Basis-Installation

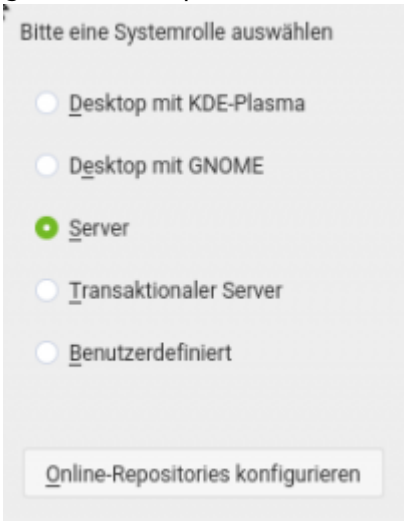
Eine Schritt für Schritt Anleitung zur Installation eines openSUSE Leap sollte wohl nicht erforderlich sein. Daher hier nur ein paar Anmerkungen zum Festplatten-Management, der Software-Paket-Auswahl sowie der anschließenden Netzwerkkonfiguration.

Zur Installation eines invis-Servers ab Version 14.0 wird ein openSUSE Leap 15.x vorausgesetzt.

Bevor Sie starten: *Schalten Sie gerade bei neuer Hardware im **UEFI** Ihres Systems die Secure-Boot Funktion ab. Dies ist Voraussetzung dafür, dass das nachfolgend beschriebene Partitionierungsbeispiel funktioniert.*

Software-Auswahl

Für die Installation eines invis-Servers müssen Sie über die Auswahl des Installationsmusters (Systemrolle) „Server“ 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. Klicken Sie zur Konfiguration der Online-Repositories einfach auf die entsprechende Schaltfläche. Die Voreingestellt Auswahl der einzubindenden Repositories muss nicht erweitert oder geändert werden.

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 eine Systemrolle entscheiden sollen. Wählen Sie wie in der Abbildung gezeigt „Server“ aus. Ein grafisches Desktop-System wird für den Betrieb eines invis-Servers nicht benötigt, ist aber möglich.

Festplatten-Management

Dem Festplattenmanagement sollten Sie besondere Aufmerksamkeit widmen, schließlich geht es um sinnvolle Nutzung Ihres Plattenplatzes, der Sicherheit Ihrer Daten und der Wartbarkeit des Servers. Wir erläutern das Management beispielhaft anhand eines von uns in der Praxis meist genutzten

Setups.

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. Die Verwendung von GPT Partitionstabellen ist ab openSUSE Leap die Vorgabe, Sie müssen also nichts anpassen.

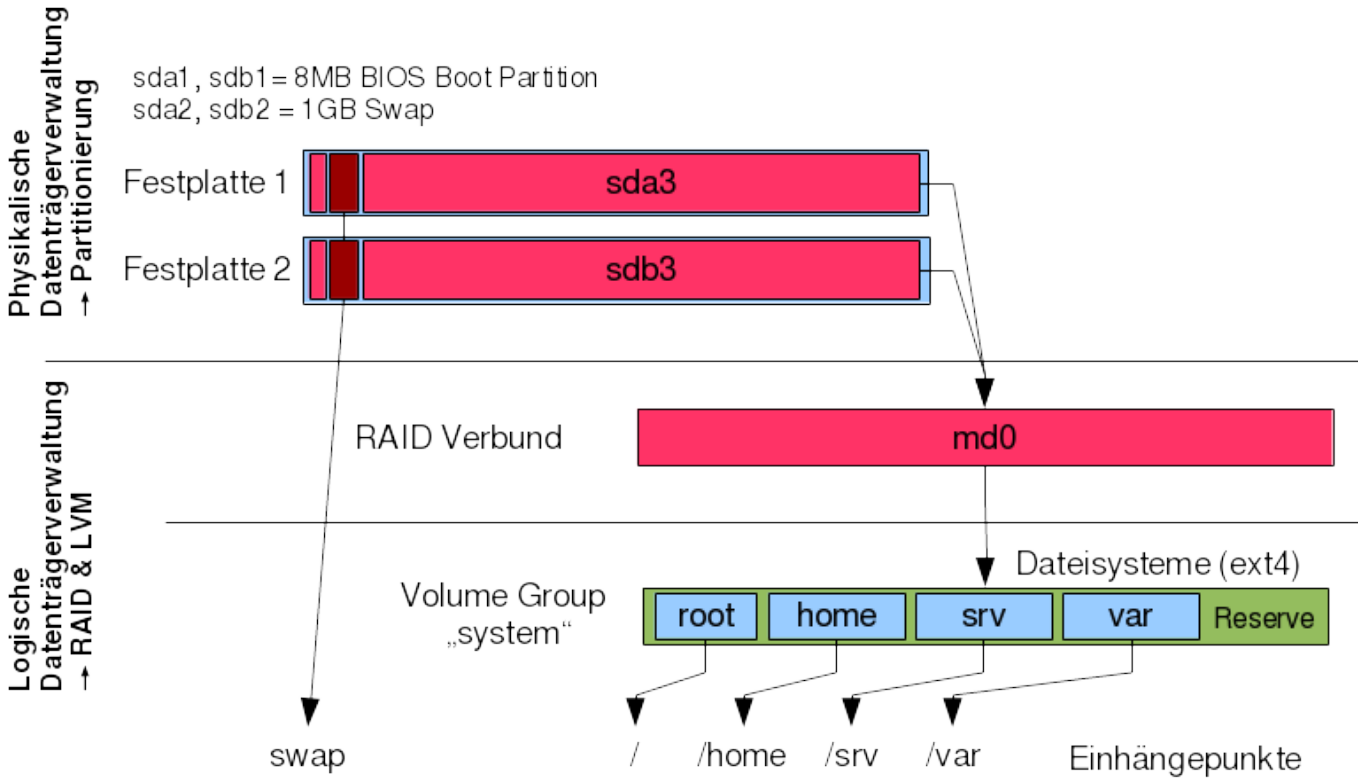
Ziel des Setups ist also eine GPT-basierte Partitionierung. Dafür muss am Anfang jeder Platte (deaktiviertes Secure Boot vorausgesetzt) eine 8MB große Patition vom Typ „BIOS Boot“ angelegt werden, in die Grub seine Boot-Records speichert. Es folgen zwei Swap-Partitionen von max. 1-2GB Größe. Der verbleibende 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.

Alternativ zu zwei individuellen Swap-Partitionen, können Sie auch ein Swap-Volume im Rahmen des nachfolgend beschriebenen Volumemanagement realisieren.

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

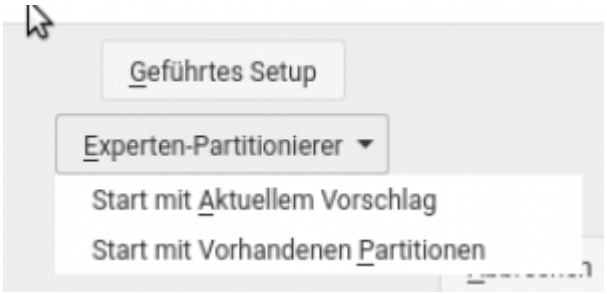
Hinweis: *Einige Funktionen des invis-Portals sowie des invis Server eigenen Backup-Tools gehen zwingend von der Kombination aus Software-RAID und LVM aus. Wählen Sie ein anderes Setup können diese Funktionen nicht oder nicht vollständig genutzt werden.*

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 Installationsanweisungen der Setup-Routine bis zur Festplatten-Partitionierung. Klicken Sie hier auf die Schaltfläche „Experten-Partitionierer“ → „Start mit vorhandenen Partitionen“.



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 Datensicherungsstrategien 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 Attachments 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.

Achtung: *Wenn Sie genau wie wir auf die Kombination aus Software-RAID, LVM und dem ext4 Dateisystem setzen, kann es insbesondere bei RAID5 Systemen zu einer unglücklichen Situation kommen. Nach dem ersten Start des installierten Servers laufen zwei sich gegenseitig stark behindernde Prozesse ab. Die RAID-Erstsynchronisation zum einen und die Fertigstellung der ext4-Dateisysteme (ext4lazyinit) zum anderen.*
Beide Prozesse behindern sich so sehr, dass weitere parallele Zugriffe auf die Datenträger kaum möglich sind. Währenddessen als an die weitere Installation des invis-Servers zu denken ist keine sehr spaßige Idee. Es kann vereinzelt sogar zu ernsten Problemen kommen.
Es gibt aus dieser Situation einen recht einfachen Ausweg. Der Kernelprozess „ext4lazyinit“ kann nur laufen, wenn das fertigzustellende Dateisystem gemountet ist. Booten Sie Ihr System nach der Basis-Installation einfach per CD/DVD in das SUSE Rettungssystem und warten Sie bis die RAID-Synchronisation abgeschlossen ist. Das dauert zwar je nach Plattengröße auch eine ganze Weile (mehrere Stunden) ist aber in der Summe immer noch deutlich schneller als alles gleichzeitig laufen zu lassen. Sie können der RAID-Synchronisation mit folgendem Kommando zuschauen:

```
rescue:~ # watch cat /proc/mdstat
```

Anpassungen

Im Anschluss an Systemrollenwahl, Partitionierung und Zeiteinstellung werden Sie gebeten einen ersten Benutzer für das System anzulegen. Dies ist nicht notwendig. Wählen Sie einfach den Punkt „Benutzereinstellung überspringen“ aus.

Damit Sie Ihren Server direkt nach dem Setup per SSH erreichen können, ist der SSH Dienst zu aktivieren und der entsprechende Port (22) in der Firewall zu öffnen. Anders als bei den Leap 42.x Versionen ist ab Leap 15.0 die Firewall wieder grundsätzlich aktiv. Nebenbei sei bemerkt, dass es sich

hierbei nicht mehr um die „SuSEfirewall2“, sondern den von RedHat entwickelten „firewalld“ handelt. Klicken Sie in der Installationszusammenfassung unter Punkt „Firewall und SSH“ auf die beiden Links „Aktivieren“ und „Öffnen“.

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.

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
https://wiki.invis-server.org/lib/exe/fetch.php?media=invis_server_wiki:invi
sprep.gz
```

Die Datei kann jetzt entpackt und ausgeführt werden:

```
invis:~ # gunzip invisprep.gz
invis:~ # chmod +x invisprep
invis:~ # ./invisprep
```

Danach kann das invis-Setup Paket installiert werden:

```
linux:~ # zypper ref
linux:~ # zypper in invisAD-setup-14
```

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: *Ab invis-Server Version 14.1 löst die Installation des Setup Pakets eine Reihe von Paketkonflikten aus. Genaugenommen sind das keine Konflikte sondern zyppers Weigerung automatisch zu akzeptieren, das lokal bereits installierte Pakete durch Pakete aus anderen Repositories aktualisiert werden. Erlauben Sie den Wechsel durch Auswahl von Lösungsvorschlag Nr.:* ***1***

Hinweis: *Beim Installieren des Setup-Paketes bemängelt* ***zypper*** *einen Paketkonflikt bezüglich unseres eigenen DHCP-Server Pakets „invisdhcp“. 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.

Achtung: *Verbinden Sie zwingend beide Netzwerkschnittstellen mit einem Gegenüber. Sie benötigen während der Installation natürlich Internetzugang, dass bedeutet, die externe Schnittstelle muss mit Ihrem Router verbunden sein, für die interne Schnittstelle genügt es sie mit einem Switch zu verbinden. Verbunden sein muss sie auf jeden Fall, da Ihr openSUSE Linux sie ansonsten deaktivieren würde, was sowohl das Netzwerksetup als auch die Installation des Servers sabotiert.*

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) sollte eine Fantasie-Domain wie beispielsweise ***.loc***, ***.lan*** oder ***.corp*** verwendet werden. Die Verwendung einer im Internet gültigen bzw. bereits vergebenen Domain führt zu Problemen beim Routing und dem EMail-Handling.

Hinweis: *Dieses Thema ist hoch umstritten. Die für die Zulassung von Top-Level-Domains zuständige Organisation ICANN warnt wegen der ständig neu zugelassenen TLDs vor Domain-Kollisionen, hat aber die Vergabe von beispielsweise .corp auf unbestimmte Zeit zurück gestellt. Infos zum Thema. Unserer Meinung nach fällt es gerade kleineren Unternehmen, an die sich unser Projekt ja wendet, schwer auch für interne Zwecke mit offiziell registrierten Domains zu arbeiten. Es steht Ihnen natürlich frei dies zu tun.*

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
eth2	*dmz*
tun1	vpn

Die erste Netzwerkkarte des Systems (extern) stellt die Verbindung des Servers mit dem Internet her - entspricht somit der externen Zone Ihrer Firewall. Je nach dem, wie der dem invis-Server vorgeschaltete Router konfiguriert ist, müssen Sie „extern“ als DHCP-Client oder gemäß den Vorgaben Ihres Providers Konfigurieren.

Falls mehr als zwei Netzwerkschnittstellen vorhanden sind, wird die dritte Schnittstelle in **dmz** umbenannt, auch wenn das invis-Server Setup dies in keiner Weise nutzt.

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“ (/16) und „255.255.255.0“ (/24) 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). Über die Unterstützung von Klasse „A“ Netzen denken wir noch nach, erachten dies aber nicht wirklich als notwendig für „kleine“ Netze.*

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 (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. Wenn Sie dies tun möchten, sollten Sie es erledigen, bevor Sie die ersten Geräte in Ihr Netzwerk aufnehmen.

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.

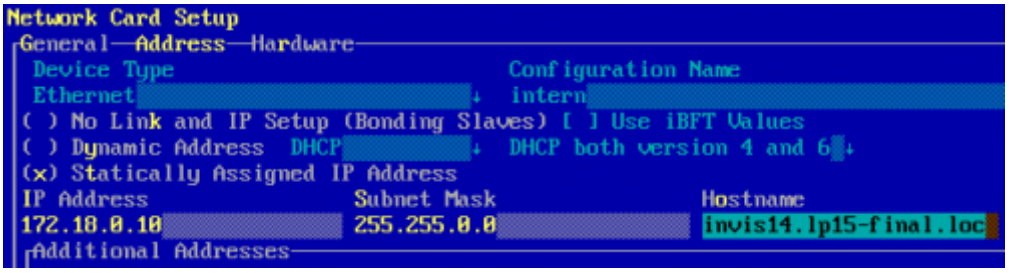
Jetzt kann das Netzwerk-Setup mit YaST abgeschlossen werden:

```
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. Der Hostname muss in YaST an zwei verschiedenen Stellen eingegeben werden. Einmal im Setup der internen Netzwerkschnittstelle und einmal unter Punkt „Hostname/DNS“. Letzteres wirkt in Yast ein wenig merkwürdig. In älteren openSUSE Leap Versionen (bis 15.0) wurde hier ebenfalls der vollqualifizierte Name eingegeben. Unter 15.2 war und ist dies nicht möglich, da das Eingabefeld keine Punkte zulässt. Ab 15.3 können Punkte wieder eingegeben werden, dennoch **darf hier nur der Hostanteil des Namens eingegeben werden**!
- **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. Diese sind in obiger Tabelle aufgeführt.



Prüfen Sie Ihre Konfiguration mit:

```
linux:~ # ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: extern: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 08:00:27:9c:9a:2f brd ff:ff:ff:ff:ff:ff
    inet 172.22.200.204/16 brd 172.22.0.255 scope global extern
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9c:9a2f/64 scope link
       valid_lft forever preferred_lft forever
3: intern: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 08:00:27:d2:de:e6 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.10/16 brd 172.18.255.255 scope global intern
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed2:dee6/64 scope link
       valid_lft forever preferred_lft forever
```

Hinweis: *Korrekt bemerkt, das in die Jahre gekommene Tool* ***ipconfig*** *ist nicht mehr Bestandteil von openSUSE leap 15.*

Zu prüfen ist auch ob der Hostname korrekt gesetzt wurde. Das nachfolgende Kommando muss den vollqualifizierten Namen (FQDN) ausgeben:

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

Hinweis: *Ohne die Option -f darf hingegen nur der Hostanteil des Namens ausgegeben werden. Wird hier ebenfalls der FQDN ausgegeben, wurde via YaST im Punkt „Hostname/DNS“ versehentlich der FQDN angegeben. Dies muss zwingend korrigiert werden!*

Hinweis: *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.