Configure CentOS/RHEL 7 Firewall

CentOS/RHEL7 distributions have, by default, a restrictive firewall mechanism based on firewalld that in turn configures the standard iptables system. The default configuration assigns the network interfaces to the public zone and blocks all ports, except 22 (SSH).

Redis Enterprise Software (RS) installation on CentOS/RHEL 7 automatically creates two firewalld system services:

- A service named redislabs, which includes all ports and protocols needed for communications between cluster nodes.
- A service named redislabs-clients, which includes the ports and protocols needed for communications external to the cluster.

These services are defined but not allowed through the firewall by default. As part of the installation process, the installer prompts you to confirm auto-configuration of a default (public) zone to allow the redislabs service.

While this process makes the installation process simple and straightforward, if the machine’s network environment is not secured it could be considered to be insecure, for example by means of an external firewall, EC2 Classic security groups. You can use firewalld configuration tools such as firewall-cmd (command line) or firewall-config (UI) to create more specific firewall policies that allow these two services through the firewall, as necessary.

Note: If databases are created with non-standard RS ports, you need to explicitly configure firewalld to make sure those ports are not blocked.

Updated: July 21, 2021