UCS Univention Corporate Server

- Basics - https://www.univention.de/blog-de/2016/07/kurz-erklaert-was-steckt-hinter-den-begriffen-ldap-openldap/
- Forum https://help.univention.com/
- Support Wiki: https://wiki.univention.de/index.php?title=Main_Page
- Benutzerhandbuch https://docs.software-univention.de/handbuch-4.4.html

Zugang

Port forwards

Per SSL `https://tokoeka.netzwissen.de:8443`

Per SSH `ssh -p 8422 tokoeka.netzwissen.de`

Konfiguration per shell

UCR - Direkte Konfiguration im System

```
ucr
```

- Auslesen ucr dump
- Setzen ucr set
- Löschen ucr unset

UDM Univention Directory Manager

Konfiguration der Objekte im OpenLDAP. Allgemeine Syntax

udm [modulname] [aktion] [option]

Beispiel

```
udm oidc/rpservice create --set name=<internal_name> \
    --position cn=oidc,cn=univention,$(ucr get ldap/base) \
    --set clientid=<client_identifier> \
    --set clientsecret=<averylongpassword> \
    --set trusted=yes \
    --set applicationtype=web \
    --set redirectURI=<URL_from_client_documentation>
```

Objekte auflisten

```
udm oidc/rpservice list

udm oidc/rpservice create --set name=owncloud oidc app \
    --position cn=oidc,cn=univention,$(ucr get ldap/base) \
    --set clientid=<client_identifier> \
    --set clientsecret=<averylongpassword> \
    --set trusted=yes \
    --set applicationtype=web \
    --set redirectURI=<URL_from_client_documentation>
```

Netzwerkeinstellungen

```
root@ucs-2370:~# ucr dump | grep interfaces
interfaces/ens18/address: 136.243.85.155
interfaces/ens18/broadcast: 136.243.85.159
interfaces/ens18/ipv6/acceptRA: false
interfaces/ens18/netmask: 27
interfaces/ens18/network: 136.243.85.128
interfaces/ens18/route/route1: net 138.201.52.40 netmask 255.255.255.248 gw
138.201.52.41
interfaces/ens18/route/route2: net 136.243.85.152 netmask 255.255.255.248 gw
138.201.52.41
interfaces/ens18/start: true
interfaces/ens18/type: static
interfaces/ens19/address: 10.10.10.17
interfaces/ens19/broadcast: 10.10.10.255
interfaces/ens19/ipv6/acceptRA: false
interfaces/ens19/netmask: 255.255.255.0
interfaces/ens19/network: 10.10.10.0
interfaces/ens19/start: true
interfaces/ens19/type: static
interfaces/handler: ifplugd
interfaces/primary: ens19
mail/postfix/inet/interfaces: 127.0.0.1
samba/interfaces/bindonly: yes
samba/interfaces: lo <interfaces/primary>
samba/register/exclude/interfaces: docker0
```

In Kurzform

```
ucr search –brief interfaces

ucr search –brief bridge

ucr search –brief gateway
```

Statische Routen setzen

https://help.univention.com/t/configuring-static-routes/8120

```
root@ucs-2370:~# univention-config-registry set
interfaces/ens18/route/route1="net 138.201.52.40 netmask 255.255.255.248 gw
138.201.52.41"
Setting interfaces/ens18/route/route1
Multifile: /etc/network/interfaces
ifdown: interface ens18 not configured
File: /etc/dhcp/dhclient.conf
RTNETLINK answers: File exists
ifup: failed to bring up ens18
File: /etc/default/ifplugd
File: /etc/issue
File: /usr/share/univention-management-console/meta.json
File: /etc/welcome.msg
```

DNS Einstellungen

```
ucr search --brief ^nameserv dns/forward
```

Jede Änderung am Netz mit

```
 /etc/init.d/networking restart
```

bestätigen

LDAP Suche

https://help.univention.com/t/cool-solution-ldap-search-user-simple-authentication-account/11818

Shell Suche erfolgt über einen LDAP User vom Typ "simple authentication account"

lokale Suche

```
ldapsearch -x -D uid=LDAPsearch,cn=users,$(/usr/sbin/ucr get ldap/base) -W
uid=Administrator
```

Remote Suche

LDAP Ports

```
  LDAP Port: 7389
  LDAP Port (SSL): 7636
```

```
ldapsearch -H LDAP://10.10.10.17 -x -D
uid=LDAPsearch,cn=users,dc=netzwissen,dc=de -W uid=Administrator
```

UCS bietet auf allen Systemen das Kommandozeilen-Tool „univention-ldapsearch„. Damit ist es „root“ Benutzern möglich, mit dem Account des aktuellproeen UCS Systems auf das LDAP zuzugreifen. Das Tool nutzt im Hintergrund „ldapsearch„, übergibt aber die korrekten Werte für LDAP Server, LDAP Basis und Authentifikation. Es reicht also die Angabe des LDAP Filters für eine Suche:

```
univention-ldapsearch "(&( objectClass=person)(uid=Administrator))"
```

LDAP Integration

Beispiel REDMINE -
https://help.univention.com/t/cool-solution-ldap-search-user-simple-authentication-account/11818

Integration Dokuwiki

```
LDAP Auth Dokuwiki gegen UCS

<?php
/**
 * Univention Corporate Server configuration for LDAP Auth Plugin
 * See https://www.dokuwiki.org/plugin:authldap:ucs for details and
explanation
 */
$conf['useacl']      = 1;
$conf['openregister']= 0;
$conf['superuser']   = '@Domain Admins';
$conf['authtype']    = 'authldap';

$conf['plugin']['authldap']['server']      = 'ldap://1.2.3.4:389';
$conf['plugin']['authldap']['starttls']    = 1;
$conf['plugin']['authldap']['usertree']    = 'cn=users, dc=basedn';
$conf['plugin']['authldap']['grouptree']   = 'cn=groups, dc=basedn';
$conf['plugin']['authldap']['userfilter']  =
'(&(uid=%{user})(objectClass=posixAccount))';
$conf['plugin']['authldap']['groupfilter'] =
'(&(objectClass=posixGroup)(|(gidNumber=%{gid})(uniqueMember=%{dn})))';

$conf['plugin']['authldap']['mapping']['mail'] = 'mailprimaryaddress';>
```

OIDC OpenID Connect

Kopano Konnectd läuft als Docker Container

systemctl status docker-app-openid-connect-provider.service

Zugang zum Container

```
docker exec -it $CONTAINER_NAME sh

printenv | grep -i "identifier"
```

```
root@idp:/etc/kopano# systemctl status docker-app-openid-connect-
provider.service
● docker-app-openid-connect-provider.service - LSB: Start the Container for
openid-connect-provider
   Loaded: loaded (/etc/init.d/docker-app-openid-connect-provider;
generated)
   Active: active (exited) since Sat 2021-08-28 08:24:23 CEST; 5s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6322 ExecStart=/etc/init.d/docker-app-openid-connect-provider
start (code=exited, status=0/SUCCESS)
```

und

```
root@idp:/etc/kopano# docker ps -a
CONTAINER ID        IMAGE
COMMAND             CREATED             STATUS                       PORTS
NAMES
152e4906aef3        docker.software-univention.de/openid-connect-
provider:2.2-konnect-0.33.11-2   "wrapper.sh"        5 weeks ago
Exited (127) 4 minutes ago                           loving_heisenberg
1f4834f74656        docker.software-univention.de/dudle:1.2
"/start.sh"         5 weeks ago         Up 8 days
0.0.0.0:40001->80/tcp   romantic_dewdney
root@idp:/etc/kopano#
```

Service Registrierung per shell

```
udm oidc/rpservice create --set name=<internal_name> \
    --position cn=oidc,cn=univention,$(ucr get ldap/base) \
    --set clientid=<client_identifier> \
    --set clientsecret=<averylongpassword> \
    --set trusted=yes \
    --set applicationtype=web \
    --set redirectURI=<URL_from_client_documentation>
```

Siehe https://docs.software-univention.de/handbuch-4.4.html#domain:oidc

Kopano Connect neu starten

```
root@idp:/etc/kopano# systemctl stop docker-app-openid-connect-
provider.service

root@idp:/etc/kopano# systemctl start docker-app-openid-connect-
provider.service
```

OpenID discovery .well-known URLs

Daimler

```
curl -.v https://sso.daimler.com/.well-known/openid-configuration -H
"Accept: application/json"
```

Netzwissen IDP

Forum

```
https://ucs-sso.netzwissen.de/auth/realms/forum/.well-known/openid-configura
tion
```

Owncloud2

https://owncloud2.netzwissen.de/.well-known/openidconnect/redirect

https://owncloud2.netzwissen.de/.well-known/openid-configuration

Forum

https://meta.discourse.org/t/openid-connect-authentication-plugin/103632

Debugging UCS

https://github.com/univention/openid-connect-provider/blob/02e492f22583197d0e01d70c4fbc304a7fbfa0b1/app/inst.tmpl#L38

https://github.com/univention/openid-connect-provider/blob/master/app/settings

univention-app logs openid-connect-provider