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 verfügt über 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.

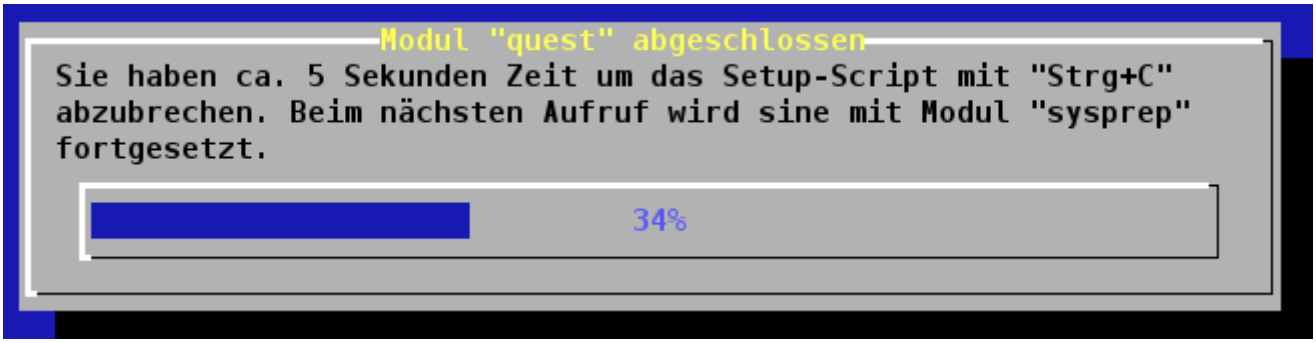
Alle vorbereiteten Konfigurationsdateien für das invis-Setup sind im Zuge des Umbaus zur RPM-basierten Installation nach

```
/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.

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.



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: ***monitoring, groupware, erp, webcdwriter, faxgate, openvpn, dokuwiki*** *und* ***owncloud.***

Weiterhin wird zwischen **interaktiven** und **automatischen** Modulen unterschieden. Interaktive verlangen Eingaben durch den Benutzer, automatische Module tun das nicht.

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 unserer Mailingliste - es beisst nicht! Die Sache mit „Sche*, das funktioniert nicht“ abzubrechen hilft niemandem.

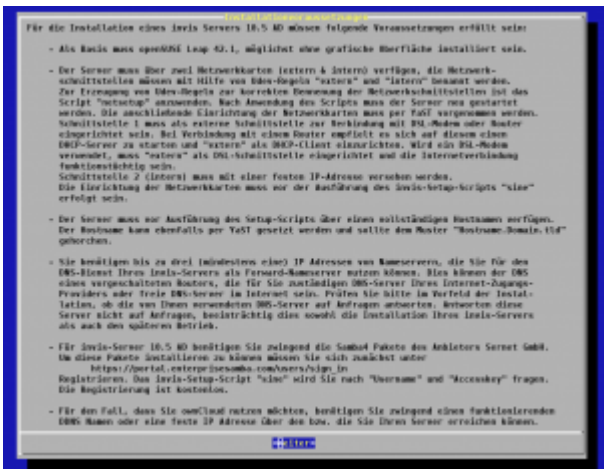
Hinweis: *Dokumentieren Sie die von Ihnen während des Scriptlaufs eingegebenen Daten mit. Das erleichtert die spätere Administration des Servers.*

Die Module im Einzelnen (Pflichtmodule)

Nachfolgend werden die einzelnen Module in Reihenfolge des Scriptlaufs erläutert. Der Name des jeweiligen Moduls wird immer bei dessen Start kurz angezeigt.

Modul: check

Typ: automatisch Das Modul „check“ fragt lediglich nach, ob alle hier beschrieben Voraussetzungen für das invis-Server Setup mit ***sine*** erfüllt sind. Wird diese Frage verneint, bricht das Script einfach ab.



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

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

Modul: quest

Typ: interaktiv

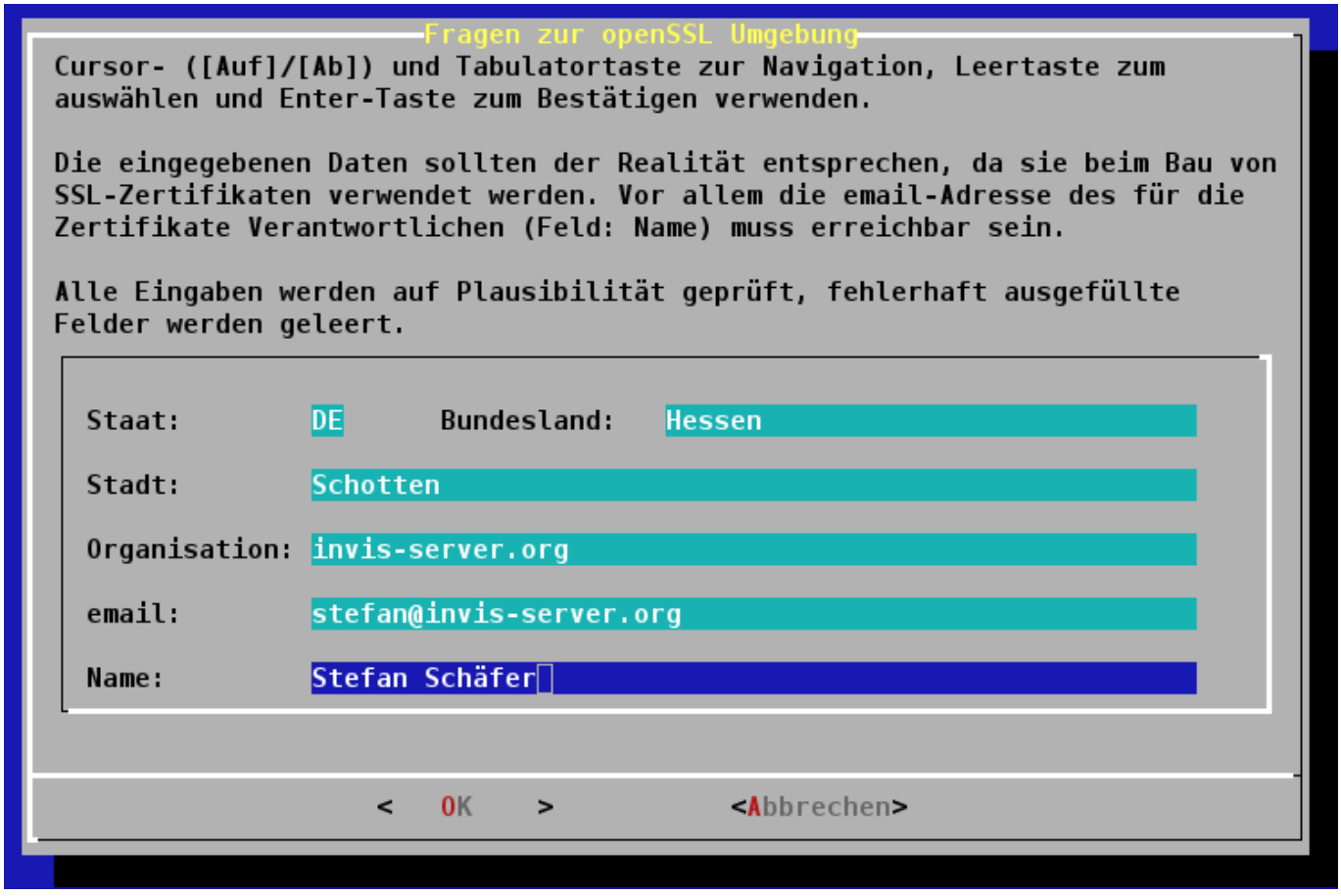
Aufgabe des Moduls „quest“ ist es Umgebungsdaten des Servers von Ihnen zu erfragen und für den weiteren Verlauf des Setups zu speichern. Gespeichert werden die abgefragten Informationen im Arbeitsverzeichnis von ***sine***, sie können später mit:

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

abgefragt werden.

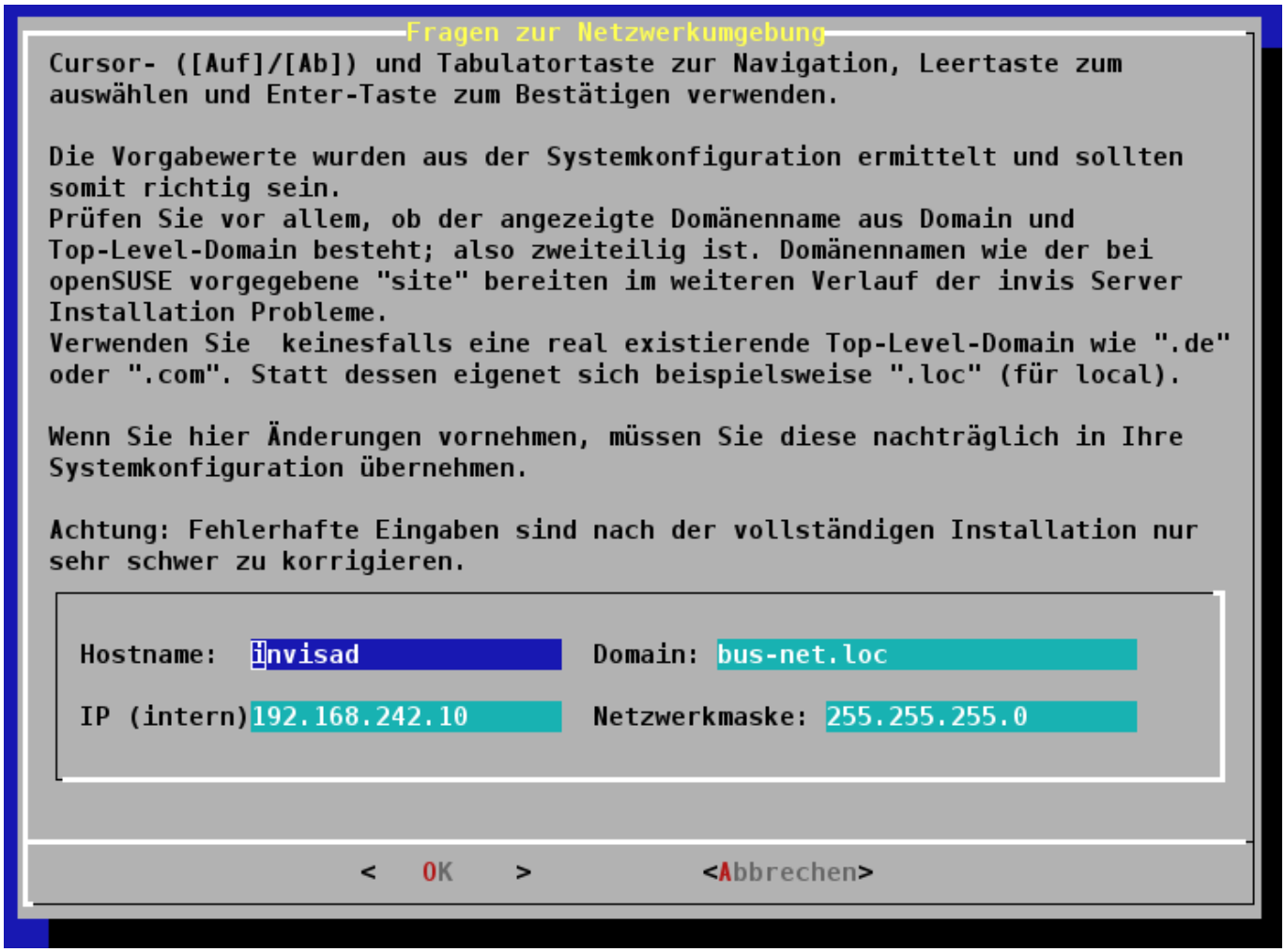
Es ist wichtig hier genau aufzupassen und korrekte Informationen einzugeben. Einige Informationen wie etwa die konfigurierten IP-Adressen und den Hostnamen versucht ***sine*** selbst zu ermitteln. Das Modul zeigt diese Informationen an. Prüfen Sie die Ausgaben bitte genau. Sollten wiedergegebene Informationen falsch oder Ausgabefelder leer sein, sollten Sie das Script abbrechen und die entsprechenden Konfigurationen korrigieren.

Die Fragestunde beginnt mit der Abfrage von Informationen für die Server-eigene CA (Zertifizierungsstelle) und PKI (Public Key Infrastructure).



Die hier von Ihnen eingegebenen Informationen werden später in jedem Server-Zertifikat sowie dem Stammzertifikat der Zertifizierungsstelle hinterlegt. Die Informationen können von jedem Client, beispielsweise Ihrem Browser angezeigt werden, sie sollen Authentizität vermitteln und somit Vertrauen schaffen. Geben Sie hier bitte ernstzunehmende Daten und keinen „Blödsinn“ ein. Blödsinn schafft kein Vertrauen.

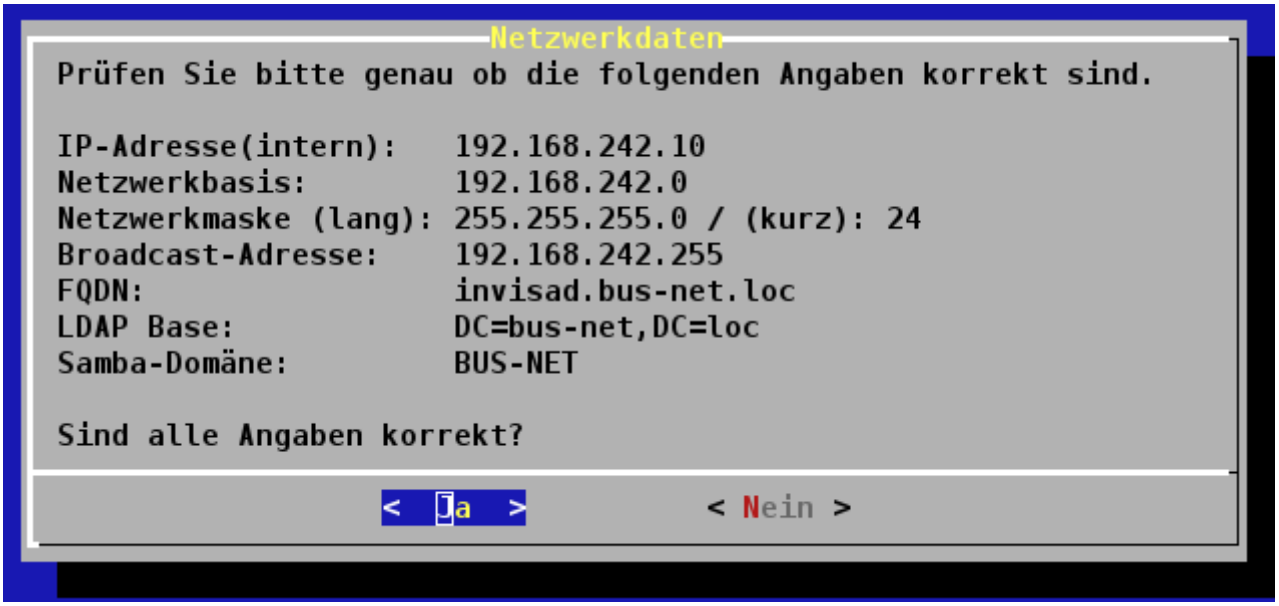
Im nächsten Schritt versucht ***sine*** Informationen über die Netzwerkkonfiguration Ihres Servers zu ermitteln und zeigt diese an:



Sollten hier einzelne Felder leer sein, wurde die Netzwerkkonfiguration des Servers nicht wie im Abschnitt Basis Installation beschrieben vorgenommen. Dies wirkt sich in aller Regel negativ auf den weiteren Verlauf des Setups wie auch den Betrieb des Servers aus. Sie können die fehlenden Daten hier eingeben, müssen aber dennoch das Setup am Ende des „quest“ Moduls abbrechen und die Netzwerkkonfiguration in YaST vervollständigen.

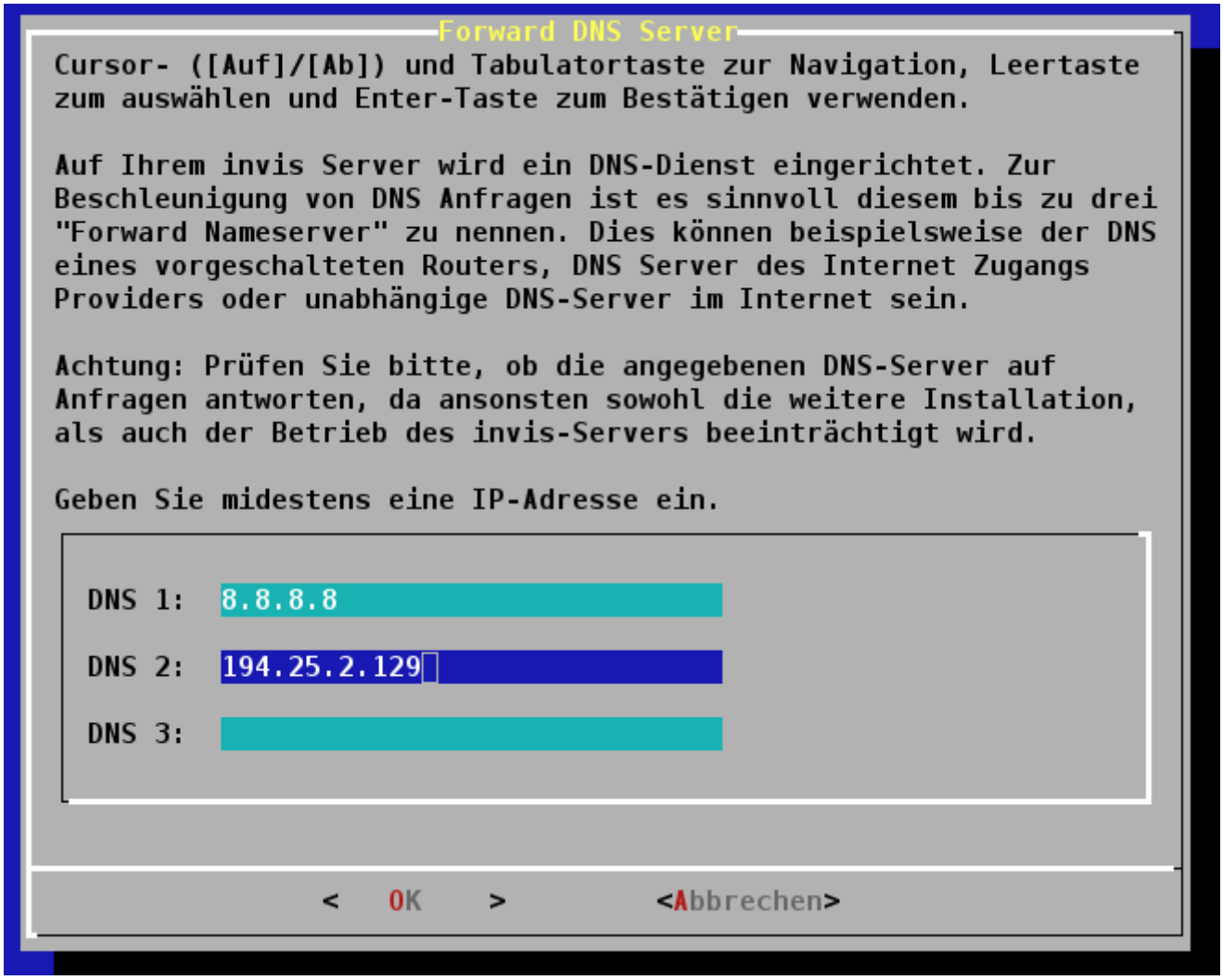
Achten Sie auch darauf, dass die hier angezeigte Domain sich aus Domain und Top-Level-Domain also „domain.tld“ besteht. Fehlt die TLD führt dies auch zu massiven Folgefehlern.

Aus den angezeigten bzw. eingegebenen Informationen berechnet ***sine*** weitere Informationen, die als Variablen für das weitere Setup gespeichert werden.



Beantworten Sie die hier gestellte Frage mit „Nein“, wird das Setup **aus gutem Grund** abgebrochen.

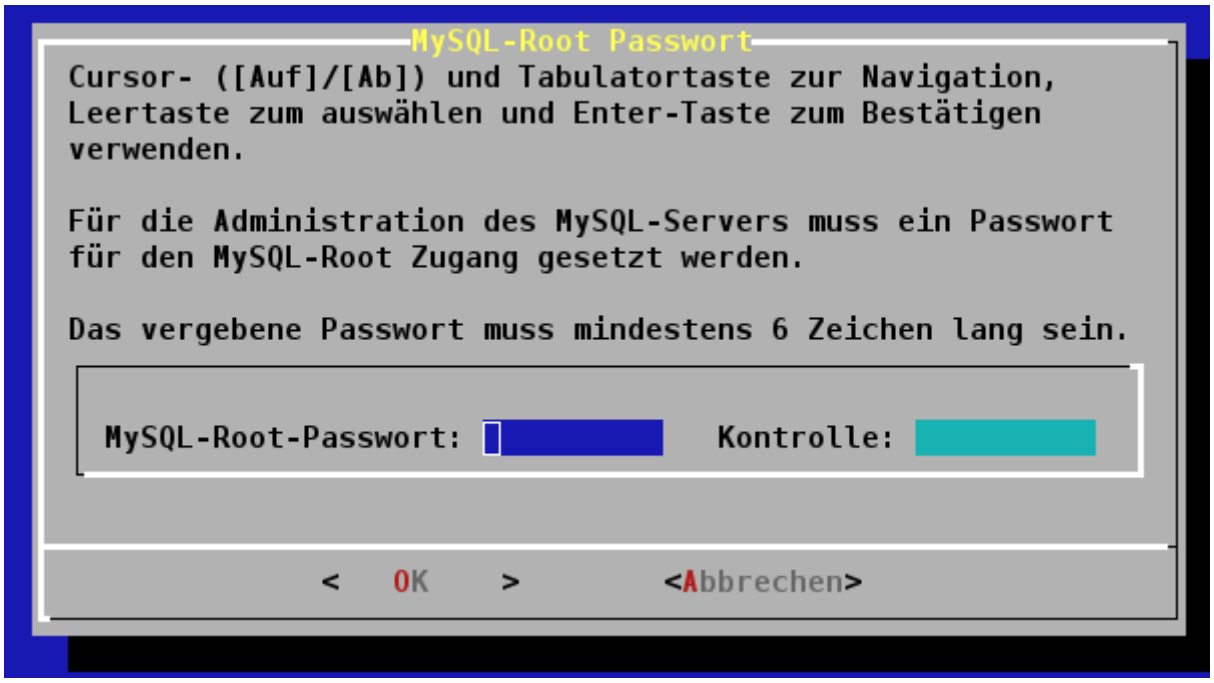
Weiter geht es mit der Abfrage der Forward-Nameserver.



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.

Auf einem invis-Server läuft immer ein MySQL/MariaDB-Server als Dantenbank-Backend für verschiedenste Applikationen. Der SQL-Dienst verfügt über eine eigene Benutzerverwaltung und eigenem „root“-Konto. Dieses Konto muss mit einem Passwort abgesichert werden.



Geben Sie das gewünschte Passwort ein.

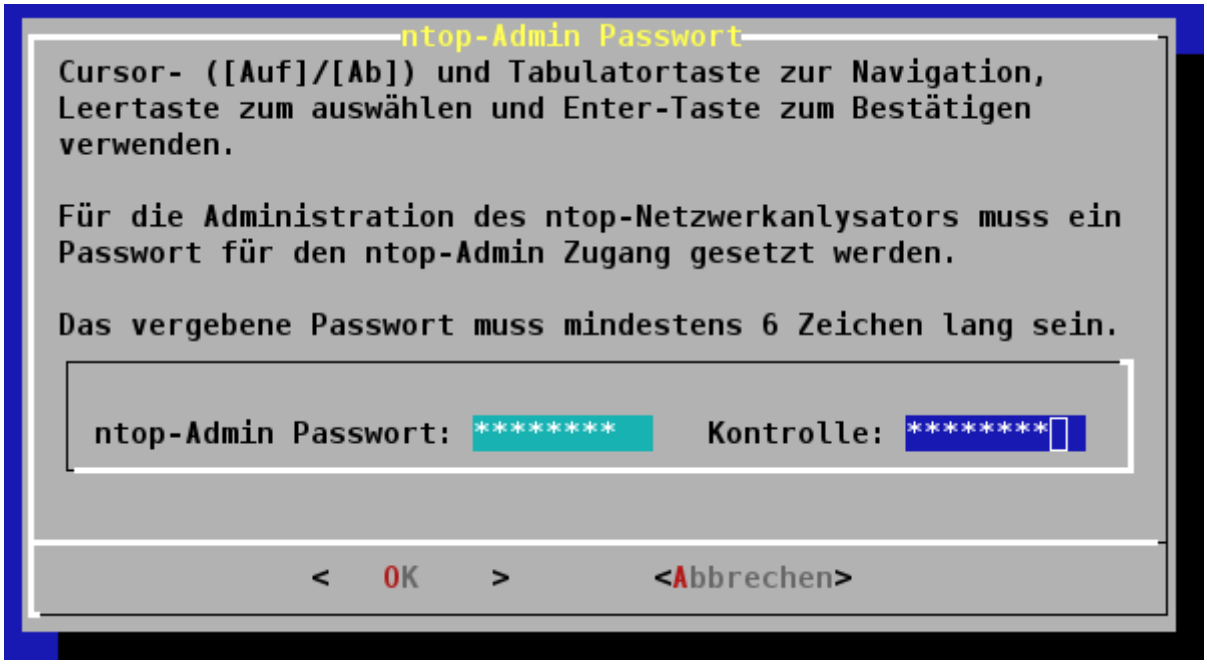
Es folgt die Frage nach der gewünschten Groupware:

Zur Auswahl stehen prinzipiell 4 verschiedene Kombinationen aus IMAP-Server und Groupware. Achten Sie unbedingt auf die Bemerkungen rechts neben der Auswahl. Noch sind für den invis-Server

Active Directory noch nicht alle geplanten Kombinationen verfügbar. Wir arbeiten daran. Derzeit (Stand: April 2016) sind lediglich Zarafa oder die Kombination aus Dovecot und Roundcubemail voll integriert.

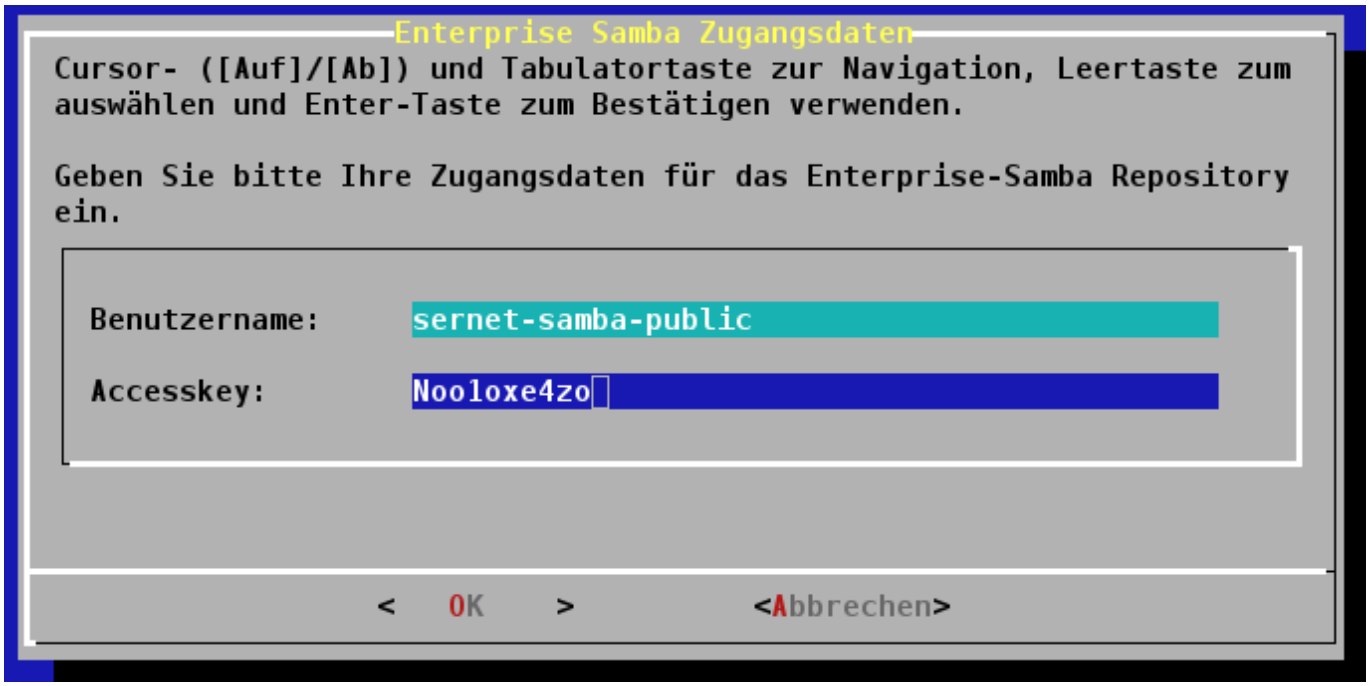
Hinweis: *Eine Installation des invis-Server ohne Groupware/Mailserver-System ist* ***nicht*** *vorgesehen. Es ist eine elementare Funktion des invis-Servers.*

Auf allen invis-Servern wird die Software **ntop**, ein Netzwerkanalyse-Werkzeug mit Weboberfläche, installiert. Auch **ntop** wird mit einem Passwort abgesichert, welches im nächsten Schritt abgefragt wird.



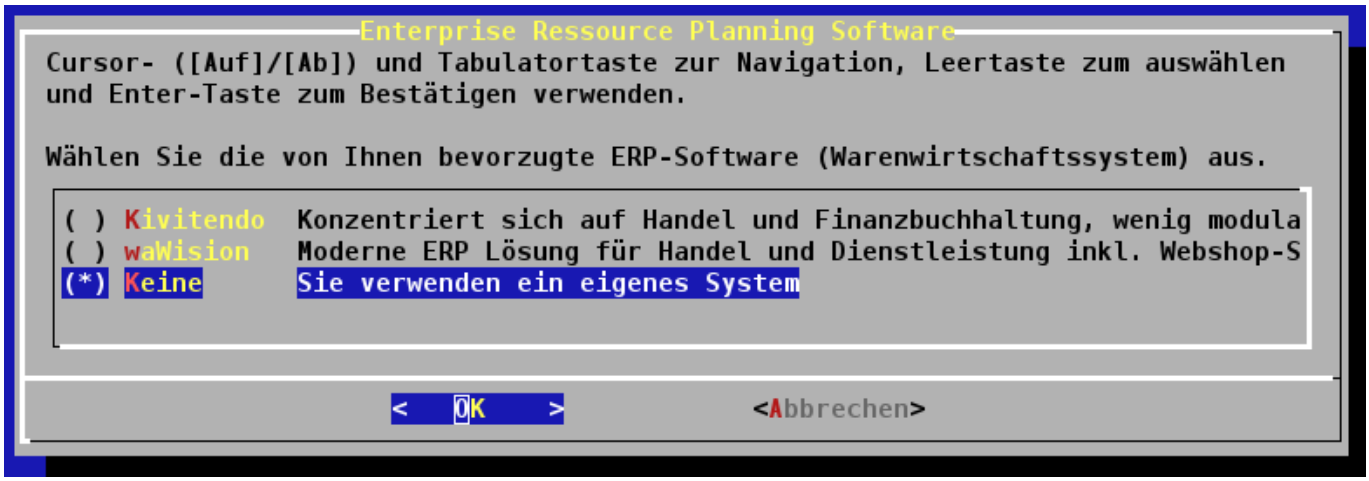
Hinweis: ***ntop*** *wird installiert aber nicht automatisch gestartet, da es sich negativ auf die Netzwerk-Performance auswirkt. Wenn Sie* ***ntop*** *beispielsweise zur Fehleranalyse benötigen, müssen Sie es im Bedarfsfall manuell starten.*

Von elementarer Bedeutung ist die jetzt folgenden Abfrage nach Zugangsdaten zum Samba-Repository der Fa. Sernet.



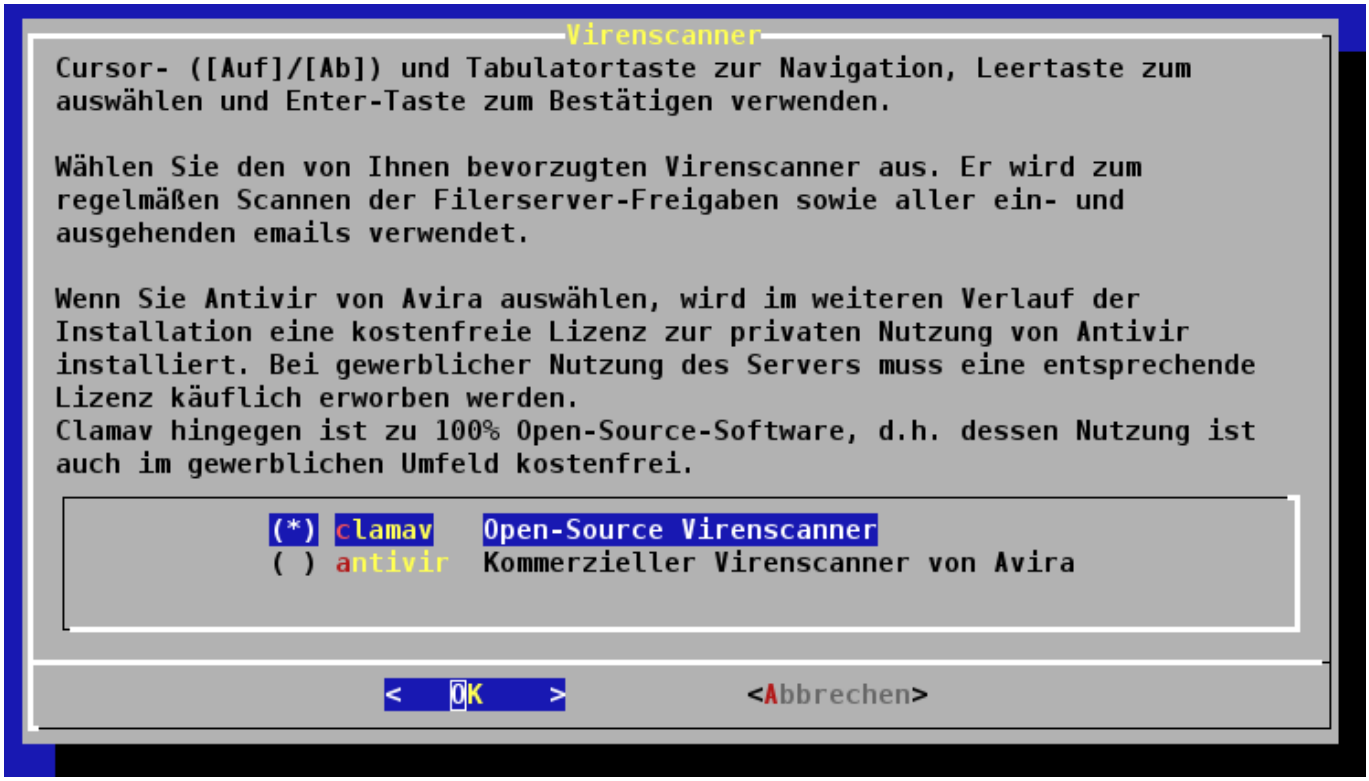
Das Repository verlangt eine Authentifizierung, ohne geht es nicht. Sie haben die Möglichkeit sich selbst kostenlos für einen Account zu registrieren oder die im Bild gezeigten öffentlichen Zugangsdaten verwenden. Weitere Hinweise dazu finden Sie hier.

Auf einem invis-Server haben Sie auch die Möglichkeit eine ERP-Software zu betreiben. Sie haben die Auswahl zwischen Wawision und Kivitendo:



Sie können sich auch dafür entscheiden keine ERP-Lösung zu installieren.

Die nachfolgende Auswahl des zu installierenden Virenscanners ist inzwischen keine mehr. Die angebotene kommerzielle Lösung von Avira wurde vom Markt genommen. Es steht derzeit also nur Clamav zur Verfügung.



Der zweite Eintrag wurde in der Hoffnung erhalten eine alternative zu Avira zu finden. Empfehlungen nehmen wir gerne entgegen!

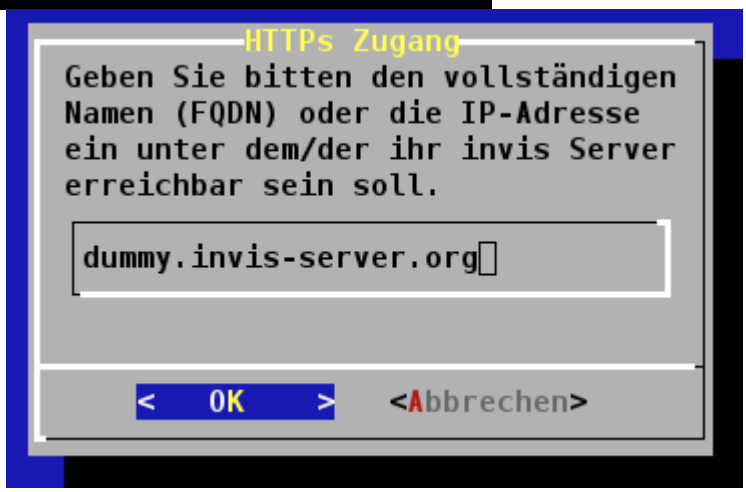
Es folgt eine weitere Software-Auswahl:

Sie können einen invis-Server mit Hilfe eines Monitoring Systems fernüberwachen. Vorbereitet haben wir die Nutzung von Nagios/Icinga und Zabbix. Wählen Sie nach Belieben.

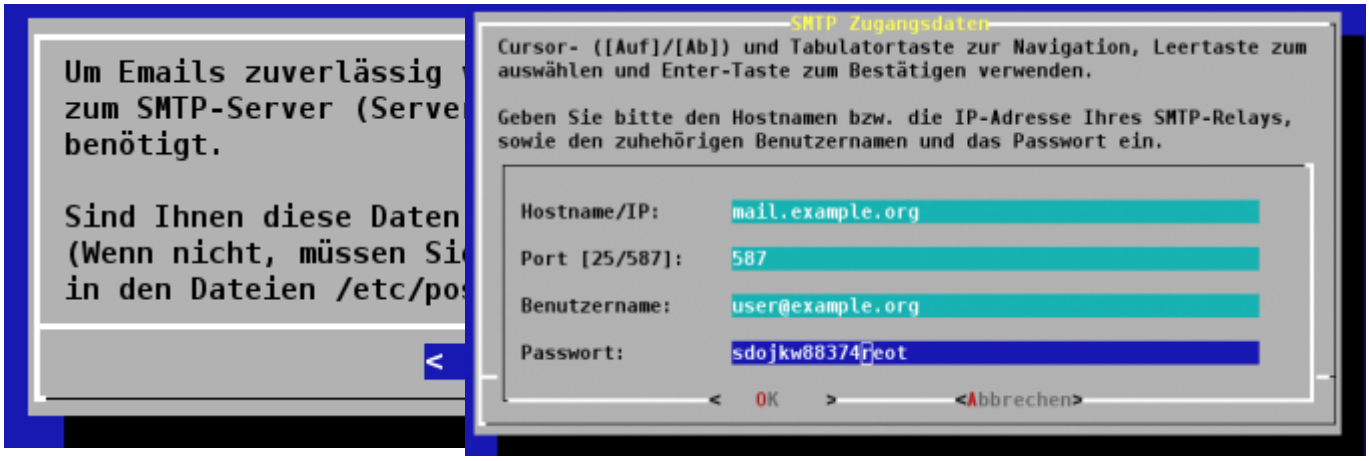
Einen invis-Server via Internet erreichen zu können ist für viele Funktionen unabdingbar. Dazu benötigen Sie einen im Internet gültigen Namen für den Server. Da die meisten invis-Server wohl an einem normalen DSL-Anschluß ohne feste IP-Adresse betrieben werden gilt es diese IP-Adresse immer wieder mit dem gültigen Namen zu verbinden.

Um dies zu tun können Sie sich auf die Dienste eines entsprechenden Anbieters im Internet verlassen oder Sie betreiben eigene DNS-Server die per DDNS aktualisiert werden können. Für letztere Möglichkeit kann ein invis-Server als DDNS-Client fungieren. Lösung Nr. 1 können Sie auf dem invisserver unterverwendung der Software „ddclient“ manuell installieren oder auf einem vorgeschalteten Router einrichten.

Unabhängig davon für welche Lösung Sie sich entscheiden, müssen Sie hier den vollqualifizierten Namen (FQDN) eingeben unter dem Ihr Server erreichbar sein soll.



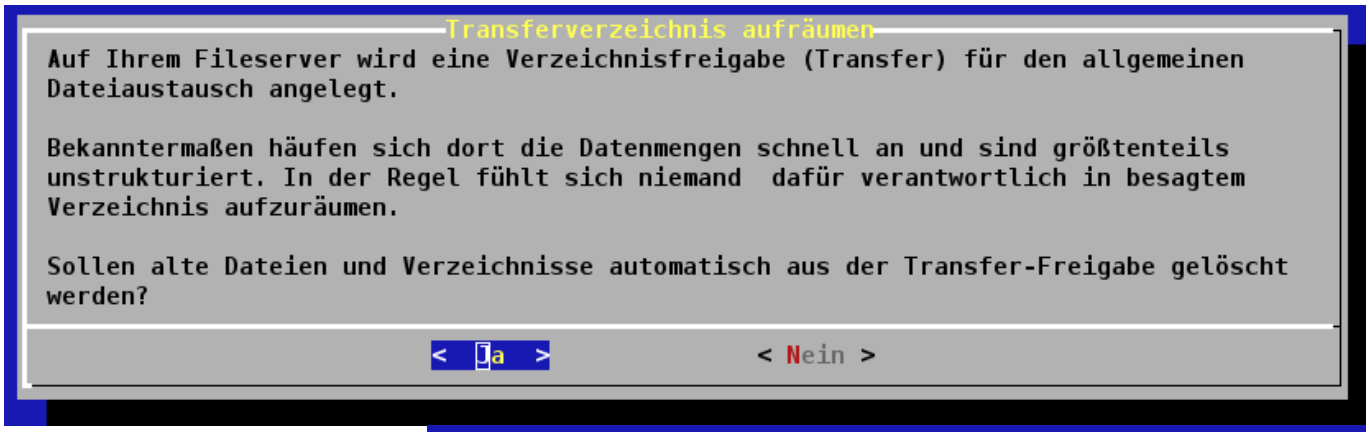
Um Emails versenden zu können benötigt ein invis-Server Zugangsdaten um sich per „SMTP-Auth“ an einem Mailrelay (Smarthost) anmelden zu können. Üblicherweise ist dies der Mailserver Ihres Internet-Service-Providers oder der des Webhosters bei dem Sie Ihre Mailkonten verwalten.



Es genügt die Angabe eines einzelnen Kontos für den Mailversand. Wenn Ihr Provider „Submission“, also den Mailversand über Port 587 unterstützt ist dies auf jeden Fall zu bevorzugen.

Sie können diese Einstellungen auch jederzeit in der Konfiguration des Dienstes Postfix überarbeiten oder, wenn Ihnen die Daten jetzt nicht zur Hand sind nachholen.

invis-Server arbeiten selbstverständlich als Fileserver im Netz. Auf ihnen sind eine Reihe von Freigaben vorkonfiguriert. Darunter die Freigabe **Transfer**. Diese Freigabe dient dem Austausch von Dateien zwischen Benutzer mit vollkommen unterschiedlichen Zugriffsrechten auf dem Server. D.h. jeder darf alles, was die Freigabe dazu prädestiniert zur **Betriebsmüllhalde** zu mutieren. Um dem entgegenzuwirken kann ein invis-Server dort selbst für Ordnung sorgen.

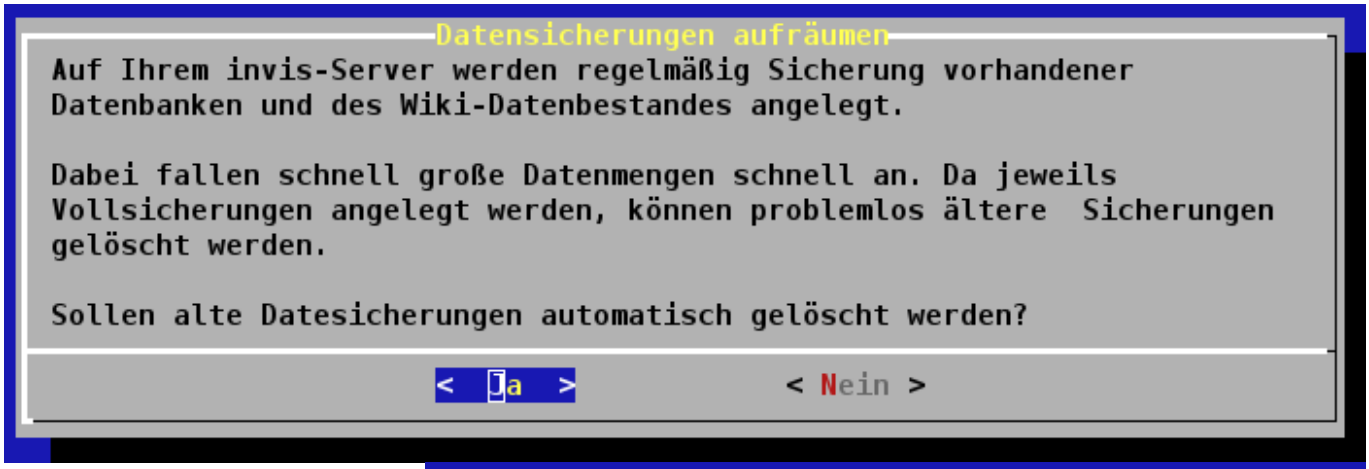


Geben Sie an, ob Sie eine automatische Bereinigung wünschen und wie alt Dateien dort maximal werden dürfen.

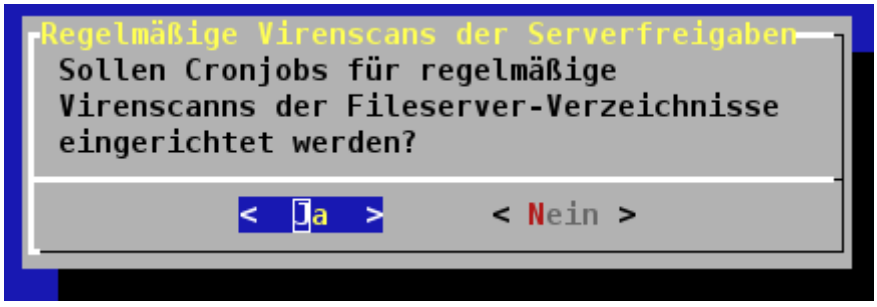
Achtung: *Vergessen Sie nicht die Nutzer über diese Funktion zu unterrichten!*

invis-Server führen intern eine Reiche von Datensicherungsaufgaben durch. Gesichert werden regelmäßig alle Datenbanken sowie das Wiki. Da dies relativ schnell eine Menge Festplattenplatz in Anspruch nimmt kann der Server auch hier regelmäßig aufräumen und alte Sicherungen löschen.

Auch hier können Sie festlegen, ob automatisch aufgeräumt werden soll und wie lange alte Datensicherungen aufbewahrt werden sollen.



Eine weitere regelmäßige Wartungsfunktion des invis-Servers ist die zyklische Überprüfung der Fileserver-Freigaben auf Viren. Sie können auswählen, ob Sie dies wünschen oder nicht.



Achtung: *Je nach Leistung Ihres Servers und Menge der zu scannenden Daten, kann es sein, dass die Scans viel zu lange brauchen und das System in die Knie zwingen. Viel wichtiger als diese Scans sind gepflegte Virenscanner auf den Client-PCs.*

Aus Sicherheitsgründen lauscht Ihr invis-Server bei Verbindungen aus dem Internet nicht auf den Standard-Ports der zugehörigen Protokolle. Statt dessen werden Ports per Zufallsgenerator fest gelegt. Zum Abschluss des „quest“ Moduls zeigt ***sine*** diese Ports an.

Fügen Sie diese Ports bitte Ihrer Dokumentation hinzu.

Modul: sysprep

Typ: interaktiv

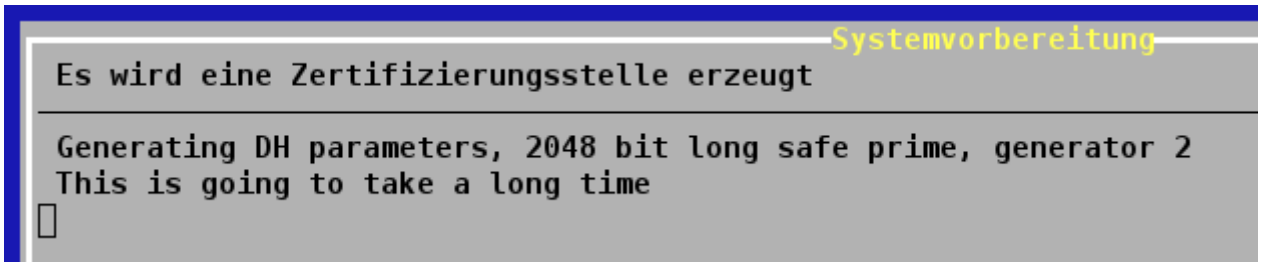
Das Modul „sysprep“ führt weitere Vorbereitungsaufgaben durch. Darunter die Installation des Virenscanners, der erforderlichen Samba-Pakete und weitere Software. Wichtigste Aufgabe ist aber die Einrichtung einer Zertifizierungsstelle (CA) für Ihren invis-Server. Mit dieser CA werden im weiteren Verlauf des Setups Sicherheitszertifikate für verschiedene Komponenten Ihres Servers erzeugt. Geht an dieser Stelle etwas schief, wirkt sich dies auf den gesamten weiteren Verlauf des Setups aus und verhindert ein korrektes Funktionieren des Servers im Anschluss.

Achtung: *Sie werden aufgefordert ein Passwort für die CA zu erdenken. Mit diesem Passwort wird der „private Schlüssel“ der CA geschützt. Dieses Passwort benötigen Sie im Verlauf des Setups und auch im anschließenden Server-Betrieb immer wieder. Geht es verloren ist reichlich Handarbeit notwendig um eine neue CA und die notwendigen Server-Zertifikate zu bauen.*

```
Note: using Easy-RSA configuration from: /etc/easy-rsa/vars
Generating a 4096 bit RSA private key
.....................................................................................................++
.....................................................++
writing new private key to '/etc/easy-rsa/bus-net.loc/private/ca.key.2OeePNbdB2'
Enter PEM pass phrase:
```

Hinweis: *Mit Erscheinen des invis-Servers in Version 10.5 wurde die gesamte Zertifikats-Infrastruktur auf die Software* ***easy-rsa*** *umgestellt. Ab diesem Zeitpunkt gibt es nur noch eine CA für alle Zertifikate. D.h. Die hier erzeugte Infrastruktur wird auch für OpenVPN genutzt. Die VPN Client-Zertifikate werden von der gleichen CA signiert wie alle anderen Zertifikate des Servers. Es wird ab sofort auch für die Erstellung von VPN-Client-Zertifikaten das Passwort der Stamm-CA benötigt.*

Wurde die CA fertig gestellt, werden noch Diffie-Hellman Parameterdateien sowie eine „Certificate-Revocation-List“ erstellt. Speziell die Erstellung der DH-Parameter nimmt einige Zeit in Anspruch.



Zur Erstellung der CRL werden Sie nach dem zuvor festgelegten Passwort der CA gefragt.

```
Note: using Easy-RSA configuration from: /etc/easy-rsa/vars
Using configuration from /etc/easy-rsa/openssl-1.0.cnf
Enter pass phrase for /etc/easy-rsa/bus-net.loc/private/ca.key:
```

Damit ist der Aufbau Ihrer PKI abgeschlossen, alle weiteren Aufgaben des sysprep-Moduls laufen automatisch ab.

Modul: samba_ad

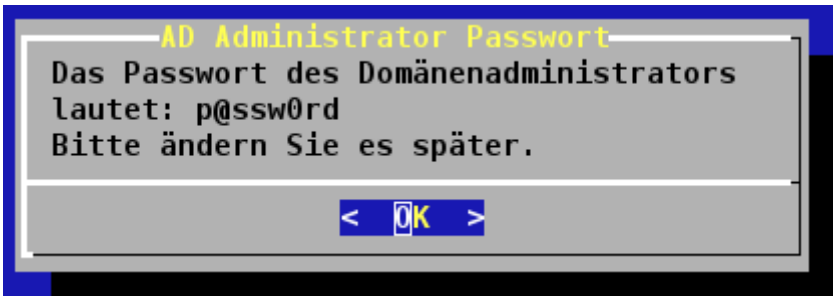
Typ: interaktiv

Das Modul „samba_ad“ baut das „Active Directory“, also die Kernkomponente des invis Servers auf. Dazu gehören das sogenannte „Domain Provisioning“, es werden Schema-Erweiterungen installiert und individuelle Daten Ihres Servers im AD gespeichert.

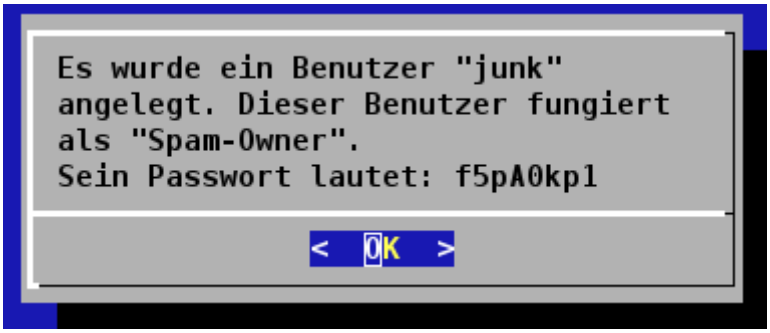
Es wird im AD ein erster Benutzer „Administrator“ angelegt, dieser Benutzer ist der Domänenadminstrator, er verfügt an jedem Windows-PC der Domäne über administrative Rechte, ihm ist es erlaubt das AD mit Hilfe der Microsoft'schen „Remote Server Administrationswerkzeugen“ (RSAT) oder dem vorinstallierten „phpLDAPAdmin“ zu bearbeiten und dieses Konto wird für Domänenbeitritte von Clinet PCs verwendet.

Achtung: *Der Benutzer „Administrator“ wird derzeit mit einem Standard-Passwort versehen, welches Sie später unbedingt ändern sollten.*

Administrator-Passwort: p@ssw0rd



Nachdem ***sine*** das LDAP-Verzeichnis aufgebaut und mit Daten gefüllt hat wird ein Benutzer „junk“ angelegt. Er ist Inhaber eines lokalen Mailkontos in das vom Server als Spam eingestufte Mails eingeliefert werden. ***sine*** generiert für dieses Konto ein zufälliges Passwort und gibt es aus:



Notieren Sie sich das Passwort, damit können Sie später auf einem beliebigen Mailclient ein Konto einrichten um das Junk-Postfach einzusehen.

Für den Zugriff auf die LDAP-Komponente des ADs wird ein Sicherheitszertifikat erzeugt, d.h. Sie benötigen das Passwort der CA.

Geben Sie das Passwort der CA ein. Alle weiteren Schritte des Moduls laufen automatisch ab.

Modul: dns

Typ: automatisch

Das Modul „dns“ richtet den Nameserver „bind“ auf Ihrem Server ein. Der Nameserver nutzt das Active Directory als Daten-Backend. Es werden eine DNS-Zone für die Rückwärtsauflösung und einige weitere DNS-Datensätze angelegt.

Modul: dhcp

Typ: automatisch

Das Modul richtet den DHCP-Dienst des invis Servers ein. Auch der DHCP-Dienst verwendet die LDAP-Komponente des Active Directories als Daten-Backend. Anders als der Nameserver kommuniziert der DCHP-Dienst unter Verwendung des LDAP-Protokolls mit dem Active Directory. D.h. Wenn Samba's AD-Komponente nicht läuft, kann auch der DHCP-Server nicht starten.

Modul: mailserver

Typ: interaktiv

Modul: cups

Typ: automatisch

Modul: fileserver

Typ: automatisch

Modul: webserver

Typ: interaktiv

Modul: mysqlserver

Typ: interaktiv

Modul: postgresql

Typ: interaktiv

Modul: firewall

Typ: automatisch

Modul: acupsd

Typ: automatisch

Optionale Module

Zu Beginn jedes nachfolgenden Moduls zeigt ***sine*** zunächst eine Erläuterung des Moduls an und fragt, ob es ausgeführt werden soll. Wird diese Frage mit „nein“ beantwortet, überspringt ***sine*** das Modul uns setzt das Setup beim nächsten Modul fort. Insofern sind alle nachfolgenden Module vom Typ „interaktiv“.

Das Überspringen eines Moduls hat, Module „groupware“ ausgenommen keine nachteiligen folgen. Wurde als Groupware Zarafa ausgewählt und dieses Modul übersprungen, steht kein IMAP-Dienst zur Verfügung.

Modul: monitoring

Modul: groupware

Modul: erp

Modul: faxgate

Modul: webcdwriter

Modul: openvpn

Modul: dokuwiki

Modul: owncloud

Modul: virtualbox