

# КОНКУРСНОЕ ЗАДАНИЕ

**Региональные чемпионаты 2021-22**

Сокращенное типовое задание – 85 баллов

Корпоративная защита от  
внутренних угроз  
информационной  
безопасности

**Модуль 1, 3, 5**

**День 1**

Менеджер компетенции: А.В. Сергеев



## Аннотация

Документ содержит типовое конкурсное задание 2021-22 региональных чемпионатов 2021-22 года по стандартам WorldSkills Russia по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности».

Конкурсное задание разработано на базе заданий Отборочных соревнований и IV Финала национального чемпионата Ворлдскиллс 2021 года. Практические задания собрали лучшие практические задачи в области обеспечения корпоративной безопасности в организациях реального сектора экономики и были апробированы на корпоративных чемпионатах ГК Росатом, ГК Роскосмос.

Использование документа печать (тиражом до 20 экз.) и распространение разрешено только в рамках организации и проведения региональных чемпионатов Ворлдскиллс. С вопросами и замечаниями можно обращаться по адресу: [avsergeev@hse.ru](mailto:avsergeev@hse.ru)

Состав рабочей группы по разработке типового КЗ:

- **А.В. Сергеев, менеджер компетенции,**  
НИУ ВШЭ, Москва;
- **А.П. Бозров, сертифицированный эксперт,**  
ГБПОУ «Колледж связи № 54», Москва;
- **А.А. Крылова, победитель МежВУЗ 2019,**  
ФГАОУ ВО «Санкт-Петербургский государственный университет  
аэрокосмического приборостроения», Санкт-Петербург;
- **А.В. Зябухина, эксперт-компатриот призёра ФНЧ 2021,**  
ГБПОУ КК "Краснодарский колледж электронного приборостроения",  
Краснодар;
- **Н.В. Матвеев, сертифицированный эксперт,**  
ФГАОУ ВО «Санкт-Петербургский государственный университет  
аэрокосмического приборостроения», Санкт-Петербург;
- **Е.В. Трапезников, сертифицированный эксперт,**  
ФГАОУ ВО «Омский государственный технический университет», Омск.

## Дополнительные сведения (шаблон)

### Общие сетевые настройки

Шлюз по умолчанию: 172.16.x.1 (x - номер рабочего места)

DNS сервер провайдера

DNS сервер компании

### Компьютер с виртуальными машинами:

Логин: root, пароль: xxXX1234

Документация находится в папке Temp на ПК участника

Дистрибутивы находятся в datastore1

Образы систем находятся в datastore1

### Контроллер домена (DEMO.LAB):

IP адрес: 172.16.x.2 Маска: 255.255.255.248

Домен: demo.lab

логин: administrator пароль: xxXX1234

### DLP-система (IWTM)

Локальный вход: логин: root пароль: xxXX1234

IP адрес: 172.16.x.3 Маска: 255.255.255.248

Веб консоль логин: officer пароль: xxXX1234

### Windows Server (IWDM):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: 172.16.x.4 Маска: 255.255.255.248

### Windows 10 (Client 1):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: 172.16.x.5 Маска: 255.255.255.248

Проверка правил передачи через сайт dlptest.com

**ОБЯЗАТЕЛЬНО**

Заполните файл /etc/hosts на виртуальной машине IWTM, в соответствии с дополнительными сведениями.

```
GNU nano 2.3.1 File: /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.3.2 demolab.demo.lab demolab
172.16.3.3 iwtm.demo.lab iwtm
172.16.3.4 iwdm.demo.lab iwdm
172.16.3.5 w10-cli1.demo.lab w10-cli1
172.16.3.6 w10-cli2.demo.lab w10-cli2
```

## Модуль 1: Установка и настройка системы

### Описание

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) одного из интеграторов DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и настроить DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом Active Directory), с которым необходимо будет осуществить интеграцию DLP-системы. До настройки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMware Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM).

Вам необходимо установить и настроить компоненты DLP-системы в соответствии с выданным заданием.

Необходимо использовать следующие виртуальные машины:

- Demo (контроллер домена demo.lab)
- IWTM (предустановленный, необходимо настроить)
- Iwdm (Windows Server для IWTM, предустановленный)
- w10-cli1 (ПК первого нарушителя)
- w10-cli2 (ПК второго нарушителя)

Сетевые настройки виртуальных машин указаны в дополнительной карточке заданий.

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в папке «InfoWatch 6.11.5» на SSD.

Если в задании необходимо сделать скриншот, необходимо называть его по номеру задания, например: Задание\_5\_копирование.png.

## Задание 1: Подготовка Active Directory

**Примечание:** необходимо проверить, что данные пользователи уже не добавлены в Active Directory. Если добавлены, не выполнять повторно.

Для дальнейших работ необходимо создать подразделение организации (Organization Unit) под названием «Office», добавить в него каталоги пользователей и компьютеров (Users и Computers).

**В каталог Users необходимо добавить следующих пользователей:**

- iwdm-admin (права доменного администратора, для машины iwdm)
- db-admin (права доменного администратора, для машины db)
- iwtm-officer (права пользователя домена, для входа в веб-консоль iwtm)
- useroffice-1 (1я машина нарушителя, права пользователя домена, w10-cli1)
- useroffice-2 (2я машина нарушителя, права пользователя домена, w10-cli2)
- ldapsync-user (права пользователя домена, для всех ldap-синхронизаций)

Ваша задача – создать и настроить вышеперечисленных пользователей в соответствии с указанными условиями.

Для всех пользователей необходимо задать пароль xxXX1234

Настройте LDAP-синхронизацию для IWTM с помощью пользователя ldapsync-user.

Для работы с консолью IWTM используйте доменного пользователя iwtm-officer (задать все встроенные роли (officer и administrator) и все области видимости).

Стоит учесть, что после ввода в домен, компьютеры необходимо переносить в ранее созданный каталог Computers (внутри OU «Office»)

В соответствии с политикой компании для обеспечения безопасности компьютеров брандмауэр должен быть активен. Для установки компонентов системы необходимо настроить правила брандмауэра с помощью групповых политик домена.

Зайти пользователями useroffice-1 на машину w10-cli1 и useroffice-2 на машину w10-cli2.

## Решение:

Необходимо зайти на VM demo.lab, перейти в оснастку «Пользователи и компьютеры Active Directory».

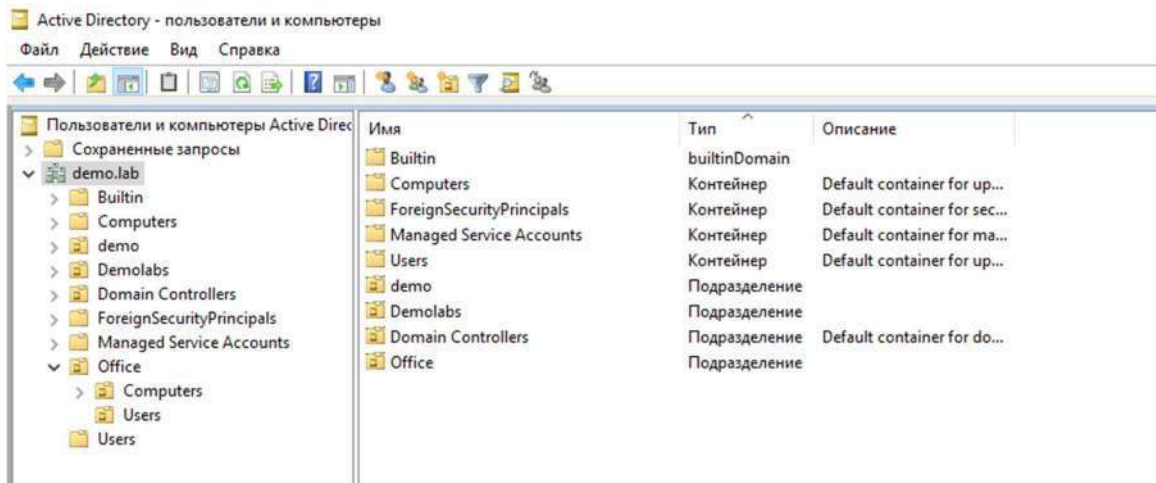


Рисунок 1 - «Оснастка Пользователи и компьютеры»

В открывшейся оснастке необходимо перейти во вкладку demo.lab, правой кнопкой мыши нажать по свободному пространству и выбрать «Создать», после чего выбрать «Подразделение». Согласно заданию, подразделение необходимо назвать «Office». В созданном подразделении нужно создать еще два, по аналогии с предыдущим. Названия: “Computers”, “Users”

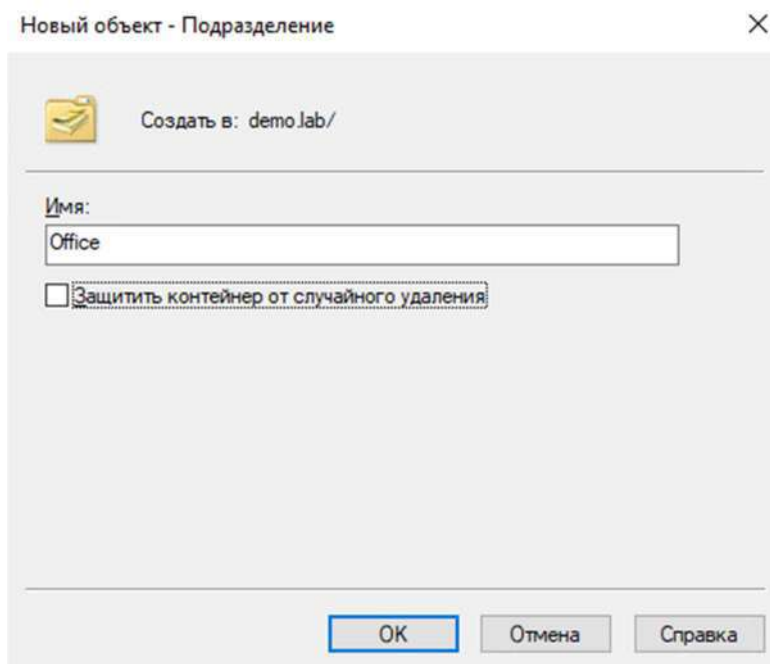


Рисунок 2 - «Создания подразделения»

Затем, необходимо создать пользователей в каталоге Users. Для удобства, советую сначала создать группу «Userss», а затем создавать пользователей.

Для создания группы нужно в подразделении Users кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Группа».

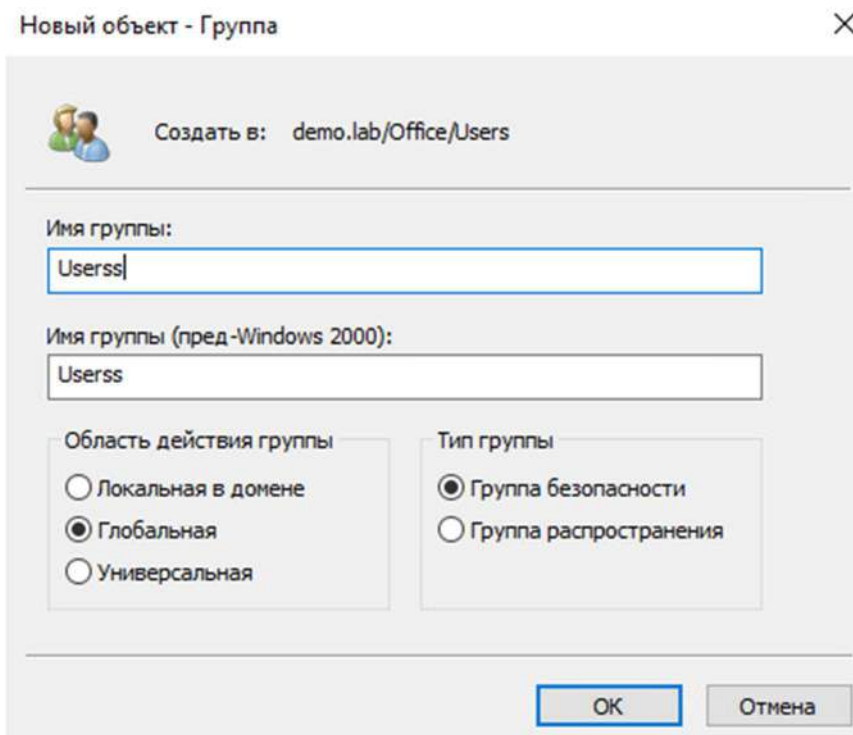
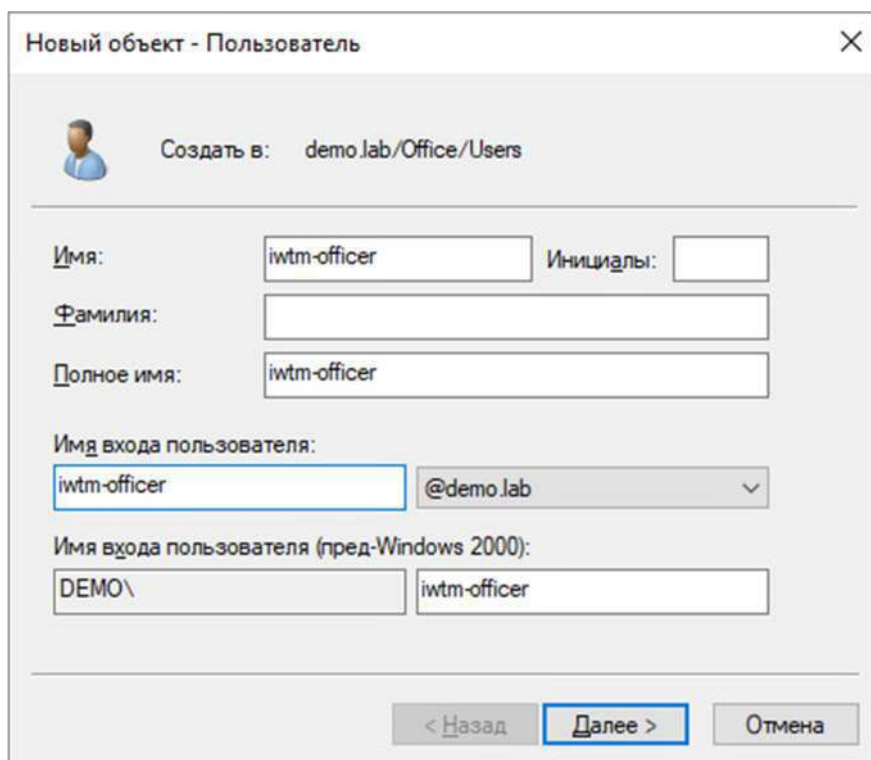


Рисунок 3 – «Создание группы»

После создания группы можно приступать к созданию пользователей. Начнем с пользователей iwtm-officer, iwdm-admin, db-admin. Эти пользователи требуют прав доменного администратора.

Для создания пользователя нужно в подразделении Users кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Пользователь». Пароль каждого пользователя должен быть **xxXX1234**. **Все галочки выставлять строго в соответствии с рисунками 4 и 5!**





Новый объект - Пользователь

Создать в: demo.lab/Office/Users

Имя: iwtm-officer Инициалы:

Фамилия:

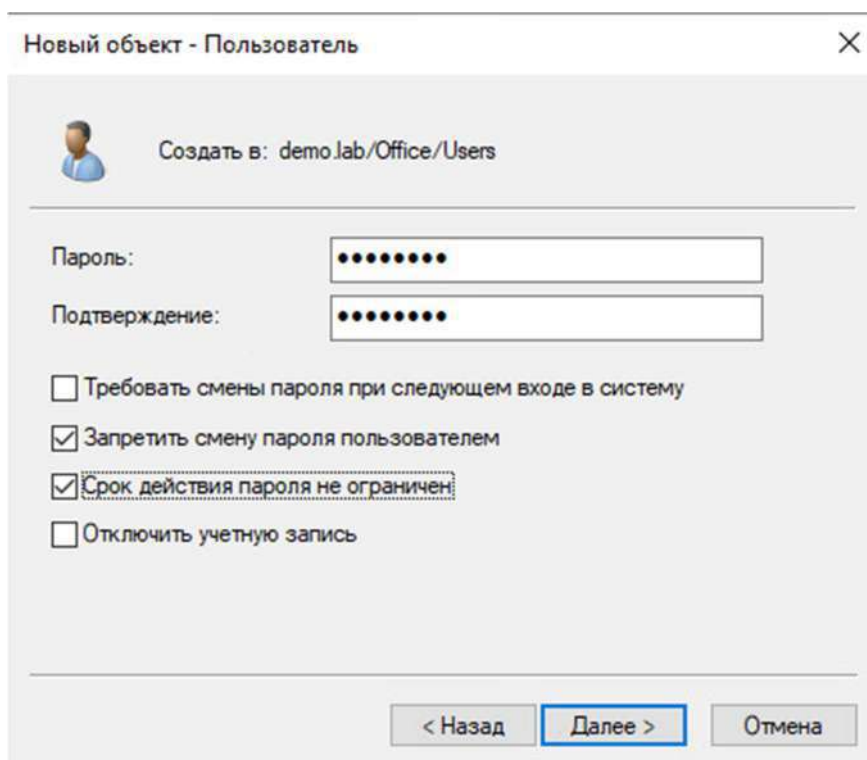
Полное имя: iwtm-officer

Имя входа пользователя: iwtm-officer @demo.lab

Имя входа пользователя (пред-Windows 2000): DEMO\ iwtm-officer

< Назад Далее > Отмена

Рисунок 4 – «Создание пользователя ч.1»



Новый объект - Пользователь

Создать в: demo.lab/Office/Users

Пароль: .....

Подтверждение: .....

☐ Требуется смена пароля при следующем входе в систему

☒ Запретить смену пароля пользователем

☒ Срок действия пароля не ограничен

☐ Отключить учетную запись

< Назад Далее > Отмена

Рисунок 5 – «Создание пользователя ч.2»

По аналогии с пользователем iwtm-officer создайте пользователей db-admin и iwdm-admin. Теперь необходимо предоставить созданным пользователям права доменного администратора. Для этого их необходимо выделить зажатой левой кнопкой мыши, нажать ПКМ на выделенных пользователях и выбрать пункт «Добавить в группу.» В открывшемся окне, необходимо ввести «Domain Admins» («Администраторы домена», если винда русская.) в поле «Введите имена выбираемых объектов».

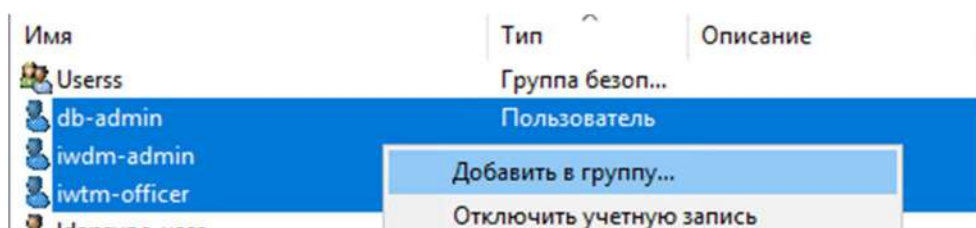


Рисунок 6 – «Добавление пользователей в группу ч.1»

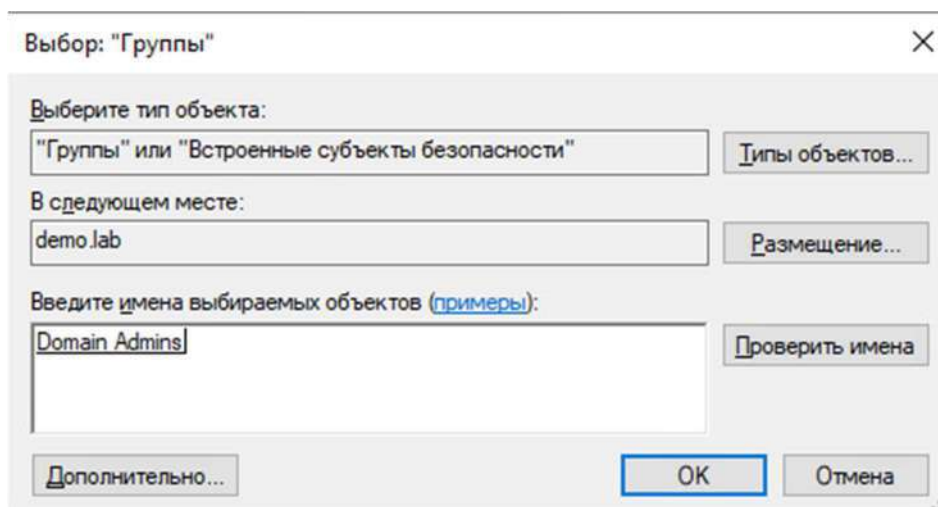


Рисунок 7 – «Добавление пользователей в группу ч.2»

Теперь можно перейти к созданию пользователей useroffice-1, useroffice-2 и ldapsync-user. Делайте это по аналогии с рисунками 4 и 5. **Однако, не добавляйте пользователей в группу Domain Admins (Администраторы домена).**

После создания всех пользователей, можно приступить к настройке LDAP-синхронизации на IWTM. Для настройки LDAP-синхронизации перейдите к WEB-интерфейсу Traffic Monitor. Для этого, в браузере введите в поисковую строку IP-адрес виртуальной машины IWTM (пр. 172.16.10.3).

Учетные данные для входа в WEB-интерфейс Traffic Monitor:

- логин: officer
- пароль: xxXX1234

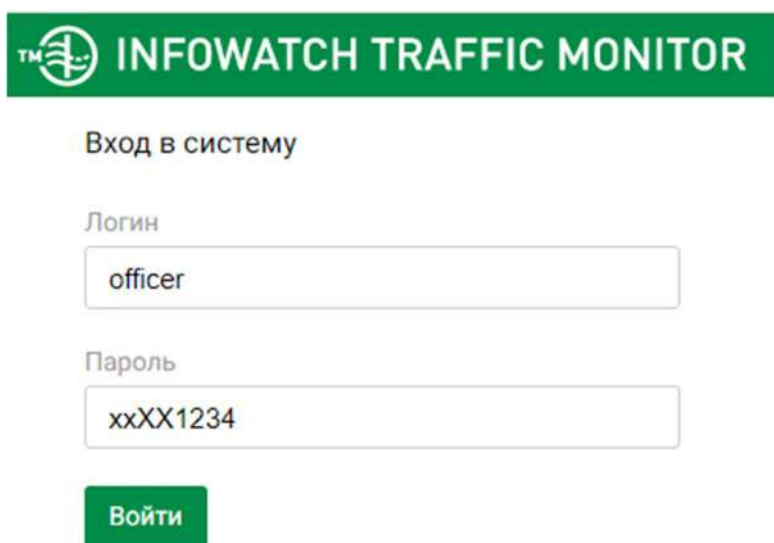


Рисунок 8 – «Вход в Traffic Monitor»

После входа в Web-интерфейс Traffic Monitor, необходимо выбрать пункт «Управление» в панели управления, в верхней части интерфейса, и выбрать подпункт «LDAP-синхронизация».

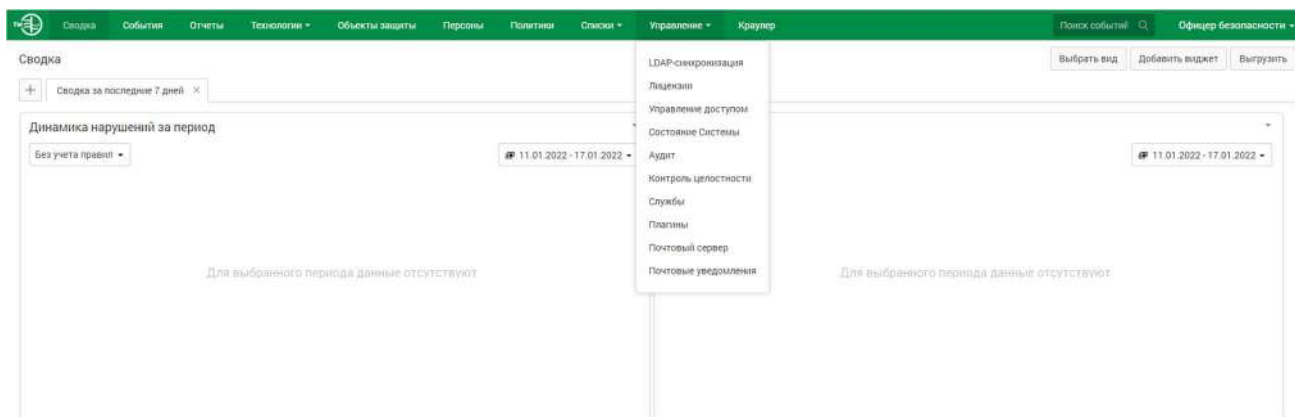


Рисунок 9 – «Переход к настройке LDAP-синхронизации»

В открывшейся вкладке, необходимо выбрать пункт «Создать», отмеченный знаком «+». Теперь, необходимо указать конфигурацию LDAP-синхронизации (Рисунок 10):

- Имя сервера: произвольное (пр. demo.lab),
- Тип сервера: Active Directory,
- Синхронизация: автоматическая,
- Период синхронизации: ежеминутно,
- Повторение: 15 минут,
- LDAP-сервер: IP-адрес виртуальной машины demo.lab (пр. 172.16.1.2),
- Использовать протокол Kerberos: нет,
- Глобальный LDAP-порт: 3268,
- LDAP-порт: 389,
- Использовать глобальный каталог: да,
- LDAP-запрос: DC=DEMO,DC=LAB
- Анонимный доступ: нет,
- Логин: ldapsync-user,
- Пароль: xxXX1234

### Добавление LDAP-сервера

Имя сервера

Тип сервера

Синхронизация ☒ Автоматическая ☐ Ручная

---

Период синхронизации

Повторение  минут

---

### Настройки соединения

LDAP-сервер

Использовать протокол Kerberos ☐

Глобальный LDAP-порт

LDAP-порт

Использовать глобальный каталог ☒

LDAP-запрос

Анонимный доступ ☐

Логин

Пароль

Рисунок 10 – «Конфигурация LDAP-синхронизации»

После настройки LDAP-синхронизации, необходимо добавить нового пользователя, который будет управлять консолью IWTM. Для создания нового пользователя, на знакомой панели управления в верхней части интерфейса веб-консоли Traffic Monitor, перейдите во вкладку «Управление» и выберите пункт «Управление доступом».

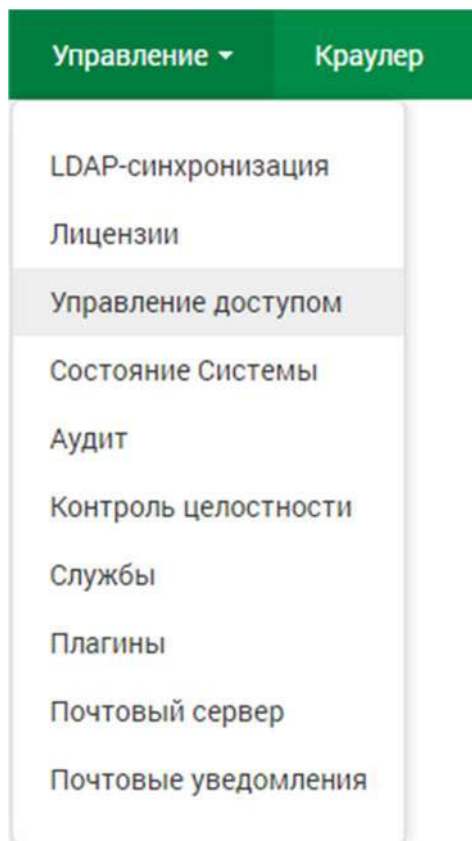


Рисунок 11 – «Управление доступом»

В открывшейся вкладке, необходимо выбрать пункт «Создать», отмеченный знаком «+» и выбрать пункт «Добавить пользователя из LDAP».

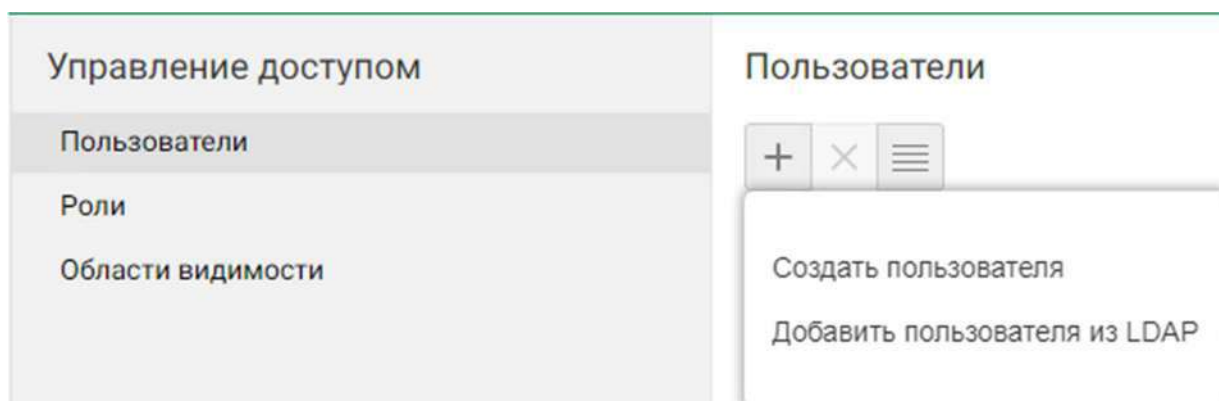


Рисунок 12 – «Добавление пользователя из LDAP ч.1»

Затем, необходимо ввести имя пользователя, который будет выступать администратором консоли, отметить нужного пользователя галочкой и нажать «Сохранить».

Выберите пользователя из LDAP

LDAP-сервер для поиска:

Поиск:

Пользователь	Доменный аккаунт	Адрес сервера	Департамент
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer@DC=DEMO.DC=LAB	172.16.1.2	

Рисунок 13 – «Добавление пользователя из LDAP ч.2»

После чего, необходимо выбрать этого же пользователя для того, чтобы перейти к его настройке. Необходимо указать почту пользователя ([iwtm-officer@demo.lab](mailto:iwtm-officer@demo.lab)), роли (Администратор, Офицер безопасности) и области видимости (Полный доступ, VIP). Нажмите кнопку «Сохранить» для применения настроек.

Пользователи

Логин	Название	Email	Роли	Области видимости	Описание
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer				
<input type="checkbox"/> administrator	Администратор		Администратор		Предустановленная
<input type="checkbox"/> officer	Офицер безопасности		Администратор, Офицер безопасности	Полный доступ	Предустановленная

Редактирование пользователя

Логин:

Статус:

Email:

Полное имя:

Роли:

Области видимости:

Описание:

Создано: 17.01.2022, 03:58 – Изменено: 17.01.2022, 03:58

Рисунок 14 – «Настройка пользователя»

После настройки LDAP-синхронизации, необходимо внести все ПК под управлением ОС Windows в домен Active Directory. Для этого, перейдите на

любой из компьютеров под управлением ОС Windows и откройте «Проводник». В открывшемся окне, в левой панели найдите пункт «Этот компьютер» и кликните на него правой кнопкой мыши, а затем выберите «Свойства».

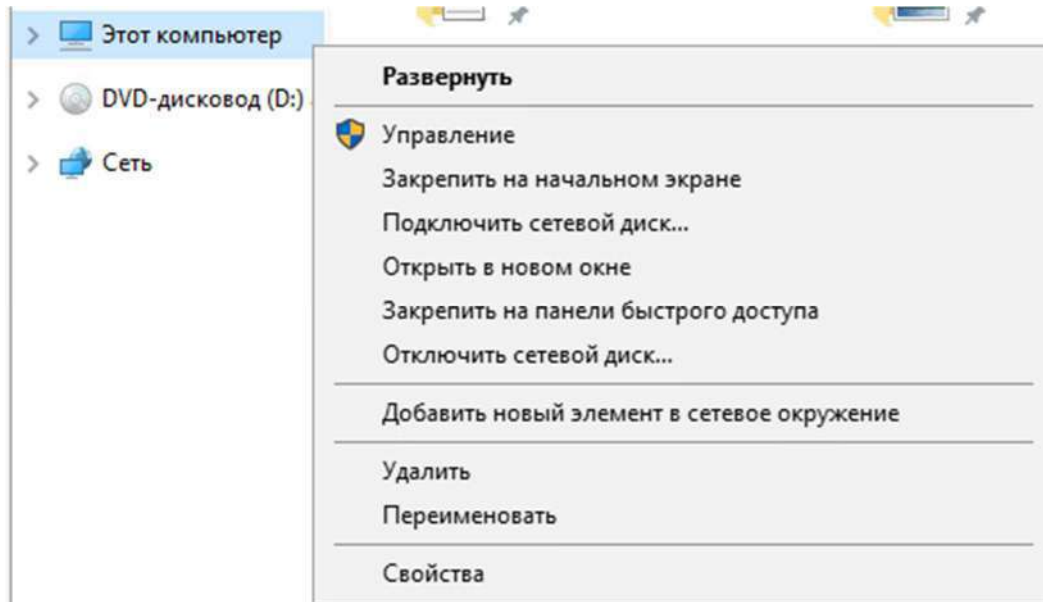


Рисунок 15 – «Переход к свойствам компьютера»

В открывшемся окне найдите подпункт «Имя компьютера, имя домена и параметры рабочей группы» в пункте «Просмотр основных сведений о вашем компьютере» и кликните «Изменить параметры». В открывшемся окне «Свойства системы», на вкладке «Имя компьютера» нажмите кнопку «Изменить».

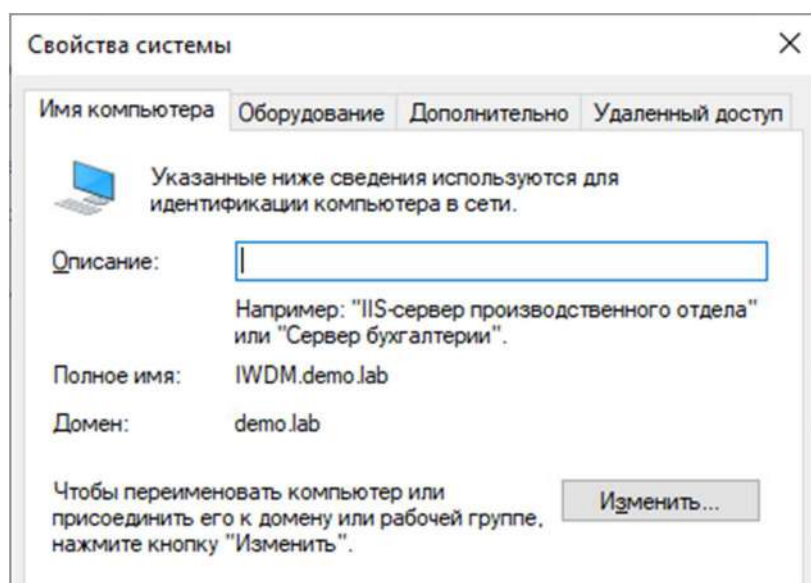


Рисунок 16 – «Добавление ПК в домен demo.lab ч.1»



В открывшемся окне переименуйте компьютер и введите имя домена (demo.lab) в соответствующие поля, после чего нажмите ОК и выполните перезагрузку.

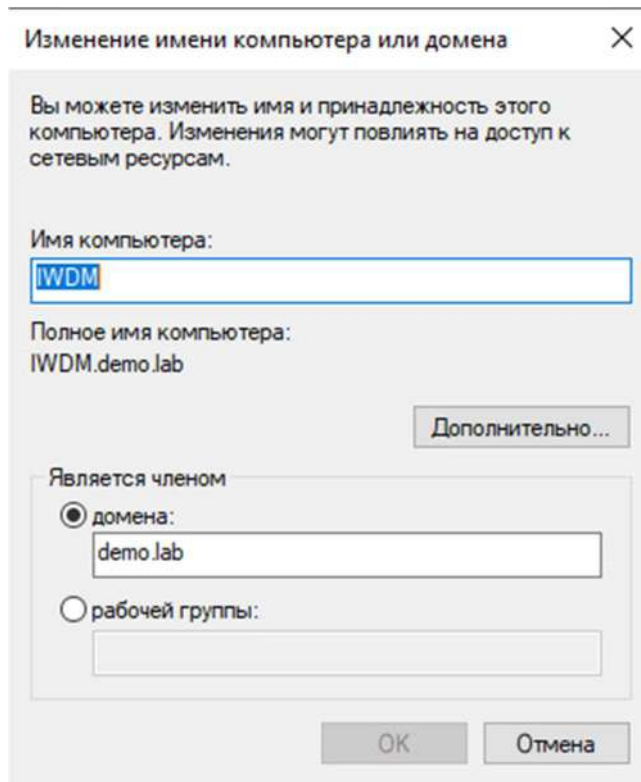


Рисунок 17 – «Добавление ПК в домен demo.lab ч.2»

Остальные компьютеры добавьте в домен по аналогии.

После добавления всех ПК в домен, вернитесь к оснастке «Active Directory Пользователи и компьютеры» на виртуальной машине demo.lab. В этой оснастке необходимо перенести добавленные в домен компьютеры в каталог «Computers» в подразделении «Office».

В открытой оснастке перейдите в каталог «Computers», который находится в корне домена demo.lab, затем выделите компьютеры и перетащите их зажатой левой кнопкой мыши в каталог «Computers» в подразделении «Office» (Рисунок 18).

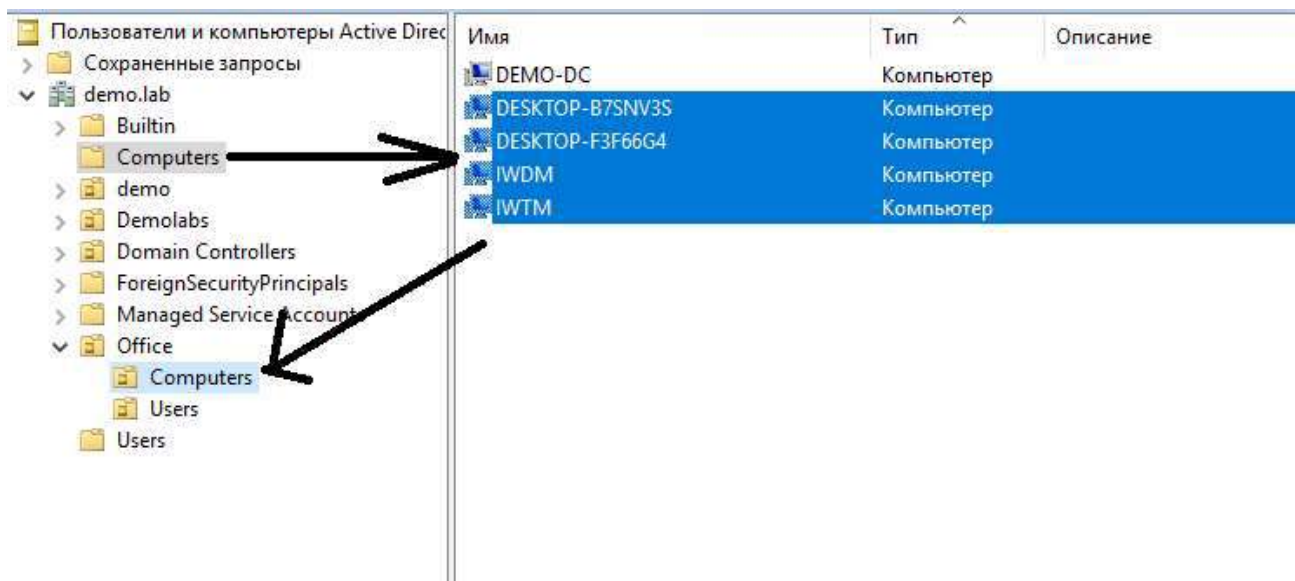


Рисунок 18 – «Перенос ПК в каталог Computers»

**ОПЦИОНАЛЬНО:** для собственного удобства, можно создать записи DNS для каждого устройства. Для этого, зайдите в Пуск → Средства Администрирования → DNS. В открывшейся оснастке выберите единственный сервер и откройте подпапку «Зоны прямого просмотра», а в ней «demo.lab».

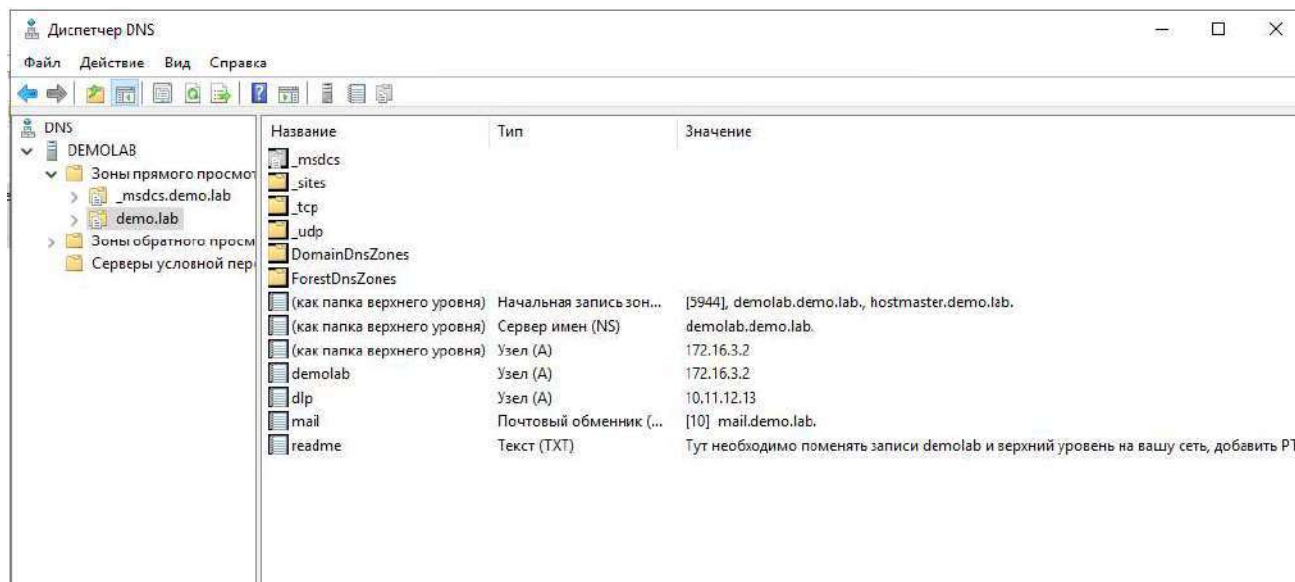


Рисунок 19 – «Зона прямого просмотра demo.lab»

В пустом пространстве нажмите ПКМ и, в открывшемся контекстном меню, выберите «Создать узел (A или AAAA)». При создании нового узла DNS, введите имя устройства и его IP-адрес (прим.: iwtm – 172.16.1.3).

Новый узел ✕

Имя (если не указано, используется родительский домен):

Полное доменное имя (FQDN):

IP-адрес:

☒ Создать соответствующую PTR-запись

☐ Разрешать любому прошедшему проверку пользователю обновлять DNS-записи с таким же именем владельца

Рисунок 20 – «Создание узла»

## Задание 2: Развертывание InfoWatch Crawler

Для контроля общих сетевых ресурсов в организации необходимо развернуть следующие сетевые компоненты InfoWatch Traffic Monitor на машину IWDM: Crawler Server и Crawler Scanner.

После установки InfoWatch Crawler необходимо создать задачу на ежедневное сканирование сетевых ресурсов (папки share\_iwtm, share\_iwdm). Предварительно требуется создать общие сетевые папки:

1. На виртуальной машине IWTM создать папку «share\_iwtm» с правами чтения и записи для всех пользователей домена
2. На виртуальной машине IWDM создать папку «share\_iwdm» с правами чтения и записи для всех пользователей домена

*Зафиксировать создание и выполнение скриншотом.*

Чтобы установить Crawler – перейдите к виртуальной машине IWDM (виртуальная машина для Device Monitor). Перейдите в проводник (может быть на рабочем столе одного из пользователей) и найдите установочный файл Crawler (Crawler\_v6\*.exe), после чего откройте его.

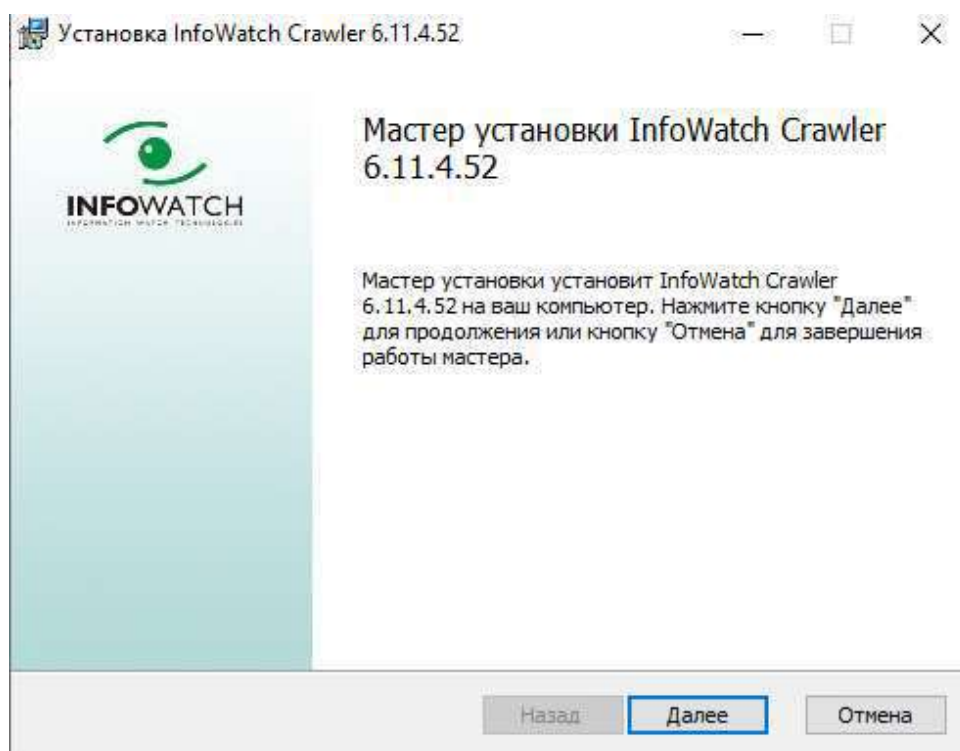


Рисунок 21 – «Установка Crawler»

Соглашайтесь со всем подряд, до пункта «Настройка базы данных».

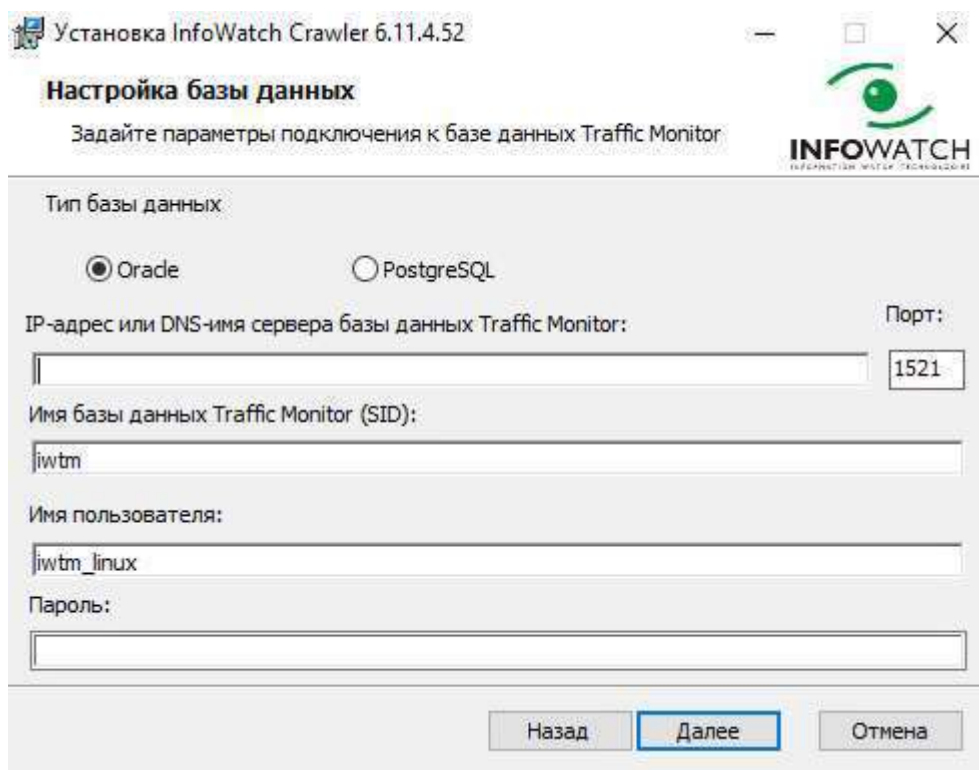


Рисунок 22 – «Настройка базы данных»

Заполните соответствующую информацию:

- Тип базы данных: PostgreSQL
- IP-адрес или DNS-имя сервера базы данных ТМ: 172.16.1.3 (или iwtm, если настроено DNS)
- Имя базы данных ТМ (SID): postgres
- Имя пользователя: iwtm
- Пароль: xxXX1234

После заполнения информации о БД, будет необходимо заполнить информацию о Traffic Monitor.

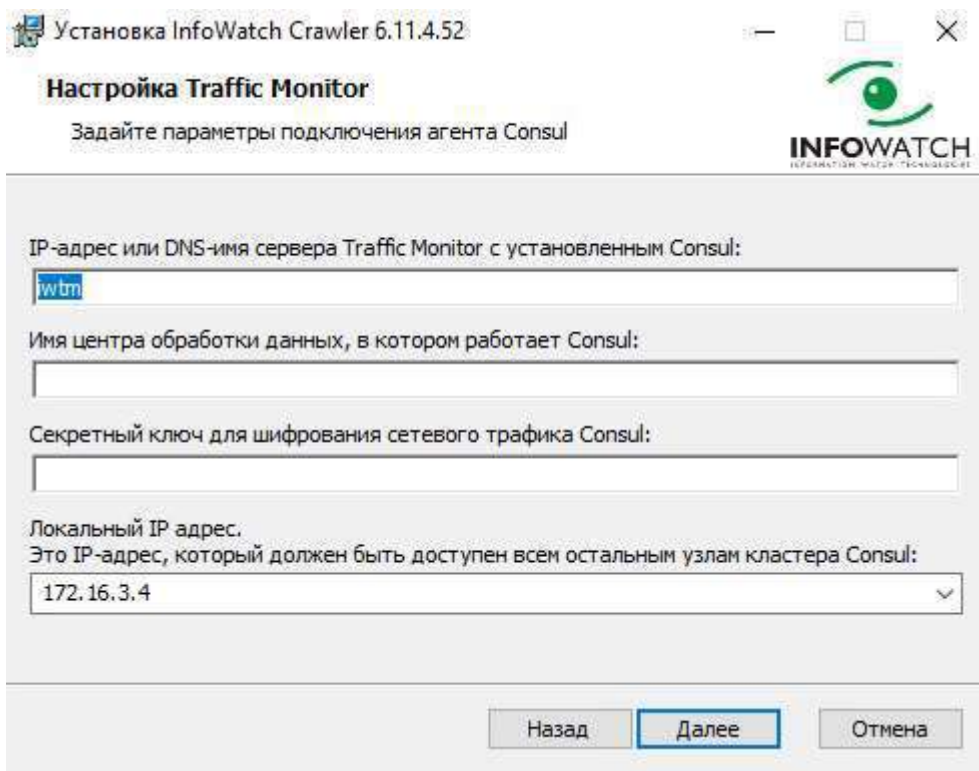


Рисунок 23 – «Настройка Traffic Monitor»

Агент Consul устанавливается вместе с Traffic Monitor по умолчанию. Для получения имени центра обработки данных и секретного ключа шифрования, вам необходимо подключиться к IWTM с помощью SSH. Для этого, откройте командную строку (Windows + R → cmd) и ввести команду `ssh root@172.16.1.3` (или `ssh root@iwtm`, если настроен DNS), ввести пароль пользователя root от виртуальной машины IWTM.

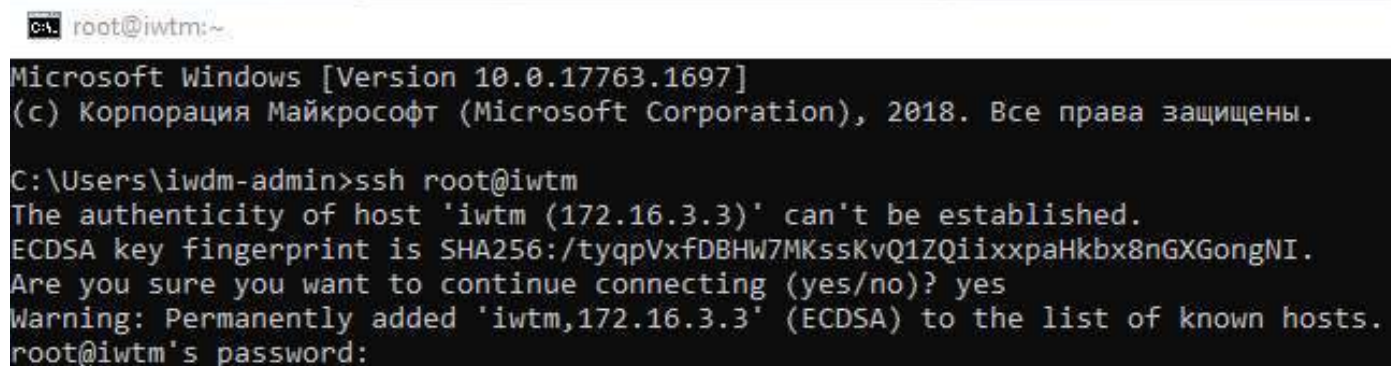


Рисунок 24 – «Подключение к IWTM»

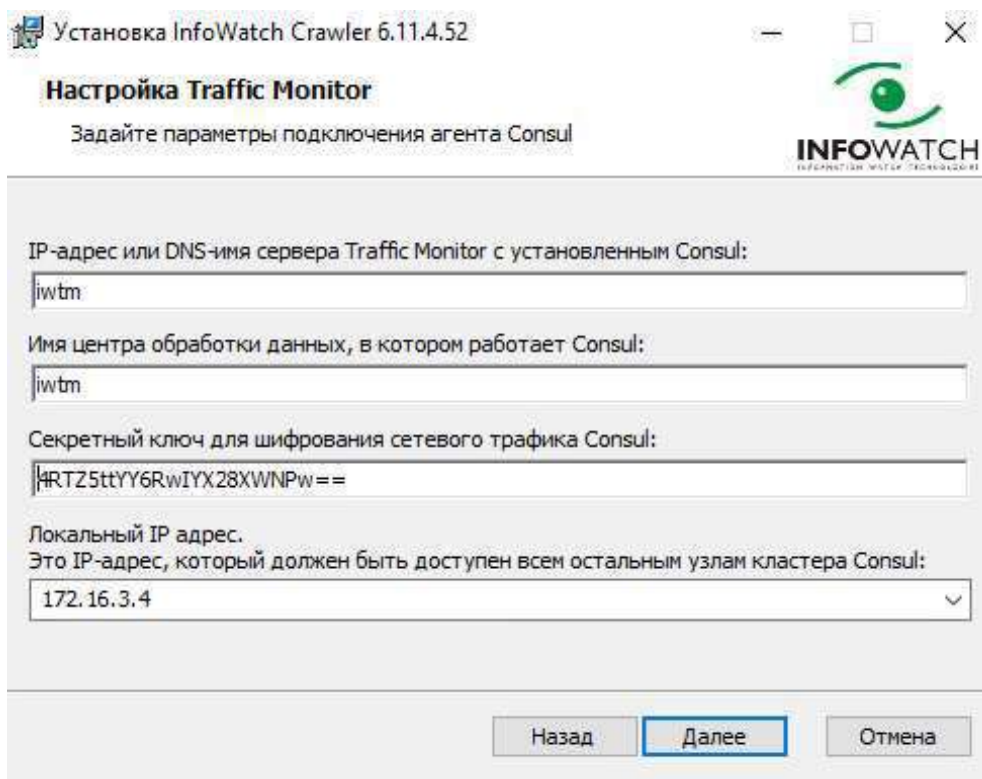
Подключившись к IWTM, вам необходимо открыть файл конфигурации службы Consul (/opt/iw/tm5/etc/consul/consul.json) и скопировать оттуда имя ЦОД



и ключ шифрования. Для того, чтобы прочитать содержимое файла, введите команду **cat /opt/iw/tm5/etc/consul/consul.json**, вывод данной команды покажет имя ЦОД (значения поля **datacenter**) и секретный ключ (значение поля **encrypt**). Скопируйте эти значения и вставьте (без кавычек) в окно установки Crawler и нажмите «Далее».

```
[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/consul.json
{
  "bootstrap_expect": 1,
  "client_addr": "127.0.0.1",
  "data_dir": "/opt/iw/tm5/var/consul",
  "datacenter": "iwtm",
  "disable_update_check": true,
  "enable_syslog": true,
  "encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",
  "leave_on_terminate": false,
  "log_level": "WARN",
  "rejoin_after_leave": true,
  "server": true,
  "skip_leave_on_interrupt": true
}
```

Рисунок 25 – «Конфигурационный файл Consul»



Установка InfoWatch Crawler 6.11.4.52

**Настройка Traffic Monitor**

Задайте параметры подключения агента Consul

IP-адрес или DNS-имя сервера Traffic Monitor с установленным Consul:  
iwtm

Имя центра обработки данных, в котором работает Consul:  
iwtm

Секретный ключ для шифрования сетевого трафика Consul:  
4RTZ5ttYY6RwIYX28XWNPw==

Локальный IP адрес.  
Это IP-адрес, который должен быть доступен всем остальным узлам кластера Consul:  
172.16.3.4

Назад Далее Отмена

Рисунок 26 – «Заполненная информация о Traffic Monitor»

Следующее, что нужно сделать, задать параметры подключения к серверу

Traffic Monitor. Для этого необходимо найти токен плагина краулера, который располагается в веб-интерфейсе IWTM. Войдите, с ранее созданной учетной записью `iwtm-officer`, и во вкладке «Управление» на верхней панели, перейдите к пункту «Плагины».

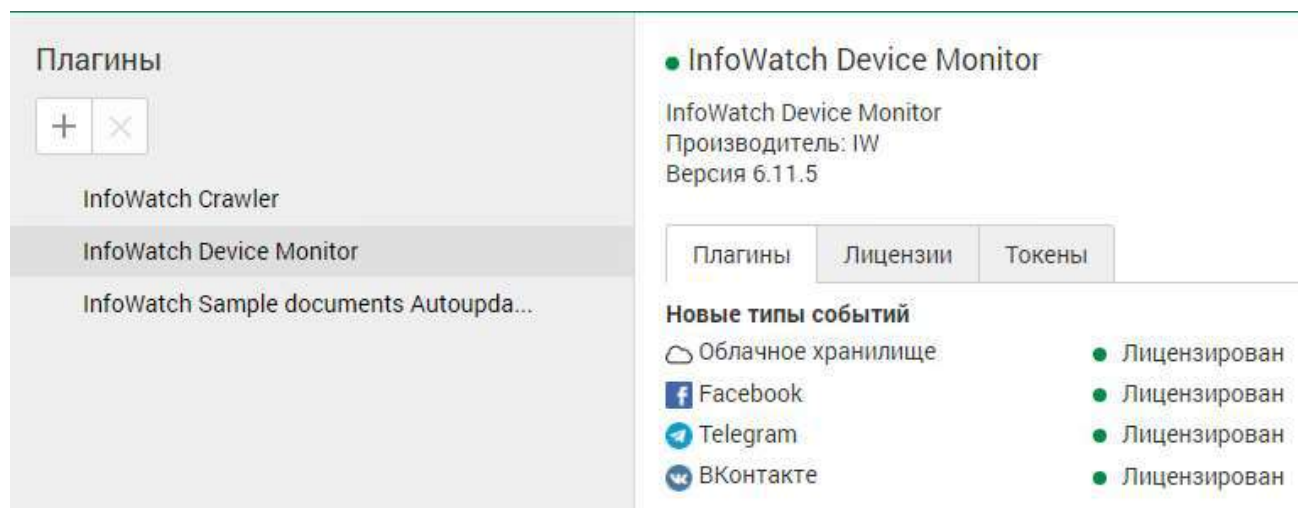


Рисунок 27 – «Плагины Traffic Monitor»

Найдите плагин «InfoWatch Crawler» и перейдите ко вкладке «Токены» внутри. Скопируйте (с помощью кнопки «Скопировать токен». Выделить токен у вас не получится.) содержание активного токена и вставьте в окно установщика Crawler.

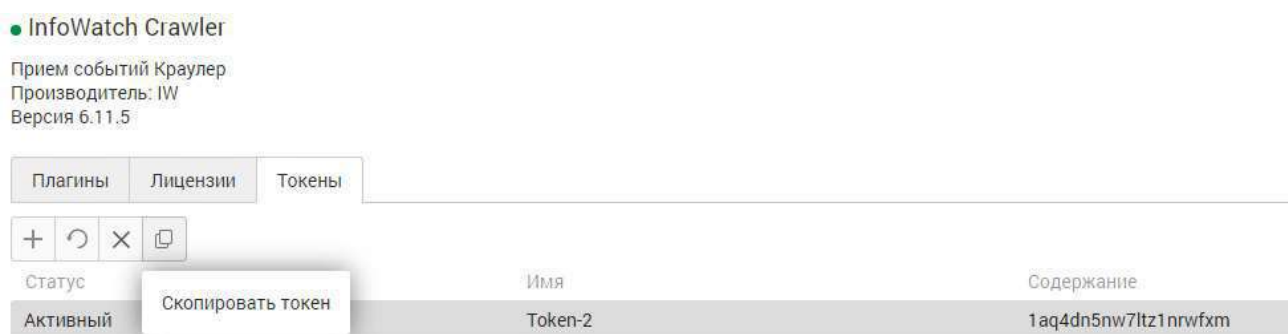


Рисунок 28 – «Токен Crawler»



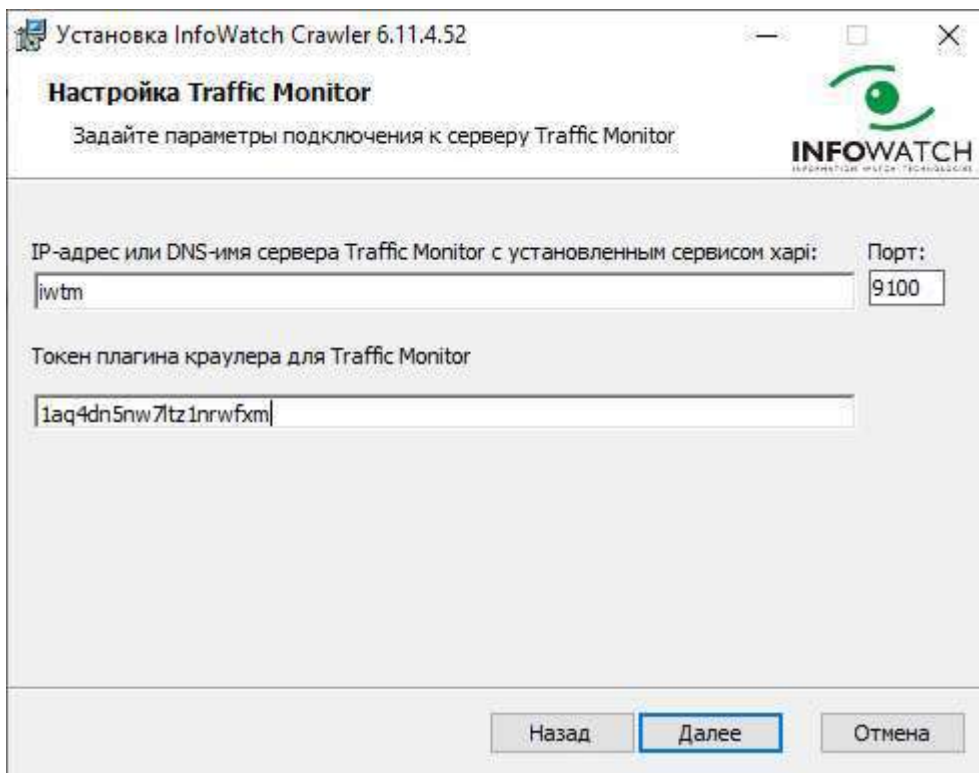


Рисунок 29 – «Заполненная информация о подключении к серверу ТМ»

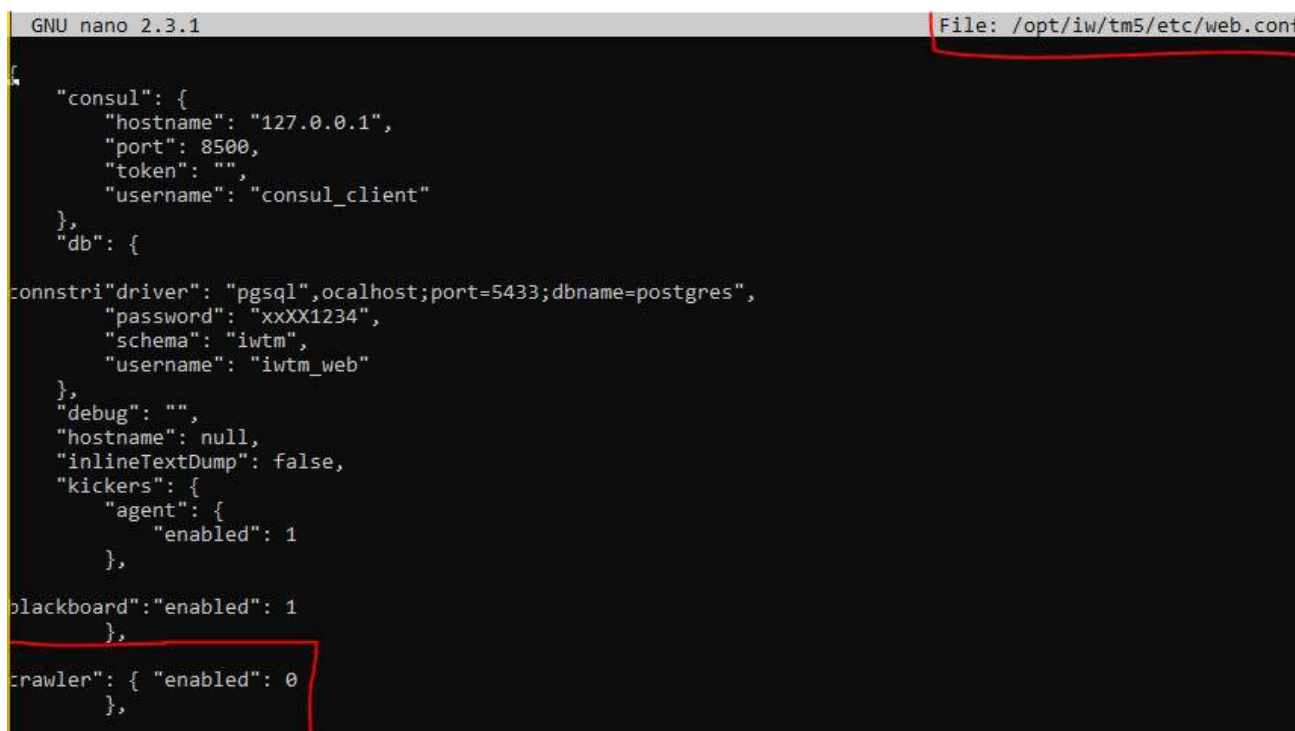
Затем, будет предложено выбрать параметры учетной записи для сервиса сканера – выбирайте «Локальная система». Далее соглашайтесь со всем, до конца установки. Crawler установлен, однако зайдя в веб-интерфейс, вы его не увидите. Чтобы заставить Crawler полноценно функционировать, откройте порты 6556 и 1337, необходимые для работы Crawler. Можете делать это любым способом, но быстрее всего это можно сделать через Powershell: откройте Powershell с правами администратора и введите следующие команды:

```
New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 1337"
-DisplayName "Crawler 1337" -Profile Any -Protocol TCP -LocalPort 1337
```

```
New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 6556"
-DisplayName "Crawler 6556" -Profile Any -Protocol TCP -LocalPort 6556
```

После открытия портов, вновь подключитесь к виртуальной машине IWTM (ssh root@iwtm) и перейдите к конфигурационному файлу /opt/iw/tm5/etc/web.conf. Откройте файл любым текстовым редактором, например

nano (прим.: nano /opt/iw/tm5/etc/web.conf) и, попадая в редактор, измените значение параметра «enabled» с «0» на «1» в параметрах «crawler».



```
GNU nano 2.3.1 File: /opt/iw/tm5/etc/web.conf
{
  "consul": {
    "hostname": "127.0.0.1",
    "port": 8500,
    "token": "",
    "username": "consul_client"
  },
  "db": {
    "driver": "pgsql",
    "connstr": "host=localhost;port=5433;dbname=postgres",
    "password": "xxXX1234",
    "schema": "iwtm",
    "username": "iwtm_web"
  },
  "debug": "",
  "hostname": null,
  "inlineTextDump": false,
  "kickers": {
    "agent": {
      "enabled": 1
    }
  },
  "blackboard": {
    "enabled": 1
  },
  "crawler": {
    "enabled": 0
  }
}
```

Рисунок 30 – «Параметры crawler в web.conf»

Теперь необходимо создать две общие папки, которые будет сканировать Crawler. Для того, чтобы создать общую папку на виртуальной машине IWTM, перейдите в терминал и установите пакет samba, с помощью команды **yum install samba**. После установки samba, создайте папку «share\_iwtm» в корне файловой системы(/) с помощью команды **mkdir /share\_iwtm**. Теперь, отредактируйте права группы с помощью команд **chown -R nobody:nobody /share\_iwtm** и **chmod -R 0755 /share\_iwtm**. Затем, перейдите к конфигурационному файлу samba и перейдите к его редактированию (**nano /etc/samba/smb.conf**).

Приведите файл smb.conf к такому виду:

```
[global]
    map to guest = Bad User

[share_iwtm]
    path = /share_iwtm
    read only = no
    guest ok = yes
    guest only = yes
```

Рисунок 31 – «Содержимое файла /etc/samba/smb.conf»

Теперь, необходимо перезапустить службу SMB и NMB. Сделайте это, с помощью команда **systemctl restart smb** и **systemctl restart nmb**. Отныне, сетевая папка на IWTM настроена и работоспособна, однако, зайти на нее с Windows-машин вы пока не можете, для этого необходимо создать GPO, позволяющее заходить в гостевые общие папки. Это будет сделано в следующем шаге.

Теперь, нужно создать общую папку на IWDWM. Это делается на порядок легче и быстрее. Создайте папку **share\_iwdm** в корне диска C:, затем перейдите к свойствам созданной папки и выберите вкладку «Доступ» (рис. 32). Нажмите «Общий доступ» и выберите пользователей в сети, с которыми нужно поделиться папкой, в нашем случае, это группа – Domain Users (Пользователи домена, если русская винда), затем нажмите «Поделиться» (рис. 33). Готово.

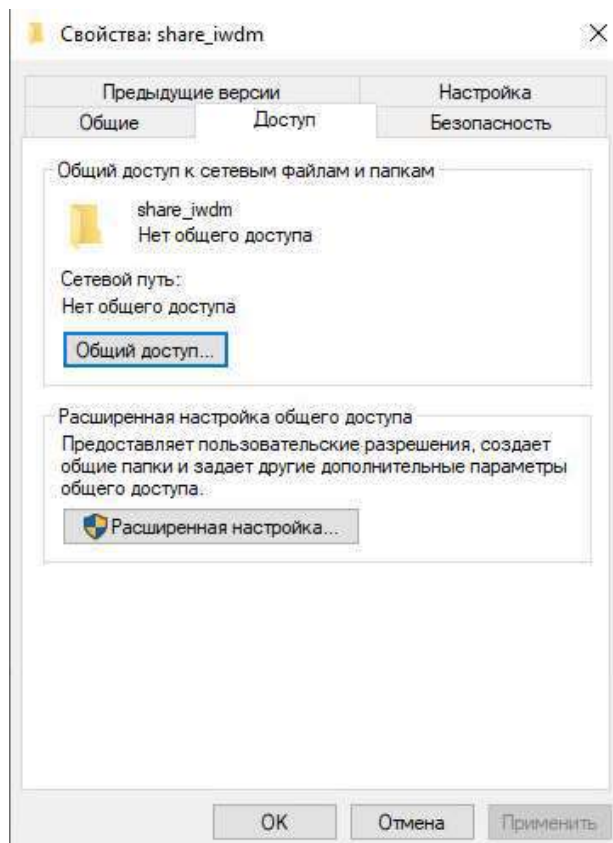


Рисунок 32 – «Доступ к share\_iwdm»

← Доступ к сети

Выберите в сети пользователей, с которыми вы хотите поделиться

Введите имя и нажмите кнопку "Добавить" либо используйте стрелку для поиска определенного пользователя.

Имя	Уровень разрешений
Domain Users	Чтение и запись ▼
iwdm-admin	Владелец

[Проблемы при предоставлении общего доступа](#)

Поделиться | Отмена

Рисунок 33 – «Доступ к share\_iwdm»

После создания двух общих папок, необходимо создать операцию сканирования краулера. Вернитесь к веб-интерфейсу Traffic Monitor и перейдите ко вкладке «Краулер» в верхней части окна. С помощью кнопки «+» (Создать задачу), создайте новую задачу сканирования.

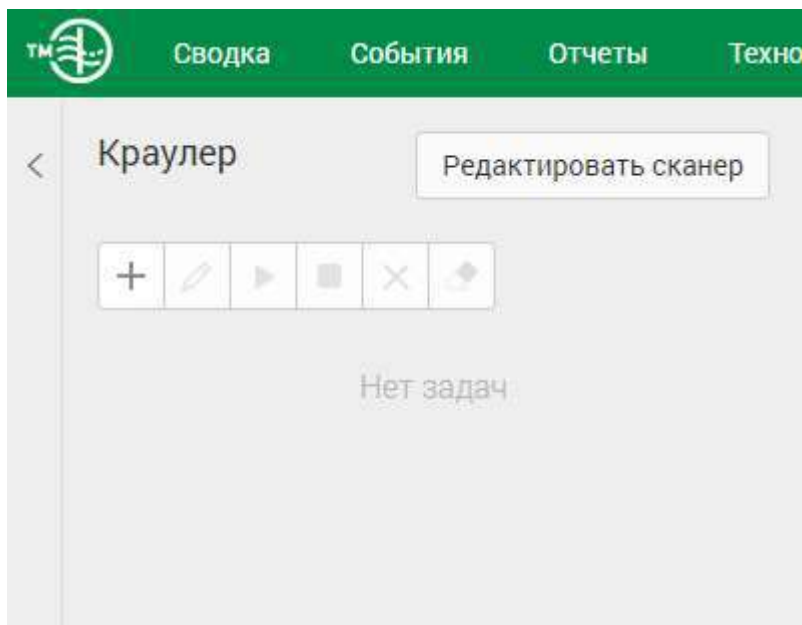


Рисунок 34 – «Краулер»

Далее, заполните параметры:

- Название: произвольное;
- Описание: произвольное;
- Цель сканирования: разделяемые сетевые ресурсы;
- Сканируемые группы и компьютеры: iwtm, iwdm;
- Режим сканирования: все папки;
- Авторизация сканера: да;
- Период сканирования: ежедневно;
- Время: 00:00.

Больше ничего менять не нужно. Создайте два любых текстовых файла в папках share\_iwtm и share\_iwdm, для проверки работы Crawler. Затем вернитесь в веб-интерфейс и запустите задачу сканирования. Готово.

## Модуль 5: Технологии агентского мониторинга

### Задание 1

Необходимо применить групповые политики Windows для OU «Office».

#### **Групповая политика 1:**

- Минимальная длина пароля должна составлять 7 символов;
  - Срок жизни пароля должен составлять 192 дня;
- Выполнение задания подтвердить скриншотами.

#### **Групповая политика 2:**

- Отключить возможность локального входа для пользователей iwtm-officer и Idapsync-user с помощью групповых политик
- Выполнение задания подтвердить скриншотами.

#### **Групповая политика 3:**

- С помощью редактора групповой политики запретить показ анимации при входе в систему. Выполнение задания подтвердить скриншотами.

#### **Групповая политика 4:**

- С помощью редактора групповой политики настройте запрет запуска msinfo32.exe. Выполнение задания подтвердить скриншотами.

#### **Групповая политика 5:**

- С помощью редактора групповой политики ограничить доступ к панели управления. Выполнение задания подтвердить скриншотами.

Для создания и редактирования групповых политик перейдите к виртуальной машине demolab (контроллер домена) и откройте оснастку «Управление групповой политикой» (Пуск → Средства Администрирования Windows → Управление групповой политикой). В открывшейся оснастке выберите лес, перейдите в подпапку «домены» и выберите соответствующий домен.

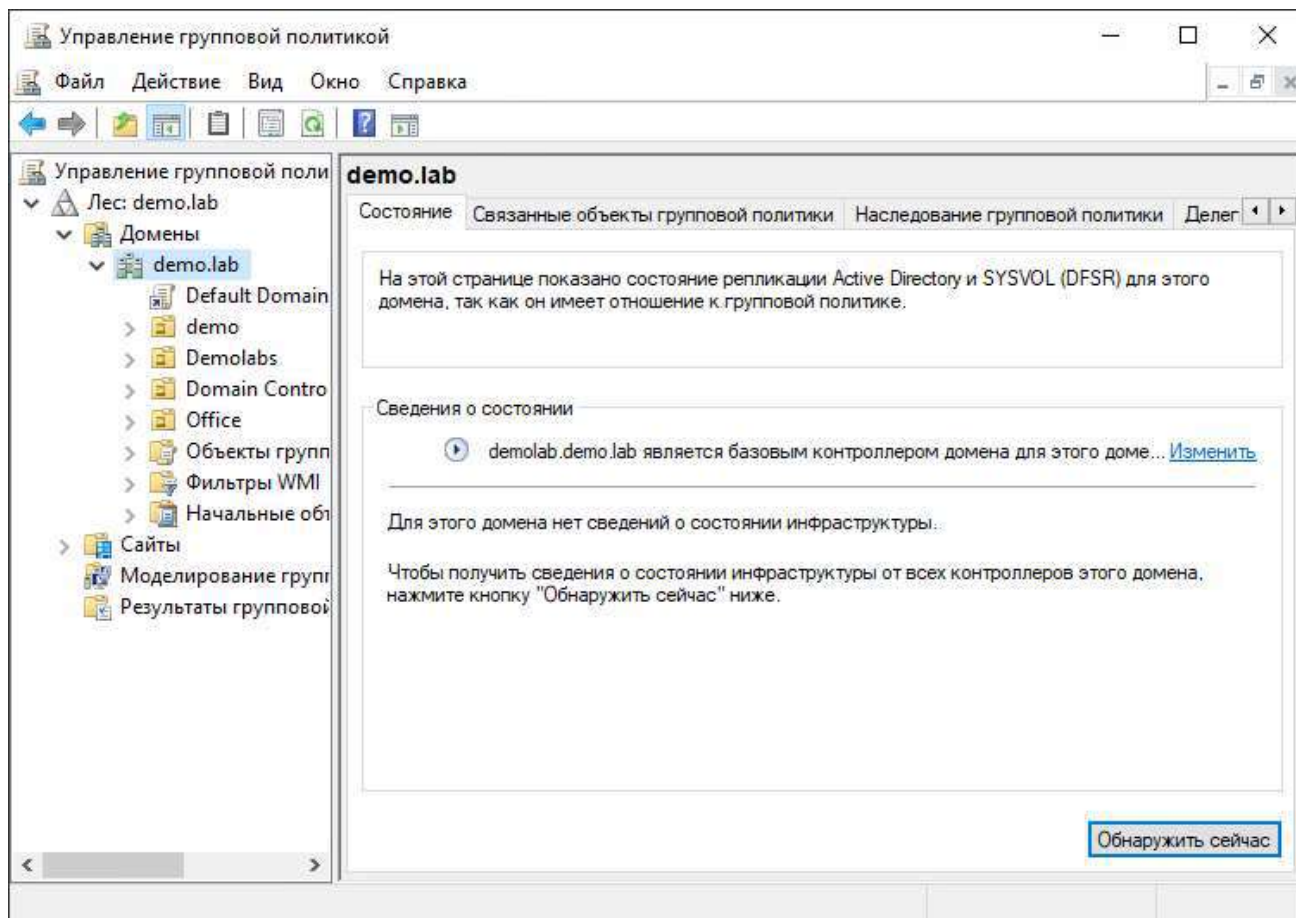


Рисунок 35 – «Управление групповыми политиками»

Кликните ПКМ по домену, чтобы открыть контекстное меню и выберите «Создать объект групповой политики в этом домене и связать его...» (рис. 36), назовите объект произвольным именем (прим.: Office). Затем сразу отредактируйте фильтры безопасности созданной политики. Для этого откройте созданный объект политики, удалите «Прошедшие проверку» (рис. 37) и добавьте группу «Domain Computers» (Компьютеры домена, если русская винда) и, созданную ранее, группу Office (рис. 38).



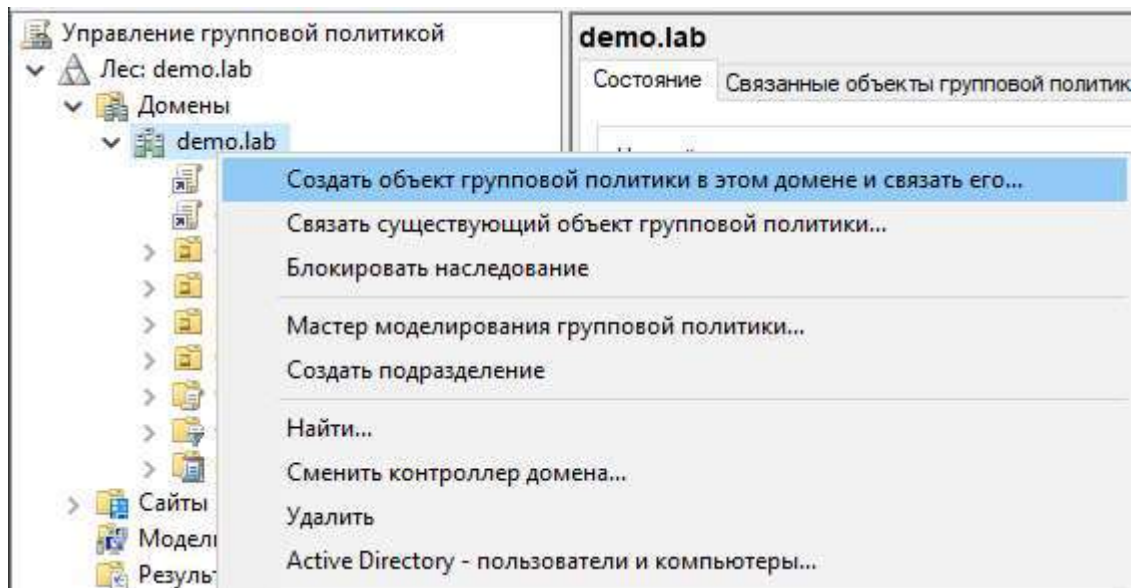


Рисунок 36 – «Создание объекта группой политики»

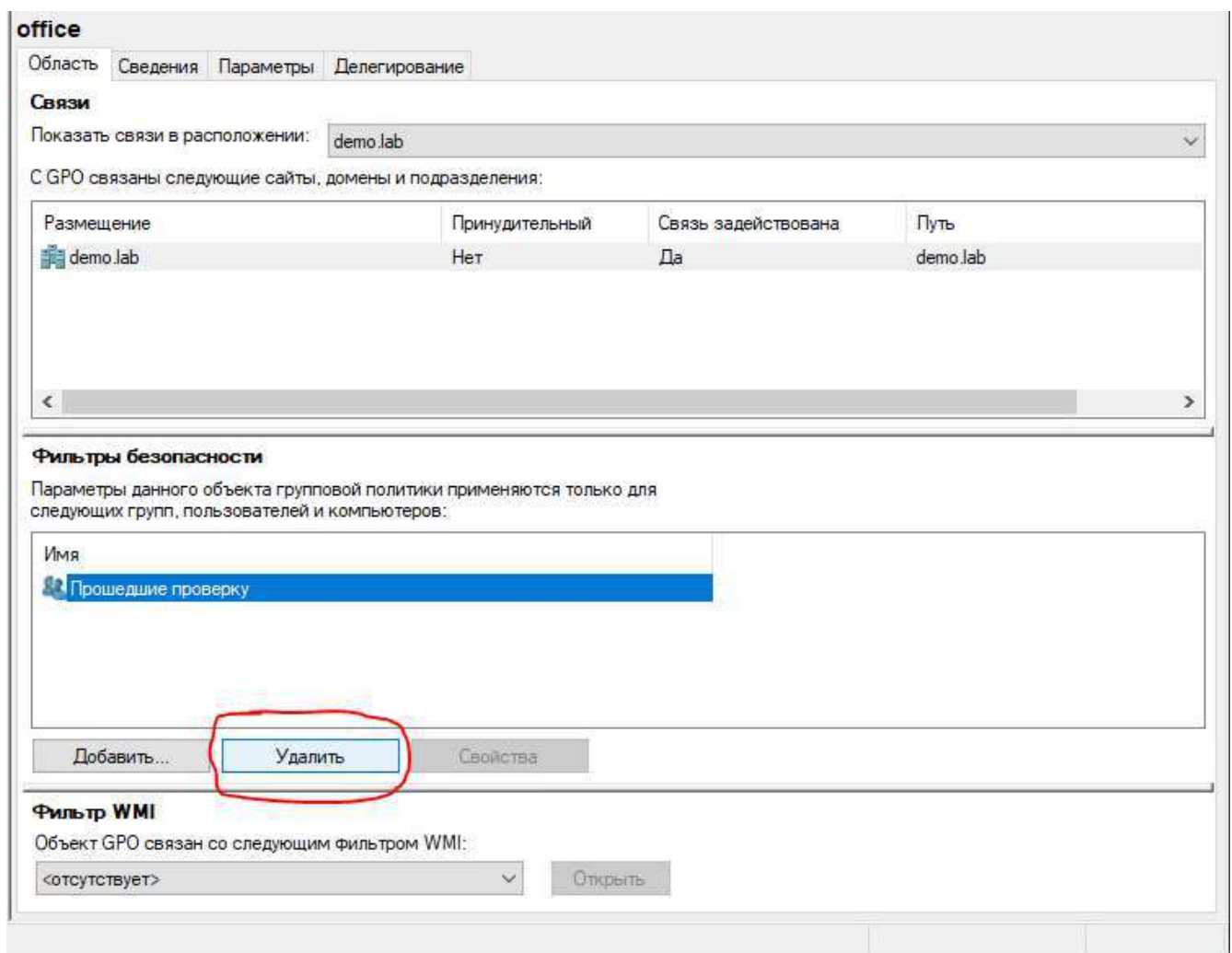


Рисунок 37 – «Редактирование фильтров безопасности»



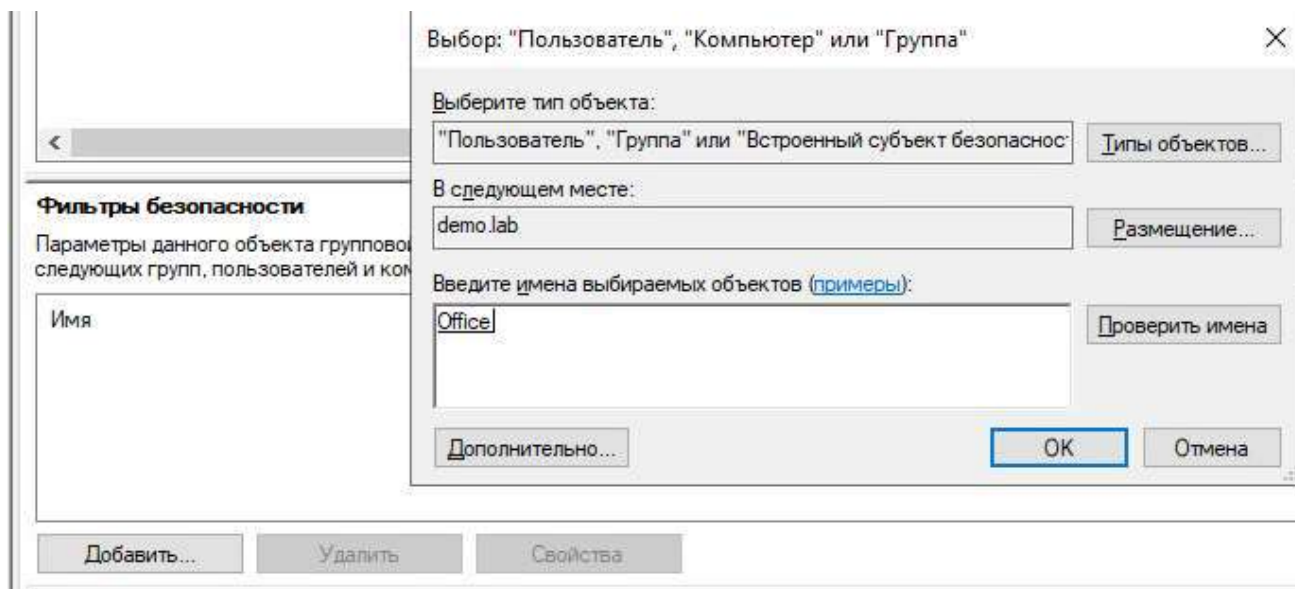


Рисунок 38 – «Добавление фильтров безопасности»

Чтобы перейти к редактированию объекта групповой политики, кликните на нем ПКМ и, в контекстном меню, выберите «Изменить», после чего откроется редактор управления групповыми политиками. Интерфейс интуитивно понятен, проблем возникнуть не должно:

- Политика 1:
  - Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политика паролей → Максимальный срок действия пароля = 192 дн. + Минимальная длина пароля = 7 зн.
- Политика 2:
  - Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя → Запретить локальный вход = DEMO\iwtm-officer, DEMO\ldapsync-user
- Политика 3:
  - Конфигурация компьютера → Политики → Административные шаблоны → Система → Вход в систему → Показать анимацию при первом входе в систему = Отключено.
- Политика 4:

- Конфигурация пользователя → Политики → Административные шаблоны → Система → Не запускать указанные приложения Windows → msinfo32.exe
- Политика 5:
  - Конфигурация пользователя → Политики → Административные шаблоны → Панель управления → Запретить доступ к панели управления = включено.
- Политика 6 (чтобы работала общая папка IWTM, это обязательно):
  - Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Рабочая станция Lanman → включить небезопасные гостевые входы = Включено.

## Задание 2

Используйте для входа в консоль IWDM доменного пользователя **iwdm-admin**.

Задать максимальные права пользователя на работу в консоли IWDM.

*Проверить работоспособность, зафиксировать настройку и выполнение скриншотом запущенной консоли.*

## Задание 3

Необходимо создать новые политики (кроме политики на устройства по умолчанию),

### **Политика 1:**

Название: «**Отдел 1**»

Группа компьютеров: Виртуальная машина пользователя **userofficer-1**

### **Политика 2:**

Название: «**Отдел 2**»

Группа компьютеров: Виртуальная машина пользователя **userofficer-2**

*Зафиксировать выполнение скриншотами.*

Перед началом работы с консолью Device Monitor необходимо установить службы Device Monitor и СУБД PostgreSQL, для этого перейдите к виртуальной машине IWDM (ВМ для работы в Device Monitor) и обнаружьте установочный файл, на подобии с Crawler, СУБД PostgreSQL (postgresql-\*-windows-x64) и запустите его. Возможно, до запуска самой программы установки PostgreSQL, установятся дополнительные компоненты.



Рисунок 39 – «Установка PostgreSQL»

Соглашайтесь со всем подряд ничего не меняя, до этапа создания пароля. В качестве пароля введите произвольный пароль, **однако крайне рекомендую поставить стандартный пароль – xxXX1234**. Далее, начиная с сетевого порта, ничего не меняйте, до конца установки. В конце установки уберите галочку с пункта «Launch Stack Builder at exit?» и закройте установочный файл. Последнее, что нужно сделать для работы БД – отредактировать файл подключений pg\_hba.conf. Перейдите к папке C:\Program Files\PostgreSQL\10\data и найдите файл pg\_hba.conf – откройте его с помощью приложения Блокнот.

В открывшейся файл добавьте строку «host all all 0.0.0.0/0», в секцию «IPv4 local connections».

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# IPv4 local connections:					
host	all		all	127.0.0.1/32	md5
host	all		all	0.0.0.0/0	md5
# IPv6 local connections:					
host	all		all	:::1/128	md5
# Allow replication connections from localhost, by a user with the					
# replication privilege.					
host	replication		all	127.0.0.1/32	md5
host	replication		all	:::1/128	md5

Рисунок 40 – «Редактирование pg\_hba.conf»

Найдите и запустите установочный файл Device Monitor (Setup.Device.Monitor.ru.\*).

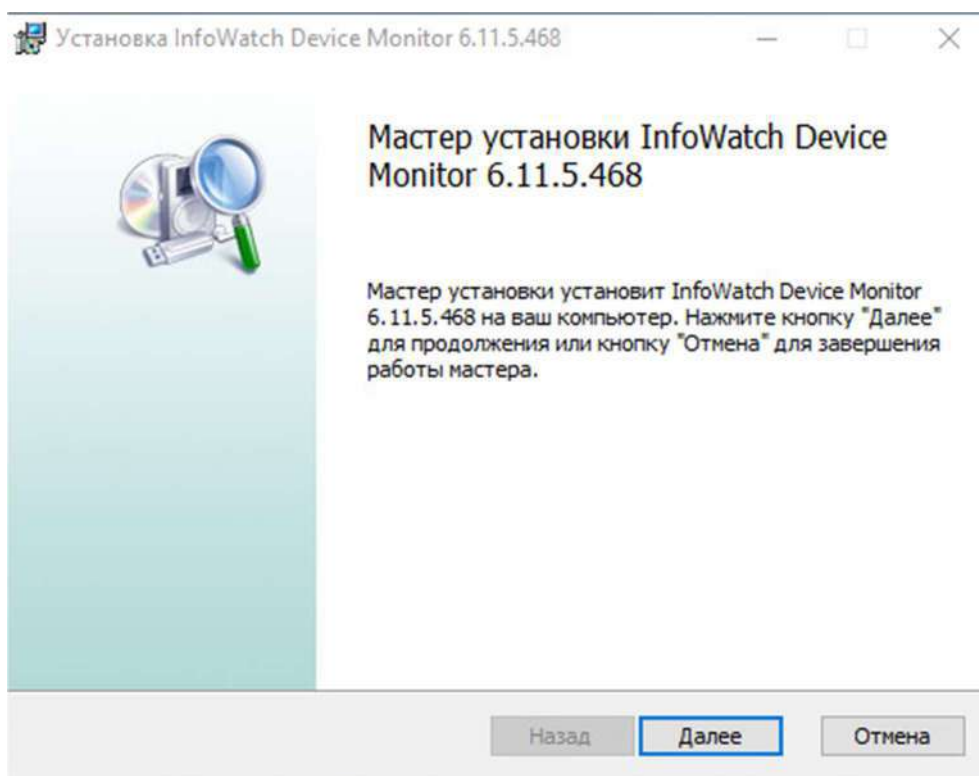


Рисунок 40 – «Установка Device Monitor»

Примите лицензионное соглашение, и, на этапе выборочной установки, выберите оба компонента (сервер и консоль управления). Перейдите к следующему этапу установки, названному «Тип устанавливаемого сервера»,

выберите тип сервера, и отметьте галочками пункты «Опубликовать сервер в Active Directory» и «Установить новую базу данных». Далее, выберите базу данных – PostgreSQL, и, перейдя к следующему этапу, введите параметры подключения к БД (рис. 40), с ранее созданным паролем.

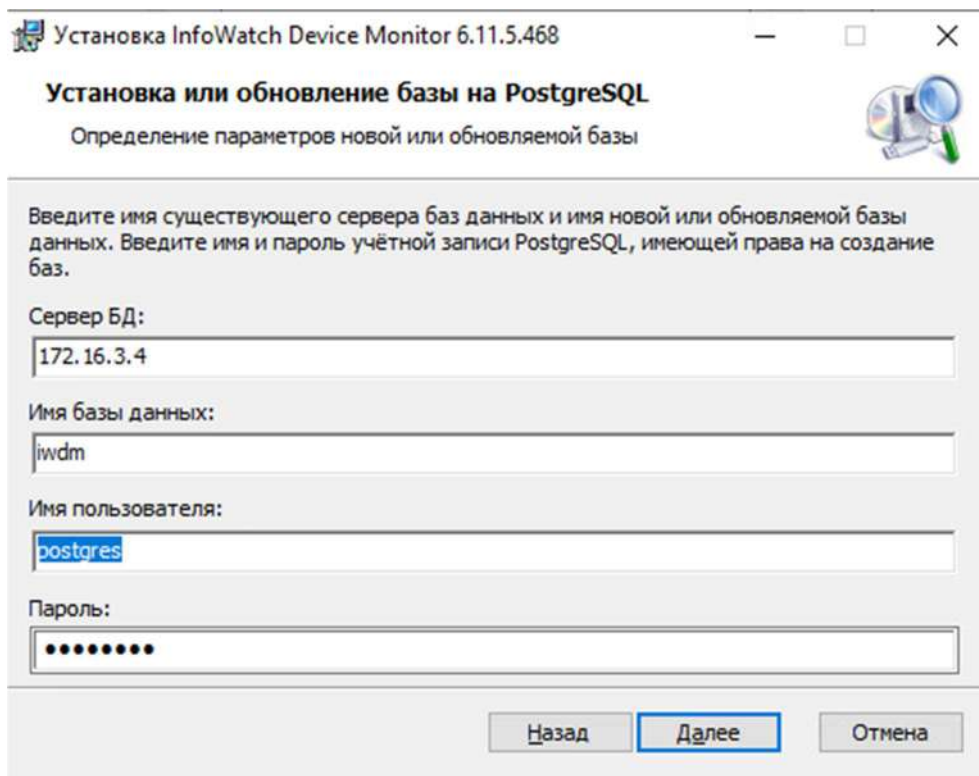


Рисунок 41 – «Параметры подключения к БД»

Соглашайтесь со всем подряд до пункта «Настройки защищенного канала». На этом пункте также согласитесь, ничего не изменяя, однако вам будет предложено сохранить ключ защищенного канала, для этого откроется окно проводника. Сохраните ключ с произвольным именем в любом месте. Продвигайтесь по установке далее, ничего не меняя. Дойдя до пункта «Учетная запись Администратора» - укажите имя администратора (admin), и пароль (xxXX1234). Затем, настройте соединение с Traffic Monitor (рис. 42), укажите адрес (iwtm) и токен авторизации (возьмите его из веб-интерфейса IWTM). Нажмите далее и установите Device Monitor. По окончании установки на рабочем столе появится ярлык «Консоль управления», для начала работы с IWDM – откройте его и войдите в консоль (адрес – localhost, логин – admin, пароль – xxXX1234).

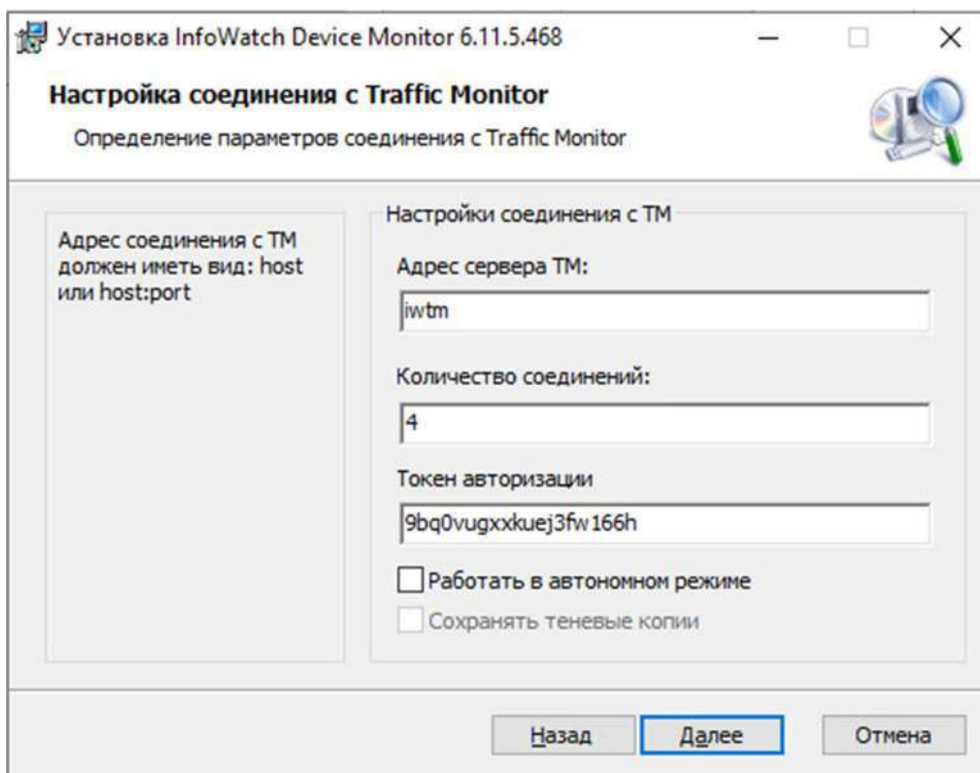


Рисунок 42 – «Параметры подключения к Traffic Monitor»

Перейдите ко вкладке «Инструменты» и откройте «Пользователи консоли и роли».

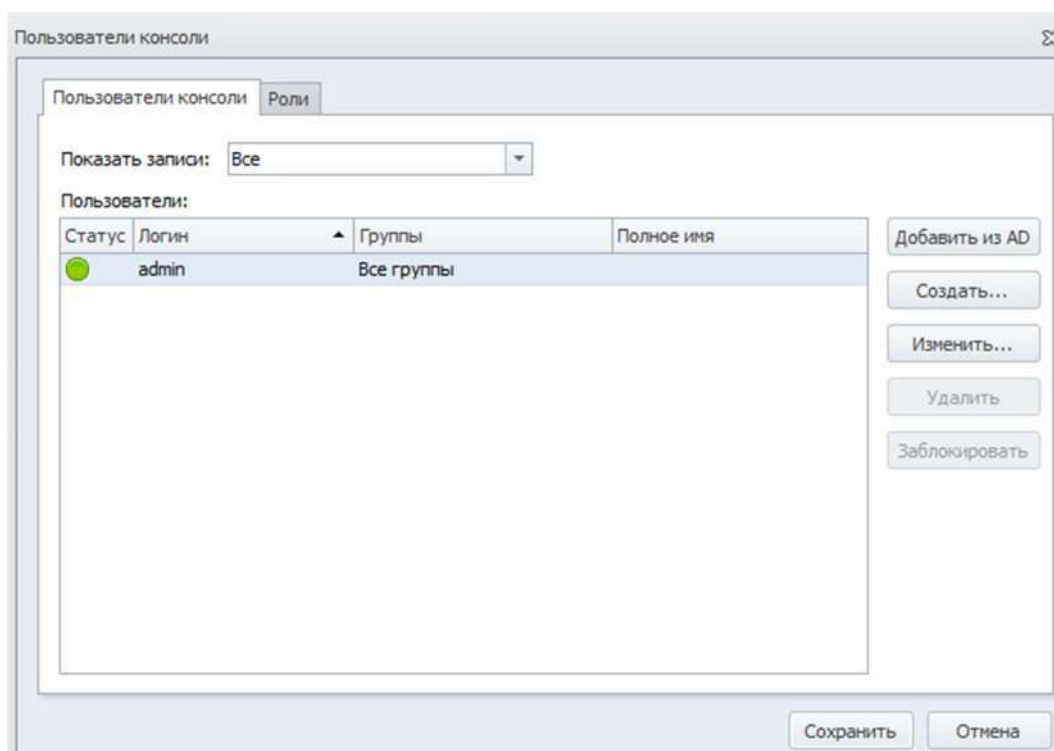


Рисунок 43 – «Пользователи консоли»

В открывшемся окне нажмите кнопку «Добавить из AD», после чего, в поле «Выберите добавляемого пользователя» введите «iwdm-admin» и нажмите «Сохранить», затем откроется дополнительное окно для управления ролями пользователя (рис. 44). Во всех доступных полях добавьте все, что только можно, ведь пользователь должен иметь максимальные права. Ваша задача сделать так, как на (рис. 45). Затем сохраните и вернитесь к настройкам. Найдите пункт «Интеграция с Active Directory», откройте его и создайте новое подключение:

- Имя домена: demo.lab;
- Синхронизировать: Компьютеры;
- Синхронизируемые директории: Все директории.

Более ничего не меняйте и сохраните подключение. Создайте второе подключение по аналогии с первым, но в пункте «Синхронизировать», выберите «Пользователи»



Создание пользователя

Логин: DEMO\jwdm-admin

Пароль: \*\*\*\*\*

Повтор пароля: \*\*\*\*\*

Полное имя: jwdm-admin

Видит сотрудников

Группа сотрудников	Роль пользователя

Добавить...  
Изменить...  
Удалить

Видит компьютеры

Группа компьютеров	Роль пользователя

Добавить...  
Изменить...  
Удалить

Общие роли

--

Выбрать  
Удалить

Сохранить

Отмена

Рисунок 44 – «Пользователи консоли»