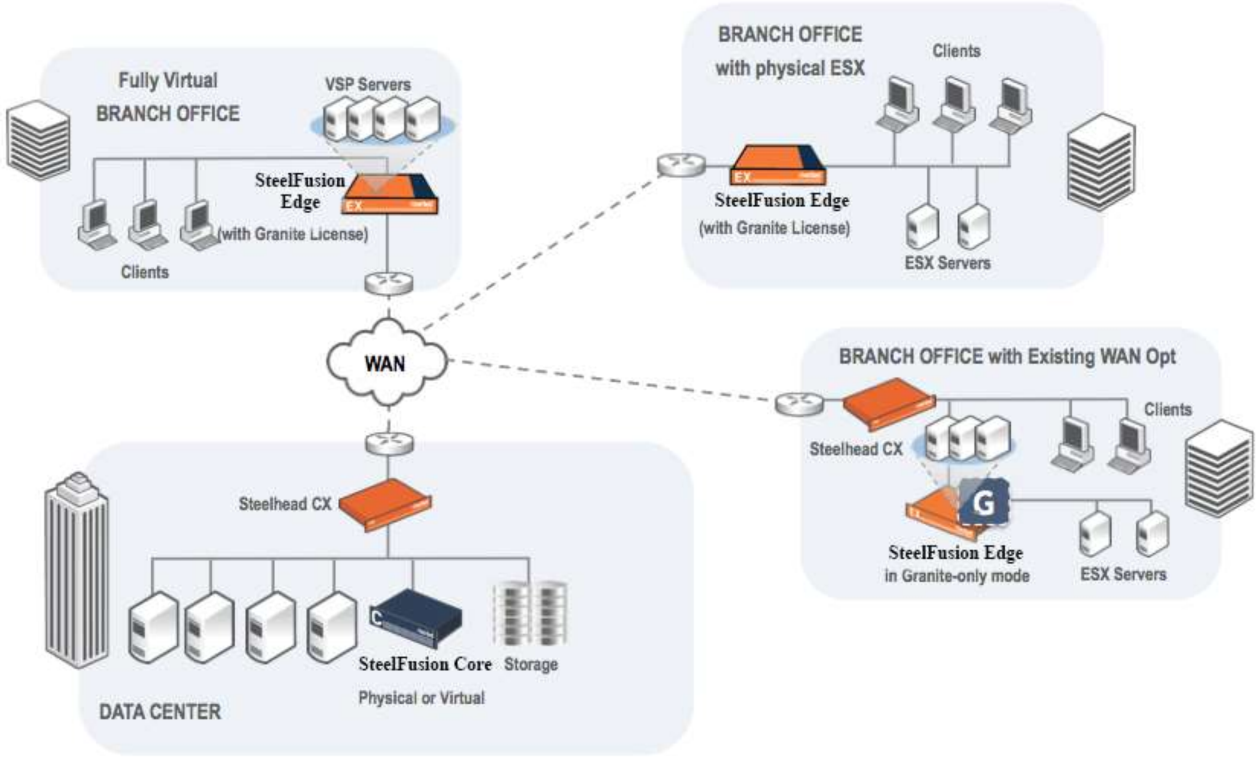


Figure 1: SteelFusion Core and SteelFusion Edge High Level Network Topologies

Best Practices for SteelFusion Deployments

There is no single way of configuring a SteelFusion appliance that ensures its optimal performance in all types and sizes of IT infrastructure. Therefore, Riverbed has developed a list of best practices that ensure the maximum performance of the appliance in a specific environment while minimizing the initial configuration and future maintenance efforts.

SteelFusion Core Deployment

Deploy on GigE networks

While iSCSI enables storage to work over IP networks, it still uses SCSI as a protocol, which is latency and bandwidth sensitive. In order to optimize performance and reliability it is recommended to deploy SteelFusion Core appliance and storage array on GigE networks.

Configure Initiators / Storage Groups or LUN Masking

It is recommended to configure Initiator/Storage Groups between SteelFusion Core and the storage system in order to avoid others hosts to access LUNs mapped to SteelFusion Core. This common practice is also known as LUN masking or Storage Access Control.

In particular when mapping Fibre Channel LUNs to the virtual SteelFusion Cores make sure that the ESXi servers in the cluster that are not hosting the virtual SteelFusion Cores don't have access to those LUNs.

Use Mutual CHAP Authentication

It is recommended to use Mutual Challenge Handshake Authentication Protocol (CHAP) authentication between SteelFusion Core and the storage device as another level of security. One-Way CHAP authentication is also supported.

Segregate Storage Traffic from Management Traffic

In order to increase overall security, minimize congestion, minimize latency and simplify the overall configuration of your storage infrastructure, it is recommended to segregate storage traffic from regular LAN traffic. Place storage traffic on its own physically separated network (or VLAN) that is routed separately from the main network.

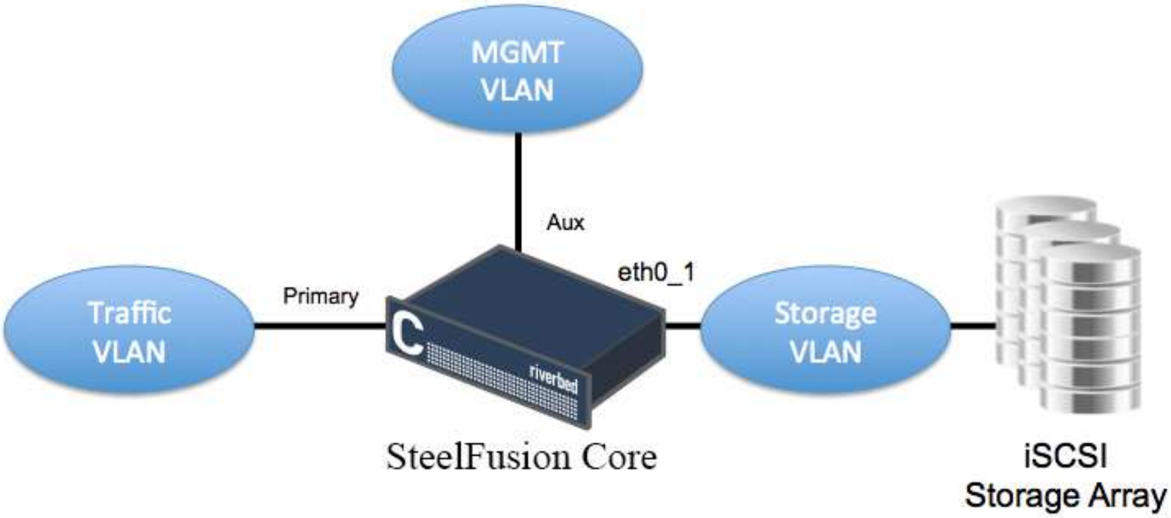


Figure 2 Traffic Segregation

Configure Jumbo Frames

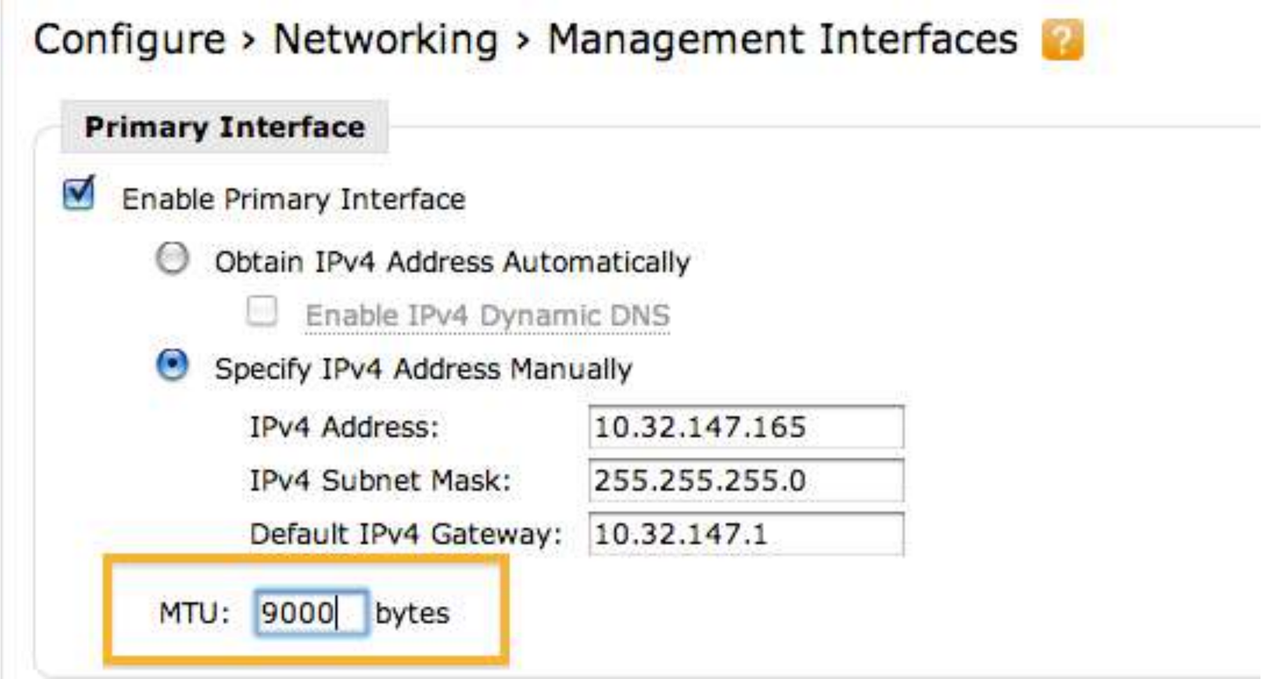
If Jumbo Frames are supported in your network infrastructure it is recommended to use jumbo frames between the SteelFusion Core appliance and the Storage array. Jumbo Frames can be used to allow more data to be transferred with each Ethernet transaction and reduce the number of frames. This larger frame size reduces the overhead on both the SteelFusion appliance and the storage device, providing the best performance for large transfer sizes.

Note: All devices, including switches and routers, between SteelFusion Core and the storage array must be configured to use the same jumbo frame size.

How to enable Jumbo Frames on SteelFusion Core

To enable jumbo frames on SteelFusion Core select Configure > Networking > Manage Interfaces and enter 9000 in the MTU size field of the interface that is connected to the storage array as shown in Figure 3

Note: 9000 bytes is the max and recommended value for iSCSI traffic.



Configure › Networking › Management Interfaces

Primary Interface

☑ Enable Primary Interface

○ Obtain IPv4 Address Automatically

□ Enable IPv4 Dynamic DNS

● Specify IPv4 Address Manually

IPv4 Address: 10.32.147.165

IPv4 Subnet Mask: 255.255.255.0

Default IPv4 Gateway: 10.32.147.1

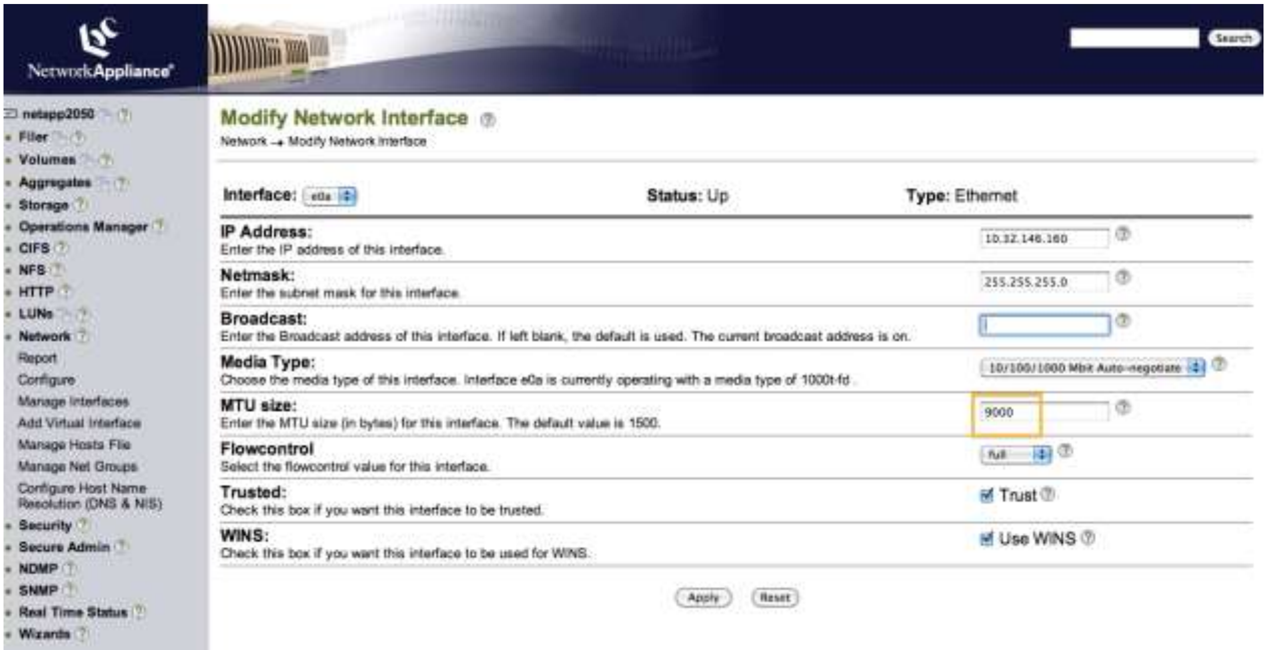
MTU: 9000 bytes

Figure 3 SteelFusion Jumbo Frames Page

How to enable Jumbo Frames on the storage array

The procedure to enable jumbo frames varies between different storage devices.

To enable Jumbo frames on a NetApp Filer for example select **Manage Interfaces** under Network from the left menu of FilerView > Select Modify to view or change the parameters of the interface as shown in Figure 4



Modify Network Interface

Network → Modify Network Interface

Interface: e0a Status: Up Type: Ethernet

IP Address: 10.32.146.160
Enter the IP address of this interface.

Netmask: 255.255.255.0
Enter the subnet mask for this interface.

Broadcast:
Enter the Broadcast address of this interface. If left blank, the default is used. The current broadcast address is on.

Media Type: 10/100/1000 Mbit Auto-negotiate
Choose the media type of this interface. Interface e0a is currently operating with a media type of 1000t-fd .

MTU size: 9000
Enter the MTU size (in bytes) for this interface. The default value is 1500.

Flowcontrol: full
Select the flowcontrol value for this interface.

Trusted: ☑ Trust
Check this box if you want this interface to be trusted.

WINS: ☑ Use WINS
Check this box if you want this interface to be used for WINS.

Figure 4 NetApp Jumbo Frames Config Page

When to PIN and Prepopulate the LUN

SteelFusion technology has built-in file system awareness for NTFS and VMFS file systems.

For un-optimized file systems

For un-optimized file systems like fat, fat32, ext3, etc. it is recommended to PIN and Prepop the LUN.
It is also recommended to PIN the LUN for applications like Databases that uses raw disk file format or proprietary file systems.

Data must be available at the branch even when WAN link is down

When the WAN link between the branch office and the data center is down data can’t go through, hence SteelFusion technology and its intelligent prefetch mechanisms don’t work. So if frequent periods of WAN outages are expected it is recommended to PIN and Prepop the LUN. If moreover long periods of WAN outages are expected it is recommended to appropriately size the “write reserve” space. By default the SteelFusion Edge appliance keeps a write reserve that is 10% of the blockstore size.

How to connect Clustered SteelFusion Cores appliances to the network

Whenever possible, use Aux interface for Management, Primary interface for Rdisk/WAN traffic, eth0_1 interface for storage iSCSI traffic, eth0_2 and eth0_3 for heartbeat between redundant cores.

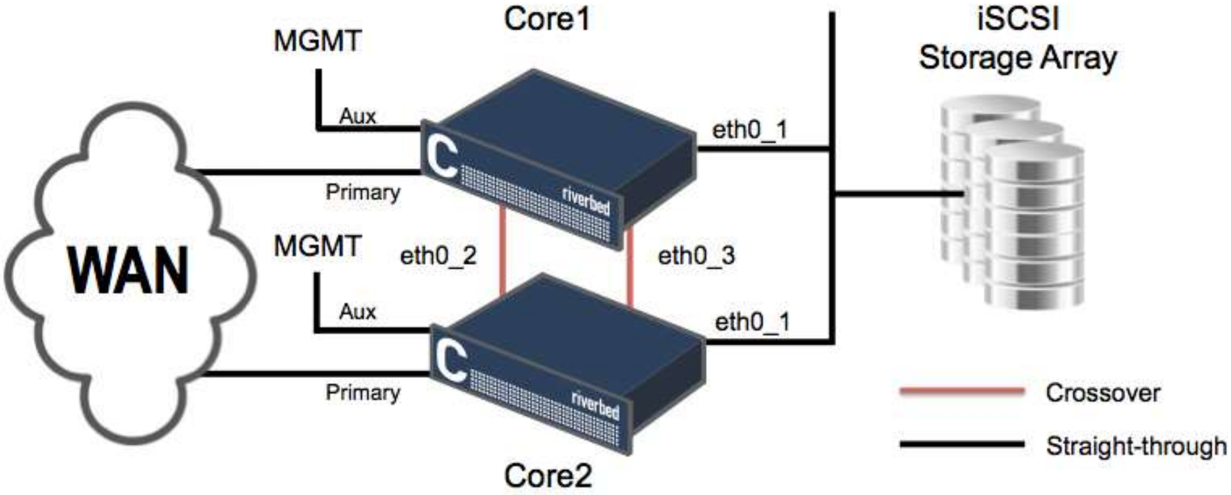


Figure 5 SteelFusion Core HA network configuration

A crossover cable or completely separate networks should be use to connect the heartbeat interfaces eth0_2 and eth0_3.

In a clustered configuration the SteelFusion Cores share with each other IPs, iSCSI, SteelFusion Edges and other settings.

On the SteelFusion Edge, you only need to configure the primary SteelFusion Core. The information about the peer (backup) SteelFusion Core is automatically relayed to the SteelFusion Edge and stored. You will be able to see the information for the peer (backup) in the Branch Storage page on the SteelFusion Edge after this happens.

SteelFusion Core Configuration Export

It is recommended to backup the configuration on an external server in case of system failure. The CLI command to export the configuration is:

```
enable
Configure terminal
Configuration bulk export scp://username:password@server/path/to/config
```

SteelFusion Core in HA Configuration Replacement:

If the configuration has been saved on an external server the failed SteelFusion Core appliance can be seamlessly replaced following these simple steps

```
enable
Configure terminal
```

```
No service enable
Configuration bulk import scp://username:password@server/path/to/config
Service enable
```

SteelFusion Edge Deployment

Separate iSCSI traffic from LAN Traffic

In the branch office in order to increase overall security, minimize congestion, minimize latency and simplify the overall configuration of your storage infrastructure, it is recommended to separate storage iSCSI and WAN/Rdisk traffic from LAN traffic.

Ports and Type of traffic

iSCSI traffic is only allowed on Primary and Aux interfaces, as shown in Figure 6. Don't configure your external iSCSI initiators to use the IP address configured on the Inpath interface.

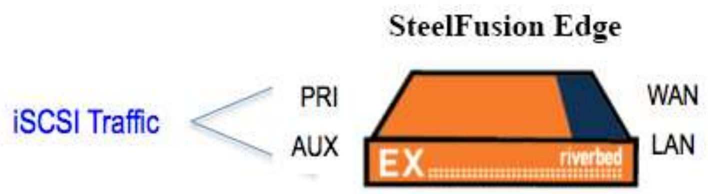
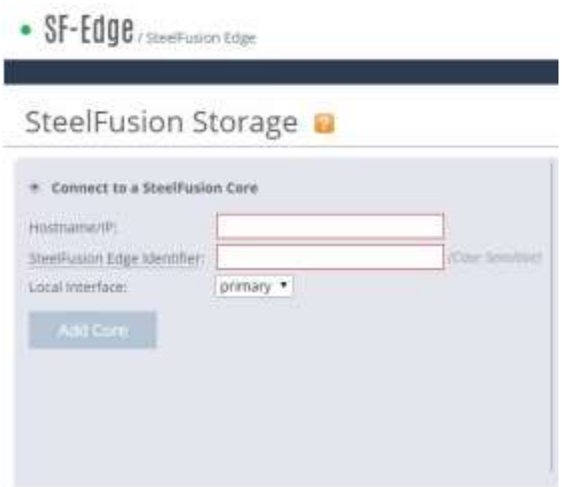


Figure 6: iSCSI traffic on Primary and Aux interfaces

SteelFusion Core Hostname/IP

In the case the branch DNS server runs on VSP and its datastore is deployed on a SteelFusion LUN, it is recommended to use the SteelFusion Core appliance IP address instead of the hostname, when specifying the SteelFusion Core appliance Hostname/IP. This is to avoid the "snake eating its tail" situation. Alternatively if you must use the hostname, deploy the DNS server on the VSP internal storage or configure host DNS entries for the SteelFusion Core hostname on the Steelhead appliance.



SF-Edge / SteelFusion Edge

SteelFusion Storage

Connect to a SteelFusion Core

Hostname/IP:

SteelFusion Edge Identifier: (Case Sensitive)

Local Interface: primary

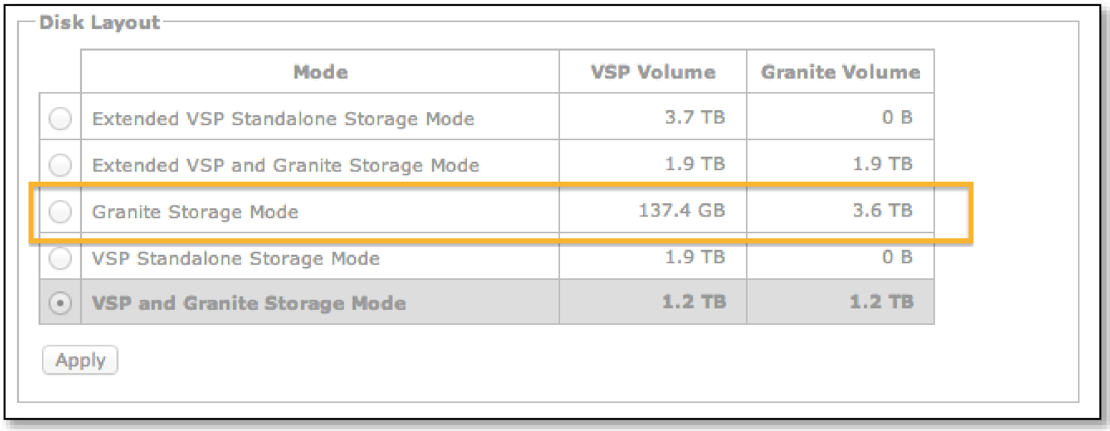
Figure 7: SteelFusion Core Hostname/IP

Configuring Disk Management

You can configure the disk layout mode in the **Administration > System Settings > Disk Management** page of the SteelFusion Edge Management Console. The disk space in the SteelFusion Edge appliance, as shown in Figure 8, can be partition in different ways depending on how the appliance is used and which license has been purchased.

VSP and SteelFusion Storage Mode is the default disk layout configured on the appliance during the manufacturing process. This mode evenly divides the disk space between VSP and SteelFusion functionalities.

However, if you plan on using the storage delivery capabilities (SteelFusion feature) of the Steelhead EX appliance, it is recommended to select the **SteelFusion Storage Mode** disk layout. In the SteelFusion storage mode, most of the disk space is dedicated to SteelFusion Blockstore cache, while leaving the required amount for VSP and WAN optimization functionalities. This mode allows you to centralized onto your data center storage both the operating system and the production data drives of the virtual servers running at the branch.



Disk Layout

	Mode	VSP Volume	Granite Volume
○	Extended VSP Standalone Storage Mode	3.7 TB	0 B
○	Extended VSP and Granite Storage Mode	1.9 TB	1.9 TB
○	Granite Storage Mode	137.4 GB	3.6 TB
○	VSP Standalone Storage Mode	1.9 TB	0 B
●	**VSP and Granite Storage Mode**	**1.2 TB**	**1.2 TB**

Figure 8 SteelFusion Edge disk layout

The **Extended VSP Standalone Storage Mode** and the legacy **VSP Standalone Storage Mode** are designed for EX appliances that do not employ the SteelFusion feature.

The **Extended VSP and SteelFusion Storage Mode** is designed for the use cases where the system administrator does not want to consolidate the virtual servers operating system drive into the data center storage, but instead wants to keep it locally on the SteelFusion Edge appliance.

Can Windows Dynamic Disks be used on SteelFusion Edge hosted Virtual Machines?

Consider a scenario where a LUN has been presented to a Windows virtual machine and has been directly mounted via the iSCSI initiator, and formatted as an NTFS volume.

Due to restrictions in the mounting process of Windows dynamic disks, it is a requirement to use Windows basic disks at all times where snapshots of that disk are being presented to a proxy host for backup purposes. The automation scripts will successfully present the snapshot, but will be unable to mount the disk. In Windows disk management, the snapshot will appear to be (offline, dynamic).

There is no way to revert an accidental change to a dynamic disk without data loss. However, you may be able to perform a SAN-based copy of the NTFS-formatted LUN and present that to a Windows host, and then either take a backup of the data via robocopy or some other tool.

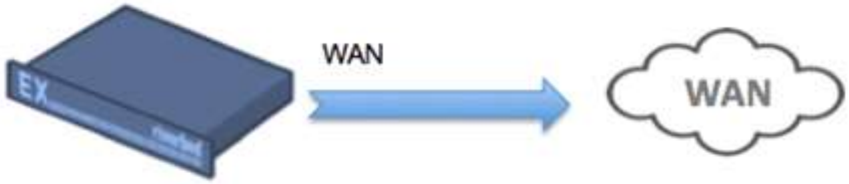
For more information, refer to Microsoft TechNet - technet.microsoft.com/en-au/library/cc753750.asp

Rdisk Traffic Routing Options

You can configure to route Rdisk traffic out of the Primary or the Inpath interfaces. It is recommended to select the Inpath interface when deploying Steelhead EX in SteelFusion Only mode. It is recommended to select Primary interface when deploying Steelhead EX in Steelhead EX + SteelFusion mode.

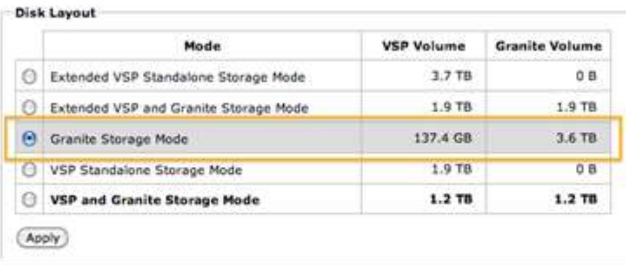
Option 1: Inpath Interface

When you configure Steelhead EX to use the Inpath interface the Rdisk traffic will be intercepted, optimized and sent directly out the WAN interface towards the SteelFusion Core appliance deployed at the data center. This option is recommended when deploying Steelhead EX in SteelFusion only mode, during prof of concepts (POC) installations or simply if the primary interface is used and dedicated to management. The drawback of this mode is the lack of redundancy in case of WAN interface failure. In this configuration only the WAN interface needs to be connected and hence link state propagation should be disabled.



SteelFusion with Granite Only option:
Use Inpath interface to connect to SteelFusion Core

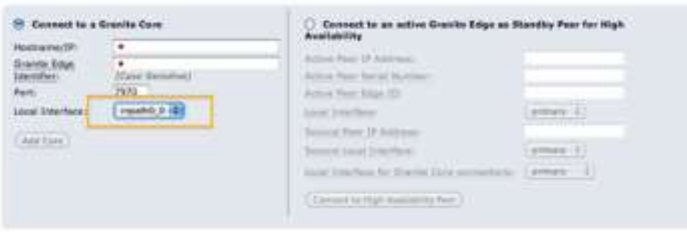
“SteelFusion” only mode



Disk Layout

	Mode	VSP Volume	Granite Volume
○	Extended VSP Standalone Storage Mode	3.7 TB	0 B
○	Extended VSP and Granite Storage Mode	1.9 TB	1.9 TB
●	Granite Storage Mode	137.4 GB	3.6 TB
○	VSP Standalone Storage Mode	1.9 TB	0 B
○	**VSP and Granite Storage Mode**	**1.2 TB**	**1.2 TB**

Rdisk Interface -> Inpath



● Connect to a Granite Core

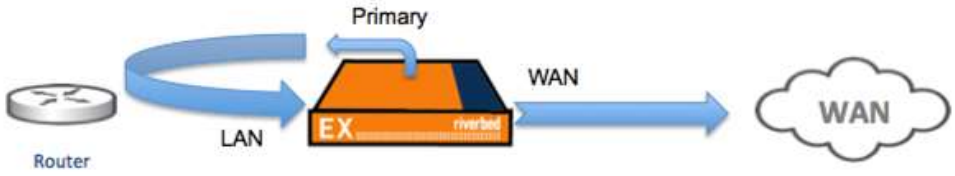
Hostname/IP: *
Granite Edge Identifier: * (Case Sensitive)
Port: 7970
Local Interface: inpath0_0

○ Connect to an active Granite Edge as Standby Peer for High Availability

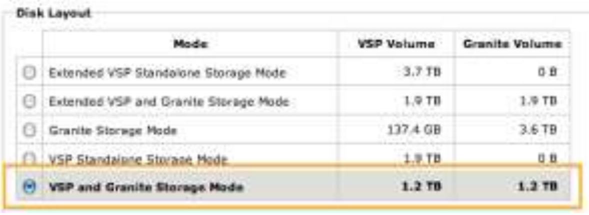
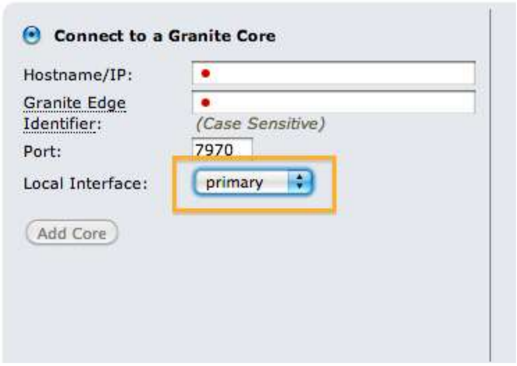
Active Peer IP Address:
Active Peer Serial Number:
Active Peer Edge ID:
Local Interface: primary
Second Peer IP Address:
Second Local Interface: primary
Local Interface for Granite Core connections: primary

Option 2: Primary Interface

When you configure Steelhead EX to use the Primary interface the Rdisk traffic will be sent unoptimized out the Primary interface to a switch or a router that will redirect the traffic back into the LAN interface of the Steelhead EX to get optimized and sent out the WAN interface towards the SteelFusion Core appliance deployed at the data center. This option is recommended when deploying Steelhead EX in + SteelFusion mode. This configuration offers more redundancy since you can have both the Inpath interfaces connected to different switches.



SteelHead EX + Granite:
Use Primary interface to connect to SteelFusion Core

“VSP” and “VSP + SteelFusion” mode	Rdisk Interface -> Primary
	

Disk Layout

	Mode	VSP Volume	Granite Volume
○	Extended VSP Standalone Storage Mode	3.7 TB	0 B
○	Extended VSP and Granite Storage Mode	1.9 TB	1.9 TB
○	Granite Storage Mode	137.4 GB	3.6 TB
○	VSP Standalone Storage Mode	1.9 TB	0 B
●	**VSP and Granite Storage Mode**	**1.2 TB**	**1.2 TB**

● **Connect to a Granite Core**

Hostname/IP: •
Granite Edge Identifier: • (Case Sensitive)
Port: 7970
Local Interface: primary

Deploying SteelFusion with WAAS

The SteelFusion Edge and SteelFusion Core appliances communicate with each other and transfer data-blocks over the WAN using 6 TCP ports: 7950, 7951, 7952, 7953, 7954 and 7970.

WCCP Topology

If branch and data center WAAS appliances are configured via WCCP as shown in Figure 9

1. Optionally configure ACL on the router to redirect the SteelFusion's 6 TCP ports to the steelhead appliances.
2. Configure a fixed target rule for SteelFusion TCP ports to the data center steelhead appliance inpath interface.

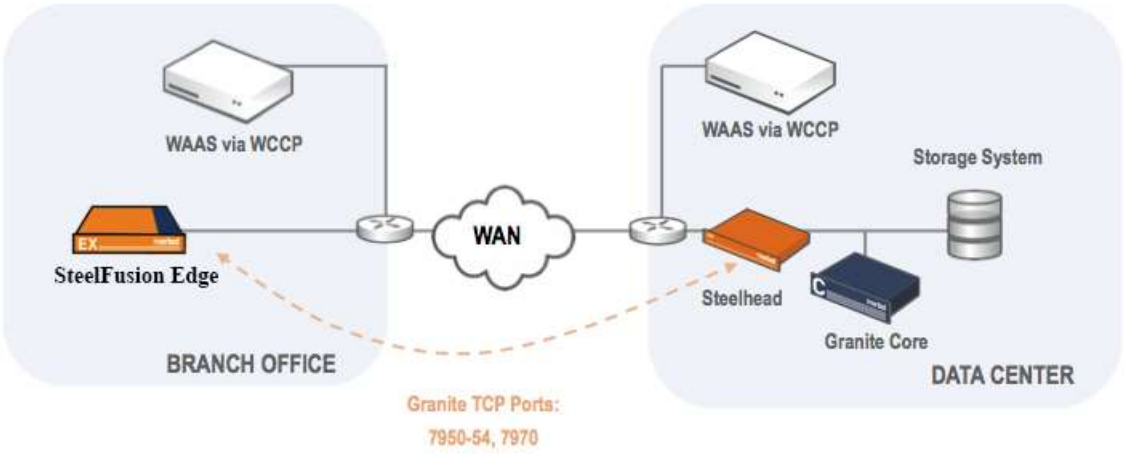
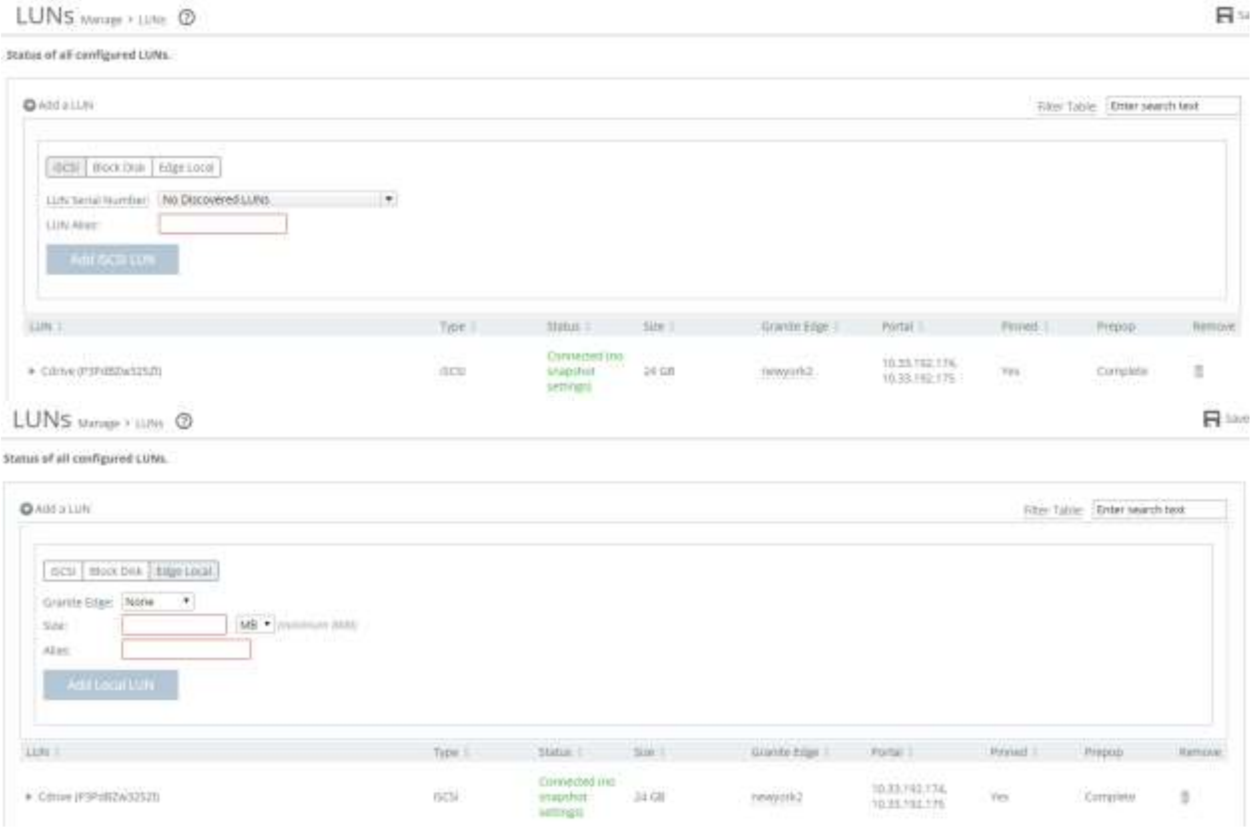


Figure 9: SteelFusion behind WAAS

Windows and ESX Server Storage Layout

Transient and temporary server data is not required in the case of disaster recovery and therefore does not need to be replicated back to the data center. For this reason it is recommended to separate transient and temporary data from the production data by implementing a layout that separates the two into multiple LUNs. In general plan on configuring one LUN for the operating system, one LUN for the production data and one LUN for the temporary swap or paging space. Doing so will greatly enhance data protection and operations recovery in case of a disaster, and moreover facilitate migration to server virtualization if today you are using physical servers.

In order to achieve these goals SteelFusion implements two types of LUNs: SteelFusion LUNs and Local LUNs, as shown in Figure 10


LUNs Manage > LUNs
Status of all configured LUNs.
Add a LUN
Filter Table: Enter search text
iSCSI | Block Disk | Edge Local

LUN Serial Number: No Discovered LUNs
LUN Alias:

LUN	Type	Status	Size	Granite Edge	Portal	Pinned	Prepop	Remove
Cdrive (P3PdBZw3252I)	iSCSI	Connected (no snapshot settings)	24 GB	newyork2	10.33.192.174, 10.33.192.175	Yes	Complete	

LUNs Manage > LUNs
Status of all configured LUNs.
Add a LUN
Filter Table: Enter search text
iSCSI | Block Disk | Edge Local

Granite Edge: None
Size: MB (minimum 8MB)
Alias:

LUN	Type	Status	Size	Granite Edge	Portal	Pinned	Prepop	Remove
Cdrive (P3PdBZw3252I)	iSCSI	Connected (no snapshot settings)	24 GB	newyork2	10.33.192.174, 10.33.192.175	Yes	Complete	

Figure 10 iSCSI and Local LUNs

SteelFusion LUNs are used to store production data. SteelFusion LUNs share the space of the SteelFusion Edge blockstore cache and the data is continuously replicated and kept in sync with the associated LUN back at the data center. The SteelFusion Edge appliance cache only keeps the working set of data blocks for these LUNs, while the remaining of the data is kept at the data center and predictably retrieved at the edge when needed. During WAN outages edge servers are not guaranteed to operate and function at 100% since some of the data that might be needed could be at the data center and not locally present in the SteelFusion Edge blockstore cache.

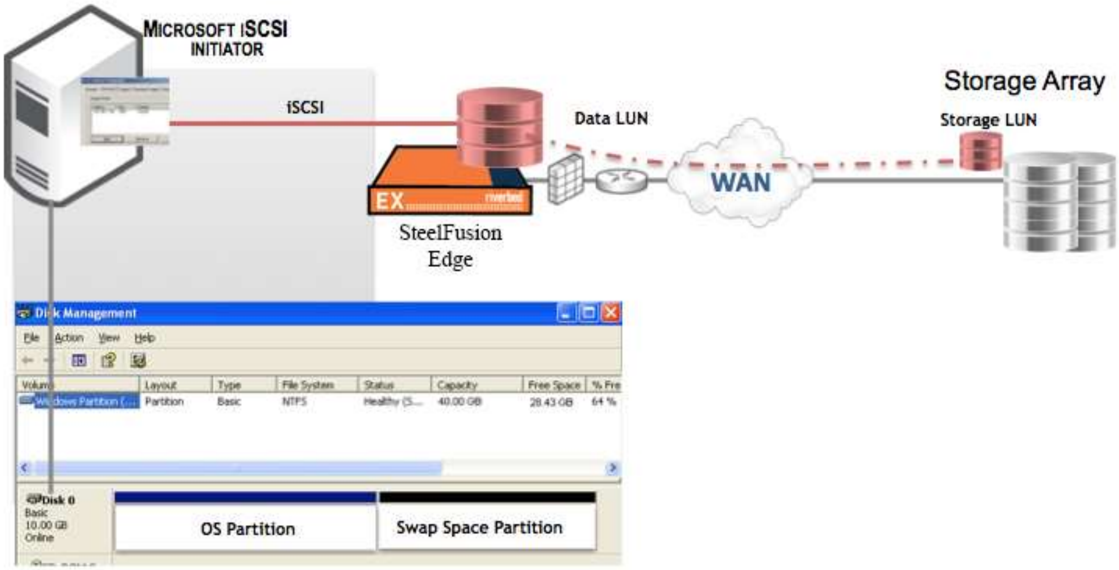
Note: A particular type of iSCSI LUN is the ***PINNED LUN****. PINNED LUNs are also used to store production data but they use dedicated space in the SteelFusion Edge appliance. The space required and dedicated in* *the SteelFusion Edge blockstore cache is equal to the size of the LUN provisioned at the data center. This allows the edge servers to continue to operate and function even during WAN outages, since 100% of data is kept in SteelFusion Edge appliance blockstore cache. Like regular SteelFusion LUNs the data is replicated and kept in sync with the associated LUN back at the data center.*

Local LUNs are used to store transient and temporary data. Local LUNs also use dedicated space in the blockstore cache of the SteelFusion Edge appliance but the data, since not required in the case of disaster recovery is never replicated back to the data center.

Physical Windows Server Storage Layout

When deploying a physical Windows server it is recommended to separate its storage in 3 different LUNs. The operating system and swap space (or page file) can reside in two partitions on the server internal hard drive (or 2 separate drives), while production data should reside on the SteelFusion iSCSI LUN.

This layout facilitates future server virtualization and service recovery in the case of hardware failure at the branch. Since the production data is hosted on a SteelFusion LUN, which is safely stored and backed up at the data center, and in case of a disaster, this data can be simply streamed on the fly to a newly deployed windows server, without having to restore the entire dataset from backup.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Fre
Windows Partition (...	Partition	Basic	NTFS	Healthy (S...	40.00 GB	28.43 GB	64 %

Figure 11 Physical server layout

Virtualized Windows Server on SteelFusion Storage Layout

When deploying a virtual Windows server into the VSP SteelFusion Edge infrastructure, separating its storage in 3 different LUNs it is also recommended.

- The operating system disk (OS LUN) can be virtualized on a VMDK file and hosted on the SteelFusion LUN, allowing for data center backup and instant recovery in the case of Edge hardware failure.
- Swap and vSwap space, containing transient data, can be stored on SteelFusion Local LUNs, since this space doesn't need to be recovered after a disaster.
- Production data will still reside on a SteelFusion iSCSI LUN, allowing for data center backup and instant recovery in the case of Edge hardware failure.

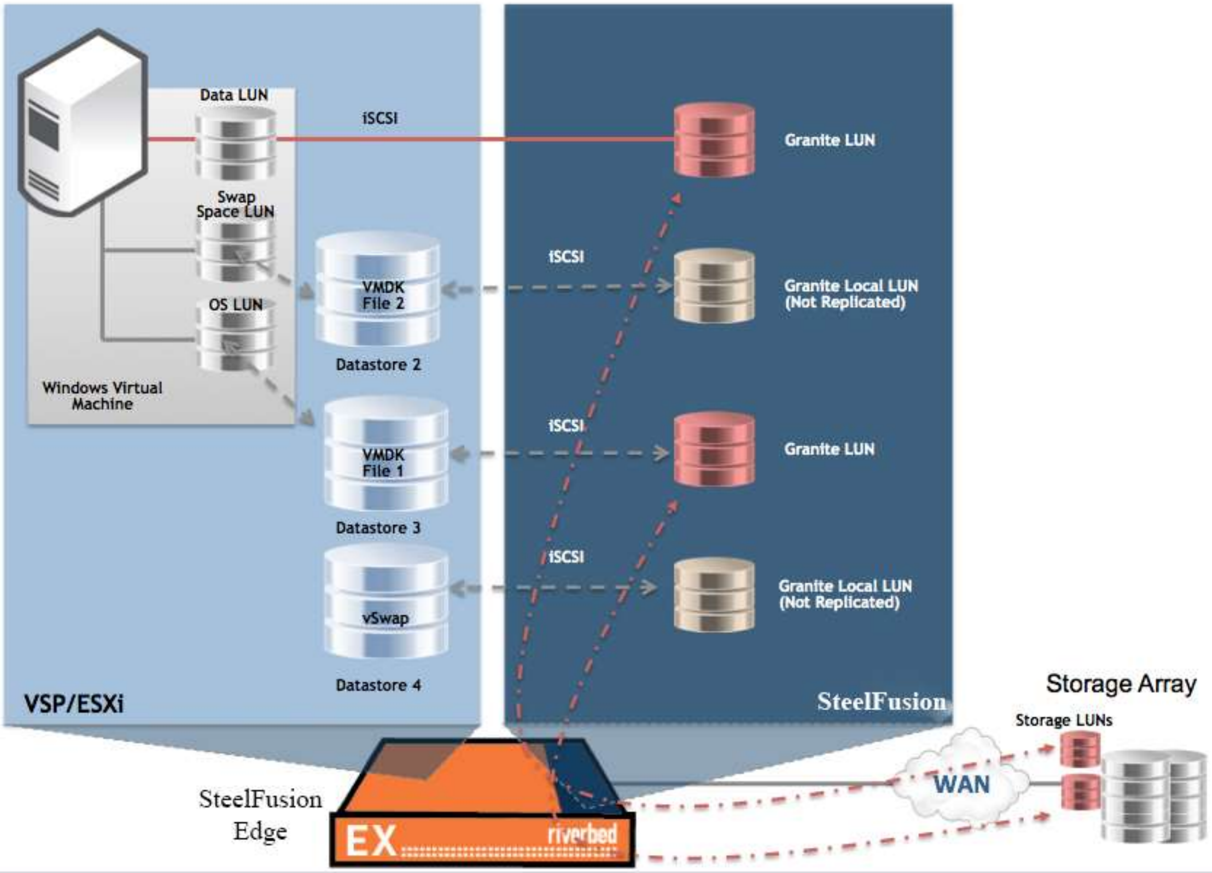


Figure 12 Virtual server layout 1

Virtualized Windows Server on ESX infrastructure with Production Data LUN on ESX Datastore Storage Layout

When deploying a virtual Windows server into an ESX infrastructure the production data can also be stored on an ESX datastore mapped to a SteelFusion LUN. Also this deployment facilitates service recovery in the case of hardware failure at the branch, since SteelFusion appliances optimize, not only LUNs formatted directly with NTFS file system, but also LUNs virtualized first with VMFS and the later formatted with NTFS.

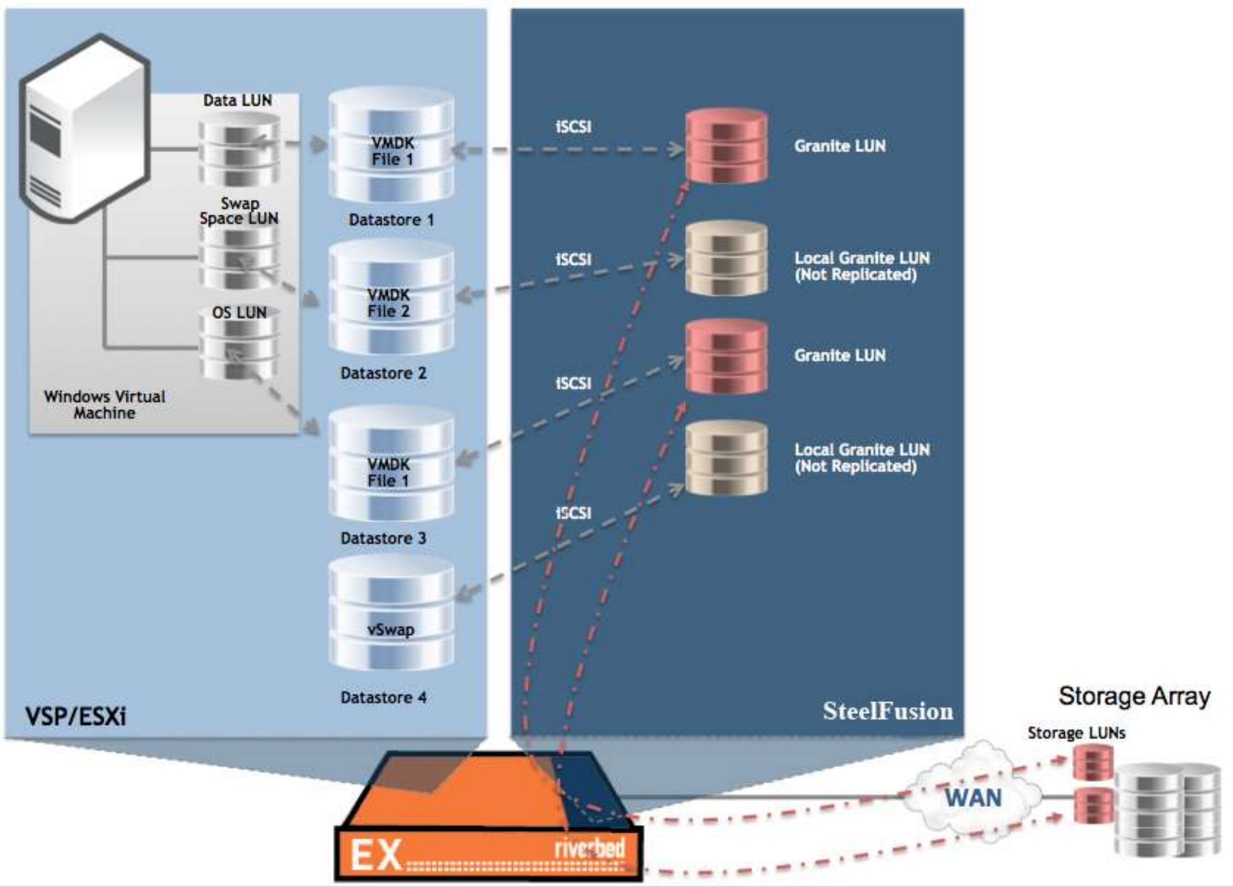
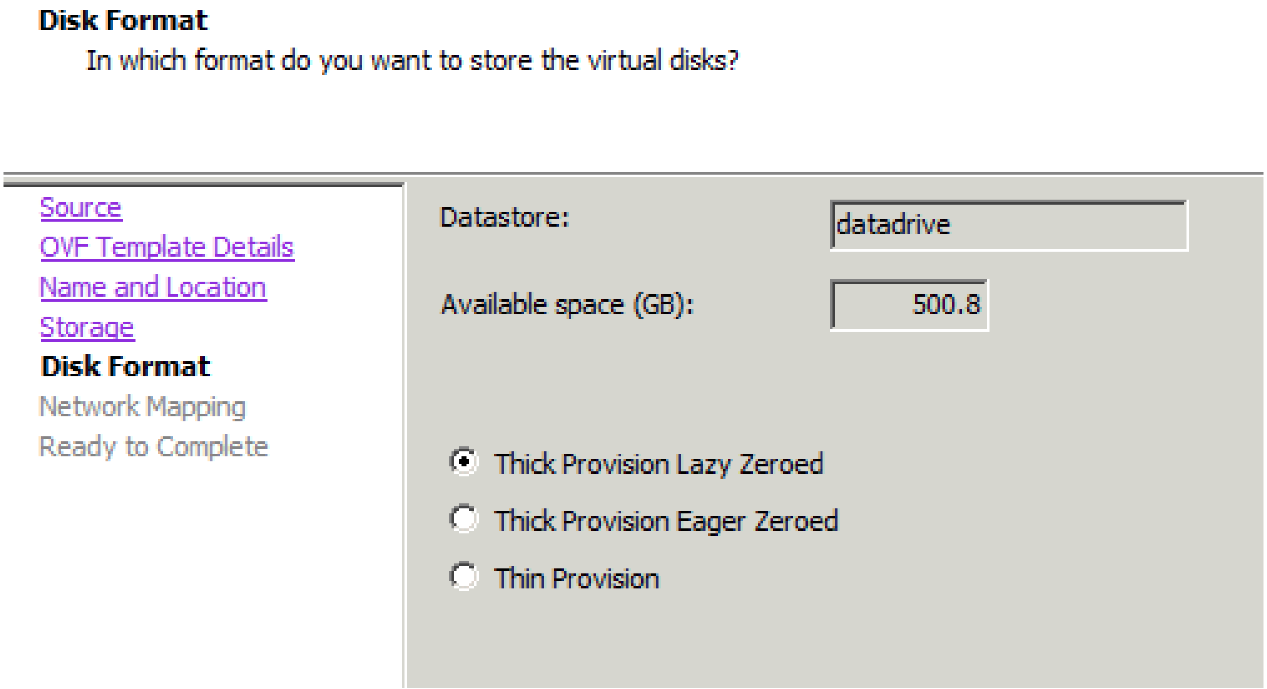


Figure 13 Virtual server layout 2

VMFS Datastores deployment on SteelFusion LUNs

When deploying **VMFS datastores on SteelFusion LUNs** make sure you choose the **Thick Provision Lazy Zeroed** disk format (VMware default).



Disk Format

In which format do you want to store the virtual disks?

Datastore: datadrive

Available space (GB): 500.8

● Thick Provision Lazy Zeroed

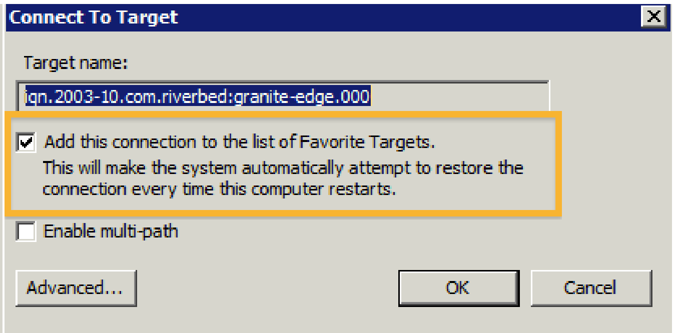
○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 14 VMware disk format

Enable Windows Persistent Bindings for mounted SteelFusion iSCSI LUNs

It is recommended to make SteelFusion LUNs persistent across windows server reboots otherwise you will need to manually reconnect them. To configure Windows servers to automatically connect to the SteelFusion LUNs after system reboots, choose the **Add this connection to the list of Favorite Targets** check box when you connect to the SteelFusion Edge iSCSI target, as shown on Figure 15



Target name:

iqn.2003-10.com.riverbed:granite-edge.000

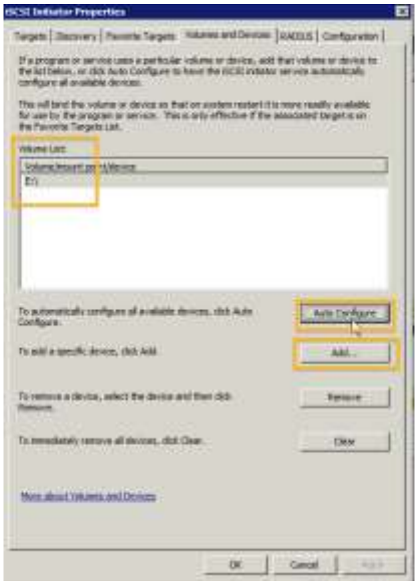
☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

Figure 15 Favorite Targets

To make SteelFusion LUNs persistent and make sure that Windows does not consider the iSCSI service fully started until connections are restored to all the SteelFusion volumes on the binding list, add the SteelFusion Edge iSCSI target to the iSCSI service's binding list. This is important particularly if you have data on a SteelFusion LUN that other services depend on. For example, if a Windows file server uses the SteelFusion iSCSI LUN as a share.

The best option is to choose the **Volumes and Devices** tab from the iSCSI Initiator's control panel and click the **Auto Configure** button, as shown on Figure 16. This will bind all available iSCSI targets to the iSCSI startup process. If you want to choose individual targets to bind, click the Add button. However, you will need to know the target's drive letter or mount point.



If a program or service uses a particular volume or device, add that volume or device to the list below, or click Auto Configure to have the iSCSI initiator service automatically configure all available devices.

This will bind the volume or device so that on system restart it is more readily available for use by the program or service. This is only effective if the associated target is on the Favorite Targets List.

Volume List:

Volume/mount point/device
E:\

To automatically configure all available devices, click Auto Configure.

To add a specific device, click Add.

To remove a device, select the device and then click Remove.

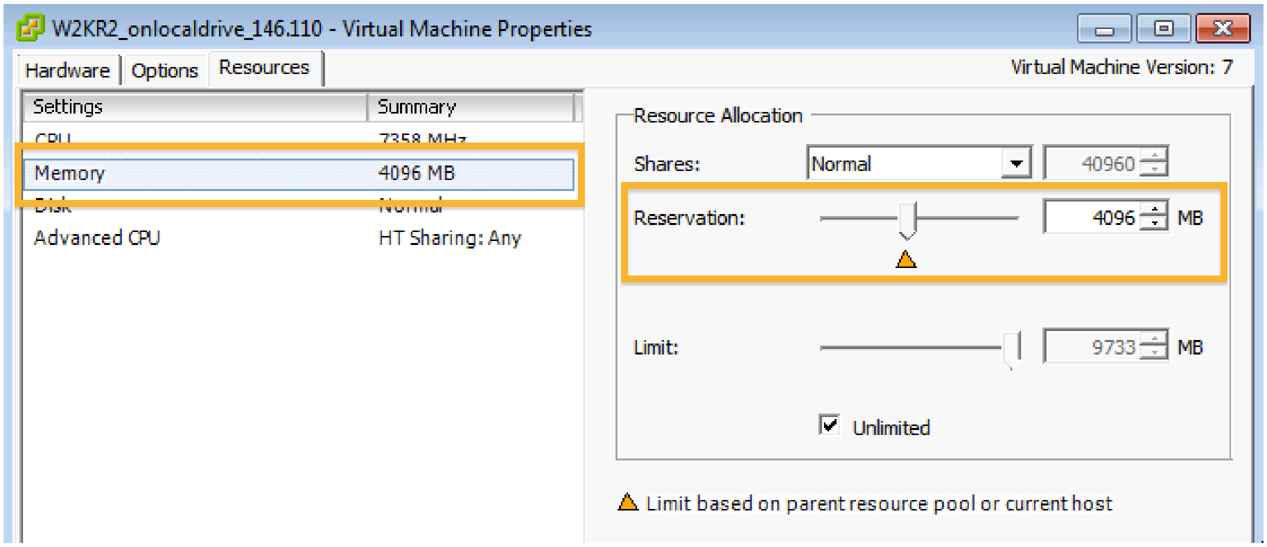
To immediately remove all devices, click Clear.

Figure 16 Target Binding

Setup Memory Reservation for Virtual Machines running on VMware ESX

By default VMware ESX dynamically tries to reclaim unused memory from guests' virtual machines, while Windows operating system uses free memory to perform caching and avoid swapping to disk.
In order to greatly improve performance of Windows virtual machines, it is recommended to configure memory reservation to the highest possible value.

Note: Setting the memory reservation to the configured size of the virtual machine results in a per virtual machine vmkernel swap file of zero bytes that will consume less storage and help increase performance by eliminating ESX host-level swapping. The guest operating system within the virtual machine maintains its own separate swap/page file.



W2KR2_onlocaldrive_146.110 - Virtual Machine Properties

Virtual Machine Version: 7

Settings	Summary
CPU	7358 MHz
Memory	4096 MB
Disk	Normal
Advanced CPU	HT Sharing: Any

Resource Allocation

Shares: Normal 40960

Reservation: 4096 MB

Limit: 9733 MB

☑ Unlimited

⚠ Limit based on parent resource pool or current host

Figure 17 Virtual Machine Memory Reservation

Boot from a Non-Pinned SteelFusion LUN

If you are booting a Windows server or client from a non–pinned SteelFusion LUN it is recommended to install the Riverbed Turbo Boot software on the Windows machine. The Riverbed Turbo Boot software greatly improves boot over the WAN performance since it allows SteelFusion Core to send to SteelFusion Edge only the files needed to the boot process.

Here the list of supported Operating Systems:

- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 r2

How to Install Riverbed Turbo Boot

1. Download turbo_boot_installer_<platform>.exe from Riverbed.com
2. Install turbo_boot_installer_<platform>.exe on the Windows virtual machine. Choose typical install

for Windows performance toolkit when asked.
3. Restart the Windows virtual machine and wait for 60 seconds after boot.
4. Verify the presence of turbo_boot.log file under C:\ProgramData\Riverbed\TurboBoot\

Running Antivirus Software

When it comes to Antivirus Software there are two common approaches to scanning data:

1. On-Demand, scan the entire LUN's data files for viruses at scheduled intervals
2. On-Access, scan the data files on the fly as they are read or written to disk

And two common locations from where to execute the scanning:

1. On-Host, antivirus software installed on the application server
2. Off-Host, antivirus software installed on dedicated servers that can access directly the application server data

In typical SteelFusion deployments where the LUNs at the data center contain the full amount of data and the branch cache contains the working set, it is recommended to run On-Demand scans at the data center and On-Access scans at the branch. Running On-Demand full file system scans at the branch will cause the SteelFusion blockstore cache to wrap and evict the working set of data leading to slow performance results. However if the LUNs are pinned, On-Demand full file system scans could also be executed at the branch. As where to execute the scanning from, the SteelFusion solution does not dictate one way versus another, but in order to minimize the server load, Off-Host virus scans are recommended.

Running Disk Defragmentation Software

Disk defragmentation software is another category of software that will possibly cause the SteelFusion blockstore cache to wrap and evict the working set of data, hence it is not recommended to execute it on SteelFusion LUNs.

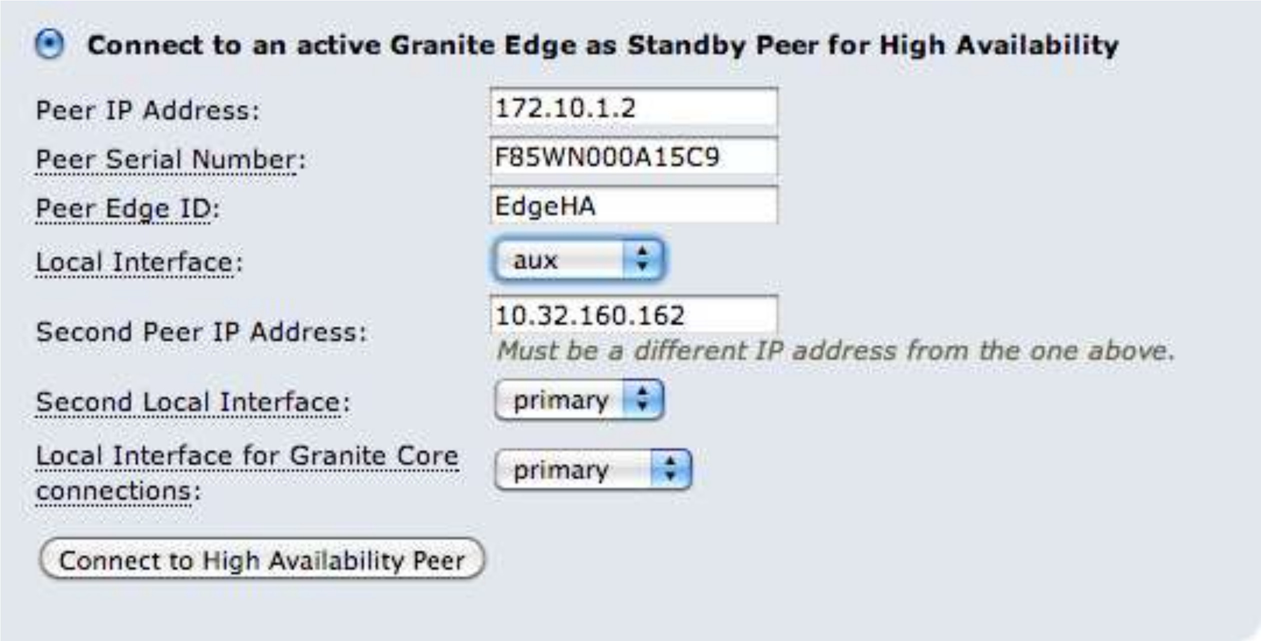
Running Backup Software

Backup software is another category of software that will possibly cause the SteelFusion blockstore cache to wrap and evict the working set of data, especially during the execution of full backups. In a SteelFusion deployment it is recommended to execute differential, incremental and synthetic full at the branch and traditional full at the data center.

Configure SteelFusion Edge High Availability

Edge high availability enables you to configure two Edge appliances so that either one can fail without disrupting the service of any of the LUNs being provided by the Core.
The active SteelFusion Edge appliance in the pair connects to the Core and serves storage data. The active peer contains the authoritative copy of the block store and configuration data. The standby SteelFusion Edge appliance is passive and does not service client requests but is ready to take over from the active peer immediately.
As the system writes new data to the active peer, it reflects the data to the standby peer, which stores a copy of the data in its local block store. The data flow across the two interfaces that you specify during the SteelFusion Edge failover configuration. The **Local Interface** is also the preferred interface for Blockstore data synchronization, it is recommended to specify the less busy interface in the system, to avoid congestion or slowdowns. In Figure 18 the preferred interface is set to **aux** since the **primary** interface is used already

for SteelFusion Core connections.



● Connect to an active Granite Edge as Standby Peer for High Availability

Peer IP Address:	172.10.1.2
Peer Serial Number:	F85WN000A15C9
Peer Edge ID:	EdgeHA
Local Interface:	aux
Second Peer IP Address:	10.32.160.162 *Must be a different IP address from the one above.*
Second Local Interface:	primary
Local Interface for Granite Core connections:	primary

Figure 18: SteelFusion Edge HA configuration

iSCSI Initiators Timeouts

Microsoft iSCSI Initiator Timeouts

By default, the Microsoft iSCSI Initiator LinkDownTime timeout value is set to 15 seconds and the MaxRequestHoldTime timeout value is set to 15 seconds. These timeout values determine how much time the initiator will hold a request before reporting an iSCSI connection error. These values can be increased to accommodate longer outages, such as a SteelFusion Edge appliance failover event or in case of single appliance a power cycle of the same.

If MPIO is installed in Microsoft iSCSI Initiator the LinkDownTime value is used. If MPIO is not installed MaxRequestHoldTime is used instead.

If you are using SteelFusion Edge in an HA configuration and MPIO is configured in the Microsoft iSCSI Initiator, change the LinkDownTime timeout value to 60 seconds to allow the failover to complete.

ESX iSCSI Initiator Timeouts

By default, the VMware ESX iSCSI initiator DefaultTimeToWait timeout is set to 2 seconds. This is the minimum time, in seconds, to wait before attempting an explicit/implicit logout or active iSCSI task reassignment after an unexpected connection termination or a connection reset. This value can be increased to accommodate longer outages, such as a SteelFusion Edge appliance failover event or in case of single appliance a power cycle of the same.

If you are using SteelFusion Edge in an HA configuration change the DefaultTimeToWait timeout value to 60 seconds to allow the failover to complete.

Network Quality of Service (QoS)

SteelFusion technology enables branch offices to utilize storage provisioned at the data center via unreliable, low bandwidth and high latency WAN links. Adding this new type of traffic to the WAN links creates new considerations in terms of guaranteeing quality of service (QoS) to existing WAN applications and to the SteelFusion Rdisk protocol to function at their best.

Rdisk Protocol Overview

In order to understand the quality of service requirements for the SteelFusion Rdisk protocol let's first describe how it works. The Rdisk protocol defines how the SteelFusion Edge and SteelFusion Core appliances communicate and how they transfer data-blocks over the WAN. Rdisk uses 5 TCP ports for data transfers and 1 TCP port for management.

The following table lists the TCP ports used by the Rdisk Protocol and maps the different Rdisk operations to each TCP port:

TCP Port	Operation:	Description
7970	Management	Used for management information exchange between Edge and Core appliances
7950	Read	Used to transfer data requests for data-blocks absent in Edge from the data center
7951	Write	Used to transfer new data created at the Edge to the data center
7952	Prefetch0	Prefetch Data for which SteelFusion has highest confidence (example: file Read Ahead)
7953	Prefetch1	Prefetch Data for which SteelFusion has medium confidence (example: Boot)
7954	Prefetch2	Prefetch Data for which SteelFusion has lowest confidence (example: Prepop)

Table 1 Rdisk Protocol TCP Ports

Note: Rdisk Protocol creates 5 TCP connections per exported LUN.

Rdisk QoS requirements

As shown on Table 2 Rdisk QoS different Rdisk operations use different TCP ports. The following table lists Rdisk QoS requirements for each Rdisk operation and relative TCP port:

TCP Port	Operation	Outgoing Branch Bandwidth	Outgoing Branch Priority	Outgoing Data Center Bandwidth	Outgoing Data Center Priority
7970	Management	Low	Normal	Low	Normal
7950	Read	Low	Business-Critical	High	Business-Critical
7951	Write	High (off-peak hours) Low (during-peak hours)	Low-Priority	Low	Normal
7952	Prefetch0	Low	Business-Critical	High	Business-Critical
7953	Prefetch1	Low	Business-Critical	Medium	Normal
7954	Prefetch2	Low	Business-Critical	Low	Best-Effort

Table 2 Rdisk QoS Requirements

QoS for SteelFusion Replication Traffic

In order to prevent SteelFusion replication traffic from consuming bandwidth required for other applications during business hours, it is recommended to allow more bandwidth for Rdisk Write traffic (port 7951) during off-peak hours a less bandwidth during peak hours. However carefully consider your RPO and RTO objectives when configuring QoS for Rdisk SteelFusion traffic.

Moreover depending upon which SteelFusion features you decide to use, different priorities and different bandwidth requirements might need to be considered.

QoS for Non-pinned LUNs

In a non-pinned LUNs scenario it is recommended to prioritize traffic on port 7950 so that the SCSI Read requests for data blocks not present on the Edge Blockstore cache can arrive from the data center LUN in timely manner. It is also recommended to prioritize traffic on ports 7952, 7953 and 7954 so that the Prefetch data can arrive at the Branch Blockstore when needed.

QoS for Pinned LUNs

In a pinned LUN scenario since the data will be all present at the edge it is only recommended to prioritize port 7951 so that the Rdisk protocol can transfer newly written data blocks from the Edge Blockstore to the data center LUN via SteelFusion Core appliance.

QoS for Branch Offices that mainly read data from the data center

In the case branch office users are not producing new data but mainly reading data from the data center like for non-pinned LUNs it is recommended to prioritize traffic on port 7950 and 7952 so that the SCSI Read requests for data blocks not present on the Edge Blockstore cache can arrive from the data center LUN in timely manner.

QoS for Branch Offices booting virtual machines from the data center

In the case branch office users are booting virtual machines from the data center and the LUNs are not pinned it is recommended to prioritize traffic on port 7953 so that the SCSI Read requests for data blocks required for Windows booting can arrive from the data center LUN in timely manner.

Time Based QoS Rules Example

This example illustrates how to configure time based QoS rules on a Steelhead appliance.

The idea is to create two recurring jobs, each undoing the other, using the standard 'job' cli command. One sets the daytime cap on throughput or a low minimum guarantee and the other then removes that cap or sets a higher minimum guarantee.

```
steelhead (config) # job 1 date-time hh:mm:ss year/month/day    “Start time”
steelhead (config) # job 1 recurring 864000                    “Occurs once a day”
steelhead (config) # job 1 command 1 <command>
steelhead (config) # job 1 command 2 <command2>                 “Commands to set daytime cap”
steelhead (config) # job 1 enable
steelhead (config) # job 2 date-time hh:mm:ss year/month/day     “Start time”
steelhead (config) # job 2 recurring 864000                       “Occurs once a day”
steelhead (config) # job 2 command 1 <command>
steelhead (config) # job 2 command 2 <command2>>                   “Commands to remove daytime cap”
steelhead (config) # job 2 enable
```

At-rest and In-flight data security

SteelFusion Edge appliance provides data at-rest encryption capabilities for the data-blocks written on the Blockstore cache for organizations that require high levels of security or face stringent compliance requirements. Encryption standards supported include AES-128, AES-192, and AES-256 and keys are maintained in an encrypted secure vault. The U.S. government declared in a 2003 review of the algorithm that any of the three key lengths is sufficient for protection of classified information up to the SECRET level, while TOP SECRET information requires 192- or 256-bit keys.
The vault is encrypted by AES with a 256-bit key and a 16-byte cipher, and must be unlocked before the Blockstore is available. The secure vault password is verified upon every power up of the appliance, assuring data confidentiality in case the SteelFusion Edge appliance is lost or stolen. Initially, the secure vault has a default password known only to the RiOS software so the SteelFusion Edge appliance can automatically unlock the vault during system startup. You can change the password and the SteelFusion Edge appliance will not automatically unlock the secure vault during system start up and the Blockstore will not be available until you enter the password.

When the system boots, the contents of the vault are read into memory, decrypted, and mounted (via EncFS, a FUSE-based cryptographic file system). Since this information is only in memory, when an appliance is rebooted or powered off, the information is no longer available and the in-memory object disappears. Decrypted vault contents are never persisted on disk storage.

It is very important to keep your secure vault password safe. Customer's private keys cannot be compromised so there is NO password recovery. In the event of a lost password, you can reset the secure vault only after erasing all the information within the secure vault.

To reset the lost the password, log in to the SteelFusion Edge appliance and using the CLI and type this command:

```
➢ enable
  # config term
  (conf)# secure-vault clear
```

By running this command, you will lose the data in the SteelFusion Edge Blockstore, if it was encrypted. You will need to re-load or regenerate the certificates and private keys.

Note: The SteelFusion Edge Blockstore encryption is the same mechanism as is used by RiOS for the Steelhead data store encryption. For detailed information see Chapter 18 (Security) of the Riverbed Steelhead Deployment Guide.

Configuring data encryption requires extra CPU resources and might affect performance, hence it is recommended to enable Blockstore encryption only if high level of security is required or dictated by compliance requirements.

Enable data at-rest Blockstore Encryption

This example illustrates how to configure Blockstore encryption on a SteelFusion Edge appliance. Like most of the configuration also for Blockstore encryption the commands are executed on the SteelFusion Core appliance at the data center.

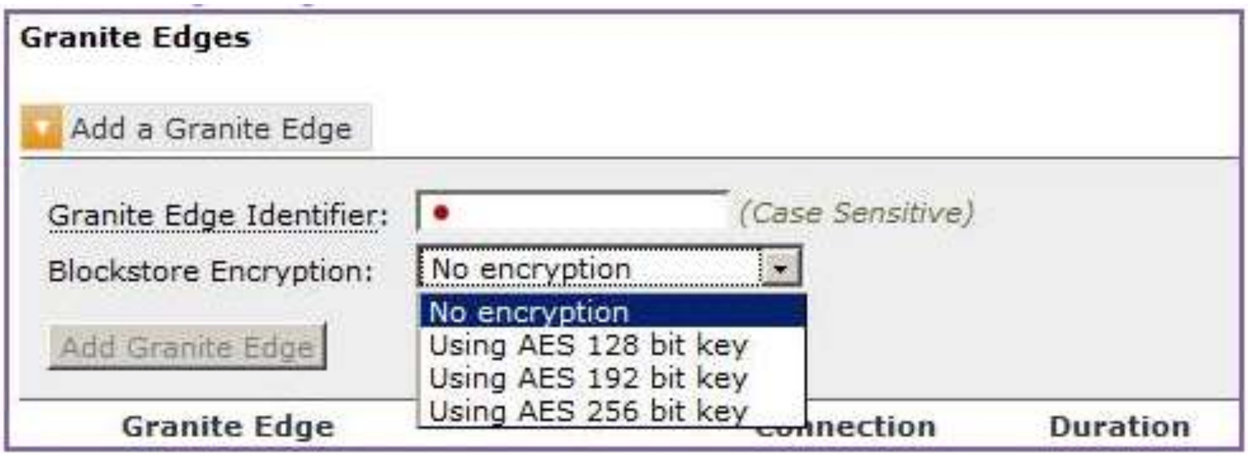
To enable encryption on the CLI enter the following command to the system prompt:

```
> enable
# configure
(config) # edge id < edge-identifier > blockstore enc-type < AES_128 | AES_192 | AES_256 | NONE >
```

To verify if encryption has been enabled on your SteelFusion Edge device enter the following command to the system prompt:

```
> enable
# show edge id <edge-identifier> blockstore
Write Reserve          : 10%
Encryption type        : AES_256
```

To enable encryption on the GUI select the encryption type from the dropdown menu when adding a new edge device to your SteelFusion Core configuration, as shown in Figure 19

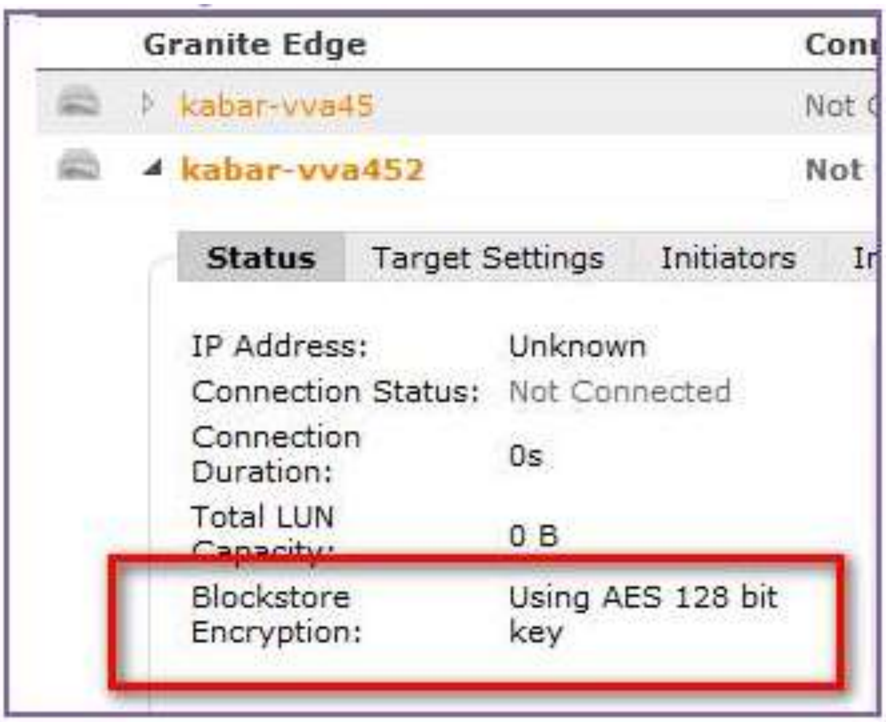

Granite Edges

Granite Edge Identifier: (Case Sensitive)

Blockstore Encryption: No encryption

Figure 19 Adding Blockstore Encryption

To verify if encryption is enabled on your SteelFusion Edge device, look at the Blockstore Encryption field on your SteelFusion Edge status window, as shown in



IP Address: Unknown
Connection Status: Not Connected
Connection Duration: 0s
Total LUN Capacity: 0 B
Blockstore Encryption: Using AES 128 bit key

Figure 20 Verify Blockstore Encryption

Enable Data in-flight Secure Peering Encryption

SteelFusion Rdisk protocol operates on clear text and hence there is a chance that branch data might be exposed to hackers while in transfer over the WAN. For this, the SteelFusion Edge appliance provides data in-flight encryption capabilities when the data-blocks are asynchronously propagated to the data center LUN. Secure Peering between SteelFusion Edge appliance and the data center Steelhead can be configured to create a secure SSL channel and protect the data in-flight over the WAN. For detailed information about the enabling data in-flight encryption, see Chapter 18 (Security) of the Riverbed Steelhead Deployment Guide.

Operating System Patching

How to perform patching at the branch for virtual servers installed on SteelFusion LUNs

You can continue to use the same methodologies and tools to perform patch management on physical or virtual branch servers booted over the WAN using SteelFusion.

How to perform patching at the data center for virtual servers installed on SteelFusion LUNs

If you want to perform virtual server patching at the data center and save a round-trip of patch software from the data center to the branch office follow these simple steps:

At the branch:

1. Power the virtual machine down.
2. Take the VMFS data store offline.

At the data center:

3. Unmap the LUN from the SteelFusion Core appliance
4. Remap and mount the LUN to a temporary ESX server
5. Power up the virtual machine, apply patches and File system updates.
6. Power the virtual machine down.
7. Take the VMFS data store offline.
8. Remap the LUN to SteelFusion Core and export it to SteelFusion Edge.

At the branch:

9. Take the VMFS data store online
10. Boot the virtual machine back up.

Conclusion

Riverbed continues to help organizations gain better control over their IT infrastructure and consolidate more to lower costs and risks without impacting the performance required to ensure user productivity in branch offices. With the SteelFusion solution, Riverbed enables a global storage infrastructure by intelligently accelerating storage protocols across the WAN, enabling new efficiency with data management, protection, and recovery while ensuring performance a the Edge. With SteelFusion, organizations can:

- Reduce costs by eliminating storage from branch offices
- Improve management efficiency as maintenance and backup can take place at the data center
- Recover faster and more effectively since the data is stored centrally, protected more frequently, and can be streamed to the branch office as needed
- Improve security of data assets via centralization and state-of-the-art encryption capabilities

Riverbed Technology, Inc.
680 Folsom Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell. RG42 1NG
United Kingdom
Tel: +44 1344 31 7100

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990