Provisioning of AD for the lab on the university

Motivation

Students at the Faculty of informatics MU are working together with teachers on various cryptographic and security topics in the lab called CROCS. Services that are available to students are primarily Windows devices and XEN virtualization. As those tools are used to experiment in cybersecurity topics, the lab has its own infrastructure to make sure that experiments will not interfere with university infrastructure. Both of them are using Active Directory as an identity provider, so the main goal will be to provision accounts to AD.

Requirements

- error handling
- deploying accounts without passwords
- sending the mail about the account creation - the password needs to be changed
- deploying groups
- different identities from university ones (security reasons)

Current architecture

The Perun is storing user information on the shared SMB mount; the CRON script is periodically taking the new data and provisioning them to the AD (creating user accounts without passwords).

Another component is web application simply called Password Changer which operates behind university single sign-on solution. The application handles the provisioning of the passwords just in time.

Proposed and implemented architecture
Benefits of the new architecture

- Absence of SMB share (maintenance of an additional part, possible race-condition)
- Push method (Perun is pushing new member accounts, CRON job elimination)
- Support for states (errors during provisioning etc.)
- Monitoring (provisioning is monitored with a university monitoring system)