Identity management for the TUB Cloud

T. Hildmann, O. Kao, C. Ritter | tubIT, CIT | EUNIS 2013
Agenda

The path of the TU Berlin towards integrated service provisioning:

- Provisioning: Entering the Cloud
- Role-Management: Authorization
- IDM & TUB Cloud: Technology
- Cloud-Storage: ownCloud @ TU Berlin
- Summary: Lessons learned
Entering the Cloud

Provisioning
tubIT-Account setup for external members to use IT services of the TU Berlin

Organisational ID: 16905001564
TU smart card (student’s version)
activating the account

With your tubIT account you can use many tubIT services, such as WLAN access, online disk, PC pool, E-mail and much more. Within the scope of account activation you will be prompted to choose a name and a password for your account.

Please enter your organisational ID into the following form. You find it on the printout you got for your provisioning or on your Campus Card - it starts with "1690".
As a student you can also enter your matriculation number into the input field "Organisational ID"

You find the initial password in the printout you got for your provisioning.

Organisational ID: 
Initial password: 
continue

E-mail contact: tubIT@tu-berlin.de
provisioning for ...

staff members

– covering letter with employment
– campus smartcard = staff member identity card

students

– covering letter with matriculation
– optionally card with or without chip, TAN list, mTAN

external members of TU Berlin

– extra-professional lecturer, graduate student studying for a doctorate without employment, foundationer, ...

– user account without smart card (with exceptions)

guests

– pseudonymous accounts for WiFi-usage only
– no access to personalized TU portal
Authorization

Role-management
Roles, Permissions and Members
three layer rbac-model
Zugewiesene Geschäftsrollen

Sonstige/r Angestellte/r(S)
PERS_Vorgesetzter(S)
KST-Verantwortlicher - 34331500 (für 34331500) - in Vertretung
TUBIS-Master (für 47001100) - in Vertretung
tubIT-Anwendungsverwalter (für 47001100) - in Vertretung
Doktorant/in (für 34331500)
HH-Antrag (für 47)
KST-Verantwortlicher - 47 (für 47)
PERS_Büroleitung - 47001100 (für 47001100) nicht entziehbar
PW-Verwalter (für 47001100)
SuperX - Studierendendaten (für 34331500)
SuperX - Studierendendaten (für 47)
Test-Fak-Statistik (für 34)
Test-Inst-Statistik (für 3433)
TUBIS-Master (für 47001100)
tubBV-Verwalter (für 47001100)
Typo3 Redakteur (für 47001100)
UB-Tester (für 47001100)
Technology

IDM & tub cloud
data-flow: directory services

- Registration Authority
- TUBIS Metadir/RBAC
- vLDAP
- LDAP
- Account Activation
- User Management
- Kerberos
- Active Directory
usage: directory services

- Typo3 Backend
- Typo3 Frontend

vLDAP

- UNIX
- SSH
- Mail
- Moses
- Moodle ...

TUBIS Metadir/RBAC

- Self-Service Apps
- Chev
- CAFM
- Hard-/Software Portal

Account Activation

- Exchange
- Windows Domain
- WiFi
- Monitoring
- vCenter ...

LDAP

User Management

- LDAP-Passwords
- AFS...

Kerberos

Registration Authority

Active Directory

Self-Service Apps

CAFM

Hard-/Software Portal

Chev

Typo3 Backend

Typo3 Frontend
Public & Private Cloud

Private Cloud

- based on VMware ESXi and View
- all central services (including IDM) running on private cloud
  - mail / exchange
  - typo3 cms
  - storage (AFS / ownCloud)
  - campus-management and administration application
  - self-services
- role-based access to services for university members
  - automatically
  - delegated

Public Cloud

- based on Zimory
- user authentication based on LDAP
- prototype for RBAC-integration available
UCS technology ("hardware virtualization")
Hardware - basic

1 UCS Chassis
8 x UCS B200 M1 Blades „half-Size“
   - 2x QC Xeon 5540 2.53 GHz
   - 48 GB RAM
   - No HDD – „boot from SAN“
   - 1 Qlogic DualPort CNA
2 x UCS 6120XP
   - Incl. 8 Port FC-Expansion Card
VMWare VSphere 4.0 license
Hardware-Expansion

2010:
2 chassis

2011:
2 chassis
2 fabric inter connects
backup data-center
vSphere 5

2012:
2 chassis
## resources for private cloud

<table>
<thead>
<tr>
<th>Produktiv-Cluster</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>256 Cores, 602 GHz</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>2,9 TB</td>
<td></td>
</tr>
<tr>
<td>SAN</td>
<td>170 TB</td>
<td></td>
</tr>
<tr>
<td>Hosts</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VMs</td>
<td>255</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test-Cluster</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>40 Cores, 79 GHz</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>384 GB</td>
<td></td>
</tr>
<tr>
<td>SAN</td>
<td>32 TB</td>
<td></td>
</tr>
<tr>
<td>Hosts</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>VMs</td>
<td>103</td>
<td></td>
</tr>
</tbody>
</table>
Public & Private Cloud

Private Cloud

- based on VMware ESXi and View
- all central services (including IDM) running on private cloud
  - mail / exchange
  - typo3 cms
  - storage (AFS / ownCloud)
  - campus-management and administration application
  - self-services
- role-based access to services for university members
  - automatically
  - delegated

Public Cloud

- based on Zimory
- user authentication based on LDAP
- prototype for RBAC-integration available
ownCloud @ TU Berlin

Cloud-Storage
storage and sharing @ TUB

central storage: Andrew File System (AFS)

- Quota
  - personal (1 GB for students, 5 GB for staff)
  - for organizational units (250 GB)
  - extensible in 1 TB steps
- access via
  - AFS-client (Windows, MacOS X, Linux, …)
  - WebAFS
  - SFTP via SSH gateway
  - http://www.user.tu-berlin.de/<nutzername>
  - Subversion (SVN)

Sharing: GigaMove using DFN-AAI (shibboleth)
Server: very good usability via AFS client module

PC/Mac: usability depends on OS system and connectivity

Laptop: some issues with client, alternative: WebAFS

Tablet: WebAFS only. Bad integration!
ownCloud @ TUB

quota

- students 10 GB
- staff members 50 GB
- organizational units will follow

accessibility

- WebDAV for stationary devices
- Sync-Client for Laptops and PCs in remote networks
- iOS / Android-Apps for Smartphones and Tablets
- Web-GUI for independent access from everywhere

share

- sharing of files and folders including corporate work
- simply using e-mail addresses TU Berlin der TU Berlin
Summary

- workflows integrate user provisioning - accounts for all university members
- RBAC based authorization using self-service user interfaces
- IDM pulls data from primary sources and pushes to directory services
- three separated clouds
  - public cloud (user’s virtual machines)
  - private cloud (services provided for users and administration)
  - storage cloud (roll-out in March 2013, not mentioned in paper)
- mobile devices raise the need for cloud services
- increasing integration in external cloud services needed