Использование SELinux для обеспечения безопасности в НАЙС ОС

Введение

Security-Enhanced Linux (SELinux) - это система управления доступом, интегрированная в ядро Linux, которая обеспечивает дополнительный уровень безопасности путем применения политики контроля доступа. В данной документации рассмотрены установка, настройка и использование SELinux в контексте обеспечения безопасности в НАЙС ОС, а также примеры использования команд.

Установка SELinux

Для установки SELinux в НАЙС ОС используется пакетный менеджер `tdnf` или `dnf`. Воспользуйтесь следующими командами для установки необходимых пакетов:

```
$ sudo tdnf install selinux-policy selinux-policy-targeted
$ sudo tdnf install policycoreutils
```

Включение SELinux

После установки необходимо включить SELinux. Для этого нужно отредактировать файл конфигурации `/etc/selinux/config` и установить параметр `SELINUX=enforcing`:

```
$ sudo vi /etc/selinux/config
```

Измените содержимое файла следующим образом:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

После внесения изменений перезагрузите систему, чтобы SELinux вступил в силу:

```
$ sudo reboot
```

Режимы работы SELinux

SELinux может работать в трех режимах:

- **enforcing** - политики SELinux применяются, и доступ ограничивается в соответствии с ними.
- **permissive** - политики SELinux не применяются, но нарушения логируются.
- **disabled** - SELinux отключен.

Для изменения режима работы SELinux используется команда `setenforce`:

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

Проверка состояния SELinux

Для проверки текущего состояния SELinux используется команда `sestatus`:

```
$ sestatus
```

Управление контекстами безопасности

Каждый файл, процесс и объект в системе имеет свой контекст безопасности. Для просмотра контекста безопасности используется команда `ls -Z`:

```
$ ls -Z /path/to/file
```

Изменение контекста безопасности

Для изменения контекста безопасности файла или каталога используется команда `chcon`:

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

Эта команда изменяет тип контекста безопасности файла на `httpd_sys_content_t`, что необходимо для правильной работы веб-сервера.

Управление политиками SELinux

Политики SELinux определяют, какие действия разрешены или запрещены в системе. Для управления политиками используются утилиты `semanage`, `audit2allow` и `audit2why`.

Добавление и удаление правил

Для добавления пользовательских правил используется утилита `semanage`:

```
$ sudo semanage fcontext -a -t httpd_sys_content_t "/my/custom/path(/.*)?"
$ sudo restorecon -Rv /my/custom/path
```

Эта команда добавляет новое правило для контекста безопасности и применяет его к указанному пути.

Разрешение заблокированных действий

Для анализа и разрешения заблокированных действий используются утилиты `audit2allow` и

`audit2why`:

```
$ sudo ausearch -m avc -ts recent | audit2allow -M mypol
$ sudo semodule -i mypol.pp
```

Эти команды создают и применяют модуль политики, который разрешает ранее заблокированные действия.

Рекомендации по безопасности

- Всегда используйте `enforcing` режим для максимальной безопасности.
- Регулярно проверяйте логи SELinux для выявления и устранения проблем с доступом.
- Используйте утилиты `semanage`, `audit2allow` и `audit2why` для управления политиками и разрешения проблем.
- Не изменяйте контексты безопасности без необходимости и понимания последствий.

Заключение

SELinux предоставляет мощный и гибкий механизм управления доступом в НАЙС ОС. Следуя приведенным рекомендациям и примерам, вы сможете эффективно контролировать и защищать свою систему, обеспечивая высокий уровень безопасности.