clearswift
by HelpSystems

Installation Guide

Clearswift Secure ICAP Gateway with Microsoft Azure

Version 5.4.3

Copyright Terms and Conditions

Contents

1. About this guide

This guide provides information for administrators installing Clearswift Secure ICAP Gateway onto a virtual machine. It covers the procedures and requirements necessary for a full installation.

1.1 Who is this guide for?

This guide is intended for use by:

- Customers installing Clearswift Secure ICAP Gateway on the Microsoft Azure platform.

2. Before installing

This section outlines prerequisites and considerations you need to make before installing the cloud-hosted Clearswift Secure ICAP Gateway .

The Gateway runs on 64-bit Red Hat Enterprise Linux (RHEL 7.8).

2.1 Types of installation

You can install the Secure ICAP Gateway on a virtual machine using Microsoft Azure.

> (i) This guide covers the installation of a new instance of the Gateway on a Microsoft Azure platform only. It does not cover installation on the Azure Classic Portal.
>
> For alternative installation types, please refer to the Clearswift Secure ICAP Gateway Installation & Getting Started Guide.

> (i) The use of online repositories to update your system will download packages. Microsoft will charge your Azure account for these transfers.

2.2 Prerequisites

Before installing, you should check that you have the following:

- A valid Microsoft Azure account
- Your subscription details

Browser support

The Clearswift Gateway supports connections using TLS 1.2 ciphers and has been tested with the following browsers:

- Mozilla Firefox - latest
- Google Chrome - latest
- Microsoft Edge (Windows 10)

3. Configuring a Virtual Machine using Microsoft Azure

The following steps show you how to create the Azure Virtual Machine (VM) required to host the Clearswift Gateway using the Azure portal.

> ⊘ For more detailed instructions on using the Microsoft Azure Management Portal, please refer the appropriate Azure documentation. Clearswift is not responsible for changes to any of the procedure steps described.

3.1 Create the Virtual Machine (VM)

1. Sign in to the Azure Management Portal.

2. From the hub menu, click the **Create a resource (+)** button and select **Compute** then **Virtual Machine** from the Azure Marketplace.

   You can now configure your VM Settings.

3.2 Configure VM basic settings

Use the **Basics** menu tab to configure the details of your Virtual Machine.

3.2.1 Project Details

1. Use the drop-down menus to select your required **Subscription** and **Resource group**.

3.2.2 Instance details

1. Enter a **Virtual machine name**. You cannot change this once the virtual machine has been created.

2. Use the drop-down menu to select the nearest data center for your **Region**. You will need this information in order to log in to the machine later.

> ⓘ Some regions might have limitations on available disk types and disk sizes. For more information on what is available, see https://azure.microsoft.com/en-us/regions/

3. Set **Availability options** as per the current policy of your organization.

4. Under **Image**, click **Browse all public and private image**. In the **Select an image** blade that is now displayed search for **RHEL 7.8**. Select this option.

5. Set **Azure Spot instance** as per the current policy of your organization.

6. Use the **Size** drop-down menu to select the Virtual Machine Size. We recommend **Standard_D2s_v3** for testing or **Standard_E2s_v3** for production use.

3.2.3 Administrator account

1. Select either **SSH public key** or **Password** for the **Authentication type**.

   a. If you selected Password:

      i. Enter a memorable **User name** and a strong **Password**.

> Microsoft requires passwords between 12 and 72 characters with three of the following: 1 lower case character, 1 upper case character, 1 number, 1 special character.

   b. If you selected SSH public key:

      i. Enter a memorable **User name**.

      ii. Select the **SSH public key source** as **Generate new key pair**. You can use an existing key that you have previously generated if required, by selecting the appropriate option from the drop-down menu.

      iii. Enter a **Key pair name**.

> The SSH key pair is generated and made available as a .pem file that can be downloaded once the virtual machine has been created.

3.2.4 Inbound port rules

1. Unless otherwise instructed, or recommended by your current organizational policy leave the settings in this section as the default settings and use the Networking tab to create access rules for known IP addresses.

At this point you can click **Review + create** to review the basic configuration and create the virtual machine, However, you will need to go back and configure Disks, Networking and Management options later. Our recommendation is to configure these options prior to using Review + create, so in this instance click **Next : Disks >** to continue.

3.3 Configure VM Disk settings

Use the **Disks**, tab to configure the disk options and data disks of your virtual machine.

3.3.1 Disk options

1. Configure the **OS disk type** and **Encryption type** to the settings recommended by your organization.

> 💡 Virtual machines are created with a default disk size of 64GB.

Data disks

1. If required, additional disks can be added or existing disks can be attached to this virtual machine. Please refer to the Microsoft Azure documentation for more information on how to achieve this.

Click **Next : Networking** to continue.

3.4 Configure VM Networking settings

Use the **Networking**, tab to configure the Network interface options of your virtual machine.

3.4.1 Network interface

1. Either use the **Virtual network** drop-down menu to use an existing virtual network or click **Create** new to add a new one.

2. Choose a virtual network as the *Subnet*. The default network location is 10.0.0.0/24. This is used internally and is not the public IP address that you will use to access your virtual machine. This is specified by **Public IP Address**, which enables you to customize a name for access to the machine.

> ⓘ This is currently a dynamic IP address and will need amending to a static IP address later in the installation.

3. We recommend adding an **Advanced** level **Network Security Group** with firewall rules, configured as follows:

Priority	Name	Port	Protocol	Source	Destination
1000	Allow-ssh	22	TCP	<Your IP address>	VirtualNetwork
1010	Allow-admin-ui-access	443	TCP	<Your IP address>	VirtualNetwork
1020	Allow-cockpit-access	9090	TCP	<Your IP address	VirtualNetwork

> Please refer to the specific Clearswift product documentation to configure the Firewall ports and protocols for the product you are installing.

4. Unless otherwise required by your organizational policy, **Accelerated networking** can be left to the default setting.

3.4.2 Load balancing

1. Unless otherwise required by your organizational policy, **Load balancing** options can be left to the default settings.

Click **Next : Management >** to continue

3.5 Configure VM Additional settings

The Management, Advanced and Tags tabs are available to configure further options for your virtual machine.

- Use the **Management** tab to configure monitoring and management options for your virtual machine.

- Use the **Advanced** tab to add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

- Use the **Tags** tab to define name/value pairs that enable you to categorize resources for use in the User Interface.

> Please review the options on these tabs and refer to your organization's current recommendations for the configuration of any settings.

When ready, click **Review + create** to check that your settings are correct and that validation has passed.

3.6 Review and Create

The Review and Create tab allows you to review any settings that you have already configured, amend if required and then create the virtual machine once satisfied with the configuration.

1. Click **Review + create** to check that your settings are correct and that validation has passed.

2. Scroll through the page to check the current configuration of your virtual machine. If any settings need amending click **Previous** until you arrive at the tab on which the setting is defined. Repeat this procedure as required.

3. Click **Next** to return to the Review and Create tab.

4. Once you are satisfied that the settings are correct, click **Create**. The virtual machine is now created.

3.6.1 Generate new key pair

If you elected to access the virtual machine using a newly generated SSH public key on the [Basic settings](#) tab then you are now prompted to download the new key.

1. Click **Download private key and create resource**.

2. When prompted, using Windows Explorer, save the .pem file to a safe location.

3.7 Configure public IP address and DNS name

Azure displays the details of configured VMs in the **All resources** section.

1. Click your *VM name* and view its Overview page.

2. From the Settings menu, select **Networking**.

3. On the Networking Overview page, click the hyperlink next to **NIC Public IP**. This opens the properties of the NIC Public IP.

4. From the Settings menu, select **Configuration**.

5. Change the **Assignment** from Dynamic to **Static**.

6. Enter the text for the **DNS name label**.

7. Click **Save**.

3.8 Increase Disk Size

Microsoft Azure Virtual Machines are automatically given a disk size of 64GB.

> (i) The root and opt partitions should be 20GB (minimum) and /var should use a minimum of 120GB for test environments and 200GB for production environments.

When you have created and configured your Virtual Machine using the Azure Management Portal, you need to stop the VM and resize the disk.

You must wait for Provisioning to finish then:

1. Stop the Virtual Machine.

2. Increase the disk size of the OS disk from the Azure portal. It is recommended that your disk size is large enough to accommodate two 20GB partitions for root and opt, and 200GB for var.

> (i) Other partitions such as usr, tmp, home and boot may already be

> ⓘ   using up to 20GB of disk space.

3. Start the Virtual Machine.

3.9 Enlarge the OS Partition

After increasing the size of the disk, you will need to resize the disk from the default size in Azure.

Follow the instructions at https://docs.microsoft.com/en-us/azure/virtual-machines/linux/resize-os-disk-gpt-partition for RHEL systems.

When the VM has restarted, perform the following steps:

1. Access your VM as a root user by using the following command:

```
#sudo su
```

2. Use the *lsblk* command to determine which logical volume (LV) is mounted on the root of the file system. In the example below, it would be 'rootvg-rootlv' in sda4 which is currently reported as 63GB

```
[root@mail02-111-co-uk azureuser]# lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                       8:0    0   128G  0 disk
├─sda1                    8:1    0   500M  0 part /boot/efi
├─sda2                    8:2    0   500M  0 part /boot
├─sda3                    8:3    0     2M  0 part
└─sda4                    8:4    0    63G  0 part
  ├─rootvg-tmplv  253:0    0     2G  0 lvm  /tmp
  ├─rootvg-usrlv  253:1    0    10G  0 lvm  /usr
  ├─rootvg-optlv  253:2    0     2G  0 lvm  /opt
  ├─rootvg-homelv 253:3    0     1G  0 lvm  /home
  ├─rootvg-varlv  253:4    0     8G  0 lvm  /var
  └─rootvg-rootlv 253:5    0     2G  0 lvm  /
sdb                       8:16   0    32G  0 disk
└─sdb1                    8:17   0    32G  0 part /mnt
```

3. Determine which disk and partition holds the LVM physical volume or volumes (PV) in the volume group named rootvg by using the pvscan command. Note the size and free space listed between the brackets ([and]):

```
[root@mail02-111-co-uk azureuser]# pvscan
  PV /dev/sda4   VG rootvg           lvm2 [<63.02 GiB / <38.02 GiB free]
  Total: 1 [<63.02 GiB] / in use: 1 [<63.02 GiB] / in no VG: 0 [0    ]
```

4. Expand the partition that contains this PV by using growpart, the device name , and the partition number. This expands the specified partition to use all the free contiguous space on the device.

```
[root@mail02-111-co-uk azureuser]# growpart /dev/sda 4
CHANGED: partition=4 start=2054144 old: size=132161536 end=134215680 new: size=266381278 end=268435422
```

5. Verify that the partition has resized as expected by using the lsblk command
   again. Notice that in the example below, sda4 has changed from 63GB to
   127GB:

```
[root@mail02-111-co-uk azureuser]# lsblk
NAME               MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                    8:0    0  128G  0 disk
├─sda1                 8:1    0  500M  0 part /boot/efi
├─sda2                 8:2    0  500M  0 part /boot
├─sda3                 8:3    0    2M  0 part
└─sda4                 8:4    0  127G  0 part
  ├─rootvg-tmplv   253:0    0    2G  0 lvm  /tmp
  ├─rootvg-usrlv   253:1    0   10G  0 lvm  /usr
  ├─rootvg-optlv   253:2    0    2G  0 lvm  /opt
  ├─rootvg-homelv  253:3    0    1G  0 lvm  /home
  ├─rootvg-varlv   253:4    0    8G  0 lvm  /var
  └─rootvg-rootlv  253:5    0    2G  0 lvm  /
sdb                    8:16   0   32G  0 disk
└─sdb1                 8:17   0   32G  0 part /mnt
```

6. Expand the PV using pvresize to use the rest of the newly expanded partition.

```
[root@mail02-111-co-uk azureuser]# pvresize /dev/sda4
  Physical volume "/dev/sda4" changed
  1 physical volume(s) resized or updated / 0 physical volume(s) not resized
```

7. Verify that the new size of the PV is as expected by reusing pvscan and
   comparing it to the original [size / free] values.

```
[root@mail02-111-co-uk azureuser]# pvscan
  PV /dev/sda4   VG rootvg          lvm2 [<127.02 GiB / <102.02 GiB free]
  Total: 1 [<127.02 GiB] / in use: 1 [<127.02 GiB] / in no VG: 0 [0   ]
```

8. Using the output from the previous step, increase the size of the root partition
   as necessary. Clearswift recommend 20GB for the root partition. For example,
   if the root partition is currently 2GB, run the following command to increase by
   18GB to 20GB:

```
# lvresize -r -L +18G /dev/mapper/rootvg-rootlv
```

9. Repeat the previous step to increase the size of the /opt and /var partitions as
   necessary. Clearswift recommend 20GB for the /opt partition and 200GB for
   the /var partition in production environments. For example, if the opt partition is
   currently 2GB and the var partition 8GB, run the following commands:

```
# lvresize -r -L +18G /dev/mapper/rootvg-optlv
# lvresize -r -L +192G /dev/mapper/rootvg-varlv
```

10. Verify whether the logical volumes have an increased file system size by using the following commands:

```
#df -Th /
#df -Th /opt
#df -Th /var
```

4. Installing the Clearswift Secure ICAP Gateway

You can install the Clearswift Secure ICAP Gateway software using the following instructions.

4.1 Installing from Clearswift Online Repositories

To install Secure ICAP Gateway from repositories hosted online by Clearswift, you will need Internet access to those repositories.

1. Assume root role at the command line.

> (i) When downloading and installing files, we recommend that you check the downloaded file can be verified against the vendor public key.

2. Download the packages containing the online repository configuration files. Click ▧ below to open a page from where the commands can be individually copied and pasted into your terminal:

```
curl -Of https://products.clearswift.net/rhel7/sig/cs-rhel7-
mirrors-22.02.04.rpm

curl -Of https://products.clearswift.net/rhel7/sig/cs-rhel7-
sig-repo-22.01.04.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://products.clearswift.net/RPM-GPG-KEY-
Clearswift
```

4. Verify the downloaded packages:

```
rpm --checksig --verbose cs-*.rpm
```

This will display the results below, where all checks respond with OK:

```
cs-rhel7-sig-repo-22.01.04.rpm:

 Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK
 Header SHA1 digest: OK (cb3e7e95769f914aba6e5f2c2bec22edd8df29a9)
 V3 RSA/SHA256 Signature, key ID 9c75f096: OK
 MD5 digest: OK (4ca922d2ae4b6925e2ddb632d990a2ae)
```

```
cs-rhel7-mirrors-22.02.04.rpm:

Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA1 digest: OK (172adf48c2225a2b7f433584ce6705655ad47137)
V3 RSA/SHA256 Signature, key ID 9c75f096: OK
MD5 digest: OK (55a611db509e4cf522bf98f93ec3d7b3)
```

5. Move Microsoft Update Repos from /etc/yum.repos.d/ directory:

```
mv /etc/yum.repos.d/rh-cloud.repo /var/tmp
```

6. Manually install the downloaded repository file packages:

```
yum -y localinstall cs-*.rpm
```

7. Remove rsyslog:

```
yum -y remove rsyslog
```

8. To install Secure ICAP Gateway, use the following command:

```
yum install -y cs-sig --enablerepo=cs-*,ext-cs-*
```

This command temporarily enables access to the Clearswift online repositories and installs the Gateway.

> (i) If Step 8 fails due to additional conflicts, you might need to remove the conflicting packages first using:
>
> yum remove <package name>

4.2 Configuring your Red Hat Enterprise Linux installation

1. If you used an SSH key when you created the Azure VM, you will need to set a user password, using the following command:

```
passwd <username>
```

2. Enable the online repositories using Red Hat Cockpit. To do this:
   i. Enter the following URL into a supported web browser to open Cockpit:
      https://<ipaddress:9090>
   ii. Login using the administrator credentials, ensuring that you have selected **Re-use my password for privileged tasks**.
   iii. Select Clearswift and then under **Product Actions**, click **Enable** in the **Enable online repositories** setting.

Before you start using your Gateway, we strongly recommend the following actions:

- Create a new administrator account to administer the Gateway.
- Disable the root user account as a security precaution.

This can be achieved using the Red Hat Cockpit application.

1. Select **Accounts** and click **Create New Account**.
   - Enter the name of the new administrator account and a strong password.
2. Click the new administrator account and enable the following role and policy:
   - Enable the Server Administrator role.
   - Select **Never lock account**. Then select 'Never lock account' and click **Change**.
   - Select **Never expire password** or the **date** on which the password will expire. Then click **Never expire password** and click **Change**.
3. Log out of Cockpit and log back in using the new administrator credentials, ensuring you have selected the 'Re-use my password for privileged tasks' setting.
4. Select Accounts and click the root user.
   - Select the **Lock Account** setting to disable the root user.

> It is good practice to create a secondary administrator account, just in case the password of the primary administrator account is lost. This can be achieved by repeating steps 4 and 5.

5. Reboot the Gateway from within the **System** menu in Red Hat Cockpit.

4.3 Configuring Secure ICAP Gateway

On restart, you will need to complete the Clearswift Secure ICAP Gateway Installation Wizard.

1. Open a supported web browser and navigate to the Secure ICAP Gateway IP address:

   https://<ip-address>/Appliance

2. Secure ICAP Gateway Installation Wizard is displayed.

> ⚠ If the Clearswift installation media has been disconnected following the reboot, you must ensure that it is reconnected before configuring the Installation Wizard. The wizard requires access to the installation media to complete the setup of your Secure ICAP Gateway.

3. Complete the wizard and click **Apply**.

4. The system might take around 5-10 minutes to apply the settings before you can use Clearswift Secure ICAP Gateway. We recommend visiting the First Steps topic in the online help when the interface is accessible.

4.4 Configuring update repositories

By default, the Clearswift online repositories are disabled after installation.

This means that any updates will need to be installed using the ISO of subsequent Secure ICAP Gateway releases.

Alternatively, if Secure ICAP Gateway has access to the Internet, it can receive updates from the Clearswift online repositories.

- Switching from offline to online repositories gives access to Red Hat security fixes, normally within 24 hours of their publication and subsequent testing to ensure there are no compatibility issues. We recommend this for most installations.

- However, you should only do this if you intend to also use online repositories for future Clearswift product upgrades.

> ⚠ Be aware that enabling online repositories is an irreversible action.

> ⚠ You should note that the use of online repositories will download updates to your system and you will be charged by Microsoft for this download.

Online repositories can be enabled by following the steps below:

1. Enter the Cockpit URL into a supported web browser to load the Cockpit administration user interface. Then login using the administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks**

option.

2. Navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

4.5 How to change your network settings

1. Use Red Hat Cockpit to configure an IP address.

2. Deploy network changes.

3. Use the Azure Management Portal UI to set a static IP address to match the configuration.

4. Try to reconnect to your system after a few minutes.

Notes:

- The IP Address must belong to the *Virtual Network* range you created earlier.

- Double check your settings before applying network configuration as it is possible to lose connection with your Virtual Machine. Please contact Clearswift Technical Support if this occurs.

- Deploy network changes in Cockpit first, before replicating them in the Azure Management Portal UI.

- The first IP address in your *Virtual Network* range is your network gateway.

- After modifying your VM's IP address in the Azure Management Portal, allow up to five minutes for Azure to apply the change. Azure might reboot your Virtual Machine during this process.

5. Upgrade

If you are upgrading your current version of Clearswift Secure ICAP Gateway on Microsoft Azure, please refer to the Installation and Getting Started Guide for detailed instructions.