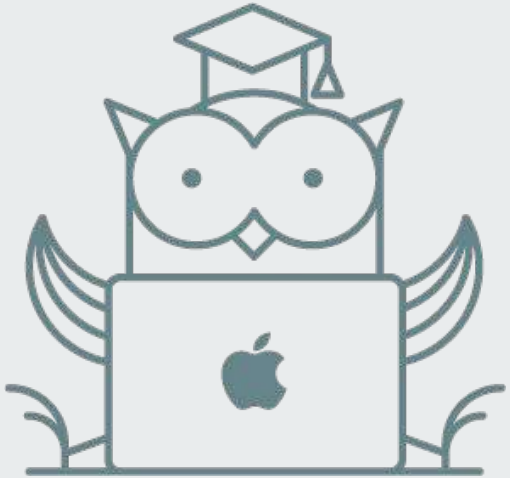
Курс «Администратор Linux»

Аутентификация, Авторизация и PAM

Занятие # 15

Дмитрий Молчанов
Григорий Ожегов



AAA

- **Authentication** - Аутентификация, процесс подтверждения пользователем своей “подлинности”. Ввод логина и пароля.
- **Authorization** - Авторизация, процесс предоставления доступа к каким-либо объектам
- **Accounting** - Запись информации о произошедших событиях.

PAM

PAM - Pluggable Authentication Modules. Подсистема которая позволяет настраивать различные комбинации модулей для различных приложений. Существует не только для Linux и является уже, своего рода, стандартом и неотъемлемой компонентой любого linux.

С помощью pam можно настроить процесс AAA в системе под свои нужды, с использованием различных аутентификационных бэкендов и дополнительных модулей - LDAP, GoogleAuthenticator, RADIUS.

Некоторые модули

Аутентификация:

- pam_unix - аутентификация в /etc/passwd
- pam_userdb - аутентификация против BDB-файла
- pam_rootok - разрешение root'у всего.

Авторизация:

- pam_wheel - авторизация для сервиса с использованием группы wheel

Модули не только позволяют реализовать процесс аутентификации, авторизации, но и обрабатывать некоторые дополнительные вещи.

- pam_mkhomedir - создание домашнего каталога пользователя

Стеки модулей PAM

- **auth**entication - Секция для аутентификации
- **account** - Секция посвященная авторизации и настроек аккаунта (заблокирован ли?)
- **password** - Секция описывающая модули используемые для модификации пароля. Разные бэкенды требуют разных действий для смены пароля.
- **session** - Accounting секция, также тут можно выполнять различные pre/post задачи для установки сессии.

Конфигурация

Конфигурация PAM хранится в /etc/pam.d (еще в /etc/pam.conf). Конфигурация первично делится по сервисам (sshd,login,su,sudo)

- /etc/pam.d/
  - *servicename* - файл с настройками стеков модулей

Внутри файла конфигурация выглядит примерно так: (/etc/pam.d/su)

```
#%PAM-1.0
auth          sufficient    pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth         sufficient    pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth         required      pam_wheel.so use_uid
auth          substack      system-auth
auth          include             postlogin
account             sufficient    pam_succeed_if.so uid = 0 use_uid quiet
account             include             system-auth
password      include             system-auth
session             include             system-auth
session             include             postlogin
session             optional      pam_xauth.so
```

Комбинирование модулей PAM

Конфигурация для каждого сервиса определяется в формате:

```
type control module-path module-arguments
```

В конфигурации, внутри каждого стека(type: auth, account и т.д.) есть один или несколько модулей, которые просматриваются по порядку (сверху-вниз) и, в зависимости от control-а (тип реакции) проверка либо продолжается, либо прекращается.

Комбинирование модулей PAM

```
type control module-path module-arguments
```

Controls:

- required - Для успешного завершения проверки этот модуль должен сработать, проверка продолжается вне зависимости от результата.
- requisite - как required, только при ошибке проверка прекращается. Возвращается ошибка первого required/requisite модуля вернувшего ошибку.
- sufficient - При успехе возвращается OK и проверка завершается
- optional - опциональный модуль. Успех или Ошибка важны только в случае если это единственный модуль в стеке.
- include - включить в текущий стек модулей стек модулей из файла
- substack - включить в текущий стек результат модулей из файла

Расширение возможностей

С помощью пакета pam_script можно быстро и гибко расширять AAA-процесс и использовать возможности PAM. Например можно настроить авторизацию пользователя в зависимости от погоды в Гонолулу.

Еще применения PAM

Помимо влияния на то как происходит аутентификация в системе можно использовать PAM как сервис(клиент). Например для встраивания системной аутентификации в какие-то свои скрипты.

Спасибо за внимание

Дмитрий Молчанов
Григорий Ожегов