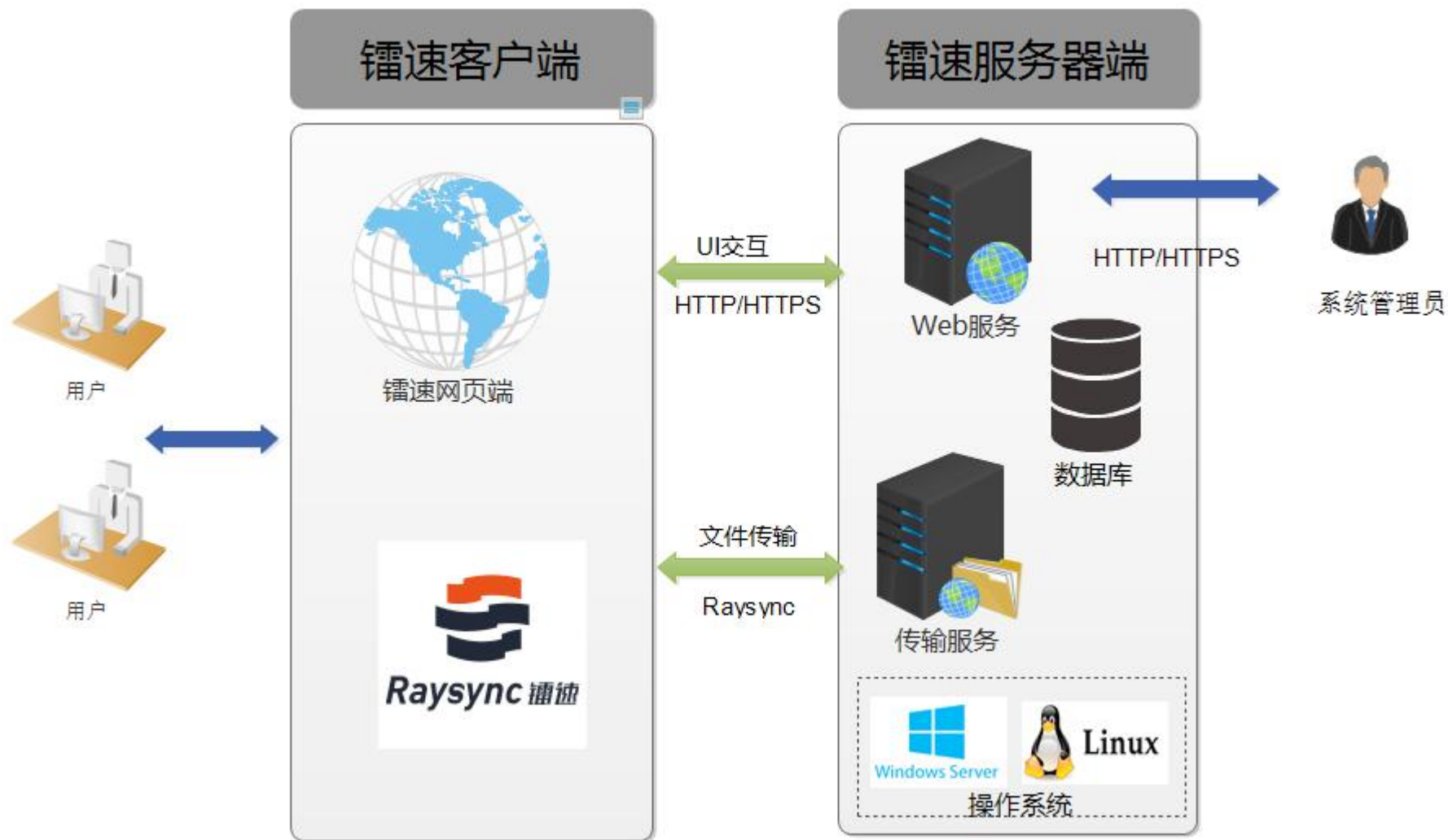


镭速产品安全技术白皮书

镭厉风行
速达全球

镭速产品架构示意图



目录

Contents

01 Web安全设计

03 传输安全设计

05 行为审计

02 账户&密码保护安全设计

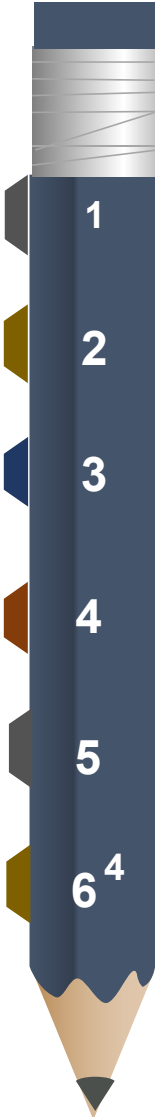
04 软件安装&运行安全设计

06 加密证书生命周期管理



01

Web安全设计

- 
- 1 用户面Web portal与管理面Web Portal支持访问IP地址隔离、端口隔离
 - 2 支持部分节点禁用用户面Web Portal或管理面Web Portal
 - 3 同时支持Http与Https，管理员可禁用Http只暴露Https服务
 - 4 Https TLS 1.3，仅开放行业公认安全的加密算法套件
 - 5 镭速登录的Web页面，session有效范围仅为当前访问页面有效，完全杜绝CSRF跨站攻击
 - 6⁴ 每次版本发布前，均使用华为云在线专业Web漏洞扫描服务进行漏洞扫描，及时修复最新发布漏洞

02

账户&密码保护安全设计

- 登录认证内置防暴力破解机制，3分钟内用户连续输错5次密码，账户将被自动锁定
- 登录中的会话标识，使用OpenSSL高强度随机函数RAND_bytes()接口生成，防止随机信息被模拟器命中





用户密码在传输过程中，通过非对称高强度加密算法进行加密，即使传输报文被拦截，攻击者也无法通过密文恢复出明文

用户密码保存在数据库中的信息，使用PBKDF2算法加用户单独的随机盐进行单向1万次不可逆加密，即使数据库信息泄露，也无法通过密文反推用户密码

强制密码强度保护，密码必须为大小写、数字、特殊符号组合，且长度大于等于8个字符

系统提供弱口令词典，用户可自定义密码强度符合但容易被社会工程学破解的弱密码，禁止系统用户使用此类密码，如<公司英文名>@123

- 登录访问IP限制机制，通过黑白IP限制登录系统。防止未经授权的访问，以及减轻潜在的恶意攻击
- 登录邮箱双因素认证，要求用户在登录时除了密码还需要提供邮箱验证码，这种方式使得攻击者即使获取了用户的密码，也难以成功登录，增强账户的安全性



03

传输安全设计

传输过程中，镭速在传输报文层面、文件块、整个文件进行Hash校验保护，保障传输内容的完整性

镭速传输客户端与镭速传输服务器之间，使用TLS 1.3进行加密，杜绝网络中间人攻击

镭速传输只需要对外暴露1个端口，即可满足所有用户访问，极大减小防火墙端口暴露风险

04

软件安装&运行安全设计

软件安装&运行安全设计

系统无内置用户名和密码，admin 管理员密码在安装过程中随机生成，在admin管理员首次登录时强制提示用户修改密码

用户上传的文件，默认权限均为660，去除文件的执行属性，防止输入文件执行行为

使用低权限用户运行镭速服务端

管理员可自定义用户可上传的文件后缀，禁止用户上传存在危险的文件

服务端程序文件other组用户权限全部关闭，防止其他用户非正常访问

管理员可开启病毒查杀和自定义敏感词文本，禁止用户上传含有病毒或携带敏感词的文件

05

行为审计

镭速服务端完整记录了用户登录、登出、上传、下载、修改密码、分享链接等完整行为日志，管理员可定期审计用户行为信息



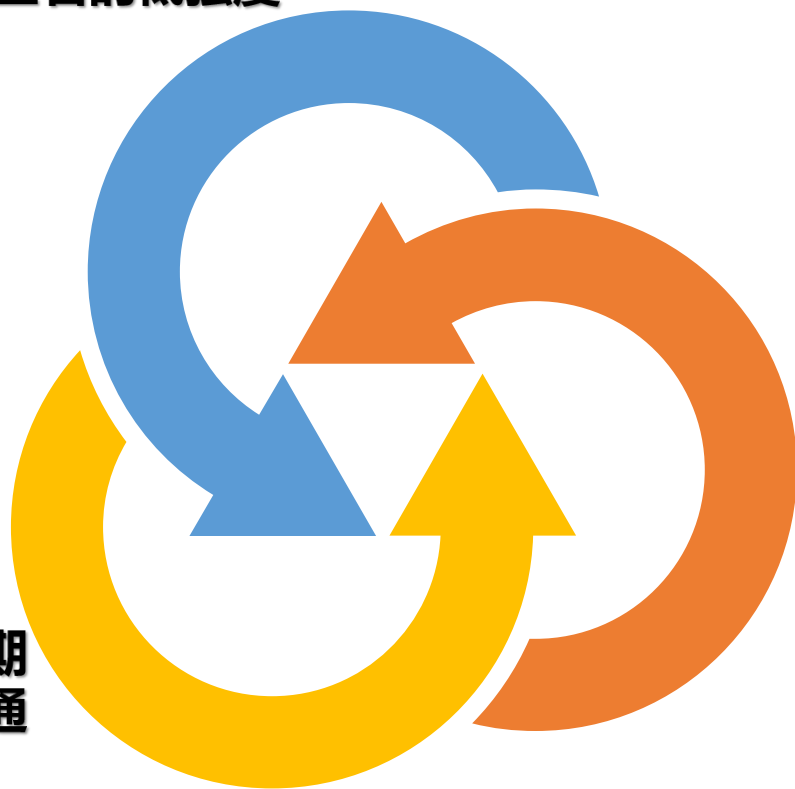
镭速服务端完整记录了管理员操作日志，包括增加、删除、修改用户信息，修改服务器信息等完整信息，审计人员可定期审计服务器管理员操作行为

06

加密证书生命周期管理

传输服务器只支持由正式根证书服务商
发型的加密证书，防止自签名的低强度
加密证书变成系统漏洞

传输客户端发现传输服务器证书过期
后，会拒绝与传输服务器进行传输通
信，并提示服务器证书已经过期



传输服务器每天检查加密证书有效时间，当有
效时间小于等于30天时，在管理面portal提示
管理员更换及时加密证书

感谢观看
期待与您合作