Задание 2: Настройка IWTM

Задание 2. Настройка IWTM

Контекст

В «песочнице» необходимо развернуть DLP-систему InfoWatch Traffic Monitor (IWTM) в режиме распределенной установки для контроля сетевого трафика. Потребуется настроить четыре виртуальные машины: базу данных, веб-интерфейс с ICAP, индексатор и прокси-сервер, объединить их в кластер Consul и настроить перехват трафика.

Задача

1. Выполнить настройки репозитория, файла hosts для правильной установки IW TM.
2. Выполнить установку IW TM в режиме “разнесения компонентов” с настройками по-умолчанию:
   1. Донастроить ВМ IWTM-DB и выполнить установку Базы Данных IWTM.
   2. Выполнить установку компонентов Web, ICAP IWTM на ВМ IWTM-Web.
   3. Выполнить установку компонента Indexer IWTM на ВМ IWTM-Indexer.
   4. Выполнить установку Proxy Squid на машину Proxy.
3. Настроить перехват трафика и LDAP-синхронизацию.
4. Подтвердить скриншотами конфигурационные файлы и статус запущенных служб IWTM.

Термины

Термин	Пояснение
IWTM	InfoWatch Traffic Monitor — DLP-система для предотвращения утечек данных
Consul	Инструмент для объединения серверов IWTM в единый кластер

Термин	Пояснение
ICAP	Internet Content Adaptation Protocol — протокол интеграции прокси и DLP
OCR	Optical Character Recognition — распознавание текста (используется FineReader)

Параметры

Параметр	Значение
IP-адрес IWTM-Web	`192.168.88.101`
IP-адрес IWTM-DB	`192.168.88.102`
IP-адрес IWTM-Indexer	`192.168.88.103`
IP-адрес Proxy	`192.168.88.200`
Логин для входа в веб-интерфейс	`officer`
Пароль для входа в веб-интерфейс	`xxxX1234`

Решение

Шаг 1. Подготовка ВМ и установщика

Что нужно сделать

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

Ход работы

1. Настраиваем сеть и файл hosts

На каждой из четырех машин запустите утилиту настройки сети:

```
nmtui
```

Укажите статический IP-адрес, 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 на каждой ВМ (по умолчанию это `/home/officer/`). 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 BM Web: `iwtm`
- На BM DB: `iwtmdb`
- На BM Indexer: `iwtmidx`
- На BM Proxy: `iwproxy`

Перезагрузите каждую машину:

```
sudo reboot
```

3. Настройка репозиториев и базовых пакетов

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

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

4. Подготовка файлов установщика

Через WinSCP перекиньте архив `TME_Astra.zip` и файл лицензии на каждую BM (в домашнюю директорию пользователя `officer`).

Создайте папку для установщика и перенесите туда файлы:

```
mkdir /dist
cp /home/officer/TME_Astra.zip ./dist/
cd /dist
```

Распакуйте архив (после этого появится папка `TME_Astra`):

```
unzip TME_Astra.zip
cd TME_Astra
```

Самое первое и важное действие: выдайте права на исполнение зеленому файлу установщика. Так как версия в названии файла может отличаться, используйте клавишу **Tab**

для автодополнения:

```
sudo chmod +x iwtm-installer-<TAB>
# Нажмите Tab, чтобы система сама дописала версию, например: iwtm-installer-7.11.0.268-astra-1.7
```

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

Что нужно сделать

Установить компонент базы данных IWTM.

Ход работы

1. Запускаем установщик

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

(Не забудьте нажать Tab, чтобы подставилось полное имя файла с версией). В меню выберите **Distributed** (Распределенная) и шаблон **Database**. Остальное — по умолчанию.

2. Настраиваем Consul Дойдите до `Configure Consul service` и укажите:

- **Network interface address:** `192.168.88.102`
- **Agent mode:** `Server`
- **Datacenter name:** `iwtm`
- **Set consul retry-join servers:** `192.168.88.102`

Завершите установку и перезагрузите ВМ.

Шаг 3. Установка Web и ICAP (ВМ IWTM-Web)

Что нужно сделать

Установить веб-консоль и перехватчики трафика.

Ход работы

1. Запускаем установщик

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

Выберите **Distributed**. На экране выбора шаблонов отметьте **Web console** и **Traffic interceptors** (Indexer ставим отдельно).

2. Настройка подключений

- При вопросе об адресе базы данных укажите IP ВМ DB: `192.168.88.102`.
- В настройках Consul (`Configure Consul service`) укажите:
  - **Network interface address:** `192.168.88.101`
  - **Agent mode:** `Server`
  - **Datacenter name:** `iwtm`
  - **Set consul retry-join servers:** `192.168.88.102`

3. Настройка OCR На шаге `Configure OCR engine` убедитесь, что выбрана опция `Would you like to use OCR engine?` и движок **ABBYY FineReader**. Завершите установку и перезагрузите ВМ.

Шаг 4. Установка Indexer (ВМ IWTM-Indexer)

Что нужно сделать

Установить компонент индексации.

Ход работы

1. Запускаем установщик

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

Выберите **Distributed**. Отметьте **только шаблон Indexer service**.

2. Настройка подключений

- Адрес базы данных: `192.168.88.102`.
- В настройках Consul укажите:
  - **Network interface address:** `192.168.88.103`
  - **Agent mode:** `Server`
  - **Set consul retry-join servers:** `192.168.88.102`.

Завершите установку и перезагрузите ВМ.

Шаг 5. Объединение в кластер и запуск IWTM

Что нужно сделать

Связать серверы в кластер Consul и запустить службы.

Ход работы

1. Объединяем серверы в кластер Зайдите на ВМ **IWTM-DB** (`iwtmdb`) и выполните команду:

```
consul join 192.168.88.101
consul members
```

Зайдите на ВМ **IWTM-Indexer** (`iwtmidx`) и выполните **ту же самую команду**:

```
consul join 192.168.88.101
consul members
```

(В списке `consul members` на любом из серверов должно отображаться 3 узла: 101, 102, 103).

2. Запускаем службы На ВМ **IWTM-Web** (`iwtm`) запустите службы:

```
iwtm start
iwtm status
```

3. Проверяем веб-интерфейс Откройте браузер и перейдите по адресу `https://192.168.88.101`. Логин: `officer`, Пароль: `xxxX1234`. В меню **Еще -> Состояние системы** проверьте, что все три сервера отображаются. Не забудьте добавить лицензию в разделе **Еще -> Лицензии**.

Шаг 6. Настройка Proxy Squid (ВМ Proxy)

Что нужно сделать

Настроить прокси-сервер Squid для перехвата HTTPS-трафика.

Ход работы

> ⚠ **Важно!** Перед началом настройки откройте официальную документацию: перейдите на сайт `https://kb.infowatch.com/`, найдите раздел IW Traffic Monitor -> Documentation, выберите вашу версию и вашу ОС (Astra Linux / RedOS). Перейдите в «Руководство администратора ONLINE» -> «Настройка Системы после установки» -> «Общие настройки» -> «Перехват трафика, передаваемого по протоколу ICAP». Сверяйтесь с этим руководством по ходу работы (сайт и калькулятор масок сети будут доступны вам на соревновании).

1. Установка Squid и отключение SELinux На ВМ `iwproxy` выполните:

```
sudo apt install squid -y
sudo sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
sudo reboot
```

2. Генерация сертификатов

```
sudo mkdir -p /etc/squid/ssl_cert /var/lib/squid/ssl_db
sudo chown -R squid:squid /etc/squid/ssl_cert /var/lib/squid
sudo openssl req -new -newkey rsa:2048 -days 3650 -nodes -x509 \
  -keyout /etc/squid/ssl_cert/iwproxy.key \
  -out /etc/squid/ssl_cert/iwproxy.crt \
  -subj  "/C=RU/ST=Moscow/L=Moscow/O=IWProxy/CN=iwproxy.demo.lab" \
  -addext "subjectAltName = DNS:iwproxy.demo.lab, DNS:iwproxy"
sudo openssl x509 -in /etc/squid/ssl_cert/iwproxy.crt -outform DER -out
/etc/squid/ssl_cert/iwproxy.der
sudo openssl dhparam -outform PEM -out /etc/squid/ssl_cert/iwproxy_dhparam.pem 2048
sudo chown squid:squid /etc/squid/ssl_cert/iwproxy*
sudo chmod 400 /etc/squid/ssl_cert/iwproxy*
```

3. Инициализация базы сертификатов

```
sudo systemctl stop squid
sudo rm -rf /var/lib/squid/ssl_db
sudo /usr/lib64/squid/security_file_certgen -c -s /var/lib/squid/ssl_db -M 20MB
```

4. Настройка конфигурации (squid.conf) Удалите старый конфиг и создайте новый:

```
sudo rm -rf /etc/squid/squid.conf
sudo nano /etc/squid/squid.conf
```

Вставьте конфигурацию (обратите внимание на IP-адрес сервера Web — `192.168.88.101`):

```
visible_hostname iwproxy.demo.lab
cache_mgr admin@iwproxy.demo.lab

acl intermediate_fetching transaction_initiator certificate-fetching
http_access allow intermediate_fetching

http_port 3128 tcpkeepalive=60,30,3 ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=20MB \
  tls-cert=/etc/squid/ssl_cert/iwproxy.crt \
```

```
  tls-key=/etc/squid/ssl_cert/iwproxy.key \
  cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS \
  options=NO_TLSv1,NO_SSLv3,SINGLE_DH_USE,SINGLE_ECDH_USE \
  tls-dh=prime256v1:/etc/squid/ssl_cert/iwproxy_dhparam.pem
sslproxy_cert_error allow all
ssl_bump stare all

sslcrtd_program /usr/lib64/squid/security_file_certgen -s /var/lib/squid/ssl_db -M 20MB
sslcrtd_children 8

icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_service service_req reqmod_precache bypass=1 icap://192.168.88.101:1344/request
adaptation_access service_req allow all

http_access allow all
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
```

Запускаем службу:

```
sudo systemctl enable squid
sudo systemctl start squid
```

5. Настройка IWTM и включение ICAP Вернитесь на ВМ **IWTM-Web** (`iwtm`).
Отредактируйте файл `luaengined.conf`:

```
sudo nano /opt/iw/tm5/etc/luaengined.conf
```

Убедитесь, что в секции `"TransportModes"` прописано:

```
"Icap": [{"Server": "192.168.88.101", "Mode": "Normal"}]
```

Отредактируйте файл `icap.conf`:

```
sudo nano /opt/iw/tm5/etc/icap.conf
```

Убедитесь, что параметр `AsyncCheck` установлен в значение `false`.

Перезапустите IWTM и включите службу ICAP (так как при разнесенной установке она по умолчанию выключена):

```
iwtm restart
sudo systemctl unmask iw_icap
sudo systemctl start iw_icap
sudo systemctl enable iw_icap
```

Проверьте, что сервер слушает порт 1344:

```
sudo ss -tlnp | grep 1344
```

Шаг 7. Проверка перехвата и LDAP-синхронизация

Что нужно сделать

Проверить перехват трафика с клиента и настроить синхронизацию пользователей.

Ход работы

1. Проверка трафика На клиенте (`astra-cli`) импортируйте сертификат `iwproxy.der` в браузер (Настройки -> Сертификаты -> Импорт) и настройте ручной прокси `192.168.88.200` порт `3128` для HTTP и HTTPS. Зайдите на любой сайт. В веб-интерфейсе IWTM в разделе **События** создайте выборку за последние 7 дней — должны появиться записи от `astra-cli`.

2. LDAP-синхронизация В IWTM перейдите в **Еще -> LDAP-Синхронизации** и создайте две синхронизации:

- **Для AD**: Имя сервера `demolab.demo.lab`, тип `Active Directory`, IP `192.168.88.100`, порт `3268`, запрос `dc=demo,dc=lab`, логин `DEMO\ldapuser`, пароль `xxXX4321`.
- **Для ALD Pro**: Имя сервера `dc.aldpro.lab`, тип `Astra Linux Directory Pro / FreeIPA`, IP `192.168.88.30`, порт `389`, запрос `cn=accounts,dc=aldpro,dc=lab`, логин `admin@ALDPRO.LAB`, пароль администратора ALD Pro. Запустите обе синхронизации.

3. Доступ для tmofficer В разделе **Управление доступом -> Добавить из LDAP** найдите пользователя `tmofficer` (из домена AD), добавьте почту и выдайте все роли и области видимости. Войдите под ним.

Как проверить

- ☐ На всех ВМ выданы права `chmod +x` на установщик
- ☐ `hosts` перенесен через WinSCP на все ВМ в `/home/officer/`
- ☐ Компонент Database установлен на `IWTM-DB`
- ☐ Компоненты Web и Interceptors установлены на `IWTM-Web`

- ☐ Компонент Indexer установлен на `IWTM-Indexer`
- ☐ На `iwtmdb` и `iwtmidx` выполнена команда `consul join` (3 узла в кластере)
- ☐ Веб-консоль IWTM открывается, статус серверов в норме
- ☐ Настроен Squid, сгенерированы сертификаты
- ☐ В `icap.conf` стоит `false`, служба `iw_icap` запущена, порт 1344 слушается
- ☐ В IWTM появляются события от `astra-cli`
- ☐ Выполнена LDAP-синхронизация, `tmofficer` может войти

Если что-то не работает

Проблема	Что делать
`Permission denied` при запуске установщика	Выполнить `chmod +x iwtm-installer-<версия>-astra-1.7`
Consul не видит узлы	Проверить IP в `consul join`, проверить доступность портов
Не открывается веб-интерфейс	Проверить `iwtm status`, проверить статус `nginx`
Прокси не пропускает HTTPS	Проверить отключение SELinux (`sestatus`), проверить `dhparam.pem`
`grep 1344` ничего не выдает	Выполнить `systemctl unmask iw_icap` и `systemctl start iw_icap`
Не работает LDAP	Проверить пароли и правильность формата логина, доступность контроллеров по портам

Revision #3
Created 2026-10-17 07:36:07 UTC by Admin
Updated 2026-10-17 13:03:27 UTC by Admin