Cloud database security

Redis Cloud provides several features to help you secure your databases. These include password-based authentication and role-based access control, network security, TLS, and encryption-at-rest.

Passwords, users, and roles

All Redis Cloud databases require a password to connect. However, we recommend going further by enabling role-based access control (RBAC). With RBAC, you can define all the roles you need, with the appropriate permissions, and assign those roles to your users.

Network security

Redis Cloud supports two types of network security: IP Restrictions and VPCs. We recommend that you employ at least one of these network security options to constrain access to your databases.

Transport Layer Security (TLS)

Redis Cloud supports Transport Layer Security (TLS) for database connections. TLS, often called “SSL”, ensures the privacy of the TCP connection between your application and database. When client authentication is enabled, TLS also ensures that those clients with an authorized key can connect to your Redis databases.

We strongly recommend enabling TLS for any application transmitting sensitive data across the wire.

Disk encryption

Redis Cloud provides encryption for all data stored on disk in Redis databases. See our encryption at rest documentation for specific details.

Updated: January 12, 2022