Управление политиками безопасности

Введение

Политики безопасности играют ключевую роль в обеспечении защищенности операционной системы и данных. Они определяют, какие действия могут выполняться пользователями и процессами, и устанавливают ограничения для предотвращения несанкционированного доступа и атак. В операционной системе НАЙС ОС управление политиками безопасности осуществляется с помощью различных инструментов, таких как SELinux, AppArmor, а также настройки групповых политик и управления пользователями. В данной документации мы рассмотрим основные методы и инструменты для управления политиками безопасности в НАЙС ОС.

Использование SELinux для управления политиками безопасности

SELinux (Security-Enhanced Linux) — это система управления политиками безопасности, которая позволяет ограничивать действия процессов и пользователей на основе настроек политики. Она использует контексты безопасности для определения прав доступа и выполняет контроль над действиями на уровне ядра операционной системы.

Установка и настройка SELinux

Для начала работы с SELinux 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
```

Включение SELinux

Откройте файл `/etc/selinux/config` для редактирования и установите режим работы SELinux:

```
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.

Проверка состояния SELinux

Используйте команду `sestatus` для проверки текущего состояния SELinux:

```
sestatus
```

Изменение режима работы SELinux

Используйте команду `setenforce` для временного переключения между режимами enforcing и permissive без перезагрузки:

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

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.

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
```

Использование AppArmor для управления политиками безопасности

AppArmor — это еще один инструмент для управления политиками безопасности в Linux. Он позволяет ограничивать действия приложений с помощью профилей, которые определяют разрешенные и запрещенные действия для каждого приложения.

Установка и настройка AppArmor

Для начала работы с AppArmor необходимо установить необходимые пакеты и включить AppArmor.

Установка пакетов AppArmor

Используйте `dnf` для установки пакетов AppArmor:

```
sudo dnf install apparmor apparmor-utils
```

Включение AppArmor

Откройте файл `/etc/default/grub` для редактирования и добавьте параметры загрузки ядра:

```
sudo nano /etc/default/grub
```

Измените строку `GRUB_CMDLINE_LINUX`, добавив `apparmor=1 security=apparmor`:

```
GRUB_CMDLINE_LINUX="... apparmor=1 security=apparmor"
```

Обновите конфигурацию GRUB и перезагрузите систему:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
sudo reboot
```

Основные команды AppArmor

Существует несколько основных команд для управления и диагностики AppArmor.

Проверка состояния AppArmor

Используйте команду `aa-status` для проверки текущего состояния AppArmor:

```
sudo aa-status
```

Управление профилями AppArmor

Используйте команду `aa-complain` для перевода профиля в режим обучения:

```
sudo aa-complain /etc/apparmor.d/usr.bin.apache2
```

Используйте команду `aa-enforce` для перевода профиля в принудительный режим:

```
sudo aa-enforce /etc/apparmor.d/usr.bin.apache2
```

Создание пользовательских профилей AppArmor

Для создания пользовательских профилей AppArmor выполните следующие шаги:

Создание нового профиля

Запустите `aa-genprof` для создания нового профиля:

```
sudo aa-genprof /usr/bin/myapp
```

Следуйте инструкциям на экране для настройки разрешений.

Редактирование профиля

Откройте созданный профиль для редактирования:

```
sudo nano /etc/apparmor.d/usr.bin.myapp
```

Добавьте или измените правила в профиле в соответствии с вашими требованиями.

Перезагрузка AppArmor

Перезагрузите службу AppArmor для применения изменений:

```
sudo systemctl restart apparmor
```

Настройка групповых политик и управления пользователями

Групповые политики и управление пользователями позволяют централизованно управлять правами доступа и настройками безопасности для групп пользователей.

Создание и управление пользователями

Для создания нового пользователя используйте команду `useradd`:

```
sudo useradd username
```

Для установки пароля пользователю используйте команду `passwd`:

```
sudo passwd username
```

Для изменения параметров пользователя, таких как домашний каталог или оболочка входа, используйте команду `usermod`:

```
sudo usermod -d /new/home/dir -s /bin/bash username
```

Создание и управление группами

Для создания новой группы используйте команду `groupadd`:

```
sudo groupadd groupname
```

Для добавления пользователя в группу используйте команду `usermod` с опцией `-aG`:

```
<

bash>
sudo usermod -aG groupname username
```

Для удаления пользователя из группы используйте команду `gpasswd`:

```
sudo gpasswd -d username groupname
```

Настройка прав доступа к файлам и директориям

Права доступа к файлам и директориям определяют, какие действия могут выполнять пользователи и группы с этими объектами. Основные команды для управления правами доступа включают `chmod`, `chown` и `chgrp`.

Изменение прав доступа с использованием команды chmod

Команда `chmod` используется для изменения прав доступа к файлам и директориям. Права доступа включают чтение (r), запись (w) и выполнение (x).

Пример команды для предоставления права выполнения владельцу файла:

```
chmod u+x filename
```

Пример команды для удаления права записи у группы:

```
chmod g-w filename
```

Изменение владельца файла с использованием команды chown

Команда `chown` используется для изменения владельца файла или директории.

Пример команды для изменения владельца файла:

```
sudo chown newowner filename
```

Для изменения владельца и группы используйте следующий синтаксис:

```
sudo chown newowner:newgroup filename
```

Изменение группы файла с использованием команды chgrp

Команда `chgrp` используется для изменения группы файла или директории.

Пример команды для изменения группы файла:

```
sudo chgrp newgroup filename
```

Использование sudo для управления правами доступа

Команда `sudo` позволяет выполнять команды от имени другого пользователя, обычно от имени суперпользователя (root). Настройка `sudo` позволяет контролировать, какие пользователи и группы могут выполнять определенные команды.

Настройка sudo

Для настройки `sudo` используйте команду `visudo`, которая открывает файл конфигурации `/etc/sudoers`:

```
sudo visudo
```

Добавьте следующие строки для предоставления пользователю `username` права выполнять все команды от имени суперпользователя:

```
username ALL=(ALL) ALL
```

Для предоставления группе `groupname` права выполнять определенные команды добавьте строку:

```
%groupname ALL=(ALL) /usr/bin/command
```

Журналирование и аудит событий безопасности

Журналирование и аудит событий безопасности позволяют отслеживать действия пользователей и процессов, выявлять подозрительные активности и проводить расследования инцидентов безопасности.

Настройка системы аудита

Для настройки системы аудита установите пакет `audit`:

```
sudo dnf install audit
```

Запустите и настройте автозапуск службы `auditd`:

```
sudo systemctl start auditd
sudo systemctl enable auditd
```

Настройка правил аудита

Для настройки правил аудита отредактируйте файл `/etc/audit/audit.rules`. Пример правила для аудита изменений файлов в директории `/etc`:

```
sudo nano /etc/audit/audit.rules
```

Добавьте строку:

```
-w /etc -p wa -k etc_changes
```

Просмотр журналов аудита

Для просмотра журналов аудита используйте команду `ausearch`:

```
sudo ausearch -k etc_changes
```

Использование SELinux для управления доступом к сетевым портам

SELinux позволяет управлять доступом к сетевым портам, ограничивая доступ к ним для определенных служб и процессов.

Просмотр текущих настроек портов

Используйте команду `semanage port -l` для просмотра текущих настроек портов:

```
sudo semanage port -l
```

Добавление нового правила для порта

Для добавления нового правила для порта используйте команду `semanage port -a`:

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

Удаление правила для порта

Для удаления правила для порта используйте команду `semanage port -d`:

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

Использование правил firewall для управления доступом

Firewall позволяет управлять доступом к сетевым ресурсам на уровне пакетов. В НАЙС ОС можно использовать `firewalld` или `iptables` для настройки правил firewall.

Установка и настройка firewalld

Для установки `firewalld` используйте `dnf`:

```
sudo dnf install firewalld
```

Запустите и настройте автозапуск службы `firewalld`:

```
sudo systemctl start firewalld
sudo systemctl enable firewalld
```

Основные команды firewalld

Для работы с `firewalld` используйте утилиту `firewall-cmd`. Вот некоторые основные команды:

Проверка состояния firewalld

```
sudo firewall-cmd --state
```

Добавление правила для разрешения сервиса

```
sudo firewall-cmd --zone=public --add-service=http --permanent
sudo firewall-cmd --reload
```

Удаление правила для сервиса

```
sudo firewall-cmd --zone=public --remove-service=http --permanent
sudo firewall-cmd --reload
```

Заключение

Управление политиками безопасности в НАЙС ОС — это важный аспект обеспечения защищенности системы и данных. Используя различные инструменты, такие как SELinux, AppArmor, групповые политики, sudo и firewall, вы можете эффективно контролировать доступ и предотвращать несанкционированные действия. Следование приведенным рекомендациям и примерам поможет вам настроить и управлять политиками безопасности в НАЙС ОС, обеспечивая высокий уровень защиты вашей системы.