UNIVERSITÄT GREIFSWALD
Wissen lockt. Seit 1456

IT-Ressourcenmanagement an der Universität Greifswald

Universitätsrechenzentrum
G.K. Grubert

gordon.grubert@uni-greifswald.de

25.09.2019

Off Topic: Status DNSSec im DFN-Bereich

11.03.2019: Ergebnis bei 342 analysierten Mitgliedern

- Nutzung von DNSSec: 42
- Nutzung von DANE: 20

Off Topic: Status DNSSec im DFN-Bereich

11.03.2019: Ergebnis bei 342 analysierten Mitgliedern

- Nutzung von DNSSec: 42
- Nutzung von DANE: 20

18.09.2019: Ergebnis bei 342 analysierten Mitgliedern

- Nutzung von DNSSec: 45
- Nutzung von DANE: 21

Off Topic: Status DNSSec im DFN-Bereich

11.03.2019: Ergebnis bei 342 analysierten Mitgliedern

- Nutzung von DNSSec: 42
- Nutzung von DANE: 20

18.09.2019: Ergebnis bei 342 analysierten Mitgliedern

- Nutzung von DNSSec: 45
- Nutzung von DANE: 21

- Anteil bezogen auf Mitgliederzahl: 12,28% auf 13,15%
- Steigerungsrate bezogen auf letzten Wert: 7,14%
- fehlende TLSA-Records für MX-Einträge

Wer kennt dies nicht?

- es ist nie ein Mitarbeiter für irgendeine IT-Ressource verantwortlich
- Vorhandensein nicht mehr benötigter Nutzeraccounts
- belegter Platz auf Fileserver von verwaisten Projekten
- vergebene IP-Adressen für nicht mehr vorhandene Geräte
- Telefonnummern für Personen, die schon lange nicht mehr beschäftigt sind

Was sind die Folgen?

- Änderungen an der IT-Infrastruktur können nicht ordentlich kommuniziert werden

  (es ist ja keiner verantwortlich)

Was sind die Folgen?

- Änderungen an der IT-Infrastruktur können nicht ordentlich kommuniziert werden

  (es ist ja keiner verantwortlich)

- Ressourcen kosten ggf. Geld

  (z.B. Storage Fileserver, Mailserver, Telefonnummern)

Was sind die Folgen?

- Änderungen an der IT-Infrastruktur können nicht ordentlich kommuniziert werden

  (es ist ja keiner verantwortlich)
- Ressourcen kosten ggf. Geld

  (z.B. Storage Fileserver, Mailserver, Telefonnummern)
- **Sicherheitsprobleme**
  z.B. durch verwaiste Firewallregeln

Was sind die Folgen?

- Änderungen an der IT-Infrastruktur können nicht ordentlich kommuniziert werden

  (es ist ja keiner verantwortlich)
- Ressourcen kosten ggf. Geld

  (z.B. Storage Fileserver, Mailserver, Telefonnummern)
- **Sicherheitsprobleme**
  z.B. durch verwaiste Firewallregeln
- **Datenschutzprobleme**
  u.U. werden Daten gespeichert, die gar nicht mehr gespeichert werden dürfen

Was ist die Lösung?

Was ist die Lösung?

Ein vollumfängliches IT-Ressourcenmanagenent für alle Dienste des Universitätsrechenzentrums!

Basis für das Ressourcenmanagement

- Herzstück ist ein OpenLDAP-Clustersystem

Basis für das Ressourcenmanagement

- Herzstück ist ein OpenLDAP-Clustersystem
- alles, was LDAP-fähig ist, wird im LDAP gespeichert
  - Nutzerdaten
  - DHCP-Konfiguration
  - DNS-Konfiguration
  - VLAN-Konfiguration
  - NACL-Berechtigungen aller Geräte

Basis für das Ressourcenmanagement

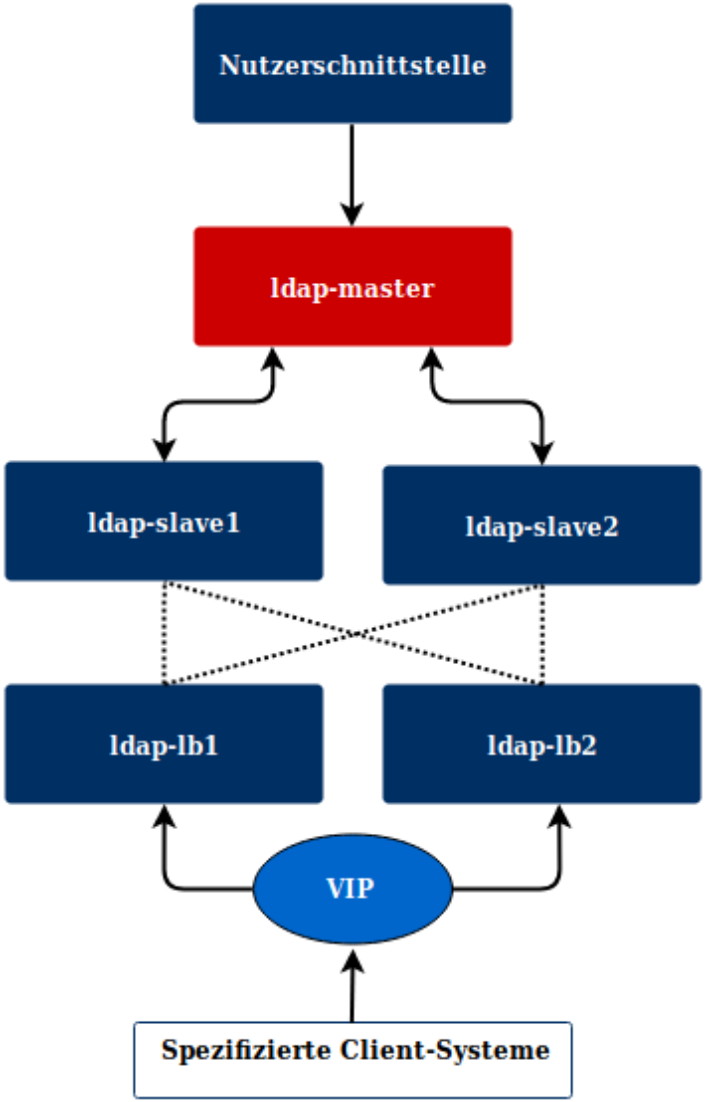
- Herzstück ist ein OpenLDAP-Clustersystem
- alles, was LDAP-fähig ist, wird im LDAP gespeichert
  - Nutzerdaten
  - DHCP-Konfiguration
  - DNS-Konfiguration
  - VLAN-Konfiguration
  - NACL-Berechtigungen aller Geräte
- vollautomatische Ankopplung an alle relevanten Systeme
  - Personalverwaltungen
  - Studierendensekretariat
  - Active Directory (wird dem OpenLDAP untergeordnet!)
  - Firewall
  - Telefonanlage
  - u.v.m.

Basis für das Ressourcenmanagement

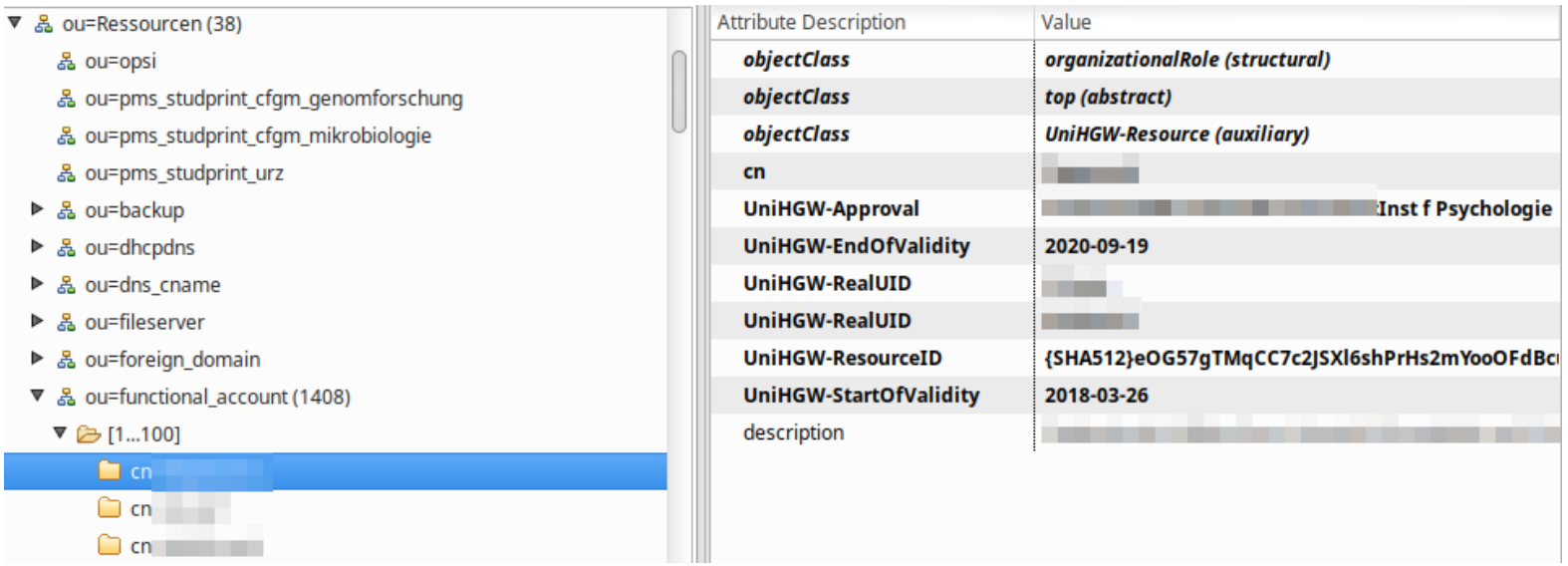
- Einführung eines Metadatenzweiges (= Ressourcen)
- Verknüpfung aller relevanten LDAP-Objekte mit dem Metadatenzweig

  (analog zu einer relationalen Datenbank)

Übersicht des OpenLDAP-Clusters



Metadatenzweig (Ressourcen)



⇒ derzeit 38 Ressourcen-Typen wie z.B.

- IP-Adressreservierungen (inkl. DNS- und DHCP-Einträgen)
- DNS-Alias-Einträge
- Funktionsaccounts
- Telefonnummern
- Netzwerkregistrierung aller dienstlichen Geräte
- Nutzung des Backup-Systems
- Zugriff auf HPC-Cluster

Metadaten

- i.d.R. mindestens **2** Verantwortliche
- Genehmiger
- Datum der Genehmigung und des Ressourcenablaufs
- Beschreibung
- eindeutige ID für eine Ressource
- Informationen über Ablaufinformationen

Attribute Description	Value
objectClass	*organizationalRole (structural)*
objectClass	*top (abstract)*
objectClass	*UniHGW-Resource (auxiliary)*
cn	
UniHGW-Approval	Inst f Psychologie
UniHGW-EndOfValidity	2020-09-19
UniHGW-RealUID	
UniHGW-RealUID	
UniHGW-ResourceID	{SHA512}eOG57gTMqCC7c2JSXl6shPrHs2mYooOFdBc
UniHGW-StartOfValidity	2018-03-26
description	

Ressourceneinrichtung: Antragsworkflow

- Nutzer stellt Antrag im Online-System
- Nutzer benennt einen Genehmiger
- Genehmiger genehmigt Antrag
- Universitätsrechenzentrum genehmigt Antrag technisch und richtet Ressource ein

Ressourcenlöschung (automatisiert)

Gründe für die Löschung

1. Ressource hat Ablaufdatum überschritten
2. Anzahl der Verantwortlichen auf 1 gesunken
3. Nutzer löscht Ressource selbständig

Ressourcenlöschung (automatisiert)

Vollautomatisierter Workflow

- alle Verantwortliche erhalten **SMIME-signierte** E-Mails
- 3 E-Mails im Abstand von 4 Wochen
- Ablaufdatum +12 Wochen überschritten und 3 Ablaufinformationen verschickt

Ressourcenlöschung (automatisiert)

Vollautomatisierter Workflow

- alle Verantwortliche erhalten **SMIME-signierte** E-Mails
- 3 E-Mails im Abstand von 4 Wochen
- Ablaufdatum +12 Wochen überschritten und 3 Ablaufinformationen verschickt

$\Rightarrow$ Löschung des Metadatensatzes im OpenLDAP

Ressourcenlöschung (automatisiert)

Vollautomatisierter Workflow

- alle Verantwortliche erhalten **SMIME-signierte** E-Mails
- 3 E-Mails im Abstand von 4 Wochen
- Ablaufdatum +12 Wochen überschritten und 3 Ablaufinformationen verschickt

$\Rightarrow$ Löschung des Metadatensatzes im OpenLDAP

- Löschung aller zugehörigen Daten im OpenLDAP
  (Verantwortung beim OpenLDAP-System)
- Löschung aller Daten in externen Systemen
  (Verantwortung beim jeweiligen Systembetreiber)

Nutzerfeedback

Negativ

- „Warum läuft die Webseite ab? Die brauche ich für immer!“
- Nutzer ignorieren 3 automatische Warnungen vor der Löschung

Nutzerfeedback

Negativ

- „Warum läuft die Webseite ab? Die brauche ich für immer!“
- Nutzer ignorieren 3 automatische Warnungen vor der Löschung

$\Rightarrow$ das hat wirklich Konsequenzen 😉

Nutzerfeedback

Negativ

- „Warum läuft die Webseite ab? Die brauche ich für immer!“
- Nutzer ignorieren 3 automatische Warnungen vor der Löschung

⇒ das hat wirklich Konsequenzen 😉

Positiv

- rein elektronischer Workflow
- schnellere Bearbeitung möglich
- gute Übersicht im Nutzerportal
- selbständige Löschung möglich

Nutzerfeedback

Kompromisse aufgrund des Nutzerfeedbacks

- persönliche Telefonnummern werden direkt an die Laufzeit des Nutzeraccounts gebunden
- einige Ressourcentypen benötigen nur einen Verantwortlichen

Ressourcenmanagement im OpenLDAP-System

Die primäre Logik des Ressourcenmanagement wird direkt im OpenLDAP-System abgebildet:

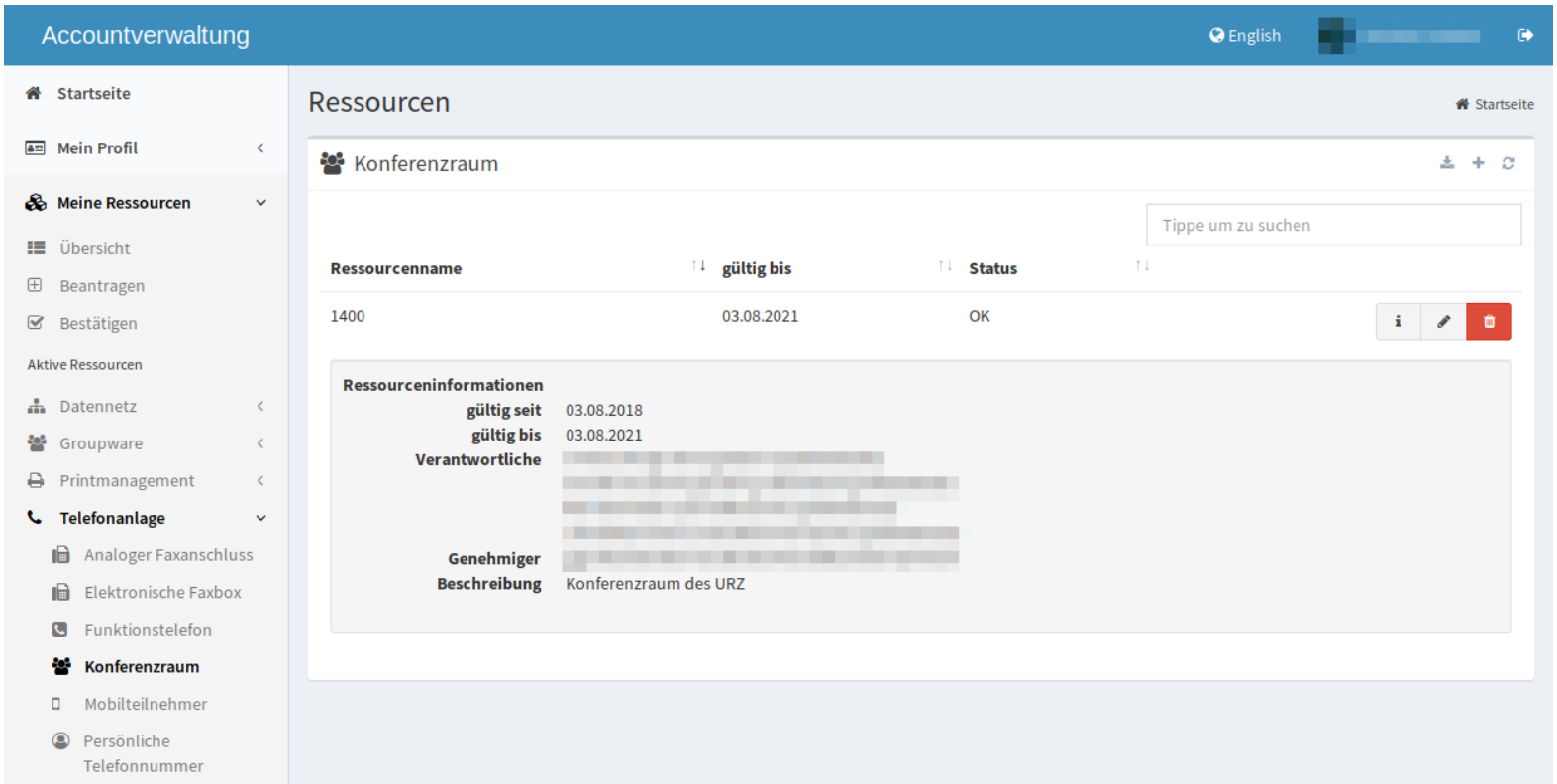
```
# [...]
. . * * * root /opt/LDAPManagement/CleanupFirewallRules.pl > /dev/null
. . * * * root /opt/LDAPManagement/PersonalUpdate.pl > /dev/null
. . * * * root /opt/LDAPManagement/GroupUpdate.pl > /dev/null
. . * * * root /opt/LDAPManagement/DHCP-DNS-Pools.pl > /dev/null
. . * * * root /opt/LDAPManagement/Cleanup.pl > /dev/null
. . * * * root /opt/LDAPManagement/ADUserSync.pl > /dev/null
# [...]
```

Ressourcenmanagement in angeschlossenen Systemen

Angeschlossene Systeme (z.B. Mailsystem) müssen selbständig die Bereinigung auf Basis des OpenLDAP-Datenbestandes vornehmen:

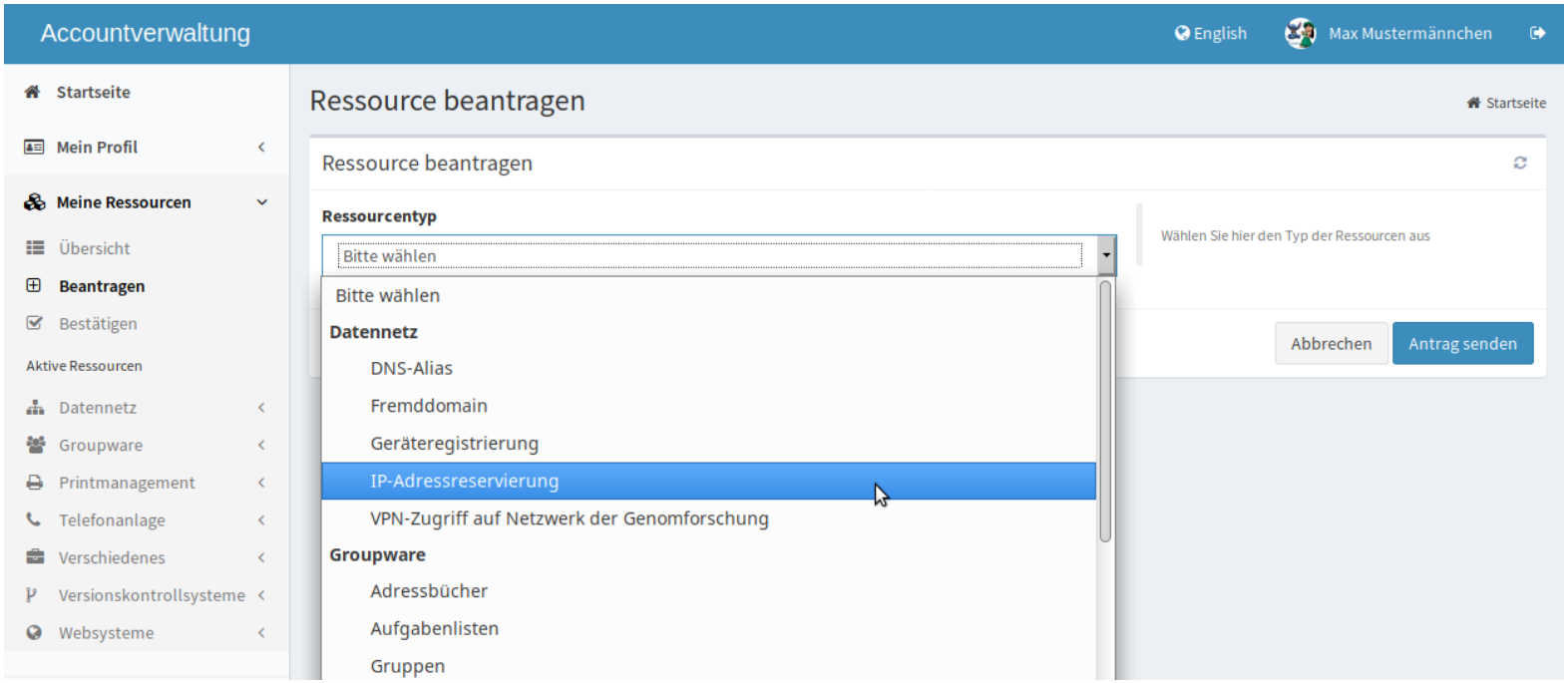
```
# [...]
. . * * * root /opt/admin-tools/DovecotRemoveMailboxes.pl > /dev/null
# [...]
```

Nutzerportal (Ressourcenübersicht)

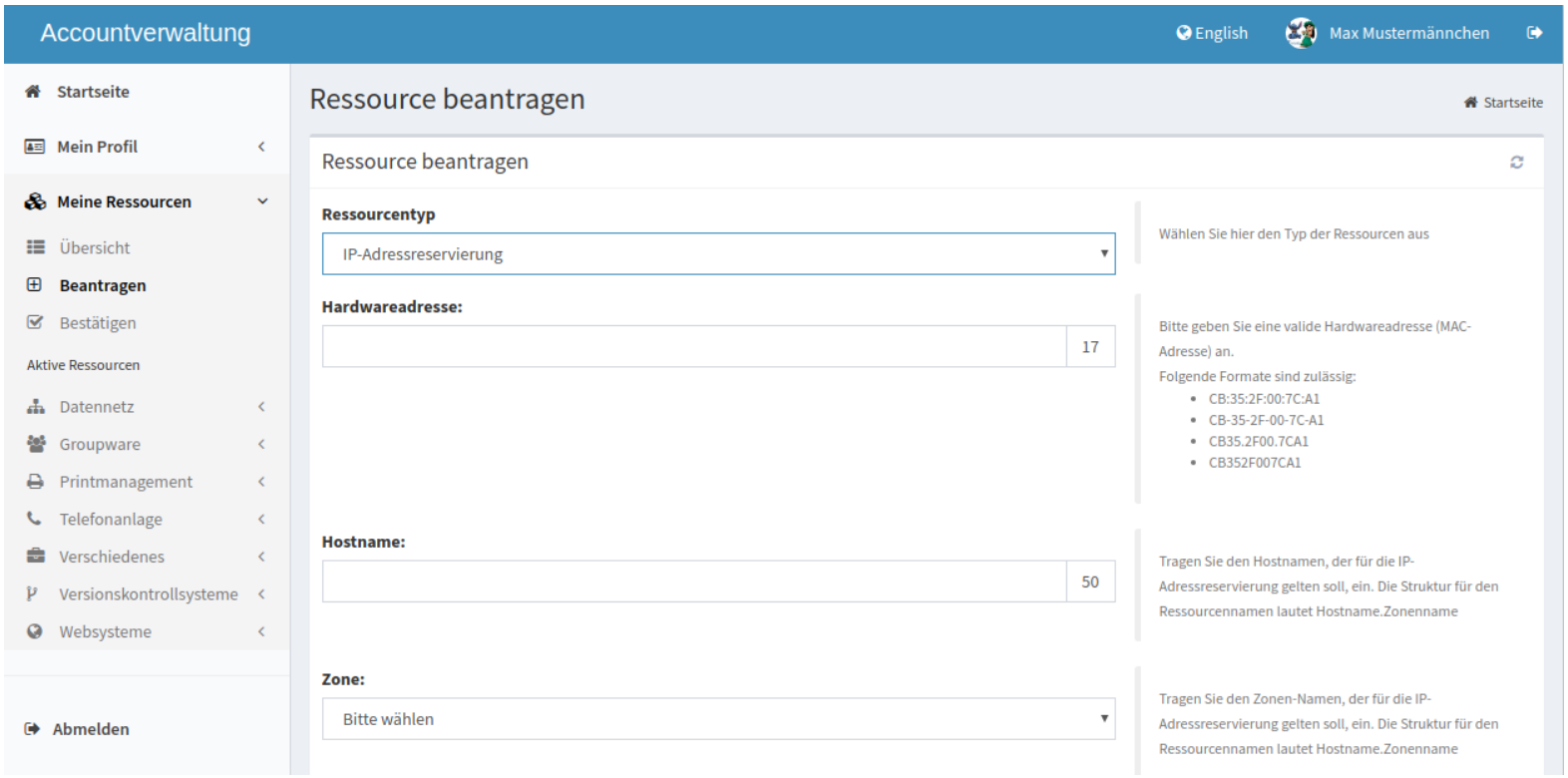


Realized in Perl (https://www.perl.org)

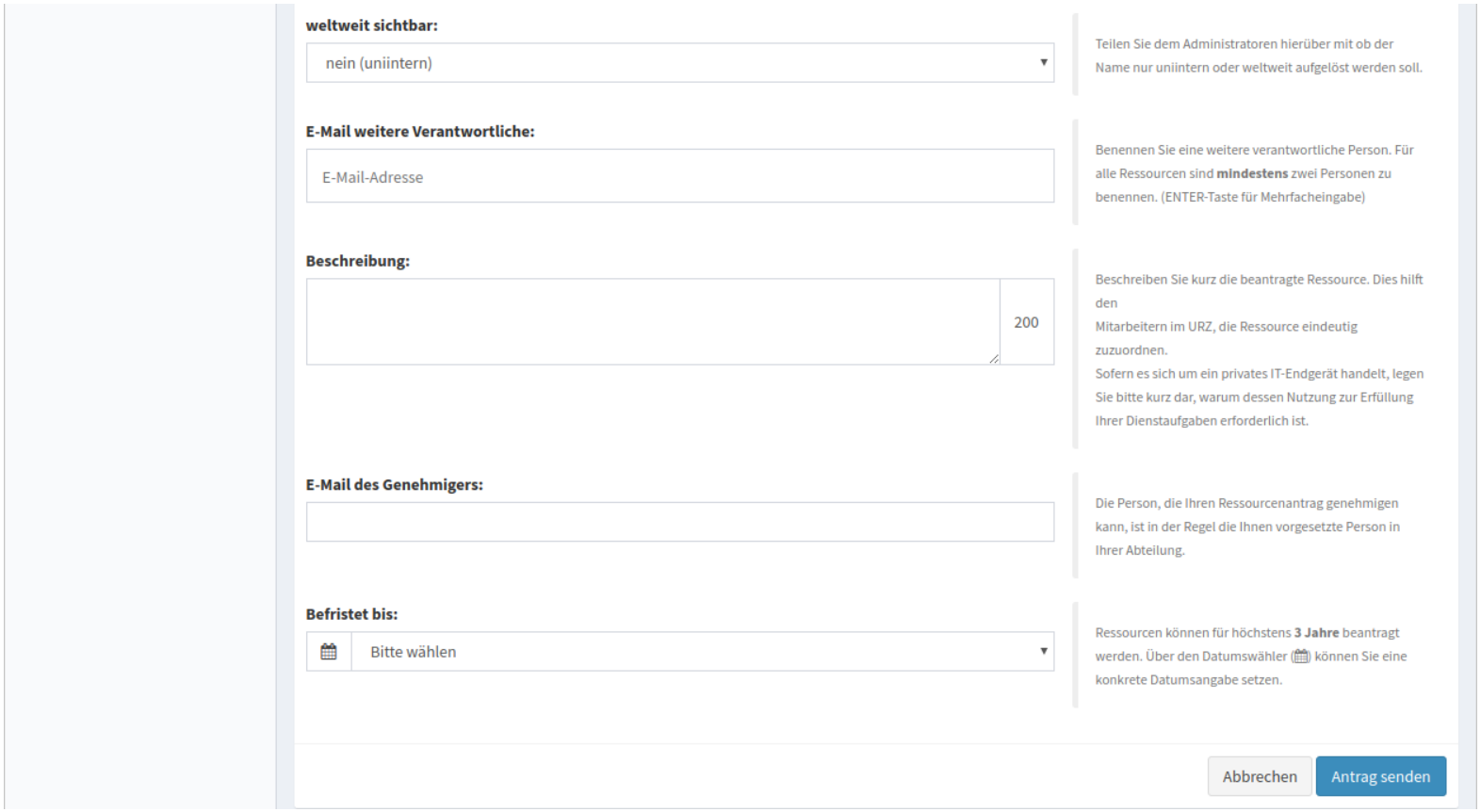
Nutzerportal (Ressource beantragen)



Nutzerportal (Ressource beantragen)



Nutzerportal (Ressource beantragen)



Nutzerportal

- die Nutzerakzeptanz steht und fällt mit dem Nutzerportal
- das Portal ist bisher mit Auszubildenden entstanden und gewachsen

Nutzerportal

- die Nutzerakzeptanz steht und fällt mit dem Nutzerportal
- das Portal ist bisher mit Auszubildenden entstanden und gewachsen

Unique Selling Point Greifswald

Wir sind wohl das einzige Rechenzentrum an einer Universität **OHNE** Anwendungs-/Webentwickler.

⇒ Wie haben viele weitere Ideen, aber die Entwicklung im Nutzerbereich stagniert momentan leider 😕

Fazit

- alles, was das Universitätsrechenzentrum Nutzern zur Verfügung stellt, wird über das Ressourcenmanagement realisiert
- vollautomatische Bereinigung aller Ressourcen
- es gibt keine „Karteileichen“ mehr
- wesentliche Verbesserung der IT-Sicherheit und des Datenschutzes erreicht
- finanzielle Einsparungen gab es kostenfrei dazu

Fazit

- alles, was das Universitätsrechenzentrum Nutzern zur Verfügung stellt, wird über das Ressourcenmanagement realisiert
- vollautomatische Bereinigung aller Ressourcen
- es gibt keine „Karteileichen“ mehr
- wesentliche Verbesserung der IT-Sicherheit und des Datenschutzes erreicht
- finanzielle Einsparungen gab es kostenfrei dazu

Backend-Realisierung mittels OpenLDAP

Man kann ohne OpenLDAP auskommen, muss es aber nicht.