



# SUSE Linux security & hardening

Piotr Szewczuk  
Starszy konsultant  
[pszewczuk@suse.com](mailto: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/>

## SUSE Support Forums

Get your questions answered by experienced Sys Ops or interact with other SUSE community experts.

[Join Our Community](#)

## Support Resources

Learn how to get the most from the technical support you receive with your SUSE Subscription, Premium Support, Academic Program, or Partner Program.

[SUSE Technical Support Handbook](#)

[Update Advisories](#)

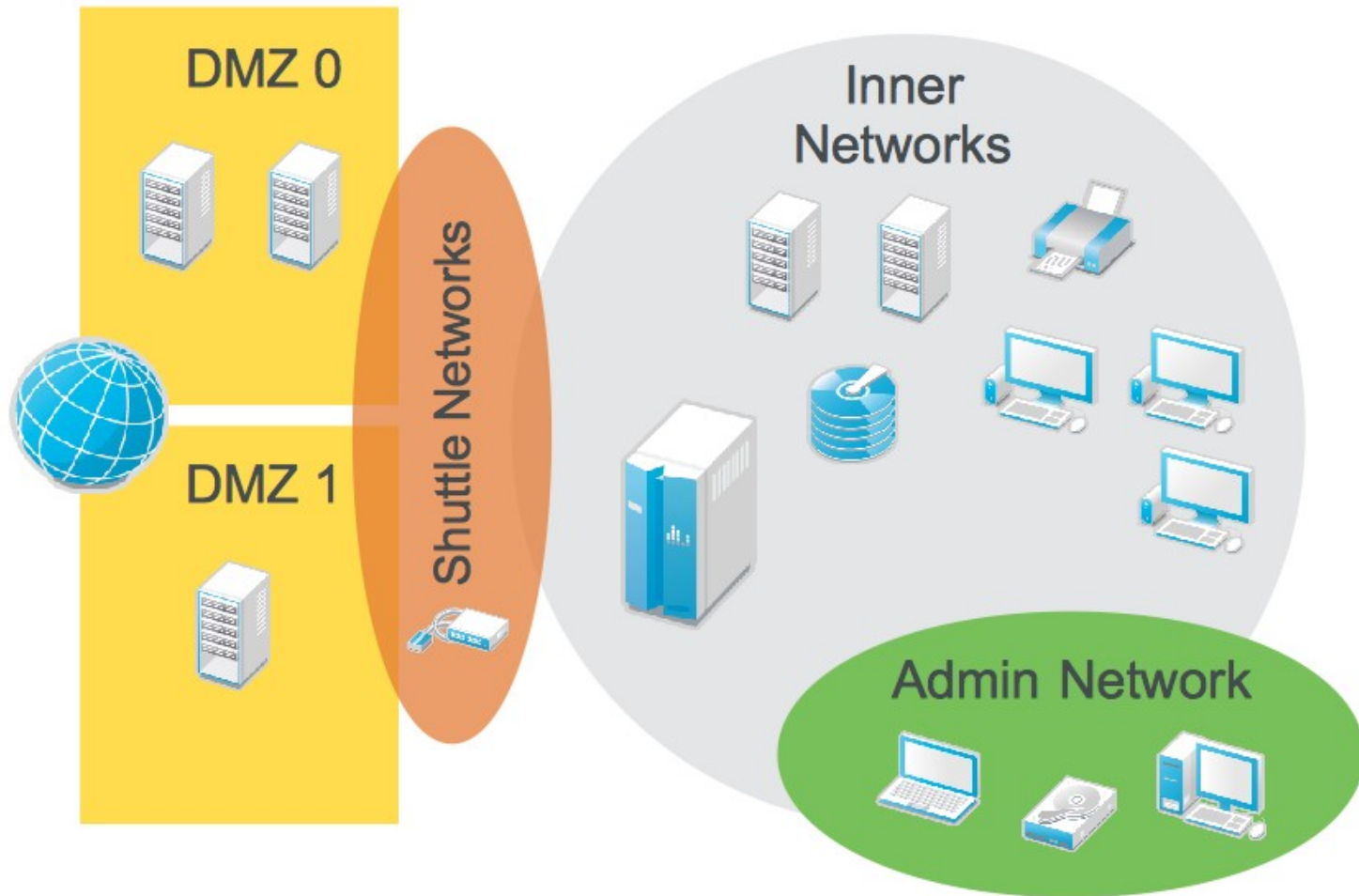
[Support FAQ](#)

## Open an Incident

Open an incident with SUSE Technical Support, manage your subscriptions, download patches, or manage user access.

[Go to Customer Center](#)

# Linux – podział sieci



# 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](#)

## 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

## 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

[Details...](#)

[Help](#)

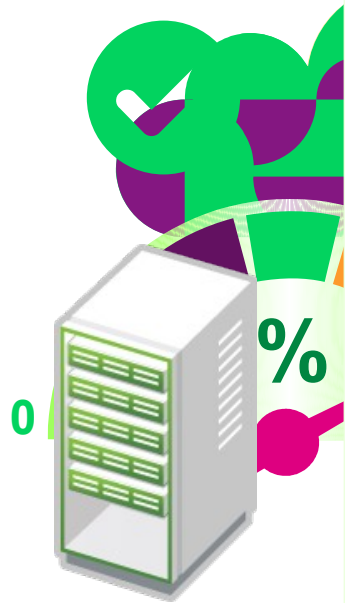
[Release Notes...](#)

[Cancel](#)

[Back](#)

[OK](#)

# SLES – bezpieczne wgrywanie poprawek



**UPDATE**

A light green vertical panel containing a blue server rack icon at the top. Below it is a large green arrow pointing to the right. At the bottom, the word "UPDATE" is written in pink capital letters.

**ROLLBACK**

A light green vertical panel containing a large pink 'X' mark in the center. At the bottom, the word "ROLLBACK" is written in pink capital letters.

**ROLLBACK**

A light green vertical panel containing a blue server rack icon at the top, which is circled in pink. Below it is a large green circular arrow icon. At the bottom, the word "ROLLBACK" is written in pink capital letters.

# SLES 12 SP1 - System plików Btrfs

YaST2 - Snapper

### Snapshots

Current Configuration: root

ID	Type	Start Date	End Date	Description	User Data
1	Single	2016-03-09 09:44:21		first root filesystem	
2	Single	2016-03-09 09:49:18		after installation	important=yes
3 & 4	Pre & Post	2016-03-09 12:49:18	2016-03-09 12:49:23	yast scc	
5 & 6	Pre & Post	2016-03-09 13:09:40	2016-03-09 13:09:44	yast scc	
7 & 8	Pre & Post	2016-03-09 13:09:46	2016-03-09 13:10:38	yast lan	
9 & 10	Pre & Post	2016-03-09 13:10:59	2016-03-09 13:11:21	yast lan	
11 & 12	Pre & Post	2016-03-09 13:11:43	2016-03-09 13:13:34	yast scc	
13 & 14	Pre & Post	2016-03-09 13:16:54	2016-03-09 13:28:51	zypp(zypper)	important=yes
15 & 16	Pre & Post	2016-03-09 19:09:55	2016-03-09 19:17:01	yast snapper	
17 & 18	Pre & Post	2016-03-09 19:17:05	2016-03-09 19:17:14	yast snapper	
19	Pre	2016-03-09 19:18:53		yast snapper	

YaST2 - Snapper

### Selected Snapshot Overview

/

13 & 14

- bin
- tar
- boot
  - .vmlinuz-3.12.53-60.30-defa
  - System.map-3.12.53-60.30
  - config-3.12.53-60.30-defau
  - do\_purge\_kernels
  - grub2
  - initrd
  - initrd-3.12.49-11-default
  - initrd-3.12.53-60.30-default
  - symvers-3.12.53-60.30-defa
  - sysctl.conf-3.12.53-60.30-d
  - vmlinuz-3.12.53-60.30-defa
  - vmlinuz
  - vmlinuz-3.12.53-60.30-defa

zypp(zypper)

Time of taking the first snapshot: 2016-03-09 13:16:54

Time of taking the second snapshot: 2016-03-09 13:28:51

Show the difference between first and second snapshot

Show the difference between first snapshot and current system

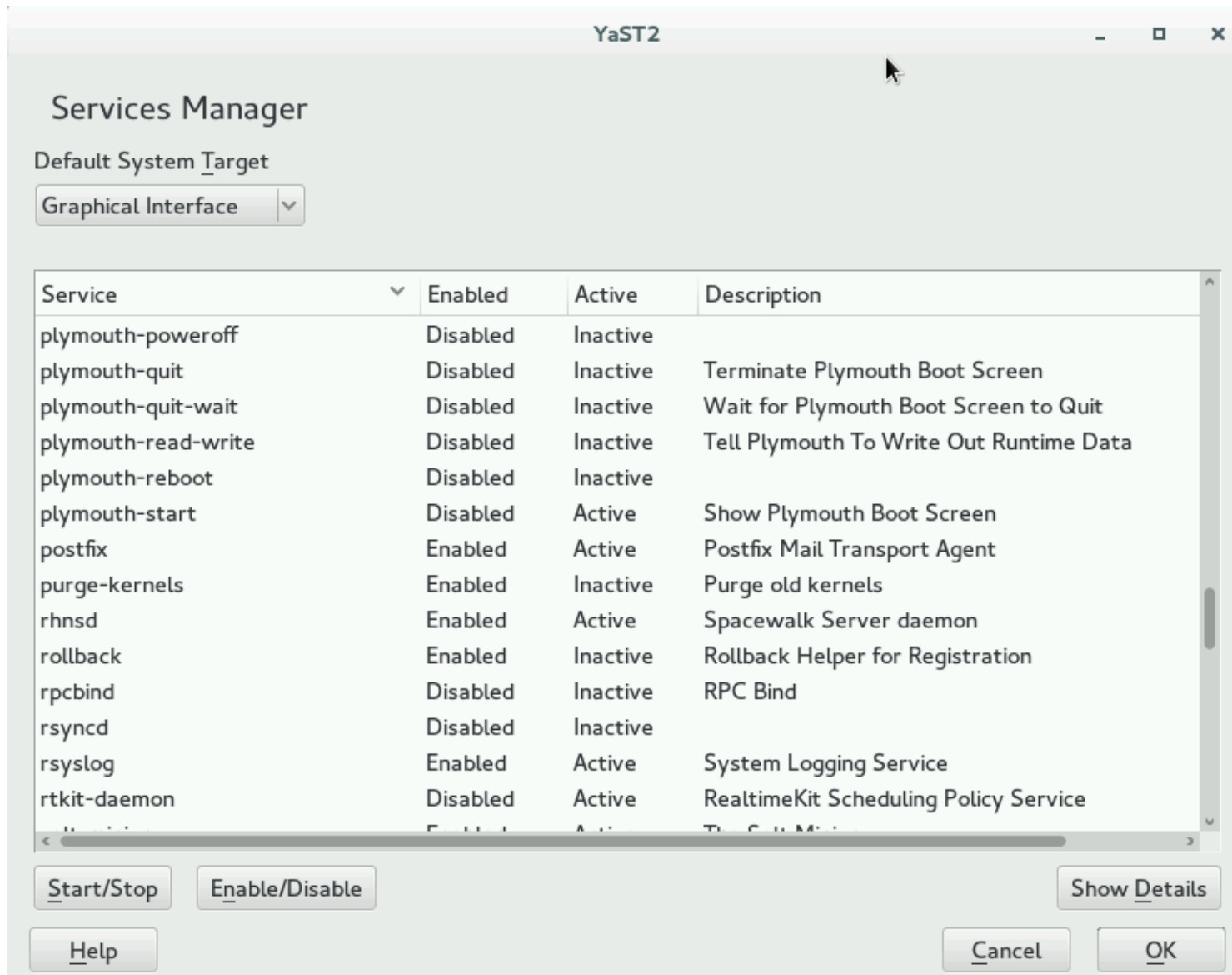
Show the difference between second snapshot and current system

New file was created.



# Konfiguracja i poprawki

# Wyłączenie zbędnych usług – YaST



The screenshot shows the YaST2 Services Manager window. At the top, the title bar reads "YaST2". Below the title bar, the window is titled "Services Manager". Underneath, there is a label "Default System Target" and a dropdown menu currently set to "Graphical Interface". The main area contains a table with the following columns: "Service", "Enabled", "Active", and "Description". The table lists several services, including Plymouth boot screen services, Postfix, rshnd, rsyslog, and rtkit-daemon. At the bottom of the window, there are four buttons: "Start/Stop", "Enable/Disable", "Show Details", and "Help". At the very bottom right, there are "Cancel" and "OK" buttons.

Service	Enabled	Active	Description
plymouth-poweroff	Disabled	Inactive	
plymouth-quit	Disabled	Inactive	Terminate Plymouth Boot Screen
plymouth-quit-wait	Disabled	Inactive	Wait for Plymouth Boot Screen to Quit
plymouth-read-write	Disabled	Inactive	Tell Plymouth To Write Out Runtime Data
plymouth-reboot	Disabled	Inactive	
plymouth-start	Disabled	Active	Show Plymouth Boot Screen
postfix	Enabled	Active	Postfix Mail Transport Agent
purge-kernels	Enabled	Inactive	Purge old kernels
rshnd	Enabled	Active	Spacewalk Server daemon
rollback	Enabled	Inactive	Rollback Helper for Registration
rpcbind	Disabled	Inactive	RPC Bind
rsyncd	Disabled	Inactive	
rsyslog	Enabled	Active	System Logging Service
rtkit-daemon	Disabled	Active	RealtimeKit Scheduling Policy Service

# YaST – Firewall

The screenshot shows the YaST2 Firewall Configuration window, specifically the 'Allowed Services' section. The window title is 'YaST2'. On the left, a sidebar contains a list of configuration options: 'Start-Up', 'Interfaces', 'Allowed Services' (highlighted in blue), 'Masquerading', 'Broadcast', 'Logging Level', and 'Custom Rules'. The main area is titled 'Firewall Configuration: Allowed Services'. Below this title, it says 'Allowed Services for Selected Zone'. A dropdown menu is set to 'External Zone'. A list of services is shown, with 'DHCPv6 Server' selected and highlighted in blue. Other services in the list include DHCPv4 Server, Netbios Server, NFS Client, NFS Server Service, NIS Client, Openslp server (SLP), PulseAudio server (TCP), Rsync server, Samba Client, Samba Server, Secure Shell Server, SMTP with Postfix, Squid Service, and VNC. To the right of the service list are two buttons: 'Add' and 'Delete'. At the bottom right, there is an 'Advanced...' button. The window also has standard window controls (minimize, maximize, close) in the top right corner.

YaST2

## Firewall Configuration: Allowed Services

Allowed Services for Selected Zone

External Zone

- DHCPv4 Server
- DHCPv6 Server**
- Netbios Server
- NFS Client
- NFS Server Service
- NIS Client
- Openslp server (SLP)
- PulseAudio server (TCP)
- Rsync server
- Samba Client
- Samba Server
- Secure Shell Server
- SMTP with Postfix
- Squid Service
- VNC

Add

Delete

Advanced...

# 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.

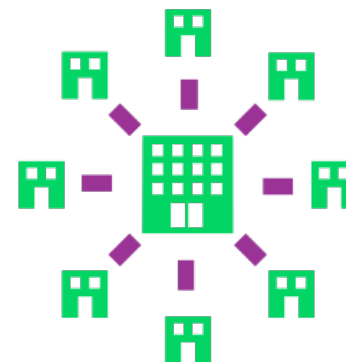
Your public key has been saved in /root/.ssh/id\_dsa.pub.

Aby przyspieszyć 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

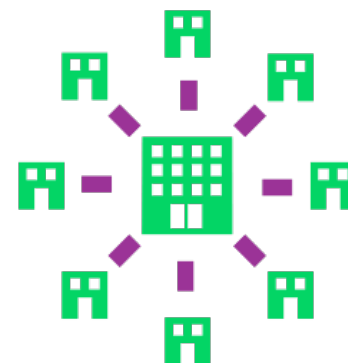
```
ssh-copy-id -i /root/.ssh/id_dsa.pub root@sles11-hae-node2
```

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
```

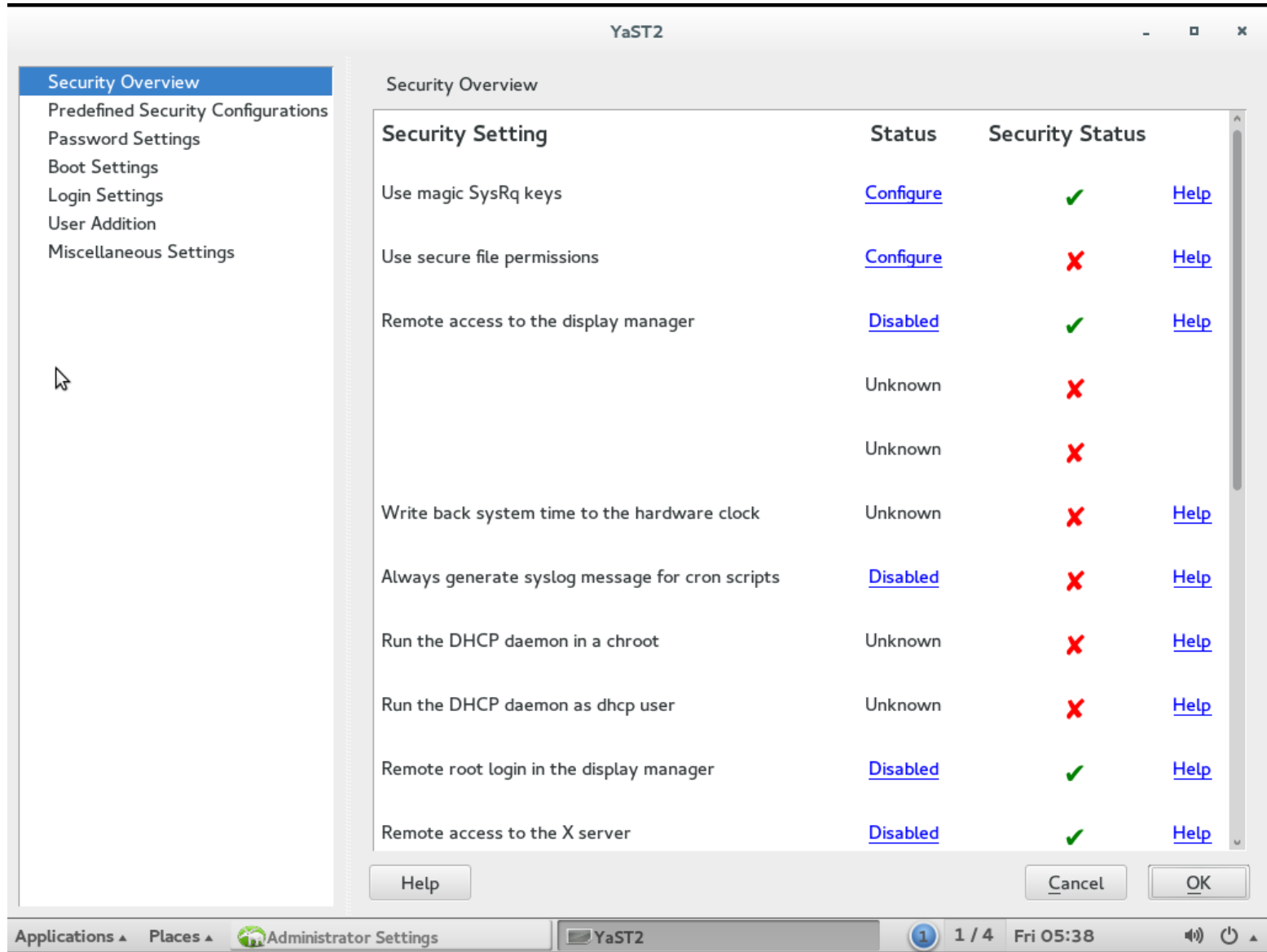




# System plików – uprawnienia

- 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



The screenshot shows the YaST2 Security Overview window. The left sidebar contains a navigation menu with the following items: Security Overview (selected), Predefined Security Configurations, Password Settings, Boot Settings, Login Settings, User Addition, and Miscellaneous Settings. The main content area displays a table of security settings.

Security Setting	Status	Security Status
Use magic SysRq keys	<a href="#">Configure</a>	✓ <a href="#">Help</a>
Use secure file permissions	<a href="#">Configure</a>	✗ <a href="#">Help</a>
Remote access to the display manager	<a href="#">Disabled</a>	✓ <a href="#">Help</a>
	Unknown	✗
	Unknown	✗
Write back system time to the hardware clock	Unknown	✗ <a href="#">Help</a>
Always generate syslog message for cron scripts	<a href="#">Disabled</a>	✗ <a href="#">Help</a>
Run the DHCP daemon in a chroot	Unknown	✗ <a href="#">Help</a>
Run the DHCP daemon as dhcp user	Unknown	✗ <a href="#">Help</a>
Remote root login in the display manager	<a href="#">Disabled</a>	✓ <a href="#">Help</a>
Remote access to the X server	<a href="#">Disabled</a>	✓ <a href="#">Help</a>

At the bottom of the window, there are buttons for Help, Cancel, and OK. The system tray at the bottom shows the Applications menu, Places menu, Administrator Settings, YaST2 window, a notification icon, and the system clock showing 1 / 4 Fri 05:38.



# Audyt i monitorowanie

# SUDO – delegacja uprawnień

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

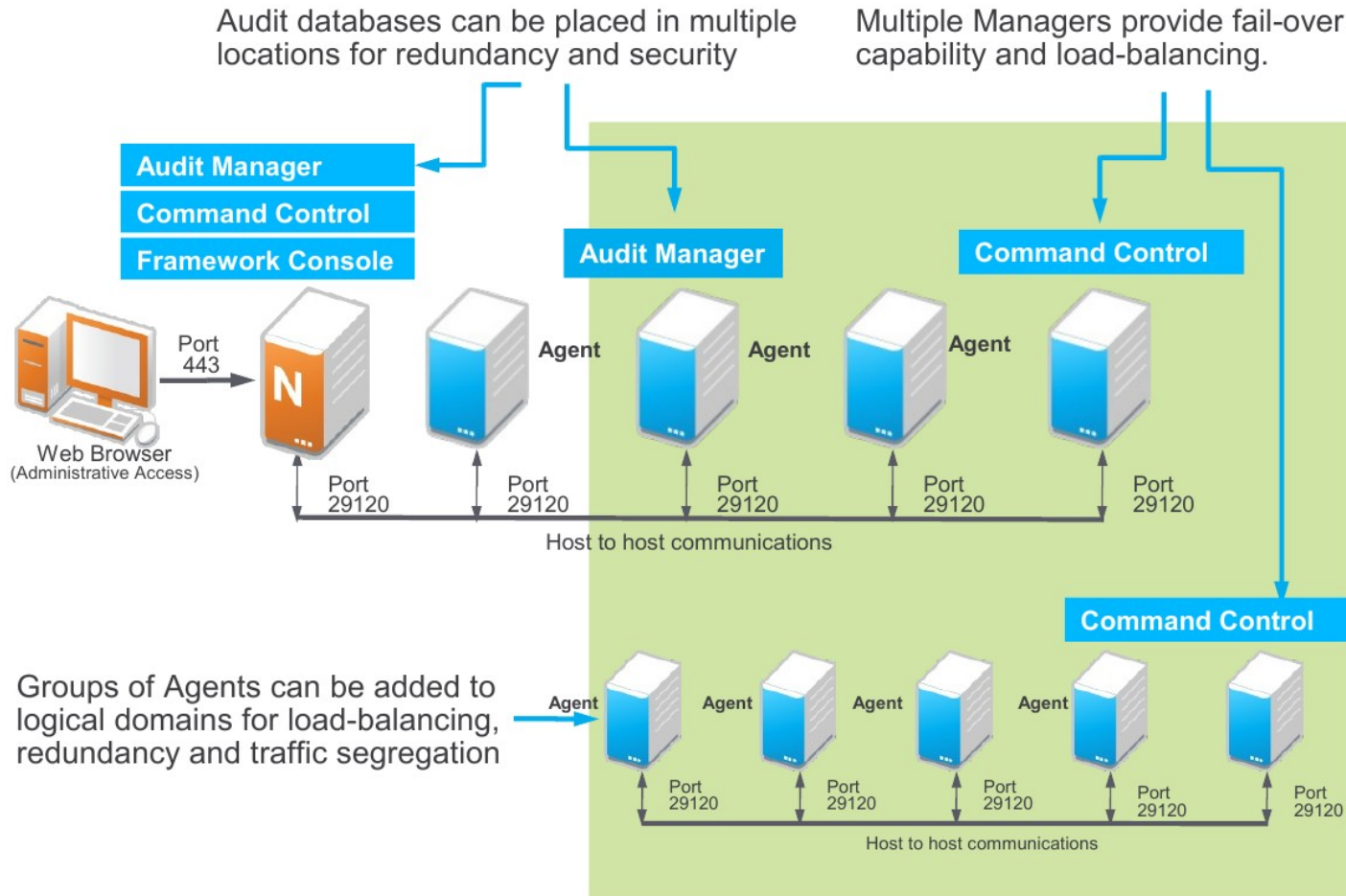
Tworzymy konto lokalnego administratora np. *lokalnyadmin* i nadajemy mu prawa do wykonywania poleceń z prawami konta „root”. Visudo

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

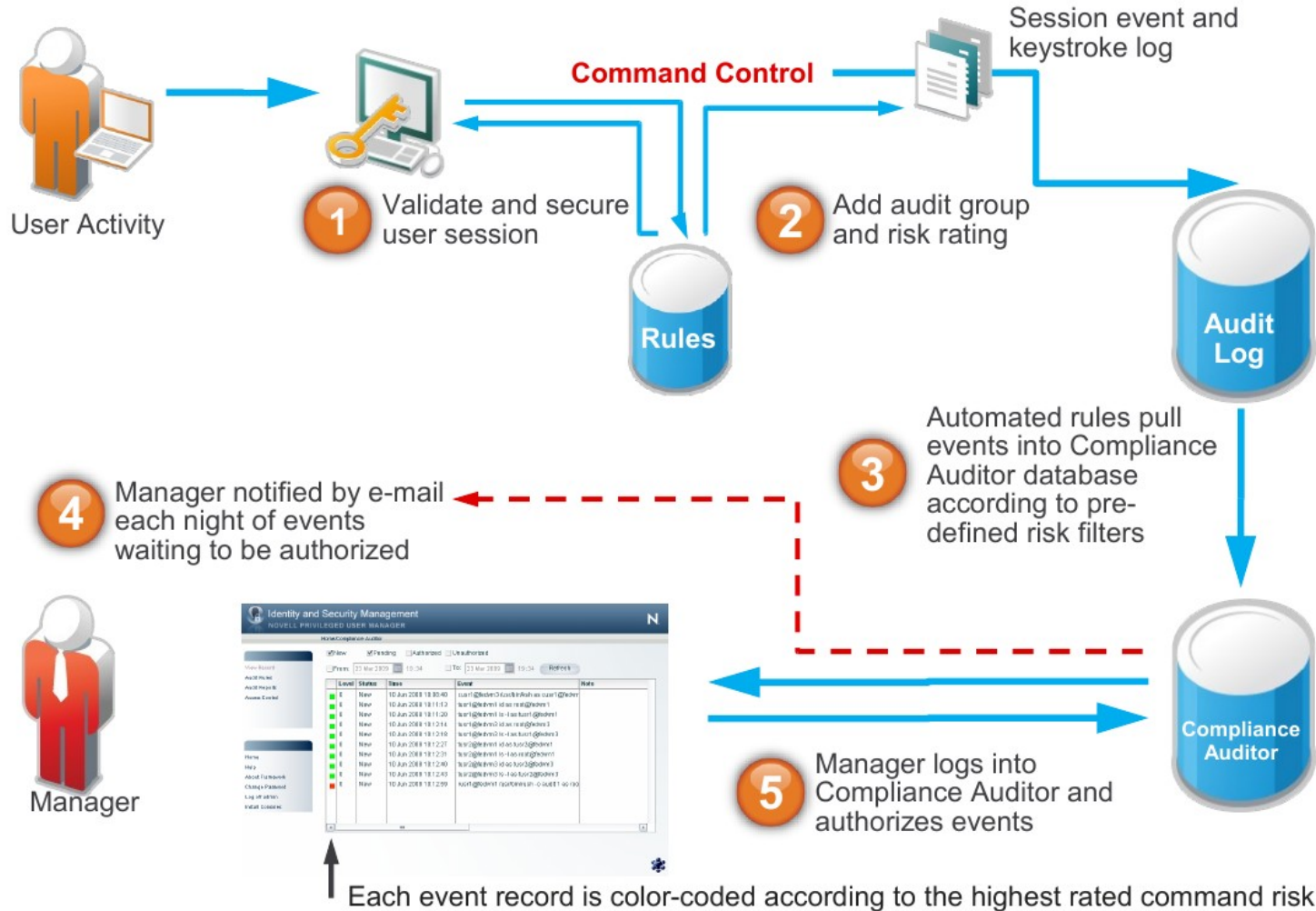
Wykonywany program należy poprzedzić poleceniem sudo np. **sudo fdisk -l**

**SUDO loguje zdarzenia !!!**

# NetIQ PAM – centralne „sudo”



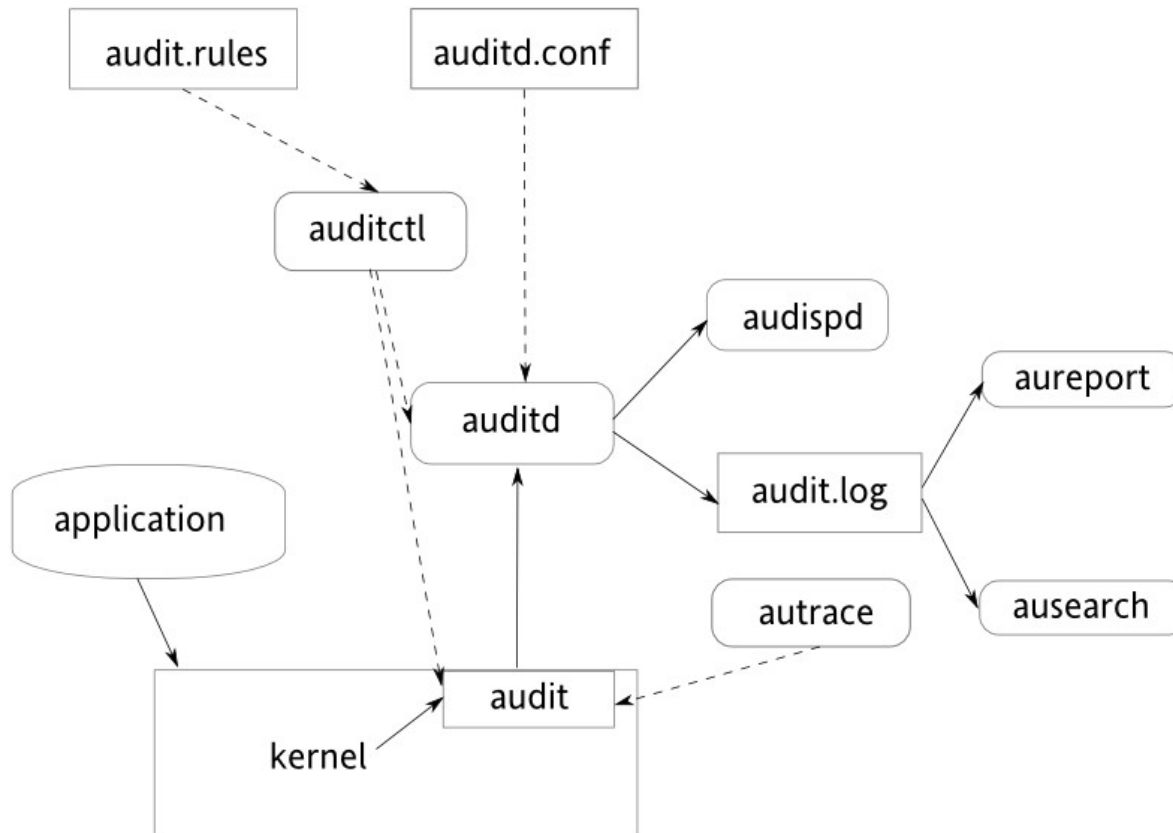
# NetIQ PAM – centralne „sudo”



# 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

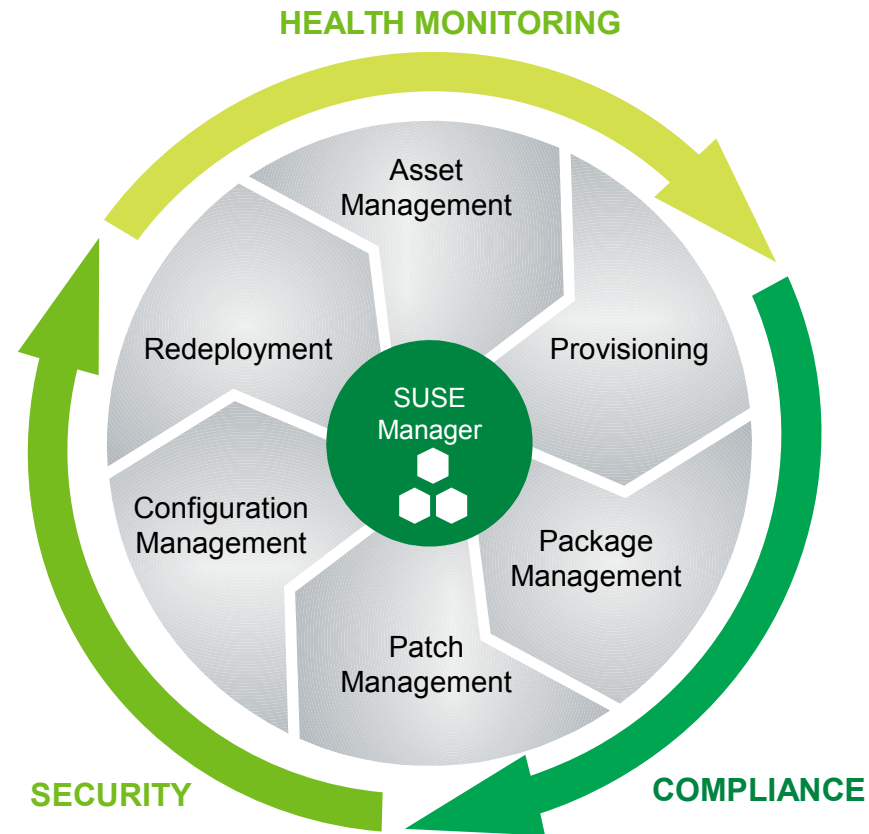
- Wdrażanie
- Zarządzanie pakietami, poprawkami
- Ponowna instalacja

## ✓ Kontrola

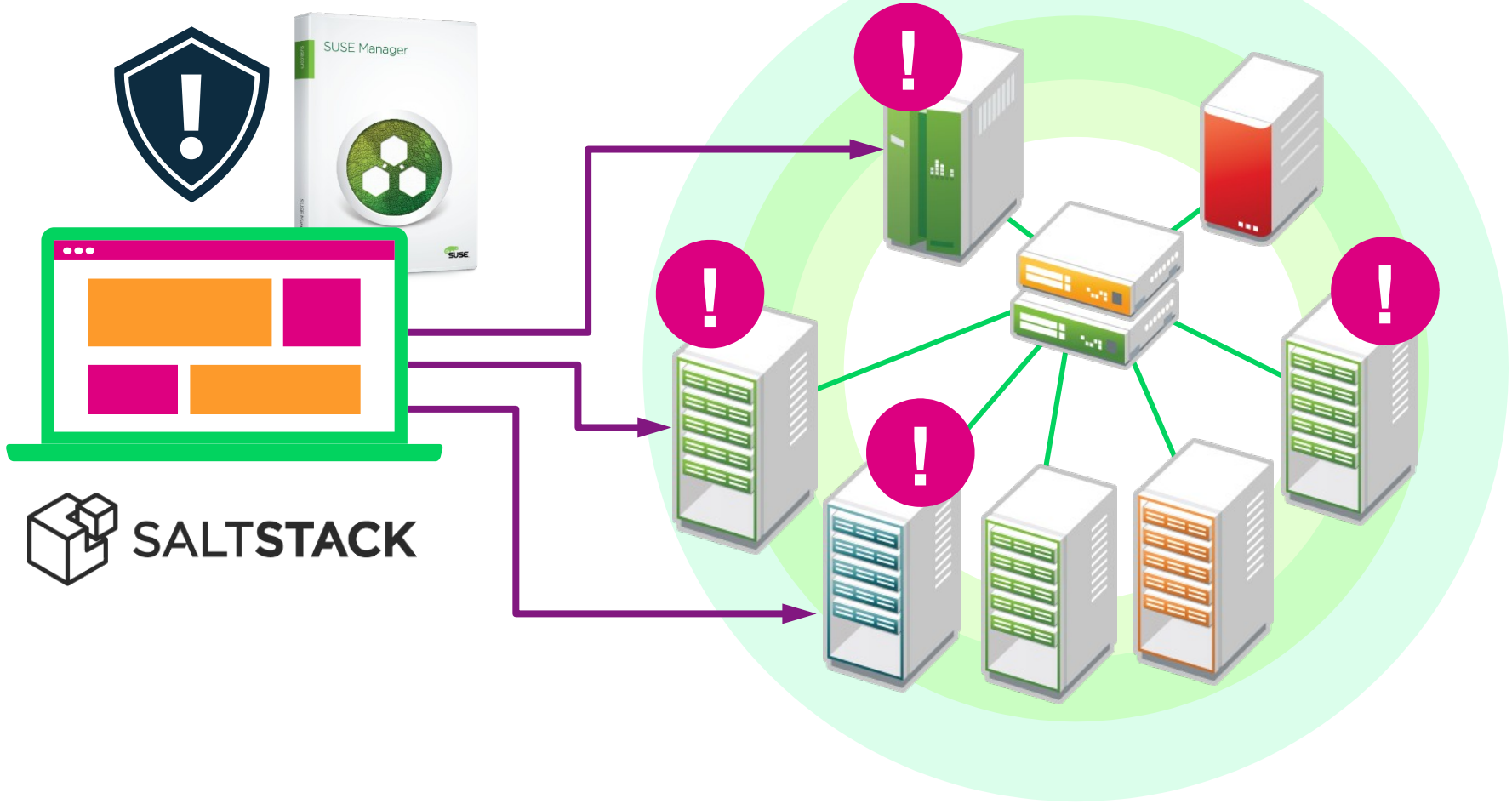
- Audyt systemów
- Raporty

## ✓ 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  
włamaniań**

# 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>

```
SLES:/ # chkrootkit
ROOTDIR is '/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `find'... not infected
```



# SIEM – NetIQ Sentinel

Q \* Search ...

Q ((((((failed) NOT (evt:"RulePerformanceSummary"))) NOT (evt:"EventSearch"))) NOT (evt:"syslog-ng: Conne ... Search

Whenever Data sources (1)

Select all Clear all Event operations...

Displaying 5 of 5 events.

**Refine**

Field counts based on the first 5 events.

Fields Clear

- CollectorNodeName (1)
- EventName (3)
- InitiatorUserName (1)
- ObserverCategory (2)
- Severity (2)
- SourceIP (1)
- TargetHostDomain (1)
- TargetHostName (1)
- TargetIP (1)
- Vulnerability (1)
- VDASOutcomeName (1)

4	10:51:16	<b>IssueSAMLToken-*Failed</b> (Security Event Management : Internal)	2016-05-07	User Session Events > Create > Failure	default
	172.28.50.2	admin2		Message: Failed to issue SAML authorization token for user admin2: Authentication failed	sentinel (172.28.4.1)
4	10:51:04	<b>IssueSAMLToken-*Failed</b> (Security Event Management : Internal)	2016-05-07	User Session Events > Create > Failure	default
	172.28.50.2	admin2		Message: Failed to issue SAML authorization token for user admin2: Authentication failed	sentinel (172.28.4.1)
1	10:41:34	<b>NetIQ Universal Event dhcpd Event</b> (Event source not in other category : NetIQ Universal Event)	2016-05-07	Message: dhcpd: receive_packet failed on eth1: Network is down	default
1	19:14:31	<b>NetIQ Universal Event dhcpd Event</b> (Event source not in other category : NetIQ Universal Event)	2016-05-06		default

# 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](http://www.suse.com)

Join us on:  
[www.opensuse.org](http://www.opensuse.org)

## **Unpublished Work of SUSE LLC. All Rights Reserved.**

This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE LLC. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

## **General Disclaimer**

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

