

Сервера доступа

Настройка NAS (Network Access Servers) серверов доступа. Здесь заводятся маршрутизаторы, коммутаторы и другое оборудование предоставляющее доступ абонентов к сети

Настройка > Сервер доступа

Основной **Покрытие** Группы:

Сервер доступа

ID	Название	NAS-Identifier	ip	Тип	Отключено	Описание		
1	NAS_Server		127.0.0.1	mpd5	Активно	NAS_Server	Пользователи	IP_Pool
2	microtik		192.168.1.234	mikrotik	Активно		Пользователи	IP_Pool
3	test_pon		10.0.0.10	rpp	Активно		Пользователи	IP_Pool
4	olt		10.0.0.12	eron	Активно		Пользователи	IP_Pool

Всего: **4**

Добавление сервера доступа

Сервер доступа

IP *

Название (a-zA-Z0-9_)*

Тип *

Alive (sec.)

Отключено

Управление

IP **POD/COA**

SSH **SNMP**

Пользователь

Пароль (PoD,RADIUS Secret,SNMP)

Адрес

Дополнительно

ID 1 (Изменения внесены: 2017-06-21 15:23:37)

Описание

Radius NAS-Identifier

MAC

Авторизация

External Accounting

Группа

RADIUS Параметры (,)

IP	IP адрес NAS сервера, если есть несколько серверов доступа с одинаковым IP обязательно заполняйте поле Radius NAS-Identifier
-----------	--

Name	Название
Radius NAS-Identifier	Идентификатор сервера (можно не вписывать). Используется в тех случаях когда на одном IP адресе несколько серверов доступа
Describe	Описание сервера
Тип	Тип сервера. В зависимости от типа по-разному обрабатываются запросы на авторизацию и аккаунтинг-информация.
MAC	MAC сервера доступа.
Authorization	Тип авторизации. SYSTEM - При хранении паролей в UNIX базе (/etc/passwd) SQL - при хранении паролей SQL базе (MySQL, PosgreSQL)
External Accounting:	Использовать внешнюю программу для ведения аккаунтинга.
:Manage:	Секция менеджмента NAS сервера
IP	IP адрес для контроля соединения. Например, для отключения пользователя с веб-интерфейса.
POD/COA PORT	POD/COA порт
SSH PORT	SSH порт
SNMP PORT	SNMP порт
User	Пользователь для контроля NAS. Также в поле есть кнопки генерации ssh ключа и загрузка его. Для генерации ключа, права на папку /usr/abills/Certs/ должны быть на запись веб сервером
Password	Пароль NAS. При изменении данных повторно наберите пароль.
Alive	<p>Время получения Alive сообщений. Используется для контроля за состоянием соединения пользователя. Этому параметру нужно присвоить то же значение, которое определено на NAS.</p> <p>Если на протяжении 5 Alive интервалов не пришёл ни один Alive пакет, сессии переносятся в секцию ZAP. Если после переноса на протяжении ещё 5 Alive периодов не пришло ни одного пакета подтверждения сессии, она считается как законченная, обсчитывается системой и заносится в лог с параметром ACCT_TERMINATE_CAUSE равным 3 - Service-Unavailable. Если в тарифном плане предусмотрен подсчёт времени сессии, то время сессии считаете, время от начала сессии до получения последнего Alive пакета. Если сессия находится в секции Zap и получает Alive пакет система автоматически переносит её обратно в секцию Online.</p> <p>Количество Alive интервалов можно определить в опции \$conf{ERROR_ALIVE_COUNT}=3</p> <p>Если NAS сервер не поддерживает RADIUS Alive пакеты (USR Netserver 8/16) тогда оставляете этот параметр по умолчанию .</p> <p>Alive пакет - периодический пакет, отправляемый RADIUS-сервером о состоянии соединения</p> <p>Рекомендуемые значения</p> <p>до 500 абонентов online - 60 больше 500 online - 300 больше 10 000 online - 600 Больше 30 000 online - 18 000</p>
Disable	Блокировка NAS сервера
RADIUS Parameters	<p>Дополнительные параметры, которые передаются NAS серверу после успешной авторизации. Имеют более высокий приоритет, чем параметры созданные системой авторизации.</p> <p>Если перед параметром поставить знак восклицания ! параметр созданный авторизатором не будет передаваться для NAS.</p> <p>При использовании нескольких пар радиус атрибутов между ними ставится запятая. При использовании атрибутов с одинаковой левой частью, правая должна дополняться при помощи плюса со знаком равенства (+=).</p> <p>Пример:</p> <p>Cisco-Service-Info = «QU;512000;256000;D;1024000;512000», cisco-avpair += «subscriber:accounting-list=BH_ACCNT_LIST1 », cisco-avpair += «ip:traffic-class=input access-group name ACL_IN_BOD1M_406 priority 20 «</p>

Если включена опция

```
$conf{RESTART_RADIUS}='/usr/local/bin/sudo /usr/local/etc/rc.d/radiusd restart';
```

после добавления или изменения данных о серверах радиус перезагружается автоматически в противном случае после изменения параметров сервера доступа обязательно перезагружайте RADIUS сервер

Настройка **sudoers**

FreeBSD

```
www ALL = NOPASSWD: /usr/local/etc/rc.d/radiusd
```

Ubuntu

```
www-data ALL = NOPASSWD: /etc/init.d/freeradius
```

Дополнительные возможности

В зависимости от типа сервера доступа можно просмотреть дополнительную информацию.

RADIUS TEST

Консоль тестирования RADIUS ответов для данного сервера доступа

Настройка > Сервер доступа

Информация IP Pools Статистика RADIUS Test Console Дополнительно SNMP

1 ASTERISK : 127.0.1.1

RAD_PAIRS

User-Name=test

Комментарии

Тип Запрос

Auth

Сохранить

Запрос

Дата	Комментарии	Запрос
2016-01-29 07:50:51		Запрос . 1
2016-09-08 05:47:55		Запрос . 2

Описание типов запросов

Тип Auth

По умолчанию система отправляет запросы на локальный RADIUS IP: 127.0.0.1 SECRET: secretpass чтобы изменить данные параметры существуют опции

<code>\$conf{RADIUS_TEST_IP}='127.0.0.1';</code>	IP тестового RADIUS сервера
<code>\$conf{RADIUS_TEST_SECRET}='secretpass';</code>	Секретный ключ тестового RADIUS сервера
<code>\$conf{RADIUS_TEST_SETTINGS} = «mpd5:User-Name=IP,Calling-Session-Id=CID;»;</code>	С этой опцией, тест сервера доступа с типом подключения 'mpd5' будет проходить с определенными значениями в ключах. Структура поля тип_подключения:поле:тип_передаваемого_значения;поля тип_подключения:поле:тип_передаваемого_значения;

Если получаете ошибку **No response from ACCESS_REQUEST server '127.0.0.1:1812**, скорей всего:

1. радиус клиентс не внесен в базу RADIUS-a(raddb/clients.conf);
2. пароль clients.conf отличается от пароля в биллинге(Управление/Пароль)

После изменений перезагрузить RADIUS:

```
# service radiusd restart
```

Тип Status

Данный тип запроса покажет статистику сервера радиуса.

По умолчанию система отправляет запросы на локальный RADIUS

IP: 127.0.0.1

Port: 18121

SECRET: adminsecret

Настройка

Нужно зайти в папку sites-enabled FreeRadius-a и сделать линк на файл status:

```
cd /usr/local/freeradius/etc/raddb/sites-enabled  
ln -s ../sites-available/status status
```

Затем в конфиг радиуса, в конец:

```
nano /usr/local/freeradius/etc/raddb/radiusd.conf
```

Вписать следующую строку

\$INCLUDE sites-enabled/status

Возможности

Можно показать отдельную статистику по аккаунтингу *Status Acct* или по авторизациям *Status Auth* или всю статистику сразу *Status All*.

Для того, чтоб увидеть статистику, нужно выбрать Тип Запроса, который хотите увидеть, и нажать кнопку **Показать**.

Тип COA Тип POD

Отправить пары для проверки Nas-a. Отправляет запрос на IP и PORT, которые прописаны в настройках Nas-a.

Console

консоль SSH/Telnet/rsh сервером доступа. Возможность отправлять команды управления и проверять доступность устройства

Поддержка управления

- Linux accel-ppp (telnet)
- FreeBSD mpd (telnet)
- Mikrotik (ssh)
- Cisco (rsh)
- Juniper

SNMP

SNMP управление. Для работы этой опции нужно подключать модуль [Snmputils](#)

Статистика

статистика работы работы серверов доступа количество подключаемых абонентов

Дополнительный

Расширенное управление сервером доступа

- Мониторинг портов
- Состояние устройства: CPU, RAM, Uptime
- Подключенный абоненты к порта

Для работы этой опции нужно подключать модуль [Equipment](#)

- [Пулы адресов](#)

Hotspot

[Mikrotik Hotspot](#)

From:
<http://abills.net.ua/wiki/> - **Advanced Billing Solution**

Permanent link:
http://abills.net.ua/wiki/doku.php/abills:docs:manual:admin:form_nas

Last update: **2018/10/31 10:44**

