Linux Administration

Server operations

Xavier Belanger

System administrator duties

- System upgrades and patching
- Data security and backups
- User access and permissions
- Monitoring and logging

Scheduled maintenance

- Upgrade and similar tasks should be scheduled at specific times to have a minimum impact on business operations.
- Changes should be documented, tested, approved and including a rollback plan.

Backups

- Data backup (both files and databases) should be running on a regular schedule. Restoration operations should be tested.
- Backup files should be stored in a safe location (not accessible from the production systems).
- Laws, regulations and compliance rules are likely going to set requirements on backups (retention time, encryption, ...).

User accesses and permissions

- As a general rule, only minimum access should be granted to users.
- Privileged access should require multi-factor authentication (MFA).
- When possible, user interactions should be logged.

Monitoring

Two types of monitoring is usually required:

- resources (CPU, memory, networking, storage, ...) in order to satisfy the system, application and users needs over time.
- events (system changes, outages, errors, ...) to detect issues as quickly as possible.

Hardening

In order to secure a system, you need to reduce any area that could lead to an issue.

- Configuration should be enforced to provide the best security possible.
- System and applications should be patched on a regular basis.