

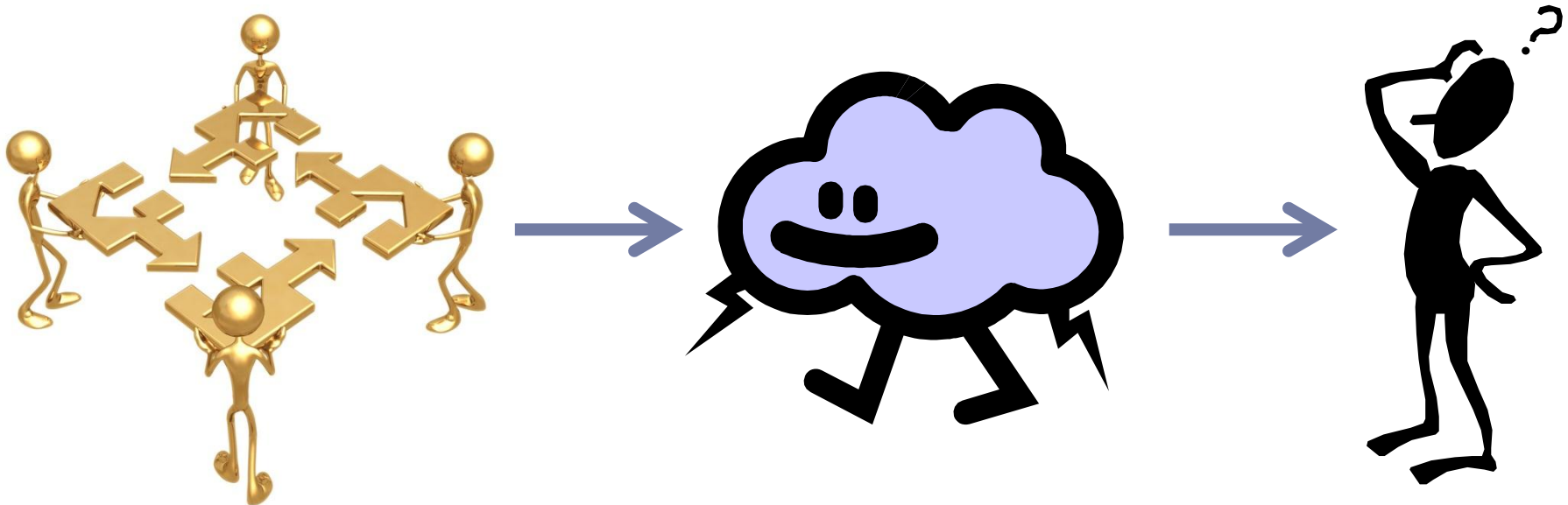


Identity Management to support Hybrid Cloud environments at higher education institutions

Lessons learnt at the Technische Universität München and the Leibniz Supercomputing Centre

EUNIS 2011

- ▶ We spent several years integrating our campus IT services.
- ▶ Then suddenly our users fell for “cloud services”.
- ▶ What does that mean for our identity management?





Our cloud-minded customer: TUM



- ▶ 26,300 students
- ▶ 141 degree courses
- ▶ 400 professors
- ▶ 4,200 academic staff
- ▶ 166 cooperations with other universities
- ▶ 548 Mio. € budget

● TUM-Locations
○ Science Network





The IT service provider: LRZ



- ▶ Services for all Munich HEIs
 - ▶ 120,000+ users
 - ▶ 2,500+ servers
 - ▶ Network covers 500+ buildings
- ▶ Supercomputing center
 - ▶ One of the three German national HPC centers
 - ▶ You wouldn't want to pay our electricity bills ;-)



Image source: Ernst A. Graf

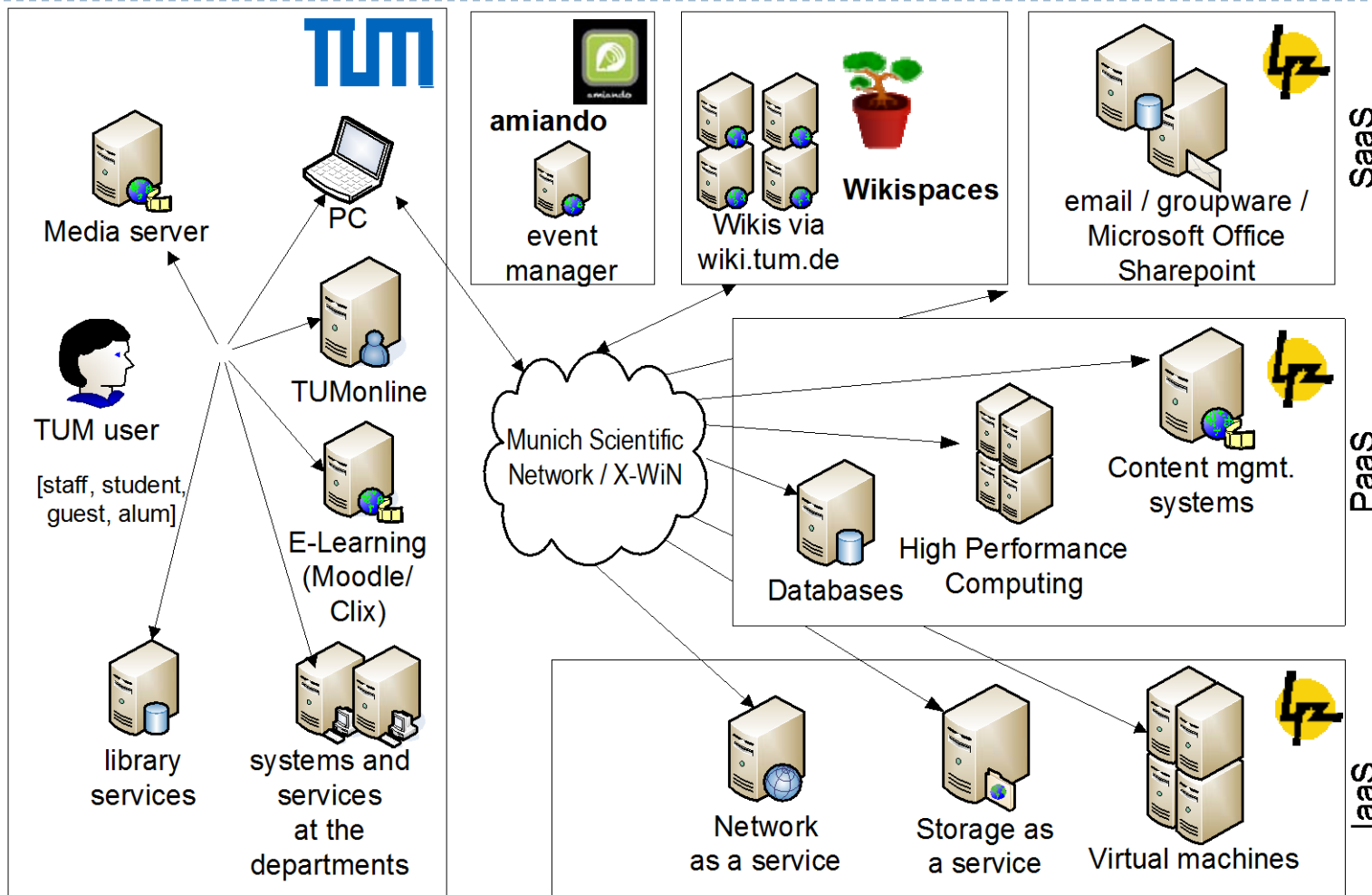
- ▶ IT services used by TUM are either...
 - ▶ TUM-internally provided (by faculties or central service institutions),
 - ▶ LRZ services (usually not TUM-exclusive), or
 - ▶ external commercial “cloud” (dynamic, pay-per-use) services, e.g. Wikispaces, Amiando event management

- ▶ “Hybrid Cloud” environment:
 - ▶ Uses multiple *AAS
 - ▶ Uses both physical and virtual machines
 - ▶ Uses services by internal as well as external cloud providers





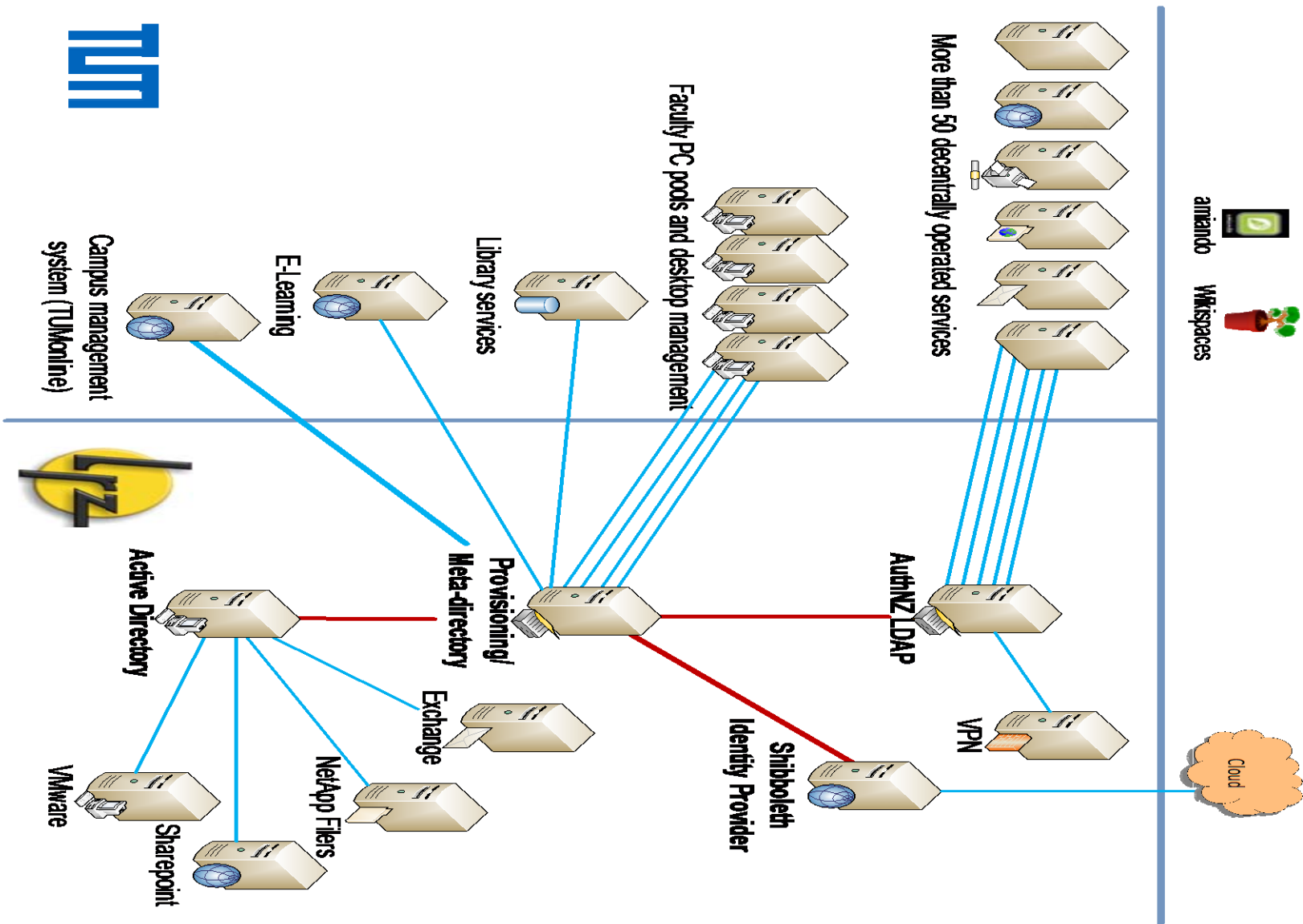
Seeing services through cloud glasses



► Challenge:
TUM's identity management must cover all services



IDM architecture TUM/LRZ



- ▶ LDAP-based AuthNZ and email directory

- ▶ Scope: Many LRZ and TUM-internal services, e.g., VPN, PC pools
- ▶ Advantages:
 - ▶ High performance
 - ▶ Minimalist data schema
 - ▶ Supported out-of-the-box by many applications
- ▶ Implemented using Novell eDirectory and OpenLDAP

Image source: mzacha/sxc.hu



- ▶ Provisioning system / meta-directory

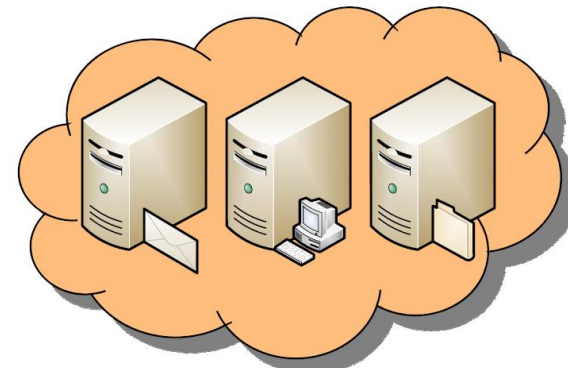
- ▶ Scope: Various TUM-internal services, e.g., library
- ▶ Advantages:
 - ▶ Data format conversion on-the-fly
 - ▶ Integrates legacy systems
 - ▶ Synchronizes locally stored user data
- ▶ Implemented using Novell Identity Manager

Image source: topfer/sxc.hu



▶ Microsoft Active Directory

- ▶ Scope: LRZ “cloud services” (VMware, NetApp, Groupware), TUM Windows PC management
- ▶ Advantages:
 - ▶ Single sign-on for non-web applications
 - ▶ Standard for many 3rd party software products



▶ Shibboleth Identity Provider (DFN-AAI federation)

- ▶ Scope: External services (regular and “cloud” services)
- ▶ Advantages:
 - ▶ Standard data schema across German HEIs
 - ▶ User consent to data sharing enhances privacy
 - ▶ Single sign-on for web applications
 - ▶ Efficient configuration for additional services





Prognosis, or: Would we do this again?



- ▶ Provisioning is complex, error-prone and cost-intensive
 - ▶ Avoid unless you really need to integrate legacy services
- ▶ Active Directory is no substitute for “real” LDAP servers
 - ▶ Its proprietary schema is no match for HEI-specific requirements
 - ▶ OpenLDAP’s performance suits heavy-duty applications much better (e.g., email relays)
 - ▶ But it is a must-have for many commercial services (e.g., VMware)
- ▶ Shibboleth is the de-facto web single sign-on standard
 - ▶ Popular for both campus-internal and federation services
 - ▶ Technological advancements must be kept in mind (e.g., OAuth for access delegation)

- ▶ Combining four different IDM components
 - ▶ causes significant capital and operational expenditure
 - ▶ but provides the flexibility required for both conventional and “cloud” services
- ▶ IDM workflows cover “cloud” requirements quite well
 - ▶ e.g., privileged account management for dynamically instantiated virtual machines
 - ▶ but additional frontends are required (e.g., VM webshop and API)
- ▶ The only constant is change

