Enable Strict Transport Security In Apache Virtual Host for Nextcloud

Enable HTTP Strict Transport Security

While redirecting all traffic to HTTPS is good, it may not completely prevent man-in-the-middle attacks. Thus administrators are encouraged to set the HTTP Strict Transport Security header, which instructs browsers to not allow any connection to the Nextcloud instance using HTTP, and it attempts to prevent site visitors from bypassing invalid certificate warnings.

This can be achieved by setting the following settings within the Apache VirtualHost file:

```
<VirtualHost *:443>
  ServerName cloud.nextcloud.com
    <IfModule mod_headers.c>
      Header always set Strict-Transport-Security "max-age=15552000;
includeSubDomains"
    </IfModule>
 </VirtualHost>
```

This example configuration will make all subdomains only accessible via HTTPS. If you have subdomains not accessible via HTTPS, remove includeSubDomains. Consider how this would affect integration with OnlyOffice Document Server hosted on a subdomain of the NextCloud domain, unless the subdomain is added to or included in the LetsEncrypt SSL certificate.

IMPORTANT: This requires the mod_headers extension in Apache.

Let's see how to enable headers module using a2modenable