Redis Enterprise Cloud安全：安全架构和配置

在 Redis Cloud 上构建应用程序时如何确保安全

HongKe 虹科

redis

介绍

安全是成为值得信赖的技术合作伙伴的关键部分。随着技术行业从传统的本地环境转向专注于云计算，透明度对于建立和维护这种信任至关重要。

本文档的目标是传达 Redis Enterprise Cloud 中可用的安全实践。本文档将使您了解每个人在云计算的共享责任模型中的责任。

Redis Enterprise Cloud

Redis Enterprise Cloud 是部署 Redis Enterprise 的最快方式。它是由 Redis 专家管理的完全托管的数据库即服务 (DBaaS) 产品。Redis Enterprise Cloud 托管在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud 的专用网络中。

Redis Enterprise Cloud 分为三个层级：基础版、专业版和旗舰版。

当您在 Redis Enterprise Cloud 上与 Redis 合作时，Redis 将专注于数据库的管理和运维，以便您可以专注于为客户提供业务价值。

1

Redis Enterprise Cloud 基础版

基础版是为开发环境和低吞吐量的应用准备的。基础版是Redis Enterprise Cloud的一个多租户设置，具有基本的支持水平。

2

Redis Enterprise Cloud 专业版

专业版是单租户云环境中完全托管的DBaaS。在此环境中，整个云帐户和网络环境都专用于单个客户。专业版提供先进的企业安全特性，适用于安全性优先的用例。

3

Redis Enterprise Cloud 旗舰版

旗舰版也是单租户云环境中完全托管的DBaaS。当你需要高级支持选项时，除了专业版提供的功能，还应该使用Redis Enterprise Cloud 旗舰版。一些自定义配置(如AWS中的Active-Active地理分布式复制和自托管)可根据请求提供。

共享责任安全模型

Redis Enterprise Cloud产品部署在 AWS、Azure 和谷歌云基础设施之上。在基础版中，此基础设施是多租户的。在 专业版和旗舰版中，所有基础设施都是单一租户专用于一个特定客户。**我们的客户可以配置部署的云提供商、区域和可用分区。**

您选择部署 Redis Enterprise Cloud部署的云提供商负责数据中心的物理安全以及网络、存储、服务器和虚拟化的安全，这些都有助于构成您的 Redis Enterprise Cloud部署的基础设施。

Amazon、Microsoft 和 Google 的公共云采用范围广泛的安全最佳实践和合规性标准。有关托管在 AWS 虚拟专用网络 (VPC) 中的资源的合规信息（包括审计、证明和认证）可在亚马逊的合规页面 . 有关托管在 Azure 虚拟网络 (VNET) 中的资源的合规性信息，请访问Microsoft 的合规性页面 . 最后，有关托管在 Google Cloud 的虚拟私有云中的资源的合规性信息可以在Google 的合规性页面 .

在责任共担模式下，Redis 管理并负责Redis Enterprise 的底层操作系统和部署。包括部署Redis的操作系统的打补丁和维护，以及Redis Enterprise的打补丁和维护。

客户负责为其帐户配置 Redis 和 Redis Cloud 管理控制台。他们还负责构建在 Redis 之上的应用程序和部署在 Redis 中的数据。

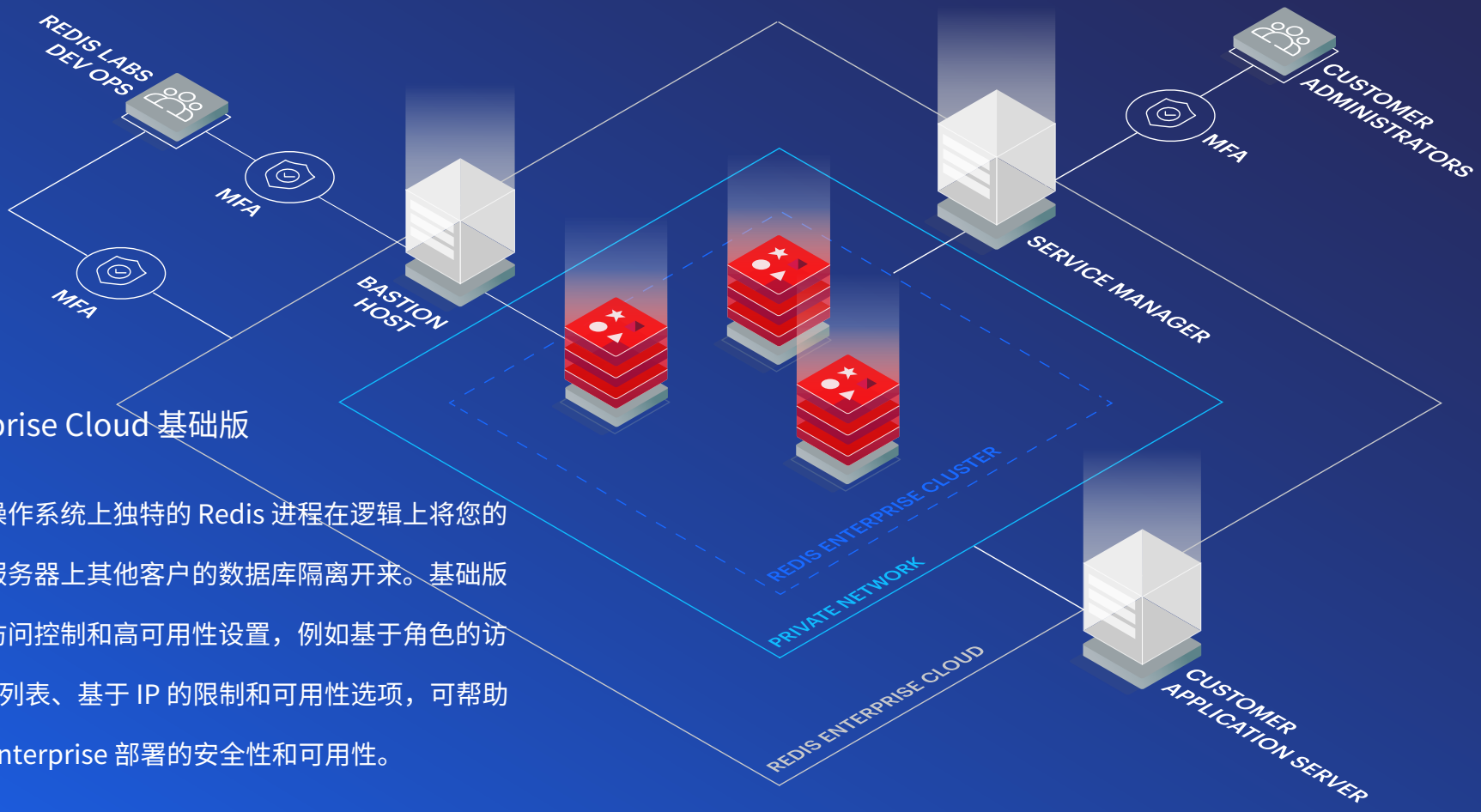
Redis Cloud 的操作实践和架构以及客户可配置的内容将在以下部分中讨论。

“我们的客户可以配置部署的云提供商、区域和可用分区。”

Redis Enterprise Cloud架构

HongKe 虹科

Redis Enterprise Cloud **基础版的云独立架构**



Redis Enterprise Cloud 基础版

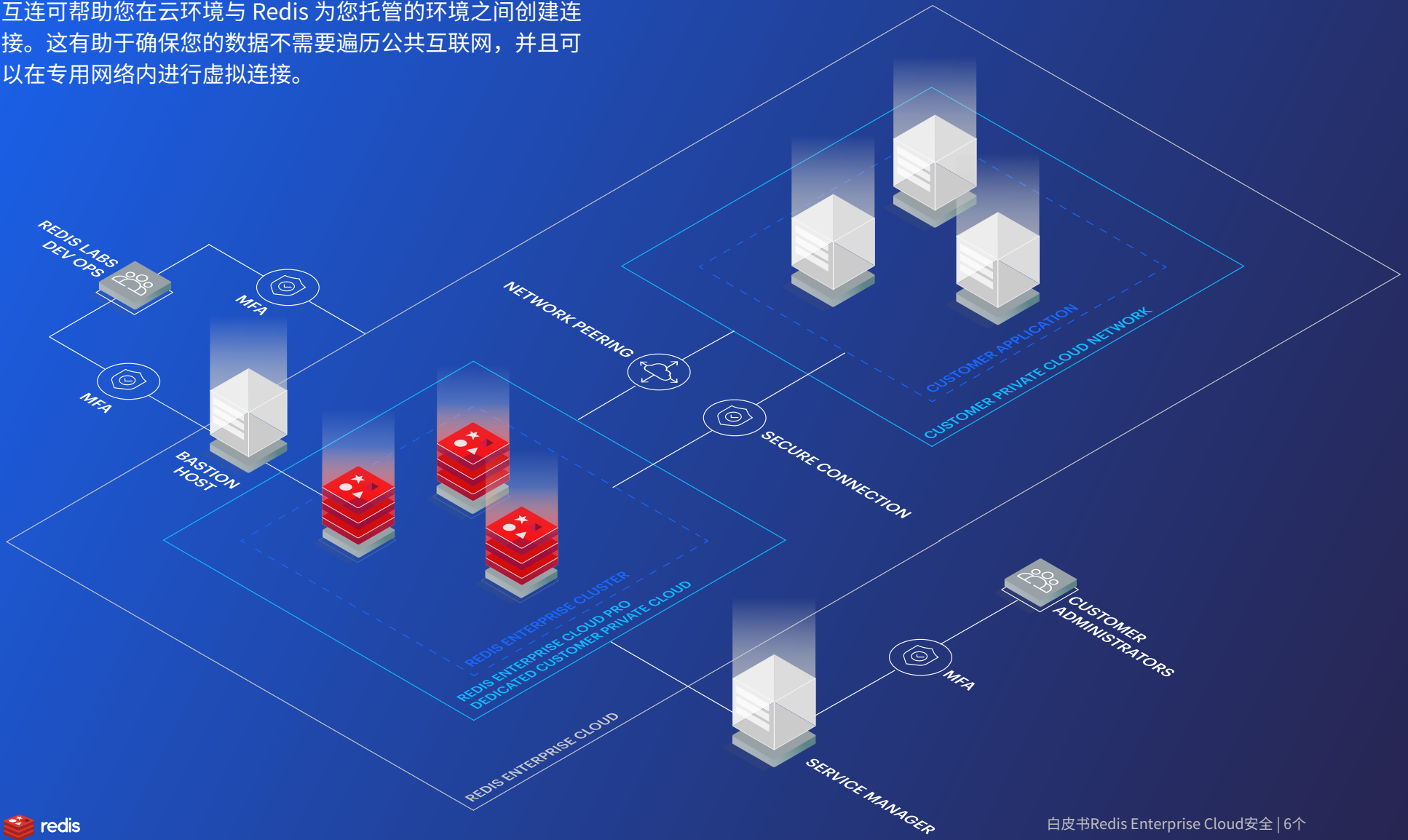
在基础版中，操作系统上独特的 Redis 进程在逻辑上将您的数据库与同一服务器上其他客户的数据库隔离开来。基础版附带可配置的访问控制和高可用性设置，例如基于角色的访问控制 (RBAC) 列表、基于 IP 的限制和可用性选项，可帮助您控制 Redis Enterprise 部署的安全性和可用性。

Redis Enterprise Cloud专业版

Redis Enterprise Cloud 专业版附带一套包含零接触安全性和可用性选项的全方位服务套件。其中包括增加对 IP 地址数量的限制和可以列入白名单的无类域间路由 (CIDR) 块、RBAC 列表、双向 TLS 身份验证和 VPC 对等选项。VPC 对等互连可帮助您在云环境与 Redis 为您托管的环境之间创建连接。这有助于确保您的数据不需要遍历公共互联网，并且可以在专用网络内进行虚拟连接。

Redis Enterprise Cloud 旗舰版

Redis Enterprise Cloud 旗舰版采用与 Redis Cloud 专业版相同的架构设计。旗舰版具有高级功能、年度保留定价，并根据要求支持诸如 Active-Active 地理分布式数据库等选项，并在您的 AWS 云帐户中托管。



客户可配置的安全控制

Redis 为 Redis Cloud 专业版和旗舰版中的客户提供了广泛的用户可配置安全选项。这有助于客户以适合其用例的方式满足其安全性和合规性标准。这些安全功能由客户负责配置和审查，可用于 Redis Enterprise 数据库以及 Redis Enterprise Cloud 管理控制台。

Redis Enterprise Cloud

管理控制台安全

Redis Enterprise Cloud 管理控制台提供了关键的安全功能，使客户能够建立基于角色的访问控制并增强身份验证安全性和责任制，以提升您的 Redis 体验。此处列出的功能在 Redis Enterprise Cloud 中可用，可帮助您安全地配置您的帐户。

基于角色的访问控制 (RBAC)

Redis Enterprise Cloud 提供基于角色的访问控制，**因此团队可以在数据库集群的订阅上进行合作。订阅是对托**管服务器集群的访问，您可以在其上配置 Redis 数据库。您的团队成员可能被设置为具有只读访问权限、读写访问权限或管理访问权限，以便团队中的每个成员都可以仅以其角色所需的访问级别一起工作。目前，可以为管理控制台用户分配三个角色：

1. 所有者：管理角色。担任此角色的用户可以查看、创建和编辑任何设置。

2. 成员：高级开发人员角色。担任此角色的用户可以查看、创建和编辑数据库。

3. 查看者：贡献者角色。担任此角色的用户可以查看数据库、它们的配置和它们的秘密。

多重身份验证 (MFA)

Redis Enterprise Cloud支持 MFA 作为对其服务进行强身份验证的一种方式。Redis 强烈建议使用 MFA 来提供额外的安全层来抵御密码猜测攻击和泄露的凭据。

“ Redis Cloud帮助客户以适合其用例的方式满足其安全性和合规性标准。 ”

HongKe 虹科

“ Redis Enterprise Cloud**客户可以为他们的数据设置强大的访问控制和可用性控制** ”

强制 MFA

管理员可以强制其 Redis Enterprise Cloud帐户中的所有用户使用 MFA。启用后，所有用户都必须在下次登录时强制配置 MFA。**它还禁用了用户关闭** MFA**的能力**。

强密码

Redis 为 Redis Enterprise Cloud 管理控制台的所有用户强制执行强默认密码策略，以降低针对客户凭据的暴力攻击风险。

管理日志记录

Redis 提供了一个服务日志，因此您可以在您的订阅中建立问责制和审计跟踪。订阅的所有者能够查看谁在帐户中进行了配置更改或配置资源，以帮助了解事件中的事件过程。这些日志可通过 Redis Enterprise Cloud 管理控制台和 Redis Enterprise Cloud API 导出。

Redis数据库安全

保护您的数据是最重要的安全功能之一。Redis Enterprise Cloud客户可以为其数据设置强大的访问控制和可用性控制这有助于您为您的用例设置适当的安全性和可用性级别。

VPC 和 VNET 对等

数据库安全的核心原则是确保您的数据库在网络级别与 Internet 正确隔离。默认情况下，Redis 将所有数据库部署在 VPC 或 VNET 中，并允许您配置对数据库的访问控制。为了帮助确保您的数据库不需要遍历公共互联网来访问您的数据，Redis 在您选择的云提供商内提供 VPC 和 VNET 对等互连。

专业版部署目前不支持 Azure。使用 Redis Cloud 旗舰版的客户可以使用 VNET 对等互连和 Azure 支持。

IP 地址和 CIDR 限制

IP 地址限制有助于确保数据只能由授权的服务器和位置访问。Redis 允许您配置授权 IP 地址和 IP 范围，以帮助确保对 DBaaS 产品的访问来自受信任的位置。Redis 强烈建议您仔细考虑 IP 地址限制，以确保只有受信任的服务器才能访问您的 Redis 数据库。

另一方面，限制 CIDR 地址范围的功能在 AWS 中可用，并且会影响您订阅中的所有数据库。

传输层安全和双向 TLS 身份验证

传输层安全 (TLS) 使用加密以保护数据在传输到您的 Redis 数据库时免遭未经授权的访问。启用双向 TLS 身份验证需要 Redis 客户端向服务器提供客户端 TLS 证书。除了客户端对服务器进行身份验证之外，这还强制服务器对客户端进行身份验证。因此，双向 TLS 身份验证不仅有助于确保连接已加密，而且还充当额外的身份验证因素。

数据访问控制

Redis Enterprise Cloud通过将基于角色的访问控制 (RBAC) 范例应用于数据库访问控制列表 (ACL)，提供了一种将数据用户限制为特定命令和键空间的便捷方式。从部署 Redis 6 的集群开始，管理员可以根据 Redis 命令、命令类别和 Redis 中的密钥配置访问控制。

管理员可以在 Redis Enterprise Cloud 管理控制台中集中管理访问控制，并将这些控制部署到他们帐户中的所有订阅和数据库中。这些角色可以应用于一个或多个数据库。

Redis 带有默认用户帐户。管理员可以禁用默认用户并利用命名用户帐户最小权限 以限制对存储在 Redis 中的数据的访问。

Redis 用户密码

Redis Enterprise Cloud 为所有数据库上的 Redis 默认用户发出随机生成的强密码。您可以修改和轮换您的 Redis 密码以满足默认用户或任何指定用户的组织策略。选择定期轮换密码的客户应记住更新其客户端代码，以防止在更改这些凭据时服务中断。为了帮助防止您将数据暴露给未经授权的来源，Redis 不支持配置未经身份验证的 Redis 连接到 Redis Enterprise Cloud。我们强烈建议要求所有用户使用强密码，尤其是默认用户（如果未禁用）。

静态数据加密

静态数据加密是许多合规性标准和安全框架的关键原则。静态数据加密有助于防止底层云提供商对主机操作系统进行未经授权的访问。Redis Enterprise Cloud 专业版和旗舰版支持所有云提供商的静态加密。Redis 利用主要云提供商提供的行业标准加密。

防止数据丢失和故障

Redis Enterprise Cloud 具有多种持久性和备份功能，有助于防止在故障事件中丢失数据。

持久化

在云世界中，处理故障的设计很重要。在 Redis 中，性能和数据丢失风险之间的权衡由逐出和持久性策略控制。逐出策略允许您处理应用程序在达到内存限制时的运行方式。Redis 可以针对广泛的逐出策略进行配置，从删除最不常用的数据到拒绝任何新的写入。有关驱逐政策的更多信息，请访问**驱逐策略文档**

由于 Redis 是一个内存数据库，如果在发生故障事件之前未将数据持久保存到磁盘，则数据可能会丢失。您可以在 Redis 中设置策略，强制服务器在确认写入事件之前将数据持久化到磁盘，以确保数据始终持久化或者您可以设置持久性的时间范围。**然而，你持久化数据的频率越高，对性能的影响就越大。这种权衡对每个数据库来说都是可配置的，以满足你的数据损失容忍度的范围。关于数据持久性的更多信息，请**阅读持久性文档 .

“在云世界中，设计以应对故障非常重要。”

备份

您可以备份持久文件，以便在整个可用区出现故障时，您可以轻松地将数据库重新部署到另一个位置，例如 Amazon S3、Azure Blob Storage、Google Cloud Storage 和 (S)FTP。

供应商锁定和迁移

Redis Enterprise Cloud 支持多个云提供商，让您可以轻松地将工作流移入和移出多个 Redis 提供商。您可以通过将数据库直接导入新集群来在托管的 Redis 提供程序、本地 Redis Enterprise 集群或开源 Redis 解决方案之间迁移。这有助于最大限度地降低供应商锁定风险并简化迁移。

可用性支持

内置容错

Redis Enterprise Cloud 专为容错而构建。在 Redis Enterprise Cloud 中，您可以从多个可用性选项中进行选择，包括复制和多个可用性区域（multi-AZ）。Redis Enterprise Cloud跨三个节点部署 Redis 以提高可用性。复制使分片能够在节点之间复制。在多AZ部署中，Redis跨多个部署同一区域内的可用性区域，以便您的 Redis 部署能够承受可用性区域故障。

Active-Active 异地分布式复制

Active-Active Geo-Distributed 复制的 Redis Enterprise 实现是基于**无冲**突复制数据类型 (CRDTs) . 使用 CRDT，应用程序可以从不同的地理位置无缝地读取和写入相同的数据集，而无需改变应用程序连接到数据库的方式。

使用 Active-Active 的两个常见场景是为地理分布的用户提供灾难恢复和更快的数据读取访问。这允许您的数据托管在全球多个位置，但保持本地延迟水平。

服务级别协议 (SLA)

Redis 为各种部署类型提供标准化的 SLA：

标准服务等级协议：三个九的正常运行时间 (99.9%)
多可用区 SLA：四个九的正常运行时间 (99.99%)
Active-Active **SLA：**五个九的正常运行时间 (99.999%)

有关 Redis Enterprise Cloud的更多信息SLA 可以在 Redis Enterprise Cloud服务水平协议 .

HongKe 虹科

“ Redis Enterprise Cloud 支持多个云提供商，让您轻松地将工作流在多个Redis提供商之间迁移。 ”

Redis 运维安全控制

Redis 的运维团队负责 Redis Enterprise Cloud的运维安全控制。Redis 通过以下方式保护 Redis Enterprise Cloud客户的 Redis 部署和管理底层操作系统：

阻塞 Redis 命令

Redis**致力于通过阻止管理命令 来减少你的攻击面。**这可以保护您的数据库免受已知攻击模式的侵害，并确保管理必须通过 Redis Enterprise Cloud 管理控制台或 Redis Cloud API 完成，而不是直接在数据库上完成操作。

升级和修补

Redis 的运维团队负责修补和维护您的 Redis 部署和底层操作系统。Redis 与开源社区合作并订阅通知服务，以帮助减少 Redis Enterprise 中可能存在的漏洞。Redis 修补程序和升级服务器以确保客户安全。
管理审查和升级，以便快速和适当地解决问题。

管理评审

当事件影响服务的安全性或可用性时，Redis 每周举行一次

操作安全

Redis 的运维团队利用堡垒主机对环境进行身份验证以进行维护和恢复活动。服务器的安全外壳 (SSH) 密钥存储在秘密保险库 . Redis 运维团队成员需要多种身份验证因素才能访问任何客户基础设施。

Redis 通过监控有权访问 Redis Enterprise Cloud堡垒主机的用户，在副总裁级别维护管理控制。这种 VP 级别的管理监控可确保只有经过培训和授权的 Redis 团队成员才能访问您的基础设施。对客户基础设施的访问受到 Redis 运维副总裁的严格控制、定期审计和管理。

应用安全

Redis 定期执行安全测试和发现程序，以解决 Redis Enterprise Cloud 产品中的安全问题。Redis 使用行业标准的风险评估方法，根据对客户和业务的重要性以及被利用的可能性来确定问题的优先级。安全测试由内部和外部资源执行。Redis 每年进行一次独立的第三方渗透测试，并由 Redis 的安全和质量保证团队进行代码审查流程和内部安全测试，以最大限度地降低引入安全漏洞的风险。Redis 还在 Redis 云管理控制台前部署了一个 Web 应用程序防火墙，以帮助保护我们的客户免受针对我们控制台的攻击。

> “副总裁级别的管理监控确保只有经过培训和授权的 Redis 团队成员才能访问您的基础设施。”

支持资源

虹科客户可以获得开源 Redis 的**技术工程师**和专家的**支**持。有多种渠道可以帮助**支**持和确保您获得最棒的 Redis 体验。

在线支持

客户可以通过 虹科在线**支**持**门**户或通过电子邮件提交**支**持票。在线**支**持**门**户直接内置于服务管理**用**户界**面**中。

电话支持

虹科通过电话和在线为客户提供 24 x 7 x 365 **支**持。电话**支**持应该**用**于紧急**生**产问题。

技术客户经理

虹科的技术客户经理团队可以帮助促进您的 Redis 环境的构建和运维。

要联系**支**持，请发送电子邮件 hongcloudtech@hkaco.com

关于 Redis

现代企业依赖于实时数据的力量。借助 Redis，组织可以以高度可靠和可扩展的方式提供即时体验。

Redis 是世界上最受欢迎的内存数据库和 Redis Enterprise 的商业提供商，它为全球个性化、机器学习、物联网、搜索、电子商务、社交和计量解决方案提供卓越的性能、无与伦比的可靠性和无与伦比的灵活性。

Redis在NoSQL、内存数据库、操作型数据库和数据库即服务(DBaaS)的顶级分析师报告中一直被评为领导者，**受到**7400**多家企业客户的信任，**

包括 5 家财富 10 强公司、4 家信用卡发行商中的 3 家 、5家顶级通信公司中的3家、5家顶级医疗保健公司中的3家、8家顶级技术公司中的6家以及7家顶级零售商中的4家。

Redis Enterprise 可作为公共云和私有云中的服务提供，作为可下载的软件在容器中提供，并用于混合云/本地部署，为流行的 Redis 用例提供支持，例如高速事务、作业和队列管理、用户会话存储、实时数据摄取、通知、内容缓存和时间序列数据。

联系我们

行业交流群

获取更多资料

hongcloudtech.com

虹科电子科技有限公司

T(+86)400-999-3848
M(+86)155 0827 0915

www.hongcloudtech.com
hongcloudtech@hkaco.com
广州市黄埔区神舟路18号润慧科技园C栋6层
各分部：广州 | 成都 | 上海 | 苏州 |西安 | 北京 | 台湾 | 香港 | 美国硅谷