Optimizing Azure Site Recovery (ASR) with Riverbed® SteelHead™ WAN Optimizers

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Copyright**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2014 Microsoft. All rights reserved. © 2014 Riverbed. All rights reserved.

Microsoft, Hyper-V, SharePoint, SQL Server, Windows, and Windows Server are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Scope 4](#_Toc401777280)

[Introduction 4](#_Toc401777281)

[Solution Overview 5](#_Toc401777282)

[Encryption 6](#_Toc401777283)

[Setup Details 7](#_Toc401777284)

[Setting up ASR - On Azure 7](#_Toc401777285)

[Setting Up ASR – On Premises 7](#_Toc401777286)

[Configuring the Azure Hosted Riverbed SteelHead CX 10](#_Toc401777287)

[General Configuration 10](#_Toc401777288)

[Enabling SSL for Optimization of Encrypted Azure Site Recovery Traffic 10](#_Toc401777289)

[Riverbed SteelHead – Configuring on-premises device 12](#_Toc401777290)

[Scenario #1: Replicating Sparse Disks 13](#_Toc401777291)

[Scenario #2: Dense Disk 14](#_Toc401777292)

[Scenario #3: Multi-VM Scenario 17](#_Toc401777293)

[Summary 19](#_Toc401777294)

# **Scope**

[**Azure Site Recovery**](http://azure.microsoft.com/en-us/services/site-recovery/) (or ASR) is a Microsoft Azure service that orchestrates the protection and recovery of your virtualized applications for business continuity disaster recovery (BCDR) purposes. This document details network optimization delivered by Riverbed**®** SteelHead™ devices when “replicating” virtual machines (VMs) to Microsoft Azure using ASR. This document is intended for IT administrators, network administrators, ASR users, ASR evaluators and IT decision makers.

*…the SteelHead solution exceeded expectations in reducing   
network traffic.”*

# **Introduction**

The two broad types of ASR are defined by the target endpoint:

* **Protection between two System Center clouds:** In this deployment, the customer owns both the primary and secondary data centers. ASR is used to protect and orchestrate workloads running in the primary data center.
* **Protection from a System Center cloud to Microsoft Azure:** In this deployment, the customer owns the primary data center and relies on Microsoft Azure for BCDR needs. Customers can save on the CAPEX and OPEX costs involved in setting up secondary data center and rely on the ASR to address their BCDR needs.

The two key metrics when recovering from a disaster are Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO refers to the data loss (measured in seconds or minutes) when recovering from a disaster and RTO refers to the time taken to recover from a disaster (measured in minutes or hours). When a disaster strikes the customer’s data center, using ASR, customers can quickly (low RTO) bring online their replicated virtual machines located in either the secondary data center or Microsoft Azure with minimum data loss (low RPO).

Failover is made possible by the Azure Site Recovery Service which initially copies designated virtual machines from the primary data center to the secondary data center or Azure (depending on the scenario) and then periodically refreshes the replicas. Replication is a network intensive operation (based on workload patterns) and WAN (or internet) bandwidth is precious. During infrastructure planning, network saturation should be considered as potential bottleneck that can prevent you from meeting company RPO objectives. SteelHeads are designed to optimize network traffic of this kind. Passing the ASR traffic through an on-premise SteelHead paired with a SteelHead CX virtual machine hosted in Azure can help you meet these RPO objectives by optimizing the network.

To test this scenario, a series of experiments were conducted in Microsoft’s Excellence Center (EEC) lab in Redmond, WA. Depending on the workload pattern in the VM, the SteelHeads eliminated more than 90% of the WAN bandwidth for initial replication and up to 80% for subsequent delta. In a bandwidth-restrictive environment, these benefits translate into major savings and allow customers to meet their RPO objectives and also replicate a larger number of VMs without clogging the organization’s internet traffic.

Microsoft and Riverbed have collaborated previously to publish two whitepapers (which can be found [here](http://www.microsoft.com/en-us/download/details.aspx?id=36786) and [here](http://www.microsoft.com/en-us/download/details.aspx?id=42627)) that studied the network optimization delivered by Riverbed’s SteelHead on Hyper-V replication traffic sent between the primary and secondary data centers.

# **Solution Overview**

When protecting applications with a System Center managed private cloud to Microsoft Azure, ASR tracks the changes to the on-premises virtual machine and writes them directly to customer’s storage account. Customers can choose to replicate their VMs every 30 seconds, 5 minutes or 15minutes. There are two major phases to replication: Initial Replication (IR) and delta replication (or DR).

Initial replication (IR) happens when a replication relationship is created for a VM. The entire VM (which can vary in size from a few gigabytes to a few terabytes) is transferred over the network from the primary site to the secondary site. The replication traffic goes over HTTPS.

After IR starts, any changes (specifically the writes) to the virtual machine are tracked in log files that are transferred periodically (as set when configuring a virtual machine for replication). Based on workload characteristics, and read/write pattern, the size of the log file in each replication interval can range from a few megabytes to a few 100 megabytes.

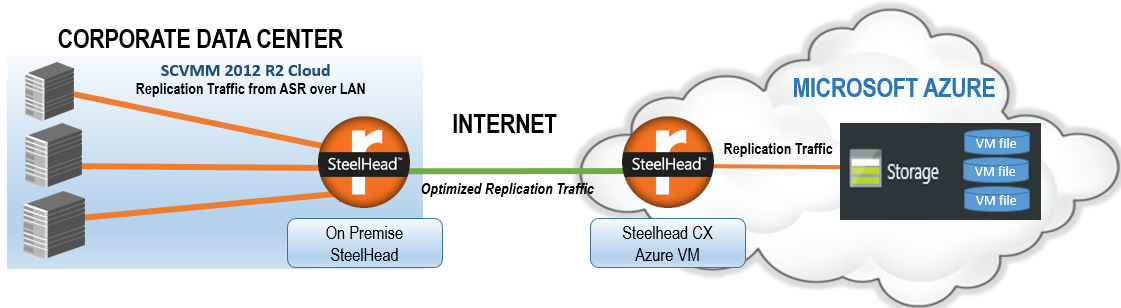
Network congestion has typically proven to be a bottleneck which prevents the customer from meeting RPO objectives. If the network is not provisioned to handle the load, time taken to transmit the log file to the storage account increases.

In this scenario, Riverbed SteelHead devices can play a critical role in ensuring that the RPO objectives are met.

WAN optimization requires two devices. When a SteelHead in the company data center is paired with an Azure hosted SteelHead CX virtual machine, traffic between the devices is highly optimized resulting in dramatically reduced bandwidth and faster replication. To achieve this, SteelHeads provide three levels of optimization.

* **TCP optimization:** Protocol optimization reduces round trips and improve throughput.
* **Deduplication:** Files that travel between SteelHeads are recorded as bit patterns on both SteelHead devices. When a SteelHead detects a pattern it has seen before, the paired SteelHead is instructed to deliver the matched content directly to the requester. In this way, the identified data does not need to traverse the network between the SteelHeads. This results in significant bandwidth reduction when replicated disks have duplicate content such as the same installation of an operating system or fixed sized virtual disks have empty space.
* **Compression:** Many virtual disks benefit significantly from compression. The SteelHead pair compresses the bit stream on one end and decompresses on the other resulting in reduced traffic over the internet. In particular, fixed sized VHDx files with empty space benefit from this optimization.

The solution is illustrated in Figure 1:



**Figure 1: Solution Architecture**

## Encryption

Encryption is available at the network layer and at rest.

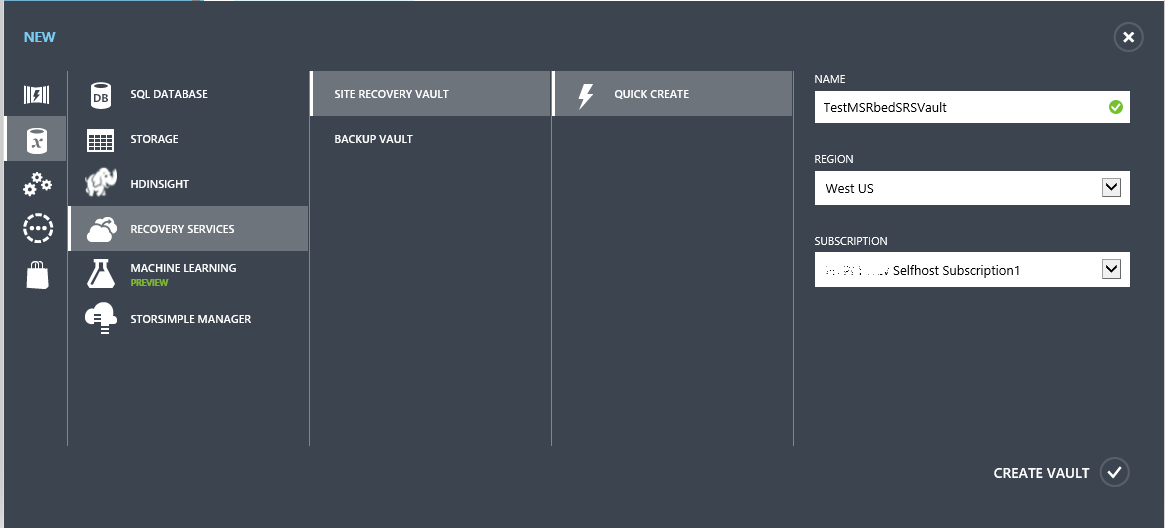
Encryption on the network layer is achieved by sending the replica traffic over HTTPS. By adding the proper certificates to the SteelHead, SSL traffic is decoded, optimized, and reencrypted such that SSL is maintained end-to-end and highly optimized.

Encryption at rest is achieved by encrypting the data on-premises using certificate keys provided by the customer. Even before the replica copy (initial or delta replication) hits the network, the ASR agent running in the Hyper-V server encrypts the payload. The encrypted data remains encrypted-at-rest on Azure and can be decrypted only by the customer when bringing up the VM in Azure (or “failover”). The encryption key is owned by the customer and never leaves the premises.

**Note that when the encrypted contents are transmitted through the SteelHeads, network optimization is rendered impractical. Consequently, you should not encrypt the contents at rest, if you intend to optimize the network traffic.**

# **Setup Details**

## Setting up ASR - On Azure

A *Site Recovery Vault* is created under the Recovery Services option in the Azure management portal as shown in Figure 2.

**Figure 2: Azure Site Recovery Vault Creation**

Once the vault is created, it is configured as detailed in the following guide - <http://azure.microsoft.com/en-us/documentation/articles/hyper-v-recovery-manager-azure/>

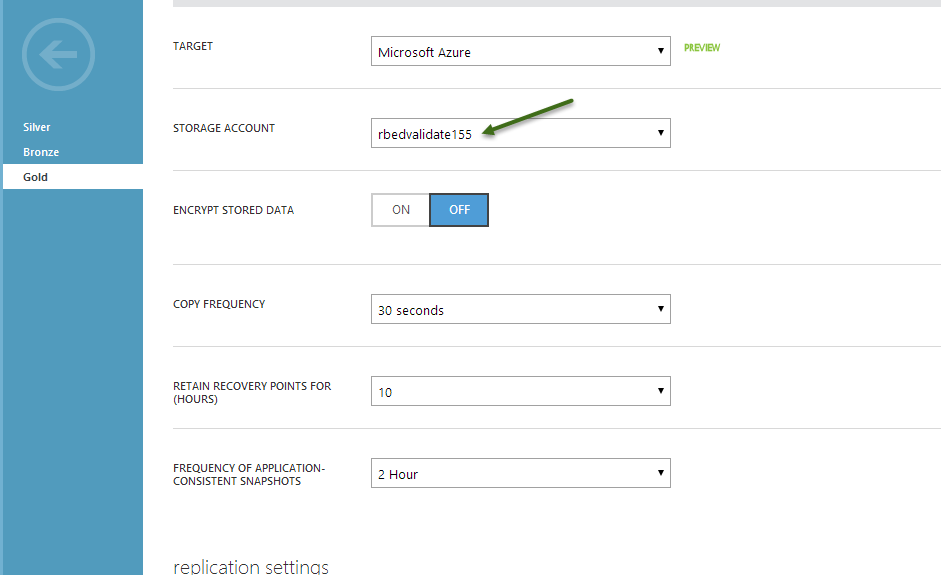
After configuring the vault, the following two agents are downloaded from the portal:

* Azure Site Recovery Provider –Install on the on-premise System Center Virtual Machine Manager
* Azure Recovery Service –Install on each Hyper-V server on-premises which acts as the “data mover to Azure” (from the on-premise Hyper-V server)

## Setting Up ASR – On Premises

The setup used for this validation effort involved a 3-node Windows Server 2012 R2 Hyper-V cluster that is managed by System Center 2012 R2 Virtual Machine Manager (VMM) and represents the customer’s primary site. Three VMM clouds (Gold, Silver, Bronze) were created for the purpose of this effort. The *Azure Recovery Services* agent is installed on each of the Hyper-V servers while the *Azure Site Recovery Provider* is installed on the VMM server. An end to end getting started guide is available at <http://msdn.microsoft.com/en-us/library/dn788903.aspx>.

After the agents are installed, the clouds (Gold, Silver, Bronze as seen in the left pane of Figure 3) show up on the portal under the configured vault. The cloud’s protection policy is configured and any VM that is part of this cloud can then be enabled for replication. The cloud is configured to receive the replication traffic to a storage account (blob store) in your subscription. Make a note of the storage account name because it will be required when configuring the on-premises SteelHead.

In the above example, the storage account which receives the replication traffic is *rbedvalidate155*, the blob store URL is *rbedvalidate155.blob.core.windows.net* as shown in Figure 4.

**Figure 3: Cloud Configuration**



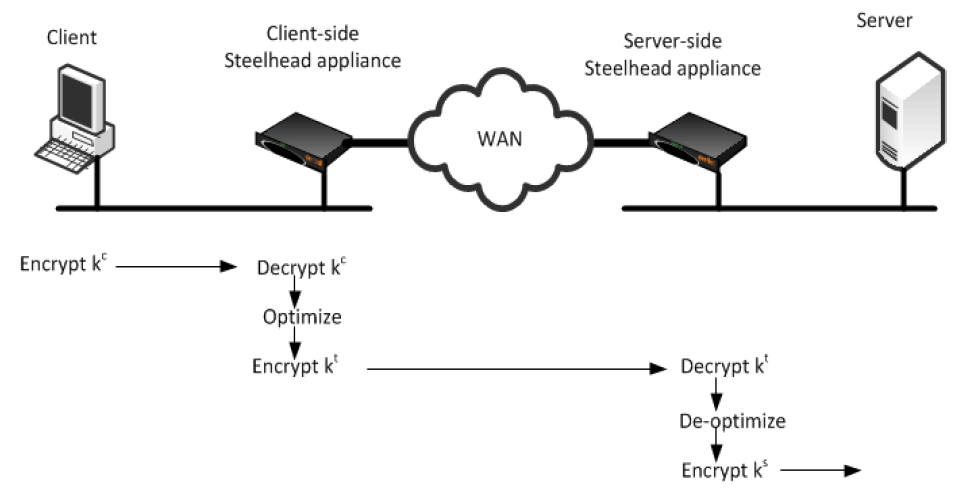
**Figure 4: Storage Account Blob URI**

As with on-premises solutions, optimization occurs between two Riverbed SteelHead devices. A physical SteelHead is required on the on-premises side and is paired with a Riverbed SteelHead CX which runs as an Azure Infrastructure as a Service VM. Traffic between these devices from the data center into Azure is optimized.

The SteelHead in Azure is referred to as the *Server-side SteelHead*while the SteelHead on the primary site is referred to as the *Client-side SteelHead*. Note that the SteelHead CX in Azure can be deployed from the Azure Virtual Machine Gallery. Refer to the document [Optimizing Azure Workloads with the SteelHead CX - Solution Guide.pdf](https://splash.riverbed.com/docs/DOC-4627) for step-by-step details.

The studies in this paper were conducted by Microsoft using the SteelHead 6050-L on the client side and ta SteelHead CX running in Azure on the server side. Both appliances were running RiOS 8.6. (RiOS is the Riverbed Operating System provided with SteelHead appliances). General configuration of the appliances is covered in detail in the following deployment document: <https://support.riverbed.com/download.htm?did=uffde61aideokpffksfk6g9vcs>. The network was throttled to 50Mbps to simulate a common bandwidth connection to Azure. Endpoints for Azure were selected for the West Coast to be closest to the Microsoft lab in Redmond.

At a high level, in order to optimize HTTPS traffic, the SteelHead decrypts the packet from the client (in this case, System Center VMM), optimizes the content and then re-encrypts the content so the traffic between the SteelHeads over the internet/WAN is secured. The server-side SteelHead (in Azure) decrypts the incoming traffic, applies optimization and then re-encrypts the traffic using the appropriate certificates for the server side (the public Microsoft certificates). The network flow is captured in the diagram taken from the deployment guide mentioned above.

***Figure 5: Data Transfer on SSL***

The keys used in Figure 6 are:

* **kc** is the session key between the client initiating the transmission and the server-side SteelHead.
* **ks** is the session key between the server-side SteelHead and the server.
* **kt** is the session key between the client-side SteelHead and the server-side SteelHead appliance for the inner secure SSL channel.

## Configuring the Azure Hosted Riverbed SteelHead CX

The SteelHead CX hosted in Azure can easily be deployed from the Azure virtual machine gallery. Complete instructions are contained in the document [Optimizing Azure Workloads with the SteelHead CX - Solution Guide.pdf](https://splash.riverbed.com/docs/DOC-4627)

### General Configuration

The following steps detail the general configuration of the SteelHead CX for Azure Site Recovery.

1. Obtain a SteelHead CX trial license from Riverbed. [Contact Riverbed](http://www.riverbed.com/contact/#overview) for details. Riverbed has offices worldwide.

Note: The SteelHead CX optimization service cannot be started until a license has been installed.

2. Deploy the SteelHead CX as described in [Optimizing Azure Workloads with the SteelHead CX - Solution Guide.pdf](https://splash.riverbed.com/docs/DOC-4627).

### Enabling SSL for Optimization of Encrypted Azure Site Recovery Traffic

In effect, you are adding a certificate to the Azure SteelHead CX that will be presented to the client when connecting to the replication service in Azure. As long as the certificate is issued by a trusted CA (usually the Enterprise CA), and has the correct common names, the certificate will be suitable for use.

1. Obtain and install an SSL license from <https://support.riverbed.com/content/support/my_riverbed/ssl.html>.

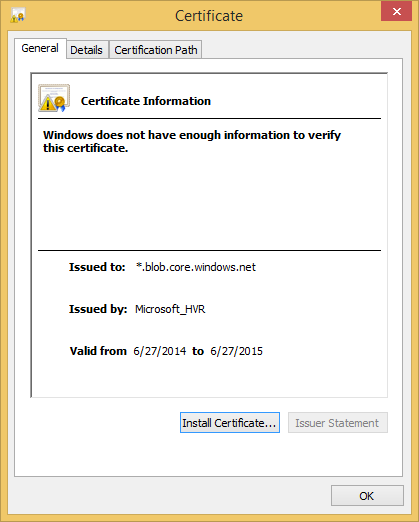
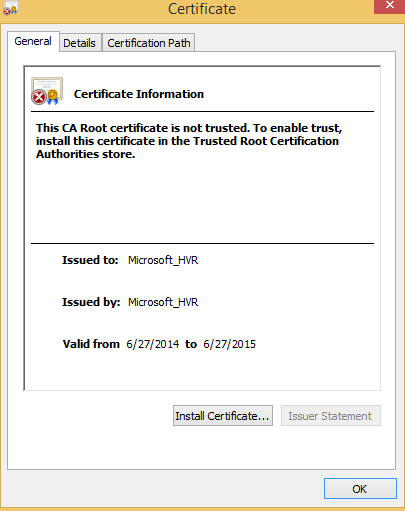
2. Remove port 443 from the secure ports list. In the SteelHead web administration portal, browse to Networking->Port Labels->Secure. If port 443 is listed in the Ports, remove the entry and click Apply, then Save.

3. Create and install the appropriate certificate.

To accomplish this task, you may need to capture the network traffic in order to properly identify the certificate in use by Azure Site Recovery.

1. Install Wireshark (<http://wireshark.org>) on the server hosting System Center Virtual Machine Manager configured to work with Azure Site Recovery.
2. Start a network capture.
3. Start the initial replication of a virtual machine.
4. Stop the network capture.
5. Using Wireshark, open the capture file.
6. Filter the capture for ssl.handshake.type==11.
7. Examine the packet information under the Secure Socket Layer section. You will see:
   1. Certificate-ID: contains the Common Name, organization, and other certificate details. In the samples taken for this and other studies, a common name of \*.blob.core.windows.net was identified.
   2. Extensions: expand to show the DNS name list, which corresponds to Subject Alternative Names used in the certificate.
   3. Also note the IP addresses used by Azure Site Recovery in the capture as this will assist with identifying optimized traffic and setting up in-path rules.

With this information in hand, create a server certificate that contains the private key and matches the Common Name and Subject Alternative Names carefully. Ensure the certificate is created using a Certificate Authority (CA) trusted by the servers that connect to the Azure Site Recovery service. In addition, the SteelHead CX hosted in Azure must also trust the CA.



**Figure 6 - CA Root Certificate to Install on Server and Proxy Certificate to Install on Azure SteelHead CX**

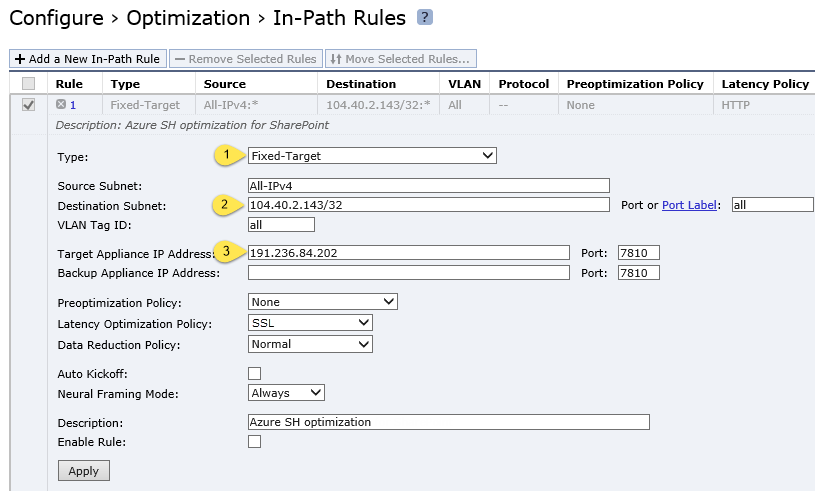
If you use a stand-alone CA to create the proxy certificate (such as those illustrated in Figure 6), insure you install the CA Root Certificate (as shown on the left) in the Trusted Root Certificate Authorities store of the local machine rather than the user certificate store. To do this, use the Microsoft Management Console and select Local Machine. [See the document *Creating Proxy Certificates for a Riverbed Steelhead Appliance with a Microsoft Certificate Authority* for step-by-step details.](https://splash.riverbed.com/docs/DOC-3473)

Deploying certificates for the SteelHead CX is the same as for physical appliances. Refer to Chapter 10, “SSL Deployments,” in the [*Steelhead Appliance Deployment Guide*](https://support.riverbed.com/bin/support/download?did=agrtjjih4pipacd6gu02b3c5uf) available on Riverbed.com/support. Additional details can be found at <https://splash.riverbed.com/docs/DOC-4068>.

## Riverbed SteelHead – Configuring on-premises device

After deploying the Azure SteelHead CX, you must pair the on-premise SteelHead with the Azure SteelHead CX. Step-by-step instructions for this simple operation are included in Chapter 4 of the referenced solution guide. Pairing the devices allows them to securely exchange traffic.

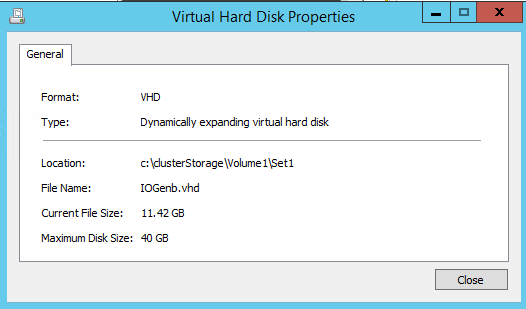
Finally, you must add a fixed-target in-path rule that will intercept Azure bound traffic and direct the traffic to the SteelHead CX in Azure.



**Figure 7: In Path Rules**

Once the setup was configured, the following tests were performed and the optimization results are captured in each section.

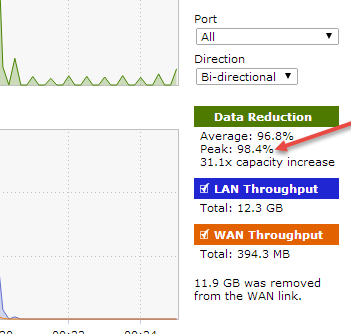
# Scenario #1: Replicating Sparse Disks

The first experiment involved studying the optimization delivered by the SteelHead when replicating a sparsely populated Windows Server 2012 R2 VM.

**Figure 8: Sparse Disk Explorer view from Guest VM**

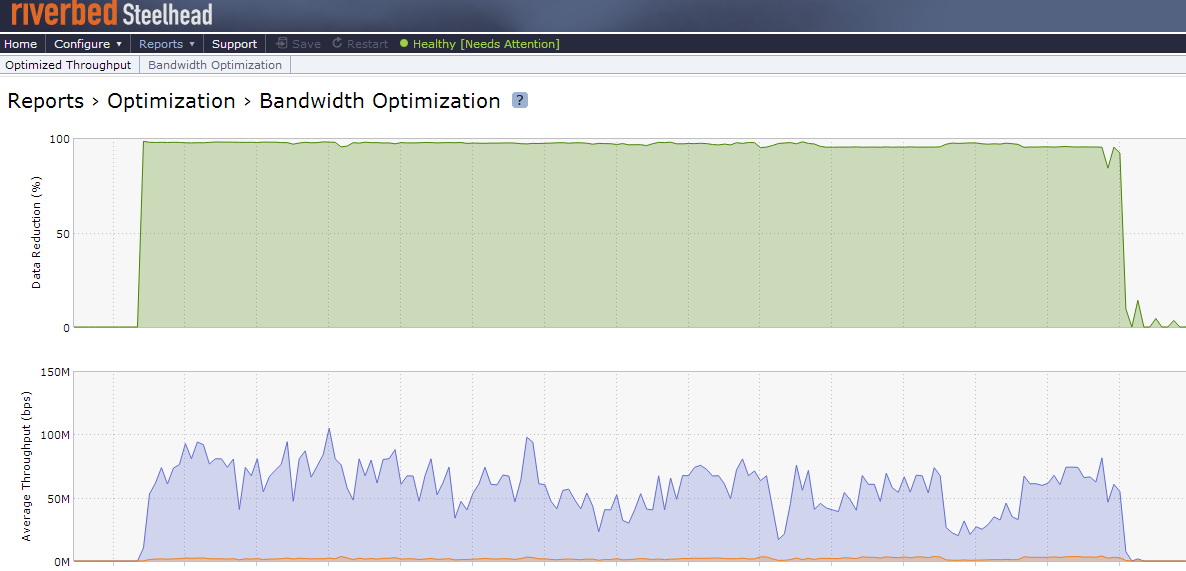
The VM was attached to a VHD that was created using the default configuration of a 127GB dynamic VHDx. Once the OS is installed, the explorer view of the VM was 11.42 GB in size as shown in Figure 8 above.

After replication starts, optimization takes a few minutes begin. In this test, due to the sparseness of the data in the disk, bandwidth reduction is very high as shown in Figure 9 below.



**Figure 9: Sparse Disk Optimization**

Given the data distribution, both the data reduction and the average throughput is consistently high as shown in Figure 10. The top graph shows data reduction while the bottom graph shows average throughput.

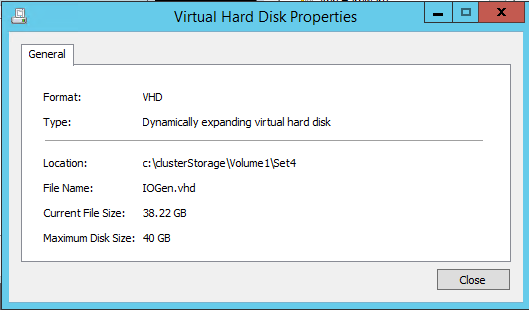
**Key Takeaway from Scenario #1:**

**Figure 10: Bandwidth Optimization for a Sparse Disk**

Replication of a sparsely populated data set delivered greater than 95% reduction of network traffic.

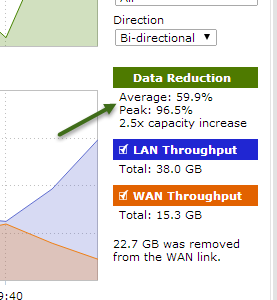
# Scenario #2: Dense Disk

After the SteelHead cache was cleared, a second VM was created and populated with random data. When the VM booted up, the file explorer in the guest showed the following details.



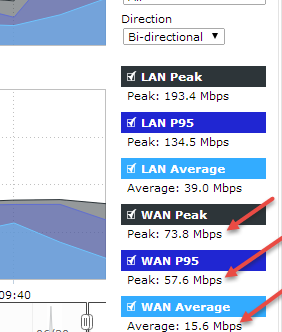
**Figure 11: Dense Disk - Explorer View**

This time around, given the nature of the disk, the optimization delivered was slightly lower at 60%.

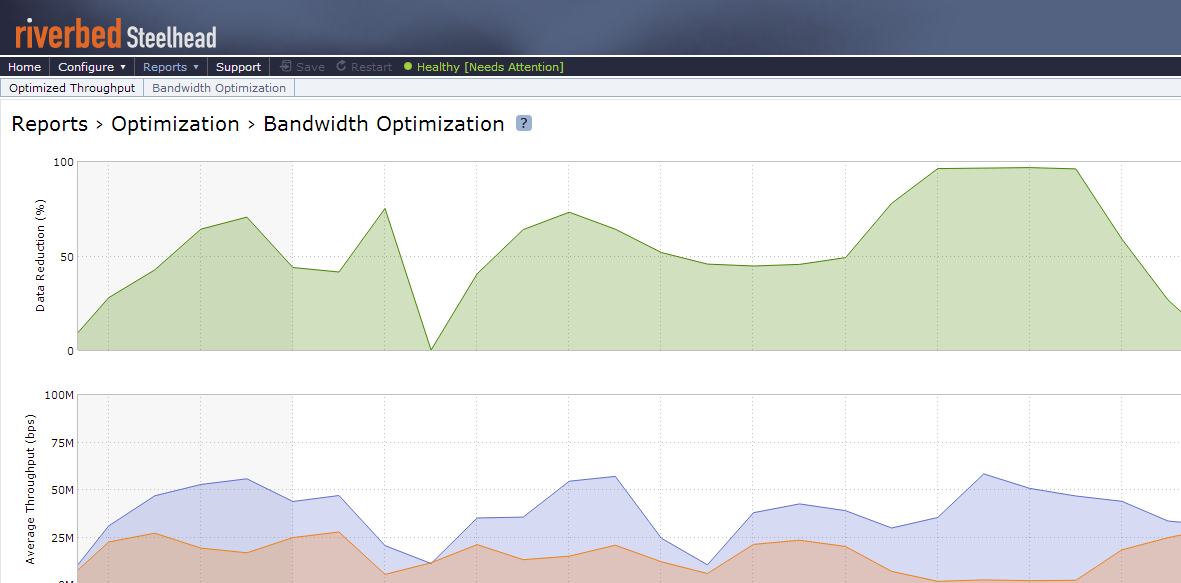


**Figure 12: Dense VHD - Optimization**

Referring to Figure 13 below, the average LAN bandwidth was 39Mbps and the average WAN bandwidth was 15.3Mbps meaning that the SteelHead solution reduced network traffic by greater than 50%. The P95 values for the LAN bandwidth and WAN bandwidth were 134.5Mbps and 73.8Mbps respectively. This translates into important savings on the networks.



**Figure 13: WAN, LAN Bandwidth - Dense disk**

Referring to Figure 14, the bandwidth optimization that started slowly, got higher over a period of time as the data reduction cache “warmed up”

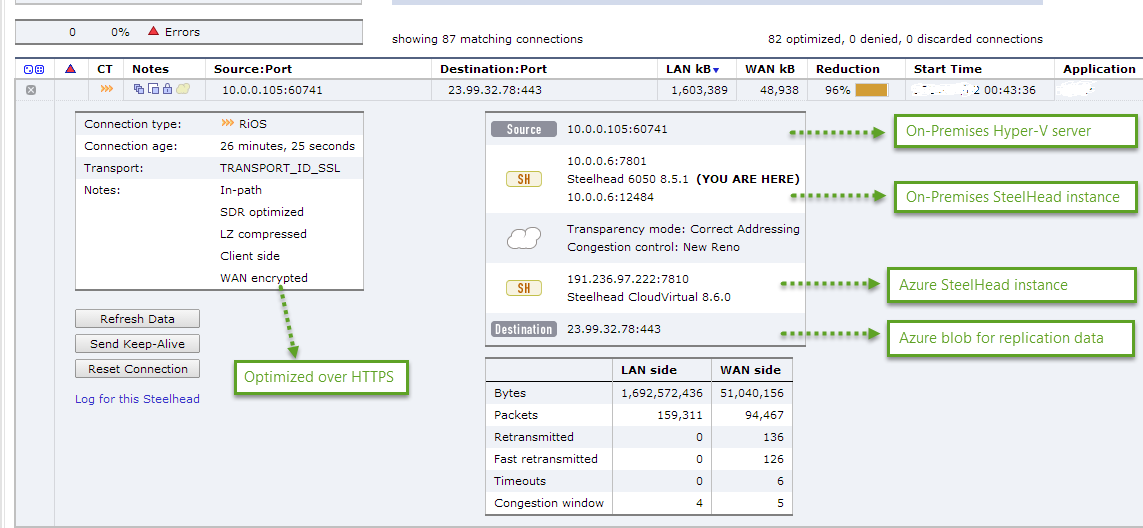
**Figure 14: Bandwidth Optimization - Dense disk**

**Key Takeaway from Scenario #2:** Replication of a densely populated data set delivers ~60% reduction of network traffic.

# Scenario #3: Multi-VM Scenario

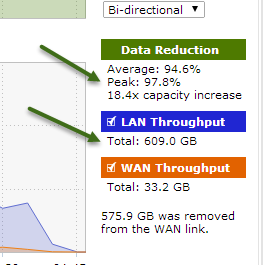
Scenario 3 tested optimization of ASR in a “scaled-out” scenario over a 7 day period using 50 virtual machines. The VM deployment consisted of:

* Physical sizes between 8 GB to 40 GB
* Logical size between 4 GB to 30 GB
* When enabling replication using ASR:
  + Spread of replication frequencies of 30sec, 5min, 15mins
  + Synthetic workloads were run inside the VM, which represent SQL, Exchange, file server data read/write characteristics.
  + The workload simulated peak times and off-business hours, weekday traffic and weekend traffic as well.
  + VMs “churned” (increasing the size of the log files that tracked the changes) between 2 MB per minute to 100 MB per minute.

Once an optimized connection is setup, the following can be seen in the Riverbed console. The key components are called out in the figure 15:

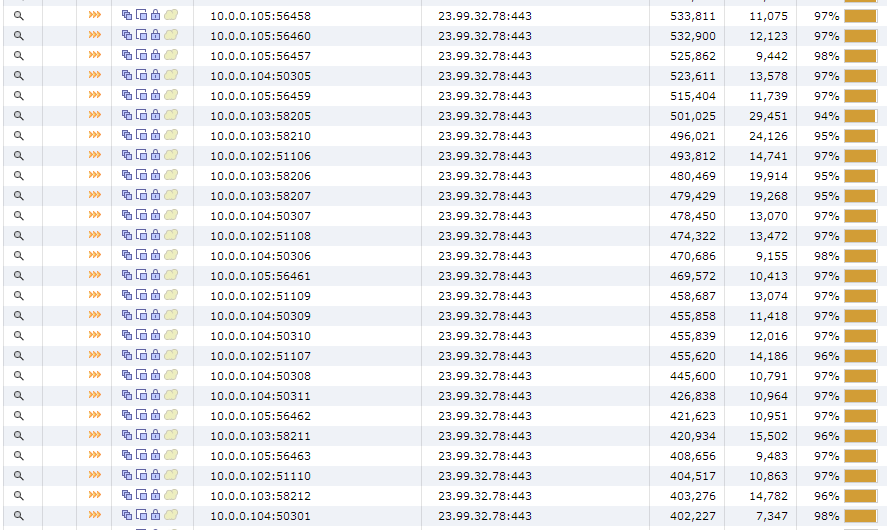
**Figure 15: Optimized Connection Details from the SteelHead Administration Console**

Snapshots of the optimization were taken at different points and high data reduction was achieved over a period of time.



**Figure 16: Data Reduction**

Data reduction is influenced by a number of factors such as read/write patterns, block size, repetition of the write patterns, workload peaks and valleys, and churn. While it is very difficult to model the application characteristics, the above experiment used a variety of tools during the entire exercise. Each time, the SteelHead solution delivered superior optimization.

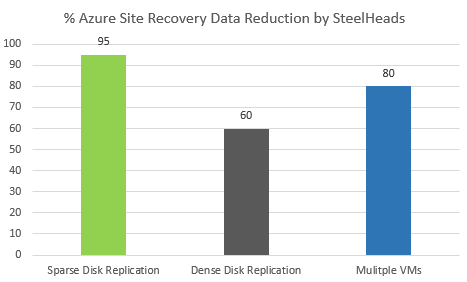
A snip of the active transfers during replication can be seen in the Figure 17, which illustrates the optimization delivered during delta replications.

**Figure 17: Current Connections page in SteelHead administration console**

**Key Takeaway from Scenario #3:** The SteelHead solution reduced network traffic more than 80% in a scaled out environment.

# Summary

Azure Site Recovery brings down the CAPEX and OPEX costs of a disaster recovery solution by enabling customers to protect their workloads to Microsoft Azure. A key component of this solution is around provisioning the network appropriately to ensure that the RPO goals are met. It is also important to ensure that the impact to the organization’s internet bandwidth is kept to the minimum. Riverbed SteelHead’s WAN optimization technology plays a crucial role in meeting this twin objective. With an industry-first Azure optimization appliance, the Riverbed SteelHead appliance provides significant savings on the internet bandwidth.

This paper illustrated the savings in a controlled environment running synthetic workloads which represent real-world applications – and the savings are very evident.

**Figure 18- Summary of results**

We found that the SteelHead solution exceeded expectations in reducing network traffic in a variety of scenarios as shown in Figure 18.

The two key takeaways are:

1. **Ease of configuration:** Azure Site Recovery and the SteelHead appliances were easy to configure and setup. This experiment was made successful with minimal interaction between the two companies – no special hooks were required from either side.
2. **Delivering high optimizations**: The Riverbed SteelHead provides a scalable, secure and efficient solution to optimize the replication traffic that was sent over HTTPS from the on-premises environment to Microsoft Azure. This significantly reduced bandwidth utilization, lowering WAN throughput required for ASR helping to ensures that ASR is able to deliver the RPO promise in scaled-out deployments. Network bandwidth is a precious commodity and the Riverbed SteelHead solution delivered greater than 90% reduction of replica traffic.