Настройка и использование AppArmor

Введение

AppArmor (Application Armor) — это система мандатного контроля доступа для операционных систем Linux, которая обеспечивает безопасность путем ограничения программ в системе. AppArmor позволяет администраторам задавать политики безопасности, определяющие, какие ресурсы могут быть доступны конкретным приложениям. В данной документации мы рассмотрим процесс установки, настройки и использования AppArmor в операционной системе НАЙС ОС, включая создание и управление профилями безопасности для различных приложений.

Установка AppArmor

Перед началом работы с AppArmor необходимо установить необходимые пакеты и включить поддержку AppArmor в системе.

Установка пакетов AppArmor

Для установки AppArmor используйте пакетный менеджер `dnf`:

```
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
```

Загрузка и выгрузка профилей

Для загрузки профиля используйте команду `apparmor_parser`:

```
sudo apparmor_parser -r /etc/apparmor.d/usr.bin.apache2
```

Для выгрузки профиля используйте команду `aa-disable`:

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

Создание и редактирование профилей AppArmor

Профили AppArmor определяют правила и ограничения для приложений. Их можно создавать и редактировать вручную или с помощью утилит AppArmor.

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. Пример профиля:

```
#include

/usr/bin/myapp {
  # Права доступа к файлам
    /etc/myapp/** r,
    /var/log/myapp/** rw,

  # Права доступа к сети
    network inet stream,
}
```

Перезагрузка AppArmor

Перезагрузите службу AppArmor для применения изменений:

```
sudo systemctl restart apparmor
```

Использование режима обучения

Режим обучения (complain mode) позволяет отслеживать нарушения правил безопасности без их применения. Это помогает создать и настроить профили без прерывания работы приложений.

Перевод профиля в режим обучения

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

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

Анализ логов режима обучения

Для анализа логов режима обучения используйте утилиту `logprof`:

```
sudo aa-logprof
```

Следуйте инструкциям на экране для обновления профиля на основе собранных данных.

Перевод профиля в принудительный режим

После завершения настройки профиля переведите его в принудительный режим с помощью команды `aa-enforce`:

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

Использование AppArmor с Docker

AppArmor может использоваться для ограничения действий контейнеров Docker, обеспечивая дополнительный уровень безопасности.

Создание профиля для контейнера Docker

Создайте профиль для Docker-контейнера. Пример профиля:

```
#include

/usr/bin/docker-default {
    capability chown,
    capability dac_override,
    capability fowner,
    capability fsetid,
    capability kill,
    capability net_bind_service,
    capability setgid,
    capability setuid,
    capability sys_chroot,
```

```
    capability sys_admin,
    mount,
    network,
    /{,usr/}bin/docker rwm,
    /var/lib/docker/** rw,
    /etc/docker/** rw,
}
```

Применение профиля к контейнеру

Запустите контейнер Docker с применением профиля AppArmor:

```
sudo docker run --security-opt apparmor=docker-default -d mycontainer
```

Интеграция AppArmor с системами мониторинга

Интеграция AppArmor с системами мониторинга позволяет отслеживать и анализировать события безопасности в реальном времени.

Установка и настройка auditd

Установите и настройте `auditd` для журналирования событий безопасности:

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

Настройка правил аудита для AppArmor

Добавьте правила аудита для AppArmor в файл `/etc/audit/rules.d/audit.rules`:

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

Добавьте строки:

```
-w /var/log/apparmor/ -p wa -k apparmor
```

Перезапуск auditd

Перезапустите службу `auditd` для применения изменений:

```
sudo systemctl restart auditd
```

Просмотр логов AppArmor

Используйте команду `ausearch` для просмотра логов AppArmor:

```
sudo ausearch -k apparmor
```

Обновление и удаление профилей AppArmor

Регулярное обновление профилей безопасности помогает поддерживать высокий уровень защиты системы.

Обновление профилей

Для обновления профиля откройте файл профиля и внесите необходимые изменения. Затем перезагрузите AppArmor для применения изменений:

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

Удаление профилей

Для удаления профиля используйте команду `aa-disable`, затем удалите файл профиля:

```
sudo aa-disable /etc/apparmor.d/usr.bin.myapp
sudo rm /etc/apparmor.d/usr.bin.myapp
```

Заключение

AppArmor является мощным инструментом для обеспечения безопасности операционной системы НАЙС ОС. С его помощью можно ограничивать действия приложений, создавать и управлять профилями безопасности, интегрировать систему с контейнерами Docker и системами мониторинга. Следуя приведенным инструкциям и примерам, вы сможете эффективно настроить и использовать AppArmor для защиты вашей системы и данных.