riverbed®

# SteelCentral Controller for SteelHead™ (Virtual Edition) Installation Guide

Version 9.9

March 2019

riverbed®

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

Part Number
712-00052-15

# Contents

# Welcome

## About this guide

Welcome to the *SteelCentral Controller for SteelHead (Virtual Edition) Installation Guide*. This guide describes how to install and configure the SteelCentral Controller for SteelHead (virtual edition) (SCC-VE).

## Audience

This guide is written for storage and network administrators who are familiar with administering and managing WANs using common network protocols such as TCP, CIFS, HTTP, FTP, and NFS.

This guide assumes you're familiar with configuring the SteelHead CX, SteelHead EX, and Interceptor.

This guide includes information relevant to these products and product features:

- Riverbed SteelCentral Controller for SteelHead (SCC)
- SteelCentral Controller for SteelHead (virtual edition) (SCC-VE)
- Riverbed SteelHead (SteelHead)
- Riverbed Optimization System (RiOS)

## Document conventions

This guide uses this standard set of typographical conventions:

| Convention | Meaning |
|---|---|
| *italics* | Within text, new terms and emphasized words appear in *italic* typeface. |
| **boldface** | Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface. |
| Courier | Code examples appear in Courier font:<br>`amnesiac > enable`<br>`amnesiac # configure terminal` |
| < > | Values that you specify appear in angle brackets: **interface <ip-address>** |
| [ ] | Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]** |
| { } | Elements that are part of a required choice appear in braces: **{<interface-name> \| ascii <string> \| hex <string>}** |
| \| | The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: **{delete <filename> \| upload <filename>}** |

# Documentation and release notes

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

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

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

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

# Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - Problems installing, using, or replacing Riverbed products? Contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415-247-7381 outside the United States. You can also go to https://support.riverbed.com.
- **Professional services** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.

- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

# 1

# Overview of the SCC-VE

This chapter provides an overview of the SCC-VE: a virtualized appliance of the SteelCentral Controller for SteelHead specifically designed for customers (such as Managed Service Providers) and users who need to centrally manage multiple, separate deployments of the Riverbed system on behalf of their customers. This chapter includes these sections:



## New features in 9.9

These new features are available in version 9.9:

- Updated VMware Tools to version 10.1.0. Learn about known issues and workarounds for this version of VMware tools here:

  https://docs.vmware.com/en/VMware-Tools/10.1/rn/vmware-tools-1010-release-notes.html#knownissues

- SCC-VE is supported on Microsoft Azure Hyper-V and available in the Microsoft Azure marketplace.

## Prerequisites

This section describes the prerequisites necessary to install the product.

### Product licensing

All licensing must be properly in place. Appliances can still be managed if appliance licenses are valid and available.

You need to have valid licenses installed on all appliances that you want to manage with the SCC-VE.

A missing base license on an appliance can cause the health of the SCC-VE to become critical and temporarily invalidates other SCC-VE licenses which in turn prevents management of appliances.

## Networking requirements

You can access each SCC-VE instance through HTTP, HTTPS, or SSH. You can configure the default access protocol in the Management Console. For details, see the *SteelCentral Controller for SteelHead User Guide*.

For SteelHead management, each SCC-VE instance requires port 80 and port 443 inbound from the SteelHeads and port 22 outbound from each SCC-VE instance to SteelHeads.

## Hardware requirements for VMware infrastructure client

The installation process requires accessing the VMware Infrastructure Client (VIC) on a Windows workstation. For requirements, see the VMware documentation.

## Hardware requirements per SCC-VE instance

The SCC-VE consists of three files:

- Hard disk 1 contains the operating system. The default value is 39 GB.
- Hard disk 2 is for statistics storage and must be provisioned according to the following table. The default value is 5 GB.
- Hard disk 3 is for RSP image and package management and must be provisioned based on total size of the image and package files. The default value is 2 GB.

The total datastore space required for the SCC-VE is the sum of the three VMDK files with a minimum value of 32 GB to a maximum of over 400 GB.

| Number of appliances managed | Hard disk 2 | RAM | CPU (effective) |
|---|---|---|---|
| Up to 50 | 50 GB | 4 GB | 2 core, 2 GHz |
| Up to 100 | 100 GB | 6 GB | 2 cores, 2 GHz |
| Up to 250* | 250 GB | 6 GB | 2 cores, 2 GHz |
| Up to 500* | 400 GB | 16 GB | 4 cores, 2.4 GHz |
| Up to 1500* | 400 GB | 32 GB | 4 cores, 4 GHz |

* Use the 64-bit SCC-VE when managing more than 100 appliances.

## Third-party software requirements.

| Component | Description |
|---|---|
| VMware | VMware ESXi 6.0, 6.5 |
| SCC Management Console | The SCC has been tested with Mozilla Firefox Extended Support Release version 38 and Microsoft Internet Explorer 11.<br>JavaScript and cookies must be enabled in your web browser. |

# Overview of the SCC-VE

The SCC-VE facilitates these administrative tasks as a multitenant solution for managing deployments of the Riverbed system across parallel network environments.

- **Multiple Instances** - The SCC-VE is a virtual appliance that's installed in your VMware ESXi cluster. You can run multiple SCC-VE instances, provided that the ESXi platform has sufficient hardware resources and the appropriate licenses are available.
- **Configuration** - The SCC-VE enables you to automatically configure new SteelHead groups or to send configuration settings to appliances in remote offices. The SCC-VE uses configuration objects (that is, policies and groups) to facilitate centralized configuration and reporting.
- **Monitoring** - The SCC-VE provides both high-level status of and detailed statistics about the performance of SteelHeads and enables you to configure event notification for managed SteelHeads.
- **Management** - The SCC-VE enables you to start, stop, restart, and reboot remote SteelHeads. You can also schedule jobs to send software upgrades and configuration changes to remote appliances or to collect logs from remote SteelHeads.
- **Partial Federation** - You can put any appliance into branch-managed mode to prevent configuration changes or maintenance operations from the SCC-VE. The SCC-VE continues to monitor and gather statistics from appliances that are branch managed.
- **Operations History** - The Operations History page in the Management Console lists all of the actions related to configuring SteelHeads that have been performed and indicates whether they were successful or not.

# VMware ESXi

VMware ESXi is a virtualization platform that enable you to install and run the SteelCentral Controller for SteelHead as a virtual appliance. For details about VMware ESXi, see http://www.vmware.com.

For details about implementation requirements for the SCC-VE, see "Prerequisites" on page 9.

# 2

# Managing Riverbed Licenses

This chapter describes the Riverbed licensing methods and how to manage Riverbed licenses. It includes these sections:



## Riverbed licensing methods

A license is a string issued by Riverbed that embeds information that ties the license to data to prevent tampering. After you install the license, the system saves it in the configuration database and enables the functionality associated with the license. Riverbed employs these licensing methods:

- **Automatic licensing** - Once you connect your SteelCentral Controller for SteelHead (virtual edition) to the network, the appliance automatically contacts the Riverbed Licensing Portal which downloads and installs the licenses.
- **Manual licensing** - You can manually fetch and activate licenses for Riverbed products using the Riverbed Licensing Portal. Go to https://licensing.riverbed.com/index.htm and follow the instructions to retrieve license keys. After you manually retrieve your license keys, you need to install them on the appropriate appliance.
- **Factory licensing** - You can have all your Riverbed licenses installed at the factory for a small fee.
- **Token method** - You use tokens to activate Riverbed software, such as the Virtual SteelCentral Controller for SteelHead Mobile, Virtual SteelStore, SteelHead (virtual edition) appliance, and Core-v. For detailed information, see the respective installation guides for these products.

**Note:** Client keys are replacing tokens starting in RiOS 9.6.

# Automatic licensing

Automatic licensing allows the appliance, once connected to the network, to automatically contact the Riverbed Licensing Portal to retrieve and install license keys onto the appliance. Automatic licensing simplifies inventory management and provides an automated mechanism of fetching licenses for Riverbed products without having to manually activate individual appliances and licenses.

If you are behind a firewall, you can retrieve licenses at the Riverbed Licensing Portal using the email option or by downloading and XML file to the SteelCentral Controller for SteelHead. For detailed information, see "Retrieving licenses using the Riverbed Licensing Portal" on page 14.

Automatic licensing also works over a web proxy. For details on setting up a web proxy, see the *SteelCentral Controller for SteelHead User Guide*.

**Note:** If automatic licensing fails, an error message appears in the Management Console. Go to the Riverbed Licensing Portal and follow the instructions for retrieving your licenses.

**To download licenses on a new appliance**

- Connect the new SCC-VE to the network.

  The SCC-VE automatically contacts the Riverbed Licensing Portal and downloads and installs the licenses. The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message.

**To replace expired licenses**

- Purchase new downloadable licenses to replace the expired license.

  At the time of the next scheduled automatic license fetch, the SCC-VE automatically contacts the Riverbed License Portal and downloads the new licenses. The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message. You do not need to delete the expired license. The system uses the license with the latest expiration date.

# Manual and token licensing using the Riverbed Licensing Portal

You can retrieve and manage Riverbed licenses using the Riverbed Licensing Portal. Once you retrieve a license from the Riverbed Licensing Portal, you need to install it.

## Retrieving licenses using the Riverbed Licensing Portal

The licensing portal requires a unique product identifier to retrieve a license. Depending on the product, the identifier can be a serial number, license request key (activation code), or a token. The steps to retrieve a license vary based on the product identifier. Online instructions guide you through the process.

**To retrieve your licenses for a virtual appliance using a token**

1. Go to the Riverbed Licensing Portal at https://licensing.riverbed.com/index.htm.
2. Enter your token as the unique product identifier.
3. To submit more than one product identifier, click the **Add** button.

4. Click **Next**.
5. Verify the token and enter your license key request (activation code).

   You need a license request key (activation code) to generate a license key. You can generate a license request key from the Management Console or command line using an available token.
6. Click **Next**.

   Licenses appear on the screen and are emailed to the customer address linked to the token.

## Installing your license keys

Because each license key is generated for a specific appliance, ensure that you install your license key on the appropriate appliance.

### To install a license using the CLI

1. Connect to the CLI of the appliance and enter configuration mode.

   For details see the *Riverbed Command-Line Interface Reference Manual*.
2. At the system prompt, enter these commands:

```
license install <license-key>
write memory
```

### To install a license using the Management Console

1. Connect to the Management Console of the appliance.

   For details, see the SCC-VE.
2. Choose Administration > Maintenance > Licenses to display the Licenses Page.
3. Copy and paste the license key provided by Riverbed Licensing Portal into the text box. Separate multiple license keys with a space, Tab, or Enter.

# 3

# Installing the SCC-VE

This chapter describes how to install and configure the SCC-VE. The SCC-VE requires SCC-VE models 8001 (32-bit) or 8151 (64-bit).

This chapter includes these sections:



## Completing the configuration checklist

Be prepared to provide values for the parameters listed in this checklist.

| Appliance | Parameter | Your value |
|---|---|---|
| SCC | Hostname | |
| | IP address | |
| | Netmask | |
| | Default gateway | |
| | DNS Server | |
| | Domain Name | |
| Remote SteelHeads | Serial number | |
| | Version | |
| | IP address or hostname | |
| | User name | |
| | Password | |

## Installing the SCC-VE

The SCC-VE supports VMware ESXi. However, installation procedures vary depending on whether you are using VMware VI or vSphere Client.

The SCC-VE is provided by Riverbed as both an .ova file for ESXi and a zip file that contains the VMX and VMDK files that are necessary to create the virtual machine.

---

**Important:** If you are using the vSphere Client, we recommend you install from the .ova file.

---

## Installing with the VMware vSphere Client

**To install with the VMware vSphere Client**

1. Obtain the OVA package from the Downloads section of the Riverbed Support site at https://support.riverbed.com. (Access requires registration.)
2. Open the VMware vSphere Client.
3. In the left column, select an ESXi host.
4. Choose File > Deploy OVF Template.
5. Select one of these methods:
   - To install from a location served by a web server, select Deploy from URL and specify the URL to the .ova file.

     Deploying directly from https://support.riverbed.com is not supported.
   - To install from a location served by a file server, select Deploy from File and point to the .ova file.
6. Click **Next**.
7. Follow the prompts for these configurations:
   - **Name and Location** - Specify a suitable name for the SCC-VE.
   - **Datastore** - Select the preferred datastore from the list.
   - **Network Mapping** - For both the Primary and Auxiliary interfaces, specify the destination networks.
8. Click **Finish** to complete the installation. For more information on hardware requirements, see "Prerequisites" on page 9.
9. Choose File > Virtual Appliance > Import to open the Import Virtual Appliance Wizard.
10. In the Import Location screen, specify the location of the virtual machine package (*.ovf), and click **Next**.

    If you downloaded the image, use the Import from file option. If Riverbed has provided you with a URL, use the Import from URL option.
11. In the Virtual Appliance Details screen, review the information to confirm that the correct virtual machine package (*.ovf) is selected, and click **Next**.
12. In the Name and Location screen, specify the name for the virtual appliance and select the directory, and click **Next**.

13. In the Host/Cluster screen, select the host or cluster on which to run the virtual appliance, and click **Next**.
14. If you selected a cluster in the preceding step, specify the specific host within the cluster (as prompted in the subsequent Specific Host screen), and click **Next**.
15. In the Datastore screen, select the data store for storing the files for the virtual appliance, and click **Next**.
16. In the Network Mapping screen, map the networks used in the virtual appliance to networks used in the virtual infrastructure, and click **Next**.
17. In the Ready to Complete screen, review the summary of the settings specified in the preceding screens.
18. Click **Finish**.

    The installation begins. The virtual machine package is approximately 2 GB in size; depending on local network conditions, the installation process might take up to forty five minutes or possibly longer.

# Completing the initial configuration

**To configure the SCC-VE**

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

   Enter **yes** at the system prompt:

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

2. Complete the configuration wizard steps as described in this table.

**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.

| Wizard prompt | Description |
|---|---|
| Step 1: Host Name? | Enter the hostname for the SCC-VE. |
| Step 2: Use DHCP? | You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SCC-VE.<br>We recommend that you don't set DHCP.<br>The default value is no. |
| Step 3: Primary IP address? | Enter the IP address for the SCC-VE. |

| Wizard prompt | Description |
|---|---|
| Step 4: Netmask? | Enter the netmask for the network on which the SCC-VE is to reside. |
| Step 5: Default gateway? | Enter the default gateway for the network on which the SCC-VE is to reside. |
| Step 6: Primary DNS server? | Enter the primary DNS server for the network on which the SCC-VE is to reside. |
| Step 7: Domain name? | Enter the domain name for the network on which the SCC-VE is to reside.<br>If you set a domain name, you need not specify the domain names when you set up remote appliances to be managed by the SCC-VE.<br>**Note:** When you configure DNS server settings, map **riverbedcmc** to the IP address for the SCC-VE. |
| Step 8: Admin password? | We strongly recommend that you change the default password at this time. The password must contain at least 6 characters.<br>The default administrator password is password. |

3. Confirm your settings.

```
You have entered the following information:
   1. Hostname: minna
   2. Use DHCP: no
   3. Primary IP address: 10.0.0.74
   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
To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
Choice:
```

   The SCC-VE configuration wizard automatically saves your initial configuration settings.

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

```
# exit
```

# Verifying your connections

### To verify your connections

1. From a remote host, connect to the SCC-VE CLI. At the system prompt, enter one of these commands:

   ```
   ssh admin@<host>.<domain>
   ```

   *-or-*

   ```
   ssh admin@<ip-address>
   ```

2. When you are prompted for a password, specify the administrator password you set when you ran the configuration wizard.

3. At the system prompt, enter ping commands to verify the connections:

   ```
   ping -I <primary-ip-address> <primary-default-gateway>
   ```

# Logging in to the SCC-VE console

After you install the SCC-VE, you can check and modify your configuration settings and view performance reports and system logs in the SCC console. You can connect to the console through any supported web browser.

To connect to the console, you must know the host, domain, and administrator password that you assigned in the configuration wizard.

---

**Important:** Cookies and JavaScript must be enabled in your web browser.

---

**Important:** Before you begin, clear your browser cache and cookies to ensure the user interface displays correctly.

---

### To connect to the SCC console

1. Enter the URL for the SCC 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. When you connect using HTTPS, you are prompted to inspect and verify the SSL certificate. This is a self-signed certificate used to provide encrypted web connections to the SCC.

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

   <domain> is the full domain name for the SCC.

   The SCC Login page displays.

2. In the text box, specify the user login: admin, monitor, a login from a RADIUS or a TACACS+ database, or a previously configured RBM account.

   The default login is admin. Users with administrator privileges can configure and administer the SCC. Users with monitor privileges can view SCC reports but they can't configure the system.

3. In the Password text box, specify the password you assigned in the configuration wizard of the SCC.

   The SCC is shipped with password as the default password.

4. Click **Sign In** to log in and display the Dashboard.

# 4

# Setting Up the SCC-VE on KVM

SteelCentral Controller for SteelHead (virtual edition) (SCC-VE) is available in Kernel-based Virtual Machine (KVM) format, model 8152.

Kernel-based Virtual Machine (KVM) is a virtualization solution for Linux on x86 hardware. A KVM consists of a loadable kernel module that provides the core virtualization infrastructure and a processor-specific module that provides virtualization extensions. Using KVM, you can run multiple virtual machines running unmodified Linux or Windows images. KVM is open source software. The kernel component of KVM is included in mainline Linux, as of version 2.6.20.

KVM supports various I/O virtualization technologies. Paravirtualized drivers, which enable direct communication between hypervisor-level drivers and guest-level drivers, provide the best performance when compared with full virtualization. The *virtio* API provides a common set paravirtualized device drivers for KVM.

**Note:** SCC-VE for KVM supports only virtio-based paravirtualized device drivers.

The SCC-VE for KVM can be launched in different ways, each method using a different procedure. This document describes how to launch an SCC-VE for KVM by using the supplied installation script and the **virsh** command.

This appendix describes how to install and configure an SCC-VE for a KVM virtual appliance. It includes these sections:

# Basic steps for setting up a SCC-VE for KVM

This section provides an overview of the basic steps to install and configure SCC-VE. Detailed procedures are provided in the sections that follow.

| Task | Reference |
|---|---|
| Verify that your KVM host system meets the installation prerequisites. | "Installation prerequisites" on page 24 |
| Obtain the SCC-VE for KVM package from Riverbed Support and unpack it. | "Obtaining the SCC-VE software package" on page 24 |
| Install the SCC-VE for KVM image on the virtual machine. | "Installing SCC-VE on a KVM" on page 25 |
| Power on the VM, restart the SCC-VE for KVM, and log in. | |

# Installation prerequisites

Ensure the KVM host system is configured to meet these requirements:

- SCC-VE requires 4096 MB of memory, 2 vCPU and 27 GB of disk space.
- SCC-VE for KVM has been tested on these operating systems together with virtio paravirtualized device drivers: CentOS 7.2, and Ubuntu 14.04.

# Obtaining the SCC-VE software package

The SCC-VE for KVM package is a tar file, image-vcx.kvm.tgz, containing these files:

- **install.sh** - Installation script that generates an XML specification file, domain.xml, for the SCC-VE instance.
- **mgmt.img** - Management disk file in qcow2 format.
- **datastore.img** - Data disk file in qcow2 format.
- **riverbed_model_tmp** - Metadata file that contains the specifications for the SCC-VE models.

To download the package from the Riverbed Support site, go to https://support.riverbed.com. Access to software downloads requires registration.

# Installing SCC-VE on a KVM

This section describes how to install SCC-VE on a KVM.

**Note:** The virtual NICs must be configured in this order: primary and auxiliary (aux). The virtual disks must be in this order: management (mgmt) and datastore.

### To install a SCC-VE on a KVM

1. Run the install script. The script prompts you for this configuration information:
   - Name for the virtual appliance (should be fewer than 80 characters).
   - Location of the mgmt.img file. For example: /mnt/riverbed/mgmt.img (This configuration parameter will be prompted if the install.sh script and the mgmt.img file are at different folder locations in the KVM host.)
   - Location of the datastore.img file: For example: /mnt/riverbed/datastore.img. (This configuration parameter will be prompted if the install.sh script and the datastore.img file are at different folder locations in the KVM host)
   - Networks (virtual) to which you want to connect the primary, auxiliary (aux) interfaces of the SCC-VE, whether these are networks or bridges.

   Install script example:

   ```
   ./install.sh
   What should the VM be named? scc_kvm_trial
   Please enter the location of mgmt.img: /mnt/riverbed/mgmt.img
   Please enter the location of datastore.img: /mnt/riverbed/datastore.img
   What network should interface primary be connected to? default
   What type of network should be used for primary, network? or bridge? network
   Using network for primary
   What network should interface aux be connected to? default
   What type of network should be used for aux, network? or bridge? network
   Using network for aux
   ```

   After the installation process is complete, this message appears:

   Successfully created a KVM virtual SCC, please use **virsh define scc_kvm_trial.xml** followed by **virsh start scc_kvm_trial.xml** to start it.

2. Start the SCC-VE by running these commands.
   - Enter the **virsh define** command followed by the **virsh start** command.

     ```
     virsh define <virtual-appliance-name>.xml
     virsh start <virtual-appliance-name>.xml
     ```

   - Alternatively you can start the SCC-VE using the **virsh create** command, but using this command will invalidate the license.

     ```
     virsh create <virtual-appliance-name>.xml
     ```

### To start or shut down the SCC-VE using virsh

**Note:** The **virsh reboot** and **virsh shutdown** commands are not support by SCC-VE.

- Use the **virsh start <virtual-appliance-name>.xml** command to start the appliance.
- Use the **virsh destroy <virtual-appliance-name>.xml** command to shut down the appliance.

### To resize the datastore on SCC-VE

Resizing of data store might be required if your SCC-VE is managing more than ten appliances. Use these commands to resize the data store disk. This requires the destroy and restart of SCC-VE.

```
virsh destroy <name-of-kvm-instance>
sudo qemu-img resize datastore.img +<size> (for example: sudo qemu-img resize datastore.img
+2GB)
virsh start <name-of-kvm-instance>
```

## Example SCC-VE specification file

The installation script creates the specification file, domain.xml, that defines key configuration elements of the virtual appliance. Here is an example SCC-VE specification file:

```
<domain type='kvm'>
  <name>scc_internal</name>
  <description>Riverbed Virtual SCC Model 8152</description>
  <memory unit='KiB'>4597888</memory>
  <vcpu placement='static'>1</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <sysinfo type='smbios'>
    <system>
      <entry name='manufacturer'>qemu</entry>
      <entry name='product'>qemu</entry>
    </system>
  </sysinfo>
  <os>
    <type arch='x86_64' machine='pc-i440fx-trusty'>hvm</type>
    <boot dev='hd'/>
    <smbios mode='sysinfo'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <devices>
    <emulator>/usr/bin/kvm-spice</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/mnt/images/mgmt.img'/>
      <target dev='vda' bus='virtio'/>
      <alias name='virtio-disk0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/mnt/images/datastore.img'/>
      <target dev='vdb' bus='virtio'/>
      <alias name='virtio-disk1'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
    </disk>
    <controller type='usb' index='0'>
      <alias name='usb0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
    </controller>
    <controller type='pci' index='0' model='pci-root'>
      <alias name='pci.0'/>
```

```
    </controller>
    <interface type='network'>
      <source network='default'/>
      <target dev='vnet0'/>
      <model type='virtio'/>
      <alias name='net0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </interface>
    <interface type=‘network’>
      <source bridge=‘default’/>
      <virtualport type='openvswitch'>
      </virtualport>
      <target dev='vnet1'/>
      <model type='virtio'/>
      <alias name='net1'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
    </interface>
    <serial type='pty'>
      <source path='/dev/pts/3'/>
      <target port='0'/>
      <alias name='serial0'/>
    </serial>
    <console type='pty' tty='/dev/pts/3'>
      <source path='/dev/pts/3'/>
      <target type='serial' port='0'/>
      <alias name='serial0'/>
    </console>
    <memballoon model='virtio'>
      <alias name='balloon0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x09' function='0x0'/>
    </memballoon>
  </devices>
  <seclabel type='none'/>
</domain>
```

# 5

# Setting Up the SCC-VE in Microsoft Azure

SteelCentral Controller for SteelHead (virtual edition) (SCC-VE) is available in Microsoft Hyper-V format. Hyper-V is the Microsoft virtualization technology. For details about Hyper-V, visit the Microsoft website:

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/

This appendix describes how to install and configure an SCC-VE on a Hyper-V virtual appliance. It includes these sections:



## Before using SCC-VE in Azure

This information will help you make the most of your SCC-VE for Azure:

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

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

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

## Prerequisites for installing SCC-VE in Azure

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

- You have access credentials to a Microsoft Azure account that allow you to create resources in the region and virtual networks where you want to deploy SCC-VE.
- You have obtained a one-time token from the Riverbed Cloud Portal to license your SCC-VE. Access the portal at https://cloudportal.riverbed.com.

- The SCC-VE instance must have continuous SSL/TLS (TCP port 443) access to the Riverbed Cloud Portal in order to verify that the license is active. If the SCC-VE cannot contact the Riverbed Cloud Portal, it will stop optimization and will by-pass connections until it can verify the license again. For enhanced security, configure a TCP proxy in the virtual machine's Networking > Host Settings.

# Installing SCC-VE in Azure

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

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

**To install SCC-VE in Azure**

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

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

   The Create a virtual machine page appears.
6. In the Basics section of the wizard, enter this information:

   Project Details

   – Select a subscription model.

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

   Instance Details

   – Enter a display name for the virtual appliance.

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

   – Specify Availability options.

   – Select the image you want to install on the virtual machine. The default is the item you selected in Step 4 on page 30.

   – Select a size for the virtual machine. The size determines the maximum amount of compute resources (CPU, RAM memory) available to the virtual machine.

Administrator Account

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

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

7. Click **Next : Disks >** to advance to the wizard's Disks tab.
8. Under Disk Options, select a disk type for the SCC-VE virtual appliance's operating system (RiOS).
9. Optionally enable Ultra SSD compatibility.
10. Under Data Disks, create and attach a disk or attach an existing disk to serve as the SCC-VE virtual appliance's data store.

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

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

11. Under the Advanced section, accept the default values.
12. Click **Next : Networking >** to advance to the wizard's Networking tab.
13. Select the network and subnet where you want to deploy the SCC-VE from the Virtual network and Subnet drop-down menus.

    If you have not already configured a virtual network and a subnet, click **Create new** to display the Create new network page. Enter an address space for the new virtual network, create subnets, and then click **OK**. See the Microsoft Azure help for assistance.

14. Optionally select a public IP address from the Public IP drop-down menu. A public IP enables you to communicate with the virtual appliance from outside the virtual network.

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

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

    If no security groups exist, click **Create new** to display the Create network security group page, specify Inbound rules and Outbound rules, and then click **OK**. See the Microsoft Azure help for assistance.

17. Accelerated networking is **Off**. Accelerated networking is not supported.
18. Under Load Balancing, select **No**.
19. Click **Next : Management >** to advance to the wizard's Management tab.

20. Optionally configure the settings under Monitoring, Identity, and Auto-Shutdown to your liking.
21. Click **Next : Guest config >** to advance to the wizard's Guest config tab.
22. Click **Next : Tags >** to advance to the wizard's Tags tab.
23. Optionally add tags.
24. Click **Next : Review + create >** to advance to the wizard's Review + create tab.
25. Review your selections and then click **Create**.
26. License your virtual appliance, and then change the default administrator password.

# Upgrading the SCC-VE software version

Microsoft Azure does not support upgrading and downgrading software versions through Azure. However, you can use this procedure to upgrade or downgrade the SCC-VE software version.

**Note:** The SCC-VE IP addresses might change during this process. You might need to update configurations that depend on those IP addresses.

**To upgrade or downgrade the SCC-VE software version**

1. Download the software package for the new version from the Riverbed Support site:

   https://support.riverbed.com

2. Log in to the SCC Management Console web interface using an administrator account.
3. Choose Administration > Maintenance: Software Upgrade to display the Software Upgrade page.
4. Under Install Upgrade, select **From Local File**.
5. Browse your file system to the software image and select the image.
6. Click **Install** to upgrade your SCC software.

   The software image can be quite large; uploading the image to the system can take a few minutes. Downloading a delta image directly from the Riverbed Support site is faster because the downloaded image includes only the incremental changes and is downloaded directly to the appliance.

   As the upgrade progresses, status messages appear.

   After the installation is complete, you're reminded to reboot the system to switch to the new version of the software.

7. Choose Administration > Maintenance: Reboot/Shutdown and click **Reboot**.

   The appliance can take a few minutes to reboot. This behavior is normal because the software is configuring the recovery flash device. Don't press Ctrl+C, unplug, or otherwise shut down the system during this first boot. There's no indication displayed during the system boot that the recovery flash device is being configured. After the reboot, the Dashboard, Software Upgrade, and Help pages in the Management Console display the RiOS version upgrade.