Einführung eines Identity Management beim Bundesamt für den Zivildienst

Who? Jörg Steffens

From? http://www.dass-it.de/

When? 4. März 2010

Rev : 9635

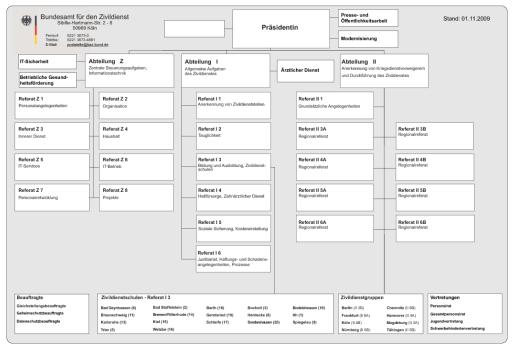
dass IT

Bundesamt für den Zivildienst

Eckdaten

- Zuständig u.a. für Verwaltung von Zivildienststellen und Bearbeitung von Kriegsdienstverweigerungsanträge
- ca. 1500 Mitarbeiter
- Sitz in Köln
- bundesweit vertreten über Zivildienstgruppen und -schulen

Bundesamt
für den Zivildienst



dass IT

dass IT GmbH

Eckdaten

- Geschäftsfelder rund um Open Source:
  - Consulting
  - Support
  - Maßgeschneiderte Anpassungen und Entwicklung
- Gegründet: 2004
- Mitarbeiter: 8

Rollenbasiertes Berechtigungskonzept

Anforderungen

- Berechtigungen nicht direkt an Personen binden, sondern
- Personen werden Stellen zugeordnet
- Stellen werden Rollen zugeordnet
- Berechtigungen werden für Rollen vergeben

Vorteile

- bildet die Organisationsstruktur des BAZ besser ab
- bei Aufgabenwechsel muss nur die Stellenzuordnung geändert werden

dass IT

Wo sollen Stellen und Rollen hinzugefügt werden?

Ausgangssituation

- Gewachsene IT
- mehrere, nicht verknüpfte Verzeichnisdienste
- Benutzerverwaltung benötigt vielen manuelle Arbeitsschritte

Ausgangsdaten

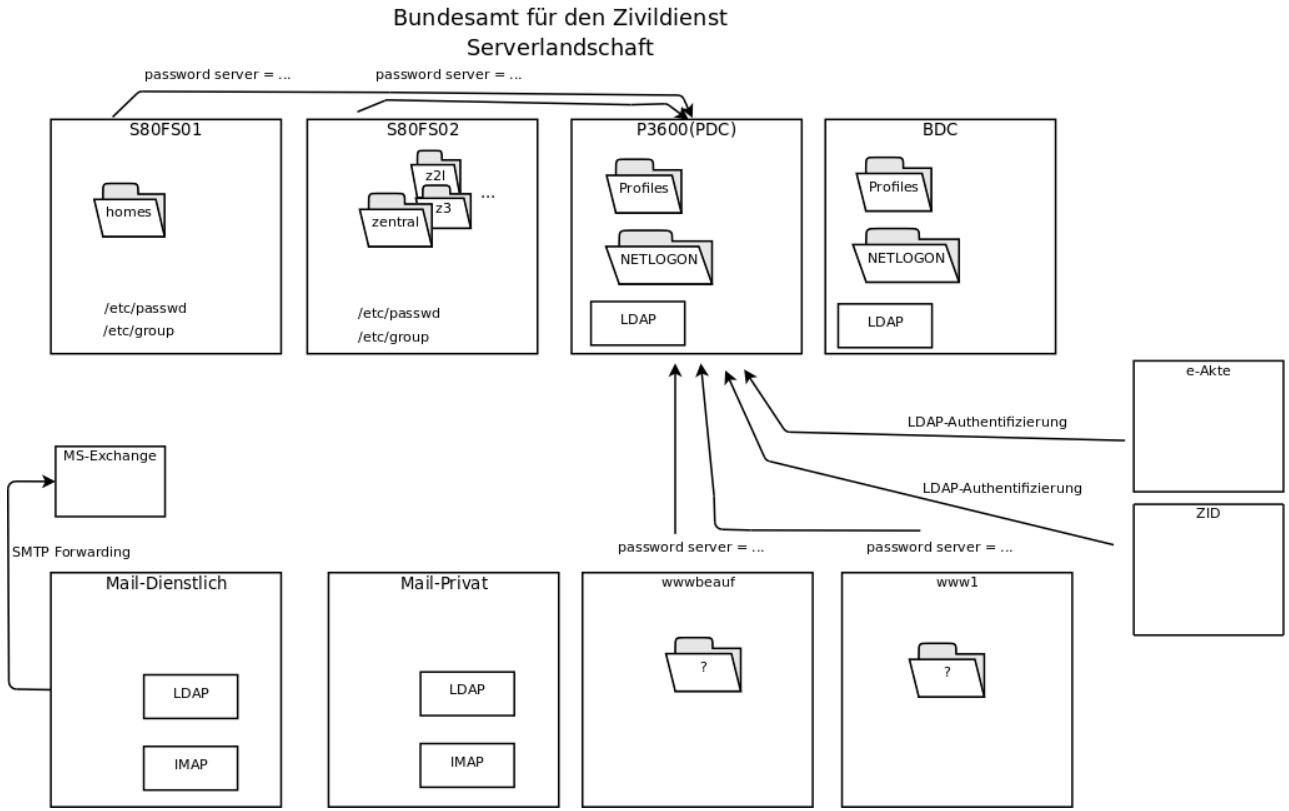
Benutzer und Gruppendaten existieren im ...

- Email-System (SLOX)
- Samba-Dateiservern (OpenLDAP)
- Active Directory (MS Exchange)
- anderen Systemen

dass IT

Ausgangssituation

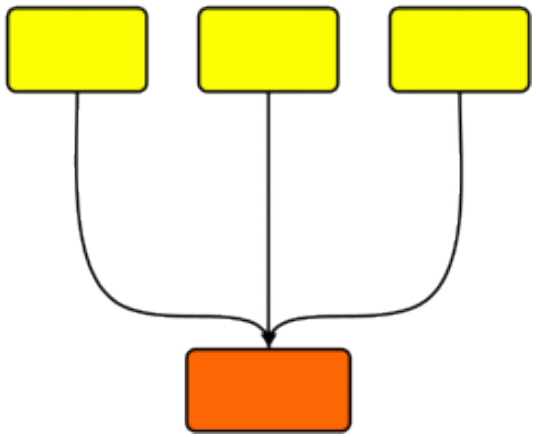
Isolierte Systeme



dass IT

Vorgehensweise

- Vereinheitlichen der Datenbasis
- Systeme verknüpfen
- Abbildung von Stellen und Rollen als spezielle Gruppen
- angepasstes Administionsfrontend erstellen



dass IT

Warum Univention Corporate Server?

- Zentrales System für Windows und Unix
- OpenLDAP als zentrale Datenquelle
- OpenLDAP Replikation, inkl. Schema (Listener/Notifier-Mechanismus)
- Kerberos (Integration in OpenLDAP)
- Samba (Konfiguration aus OpenLDAP)
- AD-Connector
- (OX-Integration)
- Administrations Web-Interface
- Anpassbarkeit der UCS Administration-Schnittstelle

dass IT

Eingesetzte Komponenten

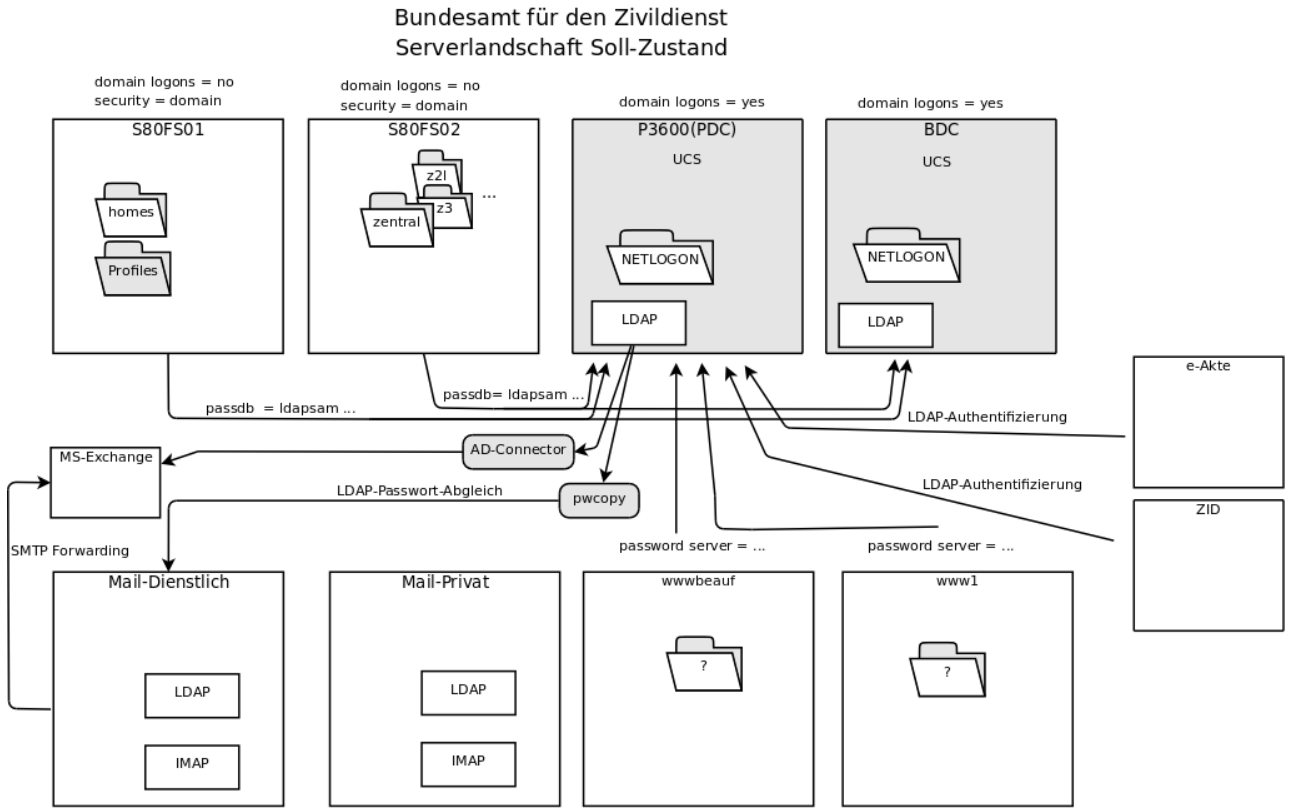
UCS

- Samba
- AD/MS-Exchange
  - AD-Connector
- Mailserver (SLOX)
  - pwcopy
- Entwicklung von kundenspezifischen Anpassungen der Benutzerverwaltung

dass IT

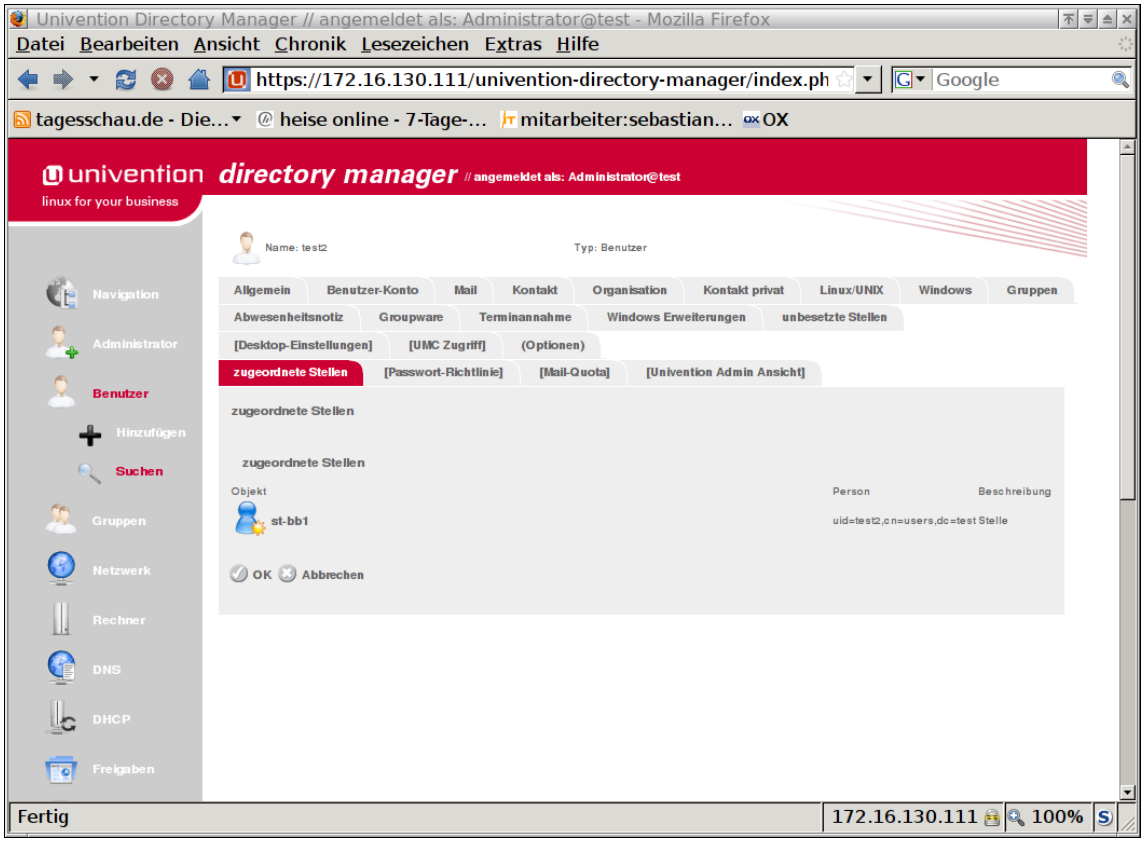
Zielsituation

Verknüpfung der Systeme



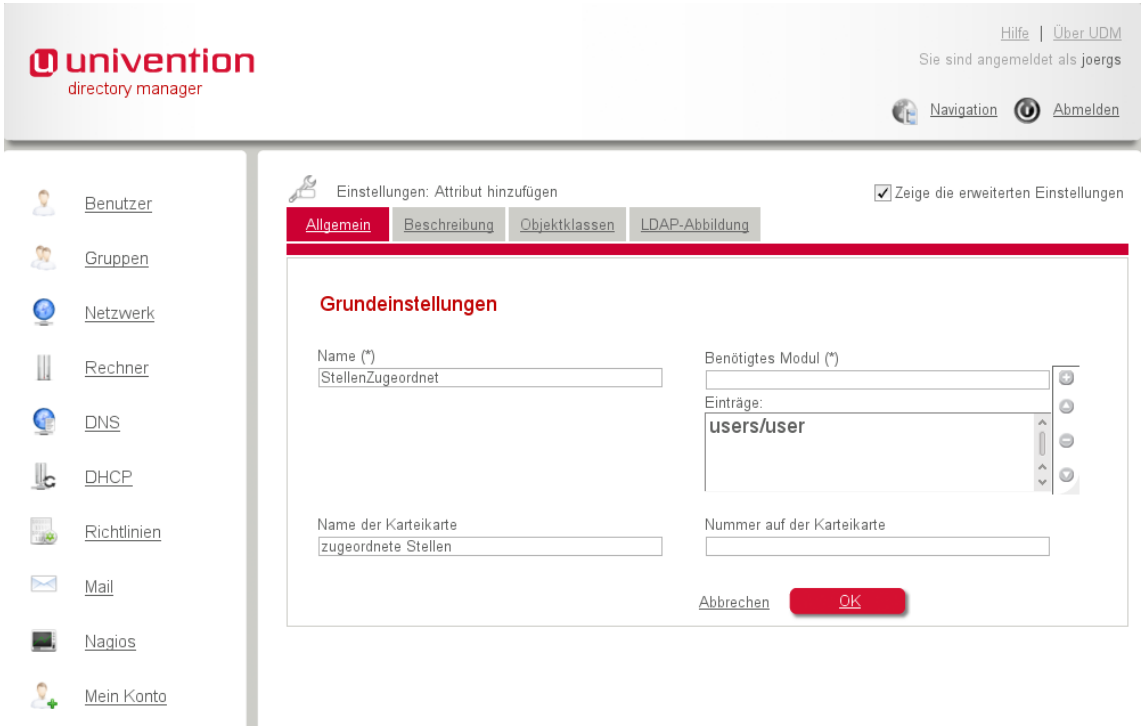
UCS Benutzer-Ansicht: Stellen

Benutzer-Ansicht: zugeordnete Stellen



Erweitern des Administrationsfrontends

Definition Ansicht: zugeordnete Stellen



UCS Erweitern: Listener-API

Passwort-Synchronisation

```
#!/usr/bin/python

name='pwcopy'
description='sync userPassword to external system'
filter='(&(objectClass=posixAccount)(mail=*)(uid=*))'
attributes=[ 'userPassword' ]

def handler(dn, new, old):
    ...
```

wird auf jedem UCS System ausgeführt, wenn der LDAP-Filter zutrifft

dass IT

Fazit

Positiv

- Übernahme der bestehenden Accounts von Samba (SLES) nach UCS
- Anpassungsmöglichkeiten im UCS
- Python Interface bei LDAP-Modifikation
- Support

Weniger Positiv

- an einigen UCS Komponenten musste nachgebessert werden

dass IT

Fragen?