
# SUSE Linux security & hardening

Piotr Szewczuk
Starszy konsultant
pszewczuk@suse.com

# O czym będziemy rozmawiać?

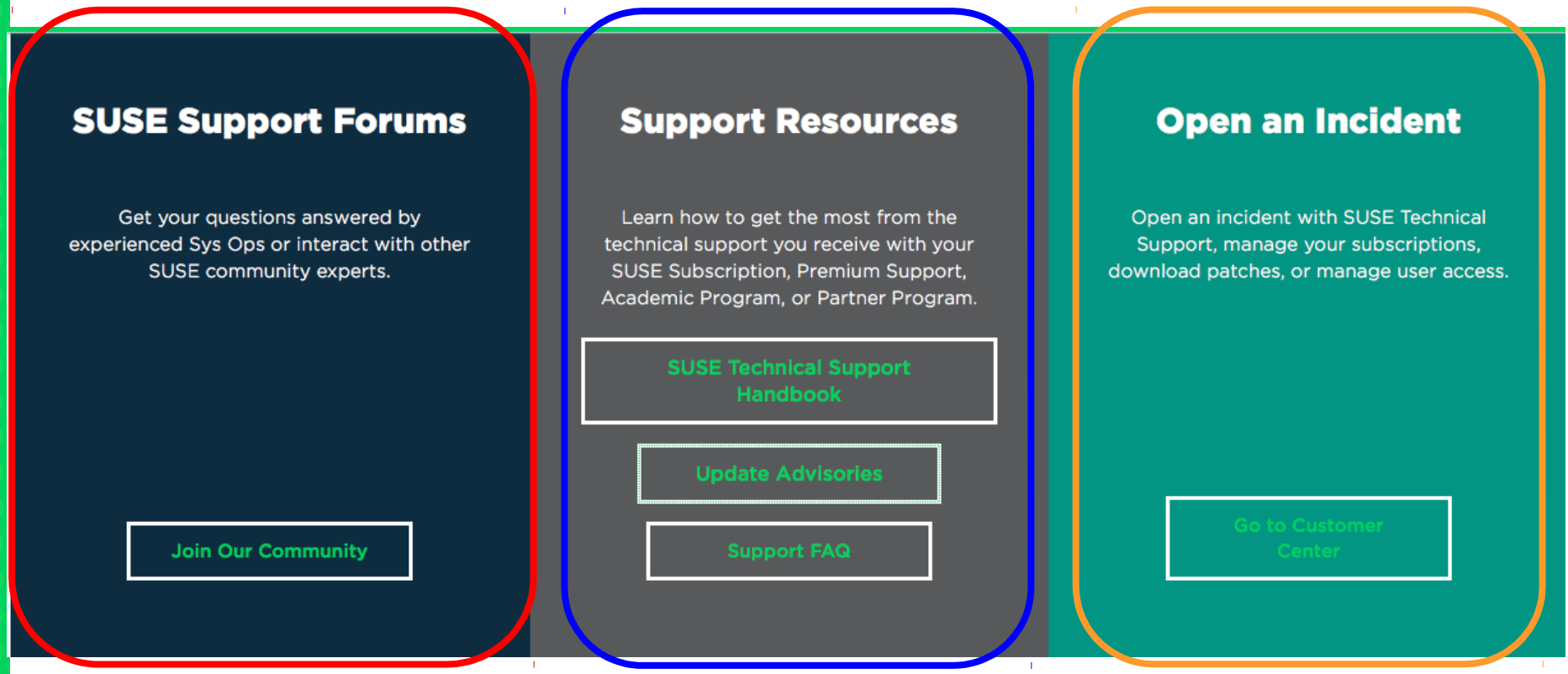
- Podstawowe operacje przy instalacji
  i po instalacji systemu SUSE Linux Enterprise Server
- Usługi systemowe, aktualizacje systemu,
  kontrola uprawnień
- Zabezpieczanie usługi SSH, kontrola uprawnień
- Wykorzystanie mechanizmów
  Host-based Intrusion Detection System (HIDS)
- Zabezpieczanie systemu za pomocą AppArmor
- Audyt i monitorowanie

# Proces utwardzania systemu Linux

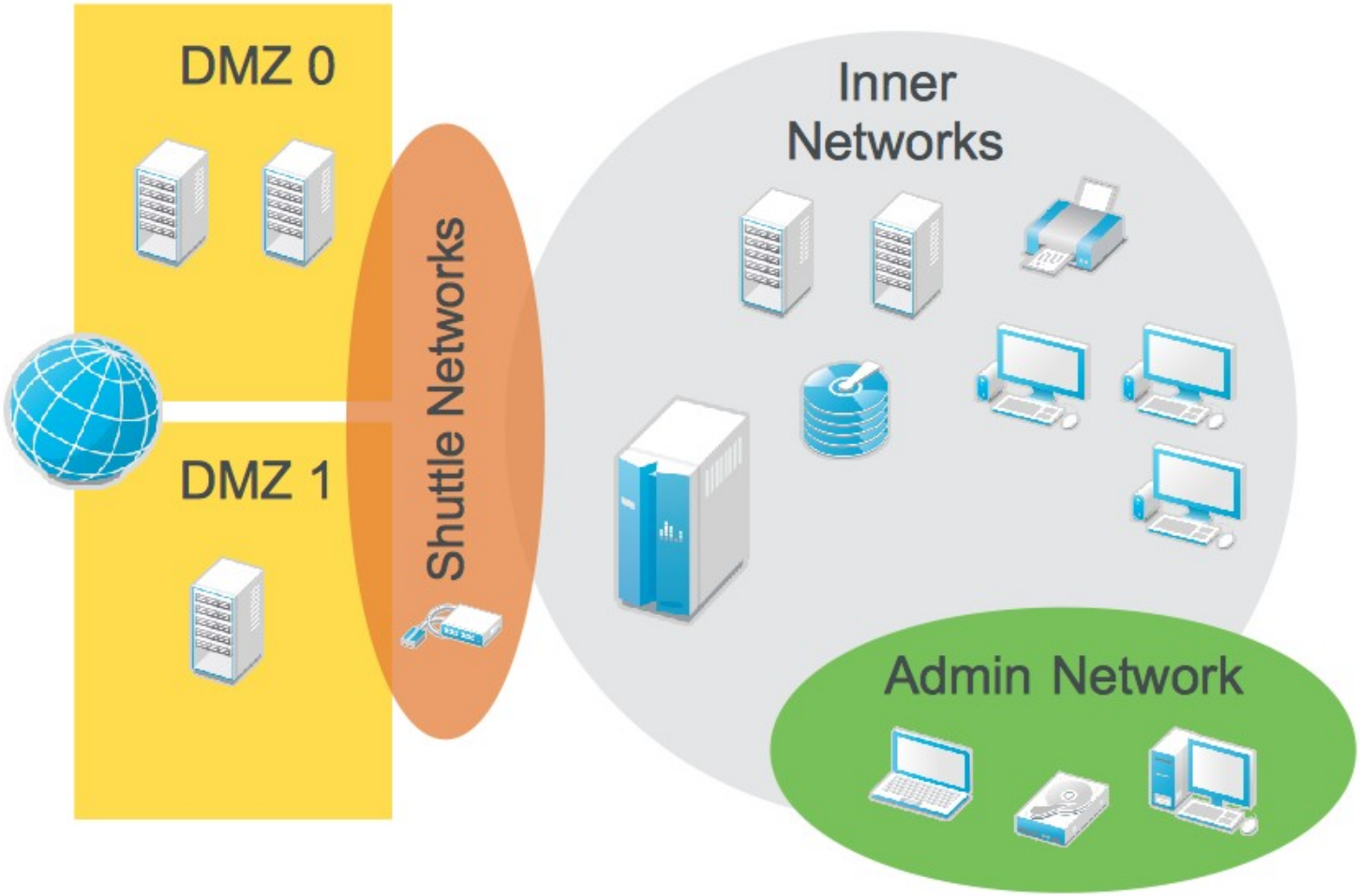
# Planowanie i instalacja

# Wsparcie dla systemów Linux

https://www.suse.com/support/



# Linux – podział sieci



Network Configuration...

# Registration

## SUSE Linux Enterprise Desktop 12

Please enter a registration or evaluation code for this product and your User Name/EMail from the SUSE Customer Center in the fields below. Access to security and general software updates is only possible on a registered system.

If you skip the registration now be sure to do so in the installed system.

Email

Registration Code

Local Registration Server...

Skip Registration

Help | Release Notes... | Abort | Back | Next

# Suggested Partitioning

- Create swap volume /dev/vda1 (1.46 GiB)
- Create root volume /dev/vda2 (10.53 GiB) with btrfs
- Create subvolume @/boot/grub2/i386-pc on device /dev/vda2
- Create subvolume @/boot/grub2/x86_64-efi on device /dev/vda2
- Create subvolume @/home on device /dev/vda2
- Create subvolume @/opt on device /dev/vda2
- Create subvolume @/srv on device /dev/vda2
- Create subvolume @/tmp on device /dev/vda2
- Create subvolume @/usr/local on device /dev/vda2
- Create subvolume @/var/crash on device /dev/vda2
- Create subvolume @/var/lib/libvirt/images on device /dev/vda2 with option "no copy on write"
- Create subvolume @/var/lib/mailman on device /dev/vda2
- Create subvolume @/var/lib/mariadb on device /dev/vda2 with option "no copy on write"
- Create subvolume @/var/lib/named on device /dev/vda2
- Create subvolume @/var/lib/pgsql on device /dev/vda2 with option "no copy on write"
- Create subvolume @/var/log on device /dev/vda2
- Create subvolume @/var/opt on device /dev/vda2
- Create subvolume @/var/spool on device /dev/vda2
- Create subvolume @/var/tmp on device /dev/vda2

Edit Proposal Settings

Create Partition Setup...

Expert Partitioner...

Help | Release Notes... | Abort | Back | Next

# Software Selection and System Tasks

| | | Pattern |
|---|---|---|
| − | | **Desktops** |
| ✓ | | GNOME (Default) |
| ✓ | | X Window System |
| − | | **Graphical Environme...** |
| ☐ | | Fonts |
| − | | **Additional Software** |
| ✓ | | Help and Support Document... |
| ✓ | | AppArmor |
| ☐ | | Laptop |
| − | | **Development** |
| ☐ | | C/C++ Compiler and Tools |
| − | | **Primary Functions** |
| ☐ | | Client to virtualization server |
| ☐ | | Web-Based Enterprise Mana... |
| − | | **Base Technologies** |
| ✓ | | Desktop Base System |
| ✓ | | 32-Bit Runtime Environment |

Details...

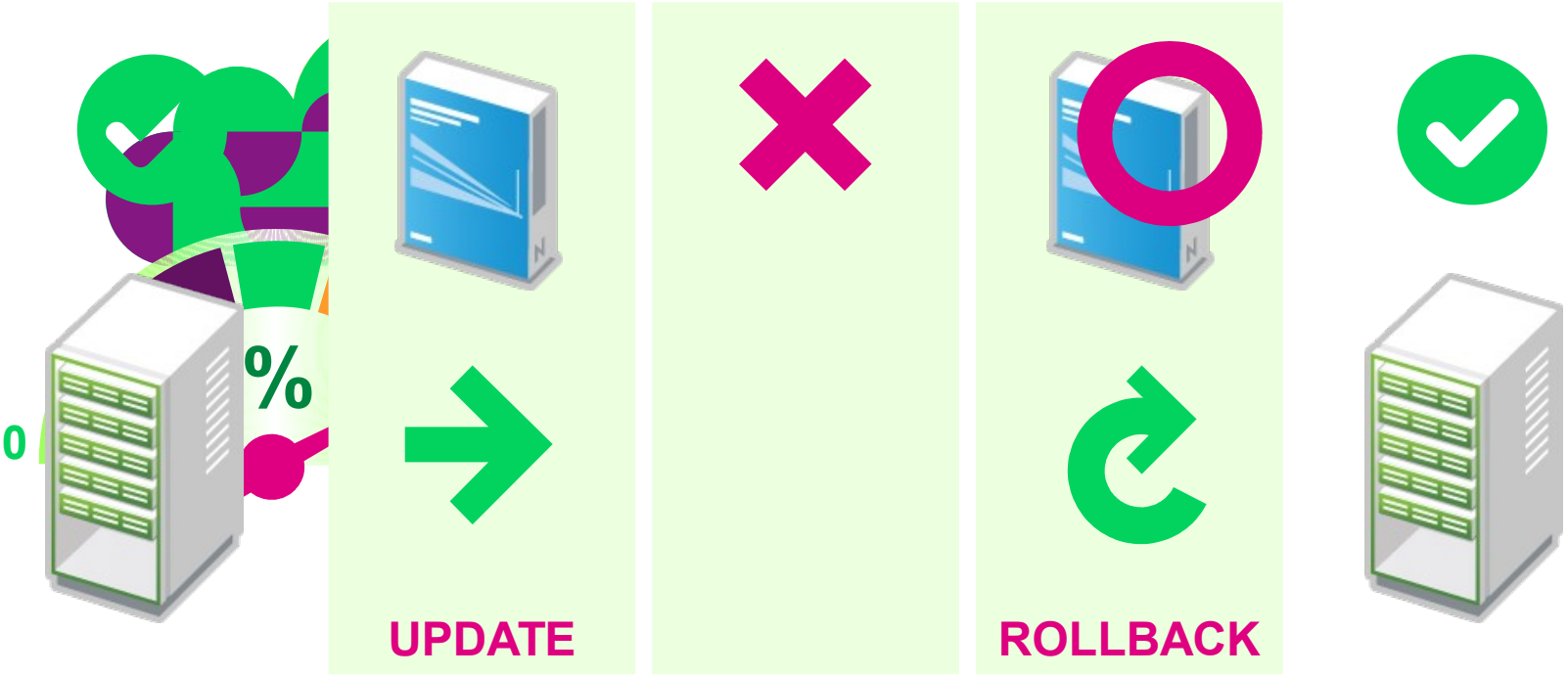
## GNOME (Default)

GNOME is SUSE Linux Enterprise. It is an intuitive and attractive desktop combining industry-leading usability with a powerful set of applications and management features that are essential to enterprise adoption.

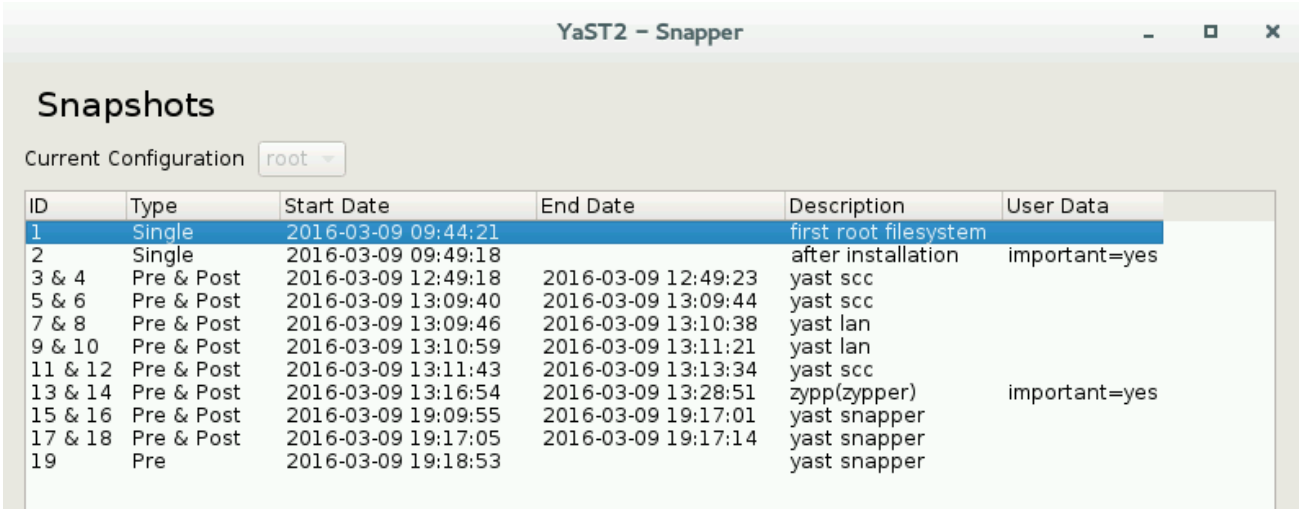
| Name | Disk Usage | Free | Total |
|---|---|---|---|
| / | 41% | 6.2 GB | 10.5 GB |

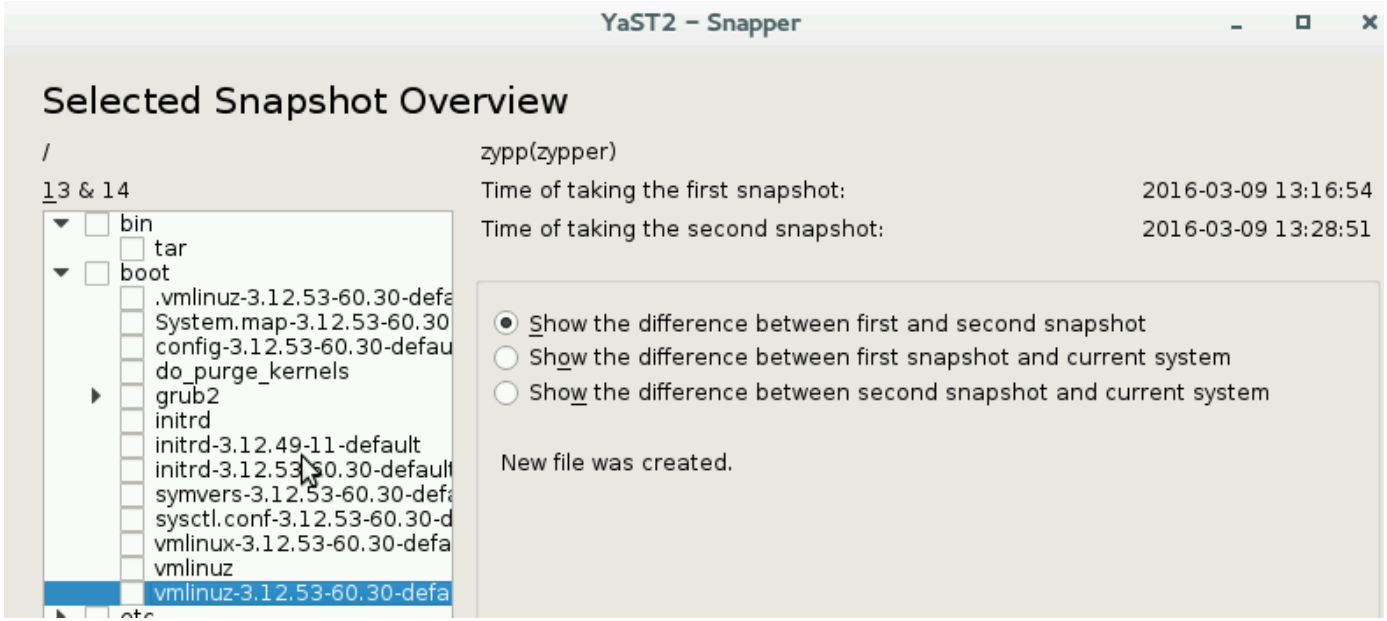
Help | Release Notes... | Cancel | Back | OK

# SLES – bezpieczne wgrywanie poprawek



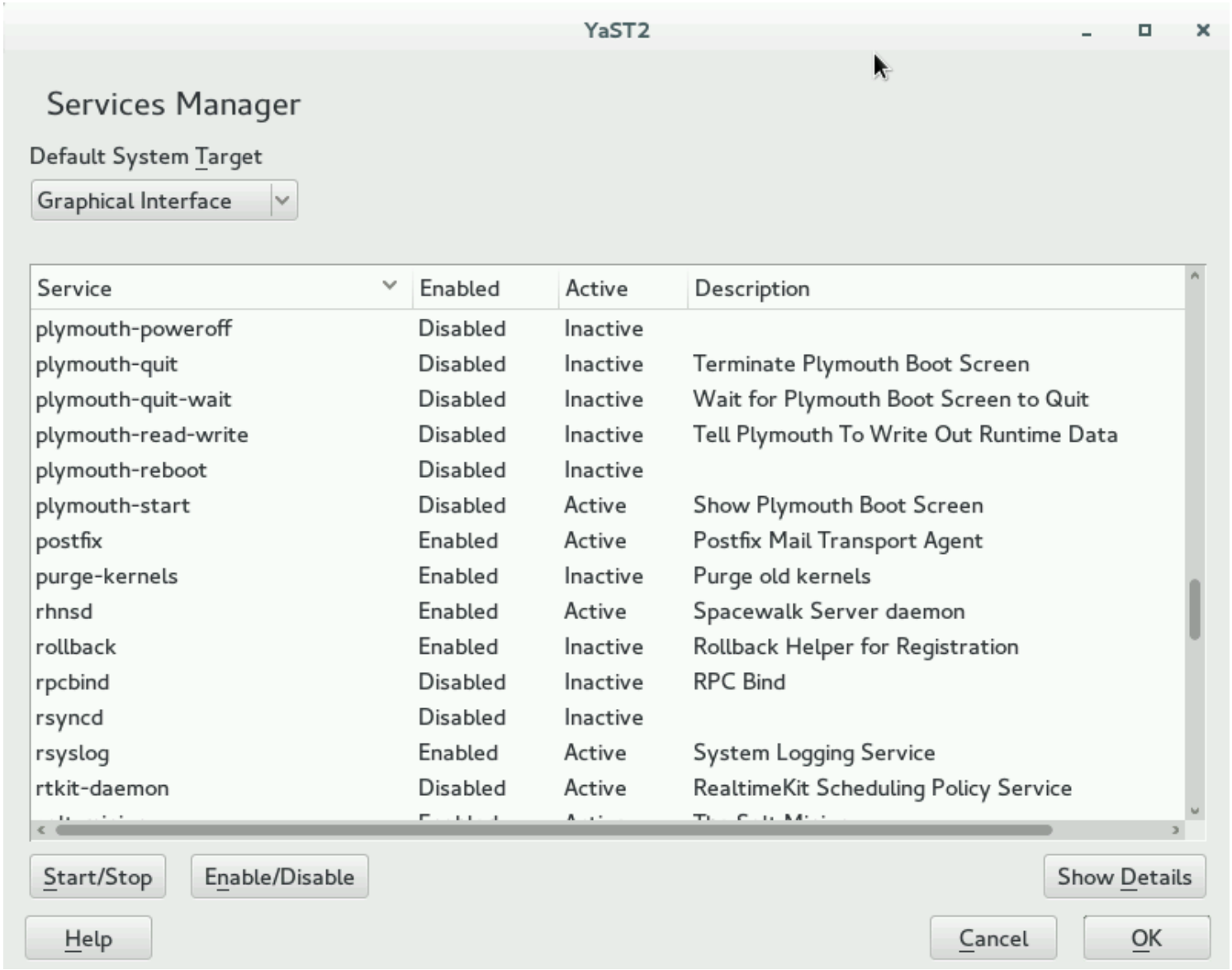
# SLES 12 SP1 - System plików Btrfs



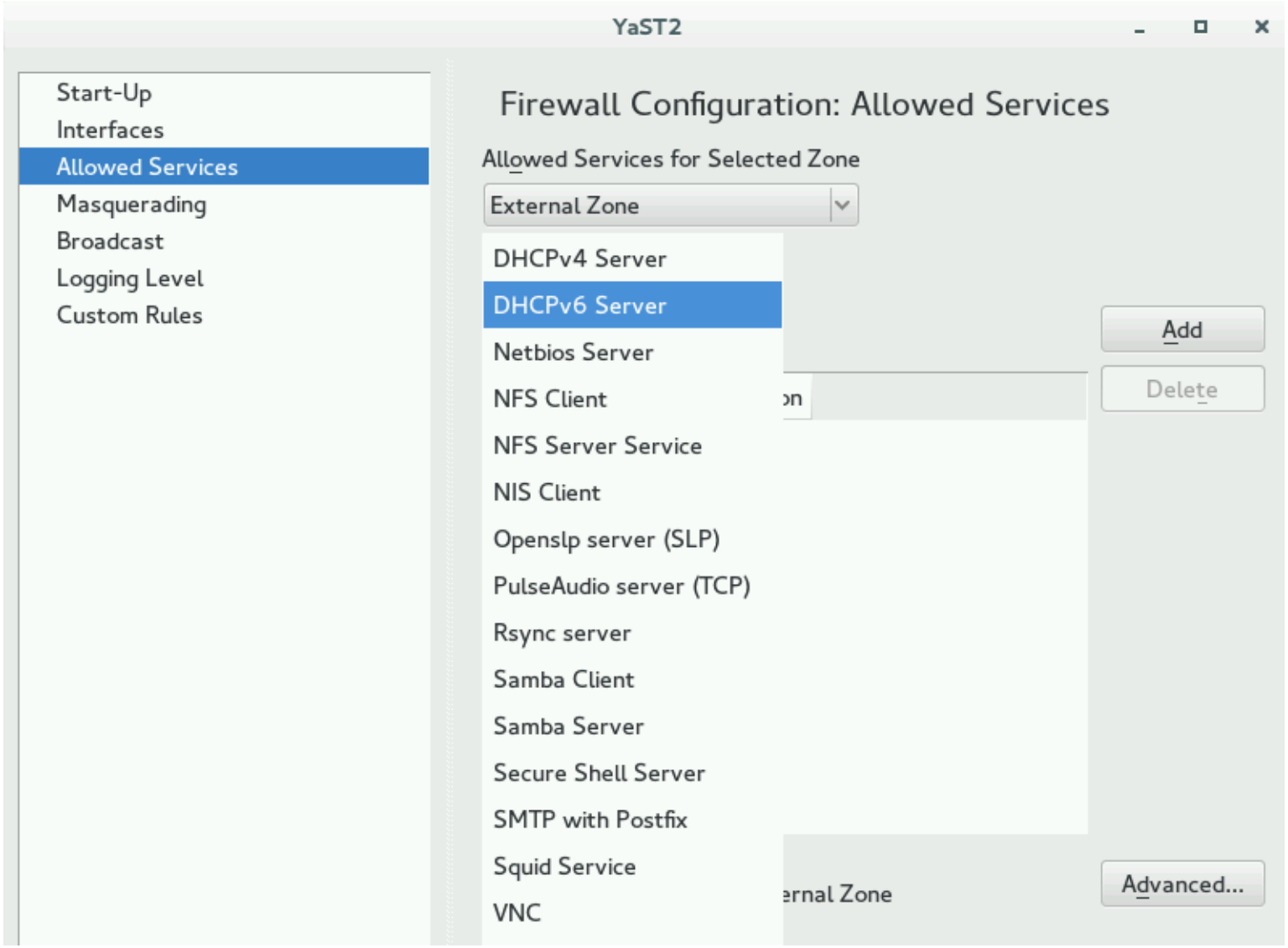



# Konfiguracja i poprawki

# Wyłączenie zbędnych usług – YaST



# YaST – Firewall



# Bezpieczne zarządzanie – SSH

**ssh-keygen -t dsa -b 1024**

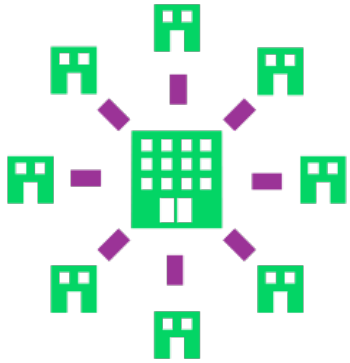
```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

Aby przyśpieszyć logowanie za pomocą ssh należy wyłączyć rozwiązywanie nazw DNS w konfiguracji serwera ssh (na zdalnym serwerze)

**#vi /etc/sshd/sshd_config**

**UseDNS no**

**#systemctl restart sshd**



# Bezpieczne zarządzanie – SSH

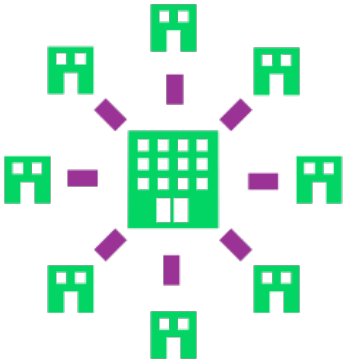
**Automatyczna propagacja kluczy ssh na serwer**

ssh-copy-id -i /root/.ssh/id_dsa.pub root@sles11-hae-node2

Zaleca się, aby lokalnie też można było logować się za pomocą ssh:

ssh-copy-id -i /root/.ssh/id_dsa.pub root@localhost

**Dodatkowe zabezpieczenia sshd**
**#vi /etc/sshd/sshd_config**
**Port 1234**
**PermitRootLogin no**
**AllowUsers lokalnyadmin**
**#systemctl restart**



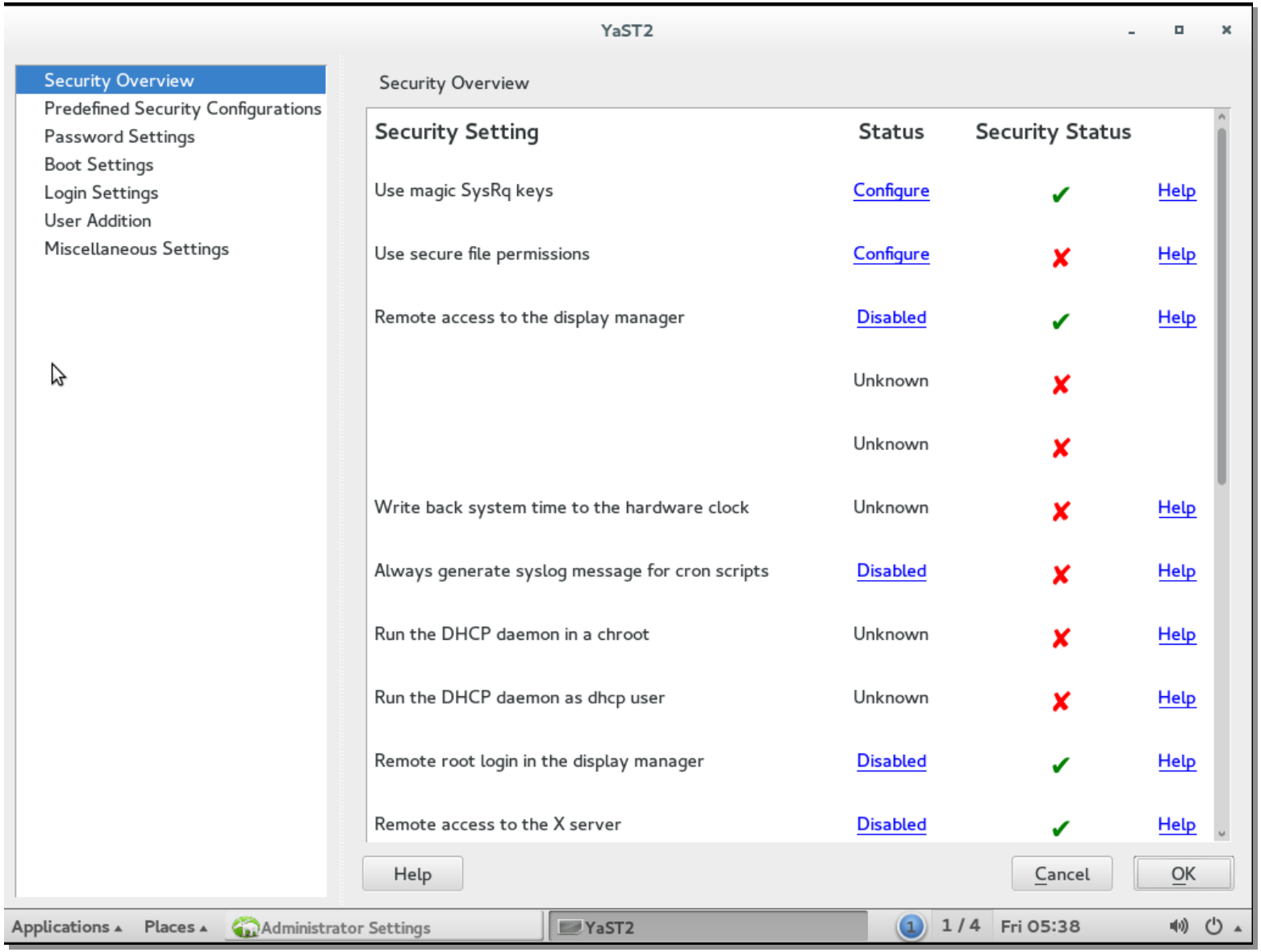
# System plików – uprawnienia

- Sprawdzanie plików i katalogów pod kątem możliwości zapisywania do nich przez wszystkich
  find / -perm -0002 -type f –print
  find / -perm -0002 -type d –print

- Sprawdzanie plików i katalogów pod kątem możliwości odczytu danych przez wszystkich
  find / -perm -0004 -type f –print
  find / -perm -0004 -type d –print

- Sprawdzanie plików pod kątem bitów suid / sgid
  find / -perm +4000 -type f –print
  find / -perm +2000 -type f -print

# YAST – Security Center



# Audyt i monitorowanie

# SUDO – delegacja uprawnień

Sudo – mechanizm nadawania praw do wykonywania programów, poleceń  w systemie Linux

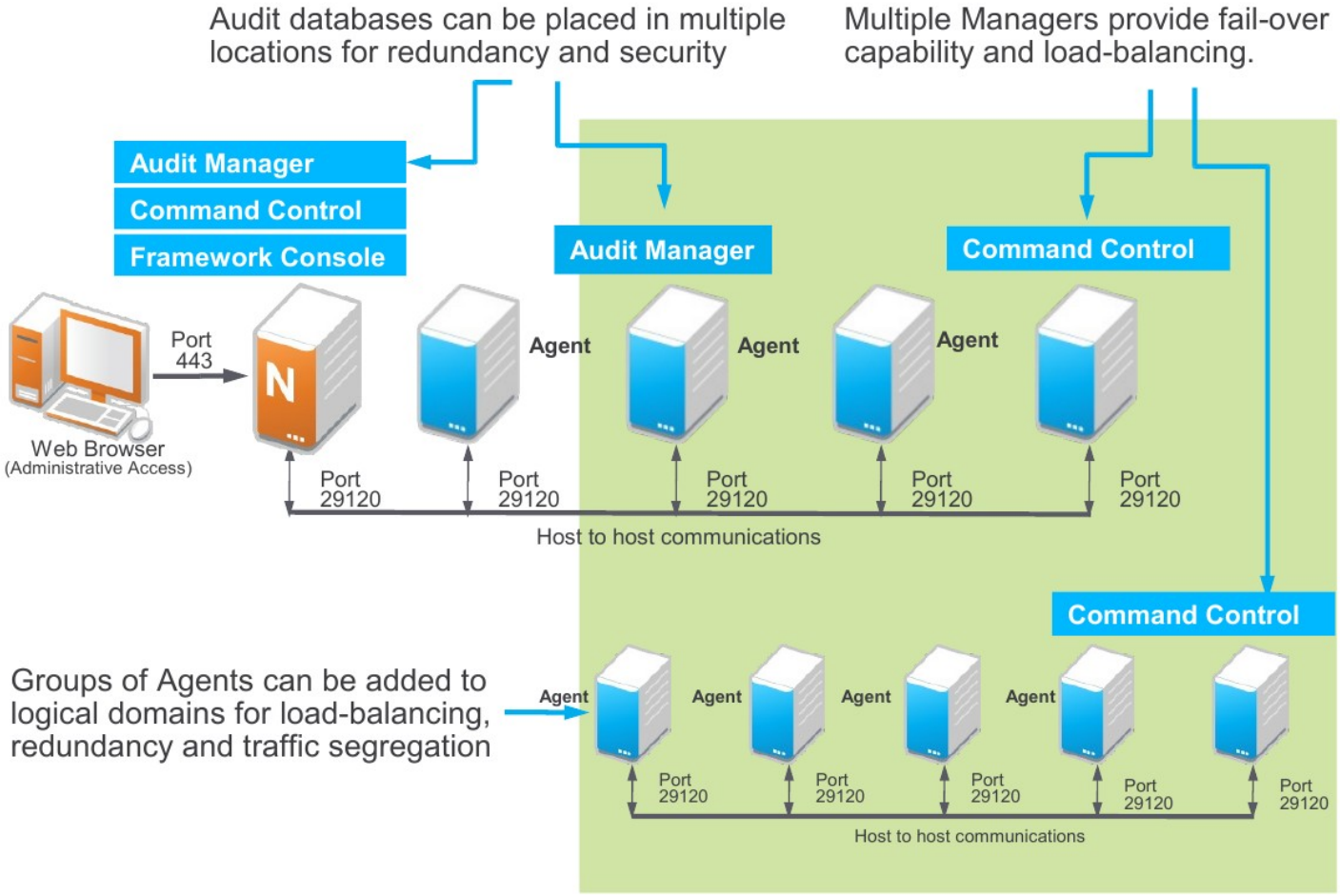
Tworzymy konto lokalnego administratora np. *lokalnyadmin*  i nadajemy mu prawa do wykonywania poleceń z prawami konta „root”.  Visudo

**Cmnd_Alias BlokCmd = /usr/bin/passwd**
**Lokalnyadmin ALL=ALL, !BlockCmd**

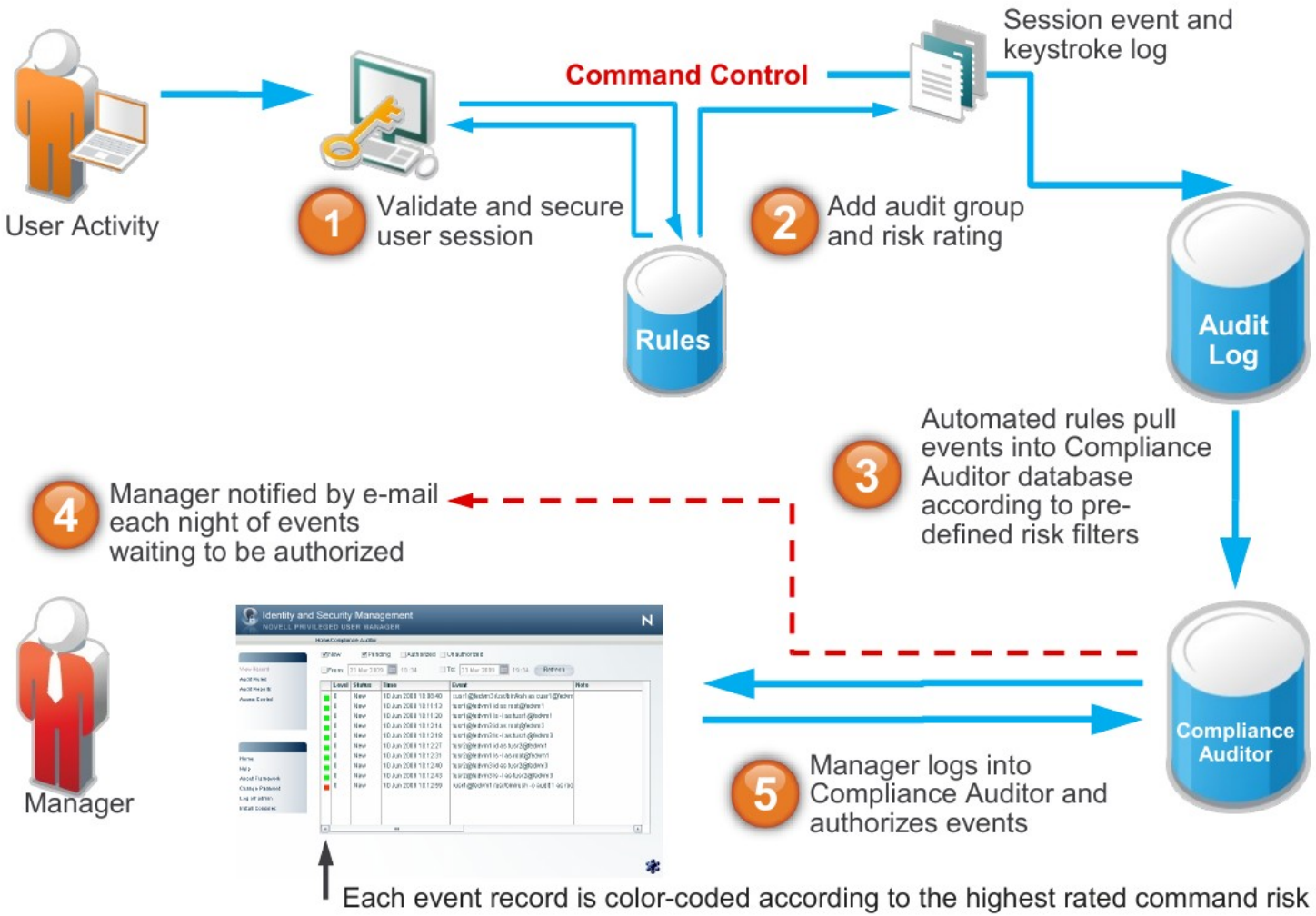
Wykonywany program należy poprzedzić poleceniem sudo np. **sudo fdisk –**l

**SUDO loguje zdarzenia !!!**

# NetIQ PAM – centralne „sudo”



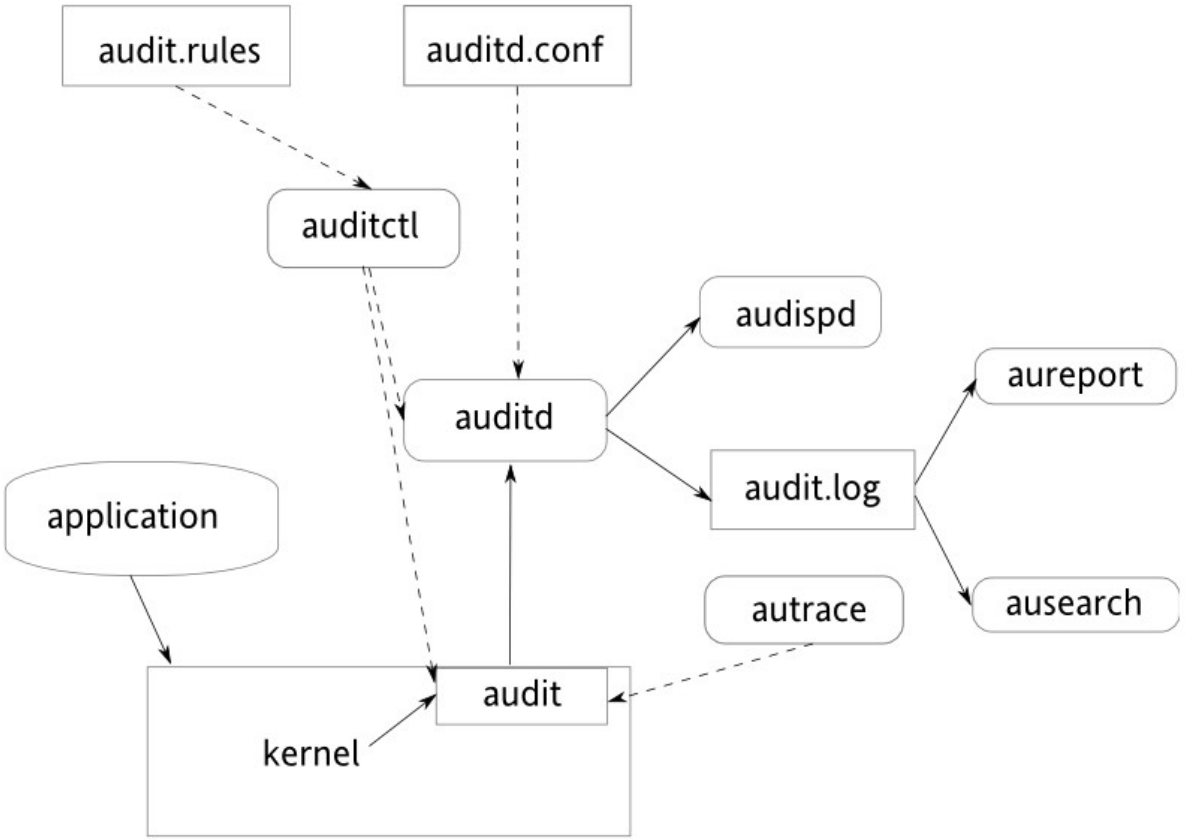
# NetIQ PAM – centralne „sudo”



# Linux Audit

**/etc/audit/auditd.conf**

**/var/log/audit/audit.log**



# Linux Audit - aureport

```
aureport

Summary Report
======================
Range of time in logs: 03/02/09 14:13:38.225 - 17/02/09 16:30:10.352
Selected time for report: 03/02/09 14:13:38 - 17/02/09 16:30:10.352
Number of changes in configuration: 24
Number of changes to accounts, groups, or roles: 0
Number of logins: 9
Number of failed logins: 15
Number of authentications: 19
Number of failed authentications: 578
Number of users: 3
Number of terminals: 15
Number of host names: 4
Number of executables: 20
Number of files: 279
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 994
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 2
Number of process IDs: 1238
Number of events: 5435
```

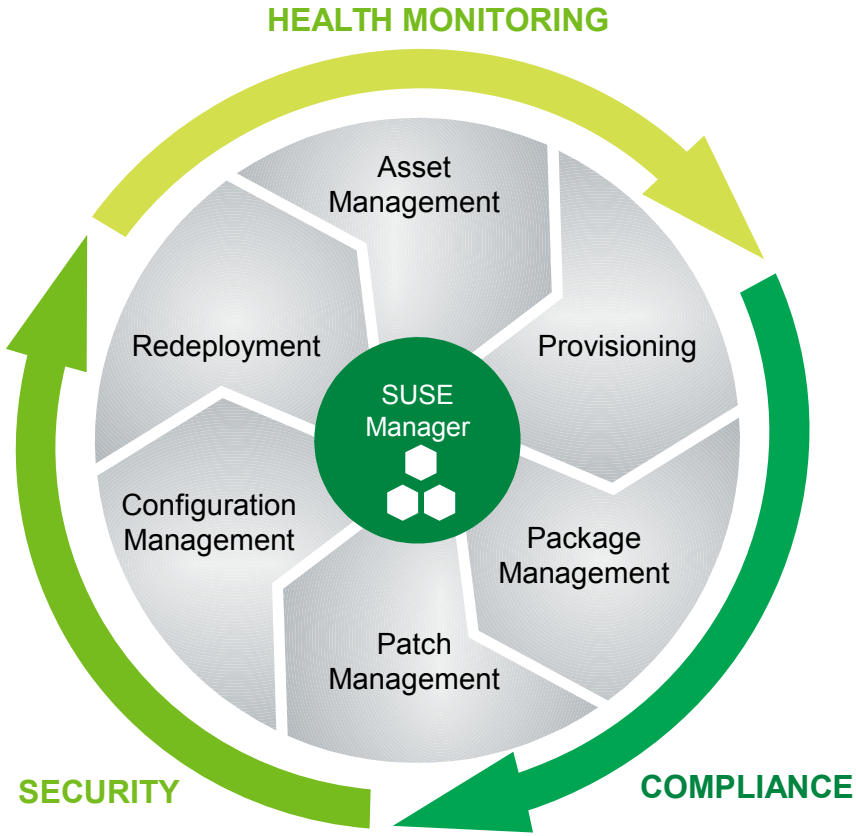
# DAC vs MAC – dwa podejścia do uprawnień

- **Discretionary Access Control (DAC) –** właściciel zasobu (użytkownik) ma prawo zarządzać prawami dostępu do swoich zasobów. Klasyczne podejście do modelu bezpieczeństwa.

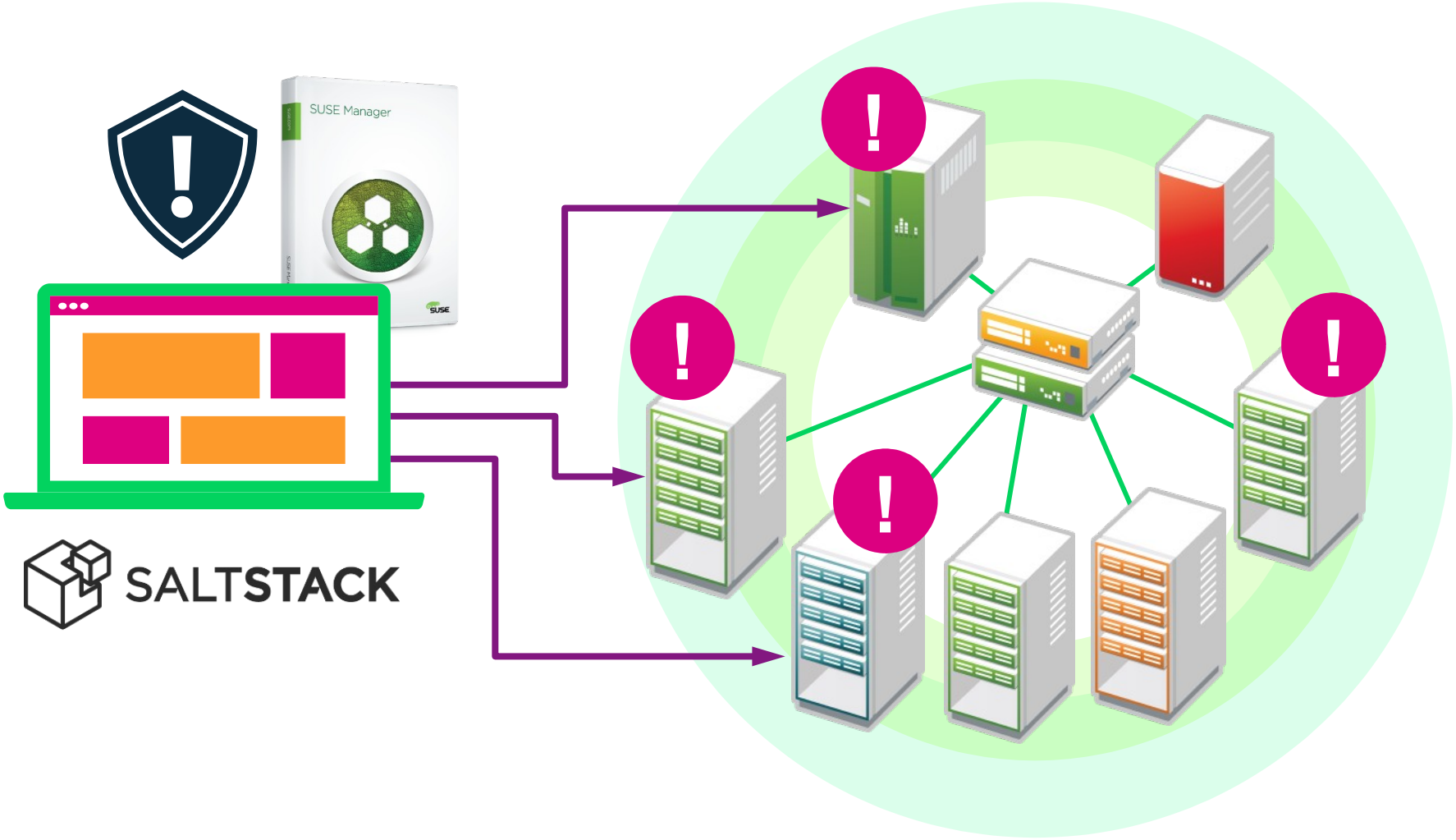
- **Mandatory Access Control (MAC) –** obowiązkowa kontrola dostępu dla podmiotów (użytkownik, proces) do obiektów (plik, katalog, urządzenie, port sieciowy). Kontrola odbywa się za pomocą odpowiednich atrybutów oraz polityk. Implementacje w SUSE Linux: AppArmor, SELinux.

# SUSE Manager

- ✓ Optymalizacja zarządzania
  - Wdrażanie
  - Zarządzanie pakietami, poprawkami
  - Ponowna instalacja
- ✓ Kontrola
  - Audyt systemów
  - Raporty
- ✓ Obsługiwane systemy
  - SLES, RHEL + CentOS z Expanded Support
  - RHEL + RHN
  - CentOS + OEL – nie wspierane komercyjnie jeszcze, ale działają ;-)



# Zarządzanie konfiguracją w oparciu o Salt




Scalable

Speed

Size

Built for Future

# Systemy monitorowania

- Nagios – część SUSE Linux
- Icinga – część SUSE Managera
- Zabbix

Co monitorujemy:
- pamięć, zużycie hdd, procesora
- ruch sieciowy
- temperatura

Należy pamiętać o konfiguracji:
- wykresów
- powiadomień

# Wykrywanie włamań

# Host Intrusion Detection System – AIDE

AIDE – program do sprawdzania integralności plików w systemie Linux.

/etc/aide.conf – plik konfiguracyjny

**aide –i** – pierwsze uruchomienie

po utworzeniu bazy aide należy ją przenieść w bezpieczne miejsce

Następnie cyklicznie sprawdzamy co zmieniło się w naszym systemie poleceniem: **aide --check**

Aktualizacja bazy: **aide --update**

# Host Intrusion Detection System – AIDE

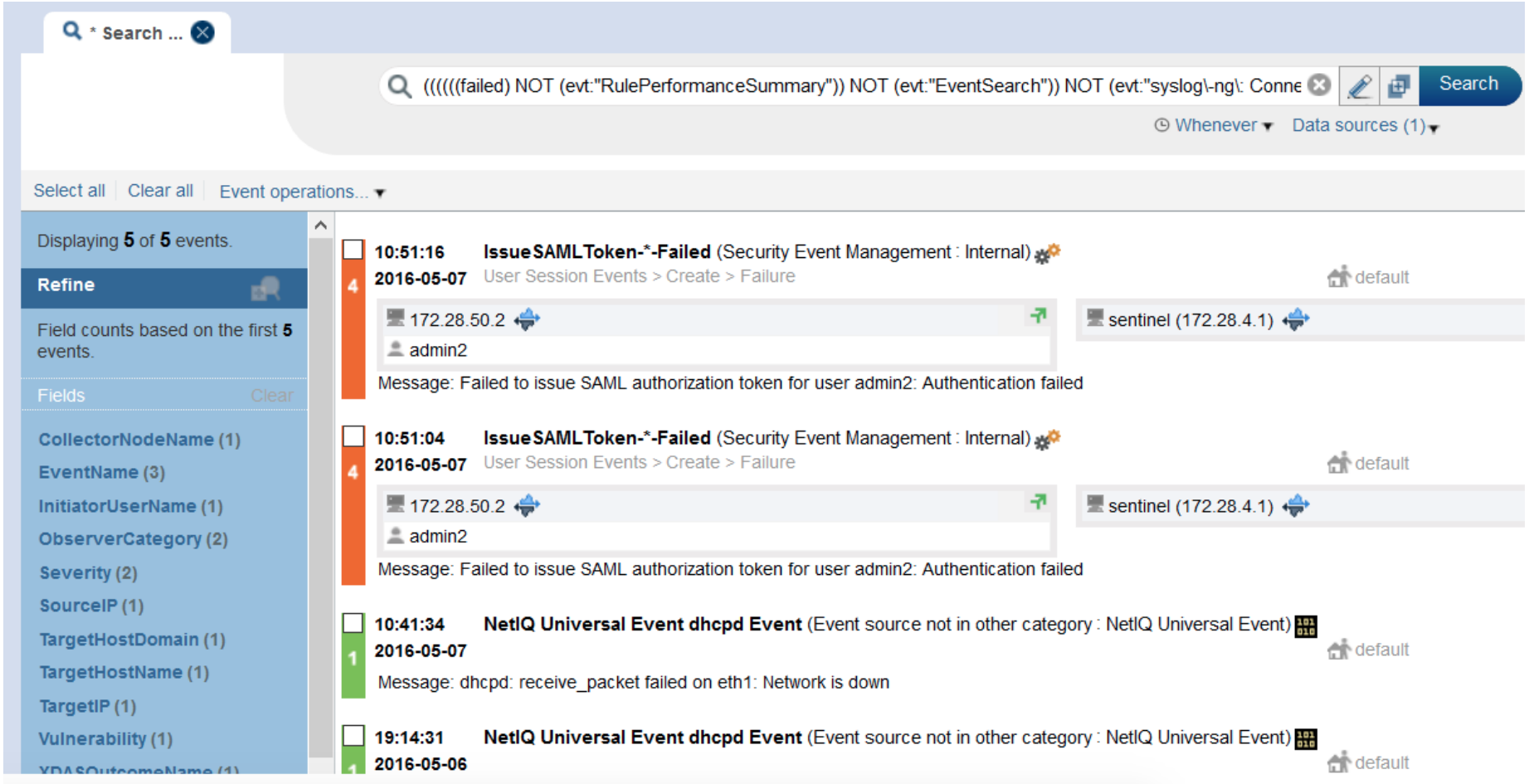
```
# Custom rules
#
Binlib          = p+i+n+u+g+s+b+m+c+sha256+sha512
ConfFiles       = p+i+n+u+g+s+b+m+c+sha256+sha512
Logs            = p+i+n+u+g+S
Devices         = p+i+n+u+g+s+b+c+sha256+sha512
Databases       = p+n+u+g
StaticDir       = p+i+n+u+g
ManPages        = p+i+n+u+g+s+b+m+c+sha256+sha512
```

```
# watch config files, but exclude, what changes at boot time, ...
!/etc/mtab
!/etc/lvm*
/etc                                            ConfFiles
```

# Host Intrusion Detection System – rootkit`y

chkrootkit, rkhunter – narzędzia nie są dostępne standardowo w SLES 11/12.
Można je zainstalować z dodatkowych kanałów na stronie:
http://software.opensuse.org

# SIEM – NetIQ Sentinel



# Testy penetracyjne

http://www.kali.org

http://www.openvas.org


**Corporate Headquarters**
Maxfeldstrasse 5
90409 Nuremberg
Germany

+49 911 740 53 0 (Worldwide)
www.suse.com

Join us on:
www.opensuse.org