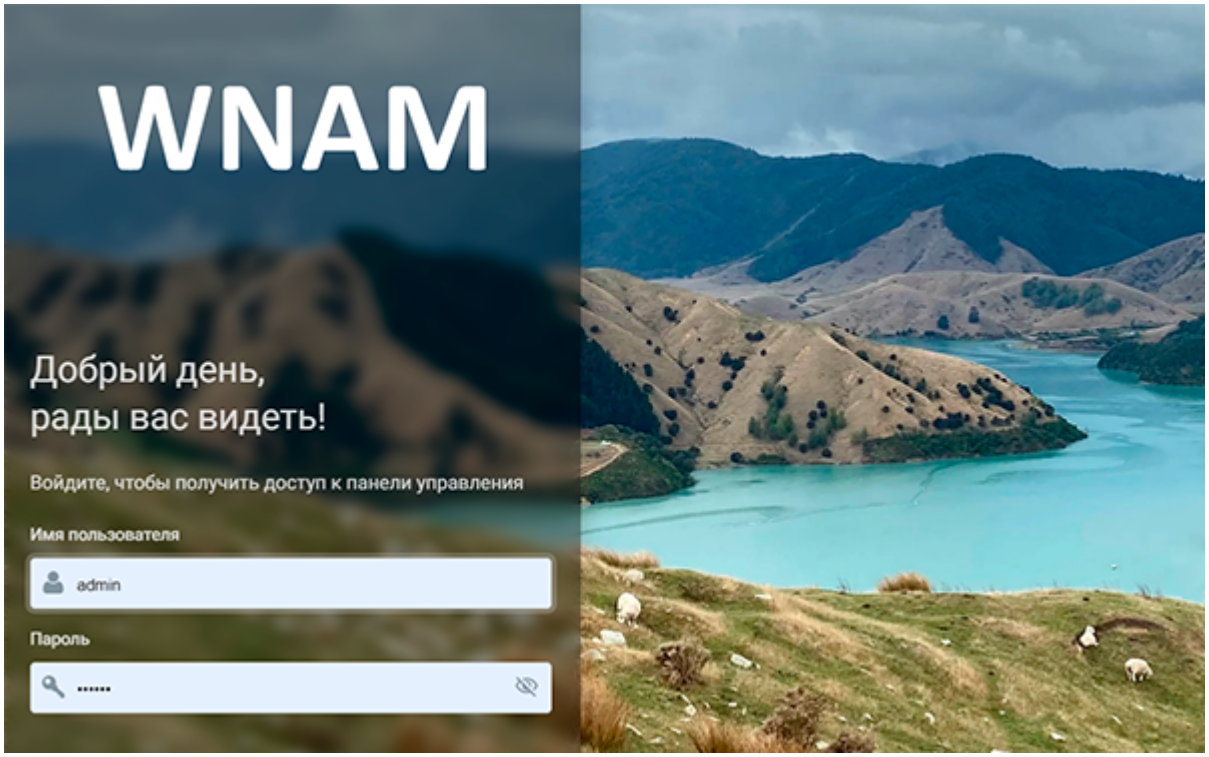
Система управления сетевым доступом WNAM 2

Документация на программное обеспечение



Оглавление

WNAM 2

Добро пожаловать!

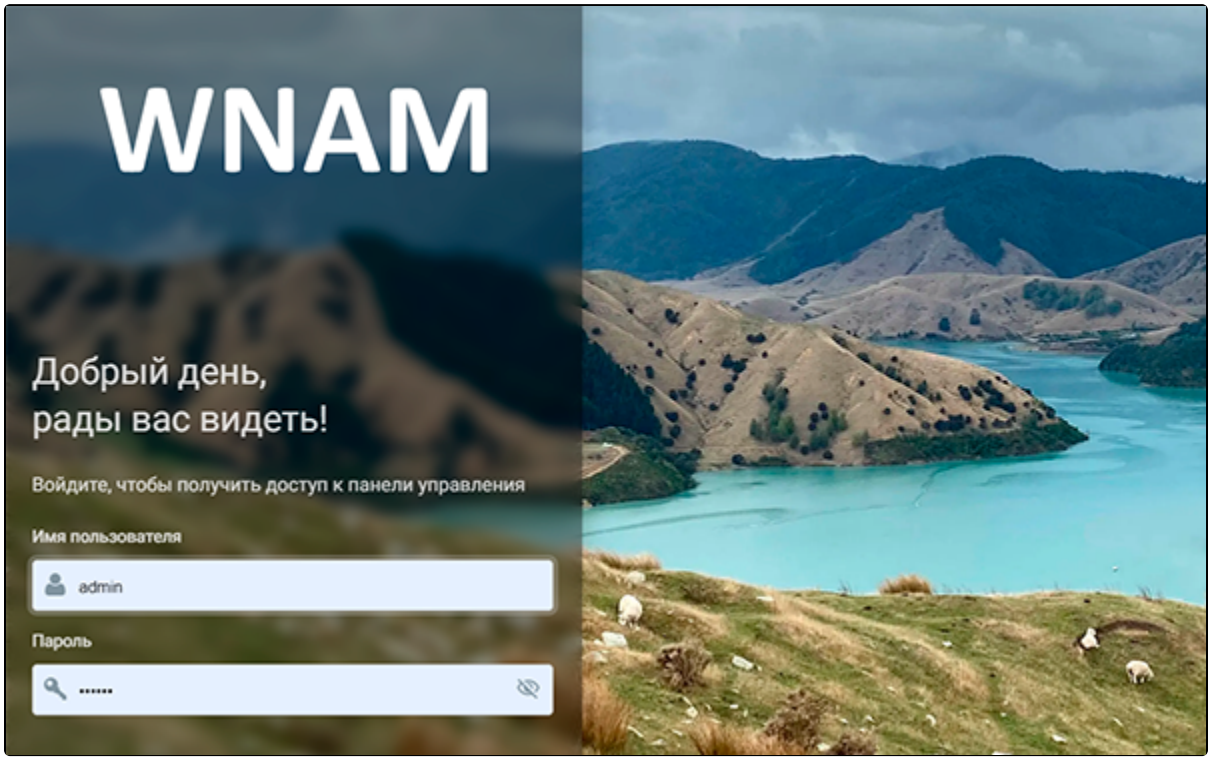
Представляем документацию на систему управления сетевым доступом WNAM поколения 2 - дальнейшее развитие системы управления беспроводным доступом WNAM 1.x.

Основываясь на более чем десятилетнем опыте создания популярного, удобного, гибкого, надежного инструмента обеспечения гостевой авторизацией в гостевых и корпоративных беспроводных и проводных сетях, мы предлагаем вам новый инструмент нашей разработки. WNAM 2 имеет улучшенные интерфейсы, API, поддержку популярной СУБД, ещё больше настроек, отчётов и возможностей для диагностики.

Размещенный здесь комплект документации относится к текущей стабильной версии программного обеспечения WNAM (2.0.457), датированной 06 ноября 2024 года.

Авторы этого документа, равно как и авторы WNAM, не несут ответственности за любой вред, ущерб, потерю денег, клиентов, порчу оборудования и прочие проблемы, вызванные вашим самостоятельным использованием данного программного обеспечения, или применением информации, изложенной здесь. Более подробно ограничение ответственности отражено в лицензионном соглашении, которое вы обязаны соблюдать.

WNAM является коммерческим продуктом (лицензии). Если у вас есть демо-лицензия, по окончании пробного периода эксплуатации (30 дней) вы обязаны любо прекратить пользоваться программой, либо приобрести лицензию у ООО "Нетамс" или у официальных партнеров.



Поиск по документации

Назначение

Программа предназначена для проведения аутентификации, авторизации и учёта подключающихся к локальной вычислительной сети пользователей, устройств и администраторов.

Она может использоваться на предприятиях, где требуется разграничение доступа к ЛВС согласно установленным правилам и политиками информационной безопасности.

Поддерживаются проводные, беспроводные и удалённые сетевые подключения, с проверкой учётных данных в службах каталога, центрах управления сертификатами; осуществляется авторизация гостевых подключений в соответствии с нормами законодательства (СМС, звонок, Госуслуги). Система реализует стандартные протоколы RADIUS и TACACS+. Обеспечивается отказоустойчивая работа, протоколирование всех операций по настройкам, учёт трафика и набранных команд. Программа управляется через веб-интерфейс и содержит развитые средства настройки, отчетности и диагностики.

Термины и определения

Для успешной настройки и последующей эксплуатации системы управления сетевым доступом WNAM 2 требуется понимание и знание применяемых в отрасли терминов и технологий. С целью повышения качества вашей работы с WNAM 2 рекомендуется ознакомиться с настоящими терминами и определениями.

> Нижеследующий текст не является исчерпывающим руководством по технологиям PKI, 802.1x и т.п, и не содержит математических принципов, применяющихся в алгоритмах шифрования на открытых ключах и цифровых подписях. Информация и определения даны в упрощенной форме. В случае необходимости более детального изучения, следует обратиться к специализированной литературе.

Абонент, пользователь, пользователь Wi-Fi, клиент

Физическое лицо, человек, подключившийся к проводной или беспроводной сети. Система WNAM 2 позволяет проводить аутентификацию и авторизацию доступа пользователей путём привязки аппаратного адреса (MAC-адреса) мобильного устройства (смартфон, телефон, планшет, мобильный компьютер) к логину, сертификату, номеру телефона с идентификацией номера путём отправки/получения СМС-сообщения, либо иному идентификатору.

Авторизация

Процесс определения результирующих прав подключающегося устройства, то есть назначенных определенных политик, например, ограничение скорости или номера VLAN.

Аккаунтинг

При успешной аутентификации и авторизации абонентское устройство получает доступ в сеть, а подключающее устройство (VPN шлюз, коммутатор ЛВС, контроллер БЛВС) формирует сведения об объеме передаваемых абонентом данных, включая дополнительные параметры (профилирование, IP-адрес и т.п.). Сессия аккаунтинга длится до того момента, пока абонент находится в сети, а подключающее устройство присылает периодические обновления (interim). Аккаунтинг не передает информацию по ресурсам, к которым подключается абонент (это функция других устройств (DPI, прокси, источники Netflow, NAT-Syslog и т.п.).

Аутентификация

Процесс определения идентичности подключающегося устройства (субъекта), путем проверки его учетной записи (логина и пароля), сертификата, анализа других параметров (например, место и дата/время подключения, тип устройства). В результате проверяющий компонент принимает решение о допуске/запрете подключения к сети.

Открытый и закрытый ключи

Автоматически сформированные очень большие числа, запакованные специальным образом (в контейнер), позволяющие осуществить операции по цифровой подписи и шифрованию данных (см. здесь). Публичный ключ содержится в сертификате и доступен всем желающим. Приватный ключ находится в защищенном хранилище мобильного устройства и никогда не передается по сети в открытом виде.

Администратор

Любой пользователь веб-интерфейса системы WNAM 2, имеющий те или иные привилегии в системе согласно её ролевой модели (например, администратор WNAM 2).

Местоположение

Территориальное место предоставления услуги сетевого доступа, например один этаж здания, один бизнес-центр, один офис. Характеризуется параметром IP-сети, из которой получают адреса клиенты, и/или иным идентификатором (обычно его передаёт хотспот), например, номер VLAN, номер и название SSID. Статистика по использованию ресурсов сети (трафик, сессии), тонкие настройки параметров авторизации/перенаправления/ограничений, производится в системе WNAM 2 с привязкой к местоположению.

Поток трафика

Информация об индивидуальной TCP/IP-сессии обмена трафиком, проводимой подключившимся абонентом в рамках сессии, и внешним ресурсом в сети. Определяется IP-адресами и TCP либо UDP-портами отправляющей или принимающей стороны, счетчиками пакетов и байт. Требует работы специализированных средств сбора такой информации на канале передачи данных, например, NetFlow.

Сетевое устройство

Физическое устройство, осуществляющее контроль и предоставление доступа в проводную или беспроводную сеть её конечным пользователям. Англоязычный эквивалент: Network Access Server (NAS). В общем случае, это маршрутизатор, или контроллер беспроводных точек Wi-Fi, или коммутатор ЛВС, или VPN-шлюз.

Сервер WNAM 2

Физический сервер или виртуальная машина, на которой установлена операционная система Linux, служебные программы (freeradius, tomcat, postgreSQL) и программное обеспечение WNAM 2.

Эндпоинт

Оконечное сетевое устройство, осуществляющее подключение к проводной или беспроводной сети, с использованием MAC адреса или персонифицированного идентификатора, характеризующееся уникальным MAC адресом. Исключая подключающиеся к открытой гостевой беспроводной сети устройства.

Сертификат

Цифровая сущность, содержащая в себе атрибуты принадлежности (название, компания, город и т.п.), даты начала и завершения валидности, публичный ключ, название и идентификатор сущности, подписавшей сертификат (другой сертификат). Служит для подтверждения "идентичности" предъявителя сертификата. При корректной настройке прослеживается цепочка "доверия" сертификатов друг другу, вплоть до сертификата, который числится в "заведомо доверенных" на устройстве.

Сессия

Сведения о факте подключения пользователя к сети с указанием ссылки на профиль абонента, а также на текущие параметры сессии: временный IP-адрес, выданный абонентскому устройству, счётчики принятых и отправленных байт, сведения о площадке, где произошло подключение, точке доступа Wi-Fi, RADIUS-идентификаторе сессии и т.п.

Стандарт 802.1x

Стандарт, описывающий процесс инкапсуляции учетных данных подключающегося устройства в протокол EAP для последующей их передачи серверу авторизации.

Удостоверяющий центр

Организация либо управляемое ею программное средство, выписывающее сертификаты оборудованию или конечным пользователям (абонентам) сети. Также имеет инструменты проверки валидности (действительности) сертификатов и публикующая списки отзыва и т.п.

Хотспот

Встроенное в устройство (сервер доступа) специальное программное обеспечение, позволяющее перехватывать (перенаправлять) HTTP- или HTTPS-сессию браузера абонента на внешний веб-сервер. В случае использования системы WNAM 2 таким веб-сервером является часть системы WNAM 2, где производится идентификация абонента и демонстрация ему заданных страниц. После проведения авторизации хотспот по команде от WNAM 2, временно разрешает абоненту доступ в сеть Интернет.

Active Directory

Служба каталога в исполнении Microsoft. Помимо запросов каталога реализует защищенные методы проверки аутентичности учетной записи пользователя, компьютера, позволяет распространять групповые политики и т.п.

CSR

Запрос на подпись сертификата, контейнер, содержащий по сути "недоделанный сертификат". Внешний Удостоверяющий центр выпускает на его основе полноценный сертификат за своей подписью.

DER

Формат файла, в котором содержится сертификат, ключ или другой объект, созданный удостоверяющим центром. Файл является бинарным и технически эквивалентен PEM.

FreeIPA

Служба каталога в открытой реализации. Входит в состав большинства (в том числе российских) дистрибутивов Linux.

LDAP

Служба каталога, справочник, а также сам протокол, по которому передаются запросы и возвращаются ответы об атрибутах учетной записи (принадлежность к группе, специфические атрибуты и т.п.). WNAM 2 использует LDAP для запроса контроллера домена Windows.

MAB или MAC Bypass

Процесс, при котором аутентификация устройства производится в упрощенном порядке, по его MAC-адресу. Применяется, когда оконечное устройство не поддерживает протокол 802.1x.

PEM

Формат файла, в котором содержится сертификат, ключ или другой объект, созданный удостоверяющим центром. Файл является текстовым и закодирован в BASE64. Сертификат, ключ и т.п. содержится в начале и конце файла в строках вида ----- BEGIN CERTIFICATE ------ и т.п.

PFX

Бинарный формат файла (контейнер), в котором содержится сертификат и приватный ключ субъекта (абонента сети). Дополнительно защищен паролем. Файл допустимо пересылать по сети для последующей установки в клиентское устройство.

PKI

Инфраструктура открытых ключей, набор инструментов для функционирования, в том числе для авторизации на основе сертификатов.

Принципы работы

Для корректной работы системы WNAM 2 необходимо настроить значительное число компонентов, а именно:

- устройства сетевого доступа NAS (контроллеры БЛВС для гостевого и/или корпоративного подключения, коммутаторы ЛВС, шлюзы VPN и т.п.);
- сетевую инфраструктуру, обеспечивающую подключение физических или виртуальных серверов WNAM 2;
- физические или виртуальные машины с ОС Linux для установки системы WNAM 2, СУБД;
- средства мониторинга;
- средства резервного копирования.

Настоятельно рекомендуется обращаться для этой цели к системным интеграторам, имеющим опыт работы с системой. Особенно, если вам требуется построение сложной, нагруженной и распределенной инсталляции системы WNAM 2. Получить рекомендации по выбору системного интегратора можно, отправив запрос на info@netams.com. Компания-разработчик системы WNAM 2 не может рекомендовать "идеальный" дизайн сопутствующих систем: сетевой инфраструктуры, средств виртуализации, средств обеспечения информационной безопасности, резервного копирования, доменной структуры Windows и т.п.

Приведенные ниже сценарии использования системы WNAM 2 описывают типовые задачи, которые встречаются у наших заказчиков. Настоятельно рекомендуется придерживаться одного из следующих примеров при проектировании и развертывании системы WNAM 2.

В работе системы вы можете одновременно использовать оба сценария. А также для использования в крупной сети настоятельно рекомендуется организовать два не связанных между собой кластера систем, работающих в разных информационных контурах: один только для гостевой, другой только для корпоративной авторизации.

Определившись со сценарием работы, необходимо оценить число серверов, требуемых системой WNAM 2 для работы, и разнесение функций системы между этими серверами. Такая оценка опирается на следующие параметры:

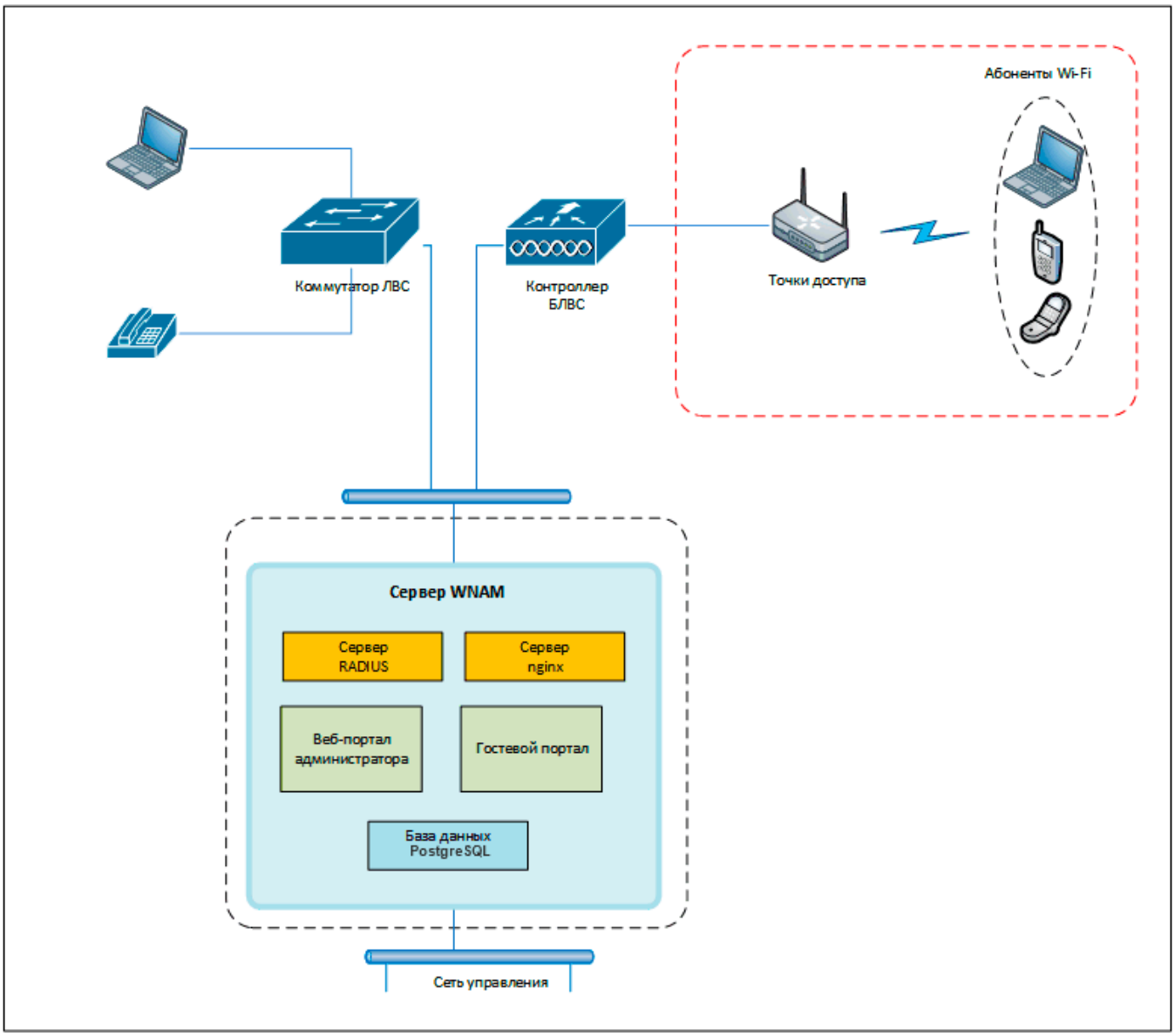
- число одновременно идущих процедур авторизации и число одновременно работающих в сети гостей / эндпоинтов;
- физические характеристики имеющихся серверов;
- требования по отказоустойчивости и географическому разнесению узлов системы.

В конечном счете, устойчивая работа системы WNAM 2 определяется нагрузкой на неё, которая напрямую связана с числом Web-, API-, TACACS+ и RADIUS-запросов, попадающих на систему. Рекомендуется проектировать объемы ресурсов таким образом, чтобы:

- нагрузка на процессор сервера не превышала 50% (т.е. величина LA сервера была вдвое меньше числа установленных процессорных ядер);
- задержка RADIUS-ответа в среднем не превышала 20 миллисекунд.

1.Типовой сценарий малой нагрузки

Если в сети находится менее 200 точек доступа (т.е. менее 1000 одновременно работающих гостевых клиентов) или корпоративная авторизация требует менее чем 200 эндпоинтов, подойдет дизайн, в котором все компоненты системы авторизации работают на одном физическом или виртуальном сервере.

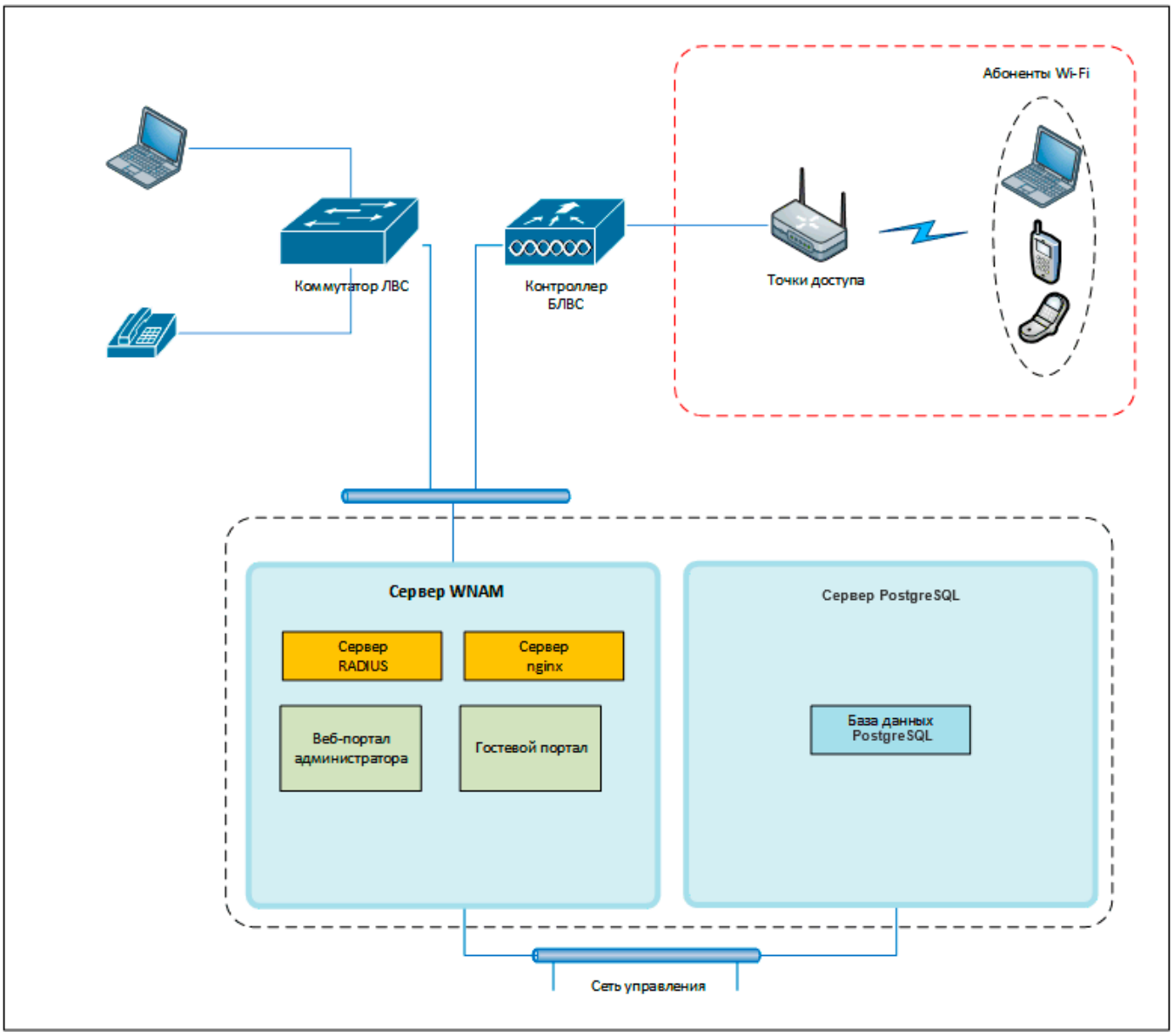


Типовые характеристики такого сервера:

- количество виртуальных процессоров: 2-4 vCPU;
- оперативная память: 8 Gb vRAM;
- объем жесткого диска: 32 Gb HDD (любого типа).

2. Сценарий средней нагрузки без отказоустойчивости

Если в сети находится менее 500 точек доступа (т.е. менее 5000 одновременно работающих гостевых клиентов) или корпоративная авторизация требует менее чем 500 эндпоинтов, рекомендовано вынести на отдельный сервер базу данных PostgreSQL.



В данном случае понадобится два одинаковых сервера с характеристиками:

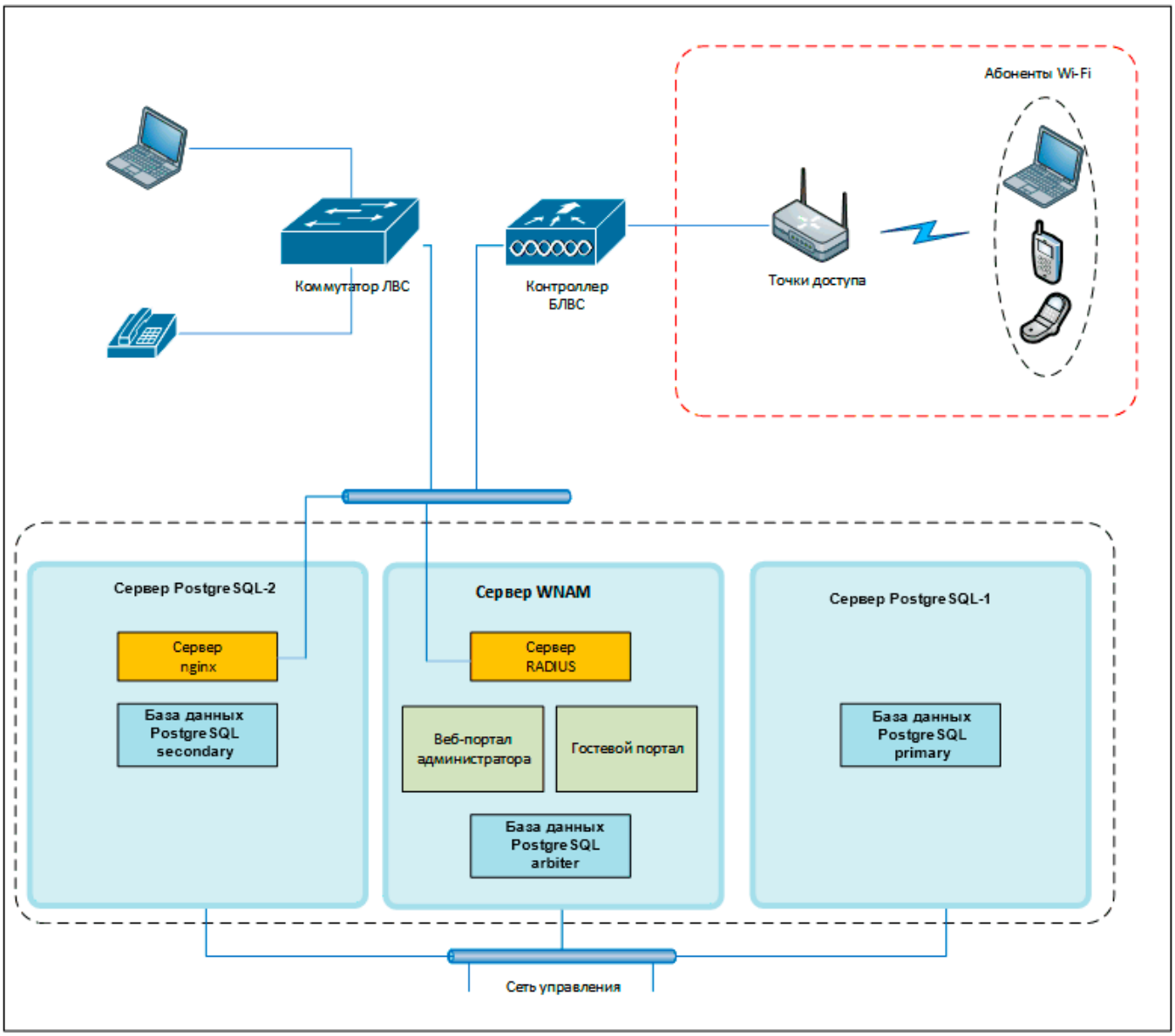
- количество виртуальных процессоров: 2-4 vCPU;
- оперативная память: 8-16 Gb vRAM;
- объем жесткого диска: 32 Gb HDD (любого типа).

Дополнительно для сервера PostgreSQL необходимо:

- объем жесткого диска: 32 Gb HDD (типа SSD, SAS или NVMe).

3. Сценарий высокой нагрузки с локальной отказоустойчивостью

Если в сети находится менее 1000 точек доступа (т.е. менее 10000 одновременно работающих гостевых клиентов) или корпоративная авторизация требует менее чем 1000 эндпоинтов, рекомендовано создать отказоустойчивый кластер PostgreSQL. Такой кластер требует двух или трёх узлов (primary, secondary), причем только два из них несут копию базы, а третий участвует в кворуме. Также желательно вынесение прокси-сервера на отдельный узел для того, чтобы перенести нагрузку обработки SSL-трафика с сервера приложения.



В случае аварии основного сервера PostgreSQL (на схеме справа) система WNAM 2 автоматически переключит запись/чтение на резервный сервер СУБД (на схеме слева).

В таком случае понадобится три одинаковых сервера с характеристиками:

- количество виртуальных процессоров: 4-8 vCPU;
- оперативная память: 16 Gb vRAM;
- объем жесткого диска: 50 Gb HDD (любого типа) системные диски.

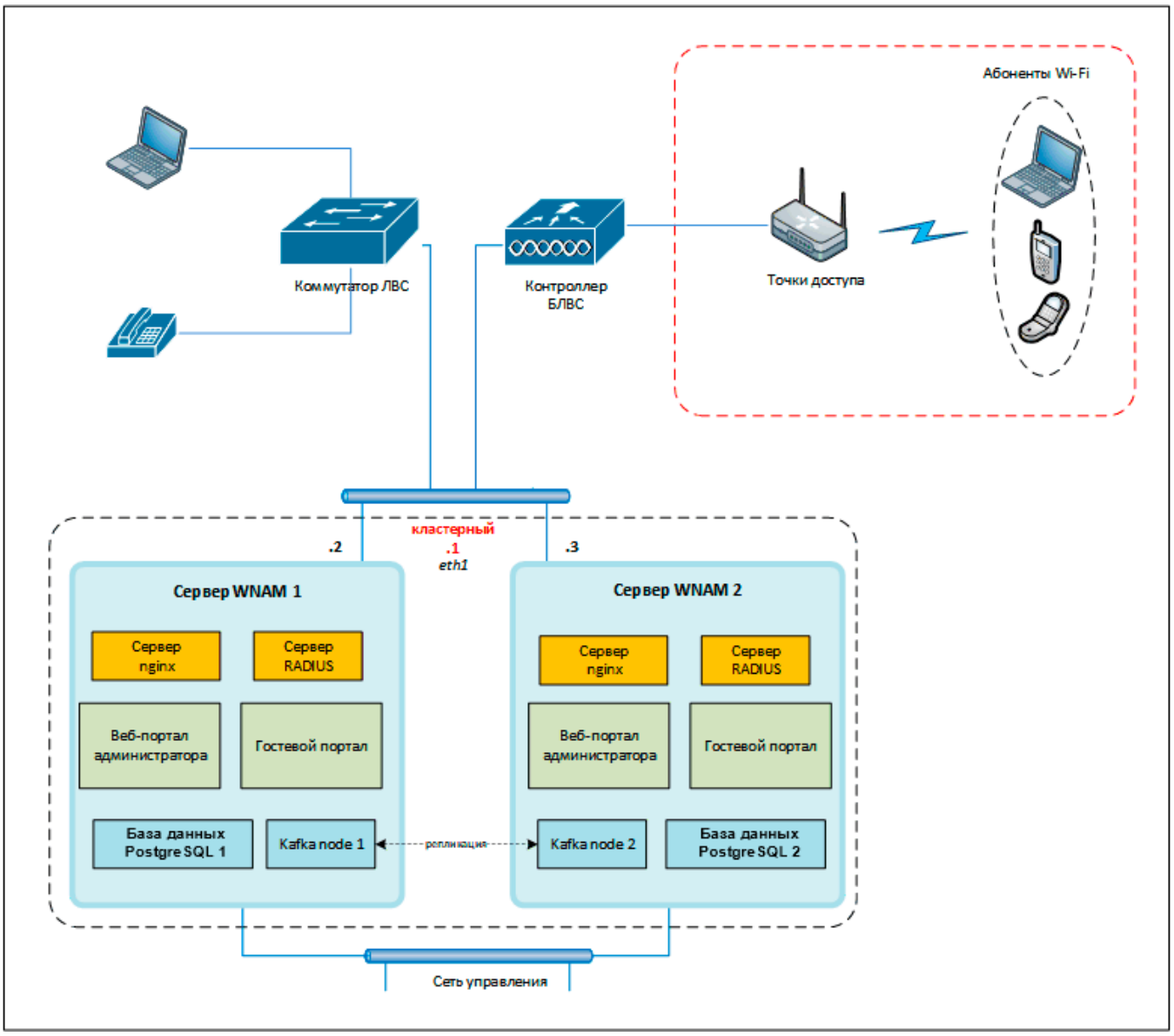
Дополнительно для двух серверов PostgreSQL (primary, secondary) необходимо:

- объем жесткого диска: 50 Gb HDD (типа SSD) - для СУБД;
- объем жесткого диска: 500 Gb HDD (типа SATA) - для дампов СУБД.

4. Сценарий средней нагрузки с распределенной отказоустойчивостью

Если сеть соответствует характеристикам сценариев 2 или 3, но при этом требуется получить полную отказоустойчивость системы, при которой её работоспособность сохраняется при выходе из строя одного из серверов системы WNAM 2, можно использовать сценарий средней нагрузки с распределенной отказоустойчивостью.

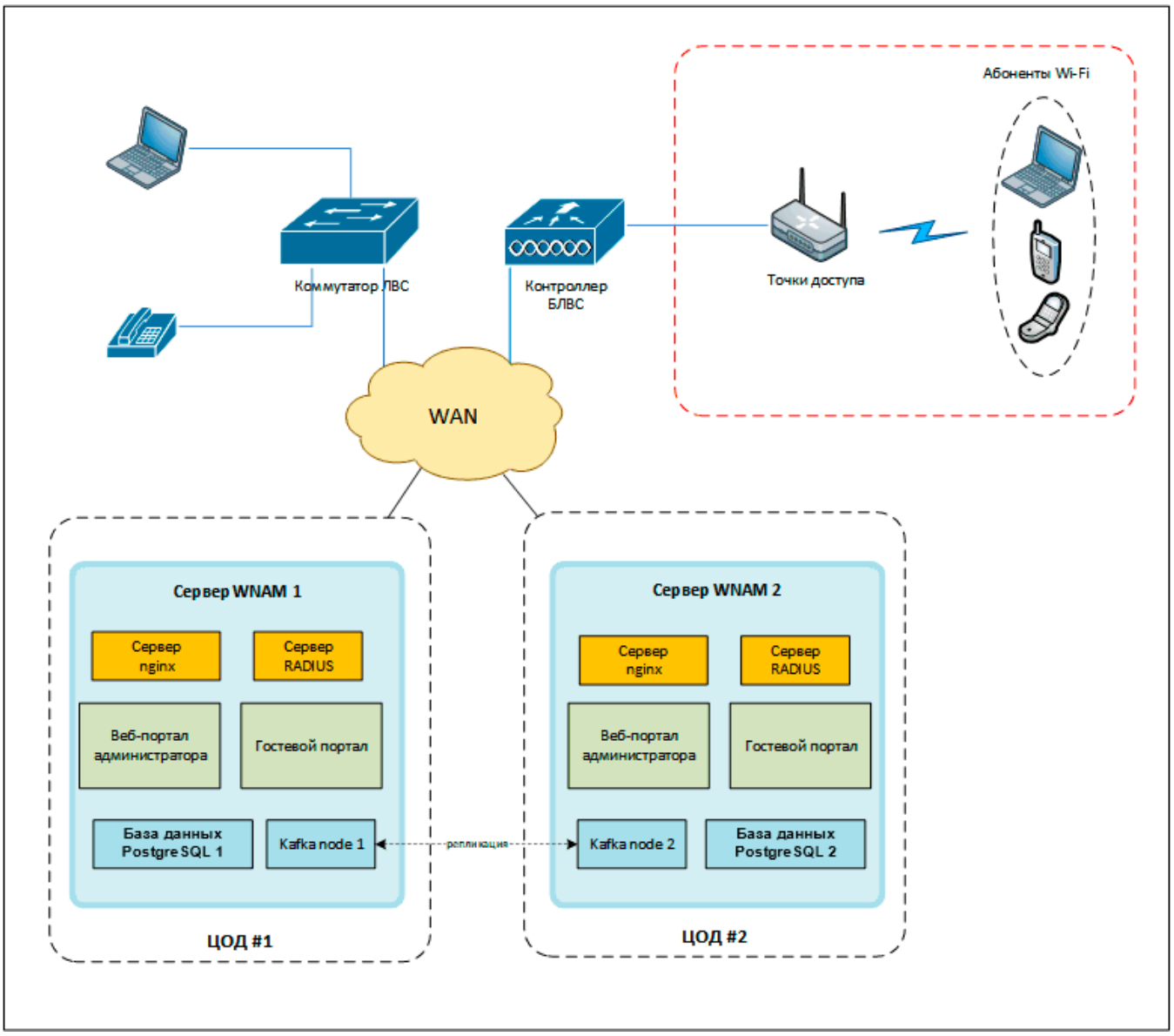
При таком сценарии (4.1) репликация данных производится не средствами кластера СУБД PostgreSQL, а путем пересылки информационных сообщений между двумя разрозненными автономными инстансами (экземплярами) PostgreSQL, каждый из которых взаимодействует только с локальным экземпляром системы WNAM 2.



В таком режиме понадобится настроить репликацию данных средствами Kafka.

Для административного доступа в веб-интерфейс, а также для редиректа HTTP-запросов клиентов от оборудования хотспота понадобится настроить кластерный IP-адрес серверов. Кластерный IP-адрес серверов (.1 на схеме) необходимо указать в качестве единственного адреса RADIUS-сервера на оборудовании.

Если не требуется использовать гостевой доступ, можно настроить любой из двух серверов системы WNAM 2 через веб-интерфейс, и в качестве RADUIS-сервера на используемом оборудовании указать оба IP-адреса (.2 и .3 на схеме).В случае аварии любого из серверов система продолжит выполнять свои функции. Преимуществом этого сценария является отсутствие необходимости иметь общий (кластерный) IP-адрес, что возможно лишь при нахождении обоих серверов в одном сетевом сегменте. Таким образом, можно настроить два сервера авторизации системы WNAM 2, находящихся в разных сетях (разных дата-центрах или даже разных городах), сценарий 4.2:

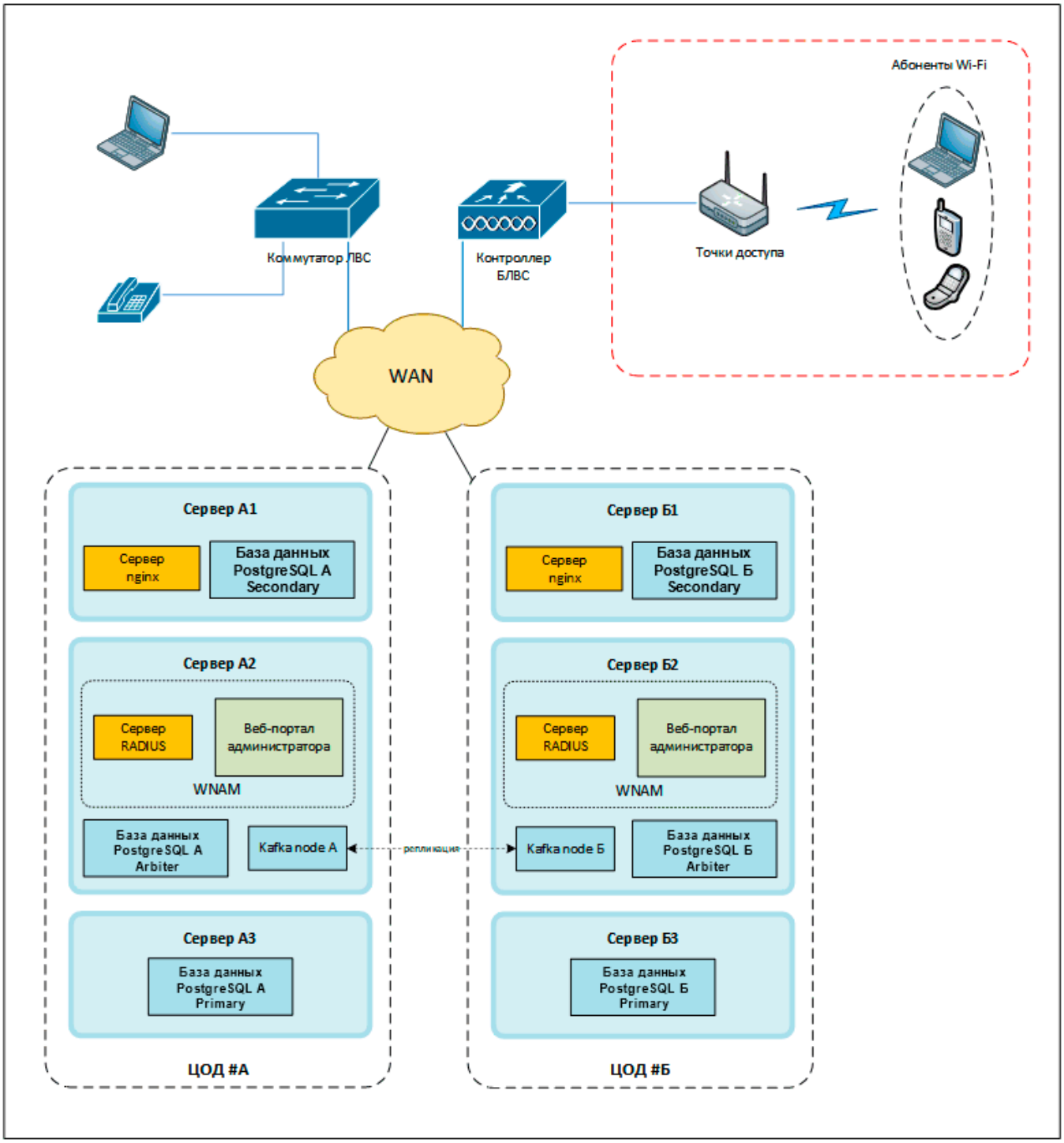


При настройке данного сценария понадобится два одинаковых сервера с характеристиками:

- количество виртуальных процессоров: 4-8 vCPU;
- оперативная память: 16 Gb vRAM;
- объем жесткого диска: 50 Gb HDD (любого типа) системные диски;
- объем жесткого диска: 50 Gb HDD (типа SSD) - для СУБД;
- объем жесткого диска: 500 Gb HDD (типа SATA) - для дампов СУБД.

5. Сценарий высокой нагрузки с распределенной отказоустойчивостью

Если нагрузка превышает характеристики сценария 3, и требуется обеспечить полную отказоустойчивость системы, возможно разнесение ролей системы авторизации на отдельные сервера и виртуальные машины в каждом экземпляре кластера. При этом в пределах узла кластера обеспечивается локальная отказоустойчивость и распределение нагрузки, а между узлами кластера - репликация конфигурационных и статистических данных.

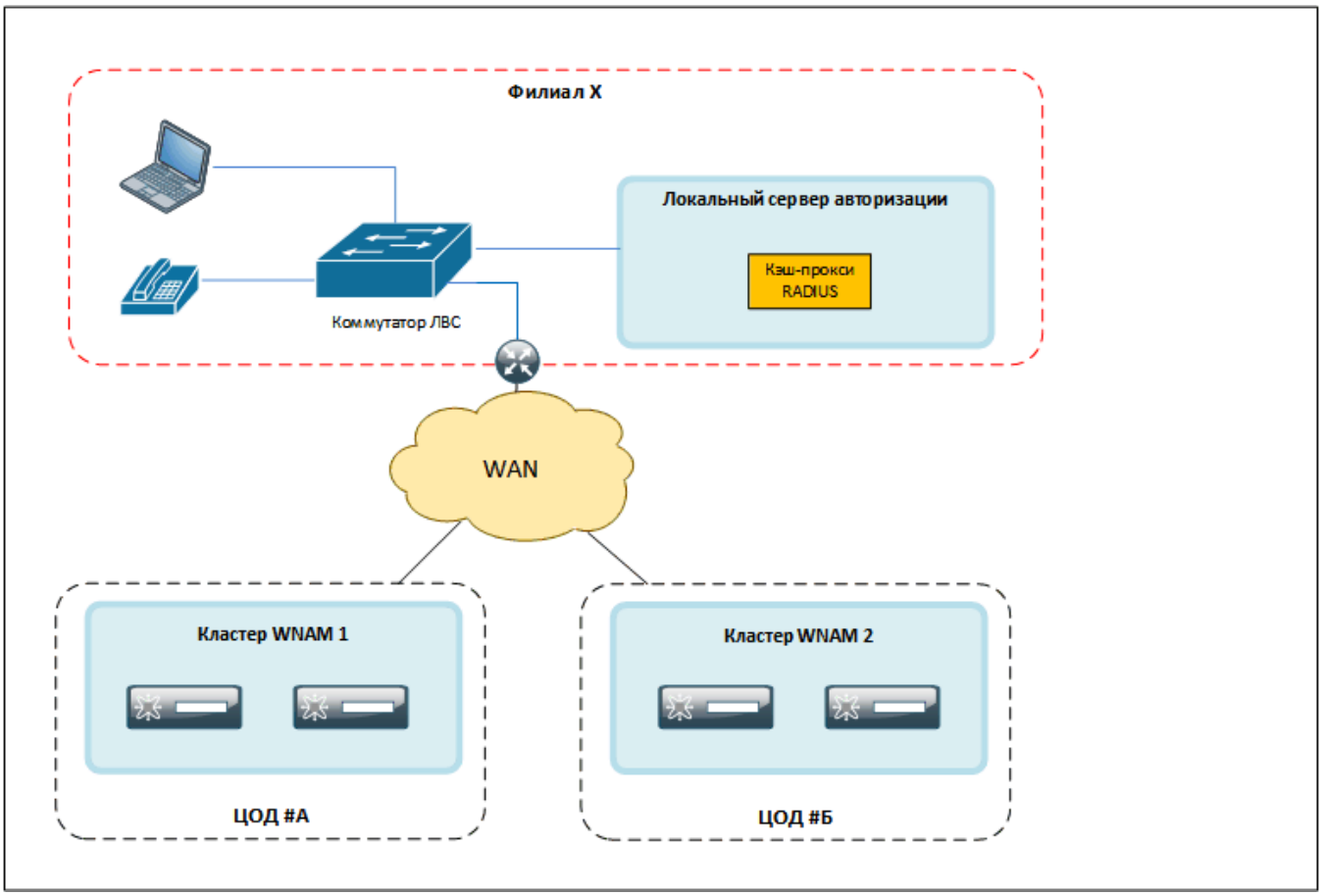


В данном сценарии понадобится создать два или три (по числу имеющихся площадок ЦОД) одинаковых кластера системы WNAM 2 в составе трех серверов, каждый из которых должен иметь такие характеристики:

- количество виртуальных процессоров: 8 vCPU;
- оперативная память: 32 Gb vRAM;
- объем жесткого диска: 50 Gb HDD (любого типа) системный диск;
- объем жесткого диска: 50 Gb HDD (типа SSD) - для СУБД (для серверов 1 и 3);
- объем жесткого диска: 500 Gb HDD (типа SATA) - для дампов СУБД (для сервера 2).

6. Сценарий высокой нагрузки с распределенной отказоустойчивостью и поддержкой изолированной работы

Если имеется множество (сотни) удалённых площадок (сайтов), с которыми невозможно гарантировать постоянное наличие сетевой связи как минимум с одним из ЦОД, в котором работает экземпляр системы WNAM 2, необходимо сформировать сетевую конфигурацию, при которой даже при отсутствии сетевой связности будет обеспечиваться работоспособность корпоративной авторизации. При этом допустима деградация услуги (например, увеличение длительности процесса авторизации, невозможность изменения настроек и/или просмотра статистики, невозможность обеспечить подключение новых устройств и т. п.). В таком случае, на каждой такой площадке необходимо установить специализированного агента авторизации (RADIUS-прокси/кэширующий сервер). В обычном режиме работы он прозрачно пропускает через себя запросы авторизации, маршрутизируя их в сторону доступных ЦОД с работающей системой WNAM 2. Результат авторизации сохраняется. При разрыве сетевой связности этот сервер проводит авторизацию устройств самостоятельно, пользуясь накопленными ранее данными.



При этом в каждом филиале потребуется развернуть виртуальную машину или Docker-контейнер с ПО, имеющим следующие требования:

- количество виртуальных процессоров: 1-2 vCPU;
- оперативная память: 2 Gb vRAM;
- объем жесткого диска: 16 Gb HDD (любого типа).

Взаимодействие компонентов

В состав системы WNAM 2 входит значительное число системного и прикладного ПО, которое взаимодействует друг с другом в пределах одного сервера (виртуальной машины), а также между серверами. В дополнение к этому, система взаимодействует с внешним миром (сервера доступа, пользовательские устройства, администраторы) по различным протоколам стэка TPC/IP. Описание такого обмена приведено в соответствующем разделе.

Резервное копирование

Настоятельно рекомендуется настроить резервное копирование системы WNAM 2 одновременно по обоим направлениям:

- для серверов, на которых работает PostgreSQL: через cron (демона-постановщика задач систем Unix) по расписанию, раз в сутки ночью, дамп базы данных в файлы, на другой (относительно основного) физический диск, с удалением старых резервных копий;
- резервное копирование виртуальной машины целиком, используя средства резервного копирования используемой платформы виртуализации.

При использовании кластерного варианта PostgreSQL можно не копировать разделы, содержащие файлы БД (в любом случае восстановить из "горячего бэкапа" кластерную БД не получится). Резервное копирование виртуальных машин должно включать в себя копии дампов БД, которые должны формироваться до того, как проводится процедура бэкап.

Системные требования

Для своей работы система WNAM 2 требует соответствующего аппаратного обеспечения (компьютера), операционной системы, обязательного и дополнительного прикладного программного обеспечения.

В качестве компьютера подойдет любой сервер или рабочая станция с современными характеристиками. Также полностью поддерживается возможность размещения системы WNAM 2 на виртуальной машине. Требуемые характеристики сервера напрямую зависят от планируемой нагрузки (число пользователей, поток запросов авторизации, объем базы данных).

Для задач среднего уровня:

- число пользователей в БД до 100 тысяч;
- порядка 1 запроса авторизации в секунду;
- до 500 одновременно работающих пользователей;
- хранение статистики до 12 месяцев,

рекомендуется сервер с 8 Гб ОЗУ, 2-4 ядрами, 100 Гб диском. Поскольку система WNAM 2 написана на языке Java, программы на котором отличаются повышенными требованиями к оперативной памяти, поэтому при большем числе одновременно работающих пользователей рекомендуется иметь от 8 до 16 Гб ОЗУ. При большом предполагаемом объеме БД, или если планируется активно пользоваться инструментами создания отчетности, рекомендуется применять быстрые (серверные, не бытовые) жесткие диски типа SSD. Следует позаботиться о наличии источника бесперебойного питания к вашему серверу, кондиционера в серверном помещении, если есть возможность - раздельных входящих электрических линий и двух блоков питания в сервере.

Расчёт требуемой дисковой ёмкости должен быть основан на длинах единичной записи, представленных в таблице.

session (сессия абонента)	500	550	3
customer (абонент)	1000	1200	1
log (лог)	380	400	4
flow (поток NetFlow)	325	350	100
adStat (показ рекламы)	240	325	2
smsStat (СМС)	240	280	1

Предельные гарантированные показатели производительности системы WNAM 2 (в кластерной конфигурации и при использовании высокопроизводительного оборудования) только для гостевой авторизации составляют:

1. Количество зарегистрированных абонентов в базе данных: не менее 1.000.000 шт.
2. Количество записей о сессиях в базе данных: не менее 100.000.000 шт.
3. Количество записей о потоках NetFlow версий 5 и 9 в базе данных: не менее 1.000.000.000 шт. (при использовании nfdump)

Для корпоративной авторизации системы WNAM 2 необходимо ознакомиться с разделом, посвященному тестированию производительности.

Система WNAM 2 полностью поддерживает работу в среде виртуализации (тестировано на VMware ESXi 5.0 и выше).

Для работы в отказоустойчивой (кластерной) конфигурации потребуется как минимум два сервера (физических или виртуальных), размещённых в одном сегменте ЛВС, либо в разных ЦОД в зависимости от выбранной схемы кластеризации. Для целей кворума кластера потребуется установить третий сервер (виртуальную машину с минимальной конфигурацией). Кластерная конфигурация системы WNAM 2 лицензируется отдельно.

Приложение написано в платформонезависимом виде (100% Pure Java), поэтому работает везде, где может работать Java JDK. Протестирована работа в среде Linux (Ubuntu, Debian, CentOS, AstraLinux, RedOS, Ubuntu, ОС ОСнова) под управлением Oracle и OpenJDK 1.8+. Настоятельно рекомендуется использовать ОС Debian последней версии. Работа под управлением FreeBSD возможна, но тестирование не проводилось. Для продуктивной работы рекомендуется использовать ОС семейства Linux, работающие в виртуальном окружении VMware, так как подобные системы более надежны, их проще администрировать, создавать резервные копии, масштабировать. Работа под ОС Windows поддерживается только в экспериментальном режиме в ознакомительных целях.

Также необходимо настроить межсетевой экран на вашем сервере. Как минимум, следует разрешить доступ по порту TCP:80 к веб-серверу в приложении WNAM 2, а также ssh (TCP:22) для управления, UDP:1812 и UDP:1813 для работы с RADIUS-сервером (только с ваших, определенных сетей). Подробнее список требуемых портов перечислен в данном разделе.

Для версии системы **WNAM 2** обязательными компонентами прикладного программного обеспечения являются:

- среда выполнения Java runtime (JRE или JDK в виде Oracle Java или OpenJDK/JRE) версии 11 или 17 (не 1.8);
- база данных PostgreSQL 14 либо PostgresPro 14 или старше
- веб-сервер Nginx 1.10 и выше ;
- браузер PhantomJS 2.1.1.

Взаимодействие компонентов

Используемые TCP/IP порты

Для работы системы WNAM 2 используются порты и протоколы, которые необходимо настроить на межсетевом экране вашего сервера, или промежуточных межсетевых экранах.

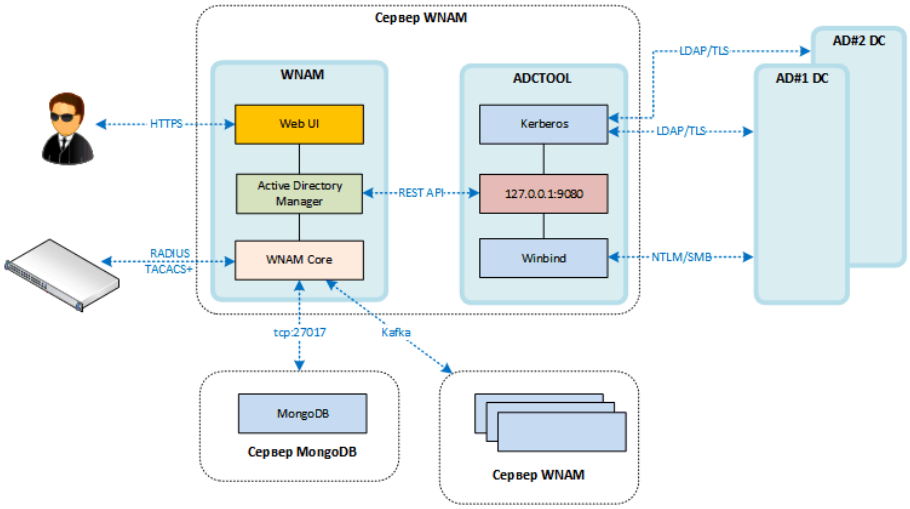
Протокол и порт	Направление	Назначение
tcp/80	к серверу	Веб-интерфейс администратора, менеджера клиента или подразделения. Пользовательские страницы портала (авторизация и реклама).
tcp/443	к серверу	Защищенное SSL соединение для веб-управления, и портала авторизации абонентов.
udp/1812	к серверу	Запросы авторизации от RADIUS-клиентов (NAS, сетевое оборудование) к RADIUS-серверу системы WNAM 2
udp/1813	к серверу	Сообщения аккаунтинга от RADIUS-клиентов (NAS, сетевое оборудование) к RADIUS-серверу системы WNAM 2
udp/1700, udp/3799	от сервера	Запросы PoD и CoA к серверам доступа Cisco ISG, Cisco WLC, Alcatel-Lucent.
udp/2000	от сервера	Запросы китайского портального протокола (аналог CoA) к серверам доступа Huawei, DCN, Ruijie, H3C, Maipu.
tcp/8728	от сервера	Запросы на определение DHCP-идентификаторов абонентов (к маршрутизаторам Mikrotik через API).
tcp/443, tcp/3000, tcp /9080 и т.п.	от сервера	Авторизация абонента и запросы на определение их DHCP-идентификаторов (к контроллерам БЛВС некоторых вендоров).
tcp/443	от сервера	Проверка действительности лицензии системы WNAM 2 на серверах ООО "Нетамс" (если нет offline-лицензии).
udp/20001	к серверу	Сообщения подтверждения звонков авторизации от агента, установленного на сервере Asterisk, либо DHCP-привязки от ISC-DHCPD / Kea, либо коллектора DHCP трафика для подсистемы профилирования.
udp/20002	к серверу	Трафик статистики Netflow v5 от маршрутизаторов (серверов) доступа.
tcp/5432	от сервера	Трафик обращений к СУБД PostgreSQL, если она работает на соседнем с системой WNAM сервере.
udp/123	от сервера	Трафик протокола синхронизации времени NTP

Дополнительно, если в вашей системе используется механизм корпоративной авторизации, понадобится следующий сетевой доступ:

Протокол и порт	Направление	Назначение
tcp/88	от сервера	Kerberos трафик от сервера системы WNAM 2 до серверов контроллеров домена ОС Windows.
udp/389, tcp /389, tcp/636	от сервера	LDAP, LDAPs (TLS in LDAP) трафик от сервера системы WNAM 2 до серверов контроллеров домена ОС Windows
udp/53, tcp/53	от сервера	DNS трафик до серверов контроллеров домена ОС Windows
udp/137-139, tcp /137-139,445	от сервера	NetBios и SMB трафик до серверов контроллеров домена ОС Windows
tcp/80	от сервера	HTTP-трафик от сервера системы WNAM 2 до серверов ОС Windows PKI для проверки CRL-списков отзывов сертификатов.

tcp/9080	от сервера	Трафик от сервера системы WNAM 2 до отдельно стоящего сервера с интеграционным модулем ADCTool, который используется для связи с MS Active Directory/FreeIPA (если таковой не работает совместно с системой WNAM 2 на одном сервере на localhost).
tcp/49	к серверу	TACACS+ запросы от сетевого оборудования для авторизации административного доступа.
tcp/9092	к серверу	Трафик кластера Kafka в случае кластеризации системы WNAM 2
udp/161	от сервера	Опрос коммутаторов по протоколу SNMP для определения CPD, LLDP-соседей (динамическое профилирование эндпоинтов)

Эти связи также схематически отражены на рисунке.



При проектировании и пуско-наладке системы WNAM 2 рекомендуется на каждом из серверов, участвующих в работе системы, настроить собственный межсетевой экран iptables / nftables.

Лицензии

Система управления сетевым доступом WNAM 2 зарегистрирована в Реестре программ ЭВМ и БД 03 июня 2024 года под номером 2024662975. Исключительные права на это программное обеспечение принадлежат компании ООО "Нетамс", которая производит распространение ПО WNAM 2 по лицензионным договорам.

Полный текст лицензионного соглашения между правообладателем и конечным пользователем (лицензиатом) можно получить, направив запрос по адресу info@netams.com с указанием лицензионного ключа вашей системы.

Система управления сетевым доступом WNAM 2 написана на языке Java (JRE версии 17) с включением шаблонов, стилей и библиотек на CSS, HTML, JS. Лицензионная политика WNAM 2 целиком основывается на положениях ст. 1233 ГК РФ. Система WNAM 2 не является ПО с открытым кодом и не поставляется на условиях какой-либо открытой лицензии. Исключение составляют распространяемые в исходных текстах на языке C утилиты взаимодействия с АТС asterisk и dhcp-серверами (они предоставляются компанией ООО "Нетамс" на условиях лицензии Apache).

Для корректной работы системы WNAM версии 2 требуется ОС семейства Linux (возможно использовать любую версию 64-бит), в том числе Российского происхождения.

В составе ОС должны присутствовать стандартные системные утилиты, а также среда исполнения Java Runtime 17 (рекомендуется OpenJDK, лицензия https://openjdk.java.net/legal/).

Дополнительно для корректной работы системы WNAM 2 необходимо установить следующее стороннее ПО, лицензионная политика которого допускает бесплатное распространение и использование:

- прокси и веб-сервер nginx (https://nginx.org/ru/) - BSD-подобная лицензия ;
- сервер SMPP-подключений kannel - собственная открытая лицензия;
- утилита генерации превью страниц phantomjs (https://phantomjs.org/) – лицензия BSD;
- сервер БД PostgreSQL - BSD-подобная лицензия.

Распространяемый дистрибутив системы WNAM 2 содержит:

- набор скомпилированных в .class Java-файлов;
- страницы пользовательского интерфейса, скрипты, конфигурационные файлы, словари и т.п.;
- набор библиотек, подключаемых на стадии выполнения.

Исходные тексты системы WNAM 2, из которых собран (скомпилирован) дистрибутив, не содержат в каком-либо виде свободно распространяемого (открытого) ПО и не заимствованы из какого-либо проекта, программного продукта или приложения.

Библиотеки используют следующий набор лицензий:

1. Apache license:
    - Spring Boot (https://github.com/spring-projects/spring-boot/blob/master/LICENSE.txt);
    - PostgreSQL JDBC Driver (https://jdbc.postgresql.org/license);
    - Embedded Apache Tomcat (http://tomcat.apache.org/legal.html);
    - Jackson FasterXML;
    - Apache commons;
    - Apache HTTP client;
    - Apache MINA;
    - Google Guava (https://github.com/google/guava/blob/master/COPYING);
    - Иные узкоспециализированные java- и css/js библиотеки.
2. GNU LGPL:
    - Logback (http://logback.qos.ch/license.html);
    - Hibernate-common (https://hibernate.org/community/license/);
3. Собственные лицензии, основанные на открытых лицензиях:
    - Angular (https://angular.dev/license);
    - BouncyCastle (MIT-лицензия, http://www.bouncycastle.org/licence.html).

Включенные в состав дистрибутива библиотеки поставляются согласно открытым лицензиям, допускающим их бесплатное распространение и использование. Компания ООО "Нетамс" не вносит изменений в эти библиотеки и использует их "as is" в полном соответствии с лицензионными требованиями каждой из них.

Для использования системы управления сетевым доступом WNAM 2 не требуется приобретения каких-либо дополнительных платных лицензируемых продуктов, пакетов или иного проприетарного ПО. Исключение составляет лицензия ОС Linux либо СУБД PostgresPro, если вы предпочитаете использовать их платные версии.

Установка

Для установки и настройки системы WNAM 2, а также дополнительного ПО, необходимого для его корректной работы, потребуется выполнить ряд действий:

1. Настроить вашу проводную или беспроводную сеть в режиме работы "без авторизации". Этим вы предварительно проверите работоспособность всех сопутствующих сетевых служб: DHCP, NAT, DNS, маршрутизации, межсетевого экранирования. Для беспроводных сетей - корректности работы радио, туннелирования трафика от точек доступа. Зачастую бывает, что при настройке авторизации администратор сталкивается с проблемами неработоспособности клиентского устройства, и начинает искать проблему там, где её нет - в настройке сервера. Не следует приступать к настройке системы WNAM 2 до тех пор, пока используемая вами проводная или беспроводная сеть полностью не настроена и не протестирована в открытом режиме работы.
2. Подготовить физический или виртуальный сервер для системы WNAM 2.
3. Получить лицензионный ключ, и ключевой файл WNAM 2.
4. Если вы устанавливаете WNAM 2 на собственный экземпляр ОС:
    a. Установить ОС и выполнить её базовые настройки (локальные пользователи, IP-адреса, маршрутизация, межсетевой экран).
    b. Установить и настроить системное ПО: PostgreSQL, java, nginx, kafka- если вы устанавливаете WNAM на собственный экземпляр ОС.
    c. Загрузить дистрибутив (deb-пакеты) и установить компоненты приложения WNAM 2.
    d. Провести редактирование базовых параметров в файлах конфигурации **application.yaml**.
    e. Настроить актуальное время на сервере
    f. Запустить сервисы WNAM 2.
5. Если вы устанавливаете WNAM 2 из образа (ISO, OVF, VMDK):
    a. Загрузить образы, импортировать их в среду виртуализации, либо записать на USB-носитель
    b. Загрузить физический/виртуальный сервер, проведя установку (ISO)
    c. Настроить актуальное время на сервере
    d. Запустить сервер
    e. Выполнить базовые настройки ОС (локальные пользователи, IP-адреса, маршрутизация, межсетевой экран).
6. Проверить запуск системы WNAM 2 анализом лог-файлов приложений.
7. Через веб-интерфейс настроить систему WNAM 2 (лицензионный файл и ключ, сетевые устройства, местоположения, правила аутентификации и авторизации, пользователи).
8. Провести тестирование подсистемы авторизации, средств формирования отчетности.
9. При необходимости, собрать кластерную конфигурацию серверов.
10. При необходимости, установить дополнительные средства мониторинга на ваш сервер.

Подробная информация по каждому из приведенных действий представлена в следующих разделах настоящей документации.

Из образа ISO

Для начала установки загрузите последний ISO образ по ссылке, полученной в welcome-письме, или предоставленной службой технической поддержки. Перепишите образ в хранилище системы виртуализации, либо запишите его на USB Flash носитель (размером от 4 Гб).

Подготовьте пустую виртуальную машину со следующими характеристиками:

- vCPU: не менее 2 ядер, для продуктивной эксплуатации от 4 до 16 ядер
- vRAM: не менее 8 Гб, для продуктивной эксплуатации от 16 до 32 Гб
- vHDD: как минимум один раздел размером 32 Гб, для продуктивной эксплуатации обязательно использование SSD/NVMe носителя; возможно подключение второго (SATA/SAS) тома объемом 100 Гб для хранения резервных копий и лог-файлов
- Network: как минимум один сетевой адаптер
- Тип операционной системы: Linux x64, самой высокой доступной версии (нами используется ядро 5.x)

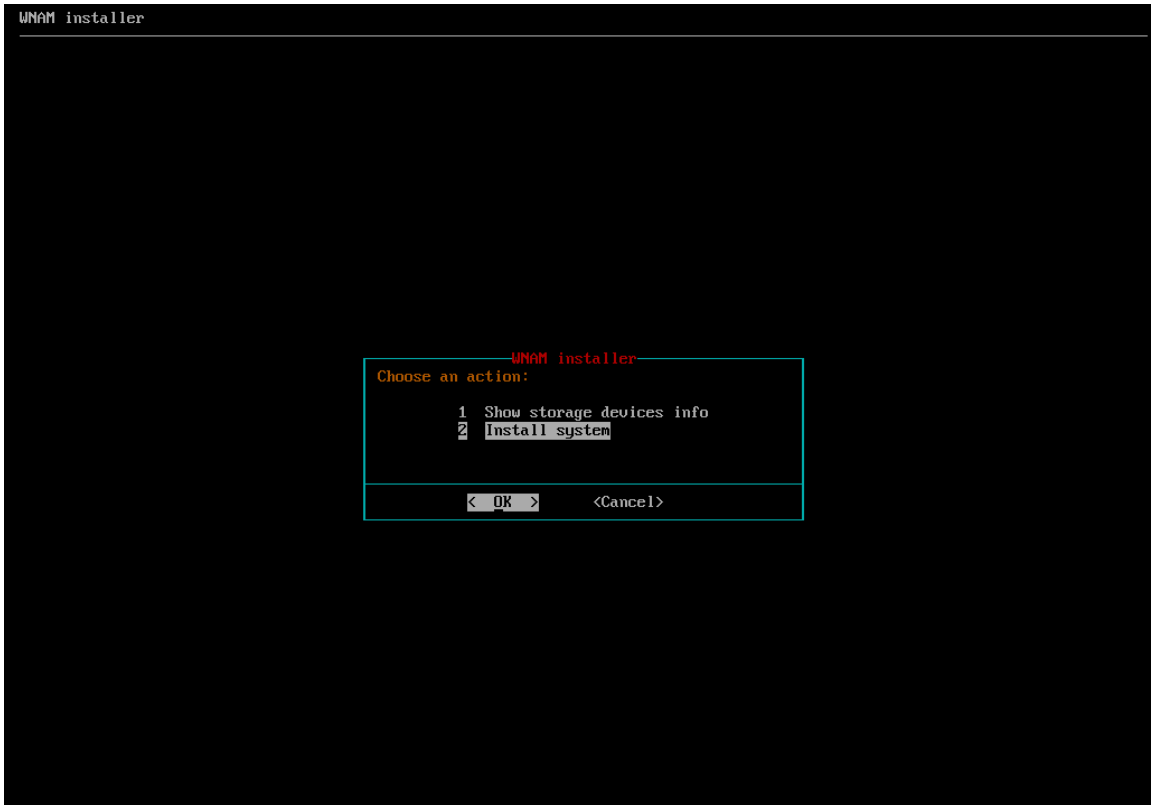
Подключите ISO-образ в виртуальную машину, и включите её. Убедитесь, что загрузка будет происходит с образа. Установка будет происходить в два этапа. Первый - развертывание образа (слепка с целевой) системы, второй - установка пакетов WNAM 2, и зависимостей.

Внимание! Предоставляемый образ исходно содержит в себе три программных системы, поставляемые нашей компанией: WNAM 1.6, WNAM 2, WNAM QoW. В конце установки выбирается, какая из систем должна быть запущена. Остальные дистрибутивы ПО деактивируются.

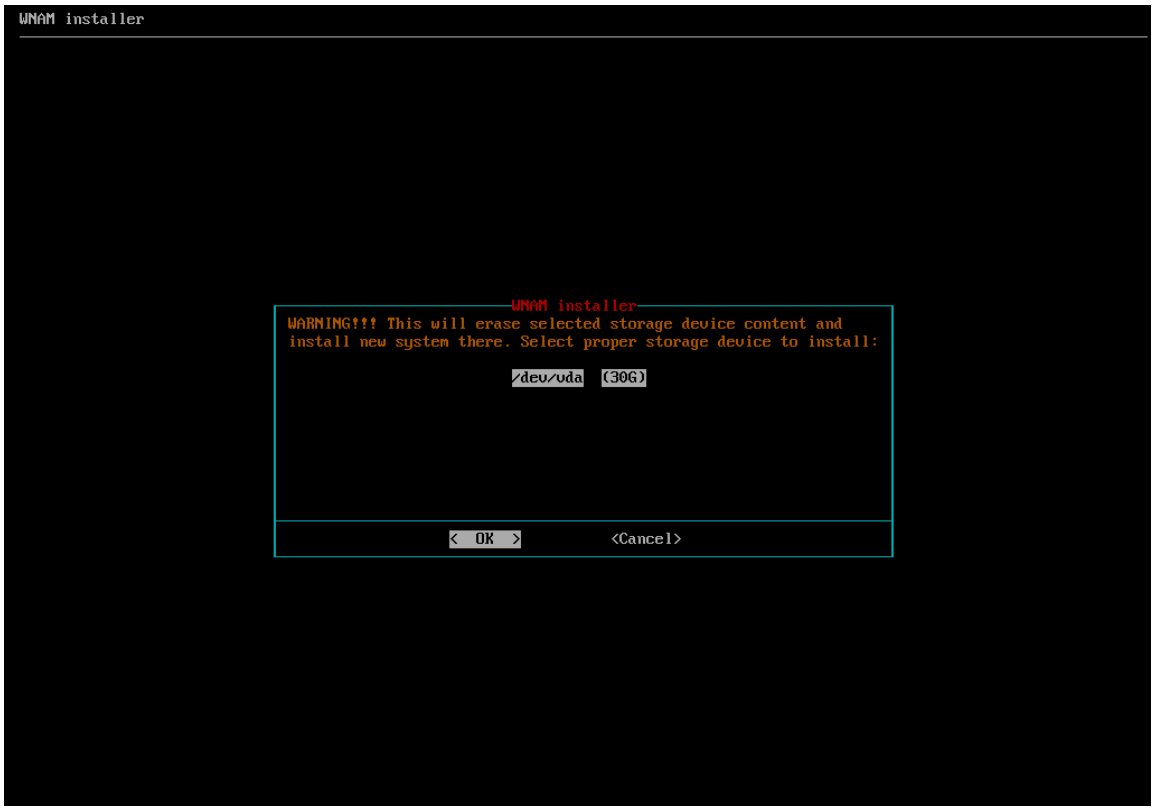
Внимание! Образ, который вы получите, основан на операционной системе Astra Linux 1.7.6 "Смоленск". Если вы планируете перевести сервер в промышленную эксплуатацию, вы должны приобрести лицензию на эту ОС. В случае поставки ПО WNAM 2 в составе ПАК, лицензия на ОС также будет предоставлена в комплекте.

Развертывание системы

1. После загрузки с ISO образа на экране появиться возможность просмотра информации о доступных дисках, и предложено начать установку системы

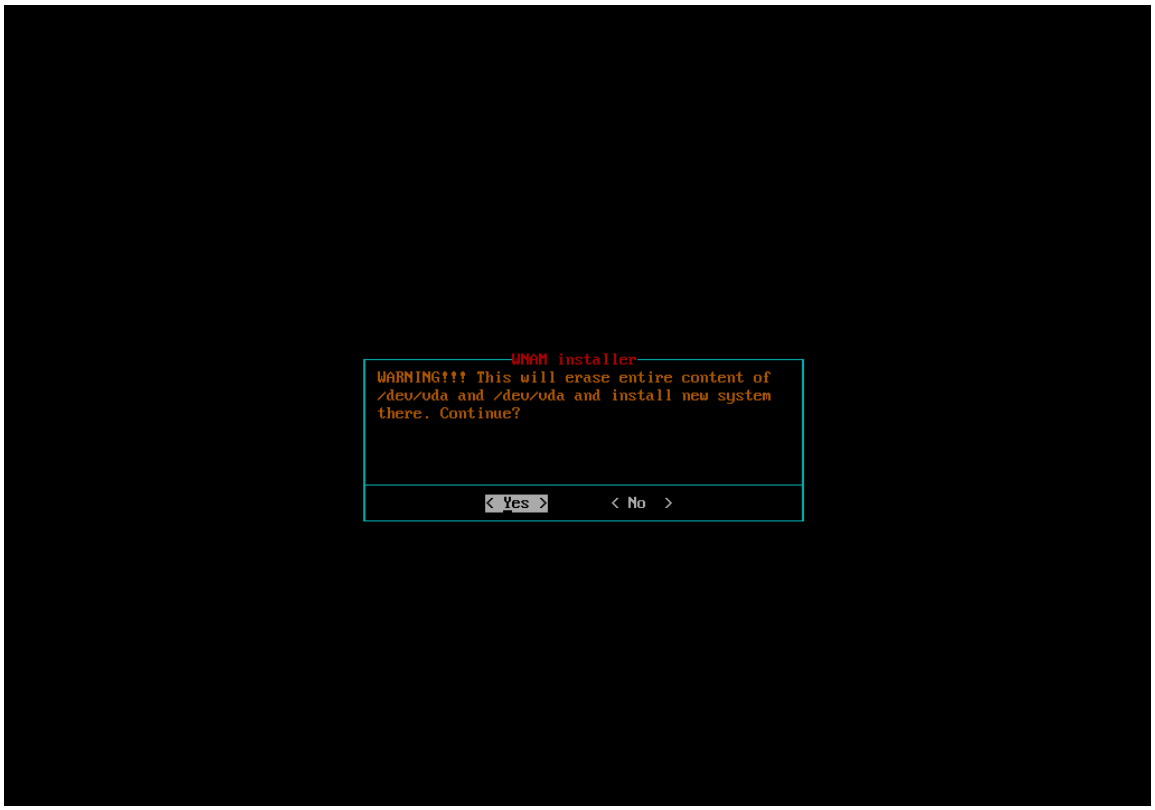


2. Следует выбрать, на какой диск установить систему



3. Предлагается возможность хранения логов на отдельном диске, если он найден

4. Предупреждение о том, что вся информация с выбранных дисков будет удалена

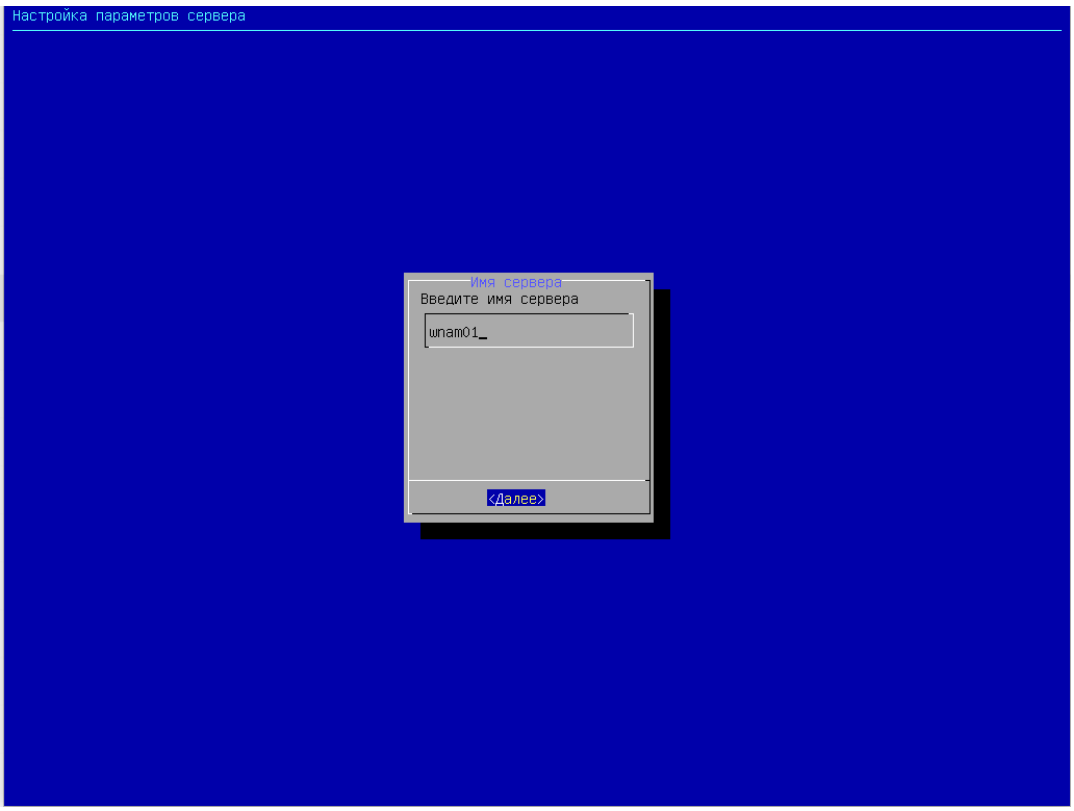


После этого начнется установка системы, и произойдет перезагрузка сервера. После перезагрузки убедитесь, что виртуальная машина загружается с диска, куда была установлена система.

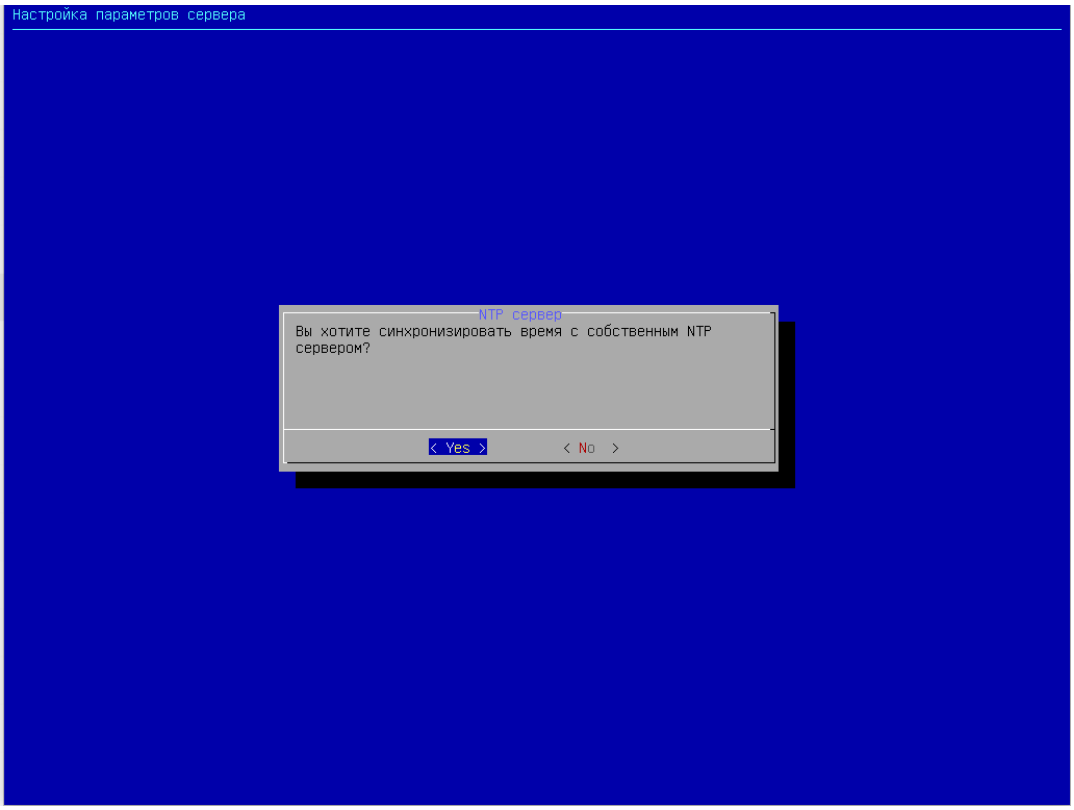
Установка пакетов WNAM 2, и зависимостей.

По окончанию загрузки на экране появится приглашение для ввода логина и пароля (учетные данные по умолчанию находятся в файле readme.txt, который расположен в репозитории рядом с образом)

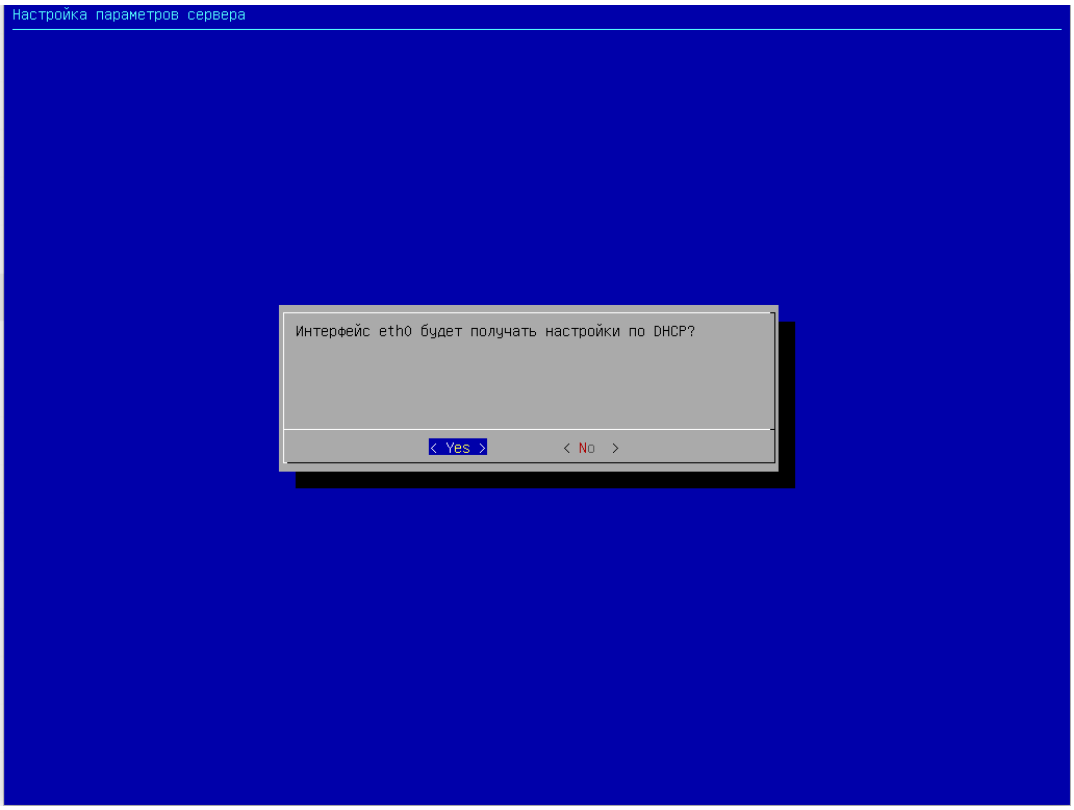
Автоматически, в первый раз, будет запущен скрипт настройки сервера. Установите имя сервера. Следует помнить, что если планируется интеграция WNAM 2 с Microsoft Active Directory, имя сервера должно быть не более 11 символов длиной (ограничение NETBIOS).



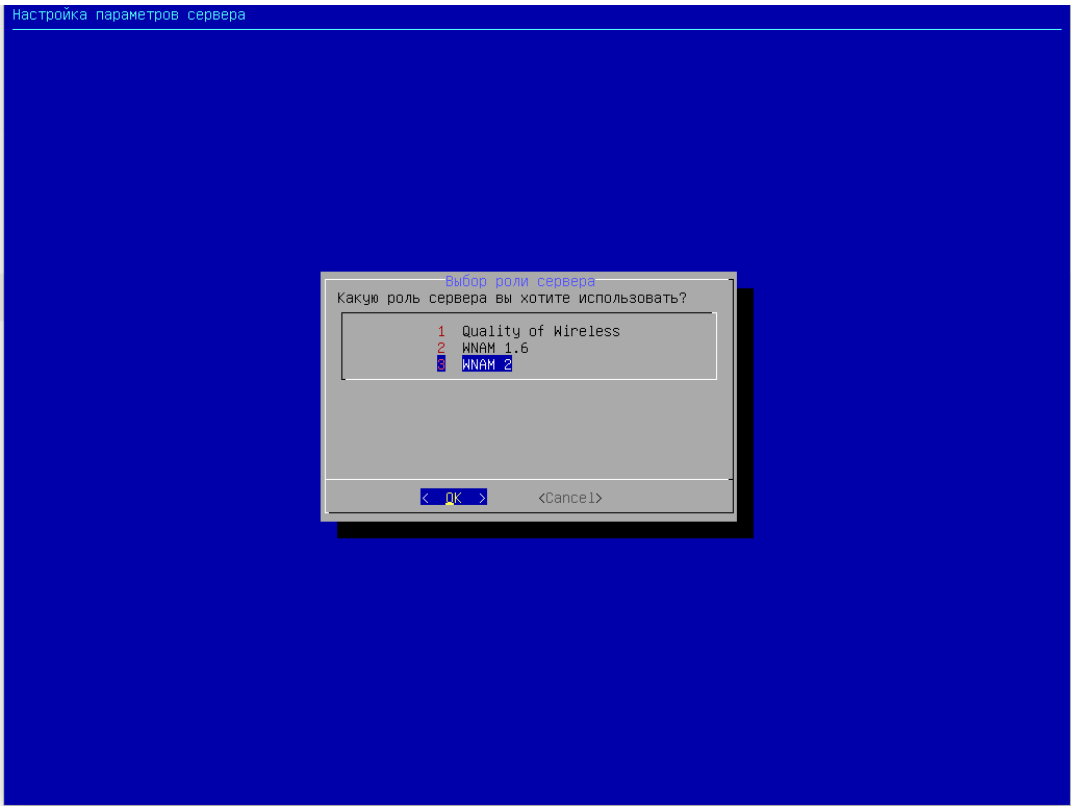
Ннастройте синхронизацию времени



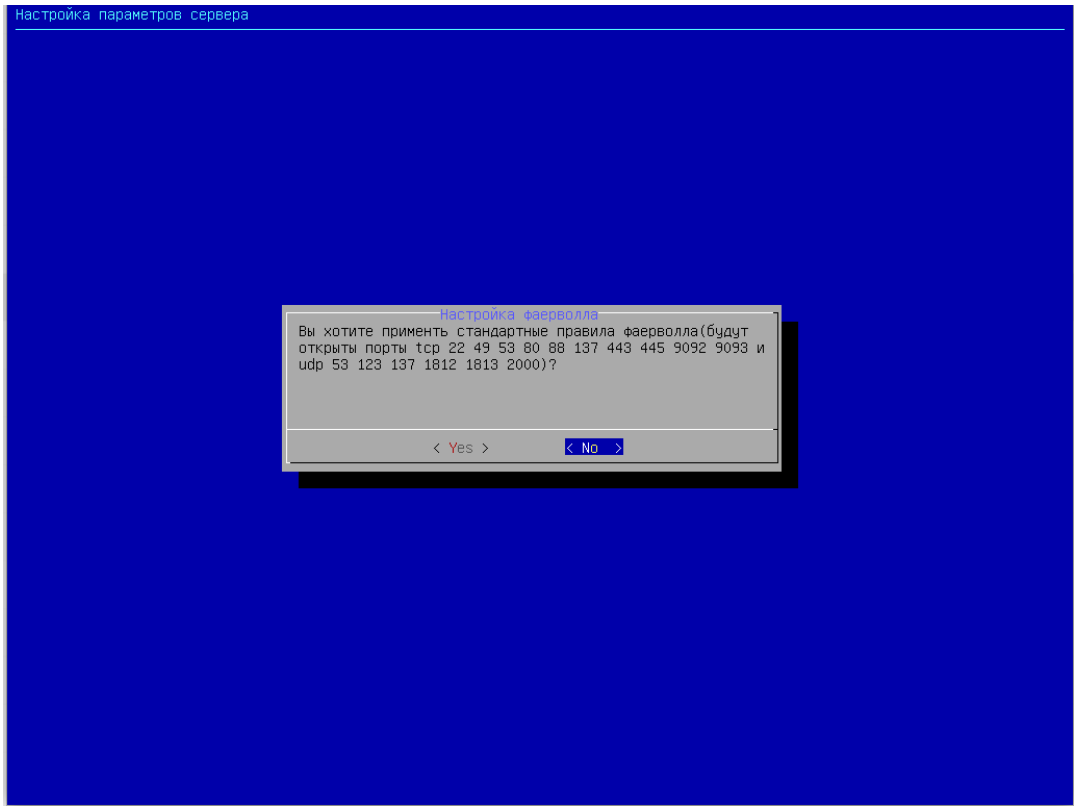
Настройте сетевые интерфейсы



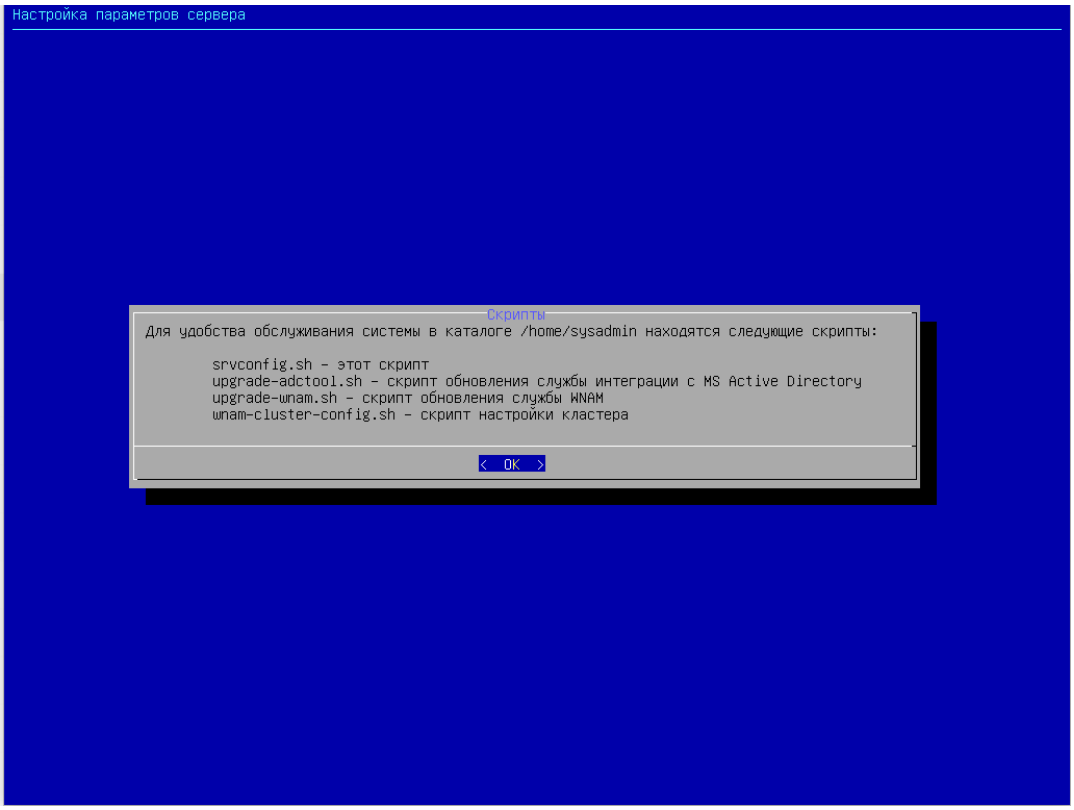
Выберите, какой из программных продуктов вы будете запускать



Произведите настройку межсетевого экрана сервера (правила iptables)



Скрипт первоначальной настройки вы всегда можете запустить заново

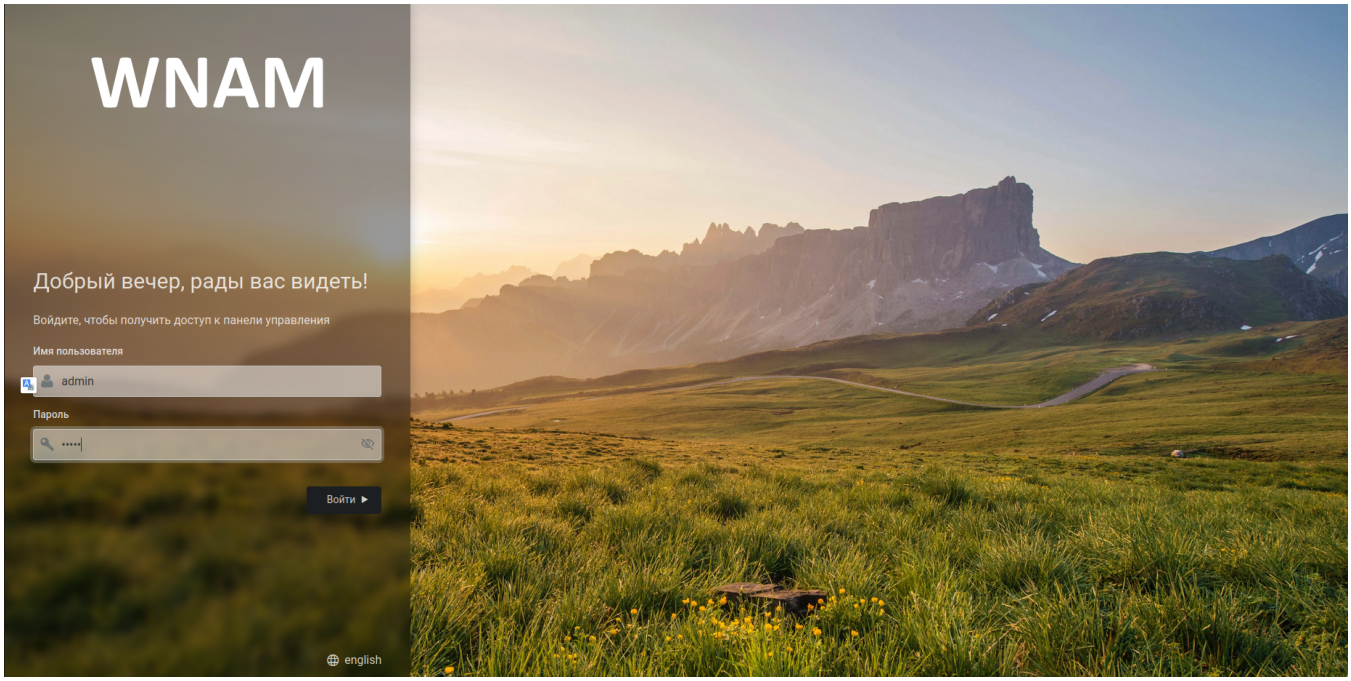


На возможные ошибки запуска сервиса kafka можно не обращать внимания. Затем он будет работать хорошо, когда вы настроите кластер. В безкластерной конфигурации этот сервис не нужен (можно сделать systemctl disable kafka).

Произойдет перезагрузка системы.

После перезагрузки можно попасть в интерфейс систему управления сетевым доступом WNAM2 по адресу http://ip_сервера

Имя пользователя по умолчанию admin , пароль admin



Из образа VM

В настоящий момент сборка актуальных образов в формате OFV/VMDK приостановлена. Вы можете установить систему WNAM 2 из ISO-образа с тем же конечным результатом.

Вручную

Формирование кластера

WNAM 2 поддерживает объединение нескольких узлов (серверов), называемых "ноды", в один общий кластер. Узлы кластера имеют общую конфигурацию, общие данных по эндпоинтам, по статистике подключений (сессии) и функционируют как единое целое в режиме Active-Active. Каждая из нод имеет собственную, локальную базу данных Postgres. Репликация данных между нодами реализуется посредством брокера kafka (а не средствами Postgres). Изменение настроек системы через веб-интерфейс одной ноды автоматически за считанные секунды распространяется и на другие ноды.

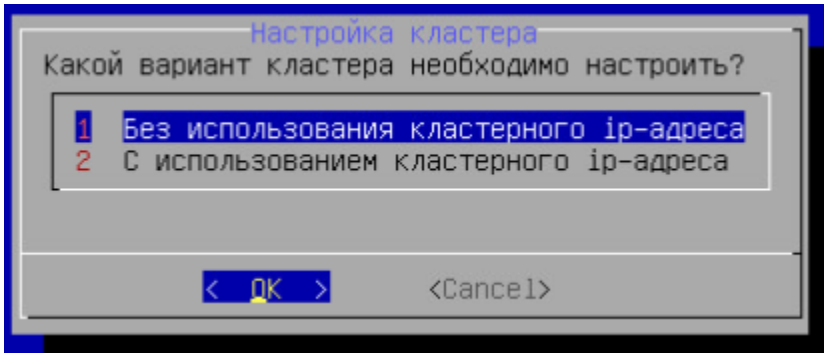
Рекомендуется создать кластер из нод WNAM 2 на самых ранних стадиях настройки системы. Ноды могут располагаться как и в одной сети, так и в разных сетях или даже ЦОДах. Синхронизация данных ведется по TCP/IP, на 3м уровне модели OSI. Общий плавающий "кластерный" IP-адрес нодам не нужен, соответственно не нужен и сервис keepalived.

Нижеследующая инструкция предполагает, что у вас формируется кластер из двух нод, которые вы только что установили из ISO-образа на два разных сервера, с IP адресами 172.16.100.17 и 172.16.200.17 соответственно. После первоначальной установки и присвоения адресов серверам, они были перезагружены.

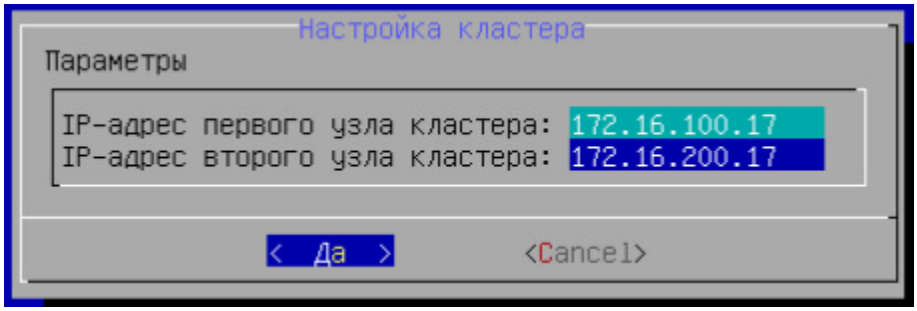
Поскольку операцию создания кластера требуется проводить всего один раз, для этой цели мы подготовили специальный shell-скрипт. Он находится в каталоге /home/sysadmin вашей системы, развернутой из образа. Скрипт настройки имеет название wnam-cluster-config.sh. Запустите его на первом сервере 172.16.100.17 с правами root:

```
sudo ./wnam-cluster-config.sh
```

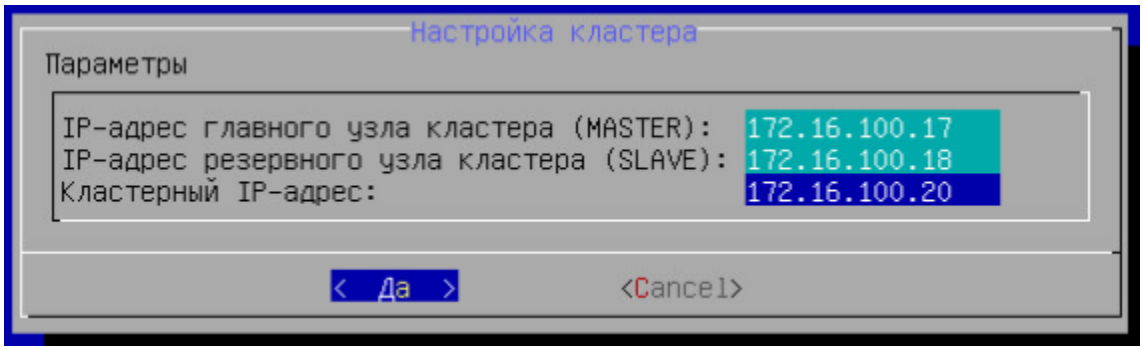
Для начала скрипт спросит какой вариант кластера вы хотите использовать: только репликация посредством kafka или репликация и использование общего кластерного ip-адреса (служба keepalived)



После выбора первого варианта скрипт выведет следующее окно настройки. Укажите там адреса обоих узлов кластера:



Для второго варианта настройки окно для ввода данных будет отличаться (в данном случае сервера должны находиться в одной подсети):



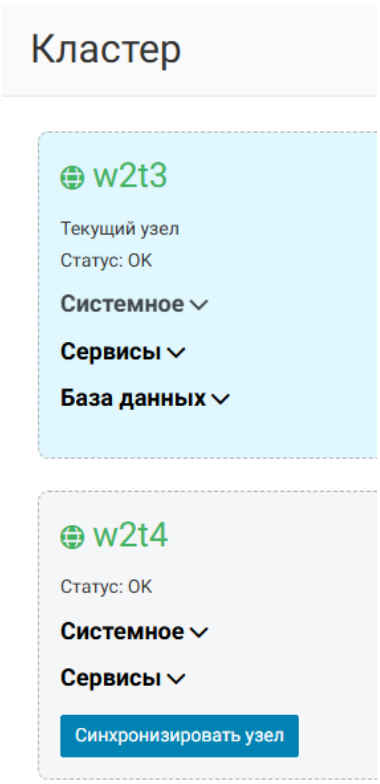
Нажмите кнопку "Да", дождитесь формирования конфигурационных файлов, запуска сервиса kafka, перезапуска WNAM.

Теперь, сделайте то же самое на втором сервере, 172.16.200.17.

> Внимание! Вы должны указать IP адреса узлов точно в той же последовательности, как и на первом сервере. Не поменяв их местами.

Также дождитесь формирования конфигураций, и перезапуска сервисов.

На любом из серверов зайдите в веб-интерфейс, и посмотрите на статус кластера в разделе Диагностика:



Если система напишет, что в очереди есть объекты на синхронизацию, нажмите на соответствующую кнопку.

Быстрый старт

Следующая ниже инструкция понадобится вам на первых шагах запуска системы WNAM 2 для авторизации администраторов (DeviceAdmin) и сетевых клиентов (NAC).

1. Запуск

При первом запуске системы WNAM 2 автоматически создаётся пустая БД с именем "wnam2_db" в работающем на сервере экземпляре СУБД PostgreSQL.

При выполнении команды

```
sudo journalctl -feu wnam2
```

должны появиться строки, отображающие этапы инициализации внутренних служб системы WNAM 2:

```
 08 11:46:12 wnam2t1 start.sh[16976]: 11:46:12.642 TRACE [com.netams.w2.cluster.AdminService:426]
- Check kafka connection...
 08 11:46:20 wnam2t1 start.sh[16976]: 11:46:20.002 TRACE [c.n.w.c.nodes.WnamClusterConsumer:28] -
Received cluster: WnamServer(id=wnam-cluster-d1e1, serverId=wnam-cluster-d1e1-71c2783549af,
main=true, time=1728377180000, customers=0, sync=false, info=null, systemInfo=SystemInfo(ram=18,
cpu=1, hdd=13), leader=true, address=1.1.1.1, version=2.0.568, role=master,
lastStartTime=1728285235376,failed=false) from
 08 11:46:20 wnam2t1 start.sh[16976]: 11:46:20.004 TRACE [c.n.w.c.nodes.lusterService:202] - Send
cluster: wnam-cluster-d1e1 to wnam-cluster-topic
 08 11:46:20 wnam2t1 start.sh[16976]: 11:46:20.426 TRACE [c.n.w.c.nodes.lusterConsumer:28] -
Received cluster: WnamServer(id=wnam-cluster-453e, serverId=wnam-cluster-453e-eaa226a63159,
main=true, time=1728377180000, customers=0, sync=false, info=null, systemInfo=SystemInfo(ram=16,
cpu=1, hdd=12), leader=true, address=1.1.1.2, version=2.0.568, role=master,
lastStartTime=1728285280017,failed=false) from
 08 11:46:22 wnam2t1 start.sh[16976]: 11:46:22.643 TRACE [com.netams.w2.cluster.AdminService:426]
- Check kafka connection...
 08 11:46:30 wnam2t1 start.sh[16976]: 11:46:30.002 TRACE [c.n.w.c.nodes.WnamClusterConsumer:28] -
Received cluster: WnamServer(id=wnam-cluster-d1e1, serverId=wnam-cluster-d1e1-71c2783549af,
main=true, time=1728377190000, customers=0, sync=false, info=null, systemInfo=SystemInfo(ram=18,
cpu=1, hdd=13), leader=true, address=1.1.1.1, version=2.0.568, role=master,
lastStartTime=1728285235376,failed=false) from
```

⚠ Внимание! Вышеприведённый набор строк является примером. Фактический результат может в незначительной форме отличаться от примера.

Если вместо них вы видите большой набор исключений (Exception), то скорее всего у вас:

- Какой-то другой системный процесс занял TCP порт 8080
- Не запущена база данных PostgreSQL либо нет связи с ней

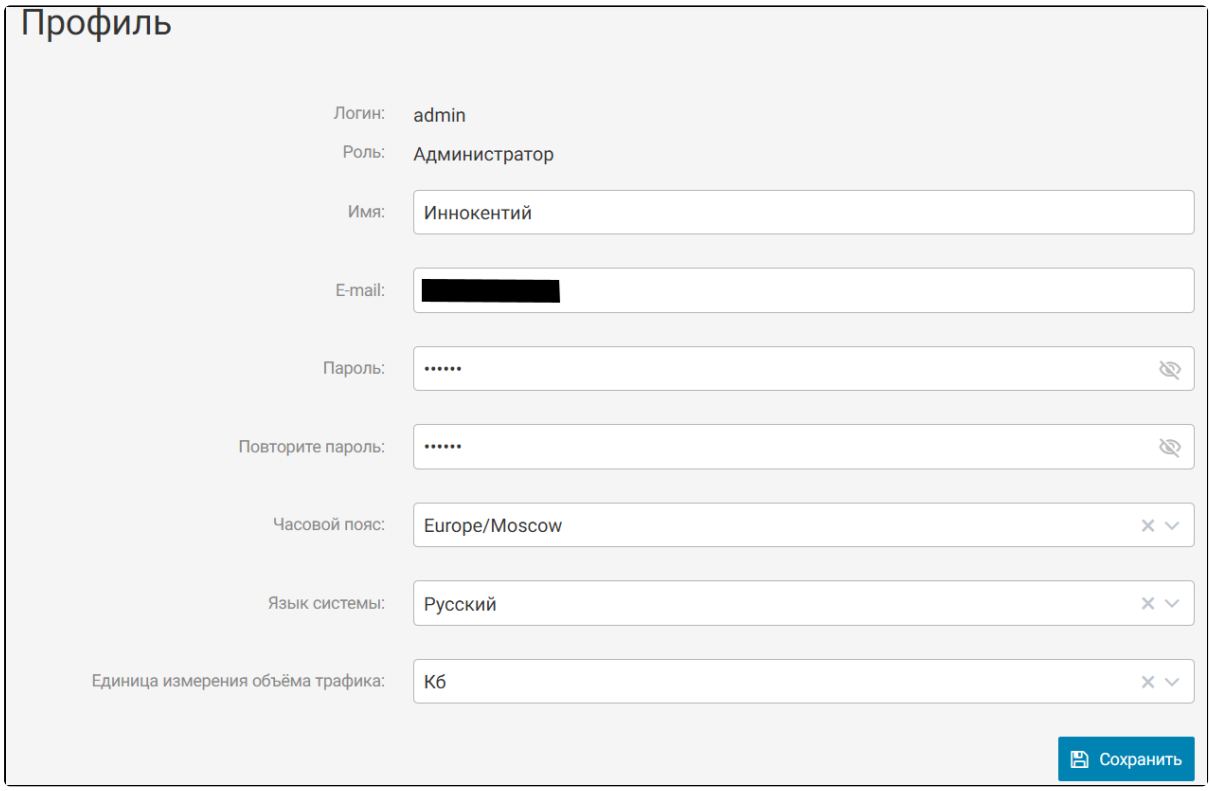
В любом случае, внимательно прочитайте эти сообщения, если не получается решить проблему, обратитесь в службу технической поддержки.

2. Вход в систему и смена пароля

Интерфейс администратора системы WNAM 2 доступен по адресу: http://имя_или_адрес_сервера/. Если при доступе к интерфейсу отображается ошибка "502 Bad Gateway", это означает, что прокси-сервер Nginx настроен некорректно, либо сервис **wnam2** (w2config) системы WNAM 2 не запустился. Следует посмотреть статус системы (**systemctl status wnam2**).

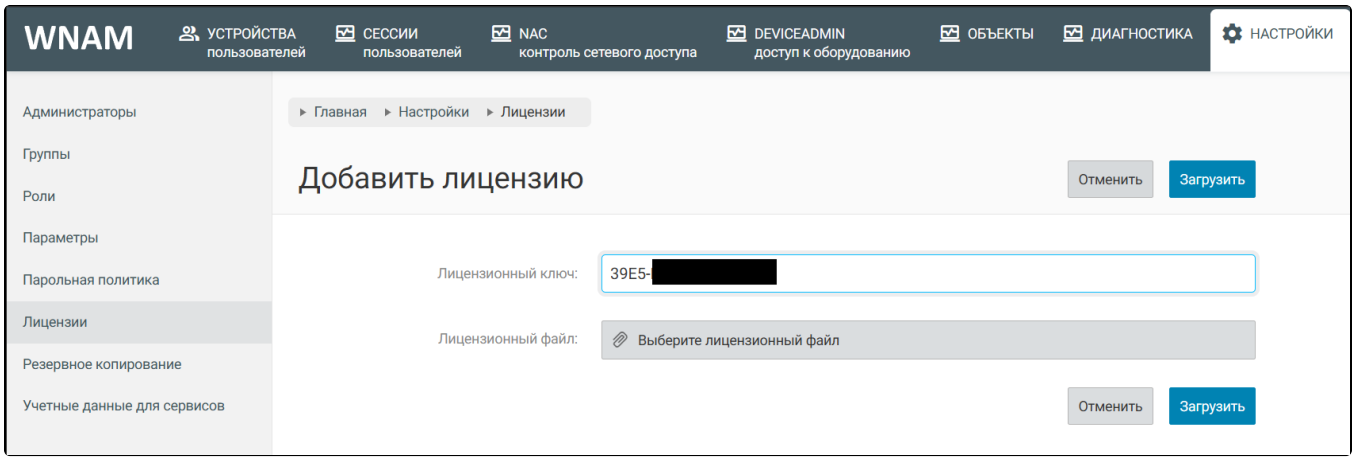
По умолчанию для администратора системы WNAM 2 установлен логин и пароль: admin, admin. После первого входа администратора в систему необходимо изменить пароль администратора. Для этого следует перейти в контекстное меню профиля "Настройки" и в поле "Пароль" задать новый пароль для администратора.

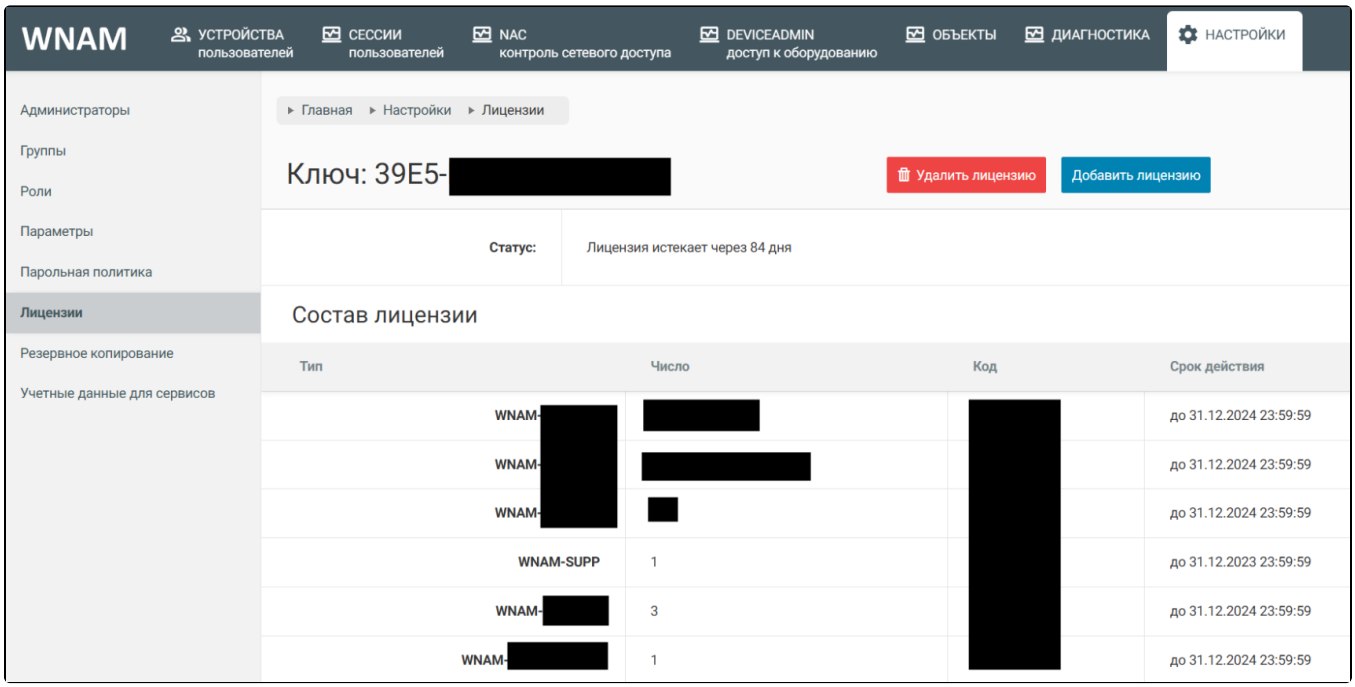
⚠ Если Вы желаете обеспечить дополнительные меры безопасности авторизации учетных записей WNAM 2, рекомендуем перейти в раздел "Настройки" – "Параметры" и настроить параметр "Запретить одновременную авторизацию с разных ip".



3. Ввод лицензионного ключа

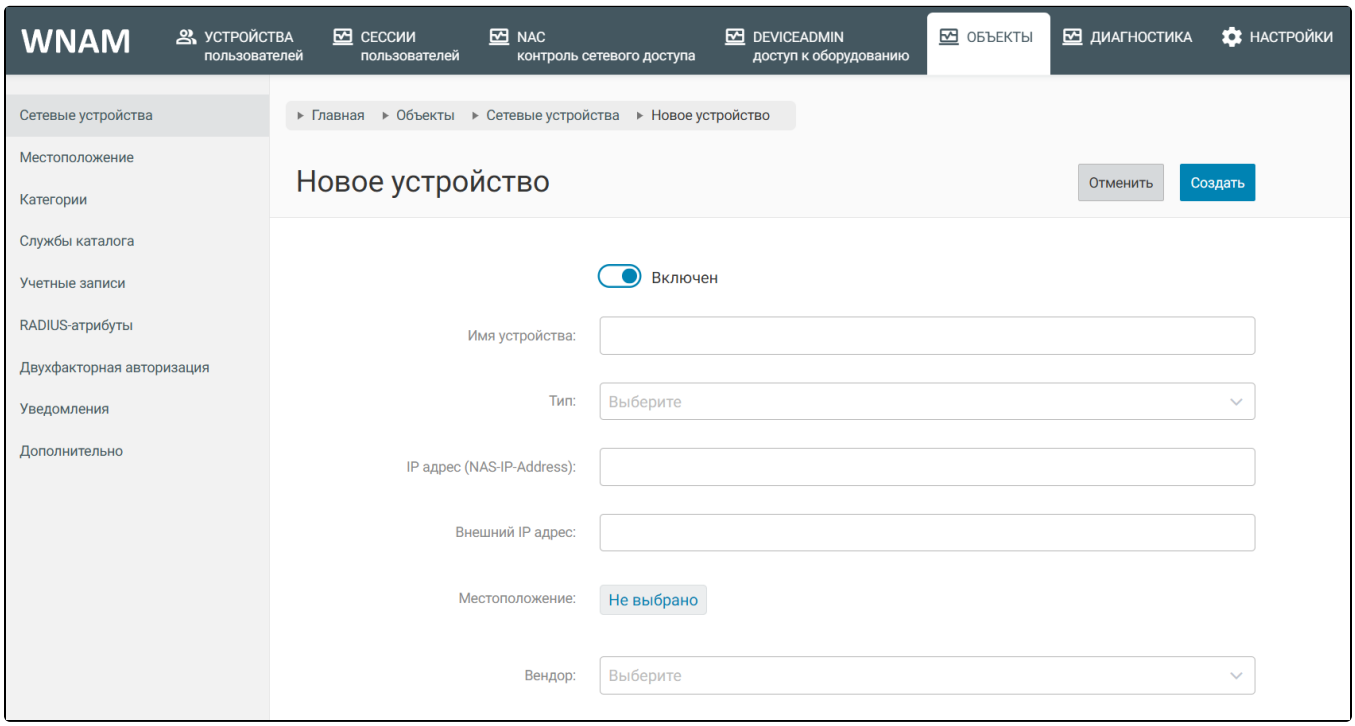
В меню "Настройки" "Лицензии" необходимо указать ваш лицензионный ключ и загрузить предоставленный ключевой файл. К системе WNAM 2 подходят файлы и ключи от системы управления гостевым доступом WNAM 1.6 (с модулем и лицензией корпоративной авторизации).





4. Создание записи о сетевом устройстве (NAS)

В меню "Главная" "Объекты" "Сетевые устройства" "Новое устройство" необходимо создать запись, соответствующую вендору используемого устройства (Cisco, Huawei и т.п.) и его типу (коммутатор, маршрутизатор, контроллер БЛВС). Это RADIUS- или TACACS+-клиент для системы WNAM 2. В общепринятой терминологии это Network Access Server, NAS.



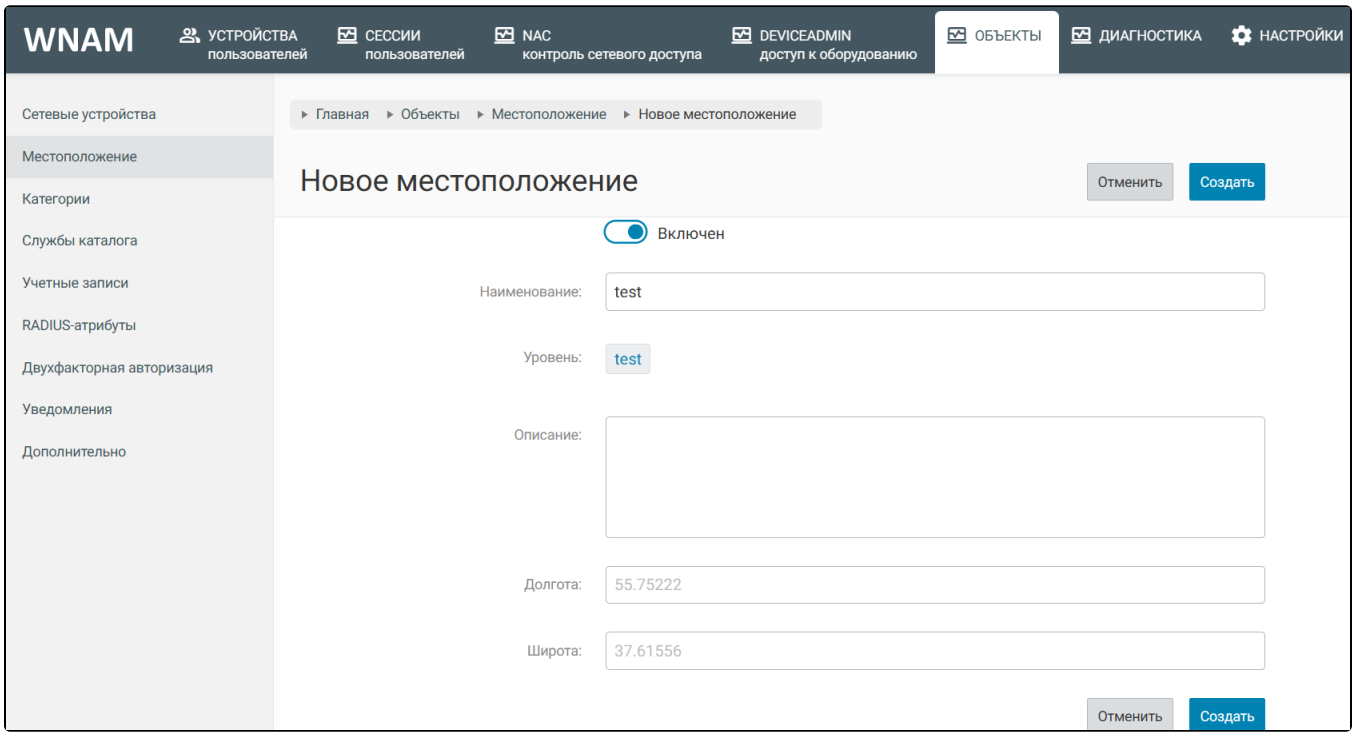
В качестве параметров следует указать:

- Имя устройства.
- Тип устройства (из выпадающего списка).
- IP-адрес устройства. Он должен совпадать с тем адресом, с которого будут отправляться RADIUS-пакеты в сторону системы WNAM 2 (параметр NAS-IP-Address). Также можно указать публичный IP-адрес сервера доступа, если он находится за NAT относительно сервера системы WNAM 2.

- Внешний IP адрес.
- Местоположение устройства (для идентификации в отчётах).
- Вендор (из выпадающего списка).
- Метка устройства (из выпадающего списка, можно оставить пустым).
- Категория критического устройства (из выпадающего списка, можно оставить пустым).
- Категория ipsec (из выпадающего списка, можно оставить пустым).
- Описание - произвольное поле (можно оставить пустым).
- Опционально - включение параметра RADIUS (необходимо указать атрибуты предварительной авторизации, атрибуты CoA / пост-авторизации, секретный ключ, порт CoA).
- Опционально - включение параметра TACACS (необходимо определить, необходимо ли переопределить настройки TACACS+).
- Опционально - включение параметра SNMP (необходимо определить, необходимо ли переопределить права доступа SNMP, переопределить проверку портов по SNMP).
- Опционально - включение параметра API (необходимо указать логин и пароль при авторизации внешней авторизации API).

5. Создание записи о местоположении объектов

Далее необходимо создать запись о первом местоположении объектов в разделе "Главная" "Объекты" "Местоположение". Данный раздел определяет географический адрес, бизнес-подразделение или любую иерархическую структуру, в которой расположены ваши сетевые устройства, и где находятся клиенты вашей сети. Детальные настройки правил аутентификации можно вести в привязке (совпадении) с местоположением..



В качестве параметров следует указать:

- Параметр активации местоположения.
- Наименование местоположения.
- Уровень вложения местоположения (возможно создание вложенного местоположения, для определения более точного наименования местоположения).
- Произвольное описание.
- Долгота.
- Широта.

6. Настройка сетевого устройства (контроллера Wi-Fi или коммутатора ЛВС)

Настройку вашего сетевого устройства необходимо выполнить в соответствии с инструкцией его производителя, изучив разделы, посвященные настройке 802.1X и TACACS+ протоколов.

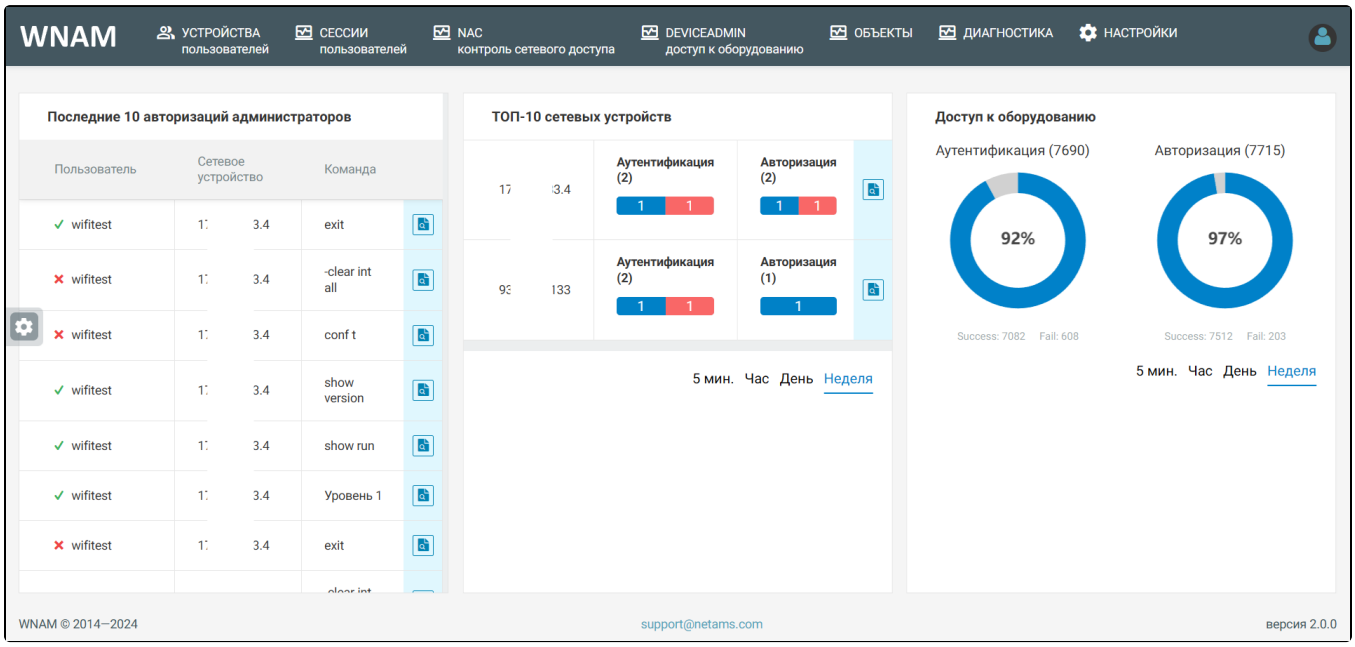
Настройка

В данном разделе описана настройка системы WNAM 2 с использованием графического веб-интерфейса. Поддерживаются современные (на 2024) год браузеры.

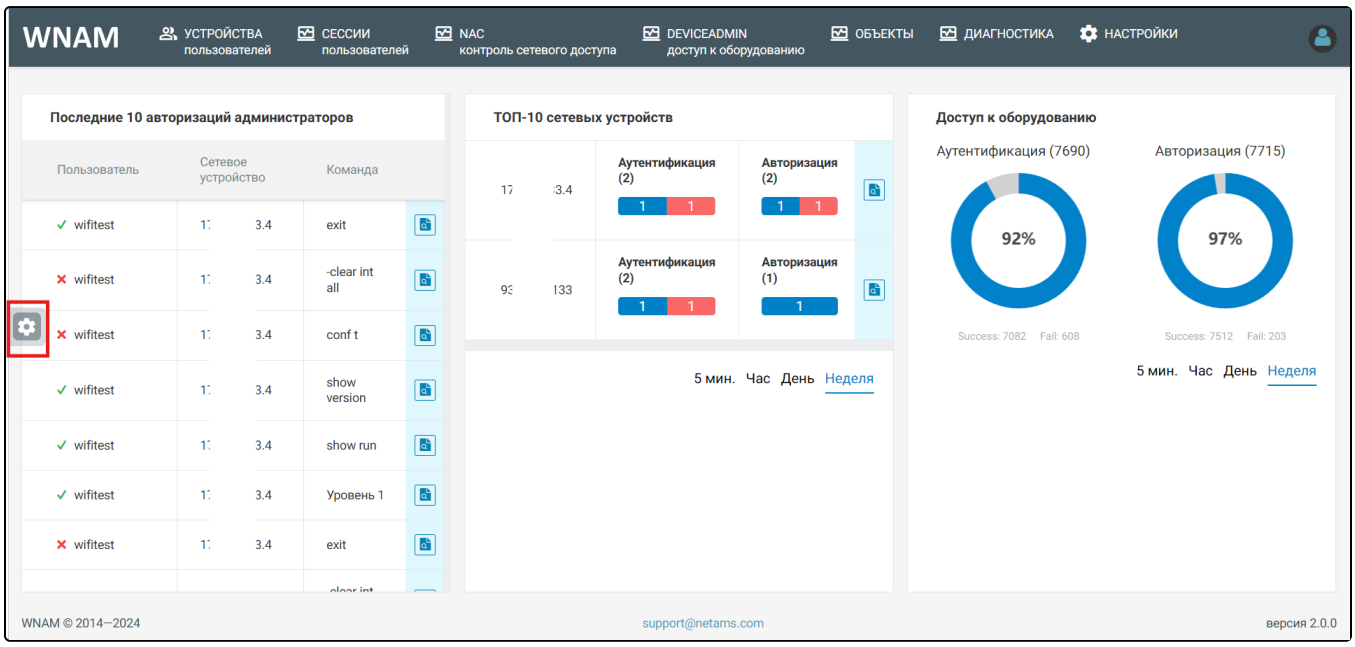
> ⚠ Важное уточнение. Те или иные настройки могут не присутствовать в зависимости от выданных прав на чтение и запись в различные области доступа системы WNAM 2. Если на той или иной учетной записи не присутствует требуемого раздела настроек WNAM 2, то скорее всего, на этой учетной записи не выданы соответствующие права и для решения данной проблемы стоит обратиться к системному администратору, или же перейти в раздел справочного материала "Роли".

Сводка

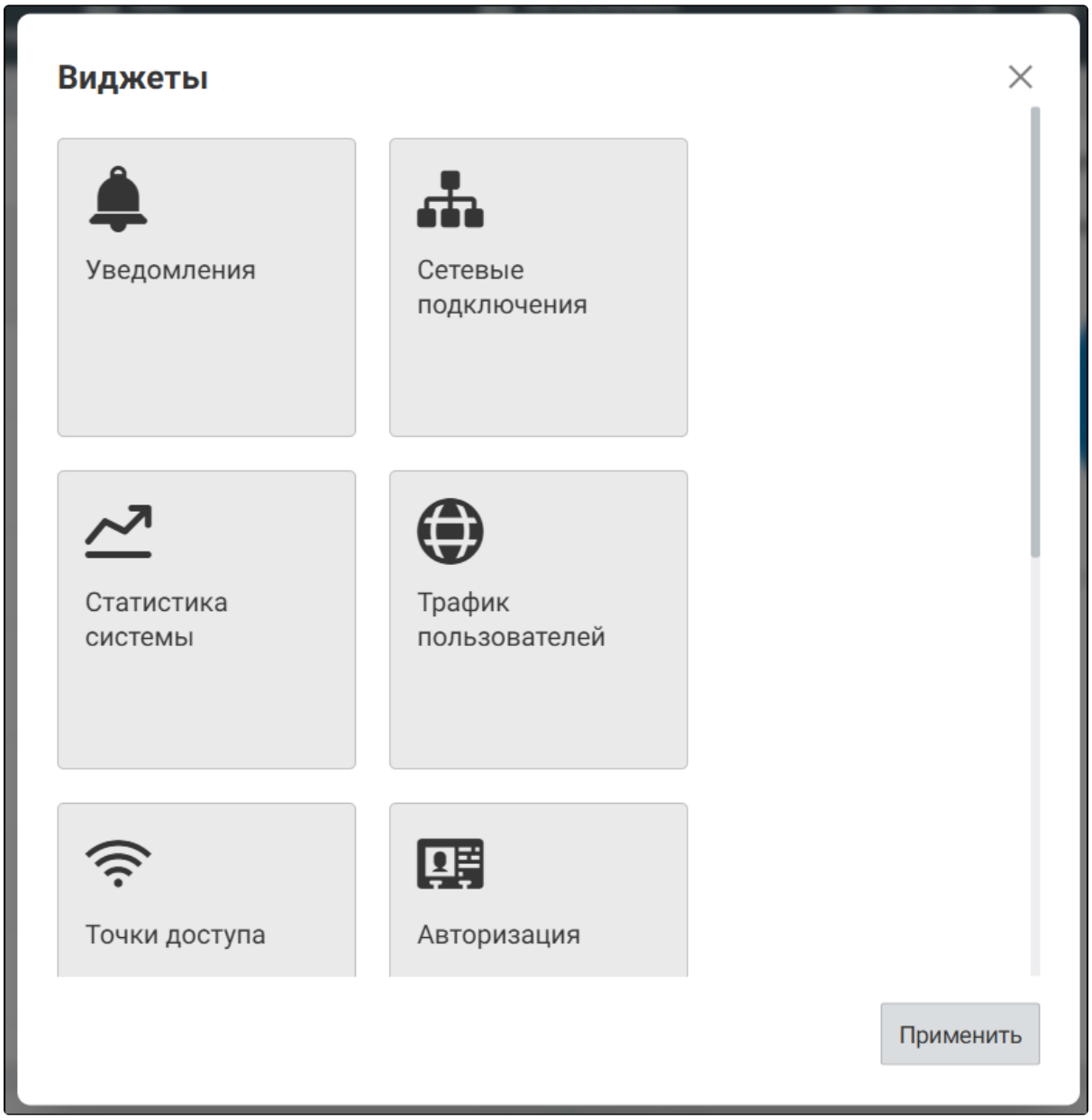
При первичном разворачивании системы WNAM 2 и дальнейшем входе будет отображаться дашборд– основная страница всей системы. В ней содержится виджеты по последним 10 авторизациям, наиболее частые авторизации и аутентификации с возможностью фильтрации по времени за какой-либо срок (неделя, день, час, последние 5 минут).



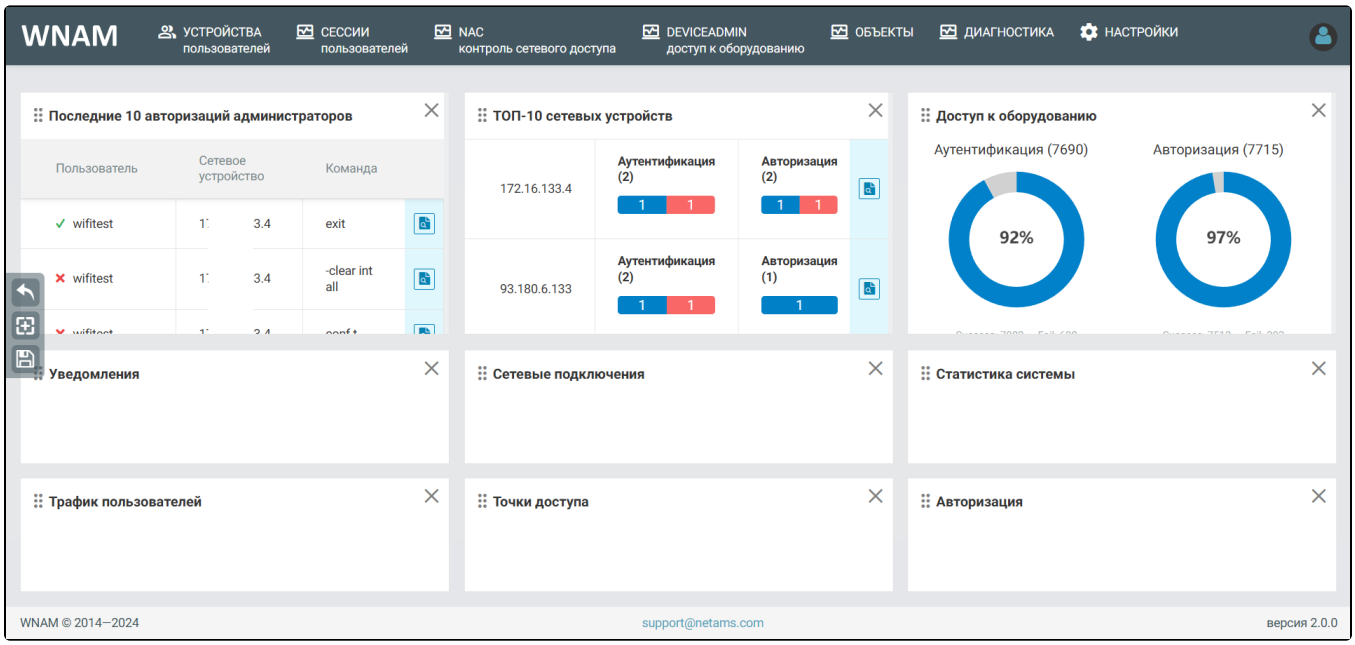
При необходимости, возможно добавить дополнительные виджеты с настройкой размеров виджетов. Для этого, в левой части экрана требуется на кнопку параметров.



После, откроется интерфейс с активацией того или иного виджета.



После выбора определенного количества виджетов и применения настроек, отобразится макет дашборда с добавленными виджетами.

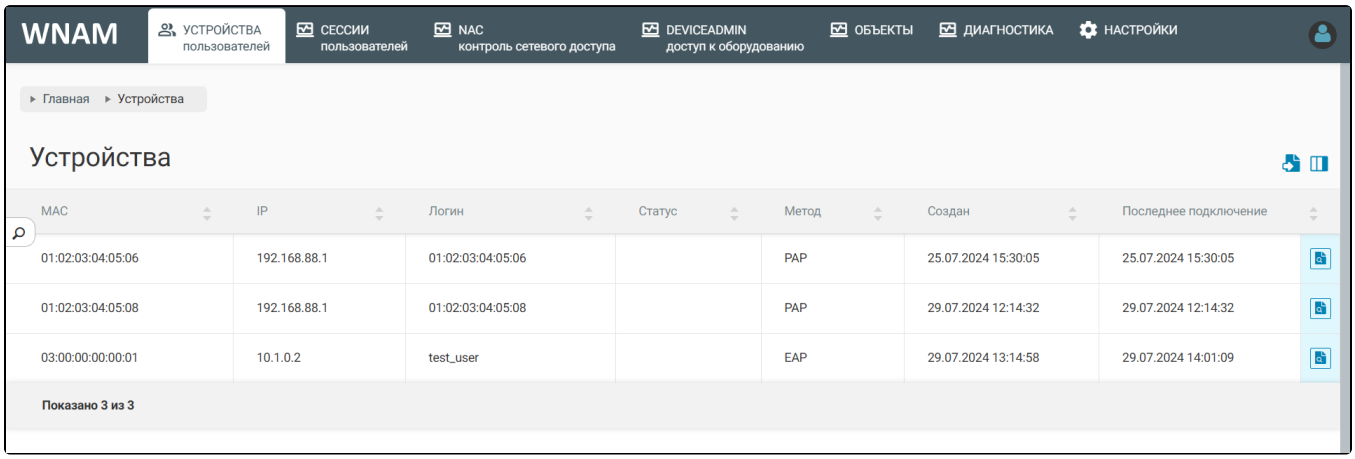


Также присутствует возможность редактировать размер виджетов и их удаление при необходимости.

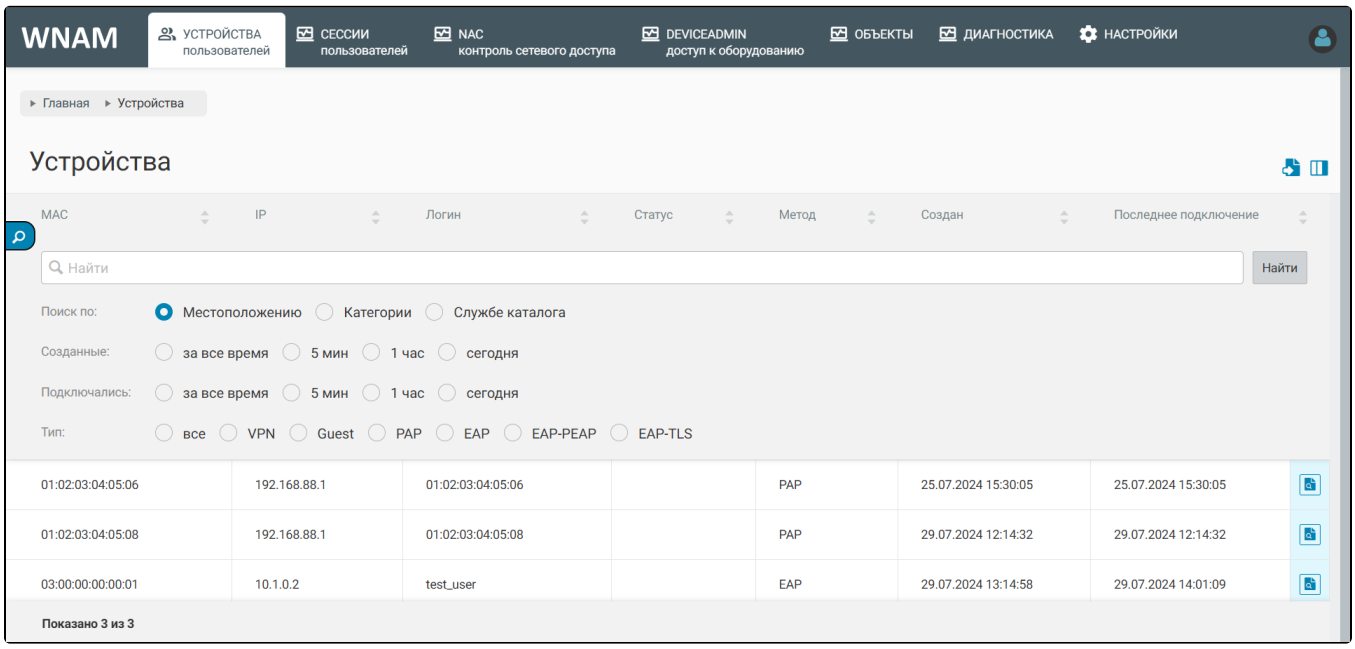
> ⚠ Уточнение, в данной статье развернута тестовая версия системы WNAM 2, поэтому вполне вероятно отсутствие некоторых данных.

Устройства пользователей

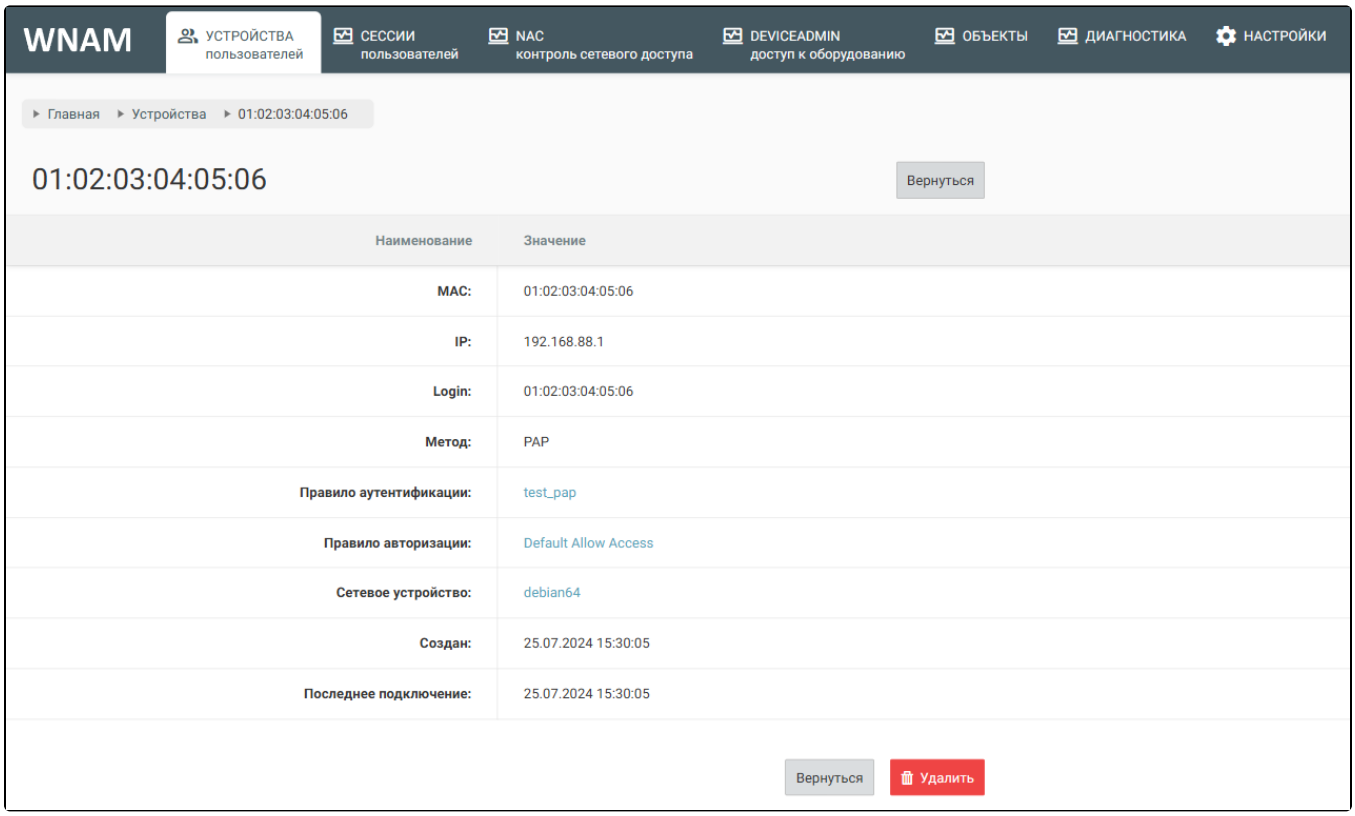
Раздел "**Пользователи**" содержит список зарегистрированных в системе пользователей - абонентов беспроводной сети. Эти записи создаются системой WNAM 2 автоматически в момент их первого подключения. Основное окно раздела "Пользователи" представляет собой таблицу со списком пользователей, которая отображает краткие записи характеристик пользователя.



Поле "Найти" позволяет найти запись о пользователе по части MAC-адреса, номеру телефона или IP-адресу. Также таблицу можно отфильтровать по типу записи (VPM, Guest, PAP, EAP, EAP-PEAP, EAP-TLS), времени создания записи (за все время, 5 минут, 1 час, сегодня), времени подключения (за все время, 5 минут, 1 час, сегодня). Помимо этого, присутствует функция поиска по местоположению, категориям и службам каталога.



При нажатии левой кнопкой мыши на контекстное меню "подробнее", содержащее детальные сведения об учётной записи пользователя в системе.



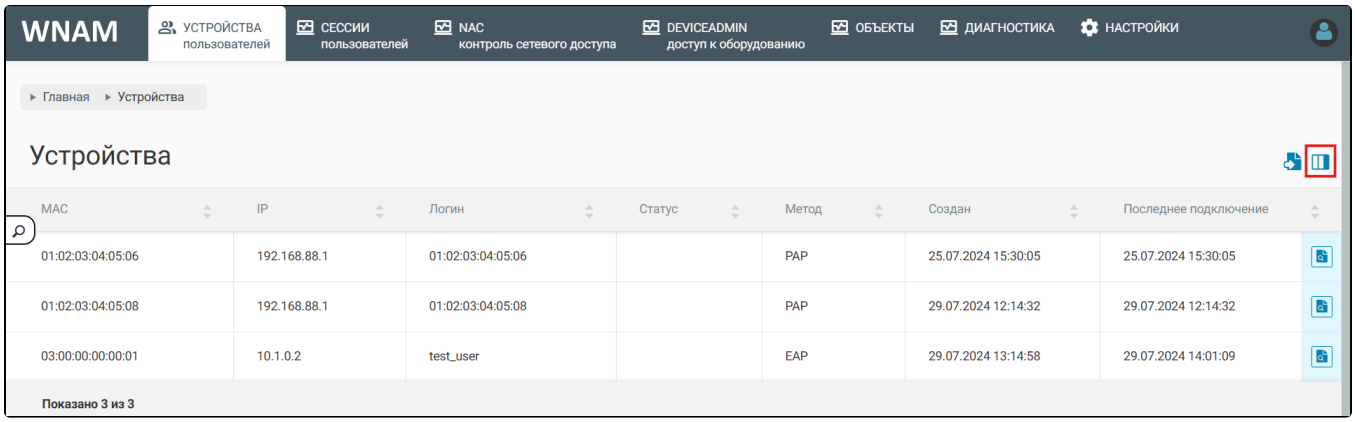
В окне отображается:

- MAC адрес;
- IP адрес;
- Логин;
- Метод;
- Правило аутентификации;
- Правило авторизации;
- Сетевое устройство;
- Дата создания;
- Последнее подключение;

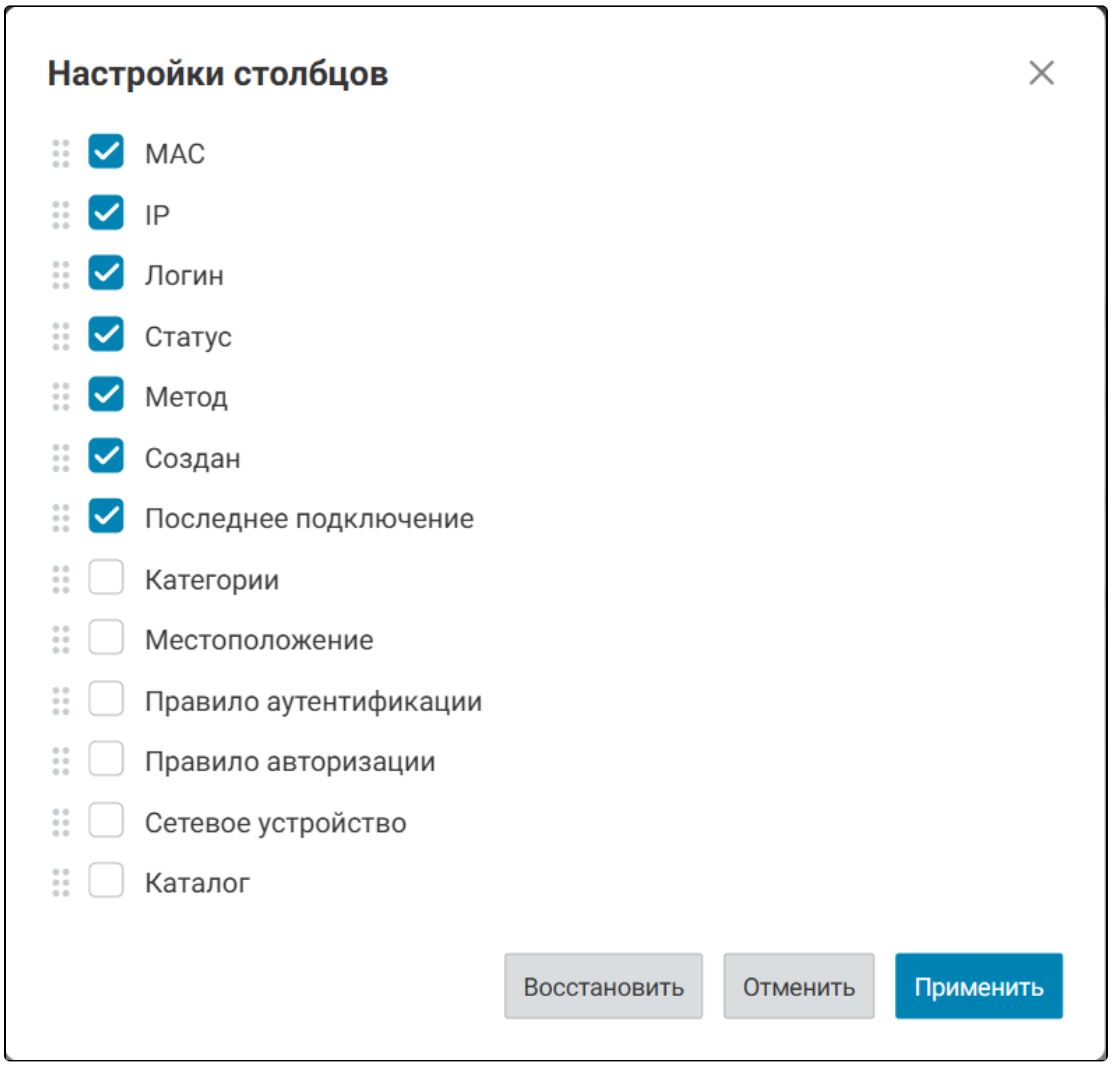
При необходимости, возможно удалить данные об учетной записи.

Настройки отображения таблицы.

Для изменения настроек отображения, необходимо нажать левой кнопкой мыши по функции настройке столбцов:



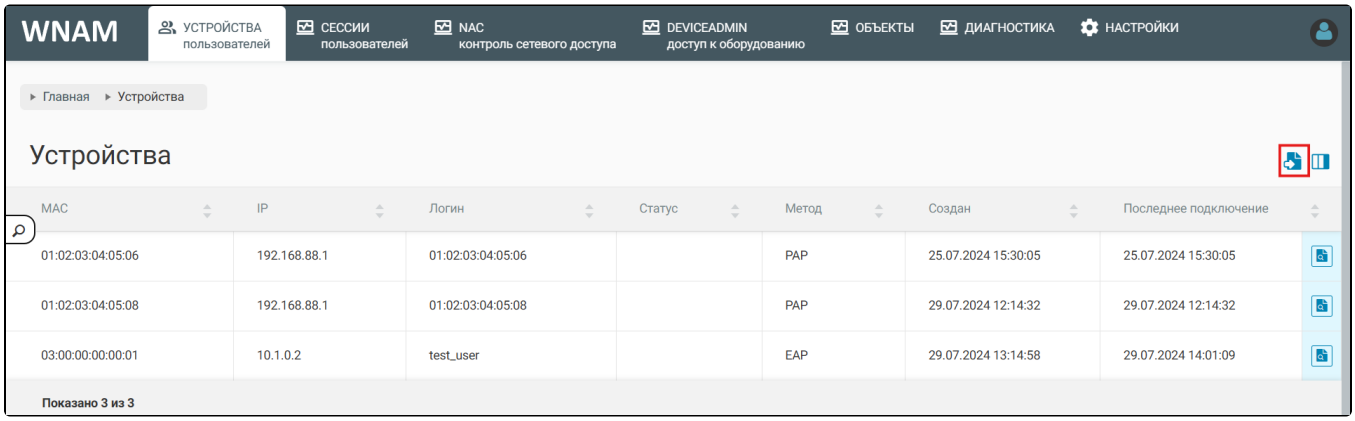
Далее, следует выбрать интересующие для отображения столбцы:



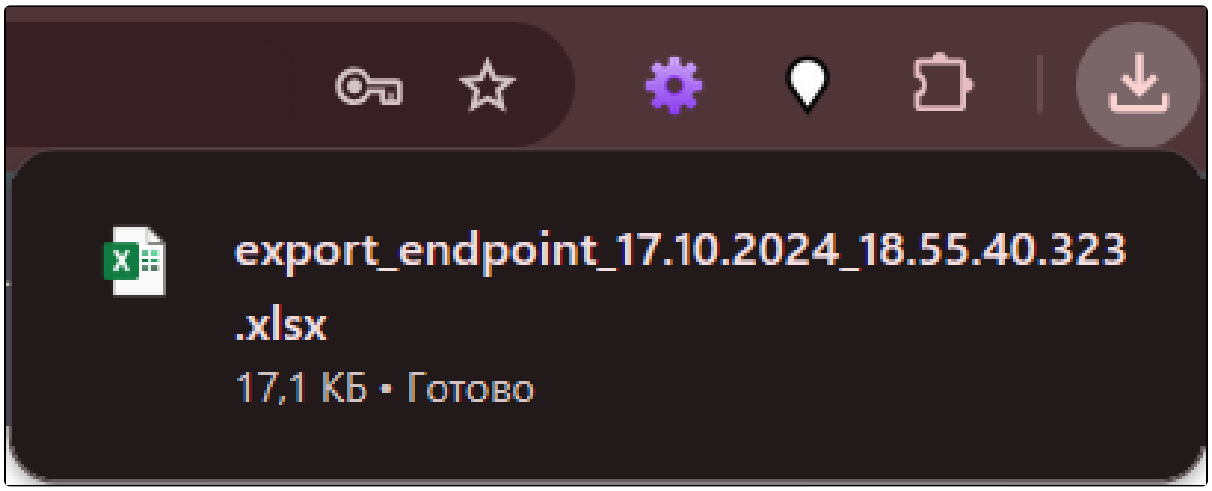
На усмотрение, возможно гибко настроить отображение столбцов, изменить порядок отображения, либо убрать неинтересующий столбец.

Экспорт данных.

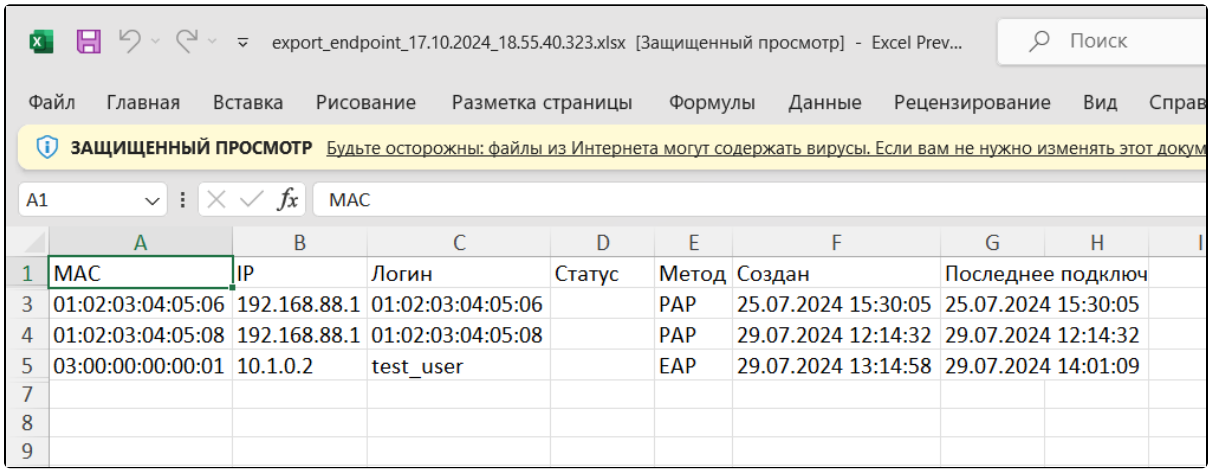
Данный вид настроек отображения можно применить как к таблице сессий TACACS+, так и к таблице сессий RADIUS. Для экспорта требуемой таблицы необходимо выбрать функцию экспорта:



После, в автоматической режиме будет произведена загрузка таблицы:



Файл содержит идентичные данные, которые представлены на странице сессий пользователей:

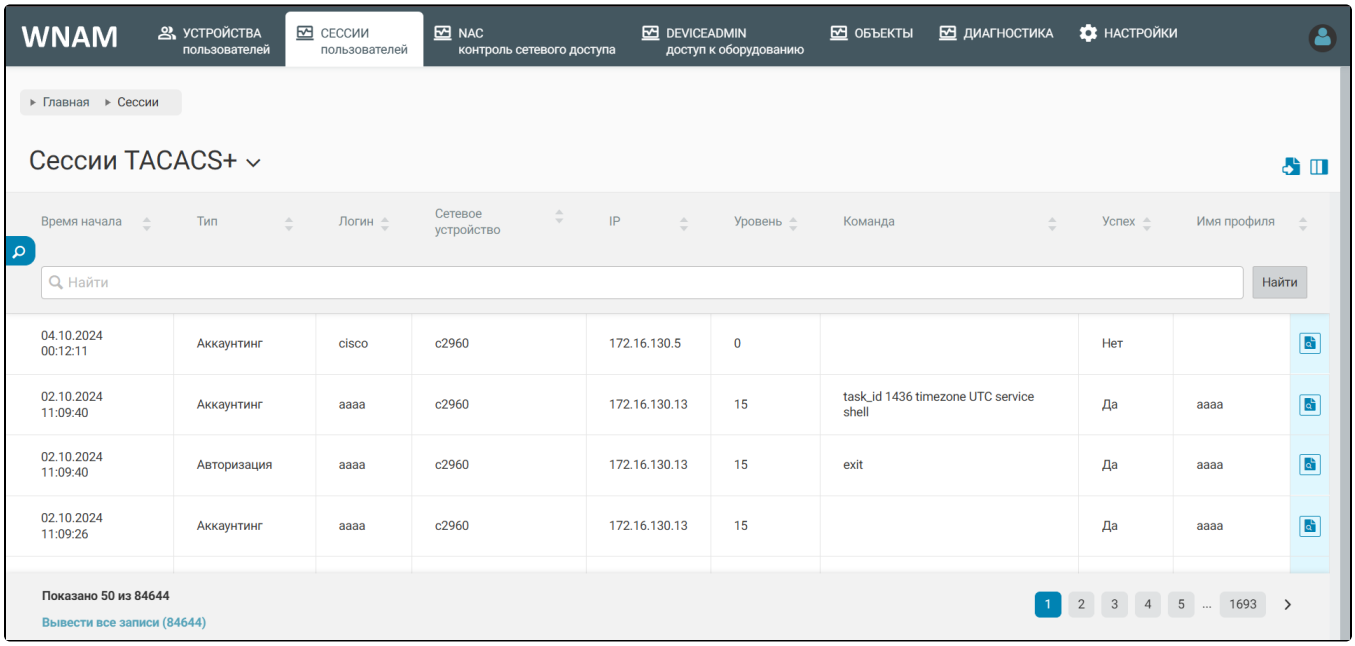


	A	B	C	D	E	F	G	H
1	MAC	IP	Логин	Статус	Метод	Создан	Последнее подключ	
3	01:02:03:04:05:06	192.168.88.1	01:02:03:04:05:06		PAP	25.07.2024 15:30:05	25.07.2024 15:30:05	
4	01:02:03:04:05:08	192.168.88.1	01:02:03:04:05:08		PAP	29.07.2024 12:14:32	29.07.2024 12:14:32	
5	03:00:00:00:00:01	10.1.0.2	test_user		EAP	29.07.2024 13:14:58	29.07.2024 14:01:09	
7								
8								
9								

Сессии пользователей

Сессии TACACS+.

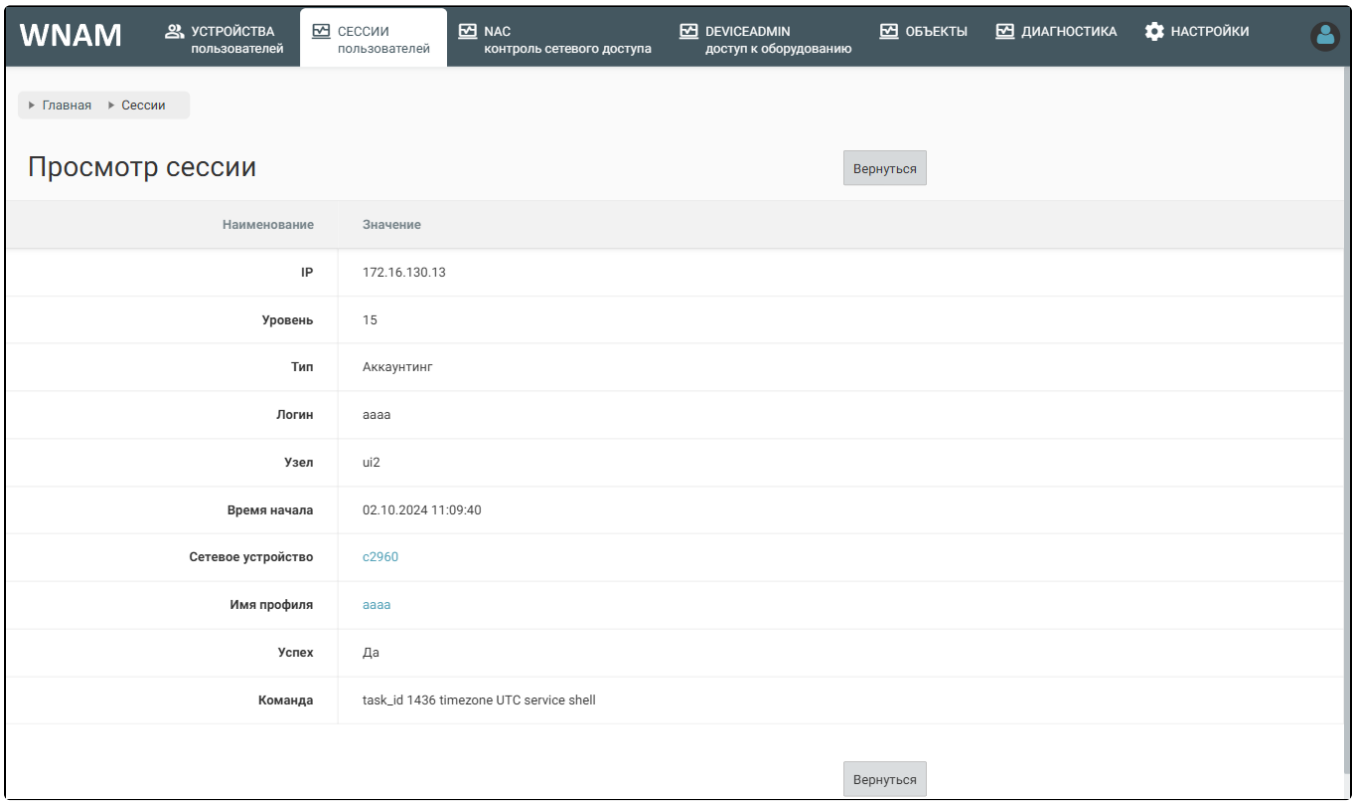
Раздел "**Сессии**" содержит список сессий - фактов подключения и работы зарегистрированных в системе пользователей - абонентов беспроводной сети. Эти записи создаются системой автоматически в момент каждого нового подключения пользователя к сети. Основное окно раздела представляет собой таблицу с краткими характеристиками записей о сессии пользователя.



Кнопка "Поиск" позволяет быстро отфильтровать таблицу по интересующему атрибуту.

Таблица содержит текущий IP-адрес пользователя (обычно, уникальный для сессии), времена начала сессии, счётчики переданных и полученных байт. Для серверов доступа некоторых типов (Linux, Mikrotik) возможно выполнить операцию "сброс сессии". Также в разделе присутствует возможность сортировки сессий по времени начала, типу сессии, логину, сетевому устройству, IP адресу, критическому уровню, выполняемой команде, успешности выполнения, наименования профиля.

При нажатии левой кнопкой мыши на контекстное меню "подробнее", содержащее детальные сведения о данной сессии.



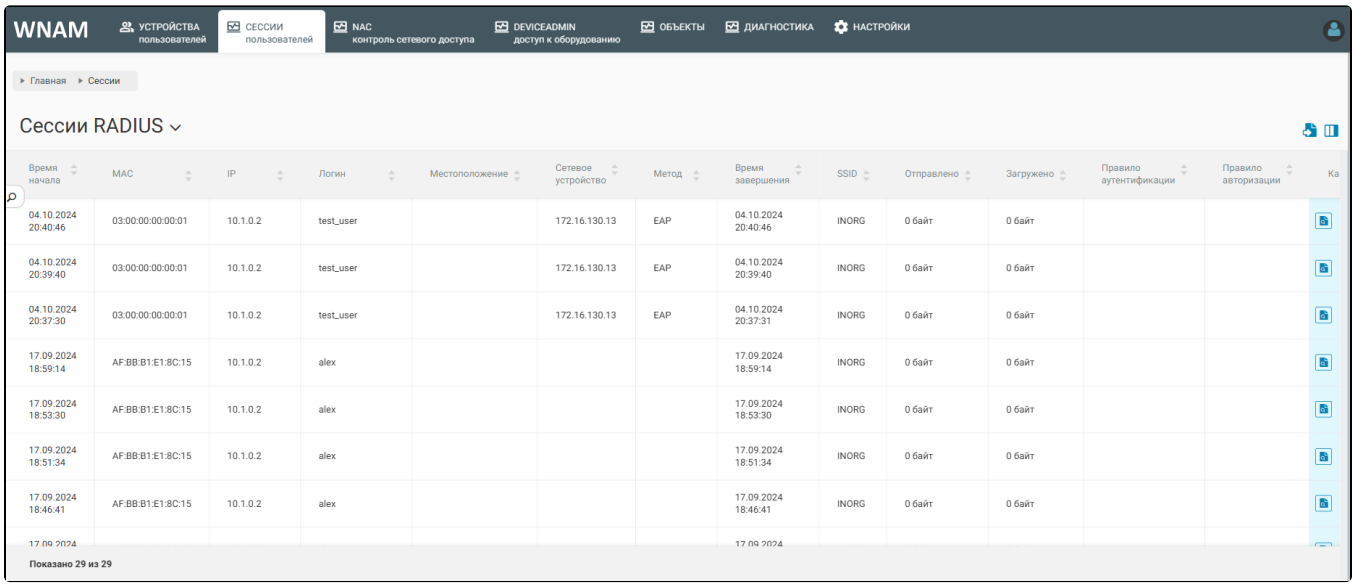
В окне отображается:

- IP адрес;
- Уровень;
- Тип;
- Логин;
- Узел;
- Длительность аутентификации;
- Сетевое устройство;
- Имя профиля;
- Успех выполнения;
- Выполняемая команда;

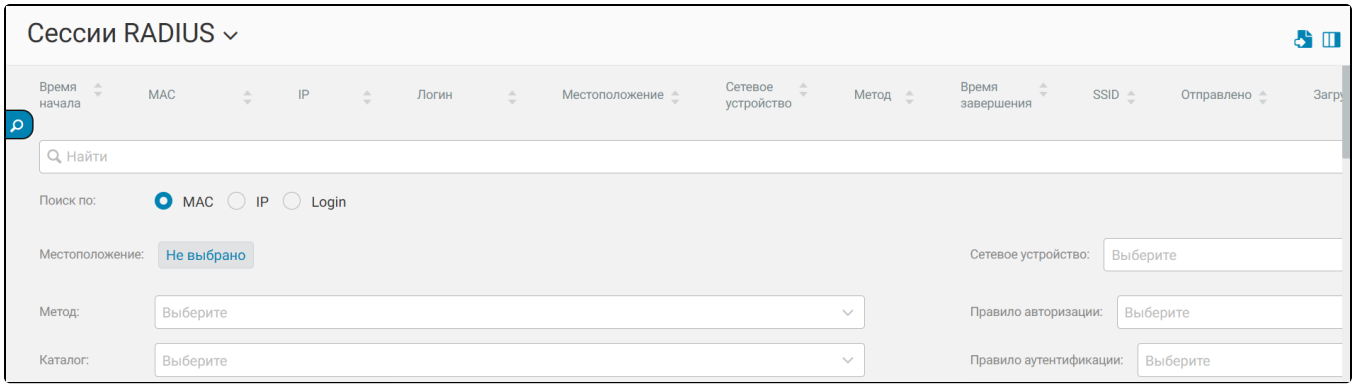
Благодаря данному окну будет возможно получить достаточную информацию о том или иной сессии пользователя.

Сессии RADIUS.

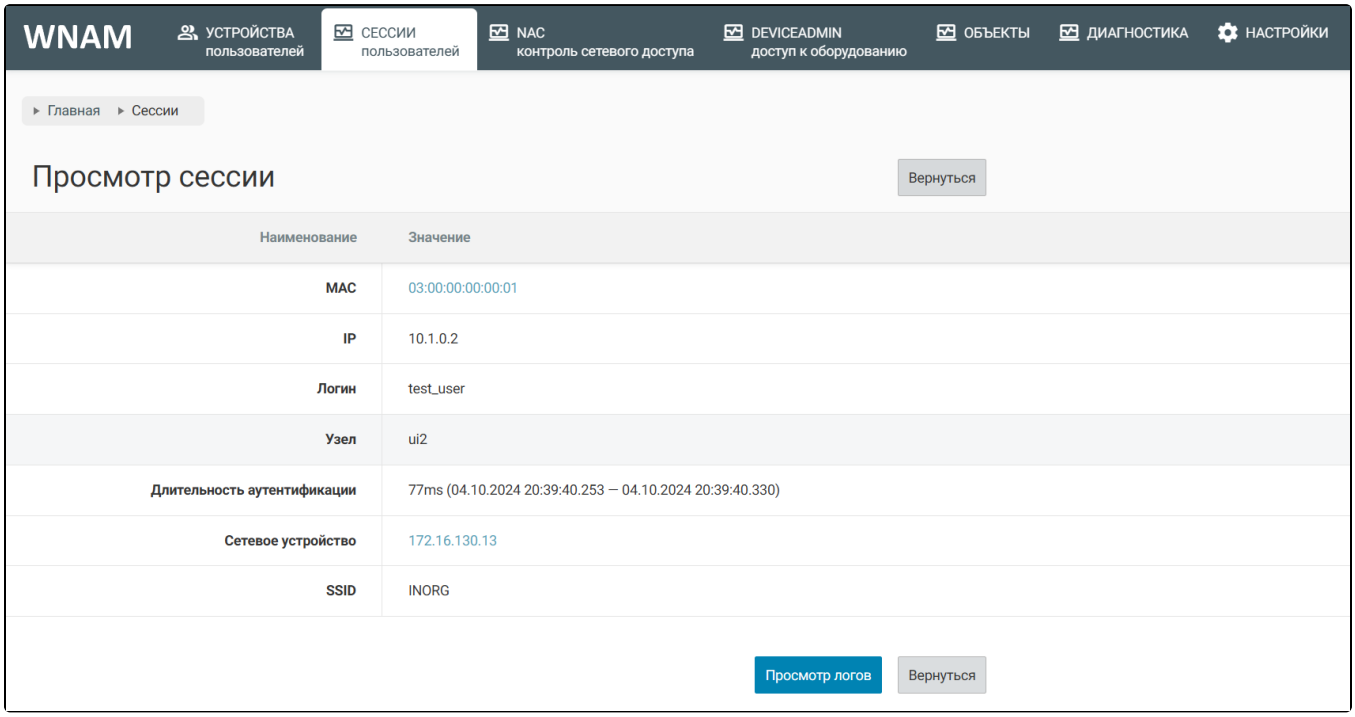
Таблица сессий Radius в своем представлении мало отличается от представления таблицы сессий TACACS+.



Функция поиска включает тонкие настройки по фильтрации записей сессий RADIUS:

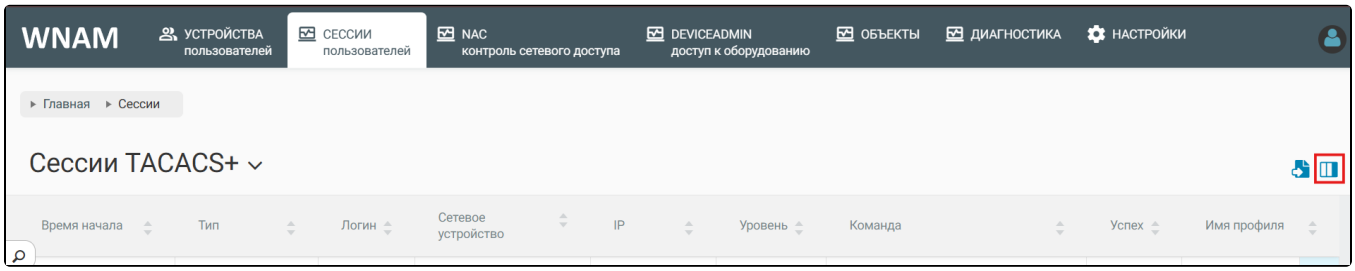


Детальное описание сессии Radius также имеют вид, похожий на сессию TACACS+ :

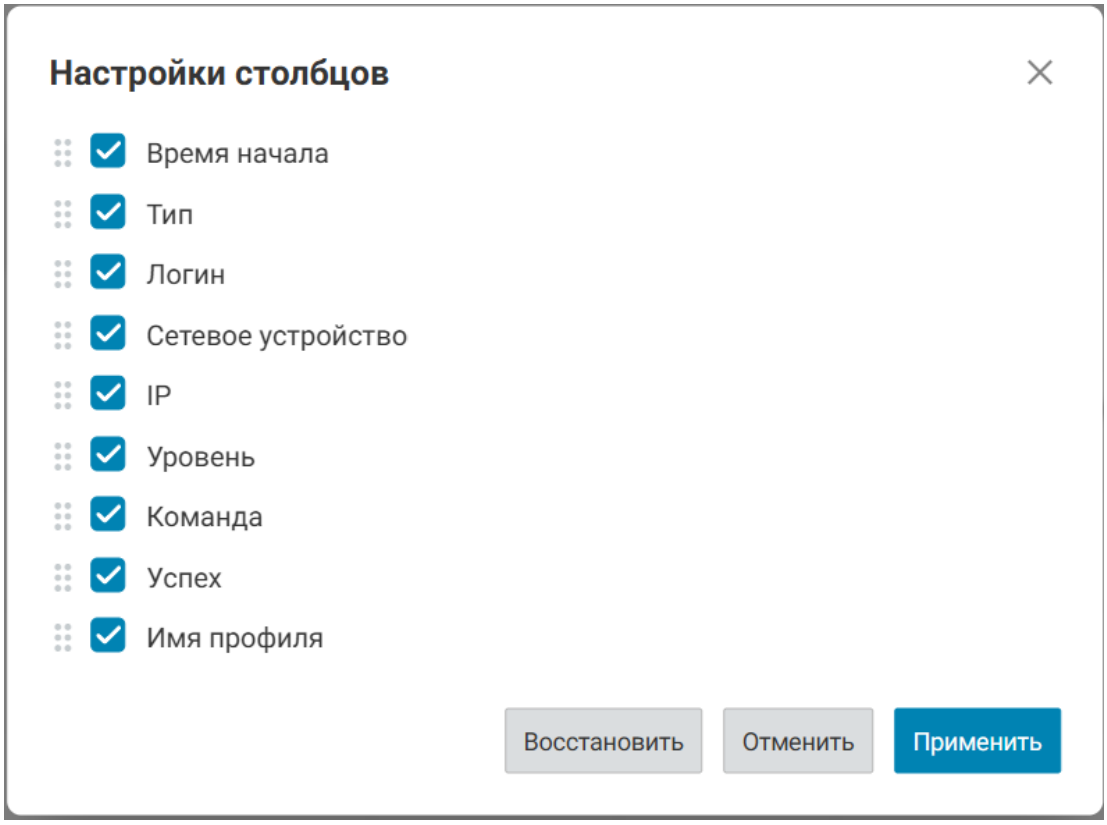


Настройки отображения таблицы.

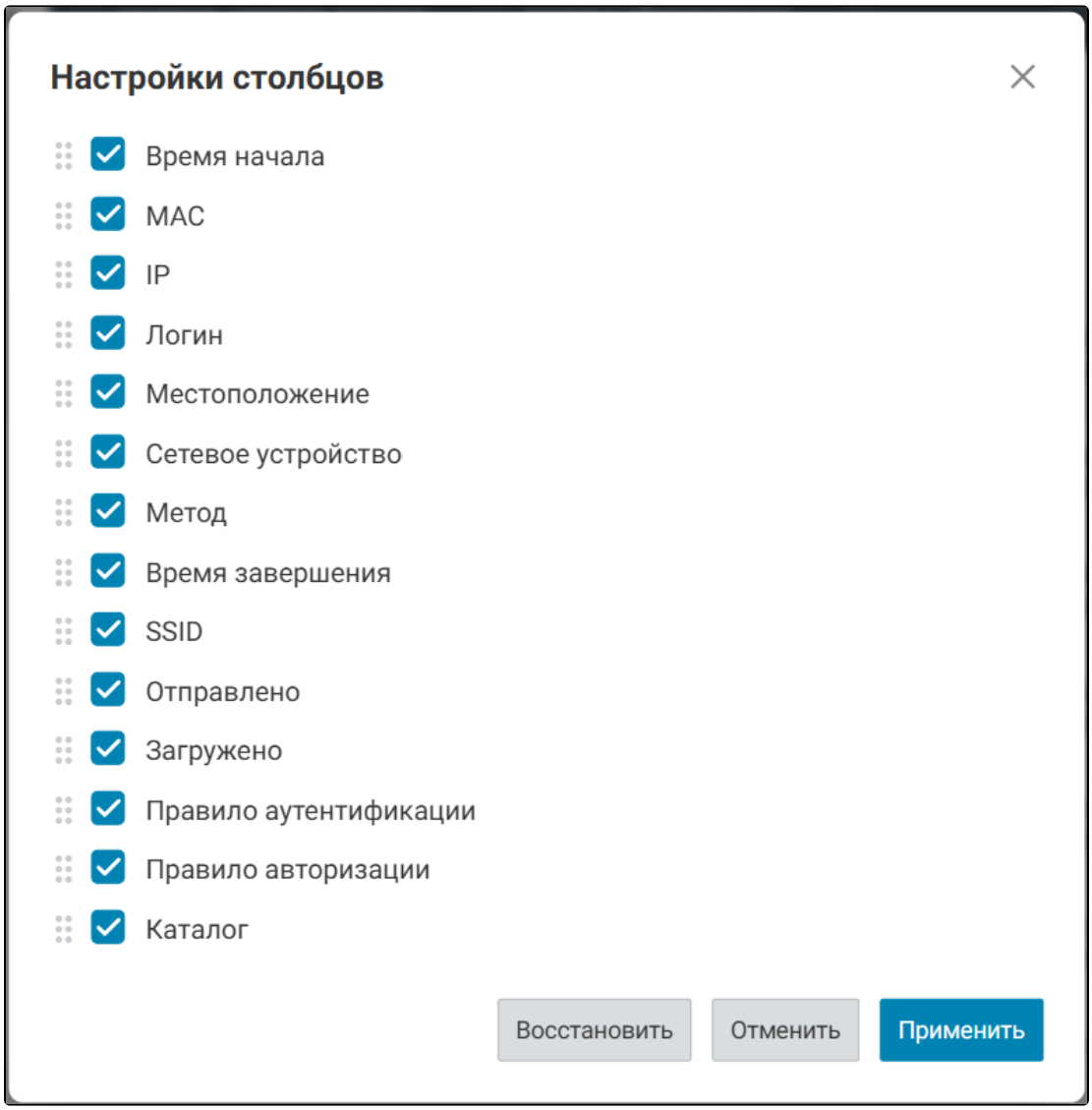
Данный вид настроек отображения можно применить как к таблице сессий TACACS+, так и к таблице сессий RADIUS. Для изменения настроек отображения, необходимо нажать левой кнопкой мыши по функции настройке столбцов:



В зависимости от выбранной таблицы, настройки столбцов могут варьироваться. Так, для таблицы сессий TACACS+, настройки будут иметь вид:



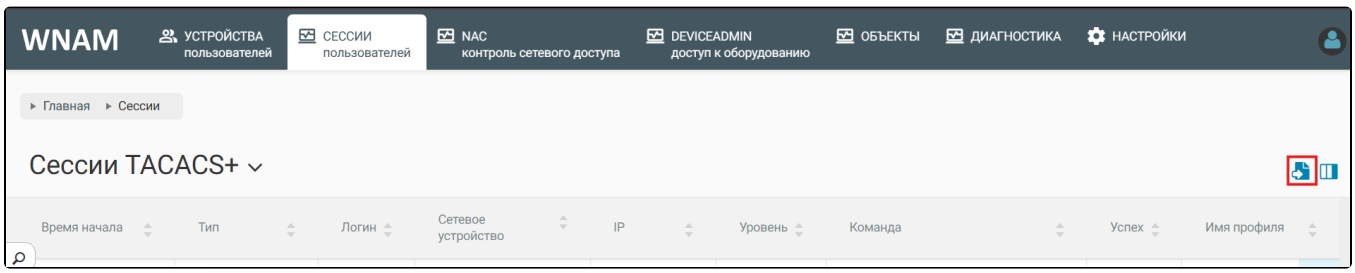
Для таблицы сессий RADIUS:



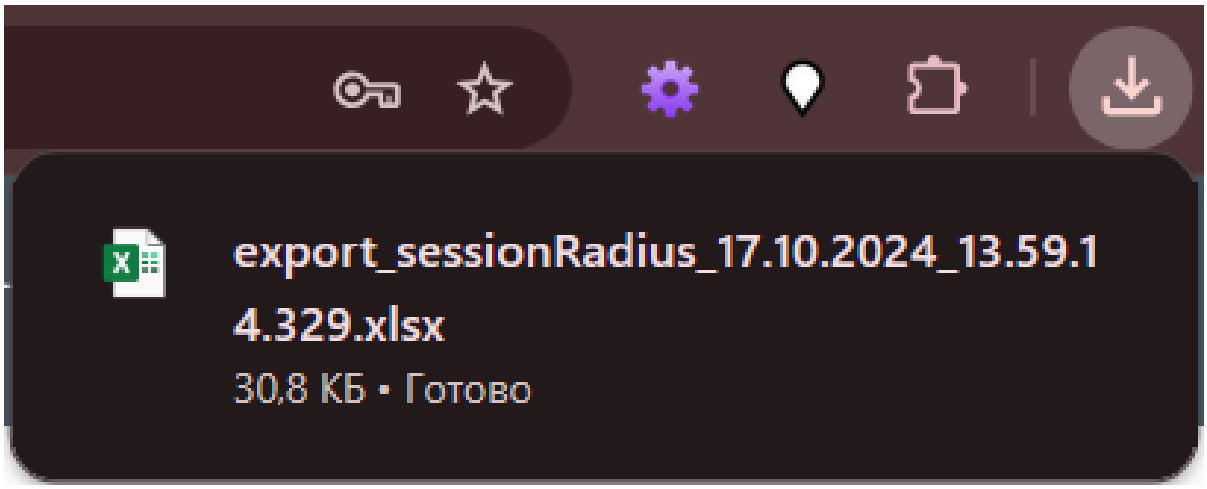
На усмотрение, возможно гибко настроить отображение столбцов, изменить порядок отображения, либо убрать не интересующий столбец.

Экспорт данных.

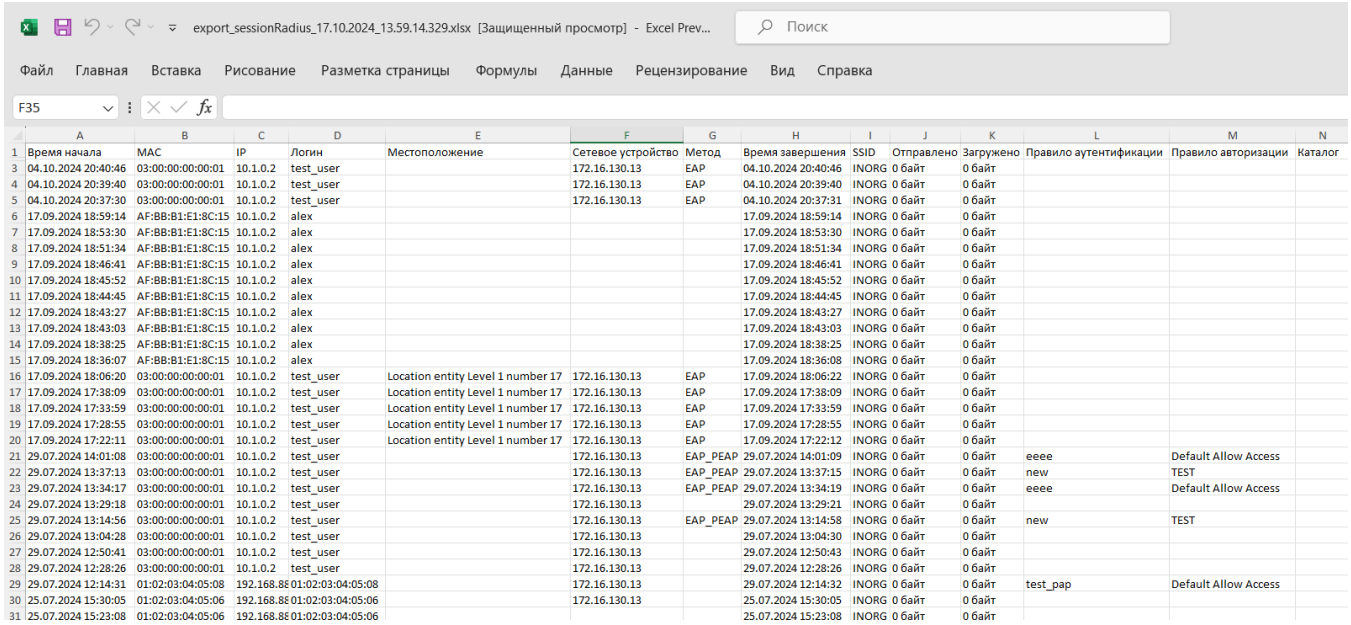
Данный вид настроек отображения можно применить как к таблице сессий TACACS+, так и к таблице сессий RADIUS. Для экспорта требуемой таблицы необходимо выбрать функцию экспорта:



После, в автоматической режиме будет произведена загрузка таблицы:



Файл содержит идентичные данные, которые представлены на странице сессий пользователей:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Время начала	MAC	IP	Логин	Местоположение	Сетевое устройство	Метод	Время завершения	SSID	Отправлено	Загружено	Правило аутентификации	Правило авторизации	Каталог
3	04.10.2024 20:40:46	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP	04.10.2024 20:40:46	INORG	0 байт	0 байт			
4	04.10.2024 20:39:40	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP	04.10.2024 20:39:40	INORG	0 байт	0 байт			
5	04.10.2024 20:37:30	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP	04.10.2024 20:37:31	INORG	0 байт	0 байт			
6	17.09.2024 18:59:14	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:59:14	INORG	0 байт	0 байт			
7	17.09.2024 18:53:30	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:53:30	INORG	0 байт	0 байт			
8	17.09.2024 18:51:34	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:51:34	INORG	0 байт	0 байт			
9	17.09.2024 18:46:41	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:46:41	INORG	0 байт	0 байт			
10	17.09.2024 18:45:52	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:45:52	INORG	0 байт	0 байт			
11	17.09.2024 18:44:45	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:44:45	INORG	0 байт	0 байт			
12	17.09.2024 18:43:27	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:43:27	INORG	0 байт	0 байт			
13	17.09.2024 18:43:03	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:43:03	INORG	0 байт	0 байт			
14	17.09.2024 18:38:25	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:38:25	INORG	0 байт	0 байт			
15	17.09.2024 18:36:07	AF:BB:B1:E1:8C:15	10.1.0.2	alex				17.09.2024 18:36:08	INORG	0 байт	0 байт			
16	17.09.2024 18:06:20	03:00:00:00:00:01	10.1.0.2	test_user	Location entity Level 1 number 17	172.16.130.13	EAP	17.09.2024 18:06:22	INORG	0 байт	0 байт			
17	17.09.2024 17:38:09	03:00:00:00:00:01	10.1.0.2	test_user	Location entity Level 1 number 17	172.16.130.13	EAP	17.09.2024 17:38:09	INORG	0 байт	0 байт			
18	17.09.2024 17:33:59	03:00:00:00:00:01	10.1.0.2	test_user	Location entity Level 1 number 17	172.16.130.13	EAP	17.09.2024 17:33:59	INORG	0 байт	0 байт			
19	17.09.2024 17:28:55	03:00:00:00:00:01	10.1.0.2	test_user	Location entity Level 1 number 17	172.16.130.13	EAP	17.09.2024 17:28:55	INORG	0 байт	0 байт			
20	17.09.2024 17:22:11	03:00:00:00:00:01	10.1.0.2	test_user	Location entity Level 1 number 17	172.16.130.13	EAP	17.09.2024 17:22:12	INORG	0 байт	0 байт			
21	29.07.2024 14:01:08	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP_PEAP	29.07.2024 14:01:09	INORG	0 байт	0 байт	eeee	Default Allow Access	
22	29.07.2024 13:37:13	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP_PEAP	29.07.2024 13:37:15	INORG	0 байт	0 байт	new	TEST	
23	29.07.2024 13:34:17	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP_PEAP	29.07.2024 13:34:19	INORG	0 байт	0 байт	eeee	Default Allow Access	
24	29.07.2024 13:29:18	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13		29.07.2024 13:29:21	INORG	0 байт	0 байт			
25	29.07.2024 13:14:56	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13	EAP_PEAP	29.07.2024 13:14:58	INORG	0 байт	0 байт	new	TEST	
26	29.07.2024 13:04:28	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13		29.07.2024 13:04:30	INORG	0 байт	0 байт			
27	29.07.2024 12:50:41	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13		29.07.2024 12:50:43	INORG	0 байт	0 байт			
28	29.07.2024 12:28:26	03:00:00:00:00:01	10.1.0.2	test_user		172.16.130.13		29.07.2024 12:28:26	INORG	0 байт	0 байт			
29	29.07.2024 12:14:31	01:02:03:04:05:08	192.168.88	01:02:03:04:05:08		172.16.130.13		29.07.2024 12:14:32	INORG	0 байт	0 байт	test_pap	Default Allow Access	
30	25.07.2024 15:30:05	01:02:03:04:05:06	192.168.88	01:02:03:04:05:06		172.16.130.13		25.07.2024 15:30:05	INORG	0 байт	0 байт			
31	25.07.2024 15:23:08	01:02:03:04:05:06	192.168.88	01:02:03:04:05:06				25.07.2024 15:23:08	INORG	0 байт	0 байт			

Контроль сетевого доступа (NAC)

Данный раздел содержит детальное описание следующего функционала:

- Аутентификация;
- Авторизация;
- Загружаемые ACL;
- Удостоверяющий центр;
- Сертификаты;
- Группы MAC адресов;
- Профилирование;
- Дополнительные настройки.

Аутентификация

Аутентификация — проверка подлинности предоставленных учетных данных того, кто запрашивает сетевой доступ. Система WNAM 2 реализует концепцию "профилей" - упорядоченных наборов правил, по которым производится такая проверка. Проверка идет последовательно по правилам, в порядке очереди. Сравниваются различные критерии и атрибуты в поступившем запросе: откуда, когда, каким способом, что при этом передаётся. Можно определить требуемое число профилей, для каждого метода авторизации, источника запроса и других критериев. При проверке списка профилей отсеиваются заведомо не совпавшие, а по окончании проверки выбирается самый первый из оставшихся.

Правила аутентификации могут быть применимы к следующим видам подключениям:

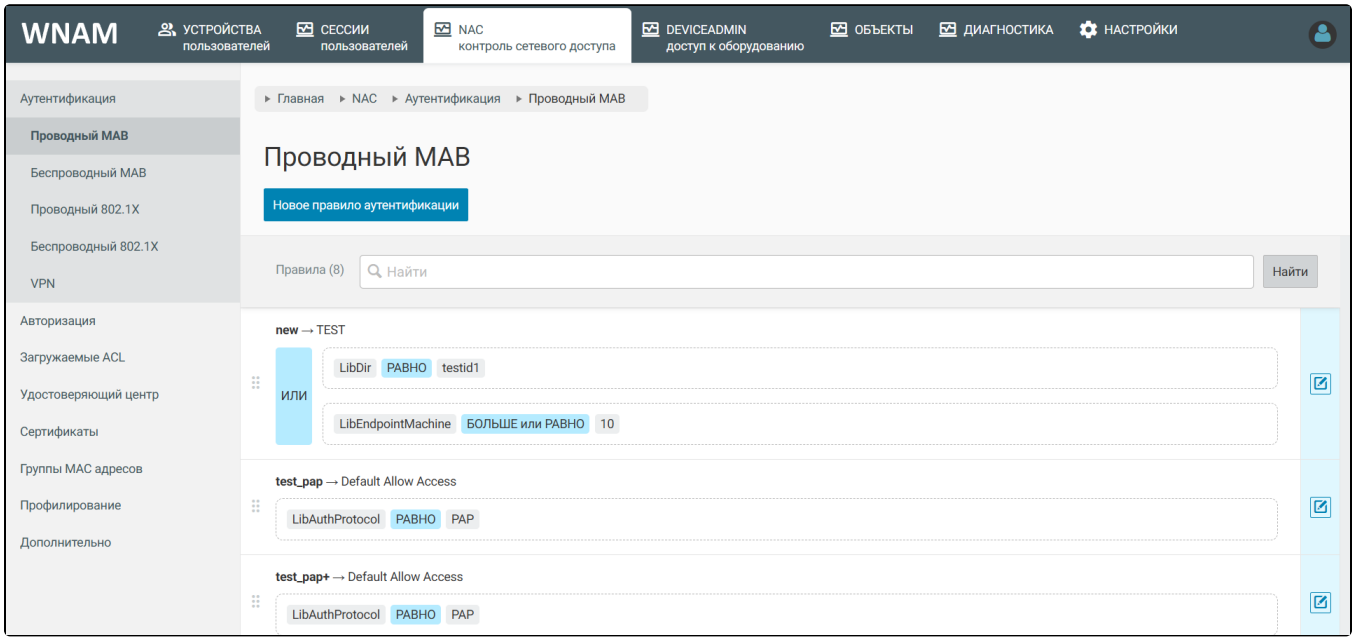
- Проводной/Беспроводной MAB;
- Проводной/Беспроводный 802,1x;
- Протокол VPN.

Внимание

В конце цепочки проверки подразумевается правило Default Deny, которое срабатывает в двух случаях:

- ошибка (exception) на стадии обработки какого-либо из правил;
- ни одно из правил аутентификации не совпало.

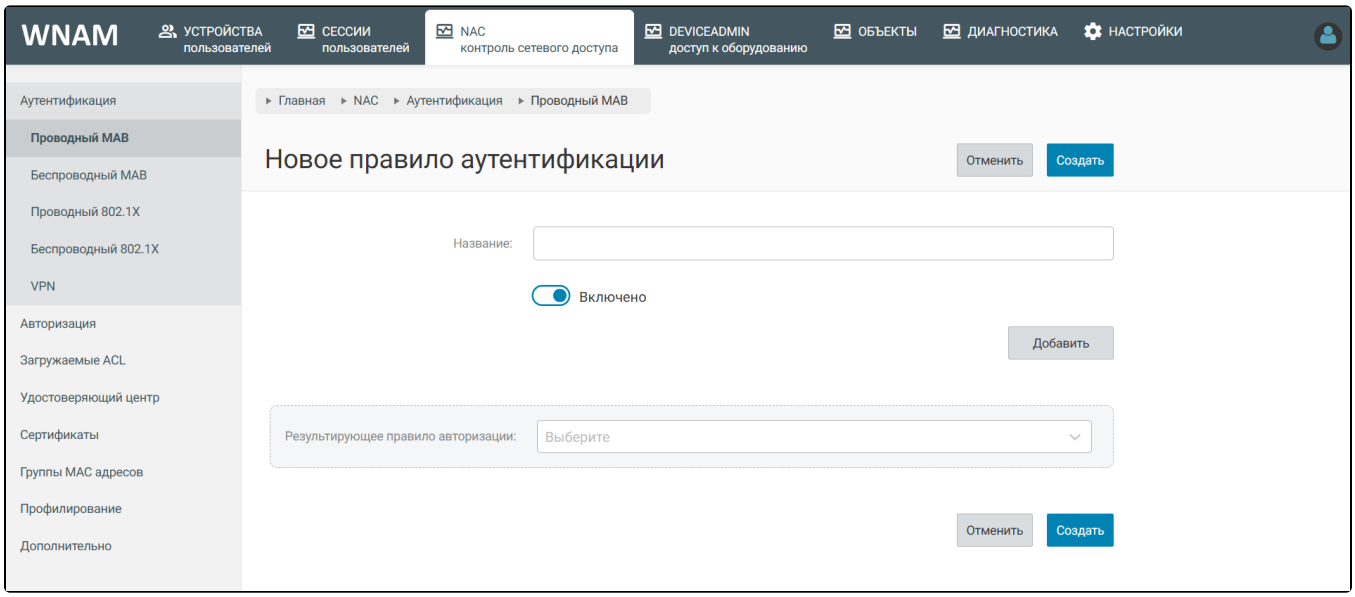
После выбора профиля определяется результат: результирующее правило авторизации. Последнее используется при выборе правила авторизации на следующем шаге проверок.



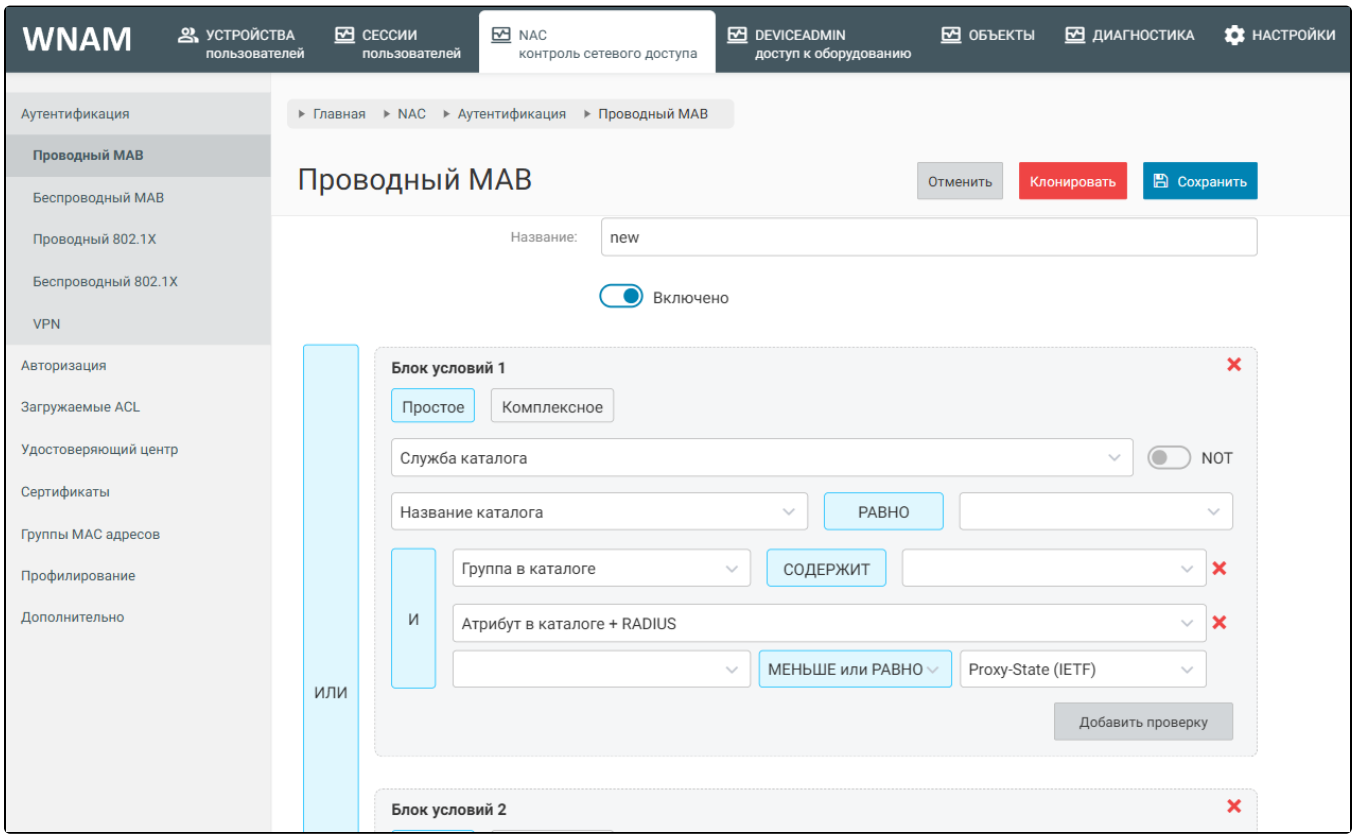
Создание и редактирование правил аутентификации

Форма создания и редактирования правил аутентификации похожи между собой, с минимальными различиями (которые также будут освещены), поэтому не имеет смысла описывать два сценария по-отдельности.

Для создания правила аутентификации, необходимо нажать на кнопку "Новое правило аутентификации", для редактирования - необходимо нажать на контекстную кнопку редактирования правила, которая находится справа от выбираемого правила. После, откроется форма по создании нового правила:



При сценарии редактирования уже имеющегося



Правила аутентификации строятся на концепции блоков для более удобного построения правил:

1. Каждый блок может содержать те или иные условия и атрибуты аутентификации (например сетевое устройство, RADIUS атрибут, профилирование, служба каталогов и т.д.).
2. В блоке может находится несколько условий в зависимости от потребности построения правил аутентификации.
3. Несколько блоков можно сгруппировать в одно комплексное условия с операторами И/ИЛИ, тем самым позволяя построить комплекс условий.

Вы можете отредактировать необходимые параметры, клонировать правило, удалить его или сохранить изменения.

⚠ Методика создания/редактирования правил аутентификации проводного/беспроводного MAB идентична для прочих видов подключения (Проводной/беспроводной MAB, 802.1x, VPN).

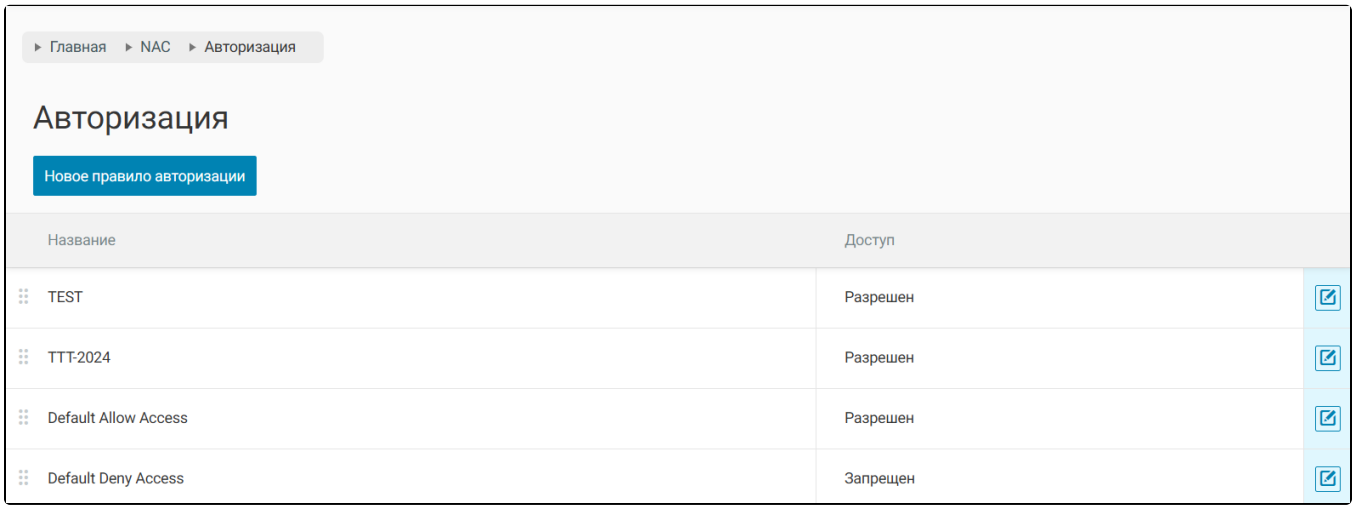
Авторизация

Авторизация — применение назначенных правил и политик аутентифицированному (подтвердившему подлинность учетных данных) абоненту сети, иначе - предоставление разрешения на выполнение действий пользователю в соответствии с назначенными ему правами. Система WNAM 2 реализует концепцию "профилей" - упорядоченных наборов правил, по которым производится такая проверка. Проверка идет последовательно по правилам, в порядке увеличения номера.
Сравниваются результаты аутентификации и выбираются атрибуты, которые будут назначены сессии доступа пользователя в возвращаемом сетевому оборудованию RADIUS-ответе. При проверке списка профилей отбрасываются заведомо не совпавшие, а по окончании проверки выбирается самый первый (по порядковому номеру) из оставшихся профилей.

В конце цепочки проверки применяется неявное правило Default Reject, которое срабатывает в трех случаях:

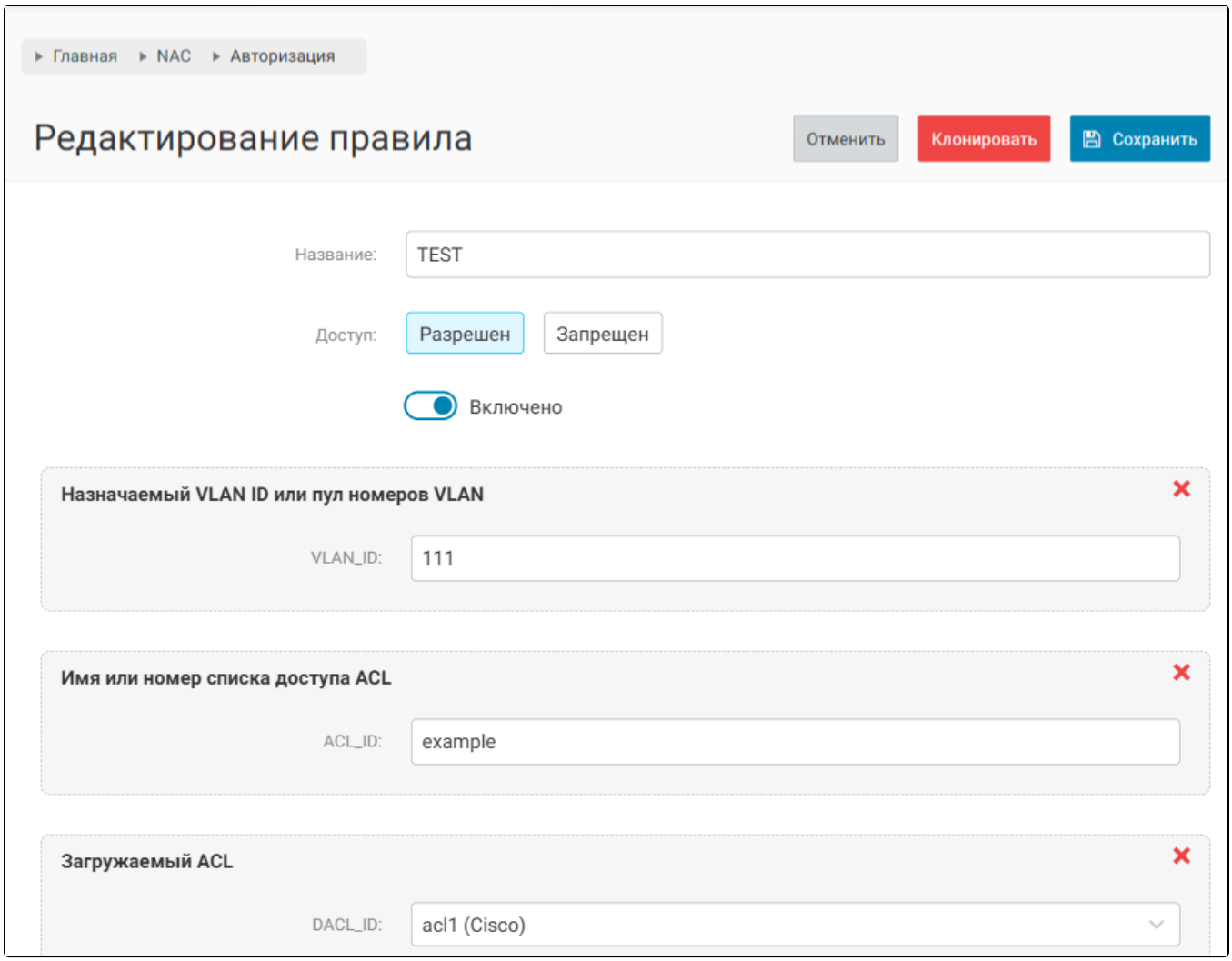
- ошибка (exception) на стадии обработки какого-либо из правил;
- ни одно правило аутентификации не совпало;
- совпало правило аутентификации Default Deny, и никаких других Deny-правил авторизации не было определено.

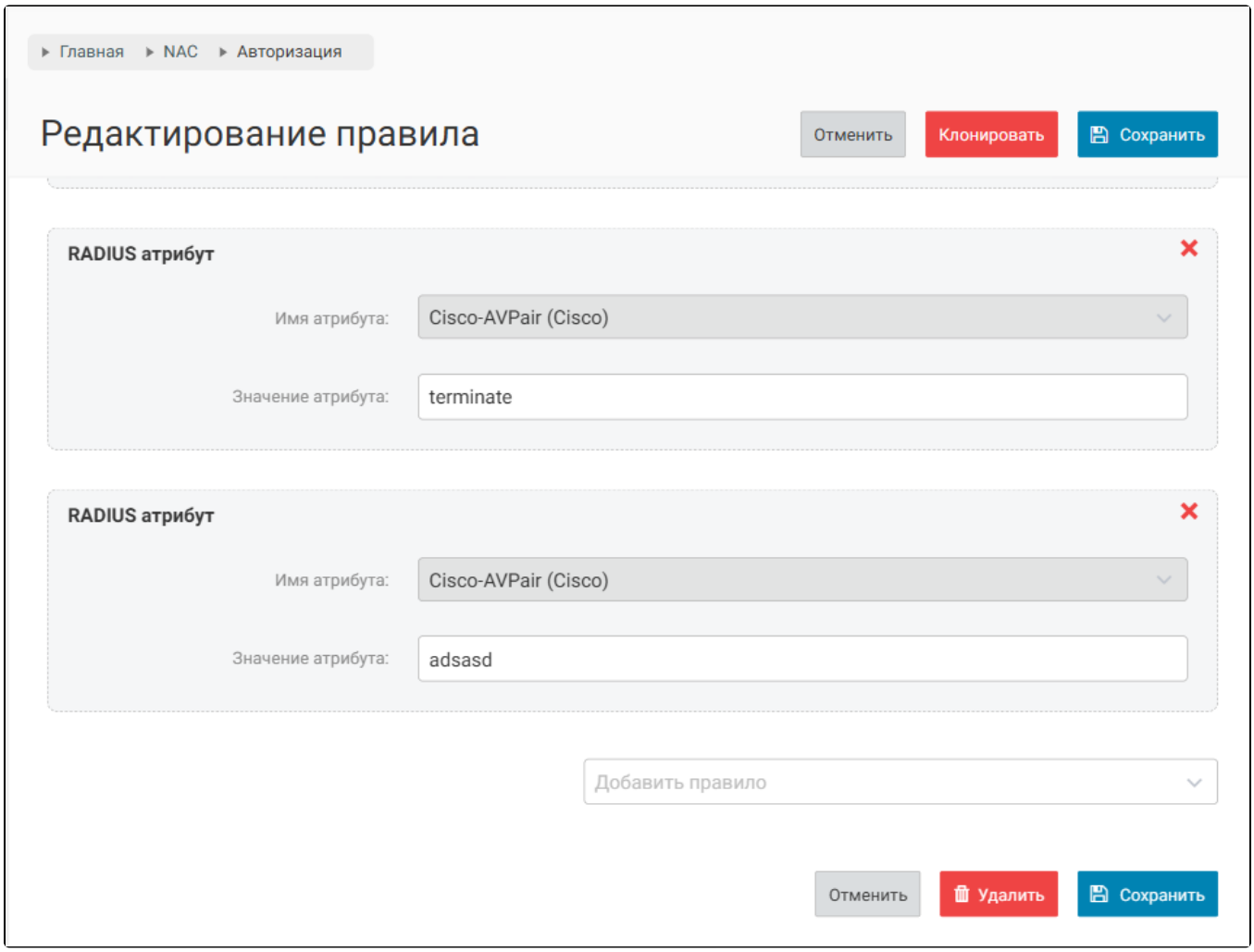
Список правил представлен в разделе "NAC - Авторизации":



В систему можно добавить сколько угодно правил. Правила также возможно поменять местами посредством перемещения позиций.

Для добавления нового правила необходимо нажать кнопку "Новое правило авторизации". При нажатии на кнопку "подробнее" в таблице открывается окно редактирования правила.


Главная
NAC
Авторизация
Редактирование правила
Отменить
Клонировать
Сохранить
Название:
TEST
Доступ:
Разрешен
Запрещен
Включено
Назначаемый VLAN ID или пул номеров VLAN
VLAN_ID:
111
Имя или номер списка доступа ACL
ACL_ID:
example
Загружаемый ACL
DACL_ID:
acl1 (Cisco)



Можно отредактировать необходимые параметры, удалить его или сохранить изменения. Ниже представлено описание настраиваемых параметров профиля.

Название - произвольное наименование правила, отображается в разделе "Диагностика" системы (пользователь его не видит).

Доступ - определяет тип RADIUS-ответа: ACCEPT или REJECT.

Включено/Отключено - определяет использование правила в работе системы.

Добавить правило - определяет, прямо или косвенно, набор атрибутов, которые будут переданы оборудованию NAS для данной сессии подключения. Возможные варианты:

- Длительность сессии;
- Загружаемый ACL - выбранный загружаемый список доступа, из заранее созданных;
- Имя или номер списка доступа ACL - номер или имя ACL, который должен быть предварительно задан на оборудовании;
- Лимит числа эндпоинтов на уникальный сертификат или логин;
- Назначаемый VLAN ID или пул номеров VLAN;
- Персональный PSK ключ (Wi-Fi);
- Возможность применения политики КИБ "Сакура";
- Реавторизация по завершении сессии;
- Тег или категория;
- RADIUS-атрибуты - набор произвольных атрибутов вида Имя=Значение, которые передаются оборудованию. Внимание! Атрибуты должны уже существовать в RADIUS-словаре системы WNAM 2. Если вы применяете экзотический атрибут и получаете ошибку, обратитесь в службу поддержки;

⚠ Набор атрибутов можно выбрать в произвольном порядке, в зависимости от потребности в создаваемом правиле. Также, в правиле возможно добавить неограниченное количество дополнительных RADIUS атрибутов.

Загружаемые ACL

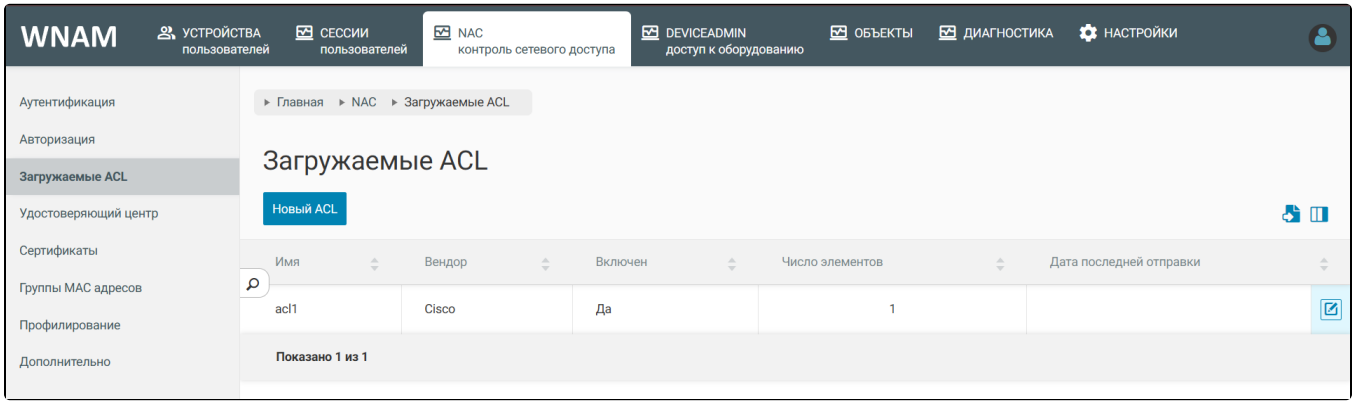
Списки управления доступом (Access Control List (ACL)) представляют собой набор правил-разрешений, которые могут быть применены к трафику пользователя на коммутаторе. Для большинства производителей сетевого оборудования ACL статически задаются на устройстве и привязываются к его сетевым портам.

Однако коммутаторы производства Cisco (Catalyst, Nexus) имеют возможность применения индивидуального ACL на порту коммутатора, после того, как на нём произведена авторизация доступа эндпоинта. Более того, содержимое этого ACL динамически загружается с сервера авторизации по протоколу RADIUS. При загрузке ACL с сервера авторизации имеется возможность на уровне системы авторизации определить, каким группам эндпоинтов назначить различные уровни доступа, ограниченные при помощи ACL.

Система WNAM 2 поддерживает:

- создание и редактирование загружаемых ACL;
- назначение заданного загружаемого ACL в профиле авторизации;
- выдачу коммутатору по запросу требуемого ACL без ограничения на его длину.

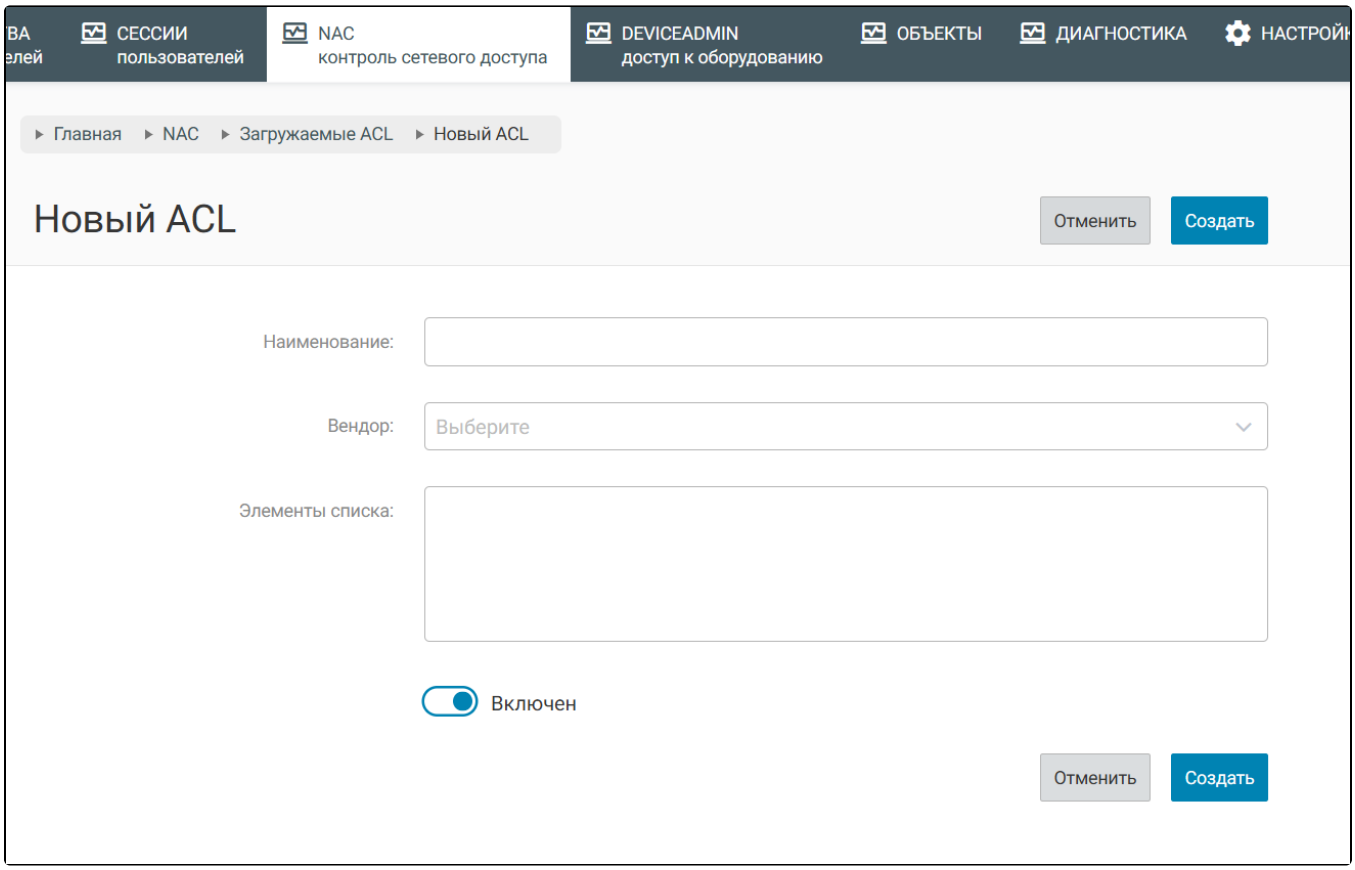
Для того, чтобы создать списки, необходимо перейти в раздел "NAC контроль сетевого доступа" "Загружаемые ACL", где можно сформировать список управления доступом или просмотреть уже загруженные списки.



Для создания нового списка необходимо нажать кнопку "Новый ACL".

Выбрать вендора оборудования, к которому список доступа будет применим.

Заполнить соответствующие поля (наименование и элементы списка).



При заполнении полей в форме следует учитывать правила:

- имя загружаемого списка должно содержать только английские буквы, цифры, дефис;
- правила в ACL указываются без номеров, без дополнительных пробелов и в формате вендора.

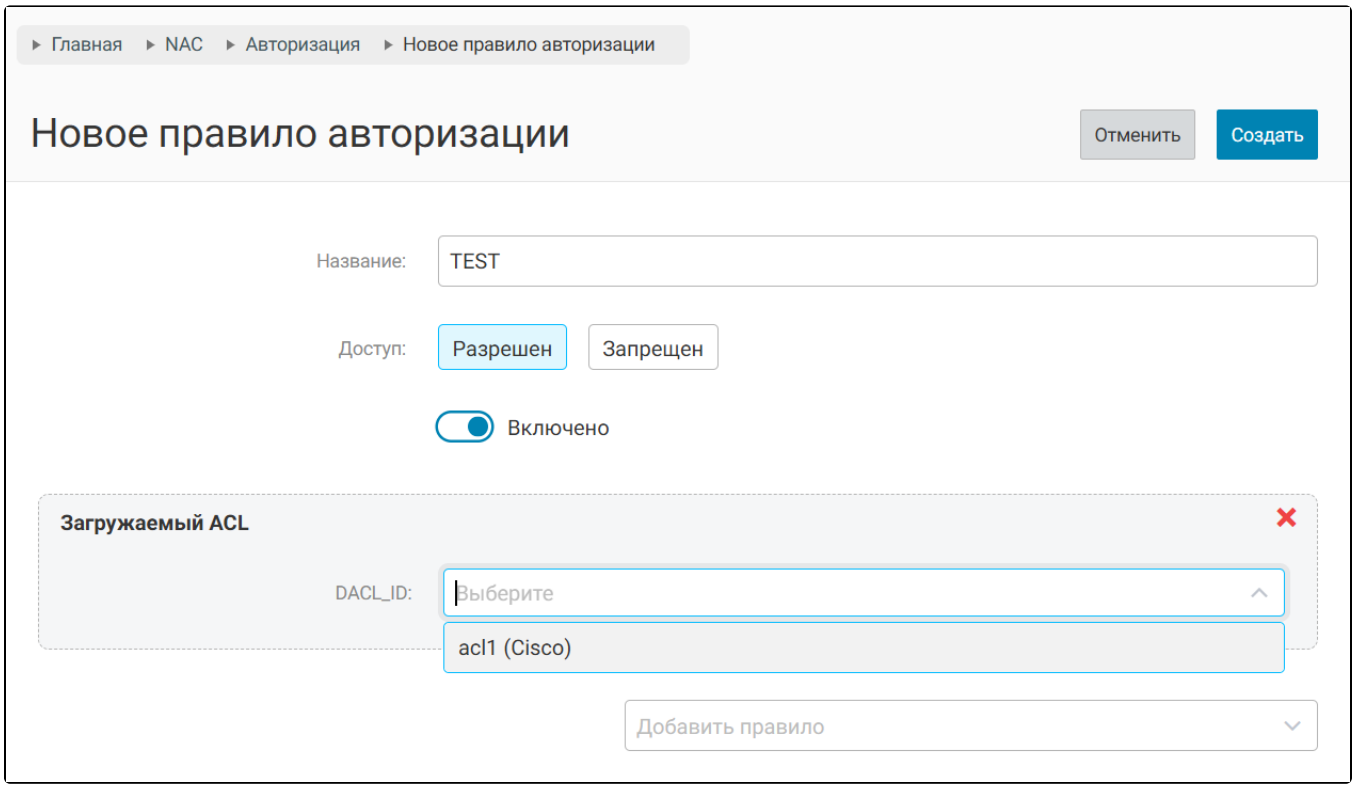
Внимание! WNAM 2 не проверяет корректность введенного ACL. Обратитесь к документации вашего вендора, в каком формате список доступа должен быть сформирован.

WNAM 2 поддерживает следующие форматы списков:

- **Cisco**: ACS:CiscoSecure-Defined-ACL, передаётся только имя списка, сам список будет загружен коммутатором дополнительными запросами.
- **Eltex**: набор атрибутов Eltex-Data-Filter, построчно кодирующих список. Документация вендора.
- **Huawei**: набор атрибутов HW-Data-Filter, построчно кодирующих список. Документация вендора.

После заполнения всех полей необходимо нажать кнопку "Сохранить". После сохранения список будет отображен в перечне загруженных ACL.

Созданный ACL можно применить в настройке требуемого правила авторизации.



При подключении эндпоинта к порту ЛВС, если произойдет срабатывание соответствующего правила, имя ACL будет передано в атрибутах:

```
16:32:51.750 TRACE [ASession.java:143] - log [60] authorization - final result: Accept with
policy 'Wired LAB'
16:32:51.751 TRACE [ASession.java:143] - log [61] authorization - add attribute: dACL Name='ACS:
CiscoSecure-Defined-ACL=#ACSACL#-IP-acl-test-1892b67bee9', lines: {}6
16:32:51.755 TRACE [ASession.java:143] - log [62] createMacCustomer - create customer entry,
MAC=CC:9D:A2:27:C6:80
16:32:51.757 TRACE [ASession.java:143] - log [63] portinfo - NAS '172.16.130.38 c2960 All
Locations#All WNAM Loc Group' port GigabitEthernet0/1 updated
16:32:51.759 TRACE [ASession.java:143] - log [64] radius - send RADIUS ACCEPT with 1 attributes
16:32:51.759 TRACE [ASession.java:143] - log [65] radius - attribute: cisco-avpair = ACS:
CiscoSecure-Defined-ACL=#ACSACL#-IP-acl-test-1892b67bee9
```

При этом коммутатор типа Cisco повторно запросит содержимое этого ACL (если таковой не был загружен ранее) и получит его:

```
16:32:51.810 INFO [WnamRadiusService.java:528] - handleRadiusPacket AUTH as=172.16.130.38,
secret_len=6, attrs=[NAS-IP-Address: 172.16.130.38, User-Name: #ACSACL#-IP-acl-test-1892b67bee9,
Vendor-Specific: Cisco[9] Cisco-AVPair: aaa:service=ip_admission, Vendor-Specific: Cisco[9] Cisco-
AVPair: aaa:event=acl-download, Message-Authenticator: 0x264a30f4d2549a263d896be6e4af328e]
16:32:51.812 DEBUG [A12Service.java:2547] - sendDownloadableACL for #ACSACL#-IP-acl-test-
1892b67bee9, Thu Jul 06 16:32:46 MSK 2023, dacl='acl-test'
16:32:51.813 DEBUG [A12Service.java:2560] - sendDownloadableACL added 6 rules, return all once
```

На стороне коммутатора загрузка ACL будет выглядеть следующим образом:

```
*Mar 12 05:36:06.506: %MAB-5-SUCCESS: Authentication successful for client (cc9d.a227.c680) on
Interface Gi0/1 AuditSessionID AC108226000000E339D9AB43
*Mar 12 05:36:06.506: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(cc9d.a227.c680) on Interface Gi0/1 AuditSessionID AC108226000000E339D9AB43
*Mar 12 05:36:06.548: RADIUS/ENCODE: Best Local IP-Address 172.16.130.38 for Radius-Server
172.16.130.5
*Mar 12 05:36:06.548: RADIUS(00000000): Send Access-Request to 172.16.130.5:1812 id 1645/63, len
140
*Mar 12 05:36:06.548: RADIUS: authenticator 1E 97 74 8F C6 29 59 7D - 8C 11 A6 F1 79 FC 57 CC
*Mar 12 05:36:06.548: RADIUS: NAS-IP-Address [4] 6 172.16.130.38
*Mar 12 05:36:06.548: RADIUS: User-Name [1] 34 "#ACSACL#-IP-acl-test-1892b67bee9"
*Mar 12 05:36:06.548: RADIUS: Vendor, Cisco [26] 32
*Mar 12 05:36:06.548: RADIUS: Cisco AVpair [1] 26 "aaa:service=ip_admission"
*Mar 12 05:36:06.548: RADIUS: Vendor, Cisco [26] 30
*Mar 12 05:36:06.548: RADIUS: Cisco AVpair [1] 24 "aaa:event=acl-download"
*Mar 12 05:36:06.548: RADIUS: Message-Authenticato[80] 18
*Mar 12 05:36:06.548: RADIUS(00000000): Sending a IPv4 Radius Packet
*Mar 12 05:36:06.548: RADIUS(00000000): Started 5 sec timeout
*Mar 12 05:36:06.557: RADIUS: Received from id 1645/63 172.16.130.5:1812, Access-Accept, len 304
*Mar 12 05:36:06.565: RADIUS: authenticator E7 F4 F3 66 48 9C 3A 21 - EB 91 D1 46 2F 2B 71 95
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 51
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 45 "ip:inacl#10=deny icmp any 1.1.1.0 0.0.0.255"
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 51
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 45 "ip:inacl#20=deny icmp any 1.1.2.0 0.0.0.255"
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 51
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 45 "ip:inacl#30=deny icmp any 1.1.3.0 0.0.0.255"
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 51
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 45 "ip:inacl#40=deny icmp any 1.1.4.0 0.0.0.255"
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 45
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 39 "ip:inacl#50=permit tcp any any eq 443"
*Mar 12 05:36:06.565: RADIUS: Vendor, Cisco [26] 35
*Mar 12 05:36:06.565: RADIUS: Cisco AVpair [1] 29 "ip:inacl#60=deny ip any any"
*Mar 12 05:36:06.565: RADIUS(00000000): Received from id 1645/63
*Mar 12 05:36:06.850: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (cc9d.a227.c680) on
Interface Gi0/1 AuditSessionID AC108226000000E339D9AB43
```

do sh ip access-lists

```
Extended IP access list xACSACLx-IP-acl-test-1892b67bee9 (per-user)
 10 deny icmp any 1.1.1.0 0.0.0.255
 20 deny icmp any 1.1.2.0 0.0.0.255
 30 deny icmp any 1.1.3.0 0.0.0.255
 40 deny icmp any 1.1.4.0 0.0.0.255
 50 permit tcp any any eq 443
 60 deny ip any any
```

Если размер загружаемого ACL велик (больше килобайта), при его отправке коммутатору список разбивается на несколько RADIUS-пакетов.

Коммутаторы других типов (не Cisco) получают ACL непосредственно в ответе, без разбивки данных. Так как, размер RADIUS-ответа не может быть большим (больше полутора килобайт), вы не сможете передать чересчур длинный ACL.

При написании правил в них вы можете воспользоваться макросами: $mac, $mac_lower, $mac_cisco, $mac_cisco_lower, $mac_condensed, $mac_condensed_lower. Соответственно это форматы вида 01:02:03:AA:BB:CC, 0102-03AA-BBCC и 010203AABBCC, также и в нижнем регистре.

При формировании отправляемого в устройство набора RADIUS-атрибутов с правилами эти макросы будут заменены MAC-адресом подключающегося клиентского устройства, в нужном формате. Так как коммутатор Cisco применяет отдельный RADIUS-запрос для получения dACL, который не содержит признака клиента, воспользоваться подобным механизмом для него не получится. Также не получится создать макрос на основе IP-адреса, т.к. он может быть назначен только после авторизации.

Тип списка доступа, который вы указываете при его создании, в основном носит справочный характер. WNAM 2 будет формировать корректный тип RADIUS-атрибута на основе типа сервера доступа, который произвел запрос, а не типа dACL. Таким образом, вы должны установить корректный тип (вендора) устройства при создании сервера доступа.

```
00.666 authorization - final result: Accept with policy 'Wired LAB'
00.668 authorization - add attribute: dACL [Huawei] Name='acl-permit-only-lan-1.1.1.1', lines: 3
```

Лог подключения:

```
23: authentication - a1profiles candidates: 1 with preliminary processing result: RadiusResponse [state=OK, attri
24: authentication - final result: Allow with policy 'EAP/AD пользователь R20 провод' and tag 'lab_lan_user'
25: authorization - a2profiles candidates: 20
26: authorization - final result: Accept with policy 'Wired LAB'
27: radius - send RADIUS ACCEPT with 8 attributes
28: radius -    attribute: MS-MPPE-Recv-Key = 0xe9245466408210a5f4e5f9acd3beb798dc64bac596687a03deae84e0d1317c7e
29: radius -    attribute: MS-MPPE-Send-Key = 0x77fa335a661245960f7ee18f71033eae8e2e529a4b57cc7b49fdb9fe47d309a7
30: radius -    attribute: EAP-Message = 0x035b0004
31: radius -    attribute: User-Name = wifitest
32: radius -    attribute: HW-Data-Filter = acl 10006 dest-ip 172.16.130.0 dest-ipmask 24 permit
33: radius -    attribute: HW-Data-Filter = acl 10007 dest-ip 1.1.1.1 dest-ipmask 32 permit
34: radius -    attribute: HW-Data-Filter = acl 10008 deny
35: radius -    attribute: Message-Authenticator = 0xd90e94fb9cde14c12b7dfab13e3c0b36
36: addIP - Set IP address 172.16.130.98 on DHCP message (MAC 00:0A:CD:44:DF:DF, Hostname: '')
```

Исключение составляет сервер доступа типа "LAN Switch": если ваш сервер доступа имеет такой тип, выбор формата направляемого атрибута определяется тем, что написано в свойствах dACL.

Удостоверяющий центр

Поскольку стандарт аутентификации и авторизации 802.1x основан на протоколе TLS, то для взаимодействия с абонентами проводной/беспроводной сети необходимо использовать **сертификат RADIUS-сервера** WNAM 2.

> Без настройки удостоверяющего центра (корневой, промежуточный сертификат CA, сертификат сервера WNAM 2 с ключом) работа по 802.1x механизмам (все протоколы авторизации типа EAP) принципиально невозможна. EAP по стандарту использует криптографию.

> Сертификат RADIUS-сервера WNAM 2 не является SSL-сертификатом, который возможно использовать для веб-интерфейса системы WNAM 2, и наоборот. В обычном сертификате веб-сервера недостаточно важных полей и свойств для полноценной работы корпоративной авторизации.

Любая экосистема сертификатов (PKI) строится на основе:

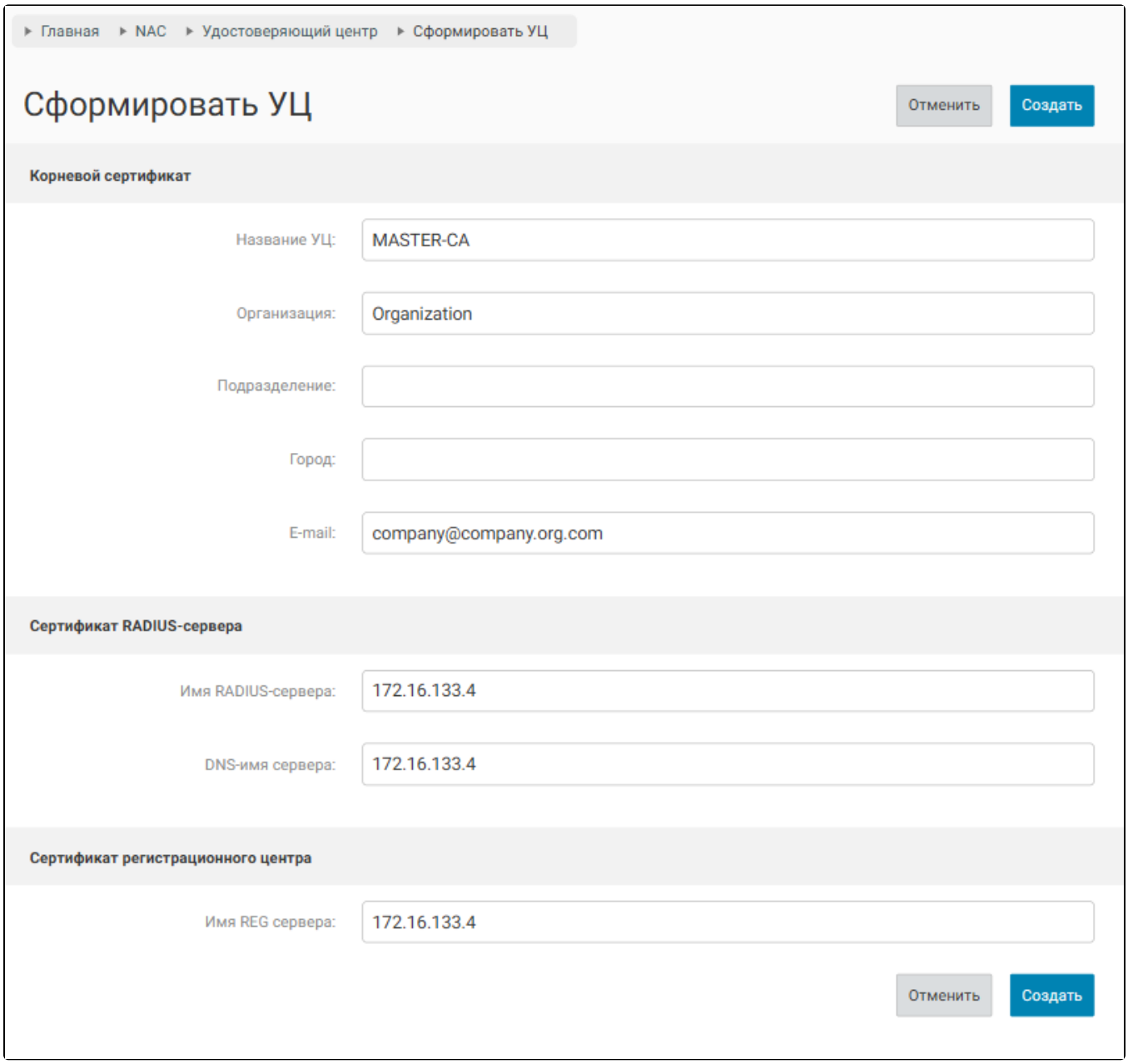
- само-подписанного корневого сертификата (сертификат должен быть в хранилище доверенных корневых сертификатов подключающегося сетевого устройства, он попадает в хранилище из операционной системы или её обновлений, устанавливается вручную через MDM-систему или через групповую политику домена);
- выпущенного экосистемой PKI сертификата сервера (сертификат используется RADIUS-сервером WNAM 2 для установления TLS-соединения с клиентом);
- выпущенного экосистемой PKI (прямо или косвенно) клиентского сертификата (используется только для EAP-TLS авторизации).

Система WNAM 2 позволяет подготовить и выпустить собственные корневой сертификат, сертификаты серверов, клиентские сертификаты, а также импортировать корневые и серверные сертификаты, выпущенные вашим центром сертификатов PKI. При этом поддерживается одновременная работа и с теми, и с другими сертификатами, нона практике используется либо встроенный в WNAM 2 центр PKI, либо ваш центр сертификатов предприятия .

При первом запуске системы WNAM 2 хранилище сертификатов пусто, и корпоративная авторизация не будет работать, пока в системе не появится хотя бы один корневой сертификат и хотя бы один сертификат сервера. Сертификаты системы настраиваются в административном интерфейсе системы WNAM 2 в разделе "NAC контроль сетевого доступа" "Удостоверяющий центр". Если сертификаты в указанном разделе отсутствуют, вы можете:

- инициализировать новый (встроенный) Удостоверяющий Центр
- импортировать сертификаты вашего имеющегося УЦ, и сформировать запрос на серверный сертификат

Процедура инициализации описана ниже.

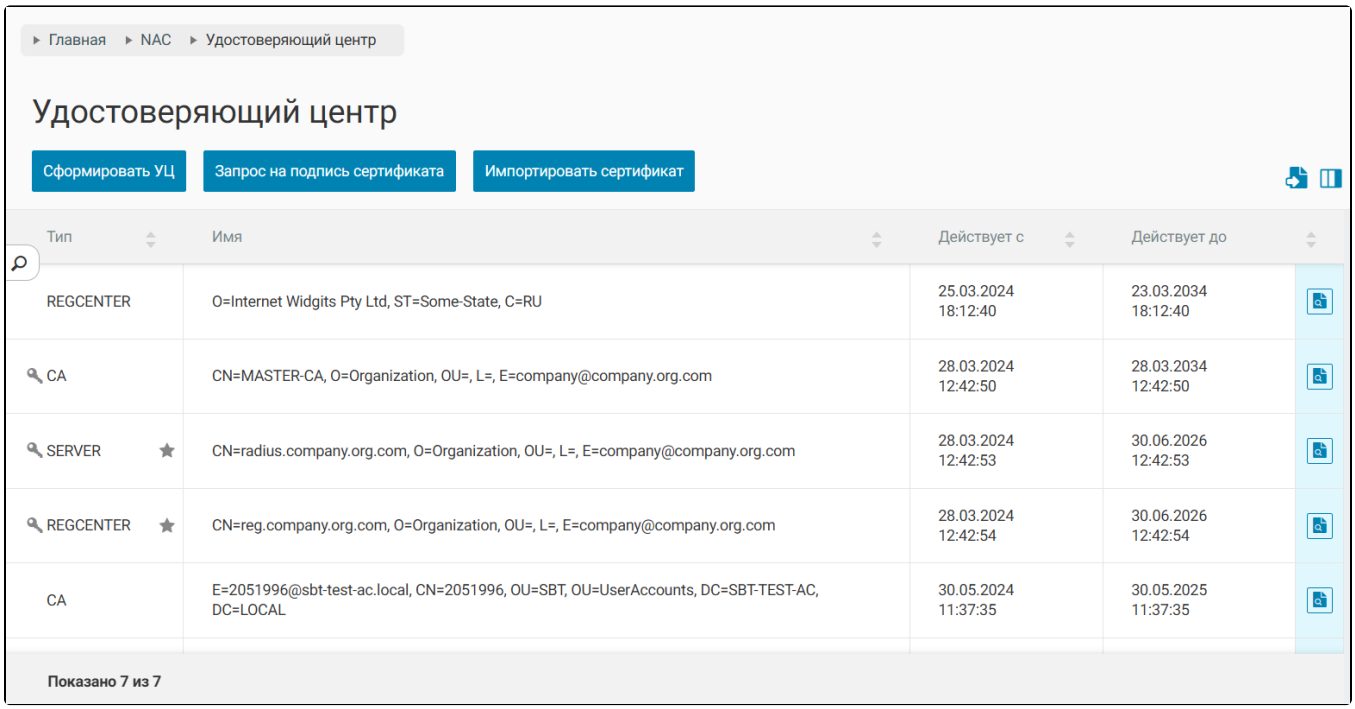


Для создания удостоверяющего Центра необходимо заполнить предложенную форму. При этом будет создано три сертификата: корневой, сертификат RADIUS-сервера и промежуточный сертификат, который будет использоваться для подписи выдаваемых сертификатов клиентам. Все три сертификата создаются вместе с закрытыми ключами и хранятся в БД WNAM 2 в коллекции **wnam2_db/certificateAuthority** в зашифрованном виде.

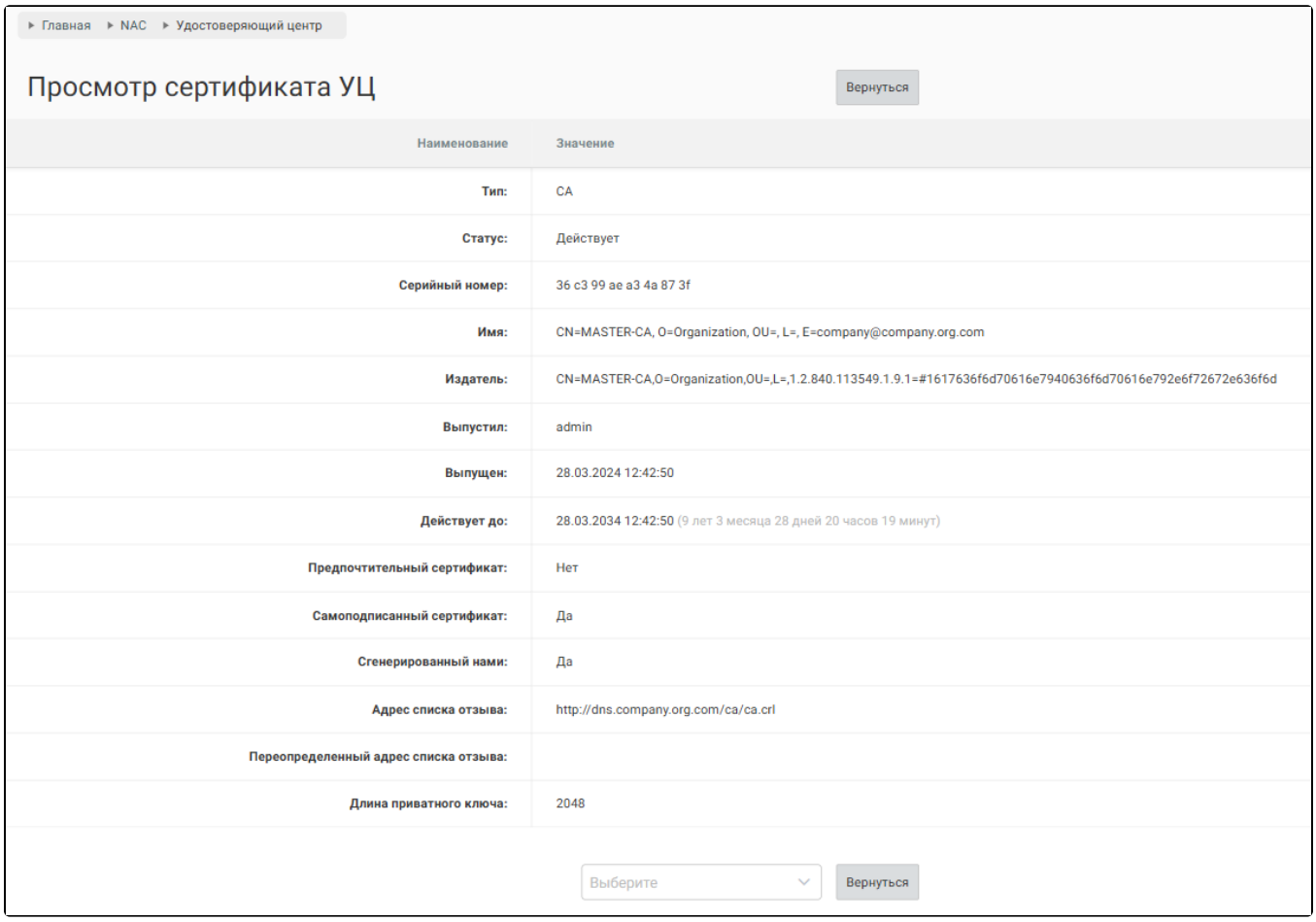
Их создание займет порядка 10 секунд, а в логе **wnam2.log** появятся записи вида:

```
14:07:29.954 DEBUG [c.n.w.manager.CACertificateManager:277] - Certificate authority creation
time: 7 sec.
14:07:29.965 DEBUG [c.n.w.manager.CACertificateManager:178] - CACertificateManager accepted
client cert issuer: CN=WNAM Lab Root CA, O=Netams. LLC, OU=Development, L=Moscow,
EMAILADDRESS=support@netams.com
14:07:29.966 DEBUG [c.n.w.manager.CACertificateManager:178] - CACertificateManager accepted
client cert issuer: CN=Registry Server, O=Netams. LLC, OU=Development, L=Moscow,
EMAILADDRESS=support@netams.com
14:07:29.966 DEBUG [c.n.w.manager.CACertificateManager:180] - CACertificateManager TLS server:
CN=Auth Server, O=Netams. LLC, OU=Development, L=Moscow, EMAILADDRESS=support@netams.com
```

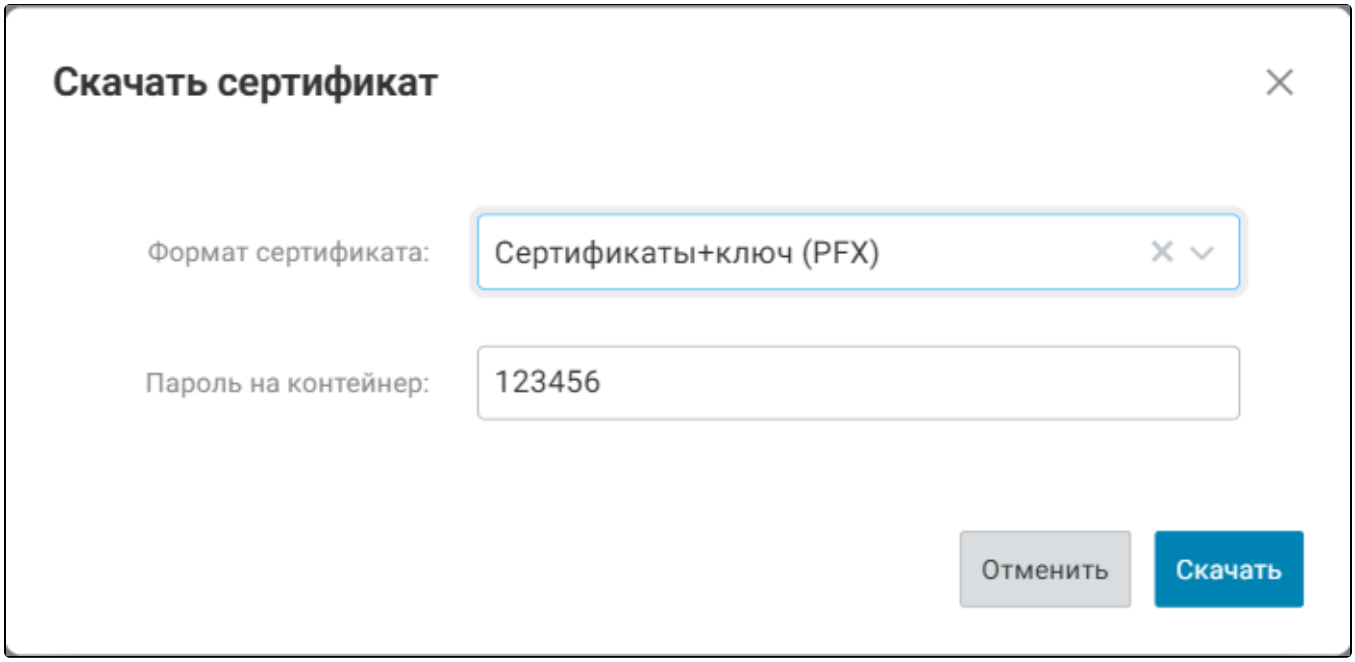
Созданные сертификаты будут отображены в таблице.



Наличие "ключа" (значок напротив сертификата) указывает на наличие закрытого ключа. Сертификат можно скачать и посмотреть его свойства. Звёздочкой отмечен предпочтительный (по умолчанию) сертификат типа SERVER или REGCENTER, что позволяет выбирать один из них, если их несколько.



Запрос на экспорт сертификата с закрытым ключом (в формате PFX) отобразит ещё одно окно, в котором необходимо задать пароль на экспортируемый контейнер типа PKCS#12 (по умолчанию "123456").



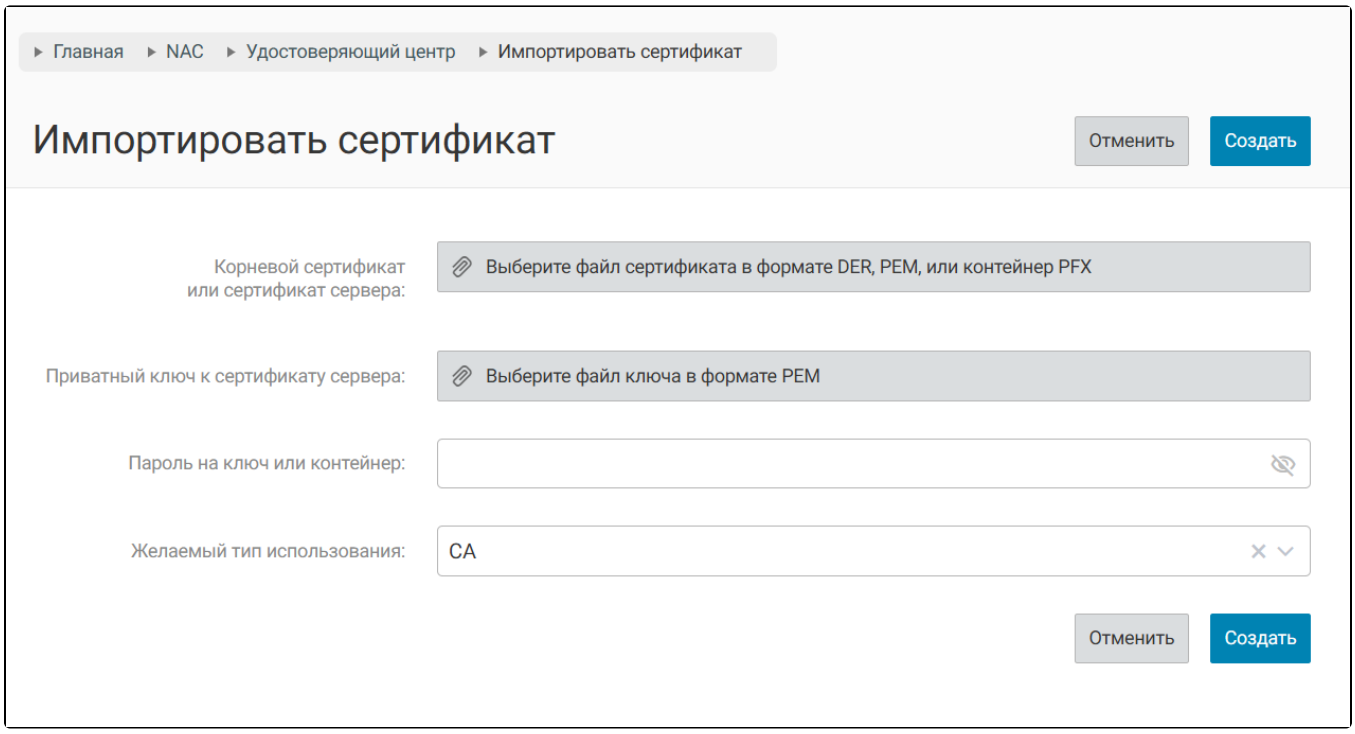
Для распространения сертификата клиентам понадобится, как минимум, сертификат удостоверяющего центра (без ключа).

Встроенный центр сертификатов системы WNAM 2 является минимально достаточным для работы авторизации. Встроенный центр сертификатов не является полноценной системой PKI, в ней нет механизмов OCSP и SCEP, а также многого другого.
В целях безопасности удалить созданные сертификаты центра сертификации из интерфейса администратора WNAM 2 нельзя: их удаление возможно только напрямую из базы данных.

Авто-создание собственного Центра можно пропустить, закрыв соответствующее окно. В таком случае необходимо импортировать в систему WNAM 2, как минимум, два сертификата:

- корневой сертификат вашего предприятия (без ключа);
- сертификат RADIUS-сервера WNAM 2, выписанный внешними средствами, включая его закрытый ключ.

Если требуется создание сертификата через запрос внешнему удостоверяющему центру, то следует действовать согласно инструкции в разделе "Запрос подписи сертификата" (здесь). Импортировать готовый сертификат можно, нажав кнопку "Импортировать сертификат" в разделе "NAC контроль сетевого доступа" "Удостоверяющий центр".



В открывшемся окне необходимо ввести требуемые параметры:

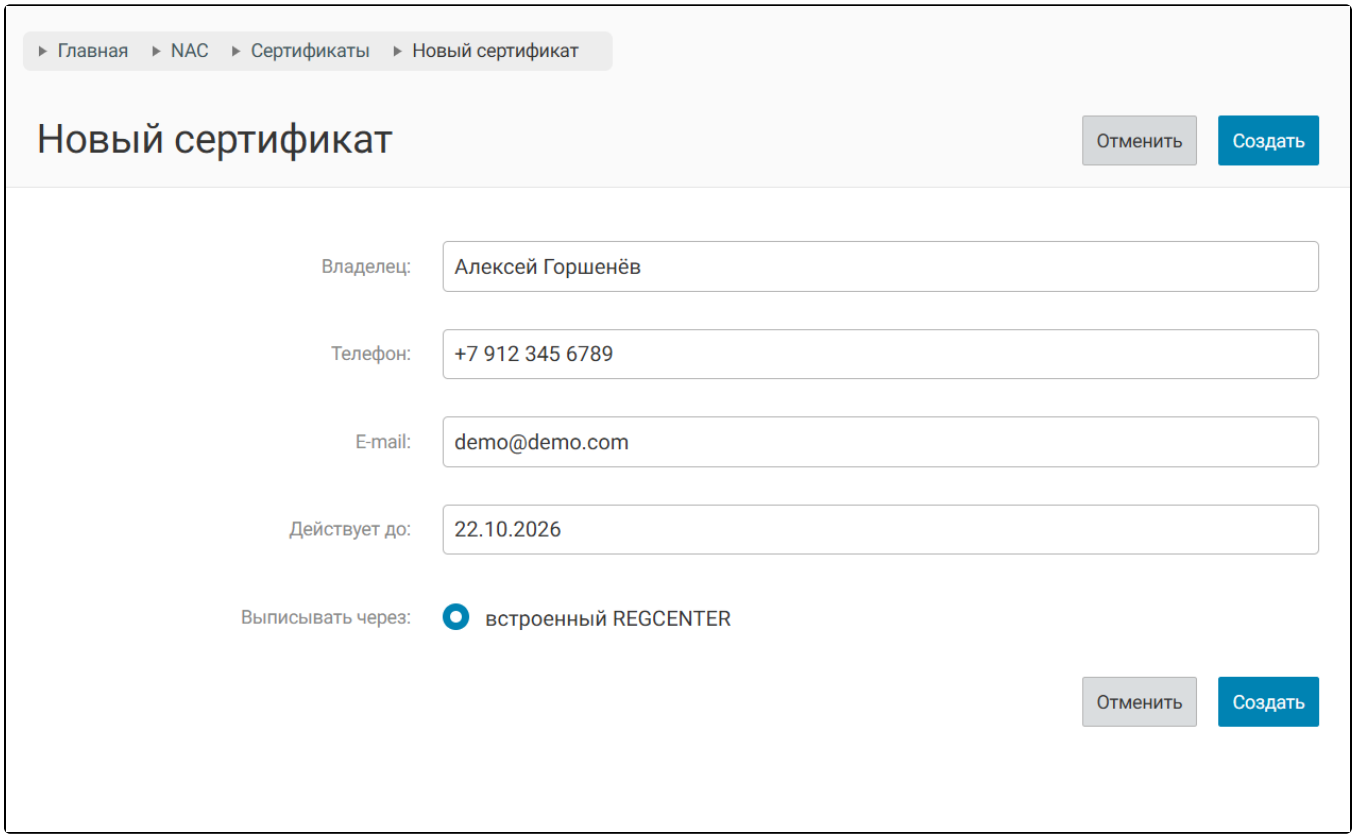
- для импорта корневого сертификата - выбрать файл сертификата в бинарном (DER) или текстовом BASE64 (PEM) формате;
- для импорта сертификата сервера необходимо выполнить одно из двух действий:
  - выбрать файл сертификата в бинарном (DER) или текстовом BASE64 (PEM) формате, а также файл закрытого ключа сертификата (в текстовом BASE64 формате в контейнере PKCS#8 или PKCS#1), при этом ключ должен быть без пароля;
  - выбрать файл контейнера сертификата в бинарном PKCS#12 (PXF или P12) формате, и задать пароль на контейнер.

Нажать кнопку импорта "Создать", после чего сертификат будет загружен и отображен в списке сертификатов.

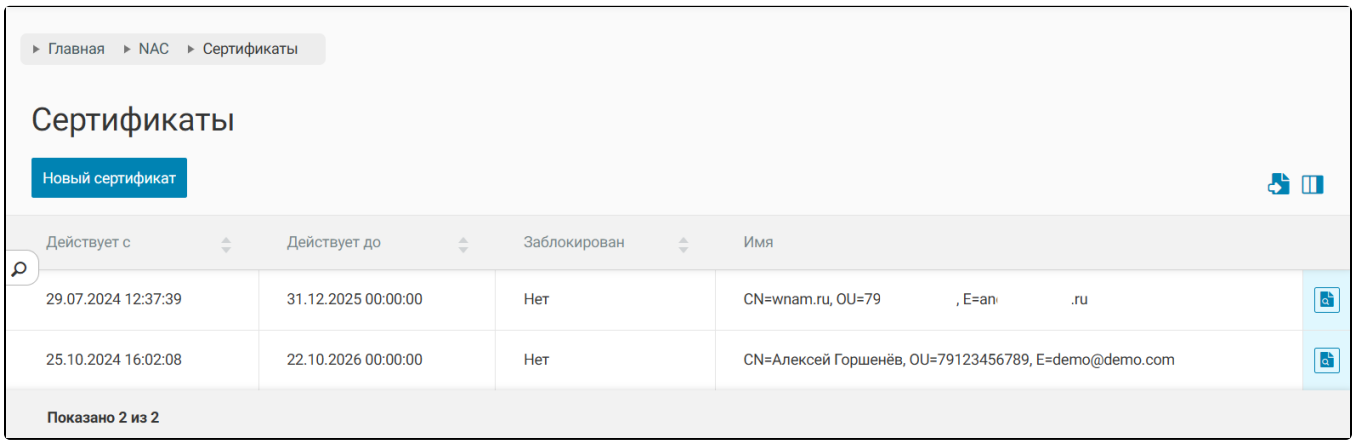
Операция импорта сертификатов вызывает переинициализацию EAP-модуля внутри RADIUS-сервера системы WNAM 2, при этом в лог-файле **wnam2.log** будут отображены все валидные серверные и CA-сертификаты.

Сертификаты

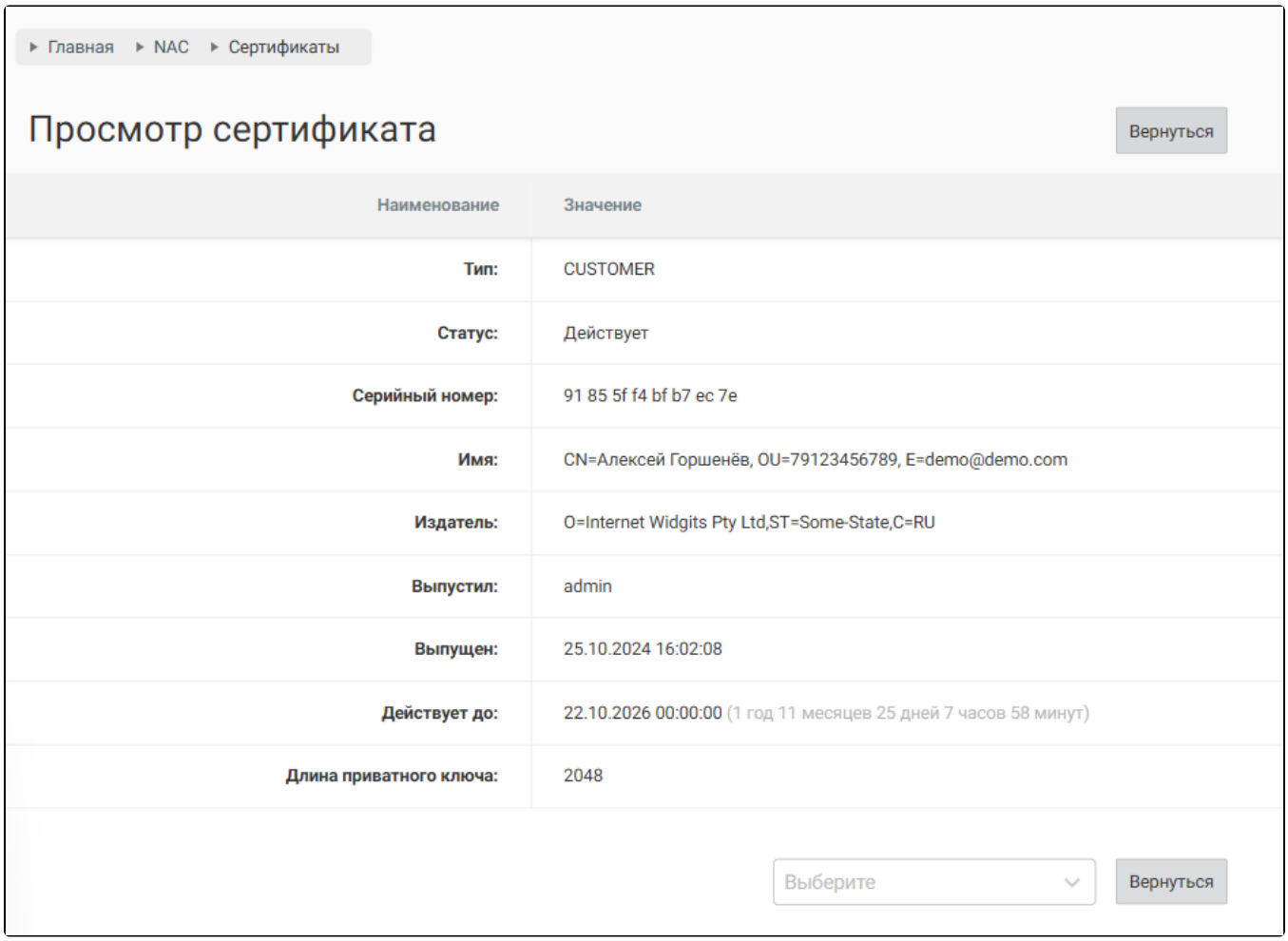
Если в вашем Удостоверяющем Центре WNAM 2 есть хотя бы один сертификат типа REGCENTER (с закрытым ключом), вы можете вручную создавать в нём сертификаты для абонентов, которые будут проходить авторизацию подключений через EAP-TLS. Для этого в меню "NAC контроль сетевого доступа" "Сертификаты" необходимо нажать кнопку "Новый сертификат" и заполнить все поля (наименование владельца сертификата, номер телефона и e-mail). После заполнения всех полей следует нажать кнопку "Выписать"



Создание сертификата занимает несколько секунд (в это время происходит генерация нового приватного ключа). Сертификат после создания будет отображен в списке.

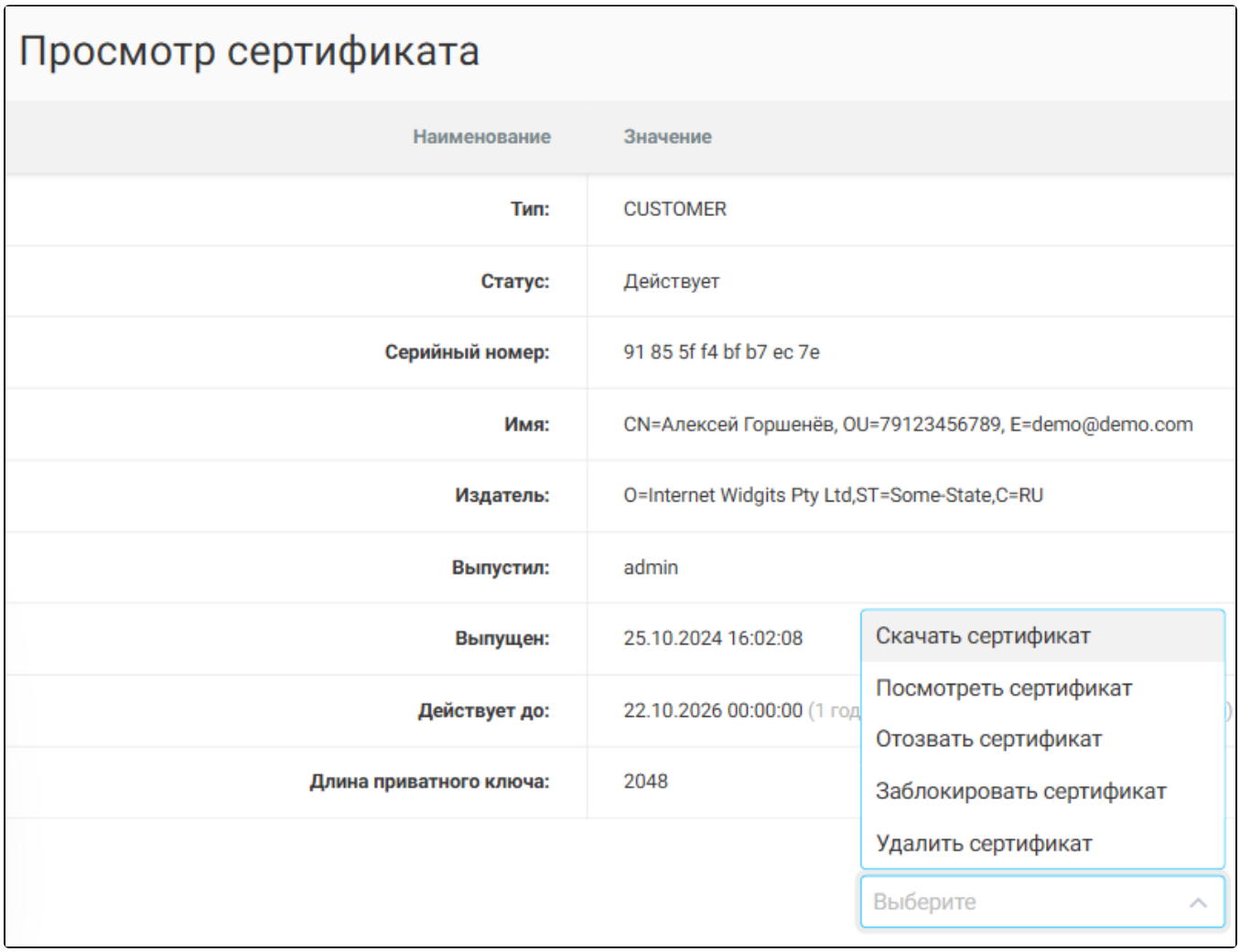


Также можно просмотреть свойства созданного сертификата, выгрузить сертификат (с ключом) в формате PFX и передать его пользователю. Для этого следует нажать на контекстное меню "открыть подробности" выбираемого сертификата.

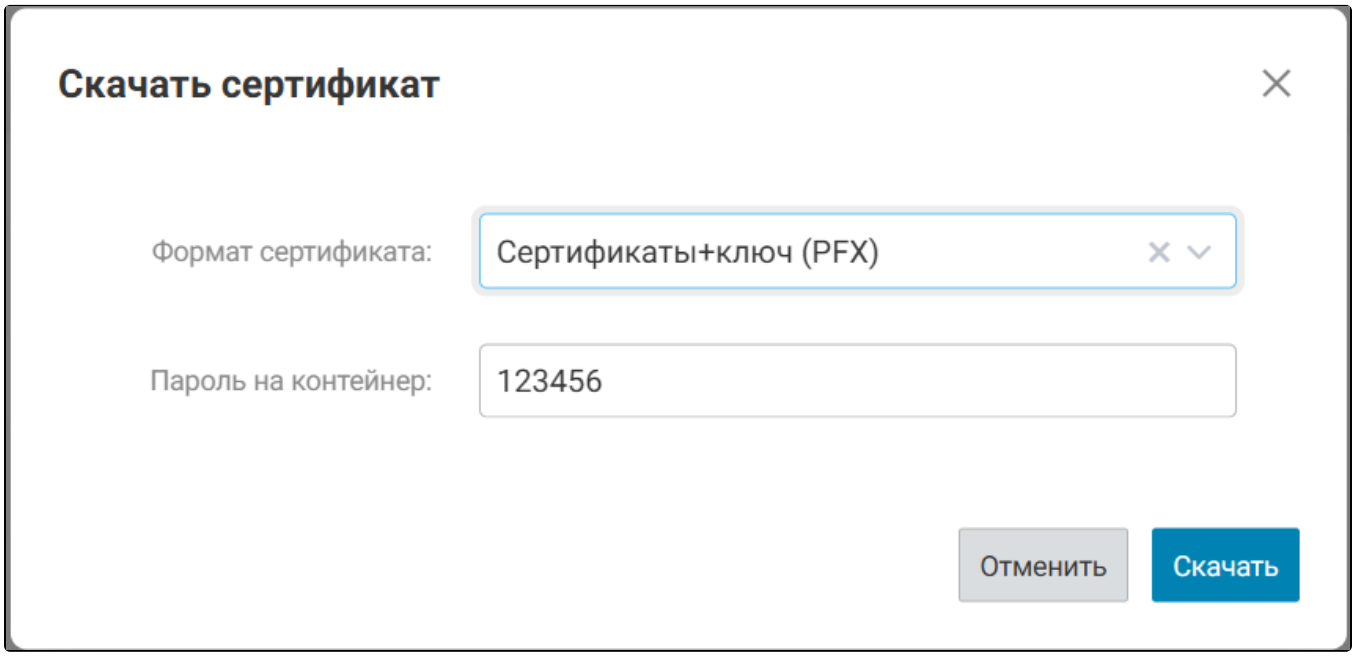


С сертификатом доступные следующие действия:

- скачать сертификат (на выбор предоставлено 5 форматов для скачивания);
- отправить сертификат на почту или телефон;
- отозвать сертификат;
- заблокировать сертификат;
- разблокировать сертификат;
- удалить сертификат.

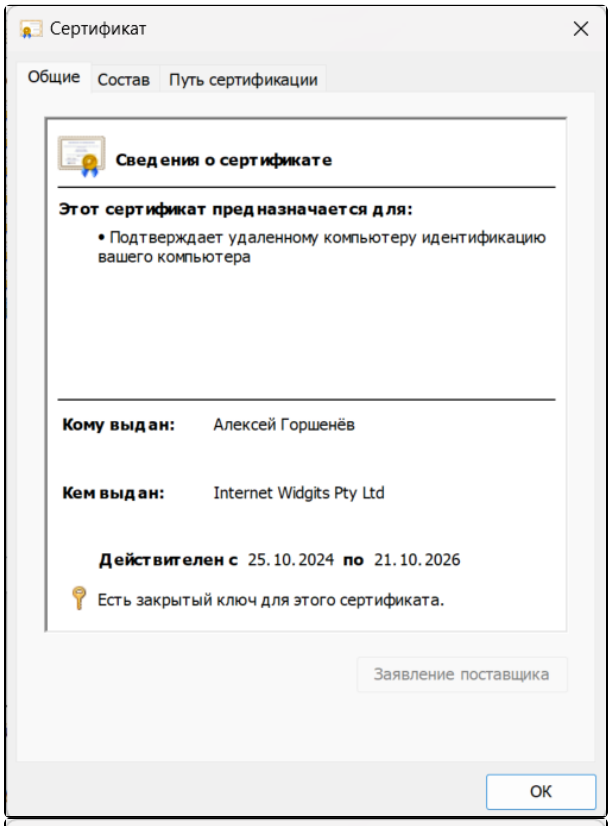


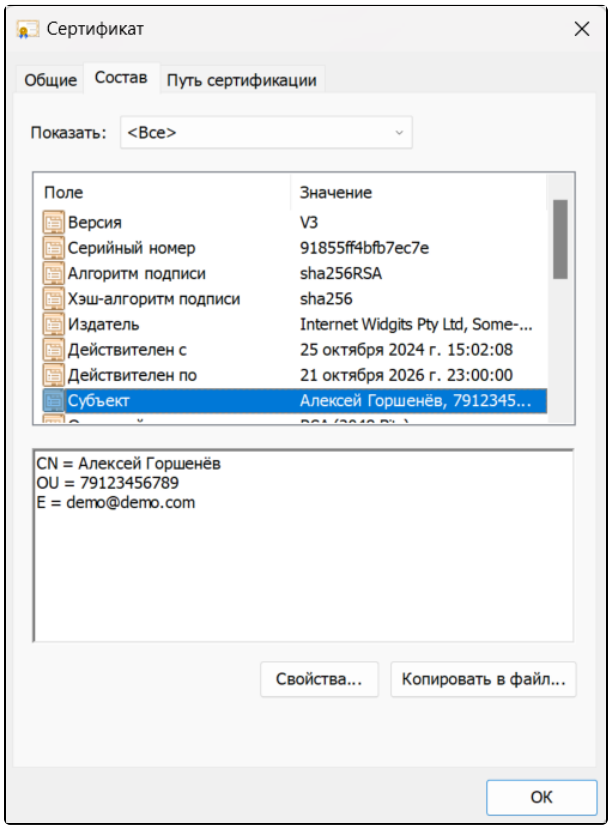
При экспорте сертификата можно указать пароль:

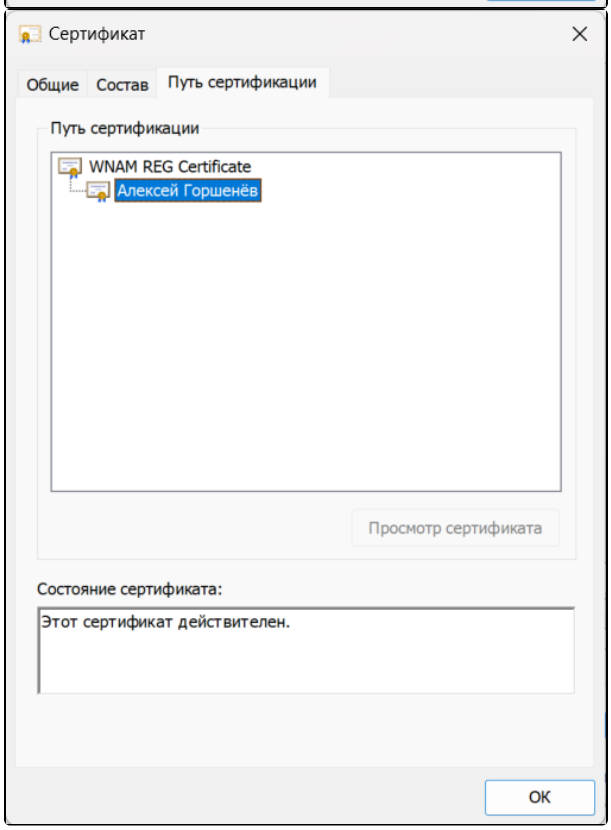


⚠ Пароль по умолчанию устанавливается **123456**.

Видно, что созданный сертификат выпущен встроенным в систему WNAM 2 регистрационным центром.







В дальнейшем будет предусмотрена функция отправки сертификата в виде устанавливаемого профиля.

Следует обратить внимание на то, что система WNAM 2 при EAP-TLS подключении может проверять клиентские сертификаты на предмет их действия (не отозван ли сертификат), запрашивая указанный в самом сертификате URL, по которому размещен список отозванных сертификатов. Для сторонних (выпущенных вашим собственным PKI) этот URL должен быть доступен серверу.

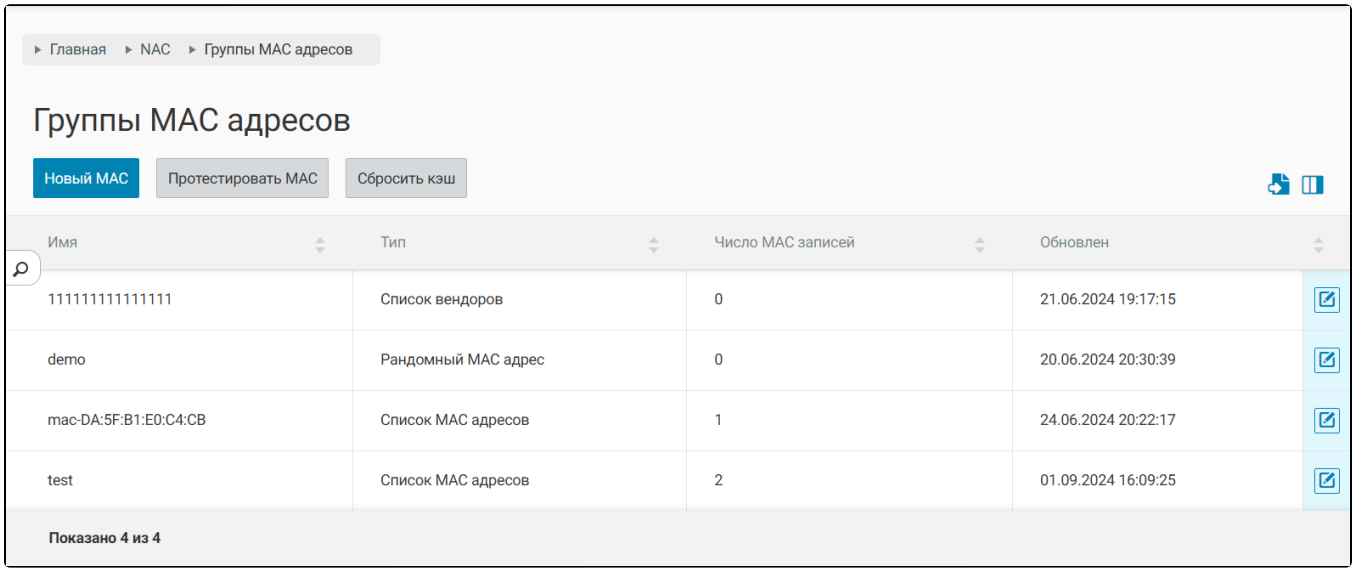
Для встроенного Центра сертификации системы WNAM 2 этот URL соответствует имени сервера, который был задан при генерации Центра в параметре "Сертификат RADIUS-сервера - DNS-имя сервера". Это должно быть именем WNAM-сервера, желательно доступным "снаружи" используемой сети. Путь до CRL всегда одинаков:

- http://имя_сервера/ca/ca.crl (для списка корневого сертификата);
- http://имя_сервера/ca/reg.crl (для списка отозванных сертификатов регистрационного Центра, которым выписываются клиентские сертификаты).

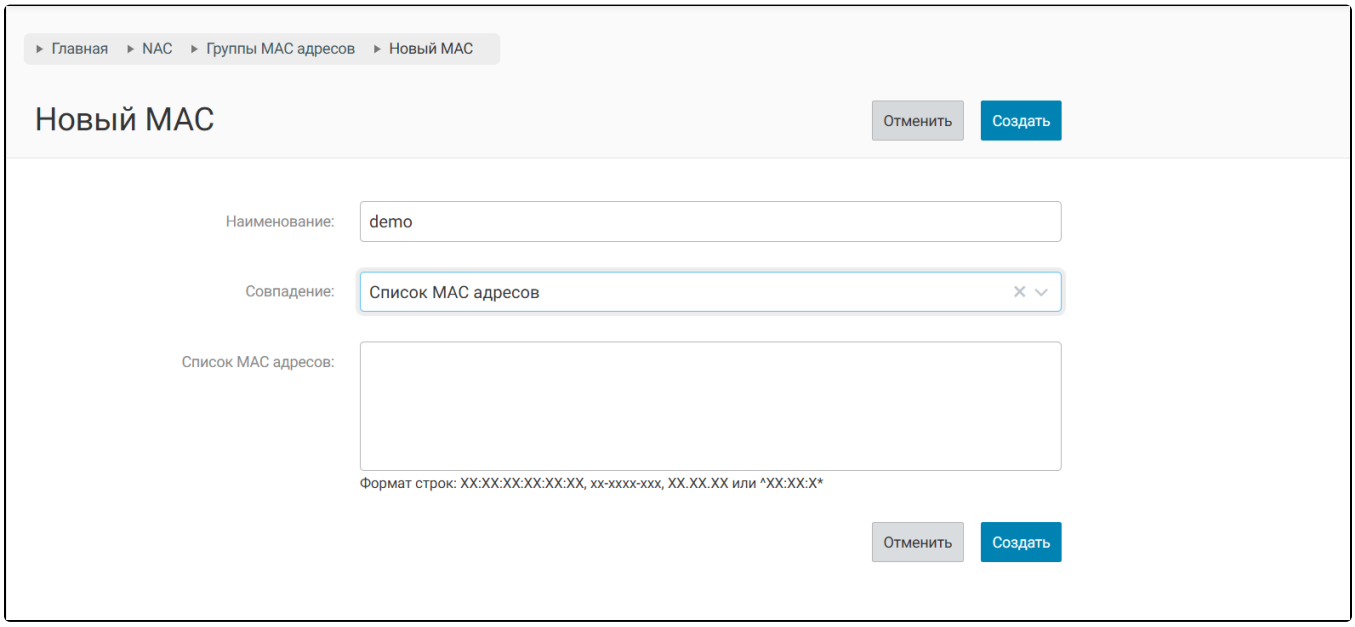
Группы MAC адресов

Профилирование устройств по группам MAC-адресов задают правила определения типа устройств на основе только его MAC-адреса. Это позволяет реализовывать гибкие политики авторизации, например, назначение VLAN или ACL в зависимости от принадлежности оконечного устройства той или иной группе. Таким образом, основываясь на MAC-адресах, возможно назначить разные VLAN компьютерам, принтерам, СКУД (системам контроля и управления доступом) и IP-камерам. В системе может быть настроено множество профилей устройств. Изначально автоматически создаются несколько встроенных профилей, которые можно редактировать самостоятельно. Это, в основном, профили с именами вендоров оборудования, наиболее часто встречающихся в таблице OUI. При необходимости можно ознакомиться с информацией о структуре MAC-адреса. Система WNAM 2 содержит в себе актуальную базу данных вендоров и присвоенных им групп адресов.

Административный интерфейс системы доступен в разделе "Главная" "NAC контроль сетевого доступа" "Группы MAC адресов" и представляет собой таблицу (список) настроенных групп, а также дополнительные кнопки.



Кнопка "Создать новый" открывает окно создания новой группы. Такое же окно открывается и при редактировании существующей группы при нажатии левой кнопкой мыши на строку таблицы.

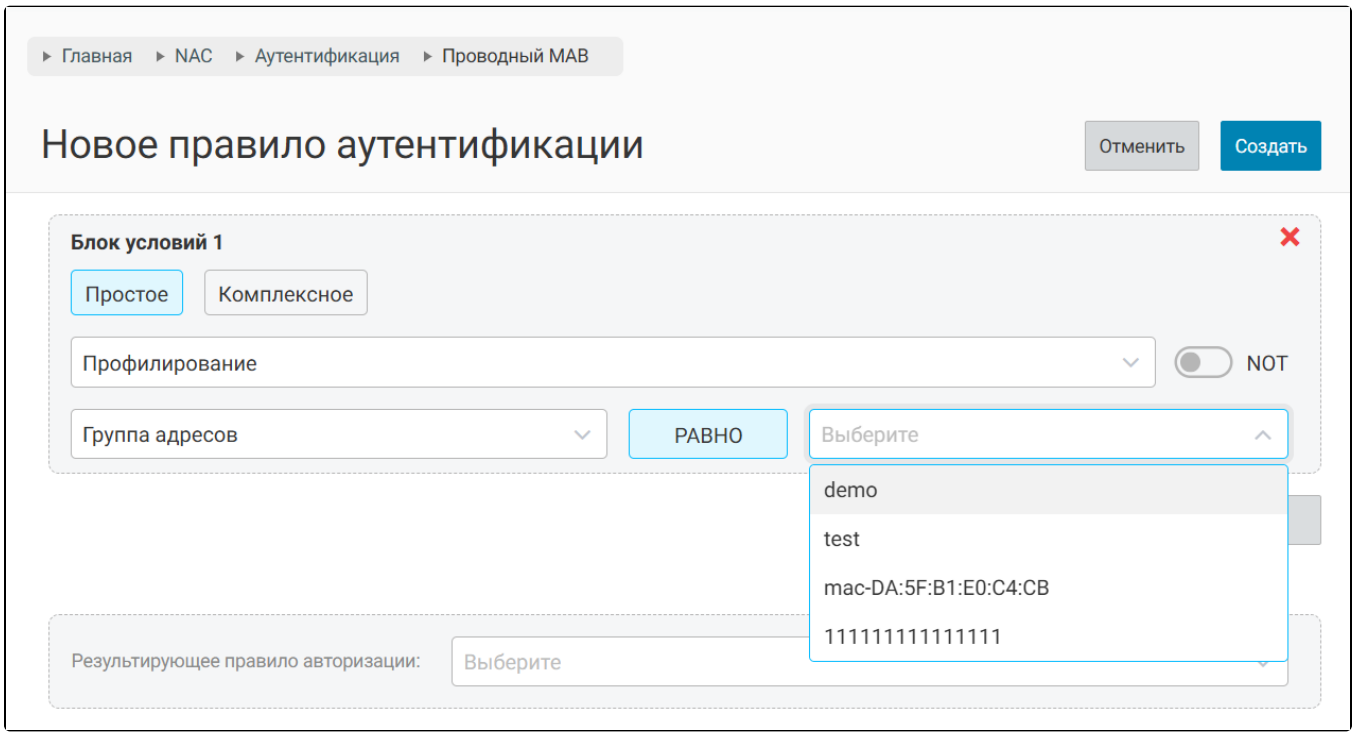


В данном окне необходимо задать название группы, и выбрать режим её работы. При этом доступны следующие варианты:

- **Список MAC адресов** предназначен для задания одного или нескольких MAC-адресов. Формат записи MAC-адреса - любой: XX:XX:XX:XX:XX:XX, xxxx-xx-xxxx, а также допустимы регулярные выражения с символами ^ и *. После сохранения выбранных настроек таблица будет отформатирована.

- **Список вендоров** предназначен для выбора необходимого вендора устройств из выпадающего списка TOP-50.
- **Вендор** предназначен для задания имени вендора в том виде, в каком он присутствует в таблице OUI.
- **Рандомный MAC адрес** предназначен для задания адреса, используемого мобильными устройствами для подключения к Wi-Fi, включая Google Random адрес.
- **Любой из выбранных вложенных профилей** отвечает за совпадение на основе других профилей, позволяет объединять несколько профилей в логические группы.

Подсистема профилирования WNAM 2 при поступлении запроса по MAC-адресу перебирает все имеющиеся профили, и в каждом профиле ищет совпадение. В результате поиска останется набор (возможно, пустой) совпавших профилей. Полученный набор применяется при анализе политик аутентификации. Для этого в настройках политики можно указать желаемый профиль.



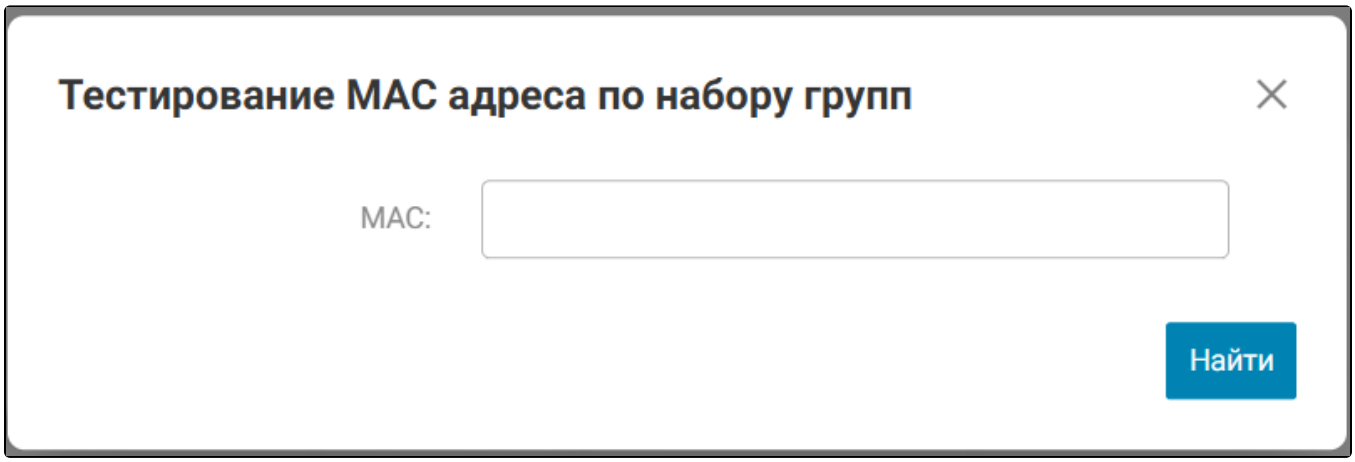
Несмотря на то, что профиль указывается только при MAC-Based, т.е. MAB-авторизации по методу RADIUS PAP, механизм профилирования срабатывает и для остальных типов (EAP-*) запросов.

При срабатывании механизма профилирования в такой проверки в лог-файле появляется запись следующего типа:

> *22:17:34.136 TRACE [ASession.java:139] - log [1] fillFromRadiusAttributes - identity: '54:88:0E:02:84:6D', portType: WirelessMAB*
> *22:17:34.145 DEBUG [DeviceProfileManager.java:70] - matchProfile mac=54:88:0E:02:84:6D, from_cache=no*
> *22:17:34.165 TRACE [ASession.java:139] - log [7]* ***matchDeviceProfiles - matched: 'Вендор: Samsung'***
> *22:17:34.205 TRACE [ASession.java:139] - log [8] findOrCreate - a1profiles candidates: 10, a2profiles candidates: 16*

Для ускорения работы система WNAM 2 использует кэширование в матчере (поисковике) профилей (длительность хранения данных в нём по умолчанию 17 часов). Кэш можно очистить, нажав на кнопку "Сбросить кэш" в основном окне списка профилей. Чистить данные в кэше следует, если были отредактированы некоторые профили и требуется, чтобы отредактированные настройки применились к ранее профилированным устройствам заново.

Дополнительно для целей тестирования в основном интерфейсе раздела "Группы MAC адресов" существует кнопка "Протестировать MAC". При нажатии на неё левой кнопкой мыши будет отображено окно теста.

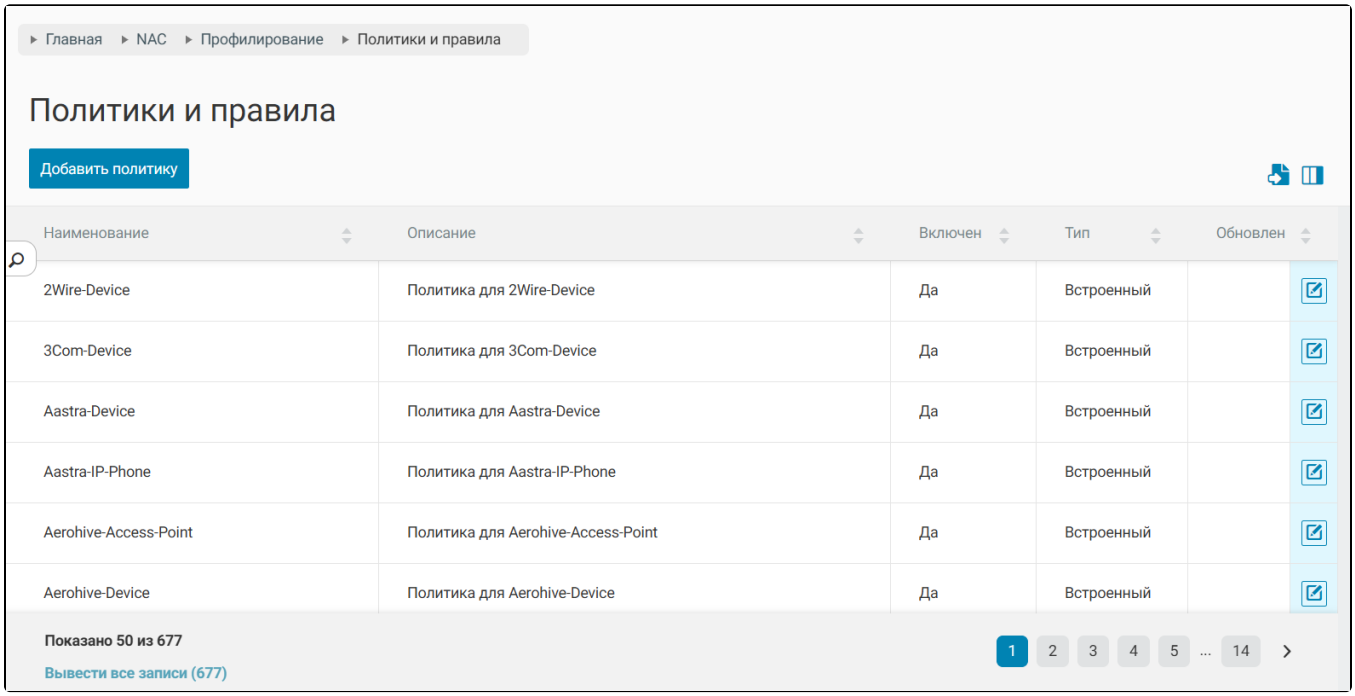


В данном окне по заданному MAC-адресу можно проверить, какому вендору соответствует MAC-адрес и какие из настроенных вами профилей устройств под него попадают.

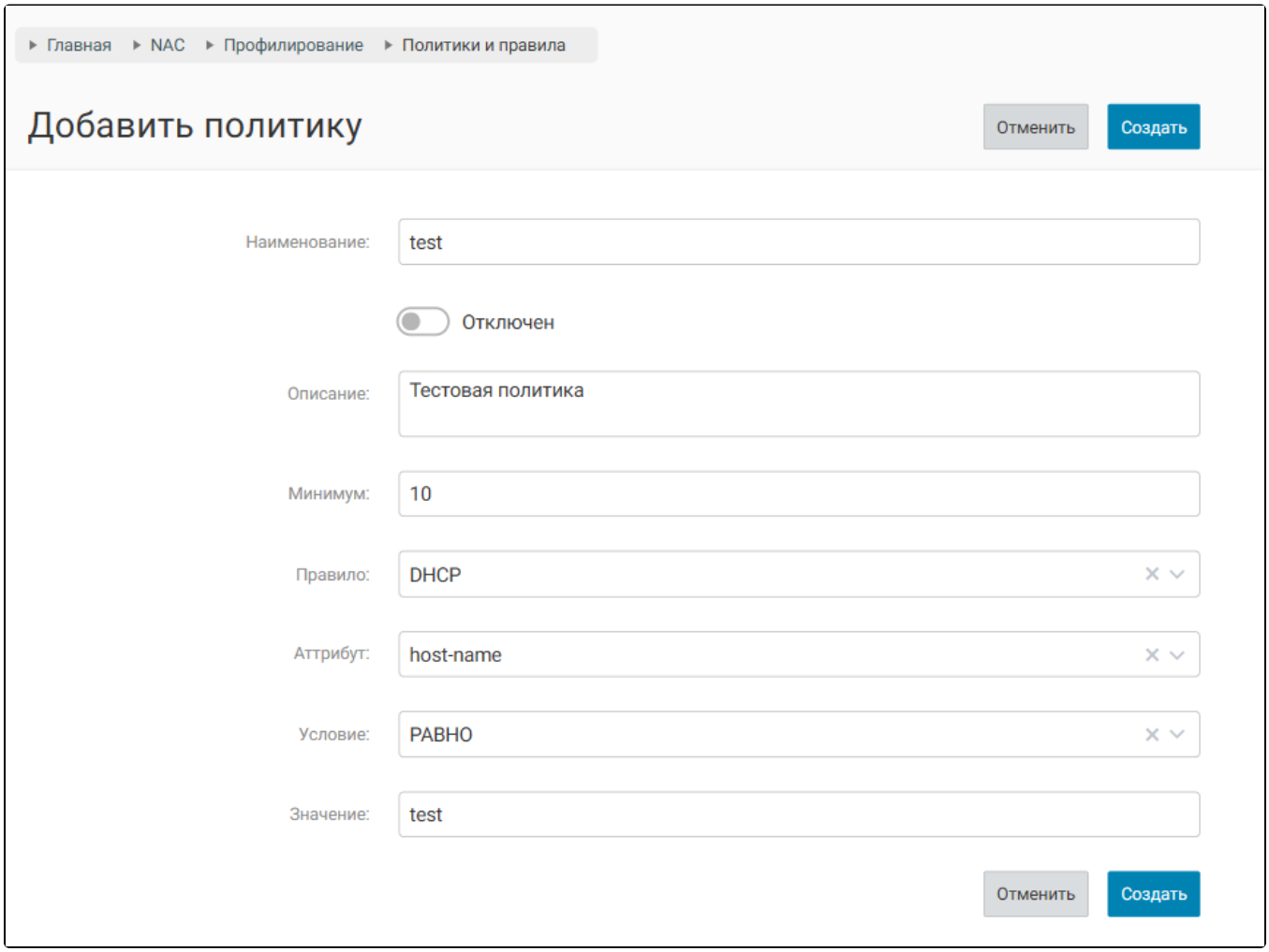
Профилирование

Под профилированием подразумевается формирование профилей на основе логических профилей, политик и правил.

Политики и правила



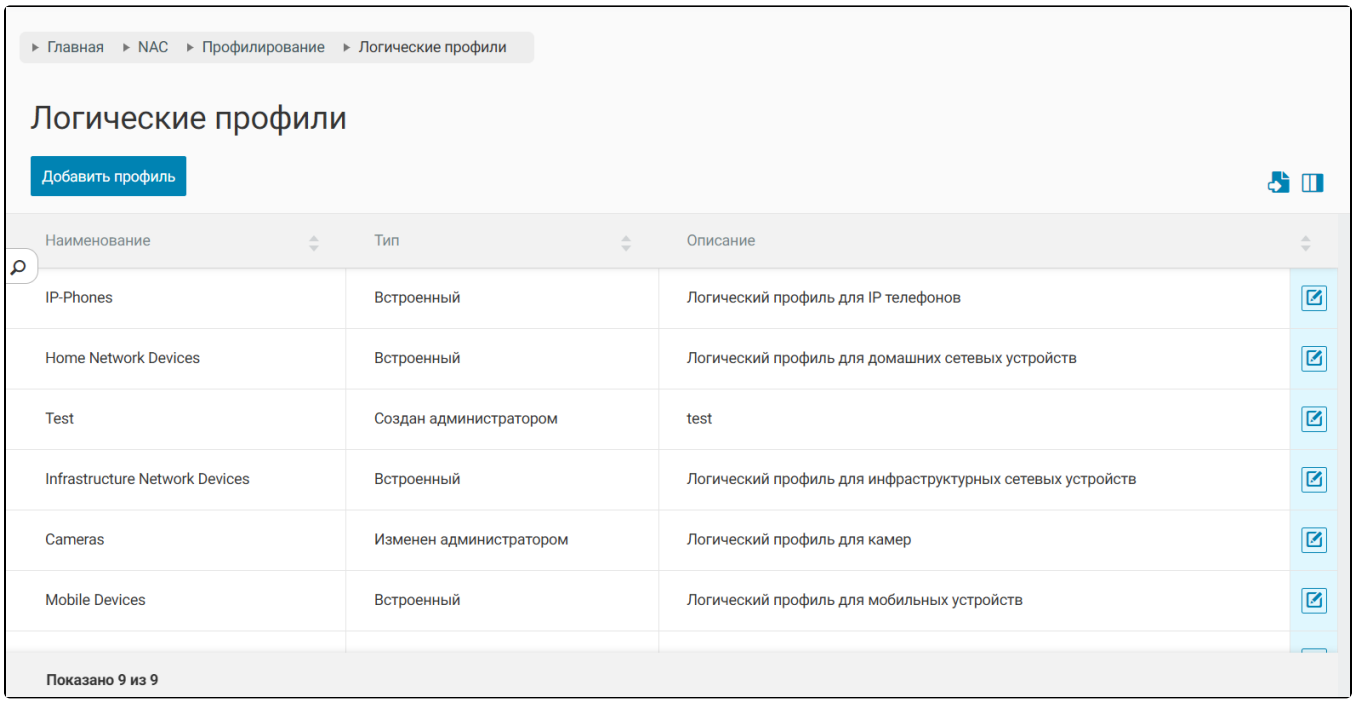
В политику входит определенное количество правил, которые позволяют верно идентифицировать то или иное устройство. При разворачивании системы WNAM 2, будет предустановлено определенное количество политик, в последствии этот список также будет возможно расширить.
Для создания новой политики необходимо выбрать меню "Добавить политику". После, будет выведена форма создания новой формы:



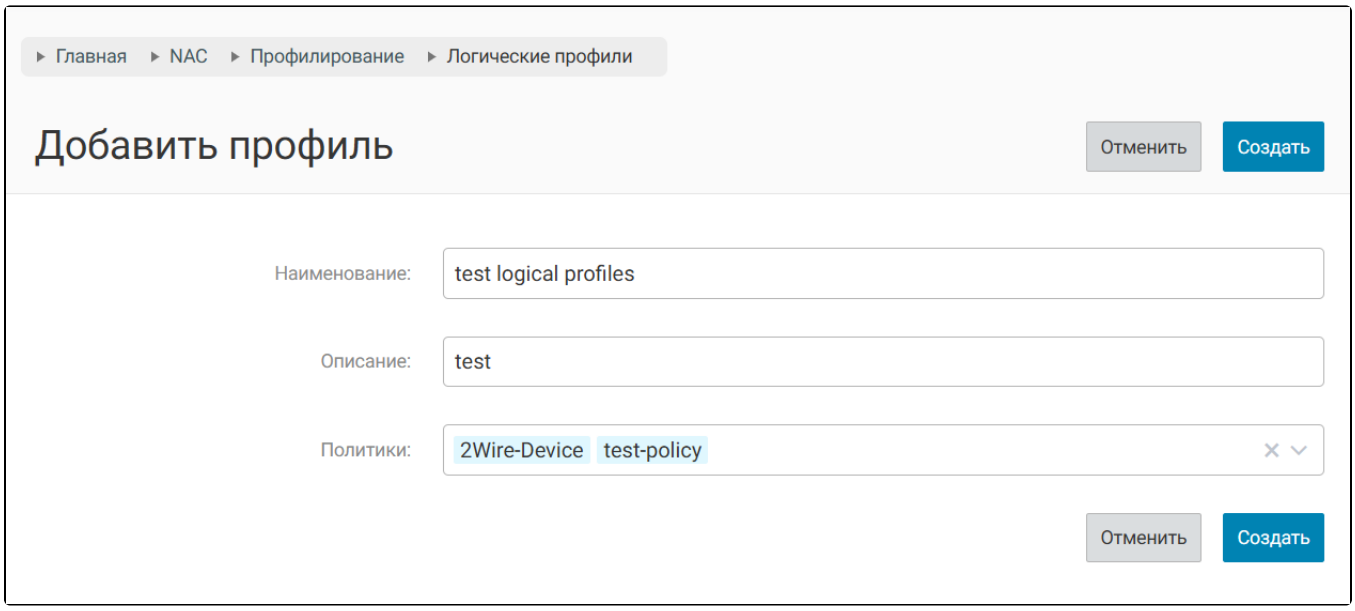
Стоит обратить внимание, важно выбрать верно выбрать применяемую категорию правила для политик. К категориям правил можно отнести DHCP, MAC, SNMP, IP, NETFLOW, CDP, LLDP, NMAP, ACIDEX, ACTIVEDIRECTORY_PROBE.

Логические профили

Логические профили ориентируются от применяемых политик, как в примере выше.



Чтобы создать логический профиль необходимо нажать "Добавить профиль". Далее будет открыта форма, в которой можно выбрать применяемые политики для использования.

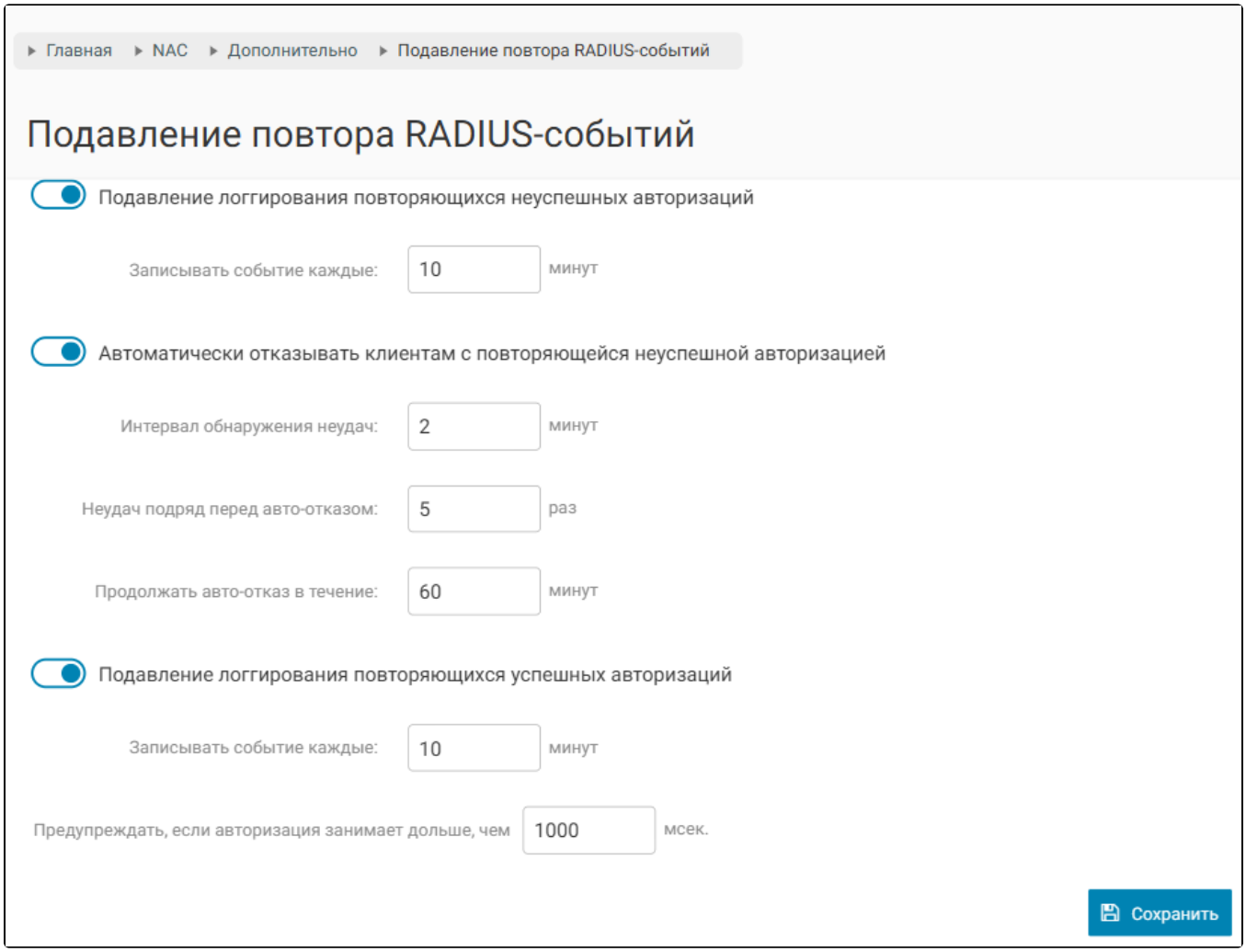


Также, возможно добавлять несколько политик.

Дополнительно

В данном разделе описываются дополнительные настройки к контролю сетевого доступа.

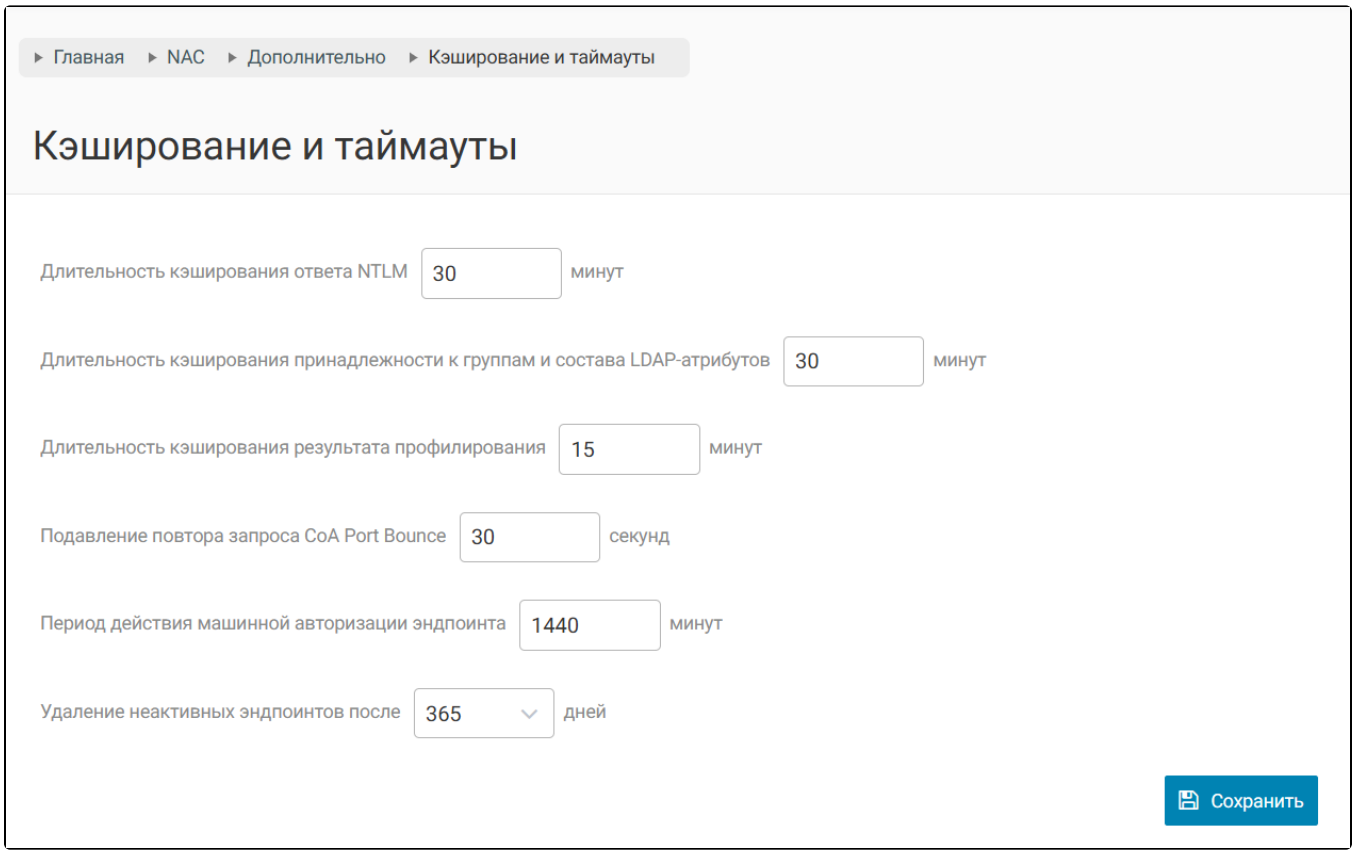
Подавление повтора RADIUS-событий



- **Подавление логгирования повторяющихся неуспешных авторизаций.** Опция будет полезна в случаях, когда необходимо содержать журналы аудита или логов в лаконичном представлении для последующего удобного анализа событий. Имеется возможность записывать событие с определенным интервалом.
- **Автоматически отказываться клиентам с повторяющейся неуспешной авторизацией.** Позволяет предотвратить нагрузку на RADIUS сервер. Имеются дополнительные настройки для интервала обнаружения неудач, количества неудачных попыток, период блокирования.
- **Подавление логгирования повторяющихся успешных авторизаций.** Принцип и логика схожа с первой опцией, но с отличием на успешные авторизации. Присутствует возможность определять интервал записи событий.

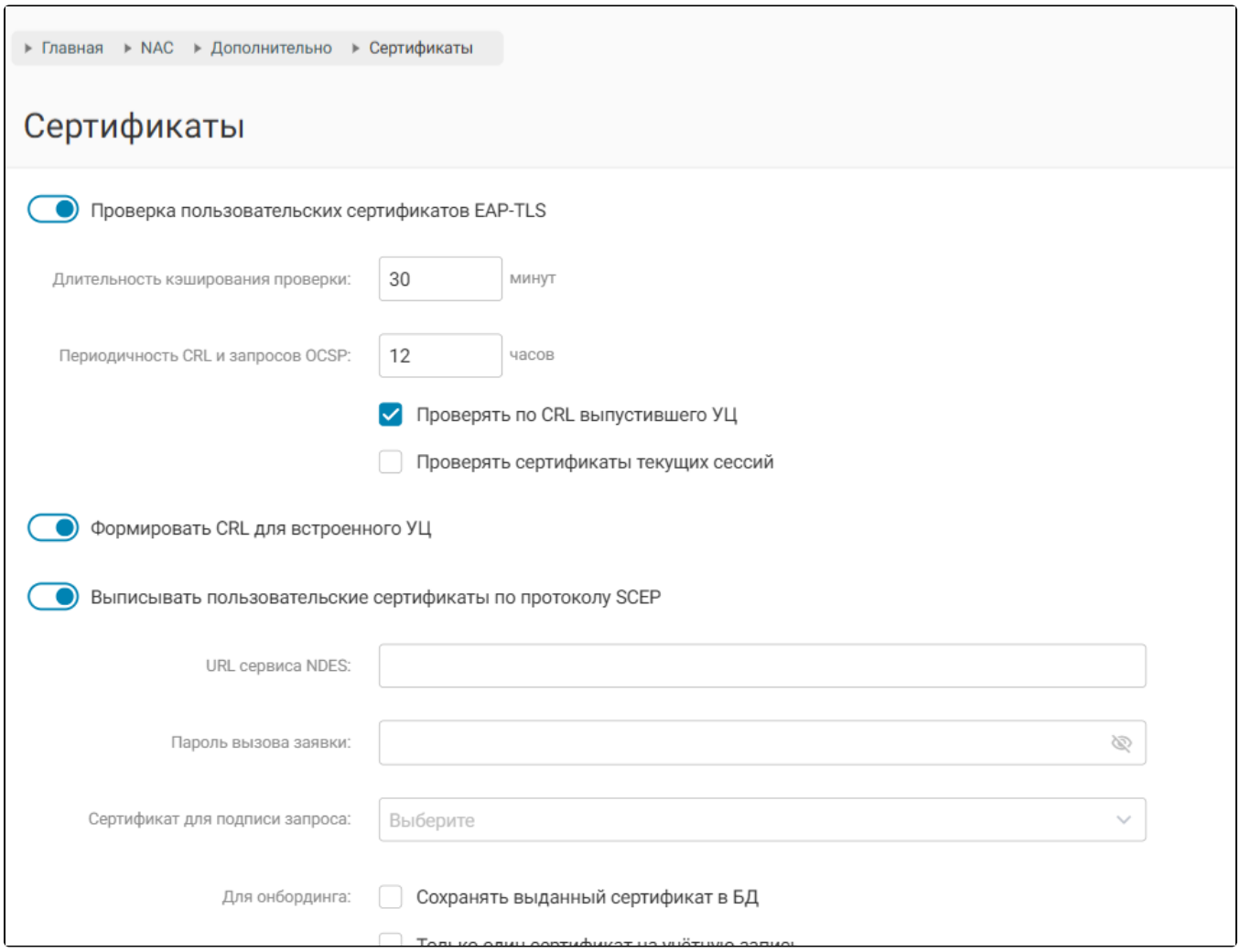
Кэширование и таймауты

Данный подраздел отвечает за определение временных интервалов хранения кэша для различных сетевых подключений.



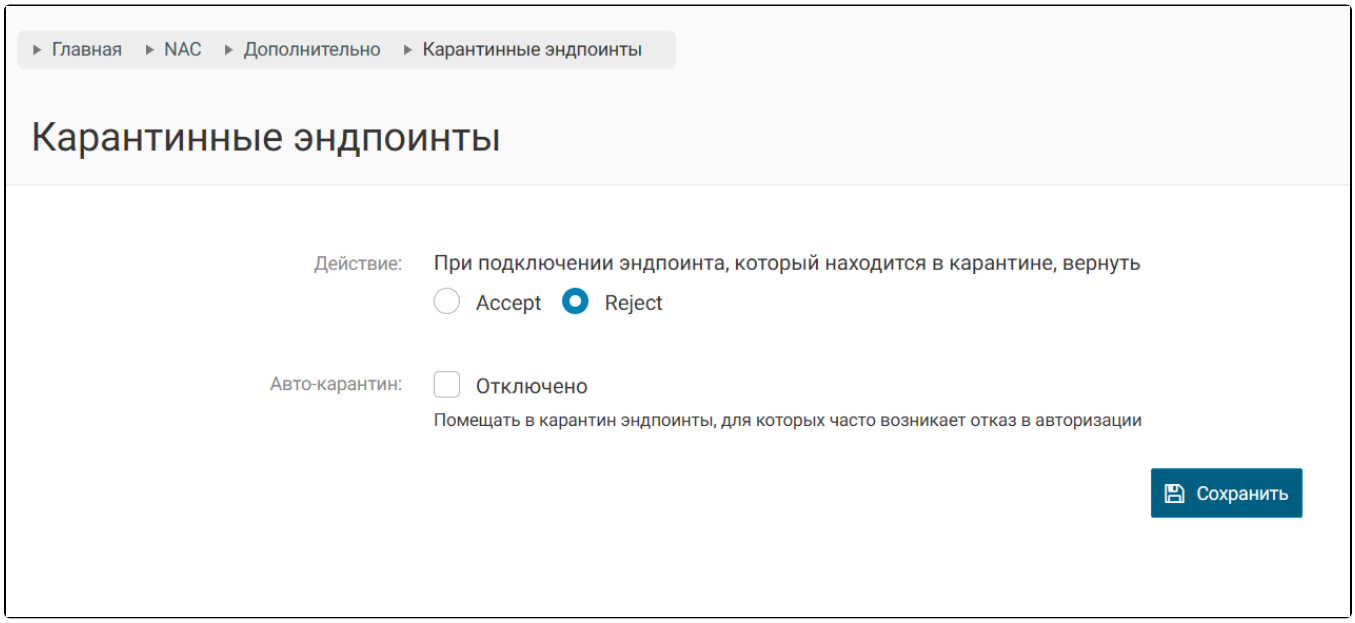
- **Длительность кэширования ответа NTLM.** Позволяет определить время кэширования ответа сетевой аутентификации в минутах.
- **Длительность кэширования принадлежности к группам и состава LDAP-атрибутов.**
- **Длительность кэширования результата профилирования.**
- **Подавление повтора запроса CoA Port Bounce.**
- **Период действия машинной авторизации эндпоинта.**
- **Удаление неактивных эндпоинтов после определенного времени.**

Сертификаты



В подраздел сертификатов можно отнести дополнительный функционал при выдачи сертификатов. Более детальную информацию можно найти в разделе "Сертификаты"

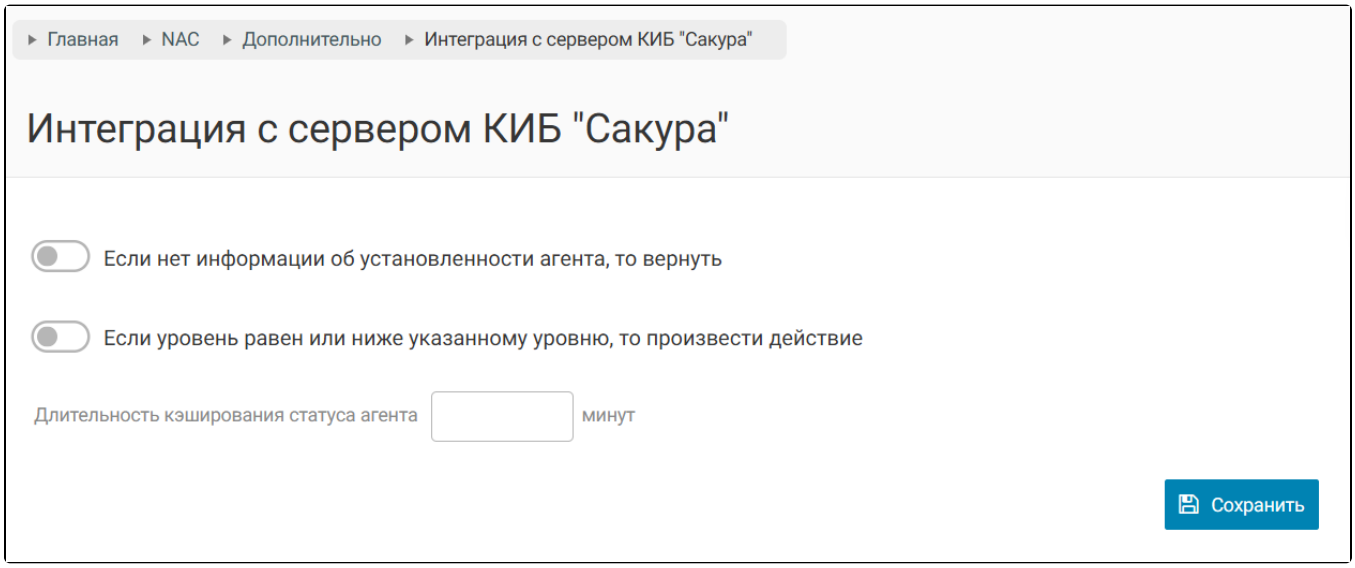
Карантинные эндпоинты



Данный раздел нацелен на разрешение событий, связанных с эндпоинтами, которые были определены в карантин.

Действие – Определяет, разрешить или отклонить подключение эндпоинта. При опции "Accept", необходимо указать, какие RADIUS атрибуты будут переданы эндпоинту.
Авто-карантин – Определяет перемещение подозрительных эндпоинтов для целей безопасности. При включенной опции, необходимо указать интервал обнаружения последовательных отказов и счетчик отказов подряд перед помещением в карантин

Интеграция с сервером КИБ "Сакура"



При включенной опции "Если нет информации об установленности агента, то вернуть" возможно определить разрешение на подключение:

- **Accept** – Разрешить подключение с передаваемыми RADIUS атрибутами.
- **Reject** – Отклонить подключение.
- **Quarantine** – Перевести в карантинное подключение

Внимание! В карантинном подключении, в которое вы переключаете авторизующийся эндпоинт посредством назначения VLAN, ACL либо dACL. у вас **обязательно** должен присутствовать сервер "Сакура".

В противном случае "не соответствующий политике" эндпоинт не сможет "вылечиться", сообщить об этом своему серверу и никогда из карантина не выйдет.

"Если уровень равен или ниже указанному уровню, то произвести действие" определяет комплекс мер, среди которых уровень срабатывания, действие, VLAN, ACL, dACL (загружаемые ACL).

Поддерживаются следующие уровни защищенности, передаваемые сервером КИБ "Сакура":

- Offline - агент был ранее установлен, но АРМ не подключен к серверу;
- Critical - критический;
- Noncritical - не критический/предупреждение;
- Info - информационный;
- Compliant - нет нарушений, соответствует политике информационной безопасности (ИБ).

Помимо этого, возможно определить длительность кэширования статуса агента в минутах.

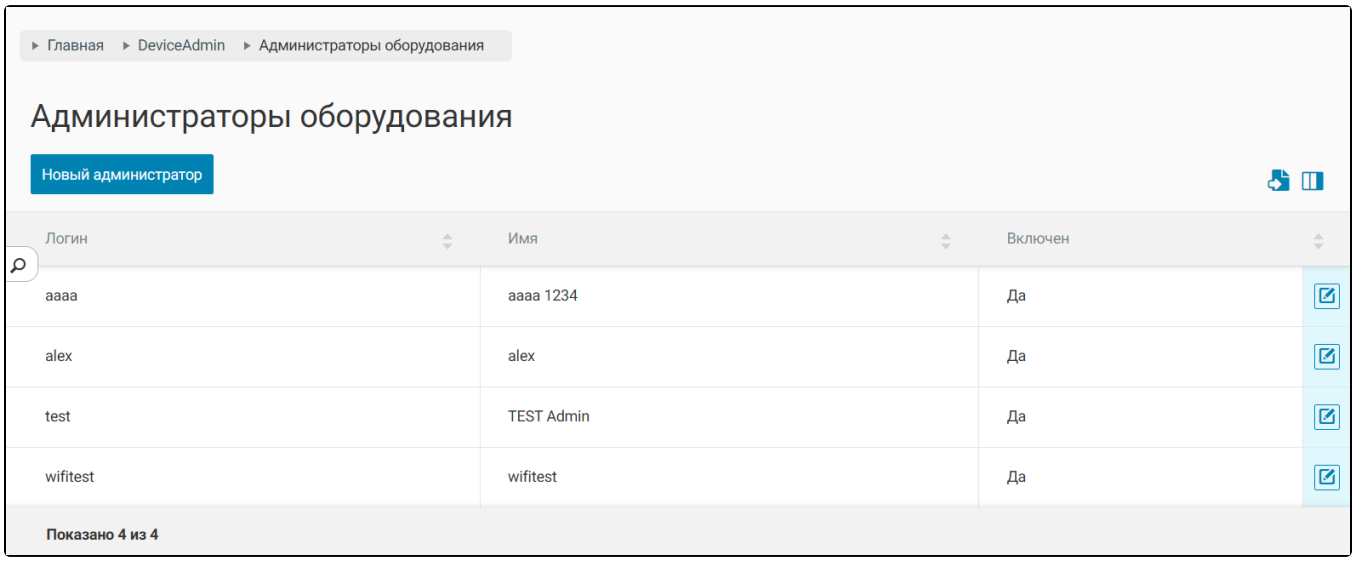
Доступ к оборудованию (DEVICE ADMIN)

Данный раздел содержит детальное описание следующего функционала:

- Администраторы оборудования;
- Группы администраторы оборудования;
- Наборы команд;
- TACACS+ и RADIUS правила;
- Парольная политика.

Администраторы оборудования

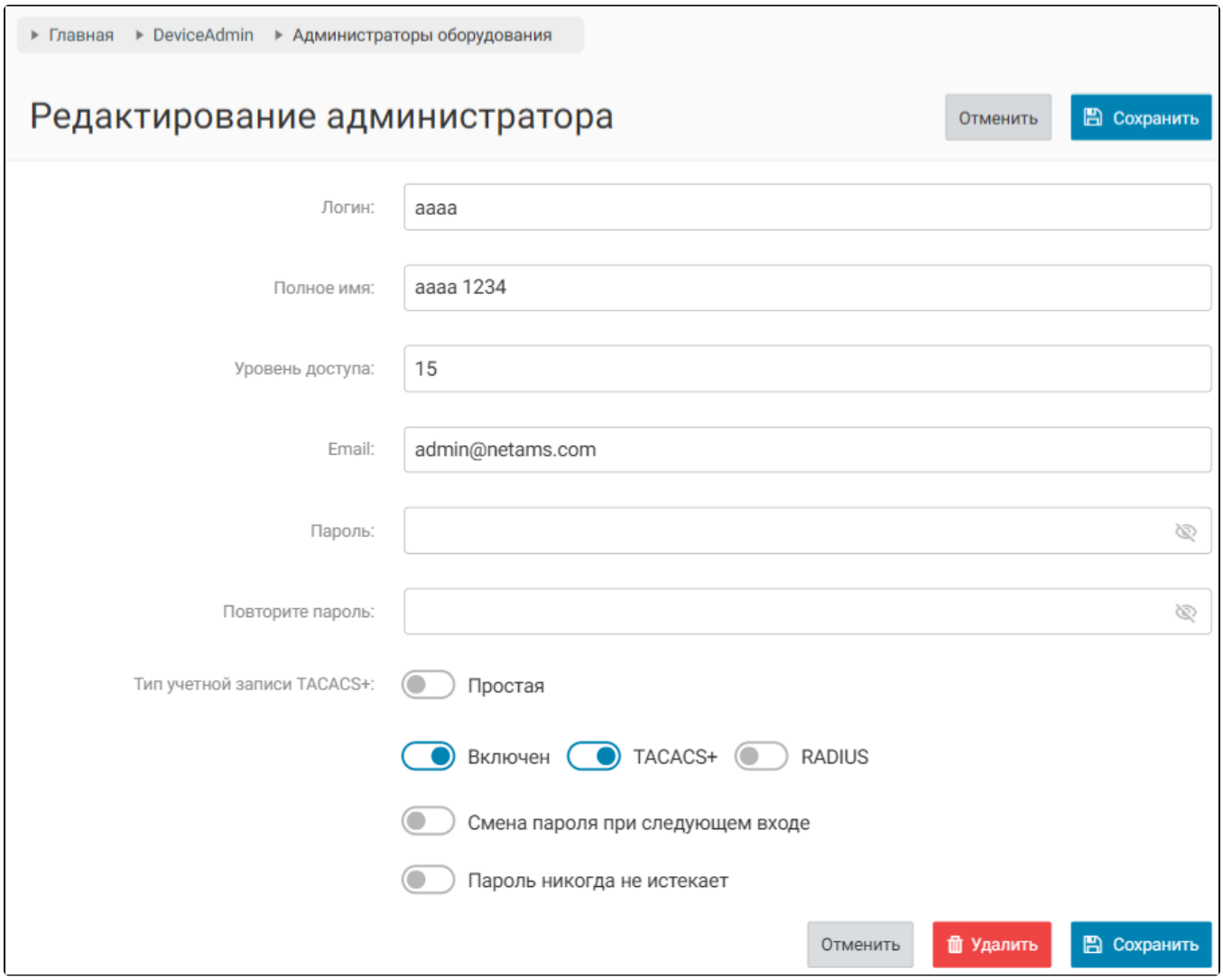
Система WNAM 2 ведет собственную базу пользователей, имеющих доступ к оборудованию. Она не пересекается с базой данных пользователей веб-интерфейса WNAM 2 и конечных пользователей сети (беспроводной или гостевой). В разделе "Главная" "Device admin" "Администраторы оборудования" расположен список всех пользователей.



Из списка пользователей можно перейти к окну редактирования групп и профилей TACACS+ и RADIUS. Сверху таблицы со списком пользователей расположены кнопки выгрузки БД в формате CVS (только видимые четыре столбца) и XLS (вся информация о пользователях).

Учетная запись пользователя определяет его права, а именно:

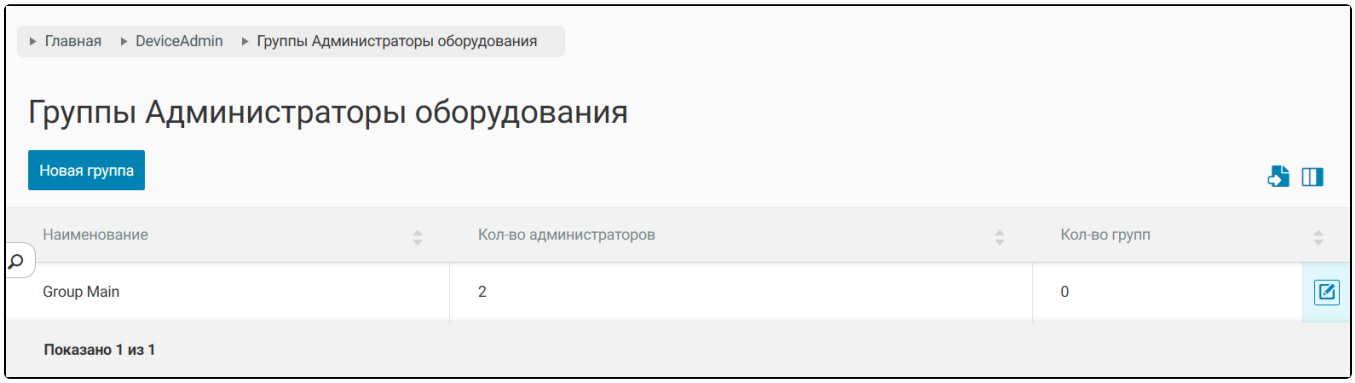
- Логин, имя;
- Уровень доступа (привилегий) в диапазоне от 0 до 15. Если он не задан или равен нулю, конечный уровень привилегий определяется профилем TACACS+, выбранным при аутентификации. Если уровень привилегий пользователя задан, используется заданный;
- Адрес email;
- Пароль и подтверждение пароля
- Признак включенности;
- Тип аутентификации TACACS+ или RADIUS;
- Признак запроса смены пароля при следующем логине;
- Признак истечении пароля через временной период.



Пользователи веб-интерфейса администратора с ролью "Администратор" также являются допустимыми пользователями TACACS+. Для них по умолчанию уровень привилегий равен 15 и разрешены все команды. Система не делает проверку на дубли имен пользователя TACACS+ и общего администрирования.

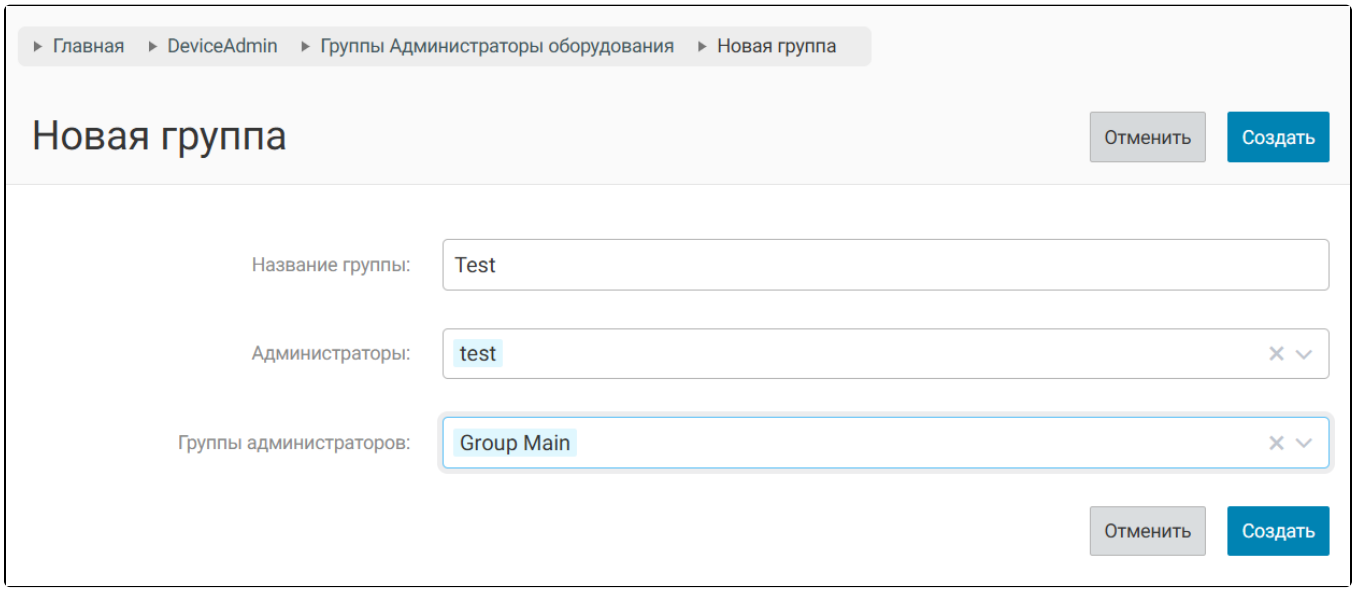
Группы Администраторы оборудования

Пользователей можно объединять в логические группы для удобства управления ими и последующего назначения профилей. В группу может входить любое число подгрупп и любое число пользователей одновременно. Каждый пользователь или группа может быть членом нескольких групп. Система WNAM 2 проводит проверку "зацикленности" групп. В веб-интерфейсе в разделе "Главная" "DeviceAdmin" "Группы Администраторы оборудования" представлен перечень всех групп.



В основном окне раздела возможно создать новые группы, а также расположено поле поиска групп пользователей. При нажатии на кнопку "Новая группа" или при нажатии левой кнопкой мыши на строку таблицы откроется окно редактирования, в котором следует:

- задать имя группы;
- выбрать пользователей из имеющихся;
- выбрать дочерние (вложенные) группы.



После выполненных настроек при создании группы необходимо нажать кнопку "Сохранить". Созданные группы пользователей используются в настройке правил TACACS+ и правил RADIUS.

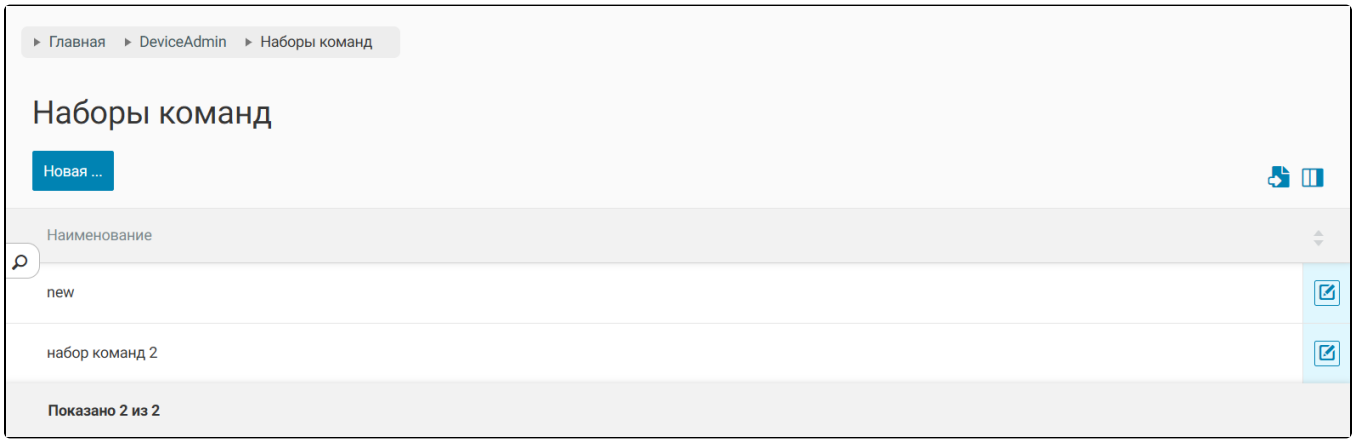
Наборы команд

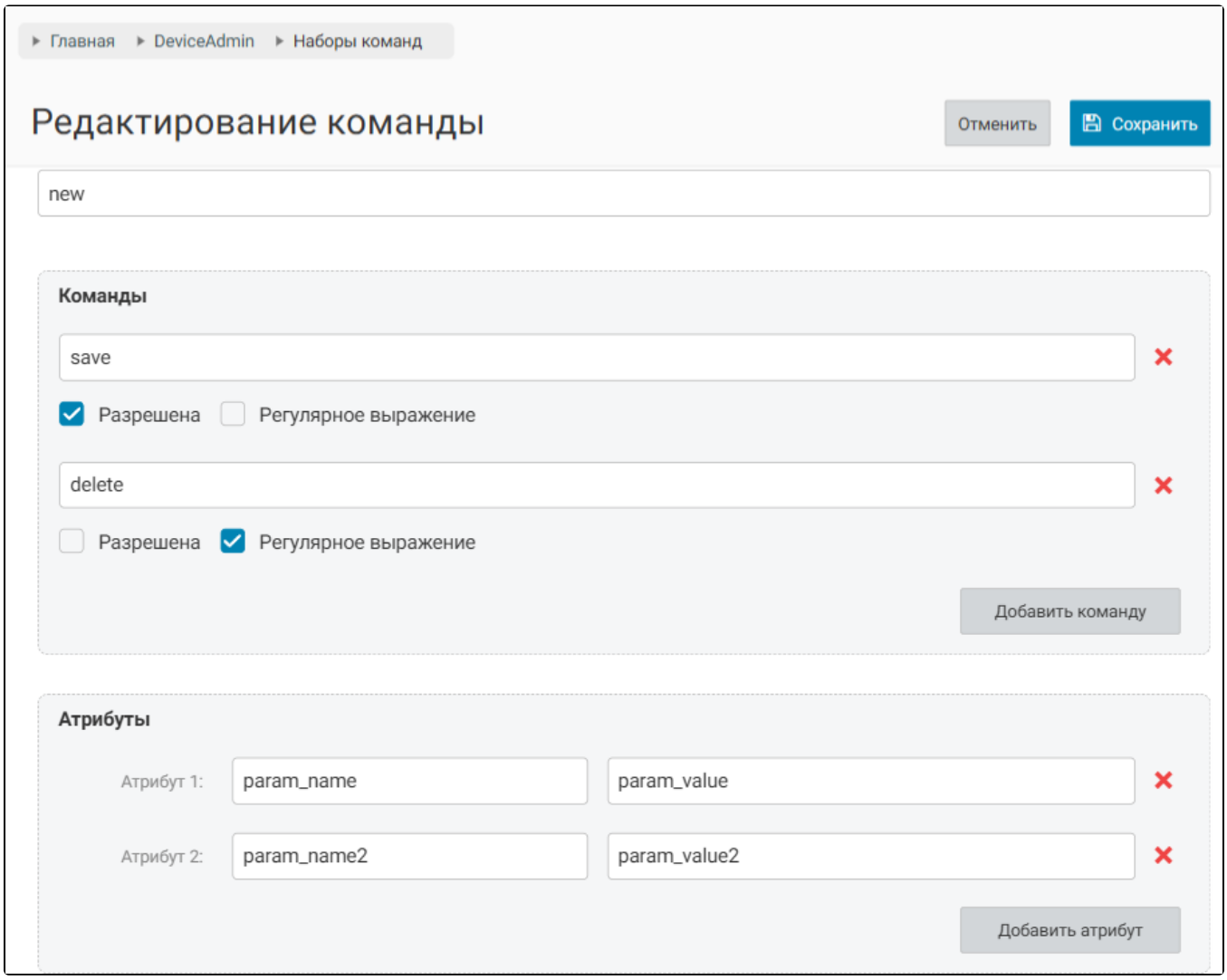
Для возможности использования общих наборов разрешенных/запрещенных команд и атрибутов в нескольких правилах WNAM 2 имеет возможность создавать наборы команд.

Они представляют собой логические объединения последовательности команд под заданным именем.

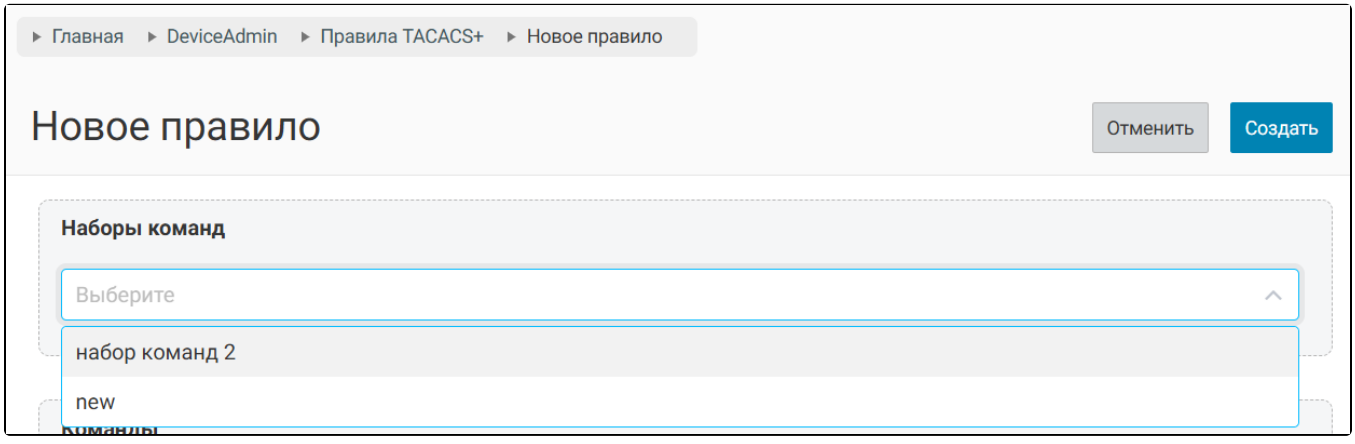
В дальнейшем, при настройке правил подключения TACACS+ и RADIUS вы можете применять как индивидуальные команды, так и ссылаться на один или несколько наборов команд.

Число создаваемых наборов команд, число элементов в наборе, не ограничивается.





Созданные наборы команд применяются в правилах TACACS+ и RADIUS:



При этом отмеченные (выбранные) наборы команд можно перемещать друг относительно друга.

При срабатывании профиля автоматически формируется список разрешенных/запрещенных команд и атрибутов, исходя из следующих правил:

Наборы разрешенных команд и наборы разрешенных атрибутов - два упорядоченных списка, действительных на время сессии TACACS+ и RADIUS подключения.

В каждый из списков попадают настройки, последовательно,

- из наборов команд (упорядоченно), настроенных в правилах подключения
- из самого профиля
- для этого пользователя

Если в список добавляется какая-либо команда, которая добуквенно уже присутствует в этом списке, она замещает собой предыдущее совпадение. Проверка идет по имени команды, без учёта регистра.

Результирующий список временно сохраняется (для сессии). В процессе авторизации набранной пользователем команды он просматривается "сверху вниз" до первого совпадения (с учетом поиска по регулярному выражению, т.е. подстроке). Первая совпавшая запись будет являться результатом авторизации (в зависимости от настройки - успешной либо нет).

Таким образом, вы можете определить один или несколько наборов команд, и "скорректировать" формируемые или правила в параметрах профиля авторизации или подключающегося (локального) пользователя. Например, допустим, что в наборе команд "КомандыДляАдминов" заданы два правила:

> *configure * - регулярное выражение - разрешено*
>
> *copy running-config startup-config - разрешено*

И в параметрах пользователя test_user задано:

> *copy running-config startup-config - запрещено*
>
> *show * - регулярное выражение - разрешено*

Результирующий набор объединяет первый блок команд со вторым, что в итоге даёт такой набор команд:

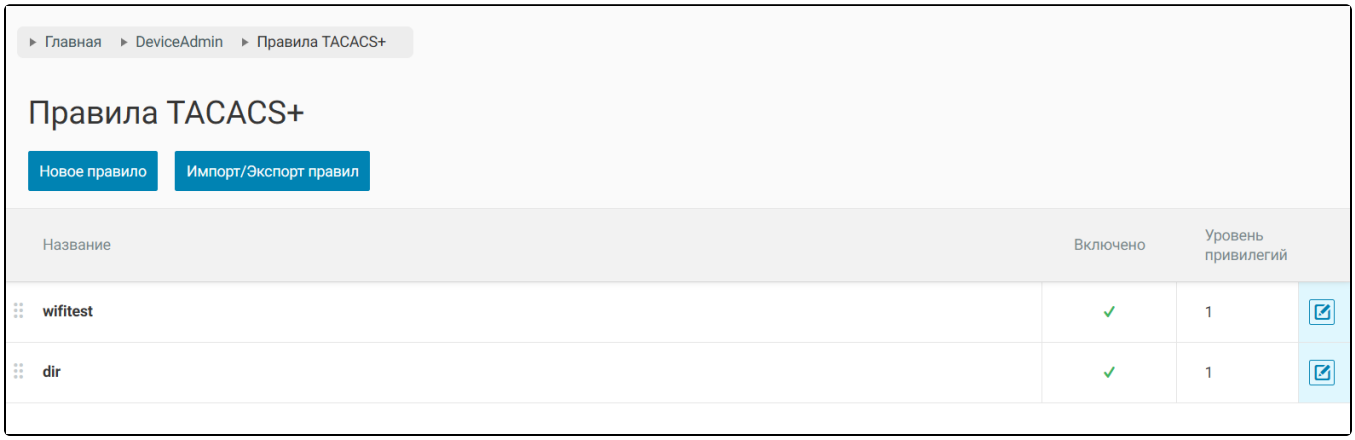
> *configure * - регулярное выражение - разрешено*
>
> *copy running-config startup-config - запрещено*
>
> *show * - регулярное выражение - разрешено*

TACACS+ и RADIUS Правила

При поступлении запроса от сервера доступа (NAS) по протоколу TACACS+ и RADIUS сервер WNAM 2 производит перебор всех настроенных и включенных TACACS+ и RADIUS правил для определения:

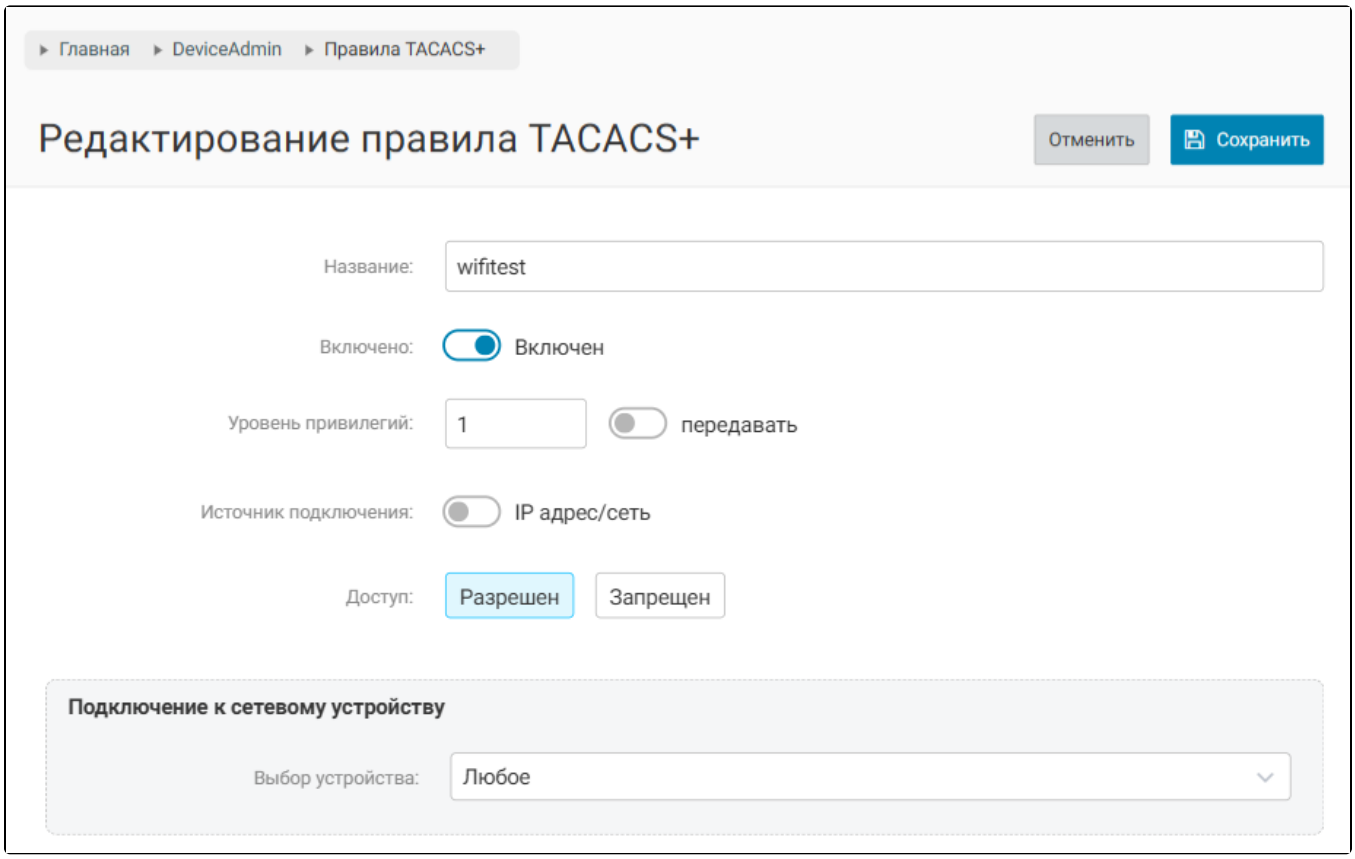
- пользователя, который запрашивает доступ;
- уровня привилегий, допустимых команд и атрибутов, которые необходимо применять к каждой сессии подключения.

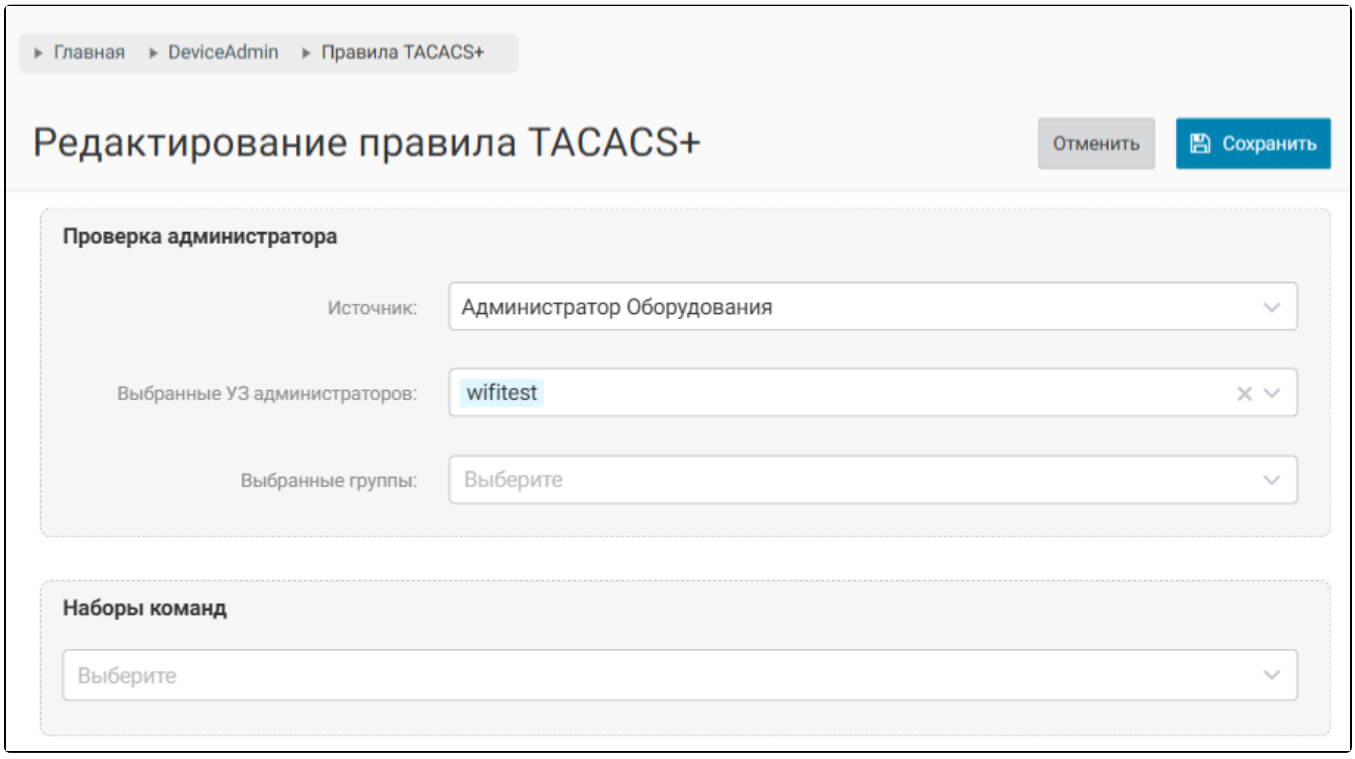
Профили определяются в разделе "Главная" "Device admin" "Правила TACACS+" (или "Правила RADIUS", в зависимости от необходимости). При старте система проверяет наличие правил в системе.

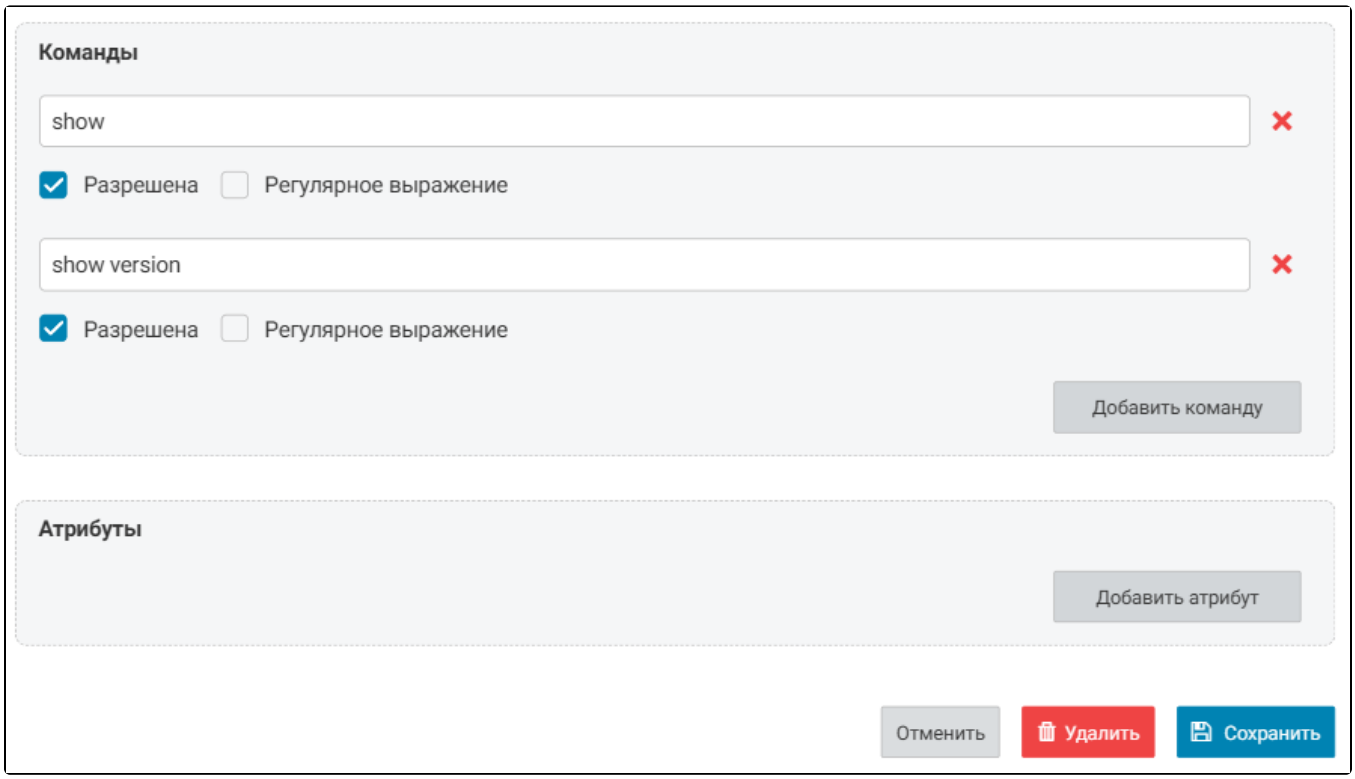


В интерфейсе раздела "Правила TACACS+" и "Правил RADIUS" расположен ряд кнопок, позволяющих создать новый профиль, а также расположено поле для поиска правил. У каждого правила есть свое положение в списке. При анализе подключения (место подключения, логин) система WNAM 2 перебирает все номера, отметая заведомо не совпадающие. В конечном итоге остается один совпавший профиль (при прочих равных параметрах остается тот, у кого меньше номер). Если ни один из профилей не подошел, доступ запрещается.

Для того, чтобы отредактировать существующий профиль необходимо нажать левой кнопкой мыши на соответствующую запись в таблице профилей и изменить настройки в открывшемся окне. Для создания или редактирования правила необходимо нажать кнопку "Новое правило" или выбрать кнопку редактирования правила в контекстном меню. При этом будет открыто окно, в котором необходимо задать, либо изменить требуемые параметры.


Главная
DeviceAdmin
Правила TACACS+
Редактирование правила TACACS+
Отменить
Сохранить
Название:
wifitest
Включено:
Включен
Уровень привилегий:
1
передавать
Источник подключения:
IP адрес/сеть
Доступ:
Разрешен
Запрещен
Подключение к сетевому устройству
Выбор устройства:
Любое


Главная
DeviceAdmin
Правила TACACS+
Редактирование правила TACACS+
Отменить
Сохранить
Проверка администратора
Источник:
Администратор Оборудования
Выбранные УЗ администраторов:
wifitest
Выбранные группы:
Выберите
Наборы команд
Выберите



Каждый из профилей имеет следующие настройки:

- наименования правила;
- признак включенности;
- приоритет (порядковый номер в таблице);
- уровень привилегий пользователя, который передается оборудованию (NAS);
- чекбокс "не передавать" означает, что при старте сессии в сторону оборудования не будет передан атрибут типа "shell: priv-lvl=...", что может быть важно для настройки работы с, например, Cisco WLC;
- источник подключения - фильтр на источник подключения (IP-адрес подключающегося клиента - администратора);
- Подключение к сетевому устройству - фильтр на цель подключения (к какому серверу доступа обращается администратор: к любому, заданному, находящемуся в иерархической группе подразделения);
- правило совпадения обращающейся учетной записи (логина):
  - администратор веб-интерфейса WNAM 2 с опциональной проверкой совпадения подстроки в логине;
  - локальный пользователь TACACS+ с фильтром по списку пользователей или групп (мульти-выбор);
  - доменный пользователь (при настроенной интеграции с Active Directory) с проверкой пароля и членства в группе (выбор, подстрока) по LDAP;
- список допустимых команд;
- список передаваемых атрибутов.

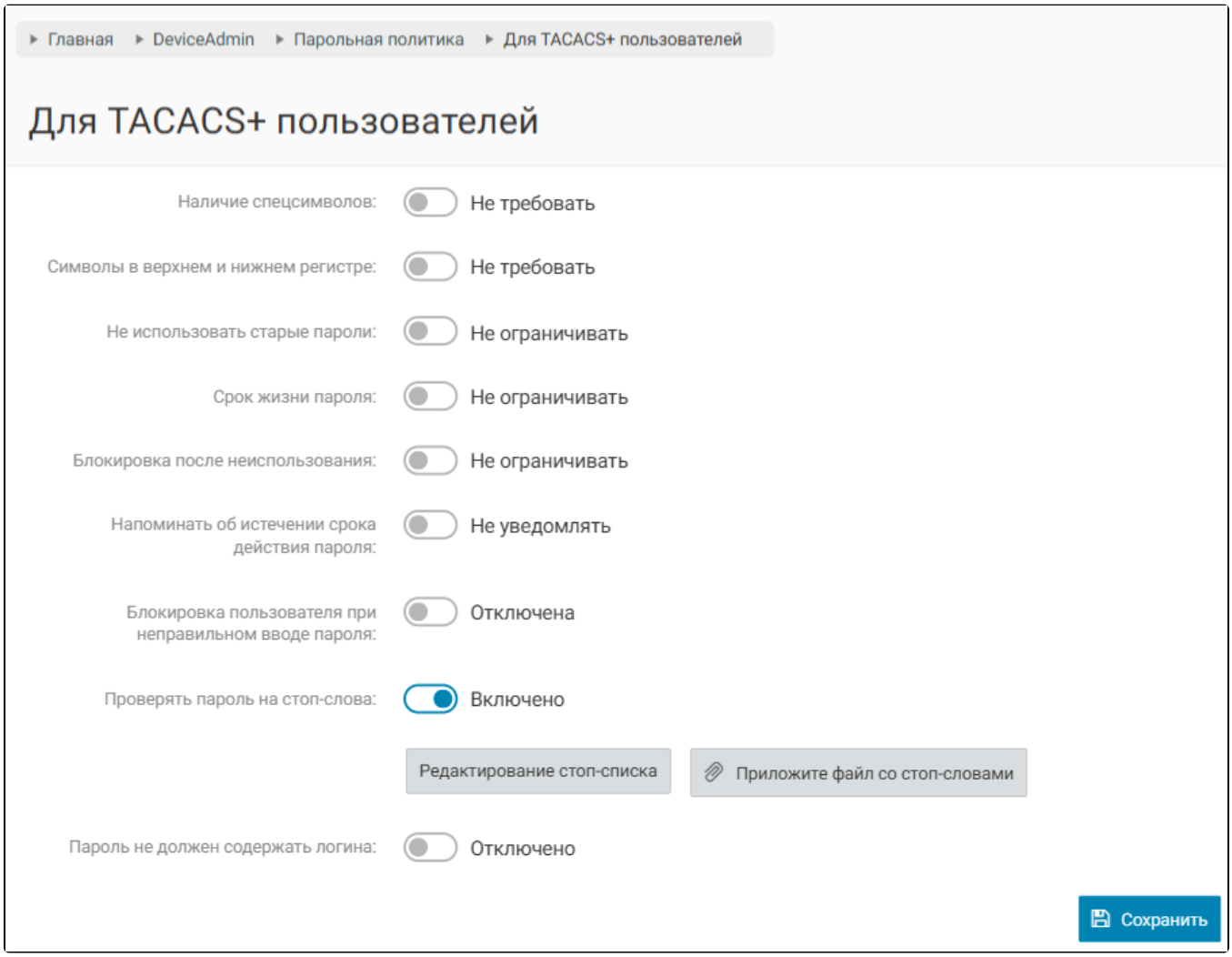
Список допустимых команд и список передаваемых атрибутов объединяются с аналогичными списками совпавшего локального пользователя TACACS+ (у других типов учетных записей эти списки отсутствуют).

Парольная политика

Парольная политика позволяет настроить систему безопасности авторизации подключений для TACACS+ подключений.

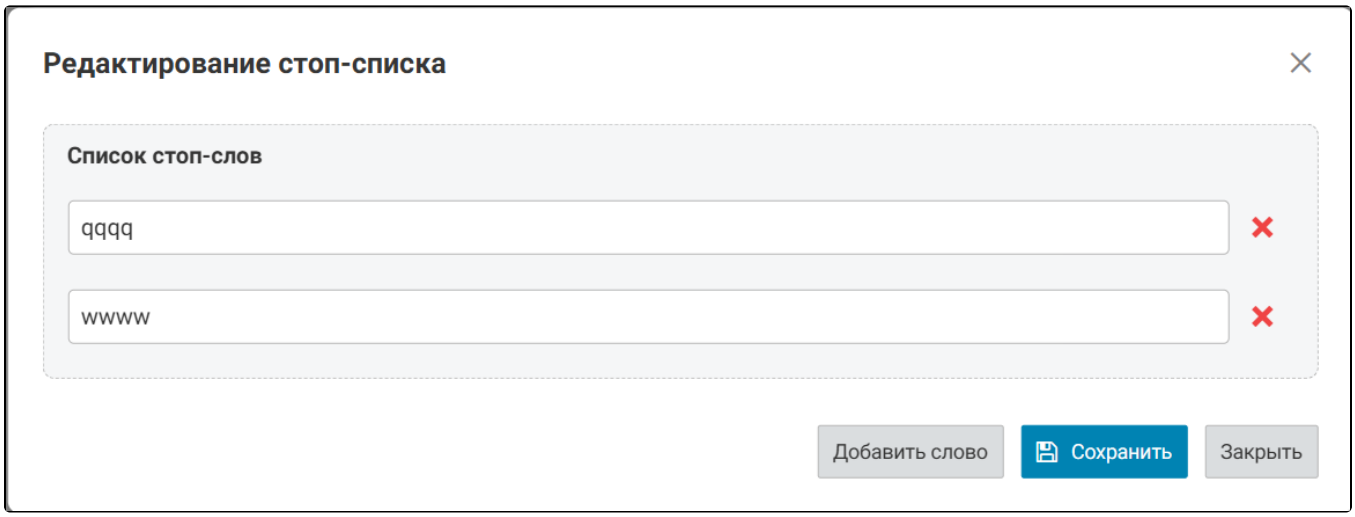
Данный раздел можно найти по пути "Главная" – "DEVICEADMIN" – "Парольная политика". Также присутствует разграничение для TACACS+ пользователей и для технических TACACS+ учетных записей.

> ⚠ Стоит обратить внимание на разделение парольных политик. При редактировании парольных политик необходимо явно определять, для каких учетных записей стоит применять различные атрибуты парольной политики.



Парольную политику можно настроить, отредактировав следующие атрибуты:

- Настроить минимальную длину пароля;
- Включить/отключить двухфакторную авторизацию;
- Требовать в пароле цифры;
- Требовать в пароле спецсимволы;
- Требовать символы в верхнем и нижнем регистре в пароле;
- Ограничение по использованию старых паролей;
- Срок жизни пароля;
- Ограничение по блокировке пароля после использования;
- Настройка уведомлений о смене пароля;
- Блокировка пользователя после ввода неправильного пароля;
- Фильтр паролей на стоп-слова. В данной настройке возможно импортировать список стоп-слов из файла, либо редактирование списка напрямую;



- Фильтр на содержание логина в пароле;

Объекты

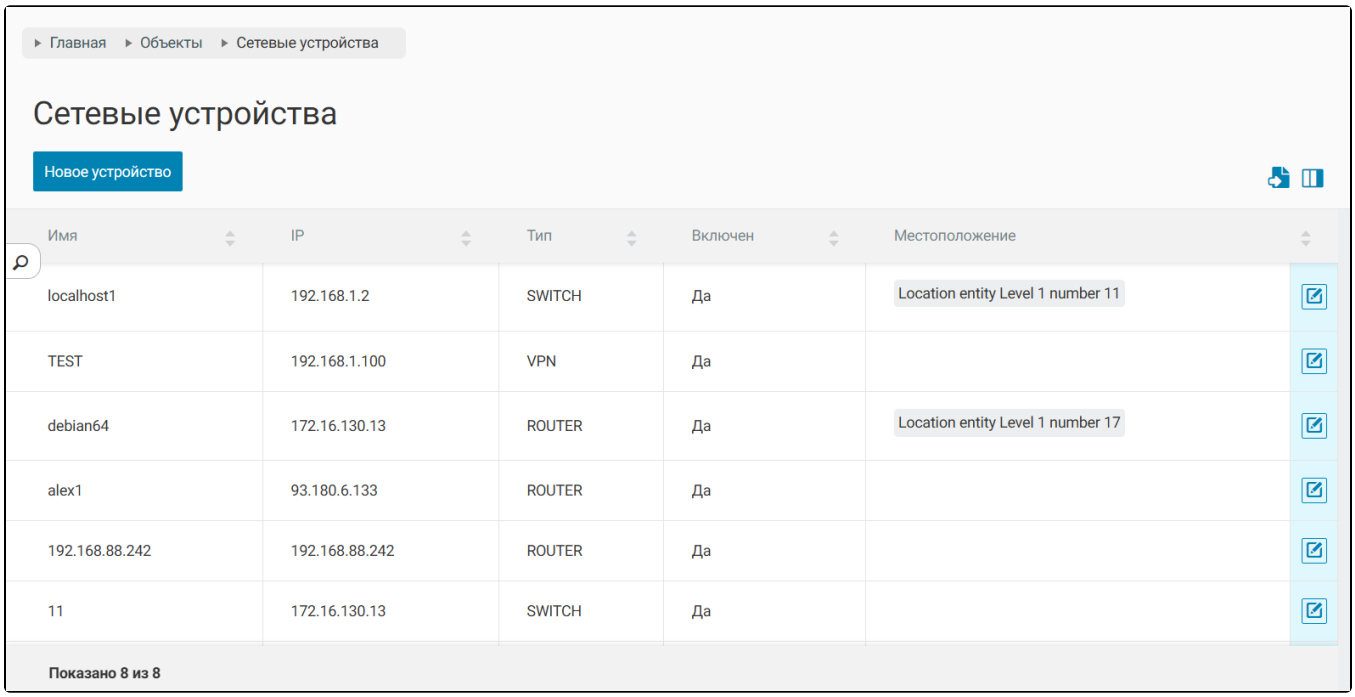
Данный раздел содержит детальное описание следующего функционала:

- Сетевые устройства;
- Местоположение;
- Категории;
- Службы каталога;
- Учетные записи;
- RADIUS-атрибуты;
- Двухфакторная авторизация;
- Уведомления;
- Дополнительные настройки.

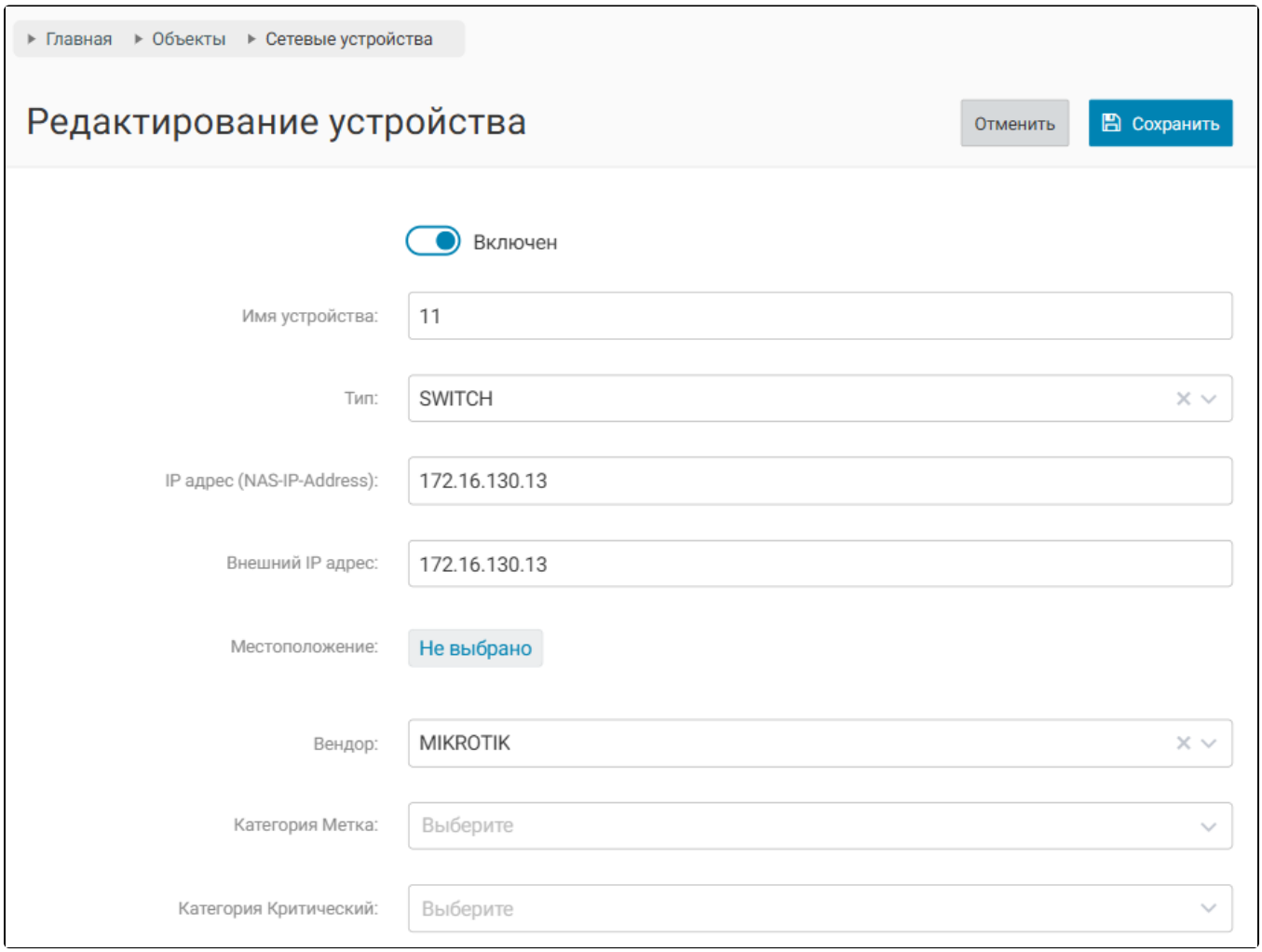
Сетевые устройства

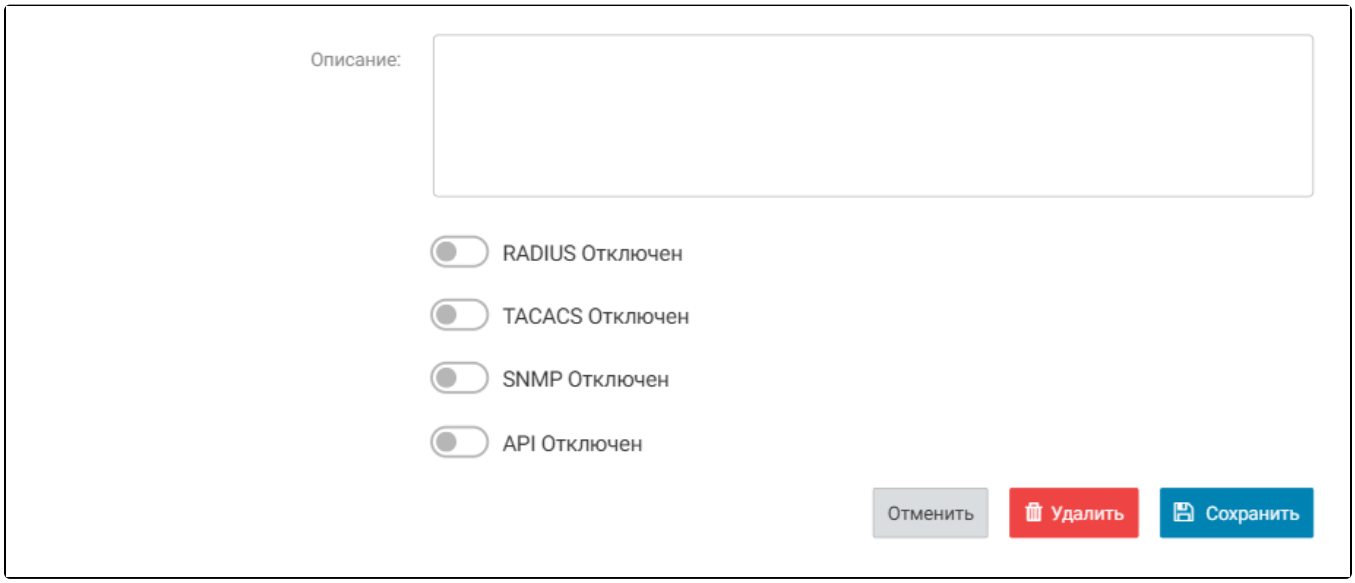
Данный пункт меню позволяет создавать, просматривать и редактировать записи об объектах типа "Сетевое устройство". Сетевым устройством в терминологии WNAM 2 является маршрутизатор или беспроводный контроллер, посредством которого обеспечивается предоставление услуги доступа в Интернет пользователю беспроводной сети. Если маршрутизатором является устройство Mikrotik или сервер Linux, то беспроводное соединение (Wi-Fi) может обеспечить радио-оборудование любого производителя. При использовании профессиональных Wi-Fi систем на основе управляемых контроллером точек доступа (Bluesocket, Ruckus, Cisco) сетевым устройством является контроллер. В качестве сетевого устройства настраивается так называемый портал перехвата (хотспот), встроенный в маршрутизатор или беспроводный контроллер. В маршрутизаторе или контроллере может быть одновременно настроено несколько хотспотов, каждый со своими настройками (параметрами Wi-Fi сети и т.п.).

Окно раздела "Объекты" "Сетевые устройства" позволяет просматривать список созданных в системе сетевых устройств и их основные параметры.



При нажатии левой кнопкой мыши на контекстное меню редактирования в строке таблицы открывается окно редактирования параметров сетевого устройства (аналогично окну создания записи о новом сетевом устройстве).





В поле **ip-адрес (NAS-IP-Address)** может быть указан в виде одного конкретного ipv4 адреса или в виде группы адресов, в том числе с помощью маски в нотации CIDR. Например, у кластерного сервера есть 2 узла. Чтобы задать адреса обоих узлов, например, 195.151.49.10, 195.151.49.11 можно использовать следующее значение в CIDR нотации: 195.151.49.10/31
Также допускается указание нескольких отдельных адресов через точку с запятой: 195.151.49.10; 195.151.49.11

В качестве параметров указывается тип сетевого устройства - один из вариантов поддерживаемых WNAM 2 устройств. Несмотря на то, что механизмы работы поддерживаемых устройств значительно различаются с точки зрения администратора и пользователя, система WNAM 2 работа с ними одинакова.

Типы сетевого устройства:

- SWITCH;
- ROUTER;
- WIRELESSCONTROLLER;
- VPN;
- FIREWALL.

Поддерживаются сетевые устройства (Вендоры), представленные в таблице.

Сетевое устройство	Описание сетевого устройства
Fplus	Программный контроллер беспроводных точек доступа Fplus.
Mikrotik	Маршрутизатор производства Mikrotik, может быть как виртуальной машиной на компьютере, так и стационарным устройством (проводной маршрутизатор типа RB2011 либо совмещенный с точкой доступа WiFi RB951Ui-2HnD).
Cisco WLC	Беспроводный контроллер Cisco WLC, может быть как виртуальной машиной (vWLC), так и аппаратным устройством CT2504/5508.
UniFi	Программный контроллер беспроводных точек UniFi.
Bluesocket vWLC	Беспроводный контроллер Bluesocket (бывший Adtran).
Ruckus ZoneDirector	Беспроводный контроллер Ruckus ZoneDirector.
Linux router	Маршрутизатор Linux, выполняющий роль портала перехвата и DHCP-сервера. Поддерживается только в случае его совмещения с сервером WNAM 2.
Zyxel NXC	Беспроводный контроллер Zyxel NXC 2500 и 5500.
Cisco ISG	Маршрутизаторы Cisco с функцией Intelligent Services Gateway, на платформах 7200, 7300, 10000, ASR.
pfSense	Маршрутизаторы на основе прошивки pfSense.
Aruba	Беспроводный контроллер Aruba.
Alcatel-Lucent SR	Маршрутизаторы Alcatel-Lucent серии SR.
HP MSM	Беспроводный контроллер HP MSM.
TP-LINK EAP /CAP	Программный контроллер беспроводных точек TP-LINK EAP.
OpenWRT/DD-WRT и Coova Chilli	Точки доступа на основе открытой ОС OpenWrt и с хотспотом CoovaChilli.
Cambium Networks	Беспроводный контроллер Cambium cnMaestro.
Huawei AC	Беспроводный контроллер и точки доступа Huawei AC и AirEngine.
H3C/HPE	Беспроводный контроллер H3C и HPE (старые модели).
Eltex	Точки доступа Eltex, настраиваемые автономно либо через SoftWlc.
Rotek	Точки доступа Rotek.
Zyxel Keenetic	Точки доступа Keenetic (используют хотспот CoovaChilli).

Motorola /Zebra WiNG	Беспроводный контроллер Motorola (Zebra) WiNG.
Avaya	Точки доступа Avaya.
DCN	Беспроводный контроллер DCN.
FortiWLC	Беспроводный контроллер FortiWLC.
Fortigate	Шлюз/маршрутизатор доступа Fortigate.
Ruijie Networks	Беспроводный контроллер Ruijie.
Juniper	Шлюз/маршрутизатор доступа Juniper MX.
Meraki	Точки доступа Cisco Meraki.
Mist	Точки доступа Mist.
Rdp.RU	Шлюз/маршрутизатор доступа Rdp.RU.
LAN Switch	Общий тип сервера доступа - коммутатор ЛВС (использует стандартный набор RADIUS-атрибутов).
Qtech	Беспроводный контроллер Qtech (Wimark).
FPK Router	Специализированные маршрутизаторы ФПК (используют хотспот CoovaChilli).

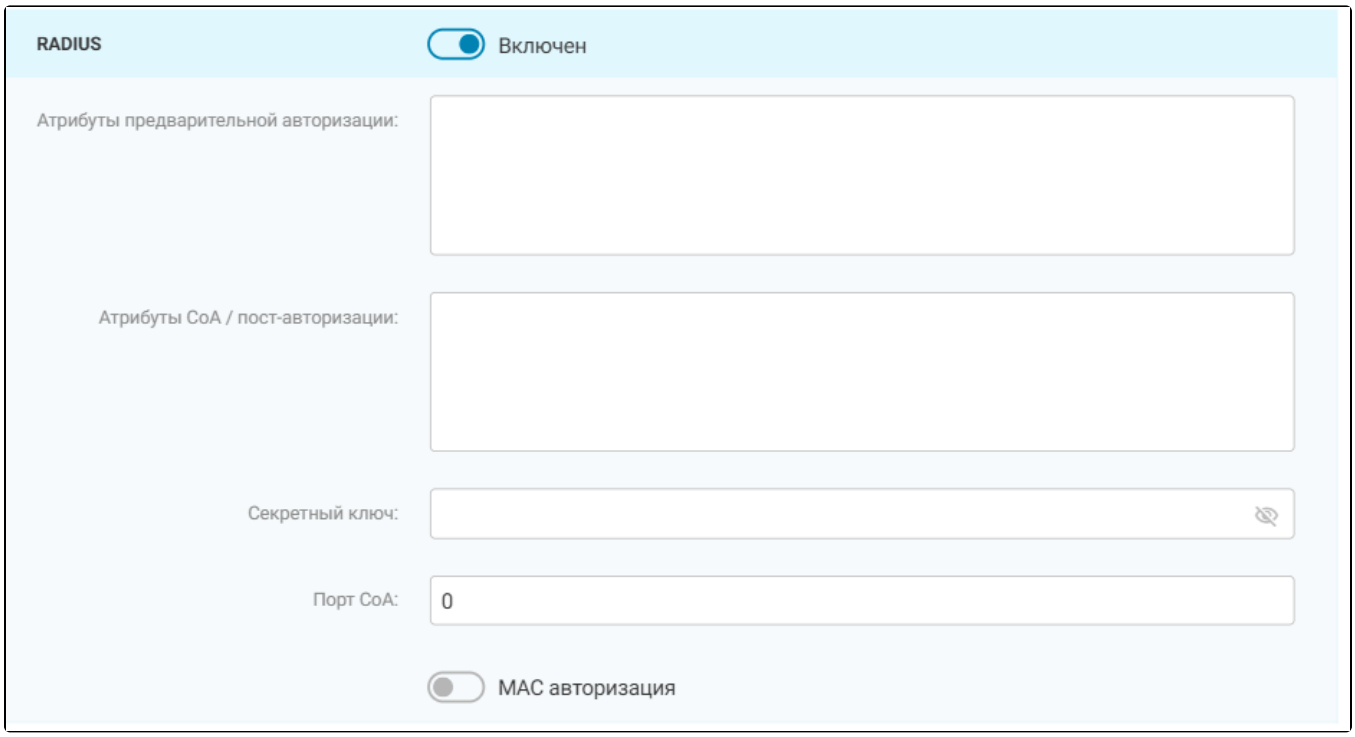
Подробнее о настройке каждого из типов устройств доступа написано в соответствующем разделе.

- IP-адрес устройства доступа, который является обязательным параметром. На основе указанного адреса будет проводиться сопоставление RADIUS-пакетов, получаемых сервером от устройства доступа и их дальнейшая обработка. Необходимо указать здесь адрес, с которого устройство доступа будет отправлять RADIUS-пакеты. Таким образом сервер доступа - это RADIUS-клиент для сервера FreeRADIUS, работающего совместно с системой WNAM 2. Этот адрес ожидается в качестве значения параметра NAS-IP-Address RADIUS-пакетов, которые сервер доступа (клиент) отправляет в сторону WNAM 2.
- Внешний IP-адрес.
- Имя устройства. В случае маршрутизатора Mikrotik и контроллера Bluesocket указание имени пользователя и пароля позволит обеспечить привязку DHCP-имени пользователя к его учётной записи и обеспечить определение ряда дополнительных параметров в момент начала аккаунтинга (RADIUS Acct-Start) сессии пользователя. Это происходит путём запроса (через API устройства) со стороны сервера WNAM 2 с применением указанных параметров входа. Рекомендуется создать соответствующую учётную запись на устройстве с правами "на чтение". Указанные в таблице параметры позволяют включить для данного сервера доступные возможности.

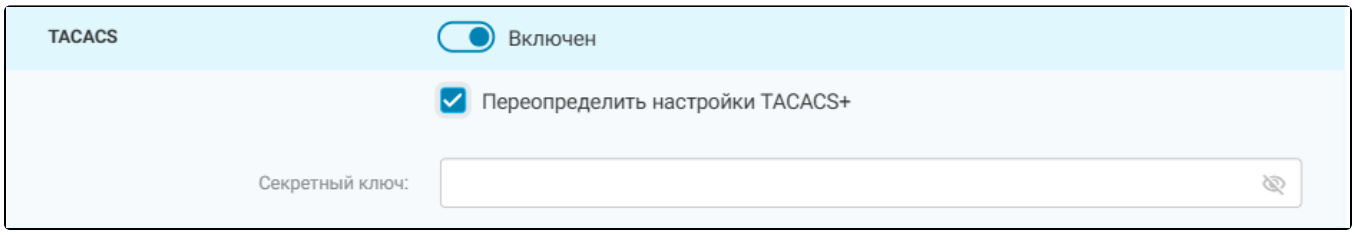
Некоторые сервера доступа (например, Mikrotik или Linux) позволяют по команде сбросить все активные сессии абонентов. Для этого используется кнопка "Сбросить сессии".

Сетевое устройство можно перевести в состояние "Выключен". В этом случае авторизация через сервер осуществляться не будет, а абоненты получат отказ во входе в сеть.

При включении параметра RADIUS отображается дополнительное меню с настройками авторизации. В данном разделе можно указать атрибуты предварительной авторизации и атрибуты пост-авторизации, секретный ключ, порт CoA, а также включить /выключить авторизацию по MAC-адресу.



При включении параметра TACACS+ отображается окно с настройками TACACS+ соединения, в котором можно указать секретный ключ. Там же можно переопределить параметры SNMP-подключения.



Также возможно определить категории и свойства категорий для определенного сетевого устройства. Подробное описание по созданию и редактированию категорий объектов описаны в соответствующем разделе.

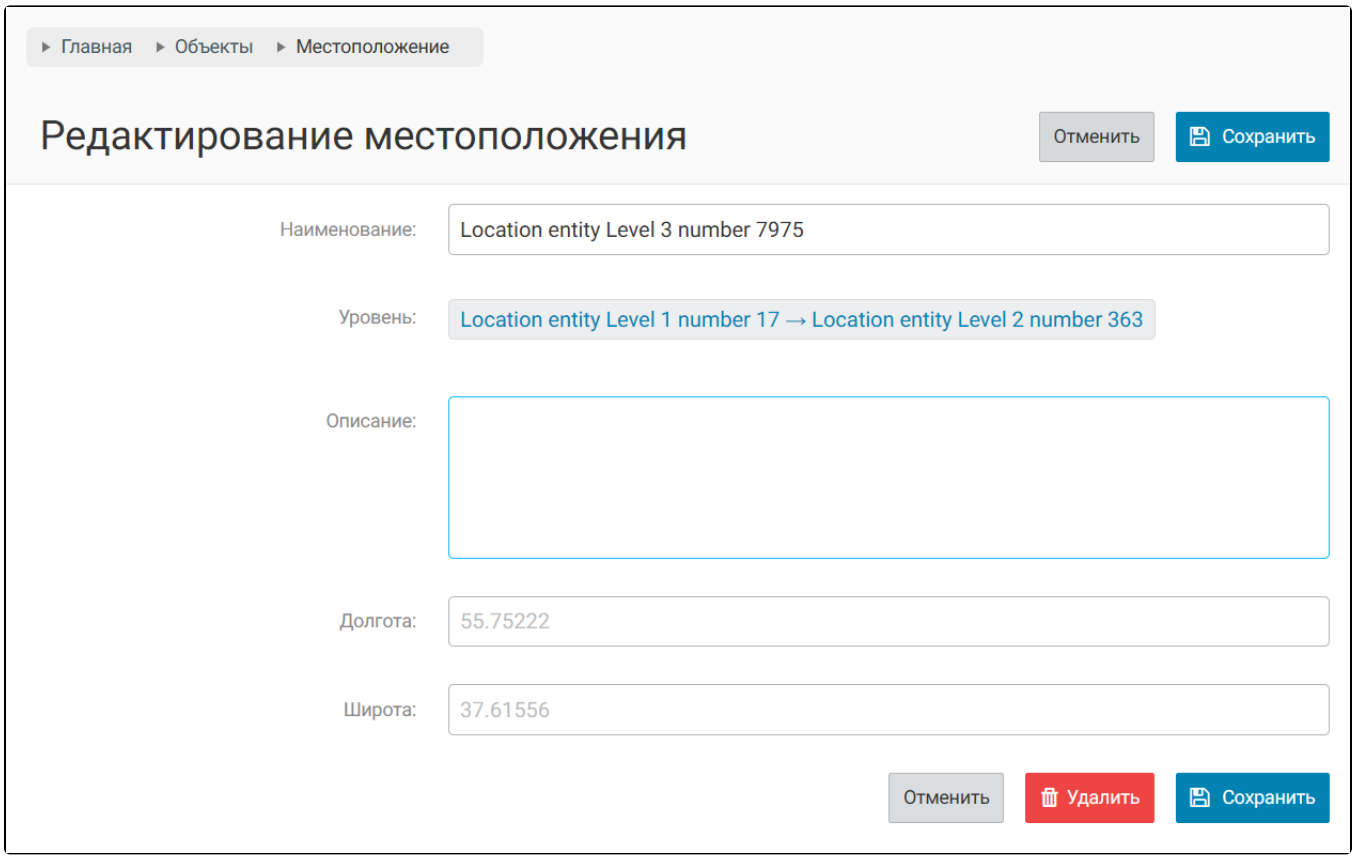
Местоположение

Данный раздел меню позволяет создавать, просматривать и редактировать записи об объектах типа "**Местоположение**". Местопол ожением в терминологии WNAM 2 называется точка оказания услуги конечному абоненту Wi-Fi, которая характеризуется географическим различием. Например, теоретическим местоположением может быть сеть, расположенная за хотспотом маршрутизатора Mikrotik, сеть одного кафе/ресторана/бизнес-центра. Вся статистическая информация в отчётах будет формироваться с точностью "до местоположения". Таким образом, не рекомендуется использовать один хотспот/одну площадку для подключения абонентов с нескольких территориально-распределенных объектов. Иначе невозможно будет в статистике различить, с какого из объектов была установлена сессия.

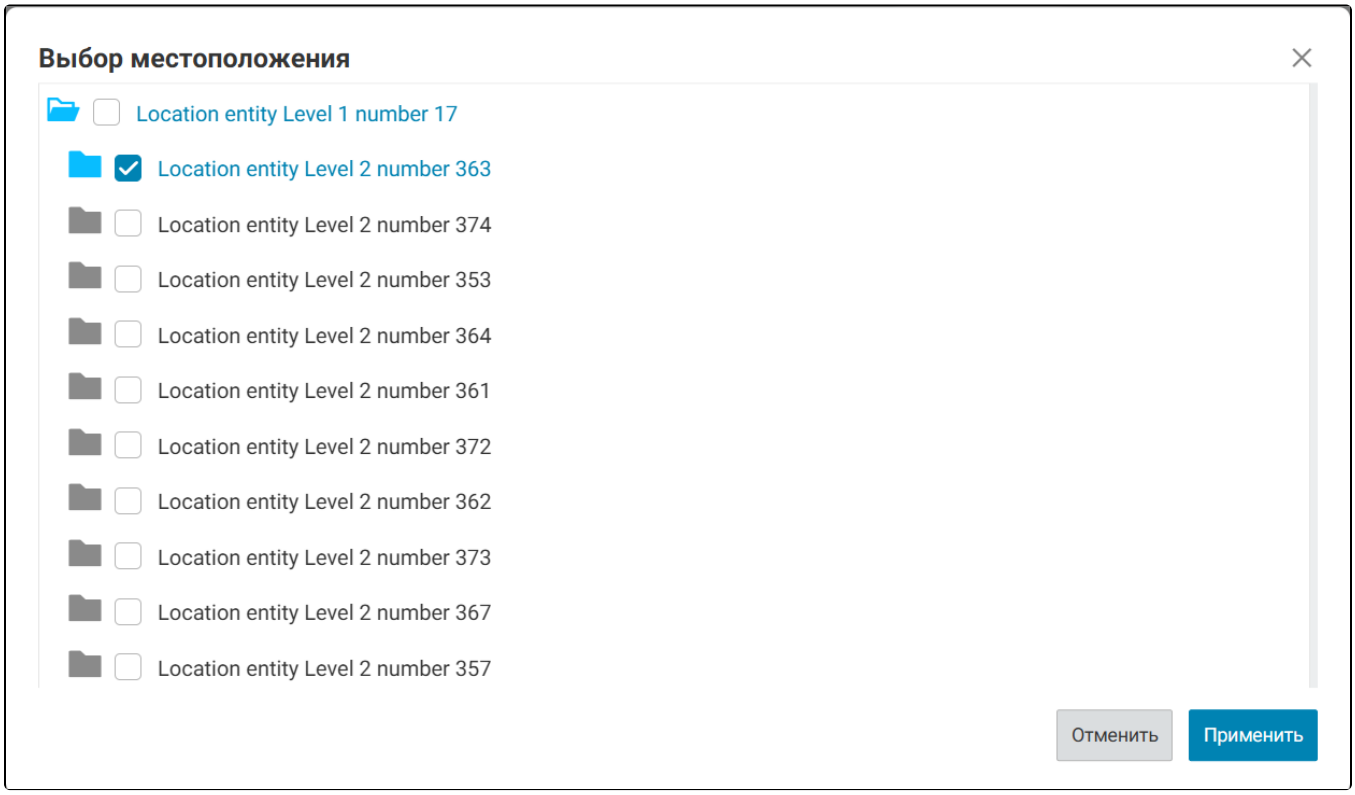
В случае управляемых контроллером радио-сетей возможно использование одного сервера доступа и нескольких площадок с распределением сессий по ним на основе IP-адресов, либо на основе идентификаторов местоположения, настраиваемых непосредственно на Wi-Fi контроллере. Рекомендуется использовать не пересекающиеся IP-адресные пространства на площадках во избежание путаницы. Приватные адреса бесплатны.

В основном окне раздела "Объекты" "Местоположение" приведена вложенный список всех местоположений.
Выключенные площадки не учитываются при подсчете числа лицензий на площадку. Таким образом, если клиент ушел, можно выключить площадку (оказание услуги на ней блокируется). При этом, статистика сохранится, освободившуюся лицензию от этой площадки можно будет использовать для нового местоположения.

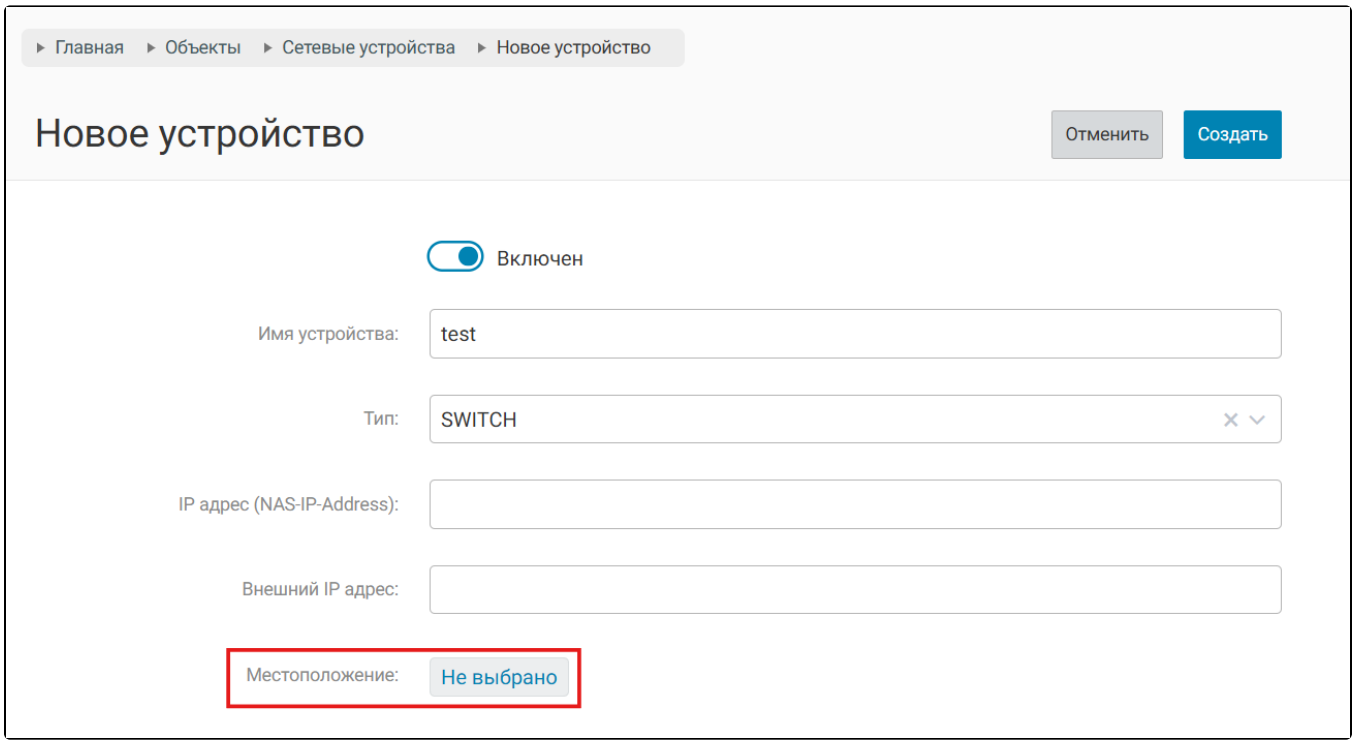
Каждое местоположение может иметь уровень вложенности. Для того, чтобы перейти на необходимый уровень вложенности, требуется нажать левой кнопкой мыши на иконке папки. Нажатие левой кнопкой мыши на строку определенного местоположения вызывает окно редактирования свойств, аналогично операции "Новое местоположение". Основными параметрами площадки являются наименование, уровень вложенности, описание, долгота и широта адреса.



При выборе уровня вложенности, необходимо учитывать функциональное разделение. Например, при реализации сети с разграничением на отделы, можно в основной уровень выделить коммерческий отдел с подуровнем на отдел продаж и подуровнем на маркетинговый отдел.

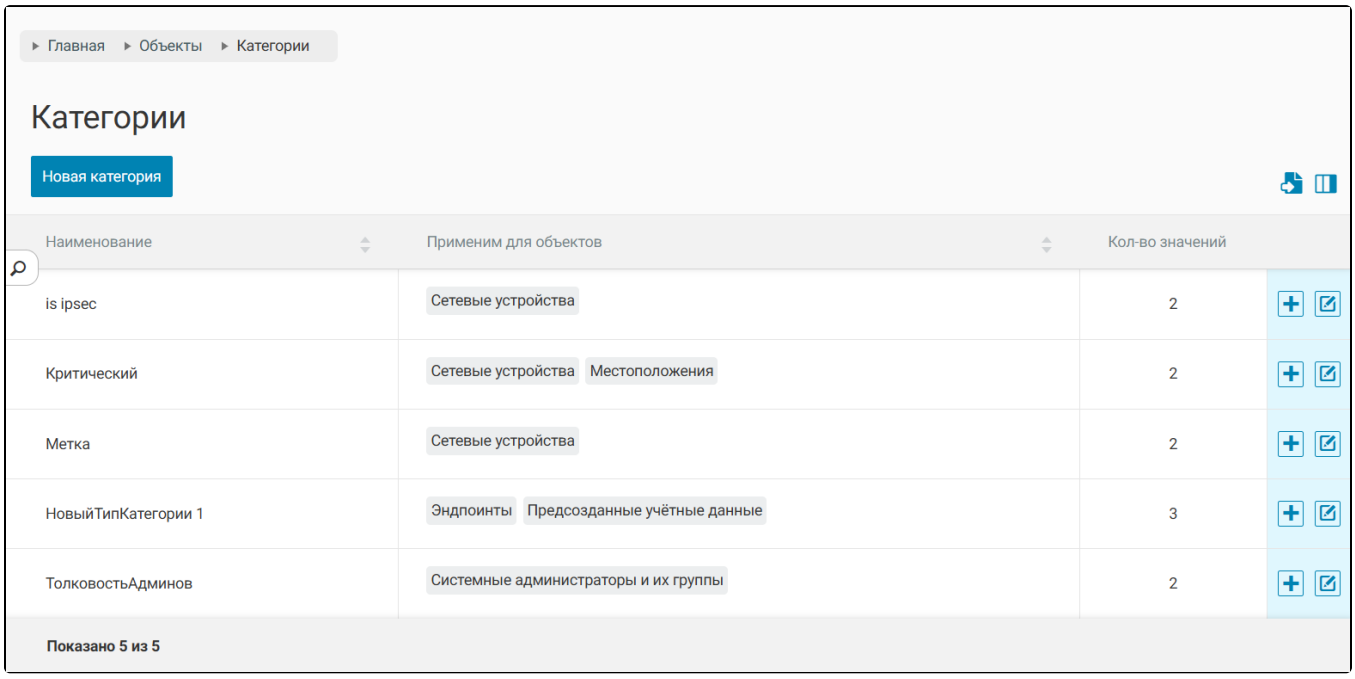


В последствии, местоположение можно определить для сетевых устройств в целях верной идентификации и определения.

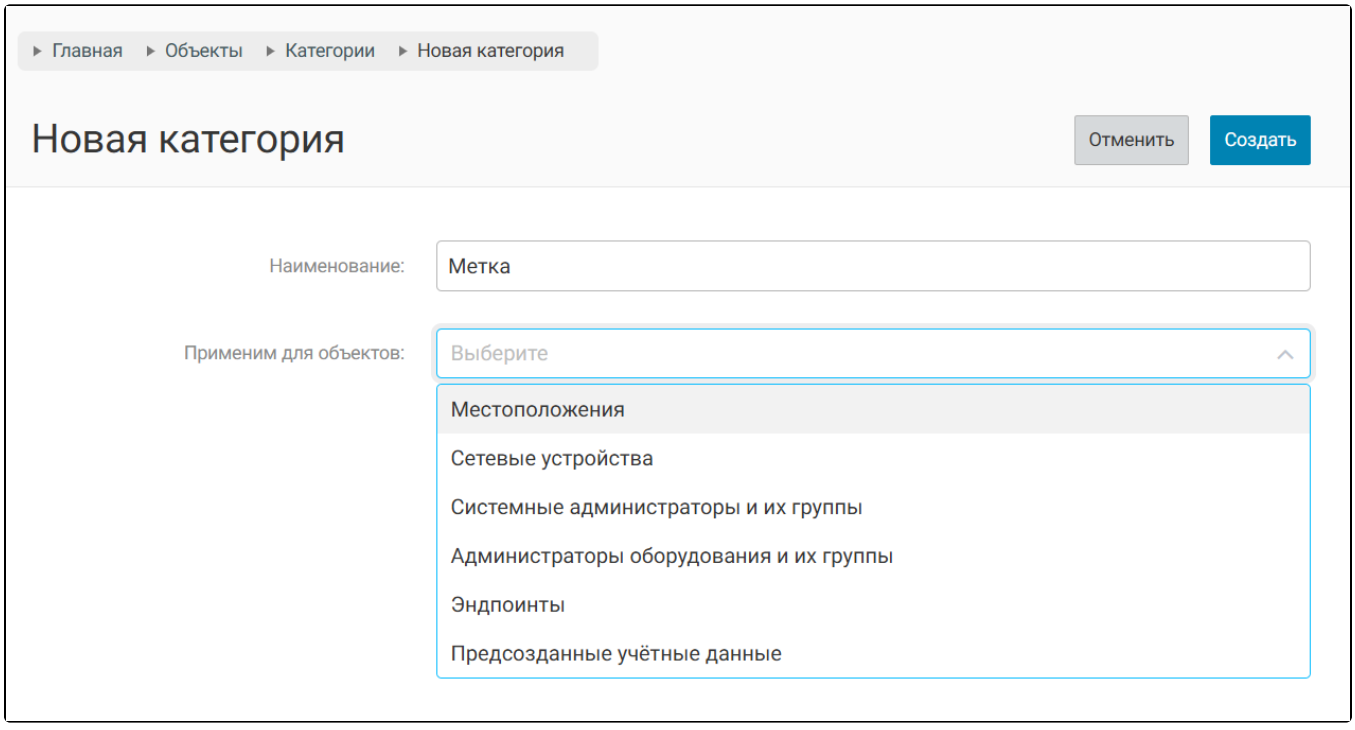

Главная
Объекты
Сетевые устройства
Новое устройство
Новое устройство
Отменить
Создать
Включен
Имя устройства:
test
Тип:
SWITCH
IP адрес (NAS-IP-Address):
Внешний IP адрес:
Местоположение:
Не выбрано

Категории

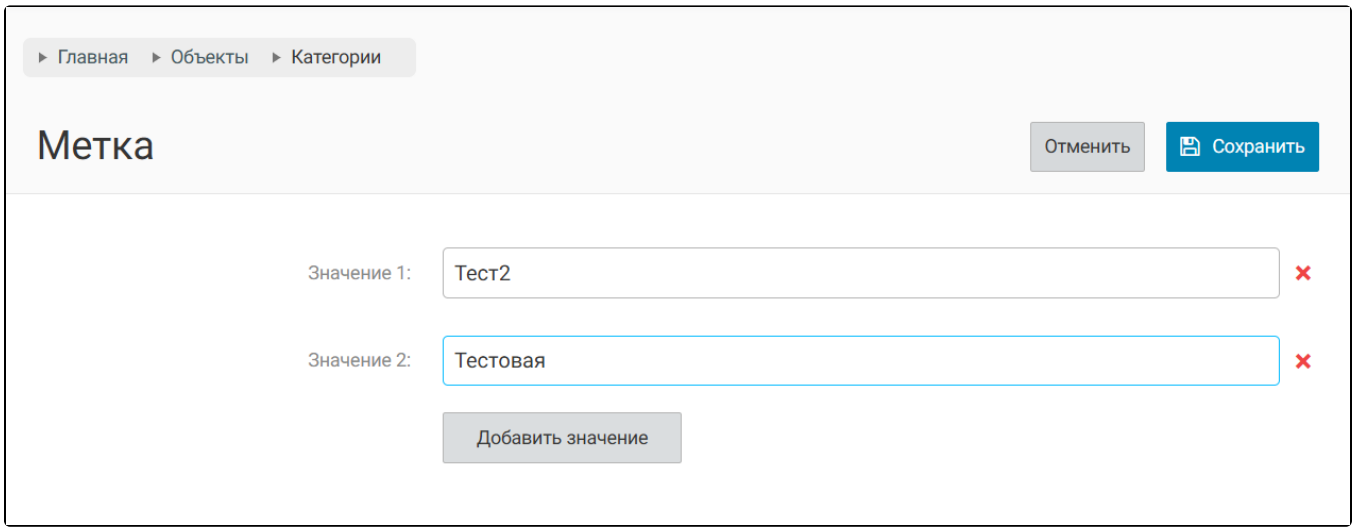
Категории предоставляют гибкую настройку фильтров для точного определения сетевых устройств. В этом разделе описываются все категории, которые могут быть применимы к различным объектам (местоположение, сетевые устройства, системные администраторы и т.д.).



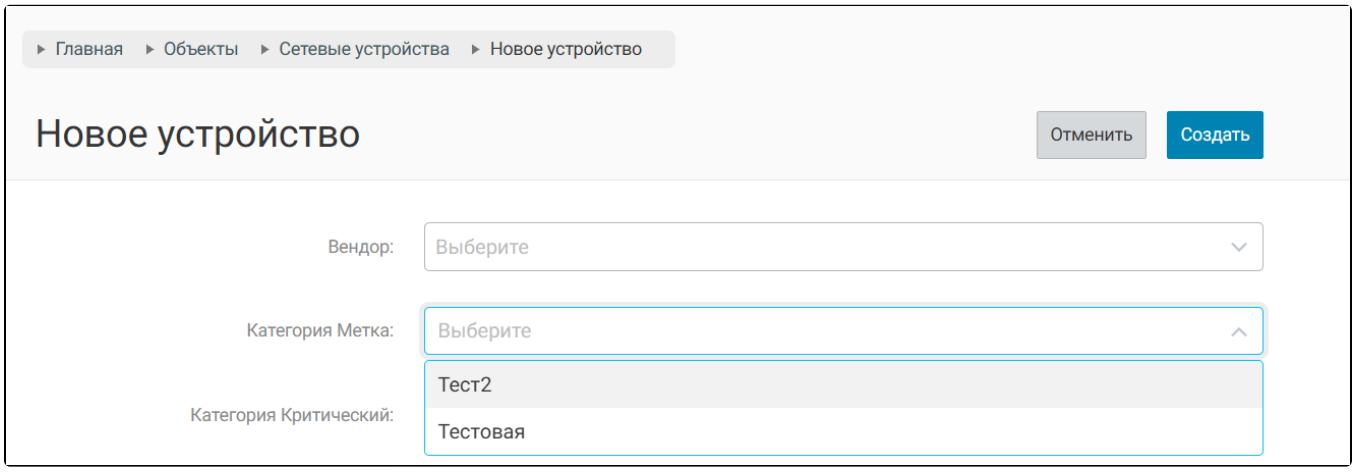
Для создания новой категории необходимо выбрать функцию "Новая категория". После, будет открыто окно, в котором требуется указать название категории и для каких объектов будет применима категория:



После создания новой категории необходимо определить значения этой категории, которые в последствии будут применимы для объектов WNAM 2. Для этого, напротив требуемой категории необходимо нажать на знак "плюс"  .



После создания категории и определения значений категории, будет возможным применение ее к требуемому объекту. В примере была создана тестовая категория "Метка", применяемая к объектам сетевых устройств:



Система категорий поможет в дальнейшем корректно определять объекты в системе WNAM 2.

Службы каталога

В зависимости от необходимости, возможно подключить два вида служб каталога:

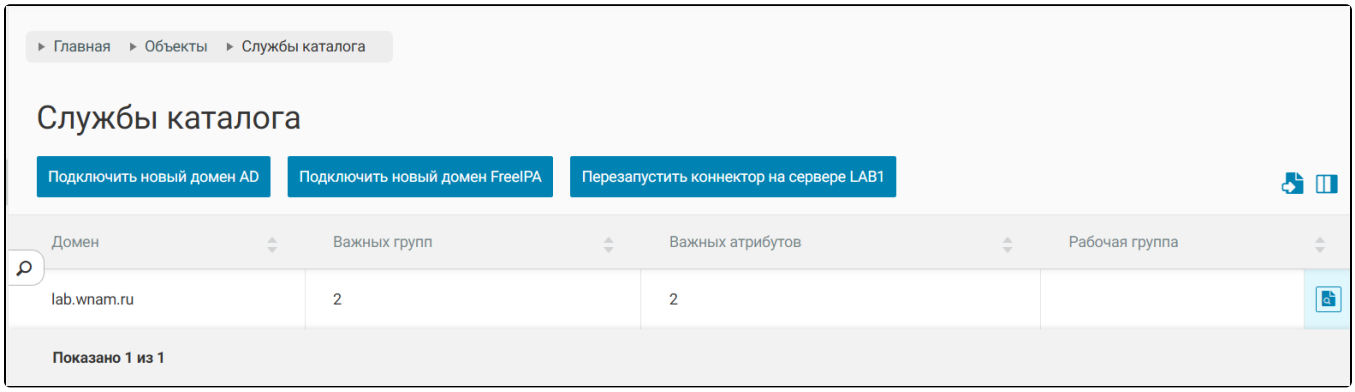
- Подключение к Active Directory
- Подключение к FreeIPA

Настройки подключения находятся в соответствующих подразделах.

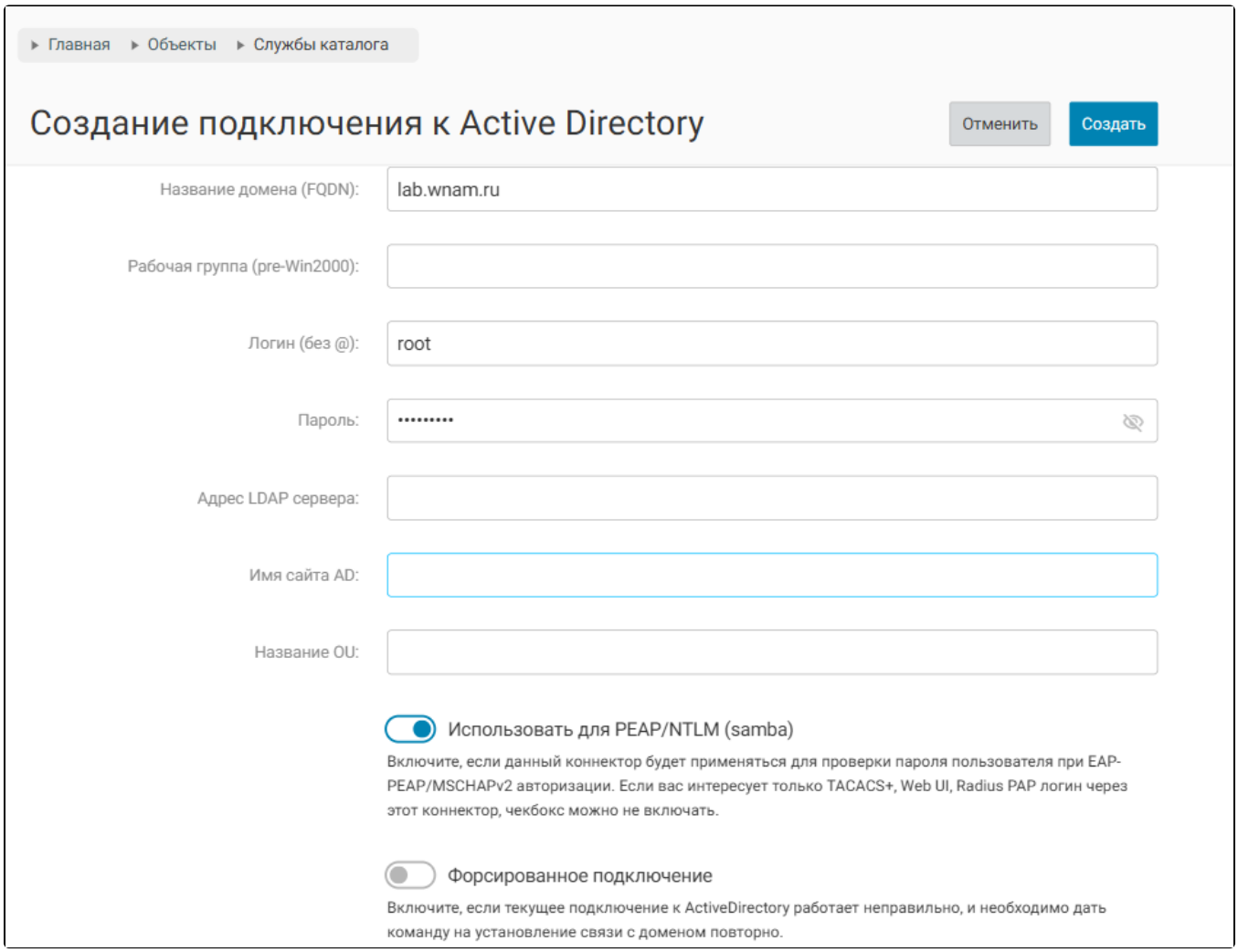
Подключение к Active Directory

Для настройки подключения к Active Directory необходимо перейти в административный интерфейс системы WNAM 2 в раздел "Объекты" "Службы каталога". В разделе "Службы каталога" будет отображено окно, которое показывает:

- Статус взаимодействия с интеграционной службой adctool с возможностью отправки команды на её перезапуск (перезапуск коннектора).
- Список подключенных доменов, с информацией:
    - название домена
    - для каждого из серверов кластера WNAM 2:
        - количество важных групп;
        - количество важных атрибутов;
        - рабочая группа.



При нажатии на кнопку "Подключить новый домен AD" будет открыто окно с вводом параметров:



Необходимо указать, как минимум, имя домена и верные учетные данные администратора, который будет подключать сервер WNAM 2 к домену (предпочтительнее с ролью доменного администратора). Вместо этого, вы можете попросить администратора вашего домена ActiveDirectory делегировать вашей собственной доменной учетной записи право создавать записи о компьютерах в домене.

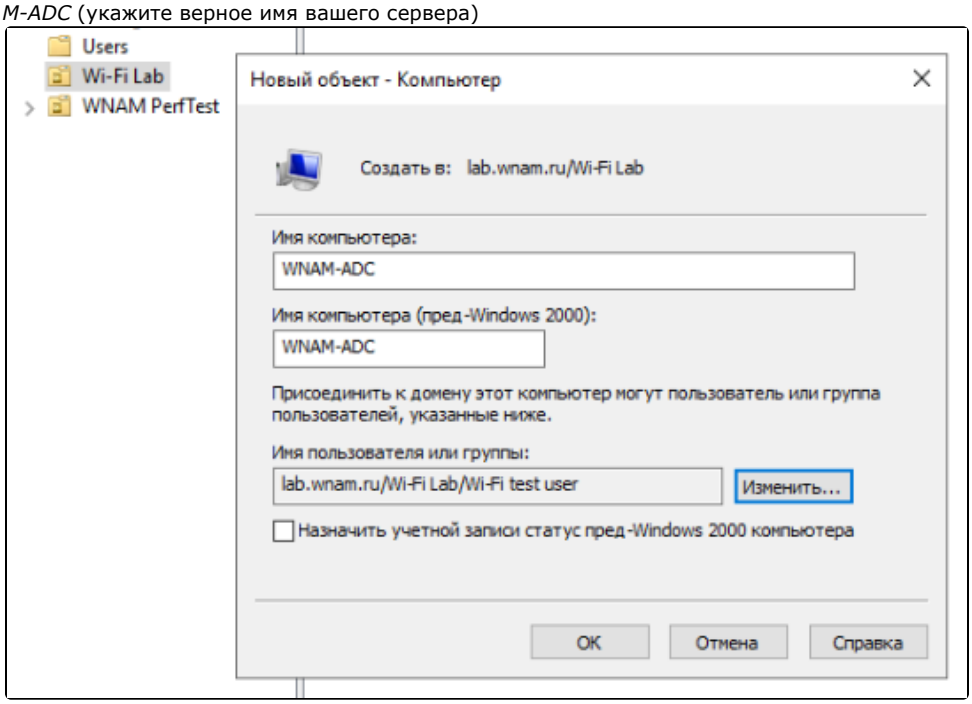
При использовании в качестве контроллера домена samba-dc в его настройках (smb.conf) нужно добавить опции:

ntlm auth = mschapv2-and-ntlmv2-only (также можно использовать опции с более низкими требованиями к безопасности ntlm auth = `ntlmv1-permitted`)

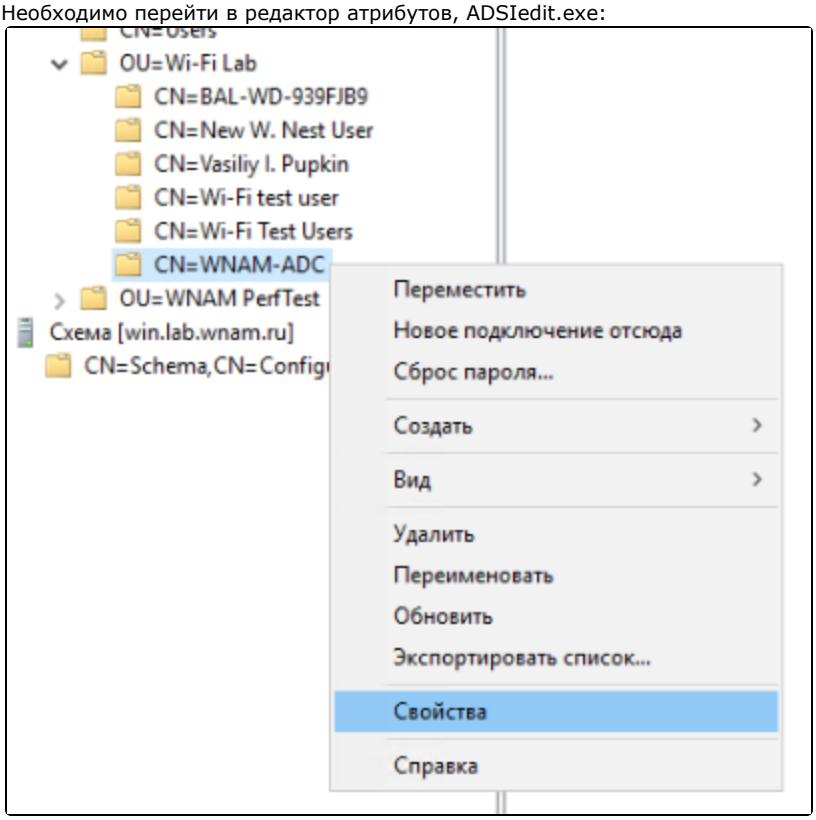
ldap server require strong auth = allow_sasl_over_tls (также можно использовать опции с более низкими требованиями к безопасности ldap server require strong auth = no)

Подключение от имени обычного пользователя можно организовать так:

1. В Active Directory в нужном OU администратором домена создаются две записи типа "Компьютер", например *WNAM* и *WNAM-ADC* (укажите верное имя вашего сервера)

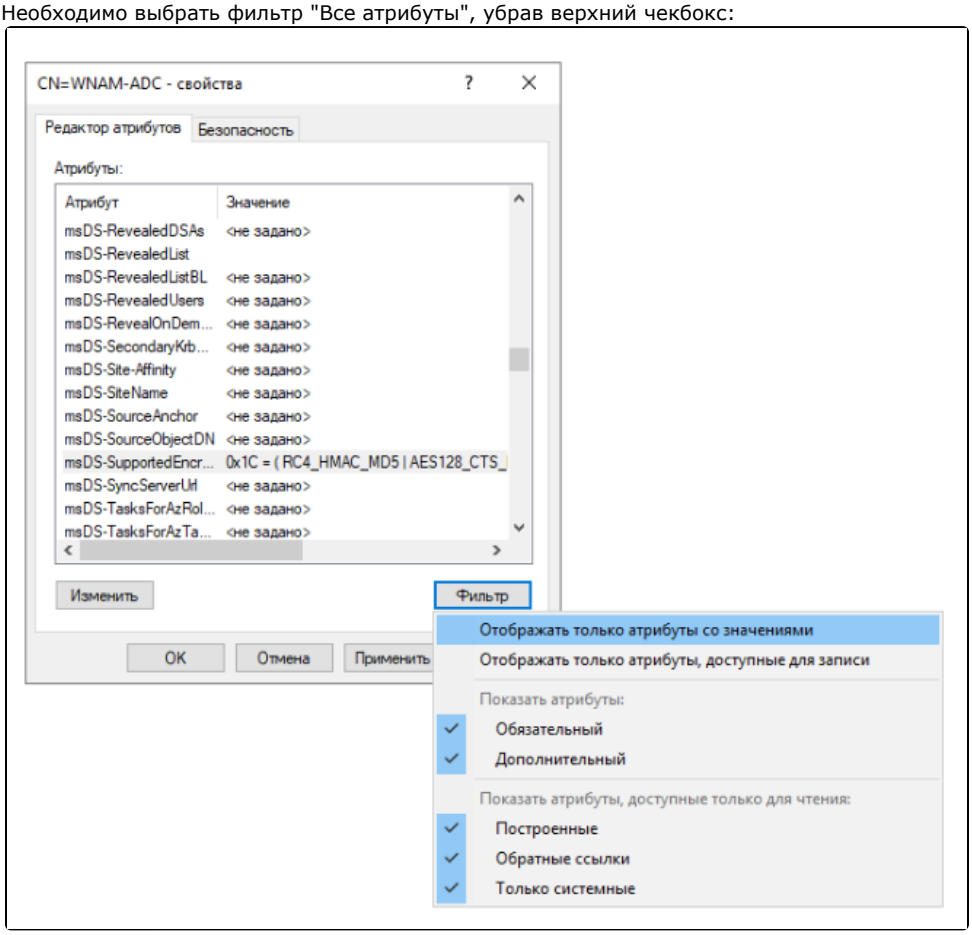


2. Он выдает права вашей учетной записи, через кнопку "Изменить"
3. Необходимо перейти в редактор атрибутов, ADSIedit.exe:

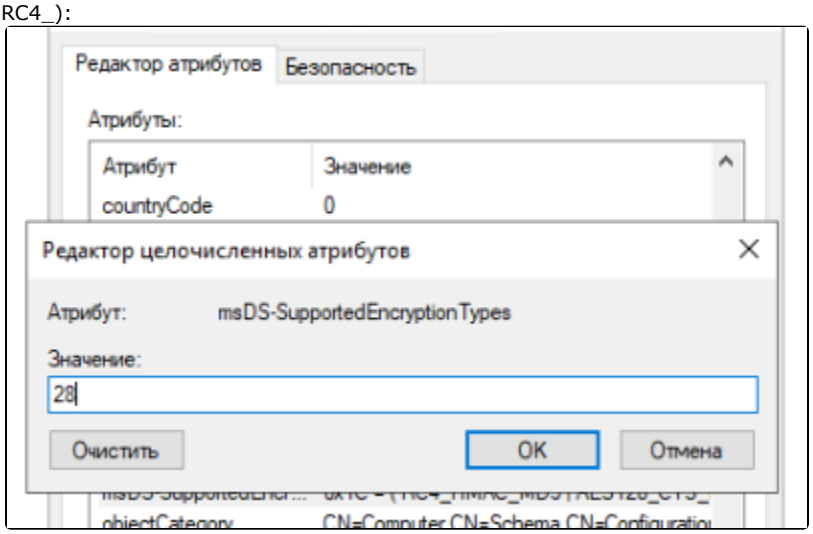


4. Изменить LDAP-свойства объекта - только той учетной записи компьютера, которая имеет имя -ADC.

5. Необходимо выбрать фильтр "Все атрибуты", убрав верхний чекбокс:



6. Необходимо поменять значение у атрибута "msDS-SupportedEncryptionTypes" с "не задано" на 28 (или 24, чтобы не было RC4_):



7. Необходимо сохранить изменения

Указанные учетные данные используются один раз, и не будут сохранены в дальнейшем. В результате подключения сервер WNAM 2 будет введен в домен как обычная рабочая станция два раза:

- под собственным именем сервера, например, WNAM, для целей NTLM-взаимодействия (используя samba/winbind);
- под именем сервера с постфиксом "-ADC", например, WNAM-ADC, для целей LDAP-взаимодействия (используя python /ldap3).

Существует жесткое ограничение на NETBIOS-имя - 15 символов. Таким образом, с учетом добавления суффикса -ADC и исходному имени, его длина не может превышать 11 символов. Не называйте ваш сервер длинным (более 11) символов именем, в противном случае ADCTool не сможет выполнить подключение к домену.

Обращаем внимание, что сервер WNAM 2 будет введен в домен дважды, как две разные рабочие станции.

Для корректной работы LDAP-подключения необходимо, чтобы ваш контроллер домена поддерживал TLS-соединение по протоколу LDAP. Система WNAM 2 не поддерживает подключение по LDAP без шифрования, т.к. оно обязательно для создания машинной учётной записи. Для поддержки шифрования в канале LDAP необходимо включить на контроллере домена поддержку TLS, для чего на контроллер домена необходимо поместить SSL-сертификат с ключом. Для того, чтобы это сделать следует обратиться к документации вендора Майкрософт либо к более детальной инструкции.

WNAM 2 поддерживает одновременное взаимодействие с несколькими несвязанными доменами (мульти-домен). Для этого вам необходимо установить на сервер WNAM 2 специальную библиотеку libwinbind-client.so (вручную, или скриптом upgrade-adctool.sh, либо она уже присутствует в эталонном образе виртуальной машины).

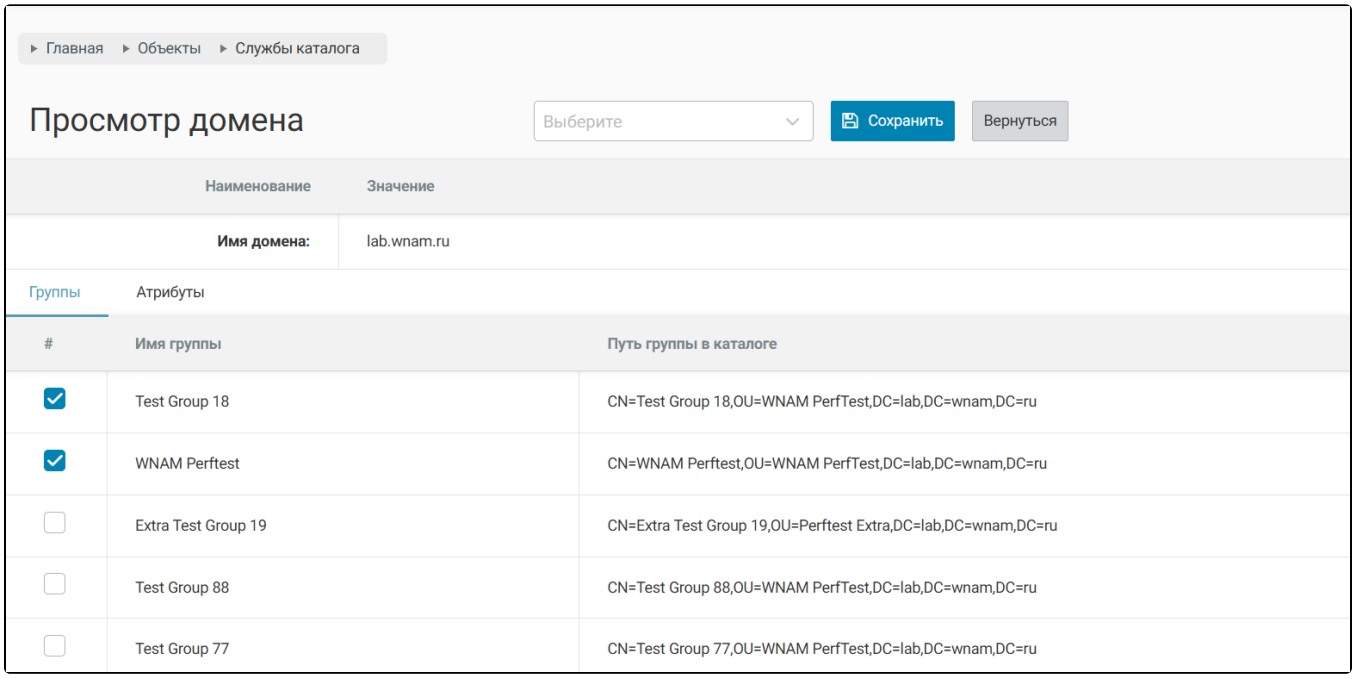
Оба механизма взаимодействия используют надежную авторизацию, основанную на автоматически обновляемых Kerberos-тикетах. При проведении запросов к контроллеру домена применяется машинная авторизация вашего сервера WNAM 2 и не используются служебные пользовательские учетные записи.

Если вы отключите чекбокс "Использовать для PEAP/NTLM (samba)" при создании подключения, запустится только LDAP-коннектор. Этого достаточно, если вы делаете подключение для проверки доменных учетных данных при логине через TACACS+, в веб-интерфейс WNAM 2, для сопоставления с группами/атрибутами при EAP-TLS авторизации.

Вы также можете указать, при необходимости, адрес вашего ближайшего LDAP-сервера, имя сайта Active Directory, если ваш домен очень большой и распределенный. Это позволит избежать ненужного поиска всех контроллеров в домене.

Если NETBIOS-имя вашего домена отличается от первой части (до точки) полного названия домена, что может случаться, если ваш домен создавался очень давно, укажите его старое имя (рабочей группы).

После добавления службы каталогов AD, автоматически импортируется список групп и атрибутов. Загрузив список групп и атрибутов, следует отметить желаемые чекбоксами и сохранить:



Если тестовая проверка прошла без ошибок, можно начать применять этот каталог (домен) в других настройках системы WNAM 2.

Подключение к FreeIPA

Система WNAM 2 в связке с adctool поддерживает взаимодействие со службой каталога FreeIPA для следующих целей:

- Авторизация RADIUS-пользователей по PAP EAP_PEAP с проверкой пароля (NT Hash).
- Авторизация RADIUS-пользователей по PAP, EAP_PEAP и EAP_TLS с проверкой членства пользователя (Identity) в доменной группе (группе каталога).
- Авторизация TACACS+ пользователей/администраторов сетевого оборудования.

Взаимодействие протестировано с сервером службы каталога FreeIPA версии 4.8.10, работающим под управлением ОС Astra Linux 1.7.3 "Смоленск". В отличии от интеграции с Microsoft Active Directory, где не требуются дополнительные настройки самого домена/контроллера домена, для FreeIPA необходимо будет выполнить определенные действия на главном сервере службы каталога.

В приведенном ниже примере используются следующие наименования:

- имя домена (каталога): astradom.wnam.ru;
- имя контроллера домена (каталога): wnam16-astra.astradom.wnam.ru;
- имя сервера, на котором установлен adctool: wnam-15.astradom.wnam.ru;

1. Настройка каталога

Необходимо зайти в консоль контроллера с правами администратора - root (либо выполнить команды через sudo).

```
###

apt install freeipa-server-trust-ad

ipa-adtrust-install --add-sids

###

ipa permission-add 'ipaNTHash service read' --attrs=ipaNTHash --type=user --right=read
ipa privilege-add 'Radius services' --desc='Privileges needed to allow radiusd servers to operate'
ipa privilege-add-permission 'Radius services' --permissions='ipaNTHash service read'

###    RADIUS-,

ipa role-add 'Radius server' --desc="Radius server role"
ipa role-add-privilege --privileges="Radius services" 'Radius server'

###    ,

ipa service-add 'wnam/wnam16-astra.astradom.wnam.ru'
```

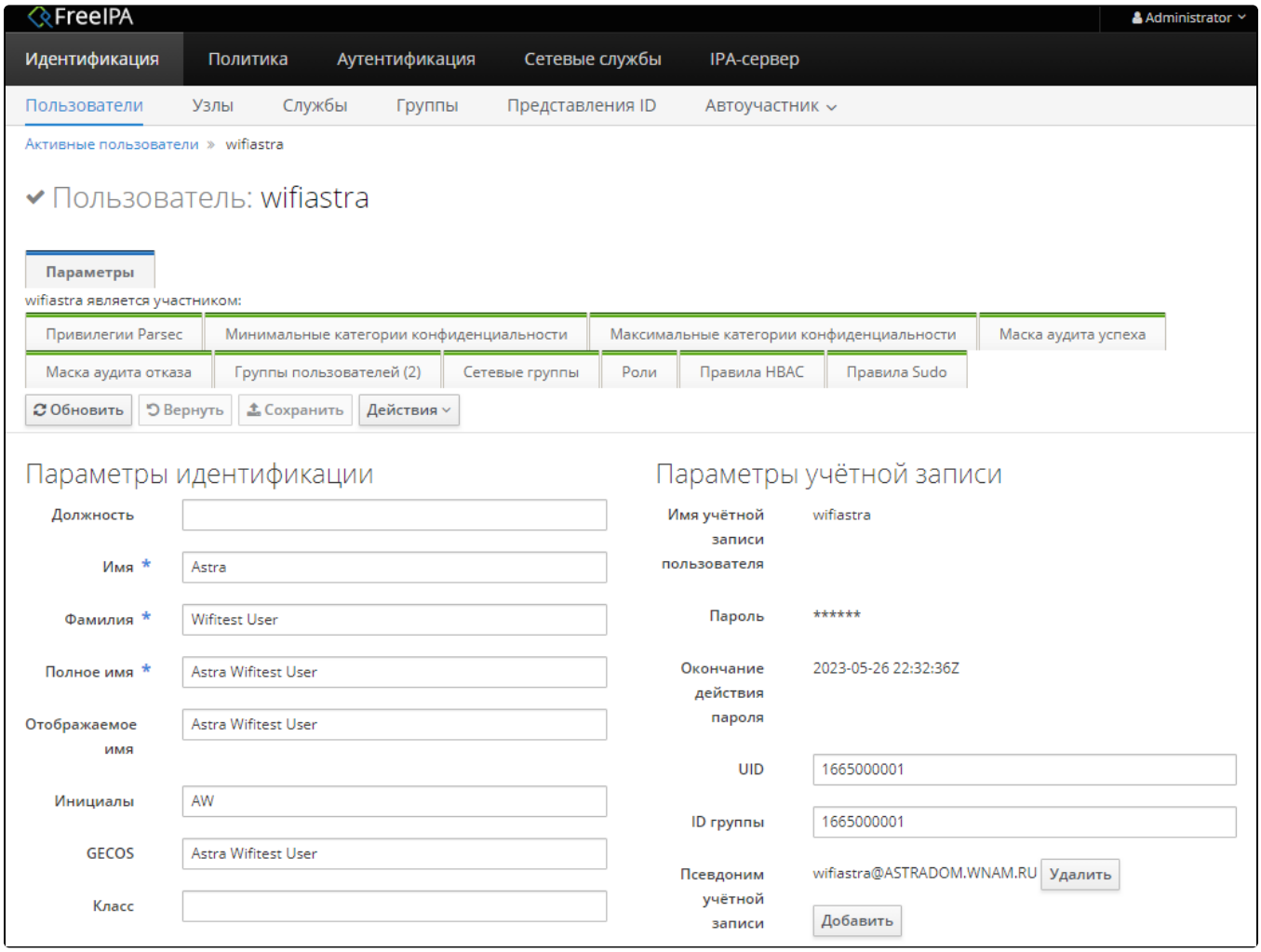
Далее необходимо создать файл **ldif.txt** с командами, которые позволят задать сервису статический пароль (в примере - Qwerty123):

```
dn: krbprincipalname=wnam/wnam16-astra.astradom.wnam.ru@ASTRADOM.WNAM.RU,cn=services,cn=accounts,
dc=astradom,dc=wnam,dc=ru
changetype: modify
add: objectClass
objectClass: simpleSecurityObject
-
add: userPassword
userPassword: Qwerty123
```

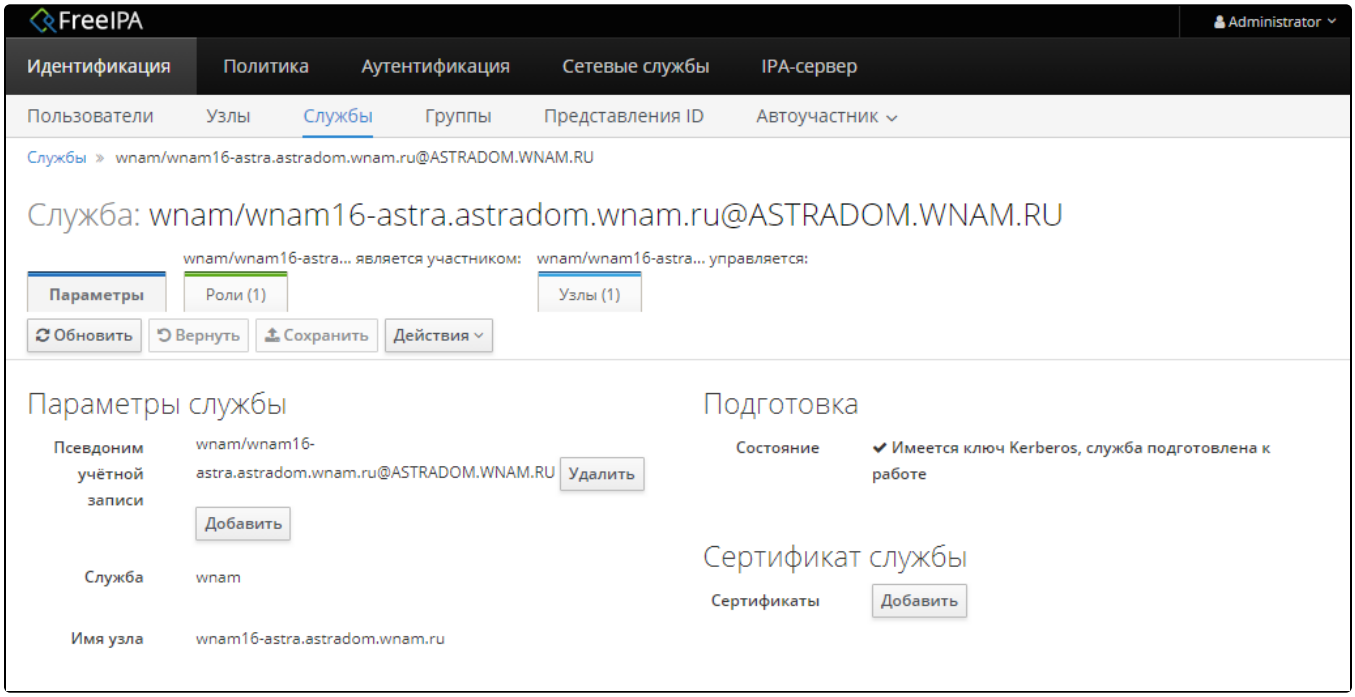
Применить команду к каталогу:

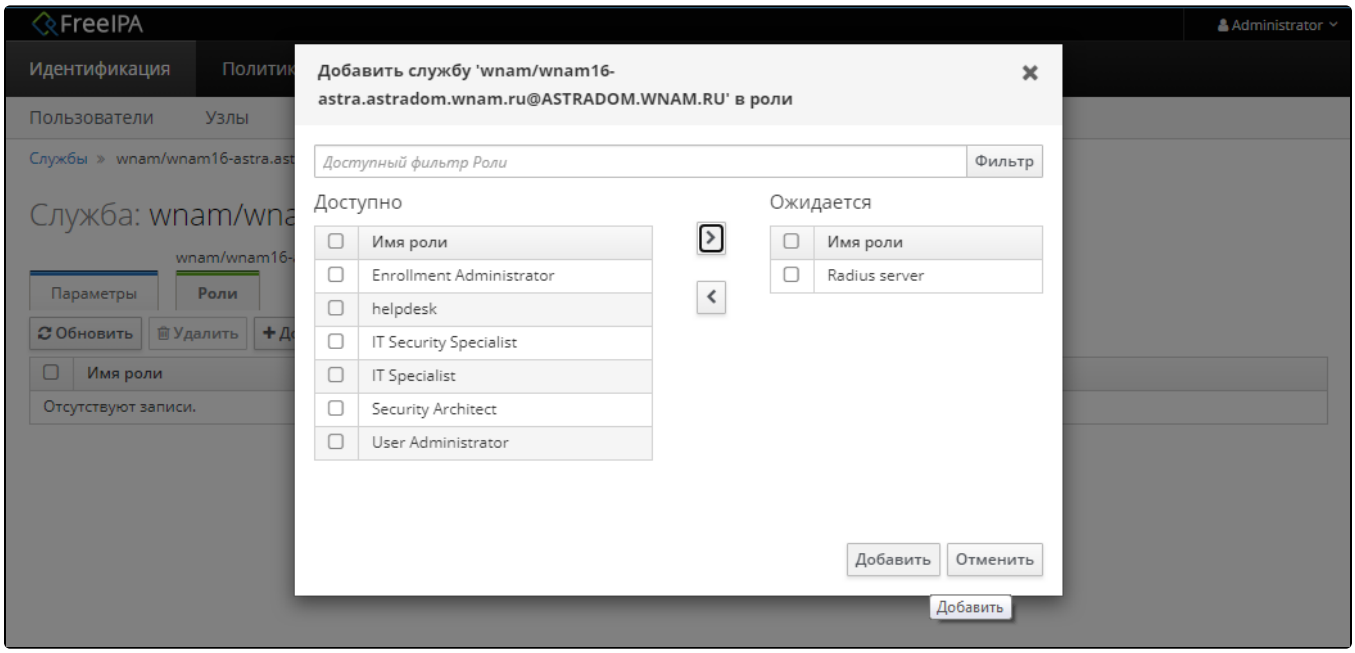
```
ldapmodify -f ldif.txt -D 'cn=Directory Manager' -W -H ldap://wnam16-astra.astradom.wnam.ru -Z
```

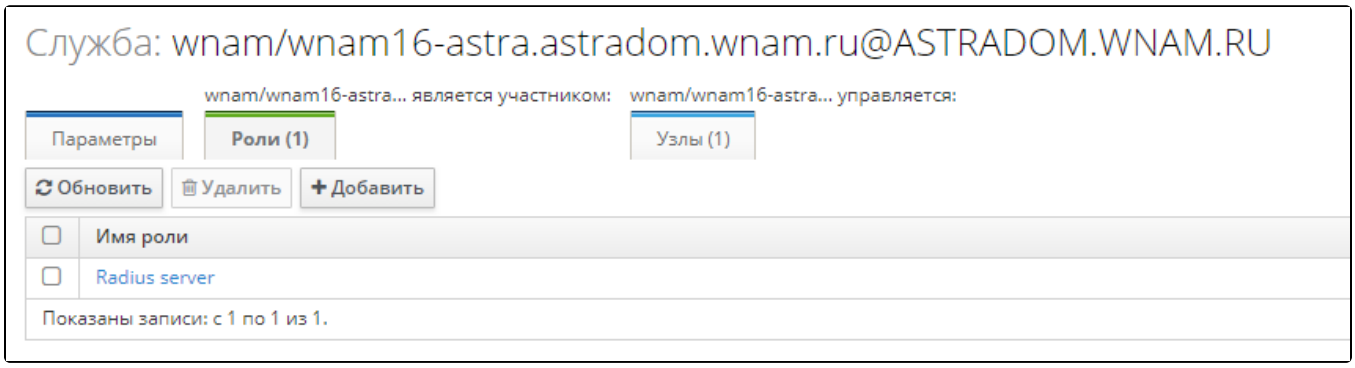
Создать пользователя **wifiastra** и задать ему пароль (пригодные для работы хэши паролей будут храниться в каталоге только после применения ipa-adtrust-install, для старых пользователей пароли необходимо будет пересоздать):

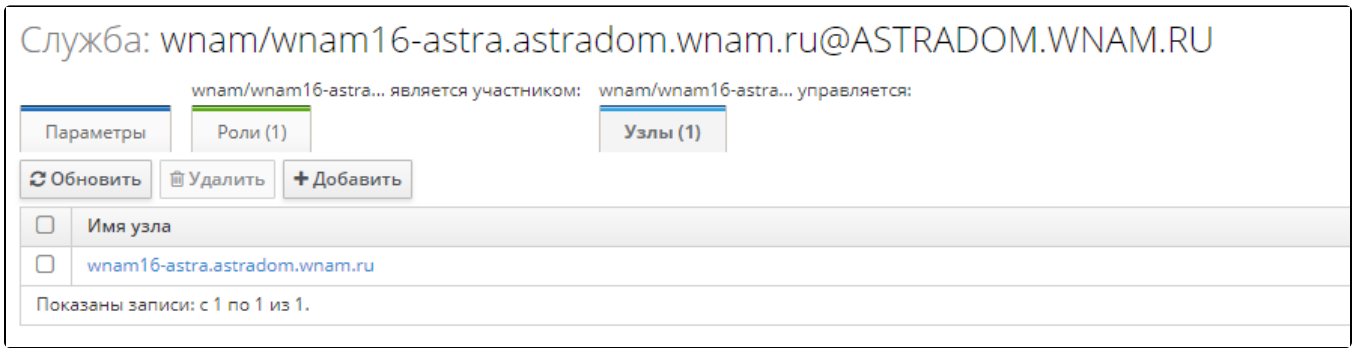


В веб-интерфейсе FreeIPA необходимо добавьте Роль "Radius server" службе wnam/wnam16-astra.astradom.wnam.ru :



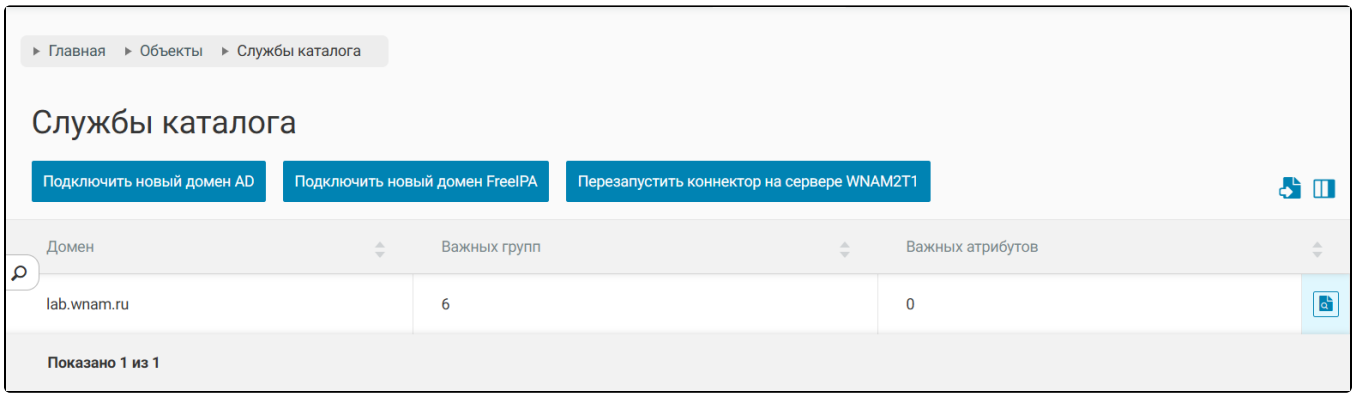






2. Настройка системы WNAM

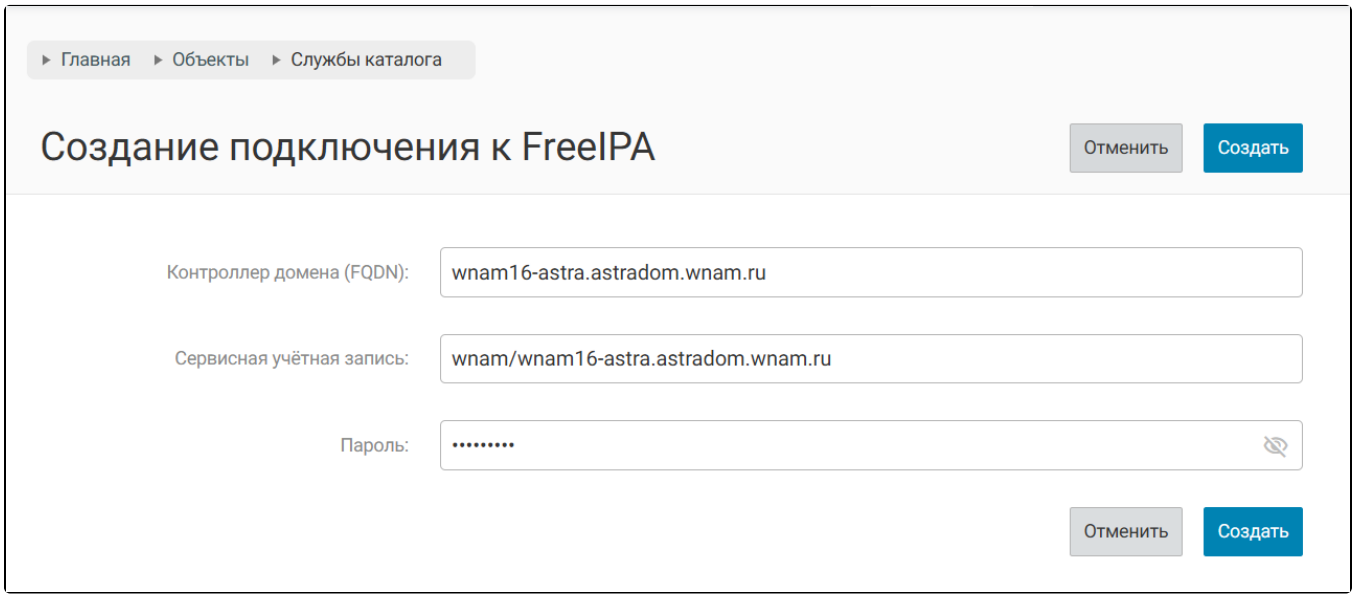
Для настройки подключения необходимо перейти в систему WNAM 2 в раздел "Объекты" "Службы каталогов" и нажать кнопку "Подключить новый домен FreeIPA":



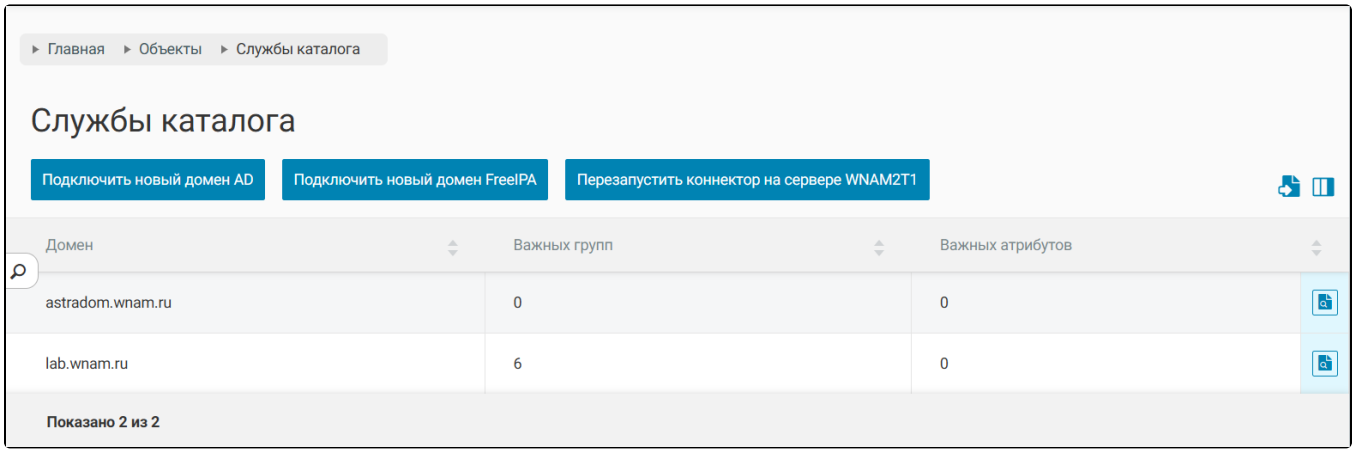
В открывшемся окне необходимо указать:

- полное имя сервера каталога;
- имя сервисной учётной записи;
- пароль сервисной учётной записи.

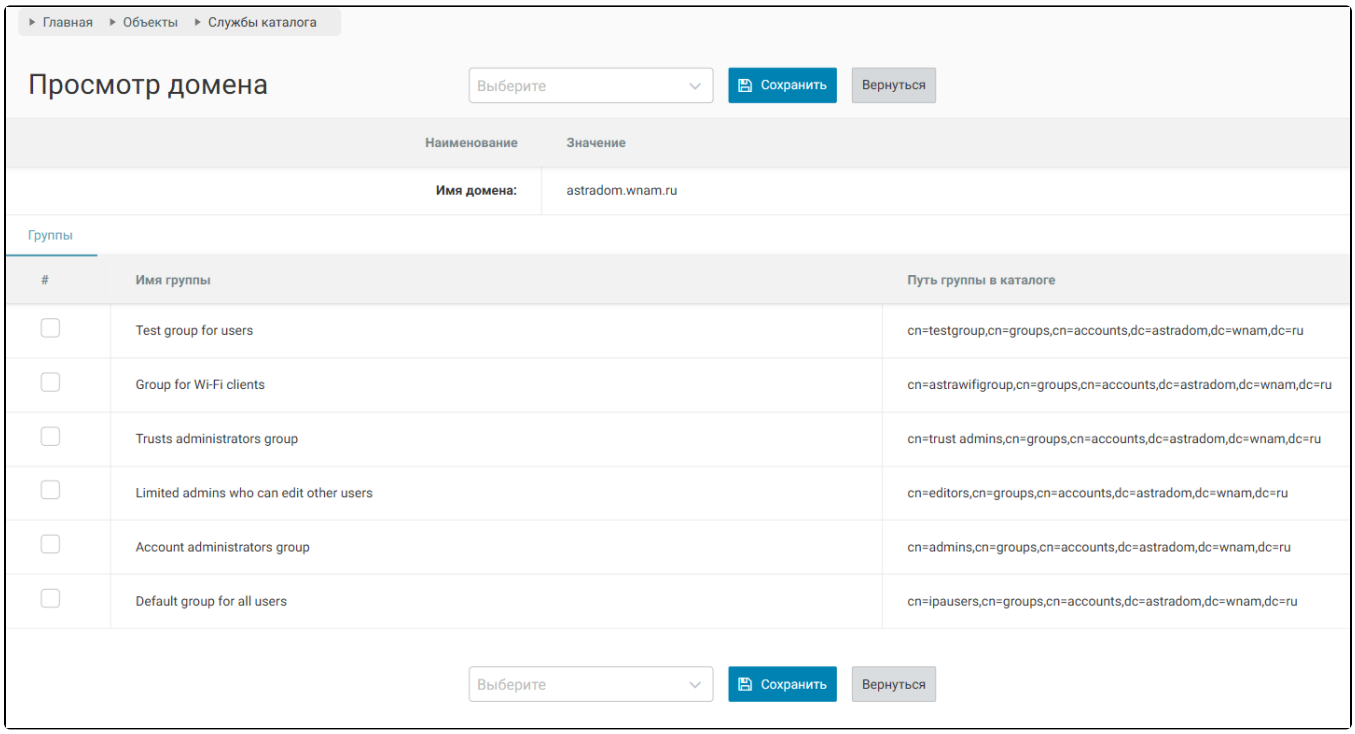
В дальнейшем эти данные будут сохранены в /home/wnam/adctool/config.json. Пароли хранятся в шифрованном виде.



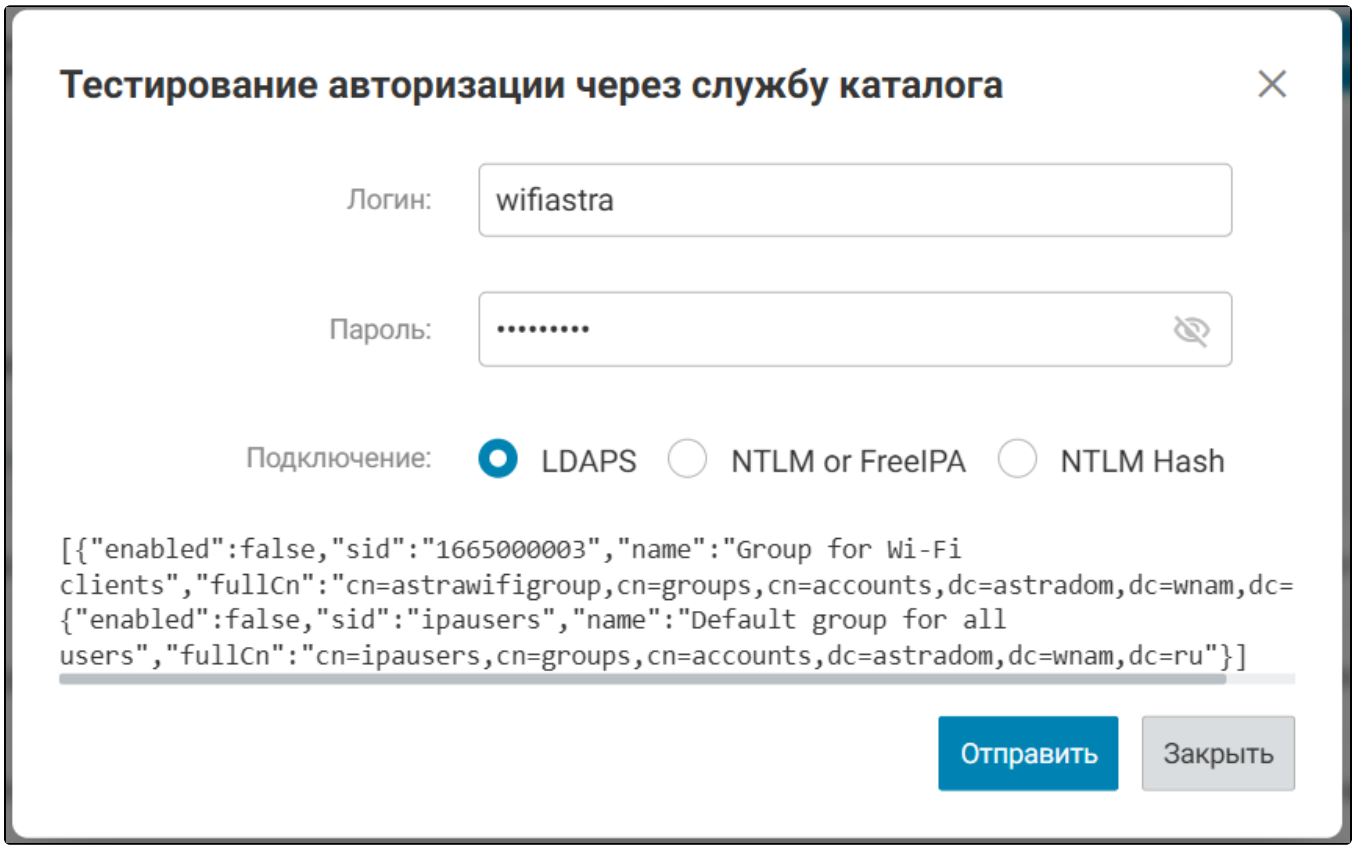
По окончании настройки подключения будет отображен статус взаимодействия:

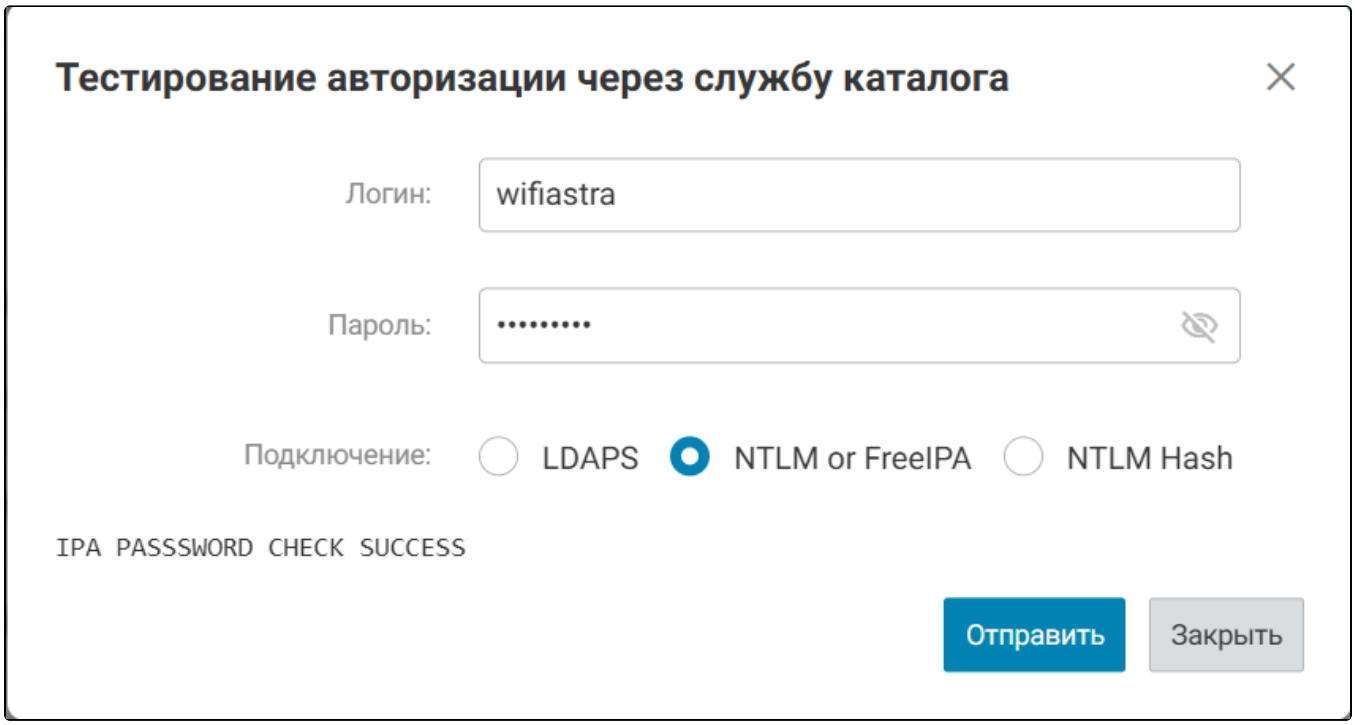


При нажатии на контекстное меню в таблице служб каталога можно выбрать и настроить группы:



А также можно проверить авторизацию через LDAP для ранее созданного тестового пользователя:



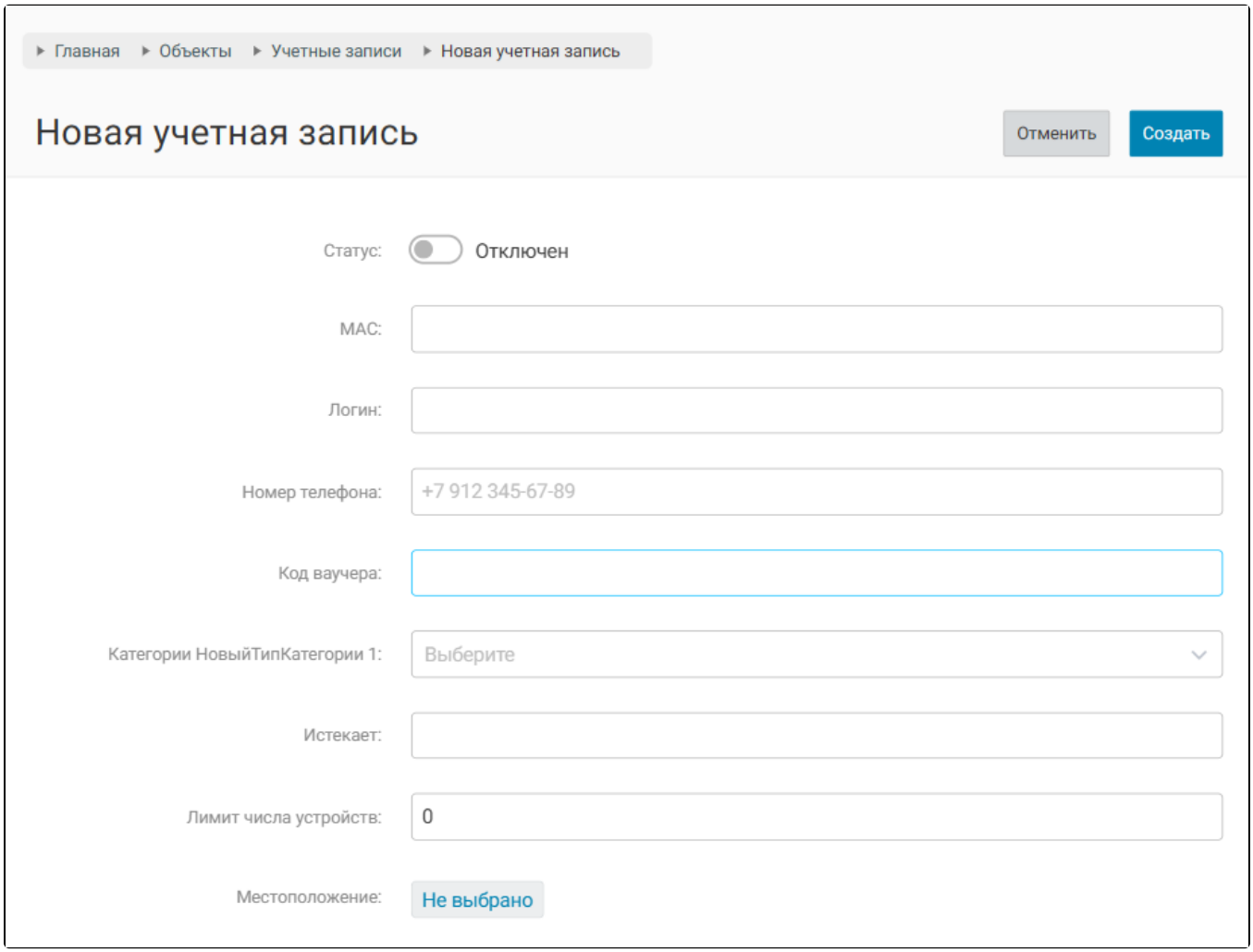


Если проверки работают, то можно применять настроенное подключение к службе каталога FreeIPA в других настройках WNAM 2.

Учетные записи

Данный раздел объектов позволяет создавать отдельно учетные записи для пользователей (подразумевается именно учетные записи участников, учетные записи администраторов находятся в другом разделе настоящей документации), которым будет необходимо предоставить доступ в интернет, на временный промежуток или нет.

При переходе в раздел учетных записей отображается таблица уже созданных учетных записей, для создания новой учетной записи необходимо выбрать кнопку "Новая учетная запись".



При создании новой учетной записи, важно учитывать следующие поля (некоторые поля можно оставить опциональными):

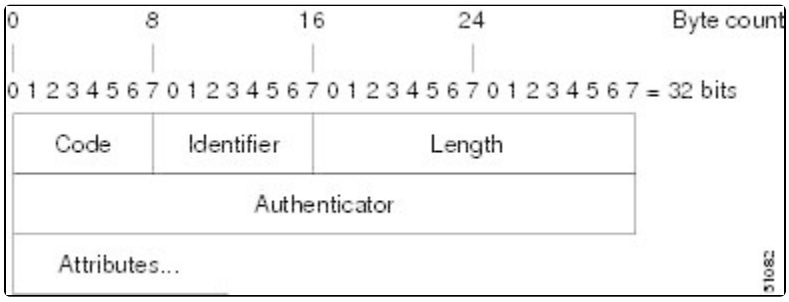
- Статус включенности;
- MAC адрес устройства для выделенной учетной записи;
- Логин для авторизации;
- Номер телефона, опция является опциональной;
- Кода ваучера;
- Опциональные категории, которые могут быть применимы для верной идентификации;
- Срок истечения учетной записи;
- Лимит числа устройств;
- Выбор местоположения для системы WNAM 2.

После указания достаточной информации, следует нажать на кнопку "Создать". После создания, учетные записи становятся доступными сразу после создания.

RADIUS-атрибуты

RADIUS атрибуты (Remote Authentication Dial-In User Service) используются для определения некоторых элементов проверки подлинности, авторизации и учета (AAA) в профиле пользователя, который хранится в управляющей программе RADIUS.

Обмен данными между сервером RADIUS и клиентом RADIUS осуществляется в RADIUS-пакеты. Поля данных передаются слева направо. Ниже представлены поля в пакете RADIUS.



Каждый пакет RADIUS содержит следующую информацию:

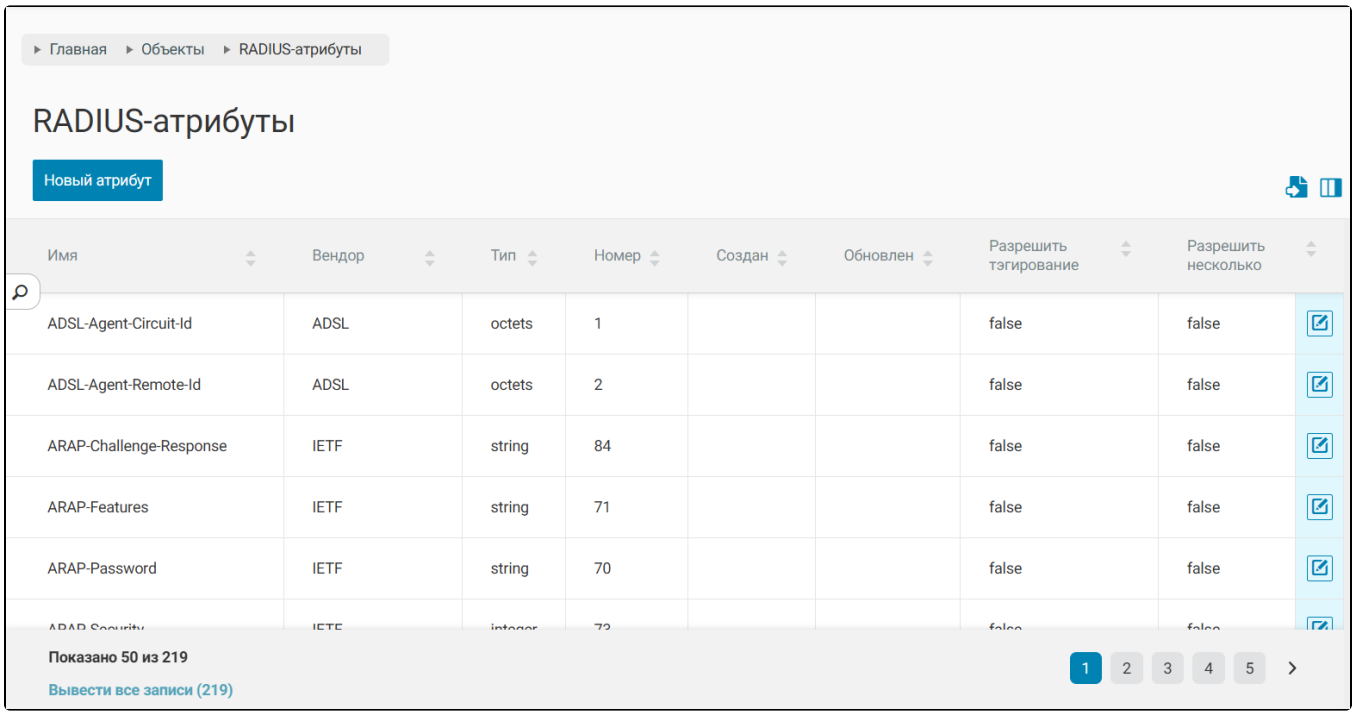
- Код - поле кода равно одному октет, он идентифицирует один из следующих типов пакетов RADIUS:
  - запрос доступа;
  - доступ-прием;
  - отказ от доступа;
  - бухгалтерский запрос;
  - бухгалтерский учет;
- Идентификатор — идентификатор поле - один октет (помогает серверу RADIUS сопоставлять запросы и ответы, а также обнаруживать повторяющиеся запросы);
- Длина - поле длины равно два октета (определяет длину всего пакета);
- Аутентификатор - поле аутентификатора составляет 16 октетов (передается самый значимый октет - первый октет, он используется для проверки подлинности ответа с сервера RADIUS). Существует два типа аутентификаторов:
  - проверка подлинности запроса (доступно в пакетах Access-Request и Accounting-Request);
  - Response-Authenticator (доступно в режимах «Доступ-принять», «Отклонить доступ», «Запросить-доступ» и пакеты «Учет-ответ»).

Существуют следующие типа пакетов RADIUS:

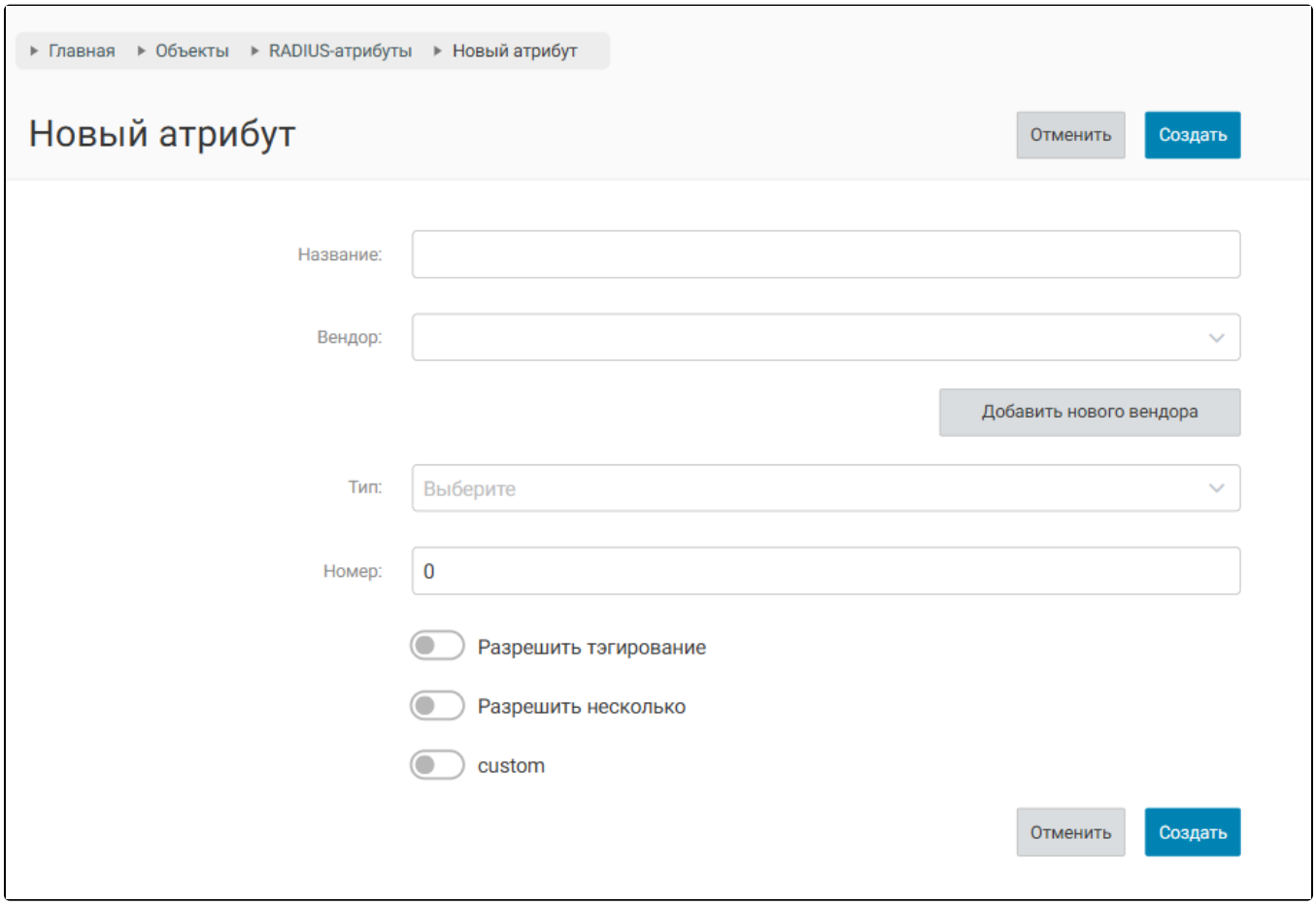
- Access-Request — отправляется от клиента на сервер RADIUS. Пакет содержит информацию, которая позволяет RADIUS-серверу определить, следует ли разрешить доступ к определенному серверу доступа к сети (NAS), который разрешает доступ пользователю. Любой пользователь, выполняющий проверку подлинности, должен отправить пакет Access-Request. После получения пакета Access-Request RADIUS-сервер должен переслать ответ.
- Access-Accept — как только RADIUS-сервер получает пакет Access-Request, он должен отправить пакет Access-Accept, если все значения атрибутов в пакете Access-Request приемлемы. Пакеты Access-Accept предоставляют сведения о конфигурации, необходимые клиенту для предоставления услуг пользователю.
- Access-Reject — как только RADIUS-сервер получает пакет Access-Request, он должен отправить пакет Access-Eject, если какое-либо из значений атрибута не является приемлемым.
- Access-Challenge — как только сервер RADIUS получает пакет Access-Accept, он может отправить клиенту пакет Access-Challenge, который требует ответа. Если клиент не знает, как реагировать, или если пакеты недействительны, RADIUS-сервер отбрасывает пакеты. Если клиент отвечает на пакет, новый пакет Access-Request должен быть отправлен вместе с исходным пакетом Access-Request.
- Accounting-Request — отправляется от клиента на сервер учета RADIUS, который предоставляет бухгалтерскую информацию. Если RADIUS-сервер успешно записывает пакет Accounting-Request, он должен отправить пакет Accounting Response.
- Accounting-Response — отправляется сервером учета RADIUS клиенту для подтверждения того, что запрос на учет был получен и успешно записан.

Типы файлов, используемых RADIUS важны для передачи аутентификационной информации от клиента к серверу. Каждый файл определяет уровень аутентификации или авторизации для пользователя: файл словаря определяет, какие атрибуты может реализовать NAS пользователя; файл clients определяет, каким пользователям разрешено делать запросы к RADIUS-серверу; пользовательские файлы определяют, какой пользователь запрашивает проверку подлинности RADIUS-сервера на основе данных безопасности и конфигурации.

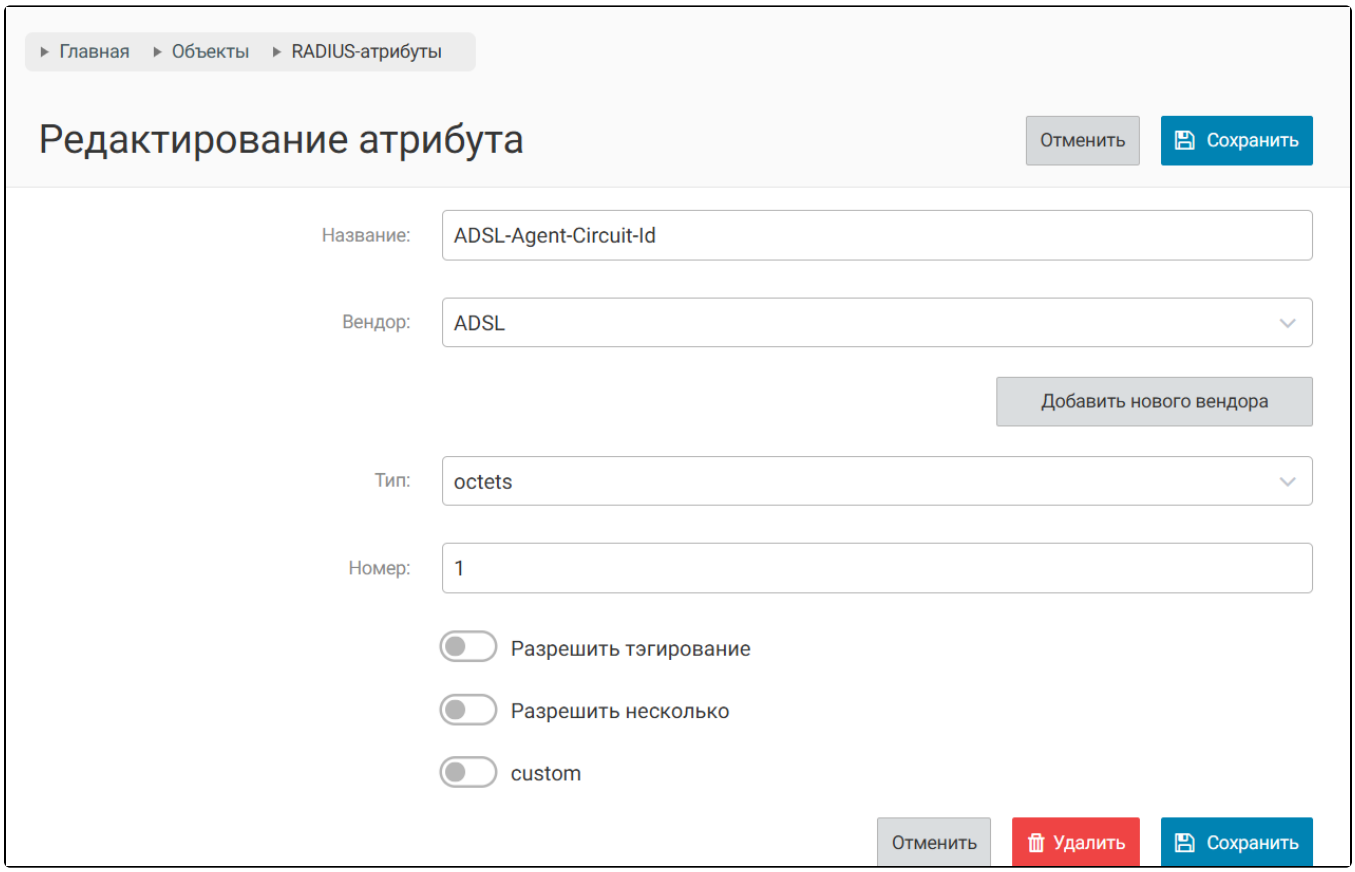
Для создания RADIUS атрибута необходимо перейти в раздел "Объекты" "RADIUS атрибуты". В данном разделе отображается список созданных атрибутов.



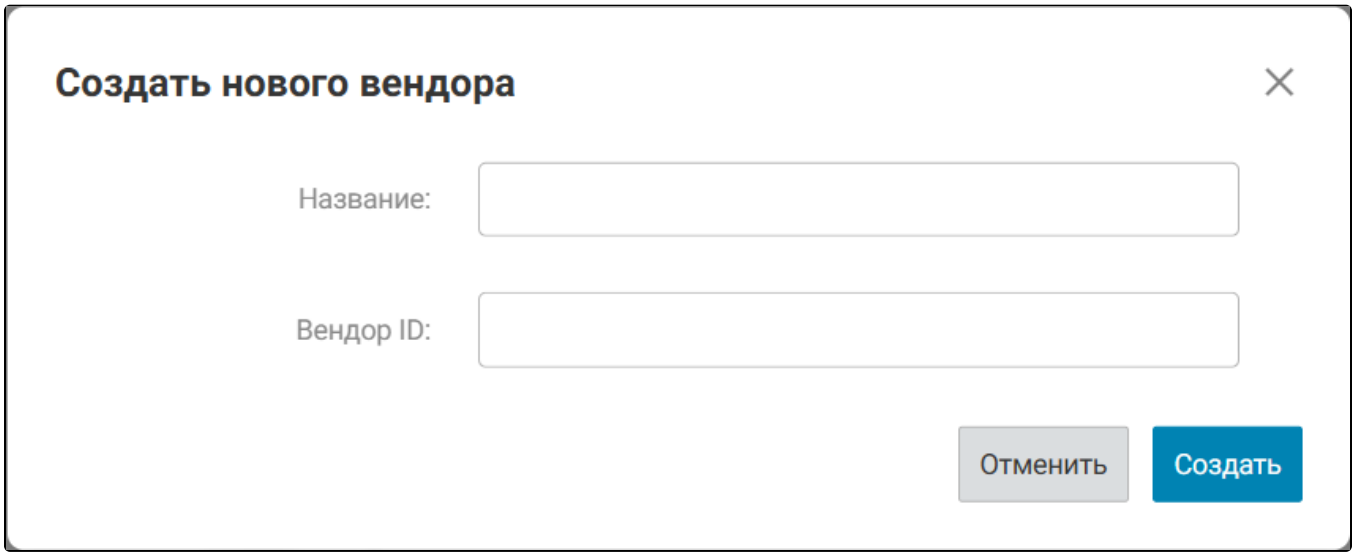
Для создания нового атрибута необходимо нажать кнопку "Новый атрибут" и заполнить соответствующие поля, после чего нажать кнопку "Сохранить изменения".



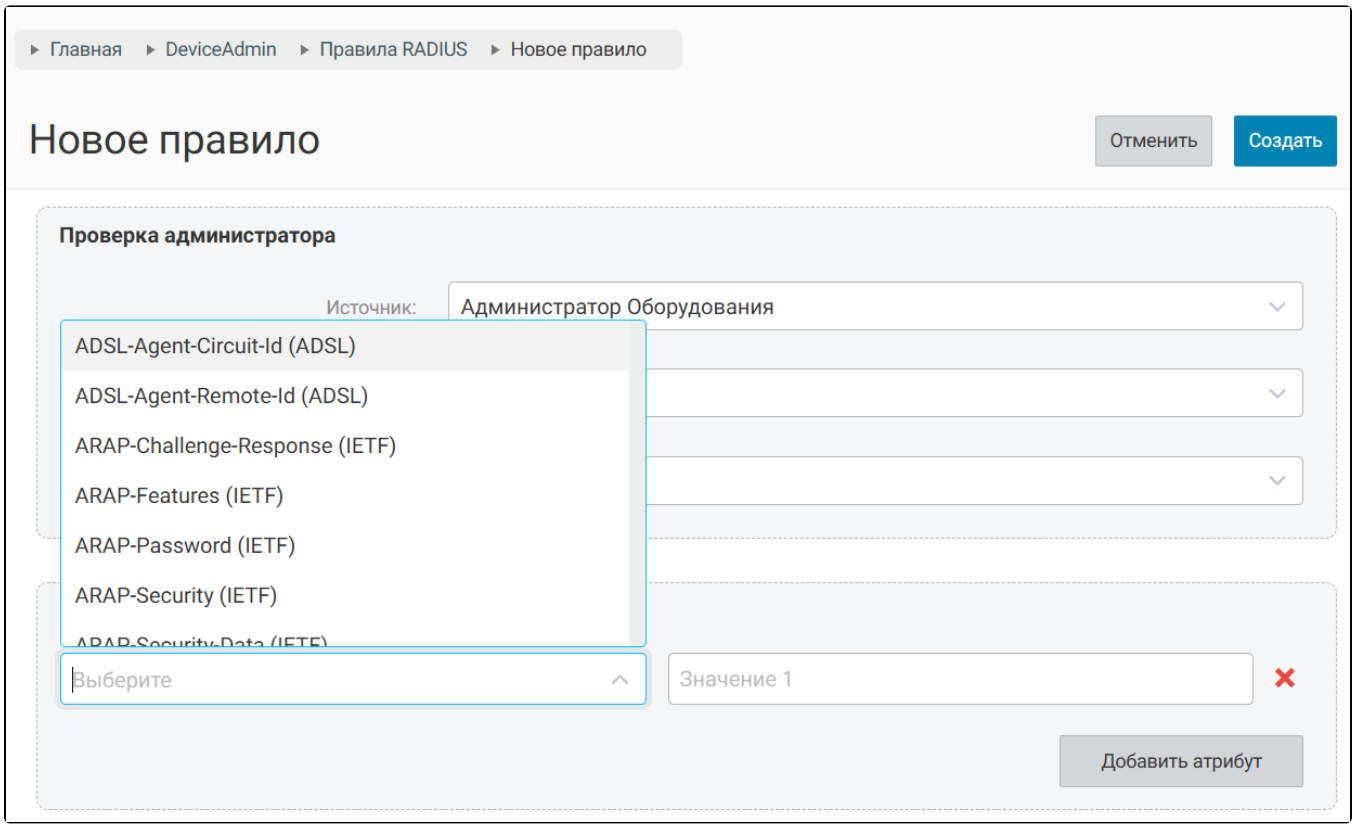
Для просмотра параметров уже созданного атрибута необходимо нажать левой кнопкой мыши на контекстное меню атрибута из списка.



Для создания нового вендора необходимо нажать кнопку "Добавить нового вендора" и заполнить соответствующие поля, после чего нажать кнопку "Создать".



После создания RADIUS-атрибута возможно использование в различных разделах системы WNAM 2. Например, в создании RADIUS правил ("Доступ к оборудованию" – "Правила RADIUS"):


Главная
DeviceAdmin
Правила RADIUS
Новое правило
Новое правило
Отменить
Создать
Проверка администратора
Источник:
Администратор Оборудования
ADSL-Agent-Circuit-Id (ADSL)
ADSL-Agent-Remote-Id (ADSL)
ARAP-Challenge-Response (IETF)
ARAP-Features (IETF)
ARAP-Password (IETF)
ARAP-Security (IETF)
Выберите
Значение 1
Добавить атрибут

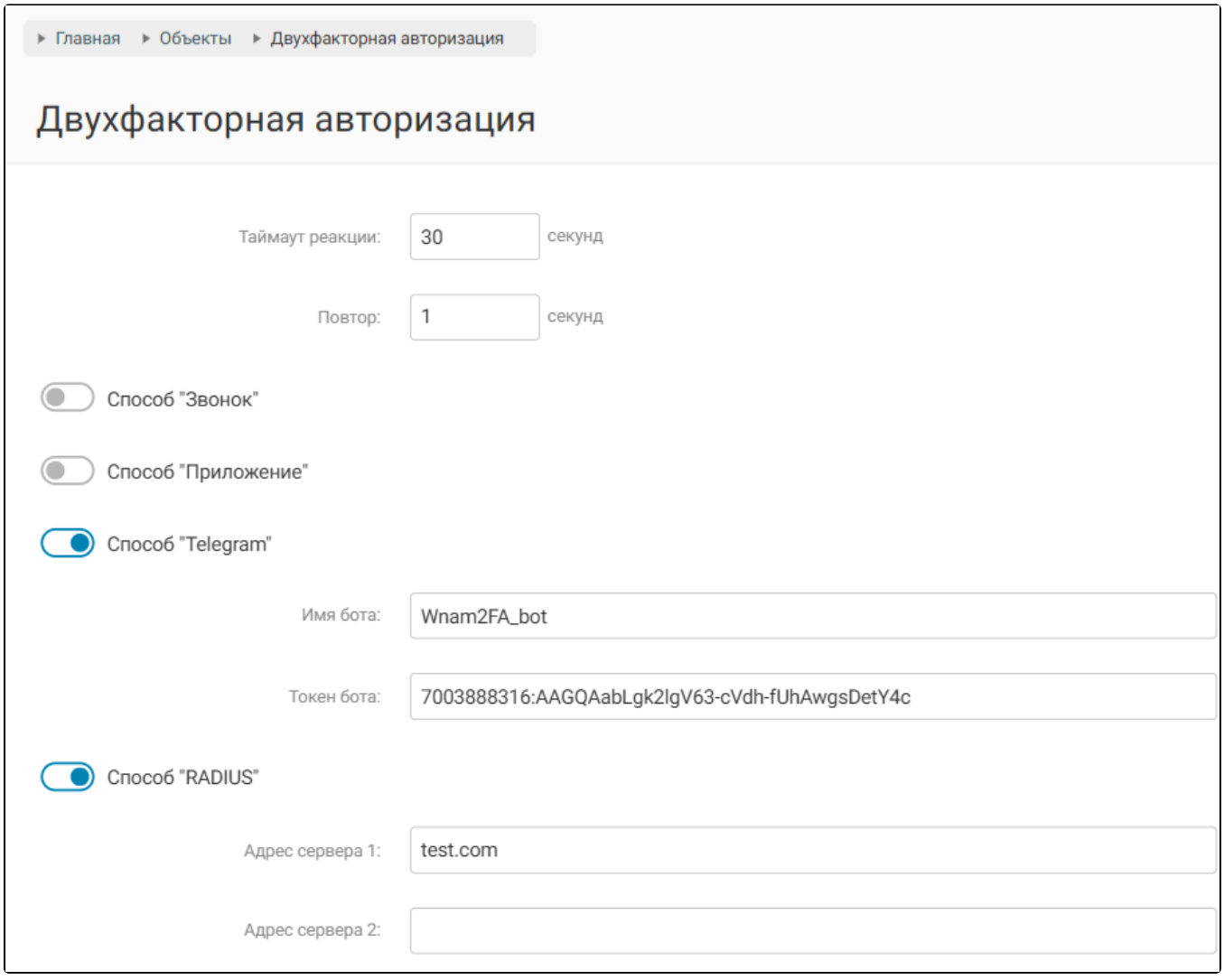
Двухфакторная авторизация

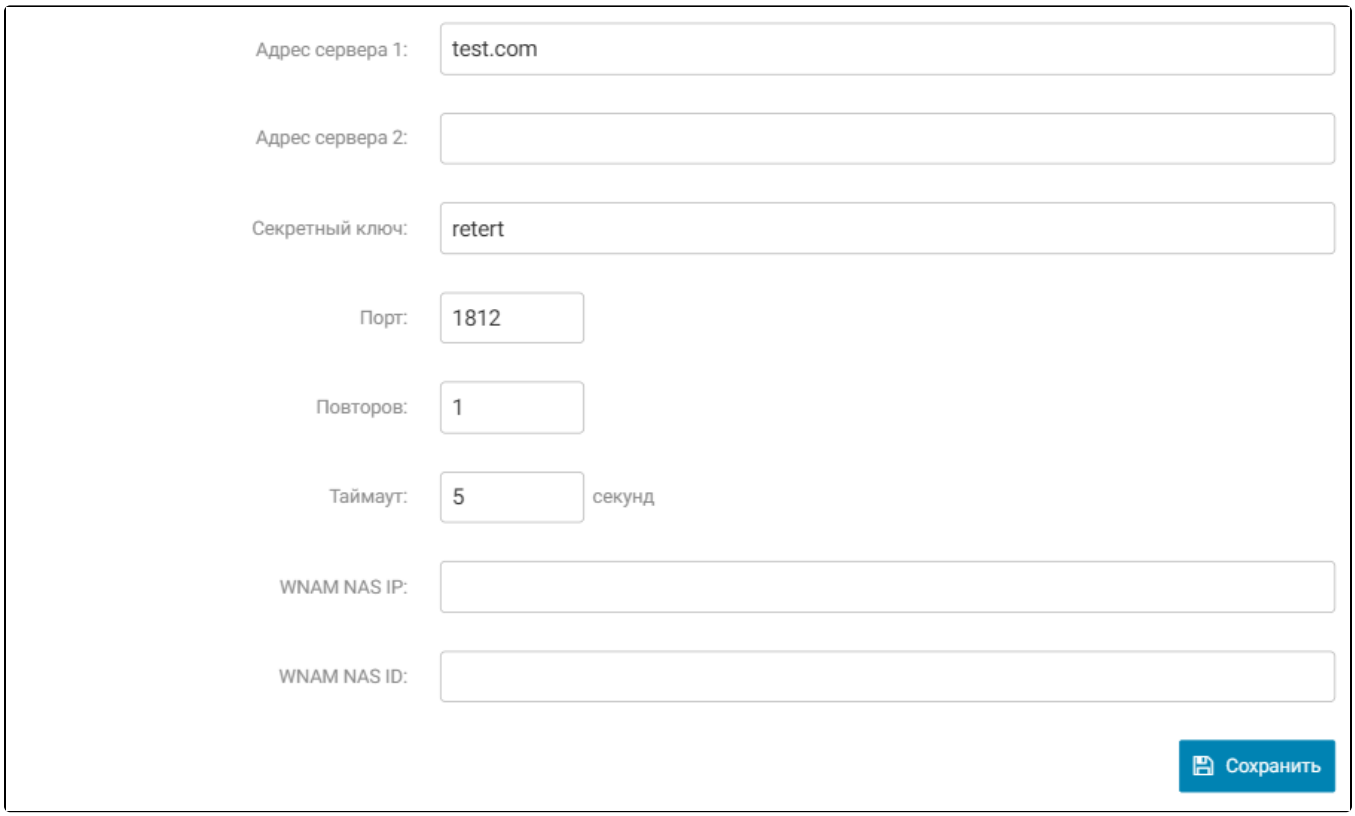
При необходимости в расширенной авторизации можно задействовать методы двухфакторной авторизации. Данный метода позволяет обеспечить дополнительную защиту при этом оставляя простоту для клиентов. В данный момент системой поддерживается следующие методы двухфакторной авторизации:

- Способ "Звонок". Позволяет делать звонок-авторизацию, при котором необходимо указать пин код в принимаемом звонке;
- Способ "Приложение". Гибкое решение при создании нативного корпоративного приложения у компании заказчика;

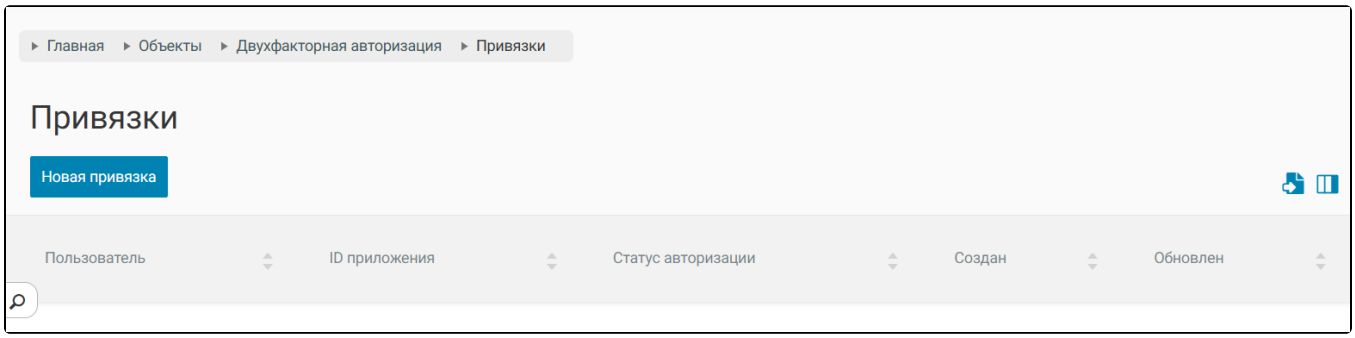
> ⚠ Важно учитывать, что при таком методе, ответственность и поддержка в подавляющем большинстве остается за заказчиком, так как неизвестно, каким образом будет построено нативное приложение.

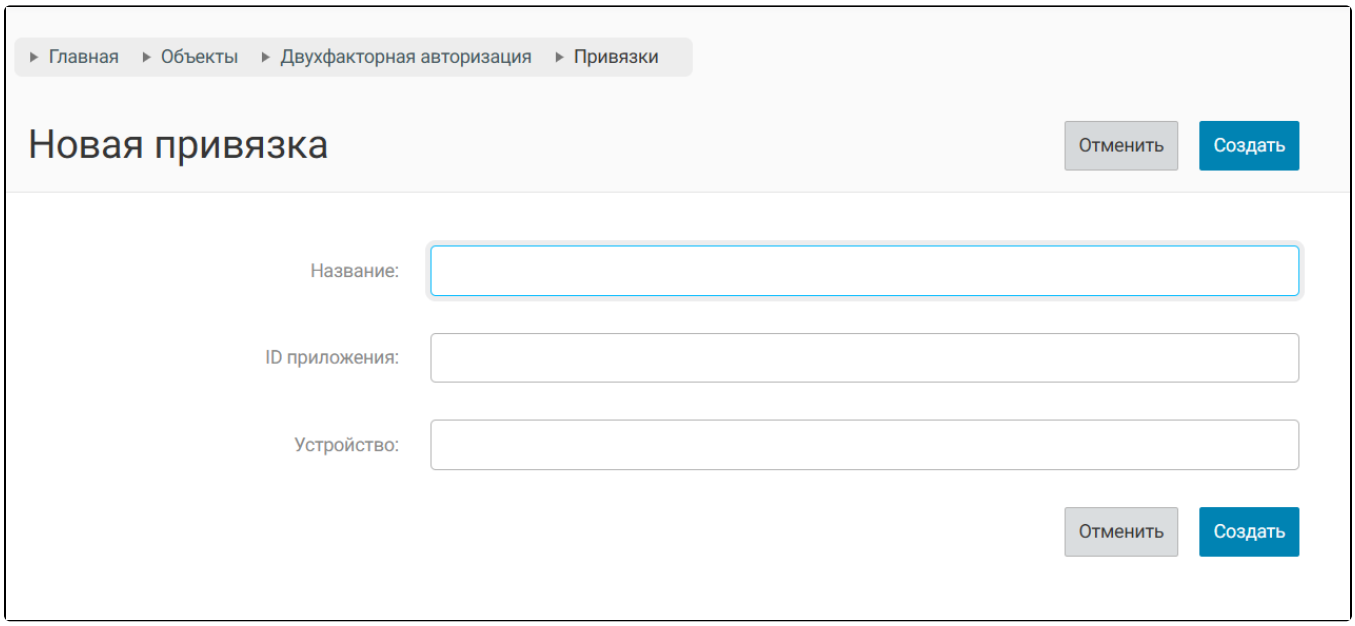
- Способ "Telegram". В данном методе клиенту необходимо указать пин код от телеграмм бота. Документацию по разработке телеграмм бота требуется уточнять на официальном сайте Telegram;
- Способ "RADIUS". Данный способ разрешает авторизацию благодаря RADIUS атрибутам. Необходимо указать адреса серверов, ключ, порт, количество повторов, таймаут, WNAM NAS IP и WNAM NAS ID.





Также возможно самостоятельно привязать какое либо приложение. Для этого необходимо перейти в подраздел "Привязки" – "Новая привязка". Далее, необходимо указать, наименование, ID приложения и устройство.




Главная
Объекты
Двухфакторная авторизация
Привязки
Новая привязка
Отменить
Создать
Название:
ID приложения:
Устройство:
Отменить
Создать

Уведомления

Система WNAM 2 поддерживает отправку уведомлений (нотификаций) о событиях в работе модуля корпоративной авторизации во внешние системы по протоколам Syslog и SNMP. В настоящий момент поддерживаются следующие типы (условия срабатывания) событий:

- Событие аудита (событие аудита - логин либо логаут интерфейса администратора, создание, изменение либо модификация (почти любого) объекта конфигурации;
- Событие NAC (событие эндпоинта - авторизация (успешная или нет) гостевого или корпоративного устройства (MAC адреса));
- Событие администрирования оборудования (событие TACACS+ логина на оборудование, а также факт ввода команды);
- Событие службы каталогов (событие сервиса-коннектора со службой каталогов Active Directory);
- Событие службы сертификатов (событие при выдаче сертификатов, регистрации центра сертификации).

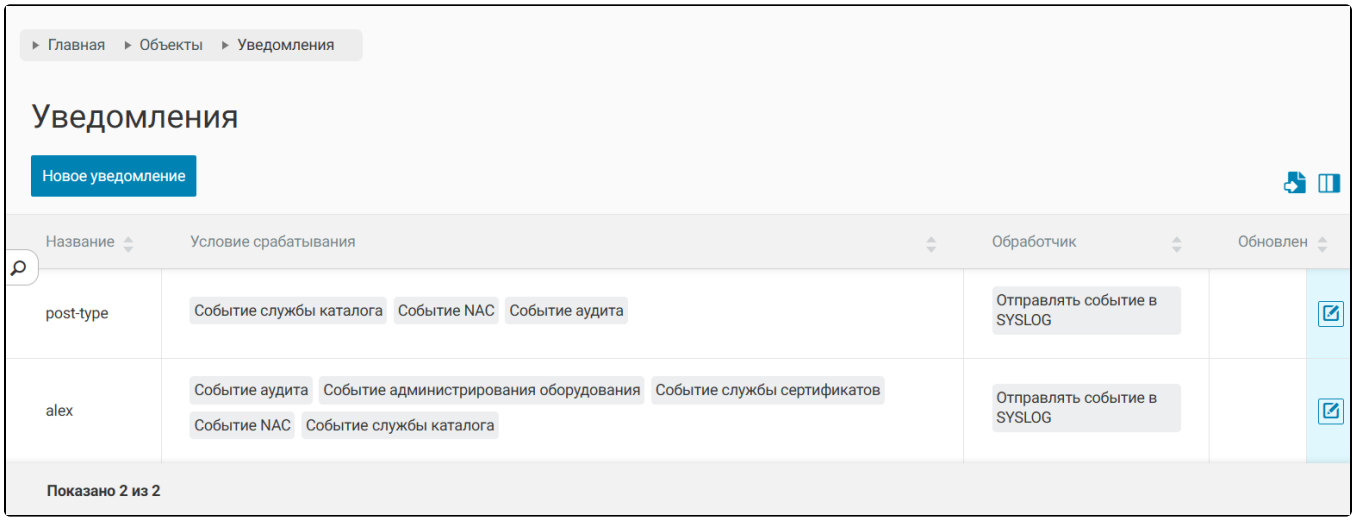
Основной задачей обновленного механизма уведомлений является отправка событий авторизации в систему SIEM предприятия.

Отправка уведомлений возможна по протоколам:

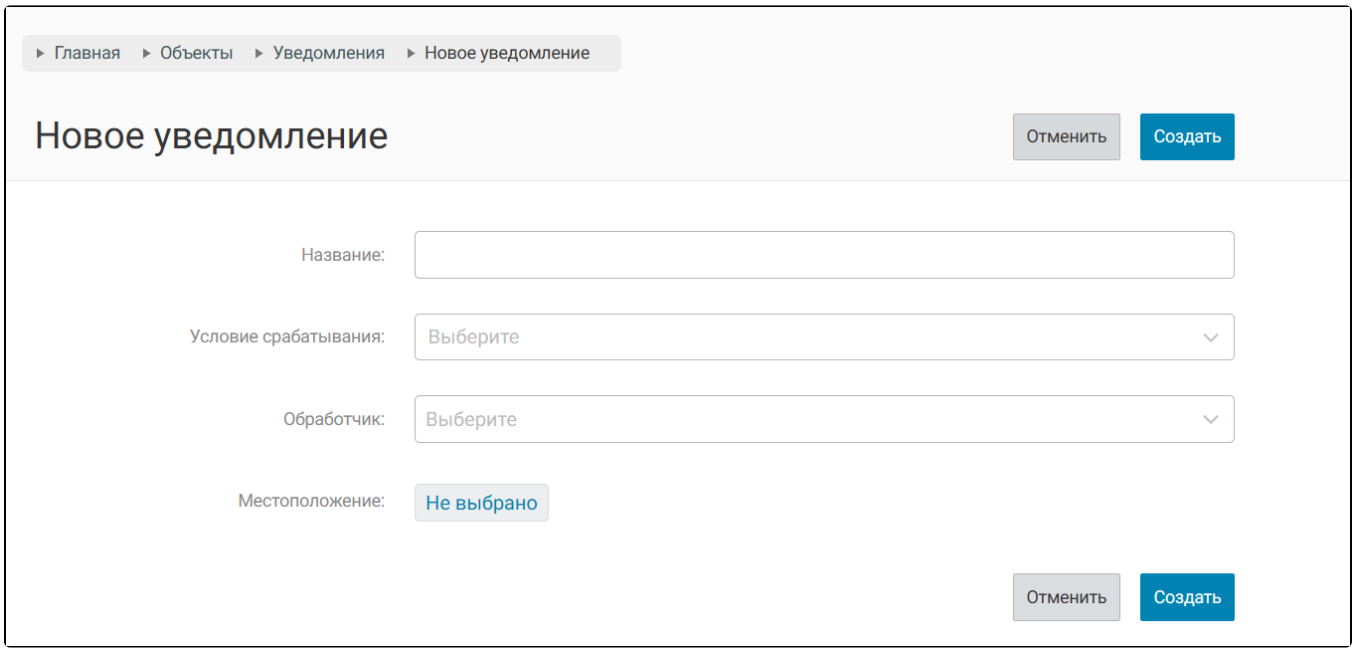
- Syslog в соответствии с RFC 5424 на TCP или UDP порт 514 (либо произвольный);
- SNMP Trap в соответствии с RFC 3416 на UDP порт 162 (версия 2c).

Если вам требуется поддержка отправки уведомлений по Syslog/TLS, SNMPv3, реакция на другие типы событий, расширение информации по имеющимся типам, вам следует обратиться в службу технической поддержки по адресу support@netams.com

Механизм формирования уведомлений по событиям корпоративной авторизации расширяет имеющийся в системе WNAM модуль Нотификаций. Можно одновременно создавать несколько получателей сообщений по разным протоколам и разного типа. Система не ограничивает число получателей уведомлений, но важно понимать помнить, что их отправка (особенно в нагруженной среде) потребляет ресурсы. Для настройки отправки уведомления следует перейти в раздел "Объекты" "Уведомления" и нажать на кнопку "Новое уведомление", в результате чего откроется окно, позволяющее создать уведомление.

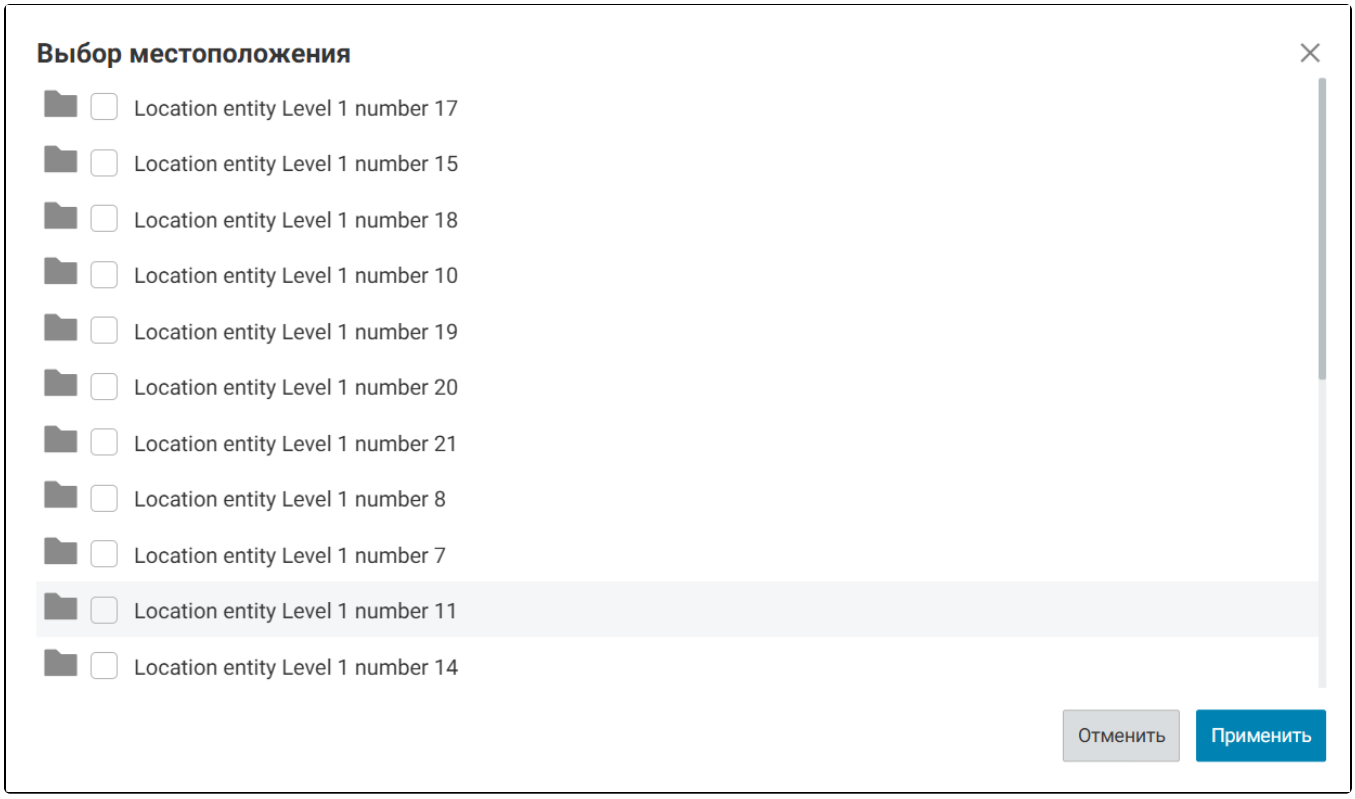


Здесь необходимо ввести требуемые данные в трёх вкладках.

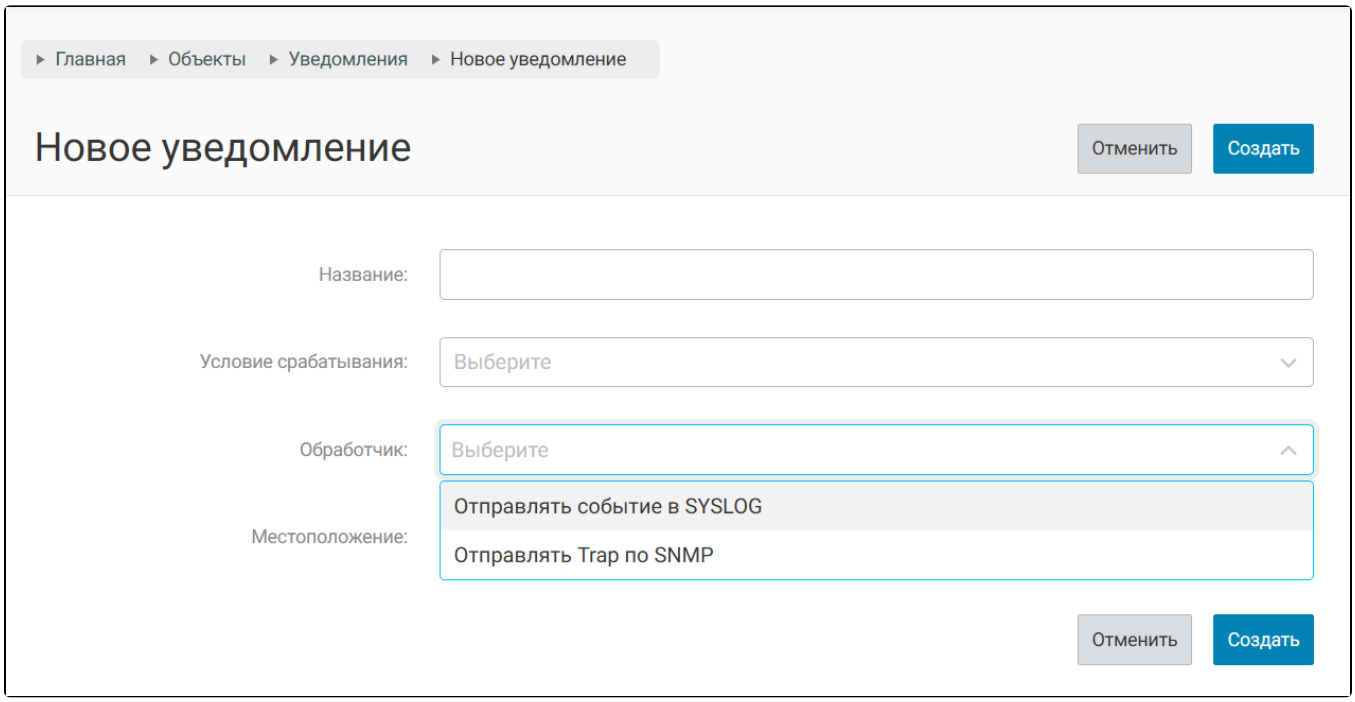


В окне создания нотификации следует указать название обработчика (получателя) уведомления, а также одно из пяти условий срабатывания событий (можно указать все, или несколько).

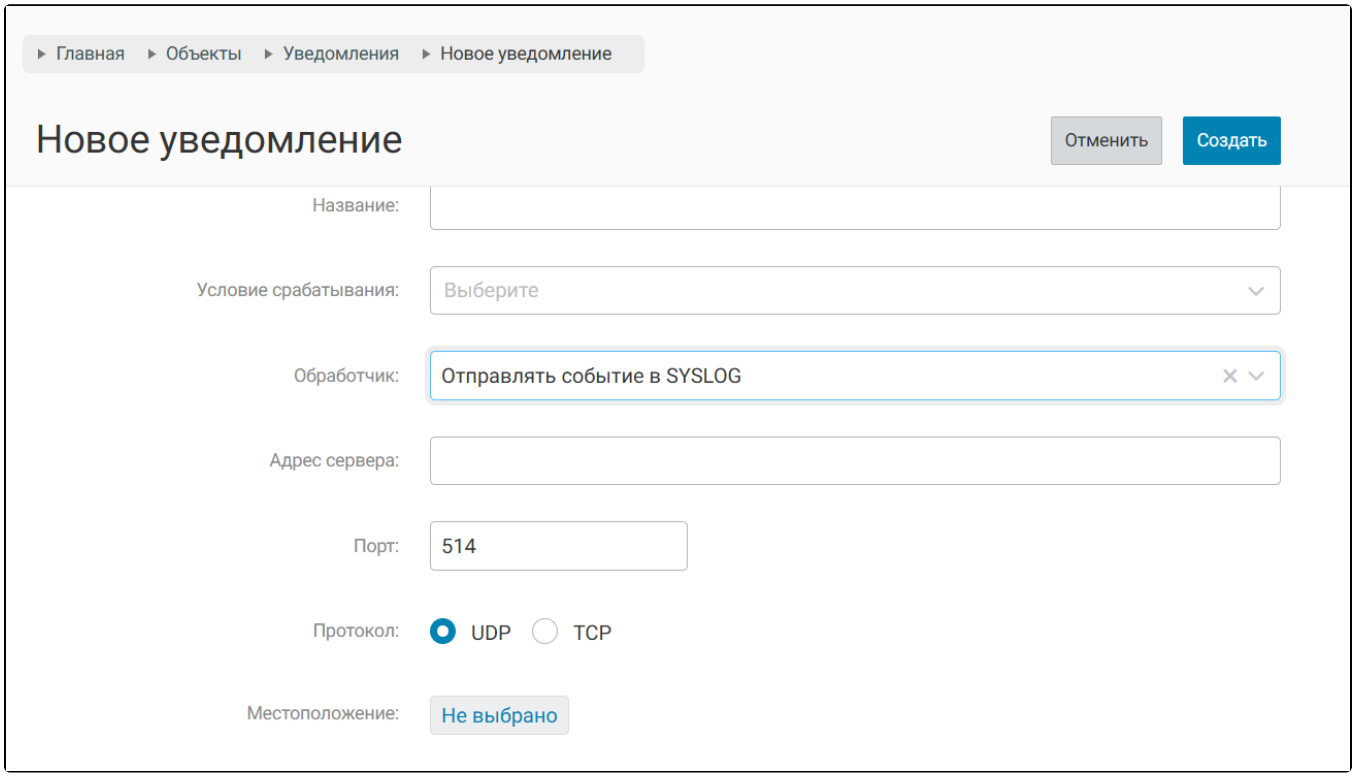
В четвертом окне создания уведомления следует отметить необходимое местоположение.



В третьей вкладке следует выбрать тип обработчика и его параметры (для SNMP-уведомления следует выбрать "Отправить Trap по SNMP).



Для Syslog-уведомления следует выбрать "Отправлять событие в SYSLOG".



Можно задать адрес получателя Syslog-сообщений с указанием нестандартного порта, а также выбрать протокол (TCP, UDP).

Затем следует сохранить изменения нажатием на кнопку "Создать". Созданное уведомление можно открыть, и провести тестовый запуск.

При наступлении соответствующего события в модуле корпоративной авторизации система WNAM 2 передаст информацию о событии в специальную очередь нотификаций, из которой все события будут обработаны и направлены по заданным каналам-получателям. При этом в лог-файле **wnam.log** появятся записи о такой отправке:

```
11:58:38.184 DEBUG [NotificationService.java:244] - Execute notification 'snmp1', handler SNMP,
event type ENDPOINT_EVENT, object: {FAIL;48:FD:A3:75:C8:F4;PAP;not-allowed-pap-mac-state}
11:58:38.184 DEBUG [NotificationService.java:320] - Notification SNMP type ENDPOINT_EVENT to:
1.1.1.1 on: {AccessServer=hAP [R20 Mikrotik LAB], AuthState=FAIL, AuthenticationProfile=,
AuthorizationProfile=Default reject, FailReason=not-allowed-pap-mac-state, Identity=48:FD:A3:75:
C8:F4, MAC=48:FD:A3:75:C8:F4, Method=PAP, NasAddress=hap, RemoteIp=10.130.129.66, SiteName=change
address ZZZ, Timestamp=06.02.2023 11:58:38, Type=ENDPOINT_EVENT, TypeStr= }

11:58:38.186 DEBUG [NotificationService.java:244] - Execute notification 'syslog1', handler
SYSLOG, event type ENDPOINT_EVENT, object: {FAIL;48:FD:A3:75:C8:F4;PAP;not-allowed-pap-mac-state}
11:58:38.186 DEBUG [NotificationService.java:375] - Notification SYSLOG type ENDPOINT_EVENT to:
1.1.1.1 on: {AccessServer=hAP [R20 Mikrotik LAB], AuthState=FAIL, AuthenticationProfile=,
AuthorizationProfile=Default reject, FailReason=not-allowed-pap-mac-state, Identity=48:FD:A3:75:
C8:F4, MAC=48:FD:A3:75:C8:F4, Method=PAP, NasAddress=hap, RemoteIp=10.130.129.66, SiteName=change
address ZZZ, Timestamp=06.02.2023 11:58:38, Type=ENDPOINT_EVENT, TypeStr= }
```

Для Syslog-нотификаций мы старались реализовать формат, максимально совместимый с исходным форматом Common Event Format, описанным в этом документе.

Следующее поле - тип события:

Тип события	Описание события
TACACS_EVENT	Событие подсистемы администрирования оборудования: аутентификация доступа, авторизация доступа, авторизация команды
AUDIT_EVENT	События подсистемы аудита: авторизация в административном веб-интерфейсе WNAM 2, изменение конфигурационных объектов
ADC_EVENT	Событие модуля взаимодействия со службой каталога: статус коннектора
ENDPOINT_EVENT	Событие подсистемы авторизации сетевого доступа: авторизация эндпоинта

Следующее поле - название события, например "Событие эндпоинта"

Следующее поле - важность (severity)

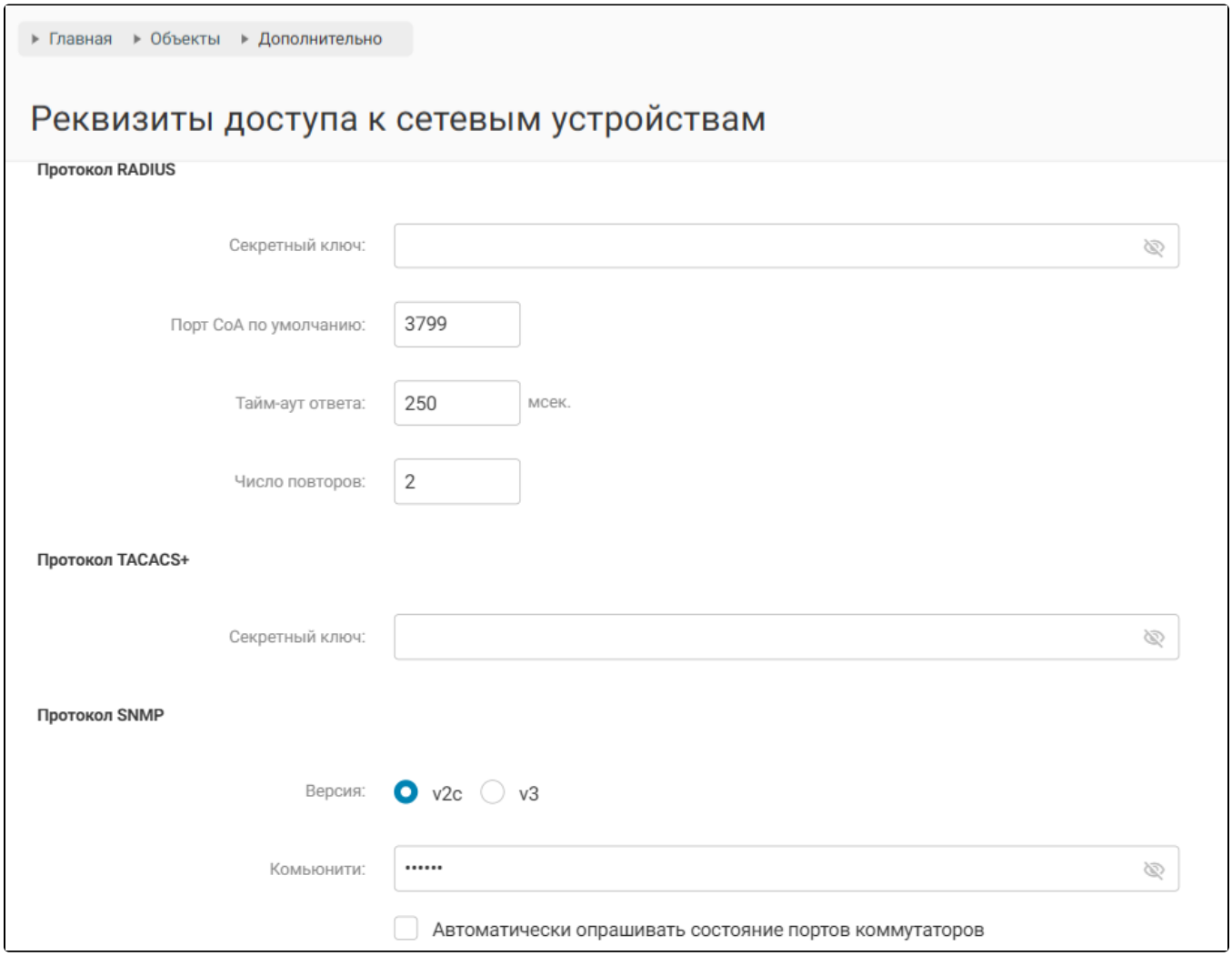
В зависимости от типа события, далее идет список пар "ключ=значение", описывающих детали события, в соответствии с этой таблицей:

Параметр	Описание
act	Результат авторизации эндпоинта, Authenticated или Rejected
app	Метод авторизации, например PAP или EAP_PEAP
smac	MAC адрес эндпоинта
suser	Identity эндпоинта
src	IP адрес эндпоинта
externalId	Идентификатор сессии аккаунтинга
cs1	Имя профиля аутентификации
cs2	Имя профиля авторизации
cs3	Имя сервера доступа (NAS)
dst	IP адрес сервера доступа (NAS)
cs4	Идентификатор сервера доступа (NAS)
cs5	Название площадки
message	Некоторые остальные параметры из записи о сессии аутентификации, разделитель ;

Дополнительные настройки

Реквизиты доступа к сетевым устройствам

В данном разделе можно отредактировать общее правило применяемых секретных ключей для различных протоколов подключения, такие как: RADIUS, TACACS+ и протокол SNMP.



Протокол RADIUS.

При необходимости, возможно настроить секретный ключ, порт CoA по умолчанию, тайм-аут ответа и число повторов.

Протокол TACACS+

В данном подразделе можно настроить секретный ключ по умолчанию.

Протокол SNMP

Здесь находится используемая версия по умолчанию, секретный ключ по умолчанию с возможностью автоматически опрашивать состояние портов коммутаторов.

Диагностика

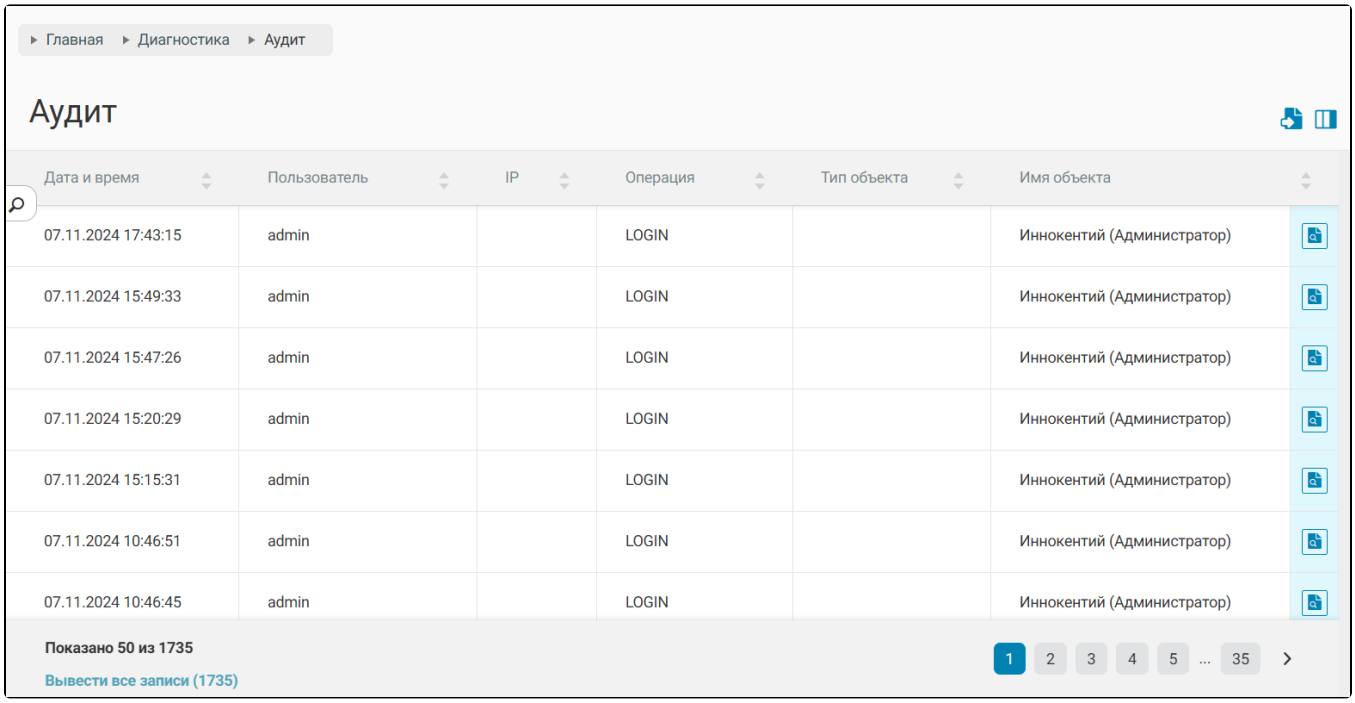
Раздел "Диагностика" интерфейса администратора системы WNAM 2 позволяет обеспечить мониторинг и траблшутинг. В разделе "Диагностика" доступны следующие данные по мониторингу работы системы:

- Аудит;
- Кластер;
- Системные события;
- Захват трафика;
- Логи.

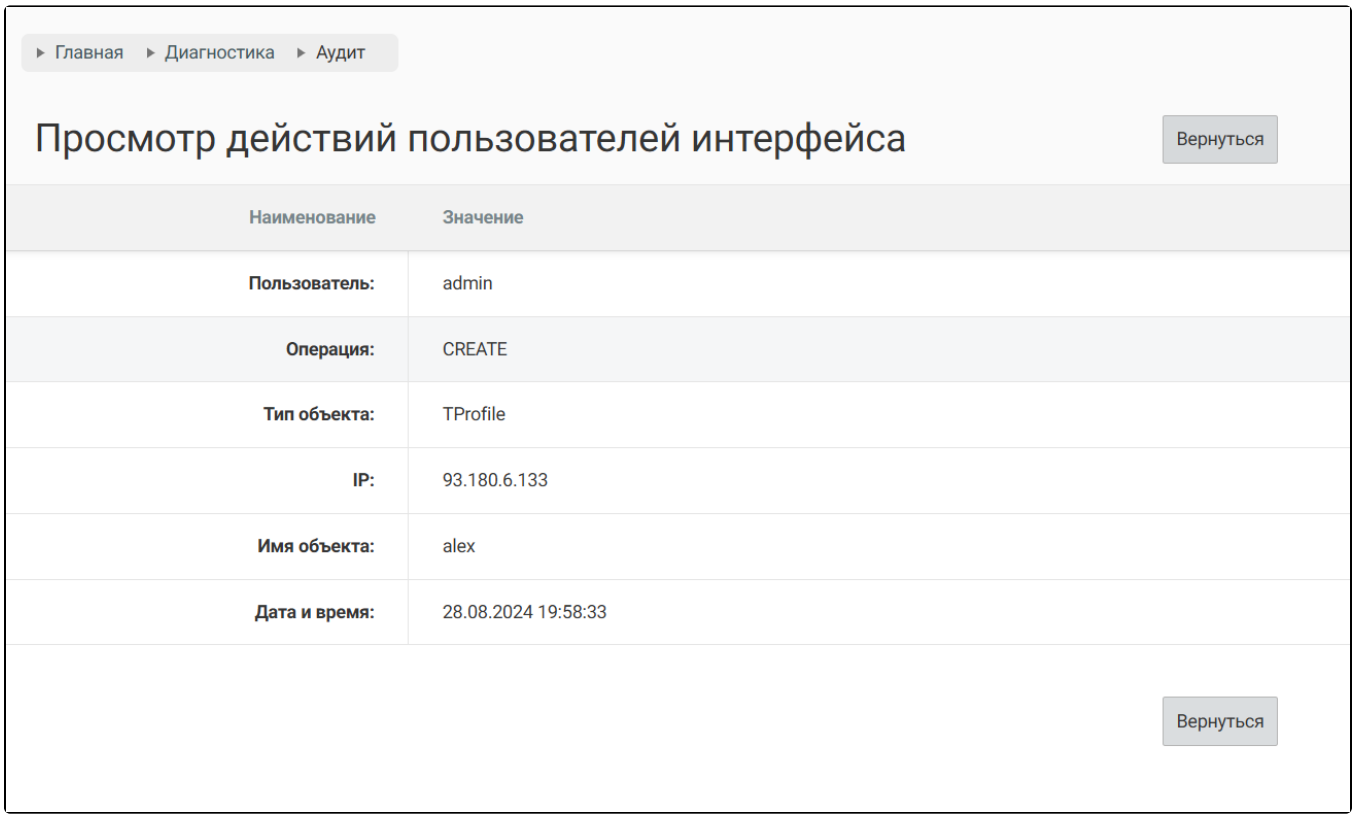
Детальная информация по каждому виду мониторинга представлена в соответствующих разделах.

Аудит

Раздел аудита позволяет отобразить все действия пользователей веб-интерфейса системы WNAM 2 (администраторов, менеджеров) по логину и по созданию/изменению/удалению объектов различного типа. Для того, чтобы просмотреть статистику действий пользователя необходимо перейти в раздел "Диагностика" "Аудит". В открывшемся окне будут доступны записи по каждому пользователю., отображающие имя пользователя, совершенную операцию, время операции, IP-адрес устройства, тип и имя объекта. Система WNAM предоставляет возможность фильтрации по времени, за которое необходимо просмотреть информацию, а также поиск по ряду полей таблицы.

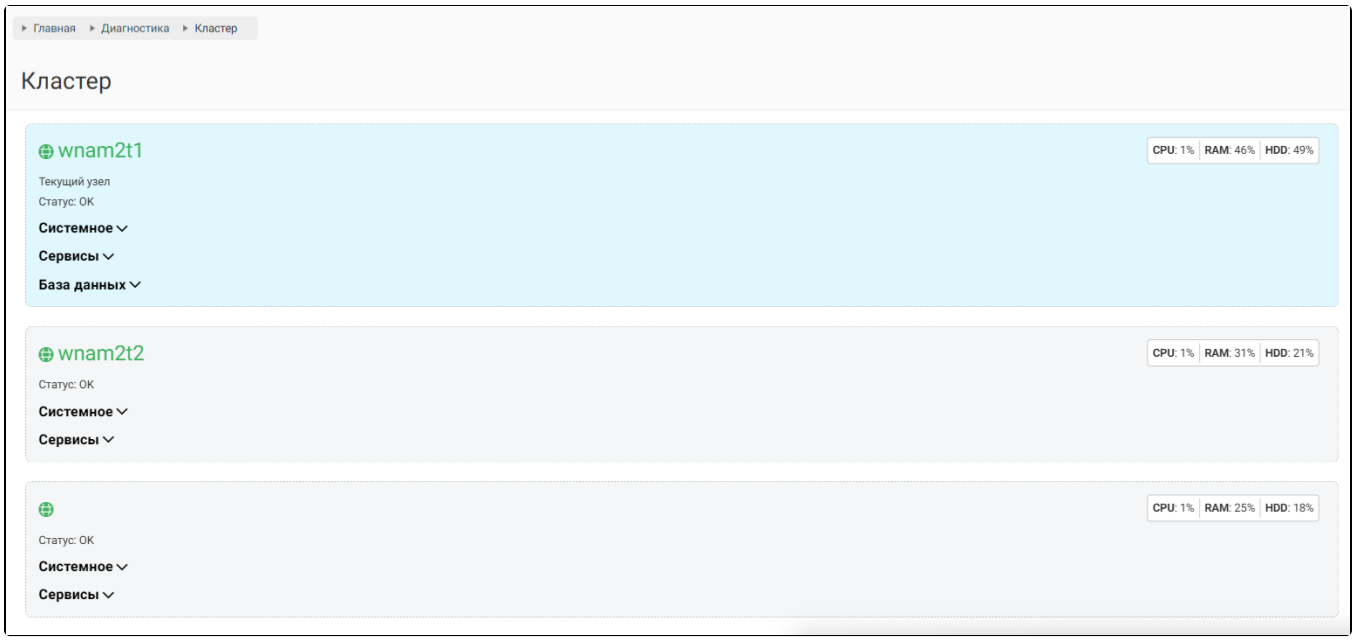


Также, при необходимости, возможно открыть в окне ту или иную запись для детальной информации. Для этого, напротив требуемой записи необходимо открыть контекстное меню с описанием записи:


Главная
Диагностика
Аудит
Просмотр действий пользователей интерфейса
Вернуться
Наименование
Значение
Пользователь:
admin
Операция:
CREATE
Тип объекта:
TProfile
IP:
93.180.6.133
Имя объекта:
alex
Дата и время:
28.08.2024 19:58:33
Вернуться

Кластер

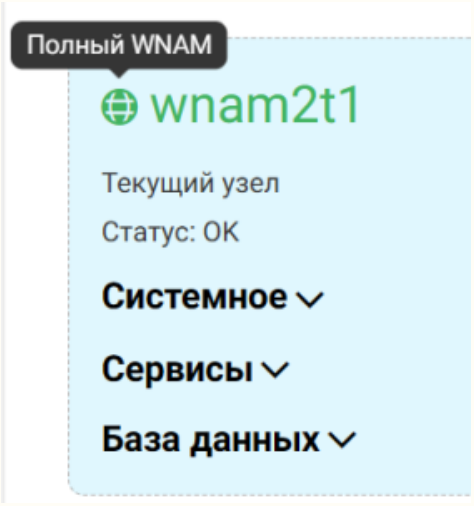
Чтобы просмотреть информацию о подключенных кластерах, достаточно перейти в раздел "Диагностика" – "Кластер". В этом разделе собрана вся статистическая информация, показатели нагрузки, статус и другие свойства, которые будут описаны ниже.

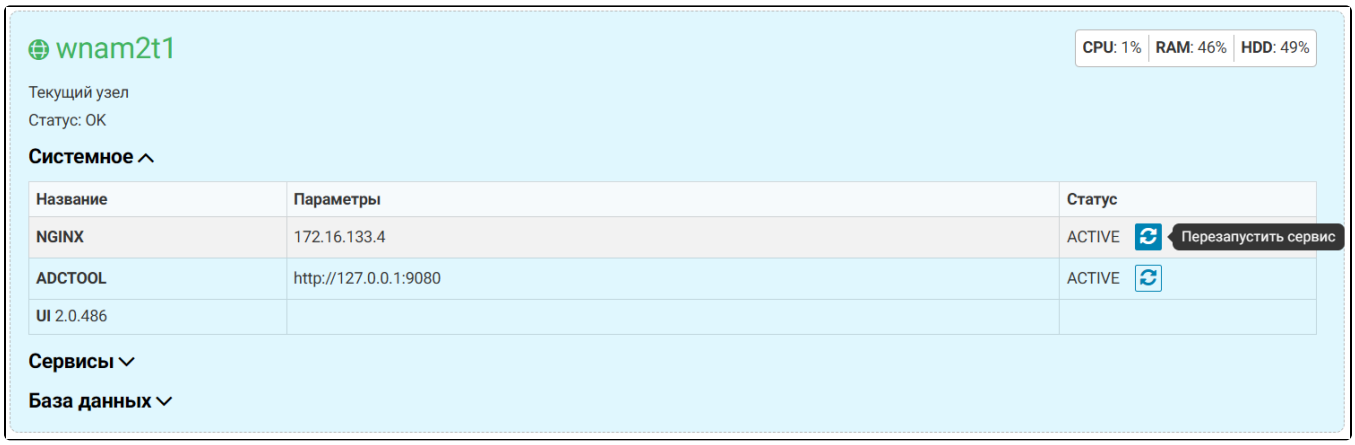


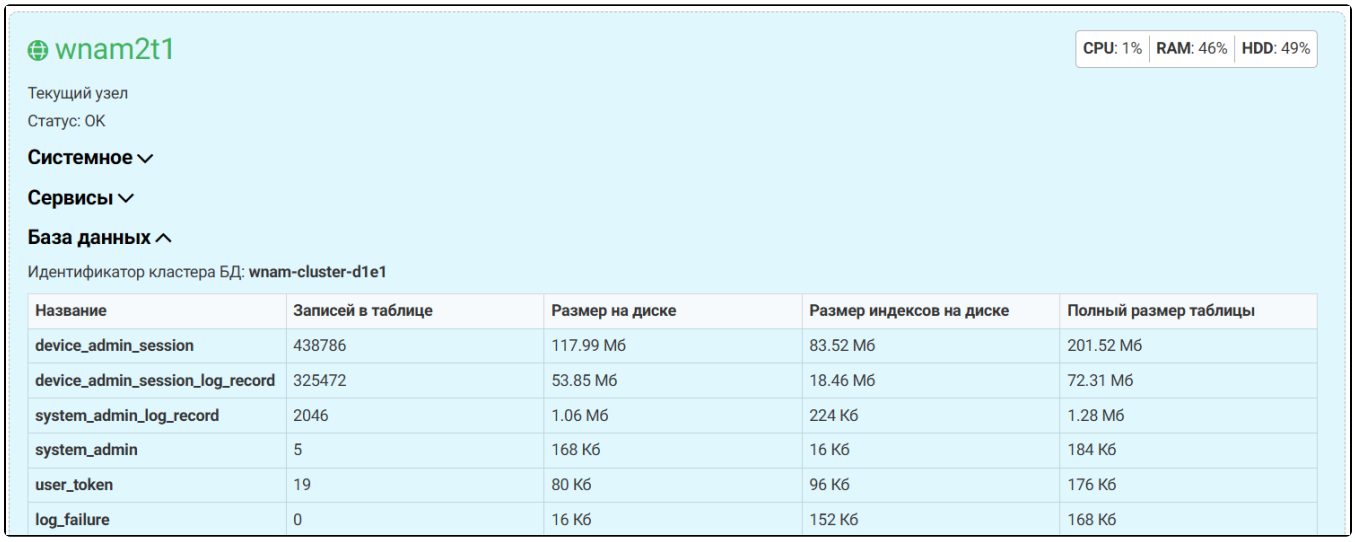
Первым всегда отображается тот кластер, который используется. У каждого кластера (узла) можно просмотреть какие процессы запущены (Системные и сервисы, у кластера, который используется также отображается используемая база данных) и при необходимости также присутствует возможность перезапустить тот или иной сервис. Для этого, необходимо открыть требуемый раздел и в таблице выбрать сервис после чего нажать на кнопку перезапуска.

Текущий узел всегда отображается цветовым обозначением и всегда находится на первой позиции.

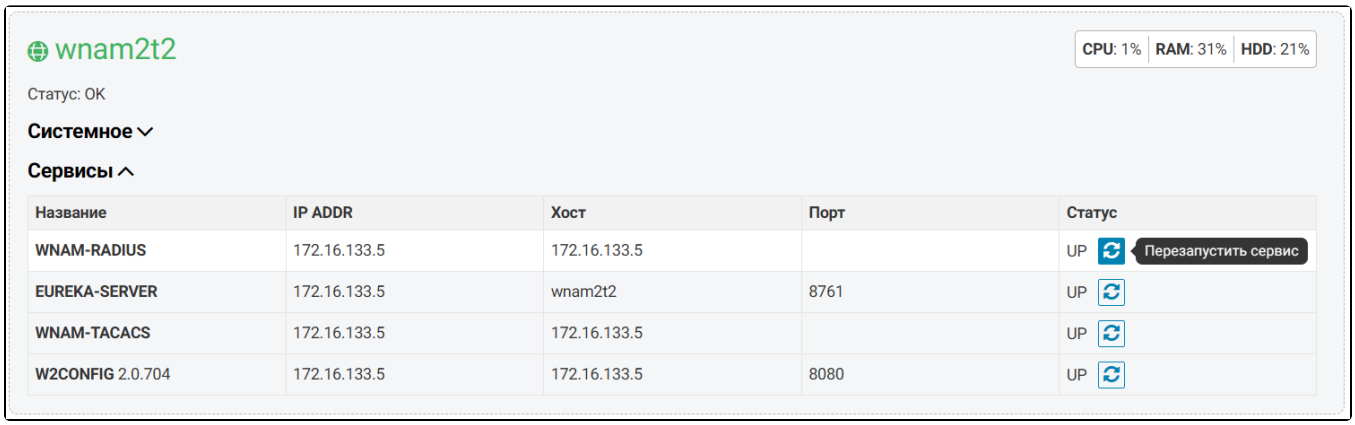
Если на тот или иной кластер была установлена система WNAM 2, то возле названия кластера будет отображаться соответствующий значок с подсказкой при наведении курсора мыши.







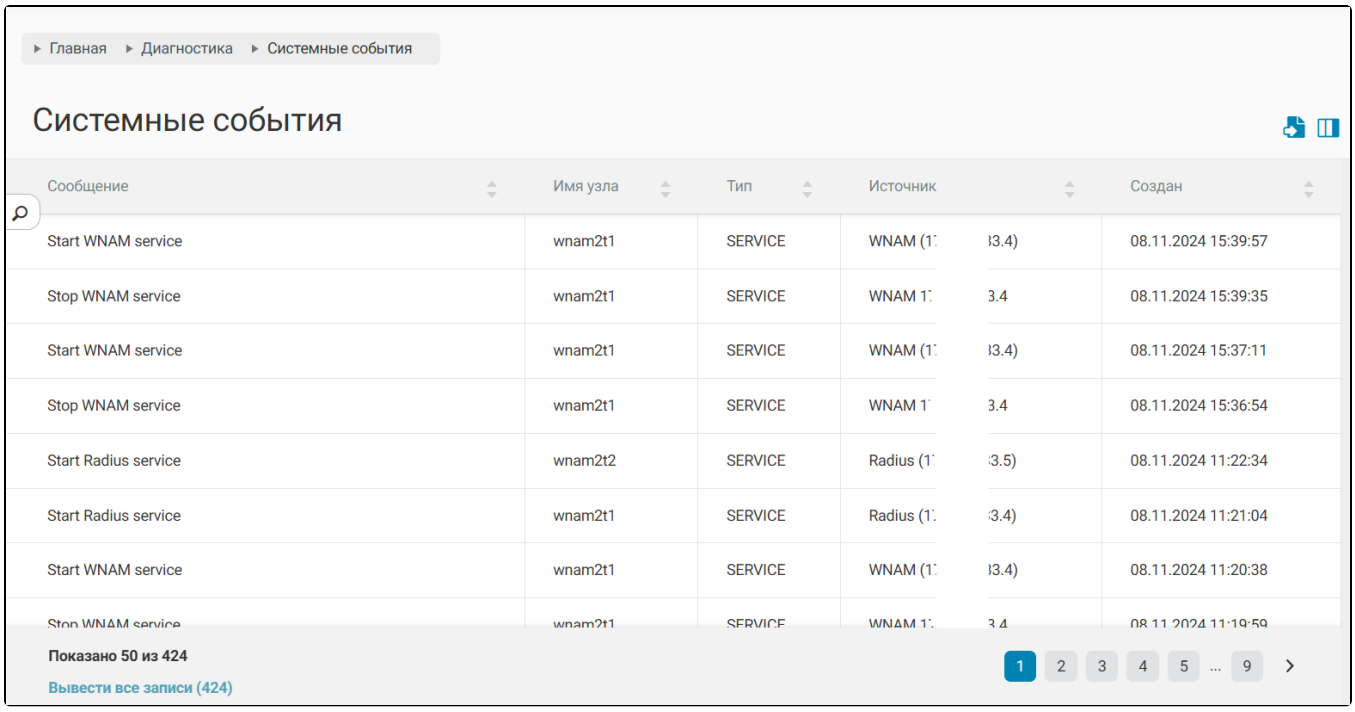
Логика отображения и функционал остальных кластеров симметрична текущему, но без возможности отображения раздела базы данных.



Также, в конце основного раздела "Кластер", находится информация подключенного распределенного кластера Kafka.

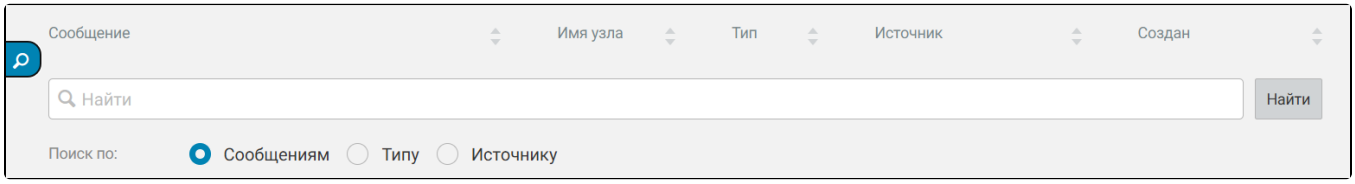
Системные события

Раздел системных событий (syslog) отображает записи о событиях системного журнала (журналы, системную консоль), сортировку и обработку в зависимости от источника сообщений.



По умолчанию, сортировка установлена по убыванию столбца даты создания системного события. Но, при необходимости, также присутствует возможность изменить сортировку по убыванию/возрастанию любого столбца.

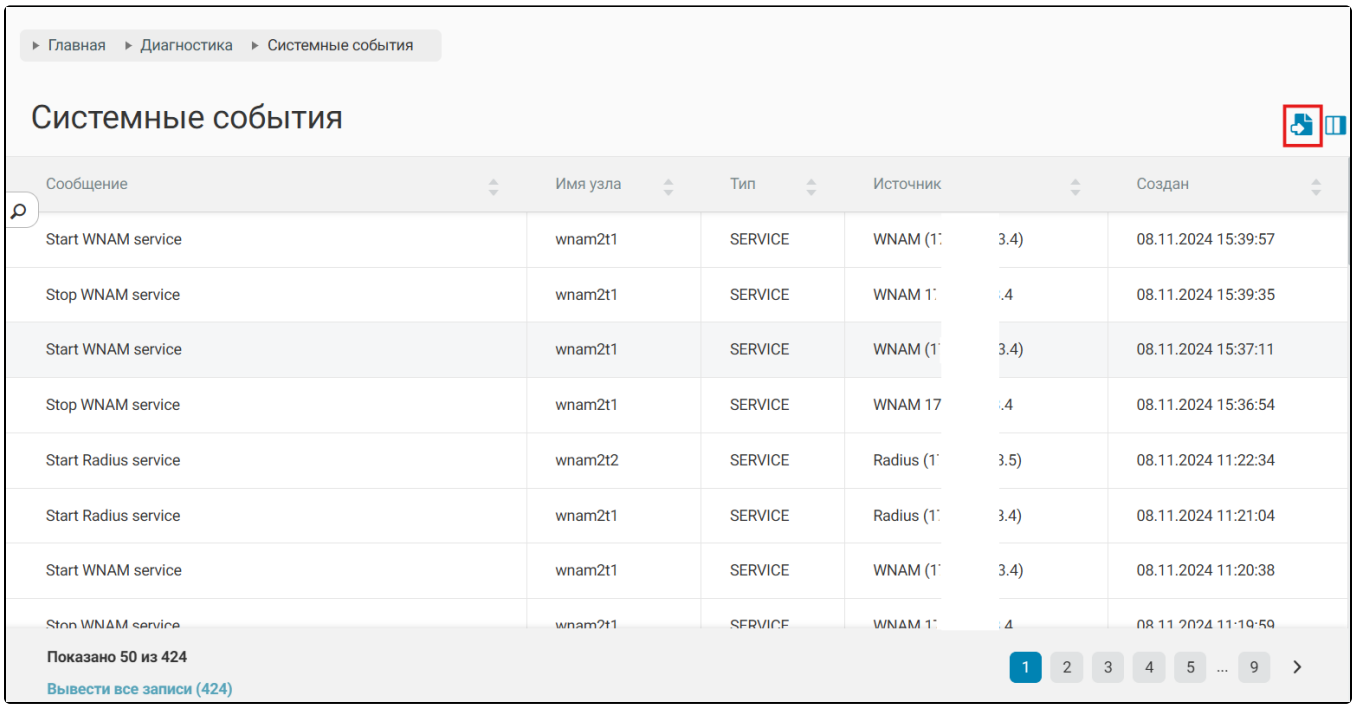
При необходимости в поиске того или иного системного события следует нажать на кнопку поиска  , которая находится слева сверху в таблице. После этого, откроется окно поиска системного события:



По умолчанию, установлен поиск по содержанию сообщения системного события. Если требуется изменить, по какому столбцу требуется производить поиск, то следует нажать на соответствующий чек-бокс.

Экспорт системных событий

Функция экспорта системных событий находится справа сверху основного раздела.

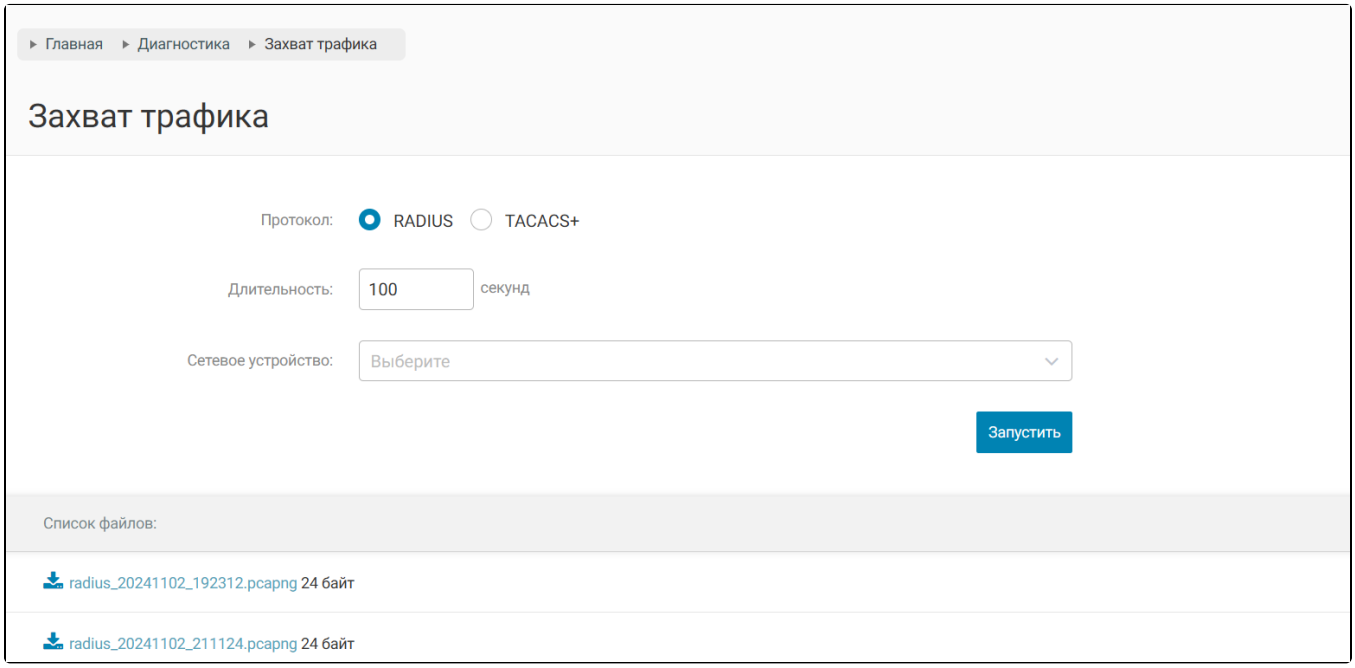


Экспортируемый файл предоставлен в формате .xlsx:

	A	B	C	D	E	F
1	Сообщение	Имя узла	Тип	Источник	Создан	
3	Start WNAM service	wnam2t1	SERVICE	WNAM (1 3.4)	08.11.2024 15:39:57	
4	Stop WNAM service	wnam2t1	SERVICE	WNAM 1 3.4	08.11.2024 15:39:35	
5	Start WNAM service	wnam2t1	SERVICE	WNAM (1 3.4)	08.11.2024 15:37:11	
6	Stop WNAM service	wnam2t1	SERVICE	WNAM 1 3.4	08.11.2024 15:36:54	
7	Start Radius service	wnam2t2	SERVICE	Radius (1 3.5)	08.11.2024 11:22:34	
8	Start Radius service	wnam2t1	SERVICE	Radius (1 3.4)	08.11.2024 11:21:04	
9	Start WNAM service	wnam2t1	SERVICE	WNAM (1 3.4)	08.11.2024 11:20:38	
10	Stop WNAM service	wnam2t1	SERVICE	WNAM 1 3.4	08.11.2024 11:19:59	
11	Delete AuditLog older 07.08.2024 20:57:45	wnam2-vt	SERVICE	WNAM 1 ..3	07.11.2024 20:57:45	
12	Delete AuditLog older 07.08.2024 19:57:56	wnam01	SERVICE	WNAM 1( ).177	07.11.2024 19:57:56	
13	Delete 68 DeviceSession older 07.05.2024 19:05:03	wnam2t2	SERVICE	WNAM 1 3.5	07.11.2024 19:05:07	
14	Delete 135 DeviceSession older 07.05.2024 19:00:09	wnam2t1	SERVICE	WNAM 1 3.4	07.11.2024 19:00:17	
15	Start Radius service	wnam2t2	SERVICE	Radius (1 3.5)	07.11.2024 18:05:52	
16	Start Radius service	wnam2t1	SERVICE	Radius (1 3.4)	07.11.2024 18:01:10	
17	Start WNAM service	wnam2t1	SERVICE	WNAM (1 3.4)	07.11.2024 18:00:11	
18	Stop WNAM service	wnam2t1	SERVICE	WNAM 1 3.4	07.11.2024 17:59:38	

Захват трафика

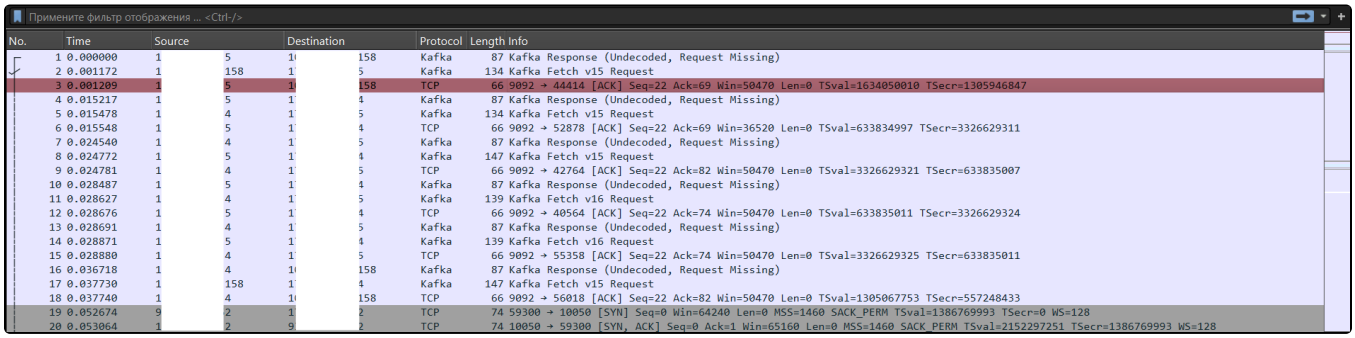
Данный раздел позволяет составить отчет передачи пакетов данных для последующего анализа потока информации.



Для составления отчета необходимо выбрать протокол, по которому необходимо проанализировать захват трафика, захват трафика за определенную длительность и определить, какие сетевые устройства будут выбраны.

После запуска захвата трафика будет сформирован файл-дамп сетевых пакетов в формате .pcap. Помимо этого, файл сохранится в разделе "Список файлов", в котором возможно будет скачать дамп сетевых пакетов.

Данный вид расширения файлов можно открыть любой программой, которая поддерживает открытие файлов в формате .pcap:



Логи

Данный раздел меню позволяет просмотреть полный протокол операций, совершаемых системой при работе системы. В логи попадают все попытки обращения на портал, RADIUS и TACACS+ взаимодействие с серверами доступа.

Для того, чтобы просмотреть лог работы системы WNAM 2 в реальном времени необходимо перейти в раздел "Диагностика" "Логи". Веб-интерфейс позволяет настроить фильтры по времени составления отчета.

После нажатия на кнопку "Получить логи", будет составлен архив, содержащий лог, собранный с нескольких сервисов за указанное ранее время. Структура файлов имеет примерно такой вид:

- **wnam2.log** – Лог системы WNAM 2;
- **wnam2-eureka.log** – Лог, собранный с сервиса Eureka;
- **wnam2-gateway.log** – Лог службы управления запросами к API веб-сервисов и системы WNAM 2;
- **wnam2-radius.log** – Лог RADIUS
- **wnam2-tacacs.log** – Лог TACACS+

Приблизительный вид лог-файла будет иметь похожую структуру

> *ноя 08 19:25:00 wnam2t1 start.sh[14865]: 19:25:00.004 TRACE [c.n.w.c.nodes.WnamClusterConsumer:19] - Received cluster: wnam-cluster-d1e1-4da2b478e977*
> *ноя 08 19:25:00 wnam2t1 start.sh[14865]: 19:25:00.005 TRACE [c.n.w.c.nodes.WnamClusterService:294] - Send cluster: wnam-cluster-d1e1 to wnam-cluster-topic*
> *ноя 08 19:25:00 wnam2t1 start.sh[14865]: 19:25:00.018 TRACE [c.n.w.c.nodes.WnamClusterConsumer:19] - Received cluster: wnam-cluster-453e-fc493ea081a9*
> *ноя 08 19:25:02 wnam2t1 start.sh[14865]: 19:25:02.699 TRACE [com.netams.w2.cluster.AdminService:454] - Check kafka connection...*

Настройки

Раздел меню "Настройки" основного интерфейса администратора позволяет выполнить все настройки, связанные с обеспечением работы системы WNAM 2. В разделе "Настройки" доступны следующие данные по настройке работы системы:

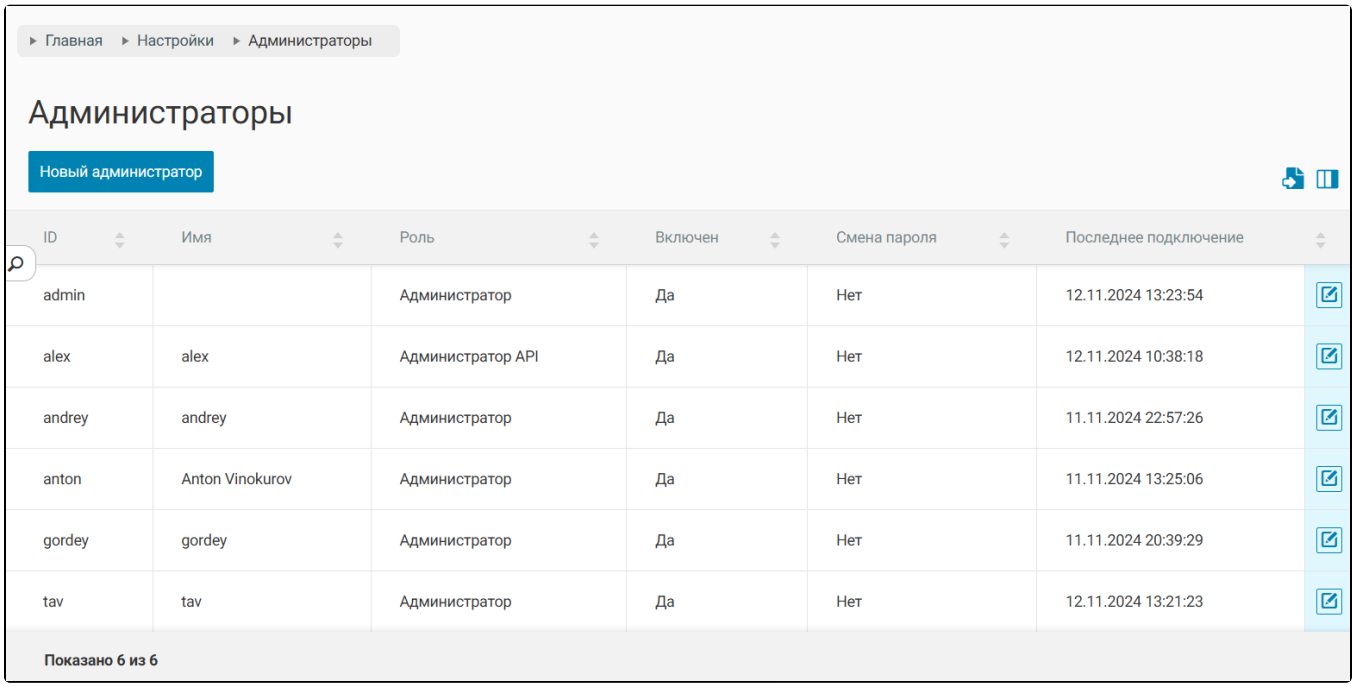
- Администраторы;
- Группы;
- Роли;
- Параметры;
- Парольная политика;
- Лицензии;
- Резервное копирование.

Детальная информация по каждому виду мониторинга представлена в соответствующих разделах.

Администраторы

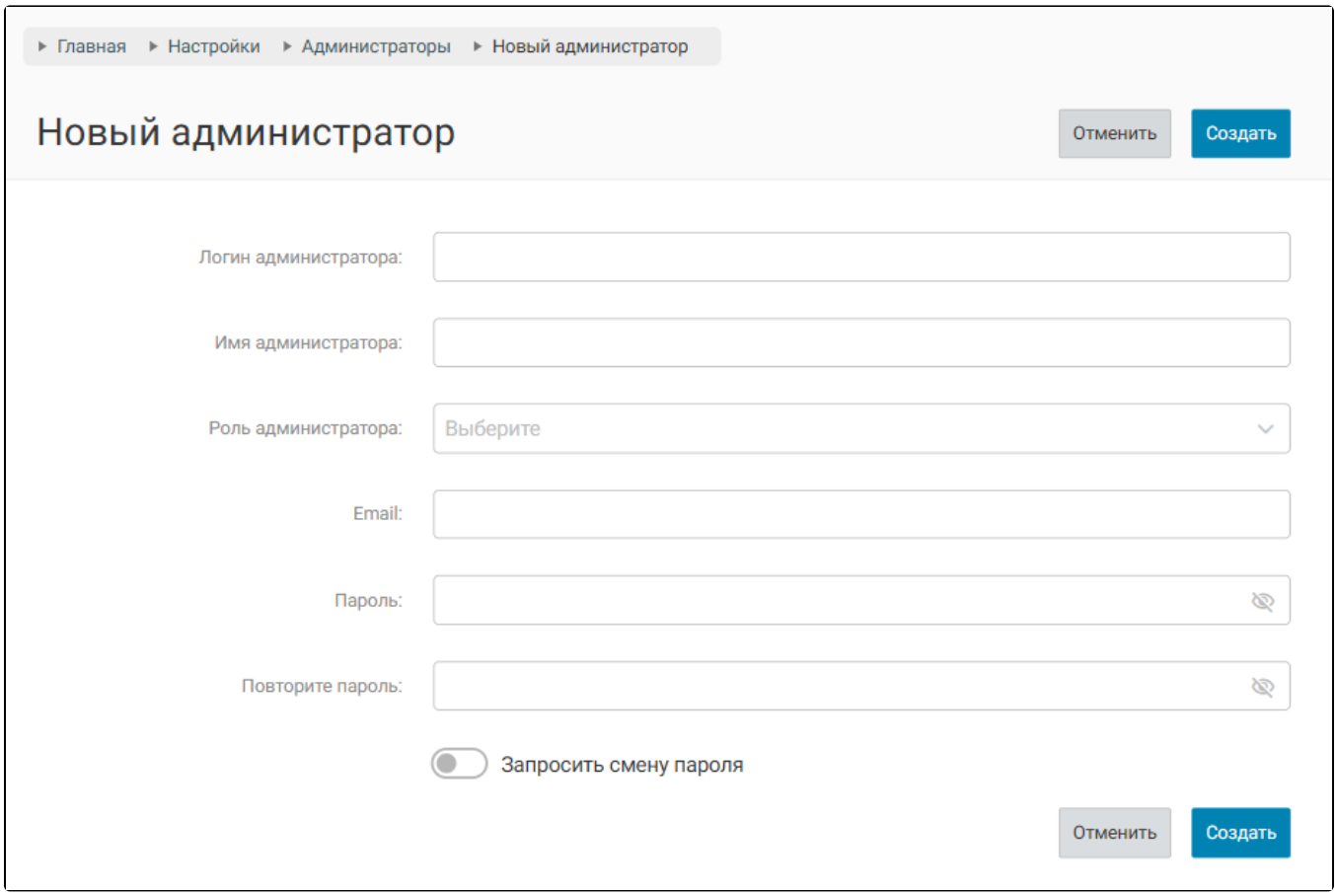
Данное меню позволяет создавать учётные записи администраторов веб-интерфейса системы WNAM 2. Интерфейс имеет ролевую модель (ролевое разграничение доступа), то есть каждый пользователь имеет индивидуальные настройки просмотра и редактирования информации, назначенные его роли.

В разделе "Настройки" "Администраторы" в основной таблице отображается перечень зарегистрированных в системе локальных учётных записей и их основные параметры.



Для создания новой учетной записи, необходимо нажать кнопку "Новый администратор".
При создании новой учетной записи администратора требуется указать следующие поля:

- Логин администратора;
- Имя администратора;
- Роль администратора. Подробнее про роли и разграничение ролей указано в соответствующей статье;
- Email;
- Пароль и повторение пароля. Подробнее о настройке паролей приведено в статье парольной политики;
- Функция запроса смены пароля при первичной авторизации.

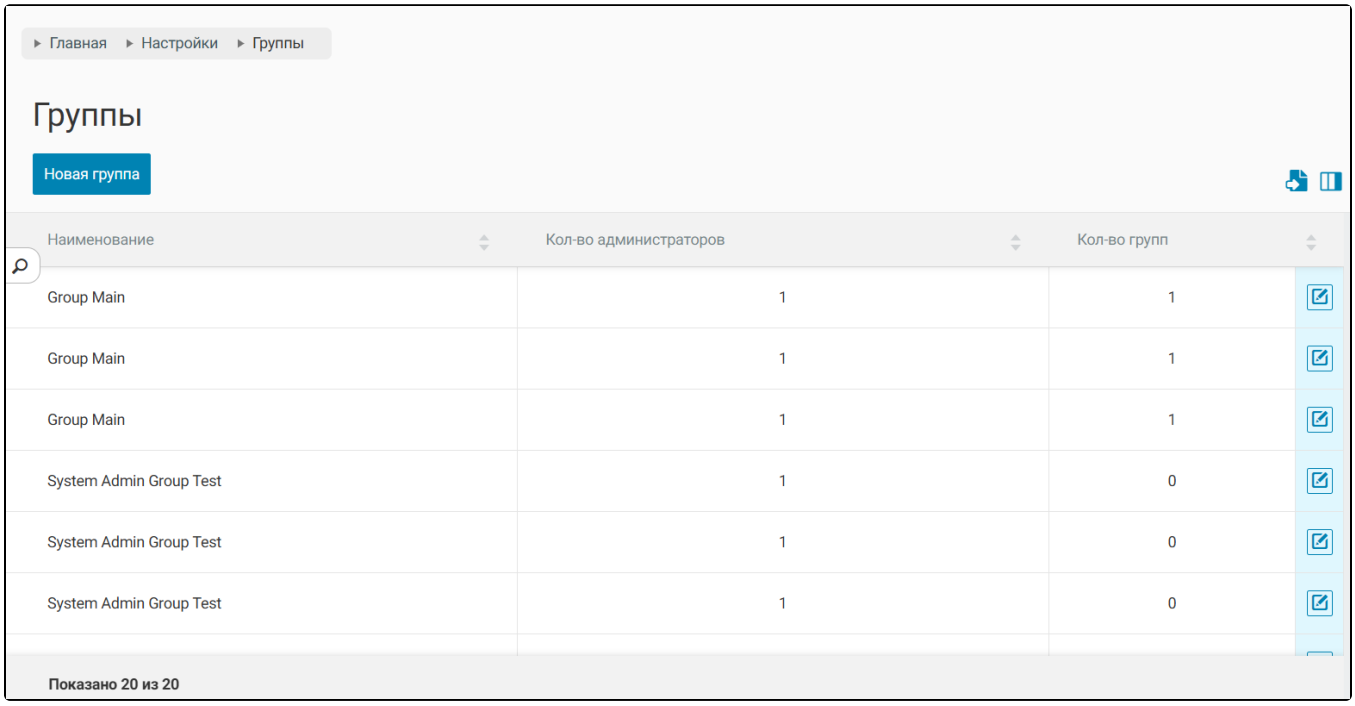


Если Вы желаете обеспечить дополнительные меры безопасности авторизации учетных записей WNAM 2, рекомендуем перейти в раздел "Настройки" – "Параметры" и настроить параметр "Запретить одновременную авторизацию с разных ip".

После создания учетной записи администратора, будет возможно провести авторизацию или передать реквизиты сотруднику.

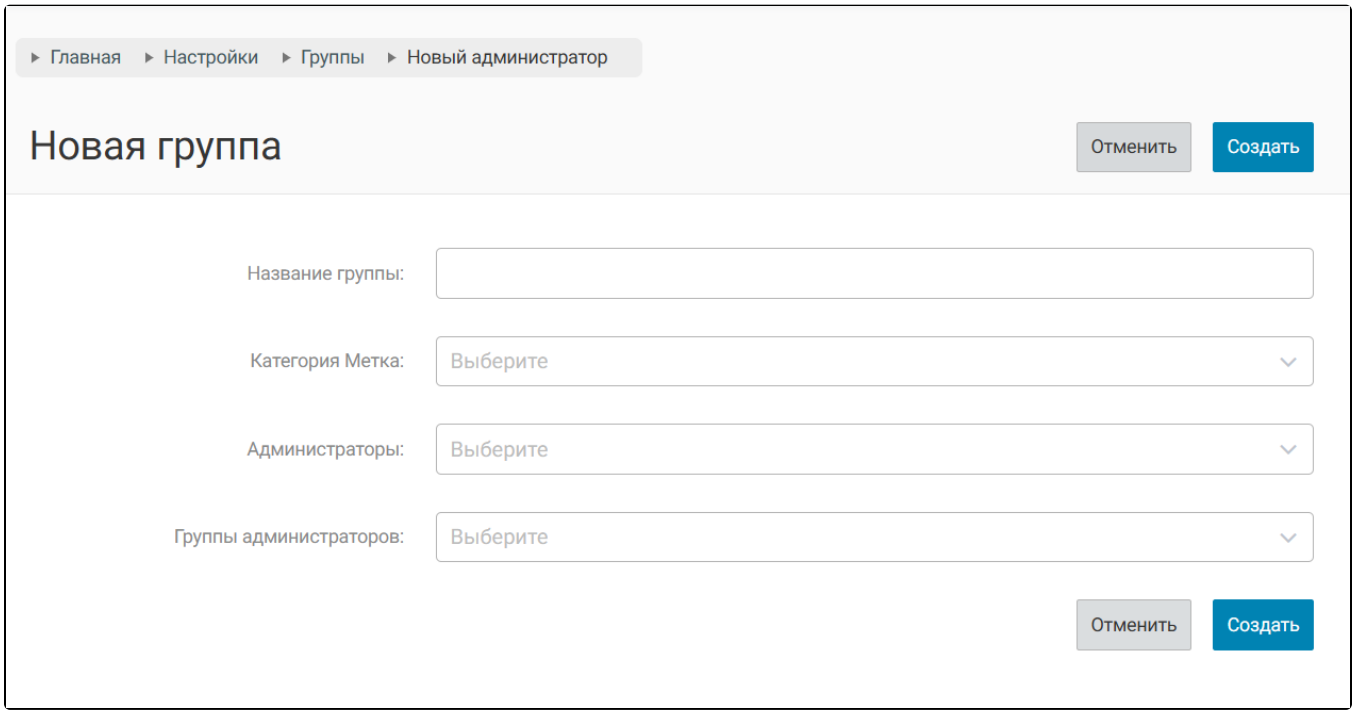
Группы

Группы позволяют объединить некоторое число администраторов в одну группу. Данное решение будет полезно в случаях, например, когда необходимо применить категории на несколько учетных записей администраторов. В группу может входить любое число подгрупп и любое число пользователей одновременно. Каждый пользователь или группа может быть членом нескольких групп. Система WNAM 2 проводит проверку "зацикленности" групп.



При нажатии на кнопку "Новая группа" или при нажатии левой кнопкой мыши на контекстное меню в строке таблицы откроется окно создания/редактирования, в котором следует:

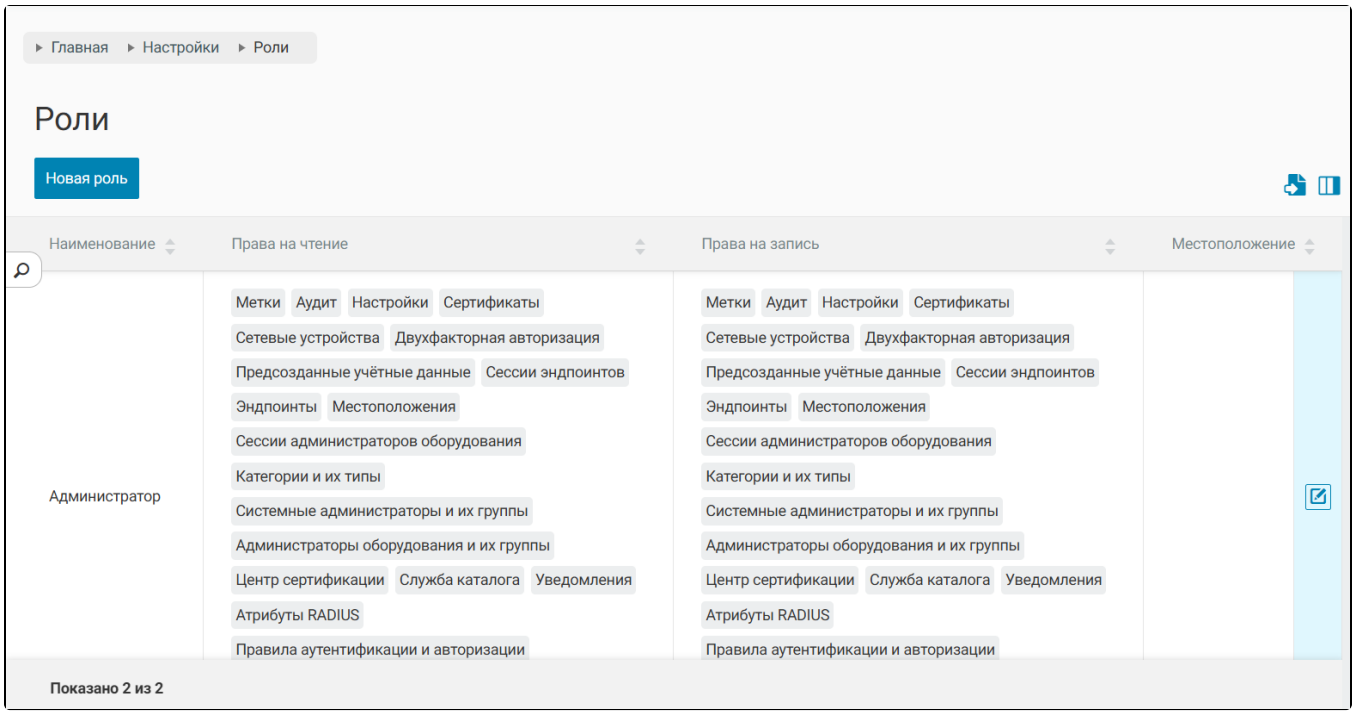
- задать название группы;
- указать применимые категории;
- выбрать пользователей из имеющихся;
- выбрать дочерние (вложенные) группы.



После выполненных настроек при создании группы необходимо нажать кнопку "создать". Созданные группы администраторов будут использоваться в зависимости от настроек применимых категорий.

Роли

Система WNAM 2 поддерживает ролевую модель, при которой администратору возможно ограничивать различные области доступа системы WNAM 2. Чтобы просмотреть список уже имеющихся ролей, необходимо перейти в "Настройки" – "Роли".

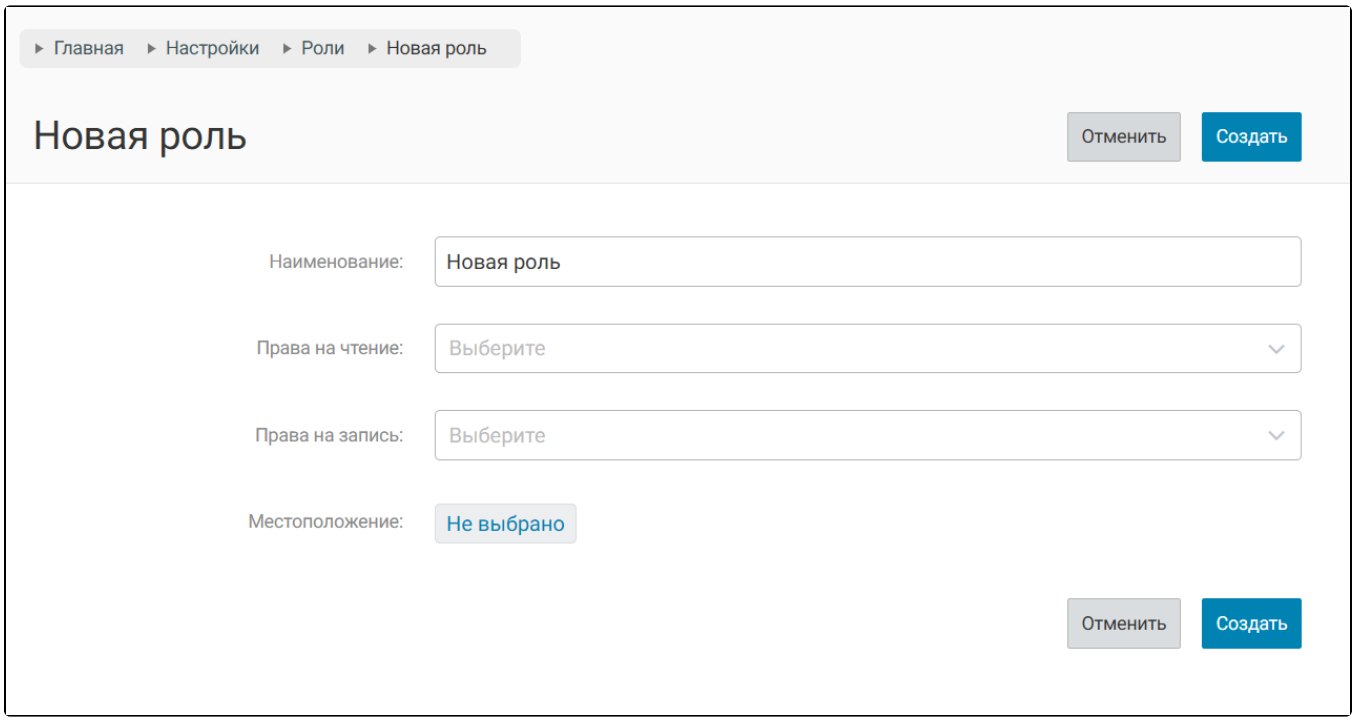


При первичной установке системы WNAM 2 уже существует две роли: "Администратор" и "Администратор API".

Для создания новой роли, необходимо нажать на соответствующую кнопку "Новая роль". После этого, будет открыто окно, в котором необходимо указать название роли, выделяемые права на чтение, выделяемые права на запись.

⚠ Под правами на чтение подразумевается свойство администратора, при котором учетной записи выдаются права на просмотр той или иной области доступа.

⚠ Под правами на запись подразумевается свойство администратора, при котором учетной записи выдаются права на запись той или иной области доступа.



В системе WNAM 2 существует следующий список областей доступа к веб интерфейсу системы WNAM 2:

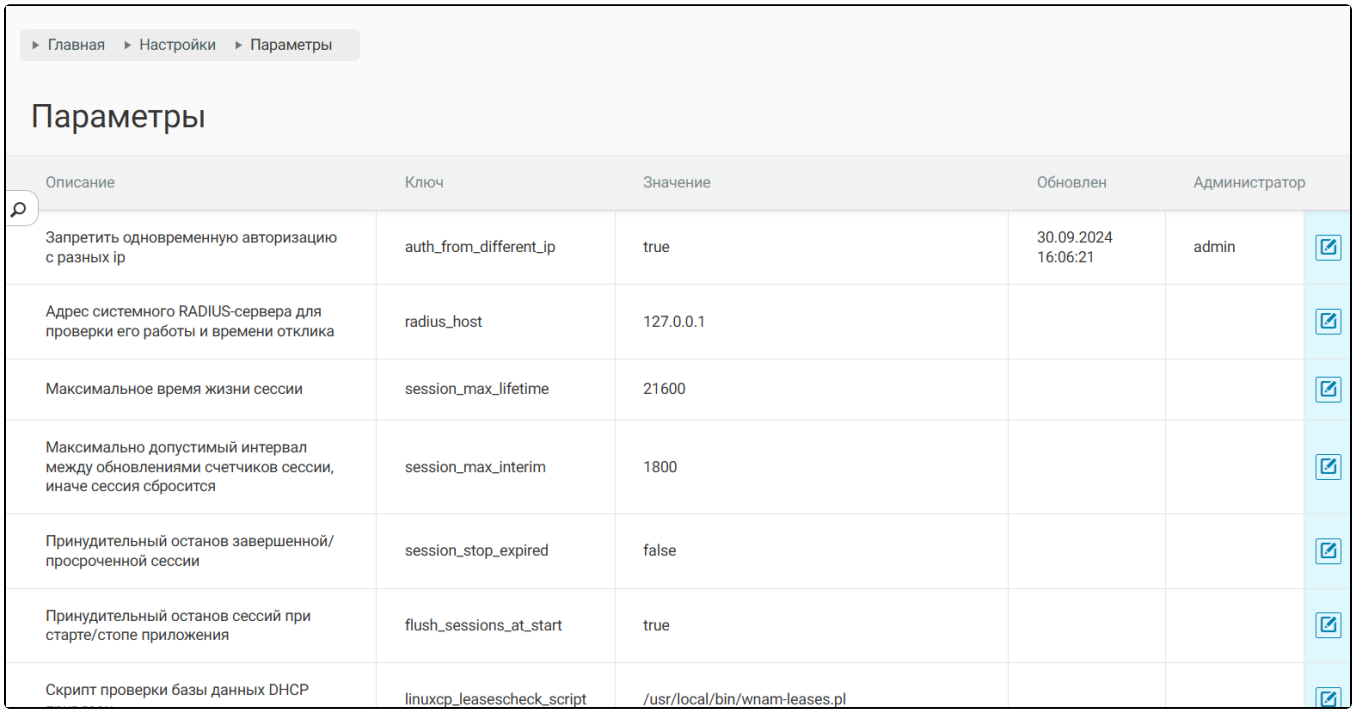
- Правила аутентификации и авторизации;
- Местоположение;
- Сетевые устройства;
- Настройки;
- Центр сертификации;
- Сертификаты;
- Службы каталога;
- Категории и их типы;
- Метки;
- Профайлер;
- Загружаемые ACL;
- Уведомления;
- Аудит;
- Атрибуты RADIUS;
- Двухфакторная авторизация;
- Системные администраторы и их группы;
- Администраторы оборудования и их группы;
- Эндпоинты;
- Пересозданные учетные данные;
- Сессии эндпоинтов;
- Сессии администраторов оборудования.

Важно явно определить, какие роли следует создавать для различных администраторов и какие области доступа следует выделять. В ином случае, существует риск безопасности.

Созданные роли в последствии возможно применить для раздела "Администраторы".

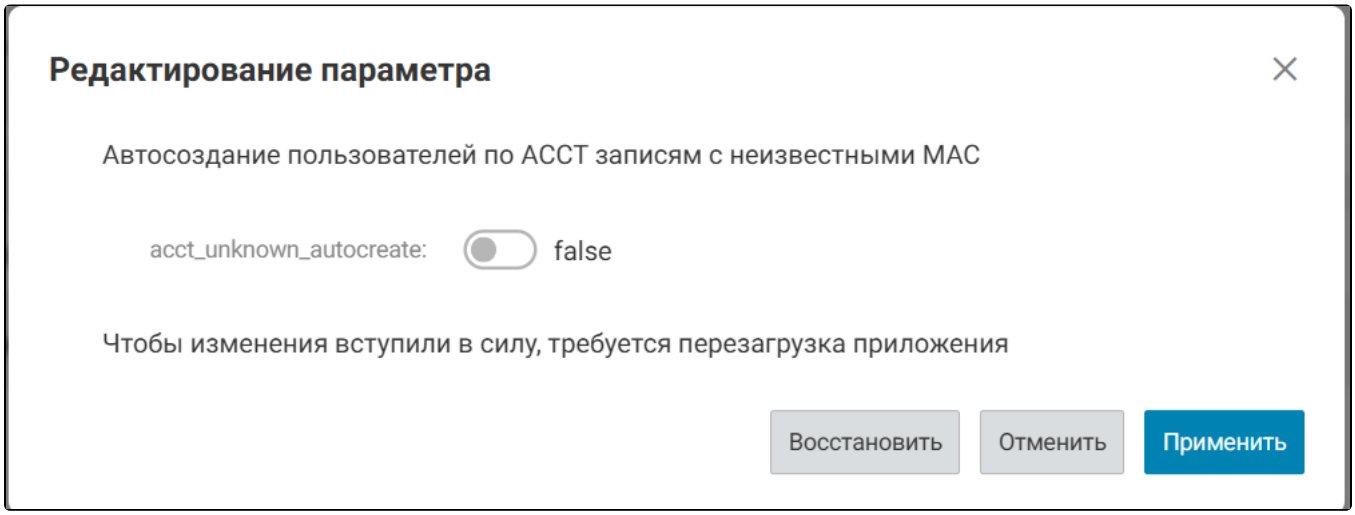
Параметры

В этом разделе определяются "тонкие настройки" системы WNAM 2. Преимущество настроек через веб-интерфейс определяется резервированием конфигурации, подсказками по формату и возможностью применения ряда настроек без перезагрузки сервиса системы WNAM 2. В настоящий момент доступно порядка 118 параметров. Для настройки параметров необходимо перейти в раздел "Настройки" "Параметры". Список параметров представлен в таблице.



В большинстве случаев параметры не следует перенастраивать, кроме отдельных задач "тонкой настройки" под контролем службы технической поддержки компании NETAMS.

Формат параметра, описание, значение по умолчанию, тип данных можно увидеть в соответствующем popup-окне при нажатии левой кнопкой мыши на параметр из списка в таблице.



По статистике, единственными параметрами, которые необходимо модифицировать, являются настройки встроенного RADIUS-сервера, а именно секретный ключ radiusd_secret и перечень сетей, где находятся ваши RADIUS-клиенты (контроллеры, точки доступа, сервисные роутеры) radiusd_networks.

Ниже будут описаны некоторые параметры, которые помогут в настройке системы WNAM 2:

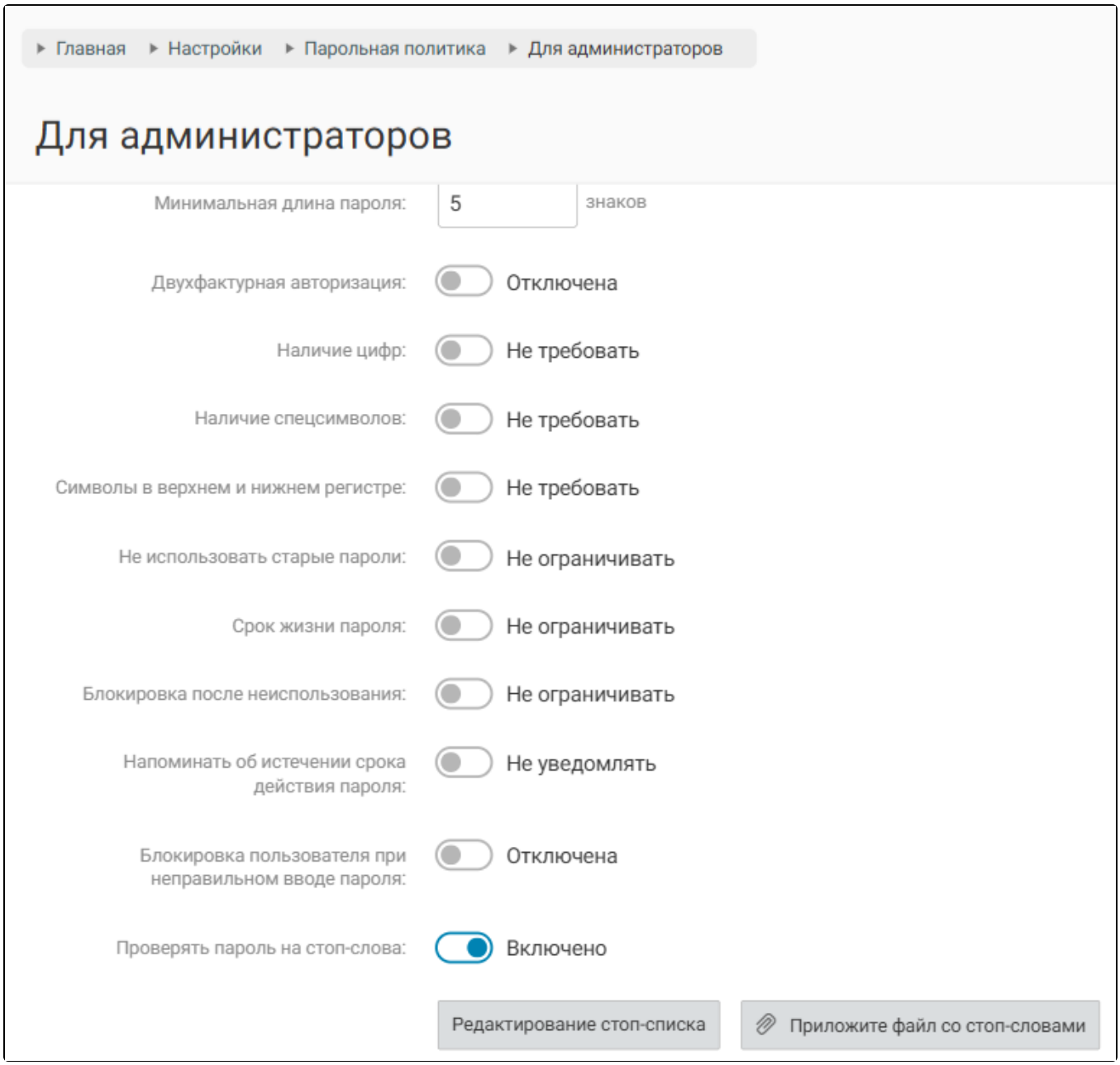
Запретить одновременную авторизацию с разных ip

Ключ данного параметра является auth_from_different_ip. Если данный параметр установлен в состояние true, то предыдущая авторизация этой учетной записи с другим IP адресом будет отозвана. В таком случае, придется заново проводить авторизацию на том устройстве, которое было отозвано.

Внимание! Данная настройка связанна именно с авторизацией IP адресов. При включенном параметре это никак не будет влиять на авторизацию в одном браузере. Т.е., возможно будет открыть несколько окон системы WNAM 2 в одном браузере.

Парольная политика

Система WNAM 2 имеет возможность применять парольную политику при создании/редактировании учетной записи. Парольная политика подразумевает использование нескольких правил для создания более защищенного пароля для целей безопасности авторизации пользователей. Данный раздел находится по пути "Настройки" – "Парольная политика".



Парольная политика имеет два профиля: для администраторов и для администраторов API. Набор правил имеет одинаковый состав для двух этих профилей. При редактировании парольной политики важно учитывать, для каких целей и для какого типов учетных записей администраторов стоит применять правила.

Парольная политика имеет ряд правил, которые можно применить:

- Минимальная длина пароля;
- Применение двухфакторной авторизация;
- Требовать наличие цифр;
- Требовать наличие спецсимволов;
- Использовать символы в верхнем и нижнем регистре;
- Не использовать старые пароли;

- Определить срок жизни пароля (в днях);
- Блокировка после неиспользования. Позволяет блокировать пароль и требовать создать новый пароль спустя назначенное время в днях;
- Напоминать об истечении срока действия пароля;
- Блокировка пользователя при неправильном вводе пароля;
- Проверять пароль на стоп-слова. Возможно настроить определенный список как внутри системы WNAM 2, так и импортировать стоп-слова в виде .txt файла или в виде архива .zip;
- Пароль не должен содержать логина;

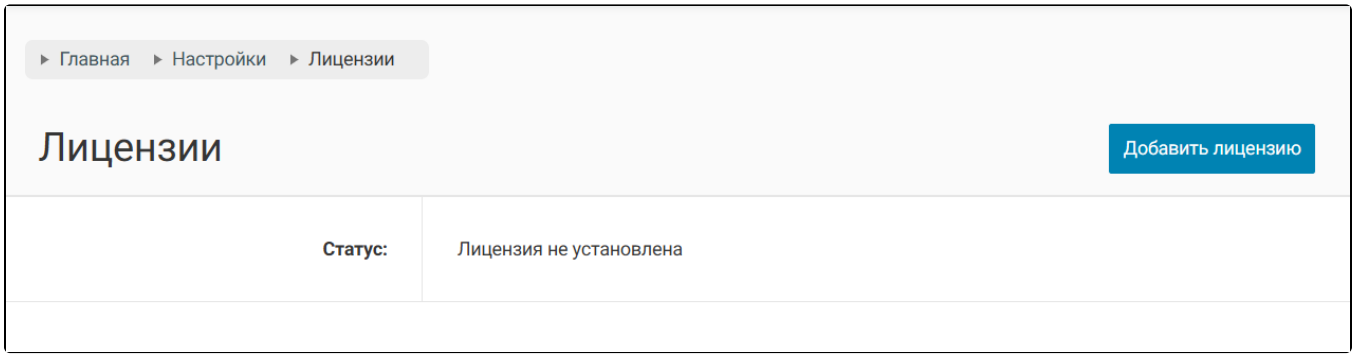
Если Вы желаете обеспечить дополнительные меры безопасности авторизации учетных записей WNAM 2, рекомендуем перейти в раздел "Настройки" – "Параметры" и настроить параметр "Запретить одновременную авторизацию с разных ip".

После нажатия на кнопку "Сохранить", парольная политика будет сразу же применена.

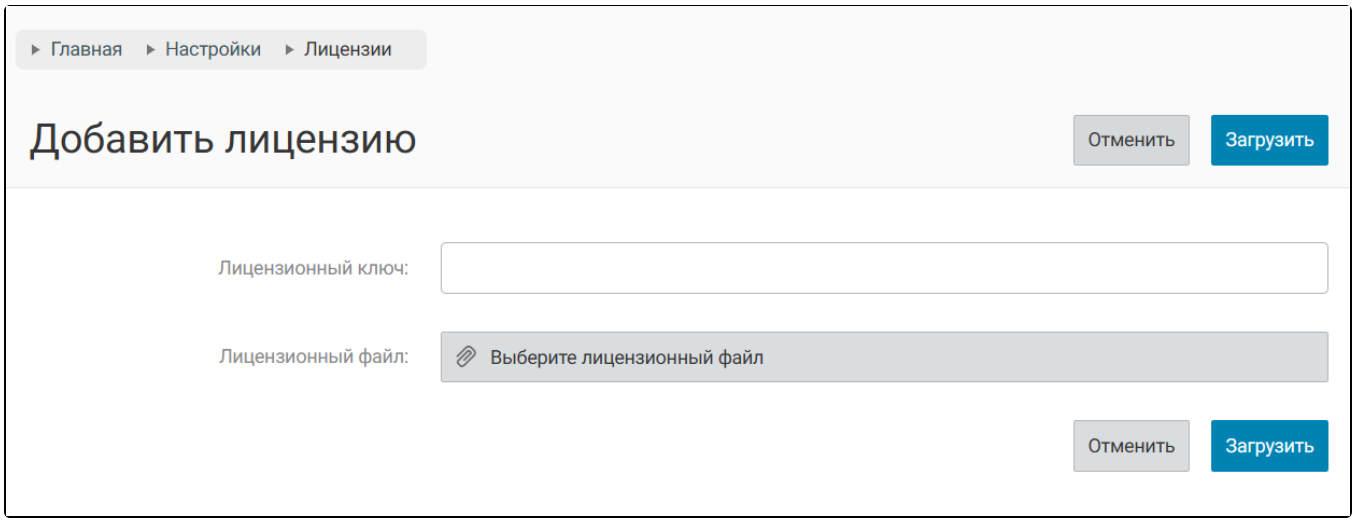
Лицензия

В данном разделе описан способ задания лицензионного ключа системы WNAM 2.

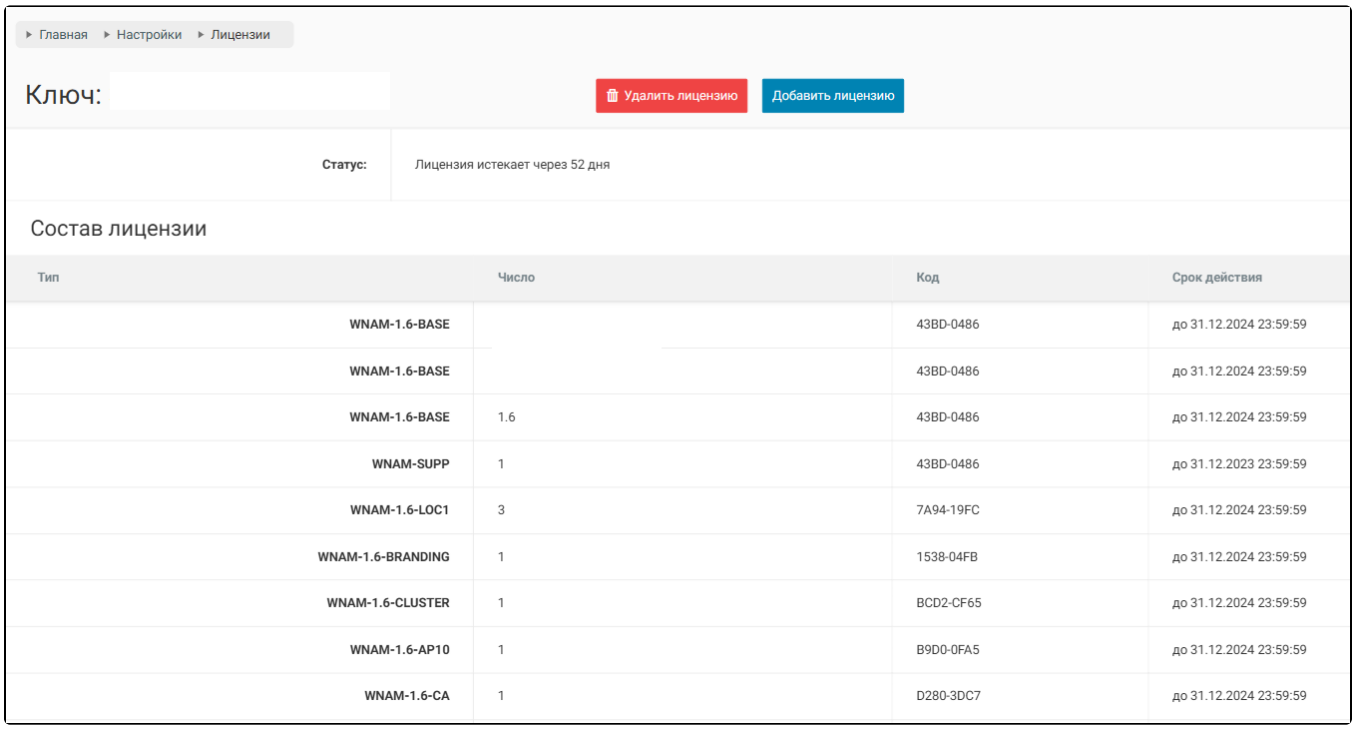
Для активации лицензии необходимо перейти в раздел "Настройки" – "Лицензии" – "Добавить лицензию".



После нажатия на кнопку "Добавить лицензию", требуется указать лицензионный ключ и выбрать лицензионный ключ.



После успешного применения ключа можно проверить включенные функции, статус лицензии, а также версию работающего дистрибутива системы WNAM 2. Для этого необходимо перейти в раздел "Настройки" "Лицензии".



В таблице отображаются следующие данные:

- основной лицензионный ключ системы;
- перечень всех выданных ключей и сроком их действия.

Основной лицензионный ключ можно добавить, вписав новый ключ в соответствующее поле и нажать кнопку "Добавить лицензию", а затем в открывшемся окне нажать кнопку "Загрузить" и выбрать соответствующий файл с полученным лицензионным ключом.

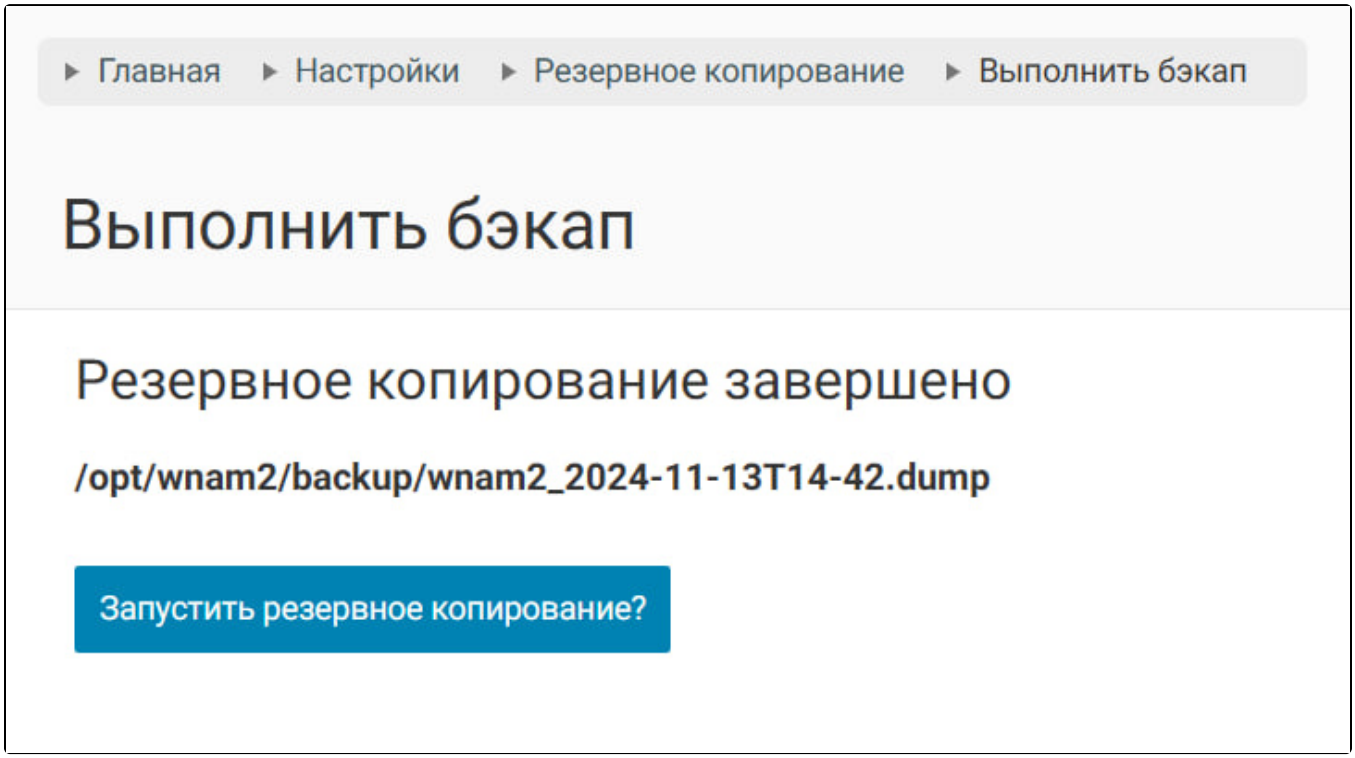
⚠ В случае, если необходимо изменить лицензионный ключ, необходимо сначала удалить нынешнюю лицензию, а после провести процедуру добавления лицензии снова. Инструкция по добавлению лицензии указана выше в данной статье.

Резервное копирование

В данной статье описаны способы резервного копирования и восстановления. Система WNMA 2 имеет возможность записывать точки возврата (бэкап) посредством файлов общего снимка всей информации системы (дамп файл, англ. dump file).

Выполнить бэкап

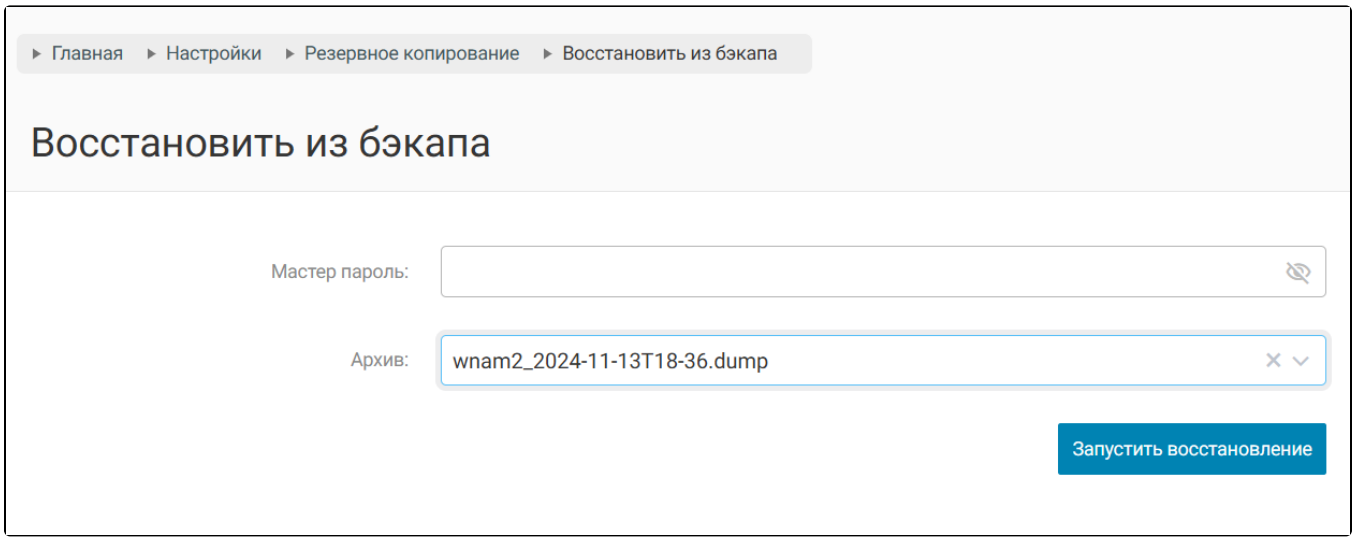
Если ранее не было настроено функции автоматического создания файлов резервного копирования, возможно сделать файлы бэкапа вручную. Для этого необходимо перейти в раздел "Настройки" – "Резервное копирование" – "Выполнить бэкап" и нажать на кнопку "Запустить резервное копирование".



После запуска создания резервного копирования, будут созданы файлы с расширением .dump в локальную базу данных в самой системе WNAM 2. Способы экспорта описаны в статье ниже, в подразделе "Импорт/экспорт дамп файла". Следующим, будет возможно провести восстановление системы из бэкапа.

Восстановить из бэкапа

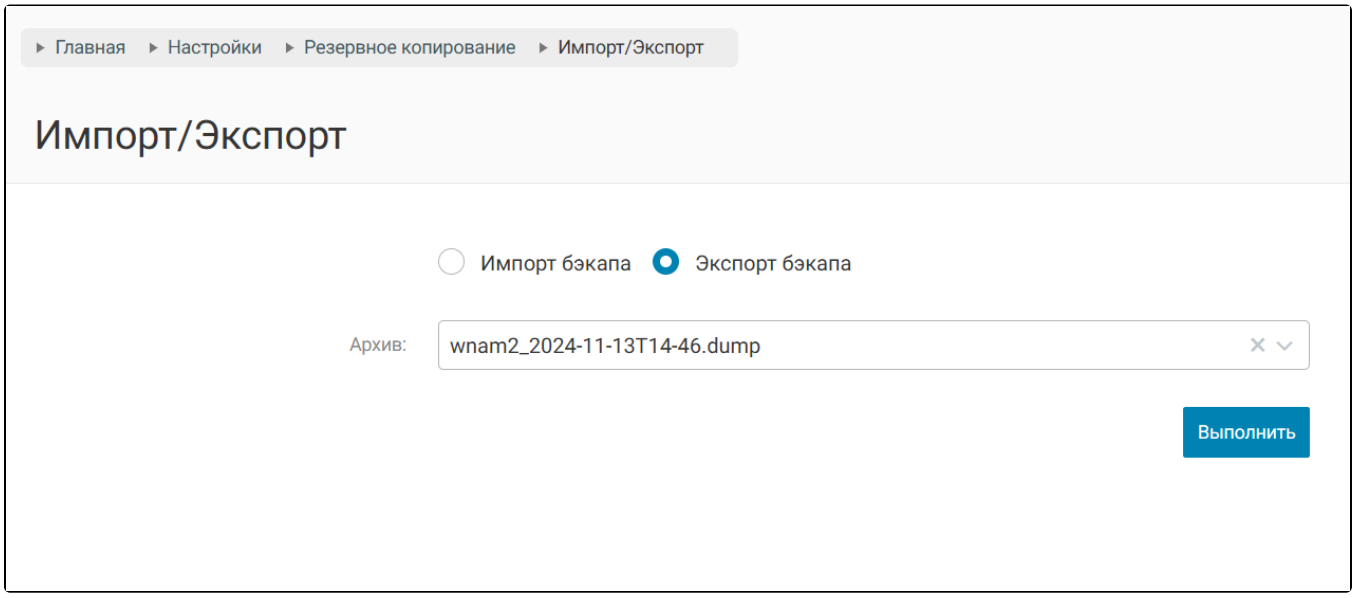
После созданной точки резервного копирования, будет доступна функция восстановления из бэкапа. Для этого необходимо перейти в раздел "Настройки" – "Резервное копирование" – "Восстановить из бэкапа". В данном разделе требуется указать мастер пароль и выбрать требуемый файл точки восстановления системы WNAM 2.



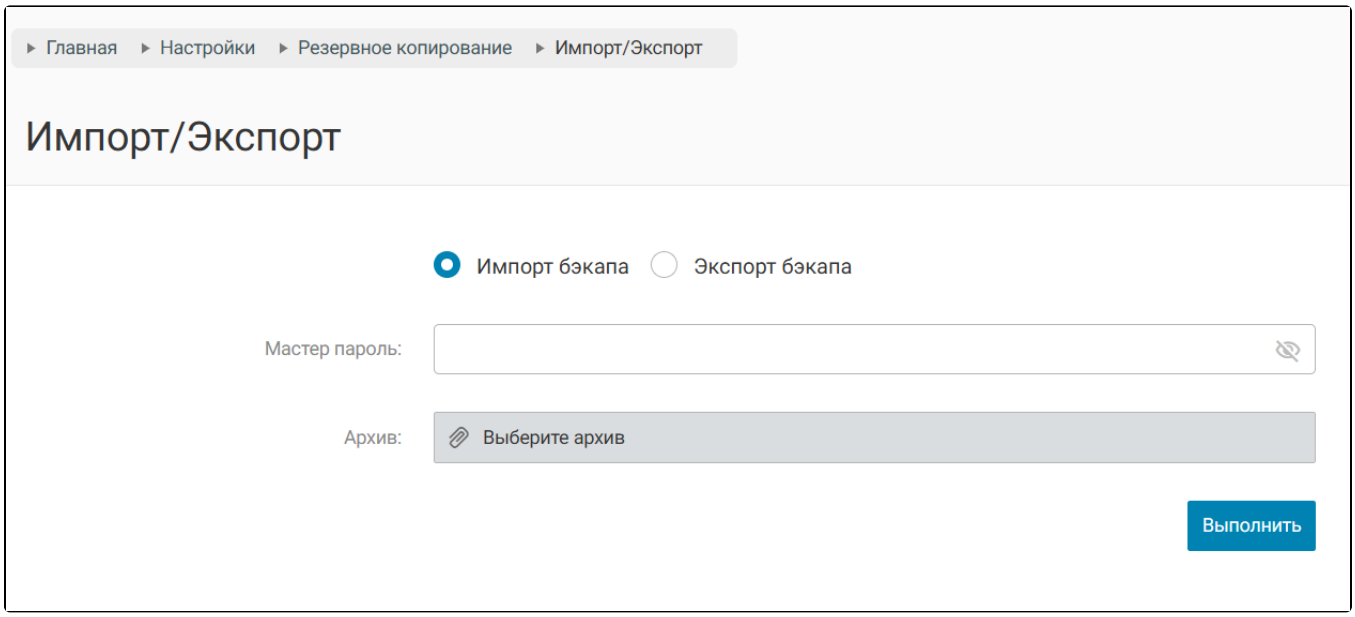
Процесс восстановления не занимается много времени. По окончании процесса восстановления, рекомендуется очистить кэш страницы, а после обновить страницу, на которой находится веб-интерфейс системы WNAM 2.

Импорт/Экспорт дамп файла

При выбранной функции "Экспорт бэкапа", если раннее было создано одно и более точек восстановлений, необходимо выбрать требуемый файл. Структура названий файлов выглядит следующим образом: wnam2_**год_месяц_день**T**час_минуты**.dump. Время датируется на момент которой был произведен бэкап системы.



При импорте файлов резервного копирования требуется указать мастер пароль и архив .zip точки резервного копирования.


Главная
Настройки
Резервное копирование
Импорт/Экспорт
Импорт/Экспорт
Импорт бэкапа
Экспорт бэкапа
Мастер пароль:
Архив:
Выберите архив
Выполнить

Траблшутинг

Восстановление пароля

Если забыт пароль администратора системы (пользователя admin), его можно сбросить в значение по умолчанию ("admin") путём прямой модификации записи в БД. Для этого на сервере системы WNAM от пользователя root необходимо выполнить команды:

```
mongo wnam_db

db.webinterfaceusers.update( { _id: "admin"} , { $set : { "password" :
"d2abaa37a7c3db1137d385e1d8c15fd2"} } )
```

Уменьшение размера базы лог-событий

Поскольку по умолчанию все объекты в БД MongDB хранятся неограниченное время, в нагруженной системе возможна генерация очень большого числа событий, которые занимают место в коллекции логов (**cmdServiceLogs**). СУБД Mongodb обладает способностью автоматически удалять объекты из коллекции, если превышено время их жизни. Для установки времени жизни сообщений в логах, равное 14 дням (14 дней - это 60*60*24*14 = 1209600 секунд), следует создать новый индекс:

```
mongo wnam_db

db.cmdServiceLogs.createIndex( { "time": 2 }, { expireAfterSeconds: 1209600 } );
```

Используемые TCP/IP порты

Для работы системой WNAM используются порты и протоколы, которые необходимо настроить на межсетевом экране используемого сервера или промежуточных межсетевых экранах. Описание портов представлено в таблице.

Протокол и порт	Направление	Назначение
tcp/80	к серверу	веб-интерфейс администратора, пользовательские страницы портала (авторизация и реклама)
tcp/443	к серверу	пользовательские страницы портала (авторизация и реклама) при использовании портала HTTPS (Mikrotik)
udp/1812	к серверу	запросы авторизации от RADIUS-клиентов к RADIUS-серверу
udp/1813	к серверу	сообщения аккаунтинга от RADIUS-клиентов к RADIUS-серверу
udp/1700, udp/3799	от сервера	запросы PoD и CoA к серверам доступа Cisco ISG, Cisco WLC, Alcatel-Lucent
tcp/49	к серверу	TACACS+ запросы от сетевого оборудования для авторизации доступа администратора

Обслуживание

Примеры

Расширенная настройка

В данном разделе подразумевается настройка дополнительных компонентов системы WNAM 2.

Кластер Kafka

Конфигурация с двумя или более узлами в разных ЦОД, каждый из которых должен иметь возможность временной изолированной работы, востребована в сценариях корпоративной авторизации по протоколу 802.1x. В связи с этим в систему WNAM 2 был добавлен механизм формирования кластера, предусматривающий:

- в каждом узле кластера на сервер (серверах) системы WNAM 2 работает брокер обмена сообщений кластера Kafka;
- все узлы кластера и все кластеры между собой связаны через брокер Kafka, который является единственным средством синхронизации данных.

Если система WNAM 2 установлена из готового образа (OVF), то брокер Kafka уже установлен в **/opt/kafka** и предварительно частично настроен. Остаётся только настроить IP-адреса узлов.

Если система WNAM 2 установлена вручную на собственный сервер, то необходимо установить кластер Kafka, пользуясь следующей инструкций: https://kifarunix.com/install-apache-kafka-on-debian/ . Установку необходимо вести в каталоге **/opt/kafka**.

Далее необходимо настроить конфигурационный файл, определив в нем роль текущего сервера и указав адреса остальных серверов кластера. Необходимо настраивать все конфигурационные файлы на каждом сервере. В данном примере таковых будет три:

- 172.16.135.10
- 10.241.200.123
- 10.241.200.124

Если требуется два сервера Kafka, они могут находиться как в одной IP-сети, так и в разных.

Пример конфигурационного файла **/opt/kafka/config/kraft/server.properties** для сервера 172.16.135.10:

```
process.roles=broker,controller
#    .       ,    1,2,3  ..
node.id=1
#   ,
controller.quorum.voters=1@172.16.135.10:9093,2@10.241.200.123:9093,3@10.241.200.124:9093
#
listeners=PLAINTEXT://172.16.135.10:9092,CONTROLLER://172.16.135.10:9093
inter.broker.listener.name=PLAINTEXT
#
advertised.listeners=PLAINTEXT://172.16.135.10:9092
controller.listener.names=CONTROLLER
listener.security.protocol.map=CONTROLLER:PLAINTEXT,PLAINTEXT:PLAINTEXT,SSL:SSL,SASL_PLAINTEXT:
SASL_PLAINTEXT,SASL_SSL:SASL_SSL
num.network.threads=3
num.io.threads=8
socket.send.buffer.bytes=102400
socket.receive.buffer.bytes=102400
socket.request.max.bytes=104857600
log.dirs=/opt/kafka/kraft-combined-logs
num.partitions=1
num.recovery.threads.per.data.dir=1
#
offsets.topic.replication.factor=3
#
transaction.state.log.replication.factor=3
transaction.state.log.min.isr=1

#
#      ,

#         ( ),   168

log.retention.hours=72



#   ,   .       ,       log.retention.bytes.
#    log.retention.hours.    -1

log.retention.bytes=1073741824



#     .     ,     .   1073741824

log.segment.bytes=268435456
```

```
# ,
log.retention.check.interval.ms=300000

#         ,   ,          .
initial.broker.registration.timeout.ms = 60000
```

После настройки конфигурационных файлов на каждом сервере необходимо инициализировать кластер Kafka. Для этого следует сформировать ключ, который должен быть уникальным в пределах вашего кластера, т.е. на каждом узле он должен быть одинаков.

Сформировать ключ можно следующей командой:

```
/opt/kafka/bin/kafka-storage.sh random-uuid

RiS_KRIffedSfMurdVxTDKw
```

Далее следует установить сформированный ключ на каждом из серверов:

```
/opt/kafka/bin/kafka-storage.sh format -t RiS_KRIffedSfMurdVxTDKw -c /opt/kafka/config/kraft
/server.properties
```

Ключ RiS_KRIffedSfMurdVxTDKw (или тот, который сформировали) должен быть один и тот же для всех серверов кластера

Следует обратить внимание, что в параметре

```
controller.quorum.voters=1@172.16.135.10:9093,2@10.241.200.123:9093,3@10.241.200.124:9093
```

числа перед @ это **node.id**, которые должны быть прописаны одинаково в конфигурациях на всех серверах кластера.

Далее необходимо создать юнит-файл сервиса Kafka и запустить его. Пример файла сервиса **/lib/systemd/system/kafka.service** :

```
[Unit]
Requires=network.target remote-fs.target
After=network.target remote-fs.target

[Service]
Type=simple
User=wnam2
ExecStart=/opt/kafka/bin/kafka-server-start.sh /opt/kafka/config/kraft/server.properties
ExecStop=/opt/kafka/bin/kafka-server-stop.sh
TimeoutSec=30
Restart=always
RestartSec=20s

[Install]
WantedBy=multi-user.target
```

Также для уменьшения объёма логирования сервиса Kafka, необходимо отредактировать конфигурационный файл **/opt/kafka /config/log4j.properties** заменив в нём **INFO**, **TRACE** и **DEBUG** на **WARN**.
Проще всего это сделать при помощи sed:

```
sed -r -i 's/(INFO|TRACE|DEBUG)/WARN/g' /opt/kafka/config/log4j.properties
```

Поскольку служба kafka запускается от пользователя wnam, следует изменить права на папку /opt/kafka

```
chown -R wnam:wnam /opt/kafka
```

Команда для создания и запуска сервиса:

```
systemctl enable kafka
```

```
systemctl start kafka

systemctl status kafka
```

Для включения системы WNAM в работу кластера следует внести необходимые правки в конфигурационный файл **/home/wnam /application.yaml**:

```
netams:
 wnam2:
  cluster:
    # optional, default false.  kafka
    kafka_enabled: true
    # optional default false,    ,    wnam,  true   ,  false
    full_sync: true
    # optional, default 1   ()   kafka
    replicas: 3
    # optional, default true.     kafka    kafka
    unclean_election: true
    # optional, default empty.  master,       .
    role: master
    # optional, default 'true'.   .   true  false,              wnam
    use_cache: true
    # optional, default false.
    show_sync: true

spring:
 #   kafka_enabled = true
 kafka:
  bootstrap-servers: 172.16.135.10:9092,10.241.200.123:9092,10.241.200.124:9092
```

После внесенных правок следует перезапустить систему WNAM 2:

```
systemctl restart wnam2
```

Если всё правильно настроено, то в интерфейсе администратора системы WNAM 2 появится раздел "Главная" "Диагностика" "Кластер", в котором будут отображены все ваши узлы кластера, их состояние и т.п.

Конфигурация SSL/TLS

В Kafka SSL по умолчанию отключен. Для включения нужно создать keystore и trueststore и внести некоторые правки в конфигурацию server.properties.

Указываем имена хостов как они прописаны в сертификатах в поле CN

```
controller.quorum.voters=1@kafka1.domain.ru:9093,2@kafka2.domain.ru:9093
```

Далее, меняем имена listener

```
listeners=SSL://kafka1.domain.ru:9092,CONTROLLER://kafka1.domain.ru:9093
inter.broker.listener.name=SSL
```

Необходимо указать адрес этого узла

```
advertised.listeners=SSL://kafka1.domain.ru:9092
controller.listener.names=CONTROLLER
```

После, меняем мапинг имен

```
listener.security.protocol.map=CONTROLLER:SSL,SSL:SSL
```

Необходимо указать параметры ssl. Данные параметры обеспечивают аутентификацию клиента по протоколу SSL/TLS.

```
ssl.keystore.location=/opt/kafka/certs/kafka.keystore.jks
ssl.keystore.password=password
ssl.truststore.location=/opt/kafka/certs/kafka.truststore.jks
ssl.truststore.password=password
ssl.key.password=password
```

Клиенты, подключающиеся к Kafka brokers, должны предоставить действительный сертификат клиента для аутентификации.

```
ssl.client.auth=required
```

Настройки WNAM 2

В application.yaml добавить настройки, указываем расположение truststore и keystore и пароли к ним.

```
spring:
  kafka:
    bootstrap-servers: kafka1.domain.ru:9092,kafka2.domain.ru:9092
    security:
      protocol: SSL
    ssl:
      protocol: SSL
      trust-store-location: "file:///opt/kafka/certs/kafka.truststore.jks"
      truststore-password: password
      key-store-location: "file:///opt/kafka/certs/client.keystore.jks"
      key-store-password: password
```

Хранилища сертификатов

⚠ Здесь приведен пример создания сертификатов для двух серверов. На этом примере также можно сгенерировать клиентские сертификаты для WNAM 2.

Создание самозаверяющего сертификата CA.

```
openssl genpkey -algorithm RSA -out ca.key
openssl req -x509 -new -key ca.key -days 3650 -out ca.crt \
-subj "/C=RU/ST=NA/L=Moscow/O=Demo/CN=domain.ru/emailAddress=admin@domain.ru"
```

Сгенерируйте закрытые ключи серверов и запросы на подпись сертификатов (CSR).

```
openssl req -new -newkey rsa:4096 -nodes -keyout server1.key -out server1.csr \
-subj "/C=RU/ST=NA/L=Moscow/O=Company Demo/CN=kafka1.domain.ru/emailAddress=admin@domain.ru"

openssl req -new -newkey rsa:4096 -nodes -keyout server2.key -out server2.csr \
-subj "/C=RU/ST=NA/L=Moscow/O=Company Demo/CN=kafka2.domain.ru/emailAddress=admin@domain.ru"
```

Создайте файл san.cnf.

✓ Расширение SAN позволяет включать дополнительные имена субъектов, такие как доменные имена или IP-адреса, в один сертификат, что позволяет сделать сертификат действительным для нескольких объектов или альтернативных имен.

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1=*.domain.ru
```

Сгенерируйте и подпишите сертификаты серверов.

```
openssl x509 -req -in server1.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server1.crt \
-days 3650 -extfile san.cnf

openssl x509 -req -in server2.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server2.crt \
-days 3650 -extfile san.cnf
```

Преобразование сертификатов серверов в PKCS12.

```
openssl pkcs12 -export -in  server1.crt -inkey server1.key -name kafka-broker1 -out kafka1.p12
openssl pkcs12 -export -in  server2.crt -inkey server2.key -name kafka-broker2 -out kafka2.p12
```

Создание Kafka KeyStore (JKS).

```
keytool -importkeystore -srckeystore kafka1.p12 -destkeystore kafka1.keystore.jks -srcstoretype pkcs12
keytool -importkeystore -srckeystore kafka2.p12 -destkeystore kafka2.keystore.jks -srcstoretype pkcs12
```

Создание Kafka TrustStore.

```
keytool -keystore kafka.truststore.jks -alias CARoot -import -file ca.crt
```