Nacharbeit

Ist das Script abgearbeitet, folgt die Feinarbeit! Es gilt jetzt vor allem Group-e und LX-Office für die Nutzung vorzubereiten.

Auch wenn ich diesen Bereich des Howtos so schnell es geht fortsetze, empfehle ich bei Problemen mit den beiden Programmen die zugehörigen Foren und Wikis.

Ich werde bei der Dokumentation der Ersteinrichtung der beiden Programme hier nur das Wesentliche erläutern, da beide Programme immer wieder kleineren und größeren Änderungen unterliegen.

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

Hinweis: *Die nachfolgenden Erläuterungen beziehen sich ausschließlich auf invis Server Active Directory und* ***nicht*** *auf invis Server Classic.*

Wird Samba4 als AD Domaincontroller betrieben gelten folgende Voreinstellung für 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).

Group-e

Um Group-e nach der Installation in einen nutzbaren Zustand zu bekommen, müssen Sie sich zunächst mit dem Benutzernamen „config“ und gleichlautendem Passwort an Group-e anmelden.

Zunächst werden Sie aufgefordert die Datenbank an die aktuelle Version der Software anzupassen. Sie benötigen dafür das Passwort des MySQL-Benutzers „root“ welches Sie im Verlauf des invis Setup-Scripts festgelegt haben.

Ist die Datenbank aktualisiert, zeigt Ihnen Group-e einen Installations-Check. Hier sehen Sie wo noch nachgearbeitet werden muss. In erster Linie ist dies die Anpassung an die bestehende LDAP-Struktur.

Den Status „BAD“ werden Sie vermutlich bei folgenden Punkten *ldap_bind* und folgenden, *cyrus_login*, *mkntpwd* und *php_mhash* sehen. Die beiden letzen Punkt sind schnell abgehakt. Das Tool *mkntpwd* ist inzwischen aus den meisten Linux-Distributionen verschwunden, dieser Fehler kann also entweder ignoriert werden oder in Sie entfernen in der „Globalen Konfiguration“ einfach den Eintrag im Feld „NT Password Command“.

Klicken Sie zunächst auf den Reiter „User Defaults“ und wählen Sie (so Sie dies möchten) als Standard-Sprache „de“ für deutsch aus. Konfigurationsänderungen sind unmittelbar nach dem Speichern wirksam.

Klicken Sie für die Anpassung an die LDAP-Umgebung auf den Reiter „Konfiguration“. Dort sind die folgenden Felder wie hier gezeigt anzupassen:

- **Mindestlänge Benutzername:** Diesen Wert setze ich auf 3, da invis Server einen User namens „fax“ kennen.
- **Passwörter nicht verwalten:** Diesen Punkt aktiviere ich, da Passwörter über das invis Protal verwaltet werden.

- **Virenscanner Kommando:** Die Vorgabe bezieht sich auf den Virenscanner „fprot“. Da invis-Server entweder mit clamav oder antivir arbeiten muss diese Zeile an den verwendeten Scanner angepasst werden. Für ***antivir*** könnte das Kommando so aussehen:

```
avscan --allfiles --scan-in-archive -q --moveto=/var/spool/infected %s
```

Weiterhin müssen die Exitcodes für infizierte und verdächtige Dateien angepasst werden. Diese sind bezogen auf ***antivir*** : **1** für infizierte Dateien und **3** für verdächtige Dateien.

Für ***clamscan*** kann eine entsprechende Zeile wie folgt aussehen:

```
clamscan --quiet --scan-archive=yes --move==/var/spool/infected %s
```

Bei Verwendung von ClamAV ist zu beachten, das ***clamscan*** keinen Exitcode für „verdächtige“ Dateien kennt. Der Exitcode für infizierte Dateien ist **1**

- **Ldap BaseDN:** dc=deine-domain,dc=loc (Selbstverständlich an Ihre Umgebung angepasst)
- **Ldap Admin Bind:** uid=admin,dc=deine-domain,dc=loc
- **Ldap Admin Password:** Das zugehörige Passwort
- **Ldap BaseDN User:** ou=Users,ou=Benutzerverwaltung
- **Ldap BaseDN Groups:** ou=Groups,ou=Benutzerverwaltung
- **Ldap DN for sambaUnixIdPool Object:** sambaDomainName=DEINE-DOMAIN,ou=Benutzerverwaltung,dc=deine-domain,dc=loc
- **Samba Server Name:** Der NetBIOS-Name des Samba-Servers, meist der Hostname in Großbuchstaben.
- **Samba HomeDrive:** Auf invis Servern ist U: als Laufwerksbuchstabe für das Home-Laufwerk vorgegeben. H: kollidiert des öfteren mit fest eingebauten Card-Readern.
- **Samba HomePath:** \\{Server}\{USERNAME} – Die Vorgabe sollte es allerdings auch tun.
- **Samba ProfilePath:** \\{SERVER}\profiles\{USERNAME} – Hier fehlen in der Vorgabe ein paar Backslashes
- **Ldap BaseDN Samba:** sambaDomainName=DEINE-DOMAIN,ou=Benutzerverwaltung

Speichern Sie Ihre Anpassungen ab. Danach sollte Group-e sich mit dem lokalen LDAP-Server vertragen, wie ein erneutes Klicken auf den „Install Check“ beweisen sollte. Jetzt können Sie dort die Gruppe „All“ und den Group-e Admin-Account „sysadmin“ (in dieser Reihenfolge) anlegen.

Klicken Sie zur Anpassung an den IMAP-Server erneut auf den Reiter „Konfiguration“ und anschließend links auf den Link „E-Mail“. Hier muss nicht viel eingestellt werden. Da der IMAP-Dienst des invis-Servers eine verschlüsselte Verbindung fordert muss die Einstellung für den IMAP Port geändert werden.

- **Port:** 143/tls/novalidate-cert – Der Eintrag novalidate-cert ist notwendig, da Group-e ansonsten selbstsignierte Zertifikate nicht akzeptiert.

Des weiteren muss noch das Passwort des Users „cyrus“ angegeben werden, da Group-e in der Lage ist die Mailkonten der User zu verwalten.

- **Admin Passwort:** ihr cyrus Passwort – Sie haben es während des Script-Laufs festgelegt.

Gelegentlich gibt es Probleme mit dem IMAP-Namensraum, wenn neben dem Group-e Webmailclient noch ein Standalone-Mailclient wie etwa Thunderbird verwendet wird. So tauchen meist mehrere „Gesendet“-Ordner auf. Um dies in den Griff zu bekommen müssen Sie ein wenig mit den Mailbox-

Bezeichnungen spielen. Ich warte hier erst mal auf die nächste Version von Group-e.

Es emphielt sich etwa für den Versand größerer Mail-Anhänge die PHP-Werte für *memory_limit*, *post_max_size* und *max_upload_filesize* zu vergrößern. In meiner Praxis haben sich Werte von 256M, 64M und 32M bewährt. Wichtig dabei ist, dass der Wert für *post_max_size* doppelt so groß wie *max_upload_filesize* ist.

Was die Grundkonfiguration der weiteren Group-e Applikationen angeht überlasse ich Sie zunächst auch sich selbst und Ihrem Spieltrieb. Ich habe allerdings auch nichts dagegen, wenn andere Nutzer sich hier am Wiki beteiligen und Tipps geben.

Nach Abschluss der Grundkonfiguration können Sie sich an Group-e als User „sysadmin“ anmelden und über das „Admin“ Icon Group-e weiter einrichten. Es gilt zunächst Ihre System-User für die Nutzung von Group-e einzurichten. Klicken Sie dazu auf die einzelnen User-Einträge, tragen Sie deren **interne** email-Adresse - username@deine-domain.loc - ein und klicken Sie die Checkbox „Group-e User aktiv“ an. Jeder Group-e User muss mindestens einer Group-e Gruppe angehören, da es derzeit aus Sicht von Group-e nur die Gruppe „all“ gibt wählen Sie diese in der Drop-Down-Liste „Primärgruppe“ aus.

Klicken Sie jetzt noch im Feld „Applikationen“ auf alle Checkboxen der Applikationen die dem User zur Verfügung stehen und speichern Sie Ihre Einstellungen ab. Damit kann sich der betreffende User an Group-e anmelden und es nutzen.

Um alle Applikationen richtig nutzen zu können, ist noch einiges an Feinschliff notwendig. Auch hierbei überlassen ich Sie Ihrem Spieltrieb und verweise auf Forum und Wiki unter http://www.group-e.info.

Kivitendo

Wie auch Group-e, ist Kivitendo nach erfolgreichem Script-Lauf bereits auf dem zukünftigen invis-Server vorinstalliert. Die anfallende Nacharbeit beschränkt sich auf das Anlegen von Datenbanken, Benutzer, Gruppen und Mandanten.

Eine Umfangreiche Dokumentation zu Kivitendo finden Sie hier:
https://steigmann.kivitendo-premium.de/doc/html/

Um die Kivitendo Nutzerdatenbank, Mandanten-Datenbanken sowie Nutzerkonten anlegen zu können, müssen Sie zunächst im Browser die Administrationsseite aufrufen. Der entsprechende Link sieht wie folgt aus:

http://ihr-server.domain.loc/kivitendo-erp/admin.pl

Sind weder Datenbanken noch Nutzerkonten eingerichtet, genügt ein Klick auf die Schaltfläche „Warenwirtschaft“ im invis-Portal. Kivitendo fragt dann selbständig, ob Sie zunächst auf die Administrationsseite wechseln möchten.

Das zunächst erfragte Administratoren-Passwort lautet schlicht: **„admin123“**. Kivitendo führt Sie anschliessend durch die Installation einer Authentifizierungsdatenbank. Folgen Sie hier einfach den Anweisungen. Als Benutzer zum Anlegen der Datenbank können müssen Sie wie vorgeschlagen den User „kivitendo“ verwenden. Für letzteren benötigen Sie selbstverständlich das von Ihnen vergebene Passwort.

Möchten Sie statt gegen eine interne Kivitendo Benutzerdatenbank, gegen ein LDAP-Verzeichnis (OpenLDAP oder Active Directory) Authentifizieren, müssen Sie vor dem Anlegen der Benutzerdatenbank in der Datei

```
/srv/www/htdocs/kivitendo/config/kivitendo.conf
```

folgende Änderungen vornehmen:

Classic & AD

```
# Which module to use for authentication. Valid values are 'DB' and
# 'LDAP'.  If 'LDAP' is used then users cannot change their password
# via kivitendo.
module = LDAP
```

Weiterhin ist der LDAP-Server zu konfigurieren. Hier unterscheiden sich Classic und AD geringfügig voneinander:

Classic

```
host          = 127.0.0.1
port          = 389
tls           = 1
attribute     = uid
base_dn       = DC=invis-net,DC=loc
filter        =
bind_dn       = uid=admin,ou=Benutzerverwaltung,dc=invis-net,dc=loc
bind_password = ldap-admin-secret
```

AD

```
host          = 127.0.0.1
port          = 389
tls           = 1
attribute     = sAMAccountName
base_dn       = DC=invis-net,DC=loc
filter        =
bind_dn       = ldap.admin@invis-net.loc
bind_password = ldap-admin-secret
```

Selbstverständlich müssen Sie die Konfigurationsdaten an Ihre Umgebung anpassen.

Steht die Authentifizierungsdatenbank, gelangen Sie auf die eigentliche Administrationsseite.

Sie müssen jetzt eine (oder auch mehrere) Mandantendatenbanken anlegen.

Klicken Sie hier im ersten Schritt auf die Schaltfläche „Datenbankadministration“ und geben Sie in den Feldern für Benutzer und Passwort wiederum die Zugangsdaten des PostgreSQL-Benutzers „kivitendo“ ein. Bestätigen Sie Ihre Eingabe durch Drücken der Schaltfläche „Datenbank anlegen“.

In der darauf folgenden Maske müssen Sie einen Datenbanknamen vergeben - dieser sollte Sinn

ergeben, beispielsweise durch einfügen des Mandantennamens - und sich für einen Kontenrahmen entscheiden. Die Vorgabe SK03 sollte in den meisten Fällen passen. Klicken Sie auf die Schaltfläche „Weiter“. Auf der nächsten Seite werden Sie über Erfolg oder Misserfolg der Aktion informiert. Geht alles glatt, gelangen Sie mit der Schaltfläche „Weiter“ zurück zur Administrationsseite.

Jetzt müssen Sie passend zur Mandantendatenbank noch den „Mandantenbenutzer“ anlegen. Klicken Sie dazu auf die Schaltfläche „Benutzer erfassen“ und füllen Sie das Formular „nach bestem Wissen und Gewissen“ aus.

In der Sektion Datenbank füllen Sie die Felder wie folgt aus:

- **Datenbankcomputer:** localhost
- **Datenbank:**: Der Name Ihrer soeben angelegten Mandantendatenbank
- **Port:** 5432
- **Benutzer:** kivitendo
- **Passwort:** Das zugehörige Passwort

Testen Sie auf jeden Fall vor dem Speichern der Eingaben die Verbindung zur Datenbank über die entsprechende Schaltfläche.

Mit den Eingabefeldern auf der rechten Bildhälfte können Sie unter anderem das „Look & Feel“ von Kivitendo in gewissem Umfang beeinflussen. Damit müssen Sie einfach experimentieren.

Ich empfehle ohnehin jedem Anwender sich zunächst eine Testdatenbank mit zugehörigem Testmandanten zu erstellen, um sich mit der Software vertraut zu machen. Ein ERP-System ist etwas ganz anderes als etwa ein Textverarbeitungsprogramm.

Mit der Schaltfläche „Speichern“ gelangen Sie wieder zurück zur Administrationsseite.

Wenn Sie den „Mandantenbenutzer“ angelegt haben müssen Sie diesen über die Schaltfläche „Gruppen bearbeiten“ noch mit Zugriffsrechten auf die Mandantendatenbank versorgen.

Nach einer noch jungfreulichen Neuinstallation existiert lediglich die Gruppe „Vollzugriff“, was in einfachen Umgebungen durchaus ausreicht. Klicken Sie die Gruppe im oberen Fenster an und anschließend auf die Schaltfläche „Bearbeiten“. Es öffnet sich eine neue Seite. In der oberen Sektion der Seite sind zwei mit „Benutzer in dieser Gruppe“ und „Benutzer nicht in dieser Gruppe“ bezeichnete Felder. Ihren neuen Benutzer sehen Sie im rechten Feld. Klicken Sie diesen Eintrag an und anschließend auf die Schaltfläche „Zu Gruppe hinzufügen“.

Über die Schaltfläche „Zurück“ sichern Sie Ihre Eingaben. Jetzt können Sie sich erstmalig mit Ihrem neuen Benutzer über die entsprechenden Felder an Kivitendo anmelden. Zukünftig gelangen Sie über die Schaltfläche „Warenwirtschaft“ im invis Portal direkt zur Kivitendo Benutzeranmeldung.

Kivitendo Taskserver

Seit Version Kivitendo Vorgänger LX-Office in Version 2.6.3 ist in der Software einen Taskmanager-Dienst zur Erinnerung an anstehende Aufgaben bzw. für Wiedervorlagen. Dieser Dienst ist bereits ins Runlevel-Konzept des Servers integriert, kann aber ohne Datenbank bez. angelegten Benutzer nicht starten.

Ist die Datenbank, wie oben beschrieben angelegt, muss in der Datei

```
/srv/www/htdocs/kivitendo-erp/config/kivitendo.conf
```

in der Rubrik **[task_server]** (ab Zeile 235) unter „login =“ ein Benutzer mit vollen Rechten eingetragen werden.

Danach kann der Tastserver mit:

```
linux:~ # systemctl start kivitendo-task-server.service
```

gestartet werden.

Hinweis: *Kivitendo ist eine sehr komplexe Software, für die wir als Projekt „invis Server“ keinen Support leisten. Wenden Sie sich, wenn Sie Hilfe benötigen bitte direkt an Forum bzw. Wiki des Kivitendo Projekts. Für Kivitendo können Sie auch kommerziellen Support erhalten, wenden Sie sich diesbezüglich an eines der Kivitendo-Partner Unternehmen: http://www.kivitendo.de/partner.html*

ownCloud

Ab invis-Server Active Directory 10.1 Rev. 21

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:** localhost
- **Port:** 389
- **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.

Fax-Server

Hinweis: *Wir werden die Pflege des Fax-Server-Moduls über kurz oder lang einstellen. Geschuldet ist dies der ISDN Deaktivierung durch die Telekom, der Tatsache, dass AVM die Fritzcard nie als PCIeX Karte heraus gebracht hat und, dass es die FCPCI-Treiber auch nicht bis in alle Ewigkeit geben wird.*

Die Nacharbeit am Fax-Server beschränkt sich auf die Konfiguration des Fax-Anschlusses sowie der Drucker-Installation auf den Clients.

Der erste Teil lässt sich am Server bequem per YaST erledigen - ein eigenes Web-Frontend, vergleichbar mit corNAz, ist zwar angedacht aber noch nicht in die Tat umgesetzt. (Freiwillige Helfer sind uns sehr willkommen.)

Starten Sie einfach auf der Kommandozeile „yast“

```
Kommandozeile: yast
```

und wechseln Sie im Hauptmenü auf den Eintrag „Network Devices“ und im entsprechenden Untermenü auf der rechten Seite auf „Fax“ und bestätigen Sie mit Enter.

Fügen Sie jetzt mit der Tastenkombination „Alt+A“ für „Add“ einen neuen Eintrag hinzu. Füllen Sie die Felder wie folgt aus:

- **User:** Der Username des Faxnutzers, im Singleuser-Mode ist dies einfach „fax“
- **Fax Numbers:** sind die MSNs auf denen eingehende Faxe erwartet werden, also schlicht Ihre Faxnummer ohne Vorwahl. Mehrere MSNs werden durch Kommata getrennt eingegeben. Wenn Sie zusätzlich ein Papierfax verwenden sollten Sie darauf achten, das Fax-Server und Faxgerät nicht auf der gleichen MSN lauschen.
- **Outgoing MSN:** Die Nummer (ohne Vorwahl) unter der Faxe versand werden.
- **Station ID:** ist Ihre Faxnummer in internationaler Schreibweise, also etwa “+49 6403 1234567„
- **Headline:** ist der Tex, der immer am oberen Rand eines Faxes auftaucht, also etwa Ihr Firmenname.
- **Action:** Dies können Sie auf der Vorgabe „MailandSafe“ belassen, was dafür sorgt das eingehende Faxe auf dem Server im SFF-Format gespeichert und im PDF-Format per Mail an den Empfänger versand werden.

Wenn Sie den Fax-Server im Multiuser-Mode an einem ISDN-Anlagenanschluss betreiben, müssen Sie für jeden Empfänger einen solchen Eintrag erzeugen und bei den Feldern „Fax Numbers“ und „Outgoing MSN“ anstelle der so genannten „MSN“ die entsprechende „EAZ“ Nummer eingeben. Die EAZ ist schlicht die jeweilige Durchwahlnummer.

Hinweis: *Wenn Sie im YaST-Untermenü genau hingeschaut haben, sollte Ihnen der Eintrag „Phone Answering Machine“ aufgefallen sein, darüber können Sie auf die gleiche Weise einen ISDN-Anrufbeantworter einrichten.*

Auf Windows-Clients muss zur Nutzung des Fax-Versands noch der Faxgate-Drucker installiert werden. (Linux-Clients können diesen ohne weitere Installation nutzen, sowie sie generell als CUPS-Clients eingerichtet sind.) Klicken Sie sich nach dem Domänenbeitritt des Windows-Clients durch die Netzwerkumgebung bis auf den invis-Server und klicken Sie dort den Drucker „Faxgate“ doppelt an. Windows wird feststellen, dass für diesen Drucker noch keine Treiber vorhanden sind und den Treiber-Installationsassistenten starten. Wählen Sie hier als Treiber den „Apple Laserwriter 12/640“ aus und stellen Sie die Treiberinstallation fertig.

Hinweis: *Wenn Sie den Drucker auf vielen Clients zu installieren haben empfiehlt sich das Hochladen der Treiber auf den Server per „Windows Add Printer Wizard“ Mehr dazu irgendwann unter „Tipps und Tricks“.*

Um ein Fax versenden zu können müssen Sie über das invis Portal den Fax-Client aufrufen und einrichten und dann einfach Ihr Fax auf den Faxgate-Drucker drucken. Der Faxgate-Drucker sucht selbsttätig im Druckdokument nach der Fax-Nummer des Empfängers. Wird diese nicht gefunden,

fordert er mit Hilfe des Faxgate-Clients zur Eingabe der Empfängernummer auf.

Die Einrichtung des Faxgate Clients ist im entsprechenden Handbuch beschrieben, auf welches Sie über die “?„ (Helpdesk-Seite) des invis Portals zugreifen können.

Fragen zum Thema beantworten wir gerne im Forum.

Einen kostenlosen SFF-Viewer für Windows, den Sie mit dem Faxgate-Client kombinieren können, finden Sie hier.

VPN-Server

Das invis Setup-Script richtet einen openVPN-Server für den „routed mode“ vor. Diese Betriebsart wird meist eingesetzt, wenn es darum geht Außendienstmitarbeitern (in diesem Zusammenhang oft als „Roadwarriers“ bezeichnet) flexiblen Zugang zu den Ressourcen des Firmennetzwerkes zu ermöglichen. Demgegenüber eignet sich der häufig erfragte „bridged mode“ eher zur statischen Verbindung zweier Netzwerke via VPN.

Im „routed mode“ wird zunächst ein gesicherter VPN-Tunnel zum VPN-Server aufgebaut und dann auf dem Client die „Default Route“ auf die Tunnelverbindung gesetzt. Das dahinter liegende Netzwerk ist vom Client aus nicht vollkommen transparent, was aus meiner Sicht die Sicherheit gegenüber dem „bridged mode“ etwa bei Verlust eines als VPN-Client eingerichteten Notebooks ein wenig erhöht.

Um Clients den Zugriff auf den VPN-Server zu ermöglichen muss auf diesen zunächst openVPN installiert werden. openVPN-Versionen für alle möglichen Betriebssysteme finden Sie hier.

Derzeit muss noch eine leere Revocation-List manuell erzeugt werden. Diese dient dazu ggf. einzelne Client-Schlüssel zu deaktivieren.

```
Kommandozeile: source ./vars
Kommandozeile: ./revoke-full dummy
```

Dieses Kommando wird mit einer Reihe von Fehlermeldungen aufgrund eines fehlenden „dummy.crt“ Zertifikats quittiert. Ignorieren Sie sie einfach, es wird trotzdem im Unterverzeichnis „keys“ die Datei namens „crl.pem“ erzeugt, ohne die OpenVPN nicht startet.

Nach der Installation wird auf dem Client eine Konfigurationsdatei für den Tunnel-Aufbau benötigt. Eine entsprechende Vorlage finden Sie unter /cfiles/openvpn im Verzeichnis des invis-Setup-Scripts. Kopieren Sie diese auf dem Client nach:

Windows: c:\Programme\openvpn\conf

Linux: /etc/openvpn

Auf Windows-Clients müssen die Dateien die Endung “.ovpn„ tragen, während unter Linux die Endung auf “.conf„ lauten muss.

Weiterhin benötigen Sie für jeden Client einen Schlüssel, den Sie auf dem Server erzeugen müssen. Wechseln Sie dazu auf dem Server ins Verzeichnis /etc/openvpn/ihredomain.loc und führen Sie folgende Kommandos aus:

```
Kommandozeile: source ./vars
Kommandozeile: ./build-key-pass clientfqdn
```

Wobei „clientfqdn“ selbstverständlich für den vollständigen Hostnamen des Clients steht. Der so erzeugte Schlüssel ist wie sie bemerkt haben passwortgeschützt. Kopieren Sie die Dateien ca.crt, clientfqdn.key und clientfqdn.crt auf sicherem Weg ebenfalls auf den einzurichtenden Client PC in das oben angegebene Verzeichnis. **Das Passwort darf nur der Nutzer des VPN-Clients kennen, schwören Sie ihn darauf ein, dass er Passwort und Client-PC niemals gemeinsam aufbewaren darf!**

Alternativ zu drei einzelnen Dateien für Private-Key, Zertifikat und Stammzertifikat, kann auch eine PKCS#12-Datei erstellt werden, die alle Komponenten in einer passwortgeschützten Datei zusammenfasst. Die Vorgehensweise ist genauso einfach:

```
Kommandozeile: source ./vars
Kommandozeile: ./build-key-pkcs12 clientfqdn
```

Hier ist nur die Datei „clientfqdn.p12“ auf sicherem Wege auf den Client.

Ein sicheres Kopieren kann beispielsweise mittels ***scp*** oder ***WinSCP*** erfolgen. Nich unüblich ist auch das Verteilen aller wichtigen Dateien per passwortgeschütztem USB-Stick, etwa, wenn sich Ihre Clients OpenVPN selbst installieren sollen. Sie haben dann die Möglichkeit, OpenVPN Installer, angepasste Konfigurationsdatei Schlüssel- und Zertifikate sowie einer Installationsanleitung bequem an Ihre Mitarbeiter weiterzugeben. Das zum Private-Key oder der PKCS#12-Datei gehörende Passwort hat allerdings auf einem USB-Stick nichts zu suchen.

Passen Sie jetzt noch die Client-Konfigurationsdatei an. Hier sind der DynDNS-Name des VPN-Servers, die Namen der Schlüsseldateien und die IP-Adressen am Ende der Datei an Ihre Umgebung anzupassen.

Je nach dem, ob Sie mit drei Dateien für Schlüssel- und Zertifikate oder mit einer PKCS#12 Datei arbeiten, muss in der Client-Konfiguration entweder:

```
ca ca.crt
cert clientfqdn.crt
key clientfqdn.key
```

oder

```
pkcs12 clientfqdn.p12
```

heissen.

Richten Sie auf einem Client mehrere VPN-Verbindungen ein, sollten Sie die Zugehörigen Schlüssel- und Zertifikatsdateien in entsprechenden Unterverzeichnissen ablegen.

```
pkcs12 filiale_ffm\clientfqdn.p12
```

So verhindern Sie Probleme mit gleichnamigen Schlüsseldateien für unterschiedliche Verbindungen und Sie schaffen sichtbar Ordnung.

Testen Sie abschließend die Verbindung indem Sie (unter Windows) die OpenVPN-GUI starten. In der Taskleite taucht daraufhin ein kleines Symbol auf. Dieses mit der rechten Maustaste angeklickt erlaubt Ihnen das direkte Starten aller bekannten VPN-Verbindungen. Sie werden daraufhin in einem geöffneten Fenster nach dem Passwort des Schlüssels gefragt. Nach der Eingabe können Sie dem Verbindungsaufbau zuschauen. Dieser sollte mit „suceeded“ beendet werden.

Sie können jetzt etwa mit dem Browser direkt (ohne HTTPS) auf den invis-Server zugreifen oder sich im Explorer über die Adresse „\\invisnetbiosname“ (steht selbstverständlich synonym für den tatsächlichen Namen Ihres invis Servers) die Samba-Freigaben des Servers anschauen.

Trennen können Sie die Verbindung ebenfals durch einen Rechtsklick auf das OpenVPN-Symbol in der Taskleiste.

Viel Spass damit.

Dokuwiki konfigurieren

```
Seit der Version 6.7-R7 wird die Installation automatisch durch das sine
Script durchgeführt. Dabei wird die Authentifizierung durch die
im LDAP vorhandenen Benutzer vorgenommen. Solange diese nicht angelegt sind
können Sie sich nur mit dem Domänen Administrator anmelden.
```

Der Rest ist „learning by doing“.

z-push konfigurieren

In der z-push Konfigurationsdatei:

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

ist die korrekte Zeitzone, für uns hier „Europe/Berlin“ einzutragen.

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

From:
https://wiki.invis-server.org/ - **invis-server.org**

Permanent link:
https://wiki.invis-server.org/doku.php?id=invis_server_wiki:installation:post

Last update: **2016/03/25 19:33**