4

Вот готовое **Задание 4. Развертывание InfoWatch Data Discovery**, оформленное строго по вашему шаблону и с учетом всех требований (пути `/home/officer/`, папка `/dist`, отключение блокировки Astra, использование токенов и настройка Samba).

Задание 4. Развертывание InfoWatch Data Discovery

Контекст

Для контроля общих сетевых ресурсов в организации необходимо развернуть компонент InfoWatch Data Discovery (IWDD) на виртуальную машину `IWDD`. Этот компонент позволяет сканировать сетевые папки и файловые хранилища на предмет наличия конфиденциальной информации, интегрируясь с основным сервером Device Monitor.

Задача

1. Создать и подготовить ВМ `IWDD`.
2. Установить Data Discovery и подключить его к мастер-узлу IWDM.
3. Зафиксировать конфигурацию через утилиту исправления.
4. Настроить интеграцию с сервером Traffic Monitor для передачи событий.
5. Создать общую сетевую папку на клиенте для тестирования.
6. Настроить задачу сканирования в веб-консоли IWDM.

Термины

Термин	Пояснение
IWDD	InfoWatch Data Discovery — модуль для поиска и контроля данных на файловых ресурсах
XAPI	Программный интерфейс, через который IWDD обменивается данными с Traffic Monitor

Термин	Пояснение
Samba	Пакет программ для организации доступа к сетевым папкам по протоколу SMB/CIFS
Мастер-узел	Главный сервер (в данном случае IWDM), управляющий кластером

Параметры

Параметр	Значение
IP-адрес IWDD	`192.168.88.105`
IP-адрес IWDM (мастер-узел)	`192.168.88.104`
IP-адрес IWTM-Web	`192.168.88.101`
IP-адрес astra-cli	`192.168.88.31`
Логин администратора IWDM	`officer`
Пароль администратора IWDM	`xxxX1234`

Решение

Шаг 1. Подготовка ВМ IWDD

Что нужно сделать

Настроить сеть, перенести файл `hosts`, задать имя хоста, настроить репозитории и подготовить файлы установщика.

Ход работы

1. Настраиваем сеть и файл hosts

На ВМ `IWDD` запустите утилиту настройки сети:

```
nmtui
```

Укажите IP-адрес `192.168.88.105`, шлюз и DNS-сервер (`192.168.88.100`). Сохраните настройки.

С рабочего стола `demolab` через WinSCP перекиньте файл `hosts` в домашнюю директорию (`/home/officer/`) и скопируйте его в системную папку:

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

Задайте имя хоста:

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

Впишите `iwdd` и перезагрузите машину:

```
sudo reboot
```

2. Установка базовых пакетов и настроек Astra

Обновите пакеты и установите необходимые утилиты:

```
sudo apt update
sudo apt install conntrack socat dotnet6 chrony open-vm-tools -y
```

> ⚠ **Важно!** На Astra Linux необходимо отключить защиту от изменения прав файлов, иначе установщик не сможет корректно развернуть компоненты:
>
> ```
> sudo astra-nochmodx-lock disable
> ```

3. Подготовка файлов установщика

Через WinSCP перекиньте архив с Data Discovery (например, `iu_discovery_setup_2.0.0.tar.xz`) и лицензию на ВМ в домашнюю директорию.

Создайте папку в корне и распакуйте установщик:

```
sudo mkdir /dist
sudo cp /home/officer/iu_discovery_setup_2.0.0.tar.xz /dist/
cd /dist
sudo tar -xf iu_discovery_setup_2.0.0.tar.xz
sudo chmod +x setup.py
```

Шаг 2. Установка Data Discovery

Что нужно сделать

Запустить установщик и подключить компонент к IWDM.

Ход работы

1. Запускаем установщик

```
sudo ./setup.py install --mode=office --productmode=central
```

2. Настройка подключения

Следуйте инструкциям на экране. Вас попросят принять лицензию (введите `y`).

Далее установщик запросит:

- **The address of Product master node:** введите IP-адрес IWDM (`192.168.88.104`).
- **Token to connect to Product master node:** введите токен для подключения.

> **Как получить токен:** Токен генерируется на мастер-узле. Зайдите на ВМ `IWDM`, откройте терминал и выполните команду, указанную в документации (или найдите его в веб-интерфейсе IWDM в разделе добавления новых узлов). Скопируйте полученную строку и вставьте в установщик IWDD.

Рисунок 1. Процесс установки Data Discovery и ввод адреса мастер-узла.

Дождитесь завершения установки.

Шаг 3. Фиксация конфигурации (Fix n.yaml)

Что нужно сделать

Применить изменения конфигурации на сервере IWDM, чтобы он увидел новый узел.

Ход работы

Перейдите на ВМ **IWDM** (`.104`). Запустите установщик IWDM еще раз:

```
cd /dist
sudo ./setup.sh
```

В меню выберите:

- **Installation type:** `Utilities`
- **Select utility:** `Fix n.yaml file`

Введите текущий IPv4-адрес вашей машины (по умолчанию `192.168.88.104`).

Рисунок 2. Запуск утилиты Fix n.yaml на сервере IWDM.

После успешного применения зайдите в веб-консоль IWDM. В разделе **Состояние системы** должен появиться новый сервер `iwdd (iwdd)` со статусом **Ready**.

Рисунок 3. Статус системы в IWDM: узел iwdd успешно добавлен.

Шаг 4. Интеграция IWDD с IWTM

Что нужно сделать

Связать Data Discovery с Traffic Monitor для передачи найденных файлов.

Ход работы

1. Получаем токен в IWTM

В веб-консоли IWTM перейдите в **Еще -> Плагины**. Найдите **InfoWatch Data Discovery**, перейдите на вкладку **Токены** и скопируйте токен (например, `Token-2`).

Рисунок 4. Раздел плагинов IWTM с токеном для Data Discovery.

2. Настраиваем интеграцию в IWDM

В веб-консоли IWDM перейдите в **Настройки системы -> Зоны и серверы**. В блоке **Экспорт данных в Traffic Monitor**:

- **Адрес XAPI:** `192.168.88.101`
- **Токен:** вставьте скопированный токен.

Нажмите **Проверить соединение** (должно быть успешно) и **Применить**.

Рисунок 5. Настройка экспорта данных XAPI в веб-консоли IWDM.

Шаг 5. Настройка общей сетевой папки (Samba)

Что нужно сделать

Создать папку на клиенте `astra-cli` для тестирования сканера.

Ход работы

Зайдите на ВМ `astra-cli` и установите Samba:

```
sudo apt update && sudo apt install samba -y
```

Остановите службы, удалите старый конфиг и создайте папку:

```
sudo systemctl stop nmbd smbd
sudo rm -rf /etc/samba/smb.conf
sudo mkdir -p /srv/samba/shared
sudo chmod 777 /srv/samba/shared
```

Создайте новый конфигурационный файл:

```
sudo nano /etc/samba/smb.conf
```

Вставьте следующий текст:

```
[global]
   workgroup = WORKGROUP
   server string = Samba Server
   security = user
   map to guest = bad user

[shared]
   path = /srv/samba/shared
   browseable = yes
   read only = no
   guest ok = yes
   create mask = 0666
   directory mask = 0777
```

Сохраните файл и перезапустите службы:

```
sudo systemctl restart nmbd smbd
```

Скопируйте в папку `/srv/samba/shared` несколько тестовых файлов (картинки, тексты), чтобы Data Discovery мог их найти.

Рисунок 6. Тестовые файлы в общей папке Samba на клиенте.

Шаг 6. Создание задачи сканирования

Что нужно сделать

Настроить задачу в IWDM для сканирования созданной папки.

Ход работы

В веб-консоли IWDM перейдите в раздел **Хранение файлов** и нажмите **Создать**.

- **Название:** `test`
- **Выполнение задачи:** `Непрерывное`
- Поставьте галочку **Отправлять файлы на анализ в Traffic Monitor**.

Рисунок 7. Настройка параметров задачи сканирования.

Перейдите в настройки хостов для этой задачи и добавьте новый хост:

- **Адрес:** `192.168.88.31` (astra-cli)
- **Тип подключения:** `SMB`
- **Авторизация:** галочка «Наследовать из задачи» (гостевой доступ).

Рисунок 8. Добавление хоста (astra-cli) в задачу сканирования.

Запустите задачу. Через некоторое время в разделе **Информация о файлах** появятся найденные файлы с указанием пути и размера.

Рисунок 9. Результаты сканирования: найденные файлы в IWDM.

Как проверить

- ☐ На ВМ IWDD установлен компонент и выполнен `Fix n.yaml`
- ☐ В IWDM в разделе «Состояние системы» узел `iwdd` имеет статус **Ready**
- ☐ В IWDM настроен адрес XAPI (`192.168.88.101`) и токен от IWTM
- ☐ На клиенте (astra-cli) создана общая папка Samba с тестовыми файлами
- ☐ В IWDM создана задача сканирования (тип SMB) для клиента
- ☐ В разделе «Информация о файлах» отображаются просканированные файлы
- ☐ События от Data Discovery успешно передаются в Traffic Monitor

Если что-то не работает

Проблема	Что делать
Ошибка при установке DD	Проверить, выполнен ли `sudo astra-nochmodx-lock disable`
IWDD не появляется в кластере	Выполнить `Fix n.yaml` на IWDM, проверить сетевую доступность
Не проходит проверка соединения XAPI	Проверить правильность адреса IWTM и актуальность токена

Проблема	Что делать
Задача не находит файлы	Проверить, что службы Samba запущены на клиенте, а папка имеет права `777`
В событиях IWTM нет данных от DD	Проверить, что в задаче IWDM стоит галочка «Отправлять файлы на анализ в Traffic Monitor»

Revision #1
Created 2026-10-18 06:31:43 UTC by Admin
Updated 2026-10-18 06:33:10 UTC by Admin