Raysync Product Safety Technology White Paper

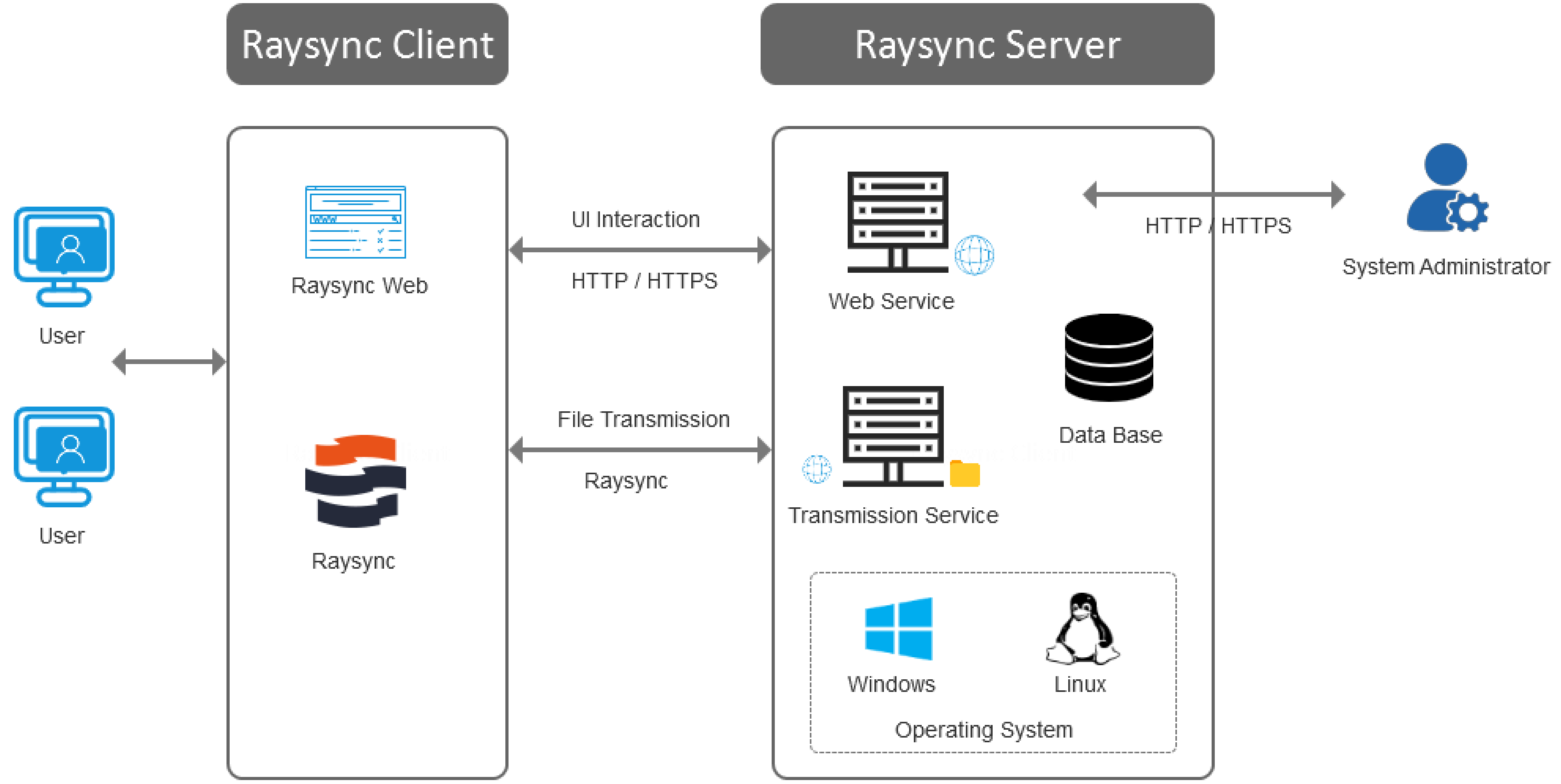
Speedy Raysync

Speedy Reach to the Globe

Raysync

www.raysync.io

Product Structure



Contents

01 Web Security Design

02 Account & Password Protection Security Design

03 Transmission Security Design

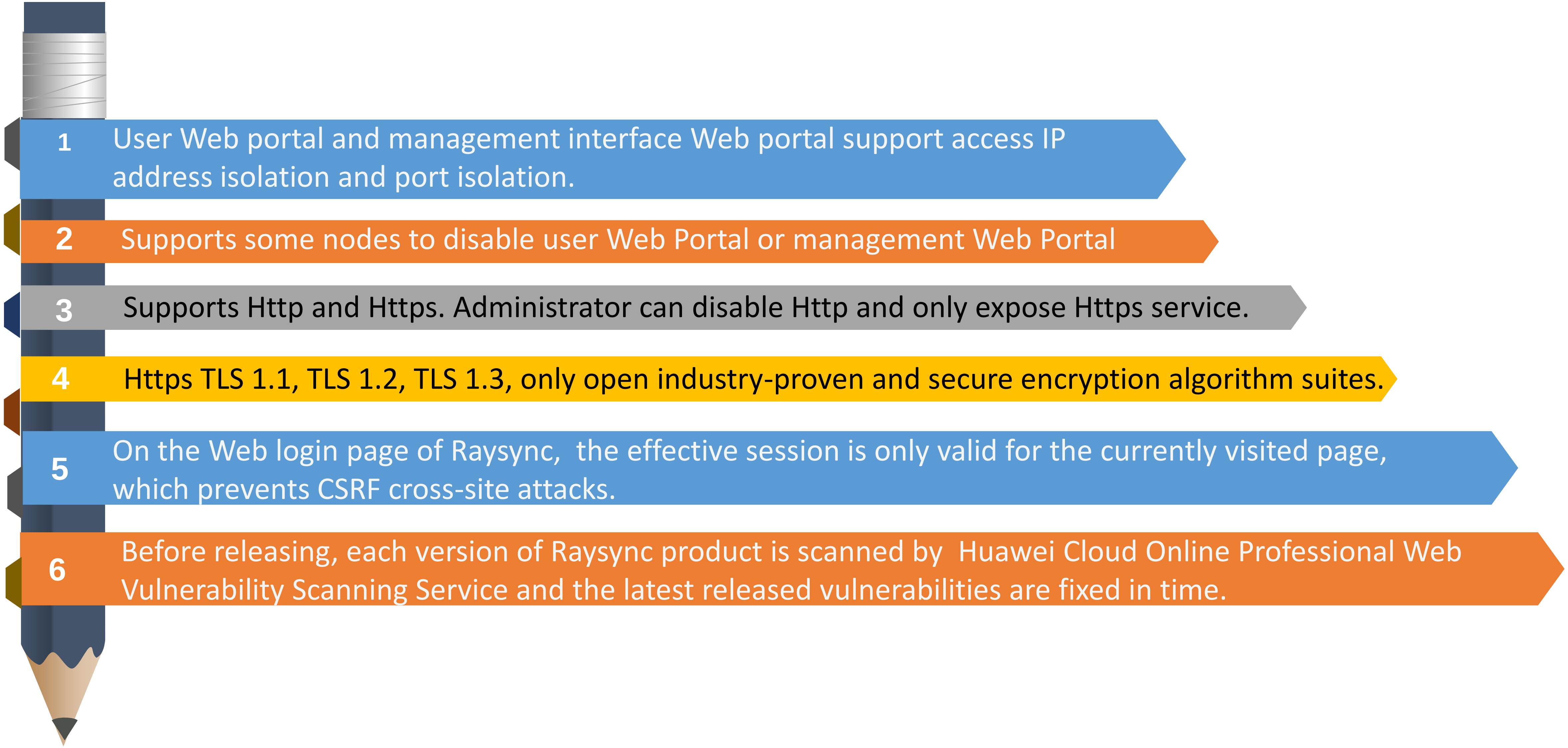
04 Software Installation & Operation Safety Design

05 Behavior Audit

06 Encryption Certificate Life Cycle Management

01 | Web Security Design

Web Security Design



1 User Web portal and management interface Web portal support access IP address isolation and port isolation.

2 Supports some nodes to disable user Web Portal or management Web Portal

3 Supports Http and Https. Administrator can disable Http and only expose Https service.

4 Https TLS 1.1, TLS 1.2, TLS 1.3, only open industry-proven and secure encryption algorithm suites.

5 On the Web login page of Raysync, the effective session is only valid for the currently visited page, which prevents CSRF cross-site attacks.

6 Before releasing, each version of Raysync product is scanned by Huawei Cloud Online Professional Web Vulnerability Scanning Service and the latest released vulnerabilities are fixed in time.

02 | Account & Password Protection Security Design

Account & Password Protection Security Design

- Login authentication has a built-in mechanism prevents brute-force attack. When the user enters wrong passwords by 5 times consecutively within 3 minutes, the account will be locked automatically.

- The session ID during login is generated by OpenSSL high-intensity random function RAND_bytes () interface, which prevents random information from being hit by the simulator.

Account & Password Protection Security Design

The user password is encrypted by asymmetric high-strength encryption algorithm during transmission. Even if the transmission message is intercepted, the attacker cannot recover the plaintext through the ciphertext.

The information stored in the database through the user password is one-way encrypted irreversibly by PBKDF2 algorithm and the user's separate random salt for 10,000 times. Even if the database information is leaked, the user password cannot be reversed through the ciphertext.

Mandatory password strength protection requires that the password must be a combination of upper cases, lower cases, numbers, special symbols in a length greater than or equal to 8 characters.

The system provides a dictionary of weak passwords.
Users can customize weak passwords that may meet requirements but still may be cracked easily by social engineering. System prohibits users using such passwords, such as <Company English Name> @ 123.

03 | Transmission Security Design

Transmission Security Design

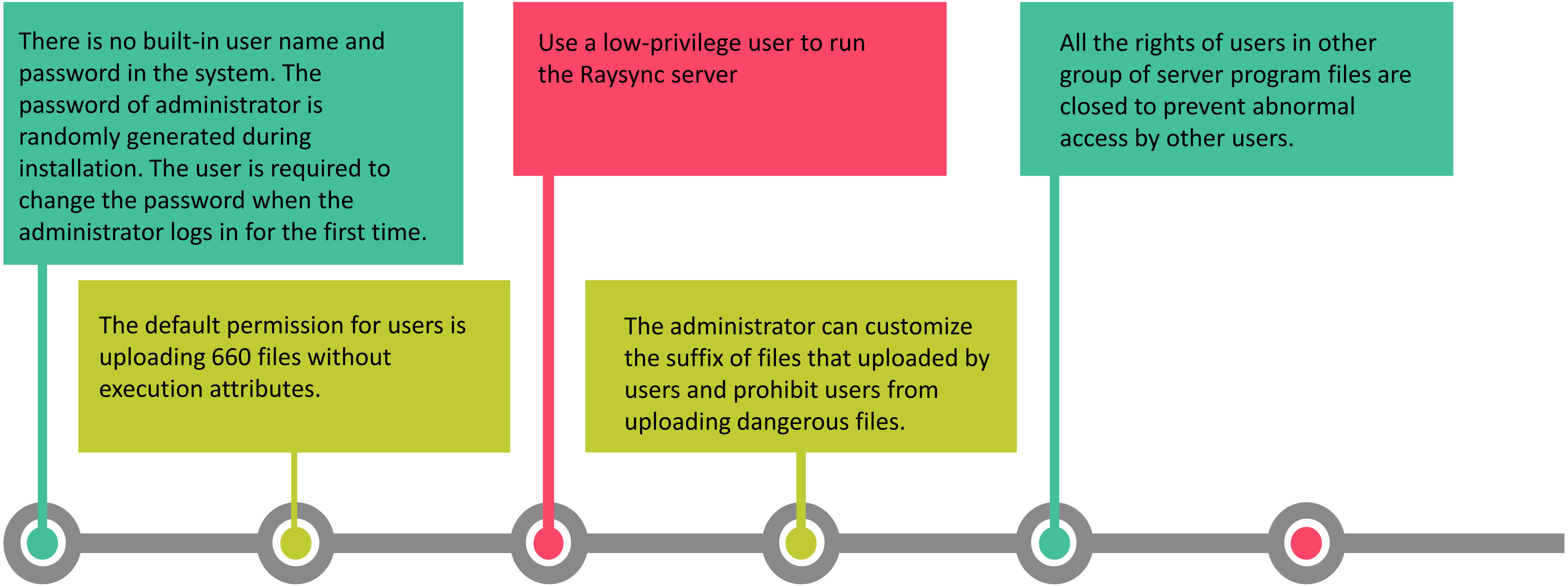
During the transmission process,
Raysync performs Hash verification protection on the transmission message level, file block and entire file to ensure the integrity of the transferred data.

TLS 1.3 encryption is applied between Raysync client and Raysync server, preventing man-in-the-middle attacks from the network.

Raysync transmission only needs to expose one port to meet all users' access, which greatly reduces the risk of firewall port exposure.

04 Software Installation & Operation Safety Design

Software Installation & Operation Safety Design



There is no built-in user name and password in the system. The password of administrator is randomly generated during installation. The user is required to change the password when the administrator logs in for the first time.

The default permission for users is uploading 660 files without execution attributes.

Use a low-privilege user to run the Raysync server

The administrator can customize the suffix of files that uploaded by users and prohibit users from uploading dangerous files.

All the rights of users in other group of server program files are closed to prevent abnormal access by other users.

05 | Behavior Audit

Behavior Audit

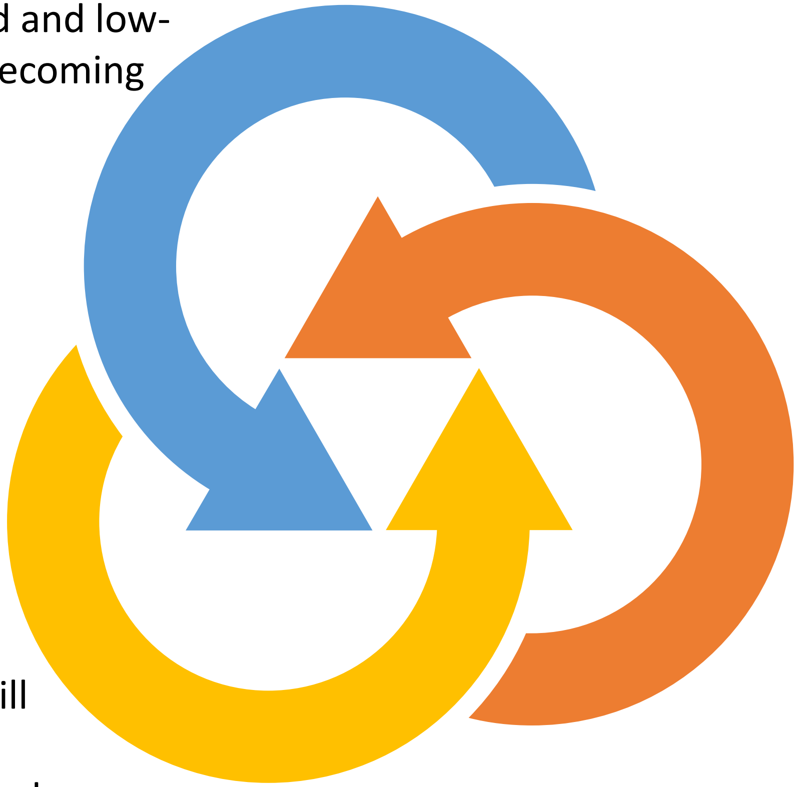
The Raysync server records the complete user behaviors log including login, logout, upload, download, password modification, sharing link, etc. The administrator can regularly audit user behaviors.

The Raysync server records the complete operation log of the administrator, including adding, deleting, modifying user information, modifying server information and other information. Auditors can regularly audit the server administrator's operation behaviors.

06 | Encryption Certificate Life Cycle Management

Encryption Certificate Life Cycle Management

The transmission server only supports encryption certificates issued by official root certificate service providers to prevent self-signed and low-strength encryption certificates from becoming system vulnerabilities.



The transmission server checks the validity of the encryption certificate every day. When the validity is less than or equal to 30 days, the server prompts the administrator to change the encryption certificate.

When the transmission client side finds an expired transmission server certificate, it will refuse to communicate with the server and prompt that the server certificate has expired.

Thank you

Look forward to our cooperation!

Raysync Cloud