ГАРДА ЛАБИРИНТ

ГАРДА ТЕХНОЛОГИИ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Содержание

ГЛОССАРИЙ

Термин / Сокращение	Значение
Супервизор	Сервер с ложными сетевыми информационными объектами
Control center	Интерфейс анализа событий и управления всей платформой
Машина	Используется для эмуляции рабочей станции
DHCP	Сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес
Токен	Набор авторизационных данных

1 ВВЕДЕНИЕ

Данный документ представляет собой пользовательскую документацию, описывающую работу в системе Гарда Лабиринт.

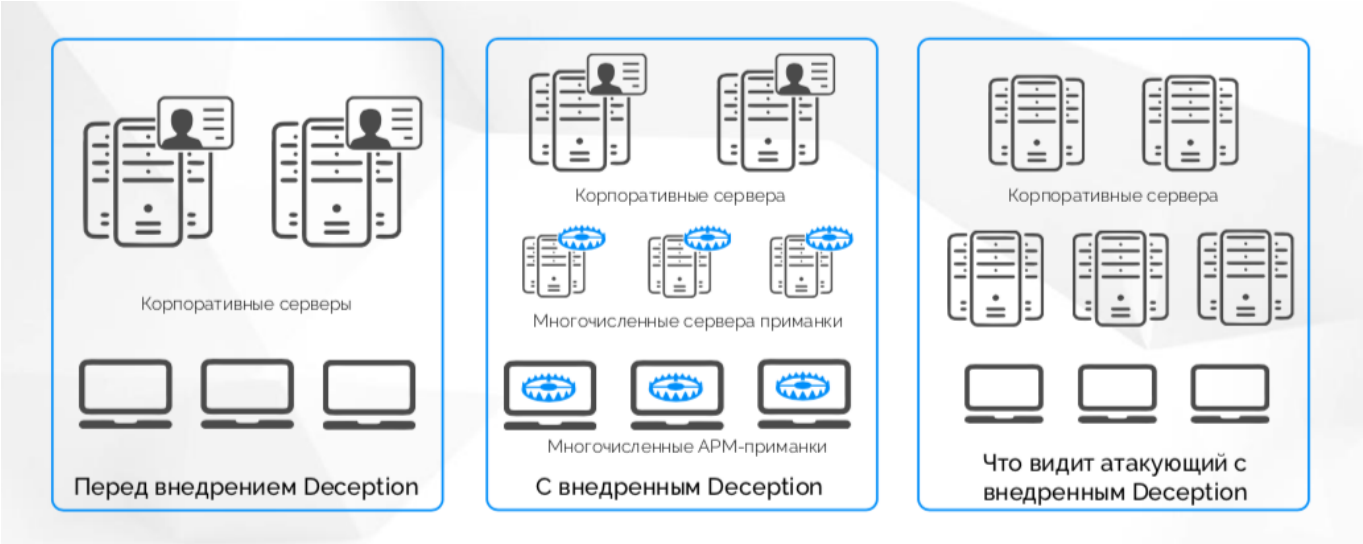
Инструкция актуальна для версий:

Центр управления	1.5.0
Супервизор	1.5.0
Агент	1.2.0

1.1 Краткое описание структуры администрируемого комплекса

Технологии Deception, или по-русски, «технологии обмана» (от англ. deception technologies) — совокупность техник имитации ИТ-инфраструктуры и дезинформации злоумышленников, используемых с целью обнаружения и замедления продвижения атак злоумышленников и позволяющих в итоге останавливать атаки до нанесения значимого ущерба.

С помощью централизованной системы управления по сети предприятия размещаются ловушки (от англ. decoys) — эмулированные устройства или устройства под управлением реальных операционных систем (Windows или Linux) с различными наборами сервисов. Так как у обычных пользователей нет легитимных причин обращаться к этим устройствам, любая попытка взаимодействия с ними будет считаться злонамеренным действием. Цель размещения ловушек заключается в том, чтобы привлечь внимание злоумышленника, отвлечь его от реальных ресурсов предприятия и занять на некоторое время и при этом собрать информацию о местоположении атакующего, его инструментах и методах атак — то есть всё необходимое, чтобы обнаружить и остановить пропущенную атаку.



После внедрения Deception инфраструктура организации начинает состоять из двух слоев: реального и ложного. Причем поддельный слой выглядит гораздо более привлекательным и заманчивым для злоумышленника. Развернутые ловушки и приманки «принимают удар на себя», увлекают злоумышленника в сети фиктивной инфраструктуры, тем самым выигрывая время для принятия контрмер, что приводит к сохранности реальных активов.

1.2 Техническое устройство решения

Control Center – Основной элемент системы, на котором размещены основные компоненты и логика работы системы. Используется для управления всей платформой.

Supervisor – Сервер с ложными сетевыми ловушками.

Agents - Агенты собирают информацию об операционной системе, конфигурации ОС и прикладного ПО, процессах и действиях пользователя. Агент размещается на пользовательских компьютерах сотрудников.

2 КОНФИГУРИРОВАНИЕ

Обзор интерфейса Гарда Лабиринт

Интерфейс Гарда Лабиринт состоит из панели разделов и основной рабочей области.

Панель разделов (1) расположена в левой части экрана и предназначена для навигации по основным разделам системы.

Рабочая область (2) в зависимости от текущего раздела отображает реестр записей раздела (например, в разделе Агенты — список всех агентов).

Разделы Гарда Лабиринт

2.1 Раздел [Главная]

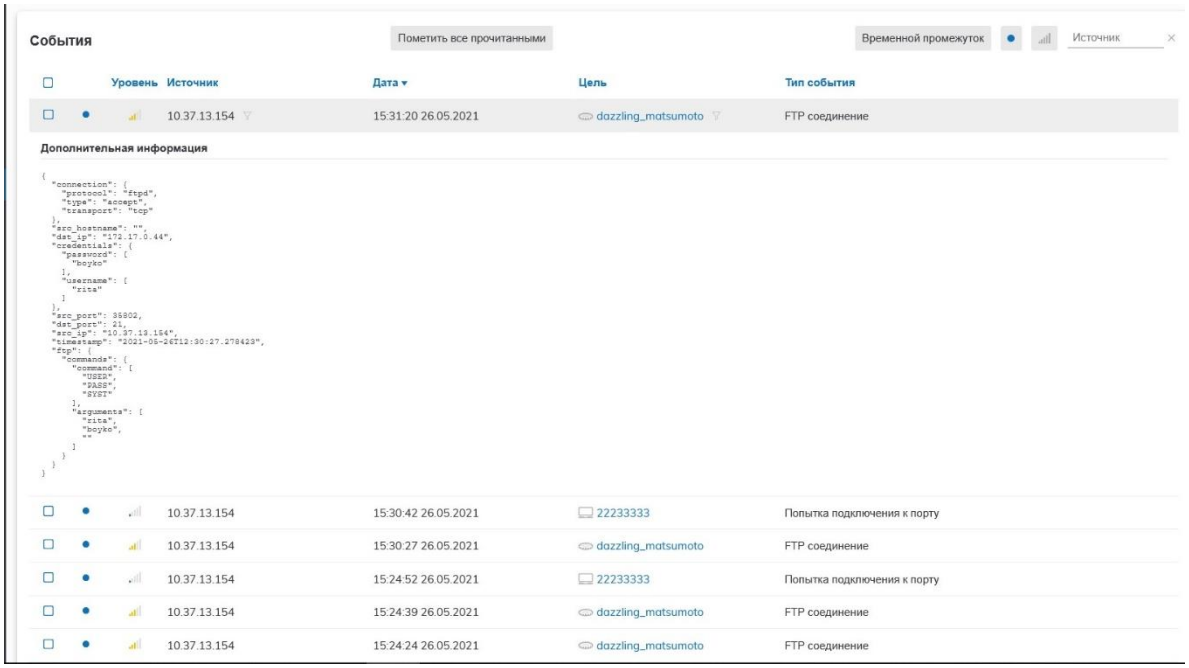
На главной странице отображается сводная информация по системе:

- Супервизоры – общее количество установленных Супервизоров;
- Машины – общее количество установленных машин;
- Ловушки – общее количество созданных ловушек;
- Пользователи – количество пользователей системы;
- События – количество событий, которые зафиксировала система.

Также на главной странице отображается список последних событий системы и показатель событий за сутки.

2.2 Раздел [События]

Раздел [События] создан для просмотра и управления событиями. Событие – запись, которая создается в системе, вследствие обнаружения в режиме реального времени атак и нарушений критериев политик безопасности. Используя данный раздел, можно получить подробную информацию об инциденте, определить уровень угрозы, а также получить дополнительную информацию по событию.

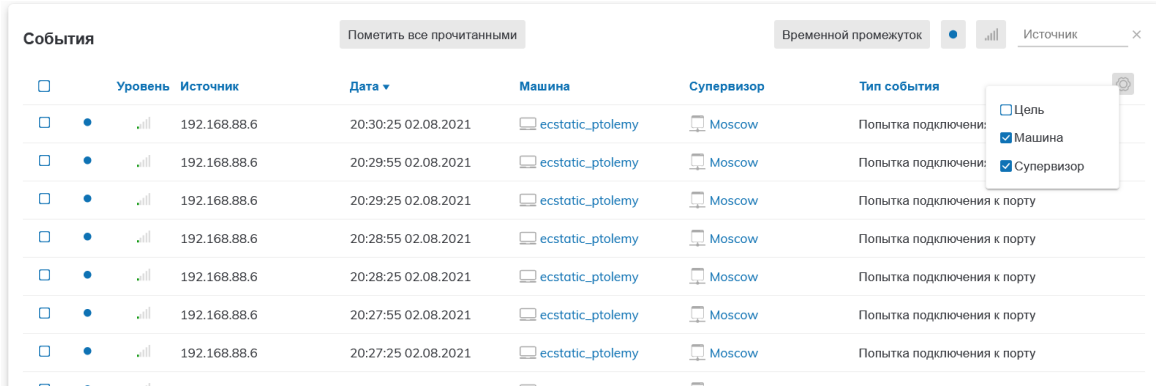


Реестр раздела состоит из следующих колонок:

- ID – уникальный идентификатор события;
- Уровень – уровень угрозы события;
- Источник – IP адрес источника;
- Дата – дата и время события;
- Цель – ловушка, на которую было направлено действие злоумышленника;
- Машина – машина на которую было направлено действие злоумышленника:
- Супервизор – супервизор который управляет атакованной целью;
- Тип события – указывает на действия злоумышленника.

При нажатии на запись откроется окно с дополнительной информацией по событию, в котором содержится информация о подключении к ловушке или машине.

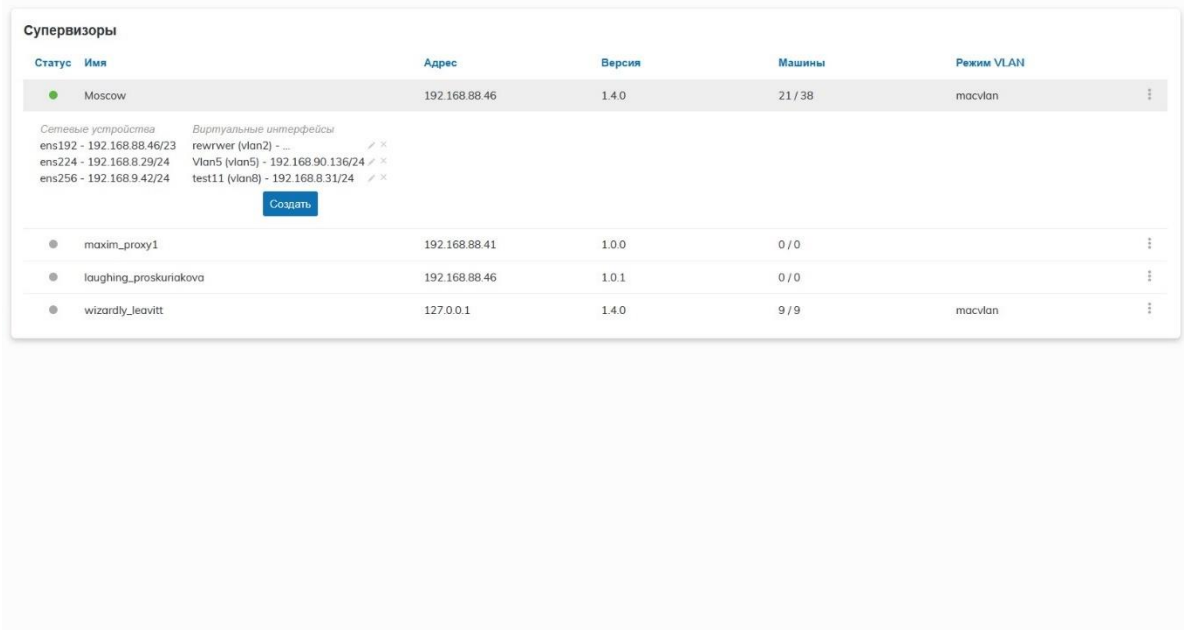
В правой части списка столбцов нажатием на шестеренку можно выбрать отображаемые поля:



2.3 Раздел [Супервизоры]

Раздел [Супервизоры] отражает информацию об установленных в сети супервизорах. Супервизор – это один из основных компонентов системы. Он представляет из себя сервер с ложными сетевыми объектами. Более подробная информация о супервизорах и их установке содержится в документе по установке системы Гарда Лабиринт.

С помощью данного раздела можно управлять супервизорами и создавать для них виртуальные интерфейсы.



2.3.1 Управление супервизором.

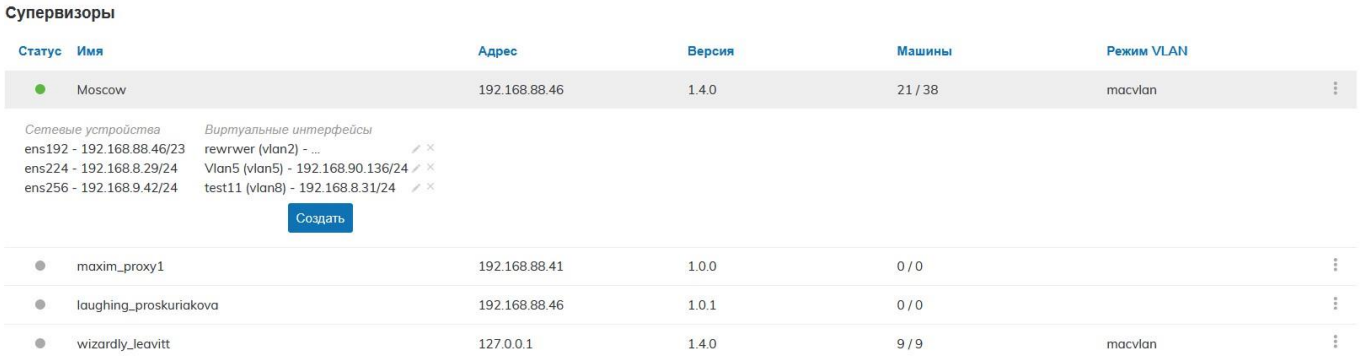
Управление осуществляется нажатием на ПКМ на записи с нужным супервизором. Основные действия:

- Редактировать
- Перезапустить
- Изменить режим VLAN
- Удалить
- Журнал событий

При нажатии на нужный супервизор отобразится информация по подключенным к нему сетевым устройствам и виртуальным интерфейсам.

Режим VLAN задается автоматически «macvlan» при установке супервизора. Существует два режима:

- macvlan – mac адрес каждого виртуального интерфейса будет отличаться от родительского интерфейса (рекомендуемый режим)
- ipvlan - mac адрес каждого виртуального интерфейса будет совпадать с родительским интерфейсом

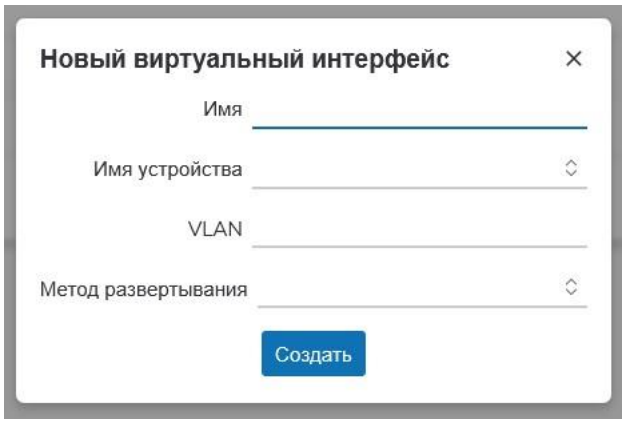


2.3.2 Создание виртуальных интерфейсов

Виртуальные интерфейсы используются, если сеть заказчика разбита на подсети (VLAN). Для размещения ловушек внутри определенной подсети необходимо создать виртуальный интерфейс:

1. Выбрать супервизор, на котором будет создан виртуальный интерфейс и нажать кнопку **Создать**.

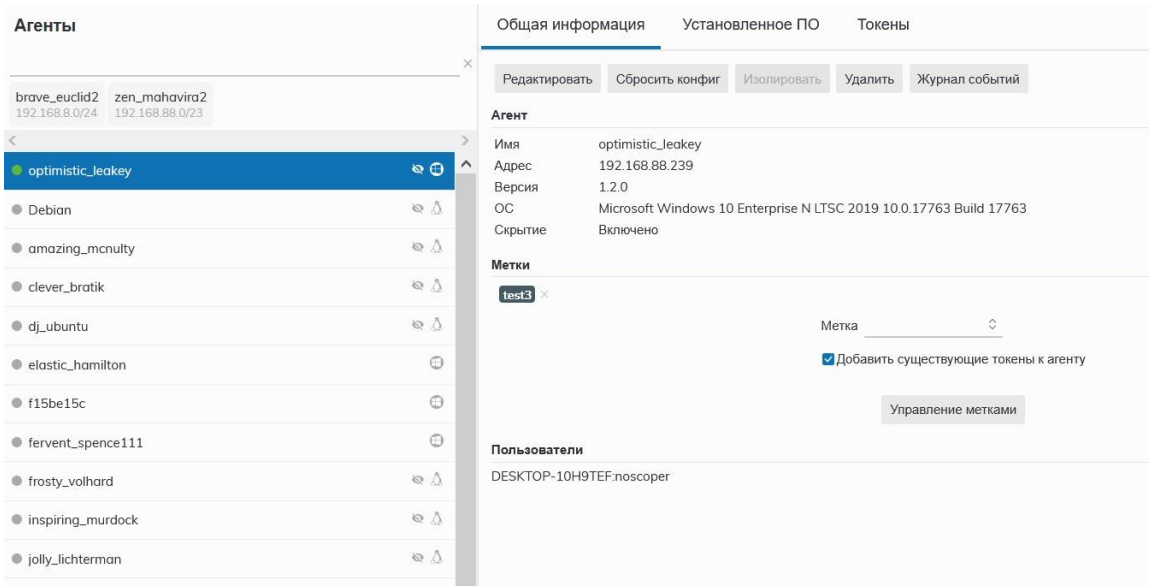
2. Заполнить все необходимые поля. Для создания необходимо указать имяVLAN, номер VLAN, устройство, от которого будет создаваться виртуальный интерфейс, и выбрать метод развертывания (Dynamic/Static. В первом случае IP адрес будет присвоен автоматически, во втором случае Ip адрес задается вручную)



2.4 Раздел [Агенты]

Агент собирает информацию об операционной системе, конфигурации ОС и прикладного ПО, процессах и действиях пользователя. Агент размещается на пользовательских компьютерах сотрудников. Агенты также используются для размещения токенов на пользовательских машинах сотрудников. Токен – это набор авторизационных данных, которые используется для подключения к ловушкам. В случае компрометации компьютера сотрудника злоумышленник сможет обнаружить токены, которые приведут его к ловушкам, что впоследствии поможет обнаружить атаку на систему. Агенты поддерживают работу со следующими операционными системами Debian, CentOS и Windows.

2.4.1 Основная информация



Слева отображены все агенты, которых можно фильтровать по подсетям, в которых они расположены. У каждого агента есть индикатор активности, который обозначает состояние машины в реальном времени (Зеленый – агент активен; Серый – агент выключен; Желтый – превышено количество лицензий). При выборе определенного агента отображается информация по агенту. Доступна следующая информация:

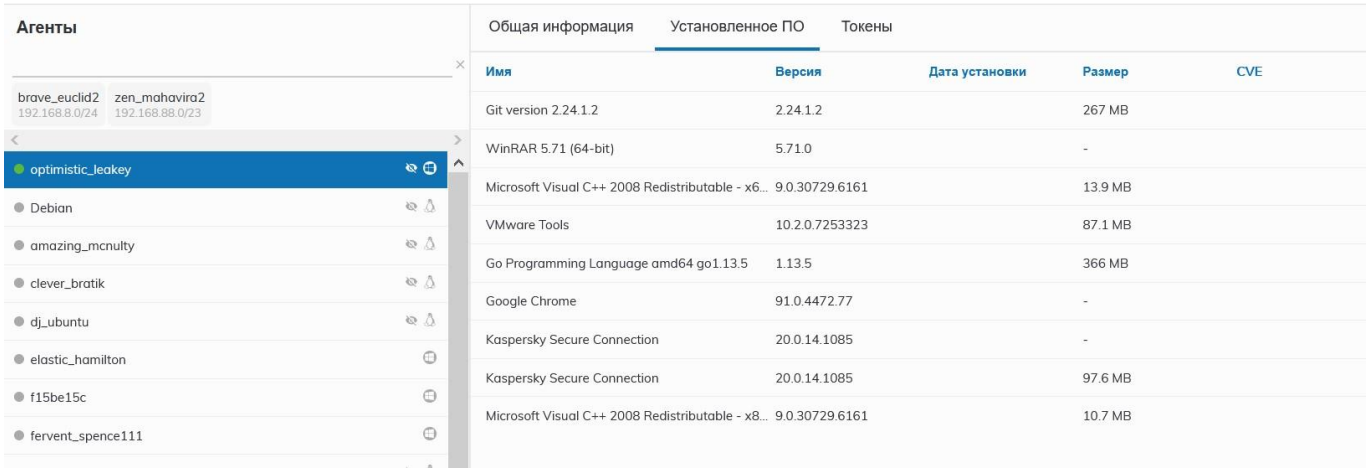
- Общая информация – адрес компьютера, ОС, пользователи;
- Установленное ПО – Отображает список ПО, установленного на агенте;
- Токены – меню управления токенами.

2.4.2 Метки

Метки используются для группировки агентов. Например, используя метки, можно отдельно выделить различные отделы компании, что позволит быстрее настроить систему.

2.4.3 Установленное ПО

После установки агента запускается сбор информации по программному обеспечению. В результате в интерфейсе Гарда Лабиринт будет отображен набор ПО, установленный на машине.

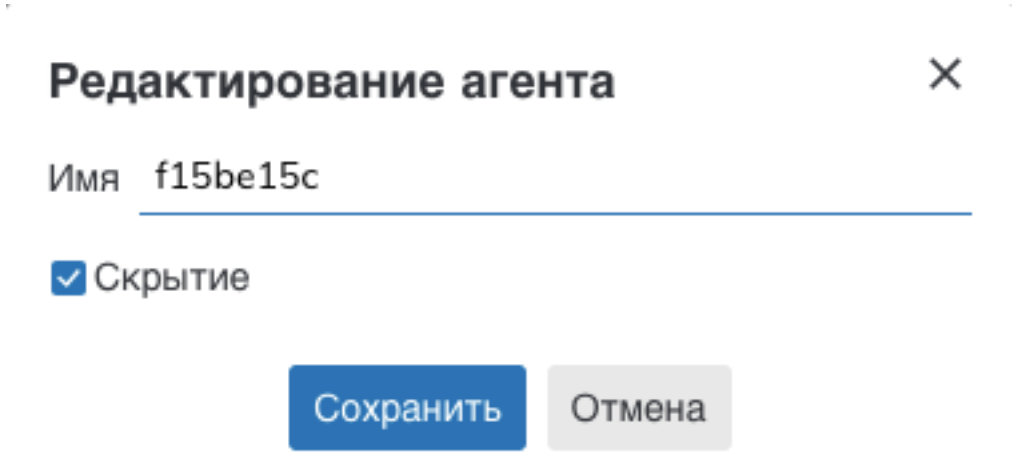


2.4.4 Работа с агентами

Для работы с агентами используется следующее меню:

Редактировать

Действие позволяет отредактировать настройки агента.



- Скрытие – скрывать агента в операционной системе.

Сбросить конфигурацию

Действие сбрасывает все настройки агента.

Изолировать ***(функционал в разработке)***

Действие изолирует рабочую машину пользователя (Отключает на ней сетевое подключение), на которой установлен агент.

Удалить

Действие удаляет агента с пользовательского компьютера и из интерфейса Гарда Лабиринт.

Журнал событий

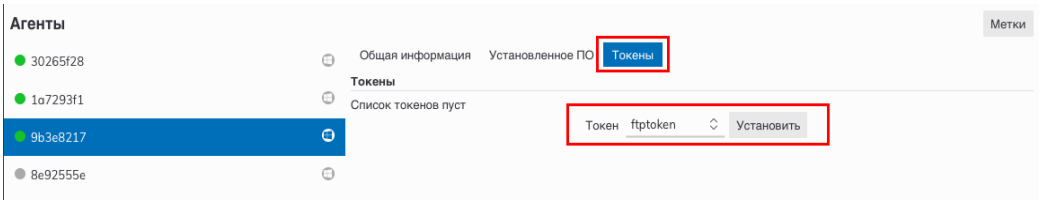
Отображает список последних событий, произошедших с выбранным агентом.

2.4.5 Токены

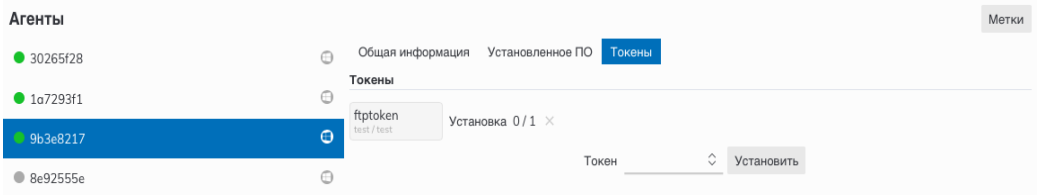
Данный функционал используется для управления токенами. С его помощью можно устанавливать и удалять токены на агентах. Работа с токенами происходит в фоновом режиме. Пользователь, который работает за компьютером с установленным агентом, не заметит установку, удаление или работу с токенами.

2.4.5.1 Размещение токена на агенте

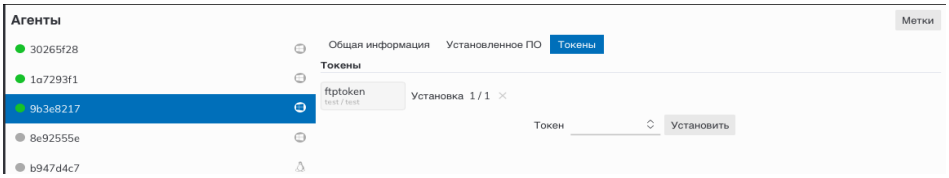
1. В разделе [Агенты] выбрать нужную пользовательскую машину, на которую нужно разместить токен.
2. Перейти во вкладку **Токены**;
3. В поле **Токен** выбрать доступный из списка токен (Создание новых токенов описано в разделе 2.5.4);
4. Нажать на кнопку **Установить**;



5. В интерфейсе отобразится токен с признаком (Установка 0/1);

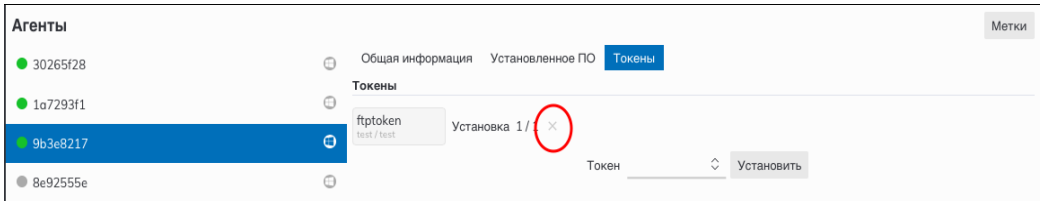


6. После успешной установки в интерфейсе отобразится токен с признаком (Установлен).

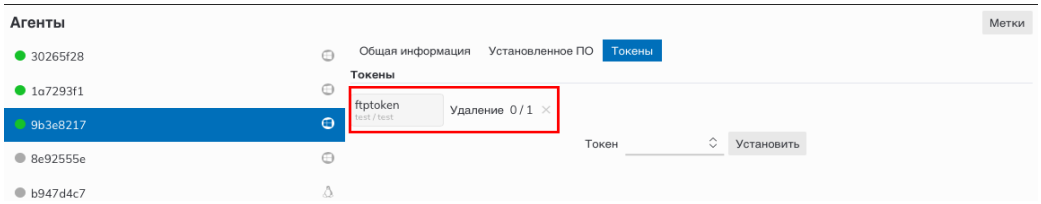


2.4.5.2 Удаление токена с агента

1. В разделе [Агенты] выбрать нужную пользовательскую машину, с которой нужно разместить токен.
2. Перейти во вкладку **Токены**;
3. Выбрать нужный токен и нажать крестик;



4. В интерфейсе токен будет отображен с признаком (Удаление 0/1);



5. После успешного удаление токен пропадет из интерфейса.

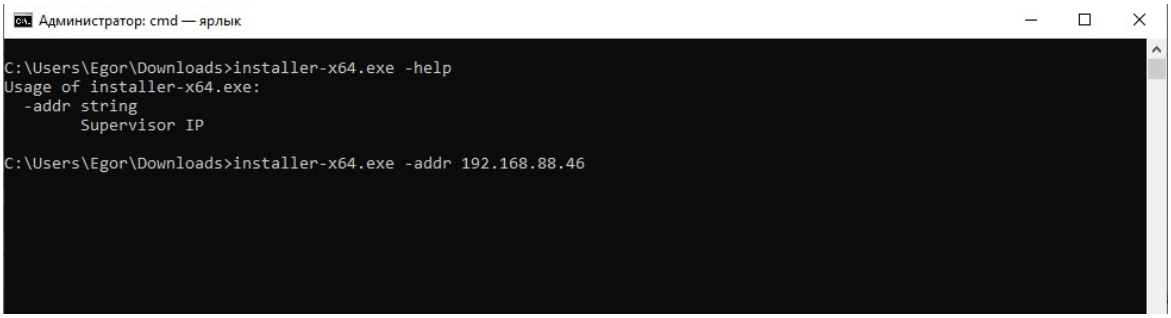
Примечание: Установка и удаление токена будут осуществлены только при наличии соединения с агентом. Для этого компьютер, на котором установлен токен, должен быть включен.

2.4.6 Установка и удаление агентов Windows x64

Установка:

В комплекте с системой поставляется исполняемый файл **installer-x64.exe**. С его помощью можно создавать и устанавливать агенты для систем Windows (от версии 7.1):

1. Открыть командную строку Windows от имени администратора.
2. Перейти в директорию, в которой расположен файл **installer-x64.exe** (переход по каталогу в командной строке осуществляется с помощью команды **cd**)
3. Выполнить следующую команду: **installer-x64.exe -addr (*адрес супервизора*)** (Пример: Создание агента для Windows x64. Адрес Supervisor 192.168.88.46)



4. После выполнения команды агент будет установлен на компьютер.

Примечание: Адрес Supervisor можно посмотреть в интерфейсе системы, перейдя в раздел [Ловушки].

Удаление:

Для удаления агента с рабочего компьютера пользователя (без подключения к интерфейсу Гарда Лабиринт) необходимо:

1. Запустить командную строку (cmd.exe) от имени системы. Для этого потребуется утилита Psexec(https://docs.microsoft.com/en-us/sysinternals/downloads/psexec).

a. PsExec не требует установки, достаточно просто скопировать ее в локальную папку. Для удобства использования можно поместить исполняемый файл в системный раздел (C:\Windows\system32)

b. Запустить командную строку от имени администратора(cmd.exe). Можно перейти в папку (C:\Windows\system32) найти cmd.exe Нажать ПКМ и в контекстном меню выбрать Запуск от имени администратора.

c. Далее ввести команду **psexec.exe -i -s cmd.exe**. Откроется новое окно командной строки.

2. В новом окне ввести команду **sc stop coreservice.**

3. Открыть папку C:\Program Files.

Если все действия в пункте 1 были выполнены корректно, то должна отобразится папка Гарда Лабиринт Agent. Ее необходимо удалить.

Обращайтесь в техническую поддержку, если у вас возникнут вопросы или проблемы при удалении.

2.5 Раздел [Ловушки]

Раздел используется для создания и управления ловушками. Ловушка — эмулированные сервисы под управлением реальных операционных систем (Windows или Linux). Так как у обычных пользователей нет легитимных причин обращаться к этим устройствам, любая попытка взаимодействия с ними будет считаться злонамеренной. Цель размещения ловушек заключается в том, чтобы привлечь внимание злоумышленника, отвлечь его от реальных ресурсов предприятия и занять на некоторое время, и при этом собрать информацию о местоположении атакующего, его инструментах и методах атак — то есть всё необходимое, чтобы обнаружить и остановить пропущенную атаку. Как только злоумышленник совершит попытку подключения к ловушке, система обнаружит это подключение и создаст соответствующее событие в системе.

На данный момент система позволяет имитировать работу следующих сетевых сервисов: FTP, memcache, Mongo, MQTT, MySQL, MSSQL, PPTP, SMB, SSH, TCP/UDP blackhole, Http proxy, RDP, HTTP/HTTPs

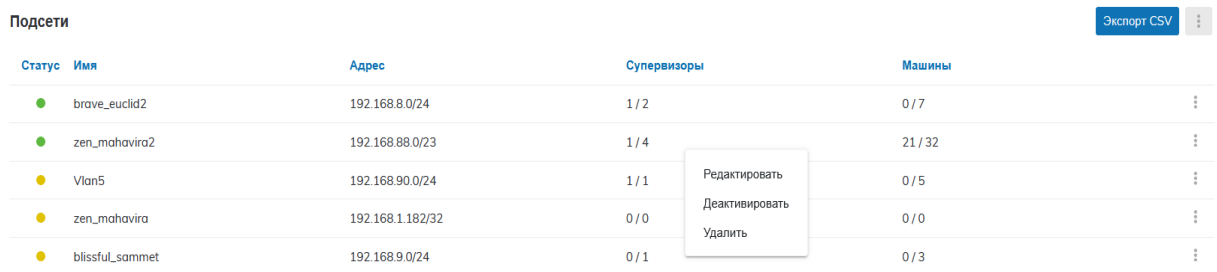
Список подсетей, машин и супервизоров можно сортировать по любому из столбцов на экране для удобства поиска необходимой записи.

2.5.1 Работа с подсетями

Все ловушки размещаются в определенной подсети заказчика. Количество подсетей, которое доступно для работы, определяется типом приобретенной

лицензии. Система отображает в интерфейсе все доступные подсети, даже если допустимое типом лицензии количество превышено.

В системе есть возможность выбирать подсети, с которыми необходимо работать. У каждой подсети есть два статуса: Активна/Деактивирована, зеленый и желтый цвет соответственно. Деактивированные подсети не используются системой и не учитываются в модели лицензирования. Для переключения статуса подсети нужно выбрать подсеть и кликнуть по ней правой кнопкой мыши.

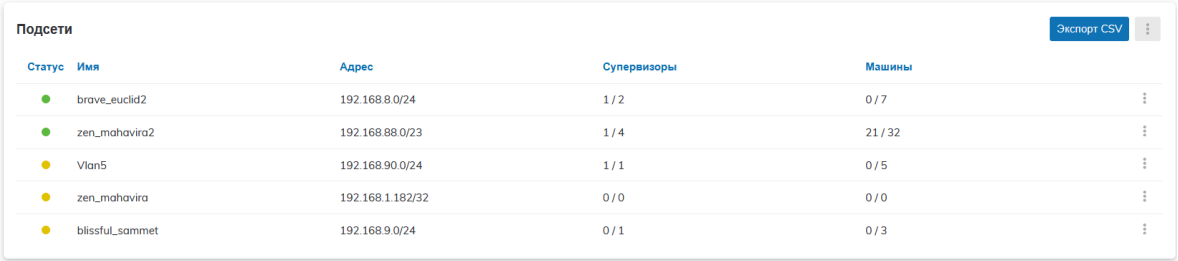


2.5.2 Машины

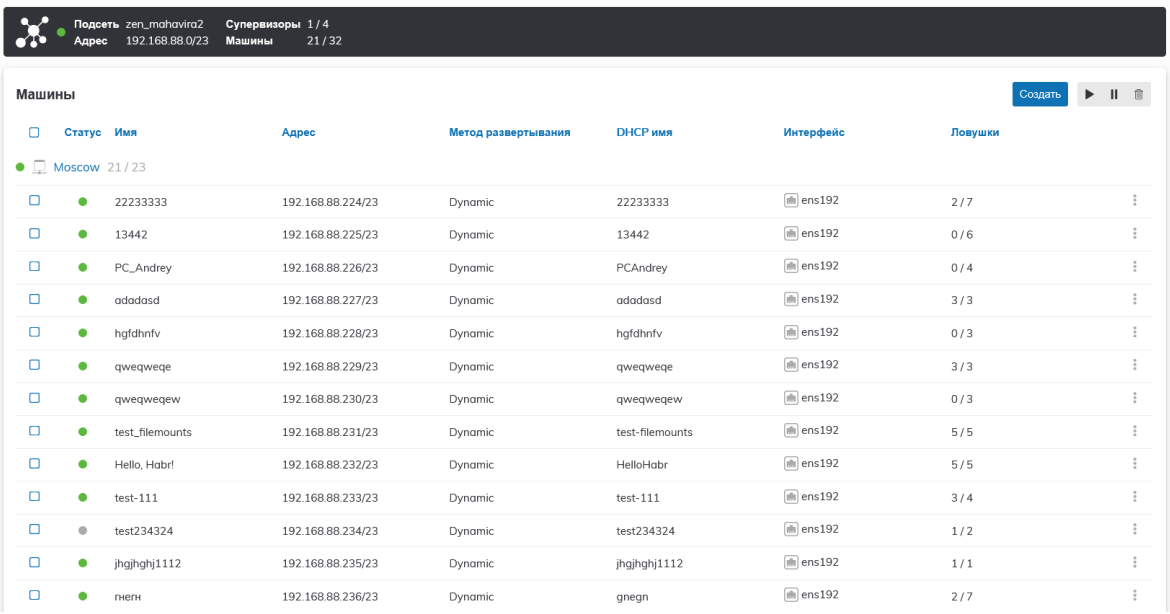
Машина – один из основных компонентов системы Гарда Лабиринт. Машина эмулирует рабочую станцию, на которой впоследствии устанавливаются ловушки.

Создание машин

В разделе [Ловушки] отображены все подсети. Первом делом необходимо выбрать подсеть, в которой разворачивается машина.

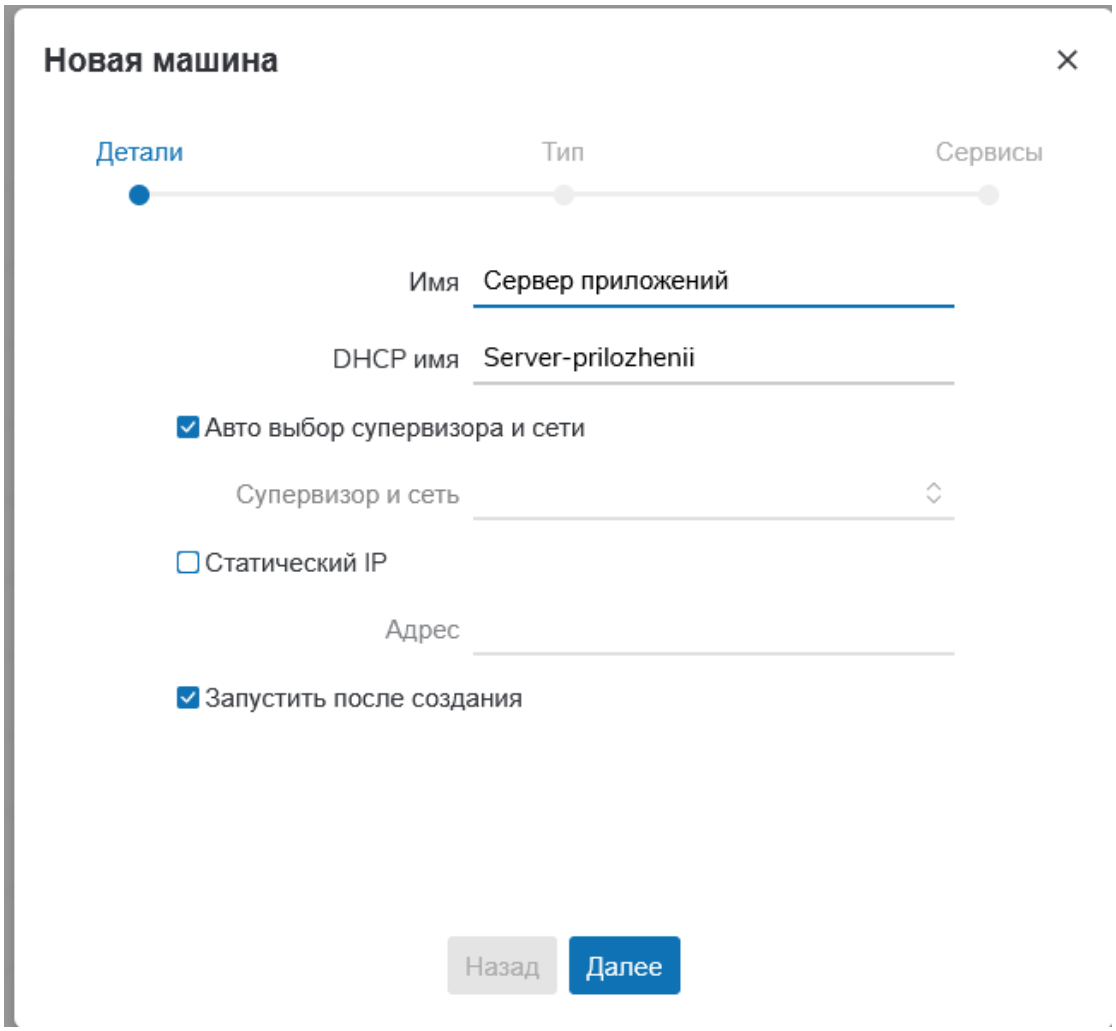


1. Отобразится окно, в котором будут отображены все созданные машины и супервизоры, на которых они размещены.



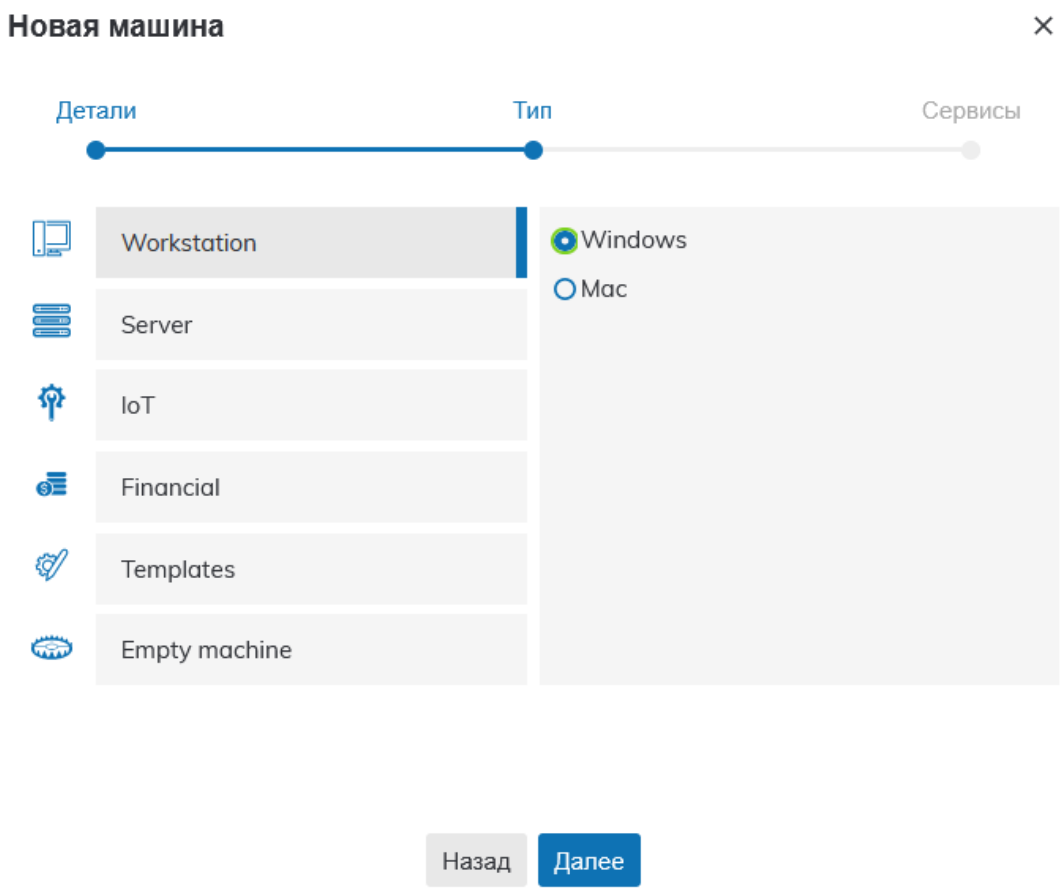
2. Для создания новой машины необходимо нажать кнопку **Создать.**
3. Пользователю будет отображено окно с основными параметрами машины:
    - Имя – Имя машины
    - Авто выбор супервизора и сети – При установленной галочке система автоматически выберет интерфейс, на котором будет создана машина, иначе необходимо будет выбрать интерфейс вручную.
    - IP адрес по DHCP или указать статический адрес.
    - Запускать после создания – автоматически запустит машину после ее создания.

Пример заполнения:



Примечание: по умолчанию используется динамический ip адрес, необходимо убедиться, что внутри сети функционирует DHCP сервер, который присвоит ip адрес.

4. На следующем этапе необходимо выбрать тип машины из вариантов:



Workstation: под управлением ОС Windows или Linux;

Server: под управлением ОС Windows или Linux;

IoT: Point of sale, Phillips Smart Light, Lexmark Printer, Axis network camera;

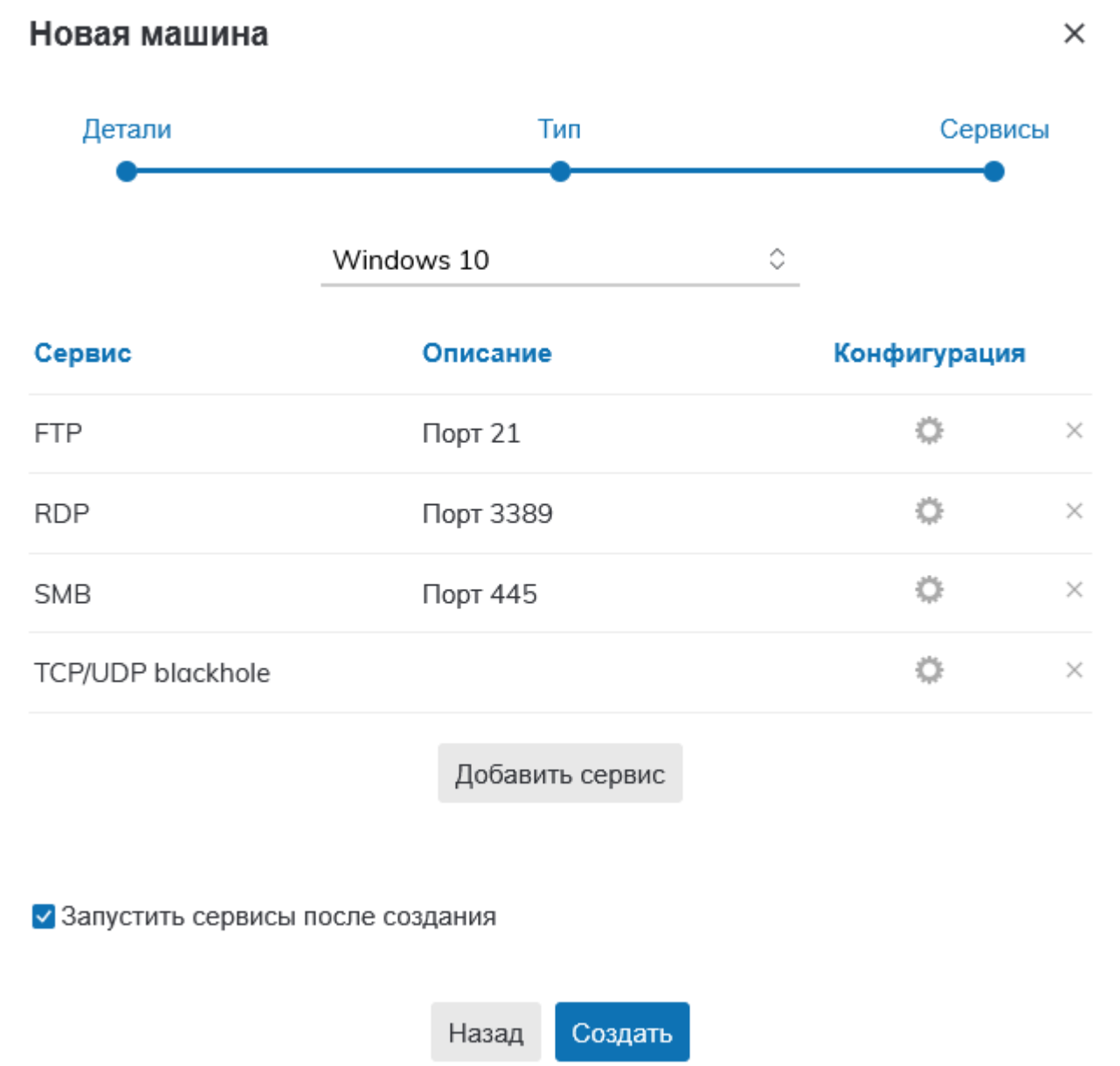
Financial: Swift web platform, Swift lite2, Swift Alliance Gateway, Swift Alliance Access, ATM;

Templates: Для создания шаблона нажмите на любую машину правой кнопкой мыши и выберите опцию "Сохранить шаблон";

Empty machine: Пустая машина.

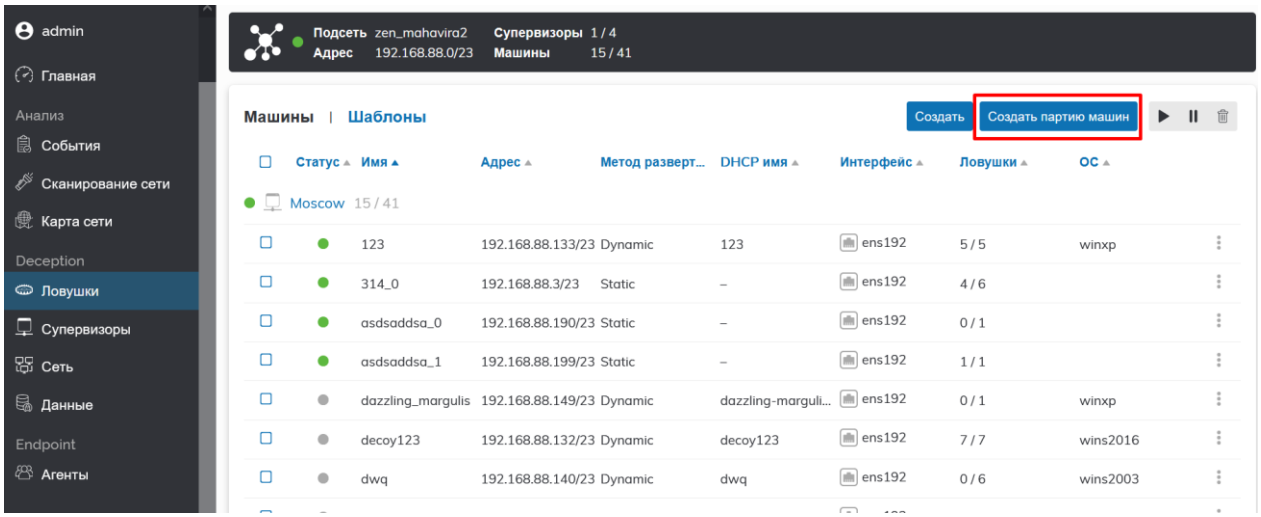
После выбора типа машины жмем «Далее» для определения перечня ловушек.

5. Создание ловушек (сервисов) на машине

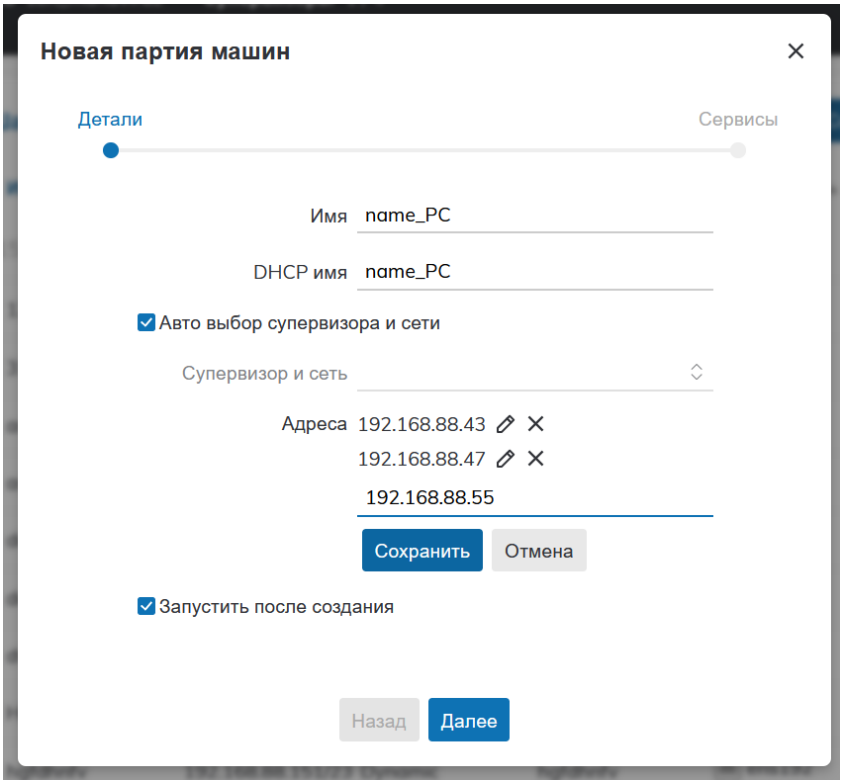


6. Создание парии машин со статической ip адресацией.

Если необходимо по шаблону (набор ловушек) создать несколько машин и назначить им определенный диапазон или список IP адресов, необходимо в списке машин нажать на кнопку «Создать партию машин»



На следующем шаге необходимо задать Имя к которому при создании добавится порядковый номер начиная с 0 и т.д. Добавьте поштучно IP адреса или введите диапазон адресов и нажмите “Далее”

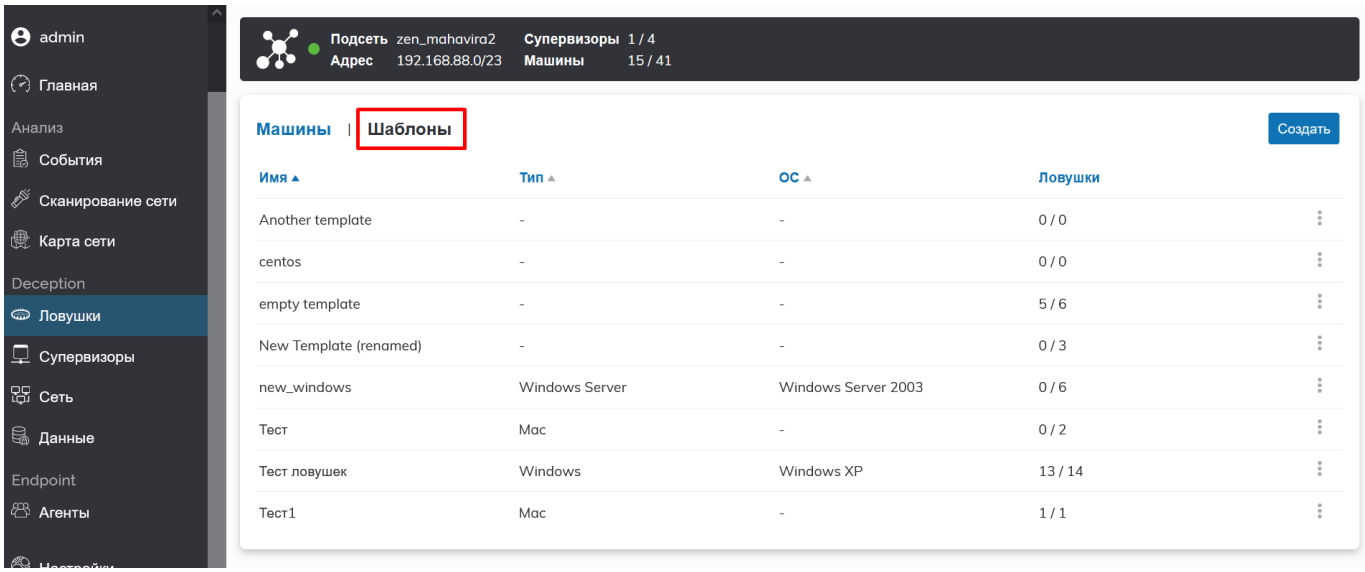


Затем необходимо выбрать заранее подготовленный шаблон в выпадающем списке и нажать на кнопку «Создать».

2.5.3 Шаблоны машин.

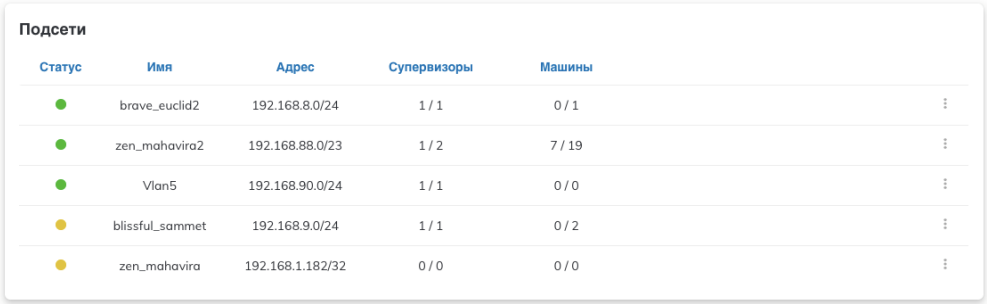
Шаблоны можно создавать как на основе уже существующих машин, нажав на любую машину правой кнопкой маши и выбрать «Создать шаблон» так и в мастере шаблонов, так же в мастере шаблонов вы можете редактировать уже имеющиеся, созданные ранее шаблоны.

Мастер шаблонов находится в списке машин справа от кнопки «Машины»

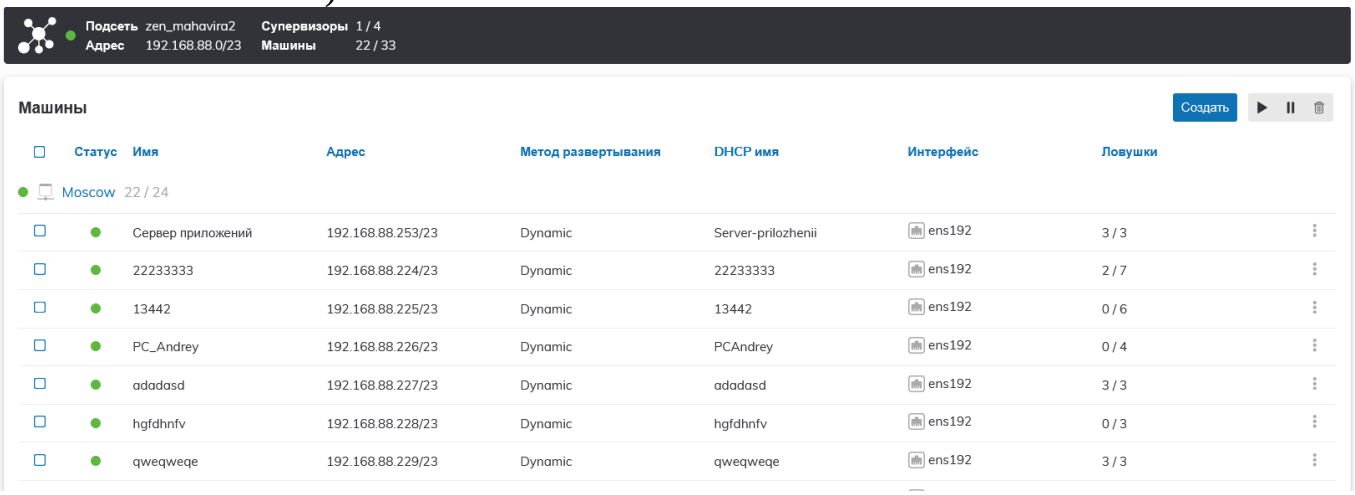


2.5.4 Создание ловушек

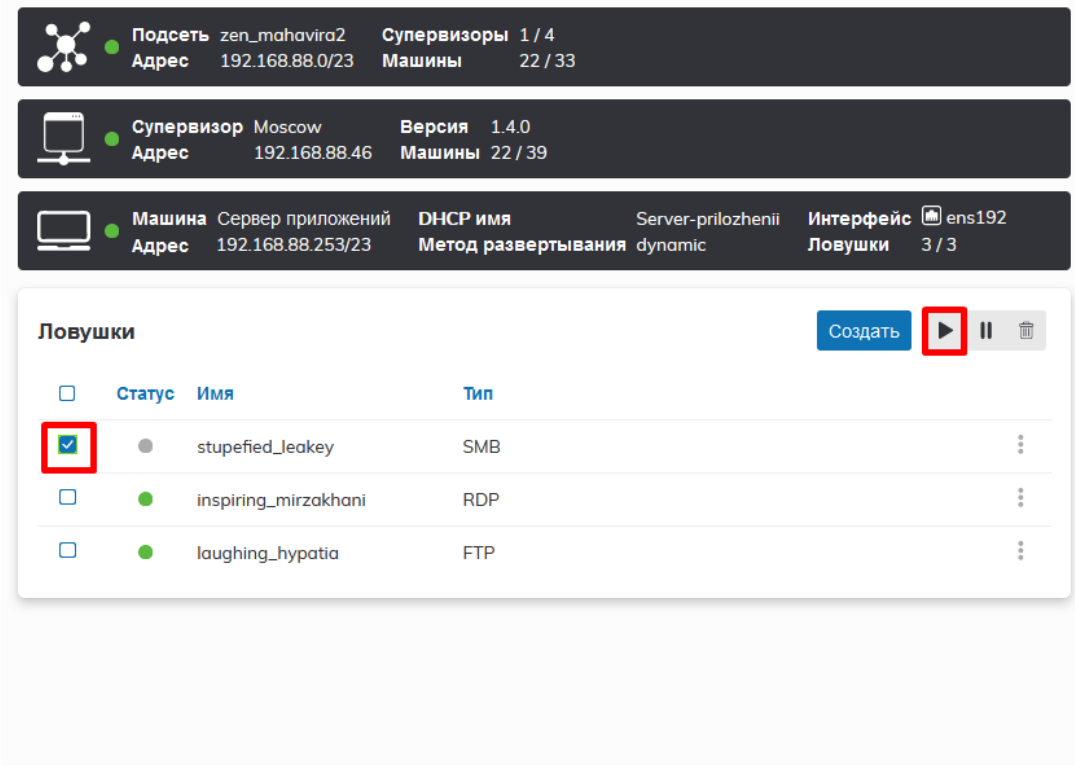
1. Ловушки можно создавать и удалять на уже существующей машине. В разделе [Ловушки] необходимо выбрать подсеть, в которой разворачивается ловушка.



2. Далее будут отображены машины, которые доступны в данной подсети. Необходимо выбрать машину из списка кликнув левой кнопкой мыши или создать новую машину по кнопке Создать (подробнее о создании новой машины в п. 2.5.2).

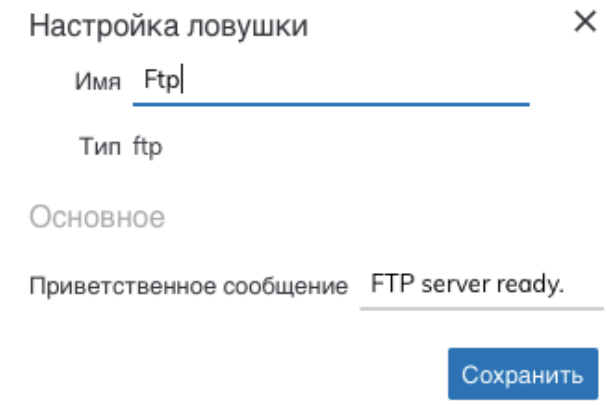


3. Откроется реестр записей с ловушками. Для создания новой ловушки необходимо нажать на кнопку **Создать**.
4. Далее необходимо выбрать тип и имя ловушки. В зависимости от типа ловушки окно с ее настройками будет отличаться. Описание представлено ниже.
5. Для запуска ловушки необходимо установить галочку для нужной ловушки и нажать на кнопку запуска (см. скриншот ниже). Или установить галочку автоматического запуска ловушки при ее создании. (Указывается при создании ловушки)



2.5.4.1 *Создание FTP ловушки*

FTP ловушка эмулирует работу ftp сервера. При подключении к ловушке пользователь увидит приветственное сообщение, которое указывается в настройках ловушки.

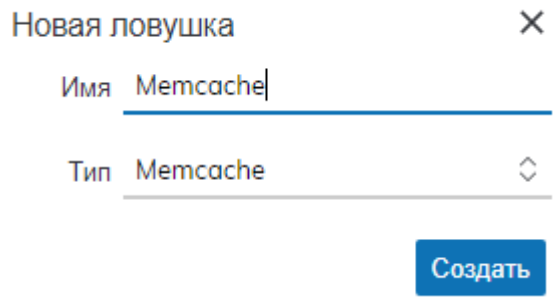


Настройки

- Приветственное сообщение.

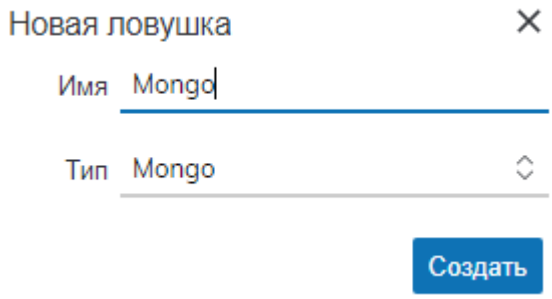
2.5.4.2 *Создание Memcache ловушки*

Memcached — программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы.



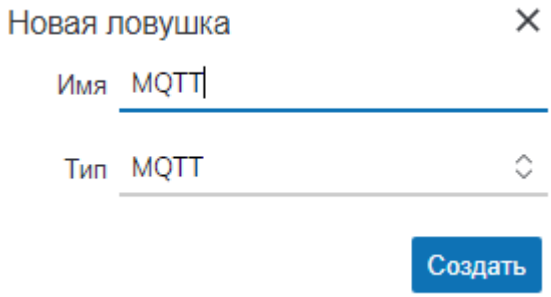
2.5.4.3 *Создание Mongo ловушки*

MongoDB — это документарная база данных. Вместо хранения данных в таблицах, состоящих из отдельных строк, как в реляционных базах, MongoDB сохраняет данные в коллекциях, состоящих из документов.



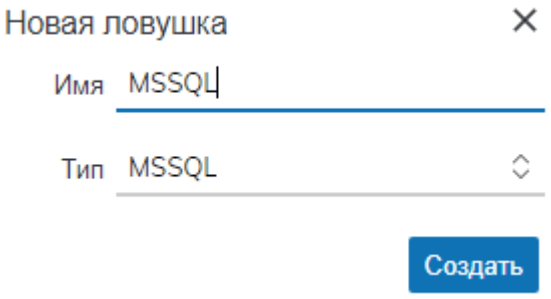
2.5.4.4 *Создание MQTT ловушки*

MQTT или Message Queue Telemetry Transport – это протокол обмена данными, созданный для передачи данных на удаленных локациях, где требуется небольшой размер кода и есть ограничения по пропускной способности канала. Вышеперечисленные достоинства позволяют применять его в IoT.



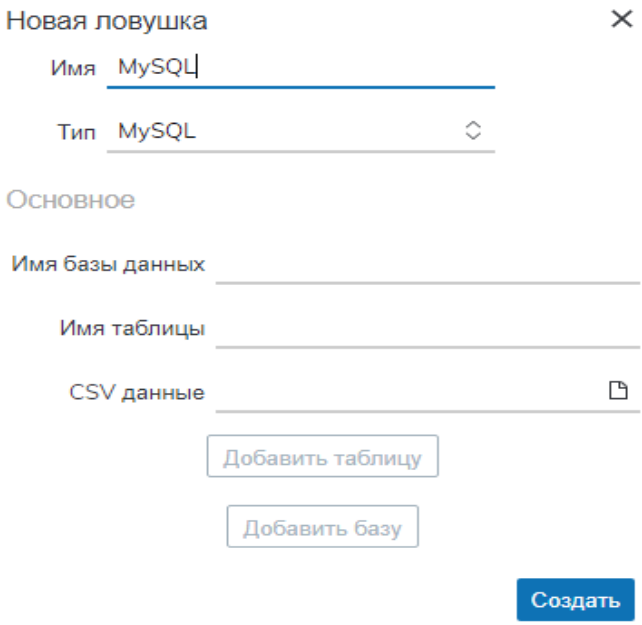
2.5.4.5 *Создание MSSQL ловушки*

Microsoft SQL Server — система управления реляционными базами данных.



2.5.4.6 *Создание MySQL ловушки*

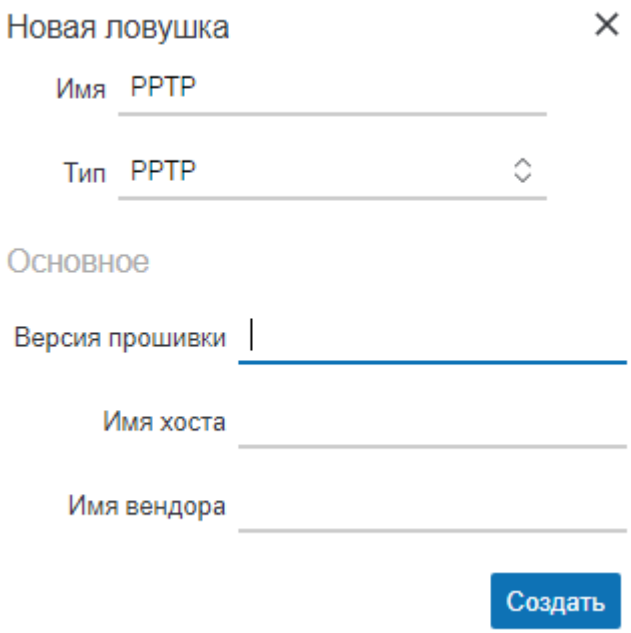
MySQL — свободная реляционная система управления базами данных.



Для ловушки с типом MySQL есть возможность дополнительно создавать таблицы базы данных, это позволит более правдоподобно эмулировать сервисы. Кнопки **Добавить таблицу** и **Добавить базу** служат для добавления дополнительных таблиц и баз.

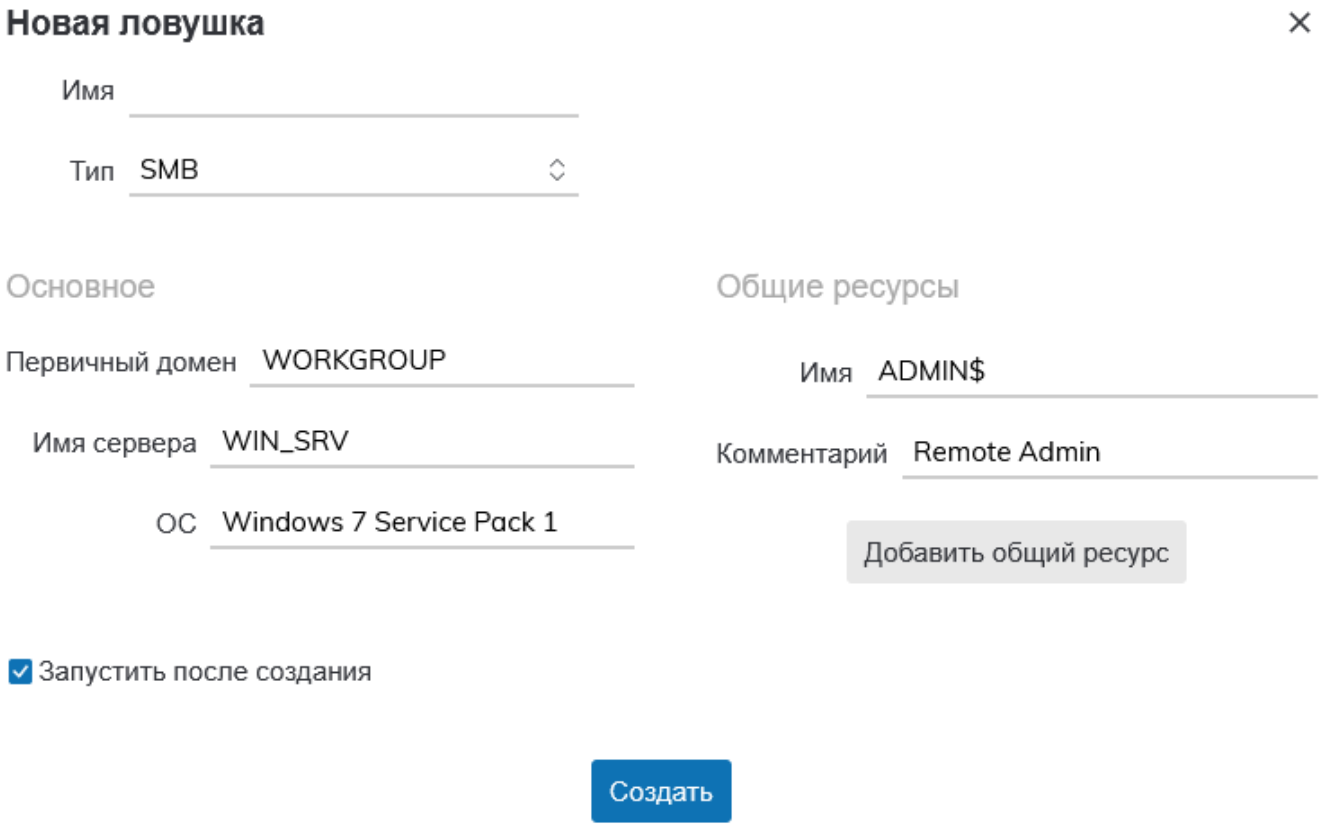
2.5.4.7 Создание PPTP ловушки

PPTP – это туннельный протокол, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищенной сети. Один из протоколов VPN.



2.5.4.8 Создание SMB ловушки

SMB - сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам.



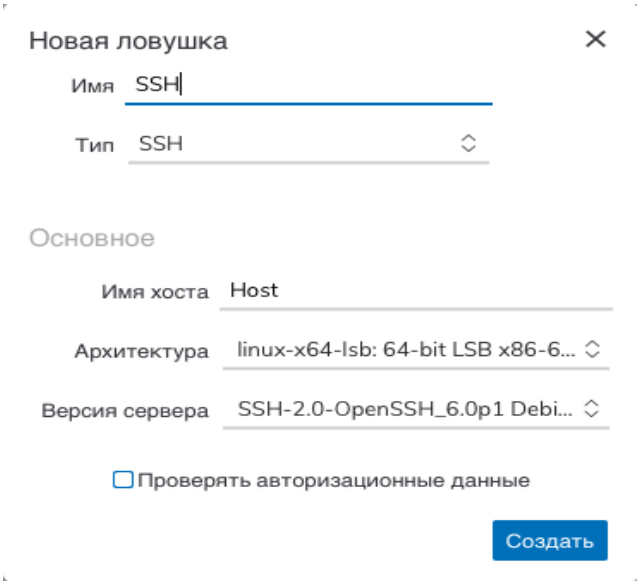
Настройки:

- Основные:
  - Первичный домен
  - Имя сервера
- Общее ресурсы:
  - Имя
  - Комментарий

Для ловушки с типом SMB есть возможность добавлять несколько типов ресурсов и указывать пути к ним. Для это используются кнопки **Добавить путь, Добавить тип, Добавить общий ресурс.**

2.5.4.9 Создание SSH ловушки

SSH сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой. SSH ловушка эмулирует работу протокола SSH на удаленной машине. В событиях возможен просмотр команд, которые использовал злоумышленник.



Настройки

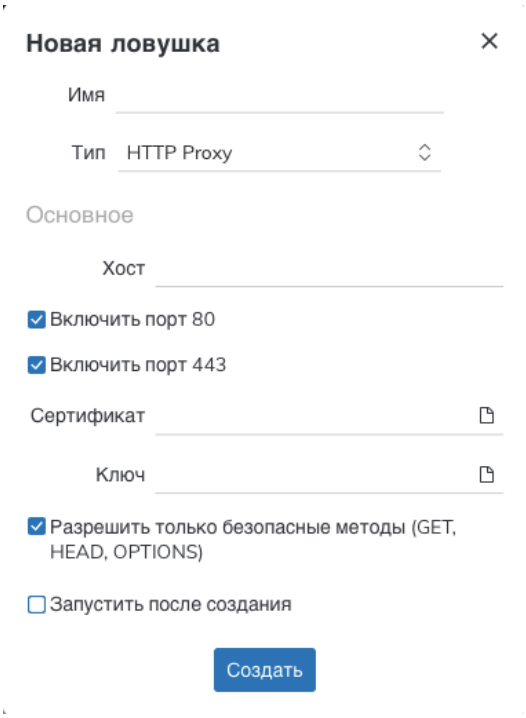
- *Основные*
  - Имя хоста;
  - Архитектура – настройки архитектуры сервера;
  - Версия сервера – настройки версий сервера;

- Проверить авторизационные данные – при неактивном значении не требуются авторизационные данные для подключения.

Примечание: ssh ловушка не сохраняет текущее состояние. Все изменения, выполненные на ней, не сохранятся при повторном подключении.

2.5.4.10 Создание HTTP Proxy ловушки

HTTP Proxy ловушка позволяет создавать ложные сетевые объекты, которые уникальны для каждой компании. Путем проксирования пакетов система создает ложные сетевые объекты, сохраняя при этом корпоративный дизайн компании. Когда злоумышленник попадет на данную ловушку, то внешне он увидит точную копию, клонированного ресурса (Например авторизационную форму с входом на корпоративный портал.) После взаимодействия с этой ловушкой система создаст соответствующее событие в системе. При настройке ловушки можно указать для нее использование небезопасных методов, поэтому использование проксирования будет безопасным.

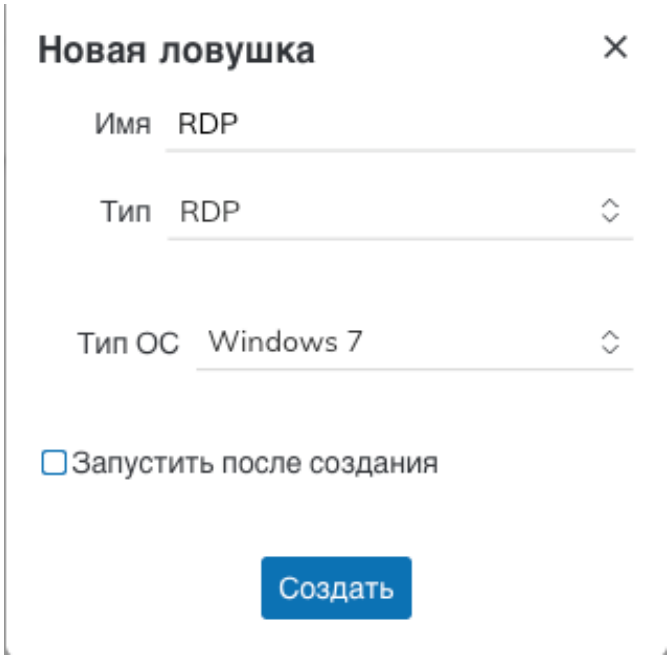


При настройке можно указать порты, по которым можно подключаться к ловушке, загружать сертификаты, ключи и использовать безопасные методы.

Примечание: на одной машине может быть только одна активная ловушка.

2.5.4.11 Создание RDP ловушки

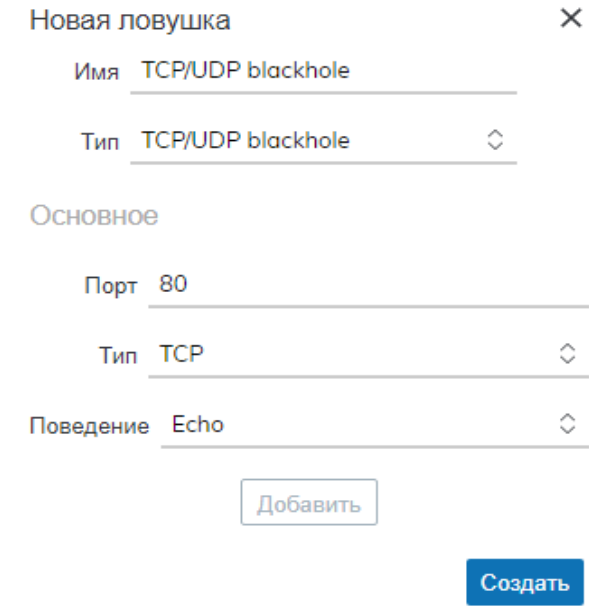
RDP ловушка эмулирует подключение по протоколу RDP.



После успешного подключения будет отображен экран входа.

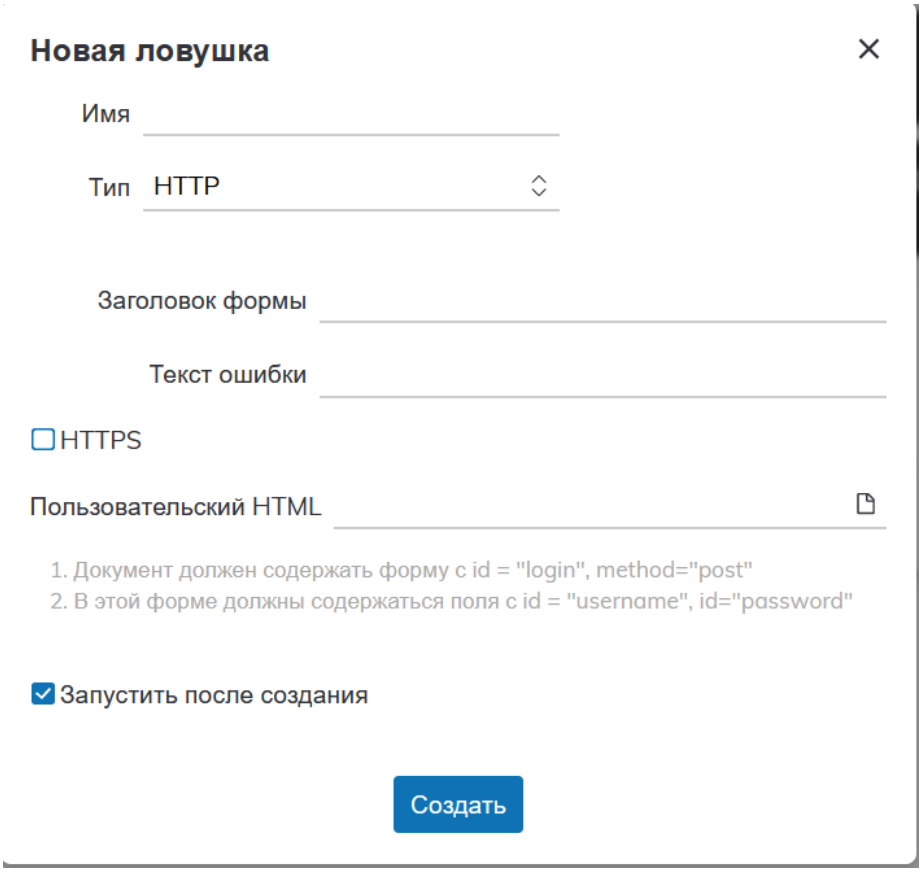
2.5.4.12 Создание TCP/UDP blackhole ловушки

TCP/UDP blackhole ловушка – обнаруживает подключение по соответствующему протоколу (TCP/UDP)



2.5.4.13 Создание HTTP/HTTPs ловушки

Ловушка эмулирует web интерфейс авторизации в корпоративный сервис с возможностью задать только заголовок формы и текст ошибки авторизации или подгрузить свою страницу html (на которой будет поле для ввода логина и пароля) и свой сертификат ssl.

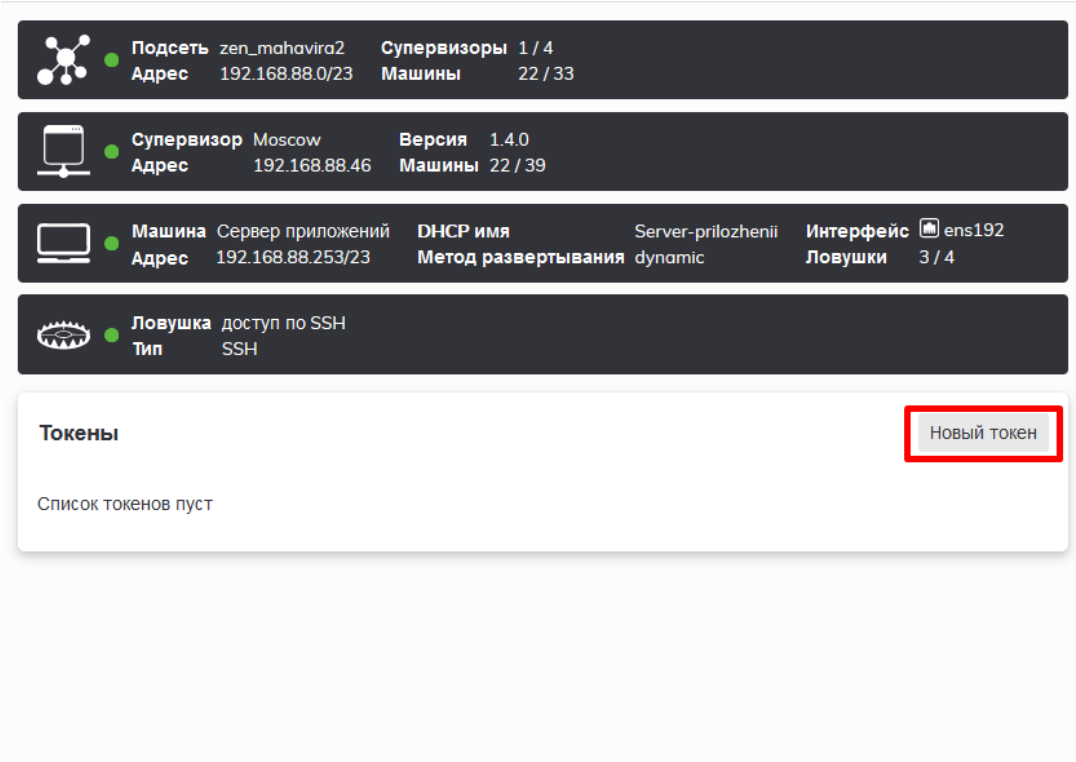


2.5.5 Создание токенов для ловушек

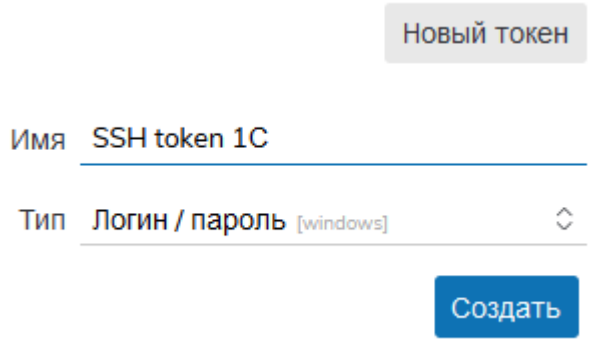
Токены применимы к следующим ловушкам: Ftp, Mongo, MQTT, MSSQL, Mysql, SSH.

Создание токена на примере SSH ловушки:

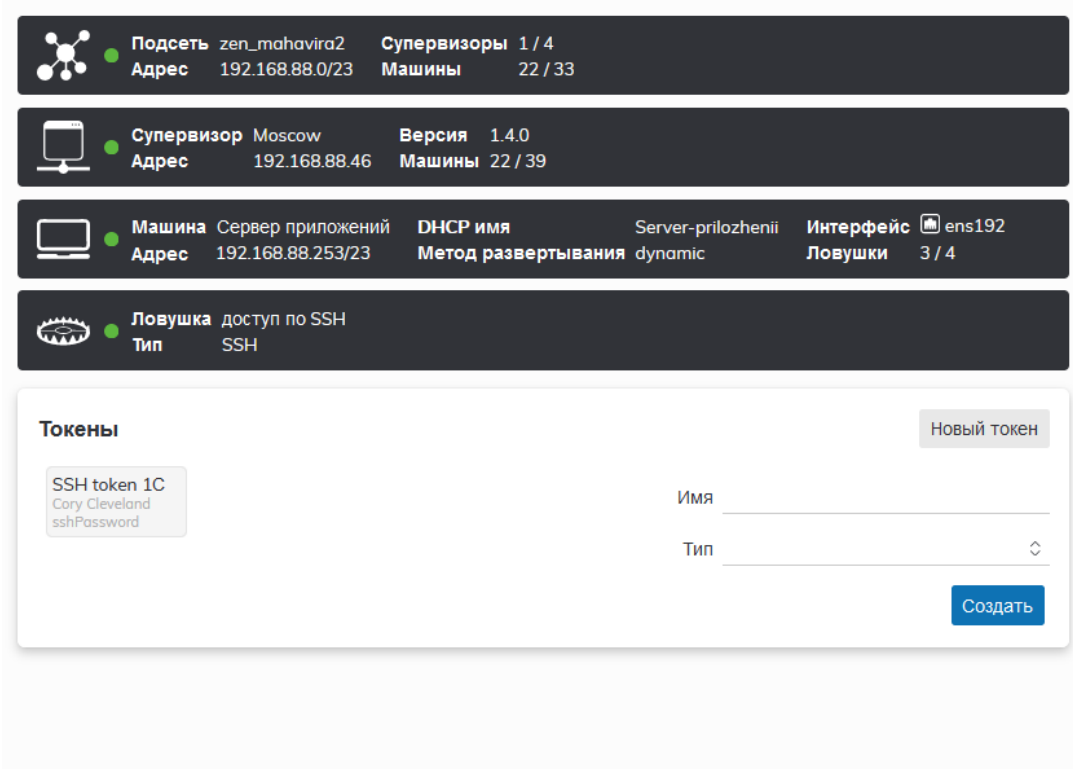
1. Выбрать нужную ловушку и кликнуть по ней.
2. Нажать кнопку **Новый токен**.



3. Указать тип, имя токена и нажать на кнопку **Создать**.

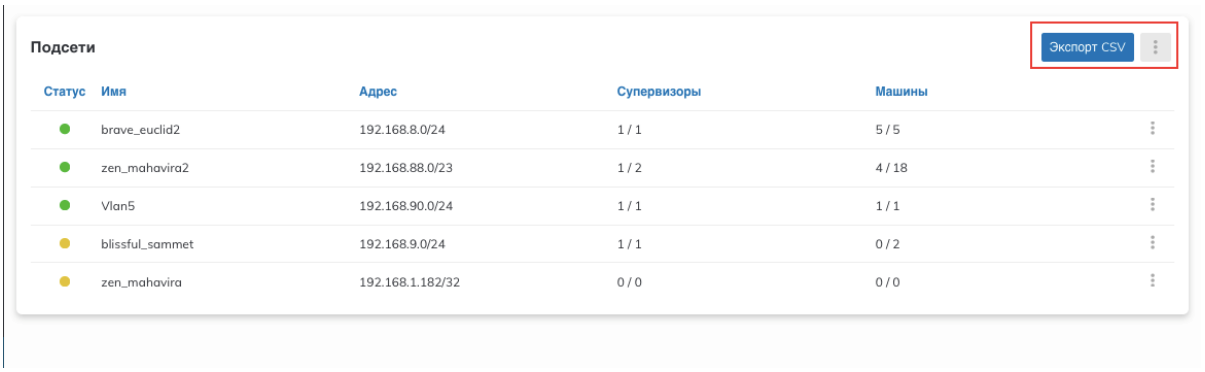


4. После обновления страницы к токену в случайном порядке добавится запись из раздела [Данные]. Логин и пароль от данного пользователя, который содержится в данной записи раздела [Данные], будет валиден при подключении к ловушке.



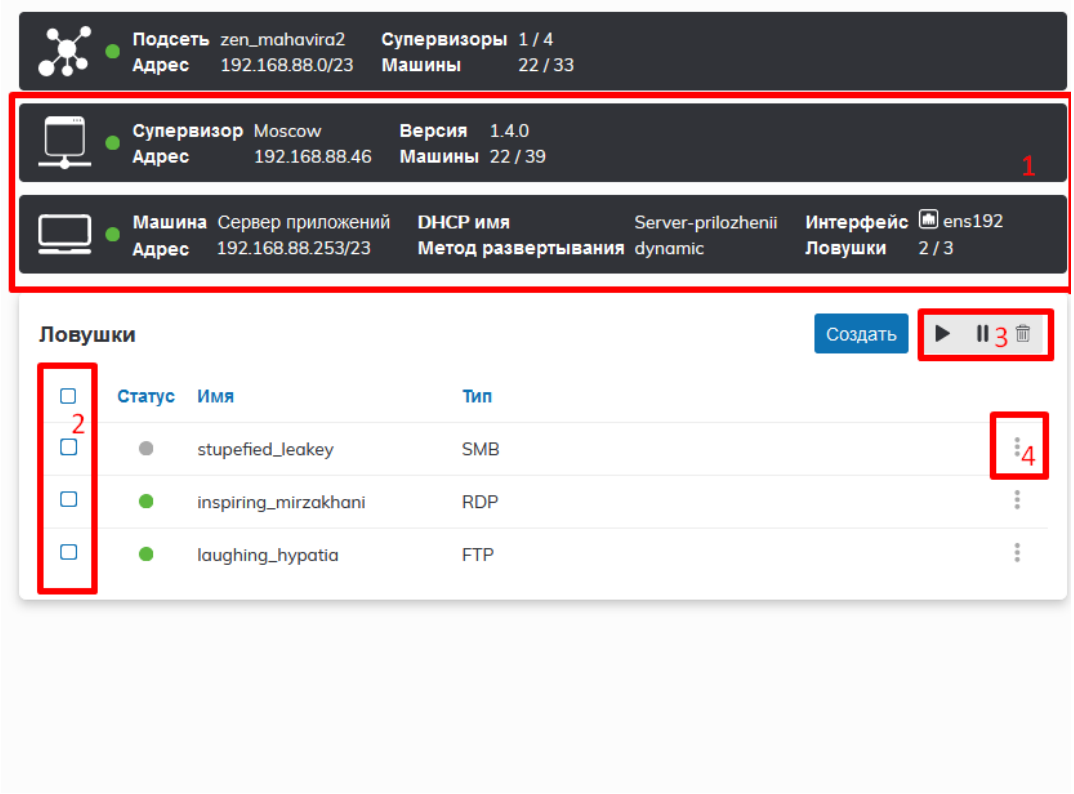
2.5.6 Экспорт в CSV

В системе предусмотрена возможность выгрузки информации по ловушкам в CSV формате. Для этого в разделе нужно нажать соответствующую кнопку, после чего начнется загрузка файла на компьютер пользователя.



2.5.7 Элементы управления

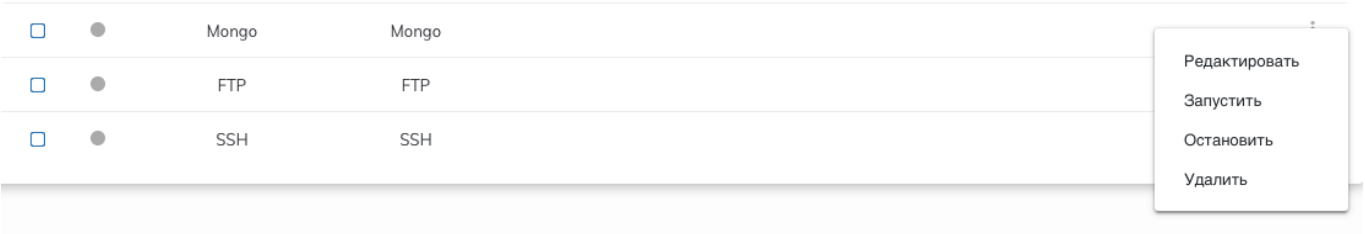
Основные элементы управления представлены на изображении ниже:



В верхней части страницы (1) отображена информация о **Супервизоре** и **машине**, на которой размещены ловушки. Для управления ловушками используется блок кнопок (3) с его помощью можно:

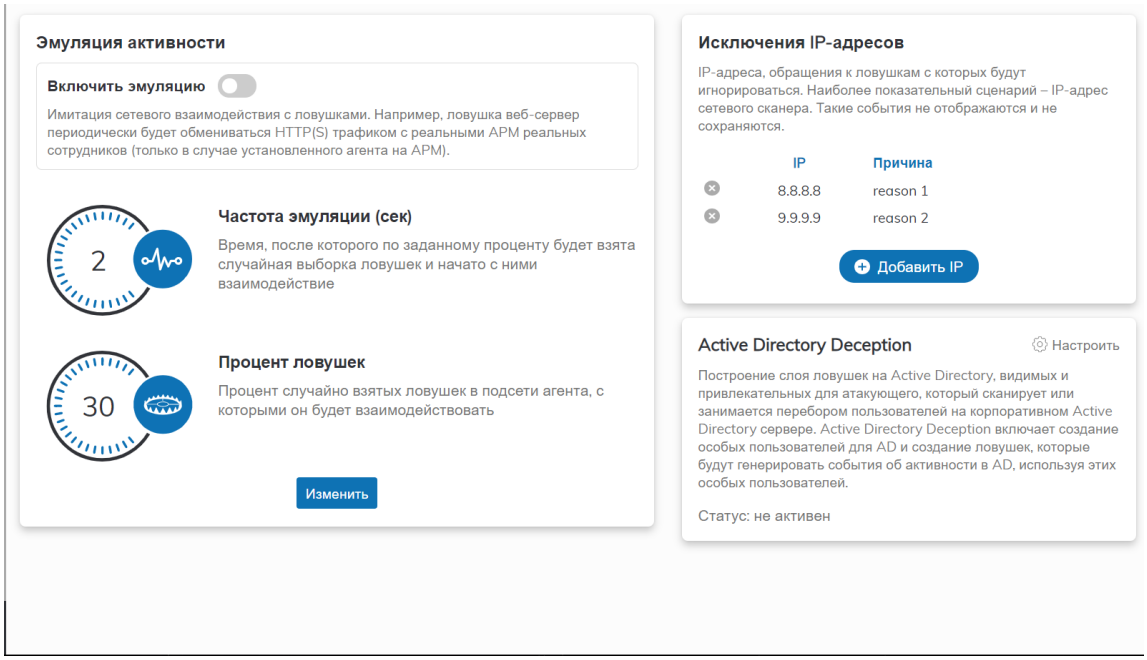
- Запустить ловушку ▶
- Отключить ловушку ⏸
- Удалить ловушку 🗑

Для этого необходимо установить галочку у нужной ловушки (2). Для изменения настроек ловушки необходимо нажать на кнопку (4) или использовать правую кнопку мыши.



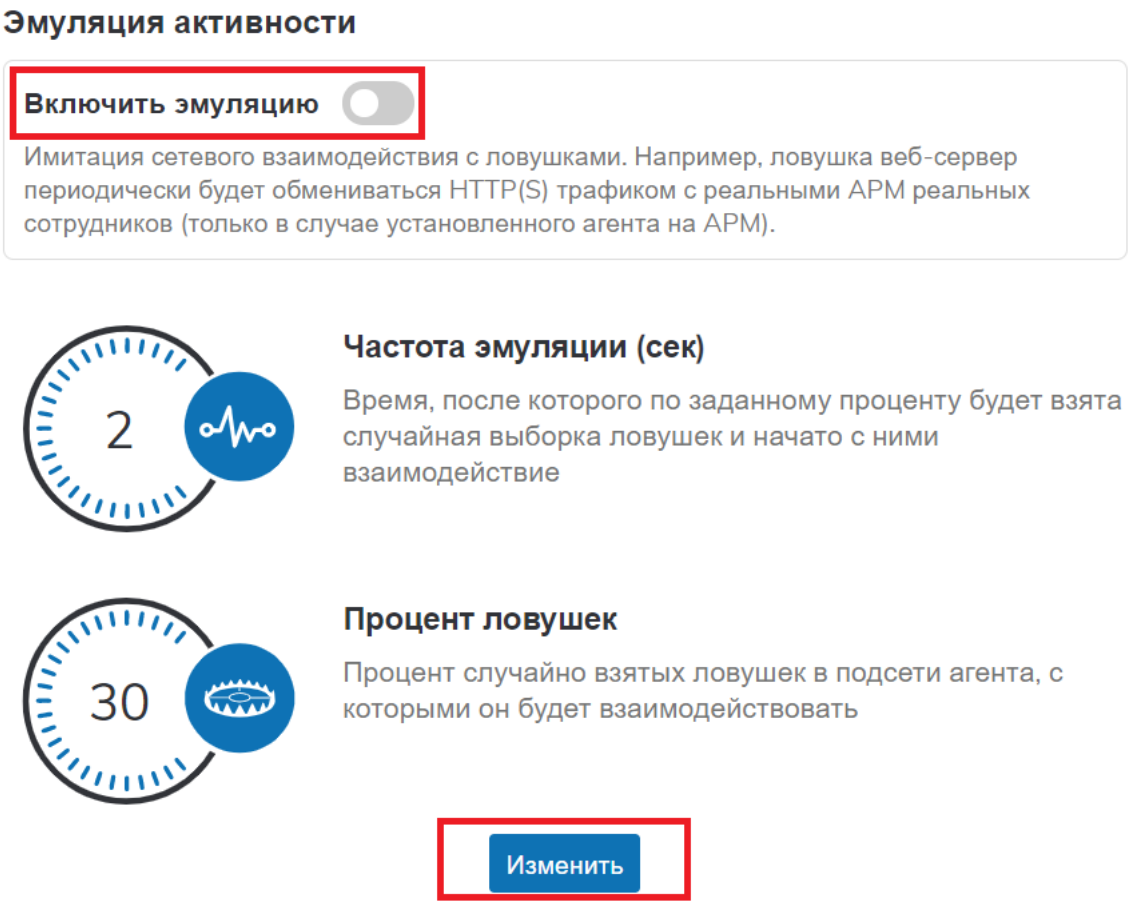
2.6 Раздел [Сеть]

Раздел [Сеть] используется для настройки эмуляции сетевой активности внутри имитированной ИТ-инфраструктуры, настройки исключений ip-адресов и настройки Active Directory.

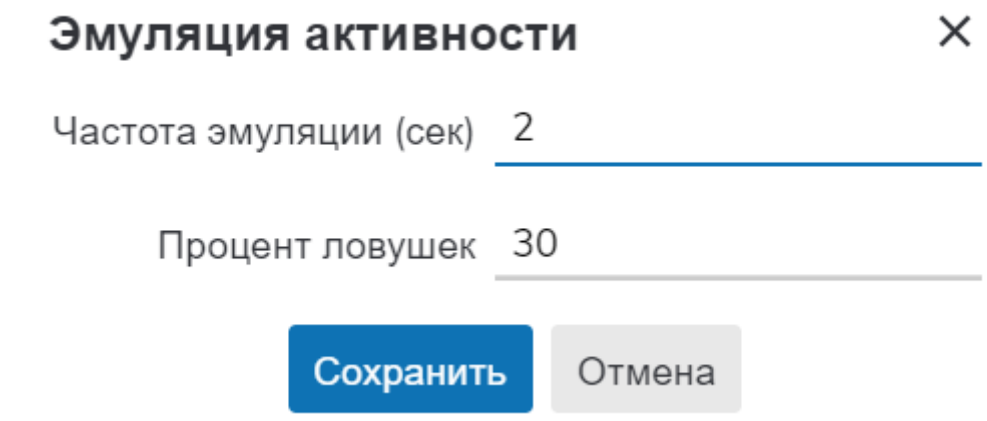


2.6.1 Эмуляция активности

Эмуляция сетевой активности осуществляется за счет того, что агенты периодически обмениваются HTTP(S) с объектами ложной инфраструктуры. Для запуска эмуляции необходимо активировать тумблер **Включить эмуляцию.** Для настройки используется кнопка **Изменить.**



- Частота эмуляции – Частота эмуляции сетевой активности;
- Процент ловушек – Процент ловушек, с которыми будет происходить эмуляция.



2.6.2 Исключенные IP

Данный функционал используется для того, чтобы система не создавала события, где источником является ip адрес, добавленный в исключенный IP. Это

поможет специалистам по безопасности проводить сканирование сети любыми другими средствами и не создать дополнительные события в системе.

При добавлении адреса в исключения есть возможность добавить причину добавления адреса в список исключений.

Для массового импорта списка исключений можно воспользоваться кнопкой «**Импорт CSV**» подготовив список исключений в формате:

- Стандартный файл cvs, разделитель - запятая

- Два столбца, первый - ip адрес в формате x.x.x.x, второй - причина добавления в исключения (без запятых!)

Первая строка - заголовки, не играют значения, но любые должны быть

Со 2 строки данные

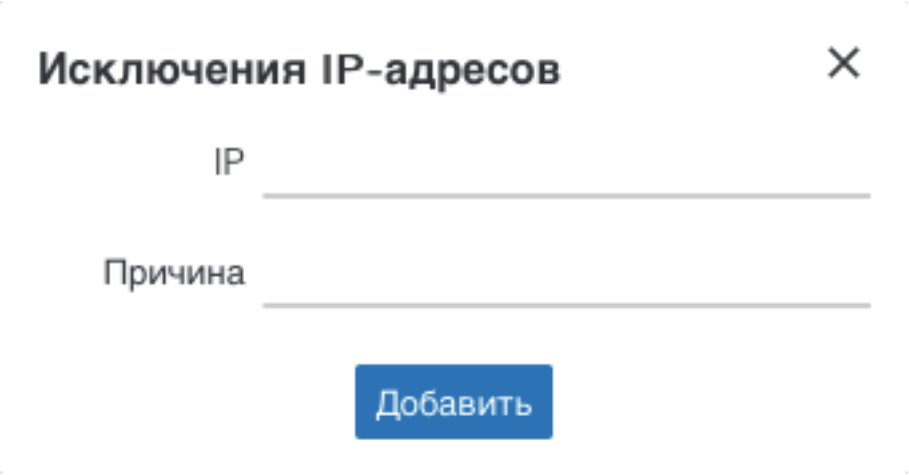
Пример:

ip, reason

1.2.3.4,security scanner

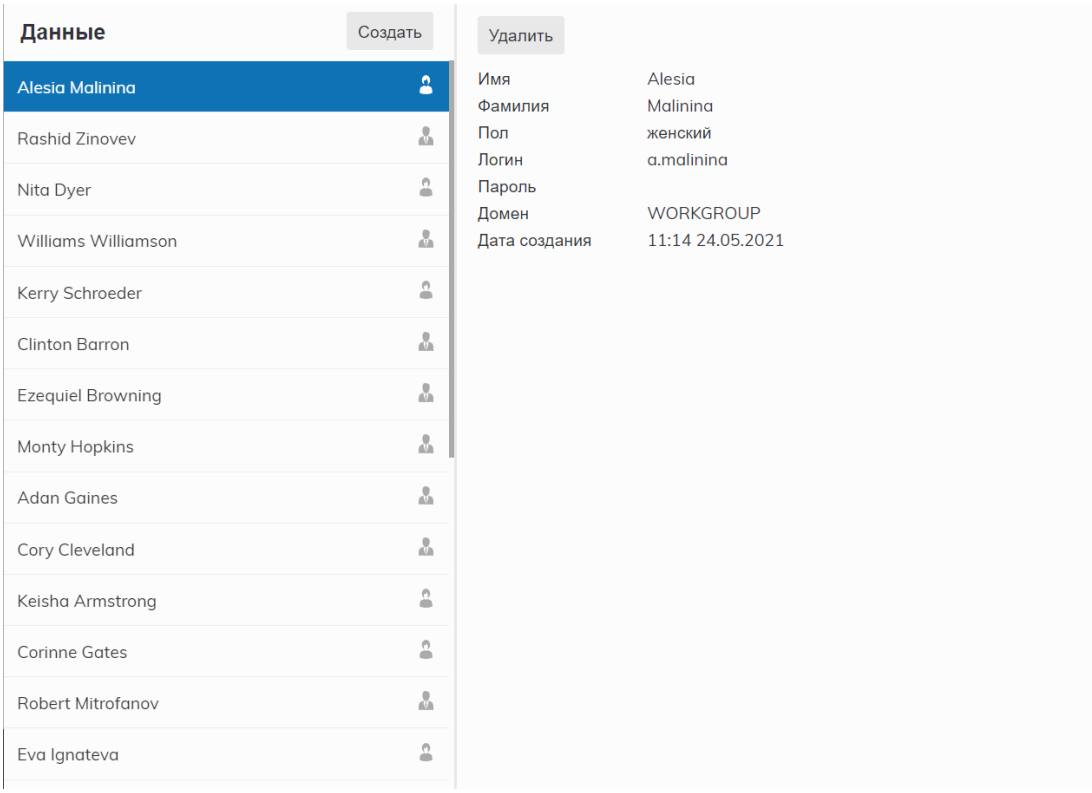
2.3.4.5,kuber

6.6.6.6,admin Fedya



2.7 Раздел [Данные]

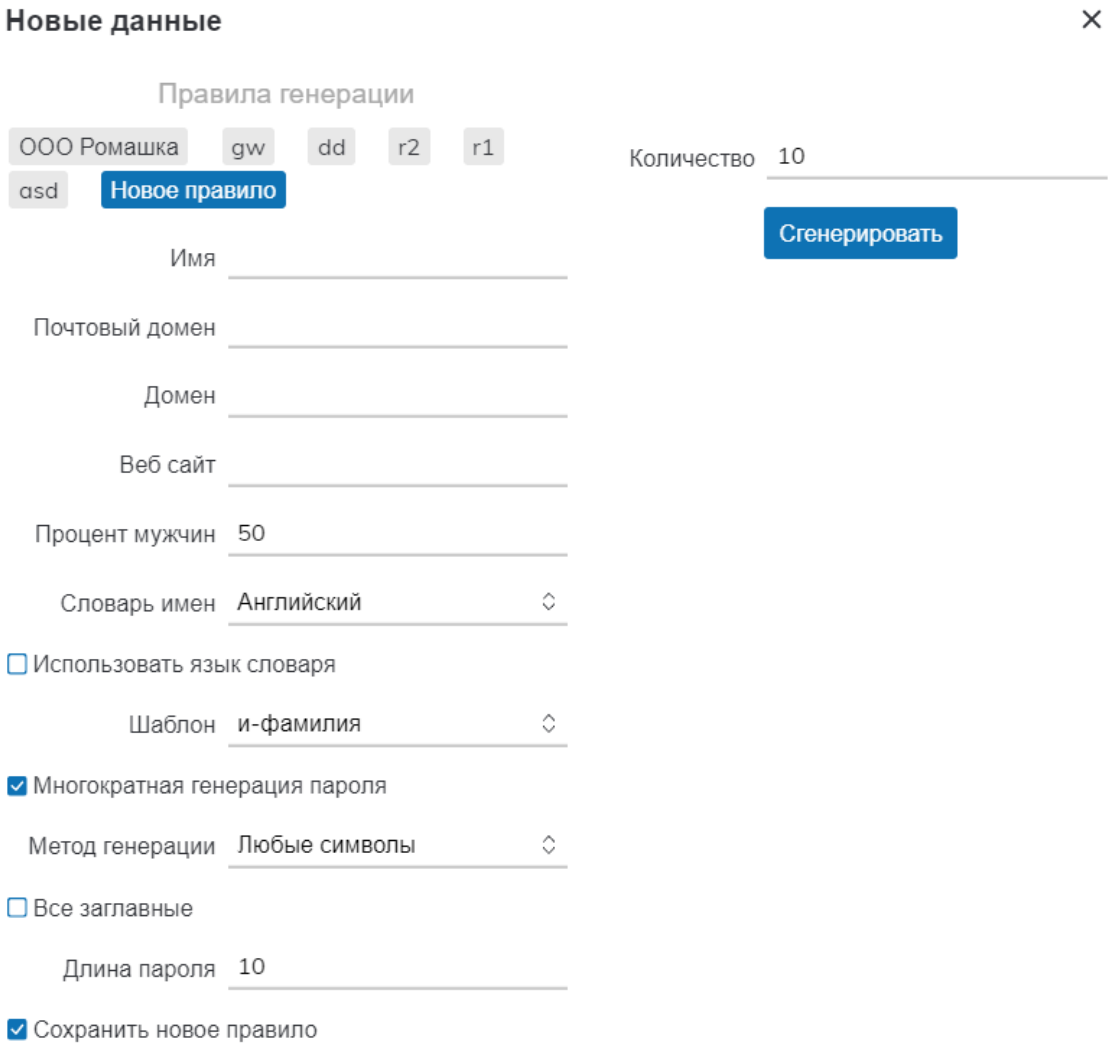
Раздел содержит авторизационные данные, которые используются в токенах для подключения к различным ловушкам.



2.7.1 Создание новых записей

Создание записей происходит по кнопке **Создать**, которая расположена в левом верхнем углу экрана.

При нажатии на кнопку отобразится окно, в котором происходит настройка правил для генерации новых записей.



Основные параметры:

- Имя – имя правила для генерации;
- Почтовый домен – домен почты, который будет присвоен новым записям;
- Домен;
- Процент мужчин – позволяет указать соотношение женщин и мужчин;
- Словарь имен – позволяет выбрать язык, на котором будут генерироваться записи;

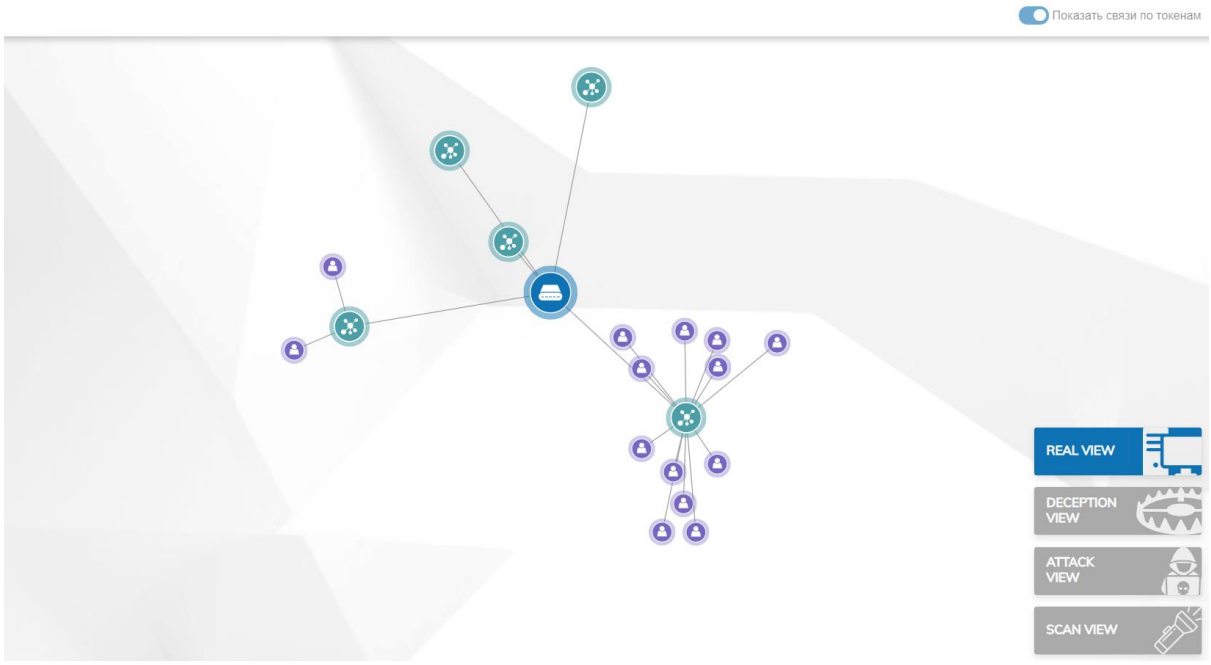
- Шаблон – настройка формата отображения имени;
- Многократная генерация пароля – если на параметре установлена галочка, то пароль для данной записи будет автоматически генерироваться в момент создания токена. Если на параметре отсутствует галочка, то пароль будет генерироваться согласно, выбранному шаблону для генерации;
- Метод генерации – позволяет выбрать метод генерации пароля;
- Все заглавные – установить все заглавные буквы для пароля;
- Длина пароля – установить фиксированную длину пароля
- Сохранить новое правило – позволяет сохранить правило для дальнейшего использования.
- Количество – количество генерируемых записей.

Для создания записей нужно заполнить все поля и нажать кнопку **Сгенерировать**.

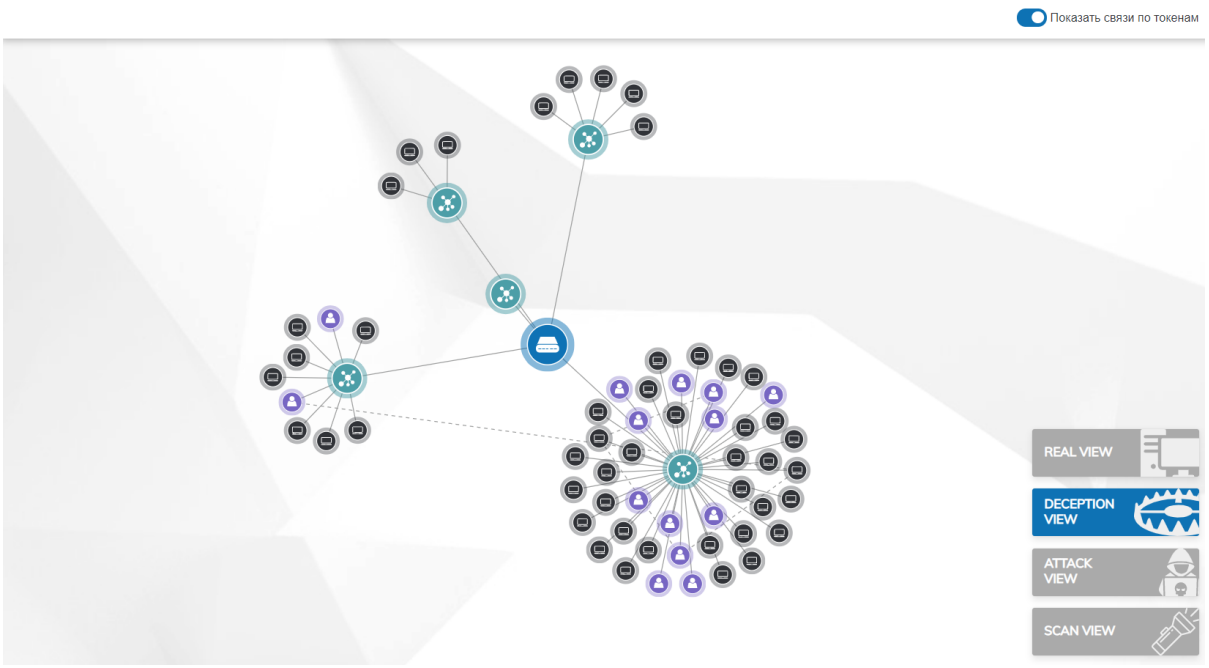
2.8 Раздел [Карта сети]

Раздел предназначен для визуализации взаимодействия сетевых устройств, ловушек и их связей. В разделе есть три представления: **Real View, Deception View, Attack View**

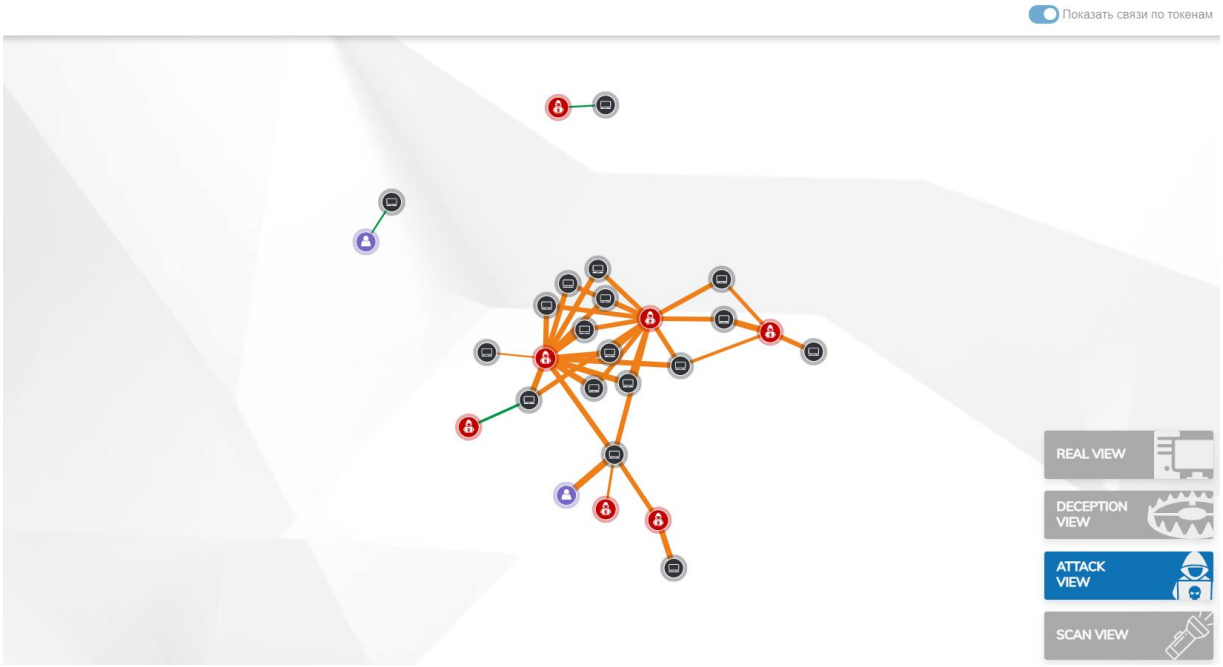
- **Real View** – Представление отображает существующую инфраструктуру заказчика, на которой не отображены ловушки. С помощью данного представления можно увидеть активные супервизоры и их связи с агентами.



- **Deception View** – Представление отображает инфраструктуру заказчика с активными машинами системы Гарда Лабиринт, на которых размещаются сетевые ловушки. Данное представление будет видеть атакующий.

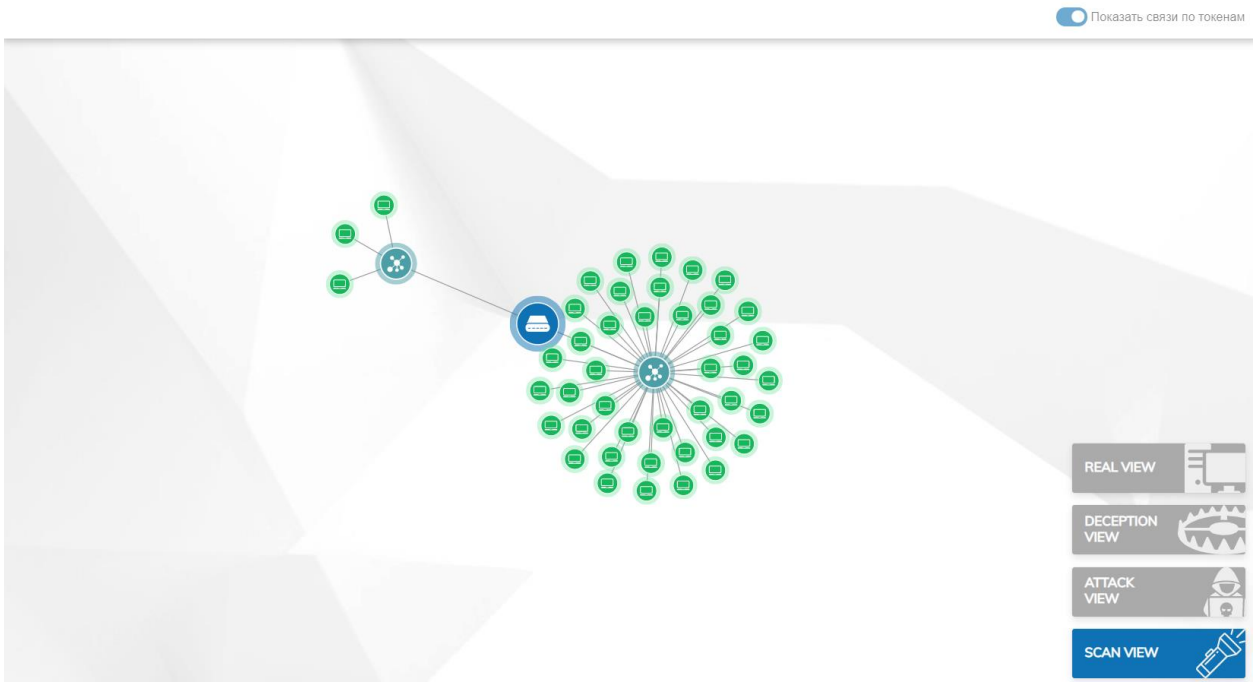


- **Attack View** – Представление отображает взаимодействие злоумышленника с сетевыми ловушками. Используя его, можно проследить цепочку действий злоумышленника.



При наведении мышки на любую иконку в карте сети, можно получить дополнительную информацию по объекту (Название, IP адрес).

Scan View – отображены результаты последнего сканирования сети.



2.9 Раздел [Сканирование сети]

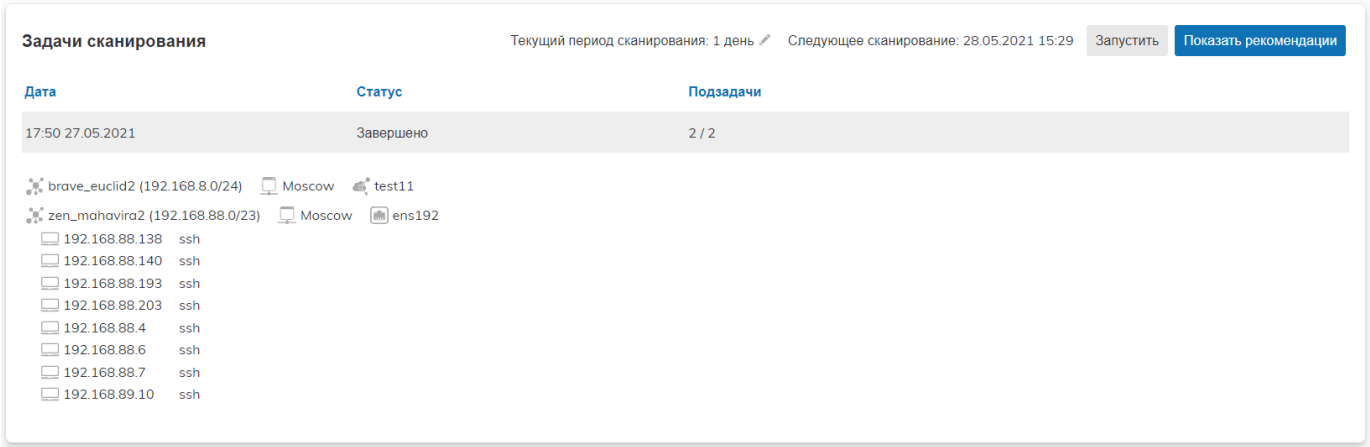
Данный раздел предназначен для сканирования сети, внутри которой будет разворачиваться имитированная IT-инфраструктура. По результатам сканирования

можно будет получить информацию о сервисах, которые активны внутри сети заказчика. Эта информация поможет в дальнейшем определить набор ловушек, которые будут наиболее эффективны в данной сети.

Примечание:

1. Для успешного сканирования и обнаружения ВСЕХ сетей должен быть открыт сетевой доступ от источника сканирования к сканируемому хосту по заданному порту (порт хоста должен быть виден для стенда с Гарда Лабиринт)

2. Сканирование запускается автоматически, с выбранной периодичностью



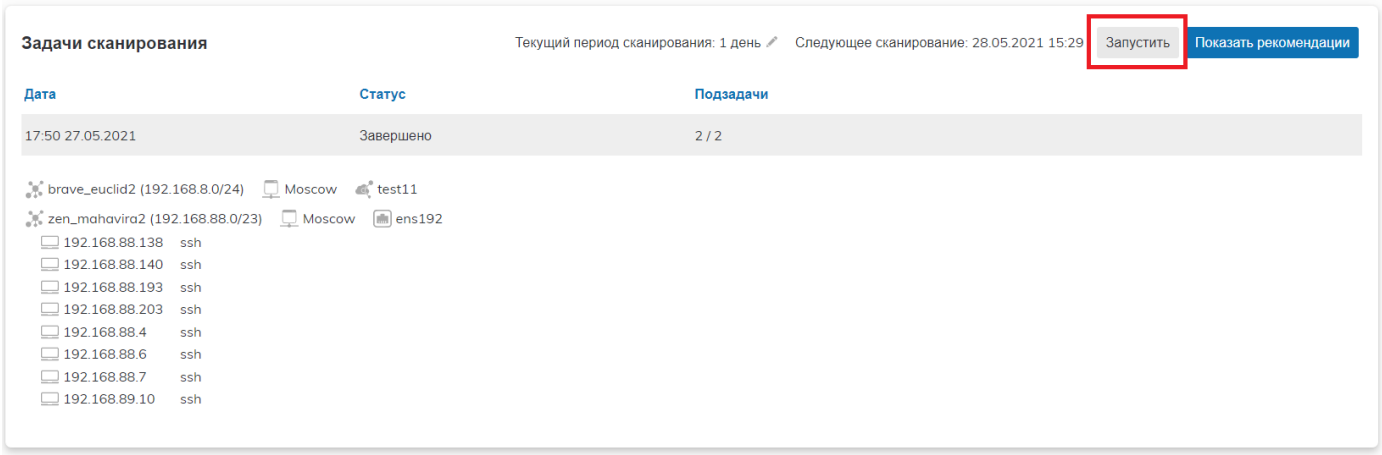
2.9.1 Запуск сканирования сети

Сканирование сети запускается автоматически, с выбранной периодичностью. Периодичность можно изменить в промежутке от 1 до 7 дней.

Также в этом разделе отображается дата следующего автоматического сканирования.

Кроме того сканирование можно запустить вручную:

1. Нажать кнопку Запустить;



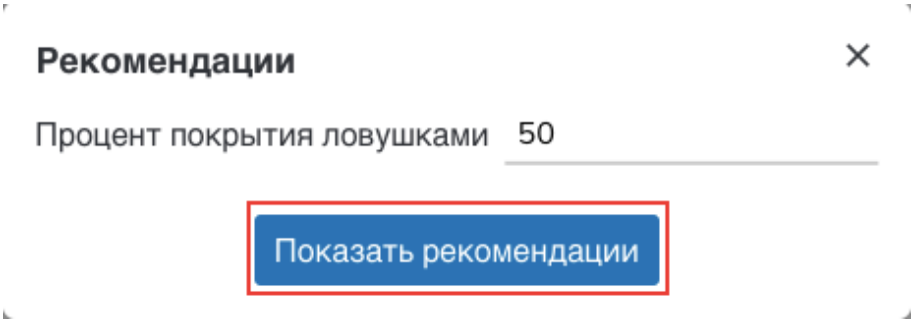
2. После успешного сканирование в интерфейсе у соответствующей записи отобразится статус (Завершено).

2.9.2 Автоматическое развертывание ловушек

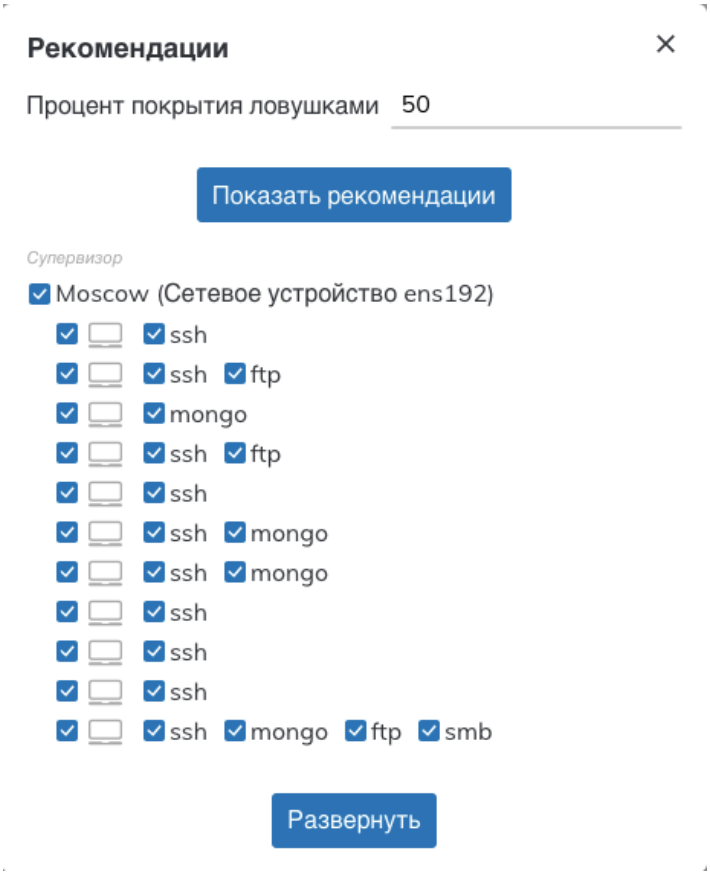
По результатам сканирование внутренней сети система Гарда Лабиринт может автоматически развернуть набор ловушек, которые будут максимально эффективны в данной сети.

Для автоматического развертывания ловушек на основе сканирования сети необходимо:

1. Нажать на кнопку **Показать рекомендации.**
2. Указать процент покрытия ловушками и нажать на кнопку **Показать рекомендации**.



3. Выбрать нужные сервисы и нажать кнопку **Развернуть**.



4. В появившемся окне будут отображены настройки ловушек, которые система создаст автоматически. Их можно изменить или оставить значения по умолчанию. Для развертывания необходимо нажать кнопку **Развернуть**.
5. Настройки по структуре совпадают с настройками ловушек из раздела **«Ловушки»**

2.10 Раздел [Настройки]

Раздел [Настройки] объединяет инструменты, используемые для настройки Гарда Лабиринт. Раздел позволяет:

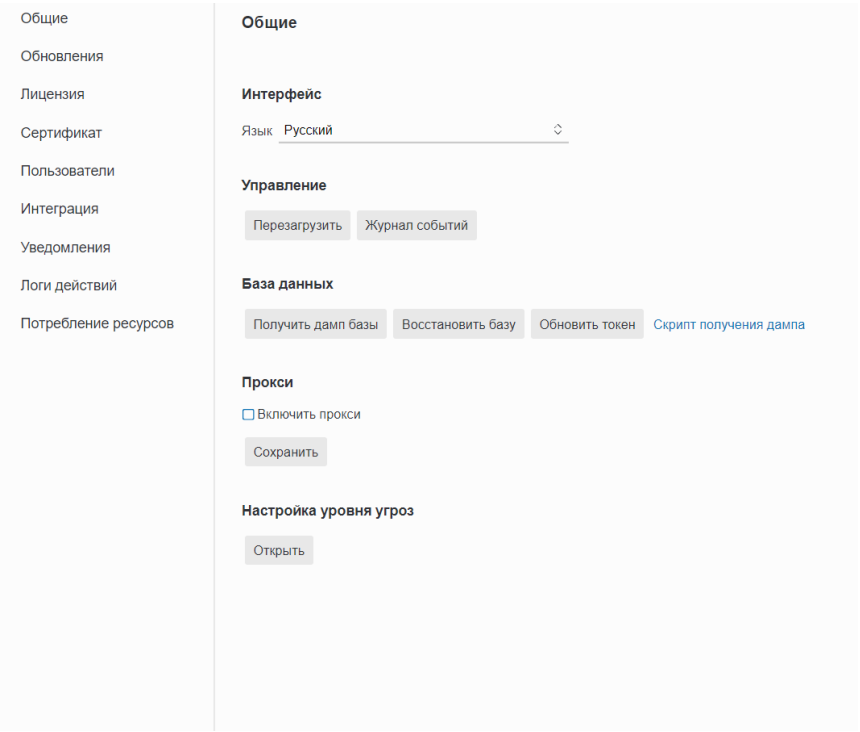
- Управлять общими настройками системы.
- Обновлять систему Гарда Лабиринт и ее компоненты.
- Управлять лицензиями системы Гарда Лабиринт
- Устанавливать сертификат доступа к веб интерфейсу
- Управлять пользователями и их пользовательскими ролями.

- Настраивать интеграцию с SIEM системами.
- Управлять уведомлениями.
- Просматривать логи действий
- Просматривать потребление ресурсов

2.10.1 Меню [Общее]

Меню [Общее] позволяет:

- выбрать язык системы Гарда Лабиринт,
- управлять Control Center,
- управлять базами данных,
- настраивать подключение через Прокси-сервер,
- настраивать потребление ресурсов



2.10.1.1 Управление

Данный блок содержит две кнопки:

- **Перезагрузить** – Используется для перезагрузки Control Center (После перезагрузки Control Center не будет обрабатывает все входящие события 30 секунд.).
- **Журнал событий** – Позволяет загрузить файлы логирования системы Гарда Лабиринт.

2.10.1.2 База данных

Данный блок содержит две кнопки:

- Получить дамп базы
- Восстановить базу
- Обновить токен

Также можно, нажав кнопку «Скрипт получения дампа», получить скрипт для выполнения запроса загрузки дампа базы данных.

2.10.1.3 Прокси

Система Гарда Лабиринт получает обновление со специального сервера. В некоторых компаниях предусмотрена политика информационной безопасности, которая не позволяет подключаться к различным источникам во внешней сети. Для этих целей существует возможность использования прокси-сервера, через который система Гарда Лабиринт сможет установить соединение с сервером обновлений и успешно загружать их.

2.10.1.4 Настройка уровня угроз

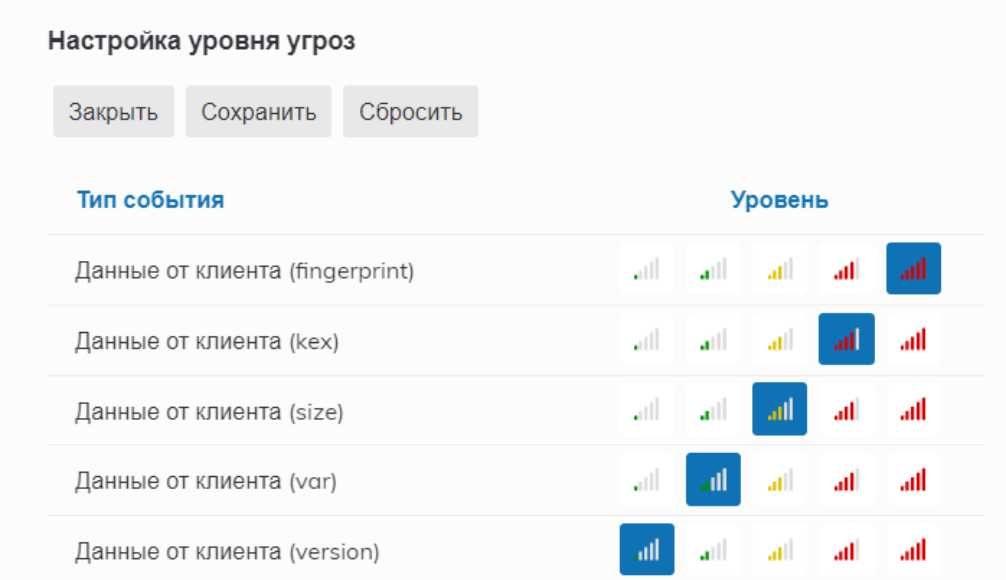
Данный блок содержит три кнопки:

- **Закрыть** – закрыть список событий
- **Сохранить** – сохранить изменения
- **Сбросить** – сбросить до заводских настроек уровня угроз

В данном пункте можно изменить уровни угроз для различных видов событий.

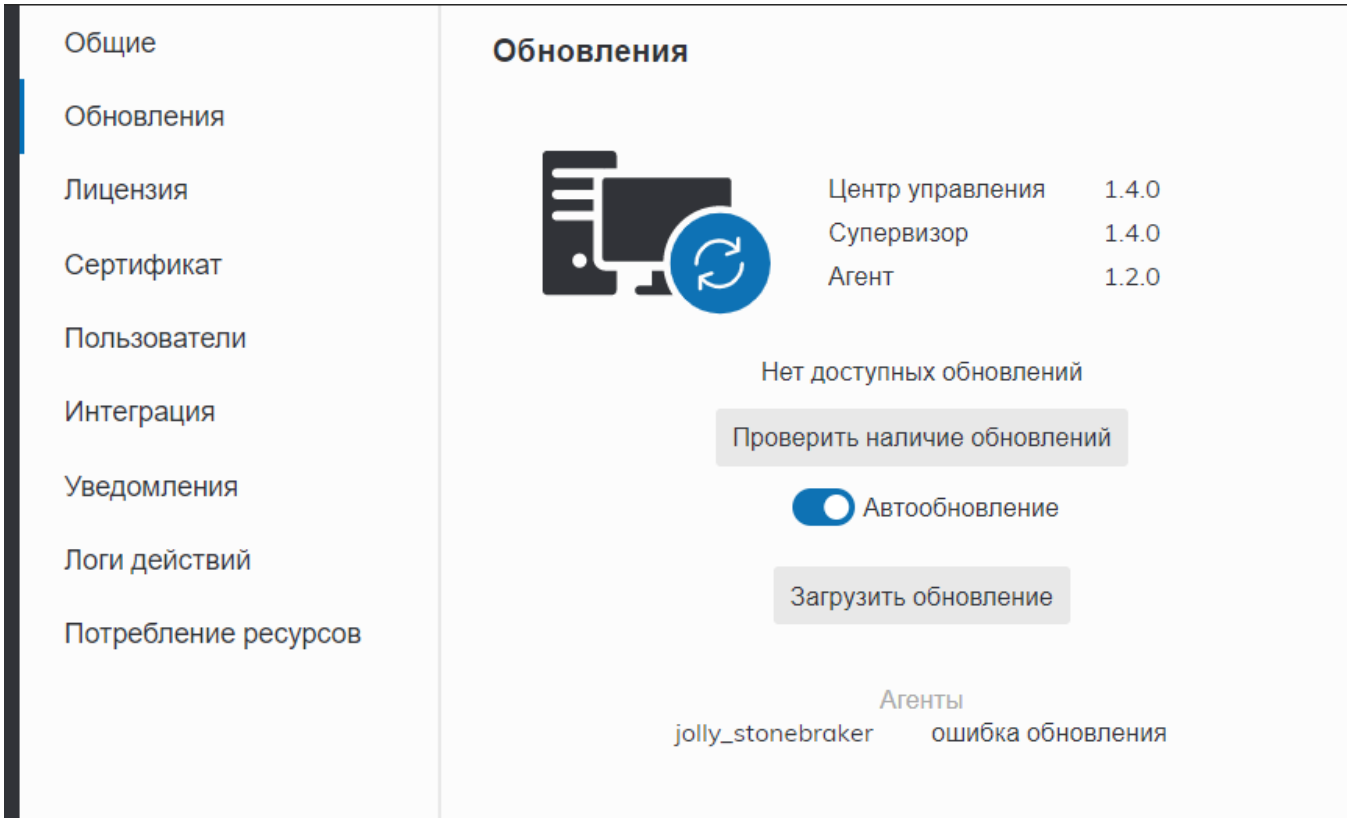
Пример:

Разным видам событий назначен разный вид угроз.



2.10.2 Меню [Обновления]

Меню [Обновления] используется для обновления системы Гарда Лабиринт и ее компонентов.



2.10.2.1 Обновление системы вручную.

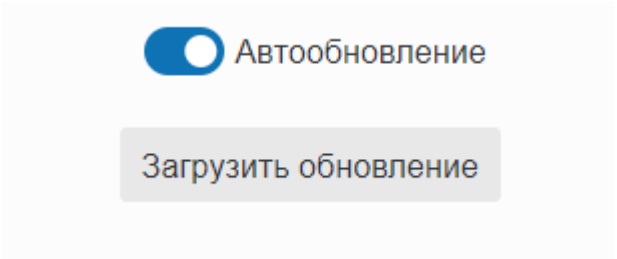
Перед обновлением системы нужно проверить наличие обновлений. Это можно сделать по кнопке **Проверить наличие обновлений**. После проверки система уведомит пользователя о результатах. Существуют следующие статусы:

- Нет доступных обновлений;
- Доступно новое обновление.

В случае, если доступно новое обновление, нужно нажать на кнопку **Обновить**. Далее система в автоматическом режиме установит обновление.

2.10.2.2 Автоматическое обновление системы

В системе предусмотрена возможность автоматического обновления системы. Для этого это нужно установить галочку на пункте **Автообновление**.



В этом случае система выполнит установку обновлений в автоматическом режиме и не потребует дополнительных действий со стороны пользователя.

2.10.3 Меню [Лицензии]

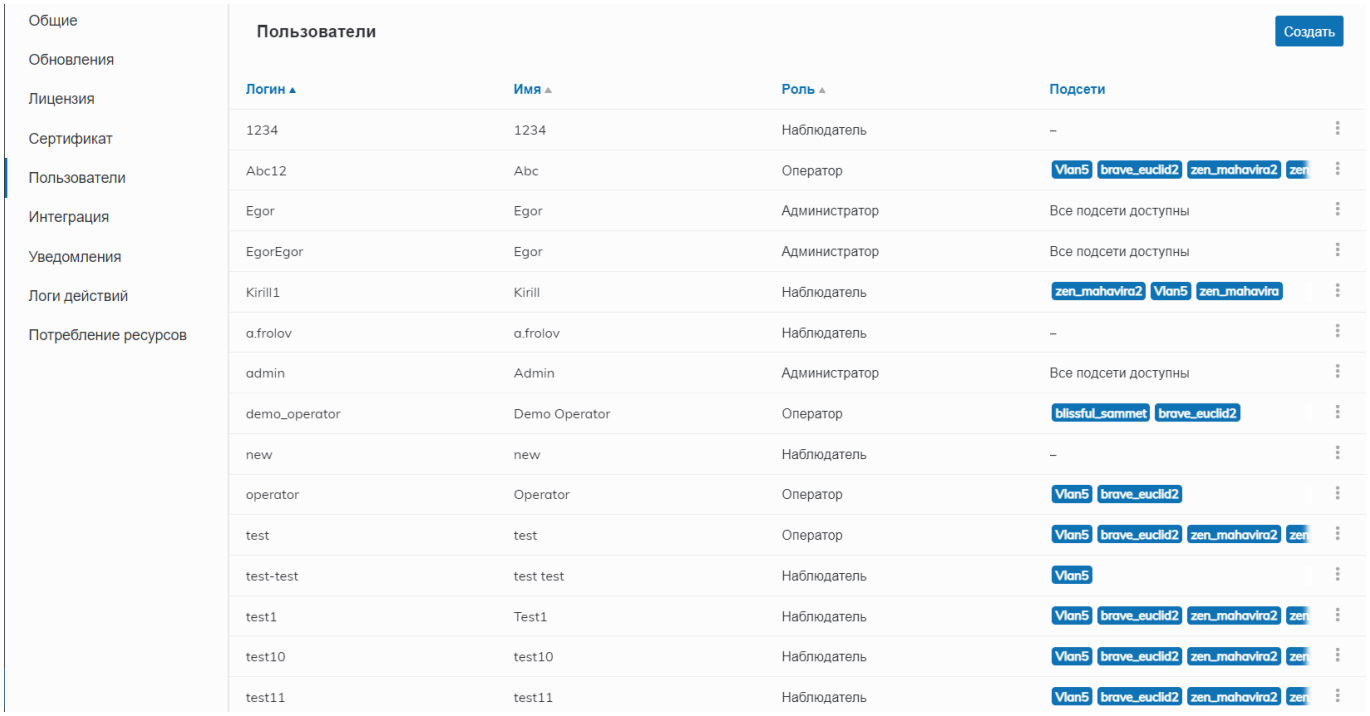
Меню используется для управления лицензиями на систему **Гарда Лабиринт**. Для получения или обновления лицензии обратитесь к службе поддержки компании Гарда Технологии.

2.10.4 Сертификат

Меня [Сертификат] позволяет получить информацию о сертификате и устанавливать новый.

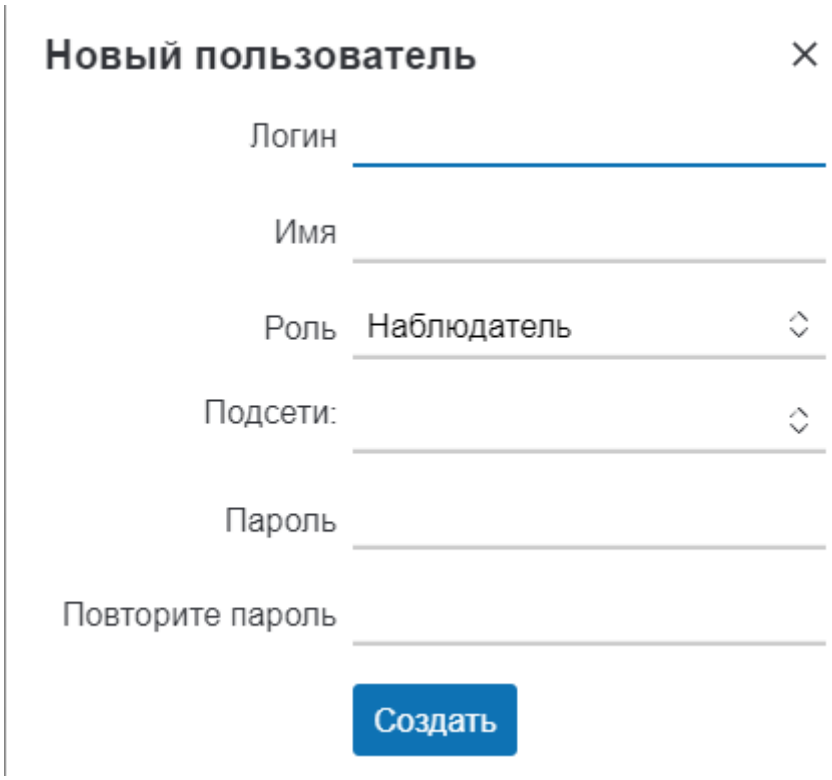
2.10.5 Меню [Пользователи]

Меню [Пользователи] используется для создания и управления пользователями в системе.



Для создания нового пользователя необходимо нажать на кнопку **Создать** и заполнить все поля**.** Для каждого пользователя в системе определяется Роль. В зависимости от роли пользователю предоставляется определенный набор прав и действий, которые он может совершать в системе. В системе существует три роли: **Администратор, оператор, наблюдатель.**

- **Администратор** – имеет полный доступ ко всем настройкам и конфигурациям системы.
- **Оператор** – может конфигурировать систему, но у него отсутствует доступ к настройкам системы Гарда Лабиринт (Создание пользователей, лицензии, обновления).
- **Наблюдатель** – имеет доступ только на чтение.

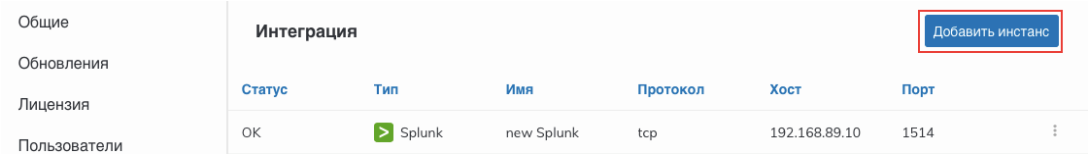


2.10.6 Меню [Интеграция]

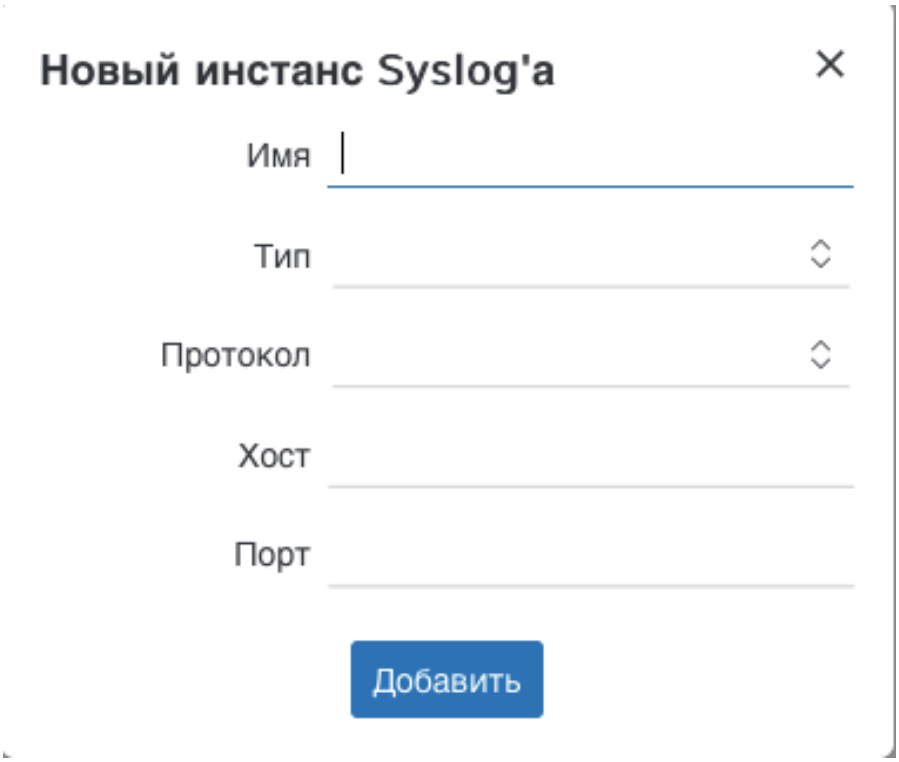
Меню используется для интеграций с SIEM системами и системами сбора логов такими как: Splunk, Prometheus и другими. Интеграция осуществляется средствами Syslog в CEF формате. Поэтому систему Гарда Лабиринт можно интегрировать с любой системой, которая поддерживает данный формат.

2.10.6.1 Добавление нового инстанса

1. Для настройки интеграций нужно нажать кнопку **Добавить инстанс**.

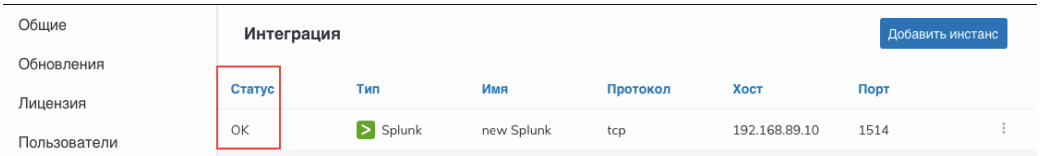


2. Заполнить все поля.



- **Имя** – Имя системы.
- **Тип** – Тип интегрируемой системы (Если отсутствует нужный тип, то необходимо выбрать тип **custom**)
- **Протокол** – протокол передачи данных(udp/tcp)
- **Хост и порт** – сетевой адрес, на который нужно передавать Syslog.

3. Нажать кнопку **Добавить**.
4. Система установит соединение с интегрируемой системой, статус подключение можно увидеть в специальной колонке **Статус**.



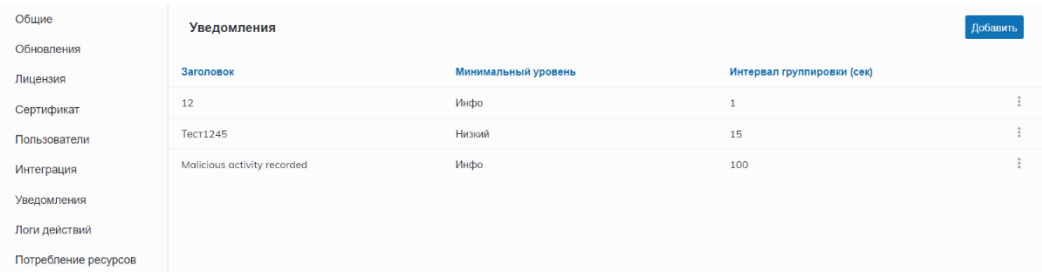
2.10.7 Меню [Уведомления]

Данное меню используется для настройки пользовательских уведомлений. В боковой панели разделов присутствует раздел для индивидуальных настроек

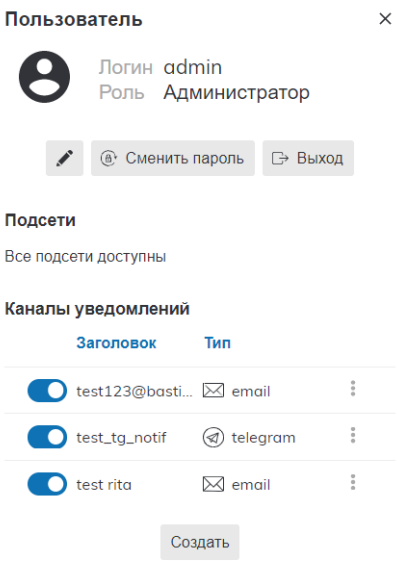
пользователя системы. В нем указываются персональные настройки пользователя и настраиваются уведомления по Email и Telegram. Использование уведомлений значительно упрощает эксплуатацию системы Гарда Лабиринт. В случае возникновения события система автоматически отправит уведомление через Email или Telegram – бот. В меню [Уведомление] происходит настройка самих уведомлений и их временных интервалов.

2.10.7.1 Добавление нового канала

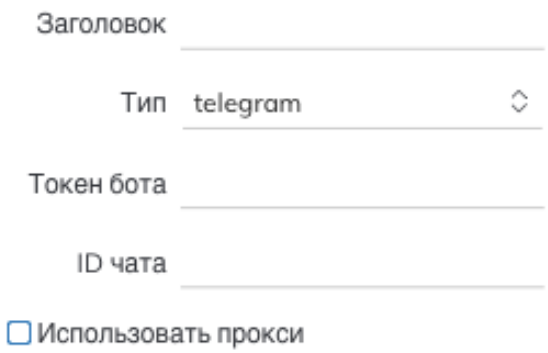
1. Перейти в раздел пользовательских настроек.



2. Нажать кнопку **Создать.**



3. Выбрать тип **Email** или **Telegram** и заполнить все поля (Получение параметров Telegram канала описано в пункте 2.10.7.2).



4. Нажать кнопку **Добавить.**

Примечание: Данные действия нужно выполнить для всех пользователей, для которых настраиваются уведомления.

2.10.7.2 Создание Telegram канала.

Для получения уведомлений в Telegram нужно предварительно создать Telegram канал и выполнить несколько настроек.

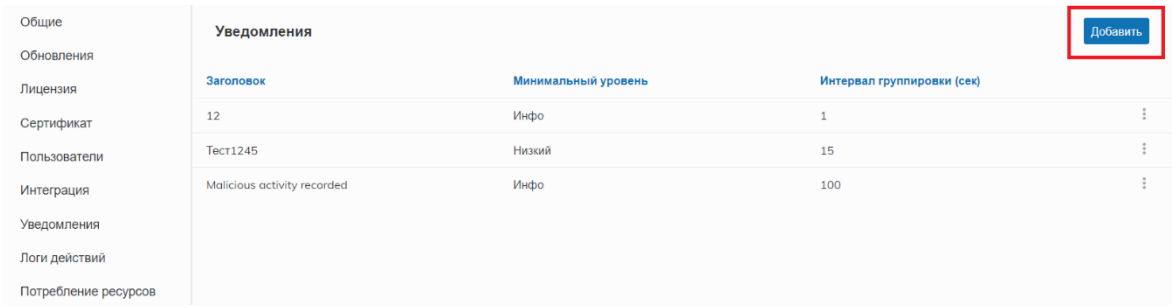
1. Написать в **@BotFather** и следовать инструкциям по созданию бота;
2. Ввести в чат с **@BotFather** команду **/mybots**;
3. Выбрать бот, который был создан в пункте 1.
4. Выбрать команду **API Token**;
5. Создать группой чат в телеграм и добавить в него бота из пункта 1;
6. Написать в групой чат сообщение **/my_id;**
7. В адресную строку браузера ввести следующий адрес https://api.telegram.org/bot<Token>/getUpdates (Вместо <Token> указать токен, полученный в п4. Указывать токен нужно без кавычек)
8. В отобразившейся информации найти атрибут: **"chat":{"id":xxxxxxx,**

API Токен из пункта 4 и chat id из пункта 8 являются основными атрибутами, которые нужно указывать при создании уведомлений в телеграмм.

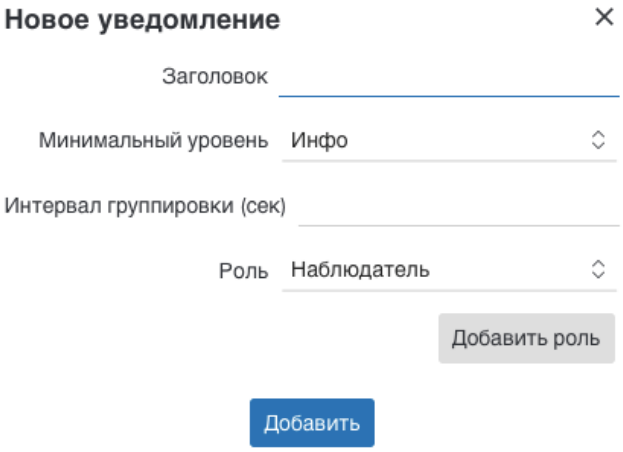
2.10.7.3 Настройка уведомлений

После привязки email или telegram необходимо настроить формат уведомлений.

1. Добавить новую запись в меню [Уведомления].



2. Заполнить все необходимые поля.



Минимальный уровень – Позволяет разграничивать события по уровню угрозы. Пользователю будут приходить уведомления только по тем событиям, где уровень угрозы выше, чем указан в настройках уведомлений.

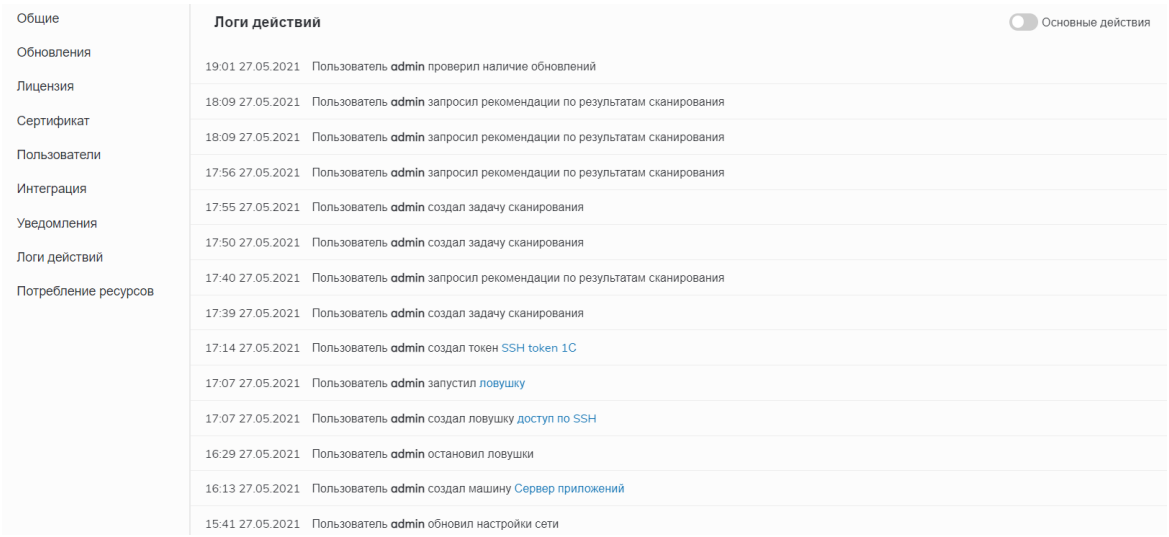
Интервал группировки – Позволяет указывать интервал группировки событий.

Роль – Роль, для которой актуальна данная настройка.

2.10.8 Меню [Лог действий]

В меню [Лог действий] содержится информация о всех действиях пользователей в системе. Таких как: Авторизация в системе, создание/изменение/удаление различных объектов системы и т.д. Любое действие,

выполненное пользователем, в системе будет отображено в данном меню.



Если переключить тумблер из состояния **«Основные действия»** в состояние **«Все действия»,** то пользователю будут доступны логи также неуспешных действий.

2.10.9 Потребление ресурсов

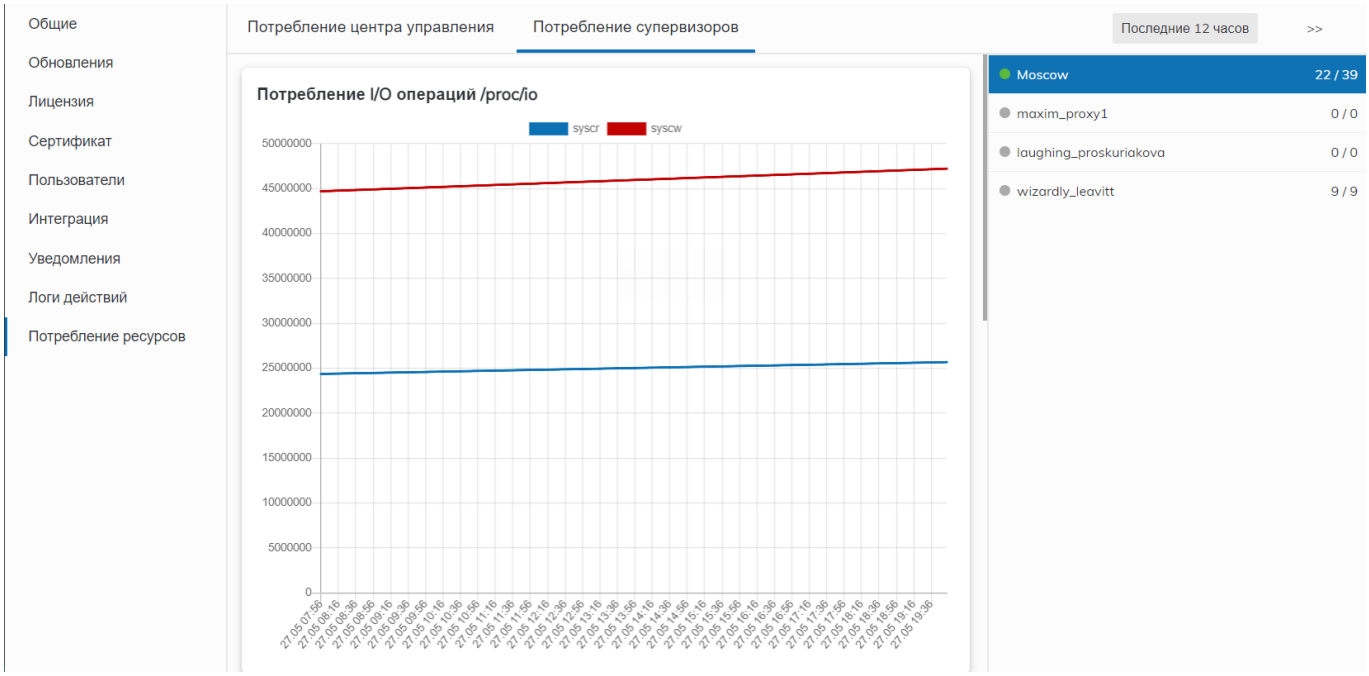
В меню [Потребление ресурсов] содержится информация о потреблении ресурсов Центром управления, и Супервизорами.

Для каждого сервера доступны графики трех метрик:

- Количество операций ввода/вывода (/proc/io)
- Потребление оперативной памяти (/proc/meminfo)
- Потребление ресурсов процессора (/proc/loadavg)

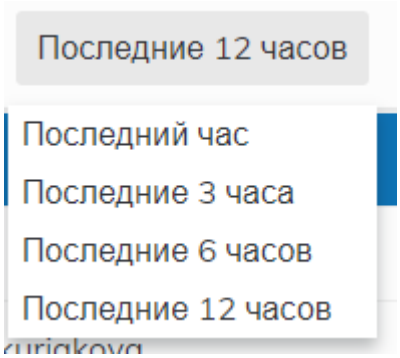
Во вкладке «Потребление центра управления» есть возможность увидеть потребление ресурсов центра управления.

Во вкладке «Потребление супервизоров» необходимо выбрать нужный супервизор из списка для того, чтобы увидеть потребление его ресурсов.



Для того, чтобы выбрать временной промежуток отображения данных на графиках, нажмите на кнопку сверху справа.

Доступны следующие варианты промежутков:



3 ПОДДЕРЖКА

3.1 Контакты

По вопросам поддержки обращайтесь:

Официальный сайт: gardatech.ru

E-mail: glb.support@gardatech.ru

Телефон: +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени)

4 О КОМПАНИИ

Гарда Технологии – российский вендор систем информационной безопасности. Команда разработчиков обладает многолетним опытом в сфере информационных технологий и создает решения для различных задач безопасности – защита конфиденциальных данных, выявление атак на внутреннюю и внешнюю инфраструктуру, защиты от DDoS, сервисы для операторов связи. Компания входит в ТОП-30 крупнейших разработчиков систем информационной безопасности России. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.