Configure CIDR allow list

CIDR Whitelist

If you are deploying Redis Cloud on your own infrastructure, you can configure your deployment to permit traffic between a specific set of IP addresses. The list of allowed addresses is called the CIDR Whitelist.

The CIDR whitelist defines a range of IP addresses and AWS security groups that control inbound and outbound traffic to the Redis Cloud VPC. When you manage the CIDR whitelist with security groups you can easily use the same security groups to manage access to your application.

To define the CIDR whitelist:

1. In Subscriptions, click on the subscription for VPC peering.
2. Go to: Security > CIDR Whitelist
3. If there are no CIDR whitelist entries, click + to create a CIDR whitelist. Otherwise, click + under the list of CIDR whitelist entries to add another entry.
4. Specify a whitelist entry as either:
   - IP Address:
     1. For the type, select IP Address.
     2. For the value, enter the IP address in CIDR format for the traffic that you want to allow access for.
   - Security Group:
     1. For the type, select Security Group.
     2. For the value, enter the ID of the AWS security group to grant access to.
5. Click .
6. Either:
   1. Add more whitelist entries - Click +.
   2. Apply the changes to the whitelist - Click Apply all changes.

Updated: January 12, 2022