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. Port 80/TCP (HTTP), ist erforderlich, wenn Sie für externe Zugriffe automatisch aktualisierte Zertifikate von Let's Encrypt verwenden möchten.
5. Port 1194/UDP für den Zugriff via OpenVPN.

Die hier als „verschoben“ bezeichneten Ports wurden von ***sine2*** zufällig generiert und während des Setups ausgegeben. Nachträglich Abfragen können Sie sie auf der Kommandozeile mit:

```
linux:~ # sine2 showconf
```

Hinweis: *Damit es möglichst nicht zu Konflikten mit anderen Diensten kommt werden zufällige Ports nur im „dynamischen Bereich“ (größer 50000) generiert.*

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.

Hinweis: *Die nachfolgenden Einstellungen werden ab invis-Server 11.4 mit unserem eigenen Passwort-tool* ***pwsettings*** *vorgenommen.*

```
invis:~ # pwsettings
```

Zu wissen, wie sich die Einstellungen mit Hilfe des ***samba-tools*** auf der Kommandozeile des Servers ändern lassen, kann allerdings auch nicht schaden. 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.

Let's Encrypt Zertifikate für Externzugriffe

Die im Laufe der invis-Server-Installation erzeugten eigenen Zertifikate bringen ein Problem mit sich. Greift jemand beispielsweise mit einem Browser via Internet auf Ihren invis-Server zu wird dies mit einer Sicherheitswarnung beantwortet. Die betrifft Zugriffe auf Z-Push, ownCloud oder auch das invis-Portal. Speziell im Falle von ownCloud ist das unschön. Gerade, wenn Sie darüber Dateien mit Dritten teilen möchten, wirkt eine Zertifikatswarnung unseriös.

Zwar lässt sich das durch den Import des Server-Stammzertifikates beheben, allerdings ist die Verteilung des Stammzertifikates an Dritte ebenfalls nicht gerade einfach.

Eine Umstellung auf „echte“ Zertifikate von Let's Encrypt behebt dieses Problem. Für die Umstellung müssen gewisse Voraussetzungen gegeben sein:

1. Der Server muss an seinem Betriebsort stehen.
2. Im vorgeschalteten Router muss Port 80 auf den invis-Server weitergeleitet sein
3. Der Server muss über einen im Internet gültigen Namen verfügen. (DDNS)

Sind alle Voraussetzungen erfüllt, genügt es für den Umstieg auf die echten Zertifikate den folgenden Befehl auszuführen:

```
invis:~ # actdehydrated
```

Alles weitere geschiet automatisch.

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.... (kommt noch)

Danach ist noch die Firewall neu zu starten:

```
linux:~ # systemctl restart firewalld.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.

Kivitendo

Kivitendo ist nach erfolgreichem Setup des invis-Servers mittels ***sine*** bereits weitgehend vorbereitet. 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:

```
# 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:

```
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*

WaWision, InvoicePlane, Kimai

Alle drei genannten Programme bringen ein Web-gestütztes geführtes Setup mit. Sie müssen die Applikation jeweils nur im Browser öffnen. Das geht am einfachsten über die entsprechenden Links in der local-Section des invis-Portals. Die Webinstaller starten jeweils automatisch.

Jedes der drei Programme benötigt eine eigene MariaDB-Datenbank, welche bereits von ***sine2*** erstellt wurden. Damit die Programm darauf zugreifen und sie mit Tabellen füllen können, benötigt der jeweilige Installer die Zugangsdaten zur Datenbank, bestehend aus Datenbankname, Benutzername des Dantenbankbenutzers und dessen Passwort.

Die Passwörter können Sie wie folgt in Erfahrung bringen:

```
invis:~ # sine2 showps
```

Datenbank & Benutzername

- WaWision: DB = wawision, Benutzer = wawision
- InvoicePlane: DB = invoiceplane, Benutzer = ip
- Kimai: DB = kimai, Benutzer = kimai

Nach dem geführten Setup sind ggf. weitere Schritte erforderlich.

Kimai

- Das Verzeichnis „installer“ unter /srv/www/htdocs/kimai ist zu löschen
- In der Datei /srv/www/htdocs/kimai/includes/autoconf.php ist in der Zeile „$authenticator“ der Parameter „kimai“ durch „activeDirectory“ zu ersetzen.

acpupsd einrichten

Das Überwachungsdienst für unterbrechungsfreie Stromversorgungen des Herstellers APC muss an Ihre USV angepasst werden. Vorgenommen wird die Konfiguration in:

```
/etc/apcupsd/apcupsd.conf
```

In der Regel werden aktuelle USVs via USB-Kabel an den Server angeschlossen. APC-USVs kennen dafür die beiden Betriebsarten „USB“ und „Modbus“. Aktuelle Modelle sind auf jeden Fall auf Modbus einzustellen, da bei Ihnen über die ältere USB-Variante nicht alle Daten ausgelesen werden können. Wie Sie die Einstellung vornehmen, entnehmen Sie bitte dem Handbuch Ihrer USV.

In oben genannter Datei sind lediglich die folgenden Optionen, an Ihre USV anzupassen:

```
...
UPSCABLE usb
...
UPSTYPE usb
```

```
...
```

Die angezeigten Parameter entsprechen den Voreinstellungen, ggf. müssen Sie UPSTYPE auf den Wert „modbus“ umstellen.

Starten Sie jetzt den Dienst neu:

```
invis:~ # systemctl restart apcupsd.service
```

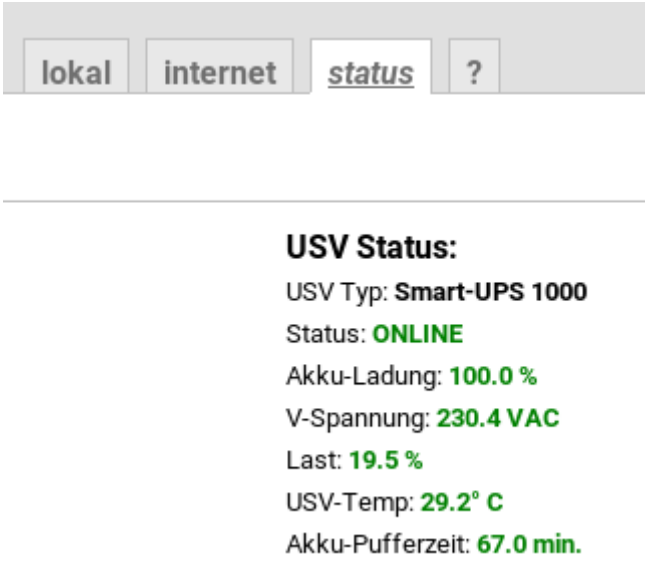
Um die Betriebsdaten der USV im invis-Portal anzuzeigen ändern Sie einfach in

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

den Parameter der Option „$STATUS_APCUPSD“ auf „true“:

```
....
// Aktivieren der APCUPS Daemon Abfrage
$STATUS_APCUPSD = true;
....
```

Auf der Status Seite des invis-Portals sieht das dann beispielsweise wie folgt aus:



VPN-Clients einrichten

Nach Durchlauf des Setup-Scripts ***sine2*** ist OpenVPN vollständig konfiguriert und bereits gestartete.

Testen können Sie dass mit:

```
linux:~ # ip link show 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. Für eine Anleitung klicken Sie auf den vorangegangenen Link.

Vorgefertigte Client-Konfigurationsdateien, die Sie lediglich anpassen müssen finden Sie in der Service-Freigabe Ihres Fileservers.

... to be continued

z-push konfigurieren

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

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

```
/etc/z-push/z-push.conf.php
```

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