# Nacharbeit

Ist das Script abgearbeitet, folgt die Feinarbeit! Es gilt jetzt die auf dem Server installierte bzw. vorbereitete Software für deren Nutzung vorzubereiten.

## Router

Wenn Sie Ihren invis-Server hinter einem Router betreiben, müssen Sie darin bis zu 5 Portweiterleitungen einrichten, wenn Sie Ihren invis-Server auch via Internet nutzen möchten.

Diese sind:

1. der vom invis Server genutzte „verschobene“ SSH-Port (TCP)
2. Port 443/TCP (HTTPs), wenn Sie ActiveSync/Z-Push nutzen möchten, um Mobilgeräte mit der Groupware des Servers zu synchronisieren.
3. der vom invis Server genutzte „verschobene“ HTTPs-Port (TCP) für den Zugriff auf das invis-Portal.
4. der vom invis Server genutzte „verschobene“ HTTPs-Port (TCP) für den Zugriff auf ownCloud.
5. Port 1194/UDP für den Zugriff via OpenVPN.

Die hier als „verschoben“ bezeichneten Ports wurden von ***sine*** zufällig generiert und während des Setups ausgegeben. Nachträglich Abfragen können Sie sie auf der Kommandozeile mit:

```
linux:~ # sine showconf
```

## Passwortsicherheit

Mit Samba4 als AD Domaincontroller gelten folgende Voreinstellung für Laufzeit und Sicherheit der Benutzerpasswörter:

| **Einstellung** | **Vorgabe** |
|---|---|
| max. Passwortlaufzeit | 43 Tage |
| Passwortkomplexität | aktiviert |
| min. Passwortlänge | 7 Zeichen |

Diese Voreinstellungen sind recht streng und können so sicherlich nicht überall Anwendung finden. Sie, als Administrator eines invis-Servers sollten sich von Ihren Anwendern aber nicht allzu viele Zugeständnisse in Sachen Passwortsicherheit abringen lassen.

Ändern lassen sich die Einstellungen mit Hilfe des ***samba-tools*** auf der Kommandozeile des Servers. Hier ein paar Beispiele:

#### Ändern der Passwortlaufzeit

```
linux:~ # samba-tool domain passwortsettings set --max-password-age=0
```

Der im Beispiel gewählte Wert **0** sorgt für eine unbegrenzte Passwortlaufzeit. Ist sicherlich nicht die beste Empfehlung, wird in der Praxis zur Stressvermeidung häufig bevorzugt.

**Passwortkomplexität**

```
linux:~ # samba-tool domain passwortsettings set --complexity=off
```

Hier kennt die Microsoft'sche Welt aus der das AD ja stammt keine Abstufungen. Möglich sind die Werte *on*, *off* und *default* wobei *default* wiederum *on* bedeutet.

Mit der Voreinstellungen werden Passwörter mit Sonderzeichen, Zahlen und Groß-/Kleinschreibung verlangt.

**Passwortlänge**

```
linux:~ # samba-tool domain passwortsettings set --min-pwd-length=5
```

Reduziert die geforderte Passwortlänge auf 5 Zeichen.

Als Benutzer **root** haben Sie natürlich die Möglichkeit Benutzerpasswörter zurückzusetzen. Dabei gelten nicht einmal die Passwortsicherheitsregeln.

```
linux:~ # samba-tool user setpassword benutzername --
newpassword=neuespasswort --must-change-next-login
```

Im gezeigten Beispiel wird dafür gesorgt, dass der betroffene Benutzer sein Passwort bei der nächsten Anmeldung ändern muss.

# NFS Fileserver

Der NFS Fileserver für Linux-Clients ist nach der Installation des invis-Servers zwar vorbereitet, wird aber nicht automatisch gestartet. Um dies Nachzuholen sind folgende Schritte durchzuführen:

Die Dienste „nfsserver“ und „rpcbind“ zum automatischen Start vorsehen und starten:

```
linux:~ # systemctl enable nfsserver.service
linux:~ # systemctl start nfsserver.service
linux:~ # systemctl enable rpcbind.service
linux:~ # systemctl start rpcbind.service
```

Anschliessend ist noch der Zugriff auf die NFS-Freigaben in der Firewall, für die interne Netzwerk-Schnittstelle zu öffnen.

Dazu ist in Datei

```
/etc/sysconfig/SuSEfirewall2
```

ist in Zeile (ca.) 414 folgendes zu ergänzen:

Aus:

```
FW_CONFIGURATIONS_INT="samba-4-ad"
```

wird

```
FW_CONFIGURATIONS_INT="nfs-kernel-server samba-4-ad"
```

Danach ist noch die Firwall neu zu starten:

```
linux:~ # systemctl restart SuSEfirewall2.service
```

Grund dafür, dass wir dies nicht automatisch ausführen ist, dass es nur in den wenigsten Fällen Linux Clients gibt (leider).

# ownCloud

***Hinweis:*** *ownCloud lässt sich nur dann sinnvoll einsetzen, wenn es sowohl aus dem lokalen Netz wie auch aus dem Internet über die gleiche URL erreichbar ist. Voraussetzung dafür ist, dass Ihr invis-Server entweder über eine feste IP-Adresse oder einen gültigen DDNS Namen erreichbar ist. Ist diese Bedingung nicht erfüllt, ist es nicht möglich, dass Sie aus dem lokalen Netzwerk eine Datei oder ein Verzeichnis in ownCloud für dritte im Internet freigeben. ownCloud würde dann eine URL erzeugen, die niemals via Internet erreichbar wäre.*

Während der ownCloud-Installation durch ***sine*** wird ownCloud grundsätzlich installiert, eine leere Datenbank angelegt und die Firewall vorbereitet. Im Anschluss daran muss die Setup Routine von ownCloud selbst durchlaufen werden und das LDAP-Plugin aktiviert und konfiguriert werden.

Sie benötigen dafür das Passwort, welches ***sine*** Ihnen mitgeteilt hat. Beim ersten Zugriff auf ownCloud startet die Setup-Routine automatisch.

Legen Sie zunächst die Zugangsdaten für das ownCloud Administrationskonto fest.

Klicken Sie jetzt auf „Speicher & Datenbank“ und wählen Sie dort als Datenbank-Typ „MySQL/MariaDB“ aus und geben Sie die Zugangsdaten zur vorbereiteten Datenbank ein:

- **Host:** localhost
- **Datenbank:** owncloud
- **Datenbank-Benutzer:** owncloud
- **Passwort:** Das von sine generierte Passwort

Melden Sie sich jetzt mit dem zuvor definierten Adminitrationskonto an ownCloud an. Klicken Sie dann auf den Pulldown Pfeil oben rechts und dann auf „Administration“.

Klicken Sie jetzt links am oberen Rand auf den Eintrag „Apps“ und dann auf das Pluszeichen. Klicken Sie als nächstes auf den Menüeintrag „Nicht aktiviert“. Aktivieren Sie aus der Liste nicht aktivierter Apps den Eintrag „LDAP user and group backend“ und melden Sie sich daraufhin einmal ab und wieder an.

Jetzt finden Sie unter „Administration“ den Eintrag „LDAP“. Dort können Sie ownCloud schrittweise an

Ihr Active Directory anbinden.

Im ersten Schritt müssen Sie die Zugangsdaten zum LDAP Server angeben:

- **Host:** ldaps://localhost
- **Port:** 636
- **Bind-DN:** ldap.admin@invis-net.loc (Ersetzen Sie die Domäne durch Ihre lokale Domäne)
- **Bind-Passwort:** Das Password für das „ldap.admin“ Konto können Sie sich mit „sine showconf“ anzeigen lassen.
- **Base-DN:** dc=invis-net,dc=loc (Ersetzen Sie die Domänenbestandteile durch die Ihrer lokalen Domäne)

***Hinweis:*** *ownCloud überprüft die Eingaben sofort. Wenn Sie also einen Fehler bei der Konfiguration machen wird dies unmittelbar angezeigt.*

Auf der zweiten Seite der Konfiguration „Nutzer-Filter“ können Einschränkungen dafür vorgenommen werden welche Benutzerkonten von ownCloud im LDAP gefunden werden. Hier sind folgende Angaben zu machen:

- **Nur diese Objekt-Klassen:** person
- **Nur von diesen Gruppen:** Lassen Sie dieses Feld leer, wenn alle invis-Nutzer auch ownCloud nutzen dürfen oder wählen Sie eine Gruppe, aus um

Logins auf die Mitglieder dieser Gruppe(n) zu beschränken. Praktischerweise sollte für diesen Zweck eine eigene Gruppe angelegt werden.

Leider macht ownCloud bei der Umsetzung dieser Angaben in eine Filterregel einen Fehler. Dies lässt sich korrigieren in dem Sie auf den Link „bearbeiten klicken und die dann angezeigte Zeile gemäss folgendem Beispiel abändern:

```
(&(|(objectclass=person))(|(memberof=CN=owncloud,CN=Users,DC=invis-
net,DC=loc)))
```

In Schritt drei „Anmeldefilter“ können Sie die Vorgabe „LDAP-Benutzername“ einfach beibehalten. Die Anmeldung erfolgt dann mit dem Login-Namen ohne angehängte Domain.

Im letzten Schritt legen Sie die Gruppen fest, die von ownCloud im LDAP gefunden und verwendet werden können. Hier sind folgende Angaben zu machen:

- **Nur diese Objekt-Klassen:** group
- **Nur diese Gruppen:** Lassen Sie das Feld leer wenn alle Gruppen der Domäne gefunden werden sollen oder wählen Sie die Gruppen aus, auf die Sie ownCloud beschränken möchten.

Damit ist die LDAP bzw. Active Directory Anbindung abgeschlossen und ownCloud bereit zur Nutzung. Einen echten Nutzen hat es natürlich nur dann, wenn Ihr Server über einen DDNS-Namen via Internet erreichbar ist.

# Tine 2.0 einrichten (experimentell)

Um Tine 2.0 nach der Grundinstallation zur Mitarbeit zu bewegen, sind einige manuelle Arbeitsschritte notwendig.

Starten Sie damit, dass Sie im Browser folgende Adresse öffnen:
http://ihrserver.domain.tld/tine20/setup.php

Sie können Sich hier mit folgenden Zugangsdaten anmelden:

***Benutzername:*** tine20setup
***Passwort:*** zufallsgeneriert

Das Passwort wurde im Verlauf der Server-Instalaltion von ***sine*** ausgegeben.

Die weitere Einrichtung von Tine 2.0 erfolgt in mehreren Schritten:

1. Akzeptieren der Lizenz- und Datenschutzbedingungen
2. Überprüfen der Systemvoraussetzungen
3. Anpassen der Tine 2.0 Konfigurationsdatei
4. Einrichten der Benutzerverwaltung
5. Einrichten der Mailserver-Anbindung
6. Verwaltung der Tine 2.0 Einzelanwendungen

Die Punkte 1 und 2 dürften keiner weiteren Erläuterungen bedürfen.

**Punkt 3** „Anpassen der Konfigurationsdatei“ erfordert eigentlich auch keine manuellen Eingriffe. Allerdings können Sie hier das Passwort des Setup-Benutzers nach eigenem Wunsch neu setzen. Ansonsten können Sie hier die Datenbankanbindung, das Logging-Verhalten und weitere „Kleinigkeiten“ einstellen. Sie finden die Konfigurationsdatei „config.inc.php“ in:

```
/var/lib/tine20/webroot
```

Sie können Sie auch manuell im Editor bearbeiten.

## Tine 2.0 Benutzerverwaltung und -authentifizierung

Diesem Punkt (4) ist große Aufmerksamkeit zu widmen, hier binden Sie Tine 2.0 an die Benutzerverwaltung des Active-Directories an.

Unterteilt ist dieser Abschnitt wiederum in mehrere Unterkategorien:

- Festlegen des Administrativen Benutzers (Initialer Admin-Benutzer)
- Benutzerauthentifizierung (Auhtentifizierungsdienst)
- Benutzerverwaltung (Speicherort der Benutzerkonten)
- Passworteinstellungen
- Weiterleitungseinstellungen

Vor allem die Abschnitte 2 und 3 müssen auf Ihre Active-Directory Umgebung angepasst werden. Konfigurieren Sie diese Abschnitte wie Nachfolgend beschrieben:

### Admin-Benutzer

Sie **müssen** hier einen Tine 2.0 Administrator einrichten. Dieses Konto wird **nicht** im Active-Directory sondern in Tines Datenbank gespeichert. Wählen Sie nach Belieben einen Benutzernamen und ein ausreichend komplexes Passwort. D.h. Verwenden Sie auf Zahlen und Sonderzeichen und nicht weniger als 7 Zeichen. Die genauen Regeln kennen wir noch nicht. Zu einfache Passwörter werden hier zwar angenommen, das Konto wird jedoch nicht angelegt. Ohne einen Tine 2.0 Admin können Sie das Setup nicht beenden.

Geht hier etwas schief, können Sie das Anlegen des Benutzers auf der Kommandozeile wiederholen:

```
linux:~ # php /usr/share/tine20/setup.php --create_admin
```

***Hinweis:*** *Es ist kein Fehler sich mal anzuschauen, was das Script „setup.php“ auf der Kommandozeile so alles kann.*

### Authentifizierungsdienst

Ziel dieses Schrittes ist es, Benutzeranmeldungen an Tine 2.0 über das Active Directory durchzuführen. Hierzu benötigen Sie die zunächst den DN und das Passwort des invis-Server LDAP-Admins.

Das Passwort finden Sie in

```
/etc/invis/invis-pws.cfg
```

Füllen Sie die nachfolgend gezeigten Konfigurationsfelder entsprechend Ihrer Umgebung durch:

- **Backend:** LDAP
- **Host:** Tragen Sie hier den voll qualifizierten Namen (FQDN) Ihres invis-Servers ein.
- **Loginname:** Hier tragen Sie den Distinguished Name (DN) des LDAP Admins ein z.B.: CN=Admin LDAP,CN=Users,DC=domain,DC=tld (Sie müssen lediglich „domain“ und „tld“ an Ihre Umgebung anpassen.)
- **Kennwort:** Das ermittelte Passwort des LDAP-Admins
- **Verbindung benötigt DN:** ja
- **Start TLS verwenden:** ja
- **Base DN:** Die Wurzel Ihres LDAP-Verzeichnisses: „DC=domain,DC=tld“ (angepasst an Ihre Umgebung.)
- **Suchfilter:** samaccountame=%s (Achten Sie auf genaue Schreibweise, ein Fehler hier und niemand kann sich an Tine anmelden.)
- **Kanonische Form der Benutzerkonten:** ACCTNAME_FORM_USERNAME
- **Kontodomänenname:** Ihre lokale Domain in der Schreibweise „domain.tld“
- **Account domain short name:** Wie oben nur ohne Top-Level-Domain

### Benutzerverwaltung

Die Konfiguration des Speichers der Benutzerkonten erfordert ähnlich Angaben, wie die der Authentifizierung. Geben Sie zu den nachfolgend gezeigten Eingabefeldern die erforderlichen Daten, angepasst an Ihre Umgebung an:

- **Backend:** ActiveDirectory
- **Host:** Tragen Sie hier den voll qualifizierten Namen (FQDN) Ihres invis-Servers ein.
- **Loginname:** Hier tragen Sie den Distinguished Name (DN) des LDAP Admins ein z.B.: CN=Admin LDAP,CN=Users,DC=domain,DC=tld (Sie müssen lediglich „domain“ und „tld“ an Ihre Umgebung anpassen.)
- **Kennwort:** Das ermittelte Passwort des LDAP-Admins
- **Verbindung benötigt DN:** ja
- **Start TLS verwenden:** ja
- **Benutzer-DN:** CN=Users,DC=domain,DC=loc (Domain und top-Level-Domain natürlich an Ihre Umgebung angepasst.)
- **Benutzerfilter:** objectclass=person
- **Benutzersuche-Bereich:** SEARCH_SCOPE_SUB
- **Gruppen-DN:** CN=Users,DC=domain,DC=loc (Domain und top-Level-Domain natürlich an Ihre Umgebung angepasst.)
- **Benutzerfilter:** objectclass=group
- **Benutzersuche-Bereich:** SEARCH_SCOPE_SUB
- **RFC-2307-Attribute beibehalten:** ja
- **Minimale Benutzer-ID:** 20000 (invis-Server UID-Nummern beginnen bei 20000)
- **Maximale Benutzer-ID:** 30000 (Mehr als 10000 Benutzer wird es auf invis-Servern wohl kaum geben)
- **Minimale Gruppen-ID:** 20000 (invis-Server GID-Nummern beginnen bei 20000)
- **Maximale Gruppen-ID:** 30000 (Mehr als 10000 Gruppen wird es auf invis-Servern wohl kaum geben)
- **UUID Attribut von Gruppen:** & **UUID Attribut von Benutzern:** objectGUID
- **Standard Benutzergruppenname:** tine20 (oder „Domain Users“, je nachdem ob Sie den Zugriff auf definierte Benutzer beschränken möchten)
- **Standard Admin-Gruppennamen:** Domain Admins
- **Nur lesender Zugriff:** ja

Bezüglich des letzten Punktes empfehlen wir hier einen rein lesenden Zugriff auf das Active-Directory, da die eigentliche Benutzerverwaltung über das invis-Portal erfolgen soll. Allerdings sind unsere diesbezüglichen Experimente noch nicht abgeschlossen.

### Passworteinstellungen

Diese Einstellungen können Sie an und für sich nach eigenem Ermessen vornehmen. Sie sollten jedoch darauf achten, dass die hier getroffenen Einstellungen nicht mit den Einstellungen des Active Directory konkurrieren.

Wir empfehlen allerdings auch hier darauf zu verzichten die Groupware zur Verwaltung Ihre Server-Benutzer zu verwenden. Wenn Sie unserer Empfehlung folgen möchten, stellen Sie den Wert **Benutzer kann Passwort ändern** auf „nein“.

### Weiterleitungseinstellungen

Auch hier können Sie nach eigenem Ermessen vorgehen. Uns fehlen hier derzeit noch die Erfahrungen um Empfehlungen aussprechen zu können.

… to be continued.

## VPN-Clients einrichten

Nach Durchlauf des Setup-Scripts ***sine*** ist OpenVPN vollständig konfiguriert und bereits gestartete.

Testen können Sie dass mit:

```
linux:~ # ifconfig vpn
```

Bekommen Sie eine positive Antwort, läuft OpenVPN.

Um Clients anzubinden müssen Sie Client-Zertifikate und OpenVPN Client-Konfigurationen erzeugen.

Das Erzeugen der Zertifikatsdateien wird seit invis-Server 11.0 mittels des Scripts ***inviscerts*** vorgenommen.

… to be continued.

## z-push konfigurieren

„z-push“ ist eine von Zarafa entwickelte Open-Source ActiveSync Implementation. Sie ermöglicht es Mobilgeräte mit Zarafa, aber auch Tine 2.0 zu synchronisieren. Weiterhin kann auch Outlook via ActiveSync an Zarafa angebunden werden.

Die Nacharbeit hier beschränkt sich auf das Eintragen der korrekten Zeitzone in die z-push Konfigurationsdatei:

```
/srv/www/htdocs/z-push2/config.php
```

```
...
define('TIMEZONE', 'Europe/Berlin');
...
```