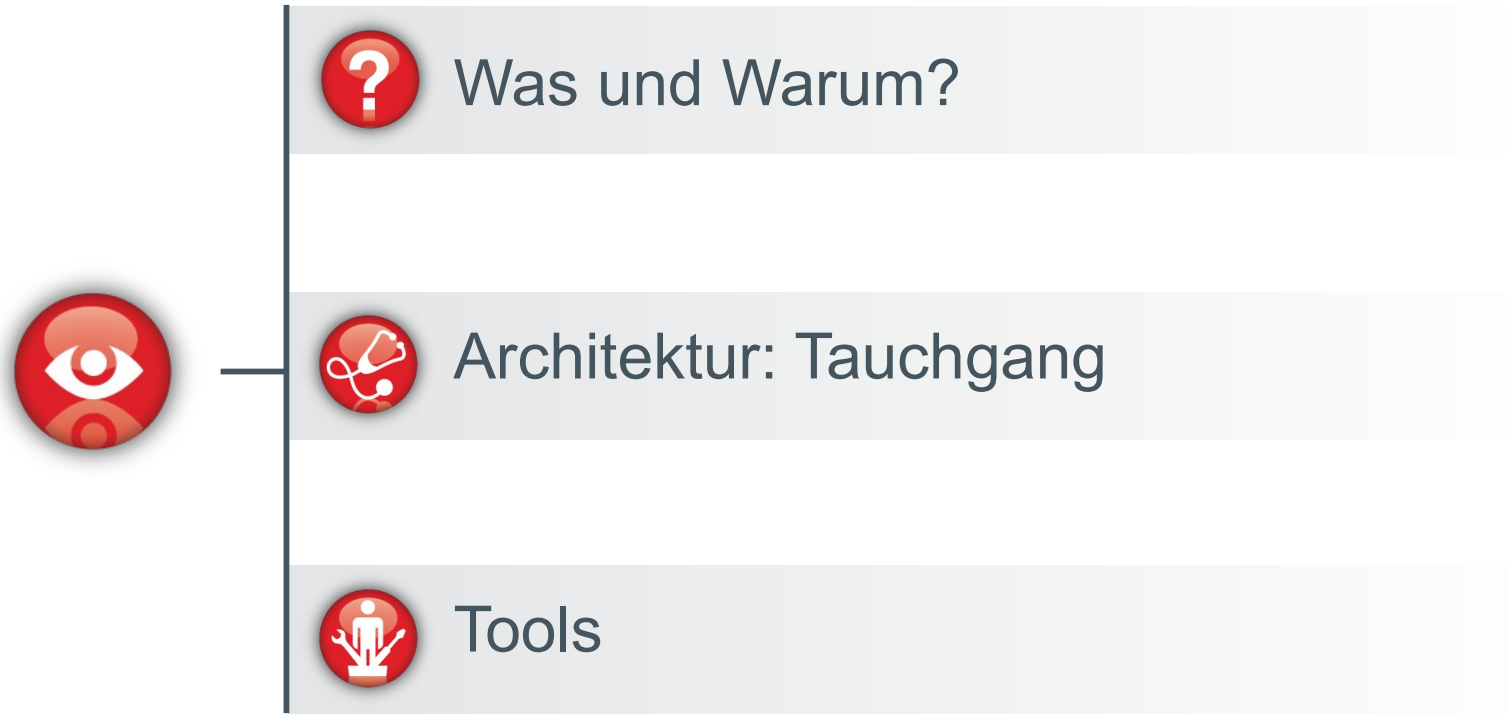
Securing Your System:

Hardening: Sinnvoll? Notwendig? Überbewertet?

Roman Drahtmüller
Linux Security Architect
draht@suse.com

Overview



Was und warum?

Was soll Systemsicherheit sein?

Sicherheit...

Gute software...

...tut, was von ihr erwartet wird, und tut es gut.

Sichere software...

...ist gute software, die *nichts anderes* tut.

...also was tun?

Software enthält Fehler

- Fehlfunktionen
- Instabilität
- Datenverlust
- Sicherheitsschwachstellen
  - Identitätsdiebstahl, Systemmißbrauch/hijacking,
  - Datendiebstahl

Zoom-Blick

Administration

- Ziele, Verantwortungen, Mandate, Team-Play

Infrastruktur

- Dienste, Netzwerktopologie, Bereichsgrenzen

Sicherheitszonen/Domänen

- Schutz und -bedarf, Domänenübergänge

Systeme

- Deployment, installation, configuration (hardening), monitoring, maintenance decommissioning

Zoom-Blick

Administration

Ziele, Verantwortungen, Mandate, Team-Play

Infrastruktur

Dienste, Netzwerktopologie, Bereichsgrenzen

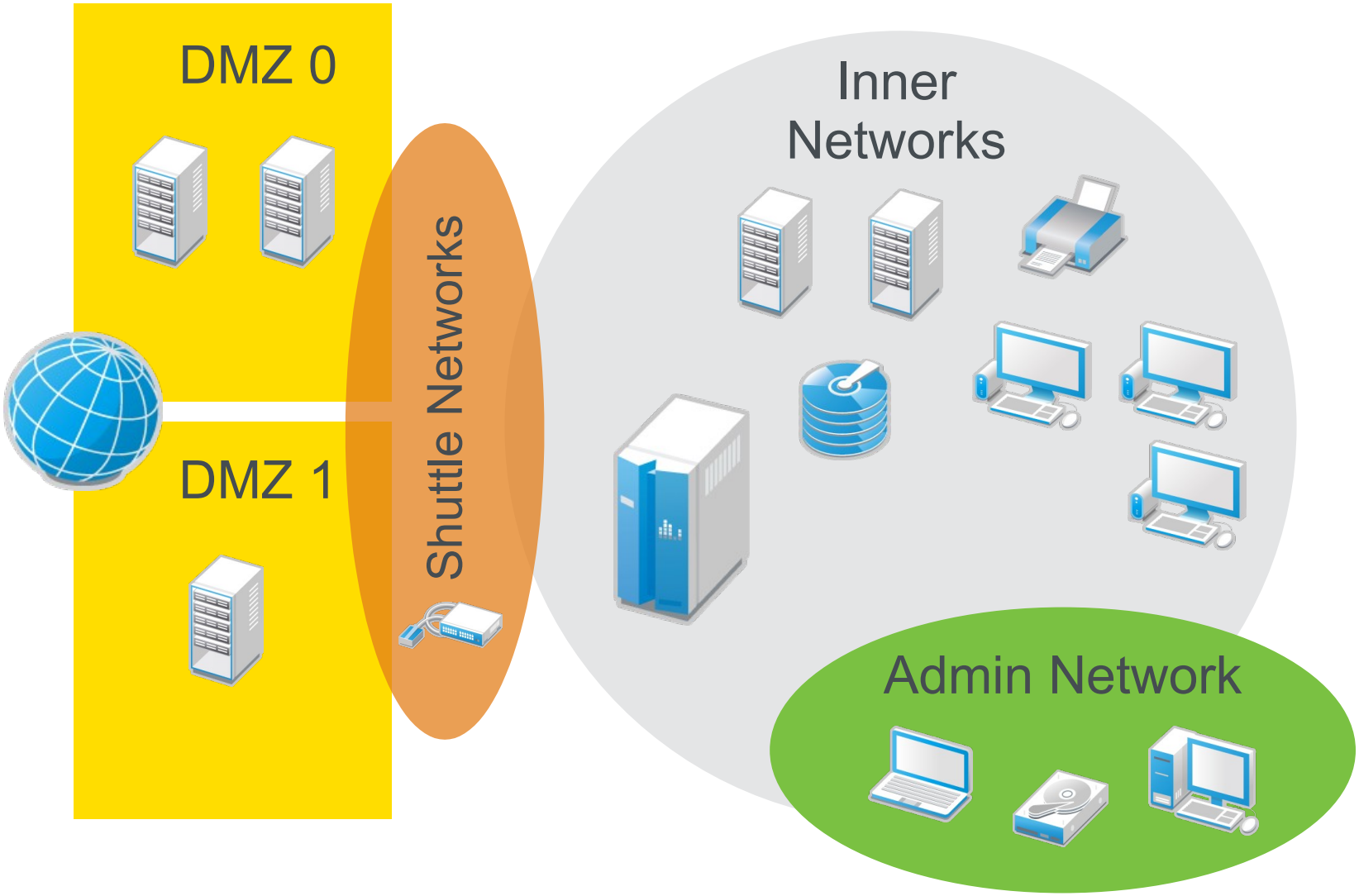
Sicherheitszonen/Domänen

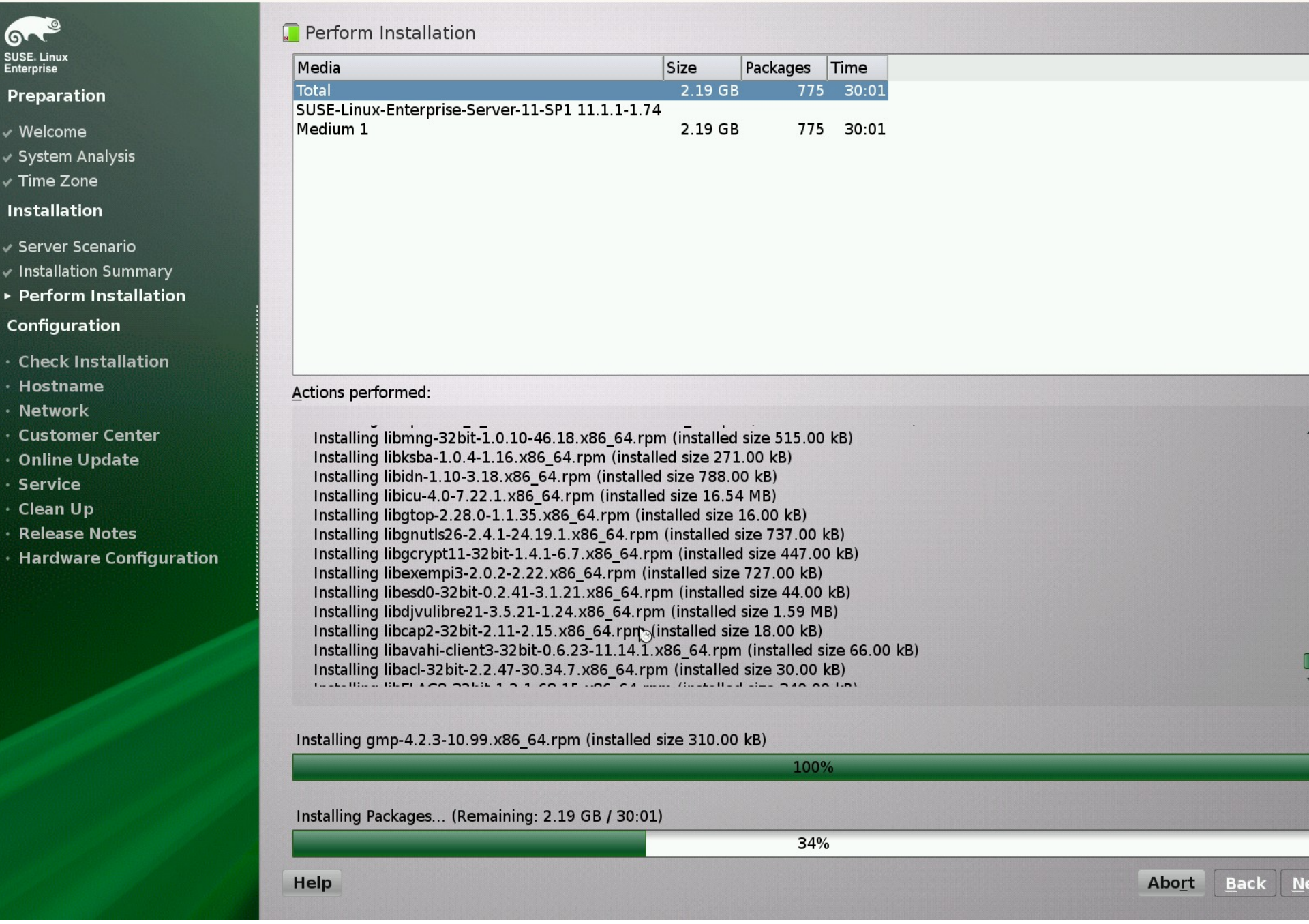
Schutz und -bedarf, Domänenübergänge

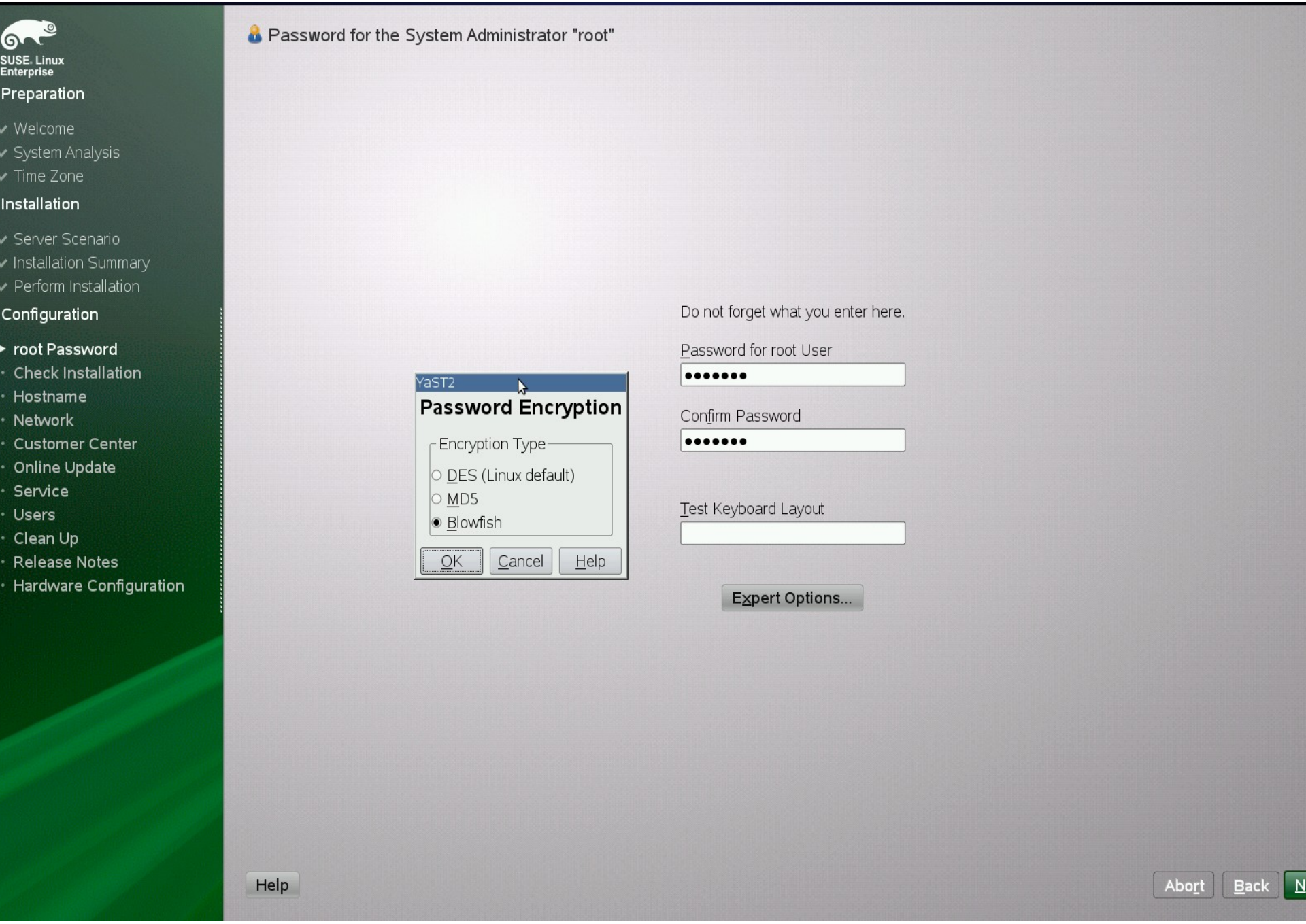
Systeme

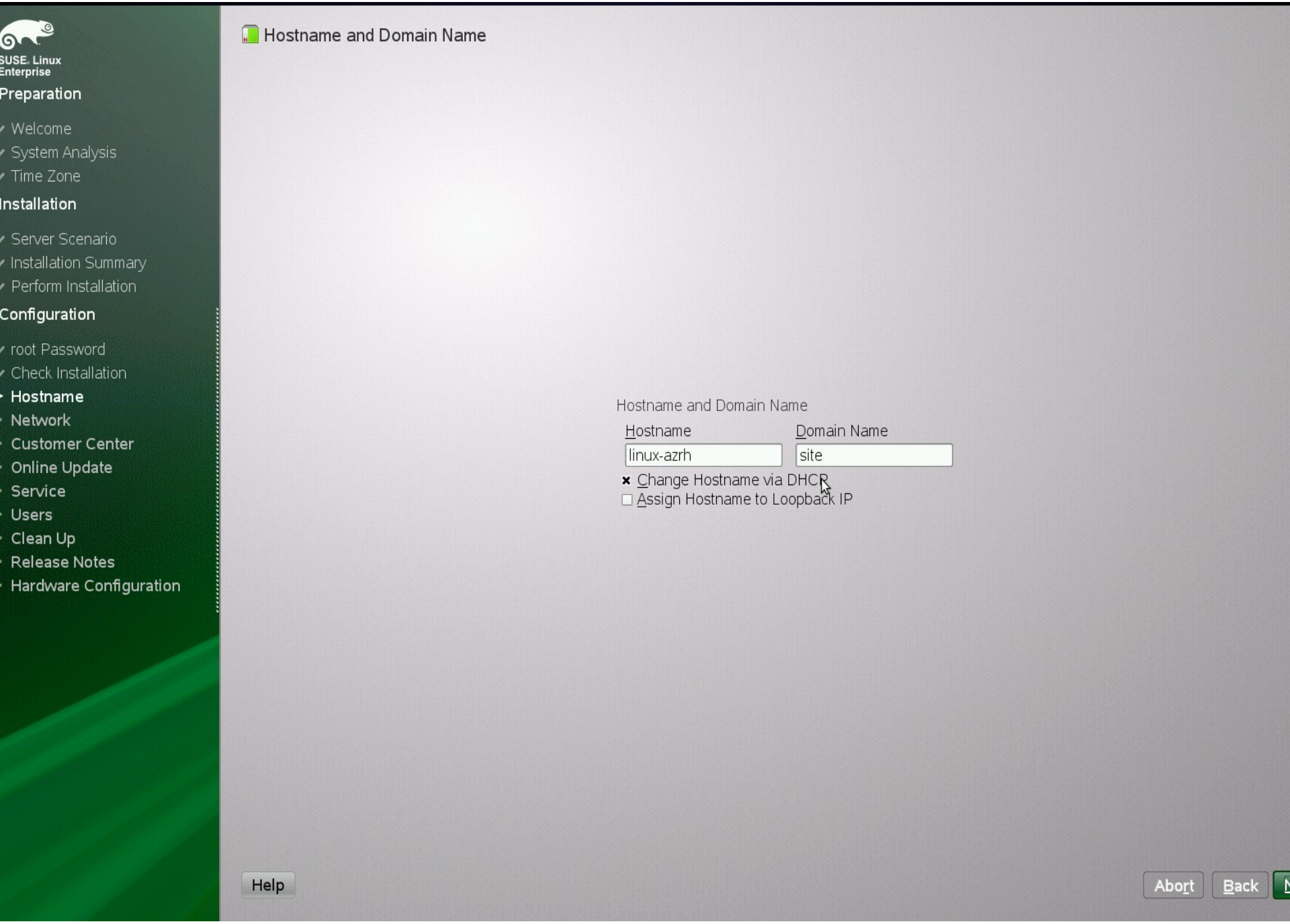
Deployment, installation, configuration (hardening), monitoring, maintenance decommissioning

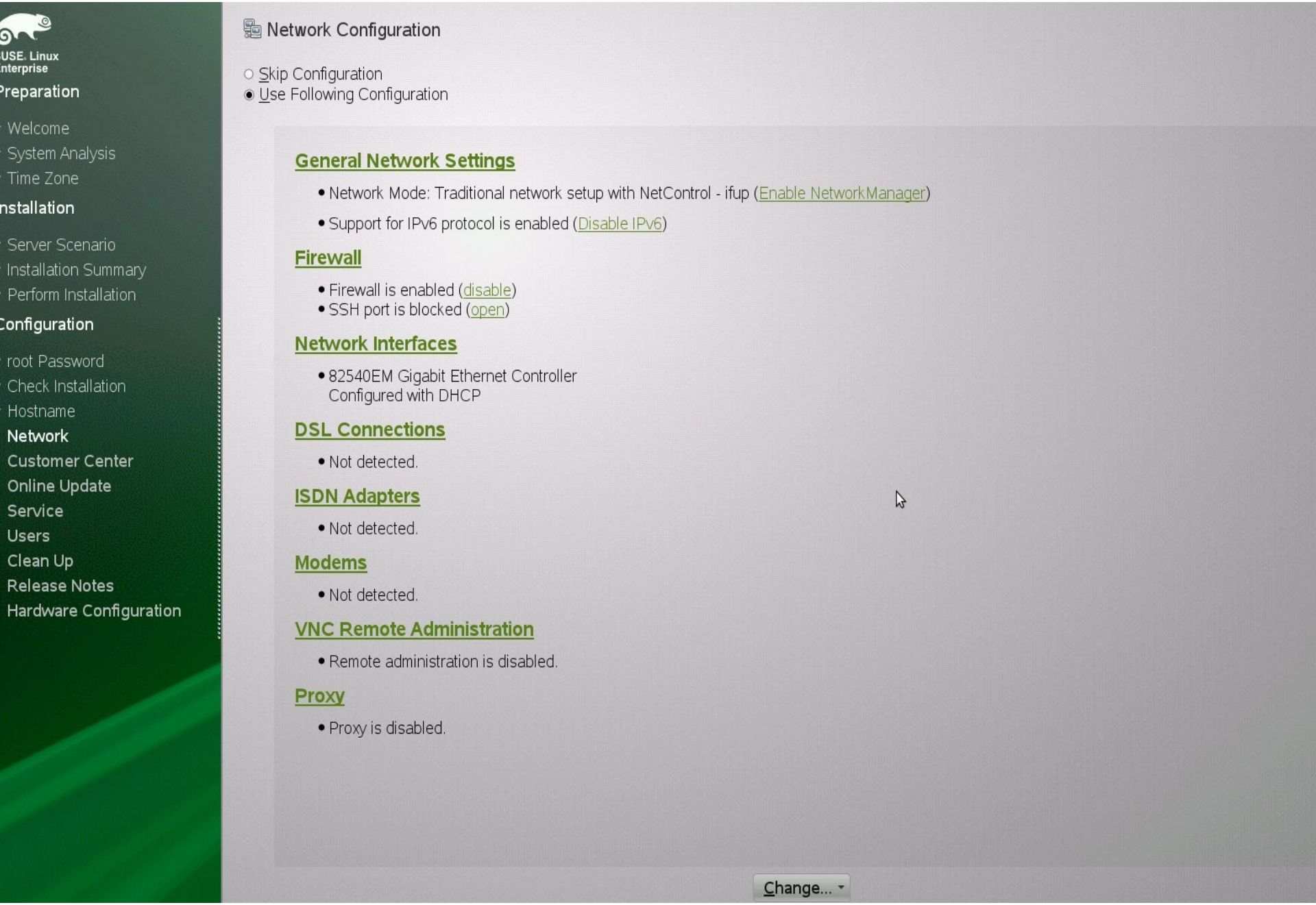
Architekturtauchgang: Inspektion und Hardening


DMZ 0
DMZ 1
Shuttle Networks
Inner
Networks
Admin Network


SUSE Linux Enterprise
Preparation
Welcome
System Analysis
Time Zone
Installation
Server Scenario
Installation Summary
Perform Installation
Configuration
Check Installation
Hostname
Network
Customer Center
Online Update
Service
Clean Up
Release Notes
Hardware Configuration
Perform Installation
Media
Size
Packages
Time
Total
2.19 GB
775
30:01
SUSE-Linux-Enterprise-Server-11-SP1 11.1.1-1.74
Medium 1
2.19 GB
775
30:01
Actions performed:
Installing libmng-32bit-1.0.10-46.18.x86_64.rpm (installed size 515.00 kB)
Installing libksba-1.0.4-1.16.x86_64.rpm (installed size 271.00 kB)
Installing libidn-1.10-3.18.x86_64.rpm (installed size 788.00 kB)
Installing libicu-4.0-7.22.1.x86_64.rpm (installed size 16.54 MB)
Installing libgtop-2.28.0-1.1.35.x86_64.rpm (installed size 16.00 kB)
Installing libgnutls26-2.4.1-24.19.1.x86_64.rpm (installed size 737.00 kB)
Installing libgcrypt11-32bit-1.4.1-6.7.x86_64.rpm (installed size 447.00 kB)
Installing libexempi3-2.0.2-2.22.x86_64.rpm (installed size 727.00 kB)
Installing libesd0-32bit-0.2.41-3.1.21.x86_64.rpm (installed size 44.00 kB)
Installing libdjvulibre21-3.5.21-1.24.x86_64.rpm (installed size 1.59 MB)
Installing libcap2-32bit-2.11-2.15.x86_64.rpm (installed size 18.00 kB)
Installing libavahi-client3-32bit-0.6.23-11.14.1.x86_64.rpm (installed size 66.00 kB)
Installing libacl-32bit-2.2.47-30.34.7.x86_64.rpm (installed size 30.00 kB)
Installing gmp-4.2.3-10.99.x86_64.rpm (installed size 310.00 kB)
100%
Installing Packages... (Remaining: 2.19 GB / 30:01)
34%
Help
Abort
Back


SUSE. Linux Enterprise
Preparation
Welcome
System Analysis
Time Zone
Installation
Server Scenario
Installation Summary
Perform Installation
Configuration
root Password
Check Installation
Hostname
Network
Customer Center
Online Update
Service
Users
Clean Up
Release Notes
Hardware Configuration
Password for the System Administrator "root"
YaST2
Password Encryption
Encryption Type
DES (Linux default)
MD5
Blowfish
OK
Cancel
Help
Do not forget what you enter here.
Password for root User
Confirm Password
Test Keyboard Layout
Expert Options...
Help
Abort
Back


SUSE. Linux Enterprise
Preparation
Welcome
System Analysis
Time Zone
Installation
Server Scenario
Installation Summary
Perform Installation
Configuration
root Password
Check Installation
Hostname
Network
Customer Center
Online Update
Service
Users
Clean Up
Release Notes
Hardware Configuration
Hostname and Domain Name
Hostname and Domain Name
Hostname
Domain Name
linux-azrh
site
Change Hostname via DHCP
Assign Hostname to Loopback IP
Help
Abort
Back


USE. Linux
nterprise
Preparation
Welcome
System Analysis
Time Zone
nstallation
Server Scenario
Installation Summary
Perform Installation
Configuration
root Password
Check Installation
Hostname
Network
Customer Center
Online Update
Service
Users
Clean Up
Release Notes
Hardware Configuration
Network Configuration
Skip Configuration
Use Following Configuration
General Network Settings
Network Mode: Traditional network setup with NetControl - ifup (Enable NetworkManager)
Support for IPv6 protocol is enabled (Disable IPv6)
Firewall
Firewall is enabled (disable)
SSH port is blocked (open)
Network Interfaces
82540EM Gigabit Ethernet Controller
Configured with DHCP
DSL Connections
Not detected.
ISDN Adapters
Not detected.
Modems
Not detected.
VNC Remote Administration
Remote administration is disabled.
Proxy
Proxy is disabled.
Change...

USE. Linux
nterprise

Preparation

- Welcome
- System Analysis
- Time Zone

nstallation

- Server Scenario
- Installation Summary
- Perform Installation

Configuration

- root Password
- Check Installation
- Hostname
- Network
- Customer Center
- Online Update
- Service
- Users
- Clean Up
- Release Notes
- Hardware Configuration

Network Configuration

○ Skip Configuration
◉ Use Following Configuration

General Network Settings

- Network Mode: Traditional network setup with NetControl - ifup (Enable NetworkManager)
- Support for IPv6 protocol is enabled (Disable IPv6)

Firewall

- Firewall is disabled (enable)

Network Interfaces

- 82540EM Gigabit Ethernet Controller
  Configured with DHCP

DSL Connections

- Not detected.

ISDN Adapters

- Not detected.

Modems

- Not detected.

VNC Remote Administration

- Remote administration is disabled.

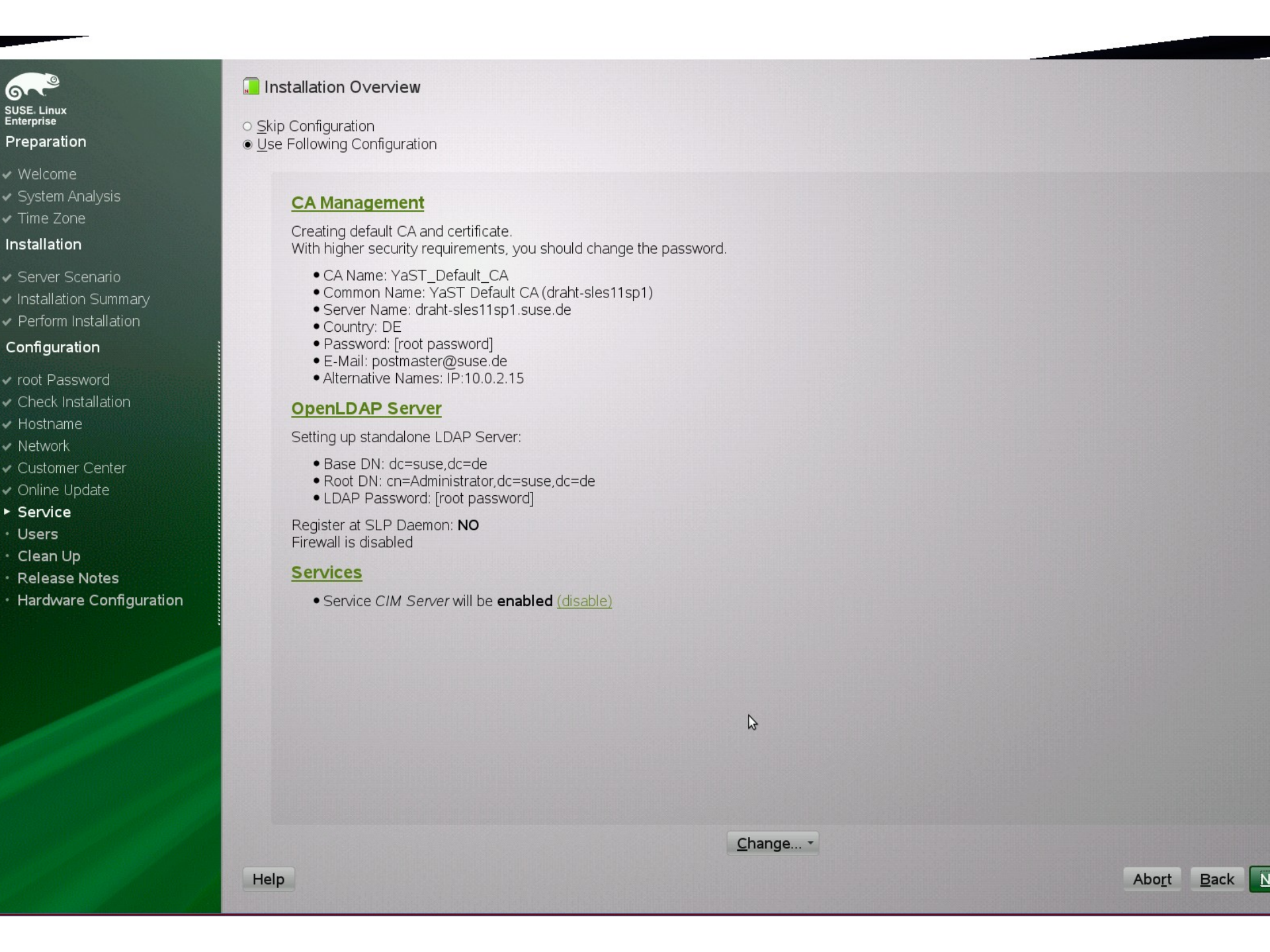
Proxy

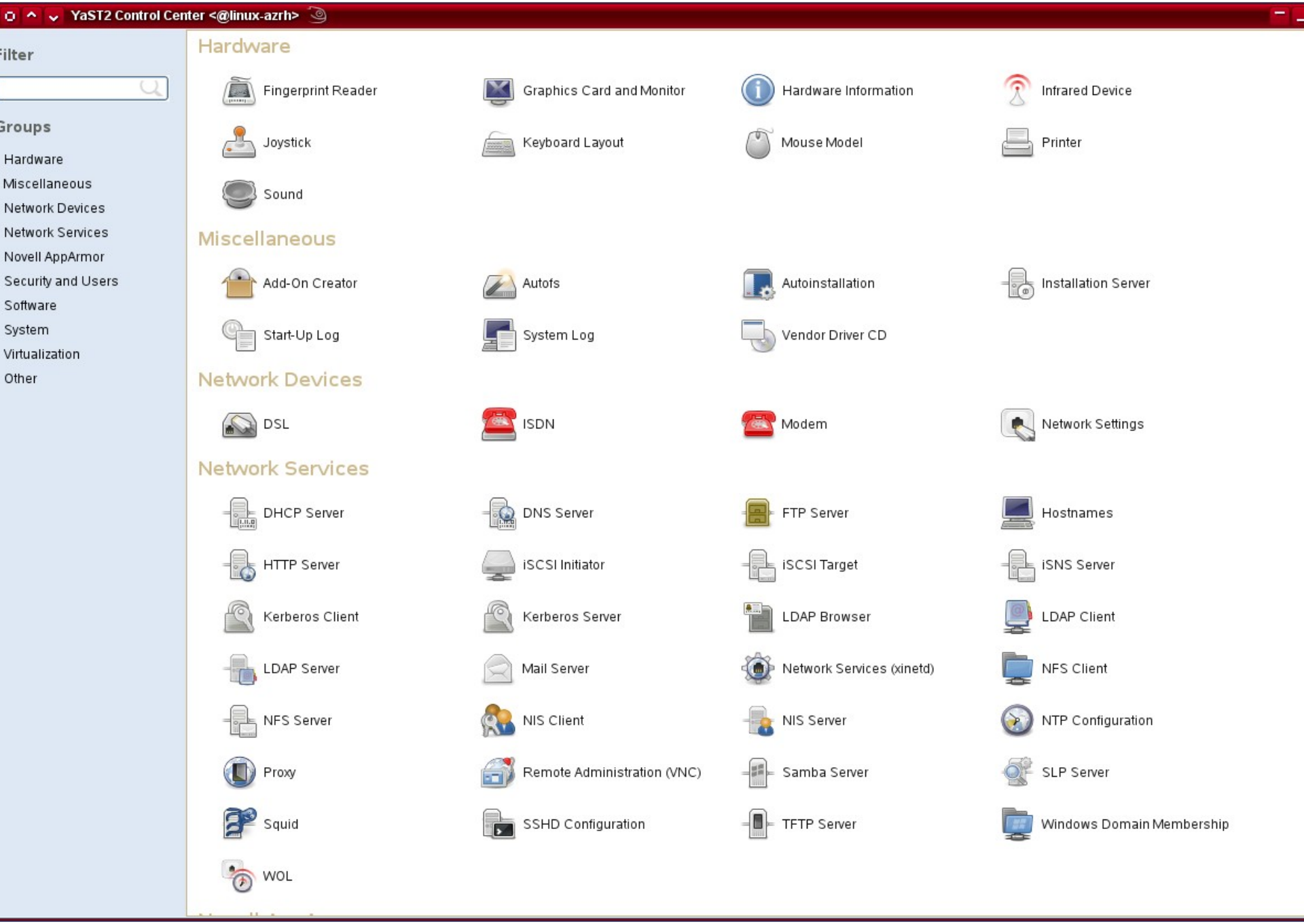
- Proxy is disabled.

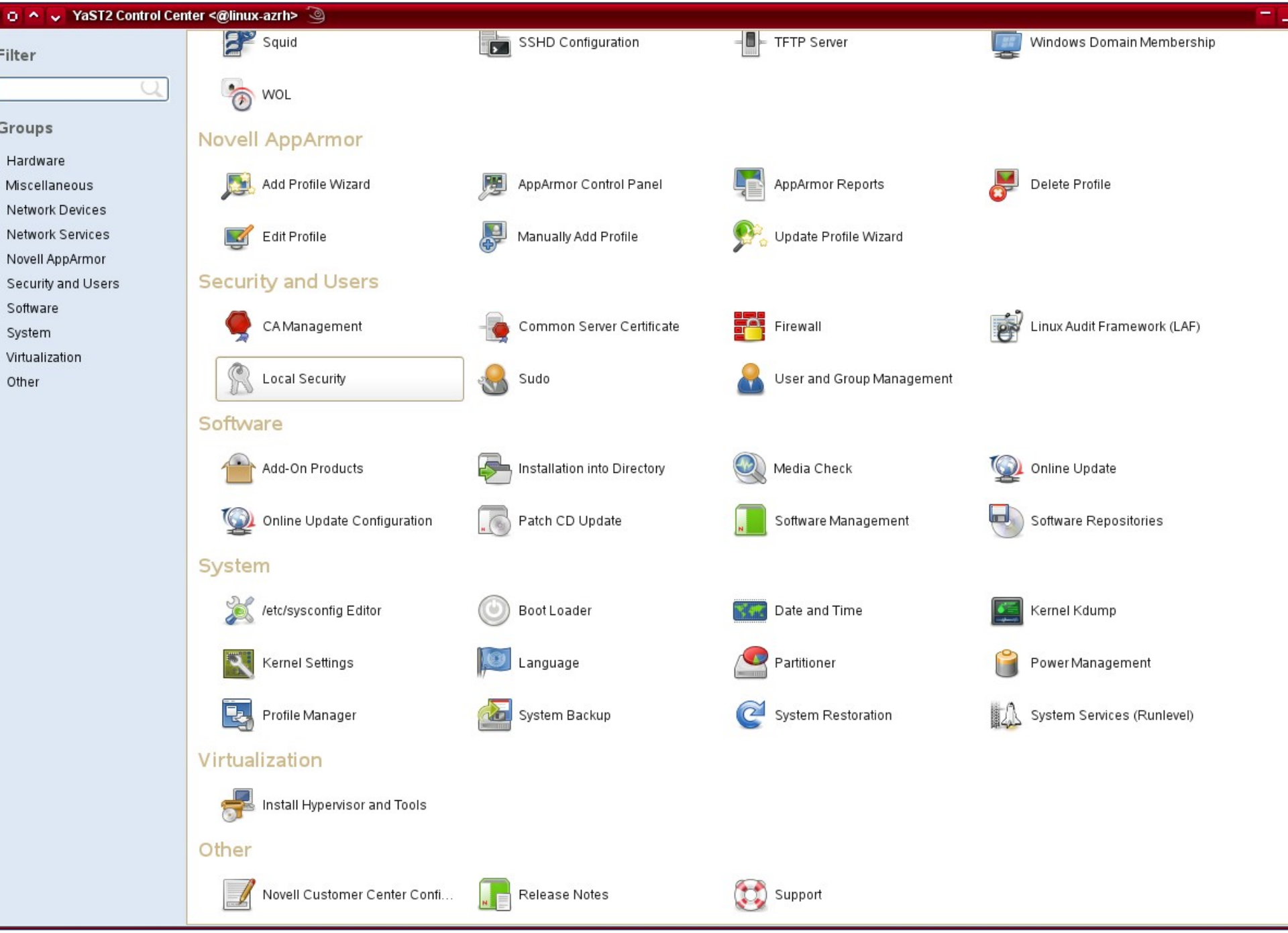
Change...

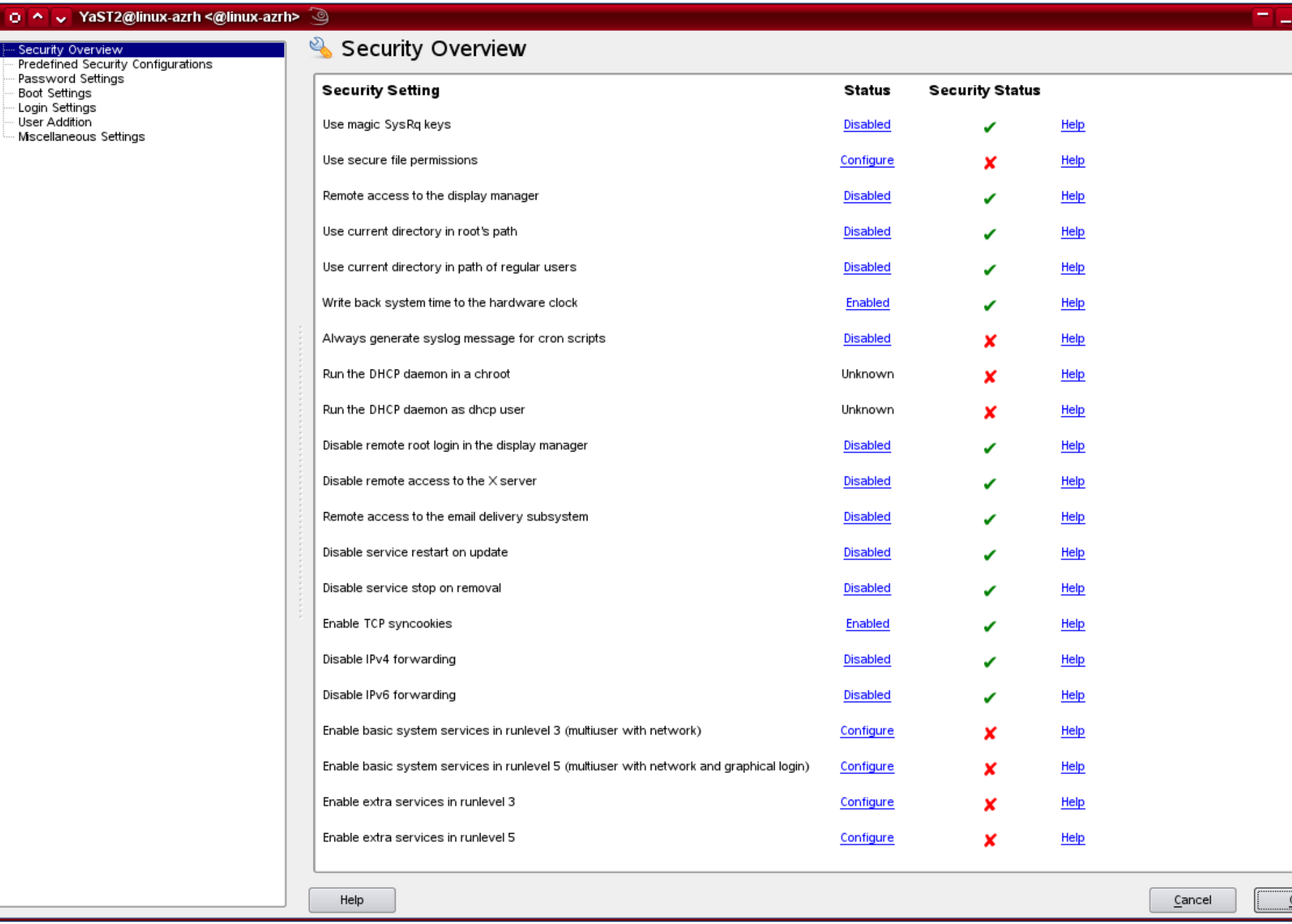
Help

Abort Back


SUSE Linux Enterprise
Preparation
Welcome
System Analysis
Time Zone
Installation
Server Scenario
Installation Summary
Perform Installation
Configuration
root Password
Check Installation
Hostname
Network
Customer Center
Online Update
Service
Users
Clean Up
Release Notes
Hardware Configuration
Installation Overview
Skip Configuration
Use Following Configuration
CA Management
Creating default CA and certificate.
With higher security requirements, you should change the password.
CA Name: YaST_Default_CA
Common Name: YaST Default CA (draht-sles11sp1)
Server Name: draht-sles11sp1.suse.de
Country: DE
Password: [root password]
E-Mail: postmaster@suse.de
Alternative Names: IP:10.0.2.15
OpenLDAP Server
Setting up standalone LDAP Server:
Base DN: dc=suse,dc=de
Root DN: cn=Administrator,dc=suse,dc=de
LDAP Password: [root password]
Register at SLP Daemon: NO
Firewall is disabled
Services
Service CIM Server will be enabled (disable)
Change...
Help
Abort
Back


YaST2 Control Center <@linux-azrh>
Filter
Groups
Hardware
Miscellaneous
Network Devices
Network Services
Novell AppArmor
Security and Users
Software
System
Virtualization
Other
Hardware
Fingerprint Reader
Graphics Card and Monitor
Hardware Information
Infrared Device
Joystick
Keyboard Layout
Mouse Model
Printer
Sound
Miscellaneous
Add-On Creator
Autofs
Autoinstallation
Installation Server
Start-Up Log
System Log
Vendor Driver CD
Network Devices
DSL
ISDN
Modem
Network Settings
Network Services
DHCP Server
DNS Server
FTP Server
Hostnames
HTTP Server
iSCSI Initiator
iSCSI Target
iSNS Server
Kerberos Client
Kerberos Server
LDAP Browser
LDAP Client
LDAP Server
Mail Server
Network Services (xinetd)
NFS Client
NFS Server
NIS Client
NIS Server
NTP Configuration
Proxy
Remote Administration (VNC)
Samba Server
SLP Server
Squid
SSHD Configuration
TFTP Server
Windows Domain Membership
WOL


YaST2 Control Center <@linux-azrh>
Filter
Groups
Hardware
Miscellaneous
Network Devices
Network Services
Novell AppArmor
Security and Users
Software
System
Virtualization
Other
Squid
SSHD Configuration
TFTP Server
Windows Domain Membership
WOL
Novell AppArmor
Add Profile Wizard
AppArmor Control Panel
AppArmor Reports
Delete Profile
Edit Profile
Manually Add Profile
Update Profile Wizard
Security and Users
CA Management
Common Server Certificate
Firewall
Linux Audit Framework (LAF)
Local Security
Sudo
User and Group Management
Software
Add-On Products
Installation into Directory
Media Check
Online Update
Online Update Configuration
Patch CD Update
Software Management
Software Repositories
System
/etc/sysconfig Editor
Boot Loader
Date and Time
Kernel Kdump
Kernel Settings
Language
Partitioner
Power Management
Profile Manager
System Backup
System Restoration
System Services (Runlevel)
Virtualization
Install Hypervisor and Tools
Other
Novell Customer Center Confi...
Release Notes
Support


YaST2@linux-azrh <@linux-azrh>
Security Overview
Predefined Security Configurations
Password Settings
Boot Settings
Login Settings
User Addition
Miscellaneous Settings
Security Overview
Security Setting
Status
Security Status
Use magic SysRq keys
Disabled
Help
Use secure file permissions
Configure
Help
Remote access to the display manager
Disabled
Help
Use current directory in root's path
Disabled
Help
Use current directory in path of regular users
Disabled
Help
Write back system time to the hardware clock
Enabled
Help
Always generate syslog message for cron scripts
Disabled
Help
Run the DHCP daemon in a chroot
Unknown
Help
Run the DHCP daemon as dhcp user
Unknown
Help
Disable remote root login in the display manager
Disabled
Help
Disable remote access to the X server
Disabled
Help
Remote access to the email delivery subsystem
Disabled
Help
Disable service restart on update
Disabled
Help
Disable service stop on removal
Disabled
Help
Enable TCP syncookies
Enabled
Help
Disable IPv4 forwarding
Disabled
Help
Disable IPv6 forwarding
Disabled
Help
Enable basic system services in runlevel 3 (multiuser with network)
Configure
Help
Enable basic system services in runlevel 5 (multiuser with network and graphical login)
Configure
Help
Enable extra services in runlevel 3
Configure
Help
Enable extra services in runlevel 5
Configure
Help
Help
Cancel

Transparenz: Was passiert im Hintergrund?

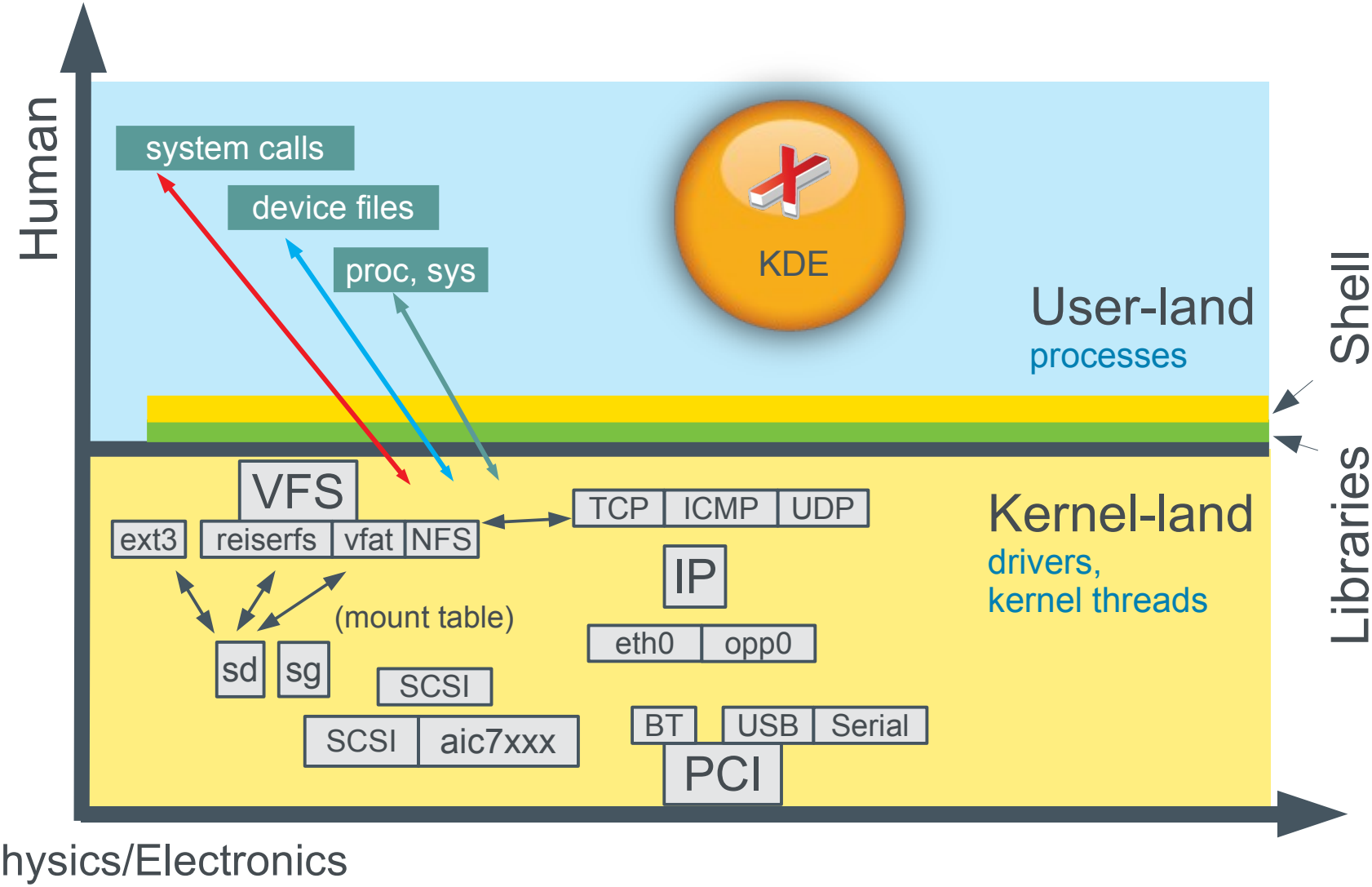
Ein anderes YaST-module

Geänderte Einträge in files in /etc/sysconfig

Änderungen direkt an Konfigurationsfiles von Diensten bzw Subsystemen

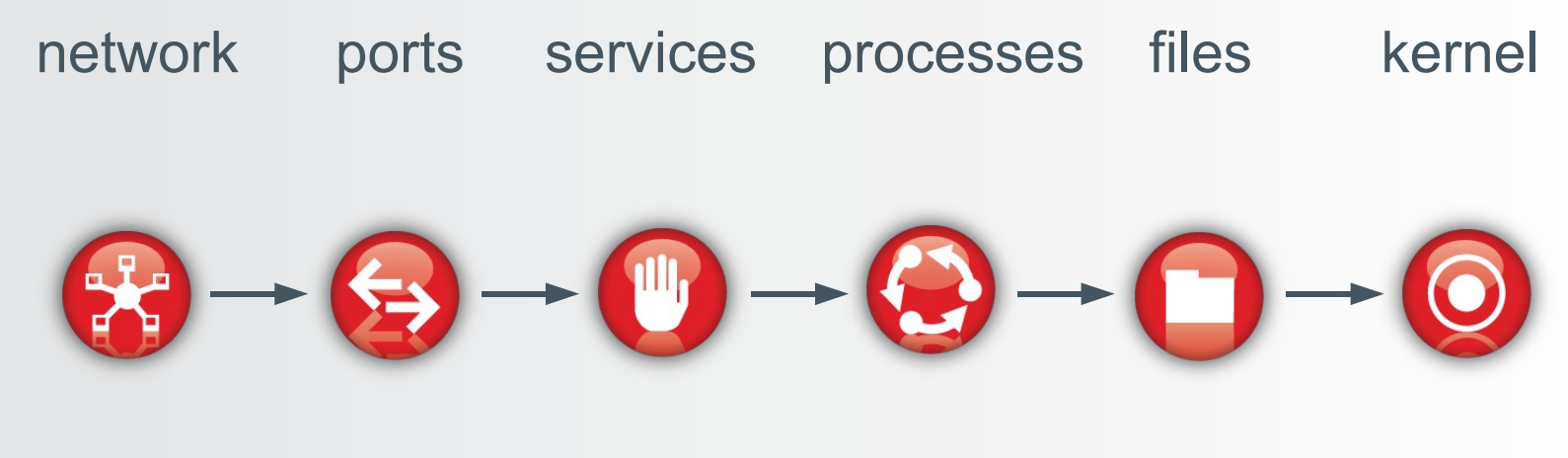
Schematical Overview:

O/S Kernel + Userland



Inspection...

Betrachte das System mit den Augen eines Angreifers:



Netzwerk (1)

Interfaces: interfaces enabled, addresses?

ip link ls; ifconfig -a

ls -la /etc/sysconfig/network

Routing setup: IP-forwarding on/off?

cat /proc/sys/net/ipv4/ip_forward

grep FORWARD /etc/sysconfig/sysctl

Netfilter Regeln: Subsystem aktiv?

iptables -L -nv

Iptables -t nat -L -nv

Netzwerk (2)

Tuning:

txqueuelen, mtu

ICMP replies, ICMP redirects

ECN, slow-start after idle

Ports

port scan: offene TCP and UDP sockets

```
nmap -sS -v -O ip.address.on.network
```

Vergleiche mit der Ausgabe von

```
netstat -anpl
```

Unterschiede...?

(Nicht alle Dienste können einem userland-Prozess zugeordnet werden! (knfsd))

Achtung: UDP sockets nicht vergessen!

Services

Alle nicht genutzten Dienste **permanent** ausschalten!

runlevel symlinks löschen (insserv -r <servicename>)

Die Server killen (rcapache2 stop)

Nachgucken, ob die wirklich tot sind!

Löschen der Pakete?

Prozesse

Man sollte dann doch jeden einzelnen Prozess persönlich kennenlernen:

```
ps faux
```

```
rpm -qfi /usr/sbin/nscd
```

...und entfernen, was nicht gebraucht wird.

Files

Permissions bei SUSE: /etc/permissions* setting in /etc/sysconfig/security

```
chkstat -set <permissions file> oder SuSEconfig
```

```
find / /usr ... -mount -type f \( -perm +2000 -o -perm +4000 \) -ls
```

Integritätssicherung: BACKUP!, AIDE, AFICK, RPM

Offsite-Datenbank! Nützlich: rsync

Mount-Optionen: /etc/fstab, /proc/mounts

Kernel: (Pseudo) filesystems

umount:

- debugfs (oder chmod)
- fuse (deinstall nach Deaktivieren)
- sysfs (system tools failen)
- tmpfs (RAM usage)
- autofs (wenn nicht genutzt)

Kernel: AppArmor!

Beispielsprofil: dhcp daemon (dhcpd)

```
#include <tunables/global>

/usr/sbin/dhcpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability dac_override,
  capability net_bind_service,
  capability net_raw,
  capability setgid,
  capability setuid,
  capability sys_chroot,

  /db/dhcpd.leases*      lrw,
  /etc/dhcpd.conf        r,
  /etc/hosts.allow       r,
  /etc/hosts.deny        r,
  /usr/sbin/dhcpd        rmix,
  /var/lib/dhcp/dhcpd.leases*   rwl,
  /var/lib/dhcp/etc/dhcpd.conf  r,
  /var/run/dhcpd.pid     wl,
}
```


suse®