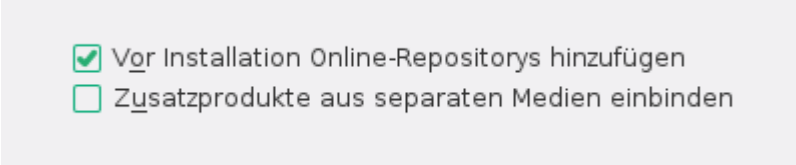
Basis-Installation

Eine Schritt für Schritt Anleitung zur Installation eines openSUSE Linux sollte wohl nicht erforderlich sein. Daher hier nur ein paar Anmerkungen zum Festplatten-Management, der Software-Paket-Auswahl sowie der anschließenden Netzwerkkonfiguration.

Software-Auswahl

Für den invis-Server müssen Sie keine zusätzliche Software installieren, das erledigt unser Setup-Tool von selbst.



Das Setup mit YaST bietet die Möglichkeit, vor der eigentlichen Installation zur Verfügung stehende Online-Repositories einzubinden. Machen Sie davon Gebrauch, da in diesem Fall nach der Installation bereits alle anstehenden Updates eingespielt wurden. Ein paar Bilder weiter, werden die einzubindenden Repositories angezeigt, hier können Sie den Vorschlag einfach übernehmen.

Starten Sie die Installation des Servers von der Netz-Installations-CD und folgen Sie den Anweisungen bis zu dem Punkt, an dem Sie sich für ein Desktop-System entscheiden sollen. Wählen Sie „Minimale Serverauswahl (Textmodus)“ aus. Ein grafisches Desktop-System wird für den Betrieb des Servers nicht benötigt.

Festplatten-Management

Wir gehen hier davon aus, dass Sie keinen Hardware-RAID-Controller im Einsatz haben, sondern statt dessen auf ein Linux-Sowftware-RAID setzen. Vorteil dieser Methode ist auf jeden Fall, die Hardware-Unabhängigkeit sowie der Preisvorteil. Die Investition in einen Hardware-RAID-Controller macht sich hinsichtlich der höheren Performance bemerkbar.

Weiterhin gehen wir von einem einfachen Setup mit lediglich zwei Festplatten aus. Die Verwendung von mehr Festplatten und höheren RAID-Leveln läuft aber prinzipiell nach dem gleichen Schema ab.

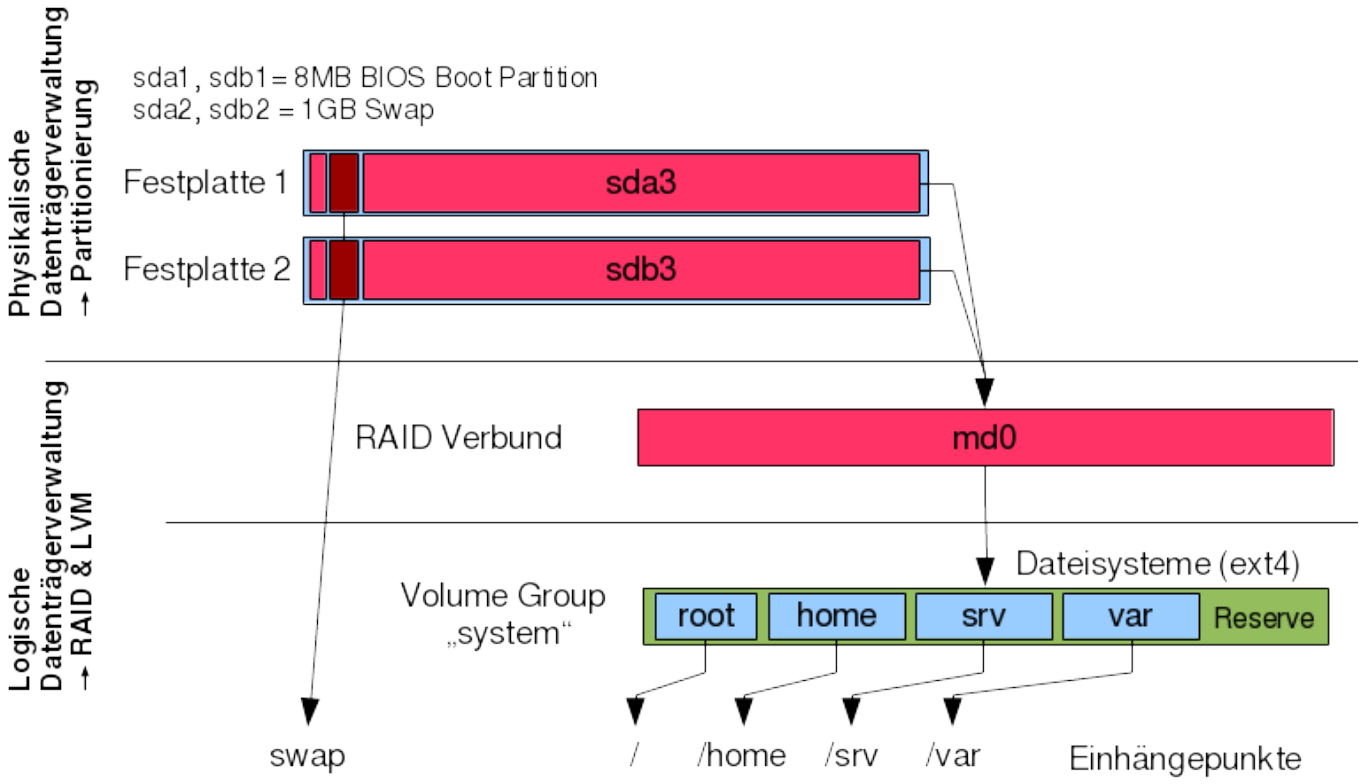
Unabhängig von der Größe der eingesetzten Festplatten bevorzugen wir eine GPT-basierte Partitionierung. Es hat sich gezeigt, dass dies im Falle eines Festplattendefekts weitaus weniger Probleme bereitet, als eine MBR basierte Partitionierung. Wenn Sie mit YaST partitionieren müssen Sie also bevor Sie Partitionen anlegen auf jeden Fall eine GPT Partitionstabelle anlegen (Festplatte auswählen → Schaltfläche „Experte“ → Partitionstabelle anlegen → GPT).

Ziel des Setups ist also eine GPT-basierte Partitionierung. Dafür muss am Anfang jeder Platte (deaktiviertes Secure Boot vorausgesetzt) eine 8MB große Patition vom Typ „BIOS Boot“ angelegt werden, in die Grub seine Boot-Records speichert. Es folgen zwei Swap-Partitionen von max. 1-2GB Größe. Der verbleibende Platz wird mit zwei Partitionen des Typs „Linux RAID“ belegt, die zu einem RAID1-Verbund kombiniert werden. Darauf aufbauend wird die Verteilung des zur Verfügung stehenden Platzes mittels Logical-Volume-Management (LVM) erledigt. Alle Überlegungen lassen sich im Verlauf der Installation bequem mit YaST vornehmen.

Hinweis: *Wer sich statt dessen an einem vollständig manuellen Setup versuchen möchten findet* ***hier*** *eine nicht ganz aktuelle Anleitung.*

Hinweis: *Einige Funktionen des invis-Portals sowie des invis Server eigenen Backup-Tools gehen zwingend von der Kombination aus Software-RAID und LVM aus. Wählen Sie ein anderes Setup können diese Funktionen nicht genutzt werden.*

Einen Überblick über das für invis-Server angestrebte Datenträger-Layout, bietet folgende Grafik:



Hinweis: *Lesen Sie für Systeme mit Festplatten größer 2TB und/oder aktiviertem UEFI-Boot bitte die entsprechenden Hinweise hier.*

Folgen Sie den Instalationsanweisungen der Setup-Routine bis zur Festplatten-Partitionierung. Klicken Sie hier auf die Schaltfläche „Partitions-Setup erstellen…“ → „Benutzerdefinierte Partitionierung (für Experten)“.

Legen Sie auf jeder der beiden (hoffentlich identischen) Festplatten folgende Partitionen an:

1. sdx1 Größe: 8MB - Typ: primär - Partitions-Typ „BIOS Boot“ bzw. „BIOS Grub“ (nicht formatieren!)
2. sdx2 Größe: 1024MB (liegt an Ihnen) - Typ: primär - Dateisystem: swap
3. sdx3 Größe: der gesamte Rest - Typ: primär - Partitions-ID: 0xFD Linux-RAID (nicht formatieren!)

Fassen Sie die jeweils die dritte Partition zu einem weiteren RAID 1 Verbund (md0) zusammen. Dieses Device wird **nicht** formatiert und erhält auch **keinen** Mountpoint.

Fügen Sie das RAID-Device md0 einer LVM-Volumegroup hinzu. Legen Sie auf dieser Volumegroup Logical-Volumes für die Mountpoints /, /var, /home und /srv an. Bevorzugtes Dateisystem hierbei ist generell **ext4**.

Achtung: *Bei der Verwendung von XFS, wie inzwischen vom YaST-Partitionierer vorgeschlagen kommt es zu Problemen bei Datensicherungsstrategieen auf Basis von LVM-Snapshots.*

Die Größen der einzelnen LVs sind von verschiedenen Faktoren abhängig. Für / (root-Dateisystem) sollten 8GB immer ausreichen. Die Größe von /var ist vor allem davon abhängig, welches Datenaufkommen Sie für SQL-Datenbanken und ggf. emails erwarten. Auch die Wahl des IMAP-Servers ist entscheidend. Dovecot legt den gesamten Datenbestand unter „/var/spool/mail“ ab, während Kopano die emails selbst in der eigenen MySQL-Datenbank speichert, deren Attachements aber zuvor abtrennt und in unserem Setup unter „/srv/kopano“ speichert.

Den Großteil des verbleibenden Rests sollten Sie auf /home und /srv verteilen. Hier gilt: Arbeiten die Anwender vor allem im Team gemeinsam an Projekten ist /srv mit viel Platz zu bedenken. Haben Sie es mit einer Horde von Individualisten zu tun, sollten Sie /home mit viel Platz bedenken.

Verteilen Sie auf keinen Fall den gesamten zur Verfügung stehenden Plattenplatz auf die genannten Volumes. Mit einer ordentlichen Reserve, können ungenutzten Platz später nach Bedarf auf die vorhandenen Volumes verteilen. Weiterhin benötigen Sie eine Reserve die Sie temporär für LVM-Snapshots als Basis für Datensicherungen nutzen können. Die Größe dieser Reserve ist abhängig von den zu erwartenden „großen“ Dateien. Wenn Sie beispielsweise virtuelle Maschinen mit großen Festplatten-Images einrichten müssen diese Images in die Reserve passen.

Anpassungen

Mit Einführung von openSUSE Leap 42.1 läuft das openSUSE Setup geringfügig anders ab. Hier ist bei der Minimal-Installation keine Firewall mehr vorgesehen. Da diese aber für den invis-Server elementar ist, sollte in der Zusammenfassung der Installationseinstellungen die Firewall und der SSH-Daemon aktiviert und dann natürlich auch der SSH-Port freigegeben werden.

Die entsprechenden Einstellungen lassen sich in der Installationszusammenfassung vornehmen.

Bestätigen Sie Ihre Einstellungen und überlassen Sie Ihren zukünftigen Server für eine Weile sich selbst; Zeit für ein Bier .

Sollten Sie bei der Installation nicht die Online-Repositories hinzugefügt haben, führen Sie nach Abschluß der Installation zunächst ein vollständiges Online-Update durch. Hierzu bietet sich entweder YaST oder die direkte Verwendung des Paketmanagers ***zypper*** an:

```
linux:~ # zypper refresh
linux:~ # zypper up
```

Da in aller Regel bei diesem ersten Update auch der Kernel aktualisiert wird, ist danach ein Neustart erforderlich.

Letzte Vorbereitungen

Um das invis-Setup einzuleiten benötigen Sie unser Setup-Paket „invisAD-setup“. Dieses Paket ist nicht in den Standard-Repositories enthalten. Es muss also ergänzend eines unserer Repositories eingebunden werden.

Zur Verfügung stehen folgende Repositories zur Vefügung:

1. **spins:invis:stable** - Stabile Version der invis-Server Setup Pakets. Nutzen Sie dieses Repository für produktiv genutzte invis-Server
2. **spins:invis:unstable** - In Entwicklung befindliche Versionen der invis-Server Setup Pakets. Nutzen Sie dieses Repository, wenn Sie uns mit Rat, Tat, Lob oder Kritik bei der Weiterentwicklung unterstützen möchten.

Ab invis-Server Version 12.0 bieten wir eigene Samba-Pakete inkl. Active-Directory an. Diese werden in gesonderten Repositories bereit gestellt. Auch hier wird zwischen „stable“ und „unstable“ unterschieden:

1. **spins:invis:stable:samba46** - Stabile und getestete Samba-Pakete
2. **spins:invis:unstable:samba** - Experimentelle Samba-Pakete zum Testen. Auch hier wünschen wir uns Feedback.

Zur Einbindung des gewünschten Repositories haben wir mit ***invisprep*** ein Script erstellt, welches diesen Schritt automatisch durchführt.

Download: invisprep

Laden Sie es auf Ihren Server herunter, entpacken Sie es und führen Sie es aus.

Hinweis: *Beim direkten Download der Datei mit* ***wget*** *ändert sich der Name der Datei. Das kann beim Entpacken zu Verwirrung führen. Dabei hilft folgende Kommandozeile:*

```
linux:~ # wget -O invisprep.gz
http://wiki.invis-server.org/lib/exe/fetch.php/invis_server_wiki:invisprep.g
z
```

Hinweis: *invisprep wurde bereits so angepasst, dass invis-Server 13.0 damit bereits aus dem unstable Zweig installiert werden kann.*

Danach kann das invis-Setup Paket installiert werden:

```
linux:~ # zypper ref
```

```
linux:~ # zypper in invisAD-setup-12
```

oder „unstable“

```
linux:~ # zypper ref
linux:~ # zypper in invisAD-setup-13
```

Seit Version 11 des invis-Servers ist die Major-Release-Nummer teil des Paketnamens. Sie müssen sie natürlich korrekt angeben. Es ist beispielsweise möglich, dass speziell im „unstable“ Repository mehrere Versionen vorhanden sind.

Hinweis: *Dass bei der Installation des invisAD-setup RPMs sehr viele weitere Software-Pakete installiert werden ist normal.* 😉

Hinweis: *Beim Installieren des Setup-Paketes bemängelt* ***zypper*** *einen Paketkonflikt bezüglich des Nameservers „bind“. Wählen Sie Lösungsvorschlag Nr.:* ***1***

Netzwerkkonfiguration

Um die Basis-Installation abzuschließen, müssen noch die beiden Netzwerkschnittstellen eingerichtet, sowie der voll qualifizierte Name (FQDN) des Servers vergeben werden.

Bei der Namensvergabe gelten folgende Regeln:

- Der Name muss dem Schema ***host.domain.tld*** gehorchen. (*host.tld* ist **nicht** zulässig!)
- Für die Top-Level-Domain (TLD) muss eine Fantasie-Domain wie beispielsweise ***.loc***, ***.corp*** oder ***.lan*** verwendet werden. Die Verwendung einer im Internet gültigen Domain führt zu Problemen beim Routing und dem EMail-Handling.

Um die Benennung der Netzwerkschnittstellen mit den einzelnen Firewall-Zonen eines invis-Servers in Verbindung zu bringen, haben wir uns entschlossen, auf Basis von udev-Regeln klare Namen für die Netzwerkschnittstellen zu vergeben. Auch die Benennung der im Laufe des Setups einzurichtenden VPN-Schnittstelle wurde ein entsprechender Name gegeben:

Früherer Gerätename	Aktueller Name
eth0	extern
eth1	intern
tun1	vpn

Die erste Netzwerkkarte des Systems (extern) stellt die Verbindung des Servers mit dem Internet her - entspricht somit der externen Zone Ihrer Firewall. Verwenden Sie vor dem Server einen Router, sollten Sie „extern“ als DHCP-Client Konfigurieren.

Die zweite Netzwerkkarte (intern) muss mit einer festen IP-Adresse versehen werden. Selbst, wenn über den Internet-Service-Provider eine feste IP-Adresse zur Verfügung steht, ist für das interne Netz die Verwendung eines eigenen Netzes zwingend.

Achtung: *Bevor Sie jetzt die Netzwerkschnittstellen Ihres invis-Servers konfigurieren ein Hinweis dazu. invis-Server können lediglich mit 16 und 24 Bit breiten Netzwerkmasken also „255.255.0.0“ und „255.255.255.0“ umgehen. Idealerweise konfigurieren Sie für die interne Netzwerkschnittstelle ein*

privates IP-Netzwerk der Klassen „B“ (172.16.0.0 bis 172.31.255.255) oder „C“ (192.168.0.0 bis 192.168.255.255).

Achtung: Vermeiden Sie es Ihrem lokalen Netzwerk typisch Adressbereiche gängiger Router-Modelle zu verpassen. Hier ein paar Beispiele von denen Sie die Finger lassen sollten:

typische IP Netze gängiger Router
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.100.0/24
192.168.178.0/24
192.168.188.0/24

Wir unterteilen die Netze der beiden unterstützten Netzwerkklassen für den DHCP-Server in verschiedene Bereiche eingeteilt (Damit ist **kein** Subnetting gemeint). Die nachfolgende Tabelle zeigt die verschiedenen Bereiche, angezeigt wird jeweils nur der Host-Anteil der IP-Adressen.

Geräteklasse	Klasse C Netz	Klasse B Netz
Server	.11 - .19	.0.11 - .0.253
Drucker	.20 - .50	.1.1 - .1.254
IP-Geräte	.60 - .90	.2.1 - .3.254
PCs	.120 - .199	.4.1 - .4.254
dyn. Bereich	.200 - .220	.200.1 - .200.254

Hinweis: *Achten Sie darauf, dass Sie der internen Netzwerkschnittstelle des Servers eine Adresse außerhalb dieser Bereiche geben. Beispielsweise 192.168.x.10 im Falle einer 24Bit Netzwerkmaske oder 172.x.0.10 im Falle einer 16Bit Netzwerkmaske.*

Die Bereiche können, **müssen aber nicht**, in der Konfiguration des invis-Portals

```
/etc/invis/portal/config.php
```

nach eigenen Anforderungen angepasst werden.

Zur Benennung der Netzwerkschnittstellen steht nach der Installation des invis-Setup RPMs mit ***netsetup*** ein eigenes Script zur Verfügung. Führen Sie es einfach ohne weitere Optionen aus:

```
linux:~ # netsetup
Es wurden Regeln zur Benennung der vorhandenen Netzwerkkarten erzeugt.

Bitte starten Sie den Server jetzt neu und konfigurieren
Sie Ihre Netzwerkkarten anschließend mit YaST.
linux:~ #
```

Nach Ausführung dieses Scripts ist ein Neustart des Servers notwendig.

Jetzt kann das Netzwerk-Setup mit YaST abgeschlossen werden:

```
linux:~ # yast lan
```

Hinweis: *Kontrollieren Sie beim Setup der Netzwerkkarten mit YaST, dass in den Karteneinstellungen unter Punkt „General“ anstelle von „On Cable Connect“, „At Boot Time“ für das initialisieren der Netzwerkkarten eingetragen ist.*

Konfigurieren Sie in YaST folgende Punkte:

- **Hostname**, entsprechend der obigen Überlegungen
- **Externe Schnittstelle**: Bei Verwendung eines Routers mit DHCP-Server einfach als DHCP-Client einrichten. Bei Verwendung eines Routers ohne aktiven DHCP-Server ist die Schnittstelle statisch entsprechend der Netzwerk-Konfiguration des Routers einzurichten und zusätzlich der Router als Gateway zu konfigurieren.
- **Interne Schnittstelle**: Hier ist eine statische Adresse einzurichten. Wichtig ist, dass mit der Adresse auch im letzten Eingabefeld der zuvor vergebene Hostname erneut einzugeben ist. Der Host-Teil der IP-Adresse sollte bezogen auf Ihr Netzwerk im Bereich von 1 bis 10 liegen, da ansonsten die Gefahr besteht, dass Ihr Server in einem der vom DHCP-Dienst verwendeten Bereiche liegt.

Prüfen Sie Ihre Konfiguration mit:

```
linux:~ # ifconfig
extern    Link encap:Ethernet  Hardware Adresse 08:00:27:DB:46:89
          inet Adresse:192.168.240.205  Bcast:192.168.240.255
Maske:255.255.255.0
          inet6 Adresse: fe80::a00:27ff:fedb:4689/64
Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:282 errors:0 dropped:96 overruns:0 frame:0
          TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:1000
          RX bytes:23953 (23.3 Kb)  TX bytes:9356 (9.1 Kb)

intern    Link encap:Ethernet  Hardware Adresse 08:00:27:1A:53:3A
          inet Adresse:192.168.222.10  Bcast:192.168.222.255
Maske:255.255.255.0
          inet6 Adresse: fe80::a00:27ff:fe1a:533a/64
Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 Sendewarteschlangenlänge:1000
          RX bytes:0 (0.0 b)  TX bytes:648 (648.0 b)
```

Zu prüfen ist auch ob der Hostname korrekt gesetzt wurde:

```
linux:~ # hostname -f
```

Achtung: *Wenn hierbei nach wie vor der von openSUSE während der Installation zufällig generierte Name (z.b. linux-lajhf1.site oder linux.suse) ausgegeben wird, kann das invis Server Setup* ***nicht*** *funktionieren. In diesem Fall bitte mit YaST das Setzen eines korrekten Hostnamens nachholen.*

Damit sind Basisinstallation und Netzwerkkonfiguration abgeschlossen.

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

Permanent link:
https://wiki.invis-server.org/doku.php?id=invis_server_wiki:installation:basesetup-110&rev=1527330700

Last update: **2018/05/26 10:31**