URZ-Nutzerforum

AFS-Berechtigungen & Dateiaustauschdienste

Holger Trapp, Daniel Klaffenbach

Universitätsrechenzentrum

10. Dezember 2014

Gliederung

1. AFS - Grundlagen und Konzepte

2. AFS-Sicherheit

3. Dateiaustausch mit externen Partnern
   - WebDAV
   - GigaMove
   - Vergleich

Charakteristika von AFS

- verteiltes Netzwerkdateisystem
- TUC: AFS-Zelle `tu-chemnitz.de`, OpenAFS
- Zellen enthalten Datei- und Datenbank-Server
- Datei-Server einer Zelle verwalten deren Dateien in speziellen Strukturen
- Lokationstransparenz
- einheitlicher AFS-Namensraum auf den Klienten
- hohe Skalierbarkeit
- Sicherheit durch Kerberos 5 (TUC: Heimdal als K5-Server)

Grundlage vieler Speicherdienste

- Homeverzeichnisse
- Projektverzeichnisse: `/afs/tu-chemnitz.de/project/...`
  - für große Datenmengen und Zusammenarbeit im Team geeignet
- WWW-Verzeichnisse für www.tu-chemnitz.de: `/afs/tu-chemnitz.de/www/root/...`
- zentrale Software-Installationen: z.B. `/afs/tu-chemnitz.de/global`

Homeverzeichnisse

- z.B. `/afs/tu-chemnitz.de/home/urz/o/otto`
- bei Linux automatisch genutzt, bei Windows Laufwerk H:
- alternative Zugänge: Web-Dateimanager WFM, Secure Copy/FTP
- `~/public_html` als persönlicher Web-Bereich
  - dessen AFS-Pfad für externe Nutzung meist nutzlos
  - Zugriff per Web: `https://www.tu-chemnitz.de/~otto/...`
  - Standard: weltweit sichtbar!!
  - ggf. einschränken: `.htaccess`, mit Punkt beginnende Verzeichniseinträge
- Ordner PRIVAT für private Dateien, BACKUP für 2 Backup-Stände

Volumes, Quota

- AFS verwaltet Dateien/Verzeichnisse in Volumes
- RW-, RO-, Backup-Volumes bzw. Volume-Instanzen
- z.B. `user.otto`, `user.otto.readonly`, `user.otto.backup`
- `/afs/.tu-chemnitz.de/...` erzwingt Nutzung der RW-Volumes
- Quota pro Volume (über IdM einstellbar)
- Kommando zur Quota-Abfrage: `fs lq`
- Volumes lassen sich an verschiedenen Stellen im AFS-Baum montieren/demontieren (`fs mkm`, `fs rmm`, AFS-Kontextmenü des Windows Explorers)

AFS-Token, PAG

- AFS-Identitätsnachweis durch zeitlich befristetes AFS-Token
- Basis: K5-TGT (Ticket Granting Ticket) und AFS-Ticket
- Standard-Gültigkeitsdauer: 25 Stunden
- Ticket-/Token-Verwaltung bei Windows: Network Identity Manager
- Kommandos: `tokens`, `klist`, `kinit`, `klog` (veraltet), ggf. `aklog`, `afslog`, `afs5log`
- Standard bei Linux: AFS-Token-Zuordnung via PAG (Process Authentication Group)
- Kommando `pagsh` startet Shell in neuer PAG (ohne Token)

ACLs, Gruppen

- Zugriffssteuerung über ACLs (Access Control Lists)
- existieren nur für Verzeichnisse, nicht für Dateien
- über Symlinks abweichender Schutz einzelner Dateien realisierbar
- `lrwxr-xr-x 1 otto user 14 11. Nov 2011 id_rsa -> ../priv/id_rsa`
- Standard-ACL für Nutzer otto: `urz:www-user l`, `otto rlidwka`
- vom IdM nächtlich gesetzt, sofern Nutzer dies nicht deaktiviert
- pro ACL max. 20 Einträge: AFS-Nutzer oder -Gruppen
- Gruppen sind flexibel und sollten stets bevorzugt werden
- Gruppen können Gruppen sowie IP-Adressen als spezielle Nutzer enthalten

Gruppen- und ACL-Management

- Gruppen-Verwaltung: https://www.tu-chemnitz.de/urz/storage/afs/manage.html
- Kommandos: `pts creategroup`, `pts adduser`, `pts removeuser`, `pts delete`, `pts mem`, `pts exa`
- grafisches ACL-Management: WFM, Windows Explorer (AFS-Kontextmenü)
- ACL-Kommandos: `fs la`, `fs sa`, `chacl`, `fsr`
- 7 ACL-Rechte:

l	lookup	- Verzeichnis betreten, Anzeige ACLs/Verzeichniseinträge
r	read	- Dateien lesen
i	insert	- Dateien/Verzeichnisse anlegen
w	write	- Dateien modifizieren
d	delete	- Dateien/Verzeichnisse löschen
k	lock	- flock erlauben
a	administer	- ACL administrieren

- Kürzel: `read`, `write`, `all`, `none`

Unix-Rechte und Standard-Gruppen

- Unix-Rechte im AFS weitgehend irrelevant, `u+rw` aber ggf. wichtig
- r- bzw. w-Recht der ACL wirkt nur, wenn `u+r` bzw. `u+w` gesetzt ist
- Zugriff für Datei-Eigentümer und Mitglieder von `system:administrators` ggf. von Unix-Rechten unabhängig
- Unix: `+x` für ausführbare Dateien erforderlich
- Standard-Gruppen:
  - `system:anyuser` (weltweit, aber an TUC Zelle/K5-Server nur intern verfügbar)
  - `system:authuser`
  - `system:administrators` (darf anders als Unix-root `chown` im AFS ausführen)
  - `system:ptsviewers`
  - `chemnitz`
  - `urz:www-user`

ACLs für neue Verzeichnisse

- neu angelegte Verzeichnisse erben die ACL des Elternverzeichnisses
- beim Verschieben eines Verzeichnises **innerhalb** eines Volumes bleibt dessen ACL erhalten
- bei Verschiebung über Volumegrenzen erfolgt de facto ein Kopieren und Löschen
- daher wird dort die ACL des Elternverzeichnisses im Ziel-Volume vererbt

Backup

- automatisch nächtlich (via CABS - Chemnitzer AFS Backup Suite)
- Symlinks `~/BACKUP/YESTERDAY`, `~/BACKUP/LAST_WEEK` auf RO- und Backup-Volume: `user.otto.readonly`, `user.otto.backup`
- WFM bietet Zugriff auch auf ältere Stände

Ausgangssituation

- Viele individuell gesetzte Rechte in `HOME`-Verzeichnissen
  $\rightarrow$ Rechte oft viel zu freizügig vergeben
- Zusätzlich: Lookup-Rechte für `system:anyuser` (außer `PRIVAT`-Verzeichnis)
  - Sensitive Daten wurden durch Nutzer auch außerhalb von `PRIVAT`-Verzeichnissen abgelegt
  - Dateinamen waren **weltweit** ersichtlich
  - Konsequenzen vielen Nutzern nicht bewusst

Maßnahmen

- Seit August 2014 Zugriff auf `HOME`-Verzeichnisse nur noch für den Benutzer selbst und den Webserver
  $\rightarrow$ Kein Zugriff mehr für `system:anyuser`
- Zugriff auf AFS-Speicherressourcen nur noch aus dem Uni-Netz

Ausgangssituation

- Viele individuell gesetzte Rechte in `HOME`-Verzeichnissen
  $\rightarrow$ Rechte oft viel zu freizügig vergeben
- Zusätzlich: Lookup-Rechte für `system:anyuser` (außer `PRIVAT`-Verzeichnis)
  - Sensitive Daten wurden durch Nutzer auch außerhalb von `PRIVAT`-Verzeichnissen abgelegt
  - Dateinamen waren **weltweit** ersichtlich
  - Konsequenzen vielen Nutzern nicht bewusst

Maßnahmen

- Seit August 2014 Zugriff auf `HOME`-Verzeichnisse nur noch für den Benutzer selbst und den Webserver
  $\rightarrow$ Kein Zugriff mehr für `system:anyuser`
- Zugriff auf AFS-Speicherressourcen nur noch aus dem Uni-Netz

Auswirkungen

- Zugriff außerhalb der Universität nur noch über VPN
- Kein Zugriff auf `HOME`-Verzeichnisse mehr für fremde Nutzer
  - `PUBLIC`-Verzeichnis nicht mehr zur Freigabe von Daten nutzbar
- Manuell gesetzte Rechte in HOME-Verzeichnissen werden regelmäßig auf sichere Standardwerte zurückgesetzt
  - URZ-Empfehlung: Freigabe von Daten nicht mehr über `HOME`-Verzeichnis
  - Wenn tatsächlich Notwendigkeit besteht, Rechte dauerhaft anzupassen
    $\rightarrow$ Deaktivierung dieser Sicherheitsfunktion über IdM-Portal:
    `https://idm.hrz.tu-chemnitz.de/user/service/storage/afs/home/`

Verbreitete Möglichkeiten

- E-Mail
  - Pro: schnell und einfach
  - Contra: Anhanggröße bei Empfängern oft stark beschränkt
- AFS
  - Pro: schnell und komfortabel, in der Uni problemlos nutzbar
  - Contra: VPN von außen notwendig, URZ-Account notwendig, Einrichtung schwierig
- Externe Cloud-Dienste
  - Pro: einfach zu benutzen
  - Contra: Abgabe der Kontrolle über die Daten, von Partnern in der Wirtschaft oft verboten

$\Rightarrow$ hier vorgestellte Alternativen: WebDAV und GigaMove

Dateiaustausch mit WebDAV

- URZ betreibt eigenen WebDAV-Dienst:
  `https://subversor.hrz.tu-chemnitz.de/fs/`
- Daten sind im URZ gespeichert
- Dateiaustausch über „Projekte“ realisiert, die einzeln angelegt werden
  - Ein Verantwortlicher pro Projekt
  - Setzen der Zugriffsrechte pro Projekt über Weboberfläche
  - Maximale Laufzeit: 12 Monate (verlängerbar)
  - Speicherplatz: 1 GB
- Zugriff unter allen gängigen Desktop-Betriebssystemen ohne Zusatz-Software
- Registrierung für externe Partner notwendig

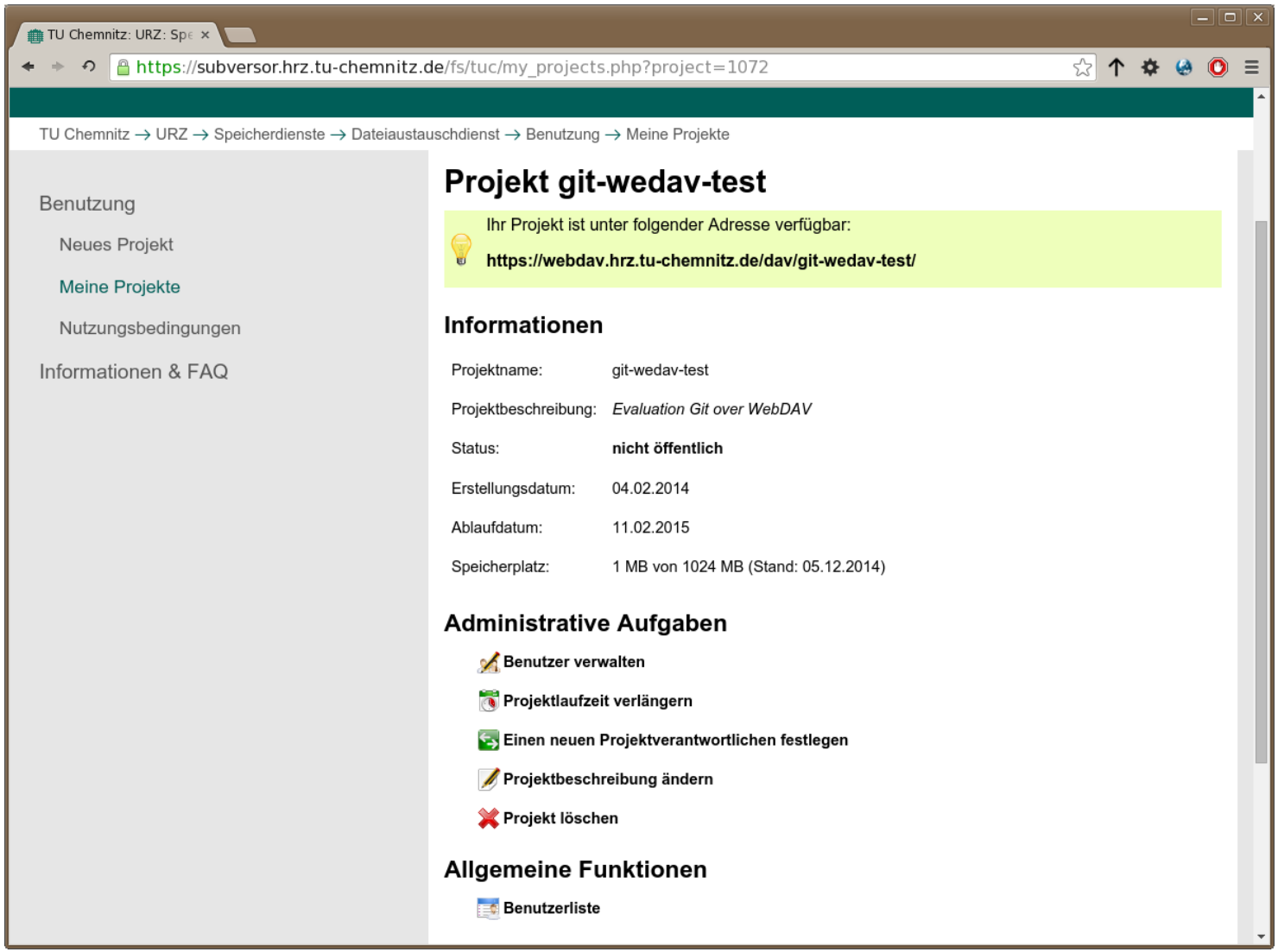

Abbildung: Ein Projekt beim Dateiaustauschdienst

Zugriff

- WebDAV-Klienten in Desktop-Betriebssysteme integriert:
  - Linux: Zugriff über GNOME- oder KDE-Dateimanager
  - OSX: Zugriff über den Finder („*Verbinden mit Server*“)
  - Windows: Zugriff über den Windows-Explorer als Netzlaufwerk

  → Zugriff i.d. Regel auch hinter restriktiven Unternehmensfirewalls möglich
- Lesender Zugriff über jeden Webbrowser
- Mobilgeräte:
  - Android: ES Datei Explorer
  - iOS: WebdavNav

GigaMove – Einfach und schnell große Dateien austauschen

- Dienst der RWTH Aachen zur Bereitstellung oder Anforderung **einzelner** Dateien
  $\rightarrow$ Dateien werden auf den Servern der RWTH Aachen gespeichert!
- Nutzbar von allen Mitgliedern der DFN AAI Föderation
  - Authentifizierung über Shibboleth (Web-Trust-Center)
  - Zustimmung der Weitergabe bestimmter Identitätsattribute erforderlich: Name, Mailadresse, Nutzerkennzeichen, Personentyp (Mitarbeiter, Student, …)
- Benutzung über Web-Browser (keine spezielle Software nötig)
- Verwendung unter:
  `https://gigamove.rz.rwth-aachen.de/`

Abbildung: GigaMove-Benutzerschnittstelle

Bereitstellung einer Datei

- Bereitstellung durch Uni-Angehörigen
- Uploads einer Datei von bis zu 2 GB Größe
- Verschlüsselte Übertragung
- Optionales Passwort und Kommentar
- Maximale Bereitstellungsdauer: 14 Tage
- Insgesamt max. 10 GB pro Nutzer

Abbildung: Dialog zum Hochladen einer Datei

$\Rightarrow$ Link zum Verschicken

Anfordern einer Datei

- Uni-Angehörige können externe Partner auffordern, eine Datei hochzuladen
- Link kann entweder direkt über GigaMove-Frontend oder manuell versendet werden
- Hochladen der Datei dann wie bereits gezeigt
- Speicherverbrauch wird der anfordernden Person angerechnet

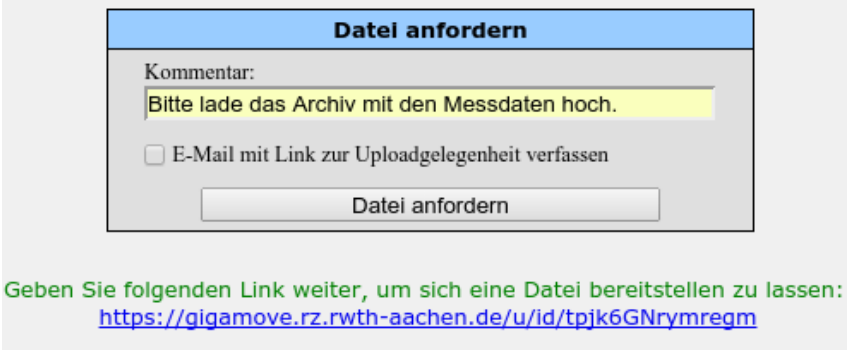

Abbildung: Dialog zur Anfordern einer Datei

Verwalten von Dateien

- Gigamove bietet Übersicht über alle bereitgestellten und angeforderten Dateien
- Links können verschickt werden
- Dateien können vorzeitig gelöscht werden

Bereitgestellt | **Angefordert**

Sie haben eine Datei angefordert, die Ihnen bisher noch nicht bereitgestellt wurde.

Kommentar	Link	Erstellt am			
Bitte lade das Archiv mit den Messdaten hoch.	https://gigamove.rz.rwth-aachen.de/u/id/tpjk6GNrymregm	05.12.2014 - 13:18			

Abbildung: Verwaltung von GigaMove-Dateien

Vergleich

	WebDAV	**GigaMove**
Anwendungsszenario	Ersatz für herumgereichte USB-Sticks (viele Dateien pro Projekt, Ordnerstruktur möglich)	Alternative für große E-Mail-Anhänge (separater Link pro Datei)
Speicherort	URZ	RWTH Aachen
Max. Größe	1 GB	2 GB
Max. Gültigkeit	12 Monate (verlängerbar)	14 Tage