

# Einführung eines Identity Management beim Bundesamt für den Zivildienst

Who? Jörg Steffens

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

When? 4. März 2010

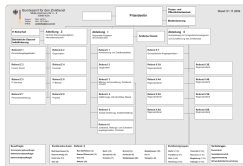
Rev : 9635

## 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



## Eckdaten

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



dass IT



dass IT

## 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

# Wo sollen Stellen und Rollen hinzugefügt werden?

## Ausgangssituation

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

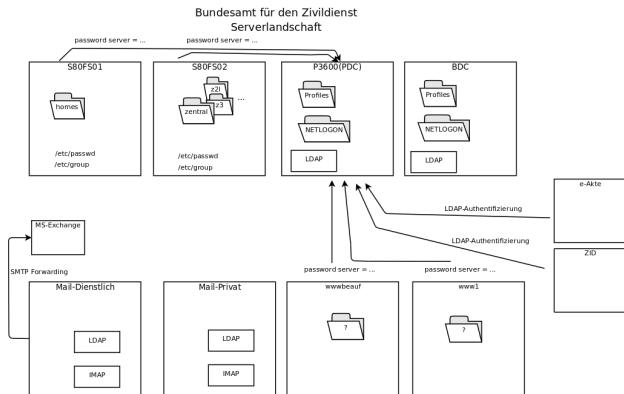
## Ausgangsdaten

Benutzer und Gruppendaten existieren im ...

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

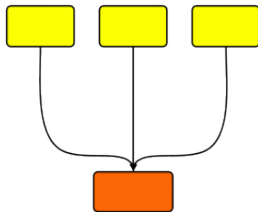
# Ausgangssituation

## Isolierte Systeme



# Vorgehensweise

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



# 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

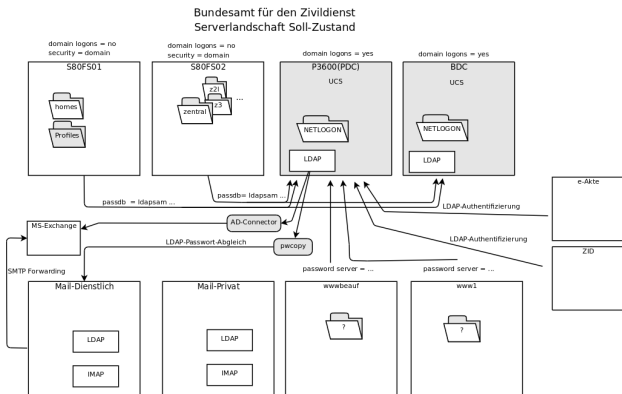


## UCS

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

# Zielsituation

## Verknüpfung der Systeme



# UCS Benutzer-Ansicht: Stellen

Benutzer-  
Ansicht:  
zugeordnete  
Stellen

The screenshot shows the UCS Directory Manager web interface. The browser address bar indicates the URL is <https://172.16.130.111/univention-directory-manager/index.php>. The page title is "univention directory manager" and the user is logged in as "angewendet.de: Administrator@test". The left sidebar contains navigation options: Navigation, Administratoren, Benutzer (selected), Hierarchien, Suchen, Gruppen, Netzwerk, Fileshare, DNS, DHCP, and Freigegeben. The main content area shows the "Benutzer" view for "Name: test2". The "zugeordnete Stellen" tab is selected, showing a table of assigned positions. The table has columns for "Objekt", "Person", and "Beschreibung". One entry is visible: "st-bb1" assigned to "stb@st2.campus.de:st2:Stelle". Below the table are "OK" and "Abbrechen" buttons. The bottom status bar shows "Fertig" and the IP address "172.16.130.111".

dass IT

## Definition Ansicht: zugeordnete Stellen

The screenshot shows the univention directory manager web interface. The top navigation bar includes the logo, user information (joeerg), and navigation links. The main content area is titled 'Einstellungen: Attribut hinzufügen' (Settings: Add Attribute) and features a sidebar with various system settings like Benutzer, Gruppen, Netzwerk, Rechner, DNS, DHCP, Richtlinien, Mail, Nagios, and Mein Konto. The 'Grundeinstellungen' (Basic Settings) tab is active, displaying a form with the following fields:

- Name (\*)**: Stellenzugeordnet
- Benötigtes Modul (\*)**: users/user
- Name der Karteikarte**: zugeordnete Stellen
- Nummer auf der Karteikarte**: (empty)

Buttons for 'Abbrechen' (Cancel) and 'OK' are visible at the bottom of the form.

```
#!/usr/bin/python

name='pwcoppy'
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

## 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

Fragen?

dass IT

dass IT