SELinux - Richtlinien Konfigurieren

SELinux Dokumentation

SELinux man pages

- SELinux-Module werden mit (automatisch generierten) `man`-Pages ausgeliefert
- Diese Manpages sind auf einem Red Hat/CentOS-System nicht standardmäßig installiert
- Sie können aus den SELinux-Richtlinienquellen hinzugefügt werden

```
# dnf install -y selinux-policy-devel
# sepolicy manpage -a -p /usr/share/man/man8
```

SELinux man pages

- Während das SELinux-Modul `bind` genannt wird, heißt die Manpage `named_selinux`.
  - Diese Manpage dokumentiert die `named process types`, die neben BIND 9 auch für den Unbound-Resolver verwendet werden:

```
# man named_selinux
```

SELinux Module

SELinux Module ausschalten

- SELinux Module können selektiv deaktiviert/aktiviert werden
- Um nur das BIND 9 SELinux-Modul zu deaktivieren

```
# semodule -d bind
```

SEModule anschalten

- Um das BIND 9 SELinux-Modul zu aktivieren

```
# semodule -ve bind
Attempting to enable module 'bind':
Ok: return value of 0.
Committing changes:
Ok: transaction number 6.
```

SELinux Fehlkonfigurationen finden

Reports des Linux Audit Subsystem

- Verstöße gegen SELinux-Richtlinien werden mit dem Linux Audit Subsystem protokolliert
- Mit dem Kommando `ausearch` können Sie die Richtlinienverletzungen eines bestimmten Prozesses auflisten
  - `-m avc` listet LSM-Richtlinienverstöße auf
  - `-x /usr/sbin/named` filtert nach Verstößen dieses Prozesses
  - `-i` (interpretieren) gibt die Daten in lesbarer Form aus

Nicht übereinstimmende Dateitypkennzeichnung

- Das SELinux-System verweigert Prozessen den Zugriff auf Daten- oder Konfigurationsdateien, wenn die Dateilabel nicht korrekt sind
- Gründe für falsche oder fehlende Dateilabel
    - Das Linux-System wurde mit deaktiviertem SELinux betrieben
    - Die Dateien befinden sich in einem nicht standardmäßigen Verzeichnis (z.B. nicht in `/etc` oder `/var/named`)
    - Die Dateien wurden in einem nicht standardmäßigen Verzeichnis erstellt und dann in das richtige Verzeichnis verschoben. Die Datei-Bezeichnungen werden bei der Erstellung einer Datei zugewiesen und ändern sich nicht, wenn sie innerhalb des gleichen Dateisystem verschoben werden.

SELinux Label anzeigen (1/2)

- SELinux Sicherheits-Kontext (Label) auf einer Datei anzeigen

```
# secon --file /etc/shadow
user: system_u
role: object_r
type: shadow_t
sensitivity: s0
clearance: s0
mls-range: s0
```

SELinux Label anzeigen (2/2)

- Sicherheitskontext auf einem Prozess anzeigen

```
# secon --pid $(pgrep dbus)
user: system_u
role: system_r
type: system_dbusd_t
sensitivity: s0
clearance: s0:c0.c1023
mls-range: s0-s0:c0.c1023
```

Das richtige SELinux Label finden

- Der Befehl **`matchpathcon`** (Match Path Context) meldet Dateien, bei denen das Dateilabel nicht mit der SELinux-Richtlinie übereinstimmen
    - Der Befehl meldet auch die erwarteten Dateilabel-Typen

```
# matchpathcon -V /var/named/named.localhost
/var/named/named.localhost has context system_u:object_r:etc_t:s0,
                           should be system_u:object_r:named_zonefile
```

Ändern des Dateilabels

- Der Befehl **chcon** (change SELinux context) kann verwendet werden, um den Typ des Dateilabel zu ändern:

```
# chcon --type named_cache_t /var/named/zonefile.db
```

Anwenden des korrekten Label aus der Richtlinie

- Der Befehl **`restorecon`** passt das Label einer Datei so an, dass es mit dem von der SELinux-Richtlinie erwarteten Label übereinstimmt

```
# restorecon -v /var/named/named.localhost
Relabeled /var/named/named.localhost ...
       from system_u:object_r:etc_t:s0 ...
       to system_u:object_r:named_zone_t:s0
```

Anpassen des erwarteten Dateikontextes für eine einzelne Datei

- Wenn Konfigurations- oder Datendateien an einem nicht standardmäßigen Speicherort abgelegt sind, sollte die SELinux-Richtlinie angepasst werden, um das richtige Kontextlabel zuzuordnen
- Der Befehl `semanage fcontext -a` fügt einen Dateikontext Label zur SELinux-Richtlinie hinzu.

Anpassen des erwarteten Dateikontextes für eine einzelne Datei

- Die Dateien werden nicht automatisch neu gekennzeichnet. Verwenden Sie `restrorecon`, um die Dateien neu zu kennzeichnen.

```
# semanage fcontext -a -t named_zone_t /srv/bind/zones/primary/example.com.db
# restorecon -vr /srv/bind/zones
Relabeled /srv/bind/zones/primary/example.com.db
        from unconfined_u:object_r:var_t:s0
        to unconfined_u:object_r:named_zone_t:s0
```

Rekursives Anpassen des Dateikontextes für alle Dateien und Verzeichnisse

- Ein neuer SELinux-Dateikontext kann rekursiv zu einem Verzeichnis hinzugefügt werden
    - Alle neuen Dateien, die in den angegebenen Verzeichnissen erstellt werden, erhalten automatisch das richtige SELinux-Dateilabel

```
# semanage fcontext -a -t named_zone_t --ftype f "/srv/bind/zones(/.*)?"
# semanage fcontext -a -t named_zone_t --ftype d "/srv/bind/zones(/.*)?"
# semanage fcontext -a -t named_cont_t --ftype f "/srv/bind/conf(/.*)?"
# semanage fcontext -a -t named_conf_t --ftype d "/srv/bind/conf(/.*)?"
```

Dateikontext automatisch anpassen

- Der Hintergrundprozess `restorecond` kann optional installiert und gestartet werden (Paket `policycoreutils-restorecond`), um Dateilabel von neu angelegten Dateien automatisch an die SELinux-Policy anzupassen
  - Je nach Einsatzbereich kann `restorecond` die Sicherheit beeinträchtigen, da SELinux-Label auf Dateien automatisch *korrigiert* werden
  - Die Datei `/etc/selinux/restorecond.conf` listed die Dateien und Verzeichnisse auf, welche von `restorecond` automatisch überwacht und berichtigt werden sollen

SELinux Richtlinien Konfigurieren

SELinux Richtlinien Schalter

- Viele SELinux Module bieten Konfigurations-Optionen an
- Über SELinux *Booleans* (Schalter) können Funktionen von Richtlinien-Modulen an- bzw. ausgeschaltet werden

SELinux Richtlinien Schalter

- Eine Liste alle SELinux Boolean-Schalter kann durch `semanage boolean -l` abgerufen werden

```
SELinux boolean                State  Default Description
abrt_anon_write                (off  ,  off)  Allow ABRT to modify public files used ...
abrt_handle_event              (off  ,  off)  Determine whether ABRT can run in the ...
antivirus_can_scan_system      (off  ,  off)  Allow antivirus programs to read non ...
antivirus_use_jit              (off  ,  off)  Determine whether antivirus programs ...
```

SELinux Schalter

- Der Befehl `getsebool` ist eine alternative Schnittstelle zu den SELinux Schaltern

```
# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
[...]
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[...]
```

SELinux Schalter

- Mit dem Befehl `semanage boolean -l --locallist` wird eine übersicht der lokalen Schalter-Anpassungen ausgegeben

```
# semanage boolean -l --locallist
SELinux boolean                State  Default Description
named_write_master_zones       (on   ,   on)  Determine whether Bind can write [...]
```

SELinux Schalter ausschalten

- Beispiel des Ausschalten eines SELinux Schalters

```
# semanage boolean --modify --off named_write_master_zones
```

Alternativ: setsebool

- Als Alternative zu `semanage boolean` kann der Befehl `setsebool` verwendet werden

```
setsebool named_write_master_zones off
```

- Um eine Änderung dauerhaft (persistent) im System zu ändern (Reboot-Fest), muss der Schalter `-P` angegeben werden

```
setsebool -P named_write_master_zones off
```

SELinux Schalter

- Bei der Neu-Installation von Software auf einem SELinux System ist es sinnvoll sich mit den SELinux Schaltern für diese Software vertraut zu machen

SELinux Netzwerk-Ports

SELinux Netzwerk-Ports und -Anwendungen

- Die SELinux Policy erlaubt Anwendungen (oder SELinux Type-Label) die Benutzung bestimmter UDP/TCP Netzwerkports
  - Versucht die Anwendung, einen anderen Port zu öffnen, so wird dies durch SELinux unterbunden
  - Beispiele: Webserver, SSH-Server, DNS-Server auf Nicht-Standard-Ports

SELinux Netzwerk-Ports und -Anwendungen

- Der Befehl `semanage port -l` listet alle Port-Definitionen pro SELinux Type-Label auf
    - Diese Liste ist lang und umfasst alle Module, nicht nur die *aktiven* SELinux Module. Benutze `grep` um die Port-Konfiguration für einen SELinux-Typ zu sehen

```
# semanage port -l | grep ssh
ssh_port_t                     tcp      22
```

SELinux Netzwerk-Ports und -Anwendungen

- Um einen Netzwerk-Dienst auf einem *nicht-standard* Port unter SELinux betreiben zu können, muss dieser Port dem SELinux-Type hinzugefügt werden:

```
# semanage port -a -t ssh_port_t -p tcp 4422
# semanage port -l | grep ssh
ssh_port_t                     tcp      22,4422
```

Durchsetzung der Richtlinie für Module ausschalten

Durchsetzung auf SELinux Module aufheben

- Es ist möglich einzelne SELinux Module in einen *permissive* Modus zu versetzten
    - In diesem Modus wird die SELinux Policy für dieses Modul nicht mehr vom Kernel durchgesetzt
    - Verstösse gegen die Policy werden jedoch weiterhin im Audit-Log protokolliert

Durchsetzung auf SELinux Module aufheben

- Ein Modul (hier `httpd_t` für Apache oder NGINX Webserver) in den *permissive* Modus setzen

```
semanage permissive -a httpd_t
```

Durchsetzung auf SELinux Module aufheben

- Alle Module auflisten, welche im *permissive* Modus laufen

```
# semanage permissive -l
```

Durchsetzung auf SELinux Module aufheben

- Permissive Modus von einem Modul entfernen

```
semanage permissive -d httpd_t
```

- Permissive Modus von **allen** Modulen entfernen

```
semanage permissive -D
```

FIN

- Ende des Kapitels "SELinux Richtlinien Konfigurieren"

Created in Master PDF Editor