Karlsruher Institut für Technologie

Zugang zu Föderationen aus Speicher-Clouds mit Hilfe von Shibboleth und WebDAV

Sebastian Rieger <sebastian.rieger@kit.edu>
Yang Xiang (Rechenzentrum Garching)
Harald Richter (Technische Universität Clausthal)

rzg RECHEN-ZENTRUM GARCHING IPP

TU Clausthal

STEINBUCH CENTRE FOR COMPUTING - SCC

Outline

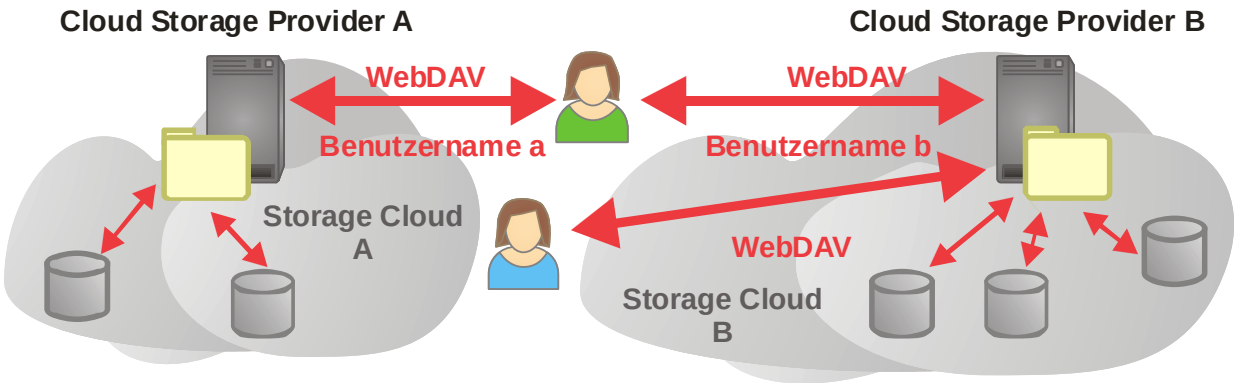
- Speicher-Clouds
- Problemstellung
- Föderatives Identity Management
- Dynamische Föderationen
- Shibboleth WebDAV Client
- Fazit und Ausblick

Speicher-Cloud Lösungen

- Online-Festplatten, Backup, „Data Storage as a Service“
  - Cloud Storage Provider (CSP)
- Isolierte Speicher-Clouds z.B.
  - Amazon S3
  - Google Storage, Windows Azure Storage
- Clients für Endnutzer basierend auf o.g. Lösungen z.B.
  - Mozy, CrashPlan, Carbonite
  - Dropbox, Ubuntu One
- Freie Speicher-Clouds: z.B. Eucalytus Walrus (S3)
  - Verwendung in Ubuntu Enterprise Cloud
- Überwiegend RESTful API
  - sep. Middleware erforderlich, keine native Unterstützung in OS
  - teils jedoch WebDAV (z.B. JungleDisk, S3WebDAV)

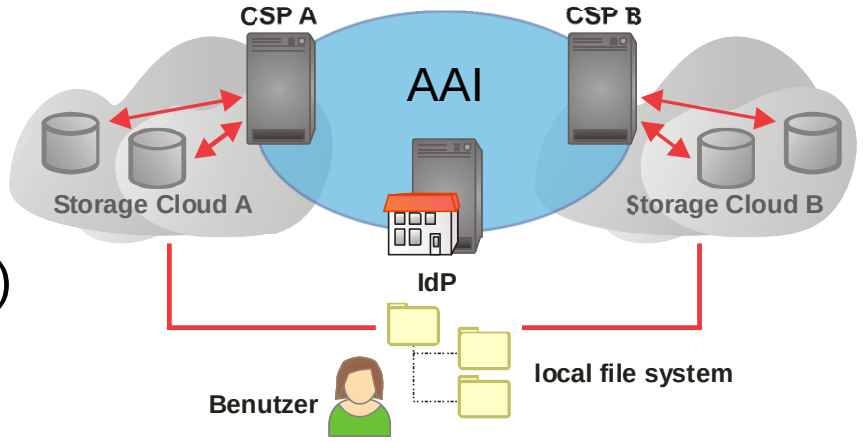
Problemstellung

- Heterogene Landschaft für Benutzer
  - separate Accounts, Logins
- Verbünde aus Speicher-Clouds
  - verteilte IT-Infrastrukturen, Private Clouds, Hybrid Clouds
- Standard von Storage Networking Industry Assoc. in Arbeit
  - Cloud Data Management Interface (CDMI), 1.0, April 2010
  - Block (iSCSI) / File Access (CIFS, NFS, WebDAV)
  - In aktuellen Storage-Lösungen noch nicht verfügbar



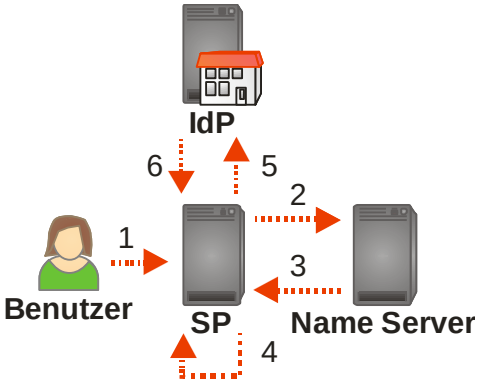
Föderatives Identity Management (AAI)

- Single Sign-On über mehrere Cloud Storage Anbieter
  - z.B. für Aggregation von Verzeichnissen
- SAML: Service / Identity Provider, Shibboleth z.B. DFN-AAI
  - Zugriff auf (C)SP Umleitung an IdP, SSO
  - Einbindung eines IdP in unterschiedliche Storage Clouds möglich
  - Problem: Lokalisierung ist Web-Browser basiert!
- Motivation: Lösung für RESTful Zugriff realisiert
  - aber kein direkter Zugriff aus OS
  - Andere Arbeiten zu Shibboleth für iRODS (Grid), work in progress Subversion (auch WebDAV, aber nur Server)



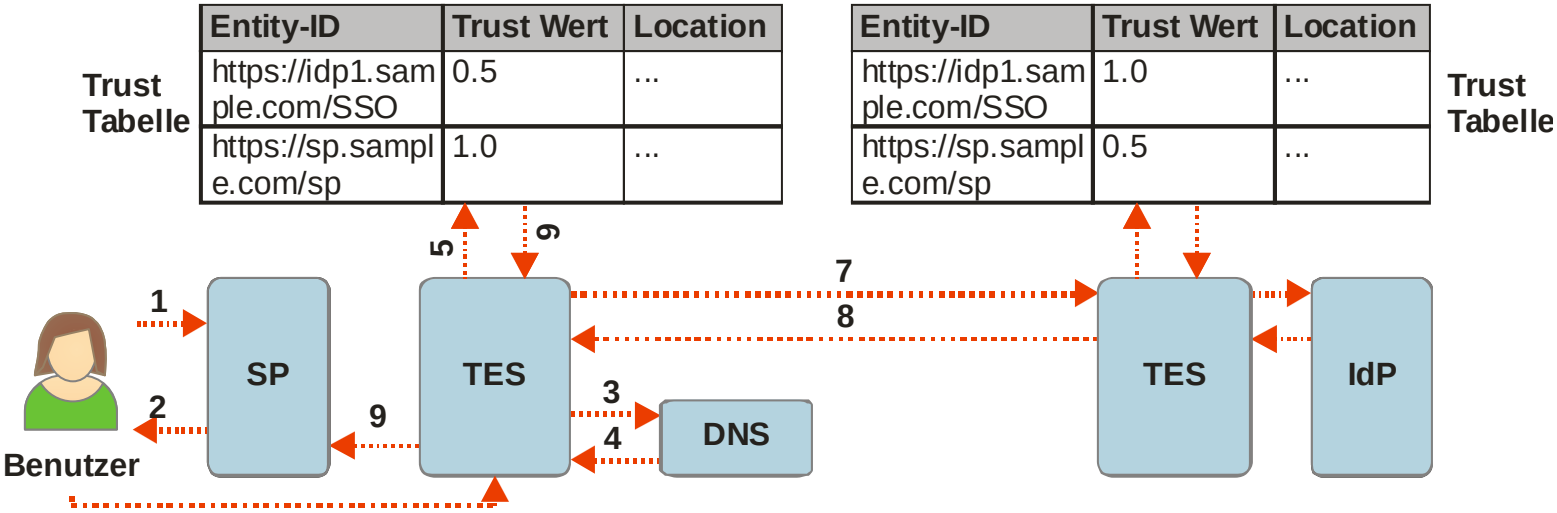
Dynamische Föderationen

- Lokalisierung des Benutzers
  - Shibboleth verwendet DS, SP leitet an DS um, Benutzer wählt IdP
  - Föderationsverbund (Konföderation) möglich z.B. eduGAIN
- Auswahl des IdP an Web-Browser gebunden
  - Verwendung in Datei Explorer / Netzlaufwerk usw. nicht möglich
  - Fluktuation von IdPs, SPs problematisch
- Dynamische Föderation
  - SP ermittelt IdP anhand der E-Mail Adresse (Benutzername) aus Domain über NAPTR Anfrage bei DNS (liefert Service URL)



  - Benutzer benötigt nur E-Mail Adresse, keine zusätzliche Auswahl im DS, ohne Web-Browser nutzbar, mehrere Identitäten möglich
  - durch Lokalisierung im DNS auch Zugriffe über Föderationsgrenzen

Dynamische Föderationen - TES



- Zusätzliches Trust Estimation System (TES) im CSP
  - Ermöglicht dynamische Föderation
  - Föderationsübergreifender Trust in IdP basierend auf Trust Wert
  - TES verwendet NAPTR DNS Requests für IdP Ermittlung
  - TES übernimmt somit die Funktion eines Discovery Service
- Standalone Tomcat Anwendung, Anbindung an Shibboleth als Plugin

Implementierung Shibboleth WebDAV Server

- WebDAV Server-Setup verwendet Standardkomponenten:
  - Apache Server
  - Standard Apache WebDAV Modul: mod_dav, bzw. mod_davfs
  - Verwendet Apache mod_auth für Authentifizierung und Autorisierung
  - hierfür Standard Shibboleth Variante: mod_shib (SP)

```
<Location /shib>
        AuthType Shibboleth
        ShibRequireSession On
        Dav On
        <LimitExcept GET OPTIONS>
                require valid-user
        </LimitExcept>
</Location>
```

Shibboleth WebDAV Server

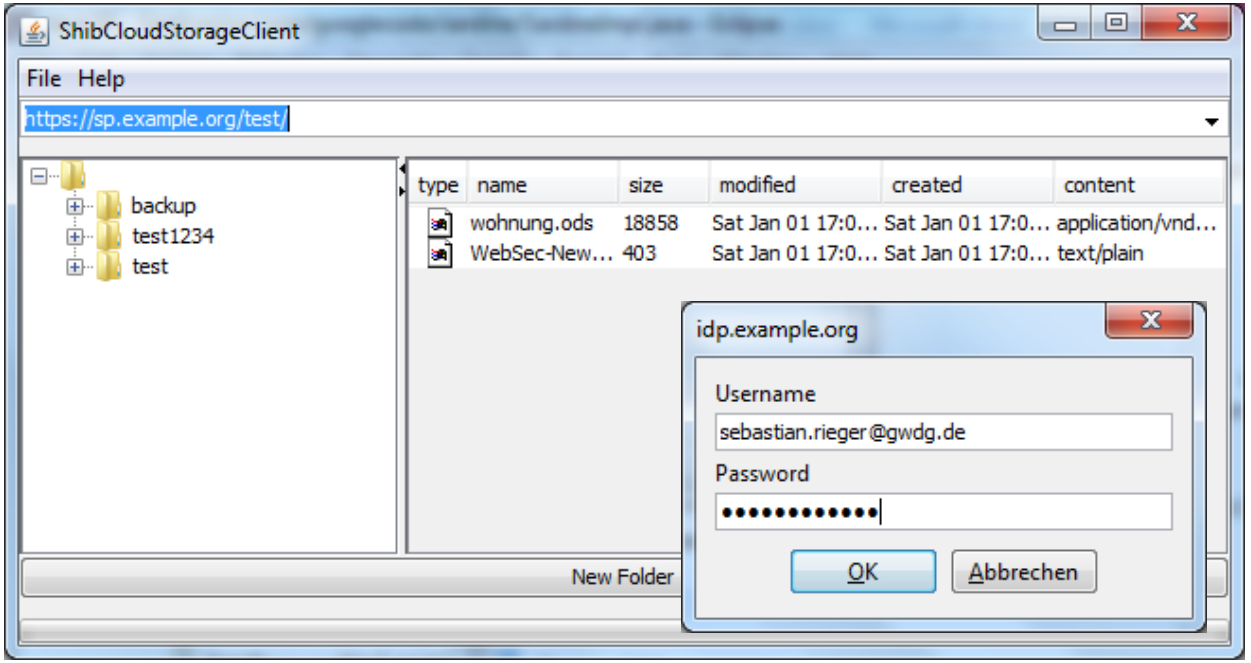
- Analog für MS IIS mit Shib SP möglich
- Test mit bestehenden WebDAV-Clients
  - Getestet: MS Windows und Ubuntu (Gnome), WebDrive, iWorks
- SAML bzw. Shibboleth wird nicht unterstützt
  - SAML redirect profile – Redirects werden nicht ausgeführt
  - SAML POST profile wird nicht unterstützt
    - Erfordert Auswertung von HTML Formularen
    - Wird z.B. bei Shibboleth per JavaScript im Web-Browser gelöst
  - Kein HTTP Session Handling
- Eigene WebDAV Client Implementierung erforderlich
  - Unterstützung von Shibboleth typischen redirects, SAML POST profile und Sessions für SSO

Shibboleth WebDAV Client

- Implementierung basierend auf Sardine
  - Open Source Java WebDAV Client
  - Sardine basiert wiederum auf Apache HTTP Client
- Erweiterung von Sardine
  - Unterstützung von HTTP redirects, in Apache HC verfügbar
  - SAML POST profile: Extraktion der Assertion und Relay State → Übermittlung an den CSP
  - Zusätzlich Session Verwaltung (Cookie) in Sardine, basierend auf Apache HC für SSO
  - SSO Handling
- SSO wird so über CSPs (unterschiedlicher Cloud Anbieter) hinweg ermöglicht

Shibboleth WebDAV Client

- Realisierung als Java Swing GUI
  - Discovery anhand E-Mail Adresse (und NAPTR)
  - Ermöglicht Zugriff auf Verzeichnisse, und Files per Drag & Drop
  - Login am ersten CSP, Redirect Handling, Asserion Extraktion
  - Session an IdP wird gespeichert → Zugriff auf nächsten CSP in Föderation
    → SSO



Shibboleth WebDAV Client

- Problem: einheitliche Autorisierung
  - Autorisierung basiert auf Web-Server und darunter liegendem FS
  - Für FS sind bei Cloud-übergreifenden Zugriffen einheitliche Identifier erforderlich
  - Windows SID (global eindeutig), Unix UID (number) (lokal eindeutig)
- Mögliche Lösungen
  - ACLs direkt im Web(DAV)-Server → erhöht Komplexität des Managements
  - Autorisierung durch Shibboleth SP
  - UID Mapping in Shibboleth SP → bei erstem Zugriff eines (externen) Benutzers, Zuordnung einer UID aus Pool des CSP → Lösungen für Deprovisioning erforderlich!

Fazit und Ausblick

- Einheitliche Autorisierung, Lösung für global eindeutige Security Identifier
- Performance-Evaluierung in standortübergreifenden Speicher-Clouds für Föderationen wie z.B. MPG-AAI oder NDS-AAI
- Evaluierung der Eignung für NoSQL-basierte Objekt-Speicher und Filesysteme (z.B. GridFS für mongodb)

Vielen Dank für die Aufmerksamkeit! Gibt es Fragen?