

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.

Achtung: Verbinden Sie die interne Netzwerkschnittstelle Ihres invis-Servers mit einem Switch bevor Sie das Setup starten. Seit openSUSE 42.1 werden nicht verbundene Netzwerkschnittstellen nicht mehr automatisch aktiviert, auch dann nicht, wenn deren Startmodus auf „at boot time“ steht. **sine** behebt dieses Problem im Laufe des Setups. Wir haben dieses Verhalten bereits als Bug an SUSE gemeldet. Das Verhalten wird seit dem immerhin in der offiziellen Dokumentation des SLES beschrieben, geändert wurde es jedoch nicht.

sine bis invis-Server 12.x

```
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.

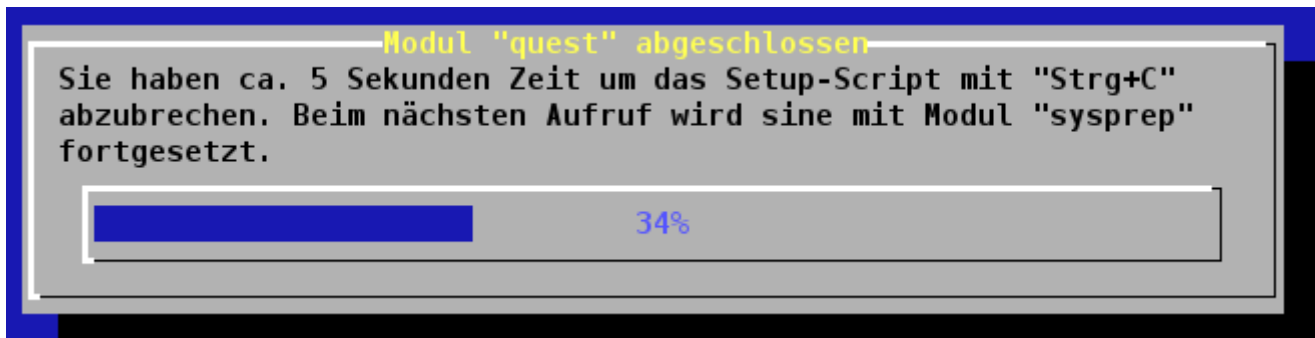
Alle vorbereiteten Konfigurationsdateien für das invis-Setup sind im Zuge des Umbaus zur RPM-basierten Installation nach

```
/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.

sine2 ab invis-Server 13.0

Die ursprüngliche Version von **sine** wuchs bis zu einem Shell-Script von ca. 3500 Zeilen und damit eigentlich viel zu groß für ein Shell-Script. Zwar bezeichnen wir es im vorangegangenen Abschnitt bereits als „modular“, jedoch bezog sich dies auf die Tatsache, dass die einzelnen Module in Form von Funktionen innerhalb des „einen“ Scripts realisiert wurden.

Dies haben wir geändert. Wir haben es in einzelne Scripts zerlegt und der neuen Version den, zugegeben wenig einfallsreichen Namen **sine2** verpasst. Entsprechend ändern sich ab invis-Server Version 13.0 die Aufrufe des Scripts:

```
linux:~ # sine2
```

sine verfügt über ein paar nützliche Aufrufparameter:

- **sine2 help** - gibt kurze Hinweise zur Verwendung
- **sine2 status** - zeigt an, mit welchem Modul sine beim nächsten Aufruf gestartet wird.
- **sine2 log** - zeigt (so bereits vorhanden) das Log-File des bisherigen sine-Durchlaufs
- **sine2 showconf** - zeigt die (so bereits vorhanden) die von sine abgefragten Konfigurationsparameter an.
- **Ab invis 14.0: sine2 showpws** - zeigt alle während des Setups generierten Passwörter an.

- **Ab invis 14.0: *sine2 reset*** - löscht alle Setup-Daten (Konfigurationsdaten, Passwörter und Installationsstatus). Diese Funktion sollten Sie nur nutzen, wenn Sie wirklich sicher sind, was Sie tun.
- ***sine2 modulname*** - ermöglicht, **nach einmalig vollständigem Durchlauf**, übersprungene optionale Module nachträglich manuell zu starten.

Das Verzeichnis

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

bleibt weiterhin das Arbeitsverzeichnis. Neu ist die Verzeichnisstruktur unter:

```
/usr/share/sine
```

Hier finden sich beispielsweise die einzelnen Modul-Skripts sowie die Konfigurationsvorlagen. Letztere sind damit aus dem Dokumentationspfad

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

in die neue Verzeichnisstruktur gewandert.

Eine detailliertere Erläuterung zum neuen ***sine2*** ist [hier](#) zu finden.

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.

Hinweis: Mit Veröffentlichung der invis-Server Release 13.0, ändert sich der nachfolgend geschilderte Installationsablauf geringfügig. Lassen Sie sich also nicht verunsichern, wenn die eine oder andere Bildschirmausgabe nicht haargenau so aussieht, wie in den hier gezeigten Screenshots. Weitere diesbezügliche Hinweise befinden sich ggf. in den einzelnen Modulbeschreibungen.

Modul: check

Typ: automatisch Das Modul „check“ fragt lediglich nach, ob alle hier beschriebenen 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).

Fragen zur openssl Umgebung

Cursor- ([Auf]/[Ab]) und Tabulatortaste zur Navigation, Leertaste zum auswählen und Enter-Taste zum Bestätigen verwenden.

Die eingegebenen Daten sollten der Realität entsprechen, da sie beim Bau von SSL-Zertifikaten verwendet werden. Vor allem die email-Adresse des für die Zertifikate Verantwortlichen (Feld: Name) muss erreichbar sein.

Alle Eingaben werden auf Plausibilität geprüft, fehlerhaft ausgefüllte Felder werden geleert.

Staat:	DE	Bundesland:	Hessen
Stadt:	Schotten		
Organisation:	invis-server.org		
email:	stefan@invis-server.org		
Name:	Stefan Schäfer		

< OK > <Abbrechen>

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:

Fragen zur Netzwerkkonfiguration

Cursor- ([Auf]/[Ab]) und Tabulatortaste zur Navigation, Leertaste zum auswählen und Enter-Taste zum Bestätigen verwenden.

Die Vorgabewerte wurden aus der Systemkonfiguration ermittelt und sollten somit richtig sein.
Prüfen Sie vor allem, ob der angezeigte Domänenname aus Domain und Top-Level-Domain besteht; also zweiteilig ist. Domännennamen wie der bei openSUSE vorgegebene "site" bereiten im weiteren Verlauf der invis Server Installation Probleme.
Verwenden Sie keinesfalls eine real existierende Top-Level-Domain wie ".de" oder ".com". Statt dessen eignet sich beispielsweise ".loc" (für local).

Wenn Sie hier Änderungen vornehmen, müssen Sie diese nachträglich in Ihre Systemkonfiguration übernehmen.

Achtung: Fehlerhafte Eingaben sind nach der vollständigen Installation nur sehr schwer zu korrigieren.

Hostname:	<input type="text" value="invisad"/>	Domain:	<input type="text" value="bus-net.loc"/>
IP (intern)	<input type="text" value="192.168.242.10"/>	Netzwerkmaske:	<input type="text" value="255.255.255.0"/>

< OK > <Abbrechen>

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.

Netzwerkdaten

Prüfen Sie bitte genau ob die folgenden Angaben korrekt sind.

IP-Adresse(intern): 192.168.242.10
Netzwerkbasis: 192.168.242.0
Netzwerkmaske (lang): 255.255.255.0 / (kurz): 24
Broadcast-Adresse: 192.168.242.255
FQDN: invisad.bus-net.loc
LDAP Base: DC=bus-net,DC=loc
Samba-Domäne: BUS-NET

Sind alle Angaben korrekt?

☒ Ja ☐ Nein

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

Weiter geht es mit der Abfrage der Forward-Nameserver.

Forward DNS Server

Cursor- ([Auf]/[Ab]) und Tabulatortaste zur Navigation, Leertaste zum auswählen und Enter-Taste zum Bestätigen verwenden.

Auf Ihrem invis Server wird ein DNS-Dienst eingerichtet. Zur Beschleunigung von DNS Anfragen ist es sinnvoll diesem bis zu drei "Forward Nameserver" zu nennen. Dies können beispielsweise der DNS eines vorgeschalteten Routers, DNS Server des Internet Zugangs Providers oder unabhängige DNS-Server im Internet sein.

Achtung: Prüfen Sie bitte, ob die angegebenen DNS-Server auf Anfragen antworten, da ansonsten sowohl die weitere Installation, als auch der Betrieb des invis-Servers beeinträchtigt wird.

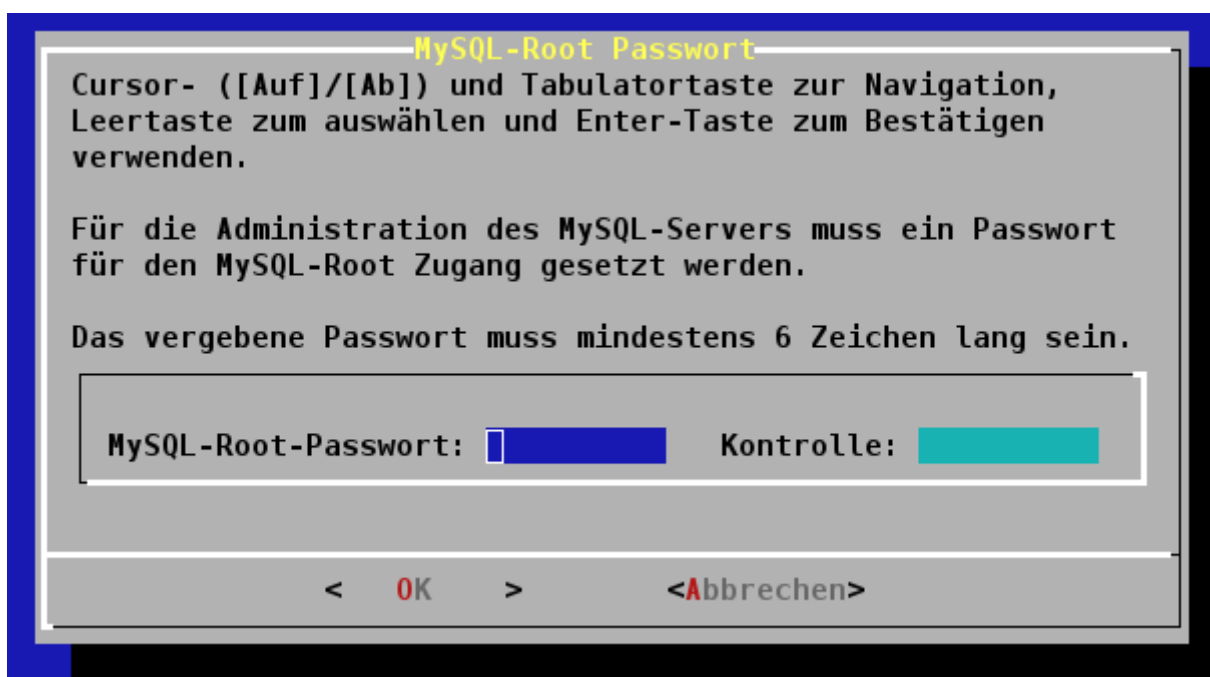
Geben Sie mindestens eine IP-Adresse ein.

DNS 1: 8.8.8.8
DNS 2: 194.25.2.129
DNS 3:

☒ OK ☐ Abbrechen

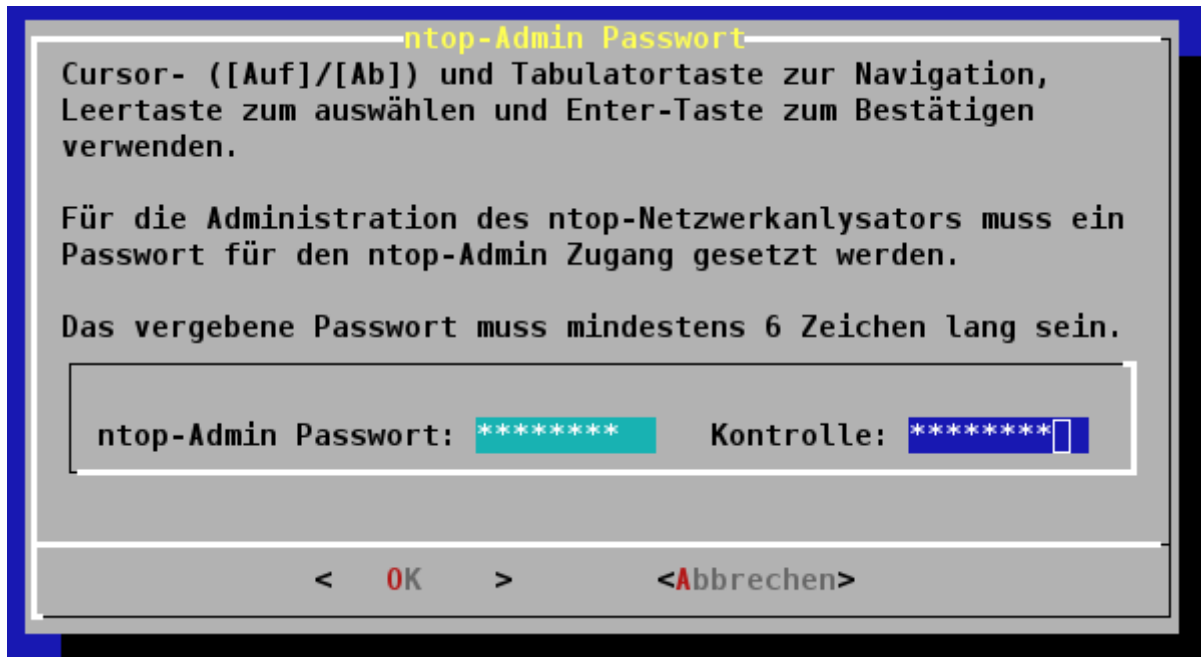
Ein invis-Server arbeitet für das an ihn angeschlossene Netzwerk als DNS-Server. Zuständig ist er primär für die Namensauflösung im lokalen Netz, er arbeitet aber auch als Caching-Nameserver für die Namensauflösung im Internet. Um diese Aufgabe zu erleichtern können ihm sogenannte „Forwarder“ bekannt 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 Datenbank-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.

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.

Es folgt die Frage nach der gewünschten Groupware:



Hinweis: Mit Veröffentlichung von invis-Server 12.0 vollziehen wir den Wechsel von Zarafa zu Kopano.

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.

Wurde Kopano (ab invis-Version 12.0) als Groupware ausgewählt, folgt ein zweites Auswahlfenster. Hier muss entschieden werden aus welchem Repository Kopano installiert werden soll. Zur Auswahl stehen:

- **Kopano Limited** – Dieses Repository wird von Kopano selbst bereit gestellt. Es enthält getestete Pakete, für die Kopano limitierten Support im Rahmen einer Subskription gewährt. Um aus diesem Repository zu installieren, muss bereits ein Subskriptionsvertrag bestehen. Mit Abschluss des Vertrages erhalten Sie Zugangsdaten zum Repository. Ohne diese Zugangsdaten ist die Kopano-Installation aus dem Limited-Repository nicht möglich. **sine** fragt die Zugangsdaten im weiteren Verlauf der Installation ab.
- **openSUSE Build Service** – Dieses Repository enthält immer die aktuellste Kopano Community Version. Die Pakete sind nicht für den Produktivbetrieb getestet und Support wird dafür nicht geleistet. **Der Einsatz der Pakete geschieht auf eigenes Risiko!** Vorsicht ist auch beim Aktualisieren geboten, da hier ohne Vorwarnung Major-Release-Upgrades geschehen können. Dies kann unter Umständen zu einem nicht funktionierenden System führen und bedarf auf jeden Fall erhöhter Aufmerksamkeit und Erfahrung im Umgang mit Kopano.



Hinweis: Bis einschließlich invis-Server Version 11.0 wurde Samba aus den Repositories der Göttinger Firma Sernet installiert. Ab Version 12.0 stellen wir selbst Samba-Pakete inkl. Active-Directory zur Verfügung. D.h. die nachfolgende Abfrage erscheint nicht mehr.

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

Enterprise Samba Zugangsdaten

Cursor- ([Auf]/[Ab]) und Tabulatortaste zur Navigation, Leertaste zum auswählen und Enter-Taste zum Bestätigen verwenden.

Geben Sie bitte Ihre Zugangsdaten für das Enterprise-Samba Repository ein.

Benutzername:

Accesskey:

< OK > <Abbrechen>

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:

Enterprise Ressource Planning Software

Cursor- ([Auf]/[Ab]) und Tabulatortaste zur Navigation, Leertaste zum auswählen und Enter-Taste zum Bestätigen verwenden.

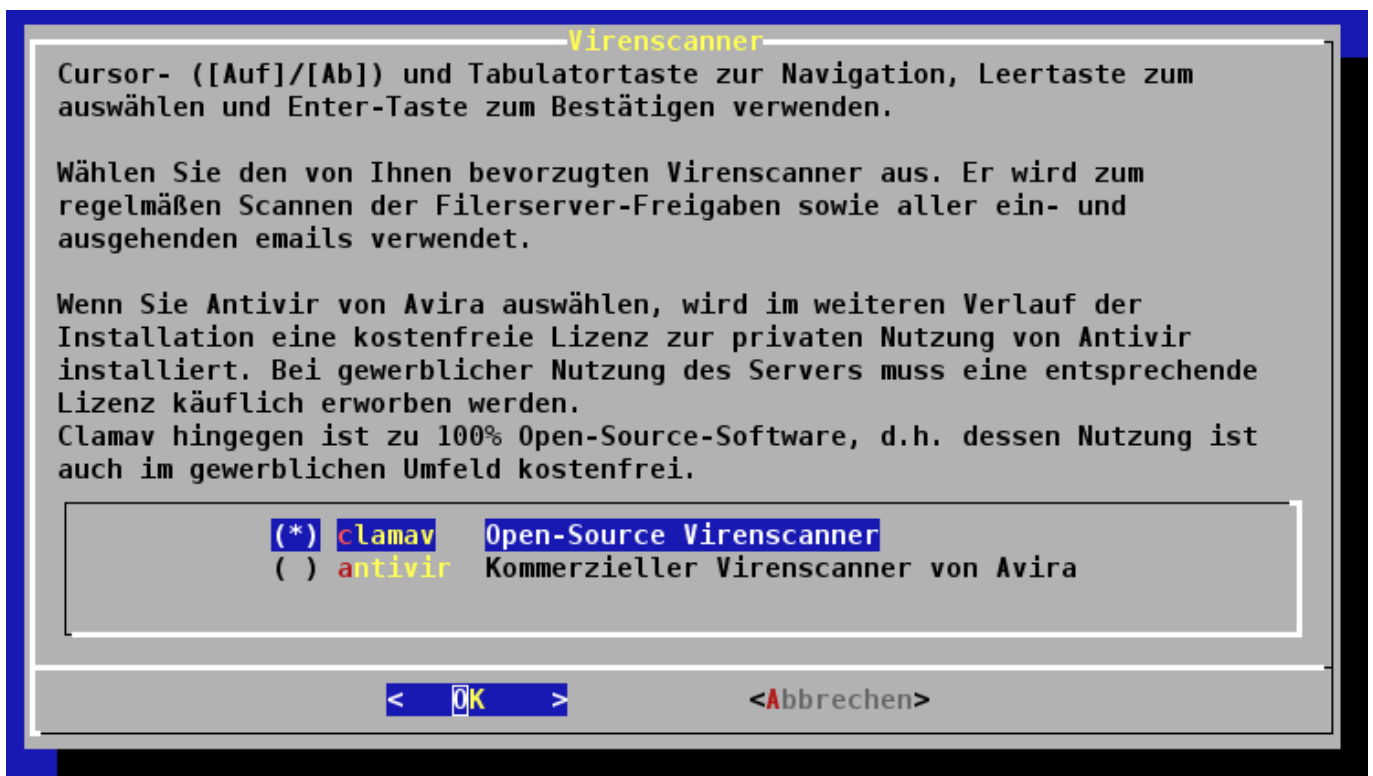
Wählen Sie die von Ihnen bevorzugte ERP-Software (Warenwirtschaftssystem) aus.

() Kivitendo	Konzentriert sich auf Handel und Finanzbuchhaltung, wenig modula
() waWision	Moderne ERP Lösung für Handel und Dienstleistung inkl. Webshop-S
(*) Keine	Sie verwenden ein eigenes System

< OK > <Abbrechen>

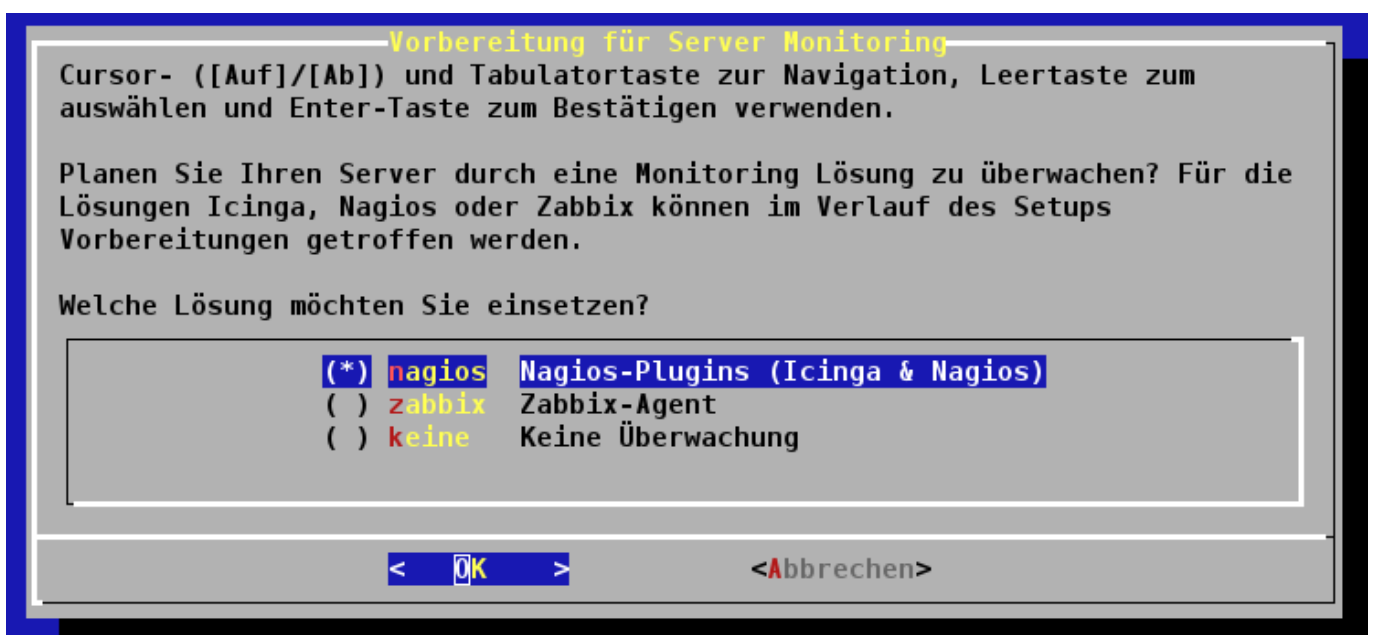
Sie können sich auch dafür entscheiden keine ERP-Lösung zu installieren.

Hinweis: Die nachfolgende Auswahl des zu installierenden Virenschanners ist inzwischen keine mehr. Die angebotene kommerzielle Lösung von Avira wurde vom Markt genommen. Es steht derzeit also nur Clamav zur Verfügung. Ab invis-Server Version 12.0 verschwindet die Abfrage ganz.



Den zweiten Eintrag haben wir in der Hoffnung erhalten eine alternative zu Avira zu finden. Empfehlungen nehmen wir auch mit dem Verschwinden der Auswahloption noch immer gerne entgegen! Wer also Erfahrung mit einem Virens Scanner unter Linux hat, welches sich gut mit AMaViS kombinieren lässt, kann uns gerne an seinen Erfahrungen teilhaben lassen.

Es folgt eine weitere Software-Auswahl:



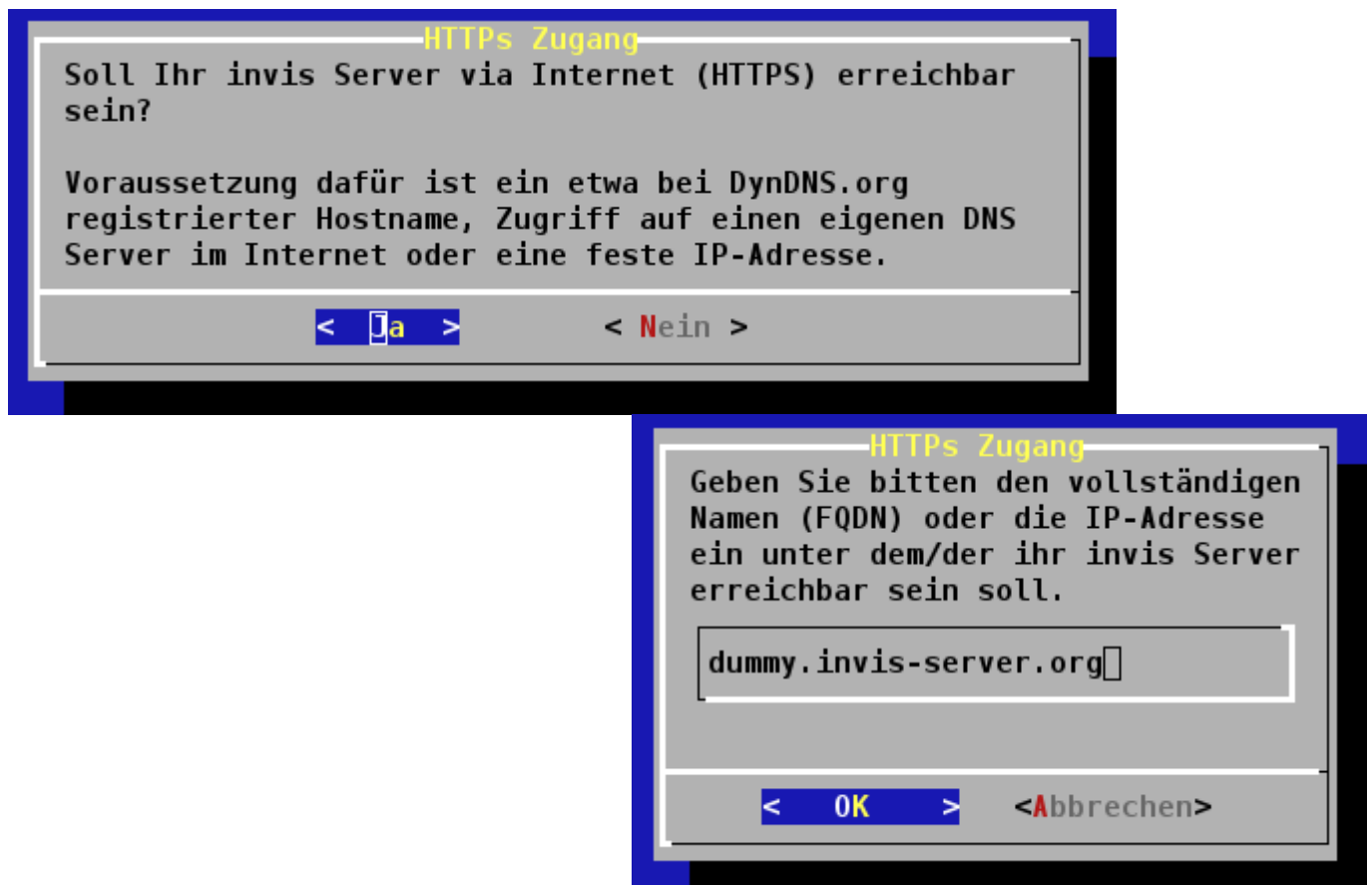
Sie können einen invis-Server mit Hilfe eines Monitoring Systems fernüberwachen. Vorbereitet haben wir die Nutzung von Nagios/Icinga und Zabbix. Wählen Sie nach Belieben.

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.

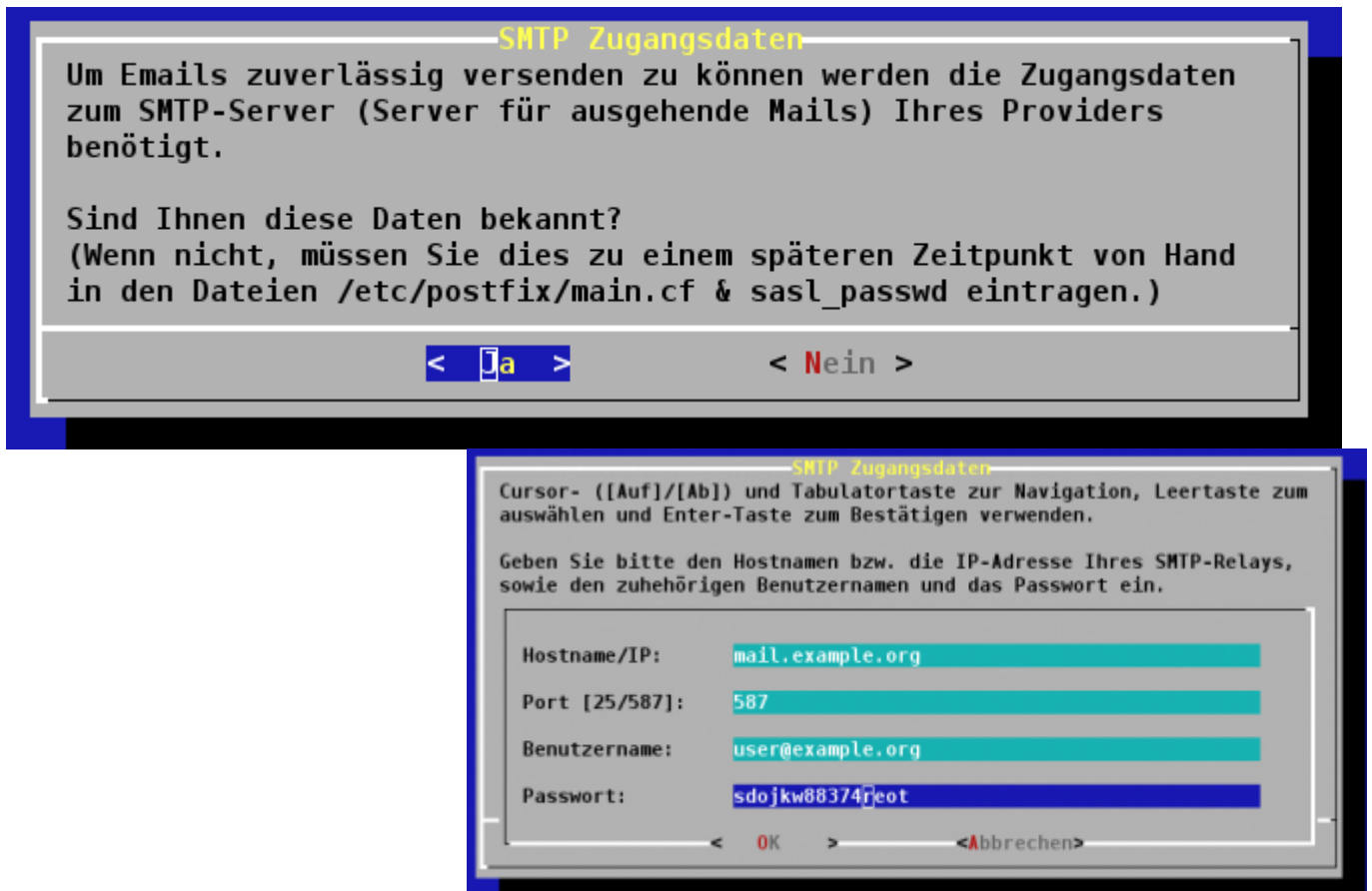
Um dies zu tun können Sie sich auf die Dienste eines entsprechenden Anbieters im Internet verlassen oder Sie betreiben eigene DNS-Server die per DDNS aktualisiert werden können. Für letztere Möglichkeit kann ein invis-Server als DDNS-Client fungieren. Lösung Nr. 1 können Sie auf dem invisserver unterverwendung 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) oder die feste IP-Adresse eingeben unter dem Ihr Server erreichbar sein soll.

Achtung: Wenn Sie nicht möchten, dass Ihr invis-Server via Internet erreichbar ist und Sie dies hier entsprechend angeben, werden im Weiteren auch keine Schlüssel und Zertifikate für den HTTPS-Zugang generiert.



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.

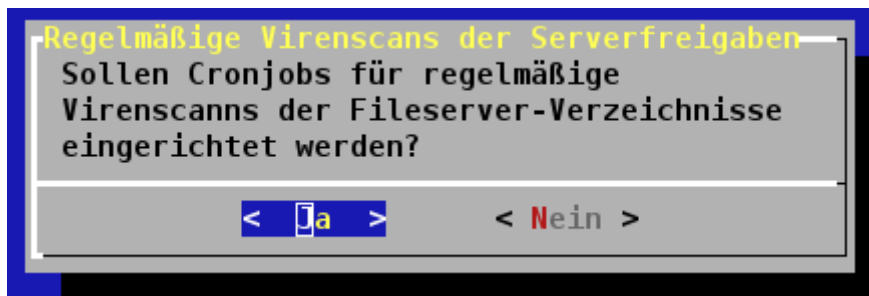
Achtung: Vergessen Sie nicht die Nutzer über diese Funktion zu unterrichten!

invis-Server führen intern eine Reihe 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. Verzichten Sie im Zweifelsfall darauf und beantworten Sie die Frage mit nein. 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.



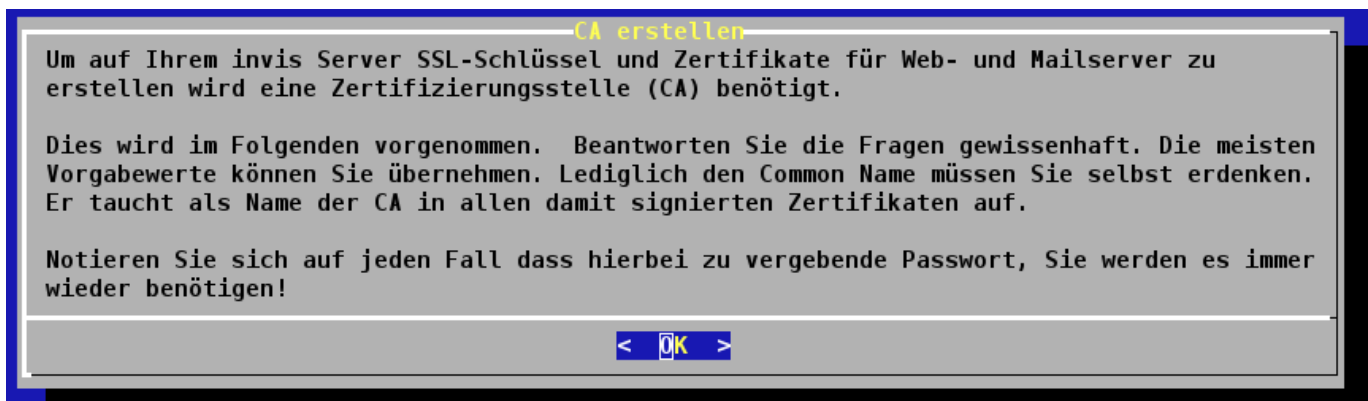
Fügen Sie diese Ports bitte Ihrer Dokumentation hinzu.

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.20eePNbdB2'
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.

sine fragt beim Erstellen der CA Informationen ab, die im Zertifikat der CA enthalten sein werden. In den meisten Fällen können Sie die Vorgaben übernehmen. Achten Sie beim CN (Common Name) darauf den Vorgabewert „Easy RSA CA“ durch eine individuelle und vor allem eindeutige Vorgabe zu ersetzen. Eine gute Idee ist hier der volle Hostname (FQHN) des Servers gefolgt vom Kürzel CA, also z.B. „invis.example-net.loc CA“.

Achtung Vor allem, wenn Sie mehrere invis-Server installieren und betreuen ist es wichtig, dass der CN im Stammzertifikat auf allen Installationen unterschiedlich ist. Wenn Sie unterschiedliche Stammzertifikate mit gleichem CN in einen Zertifikatsspeicher, beispielsweise Ihres Browsers integrieren, hat er später keine Möglichkeit zu unterscheiden mit welchem dieser Stammzertifikate ein zu verifizierendes Server-Zertifikat signiert wurde.

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.

```
Systemvorbereitung
Es wird eine Zertifizierungsstelle erzeugt

Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
█
```

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

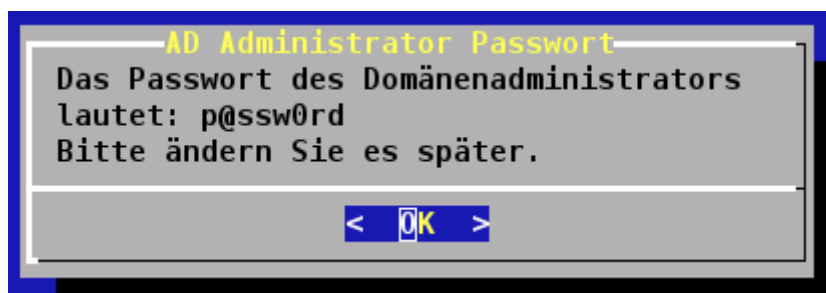
Typ: interaktiv

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 Domänenadministrator, 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.

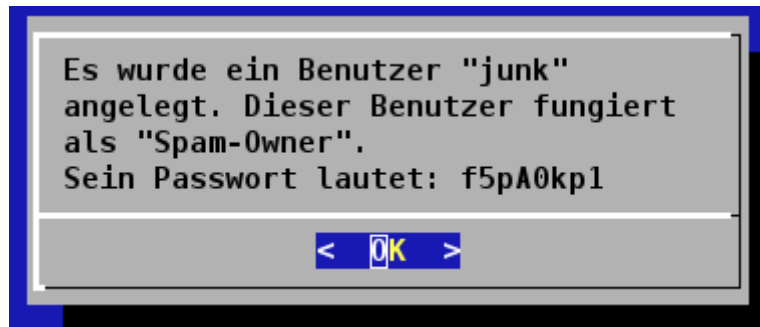
Achtung: Der Benutzer „Administrator“ wird derzeit mit einem Standard-Passwort versehen, welches Sie später unbedingt ändern sollten.

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

In diesem Modul werden zunächst Schlüssel und Zertifikat für die Mailserver-Dienste generiert. Selbstverständlich benötigen Sie wieder das Passwort Ihrer CA.

```
Es werden Schlüssel und Zertifikat für "mail.bus-net.loc" erzeugt.  
  
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/mail.bus-net.loc.key.K01GQ0CHCj'  
-----  
Using configuration from /etc/easy-rsa/openssl-1.0.cnf  
Enter pass phrase for /etc/easy-rsa/bus-net.loc/private/ca.key:
```

Wenn Sie sich für Zarafa als Groupware und Postfachserver entschieden haben wird in diesem Modul eine LDAP-Schemaerweiterung für Zarafa installiert. Dieser Vorgang kann je nach Leistung Ihres Server eine Weile dauern:

```
Writecounter: 12
Writing zarafa-display-ads.ldf.sed.408 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 13
Writing zarafa-display-ads.ldf.sed.409 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 14
Writing zarafa-display-ads.ldf.sed.40B to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 15
Writing zarafa-display-ads.ldf.sed.40C to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 16
Writing zarafa-display-ads.ldf.sed.40D to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 17
Writing zarafa-display-ads.ldf.sed.40E to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 18
Writing zarafa-display-ads.ldf.sed.410 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 19
Writing zarafa-display-ads.ldf.sed.411 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 20
Writing zarafa-display-ads.ldf.sed.412 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
Writecounter: 21
Writing zarafa-display-ads.ldf.sed.413 to -H /var/lib/samba/private/sam.ldb ...
Modified 3 records successfully
```

Das durchlaufen der oben gezeigten Meldung ist normal! Der „Writecounter“ läuft bis zu einem Wert von etwa 800 hoch.

Zum Abschluss des Moduls werden Sie noch gefragt, ob Sie den Mailinlisten-Dienst „Mailman“ benötigen. Antworten Sie nach belieben, ich bin immer froh, wenn ich ihn nicht benötige. 😊

Mailman Installation

Mailman, der freie Mailinglisten-Manager

Zur Erweiterung der Funktionalität der Mailserver-Komponente Ihres invis-Servers können Sie mit Mailman einen mächtigen Mailinglisten-Manager installieren.

Mit Mailman lassen sich vergleichsweise einfach Diskussionslisten oder Newsletter mit Opt-in und Opt-out Funktion erstellen und verwalten.

Mailman bringt zur Verwaltung ein leistungsstarkes Webfrontend sowie zahlreiche Kommandozeilenwerkzeuge mit.

Weitere Informationen unter: <http://www.list.org>

Modul: cups

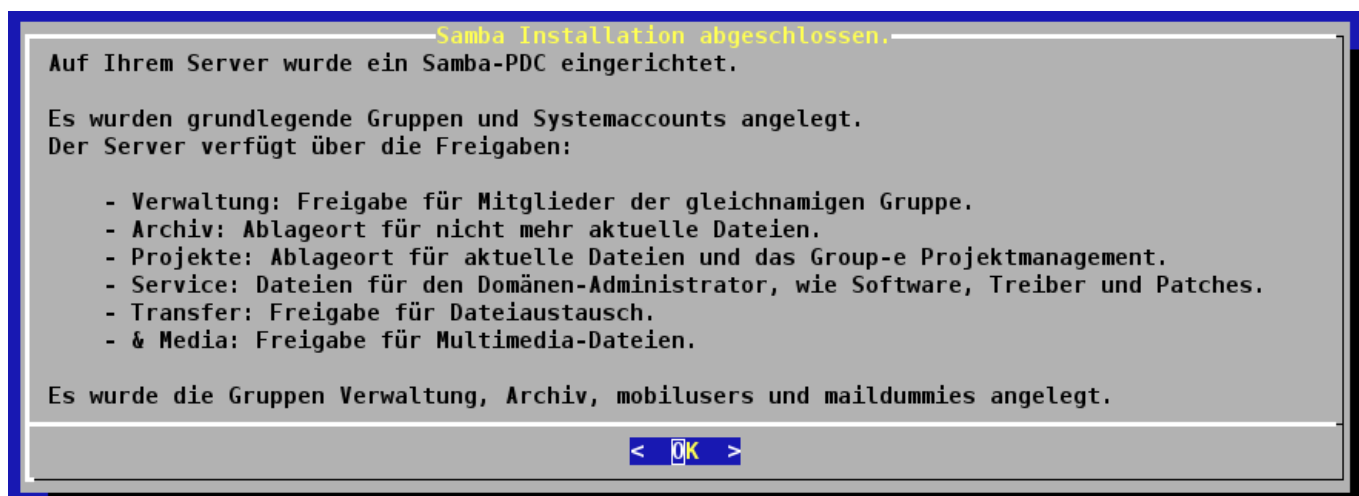
Typ: automatisch

Eingerichtet wird der Druckspooler CUPS.

Modul: fileserver

Typ: automatisch

Auch bei der Einrichtung des Filservers sind keine weiteren Angaben Ihrerseits erforderlich. Das Modul teilt Ihnen lediglich mit, was es gemacht hat.

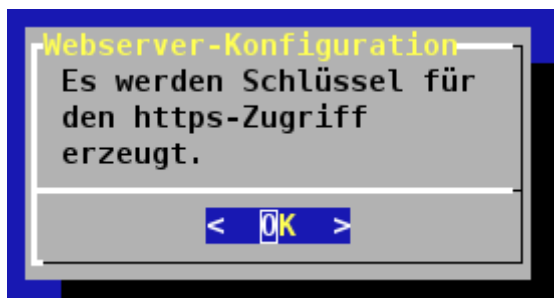


Wäre möglich, dass wir in zukünftigen Versionen auf diese Ausgabe verzichten.

Modul: webserver

Typ: interaktiv

Hier werden erneut Schlüssel und Server-Zertifikat, diesmal für den Webserver erzeugt. Sie benötigen also erneut das Passwort Ihrer CA.



Alles weitere läuft wieder automatisch ab. Hier wird unter anderem das invis-Portal installiert.

Modul: mysqlserver

Typ: automatisch

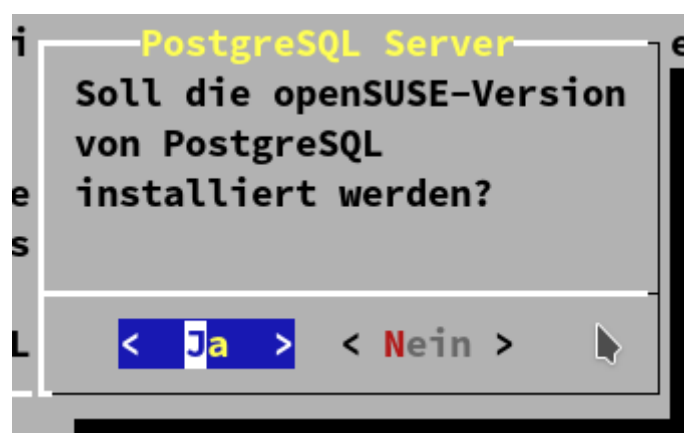
Der MariaDB-Dienst wird zum Leben erweckt. Das Modul gibt einen Hinweis bezüglich der Speichernutzung durch MariaDB aus. Die Anzeige verschwindet nach einigen Sekunden von alleine wieder.

Modul: postgresql

Typ: interaktiv

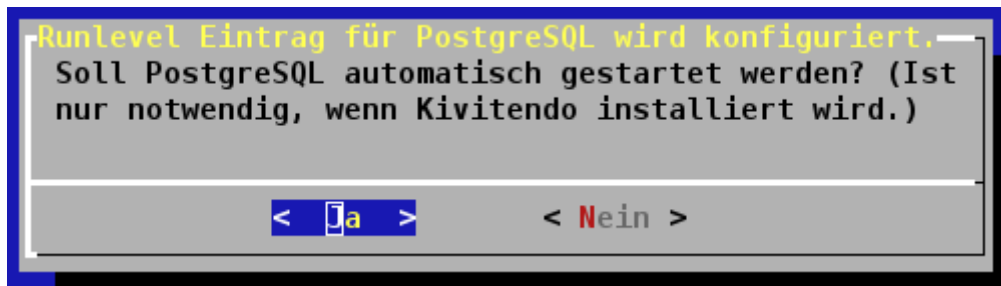
Der PostgreSQL-Dienst wird lediglich benötigt, wenn Sie Kivitendo als ERP-Lösung installieren möchten, oder manuell eigene Software wie etwa die ERP-Lösung 1C nachinstallieren.

Im Falle von 1C wird eine speziell dafür gepatchte PostgreSQL-Version benötigt, dies wird vom invis-Server unterstützt. Dazu erscheint folgende Abfrage:



Beantworten Sie die Frage mit „ja“ wird die reguläre aktuelle Version von PostgreSQL installiert, bei „nein“ die für 1C gepatchte Version.

Anschließend wird gefragt, ob PostgreSQL automatisch gestartet werden soll. Wie gesagt ist dies nur notwendig, wenn er auch gebraucht wird.



Damit ist auch dieses Modul abgeschlossen.

Modul: firewall

Typ: automatisch

Dieses Modul richtet die Firewall des Servers ein. Dabei wird auch der verschobene SSH-Port für den Zugriff von extern gesetzt. Sollten Sie via SSH über Port 22 mit dem Server verbunden sein, wird diese Verbindung nicht unmittelbar unterbrochen. Erst eine gewisse Idle-Time, wenn also keine Daten über die Verbindung laufen führt zum Kappen der Verbindung. Danach kann die Verbindung bei externem Zugriff nur noch über den verschobenen Port aufgebaut werden.

Beenden Sie **sine** daher am besten nach dem Modul, trennen Sie die SSH-Verbindung und bauen Sie über den neuen Port wieder auf. Danach können Sie **sine** wieder starten.

Modul: openvpn

Typ: automatisch

Ein VPN-Zugang zum Server ist eigentlich ein Muss, vorausgesetzt Ihr Server ist via Internet erreichbar.

Modul: acupsd

Typ: interaktiv

Es wird der USV-Überwachungsdienst „acupsd“ installiert und vorbereitet. Dieser Dienst funktioniert lediglich in Verbindung mit unterbrechungsfreien Stromversorgungen der Fa. APC. Damit ist es möglich den Server im Falle eines Stromausfalls rechtzeitig automatisch herunterzufahren um Schäden zu vermeiden. Weiterhin können die Betriebsdaten der USV ausgelesen und im invis-Portal angezeigt werden.

Das Modul fragt, ob Sie **apcupsd** installieren möchten.

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 und 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 Zaráfa ausgewählt und dieses Modul übersprungen, steht kein IMAP-Dienst zur Verfügung.

Modul: monitoring

Hier ist lediglich der Installation der Monitoring Umgebung zuzustimmen. Die Auswahl des zu verwendenden Systems ist bereits im Verlauf des Moduls „quest“ erfolgt.

Modul: groupware

Auch hier ist lediglich der Installation der bereits ausgewählten Groupware zuzustimmen. Je nach gewählter Groupware ist vor allem das jeweilige Kapitel zur „Nacharbeit“ zu beachten.

Wurde Tine 2.0 als Groupware gewählt, notieren Sie sich bitte das angezeigte Passwort. Sie benötigen es für alle weiteren Einrichtungsschritte.

Modul: erp

Das übliche. Stimmen Sie der Installation der zur Verwendung gewählten ERP-Lösung zuzustimmen. Im Falle von „Wawision“ müssen Sie sich lediglich das im Verlauf des Moduls angezeigte Datenbank-Passwort notieren. Sie benötigen es zur späteren Einrichtung der Software.

Modul: faxgate

Dieses Modul sollten Sie überspringen, Fax auf ISDN-Basis ist gegenwärtig kaum noch machbar. Überdies ist das Modul auch nicht mehr vollständig funktionsfähig, da die notwendigen FCPCI-Treiber nicht mehr automatisch installiert werden können.

Modul: webcdwriter - Entfällt ab invis-Version 13.0

WebCDwriter ist irgendwie aus nostalgischen Gründen noch Bestandteil des invis-Servers. ...aber wer braucht noch heute noch eine Software zum Brennen von CDs. (genau CDs, nicht DVDs oder gar BlueRay).

Modul: openvpn

Hinweis: Ab invis-Server Version 13.0 haben wir dieses Modul zum Pflichtmodul gewandelt und entsprechend vorverlegt.

Ein VPN-Zugang zum Server ist eigentlich ein Muss, vorausgesetzt Ihr Server ist via Internet erreichbar.

Sie sollten der Installation zustimmen und das entsprechende Kapitel unter Nacharbeit lesen.

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: owncloud

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

From:
<https://wiki.invis-server.org/> - invis-server.org

Permanent link:
https://wiki.invis-server.org/doku.php?id=invis_server_wiki:installation:sine-110&rev=1527355272

Last update: 2018/05/26 17:21

