

1) Транспортировка грузов например: kdO-666.Д или jfd-13.ЮШ:

[a-zA-z]{3,3}-([02-9]{0,1}[0-9]{1})|[0-9]{0,1}[0124-9]{1}|[0-5789]{1}|[0-9]{1}[0-9]

Для jfd-0013.ЮШ:

[a-zA-z]{3,4}-(1000|([1-9]\d\d\d)|(0[1-9]\d\d)|(00[023-9]\d)|(001[024-9])).[A-Я]{1,3}

Для kdO-0777.Д:

[a-zA-z]{3,4}-(1000|([1-9]\d\d\d)|(0[0-689]\d\d)|(07[0-689]\d)|(077[0-689])).[A-Я]{1,3}

2) Пропуск автомобилей: К333ОТ777 (77, 97, 99, 177, 197, 199, 777, 799):

K666OT13:

1. [АВЕМНОРСТУХ]\d{3}[АВЕКМНОРСТУХ]{2}(13|77|97|99|177|197|777|799)
2. K([0-5789]\d\d)|(6[0-5789]\d)|(66[0-5789])[АВЕКМНОРСТУХ]{2} (13|77|97|99|177|197|777|799)
3. K666[АВЕКМНОРСТУХ][АВЕКМНОРСТУХ] (13|77|97|99|177|197|777|799)
4. K666O[АВЕКМНОРСТУХ](13|77|97|99|177|197|777|799)
5. K666OT(77|97|99|177|197|777|799)

3) Для magnet-сылок:

1) magnet:[\?](A-aZ-z){1,})?([0-9]{1,})?((.*){1,})?([\r\n\t\s]{1,})?

2) magnet:[^\s]+urn[^\s]+

4) Для технических чертежей:

(Пример: ART-0096+ASD/66, VBN-1386-ВАЧ-345)

[ABCF-Z]{3}[\-](((0[0-9]{3})(1[0-9]{3})(2[0-9]{3})(3[0-9]{3})(4[0-2]{1}[0-9]{2}))(445[1-9]{1}))[+)(([A-Я]{3}[\-][0-9]{3})([A-Z]{3}[/][0-9]{2}))) ГОТОВАЯ!!!!!! ЛУЧШЕ ЭТА!!!!

[ABCF-Z]{3}[\-](((0001|5000)(0[0-9]{2}[2-9]{1})(1[0-9]{3})(2[0-9]{3})(3[0-9]{3})(4[0-2]{1}[0-9]{2}))(445[1-9]{1})(446[0-9]{1})(4[5-9]{1}\d{2}))[+)(([A-Я]{3}[\-][0-9]{3})([A-Z]{3}[/][0-9]{2}))) ГОТОВАЯ!!!!!! ЛУЧШЕ ВООБЩЕ ЭТА!!!!

[ABCF-Z]{3}[\-]((5000|(0[0-9]{2}[1-9]{1})(1[0-9]{3})(2[0-9]{3})(3[0-9]{3})(4[0-2]{1}[0-9]{2}))(445[1-9]{1})(44[6-9]{1}[0-9]{1})(4[5-9]{1}\d{2}))[+)(([A-Я]{3}[\-][0-9]{3})([A-Z]{3}[/][0-9]{2}))) ГОТОВАЯ!!!!!! **ЛУЧШЕ ВООБЩЕ ЭТА!!!!**

5) Для номера телефонов:

1) ((\+)?7|8)?([\s])?([-])?([\s])?(([])?(9){1}[0-9]{2})(D)?([\s])?([-])?([\s])?([0-9]{3})([\s])?([-])?([\s])?([0-9]{2})([\s])?([-])?([\s])?([0-9]{2})

Тоже самое что и 2, только вместо **([-])?** Ставиться так **([-]?)**

2) ((\+)?7|8)?([\s])?([-]?)?([\s])?(([])?(9){1}[0-9]{2})(D)?([\s])?([-?]?)?([\s])?([0-9]{3})([\s])?([-?]?)?([\s])?([0-9]{2})([\s])?([-?]?)?([\s])?([0-9]{2})

6) Для моделей кроссовок: ShowMakers 0444 35-45 .5 RU 5-11 UK

ShowMakers\s\d{4}\s(((3[5-9])|(4[0-4]))(.5?)|(45))\sRU
ShowMakers\s\d{4}\s ((([5-9])|(1[01]))(.5?)|\sUK

(ShowMakers|Chapionships|Markerwons|Lee-Broks>All-Mars)\s\d{4}\s(((3[5-9])|(4[0-4]))(.5?)|(45))\sRU

(ShowMakers|Chapionships|Markerwons|Lee-Broks>All-Mars)\s\d{4}\s ((([5-9])|(1[01]))(.5?)|\sUK

(ShowMakers|Chapionships|Markerwons|Lee-Broks>All-Mars)(\s\d{4}\s
(((3[5-9])|(4[0-4]))(.5?)|(45))\sRU)|(\d{4}\s ((([5-9])|(1[01]))(.5?)|\sUK)

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить потенциальную утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты доменов компаний: demo и demolab, демо, демолаб.

Возможные домены первого уровня: ru, su, org, lab, рф.

Детектирование только частей адресов (например @demo.ru) недопустимо.

Пример формата адресов: e-mail@demolab.ru , mail+tag@demo.lab ,
мой.меил@демолаб.рф , элепочта@демо.рф и т. п.

Разрешенные спецсимволы в корпоративной почте: _ . - +

([\w]{1,}[\s.+]?[-]?[_?])([\w]{1,}[\s.+]?[-]?[_?])
(@([DdДд][EeEe][MmMm][OoOo][\s.]?([LlЛл][AaAa][BbБб])?[.](ru|su|org|lab|рф)))

Чтобы настроить на работу экстрактор ABBYY FineReader Engine 11:

1. Удалите символьную ссылку `rm -f /opt/iw/tm5/bin/iw_image2text`.
2. Создайте символьную ссылку:
`ln -s /opt/iw/tm5/bin/iw_image2text_fre /opt/iw/tm5/bin/iw_image2text`

Если в качестве OCR-экстрактора используется ABBYY FineReader Engine 11, необходимо настроить лицензию ABBYY.

Для этого:

1. Введите полученные серийный номер и пароль в конфигурационный файл:
/opt/iw/tm5/etc/image2text_fre.conf
 - в поле **SerNum** введите серийный номер;
 - в поле **Pwd** введите пароль.
1. Скопируйте полученный файл с лицензией (формат .LocalLicense) в директорию:
/var/lib/ABBYY/SDK/11/Licenses.
3. Убедитесь, что у пользователя `iwtm` есть права на доступ к скачанному файлу.
4. Перезапустите сервис **iw_warpd**

Настройки OCR задаются в справочнике демона iw_bookworm в каталоге /opt/iw/tm5/etc/config-perm/bookworm:

- /opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml**
3. Включить использование OCR (`ocr_enabled="true"`).

Включаем OCR-экстрактор для анализа перехваченных изображений:

vi /opt/iw/tm5/etc/warpd.conf

Установить значение параметра: EnableOCR true

Для сохранения и выхода нажать Escape и набрать :wq и нажать Enter

Чтобы изменить ограничение на размер пересылаемого изображения:

2. Перейдите в директорию:

- vi /opt/iw/tm5/etc/image2text_fre.conf (для FineReader Engine 11)**
2. Отредактируйте параметры **MaxSizeInKb** (верхняя граница) и **MinSizeInKb** (нижняя граница). По умолчанию установлено 1536 КБ и 200 КБ соответственно.

Для сохранения и выхода нажать Escape и набрать :wq и нажать Enter

Для включения OCR на всех уровнях сразу (на уровне сервиса, типа события и на уровне протокола) необходимо в нижней строке файла ocr_custom.xml заменить `<ocr_options node="*" ocr_enabled="false">` на `<ocr_options node="*" ocr_enabled="true">`

Чтобы активировать быстрый режим обработки документов, в конфигурационном файле

/opt/iw/tm5/etc/image2text_fre.conf, расположенному в директории `/opt/iw/tm5/etc`, укажите путь до файла с настройками пользовательского профиля в параметре **"ABBYYProfile":"etc/FRProfile_fast.ini"** и сохраните изменения.

Установка IWTM на CentOS 7

Ip a – Проверить ip адреса

Ping ya.ru – проверить что пингуется, значит сеть работает

yum update – загрузить репозиторийные файлы (почти как в линуксе) при загрузке нажимать (y/d/n) и (y/n)

nmtui – заменить имя и ip адрес (edit connection – изменить ip адрес, set system hostname – изменить имя)

ping <название машины>

Через программу WinSCP скопировать на CentOS файлы

chmod +x iwtm-installer..... – сделать исполняемым файлом

./iwtm-installer..... – Установка IWTM

su – войти под root

iwtm stop

iwtm start/stop/enable/disable/sniffer

Резервная копия базы данных IWTM:

- 1) Создайте директорию для хранения файлов резервной копии:**
mkdir /opt/IWTM_Backup_Files

- 2. Создайте следующие поддиректории:**

```
mkdir /opt/IWTM_Backup_Files/postgres  
mkdir /opt/IWTM_Backup_Files/pgdata  
mkdir /opt/IWTM_Backup_Files/arch
```

- 3. Ввести команду iwtm stop**

4 скопируйте содержимое директории /u01/postgres/ в директорию

/opt/IWTM_Backup_Files/postgres

- скопируйте содержимое директории /u02/pgdata/ в директорию /opt/IWTM_Backup_Files/pgdata
- скопируйте содержимое директории /u02/pgdata1/ в директорию /opt/IWTM_Backup_Files/pgdata1
- скопируйте содержимое директории /u02/arch/ в директорию /opt/IWTM_Backup_Files/arch

Чтобы восстановить базу данных с помощью создания новой базы данных:

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД;

2. Остановите сервисы PostgreSQL:

service postgresql-9.6 stop

service pgagent-9.6 stop

Чтобы остановить на IWTM с 1 дня ввести команду:

service postgresql stop

service pgagent stop

4. Выполните следующие шаги:

- a. Удалите все содержимое каталогов /u01/postgres/, /u02/pgdata/, /u02/pgdata1/, /u02/arch/**
- b. Скопируйте содержимое директории /opt/IWTM_Backup_Files/postgres в директорию /u01/postgres/**
- c. Скопируйте содержимое директории /opt/IWTM_Backup_Files/pgdata/ в директорию /u02/pgdata/**
- d. Скопируйте содержимое директории /opt/IWTM_Backup_Files/pgdata1/ в директорию /u02/pgdata1/**
- e. Скопируйте содержимое директории /opt/IWTM_Backup_Files/arch/ в директорию /u02/arch/**

5. Проверьте права. При необходимости, измените их:

chown postgres /u01/postgres/ -R

chown postgres /u02/pgdata/ -R

chown postgres /u02/pgdata1/ -R

chown postgres /u02/arch/ -R

6. Запустите базу данных:

service postgresql-9.6 start

service pgagent-9.6 start

service postgresql stop

service pgagent stop

Чтобы подключиться к удаленной базе данных IWDM, необходимо в файле pg_hba.conf, добавить ip адрес компьютера, где установлена сама БД!!!!!!!!!!!!!!

```
ERROR! Unknown daemons name: iw_xap
xt_ts.service
Available daemons:
iw_adlibitum
iw_agent
iw_analysis
iw_blackboard
iw_bookworm
iw_capstack
iw_cas
iw_configerator
iw_deliver
iw_icap
iw_icap_buf
iw_image_autoling
iw_indexer
iw_is
iw_kicker
iw_licensed
iw_luaengined
iw_messed
iw_pas
iw_proxy_http
iw_proxy_icq
iw_proxy_smtp
iw_qmover_client
iw_qmover_server
iw_sample_compiler
iw_smtpd
iw_sniffer
iw_system_check
iw_tech_tools
iw_text_autoling
iw_updater
iw_warpd
iw_x2db
iw_x2x
iw_xapi_puppy
iw_xapi_xapi
```



/opt/iw/tm5/etc/sniffer.conf

ListenHost. 192.168.30.45.

ListenPort – 80

Архивирование файлов в Astra Linux

Зайти по админом: sudo -s

Архивирование файлов

tar -cvf **u1postgres.tar.gz** /u1/postgres/

u1 – название файла

/u1/ – файлы которые нужно закинуть в архив

Разархивирование файла

tar -xvf **u1postgres.tar.gz** -C /u1/postgres

Сжать архив:

tar -zcvf **u1postgres.tar.gz** /u1/postgres/

c - создать архив в linux

d - сравнить файлы архива и распакованные файлы в файловой системе

j - сжать архив с помощью Bzip

z - сжать архив с помощью Gzip

r - добавить файлы в конец архива

t - показать содержимое архива

u - обновить архив относительно файловой системы

x - извлечь файлы из архива

v - показать подробную информацию о процессе работы

f - файл для записи архива

-C - распаковать в указанную папку

```
/opt/iw/tm5/etc/certification/  
openssl pkcs12 -clcerts -nokeys -in CA.pfx -out CA.tmp.crt  
openssl pkcs12 -in Server.pfx -out Server.key.pem -nocerts -nodes  
openssl pkcs12 -clcerts -nokeys -in Server.pfx -out Server.tmp.crt
```

sudo service nginx stop

```
sudo nano /etc/nginx/conf.d/iwtm.conf  
ssl_certificate /opt/iw/tm5/etc/certification/Server.tmp.crt  
ssl_certificate_key /opt/iw/tm5/etc/certification/Server.key.pem  
ssl_client_certificate /opt/iw/tm5/etc/certification/CA.tmp.crt;  
ssl_verify_client on;
```

Удалить listen 80 ssl;
sudo service nginx start

ПОДКЛЮЧЕНИЕ ПО SSH МЕЖДУ ASTRA LINUX (НАПРИМЕР: IWTM-NODE И IWTM-DB)

Пример задания: сгенерируйте RSA-ключ на IWTM DB и настройте межсерверный доступ по SSH с IWTM Node на IWTM DB.

- 1) На машине IWTM DB открыть терминал и ввести команду: **ssh-keygen**;
- 2) Первый раз нажать Enter;
- 3) Во второй раз ввести пароль;
- 4) Ввести команду: **cd .ssh/**;
- 5) Ввести команду: **cat «имя файла с ключом»: cat id_rsa** или **cat id_rsa.pub**
- 6) На первой машине ввести команду: **nano authorized_keys** и вставить открытый ключ;
- 7) Скопировать закрытый ключ **id_rsa** на вторую машину;
- 8) На второй машине создать каталог **ssh: mkdir .ssh/**;
- 9) Перейти в данный каталог: **cd .ssh/**;
- 10) Ввести название файла любое (например: **key.private**): **nano key.private**;
- 11) Вставить закрытый ключ;
- 12) Далее ввести команду: **chmod 0700 key.private**;
- 13) На первой машине: **chmod 0700 authorized_keys**;
- 14) Подключиться по SSH, ввести команду: **ssh -i key.private «имя пользователя@ip адрес»**.

VIPNET

Установка Client на Astra Linux

Скачать на флешку папку: **gost_ru_gui** и ключ

Создать папку: **mkdir install**

Скопировать в эту папку папку **gost_ru_gui** и ключ

sudo gpkg -i vipnetclient-gui_s_gost_ru_amd64_4.12.2-12236.deb

Cluster

failover stop

failover config edit

failover config mode cluster и выбрать Yes

failover start

Пример:

1 координатор

eth0 – 192.18.30.2/27

eth1 – 172.21.30.1/26

eth2 – 192.168.30.1/24

[channel] eth0 – 192.18.30.2/27

[channel] eth1 – 172.21.30.1/26

[sendconfig] – 192.168.30.2/24

2 координатор (Cluster)

eth0 – 192.18.30.2/27

eth1 – 172.21.30.1/26

eth2 – 192.168.30.2/24

[channel] eth0 – 192.18.30.2/27

[channel] eth1 – 172.21.30.1/26

[sendconfig] – 192.168.30.1/24

Задание 3.2. Policy manager

3.2.1 Создать шаблон политики безопасности, т. е. определить сетевой фильтр в соответствии с которым Net2-Astra-Cli должен быть доступен по SSH только с узлов Admin CA и внешней сети (фильтр защищенной сети) для работоспособности соединения с Net3-Open.

Назначить сформированный шаблон сетевым узлам, отправить политику безопасности на сетевой узел.

Зафиксировать результат (скриншотами) через журнал отправки и применения политик безопасности, на узлах в Мониторе просмотреть списки сетевых фильтров.

ОТВЕТ:

Имя: 3.2.1

Сетевые узлы: User3

Локальные фильтры открытой сети:

Имя: С незащищенной сети

Действие: Пропускать трафик

Источники: IP адрес Net3-Open

Назначения: Мой узел

Протоколы: 22

Фильтры защищенной сети:

Имя: С защищенной сети

Действие: Пропускать трафик

Источники: Мой узел

Назначения: User3

Протоколы: 22

3.2.2 Создать шаблон политики безопасности для запрета на использование популярных соцсетей vk.com, facebook.com, tiktok.com с узлов пользователей сети (клиенты).

Применить политику к клиентам.

Зафиксировать результат (скриншотами) настройки и проверки.

ОТВЕТ:

Имя: 3.2.2

Сетевые узлы: выбрать все

Локальные фильтры открытой сети:

Имя: Запрет на использование соц. сетей

Действие: Блокировать трафик

Источники: Мой узел

Назначения: DNS-имя и ввести «vk.com, facebook.com, tiktok.com».

3.2.3 Создать шаблон политики безопасности для возможности подключения защищенных и незащищенных узлов своей сети по протоколу RDP к AdminCA. Также необходимо включить RDP доступ на данном узле. Применить политику к устройствам. Зафиксировать результат (скриншотами) настройки и проверки.

ОТВЕТ:

Имя 3.2.3

Сетевые узлы: AdminCA

Локальные фильтры открытой сети:

Имя: С незащищенной сети

Действие: Пропускать трафик

Источники: IP адрес не защищенного узла

Назначения: Мой узел

Протоколы: 3389

Фильтры защищенной сети:

Имя: С защищенной сети

Действие: Пропускать трафик

Источники: другие узлы

Назначения: Мой узел

Протоколы: 3389

ВКЛЮЧИТЬ RDP НА ADMINCA!!!!!!