



Identity Management & Cloud-Dienste bei der GWDG

Konzepte und
Realisierungsmöglichkeiten

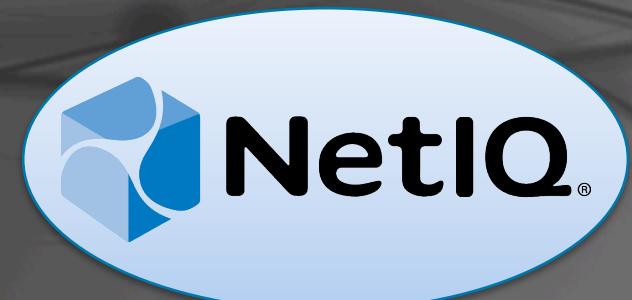
Herbsttreffen ZKI AK Verzeichnisdienste – Christof Pohl

Agenda

- MetaDir IDM
- Cloud-Dienste
- Herausforderungen & Ziele
- IDM.MMXV
- Gesamtarchitektur
- Fazit

MetaDir IDM (1/2)

- Der Dienst
 - IDM für die Universität Göttingen und die Max-Planck Gesellschaft (MPG)
 - Provisionierung aller GWDG-RZ-Dienste
 - IDM Service-Portal: IDM als Dienst
 - Benutzerverwaltung für MPG-IT-Verantwortliche
 - Gruppen- und Rollenmanagement
 - Self-Service-Funktionen für Nutzer
- Das Produkt: NetIQ Identity Manager
 - Produktivbetrieb seit 2005



MetaDir IDM (2/2)

- Der Betrieb
 - Universität Göttingen
 - 34.000 Studierende (HIS)
 - 39.000 Beschäftigte (SAP HR)
 - Max-Planck Gesellschaft
 - 82 Institute (18 angebundene Institute, 10 in Vorbereitung)
 - 12.000 Identitäten
 - Externe Nutzer: GWDG-Account
 - Aus Industrie, Wissenschaft, Forschung und Lehre
 - Kooperationen, Projekt-Konsortien, Auftragsnehmer, ...



Cloud Share (1/2)

- Der Dienst
 - Dateisynchronisierung zwischen verschiedenen Geräten und Betriebssystemen
 - Austausch von Dateien mit Dritten
 - Bekanntes Vorbild: Dropbox
- Das Produkt: Powerfolder
 - Server mit vielen Funktionen (Versionierung, Deduplizierung, Verschlüsselung, ...)
 - Clients für Desktops und Mobilgeräte
 - Client-Usability bietet Raum für Verbesserungen



CloudShare (2/2)

- Der Betrieb
 - Standard: 50 GB Speicherkapazität
 - Datenschutz und Datensicherheit nach deutschen Standards
 - Service Level Agreements
 - Zertifiziert nach DIN EN ISO 9001
 - Status: Produktivbetrieb seit 11/2012



Compute Cloud (1/2)

- Der Dienst
 - Schnelle, bedarfsorientierte Bereitstellung und Konfiguration Virtueller Maschinen (VMs)
 - Konfigurationsanpassungen an VM-Ressourcen (Cores, RAM, Storage, Netzwerk) „on-the-fly“, rund um die Uhr
 - Bekanntes Vorbild: Amazon EC2
- Das Produkt: OpenStack
 - Open Source VM-Management Software
 - Breite Unterstützung (CERN, Canonical, IBM, RedHat, SuSE, HP, Yahoo, Cisco, ...)



Compute Cloud (2/2)

- Der Betrieb
 - Virtualisierung auf Basis von KVM mit libvirt
 - Automatische Installation von physikalischen Knoten und VMs mit Foreman und Puppet
 - Monitoring & Verbrauchsmessung mit OpenTSDB
 - VMs ca. 50 – 80% günstiger als bei Amazon EC2
 - Status: Closed Beta (ca. 100 Tester)



- Der Dienst: bietet skalierbare
 - Applikationen (WordPress, Redmine, Joomla, ...)
 - Programmierumgebungen (PHP, Python, Ruby, Perl, ...)
 - Anwendungsserver (Tomcat, JBoss, Glassfish, ...)
 - Bekanntes Vorbild: Google App Engine
- Das Produkt: OpenShift
 - Status: fortgeschrittene Evaluationsphase
- Der Betrieb
 - Nutzung der Compute Cloud als Basis-Infrastruktur



Dienste für Forschungsdatenmanagement



- Der Dienst
 - REST-API als Single Point Of Access für Datenobjekte, Metadaten und eine Suchmaschine
- Die Produkte
 - Object Storage: iRODS, Hadoop, Ceph
 - Metadaten: CouchDB (NoSQL)
 - Enterprise Search Engine: ElasticSearch
- Der Betrieb
 - Pilotbetrieb in mehreren Forschungsprojekten



Herausforderungen

- MetaDir
 - Gültiger Lizenzvertrag bis Herbst 2015
 - Erwartung: anschließende Lizenzverlängerung nur zu deutlich höheren Preisen möglich
- Cloud-Dienste
 - Steigende Zahl von Kunden außerhalb der UniGÖ und der MPG
 - Unterstützung relevanter Cloud-Charakteristiken (Measured Service)

Ziele

MetaDir

- Schaffung einer zentralen ID-Quelle unabhängig von einem IDM-Produkt
- Aufbau von Know-how für alternative Produkte

Cloud-Dienste

- Zentralisierung des Kunden-Accountings
- Online-Kundenportal als GUI

Realisierung

- Zentrale „GWDG-DB“ für Identitäten und Accounting
- Kundenportal zur Registrierung externer Kunden in der GWDG-DB

Status Quo: IDM im Umbruch

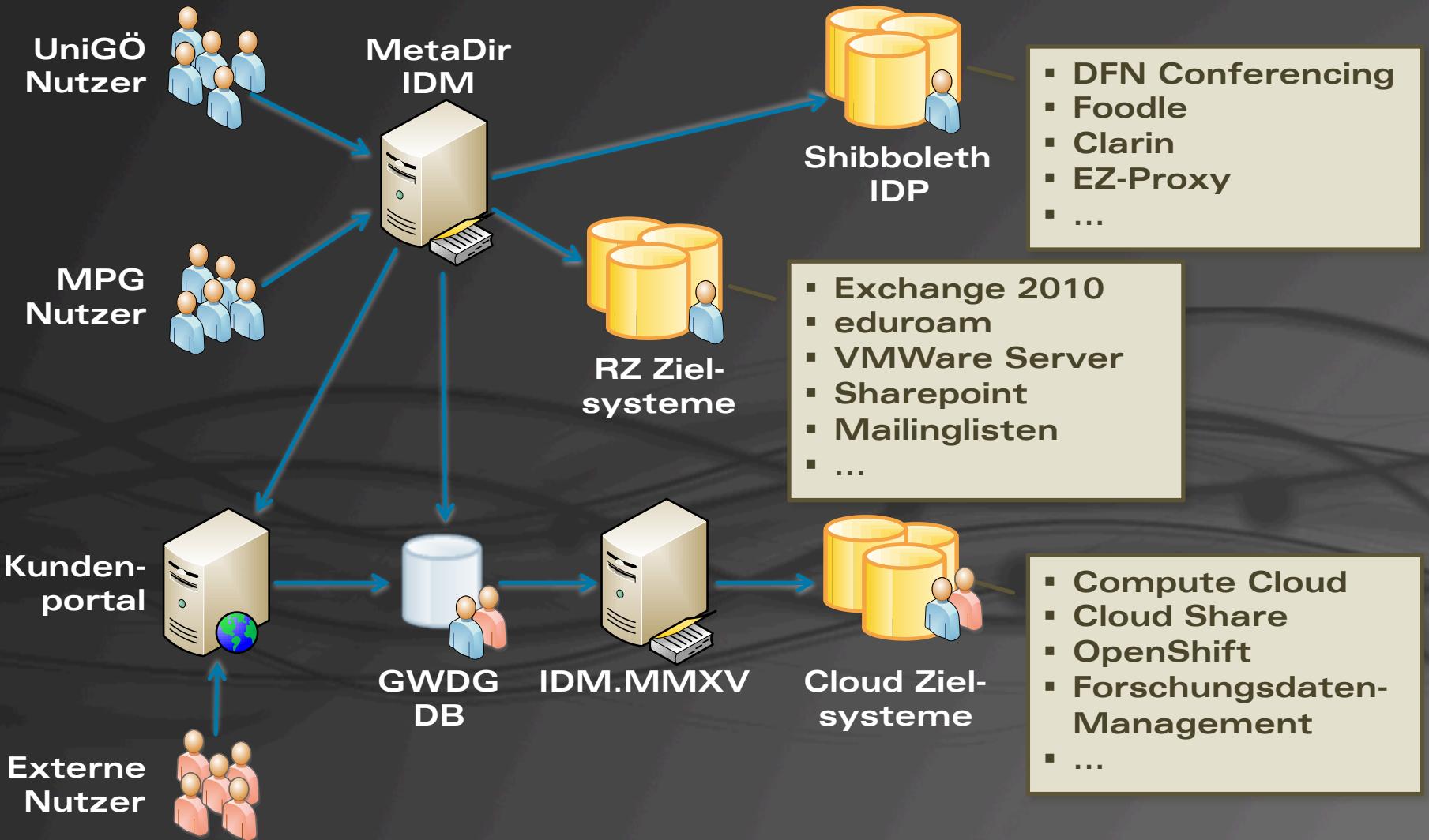


- Cloud Share
 - Metadir-LDAP für Uni GÖ und MPG
 - Externe Nutzer: Radius (eduroam) oder Beantragung GWDG-Account
- Compute Cloud
 - Closed Beta: keine IDM-Anbindung
 - Offene Beta: Nutzung der GWDG-DB als ID-Quelle
- Perspektive: IDM-Lösung mit der GWDG-DB für alle Cloud-Dienste

- Die Produkte
 - Derzeit: LDAP Synchronisation Connector (LSC)
 - Geplant: internes Pilot-Projekt mit OpenIDM
- Provisionierung von Identitäten in die Cloud-Systeme
 - Individuelle Verzeichnisse (LDAP, AD) je Dienst
 - Rollenbasierte Provisionierungsprozesse
 - Datenschutz: minimale Identitätsattribute je Dienst



Gesamtarchitektur



Fazit

Cloud-Dienste der GWDG

Ausgewogener Kompromiss aus Skalierbarkeit und Elastizität, sowie Datenschutz/-sicherheit

Identity Management

Langfristige Strategien, validen Exit-Optionen insbesondere für kommerzielle Produkte

Cloud IT- Infrastruktur

Hohe Komplexität, weiterhin Gegenstand von Forschung und Entwicklung