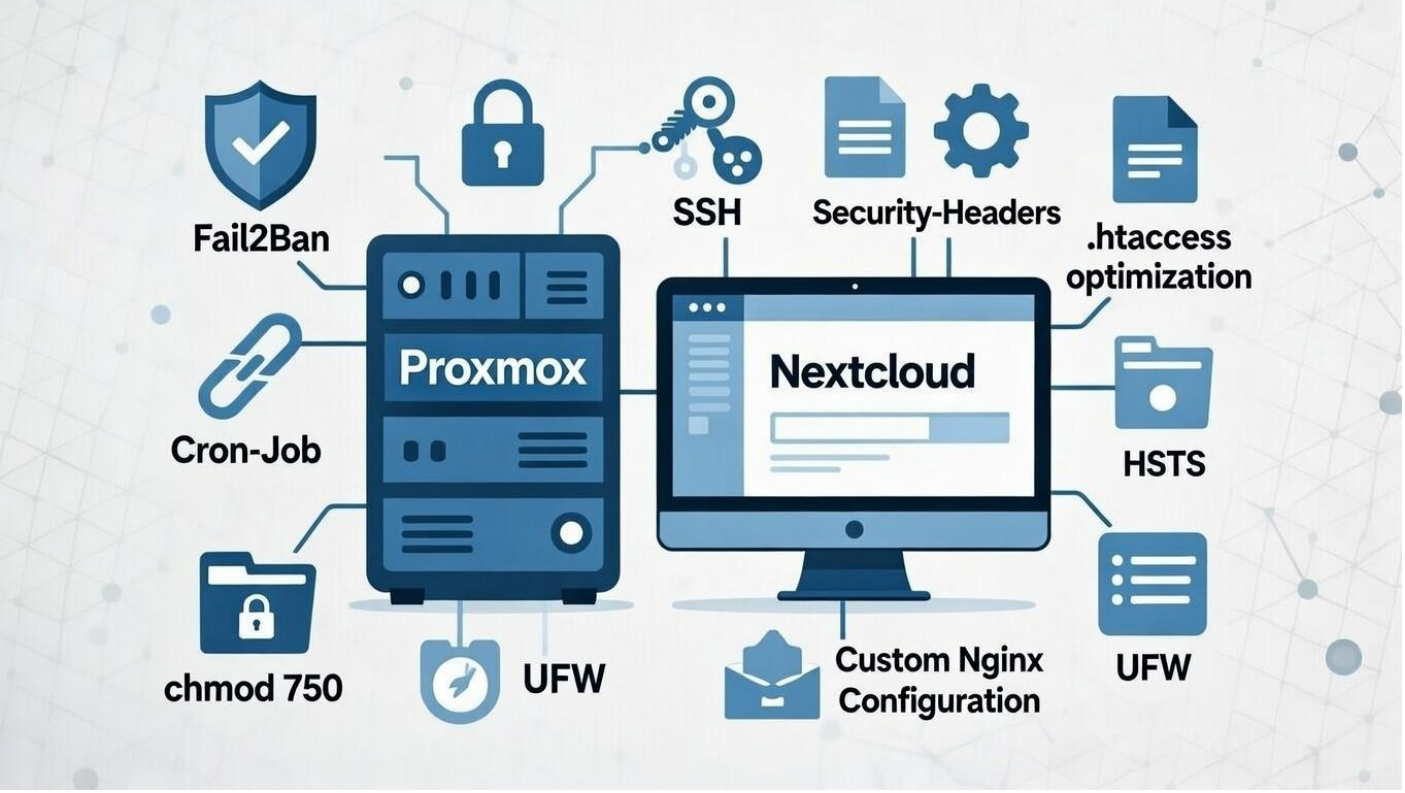
Part 4: Recommended Security Settings and System Hardening



Below are several items you should review again after completing the setup. You may already have configured many of them, but a second verification is always advisable.

Update the System and Install Base Packages

After the first boot, log in as `root` or `ncadmin` (depending on console or SSH access) and immediately run:

```
apt update && apt full-upgrade -y
```

This installs all security updates and bug fixes released since the ISO was built.

Then install useful base utilities:

```
apt install sudo vim htop curl wget net-tools -y
```

This ensures sudo availability for regular users and provides improved system and networking tools.

Harden SSH – Disable Password Login and Use Keys

SSH is enabled during installation but not yet hardened.

Edit:

```
sudo nano /etc/ssh/sshd_config
```

Set:

```
PermitRootLogin prohibit-password
PasswordAuthentication no
```

Generate an SSH key on your client:

```
ssh-keygen
```

Copy the public key to the server:

```
ssh-copy-id ncadmin@your-vm-ip
```

Restart SSH:

```
systemctl restart ssh
```

From this point forward, only key-based authentication is allowed, effectively preventing password brute-force attacks.

Configure Cron for Nextcloud

Nextcloud requires a recurring background job (file scanning, mail delivery, app updates, etc.).

Create a cron job:

```
crontab -e
```

Add:

```
*/5 * * * * php -f /var/www/cloud.zn80.net/cron.php
```

Alternatively, use a systemd timer.

Without cron, background tasks run only during active web sessions, which can cause delays or stuck jobs.

Note: Normally, the cron job is created with:

```
crontab -u www-data -e
```

This may not work in this setup if the ownership of the configuration file has been changed earlier.

Install Fail2Ban Against Brute-Force Attacks

Install Fail2Ban:

```
apt install fail2ban -y
```

Enable and start it:

```
systemctl enable --now fail2ban
```

Fail2Ban monitors SSH logs and bans IP addresses after multiple failed login attempts (default: 5 attempts within 10 minutes). The Debian defaults are typically sufficient for a homelab environment.

Optional: Adjust `/etc/fail2ban/jail.local` for longer ban durations or email notifications.

.htaccess Optimization and Security Headers

After installation, update the `.htaccess` file:

```
sudo -u www-data php occ maintenance:repair
```

Add security headers in the Apache VirtualHost configuration (preferably under `*:443`) or in your reverse proxy configuration:

```
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-XSS-Protection "1; mode=block"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

If running behind Nginx Proxy Manager, add the following under the proxy host's custom configuration:

```
add_header X-Content-Type-Options "nosniff" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-XSS-Protection "1; mode=block" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
```

These headers mitigate:

- MIME sniffing attacks (`nosniff`)
- Clickjacking (`SAMEORIGIN`)
- Reflected XSS (`mode=block`)
- Unnecessary referrer exposure (`strict-origin-when-cross-origin`)

Enable HSTS (Strict-Transport-Security)

Within the proxy host SSL settings, enable:

- **Force SSL**
- **HSTS Enabled**
- **HSTS Subdomains** (if applicable)

Nextcloud expects at least:

```
max-age=15552000
```

If necessary, manually add:

```
add_header Strict-Transport-Security "max-age=15552000;
includeSubDomains" always;
```

Important: Only enable HSTS if HTTPS is permanently available.

Additional Reverse Proxy Adjustments (Optional)

To prevent header conflicts or WebSocket upgrade issues:

```
proxy_hide_header Upgrade;
proxy_hide_header Connection;
```

For additional protection:

```
add_header Permissions-Policy "geolocation=(), microphone=(),
camera=()" always;
```

After saving, test the Nextcloud instance (Admin ? Overview / Security scan).

Adjust Data Directory Permissions

The data directory `/srv/cloud.zn80.net/data` should preferably use:

```
chmod 770 /srv/cloud.zn80.net/data
chown -R www-data:www-data /srv/cloud.zn80.net/data
```

While `750` may work, `770` is recommended to prevent permission issues during app installation or large uploads.

Enable Firewall with UFW

If the server is directly exposed to the internet, install UFW:

```
apt install ufw -y
```

Allow necessary ports:

```
ufw allow OpenSSH
ufw allow 80,443/tcp
```

Enable and verify:

```
ufw enable
ufw status verbose
```

UFW blocks all other ports by default.

Additional Security Recommendations

- Use a dedicated sudo-capable user and avoid permanent root login.
- Enable automatic security updates:

```
apt install unattended-upgrades -y
```

Review configuration in:

```
/etc/apt/apt.conf.d/50unattended-upgrades
```

Check for updates regularly:

```
apt list --upgradable
```

With these measures in place, your Nextcloud instance should achieve strong security ratings (e.g., A/A+ on securityheaders.com or Mozilla Observatory) and display no major warnings in the Nextcloud admin security overview.

Revision #10

Created 2026-02-01 12:48:12 UTC by Carsten

Updated 2026-02-14 15:14:07 UTC by Carsten