Anwendug des Setup-Scripts

Auch nach der Umstellung auf ein RPM-basiertes Setup wird die weitere Installation vom Setup-Script (***sine*** – „**s**erver **i**nstallation **n**ow **e**asy“) ausgeführt.

```
linux:~ # sine
```

sine kennt seit invis-Version 9.2 (openSUSE 13.1) ein paar nützliche Aufrufparameter:

- sine help - gibt kurze Hinweise zur Verwendung
- sine status - zeigt an, mit welchem Modul sine beim nächsten Aufruf gestartet wird.
- sine log - zeigt (so bereits vorhanden) das Log-File des bisherigen sine-Durchlaufs
- sine showconf - zeigt die (so bereits vorhanden) die von sine abgefragten Konfigurationsparameter an.
- sine modulname - ermöglicht, **nach einmalig vollständigem Durchlauf**, übersprungene optionale Module nachträglich manuell zu starten.

Das Arbeitsverzeichnis von ***sine*** ist unter

```
/var/lib/sine
```

zu finden. Dort sind Konfigurations-, Log-, sowie Temporärdateien des Script-Laufs zu finden.

Alle vorbereiteten Konfigurationsdateien für das invis-Setup sind im Zuge des Umbaus zur RPM-basierten Installation nach

```
/usr/share/doc/packages/invis-setup/examples
```

gewandert, später als „Examples-Verzeichnis“ benannt.

sine ist Modular aufgebaut. Alle Module werden der Reihe nach abgearbeitet. Wenn Sie etwa mit „STRG+C“ den Script-Lauf an beliebiger Stelle unterbrechen, setzt ein erneuter Start das Script am Beginn des abgebrochenen Moduls fort. In aller Regel hat dies keine unerwünschten Folgen.

Unterschieden wird zwischen Pflicht- und optionalen Modulen, wobei zunächst die Pflichtmodule in logischer Reihenfolge abgearbeitet werden. Zu Beginn eines optionalen Moduls, fragt das Script ob dieses Modul ausgeführt werden soll. Nach einem vollständigen Durchlauf des Scripts (es spielt keine Rolle, ob optionale Module ausgelassen wurden) können die optionalen Module einzeln wie oben aufgeführt manuell aufgerufen werden. Die optionalen Module sind: *nagios, groupware, erp, webcdwriter, faxgate, openvpn, dokuwiki und etherpad.*

Da das Script in Sachen Optik sicherlich nicht der Weisheit letzter Schluss ist, empfiehlt es sich während des Durchlaufs genau hinzuschauen und möglichst alles zu lesen. Sollten beim Script-Lauf Dinge unklar sein, scheuen Sie bitte nicht die Nutzung unseres Forums - es beisst nicht! Die Sache mit „Sche*, das funktioniert nicht“ abzubrechen hilft niemandem.

Bevor Sie jetzt das Script starten, sollten Sie sich fürs Verständnis dessen, was ein invis-Server ist, folgenden Beitrag durchlesen Aufbau und Funktion.

Hinweis: *Die Setups zwischen* ***invis-server Classic*** *und* ***invis-server AD*** *unterscheiden sich an einigen Stellen voneinander. In der folgenden Beschreibung wird jeweils auf die Unterschiede*

hingewiesen. Sie sollten die Anleitung allerdings ungeachtet der gewählten Variante komplett lesen!

Die Module im Einzelnen (Pflichtmodule)

Nachfolgend erläutere ich die einzelnen Module in Reihenfolge des Scriptlaufs. Der Name des jedes Moduls wird immer bei dessen Start kurz angezeigt.

Modul: check

Das erste Script-Modul fragt Sie zunächst, ob alle Installationsvoraussetzungen für die invis Server Installation erfüllt sind und führt diese noch einmal auf.

Wird die Frage verneint, bricht das Script ab.

Andernfalls werden einige grundlegende Vorbereitungen für die weitere Installation getroffen. Dazu gehören:

- die Aktualisierung des Paketmanagers zypper,
- die Durchführung eines Online-Updates,
- die Installation grundlegender Pakete,
- die Synchronisation der Server-Uhr und
- die Konfiguration des Boot-Managers.

Nach Abschluss jeden Moduls haben Sie 5 Sekunden Zeit das Script mit „Strg+C“ abzubrechen. Beim nächsten Aufruf wird das Script mit dem nächsten Modul fortgesetzt.

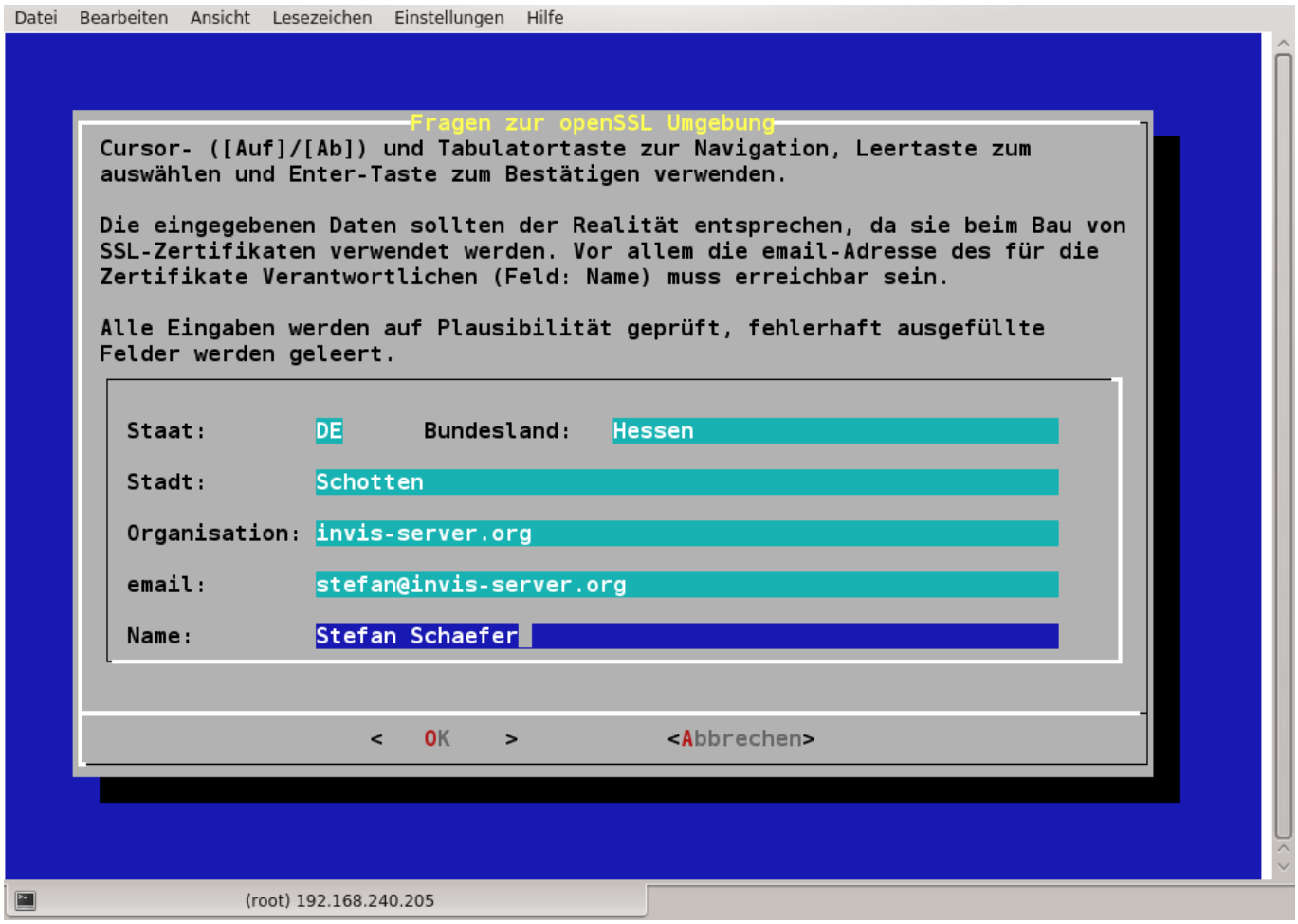
Wird die Installation eines Servers auf diese Weise für mehr als einen Tag unterbrochen, empfiehlt es sich vor dem Fortführen der Installation manuell ***zypper ref*** auszuführen, da die Möglichkeit besteht, dass sich in den Repositories inzwischen Veränderungen ergeben haben können.

Modul: quest

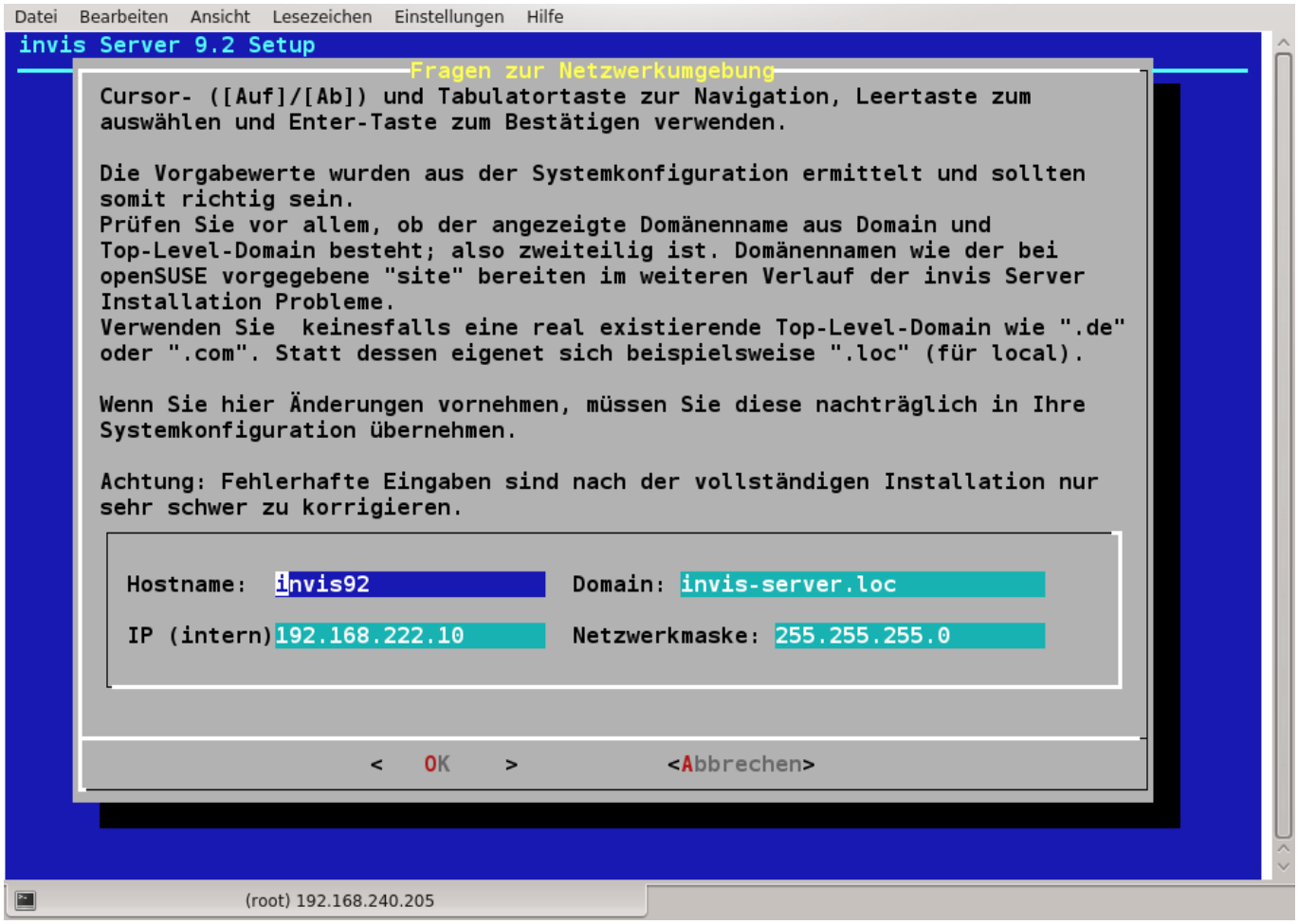
Dieses Modul stellt Fragen nach der Umgebung in der der Server eingesetzt werden soll, sowie nach einigen notwendigen Passwörtern. Das Script versucht dabei Vorgabewerte für die Antworten selbsttätig zu ermitteln. Das klappt natürlich nicht bei den Passwörtern 😉.

Alle abgefragten Daten werden anschließend in der Datei „invis_confdata“ im ***sine*** Arbeitsverzeichnis gespeichert. Achten Sie darauf, dass diese Datei nach Beendigung der Installation nicht für jedermann lesbar im Netz herum geistert. Wäre unschön, wenn Ihr Netz voller Administratoren wäre....

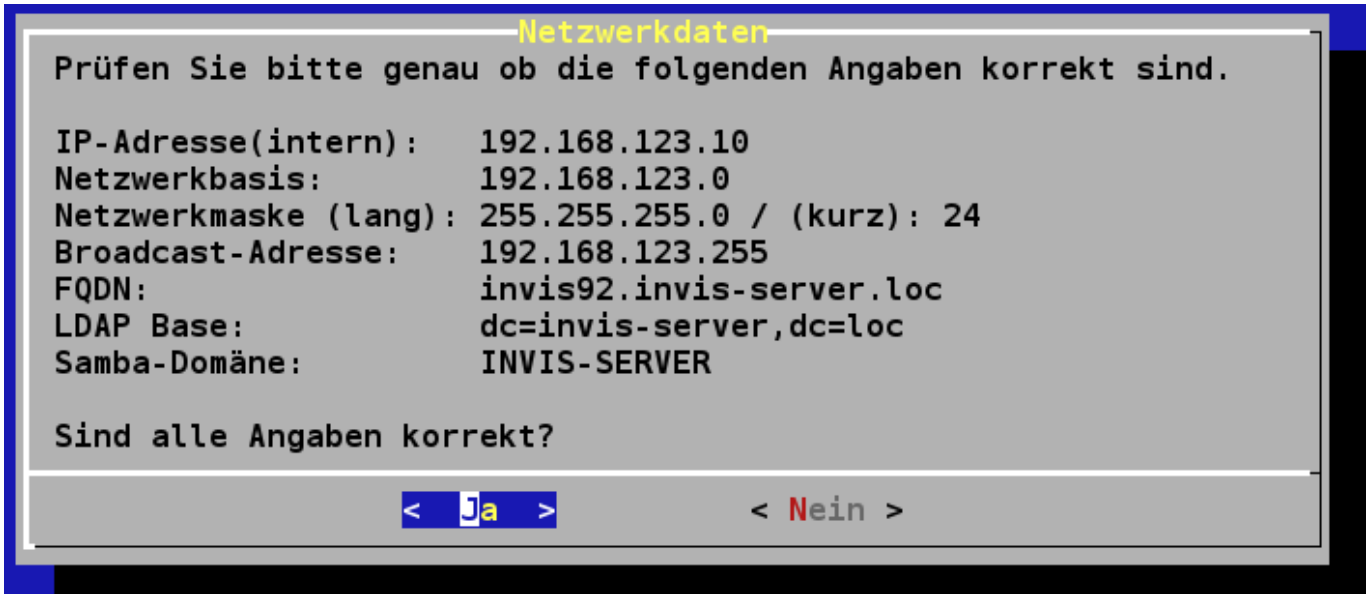
Zunächst werden Sie gebeten Informationen für den Aufbau einer eigenen Zertifizierungsstelle (CA) einzugeben. Diese Informationen werden nachfolgenden auch für die Erstellung von Schlüsseln und Zertifikaten für verschiedene Serverdienste benötigt.



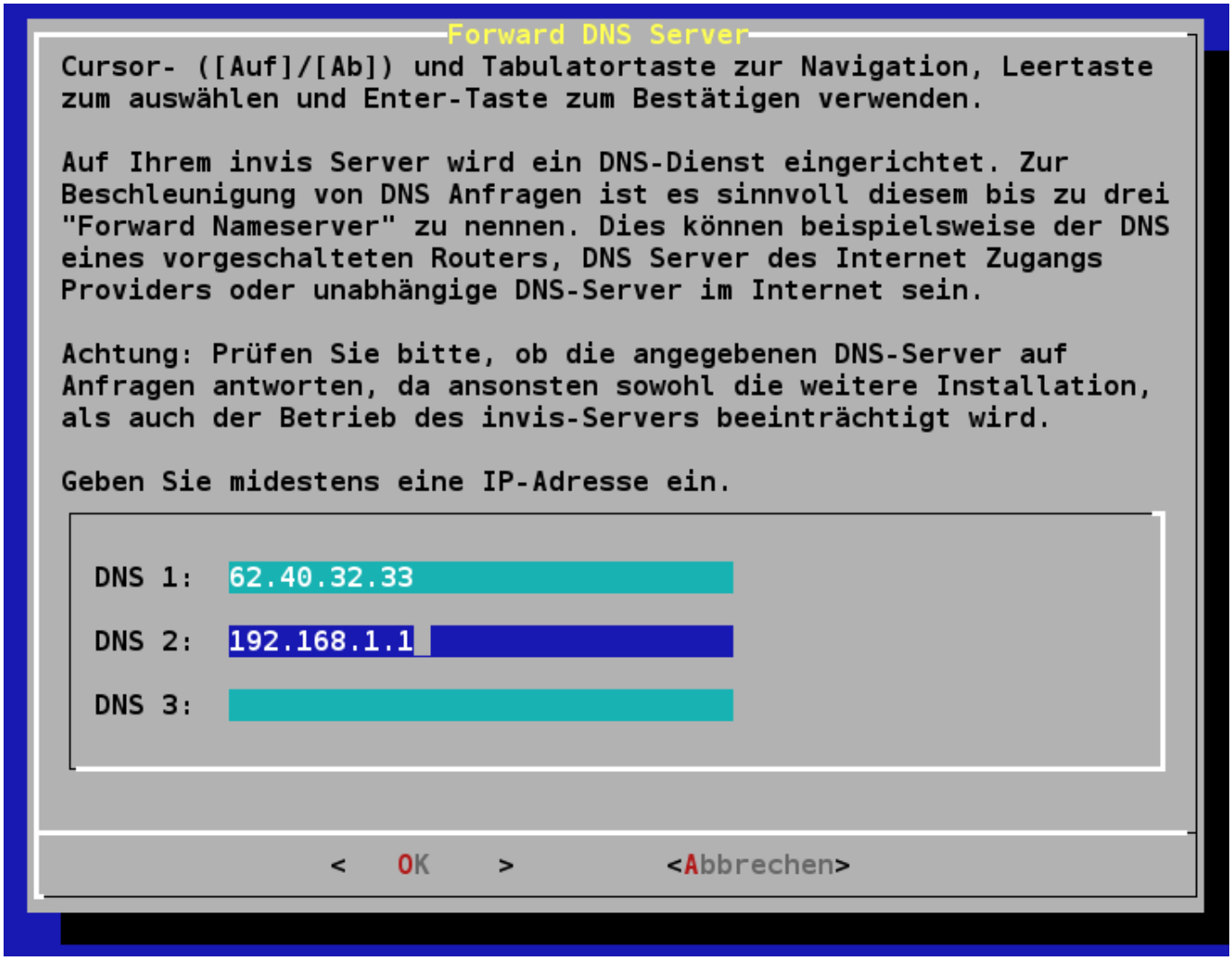
Im Anschluss daran wird die Netzwerkkonfiguration abgefragt und überprüft.



Die Daten werden automatisch ermittelt, sind einzelne Eingabefelder leer, ist die vorbereitende Netzwerkkonfiguration nicht vollständig abgeschlossen worden. Sie können die korrekten Daten hier manuell eingeben, müssen aber idealerweise im Anschluss an das Quest-Modul die Netzwerkkonfiguration mittels YaST nachgeholt werden.



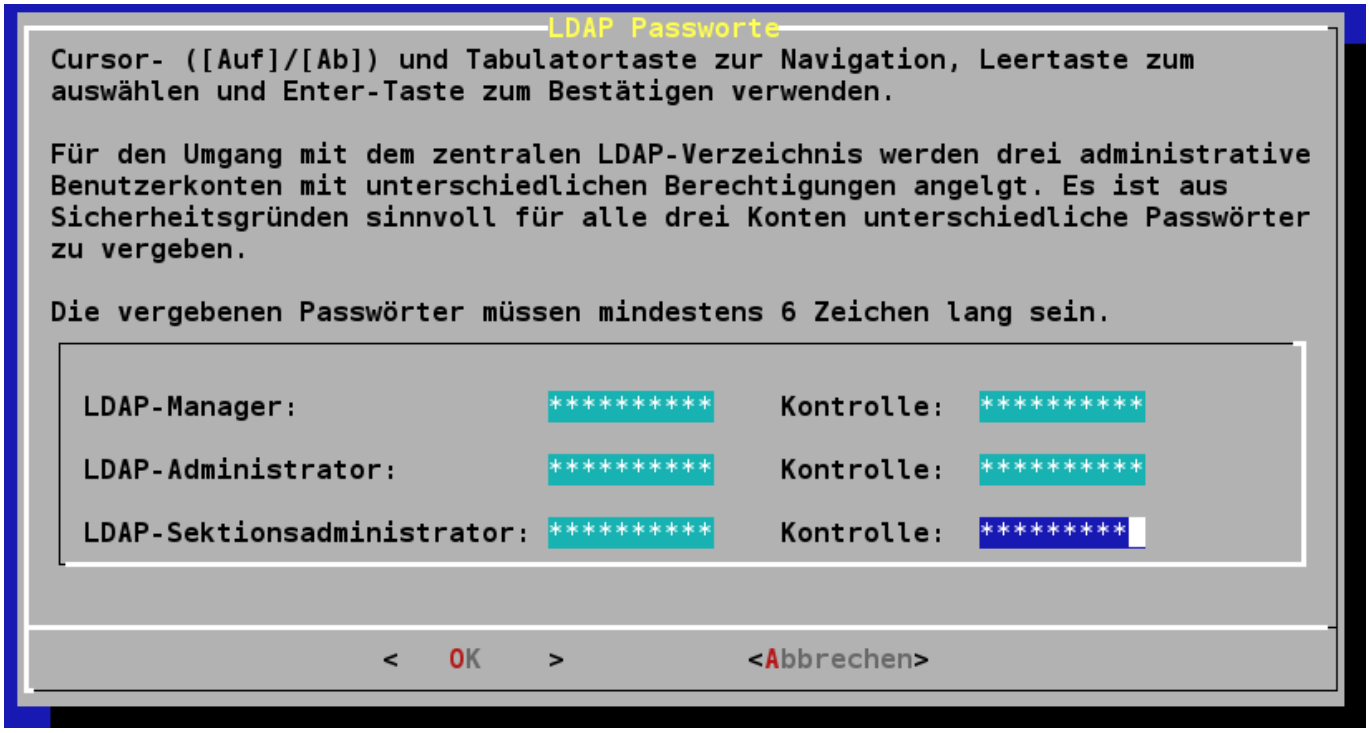
Im zweiten Bild der Netzwerkdaten, müssen alle Zeilen werte enthalten, ist dies nicht der Fall wird es bei der weiteren Konfiguration des Servers zu Fehlern kommen.



Ein invis-Server arbeitet für das an ihn angeschlossene Netzwerk als DNS-Server. Zuständig ist er primär für die Namensauflösung im lokalen Netz, er arbeitet aber auch als Caching-Nameserver für die Namensauflösung im Internet. Um diese Aufgabe zu erleichtern können Ihm sogenannte „Forwarder“ bekannt gemacht werden. Forwarder sind DNS-Server, die die Namensabfrage im Internet beschleunigen können. Das Setup-Script fragt nach bis zu drei Forward-DNS Servern. Sie können hier ggf. einen vorgeschalteten Router, die DNS-Server Ihres Providers oder freie DNS-Server im Internet angeben.

Nur invis-server Classic

Es werden Passwörter für unterschiedlich berechtigte LDAP-Administratoren, den MySQL-root-Account, den ntop-Admin und ggf. den Cyrus-Administrationsaccount erfragt.



Bei den Passwörtern für die LDAP-Admins wird zwischen dem LDAP-Manager, dem LDAP-Admin und Sektions-Admins unterschieden. Der Account des LDAP-Managers wird nicht im LDAP-Verzeichnis selbst sondern in der Datei slapd.conf angelegt. Ungeachtet aller gesetzten LDAP-Zugriffsrechte (ACLs) darf der LDAP-Manager immer schreibend auf das gesamte Verzeichnis zugreifen.

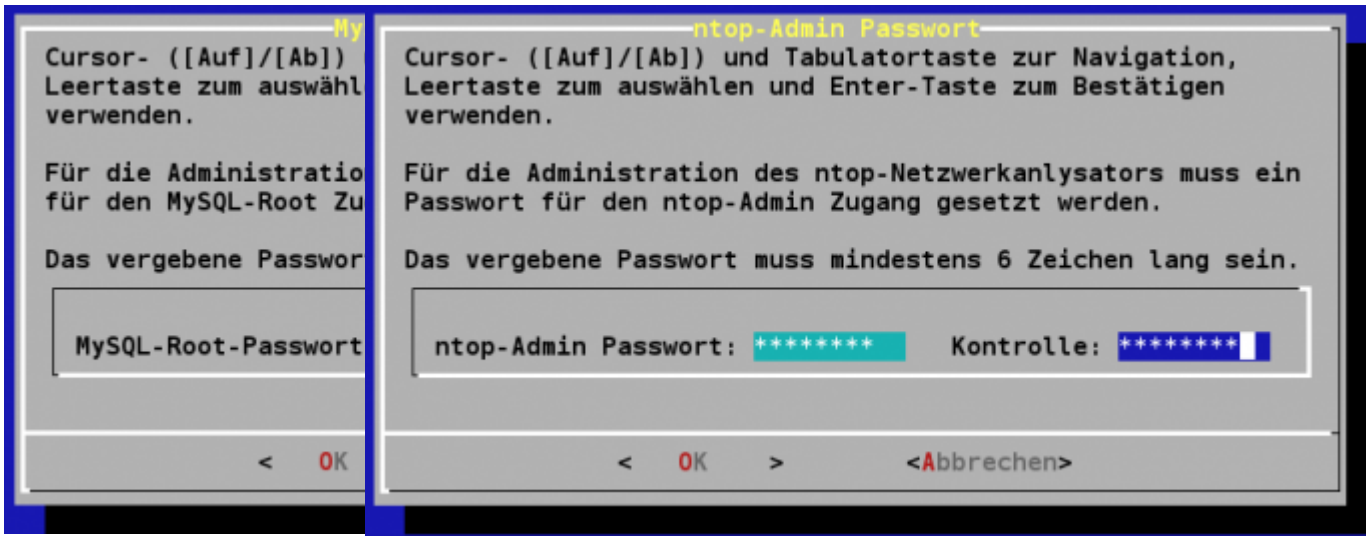
Demgegenüber ist der LDAP-Admin ein Objekt im LDAP mit globalen Administrationsrechten, die sich aber über ACLs definieren lassen.

Die Sektions-Admins sind jeweils nur für einen Zweig im LDAP - etwa die DHCP Konfiguration - administrationsberechtigt.

invis-Server AD

Hier übernimmt der Domänenadministrator zunächst die Rolle der AD-Verwaltung. Dessen Passwort wird derzeit im Laufe der Installation statisch auf den Wert: „p@ssw0rd“ gesetzt und sollte später geändert werden.

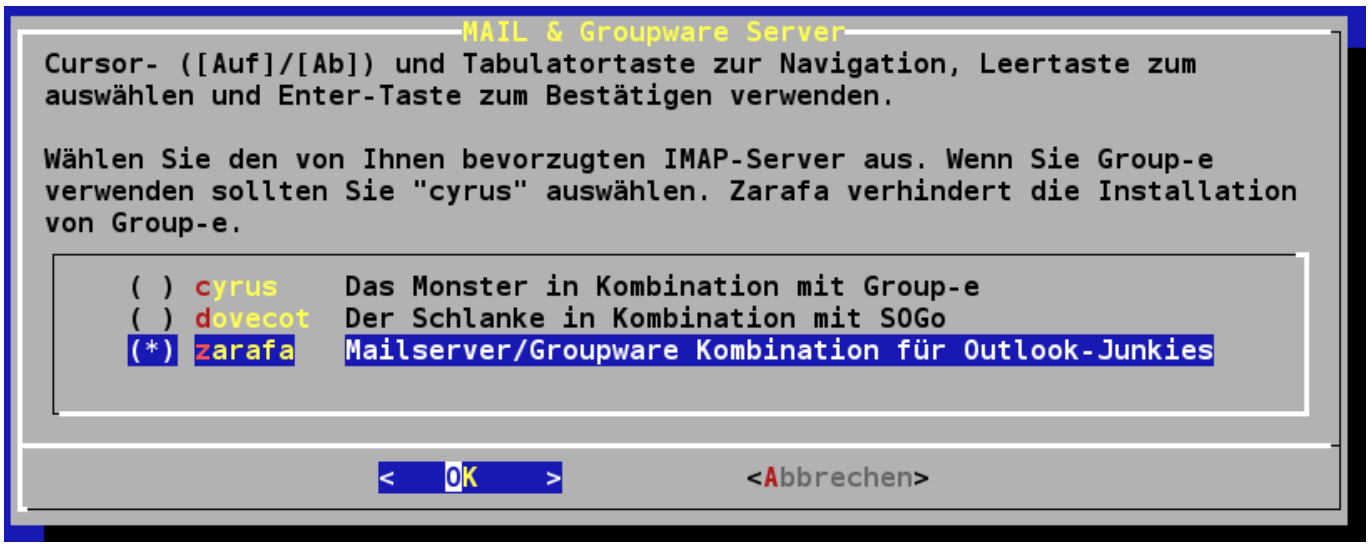
Es folgt die Abfrage des Passwortes für den MySQL root-Account.



---

invis-server Classic

Die nächste Frage zielt auf die gewünschte Kombination aus Mailserverkomponenten und Groupware ab.



Beim Mailserver-Setup wird zwischen drei Szenarios unterschieden:

- **Postfix**, **Cyrus-IMAP** und **Group-e**
- **Postfix** und **Zarafa**
- **Postfix**, **Dovecot-IMAP** und **SoGo**

Produktiv ist derzeit vor allem die zweite Kombination zu empfehlen, sie ist in der Praxis erprobt.

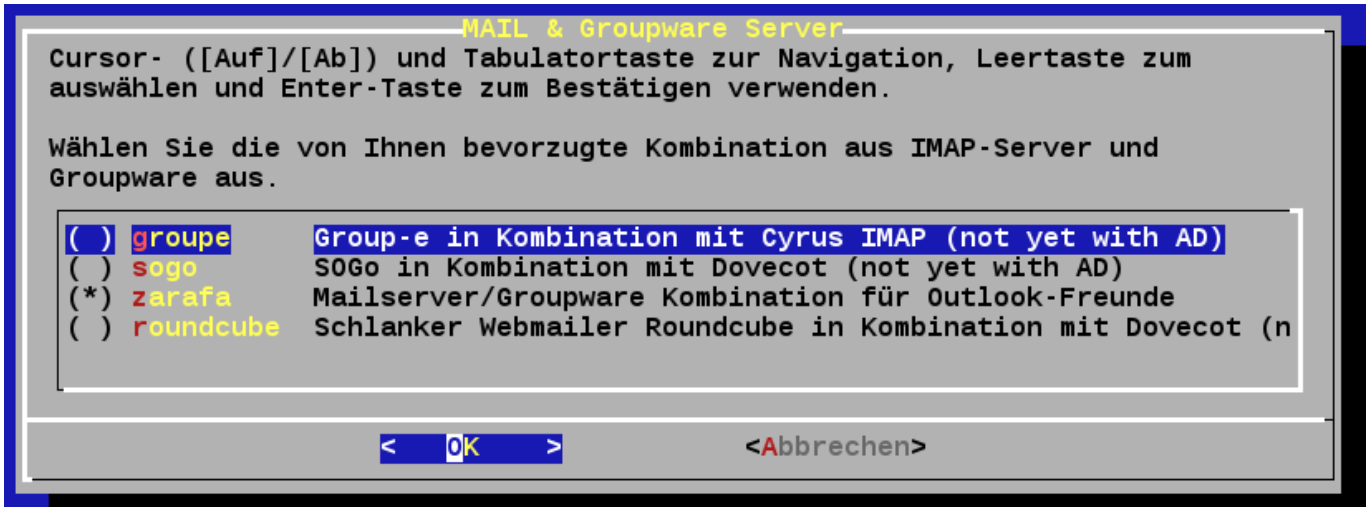
Kombination Nr. 1 dürfte bei weitem den größten Funktionsumfang bieten, allerdings ist die Einrichtung von Group-e kein Spaziergang.

Kombination Nr. 3 ist erst seit kurzem Teil des Setups. Es wurde auf Wunsch eines Kunden implementiert. Es fehlen noch Informationen über SoGos Alltagstauglichkeit.

Die beiden Groupware-Systeme Group-e und Zarafa lassen sich nicht miteinander vergleichen, sie verhalten sich wie Äpfel und Birnen zueinander. Während Zarafa den Fokus darauf legt als Exchange-Alternative in Betracht zu kommen und sich daher funktional auf Grouware-Kernfunktionen (Kalender, Kontakte, Aufgaben und Mail) beschränkt, ist Group-e eine Groupware-Lösung mit der sich auch ein einfaches Projekt, Zeit und Dokumentenmanagement, also regelrechte Workflows abbilden lassen. Group-e setzt allerdings für den vollen Funktionsumfang die Nutzung des Webclients voraus. Ein Fatclient oder gar die Anbindung von Outlook sind nicht im Fokus der Entwickler.

In Sachen Anbindung von mobilen Clients sind beide Systeme miteinander vergleichbar. Group-e bietet SyncML und ActiveSync, Zarafa ActiveSync und Blackberry als Synchronisationsmöglichkeiten für Smartphones an.

invis-Server AD

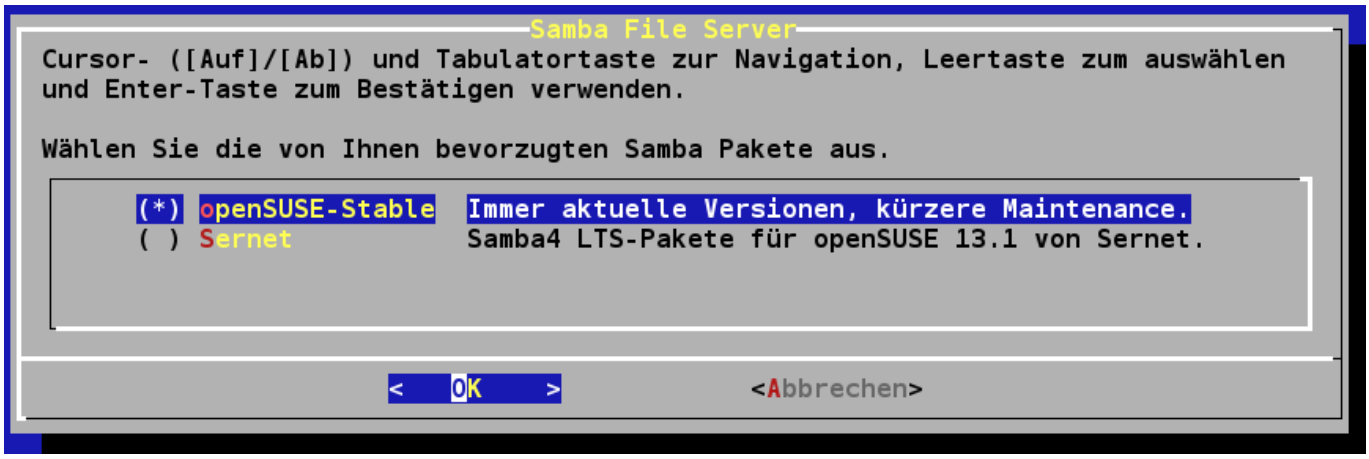


Achtung: *Wir haben die Abfrage für die unterschiedlichen Mailserver- bzw. Groupware-Setups in der Fragestunde gelassen. Derzeit funktioniert das Setup aber ausschließlich mit* ***Zarafa****. Eine Entscheidung, wie mit den anderen Optionen verfahren wird steht noch aus und ist unter anderem davon abhängig in wie weit die anderen Systeme eine AD-Integration erwägen.*

---

invis-server Classic

Zentrales Element einer invis-Server Installation ist der Fileserver Samba. Gewählt werden kann zwischen Samba-Paketen aus dem Distributionsumfang oder RPM-Paketen der Göttinger Firma Sernet.



Vorteil der Sernet-Pakete ist sicherlich deren Longterm-Support. Sernet stellt seine Samba Pakete auch noch auf Jahre über den Maintenance-Zeitraum einer openSUSE-Version hinaus zur Verfügung. Nachteil ist, dass es eine Weile dauern kann bis Pakete für taufrische openSUSE-Versonen zur Verfügung stehen. **(Stand Januar 2014 - Es stehen noch keine Sernet-Pakete für openSUSE 13.1 zur Verfügung, es ist aber möglich die Pakete der Vorgängerversion 12.3 zu installieren)**.

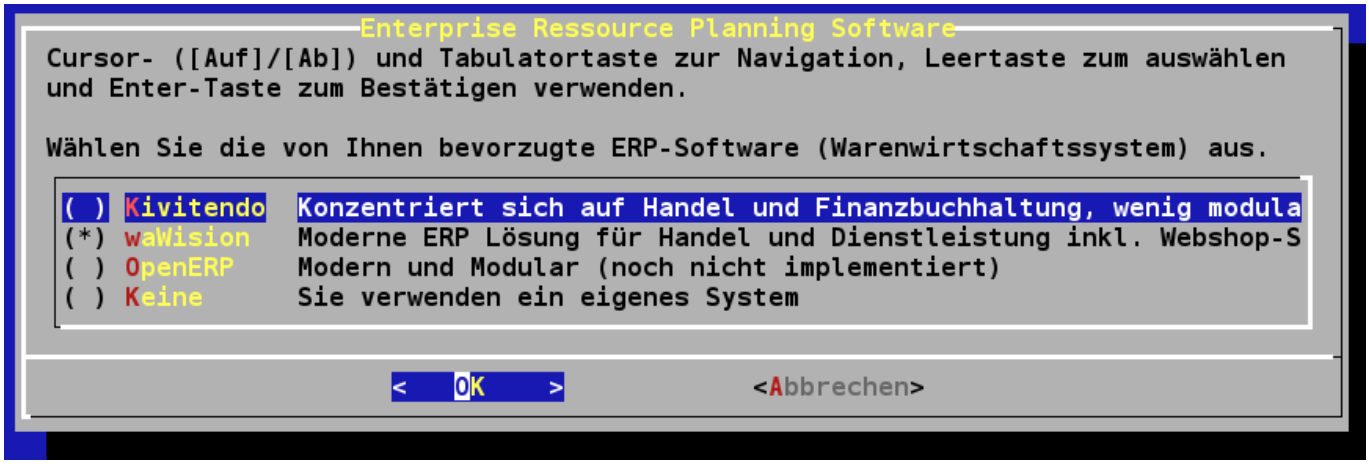
Hinweis: *Das im Sernet-Repository enthaltene Paket „sernet-samba-ad“ wird an dieser Stelle* ***nicht*** *installiert, da es mit OpenLDAP in Konflikt steht. D.h. auch mit diesen Paketen ist vorerst nur eine klassische Samba Installation möglich. Wir arbeiten an einer Upgrade-Möglichkeit zu ActiveDirectory.*

Installiert wird bereits Samba 4, auch wenn Samba nach wie vor klassisch, also ohne ActiveDirectory betrieben wird. Mit den openSUSE Paketen wäre dies auch derzeit noch nicht möglich. Um die Samba4 Pakete von Sernet installieren zu können ist eine persönliche Registrierung auf https://portal.enterprisesamba.com/ erforderlich. Dort erhalten Sie Zugangsdaten, die von ***sine*** abgefragt und in die entsprechende Repository-Datei eingetragen werden müssen. Ohne diesen Schritt kann keine Software aus dem Repository installiert werden.

invis-Server AD

Um ein Active Directory zu ermöglichen müssen die Sernet-Samba Pakete gewählt werden. In diesem Fall wird das Paket **sernet-samba-ad** installiert. Die openSUSE Pakete beinhalten diese Komponente derzeit noch nicht.

Seit Version **6.9-R1** ist neu, dass zwischen unterschiedlichen Mailserver- und ERP-Software-Setups ausgewählt werden kann.

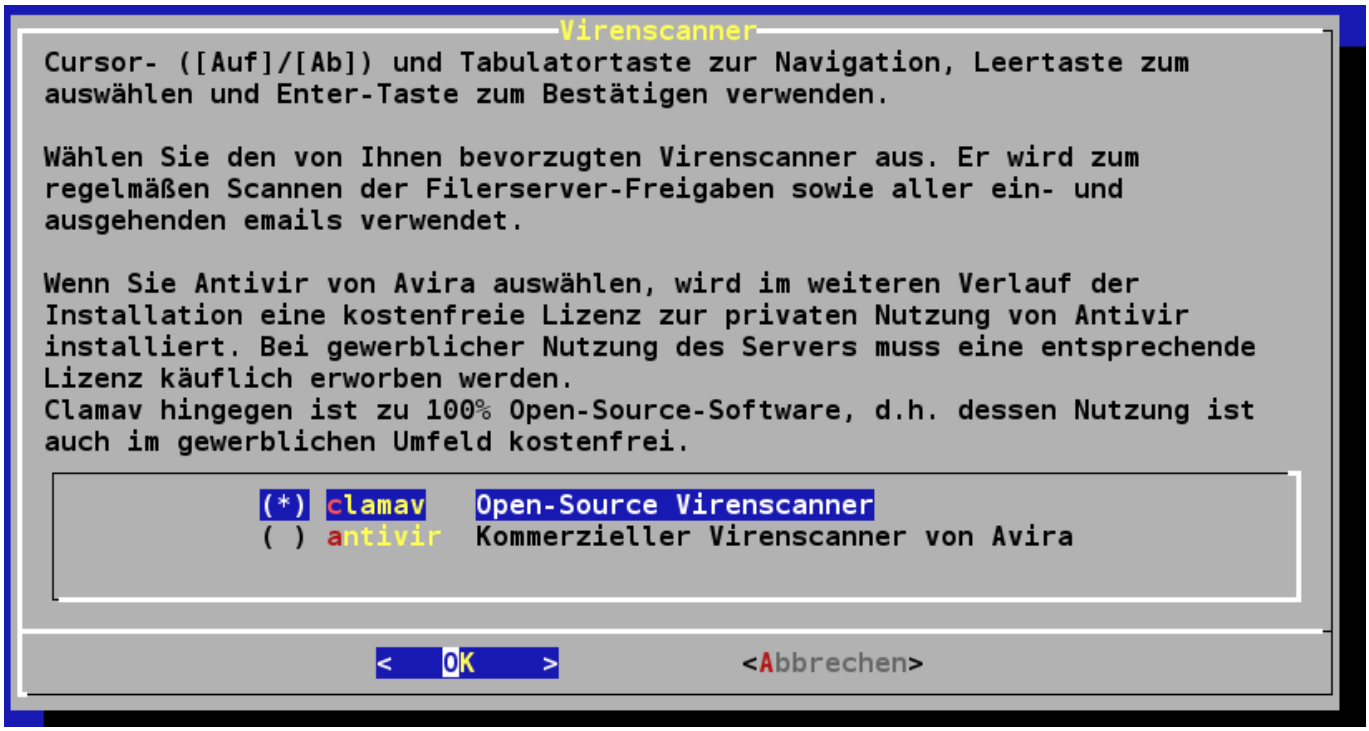


Achtung: *OpenERP ist derzeit (Stand 9.x) noch immer nicht soweit implementiert, dass es produktiv einsetzbar ist. Eine funktionierende Installation ist nicht möglich. Ursache dafür sind Probleme beim Bau der notwendigen RPM-Pakete. eine detaillierte Beschreibung des Problems finden Sie* ***hier*** *Über Hilfe beim Beseitigen des Problems würden wir uns freuen. Eine funktionierende manuelle Installation ist möglich. Die aktuelle Version finden Sie* ***hier*** *zum herunterladen.*

Zu entscheiden, ob Kivitendo oder WaWision besser zu Ihren Anforderungen passt dürfte nicht leicht sein. Informieren Sie sich am besten im Vorfeld über die Produkte:

- **Kivitendo** - http://www.kivitendo.de/
- **WaWision** - http://www.wawision.de/

Für den Einsatz im Mailserver, wie auch für die auf dem Fileserver abgelegten Dateien wird auf invis-Servern auch eine Antiviren Lösung installiert. Zur Auswahl stehen derzeit die Open-Source-Lösung ClamAV, sowie Avira Workstation für Unix.



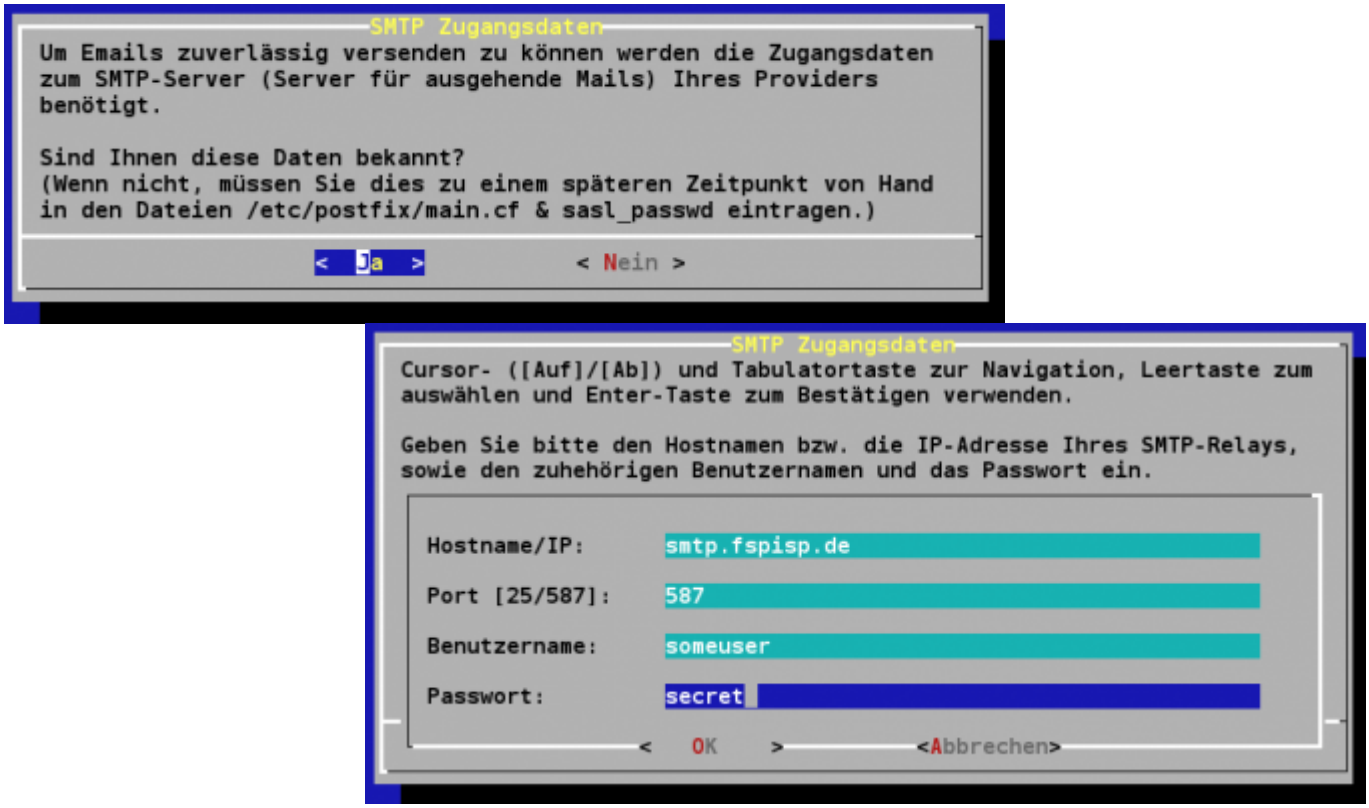
Hinweis: *Beachten Sie bei der Frage nach dem gewünschten Viren-Scanner, dass der angebotene*

Avira Antivir für den gewerblichen Einsatz käuflich erworben werden muss. Das Setup-Script lädt zwar automatisch einen Lizenzschlüssel herunter, dieser ist allerdings nur für den privaten Einsatz oder Evaluationszwecke gedacht. Hinzu kommt, dass Avira die Unterstützung des Betriebssystems Linux leider abgekündigt hat. Wir halten Ausschau nach einer Alternative. Aktualisierungen der Virendefinitionsdateien stellt Avira derzeit noch bereit.

Idealerweise sollte Ihr invis-Server auch via Internet (HTTPs, SSH, VPN) erreichbar sein. Hierfür benötigen Sie entweder eine feste IP-Adresse oder einen DDNS-Namen. Dies wird im nächsten Schritt erfragt.

Hinweis: *Wenn die Frage, ob der invis Server via Internet (HTTPS) erreichbar sein soll mit „nein“ beantwortet wird, wird der Apache-Webserver* ***NICHT*** *für den HTTPS-Zugriff eingerichtet. Wenn Sie dies später von Hand nachholen möchten, finden Sie im Examples-Verzeichnis im Unterverzeichnis webserver unter dem Namen „invis-sslvh.conf“ eine Vorlage-Datei für einen SSL vhost. Kopieren Sie diese nach /etc/apache2/vhosts.d und passen Sie sie an Ihre Gegebenheiten an. Die Schlüssel für den HTTPS Zugriff müssen Sie dann allerdings selbst erzeugen. Hierfür können ist das Script* ***serverkeys*** *aus der invis toolbox gedacht.*

Weiterhin wird gefragt, ob die Zugangsdaten für den Postausgangsserver (SMTP Relay) Ihres Mailproviders vorliegen.



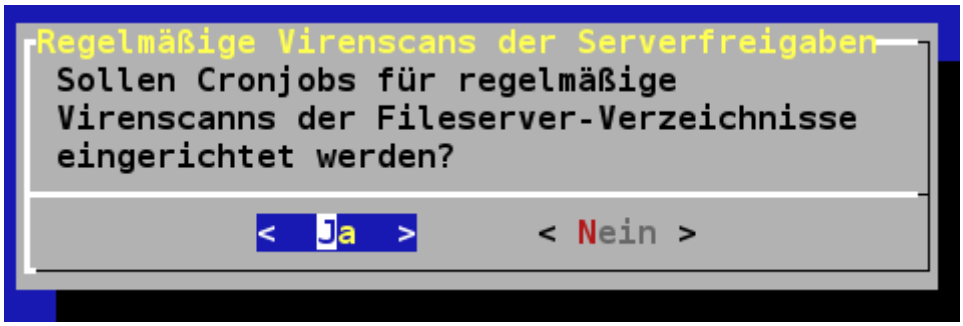
Ist dies nicht der Fall, lassen sich diese Daten auch zu einem späteren Zeitpunkt direkt in der Postfix-Konfiguration nachtragen. Ohne einen solchen Postausgangsserver wird es, speziell dann, wenn Ihr invis-Server hinter einem DSL-Anschluss ohne feste IP-Adresse nicht möglich sein zuverlässig Emails zu versenden.

---

invis-Server stellen einige Netzwerkfreigaben zur Verfügung, darunter die Freigabe „Transfer“, die für den allgemeinen Dateiaustausch gedacht ist. Jeder Benutzer hat darauf Schreibrechte. Die Praxis hat gezeigt, dass solche Freigaben schnell zur „Betriebsmüllhalde“ mutieren und sich immer größere Datenmengen ungeordnet ansammeln. Dem entgegenzuwirken bietet der invis-Server die Möglichkeit Dateien und Verzeichnissen, die hier abgelegt werden, ein Verfallsdatum zu geben, nachdem die Dateien automatisch gelöscht werden.

Sie werden hier gefragt, ob Sie diesen Automatismus wünschen und wie alt in „Transfer“ abgelegte Dateien werden dürfen.

Anschließend wird gefragt, ob Sie regelmäßige Virenscans der Fileserver-Freigaben wünschen. Es sei darauf hingewiesen, dass der im invis-Server integrierte Virenscanner nicht als Echtzeit-Scanner arbeitet. Dies muss also auf den angeschlossenen Arbeitplatz-Computern der Fall sein.

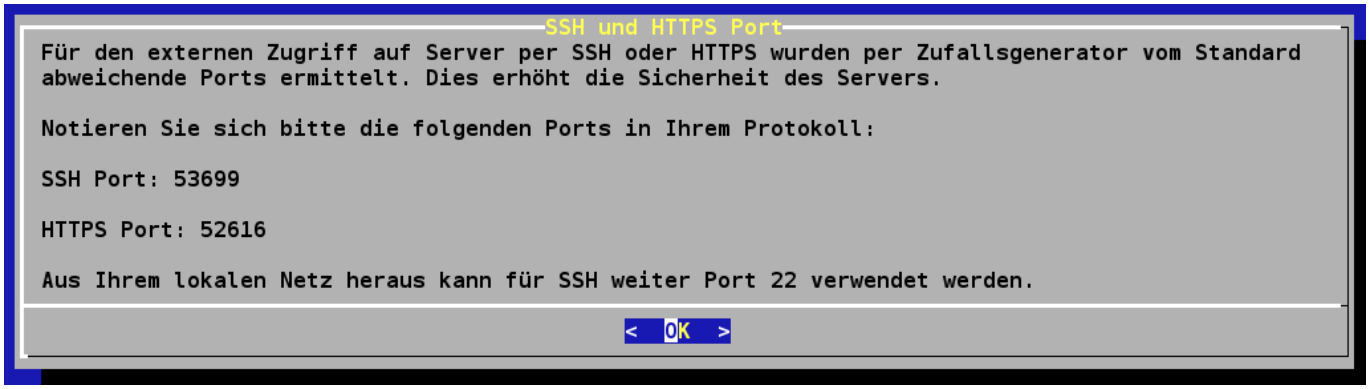


Neu hinzugekommen ist noch ein weiterer Frage-Block zum Thema „ownCloud-Synchronisation“. invis-Server bieten die Möglichkeit ein beliebiges Verzeichnis mit einem ownCloud-Konto zu verknüpfen. Hier werden neben dem Namen des ownCloud-Servers und den entsprechenden Zugangsdaten auch das zu synchronisierende Verzeichnis erfragt. Vorgegeben wurde als Verzeichnis:

```
/srv/shares/media/owncloud
```

Wenn hier ein anderes Verzeichnis genutzt werden soll, sollte darauf geachtet werden, dass das angegebene Verzeichnis im Bereich der File-Server Freigaben liegt.

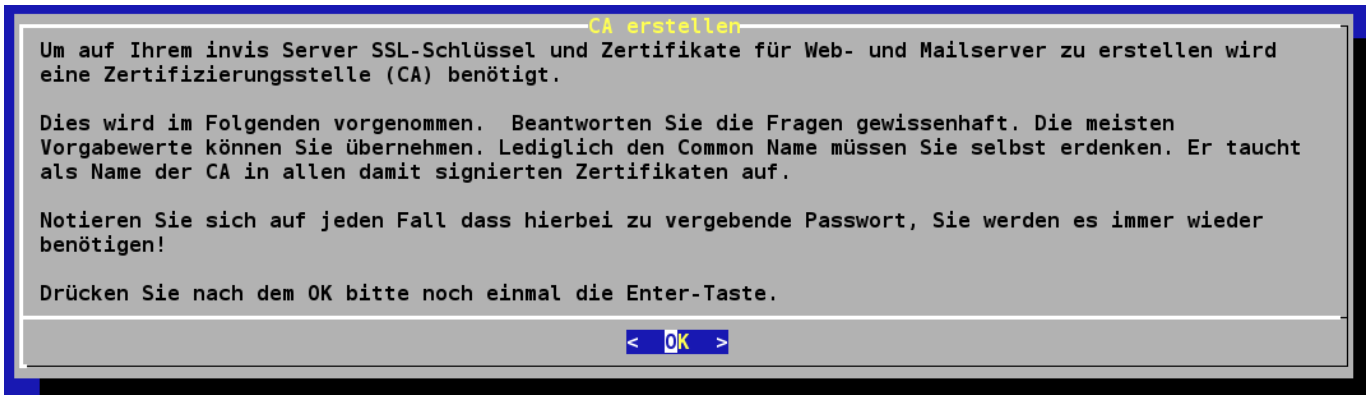
Zum Abschluss dieses Moduls zeigt ***sine*** Ihnen noch die verschobenen Ports für den externen SSH und HTTPs Zugriff auf den Server.



Das Verschieben dieser Ports ist als Schutz gegen unerwünschte automatisierte Login-Versuche an Ihrem Server gedacht. Auch wenn diese Ports schnell mit einem Portscanner gefunden werden können, hat sich gezeigt, dass die meisten Loginversuche von automatisierten Tools ausgehen, die lediglich auf den Standardports anfragen.

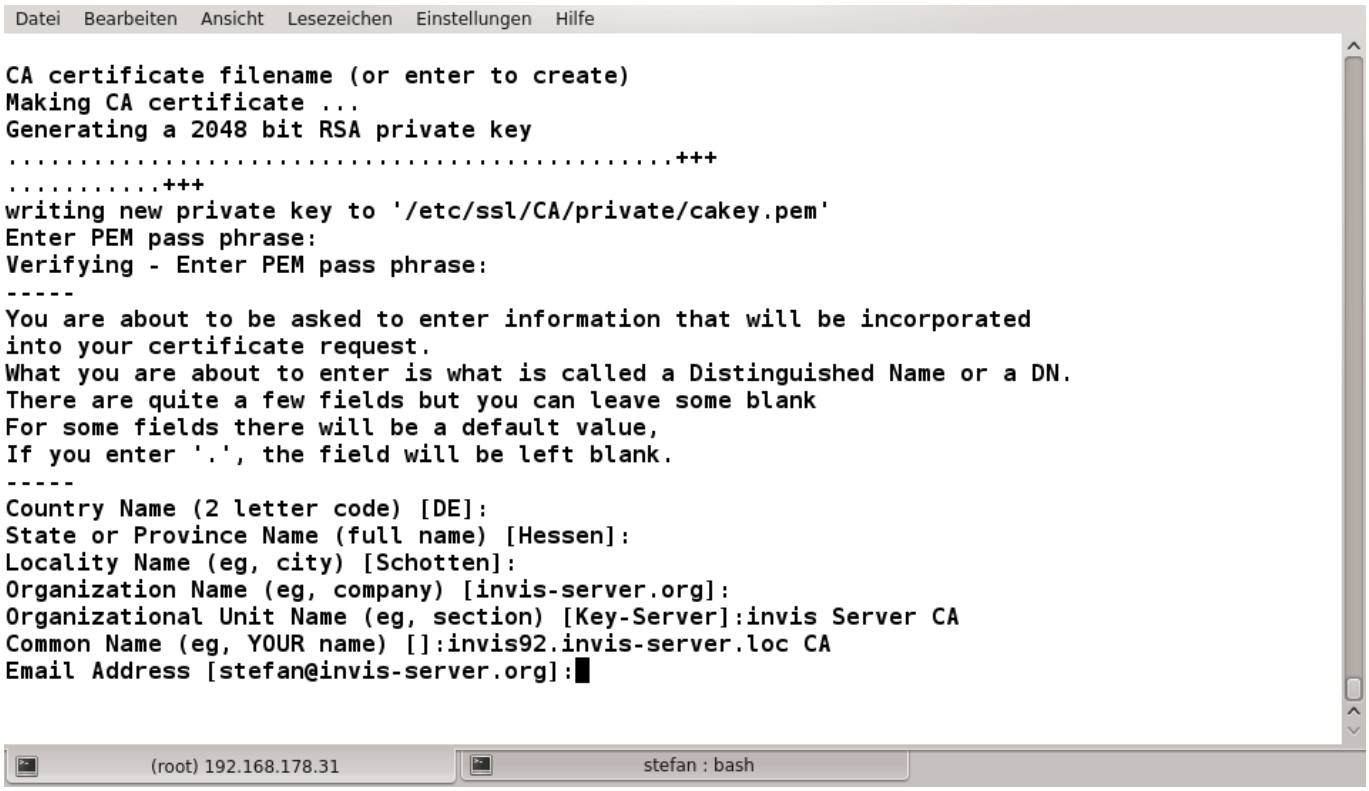
Modul: sysprep

Aufgabe dieses Moduls ist den invis Server vorzubereiten. Es legt zunächst, bevor irgendwelche Konfigurationsänderungen vorgenommen werden, ein Backup-Archiv Ihres /etc Verzeichnisses an. Weiterhin wird der Virenscanner installiert und die zugehörigen Dienste gestartet. Es wird eine CA (Certifikation Authority - Zertifizierungsstelle) zur Signierung selbst erzeugter Schlüssel angelegt. Im Verlauf dieses Arbeitsschrittes werden Ihnen einige Fragen gestellt, für die die meisten mit Vorgabewerten versehen sind. Die Vorgaben können Sie einfach mit „Enter“ übernehmen, alle anderen Fragen können Sie nach eigenem Ermessen beantworten.



Für die CA wird eine eigener „Private Key“ erzeugt, der mit einem Passwort versehen ist. Dieses Passwort müssen Sie sich ausdenken und eingeben. Sie sollten dies mitprotokollieren, da dieses Passwort im weiteren Verlauf des Scripts wie auch beim eigenen Erzeugen von weiteren Schlüsseln immer wieder benötigt wird. Dieses Passwort ist **NICHT** für jedermanns Augen bestimmt. Machen Sie dieses Passwort bekannt, ist Ihre CA mehr oder minder wertlos.

Achtung: *Nach dem bestätigen des im vorangegangenen Bild gezeigten Textes erscheint lediglich ein leerer Bildschirm. Damit es weitergeht muss zwingend noch einmal die Enter-Taste gedrückt werden.*



Das Modul installiert die ausgewählten Samba-Pakete, konfiguriert und startet den NTP-Dienst, richtet das Netzwerküberwachungstool „ntop“ ein und erledigt grundlegende Systemeinstellungen.

Modul: ldap (invis-server classic) bzw. ad (invis-server AD)

Classic

Dieses Modul richtet die LDAP-Umgebung für den invis-Server ein. Dazu gehört das Aufsetzen des Servers selbst, das einbinden der benötigten Schema-Dateien, das Anlegen des LDAP-Verzeichnisses sowie die Installation der smbldap-tools und phpLDAPAdmin, wichtigen Werkzeugen beim Verwalten des Verzeichnisses.

AD

Bezogen auf die AD-Variante des invis-Servers wird an dieser Stelle bereits die Active-Directory Domäne vollständig aufgebaut. D.h. das „Domain Provisioning“ wird bezogen auf die Classic-Variante vorgezogen. Die oben erwähnten smbldap-tools werden für die AD-Variante nicht benötigt.

Da der LDAP-Server auch verschlüsselt erreichbar sein soll wird ein entsprechendes Schlüssel/Zertifikats-Paar benötigt. Die Übergabe der für das Zertifikat notwendigen Informationen geschieht voll automatisch, Sie müssen lediglich zur Erstellung eines Sicherheitszertifikates das Passwort der Server-CA eingeben.

```
Es werden Schlüssel und Zertifikat für den ldap-Server "invis92.invis-server.loc" erzeugt.
/etc/ssl
Generating a 2048 bit RSA private key
...................+++
...................+++
writing new private key to 'server-key.pem'
-----
Using configuration from /etc/ssl/openssl.cnf
Enter pass phrase for /etc/ssl/CA/private/cakey.pem:
```

Anschließend werden Sie aufgefordert die Zertifikatsinformationen einer Sichtprüfung zu unterziehen und zu bestätigen, dass alle Angaben korrekt sind.

```
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 15448735250527764103 (0xd664eedc04c33e87)
        Validity
            Not Before: Jan  6 09:50:25 2014 GMT
            Not After : Dec 27 09:50:25 2015 GMT
        Subject:
            countryName               = DE
            stateOrProvinceName       = Hessen
            localityName              = Schotten
            organizationName          = invis-server.org
            organizationalUnitName    = ldap-Server
            commonName                = invis92.invis-server.loc
            emailAddress              = stefan@invis-server.org
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                24:FF:D6:CB:62:2E:98:ED:64:F6:C8:51:01:99:57:DD:55:85:C2:77
            X509v3 Authority Key Identifier:
                keyid:4E:22:11:EA:AB:1E:AC:31:96:0C:CE:C2:3D:A2:32:A0:68:85:F5:B5

Certificate is to be certified until Dec 27 09:50:25 2015 GMT (720 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```

Damit ist auch dieses Modul abgeschlossen.

Module: dns und dhcp

Auch diese beiden Module laufen ohne Ihr Zutun. Sie konfigurieren beide Serverdienste, legen die zugehörige Struktur im LDAP-Verzeichnis an und starten die Dienste.

Modul: mailserver

Das Modul Mailserver richtet in Abhängigkeit der von Ihnen gewählten Komponenten mit Postfix, Zarafa, Cyrus- oder Dovecot-IMAP, Amavisd-new, fetchmail und Mailman einige Dienste ein. Dabei ist Ihre Mitarbeit an mehreren Stellen gefordert.

Zunächst wird ein Schlüssel/Zertifikatspar für den Mailserver erstellt. Dies ermöglicht IMAP- und SMTP-Datenverkehr per TLS zu verschlüsseln und läuft in gleicher Weise wie beim Modul „ldap“ ab. Sie benötigen hier lediglich das Passwort Ihres CA-Schlüssels.

Abschließend wird das Mailinglisten System Mailman eingerichtet. Hier müssen Sie lediglich ein initiales Passwort sowie die email-Adresse des zuständigen Admins eingeben. (Mailman wird zukünftig aller Voraussicht nach aus dem Modul „mailserver“ entfernt und als eigenständiges optionales Modul angeboten.)

```
Neues Webseite Passwort:
Passwort best@tigen:
Passwort erfolgreich ge@ndert.
E-Mail-Adresse des Listenverwalters: domadmin@invis-server.loc
Erstmaliges Passwort f@r die Liste mailman:
Enter dr@cken, um den Besitzer der Liste mailman zu benachrichtigen...
```

Das Mailman Einrichtungswerkzeug versucht an den zuvor angegebenen Listen-Admin eine Email zu versenden. Wenn so wie im gezeigten Bild eine Email-Adresse eines noch nicht auf dem Server eingerichteten Benutzers eingegeben wurde, schlägt die Zustellung dieser Mail natürlich fehl. Das ist allerdings nicht wirklich von Belang.

Modul: cups

Dies Modul richtet, wie zu vermuten ist, den Druckserver CUPS ein. Auch dieses Modul ist ein Selbstläufer.

Modul: fileserver (samba & nfs)

Die Einrichtung eines LDAP/Samba-Domaincontrollers erledigt das Modul so gut wie selbsttätig. Dabei legt es die komplette Benutzer- und Gruppen-Struktur, wie in einer „Windows NT Domänenstruktur“ üblich an. Machen Sie sich später mittels phpLDAPAdmin (zu erreichen über den Administrationsbereich im invis Portal) mit der Struktur vertraut. Dabei entsprechen auch die Gruppen-IDs den entsprechenden RIDs aus der Windows-Welt.

Weiterhin legt das Script unter /srv/shares einige Freigaben (Verwaltung, Aktuell, Archiv, Gruppen, Media, Transfer) an. Diese sind in Abhängigkeit des gedachten Verwendungszwecks mit unterschiedlichen Zugriffsrechten versehen. Allen gemeinsam ist das gesetzte SGID-Bit, welches dafür sorgt, dass Dateien und Verzeichnisse die in einer Freigabe angelegt werden von dieser die besitzende Gruppe erben. Dies erleichtert das gruppenweise Zusammenarbeiten auf dem Fileserver. Schauen Sie sich auch dies fürs Verständnis einmal genauer an.

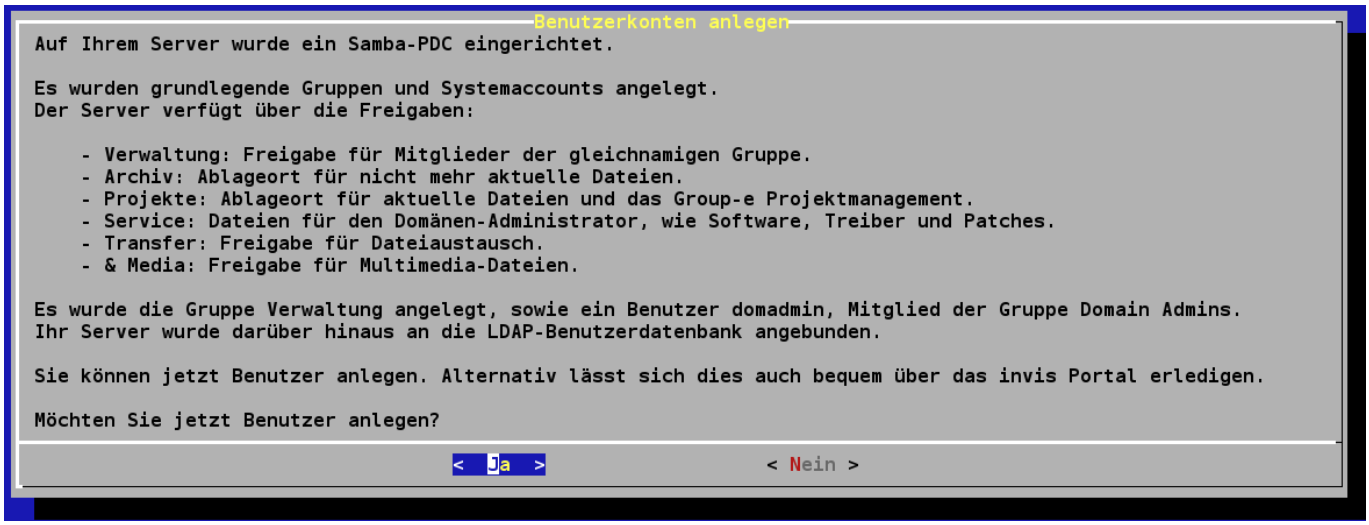
Alle Freigaben sind mit einem „Netzwerk-Papierkorb“ ausgestattet. D.H. alle von Anwendern in einer

Freigabe gelöschten Dateien und Ordner werden unter Beibehaltung der Verzeichnisstruktur in den Ordner „.recycle“ innerhalb der jeweiligen Freigabe verschoben. Um ein Überlaufen der Festplatten zu verhindern werden ältere Dateien automatisch vom Tool ***clean_recycle*** in regelmäßigen Abständen automatisch aus dem Papierkorb entfernt.

Während des Aufbaus der Domänenstruktur werden Sie nach dem Passwort des Benutzers „root“ sowie dem eines neu angelegten Users „domadmin“ und eines Benutzers „junk“ gefragt. Das root-Passwort benötigt Samba etwa um automatisch Maschinen-Konten anlegen zu können. Der User „domadmin“ ist, wie der Name vermuten lässt ein Windows-Domänenadministrator. Dieser hat auf allen der Domäne beigetretenen Windows-Clients Administrationsrechte, nicht aber auf dem Linux Server selbst. Der Benutzer „junk“ ist ein Dummy-User, an denn vom Mailserver als Spam eingestufte Emails gesendet werden.

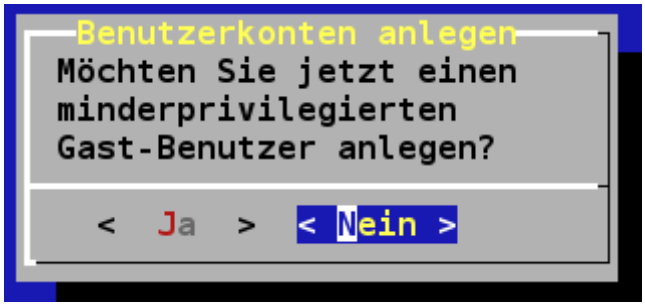
```
Changing UNIX password for junk
New password:
Retype new password:
```

Wenn die Domänen-Struktur steht, haben Sie hier im Script bereits die Möglichkeit nach belieben Benutzer anzulegen. Das Script unterscheidet zwischen normalen Domänen Benutzern, Verwaltungsmitgliedern (dürfen auf die Freigabe Verwaltung zugreifen) und Mail-Dummys (reine Linux-Benutzeraccounts, die sich nicht an Windows-PCs anmelden können). Sind alle Benutzerkonten nach Ihrem Wunsch angelegt, fragt das Script noch, ob es einen Gast-Account anlegen soll. Gäste können sich an Windows-Clients anmelden, haben aber so gut wie keine Rechte und dürfen nur auf die Freigabe Transfer zugreifen. Gedacht etwa als Accounts die nur im Internet surfen dürfen.



Hinweis: *Diese Funktion wird von uns seit längerem nicht mehr aktiv gepflegt. D.h. Sie sollten Benutzer über das Web-Portal des invis-Servers anlegen. Ignorieren Sie diese Möglichkeit hier einfach. Wir werden Sie sicherlich irgendwann aus* ***sine*** *entfernen.*

Es wird nachfolgend gefragt, ob Sie einen Gastbenutzer anlegen möchten. Auch dies ist nicht nortwendig.



Eine weitere Funktion dieses Moduls ist, den Server selbst als LDAP-Client via SSSD zu konfigurieren. Dies ist notwendig, danit sich die im LDAP angelegten Benutzer auch direkt am Server anmelden können. Testen Sie dies am besten mit einem beliebigen Benutzer aus. Schlägt die Anmeldung fehl sind einige Funktionen des Servers nicht verfügbar.

Achtung: *SSSD ist ein „caching“ Daemon. D.h. er speichert Benutzerinformationen aus dem LDAP zwischen. Leider funktioniert (in meinen Augen) das frisch halten des Caches nicht optimal. D.h. Es kann sein, dass sie für frisch angelegte Benutzer oder Gruppen erst nach einigen Minuten Wartezeit Zugriffsrechte im Dateisystem setzen können.*

Achtung*: Die Funktion Freigaben auch via NFS verfügbar zu machen ist in diesem Modul enthalten, wird aber nicht automatisch aktiviert. Dazu ist etwas manuelle Nacharbeit notwendig. (Siehe unten)*

Modul: web

Wie der Name vermuten lässt geht es hier um die Einrichtung des Webservers Apache, aber auch um die Installation des invis-Portals. Seit invis-Server Version 9.0 ist auch die Einrichtung des Dienstes „shellinabox“ Teil dieses Moduls. „shellinabox“ ermöglicht den SSH-Login am Server aus dem Webportal des invis-Servers heraus.

Die Webserver-Konfiguration basiert auf namensbasierten vhosts. ***sine*** richtet zwei vhosts eingerichtet, von denen einer für den regulären HTTP-Zugriff aus dem lokalen Netz heraus gedacht ist und der zweite für den HTTPs-Zugriff via Internet.

Der zweite vhost wird vom Script nur dann installiert, wenn im Modul „quest“ ein DynDNS-Name eingegeben wurde. (Beachten Sie diesbezüglich den Hinweis in der Beschreibung des quest-Moduls.)

Wird der vhost für den externen Zugriff eingerichtet, erstellt das Script einen Schlüssel/Zertifikat Satz. Auch hier benötigen Sie lediglich das Passwort des CA-Keys.

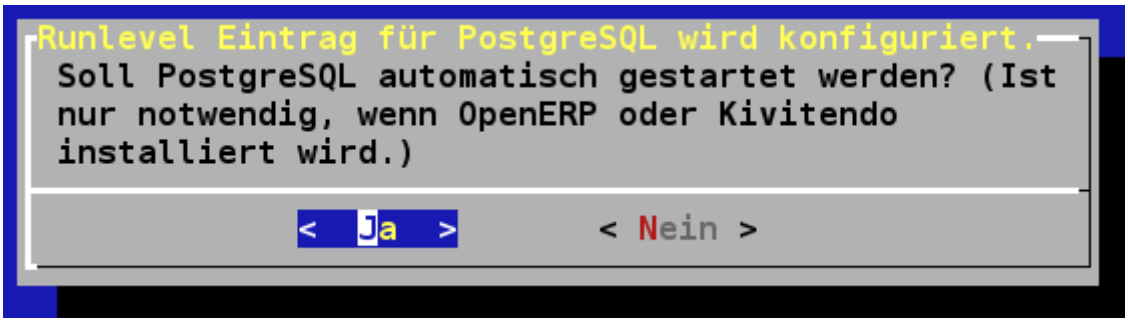
Module: mysqlserver und postgresqlserver

Das diese beiden Module genau das tun, was die Namen vermuten lassen dürfte selbstverständlich sein. Sie richten sowohl einen MySQL, bzw. ab Version 10.0 MariaDB als auch einen PostgreSQL Server ein.

Die Frage nache dem „Warum beide“ beantworte ich lieber bevor sie gestellt wird. Die in invis Server integrierte Groupware „Group-e“ setzt einen MySQL-Server voraus, während das Warenwirtschaftssystem Kivitendo schlicht PostgreSQL benötigt. Beide Systeme haben einfach unterschiedliche Stärken. So profitieren Group-e und Zarafa vermutlich von der Performance des Einen, während Kivitendo auf die Transaktionssicherheit des Anderen baut.

Hinweis: *Seit invis Version 7.0 wurde der Start des PostgreSQL Servers optional gestaltet. D.h. PostgreSQL wird installiert und konfiguriert, aber nur auf Wunsch gestartet.*

Hinweis: *Ab invis Server 10.0 (Active Directory) werden die Speicherreservicerungen für die InnoDB-Engine von MariaDB bzw. MySQL dynamisch berechnet und eingerichtet. Dabei kann es vorkommen, dass wenn viel RAM zur Verfügung steht beim ersten Start von MariaDB bzw. MySQL sehr große Dateien auf der Festplatte angelegt werden. Dies kann unter Umständen sehr lange dauern. Wenn es also so aussieht, als würde* ***sine*** *still stehen, haben Sie einfach noch ein wenig Geduld. Auch eine etwaige Fehlermeldung des Systemd bez. eines fehlgeschlagenen Start des Dienstes kann getrost ignoriert werden. Systemd fehlt es scheinbar an der notwendigen Geduld.*



Hinweis: *Seit openSUSE Version 12.x wurde MySQL durch MasiaDB ersetzt. Wird beim invis-Setup „Zarafa“ als Groupware ausgewählt, wird aufgrund einer Inkompatibilität allerdings wieder auf MySQL zurück gewechselt.*

Modul: firewall

Dieses Modul richtet die im openSUSE Lieferumfang enthaltene SuSEfirewall2 ein. Es ist ein Selbstläufer

Die Einrichtung einer Firewall würde ich aber niemals ohne Kontrolle einfach so einem Setup-Script überlassen.

Daher mein Tipp: *Machen Sie sich UNBEDINGT mit der zugehörigen Konfigurationsdatei*

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

vertraut. Nicht umsonst endete der einleitende Kommentar in dieser Datei lange Zeit mit den Worten „Good Luck“.

Wenn Sie selbständig Änderungen an der Firewall-Konfiguration vornehmen, können Sie diese Änderungen mit:

```
linux:~ # rcSuSEfirewall2 reload
```

übernehmen.

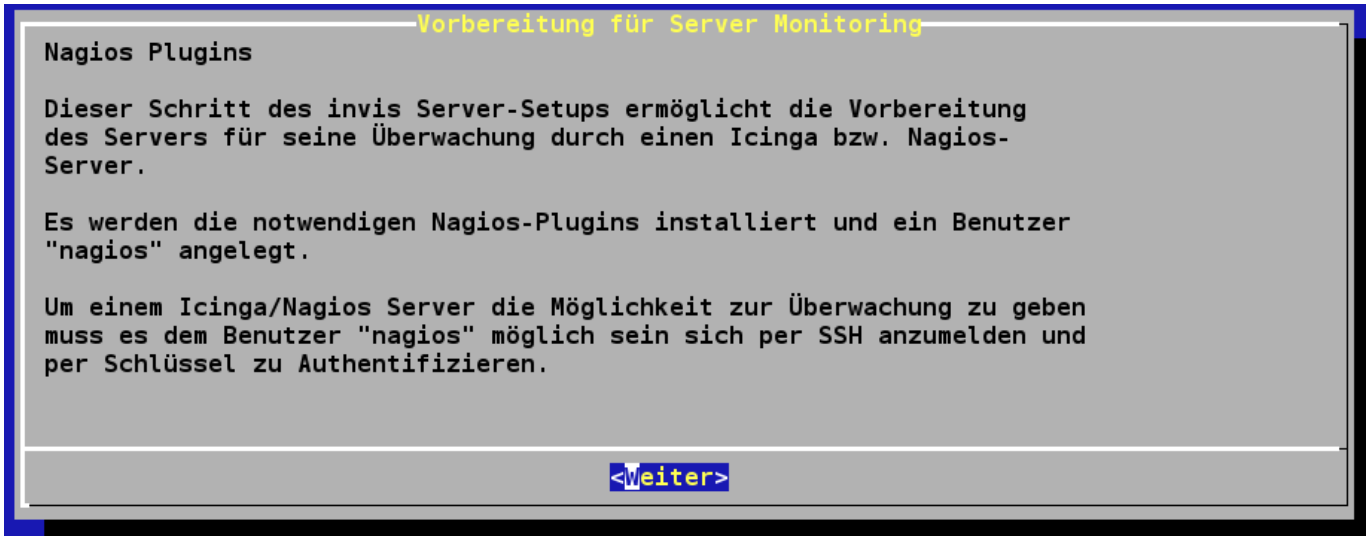
Achtung: *Nach Abschluss dieses Moduls ist Ihr Server per SSH nur noch auf dem vom Modul „quest“ ausgegebenen verschobenen SSH-Port erreichbar.*

Optionale Module

Bei allen nachfolgend beschriebenen Modulen haben Sie die Möglichkeit die jeweilige Installation zu überspringen. Sie bekommen zu Beginn des Moduls einen kurzen Text eingeblendet, der die vom Modul einzurichtende Software beschreibt. Im Anschluss daran werden Sie gefragt, ob sie die jeweilige Installation wünschen oder nicht.

Modul: nagios

Wenn Sie planen Ihren invis-Server mit einem Monitoring-System wie Icinga oder Nagios zu überwachen, benötigen Sie einen Satz an Nagios-Plugins. Das Modul „nagios“ installiert einen gängigen Satz an Plugins.



Zusätzlich zur Installation der Plugins wird ein Benutzer namens „nagios“ angelegt, der für den Zugang eines Monitoring-Servers genutzt werden sollte.

Modul: groupware

Dies ist das zweite optionale Modul im Script. Da jedoch ein Backoffice Server ohne brauchbares Groupware-System nur eine halbe Sache ist, würde ich dieses Modul nicht überspringen. Jedenfalls stellt dieses Modul - wie auch alle folgenden - zu Beginn die Frage, ob Sie es ausführen möchten.

Abhängig von der im Modul „quest“ getroffenen Entscheidung bezüglich Groupware und IMAP-Server wird hier ***Group-e***, ***Zarafa*** oder ***SoGo*** zur Installation vorgeschlagen.

Zarafa

Installiert wird immer die aktuelle Open-Source-Version des Zarafa-Servers inklusive Webaccess und modernerer Webapp.

Um Outlook anbinden zu können ist die Installation des Zarafa-License-Daemons notwendig, der nicht Bestandteil der openSUSE Pakete ist und von uns auch für openSUSE nicht als RPM-Paket zur Verfügung gestellt werden kann. Statt dessen bieten wir den License-Daemon als Erweiterungspaket

auf der invis-Server Website zum gesonderten Download an.

Wenn Sie Zarafa als Groupware gewählt haben, erfolgt keine Abfrage, ob Sie den Durchlauf dieses Moduls wünschen oder nicht. Dies ist so beabsichtigt, da Zarafa Teile der Mailserver-Funktionen integriert mitbringt. D.h. ohne Zarafa Installation, würde der invis-Server nicht funktionieren.

Group-e

Ist alle Software installiert wird eine MySQL-Datenbank für Group-e eingerichtet. Diese Prozedur verlangt ganze drei mal hintereinander die Eingabe des MySQL-Root Passwortes. (Dies geschieht nicht um Sie zu ärgern.)

Gegen Ende des Modul-Durchlaufs wird noch ein Mail-Dummy User für die Projektverwaltung der Groupware angelegt, Ihre Aufgabe hierbei ist lediglich die Vergabe eines Benutzerpasswortes.

Um von der Vorinstallation zu einer Nutzbaren Group-e Installation zu gelangen lesen Sie bitte im Kapitel „Nacharbeit“ den Abschnitt „Group-e“,

SoGo

Beschreibung folgt…

Modul: erp

Nr. 2 aus der Reihe der optionalen Module installiert das zu Beginn gewählte Warenwirtschafts- bzw. ERP-Systems.

Zur Auswahl stehen die Systeme:

- WaWision
- Kivitendo

Während das WaWision-Setup an dieser Stelle vollständig automatisch abläuft, erfordert Kivitendo ein bisschen Unterstützung.

waWision

Nach der Installation des waWision Software-Paketes wird eine leere MySQL-Datenbank nebst zugehörigem Benutzer angelegt. ***sine*** zeigt Ihnen die Zugangsdaten:

Notieren Sie sich diese Informationen, Sie werden beim späteren Vervollständigen des Setups benötigt.

Kivitendo

Nach der Installation der Kivitendo-ERP Pakete, wird ein PostgreSQL-Datenbank Benutzer unter dem Namen „kivitendo“ angelegt. Für diesen müssen Sie sich selbstverständlich wieder mal ein Passwort ausdenken. Die Eingabe des Passwortes ist doppelt erforderlich, einmal beim Anlegen des Benutzers selbst und danach noch einmal für die Kivitendo-Konfiguration. Achten Sie darauf, dass Sie in beiden Fällen das gleiche Passwort eingeben.

Im Anschluss daran müssen Sie sich für eine Authentifizierungsmethode entscheiden, ich empfehle die Vorgabe „SQL“ zu übernehmen, Erläuterungen dazu finden Sie im Kapitel „Nacharbeit“ dieser Anleitung, im Abschnitt „LX-Office“

Damit ist auch dieses Modul abgearbeitet.

Modul: faxgate

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.*

Achtung: *Seit invis 8.0-R1 funktioniert das Modul nicht mehr vollständig, da Foehr-IT keine fcpci-Kernelmodule für den Kernel für openSUSE ab 12.2 bereit hält. Die Treiber müssen manuell herunter geladen und installiert werden, alles andere kann das Faxgate-Modul erledigen. Die Kernel-Module sind* ***hier*** *zu finden.*

Dieses Modul setzt einen CAPI-basierten Faxserver auf. Das setzt voraus, dass Ihr zukünftiger invis Server über eine FritzCard PCI verfügt (andere Modelle haben wir nie getestet). Alternativ funktioniert es auch mit einer FritzCard DSL einer Kombination aus ISDN-Karte und DSL-Modem, die allerdings im Handel nicht mehr erhältlich ist.

Das Script erkennt den Typ der eingesetzten FritzCard selbständig, läd das entsprechende Kernel-Modul von Foehr IT herunter und installiert es automatisch. Verwendet wird dazu das Tool ***fcinst*** aus der invis Toolbox. Sie können dieses Script auch direkt benutzen, beispielsweise für ein Update des FritzCard-Treibermoduls, etwa nach einem Kernel-Update.

Ist das Kernel-Modul erfolgreich installiert, müssen Sie wieder einmal der Installation zusätzlicher

Software zustimmen.

Im Anschluss an die Software-Installation müssen Sie festlegen, ob Sie Ihren Fax-Server im Single- (Vorgabe) oder Multiuser-Betrieb nutzen möchten. Der Singleuser-Betrieb geht von einer einzigen Faxnummer aus, alle auf dieser Nummer eingehenden Faxe werden im PDF-Format per Mail an einen speziell für diesen Zweck eingerichteten Benutzer „fax“ gesendet. Diese Konfiguration dürfte vor allem in Verbindung mit einem ISDN-Mehrgeräteanschluss das Mittel der Wahl sein.

Im Gegenzug dazu macht die Multiuser-Konfiguration mit ISDN-Anlagenanschlüssen Sinn, bei denen aus einem großen Rufnummern-Pool Mitarbeitern einzelne Faxnummern zugewiesen werden können. In diesem Fall werden eingehende Faxe im PDF-Format per Mail direkt an den entsprechenden Benutzer gesendet.

Wird der Singleuser-Betrieb gewählt legt das Script den Benutzer „fax“ selbst an - Sie werden hierbei natürlich nach einem Passwort gefragt.

Unabhängig vom Betriebsmodus wird für den Faxversand eine entsprechende CUPS-Druckerwarteschlange unter dem Namen „faxgate“ eingerichtet. Dieser Drucker steht auch via Samba zur Verfügung.

Die individuelle Einrichtung des Fax-Servers, wie etwa die Eingabe der Faxnummern geschieht per YaST. Mehr dazu im Kapitel „Nacharbeit“, Abschnitt „Fax-Server“

Modul: webcdwriter

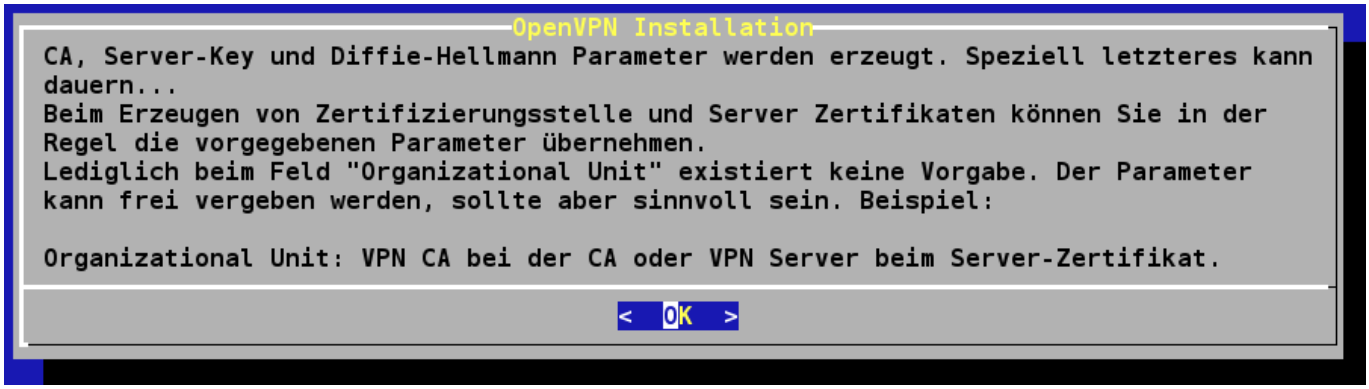
Diese Modul läuft völlig automatisch. Es installiert den Java-basierten Webcdwriter nebst zugehöriger Server-Sorftware. Dieses Software-Paket ermöglicht die Nutzung des CD/DVD-Brenners Ihres Servers via Netzwerk, also von jedem Arbeitsplatz aus.

Hinweis: in der hier installierten Open Source Version ist lediglich das Brennen von CDs möglich. Das Brennen von DVDs verlangt ein kostenpflichtiges Update. Mehr Infos dazu auf Internet-Seite des Autors.

Modul: openvpn

Dieses Modul installiert die beliebte Open Source VPN-Lösung openVPN, die es Ihnen ermöglicht von Unterwegs via Internet auf Ihren Server bzw. Ihr Netzwerk zuzugreifen.

Zunächst wird auch hier weiterere Software installiert. Ist diese Installation abgeschlossen wird (auch wenn dies widersinnig erscheinen mag) eine zweite CA (Zertifizierungsstelle) speziell für openVPN eingerichtet.



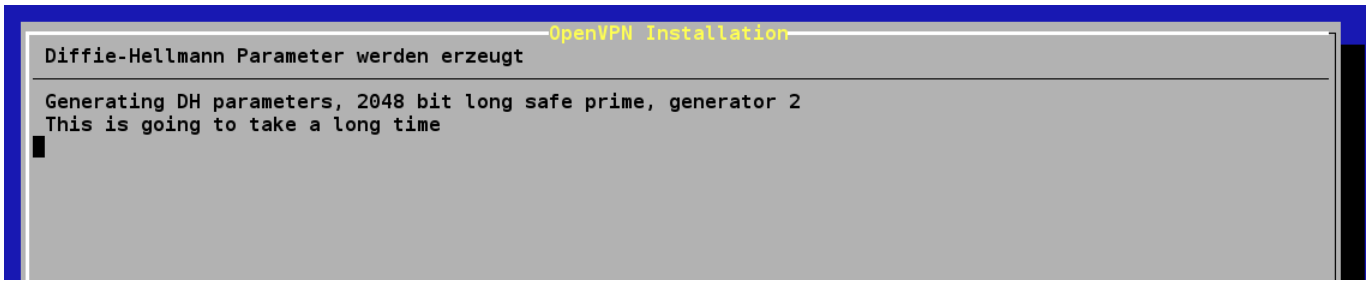
Sinnvoll ist dies, weil die Erzeugung von Schlüsseln und Zertifikaten für openVPN-Server und Clients mit anderen Vorgaben geschieht als bei den Schlüsseln für den Rest des Servers. Zum Einsatz kommt hier „easyRSA“ ein leicht zu handhabendes Werkzeug zur Verwaltung der Schlüssel.

Sowohl beim Erzeugen der CA, als auch beim Generieren des Schlüssel/Zertifikats-Paares für den VPN-Server selbst, stellt das Script (genauer gesagt easyRSA) einige vermutlich schon bekannte Fragen. Die Vorgabewerte sind Ihren Eingaben im Modul „quest“ entnommen und können somit ohne Weiteres akzeptiert werden. Verändern müssen Sie nur wenige Einstellungen, der für den Server entscheidende „Common Name“ wird aus den vorherigen Eingaben bereits als Vorgabe verwendet und darf nicht geändert werden.

Zunächst wird die CA erzeugt:

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/invis-server.loc/keys
Generating a 2048 bit RSA private key
..............................+++
..........................+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [Hessen]:
Locality Name (eg, city) [Schotten]:
Organization Name (eg, company) [invis-server.org]:
Organizational Unit Name (eg, section) [changeme]:VPN Server
Common Name (eg, your name or your server's hostname) [changeme]:dummy.invis-server.org VPN CA
Name [Stefan Schaefer]:
Email Address [stefan@invis-server.org]:
```

Danach werden auf Primzahlen basierende Diffie-Hellmann Parameter berechnet, was eine Weile dauern kann. Wenn sich auf dem Bildschirm scheinbar nichts tut ist das durchaus normal. Haben Sie Geduld.



Zum Abschluss wird noch das Schlüssel/Zertifikatspaar des Servers selbst erzeugt:

```
Generating a 2048 bit RSA private key
.............................................+++
...............+++
writing new private key to 'dummy.fsproductions.de.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [Hessen]:
Locality Name (eg, city) [Schotten]:
Organization Name (eg, company) [invis-server.org]:
Organizational Unit Name (eg, section) [changeme]:VPN Server
Common Name (eg, your name or your server's hostname) [dummy.fsproductions.de]:
Name [Stefan Schaefer]:
Email Address [stefan@invis-server.org]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/invis-server.loc/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
stateOrProvinceName   :PRINTABLE:'Hessen'
localityName          :PRINTABLE:'Schotten'
organizationName      :PRINTABLE:'invis-server.org'
organizationalUnitName:PRINTABLE:'VPN Server'
commonName            :PRINTABLE:'dummy.fsproductions.de'
name                  :PRINTABLE:'Stefan Schaefer'
emailAddress          :IA5STRING:'stefan@invis-server.org'
Certificate is to be certified until Jan  9 12:42:56 2024 GMT (3650 days)
Sign the certificate? [y/n]:
```

Danach wird der openVPN Dienst gestartet. Mit „ifconfig“ können Sie dies im Anschluss geprüft werden:

```
invis92:~ # ifconfig
extern    Link encap:Ethernet  Hardware Adresse 08:00:27:39:26:91
          inet Adresse:192.168.240.207  Bcast:192.168.240.255  Maske:255.255.255.0
          inet6 Adresse: fe80::a00:27ff:fe39:2691/64 Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8877 errors:0 dropped:631 overruns:0 frame:0
          TX packets:5852 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:1000
          RX bytes:9923493 (9.4 Mb)  TX bytes:550205 (537.3 Kb)

intern    Link encap:Ethernet  Hardware Adresse 08:00:27:D8:1C:50
          inet Adresse:192.168.123.10  Bcast:192.168.123.255  Maske:255.255.255.0
          inet6 Adresse: fe80::a00:27ff:fed8:1c50/64 Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:1000
          RX bytes:0 (0.0 b)  TX bytes:12852 (12.5 Kb)

lo        Link encap:Lokale Schleife
          inet Adresse:127.0.0.1  Maske:255.0.0.0
          inet6 Adresse: ::1/128 Gültigkeitsbereich:Maschine
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:6250 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6250 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:0
          RX bytes:884054 (863.3 Kb)  TX bytes:884054 (863.3 Kb)

vpn       Link encap:UNSPEC  Hardware Adresse 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet Adresse:192.168.166.1  P-z-P:192.168.166.2  Maske:255.255.255.255
          UP PUNKTZUPUNKT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

invis92:~ #
```

Es muss eine Netzwerkschnittstelle namens „vpn“ angezeigt werden.

Mehr zur Einrichtung des openVPN-Servers sowie der Erzeugung der Schlüssel für VPN-Clients im Kapitel „Nacharbeit“, Abschnitt „VPN-Server“.

Modul: dokuwiki

Dieses Modul installiert das einfache und Ressourcen-schonende Wikisystem „Dokuwiki“, nebst dem Monoboot-Template. Optisch ist es damit kaum vom bekannten Mediawiki zu unterscheiden. Es benötigt allerdings keine SQL-Datenbank und verfügt von Haus aus über eine Benutzerverwaltung mit ACLs.

Auch die Einrichtung von Dokuwiki erfordert etwas „Nacharbeit“, mehr dazu im Abschnitt „Dokuwiki konfigurieren“.

Modul: etherpad

Hinweis: *Das Modul* ***etherpad*** *ist derzeit in allen invis-Versionen (9.2, 10.1 und 10.2) aufgrund von Inkompatibilitäten mit „nodejs“ deaktiviert. Ob und/oder wann wir es wieder zum Leben erwecken ist derzeit unbestimmt.*

Funktionaler Neuzugang im invis-Server Funktionsumfang ist die Software Etherpad-Lite. Sie ist dazu

gedacht mit mehreren Personen simultan an Texten zu arbeiten. Die Texte können in verschiedene Formate, darunter auch Dokuwiki exportiert werden. Sehr praktisch vor allem, wenn dezentral und dennoch im Team gearbeitet werden soll.

Dieses Modul verlangt lediglich einmal die Eingabe des MySQL-root Passwortes.

Modul: owncloud

Dieses Modul installiert ownCloud. Der wesentliche Teil der des Setups muss allerdings manuell vorgenommen werden. Siehe Abschnitt Nacharbeit „ownCloud“.

Das Modul legt eine Datenbank an und gibt, genau wie im Modul Wawision deren Zugangsdaten aus. Notieren Sie sich diese, sie werden für den manuellen Abschluss der onwCloud Installation benötigt.

Modul: virtualbox

Dieses Modul läuft vollkommen automatisch ab. Für die Verwendung von VirtualBox steht nach der Installation im invis-Portal im Bereich „Administration“ das Tool „phpVirtualBox“ zur Verfügung.

Fertig

Ist das Modul „openvpn“ erfolgreich abgearbeitet, haben Sie es geschafft - Ihr Server ist bereits weitestgehend einsatzbereit.

Um von „weitestgehend“ zu „vollständig“ zu gelangen lesen Sie einfach den folgenden Abschnitt.