阿尔卡特朗讯 Rainbow

安全白皮书 - 2018 年 7 月

Rainbow™
www.openrainbow.com

阿尔卡特朗讯Rainbow是一款基于云的企业级统一通信即服务解决方案，同时支持混合云部署。Rainbow可为企业提供全球化的协作与通信解决方案，同时满足各类企业客户的特定需求，这些客户包括从需要高性价比的移动化应用的小型企业，到希望跨越复杂的IT环境和多个地理位置来部署统一通信应用并将其集成到业务流程中的跨国公司。Rainbow采用可扩展的云计算SaaS和CPaaS平台，旨在实现高可用性和扩展性。我们将保护用户数据的机密性、完整性和可用性，并将您对我们的信任和信心视为重中之重。

责任模式

Rainbow的基础架构从设计之初便考虑了安全性，这意味着它是一个可靠且可扩展的平台，使客户能够快速、安全地对接并部署定制化应用。我们的基础架构根据云行业标准的安全控制措施和策略（如OWASP）进行构建和管理。 我们采用冗余且分层的控制方式，并不断进行验证和测试，可自动确保对底层基础架构进行安全可靠的全天候（7x24）监控。

ALE采用安全责任分担模式运行，ALE负责Rainbow底层基础架构和服务的安全性，同时让客户在应用层管理其各自的安全性，包括与云的连接，以及在Rainbow范围内公司和用户的隐私规则、身份和访问控制管理，如图1所示：

图1：Rainbow安全责任分担模式

物理和环境安全

基础架构中数据的保密性、服务内容的完整性和存储数据的可用性是我们最关心的问题。ALE负责保护运行Rainbow所有服务的全球基础架构，包括运营Rainbow服务所需的硬件、软件、网络设备和配套设施。Rainbow数据中心遵循ISO-27001和SOC认证技术，通过带刺的铁丝网隔离，周边区域和建筑物入口有全天候视频严密监控并由专业安保人员控制人员的出入。获得授权的工作人员须佩戴通过RFID管控的署名胸卡，其个人身份会定期进行核验。

了解更多关于Rainbow云服务的信息，请访问：

www.openrainbow.com/zh-hans

Alcatel·Lucent Enterprise

为预防火灾风险，每个数据中心的房间都配有火灾探测和灭火系统以及防火门。 火灾探测系统在所有数据中心环境、机械和电气基础设施空间、冷却室和发电机设备室内都使用烟雾探测传感器，符合APSAD R4规则并通过N4合规性认证。

每个数据中心的电力系统均设计为完全冗余和可维护，对运营无干扰，可以全天候（7x24）运行，并可以支持48小时本地供电，以应对供电网络的任何故障。不间断电源（UPS）还可在发生电气故障时提供备用电源。

我们的数据中心依托于遍布全球的光纤网络，在欧洲地区提供高达4.5 Tbps的总网络带宽容量，在北美地区则提供8 Tbps的总带宽容量。数据中心在网络层使用专有的分布式拒绝服务（DDoS）防御技术，以保护我们的服务免受各种攻击，1秒内就能检测到异常，过滤非法流量（容量高达4Tb），同时让合法数据包在1毫秒内就通过。

地理位置分布

为了满足各地法律法规的要求，并为用户提供最佳体验，Rainbow的架构支持地理上彼此分隔的多地区部署。 我们保证用户的敏感数据不会因为跨越边界而遭到复制，从而确保区域级数据隐私。同时，Rainbow服务是跨区域部署的，以最大限度地减少用户服务延迟，同时确保数据的安全边界。

撰写本文时，如图2所示，用户数据分属于4个关键区域：北美，欧洲中东及非洲（默认），德国和亚太地区，接下来的几个月预计将覆盖美国本土、拉丁美洲和中国大陆。我们的主数据中心分布在加拿大、法国、德国和新加坡。二级数据中心（不托管数据，仅作为缓存和媒体中继），位于英国和澳大利亚。我们还提供专用数据中心来托管医疗敏感数据。目前，在北美、欧洲和亚太地区有19个边缘点或入网点（PoP），通过IP Anycast机制为我们的用户直接提供静态资源本地访问，从而分流我们的网络基础设施的负荷。

图 2： Rainbow 可服务的区域

了解更多关于Rainbow云服务的信息，请访问：

www.openrainbow.com/zh-hans

Alcatel·Lucent Enterprise

业务连续性

ALE设计Rainbow可以容忍站点、数据中心、系统或硬件的故障，从而把对客户的干扰降到最低限度。我们所有的服务都以N+1冗余配置部署，以确保没有单点故障（SPOF）；并有足够的计算能力，以便在服务器出现故障时能利用其余服务器实现负载均衡。所有应用请求均匀分布在内部和外部的负载均衡器中。数据库和用户生成的数据都经过多次复制，并按区域进行备份，以确保不会出现任何可能的损失。我们添加了GeoDNS机制和自动故障转移支持，以应对潜在的互联网路由问题，并确保用户访问最近的入网点。Rainbow整个产品架构能够自动确保各种组件完全可靠，且支持可再生式部署。

Rainbow客户支持和运营团队采用行业标准诊断流程，在遇到影响业务的事件时有助于快速找到解决方案。运维人员提供全天候（7x24x365）服务，检测各种事件并管理事件的影响和解决方法。ALE内部沟通体系已经就绪，以确保云运营团队的员工了解他们各自的角色和职责，以及如何及时沟通重大事件。ALE还部署了各种外部沟通机制为其客户群提供支持。如今，相关机制已经建立，可及时通知客服团队任何影响用户体验的操作问题。

现有Rainbow基础架构的日常运行、紧急情况和配置更改，只能由ALE云运营团队的指定员工授权、测试、核准、自动化和部署。 Rainbow基础架构进行更新时尽量减少对客户及其服务使用的影响。更改在应用于生产环境之前需要进行测试，以帮助确保更改符合预期，且不会对性能产生负面影响。所有变更必须获得内部变更顾问委员会（CAB）成员的授权，以便观察和了解潜在的业务影响。

关键更改将定期部署（欧洲中部时间星期日）。如生产系统需要（偏离标准变更管理程序）进行紧急变更，应进行记录并获得相应的许可。

设计原则

Rainbow提供多种安全功能和服务，以提高隐私保护并控制网络访问，其中包括防火墙、传输中加密（所有服务采用最高级别的TLS协议规范），以及DDoS控制技术。

Rainbow的安全策略部署了流量控制规则，默认拒绝所有流量，只在各种负载均衡器上开启必要的端口。我们的系统只接受呼入HTTPS / WSS（443）连接，所有纯文本访问都被转到TLS安全连接。 在高度安全的负载均衡器、邮件服务器和WebRTC媒体中继的范围内；没有任何组件暴露于公共互联网，或通过公共互联网访问。这种服务器的操作只能通过基于双因子身份验证的受限VPN、在高度受控的访问环境内进行，遵循无密码策略，防止任何可能的暴力攻击。

我们公开接口的安全质量控制依托于Qualys SSL Labs等外部工具，以确保我们维持适当的服务水平。我们使用来自Comodo CA的标准通配符SSL/ TLS证书，99.9%的网络浏览器信任这些证书，这些证书使用256位EC密钥并使用RSA SHA-256签名。我们的策略是仅支持最强密码，强制执行TLSv1.2连接（并禁用SSLv2、SSLv3、TLSv1.0和TLSv1.1），从而拒绝安全性能较弱的浏览器和客户端（如IE 6-10、Safari 5-6、Android < 4.4、 Java 6-7 和OpenSSL <1.0）的访问。

Rainbow 负载均衡器支持完全正向保密（PFS），使用Diffie-Hellmann （DH）和椭圆曲线Diffie-Hellmann密钥交换协议（ECDHE）密码套件、降级攻击预防、OCSP装订，可以安全抵御所有最新肆虐的威胁，如DROWN、 BEAST、 POODLE、HeartBleed和Spectre攻击等。我们的策略是模糊化应用服务器的版本号，以防止基于扫描的攻击。

了解更多关于Rainbow云服务的信息，请访问：

www.openrainbow.com/zh-hans

Alcatel·Lucent Enterprise

我们使用严格安全传输机制（HSTS）并在浏览器公共HSTS白名单中预加载以强制执行TLS连接。 所有的Rainbow服务器都在GNU/Linux Debian发行版上运行，配置为始终遵循最新的安全分支，确保在零日攻击时升级系统软件包。Rainbow生产网络是一个完全独立运作的信息系统，通过复杂的网络安全和认证机制与ALE公司的网络隔离。

应用层

为帮助确保只有授权的Rainbow用户和管理员访问其帐户和相关资源，Rainbow使用多种类型的证书进行身份验证。 通过关联用户的电子邮件地址和他的个人密码，基于TLS使用基本身份验证完成用户认证，并依托于署名的JSON Web令牌（JWT）实现进一步API调用。最终用户的密码在Rainbow的内部数据库中随机排列和加密。因此出于安全考虑，被遗忘的证书将无法恢复，从而在用户万一遇到数据泄露事件时提供额外的安全性防护。Rainbow系统随后将重置用户密码。 访问Rainbow帐户需要密码，密码在帐户创建时确定，并可以随时更改。 用户密码必须具有高度复杂性，最少有8个字符，至少有1个小写字母、1个大写字母、1个数字和1个特殊字符。Rainbow的多重要素身份验证（MFA）是帐户自助注册或密码重置机制的附加安全层。6位一次性临时PIN码将被发送至用户的电子邮箱，用户必须在Rainbow中填写该验证码以完成密码设置。

一旦通过验证，Rainbow访问控制列表将确保每个用户都可获得与其属性相对应的功能。公司的管理员有权将用户与其公司关联，提升用户的Rainbow服务等级并更新在Rainbow系统内公司层面的可视性。除了公开的“Rainbow”企业用户群之外，各家企业用户在默认情况下是彼此隔离的，用户不能与其他公司的人联系，如图3所示。用户只能看到自己公司的同事或属性为公共的用户。

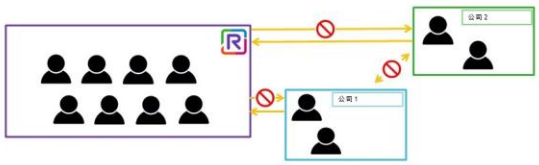

图 3: Rainbow 公司的可见性

强制数据边界可以阻止对用户和公司数据的任何逻辑访问，但获得明确授权的同事除外。

安全框架合规性

ALE为其客户提供Rainbow基础架构，其设计和管理符合云安全标准，我们的托管服务提供商通过了ISO27001:2013、SOC 1 / SSAE 16 / ISAE 3402（原SAS 70）、SOC 2和SOC 3标准认证，我们的运营团队成员也通过了ISO27001“Lead Implementer”认证。

通过第三方网络漏洞扫描程序、Web应用程序扫描和外部独立机构的人工安全审计，我们的基础架构和软件解决方案得以不断接受审查。 安全是我们的首要任务，所有必要行动都是为了控制或消除任何已发现的威胁。

数据隐私合规性

Rainbow服务旨在符合个人数据保护规则和法规，特别是符合欧洲通用数据保护法（GDPR），该法规为个人实施隐私和数据保护。GDPR的三大原则，也是Rainbow数据安全理念的指导方针：从设计开始就注重隐私、默认安全性和问责制。保护我们客户的数据至关重要，因此我们构建了安全机制和流程，以确保高度安全性，尊重数据主体的隐私：您的数据仅属于自己，除非有必要，不会被用于任何商业用途，也不会转移至任何第三方，个人数据保护的级别至少达到GDPR要求的水平，转移您的数据需要事先获得您的许可。用户数据也会在其所属地保存，从而确保符合任何适用的地方法律。

Alcatel·Lucent Enterprise