

Задача 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Office” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Office” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: iwtm-officer, пароль: xxXX1122, права пользователя домена
Логин: ldap-user, пароль: xxXX1122, права пользователя домена

Логин: iwdm-admin, пароль: xxXX1122, права администратора домена и локального администратора

Логин: user-agent, пароль xxXX1122, права пользователя домена

Логин: user-gr, пароль xxXX1122, права пользователя домена

Задача 1: Решение

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

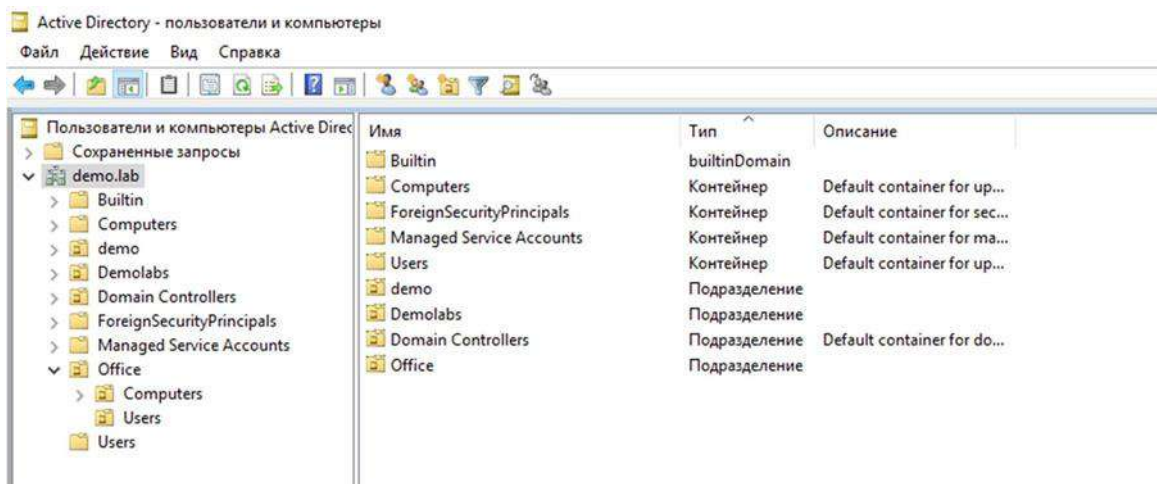


Рисунок 1 - Оснастка Пользователи и компьютеры

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».

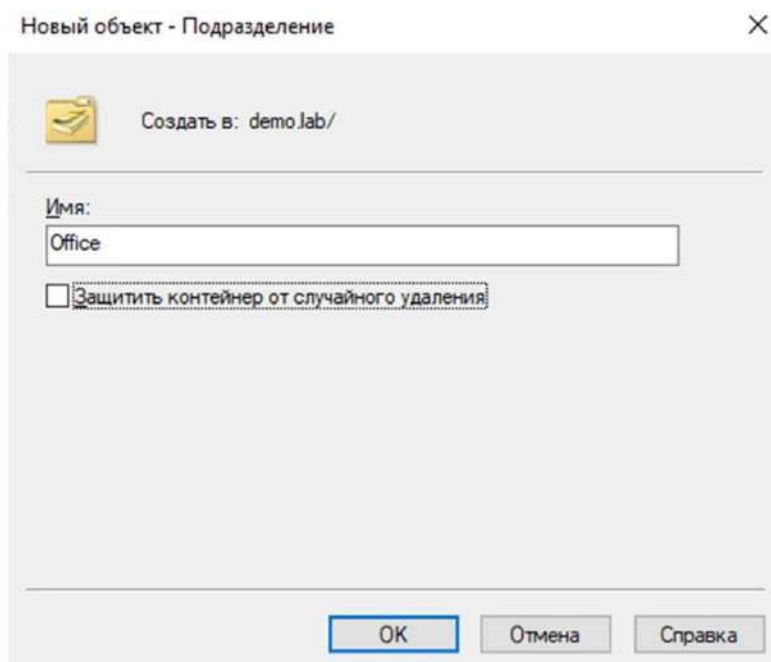


Рисунок 2 - Создания подразделения

Затем, необходимо создать пользователей. Для удобства, советую сначала создать группу «Userss», а затем создавать пользователей. Для создания группы нужно в подразделении кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Группа».

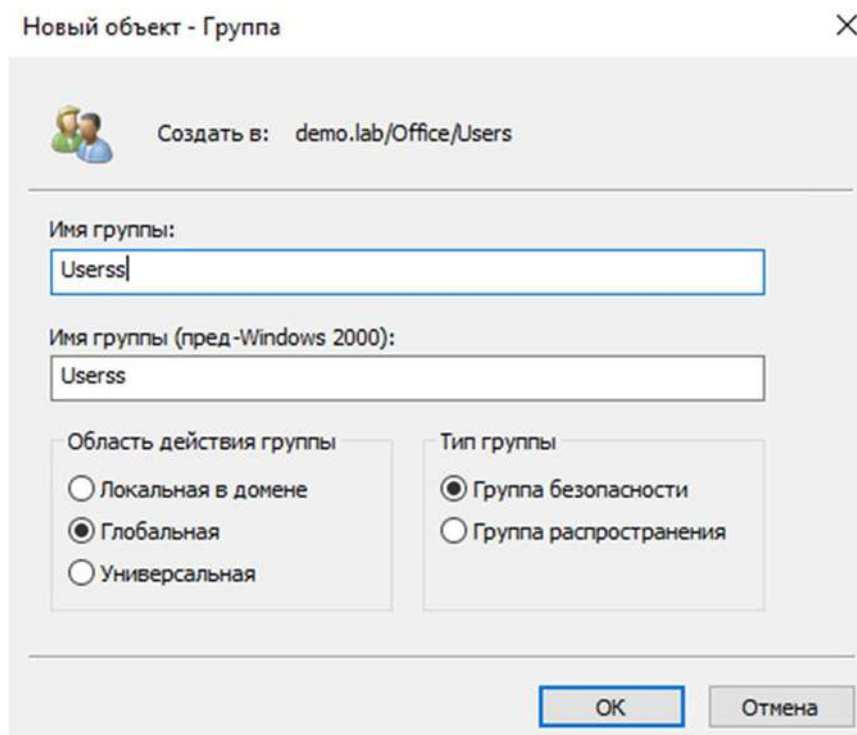


Рисунок 3 – Создание группы

После создания группы можно приступать к созданию пользователей. Начнем с пользователя iwdm-admin. Этот пользователь требует прав доменного и локального администратора.

Для создания пользователя нужно в подразделении Users кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Пользователь». Пароль каждого пользователя должен быть **xxXX1122**. Все галочки выставлять строго в соответствии с рисунками 4 и 5!

Новый объект - Пользователь

Создать в: demo.lab/Office

Имя: iwdm-admin Инициалы:

Фамилия:

Полное имя: iwdm-admin

Имя входа пользователя: iwdm-admin @demo.lab

Имя входа пользователя (пред-Windows 2000): DEMO\ iwdm-admin

< Назад Далее > Отмена

Рисунок 4 – Создание пользователя ч.1

Новый объект - Пользователь

Создать в: demo.lab/Office

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 5 – Создание пользователя ч.2

Теперь необходимо предоставить созданному пользователю права доменного администратора. Для этого необходимо нажать ПКМ на созданном пользователе и выбрать пункт «Добавить в группу». В открывшемся окне, необходимо ввести «Domain Admins» («Администраторы домена», если винда русская.) в поле «Введите имена выбираемых объектов».

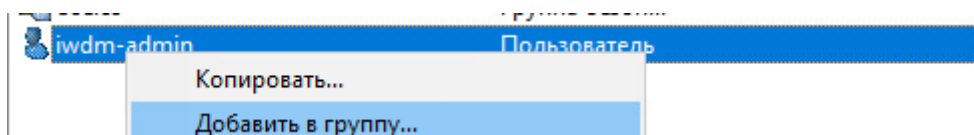


Рисунок 6 – «Добавление пользователей в группу ч.1»

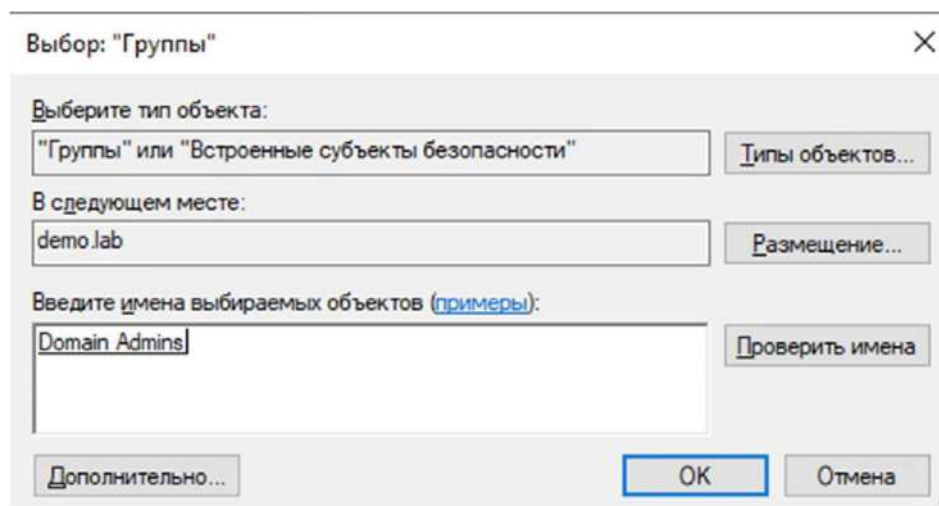


Рисунок 7 – «Добавление пользователей в группу ч.2»

Итак, теперь пользователь состоит в группе Доменных администраторов, теперь нужно также предоставить ему права локального администратора. Для этого, будет необходимо создать групповую политику.

Для создания групповой политики перейдите в оснастку «Управление групповой политикой» (рис. 7) в меню «Средства» в Диспетчере серверов. Затем, войдите во вкладку *demo.lab*, по ней же нажмите ПКМ и выберите «Создать объект групповой политики в этом домене и связать его» (рис.8). Назовите объект политики «Local Admins», другие параметры не меняйте.

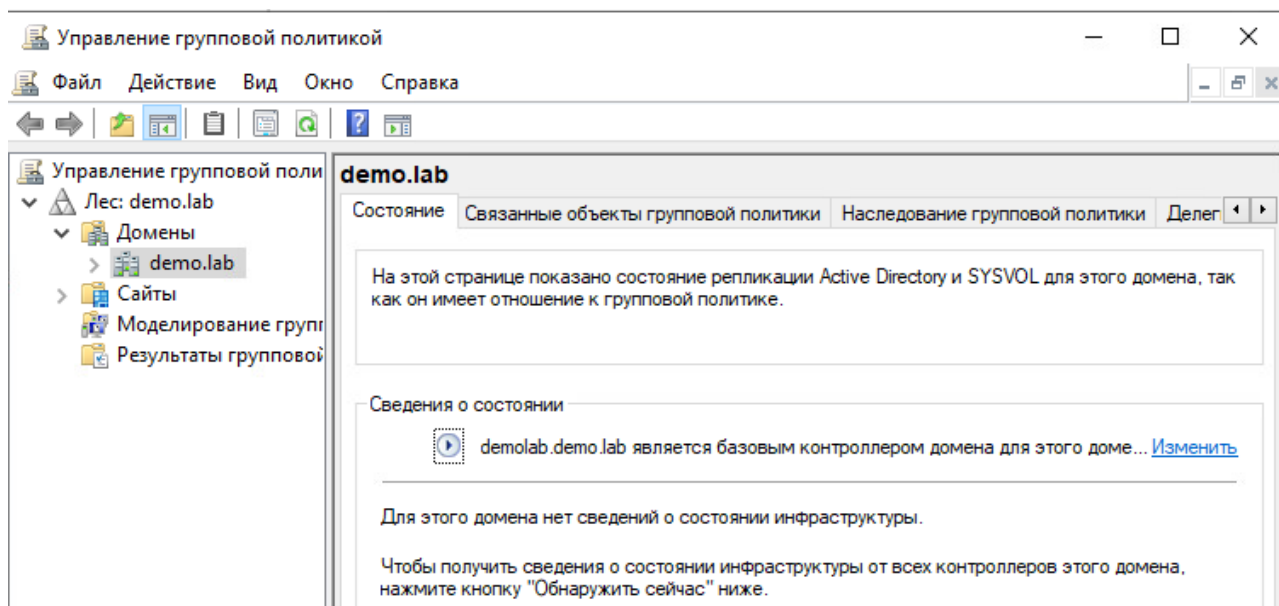


Рисунок 8 – Управление групповой политикой

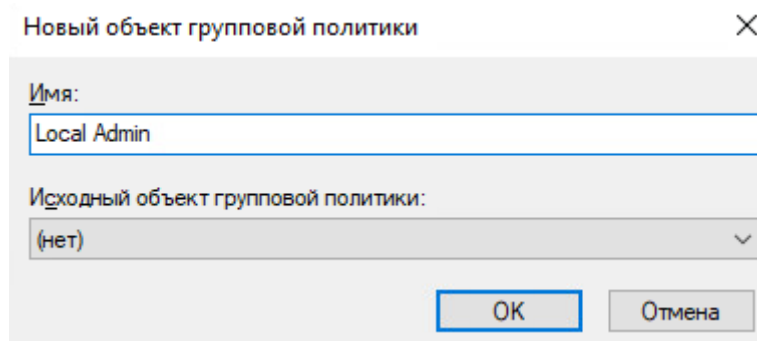


Рисунок 9 – Создание групповой политики

Дважды нажмите ЛКМ для перехода к только что созданной политике и измените «Фильтры безопасности» политики. Для этого, сначала удалите объект «Прошедшие проверку», после чего добавьте объект «Domain Computers» (компьютеры домена на русском).

После изменения фильтров безопасности нажмите ПКМ на объект политики «Local Admins» и выберите «Изменить», после чего откроется «Редактор управления групповыми политиками». Перейдите по пути «Конфигурация компьютера – Настройка – Параметры панели – Локальные пользователи и группы». В свободном поле кликните ПКМ, выберите «Создать – Локальная группа», после чего откроется окно «Новые свойства локальной группы». Конфигурируйте настройки в соответствии с рисунком 10.

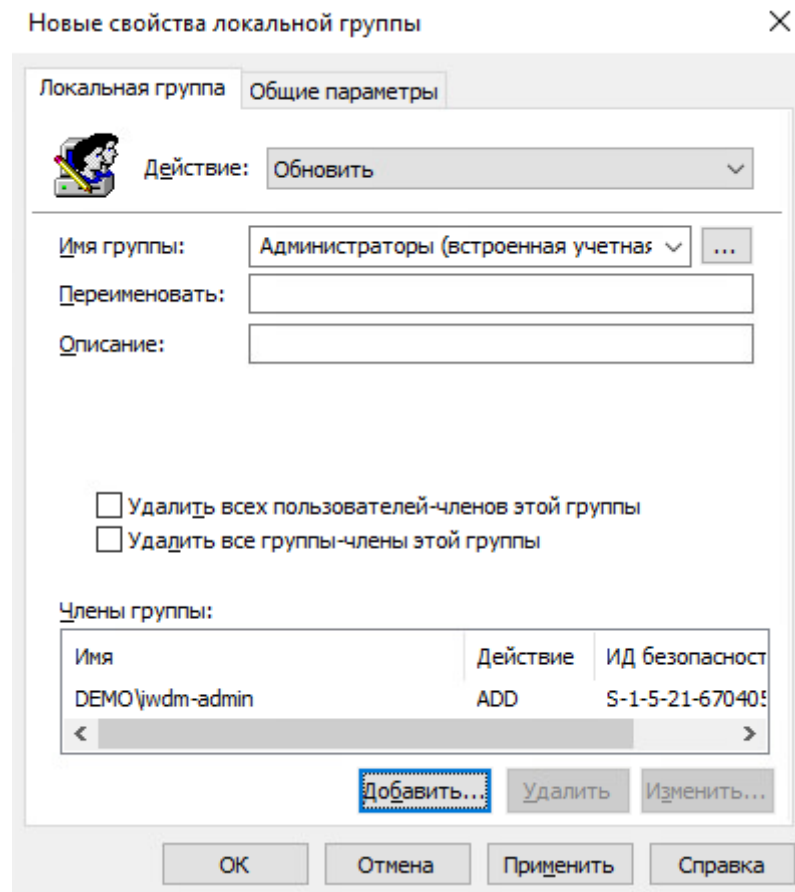


Рисунок 10 – Редактирование свойств локальной группы

Сохраните и примените настройки. Теперь покиньте оснастку групповых политик и вернитесь к оснастке «Пользователи и Компьютеры Active Directory».

Создайте пользователей iwtm-officer, ldap-user, iwdm-admin, user-agent и user-gp. **Кроме создания пользователей ничего не требуется, ни в какие группы их добавлять не надо.**

Задача 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен. Необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно.

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

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя `ldap-user`.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена `iwtm-officer` с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

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» на рабочем столе компьютера.

Задача 2: Решение

Выполнение этого задания начинайте с IP-адресации. Убедитесь, что все IP-адреса выставлены верно, и что все виртуальные машины находятся в одной сети и доступны друг другу. Для проверки доступности используйте команду **ping <адрес>**.

Подсказка:

Для установки адреса на виртуальную машину IWTM используйте **nmtui**. В условиях его отсутствия используйте команду: **ip a a <адрес>/<короткая маска > dev <интерфейс>**

Чтобы узнать IP-адрес виртуальной машины IWTM используйте команду **ip a** или **nmtui**.

Если адрес не установлен, попробуйте обратиться к документации, выдаваемой на экзамене, или к файлу /etc/hosts. Введите команду /etc/hosts и найдите адрес, сопоставляемый с названием виртуальной машины.

После того, как вы узнали IP-адреса всех устройств в виртуальной сети перейдите к настройке DNS. Для этого, откройте оснастку DNS во вкладке «Средства» Диспетчера серверов на виртуальной машине Demo.lab. Затем, перейдите по пути «DEMOLAB – Зоны прямого просмотра – demo.lab». Щелкните по пустому пространству и нажмите «Создать узел (A или AAAA...)».

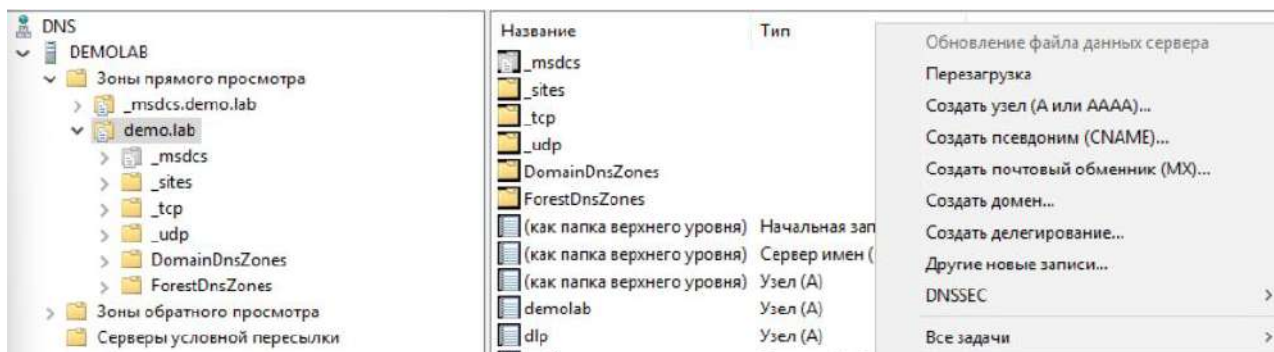


Рисунок 11 – Оснастка DNS

Создайте DNS запись для каждой виртуальной машины аналогично примерам на рисунках 12 и 13

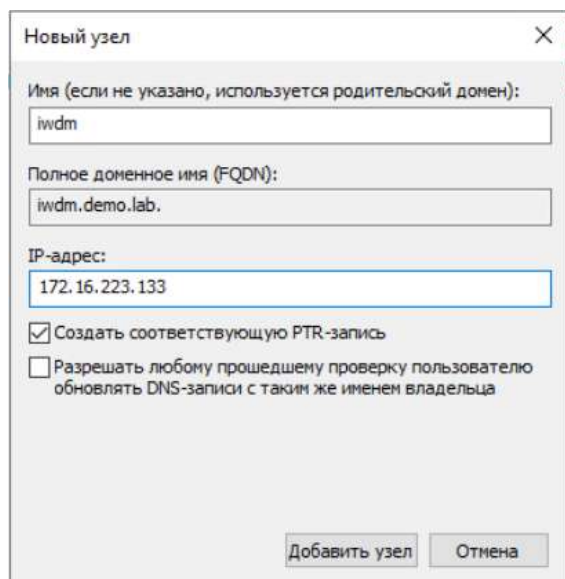


Рисунок 12 – Создание DNS записи

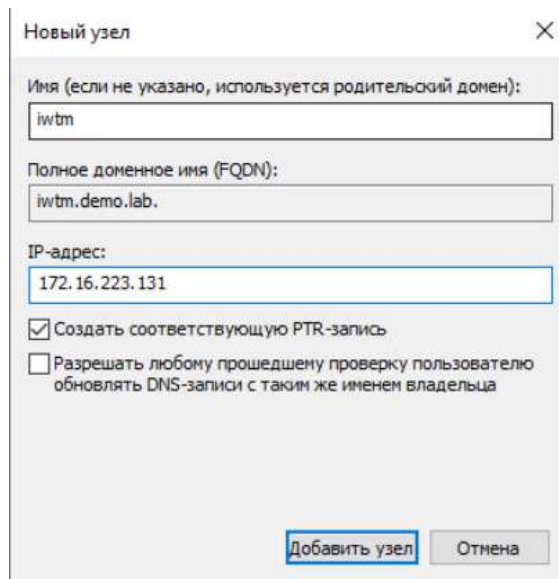


Рисунок 13 – Создание DNS записи

После создания DNS-записей откройте браузер и введите в поисковую строку **iwtm/** (слэш обязателен!), после чего откроется веб-интерфейс консоли управления Traffic Monitor.

Учетные данные для входа в WEB-интерфейс Traffic Monitor:

- логин: officer
- пароль: xxXX1234

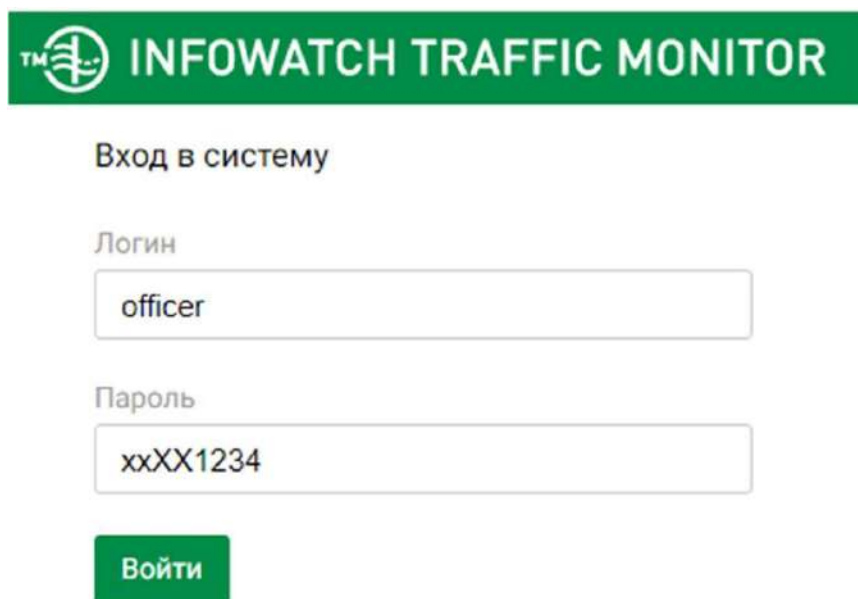


Рисунок 13 – «Вход в Traffic Monitor»

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

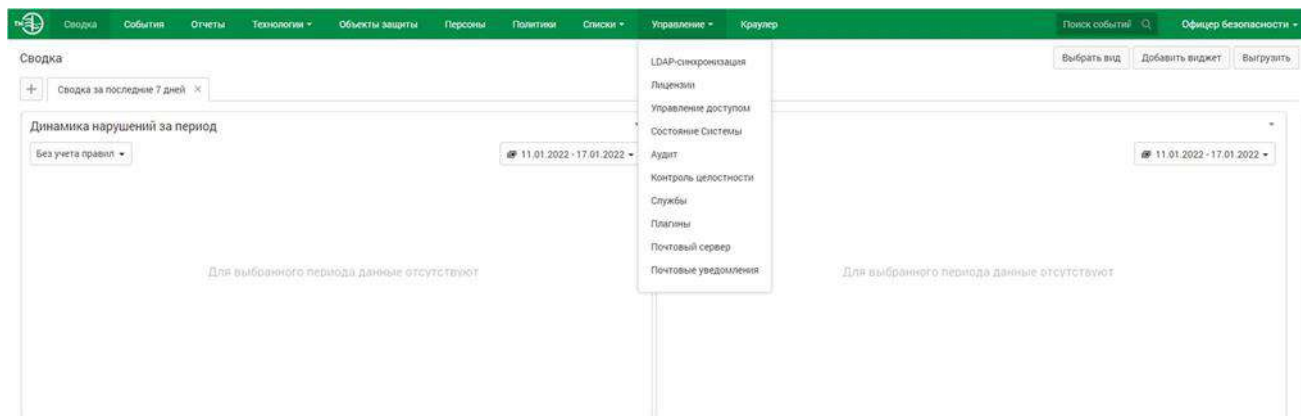


Рисунок 14 – «Переход к настройке LDAP-синхронизации»

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/DNS виртуальной машины demo.lab (пр. 172.16.1.2, или пр. demolab),
- 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: ldap-user,

– Пароль: xxXX1122.

Конфигурация должна совпадать с конфигурацией с рисунка 15. После ввода всех параметров, нажмите кнопку «Проверить соединение» - если проверка соединения прошла успешно сохраните и примените конфигурацию. В обратном же случае – перепроверьте настройки синхронизации.

Имя сервера

Тип сервера

Синхронизация

Период синхронизации

Выполнять каждые

Настройки соединения

LDAP-сервер

Тип соединения

Использовать протокол Kerberos ☐

Глобальный LDAP-порт

LDAP-порт

Использовать глобальный каталог ☒

LDAP-запрос

Анонимный доступ ☐

Логин

Пароль

Рисунок 15 – 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».

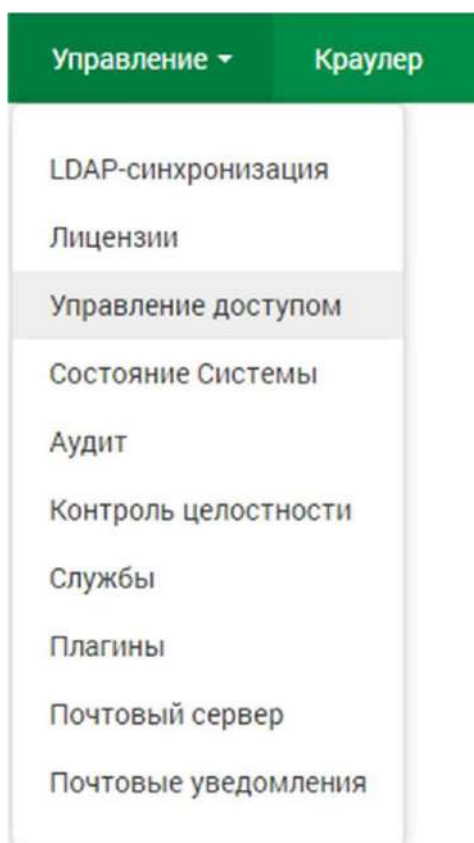


Рисунок 16 – Управление доступом

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

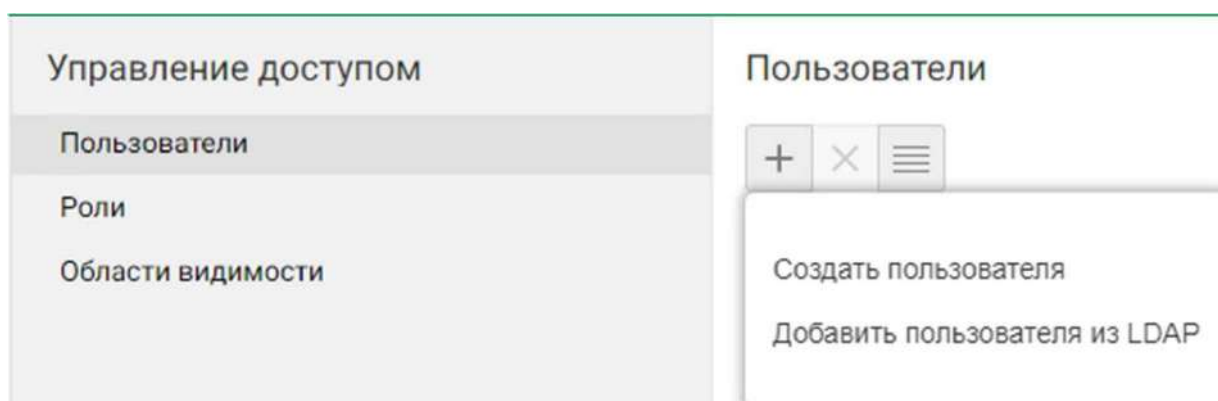


Рисунок 17 – Добавление пользователя из LDAP ч.1

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

Пользователь	Доменный аккаунт	Адрес сервера	Департамент
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer@DC=DEMO.DC=LAB	172.16.223.132	
<input type="checkbox"/> iwtm-officer			
<input type="checkbox"/> iwtm-officer			

Рисунок 18 - 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), роли (Администратор, Офицер безопасности) и области видимости (Полный доступ, VIP). Нажмите кнопку «Сохранить» для применения настроек.

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

Редактирование пользователя

Логин: iwtm-officer

Статус: Активен

Email: iwtm-officer@demo.lab

Полное имя: iwtm-officer

Роли: Администратор, Офицер безопасности

Области видимости: Полный доступ, VIP

Описание:

Создано: 17.01.2022, 03:58 — Изменено: 17.01.2022, 03:58

Сохранить Отменить

Рисунок 19 – 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».

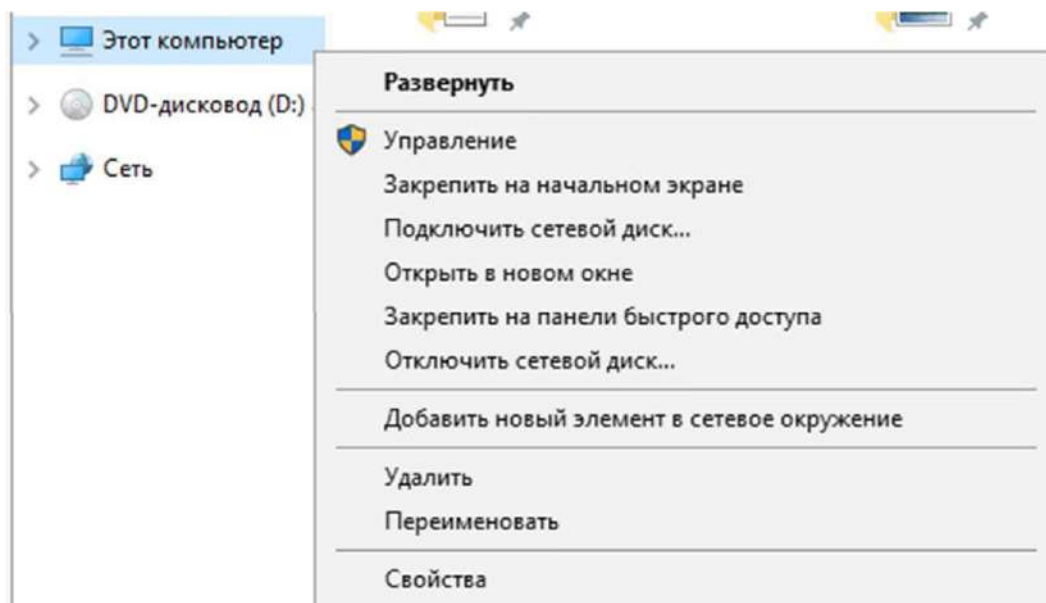


Рисунок 20 – Переход к свойствам компьютера

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».

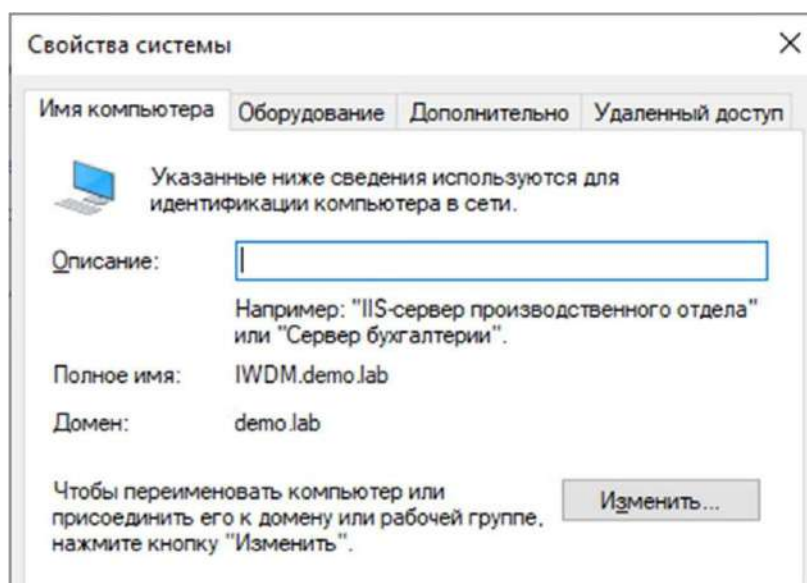


Рисунок 21 – Добавление ПК в домен demo.lab ч.1

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

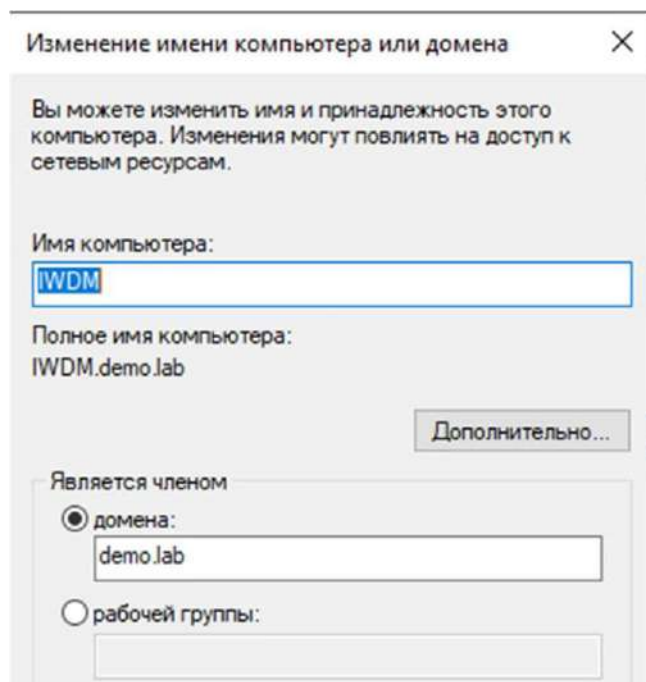


Рисунок 22 – «Добавление ПК в домен demo.lab ч.2

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 подразделение «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 подразделение «Office» (Рисунок 18).

Задача 3: Установка и настройка сервера агентского мониторинга

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя iwdm-admin, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие данные, измененные вами, в текстовом файле «отчет.txt» с на рабочем столе компьютера.

Задача 3: Решение

Для того, чтобы приступить к выполнению этой задачи – вам необходимо установить InfoWatch Device Monitor и СУБД PostgreSQL на виртуальную машину IWDM. Найдите инсталляционные файлы, которые обычно, располагаются в подключенном к IWDM диске и инициализируйте процесс установки приложений. Начинайте с PostgreSQL.

Соглашайтесь со всем подряд ничего не меняя, до этапа выбора компонентов. В качестве компонентов выберите только «PostgreSQL Server» и «Command Line Tools». Затем снова пропускайте любой выбор, до момента установки пароля пользователю. В качестве пароля введите **стандартный пароль – xxXX1122**. По окончании установки, закройте установочное окно.

Найдите и запустите установочный файл Device Monitor (Setup.Device.Monitor.ru.*). 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 базуданных – PostgreSQL, и, перейдя к следующему этапу, введите параметры подключения к БД (рис. 23), с ранее созданным паролем.

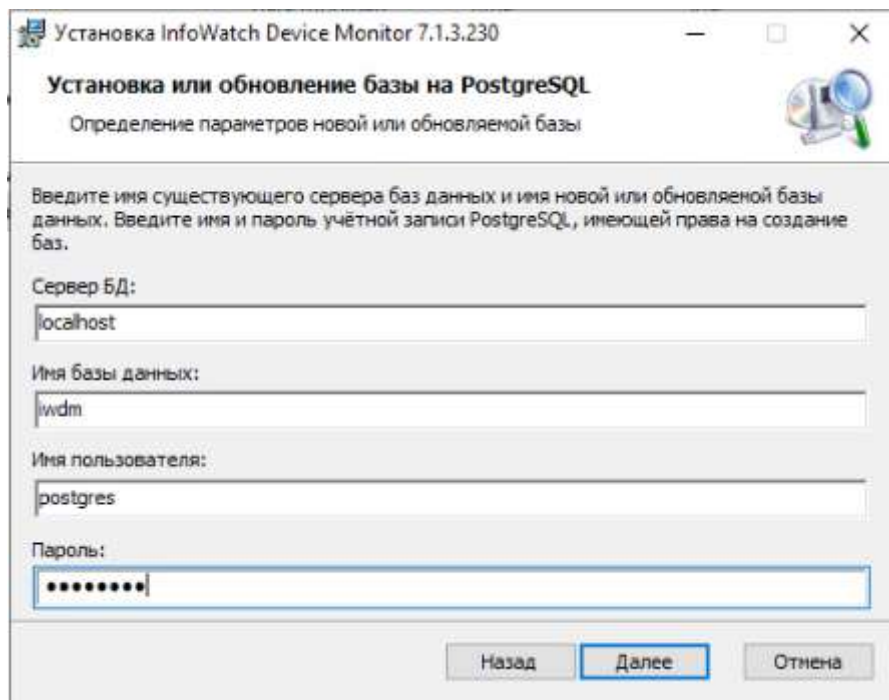


Рисунок 23 – конфигурация подключения к БД

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 (xxXX1122).

Затем, настройте соединение с Traffic Monitor (рис. 24), укажите адрес (iwtm) и токен авторизации (возьмите его из веб-интерфейса IWTM – Управление – Плагины – Infowatch Device Monitor – токен). 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 – xxXX1122).

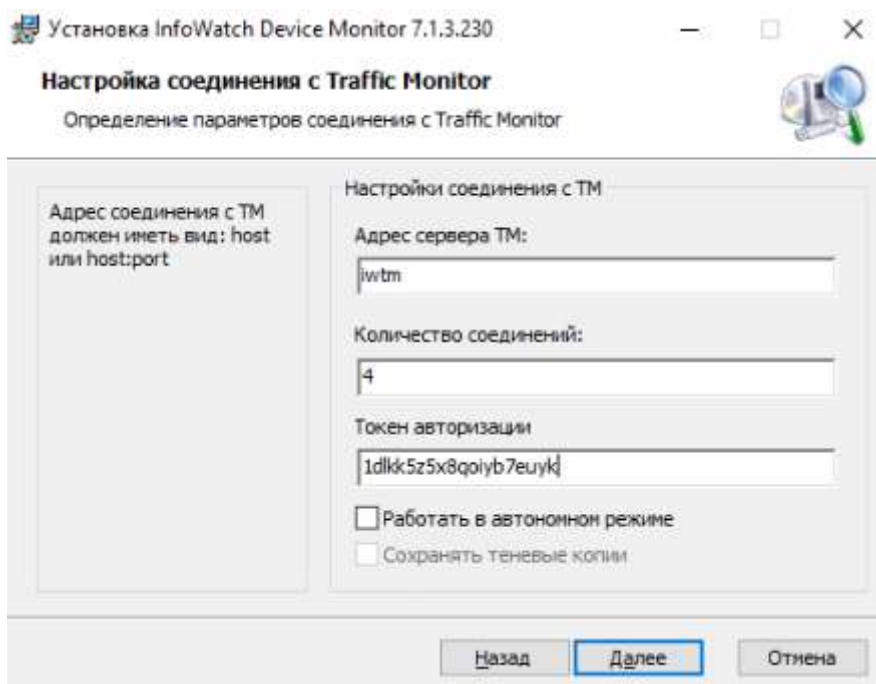


Рисунок 24 – Настройка соединения с Traffic Monitor

Установите приложение. По окончании установки, закройте окно и запустите ярлык «Консоль управления». После открытия консоли введите параметры подключения – адрес (localhost), логин и пароль.

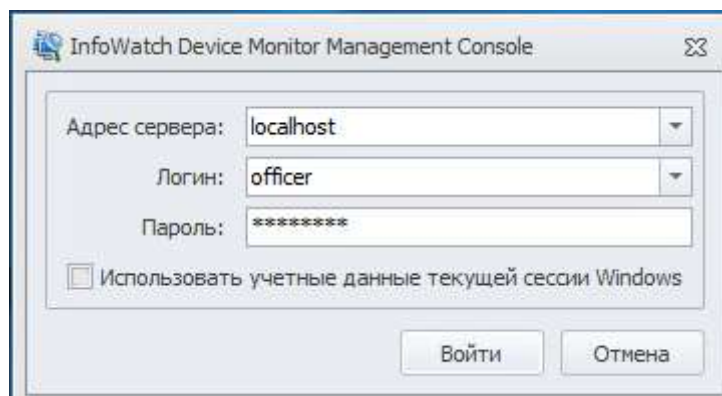


Рисунок 25 – Подключение к серверу

После входа в консоль управления, необходимо создать синхронизацию со службой каталогов. Для этого необходимо перейти ко вкладке «Инструменты – Настройки – Интеграция со службами каталогов», а затем нажать зеленый плюс в верхней части интерфейса, после чего ввести адрес домена (прим. demo.lab), указать тип «авто» и тип авторизации «учетные данные пользователя»

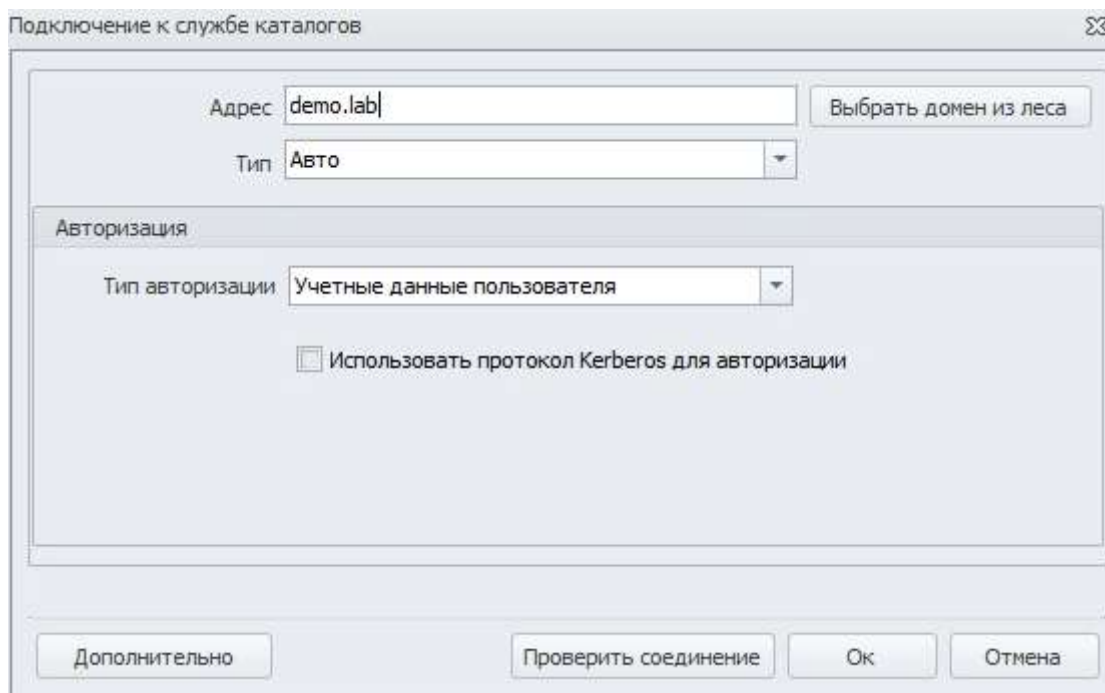


Рисунок 26 – Подключение к службе каталогов

После заполнения параметров подключения необходимо нажать «ОК» и дождаться успешного подключения. После добавления, необходимо добавить синхронизацию пользователей и компьютеров домена. Для этого необходимо нажать зеленый плюс в подвкладке «Настройки синхронизации», после чего ввести параметры синхронизации:

- Имя домена: demo.lab;
- Синхронизировать: компьютеры;
- Синхронизируемые директории: demo,
- Политика по умолчанию: политика на устройства.

Нажать «Ок», повторить с пользователями. Применить и сохранить.

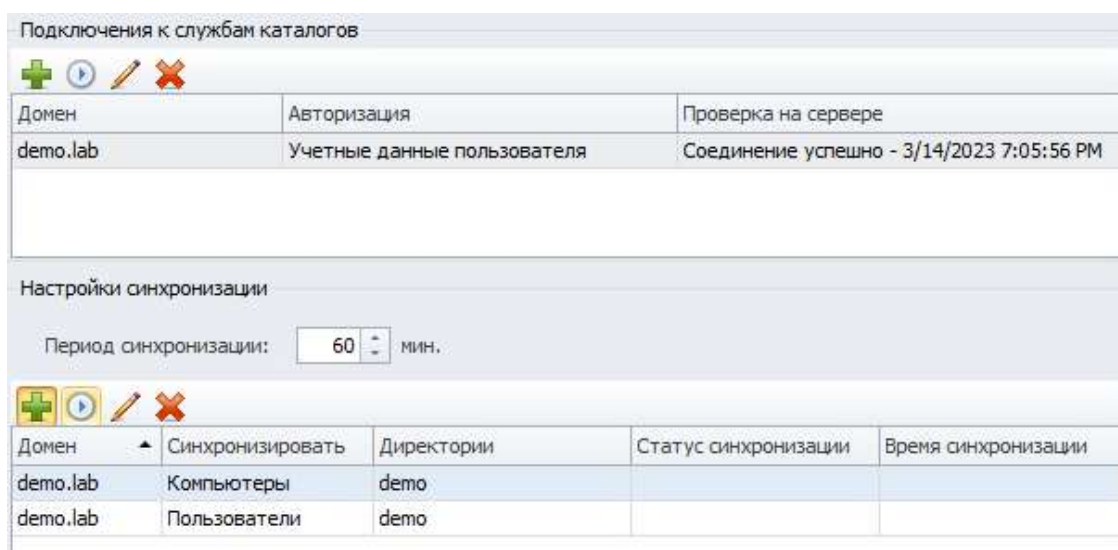


Рисунок 26 – Настройка синхронизации

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя `iwdm-admin`, установить полный доступ к системе, установить все области видимости. Для создания пользователя необходимо перейти ко вкладке «Инструменты – Пользователи консоли и роли», там найти кнопку «Добавить из AD», после чего нажать на вкладку `demo.lab`, найти в поиске пользователя `iwdm-admin` (которого, создавали раньше) и нажать «Сохранить».

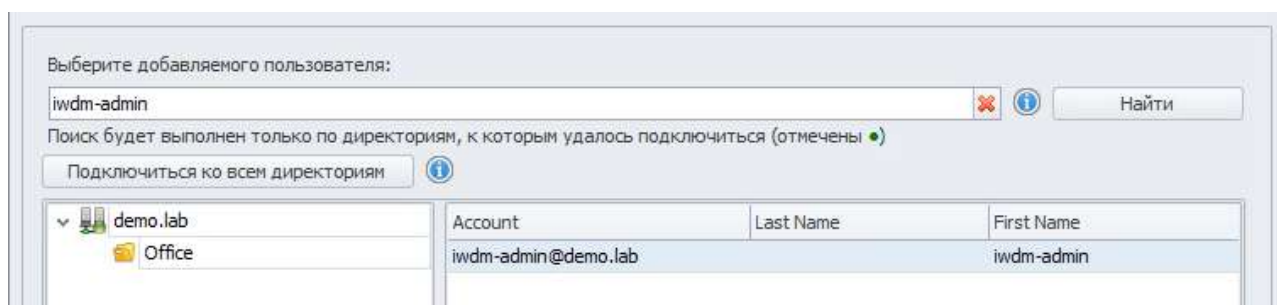


Рисунок 27 – Добавление пользователя

А затем установить настройки пользователя в соответствии с рисунком 28 – дать ему полный доступ ко всем контурам и ролям. Применить и сохранить.

Создание пользователя

Σ3

Логин: DEMO\jwdm-admin

Пароль: *****

Повтор пароля: *****

Полное имя: jwdm-admin

Видит сотрудников

Группа сотрудников	Роль пользователя
Все группы	Офицер безопасности группы

Добавить...

Изменить...

Удалить

Видит компьютеры

Группа компьютеров	Роль пользователя
Все группы	Офицер безопасности группы

Добавить...

Изменить...

Удалить

Общие роли

Администратор	Выбрать
Офицер безопасности	Удалить

Сохранить

Отмена

Рисунок 28 – Права и роли пользователя

Задача 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user2.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Test” на домене.

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена. Необходимо создавать отдельные объекты групповых политик на каждое Задача и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задача 4: Решение

Введите клиентские виртуальные машины в домен по аналогии с IWDM. Сразу после введения ВМ в домен, на панели задач нажмите ПКМ на иконку, отвечающую за сетевое подключение, и выберите «Открыть “Параметры сети и Интернет”».

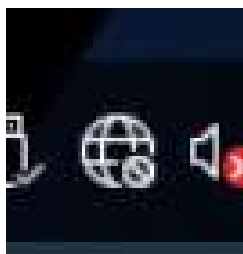


Рисунок 29 – Состояние сети

В открывшемся окне нажмите «Центр управления сетями и общим доступом», затем (слева) откройте окно изменить дополнительные параметры общего доступа. В открывшемся окне **в каждом профиле выберите разрешающее действие.**

УБЕДИТЕСЬ В ТОМ, ЧТО ВРЕМЯ НА КЛИЕНТАХ И СЕРВЕРЕ СОВПАДАЕТ.

Теперь вернитесь к консоли управления DM, перейдите ко вкладке «Задачи» и нажмите «Создать задачу» (зеленый плюс). Установите произвольное название, а в качестве типа задачи выберите «задача первичного распространения»

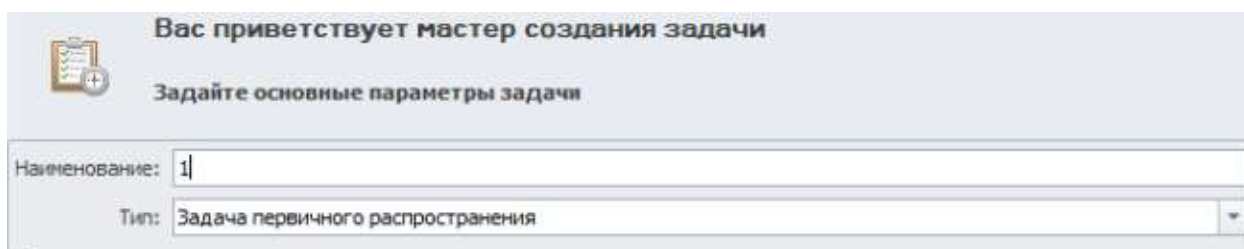


Рисунок 30 – Создание задачи

Затем, выберите компьютеры, на которые будет распространяться задача.

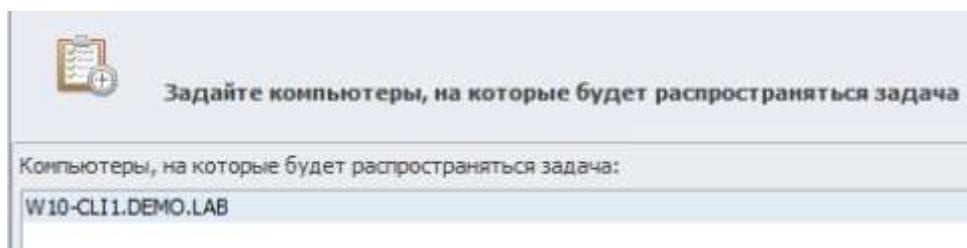
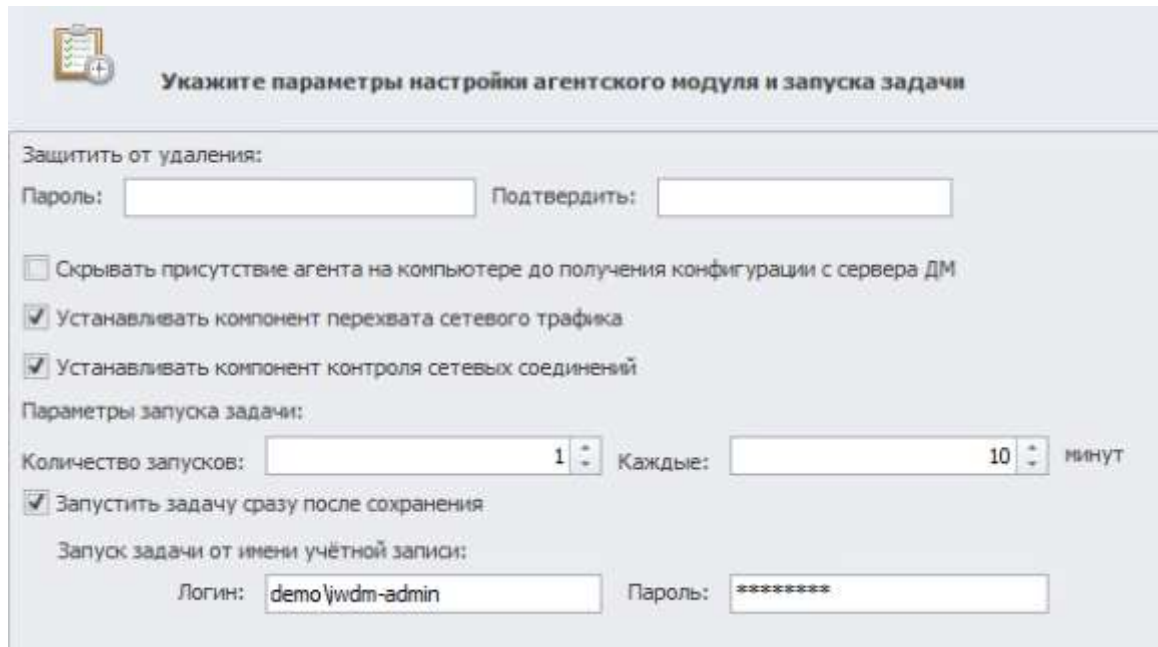


Рисунок 31 – Создание задачи

Далее соглашайтесь на все подряд, до пятого шага. На пятом шагу установите логин и пароль пользователя, от которого будет выполняться задача. Обязательно указывайте **ДОМЕН** в логине. Пример на рисунке 32.



Укажите параметры настройки агентского модуля и запуска задачи

Защитить от удаления:

Пароль: Подтвердить:

☐ Скрывать присутствие агента на компьютере до получения конфигурации с сервера ДМ

☒ Устанавливать компонент перехвата сетевого трафика

☒ Устанавливать компонент контроля сетевых соединений

Параметры запуска задачи:

Количество запусков: Каждые: минут

☒ Запустить задачу сразу после сохранения

Запуск задачи от имени учётной записи:

Логин: Пароль:

Рисунок 32 – Шаг 5

На шаге 6 установите параметры обоих пунктов на «Не ожидать». Примите настройки, после чего задача автоматически запустится.

Для установки агента мониторинга на вторую виртуальную машину с помощью групповых политик. Для начала, необходимо получить установочный пакет агента Device Monitor. Для этого перейдите к серверу Device Monitor, в консоль управления, во вкладку «Инструменты – Создать пакет установки». Выбрать папку назначения для сохранения установочных пакетов (произвольное, главное не потеряйте). Далее соглашайтесь на все, вплоть до шага 4. На шаге 4 необходимо установить «не ожидать» и «не уведомлять». Завершите создание пакета, скопируйте 64-битный пакет установки (можно понять из названия) на общую папку \\demolab\share.

Перейдите к виртуальной машине demo.lab, перейдите в диспетчере серверов ко вкладке «средства», в оснастку «Управление групповой политикой».

Создайте новый объект групповой политики, произвольно его назовите, после чего измените фильтры безопасности: удалите «прошедшие проверку» и добавьте второй компьютер в фильтры, а также пользователя для второго ПК.

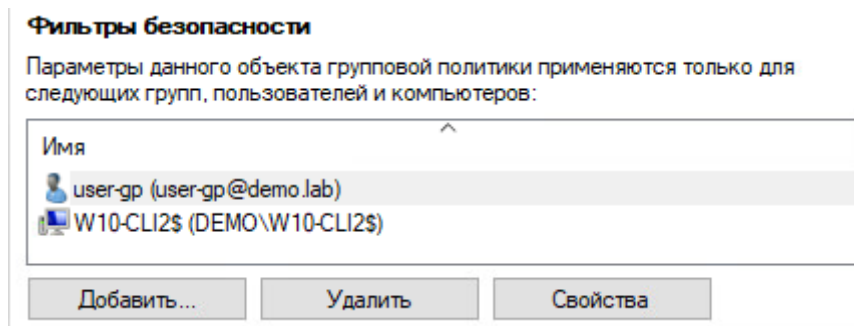


Рисунок 33 – Фильтры безопасности

Перейдите к изменению параметров политики и пройдите по пути «Конфигурация компьютера – Политики – Конфигурация программ – установка программ», в свободном пространстве нажмите ПКМ, затем «создать – пакет...», выберите установочный файл по \\demolab\share. В качестве метода развертывания выберите «особый» или «назначенный».

В открывшемся окне можно настроить дополнительные параметры MSI пакета, но этого делать не надо.

Задача 5: Проверка работоспособности системы

Установка и настройка подсистемы сканирования сетевых ресурсов.

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

Необходимо создать общий каталог Test в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

Задача 5: Решение

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_v*.exe), после чего откройте его.



Рисунок 34 – «Установка Crawler

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

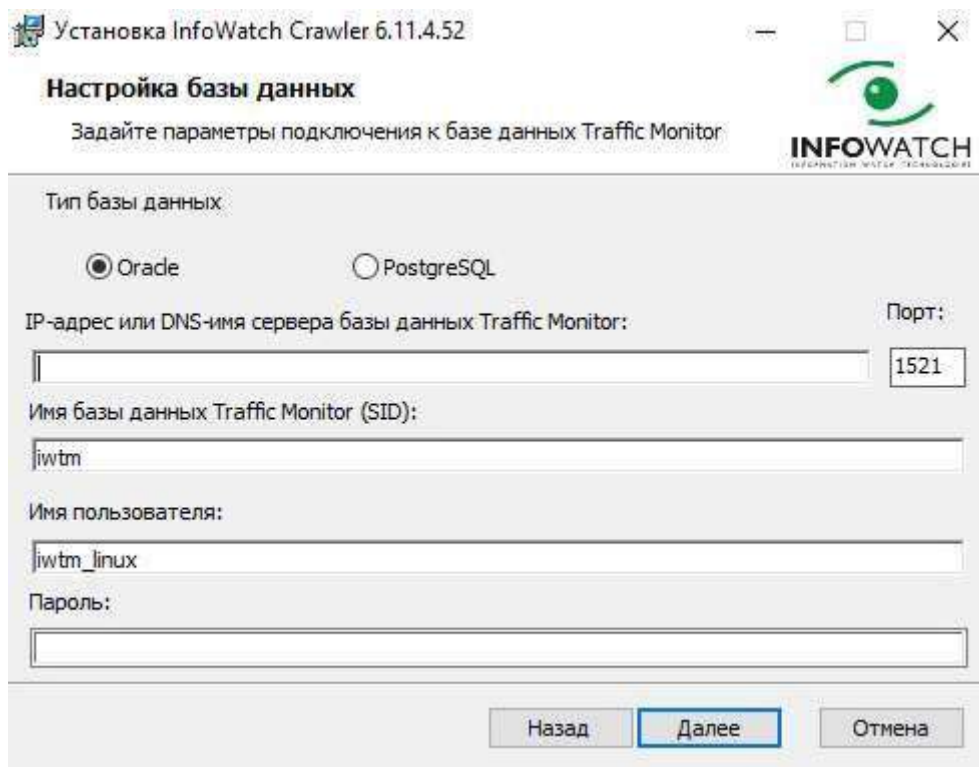


Рисунок 35 – Настройка базы данных

Заполните соответствующую информацию:

- Тип базы данных: PostgreSQL
- IP-адрес или DNS-имя сервера базы данных ТМ: адрес или DNS-имя Traffic

Monitor

- Имя базы данных ТМ (SID): postgres
- Имя пользователя: iwtm
- Пароль: xxXX1234

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

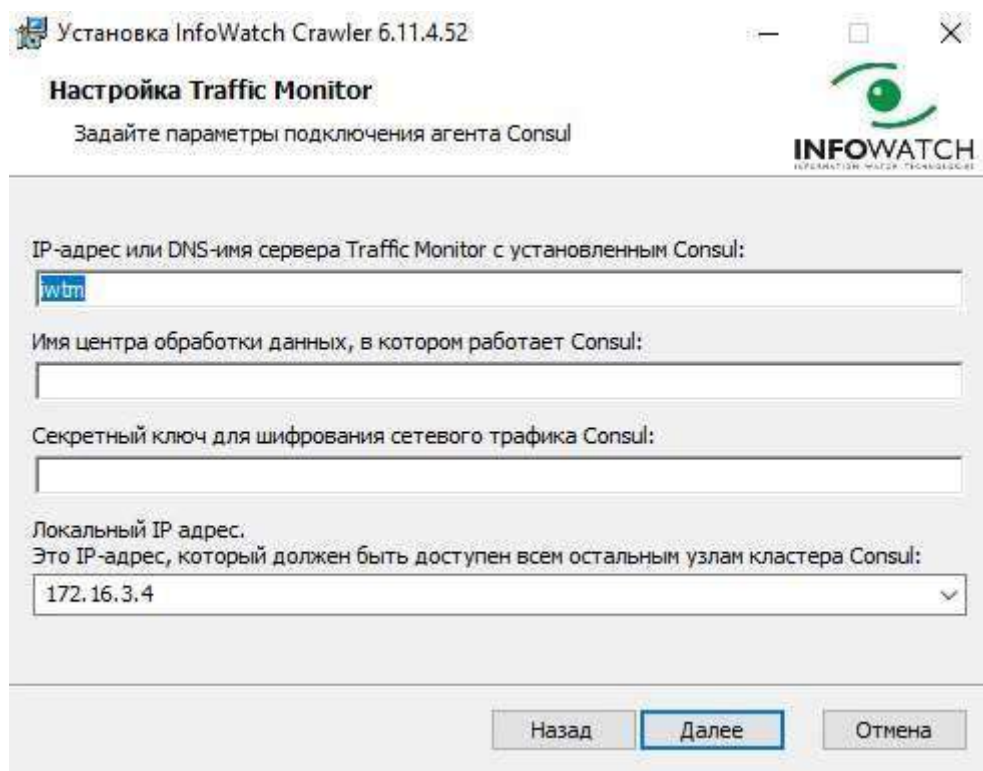


Рисунок 36 – Настройка Traffic Monitor

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.

```
root@iwtm:~  
Microsoft Windows [Version 10.0.17763.1697]  
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.  
C:\Users\iwdm-admin>ssh root@iwtm  
The authenticity of host 'iwtm (172.16.3.3)' can't be established.  
ECDSA key fingerprint is SHA256:/tyqpVxfDBHW7MKssKvQ1ZQiixpraHkbx8nGXGongNI.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'iwtm,172.16.3.3' (ECDSA) to the list of known hosts.  
root@iwtm's password:
```

Рисунок 37 – 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
}[root@iwtm ~]#
```

Рисунок 38 – «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 39 – «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».

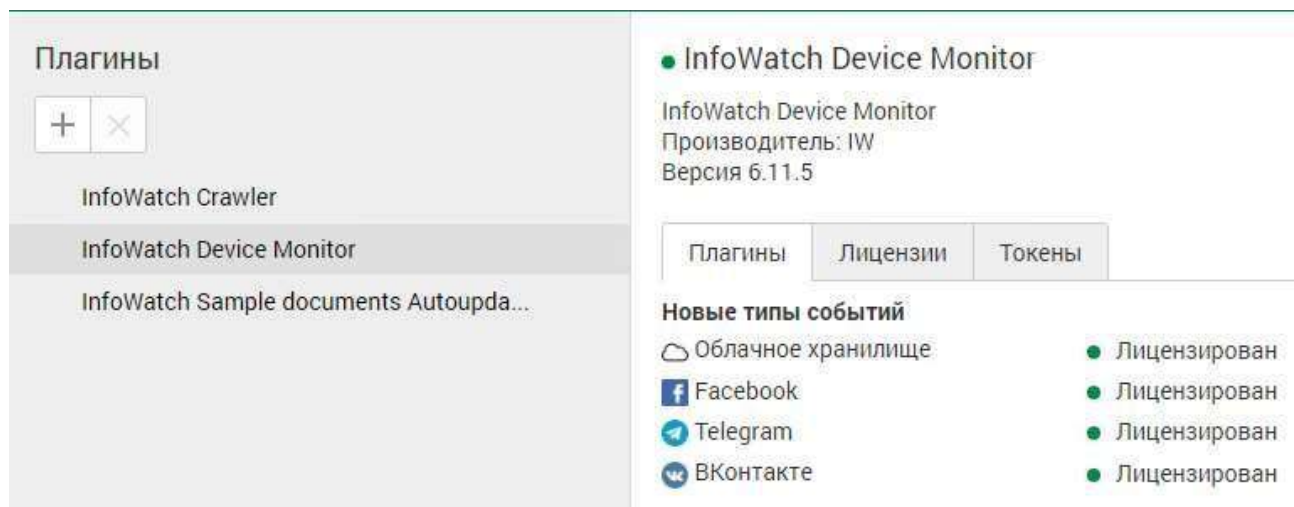


Рисунок 40 – «Плагины Traffic Monitor»

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 41 – «Токен Crawler»

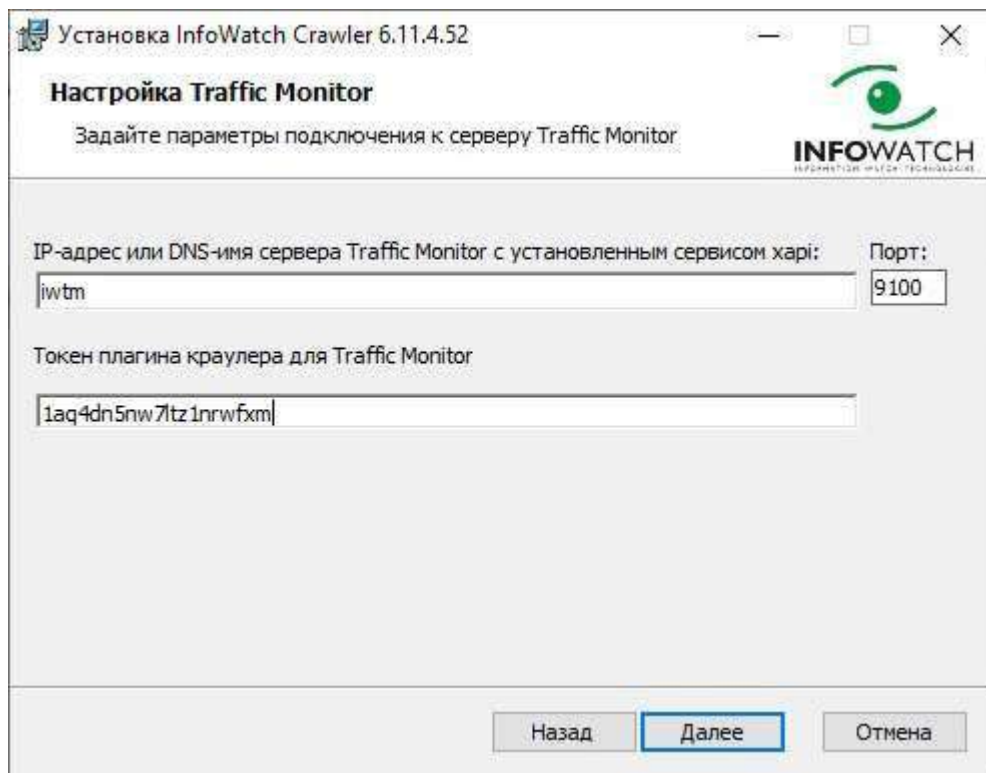


Рисунок 42 – «Заполненная информация о подключении к серверу ТМ»

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».

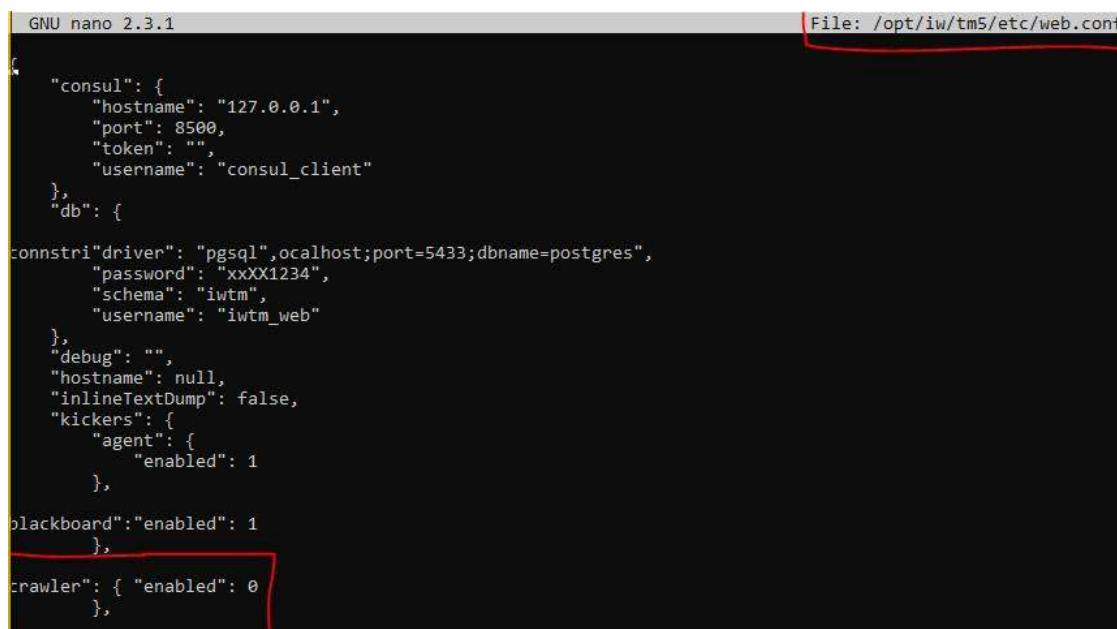


Рисунок 30 – «Параметры crawler в web.conf»

Теперь, нужно создать общую папку на IWDМ. Создайте папку **Test** 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».

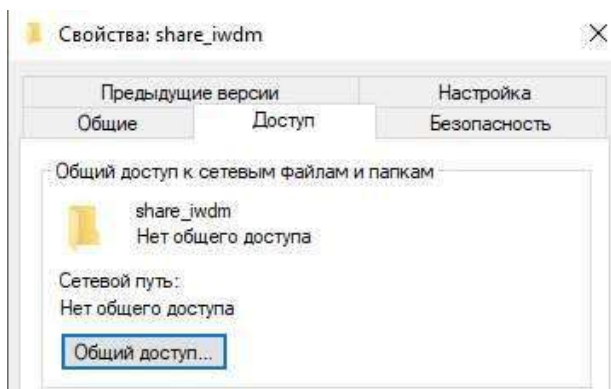


Рисунок 31 – создание общей папки

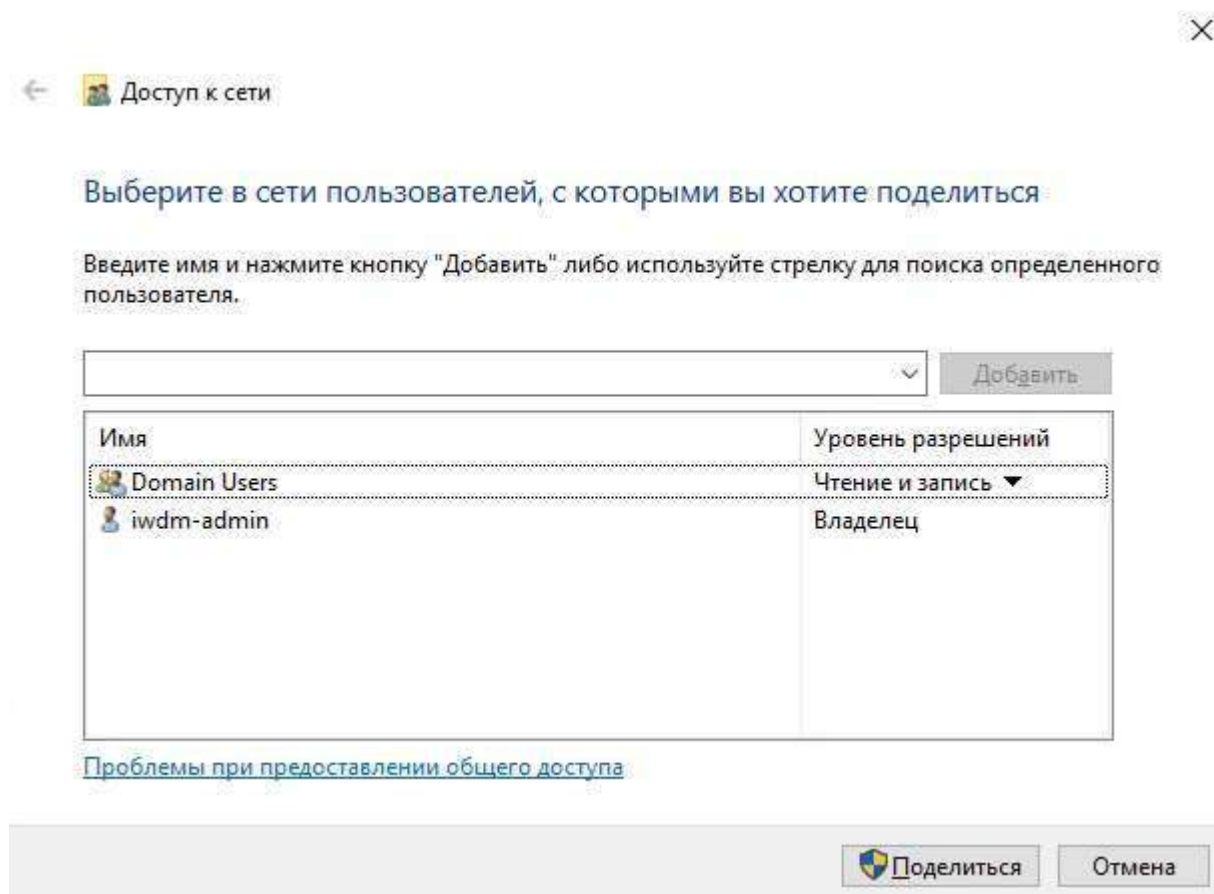


Рисунок 32 – создание общей папки

Обязательно необходимо проверить, существуют ли DNS-записи для IWDМ, и существуют ли они на сервере IWТМ. Для этого необходимо перейти к виртуальной машине IWТМ. Если вы используете DNS-сервер Active Directory, то на IWТМ введите команду **nmtui**. Перейдите к редактированию сетевого подключения и убедитесь, что в графе **DNS Servers** установлен адрес виртуальной машины Demo.lab.

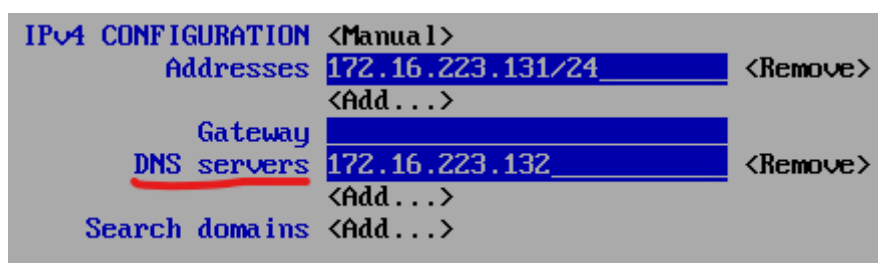


Рисунок 33 – Настройки nmtui

Если вы не используете DNS-сервер, то перейдите к файлу `/etc/hosts` и убедитесь, что в нем есть запись для `iwdm.demo.lab`, подобно той, что приведена на рисунке 34. Для проверки работоспособности DNS, выполните команду **ping iwdm**.

```
[root@iwtm ~]# cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.223.131 iwtm.demo.lab iwtm
172.16.223.133 iwdm.demo.lab iwdm
[root@iwtm ~]# _
```

Рисунок 34 – Файл `/etc/hosts`

После того, как вы убедились, что DNS-запись присутствует и работает, 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.

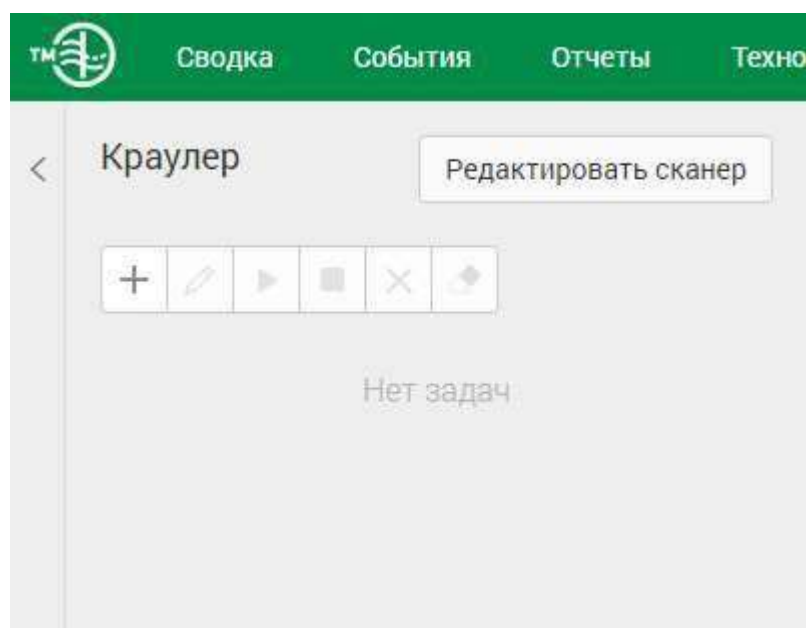


Рисунок 33 – Краулер

Далее, заполните параметры:

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

Больше ничего менять не нужно. Создайте любой текстовый файл в папке Test на виртуальной машине IWDM, для проверки работы Crawler. Затем вернитесь в веб-интерфейс и запустите задачу сканирования.

Задача 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом. Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную. Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задача 6: РЕШЕНИЕ

Не делайте. Автор не знает как это сделать так, чтобы оно работало.

Задача 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должны удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Дополнительная информация сертификатов должна включать в себя:

- Страна: RU
- Город: Moscow
- Компания (и иные дополнительные поля): demo lab
- Отдел: IT
- Почтовый адрес: из домена demo.lab
- Пароли ключей (если применимо): xxXX1122 Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли IWTM.

В случае невозможности это сделать, установить сертификат на машину

домена и отобразить это в отчете.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты»

Содержимое команд по генерации ключей и сертификатов в текстовом файле «сертификаты.txt» на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т. п.

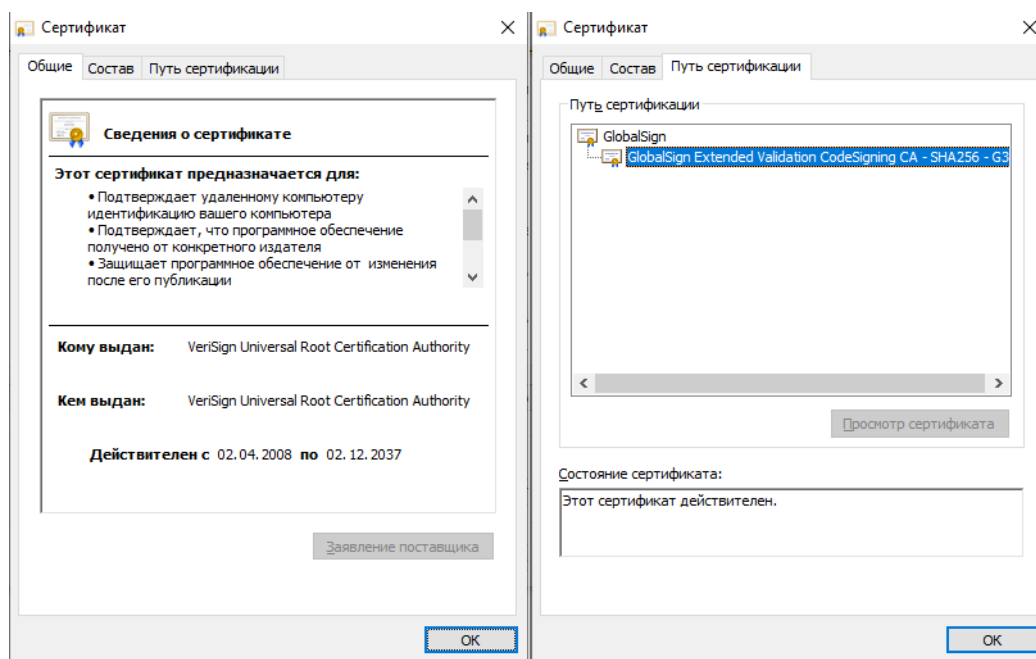


Рис1. Пример скриншотов задания

Задача 7: РЕШЕНИЕ

Обнаружьте файл `f` и `cert.sh`, который располагается по следующей ссылке <https://github.com/ragevna/F7/>.

Загрузите или скопируйте/перенесите файл на виртуальную машину IWTM.

Загрузить файлы напрямую на виртуальную машину можно с помощью команд:

```
curl https://raw.githubusercontent.com/ragevna/F7/main/cert.sh >> cert.sh
```

В файле `cert.sh` в соответствии с заданием измените переменные `C` (страна), `ST` (город), `L` (Область), `O` (организация), `pass` (пароль), `EMAIL` (электронная почта).

Затем установите возможность выполнения файла **`cert.sh`** с помощью команды **`chmod +x certs.sh`**. И выполните его с помощью команды **`./certs.sh`**. После выполнения скрипта в папке `ca` появятся новые файлы, однако нас интересует файл `bundle.pfx`, который необходимо передать на виртуальную машину `demo.lab`. Для этого перейдите к виртуальной машине `demo.lab` откройте Powershell с правами администратора и введите следующую команду **`scp root@<IP-адрес IWTM>:/ca/bundle.pfx C:/Share`**. Введите пароль от пользователя `root`, а затем перейдите к папке `C:/Share` на сервере `demo.lab` и дважды кликните на файл `bundle.pfx`. После чего начнется импорт сертификатов.

В качестве расположения хранилища выберите «Локальный компьютер».

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☐ Текущий пользователь

☒ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

Рисунок 34 - Мастер импорта сертификатов

Утвердите расположение сертификата, введите пароль от сертификатов, который указан в переменной `pass` в скрипте `certs.sh`. В качестве параметров импорта отметьте галочку “Включить все расширенные свойства”.

Защита с помощью закрытого ключа

Для обеспечения безопасности закрытый ключ защищен паролем.

Введите пароль для закрытого ключа.

Пароль:

xxXX1234

☒ Показывать пароль

Параметры импорта:

☐ Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.

☐ Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.

☐ Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)

☒ Включить все расширенные свойства.

Рисунок 35 – Защита с помощью закрытого ключа

В качестве хранилища сертификатов отметьте радиобокс “поместить все сертификаты в следующее хранилище”, а хранилище “Доверенные корневые центры сертификации”.

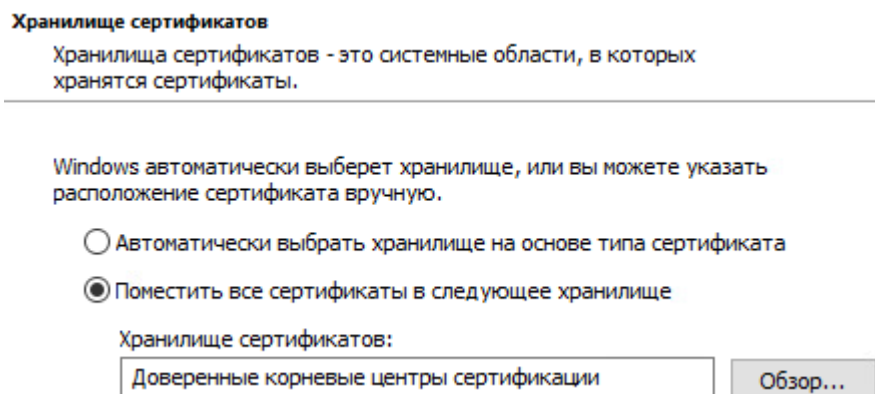


Рисунок 36 – Хранилище сертификатов

Согласитесь со всем, завершите импорт. Закройте Google Chrome и обратитесь к IWTM из браузера одним из следующих путей:

1. по имени iwtm/ в Google Chrome;
2. по имени iwtm.demo.lab/ в Google Chrome;
3. по IP-адресу в Google Chrome;

Если рядом с адресом сайта появится закрытый замочек – задание выполнено.