riverbed®

SteelHead™ (in the Cloud) User Guide

Version 9.12

Document revision: March 22, 2021

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107
www.riverbed.com

Part Number
712-00072-13

Contents

Welcome

About this guide

Welcome to the *SteelHead (in the Cloud) User Guide*. This guide describes how to deploy, configure, and manage Riverbed virtual appliances in cloud environments.

This guide includes information relevant to these components:

- SteelHead (in the cloud) (SteelHead-c)
- SteelHead SaaS (formerly Steelhead Cloud Accelerator)
- Riverbed Cloud Portal

Audience

This guide is written for storage and network administrators familiar with administering and managing WANs using common network protocols such as TCP, SMB, HTTP, FTP, and NFS. Familiarity with virtualization and cloud technologies is helpful.

Document conventions

This guide uses this standard set of typographical conventions:

Convention	Meaning
italics	Within text, new terms and emphasized words appear in *italic* typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface.

Monospace	Code examples appear in monospace font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: **{delete <filename> | upload <filename>}**

Software requirements for associated products

This table summarizes the software requirements for associated Riverbed products.

Riverbed component	Hardware and software requirements
Riverbed Cloud Portal	Any computer that supports a web browser with a color image display. The Management Console has been tested with Mozilla Firefox Extended Support Release version 17.0 and Microsoft Internet Explorer 7.0 through 9.0. Internet Explorer 7.0 and 8.0 must refresh reports every 4 minutes due to performance issues. Consider using a different browser to view reports. JavaScript and cookies must be enabled in your web browser.

Documentation and release notes

The most current version of all Riverbed documentation can be found on the Riverbed Support site at https://support.riverbed.com.

See the Riverbed Knowledge Base for any known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. To access the Riverbed Knowledge Base, log in to the Riverbed Support site at https://support.riverbed.com.

Each software release includes release notes. The release notes list new features, known issues, and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at https://support.riverbed.com.

Examine the release notes before you begin the installation and configuration process.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - 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** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.
- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

1

Riverbed Cloud Services

This chapter describes Riverbed cloud services. It includes these sections:

About Riverbed Cloud Services

Public, private, and hybrid cloud environments all face the same performance limitations of today's applications and networks. To maximize the flexibility and savings of the public cloud, you must first overcome the same latency and bandwidth constraints that challenge distributed IT infrastructure environments.

Riverbed cloud services help transform the cloud into an extension of the data center. SteelHead-c virtual appliances accelerate the migration of data and applications to the cloud, while speeding access to that data from anywhere. Compatibility with industry leading cloud environments eliminates vendor lock-in.

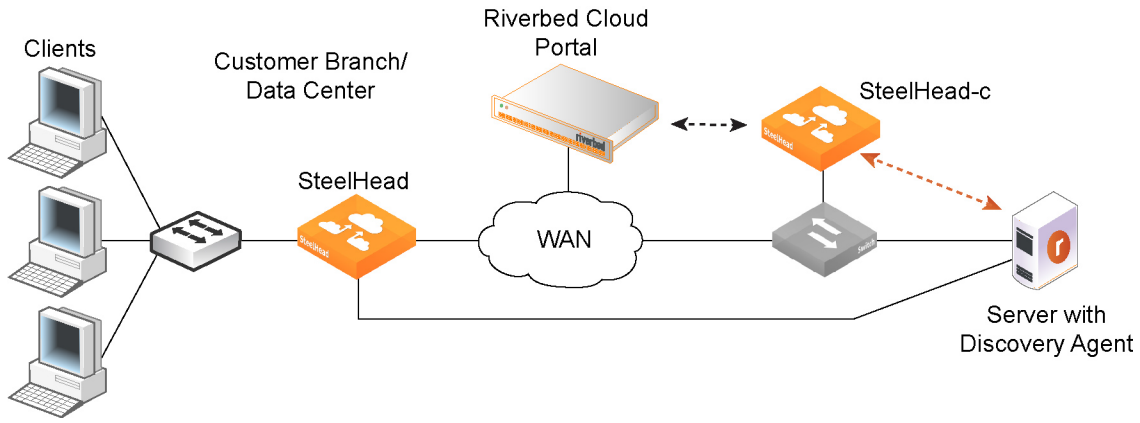
As you migrate services to the cloud, and later broaden your application and data footprint there, SteelHead-c virtual appliances ensure you will meet application performance service level agreements (SLAs), regardless of network latency and enterprise bandwidth limitations, to ensure seamless public-cloud integration through features like:

- transparent cloud interception.
- a flexible cloud pricing model.
- portal-based management.
- elastic sizing and cloning.
- interoperability with SteelHead-c virtual appliances, SteelHead physical appliances, and Client Accelerator.

Riverbed Cloud Services system components

This section provides an overview of the Riverbed cloud services system and its components. Figure 1-1 shows an overview of Riverbed cloud services.

Figure 1-1. Riverbed cloud services



The Riverbed cloud services system consists of these components:

- Riverbed Cloud Portal - A web portal hosted and managed by Riverbed. The Riverbed Cloud Portal manages licensing, deployment, and discovery of your SteelHead-c virtual appliances. For details, see Chapter 2, "Using the Riverbed Cloud Portal."
- **SteelHead-c** - Software form factor of SteelHead CX that is purpose-built for compatibility with a variety of IaaS vendors.
- Discovery Agent - Software that can be installed in the cloud where your optimized applications are hosted. The Discovery Agent assists client-side SteelHead appliances in locating peer SteelHead-c virtual appliances on the server side. It also provides failure detection and load balancing. For details, see Chapter 3, "Using the Discovery Agent."

Note: The Riverbed Cloud Portal uses elastic scaling technology. As a result, the portal is not always served from a static IP address. Ensure that all appliances that you want to communicate with the Riverbed Cloud Portal are configured to use DNS and hostnames for the portal.

Supported deployments

This section illustrates the client-server deployments that Riverbed cloud services support.

Figure 1-2 shows a deployment in which the server-side servers are behind a SteelHead-c in a network address translated (NATed) environment.

Figure 1-2. Servers in the cloud behind a SteelHead-c in a NATed environment

Figure 1-3 shows a deployment in which the servers in the cloud are behind a SteelHead-c. In this case, the network does not have NAT: for example, when you use an Amazon Virtual Private Cloud (VPC).

Figure 1-3. Servers in the cloud behind a SteelHead-c

Figure 1-4 shows a deployment in which the clients in the cloud are behind a SteelHead-c. In this case, the network does not have NAT: for example, when you use an Amazon VPC. In this deployment, you must use a Discovery Agent in the network.

Note: Riverbed cloud services do not support clients in the cloud in a NATed environment.

Figure 1-4. Clients in the cloud behind a SteelHead-c

SteelHead-c models and required virtual machine resources

This section lists available SteelHead-c models, their supported maximum limits, and the minimum virtual machine resources required for each model.

This table lists SteelHead-c models and their supported maximum limits.

SteelHead-c model	Optimized WAN capacity	Maximum # of connections (all IaaS vendors)
CCX-SUB-PERF-TIER1	10 Mbps	1250
CCX-SUB-PERF-TIER2	50 Mbps	4500
CCX-SUB-PERF-TIER3	200 Mbps	9000
CCX-SUB-PERF-TIER4	500 Mbps	1,000
CCX-SUB-PERF-TIER4-H	500 Mbps	30,000
CCX-SUB-PERF-TIER5	1 Gbps	1,000
CCX-SUB-PERF-TIER5-H	1 Gbps	50,000

Each SteelHead-c instance requires at least two virtual disks. One disk stores the SteelHead-c configuration and management resources (this disk is automatically deployed when you create the virtual appliance); the other disk serves as the data store (you must manually add this disk). In AWS, virtual disk drives are referred to as Elastic Block Stores (EBS). Hard disk drives (HDDs), also known as magnetic drives, can be used for most models, but solid state drives (SSDs) can provide higher performance.

Note: We recommend SSD drives for models CCX-SUB-PERF-TIER3 and greater.

This table lists SteelHead-c models and the disk capacities needed for each.

SteelHead-c model	Configuration and management disk size	Data store disk size
CCX-SUB-PERF-TIER1	38 GB	430 GB
CCX-SUB-PERF-TIER2	38 GB	430 GB
CCX-SUB-PERF-TIER3	40 GB	430 GB (SSD)
CCX-SUB-PERF-TIER4 CCX-SUB-PERF-TIER4-H	40 GB	1.2 TB (SSD) Azure: 2 x 512 GB (SSD)
CCX-SUB-PERF-TIER5 CCX-SUB-PERF-TIER5-H	40 GB	2.4 TB (SSD) Azure: 4 x 512 GB (SSD)

This table lists SteelHead-c models and the minimum instance type, or minimum virtual machine CPU and RAM, required to run each.

SteelHead-c model CCX-SUB-PERF-	Microsoft Azure VM size	Amazon EC2 instance type	Oracle OCI VM shape	VMware ESXi VM size
TIER1	A2_v2 (Standard) 2 vCPUs 4 GB RAM	m4.large 2 vCPUs 8 GB RAM	VM.Standard2.1 1 OCPU 15 GB RAM	2 CPU/1200 MHz 3 GB RAM
TIER2	A4_v2 (Standard) 4 vCPUs 8 GB RAM	m4.large 2 vCPUs 8 GB RAM	VM.Standard2.1 1 OCPU 15 GB RAM	4 CPU/1200 MHz 8 GB RAM
TIER3	D3_v2 (Standard) 4 vCPUs 14 GB RAM	m4.2xlarge 8 vCPUs 32 GB RAM	VM.Standard2.2 2 OCPU 30 GB RAM	4 CPU/2.2 GHz 14 GB RAM
TIER4 TIER4-H	D14_v2 (Standard) 16 vCPUs 112 GB RAM	m4.4xlarge 16 vCPUs 64 GB RAM	—	—
TIER5 TIER5-H	D15_v2 (Standard) 20 vCPUs 140 GB RAM	m4.10xlarge 40 vCPUs 160 GB RAM	—	—

System limitations and dependencies

SteelHead-c images can be installed on AWS, VMware ESX/ESXi, Microsoft Azure, and Oracle Cloud Infrastructure (OCI) virtual machines. The Riverbed Cloud Portal supports licensing and simple management for SteelHead-c virtual appliances on all virtual machine platforms.

All SteelHead-c virtual appliances, including virtual appliances intended for AWS China or AWS GovCloud regions, must be manually deployed. However, SteelHead-c virtual appliances can be automatically licensed through the Riverbed Cloud Portal providing they have web access to the portal.

Hybrid networking features such as path selection and secure transport are not supported. Also, SCPS licenses are not supported.

Limitations on AWS

This section describes the deployment and feature options that the SteelHead-c for AWS does not support.

Deployment limitations

- **Automatic peering** - The SteelHead-c does not use automatic peering. When you run a server in the cloud, you deploy the SteelHead-c to be the furthest SteelHead in the network, because the Discovery Agent on the server is configured to use the SteelHead-c automatically. When you run a client in the cloud, and there are multiple SteelHeads in the path to the server, the SteelHead-c is selected for optimization first. You can enable automatic peering on the remote SteelHeads to make the SteelHead-c peer with the furthest SteelHead in the network.
- **Simplified routing** - The SteelHead-c for AWS is not deployed in-path, but rather in its unique out-of-path method using one interface. Simplified routing does not apply.
- **WCCP/PBR/L4** - The SteelHead-c for AWS uses a unique redirection mechanism that enables deployments in any cloud environment. The SteelHead-c also supports WCCP/PBR/L4 redirection when made available by the cloud provider. Amazon EC2 does not support these traditional redirection mechanisms.
- **Connection forwarding** - The SteelHead-c uses a unique out-of-path method; connection forwarding does not apply.

Feature limitations

- **RSP** - The SteelHead-c for AWS is a virtual SteelHead deployed into the AWS virtualization environment. You need not run virtualization on top of virtualized software.
- **PFS** - It is easier and simpler for you to run a separate file server instance in the cloud and not use the SteelHead for Proxy File Service (PFS).
- **WAN visibility mode** - The SteelHead-c currently supports only correct addressing. It does not support full transparency and port transparency.

- **CIFS prepopulation** - CIFS prepopulation is not supported on the SteelHead-c for AWS because it requires the Riverbed Copy Utility (RCU) to run on a different interface. Prepopulation also requires a switch to make the traffic loop back through the SteelHead, which is not possible in the cloud. If you want prepopulation, you can install the RCU or a similar tool on a machine in the cloud. You would most likely configure prepopulation on the remote SteelHead instead of the SteelHead-c.

Limitations on VMware ESX/ESXi

This section describes the deployment and feature options that the ESX SteelHead-c does not support.

Deployment limitations

- **Automatic peering** - ESX SteelHead-c virtual appliances deployed with Web Cache Communication Protocol (WCCP) or Policy-Based Routing (PBR) support automatic peering. ESX SteelHead-c virtual appliances deployed with the Discovery Agent do not support automatic peering.
- **Simplified routing** - ESX SteelHead-c virtual appliances deployed in-path with the Discovery Agent support simplified routing. ESX SteelHead-c virtual appliances deployed with WCCP or PBR do not support simplified routing.

Feature limitations

- **RSP** - RSP enables virtualization in physical SteelHead appliances. SteelHead-c is a virtual SteelHead CX appliance running on a virtual machine. There is no need for additional layers of virtualization.
- **PFS** - It is easier to run a separate file server instance in the cloud and not use the SteelHead-c for Proxy File Service (PFS).
- **WAN visibility mode** - ESX SteelHead-c virtual appliances deployed with WCCP or PBR support WAN visibility mode. When deployed with the Discovery Agent, however, WAN visibility mode is not supported.
- **CIFS prepopulation** - ESX SteelHead-c virtual appliances deployed with WCCP or PBR support CIFS prepopulation. When deployed with the Discovery Agent, however, CIFS prepopulation is not supported.

Reduced data store feature

Note: This feature is only supported on ESX-based SteelHead-c virtual appliances.

In SteelHead-c versions before 1.2, you must allocate a data store volume of exactly 440 GB for the virtual appliance; otherwise, the SteelHead-c does not function correctly.

The reduced data store support feature in SteelHead-c 1.2 first checks if 440 GB of disk space is allocated for the data store. If less than 440 GB of disk space has been provisioned, the SteelHead-c software creates a 30-GB data store. This allows you to create SteelHead-c that require less disk space but still provide WAN optimization. The optimization performance is impacted when you do not use a 440-GB disk for the data store. Performance depends on the size of your working data set.

The SteelHead-c uses either 440 GB or 30 GB. If you allocate a disk space that is less than 440 GB, but later than 30 GB (such as 250 GB), the SteelHead-c uses only 30 GB; it disregards 220 GB. If you allocate less than 30 GB, the SteelHead-c does not function correctly.

After you create a disk, if you resize it to 440 GB, the SteelHead-c still uses only 30 GB. To increase the data store size to 440 GB, you must delete the original disk and create a new 440 GB disk. Doing this reverts the data store to a "cold" state; performance improves as the SteelHead executes subsequent data transfers over the WAN.

Limitations on Microsoft Azure

These limitations apply to the SteelHead-c for Azure:

- Multiple NICs, PBR, and WCCP are not supported.
- The CCX-SUB-PERF-TIER5 models for Azure use multiple disks with FTS to achieve their large data store capacity. Because of this different disk layout, upgrading to these models requires clearing the data store. See "Upgrading and downgrading SteelHead-c RiOS software" on page 17.

Licensing SteelHead-c virtual appliances

Licenses for SteelHead-c virtual appliances are stored on the Riverbed Cloud Portal. Each license is associated with a one-time token unique to it. Applying a one-time token to a SteelHead-c enables the virtual appliance to contact the portal and to associate the token's license with the SteelHead-c. To obtain a one-time token, you must have an account on the Riverbed Cloud Portal. Typically, Riverbed will establish a user account on the portal for you after you purchase a cloud product, and Riverbed will send you an email with details and login information about your account. After your account is established, you can log in and view your purchased licenses. Select a license to view details about it, including the one-time token associated with it.

Note: For virtual appliances that cannot be provisioned through the portal, the token must manually be applied to the appliance.

To obtain a one-time token

1. Log in to the Riverbed Cloud Portal.
2. Select the Cloud Appliances tab and select Licenses to display the Licenses page.
3. Select the serial number of an unprovisioned license to display the License Details page.
4. Copy the one-time token displayed on the License Details page.

To apply the token using the portal

1. Open another browser window and navigate to the appliance's management console.
2. Navigate to this console page:
   - If you are licensing a SteelHead-c running RiOS 8.6.x or earlier, choose Configure > Maintenance > Licenses.
   - If you are licensing a SteelHead-c running RiOS 9.0.x or later, choose Administration > Maintenance: Licenses.
3. Under the Cloud Licensing section, paste the one-time token into the One-time Token field.
4. Click **Initialize License Client**.

To apply the token using the command-line interface

1. Log in to the appliance's command-line interface as admin.

   The default password is **password**. If you specified administrator credentials at the time you created the virtual appliance instance, use those credentials.

2. Enable configuration mode:

   ```
   enable
   configure terminal
   ```

3. Enter this command:

   ```
   license client init <one-time-token>
   ```

4. Verify that the license is applied:

   ```
   show licenses
   ```

Upgrading and downgrading SteelHead-c models

To upgrade a SteelHead-c virtual appliance to a model that does not require a higher-capacity virtual machine, simply purchase a license for the new SteelHead-c model. Downgrading a SteelHead-c model is as simple as downgrading the license to that of a lower-end model. The SteelHead-c detects any change in the license associated with it when it communicates with the Riverbed Cloud Portal.

To upgrade a SteelHead-c virtual appliance to a model that requires a higher-capacity virtual machine:

1. Purchase a license for the new SteelHead-c model.
2. Deprovision the original SteelHead-c virtual appliance and its underlying virtual machine.
3. Provision a new virtual machine that meets the requirements of the new SteelHead-c model.
4. Obtain the image for the new SteelHead-c model and install it on the virtual machine.

Downgrading a SteelHead-c model is as simple as downgrading the license to that of a lower-end model.

Upgrading and downgrading SteelHead-c RiOS software

You can upgrade and downgrade the operating system software on your SteelHead-c for AWS virtual appliances through the Riverbed Cloud Portal by performing the task described in this section.

You can upgrade and downgrade the operating system software on your SteelHead-c virtual appliances hosted on other cloud platforms in the same manner as physical SteelHead appliances by using the Software Upgrade page in an appliance's management console. For details, see the *SteelHead User Guide* and "To upgrade a SteelHead-c for Azure or ESX/ESXi to RiOS 9.2 or later" on page 18.

To upgrade or downgrade RiOS software on SteelHead-c for AWS

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to upgrade.
3. Select Appliances.
4. Select the name of the appliance you want to upgrade or downgrade.
5. Select the Summary tab.
6. Stop the appliance.
7. Select a version from the Version drop-down list.
8. Click **Update Details**.

Note: The SteelHead-c IP addresses will change. Ensure that you update any rules or configurations that depend on it such as fixed-target rules on on-premise SteelHeads that peer your SteelHead-c, on-premise firewall configurations, or security group configurations.

To upgrade a SteelHead-c for Azure or ESX/ESXi to RiOS 9.2 or later

With RiOS 9.2 and later, SteelHead-c images use a partition layout for the data store disk that is different from the layout of SteelHead-c images using previous versions of RiOS.

Because of this change, upgrading through the virtual appliance's console or the CLI will not work. For Azure and ESX/ESXi environments, you must first create SteelHead-c running RiOS 9.2 or later and then manually transfer the license, configuration file, and data store disk from a pre-RiOS 9.2 or later SteelHead-c to the RiOS 9.2 or later SteelHead-c.

Note: Upgrading any SteelHead-c model on Azure to RiOS 9.5 clears the SteelHead-c data store.

Note: If you are using SteelHead-c, ensure that you reconfigure the Discovery Agent to use the primary IP address of the new RiOS 9.2 or later SteelHead-c and that you restart the Discovery Agent.

1. Create a new SteelHead-c running RiOS 9.2 or later. Do not create a new data store disk for it.
2. Deactivate the license for the pre-RiOS 9.2 SteelHead-c on the Riverbed Cloud Portal and on the virtual appliance itself.
3. Remove the data store disk from the pre-RiOS 9.2 SteelHead-c using the procedure for your platform.

   Azure:

   - In the Azure portal, select the Virtual Machines tab.
   - Select the virtual machine that is hosting the virtual appliance
   - Click **Detach Disk**.
   - Select the data store disk and click **OK**. Remember the name of the data store disk.

   ESX:

   - Log in to vSphere or the host for the virtual machine hosting the virtual appliance.

- Find the virtual machine hosting the virtual appliance and power the virtual machine off.
- Choose Edit Settings > Hard Disk options and delete the data store disk.
- Power on the virtual machine.

4. Attach the disk from Step 3 to the RiOS 9.2 or later SteelHead-c that you created in Step 1.

   Azure:

   - In the Azure portal, select the Virtual Machines tab.
   - Select the virtual machine that is hosting the new virtual appliance.
   - Click **Attach**, and then click **Attach Disk**.
   - Select the data store disk from Step 3 from the Available Disks dropdown menu and click **OK**.

   ESX:

   - Log in to vSphere or the host for the virtual machine hosting the new virtual appliance.
   - Select the virtual machine hosting the new virtual appliance
   - Navigate to Edit Settings > New Device and select Existing Hard Disk.
   - Click **Add,** and navigate to the data store disk from Step 3 (.vmdk file), and click **Add**.
   - If the virtual machine is not running, power it on.

5. Copy the configuration file from the pre-RiOS 9.2 SteelHead-c to the RiOS 9.2 or later SteelHead-c that you created in Step 1. If you have SteelCentral Controller for SteelHead you can use it to copy the configuration file to the new RiOS 9.2 or later SteelHead-c. See the *SteelCentral Controller for SteelHead User Guide*.

   If you do not have SteelCentral Controller for SteelHead, use this procedure to copy the configuration file to the new RiOS 9.2 or later SteelHead-c.

   - Connect to the command-line interface (CLI) for the pre-RiOS 9.2 SteelHead-c. See the *Riverbed Command-Line Interface Reference Manual*.
   - Use the **scp** command to copy the configuration to a location that is accessible to both the pre-RiOS 9.2 SteelHead-c and the RiOS 9.2 or later SteelHead-c.

     ```
     sh (config)# configuration upload <config-file-name> <destination ftp/http/scp server>
     ```

   - Connect to the CLI for the RiOS 9.2 or later SteelHead-c and use the **fetch** command to copy the configuration file from the upload location to the RiOS 9.2 or later SteelHead-c.

     ```
     sh (config)# configuration fetch <ftp/http/scp server>/<config-file-name>
     ```

   - On the RiOS 9.2 or later SteelHead-c, show configurations. The list includes the new configuration file.

     ```
     sh (config)# show configuration files
     initial.bak              2016/03/29 20:30:34
     <config-file-name>       2016/03/29 22:22:48
     initial (active)         2016/03/29 20:37:58
     ```

   - Apply the configuration.

     ```
     sh (config)# configuration switch-to <config-file-name>
     ```

6. Activate the license from Step 2 on the RiOS 9.2 or later SteelHead-c.

7. Log in to the console for the RiOS 9.2 or later SteelHead-c and ensure that the status for the virtual appliance is **healthy**.
8. Delete the old instance of the virtual appliance.

2

Using the Riverbed Cloud Portal

This chapter describes how to use the Riverbed Cloud Portal. It includes these sections:

About Riverbed Cloud Portal

The Riverbed Cloud Portal is a web-based portal hosted and maintained by Riverbed. The portal offers these features:

- License management for all your SteelHead-c and SteelHead SaaS virtual appliances.
- Light-weight appliance management.
- Direct provisioning of virtual appliances to supported cloud platforms.
- Automated appliance discovery in supported cloud platforms.

The portal is divided into two main sections, accessible through the Cloud Appliances tab and the Cloud Accelerator tab. The Cloud Appliances section is accessible to all customers with a Riverbed Cloud Portal account, and it is where you can manage your SteelHead-c virtual appliances. The Cloud Accelerator section is accessible only to customers who are subscribed to the Riverbed SteelHead SaaS service. SteelHead SaaS accelerates SaaS applications, such as Salesforce and Microsoft Office 365, over the Akamai network. For complete details about this service, see the *SteelHead SaaS User Guide*.

Access the portal at https://cloudportal.riverbed.com.

If you do not have a portal account, contact a Riverbed sales person at http://www.riverbed.com.

About company associations

At least one *company* is associated with every portal account. Configuring multiple companies under an account enables you to organize your SteelHead-c virtual appliances by organization. When you log in to the portal, the information displayed on the various portal pages pertains to appliances associated with the currently selected company.

You can select a different company by clicking **Change Company** in the upper-left corner.

Accessing account settings

Account settings include name, email address, and companies associated with the account. You can also change your password in this page.

To view account settings

1. Mouse over your email address in the upper-right corner of the portal.
2. Select Account Settings.

To change your password

1. In the Account Settings page, click **Change Password**.
2. Enter old password.
3. Enter new password.
4. Confirm new password.
5. Click **Change Password**.

Viewing event history

The Event History report displays all of the events that occurred for a particular company. This page enables multiple end users in the same company to view all events pertaining to their company. It describes events such as creation and deletion of users and optimization groups, registration of Discovery Agents, and the registration, provisioning, and deprovisioning of SteelHead-c virtual appliances.

The Event History page displays this information for each event:

- **Date** - Date when the event occurred.
- **User** - Username of the entity that performed the action.
- **Description** - Description of the event.

To view the event history report

Mouse over your username in the upper-left section of the page and select Event History.

Finding support

The Support menu provides these options:

- **Help** - Launches the online help information about the portal.
- **News** - Displays relevant news stories published on the portal by Riverbed employees.
- **Downloads** - Navigates to the page on the Riverbed Support site where you can access software images used along with the portal. For example, you can download the Discovery Agent, which is used on virtual servers optimized by a SteelHead-c or a SteelHead SaaS appliance.
- **Cloud Support** - Navigates to the page on the Riverbed Support site where you can download software images and product documentation.

Viewing service summary

The Service Summary page provides a dashboard view of the system. It displays:

- **Company** - Displays the name of the currently selected organization.
- **Riverbed Appliances** - Lists the appliances that are currently provisioned for the selected organization. Select the name of an appliance for details about it.
- **Licenses** - Lists the serial number, type, and model of each available license.
- **Optimization Groups** - Displays the optimization groups you configured. Select an optimization group name for details about it.
- **Portal News** - Displays the last three news stories published by Riverbed employees to the portal.
- **Recent Events** - Describes recent events and activity in your company. For example, it might report that a user launched or shut down a particular appliance or provide a list of licenses granted to the company.

Managing licenses

The portal acts as a license server for your cloud appliances. Licenses are stored on the portal and each license is associated with a *one-time token* that is unique to it. You use the one-time tokens to associate a specific appliance with a specific license.

Note: When a license expires, the appliance automatically stops the optimization service. The license expires on the termination date regardless of whether you use it.

To view summary information about your licenses

In the Cloud Appliances tab, select Licenses. The Licenses page displays information about your unused, active, and expired licenses.

The Unused Licenses table and the Expired Licenses table display this information:

Parameter	Description
Serial Number	The license serial number. Select the serial number for more details about the license.
Model	The SteelHead-c model.

The Active Licenses table displays this information:

Parameter	Description
Serial Number	The license serial number. This number is also the appliance serial number. Select the serial number for more details about the license.
Appliance	Displays the user-configurable name and the type (such as ESX or AWS) of appliance.
Version	The software version of RiOS running on the appliance. This information is displayed only for active licenses that have been provisioned through the Riverbed Cloud Portal.

Viewing license details

You can access detailed information about a specific license by selecting the license serial number in the Licenses page. The License Details page contains three tabbed sections: Details, Features, and Event Log.

To view license details

In the License Details page, select the Details tab to view this information:

- **License Serial Number** - Displays the serial number of the license and of the appliance.
- **State** - Indicates the current state of the appliance that is associated with the selected license. See "About SteelHead-c virtual appliance license states" on page 29.
- **Product Type** - Displays the type of product (SteelHead-c).
- **One Time Token** - (Unused licenses only.) Displays the token associated with the selected license. Enter this value into a manually provisioned appliance to associate the selected license with the appliance. The licensing process is automatic for appliances that are provisioned through the portal.
- **One Time Token State** - Indicates the status of the one-time token and the date and time it expires.
- **Appliance Software Version** - Displays the RiOS version on the appliance. Displayed only for running appliances.
- **Last Checkout** - Displays the date and time when the appliance last checked out the license.

To view license features

Select the Features tab to view license information:

- **Feature** - Displays the model of the appliance.

- **Status** - Indicates whether the license is valid or invalid.
- **Start date** - Displays the date and time when the feature becomes active.
- **End date** - Displays the date and time when the feature becomes inactive.
- **Termination date** - Displays the date and time when the license expires. The license expires on the termination date regardless of whether you use it.

To view license-related events

1. Select the Events Log tab.
2. Optionally set these parameters:
   - Specify the level of log detail you want:

Log level	Description
Critical	Reports conditions that severely affect the functionality of the appliance.
Error	Reports conditions that affect the functionality of the appliance.
Warning	Reports conditions that could affect the functionality of the appliance, such as authentication failures.
Notice	Reports normal but significant conditions, such as a configuration change.
Informational	Reports informational messages that provide general information about system operations.
Debug	Reports messages that help you debug a failure.

   - Specify the number of records to display per page.
   - Specify whether the system should periodically refresh the display.

Each log entry contains an entry ID, time stamp, IP address of the system where the event was initiated, username of the user who initiated the event, log level, and message.

Deploying an appliance in AWS

This section describes how to deploy a SteelHead-c virtual appliance to AWS by using the Riverbed Cloud Portal.

Note: Manual deployment is the only supported deployment method for AWS GovCloud (US) and AWS in China regions.

When you provision a license to AWS, the portal automatically creates a licensed SteelHead-c virtual appliance hosted on a virtual machine in the AWS cloud service.

Additionally, a region-free Amazon Machine Image (AMI) for SteelHead-c is available on the Amazon Web Services (AWS) marketplace. This product is called SteelHead-c for AWS Marketplace and has these benefits:

- You can instantiate SteelHead-c instances directly from AWS Marketplace.
- You update SteelHead-c instances directly from the SteelHead Management Console. You accomplish this task by downloading the image from the Riverbed Support site, then use the SteelHead Management Console to select the downloaded image and install it.

- You can use a license from the Riverbed Cloud Portal to activate the SteelHead-c for AWS Marketplace. This feature is known as Bring Your Own License (BYOL).

To provision a SteelHead-c to AWS through the Riverbed Cloud Portal

1. Log in to the portal and select the Cloud Appliances tab.
2. Select Licenses.
3. Select an unused license.
4. In the License Details page, select the Details tab.
5. Click **Provision to AWS**. The Launch SteelHead-c dialog box is displayed.
6. Complete the configuration as described in this table.

Item	Description
Appliance Name	Enter a display name for the appliance.
Description	Enter a description for the appliance.
Version	Select a RiOS software version from the drop-down list.
Optimization Group	Select an optimization group in which to add the appliance.
Region	Select the geographic region closest to you from the drop-down list.
Availability Zone	Select a geographic zone from the drop-down list. For example, for the Amazon US East cloud, you can choose us-east-1a, us-east-1b, us-east-1c, or us-east-1d. A zone is a physical data center site managed by Amazon that provides standby computing power to its assigned regions. Appliances communicate through IP addresses, and there are no traffic restrictions between zones (or costs for data passing between zones).
VPC Subnet	Select a subnet for the Virtual Private Cloud (VPC) IP address from the drop-down menu. Subnets are segments of a VPC's IP address space. The subnets enable you to separate the isolated resources (such as Amazon EC2 instances) in the VPC based on security and operational requirements. If you create more than one subnet in a VPC, they are attached to each other by a logical router, in a star topology. If you do not select a subnet, the system provisions the appliance in the public AWS cloud.
Elastic IP Address	Select an elastic IP address from the drop-down list. Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An elastic IP address is associated with your account, not a particular instance, and you control that address until you choose to explicitly release it. The portal allows you to associate an elastic IP address with your SteelHead-c. If you choose to assign an elastic IP address to a SteelHead-c, it means that every time the SteelHead-c is started it will have the same IP address.
Key Pair	Select an SSH key pair in your Amazon account for the appliance. **Note:** You must select a Key Pair or specify an Admin Password or do both.
Admin Password	Specify a password for the SteelHead-c administrator. The username is *admin*.

Item	Description
Confirm Admin Password	Confirm the administrator password entered in the previous field.
Network Access	Select the check box Allow network access from my location to enable other SteelHeads and computers at your location to access the appliance.

7. Click **Launch** to provision the SteelHead-c.

   The system creates a SteelHead-c in AWS and applies the license to it. After the provisioning process is complete, the SteelHead-c automatically restarts and the portal displays the Appliance Summary page.

Regenerating a one-time token

Each Riverbed license issued through the portal is associated with a one-time token unique to that license. The one-time token provides the appliance with secure access to the portal and associates its license with the appliance.

When an appliance, and its license, is provisioned through the portal, the token is automatically associated with the appliance. For appliances that cannot be provisioned through the portal, the token must manually be applied to the appliance. See "Licensing SteelHead-c virtual appliances" on page 16.

In rare cases, it may be necessary to regenerate the one-time token. Regenerating a token creates a new unique token for the license, and the old token becomes obsolete. The new token must be applied to the appliance. These situations might require regenerating a token:

- A token has been compromised and there is a possibility that an unauthorized entity can obtain the associated license.
- An existing and formerly licensed appliance has been missing for a long enough time that the portal reclaims its license.

Regenerating the one-time token can reassociate the appliance with its former license.

To regenerate a one-time token

1. In the Licenses page, select the serial number for which you want to generate a one-time token.
2. In the License Details page, select the Details tab.
3. Click **Regenerate Token**.

Reclaiming a license

After an appliance is registered, the license associated with it cannot be used by other appliances. Reclaiming a license removes the appliance from the portal database and generates a new one-time token for the license. The previous one-time token that was installed on the appliance is no longer valid. The portal displays the license in the Unused Licenses section of the Licenses page.

Reclaiming a license does not affect the appliance's underlying virtual machine. If you want to fully deprovision the appliance, you must manually deprovision it using tools available from your cloud platform provider.

The ability to reclaim a license can be useful in situations like evaluating several cloud platform providers. You need only one license to include the SteelHead-c as part of the evaluation, because the license is portable between different cloud providers.

Registering SteelHead-c virtual appliances

Auto-registration is the process in which a licensed appliance reports to the Riverbed Cloud Portal and if a one-time token is installed on the appliance, the portal automatically creates an entry in its database for the appliance. After the appliance is registered, it is listed as a Riverbed Appliance in your portal account.

An appliance can be unregistered by reclaiming its license or by regenerating the one-time token associated with its license. See "Regenerating a one-time token" on page 27 and "Reclaiming a license" on page 27.

Managing SteelHead-c virtual appliances

The Appliances page lists all appliances associated with the currently selected company and includes this information about each appliance.

Note: Some features are available only for appliances hosted in AWS and deployed directly through the portal.

- **Name** - Displays the user-configurable appliance name. This name is specific to the Riverbed Cloud Portal; it might not appear in a cloud vendor's management tool (such as the Amazon EC2 Management Console) because the vendor might not support such metadata.
- **Cloud** - Indicates the cloud service or platform on which the appliance is hosted.
- **License** - Displays the Riverbed license associated with the appliance.
- **State** - Indicates the current state of the appliance or its license or both.
- **VM Uptime** - Displays the duration for which the appliance has been running.
- **Creation Time** - Indicates date and time when the appliance was provisioned.
- **Description** - Displays the user-configurable description entered when the appliance was created.

You can view information about and perform simple management operations on specific appliances directly through the portal by selecting the name of an appliance listed on the Appliances page.

You can also manage your SteelHead-c virtual appliances through the SteelCentral Controller for SteelHead. See the *SteelCentral Controller for SteelHead User Guide* for details.

An appliance's home page is organized into tabs.

Cloud platform	Tab	Description
All cloud platforms	Summary	Displays basic information about the appliance such as Name, Description, State, License, Version, and a link to the appliance's management console.
	Details*	Displays information such as Uptime, Creation Time, UUID, and Architecture.
	Event Log	Displays information about events associated with the appliance.
AWS only	Network Controls	Displays information about the appliance's network configuration.
	AWS Console	Displays output of the virtual serial console that is connected to the host virtual machine.
* Details for SteelHead-c for AWS virtual appliances are different than those for appliances on other platforms.		

To view a list of all appliances under the currently selected company

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliances you want to view.
3. Select Appliances.

About SteelHead-c virtual appliance license states

This table lists the possible states for a license.

Cloud Platform	State	Description
AWS	Unprovisioned	The license is not used.
	Unknown	The portal cannot determine the state of the license, probably due to an error.
	Not Running	The license is attached to a Riverbed appliance, but the appliance is not running.
	Running	The license is attached to a Riverbed appliance, and the appliance is running.
	Stopping	The license is attached to a Riverbed appliance, but the appliance is in the process of being stopped.
	Starting	The license is attached to a Riverbed appliance, but the appliance is in the process of starting.
	Missing	The license is attached to a Riverbed appliance, but the appliance is missing. This usually occurs when the appliance is deleted by tools other than the Riverbed Cloud Portal. If the license is in the Missing state, deprovision the appliance to release the license and provision it again.

Cloud Platform	State	Description
ESX/ESXi, Azure	Active	The license is associated with a running appliance.
	Inactive	The license is associated with an appliance that is not in use.
	Unlicensed	No license is associated with the appliance.

Viewing appliance properties

You can view information about, and perform simple operations on, a specific appliance in the Summary tab of the appliance's page. The Summary tab displays this information.

Note: Appliances in the GovCloud and China regions display Name, License, and a link to the appliance's console. You can also reclaim licenses used by appliances in those regions and to use with any SteelHead-c anywhere.

- **Name** - Displays the user-configurable name of the appliance. This name is specific to the Riverbed Cloud Portal and might not appear in a cloud vendor's management tool.
- **Description** - Displays the user-configurable description entered when the appliance was created.
- **State** - Indicates the current state of the appliance. See "About SteelHead-c virtual appliance license states" on page 29.
- **License** - Displays the Riverbed license associated with the appliance.
- **Version** - Displays the version number of the RiOS software on the appliance.
- **Management Console** - Displays a link to the appliance's Management Console. It displays Not Available until the appliance is fully provisioned.

To view appliance properties

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to view.
3. Select Appliances.
4. Select the name of the appliance you want to view.
5. Select the Summary tab.

Editing an appliance name

You can edit the name of an appliance in the Appliance Summary page.

To edit the name of an appliance

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to edit.
3. Select Appliances.

4. Select the name of the appliance you want to edit.
5. Select the Summary tab.
6. Enter a new name in the Name text field.
7. Click **Update Details**.

Changing appliance RiOS version

You can change the version of RiOS running on the appliance in the Appliance Summary page.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform. RiOS software on appliances on other cloud platforms can be upgraded through the SteelHead Management Console or Riverbed CLI commands.

Accessing the management console for an appliance

The management console enables you to perform many management activities on an appliance. You can access the management console to an appliance from the Appliance Summary page.

Prerequisites: Ensure that the appliance is fully provisioned, licensed, and running.

To access the management console to an appliance

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to access.
3. Select Appliances.
4. Select the name of the appliance you want to access.
5. Select the Summary tab.
6. Select the link under Management Console.
7. In the Management Console login page, enter your credentials for the appliance.

Starting, shutting down, and deprovisioning an appliance

You can start, shut down, and deprovision an appliance in the Appliance Summary page.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

- Starting an appliance starts the optimization service. The **Start** button is enabled only if the appliance is currently stopped.
- Shutting down an appliance stops the optimization service. The **Shut down** button is enabled only if the appliance is currently running.
- Deprovisioning an appliance deletes the configuration volume and all data store volumes. The license is reclaimed and available for reuse. The **Deprovision** button is enabled only if the appliance is not running. This operation cannot be undone.

To start, shut down, or deprovision an appliance

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to modify.
3. Select Appliances.
4. Select the name of the appliance you want to modify.
5. Select the Summary tab.
6. Click the button that corresponds to the action you want to take (**Start**, **shut down**, or **Deprovision**).

Viewing SteelHead-c for AWS virtual appliance details

The AWS Details tab in the Appliance Details page contains AWS-specific information about an appliance hosted on the AWS cloud service. You can view this information in the AWS Details tab:

- **EC2 Instance Uptime** - Indicates the duration for which the virtual appliance has been running.
- **Creation Time** - Displays the time when the virtual appliance was created.
- **Availability Zone** - Indicates the zone where the virtual appliance is provisioned. Zones are physical sites that Amazon provides, which are racked and ready to supply additional computing power to the region to which they are assigned.
- **Key Pair** - Displays the SSH key pair in your Amazon account for the virtual appliance.
- **Subnet** - Indicates the subnet for the Virtual Private Cloud (VPC) IP address.
- **AMI** - Displays the name of the virtual machine, or Amazon Machine Instance (AMI), hosting the virtual appliance; the appliance name can be different than the AMI name.
- **Last Known Instance ID** - Displays the last known EC2 instance ID associated with the appliance.
- **Instance Type** - Displays the type of EC2 instance launched when the virtual appliance is started.
- **Architecture** - Displays the virtual appliance architecture type: i386 (32-bit) or x86_64 (64-bit).
- **Configuration Volume** - Indicates the volume that stores the virtual appliance configuration and log files. Also displays the Elastic Block Store (EBS) volume ID and the total size of the volume.
- **Datastore Volume** - The EBS volume that stores the appliance data store. Some SteelHead-c models do not use a dedicated EBS volume for the data store; this information is not displayed for those models.

To view AWS appliance details

Prerequisite: The appliance must be hosted, licensed, and running on the AWS cloud service.

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to view.
3. Select Appliances.
4. Select the name of the appliance you want to view.

5. Select the AWS Details tab.

Viewing network controls and security groups

The Network Controls tab displays information about the appliance's network configuration. You can also configure custom rules and access security group information here.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

The Network Controls tab contains these items:

- **Elastic IP Address** - Displays the selected elastic IP address. Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An elastic IP address is associated with your account, not a particular instance, and you control that address until you choose to explicitly release it. The Riverbed Cloud Portal allows you to associate an elastic IP address with your SteelHead-c. If you choose to assign an elastic IP address to a SteelHead-c, it means that every time the SteelHead-c is started it will have that same IP address.
- **Public IP Address** - Displays the current public IP address of the appliance.
- **Public DNS Name** - Displays the public DNS name of the appliance.
- **Private IP Address** - Displays the current private (cloud vendor) IP address of the appliance.
- **Private DNS Name** - Displays the internal DNS name of the appliance.
- **Security Group Name** - Displays the name of the security group where the appliance belongs.
- **Discovery Service Rules**
  - **Protocol** - Displays the protocol used to communicate with the portal (TCP, UDP, or ICMP).
  - **From Port** - Displays the starting port number of a range of ports that peer nodes are allowed to access.
  - **To Port** - Displays the ending port number of a range of ports that peer nodes are allowed to access.
  - **Source** - Displays the IP address of the source node.
  - **Policy** - Indicates the rule policy for access to the appliance (Allow or Deny).
  - **Delete** - Deletes the Discovery Service Rule.
- **Custom Rules** - This section contains the same information fields as Discovery Service Rules.

To view Network Controls

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to view.
3. Select Appliances.
4. Select the name of the appliance you want to view.
5. Select the Network Controls tab.

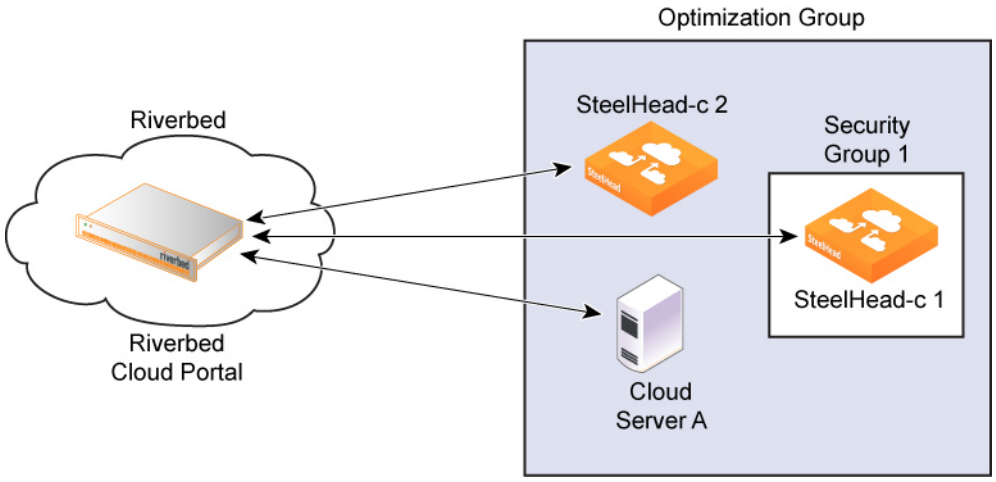
Configuring security groups

Correctly configured security groups are critical for an appliance in an optimization group to discover and optimize with its peers. The Riverbed Cloud Portal automates many steps in the security group configuration.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

For example, consider a configuration in which SteelHead-c 1, SteelHead-c 2, and Cloud Server A are members (nodes) of the same optimization group. The Riverbed Cloud Portal automatically creates a security group (Security Group 1) when SteelHead-c 1 is provisioned.

Figure 2-1. Security groups example



Initially, Security Group 1 does not let SteelHead-c 2 or Cloud Server A access SteelHead-c 1. However, after each node in the optimization group communicates with the Riverbed Cloud Portal and transmits its IP address, the portal automatically adds rules, called *discovery service rules,* to Security Group 1 so that the group allows access to SteelHead-c 1 from the node.

To complete the configuration, you must also add your own rules, called *custom rules,* because:

- You can configure and manage a SteelHead-c only if its security group allows connections from outside AWS on ports 22, 80, and 443.
- SteelHeads outside the AWS cloud must access ports 7800 and 7810 of the SteelHead-c for AWS to optimize connections to it.

Custom rules are not added to the security group for the Discovery Service and are not tracked by the Riverbed Cloud Portal.

The Riverbed Cloud Portal ensures that discovery service rules are automatically added to the security group whenever you restart the appliance. Even if you delete a Discovery Service Rule using a third-party tool such as the AWS user interface, the portal adds it back when you restart the appliance.

To remove a Discovery Service Rule, you must delete it from the Riverbed Cloud Portal by clicking **delete** in the Discovery Service Rule table.

You can add or delete custom rules through the Riverbed Cloud Portal, which adds or deletes the rules from the security group immediately. But if you subsequently delete a Custom Rule from the security group using a third-party tool, the Riverbed Cloud Portal does not ensure that the rule is reapplied when you start the appliance. The custom rules table simply reflects what is currently configured for the security group in the Amazon cloud at the time you visit the page on the Riverbed Cloud Portal.

For optimization to work, you must add rules to the Cloud Server security group to allow traffic from the SteelHead-c to reach the server TCP ports used by the application you want to optimize.

When the Discovery Agent is installed on the server, you must enable access to the UDP source port 7801 and destination port 7801 from the SteelHead-c on the server's security group.

Adding custom rules for security groups

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

To add a custom rule

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance for which you want to add a custom rule.
3. Select Appliances.
4. Select the name of the appliance for which you want to add a custom rule.
5. Select the Network Controls tab.
6. Click **Add Custom Rule**.
7. In the Add Custom Rule dialog box, complete these items:
   - **Protocol** - Select a protocol for communication with the portal (TCP, UDP, or ICMP).
   - **From Port** - Specify the starting port number for a range of ports on the appliance that peer nodes are allowed to access.
   - **To Port** - Specify the ending port number of a range of ports on the appliance that peer nodes are allowed to access.
   - **Source** - Click **Get My Host Address** to enter IP address of the virtual machine hosting the appliance.
8. Click **Add** to add the rule.

Viewing the AWS console

The AWS Console page displays the output of the virtual serial console connected to the EC2 instance hosting the appliance.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

To view the AWS console

1. In the Cloud Appliances tab on the Riverbed Cloud Portal, select Appliances and select the name of the appliance in the Appliances page to display the Appliance Summary page.
2. Select the AWS Console tab to display the output of the virtual serial console connected to the EC2 instance.

Viewing the event log for an appliance

The Event Log page displays this information for each message listed in the log:

- **ID** - Displays the serial number of the event.
- **Timestamp** - Displays the date and time when the event occurred.
- **IP Address** - Displays the IP address of the client machine that initiated the action. In NAT environments, this address might be network address translated.
- **User** - Displays the username of the entity that performed the action.
- **Log Level** - Indicates the severity level of the event.
  - **Critical** - Indicates the conditions that affect the functionality of the appliance.
  - **Error** - Indicates the conditions that probably affect the functionality of the appliance.
  - **Warning** - Indicates the conditions that could affect the functionality of the appliance, such as authentication failures.
  - **Notice** - Indicates normal but significant conditions, such as a configuration change.
  - **Informational** - Displays informational messages that provide general information about system operations.
  - **Debug** - Displays messages that help you debug a system failure.
- **Message** - Displays the log message that describes the event.

To view the appliance event log

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to view.
3. Select Appliances.
4. Select the name of the appliance you want to view.
5. Select the Event Log tab.
6. Select a severity level. The log contains messages of severity levels up to and including the selected level.
7. Specify the maximum number of records to display on a page. The default value is 20.

Managing optimization groups

Optimization groups enable you to associate multiple appliances with an application server for load balancing. The Optimization Group page lists existing groups and enables you to add new groups. Select a group name to access additional properties of that group.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

These load-balancing policies are available:

- **Priority** - Selects a SteelHead-c for load balancing until its connection count exceeds the maximum limit and then moves on to the next available SteelHead-c. When the first SteelHead-c's load decreases below the maximum limit, it is available again. This is the default policy.
- **Round robin** - Selects a SteelHead-c and then another (using the round-robin policy) for load balancing. Use the round robin policy only if the connection rate is high and you need more than one SteelHead-c to handle the load.

Adding or deleting optimization groups

Optimization groups are relevant only to appliances on AWS.

To add an optimization group

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance for which you want to add an optimization group.
3. Select Optimization Groups.
4. Click **Add New Optimization Group**.
5. Enter a display name for the group.
6. Enter a description for the group.
7. Select a Load Balance Policy.
8. Click **Create**.

To delete an optimization group

1. In the Optimization Group page, select the name of the group you want to delete.
2. Select the Summary tab.
3. Click **Delete Group**.

Editing optimization groups

You can edit a group's display name, description, and load-balancing policy, and you can add appliances and application servers to the group. The Optimization Group Details page is organized into these tabs:

- **Summary** - Displays the name, description, and load-balancing policy.

- **Group Members** - Displays the appliances and servers associated with the group. Includes the public IP and the internal IP for each entity.
- **Event Log** - Displays log information.

To edit an optimization group

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to edit.
3. Select Optimization Groups.
4. Select the name of the group you want to edit.
5. Select the Summary tab.
6. Click **Modify Optimization Group**.
7. Edit the name, description, and load-balancing policy and click **Update**.

To add an appliance to the optimization group

1. In the Optimization Group Details page, select the Group Members tab.
2. Click **Add SteelHead**.
3. Select an appliance from the drop-down list.
4. Specify the priority in which the SteelHead-c should be selected for optimization. A larger numerical value signifies a higher priority.
5. Click **Add**.

To add a server to the optimization group

1. In the Optimization Group Details page, select the Group Members tab.
2. Click **Add Server**.
3. Select a server from the drop-down list.
4. Select the server type.
5. Click **Add**.

Viewing event log information for an optimization group

Event log entries include this information:

- **ID** - Displays the serial number of the event.
- **Timestamp** - Displays the date and time when the event occurred.
- **IP Address** - Displays the IP address of the client machine that initiated the action. In NAT environments, this address might be network address translated.
- **User** - Displays the username of the entity that performed the action.

- **Log Level** - Indicates the severity level of the event.
  - **Critical** - Indicates the conditions that affect the functionality of the appliance.
  - **Error** - Indicates the conditions that probably affect the functionality of the appliance.
  - **Warning** - Indicates the conditions that could affect the functionality of the appliance, such as authentication failures.
  - **Notice** - Indicates normal but significant conditions, such as a configuration change.
  - **Informational** - Displays informational messages that provide general information about system operations.
  - **Debug** - Displays messages that help you debug a system failure.
- **Message** - Displays a log message that describes the event.

To view the event log associated with the optimization group

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to view.
3. Select Optimization Groups.
4. Select the name of the group you want to view.
5. Select the Event Log tab.
6. Select a severity level. The log contains messages up to and including the selected level.

Adding or removing AWS credentials

The Amazon Web Services Credentials page enables you to manage your AWS account and to update your AWS security credentials.

To update AWS credentials

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company that contains the appliance you want to update.
3. Select Amazon Web Services Credentials.
4. Click **Update AWS Credentials** to display the Amazon Web Services Credentials dialog box.
5. Edit the AWS account number, access key ID, and secret access key.
6. Click **Update**.

Viewing the discovered appliances report

The Discovered Appliances report page displays the list of appliances deployed and operational.

Note: This feature is available to appliances provisioned through the portal to the AWS cloud platform.

The Discovered Appliances report page displays this information:

- **Group** - Indicates the optimization group with which the appliance is associated.
- **Name** - Displays the name of the discovered appliance.
- **Public IP address** - Displays the current public IP address of the discovered appliance.
- **Internal IP address** - Displays the current internal IP address of the discovered appliance. This a private network IP address and is reachable only by machines within the same private network. The private network is supplied by the cloud platform provider.
- **Type** - Indicates the type of appliance.

To view the discovered appliances report

1. Log in to the portal and select the Cloud Appliances tab.
2. If your user account is associated with multiple companies, select the company you want to view.
3. Click **Discovered Appliances**.

3

Using the Discovery Agent

This chapter describes how to use the Riverbed Discovery Agent. It contains these sections:

Overview of the Discovery Agent

The Discovery Agent is a software package that you download from the Riverbed Support site and install on the client or server in the cloud that is optimized.

In a server-side Discovery Agent deployment, when a client SteelHead connects to a server with Discovery Agent installed, the Discovery Agent redirects any autodiscovery probe request to SteelHead-c from its list. Then, the client SteelHead discovers and starts peering and optimizing with the server-side SteelHead-c. After the autodiscovery process completes, the connection is terminated locally with the SteelHeads without going over the WAN.

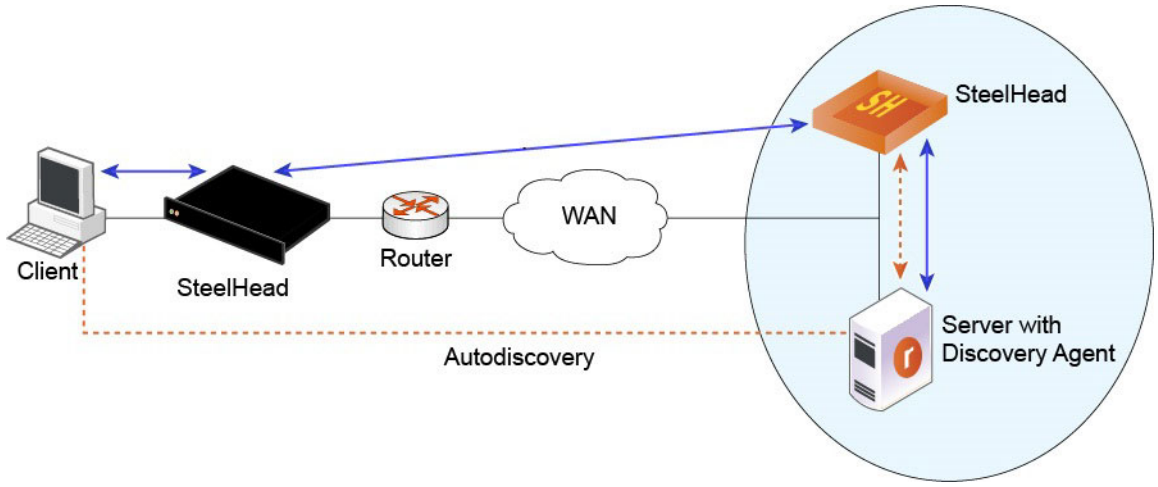
In a client-side Discovery Agent deployment, when a client with Discovery Agent installed connects to a server, the Discovery Agent redirects any TCP connection to a configured SteelHead-c from its list. Then, the client-side SteelHead-c sends an autodiscovery probe, discovers the remote SteelHead, and starts peering and optimizing with it.

The Discovery Agent provides these features:

- **Optimization** - Enables you to intercept (and optimize) inbound and outbound connections from the cloud.
- **Autodiscovery** - Enables SteelHeads to automatically find SteelHead-c virtual appliances and to optimize traffic through them. Autodiscovery relieves you of having to manually configure the SteelHeads with fixed target rules to find the remote SteelHead-c.

- **Transparency** - Enables the application on the server to continue to send and receive data from the same client IP address (as if there was no SteelHead) so that logging, reporting, or any feature that uses the IP address continues to work the same as before you configured the SteelHead.
- **Failure detection** - Detects SteelHead-c failures and connectivity issues to the SteelHead-c so that traffic can be passed through instead of being redirected to the failed SteelHead-c.
- **Load balancing** - Redirects all traffic to the SteelHead you select. If there are multiple SteelHeads in the group, the Discovery Agent uses the round-robin or priority load balancing method to select a SteelHead. When the primary SteelHead is unavailable or overloaded, it redirects all new connections to the next SteelHead on the list.

Figure 3-1. Discovery Agent overview



In Figure 3-1, the Discovery Agent enables the client-side SteelHead and the server-side SteelHead in the cloud to discover each other.

When the client connects to the server, the client-side SteelHead sends an autodiscovery probe to the server. The Discovery Agent redirects the autodiscovery probe to the SteelHead-c. The SteelHead-c sends an autodiscovery probe response back to the Discovery Agent, which sends it to the client-side SteelHead. After the client-side SteelHead receives the probe response, it starts peering with the SteelHead-c to intercept and optimize the connection from the client to the server.

The Discovery Agent running on the server machine provides transparency using network address translation (NAT) on the packets between the server-side SteelHead and the server to seem as if they are between the client and the server.

Similarly, it provides transparency for the client-side SteelHead in the cloud. The Discovery Agent translates outer connection packets, between the client-side SteelHead in the cloud and the client in the cloud, on the client machine to seem as if they are between the server and the client.

Discovery Agent requirements

The Discovery Agent requires this hardware:

- **Disk** - At least 160 MB on Windows and 120 MB on Linux. The Discovery Agent uses this space to store binary files, configuration files, and log files.

- **RAM** - At least 110 MB for 20000 optimized connections (the current limit).
- **CPU** - Depends on the throughput. For example, the Discovery Agent uses 5 to ten percent of a 2.66 GHz CPU to process 1 Gbps of optimized traffic.

Obtaining the client ID and client key from the Riverbed Cloud Portal

Before you install and configure the Discovery Agent, you must obtain the client ID and client key for the SteelHead-c (this does not apply to SteelHead-c virtual appliances for Azure and ESX/ESXi) or server from the Riverbed Cloud Portal. You must enter the client ID and client key either during installation or when you configure the Discovery Agent.

To obtain the client ID and client key

1. Log in to the Riverbed Cloud Portal.
2. Select the Cloud Appliances tab > Optimization Groups to display the Optimization Groups page.
3. Select a group name to display the Optimization Group Summary page for the group.
4. Select the Group Members tab to display the Group Members page.
5. If the group already contains the server or the SteelHead-c on which you want to configure the Discovery Agent, its name appears in the Name column. If not, add the server or SteelHead-c to the group.
6. Select the server or the SteelHead-c name in the Name column to display the Optimization Group Member Details page.

   When you add a SteelHead-c or a virtual server to the optimization group, the Riverbed Cloud Portal automatically generates a client ID and client key that identifies it.
7. Copy the client ID and client key displayed on this page into a text editor.

Installing the Discovery Agent

You can download the Discovery Agent from the Riverbed Cloud Portal and install it on a Windows or Linux server.

Installing the Discovery Agent on Windows servers

The Discovery Agent can be installed on these server operating systems:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2003 R2 - 32 bit and 64 bit

- Windows Server 2008 - 32 bit and 64 bit
- Windows client Windows 7 - 32 bit and 64 bit

Note: Riverbed does not support the Client Accelerator endpoint and the Discovery Agent on the same Windows computer.

To install the Discovery Agent on a Windows server

1. From the Riverbed Support site, choose Software & Documentation > SteelHead.
2. From the left navigation bar, click Cloud SteelHead.
3. In the Software tab, choose a version between 1.1.1 and 1.2.3.
4. Select the link for the Discovery Agent package you want and save the file.
5. Log in to the Windows server and double-click the executable file to display the Discovery Agent Installation Wizard.
6. Click **Next** to display the Discovery Agent Installation Warning message.

   When you install, uninstall, or upgrade the Discovery Agent on a Windows server, there is a temporary loss of network connectivity. Save your work and close any Windows program that might be affected by the disruption before you continue.
7. Click **Cancel** to quit the program, or click **Next** to continue with the installation.
8. Read and accept the license agreement and click **Next** to display the Riverbed Discovery Agent Configuration page.
9. Select the cloud type (**AWS** or **Other**) from the drop-down list.
10. If you select the cloud type **AWS**, click **Next** to display the Riverbed Portal Configuration page; go to Step 13 if you select the cloud type **Other**.
11. Optionally, enter the client ID and client key (for the SteelHead-c for AWS) that you obtain from the Riverbed Cloud Portal in the text boxes and click **Next**. This does not apply to SteelHead-c virtual appliances for Azure and ESX/ESXi.

    You can choose one of these actions:

    – Enter the client ID and client key in the installation wizard to automatically configure the Discovery Agent and have it communicate with the Riverbed Cloud Portal.

    – Click **Skip** and specify the client ID and client key when you configure the Discovery Agent

    – Not specify these values (if you are using the manual mode to configure the Discovery Agent).
12. Select Use Proxy to connect to Cloud Portal to specify a proxy IP address or hostname when connecting to the Riverbed Cloud Portal.
13. Select Use Local Portal to configure the Discovery Agent using the local portal mode and click **Next**.
14. Select a folder in which the Discovery Agent should be installed and click **Install**.
15. Click **Finish** to complete the installation.

The Discovery Agent starts automatically and the Riverbed icon appears on the system tray. A gray icon signifies that the Discovery Agent service is starting or has failed to start. If the Discovery Agent does not start, reboot the system and check that the Discovery Agent starts after rebooting.

Installing the Discovery Agent on Linux servers

You can download the Discovery Agent package from the Riverbed Cloud Portal.

Note: The README file in the Discovery Agent download package contains installation and configuration information.

The Discovery Agent supports the follows Linux servers:

- RedHat Linux (RHEL) 7
- CentOS 5.0, 5.2, 5.3, 5.4, 6.3, 7.3, and 7.5 - 32 bit and 64 bit
- Linux Ubuntu 8.04, 10.04, and 14.04 - 32 bit and 64 bit
- Linux Fedora (Fedora core 8) - 32 bit and 64 bit

To install the Discovery Agent on a Linux server

1. From the Riverbed Support site, select Software & Documentation.
2. In the Search text box, enter Discovery Agent and click the arrow icon.
3. Select the link for the Discovery Agent package you want and save the file.
4. Copy the downloaded tar file to the Linux server and log in to the server as the root user.
5. Uncompress the tar file and extract its contents by entering this command on the Linux command line:

   ```
   tar -zxvf <filename>.tar.gz
   ```

6. Follow the steps in the README file to install and configure the Discovery Agent on the Linux server.

Configuring the Discovery Agent

You configure the Discovery Agent using the Riverbed Cloud Portal.

To configure the Discovery Agent

1. Obtain the client ID and client key from the Riverbed Cloud Portal. For details, see "Obtaining the client ID and client key from the Riverbed Cloud Portal" on page 43.

   To associate a virtual server running the Discovery Agent with the SteelHead-c in the same optimization group, enter the client ID and client key manually using the Discovery Agent Windows user interface or the Linux configuration script.

   Ensure that you use the client ID and the client key that you copied from the Optimization Group Member Details page in the Riverbed Cloud Portal.

   The SteelHead-c and the virtual server use the client ID and client key to identify themselves when communicating with the Riverbed Cloud Portal. By default, the Discovery Agent establishes communication with the Riverbed Cloud Portal.

If you are using a different portal (than the Riverbed Cloud Portal), you must configure the Discovery Agent to communicate with your portal.

If you are not using a portal at all, configure the client ID and client key in the Discovery Agent. For details, see the online help in the Discovery Agent Windows interface or the README file on the Linux server.

2. To configure the Discovery Agent on your Linux server, see "Configuring the Discovery Agent on Linux servers" on page 46.
3. To configure the Discovery Agent on your Windows server, see "Configuring the Discovery Agent on Windows servers" on page 46.

Important: In a client-side Discovery Agent deployment, the Discovery Agent drops packets if the network interface has an MTU value set above 1500. By default, an AWS deployment sets the MTU of network interfaces in SteelHead-c and the Discovery Agent to 9001. Using these default values can result in packet loss and unoptimized traffic. For details and steps to change the MTU value, see KB S33702.

Configuring the Discovery Agent on Linux servers

Follow the instructions in the Linux Discovery Agent README file (which you download from the Riverbed Cloud Portal) to configure the Discovery Agent on a Linux server.

Configuring the Discovery Agent on Windows servers

You can choose the Riverbed Cloud Portal, manual configuration, or a local portal as the discovery mechanism. To configure the Discovery Agent on Windows, update the Riverbed Cloud Portal or SteelHead settings based on the discovery mode you choose, as follows:

- "Configuring the Discovery Agent using the Riverbed Cloud Portal" on page 46
- "Configuring the Discovery Agent manually" on page 47
- "Configuring the Discovery Agent using the local portal mode" on page 48

Configuring the Discovery Agent using the Riverbed Cloud Portal

For SteelHead-c for AWS virtual appliances, you can configure the Discovery Agent using the Riverbed Cloud Portal.

To configure the Discovery Agent using the Riverbed Cloud Portal

1. Log in to your Windows server and double-click the Riverbed Discovery Agent icon in the system tray.
2. Select the Settings tab in the Discovery Agent to display the Settings page.
3. Click **Configure** to display the Configure Discovery Agent page.

   The default Use Riverbed Portal mode is automatically selected.

4. Click **Edit** to display the Riverbed Portal Configuration dialog box.
5. Specify these parameters in the Riverbed Portal Configuration dialog box.

Parameter	Description
Client ID	Copy and paste the client ID from the Riverbed Cloud Portal. For details, see "Obtaining the client ID and client key from the Riverbed Cloud Portal" on page 43.
Client Key	Copy and paste the client key from the Riverbed Cloud Portal. For details, see "Obtaining the client ID and client key from the Riverbed Cloud Portal" on page 43.
Configure HTTP Proxy	Select the check box to make the fields below editable and configure an HTTP proxy server to connect to the Riverbed Cloud Portal.
Proxy Hostname or IP	Enter the proxy server hostname or IP address.
Proxy Port	Enter the port number of the proxy server.

6. Click **OK** to apply your changes or **Cancel** to cancel the operation and close the dialog box.

Configuring the Discovery Agent manually

If you are using the Discovery Agent with SteelHead-c virtual appliances for Azure and ESX/ESXi, you must manually configure the Discovery Agent.

To configure the Discovery Agent manually

1. Log in to your Windows server and double-click the Riverbed Discovery Agent icon in the system tray.
2. Select the Settings tab in the Discovery Agent to display the Settings page.
3. Click **Configure** to display the Configure Discovery Agent page.
4. Click **Manual** to display the Manual Configuration page.
5. Choose a load-balancing policy from the drop-down list:
   - **Priority** - Selects a SteelHead-c for load balancing until its connection count exceeds the maximum and then moves on to the next available SteelHead-c. When the load of the first SteelHead-c decreases below the maximum, it is available again. This policy is the default setting.
   - **Round robin** - Selects a SteelHead-c and then another (using the round-robin policy) for load balancing. Use the Round Robin policy only if the connection rate is high and you need more than one SteelHead-c to handle the load.
6. Either specify a SteelHead-c to connect to the Discovery Agent or click **New** to add a new SteelHead-c to connect to the Discovery Agent.
7. Enter the IP address of the SteelHead-c and click **OK**.

   The SteelHead-c is added to the SteelHead List in the Configuration Dialog box.

Use the arrows to adjust the priority in which the Discovery Agent connects to the SteelHead-c virtual appliances.

Configuring the Discovery Agent using the local portal mode

If you are using your own local portal and not the Riverbed Cloud Portal, you can configure the Discovery Agent using the local portal mode for SteelHead-c for AWS virtual appliances.

1. Log in to your Windows server and double-click the Riverbed Discovery Agent icon in the system tray.
2. Select the Settings tab in the Discovery Agent to display the Settings page.
3. Click **Configure** to display the Configure Discovery Agent page.
4. Click **Configure Local Portal** to display the Local Portal Configuration page.

   The Local Portal Configuration page displays the portal hostname or IP address, client ID, and client key, and proxy settings that you specified in the installation wizard.
5. Click **Edit** to display the Riverbed Portal Configuration dialog box.
6. Specify these parameters in the Riverbed Portal Configuration dialog box.

Parameter	Description
Client ID	Specify the client ID of your SteelHead-c or server on which you want to configure the Discovery Agent.
Client Key	Specify the client key of your SteelHead-c or server on which you want to configure the Discovery Agent.
Configure HTTP Proxy	Select the check box to make the fields below editable and configure an HTTP proxy server to connect to the portal.
Proxy Hostname or IP	Enter the proxy server hostname or IP address.
Proxy Port	Enter the port number of the proxy server.

7. Click **OK** to apply your changes or **Cancel** to cancel the operation and close the dialog box.

Configuring transparency modes

You configure the Discovery Agent transparency modes in the Configure > Optimization > General Service Settings in the In-Path Settings section (Enable Agent-Intercept option). For details, see the *SteelHead User Guide*.

The Discovery Agent provides three transparency modes for connections between the client or server and the corresponding SteelHead. You configure the transparency mode you choose in the SteelHead-c and it is transmitted to the Discovery Agent.

The transparency mode you select does not affect the packets of the connection on the network. When you view the packets on the network, they are still addressed between the client or the server and the SteelHead. The Discovery Agent performs network address translation (NAT) for these packets before sending them up the stack. Therefore, the transparency mode affects what IP address is visible to the application and the client or server machine's network stack.

Select a transparency mode:

- **Safe transparent** - If the client is behind a NAT device, the client connection to the application server is nontransparent—the application server detects the connection as a connection from the SteelHead-c IP address, not the client IP address. All connections from a client that is not behind a NAT device are transparent, which means that the server detects the connections from the client IP address instead of the SteelHead-c IP address.
- **Restricted transparent** - All client connections are transparent with these restrictions:
  - If the client connection is from a NAT network, the application server detects the private IP address of the client.
  - You can use this mode only if there is no conflict between the private IP address ranges (there are no duplicate IP addresses) and ports.

  This mode is the default setting.
- **Nontransparent** - All client connections are nontransparent—the application server detects the connections from the server-side SteelHead IP address, not the client IP address. We recommend that you use this mode only if you cannot use one of the other two modes.

Enabling optimization using the Discovery Agent

To enable optimization using the Discovery Agent, connect to the SteelHead-c CLI and enter these commands to enable the agent-intercept mode:

```
enable
configure terminal
in-path agent-intercept enable
in-path enable
```

Note: The optimized application server with Discovery Agent installed on it must connect to the primary interfaces on the SteelHead-c virtual appliance.

4

Using SteelHead-c for VMware ESX/ESXi

This chapter describes how to use SteelHead-c virtual appliances for ESX/ESXi. It includes these sections:

Overview of SteelHead-c virtual appliances for ESX/ESXi

VMware ESX/ESXi is hypervisor software that enables the creation and management of virtual machines. Virtual machines act as hosts for SteelHead-c virtual appliances. Installing a SteelHead-c image on a virtual machine is much like installing RiOS software on physical Riverbed hardware.

The Riverbed Cloud Portal supports licensing and basic status reporting for ESX/ESXi-hosted SteelHead-c virtual appliances.

SteelHead-c for ESX/ESXi Limitations

SteelHead-c for ESX/ESXi has these limitations:

- **Provisioning** - You must provision ESX resources manually. You can use any provisioning tool provided by VMware-based cloud providers such as vSphere.
- **Virtual machine operations** - You must use the cloud provider toolset (such as the vSphere tools or Cloud Console) to start, stop, pause, and resume the virtual machine.
- **Discovery** - The portal does not provide discovery services for SteelHead-c, because a SteelHead-c deployed on an ESX cloud requires static IP addresses to work correctly.

SteelHead-c for ESX/ESXi requirements

This table describes the SteelHead-c for ESX/ESXi requirements.

Component	Requirement
Supported vSphere releases	4.0 and later.
Provisioning	OVA package deployment.
License management	Connectivity between SteelHead-c and the SteelHead-c (TCP port 80 connection to cloudportal.riverbed.com).
Virtual hardware	64 bit only. vCPU: One 1.2 vCPU to four 2-GHz vCPUs Reserved RAM: 2 GB to 6 GB Disk capacity: 470 GB
IP addressing	Static, when you use the Discovery Agent. SteelHead-c does not support accessing client-side SteelHeads with overlapping IP addresses.
Firewall setting	Disabled (if the rules exclude the TCP option) or modified target rules. Enable port 80 to access cloudportal.riverbed.com. SteelHead-c supports only traffic in clear text or SSL encryption. It does not support IPsec encryption.
Discovery Agent	Supported Windows versions: Windows 2003, Windows 2008 R1, and Windows 7. Supported Linux versions: CentOS 5.0, 5.2, 5.3, 5.4, 6.3, 7.3, and 7.5 - 32 bit and 64 bit, Linux Ubuntu 8.04 and 10.04, and RedHat 4 and 5.
Server VM limitations	Only supports server VMs with a single virtual NIC.

Basic steps to deploy a SteelHead-c for ESX/ESXi

This table lists the deployment tasks.

Task	Reference
1. Install the SteelHead-c using VMware vSphere.	"Installing the SteelHead-c virtual appliance for ESX/ESXi" on page 53
2. Configure the resources that the ESX server will be granting the SteelHead-c.	"Configuring ESX resources" on page 55
3. Complete the initial configuration of the SteelHead-c.	"Completing the initial configuration" on page 56
4. Obtain the one-time token from the Riverbed Cloud Portal.	"Licensing SteelHead-c virtual appliances" on page 16
5. Apply the one-time token to the SteelHead-c.	"Licensing SteelHead-c virtual appliances" on page 16

Task	Reference
6. Use the Riverbed Cloud Portal to monitor the SteelHead-c.	"Using the Riverbed Cloud Portal" on page 21
7. If you decide not to use the Discovery Agent, go to Step 9.	
8. Install and manually configure the Discovery Agent on the server. You cannot use the Riverbed Cloud Portal to configure the Discovery Agent for SteelHead-c. You must use the manual mode.	"Using the Discovery Agent" on page 41
9. If you are not using the Discovery Agent, configure the client-side SteelHead in-path rules to point to the SteelHead-c for server.	*SteelHead User Guide*
10. If your network is NATed, go to Step 11.	
11. If you are not using the Discovery Agent, configure the SteelHead-c for public or private IP address mapping.	

Installing the SteelHead-c virtual appliance for ESX/ESXi

Riverbed provides the SteelHead-c for ESX/ESXi as an image that contains the VMX and VMDK files necessary to create the virtual machine.

The SteelHead-c image is an installable Open Virtual Appliance (OVA) package. OVA is a platform-independent, efficient, extensible, and open packaging distribution format. The OVA package provides a complete specification of the SteelHead-c, including its virtual disks, CPU, memory, networking, and storage. To install a SteelHead-c model other than the base model, first install the base model and then upgrade it to a higher model.

The OVA is a compressed package that quickly creates a virtual machine with predefined settings.

To obtain the OVA package, log in to your customer account at https://support.riverbed.com.

Each package contains predefined hardware requirements and configuration for the base model SteelHead-c. Do not open or modify any of the files in the package. The package files take up several gigabytes of disk space (the package itself is less than 1 GB).

Note: A SteelHead-c for ESX/ESXi requires a 440-GB virtual disk. This size is bigger than the 256 GB maximum virtual disk size deployable in an ESX cluster when you use the Virtual Machine File System (VMFS) default block size of 1 MB. Therefore, before installing a SteelHead-c, ensure that the target data store (VMFS) has a block size greater than 1 MB. This limitation is not valid if you use Network File System (NFS).

To install a SteelHead-c for ESX/ESXi

1. Obtain the VM package from https://support.riverbed.com and download it locally.
2. Extract the contents of the OVA package using the **tar -xvf** command or a freeware application such as 7-zip.

3. Open VMware vSphere, enter the hostname or host IP address, enter your username and password, and click **Login**.
4. Choose File > Deploy OVF template.
5. Select Deploy from file, click **Browse**, select the OVA file, and click **Open**.
6. Click **Next** to display the OVF Template Details page.
7. Verify that the OVA file is the one you want to deploy, and click **Next** to display the Name and Location page.
8. Enter a name for the virtual machine.
9. Click **Next** to display the Datastore page.
10. Select a data store in which to store the virtual machine and its virtual disk files. Here are some tips about the data store:
    - The standard installation puts both VMDKs on a single data store.
    - The data store holds the virtual machine files and is not used for the Riverbed Optimization System (RiOS) data store.
    - Make sure the data store you select has enough capacity for the OVA package to install.
    - We recommend that you put the larger VMDK containing the RiOS data store on the fastest available data store. The data store should have enough room to expand to the required size of the SteelHead-c model.
    - The smaller VMDK containing the management system can be installed on any data store type.
    - Do not share host physical disks (such as SCSI or SATA disks) between VMs. Select an unshared disk for the data store disk.
    - Do not delete data store disk 1 (DS1).
11. Click **Next** to display the Disk Format page.
12. On the Disk Format page, select Thick provisioned format.

    Thick provisioning preallocates all storage.
13. Click **Next** to display the Network Mapping page.
14. Select the destination network name and choose a network from the drop-down list to map the source network to a destination network.

    Ensure that the LAN and WAN interfaces (NIC3 and NIC4 in ESXi) are not connected to the same virtual switch. Otherwise, the system displays the error message:

    ```
    Failed to apply configuration change(s) Internal error: module commit apply function of the module rbt.
    ```

    Note: Make sure that you map each source network to a unique destination network. If a source network is mapped to the same destination as another source, an error message appears. Mapping source networks to the same destination network can create a loop in the system and might make your ESX host unreachable.
15. Click **Next** to display the Ready to Complete page.
16. Verify the deployment settings and click **Finish**.

A dialog box shows the amount of time it will take for the deployment to complete.

When the deployment finishes, a dialog box tells you that the deployment was successful.

17. Click **Close**.

    The new virtual machine appears under the hostname or host IP address to the virtual machine inventory.

Configuring ESX resources

Before you power on the SteelHead-c, you must configure the resources that the ESX server will be granting the SteelHead-c.

To configure ESX resources

1. Right-click the virtual machine you created and click **Edit Settings** to display the Virtual Machine Properties page.
2. Select the Hardware tab and click **Memory** in the Hardware column.
3. Increase the memory size to at least the minimum required by the model you want to use.
4. Click **OK** to save your changes.
5. Click **Edit Settings** and select the Hardware tab. Click **CPUs** in the Hardware column.
6. Set the number of virtual processors to at least the minimum required for the model you want to use.
7. Click **OK** to save your changes.
8. Click **Edit Settings**, select the Resources tab, and select CPU.
9. Under Resource Allocation, change the Reservation to at least the minimum required for the model you want to use.
10. Click **OK** to save your changes.
11. Select the virtual machine and choose Power > Power On.
12. Select the Console tab.

    The SteelHead-c starts and the login prompt appears.

13. Log in to the SteelHead-c using the default login **admin** and the default password **password**.

Completing the initial configuration

This section describes how to complete the initial configuration of the SteelHead-c for ESX/ESXi.

To configure the SteelHead-c for ESX/ESXi

1. After you log in to the SteelHead-c as administrator, the system prompts you to start the configuration wizard.

```
Enter yes at the system prompt:
Configuration wizard.
Do you want to use the wizard for initial configuration? yes
```

Note: Press Enter to enter the default value. If you mistakenly answer **no**, you can start the configuration wizard by entering **configuration jump-start** at the system prompt.

Note: Press ? for help. Press Ctrl+B to go back to the previous step.

2. Complete the configuration wizard steps on the client-side SteelHead-c as described in this table.

Wizard prompt	Description	Example
Step 1: Hostname?	Enter the hostname for the SteelHead.	Step 1: `Hostname? amnesiac`
Step 2: Use DHCP on the primary interface?	You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead-c. We recommend that you do not set DHCP. The default value is **no**.	Step 2: `Use DHCP? no`
Step 3: Primary IP address?	Enter the IP address for the SteelHead-c.	Step 3: `Primary IP address? 10.10.10.6`
Step 4: Netmask?	Enter the netmask address.	Step 4: `Netmask? 255.255.0.0`
Step 5: Default gateway?	Enter the default gateway for the SteelHead.	Step 5: `Default gateway? 10.0.0.1`
Step 6: Primary DNS server?	Enter the primary DNS server IP address.	Step 6: `Primary DNS server? 10.0.0.2`
Step 7: Domain name?	Enter the domain name for the network in which the SteelHead-c is to reside. If you set a domain name, you can enter hostnames in the system without the domain name.	Step 7: `Domain name? example.com`
Step 8: Admin password?	We strongly recommend that you change the default administrator password. The password must be a minimum of six characters.	Step 8: `Admin password? xxxyyy`
Step 9: SMTP server?	Enter the SMTP server name. External DNS and external access for SMTP traffic is required for email notification of events and failures to function. **Note:** Make sure that you provide a valid SMTP server to ensure email notifications for events and failures.	Step 9: `SMTP server? natoma`
Step 10: Notification email address?	Enter a valid email address to which notification of events and failures are to be sent.	Step 10: `Notification email address? example@example.com`

Wizard prompt	Description	Example
Step 11: Set the primary interface speed?	Enter the speed on the primary interface (the SteelHead-c). Make sure that this value matches the settings on your router or switch. The default value is **auto**.	Step 11: `Set the primary interface speed? [auto] auto`
Step 12: Set the primary interface duplex?	Enter the duplex mode on the primary interface. Make sure that this value matches the settings on your router or switch. The default value is **auto**.	Step 12: `Set the primary interface duplex? [auto] auto`

3. The system confirms your settings:

```
   You have entered the following information:
   1. Hostname: amnesiac
   2. Use DHCP on primary interface: no
   3. Primary IP address: 10.10.10.6
   4. Netmask: 255.255.0.0
   5. Default gateway: 10.0.0.1
   6. Primary DNS server: 10.0.0.2
   7. Domain name: example.com
   8. Admin password: xxxyyy
   9. SMTP server: natoma
   10. Notification email address: example@example.com
   11. Set the primary interface speed: auto
   12. Set the primary interface duplex: auto
To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
Choice:
```

   The SteelHead-c configuration wizard automatically saves your configuration settings.

4. To log out of the system, enter this command at the system prompt:

```
amnesiac > exit
```

Logging in to the SteelHead-c Management Console

This section describes how to log in to the SteelHead-c Management Console. The Management Console makes managing the SteelHead-c simpler through a web browser interface.

You can connect to the SteelHead-c through any supported web browser. To connect to the SteelHead-c, you must know the hostname and domain, or the IP address, of the virtual appliance.

For first-time login, the default username is **admin** and the default password is **password**. If you specified administrator credentials at the time you created the virtual appliance instance, use those credentials.

Cookies and JavaScript must be enabled in your browser.

To log in to the management console

1. Enter the URL for the SteelHead-c in the location box of your browser:

```
<protocol>://<host>.<domain>
```

<protocol> is HTTP or HTTPS. The secure HTTPS uses the SSL protocol to ensure a secure environment. If you use HTTPS to connect, you are prompted to inspect and verify the SSL key.

<host> is the IP address or hostname you assigned to the SteelHead-c during the initial configuration. If your DNS server maps the IP address to a name, you can specify the DNS name.

<domain> is the full domain name for the SteelHead-c.

Note: Alternatively, you can specify the IP address instead of the host and domain.

The Management Console Login page appears.

2. In the Username text box, enter the user login: admin or monitor. The default login is admin.

   Users with administrator privileges can configure and administer the SteelHead. Users with monitor privileges can view connected SteelHeads and reports. A monitor user cannot make configuration changes, modify private keys, view logs, or manage cryptographic modules in the system.

3. In the Password text box, enter the default password or the one you assigned when you created the virtual appliance instance.

4. Click **Log In** to display the Home page.

5

Using SteelHead-c for Microsoft Azure

This chapter describes how to use SteelHead-c virtual appliances for Microsoft Azure. It includes these sections:

Before using your SteelHead-c for Azure

This information will help you make the most of your SteelHead-c for Azure:

- In Azure, NAT rules to a virtual machine are very aggressive. These rules can cause frequent failures of the inner connection pool. To avoid this issue, configure your client-side SteelHead appliances that pair with a SteelHead-c for Azure so that their inner keepalive interval is 30 seconds or less.

  ```
  cfe (config) # protocol connection addr <azure-sh-ip> inner-intvl 30 oob-intvl 30
  ```

- License your SteelHead-c for Azure after you create it.
- Out-of-path deployment using fixed-target rules and agent-intercept deployment using Discovery Agent are supported.

Prerequisites for installing SteelHead-c in Azure

Before you install the virtual appliance, ensure that these prerequisites are met:

- You have access credentials to a Microsoft Azure account that allow you to create resources in the region and virtual networks where you want to deploy SteelHead-c.
- You have obtained a one-time token from the Riverbed Cloud Portal to license your SteelHead-c. Access the portal at https://cloudportal.riverbed.com.
- The SteelHead-c instance must have continuous SSL/TLS (TCP port 443) access to the Riverbed Cloud Portal in order to verify that the license is active. If the SteelHead-c cannot contact the Riverbed Cloud Portal, it will stop optimization and will by-pass connections until it can verify the license again. For enhanced security, configure a TCP proxy in the virtual machine's Networking > Host Settings.

Installing a SteelHead-c on an Azure virtual machine

This section provides instructions for installing a SteelHead-c virtual appliance on an Azure Hyper-V virtual machine using the default mode (Create a virtual machine wizard.) The programmatic deployment mode is not covered in this document. See the Azure documentation for details about that mode.

Note: The default deployment mode in Microsoft Azure has changed from Classic (programmatic) to Resource Manager (wizard.) SteelHead-c can be deployed in either mode; however, resources deployed through different deployment modes cannot interoperate. Select the deployment mode that matches the rest of your infrastructure in Azure.

Important: For RiOS 9.12.0 and later, the default password is **password** regardless of the value you specified while provisioning or creating the Cloud SteelHead from the Azure marketplace image. You can change the password after you provision the system using the Cloud SteelHead UI or CLI. (This caveat is only applicable for Azure Cloud SteelHeads launched from Azure marketplace.)

To install using the Microsoft Azure portal

1. Log in to the Microsoft Azure portal and navigate to your dashboard.
2. Click **Create a resource**.

   The New page appears. On this page you can find Marketplace items by search, type, or popularity.
3. Search for keywords: Riverbed SteelHead.
4. Select an image from the available options.
5. In the image details pane, near the bottom, click **Create**.

   The Create virtual machine wizard displays.

   If you want to deploy the SteelHead-c using Azure's programmatic mode, select Want to deploy programmatically? Get started ->. See the note at the beginning of this section, "Installing a SteelHead-c on an Azure virtual machine" on page 62.
6. In the Basics section of the wizard, enter this information:

   Project Details

   – Select a subscription model.

   – Select a resource group, or click Create new if you want to place the virtual appliance you are creating into a new resource group.

   Instance Details

   – Enter a display name for the virtual appliance.

   – Select the region where you want to deploy the virtual appliance.

   – Specify Availability options.

   – Select the image you want to install on the virtual machine. The default is the item you selected in Step 4 on page 62.

- Select a size for the virtual machine. The size determines the maximum amount of compute resources (CPU, RAM memory) available to the virtual machine. See "SteelHead-c models and required virtual machine resources" on page 11 to find the amount of resources required to run the SteelHead-c model you want to deploy.

Administrator Account

Note: The account that you create in this step is not used. However, use the password you specify here along with the username **admin** for first-time login. After initial login, you can change your credentials at any time.

- Specify how administrators will authenticate when logging in to the Hyper-V virtual machine.

7. Click **Next : Disks >** to advance to the wizard's Disks tab.
8. Under Disk Options, select a disk type for the SteelHead-c virtual appliance's operating system (RiOS).
9. Optionally enable Ultra SSD compatibility.
10. Under Data Disks, create and attach a disk or attach an existing disk to serve as the SteelHead-c virtual appliance's data store. See "SteelHead-c models and required virtual machine resources" on page 11 to find the minimum disk size required to run your model SteelHead-c.

    If you do not already have a data store disk, select Create and Attach a new disk.

    - In the Create a new disk page, specify these settings: disk type, display name, size in gigabytes (GB), source type.
    - Click **OK**. A virtual disk with your settings is allocated. The Create a new disk page closes and you are returned to the wizard's Disk tab. The newly allocated disk is listed under Data Disks.
    - Select Read/Write from the Host Caching drop-down menu corresponding to the newly allocated disk.

    If you already have a data store disk, select Attach an existing disk.

    - A row is added to the Data Disks table.
    - Select a disk from the Name drop-down menu.
    - Select Read/Write from the Host Caching drop-down menu corresponding to the newly added disk.
11. Under the Advanced section, accept the default values.
12. Click **Next : Networking >** to advance to the wizard's Networking tab.
13. Select the network and subnet where you want to deploy the SteelHead-c from the Virtual network and Subnet drop-down menus.

    If you have not already configured a virtual network and a subnet, click **Create new** to display the Create new network page. Enter an address space for the new virtual network, create subnets, and then click **OK**. See the Microsoft Azure help for assistance.
14. Optionally select a public IP address from the Public IP drop-down menu. A public IP enables you to communicate with the virtual appliance from outside the virtual network.

If you want to use a public IP but none exist, click **Create new** to display the Create public IP address page. Enter a display name for the new IP address, specify SKU and assignment, and then click **OK**. See the Microsoft Azure help for assistance.

15. NIC network security group is **Advanced**. NIC network security group settings are preconfigured.
16. Select a network security group from the Configure network security group drop-down menu.

    If no security groups exist, click **Create new** to display the Create network security group page, specify Inbound rules and Outbound rules, and then click **OK**. See the Microsoft Azure help for assistance.
17. Accelerated networking is **Off**. Accelerated networking is not supported.
18. Under Load Balancing, select **No**.
19. Click **Next : Management >** to advance to the wizard's Management tab.
20. Optionally configure the settings under Monitoring, Identity, and Auto-Shutdown to your liking.
21. Click **Next : Guest config >** to advance to the wizard's Guest config tab.
22. Click **Next : Tags >** to advance to the wizard's Tags tab.
23. Optionally add tags.
24. Click **Next : Review + create >** to advance to the wizard's Review + create tab.
25. Review your selections and then click **Create**.
26. License your virtual appliance. See "Licensing SteelHead-c virtual appliances" on page 16.

6

Using SteelHead-c for Oracle Cloud Infrastructure

This chapter describes how to use SteelHead-c virtual appliances for Oracle Cloud Infrastructure. It includes these sections:

Out-of-path deployment using fixed-target rules and agent-intercept deployment using Discovery Agent are supported.

Prerequisites for installing SteelHead-c in Oracle Cloud Infrastructure

Before you install the virtual appliance, ensure that these prerequisites are met:

- You have access credentials to an Oracle Cloud Infrastructure account that allow you to create resources in the region and virtual networks where you want to deploy SteelHead-c.
- You have obtained a one-time token from the Riverbed Cloud Portal to license your SteelHead-c. Access the portal at https://cloudportal.riverbed.com.
- The SteelHead-c instance must have continuous SSL/TLS (TCP port 443) access to the Riverbed Cloud Portal in order to verify that the license is active. If the SteelHead-c cannot contact the Riverbed Cloud Portal, it will stop optimization and will by-pass connections until it can verify the license again. For enhanced security, configure a TCP proxy in the virtual machine's Networking > Host Settings.

Installing a SteelHead-c on an Oracle Cloud Infrastructure virtual machine

This section provides instructions for installing a SteelHead-c virtual appliance on an Oracle Cloud Infrastructure VM. You will first provision the virtual appliance and then create and attach a block volume to serve as the data store disk for the virtual appliance.

To install using the Oracle Cloud Infrastructure portal

1. Log in to the Oracle Cloud Infrastructure portal and navigate to your dashboard.
2. Choose Menu > Compute > Partner Images.

3. Choose the compartment where you want to deploy the virtual appliance from the List Scope > Compartment menu.
4. Find the Riverbed SteelHead-c image in the Images section. You can sort the list of images by display name if you need help finding it.
5. Click the display name of the image.

   The Image Details page appears.
6. Click **Create Instance**.

   The Create Compute Instance page appears.
7. Enter a display name for the instance.
8. Select an availability domain for the instance.
9. Select Virtual Machine for the instance type.
10. Select an instance shape appropriate to the SteelHead-c model you want to run. See "SteelHead-c models and required virtual machine resources" on page 11.
11. Accept the default values for the remaining items.
12. Click **Create**.

    The Instance Details page appears and displays the progress of the provisioning process. After the process completes, create a block volume to the instance.

To create a block volume for the virtual appliance data store

1. Choose Menu > Block Storage > Block Volume.
2. Choose the same compartment where you deployed the virtual appliance from the List Scope > Compartment menu.
3. Select the same availability zone where you deployed the virtual appliance from the Filters > Availability Domains options.
4. Click **Create Block Volume**.

   The Create Block Volume dialog box appears.
5. Choose the same compartment where you deployed the virtual appliance from the Create in Compartment menu.
6. Enter a display name for the volume.
7. Select the same availability zone where you deployed the virtual appliance from the Availability Domain menu.
8. Enter a size in gigabytes (GB) for the volume that is appropriate for the SteelHead-c model you want to run. See "SteelHead-c models and required virtual machine resources" on page 11.
9. Optionally, select a backup policy.
10. Optionally, define and add tags.

11. Select View Detail Page After This Resource Is Created.
12. Click **Create Block Volume**.

    The Block Volume Details page appears and displays the progress of the provisioning process. After the process completes, attach the block volume to the instance.

To attach the block volume to the virtual appliance

1. Choose Menu > Compute > Instances and find your SteelHead-c instance.
2. Click the display name of the instance to view its details.
3. In the Resources section on the Instance Details page, click Attached Block Volumes.
4. Click Attach Block Volume.

   The Attach Block Volume dialog box appears.
5. Select Paravirtualized under Choose how you want to attach your block volume. You must select Paravirtualized; do not select iSCSI.
6. Choose the same compartment where you deployed the virtual appliance from the Block Volume Compartment menu.
7. Select the volume you created in the previous procedure, "To create a block volume for the virtual appliance data store" on page 66.
8. Select read/write under Access to enable the virtual appliance to write to and read from the block volume.
9. Click **Attach**.

   The Instance Details page is updated with a new entry for the volume under the Attached Block Volumes section. Details about the volume, including the progress of the attachment process appear in that entry.

After your SteelHead-c virtual appliance is installed, you can license your virtual appliance and then change the default administrator password. See "Licensing SteelHead-c virtual appliances" on page 16.

7

Using Amazon Virtual Private Cloud

This chapter describes the Amazon Virtual Private Cloud (VPC). It includes these sections:

About Amazon VPC

Amazon VPC enables you to create a virtual topology (including subnets and route tables) for your Amazon Elastic Compute Cloud (EC2) resources. It enables you to create an isolated portion of the AWS cloud (a VPC) and launch Amazon EC2 instances that have private (RFC 1918) addresses in the range of your choice (for example, 10.0.0.0/16).

Amazon VPC provides various levels of security. At the highest level, the VPC enables you to connect to a private network through a VPN tunnel. You can also access the private subnet through an Internet gateway that enables traffic to flow between the Internet and all the instances in your VPC.

You can also configure a VPC to be in-between, with both a VPN gateway and an Internet gateway to enable some instances to receive Internet traffic (for example, web servers), whereas others could remain unexposed (for example, database servers).

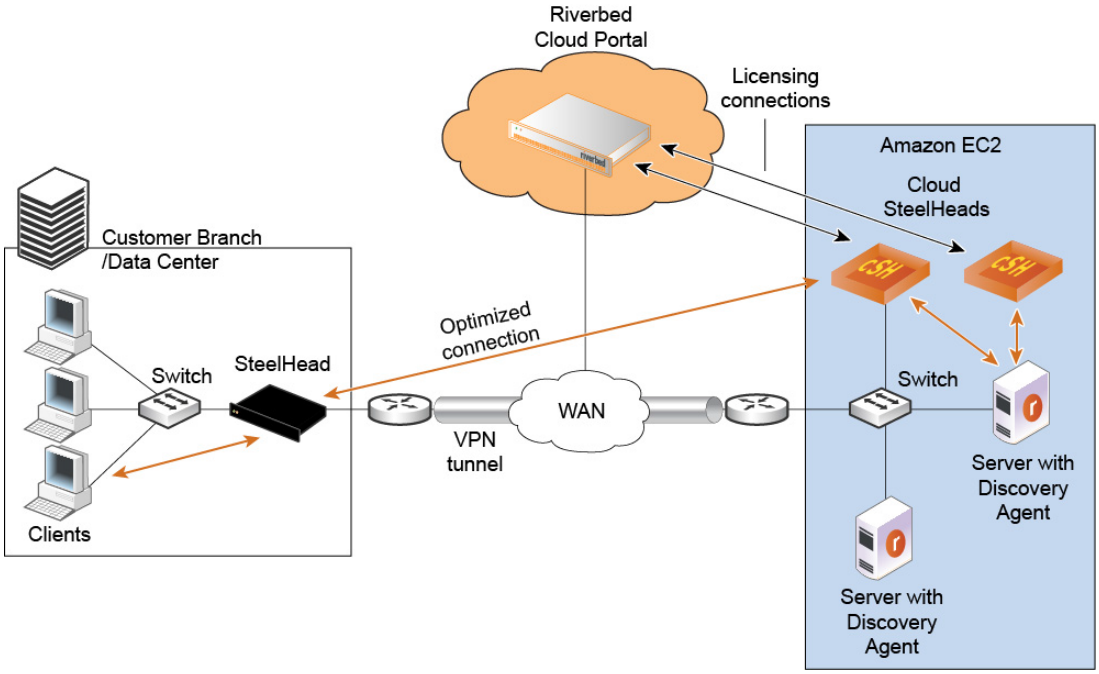
This section describes how to deploy a SteelHead-c virtual appliance using different levels of security and includes configuration caveats.

Using a VPC with a VPN connection to the data center

When you connect to the Amazon VPC through a VPN tunnel using either a software or hardware IPsec gateway, you use the highest level of security. In this scenario, the SteelHead-c has a single IP address from the pool of private VPC addresses. Therefore, there is no special configuration required to deploy the SteelHead-c. As long as you connect the SteelHead-c to the Riverbed Cloud Portal, both autodiscovery and auto-reconfiguration (that is, when instances change their IP addresses, the portal automatically detects it) works.

Figure 7-1 shows how to deploy SteelHead-c and servers in Amazon VPC with a VPN connection to the data center.

Figure 7-1. Using Amazon VPC through a VPN tunnel (without NAT)



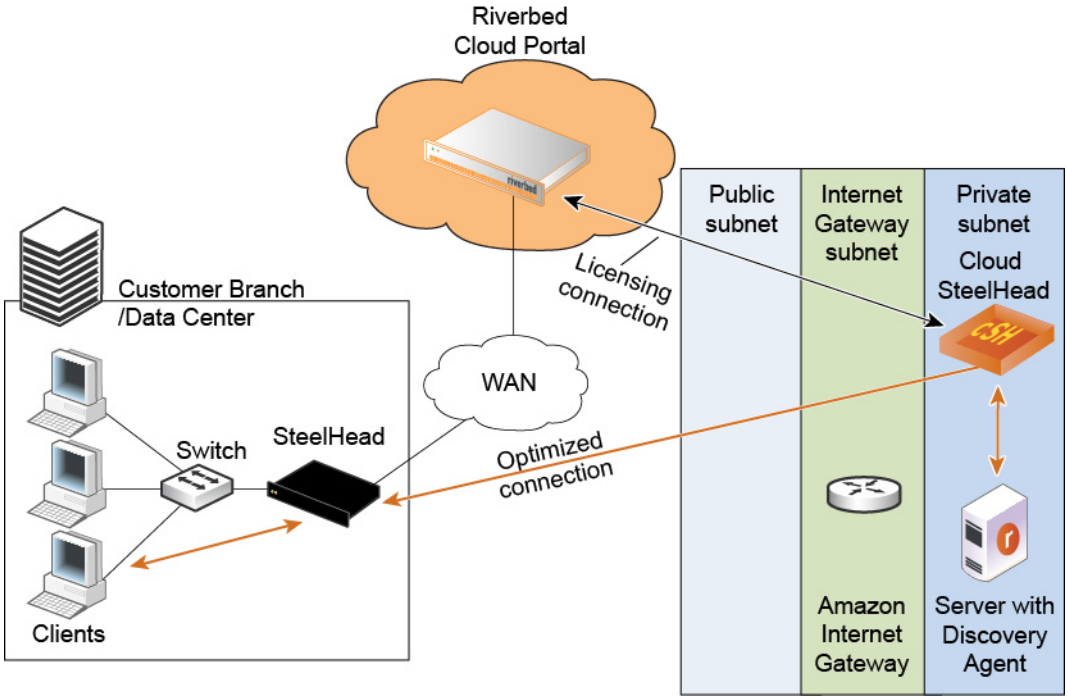
In the network shown in Figure 7-1, servers in Amazon use private IP addresses. The VPC with VPN tunnel provides an extension of your intranet into AWS.

Using a VPC without a VPN connection to the data center

When you use a VPC without a VPN connection to the customer data center, you access the Amazon VPC through the Amazon Internet gateway that translates the private IP addresses in the VPC to public IP addresses. In this scenario, the Riverbed Cloud Portal detects the private IP address of the SteelHead-c and Discovery Agent servers. It also detects the elastic IP address that you manually configure using the AWS console. Ensure that you configure the ACL and security groups in the AWS console so that the SteelHead-c can communicate with the Riverbed Cloud Portal.

Figure 7-2 shows how to deploy the SteelHead-c and server in Amazon VPC using a VPC without a VPN connection to the customer data center.

Figure 7-2. Using Amazon VPC through the internet (with NAT)



Configuring security groups

This section describes how to configure security groups when you connect to the VPC through the VPN (without NAT) and when you connect to the VPC through the Internet (with NAT).

Connecting to the VPC through the VPN (without NAT)

Configure a VPC through the VPN by modifying the security group of the AWS EC2 instances running the Discovery Agent:

1. Add the private IP address of the remote server for the ports used by the application to optimize.
2. Add the security group of the SteelHead-c (enable access to all ports).
3. On the SteelHead-c security group, add the public IP address of the remote SteelHead and enable it to access port 7800 and port 7810.

Connecting to a VPC through the internet (with NAT)

Configure a VPC without IPsec tunnel by modifying the security group of the AWS EC2 instances running the Discovery Agent:

1. Add the public IP address of the machines that access the server from outside the VPC, such as the virtual appliances in the customer data center.

2. Add the security group of the SteelHead-c (enable access to all ports).
3. On the SteelHead-c security group, configure these settings:
   - Add the public IP address of the machines that access the server from outside the VPC, such as the virtual appliances in the customer data center.
   - Enable access to port 7800 and port 7810 for TCP.
   - Add the private IP addresses of all local AWS instances running the Discovery Agent, allowing access to all ports for TCP and UDP.

A

Manually Provisioning a SteelHead-c for AWS

While the Riverbed Cloud Portal makes it easy to provision SteelHead-c, some customers may want to manually deploy their SteelHead-c virtual appliances. You might want to do this if:

- you are provisioning SteelHead-c virtual appliances in the AWS GovCloud (US) region.
- you are provisioning SteelHead-c virtual appliances in the AWS China region.
- you have multiple AWS accounts and need SteelHead-c in more than one of them.
- you are provisioning CCX-SUB-PERF-TIER model series SteelHead-c virtual appliances.

This appendix includes these sections:

Before you begin

Riverbed Support needs to grant you access to the Riverbed AMIs. Ensure that your Riverbed Support representative has this information so that they can enable your AWS account with permission to view and launch the appropriate private AMIs.

Note: If you have multiple accounts, ensure you provide the ID for the account associated with the region where you want to run your SteelHead-c virtual appliances.

Your Riverbed AMIs will be accessible under your EC2 dashboard > Images > AMIs > Private AMIs.

- AWS account ID
- AWS regions where you want to run your SteelHead-c virtual appliances
- SteelHead-c RiOS versions you want to run

Launching a SteelHead-c for AWS

This section describes how to create a SteelHead-c for AWS virtual appliance and start it.

To complete this process you must provide an Amazon Machine Image (AMI), security group, key pair, and one-time token. Have this information at hand before beginning the process.

To create a SteelHead-c for AWS

1. Log in to your AWS account.
2. Navigate to the EC2 dashboard.
3. Select AMIs in the Images section of the navigation pane.
4. Select Private Images from the drop-down menu to the left of the search bar.
5. Choose the AMI that Riverbed Support shared with you and click **Launch**. See "Before you begin" on page 73.
6. Select an instance type based on the SteelHead-c model you are deploying. See "SteelHead-c models and required virtual machine resources" on page 11.
7. Click **Next: Configure Instance Details**.
8. Expand the Advanced Details section.
9. Under User Data, select As Text and enter this information into the text field:

   ```
   ds=/dev/xvdq
   passwd=$1$xcuHq/$a/qZ8zGpzy.NHsKjJ8Yla.
   appname=ManuallyDeployedSteelHead
   lshost=cloudportal.riverbed.com
   rvbd_dshost=cloudportal.riverbed.com
   lott=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
   ```

   where:

   - **ds** - The device node in which the SteelHead-c expects the data store EBS volume to appear. Due to changes in EC2 architecture, set this to /dev/xvdq. It matches the /dev/sdm device node mapping you set for the data store EBS volume.
   - **passwd** - The password hash for the admin user. In this example, set this value to `$1$xcuHq/$a/qZ8zGpzy.NHsKjJ8Yla`. You can log in to the SteelHead-c with the username **admin** and the default password **password**. Ensure that you change the default password after you log in for the first time.
   - **appname** - Name of the SteelHead-c.
   - **lshost** -Fully qualified domain name of the licensing server. This name is usually the Riverbed Cloud Portal.
   - **rvbd_dshost** - Fully qualified domain name of the discovery server. This name is usually the Riverbed Cloud Portal.
   - **lott** - One-Time Token used to redeem the license. You obtain this token from the SteelHead-c license on the Riverbed Cloud Portal. You can also provide the One-Time Token after you launch the SteelHead-c.
10. Click **Next: Add Storage**.
11. Add and configure two volumes in addition to the root volume. One of these volumes will store the SteelHead-c software and serve as the configuration and management services disk. The other will serve as the data store disk.
    - Click **Add a New Volume** twice.

- Under the Device column, select /dev/sdk for the configuration and management services disk and select /dev/sdm for the data store disk.
- Under the Size (GiB) column for each disk, specify a size based on the SteelHead-c model. See "SteelHead-c models and required virtual machine resources" on page 11.
- Under Volume Type, you can choose Magnetic unless the SteelHead-c model you are deploying requires a solid state drive (SSD). We recommend SSD volumes for all CCX-SUB-PERF-TIER models.

12. Click **Next: Tag Instance**.
13. (Optional) Add tags. You might find tags useful if you want to group resources together, for example.
14. Click **Next: Configure Security Group**.
15. Choose a security group for the virtual appliance.

    To connect the SteelHead-c, the Discovery Agent, and the client-side SteelHead, configure the security group so that:

    - the SteelHead-c allows UDP connections coming in from the Discovery Agent on port 7801.
    - the SteelHead-c allows TCP connections coming in from the client-side SteelHead on ports 7800 and 7810 to 7850 for optimization.
    - the SteelHead-c allows CLI and UI access on ports 22, 80, and 443.
    - the configuration allows TCP connections from the SteelHead-c and the client-side SteelHead.

16. Click **Review and Launch**.
17. Review the instance details.
18. Click **Launch** to launch the virtual appliance.

Connecting to the SteelHead-c management console

After you connect to the SteelHead-c management console for the first time, the SteelHead-c loads the attached volumes and starts. You might have to wait for a few minutes for the management console to display.

To connect to the SteelHead-c Management Console

1. Log in to your AWS account.
2. Navigate to the EC2 dashboard.
3. Select **Instances** in the Instances section of the navigation pane.
4. Click **Connect**.
5. In the Connect to Your Instance dialog box, select a connection method and follow the instructions in the dialog box.
6. Log in to the SteelHead-c Management Console using your username and password. For first-time login, use **admin** for the username and **password** for the password.

After deployment and licensing, the SteelHead-c appears in the Riverbed Cloud Portal with a name based on the ID of its management volume.

Upgrading the RiOS software version

This section provides instructions for upgrading the RiOS software on instances that have been manually deployed.

Note: The SteelHead-c IP addresses will change. Ensure that you update any rules or configurations that depend on it such as fixed-target rules on on-premise SteelHeads that peer your SteelHead-c, on-premise firewall configurations, or AWS security group configurations.

To upgrade RiOS software on a SteelHead-c virtual appliance

1. Stop the SteelHead-c virtual appliance and delete the AMI.
2. Provision a new AMI, using the same launch parameters that you used for the old one.
3. Reattach the management and data store volumes associated with the old instance.

The SteelHead-c IP addresses change after you complete this step. As mentioned in the above note, ensure you update any configurations that depend on these IP addresses.

B

Manually Provisioning a SteelHead-c for AWS Marketplace

While the Riverbed Cloud Portal makes it easy to provision SteelHead-c, some customers may want to manually deploy their SteelHead-c virtual appliances. You might want to do this if:

- you are provisioning SteelHead-c virtual appliances in the AWS GovCloud (US) region.
- you are provisioning SteelHead-c virtual appliances in the AWS in China region.
- you have multiple AWS accounts and need SteelHead-c in more than one of them.
- you are provisioning CCX-SUB-PERF-TIER model series SteelHead-c virtual appliances.

This appendix includes these sections:

Before you begin

Riverbed Support needs to grant you access to the Riverbed AMIs. Ensure that your Riverbed Support representative has this information so that they can enable your AWS account with permission to view and launch the appropriate private AMIs.

Note: If you have multiple accounts, ensure you provide the ID for the account associated with the region where you want to run your SteelHead-c virtual appliances

Your Riverbed AMIs will be accessible under your EC2 dashboard > Images > AMIs > Private AMIs.

- AWS account ID
- AWS regions where you want to run your SteelHead-c virtual appliances
- SteelHead-c RiOS versions you want to run

Launching a SteelHead-c for AWS Marketplace

This section describes how to create a SteelHead-c for AWS Marketplace virtual appliance and start it.

To complete this process you must provide an Amazon Machine Image (AMI), security group, key pair, and one-time token. Have this information at hand before beginning the process.

To create a SteelHead-c for AWS Marketplace

1. Log in to your AWS account.
2. Navigate to the EC2 dashboard.
3. Select AMIs in the Images section of the navigation pane.
4. Select Public Images from the drop-down menu to the left of the search bar.
5. Choose the Riverbed SteelHead AMI and click **Launch**. See "Before you begin" on page 77.
6. Select an instance type based on the SteelHead-c model you are deploying. See "SteelHead-c models and required virtual machine resources" on page 11.
7. Click **Next: Configure Instance Details**.
8. Expand the Advanced Details section.
9. Under User Data, select As Text and enter this information into the text field:

   ```
   ds=/dev/xvdq
   appname=MarketplaceDeployedSteelHead
   lshost=cloudportal.riverbed.com
   rvbd_dshost=cloudportal.riverbed.com
   lott=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
   ```

   where:

   ds - The device node in which the SteelHead-c expects the data store EBS volume to appear. Due to changes in EC2 architecture, set this to /dev/xvdq.

   appname - Name of the SteelHead-c.

   lshost -Fully qualified domain name of the licensing server. This name is usually the Riverbed Cloud Portal.

   rvbd_dshost - Fully qualified domain name of the discovery server. This name is usually the Riverbed Cloud Portal.

   lott - One-Time Token used to redeem the license. You obtain this token from the SteelHead-c license on the Riverbed Cloud Portal. You can also provide the One-Time Token after you launch the SteelHead-c.

10. Click **Next: Add Storage**.
11. Click **Next: Tag Instance**.
12. (Optional) Add tags. You might find tags useful if you want to group resources together, for example.
13. Click **Next: Configure Security Group**.
14. Choose a security group for the virtual appliance.

    To connect the SteelHead-c, the Discovery Agent, and the client-side SteelHead, configure the security group so that:

    – The SteelHead-c allows UDP connections coming in from the Discovery Agent on port 7801 to 7850.

- The SteelHead-c allows TCP connections coming in from the client-side SteelHead on ports 7800 and 7810 to 7850 for optimization.
- the SteelHead-c allows CLI and UI access on ports 22, 80, and 443.
- The configuration allows TCP connections from the SteelHead-c and the client-side SteelHead.

15. Click **Review and Launch**.
16. Review the instance details.
17. Click **Launch** to launch the virtual appliance.
18. Add and configure a data store disk. This volume is in addition to the root volume.
    - Navigate to Volumes in AWS Console.
    - Click **Create Volume**.
    - Under the Size (GiB) column, specify a size based on the SteelHead-c model. See "SteelHead-c models and required virtual machine resources" on page 11.
    - Under Volume Type, choose Magnetic unless the SteelHead-c model you are deploying requires a solid state drive (SSD).
    - Under Availability zone, choose the zone where the SteelHead-c resides.
    - After the volume is created, select it.
    - Select Actions in AWS Console, and then click **Attach Volume**.
    - Under Instance, select the instance-id of SteelHead-c.
    - Under Device, enter /dev/xvdq and click **Attach**.

Connecting to the SteelHead-c management console

After you connect to the SteelHead-c management console for the first time, the SteelHead-c loads the attached volumes and starts. You might have to wait for a few minutes for the management console to display.

To connect to the SteelHead-c Management Console

1. Log in to your AWS account.
2. Navigate to the EC2 dashboard.
3. Select **Instances** in the Instances section of the navigation pane.
4. Click **Connect**.
5. In the Connect to Your Instance dialog box, select a connection method and follow the instructions in the dialog box.
6. Log in to the SteelHead-c Management Console using your username and password. For first-time login, use **admin** for the username and the SteelHead-c instance ID for the password.

After deployment and licensing, the SteelHead-c appears in the Riverbed Cloud Portal with a name based on the ID of its management volume.

Upgrading the RiOS software version

This section provides instructions for upgrading the RiOS software on instances that have been manually deployed.

Note: The SteelHead-c IP addresses will change. Ensure that you update any rules or configurations that depend on it such as fixed-target rules on on-premise SteelHeads that peer your SteelHead-c, on-premise firewall configurations, or AWS security group configurations.

To upgrade RiOS software on a SteelHead-c virtual appliance

1. Download the new image from the Riverbed Support site.
2. Log in to your SteelHead-c Management Console and navigate to Administration > Maintenance: Software Upgrade.
3. Under the Install Upgrade section, choose From Local File.
4. Click **Choose File** and use the file browser to select the image file you downloaded.
5. Optionally select Schedule Upgrade for Later and choose a date and time to automatically perform the installation.
6. Click **Install**.

The SteelHead-c IP addresses change after you complete this step. As mentioned in the above note, ensure you update any configurations that depend on these IP addresses.