Manual

Cryptify Interworking Router

Table of Contents

Scope

This document describes how to install and configure the Cryptify Interworking Router (CIR). It assumes the reader is familiar with the Ubuntu or RedHat Enterprise Linux.

Prerequisites

The CIR requires a server running 64-bit versions of Ubuntu 20.04 LTS, Ubuntu 24.04 LTS, RedHat Enterprise Linux (RHEL) 8 or RHEL 9.

The CIR needs to be installed on each server that should establish interworking connections to remote CRS installations.

NOTE: Local CRS instances need to be running version 4.27.0 (or higher) to support connecting to interworking CRS instances via the CIR.

Basic concepts

The basic operation of the CIR is to act as an interworking router between the local CRS cluster and all configured remote interworking CRS instances.

The purpose of the CIR is to allow your own administered CRS cluster to be opaque for all the remote interworking CRS instances. This will enable you to make changes in your own CRS cluster without effecting the remote interworking CRS instances.

Administrative tasks

Installation

To install the CIR for the first time, simply use the package installer for your operating system:
```
Ubuntu$ sudo dpkg -i cir-3.x.y-amd64-ubuntu.deb
RHEL$ sudo rpm -i cir-3.x.y-x86_64-rhel.rpm
```
where the `.deb`/`.rpm` installation package is provided by Cryptify.

When installing the CIR, a new user – `ciruser` – is added to the system and used to run the service.

After installing the CIR, the service must be configured and then started before it can be used.

Upgrading

To upgrade the CIR, simply use the package installer for your operating system:
```
Ubuntu$ sudo dpkg -i cir-3.x.y-amd64-ubuntu.deb
RHEL$ sudo rpm -U cir-3.x.y-x86_64-rhel.rpm
```
where the `.deb`/`.rpm` installation package is provided by Cryptify.

Diagnostic logging

The diagnostic output that is generated, is automatically written to the standard system log provided by `systemd`, which is accessed using `journalctl`.

Some common commands to read the log file include:
- Read the entire log file:
  ```
  $ sudo journalctl -u cir
  ```
- Read the end of the log file and wait for new messages:
  ```
  $ sudo journalctl -f -u cir
  ```
- Read messages logged within the last hour:
  ```
  $ sudo journalctl -u cir --since "1 hour ago"
  ```
- Read the last 100 messages and wait for new messages:
  ```
  $ sudo journalctl -u cir -f -n 100
  ```

Note that by default, the `systemd` journal is *not* persisted past reboots. To persist the log file past reboots on a default system installation, run:
```
$ sudo mkdir -p /var/log/journal
$ sudo systemd-tmpfiles --create --prefix
/var/log/journal
$ sudo systemctl restart systemd-journald
```

Starting and stopping

The CIR service is controlled using the standard `systemd` commands.

Some common commands include the following.
- Starting the service:
  ```
  $ sudo systemctl start cir
  ```
- Stopping the service:
  ```
  $ sudo systemctl stop cir
  ```
- Checking the status of the service:
  ```
  $ sudo systemctl status cir
  ```

Uninstallation

To uninstall the CIR, use the package manager for your operating system:
```
Ubuntu$ sudo dpkg -r cir
RHEL$ sudo rpm -e cir
```

Uninstalling the CIR does not remove the configuration files.

Configuration

The CIR is configured using the included `cir-cli` program. Some changes (Setting IP) requires the CIR to be restarted for the changes to take effect:
```
$ sudo systemctl restart cir
```

Configuring IP Address

Setting IP

The CIR needs to be configured with the public IP-Address of its network interface to be able to work correctly.

To set the public IP-Address, use:
```
$ cir-cli ip set <IP-Address>
```
where *<IP-Address>* is the public IP-Address that the CIR:s network interface is configured with

NOTE: *This configuration requires the CIR to be restarted beforing taking effect.*

Showing IP

To show the current IP-Address, use:
```
$ cir-cli ip show
```

Configuring clusters

A cluster is a group of hosts (CRS Instances) which are treated as a collective. The CIR currently supports the following clusters:
- local
  - This is your own hosts that you administer.
- remote
  - This is all the interworking hosts that your local cluster should be able to communicate with.

Adding cluster hosts

To add a host to a cluster, use:
```
$ cir-cli cluster modify <cluster-identifier> add host
<Psk-Id> <Psk> [options]
```
where *<cluster-identifier>* is one of:
- local
- remote

The *<Psk-Id>* is the psk id which the host will use when identifying itself and *<Psk>* is the pre-shared-key that the interworking router should use to establish the secure connection.

The available *[options]* is any of:
- --ip=<IP Address>
  - The ip address that the interworking router should use when establishing outgoing connections towards the host (**If omitted it will be set to *<Psk-Id>* from above**).
- --port=<Port Number>
  - Where *<Port Number>* is the port number which the interworking router should connect to (**Default 8080**)
- --comment=<Host Comment>
  - Where *<Host Comment>* is a comment which will be include for this host to allow easier overview and administration.

Removing cluster hosts

To remove a host from a cluster, use:
```
$ cir-cli cluster modify <cluster-identifier> remove host
<IP-Address>
```
where *<cluster-identifier>* is one of:
- local
- remote

The *<IP-Address>* is the hosts configured public ip address.

Showing clusters

To show the current clusters, use:
```
$ cir-cli cluster list
```
and to show information about a specific cluster, use:
```
$ cir-cli cluster show <identifier>
```

Showing cluster status

To show the status of a cluster, use:
```
$ cir-cli cluster status
```
which will write the cluster status to the standard system log provided by `systemd`, which is accessed using `journalctl.`

Configuring log-level

Setting log-level

The log-level determines how much information that the CIR will write to the standard system logs.

To set the log-level, use:
```
$ cir-cli log-level set <level>
```
Where *<level>* is one of:
- ERROR
  - Will only log errors.
- WARN
  - Will log everyting from *ERROR* and any warnings.
- INFO **(Defualt)**
  - Will log everyting from *WARN* and also connection status events for clusters.
- TRACE
  - Will log everyting from *INFO* and also log a trace of each message as it is passed through the CIR.

Showing log-level

To show the current log-level, use:
```
$ cir-cli log-level show
```