

# Модули аутентификации РАРМ

# РАМ

РАМ — это подключаемые модули безопасности, предоставляющие администраторам дополнительные методы подтверждения подлинности пользователя.

Модули РАМ позволяют использовать несколько схем аутентификации. Практически все приложения, нуждающиеся в проверке подлинности пользователя (POP, SSH и др.), применяют РАМ.

# Модули РАМ

Модули РАМ позволяют использовать несколько схем аутентификации. Практически все приложения, нуждающиеся в проверке подлинности пользователя (POP, SSH и др.), применяют РАМ.

# Каталог /etc/pam.d

В каталоге /etc/pam.d размещаются файлы настроек, задающие набор модулей PAM, которые должна использовать та или иная программа. Имя файла совпадает с названием программы – например, для SSH-сервера это файл sshd, для программы login – файл login и т. д

# Содержимое каталога /etc/security

- ▶ `access.conf`— управляет доступом к системе, позволяет задать не только, кто и куда может зайти, но и откуда. Эти настройки обслуживает модуль  `pam_access` ;
- ▶ `console.perms`— определяет права, получаемые привилегированными пользователями к консоли во время входа в систему и возвращаемые при выходе. Эти настройки обслуживает модуль  `pam_console` ;
- ▶ `group.conf` — позволяет указать, какой группе будет принадлежать служба, запущенная определенным пользователем в определенное время с определенного терминала. Эти настройки обслуживают модули  `pam_time`  и  `pam_group` ;
- ▶ `limits.conf` — позволяет ограничить системные ресурсы. Эти настройки обслуживает модуль  `pam_limits` ;
- ▶ `pam_env.conf`— здесь можно ограничить возможности пользователей изменять определенные переменные среды. Эти настройки обслуживает модуль  `pam_env` ;
- ▶ `time.conf` — позволяет ограничивать вход пользователей в систему по времени. Например, с его помощью можно запретить вход администратора с первой консоли по выходным. Эти настройки обслуживает модуль  `pam_time` .

# Ограничение доступа к системе

Файл `access.conf` позволяет ограничить доступ пользователей к вашему компьютеру.

Предположим, что пользователям `den` и `admin` разрешено администрировать сервер, а остальным пользователям — нечего даже делать у консоли сервера (и это правильно!).

Тогда в файл `access.conf` нужно добавить строку:

```
-:ALL EXCEPT root den admin:ALL
```

Такая запись означает: запретить регистрацию в системе всем пользователям, кроме пользователей `root`, `den` и `admin` — эти три пользователя могут регистрироваться с любой консоли и с любого IP-адреса (если регистрация происходит по SSH)

# Ограничение доступа к системе

Довольно часто администратор работает за своим компьютером — отдельной рабочей станцией — и будет регистрироваться на сервере только с этого компьютера.

В таком случае в файл `access.conf` можно добавить строки следующего вида:

```
-:ALL EXCEPT root: 192.168.1.2
```

```
-:ALL: LOCAL
```

Здесь `192.168.1.2` — адрес рабочей станции администратора, вход на сервер будет разрешен только с этого IP-адреса. Вторая строка запрещает локальный доступ всех пользователей и даже пользователя `root`. Будьте осторожны с этой строкой — если что-то случится с компьютером `192.168.1.2` или, вообще, с сетью, вы не сможете зайти в систему.

# Включение ограниченного доступа

Но одного редактирования файла `access.conf` для задеирования его опций недостаточно. Чтобы система и SSH при проверке подлинности пользователей использовала PAM, нужно в файлы `/etc/pam.d/system-auth` и `/etc/pam.d/sshd` добавить следующую строку:

```
account required /lib/security/pam_access.so
```

# Борьба с простыми паролями

Пользователи частенько стараются облегчить себе жизнь и устанавливают очень простые пароли, которые очень просто и взламываются — точнее, подбираются. В файле `/etc/pam.d/system-auth` администратор может указать, каким он хочет видеть безопасный пароль.

- ▶ `minlen=N` – минимальная длина пароля (нужно как минимум 6 символов – это исключит короткие и легко подбираемые пароли);
- ▶ `dcredit` – если задан этот параметр, то допустимое минимальное количество символов будет уменьшено на величину этого параметра при условии, что в пароле есть хотя бы одна цифра.
- ▶ `ucredit` – то же самое, что и `dcredit`, но определяется наличием буквы в верхнем регистре;
- ▶ `lcredit` – то же самое, что и `dcredit`, но определяется наличием буквы в нижнем регистре (применяется редко, но не позволяет пользователям перехитрить систему и использовать короткий пароль, состоящий из букв в верхнем регистре);
- ▶ `ocredit` – то же самое, что и `dcredit`, но определяется наличием специального символа;
- ▶ `retry=N` – количество попыток ввода пароля, после чего учетная запись будет заблокирована.

# Регистрация только в рабочее время

Целесообразно разрешить пользователям регистрироваться в системе только в рабочее время — вне рабочего времени им делать в системе нечего. Откройте файл `/etc/security/time.conf` и добавьте в него следующую строку:

```
login;tty* & !tty*; !root & den & ; !A10800-1800
```

После этого откройте файлы `/etc/pam.d/system-auth` и `/etc/pam.d/sshd` и добавьте в них строку:

```
account required /lib/security/pam_time.so
```

Таким образом регистрация в системе всем пользователям (кроме пользователей `root` и `den`) разрешена только в рабочее время (с 8-00 до 18-00). Пользователи `root` и `den` могут регистрироваться в любое время суток.

# Ограничение на используемые системные ресурсы

Один из видов атак (атака на отказ, DoS) заключается в загрузке программой злоумышленника всех системных ресурсов, в результате чего система оказывается не в состоянии выполнять полезные действия и обслуживать других пользователей. Для защиты от таких атак можно использовать файл `/etc/security/limits.conf`, позволяющий установить лимиты на использование системных ресурсов. Формат файла следующий:

домен тип элемент значение

# Ограничение на используемые системные ресурсы

Здесь поле домен — это имя пользователя или имя группы (группа указывается так: @имя). Если нужно, чтобы ограничение распространялось на всех пользователей и на все группы, следует указать \*. Второе поле задает тип ограничения:

- ▶ `soft` — «мягкое» ограничение, которое еще можно незначительно превысить;
- ▶ `hard` — «жесткое» ограничение, превысить которое уже нельзя.

# Ограничение на используемые системные ресурсы

В качестве поля элемент можно использовать следующие значения:

- ▶ `core` — ограничивает размер файла ядра (в Кбайт);
- ▶ `data` — максимальный размер сегмента данных (в Кбайт);
- ▶ `fsize` — максимальный размер файла (в Кбайт);
- ▶ `nofile` — максимальное число одновременно открытых файлов;
- ▶ `nproc` — количество процессов, которые может запустить пользователь;
- ▶ `stack` — максимальный размер стека (в Кбайт);
- ▶ `cpu` — максимальное процессорное время (в минутах);
- ▶ `maxlogins` — максимальное количество регистраций пользователя (в Linux по умолчанию разрешается одному пользователю войти в систему неограниченное количество раз: с разных консолей, по SSH, FTP и т. д.);
- ▶ `priority` — приоритет, с которым будут выполняться процессы пользователя/группы.

# Ограничение на используемые системные ресурсы

Последнее поле значение задает сам лимит для выбранного элемента — например:

- ▶ для группы `students` установлен жесткий лимит на количество процессов, равный 30:

```
@students hard nproc 30
```

- ▶ пользователю `ftp` вообще запрещено запускать какие-либо процессы:

```
ftp hard nproc 0
```