Использование списков контроля доступа (ACL) для обеспечения безопасности в НАЙС ОС

Введение

Списки контроля доступа (Access Control Lists, ACL) позволяют более гибко управлять правами доступа к файлам и каталогам по сравнению с традиционной моделью Unix-подобных прав доступа. В данной документации рассмотрены установка, настройка и использование ACL в контексте обеспечения безопасности в НАЙС ОС, а также примеры использования команд.

Установка поддержки ACL

Для использования ACL в НАЙС ОС необходимо установить соответствующие утилиты. Используйте пакетный менеджер `tdnf` или `dnf` для установки:

```
$ sudo tdnf install acl
```

Проверка поддержки ACL файловой системой

Чтобы использовать ACL, файловая система должна поддерживать эту функциональность. Вы можете проверить, смонтирована ли файловая система с поддержкой ACL, с помощью команды:

```
$ mount | grep acl
```

Если ACL не включены, вы можете смонтировать файловую систему с поддержкой ACL, добавив опцию `acl` в `/etc/fstab` или с помощью команды `mount`:

```
$ sudo mount -o remount,acl /dev/sdXn /mount/point
```

Основные команды для работы с ACL

Для управления ACL используются команды `getfacl` и `setfacl`.

Просмотр текущих ACL

Для отображения текущих ACL файла или каталога используется команда `getfacl`:

```
$ getfacl /path/to/file
```

Эта команда выведет текущие ACL для указанного файла или каталога.

Установка ACL

Для установки ACL используется команда `setfacl`. Примеры установки различных типов прав доступа:

Добавление прав для пользователя

```
$ setfacl -m u:username:rwx /path/to/file
```

Эта команда добавляет права чтения, записи и выполнения (rwx) для пользователя `username` к указанному файлу.

Добавление прав для группы

```
$ setfacl -m g:groupname:rx /path/to/file
```

Эта команда добавляет права чтения и выполнения (rx) для группы `groupname` к указанному файлу.

Добавление прав для всех пользователей

```
$ setfacl -m o::r /path/to/file
```

Эта команда добавляет право чтения (r) для всех пользователей к указанному файлу.

Удаление ACL

Для удаления определенных прав доступа используется ключ `-x`:

```
$ setfacl -x u:username /path/to/file
```

Эта команда удаляет все права для пользователя `username` к указанному файлу.

Удаление всех ACL

Для удаления всех ACL и возврата к стандартным Unix-подобным правам используется ключ `-b`:

```
$ setfacl -b /path/to/file
```

Эта команда удаляет все ACL с указанного файла.

Рекомендации по безопасности

- Используйте ACL для тонкой настройки прав доступа к файлам и каталогам, особенно в многопользовательских системах.
- Регулярно проверяйте и обновляйте ACL для предотвращения несанкционированного

доступа.
- Обратите внимание на наследуемые ACL при создании новых файлов и каталогов внутри директорий с установленными ACL.
- Используйте команды `getfacl` и `setfacl` для управления правами доступа и мониторинга текущих настроек безопасности.

Заключение

ACL предоставляет мощный и гибкий механизм управления правами доступа в НАЙС ОС. Следуя приведенным рекомендациям и примерам, вы сможете эффективно контролировать доступ к своим файлам и каталогам, повышая уровень безопасности вашей системы.