# invis-AD 10.x auf invisAD 12.x

Die beste Möglichkeit eines Upgrades stellt eine Neuinstallation eines aktuellen invis-Servers mit anschließender Datenmigration dar.

***Achtung:*** *Ändern Sie bei der Neuinstallation auf keinen Fall etwas an der Namensgebung des Servers oder der Domäne und genauso wenig an der IP-Addressierung! Behalten Sie alle entsprechenden Einstellungen der ursprünglichen Installation bei.*

***Hinweis:*** *Sie sollten sich auf jeden Fall eine lauffähige Version Ihres bestehenden invis-Server erhalten. Installieren Sie also am besten auf neue Festplatten.*

***Hinweis:*** *Wenn Sie genau wie ich auf Logical-Volume-Management setzen sollten sie der VolumeGroup der Neuinstallation einen anderen Namen geben als die der alten Installation. Nur auf diese Weise können Sie die Festplatten beider Installationen gleichzeitig in einem Server eingebaut haben und Daten ohne Umweg über eine externe Platte von der alten auf die neue Installation migrieren.*

Die nachfolgenden Anleitungen gehen davon aus, dass Zarafa als Groupware eingesetzt wurde und auf der Neuinstallation dessen Nachfolger Kopano zum Einsatz kommt.

## Vorbereitung

Im ersten Schritt sind wichtige Dienste in der alten Installation zu stoppen, sie sollten auch aus dem Boot-Konzept des Server entfernt werden. Allem voran „fetchmail“

#### fetchmail

```
invis:~ # systemctl disable fetchmail.service
invis:~ # systemctl stop fetchmail.service
```

#### Samba

```
invis:~ # rcsernet-samba-ad stop
invis:~ # chkconfig -d /etc/init.d/sernet-samba-ad
```

#### Zarafa

```
invis:~ # runzarafa stop
invis:~ # chkconfig -d /etc/init.d/zarafa-server
```

Sichern Sie zunächst in der alten Installation die das Active-Directory, die Zarafa-Datenbank und das gesamte „/etc“ Verzeichnis.

#### Active Directory

```
invis:~ # adbackup
```

Die Sicherung finden Sie unter

```
/srv/shares/archiv/sicherungen/ad/
```

```
invis:~ # zdbdump
```

Die Sicherung der Zarafa-Datenbank ist unter

```
/srv/shares/archiv/sicherungen/datenbanken/
```

zu finden. Für die Zarafa Sicherungen werden dort Unterverzeichnisse benannt nach dem Sicherungsdatum angelegt.

Packen Sie jetzt noch das /etc-Verzeichnis in ein Tar-Archiv:

```
invis:~ # tar -czf etc.tar.gz /etc
```

Kopieren Sie sich alle Sicherungen auf einen USB-Stick oder ähnliches. Jetzt können Sie den Server herunterfahren und fürs erste die Festplatten der alten Installation vom Server trennen. Bauen Sie die neuen ein und installieren Sie den neuen invis-Server entsprechend der Anleitung hier im Wiki.

## Konfigurationen übernehmen

Im Grunde sind nur wenige Konfigurationseinstellungen aus der alten Server-Installation übernommen werden. Wichtig ist natürlich die Konfiguration des SMTP Relayhosts und so sie es nutzen die DDNS-Konfiguration.

### Relayhost

Übernehmen Sie in der Datei

```
/etc/postfix/main.cf
```

die Einstellung des Parameters „relayhost“:

```
...
relayhost = [your.smtphost.de]:587
...
```

Kopieren Sie dann noch die beiden Dateien „sasl_passwd“ und „sasl_passwd.db“ aus „/etc/postfix“ der alten Installation ins gleiche Verzeichnis der neuen und bewegen Sie Postfix zum erneuten Einlesen seiner Konfiguration:

```
invis:~ # postfix reload
```

### DDNS

***Hinweis:*** *Mit* ***DDNS*** *ist an dieser Stelle lediglich „echtes“ Dynamic DNS und nicht etwa die Nutzung von Diensten wie „dynDNS“ oder vergleichbaren, auch wenn es letztlich um die gleiche Sache geht. Um echtes DDNS zu nutzen brauchen Sie Zugriff auf einen entsprechend eingerichteten DNS-Server.*

Sie benötigen die beiden zum DDNS-Verfahren gehörenden Schlüssel-Dateien. Diese sind in invis-Server-Installationen kleiner Version 11.0 unter

```
/etc/ssl/ddns/
```

zu finden und gehören in Versionen größer 11.0 nach:

```
/etc/invis/ddns
```

Kopieren Sie die Dateien einfach aus der Sicherung des /etc-Verzeichnisses.

Danach ist die DDNS-Funktion des invis-Servers noch zu aktivieren. Sie benötigen Dazu die fünfstellige Zahl aus dem Namen der DDNS-Schlüsseldateien.

Die Konfiguration erfolgt in der Datei:

```
/etc/invis/invis.conf
```

```
...
# DDNS-Update
# Verwenden Sie anstelle von z.B. DynDNS.org einen eigenen DNS-Server, den
Sie per DDNS aktualisieren?
# [j/n]
ddnsOn:j

# Adresse des Nameservers
nameServer:dnsmain.example.de

# Hostname (FQDN) Ihres Servers im Internet
fqdn:invis.example.de

# Schlüsselnummer Ihres DDNS-Keys
keyNumber:21165
...
```

Passen Sie Ihre Konfiguration entsprechend dem obigen Beispiel an. Testen können Sie das Setup mit folgendem Kommando:

```
invis:~ # inetcheck
```

Treten hierbei Fehler auf sollten Sie zunächst kontrollieren, ob die Systemzeit Ihres Servers korrekt ist.

## Wiederherstellung des Active Directory

Am besten sichern Sie in der neuen Installation das noch jungfräuliche Active Directory auf die gleiche Weise wie zuvor in der alten Installation, wer weiss wozu es gut ist.

Zwischen invisAD Version 10.x und 12.x hat sich die verwendete Samba-Version grundlegend geändert. Zum einen kommt statt Version 4.2.x jetzt 4.5.x zum Einsatz und zum anderen setzen wir jetzt statt der Pakete von Sernet jetzt eigene Pakete ein.

Stoppen Sie im ersten Schritt Samba und den sssd-Dienst:

```
invis:~ # systemctl stop sssd.service
invis:~ # systemctl stop samba.service
```

Löschen Sie jetzt den gesamten Inhalt des Verzeichnisses:

```
/var/lib/samba/
```

Entpacken Sie jetzt die Sicherung der Active-Directory Sicherung des alten Servers:

```
invis:~ # tar -xzf Samba_20170429.tar.gz
```

Im Verzeichnis der entpackten Sicherung finden Sie zwei gesicherte Verzeichnisse „var/cache/samba“ und „var/lib/samba“. Sie benötigen nur letzteres. Kopieren Sie den Inhalt von „var/lib/samba“ nach „/var/lib/samba“ und starten Sie Samba wieder:

```
invis:~ # cp -r Samba_20170429/var/lib/samba/ /var/lib/samba
invis:~ # systemctl start samba
```

Innherhalb des Active Directory hat sich durch die Aktualisierung der Version strukturell einiges geändert. Diese Teile werden jetzt von Samba als fehlerhaft angesehen und müssen repariert werden:

```
invis:~ # samba-tool dbcheck --fix --yes
```

Lassen Sie sich nicht von der Menge der Fehler erschrecken, das ist vollkommen normal und stellt kein Problem dar.

Nur zur Sicherheit überprüfen Sie auch noch die ACL des ADs und der GPOs:

```
invis:~ # samba-tool dbcheck --reset-well-known-acls
```

Jetzt müssen Sie aus der Sicherung des /etc-Verzeichnisses aus der alten Installation die Kerberos-Keytab wiederherstellen. Kopieren Sie einfach die Datei **krb5.keytab** aus der Sicherung direkt ins /etc-Verzeichnis der Neuinstallation. Danach können Sie auch den sssd-Dienst wieder starten.

```
invis:~ # systemctl start sssd.service
```

Prüfen Sie wie folgt, ob dem System alle Benutzer der alten Installation bekannt sind:

```
invis:~ # getent passwd
```

Ist das nicht der Fall führen Sie folgendes Script aus:

```
invis:~ # delssscache
```

Jetzt sollten, ggf. nach einer kurzen Wartezeit, alle Benutzer angezeigt werden können.

## invis-Portal Einträge anpassen und Portal wiederherstellen

Mit der Weiterentwicklung des invis-Servers haben sich auch ein paar Veränderungen im invis-Portal ergeben. Nicht zuletzt die Änderung von „Zarafa“ zu „Kopano“ hat zur Folge, das der „Groupware“ Link im Portal ins Leere zeigt. Gleiches gilt beispielsweise für die Zeiterfassungssoftware Kimai, die erst seit Kurzem in den invis-Server integriert ist.

In der Datei

```
/var/lib/sine/ldif/04_iportal-initial.ldif
```

sind alle Portal-Einträge im LDIF-Format enthalten und können einzeln oder zu mehreren importiert werden. Nachfolgend wird beispielhaft der Kopano-Link gezeigt:

```
# Groupware KopanoApp
dn: cn=KopanoApp,cn=invis-Portal,cn=Informationen,cn=invis-server,DC=afe-
net,DC=loc
objectClass: top
objectClass: iPortEntry
iPortEntryName: KopanoApp
cn: KopanoApp
iPortEntrySSL: FALSE
iPortEntryURL: [servername]/webapp
iPortEntryDescription: Die moderne Webapp der Groupware "Kopano" bietet
Zugriff auf E-Mails, Terminkalender, Aufgabenverwaltung und Notizen in
frischem "Look & Feel".
iPortEntryActive: FALSE
iPortEntryPosition: Lokal
iPortEntryButton: Groupware
iPortEntryPriv: user
```

Suchen Sie sich in dieser Datei alle für Ihre Installation fehlenden Links und kopieren Sie diese in eine neue LDIF-Datei.

Die auf diese Weise generierte LDIF-Datei kann wie folgt ins Activ-Directory integriert werden:

```
invis:~ # ldbadd -v -H /var/lib/samba/private/sam.ldb kopano.ldif
```

Danach können die gewünschten Portal-Einträge aktiviert, bzw. unerwünschte deaktiviert werden. Hier wieder am Beispiel Zarafa/Kopano. Zunächst den alten Portaleintrag deaktivieren:

```
invis:~ # swpestat ZarafaApp FALSE
```

Jetzt den neuen Kopano-Link aktivieren:

```
invis:~ # swpestat KopanoApp TRUE
```

Sie können sich den aktuellen Status der Portal-Einträge anzeigen lassen:

```
invis:~ # swpestat status
```

Das invis-Portal muss sich am LDAP-Dienst des Active Directory anmelden. Durch den Import des alten Active Directory stimmen die Zugangsdaten in der Portal-Konfiguration nicht mehr. Geändert hat sich das Passwort des Benutzers „ldap.admin“. Sie finden dessen Passwort aus der alten Installation in der Datei

```
/etc/invis/invis-pws.conf
```

in der Sicherung des alten /etc-Verzeichnisses.

Tragen Sie das Passwort in die Datei

```
/etc/invis/portal/config.php
```

in folgende Zeile ein:

```
...
$LDAP_BIND_PW = 'iX9inbrgfh';
...
```

Jetzt müsste sich das Portal im Browser wieder öffnen lassen.

## LDAP Authentifizierung

Neben dem Portal müssen sich noch eine Reihe anderer Dienste oder Scripts mit den gleichen Zugangsdaten am LDAP-Dienst des Active Directory anmelden. Nachfolgend die Liste der Dateien, in denen das Passwort angepasst werden muss:

- **/etc/invis/invis-pws.conf**
- **/etc/invis/portal/config.php**
- **/etc/postfix/ldap-users.cf**
- **/etc/postfix/ldap-users2.cf**
- **/etc/postfix/groups.cf**
- **/etc/postfix/r-canonical.cf**
- **/etc/postfix/s-canonical.cf**
- **/etc/kopano/ldap.cfg** (ldap_bind_passwd = )

## Kopano Datenbak wiederherstellen

Bei der Neuinstallation des invis-Servers wurde selbstverständlich eine neue Datenbank für Kopano angelegt, Sie können diese entweder mit der Sicherung der Zarafa-Datenbank überschreiben oder eine weitere Datenbank anlegen. Ich gehe den zweiten Weg:

Melden Sie sich dafür an der MySQL-Shell an und erzeugen Sie eine neue Datenbank:

```
invis:~ # mysql -u root -p
Server version: 10.0.29-MariaDB SLE 12 SP1 package

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

MariaDB [(none)]> create database kopano2017;
```

Jetzt müssen Sie noch dem bereits existierenden Datenbank-Benutzer „kopano“ alle Rechte daran gewähren und dann die MySQL-Shell wieder verlassen:

```
MariaDB [(none)]> grant all privileges on kopano2017.* to kopano@localhost;
Query OK, 0 rows affected (0.00 sec)
MariaDB [(none)]> quit
Bye
invis:~ #
```

Spielen Sie jetzt die Sicherung der alten Zarafa-Datenbank in die neu angelegte Datenbank ein:

```
invis:~ # gunzip < zarafa.invisad.20170429.gz | mysql -u root -p kopano2017
```

Jetzt ist in der Datei

```
/etc/kopano/server.cfg
```

der Datenbankname anzupassen:

```
...
# Database to connect to
mysql_database          = kopano2017
...
```

Danach muss der Kopano-Server Dienst neu gestartet werden:

```
invis:~ # systemctl restart kopano-server.service
```

Wenn jetzt Ihre Festplatte deutliche Aktivität zeigen liegt dies daran, dass der Kopano-Search Dienst die Datenbank indiziert. Dies ist also ein gutes Zeichen.

Sie können sich jetzt an der Kopano-Webapp testweise anmelden und nachsehen, ob der Datenbank

import funktioniert hat. Bedenken Sie aber, dass wir die Attachements noch nicht wieder hergestellt haben. Diese liegen im Dateisystem und nicht in der Datenbank.

## ownCloud Migration

Die Migration einer bestehenden und umfangreich genutzten ownCloud-Installation ist leider alles Andere als einfach. Begründet liegt dies darin, dass zumindest bis ownCloud Version 9.x im Grunde der Reihe nach von der Ausgangsversion bis zur Zielversion auf alle dazwischen liegenden Versionen aktualisiert werden muss. (Einer der Schwachpunkte von ownCloud, der zukünftig aber ausgeräumt werden soll.)

Die einzelnen Migrationsschritte sollten bzw. müssen auf der alten invis-Installation vorgenommen werden. Führen Sie die Updates am besten aus den Quellpaketen aus. RPM-Pakete werden sie für alle Zwischenschritte kaum bekommen.

Googlen Sie folgendes „owncloud upgrade“ nach und Sie finden eine Reihe von Anleitungen für die verschiedenen Versionssprünge. Eine kurze Zusammenfassung der Upgrade-Schritte finden Sie auch hier im Wiki.

Wenn Sie lediglich die Datenverzeichnisse migrieren möchten, gestaltet sich die Sache einfacher. Richten Sie die ownCloud-Neuinstallation einfach wie hier im Wiki beschrieben ein und Kopieren Sie die Daten wie im nachfolgenden Kapitel beschrieben.

## Daten wiederherstellen

Jetzt müssen Sie zunächst die Festplatte(n) der alten invis-Installation mit dem Server verbinden.

Hängen Sie jetzt der Reihe nach die alten Volumes ein und synchronisieren Sie Ihre Daten. Beginnen wir mit „/srv“. Das nachfolgende Beispiel geht davon aus, dass die alte Installation auf LVM basierte und gemäß der Anleitung hier im Wiki aufgebaut war.

```
invis:~ # mount /dev/system/srv /mnt
```

### Zarafa Attachments

Zunächst sollten die Attachments der alten Zarafa Installation synchronisiert werden. Mittel der Wahl ist das Tool ***rsync***:

```
invis:~ # rsync -av /mnt/zarafa/attachments/ /srv/kopano/attachments/
```

Achten Sie darauf, dass beide Pfadangaben mit einem Slash abgeschlossen werden. Die Option „-a“ (Archiv) sorgt dafür, dass klassische Zugriffsrechte erhalten bleiben und rekursiv in die zu synchronisierende Verzeichnisstruktur eingetaucht wird.

Danach sind die Besitzrechte der Attachment-Verzeichnisstruktur an Kopano anzupassen:

```
invis:~ # chown -R kopano.kopano /srv/kopano/attachments
```

### ownCloud und Dokuwiki Datenverzeichnisse

Synchronisieren Sie die Datenverzeichnisse wie bereits die Zarafa-Attachements:

#### ownCloud

```
invis:~ # rsync -av /mnt/www/htdocs/owncloud/data/
/srv/www/htdocs/owncloud/data/
```

#### Dokuwiki

```
invis:~ # rsync -av /mnt/www/htdocs/dokuwiki/data/
/srv/www/htdocs/dokuwiki/data/
```

### Fileserver Datenbestand

Beim Wiederherstellen des File-Server Datenbestandes ist auf zwei Dinge zu achten:

1. Die Freigabe „projekte“ wurde im Zuge der invis-Server Weiterentwicklung entfernt. Als Ersatz kommt entweder Die Freigabe „aktuell“ in Frage oder Sie legen über das invis-Portal eine Gruppe Namens „projekte“ an. Dabei wird unter „/srv/shares/gruppen“ ein Arbeitsverzeichnis namens „projekte“ angelegt, welches als Ersatz in Frage kommt. Dabei ist zu beachten, dass alle Benutzer die damit arbeiten sollen auch Mitglied der Gruppe „projekte“ sein müssen.
2. Je nach dem wie Sie vorher gearbeitet haben, sind zusätzlich zu den klassischen Unix Besitz- und Zugriffsrechten auch sogenannte POSIX-ACLs gesetzt. Diese dürfen bei der Datenübertragung nicht verloren gehen. Bei den Windows-Benutzer-Profilen beispielsweise sind definitiv POSIX-ACLs gesetzt.

Das Kopieren der Daten können Sie entweder bequem mit dem *Midnight Commander* (***mc***) oder besser mit ***rsync*** vornehmen. Dabei beherrscht ***rsync*** auch den fehlerfreien Umgang mit POSIX-ACLs. Das nachfolgende Beispiel zeigt die Datenmigration anhand der Profilverzeichnisse:

```
invis:~ # rsync -aHAXv /mnt/shares/profiles/ /srv/shares/profiles/
```

Die Optionen „HAX“ erhalten dabei Hardlinks, ACLs und erweiterte Dateiattribute. Gehen Sie auf gleiche Weise mit allen anderen Verzeichnissen Ihres Datenbestandes vor. Gleiches gilt für die Home-Verzeichnisse der alten Installation. Diese befinden sich, wenn Sie entsprechend der Anleitungen hier im Wiki installiert haben im Logical-Volume „/dev/system/home“.

### Weitere Daten

Aus dem Volume des /var-Verzeichnisses können Sie noch die Daten des Email-Abrufs synchronisieren. Die Daten sind zwar auch im Active-Directory enthalten, jedoch müssten alle Benutzer manuell wieder auf „Anwesend“ gesetzt werden. Ein Kopieren der Daten erübrigt dies.

Mounten Sie dazu das /var-Volume und kopieren Sie folgende Dateien:

```
invis:~ # cp /mnt/lib/cornaz/build/.fetchmailrc /var/lib/cornaz/build/
invis:~ # cp /mnt/lib/cornaz/inuse/.fetchmailrc /var/lib/cornaz/inuse/
```

## Abschluss

Damit ist die Migration abgeschlossen. Das einzige was zu tun bleibt ist die Festplatten der alten Installation vom Server zu trennen und idealerweise als Langzeit-Archiv im Tresor zu verstauen.

Wenn der Server in Betrieb ist, sollten Sie nicht vergessen für externe Zugriffe auf Server-Zertifikate von Let's Encrypt umzusteigen. Wie das funktioniert, ist **hier** beschrieben.

Viel Spaß mit Ihrem neuen invis-Server.