

Настройка TACACS-авторизации на MES23xx/ 33xx/35xx/5324

Eltex Knowledge Base

Exported on 09/23/2024

Table of Contents

No headings included in this document

Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, при этом поддерживая совместимость с RADIUS и другими процессами проверки подлинности.
Конфигурацию будем выполнять на базе коммутатора MES2324.

1. Для начала необходимо указать ip-адрес tacacs-сервера и указать key:

```
console(config)# tacacs-server host 192.168.10.5 key secret
```

2. Далее установить способ аутентификации для входа в систему по протоколу tacacs+:

```
console(config)# aaa authentication login authorization default tacacs local
```

Примечание: На коммутаторах серии 23xx, 33xx, 53xx используется алгоритм опроса метода аутентификации break (после неудачной аутентификации по первому методу процесс аутентификации останавливается). Начиная с версии 4.0.6 доступна настройка метода опроса аутентификации break/chain. Алгоритм работы метода chain - после неудачной попытки аутентификации по первому методу в списке следует попытка аутентификации по следующему методу в цепочке. На коммутаторах серии 1000, 2000, 3000 уже имеется этот функционал.

3. Установить способ аутентификации при повышении уровня привилегий:

```
console(config)# aaa authentication enable default tacacs enable
```

Чтобы не потерять доступ до коммутатора (в случае недоступности radius-сервера), рекомендуется создать учетную запись в локальной базе данных, и задать пароль на привилегированный режим.

4. Создать учетную запись:

```
console(config)# username tester password eltex privilege 15
```

5. Задать пароль на доступ в привилегированный режим:

```
console(config)# enable password eltex
```

6. Разрешить ведение учета (аккаунта) для сессий управления.

```
console(config)# aaa accounting login start-stop group tacacs+
```

7. Включить ведение учета введенных в CLI команд по протоколу tacacs+.

```
console(config)# aaa accounting commands stop-only group tacacs+
```

Примечание: По умолчанию используется проверка по локальной базе данных (aaa authentication login default local).

8. Включить авторизацию вводимых команд на сервере Tacacs:

```
console(config)# aaa authorization commands default group tacacs+ local
```

После этого каждая вводимая команда будет проходить авторизацию на сервере.

Примечание: Данный функционал доступен с версии 4.0.16.