

MFASOFT

Secure Authentication Server

Интеграция с Linux сервисами

Оглавление

Введение.....	4
Поток данных.....	4
Настройка на стороне SAS	5
Настройка на стороне Linux	6
Настройка двухфакторной аутентификации в сервисе SSH	7
Настройка двухфакторной аутентификации при графическом входе	8

© 2023 ООО «СИС разработка», Москва, Россия

RU.73288061.58.29.29-11 ИП 01

Версия 1.6

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ООО «СИС разработка».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ООО «СИС разработка», 117246, г. Москва, Научный проезд, д. 17.

Веб-сайт ООО «СИС разработка»: <https://mfasoft.ru>

Телефон службы поддержки: +7 (495) 228-02-08

Адрес электронной почты службы поддержки: support@mfasoft.ru

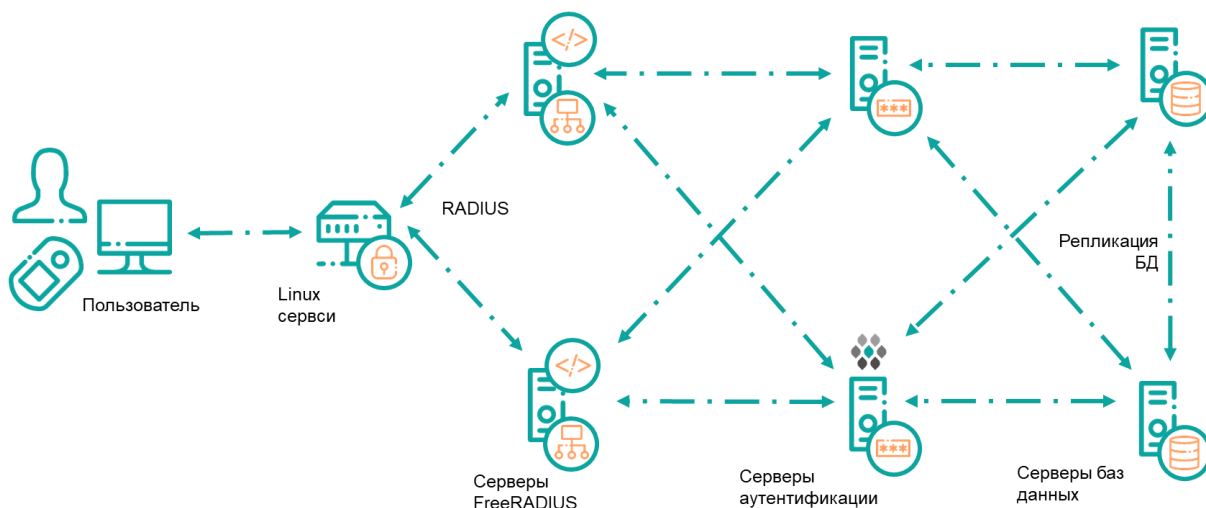
Введение

Для того, чтобы использовать двухфакторную аутентификацию в сервисах Linux можно использовать механизм подключаемых модулей аутентификации (Pluggable Authentication Module, PAM). PAM выполняет роль посредника, перенаправляя запросы от команд и сервисов, использующих базовый механизм аутентификации и авторизации Linux, к внешним поставщикам, причем для каждой из таких команд или сервисов использование PAM можно настроить индивидуально.

Большинство дистрибутивов Linux поддерживают модуль `ram_radius`, реализующий функции клиента RADIUS, а в составе SAS присутствует (см. раздел «Установка») образ контейнера FRA со шлюзом RADIUS. Поэтому модифицировать программный код Linux не нужно, и интеграция сводится к разворачиванию контейнеров с компонентами RADIUS (см. раздел «Установка»). Ниже приведен пример интеграции для операционных систем семейства ALT Linux (Workstation и Server).

Поток данных

На следующем рисунке представлен поток данных при выполнении двухфакторной аутентификации в Linux. Схема включает отказоустойчивые узлы, обеспечивающие доступность функции аутентификации при возникновении сбоев в инфраструктуре.



- 1) Пользователь делает запрос на двухфакторную аутентификацию в Linux системе
- 2) `ram_radius` модуль, интегрированный в Linux сервис, делает запрос на первый RADIUS сервер с установленным FRA модулем. В случае, если первичный RADIUS

сервер не доступен, то по истечению временного интервала, установленного в файле конфигурации делается запрос на второй RADIUS сервер

- 3) RADIUS сервер получает запрос и передает его FRA модулю для дальнейшей обработки. FRA модуль делает запрос на ближайший (чаще всего установленный на том же хосте) сервер аутентификации. В случае если сервер аутентификации не доступен, то делается запрос на вторичный сервер аутентификации
- 4) Сервер аутентификации делает верификацию идентификационных и аутентификационных данных, возвращает ответ FRA модулю. FRA модуль возвращает ответ на RADIUS сервер. RADIUS сервер возвращает ответ в ram_radius модуль, который принимает решение об аутентификации пользователя в Linux сервисе.

Взаимодействие между ram_radius модулем и RADIUS сервером осуществляется через RADIUS протокол. По этой причине должен быть разрешен сетевой поток от хоста Linux к RADIUS серверу по протоколу UDP на порты 1812 и 1813.

Требования к сетевому взаимодействию между узлами SAS сервера представлены в руководстве администратора на изделие.

Настройка на стороне SAS

Для организации аутентификации пользователей по протоколу RADIUS необходимо в консоли администрирования добавить узлы аутентификации FRA модулей. Для этого в консоли необходимо перейти к узлу «Виртуальные сервера» - <Виртуальный сервер> - Настройки – «Узлы аутентификации», добавить узел с FRA модулем. В случае использования резервного RADIUS сервера необходимо также добавить информацию о нем.

Далее необходимо добавить Linux хост в список RADIUS клиентов. Для этого необходимо добавить RADIUS клиента в файл clients.conf (данный файл должен пробрасываться в докер FRA путем выполнения команды `-v <Полный путь к файлу>/clients.conf:/etc/freeradius/3.0/clients.conf`):

Пример записи:

```
client alt_linux {  
    ipaddr = 10.79.63.19  
    secret = QAZwsx22!  
}
```

где alt_linux – произвольное имя RADIUS клиента

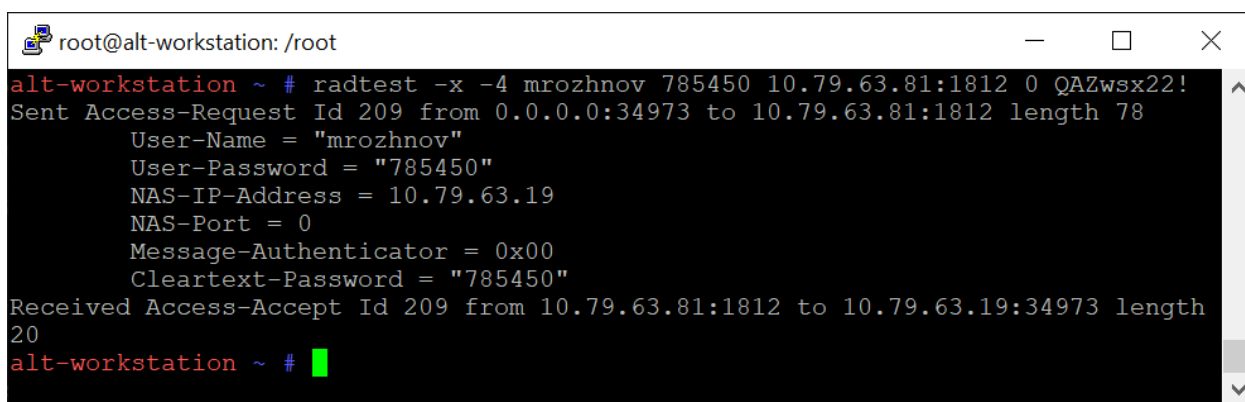
ipaddr – IP адрес RADIUS клиента (Linux хоста)

secret – общий секрет

Для проверки корректной настройки можно воспользоваться модулем radtest, входящим в состав freeradius-utils. Для этого необходимо выполнить следующую команду на Linux хосте:

```
# radtest -x -4 <логин пользователя в SAS> <код доступа пользователя в SAS – значение OTP> <IP адрес RADIUS сервера>:1812 0 <общий секрет>.
```

В случае успешной аутентификации приложение должно выдать сообщение «Access-Accept»



```
root@alt-workstation: /root
alt-workstation ~ # radtest -x -4 mrozhnov 785450 10.79.63.81:1812 0 QAZwsx22!
Sent Access-Request Id 209 from 0.0.0.0:34973 to 10.79.63.81:1812 length 78
  User-Name = "mrozhnov"
  User-Password = "785450"
  NAS-IP-Address = 10.79.63.19
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "785450"
Received Access-Accept Id 209 from 10.79.63.81:1812 to 10.79.63.19:34973 length 20
alt-workstation ~ #
```

Настройка на стороне Linux

Перед непосредственной интеграцией pam_radius модуля с различными сервисами его необходимо установить, выполнив команду: apt-get install pam_radius. В случае, если необходимо заменить стандартные приглашения ввода OTP и информацию о «Challenge-Response» рекомендуется выполнить пересборку pam_radius модуля из исходных текстов (информация о пересборке и кастомизации исходного текста представлена ниже)

Далее необходимо добавить параметры RADIUS серверов в файле /etc/raddb/server.

```
10.79.63.20 QAZwsx22! 60
```

```
10.79.63.21 QAZwsx22! 60
```

где первая строка – параметры конфигурации первого RADIUS сервера, вторая строка – параметры конфигурации второго RADIUS сервера

Каждая строка содержит следующие параметры:

- 1) IP адрес RADIUS сервера

- 2) Общий секрет
- 3) Время отклика RADIUS сервера в секундах (в случае отсутствия отклика от первого RADIUS сервера, запрос будет отправлен на второй RADIUS сервер).
Рекомендуется выставить значение 60 секунд в случае использования push аутентификации.

Настройка двухфакторной аутентификации в сервисе SSH

Для настройки двухфакторной аутентификации в настройках сервиса SSH необходимо внести следующие изменения в файле `/etc/openssh/sshd_config`:

PasswordAuthentication yes

PermitEmptyPasswords no

ChallengeResponseAuthentication yes

UsePAM yes

Далее необходимо внести изменения в настройках PAM модуля для службы SSH в файле `/etc/pam.d/sshd`. Ниже представлена конфигурация, когда первоначально запрашивается значение OTP, а далее запрашивается Linux пароль:

#%PAM-1.0

auth requisite pam_succeed_if.so user != root quiet

auth include system-auth-local

*auth required pam_radius_auth.so conf=/etc/raddb/server prompt=Enter OTP
force_prompt*

account include common-login

password include common-login

session include common-login

Первая строка разрешает аутентификацию только для пользователей, отличных от root. Вторая строка требует Linux аутентификацию. Третья строка требует RADIUS аутентификацию (значение параметра Enter OTP содержит неразрывный пробел).

После внесения изменений необходимо перезапустить SSH сервис, выполнив команду: `# systemctl restart sshd`

```
mrozhnov@alt-workstation: /home/mrozhnov
login as: mrozhnov
Keyboard-interactive authentication prompts from server:
| Password:
| Enter OTP:
End of keyboard-interactive prompts from server
Last login: Fri Dec 15 13:52:00 2023 from 10.79.63.1
mrozhnov@alt-workstation ~ $
```

Аналогичная настройка требуется для ALT Linux Server:

```
mrozhnov@alt-server: /home/mrozhnov
login as: mrozhnov
Keyboard-interactive authentication prompts from server:
| Password:
| Enter OTP:
End of keyboard-interactive prompts from server
Last login: Fri Dec 15 14:37:02 2023 from 10.79.63.1
[mrozhnov@alt-server ~]$
```

Настройка двухфакторной аутентификации при графическом входе

Для настройки двухфакторной аутентификации при графическом доступе необходимо внести следующие изменения в файле `/etc/pam.d/lightdm`:

##PAM-1.0

auth required pam_shells.so

auth required pam_succeed_if.so quiet uid ne 0

auth sufficient pam_succeed_if.so user ingroup nopasswdlogin

auth include system-auth-local

auth requisite pam_succeed_if.so uid != 0

*auth required pam_radius_auth.so conf=/etc/raddb/server prompt=OTP
force_prompt*

-auth optional pam_gnome_keyring.so

-auth optional pam_mate_keyring.so

account include common-login

password include common-login

session substack common-login

session optional pam_console.so

-session optional pam_ck_connector.so

session required pam_namespace.so

-session optional pam_gnome_keyring.so auto_start

-session optional pam_mate_keyring.so auto_start

Далее необходимо завершить активную графическую сессию и повторно войти в систему.

