

invis-Server-Setup mit sine2

Mit dem Umstieg auf openSUSE Leap 16.0 und invis-Server 16.0 haben wir das Server-Setup erst einmal gründlich abgespeckt. Im ersten Schritt geht es uns darum einen stabilen Infrastruktur-Server zu realisieren, entsprechend liegt der Fokus auf den grundlegenden Diensten wie ActiveDirectory, DHCP und DNS. Erhalten bleiben ein Webserver-Setup zum Betrieb des invis-Portals, ein sauberes Firewall-Setup, OpenVPN wie auch eine einfacher Mailserver auf Basis von Dovecot und Postfix.

Aus dem Setup entfernt wurden zunächst die Groupware **Kopano**, dessen Entwicklung wurde eingestellt. Gleiches gilt für **ownCloud**, was wir in naher Zukunft durch **openCloud** ersetzen werden. Ebenfalls verschwunden ist die Zeiterfassungssoftware **Kimai** und jedwede ERP Lösung.

Erhalten bleibt allerdings **Dokuwiki** und auch die Möglichkeit virtuelle Maschinen per **Virtualbox** auf dem Server zu installieren.

Hinzu kommt zunächst die Möglichkeit den Server mittels der Web-basierten Software **Cockpit** zu administrieren. Spannend daran ist, dass Leap 16 mit **Podman** ein modernes Container-Management mitbringt, welches ebenfalls per **Cockpit** administriert werden kann.

Anwendung 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 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 beschriebenen 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 die für einen invis-Server unerlässlich sind.

Modul: quest

... in Arbeit!

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:~ # sine2 showconf
```

und

```
linux:~ # sine2 showpws
```

abgefragt werden.

Es ist wichtig hier genau aufzupassen und korrekte Informationen einzugeben. Einige Informationen wie etwa die konfigurierten IP-Adressen 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.

Hinweis: Im Zuge der Weiterentwicklung des invis-Servers verändern sich die Abfragen hin und wieder. Nicht jede Änderung wird hier unmittelbar in die Setup-Beschreibung aufgenommen. Das ist einfach eine Frage des Aufwands. Wir geben uns aber Mühe die Abfragen so zu formulieren, dass sie auch ohne Beschreibung hier zu beantworten sind.

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 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.

IT Dienstleister

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

Geben Sie bitte Kontaktdaten des für den Server verantwortlichen Administrators ein.

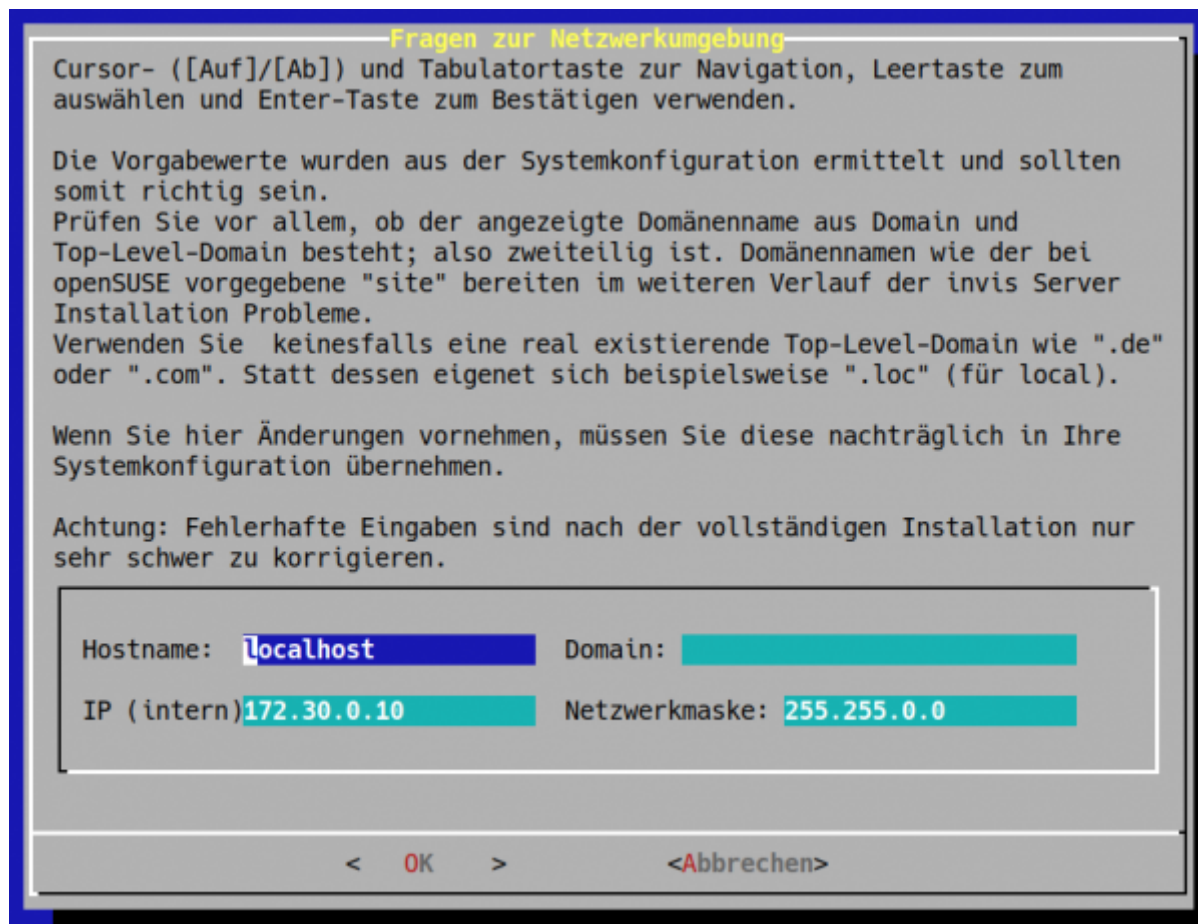
email:	hilfe@it-fuzzi.to
Name:	Peter Admin-Schmidt

< OK > <Abbrechen>

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

Ab invis-Server Version **14.2** erscheint danach ein weiteres Fenster in dem nach Kontaktdaten gefragt wird. Hier müssen Name und Email-Adresse eines vor Ort Verantwortlichen eingegeben werden. Dieser Kontakt enthält alle Mails die an den externen Betreuer gehen in CC.

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



Neu ab invis-server 16.0 ist, dass im Feld Hostname „localhost“ steht und das Feld Domain leer ist. Dies ist zwingend auszufüllen. Der Hostname wird dann im folgenden automatisch gesetzt, was bedeutet, dass die Dateien

/etc/hostname

und

/etc/hosts

automatisch angepasst werden.

Hostname:	invis	Domain:	invis-net.lan
IP (intern)	172.30.0.10	Netzwerkmaske:	255.255.0.0

Sollten die Felder für IP-Adresse und Netzmaske leer sein oder falsche Daten zeigen, 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 mit unserem Script **netdevconf** 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.

Netzwerkdaten

Prüfen Sie bitte genau ob die folgenden Angaben korrekt sind.

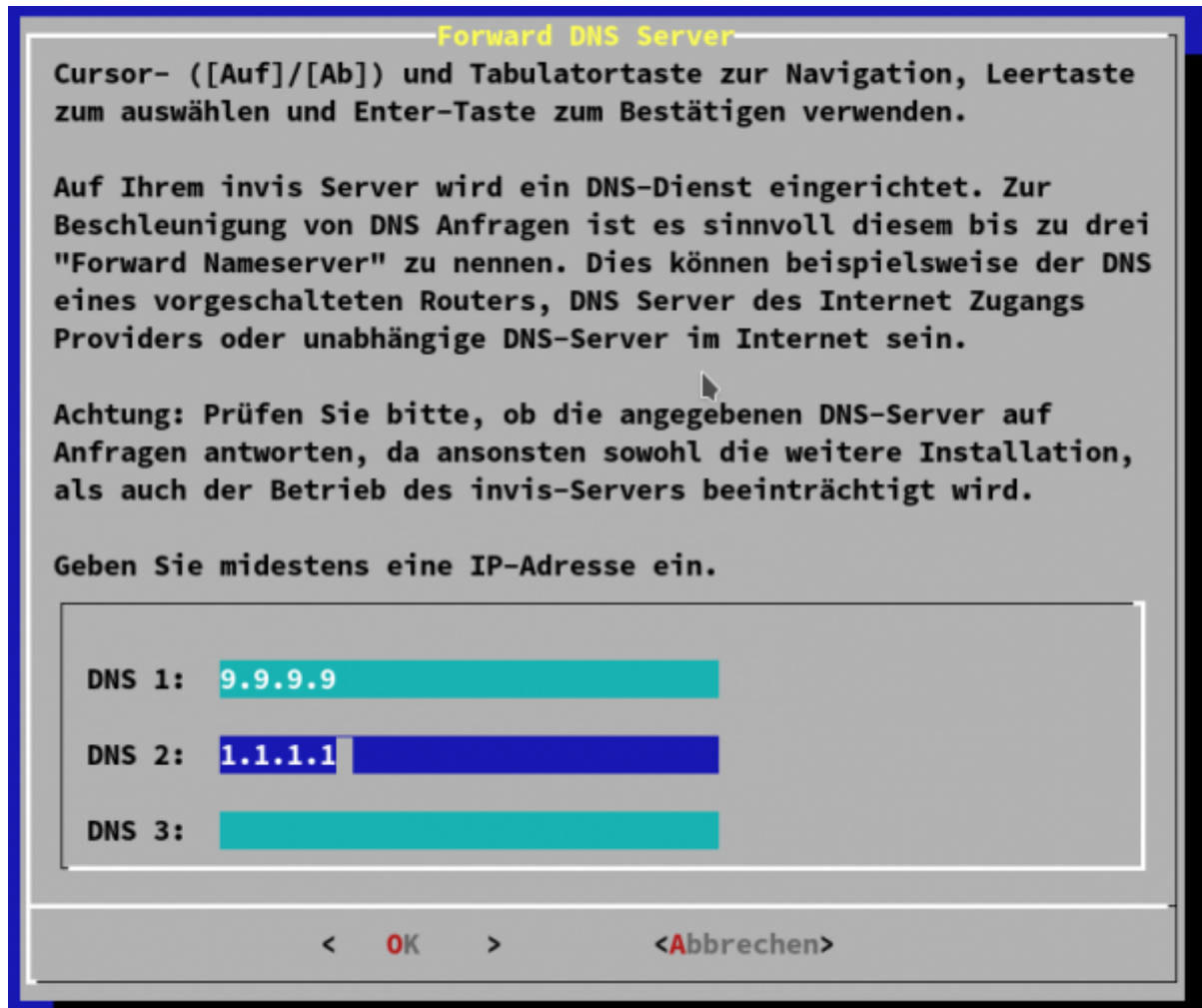
IP-Adresse(intern):	172.30.0.10
Netzwerkbasis:	172.30.0.0
Netzwerkmaske (lang):	255.255.0.0 / (kurz): 16
Broadcast-Adresse:	172.30.255.255 172.30.0.0
FQDN:	invis.invis-net.lan
LDAP Base:	DC=invis-net,DC=lan
Samba-Domäne:	INVIS-NET

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.



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**

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

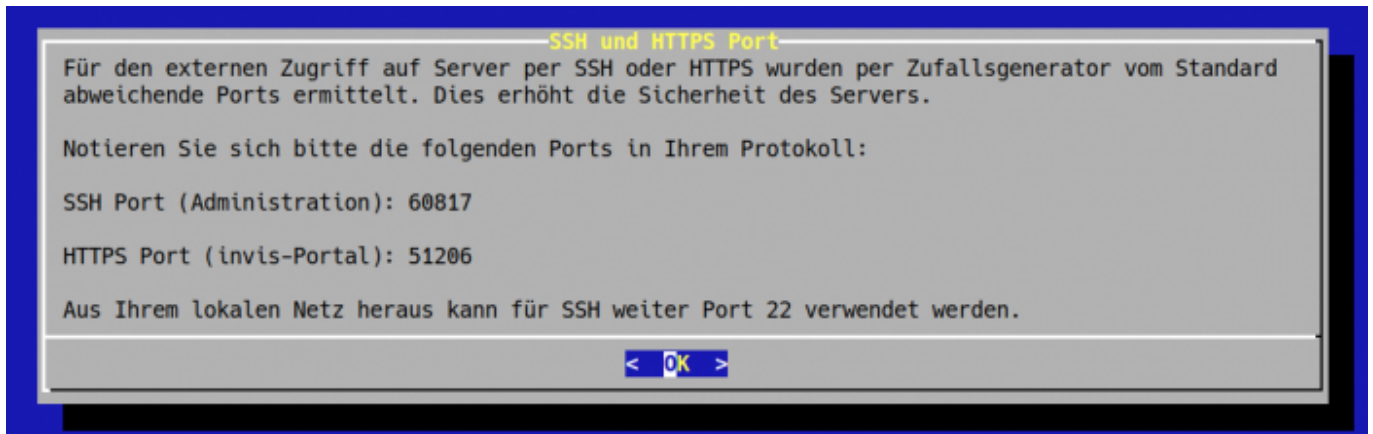
auf dem invis-Server die Software „ddclient“ installieren oder diese Funktion auf einem vorgeschalteten Router einrichten.

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.



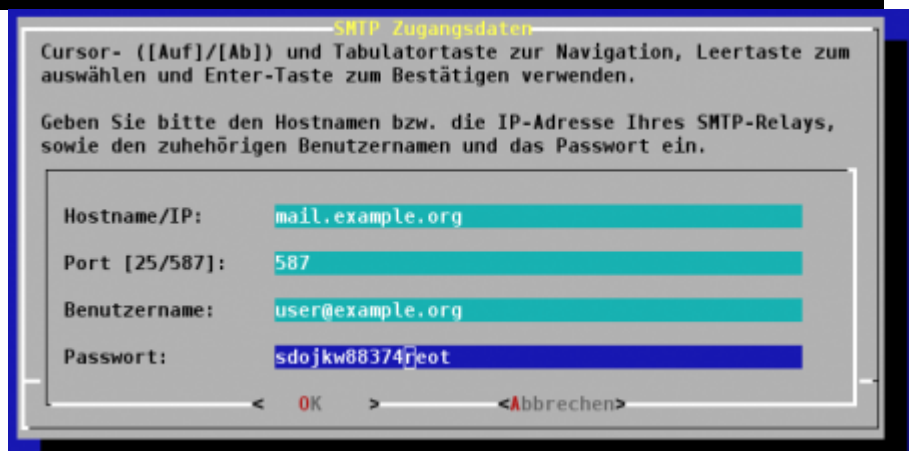
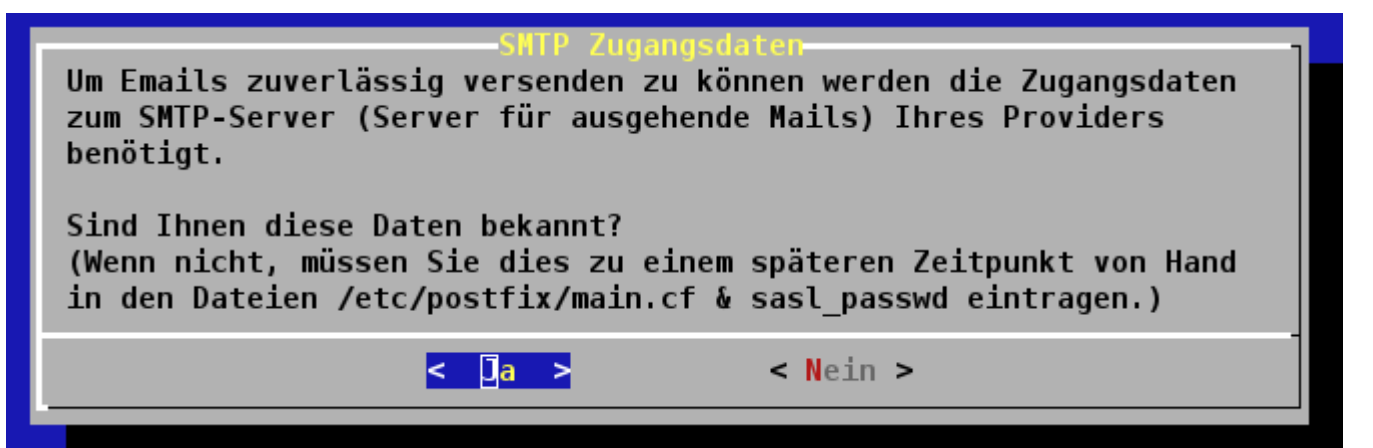
Aus Sicherheitsgründen lauscht Ihr invis-Server bei Verbindungen aus dem Internet nicht auf den Standard-Ports der zugehörigen Protokolle. Statt dessen werden Ports per Zufallsgenerator fest gelegt. Zum Abschluss des „quest“ Moduls zeigt **sine** diese Ports an.



Fügen Sie diese Ports bitte Ihrer Dokumentation hinzu.

Anders als bei früheren Versionen werden hier nur die Ports für SSH und invis-Portal Zugriffe via HTTPS ausgegeben.

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 zunächst 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.

Einzelne Provider wie etwa IONOS sind dazu übergegangen dass sich jede Mailadresse von der aus eine Mail versendet werden soll auch eine individuelle Authentifizierung am Provider-Mailserver

erfolgen muss. Dies unterstützt der invis-Server ebenfalls, dass kann aber im laufenden Betrieb weitgehend automatisiert konfiguriert werden.

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

Das invis-Portal zeigt dem Nutzer einige Status-Daten des Servers, darunter auch Informationen zum Zustand der Festplatten. Abhängig vom verwendeten Festplattentyp und der dementsprechend vom Hersteller gewährten Garantie wird der verbleibende Lebenszeitraum der Festplatten geschätzt. Dabei wird davon ausgegangen, dass eine Festplatte den Garantiezeitraum üblicherweise unbeschadet übersteht und am Ende des Zeitraums über einen vorsorglichen Tausch der Platten nachgedacht werden sollte. Beachten Sie dabei aber, dass dies nur eine Empfehlung ist, eine Festplatte auch deutlich länger leben aber auch viel früher den Geist aufgeben kann. Geben Sie einfach an welchen Typ Festplatte Sie einsetzen.



An dieser Stelle folgten bisher die Fragen nach zu verwendender Groupware und einer ERP-Lösung. Beides wurde entfernt. Eine ERP-Lösung wird gar nicht installiert und anstelle einer Groupware wird ein einfacher IMAP-Server in Kombination mit der Webmail-App **Roundcubemail** installiert.

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.

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.



Damit ist die Fragestunde beendet. Alle Angaben werden zur weiteren Konfiguration des Servers in einer Datei gespeichert. Die eingegebenen Daten lassen sich jederzeit mit folgendem Kommando abrufen:

```
invis:~ # sine2 showconf
```

Modul: sysprep

Typ: interaktiv

Das Modul „sysprep“ führt weitere Vorbereitungsaufgaben durch. Darunter auch die Installation des Virenschanners. Installiert wird **ClamAV**; dass dies nicht bereits im Modul „check“ geschieht liegt daran dass wir uns vorbehalten auch kommerzielle Virenschanner zu unterstützen und dies zukünftig wieder im Modul „quest“ abzufragen.

Weiterhin werden automatisiert einige grundlegende Systemkonfigurationen vorgenommen.

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.

```
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:
```

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 3 interne Server-Zertifikate, Diffie-Hellman Parameterdateien sowie eine „Certificate-Revocation-List“ (CRL) 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:█
```

Anders als in früheren Versionen unseres Setup-Scripts 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 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 Client 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. Auch wenn **Kopano** nicht mehr Teil des Setups ist, werden im Verlauf des Moduls die Kopano-LDAP-Schemaerweiterungen eingespielt. Das schadet der Installation des Servers nicht, auch wenn das Einspielen der Erweiterungen eine Weile dauert. Daraus ergibt sich die Möglichkeit **Kopano** beispielsweise in einer eigenen VM in Ermangelung an Alternativen noch weiter zu verwenden.

```
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 DHCP-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: cockpit

Typ: automatisch

Das Modul richtet das neue openSUSE Administrationswerkzeug ein. Cockpit ist ein Web-basiertes Tool zur Server-Administration und soll früher oder später das entfernte YaST funktional ersetzen.

Derzeit wird Cockpit lediglich installiert und gestartet, zukünftig wird es mehr in die invis-Server Administration integriert.

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 Fileservers sind keine weiteren Angaben Ihrerseits erforderlich. Es werden die Standard-Freigaben des invis-Servers eingerichtet.

Modul: webserver

Typ: automatisch

Dieses Modul richtet den Webserver Apache inklusive aller virtuellen Hosts und das invis-Portal ein.

Modul: keycloak

Typ: automatisch

Dieses Modul richtet Keycloak einen freien OpenID-Provider ein. Keycloak kann als Bindeglied zwischen OpenID kompatibler Software und der Benutzerverwaltung im Active Directory fungieren.

Modul: mariadbserver

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 im Grunde nicht benötigt, außer Sie möchten manuell eigene Software nachinstallieren die auf PostgreSQL angewiesen ist. Es ist also eine rein vorsorgliche Installation.

Es wird hier lediglich 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 eine Firewall auf Basis der Software **firewalld** auf Ihrem invis-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 **sine2** daher am besten nach dem Modul, trennen Sie die SSH-Verbindung und bauen Sie über den neuen Port wieder auf. Danach können Sie **sine2** wieder starten.

Modul: openvpn

Typ: interaktiv

Ein VPN-Zugang zum Server ist eigentlich ein Muss, vorausgesetzt Ihr Server ist via Internet erreichbar. Im Verlauf dieses Moduls müssen Sie nicht viel tun. Es werden lediglich 2 mal Informationen für Sie ausgegeben. Da ich weiß wie das in der Praxis abläuft (Info → weg klicken... 😊), möchte ich Ihre Aufmerksamkeit hier zusätzlich auf die zweite Info lenken:



Auf dem fertig installierten invis-Server finden Sie in der Freigabe „Service“ im Verzeichnis „VPN-Clients“ Beispielkonfigurationen für verschiedene Client-Betriebssysteme. Auch mit dem Tool **inviscerts** generierte Client-Zertifikate finden Sie dort.

Modul: monitoring

Typ: automatisch

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

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

Modul: groupware

Typ: automatisch

Nach dem Wegfall von Kopano als Groupware wird hier nur noch automatisiert der Webmailer Roundcubemail installiert und eingerichtet.

Modul: dokuwiki

Typ: interaktiv

Dieses Modul installiert das einfache und Ressourcen-schonende Wikisystem „Dokuwiki“, nebst dem Template Bootstrap3 und einiger Erweiterungsmodule. Es benötigt keine SQL-Datenbank und verfügt von Haus aus über eine Benutzerverwaltung mit ACLs, wird beim invis-Server aber an das vorhandene Active Directory angebunden.

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

Modul: virtualbox

Typ: interaktiv

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?

Damit ist das Script-geführte Setup Ihres invis-Servers abgeschlossen. Fertig ist es hingegen noch nicht. Schenken Sie jetzt dem Abschnitt Nacharbeit besondere Aufmerksamkeit. Ein Großteil der installierten Applikationen müssen noch durch ein individuelles Setup laufen bevor sie genutzt werden können.

Bevor Sie jedoch an die Nacharbeit gehen, starten Sie den Server neu und vergessen Sie nicht, dass er danach über die externe Schnittstelle per SSH nur noch über den abgeänderten Port erreichen.

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

Permanent link:
https://wiki.invis-server.org/doku.php?id=invis_server_wiki:installation:sine-160

Last update: **2026/03/09 08:15**

