

Задание 1: Подготовка домена Active Directory.

Создаем подразделения (Organization Unit) под названием “FinalOfficeAD”. Нажимаем правую кнопку мыши demo.lab > создать > подразделение, убираем флажок и даем название для подразделения. Таким же образом добавляем в него два каталога под названиями “Users” и “Computers” (Рисунок 1)

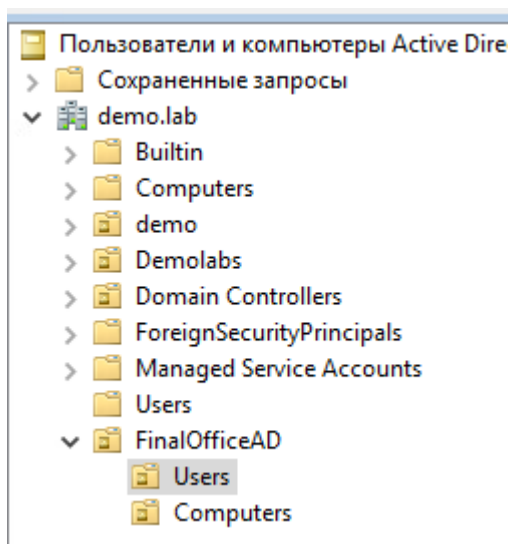


Рисунок 1 – созданные подразделения

В только что созданном подразделении users, создаем необходимых пользователей, правой кнопкой мыши > создать > пользователь. Вписываем имя пользователя по заданию, далее ставим пароль и убираем флажки. (Рисунок 2)

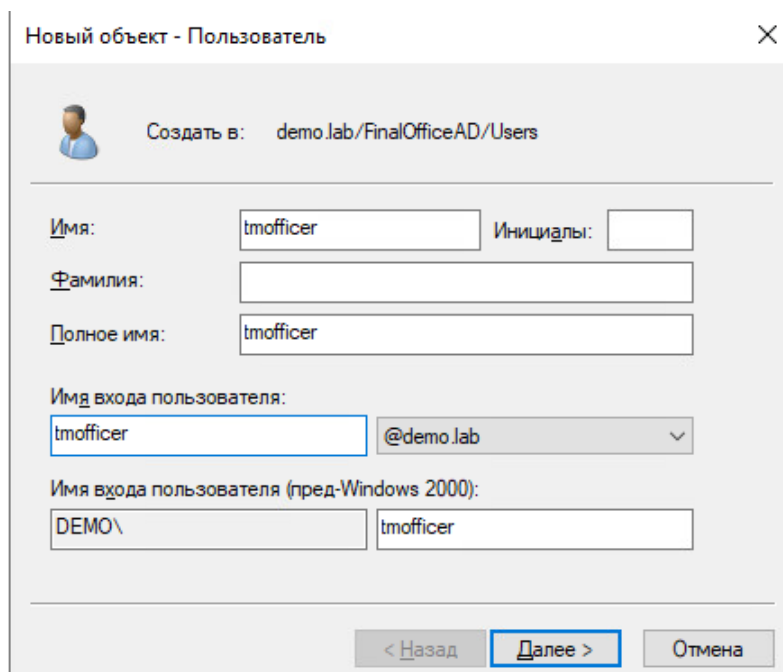


Рисунок 2 – создание пользователя

После того, как создали всех необходимых пользователей, добавляем пользователей, которые указаны в задании в группы доменных администраторов. Дважды кликаем на пользователя, далее заходим во вкладку “Член групп” > добавить, вписываем Domain Admins, нажимаем “ок”, выбираем нашу группу domain admins и задаем, как основную группу. (Рисунок 3)

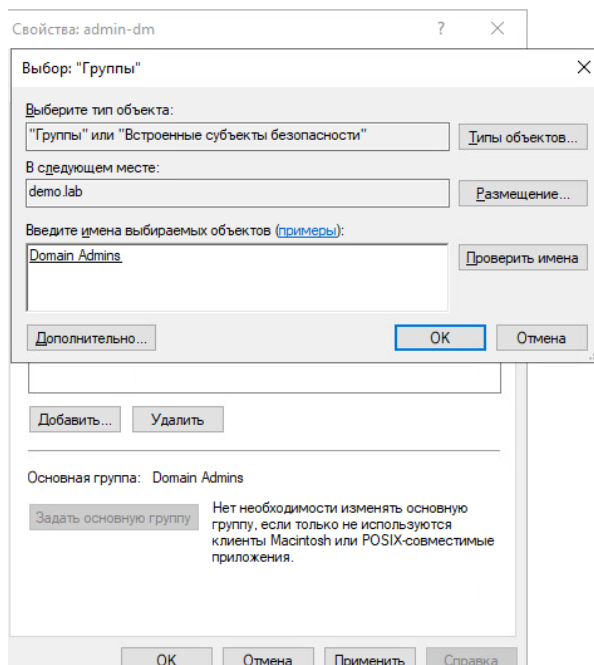


Рисунок 3 – добавление в группу доменных администратор

Для того, чтобы в дальнейшем сделать синхронизацию с доменом aldpro.lab, надо создать запись в файле с хсоетами для этого, запустить блокнот от имени администратора, далее файл > открыть и переходим по пути C:\Windows\System32\drivers\etc, ставим “все файлы” и открываем файл hosts. (Рисунок 4)

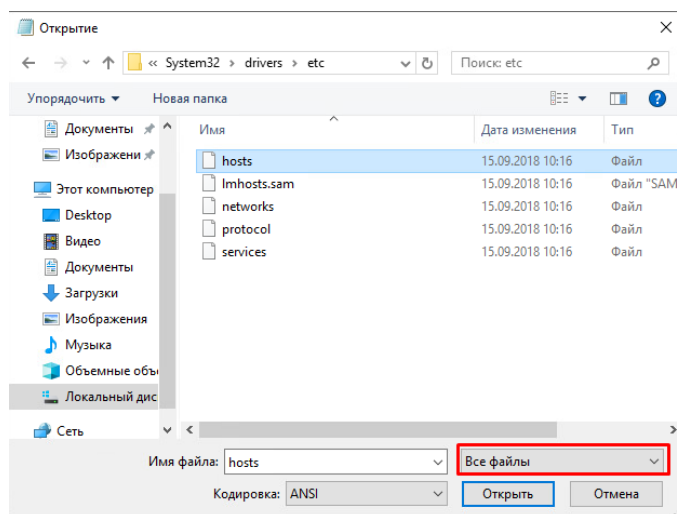
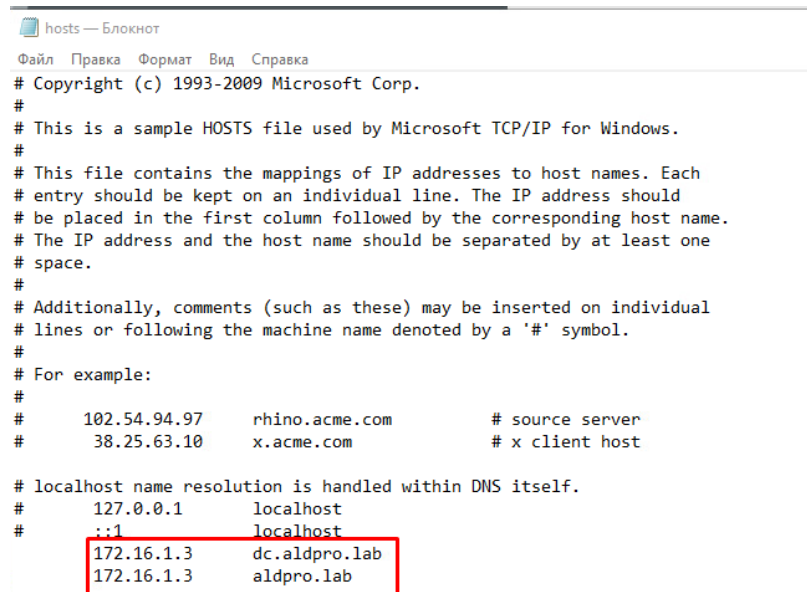


Рисунок 4 – файл с записями о хостах

После того, как открыли файл вписываем в него ip адрес домена alldpro.lab и указываем запись для контроллера домена. (Рисунок 5)



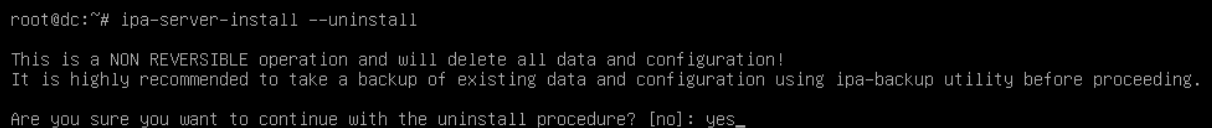
```
hosts — Блокнот
Файл  Правка  Формат  Вид  Справка
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host


# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1            localhost
172.16.1.3       dc.alldpro.lab
172.16.1.3       alldpro.lab
```

Рисунок 5 – изменение записей о хостах.

Задание 2: Подготовка домена alldpro.

Чтобы домен на alldpro корректно работал, его надо переустановить, для этого удаляем командой ipa-server-install --uninstall и вылезет подтверждение об удалении домена, прописываем “yes”. (Рисунок 6)



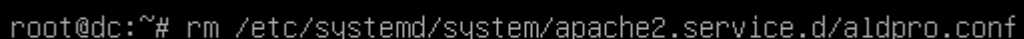
```
root@dc:~# ipa-server-install --uninstall

This is a NON REVERSIBLE operation and will delete all data and configuration!
It is highly recommended to take a backup of existing data and configuration using ipa-backup utility before proceeding.

Are you sure you want to continue with the uninstall procedure? [no]: yes_
```

Рисунок 6 – удаление домена alldpro.

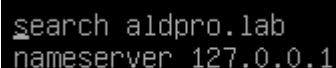
После того как процесс удаления завершается, надо удалить конфигурационный файл apache для alldpro. Конфигурационный файл находится по пути /etc/systemd/system/apache2.service.d/alldpro.conf. После его удаления, перезагружаем машину. (Рисунок 7)



```
root@dc:~# rm /etc/systemd/system/apache2.service.d/alldpro.conf
```

Рисунок – 7 удаление конфигурационного файла apache для alldpro

Далее потребуется отредактировать файлы /etc/resolv.conf и /etc/network/interfaces, /etc/hosts. (Рисунок 8)



```
search alldpro.lab
nameserver 127.0.0.1
```

Рисунок 8 – редактирование /etc/resolv.conf

Редактирование конфигурационного файла /etc/hosts. (рисунок 9)

```
#astra-freeipa-server
127.0.0.1 localhost localhost.localdomain
172.16.1.3 dc.aldpro.lab dc
172.16.1.4 iwtm.demo.lab iwtm
172.16.1.2 demolab.demo.lab

::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Рисунок 9 – редактирование конфигурационного файла

Редактирование конфигурационного файла /etc/network/interfaces. (Рисунок 10)

```
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 172.16.1.3/24
    gateway 172.16.1.1
```

Рисунок 10 – редактирование /etc/network/interfaces

Теперь можно перейти к установке aldpro. Ничего дополнительного скачивать не надо, так как aldpro была установлена ранее, теперь нужно только запустить установку `sudo aldpro-server-install -d <домен> -n <имя_сервера> -p <пароль> --ip <IP-адрес_контроллера_домена> --no-reboot.` (Рисунок 11)

```
root@dc:/home/astra# sudo aldpro-server-install -d aldpro.lab -n dc -p xxxX1234 --ip 172.16.1.3 --no-reboot
[INFO ] Executing command systemctl in directory '/root'
[INFO ] Executing command systemd-run in directory '/root'
```

Рисунок 11 – установка домена aldpro.lab

Задание 3: Настройка отношений доверия.

Подготовка машины astra-cli для ввода в домен. Настройка соединения. В терминале прописываем `nmtui` открывается графический network manager > изменить соединение, выбираем наше соединение, конфигурация IPv4 > вручную и выставляем все необходимые настройки > ок > назад > подключиться и отключаемся и снова подключаемся к сети. (Рисунок 12)

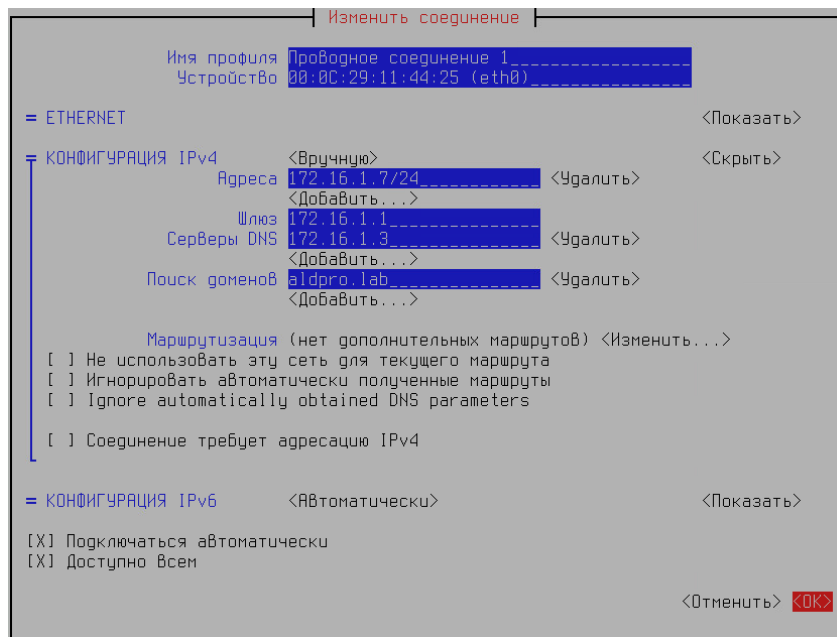


Рисунок 12 – настройка соединения

Изменение хостнейма, в терминале прописываем `hostnamectl set-hostname <имя сервера>.<домен>` (Рисунок 13)

```
root@astra-cli:/home/locadm# hostnamectl set-hostname astra-cli.aldpro.lab
root@astra-cli:/home/locadm# hostname
astra-cli.aldpro.lab
```

Рисунок 13 – изменение хостнейма

Далее редактируем файл `/etc/hosts`. (Рисунок 14)

```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost.localdomain localhost
127.0.1.1    astra-cli
172.16.1.7   astra-cli.aldpro.lab

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Рисунок 14 – изменение файла hosts

Редактируем файл `/etc/apt/sources.list`. Изменяем репозитории на frozen. (Рисунок 15)

```
GNU nano 3.2 /etc/apt/sources.list
# Astra Linux repository description https://wiki.astralinux.ru/x/0oLiC
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-main/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-update/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-extended/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-base/ 1.7_x86-64 main contrib non-free
```

Рисунок 15 – изменение репозитория

Также добавляем репозитории aldpro, заходим в `/etc/apt/sources.list.d/aldpro.list` (Рисунок 16)

```
GNU nano 3.2 /etc/apt/sources.list.d/aldpro.list
deb https://dl.astralinux.ru/aldpro/stable/repository-main/ 2.1.0 main
deb https://dl.astralinux.ru/aldpro/stable/repository-extended/ generic main
```

Рисунок 16 – добавленные репозитории

Создаем файл, который будет определять приоритет заходя в /etc/apt/preferences.d/aldpro и добавляем, как на рисунке 17(Рисунок 17)

```
GNU nano 3.2
Package: *
Pin: release n=generic
Pin-Priority: 900
```

Рисунок 17 – определение приоритета

Устанавливаем клиента для ввода в домен. Командой *sudo DEBIAN_FRONTEND=noninteractive apt-get install -q -y aldpro-client*.

Вводим клиента в домен командой. *sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer -c aldpro.lab -u admin -p xxXX1234 -d astra-cli -i -f*. (Рисунок 18)

```
root@astra-cli:~# sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer -c aldpro.lab -u admin -p xxXX1234 -d astra-cli -i -f
systemctl mask aldpro-client-service-discovery.service
Created symlink /etc/systemd/system/aldpro-client.service → /dev/null.
/usr/bin/astra-freeipa-client -d "aldpro.lab" -u "admin" -p "xxXX1234" -y --par "--hostname=astra-cli.aldpro.lab --force-join"
Discovery was successful!
Client hostname: astra-cli.aldpro.lab
Realm: ALDPRO.LAB
DNS Domain: aldpro.lab
IPA Server: dc.aldpro.lab
BaseDN: dc=aldpro,dc=lab
Synchronizing time
Configuration of chrony was changed by installer.
Attempting to sync time with chronyc.
Time synchronization was successful.
Successfully retrieved CA cert
  Subject: CN=CA Signing Certificate
  Issuer: CN=CA Signing Certificate
  Valid From: 2024-04-09 06:06:11
  Valid Until: 2044-04-04 06:06:11

Enrolled in IPA realm ALDPRO.LAB
Created /etc/ipa/default.conf
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sss/sssd.conf
Configured /etc/krb5.conf for IPA realm ALDPRO.LAB
Systemwide CA database updated.
Hostname (astra-cli.aldpro.lab) does not have A/AAAA record.
Missing reverse record(s) for address(es): 172.16.1.7.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring aldpro.lab as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
rm -f /etc/salt/minion_id
/usr/bin/python3 /opt/rbta/aldpro/client/bin/aldpro-service-discovery.py
[INFO ] Executing command systemctl in directory '/root'
[INFO ] Executing command systemd-run in directory '/root'
salt-call state.apply aldpro.subsystems.common.clients_update queue=True
```

Рисунок 18 – Успешный вход в домен.

После того как мы ввели astra-cli в домен. Можно приступать к доверительным отношениям и миграции с demo.lab. Надо указать на AD сервер dns aldpro.lab и наоборот, еще надо создать сервер условной пересылки на ad, заходим в dns > серверы условной пересылки, правой кнопкой мыши > создать сервер условной пересылки. (Рисунок 19)

Создать сервер условной пересылки

DNS-домен:
aldpro.lab

IP-адреса основных серверов:

IP-адрес	FQDN сервера	Проверка выполнена
172.16.1.3	dc.aldpro.lab	Сервер с таким IP-адресом...

☐ Сохранять условный сервер пересылки в Active Directory и реплицировать ее следующим образом:
Все DNS-серверы в этом лесу

Время ожидания пересылки (сек): 5

Полное доменное имя сервера будет недоступно, если не настроены соответствующие зоны обратного просмотра и записи.

ОК Отмена

Рисунок 19 – создание сервера условной пересылки

Дальше заходим в веб-интерфейс aldpro, желательно делать это по доменному имени, так как бывает ошибка, если пытаться через ip. После того, как зашли заходим в управление доменом > интеграции с MS AD. Выбираем новое подключение, как показано на рисунке. (Рисунок 20)

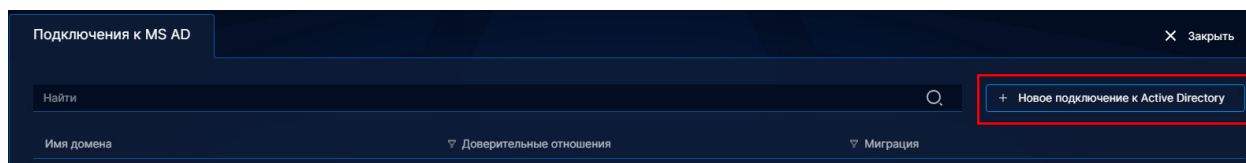


Рисунок 20 – добавление подключения к MS AD.

Дальше открывается окно нового подключения к AD, где уже вписываем ша домен AD. Ставим галочку доверительные отношения и вписываем учетную запись для доверительных отношений (!!! Учетная запись должна обладать правами администратора домена !!!). Далее ставим галочку Миграция объектов AD. Заполняем поля как на рисунке. (Рисунок 21)

Рисунок 21 – создание доверительных отношений

После того как сохранили и подтвердили, должно появиться подключение с доменом demo.lab (Рисунок 22)

demo.lab	Двусторонние	Да
----------	--------------	----

Рисунок 22 – активные доверительные отношения

Дальше нажимаем на эти доверительные отношения и переходим во вкладку “сопоставление полей при миграции” и нажимаем запустить миграцию. (Рисунок 23)



Рисунок 23 – запуск миграции

После этого откроется окно, в котором надо заполнить поля. Выбираем подразделение, которое хотим мигрировать и выбираем подразделение, в котором оно будет находиться. Остальные поля заполняем, как на рисунке и нажимаем сохранить вылезит окошко подтверждения, нажимаем ДА. После этого начнется процесс миграции. (Рисунок 24)

Основное

demo.lab

Подразделение Active Directory обязательно

FinalOfficeAD x | ▼

Подразделение ALD Pro обязательно

aldpro.lab x | ▼

Объект миграции

- ☒ Группы Пользователей
- ☒ Организационное Подразделение
- ☒ Пользователи

Пароль пользователя обязательно

..... 🔒

Логин администратора ALD Pro обязательно

admin

Пароль администратора ALD Pro обязательно

..... 🔒

Рисунок 24 – запуск миграции

Проверяем успешность миграции через `astra-cli`, заходим через пользователя `useroffice`, тот который был создан в AD. Домен должен быть выбран `aldpro`. (Рисунок 25)

Вход в astra-cli.aldpro.lab

aldpro.lab

useroffice

.....

Войти >

Рисунок 25 – вход доменного пользователя ad

После того как нажмете войти, то предложит сменить пароль. Меняете пароль и заходите (Рисунок 26)

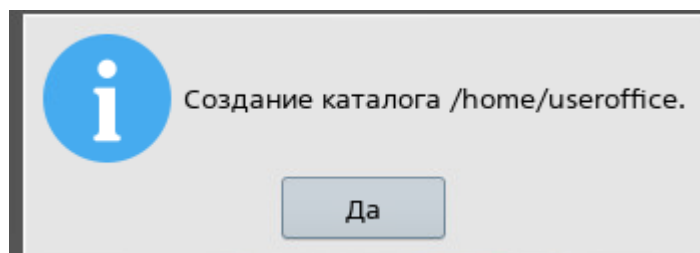


Рисунок 26 – создание каталога пользователя

Задание 4: Настройка IWTM

Теперь можно переходить к установке infowatch traffic monitor. Перед запуском добавляем установочный диск, диск разработчика, диск с файлами для установки tm. (Рисунок 27)

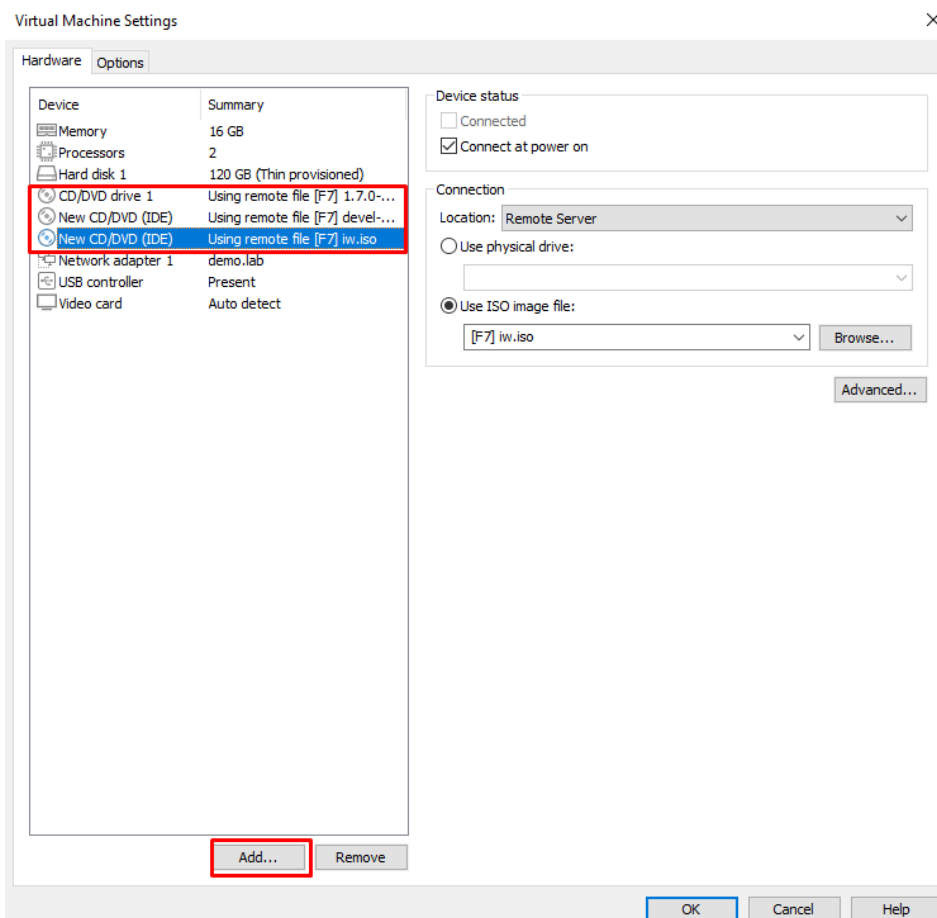


Рисунок 27 – добавление дисков

При заходе в astra linux без интерфейса. Может попросить ввести integrity level, надо вводить 63, потому что могут возникать ошибки, если вводить значение меньше. Создаем директории в которые будут подключаться наши диски. Затем монтируем диски в созданные директории. (Рисунок 28)

```

root@iwtm:~# mkdir /media/cdrom1
root@iwtm:~# mkdir /media/cdrom2
root@iwtm:~# mount /dev/sr0 /media/cdrom0
mount: /media/cdrom0: WARNING: device write-protected, mounted read-only.
root@iwtm:~# mount /dev/sr1 /media/cdrom1
mount: /media/cdrom1: WARNING: device write-protected, mounted read-only.
root@iwtm:~# mount /dev/sr2 /media/cdrom2
mount: /media/cdrom2: WARNING: device write-protected, mounted read-only.

```

Рисунок 28 – монтирование дисков

После того как диски подключены, проверяем, что где лежит, и установочный файл `tm` копируем в `/root/`, командой `cp -r Astra/ /root/` (Рисунок 29)

```

root@iwtm:/media/cdrom2# cp -r Astra/ /root/

```

Рисунок 29 – копирование установочных файлов

После этого устанавливаем `ca-certificate`, он находится на установочном диске в директории `pool/main/c/ca-certificates/`, переходим в эту директорию и устанавливаем сертификаты командой `dpkg -i <название файла.deb>` (Рисунок 30)

```

root@iwtm:/media/cdrom0# cd pool/main/c/ca-certificates/
root@iwtm:/media/cdrom0/pool/main/c/ca-certificates# ls
ca-certificates_20190110_all.deb  ca-certificates-udeb_20190110_all.udeb
root@iwtm:/media/cdrom0/pool/main/c/ca-certificates# dpkg -i ca-certificates_20190110_all.deb
Выбор ранее не выбранного пакета ca-certificates.
(Чтение базы данных ... на данный момент установлено 37227 файлов и каталогов.)
Подготовка к распаковке ca-certificates_20190110_all.deb ...
Распаковывается ca-certificates (20190110) ...
Настраивается пакет ca-certificates (20190110) ...
debconf: не удалось инициализировать интерфейс: Dialog
debconf: (Ни одна из dialog-подобных программ не установлена, поэтому вы не можете использовать dialog-интерфейс. at /usr/share/
perl5/Debconf/FrontEnd/Dialog.pm line 76.)
debconf: будет использован интерфейс: Readline
Updating certificates in /etc/ssl/certs...
128 added, 0 removed; done.
Обрабатываются триггеры для man-db (2.8.5-2) ...
Обрабатываются триггеры для ca-certificates (20190110) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
root@iwtm:/media/cdrom0/pool/main/c/ca-certificates#

```

Рисунок 30 – установка `ca-certificates`

Настраиваем `ip` адрес (Рисунок 31)

```

GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 172.16.1.4/24
    gateway 172.16.1.1_

```

Рисунок 31 – настройка `ip` на `iwtm`

Далее редактируем файл /etc/hosts (Рисунок 32)

```
127.0.0.1      localhost
172.16.1.4     iwtm
172.16.1.3     dc.aldpro.lab dc
```

Рисунок 32 – редактируем файл /etc/hosts

Редактируем файл /etc/apt/source.list (Рисунок 33)

```
deb file:/media/cdrom0/ 1.7_x86-64 contrib main non-free
deb file:/media/cdrom1/ 1.7_x86-64 contrib main non-free
```

Рисунок 33 – редактируем конфигурационный файл

Переходим в директорию куда копировали установочные файлы. Делаем установочный файл исполняемым и потом запускаем. (Рисунок 34)

```
root@iwtm:~/Astra# chmod +x iwtm-installer-7.7.2.136-astra-smolensk-1.7
root@iwtm:~/Astra# ./iwtm-installer-7.7.2.136-astra-smolensk-1.7_
```

Рисунок 34 – начало установки

Все настройки оставляем по умолчанию. Ждем пока установка завершится. (Рисунок 35)

```
#####
Installing DB packages...done
Installing Traffic Monitor packages...done
Installing DB schema...done
Configuring operating system...done|
Starting services..#

-----
InfoWatch Traffic Monitor installation has finished

In case of distributed installation product startup
must be done in the following order:

Database, Web, Indexer, Interceptors

Remove extracted installer data [Y/n]:

Please re-login to apply environment changes.
root@iwtm:~/Astra# _
```

Рисунок 35 – Завершении установка

После завершения установки заходим веб-интерфейс iwtm`a, логин officer, пароль ххХХ1234. Далее активируем лицензию, управление > лицензии, нажимаем на + , если лицензия не отображается, то выбираем “все файлы”, выбираем лицензию, сохраняем и подтверждаем. (Рисунок 36)

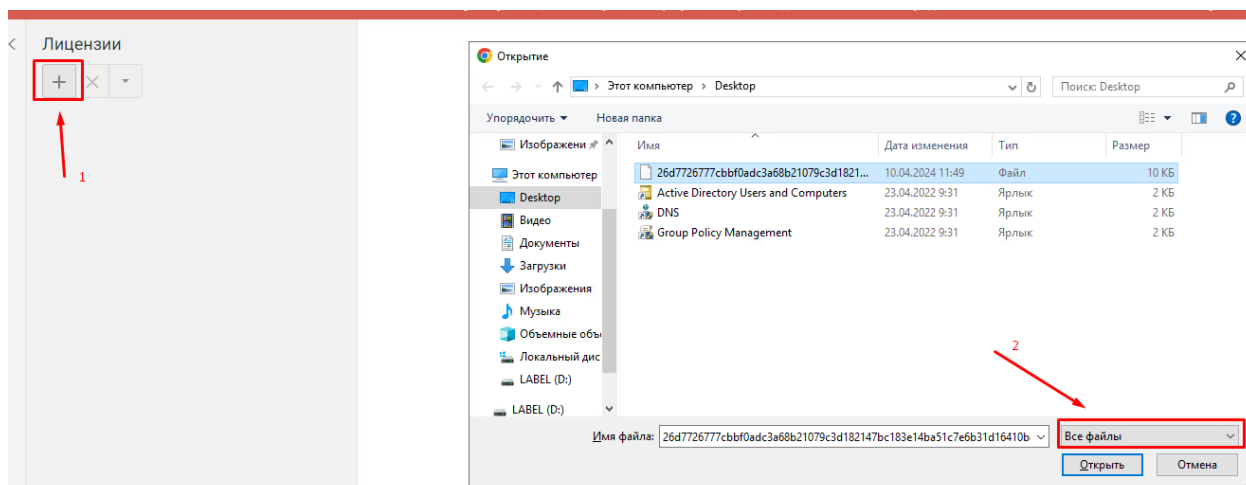


Рисунок 37 – добавление лицензии

Создание ldap синхронизации с AD, переходим управление > ldap-синхронизация, также как в лицензиях нажимаем + , задаем имя сервера, выбираем тип сервера, в пункте ldap-сервер вписываем ip адреса сервера, с которым синхронизируем, в ldap-запрос домен, как скриншоте, и последние учетная запись под которой делаем синхронизацию. (Рисунок 38)

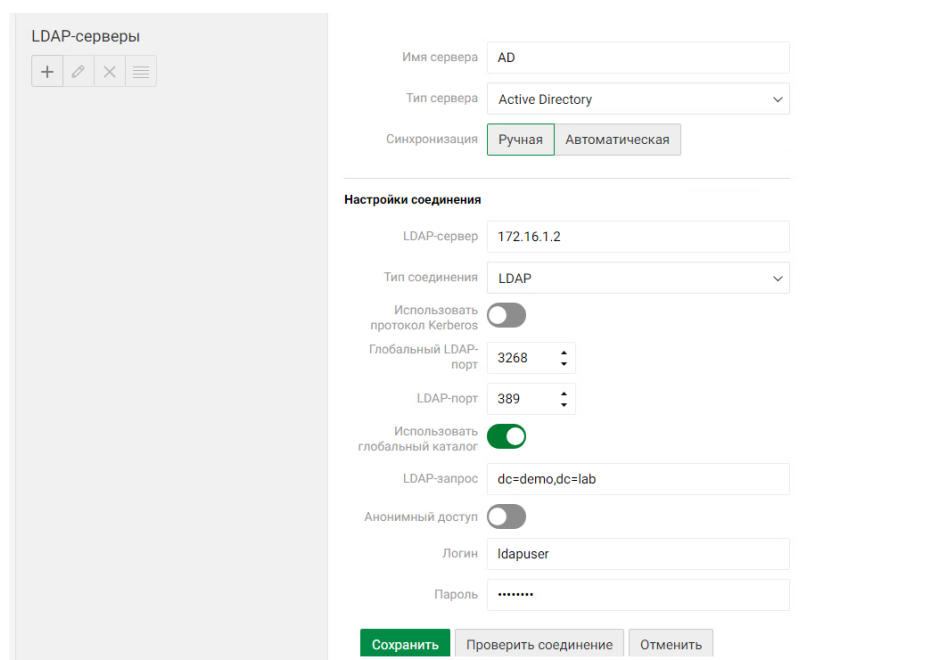


Рисунок 38 – создание ldap-синхронизации с AD

После сохранения, нажимаем на дополнение и нажимаем “запустить синхронизацию”, дальше должен появиться результат синхронизации. (Рисунок 39)

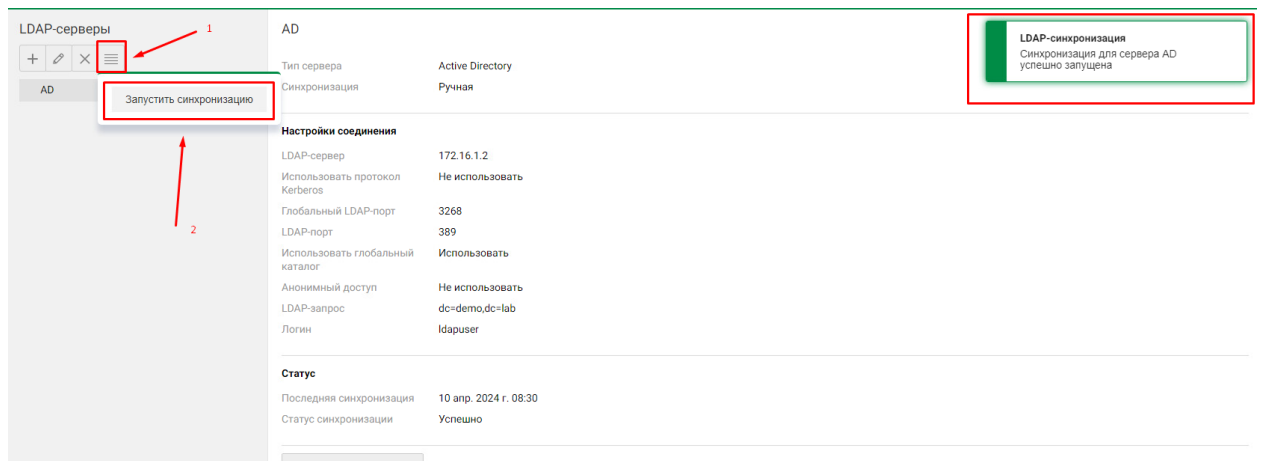


Рисунок 39 – запуск ldap синхронизации

Перед созданием синхронизации надо добавить запись в /etc/hosts на iwtm(Рисунок 40)

```
127.0.0.1    localhost
172.16.1.4   iwtm
172.16.1.3   dc.aldpro.lab dc

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Рисунок 40 – изменение записи

Создаем ldap-синхронизацию с ALD, также нажимаем добавить синхронизацию, задаем имя, тип сервера выбираем ALD PRO/FreeIPA, ldap-сервер ip адрес сервера aldpro, в логин обязательно надо указать домен!!! (Рисунок 41)

The screenshot shows the 'LDAP-серверы' (LDAP servers) management interface with the 'AD' server selected. The 'Тип сервера' (Server type) dropdown is set to 'Astra Linux Directory Pro / FreeIPA' and is highlighted with a red box. The 'Синхронизация' (Synchronization) tabs show 'Ручная' (Manual) selected. The 'Настройки соединения' (Connection settings) section includes: 'LDAP-сервер' (LDAP server) set to '172.16.1.3', 'Тип соединения' (Connection type) set to 'LDAP', 'Использовать протокол Kerberos' (Use Kerberos protocol) toggle turned off, 'LDAP-порт' (LDAP port) set to '389', 'LDAP-запрос' (LDAP query) set to 'dc=aldpro,dc=lab', and 'Логин' (Login) set to 'admin@aldpro.lab' (highlighted with a red box). The 'Пароль' (Password) field is masked with dots. At the bottom, there are buttons: 'Сохранить' (Save), 'Проверить соединение' (Check connection), and 'Отменить' (Cancel).

Рисунок 41 – создание ldap синхронизации с ALD PRO

Далее точно также запускаем синхронизацию(Рисунок 42)

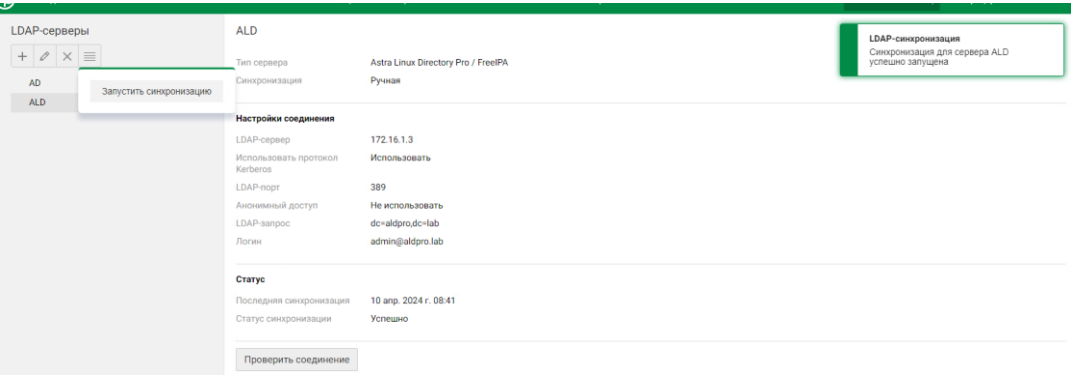


Рисунок 42 – запуск ldap-синхронизации

Чтобы добавить доменного пользователя для работы с консолью tm, переходим управление > управление доступов, во вкладке пользователи нажимаем + , добавить пользователя из ldap , выбираем ldap-сервер с которого надо добавить пользователя, в поиске пишем имя пользователя и сохраняем (Рисунок 43)

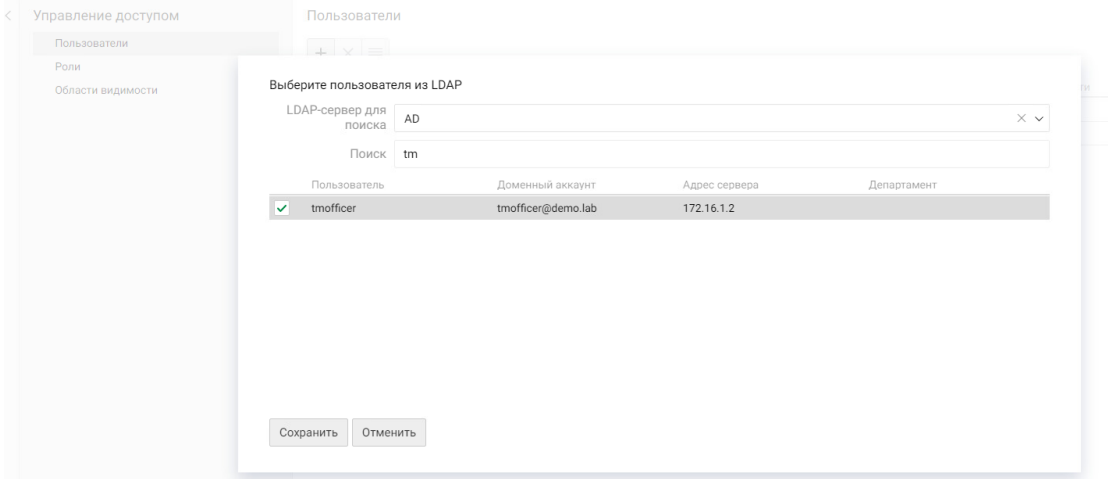


Рисунок 43 – добавление пользователя из ldap

Дальше если надо добавить роли и области видимости, то нажимаем на пользователя и добавляем все необходимое через +. (Рисунок 44)

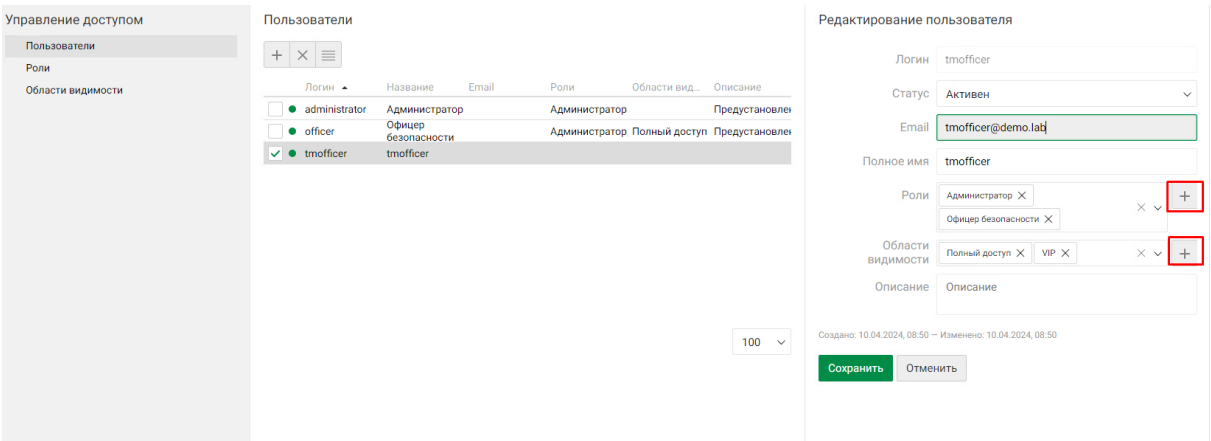


Рисунок 44 – добавление ролей и областей видимости

Задание 5: Настройка IWDM

Изменение конфигурационных файлов, /etc/hosts. (Рисунок 45)

```
GNU nano 3.2

127.0.0.1    localhost
172.16.1.5   iwdm

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Рисунок 45 – редактирование /etc/hosts

Изменение конфигурационных файлов, /etc/network/interfaces (Рисунок 46)

```
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 172.16.1.5
    gateway 172.16.1.1
```

Рисунок 46 – редактирование /etc/network/interfaces

Изменение конфигурационных файлов, /etc/resolv.conf (Рисунок 47)

```
GNU nano 3.2

search demo.lab
nameserver 172.16.1.2
```

Рисунок 47 – редактирование /etc/resolv.conf

Изменение конфигурационных файлов, /etc/apt/sources.list. После изменения репозитория, обновляем пакеты командой `sudo apt update`. (Рисунок 48)

```
GNU nano 3.2 /etc/apt/sources.list

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

Рисунок 48 – изменение сетевых репозитория

Для установки dotnet 6 потребуется wget, устанавливаем командой `sudo apt install wget`. Далее переходим к установке, первая команда добавление ключа подписания пакетов MS в список доверительных ключей `wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/microsoft.asc.gpg > /dev/null`, далее загружаем параметры репозитория ms `sudo wget https://packages.microsoft.com/config/debian/10/prod.list -O /etc/apt/sources.list.d/microsoft-prod.list`, далее обновляем пакеты командой `sudo apt update`, дальше надо установить dotnet 6.0 командой `sudo apt install dotnet-sdk-6.0`, после запуска принимаем установку (Рисунок 49)

```
root@iwdm:~# wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/microsoft.asc.gpg > /dev/null
--2024-04-10 14:33:28-- https://packages.microsoft.com/keys/microsoft.asc
Распознаётся packages.microsoft.com (packages.microsoft.com)... 13.107.246.74, 13.107.213.74, 2620:1ec:bdf::74, ...
Подключение к packages.microsoft.com (packages.microsoft.com) [13.107.246.74]:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 983 [application/octet-stream]
Сохранение в: «STDOUT»

-                                     100%[=====]          983  --.-KB/s   за 0с

/2024-04-10 14:33:28 (17,6 MB/s) - записан в stdout [983/983]

root@iwdm:~# sudo wget https://packages.microsoft.com/config/debian/10/prod.list -O /etc/apt/sources.list.d/microsoft-prod.list
--2024-04-10 14:33:36-- https://packages.microsoft.com/config/debian/10/prod.list
Распознаётся packages.microsoft.com (packages.microsoft.com)... 13.107.213.74, 13.107.246.74, 2620:1ec:46::74, ...
Подключение к packages.microsoft.com (packages.microsoft.com) [13.107.213.74]:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 74 [application/octet-stream]
Сохранение в: «/etc/apt/sources.list.d/microsoft-prod.list»

/etc/apt/sources.list.d/microsoft-prod.list 100%[=====]          74  --.-KB/s   за 0с

2024-04-10 14:33:36 (16,6 MB/s) - «/etc/apt/sources.list.d/microsoft-prod.list» сохранён [74/74]

root@iwdm:~# sudo apt update
Пол:1 https://packages.microsoft.com/debian/10/prod buster InRelease [6 538 B]
Игн:2 https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main 1.7_x86-64 InRelease
Сущ:3 https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update 1.7_x86-64 InRelease
Сущ:4 https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base 1.7_x86-64 InRelease
Сущ:5 https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended 1.7_x86-64 InRelease
Сущ:6 https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main 1.7_x86-64 Release
Пол:7 https://packages.microsoft.com/debian/10/prod buster/main all Packages [2 393 B]
Пол:8 https://packages.microsoft.com/debian/10/prod buster/main amd64 Packages [213 kB]
Получено 222 kB за 2с (133 kB/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 267 пакетов. Запустите «apt list --upgradable» для их показа.
root@iwdm:~# sudo apt install dotnet-sdk-6.0
```

Рисунок 49 – установка dotnet 6.0

Также потребуется база данных Postgresql для того, чтобы ее установить надо ввести команду `sudo apt install postgresql`, соглашаемся с установкой БД. (Рисунок 50)

```
root@iwdm:~# sudo apt install postgresql
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 liblvm11 libpq5 libxslt1.1 libz3-4 postgresql-11 postgresql-client-11 postgresql-client-common postgresql-common sysstat
Предлагаемые пакеты:
 postgresql-doc postgresql-doc-11 libjson-perl isag
Следующие НОВЫЕ пакеты будут установлены:
 liblvm11 libpq5 libxslt1.1 libz3-4 postgresql postgresql-11 postgresql-client-11 postgresql-client-common postgresql-common
sysstat
Обновлено 0 пакетов, установлено 10 новых пакетов, для удаления отмечено 0 пакетов, и 267 пакетов не обновлено.
Необходимо скачать 42,6 МБ архивов.
После данной операции объём занятого дискового пространства возрастёт на 166 МБ.
Хотите продолжить? [Д/н] _
```

Рисунок 50 – установка БД

После того как БД установилась надо изменить пароль пользователя postgres, для этого вводим команду `sudo -u postgres psql`, чтобы войти в БД, далее `\password`;, и вводим новый пароль, затем выходим командой `\q`. (рисунок 51)

```
root@iwdm:~# sudo -u postgres psql
could not change directory to "/root": Отказано в доступе
psql (11.21 (Debian 1:11.21-astra.se8))
Type "help" for help.

postgres=# \password
Enter new password for user "postgres":
Enter it again:
postgres=# \q_
```

Рисунок 51 – изменение пароля пользователя

Дальше надо установить пакеты socat и conntrack, командой `apt install <название пакета>` (Рисунок 52)

```
root@iwdm:~# apt install socat && apt install conntrack_
```

Рисунок 52 – Установка пакетов

Монтируем диск с установочными файлами и копируем файлы установки для device monitor. Далее переходим в директорию в которую скопировали файлы, создаем папку, копируем в эту папку с файлами для установки, переходим в нее, и распаковываем командой `tar xvf <название>.tar.xz`. (Рисунок 53)

```
root@iwdm:~# mount /dev/sr0 /media/cdrom0
mount: /media/cdrom0: WARNING: device write-protected, mounted read-only.
root@iwdm:~# cd /media/cdrom0
root@iwdm:/media/cdrom0# ls
1.8.0  Astra 'linux server'  Лицензия
root@iwdm:/media/cdrom0# cp -r linux\ server/ /root/
root@iwdm:/media/cdrom0# cd /root/linux\ server/
root@iwdm:~/linux server# mkdir dm
root@iwdm:~/linux server# l
bash: l: команда не найдена
root@iwdm:~/linux server# ls
dm  install.sh  iw_devicemonitor_setup_7.11.1.38.tar.xz  iwdms.zip
root@iwdm:~/linux server# cp iw_devicemonitor_setup_7.11.1.38.tar.xz dm/
root@iwdm:~/linux server# cd dm
root@iwdm:~/linux server/dm# tar xvf iw_devicemonitor_setup_7.11.1.38.tar.xz
```

Рисунок 53 – Подготовка к установке dm

После распаковки файлов, запускаем файл `./setup.py install`, начнется процесс установки, соглашаемся с пользовательским соглашением. (Рисунок 54)

```

3.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в
Документации к ПО. Однако все Ваши требования относительно работоспособности ПО Вы можете
предъявлять только к своему лицензиару в рамках заключенного между вами лицензионного
договора.
3.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется
регулярно создавать резервные копии своих файлов.

4. Права на интеллектуальную собственность.

4.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной
собственности, воплощенные в ПО и /или любой предоставленной Вам документации, принадлежат
Правообладателю. Ничто в данном Соглашении не предоставляет Вам никаких прав на указанные
объекты интеллектуальной собственности иные, чем предоставленные Вам по Договору,
page 2, press enter for next page or q for end reading:
заклученному между Вами и Вашим лицензиаром.
4.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются
собственностью Правообладателя.
4.3. Вы не можете удалять или изменять уведомления об авторских правах или другие
проприетарные уведомления на любой копии ПО.

5. Права на информацию, доступ к которой получен Вами в рамках осуществления настоящего
Соглашения.

5.1. Вы соглашаетесь с тем, что Вам не принадлежат никакие права на любую информацию,
доступ к которой получен Вами в рамках осуществления настоящего Соглашения.
5.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы
работы, другая информация.
5.3. Указанная выше информация будет использоваться Вами только в целях осуществления
предоставленных Вам по договору прав на ПО без права использования указанной информации в
собственных интересах и за пределами Договора, заключенного между Вами и Вашим
лицензиаром.

6. Вы проинформированы о том, что ПО содержит открытое программное обеспечение,
распространяемое под определенными лицензиями, с которыми вы можете ознакомиться в файле
licenses.inf, распространяемом с ПО в составе дистрибутива. Каждый из предоставляемых
дистрибутивов ПО содержит файл licenses.inf, соответствующий составу конкретного
дистрибутива.

7. Контактная информация Правообладателя ООО «Лаборатория Инфовотч».

Тел./факс: +7(495)229-00-22
Коммерческий департамент: sales@infowatch.com
Служба технической поддержки: support@infowatch.com
Веб-сайт: www.infowatch.ru

Do you accept the license agreement?
input y or n:y

```

Рисунок 54 - принятие пользовательского соглашения

Затем, когда приняли пользовательское соглашение оставляем все параметры дефолтными и ждем конца установки и проверяем поды командой `kubectl get pods -n infowatch` (Рисунок 55)

```

root@iwdm:~/linux server/dm# kubectl get pods -n infowatch
NAME                                READY    STATUS    RESTARTS   AGE
activitytracker-central-7f6c49fc4b-12bzp    1/1      Running   0           2m21s
clickhouse-central-cf7f9f9cc-pk555         1/1      Running   0           3m30s
cluster-agent-2kkkd                         1/1      Running   0           41s
cluster-central-676db4d947-hv97d           1/1      Running   0           2m42s
comment-central-69f8476575-mc2cw           1/1      Running   0           3m1s
configstorage-central-648b64994f-jfzzh      1/1      Running   0           30s
datastorage-central-764658bdc9-vb227       1/1      Running   0           3m19s
department-central-54fd885f9-rdtxc         1/1      Running   0           2m50s
dicsyncdrvldap-central-7f5d7cb859-5hsn4     1/1      Running   0           3m7s
dicsyncdrvltm-central-56c877c559-rrfxs      1/1      Running   0           3m8s
dictionary-central-594bfd54df-hnxct        1/1      Running   0           3m12s
dossier-central-58c6c67778-r1vfq           1/1      Running   0           2m51s
epevents-central-7d6f7c6bd5-fr5k2          1/1      Running   0           2m38s
factsstorage-central-846c57967d-7lvs1       1/1      Running   0           2m53s
guard-central-7655b5fbbb-1c4h7             1/1      Running   0           30s
guiapps-central-5bc455b8c5-8657b           1/1      Running   0           29s
intcoordinator-central-797b665f64-5vqnj     1/1      Running   0           3m10s
investigations-central-575d698d6d-zjqjr     1/1      Running   0           2m17s
license-central-84f7988cff-42gm5            1/1      Running   0           28s
mailer-central-8666dcf4d7-m4wfw            1/1      Running   0           2m19s
nats-central-6569cf95c9-b7qjm              1/1      Running   0           3m23s
objects-central-547c6685f6-npc9h           1/1      Running   0           3m14s
policy-central-85cd445656-1dt8h            1/1      Running   0           3m3s
postgresql-central-ffd885db8-6jfsn         1/1      Running   0           3m26s
profile-central-7f7f9dbbb8-nlcfh            1/1      Running   0           2m57s
queryfacade-central-6f94684766-6r4n9       1/1      Running   0           2m48s
reiscatalog-central-67cb769585-hqsx2       1/1      Running   0           2m55s
report-central-6d4f966657-hqw2x            1/1      Running   0           2m34s
structure-central-d7b4c4b87-qnpw7          1/1      Running   0           3m5s
tarantool-central-f5fb57d8f-hkzsw          1/1      Running   0           3m28s
taskscheduler-central-8587d8c97b-5fdg8     1/1      Running   0           2m59s
textsearcher-central-5bdd5c57fb-6h8cm       1/1      Running   0           2m33s
textuploader-central-c6cd97fd6-1kvk9       1/1      Running   0           2m31s
tusker-central-bfddc59cb-glwwq             1/1      Running   0           3m17s
webgui-central-59db4746bc-5ptnt            1/1      Running   0           43s
workstation-central-5c9d54f4fb-ctg4v        1/1      Running   0           2m23s

```

Рисунок 55 – проверка подов

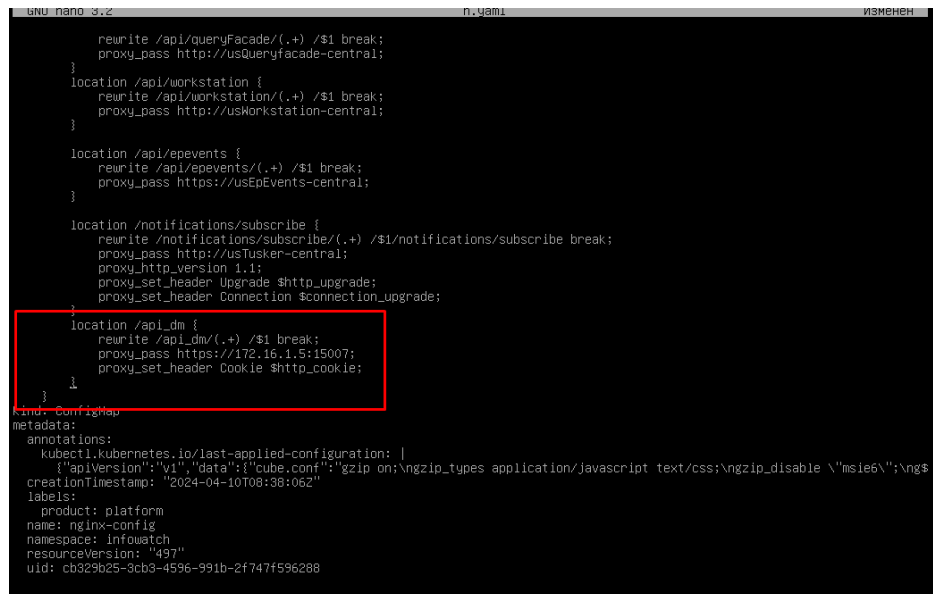
Вводим команду `kubectl get configmap nginx-config -o yaml -n infowatch > n.yaml` и редактируем файл `n.yaml` вносим новый сервер `server location`,

!!!важно формат .yaml не поддерживает табуляцию!!!

`nano n.yaml`

```
location /api_dm {  
    rewrite /api_dm/(.+) /$1 break;  
    proxy_pass https://SERVER_IP_ADRESS:15007;  
    proxy_set_header Cookie $http_cookie;  
}
```

} (Рисунок 56)



```
GNU nano 3.2 n.yaml ИЗМЕНЕН  
    rewrite /api/queryFacade/(.+) /$1 break;  
    proxy_pass http://usQueryFacade-central;  
}  
location /api/workstation {  
    rewrite /api/workstation/(.+) /$1 break;  
    proxy_pass http://usWorkstation-central;  
}  
  
location /api/epevents {  
    rewrite /api/epevents/(.+) /$1 break;  
    proxy_pass https://usEpEvents-central;  
}  
  
location /notifications/subscribe {  
    rewrite /notifications/subscribe/(.+) /$1/notifications/subscribe break;  
    proxy_pass http://usTusker-central;  
    proxy_http_version 1.1;  
    proxy_set_header Upgrade $http_upgrade;  
    proxy_set_header Connection $connection_upgrade;  
}  
  
location /api_dm {  
    rewrite /api_dm/(.+) /$1 break;  
    proxy_pass https://172.16.1.5:15007;  
    proxy_set_header Cookie $http_cookie;  
}  
↓  
kind: ConfigMap  
metadata:  
  annotations:  
    kubernetes.io/last-applied-configuration: |  
      {"apiVersion":"v1","data":{"cube.conf":"gzip on;\ngzip_types application/javascript text/css;\ngzip_disable \\"msie6\\";\ngzip_min_length 1000;\ngzip_proxies proxy;\ngzip_vary on;"},"kind":"ConfigMap","metadata":{"creationTimestamp":"2024-04-10T08:38:06Z"},"name":"nginx-config","namespace":"infowatch","resourceVersion":"497","uid":"cb329b25-9cb3-4596-991b-2f747f596288"}}
```

Рисунок 56 – редактирование файла `n.yaml`

После того как отредактировали и сохранили файл надо принять все изменения командой `kubectl apply -f n.yaml`, затем перезагрузить под `kubectl rollout restart deployment webgui-central -n infowatch` (Рисунок 57)

```
root@iwdm:~/linux server/dm# kubectl apply -f n.yaml  
configmap/nginx-config configured  
root@iwdm:~/linux server/dm# kubectl rollout restart deployment webgui-central -n infowatch  
deployment.apps/webgui-central restarted
```

Рисунок 57 – принятие изменений

После всех действий проверяем доступность нашего веб-интерфейса `dm`a`. важно понимать, что мы установили только веб-интерфейс(Рисунок 58)

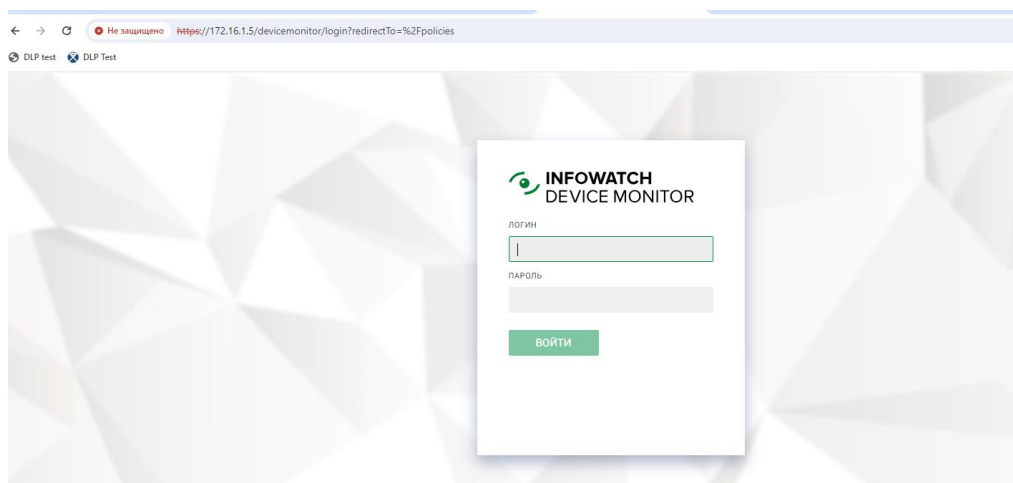


Рисунок 57 – веб-интерфейс iwdm

Дальше устанавливаем платформу. Переходим в директорию с файлами и делаем скрипт исполняемым командой `chmod +x ./install.sh`, далее запускаем этот скрипт, соглашаемся. Выбираем язык, принимаем лицензию, выбираем как будет разворачиваться (центральный/филиал), создаем новую базу данных, пишем ip где находится БД, остальное оставляем по дефолту, дальше ip адрес tm`а, токен (можно посмотреть в tm`е Управление > плагины > InfoWatch Device Monitor > токен) Дальше надо взять открытый ключ платформы.(Рисунок 58)

```
root@iwdm:~/linux server# ls
dm install.sh iw_devicemonitor_setup_7.11.1.38.tar.xz iwdms.zip
root@iwdm:~/linux server# chmod +x ./install.sh
root@iwdm:~/linux server# ./install.sh
Do you wish to install IW DMS? [Y/N]: y
Creating short link to log folder
Extracting DM Server files
IW DMS extracted.
Run primary configuration script? [Y/N]: y
Select the language of the installed server:
  press R for Russian language
  press E for English language
server language [R/E]: R
Please read license agreement
  press L - show license agreement
  press C - Accept and continue
  press Q - Quit
Your choice [L/C/Q]: C
Define type of installed server:
  press P for primary Server
  press S for secondary Server
server type [P/S]: P
PostgreSQL Database type:
  press N for create new database
  press U for updating an existing database
server type [N/U]: N
Enter PostgreSQL server name (host name or ip): 172.16.1.5
Enter PostgreSQL server communication port [5432]:
Enter database name [iwdm]:
Enter database user name [postgres]:
Enter database user password:
Enter pfx file path [/opt/iw/dmsserver/ssl.pfx]:
PFX file not exists. Create new? [Y/N]: y
Enter IW Traffic Monitor address: 172.16.1.4
Enter IW Traffic Monitor auth token: 1297bjrdyzzqa12duq6f
Enter platform public key file path:
```

Рисунок 58 – запуск скрипта

Чтобы взять открытый ключ надо сочетанием клавиш alt+f2 открыть другое окно консоли, прописать команду `kubectl get secret guardkeys-central -n infowatch -o 'go-template={{index .data "ec256-public.pem"}}' | base64 -d > /opt/iw/dmserver/bin/guard.pem` и сделать службу `iwdms` сделать исполняемой от пользователя `iwdms` командой `chown -f iwdms:iwdms /opt/iw/dmserver/bin/guard.pem` (Рисунок 59)

```
root@iwdm:~# kubectl get secret guardkeys-central -n infowatch -o 'go-template={{index .data "ec256-public.pem"}}' | base64 -d > /opt/iw/dmserver/bin/guard.pem
root@iwdm:~# chown -f iwdms:iwdms /opt/iw/dmserver/bin/guard.pem
root@iwdm:~#
```

Рисунок 59 – получение открытого ключа платформы

После получения открытого ключа, продолжаем установку, (Рисунок 60)

```
PFX file not exists. Create new? [Y/N]: y
Enter IW Traffic Monitor address: 172.16.1.4
Enter IW Traffic Monitor auth token: 1297bjrdyzzqa12duq6f
Enter platform public key file path:
Platform public key file is not set. Later you should create file '/opt/iw/dmserver/bin/guard.pem' manually and restart iwdms daemon. Continue? [Y/N]: y
```

Рисунок 60 – продолжение установки

Дальше, чтобы приходили события нужно установить сертификат с `tm`a` на `dm`. Чтобы было проще, подключаемся с `astra-cli` по `ssh` к `iwtm`, ищем директорию в которой находится сертификат, на сервере `tm`a` открываем файл по пути `/opt/iw/tm5/etc/xapi.conf` в секции `ThriftServers` надо найти параметр `TrustedCertificatesPath`, там будет указан дальнейший путь (Рисунок 61)

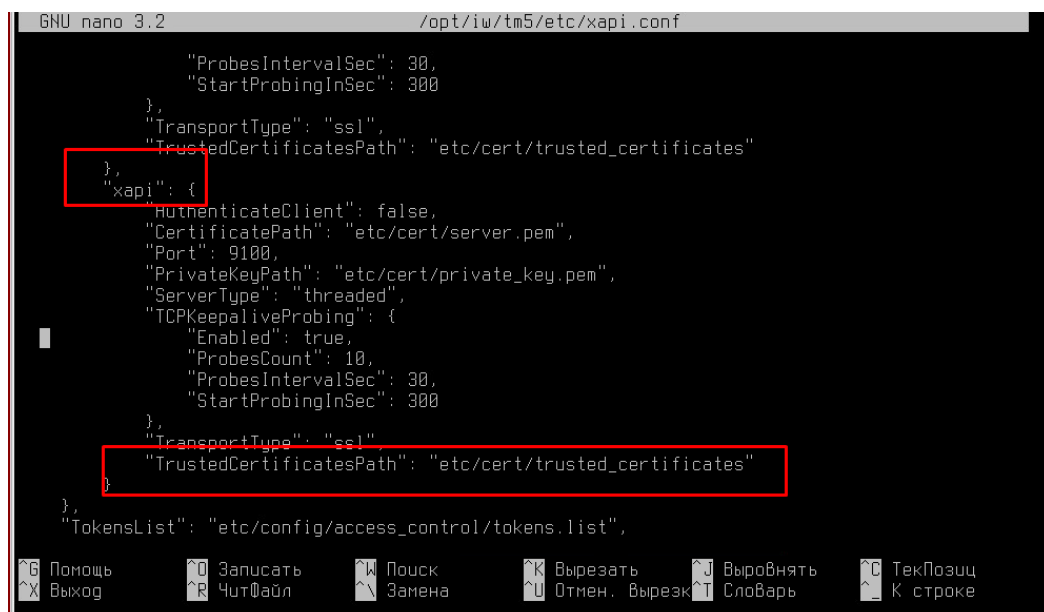


Рисунок 61 – просмотр директории

Надо обратить внимание на то что указан относительный путь, поэтому полный путь будет `/opt/iw/tm5/cert/trusted_certificates`, последнее и есть, то что нам нужно просмотреть и скопировать (Рисунок 62)

```

locadm@iwtm:~$ cat /opt/iw/tm5/etc/cert/trusted_certificates
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAIIsUMjTEPwZHMA0GCSqGSIb3DQEBCwUAMF8xCzAJBgNV
BAYTA1JVMQ8wDQYDVQQIDA2Nb3Njb3cxZDZANBgNVBACMBk1vc2NvdzESMBAGA1UE
CgwJSW5mb1dhbGNoMQswCQYDVQQLDAJURDENMA5GA1UEAwwEWEFQSTAEFw0xNjEy
MDEwNjQ2MjNaFw0yNjExMjMjNjNaMF8xCzAJBgNVBAYTA1JVMQ8wDQYDVQQQID
A2Nb3Njb3cxZDZANBgNVBACMBk1vc2NvdzESMBAGA1UECgwJSW5mb1dhbGNoMQsw
CQYDVQQLDAJURDENMA5GA1UEAwwEWEFQSTCCAS1wDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANZ6B4NjrQcgMMDKs02F1txv5cT7lQrhbbq375+I+W52Yqilg20h
20p1bRefSfoY9x8gd60u66nBqP7Z/7rgA2wv0WlykC1rdsTDMYRyj9fcD45TW8TMH
MwmyeVgEPkwVdcgDhvRo0gcht17BmLcQ2G8PzYxKmbHO/tWDX0ft+t/Eur7WaVsR
8xy+WPhSvJLzxga3BjzJ0W8Sm7Jc2vDU949TJS01PKvSEe7+VNh09xf2bWnyHNMR
Jevhbp5D0HAM+TN7LaRAF3F5e2icsy1d/Mc1Rn5xVzw6Hp6Ih82HDtD10H/jYxwB
zi0xGYX4JoCMnFiboHB0beA09U7EVenGGuMCAwEAAANQME4wHQYDVRR0BBYEFCSk
yhC1XUHL16qtSXNThNtCL/NrMB8GA1UdIwQYMBaAFCSkyhC1XUHL16qtSXNThNtC
L/NrMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAASx50qFHe/2gOLM
KYfHPdRaRqNvVlwVnhChb6xS5bBqnTm6YAB+BvPHAcnIjIdDSCpZ1LYMM3aSNh3c
a9fgztwDSNLof0uSJ4Hhx1xUr01cL9ja20stemAPooF+2/FRGmcc71TtoUGenpP8
GWR1KXuNNBbmfo++HnTWjedtpwzpjS2+p4XrhThx/2jXcrM8+R1bJ66/2pKUBPD
I3n+Ko0oIt6HaqCHewVEFLAjuTUPEz7aBtBc3M1uAIhJABTQrWx1SUX27r5Jfft
8M2+Zvi76MSJoPrHVdX43ekmWr/qCpCLJc1fjr+OMgC15/ns8oUy2A211A5f2VwH
qnSsX2g=
-----END CERTIFICATE-----

```

Рисунок 62 – копирование сертификата

Дальше разрываем соединение по ssh с iwtm и подключаемся к iwdm, прописываем nano tmca.crt, вставляем скопированный сертификат и сохраняем (Рисунок 63)

```

GNU nano 3.2 tmca.crt Изменён
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAIIsUMjTEPwZHMA0GCSqGSIb3DQEBCwUAMF8xCzAJBgNV
BAYTA1JVMQ8wDQYDVQQIDA2Nb3Njb3cxZDZANBgNVBACMBk1vc2NvdzESMBAGA1UE
CgwJSW5mb1dhbGNoMQswCQYDVQQLDAJURDENMA5GA1UEAwwEWEFQSTAEFw0xNjEy
MDEwNjQ2MjNaFw0yNjExMjMjNjNaMF8xCzAJBgNVBAYTA1JVMQ8wDQYDVQQQID
A2Nb3Njb3cxZDZANBgNVBACMBk1vc2NvdzESMBAGA1UECgwJSW5mb1dhbGNoMQsw
CQYDVQQLDAJURDENMA5GA1UEAwwEWEFQSTCCAS1wDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANZ6B4NjrQcgMMDKs02F1txv5cT7lQrhbbq375+I+W52Yqilg20h
20p1bRefSfoY9x8gd60u66nBqP7Z/7rgA2wv0WlykC1rdsTDMYRyj9fcD45TW8TMH
MwmyeVgEPkwVdcgDhvRo0gcht17BmLcQ2G8PzYxKmbHO/tWDX0ft+t/Eur7WaVsR
8xy+WPhSvJLzxga3BjzJ0W8Sm7Jc2vDU949TJS01PKvSEe7+VNh09xf2bWnyHNMR
Jevhbp5D0HAM+TN7LaRAF3F5e2icsy1d/Mc1Rn5xVzw6Hp6Ih82HDtD10H/jYxwB
zi0xGYX4JoCMnFiboHB0beA09U7EVenGGuMCAwEAAANQME4wHQYDVRR0BBYEFCSk
yhC1XUHL16qtSXNThNtCL/NrMB8GA1UdIwQYMBaAFCSkyhC1XUHL16qtSXNThNtC
L/NrMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAASx50qFHe/2gOLM
KYfHPdRaRqNvVlwVnhChb6xS5bBqnTm6YAB+BvPHAcnIjIdDSCpZ1LYMM3aSNh3c
a9fgztwDSNLof0uSJ4Hhx1xUr01cL9ja20stemAPooF+2/FRGmcc71TtoUGenpP8
GWR1KXuNNBbmfo++HnTWjedtpwzpjS2+p4XrhThx/2jXcrM8+R1bJ66/2pKUBPD
I3n+Ko0oIt6HaqCHewVEFLAjuTUPEz7aBtBc3M1uAIhJABTQrWx1SUX27r5Jfft
8M2+Zvi76MSJoPrHVdX43ekmWr/qCpCLJc1fjr+OMgC15/ns8oUy2A211A5f2VwH
qnSsX2g=
-----END CERTIFICATE-----

```

Рисунок 63 – создание сертификата на iwdm

Сохранили, отключились от iwdm. Переходим к iwdm проверяем сертификат и копируем в /usr/local/share/ca-certificates/ командой `sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt` (Рисунок 64)

```
locadm@iwdm:~$ ls
tmca.crt
locadm@iwdm:~$ sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt
[sudo] пароль для locadm:
locadm@iwdm:~$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

Рисунок 64 – добавление сертификата на dm`e

Далее делаем синхронизацию с iwtm и AD. Нажимаем на настройки, переходим в интеграции, добавляем интеграцию с iwtm и AD. При добавлении синхронизации с tm потребуется токен. Синхронизация с AD аналогична, tm с AD (Рисунок 65)

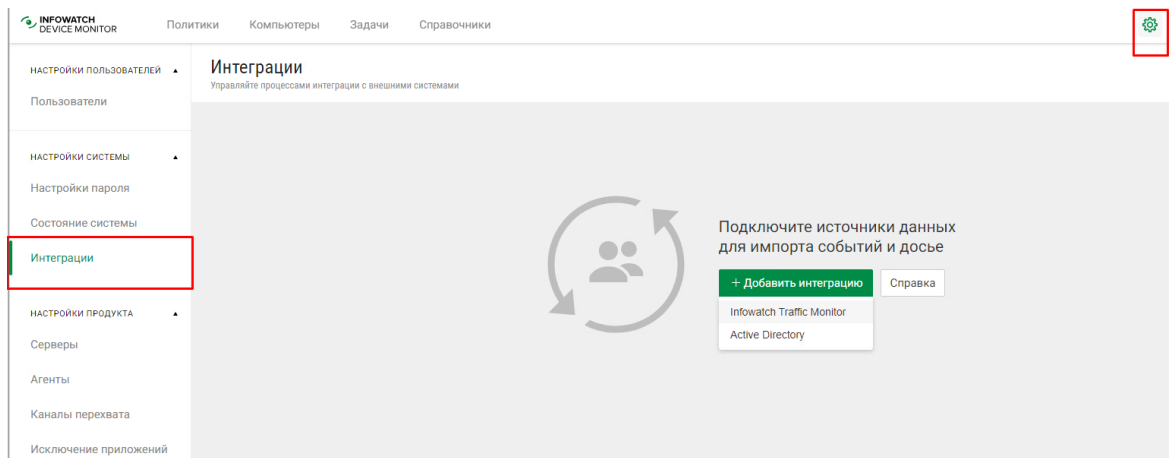


Рисунок 65 – добавление интеграций

Дальше устанавливаем агента через задачу распространения. Первым делом создаем политику. (Рисунок 66)

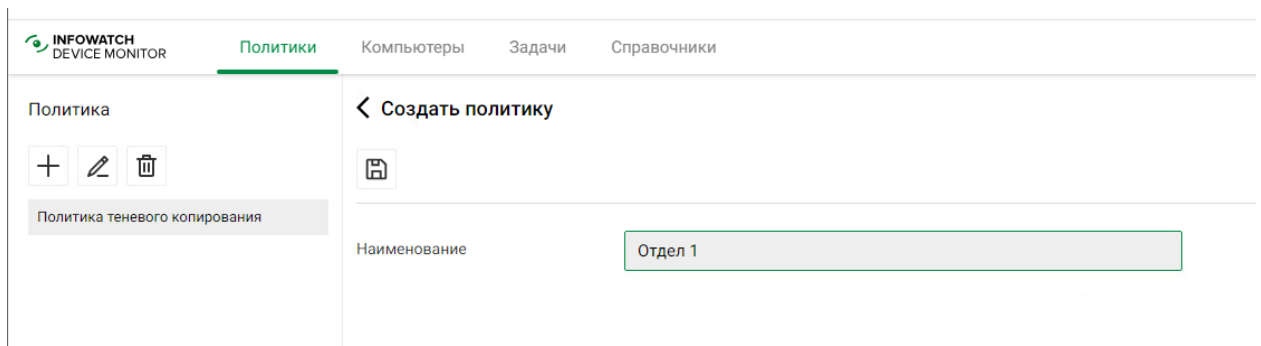


Рисунок 66 – создание политики

Чтобы установить агента через задачу распространения без ошибок, надо изменить запись в /etc/hosts на iwdm и astra-cli (Рисунок 67)


```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost
172.16.1.5   iwdm
172.16.1.7   astra-cli.aldpro.lab astra-cli
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Рисунок 67 – изменение записи в /etc/hosts на iwdm

Дальше изменяем запись на astra-cli (Рисунок 68)

```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost.localdomain localhost
127.0.1.1    astra-cli
172.16.1.7   astra-cli.aldpro.lab
172.16.1.5   iwdm
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Рисунок 68 – изменение записи на хостах astra-cli

Заходим в веб-интерфейс dm`a, создаем задачу (Рисунок 69)

INFOWATCH
DEVICE MONITOR

Политики Компьютеры **Задачи** Справочники

Задачи

Нет созданных задач

Создать задачу

Наименование: Задача распр

Описание:

Количество запусков задачи: 10 Каждые 10 минут

Точки распространения: ☒ Использовать все доступные точки распространения

Версия: 7.11.1

Количество попыток загрузки пакета: 10

Рисунок 69 – создание задачи

Дальше нажимаем +, выбираем компьютер из списка (Рисунок 70)

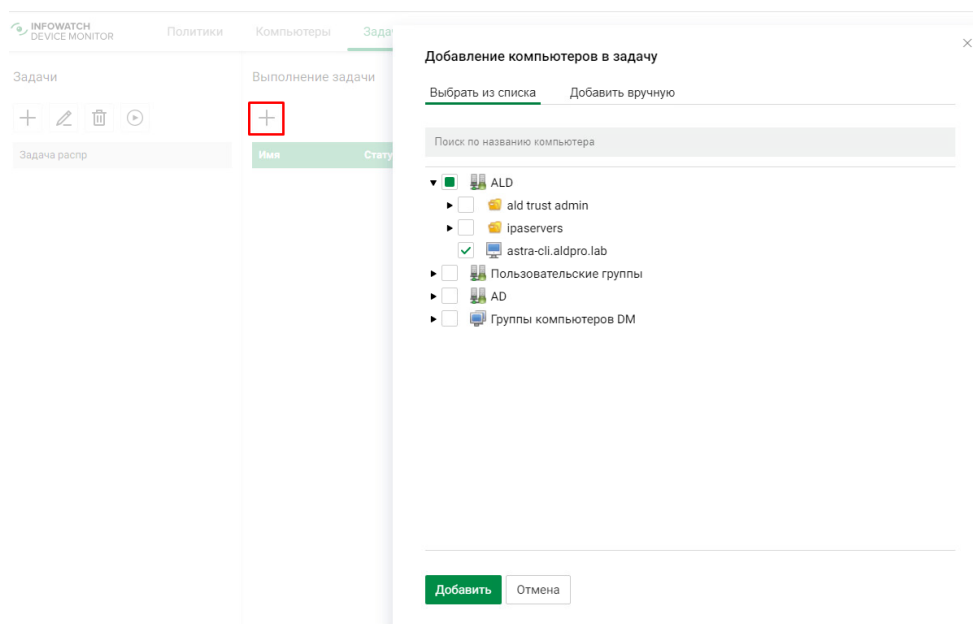


Рисунок 70 – добавление компьютера в задачу

После добавления компьютера запускаем задачу (Рисунок 71)

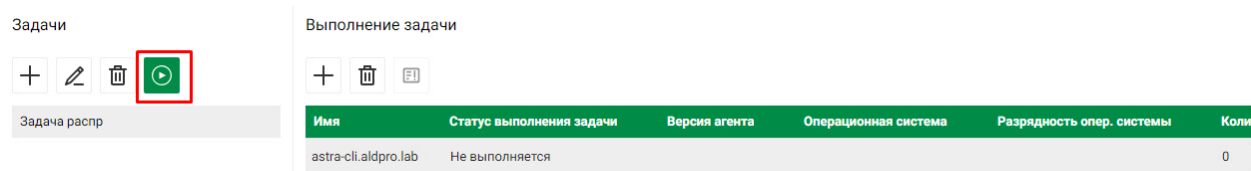


Рисунок 71 – запуск задачи распространения

Дальше вводим данные locadm, и пароль от него. После запуска пойдет выполнение задачи. (Рисунок 72)

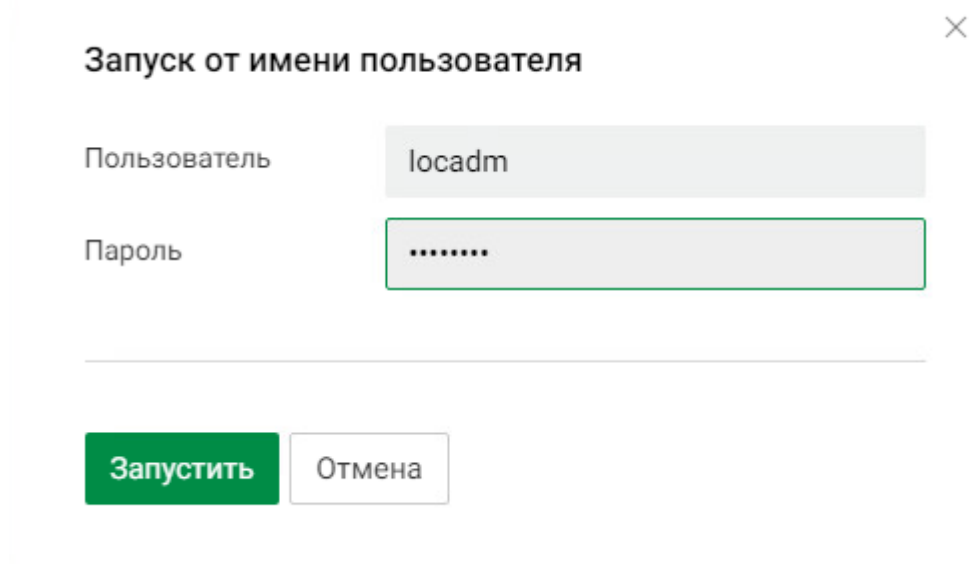


Рисунок 72 – запуск задачи

После выполнения задачи должно быть написано в статусе выполнена (Рисунок 73)

Имя	Статус выполнения задачи	Версия агента	Операционная система	Разрядность опер. системы
astra-cli.alopro.lab	✔ Выполнена		AstraLinux maximum(smolensk) 1.7.3	x64

Рисунок 73 – статус выполнения задачи

После задачи распространения создаем группу компьютеров и привязываем ее к политики которую создали, в нашем случае «отдел 1» . После создания добавляем компьютер с агентом. (Рисунок 74)

Рисунок 74 – создание группы компьютеров

Создадим в iwdm правило на перехват трафика (Рисунок 75)

Рисунок 75 – правило для перехвата трафика

В iwtm создадим проверочную политику. Заходим в Технологии > текстовые объекты, нажимаем создать пишем навание. (Рисунок 76)

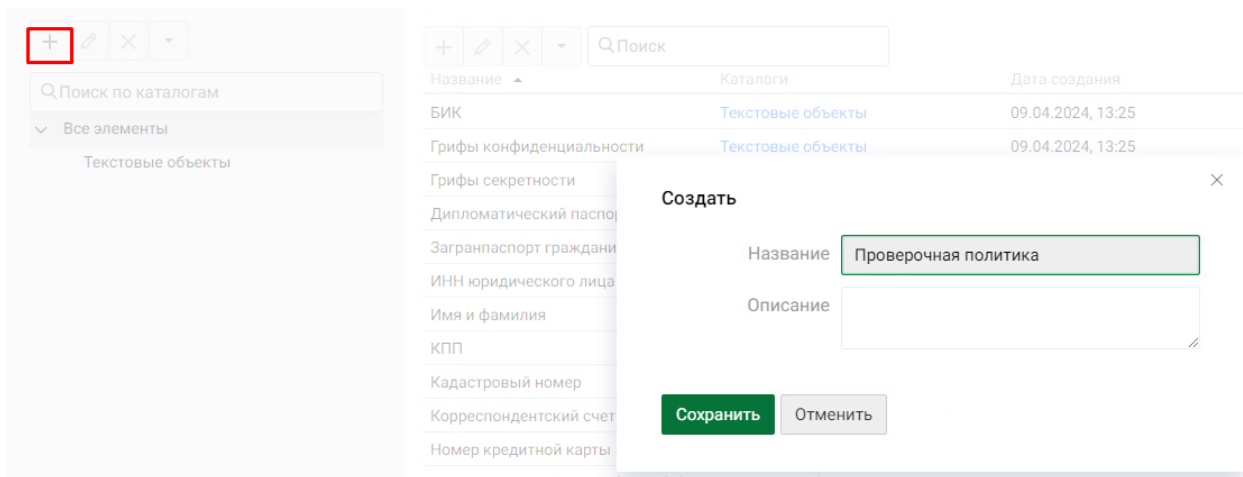


Рисунок 76 – создание проверочной политики

Далее нажимаем на проверочную политику, создаем текстовый объект (Рисунок 77)

Проверочная политика

Создание текстового объекта

Название: Проверочная политика

Страна: Российская Федерация

Описание:

Сохранить Отменить

Рисунок 77 – создание текстового объекта

Нажимаем изменить (Рисунок 78)

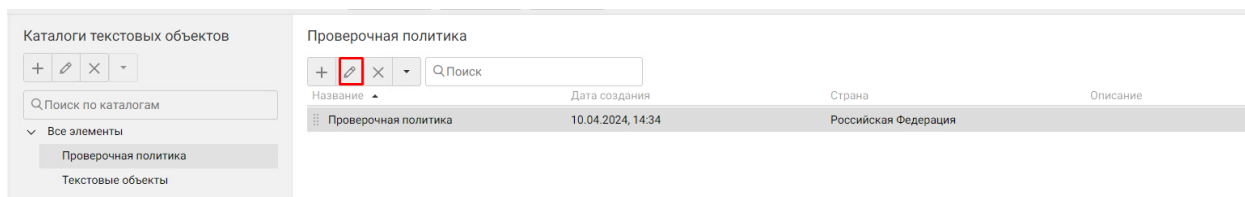


Рисунок 78 – изменение политики

Создаем шаблон и редактируем шаблон прописав строку «проверочная политика», сохраняем и надо будет еще раз сохранить !!!(Рисунок 79)

Статус ? ☒

Тип шаблона **Строка** Регулярное выражение

Строка Проверочная политика

Описание

Сохранить Отменить

Рисунок 79 – создание шаблона

Далее переходим «Объект защиты», создаем объект «проверочная политика» (Рисунок 80)

Создание объекта защиты

Категории Текстовые объекты 1 Эталонные документы Бланки Печати Выгрузки из БД Графические объекты

Каталоги текстовых объектов

Поиск по каталогам

Все элементы

☒ Проверочная полити...

☐ Текстовые объекты

Текстовые объекты

Поиск

Название	Дата создания	Страна	Описание
Проверочная политика	10.04.2024 14:34	Российская Федерация	

10

Создать Отменить ☐ Создать объект защиты на каждый выбранный элемент

Рисунок 80 – Добавление объекта защиты

Добавляем условие (Рисунок 81)

Создание объекта защиты

Название Введите название

Статус ? ☒

Элементы технологий Условия обнаружения

Добавить условие

Условие ☐ Детектировать в пределах элемента события ?

Проверочная политика
Каталог текстовых объектов

Порог встречаемости

1

Отрицание ? ☐

Описание

Создать Отменить

Рисунок 81 – условие для политики

Дальше переходим в политики, добавляем политику, создаем политику защиты данных, изменяем название, выбираем защищаемые данные (Рисунок 82)

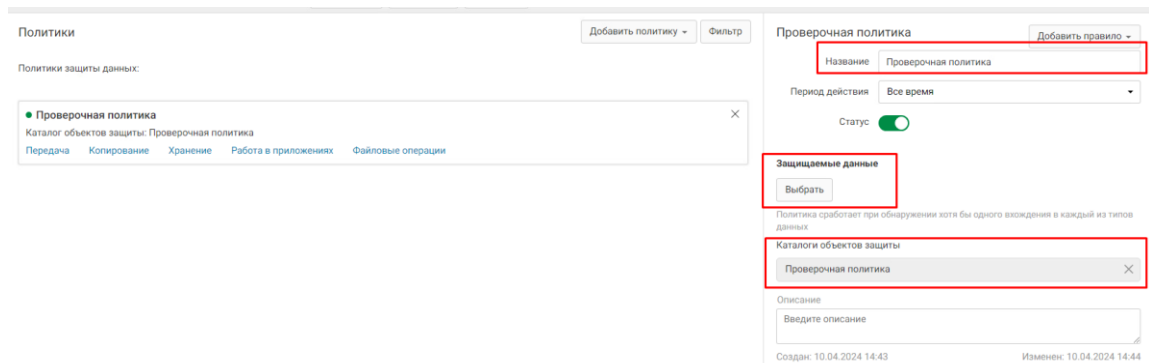


Рисунок 82 – создание проверочной политики

Добавляем правило на передачу, копирование и хранения (Рисунок 83)

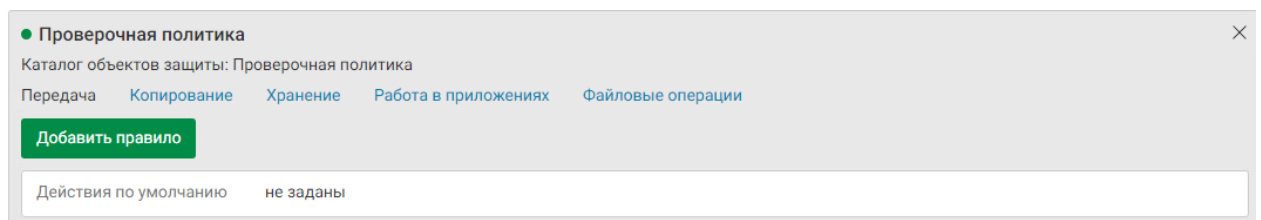


Рисунок 83 – добавление правила передачи

После того как создали правила, то применяем, чтобы политика вступила в силу (Рисунок 84)

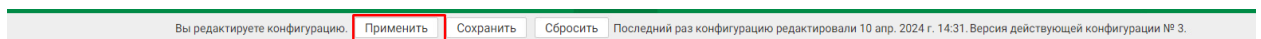


Рисунок 84 – применение конфигурации

После применения конфигурации, заходим на astra-cli (здесь клиент) в браузере ищем dlptest.com, переходим в http/https и пишем «проверочная политика» и отправляем (Рисунок 85)

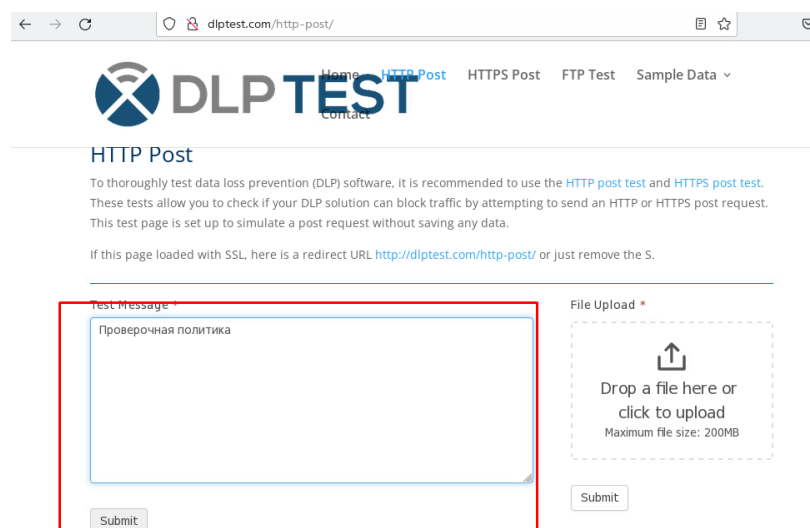


Рисунок 85 – проверка работоспособности политики

После отправки тестового сообщения ждем некоторое время. В iwtm заходим в события, запускаем запрос. (Рисунок 86)

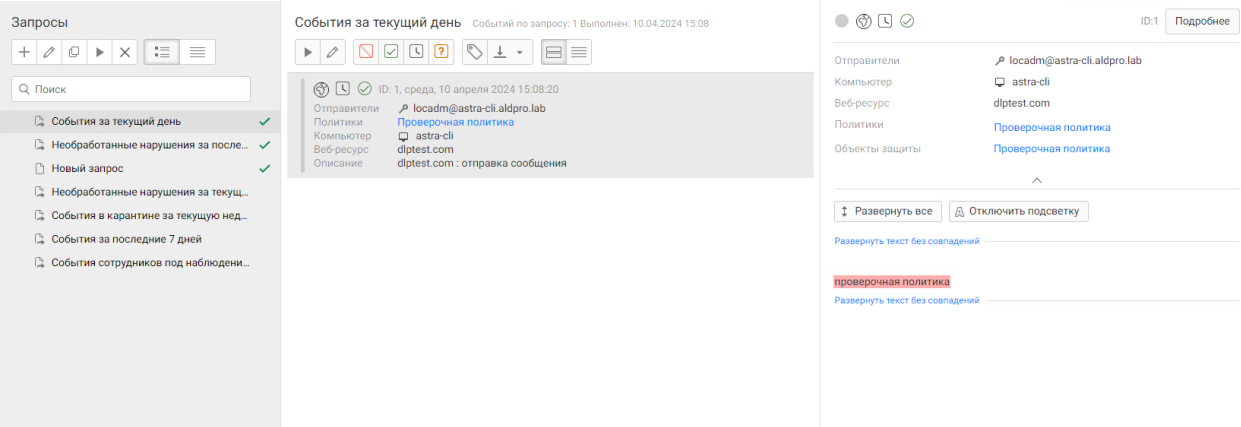


Рисунок 86 – проверка политики