Конфигурация SELinux

Введение

SELinux (Security-Enhanced Linux) — это набор изменений для ядра Linux и утилит, который реализует поддержку политики контроля доступа. SELinux предоставляет механизм для поддержки изоляции процессов и ограничения доступа к файлам и системным ресурсам на основе установленных правил политики безопасности. В данной документации мы рассмотрим основы работы с SELinux в операционной системе НАЙС ОС, включая установку, настройку и управление политиками.

SELinux может работать в одном из трех режимов: enforcing (принудительный), permissive (разрешающий) и disabled (отключен). В режиме enforcing все правила политики безопасности применяются, а действия, нарушающие политику, блокируются. В режиме permissive нарушения политики логируются, но не блокируются. Режим disabled полностью отключает SELinux. Мы рассмотрим, как переключаться между этими режимами, а также как создавать и управлять политиками SELinux.

Установка и настройка SELinux

Для начала работы с SELinux в НАЙС ОС необходимо установить необходимые пакеты и включить SELinux.

Установка пакетов SELinux

Используйте `dnf` для установки пакетов SELinux:

```
sudo dnf install selinux-policy selinux-policy-targeted policycoreutils
setroubleshoot
```

Проверка состояния SELinux

Используйте команду `sestatus` для проверки текущего состояния SELinux:

```
sestatus
```

Включение и выключение SELinux

Для изменения режима работы SELinux отредактируйте файл `/etc/selinux/config`:

```
sudo nano /etc/selinux/config
```

Измените строку `SELINUX` на одно из следующих значений:

- `SELINUX=enforcing` — включить принудительный режим
- `SELINUX=permissive` — включить разрешающий режим
- `SELINUX=disabled` — отключить SELinux

Для применения изменений перезагрузите систему:

```
sudo reboot
```

Основные команды SELinux

Существует несколько основных команд для управления и диагностики SELinux.

Команда getenforce

Команда `getenforce` используется для проверки текущего режима SELinux:

```
getenforce
```

Команда setenforce

Команда `setenforce` используется для временного переключения между режимами enforcing и permissive без перезагрузки:

```
sudo setenforce 1 # Включить enforcing
sudo setenforce 0 # Включить permissive
```

Команда semanage

Команда `semanage` используется для управления SELinux политиками, включая изменение контекстов файлов и управление портами.

Изменение контекста файла

```
sudo semanage fcontext -a -t httpd_sys_content_t "/var/www/html(/.*)?"
```

Применение изменений контекста

```
sudo restorecon -R /var/www/html
```

Управление портами

```
sudo semanage port -a -t http_port_t -p tcp 8080
```

Контексты SELinux

Каждый файл, процесс и порт в системе имеют контекст SELinux, который определяет права доступа. Контексты состоят из нескольких полей, таких как пользователь, роль, тип и уровень (если используется MLS).

Просмотр контекста файлов

Для просмотра контекста файлов используйте команду `ls -Z`:

```
ls -Z /path/to/directory
```

Просмотр контекста процессов

Для просмотра контекста процессов используйте команду `ps -eZ`:

```
ps -eZ | grep process_name
```

Изменение контекста файлов

Для изменения контекста файлов используйте команду `chcon`:

```
sudo chcon -t httpd_sys_content_t /var/www/html/index.html
```

Управление политиками SELinux

Политики SELinux определяют, какие действия могут выполнять процессы и пользователи. Существует несколько видов политик: targeted, strict и mls. Наиболее часто используется политика `targeted`, которая применяет правила безопасности к определенным демонам и процессам.

Активация политики

Для активации политики SELinux используйте команду `semanage`:

```
sudo semanage policy -a my_policy
```

Просмотр активных политик

Для просмотра списка активных политик используйте команду `semanage`:

```
sudo semanage policy -l
```

Создание пользовательской политики

Для создания пользовательской политики сначала создайте файл с определением политики. Например, создайте файл `my_policy.te`:

```
nano my_policy.te
```

Добавьте в файл следующее содержимое:

```
module my_policy 1.0;

require {
    type httpd_t;
    type httpd_sys_content_t;
    class file { read write };
}

# Разрешить httpd_t читать и писать в httpd_sys_content_t
allow httpd_t httpd_sys_content_t:file { read write };
```

Скомпилируйте и загрузите политику:

```
checkmodule -M -m -o my_policy.mod my_policy.te
semodule_package -o my_policy.pp -m my_policy.mod
sudo semodule -i my_policy.pp
```

Устранение проблем с SELinux

Иногда SELinux может блокировать легитимные действия, что требует диагностики и устранения проблем. Для этого используются инструменты `auditd` и `sealert`.

Установка и настройка auditd

Установите `auditd` для журналирования событий SELinux:

```
sudo dnf install audit
sudo systemctl start auditd
sudo systemctl enable auditd
```

Просмотр журналов аудита

Журналы аудита можно просматривать с помощью команды `ausearch`:

```
sudo ausearch -m avc
```

Использование sealert для анализа проблем

Утилита `sealert` помогает анализировать сообщения об ошибках SELinux и предлагает рекомендации по их устранению.

Анализ журналов аудита

```
sudo sealert -a /var/log/audit/audit.log
```

Использование booleans в SELinux

Booleans в SELinux позволяют включать и выключать определенные функции политики безопасности без необходимости перезагрузки системы или пересборки политики.

Просмотр доступных booleans

Для просмотра списка доступных booleans используйте команду `getsebool`:

```
sudo getsebool -a
```

Изменение значения boolean

Для изменения значения boolean используйте команду `setsebool`:

```
sudo setsebool httpd_can_network_connect on
```

Постоянное изменение значения boolean

Для постоянного изменения значения boolean используйте опцию `-P`:

```
sudo setsebool -P httpd_can_network_connect on
```

Использование SELinux в Docker контейнерах

SELinux может использоваться для повышения безопасности Docker контейнеров, изолируя их от хоста и других контейнеров.

Включение поддержки SELinux в Docker

Убедитесь, что Docker установлен с поддержкой SELinux. Если нет, установите Docker с соответствующей опцией:

```
sudo dnf install docker
sudo systemctl start docker
sudo systemctl enable docker
```

Запуск контейнеров с поддержкой SELinux

Для запуска контейнера с поддержкой SELinux используйте опцию `--security-opt`:

```
sudo docker run --security-opt label=type:svirt_lxc_net_t -it centos /bin/bash
```

Управление контекстами SELinux в Docker

Используйте команду `chcon` для изменения контекста файлов и директорий, используемых контейнерами:

```
sudo chcon -Rt svirt_sandbox_file_t /path/to/dir
```

Заключение

Конфигурация и управление SELinux в НАЙС ОС обеспечивает высокую степень безопасности системы, контролируя доступ к ресурсам и изолируя процессы. Используя инструменты и методы, описанные в данной документации, вы сможете эффективно настроить и управлять SELinux, обеспечивая надежную защиту вашей системы. Следование приведенным рекомендациям поможет предотвратить несанкционированный доступ и сохранить целостность данных.