Identity management in University POLITEHNICA of Bucharest

Mihai Carabaș
mihai.carabas@cs.pub.ro

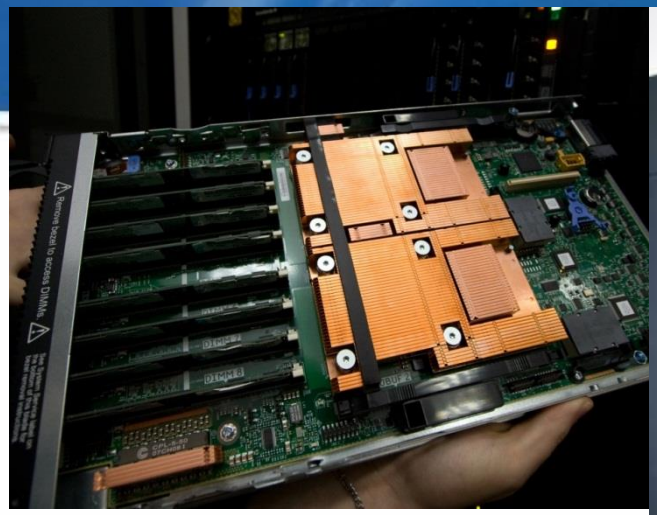
National Center for Information Technology (NCIT)
University Politehnica of Bucharest

Agenda

- About me
- The size of the organization
- Identity management framework
- Directory Services pre-requisites
- 389 Directory Server Setup
- Active Directory Setup
- Services using LDAP

About me

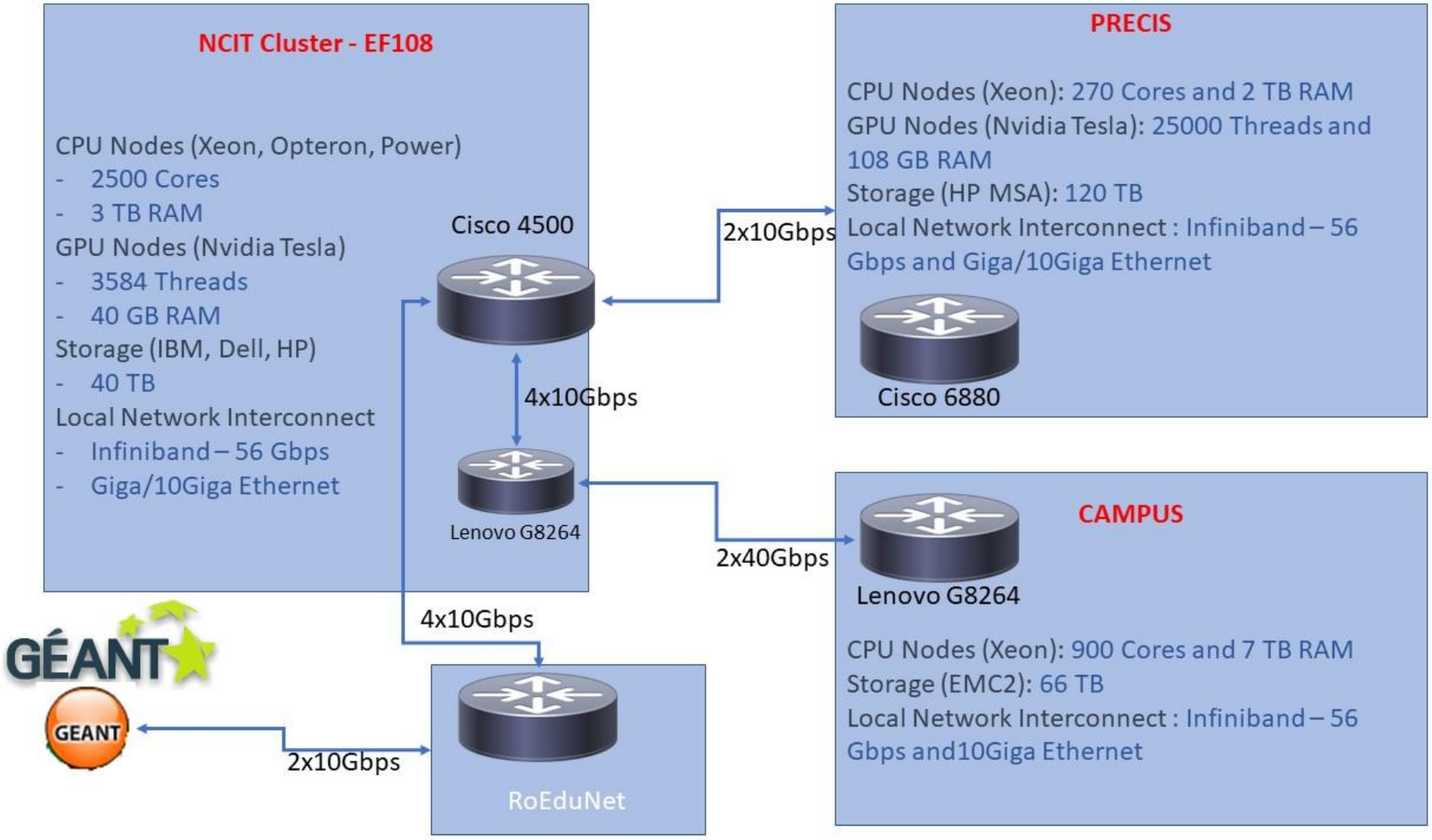
- Associate professor at University POLITEHNICA of Bucharest
- PhD in virtualization of embedded devices in 2017
- In my spare time, hosting Production Services for the whole University
  - e-Learning Platforms
  - Identity Management System (hybrid LDAP/AD)
  - Cloud Controller Services
  - Grid Services (CE, SE, WMS, LFC, ARGUS, VOBOX)



UPB

Computer Science & Engineering Department

UPB Datacenters



The size of the organization

- 14 Faculties
- 3000 employees (Profesors + Administrative personnel)
- 25 000 students yearly (bachelor, master, PhD)
- 100.000 identities (gathered from 2007 until now)

Identity provisioning

- Current sources of data
  - Students database (custom one, managed internally: https://studenti.pub.ro)
  - Human Resources database (external developed)

- Custom framework
  - Frontend (scripts) written in Perl (due to good support un UTF8: **ț vs t**, **ș vs s**, etc.)
  - Backend written as procedures in SQL
  - Connectors to pull data from different databases
    - Basically SQL queries

Managing changes

- How do we get the new users?
  - Create a custom SQL query to exclude the current users
- How do we get changes of current users?
  - Iterate through each user and make a query to see if there are any changes
- Takes a lot for 25.000 entries and put a big stress on the source database

Managing changes (2)

- Get all the data with a single SELECT *
  - Very fast and no stress on the source database
- Use two tables
  - One with the current SELECT
  - The other with the previous SELECT
- Create a stored procedure in SQL that would do a diff between those two tables and would result these operations: add / remove / modify

Managing changes (3)

- At the beginning of the year the first synchronization for 25000 student profiles is about 3 hours
- Subsequent synchronization for 25000 students takes about 5 minutes
- We run it every night to create the identity profiles

Directory Services pre-requisites

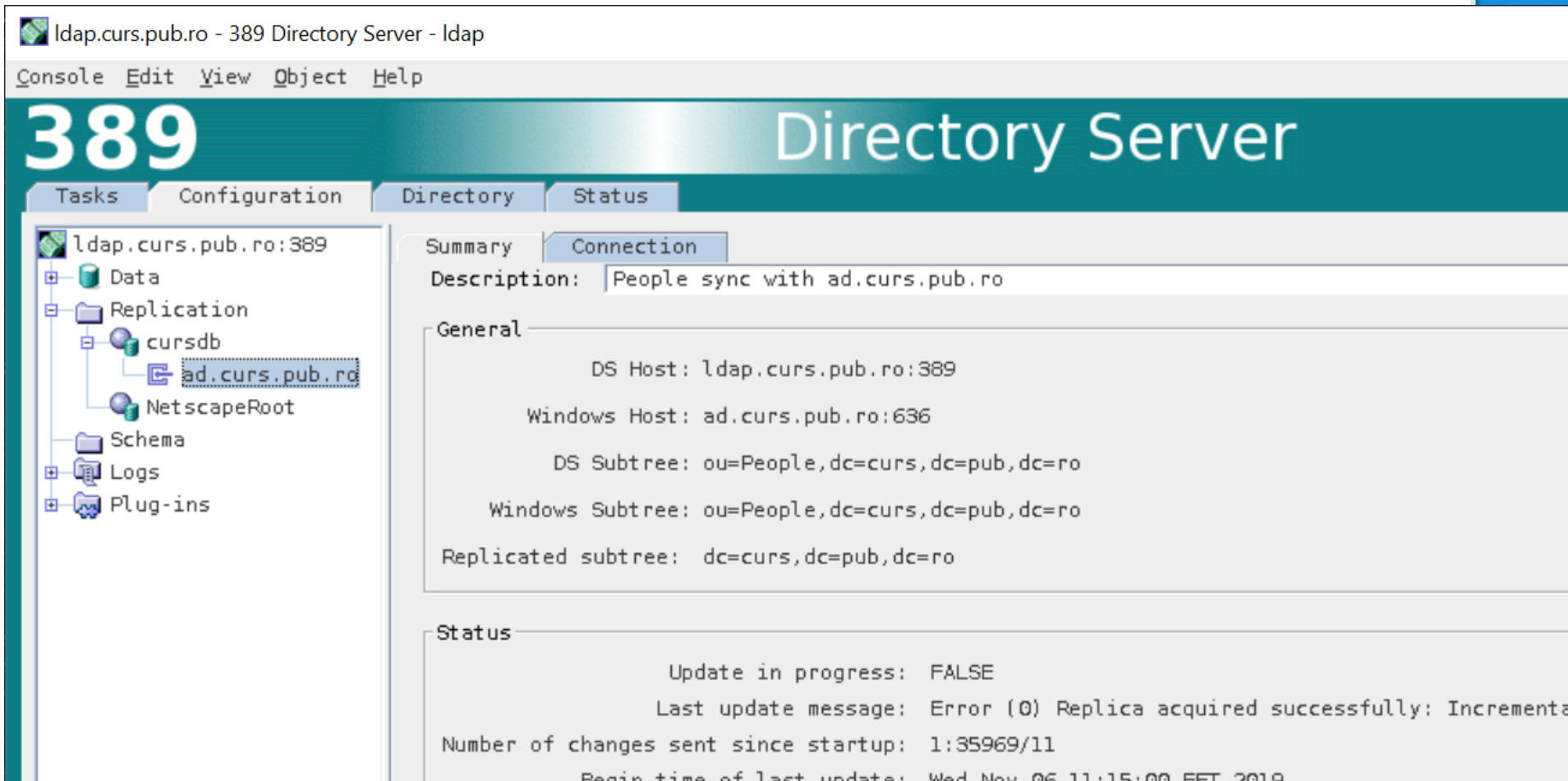
- Provide authentication to internal services like:
  - Elearning platform
  - Email server
  - Wi-fi authentication
- Provide authentication for external services like:
  - Microsoft products
  - Eduroam
- 389 DS -> sync agreements -> Active Directory

389 Directory Server Setup

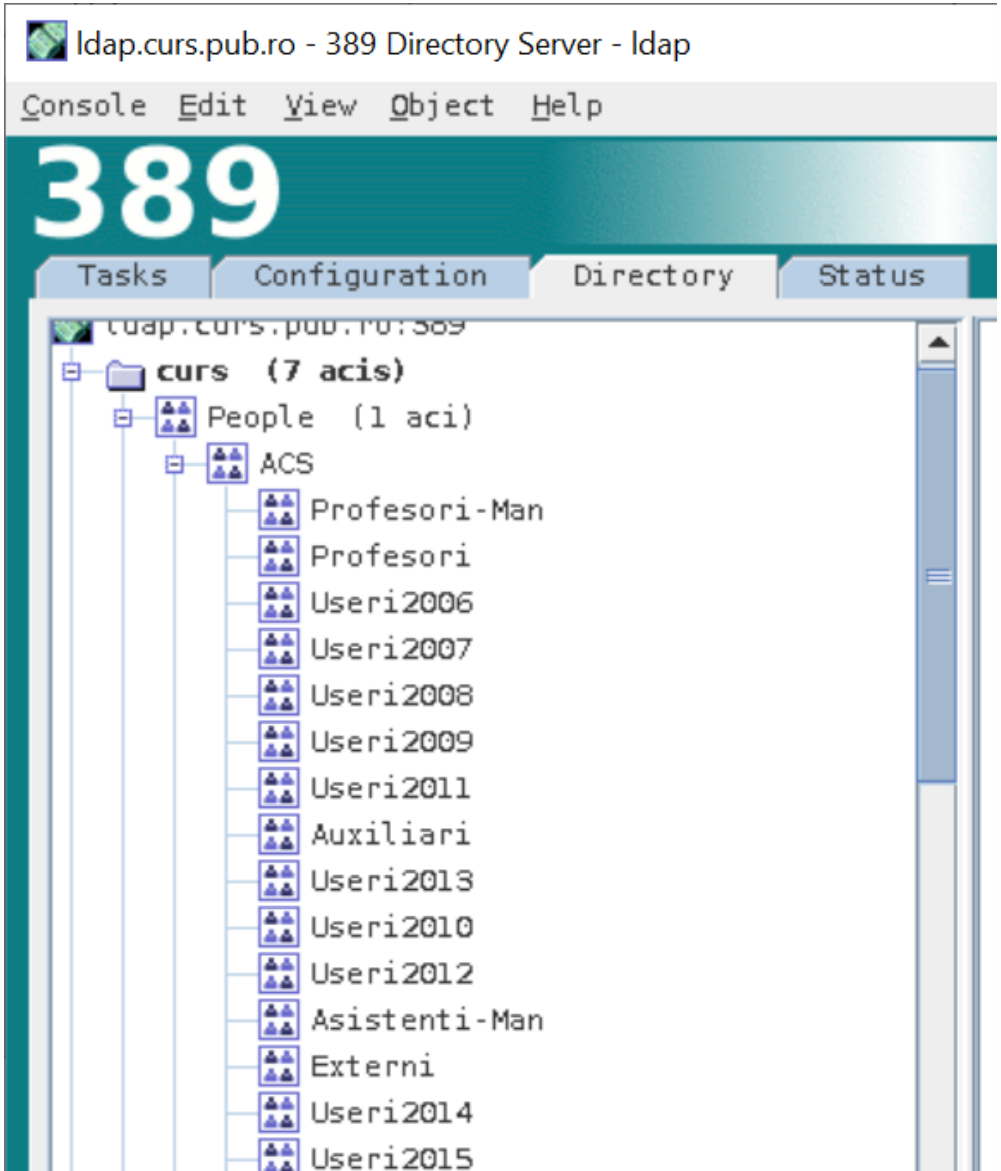
- Fedora release 29 (Twenty Nine)
  - Usually we use CentOS7 but to have the latest package when 389DS is released, we swapped for 389DS to Fedora
- 389 DS 1.4.0.27
- Hyper-V virtual machine on a HA cluster (live migration, disaster recovery replication)
- 8GB of RAM (only 1 used), 4 vCPUs

389 Directory Server Setup (2)

- Active Directory Sync Agreement



Directory Structure



Issues with Sync 389DS-AD

- Attribute uid -> sAMAccountName
  - sAMAccountName is limited to 20 characters
  - We had to trim all the accounts
- userPrincipalName does not have a mapping in 389DS
  - It is basically copied from sAMAccountName
  - If we change the uid, only sAMAccountName
  - We have a background script that periodically makes sAMAccountName equals to userPrincipalName
- uid and sAMAccountName have different restrictions
  - 389DS entries valid which were not being replicated to AD
  - Ex: uid mihai.carabas. is ok in 389DS and not ok in AD

How do we generate usernames

- Multiple rules in our framework, adjusted during the years
- Basically: firstname.lastname
- If conflicts: change the order, use the first letter of the firstname only or add numbers at the end
- Very important: delete non-alpha-numberic characters from the beginning and the end (see sAMAccountName restrictions)
- Maximum 20 characters
- Having 100.000 users, from 2007 until now, at this point we receive complaints about their usernames (especially regarding the numbers)

Active Directory Setup

- Windows 2012R2
- 8GB of RAM, 4 vCPUs
- Roles of AD DS and DNS
- 100.000 synced from 389DS
- A couple of servers

Services using LDAP

- Internal services (usually open source)
  - eLearning platform: Moodle – 389DS
  - Employers e-mail server: Zimbra – 389DS
  - Cluster infrastructure: Authentication on Linux – 389DS with SSSD
  - WiFi authentication (eduroam): 802.1X – Active Directory (using EAP-MSCHAPv2, old Windows 7 had problems EAP-TLS)
  - Cloud infrastructure (Openstack) – 389DS

- External services (free for University from Microsoft / Google / Vmware)
  - Active Directory (Azure AD): Microsoft Imagine (windows licences for teachers and students), Student Emails (O365)

Future steps

- Keep both technologies (389DS and Active Directory)
  - To have options in case of…
- Create a SSO portal in order to be used instead of creating a service account in LDAP for every service
  - Usually I am not the only administrator of a given platform, and other people having access to LDAP credentials, it is not good at all from security perspective
- Create a portal for a user to manage its identity and see the services it has access to

Thank you for your attention

Q & A

cluster.grid.pub.ro
cs.pub.ro