Einrichten von SELinux

In den meinsten Foren steht wenn es Probleme mit den Firewalls und SELinux auf den Systemen gibt "abschalten"

Da kräuseln sich mir als Administrator immer die Nackenhaare.

Die Systeme werden mit diesen Tools ausgeliefert damit Linux sicherer wird und nicht damit man die Sicherheit einfach ausschaltet.

Aktuellen SELinux Status abfragen:

root # **getenforce**

Enforcing

oder:

root # **sestatus**

SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28

Ein- und Ausschalten von SELinux

Um ziwschen enforcing und permissive zu wechseln, wird der Befehl **setenforce** verwendet.

Enofrcing einschalten:

root # **setenforce 1**
Enforcing

root # **setenforce 0**
Permissive Dauerhafte Konfiguration:

Die Standardkonfiguration von SELinux ist in der /etc/selinux/config einzustellen

cat /etc/selinux/config # This file controls the state of SELinux on the system on boot. # SELINUX can take one of these three values:

```
#       enforcing - SELinux security policy is enforced.

#       permissive - SELinux prints warnings instead of enforcing.

#       disabled - No SELinux policy is loaded.

SELINUX=enforcing


# SELINUXTYPE can take one of these four values:

#       targeted - Only targeted network daemons are protected.

#       strict   - Full SELinux protection.

#       mls      - Full SELinux protection with Multi-Level Security

#       mcs      - Full SELinux protection with Multi-Category Security

#                  (mls, but only one sensitivity level)

SELINUXTYPE=strict
```

Vollständige Deaktivierung

Vorsicht: Nachdem SELinux abgeschaltet wurde, werden veränderte oder neu angelegte Dateien nicht mehr
mit dem entsprechenden SELinux Kontext versehen.
Dies hat zur Folge, dass wenn SELinux wieder eingeschaltet wird, SELinux diese Dateien nicht lesen/laden wird.
Eine vollständige Rekonfiguration der betroffenen Dateien wäre dann die Folge, sobald SELinux wieder reaktiviert werden soll.

Pfad: /boot/grub/grub.conf.

```
default 0  timeout 3    title RedHat Hardened (SELinux disabled)  root (hd0,0)  kernel /kernel
```

root=/dev/md3 real_rootflags=data=journal selinux=0 dolvm domdadm rootfstype=ext4 devtmpfs.mount=0

initrd /initramfs

Deaktivierung von SELinux: selinux=0

Persistente Kontextänderungen

Hinzufügen

Um persistente Kontextänderungen vornehmen zu können, wird der Befehl **semanage fcontext** verwendet .
Die Option -a fügt einen neuen Kontext hinzu, während -t einen Typ definiert.

semanage fcontext -a -t httpd_sys_rw_content_t "/var/www/webserver_dateien(/.*)?" **Anzeigen der local definierten SELinux File contexts**

[root@server web-logs]# semanage fcontext --list -C SELinux fcontext type Context /usr/sbin/httpd-scl-wrapper all files system_u:object_r:httpd_exec_t:s0

SELinux Local fcontext Equivalence

/opt/rh/rh-php56/root = /

/opt/rh/httpd24/root = /

/usr/lib/systemd/system/rh-php56-php-fpm.service = /usr/lib/systemd/system/php-fpm.service

/var/log/httpd24 = /var/log/httpd

/var/opt/rh/rh-php56 = /var

/etc/opt/rh/rh-php56 = /etc

Viel Spass beim Ausprobieren.

Euer Admin