Anwendug des Setup-Scripts

Auch nach der Umstellung auf ein RPM-basiertes Setup wird die weitere Installation vom Setup-Script (***sine2*** – „**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.*

```
linux:~ # sine2
```

sine2 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.
- ***sine2 showpws*** - zeigt alle während des Setups generierten Passwörter an.
- ***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.

sine2 verwendet das Verzeichnis

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

als Arbeitsverzeichnis für die Ablage von Informationen zur Steuerung des Script-Laufs. Mit Einführung von ***sine2*** ist die Verzeichnisstruktur unter:

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

hinzugekommen. Hier finden sich beispielsweise die einzelnen Modul-Scripts sowie die Kopnfigurationsvorlagen. 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.

Bei der Entwicklung der invis-Server Version 14.0 haben wir besonderes Augenmerk darauf gelegt den Script-Lauf zu vereinfachen. Das Script erledigt jetzt wesentlich mehr Schritte selbständig auch die Anzahl der Informationsabfragen wurde deutlich reduziert. Dadurch wird der Durchlauf des Scripts bei weitem seltener durch Interaktionen unterbrochen als in früheren Versionen. So werden beispielsweise keine automatisch generierten Passwörter mehr in Form von Ausgabefenstern

angezeigt, mit der Bitte diese zu dokumentieren. Alle Passwörter landen jetzt in einer sine2-Arbeitsdatei und können wie oben beschrieben mit der Option „showpws“ ausgegeben werden. Die Ausgabe setzt root-Rechte voraus.

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



Nach einem kurzen Datenschutzhinweis fragt das Modul „check“ lediglich nach, ob alle hier beschrieben Voraussetzungen für das invis-Server Setup mit ***sine2*** 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 Software-Pakete.

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 ***sine2***, sie können später mit:

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

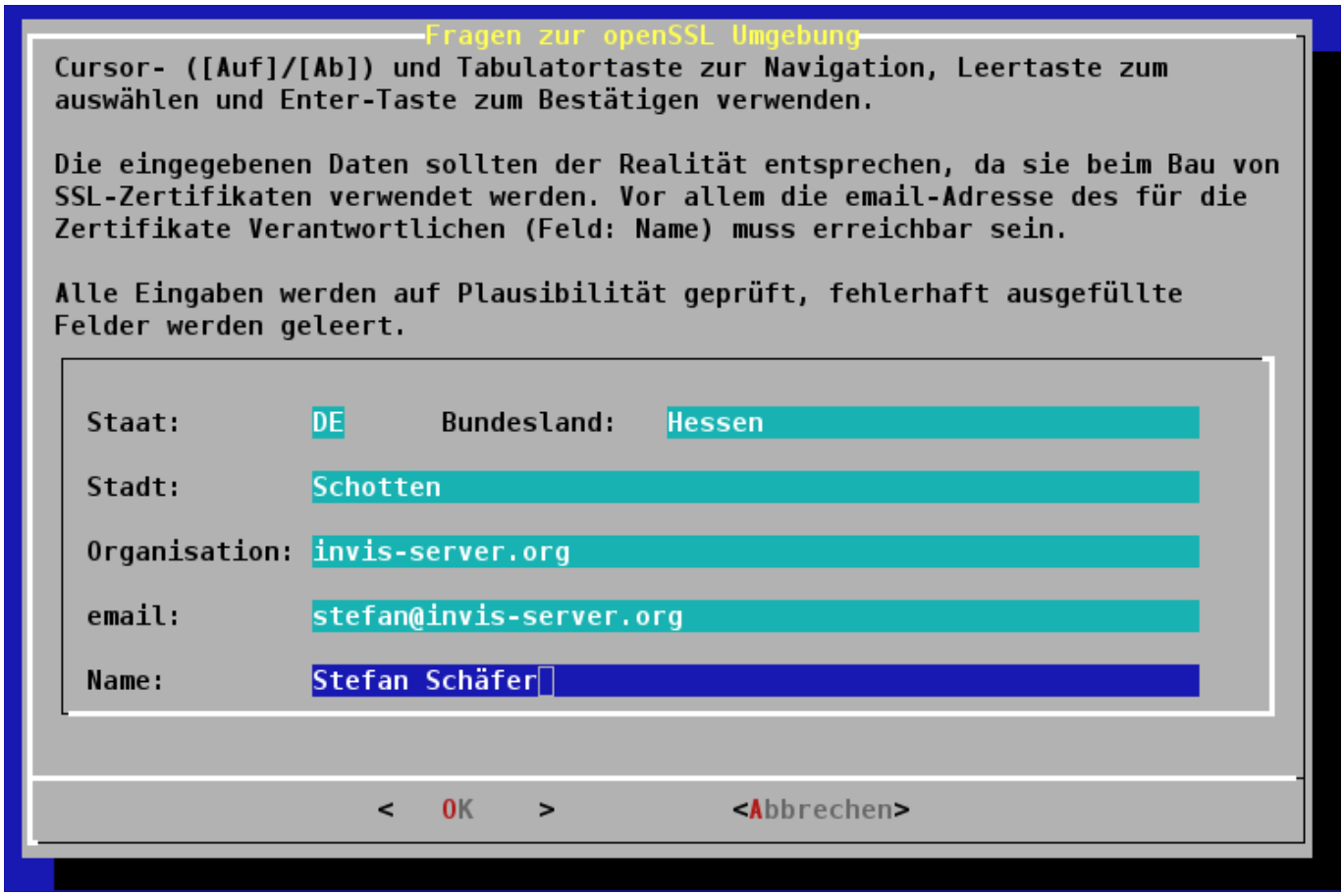
und

```
linux:~ # sine showpws
```

abgefragt werden.

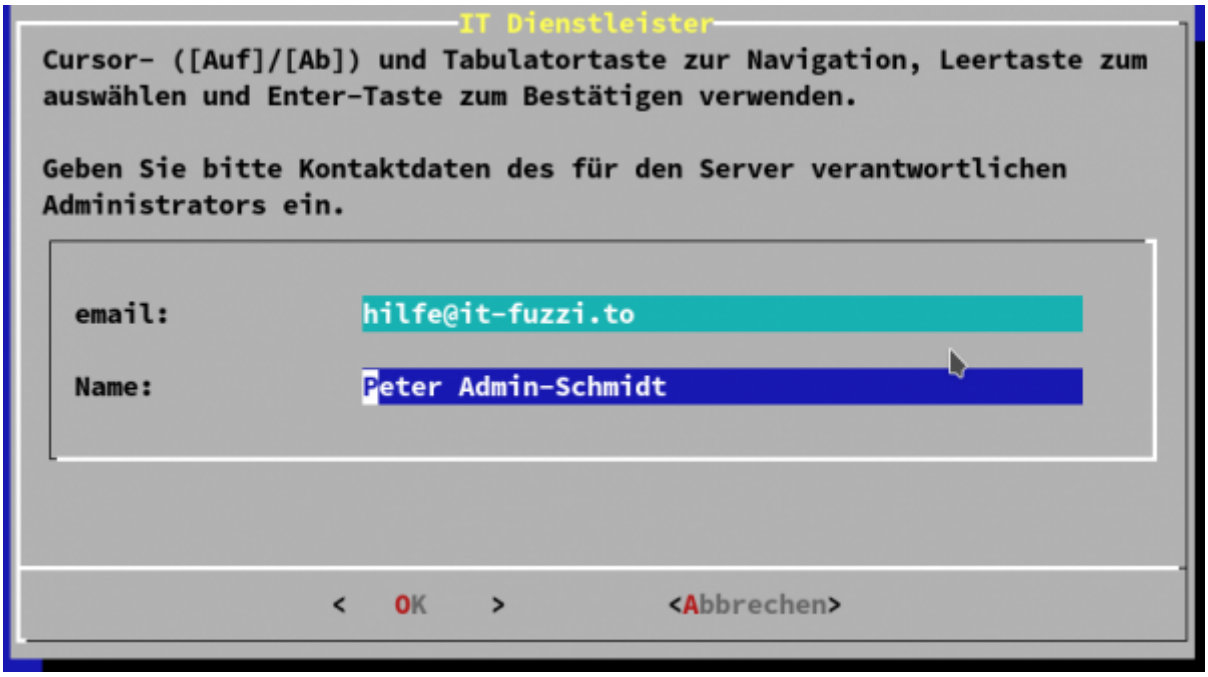
Es ist wichtig hier genau aufzupassen und korrekte Informationen einzugeben. Einige Informationen wie etwa die konfigurierten IP-Adressen und den Hostnamen ermittelt ***sine2*** selbst. Das Modul zeigt diese Informationen an. Prüfen Sie die Ausgaben bitte genau. Sollten wiedergegebene Informationen falsch 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).



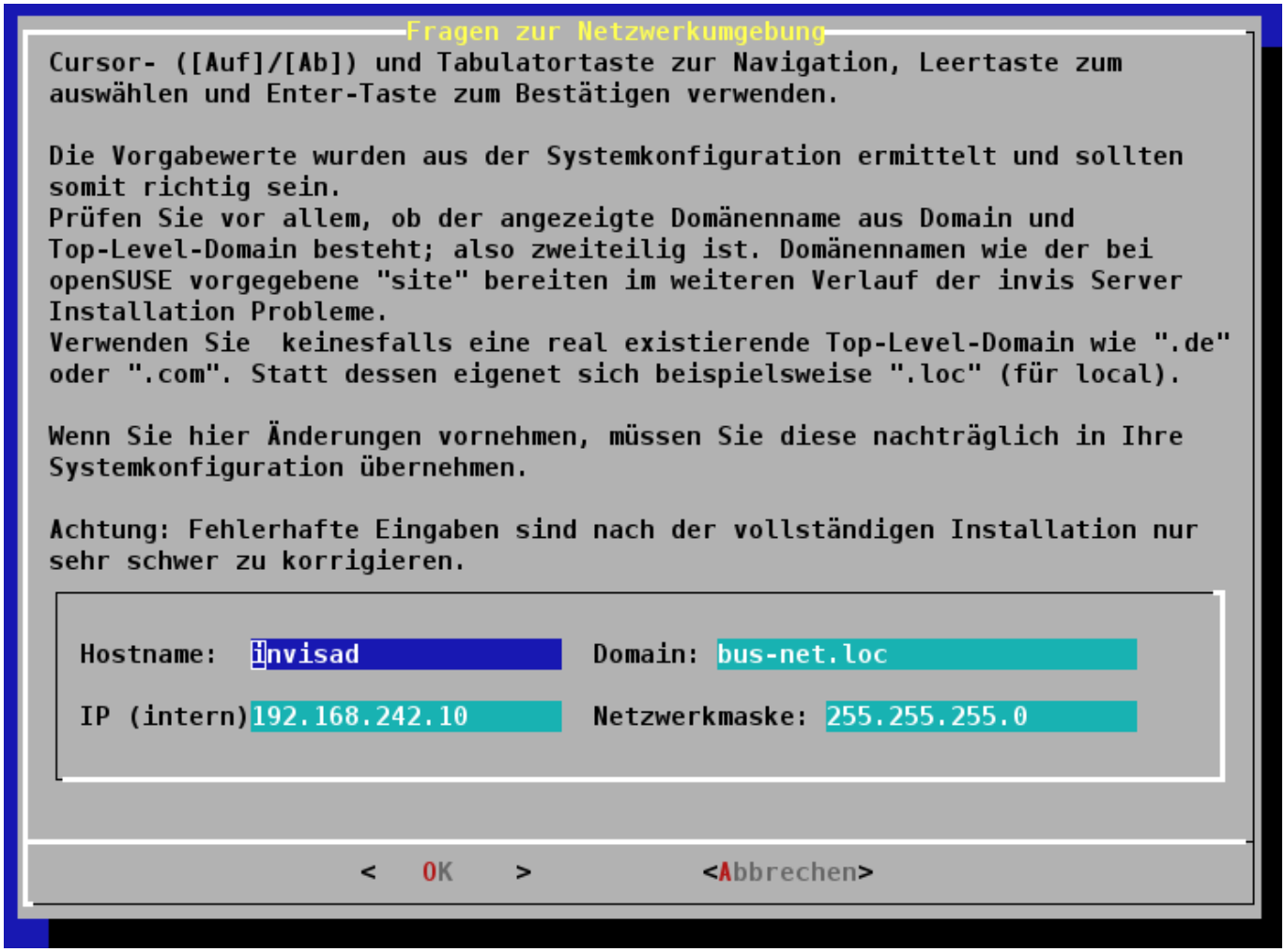
Die hier von Ihnen eingegebenen Informationen werden später in jedem Server-Zertifikat sowie dem Stammzertifikat der Server-eigenen Zertifizierungsstelle hinterlegt. Die Informationen können von jedem Client, beispielsweise Ihrem Browser angezeigt werden, sie sollen Authentizität vermitteln und somit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

Im nächsten Schritt werden Kontaktinformationen des für die Server-Administration zuständigen Administrators abgefragt.



Die eingegebene E-Mail-Adresse wird vom Server genutzt um ggf. Warnmails an den Dienstleister zu senden.

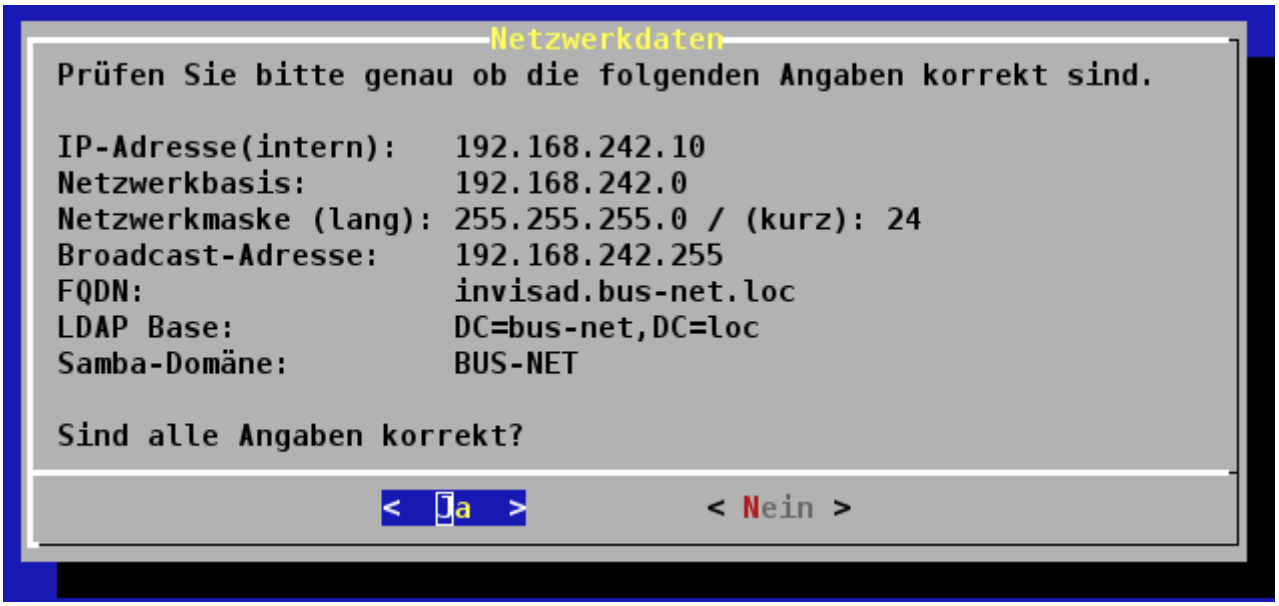
Im nächsten Schritt versucht ***sine2*** Informationen über die Netzwerkkonfiguration Ihres Servers zu ermitteln und zeigt diese an:



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.

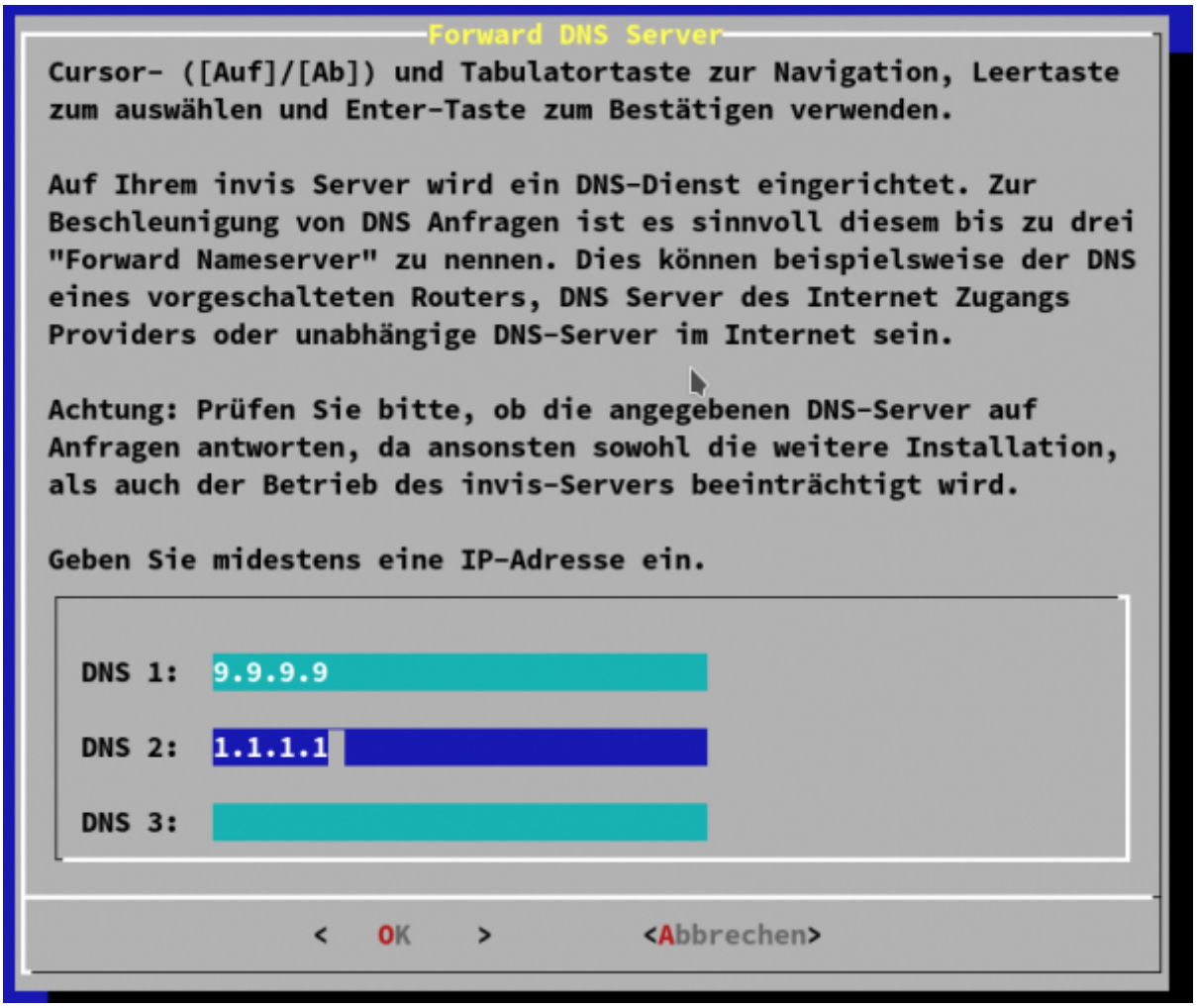
Achten Sie auch darauf, dass die hier angezeigte Domain sich aus Domain und Top-Level-Domain also „domain.tld“ besteht. Fehlt die TLD führt dies auch zu massiven Folgefehlern.

Aus den angezeigten bzw. eingegebenen Informationen berechnet ***sine2*** 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.

Die in der Beispiel-Abbildung angegebenen DNS-Server „9.9.9.9“ und „1.1.1.1“ sind tatsächlich eine gute Wahl. Hinter beiden Adressen, stehen Dienstleister die sich dem Datenschutz verpflichtet fühlen. Informationen zu beiden Diensten liefert Heise:

- **9.9.9.9 - Anbieter: Quad9**
- **1.1.1.1 - Anbieter: Cloudflare**

Es folgt die Frage nach der gewünschten Groupware:



Zur Auswahl stehen derzeit 3 verschiedene Kombinationen aus IMAP-Server und Groupware. Achten Sie unbedingt auf die Bemerkungen rechts neben der Auswahl. Noch sind für invis-Server 14.x nicht alle geplanten Kombinationen verfügbar. Wir arbeiten daran. Derzeit (Stand: Mai 2018) sind lediglich Kopano und die Kombination aus Dovecot und Roundcubemail voll integriert. Die Lösung eGroupware haben wir anstelle von Tine20 ins Auge gefasst. Konkrete Pläne für eine Implementation gibt es derzeit jedoch noch nicht.

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

Wurde Kopano als Groupware ausgewählt, folgt ein zweites Auswahlfenster. Hier muss entschieden werden aus welchem Repository Kopano installiert werden soll. Zur Auswahl stehen:

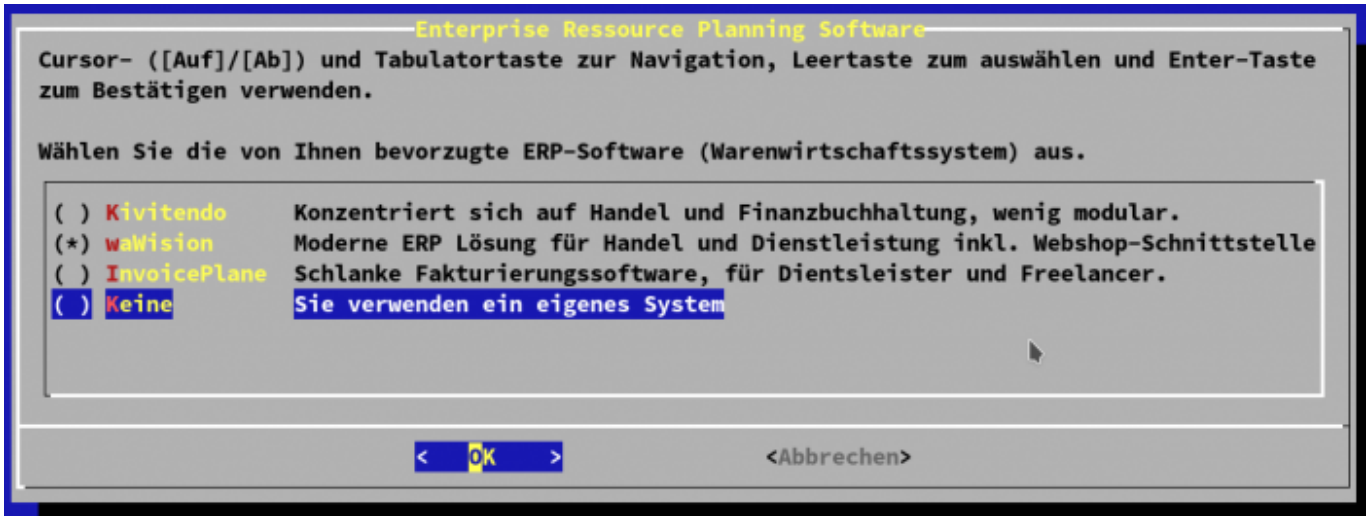
- **Kopano Limited** – Dieses Repository wird von Kopano selbst bereit gestellt. Es enthält getestete Pakete, für die Kopano limitierten Support im Rahmen einer Subskription gewährt. Um

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.



Auf einem invis-Server haben Sie auch die Möglichkeit eine ERP-Software zu betreiben. Sie haben die Auswahl zwischen WaWision, Kivitendo und der wesentlich einfacheren Fakturierungslösung InvoicePlane:



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

Es folgt eine weitere Software-Auswahl:



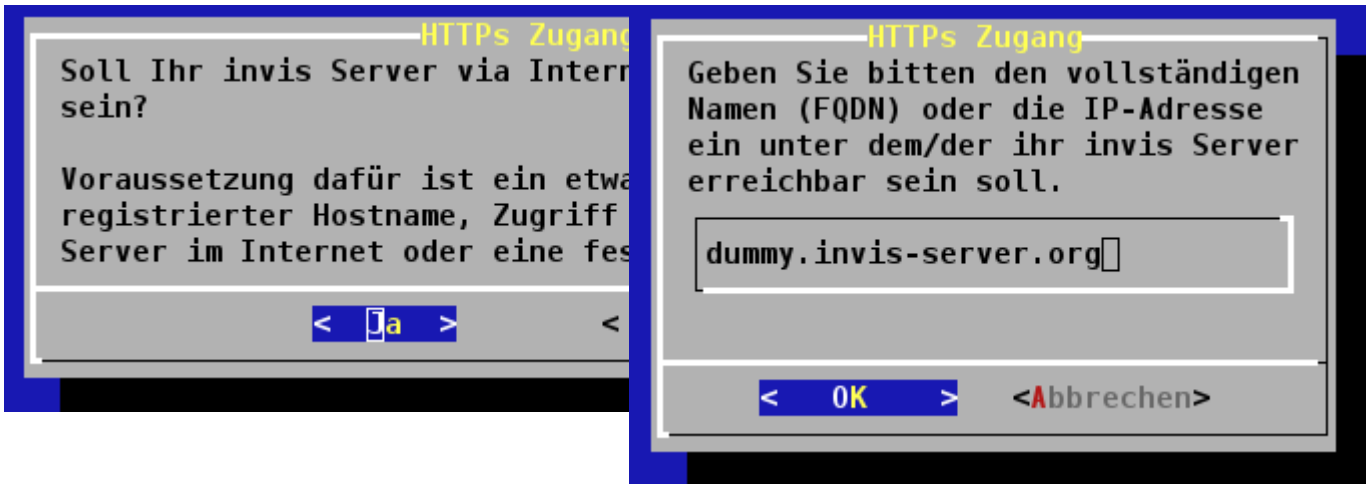
Sie können einen invis-Server mit Hilfe eines Monitoring Systems fernüberwachen. Vorbereitet haben wir die Nutzung von Nagios/Icinga und Zabbix. Wählen Sie nach Belieben.

Einen invis-Server via Internet von überall 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 die vom Provider zugewiesene dynamische IP-Adresse immer wieder mit dem gültigen Namen zu verbinden.

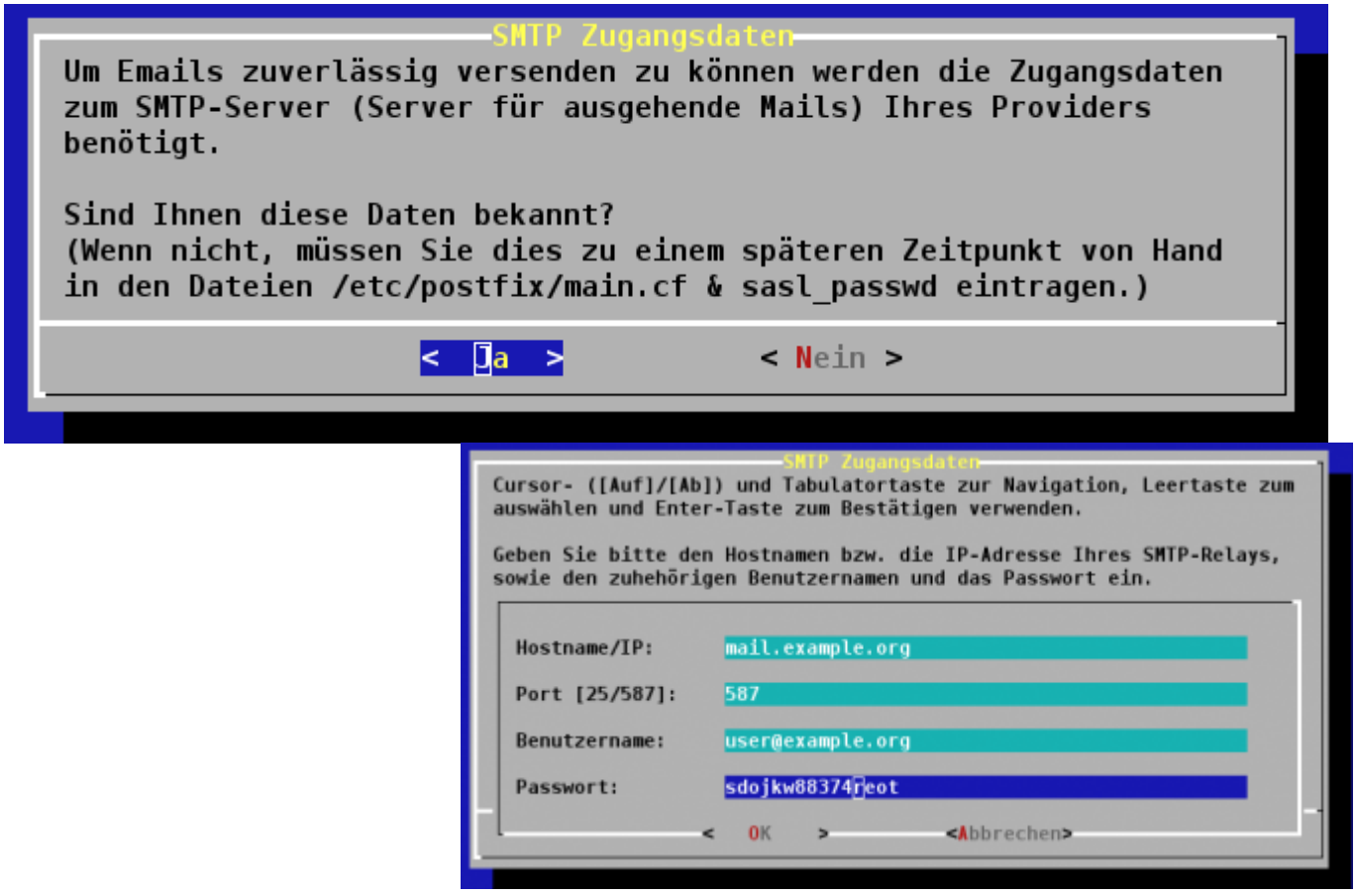
Um dies zu tun können Sie sich auf die Dienste eines entsprechenden Anbieters im Internet verlassen oder Sie betreiben eigene DNS-Server die per DDNS aktualisiert werden können. Für letztere Möglichkeit kann ein invis-Server direkt als DDNS-Client fungieren.\\Für Möglichkeit Nr. 1 können Sie auf dem invis-Server die Software „ddclient“ installieren oder diese Funktion 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.*



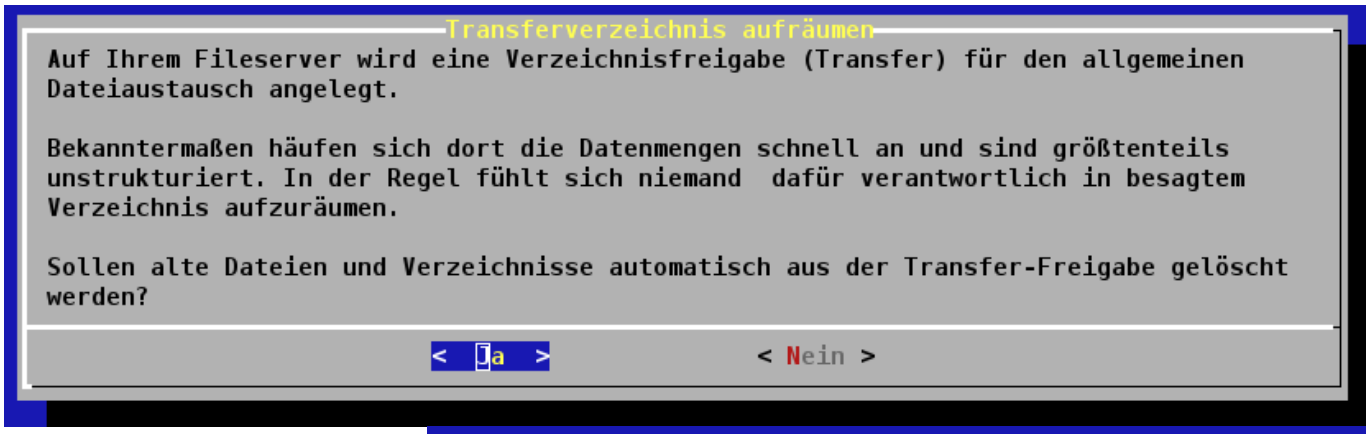
Um Emails versenden zu können benötigt ein invis-Server Zugangsdaten um sich per „SMTP-Auth“ an einem Mailrelay (Smarthost) anmelden zu können. Üblicherweise ist dies der Mailserver Ihres Internet-Service-Providers oder der des Webhosters bei dem Sie Ihre Mailkonten verwalten.



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.





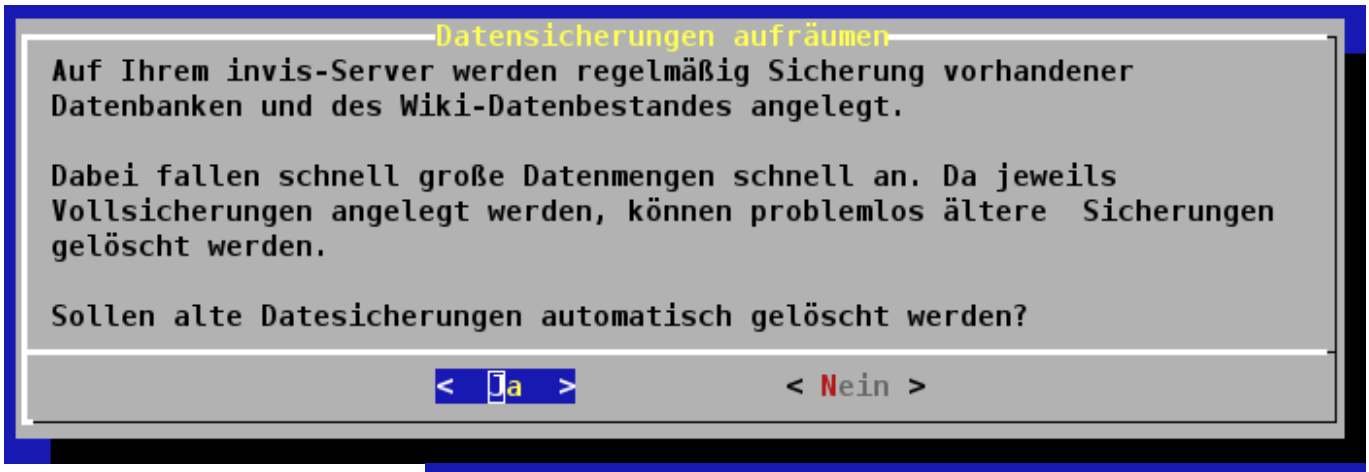
Geben Sie an, ob Sie eine automatische Bereinigung wünschen und wie alt Dateien dort maximal werden dürfen.

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

---

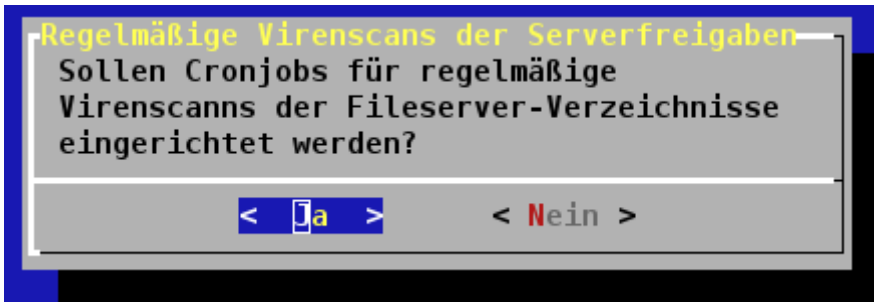
invis-Server führen intern eine Reiche von Datensicherungsaufgaben durch. Gesichert werden regelmäßig alle Datenbanken sowie das Wiki. Da dies relativ schnell eine Menge Festplattenplatz in Anspruch nimmt kann der Server auch hier regelmäßig aufräumen und alte Sicherungen löschen.

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



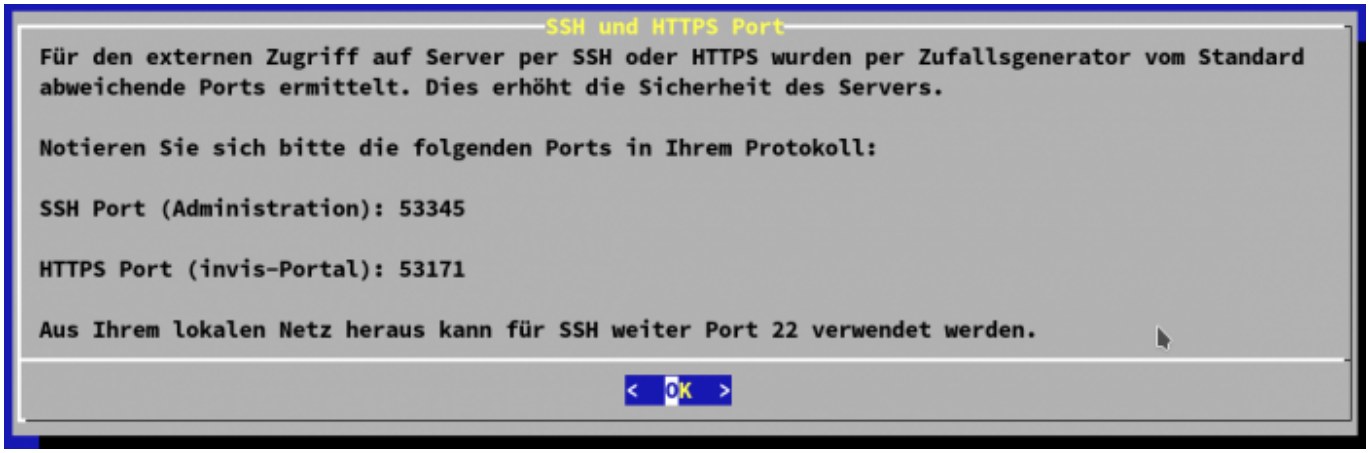


Eine weitere regelmäßige Wartungsfunktion des invis-Servers ist die zyklische Überprüfung der Fileserver-Freigaben auf Viren. Sie können auswählen, ob Sie dies wünschen oder nicht.



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. 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.

Anders als bei früheren Versionen werden in der Regel nur 2 Ports (SSH & invis-Portal via HTTPs) ausgegeben. Bei älteren Versionen wurde noch ein Port für den Zugriff auf ownCloud generiert. Dies hat sich in der Praxis als kontraproduktiv erwiesen. Beim Teilen von Dateien generierte Links die einen solchen Port enthielten waren für viele Empfänger dann nicht erreichbar, wenn der Empfänger hinter einem Proxy-Server saß.

Modul: sysprep

Typ: interaktiv

Das Modul „sysprep“ führt weitere Vorbereitungsaufgaben durch. Darunter die Installation des Virenscanners, der erforderlichen Samba-Pakete und weitere Software. Weiterhin werden grundlegende Systemkonfigurationen getroffen.
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 nachfolgenden 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. Wir haben*

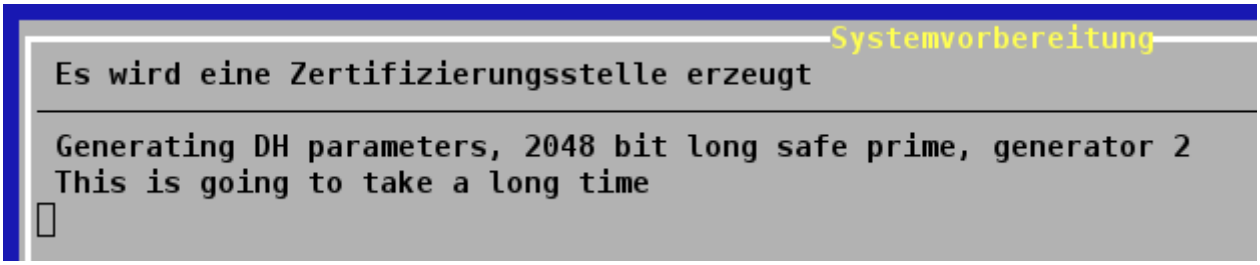
versucht auf die händische Eingabe von Passwörtern im Script-Lauf vollständig zu verzichten. An dieser Stelle ist uns das leider nicht gelungen.



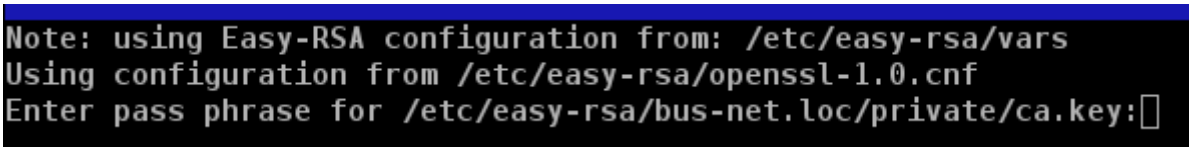
sine fragt beim Erstellen der CA Informationen ab, die im Zertifikat der CA enthalten sein werden. In den meisten Fällen können Sie die Vorgaben übernehmen. Achten Sie beim CN (Common Name) **unbedingt** darauf den Vorgabewert „Easy RSA CA“ durch eine individuelle und vor allem eindeutige Vorgabe zu 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.



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



Anders als in früheren Versionen unseres Setup-Scritps werden jetzt alle drei vom Server benötigten Schlüssel-/Zertifikatspaare direkt im Anschluss an die Erstellung der CA generiert. Dies erfordert, dass Sie das gewählte Passwort, auch wenn es langweilig ist jetzt noch 3 mal (LDAP-Server- und Mail-Server-Zertifikat, sowie das Zertifikat für externe Zugriffe und OpenVPN) eingeben müssen. Der dadurch erkaufte Vorteil sind drei Unterbrechungen weniger in den nachfolgenden sine2-Modulen.

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

Ihre einzige Aufgabe innerhalb dieses Moduls ist es das oben genannte Passwort zur Kenntnis zu nehmen und dessen Ausgabe zu quittieren.

Nachdem ***sine2*** 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 schreibt es in die sine2-Passwortdatei.

Bringen Sie für dieses Modul ein wenig Geduld auf. Es werden im Verlauf des Moduls auch die Kopano-Schemaerweiterungen eingespielt, dass auch wenn Sie Kopano gar nicht nutzen möchten (Strategische Gründe). Das Einspielen der Erweiterungen dauert eine Weile.

```
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.

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: automatisch

In diesem Modul wird alle für die Mailserver-Funktion benötigte Software installiert und soweit möglich vorkonfiguriert.

Modul: cups

Typ: automatisch

Eingerichtet wird der Druckspooler CUPS inklusive eines virtuellen PDF-Druckers.

Modul: fileserver

Typ: automatisch

Auch bei der Einrichtung des Filservers sind keine weiteren Angaben Ihrerseits erforderlich. Es werden die Standard-Freigaben des invis-Servers eingerichtet.

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

Permanent link:
https://wiki.invis-server.org/doku.php?id=invis_server_wiki:installation:sine-140&rev=1527354109

Last update: **2018/05/26 17:01**