[**https://github.com/minio/minio/issues/21592**](https://github.com/minio/minio/issues/21592)

**FTPS does not use renewed certificate without MinIO restart**

**Case Study 1 – Question 5**

FTPS (File Transfer Protocol Secure) is MinIO’s secure file transfer option that uses TLS/SSL certificates for encrypted communication.

Certificates (like those from Let’s Encrypt) usually expire and renew automatically.

Problem Explained

When a new TLS certificate is renewed (for example, minio.crt and minio.key are replaced with updated ones),

MinIO continues using the old certificate until the server process is restarted.

In other words:

Even though the new certificate files exist on disk,

MinIO’s FTPS service does not reload them automatically,

So clients still see the expired certificate.

**Technical Reason**

When MinIO starts, it loads the SSL certificate into memory.

During runtime, there is no built-in watcher to detect certificate changes.

So when the certificate renews (e.g., via Certbot or cron job),

The old certificate remains in use until the MinIO server restarts and reloads it.

Workaround / Fix

To make MinIO use the renewed certificate:

Restart the MinIO service after certificate renewal.

Or

Automate the restart using a cron job or systemd hook after the certificate renewal script runs.

Example (Linux systemd):

systemctl restart minio

If you’re using Let’s Encrypt, you can add a --deploy-hook:

certbot renew --deploy-hook "systemctl restart minio"

**CONCLUSION**

MinIO’s FTPS keeps using the old SSL certificate because it loads it only at startup.

When a new certificate is renewed, MinIO must be restarted to use it — otherwise, clients still see the expired one.