

# Enhancing the user life-cycle management in EGI Federated Cloud

Slávek Licehammer

EGI Community Forum 2015



# Simple approach

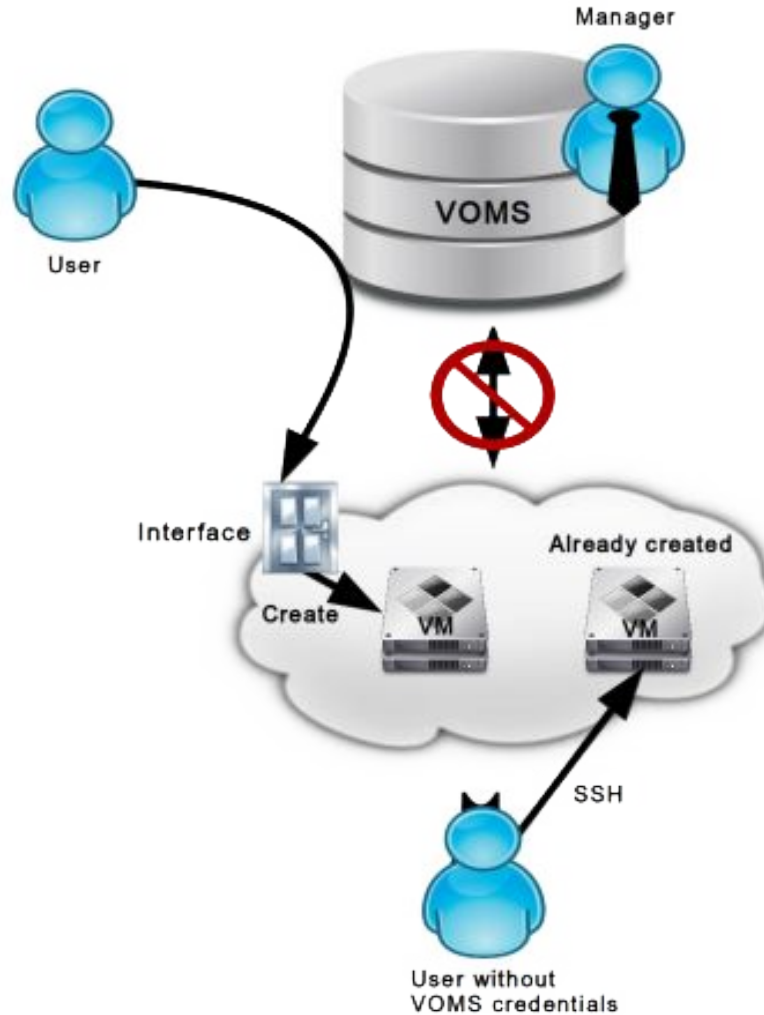
- Users are managed in VOMS
- Users with valid VOMS proxy can access FedCloud infrastructure
- Autocreate of accounts
- Site knows only DN of users



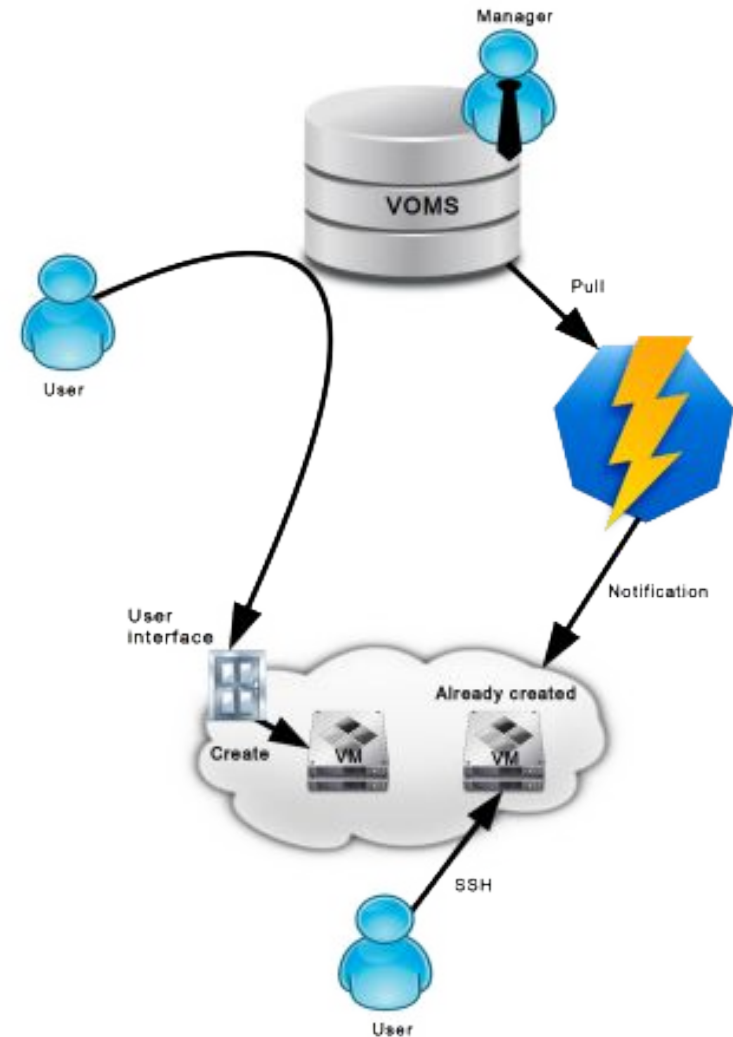
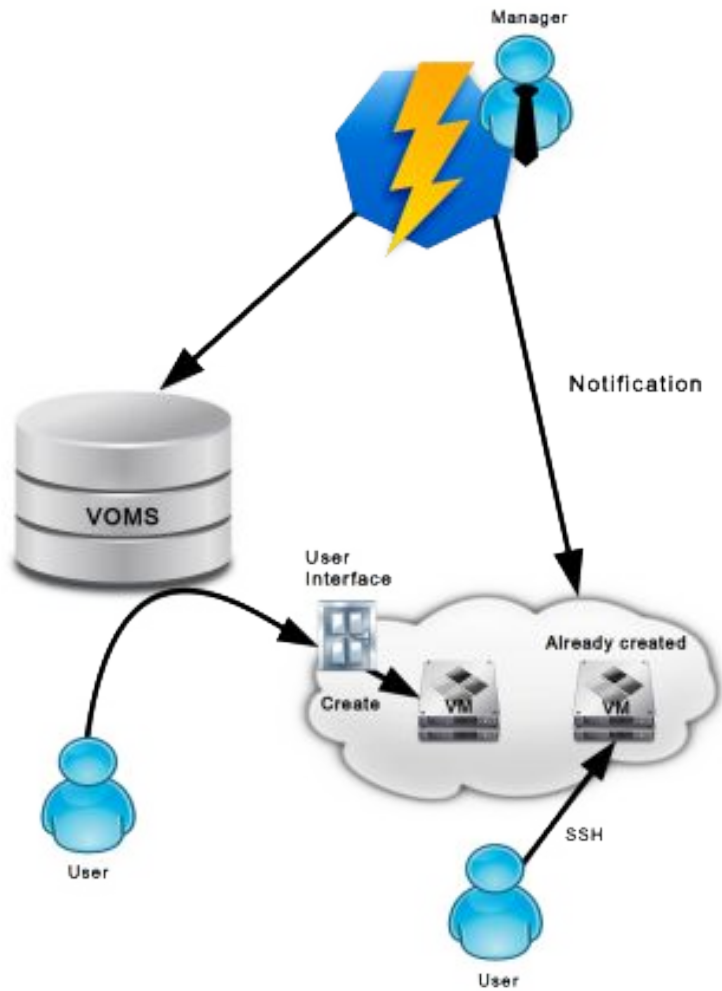
# Issues

- User life-cycle
  - Stop/suspend VMs of expired users
- Change of user's credentials
  - Users want to access existing VMs with new certificate
- Utilization of user's attributes
  - e.g. user e-mail
- Dealing with security incidents
  - Collaboration with EGI CSIRT

# Simple approach



# Management using Perun





# Solution using Perun

- Push model (provisioning / deprovisioning)
  - Services are notified about changes
  - Services can react appropriately
  - Does not add single point of failure
- User management in Perun
  - Customizable enrollment
  - Import users from other system
  - Group management
  - Access management



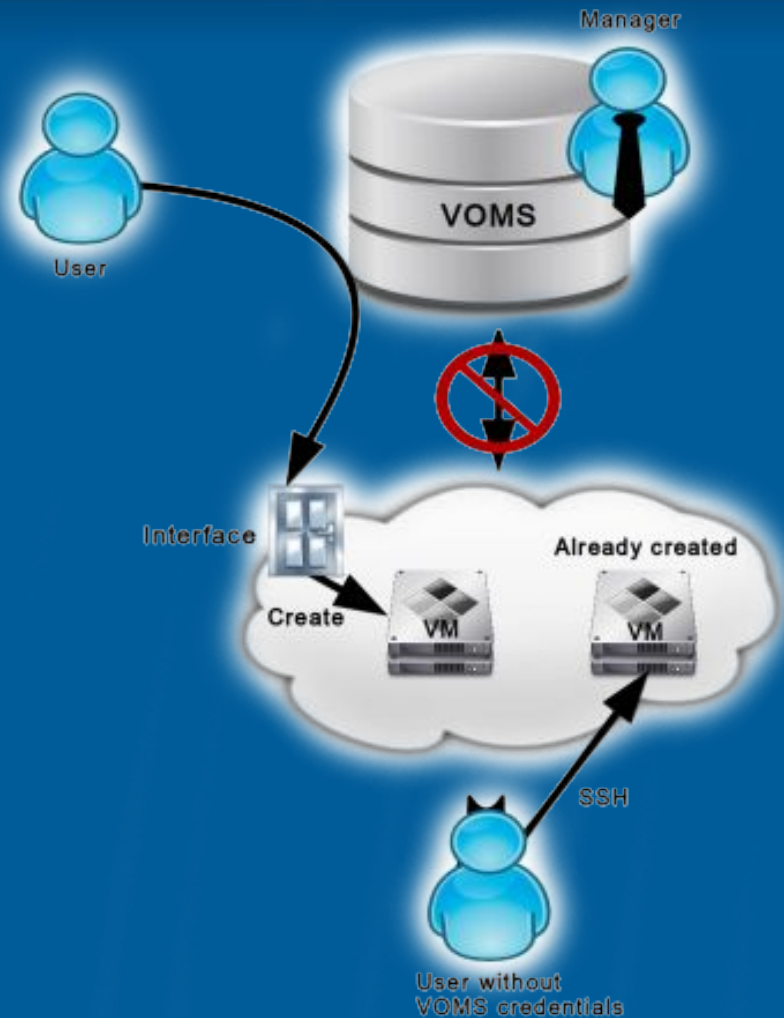
# Identity consolidation

- User's have several identities
  - X.509, eduGain, EGI SSO, ...
- Link several identities to one user account
  - Services knows the user is same regardless of the identity that he/she uses
  - Enable change of identity
    - e.g. new certificate
    - migration from “long tail of science” to normal account

# Collaboration with EGI CSIRT



- ARGUS server is used for banning users
- Not supported in cloud platforms
- Block users on VOMS level is not sufficient





# Collaboration with EGI CSIRT



- Introducing security teams inside Perun
- Security team publishes blacklist of users
  - Will be synchronized with ARGUS
- Site/Service decide which security team trusts
- Services/Sites get notified about blacklisted users using push model
  
- Pilot on CESNET's OpenNebula site with collaboration with EGI CSIRT



# Summary and conclusion

- Using Perun
  - EGI core service
  - Manage VO / synchronize with VOMS
- Push model
  - Deal with user life-cycle, attributes and identities
- Collaboration with EGI CSIRT
  - Ban users on cloud sites
- Used on Fedcloud sites which use OpenNebula
- Working on integration with LTOS pilot



**perun**

<http://perun.cesnet.cz>

[perun@cesnet.cz](mailto:perun@cesnet.cz)