

SteelFusion™ with Amazon Web Services Storage Gateway

Solution Guide

July 2014

NOTICE: **New Product Names**

The contents of this asset do not reflect our recent product name changes. Here are the new Riverbed® names:

Old Names	New Names
Steelhead	SteelHead™
RPM, OPNET, Cascade	SteelCentral™
Stingray	SteelApp™
Granite	SteelFusion™
Flyscript	SteelScript™
Whitewater	SteelStore™

© 2014 Riverbed Technology, Inc. All rights reserved.

Riverbed®, SteelApp™, SteelCentral™, SteelFusion™, SteelHead™, SteelScript™, SteelStore™, Steelhead®, Cloud Steelhead®, Virtual Steelhead®, Granite™, Interceptor®, Stingray™, Whitewater®, WWOS™, RiOS®, Think Fast®, AirPcap®, BlockStream™, FlyScript™, SkipWare®, TrafficScript®, TurboCap®, WinPcap®, Mazu®, OPNET®, and Cascade® are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

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

PREFACE	3
About This Guide	3
<i>Audience</i>	3
Contacting Riverbed.....	3
<i>Internet</i>	3
<i>Technical Support</i>	3
<i>Professional Services</i>	3
Chapter 1 Solution Overview	4
SteelFusion Overview	4
Amazon Web Services Storage Gateway Storage Concepts Review.....	5
A New Paradigm For Delivering Hybrid Cloud Branch Services	6
Chapter 2 Deploying SteelFusion Appliances with AWS Storage Gateway	8
Deployment Prerequisites	8
Overview	8
Deployment Steps.....	9
<i>AWS Storage Gateway Deployment Steps</i>	9
<i>SteelFusion Core Deployment Steps</i>	11
<i>Configure Initiator Access for Branch Servers on the SteelFusion Core</i>	15
Chapter 3 Performing Branch Disaster Recovery.....	19
Configure the LUN to a New SteelFusion Edge at a Different Branch	19
Configure the LUN Directly to a Windows Server in the Data Center	20
Configure the LUN to Directly to a VMware ESXi Server in the Data Center	21
Chapter 4 Performing Data Center Disaster Recovery	23
Chapter 5 Solution Recommendations and Best Practices	26
AWS Storage Gateway Best Practices	26
SteelFusion Best Practices	26

PREFACE

Welcome to the SteelFusion solution guide for Amazon Web Services Storage Gateway. Read this preface for an overview of the information provided in this guide and contact information. This preface includes the following sections:

- About This Guide
- Contacting Riverbed

About This Guide

This paper details the steps to deploy Riverbed® SteelFusion appliances with an existing Amazon Web Services Storage Gateway in order to expose one or more iSCSI LUNs to a data center or remote site. After completing the steps in this guide, the iSCSI LUNs available through the SteelFusion Edge can then be attached to the desired systems through normal attach procedures in the operating system or device.

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:

- Amazon Web Services Storage Gateway management interface.
- Riverbed SteelHead™ management interface.
- Riverbed SteelHead appliance installation and configuration process

Note: The SteelFusion solution was previously referred to as Granite. Not all product user interfaces (UI) and documentation have been updated to reflect this new name. Several images and references to Granite in this document are intentional and designed to reflect the current versions of these products. SteelFusion and Granite refer to the same product, and the name does not impact the operations or performance of the solution. These terms are interchangeable.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

Internet

You can learn about Riverbed products through the company Web site: <http://www.riverbed.com>.

Technical Support

If you have problems installing, using, or replacing Riverbed products, contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States. You can also go to <https://support.riverbed.com>.

Professional Services

Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/us/products/professional_services/.

Chapter 1 Solution Overview

According to IDC, to meet the demands of global customer and global talent requirements, companies have to maintain remote offices. Companies are spending over \$4 billion on remote office IT support. These islands of distributed branch infrastructure have been necessary to meet local performance and reliability needs to ensure the productivity of these remote offices; however, they are costly and inefficient to manage. Because of these inefficiencies, companies rarely can afford to have the expertise in branches to maintain operation and protect data in such distributed infrastructure. Therefore when branch offices suffer outages due to natural or manmade disasters, productivity and data are compromised and company revenue is impacted. Centralizing and consolidating data is key to eliminating these issues; however only 8 percent of branch offices consolidate data in the data center, which increases companies' exposure to data theft, data loss and downtime due to outages or natural disasters.

Riverbed SteelFusion is a branch converged infrastructure solution, encompassing server, projected storage, networking, and WAN optimization. SteelFusion can be fully deployed and administer from a central location, eliminates the need for remote onsite IT. SteelFusion allows for the consolidation of all data/storage (server OS's, application, and data) into the datacenter, where it can be managed and protected (backed up), while projecting it out the branch. This is accomplished without sacrificing any of the benefits (performance & access) of having servers and data at the Edge, close to end-users. SteelFusion ability to have near-instant continuance of operations to any location, guarantees the highest operational levels with little to no loss in productivity. With SteelFusion, businesses can restore operations in a matter of minutes vs. days, centrally protect and secure data, and significantly lower the TCO of branch and remote offices.

Riverbed SteelFusion appliances can help consolidate distributed data, improve security, and reduce administration for managing remote / branch office environments. When utilized with Amazon Web Services Storage Gateway (AWS Storage Gateway), SteelFusion can expose one or more iSCSI LUNs to remote / branch offices. After completing the steps in this guide, the iSCSI LUNs can then be attached to the desired systems through normal attach procedures in the operating system or device.

This chapter includes the following sections:

- SteelFusion Overview
- Amazon Web Services Storage Gateway Storage Concepts Review

SteelFusion Overview

SteelFusion is a converged infrastructure solution purpose-built for the branch. Unlike traditional converged infrastructures, SteelFusion enables “stateless” branch services. Users access applications running locally in the branch while the primary data is centralized in the datacenter. Decoupling compute from its underlying storage allows applications to run in a stateless mode, which reduces your branch footprint and centralizes management of your branch services.

SteelFusion consists of two components:

- **SteelFusion Edge:** A converged appliance that integrates server, storage, network, and virtualization to run local branch apps, eliminating the need for additional branch infrastructure.
- **SteelFusion Core:** A storage delivery controller in the datacenter that interfaces with your storage area network (SAN). This projects centralized data out to branches, eliminates branch backups, and provides instant provisioning and recovery of branch services.

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

SteelFusion Core mounts iSCSI or Fibre Channel LUNs provisioned in the data center and shares the storage resources with branch offices running the SteelFusion Edge appliance. SteelFusion Edge virtually presents one or more iSCSI targets in the branch which can be utilized by services and systems running both within the Riverbed Virtual Services Platform (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.

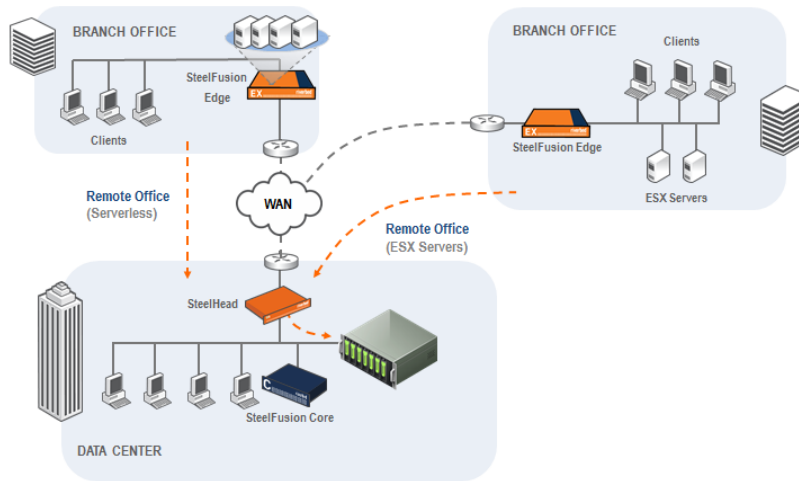


Figure 1: SteelFusion High Level Topology

Amazon Web Services Storage Gateway Storage Concepts Review

The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. The service allows you to securely store data in the AWS cloud for scalable and cost-effective storage. The AWS Storage Gateway supports industry-standard storage protocols that work with your existing applications. It provides low-latency performance by maintaining frequently accessed data on-premises while securely storing all of your data encrypted in Amazon Simple Storage Service (Amazon S3) or Amazon Glacier.

The AWS Storage Gateway delivers 2 configurations which are compatible with SteelFusion:

Gateway-Cached Volumes: You can store your primary data in Amazon S3, and retain your frequently accessed data locally. Gateway-Cached volumes provide substantial cost savings on primary storage, minimize the need to scale your storage on-premises, and retain low-latency access to your frequently accessed data, as shown in Figure 2 Amazon Web Services Storage Gateway.

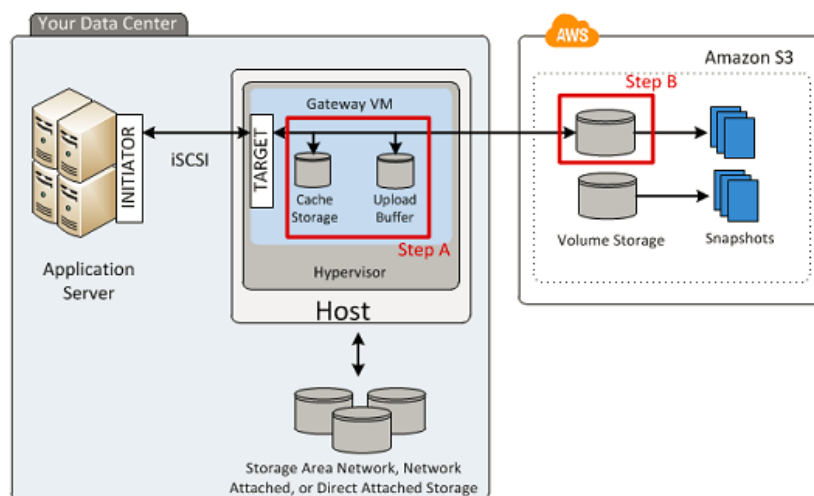


Figure 2 Amazon Web Services Storage Gateway (Gateway-Cached Configuration)

Gateway-Stored Volumes: In the event you need low-latency access to your entire data set, you can configure your on-premises gateway to store your primary data locally, and asynchronously back up point-in-time snapshots of this data to Amazon S3 as shown in Figure 3. Gateway-Stored volumes provide durable and inexpensive off-site backups that you can recover locally or from Amazon EC2 if, for example, you need replacement capacity for disaster recovery.

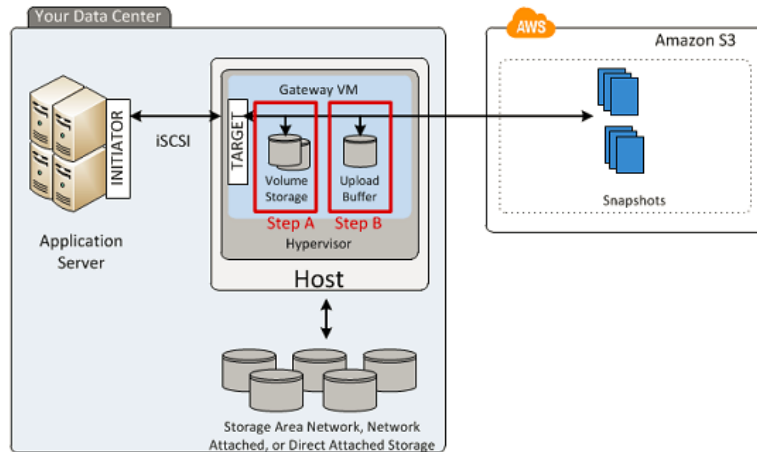


Figure 3 Amazon Web Services Storage Gateway (Gateway-Stored Configuration)

A New Paradigm For Delivering Hybrid Cloud Branch Services

SteelFusion, when used in conjunction with an AWS Storage Gateway and Amazon cloud storage, delivers unparalleled data availability, flexibility and protection for branch infrastructure, while simultaneously reducing data center storage requirements and improving data availability and recoverability by leveraging cheap, elastic cloud storage delivered via Amazon cloud storage services (Figure 4 SteelFusion and AWS Storage Gateway). By using an AWS Storage Gateway with SteelFusion, businesses can begin the transition to a storage-less data center, where all storage is served by the cloud on demand, through SteelFusion, to applications and users.

Branch offices with constrained network links now enjoy all the same cloud storage benefits that data centers enjoy through the use of SteelFusion and Amazon without compromising data, performance, and application availability. The problems of delivering cost effective storage to branches that can be managed and controlled centrally has been improved, allowing for an storage tier that can efficiently and effectively scale with business requirements. Rebuilding damaged or destroyed branch office environments is no longer a days-long recovery time objective, but one that can be compressed to as little as an hour, even though data resides two links away within Amazon cloud storage. And with the ability to utilize Amazon Direct Connect capabilities, SteelFusion can consolidate storage services away from the data center into managed public or private clouds, allowing businesses to access cloud storage at high bandwidth speeds and without the need to have a true data center storage environment.

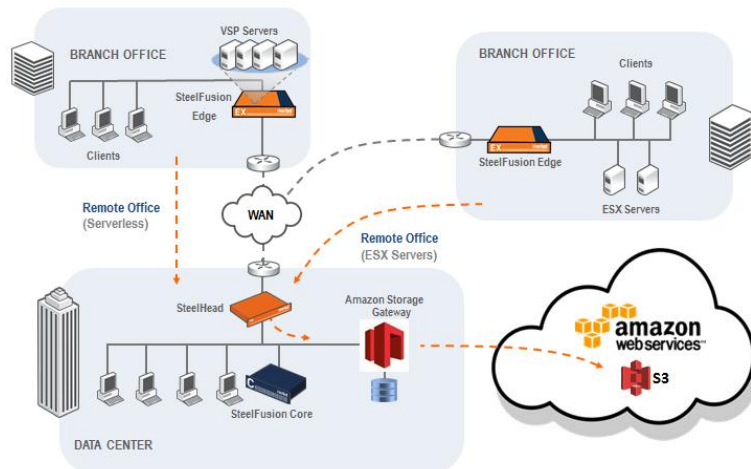


Figure 4 SteelFusion and AWS Storage Gateway Topology

Chapter 2 Deploying SteelFusion Appliances with AWS Storage Gateway

This chapter describes the process and procedures for deploying SteelFusion appliances with the AWS Storage Gateway. It includes the following sections:

- Deployment Prerequisites
- Overview
- Deployment Steps
 - AWS Storage Gateway Deployment Steps
 - SteelFusion Core Deployment Steps

Deployment Prerequisites

- An Amazon Web Services Storage Gateway licensed and configured in either gateway cache or gateway stored mode.
- Administrator access to the Amazon Web Services Storage Gateway and SteelFusion appliances to make changes such as enabling iSCSI, adding initiator groups, etc.
- SteelFusion Core and SteelFusion Edge appliances installed and powered up.

Overview

The deployment steps required to deliver LUNs via SteelFusion appliances from an existing Amazon Web Services Storage Gateway are broken down into the following sections:

AWS Storage Gateway Deployment Steps

1. Deploy the AWS Storage Gateway virtual appliance
2. Configure local storage for the AWS Storage Gateway
3. Activate the AWS Storage Gateway
4. Configure the storage volume for the AWS Storage Gateway

SteelFusion Core Deployment Steps

1. Add the LUN from the AWS Storage Gateway to SteelFusion Core
2. Configure initiator access for the SteelFusion Edge to the projected LUN from SteelFusion Core

Deployment Steps

AWS Storage Gateway Deployment Steps

1. From the [Amazon web services storage gateway page](http://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStartedDownloadVM-common.html), download and install the AWS Storage Gateway virtual machine (VM), as shown in Figure 5 and Figure 6. Install in either a Gateway-cached or Gateway-Stored configuration. Refer to the directions on the following page for details about downloading the VM:
<http://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStartedDownloadVM-common.html>

Setup and Activate Gateway
Close

Choose How You Want to Run Your Gateway

Please select a configuration for running your gateway

☒ **Gateway-Cached volumes:** Maintain local, low-latency access to your most recently accessed data while storing all your data in Amazon S3.

☐ **Gateway-Virtual Tape Library:** Durably store data on Amazon Glacier while leveraging your existing tape-based processes.

☐ **Gateway-Stored Volumes:** Schedule off-site backups to Amazon S3 for your on-premises data.

[Learn More About Gateway Configurations](#)

Continue

Figure 5 AWS Storage Gateway Type Selection

Setup and Activate Gateway
Close

You will need a host in your datacenter to deploy the gateway virtual machine (VM). Pick a host that meets these [minimum requirements](#).

[< Back](#)

Continue

Figure 6 AWS Storage Gateway VM Deployment

2. Once the VM is installed you will need to size and configure local storage volumes for the AWS Storage Gateway to use as either cache and buffer volumes (Gateway-Cached configuration), or as buffer and storage volumes (Gateway-Stored configuration), as shown in Figure 7. Refer to the directions on the following page for details:
<http://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStartedPLDSMain-vm-common.html>

Setup and Activate Gateway

Close



Step 2 of 2 (Allocate Disks to Cache Storage)

Again using your VMware vSphere client, allocate one or more local disks to your gateway VM to cache recently accessed data on-premises. These disks, called cache storage, are used to provide low-latency access to data you actively access.

[Step-by-Step Instructions](#)

Calculator

Enter the size of your upload buffer:

 GBs

For corporate file sharing workloads, enter 20% of your current on-premises file share storage.

For other workloads like backup, leave blank:

 GBs

Recommended storage for caching data:

-- GBs

[« Back](#)

Continue

Figure 7 Allocate Local Disks for the VM

- Next you will need to activate the AWS Storage Gateway, as shown in Figure 8. Refer to the directions on the following page for details:

<http://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStartedActivateGateway-common.html>

Setup and Activate Gateway

Close



Using your VMware vSphere client, right mouse-click on your deployed gateway VM and select Power On. Next, click on the Summary tab and retrieve the IP Address of your VM (it may take a couple of minutes for the IP Address to appear once you've powered on your VM). Type the IP Address into the box below.

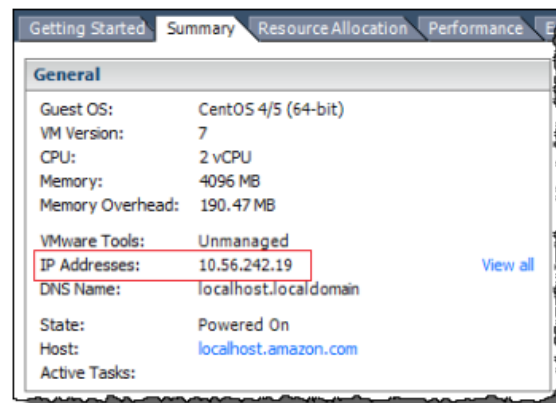
Clicking "Proceed to Activation" will redirect you to the activation page (your browser must be running on a machine with network connectivity to your local gateway host).

[Step-by-Step Instructions](#)

Enter IP Address Below:

[« Back](#)

Proceed to Activation



Screenshot showing the Summary tab.

Figure 8 Activate VM

- Configure storage in Amazon S3 for the AWS Storage Gateway, as shown in Figure 9. If using a Gateway-Cached configuration, specify the volume size you want to create. If using a Gateway-Stored configuration, specify the local volume in the VM you created previously that will be assigned for use. Refer to the directions on the following page for details: <http://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStartedCreateVolumes.html>

Configure Your Activated Gateway
close

▼
○

CONFIGURE LOCAL STORAGE
CREATE VOLUME

Create an iSCSI storage volume up to 32 TBs in size. This volume will be stored in Amazon S3, with only a cache of recently accessed data kept locally. Your client applications will connect to this volume over an iSCSI interface. [Learn More.](#)

Capacity:

TBs

TBs

GBs

(Max: 32 TBs)

iSCSI Target Name:

Based on Snapshot ID:

Host IP:

Port:

Cancel
Create Volume

Figure 9 Configure iSCSI Storage

SteelFusion Core Deployment Steps

Both the physical SteelFusion Core or the SteelFusion Core Virtual Edition can be used to connect to the Amazon Storage gateway.

Add the LUN from the AWS Storage Gateway to SteelFusion Core

- Open the **Configure** menu from the top menu of the SteelFusion Core web user interface and select **Setup Wizard** to open the wizard as shown in Figure 10.

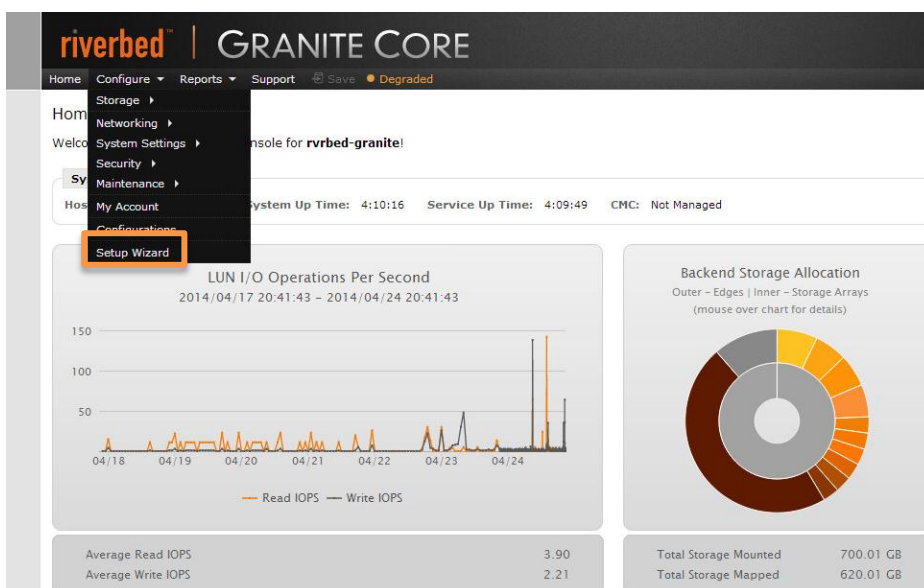


Figure 10 SteelFusion Setup Wizard

- On the welcome page select **LUN Mapping** to open the LUN mapping wizard as shown in Figure 11.

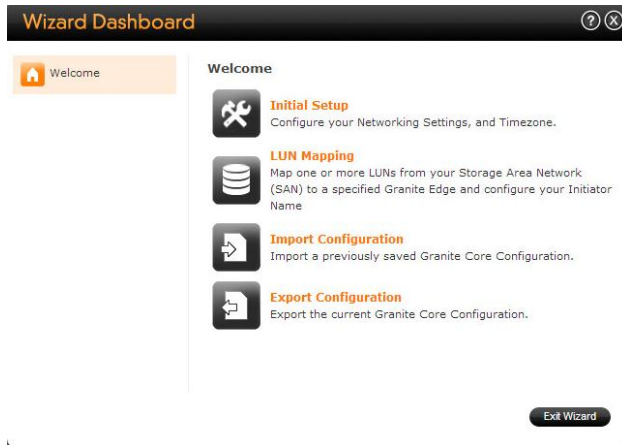


Figure 11 Welcome Page

- Verify the SteelFusion Core iSCSI Initiator Name and click **Next** twice. Enter the **IP address** for the Amazon Web Services Storage Gateway iSCSI interface and select **Next** as shown in Figure 12.

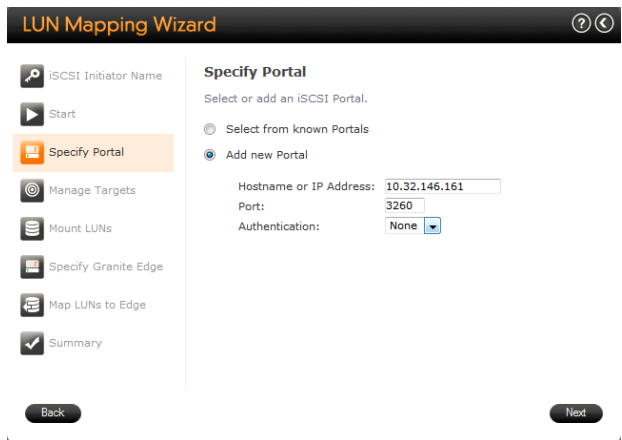


Figure 12 Portal Configuration Page

- The Amazon Web Services Storage Gateway iSCSI Target should now be present in the Manage Targets window. Select the **node name** and select **Next** as shown in Figure 13.

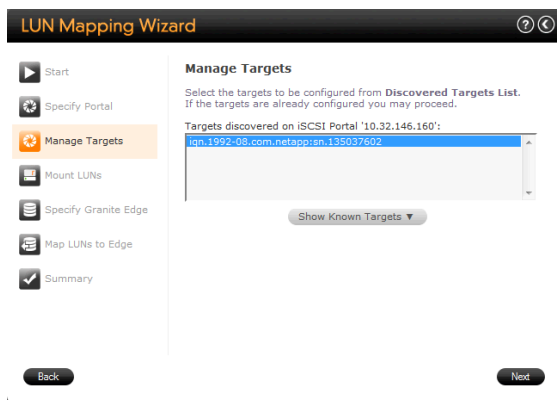


Figure 13 Target Configuration Page

5. The discovered LUN serial numbers should now be present in the Mount LUNs window. Select the **LUN** you wish to export to the branch office and select **Next** as shown in Figure 14.

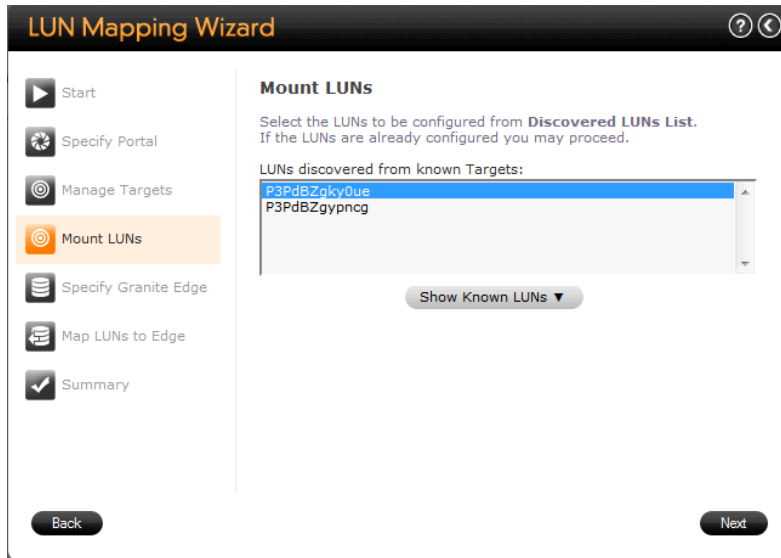


Figure 14 Mount LUNs Page

6. Select the **SteelFusion Edge appliance** you would like to export the LUN to and select **Next**, as shown in Figure 15.



Figure 15 SteelFusion Edge Mapping Page

Note: Determine the SteelFusion Edge Identifier in the **Configure > Granite > Granite Storage** configuration page of the SteelFusion Edge web user interface as shown in Figure 16.

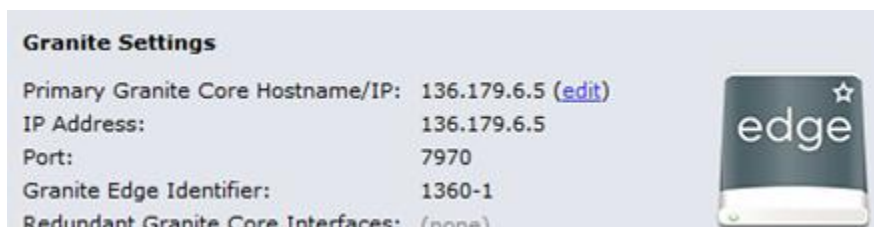


Figure 16 SteelFusion Edge Identifier

- The Amazon Web Services Storage Gateway LUN serial number should now be present in the Map LUNs to Edge window. Select the **LUN serial number** and select **Next** to map this iSCSI LUN to the remote SteelFusion Edge appliance as shown in Figure 17.

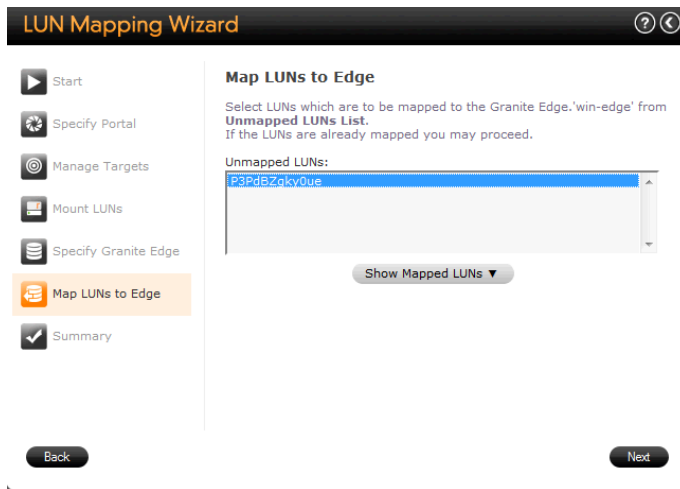


Figure 17 Map LUNs page

- You have completed the LUN Mapping. Select **Exit** to finish as shown in Figure 18.

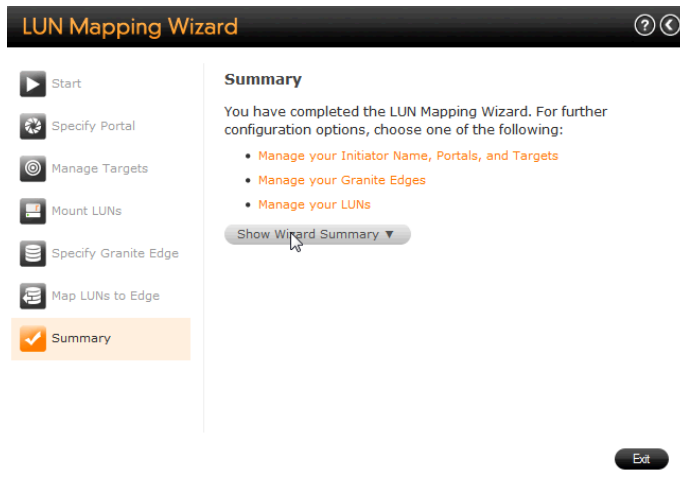


Figure 18 LUN Summary Page

9. Next, verify that the LUN has been exported to SteelFusion Edge by navigating to the **Configure > Granite > Granite Storage** configuration page of the SteelFusion Edge web user interface as shown in Figure 19.

riverbed Steelhead EX

Home | Configure | Reports | Support | Save | Restart | Degraded

Granite Storage

Configure > Granite > Granite Storage

Granite Settings

Primary Granite Core Hostname/IP: 136.179.6.5 ([edit](#))
 IP Address: 136.179.6.5
 Port: 7970
 Granite Edge Identifier: 1360-1
 Redundant Granite Core Interfaces: (none) [Add Hostname/IP](#)
 Local Interfaces: primary ☒ [Add Interface](#)
[Remove Core](#)

Granite Core Connection Status
 Connected to Granite Core

Blockstore Allocation | Target Details | Initiators | Initiator Groups | **LUNs** | MPIO

	LUN Alias (Serial) ↑↓	Type ↑↓	Status ↑↓	LUN ID ↑↓	Size ↑↓	Cached Data ↑↓	Pinned ↑↓	Client Type ↑↓
	Q 1360-1Desktop (0001H)DUhpmV	iSCSI	Connected	2	30.0057 GB	3081.6 MB	No	Other
	Q 54FreeFileServer (0001H)DUhpnR	iSCSI	Connected	3	20 GB	724.1 MB	No	Other

Figure 19 SteelFusion Edge LUNs Page

Configure Initiator Access for Branch Servers on the SteelFusion Core

SteelFusion appliances implement the concept of initiator groups. By default the exported LUNs from SteelFusion are not associated to any initiator or initiator group, as shown in Figure 20.

[+ Add a Granite Edge](#)

Granite Edge	Connection	Duration	IP Address	Mapped LUNs	LUN Capacity	Remove
win-edge	Connected	35m 32s	10.32.98.30	1 LUN	60.00 GB	

Status | Target Settings | Initiators | Initiator Groups | **LUNs** | Prepopulation

[+ Map LUNs to this Granite Edge](#)

LUN	Size	Online/Offline	Accessible	Pinned	Unmap
alias-P3Pd8Zgky0ue (P3Pd8Zgky0ue)	60.0038 GB	Online	No	No	

Manage Access Lists (To perform other operations on this LUN, [click here.](#))

Groups Granted Access [Edit ▶](#)

None

Initiators Granted Access [Edit ▶](#)

None

Figure 20 Default Initiator and Initiator Group Configuration

1. Configure initiators and initiator groups in the **Configure > Storage > SteelFusion Edges** page of the SteelFusion Core GUI.

Select the SteelFusion Edge for which you would like to configure initiators groups, select **Initiators**, select **Add an Initiator**, enter the **initiator IQN or EUI** number and select **New Group** as shown in Figure 21.

Note: Refer to documentation from the server vendor that will act as the iSCSI initiator for determining the IQN or EUI number

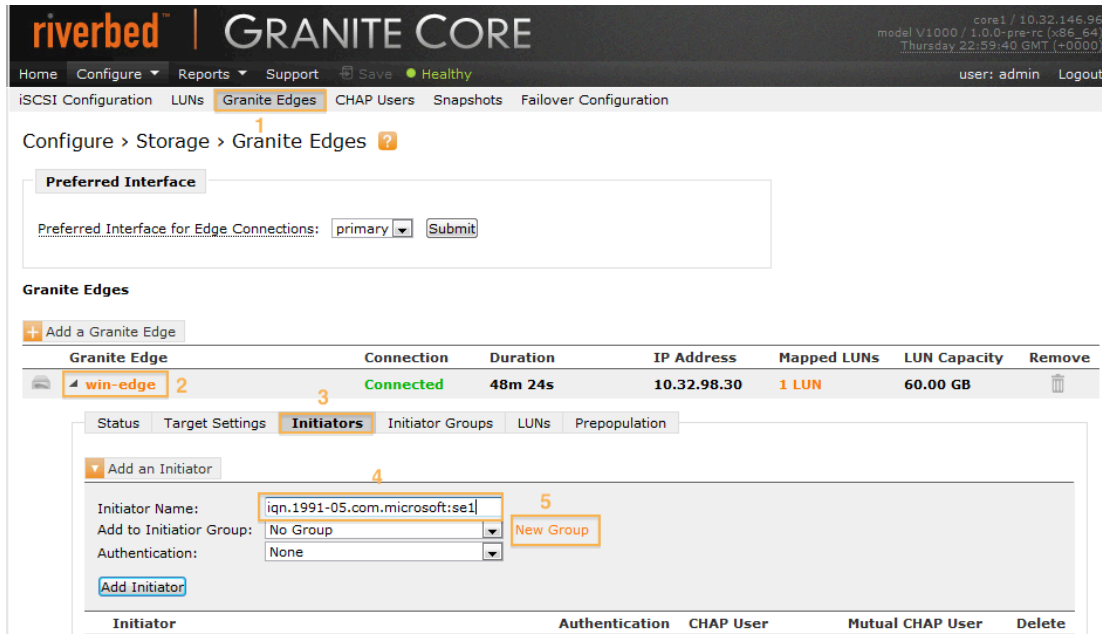


Figure 21 SteelFusion Initiator Page

2. Enter a new **Group Name** and select **Add** as shown in Figure 22.

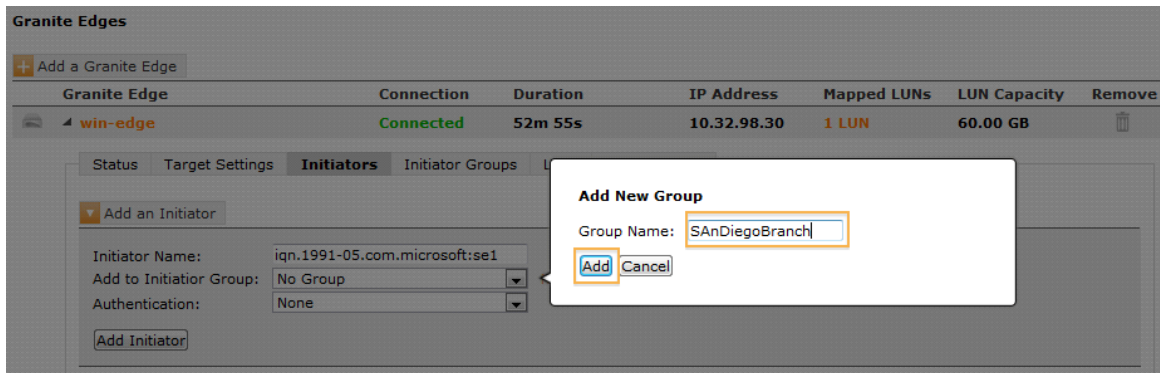


Figure 22 Add Group Dialog

3. Complete the procedure by selecting **Add Initiator** as shown in Figure 23.

Granite Edge	Connection	Duration	IP Address	Mapped LUNs	LUN Capacity	Remove
win-edge	Connected	53m 55s	10.32.98.30	1 LUN	60.00 GB	

Status Target Settings **Initiators** Initiator Groups LUNs Prepopulation

Add an Initiator

Initiator Name:
 Add to Initiator Group: New Group
 Authentication:
Add Initiator

Initiator	Authentication	CHAP User	Mutual CHAP User	Delete
No initiators added.				

Figure 23 Add Initiator Page

4. Select **LUNs** and select the **Amazon Web Services Storage Gateway LUN** that you would like to configure with the initiator group created above. By default none of the groups and none of the initiators are allowed to access this LUN.
5. Select **Edit** to remove the **None** initiator group from the Groups Granted Access section and add the newly created initiator group from above as shown in Figure 24.

Granite Edges

Add a Granite Edge

Granite Edge	Connection	Duration	IP Address	Mapped LUNs	LUN Capacity	Remove
win-edge	Connected	55m 31s	10.32.98.30	1 LUN	60.00 GB	

Status Target Settings Initiators Initiator Groups **LUNs** Prepopulation

Map LUNs to this Granite Edge

LUN	Size	Online/Offline	Accessible	Pinned	Unmap
alias-P3Pd8Zgky0ue (P3Pd8Zgky0ue)	60.0038 GB	Online	No	No	

Manage Access Lists (To perform other operations on this LUN, click here.)

Groups Granted Access Edit
 None

Initiators Granted Access Edit
 None

Figure 24 SteelFusion LUN Masking Page

6. Select the **initiator group** from the Not Granted box and select **Add** to add it to the Groups Granted Access box as shown in Figure 25.

Granite Edges

+ Add a Granite Edge

Granite Edge	Connection	Duration	IP Address	Mapped LUNs	LUN Capacity	Remove
win-edge	Connected	57m 31s	10.32.98.30	1 LUN	60.00 GB	

Status Target Settings Initiators Initiator Groups **LUNs** Prepopulation

+ Map LUNs to this Granite Edge

LUN	Size	Online/Offline	Accessible	Pinned	Unmap
alias-P3Pd8Zgky0ue (P3Pd8Zgky0ue)	60.0038 GB	Online	No	No	

Manage Access Lists (To perform other operations on this LUN, click here.)

Groups Granted Access ◀ Hide

None

◀ Add

Remove ▶

Not Granted

SanDiegoBranch

all

Initiators Granted Access Edit ▶

None

Figure 25 Add Initiator Group

7. Verify that the new initiator group is now under the Group Granted Access box and the default all initiator group is still under the Not Granted box as shown in Figure 26.

LUN	Size	Online/Offline	Accessible	Pinned	Unmap
alias-P3Pd8Zgky0ue (P3Pd8Zgky0ue)	60.0038 GB	Online	Yes	No	

Manage Access Lists (To perform other operations on this LUN, click here.)

Groups Granted Access ◀ Hide

SanDiegoBranch

◀ Add

Remove ▶

Not Granted

all

Initiators Granted Access Edit ▶

None

Figure 26 Verify Initiator Groups

8. To instead allow all initiators at the branch office to access the LUN, add the default **all** initiator group to the Group Granted Access box, as shown in Figure 27.

+ Map LUNs to this Granite Edge

LUN	Size	Online/Offline	Accessible	Pinned	Unmap
alias-P3Pd8Zgky0ue (P3Pd8Zgky0ue)	60.0038 GB	Online	Yes	No	

Manage Access Lists (To perform other operations on this LUN, click here.)

Groups Granted Access ◀ Hide

all

◀ Add

Remove ▶

Not Granted

SanDiegoBranch

Initiators Granted Access Edit ▶

None

Figure 27 Access to All Initiators

Chapter 3 Performing Branch Disaster Recovery

In the unlikely event there is a significant disruption at a branch (such as a natural disaster), SteelFusion can be used to quickly recover branch data and services, either to another branch location, or within the data center itself. Since the data is stored within a LUN provided by the AWS Storage Gateway, SteelFusion core can redirect the LUN from the original branch to another branch with SteelFusion. Alternatively, you can directly mount the LUN to a Windows server or VMware ESXi host in the data center.

Note that a branch outage will result in a crash consistent LUN state to exist for the LUN delivered by the AWS Storage Gateway to SteelFusion, so the amount of data loss will depend on how much pending data SteelFusion was in the process of synchronizing to the AWS Storage Gateway LUN at the time the branch outage occurred.

Configure the LUN to a New SteelFusion Edge at a Different Branch

Reconfiguring a LUN for access by a new or different SteelFusion Edge is straight forward. Because a branch outage disconnects the AWS Storage Gateway LUN from the original SteelFusion Edge, SteelFusion Core will need to perform the following steps in order to associate the LUN for use by a new or different SteelFusion Edge:

1. Login to the SteelFusion Core GUI, and select **Configure > Storage > LUNs** and identify the LUNs that are associated with the original SteelFusion Edge that is experiencing the outage, as shown in Figure 28. Note the LUN name that it has been given (also known as the LUN alias name).

Configure > Storage > LUNs ?

Status of all configured luns.



+ Add a LUN				
LUN ↑↓	Type ↑↓	Status ↑↓	Size ↑↓	Granite Edge ↑↓
 > Cdrive (P3PdBZqTVC4y)	iSCSI	Degraded	43.0049 GB	edgeA
 > Ddrive (P3PdBZgypncg)	iSCSI	Degraded	20.0013 GB	edgeA

Figure 28 LUN and Edge Identification

2. SSH to the SteelFusion Core management interface, and login. From the command prompt, issue the following commands to disassociate the LUN from the original SteelFusion Edge, using the LUN alias name and the SteelFusion Edge name identified in the previous step:

```
en
conf t
edge modify id <Original_SteelFusion_Edge_Name> clear-serial
storage iscsi lun modify lun-alias <LUN_Alias_Name> unmap force
```

For example:

```
en
conf t
edge modify id edgeA clear-serial
storage iscsi lun modify lun-alias Ddrive unmap force
```

3. Go to **Configure > Storage > Granite Edges**, and select the **LUN** tab of the new or replacement SteelFusion Edge. You will need to map the LUN to this new Edge, as shown in Figure 29.

Configure > Storage > Granite Edges ?

Granite Edges

+ Add a Granite Edge

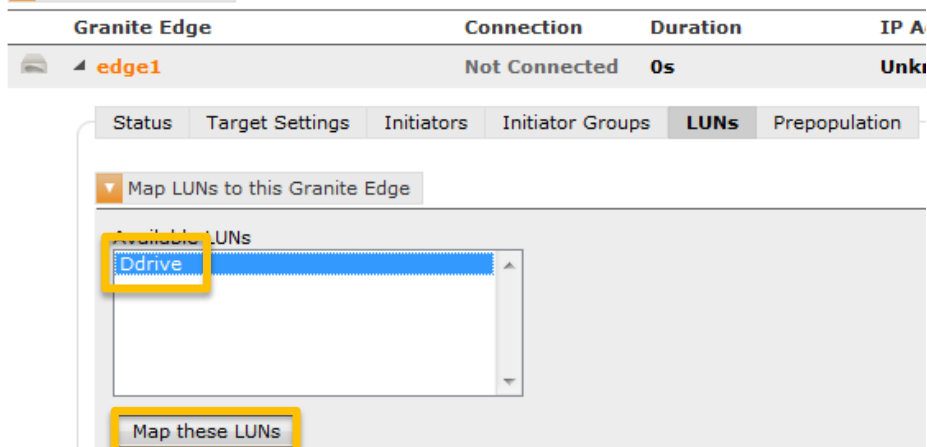


Figure 29 Map LUN to a New or Replacement Edge

4. Configure initiator access for the LUN at the new branch, as described in the section **Configure Initiator Access for Branch Servers on the SteelFusion Core**. The new or replacement SteelFusion Edge will now have access to the LUN and can deliver the LUN to the end server or ESXi host for use.

Configure the LUN Directly to a Windows Server in the Data Center

If the AWS Storage Gateway LUN is a NTFS volume, you may directly mount the LUN to a corresponding Windows server in the data center, without the use of SteelFusion. To accomplish this, perform the following steps:

1. Login to the SteelFusion Core GUI, and select **Configure > Storage > LUNs** and identify the LUNs that are associated with the original SteelFusion Edge that is experiencing the outage, as shown in Figure 30. Note the LUN name that it has been given (also known as the LUN alias name).

Configure > Storage > LUNs ?

Status of all configured luns.

+ Add a LUN

LUN ↑↓	Type ↑↓	Status ↑↓	Size ↑↓	Granite Edge ↑↓
<div> <div></div> <div>Cdrive (P3PdBZqTVC4y)</div> </div>	iSCSI	Degraded	43.0049 GB	edgeA
<div> <div></div> <div>Ddrive (P3PdBZgypncg)</div> </div>	iSCSI	Degraded	20.0013 GB	edgeA

Figure 30 LUN and Edge Identification

2. SSH to the SteelFusion Core management interface, and login. From the command prompt, issue the following commands to disassociate the LUN from the original SteelFusion Edge and remove it from SteelFusion core, using the LUN alias name and the SteelFusion Edge name identified in the previous step:


```

en
conf t
edge modify id <Original_SteelFusion_Edge_Name> clear-serial
storage iscsi lun modify lun-alias <LUN_Alias_Name> unmap force
storage iscsi lun remove lun-alias <LUN_Alias_Name> force
      
```

For example:

```
en
conf t
edge modify id edgeA clear-serial
storage iscsi lun modify lun-alias Ddrive unmap force
storage iscsi lun remove lun-alias Ddrive force
```

- On the Windows server which will mount the LUN, start the iSCSI Initiator program to mount the LUN, as shown in Figure 31. Use the AWS Storage Gateway Portal IP address that was configured when setting up the AWS Storage Gateway, and not the SteelFusion Core IP address, when adding the LUN.

Programs (1)

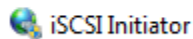


Figure 31 Windows iSCSI Initiator

Configure the LUN to Directly to a VMware ESXi Server in the Data Center

If the AWS Storage Gateway LUN is a VMFS configured volume, you may directly mount the LUN to a corresponding ESXi server in the data center, without the use of SteelFusion. To accomplish this, perform the following steps:

- Login to the SteelFusion Core GUI, and select **Configure > Storage > LUNs** and identify the LUNs that are associated with the original SteelFusion Edge that is experiencing the outage, as shown in Figure 32. Note the LUN name that it has been given (also known as the LUN alias name).

Configure > Storage > LUNs ?

Status of all configured luns.

+ Add a LUN				
LUN ↑↓	Type ↑↓	Status ↑↓	Size ↑↓	Granite Edge ↑↓
▷ Cdrive (P3PdBZqTVC4y)	iSCSI	Degraded	43.0049 GB	edgeA
▷ Ddrive (P3PdBZgypncg)	iSCSI	Degraded	20.0013 GB	edgeA

Figure 32 LUN and Edge Identification

- SSH to the SteelFusion Core management interface, and login. From the command prompt, issue the following commands to disassociate the LUN from the original SteelFusion Edge and remove it from SteelFusion core, using the LUN alias name and the SteelFusion Edge name identified in the previous step:

```
en
conf t
edge modify id <Original_SteelFusion_Edge_Name> clear-serial
storage iscsi lun modify lun-alias <LUN_Alias_Name> unmap force
storage iscsi lun remove lun-alias <LUN_Alias_Name> force
```

For example:

```
en
conf t
edge modify id edgeA clear-serial
storage iscsi lun modify lun-alias Ddrive unmap force
storage iscsi lun remove lun-alias Ddrive force
```

- On the ESXi server which will mount the LUN, go to the **Configuration** Tab, select **Storage Adapters** from the left menu, right click the iSCSI Storage Adapter and select Properties, as shown in Figure 33 ESXi iSCSI Software Adapter Properties. Use the AWS Storage Gateway Portal IP address that was configured when setting up the AWS Storage Gateway, and not the SteelFusion Core IP address, when adding the LUN.

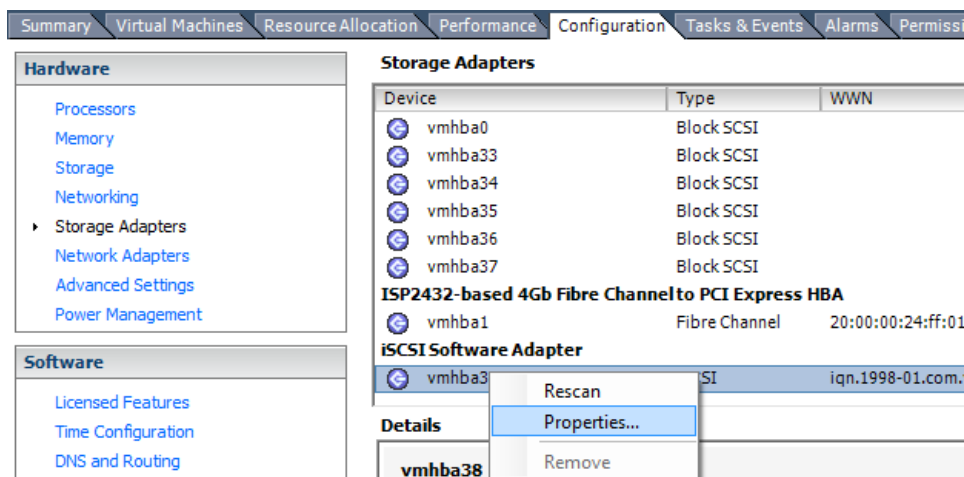


Figure 33 ESXi iSCSI Software Adapter Properties

- Perform a **Rescan** to add the LUN, and then add the volume using the **Storage** menu item, and the **Add Storage** wizard.

Chapter 4 Performing Data Center Disaster Recovery

Performing disaster recovery (DR) with an AWS Storage Gateway differs slightly from traditional storage disaster recovery since the data or data snapshots are stored in Amazon cloud storage, rather than on another SAN storage device at a DR site. The benefits of having cloud based snapshots available for recovery is that you do not have to maintain power, networking, and other infrastructure until such time that a DR recovery is needed. When a DR event occurs, you can deploy a new virtual instance of an AWS Storage Gateway and SteelFusion to perform recovery of required services for branch offices, as shown in Figure 34. This deployment can be done either within a new data center, or within a specialized facility that can use the [Amazon Direct Connect](#) features to connect to Amazon cloud storage services directly over high bandwidth networks.

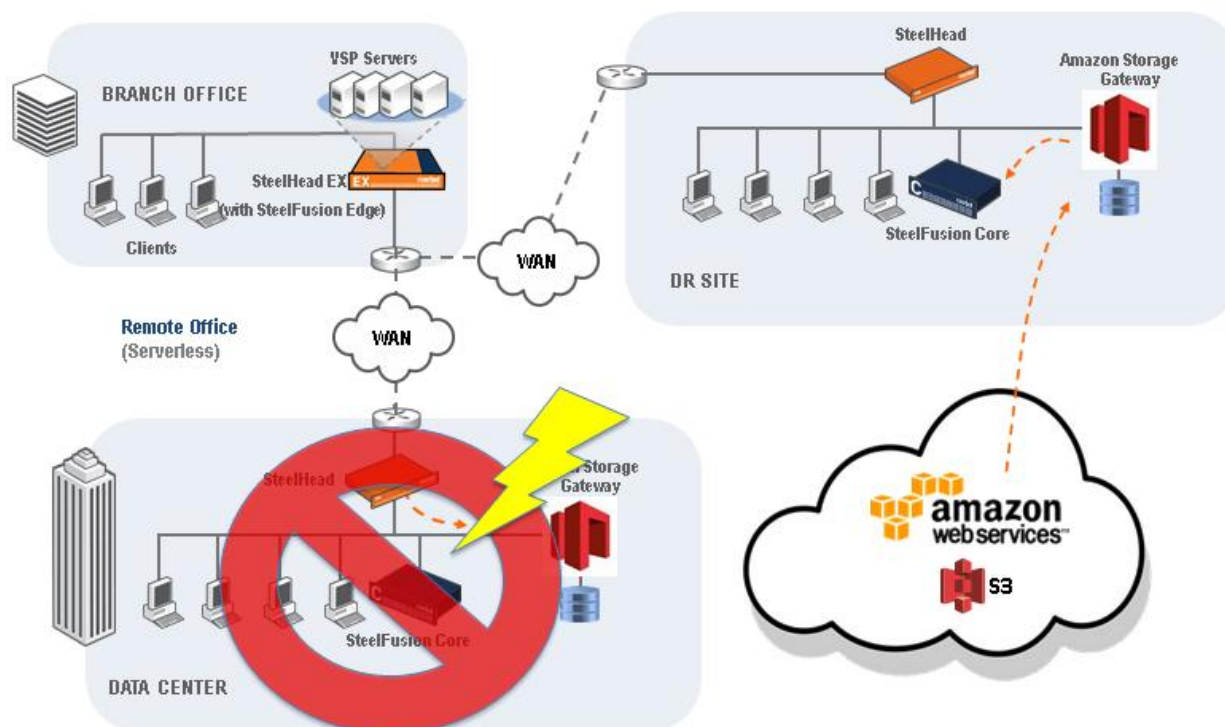


Figure 34 DR Recovery Overview

DR Recovery with the AWS Storage Gateway and SteelFusion

1. Deploy a new AWS Storage Gateway at the DR site, similar to the steps outlined in Chapter 2 above. During step 4, in which you deploy a new volume for the AWS Storage Gateway, you will instead configure the new volume as a recovered volume from a previous snapshot (Figure 35 and Figure 36). Refer to the directions on the following page for details: <http://docs.aws.amazon.com/storagegateway/latest/userguide/RestoringSnapshotVolume.html>

Create Storage Volume close

Disk: SCSI (0:2) ☐ Preserve existing data

iSCSI Target Name: iqn.1997-05.com.amazon:myvolumerestored

Based on Snapshot ID: snap-5d6b8e3e

Size: 1 GiB

Host IP: 10.56.250.1

Port: 3260

Cancel Create Volume

Figure 35 Volume Recovery from Snapshot (Gateway-Stored Configuration)

Configure Your Activated Gateway
close

Create an iSCSI storage volume up to 32 TBs in size. This volume will be stored in Amazon S3, with only a cache of recently accessed data kept locally. Your client applications will connect to this volume over an iSCSI interface. [Learn More.](#)

Capacity: TBs (Max: 32 TBs)

iSCSI Target Name:

Based on Snapshot ID:

Host IP:

Port:

Figure 36 Volume Recovery from Snapshot (Gateway-Cached Configuration)

2. After recovering the AWS Storage Gateway, you will need to deploy a new SteelFusion Core, as outlined in the previous chapter above. When adding the iSCSI target and LUN, you will point to the new iSCSI target and attach to the new LUN delivered by the DR AWS Storage Gateway, and provide initiator access to the correct host(s) at the branch which will need access (for example, SteelFusion Edge).

Note: If you want to recover data from the LUN directly in the data center, you may mount the LUN directly to a Windows or ESXi host as described in the sections **Configure the LUN Directly to a Windows Server in the Data Center** and **Configure the LUN to Directly to a VMware ESXi Server in the Data Center**. SteelFusion is not required in this case and data can be directly recovered via Windows or VMware iSCSI connections to the LUN.

3. When data access occurs (such as from an ESXi server at the branch launching a VM delivered via SteelFusion), SteelFusion will make requests for the data from the AWS Storage Gateway, and deliver that received data from the recovered snapshot to SteelFusion across the WAN to the branch SteelFusion Edge.
4. The data recovery time will depend on your WAN speed between Amazon S3 and your SteelFusion Core, and the WAN speed between your SteelFusion Core and your SteelFusion edge. For example, if your SteelFusion Core is on a 1 gb/s Direct Connect link to Amazon S3, your recovery time will most likely depend on the WAN speed at which SteelFusion traffic can pass from the DR site to the branch. In the below example, a 100mb/s WAN to the branch could yield a Windows VM boot time of roughly 20-30 minutes. Alternatively, your DR procedures may dictate to recover the branch environment at the DR site, rather than at the branch, which could reduce the amount of time needed to initially recover services and bring them online for users.

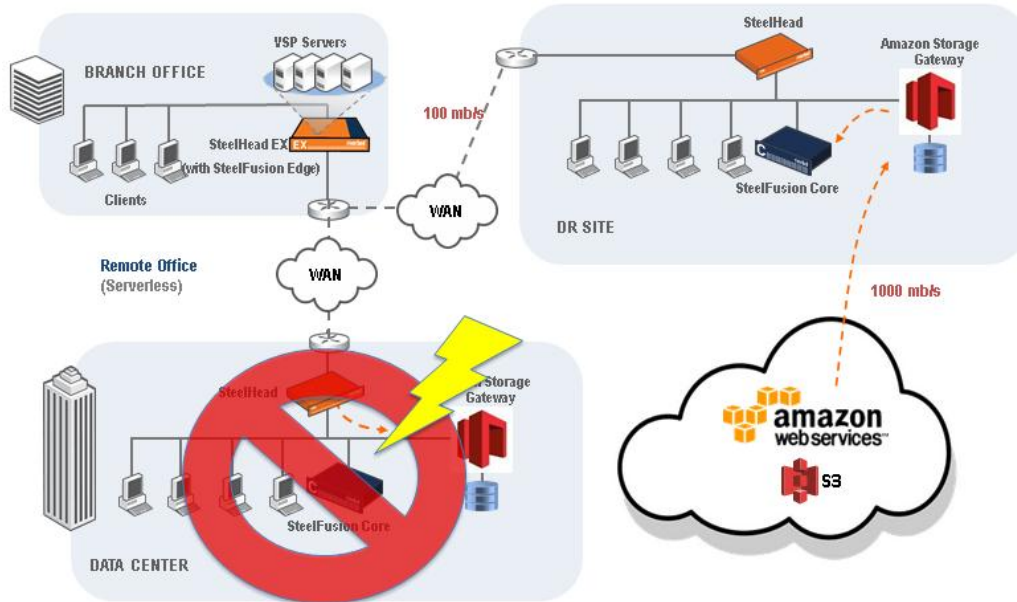


Figure 37 DR Recovery Speed Example

Chapter 5 Solution Recommendations and Best Practices

The following recommendations are best practices are intended to guide you to achieving optimal performance while reducing configuration and maintenance requirements.

AWS Storage Gateway Best Practices

Best Practice	Description
Mutual CHAP	If the intranet network is trusted, mutual CHAP is not required and does not need to be configured on the AWS Storage Gateway and SteelFusion core.
Gateway Volume Storage Size	It is recommended to configure storage for the AWS Storage Gateway according to the best practices laid out by the AWS Storage Gateway calculator online. If using a Gateway Cached Volume configuration, make sure the cache and buffer volumes are sized appropriately. If using a Gateway Stored Volume configuration, make sure the storage volume is sized appropriately as you would with a normal SAN volume.

SteelFusion Best Practices

Best Practice	Description
Mutual CHAP	If the intranet network is trusted, mutual CHAP is not required and does not need to be configured on the AWS Storage Gateway and SteelFusion core.
SCSI Reservations	AWS Storage Gateway does not currently support SCSI-3 reservations, so disable SCSI reservations on SteelFusion core prior to adding the volume to a SteelFusion core. Use the command: <code>storage iscsi lun modify-all scsi-res disable</code>
Volume Crash Consistency	SteelFusion relies on the AWS Storage Gateway to provide crash consistent snapshots of the storage LUNs. Amazon EBS snapshots can be taken of LUNs and managed through the Amazon Web Services Management Console.



Riverbed Technology, Inc.
680 Folsom Street
San Francisco, CA 94107
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