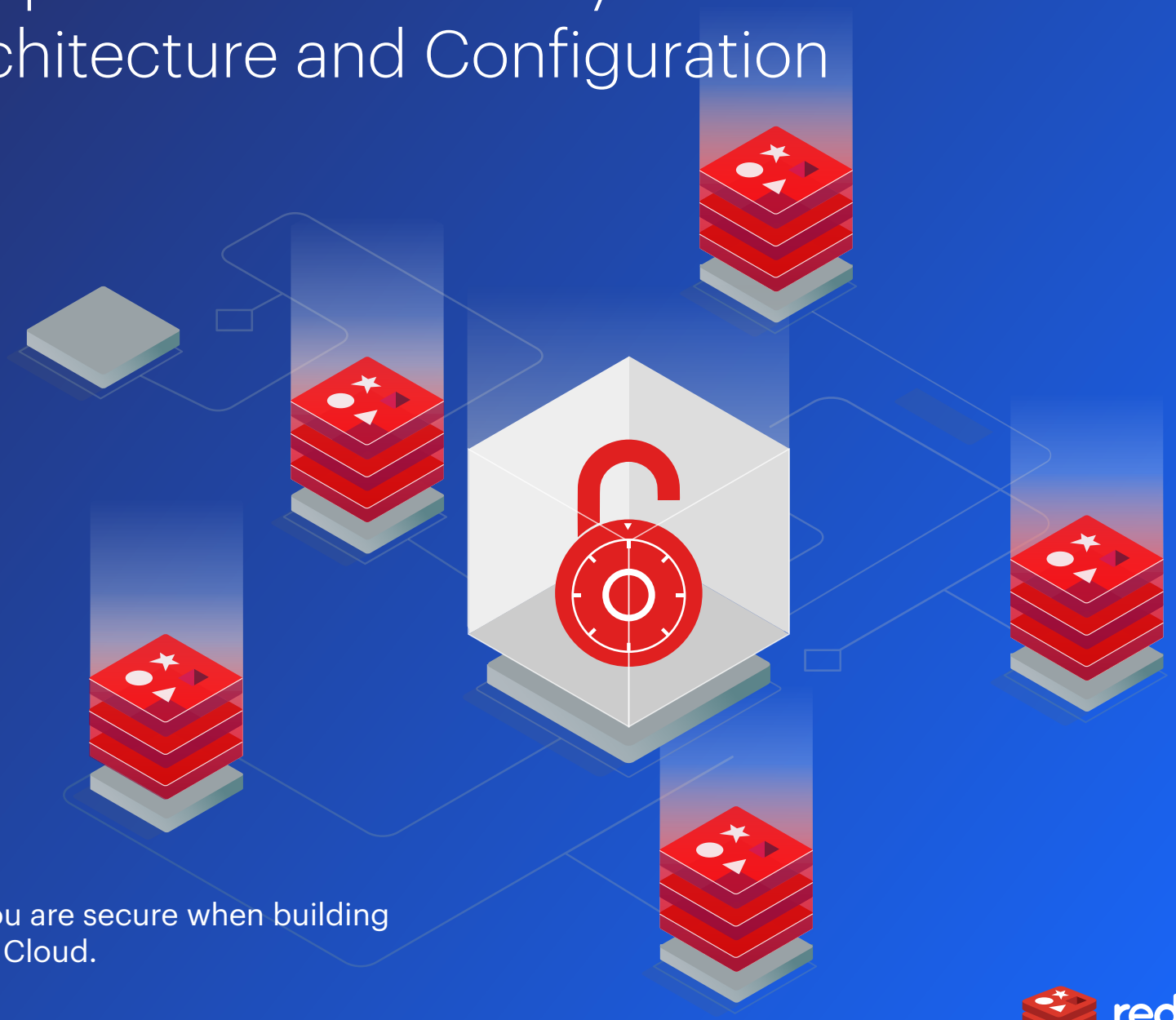
Redis Enterprise Cloud Security: Secure Architecture and Configuration



How to ensure that you are secure when building applications on Redis Cloud.

redis

Introduction

Security is a critical part of being a trusted technology partner. As the technology industry shifts from traditional on-premises environments to focus on the cloud, transparency is critical to establishing and maintaining that trust.

This document's goal is to communicate the security practices available in Redis Enterprise Cloud. This document will enable you to understand everyone's responsibilities in the shared-responsibility model of cloud computing.

Redis Enterprise Cloud

Redis Enterprise Cloud is the fastest way to deploy Redis Enterprise. It is a fully hosted Database-as-a-Service (DBaaS) offering managed by Redis experts. Redis Enterprise Cloud is hosted in private networks within Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

Redis Enterprise Cloud comes in three tiers: Essentials, Pro, and Ultimate.

When you partner with Redis on Redis Enterprise Cloud, Redis focuses on the management and operations of your database so that you can concentrate on delivering business value to your customers.

1

Redis Enterprise Cloud Essentials

Essentials is intended for development environments and low-throughput applications. Essentials is a multi-tenant setup of Redis Enterprise Cloud with basic levels of support.

2

Redis Enterprise Cloud Pro

Pro is a fully managed and hosted DBaaS in a single-tenant cloud environment. In this environment, the entire cloud account and network environment is dedicated to a single customer. Pro offers advanced enterprise security features and is appropriate for use cases where security is a priority.

3

Redis Enterprise Cloud Ultimate

Ultimate is also a fully managed and hosted DBaaS in a single-tenant cloud environment. Redis Enterprise Cloud Ultimate should be used when you need advanced support options in addition to the features offered by Pro. Some custom configurations, such as Active-Active geo-distributed replication and self-hosting in AWS, are available upon request.

The shared-responsibility security model

Redis Enterprise Cloud offerings are deployed on top of AWS, Azure and Google Cloud infrastructure. In Essentials, this infrastructure is multi-tenant. In Pro and Ultimate, all infrastructure is single tenant and dedicated to one specific customer. The cloud provider, region, and availability zone of a deployment is configurable by our customers.

The cloud provider you choose to deploy your Redis Enterprise Cloud deployment is responsible for the physical security of the data centers and the security of the network, storage, servers, and virtualization that help make up the infrastructure of your Redis Enterprise Cloud deployment.

Amazon, Microsoft, and Google's public clouds embrace a wide range of security best practices and compliance standards. Compliance information—including audits, attestations, and certifications— about resources hosted in AWS virtual private networks (VPC) may be found on Amazon's compliance page. Compliance information about resources hosted in Azure virtual networks (VNETs) may be found on Microsoft's compliance page. Finally, compliance information about resources hosted in Google Cloud's virtual private clouds may be found on Google's compliance page.

Under the shared-responsibility model, Redis manages and is responsible for the underlying operating system and deployment of Redis Enterprise. This includes the patching and maintenance of the operating system that Redis is deployed on as well as the patching and maintenance of Redis Enterprise.

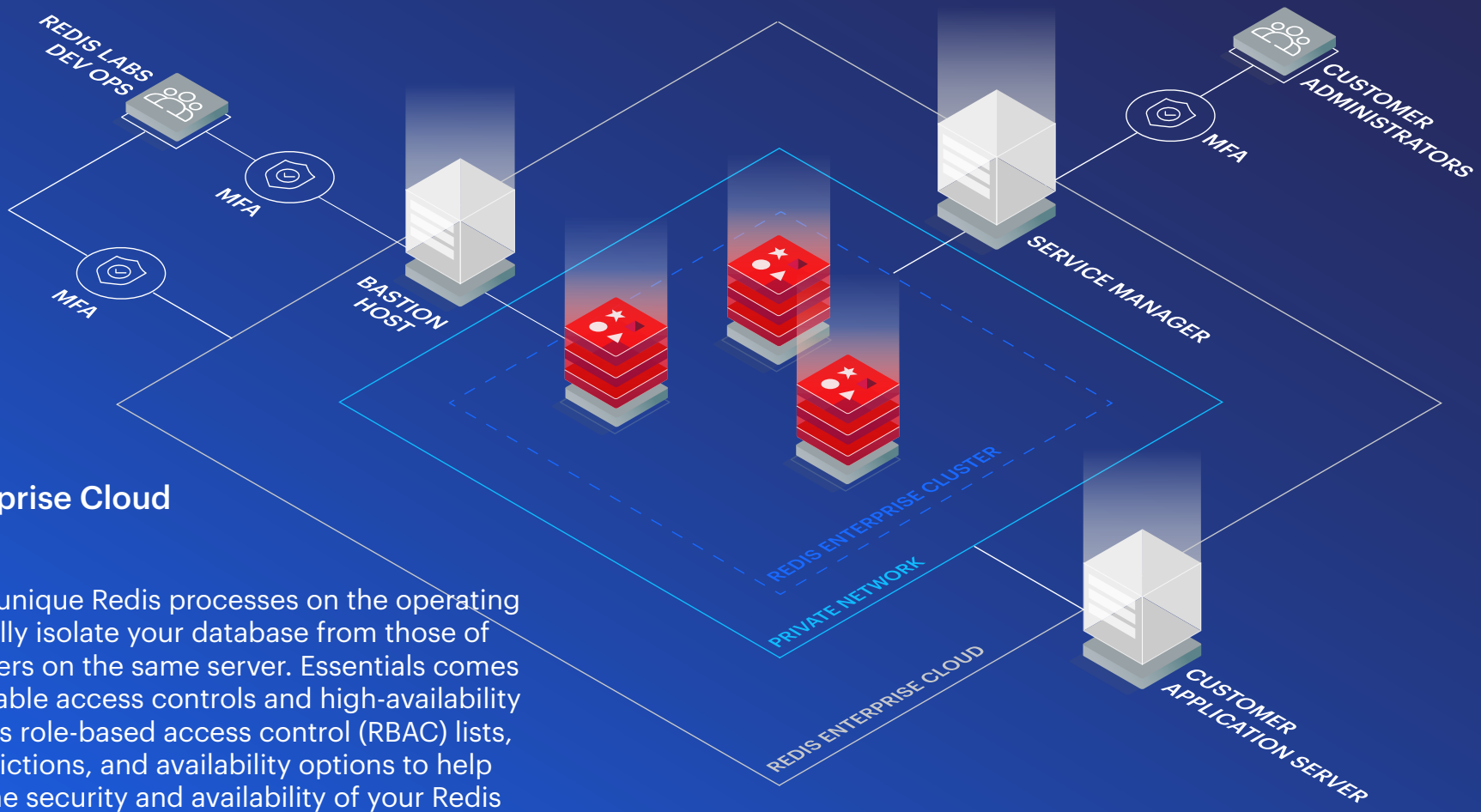
Customers are responsible for the configuration of Redis and the Redis Cloud Admin console for their account. They are also responsible for the applications built on top of Redis and the data that is deployed within Redis.

The operational practices and architecture of Redis Cloud as well is what is configurable by customers is discussed in the following sections.

"The cloud provider, region, and availability zone of a deployment is configurable by our customers. "

Redis Enterprise Cloud Architecture

REDIS ENTERPRISE CLOUD ESSENTIALS CLOUD-AGNOSTIC ARCHITECTURE



Redis Enterprise Cloud Essentials

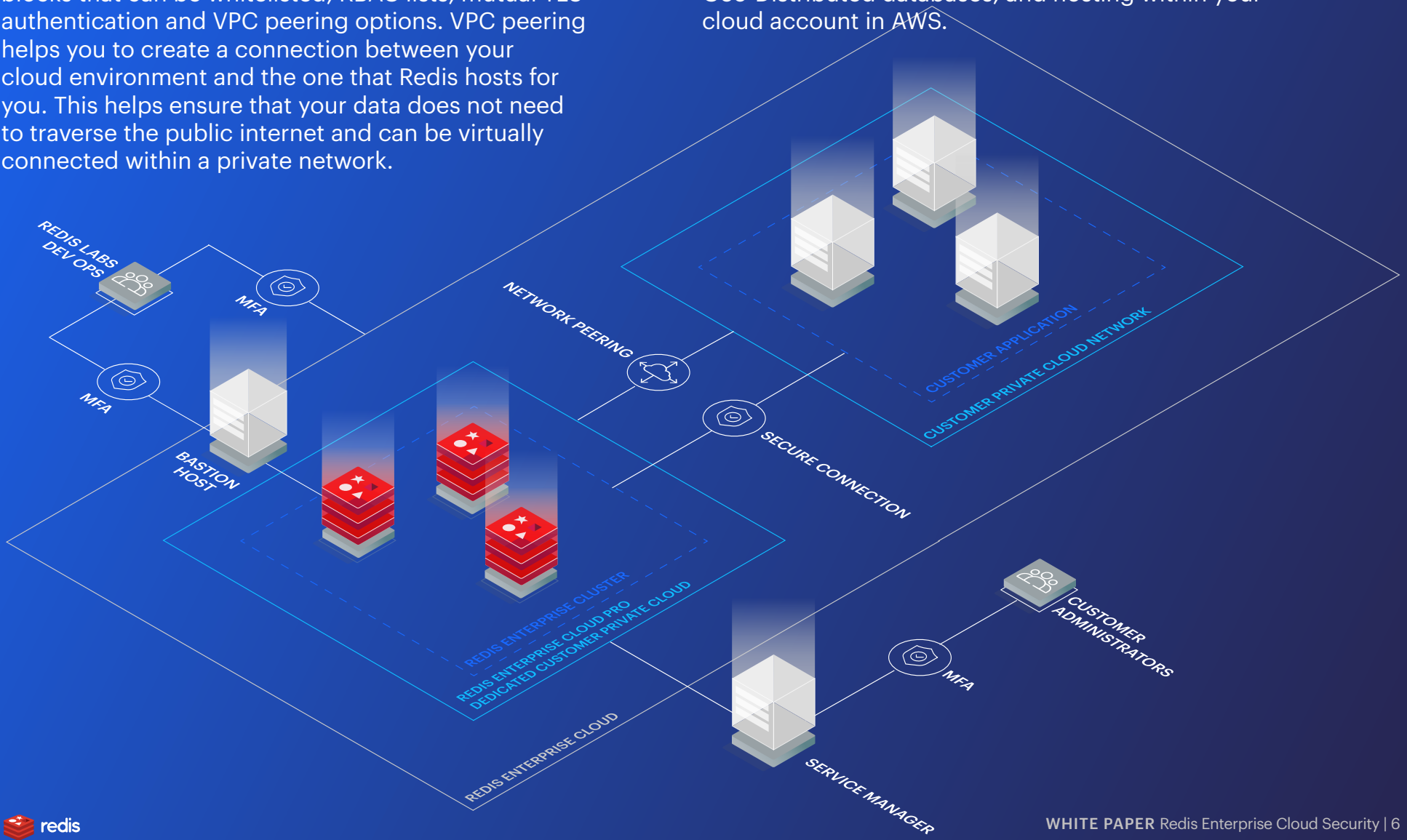
In Essentials, unique Redis processes on the operating system logically isolate your database from those of other customers on the same server. Essentials comes with configurable access controls and high-availability setups such as role-based access control (RBAC) lists, IP-based restrictions, and availability options to help you control the security and availability of your Redis Enterprise deployment.

Redis Enterprise Cloud Pro

Redis Enterprise Cloud Pro comes with a full-service suite of zero-touch security and availability options. These include increased limits to the number IP addresses and classless inter-domain routing (CIDR) blocks that can be whitelisted, RBAC lists, mutual TLS authentication and VPC peering options. VPC peering helps you to create a connection between your cloud environment and the one that Redis hosts for you. This helps ensure that your data does not need to traverse the public internet and can be virtually connected within a private network.

Redis Enterprise Cloud Ultimate

Redis Enterprise Cloud Ultimate is designed with the same architecture as Redis Cloud Pro. Ultimate comes with advanced features, annual reserved pricing, and upon request supports options such as Active-Active Geo-Distributed databases, and hosting within your cloud account in AWS.



Customer-configurable security controls

Redis makes a wide array of user-configurable security options available to customers in Redis Cloud Pro and Ultimate. This helps customers meet their security and compliance standards in a way that is appropriate for their use case. These security features are the customer's responsibility to configure and review and are available for the Redis Enterprise database as well as in the Redis Enterprise Cloud admin console.

Redis Enterprise Cloud admin console security

The Redis Enterprise Cloud admin console offers critical security features that allow customers to establish role-based access control and enhanced authentication security and accountability for your Redis experience. The features listed here are available within Redis Enterprise Cloud to help you securely configure your account.

Role-based access control (RBAC)

Redis Enterprise Cloud offers role-based access control so teams can collaborate on subscriptions of database clusters. A subscription is access to a hosted cluster of servers on which you can configure Redis databases. Members of your team may be set up with read-only access, read-write access, or administrative access so that each member of the team can work together with only the level of access required for their role. Currently, three roles can be assigned to admin console users:

1. Owner: The administrative persona. Users in this role may view, create, and edit any setting.
2. Member: The senior developer persona. Users in this role can view, create, and edit databases.
3. Viewer: The contributor persona. Users in this role can view databases, their configurations, and their secrets.

Multi-factor authentication (MFA)

Redis Enterprise Cloud supports MFA as a means of strong authentication to its services. Redis strongly recommends using MFA to provide an additional layer of security against password-guessing attacks and compromised credentials.

"Redis Cloud helps customers meet their security and compliance standards in a way that is appropriate for their use case."

"Redis Enterprise Cloud customers can set robust access controls and availability controls for their data."

Enforced MFA

Administrators can force all users within their Redis Enterprise Cloud account to use MFA. When this is enabled, all users are forced to configure MFA on their next login. It also disables users' ability to turn off MFA.

Strong passwords

Redis enforces a strong default password policy for all users of the Redis Enterprise Cloud admin console to decrease the risk of a brute force attack against a customer's credentials.

Administrative logging

Redis offers a service log so you can establish accountability and an audit trail within your subscription. Owners of the subscription are able to review who made configuration changes or provisioned resources within an account to help understand the course of events in an incident. These logs are exportable through the Redis Enterprise Cloud admin console and the Redis Enterprise Cloud API.

Redis database security

Protecting your data is among the most important security functions. Redis Enterprise Cloud customers can set robust access controls and availability controls for their data. This helps you set appropriate levels of security and availability for your use case.

VPC and VNET peering

A core tenet of database security is to ensure that your database is properly isolated from the internet at the network level. By default, Redis deploys all databases in a VPC or VNET, and allows you to configure access controls to your database. To help ensure that your database does not need to traverse the public internet for you to access your data, Redis offers VPC and VNET peering within the cloud provider of your choice.

Azure is not supported for Pro deployments at this time. VNET peering and Azure support are available to customers with Redis Cloud Ultimate.

IP address and CIDR restrictions

IP address restrictions help ensure that data is accessible only by authorized servers and locations. Redis allows you to configure authorized IP addresses and IP ranges to help ensure that access to the DBaaS offering comes from a trusted location. Redis strongly recommends that you carefully consider IP address restrictions to ensure that only trusted servers can access your Redis database. On the other hand, the ability to restrict on CIDR address ranges is available within AWS and impacts all databases within your subscription.

Transport layer security and mutual TLS authentication

Transport layer security (TLS) uses encryption to protect data from unauthorized access while in transit to your Redis database. Enabling mutual TLS authentication requires Redis clients to present a client TLS certificate to the server. This forces the server to authenticate the client in addition to the client authenticating the server. Mutual TLS authentication therefore not only helps to ensure that the connection is encrypted, but serves as an additional authentication factor.

Data access control

Redis Enterprise Cloud offers a convenient way to restrict data users to specific commands and keyspaces, by applying the role-based access control (RBAC) paradigm to the database access control lists (ACLs). Starting with clusters deployed with Redis 6, administrators can configure access controls based on Redis commands, command categories, and keys in Redis.

Administrators can centrally manage access controls in the Redis Enterprise Cloud admin console and deploy these controls across all subscriptions and databases in their accounts. These roles may be applied to one or many databases.

Redis comes with a default user account. Administrators may disable the default user and leverage named user accounts with least-privilege permissions in order to restrict access to the data stored in Redis.

Redis user passwords

Redis Enterprise Cloud issues strong, randomly generated passwords for the Redis default user on all databases. You can modify and rotate your Redis passwords to meet your organizational policies for the default user or any named user. Customers choosing to perform regular password rotations should remember to update their client-side code to prevent service disruptions when changing these credentials. To help protect you from exposing your data to unauthorized sources, Redis does not support the configuration of unauthenticated Redis connections to Redis Enterprise Cloud. We strongly recommend requiring strong passwords for all users, especially default users if they are not disabled.

Data-at-rest encryption

Data-at-rest encryption is a key tenet of many compliance standards and security frameworks. Data-at-rest encryption helps prevent unauthorized access to the host operating system from the underlying cloud provider. Redis Enterprise Cloud Pro and Ultimate support encryption at rest for all cloud providers. Redis leverages the industry-standard encryption provided by the major cloud providers.

Protecting against data loss and failures

Redis Enterprise Cloud comes with multiple persistence and backup features to help prevent data loss in a failure event.

Persistence

In the cloud world, it's important to design to deal with failure. In Redis, the tradeoff between performance and the risk of data loss is controlled by eviction and persistence policies. Eviction policies allow you to handle how the application will function in the event of hitting a memory limit. Redis may be configured for a broad range of eviction policies ranging from removing the least-frequently used data to denying any new writes. More information about eviction policies can be found in the eviction policy documentation.

Because Redis is an in-memory database, data can be lost if it is not persisted to disk prior to a failure event. You can set policies in Redis that force the server to persist data to disk prior to acknowledging a write event to ensure that data is always persisted

> "In the cloud world, it's important to design to deal with failure."

or you can set timeframes for persistence. The more frequently you persist data, however, the greater the performance impact. This tradeoff is configurable for each database to meet your ranges of data loss tolerance. For more information on data persistence, read the persistence documentation.

Backup

You can back up persisted files so that if an entire availability zone goes down, you can easily redeploy your database to another location, such as Amazon S3, Azure Blob Storage, Google Cloud Storage, and (S)FTP.

Vendor lock-in and migration

Redis Enterprise Cloud supports multiple cloud providers and lets you easily move workflows to and from multiple Redis providers. You can migrate between hosted Redis providers, an on-premises Redis Enterprise cluster, or an open-source Redis solution by importing your database directly into the new cluster. This helps minimize vendor lock-in risk and make migration simpler.

Availability Support

Built-in fault tolerance

Redis Enterprise Cloud is built for fault tolerance. Within Redis Enterprise Cloud, you can select from several availability options, including replication and multiple availability zones (multi-AZ). Redis Enterprise Cloud deploys Redis across three nodes for improved availability. Replication enables shards to be replicated between nodes. In a multi-AZ deployment, Redis is deployed across multiple availability zones within the same region so that your Redis deployment can withstand an availability-zone failure.

Active-Active geo-distributed replication

The Redis Enterprise implementation of Active-Active Geo-Distributed replication is based on Conflict-Free Replicated Data Types (CRDTs). With CRDTs, applications can read and write to the same data set from different geographical locations seamlessly without changing the way the application connects to the database.

Two common scenarios for use of Active-Active are to provide disaster recovery and faster data read-access for geographically distributed users. This allows your data to be hosted in multiple locations around the globe but maintain local latency levels.

Service-level agreements (SLAs)

Redis offers standardized SLAs for various deployment types:

Standard SLA: Three-nines uptime (99.9%)
Multi-AZ SLA: Four-nines uptime (99.99%)
Active-Active SLA: Five-nines uptime (99.999%)

More information about Redis Enterprise Cloud's SLAs may be found in the Redis Enterprise Cloud Service Level Agreement.

"Redis Enterprise Cloud supports multiple cloud providers and lets you easily move workflows to and from multiple Redis providers."

Redis operational security controls

Redis' operations team is responsible for the operational security controls of Redis Enterprise Cloud. Redis protects Redis Enterprise Cloud customers' Redis deployments and manages the underlying operating system in the following ways:

Blocking Redis commands

Redis works to reduce the attack surface you present by blocking administrative commands. This protects your databases against known attack patterns and ensures that administration must be done through the Redis Enterprise Cloud admin console or the Redis Cloud API, not directly on the database.

Upgrades and patching

Redis' operations team is responsible for patching and maintaining your Redis deployment and the underlying operating system. Redis partners with the open source community and subscribes to notification services to help reduce possible vulnerabilities within Redis Enterprise. Redis patches and upgrade servers as appropriate to secure customers.

Management review

When incidents impact the security or availability of services, Redis holds weekly management reviews and escalations in order to quickly and appropriately resolve issues.

Operations security

Redis' operations team leverages a bastion host to authenticate to environments for maintenance and recovery activities. Secure shell (SSH) keys to your servers are stored in a secrets vault. Redis operations team members require multiple factors of authentication in order to access any customer infrastructure.

Redis maintains management control—at the Vice President level—through monitoring of users with access to Redis Enterprise Cloud bastion hosts. This VP-level management monitoring ensures that only trained and authorized Redis team members can access your infrastructure. Access to customer infrastructure is tightly controlled, periodically audited, and managed by the Vice President of Operations at Redis.

Application security

Redis performs regular security testing and discovery procedures to address security issues within Redis Enterprise Cloud products. Using industry-standard risk-assessment methods, Redis prioritizes issues based on the criticality to customers and the business, as well as the likelihood of exploitation. Security testing is performed by both internal and external resources. Redis conducts annual, independent, third-party penetration tests, as well as code-review processes and internal security testing by the security and quality-assurance teams at Redis to minimize the risk of security vulnerabilities being introduced. Redis also has deployed a web application firewall in front of the Redis Cloud admin console to assist in protecting our customers from attacks against our console.

"VP-level management monitoring ensures that only trained and authorized Redis team members can access your infrastructure."

Support resources

Redis customers can get support from the curators and experts of open source Redis. There are several channels to help support and ensure your successful redis experience.

Online support

Customers can submit a support ticket through the Redis online support portal or via email. The online support portal is built directly into the service-management user interface.

Phone support

Redis offers 24 x 7 x 365 support over the phone and online for customers. Phone support should be used for urgent production issues.

Technical Account Managers

Redis' team of technical account managers are available to help facilitate the build out and operations of your Redis environment.

To contact support, please email **support@redis.com**

About Redis

Modern businesses depend on the power of real-time data. With Redis, organizations deliver instant experiences in a highly reliable and scalable manner.

Redis is the world's most popular in-memory database, and commercial provider of Redis Enterprise, which delivers superior performance, matchless reliability, and unparalleled flexibility for personalization, machine learning, IoT, search, e-commerce, social, and metering solutions worldwide.

Redis, consistently ranked as a leader in top analyst reports on NoSQL, in-memory databases, operational databases, and database-as-a-service (DBaaS), is trusted by more than 7,400 enterprise customers, including five Fortune 10 companies, three of the four credit card issuers, three of the top five communication companies, three of the top five healthcare companies, six of the top eight technology companies, and four of the top seven retailers.

Redis Enterprise, available as a service in public and private clouds, as downloadable software, in containers, and for hybrid cloud/on-premises deployments, powers popular Redis use cases such as high-speed transactions, job and queue management, user session stores, real time data ingest, notifications, content caching, and timeseries data.

Corporate Headquarters
700 E El Camino Real Suite 250
Mountain View, CA 94040

t: +1 (415) 930-9666
info@redis.com
redis.com