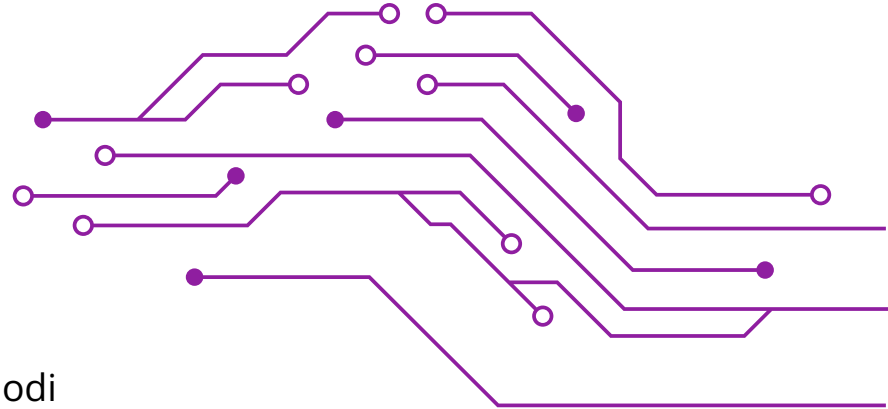
Agile Penguin

SELinux – Basics



Einführung in das Rechtekonzept, die Sicherheitsmodi und -konfigurationen

20.11.2024 | Jona Sander

Einführung in SELinux

Bedeutung:
Security Enhanced Linux (SELinux)
(Eine Sicherheitsarchitektur für Linux-Systeme)

Entwickelt von der NSA um Sicherheitsrichtlinien für die Zugriffskontrolle von Linux-Installationen zu schaffen

Installation:
Standardmäßig in RHEL integriert. Kann bei anderen Linux-Distributionen nachinstalliert werden.

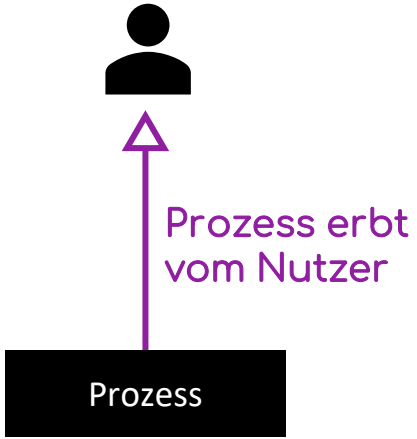
Rechtekonzept unter Linux

Discretionary Access Control (DAC)

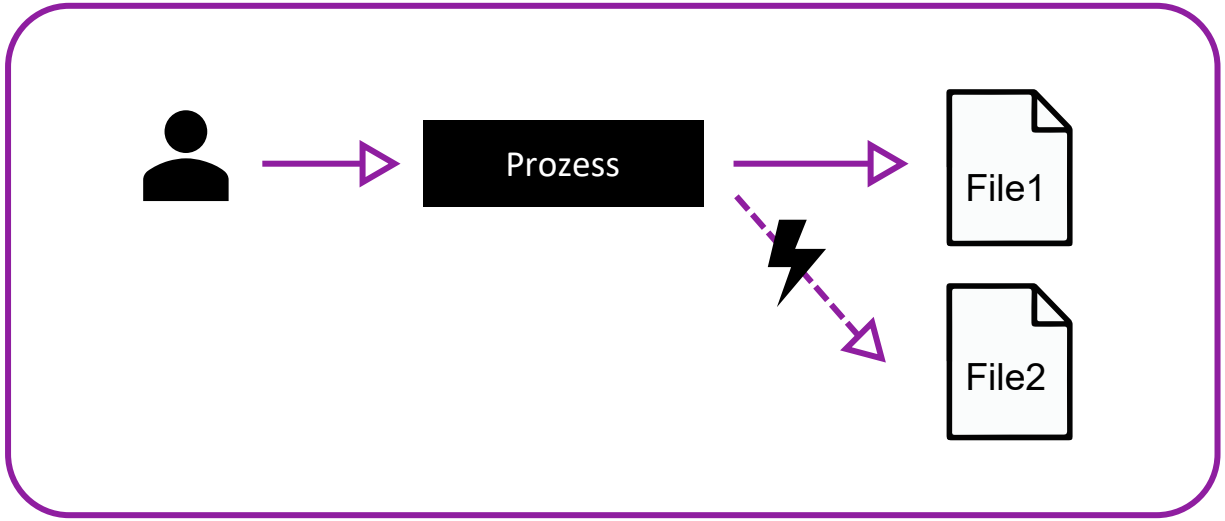
- owner, group, others

Kernprinzipien:

- Rechte basieren auf Nutzern, Gruppen und Berechtigungen.
- Prozesse erben die Rechte des Nutzers, der sie startet.



Rechtekonzept unter Linux



SELinux Rechtekonzept

Mandatory Access Control (MAC)

Nicht durch Ownership:
Zugriffskontrolle basiert **nicht** auf herkömmlichen Dateibesitz-Konzepten

Unveränderlich:
Sicherheitsrichtlinien sind **„in Stein gemeißelt“** für jede einzelne Datei

Arbeitet mit Labels:
Jede Datei und Ressource wird mit **Labels** versehen, die die Zugriffsbeschränkungen definieren

Losgelöst von DAC:
Funktioniert unabhängig vom traditionellen **Discretionary Access Control (DAC)**-Modell

Rechtekonzept und SELinux

Die meisten System-Prozesse werden von root gestartet
(da Netzwerkports, Systemdateien etc verwendet werden)

Szenario

Upload einer schadhaften Software durch User
- Hijacking des System Prozesses
- SW hätte Zugriff auf alles

Abhilfe: SELinux auf Fileebene

SELinux Modi

1. **Enforcing (an):**
   SELinux ist aktiv und erzwingt die definierten Richtlinien.

2. **Permissive (nur Logging):**
   SELinux blockiert keine Aktionen, aber protokolliert Verstöße.

3. **Disabled (aus):**
   SELinux ist vollständig deaktiviert.

SELinux Operating Policies

Strict	Alle Aktivitäten unterliegen den Einschränkungen von SELinux
Targeted	Policy greift nur für ausgewählte Prozesse, wie beispielsweise httpd, named etc.

SELinux Status Shell

sestatus

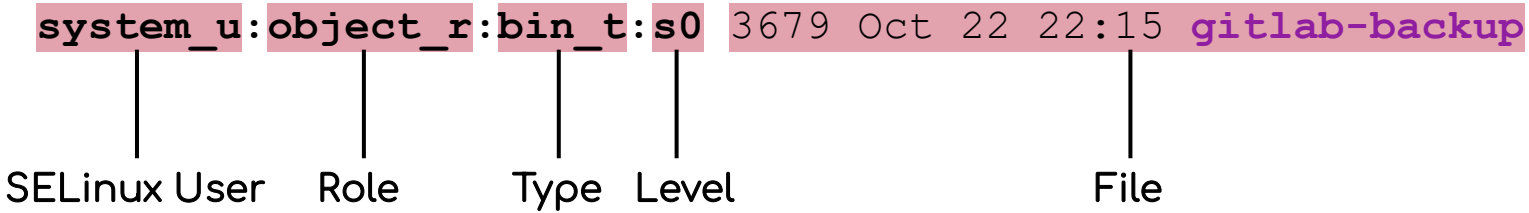
```
# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

SELinux Security Context

ls -Z

```
$ ls -laZ /opt/gitlab/bin/
total 44
drwxr-xr-x.  2 root root system_u:object_r:bin_t:s0 4096 Nov  4 19:12 .
drwxr-xr-x. 11 root root system_u:object_r:usr_t:s0 4096 Nov  4 19:12 ..
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 3679 Oct 22 22:15 gitlab-backup
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0  703 Oct 22 22:15 gitlab-backup-cli
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 1418 Oct 22 22:15 gitlab-ctl
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0  261 Oct 22 22:15 gitlab-healthcheck
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0  702 Oct 22 22:15 gitlab-psql
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 1450 Oct 22 22:15 gitlab-rails
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 1449 Oct 22 22:15 gitlab-rake
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 1311 Oct 22 22:15 gitlab-redis-cli
-rwxr-xr-x.  1 root root system_u:object_r:bin_t:s0 1449 Oct 22 22:15 gitlab-ruby
```

SELinux Security Context



Benutzer (User) – wem ist der Prozess / das Objekt zugeordnet?

Rolle (Role) – Welche Berechtigung hat er/es?

Typ (Type) – Welche Aktion ist erlaubt?

Level (Level) – Kritikalität bzw Sicherheitsstufe?

SELinux Security Context

chcon (setzt Context **temporär** um, mit versch. Parametern kann Typ, User, etc umgesetzt werden)

restorecon (zurücksetzen)

```
$ ls -lZ
-rw-r--r--. 1 jona jona unconfined_u:object_r:user_home_t:s0 18 Nov 16 16:46 test.txt

$ chcon -t httpd_sys_content_t test.txt

$ ls -lZ
-rw-r--r--. 1 jona jona unconfined_u:object_r:httpd_sys_content_t:s0 18 Nov 16 16:46
test.txt

$ restorecon test.txt
$ ls -lZ
total 4
-rw-r--r--. 1 jona jona unconfined_u:object_r:user_home_t:s0 18 Nov 16 16:46 test.txt
```

SELinux Security Context

Persistentes Umsetzen wird mit **semanage** vorgenommen

restorecon (bestätigen)

```
$ ls -lZ
-rw-r--r--. 1 jona jona unconfined_u:object_r:user_home_t:s0 18 Nov 16 16:46 test.txt

$ sudo semanage fcontext -a -t httpd_sys_content_t /home/jona/Documents/test.txt
$ restorecon test.txt

$ ls -lZ
-rw-r--r--. 1 jona jona unconfined_u:object_r:httpd_sys_content_t:s0 18 Nov 16 16:46
test.txt
```

Wichtig: der komplette Pfad muss angegeben werden!

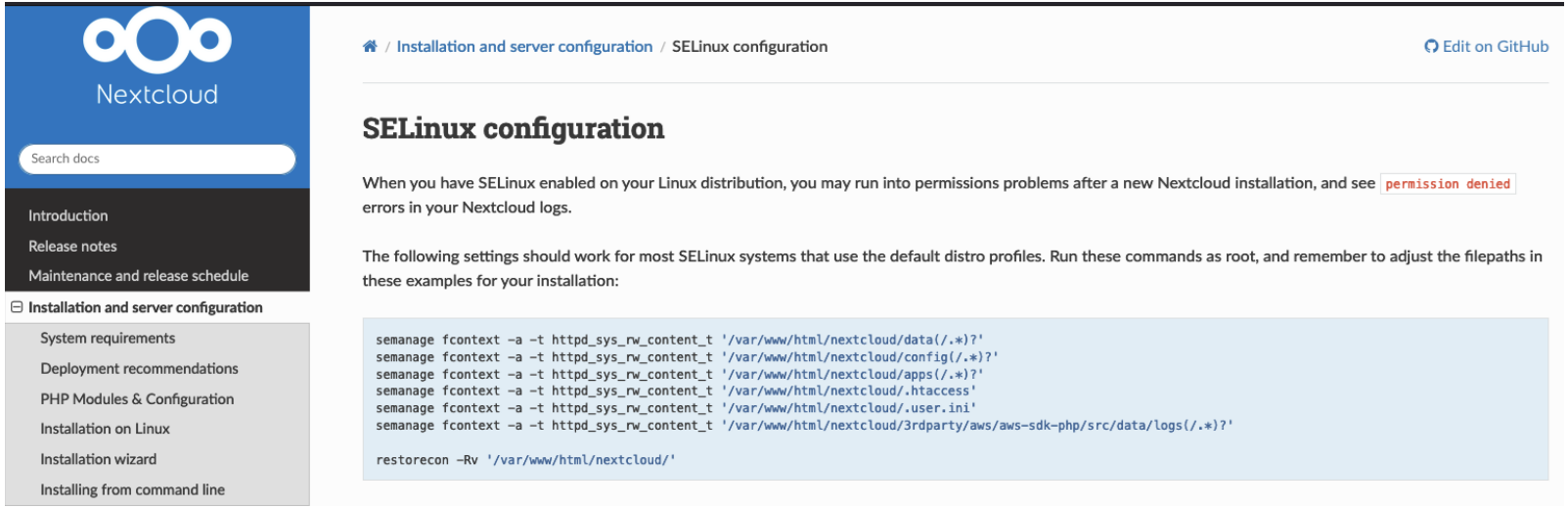
Konfigurationsoptionen

Vordefinierte Optionen um Sicherheitsrichtlinien ein- oder auszuschalten

```
setsebool [OPTIONEN] BOOLEAN-WERT
```

Eine Liste aller möglichen Optionen erhält man mit `getsebool -a`

Beispiel Nextcloud



https://docs.nextcloud.com/server/latest/admin_manual/installation/selinux_configuration.html

SELinux vs Firewall

- SELinux ist ein Mandatory Access Control (MAC)-System, das den Zugriff auf Ressourcen wie Dateien, Prozesse und Netzwerkverbindungen anhand vordefinierter Sicherheitsrichtlinien steuert.
- Es definiert, welche Prozesse auf welche Ressourcen zugreifen dürfen, basierend auf Benutzerrollen, Typen und Sicherheitskontexten.
- Es schützt vor unautorisierten Zugriffen und Sicherheitsverletzungen innerhalb des Systems.

- Eine Firewall ist ein Netzwerk-Sicherheitsgerät oder Software, das den ein- und ausgehenden Datenverkehr überwacht und basierend auf Regeln wie IP-Adressen, Ports und Protokollen kontrolliert.
- Sie blockiert unerwünschten Datenverkehr und schützt das Netzwerk vor externen Bedrohungen.

Logs

Logfiles: SELinux protokolliert Verstöße in /var/log/audit/audit.log.

audit2why und audit2allow:
Tools zur Analyse von Protokollen und Erzeugung von Erlaubnissen, wenn eine Aktion blockiert wird.

DANKE FÜR DIE AUFMERKSAMKEIT