**Управление аутентификацией и авторизацией с помощью PAM**

PAM — это модуль, который подключается к различным программам, выполняющим аутентификацию, и предоставляет единый интерфейс управления правами доступа. Astra Linux поддерживает использование PAM для управления аутентификацией и авторизацией.

Файлы конфигурации PAM находятся в /etc/pam.d/ .

Любой файл конфигурации PAM состоит из строк, каждая из которых содержит:

* имя модуля;
* тип службы;
* аргументы модуля, разделённые пробелами.

Тип службы определяет, к какому типу пакета PAM он будет относиться, например заголовок (header), футер (footer) и так далее.

Аргументы зависят от модуля, который был выбран.

Пример настройки использования PAM для аутентификации в файле /etc/pam.d/login выглядит так:

#%PAM-1.0

auth requisite pam\_securetty.so

auth requisite pam\_nologin.so

auth include system-auth

account include system-auth

session include system-auth

Для авторизации PAM использует правила, заданные в файле /etc/security/access.conf.

В этом файле можно задавать правила для доступа пользователей к определённым системным ресурсам.

Пример правила в файле /etc/security/access.conf:

# Allow root user full access

+:root:ALL

# Allow user «example» to access system resources only from local IP addresses

+ :example :192.168.0.0/16

— :example : ALL

где

+:root:ALL  позволяет пользователю root полный доступ к системным ресурсам.

+ :example :192.168.0.0/16 позволяет пользователю example получить доступ только с IP-адресов в диапазоне 192.168.0.0/16.

- :example : ALL запрещает пользователю example доступ ко всем остальным системным ресурсам.

Конфигурация PAM в Astra Linux содержит правила управления паролями пользователей. Например, можно задать минимальную длину пароля или максимальное количество попыток входа для безопасной аутентификации.

Допустим, мы хотим установить минимальную длину пароля в восемь символов. Для этого мы добавляем в файл /etc/pam.d/passwd строку:

password requisite pam\_pwquality.so minlen=8

Эта строка обозначает использование PAM-модуля pam\_pwquality для проверки безопасных условий пароля. Параметр minlen=8 указывает, что длина пароля не должна быть меньше восьми символов. Теперь при попытке создания или изменения пароля пользователь будет получать ошибку, если длина пароля меньше восьми символов.

Также PAM используется для установки максимального количества попыток входа пользователя в систему. Для этого можно использовать модуль pam\_tally2

Показать, как это делать