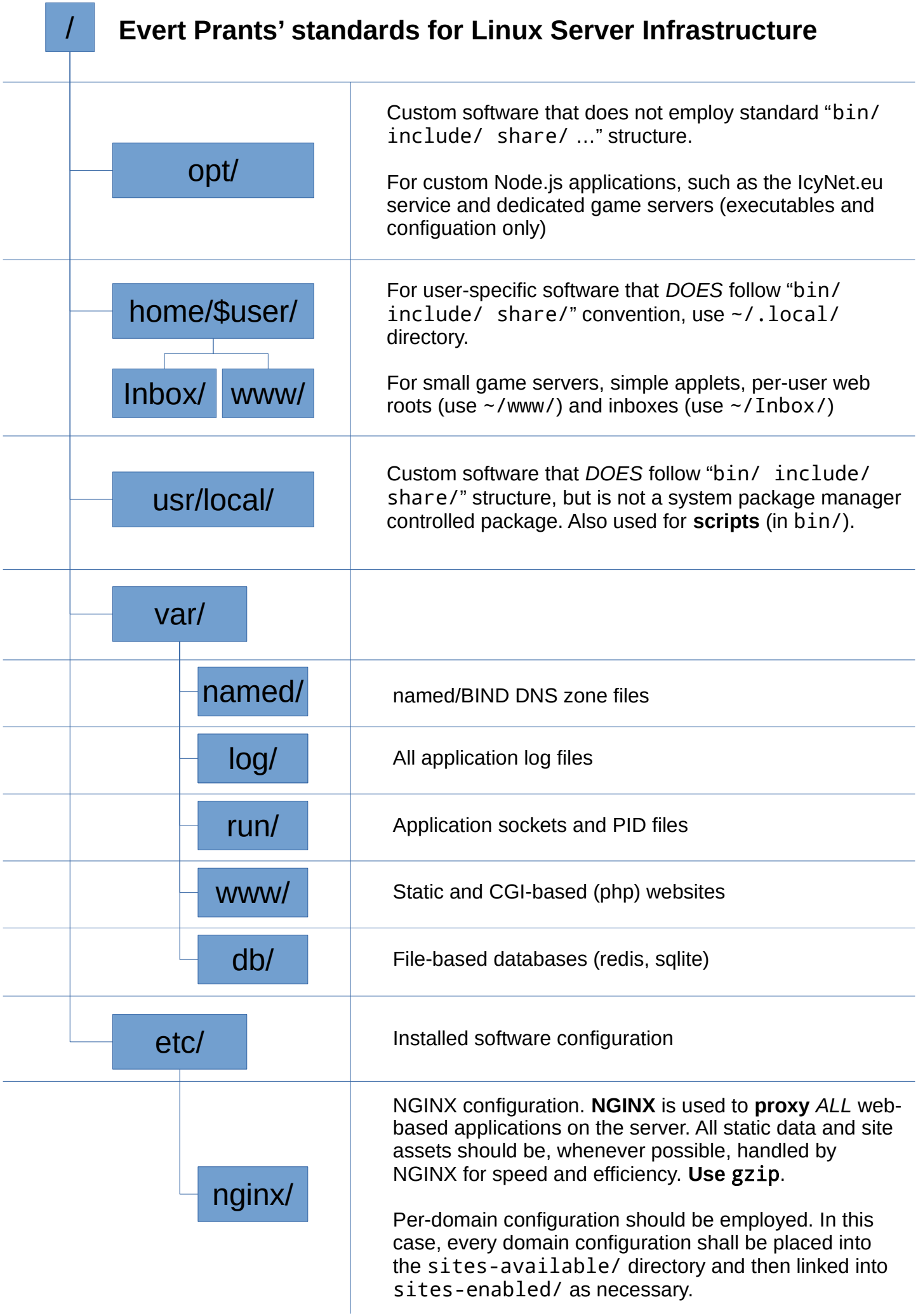
/ Evert Prants' standards for Linux Server Infrastructure



Backups

Here are some of the types of backups that can be implemented in this structure:

- Full disk image
- Compressed file of all services' configurations and data
- Per-service compressed file backup of configurations and data
- Per-service diff from previous backups

Disk image backups are intensive in both processing power and storage resources, thus they should be done in moderation (e.g. once a month).

It is recommended to create backups of critical information hourly, such as user data (transactions, tokens, etc.). User-generated content (files) should be backed up daily if the files are critical or accessed often, or weekly in case the files are not important to the service's operation (e.g. profile pictures) or not accessed/modified frequently.

Backup and recovery procedures should be automated as much as possible.

Mounts

For storage devices attached to the server, it is recommended to mount all of them into *descriptive* sub-directories of `/mnt/`, for clarity (make sure to use proper permissions on the mounts!)

For storage devices dealing with application data, such as user files (nextcloud) or media servers, the **`/srv/` directory** should be used **in addition**. In a single-partition server, the `/srv/` directory is the **only** recommended storage place for large application data (which is not stored in a database structure).

Other decisions

Evert's systems usually do not use docker images, as in my opinion, they are not necessary. Most of my services are deployed locally on the system. I do not see any significant security or performance benefits to using a docker image, for the most part. The only instances I would consider using docker is when the application is exceedingly large, requires multiple dependent applications that are not used by any other service on the system and/or software that depends heavily on outdated libraries that when updated, break the software and require re-building.

FTP servers are to be avoided. I know that FTPS exists but I still do not recommend FTP services. For file transfer, we have better, more secure and more modern technologies such as SSHFS/SCP (SFTP) and WebDAV.

For security purposes, all services have their own dedicated user and users with administrative rights (root and users in /etc/sudoers) are **only** to be logged in using SSH keys.