Configure Cron Jobs and File Permissions Safely

Hosting Management · https://support.jansma.vip/docs/vip-hosting/hosting-management/configure-cron-jobs-and-file-permissions-safely/

Scheduled tasks and file permissions are powerful hosting controls. Configure them with least privilege, predictable logging and a clear rollback plan.

Create a cron job

1. Identify the exact command or secure URL and how often it genuinely needs to run.
2. Use absolute paths and the correct runtime version.
3. Redirect useful output to a protected log or notification destination.
4. Run the command manually once, then schedule a conservative interval.
5. Confirm the expected result and monitor repeated failures.

File permissions

Files should normally be writable only by the account that needs them; directories require execute permission for traversal. Avoid world-writable permissions. Use the hosting permission checker or file manager to identify unsafe settings, then correct only the affected paths. Application-generated upload and cache directories may need different permissions from executable code.

Safe operation

Do not place passwords or tokens directly in a cron command visible to other tools. Prevent overlapping jobs where possible, set timeouts and remove obsolete schedules. If a permission change causes an error, restore the previous value and review ownership before broadening access.