Production Checklist

Table of contents

Here's a list of points you should take care of when running Lenya in a production environment. It covers only the most obvious aspects, but it might prevent you from falling in the biggest traps in first real-world project.

1. General Deployment Recommendations

- Seperate your web application from your data. This applies to the content, access control, and work data (search index, cache).
- When creating backups of your data, make sure you'll still know which version of the application they're compatible with when you need them again.
- Always have two instances of Lenya ready, and make sure you can switch between them immediately (e.g., by changing a symlink to a proxy configuration file).
- Consider using vendor branches for Lenya, Cocoon etc. This helps you to stay flexible when you're faced with bugs, endorsed library issues etc.
- When you deploy a version of your application, **always** create a branch in your code versioning system. This way, you can merge essential bugfixes from the trunk and re-deploy the application. **Never** deploy an un-tagged development version.

2. During Development

- Run sophisticated and thorough load tests early and often.
- Run search engine crawlers on your site. Observe the performance behaviour and session handling.
- Test the site in various browsers, using various settings (disabling JavaScript etc.), and preferrably using different bandwidths.
- Make sure you don't create weak points for DoS attacks (e.g. by expensive dynamic generation of non-cached pages based on request parameters).

3. Preparation (Internal Pilot Phase)

- Set the log level to *ERROR*.
- Make sure that the logs stay clean. If exceptions occur, mercilessly track them down and eliminate their causes. Even if you consider some exceptions "normal" behaviour - they aren't.

4. Production

- Double-check your access control settings.
- Set the log level to *FATAL* or at least *ERROR*.
- Disable all modules which accept request to dynamically generate images to prevent DoS attacks.
- Consider disabling image upload.
- Set the session expiration time to the least acceptable value.
- Prepare for maintenance (updates etc.), either by switching the application or by showing a friendly information page.
- Prepare for a worst-case scenario. For instance, have a statically exported version of the site ready.