

Migration Univention Corporate Server & Kopano nach Zamba AD & Mailcow

Nachdem viele kleinere Kunden nur den Domaincontroller benötigen, jedoch UCS + Kopano für den Betrieb nutzen, kann UCS bei vielen Kunden nun ersetzt werden.

Das Upgrade auf UCS 5.2 zeigt erneut, dass sich der Aufwand eines Upgrades nicht mehr mit dem Nutzen eines Domaincontrollers rechnet.

“ Updates von Mailcow und Zamba AD Controller laufen künftig in wenigen Minuten, nicht mehrere Stunden

Kunden die Keycloak und eine supportete Umgebung wünschen bleiben bitte bei Univention!!!

Entsprechende Kurse finden Sie auf cloudistboese.de unter Mailcow und Domaincontroller ablösen!

Systemvoraussetzungen

- Bestehender Univention Corporate Server im AD Modus
- Kopano oder vergleichbare Groupware mit IMAP
- Proxmox VE >8.x mit Linux Container mit installiertem GIT

Installation zweiter Domaincontroller

Installation auf Proxmox im z. B. /root Ordner



```
git clone -b dev https://github.com/bashclub/zamba-lxc-toolbox
```

```
cd zamba-lxc-toolbox
```

```
cp conf/zamba.conf.example conf/zamba.conf
```

In der zamba.conf folgende Parameter an das System anpassen

```
## LXC_TEMPLATE_STORAGE="local" #LXC Template Store
LXC_ROOTFS_SIZE="32" #DCs Root Size
LXC_ROOTFS_STORAGE="rpool-data" #or local-zfs #DCs Root Store
LXC_SHAREFS_SIZE="100" #DCs Root Backup Size
LXC_SHAREFS_STORAGE="rpool-data" #or local-zfs #DCs Backup Store
LXC_HOSTNAME="zmb-ad"
LXC_DOMAIN="windomain.local"
LXC_IP="10.0.0.254/24"
LXC_GW="10.0.0.1"
LXC_DNS="10.0.0.4" #your old UCS IP, If Windows Step Down to Level 2008R2
first!
LXC_BRIDGE="vmbr0"
LXC_PWD='Admin123'
ZMB_REALM="WINDOMAIN.LOCAL"
ZMB_DOMAIN="WINDOMAIN"
ZMB_ADMIN_USER="administrator"
ZMB_ADMIN_PASS='Admin123'
```

Die installation des LXCs als zweiten DC starten wir mit

bash install.sh -i 100 #für Container 100

Im Menü wählen wir Zamba-AD-Member

Nach der Installation können wir in den Container gelangen mit

pct enter 100

su -

```
wbinfo -u
```

```
wbinfo -g
```

Dort Finden wir im Idealfall alle User und Gruppen, was den Erfolg bestätigt

Folgende Anpassung in der smb.conf macht das Leben leichter

```
## vi /etc/samba/smb.conf
```

```
[global]
```

```
ldap server require strong auth = no
```

```
dns forwarder = 1.1.1.1 1.0.0.1
```

It was DNS

An dieser Stelle erhalten alle Computer mit festen IPs den neuen DNS-Server, der alte DNS Server vom UCS kann jetzt raus.

Im DHCP Server ersetzen wir ebenfalls den DNS Server mit dem neuen DC, der alte DNS Server vom UCS kann raus

Installation Mailcow

```
vi conf/zamba.conf.example conf/zamba.conf
```

Die Installation der Mailcow benötigt keine spezielle Anpassung im unteren Bereich außer dem LXC_HOSTNAME und den Netzwerkeinstellungen

```
## bash install.sh -i 101 #für Container 101
```

Im Menü wählen wir Mailcow

Nach der Installation von Mailcow

```
## pct enter 100
```

```
su -  
  
cd /opt/mailcow-dockerized  
  
./update.sh
```

Danach rufen wir das Mailcow Webinterface mit der Admin Seite auf

“ <https://10.0.0.253/admin>

Folgende Schritte sind unerlässlich

- **Admin Passwort ändern** - System / Konfiguration / Administrator bearbeiten
- **Alle Domänen eintragen und Schwellwerte beachten!** - E-Mail / Konfiguration / Domains
- **Benutzer in der AD anlegen, z. B. bind-mailcow** - Windows Active Directory und Benutzer oder UMC
- **LDAP in Mailcow konfigurieren** - System / Konfiguration / Zugang / Identity Provider
 - Identity Provider: LDAP
 - Host: IP neue ZMB-AD
 - Port: 389 (Active Directory)
 - Benutze SSL: an
 - Ignoriere SSL Fehler: an
 - Base DN: CN=Users,DC=windomain,DC=local
 - Username Feld: mail
 - Attribute Feld: mail
 - Bind DN: CN=bind-mailcow,CN=Users,DC=windomain,DC=local
 - Bind Passwort: wurde oben angelegt
 - Attribute Mapping / Standardvorlage / Default
 - Benutzer beim Login erstellen: an
 - Vollsynchronisation: an
 - Importiere Benutzer: an
 - Sync / Import interval (min): 1 (für den Anfang)
- **Erfolg Kontrollieren** - Mailboxen Mailbox
- **Mails Synchronisieren - E-Mail / Synchronisationen / Neuen Sync Job erstellen**
 - Host: IP Kopano
 - Port 993
 - Benutzername: Windows Login name
 - Elemente ausschließen (Regex) Inhalt entfernen, zu gefährlich
 - Lösche Duplikate im Ziel (--delete2duplicates) nur so lange die Mails noch auf Kopano laufen, danach raus!

- **“** Kopano hat per default IMAP deaktiviert, daher ggf. in der server.conf mal nach disable suchen
oder
In UMC im User unter Kopano IMAP aktivieren

- **Erfolg der Synchronisation im Dialog und dessen Logs kontrollieren**
- **Kalendereinträge der Benutzer exportieren**

| | |
|---|---|
| http://kopano:8080/caldav/<user>/<folder-name>/ | Calendar/task folder in user's store. Make sure the calendar/task folder already exists. |
| http://kopano:8080/caldav/<user>/<sub-folder>/ | Self created subcalendar in the user's own store. Location through actual subfolders in Zarafa is irrelevant. |
| http://kopano:8080/caldav/<other-user>/<folder-name>/ | Shared calendar/task folder of other user |
| http://kopano:8080/caldav/public/<foldername>/ | Calendar/task folder in the public folder |
| http://kopano:8080/caldav/<user>/ | Default calendar of the current user. Although this works for most clients, this URL is not recommended. |

- Die exportierten Dateien können im Mailcow SoGo Frontend oder Mailclient direkt importiert werden
- **Export Kontakte** - geht nur über alten Mailclient, da dein Carddav Server vorhanden
- **Aliase finden und anlegen**
 - univention-ldapsearch -LLL | grep @ | grep mailAlternative
 - Aliase eintragen - E-Mail -Aliasasse / Alias hinzufügen
- **Weiterleitungen finden**
 - univention-ldapsearch -LLL | grep mailForward # Listet Weiterleitungen
 - Weiterleitung wird im SoGo Webfrontend unter E-Mail konfiguriert, nicht in Mailcow!!!
- **Mailcow online stellen**
 - **NAT Ports setzen, z. B. auf OPNsense als Alias**
 - **p_mailcow 80 443 465 993 4190**
 - **h_mailcow 10.0.0.253**
 - **Port Forwarding**
 - **any > WAN IP > p_mailcow > h_mailcow**
- **Mailcow neu starten**

“ pct enter 100

su -

cd /opt/mailcow-dockerized

docker compose down

```
# Optional bei PMG Einsatz greylisting aus
# vi /opt/mailcow-dockerized/data/conf/rspamd/local.d/greylist.conf
# enabled = false;

docker compose up -d
```

- Kontrolle ob Letsencrypt HTTP Challenge funktioniert
 - docker compose logs --tail=200 -f acme-mailcow
- Alternativ eigenes Zertifikat unter /opt/mailcow-dockerized/data/assets/ssl
 - cert.pem
 - key.pem
- DNS Werte beim Provider anpassen oder kontrollieren - E-Mail / Domains / DNS

Abschluss der Arbeiten

- Synchronisationen nach Erfolg deaktivieren
- Optional PMG auf Mailcow verweisen
- Alten Univention Corporate Server abschalten
- **Takeover Active Directory**

- ```
“ pct enter 100
su -
samba-tool fsmo transfer --role=all -Uadministrator
samba-tool domain demote --remove-other-dead-
server=UCS
rm /etc/cron.d/sysvol-sync
```

- **Bereinigung**
  - **RSAT DNS Konsole nach alten Fragmenten durchsuchen und entfernen**
  - **Optional Metadata Cleanup**
- **Anpassung von bestehenden an UCS angebundenen LDAP Clients**
  - **Bind User pro Rolle anlegen, an keinen PC Anmelden wählen**
  - **Dialog des LDAP Clients besuchen und folgende Werte ändern**
    - **IP = neuer ZMB-AD**
    - **Port 7389 zu 389**
    - **UID zu sAMAccountName**
    - **Bind DN uid zu cn ändern**

## Proxmox Mail Gateway

- /opt/mailcow-dockerized/data/conf/rspamd/local.d/greylist.conf
  - enabled = false;
  - docker compose restart rspamd-mailcow

- Konfiguration / Routing / Networks
  - ipvompmg:26
  - greylisting aus
- In allen Maildomains die PMG nutzen
  - Senderabhängige Transport Maps
  - ID 1: ipvompmg:26
- Im Proxmox Mail Gateway
  - Configuration / Mailproxy
    - Relay Domaoin
    - Transport zur Mailcow, kein MX
- Beim DNS Provider PMG Settings überschreiben teile den Mailcow Empfehlung

## Mailpiler

- Identische Installation, siehe LXC Toolbox zuvor
- Empfang aus dem Archiv
  - system / konfiguration / einstellungen / weiterleitungs-hosts
  - ip vom Mailpiler eintragen
- BCC an das Archiv
  - system / konfiguration / routing / transport
    - Ziel piler.windomain.local
    - Next Hop 10.0.0.x
  - e-mail / konfiguration / adressumschreibung / bcc-maps
    - mapping pro domain eintragen (1x eingehend, 1x ausgehend)
      - pro Maildomäne Empfängerabhängig und Senderabhängig
        - Lokales Ziel: sysops.tv
        - BCC-Ziel piler@piler.windomain.local
        - Domain: sysops.tv
- **Kontrolle im Mailpiler unter /var/log/mail.log**
- **LDAP Anpassung wäre in config-site.php im Piler möglich, jedoch nicht für Aliase!**

---

Version #9

Erstellt: 23 Juni 2025 13:04:26 von Christian Zengel (sysops GmbH)

Zuletzt aktualisiert: 23 Juni 2025 15:47:06 von Christian Zengel (sysops GmbH)