

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-Ressourcenmanagement 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

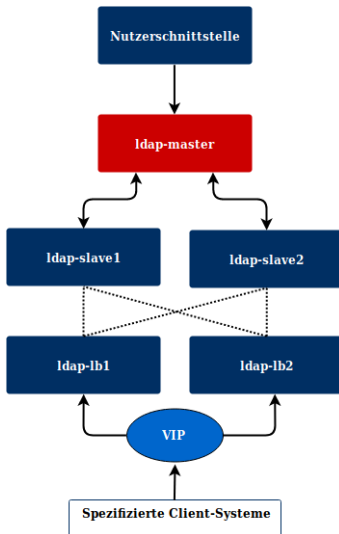
- Herzstück ist ein OpenLDAP-Clustersystem
- alles, was LDAP-fähig ist, wird im LDAP gespeichert
 - Nutzerdaten
 - DHCP-Konfiguration
 - DNS-Konfiguration
 - VLAN-Konfiguration
 - NACL-Berechtigungen aller Geräte
- vollautomatische Ankopplung an alle relevanten Systeme
 - Personalverwaltungen
 - Studierendensekretariat
 - 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)

The screenshot shows the Active Directory console with the 'ou=Ressourcen (38)' container selected. The left pane displays a tree view of the container's contents, including sub-objects like 'ou=opsi', 'ou=pms_studprint_cfgm_genomforschung', and 'ou=functional_account (1408)'. The right pane shows the attributes of the selected container.

Attribute	Description	Value
objectClass		organizationalRole (structural)
objectClass		top (abstract)
objectClass		UniHGW-Resource (auxiliary)
cn		[REDACTED]
UniHGW-Approval		[REDACTED] Inst f Psychologie
UniHGW-EndOfValidity		2020-09-19
UniHGW-RealUID		[REDACTED]
UniHGW-RealUID		[REDACTED]
UniHGW-ResourceID		{SHA512}eOG57gTMqCC7c2J5Xl6shPrHs2mYooOFdBc
UniHGW-StartOfValidity		2018-03-26
description		[REDACTED]

⇒ derzeit 38 Ressourcen-Typen wie z.B.

- IP-Adressreservierungen (inkl. DNS- und DHCP-Einträge)
- 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
<i>objectClass</i>	<i>organizationalRole (structural)</i>
<i>objectClass</i>	<i>top (abstract)</i>
<i>objectClass</i>	<i>UniHGW-Resource (auxiliary)</i>
cn	[REDACTED]
UniHGW-Approval	[REDACTED] Inst f Psychologie
UniHGW-EndOfValidity	2020-09-19
UniHGW-RealUID	[REDACTED]
UniHGW-RealUID	[REDACTED]
UniHGW-ResourceID	{SHA512}eOG57gTMqCC7c2J5Xl6shPrHs2mYooOFdBc
UniHGW-StartOfValidity	2018-03-26
description	[REDACTED]

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
- ⇒ 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
- ⇒ 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
- ⇒ 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)

The screenshot shows a web application interface for 'Accountverwaltung' (Account Management). The main content area is titled 'Ressourcen' (Resources) and displays a list of resources. The first resource is 'Konferenzraum' (Conference Room).

Resource List:

Ressourcenname	gültig bis	Status
1400	03.08.2021	OK

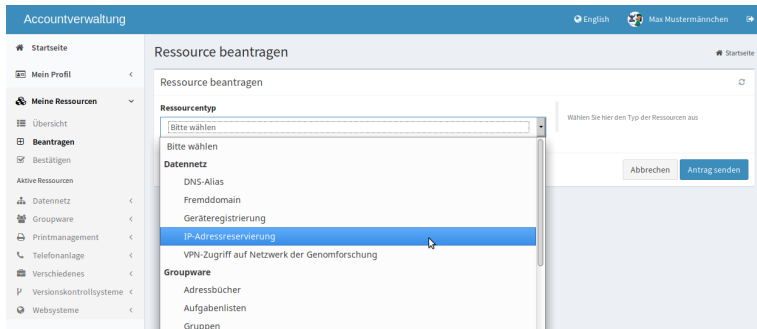
Resource Information (for 1400):

- gültig seit:** 03.08.2018
- gültig bis:** 03.08.2021
- Verantwortliche:** [Redacted]
- Genehmiger:** [Redacted]
- Beschreibung:** Konferenzraum des URZ

The interface includes a sidebar with navigation options like 'Startseite', 'Mein Profil', 'Meine Ressourcen', and 'Telefonanlage'. The top right shows the language is set to English.

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

Nutzerportal (Ressource beantragen)



Accountverwaltung English Max Mustermannchen

Ressource beantragen

Ressource beantragen

Ressourcentyp

Bitte wählen

Bitte wählen

Datennetz

- DNS-Alias
- Fremddomain
- Geräteregistrierung
- IP-Adressreservierung**
- VPN-Zugriff auf Netzwerk der Genomforschung

Groupware

- Adressbücher
- Aufgabenlisten
- Gruppen

Wählen Sie hier den Typ der Ressourcen aus

Abbrechen Antrag senden

Nutzerportal (Ressource beantragen)

Accountverwaltung English Max Mustermannchen

Startseite

Startseite

Mein Profil

Meine Ressourcen

- Übersicht
- Beantragen
- Bestätigen

Aktive Ressourcen

- Datennetz
- Groupware
- Printmanagement
- Telefonanlage
- Verschiedenes
- Versionskontrollsysteme
- Websysteme

Abmelden

Ressource beantragen

Ressource beantragen

Ressourcentyp

IP-Adressreservierung

Hardwareadresse:

17

Hostname:

50

Zone:

Bitte wählen

Wählen Sie hier den Typ der Ressourcen aus

Bitte geben Sie eine valide Hardwareadresse (MAC-Adresse) an.


Folgende Formate sind zulässig:

- CB:35:2F:00:7C:A1
- CB-35-2F-00-7C-A1
- CB35.2F00.7CA1
- CB352F007CA1

Tragen Sie den Hostnamen, der für die IP-Adressreservierung gelten soll, ein. Die Struktur für den Ressourcennamen lautet Hostname.Zonenname

Tragen Sie den Zonen-Namen, der für die IP-Adressreservierung gelten soll, ein. Die Struktur für den Ressourcennamen lautet Hostname.Zonenname

Nutzerportal (Ressource beantragen)

weltweit sichtbar: <input type="text" value="nein (uniintern)"/>	Teilen Sie dem Administratoren hierüber mit ob der Name nur unilintern oder weltweit aufgelöst werden soll.
E-Mail weitere Verantwortliche: <input type="text" value="E-Mail-Adresse"/>	Benennen Sie eine weitere verantwortliche Person. Für alle Ressourcen sind mindestens zwei Personen zu benennen. (ENTER-Taste für Mehrfacheingabe)
Beschreibung: <input type="text" value=""/> 200	Beschreiben Sie kurz die beantragte Ressource. Dies hilft den Mitarbeitern im URZ, die Ressource eindeutig zuzuordnen. Sofern es sich um ein privates IT-Endgerät handelt, legen Sie bitte kurz dar, warum dessen Nutzung zur Erfüllung ihrer Dienstaufgaben erforderlich ist.
E-Mail des Genehmigers: <input type="text"/>	Die Person, die Ihren Ressourcenantrag genehmigen kann, ist in der Regel die Ihnen vorgesetzte Person in Ihrer Abteilung.
Befristet bis: <input type="text" value="Bitte wählen"/>	Ressourcen können für höchstens 3 Jahre beantragt werden. Über den Datumswähler  können Sie eine konkrete Datumsangabe setzen.
<input type="button" value="Abbrechen"/> <input type="button" value="Antrag senden"/>	

Nutzerportal

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

Nutzerportal

- die Nutzerakzeptanz steigt 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 „Kartelleichen“ 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 „Kartelleichen“ 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.