Задание 3: Развертывание DLP уровня хоста. InfoWatch Device Monitor

Задание 3. Установка и настройка IWDM

Контекст

В «песочнице» необходимо развернуть систему контроля рабочих станций InfoWatch Device Monitor (IWDM). Требуется установить базу данных PostgreSQL на отдельную ВМ, развернуть сервер IWDM, интегрировать его с контроллером домена Active Directory, синхронизировать данные с InfoWatch Traffic Monitor и удаленно установить агент Device Monitor на ПК нарушителя `IW-CLI`.

Задача

1. Создать ВМ `IWDM-DB`.
2. Установить базу данных PostgreSQL на машину `IWDM-DB`.
3. Установить Сервер `IWDM` на машину `IWDM`.
4. Установить InfoWatch Device Monitor Agent на ПК `IW-CLI` нарушителя путем удаленного распространения через задачи в Device Monitor. Зафиксировать скриншотами.
5. Выполнить синхронизацию с `IWTM`. Осуществить интеграцию сервера безопасности `IWDM` с Active Directory. Необходимо синхронизировать каталог компьютеров и пользователей. Зафиксировать скриншотами.

Термины

Термин	Пояснение
IWDM	InfoWatch Device Monitor — система контроля рабочих станций и устройств (USB, принтеры, сеть)
IWDM-DB	Сервер базы данных для InfoWatch Device Monitor
Device Monitor Agent	Программный агент, устанавливаемый на рабочие станции для контроля
Консоль IWDM	Приложение для администрирования Device Monitor (обычно устанавливается на Windows-машину администратора)

Параметры

Параметр	Значение
IP-адрес IWDM	`192.168.88.104`
IP-адрес IWDM-DB	`192.168.88.105`
IP-адрес IWTM-Web	`192.168.88.101`
IP-адрес Контроллера AD	`192.168.88.100`
Логин администратора AD	`admin-dm`
Пароль администратора AD	`xxXX4321`

Решение

Шаг 1. Подготовка ВМ IWDM-DB и IWDM

Что нужно сделать

Настроить сеть, перенести файл `hosts` с `demolab`, задать имена хостов, настроить репозитории и подготовить файлы установщика на обеих ВМ.

Ход работы

1. Настраиваем сеть и файл hosts

На ВМ `IWDM-DB` и ВМ `IWDM` запустите утилиту настройки сети:

```
nmtui
```

Укажите статический IP-адрес (`.105` для БД и `.104` для сервера), шлюз и DNS-сервер (`192.168.88.100`). Сохраните настройки.

Затем с рабочего стола `demolab` через WinSCP перекиньте заранее подготовленный файл `hosts` в домашнюю директорию пользователя (`/home/officer/`) на обе ВМ. После этого скопируйте его в системную папку:

```
sudo cp /home/officer/hosts /etc/hosts
```

2. Задаем имена хостов

Измените имя хоста на каждой машине в файле `/etc/hostname`:

```
sudo nano /etc/hostname
```

- На ВМ DB: `iwdmdb`
- На ВМ Сервер: `iwdm`

Перезагрузите машины:

```
sudo reboot
```

3. Настройка репозиториев и базовых пакетов

Откройте файл `/etc/apt/sources.list` на каждой ВМ и убедитесь, что подключены официальные репозитории Astra Linux и InfoWatch. Затем обновите список пакетов:

```
sudo apt update
sudo apt install chrony open-vm-tools -y
```

4. Подготовка файлов установщика

Через WinSCP перекиньте архив с установщиком IWDM и файл лицензии на ВМ `IWDM` (в домашнюю директорию `officer`).

Создайте папку в корне системы, перенесите туда файлы и распакуйте архив:

```
sudo mkdir /dist
sudo cp /home/officer/название_архива_IWDM.zip /dist/
cd /dist
sudo unzip название_архива_IWDM.zip
```

Важно: выдайте права на исполнение зеленому файлу установщика (используйте **Tab** для автодополнения названия):

```
sudo chmod +x iwdm-installer-<TAB>
```

Шаг 2. Установка Базы Данных (ВМ IWDM-DB)

Что нужно сделать

Установить СУБД PostgreSQL.

Ход работы

На ВМ `IWDM-DB` установите сервер PostgreSQL 11 и необходимые утилиты:

```
sudo apt install postgresql postgresql-11 postgresql-client-11 chrony -y
```

Проверьте, что служба запущена:

```
sudo systemctl status postgresql
```

Шаг 3. Установка Сервера IWDM (ВМ IWDM)

Что нужно сделать

Развернуть сервер Device Monitor.

Ход работы

Запустите установщик из папки `/dist`:

```
sudo ./iwdm-installer-<TAB>
```

Следуйте инструкциям мастера установки. При выборе роли компонента укажите **Сервер Device Monitor** (Server). В качестве адреса базы данных укажите IP-адрес ВМ `IWDM-DB` (`192.168.88.105`).

По завершении установки проверьте статус служб:

```
sudo systemctl status iwdm
```

Шаг 4. Подключение консоли и интеграция с AD

Что нужно сделать

Подключиться к серверу с помощью консоли IWDM (обычно это клиентское приложение на Windows), интегрировать сервер с Active Directory и IWTM.

Ход работы

1. Подключение к серверу

Запустите консоль **InfoWatch Device Monitor** на вашей машине администратора (Windows). В окне подключения укажите IP-адрес сервера IWDM (`192.168.88.104`) и учетные данные администратора.

Рисунок 1. Окно подключения к серверу IWDM.

2. Интеграция с Active Directory

В дереве консоли перейдите в раздел **Сервер -> Службы -> Active Directory**.

Укажите параметры подключения:

- **Сервер:** `192.168.88.100`
- **Пользователь:** `admin-dm`
- **Пароль:** `xxXX4321`
- **Базовый DN:** `dc=demo,dc=lab`

Нажмите **Проверить соединение** и сохраните изменения. Теперь перейдите в раздел **Пользователи** и **Компьютеры** и запустите синхронизацию с AD.

Рисунок 2. Настройка интеграции с AD и запуск синхронизации.

3. Синхронизация с IWTM

Перейдите в раздел **Сервер -> Службы -> InfoWatch Traffic Monitor**. Укажите адрес сервера IWTM: `https://192.168.88.101`. Введите учетные данные (`officer` / `xxxX1234`).

После сохранения проверьте, что статус подключения — «Успешно». Перейдите в раздел **Компьютеры** и убедитесь, что данные синхронизировались.

Рисунок 3. Настройка интеграции с IWTM и статус успешного подключения.

Шаг 5. Удаленная установка агента на IW-CLI

Что нужно сделать

Распространить агент Device Monitor на ПК нарушителя через консоль управления.

Ход работы

1. Создание задачи на установку

В консоли IWDM перейдите в раздел **Задачи** и нажмите **Добавить задачу**. Выберите тип задачи: **Установка / обновление / удаление программы**.

Укажите имя задачи, например, `Install_DM_Agent`.

2. Настройка параметров установки

На шаге выбора программного обеспечения укажите **InfoWatch Device Monitor Agent**. На шаге выбора целевых компьютеров найдите ПК `astra-cli` (он должен быть в списке после синхронизации с AD/ALD Pro) и добавьте его.

Запустите задачу на выполнение (кнопка **Выполнить**). Дождитесь, пока статус задачи сменится на «Выполнено».

Рисунок 4. Создание задачи на установку агента и выбор ПК `astra-cli`.

Рисунок 5. Успешное завершение задачи по установке агента.

Как проверить

- ☐ На ВМ IWDM-DB установлена и запущена PostgreSQL
- ☐ На ВМ IWDM установлен и запущен Сервер Device Monitor
- ☐ Консоль IWDM успешно подключается к серверу
- ☐ В консоли IWDM настроена интеграция с Active Directory, списки пользователей и компьютеров синхронизированы
- ☐ Настроена интеграция IWDM с сервером IWTM
- ☐ Задача на установку агента на ПК `astra-cli` успешно выполнена
- ☐ В консоли IWDM во вкладке «Компьютеры» ПК `astra-cli` отображается с активным агентом

Если что-то не работает

Проблема	Что делать
Не подключается консоль IWDM	Проверить статус служб на сервере (`systemctl status iwdm`), проверить доступность портов
Ошибка при интеграции с AD	Проверить правильность логина, пароля и Base DN (`dc=demo,dc=lab`). Убедиться, что ВМ IWDM видит контроллер домена
Задача на установку агента «Зависла»	Проверить, включен ли ПК `astra-cli`, доступен ли он по сети и не блокирует ли его брандмауэр

Проблема	Что делать
Агент не устанавливается	Проверить, что в IWDM добавлен правильный дистрибутив агента и совпадают разрядности ОС

Revision #2
Created 2026-10-17 13:44:08 UTC by Admin
Updated 2026-10-17 13:44:46 UTC by Admin