

Cloud Steelhead Appliance® Quick Reference

This quick reference card provides quick start information for the Cloud Steelhead appliance (CSH). For details, see the *Riverbed Cloud Services Deployment Guide* and the *Steelhead Management Console User’s Guide* on the Riverbed Support site located at <https://support.riverbed.com>.

Deploying the CSH in AWS

Provisioning the AWS CSH

1. Log in to cloudportal.riverbed.com.
2. Click an available license, then click **Provision to AWS**, and follow prompts.
3. Go to the AWS Details page on the Riverbed Cloud Portal and find the IP address of the CSH.
4. Start an SSH session to the CSH.
5. Enter the command **show licenses**.
6. Check that the license status is active. It can take up to 10 minutes for the license to be first checked out of the Riverbed Cloud Portal, after the system boots.

Installing and Configuring the Discovery Agent

1. To enable the Discovery Agent, from the CSH CLI, type the following commands:

```
in-path agent-intercept enable
in-path enable
```
2. Download the Discovery Agent on your AMI appliance from <https://support.riverbed.com/software/cloud.htm>.
3. Create an optimization group from the Riverbed Cloud Portal.
4. Add the CSH and a server to the optimization group.
5. Install the Discovery Agent.
6. In the Riverbed Cloud Portal, choose Optimization Group > Server entry. Copy the Client ID and Client Key and paste the strings into the Discovery Agent setup wizard and complete the installation.
7. Check that the CSH and Discovery Agent are connected.

Configuring Security Groups

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

1. Add the public IP address of the remote site for the ports used by the application to optimize.
2. Add the security group of the CSH (enable access to all ports).

On the CSH security group:

- Add the public IP address of the remote site and enable it to access port 7800 and port 7810.

You can configure security groups for VPC optimization either over a VPN tunnel or through an Internet gateway.

Option 1 - Configuring security groups for VPC optimization over a VPN tunnel

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

1. Add the private IP address of the remote site for the ports used by the application to optimize.
2. Add the security group of the CSH (enable access to all ports).

On the CSH security group:

- Add the private IP address of the remote site and enable it to access port 7800 and port 7810.

Option 2 - Configuring security groups for VPC optimization through an Internet gateway

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

- Add the public IP address of the appliances that access the server from outside the VPC (such as appliances in the customer data center).

On the CSH security group:

1. Add the public IP address of the remote Steelhead and enable it to access port 7800 and port 7810.
2. Add the private IP addresses of all local AWS instances running the Discovery Agent, enabling access to all ports. This step is required only if the AWS instances want to connect to a server on the Internet.

Configuring Enterprise firewalls

1. Enable outgoing access to port 7800.
2. Ensure that TCP options are allowed through the firewall.

Deploying the CSH on a VMware ESX Cloud

Installing the ESX CSH

1. Download the CSH OVA file from:
<https://support.riverbed.com/software/cloud.htm>
2. Either, from the vSphere Client:
 - Choose File > Deploy OVF Template and follow prompts.

Or, from the vCloud Director:

1. Create an entry in the account catalog.
 - Choose Catalogs > vAPP Templates > Upload.
2. Deploy the CSH vAPP from the catalog:
 - Choose MyCloud > vApp > Add from Catalog.

Note: The vCloud Director cannot handle OVA files. To convert the OVA file to OVF format, change the file type to .tar and then extract it using Winzip-7 or a similar tool.

3. Change the virtual hardware configuration to match the model you selected.

The following table shows the vCPU and memory for different ESX Cloud Steelhead models.

Model	vCPU	Memory (reserved)
CSH-250-L	1 (1200 MHz)	2 GB
CSH-250-H	1 (1200 MHz)	2 GB
CSH-550-H	2 (1200 MHz)	3 GB
CSH-1050-M	2 (1800 MHz)	3 GB
CSH-1050-H	2 (1800 MHz)	4 GB
CSH-2050-L	4 (2000 MHz)	6 GB
CSH-2050-LT	4 (2000 MHz)	6 GB
CSH-2050-LXT	4 (2000 MHz)	6 GB

4. Connect the primary (#1) and then the auxiliary (#2) interfaces.
5. Configure the IP address, netmask, default gateway, and DNS server of the primary interface.
6. Obtain the one-time token from the Riverbed Cloud Portal and configure the token on the CSH either through the command-line interface or the Management Console.
7. Go to the AWS Details page on the Riverbed Cloud Portal and find the IP address of the CSH.
8. Start an SSH session to the CSH.
9. Enter the command **show licenses**.
10. Check that the license status is active. It can take up to 10 minutes for the license to be first checked out from the Riverbed Cloud Portal, after the system boots.

Using the Discovery Agent for traffic redirection

1. To enable the Discovery Agent, from the CSH CLI, type the following commands:

```
in-path agent-intercept enable
in-path enable
```
2. Download the Discovery Agent on your VPC instance from <https://support.riverbed.com/software/cloud.htm>.
3. Run the Discovery Agent installation wizard.
4. In the Discovery Agent installation wizard, select the cloud type **Other**.
5. Click **Skip** on the Riverbed Portal Configuration page and select the Manual configuration mode.
6. After the installation is complete, in the Discovery Agent UI choose Settings > Configure and add the IP address of the CSH.
7. Choose Support > Restart Service on the Discovery Agent UI.
8. Check that the CSH and Discovery Agent are connected.

Configuring NAT IP Address mapping

1. On the CSH, choose Configure > Optimization > NAT IP Address Mapping to display the NAT IP Address Mapping page.
2. Check the **Enable Address Mapping Support** check box.
3. Select **Add a New Map**, specify the Public IP and Private IP, and click **Add**.

Configuring WCCP

1. On the CSH, choose Configure > Optimization General Service Settings to display the General Service Settings page.
2. Check the **Enable In-Path Support** checkbox and under it check the **Enable L4/PBR/WCCP/Interceptor Support** checkbox.
3. Choose Configure > Networking > WCCP to display the WCCP page.
4. Check the **Enable WCCP v2 Support** checkbox.
5. Specify the TTL (Time to Live) boundary for the WCCP protocol packets in the Multicast TTL text field. The default value is 16.
6. Select **Add a New Service Group** and specify the Interface, Service Group II, Protocol, Password, Password Confirm, Priority, Weight, Encapsulation Scheme, Assignment Scheme, Source Mask, Destination Mask, Source Hash, Destination Hash, Ports, and Router IP Address(es).
7. Click **Add**.
8. Configure the same service group on the router.

