

Софт

- [Guacamole](#)
- [Proxmox + Grafana + Prometheus](#)
- [MSSQL](#)
 - [Обслуживание 1C MSSQL](#)
 - [MSSQL борщ](#)
- [Outlook](#)
- [Windows](#)
- [RDP](#)
- [LVM](#)
- [Portainer.io](#)
- [Работа с жесткими дисками в Linux](#)
- [Программирование C](#)
- [FFmpeg](#)
- [Zabbix](#)
- [Proxmox mail gateway](#)
- [ProFTPD](#)
- [Postgres 1C ZFS](#)
- [IPTables](#)
- [ZFS](#)
- [OpenVPN](#)
- [Nextcloud](#)
- [Linux Server](#)
- [Linux Desktop](#)
- [PfSense](#)
- [Ikev2 ipsec/wireguard/3proxy/clamav updater 4 in 1](#)
- [Proxmox Virtual Environment](#)

- [Перестала запускаться MariaDB](#)
- [OpenConnect VPN Cisco](#)
- [dig](#)
- [Sing-box](#)

Guacamole

Выключить TOTP для определённого пользователя

Внутри контейнера с postgres от guaca

```
su postgres  
psql  
\c guacamole_db  
select * from guacamole_user_attribute;  
update guacamole_user_attribute set attribute_value='totpdisabled' where user_id=<userid> and  
attribute_name='guac-totp-key-secret';
```

Решение взято [тут](#)

[Шпаргалка postgre](#)

Proxmox + Grafana + Prometheus

Начало

<https://www.dmosk.ru/miniinstruktions.php?mini=prometheus-stack-docker>

<https://community.hetzner.com/tutorials/proxmox-prometheus-metrics>

MSSQL

Обслуживание 1С MSSQL

Материалы по вопросу

<https://plast.com.kz/config-sql-server-1c-maintenance-plans/>

<https://its.1c.ru/db/metod8dev#content:5837:hdoc:p4>

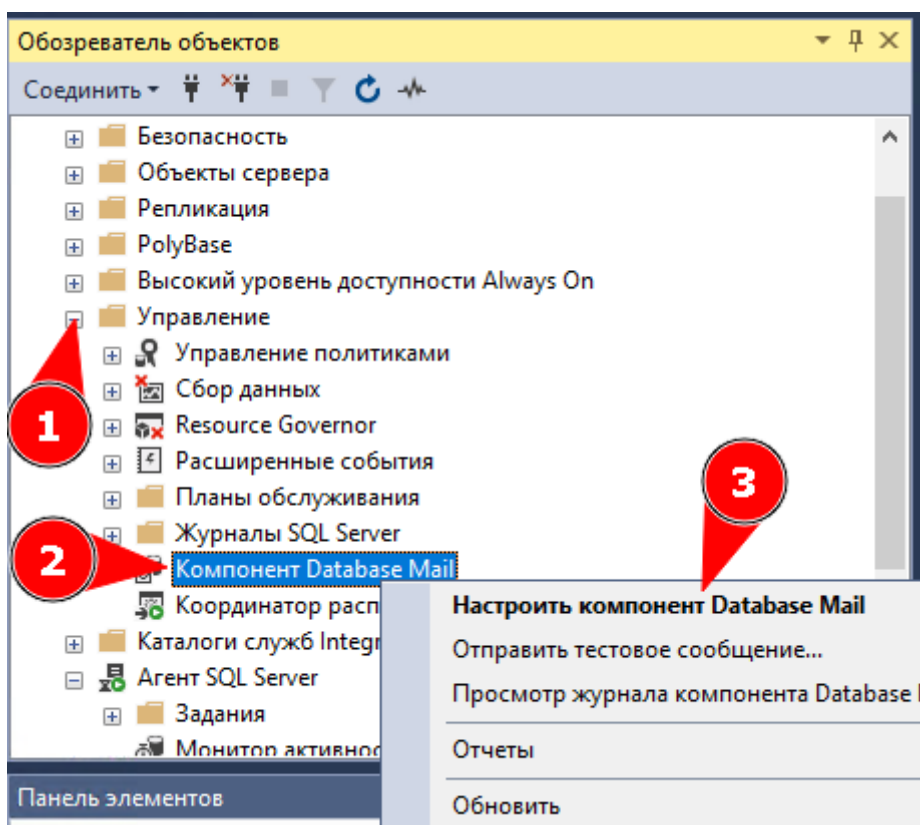
https://interface31.ru/tech_it/2012/08/obslyzhivanie-baz-1s-v-ms-sql-server-chast-2.html

https://interface31.ru/tech_it/2012/02/obslyzhivanie-baz-1s-v-ms-sql-server-chast-1.html

<https://forum.infostart.ru/forum86/topic289736/>

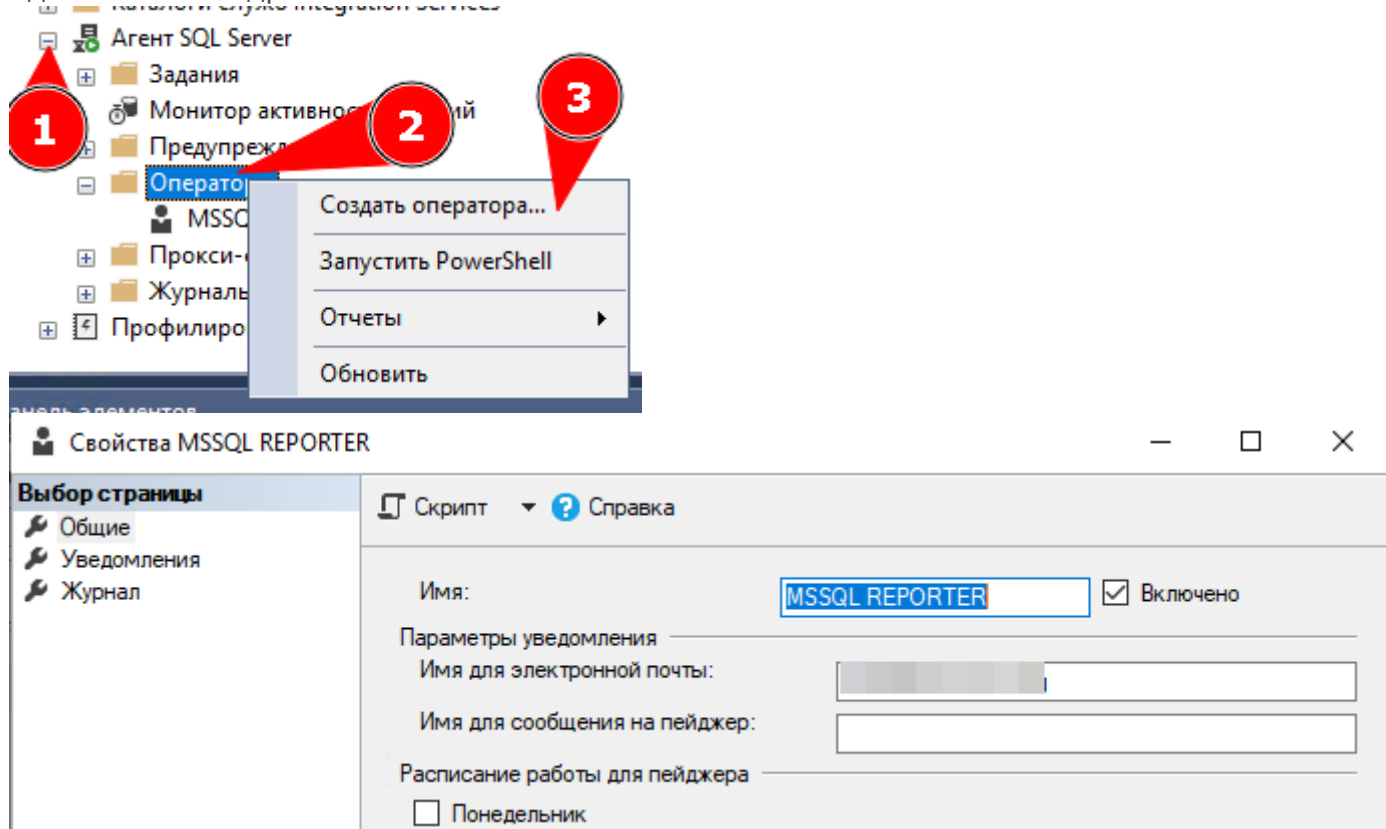
<http://www.gilev.ru/forum/viewtopic.php?f=15&t=1844>

Email уведомления

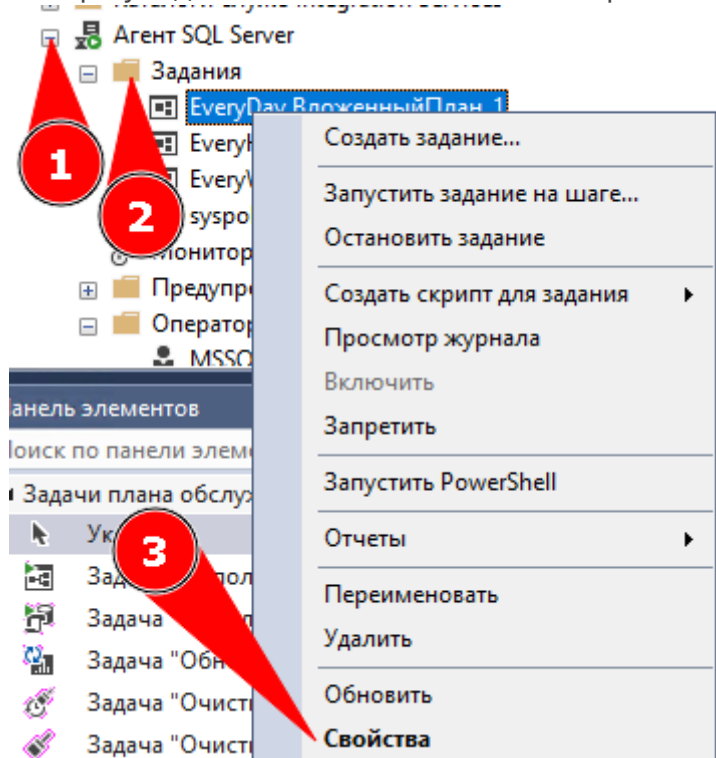


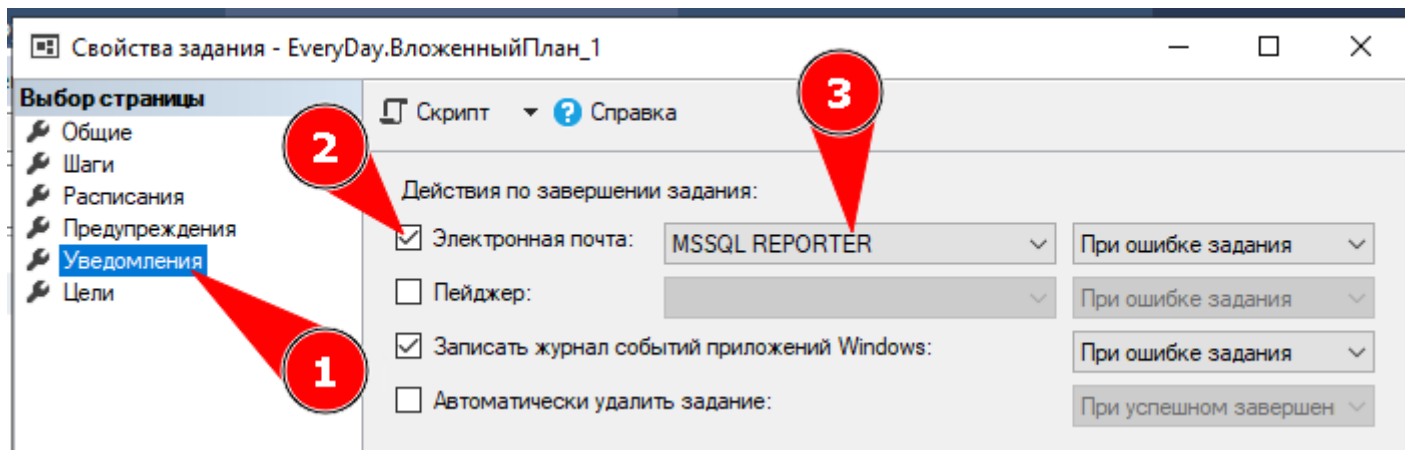
Нужно ввести параметры почты **от имени кого** будут отправлены уведомления.

Заведите оператора, укажите адрес **куда** надо направлять уведомления. В моём случае это один и тот же адрес.

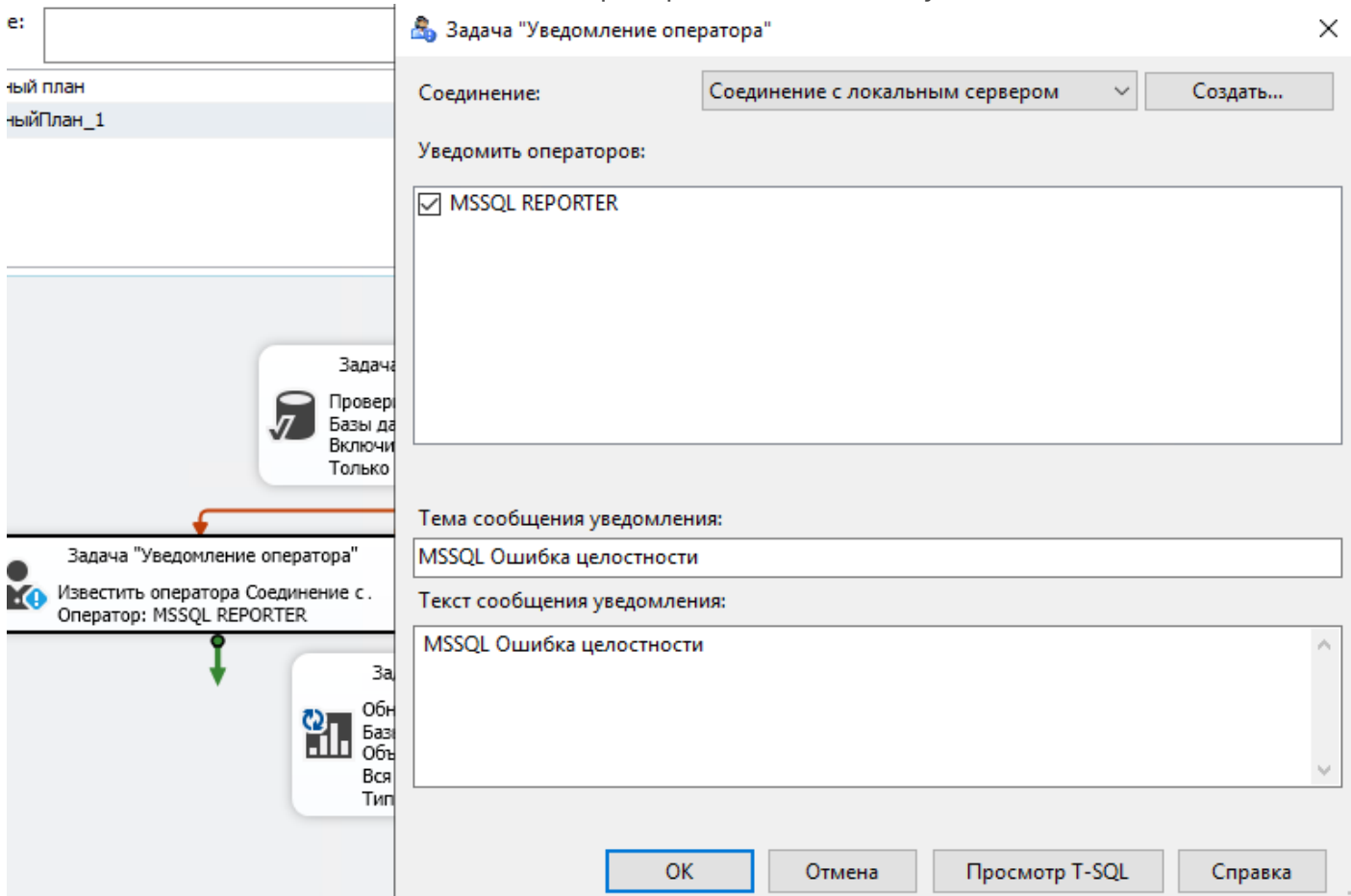


Теперь уведомление можно включить при ошибке выполнения плана обслуживания:





Или добавив действие "Уведомление оператора" сам план обслуживания:



MSSQL борщ

Включить индексирование таблиц 8.3.22

Реорганизация индексов вызывала ошибку по причине: **поскольку отключена блокировка на уровне страницы**

```
USE [basename]
GO

DECLARE @object_schema VARCHAR(256);
DECLARE @object_name VARCHAR(256);
DECLARE @index_name VARCHAR(256);

DECLARE db_cursor CURSOR FOR
SELECT OBJECT_SCHEMA_NAME(object_id) AS object_schema,
       OBJECT_NAME(object_id)      AS object_name,
       name                        AS index_name
FROM   sys.indexes
WHERE  allow_page_locks = 0 AND OBJECT_SCHEMA_NAME(object_id) != 'sys';

OPEN db_cursor;
FETCH NEXT FROM db_cursor INTO @object_schema, @object_name, @index_name;
WHILE @@FETCH_STATUS = 0
BEGIN

    EXEC ('ALTER INDEX ' + @index_name + ' ON ' + @object_schema + '.' + @object_name + ' SET
(ALLOW_PAGE_LOCKS = ON)');

    FETCH NEXT FROM db_cursor INTO @object_schema, @object_name, @index_name;

END;
CLOSE db_cursor;
```

```
DEALLOCATE db_cursor;
```

Взято [отсюда](#)

Проверить фрагментацию MSSQL

```
DECLARE @db_id SMALLINT;

SET @db_id = DB_ID(N'MyBaseSQL');

IF @db_id IS NULL
BEGIN;
    PRINT N'Неправильное имя базы';
END;

ELSE
BEGIN;
    SELECT
        object_id AS [ID объекта],
        index_id AS [ID индекса],
        index_type_desc AS [Тип индекса],
        avg_fragmentation_in_percent AS [Фрагментация в %]
    FROM sys.dm_db_index_physical_stats(@db_id, NULL, NULL, NULL , 'LIMITED')
    ORDER BY [avg_fragmentation_in_percent] DESC;
END;

GO
```

Взято [отсюда](#)

Остановить резервное копирование MSSQL

В SQL запроснике найти PID резервного копирования:

```
SELECT session_id as SPID, command, a.text AS Query, start_time, percent_complete,  
dateadd(second,estimated_completion_time/1000, getdate()) as estimated_completion_time  
FROM sys.dm_exec_requests r CROSS APPLY sys.dm_exec_sql_text(r.sql_handle) a  
WHERE r.command in ('BACKUP DATABASE','RESTORE DATABASE')
```

И завершить процесс (тут же, в запроснике):

```
KILL НомерПроцесса
```

Шифрованные копии MSSQL

Зашифровать копии

Создайте учетные данные SQL Server. Для создания учетных данных SQL Server подключитесь к ядру СУБД, откройте новое окно запроса, скопируйте в него следующий пример и нажмите кнопку **Выполнить**. (Я этот шаг пропустил)

```
CREATE CREDENTIAL mycredential  
WITH IDENTITY= 'mystorageaccount' - this is the name of the storage account you specified when creating a  
storage account  
, SECRET = '<storage account access key>' - this should be either the Primary or Secondary Access Key for the  
storage account
```

Создайте главный ключ базы данных. Выберите пароль для шифрования копии главного ключа базы данных, которая будет храниться в базе данных. Подключитесь к ядру СУБД, откройте новое окно запроса, скопируйте в него следующий пример и нажмите кнопку **Выполнить**. (Устанавливаете мастер ключ шифрования)

```
-- Creates a database master key.  
-- The key is encrypted using the password "<master key password>"  
USE Master;
```

```
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<master key password>';
GO
```

Создайте сертификат резервной копии. Создайте сертификат резервной копии в базе данных master. Вставьте следующий пример в окно запроса и нажмите **Выполнить**.

```
USE Master;
GO
CREATE CERTIFICATE MyTestDBBackupEncryptCert
    WITH SUBJECT = 'MyTestDBBackupEncryptCert ';
GO
```

Выполните резервное копирование базы данных. Укажите алгоритм шифрования и сертификат для использования. Скопируйте следующий пример в окно запроса и нажмите кнопку **Выполнить**.

```
BACKUP DATABASE [MyTestDB]
TO URL = N'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Backup\MyTestDB.bak'
WITH
    CREDENTIAL 'mycredential' - this is the name of the credential created in the first step.
    ,COMPRESSION
    ,ENCRYPTION
    (
        ALGORITHM = AES_256,
        SERVER CERTIFICATE = MyTestDBBackupEncryptCert
    ),
    STATS = 10
GO
```

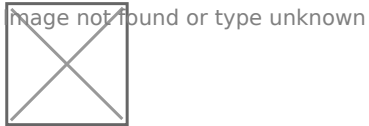
Расшифровать копии

Взято [отсюда](#)

При попытке прочитать содержимое зашифрованной копии будет выдана ошибка “Cannot find server certificate with thumbprint”

```
Msg 33111, Level 16, State 3, Line 1
Cannot find server certificate with thumbprint '0xE11A199C1059C6F1E0223B56581CDCF3F043DFE8'.
Msg 3013, Level 16, State 1, Line 1
RESTORE DATABASE is terminating abnormally.
```

Сертификаты хранятся тут:



Выгрузите информацию со старого сервера вот таким запросом.

```
USE Master
go
BACKUP CERTIFICATE DB_Encrypt_Cert
TO FILE = 'Z:\Backup\DB_Encrypt_Cert.cer'
WITH PRIVATE KEY(
FILE = 'Z:\Backup\DB_Encrypt_Cert.prvk',
ENCRYPTION BY PASSWORD = 'StrongPassword'
)
```

Загрузите в новый вот таким:

```
CREATE CERTIFICATE DB_Encrypt_Cert
FROM FILE = 'E:\MSSQL\DB_Encrypt_Cert.cer'
WITH PRIVATE KEY(
FILE = 'E:\MSSQL\DB_Encrypt_Cert.prvk',
DECRYPTION BY PASSWORD = '7Hx81GbNaxHP65rsSfiKAaVvKvN5beUY'
)
```

Теперь можно восстанавливать базу на новом сервере как обычно.

Outlook

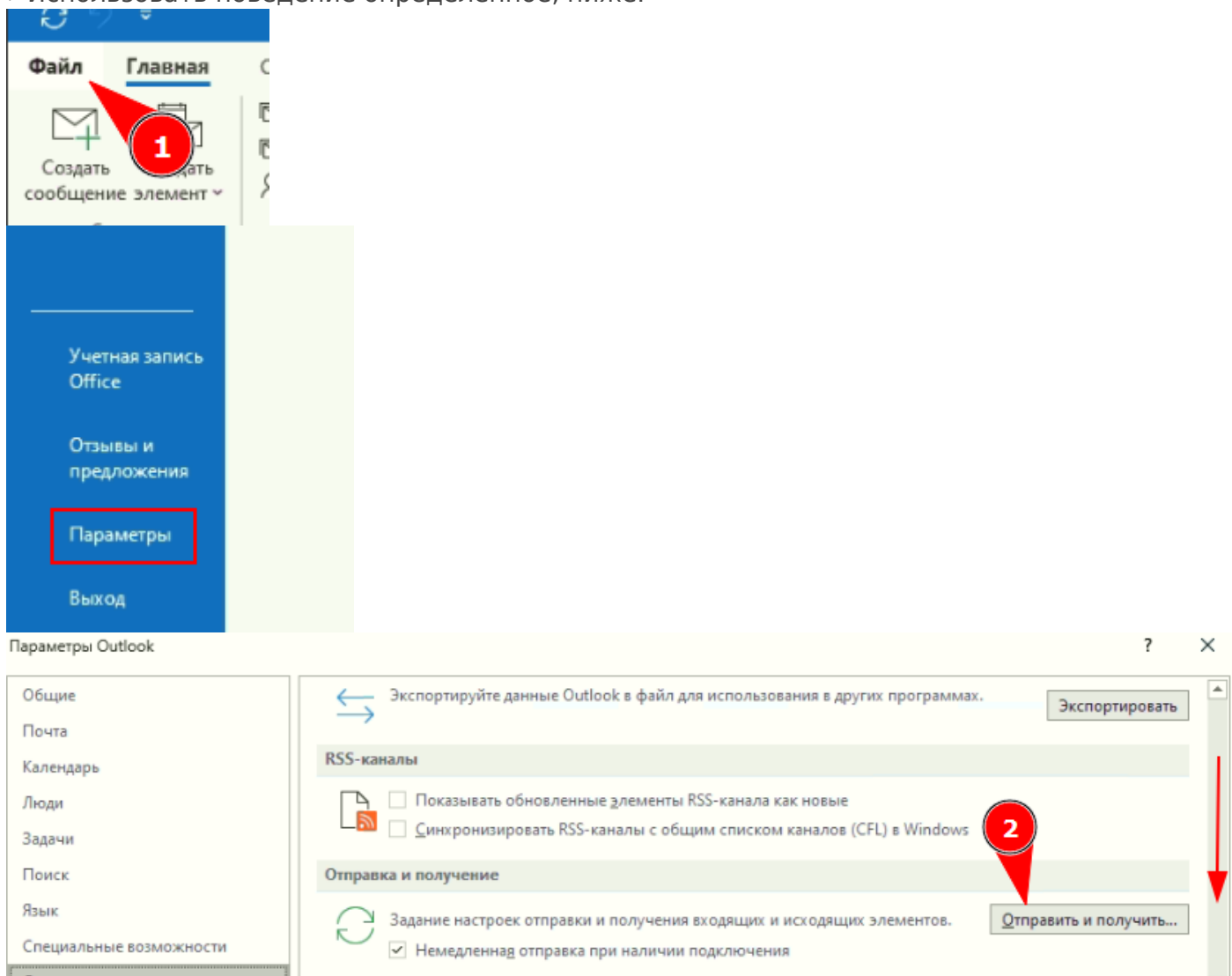
Не синхронизируется Outlook

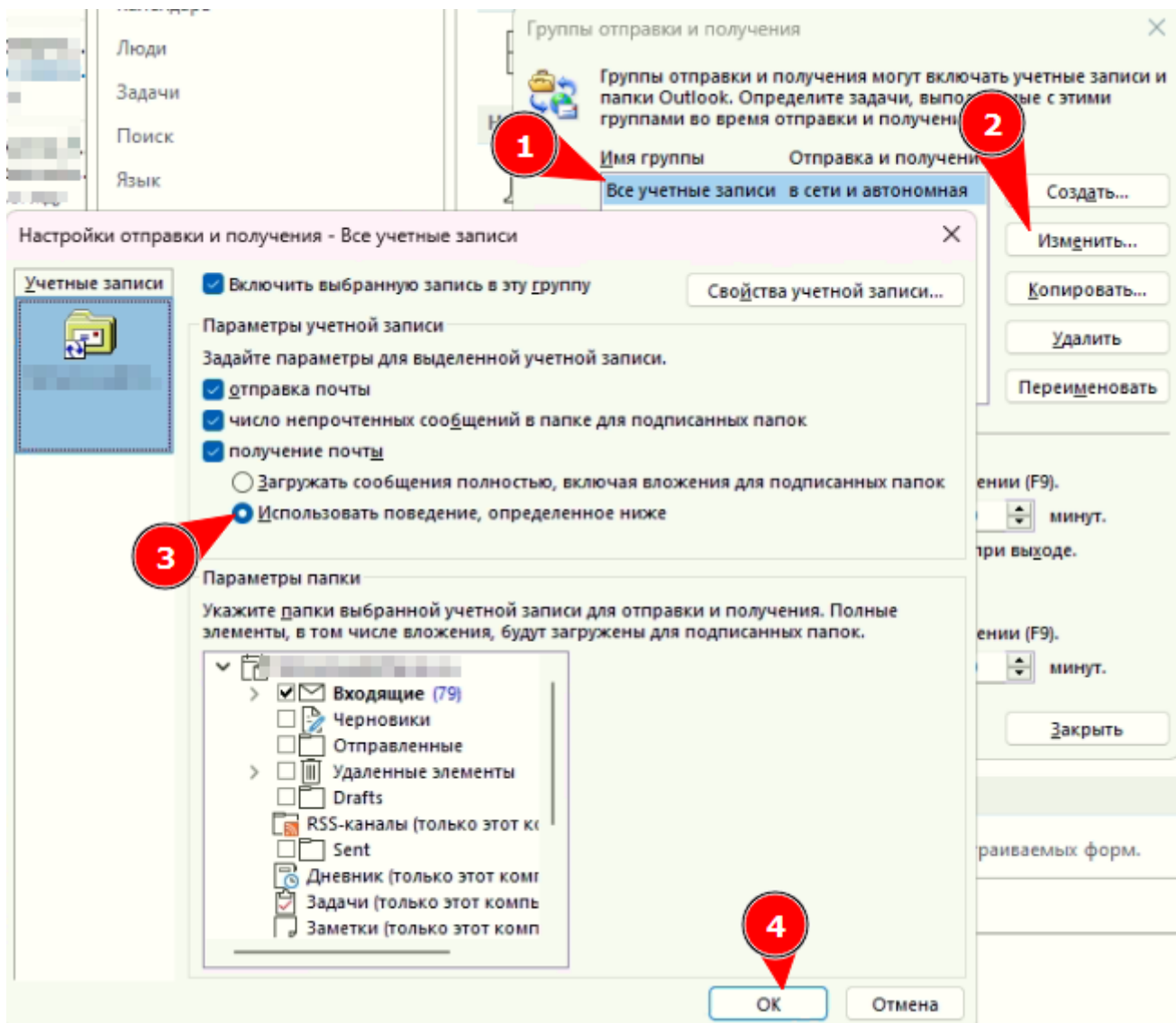
Происходит бесконечная отправка получение почты. Отправляемые письма складируются в исходящих и не уходят, пока не Outlook заново не будет открыт. Входящая почта приходит так же, в момент открытия, дальше в отправляет-получает постоянно, даже если уже выкачал весь ost файл заново, при синхронизации минимального периода (месяца). В текущем случае версия 2021.

Использовать поведение определённое, ниже

Наиболее вероятно, помогла статья [Дмитрия Хлебалина](#)

Файл->Параметры->Дополнительно->Отправить и получить->Все записи->Изменить->Использовать поведение определённое, ниже:





Перезапустить Outlook.

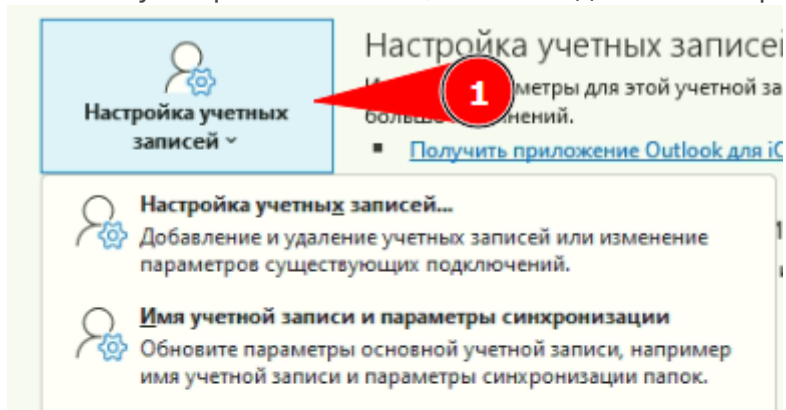
Создать новый профиль Outlook

На [форуме MS](#) попадалась ветка, где были похожие симптомы.

Этот совет не помог:

Файл -> параметры -> центр управления безопасностью -> параметры центра управления безопасностью -> защита эл. почты - поставить птички(галочки) разрешить сценарии в общих и общедоступных папках

По совету второго человека, был заведён новый профиль Outlook:



После перезапуска, при выборе профиля, нужно задать имя и "создать".

Сначала был создан новый профиль, а потом попалась статья Дмитрия, поэтому что из них сработало наверняка неизвестно.

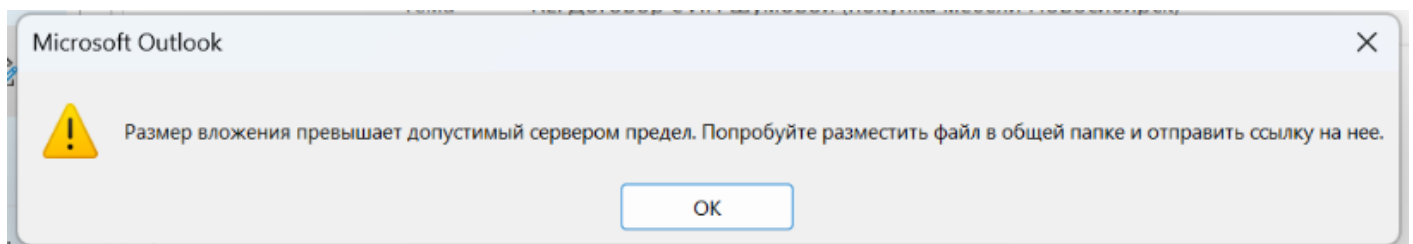
Производительность поиска будет снижена, так как служба Windows Search отключена групповой политикой

Windows 11, Outlook 2021. При поиске в Outlook появляется это сообщение, информация о индексации недоступна (нет кнопок).

Была включена и запущена служба Windows Search. Сообщение не исчезло.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search\PreventIndexingOutlook изменён с 1 на 0, после чего сообщение исчезло, появились кнопки работы с индексами, пошла индексация писем. Поиск по итогу работает.

Размер вложения превышает допустимый сервером предел

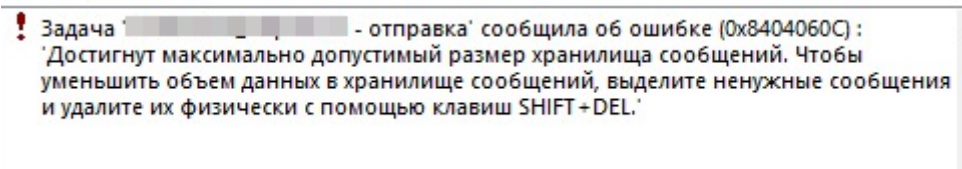
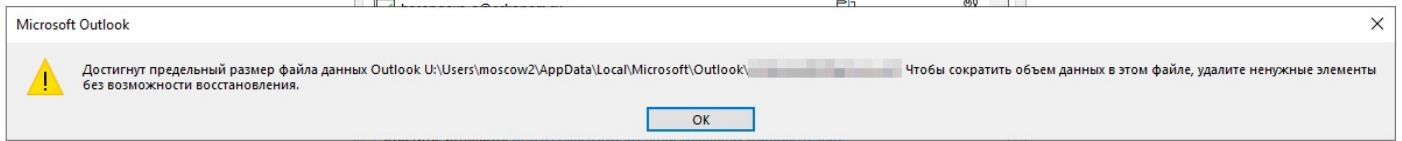


+(DWORD32)

HKEY_CURRENT_USER\Software\Microsoft\Office\x.0>\Outlook\Preferences\MaximumAttachmentSize = 0

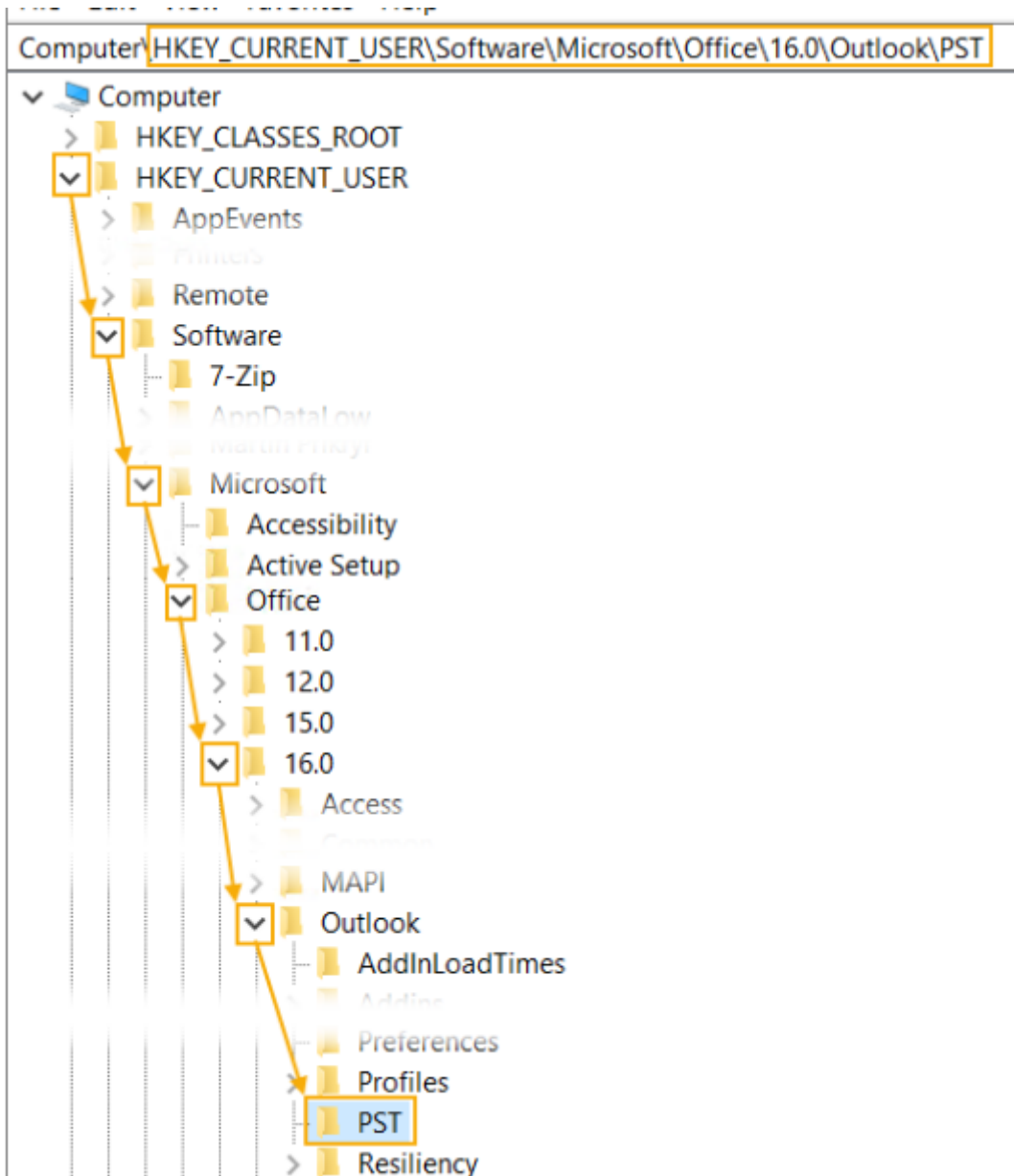
<https://learn.microsoft.com/ru-ru/outlook/troubleshoot/message-body/attachment-size-exceeds-the-allowable-limit-error>

Достигнут предельный размер файла данных



Нужно увеличить:

- MaxLargeFileSize например до 100G 102400 dec
- WarnMaxLargeFileSize до 95G 97280 dec



https://support.intermedia.com/app/articles/detail/a_id/17301/~how-to-increase-the-size-limit-of-your-pst-and-ost-files-in-outlook-for-windows%3F

В одном случае, не удалось получить эффекта от изменения параметров PST файлов, для файла OST (он в 50 упирается).

В другом (Win 11 + Ou 2021) сработало этим рег файлом (97-100 GB):

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\PST]

"MaxLargeFileSize"=dword:00019000

"WarnLargeFileSize"=dword:00017c00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Outlook\PST]

"MaxLargeFileSize"=dword:00019000
"WarnLargeFileSize"=dword:00017c00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Outlook\PST]
"MaxLargeFileSize"=dword:00019000
"WarnLargeFileSize"=dword:00017c00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\12.0\Outlook\PST]
"MaxLargeFileSize"=dword:00019000
"WarnLargeFileSize"=dword:00017c00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\11.0\Outlook\PST]
"MaxLargeFileSize"=dword:00019000
"WarnLargeFileSize"=dword:00017c00

Windows

Ошибка установки MSI пакета Код ошибки 2755

Надо запускать через msixexec в cmd из под админа.

```
msixexec /package lala.msi
```

[Подсмотрено тут](#)

Выключить рекламу Windows 11

Поставить, запустить [OFGB](#)

Windows 11 установить без интернета

Чтобы появилась кнопочка "У меня нет интернета", надо нажать Shift + F10, ввести команду:

```
OOBE\BYPASSNRO
```

Дождаться перезагрузки. Взято [отсюда](#)

Подготовка терминальной Windows

[Как переместить C:\Users](#)

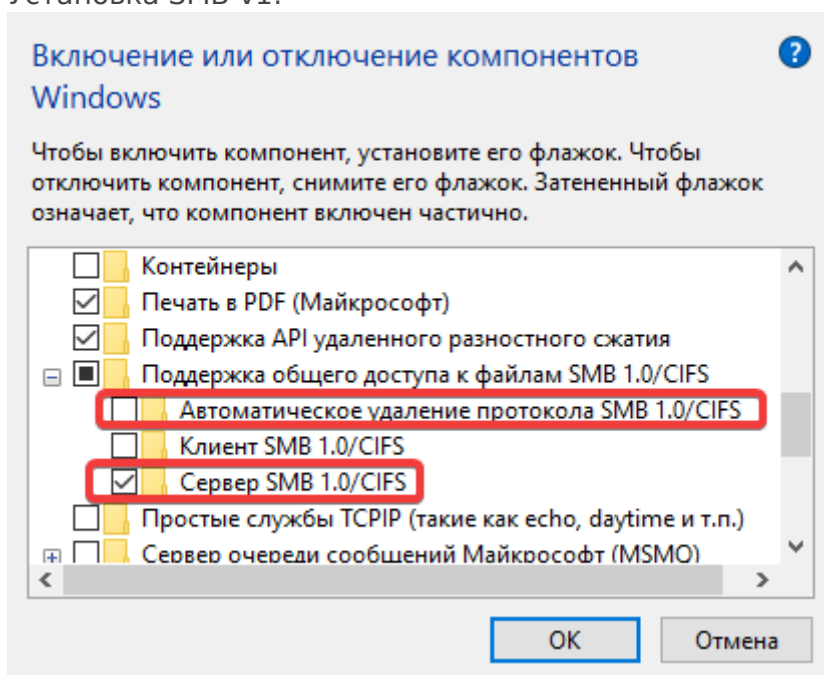
[Активация лицензий](#)

[Фризы RDP в Windows 2022](#)

[Выключение DFSS](#)

Включить samba v1 в windows 10

Установка SMB v1:



Выключение v2

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

Взято [отсюда](#)

Очистка очереди печати Windows

```
net stop spooler  
del %systemroot%\system32\spool\printers\*.shd /F /S /Q  
del %systemroot%\system32\spool\printers\*.spl /F /S /Q  
net start spooler
```

Excel не сохраняет файл без прав на удаление любого файла в папке

```
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General\EnableSimpleCopyForSaveToUNC  
DWORD (32-bit) -> 1
```

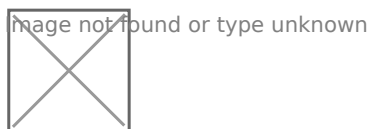
<https://support.microsoft.com/en-us/topic/-access-denied-error-message-when-you-save-a-workbook-to-a-unc-share-in-excel-2010-or-excel-2013-4df84394-0cca-a756-436b-9494331218e7>

Маршрут VPN

При выключении в VPN маршрута по умолчанию, приходилось запускать батник примерно такого содержания, чтобы проложить маршрут до целевой машины:

```
route add 172.96.0.4 172.93.0.249
```

Вместо этого в powershell:



Выполняете команду:

```
Add-VpnConnectionRoute -ConnectionName "VPNConnection" -DestinationPrefix "176.16.0.4/32" -PassThru
```

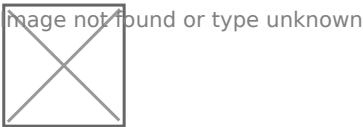
Где вместо VPNConnection название вашего VPN подключения, а 176.16.0.4 это адрес целевой машины (например, RDP сервера)

Теперь маршрут будет добавляться автоматически при подключении.

Кто открыл файл в Windows

```
Openfiles /Query /fo csv
```

или mmc



Зайти под USR1CV8

Политика "Локальный компьютер"

Конфигурация компьютера

Конфигурация программ

Конфигурация Windows

Политика разрешения имен

Сценарии (запуск/завершение)

Параметры безопасности

Политики учетных записей

Локальные политики

Политика аудита

Назначение прав пользователя

Параметры безопасности

Брандмауэр Windows в режиме повышенной безопасности

Политики диспетчера списка сетей

Политики открытого ключа

Политики ограниченного использования программ

Политики управления приложениями

Политики IP-безопасности на "Локальный компьютер"

Конфигурация расширенной политики аудита

QoS на основе политики

Административные шаблоны

Конфигурация пользователя

Конфигурация программ

Конфигурация Windows

Сценарии (вход/выход из системы)

Параметры безопасности

Политики открытого ключа

QoS на основе политики

Административные шаблоны

Политика

Архивация файлов и каталогов

Блокировка страниц в памяти

Восстановление файлов и каталогов

Вход в качестве пакетного задания

Вход в качестве службы

Выполнение задач по обслуживанию томов

Добавление рабочих станций к домену

Доступ к диспетчеру учетных данных от имени доверенн...

Доступ к компьютеру из сети

Завершение работы системы

Загрузка и выгрузка драйверов устройств

Замена маркера уровня процесса

Запретить вход в систему через службу удаленных рабоч...

Запретить локальный вход

Изменение метки объекта

Изменение параметров среды изготовителя

Изменение системного времени

Изменение часового пояса

Имитация клиента после проверки подлинности

Локальный вход в систему

Настройка квот памяти для процесса

Обход перекрестной проверки

Отказывать в доступе к этому компьютеру из сети

Отказывать во входе в качестве пакетного задания

Отказывать во входе в качестве службы

Отключение компьютера от стыковочного узла

Параметр безопасности

Администраторы, Операторы архива

MSSQL, Администратор

Администраторы, Операторы архива

RTL\admin

NETWORK SERVICE, SQLServer2005SQLBrowserUser\$NEWONEC, USR1CV8, MSSQL, TESTSRV, Администраторы

Все, Администраторы, Пользователи, Операторы архива

Администраторы, Операторы архива

Администраторы

LOCAL SERVICE, NETWORK SERVICE, NT SERVICE\SQLSERVERAGENT, NT SERVICE\MSSQLSE

USR1CV8

Администраторы

LOCAL SERVICE, Администраторы

LOCAL SERVICE, Администраторы

LOCAL SERVICE, NETWORK SERVICE, Администраторы, IIS_IUSRS, СЛУЖБА

Администраторы, Пользователи, Операторы архива

LOCAL SERVICE, NETWORK SERVICE, Администраторы, NT SERVICE\SQLSERVERAGENT, NT

Bce, LOCAL SERVICE, NETWORK SERVICE, Администраторы, Пользователи, Операторы арх

USR1CV8

Администраторы

1

2

3

4

5

6

RDP

Windows 2022 фриззы в RDP

Проблема полностью описана [тут](#)

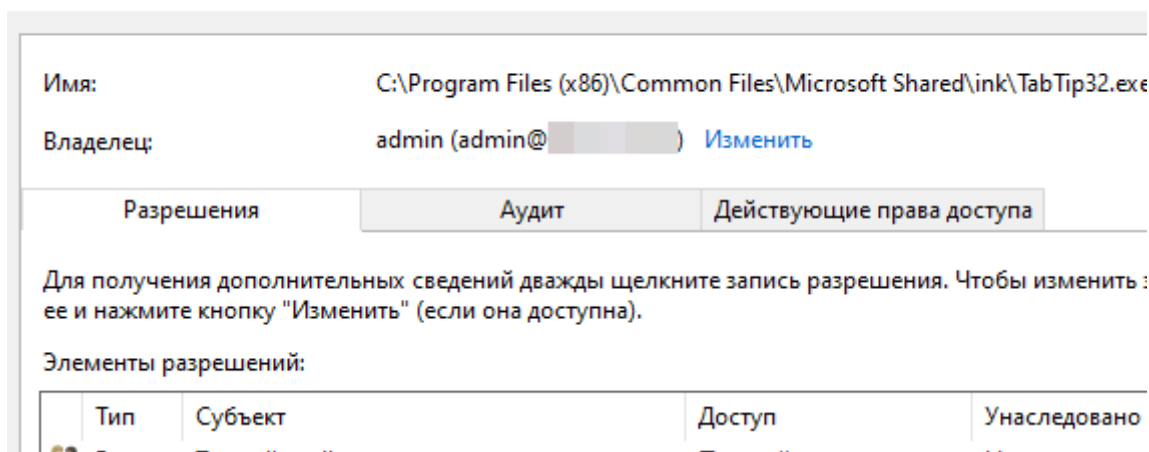
В свежееустановленном RDP сервере 2022 нужно переименовать файлы:

C:\Program Files (x86)\Common Files\Microsoft Shared\ink\TabTip32.exe в TabTip32.exe.orig (Оригинальный)

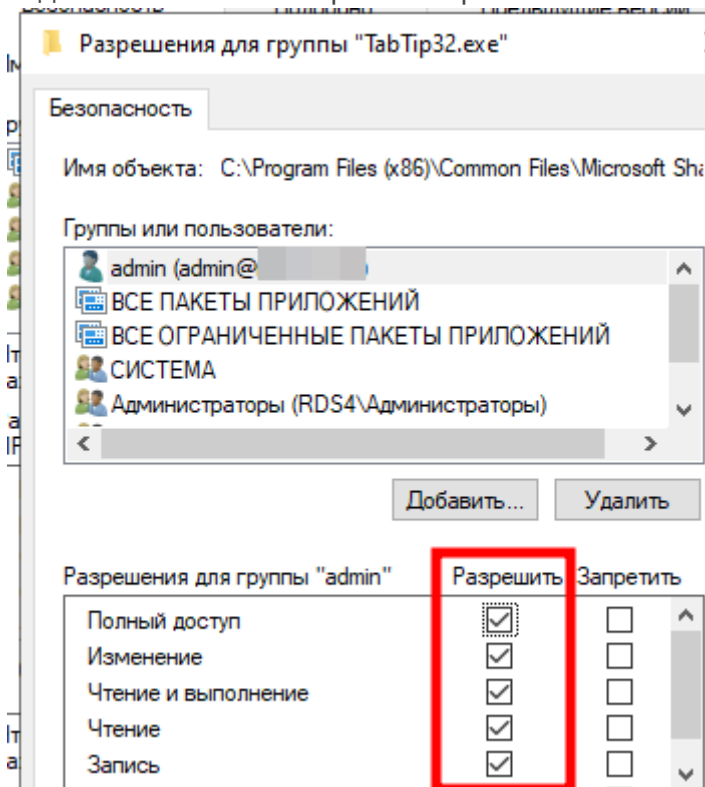
C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe в TabTip.exe.orig (Оригинальный)

Для этого нужно объявить себя владельцем файла:

Дополнительные параметры безопасности для "TabTip32.exe"



И дать себе полные права на файл:



Не сохраняется пароль

Посвящаю эту статью половине потерянного сегодня мной дня. Моя проблема заключалась в том, что пароль не сохранялся только для шлюза удалённых рабочих столов. Проблема была в том, что URL шлюза в DNS был прописан CNAME, а не A. Клиент искал сохраненные учетки не для того URL, который был задан в поле шлюз, а для того, на который ссылается CNAME. Узнал я это случайно набрав <https://my.domain.ru/rpc>, там отразился DNS A узел.

Вот варианты решения, которые я науглил за пол дня.

<https://moonback.ru/page/windows-rdp-password>

<https://superuser.com/questions/1136306/remember-me-feature-does-not-work-when-rd-getaway-is-used>

Всё остальное является производным от них.

Отмечу софтину mRemoteNG тем, что она подсказывает какую KB нужно поставить, если в ответ на все попытки установить RDP свежее ось пишет, что эта KB ему не подходит. Если всё равно не ставится - попробуйте скачать английскую версию этого же KB.

Невозможно установить желаемое масштабирование в RDP 8.1+

Отключаете проверку масштаба клиента со стороны сервера:

1. Run regedit and follow this registry key :
**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations**
2. In **WinStations** registry key, **create a DWORD (32-bit) value**
IgnoreClientDesktopScaleFactor
3. Set this value to **1**

И перелогиниваетесь пользователем. Перезапускать терминальный сервер - не нужно.

Зависает подключение к удаленному рабочему столу

(RDP) при подключении через VPN

Помогло отключение UDP на стороне клиента:

Правка реестра. В ветке `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client` необходимо создать параметр `fClientDisableUDP` и установить значение 1.

Взял [тут](#)

RDP MSI

msiexec.exe бывает виснет в RDP. Помогает шевеление

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\TSAppSrv\TSMSI\Enable](#)

<https://community.flexera.com/t5/InstallShield-Forum/Problems-with-windows-server-2008-r2-and-terminalserver/m-p/18142>

LVM

Удалить по UUID

```
vgremove -S uuid=XYZ
```

Portainer.io

Подготовка виртуальной машины

Установка производится на lxc машину, с установленным на неё Debian 12 и включенными keyctl, nesting и fuse в features:



Чтобы попасть на неё без пароля с хостовой машины:

```
pct enter 181
```

Возможно вам понадобится включить ключи ssh-rsa в /etc/ssh/sshd_config

```
PermitRootLogin prohibit-password  
PubkeyAcceptedKeyTypes=+ssh-rsa
```

Устанавливаем yandex репозитории (выше скорость загрузки пакетов):

/etc/apt/sources.list

```
deb https://deb.debian.org/debian bookworm main  
deb-src https://deb.debian.org/debian bookworm main  
  
deb https://deb.debian.org/debian bookworm-updates main  
deb-src https://deb.debian.org/debian bookworm-updates main  
  
deb http://security.debian.org/ bookworm-security main  
deb-src http://security.debian.org/ bookworm-security main
```

Обновляем систему, устанавливаем часовой пояс и локали, установим немного софта:

```
apt update && apt full-upgrade -y  
dpkg-reconfigure tzdata  
dpkg-reconfigure locales  
apt install curl mc sudo curl wget
```

Установка docker & docker-compose

Docker

```
apt -y install apt-transport-https ca-certificates gnupg2 software-properties-common  
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -  
add-apt-repository \  
"deb [arch=amd64] https://download.docker.com/linux/debian \  
$(lsb_release -cs) \  
stable"  
apt update  
apt -y install docker-ce docker-ce-cli containerd.io fuse-overlayfs  
systemctl enable --now docker
```

Docker-compose

```
curl -s https://api.github.com/repos/docker/compose/releases/latest | grep browser_download_url | grep docker-  
compose-linux-x86_64 | cut -d '"' -f 4 | wget -qi -  
chmod +x docker-compose-linux-x86_64  
mv docker-compose-linux-x86_64 /usr/local/bin/docker-compose
```

Не запускается lxc

Узнать причину:

```
lxc-start -n 181 -F -l DEBUG -o lxc-181.log
```

В моём случае потребовалось изменить максимальную версию debian тут:
/usr/share/perl5/PVE/LXC/Setup/Debian.pm

```
$version = 4;  
  
die "unsupported debian version '$version'\n"  
-----> if !($version >= 4 && $version <= 13 ;
```

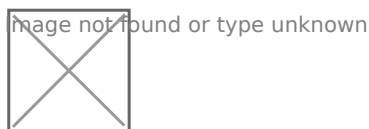
Portainer.io

```
docker volume create portainer_data  
docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v  
/var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
```

Далее идём на <https://your.machine.ip:9443/>

Устанавливаем пароль для admin и заходим в админку portainer

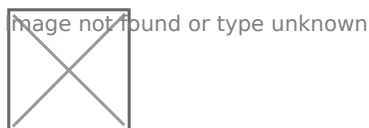
Чтобы зайти в свой экземпляр (portainer может рулить множеством экземпляров) надо щёлкнуть сюда:



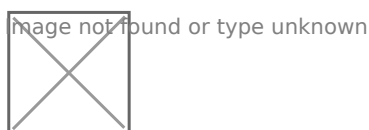
Nginx Proxy Manager

Установка

Попробуем поставить сие программное средство в portainer:



ыНазовите его как-нибудь, вставьте содержимое docker-compose.yml в web форму:



И жмём кнопку в самом низу:



Image not found or type unknown

Админка будет ожидать вас на 81-ом порту.

Email: admin@example.com

Password: changeme

Работа с жесткими дисками в Linux

Ссылки

[Все управляшки HW RAID](#)

[Управление Adaptec](#)

Создать Simple Volume можно так:

```
arcconf create 1 LOGICALDRIVE MAX volume 0,1
```

[Рескан scsi шины в linux](#)

[Замена загрузочного диска](#)

[Замена диска zfs](#)

Загрузка zfs с SD 380 HBA

HP DL380 gen8 имеет на борту p420i raid контроллер. ZFS как вы знаете, любит работать с дисками напрямую. p420i на удивление, умеет переключаться в HBA режим, но грузиться с него у вас не получится.

Вот человек предлагает решение:

https://www.reddit.com/r/homelab/comments/ap9usf/proxmoxzfs_installed_on_hp_dl360p/ Но с лёту у меня не получилось сделать так же как он. Рассказываю как сделал я.

Для не умеющих читать по-английски.

1. Устанавливаем proxmox на жесткие диски как обычно в режиме zfs raid 1
2. Включаем флешку во внутренний SD
3. Загружаемся в live cd и указываем, что /boot теперь находится на SD
4. ставим граб на SD

- 5 Перезагружаемся, редактируем граб прям из него самого
- 6 Загружаемся в нашу систему, делаем grub-update grub-install

Во-первых debian live-cd не смог примонтировать в режиме записи zfs. В дебиане используется 0.7, а тут уже 0.8. Короч... Вам не нужен ни дебиан, ни убунту, грузимся с proxmox iso и выбираем debug режим.

Там пишем exit или Ctrl+D и оказываемся в консоли, в которой уже есть что нужно.

Далее я пошёл другим путём (так как предложенным у меня не получилось), я примонтировал zfs

```
zpool import -f -R /mnt rpool
```

и чрутнулся в него

```
mount -t proc /proc/ /mnt/proc  
mount -rbind /dev/ /mnt/dev  
mount -rbind /sys/ /mnt/sys  
chroot /mnt bash
```

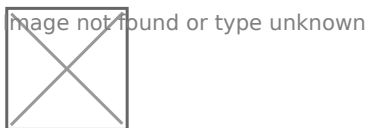
Теперь я в своей системе и отсюда я уже готовлю флешку, как описано в статье, и делаю grub-install на SD.

Далее при загрузке grub, через e, как указано в статье, меняю пути и название диска и загружаюсь в систему.

Система не грузится, iniramfs предлагает ввести команду, говорит, что rpool уже был в другой системе и нужно его импортировать в эту.

В самом его ругательстве написана строка, чинящая эту проблему. Вам надо её ввести «zpool import -f ... rpool» и система загрузится.

После загрузки сделайте grub-update, grub-install. Грузитесь на здоровье!



Программирование С

Запуск скриптов с рутовыми правами без доступа к скриптам

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

void RemoveSlash(char* source)
{
    char* i = source;
    char* j = source;
    while(*j != 0)
    {
        *i = *j++;
        if(*i != '/')
            i++;
    }
    *i = 0;
}

int main(int argc, char** argv) {
    if (argc < 2) {
        printf("Usage: runme scriptname\n");
        exit(-1);
    }
    char myoutput_array[5000];

    strcat(myoutput_array, "bash /opt/scripts/");
    RemoveSlash(argv[1]);
    strcat(myoutput_array, argv[1]);
    strcat(myoutput_array, "\n");
```

```
/printf("%s", myoutput_array);/  
setuid(0);  
system(myoutput_array);  
return 0;  
}
```

```
gcc -o test test.c  
cp test /usr/bin/runme  
chmod 4775 /usr/bin/runme
```

FFmpeg

Объединение двух видео в Linux

cat output.txt

```
file '/path/to/file/1.mp4' file '/path/to/file/2.mp4'
```

```
ffmpeg -f concat -safe 0 -i ./file -c copy output.mp4
```

Удалить звук

```
ffmpeg -i example.mkv -c copy -an example-nosound.mkv
```

Наложить звук

```
ffmpeg -i video.mp4 -i audio.wav -c:v copy -c:a aac -strict experimental output.mp4
```

Выдернуть звук из видео

```
ffmpeg -i filename.mp4 filename.mp3
```

Разрезать видео

```
ffmpeg -i Plov.mov -ss 00:12:00 -to 00:21:54 -c copy Plov2.mov
```


Zabbix

Ссылки

[Мониторинг температуры процессора](#)

[Мониторинг состояния пуллов zfs](#)

Шифрованный клиент

На стороне клиента

Клиент Windows

Для винды стандартный дистрибутив не включает TLS. Качать клиенты с поддержкой TLS [тут](#). Качаем клиент, распаковываем в созданную самостоятельно папку «C:\Program Files\zabbix». Создаём файл «C:\Program Files\zabbix\conf\zabbix_agentd.conf»

```
#ip address Zabbix server
Server=192.168.x.x

# Unique hostname. Required for active checks.
Hostname=host.local

# Listen port. Default is 10050
ListenPort=10050

# Name of log file.
LogFile=c:\program files\zabbix\zabbix_agentd.log

# Maximum size of log file in MB. Set to 0 to disable automatic log rotation.
LogFileSize=10


TLSConnect = psk
TLSAccept=psk
TLSPSKIdentity=PSK 001
TLSPSKFile=C:\Program Files\zabbix\conf\key.txt
```

Внимание! TLSPSKIdentity на разных клиентах должен быть разным. При двух одинаковых связь с обоими работать не будет!

Номер порта желательно заменить на что-нибудь подальше, но не слишком. Zabbix клиент почему-то не запускается на портах выше какого-то (точно не помню какого).

В C:\Program Files\zabbix\conf\key.txt помещаем ключ. Я использую команду «openssl rand -hex 32» в каком-нибудь линуксе. По факту строка 64 случайных символов.

В консоли из под админа устанавливаю и запускаю службу:

```
"c:\program files\zabbix\win64\zabbix_agentd.exe" --config "c:\program files\zabbix\conf\zabbix_agentd.conf" --install  
"c:\program files\zabbix\win64\zabbix_agentd.exe" --config "c:\program files\zabbix\conf\zabbix_agentd.conf" --start
```

Готово. Не забудьте открыть порт.

Клиент Linux

```
apt install zabbix-agent cd /etc/zabbix/ cp ./zabbix_agentd.conf ./zabbix_agentd.conf.bak
```

zabbix_agentd.conf

```
apt install zabbix-agent  
cd /etc/zabbix/  
cp ./zabbix_agentd.conf ./zabbix_agentd.conf.bak
```

На стороне сервера



Proxmox mail gateway

Блокировка содержимого в rar архивах

Для того, чтобы pmg смотрел вовнутрь rar архивов, надо дописать в конец apt источников в /etc/apt/sources.list строки non-free примерно так:

```
deb http://ftp.debian.org/debian bullseye main contrib non-free
deb http://ftp.debian.org/debian bullseye-updates main contrib non-free
deb http://security.debian.org/debian-security bullseye-security main contrib non-free
```

И установите следующие пакеты:

```
apt update
apt install libclamunrar p7zip-rar
```

Возможно понадобится перезапуск служб pmg.

Автоматическое обучение

<https://www.crc.id.au/2020/05/06/training-spamassassins-bayes-filter-with-proxmox-mail-gateway/>

ProFTPd

Настройка ProFTPd

Задача тупо поставить ftp. Пускать только в домашние папки пользователей. Поддерживать русские буквы.

Берём стандартный proftpd.conf и дописываем в конец:

```
DefaultRoot      ~
PassivePorts      50200 50201 # Этот диапазон надо будет прокинуть через NAT вместе с 21
MasqueradeAddress XX.XX.XX.XX # Внешний IP

LangDefault       ru_RU.UTF-8
LangEngine        on
LangPath          /usr/share/locale
UseEncoding       UTF-8 WINDOWS-1251
```

Теперь любой пользователь, под своим паролем может заходить к себе в HOME.

Под виндой русские буквы корректно отображаются. Чтобы тоже самое было в FileZilla надо указать кодировку cp1251:

Postgres 1C ZFS

Установка Postgres

[Великолепная сатья по установке 1C на linux от rarus](#)

В статье указана устаревшая ссылка на скрипт установки PGPro, вот новая:

wget <https://repo.postgrespro.ru/pg1c-14/keys/pgpro-repo-add.sh>

Получить PostgresPro бесплатно можно на сайте 1c.postgres.ru

[Рекомендации от posgrespro для 1C](#)

[Полезное для linux+postgres](#)

[Postgres + PGAF \(Failover за Postgres\)](#)

[Советы от Гилёва по части PostgreSQL](#)

[Неплохая статья с примером обслуживания базы](#)

[Настройка PostgreSQL для 1C](#)

Основные моменты ZFS

В postgres:

```
full_page_writes = off
```

По [ссылке](#) дано объяснение по каждому из пунктов. В частности почему размер блока стоит делать побольше, и почему не надо делать logbias=throughput

Параметры ядра для postgres

```
vm.swappiness=1  
kernel.sched_migration_cost_ns = 5000000
```

kernel.sched_autogroup_enabled = 0

vm.dirty_background_bytes = 67108864

vm.dirty_bytes = 536870912

vm.zone_reclaim_mode = 0

IPTables

Проброс портов с localhost на внешний адрес

Системные переменные

```
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
echo "net.ipv4.conf.all.route_localnet=1" >> /etc/sysctl.conf
sysctl -p
```

/etc/rc.local

```
#!/bin/sh -e

YourIP=127.0.0.1
YourExternalIP=`ifconfig | grep -Eo 'inet (addr:)?([0-9]*\.){3}[0-9]*' | grep -Eo '([0-9]*\.){3}[0-9]*' | grep -v '127.0.0.1'`
YourPort=20000:30000
TargetIP=xx.xx.xx.xx
TargetPort=80

iptables -t nat -F
iptables -t nat -A PREROUTING --dst $YourIP -p tcp --dport $YourPort -j DNAT --to-destination $TargetIP:$TargetPort
iptables -t nat -A POSTROUTING -p tcp --dst $TargetIP --dport $TargetPort -j SNAT --to-source $YourExternalIP
iptables -t nat -A OUTPUT --dst $YourIP -p tcp --dport $YourPort -j DNAT --to-destination $TargetIP:$TargetPort
```

ZFS

Удалить снапшоты

```
zfs list -H -o name -t snapshot | xargs -n1 zfs destroy
```

OpenVPN

Адаптация старых OpenVPN конфигов к новым релизам OpenVPN

2.3 → 2.4

При переходе часто встречается ошибка. Текстового примера под рукой нет

Добавить

```
tls-cipher "DEFAULT:@SECLEVEL=0"
```

в начало .conf файла, вот так:



tls-remote Unrecognized option

Options error: Unrecognized option or missing or extra parameter(s) in lala.ovpn:95: tls-remote (2.5.7)

Use --help for more information.

tls-remote упряднён:

```
tls-remote lala.my.com
```

Вместо него:

```
verify-x509-name lala.my.com name
```

Варианты синтаксиса:

```
verify-x509-name 'C=KY, ST=GrandCayman, L=GeorgeTown, O=GoldenFrog-Inc, CN=uk1.vpn.giganews.com'
```

Add the server's cipher ('BF-CBC') to --data-ciphers

OPTIONS ERROR: failed to negotiate cipher with server. Add the server's cipher ('BF-CBC') to --data-ciphers (currently 'AES-256-GCM:AES-128-GCM') if you want to connect to this server.

Надо добавить в конфиг:

```
cipher BF-CBC
```

Autostart OpenVPN systemd

In order to configure OpenVPN to autostart for systemd, complete the following steps:

Run the command:

```
# sudo nano /etc/default/openvpn
```

and uncomment, or remove, the “#” in front of

```
AUTOSTART="all"
```

then press ‘Ctrl X’ to save the changes and exit the text editor.

Move the .ovpn file with the desired server location to the ‘/etc/openvpn’ folder:

```
# sudo cp /location/whereYouDownloadedConfigfilesTo/Germany.ovpn /etc/openvpn/
```

Edit the .ovpn file you copied in the previous step and change the line ‘auth-user-pass’ to ‘auth-user-pass pass’:

```
# sudo nano /etc/openvpn/Germany.ovpn
```

then press ‘Ctrl X’ to save the changes and exit the text editor.

In the '/etc/openvpn' folder, create a text file called pass:

```
# sudo nano /etc/openvpn/pass
```

and enter your IVPN Account ID (starts with 'ivpn') on the first line and any non-blank text on the 2nd line, then press 'Ctrl X' to save the changes and exit the text editor.

(Optional) Change the permissions on the pass file to protect the credentials:

```
# sudo chmod 400 /etc/openvpn/pass
```

Rename the .ovpn file to 'client.conf':

```
# sudo cp /etc/openvpn/Germany.ovpn /etc/openvpn/client.conf
```

On Ubuntu 16.04 LTS, OpenVPN installs and initiates a service by default. If you are using Ubuntu 16.04 LTS, skip to step 10.

For Ubuntu 18.04 LTS and up, enable the OpenVPN service to run while booting:

```
# sudo systemctl enable openvpn@client.service
```

Reload the daemons:

```
# sudo systemctl daemon-reload
```

Start the OpenVPN service:

```
# sudo service openvpn@client start
```

Reboot and test if it is working by checking the external IP:

```
# curl ifconfig.co
```

If curl is not installed:

```
# sudo apt install curl
```

<https://www.ivpn.net/knowledgebase/linux/linux-autostart-openvpn-in-systemd-ubuntu/>

Nextcloud

Не отображаются файлы

```
sudo -u www-data php /var/www/nextcloud/occ files:scan --all
```

Очистка корзины групповых папок

Из интерфейса нельзя очистить корзину, в консоли это сделала команда:

```
sudo -u <nextcloud_user> php /var/www/nextcloud/occ groupfolders:trashbin:cleanup
```

В моём случае nextcloud_user - www-data

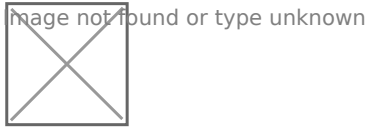
Взял [тут](#)

Не загружаются большие файлы из наружного контура

Настройка NGINX

```
proxy_set_header Host $host;  
proxy_set_header X-Forwarded-Proto $scheme;  
proxy_set_header X-Real-IP $remote_addr;  
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
proxy_max_temp_file_size 16384m;  
client_max_body_size 0;
```

Этот код нужно вставить сюда:

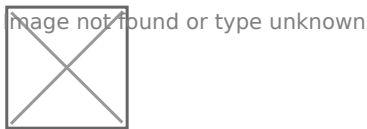


Выяснилось ещё, что при отправке на облако 6Gb файла, корневой раздел виртуальной машины с nginx проху manager увеличивается на 6Gb. После загрузки файла - уменьшается. Без увеличения раздела nginx файл загрузить не удалось. Выключение Cache Assets в nginx не помогло.

Ошибка удаления групповых файла/папки Nextcloud

Симптом

В nextcloud, в моём случае в версиях от наверное 15-ой до 22-ой невозможно удалить файлы и папки, находящиеся в группе:



Вот так настроены логи

```
'log_type' => 'file',  
'logfile' => 'nextcloud.log',  
'loglevel' => 3,  
'logdateformat' => 'F d, Y H:i:s',
```

Выдали:

```
"Failed to move groupfolder item to trash"
```

Решение

```
cd /var/www/nextcloud/data/__groupfolders  
mkdir trash
```

```
cd trash
mkdir 1 10 2 3 4 5 6 7 8 9
cd ..
chown -R www-data:www-data trash
```

Взято [отсюда](#)

Сопряжение OnlyOffice + NextCloud через JWT ключ

Onlyoffice

```
docker run -i -t -d -p 80:80 --restart=always -e JWT_ENABLED=true -e JWT_SECRET=bla123BLA321BIA1 -e JWT_HEADER=BlaBlaJwt onlyoffice/documentserver
```

Nextcloud

```
'onlyoffice' => .
array (
  'verify_peer_off' => true,
  'jwt_header' => 'BlaBlaJwt',
  'jwt_secret' => 'bla123BLA321BIA1',
),
```

Linux Server

Добавить шифрованный том LVM

```
cryptsetup -v luksFormat /dev/sdx  
cryptsetup -v open /dev/sdx cryptdevol  
pvcreate --metadatasize 250k -y -ff /dev/mapper/cryptdevol  
vgcreate cryptdevlvm /dev/mapper/cryptdevol
```

Добавить ssh-rsa в поддерживаемые

```
lxc-attach -n 100  
PubkeyAcceptedKeyTypes +ssh-rsa
```

Отдельный SSH сервер для отдельного пользователя

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config_custom  
echo 'Port 666' >> /etc/ssh/sshd_config_custom  
echo 'AllowUsers customuser' >> /etc/ssh/sshd_config_custom  
cp /lib/systemd/system/ssh.service /lib/systemd/system/ssh_custom.service
```

Пример рабочего файла /lib/systemd/system/ssh_custom.service:

```
[Unit]  
Description=OpenBSD Secure Shell server  
Documentation=man:sshd(8) man:sshd_config(5)
```

```
After=network.target auditd.service
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStartPre=/usr/sbin/sshd -t -f /etc/ssh/sshd_config_custom
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS -f /etc/ssh/sshd_config_custom
ExecReload=/usr/sbin/sshd -t -f /etc/ssh/sshd_config_custom
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify
RuntimeDirectory=sshd
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
```

Обратите внимание на удалённую строку `Alias=sshd.service` относительно оригинального `/lib/systemd/system/ssh.service`

Монтирование LVM not available

```
lvchange -ay /dev/LVM/lala
mount /dev/LVM/lala /mnt
umount /dev/LVM/lala
lvchange -an /dev/LVM/lala
```

NTP клиент

```
apt install systemd-timesyncd
```

Linux Desktop

Linux PPTP клиент

Отличные материалы:

<https://adminim.by/sovetyi/nastroyka-vpn-pptp-na-linux-debian/>

<https://wiki.debian.org/ru/pptp-linux>

Wireguard add connection

```
nmcli connection import type wireguard file
```

Tap to click

```
sudo apt install xserver-xorg-input-synaptics
```

Мерцает экран после сна i915

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash i915.enable_psr=0 i915.enable_rc6=0"
```

Свободные IP в сети

```
nmap -v -sn -n 192.168.1.0/24 -oG - | awk '/Status: Down/{print $2}'
```

PfSense

Настройка сети в случае базирования pfSense на KVM

PfSense отлично ведёт себя на kvm (гостевая система) если

1) поставить драйвер virtio:



2) Включить **Disable hardware checksum offload** в **System/Advanced/Networking** в **pfSense**:



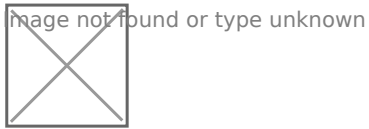
Если этого не сделать, то периодически будут проблемы. С этими настройками проблем нет уже несколько лет.

Настройка внутренней и внешней зон DNS

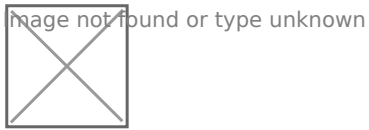
На PfSense работает обычный bind. Вы просто настраиваете его мышкой. Как сделать разные адреса для внутренней и внешней зон не очень понятно.

Для начала поставим BIND (DNS сервер)



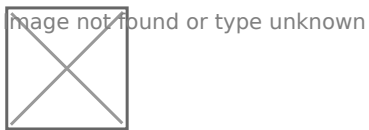


Дожидаемся установки, настраиваем:

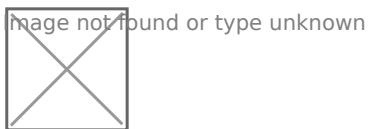
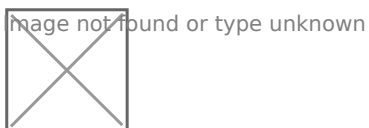
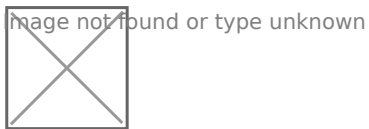


Добавляем views, внутренний :

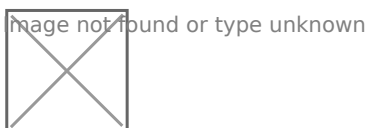
Сначала вкладку Settings:



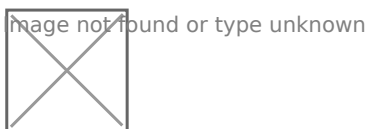
Включаем сервер, у меня нет IPv6 и да, я хочу, чтобы dns работал на всех интерфейсах.
Спускаюсь ниже, включаю сервера, на dns сервер провайдера или публичный dns:



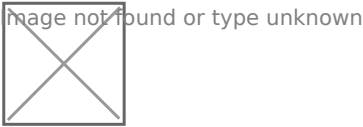
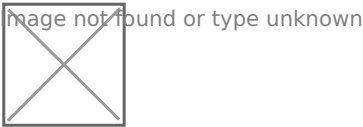
и внешний:



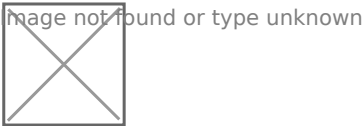
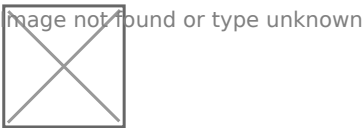
Далее, создаём зоны:



Внутреннюю:



И внешнюю:



Ikev2

ipsec/wireguard/3proxy/clam av updater 4 in 1

В примере используется следующая конфигурация:

Внешний IP: **91.149.232.254**

Внешний интерфейс: **eth0**

ikev2 сеть: **10.10.30.0/24**

Подсеть с которой разрешен доступ к 3проху: **94.229.240.0/20**

Доступ к админке WireGuard разрешен с ip: **94.229.246.136**

Далее по тексту меняем их на свои

1) Обновляем дистр и ставим нужные пакеты

Для Ubuntu

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-  
archive-keyring.gpg  
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]  
https://download.docker.com/linux/ubuntu \  
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Для Debian

```
curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor -o /usr/share/keyrings/docker-archive-  
keyring.gpg  
echo \  
"deb [arch="$(dpkg --print-architecture)" signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]  
https://download.docker.com/linux/debian \  
"$(. /etc/os-release && echo "$VERSION_CODENAME)" stable" | \  

```

```
tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Для Ubuntu\Debian

```
apt update
apt upgrade
reboot
apt install ufw fail2ban ca-certificates gnupg lsb-release build-essential docker-ce docker-ce-cli containerd.io mc
zip strongswan libstrongswan-standard-plugins strongswan-pki nginx python3-pip mc
/etc/init.d/nginx start
```

Устанавливаем и настраиваем ClamAV:

```
pip3 install cvdupdate
cvd config set --dbdir /var/www/html
cvd update
crontab -e
В крон добавляем задачу:
30 */4 * * * /bin/sh -c "/usr/local/bin/cvd update &> /dev/null"
```

2) Ставим 3проху для обхода блокировок

```
wget https://github.com/z3APA3A/3proxy/archive/0.9.3.tar.gz && tar xzf 0.9.3.tar.gz && cd 3proxy-* && make -f
Makefile.Linux
adduser --system --disabled-login --no-create-home --group proxy3
mkdir -p /var/log/3proxy && mkdir /etc/3proxy
cp bin/3proxy /usr/bin/
chown proxy3:proxy3 -R /etc/3proxy
chown proxy3:proxy3 /usr/bin/3proxy
chown proxy3:proxy3 /var/log/3proxy
id proxy3
nano /etc/3proxy/3proxy.cfg
```

Конфиг /etc/3proxy/3proxy.cfg заменить uid/gid полученные из id proxy3:

```
setgid 115
setuid 110

nserver 1.1.1.1
```

```
nserver 8.8.8.8
```

```
nscache 65536
```

```
timeouts 1 5 30 60 180 1800 15 60
```

```
external 91.149.232.254
```

```
internal 91.149.232.254
```

```
daemon
```

```
log /var/log/3proxy/3proxy.log D
```

```
logformat "- +_L%t.%N.%p %E %U %C:%c %R:%r %O %l %h %T"
```

```
rotate 30
```

```
auth none
```

```
#auth strong
```

```
#users sega:CL:pass
```

```
allow * * * 80-88,8080-8088 HTTP
```

```
allow * * * 443,8443 HTTPS
```

```
socks -p8083
```

```
proxy -n
```

Добавляем в автозагрузку:

```
nano /etc/systemd/system/3proxy.service
```

```
[Unit]
```

```
Description=3proxy Proxy Server
```

```
[Service]
```

```
Type=simple
```

```
ExecStart=/usr/bin/3proxy /etc/3proxy/3proxy.cfg
```

```
ExecStop=/bin/kill -x /usr/bin/pgrep -u proxy3`
```

```
RemainAfterExit=yes
```

```
Restart=on-failure
```

```
[Install]
```

```
WantedBy=multi-user.target
```

Применяем юнит:

```
systemctl daemon-reload
```

```
systemctl enable 3proxy
```

3) Подготавливаем ufw

3.1) Для работы с докером:

```
nano /etc/ufw/after.rules
```

Добавить в конец файла

```
# BEGIN UFW AND DOCKER

*filter

:ufw-user-forward - [0:0]
:ufw-docker-logging-deny - [0:0]
:DOCKER-USER - [0:0]
-A DOCKER-USER -j ufw-user-forward

-A DOCKER-USER -j RETURN -s 10.0.0.0/8
-A DOCKER-USER -j RETURN -s 172.16.0.0/12
-A DOCKER-USER -j RETURN -s 192.168.0.0/16

-A DOCKER-USER -p udp -m udp --sport 53 --dport 1024:65535 -j RETURN

-A DOCKER-USER -j ufw-docker-logging-deny -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -d 192.168.0.0/16
-A DOCKER-USER -j ufw-docker-logging-deny -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -d 10.0.0.0/8
-A DOCKER-USER -j ufw-docker-logging-deny -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -d 172.16.0.0/12
-A DOCKER-USER -j ufw-docker-logging-deny -p udp -m udp --dport 0:32767 -d 192.168.0.0/16
-A DOCKER-USER -j ufw-docker-logging-deny -p udp -m udp --dport 0:32767 -d 10.0.0.0/8
-A DOCKER-USER -j ufw-docker-logging-deny -p udp -m udp --dport 0:32767 -d 172.16.0.0/12

-A DOCKER-USER -j RETURN

-A ufw-docker-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW DOCKER BLOCK] "
-A ufw-docker-logging-deny -j DROP

COMMIT

# END UFW AND DOCKER
```

3.2) Для работы с ikev2:

```
nano /etc/ufw/before.rules
```

В начало файла

```
*nat
-A POSTROUTING -s 10.10.30.0/24 -o eth0 -m policy --pol ipsec --dir out -j ACCEPT
-A POSTROUTING -s 10.10.30.0/24 -o eth0 -j MASQUERADE
COMMIT

*mangle
-A FORWARD --match policy --pol ipsec --dir in -s 10.10.30.0/24 -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -m
tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
COMMIT
```

3.3) Разрешающие правила ufw:

```
ufw allow 22
#HTTP
ufw allow 80
#IPSEC
ufw allow 500,4500/udp
#Доступ к Зроху и нужных ip/подсетей
ufw allow from 94.229.240.0/20 to any port 8083
ufw allow from 94.229.240.0/20 to any port 3128
#Админка WireGuard
ufw route allow from 94.229.246.136 to any port 51821
#WireGuard порт
ufw route allow from any to any port 51820
#доступ из сетей docker во внешний мир
ufw route allow from 172.16.0.0/12 to any
#Доступ из ipsec сети
ufw route allow from 10.10.30.0/24 to any
#Включаем фаервол
ufw enable
```

4) Настройка Ikev2

```
cd /etc/ipsec.d
```

#Генерируем ключи:

#CA

```
ipsec pki --gen --type rsa --size 4096 --outform pem > private/ca.pem  
ipsec pki --self --ca --lifetime 3650 --in private/ca.pem --type rsa --digest sha256 --dn "CN=91.149.232.254" --  
outform pem > cacerts/ca.pem
```

Серверный

```
ipsec pki --gen --type rsa --size 4096 --outform pem > private/debian.pem  
ipsec pki --pub --in private/debian.pem --type rsa | ipsec pki --issue --lifetime 3650 --digest sha256 --cacert  
cacerts/ca.pem --cakey private/ca.pem --dn "CN=91.149.232.254" --san 91.149.232.254 --flag serverAuth --  
outform pem > certs/debian.pem
```

Клиенты(client1,client2,client3 и т.д.):

```
ipsec pki --gen --type rsa --size 4096 --outform pem > private/client1.pem  
ipsec pki --pub --in private/client1.pem --type rsa | ipsec pki --issue --lifetime 3650 --digest sha256 --cacert  
cacerts/ca.pem --cakey private/ca.pem --dn "CN=client1" --san client1 --flag clientAuth --outform pem >  
certs/client1.pem
```

Генерируем pfx сертификат

```
openssl pkcs12 -export -out client1.pfx -inkey private/client1.pem -in certs/client1.pem -certfile cacerts/ca.pem  
zip client1.zip client1.pfx && mv client1.zip /var/www/html
```

Правим конфиги:

```
nano /etc/ipsec.conf
```

```
config setup  
    uniqueids=never  
    charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2, mgr 2"  
  
conn %default  
    keyexchange=ikev2  
    ike=aes256-aes128-sha256-sha1-modp3072-modp2048-modp1024  
    esp=aes256-aes128-sha256-sha1-modp3072-modp2048-modp1024  
    #ike=aes128gcm16-sha2_256-prfsha256-ecp256!  
    #esp=aes128gcm16-sha2_256-ecp256!  
    fragmentation=yes  
    rekey=no  
    compress=yes  
    dpdaction=clear
```



```
left=%any
leftauth=pubkey
leftsourceip=91.149.232.254
leftid=91.149.232.254
leftcert=debian.pem
leftsendcert=always
leftsubnet=0.0.0.0/0
right=%any
rightauth=pubkey
rightsourceip=10.10.30.0/24
rightdns=8.8.8.8,8.8.4.4
```

```
conn ikev2-pubkey
    auto=add
```

```
nano /etc/ipsec.secrets
```

```
: RSA debian.pem
```

```
ipsec restart
```

WireGuard

```
mkdir /opt/wireguard/ && cd /opt/wireguard/ && nano docker-compose.yml
```

```
version: "3.8"

services:
  wg-easy:
    environment:
      # ⚠ Required:
      # Change this to your host's public address
      - WG_HOST=91.149.232.254

      # Optional:
      - PASSWORD=PASS
      # - WG_PORT=51820
      #- WG_DEFAULT_ADDRESS=10.99.99.1
      - WG_DEFAULT_DNS=1.1.1.1
      # - WG_MTU=1420
```

```
# - WG_ALLOWED_IPS=192.168.15.0/24, 10.0.1.0/24
# - WG_PRE_UP=echo "Pre Up" > /etc/wireguard/pre-up.txt
# - WG_POST_UP=echo "Post Up" > /etc/wireguard/post-up.txt
# - WG_PRE_DOWN=echo "Pre Down" > /etc/wireguard/pre-down.txt
# - WG_POST_DOWN=echo "Post Down" > /etc/wireguard/post-down.txt
```

image: weejewel/wg-easy

container_name: wg-easy

volumes:

- ./etc/wireguard

ports:

- "51820:51820/udp"

- "51821:51821/tcp"

restart: unless-stopped

cap_add:

- NET_ADMIN

- SYS_MODULE

sysctls:

- net.ipv4.ip_forward=1

- net.ipv4.conf.all.src_valid_mark=1

```
docker compose up -d
```

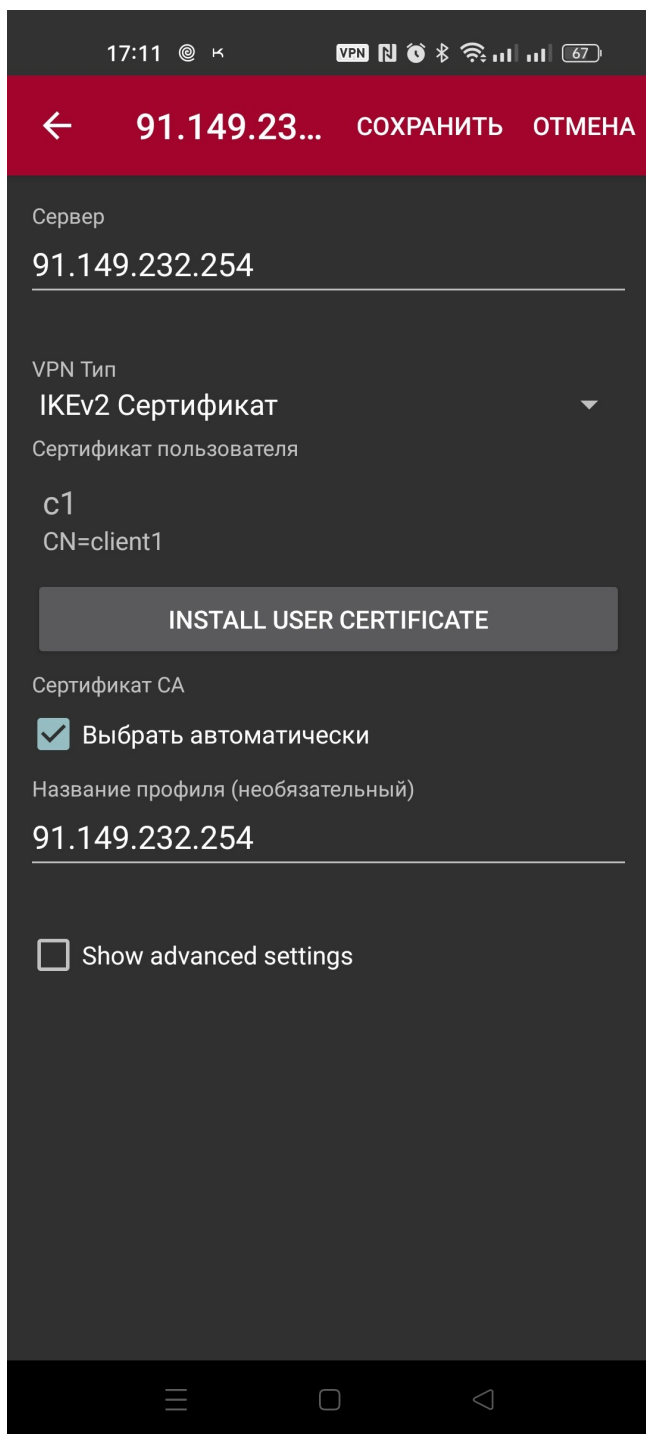
Ну и на последок

```
reboot
```

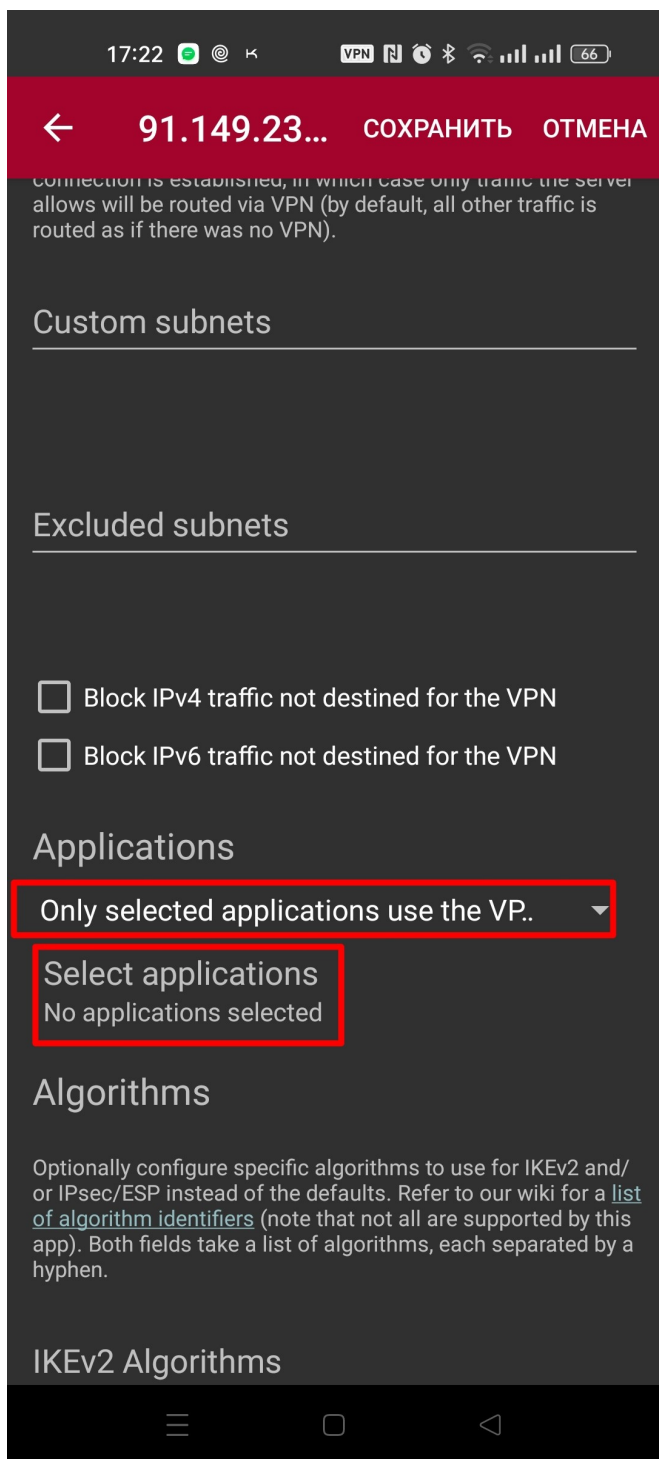
Для ikev2 на андроиде используем [strongSwan](#)

1) скачиваем созданный сертификат на телефон <http://91.149.232.254/client1.zip> и распаковываем его.

2) Запускаем приложение и создаем новый профиль, указываем сервер и тип vpn: IKEv2
Сертификат и жмем install user certificate и указываем на сертификат который мы скачали и распаковали в 1 пункте.



2.1) Если нужно что бы через впн работали только определенные приложения то ставим галочку на Show advanced settings и листаем до Applications, Жмем по All applications use the vpn и выбираем only selected applications use the vpn. Ниже появится пункт Select applications, нажимаем его и выбираем нужные нам приложения



3) Сохраняем настройки и подключаемся к vpn

Зпроху используется совместно с [плагином для браузера](#)

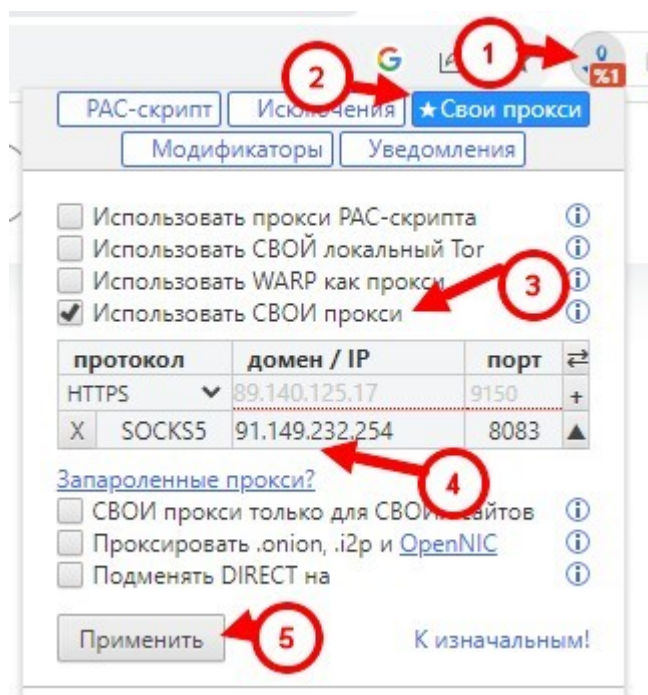
1) После установки плагина открываем его настройки

2) Выбираем пункт "Сво прокси"

3) Ставим галочку использовать СВОИ прокси

4) Жмем плюсики и добавляем наш прокси (протокол: SOCKS5, ip: ip_servera, port:8083)

5) жмем применить



После этого идем на сайт который не доступен в россии, например <https://ark.intel.com> и открываем настройки, переходим в исключения и добавляем *.intel.com (обычно плагин подставляет домен сам) Ставим переключатель на ДА и жмем готово. Снова открываем <https://ark.intel.com> и у нас открывается сайт без проблем(если он не заблокирован в стране где установлен наш сервер)

☒ авто

☒ да

☐ нет

☒ Учитывать исключения

☐ Ограничиться только [белым списком](#)

☐ Сбирать [последние ошибки](#) сайтов



- СЛОМАЛСЯ (заблокирован)
antizapret.prostovpn.org (ОБН5)
- Нужно ли менять DNS-сервера? (proton.me)
- Внеэеетровые блокировки добавлены в PAC-скрипт "Антицензорити"
- Готовь Тог пока не поздно
- СВОИ бесплатные прокси через CloudFlare WARP (нестабилен)
- Ускорение сёрфинга при помощи белого списка
- Версия для FireFox (Бета)
- Частые проблемы
- Новости PAC-скрипта «Антизапрет»
- Альтернативы нашему расширению

Готово

Поддержать

Проблемы?

Proxmox Virtual Environment

TASK ERROR: unsupported Debian version

Не удастся запустить или развернуть lxc контейнер свежего дистрибутива, на устаревшем PVE:

```
extracting archive '/var/lib/vz/template/cache/ubuntu-23.10-standard_23.10-1_amd64.tar.gz'
Total bytes read: 546263040 (521MiB, 110MiB/s)
Detected container architecture: amd64
Logical volume "vm-131-disk-0" successfully removed
TASK ERROR: unable to create CT 131 - unsupported Ubuntu version '23.10'
```

Надо поменять скрипт `/usr/share/perl5/PVE/LXC/Setup/Ubuntu.pm` так:

```
my $known_versions = {
    '23.10' => 1, # mantic <-----
    '20.04' => 1, # focal LTS
    '19.10' => 1, # eoan
```

или `/usr/share/perl5/PVE/LXC/Setup/Debian.pm` так:

```
die "unsupported debian version '$version'\n"
if !($version >= 4 && $version <= 13);
```

Как применить изменения не перезагружая PVE машину - не знаю.

Взял [тут](#)

Перестала запускаться MariaDB

```
mv /var/lib/mysql/tc.log /root/  
systemctl restart mariadb
```


OpenConnect VPN Cisco

<https://struchkov.dev/blog/ru/openconnect-vpn-server-cli/>

Не пробовал, но выглядит круто

<https://gist.github.com/alirezaomidi/9eeea3aa0a0a5a3404ea82f12741a475>

dig

Онлайн проверка

<https://xseo.in/dig>

Проверка SRV записи

dig +short _matrix._tcp.example.com SRV

Sing-box

```
{
  "log": {
    "level": "info"
  },
  "inbounds": [
    {
      "type": "http",
      "listen": "0.0.0.0",
      "listen_port": 10801
    }
  ],
  "outbounds": [
    {
      "type": "vless",
      "tag": "proxy",
      "server": "router.lala.org",
      "server_port": 18138,
      "uuid": "e2f6aa9e-0706-4485-853e-lallaxxxhui1",
      "tls": {
        "enabled": true,
        "server_name": "sovietunion.su",
        "utls": {
          "enabled": true,
          "fingerprint": "chrome"
        }
      },
      "reality": {
        "enabled": true,
        "public_key": "boberKurWaJa-Perdo_leJebanoeWXVLO_INKOrogxQ",
        "short_id": "423d37"
      }
    }
  ]
}
```