

Министерство образования и науки РС(Я)  
ГАПОУ РС(Я) «Якутский колледж связи и энергетики им. П.И. Дудкина»

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**  
по подготовке и выполнению  
заданий демонстрационного экзамена  
по компетенции №F7 «Корпоративная защита от внутренних угроз  
информационной безопасности»

Якутск 2022

## **АННОТАЦИЯ**

Методические рекомендации для студентов учреждений СПО по подготовке и выполнению заданий демонстрационного экзамена по компетенции №F7 «Корпоративная защита от внутренних угроз информационной безопасности» / Автор–составитель: Петров А.М. – Якутск: ГАПОУ РС(Я) «Якутский колледж связи и энергетики им. П.И. Дудкина», 2022.

## СОДЕРЖАНИЕ

Введение	4
1. Установка и настройка операционных систем	5
1.1. Установка сервера AD-demo.lab	5
1.2. Установка сервера Device Monitor	11
1.3. Установка сервера Traffic Monitor	12
1.4. Установка «Нарушителей»	21
2. Установка и конфигурирование компонентов dlp системы	22
2.1. Настройка контроллера домена	22
2.2. Настройка DLP сервера	26
2.3. Проверка работоспособности сервера и клиента агентского мониторинга.	33
2.4. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)	46
2.5. Проверка работоспособности системы	53
Заключение	54
Список использованных источников	55

## **ВВЕДЕНИЕ**

Настоящие методические рекомендации по модулю «Установка и конфигурирование DLP системы» по стандартам демонстрационного экзамена Ворлдскиллс Россия разработаны для обучающихся образовательных учреждений при реализации основных профессиональных образовательных программ среднего профессионального образования для подготовки и выполнения заданий по компетенции №F7 «Корпоративная защита от внутренних угроз информационной безопасности» в 2022 году.

Методические рекомендации разработаны с целью эффективной организации подготовки обучающихся к процедуре демонстрационного экзамена в образовательных организациях, реализующих программы среднего профессионального образования.

Цель методических рекомендаций - объяснить студентам технологию работы на площадке демонстрационного экзамена и алгоритм выполнения задания демонстрационного экзамена в условиях введения режима повышенной готовности.

## 1. УСТАНОВКА И НАСТРОЙКА ОПЕРАЦИОННЫХ СИСТЕМ

Разворачиваем операционные системы:

1. AD Сервер с контроллером домена;
2. DLP сервер;
3. Виртуальная машина сервера агентского мониторинга;
4. Виртуальные машины «нарушителей».

### 1.1. Установка сервера AD-demo.lab

Установите виртуальную машину Windows Server 2019, затем задайте сетевые настройки в соответствии с рисунком.

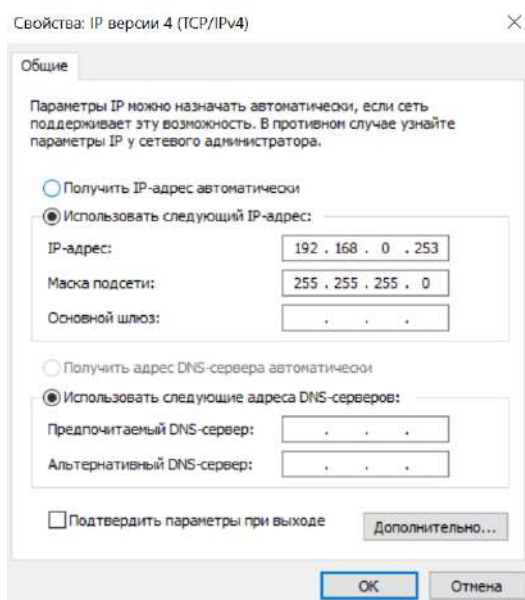


Рисунок 1.1 – Настройка сети AD-demo.lab

Перед разворачиванием домена задайте пароль администратору, для этого открываем "Управление компьютером" – "Служебные программы" – "Локальные пользователи" – "Пользователи", найдите администратора и задайте ему пароль - ххXX1234.

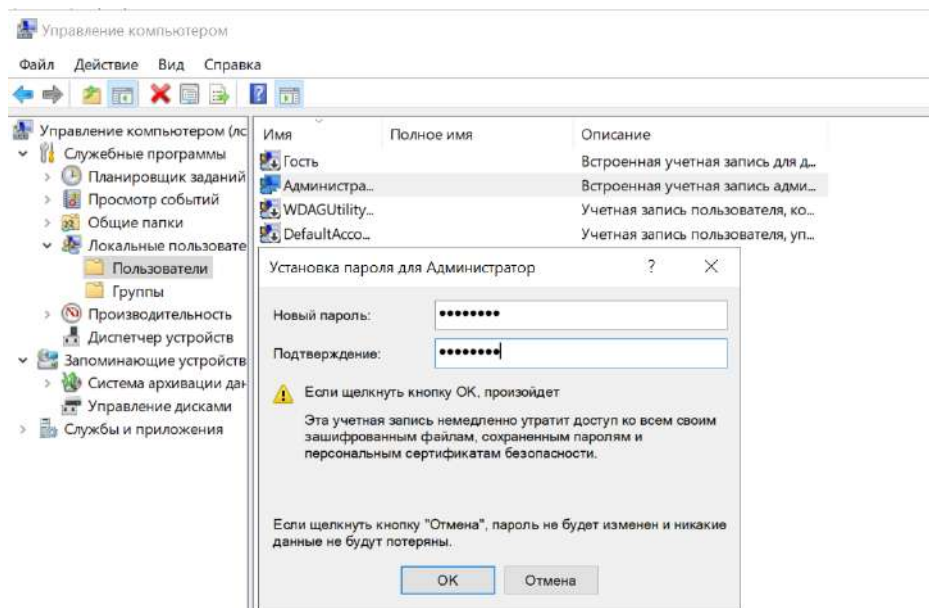


Рисунок 1.2 – Установка пароля для администратора

Установка Active Directory через сервер менеджеров. Для того, чтобы развернуть домен, откройте диспетчер серверов и в пункте "Управление" нажмите "Добавить роли и компоненты".



Рисунок 1.3 – Роли и компоненты

Выберите сервер, на который будут установлены роли и компоненты и нажмите "Далее".

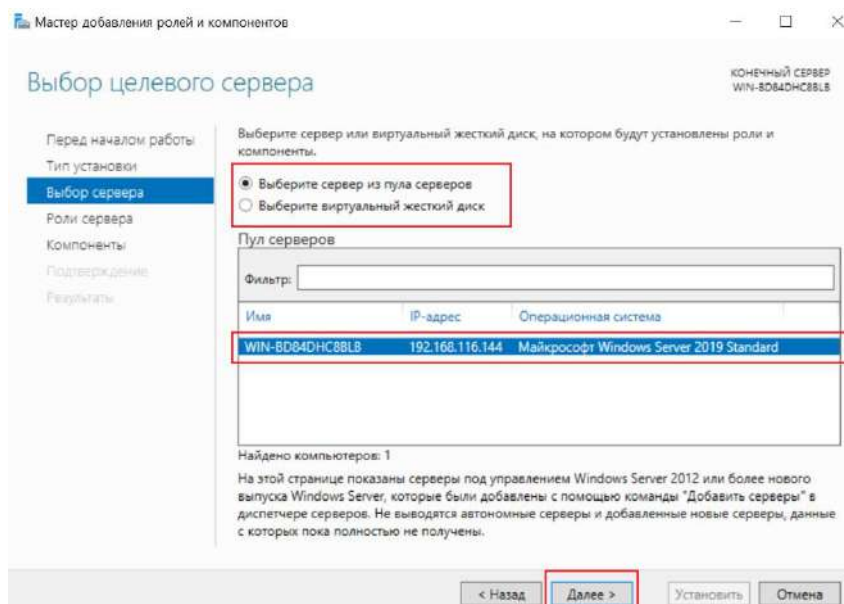


Рисунок 1.4 – Выбор целевого сервера

Установите флажок напротив выбранных ролей сервера, в данном случае это – Доменные службы Active Directory, нажмите "Далее".

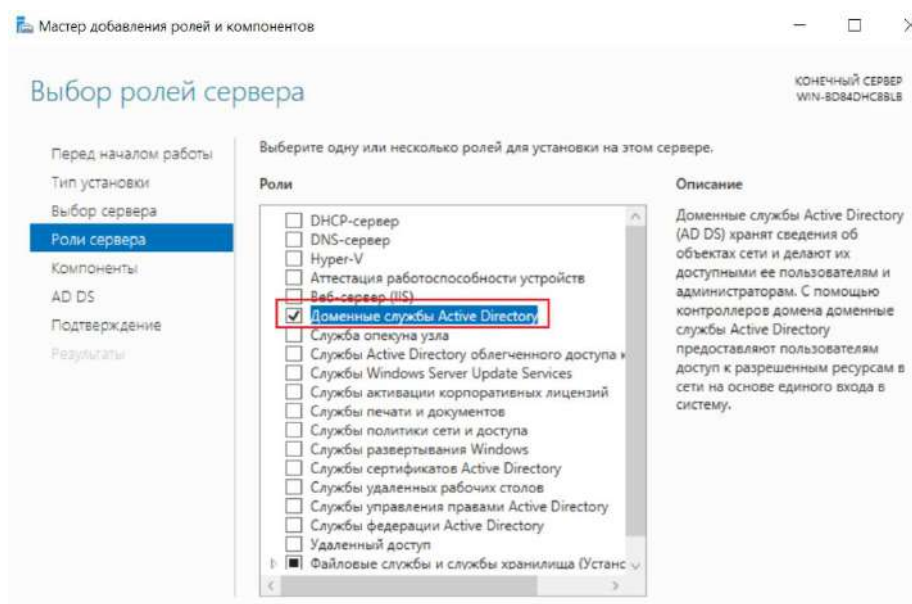


Рисунок 1.5 – Выбор ролей сервера

В компонентах установите флажок напротив "Функции .NET Framework 3.5".

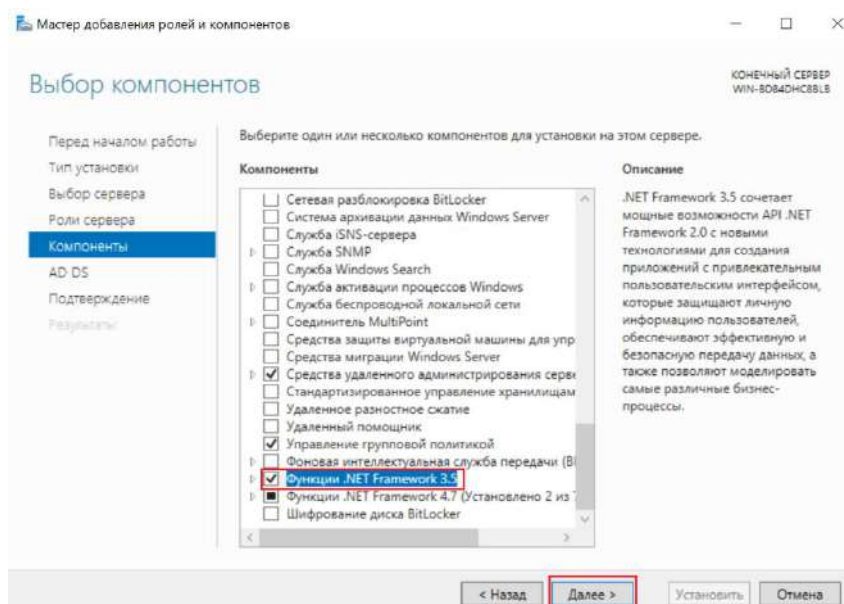


Рисунок 1.6 – Выбор компонентов

Ставим флажок напротив "Автоматический перезапуск конечного сервера, если требуется", нажмите "Установить". В результате произойдет установка выбранных ролей сервера.

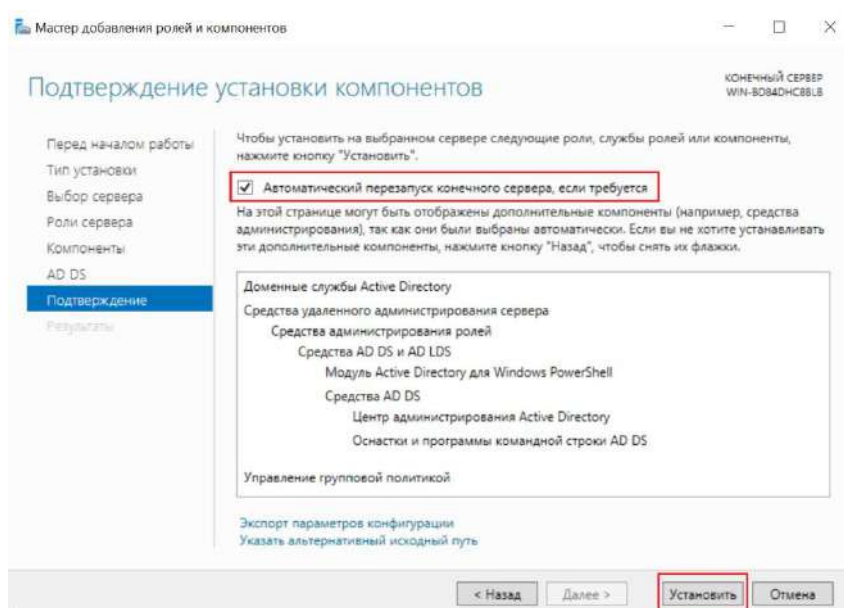


Рисунок 1.7 – Подтверждение установки

После установки необходимо повысить роль сервера до уровня контроллера домена. Для этого нажмите "Повысить роль этого сервера до уровня контроллера домена".



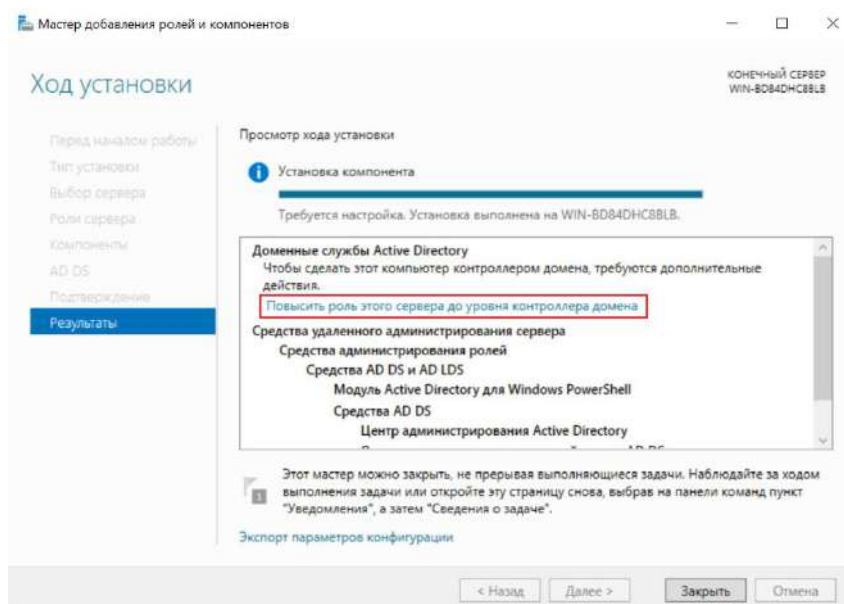


Рисунок 1.8 – Повышение роли сервера

Запускается мастер конфигурации доменных служб Active Directory. В разделе "Операция развёртывания" нужно выбрать один из трёх вариантов:

- Добавить контроллер домена в существующий домен
- Добавить новый домен в существующий лес
- Добавить новый лес

Первый вариант не подходит, так как нет текущего домена, создаём новый. По той же причине второй вариант тоже не подходит. Выберите "Добавить новый лес". И дайте имя корневого домена – demo.lab.

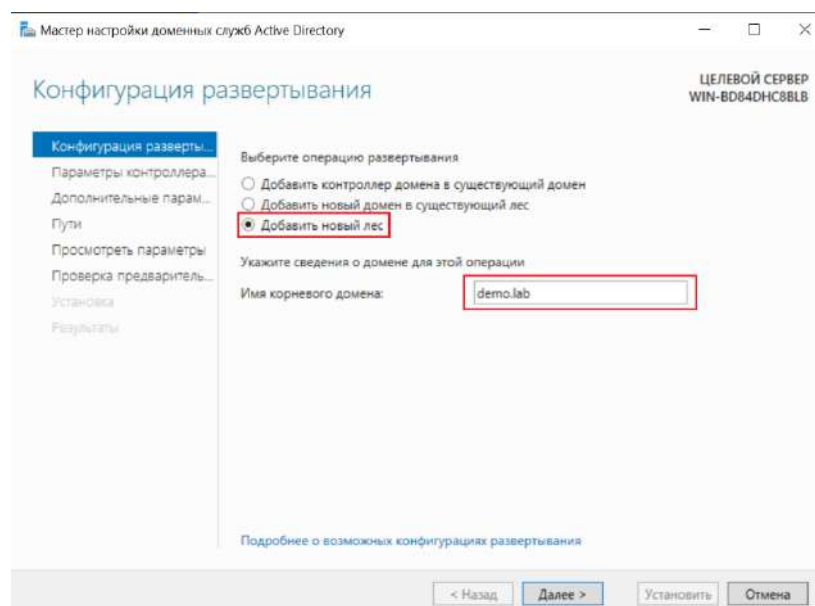


Рисунок 1.9 – Конфигурация развёртывания

В режиме работы леса и режиме работы домена указываются минимальные версии серверной операционной системы, которая будет поддерживаться доменом.

Указываем пароль для режима восстановления служб каталогов (DSRM) – xxXX1234.

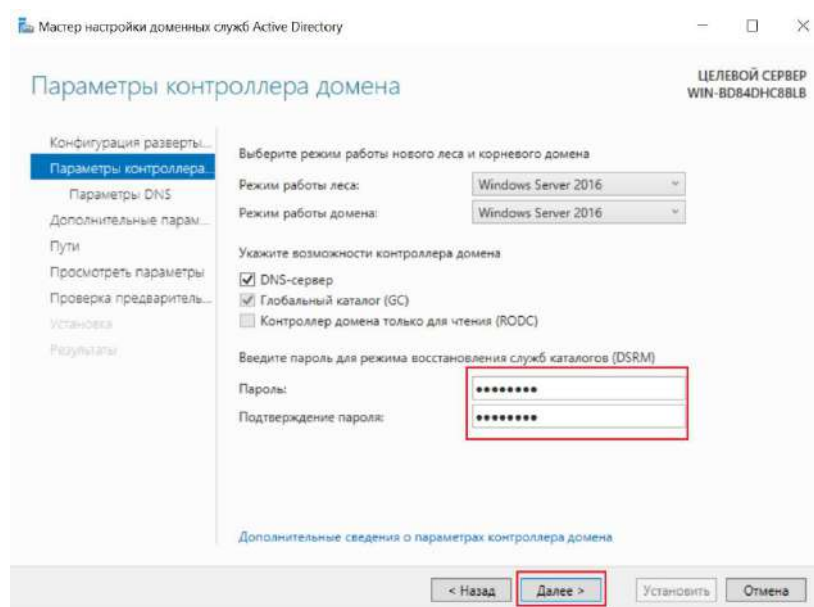


Рисунок 1.10 – Параметры контроллера домена

После успешной проверки предварительных требований нажмите "Установить". Начнется процесс установки

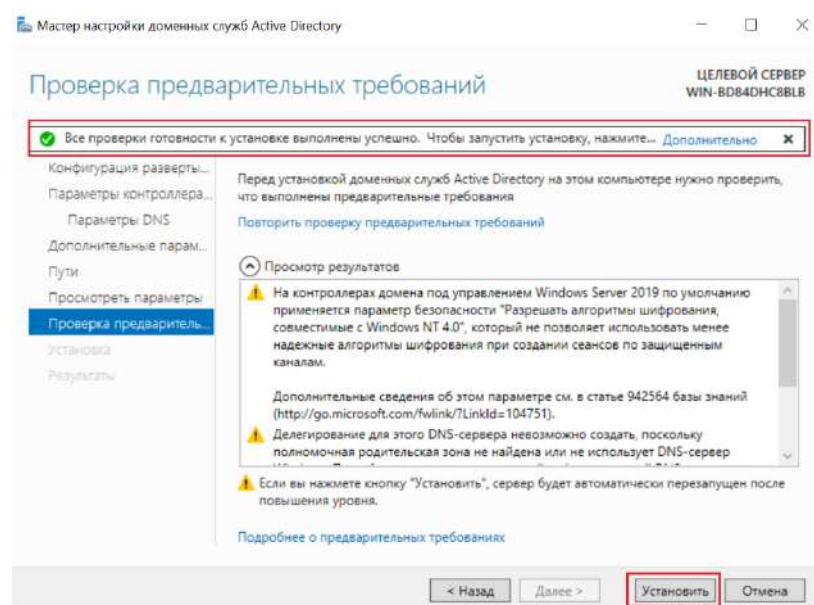


Рисунок 1.11 – Установка

После завершения установки, выйдет окно с предупреждением о перезагрузке сервера. Нажмите "Заккрыть", после начнется перезагрузка системы.

## 1.2. Установка сервера Device Monitor

Установите виртуальную машину Windows Server 2019, затем задайте сетевые настройки в соответствии с рисунком.

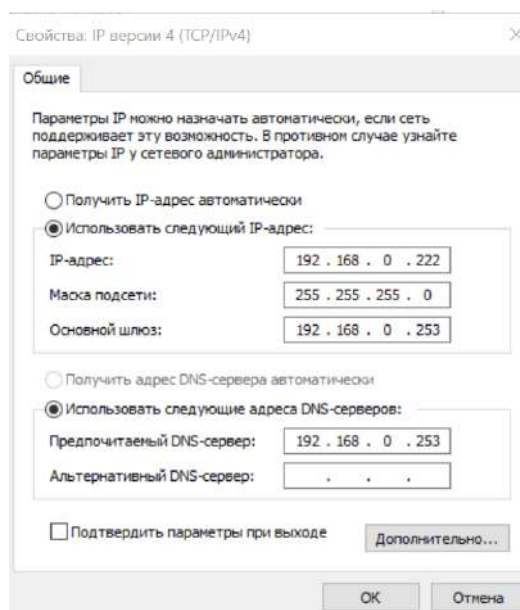


Рисунок 1.12 – Настройки сети DM

После настройки сети, переименуйте и введите виртуальную машину DM в домен demo.lab.

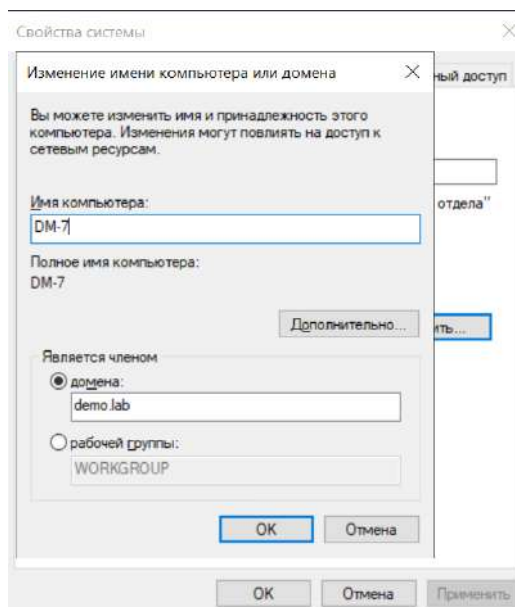


Рисунок 1.13 – Изменение имени и домена DM

### 1.3. Установка сервера Traffic Monitor

Первый экран мастера установки (kickstart) позволяет выбрать одно из следующих действий:

- **TM Enterprise** – начнется установка InfoWatch Traffic Monitor Enterprise;
- **TM Standard** – начнется установка InfoWatch Traffic Monitor Standard;
- **Boot from local drive** – выполняется загрузка с локального диска компьютера;
- **Rescue installed system** – выполняется аварийное восстановление системы InfoWatch Traffic Monitor;
- **Rescue installed system** – выполняется аварийное восстановление системы InfoWatch Traffic Monitor.

Выбираем TM Enterprise и нажимаем Enter

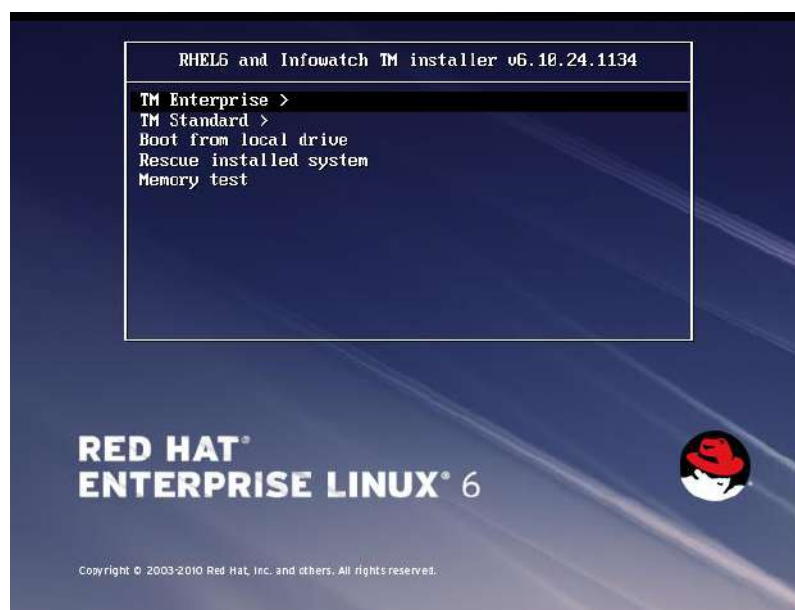


Рисунок 1.14 – Первый экран мастера установки

Для редакции Enterprise инсталлятор предложит выбрать СУБД, которая должна быть установлена:

- DB – Oracle Enterprise;
- DB – PostgreSQL.

Выбираем DB – PostgreSQL.



Рисунок 1.15 – Выбор СУБД

Выбор режима установки. После выбора СУБД потребуется выбрать режим установки. Набор режимов зависит от выбора, сделанного на предыдущих шагах установки. В случае выбора базы данных PostgreSQL, будут предоставлены следующие режимы установки:

- **TMS All-in-one: TM+DB server - PostgreSQL** – все компоненты Системы (с СУБД Oracle или 21 PostgreSQL) устанавливаются на один сервер;
- **TME DB server PostgreSQL** – установка базы данных вместе с выбранной СУБД на отдельный компьютер;
- **TME Node server PostgreSQL** – установка сервера Traffic Monitor на отдельный компьютер.

Выберите режим установки *TMS All-in-one: TM+DB server – PostgreSQL* и нажмите Enter.

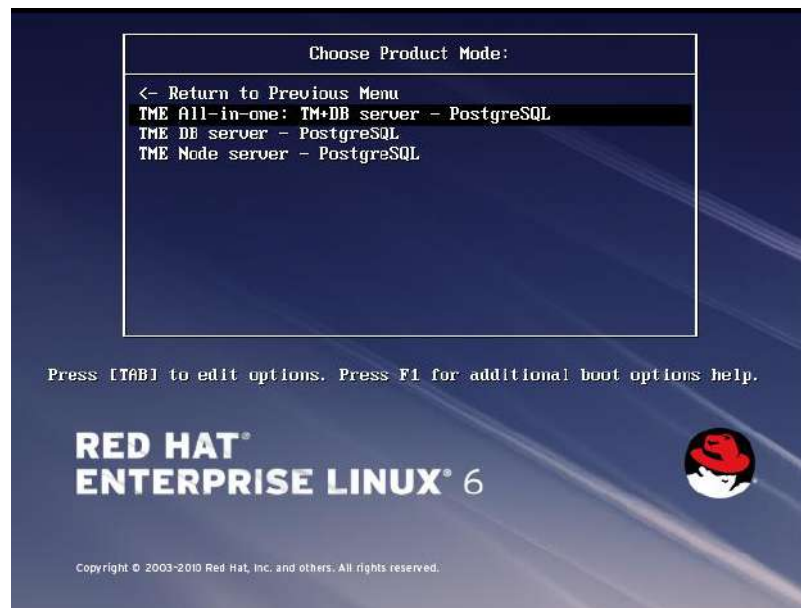


Рисунок 1.16 – Выбор режима установки

Укажите настройки часового пояса для сервера: Asia/Yakutsk и нажимаем Next.

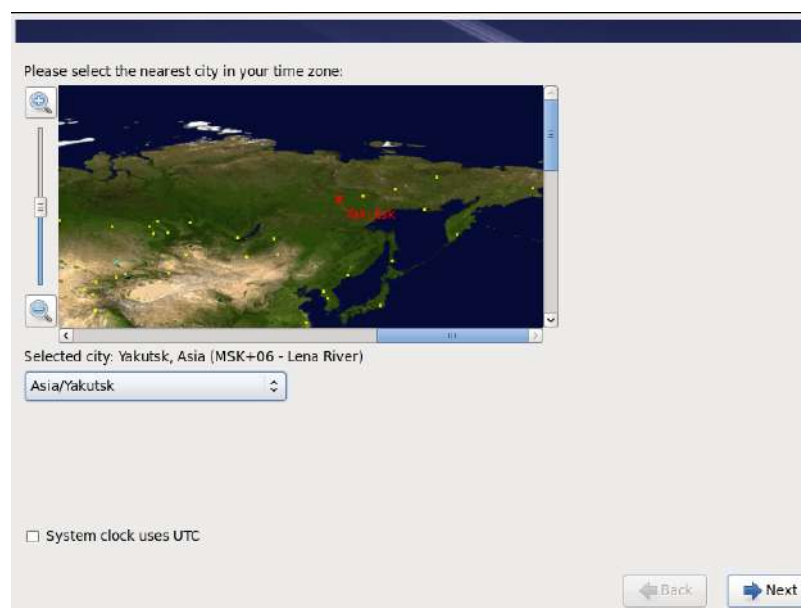


Рисунок 1.17 – Выбор часового пояса

Необходимо установить пароль для суперпользователя системы root. Если введенный пароль не соответствует правилам безопасности, на экране отобразится предупреждающее окно Weak Password. Используйте кнопки:

- Use anyway – если вы хотите использовать введенный пароль без учета рекомендаций;
- Cancel – если вы хотите изменить введенный пароль.

Устанавливаем пароль – ххХХ1234, в окне Weak Password выбираем Use anyway.

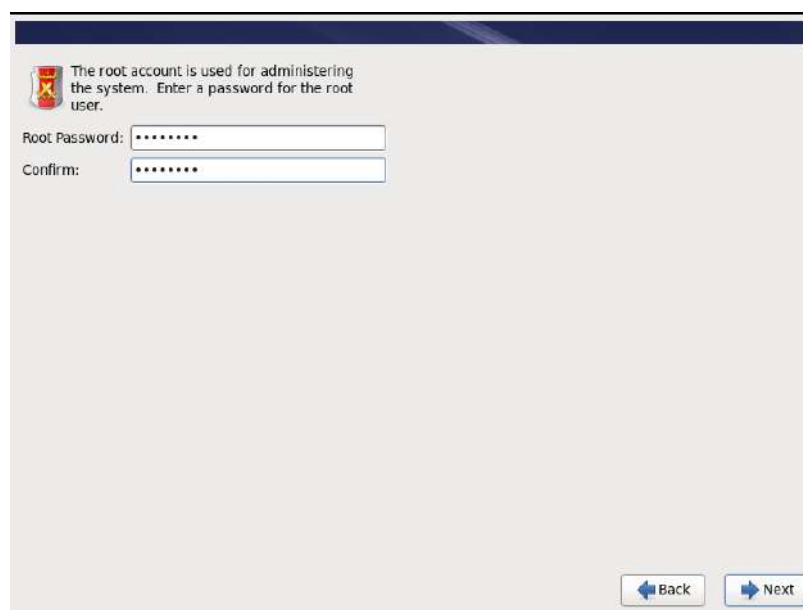


Рисунок 1.18 – Пароль для суперпользователя

Определите способ разбиения дискового пространства, выберите Use All Space и нажмите Next.

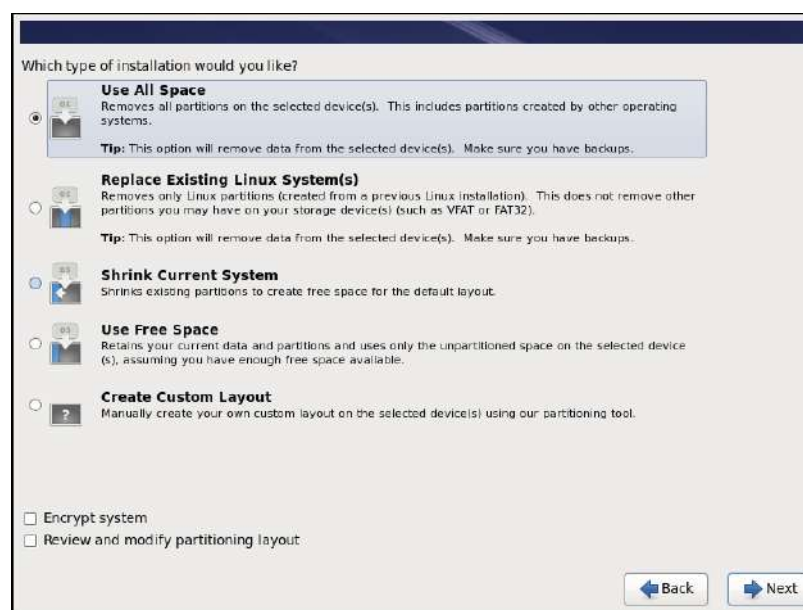


Рисунок 1.19 – Дисковое пространство

Настройка сети. На данном этапе необходимо сконфигурировать сетевое подключение. При настройке Device configuration будет предложено выбрать сетевой интерфейс из имеющихся (eth0 и другие) или создать новый (<New Device>).



Зайдите в конфигурацию интерфейса eth0.

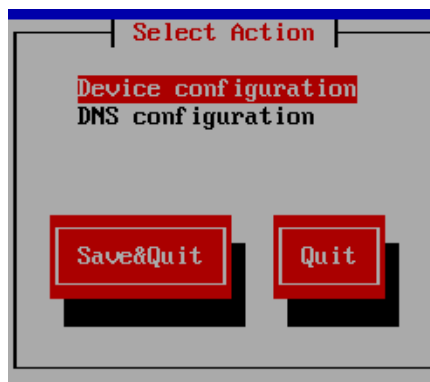


Рисунок 1.20 – Настройка сети

Для использования сетевого интерфейса нужно указать его сетевые настройки (статический IP-адрес машины и прочее). Если Система будет получать данные настройки от DHCP-сервера, нужно включить опцию Use DHCP (с помощью клавиши пробел). Так-как для нашей системы не нужно получать настройки от DHCP-сервера выключаем опцию Use DHCP, и задаем параметры:

- Static IP – 192.168.0.14;
- Netmask – 255.255.255.0;
- Default gateway IP – 192.168.0.253;
- Primary DNS Server – 192.168.0.253.

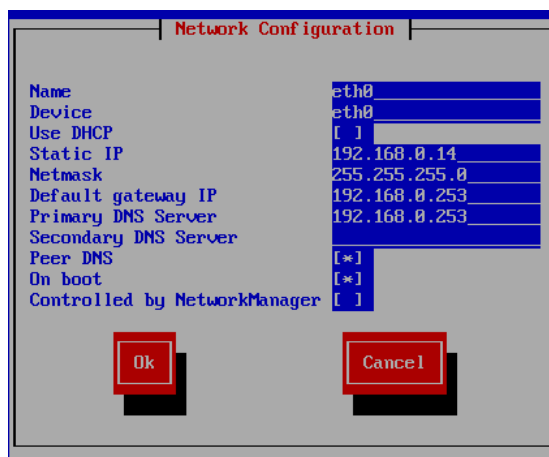


Рисунок 1.21 – Конфигурация сетевого интерфейса eth0

Сохраняем конфигурацию интерфейса с помощью кнопки Save.



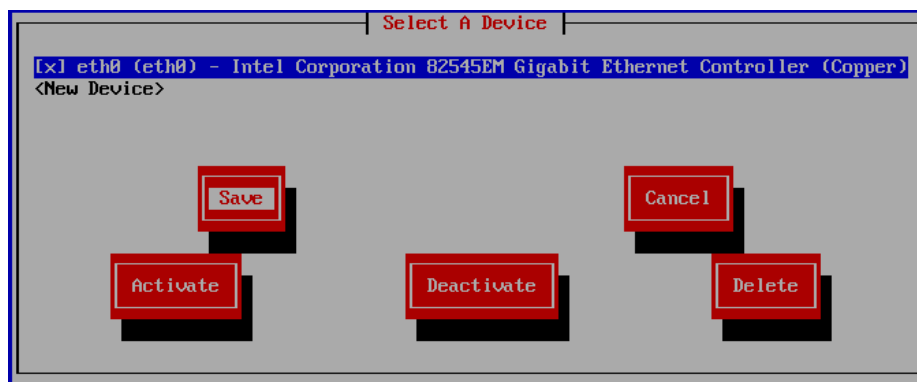


Рисунок 1.22 – Сохранение конфигурации

После настройки сетевой карты переходим к настройке DNS-конфигурации. При настройке DNS configuration нужно будет указать необходимые параметры сервера:

- Hostname – TM;
- Primary DNS – 127.0.0.1.

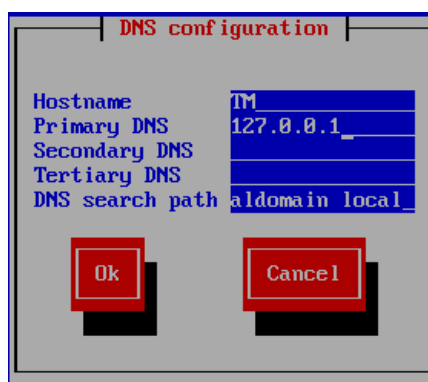


Рисунок 1.23 – DNS конфигурация

Система обработает введенные данные и попросит подтверждения настроек. На данном этапе необходимо проверить указанные сетевые настройки. Если настройки некорректны, введите N и укажите правильные параметры. Если настройки корректны, введите Y для подтверждения и нажмите Enter.

```
Shutting down interface eth0: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: lo: Disabled Privacy Extensions: [ OK ]
Bringing up interface eth0: c1800: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_UP): eth0: link is not ready
BRCM: adding VLAN 0 to HW filter on device eth0
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Determining if ip address 192.168.0.14 is already in use for device eth0...
[ OK ]

/etc/hosts:
127.0.0.1 localhost.localdomain localhost
127.0.0.1 ::1 ::1

DNS configuration (/etc/resolv.conf):
: generated by /sbin/dhclient-script
search localdomain local
nameserver 192.168.0.253

IP configuration (ip addr show):
1: lo:
    inet 127.0.0.1/8 scope host lo
2: eth0:
    inet 192.168.0.14/24 brd 192.168.0.255 scope global eth0

IP ROUTE configuration (ip route show):
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.14
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.0.253 dev eth0
HOSTNAME: TM
Are the network settings correct (y/n)? y
Warning: hostname is composed wrong (does not have a dot or has a digit after a dot)! Product may be installed incorrectly! Proceed only if you are sure on what
you are doing. Continue? (y/n) y
```

Рисунок 1.24 – Подтверждение настроек сети

Имя центра обработки данных оставляем по умолчанию и нажимаем ОК.

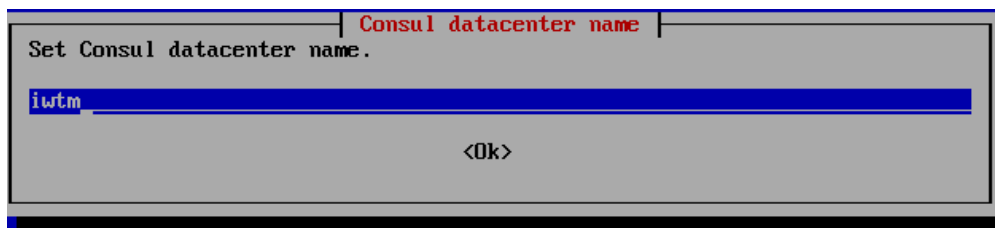


Рисунок 1.25 – Имя центра обработки данных

На данном этапе требуется выбрать одну из следующих опций настройки сервера для синхронизации времени (NTP-server). На Default\_GW - шлюз, используемый компьютером по умолчанию, нажмите пробел, затем ОК.

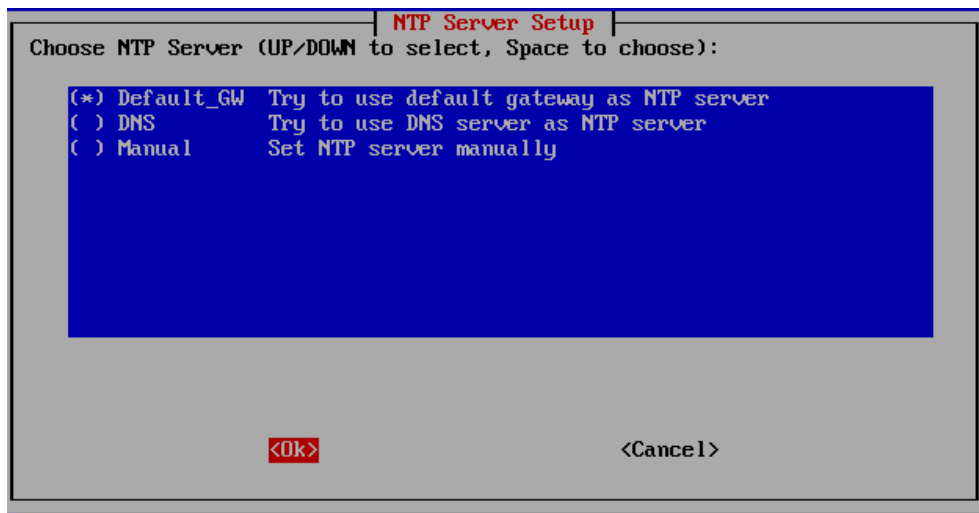


Рисунок 1.26 – Настройка синхронизации

В настройке локализации предлагается выбрать:

**CFDb** - языковые настройки для таких предустановленных сущностей, как категории и термины, списки, предустановленные фильтры и политики по умолчанию.

**Interface** - основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек.

**Search Indexer** - язык, по которому будет проводиться индексация.

Оставьте по умолчанию и нажмите Асепт

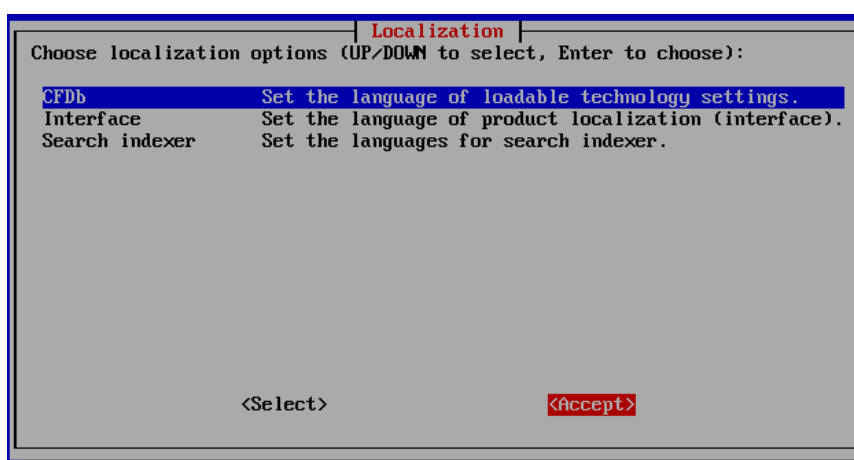


Рисунок 1.27 – Локализация

В открывшемся окне требуется проверить, что выбранные языки для предустановленных сущностей, интерфейса и индексации указаны правильно, затем нажать Yes.

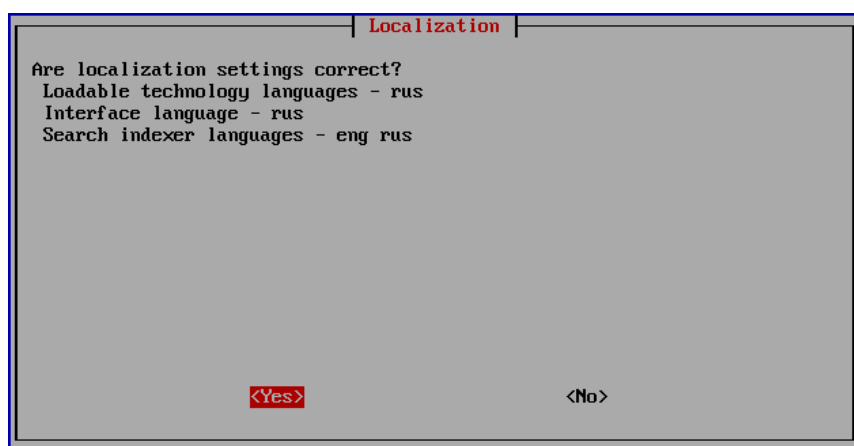


Рисунок 1.27.1 – Подтверждение локализации

В параметрах хранения базы данных так же оставьте по умолчанию и нажмите Save settings.

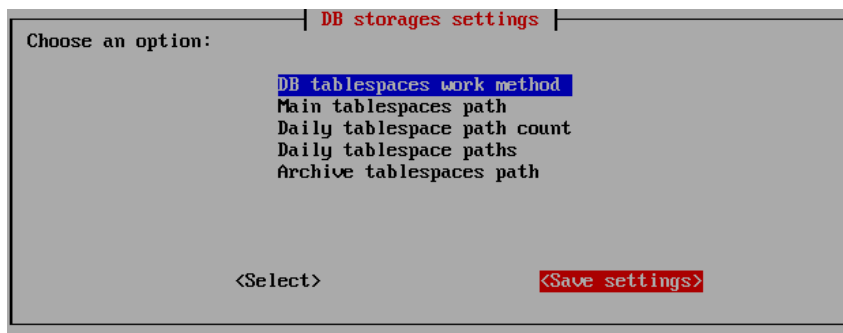


Рисунок 1.28 – Параметры хранения базы данных

В открывшемся окне требуется подтвердить, что параметры указаны верно и нажать Yes.

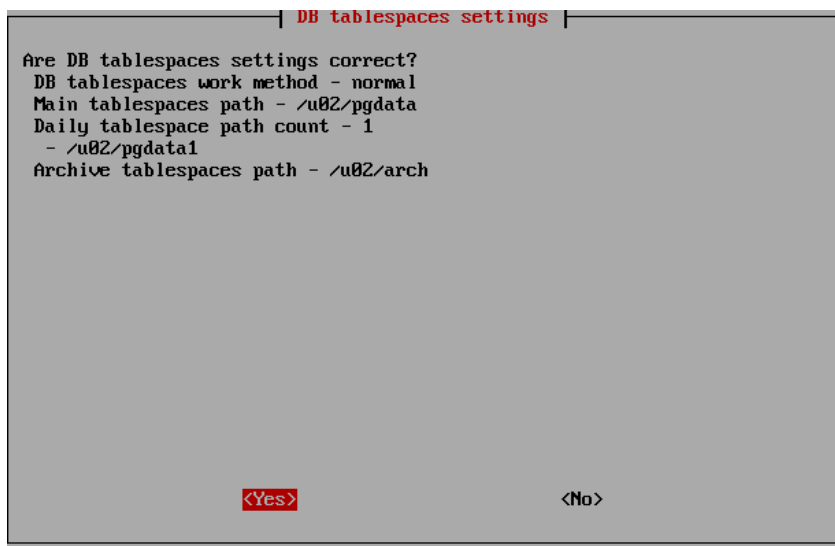


Рисунок 1.28.1 – Подтверждение параметров хранения

Настройки автоматического удаления событий из БД оставьте по умолчанию и нажмите Save settings.

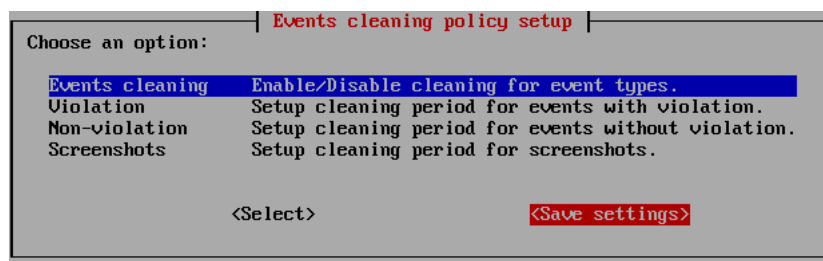


Рисунок 1.29 – Параметры автоматического удаления событий из БД

После всех действий начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

#### 1.4. Установка «Нарушителей»

Установите две виртуальные машины Windows 10, затем задайте сетевые настройки в соответствии с рисунками 1.30 и 1.31.

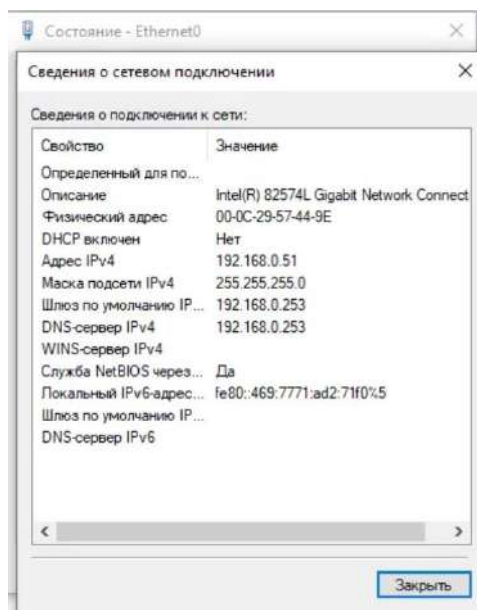


Рисунок 1.30 – Настройки сети Client1-7

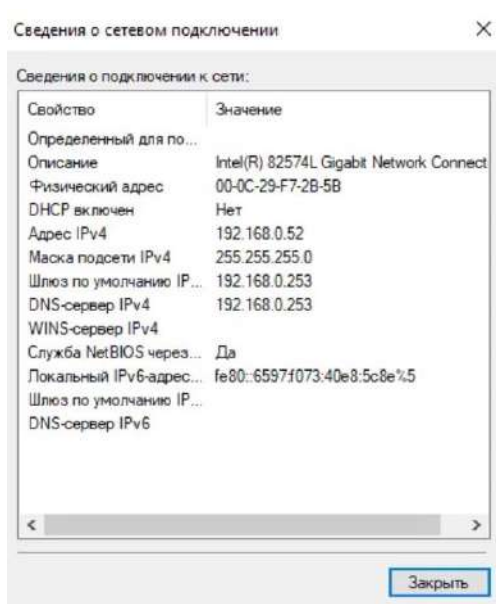


Рисунок 1.31 – Настройка сети Client2-7

После настроек сети, переименуйте и введите виртуальные машины в домен demo.lab.

## 2. УСТАНОВКА И КОНФИГУРИРОВАНИЕ КОМПОНЕНТОВ DLP СИСТЕМЫ

### 2.1. Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

- Логин: user1, пароль: 12345678, запретить локальный вход в систему;
- Логин: user2, пароль: 12345678, запретить локальный вход в систему.

Настройте сложность пароля для пользователей, Group Policy Management (на рабочем столе) - demo.lab - Default Domain Policy (по нему правая мышка кнопки).

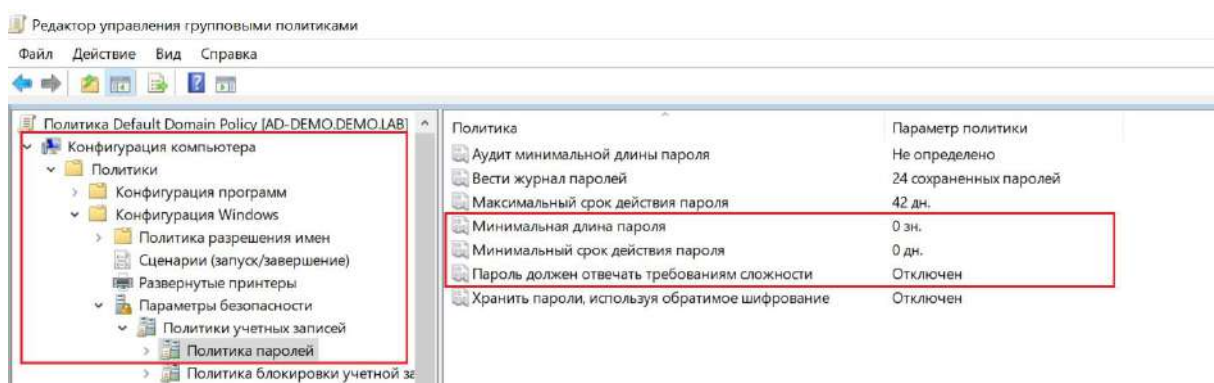



Рисунок 2.1 – Политика паролей

Для добавления новых пользователей зайдите в Active Directory – пользователи и компьютеры:

1. Перейдите в пользователи домена;
2. Создайте нового пользователя User1 (см. рис. 2.2);
3. Задайте пароль для пользователя – 12345678 и установите флажок в «Запретить смену пароля пользователем» (см. рис. 2.3).

Новый объект - Пользователь ✕

 Создать в: demo.lab/Users

---

Имя:  Инициалы:

Фамилия:

Полное имя:

Имя входа пользователя:

@demo.lab ▼


Имя входа пользователя (пред-Windows 2000):

---

< Назад Далее > Отмена

Рисунок 2.2 – Новый пользователь User1

Новый объект - Пользователь ✕

 Создать в: demo.lab/Users

---

Пароль:

Подтверждение:

☐ Требовать смены пароля при следующем входе в систему

☒ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

---

< Назад Далее > Отмена

Рисунок 2.3 – Пароль для нового пользователя

Повторите действия для создания нового пользователя – User2.

Далее, чтобы запретить локальный вход в систему пользователям User1 и User2 зайдите в редактор управления групповыми политиками:

1. В редакторе управления групповыми политиками перейдите в раздел «Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Локальные политики – Назначение прав пользователя»;

2. Найдите политику «Запретить локальный вход», перейдите в свойства политики и добавьте пользователей, на которых хотите применить политику.

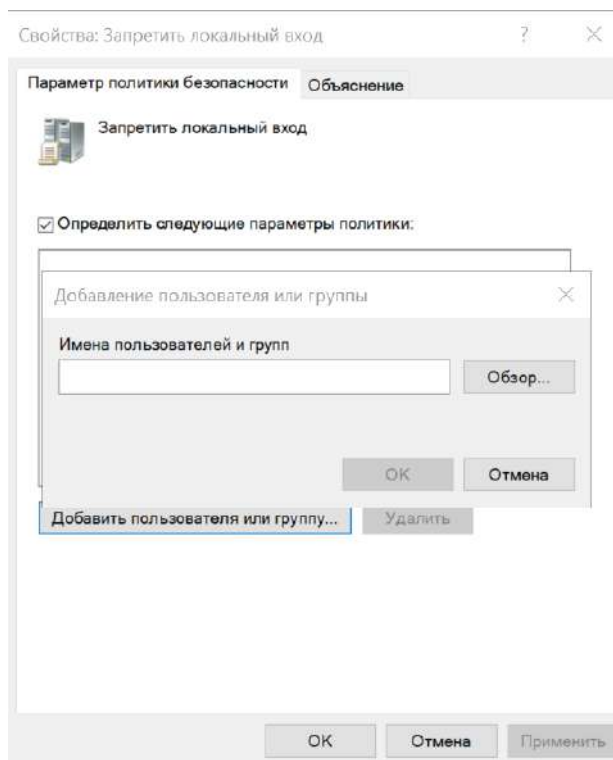


Рисунок 2.4 – Добавления пользователей

После добавления пользователей окно «Свойства: Запретить локальный вход» примет следующий вид:



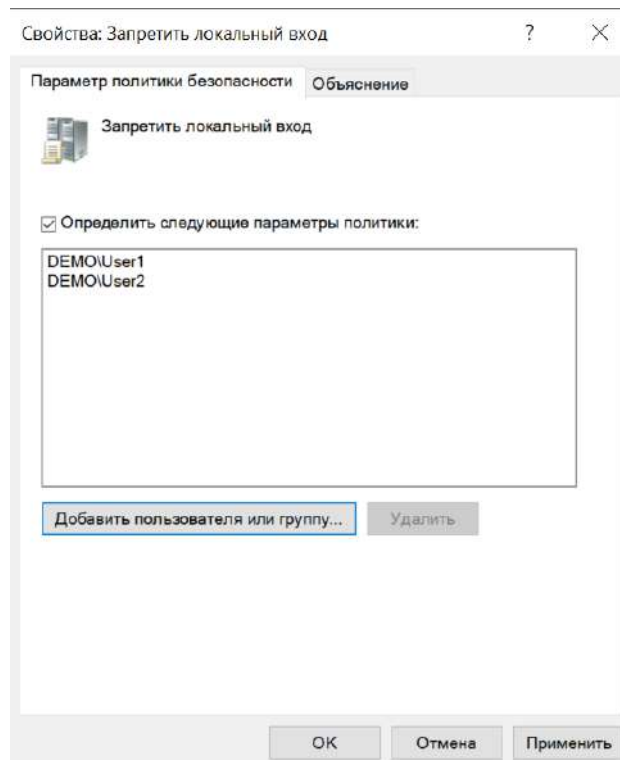


Рисунок 2.5 – Запрет на локальный вход

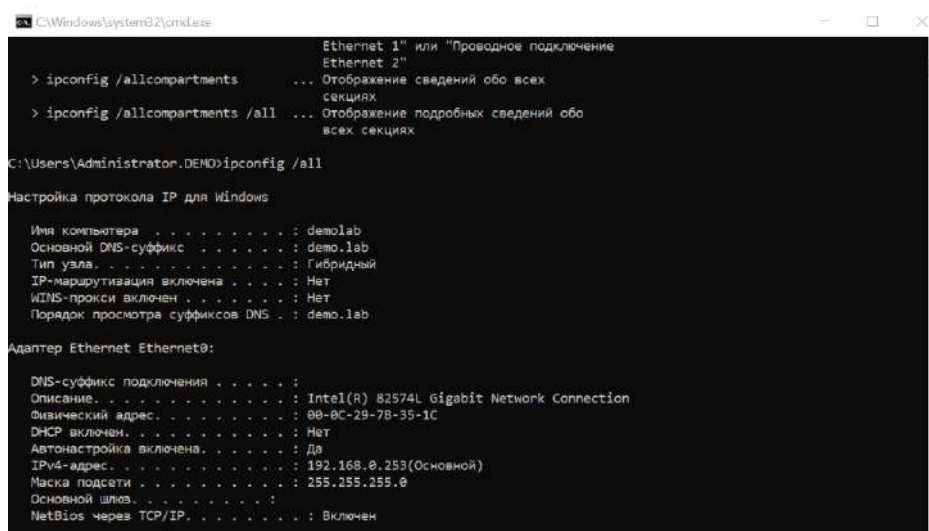
Примените настройки и закройте.

## 2.2. Настройка DLP сервера

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Для этого сочетанием клавиш «Win + R» вызовите диалоговое окно «Выполнить» в сервере и введите – cmd:

В открывшемся окне консоли пропишите команду – ipconfig /all.



```
C:\Windows\system32\cmd.exe
> ipconfig /all
Ethernet 1" или "Проводное подключение
Ethernet 2"
... Отображение сведений обо всех
Секциях
> ipconfig /allcompartments /all ... Отображение подробных сведений обо
всех секциях

C:\Users\Administrator.DEMO>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : demolab
Основной DNS-суффикс . . . . . : demo.lab
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : demo.lab

Адаптер Ethernet Ethernet0:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) 82574L Gigabit Network Connection
Физический адрес. . . . . : 00-0C-29-7B-35-1C
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 192.168.0.253(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
NetBios через TCP/IP. . . . . : Включен
```

Рисунок 2.6 – Локальная консоль

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

Для проверки откройте браузер «Chrome» и в адресной строке введите IP адрес Traffic Monitor – сервера, логин – Administrator, пароль – xxXX1234.

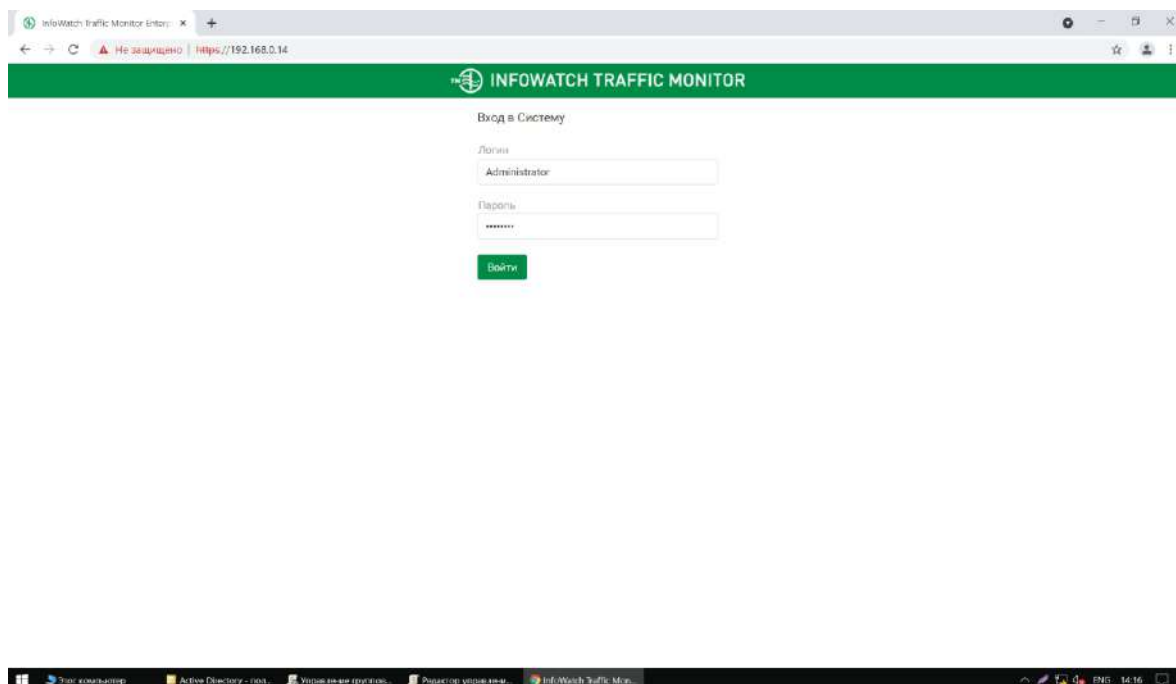


Рисунок 2.7 – Вход в систему

Проверьте лицензию: «Управление - Лицензии».

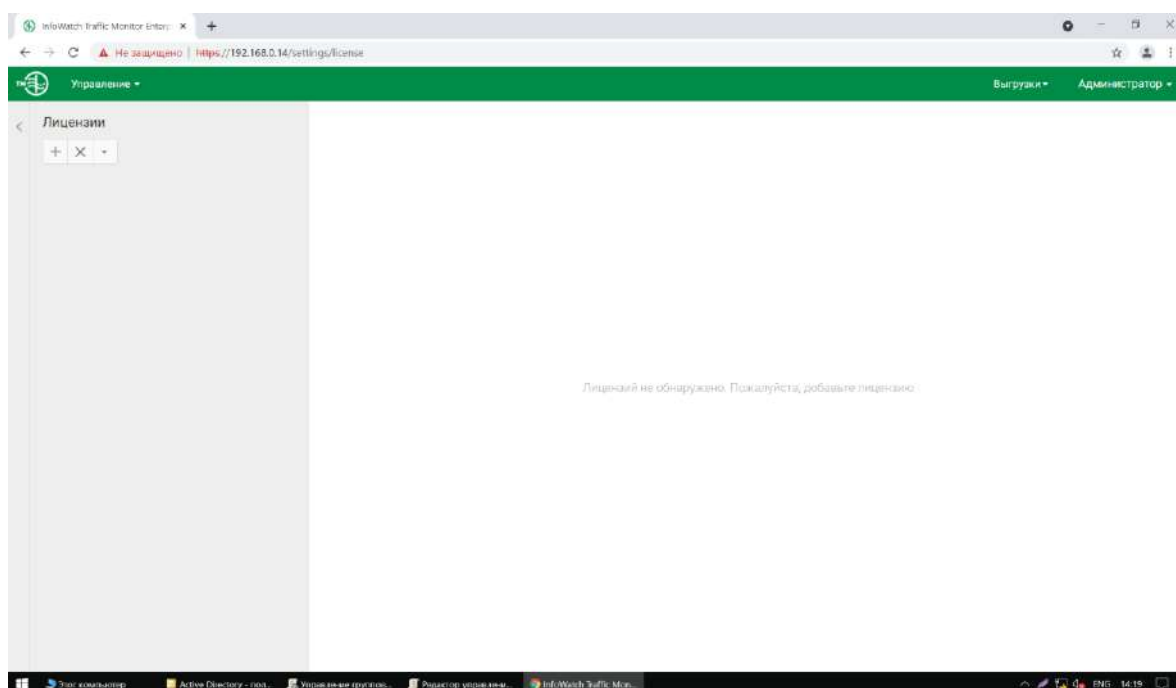


Рисунок 2.8 – Лицензии

Если нет лицензии добавьте вручную, для этого нажмите на «+» и выберите файл с лицензией – [Название лицензии].license.

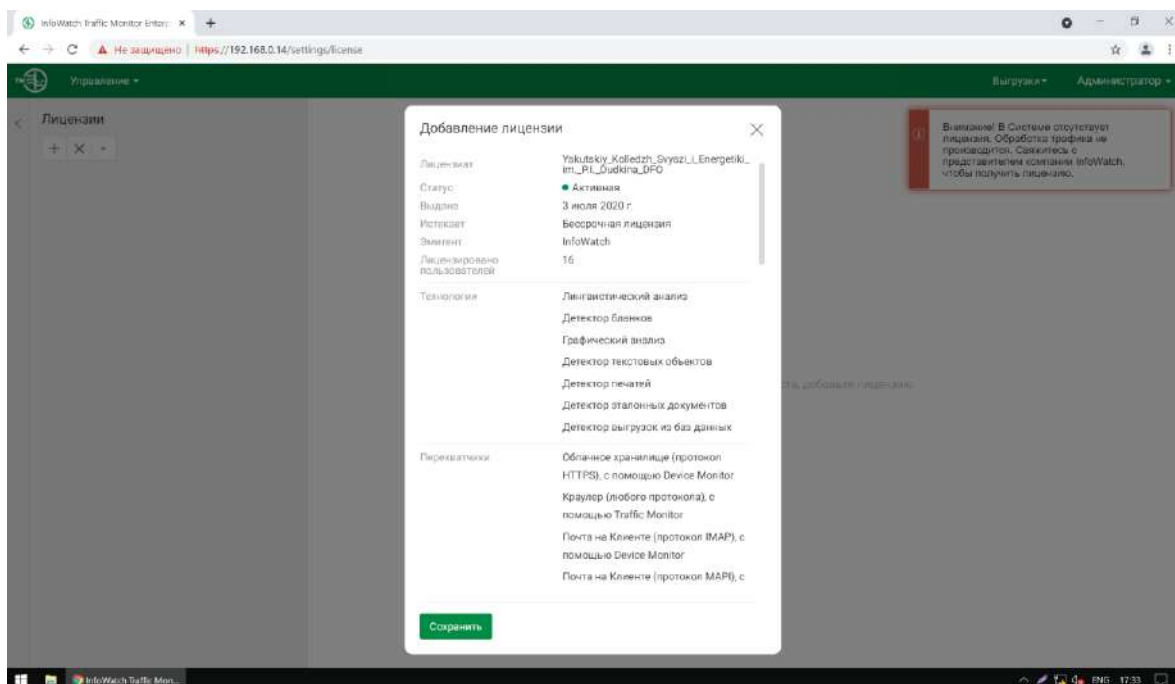


Рисунок 2.9 – Добавление лицензии

После добавления лицензии страница примет следующий вид:

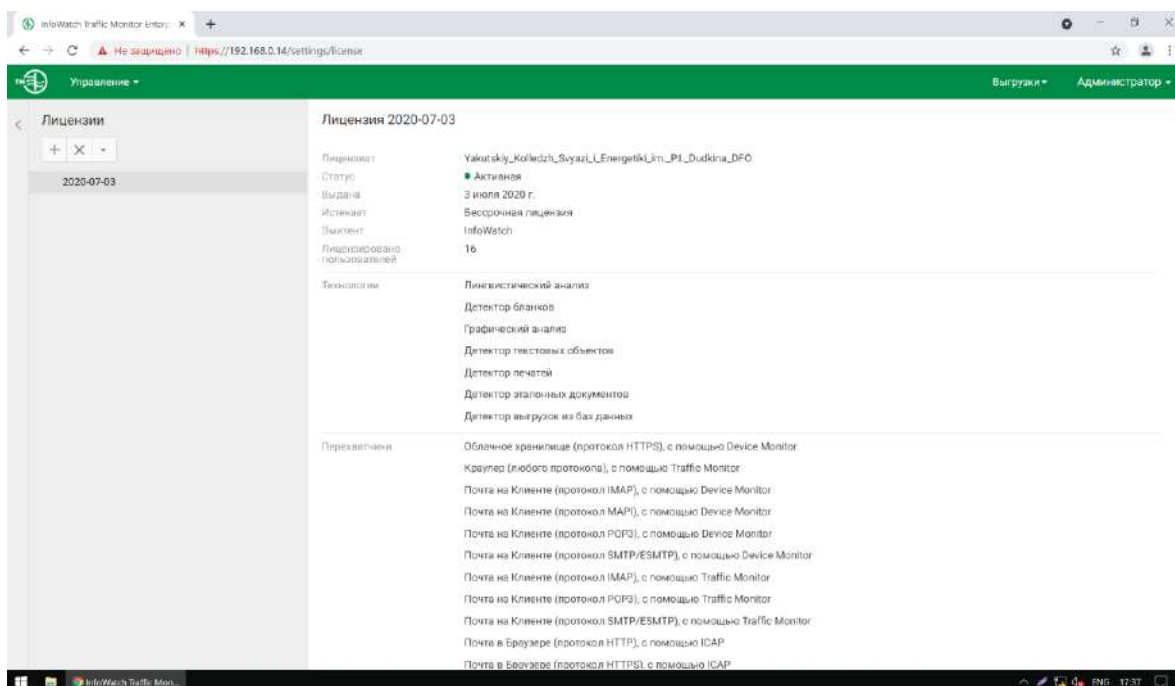


Рисунок 2.10 – Страница с лицензией

Далее необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя:

- Перейдите в «Управление – LDAP синхронизация»;
- Добавьте новый сервер – demo.lab (см. рис. 2.11);

- с. Проверьте соединение (должно появиться уведомление о успешной проверке соединения), после успешной проверки сохраните;
- d. Запустите синхронизацию, после синхронизации статус синхронизации изменится на – «Успешно» (см. рис. 2.12).

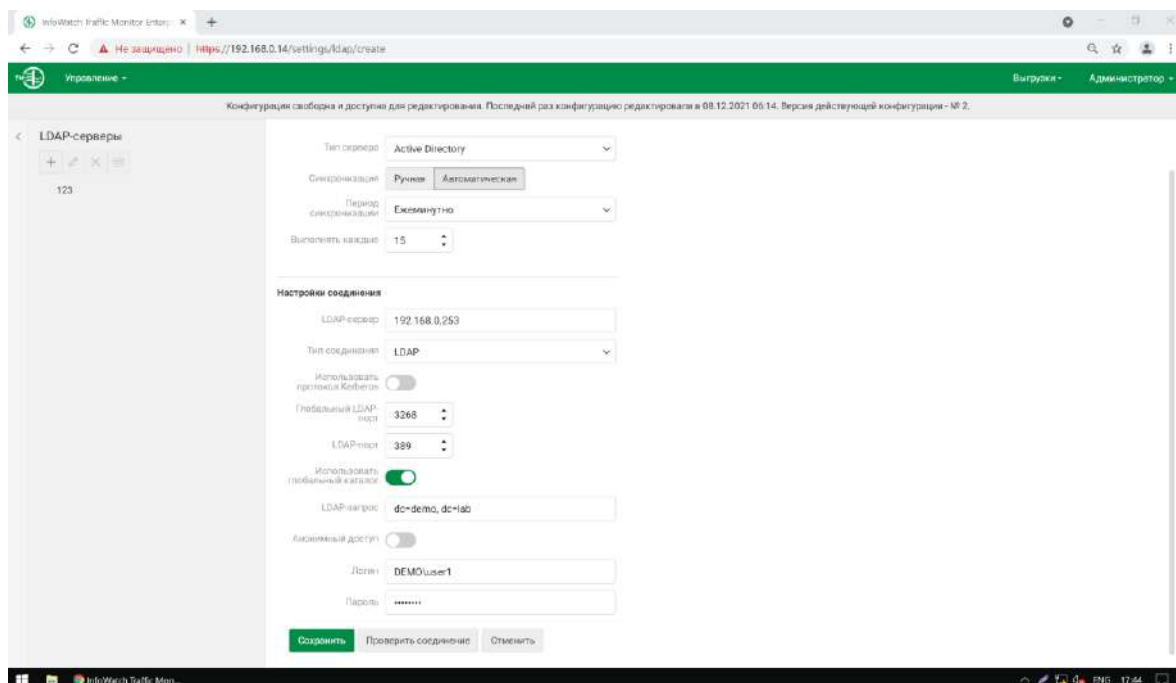


Рисунок 2.11 – Добавление сервера

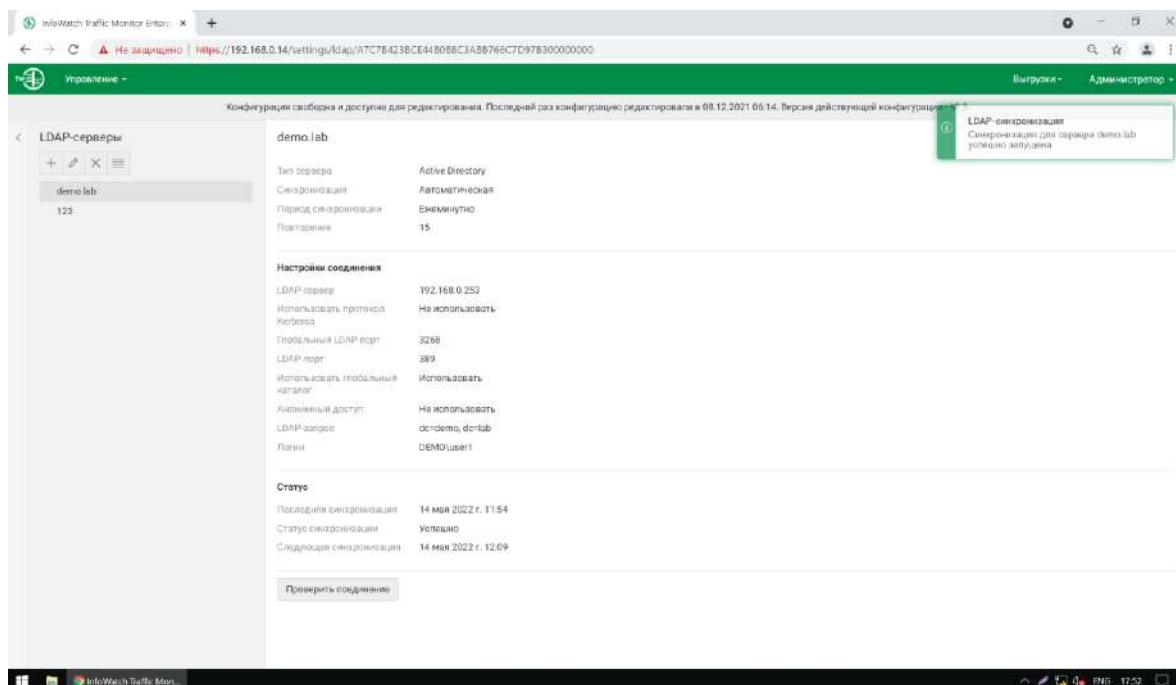


Рисунок 2.12 – Успешная синхронизация

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами на администрирование системы, полный доступ на все области видимости:

- a. Перейдите на страницу «Управление доступом»;
- b. Добавьте пользователя из LDAP системы – user1 (см. рис. 2.13);
- c. Выдайте полные права на администрирование системы и полный доступ на все области видимости (см. рис. 2.14).

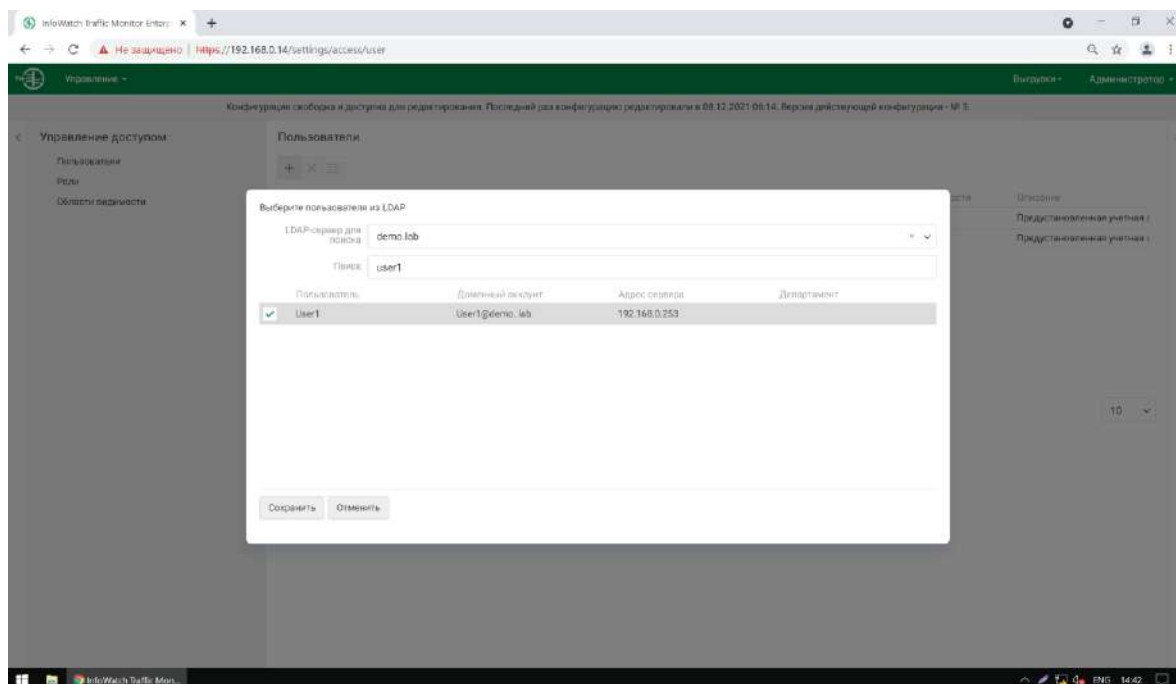


Рисунок 2.13 – Добавление пользователя

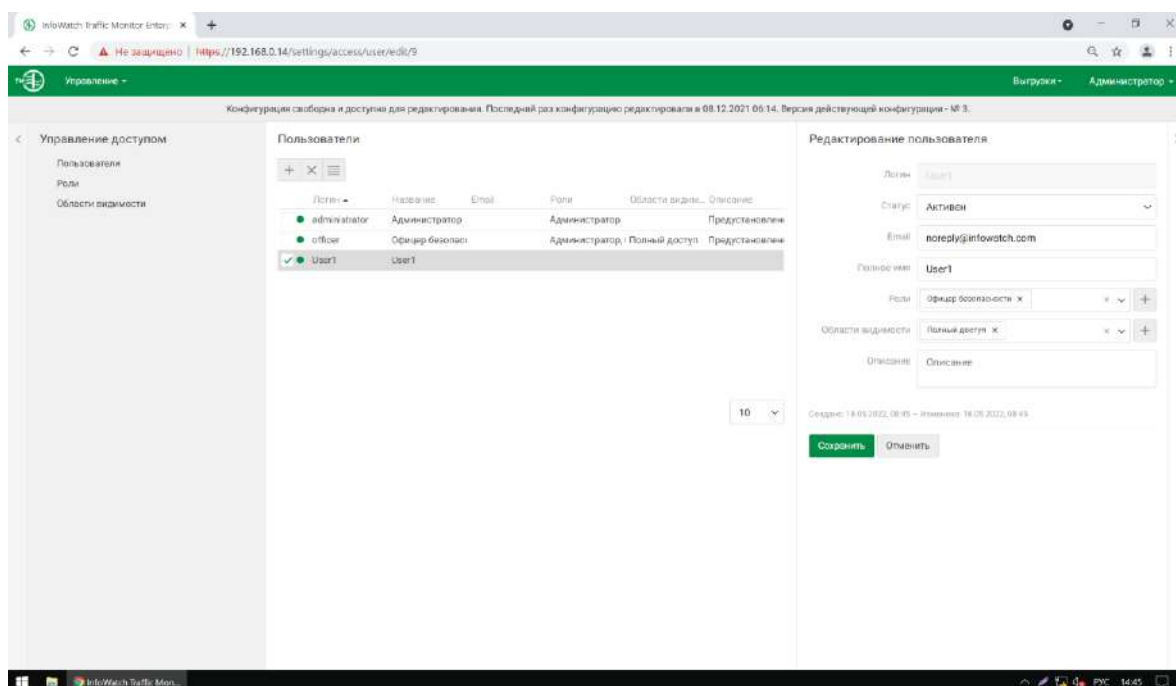


Рис. 2.14 – Роли и область видимости пользователя User1

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWTM:

- a. Создайте файл «отчет.txt» с заголовком IWTM;
- b. Сохраните токен Crawler – «перейдите на страницу плагина – InfoWatch Crawler – Токены» (см. рис. 2.15);
- c. Сохраните токен Device Monitor - «перейдите на страницу плагина – InfoWatch Device Monitor – Токены» (см. рис. 2.16);
- d. Добавьте токены, логины и пароли от учетных записей в ранее созданный файл «отчет.txt». (см. рис. 2.17).

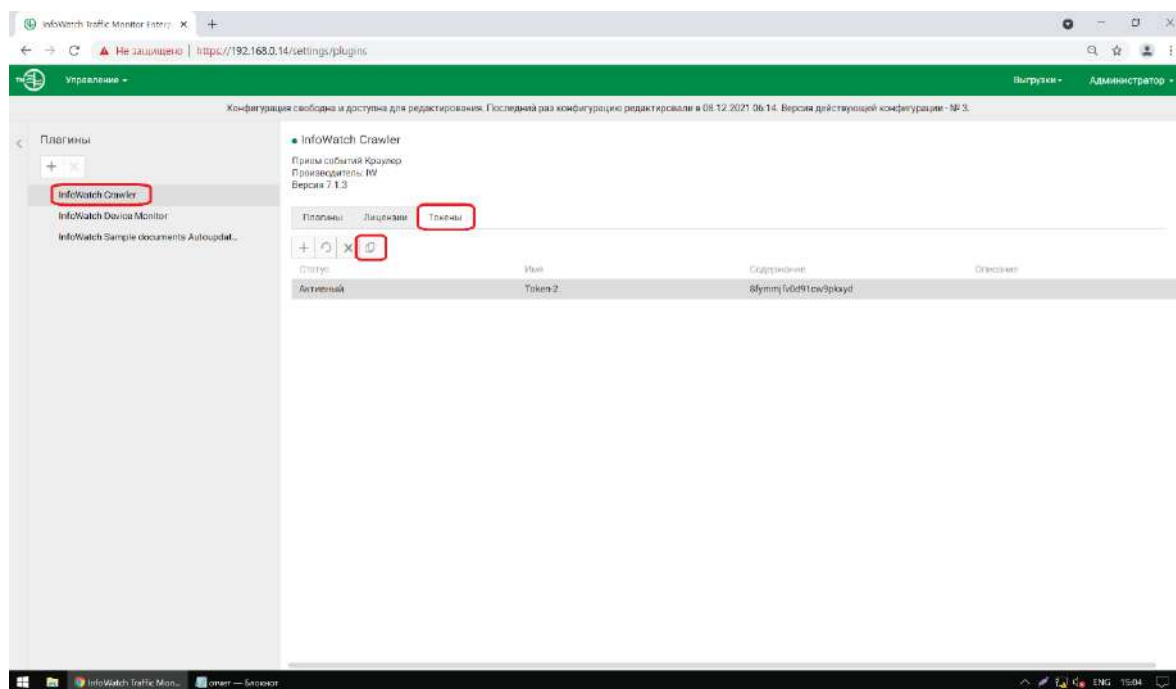


Рисунок 2.15 – Токен Crawler

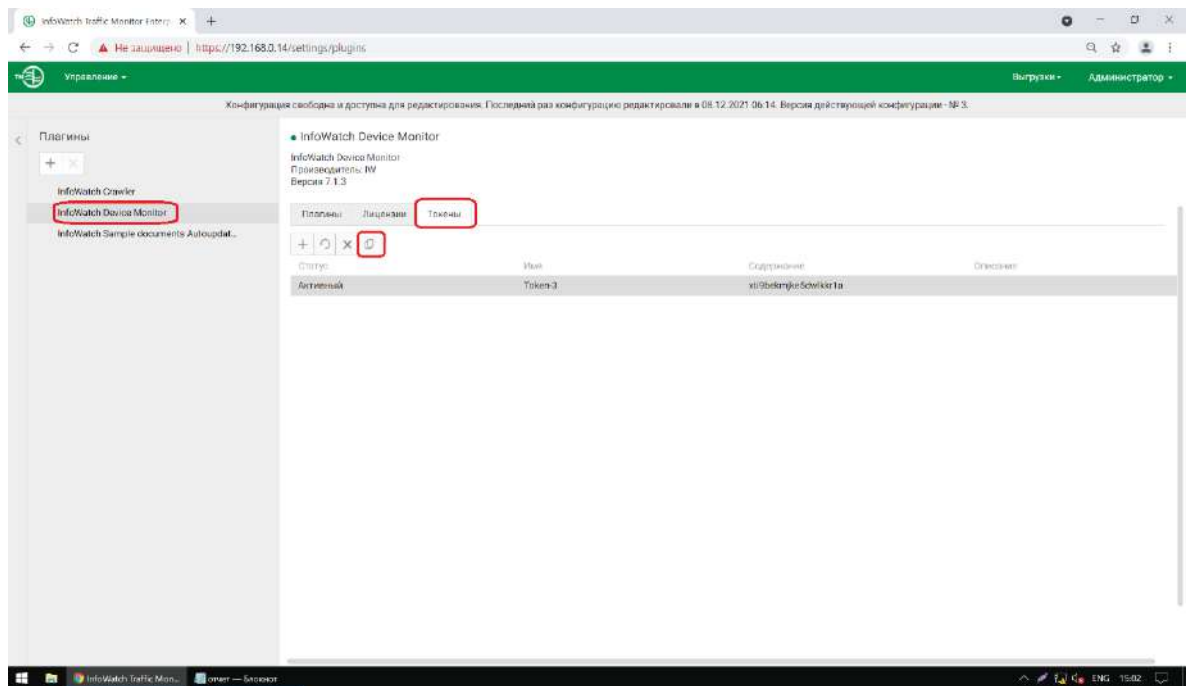


Рисунок 2.16 – Токен Device Monitor

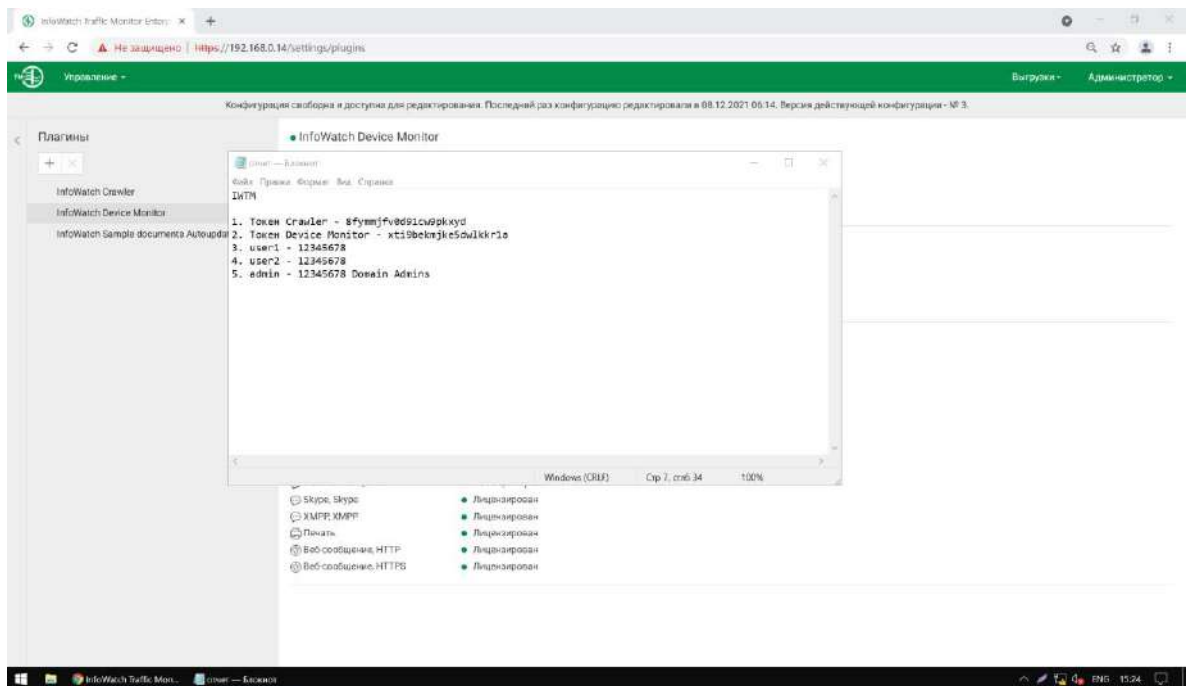


Рисунок 2.17 – отчет.txt



### 2.3. Проверка работоспособности сервера и клиента агентского мониторинга.

Необходимо запустить и войти в консоль управления сервером агентского мониторинга.

Переключитесь в виртуальную машину DM и зайдите под пользователем – admin с паролем 12345678.

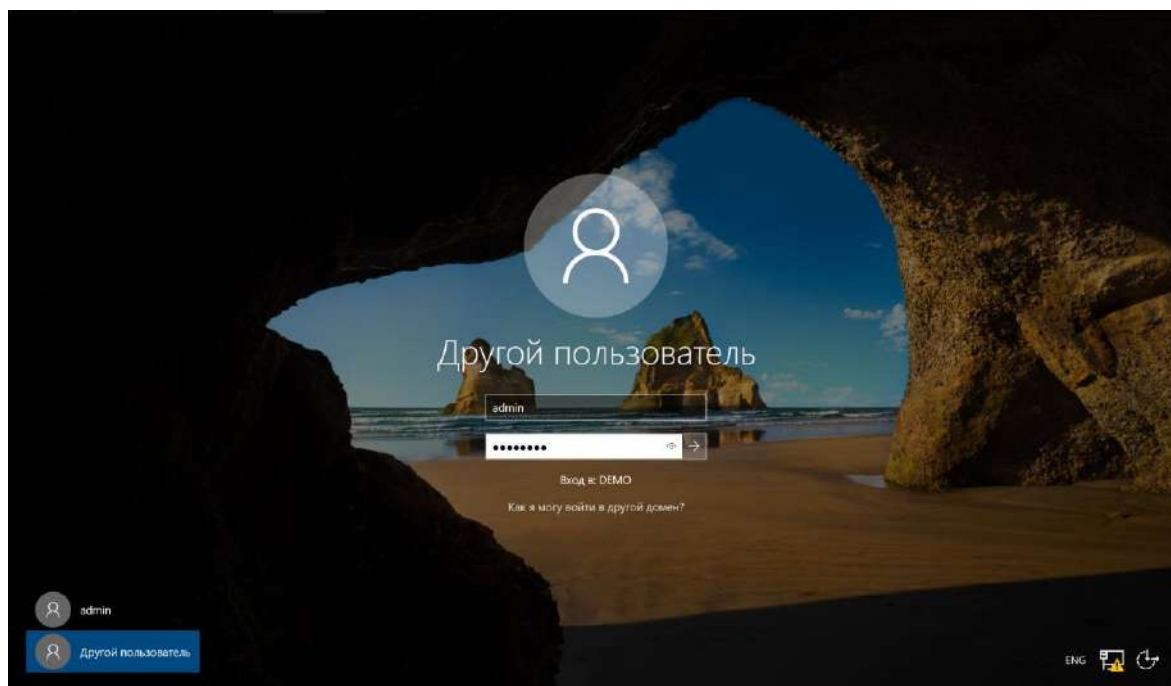


Рисунок 2.18 – Вход в DM-7

Скопируйте установочные пакеты с другого пользователя к себе на рабочий стол

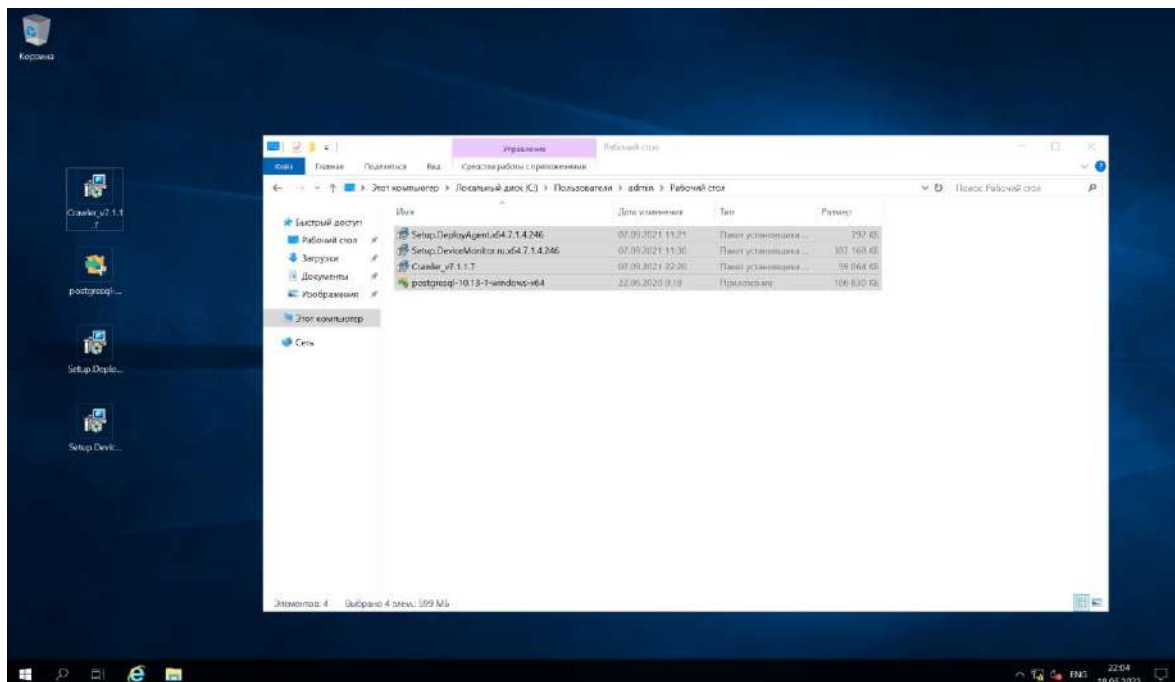


Рисунок 2.19 – Установочные пакеты

Перейдите в AD-demo.lab и дайте доступ в качестве службы для нашего пользователя, для этого переходим в «Пуск – Средства администрирования – локальная политика безопасности – Параметры Безопасности – Локальные политики – Назначение прав пользователя – Вход в качестве службы».

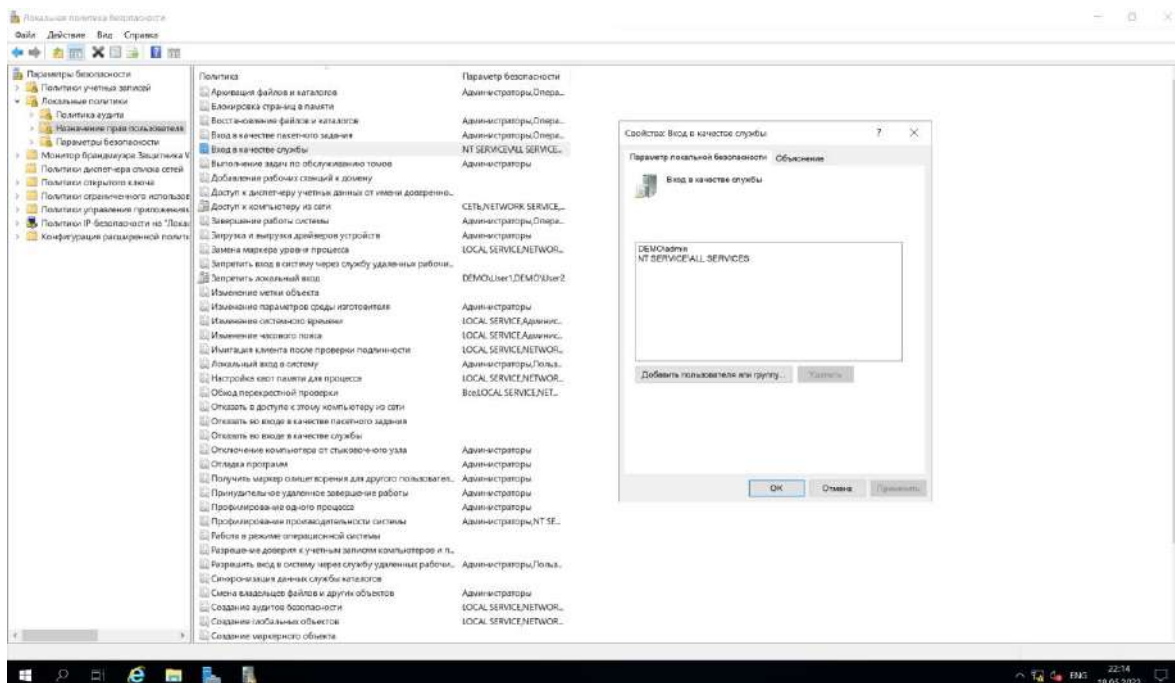


Рисунок 2.20 – Назначение прав пользователя

Установите postgresql, при установке будет создан супер-пользователь postgres, для которого нужно прописать пароль, используем – P@ssw0rd.

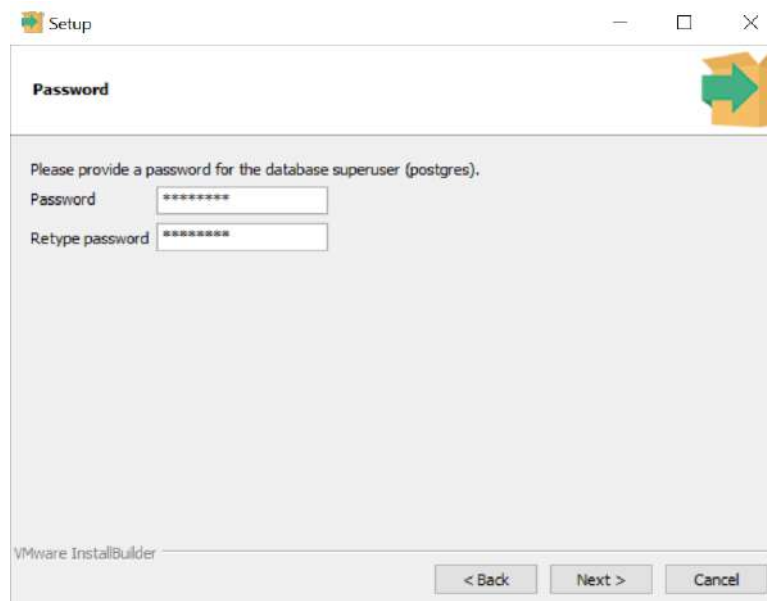


Рисунок 2.21 – Назначение пароля для postgres

Далее необходимо установить Device Monitor:

1. Запустите мастер установки Setup.DeviceMonitor, в результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите "Далее";
2. Примите условия лицензионного соглашения, отметьте поле «Я принимаю условия настоящего лицензионного соглашения» и нажмите "Далее";
3. На шаге Выборочная установка оставьте по умолчанию компоненты. Нажмите "Далее";
4. На шаге "Тип устанавливаемого" сервера выберите "Основной сервер";

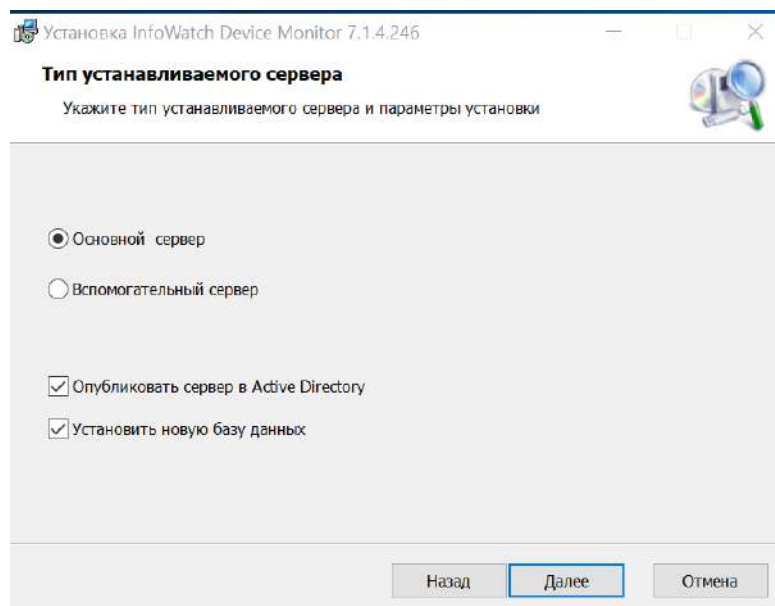


Рисунок 2.22 – Выбор устанавливаемого сервера

5. Укажите СУБД, под управлением которой будет находиться база данных Device Monitor, поставьте флажок напротив "PostgreSQL";

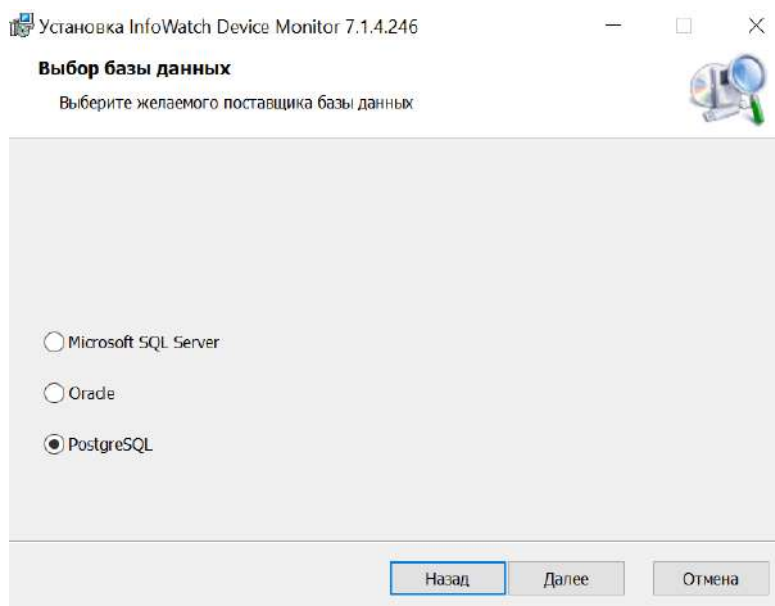


Рисунок 2.23 – Выбор базы данных

6. При использовании PostgreSQL задайте следующие параметры:
  - a. Сервер БД – localhost;
  - b. Имя базы данных – DM;
  - c. Имя пользователя – postgres;
  - d. Пароль – P@ssW0rd.

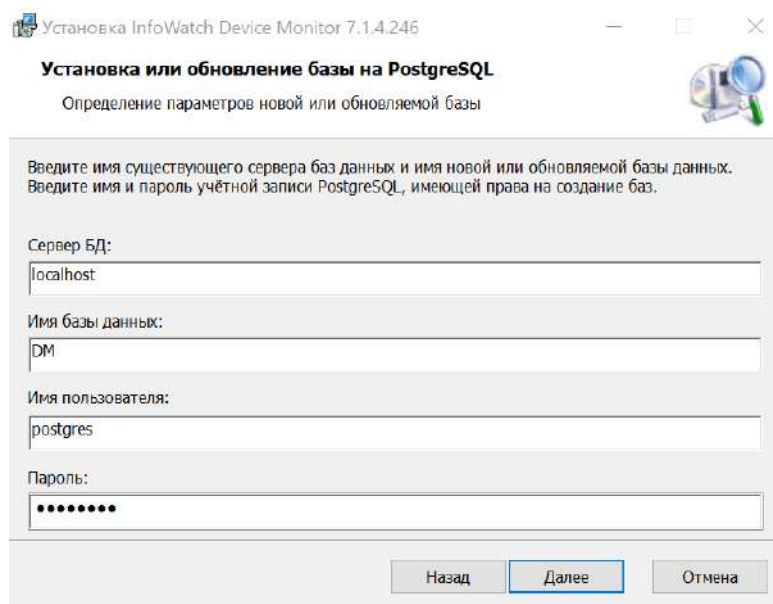


Рисунок 2.24 – Параметры новой базы данных

7. Настройки сетевых параметров сервера оставьте по умолчанию и нажимаем "Далее";

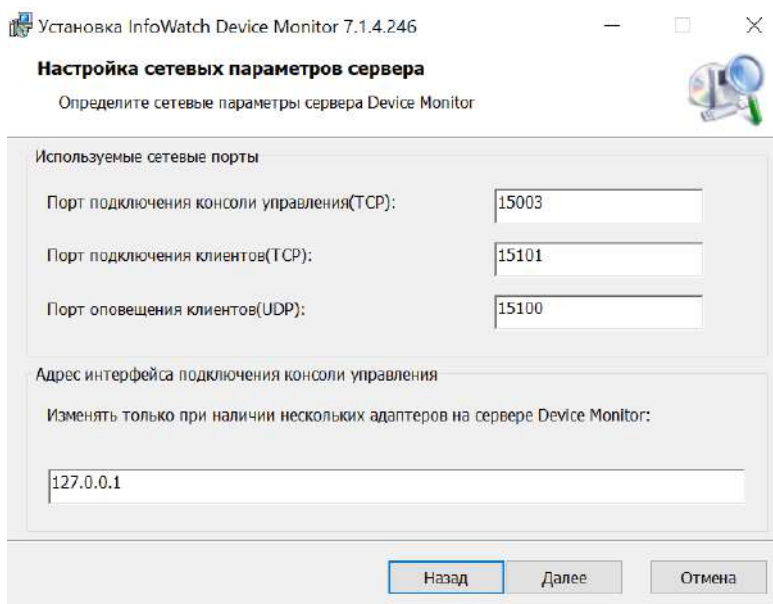


Рисунок 2.25 – Параметры сетевых параметров сервера

8. Порт защищенного канала оставьте по умолчанию. Так как установка выполняется впервые оставьте настройку – "Создать новый ключ";

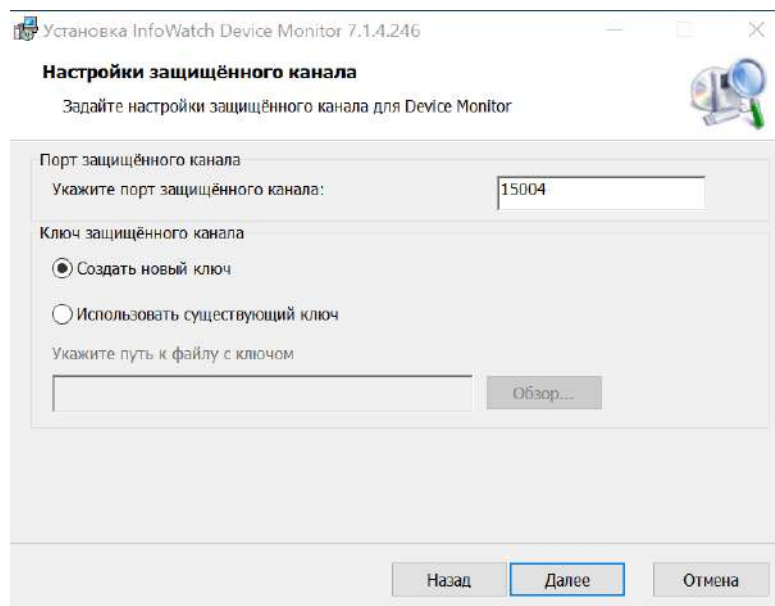


Рисунок 2.26 – Параметры защищенного канала

9. Необходимо выбрать учетную запись, от имени которой будет запускаться служба сервера InfoWatch Device Monitor: Имя пользователя – DEMO\admin, Пароль – 12345678;

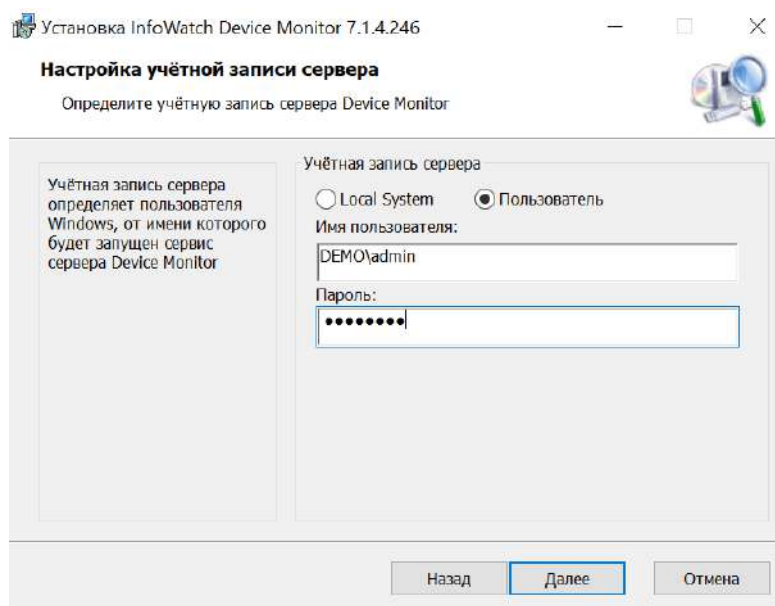


Рисунок 2.27 – Параметры учетной записи

10. Укажите учетную запись Администратора сервера DM – в "Имя пользователя" введите – admin, пароль – 12345678;

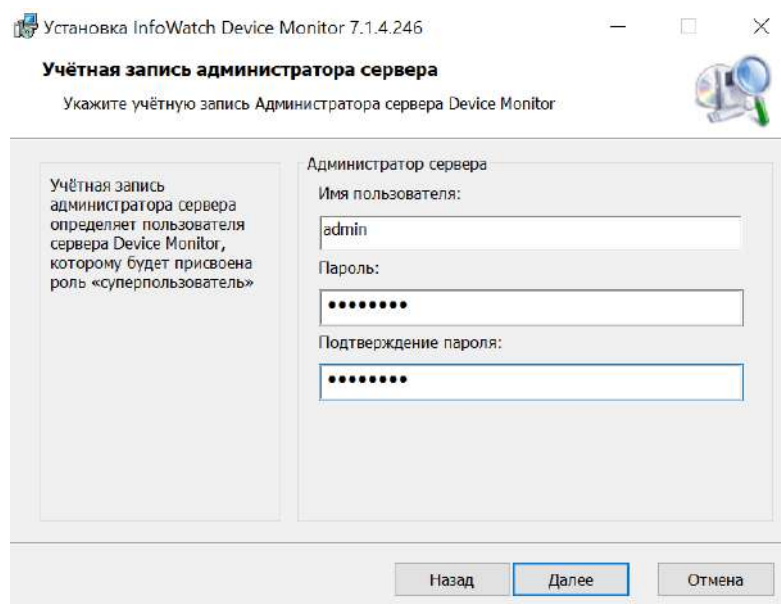


Рисунок 2.28 – Настройка учетной записи администратора сервера

11. Задайте параметры соединения с Traffic Monitor, введите "IP адрес ТМ – сервера" – 192.168.0.14, а также токен Device Monitor которую сохраняли в «отчет.txt» токен Device Monitor;

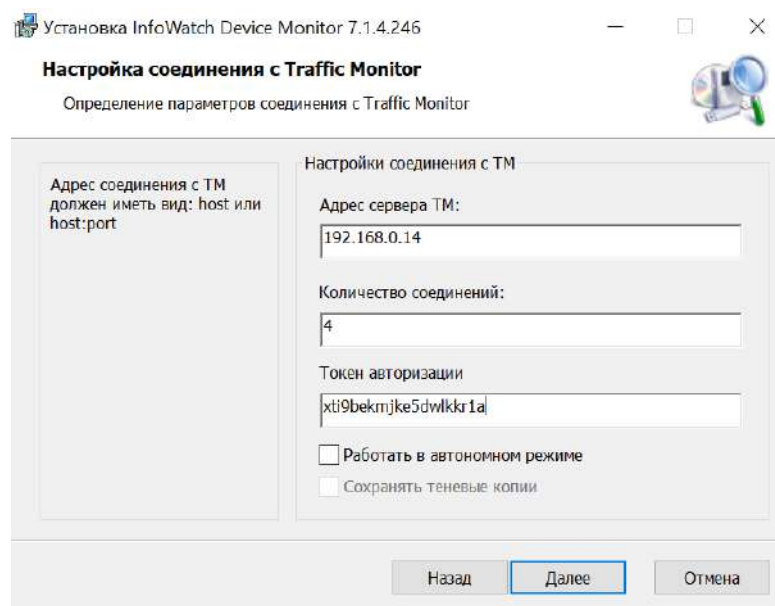


Рисунок 2.30 – Параметры соединения с сервером Traffic Monitor

12. Завершение установки. Нажмите "Установить", чтобы начать установку Сервера, в противном случае произойдет полный откат установки.

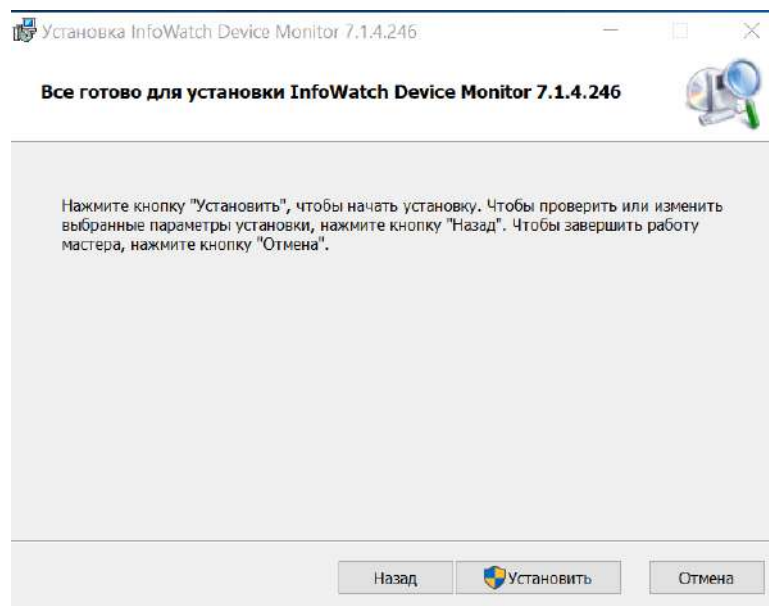


Рисунок 2.31 – Завершение установки

После завершения установки заходим в консоль Device Monitor – Адрес сервера – 192.168.0.222 (IP адрес ДМ сервера), Логин – admin, Пароль – 12345678.

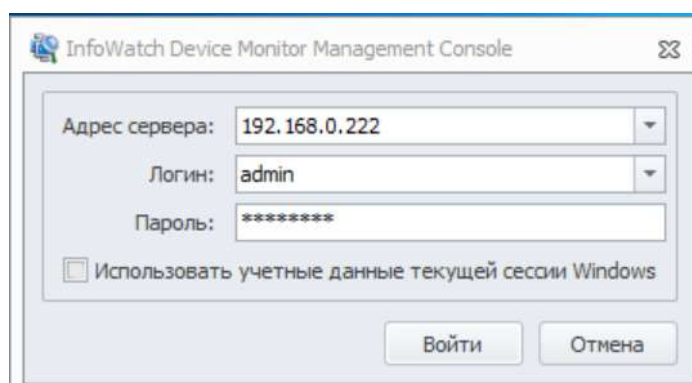


Рисунок 2.32 – Вход в Device Monitor

Настройте синхронизацию с LDAP, для этого зайдите в «Инструменты – Настройки – Интеграция со службами каталогов» в окне «Подключение к службам каталогов» нажмите на кнопку «+» (см. рис. ).



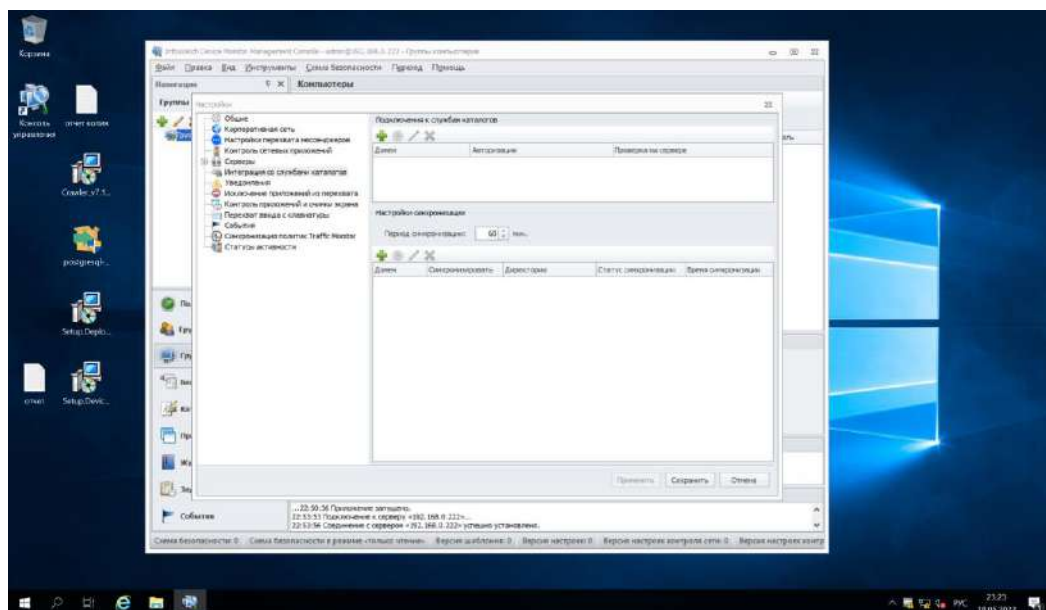


Рисунок 2.33 – Окно интеграции со службами каталогов

Задайте следующие параметры:

- В поле «Адрес» введите – demo.lab;
- Тип выберите – Microsoft Active Directory;
- Параметры авторизации оставьте по умолчанию;
- Проверьте соединение, после успешной проверки появится окно, информирующее о успешной подключении с сервера, нажмите "Ок".

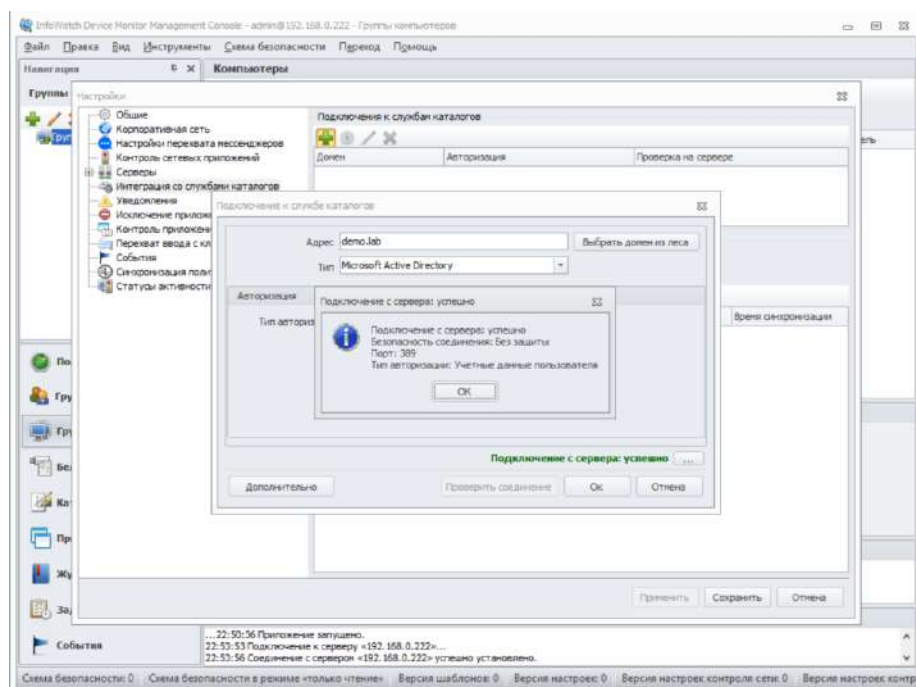


Рисунок 2.34 – Успешное подключение с сервера

Перейдите на AD-demo.lab и вырежьте пользователей с «Users» на «demo»:

- Откройте «Active Directory – пользователи и компьютеры»;
- Перейдите в папку «Users» и выделяем пользователей;
- Вырежьте выделенных пользователей;
- Перейдите в папку «Demo» и вставьте пользователей.

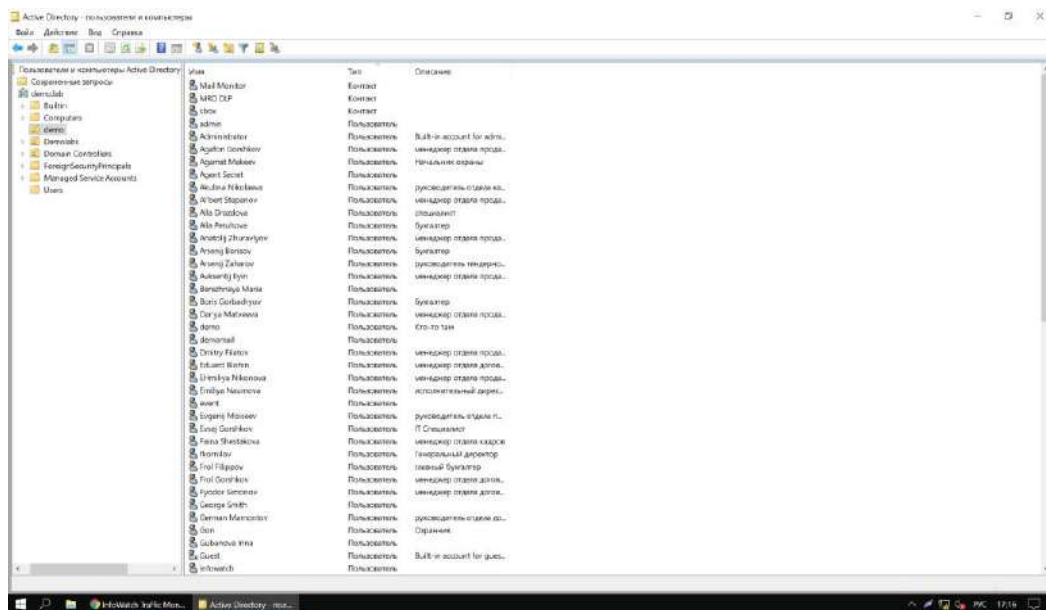
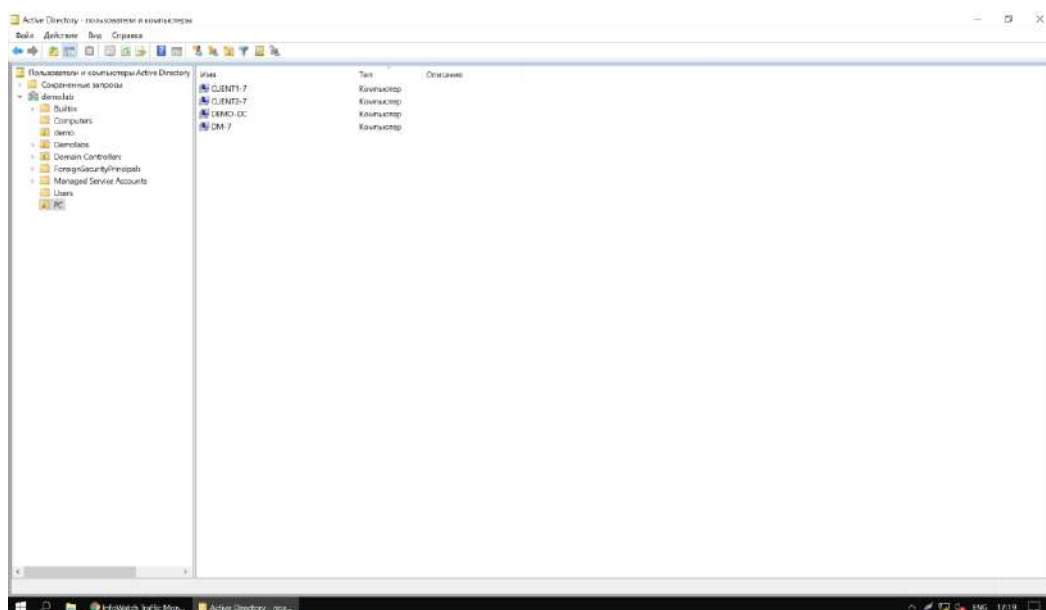


Рисунок 2.35 – Перевод пользователей в подразделение demo

Далее создайте подразделение «PC» и в созданное подразделение вырежьте из папки «Computers» компьютеры, которые подключены к домену demo.lab.



## Рисунок 2.36 – Перевод компьютеров в подразделение PC

Вернитесь к DM-серверу и синхронизируйте каталог пользователей и компьютеров с Active Directory:

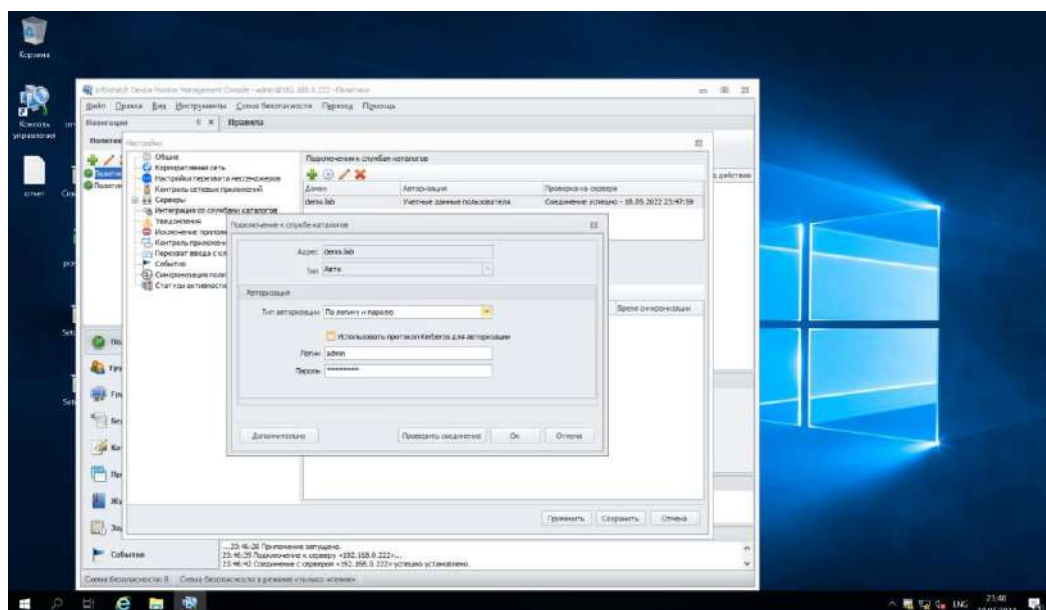


Рисунок 2.37 - Синхронизация

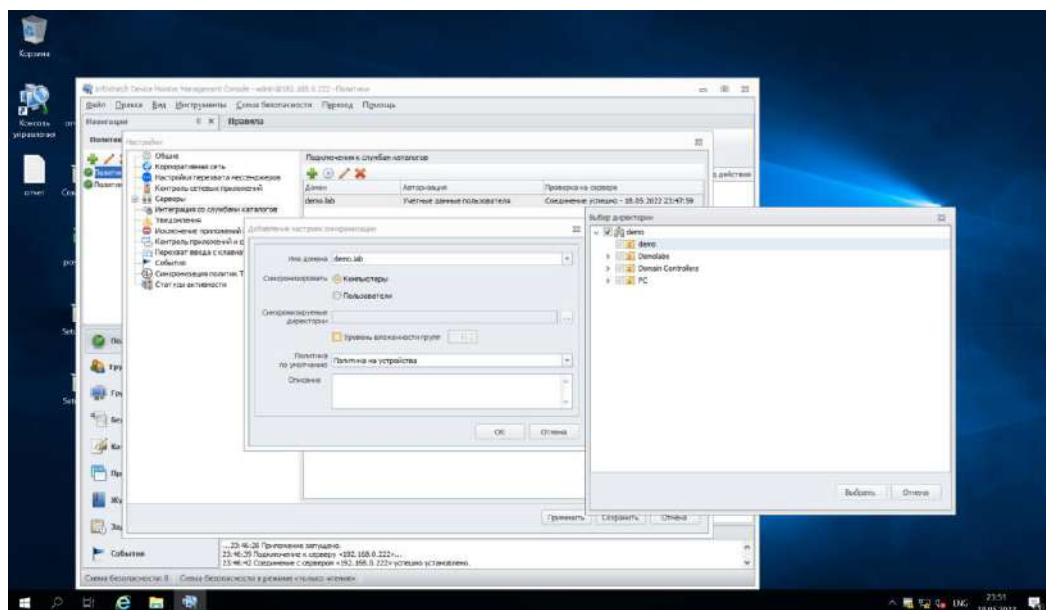


Рисунок 2.38 – Синхронизация компьютеров

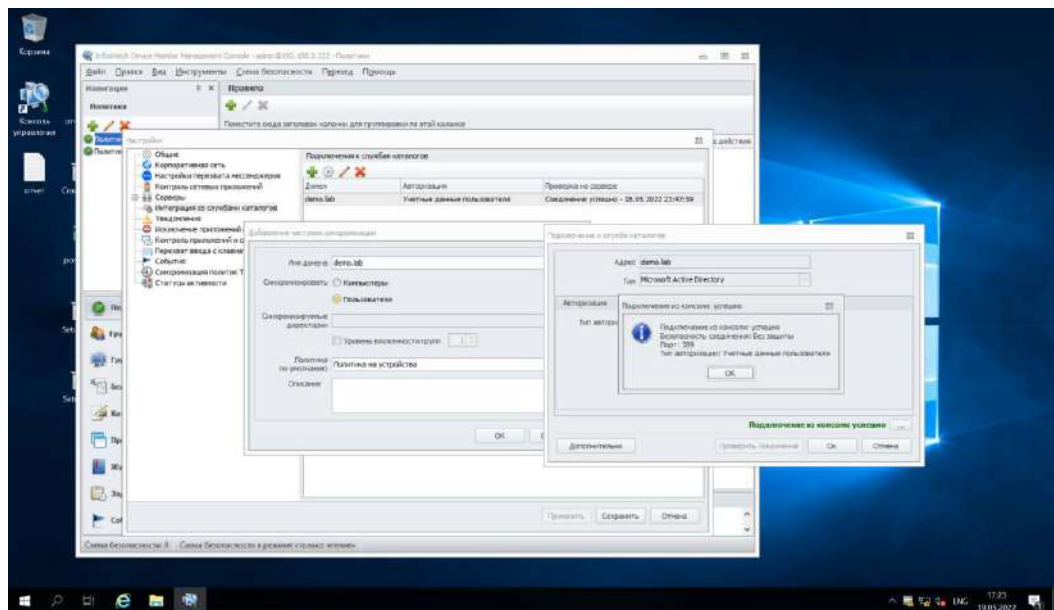


Рисунок 2.39 – Синхронизация пользователей

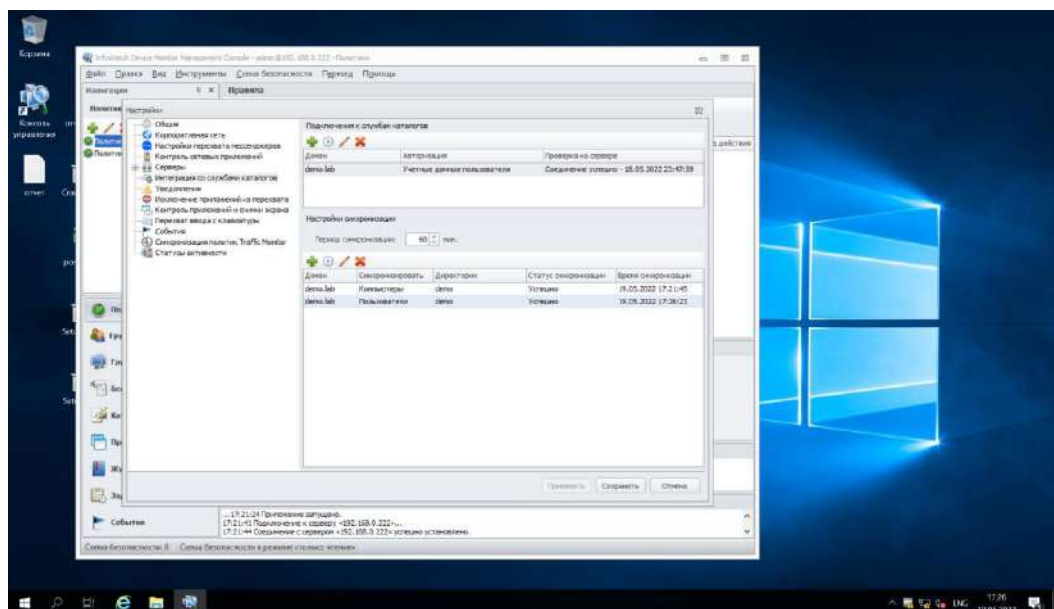


Рисунок 2.40 – Успешная синхронизация

Создайте отчет с заголовком IWDM, в отчете напишите доступ к database postgre и доступ к консоли управления, сохраните и закройте файл.

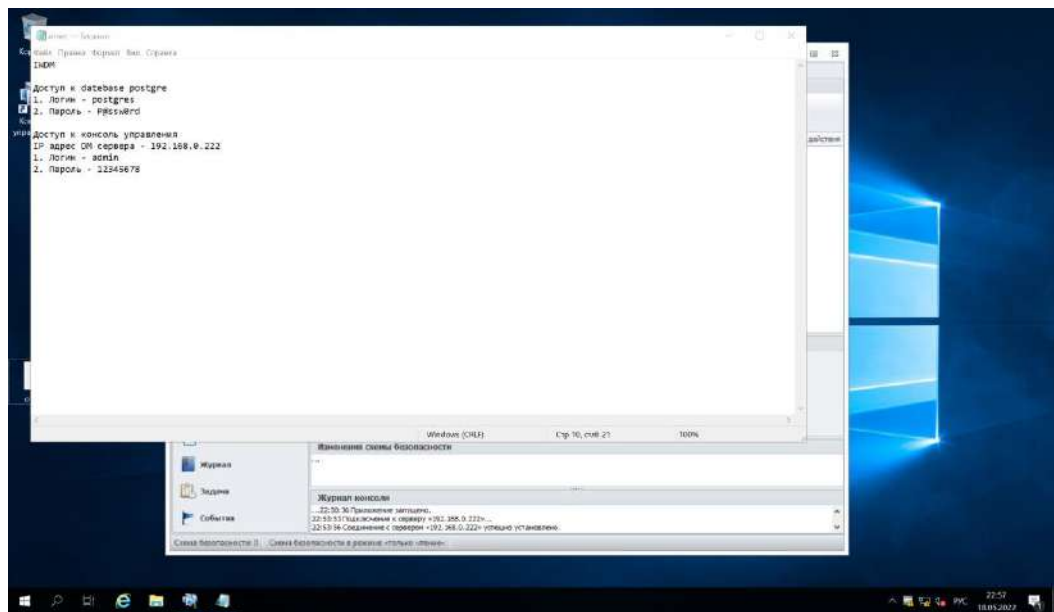


Рисунок 2.41 – Отчет IWDM

## 2.4. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга.

Чтобы установить Crawler:

1. Запустите установочный пакет Crawler\_vx.x.xxx.msi, где x.x.xxx – номер версии;
2. В окне приветствия мастера установки InfoWatch Crawler нажмите "Далее";
3. В окне выбора области установки нажмите "Далее";
4. На шаге "Выборочная установка" выберите какие компоненты Crawler нужно установить и укажите директорию, в которую будет установлен компонент. Выберите "Сервер Краулер" и нажмите "Далее";
5. Укажите параметры соединения службы InfoWatch.Crawler.Server с базой данных Traffic Monitor, нажмите "Далее";
  - a. IP – 192.168.0.14;
  - b. Пароль – ххXX1234.

Установка InfoWatch Crawler 7.1.1.7

**Настройка базы данных**

Задайте параметры подключения к базе данных Traffic Monitor

Тип базы данных

☒ PostgreSQL

IP-адрес или DNS-имя сервера базы данных Traffic Monitor: 192.168.0.14 Порт: 5433

Имя базы данных Traffic Monitor (SID): postgres

Имя пользователя: iwtm\_linux

Пароль: .....

Назад Далее Отмена

Рисунок 2.42 - Параметры соединения с базой данных Traffic Monitor

6. Укажите параметры подключения агента Consul к серверу Traffic Monitor, чтобы узнать "Имя центра обработки данных" и "секретный ключ для

шифрования сетевого трафика Consul", перейдите в трафик монитор и откройте директорию с помощью команды – `cd /opt/iw/tm5/etc/consul`, далее откройте файл – `cat consul.json`. Необходимые для установки данные находятся в блоках:

- a. `datacenter` - Имя центра обработки данных, в котором работает Consul;
- b. `encrypt` - Секретный ключ для шифрования сетевого трафика Consul.

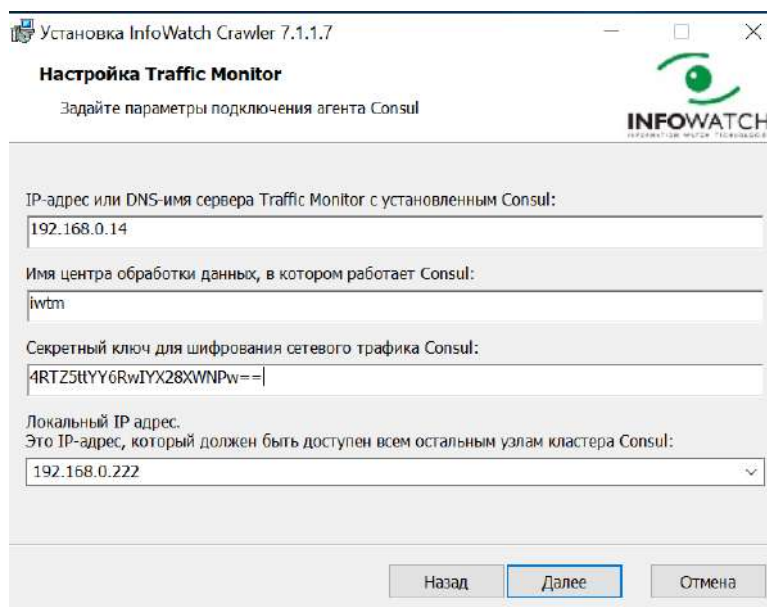


Рисунок 2.43 – Параметры подключения агента Consul

```
1 {
2   "bootstrap_expect": 1,
3   "client_addr": "127.0.0.1",
4   "data_dir": "/opt/iw/tm5/var/consul",
5   "datacenter": "jwrm",
6   "disable_update_check": true,
7   "enable_suslog": true,
8   "encrypt": "4RTZ5tYY6RwIYX28XWNPw==",
9   "leave_on_terminate": false,
10  "log_level": "WARN",
11  "rejoin_after_leave": true,
12  "server": true,
13  "skip_leave_on_interrupt": true
14 }
```

Рисунок 2.44 – Файл Consul



7. Задайте параметры подключения к серверу Traffic Monitor. Токен плагина краулера берем из ранее созданного файла "отчет.txt";

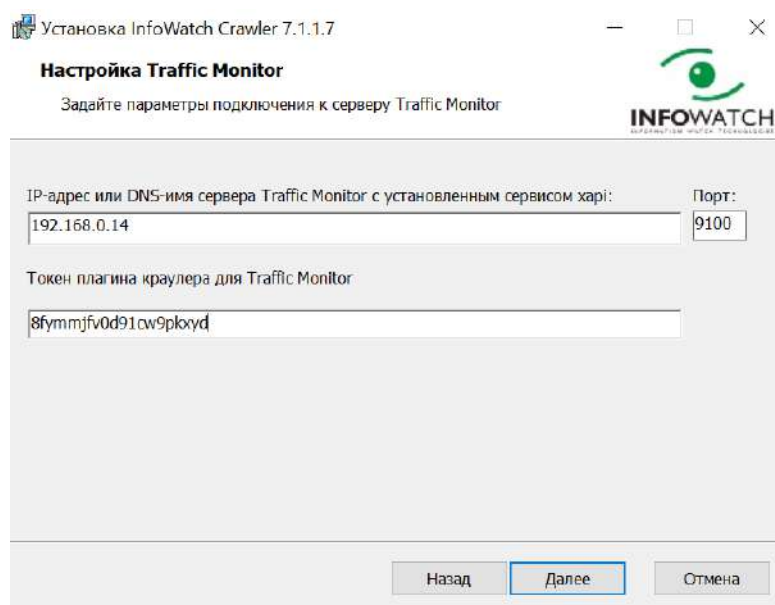


Рисунок 2.45 – Параметры подключения

8. Укажите от имени какой учетной записи будет запускаться служба InfoWatch.Crawler.Scanner. Поставьте флажок запись учетной службы на "Пользователь" и введите доменного пользователя – DEMO\admin с паролем 12345678;

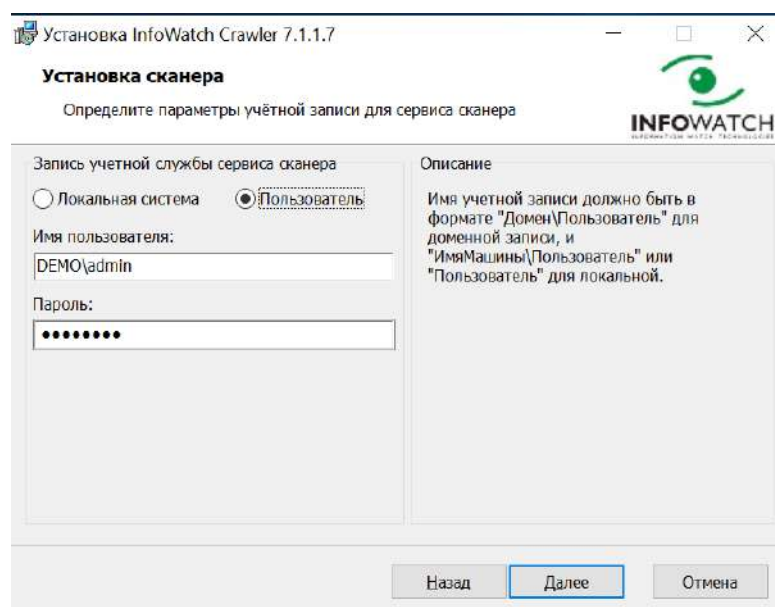


Рисунок 2.46 – Параметры учетной записи для сервиса сканера

9. Параметры сканера оставьте по умолчанию и нажмите "Далее";



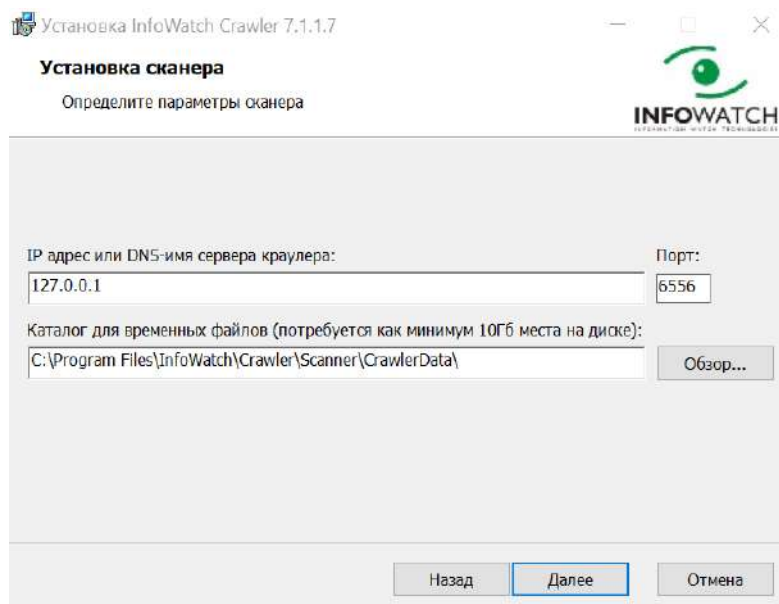


Рисунок 2.47 – Параметры сканера

10. Нажмите "Установить", чтобы начать установку Краулер. По окончании установки нажмите "Готово".

Далее перейдите в AD-demo.lab. Откройте браузер и пропишите IP адрес ТМ в адресной строке. Далее введите: Логин – user1, Пароль – 12345678.

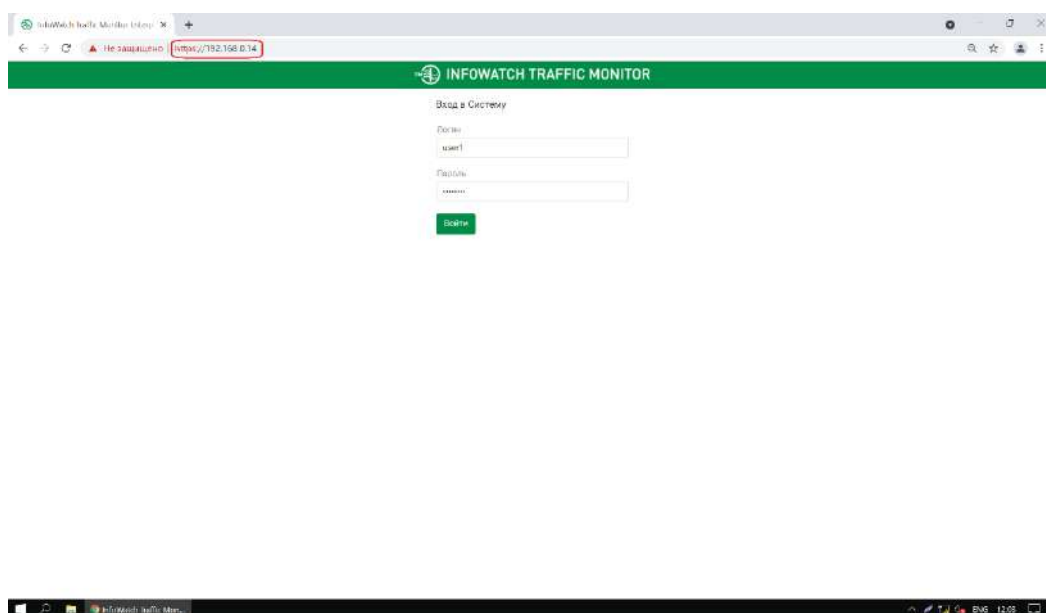


Рисунок 2.48 – Вход в консоль ТМ

Зайдите на страницу "Краулер", чтобы включить динамическое обновление, перейдите в ТМ и введите команду – `vi/opt/iw/tm5/etc/web.conf`, отредактируйте значение параметра «enabled» секции CRAWLER с 0 на 1,

чтобы редактировать нажмите на INSERT, после редактирования выйдите с сохранением, для этого нажмите на ESC, «shift» + «:» и введите – wq.

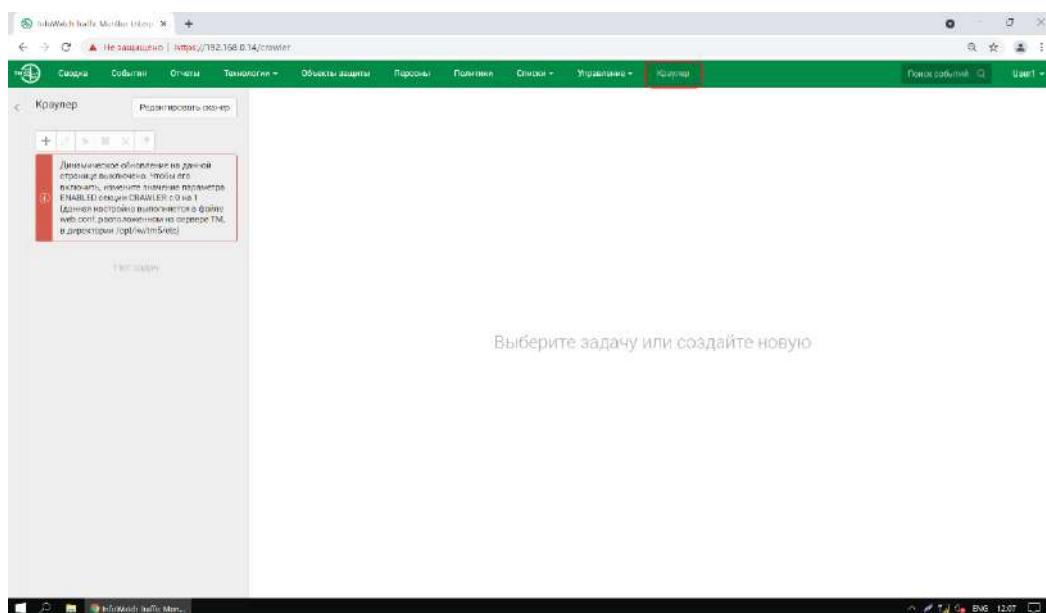


Рисунок 2.49 – Страница "Краулер"



Рисунок 2.50 – Включение динамического обновления

Необходимо создать общий каталог Share в корне диска и установить права доступа на запись и чтение для всех пользователей

Перейдите на виртуальную машину DM и в локальном диске C:\ создайте папку Share, после откройте свойства папки, перейдите в Доступ – Общий доступ, добавьте всех пользователей и выдайте уровень разрешения «Чтение и запись».

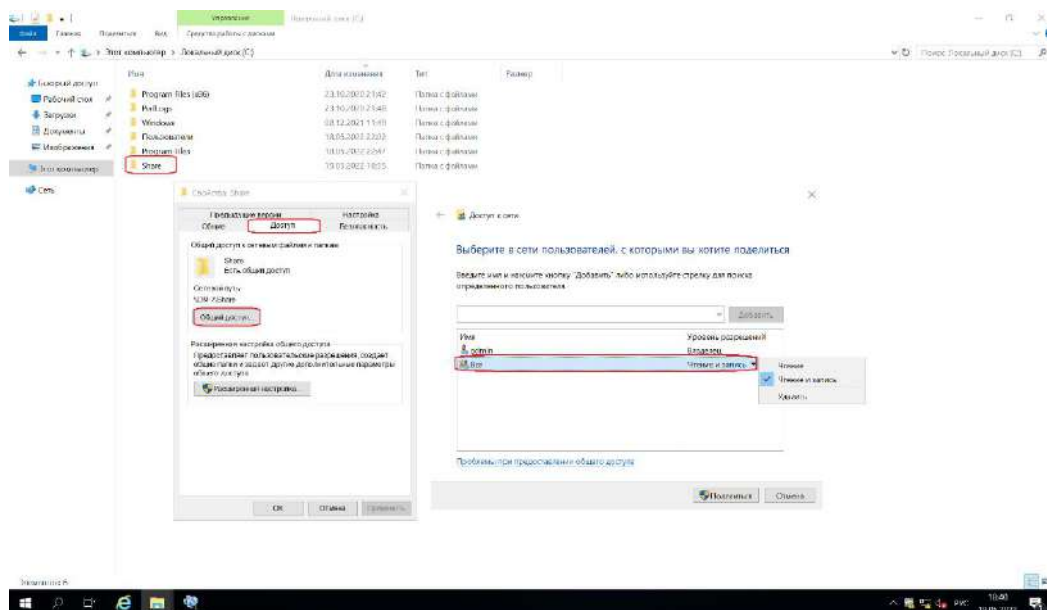


Рисунок 2.51 – Доступ к папке Share

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Перейдите на рабочее место AD-demo.lab, в ранее открытой странице создайте задачу с названием Share, в объекте сканирования выберите компьютер DM-7, чтобы выбрать только папку Share, режим сканирования выставьте – «Только папки», с помощью фильтра выберите папку Share и сохраните, после сохранения откройте отчет.

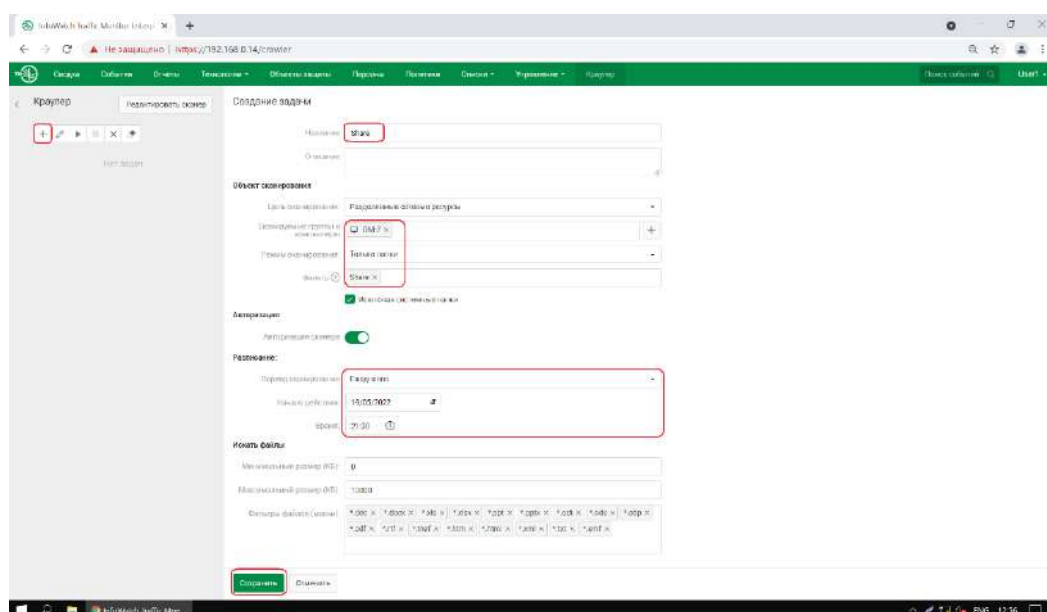


Рисунок 2.52 – Создание задачи Share

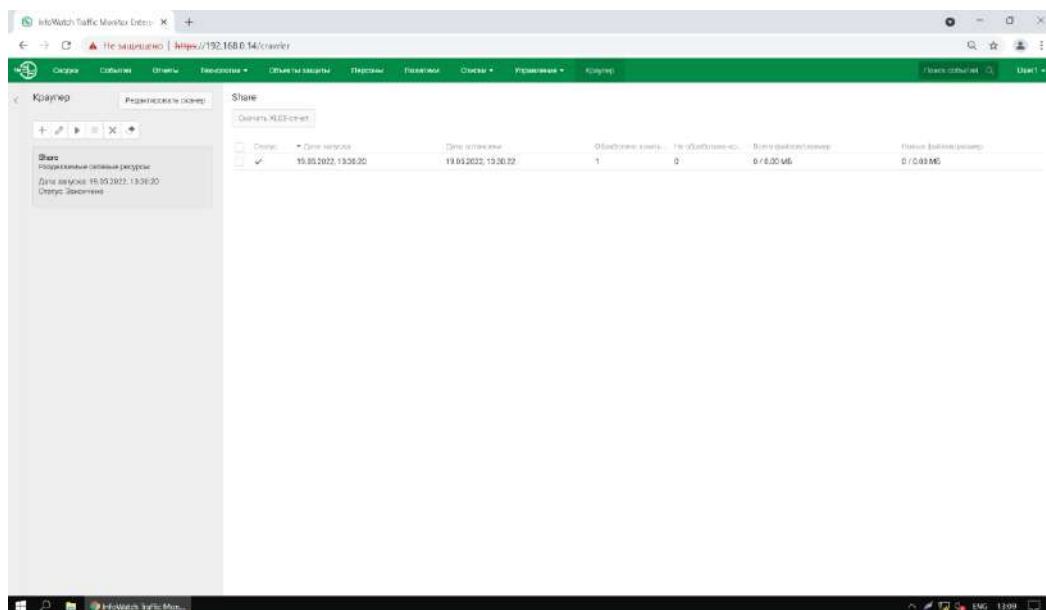


Рисунок 2.53 – Созданная задача

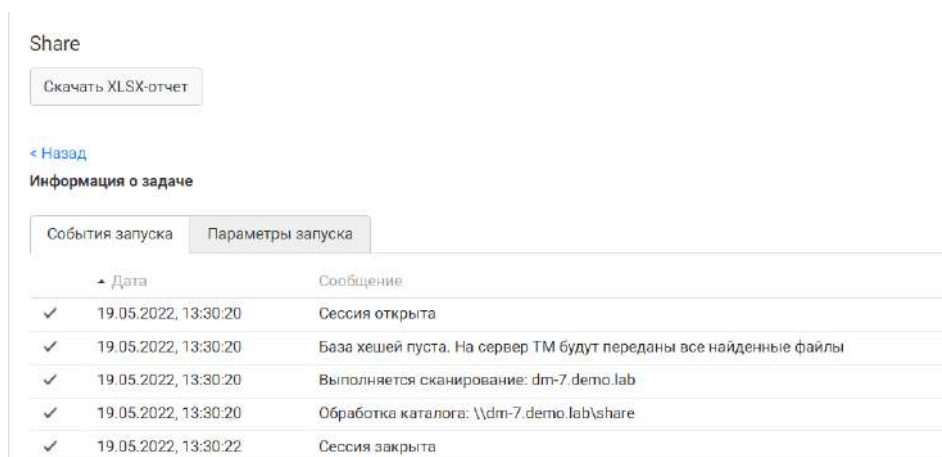


Рисунок 2.54 – Отчет задачи Share

Зафиксируйте выполнение задания скриншотом настройки в web-консоли:

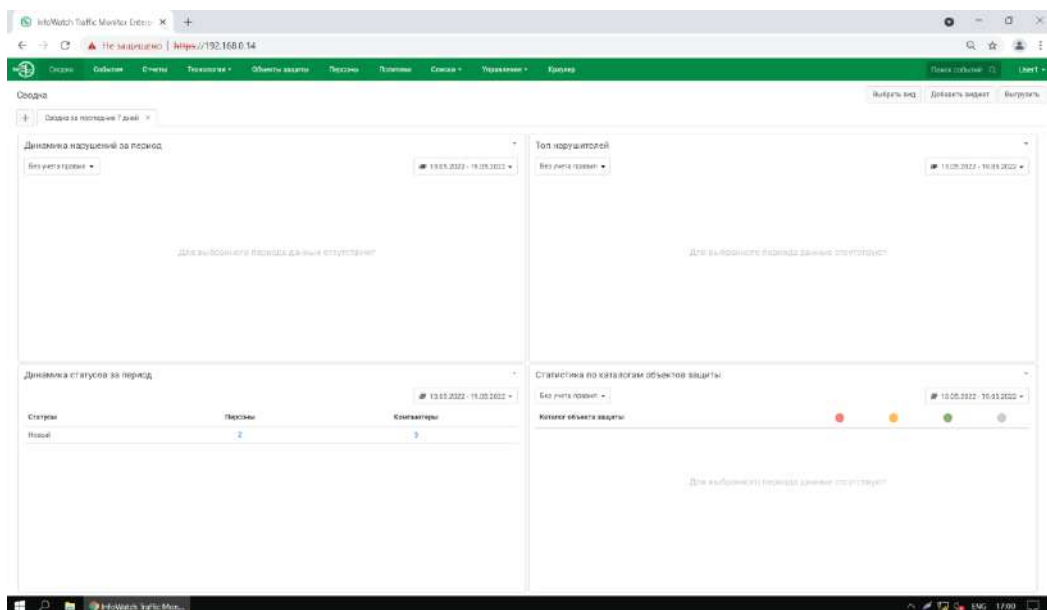


Рисунок 2.55 – Веб консоль ТМ

## 2.5. Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания 16 событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

## **ЗАКЛЮЧЕНИЕ**

Настоящие методические указания включают в себя разделы, которые распространяются на студентов, участвующих в итоговой аттестации в виде демонстрационного экзамена по профессиям и специальностям среднего профессионального образования, разработаны с целью эффективной организации подготовки обучающихся по модулю «Установка и конфигурирование DLP системы» по стандартам демонстрационного экзамена по коду 1.3 по компетенции №F7 «Корпоративная защита от внутренних угроз информационной безопасности».

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Распоряжение Министерства Просвещения Российской Федерации от 01.04.2020 года № Р-36 «О внесении изменений в Приложение к распоряжению Министерства просвещения Российской Федерации от 01.04.2020 года №Р-42 «Об утверждении методических рекомендаций о проведении аттестации с использованием механизма демонстрационного экзамена».
2. Приказ Союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия) от 29 октября 2018 г. № 29.10.2018-1 «Об утверждении перечня компетенций ВСП».
3. InfoWatch EndPoint Security «Руководство пользователя» – [https://www.infowatch.ru/sites/default/files/products/EndpointSecurity/InfoWatch\\_Endpoint\\_Security\\_user\\_guide\\_120116.pdf](https://www.infowatch.ru/sites/default/files/products/EndpointSecurity/InfoWatch_Endpoint_Security_user_guide_120116.pdf).