Riverbed® Cloud Services User's Guide

RiOS® Version 9.0

November 2014

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com

Part Number
712-00072-06

Contents

Preface

Welcome to the *Riverbed Cloud Services User's Guide.* Read this preface for an overview of the information provided in this guide and the documentation conventions used throughout, and contact information. This Preface includes the following sections:

About This Guide

The *Riverbed Cloud Services User's Guide* describes how to deploy, configure, and manage Riverbed virtual appliances in Cloud environments.

This guide includes information relevant to the following products:

- 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, CIFS, HTTP, FTP, and NFS. Familiarity with virtualization and cloud technologies is helpful.

Document Conventions

This guide uses the following 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.

Courier	Code examples appear in Courier 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 represents a choice to select one keyword or variable to the left or right of the symbol. The keyword or variable can be either optional or required: **{delete <filename> | upload <filename>}**

Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the SteelHead-c.

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 v7.0 through v9.0. Internet Explorer v7.0 and v8.0 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.

Riverbed CLI Hardware Requirements	Software and Operating System Requirements
One of the following: • An ASCII terminal or emulator that can connect to the serial console (9600 baud, 8 bits, no parity, 1 stop bit, and no flow control) • A computer with a Secure Shell (ssh) client that is connected by an IP network to the appliance primary interface	Secure Shell (ssh). Free ssh clients include PuTTY for Windows computers, OpenSSH for many UNIX and UNIX-like operating systems, and Cygwin.

Documentation and Release Notes

To obtain the most current version of all Riverbed documentation, go to the Riverbed Support site at https://support.riverbed.com.

If you need more information, 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 identify new features in the software as well as known 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** - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States. You can also go to https://support.riverbed.com.
- **Professional services** - Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/services-training/Services-Training.html.
- **Documentation** - The Riverbed Technical Publications team continually strives to improve the quality and usability of Riverbed documentation. Riverbed appreciates any suggestions you might have about its online documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

CHAPTER 1 Riverbed Cloud Services

This chapter describes Riverbed cloud services. It includes the following 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 datacenter by eliminating the barriers to enterprise-class cloud deployments.SteelHead-c appliances accelerate the migration of data and applications to the cloud, while speeding access to that data from anywhere. Compatibility with Microsoft Azure, Amazon Web Services, and VMware ESX-based cloud environments eliminates vendor lock-in by offering the freedom to optimize applications hosted in nearly any cloud and move between cloud providers with ease.

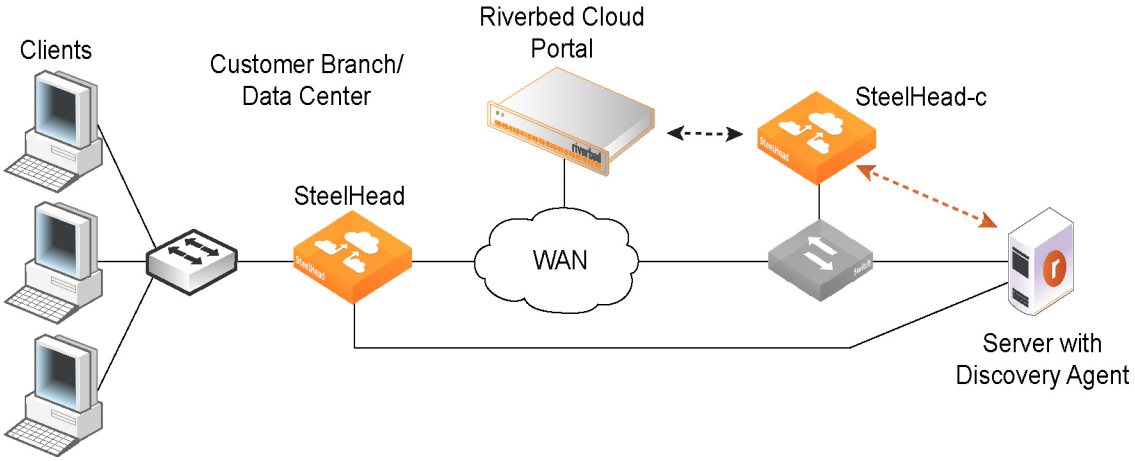
As you migrate services to the cloud, and later broaden your application and data footprint there, SteelHead-c appliances ensure you will meet application performance SLAs, regardless of network latency and enterprise bandwidth limitations, to ensure seamless public-cloud integration through features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

- Transparent cloud interception
- Flexible cloud pricing model
- Portal-based management
- Elastic sizing and cloning
- Interoperability with SteelHead physical appliances, SteelHead virtual appliances, and SteelHead Mobile.

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 the following 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 instances. For details, see Chapter 2, "Riverbed Cloud Portal."

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.

- SteelHead-c - Software form factor of SteelHead CX which are 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 appliances on the server-side. It also provides failure detection and load balancing. For details, see Chapter 3, "Using the Discovery Agent."

Supported Deployment Modes

Riverbed cloud services support the following client/server deployments.

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: This deployment mode is not applicable to SteelHead-c on Azure.

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

For details, see "Using the Discovery Agent" on page 37

Figure 1-4. Clients in the Cloud Behind a SteelHead-c

SteelHead-c Models and Required Resources

The following tables list available SteelHead-c models and the minimum virtual machine resources required for each model.

SteelHead-c Model	Minimum Azure Host VM	Minimum Amazon Target	Minimum ESX/ ESXi Requirements	Minimum Bandwidth (all IaaS vendors)	Maximum Connections (all IaaS vendors)	Total Data Store Disk Size (all IaaS vendors)*
CCX-255U	Small/A1	m1.small	1 CPU/1000MHz 2GB RAM 38GB disk space for management disk	2Mbps	50	440GB
CCX-255L	Small/A1	m1.small	1 CPU/1000MHz 2GB RAM 38GB disk space for management disk	6Mbps	75	440GB
CCX-255M	Small/A1	m1.small	1 CPU/1000MHz 2GB RAM 38GB disk space for management disk	6Mbps	150	440GB
CCX-255H	Small/A1	m1.small	1 CPU/1000MHz 2GB RAM 38GB disk space for management disk	6Mbps	230	440GB
CCX-570L	Medium/A2	m1.large	1 CPU/1200MHz 3GB RAM 38GB disk space for management disk	6Mbps	250	460GB
CCX-570M	Medium/A2	m1.large	1 CPU/1200MHz 3GB RAM 38GB disk space for management disk	10Mbps	400	460GB
CCX-570H	Medium/A2	m1.large	1 CPU/1200MHz 3GB RAM 38GB disk space for management disk	10Mbps	650	460GB
CCX-770L	Medium/A2	m1.large	2 CPU/1200MHz 3GB RAM 38GB disk space for management disk	10Mbps	900	460GB
CCX-770M	Medium/A2	m1.large	2 CPU/1200MHz 3GB RAM 38GB disk space for management disk	10Mbps	1500	460GB

SteelHead-c Model	Minimum Azure Host VM	Minimum Amazon Target	Minimum ESX/ ESXi Requirements	Minimum Bandwidth (all IaaS vendors)	Maximum Connections (all IaaS vendors)	Total Data Store Disk Size (all IaaS vendors)*
CCX-1555L	Large/A3	m1.large	4 CPU/1200MHz 8GB RAM 38GB disk space for management disk	50Mbps	3000	460GB
CCX-1555M	Large/A3	m1.large	4 CPU/1200MHz 8GB RAM 38GB disk space for management disk	50Mbps	4500	460GB

* Amazon AWS refers to data store disks as Elastic Block Stores (EBS).

System Limitations and Dependencies

SteelHead-c images can be installed on Amazon AWS, VMware ESX/ESXi, and Microsoft Azure virtual machines. The Riverbed Cloud Portal supports licensing and simple management for SteelHead-c appliances on all virtual machine platforms. Deploying SteelHead-c instances from the portal, however, is supported only with Amazon AWS. Deploying SteelHead-c instances onto VMware ESX/ESXi or Microsoft Azure must be done manually.

For deploying on VMware ESX/ESXi, see Chapter 4, "Using SteelHead-c Appliances on VMware ESX/ESXi."

For deploying on Microsoft Azure, see Chapter 5, "Using SteelHead-c Appliances in Microsoft Azure."

Limitations on Amazon AWS

The following section lists and describes the features and deployment options that the AWS SteelHead-c 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 AWS SteelHead-c is not deployed in-path, but in its unique out-of-path method, using one interface. Simplified routing does not apply.

WCCP/PBR/L4 – The AWS SteelHead-c 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.

Features Limitations

RSP – The AWS SteelHead-c 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 AWS SteelHead-c 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

The following section list and describes the features and deployment options that the ESX SteelHead-c does not support.

Deployment Limitations

Automatic peering – ESX SteelHead-c instances deployed with WCCP or PBR support automatic peering. ESX SteelHead-c instances deployed with the Discovery Agent do not support automatic peering.

Simplified routing – ESX SteelHead-c instances deployed in-path with the Discovery Agent support simplified routing. ESX SteelHead-c instance deployed with WCCP or PBR do not support simplified routing.

Features 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 instances 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-cs instances 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-cs appliances.

In SteelHead-c versions before v1.2, you must allocate a data store volume of exactly 440 GB for the appliance; otherwise, the SteelHead-c does not function correctly.

The reduced data store support feature in SteelHead-c v1.2 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-cs 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 appliance will use either 440 GB or 30 GB. If you allocate a disk space that is less than 440 GB, but greater than 30 GB (such as 250 GB), the SteelHead-c uses only 30 GB; it disregards 220 GB. If you allocate less than 30GB, 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

The following section list and describes the limitations of the Azure SteelHead-c:

- Discovery Agent is not supported.
- Only Out-of-path deployments are supported.
- Multiple NICs, PBR, and WCCP are not supported.

Licensing SteelHead-c Appliances

Licenses for SteelHead-c 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 an appliance enables the appliance to contact the portal and to associate the token's license with the appliance. 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 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. Click a license to view details about it, including the one-time token associated with it.

To license a SteelHead-c appliance

1. Log in to the Riverbed Cloud Portal.
2. Select the Cloud Appliances tab > Licenses to display the Licenses page.
3. Click the Serial Number of an unprovisioned license to display the License Details page for the license.
4. Copy the one-time token displayed on the License Details page.
5. Open another browser window and navigate to the appliance's management console.
6. Navigate to the following console page:

   If you are licensing an appliance running RiOS 8.6.x or less, go to Configure > Maintenance > Licenses.

   If you are licensing an appliance running RiOS 9.0.x or greater, go to Administration > Maintenance: Licenses.

7. Under the Cloud Licensing section, paste the one-time token into the One-time Token field.
8. Click Initialize License Client.

To license a SteelHead-c appliance using the command line

1. Obtain a one-time token as detailed in the previous procedure.
2. Log in to the appliance's command-line interface as admin.
3. Enable configuration mode:

```
enable
config term
```

4. Enter the following command:

```
license client init <one-time token from the cloud portal>
```

5. Verify that the license is applied:

```
show licenses
```

Upgrading and Downgrading SteelHead-c Models

To upgrade a SteelHead-c instance 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 reverting the license to that of a lower-end model. The SteelHead-c instance will detect any change in the license associated with it when it communicates with the Riverbed Cloud Portal.

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

1. Purchase a license for the new SteelHead-c model.
2. De-provision the original SteelHead-c instance 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 reverting the license to that of a lower-end model.

Comparing SteelHead-c Features Across Cloud Providers

The following table compares the SteelHead-c features across cloud providers.

Feature	AWS	ESX	Azure
Provisioning	Through Riverbed Cloud Portal. You can also choose manual provisioning.	Manual	Manual through Azure Image Gallery
License activation	Automatic at provisioning	Manual	Manual
License portability	Yes	Yes	Manual
Deployment	Agent-intercept (with Discovery Agent) Out-of-path	Agent-intercept (with Discovery Agent) Out-of-path In-path Virtual in-path	Out-of-path
Optimization group	Yes (configured through the Riverbed Cloud Portal)	Yes (configured manually)	No
NAT IP address mapping	Using the optimization group or manually	Manual	Manual
Disk requirements	430GB + (10GB or 30GB of management disk)	440GB + 30GB of management disk	440GB + 30GB of management disk

CHAPTER 2 Riverbed Cloud Portal

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

About Riverbed Cloud Portal

The Riverbed Cloud Portal is a Web-based portal hosted and maintained by Riverbed. The portal offers the following features:

- License managment for all your SteelHead-c and SteelHead SaaS appliances.
- Light-weight appliance management.
- Direct provisioning of 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 is where you can manage your SteelHead-c 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's Guide*.

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

About Companies

At least one *company* is associated with every portal account. Configuring multiple companies under an account enables you to organize your SteelHead-c 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. Hover your cursor 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 appliances.

The Event History page displays the following information for each event:

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

To view the event history report

Hover the cusor over your user name in the upper-left section of the page and select Event History.

Finding Support

The Support menu provides the following options:

- **Help** - Launches the online help information about the portal
- **News** - Dipslays 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. Click 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. Click 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 user xyz 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, click Licenses. The Licenses page displays two tables, one that contains information about your active licenses and another with information about your unused licenses.

The Unused Licenses table displays the following information:

Parameter	Description
Serial Number	The license serial number. Click the serial number for more details about the license.
Model	The SteelHead-c model, or "Expired" if the license is expired.

The Active Licenses table displayes the following information:

Parameter	Description
Serial Number	The license serial number. This is also the appliance serial number. Click 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 clicking on the license serial number in the Licenses page. The License Details page contains the following three tabbed sections: Details, Features, and Event Log.

To view license details

In the License Details page, select the Details tab to view the following 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 Appliance State" on page 23.
- **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 the following 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 the following parameters:
   - Specify the level of log detail you want:

Log Leve	Description
Critical	Reports conditions that severly 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, timestamp, IP address of the system where the event was initiated, user name of the user who initiated the event, log level, and message.

Provisioning an Appliance to AWS

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

Prerequisite: Ensure that you have an AWS account and know your AWS login credentials.

1. Log in to the portal and select the Cloud Appliances tab.
2. Click Licenses.
3. Click on 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 the following 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 datacenter site managed by Amazon which provide stand-by computing power to their 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 user name is *admin*.
Confirm Admin Password	Confirm the administrator password entered in the previous field.
Network Access	Check the checkbox 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 appliance.

   The system creates a SteelHead-c appliance in AWS and applies the license to it. After 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 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 can not be provisioned through the portal, the token must manually be applied to the appliance. See "Managing Licenses" on page 18.

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. Situations that might require regenerating a token include if a token has been compromised and there is a possibility that an unauthorized entity can obtain the associated license; or if 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, click the serial number of the license you want.
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 applaince 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 appliance as part of the evaluation, because the license is portable between different Cloud providers.

Registering SteelHead-c 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 it's 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 it's license or by regenerating the one-time token associated with its license. See "Regenerating a One-time Token" on page 21 and "Reclaiming a License" on page 21.

Managing SteelHead-c Appliances

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

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

- **Name** - Diplays 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 and/or its license.
- **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 clicking on the name of an appliance listed on the Appliances page.

You can also manage your SteelHead (in the cloud) appliances through the SteelCentral Controller for SteelHead. See the *SteelCentral Controller for SteelHead User's Guide* for details.

An appliance's home page is organized into the following 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 managment console.
	Details*	Displays information such as Uptime, Creation Time, UUID, Architecture, etc.
	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 AWS 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.
3. Click Appliances.

About Appliance State

The following table lists the possible states for a license or appliance.

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.
ESX/ESXi, Azure	Active	The license associated with a running appliance.
	Inactive	The license associated with an appliance that is not in use.
	Unlicensed	There is no license 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 the following information:

- **Name** - Diplays 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 Appliance State" on page 23.
- **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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Summary tab.

Editing Appliance Name

You can edit the name of the 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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Summary tab.
6. Type 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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Summary tab.
6. Click the link under Management Console.
7. In the Management Console login page, enter your credentials for the appliance.

Starting, Stopping, and Deprovisioning an Appliance

You can start, stop, 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. This button is enabled only if the appliance is currently stopped.
- Stopping an appliance stops the optimization service. This 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. This button is enabled only if the appliance is not running. This operation can not be undone.

To start, stop, 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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Summary tab.
6. Click the button that corresponds to the action you want to take (**Start**, **Stop**, or **Deprovision**).

Viewing AWS 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 the following information in the AWS Details tab:

- **EC2 Instance Uptime** - Indicates the duration for which the appliance has been running.
- **Creation Time** - Displays the time when the appliance was created.
- **Availability Zone** - Indicates the zone where the 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 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 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 appliance is started: m1.small, for example.
- **Architecture** - Displays the appliance architecture type: i386 (32-bit) or x86_64 (64-bit)
- **Configuration Volume** - Indicates the volume that is stores the appliance configuration and log files. Also displyas 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.
3. Click Appliances.
4. Click the name of the appliance you want.
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 the following 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 portocol used to communicate with the portal (TCP, UDP, or ICMP).
  - **From Port** - Displays the starting port number of a range of ports on the appliance that peer nodes are allowed to access.
  - **To Port** - Displays the ending port number of a range of ports on the appliance 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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Network Controls tab.

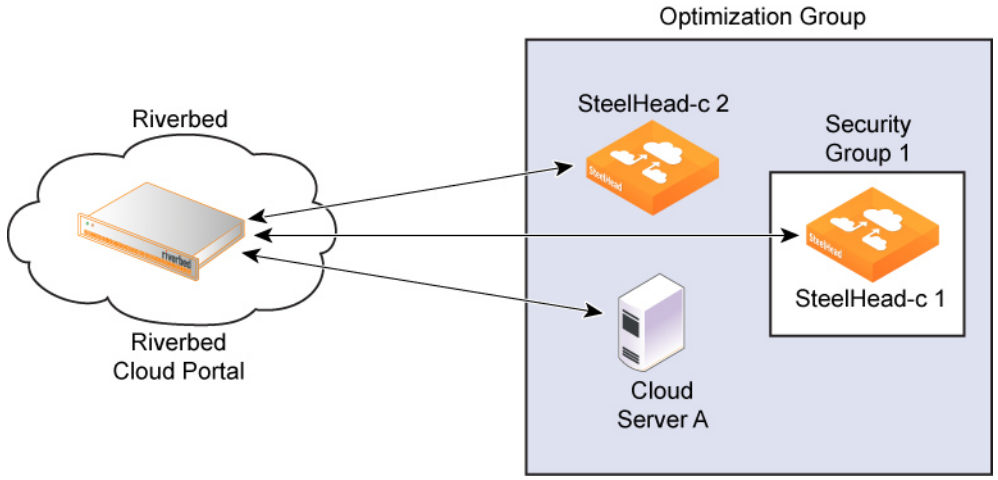
Configuring Security Groups

Correctly configured security groups are critical for a node in an optimization group to contact its peers during discovery and for optimization to work. 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 Group1 does not let SteelHead-c2 or Cloud Server A access SteelHead-c1. 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 Group1 so that the group allows access to SteelHead-c1 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 optimizing the connections.

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 (described in the following section).

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 you want.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Network Controls tab.
6. Click **Add Custom Rule**.
7. In the Add Custom Rule dialog box, complete the following items:
   - **Protocol** - Select a portocol 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, click Appliances and click 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 the following 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 user name 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.
3. Click Appliances.
4. Click the name of the appliance you want.

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. Click 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.

The following 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 mode.
- **Round Robin** - Selects a SteelHead-c and then another (using the round-robin method) for load balancing. Use the Round Robin mode 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 you want.
3. Click 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 Otimization Group page, click 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, load-balancing policy, and you can add appliances and application servers to the group. The Optimization Group Details page is organize into the following tabs:

- Summary tab - Displays the name, description, 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.
3. Click Optimization Groups.
4. Click the name of the group you want to edit.
5. Select the Summary tab.
6. Click **Modify Optimization Group**.
7. Change the name, description, and load-balancing policy to your liking and click **Update**.

To add a 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 the following 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 user name 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 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 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.
3. Click Optimization Groups.
4. Click the name of the group you want to edit.
5. Select the Even 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.
3. Click 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 to your liking.
6. Click **Update**.

Viewing 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 Discoverd Appliances report page displays the following 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 - Dispalys the current internal IP address of the discovered appliance. This a private network IP address and is reachable only by machines within the same privare 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.
3. Click Discovered Appliances.

Upgrading RiOS Software on an AWS Appliance

You can upgrade or revert to a backup version of the software on your AWS appliance in the Appliance Summary page.

Note: ESX/ESXi and Azure-hosted appliances can be upgraded in the same manner as physical appliances by using the Software Upgrade page in the appliance's management console. For details, see *SteelHead Management Console User's Guide*.

To upgrade or revert RiOS software on an AWS SteelHead-c 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.
3. Click Appliances.
4. Click the name of the appliance you want.
5. Select the Summary tab.
6. Select a version from the Version drop-down list.
7. Click **Update Details**.
8. Ensure that the appliance is rebooted.

CHAPTER 3 Using the Discovery Agent

This chapter describes how to use the Riverbed Discovery Agent. It contains the following 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.

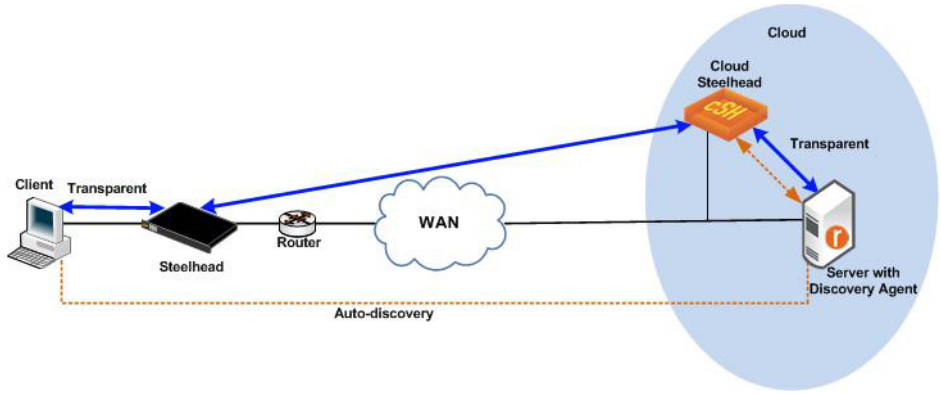
In a server-side Discovery Agent deployment, when a client SteelHead connects to a server with Discovery Agent installed, the Discovery Agent redirects any auto-discovery probe request to a configured SteelHead-c from its list. Then, the client SteelHead discovers and starts peering and optimizing with the server-side SteelHead-c. After the auto-discovery 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 auto-discovery probe, discovers the remote SteelHead, and starts peering and optimizing with it.

The Discovery Agent provides the following features:

- **Optimization** - Enables you to intercept (and optimize) inbound and outbound connections from the cloud.
- **Auto-discovery** - Enables SteelHeads to automatically find AWS SteelHead-c appliances and to optimize traffic through them. Auto-discovery relieves you of having to manually configure the SteelHeads with fixed target rules to find the remote AWS 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 AWS SteelHead-c failures and connectivity issues to the AWS SteelHead-c so that traffic can be passed through instead of being redirected to the failed AWS 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 auto-discovery probe to the server. The Discovery Agent redirects the auto-discovery probe to the AWS SteelHead-c. The AWS SteelHead-c sends an auto-discovery 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 AWS 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 NATs 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 the following 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 5-10% 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 AWS SteelHead-c (this does not apply to the ESX SteelHead-c) 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. Click 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. Click the server or the AWS SteelHead-c name in the Name column to display the Optimization Group Member Details page.

   When you add an AWS 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 supports the following Windows servers:

- 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 SteelHead Mobile Client and the Discovery Agent on the same Windows computer.

To install the Discovery Agent on a Windows server

1. From the Riverbed Support Website, click Software & Documentation.
2. In the Search text box, type **Discovery Agent** and click the arrow icon.
3. Click the link for the Discovery Agent package you want and save the file.
4. Log in to the Windows server and double-click the executable file to display the Discovery Agent Installation Wizard.
5. 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.
6. Click **Cancel** to quit the program, or click **Next** to continue with the installation.
7. Read and accept the license agreement and click **Next** to display the Riverbed Discovery Agent Configuration page.
8. Select the cloud type (**AWS** or **Other**) from the drop-down list.
9. If you select the cloud type **AWS**, click **Next** to display the Riverbed Portal Configuration page; go to Step 12 if you select the cloud type **Other**.

10. Optionally, type the client ID and client key (for the AWS SteelHead-c) that you obtain from the Riverbed Cloud Portal in the text boxes and click **Next**. This does not apply to ESX SteelHead-cs.

    You can choose one of the following 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).

11. Select **Use Proxy to connect to Cloud Portal** to specify a proxy IP address or hostname when connecting to the Riverbed Cloud Portal.

12. Select **Use Local Portal** to configure the Discovery Agent using the local portal mode and click **Next**.

13. Select a folder in which the Discovery Agent should be installed and click **Install**.

14. 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:

- Centos 5.0, 5.2, 5.3, and 5.4 - 32 bit and 64 bit
- Linux Ubuntu 8.04 and 10.04 - 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 Website, click Software & Documentation.

2. In the Search text box, type **Discovery Agent** and click the arrow icon.

3. Click 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 the following 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 39.

   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 42.

   To configure the Discovery Agent on your Windows server, see "Configuring the Discovery Agent on Windows Servers" on page 42.

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 43
- "Configuring the Discovery Agent Manually" on page 43
- "Configuring the Discovery Agent Using the Local Portal Mode" on page 44

Configuring the Discovery Agent Using the Riverbed Cloud Portal

For AWS SteelHead-c appliances, you can configure the Discovery Agent using the Riverbed Cloud Portal. This mode does not apply to ESX SteelHead-cs.

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. Select **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 the following 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 39.
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 39.
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	Type the proxy server hostname or IP address.
Proxy Port	Type 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 the ESX SteelHead-c, you must configure it manually.

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 one of the following load-balancing policies 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 is the default mode.
   - **Round Robin** - Selects a SteelHead-c and then another (using the round-robin method) for load balancing. Use the Round Robin mode 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. Type 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 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 AWS SteelHead-c appliances. This mode does not apply to ESX SteelHead-cs.

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 the following 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	Check the check box to make the fields below editable and configure an HTTP proxy server to connect to the portal.
Proxy Hostname or IP	Type the proxy server hostname or IP address.
Proxy Port	Type 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 Management Console User's 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 one of the following transparency modes:

- **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 and 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 the following 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 is the default mode.
- **Non-transparent** - All client connections are nontransparent—the application server detects the connections from the server-side SteelHead IP address and not the client IP address. Riverbed recommends 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 the following commands to enable the agent-intercept mode:

```
en
conf term
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 appliance.

CHAPTER 4 Using SteelHead-c Appliances on VMware ESX/ESXi

This chapter describes how to use VMware ESX SteelHead-c appliances. It includes the following sections:

Overview of ESX SteelHead-c Appliances

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

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

Limitations

ESX SteelHead-cs have the following 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 ESX SteelHead-cs, because a SteelHead-c deployed on an ESX cloud requires static IP addresses to work correctly.

ESX SteelHead-c Requirements

The following table describes the ESX SteelHead-c requirements.

Component	Requirement
Supported vSphere releases	v4.0 and higher
Provisioning	OVA package deployment
License management	Connectivity between SteelHead-c and the Riverbed Cloud Portal (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 ESX 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, and 5.4 - 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.

Virtual Hardware Requirements

For details about virtual hardware requirements for different models of ESX SteelHead-c appliances, see "SteelHead-c Models and Required Resources" on page 8.

Basic Steps to Deploy an ESX SteelHead-c

The following table lists the deployment tasks:

Task	Reference
1. Install the ESX SteelHead-c using VMware vSphere.	"Installing the ESX SteelHead-c" on page 49
2. Configure the resources that the ESX server will be granting the ESX SteelHead-c.	"Configuring ESX Resources" on page 51
3. Complete the initial configuration of the ESX SteelHead-c.	"Completing the Initial Configuration" on page 52

Task	Reference
4. Obtain the one-time token from the Riverbed Cloud Portal.	"Managing Licenses" on page 18
5. Apply the one-time token to the ESX SteelHead-c.	
6. Use the Riverbed Cloud Portal to monitor the ESX SteelHead-c.	"Monitoring ESX SteelHead-c Appliances" on page 55
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 ESX SteelHead-cs. You must use the Manual Mode.	"Installing the Discovery Agent" on page 40
9. If you are not using the Discovery Agent, configure the client-side SteelHead in-path rules to point to the ESX SteelHead-c for server.	*SteelHead Management Console User's Guide*
10. If your network is NATed, go to Step 11.	
11. If you are not using the Discovery Agent, configure the ESX SteelHead-c for public or private IP address mapping.	

Installing the ESX SteelHead-c

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

The ESX 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 ESX SteelHead-c, including its virtual disks, CPU, memory, networking, and storage. To install an ESX 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 ESX SteelHead-c. Do not open or modify any of the files in the package. The package files take up several GBs of disk space (the package itself is less than one GB).

Note: An ESX SteelHead-c requires 440 GB virtual disk. This size is bigger than the 256GB maximum virtual disk size deployable in an ESX cluster when you use the Virtual Machine File System (VMFS) default block size of 1MB. Therefore, before installing an ESX 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 an ESX SteelHead-c

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, type the hostname IP address or name, type your user name and password, and click **Login**.
4. Choose File > Deploy OVF template.
5. Click 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. Type 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. The following 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.
    - Riverbed recommends 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 ESX 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.
    ```

Important: 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 ESX SteelHead-c, you must configure the resources that the ESX server will be granting the ESX 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 1200 at least the minimum required for the model you want to use.

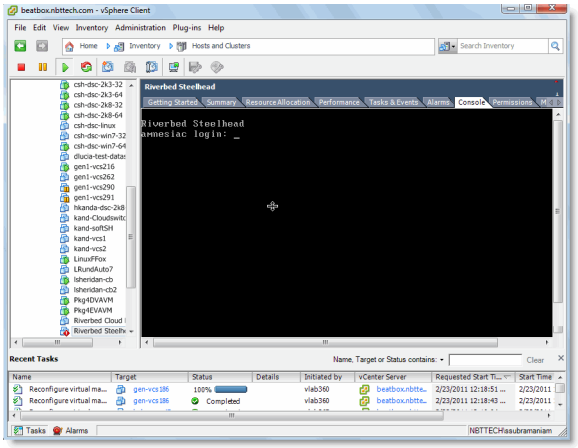
10. Click **OK** to save your changes.

11. Select the virtual machine and choose Power > Power On.

12. Select the Console tab.

    The ESX SteelHead-c starts and the login prompt appears.

Figure 4-1. ESX SteelHead-c Console Login



13. Log in to the ESX 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 ESX SteelHead-c.

To configure the ESX SteelHead-c

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

   Enter **yes** at the system prompt: for example,

   ```
   Configuration wizard.
   Do you want to use the wizard for initial configuration? yes
   ```

Tip: 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.

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

---

2. Complete the configuration wizard steps on the client-side ESX SteelHead-c as described in the following 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 ESX SteelHead-c. Riverbed recommends 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 ESX 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 ESX 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?	Riverbed strongly recommends that you change the default administrator password. The password must be a minimum of 6 characters. The default administrator password is **password**.	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. Important: 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 ESX 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 ESX SteelHead-c configuration wizard automatically saves your configuration settings.

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

```
amnesiac> exit
```

Logging in to the ESX SteelHead-c Management Console

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

You can connect to the ESX SteelHead-c through any supported Web browser. To connect to the ESX SteelHead-c, you must know the host, domain, and administrator password that you assigned during the initial setup.

Note: Cookies and JavaScript must be enabled in your browser.

To log in to the ESX SteelHead-c

1. Enter the URL for the ESX 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 ESX SteelHead-c during the initial configuration. If your DNS server maps the IP address to a name, you can specify the DNS name.

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, type 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, type the password you assigned in the configuration wizard.

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

Monitoring ESX SteelHead-c Appliances

The Riverbed Cloud Portal enables you to monitor ESX SteelHead-c appliances. It provides enough information about each ESX SteelHead-c so that you can easily identify the relevant virtual machine in your private cloud using third-party tools such as VMware vCenter.

To view information about an ESX SteelHead-c

1. In the Cloud Appliances tab on the Riverbed Cloud Portal, click Appliances to display the Appliances page.

2. Click the name of the ESX SteelHead-c in the Name column to display the ESX SteelHead-c Summary page.

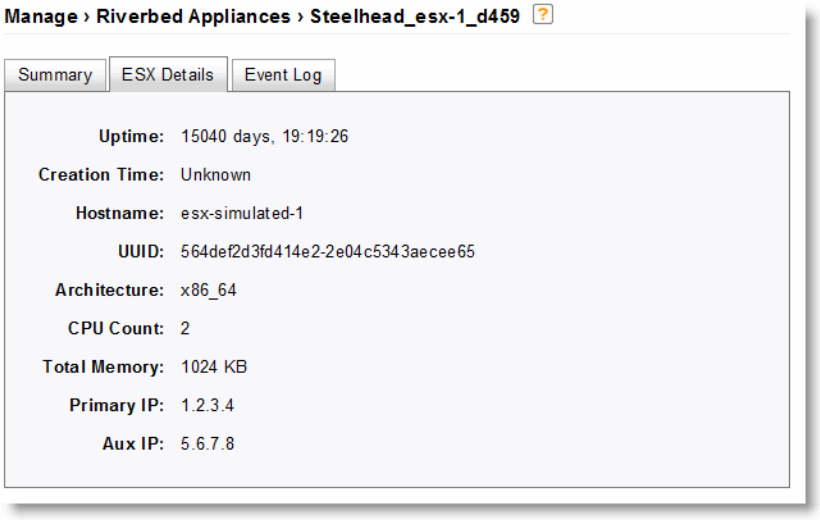
3. In the ESX SteelHead-c Summary page, complete the configuration as described in the following table.

Parameter	Description
Name	Name of the appliance. This name is specific to the Riverbed Cloud Portal. You can change the name by typing a new name in the text box and clicking **Update Appliance**.
Description	Specify a description for the appliance.

Parameter	Description
State	Current state of the ESX SteelHead-c license. It can have one of the following values: • **Active** - The license associated with the appliance is in use. • **Inactive** - The license associated with the appliance is not in use. • **Unlicensed** - There is no license associated with the appliance.
License	The license that the appliance is using. Click the license name for more details about the license.
Version	The version of Riverbed software running in the virtual machine.
Management Console	Link to the ESX SteelHead-c Management Console.
Update Appliance	Updates the appliance with the changes you made to its name and description.
Reclaim License	See "Reclaiming a License" on page 21.

4. Select the ESX Details tab to display the ESX details page for the appliance.

Figure 4-2. ESX Details Page



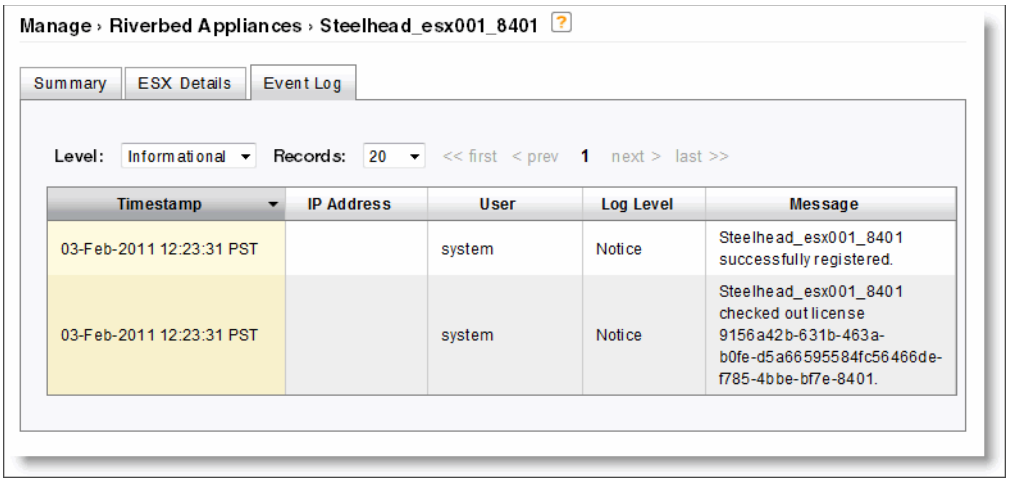
The ESX Details page displays the following parameters.

Parameter	Description
Uptime	The duration for which the appliance has been running.
Creation Time	The time at which the appliance was provisioned.
Hostname	Name of the host machine on which the ESX SteelHead-c is running.
UUID	The Unique Identifier for the appliance. The ESX system generates this number when you first create the virtual machine (appliance).
Architecture	The architecture type of the appliance: i386 (32 bit) or x86_64 (64 bit).
CPU Count	Number of CPU cores in the appliance.
Total Memory	Total memory of the appliance, in 1024 byte units.

Parameter	Description
Primary IP	IP address of the primary interface of the appliance. If you did not assign an IP address for the primary interface, the ESX Details page displays this value as **Unknown**.
Aux IP	IP address of the auxiliary interface of the appliance. If you did not assign an IP address for the auxiliary interface, the ESX Details page displays this value as **Unknown**.

5. Select the Event Log tab to display the Event Log page for the ESX SteelHead-cs.

Figure 4-3. ESX SteelHead-c Event Log Page



The ESX SteelHead-c event log page displays the following.

Control	Description
Level	Select the minimum severity level for the event log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • **Critical** - Conditions that affect the functionality of the appliance. • **Error** - Conditions that probably affect the functionality of the appliance. • **Warning** - Conditions that could affect the functionality of the appliance, such as authentication failures. • **Notice** - Normal but significant conditions, such as a configuration change. • **Informational** - Informational messages that provide general information about system operations. • **Debug** - Messages that help you debug a failure.
Records	Specify the maximum number of records to display. The default value is **20**.
Timestamp	Date and time at which the event occurred. Click the arrow to sort this column in descending order.
IP Address	IP address of the client machine that initiated the action.
User	Name of the user who performed the action.

Control	Description
Log Level	Severity level of the log message.
Message	Log message that describes the action that occurred.

Upgrading ESX SteelHead-c Software

You can upgrade ESX SteelHead-c software using the Software Upgrade page in the same way that you upgrade software on the SteelHead. For details, see *SteelHead Management Console User's Guide*.

Note: SteelHead-c images are posted in the Software > Cloud SteelHead section of the Riverbed Support site.

CHAPTER 5 Using SteelHead-c Appliances in Microsoft Azure

This chapter describes how to use SteelHead-c appliances in Microsoft Azure. It includes the following sections:

Before Using Your Microsoft Azure SteelHead-c Appliance

The following information will help you make the most of your Microsoft Azure SteelHead-c:

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

  ```
  cfe (config) # protocol connection addr <AzureSH IP> inner-intvl 30 oob-intvl 30
  ```

- Manually license your Azure SteelHead-c after the instance has been created. The Python script packaged with the SteelHead-c image enables you to perform this activity through the script.
- Only server-side, out-of-path deployments are supported.
- The following Azure network deployment constructs are supported:
  - A SteelHead-c optimizing traffic to and from a server deployed into an Azure Virtual Network.

    The SteelHead-c is created as a new Cloud Service in the same virtual network as the server. A fixed-target rule pointing to the internal IP address of the Azure SteelHead-c is configured on the client-side SteelHead appliance.
  - A SteelHead-c optimizing traffic to and from a server deployed into an Affinity Group.

    The SteelHead-c is created as a new Cloud Service in the same Affinity Group as the server. A fixed-target rule pointing to the public VIP address of the Azure SteelHead-c is configured on the client-side SteelHead appliance.

For best performance, create an Affinity Group and place the SteelHead-c and its data store in it. Placing the SteelHead-c and its data store in the same Affinity Group ensures a low latency between the appliance and its data disk.

– A SteelHead-c optimizing traffic to and from a server deployed into a Cloud Service, or all other types of servers set up for optimization using an Azure SteelHead-c appliance.

  The SteelHead-c is created as a new Cloud Service in the same Region Location as the server. A fixed-target rule pointing to the public VIP address of the Azure SteelHead-c is configured on the client-side SteelHead appliance.

  For best performance, create an Affinity Group and place the SteelHead-c and its data store in it. Placing the SteelHead-c and its data store in the same Affinity Group ensures a low latency between the appliance and its data disk.

- You can choose among the following three methods to install your SteelHead-c into your Azure environment:
  – Use the PowerShell script packaged with the SteelHead-c image.
  – Use the Azure Portal and the Azure CLI provided by Microsoft, following the instructions in the README included with the SteelHead-c download package.

Installation Prerequisites

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

- You have access credentials to a Microsoft Azure account.
- You have obtained a one-time token from the Riverbed Cloud Portal to license your SteelHead-c. You can access the portal at the following URL:

  https://cloudportal.riverbed.com

Installing a SteelHead-c Appliance on an Azure Virtual Machine

This section provides instructions for installing a SteelHead-c appliance on an Azure VM.

To install using the Microsoft Azure Management portal

1. Login to the Microsoft Azure Management portal.
2. Click New.
3. Select Compute > Virtual Machine > From Gallery.
4. In the Choose an Image screen, select All > Riverbed SteelHead CX.

5. Ensure the following items are configured as listed below:
   - Leave the New User Name item set to its default value.
   - De-select the Upload compatible SSH key for authentication check box.
   - Check the box for Provide a Password.
   - Enter a password.

Note: The user name and password that you create in this step are not used; to log in to your appliance for the first time, use the default credentials of "admin" and "password". After initial log in, you can change your credentials at any time.

---

6. Click the next button ("->").
7. Select the Region/Affinity Group most appropriate to your type of deployment. See "Before Using Your Microsoft Azure SteelHead-c Appliance" on page 59.
8. Click the next button ("->").
9. Add port 7800, 7810, 7850, 443, 80, and 22 to the list of end points. Leave all other items set to their default values.
10. Check the check box to finish provisioning.
11. After the appliance is provisioned, add the datastore disk:
    - Click on Virtual Machines and highlight the your SteelHead-c.
    - Select Attach > Attach Empty Disk and specify the size of the disk as 430 GB.
12. Configure a DNS.
13. License your appliance. See "Managing Licenses" on page 18.

Performing Initial Configuration of Your Azure Appliance

This section describes how to complete the initial configuration of your Azure appliance.

To configure the appliance

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

   Enter **yes** at the system prompt: for example,

   ```
   Configuration wizard.
   Do you want to use the wizard for initial configuration? yes
   ```

Complete the configuration wizard steps on the client-side appliance as described in the following table.

Wizard Prompt	Description	Example
Step 1: Hostname?	Enter the hostname for the appliance.	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 appliance. Riverbed recommends 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 appliance.	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 appliance 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?	Riverbed strongly recommends that you change the default administrator password. The password must be a minimum of 6 characters. The default administrator password is **password**.	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. **Important:** 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. 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`

2. 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 configuration wizard automatically saves your configuration settings.

3. To log out of the system, enter the following command at the system prompt:

```
amnesiac> exit
```

Monitoring Your Azure Appliances

The Riverbed Cloud Portal enables you to monitor your SteelHead-c appliances.

To view information about an appliance

1. In the Cloud Appliances tab on the Riverbed Cloud Portal, click Appliances to display the Appliances page.

2. Click the name of the appliance in the Name column to display the Summary page.

3. In the summary page, complete the configuration as described in the following table.

Parameter	Description
Name	Name of the appliance. This name is specific to the Riverbed Cloud Portal. You can change the name by typing a new name in the text box and clicking **Update Appliance**.
Description	Specify a description for the appliance.
State	Current state of the license. It can have one of the following values: • **Active** - The license associated with the appliance is in use. • **Inactive** - The license associated with the appliance is not in use. • **Unlicensed** - There is no license associated with the appliance.
License	The license that the appliance is using. Click the license name for more details about the license.
Version	The version of Riverbed software running in the virtual machine.
Management Console	Link to the appliance's Management Console.
Update Appliance	Updates the appliance with the changes you made to its name and description.
Reclaim License	Click this button to deregister the appliance and release its license. The appliance reverts to the unlicensed state and is no longer listed on the Riverbed Cloud Portal. It also regenerates the one-time token for the license. You can use the new one-time token to license a different SteelHead-c. After you reclaim its license, you must manually deprovision the appliance's resources in the cloud.

4. Select the Azure Details tab to display the Azure details page for the appliance.

   The Azure Details page displays the following parameters.

Parameter	Description
Uptime	The duration for which the appliance has been running.
Creation Time	The time at which the appliance was provisioned.
Hostname	Name of the host machine on which the appliance is running.
Architecture	The architecture type of the appliance.
CPU Count	Number of CPU cores in the appliance.
Total Memory	Total memory of the appliance, in 1024 byte units.
Primary IP	IP address of the primary interface of the appliance. If you did not assign an IP address for the primary interface, the details page displays this value as **Unknown**.
Aux IP	IP address of the auxiliary interface of the appliance. If you did not assign an IP address for the auxiliary interface, the details page displays this value as **Unknown**.

5. Select the Event Log tab to display the Event Log page.

The event log page displays the following.

Control	Description
Level	Select the minimum severity level for the event log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • **Critical** - Conditions that affect the functionality of the appliance. • **Error** - Conditions that probably affect the functionality of the appliance. • **Warning** - Conditions that could affect the functionality of the appliance, such as authentication failures. • **Notice** - Normal but significant conditions, such as a configuration change. • **Informational** - Informational messages that provide general information about system operations. • **Debug** - Messages that help you debug a failure.
Records	Specify the maximum number of records to display. The default value is **20**.
Timestamp	Date and time at which the event occurred. Click the arrow to sort this column in descending order.
IP Address	IP address of the client machine that initiated the action.
User	Name of the user who performed the action.
Log Level	Severity level of the log message.
Message	Log message that describes the action that occurred.

Upgrading Your Azure SteelHead-c Appliance

You can upgrade the appliance's software using the Software Upgrade page in the same way that you upgrade software on the SteelHead. For details, see *SteelHead Management Console User's Guide*.

Note: SteelHead-c images are posted in the Software > Cloud SteelHead section of the Riverbed Support site.

To upgrade an appliance model, use the following procedure:

1. Purchase and install the new license. For details about installing a license, see "Managing Licenses" on page 18.
2. Re-configure the virtual machine so that it has the resources necessary to host the model SteelHead-c you want.

CHAPTER 6 Using Amazon Virtual Private Cloud

This chapter describes the Amazon Virtual Private Cloud (VPC). It includes the following 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).

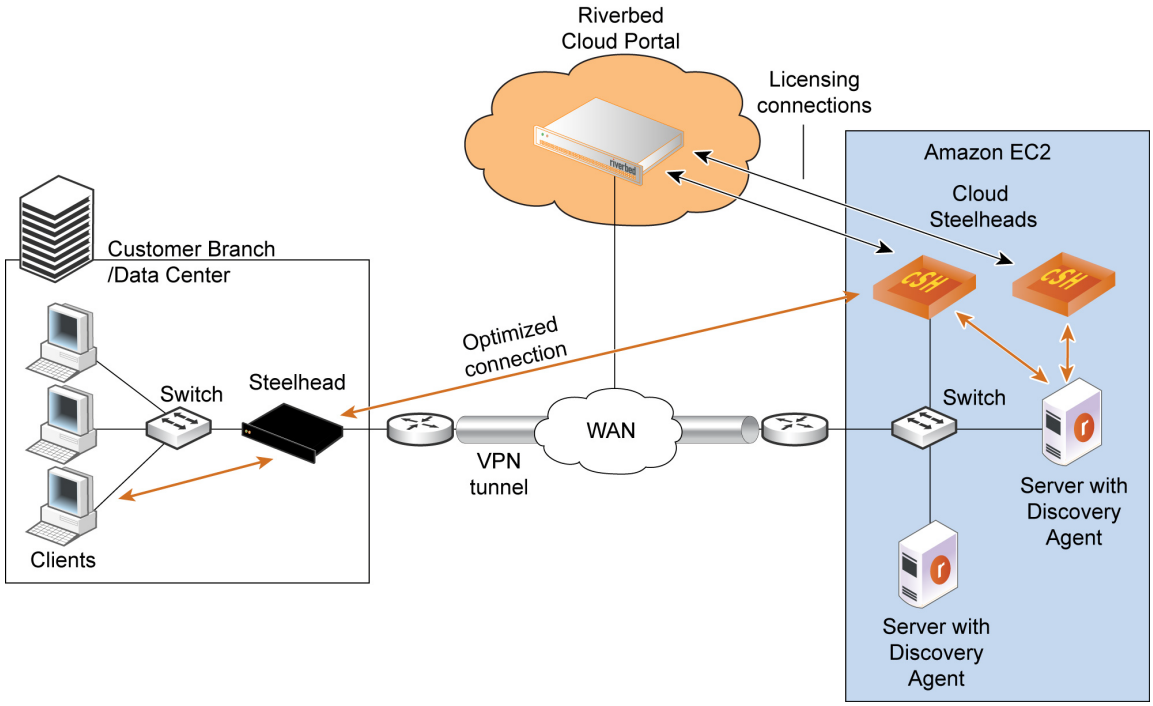
The following section describes how to deploy SteelHead-cs using different levels of security and includes configuration caveats.

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 auto-discovery and auto-reconfiguration (when instances change their IP addresses, the portal automatically detects it) works.

Figure 6-1 shows how to deploy SteelHead-cs and servers in Amazon VPC with a VPN connection to the data center.

Figure 6-1. Using Amazon VPC Through a VPN Tunnel (Without NAT)



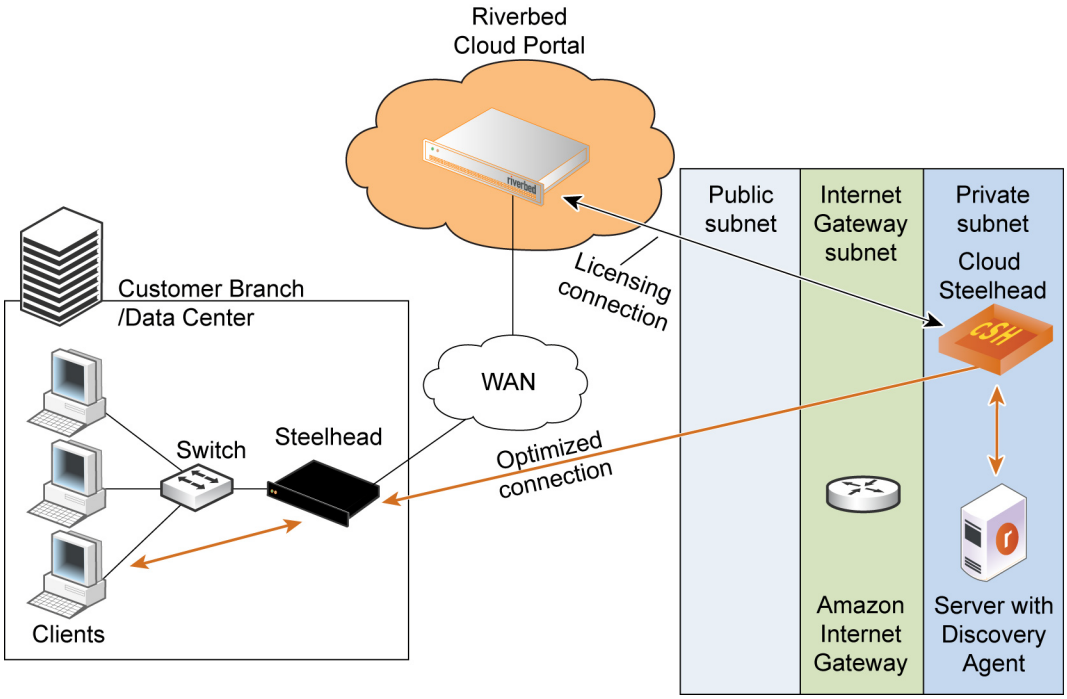
In the network shown in Figure 6-1, servers in Amazon use private IP addresses. The VPC with VPN tunnel provides an extension of your intranet into Amazon AWS.

Using a VPC Without a VPN Connection to the Data Center

When you use you 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. For details about AWS, see http://aws.amazon.com/documentation/.

Figure 6-2 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 6-2. 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).

On the security group of the AWS EC2 instances running the Discovery Agent:

Connecting to the VPC Through the VPN (Without NAT)

To configure a VPC through the VPN, in 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).

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)

To configure a VPC without IPSec tunnel, in 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 appliances in the customer data center.
2. Add the security group of the SteelHead-c (enable access to all ports).

On the SteelHead-c security group:

1. Add the public IP address of the machines that access the server from outside the VPC, such as the appliances in the customer data center.
2. Enable access to port 7800 and port 7810 for TCP
3. Add the private IP addresses of all local AWS instances running the Discovery Agent, allowing access to all ports for TCP and UDP, if the AWS instances want to connect to a server on the Internet.

APPENDIX A Provisioning an AWS SteelHead-c Manually

This appendix describes how to provision a SteelHead-c in the Amazon Web Services (AWS) cloud without using the Riverbed Cloud Portal. For Amazon AWS, EC2, and VPC documentation, go to:

http://aws.amazon.com/documentation/.

This appendix includes the following sections:

To provision an AWS SteelHead-c manually, you create two Elastic Block Store (EBS) volumes, use the EC2 Classic Wizard to create the AWS SteelHead-c instance, and after it boots and displays the status "running", attach the volumes to the AWS instance.

Creating EBS Volumes

This section describes how to create the EBS volumes, Configuration Volume and Datastore Volume.

Creating the Configuration Volume

Configuration Volume is the volume that the SteelHead-c uses to store its configuration and logs. You must allocate 30 GiB as the size for all SteelHead-c models except SteelHead-c-250-H and the CCX-255 models. Specify 10 GiB as the size for those models.

To create the Configuration Volume

1. Log in to the AWS Management Console at console.aws.amazon.com.
2. Enter your user name and password and click **Sign in using our secure server**.
3. Click EC2 to display the EC2 page.
4. Click **Volumes** in the navigation pane.

5. Click **Create Volume** to display the Create Volume dialog box.
6. In the Create Volume dialog box, leave the Volume Type as Standard.
7. Specify 30 GiB as the Size for all SteelHead-c models except SteelHead-c-250-H and the CCX-255 models. Specify 10 GiB as the size for those models.
8. Select the availability zone from the drop-down list. Ensure that you select the same availability zone where you plan to launch the instance. In this example, you select us-east-1b.
9. Click **Yes, Create** to create the Configuration Volume.

Note: The system names the SteelHead-c instance based on the Configuration Volume ID.

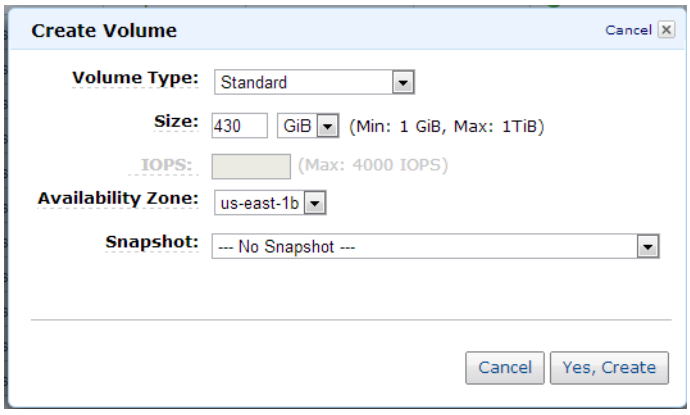
Creating the Datastore Volume

To store the data store on a persistent EBS volume, you must create a second volume that is 430 GiB in size. Ensure that you create the data store zone in the same availability zone where you plan to launch the instance.

To create the Datastore Volume

1. Log in to the AWS Management Console at console.aws.amazon.com.
2. Enter your user name and password and click **Sign in using our secure server**.
3. Click EC2 to display the EC2 page.
4. Click **Volumes** in the navigation pane.
5. Click **Create Volume** to display the Create Volume dialog box again.

Figure 6-3. Create Volume Dialog Box - Data Store Volume



6. Leave the Volume Type as Standard.
7. Specify 430 GiB (at least 430 GiB minimum) as the Size.

8. Select the availability zone from the drop-down list. Ensure that you select the same availability zone where you plan to launch the instance. In this example, you select us-east-1b.

9. Click **Yes, Create** to create the Datastore Volume.

Launching an AWS SteelHead-c Instance

This section describes how to create an AWS SteelHead-c instance and boot it.

To complete this process you must provide an AMI, security group, key pair, and one-time token. Ensure that you determine these values before beginning the process.

To create an AWS SteelHead-c instance

1. Click **Instances** in the navigation pane to display the instances page.

2. Click **Launch Instance** to display the EC2 wizard page.

3. Select the Classic Wizard and click **Continue** to display the Choose an AMI page.

4. Select the My AMIs tab.

5. Select the AMI that you want to launch from the list.

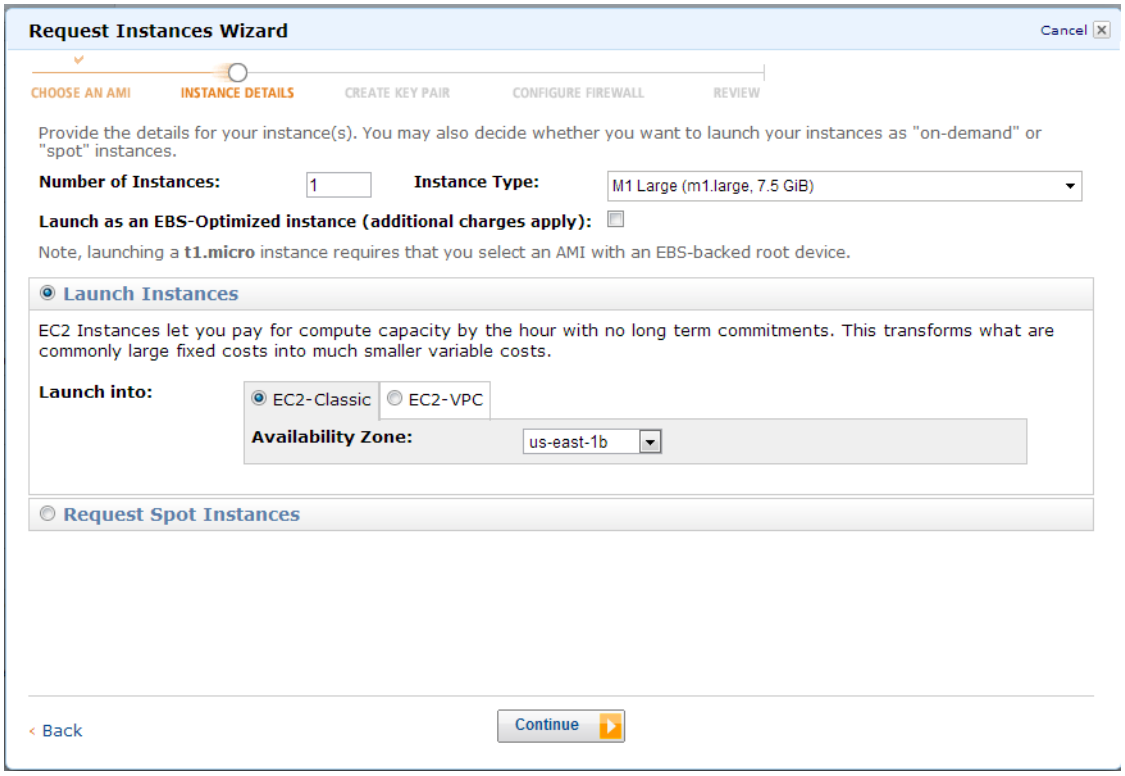
Note: Contact Riverbed Support (at https://support.riverbed.com) for the correct AMI ID. The AMI must be authorized to launch your AWS account; therefore, you must provide your AWS credentials to Riverbed Support so that they can enable your AWS account with permissions to launch the AMI.

Choose the AMI you want to launch based on the following factors:

- SteelHead-c software version you want to run
- SteelHead-c model you want to provision
- AWS region in which you want to provision

6. Click **Select** to display the Instance Details page.

Figure 6-4. Instance Details Page - Availability Zone Section



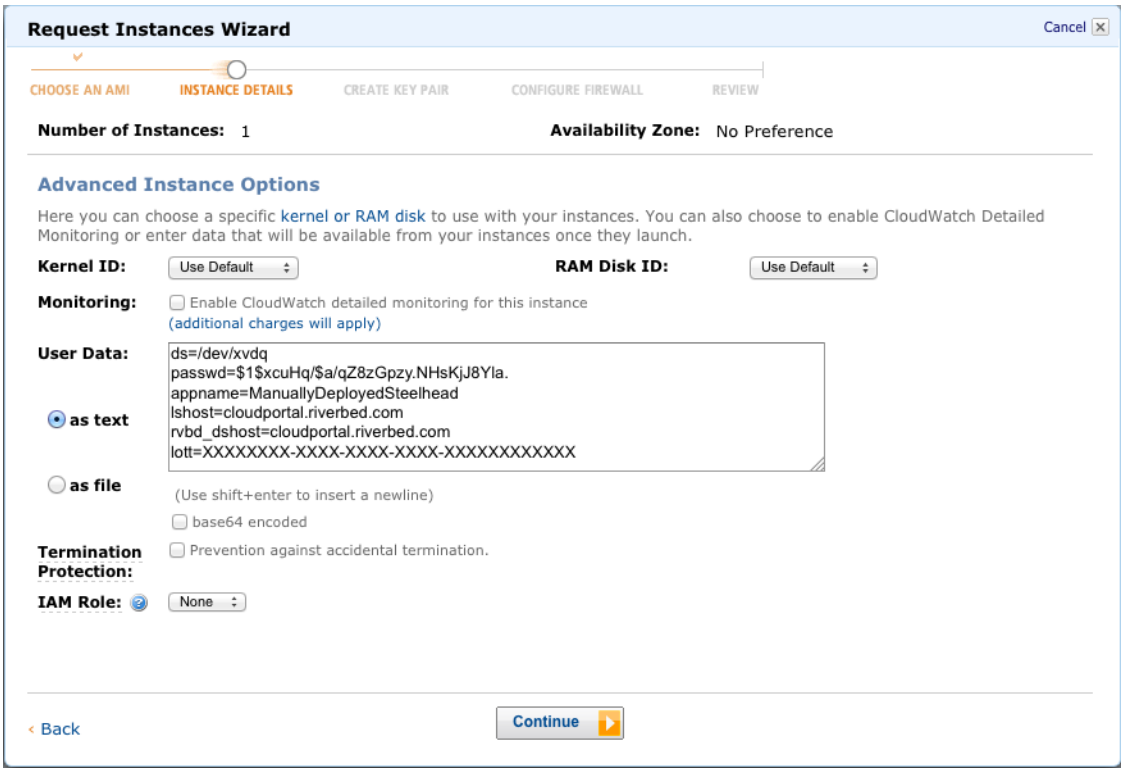
7. Select an instance type (m1.large for all SteelHead-c models except SteelHead-c-250) from the drop-down list. Select m1.small for SteelHead-c-250 models.

8. Under Launch Instance, select EC2-Classic.

9. Select the availability zone from the drop-down list. Ensure that you select the same availability zone where you plan to launch the instance. In this example, you select us-east-1b.

10. Click **Continue** to display the User Data page.

Figure 6-5. Instance Details Page - User Data Section



11. Under User Data, click **as text**.

12. Type the following user data in 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
```

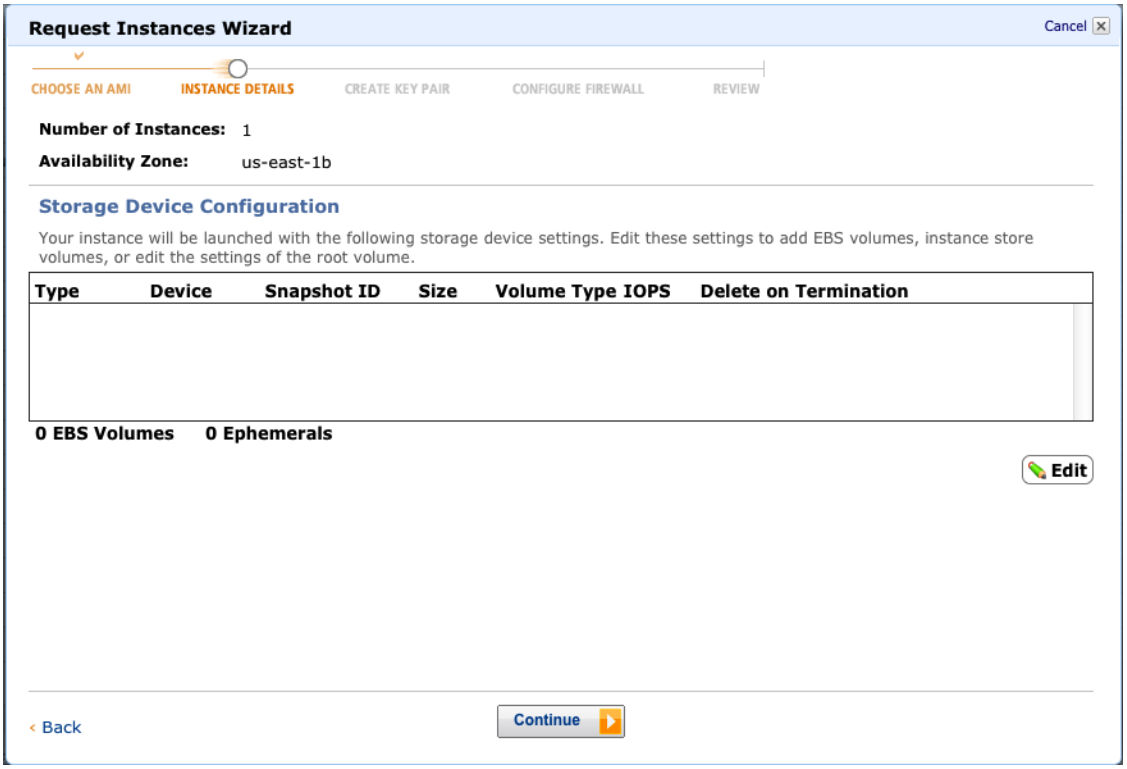
where:

- ds - The device node in which the SteelHead-c expects the Datastore EBS volume to appear. Due to changes in EC2 architecture, leave set this to /dev/xvdq. It matches the /dev/sdm device node mapping you set for the Datastore 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 user name “admin” and password “thepassword”. Ensure that you change the 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 is usually the Riverbed Cloud Portal.
- rvbd_dshost - Fully qualified domain name of the discovery server. This 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.

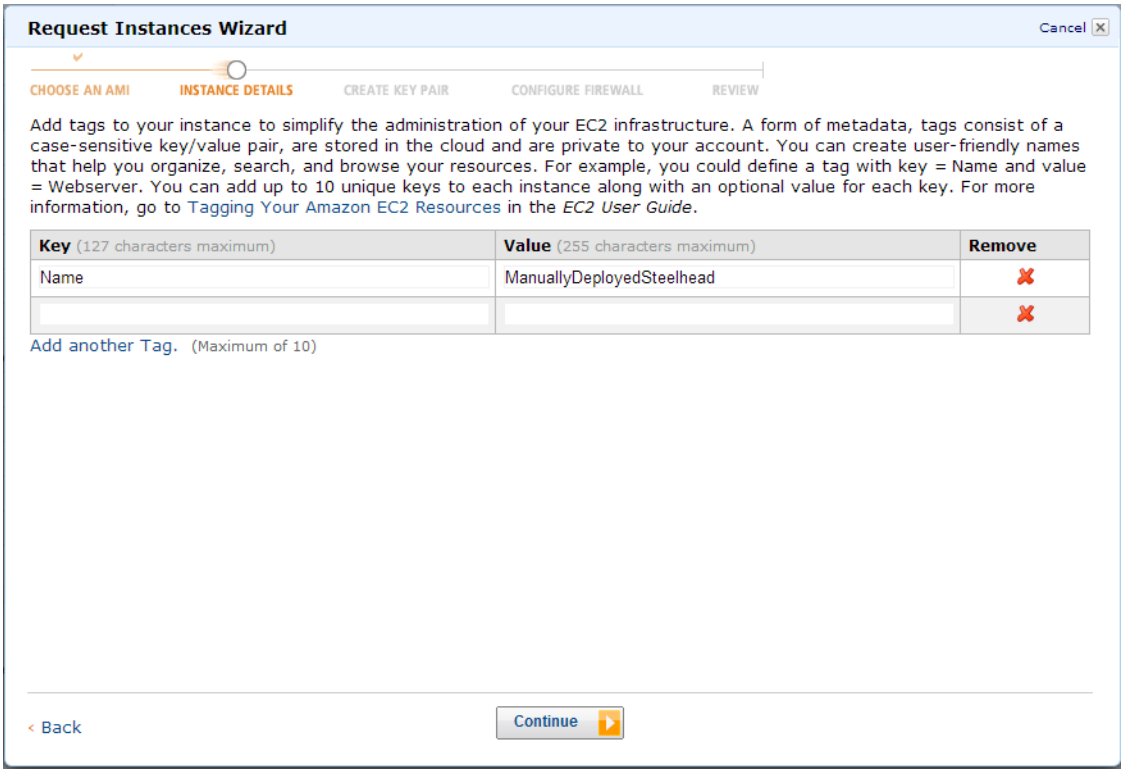
13. Click **Continue** to display the Storage Device Configuration section of the Instance Details page.

Figure 6-6. Instance Details Page - Storage Device Configuration Section



14. Leave the storage device configuration section blank and click **Continue** to display the Adding Tags section of the Instance Details page.

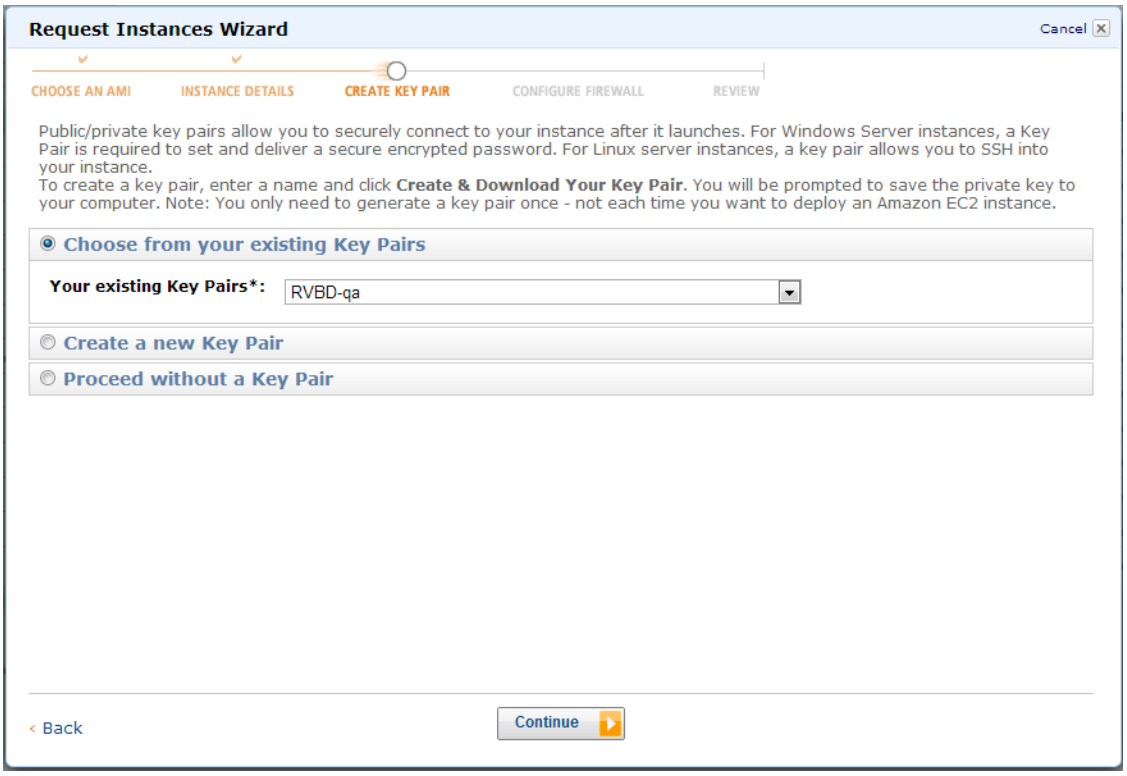
Figure 6-7. Instance Details Page - Adding Tags



15. Under Value, type a value for the key Name (in this example: **ManuallyDeployedSteelHead**). This name appears in the instances listed after you launch the instance. It helps you find your instance when you want to attach the EBS volumes to the instance.

16. Click **Continue** to display the Create Key Pair page.

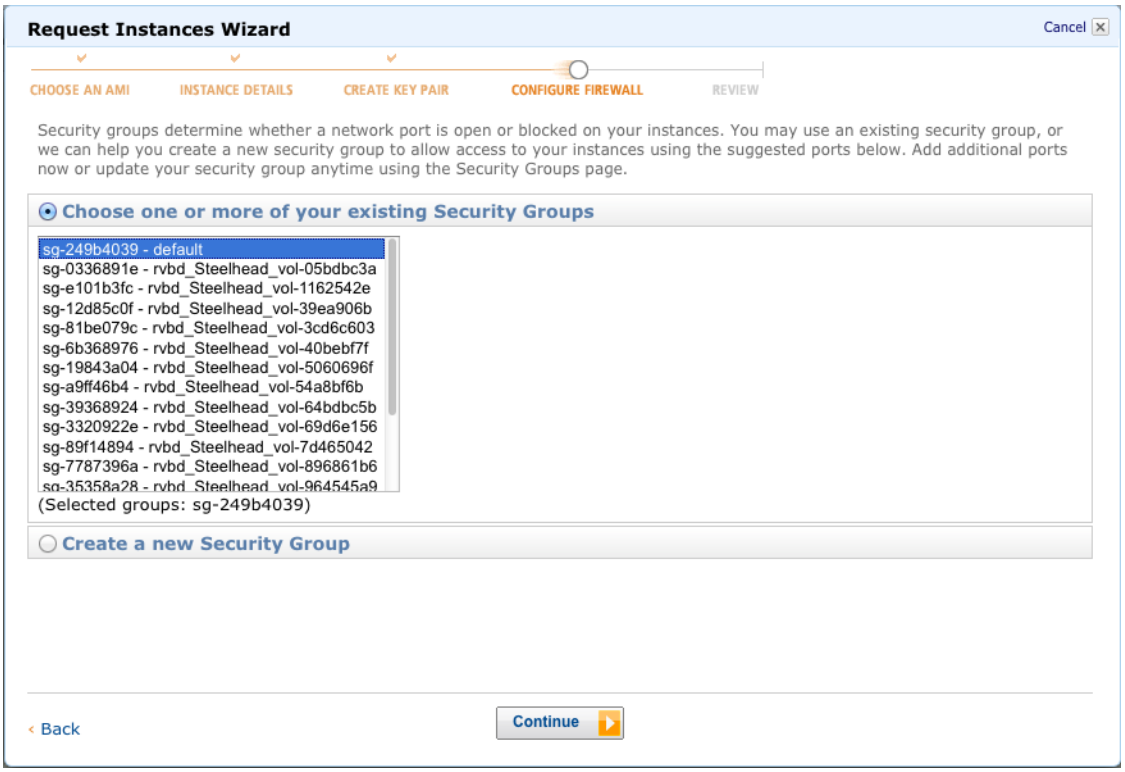
Figure 6-8. Create Key Pair Page



17. Select an existing key pair from the drop-down list.

18. Click **Continue** to display the Configure Firewall page.

Figure 6-9. Configure Firewall Page



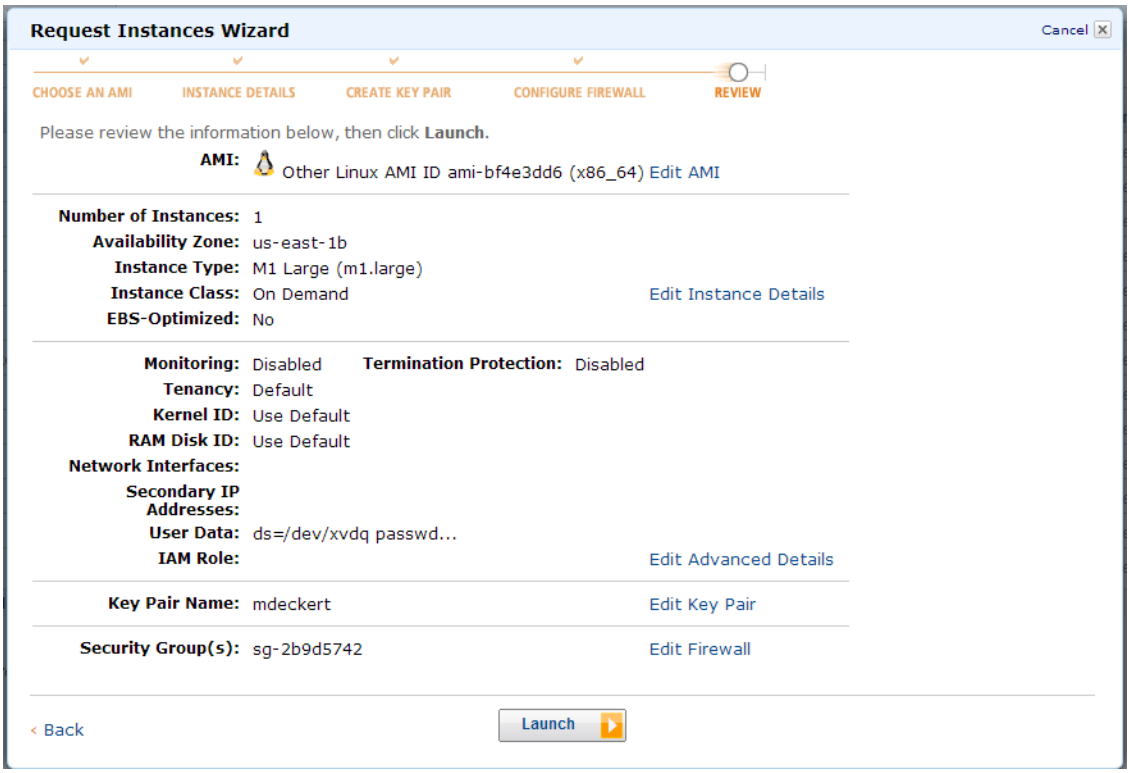
19. Scroll and choose a security group to add the instance.

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

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

20. Click **Continue** to display the Review page.

Figure 6-10. Review Page

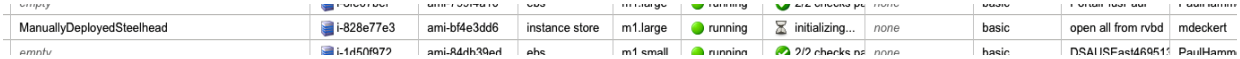


21. Review the instance details.

22. Click **Launch** to launch the instance.

23. The AWS page displays the instance status as pending and then running.

Figure 6-11. Instance Status Page



Attaching the EBS Volumes to the Instance

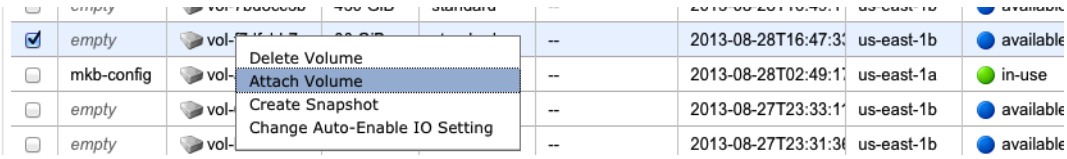
After you create and boot a SteelHead-c instance, and it is in the “running” state, you attach the Configuration Volume to the instance.

To attach the Configuration Volume to the SteelHead-c instance

1. Click **Volumes** in the navigation pane to display the Volumes page that contains both the Configuration Volume and the Datastore Volume.

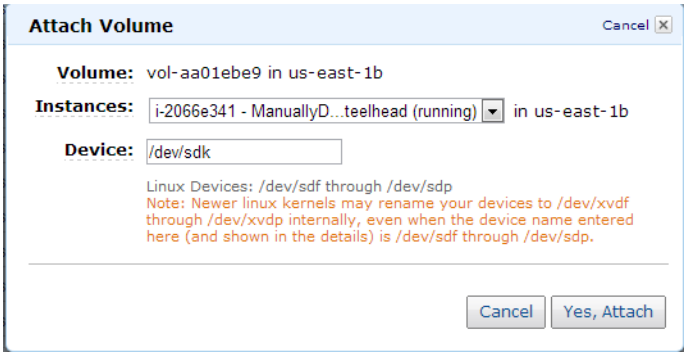
2. Right-click the Configuration Volume that you created to display a menu of actions that you can perform on the volume.

Figure 6-12. Attach Volume Menu



3. Select Attach Volume to display the Attach Volume dialog box.

Figure 6-13. Attach Volume Dialog Box



4. In the Attach Volume dialog box, select an instance name from the drop-down list.

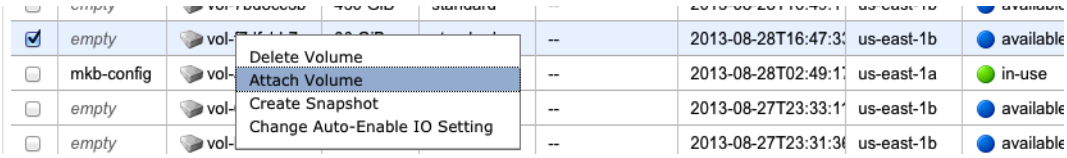
5. Specify /dev/sdk as the Device name for the Configuration Volume.

6. Click **Yes, Attach**.

To attach the Datastore Volume to the SteelHead-c instance

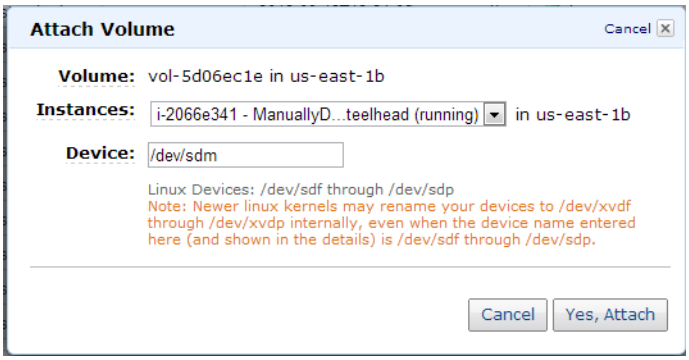
1. Right-click the Datastore Volume that you created to display a menu of actions that you can perform on the volume.

Figure 6-14. Attach Volume Menu



2. Select Attach Volume to display the Attach Volume dialog box.

Figure 6-15. Attach Volume Dialog Box



3. In the Attach Volume dialog box, select the instance name from the drop-down list.

4. Specify /dev/sdm as the Device name for the Datastore Volume.

5. Click **Yes, Attach**.

Connecting to the SteelHead-c Management Console

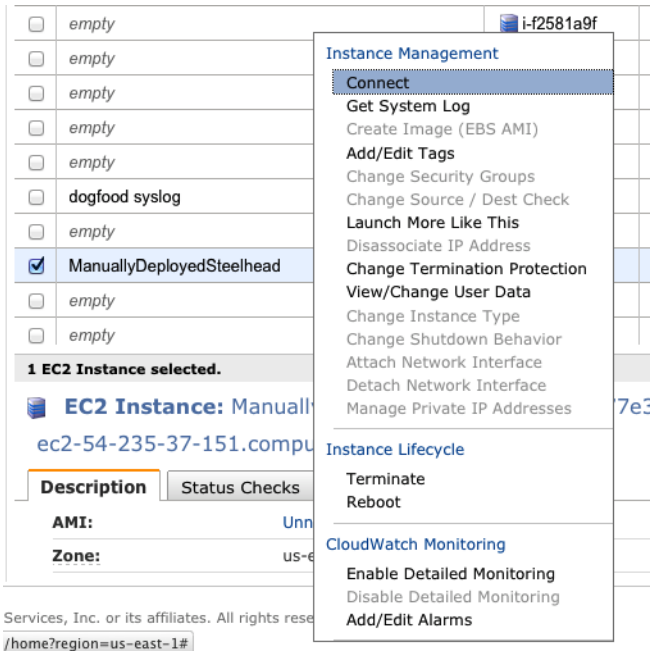
After you attach the EBS volumes to the SteelHead-c instance, you can log in to the SteelHead-c Management Console and optimize connections.

To connect to the SteelHead-c Management Console

1. Click **Instances** in the navigation pane to display the instances page.

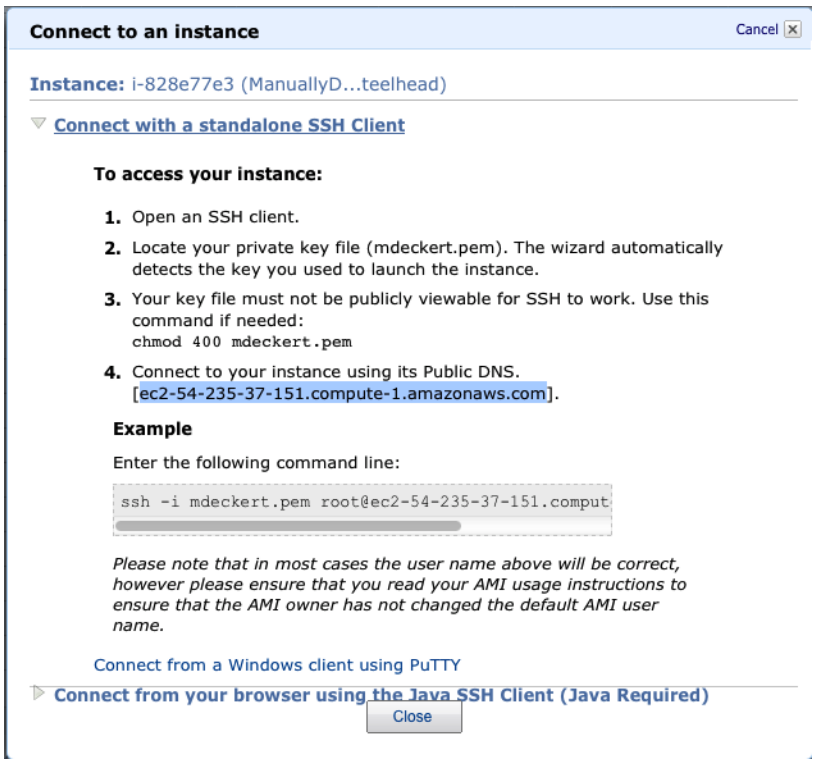
2. Right-click the name of the instance that you launched to display the Instance Management menu.

Figure 6-16. Instance Management Menu



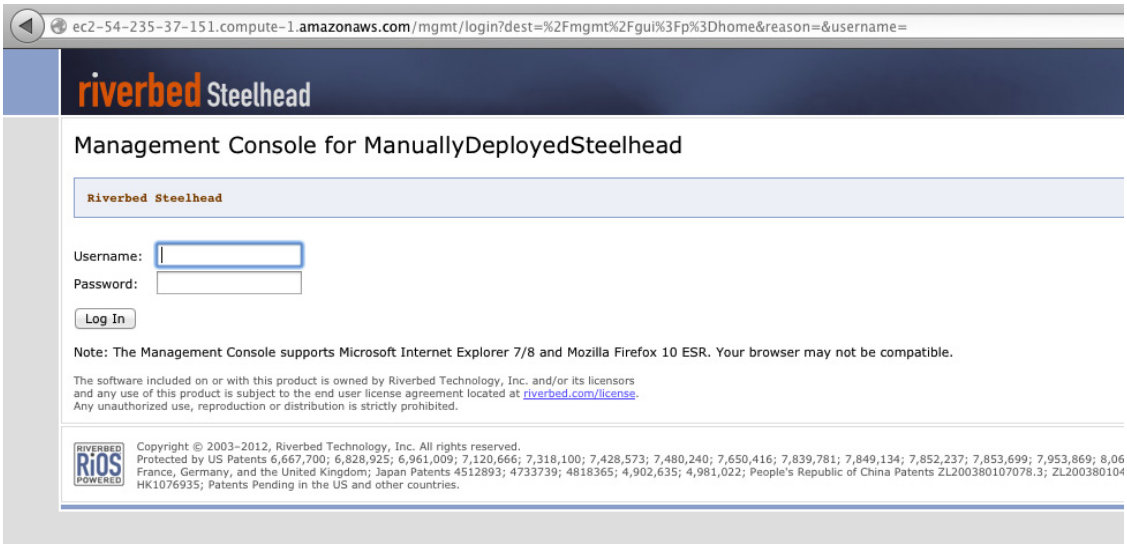
The system displays the Connect to an instance page.

Figure 6-17. Connect To An Instance Page



3. Copy the public DNS name of the instance from this page and paste it into a browser window to display the SteelHead-c Management Console (after a few minutes).

Figure 6-18. SteelHead-c Management Console



Note: The SteelHead-c loads the attached volumes and then boots. You might have to wait for a few minutes for the Management Console to appear.

---

4. Log in to the SteelHead-c Management Console using your username and password.

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

The system automatically adds it to the default optimization group. You can also add it to other optimization groups.

Upgrading the RiOS Version

You cannot upgrade the RiOS image on an AWS SteelHead-c in the same way that you upgrade it on physical SteelHeads. If you provisioned your SteelHead-c using the Riverbed Cloud Portal, you can also upgrade the RiOS version through the Riverbed Cloud Portal. For manually provisioned SteelHead-c appliances, use the following steps:

1. Stop the SteelHead-c instance by terminating the associated EC2 instance.

2. Launch a new EC2 Instance using the new AMI desired and same launch parameters that you used the first time.

3. Re-attach the Configuration Volume and Datastore Volume associated with the old instance.

The new and upgraded SteelHead-c image is ready to use again.

The SteelHead-c IP addresses change after this step. Ensure that you update any rules or configurations that depend on it.

Managing the SteelHead-c

You can stop, start, or deprovision the SteelHead-c in the AWS cloud.

Stopping the SteelHead-c

To stop the SteelHead-c, simply terminate the associated EC2 instance.

Starting the SteelHead-c

To start the SteelHead-c, launch a new EC2 instance using the same AMI and user data and re-attach the Configuration Volume to /dev/sdk and the Datastore Volume to /dev/sdm.

Deprovisioning the SteelHead-c

To deprovision the SteelHead-c, terminate the EC2 instance and delete the Configuration Volume and all Datastore Volumes.

Index