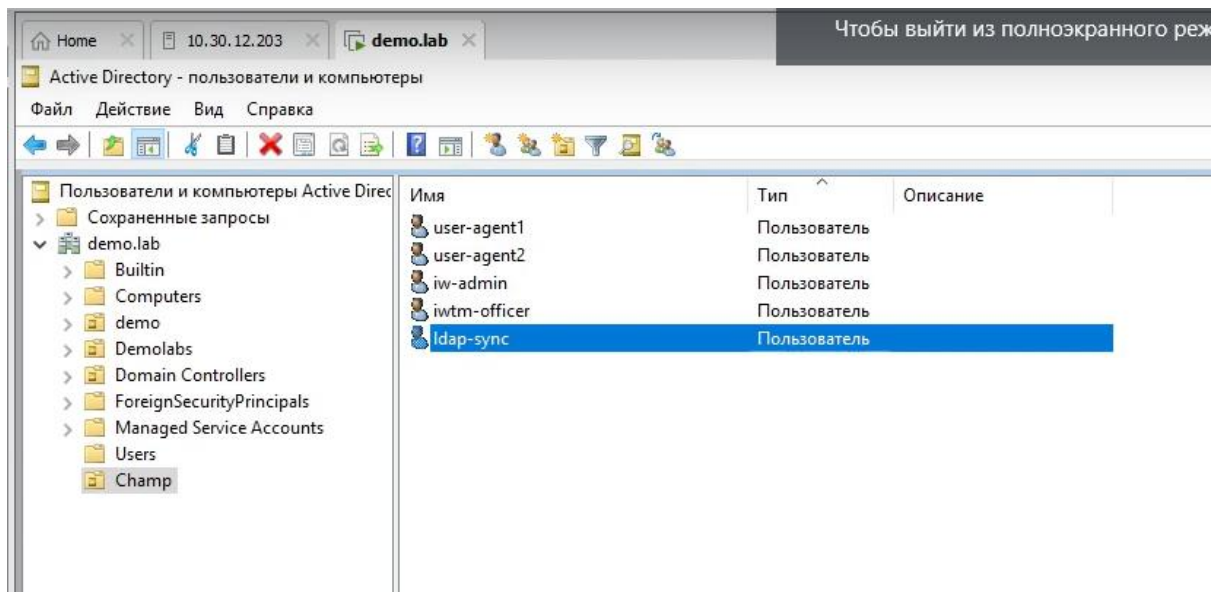
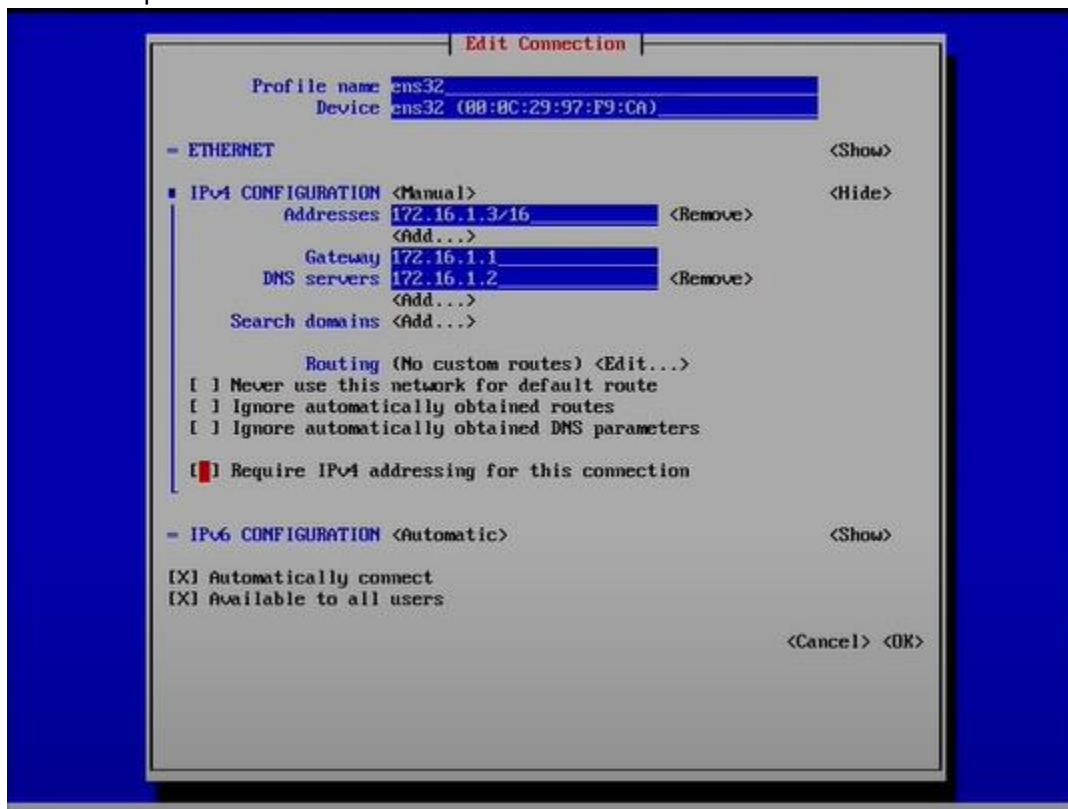


Задание 1

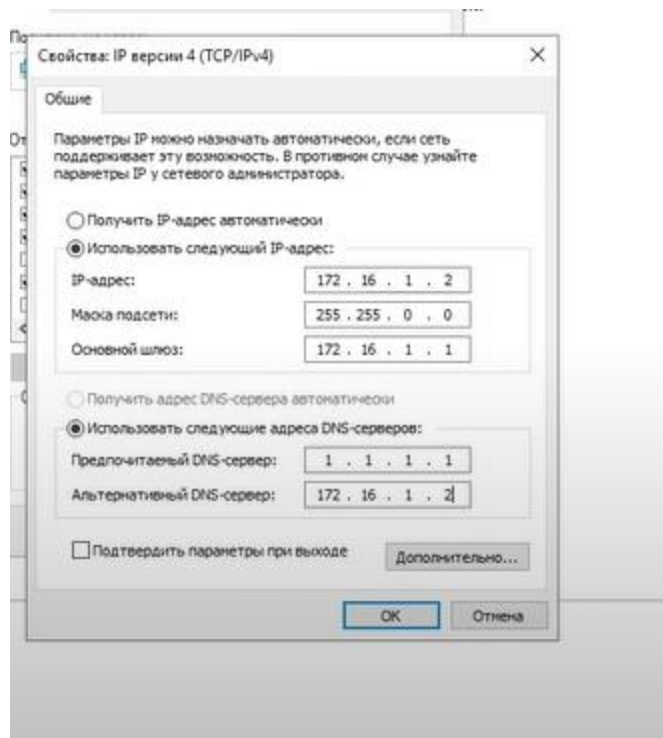


Вместо champ, company выдасть Domain Admins, и просто Admin

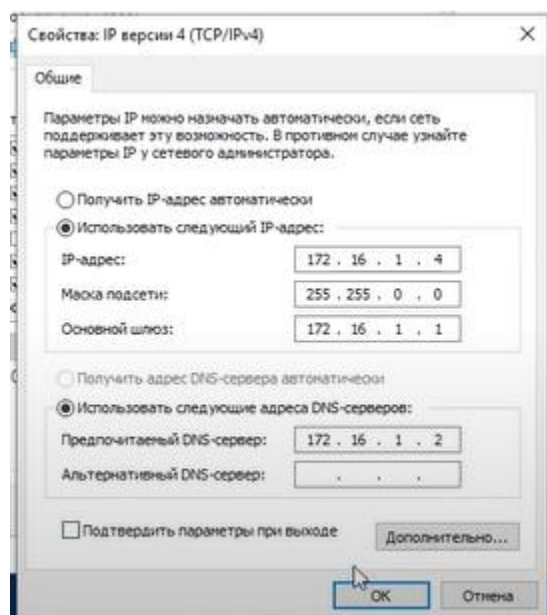
Поменять ip IWTM



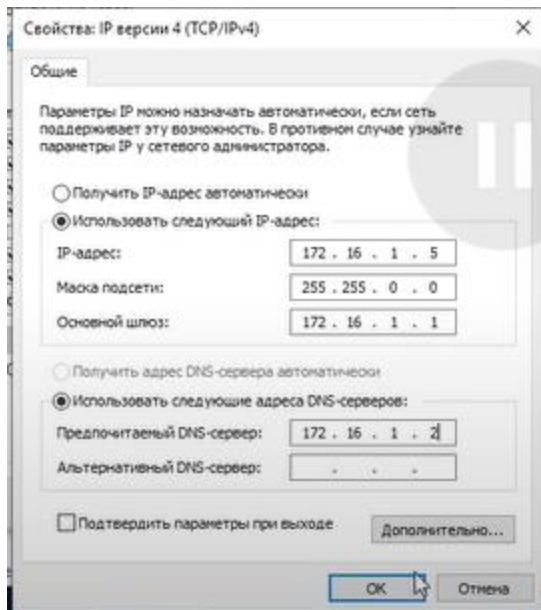
Demo.lab



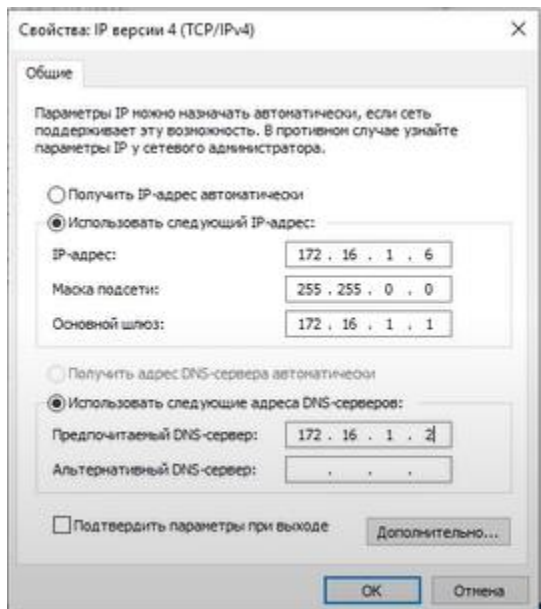
IWDM



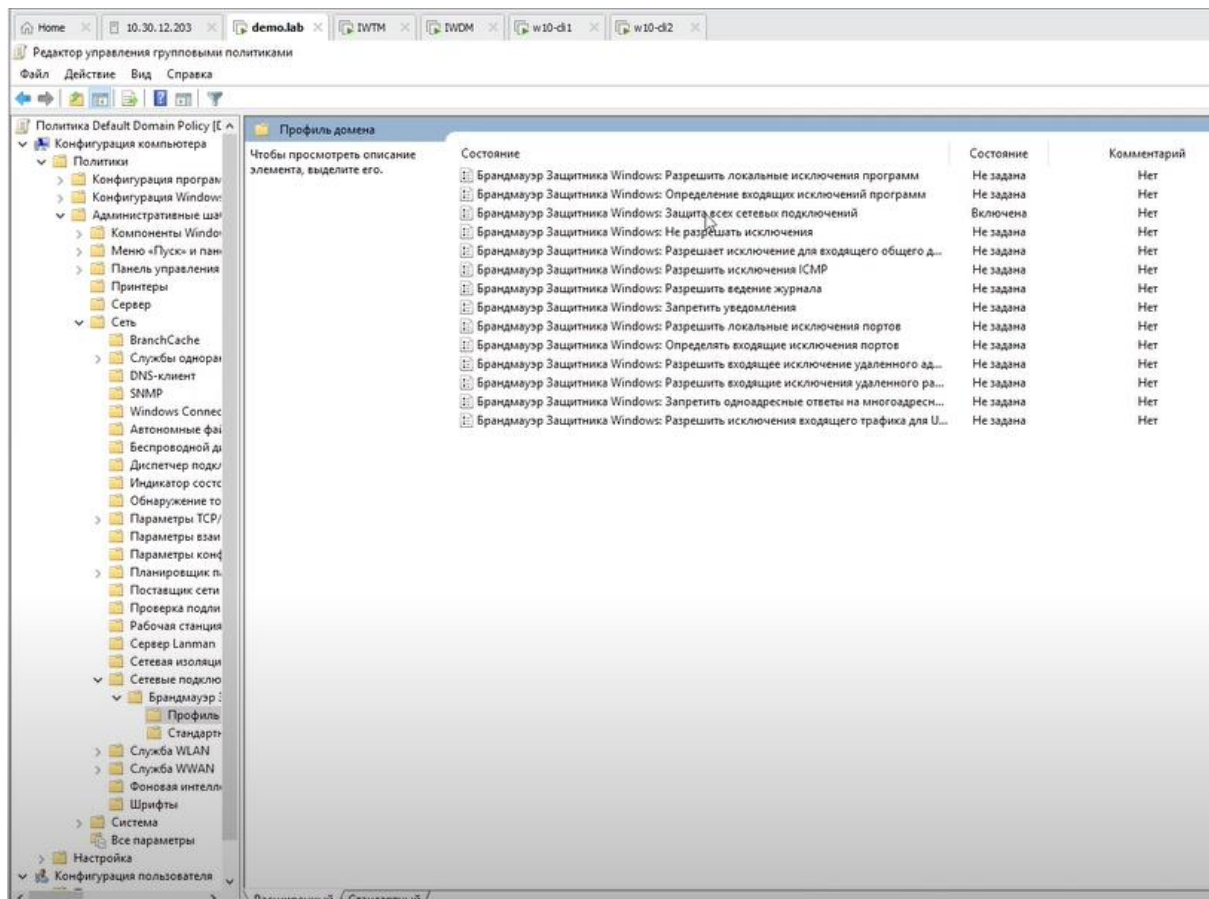
CLI 1



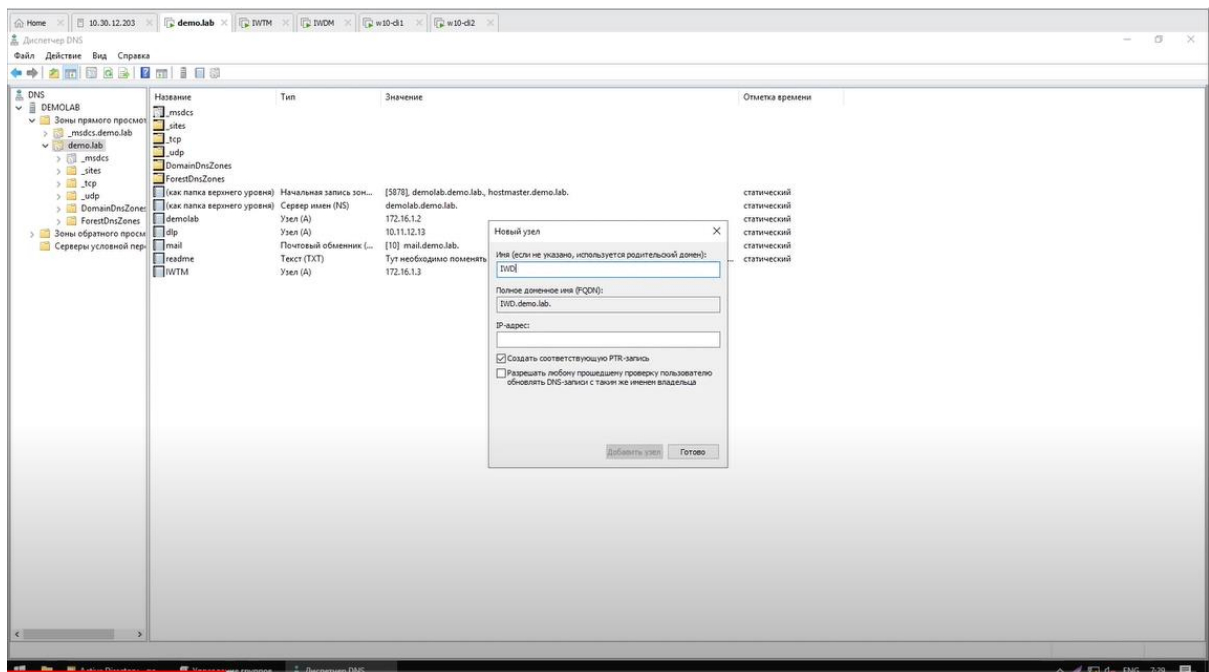
CLI 2



Отключить брандмауэр



Добавить все машины в днс



Подключить все машины в домен

Со своими пользователями

IWDM-Monitor admin

Cli – user agent

Ldap sync -sync user

lwtm admin – dlp-admin

Задание 2.

Далее через демолаб заходим в инфовоч

Логин офицер

Управление>LDAP

Добавление LDAP-сервера

Имя сервера	<input type="text" value="demo.lab"/>
Тип сервера	<input type="text" value="Active Directory"/>
Синхронизация	<input checked="" type="button" value="Автоматическая"/> <input type="button" value="Ручная"/>
Период синхронизации	<input type="text" value="Ежесекундно"/>
Повторение	<input type="text" value="15"/> <input type="button" value="↑"/> <input type="button" value="↓"/> минут

Настройки соединения

LDAP-сервер	<input type="text" value="172.16.1.2"/>
Использовать глобальный каталог	<input checked="" type="checkbox"/>
LDAP-запрос	<input type="text" value="dc=demo, dc=lab"/>
Анонимный доступ	<input type="checkbox"/>
Логин	<input type="text" value="ldap-sync"/>
Пароль	<input type="password" value="....."/>
<input checked="" type="button" value="Сохранить"/> <input type="button" value="Проверить соединение"/> <input type="button" value="Отменить"/>	

Другой пользователь

Управление>управление доступом

Пользователи>плюсик и dlp admin добавить

Редактирование пользователя

Логин:

Статус:

Эмэйл:

Полное имя:

Роли:

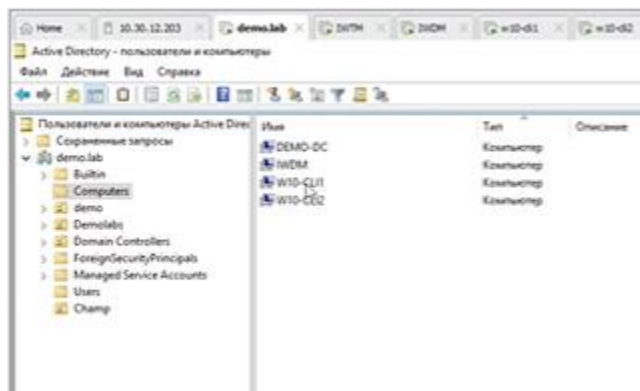
Области видимости:

Описание:

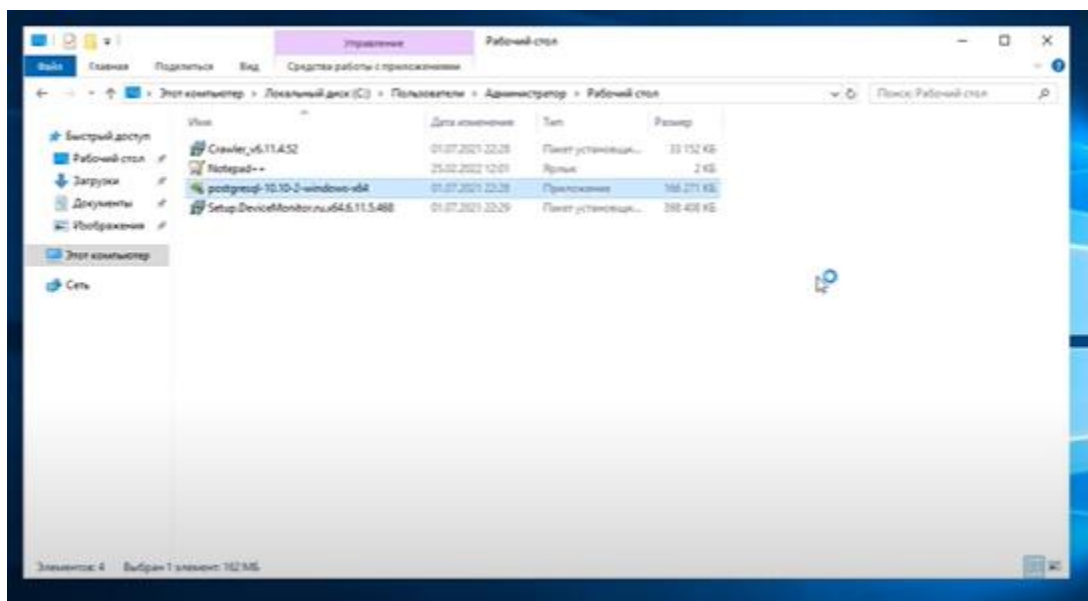
Создано: 13.05.2022, 04:40 — Изменено: 13.05.2022, 04:40

Создать txt файл и сохранить со всей инфой

Задание 3



Перекинуть ПК в подразделение



Зайти на рабочий стол админа где лежат установщики IWDM

И установить постгрес

Но сначала надо что бы установился вижуал

Установка

NEXT

Все галочки кроме стак билдинга

Next

Пароль xxXX1234

Next

Next

Next

Next до установки

Finish

Установка девайс монитора так же через рабочий стол админа

Везде далее, подключаем постгрес

Установка InfoWatch Device Monitor 6.11.5.468

Установка или обновление базы на PostgreSQL

Определение параметров новой или обновляемой базы

Введите имя существующего сервера баз данных и имя новой или обновляемой базы данных. Введите имя и пароль учётной записи PostgreSQL, имеющей права на создание баз.

Сервер БД:
localhost

Имя базы данных:
iwdm

Имя пользователя:
postgres

Пароль:
....

Назад Далее Отмена

Пароль xx

Далее

Создать ключ

Сохранить на рабочий стол

Установка InfoWatch Device Monitor 6.11.5.468

Учётная запись администратора сервера

Укажите учётную запись Администратора сервера Device Monitor

Учётная запись администратора сервера определяет пользователя сервера Device Monitor, которому будет присвоена роль «суперпользователь»

Администратор сервера

Имя пользователя:

Пароль:

Подтверждение пароля:

Назад Далее Отмена

Dlr админ с паролем иксы

Получить токен

Логинимся под монитором или какой там с фул доступом

Управление > плагины > Device monitor > Токены

Что бы не было конфликтов создать новый токен

Установка InfoWatch Device Monitor 6.11.5.468

Настройка соединения с Traffic Monitor

Определение параметров соединения с Traffic Monitor

Адрес соединения с ТМ должен иметь вид: host или host:port

Настройки соединения с ТМ

Адрес сервера ТМ:

Количество соединений:

Токен авторизации

☐ Работать в автономном режиме

☐ Сохранять теневые копии

Назад Далее Отмена

Установить

Далее после установки запустить

Локал хост

ДЛП админ и иксы

Что бы не было всякой возни надо сделать модуль 2!

Создаём новую политику рулес

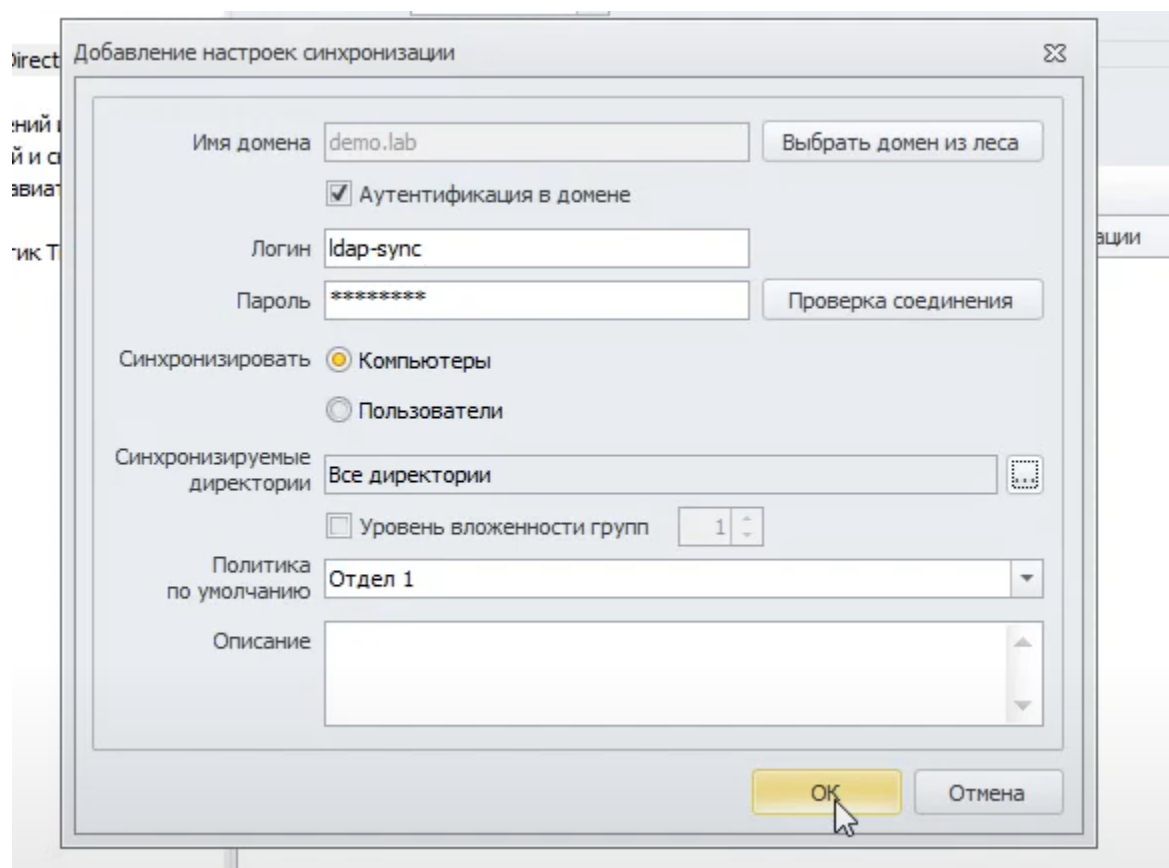
Создаём новую группу компани

Далее сохранить

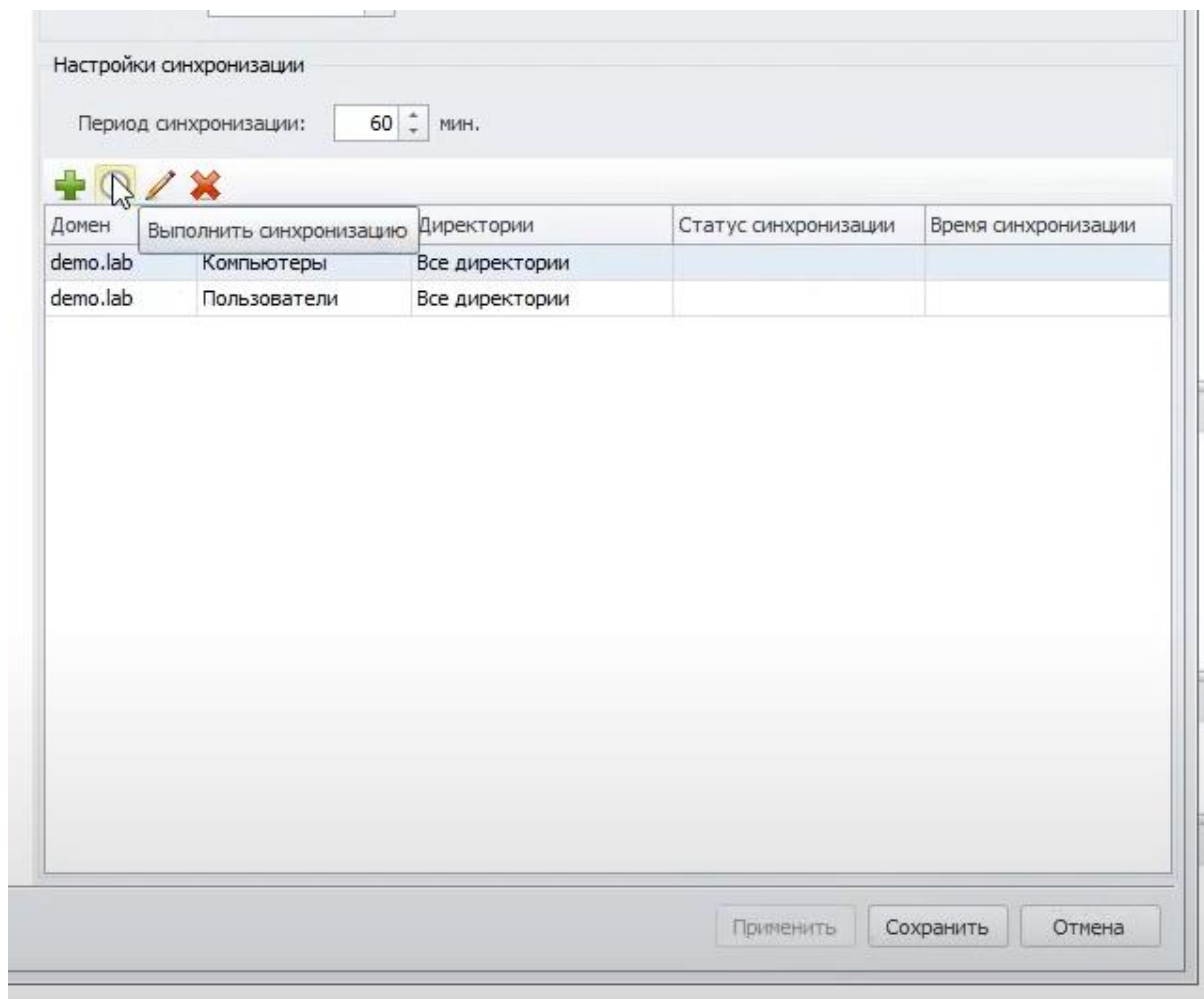
Инструменты > настройка> Интеграция с адешкой

172.16.1.2

389



Так же пользователей



И запустить это всё

Задание 4.

Зайти на клиента

Брэндмаур отключён ещё до этого
но можно ещё создать входящее правило
для порта
все локальные порты
далее
далее
название любое

Исходящее тоже самое


Потом включить сетевое обнаружение на клиенте и вdm
так же создать правила такие же на вdm

Дальше дивайс монитор, создать новую задачу

Название рандом
далее
выбрать клиент один

На шаге 5

Мастер создания задачи

 **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:


Шаг 5 из 7

< Назад **Далее >** Отмена

Указать пользователя из задания

Шаг 6

Мастер создания задачи Σ

 **Укажите параметры перезагрузки**

Ожидать перезагрузки без уведомления сотрудника: ☒ Не ожидать
☐ Ожидать час(ов)
☐ Ожидать бесконечно

Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки: ☒ Не уведомлять
☐ Уведомлять в течение час(ов) каждые минут(ы)
☐ Уведомлять бесконечно каждые минут(ы)

Текст уведомления:

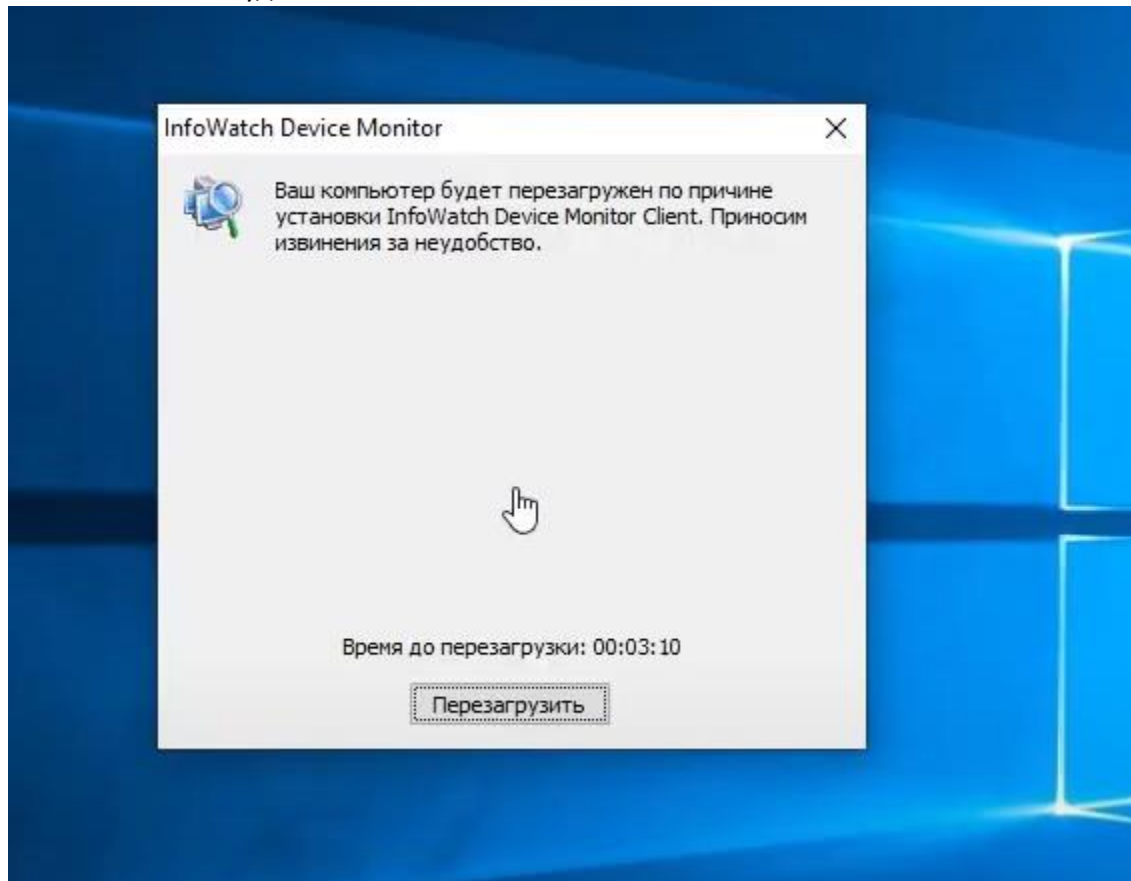
☒ Показать предупреждение перед принудительной перезагрузкой

Шаг 6 из 7

< Назад Далее > Отмена

Далее , готово.

После того как всё удачно на клиенте появится такое окно



После этого задание 4 всё

Модуль 2.

Первое задание сделали выше

Задача 2: смена пароля удаления агента

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: xxXX1234

Зафиксировать выполнение скриншотом.

Это надо делать методом тыка потому что нету гайда

Правило 1 и так же аналогично с локальным принтером

Создание правила

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Тип устройства:

Доступ

☒ Использование запрещено

Правило 2 Тут чисто под своё подгоняем

Создание правила ☒

Наименование:

Перехватчик:

Правило применяется на ОС: Windows, Astra Linux

Настройки доступа к облачным хранилищам

Название	Доступ разрешен	Доступ запрещен	Только скачивание
Google Drive	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
DropBox	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
YandexDisk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
OneDrive	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
EverNote	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SugarSync	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Настройки теневого копирования файлов, отправляемых в облачные хранилища

☒ Включить теневое копирование

☒ Минимальный размер файла для создания события: Кб

☒ Максимальный размер теневой копии: Кб

☒ Действует всегда

Действует с:

По:

Что бы сделать 3е правило надо создать список приложений, для этого в оснастке приложения создать список

Добавить приложение Σ3

Описание: ✖ mspaint.exe

Описание и тип отображаются в списке. Сравнение по этим атрибутам не выполняется

Выберите атрибуты, по которым будет проверяться соответствие приложений:

☒ Только по имени приложения

☐ По подробной информации

☐ По расположению

Имя приложения: mspaint.exe

Туда закинуть наши приложения

И потом добавить список в правило

Создание правила


Наименование:


Перехватчик:

Правило применяется на ОС: Windows

Запрет запуска приложений

☒ Запретить запуск приложений с использованием списков


Белые списки (неактивны) 
Запрет всех приложений, кроме указанных в списке

Черные списки (активны) 
Блокируются приложения из списка


Смена режима белые/черные списки [здесь](#)

Запрет буфера обмена

☐ В терминальной сессии между разными рабочими станциями (для любых приложений)

☐ В приложениях из списка 

Запрет печати

☐ В приложениях из списка 

Тип принтера

- ☒ Локальный
- ☒ Сетевой
- ☒ Терминальный

☒ Действует всегда

Действует с:

По:

Сохранить Отмена

Правило 4

По той же схеме делаем список с запретными приложениями закидываем его в правило

Создание правила

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Запрещать сотруднику создавать снимок экрана

☐ Всегда

☒ Если запущены приложения:

☒ Действует всегда

Действует с:

По:

Правило 5

Создание правила

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Тип устройства:

Доступ

☒ Нет доступа

☐ Только чтение

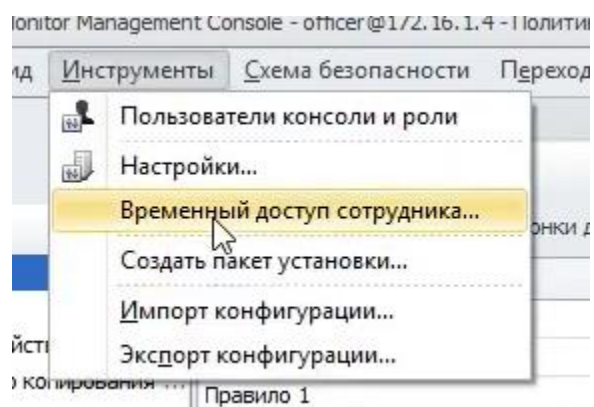
☐ Использование разрешено

☒ Действует всегда

Действует с:

По:

Правило 6



Всё по дефолту потом тут ставить 120 минут – 2 часа для тупых

Временный доступ сотрудника

✕

Учетная запись:

Введите значение для поиска...

▼

Тип устройства:

Флоппи-дисковод

▼

Код запроса:

Время доступа:

30 минут

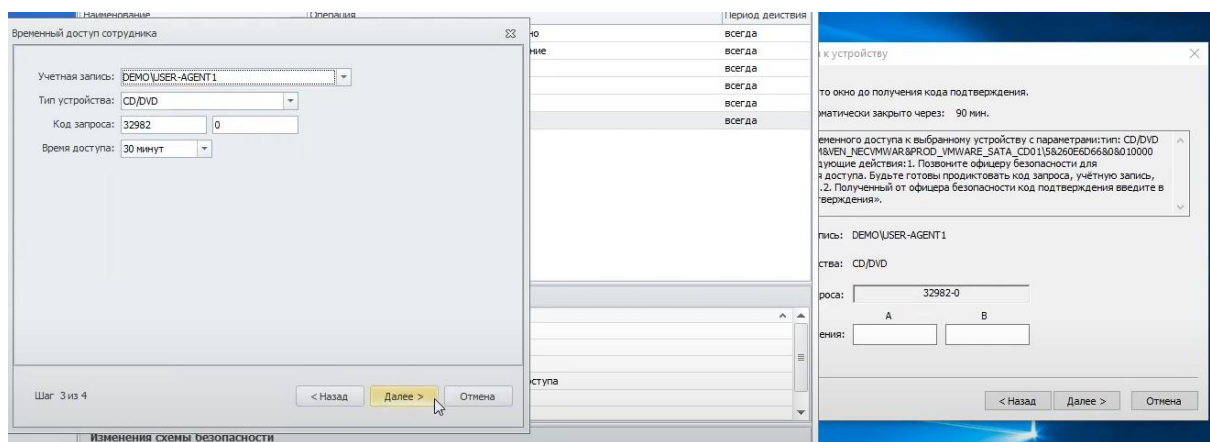
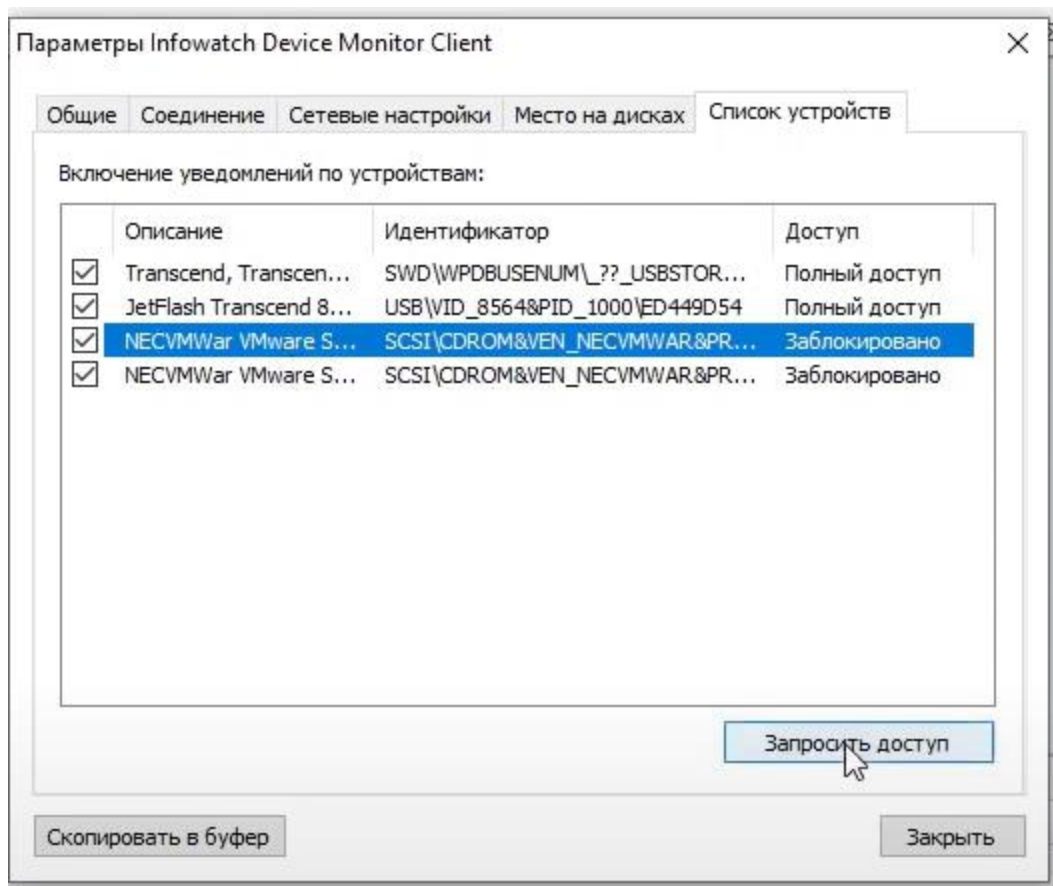
▼

Шаг 3 из 4

< Назад

Далее >

Отмена



Правило 7

Создание правила

Наименование: Новое правило автоматического создания снимков экрана

Перехватчик: ScreenShot Monitor

Правило применяется на ОС: Windows

Автоматически создавать снимок экрана:

☒ Всегда

☐ Если активны приложения:

Снимок экрана будет создаваться при смене активного окна, либо каждые 60 сек.

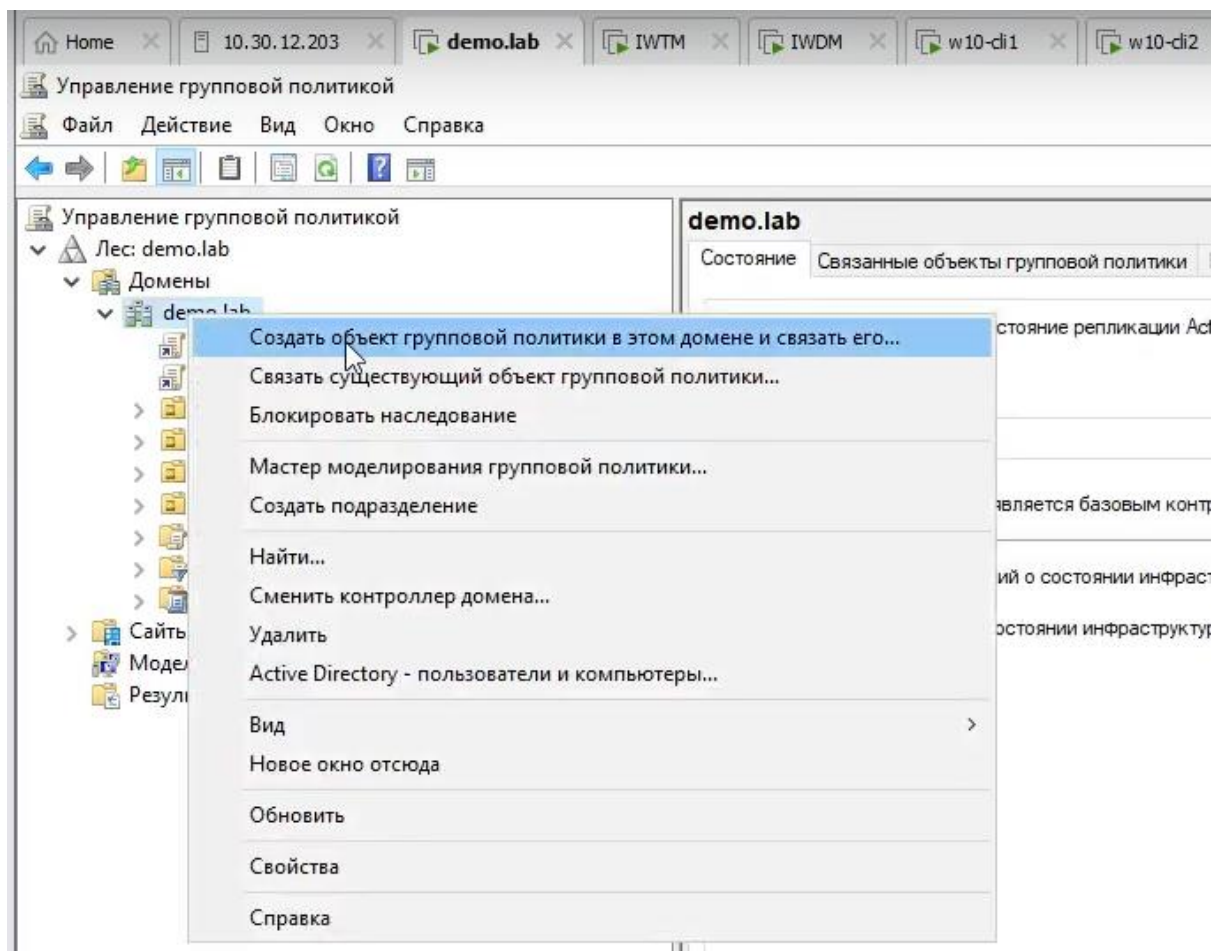
☒ Действует всегда

Действует с:

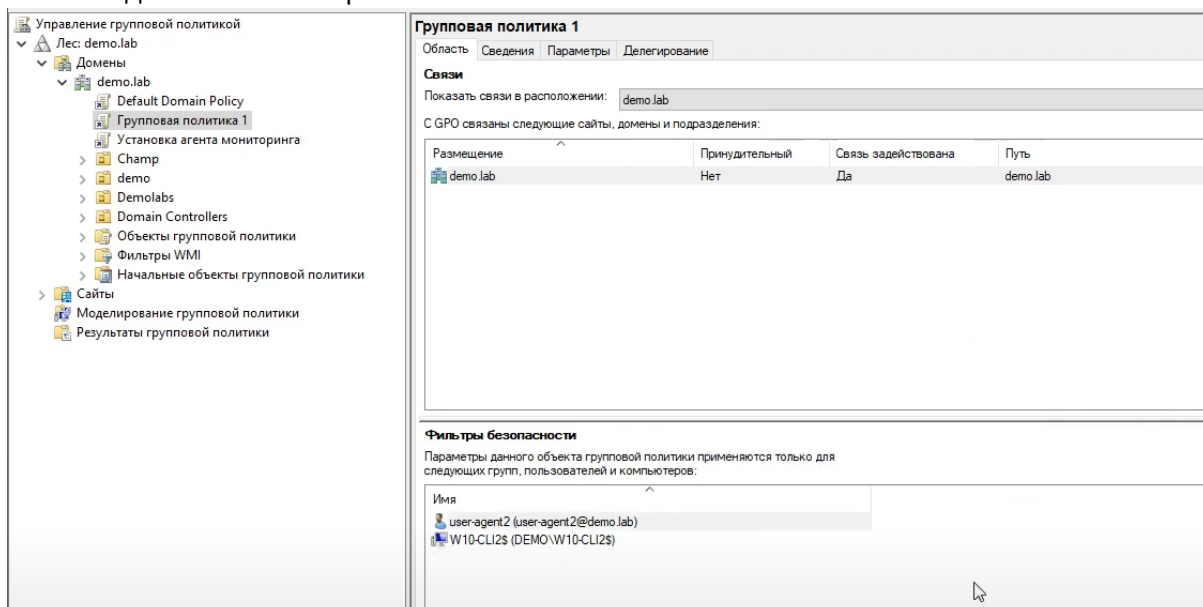
По:

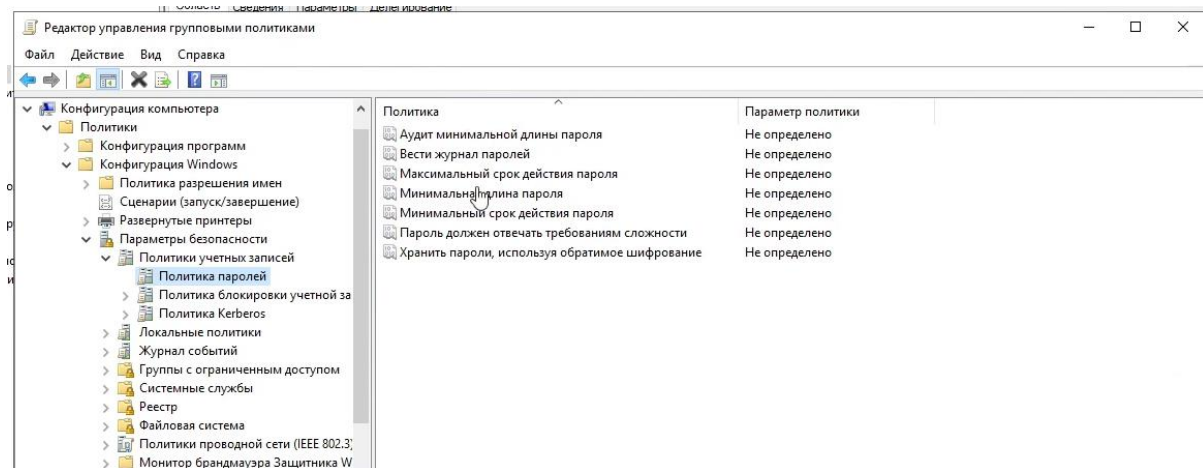
Тут только браузер поставить

гпо



Потом надо её вот так настроить



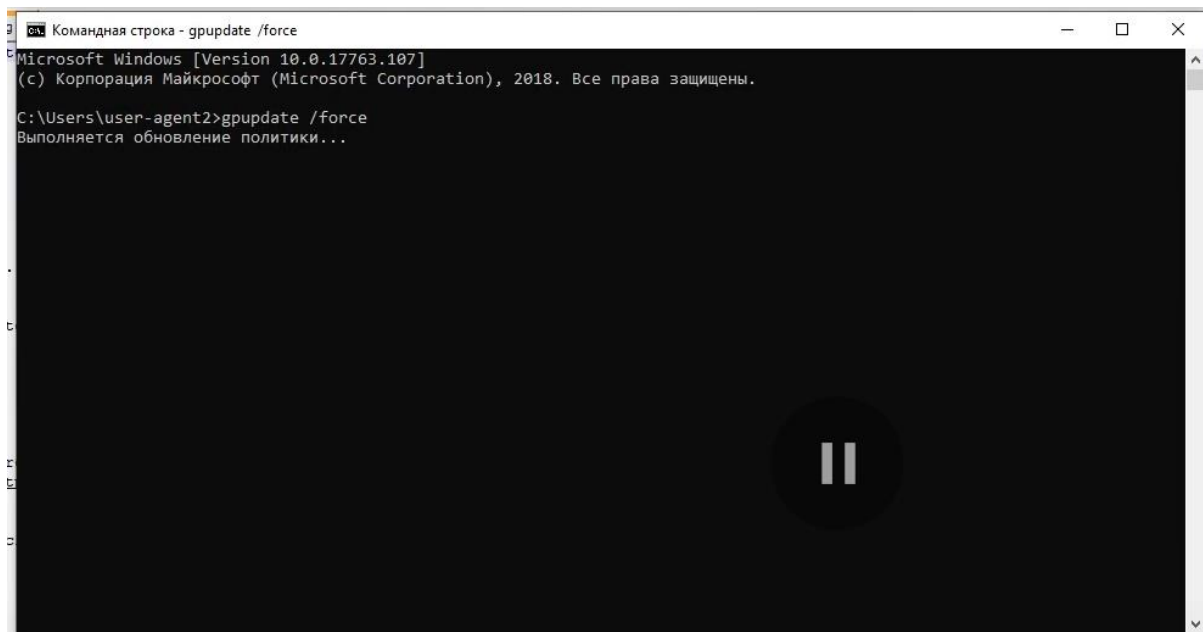


Тут всё по заданию

Потом создать ещё одну политику 2

Так же 3 и 4

Ну там можно нагуглить



Потом сделать вот так на клиенте

Конец кто долистал мужик