Использование Active Directory в качестве внешней службы каталогов

1. Требования

- Развернутый и настроенный домен `Active Directory`, в примере используется `ad.example.ru`;
- Создана сервисная учётная запись, в примере используется пользователь `zvirt` с паролем `P@ssw0rd`;
- Настроенный DNS на разрешение SRV-записи `_ldap._tcp.gc._msdcs.example.ru`;
- Для настройки безопасного соединения между сервером LDAP и менеджером управления нужен подготовленный сертификат центра сертификации в формате `pem`;
- Если анонимный поиск по LDAP запрещен, то необходимо предоставить сервисному пользователю разрешения на просмотр всех пользователей и групп в Active Directory;
- Если Active Directory охватывает несколько доменов, необходимо обратить внимание на ограничения описанные в файле `/usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties`;
- Установлен пакет `ovirt-engine-extension-aaa-ldap-setup` на менеджере управления.

Перейдите на менеджер управления виртуализацией и убедитесь в том, что в системе установлен пакет `ovirt-engine-extension-aaa-ldap-setup`:

```
rpm -q ovirt-engine-extension-aaa-ldap-setup
```

Произведите установку, в случае его отсутствия:

```
dnf install ovirt-engine-extension-aaa-ldap-setup
```

2. Подключение Active Directory

2.1. Подключение Active Directory (на примере протокола `plain`)

1. Перейдите на менеджер управления и запустите `ovirt-engine-extension-aaa-ldap-setup` для интерактивной установки:

```
ovirt-engine-extension-aaa-ldap-setup
```

2. Выберите тип LDAP. Для `Active Directory` выбрать пункт `3`.

```
Available LDAP implementations:
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IBM Security Directory Server
5 - IBM Security Directory Server RFC-2307 Schema
6 - IPA
7 - Novell eDirectory RFC-2307 Schema
8 - OpenLDAP RFC-2307 Schema
9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select:
```

3. Введите имя леса `Active Directory`.

```
Please enter Active Directory Forest name: ad-example.zvirt.com
[ INFO  ] Resolving Global Catalog SRV record for ad-example.zvirt.com
[ INFO  ] Resolving LDAP SRV record for ad-example.zvirt.com
```

4. Выберите протокол подключения (в примере используется `plain`):

```
NOTE:
It is highly recommended to use secure protocol to access the LDAP server.
Protocol startTLS is the standard recommended method to do so.
Only in cases in which the startTLS is not supported, fallback to non
standard ldaps protocol.
Use plain for test environments only.
Please select protocol to use (startTLS, ldaps, plain) [startTLS]: plain
```

5. Введите имя (DN) сервисного пользователя. Пользователь должен иметь разрешения для просмотра всех пользователей и групп на сервере каталогов. Если анонимный поиск разрешен, нажмите `Enter` без ввода.

```
Enter search user DN (empty for anonymous):
cn=user1,ou=Users,dc=test,dc=example,dc=com
Enter search user password:
```

Рекомендуется использовать запись в формате `CN=zvirt,DC=example,DC=ru`.

Получить данную строку можно, если перейти в оснастку `Active Directory` - `пользователи и компьютеры` - `Вид` - `Дополнительные компоненты`. Затем найти необходимую учетную запись, открыть `Свойства` - `Редактор атрибутов` - `distinguishedName`. Скопировать данное значение и указать его в сценарии подключения.

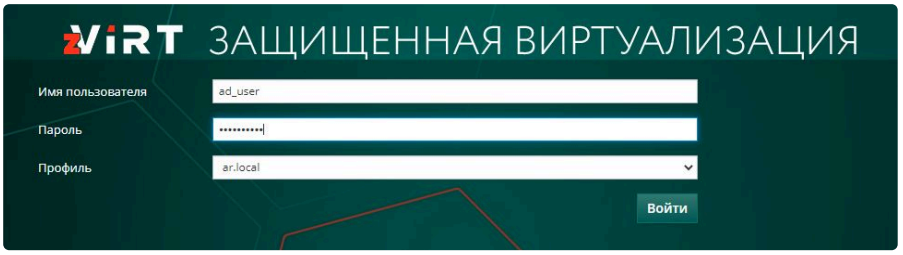
При указании в формате `uid=zvirt,dc=example,dc=ru` возможно возникновение ошибки: `ERROR otopi.plugins.ovirt_engine_extension_aaa_ldap.ldap.common common._customization_late:835 Cannot authenticate using 'uid=zvirt,dc=example,dc=ru`.

6. Укажите использовать SSO для виртуальных машин или нет. Функция включена по умолчанию, но ее нельзя использовать, если используется SSO для входа на портал администрирования. Имя профиля должно совпадать с именем домена.

```
Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:
```

7. Укажите имя профиля. Имя профиля доступно пользователям на странице входа. В этом примере используется `ar.local`.

```
Please specify profile name that will be visible to users:ar.local
```



Пользователям необходимо выбрать нужный профиль из раскрывающегося списка при первом входе в систему. Затем информация сохраняется в файлах `cookie` браузера и используется при следующем входе пользователя в систему.

Чтобы переименовать профиль после настройки домена, отредактируйте значение параметра `ovirt.engine.aaa.authn.profile.name` в файле `/etc/ovirt-engine/extensions.d/example.com-authn.properties`.

Перезапустите службу `ovirt-engine`, чтобы изменения вступили в силу.

8. Протестируйте возможность поиска по LDAP и вход в систему, чтобы убедиться, что домен `Active Directory` правильно подключен к zVirt. Для проверки возможности входа (login) необходимо указать имя учетной записи и пароль. Для проверки возможности поиска по LDAP от имени пользователя необходимо выбрать `Principal`, при использовании групп выбрать `Group`. В пункте `Resolve Groups` ввести `Yes` для получения информации о группе. Ввести `Done` для завершения настройки. По завершению настройки будут созданы три файла конфигурации.

```
NOTE:
It is highly recommended to test drive the configuration before applying it
into engine.
Login sequence is executed automatically, but it is recommended to also
execute Search sequence manually after successful Login sequence.
Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Login
Enter search user name: testuser1
Enter search user password:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Search
Select entity to search (Principal, Group) [Principal]:
Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
[ INFO  ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Done
[ INFO  ] Stage: Transaction setup
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Package installation
[ INFO  ] Stage: Misc configuration
[ INFO  ] Stage: Transaction commit
[ INFO  ] Stage: Closing up
          CONFIGURATION SUMMARY
          Profile name is: redhat.com
          The following files were created:
              /etc/ovirt-engine/aaa/redhat.com.properties
              /etc/ovirt-engine/extensions.d/redhat.com-authz.properties
              /etc/ovirt-engine/extensions.d/redhat.com-authn.properties
[ INFO  ] Stage: Clean up
          Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-
setup-20160114064955-1yar9i.log:
[ INFO  ] Stage: Pre-termination
[ INFO  ] Stage: Termination
```

9. После выполнения подключения Active Directory к zVirt перезапустите службу `ovirt-engine`:

```
systemctl restart ovirt-engine
```

10. Созданный профиль теперь доступен на портале администрирования и на страницах входа. Чтобы назначить учетным записям пользователей соответствующие роли и разрешения, например, для входа на портал виртуальных машин, см. Предоставление прав пользователям Active Directory.

2.2. Дополнительные действия при подключении Active Directory с использованием протоколов startTLS или

LDAPS

Необходимо:

1. Загрузить корневой сертификат центра сертификации или самоподписанный сертификат контроллера Active Directory в формате `.cer` (Base 64 encoded X.509) на менеджер управления в каталог `/root`.
2. Добавить сертификат в `доверенные корневые центры сертификации`:

```
cp ca.cer /etc/pki/ca-trust/source/anchors/
update-ca-trust force-enable
update-ca-trust extract
```

3. Убедиться, что SRV-записи успешно разрешается:

```
dig _ldap._tcp.gc._msdcs.example.ru SRV
dig _ldap._tcp.example.ru SRV
```

> Для настройки подключения с использованием `ldaps` контроллеру Active Directory должен быть выдан сертификат `Kerberos Authentication`.

4. Запустить `ovirt-engine-extension-aaa-ldap-setup`, пройти процедуру подключения Active Directory и на вопросе `Please select protocol to use` выбрать протокол (в примере `startTLS`). Например:

```
NOTE:
It is highly recommended to use secure protocol to access the LDAP server.
Protocol startTLS is the standard recommended method to do so.
Only in cases in which the startTLS is not supported, fallback to non
standard ldaps protocol.
Use plain for test environments only.
Please select protocol to use (startTLS, ldaps, plain) [startTLS]: startTLS
Please select method to obtain PEM encoded CA certificate (File, URL,
Inline, System, Insecure): System ①
Please enter the password:
```

① Возможно указать следующие значения:

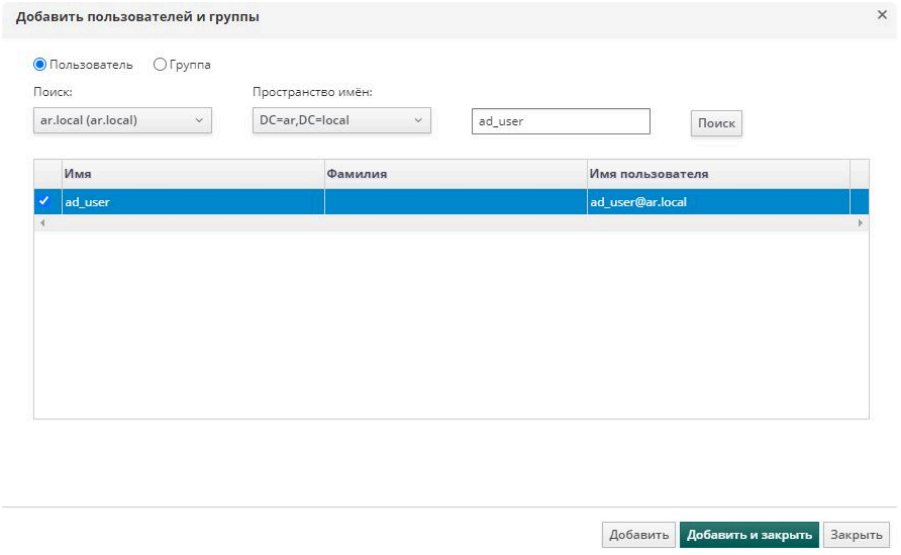
- `File` - позволяет указать полный путь к сертификату.
- `URL` - позволяет указать URL-адрес сертификата.
- `Inline` - позволяет вставить содержимое сертификата в терминал.
- `System` - позволяет указать расположение по умолчанию для всех файлов CA.
- `Insecure` - пропускает проверку сертификата, но соединение по-прежнему шифруется с помощью TLS.

3. Предоставление прав пользователям Active Directory

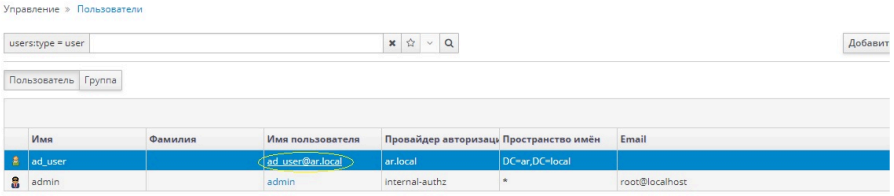
По умолчанию пользователи домена не могут входить в систему, поэтому им необходимо назначить нужные права доступа.

Порядок действий:

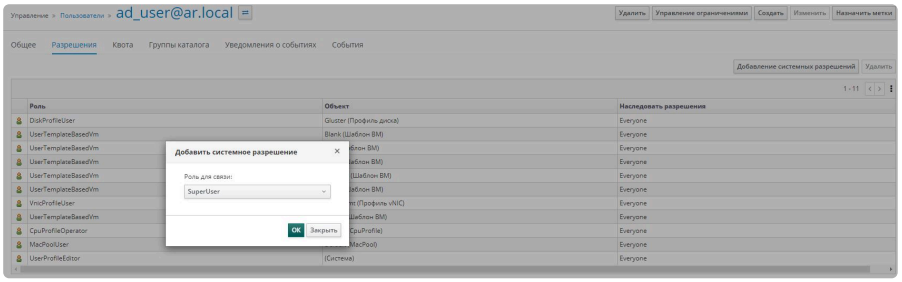
1. Перейдите на портал администрирования с использованием учётной записи администратора.
2. Перейдите в **Управление** > **Пользователи**, нажмите **[Добавить]**. В выпадающем списке **Поиск** выберите имя добавленного домена. В пустом поле введите имя учетной записи которую требуется добавить и нажмите **[Поиск]**, выберите пользователя и нажмите **[Добавить]** или **[Добавить и закрыть]**.



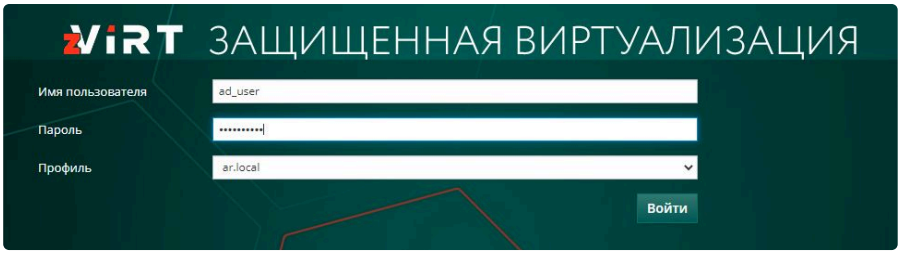
3. Выберите добавленного пользователя, нажав на его имя в поле **Имя пользователя**.



4. Перейдите в раздел **Разрешения**, нажмите **[Добавление системных разрешений]**.



5. Если назначенные права позволяют входить пользователю на портал, то выполните вход от имени пользователя, выбрав в поле **Профиль** имя домена.



4. Удаление подключения Active Directory

4.1. Удаление профиля

Перейдите в консоль менеджера управления и удалите конфигурационные файлы:

```
rm -f /etc/ovirt-engine/extensions.d/example.ru.properties
rm -f /etc/ovirt-engine/extensions.d/example.ru-authn.properties
rm -f /etc/ovirt-engine/aaa/example.ru.properties
```

Затем произведите перезапуск службы `ovirt-engine`:

```
systemctl restart ovirt-engine
```

4.2. Удаление пользователей

Перейдите на портал администрирования с рабочего места администратора и удалите пользователей, которые используют удаленный профиль.

5. Дополнительные сведения

5.1. Проверка подключения к LDAP-серверу

При подключении к внешнему серверу аутентификации может возникнуть потребность в проверке, например, наличия в каталоге пользователя, от имени которого zVirt будет осуществлять подключение.

На менеджере управления следует установить пакет `openldap-clients`:

```
dnf config-manager --enable baseos
dnf install openldap-clients
dnf config-manager --disable baseos
```

Сделать запрос:

```
ldapsearch -H ldap://name_server -x -W -D "
<Тут_логин_Администратора_домена>@domain.name" -b "dc=domane,dc=name" "
(sAMAccountName=zvirtadm)"
```

5.2. Диагностика и исправление ошибок при подключении Active Directory

Если попытка подключения к внешнему серверу аутентификации Active Directory заканчивается неудачно и в логе есть запись вида `Cannot resolve principal 'ovirtadm@nprt.nn'`, то это может сигнализировать о том, что служба глобального каталога работает не на стандартном порту `3268`, а `389`. Следует проверить сервисные записи DNS:

```
dig _ldap._tcp.gc._msdcs.nprt.nn SRV
dig _ldap._tcp.nprt.nn SRV
```

Если действительно обе службы (и локальный контроллер домена тоже) работают на одном порту, то следует для глобального каталога установить порт `3268`.

5.3. Ограничения

Профиль `LDAP_MATCHING_RULE_IN_CHAIN` используется для получения групп пользователей. На текущий момент в данном профиле есть проблема, которая заключается в том, что он не может разрешить локальное доменное имя группы принадлежащей нескольким доменам. Например:

Если пользователь `user1` является членом `group1`, а `group1` является членом `group2`, то этот профиль не разрешит данную конфигурацию. Профиль может разрешить конфигурацию, если `user1` будет непосредственным членом `group2` в `AD2`. Шаблон `LDAP_MATCHING_RULE_IN_CHAIN` используется, так как дает значительный прирост производительности по сравнению с рекурсивным обходом.

5.4. Долгий вход доменного пользователя

При большом количестве объектов в Active Directory и/или большом количестве доменных групп у пользователя, вход доменного пользователя может занимать продолжительное время, также при открытие окна разрешений пользователя может занимать длительное время или приводить к зависанию менеджера управления. Для решения данных проблем необходимо исправить файл конфигурации `/etc/ovirt-engine/aaa/example.ru.properties`. Параметр `include = <ad.properties>` заменить на `include = <ad-recursive.properties>`.

Обновления пароля для пользователя admin

При планировании смены пароля пользователя *admin* необходимо предусмотреть сервисное окно в работе сервиса engine, т.к. потребуется перезагрузка провайдера. Работа и доступность ВМ при этом не будут прерываться.

Порядок действий:

1. Подключитесь по SSH к Менеджеру управления
2. Выполните команду для сброса пароля:

```
ovirt-aaa-jdbc-tool user password-reset admin --password-valid-to="2025-08-01 12:00:00-0800"
    Password:
    updating user admin...
    user updated successfully
```

Нужно задать значение для `--password-valid-to`, иначе срок действия пароля будет по умолчанию установлен как истекающий прямо сейчас. Дата указывается в формате `гггг-ММ-дд ЧЧ:мм:ссX` (`yyyy-MM-dd HH:mm:ssX`). В этом примере -0800 обозначает GMT минус 8 часов. Для просмотра полного списка параметров выполните `ovirt-aaa-jdbc-tool user password-reset --help`.

Если пользователь заблокирован, его можно разблокировать с помощью команды `ovirt-aaa-jdbc-tool user unlock admin`.

3. Перейдите на портал администрирования и авторизуйтесь.
4. Нажмите **Управление (Administration) > Провайдеры (Providers)**.
5. Выберите **ovirt-provider-ovn**.
6. Нажмите **[Изменить (Edit)]** и введите новый пароль в поле **Пароль (Password)**.
7. Нажмите **[Тестировать (Test)]**, чтобы проверить, проходит ли успешно аутентификация с предоставленными учетными данными.
8. После успешной проверки аутентификации нажмите **[OK]**.
9. Перезапустите сервис провайдера:

```
systemctl restart ovirt-provider-ovn.service
```

Настройка менеджера управления для аутентификации с помощью SSO через LDAP и Kerberos на веб-портале zVirt

SSO позволяет пользователям входить на портал администрирования и пользовательский портал без ввода пароля. Учетные данные получаются с сервера Kerberos.

Если используется SSO для входа на веб-портал, аутентификация на ВМ с помощью SSO невозможна.

1. Шаг 1. Перейдите на контроллер домена

1. Создайте сервисную учётную запись (далее-УЗ).
   - В поле `Имя` укажите имя для УЗ (в примере используется `zvirt`);
   - В поле `Имя входа пользователя` укажите `HTTP/srv.domain.local`; где `srv` - имя сервера менеджера управления виртуализацией, `domain.local` - имя домена.
2. Откройте свойства УЗ и перейдите на вкладку `Учетная запись` в `Параметры учетной записи`:
   - Выключите `Требовать смены пароля при следующем входе в систему`;
   - Включите `Срок действия пароля не ограничен` (опционально);
   - Включите `Данная учетная запись поддерживает 128-разрядное шифрование` и `Данная учетная запись поддерживает 256-разрядное шифрование`;
   - Сохраните изменения.
3. Откройте интерпретатор командной строки (`cmd`) с правами администратора и создайте файл `keytab` для службы `Apache`:

   ```
   ktpass /out C:\Temp\http.keytab /princ HTTP/srv.domain.local@DOMAIN.LOCAL
   /pass PASSWORD /mapuser $ZVIRT_USER_DN /ptype KRB5_NT_PRINCIPAL /crypto ALL
   ```

   Вместо `$ZVIRT_USER_DN` введите `Distinguished Name` пользователя, который был создан на первом шаге
4. Перейдите в директорию `Temp`:

   ```
   cd C:\Temp
   ```

5. Скопируйте полученный ключ на менеджер управления среды виртуализации:

```
scp http.keytab root@srv.domain.local:/etc/httpd
```

2. Шаг 2. Перейдите в консоль менеджера управления виртуализации

1. Установите права доступа на файл `keytab`:

```
chown apache /etc/httpd/http.keytab
chmod 400 /etc/httpd/http.keytab
```

2. Установите контекст Selinux для keytab файла:

```
semanage fcontext -a -e /etc/httpd/httpd.conf /etc/httpd/http.keytab
restorecon -Rv /etc/httpd/http.keytab
```

3. Установите необходимые пакеты:

```
dnf install -y ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap mod_auth_gssapi mod_session
```

> В случае недоступности пакетов `mod_auth_gssapi` и `mod_session` в репозитории необходимо:
>
> - Включить дополнительный репозиторий: `dnf config-manager --enable appstream`;
> - Установить пакеты: `dnf install -y mod_auth_gssapi mod_session`;
> - Выключить дополнительный репозиторий: `dnf config-manager --disable appstream`.

4. Скопируйте файл `ovirt-sso.conf` в каталог веб-сервера `Apache`:

```
cp /usr/share/ovirt-engine-extension-aaa-ldap/examples/ad-sso/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

5. Скопируйте шаблоны конфигурации и укажите соответствующее имя домена в названии файла.

   Файл конфигурации LDAP

   ```
   cp /usr/share/ovirt-engine-extension-aaa-ldap/examples/ad-sso/aaa/profile1.properties /etc/ovirt-engine/aaa/domain.local.properties
   ```

   Файл конфигурации авторизации

```
cp /usr/share/ovirt-engine-extension-aaa-ldap/examples/ad-sso/extensions.d/profile1-authz.properties /etc/ovirt-engine/extensions.d/domain.local-authz.properties
```

Файл конфигурации аутентификации

```
cp /usr/share/ovirt-engine-extension-aaa-ldap/examples/ad-sso/extensions.d/profile1-http-authn.properties /etc/ovirt-engine/extensions.d/domain.local-http-authn.properties
```

Файл конфигурации проверки подлинности

```
cp /usr/share/ovirt-engine-extension-aaa-ldap/examples/ad-sso/extensions.d/profile1-http-mapping.properties /etc/ovirt-engine/extensions.d/domain.local-http-mapping.properties
```

6. Отредактируйте файл конфигурации `LDAP`, при необходимости укажите тип сервера `LDAP`, а также укажите имя домена, учетную запись и пароль для неё:

```
nano /etc/ovirt-engine/aaa/domain.local.properties
```

Пример основных параметров:

```
vars.forest = domain.local
vars.user = $ZVIRT_USER_DN
vars.password = PASSWORD
```

Вместо $ZVIRT_USER_DN введите Distinguished Name пользователя, который был создан на первом шаге

7. Отредактируйте файл конфигурации `аутентификации`. Имя профиля, видимое пользователям на веб-портале, определяется параметром `ovirt.engine.aaa.authn.profile.name`:

```
nano /etc/ovirt-engine/extensions.d/domain.local-http-authn.properties
```

Приведите указанные параметры к виду:

```
ovirt.engine.extension.name = domain.local-http-authn
ovirt.engine.aaa.authn.profile.name = domain.local-http
ovirt.engine.aaa.authn.authz.plugin = domain.local-authz
ovirt.engine.aaa.authn.mapping.plugin = domain.local-http-mapping
```

8. Отредактируйте файл конфигурации `авторизации`:

```
nano /etc/ovirt-engine/extensions.d/domain.local-authz.properties
```

Приведите указанные параметры к виду:

```
ovirt.engine.extension.name = domain.local-authz
config.profile.file.1 = ../aaa/domain.local.properties
```

9. Отредактируйте файл конфигурации `проверки подлинности`:

```
nano /etc/ovirt-engine/extensions.d/domain.local-http-mapping.properties
```

Приведите указанный параметр к виду:

```
ovirt.engine.extension.name = domain.local-http-mapping
```

10. Установите права доступа на файлы конфигурации:

```
chown ovirt:ovirt /etc/ovirt-engine/aaa/*
chown ovirt:ovirt /etc/ovirt-engine/extensions.d/*
chmod 600 /etc/ovirt-engine/aaa/domain.local.properties
chmod 640 /etc/ovirt-engine/extensions.d/domain.local*
```

11. Перезапустите службы `apache` и `ovirt-engine`:

```
systemctl restart httpd.service
systemctl restart ovirt-engine.service
```

3. Шаг 3. Настройка браузера

3.1. Настройка SSO-аутентификация через Kerberos для браузера Mozilla Firefox

При использовании браузера Mozilla Firefox для входа на веб-портал zVirt с помощью режима аутентификации по протоколу `Kerberos`, необходимо выполнить дополнительную настройку браузера.

Для этого в адресной строке браузера необходимо набрать `about:config` и в значение параметров `network.negotiate-auth.trusted-uris`, `network.automatic-ntlm-auth.trusted-uris` добавить имя доменной зоны или сервера аутентификации, например, `domain.local` или `srv-ad01.domain.local`.

3.2. Настройка SSO-аутентификация через Kerberos для браузеров `Internet Explorer` и `Google Chrome`

При использовании браузеров `Internet Explorer` и `Google Chrome` для входа на веб-портал zVirt и режима аутентификации по протоколу `Kerberos`, необходимо выполнить настройку в браузере `Internet Explorer`.

1. Открыть браузер `Internet Explorer`.
2. В контекстном меню настроек выбрать пункт `Internet Options` (Свойства браузера);
3. В диалоговом окне настроек выбрать `Security` (Безопасность);
4. Выбрать зону `Local Intranet` (Местная интрасеть), нажать кнопку `Sites` (Сайты);
5. В появившемся диалоговом окне отметить параметры `Все сайты интрасети…`, `Все сайты`, `подключение…` и `Все сетевые пути`.
6. Нажать кнопку `Advanced` (Дополнительно).
7. В появившемся диалоговом окне ввести URL-адрес веб-портала zVirt (например, https://zvirt.domain.local/) и нажать **[Add (Добавить)]**.
8. Закрыть все диалоговые окна с сохранением настроек нажатием **[OK]**.

4. Настройка с SSL/TLS.

4.1. Настройка startTLS

1. Добавить корневой сертификат центра сертификации или самоподписываемый сертификат контроллера Active Directory.

   Загрузить сертификат в формате .cer(Base 64 encoded X.509) на сервер в каталог /root.

   Добавить сертификат в хранилище доверенных корневых центров сертификации:

   ```
   keytool -importcert -noprompt -trustcacerts -alias MyCer -file
   /root/MyCer.cer -keystore /etc/ovirt-engine/aaa/myrootca.jks -storepass
   password
   ```

2. Убедиться, что SRV-записи успешно резолвится:

   ```
   dig _ldap._tcp.gc._msdcs.example.ru SRV
   dig _ldap._tcp.example.ru SRV
   ```

3. Раскоментировать и отредактировать в файле `/etc/ovirt-engine/aaa/domain.local.properties` строки:

```
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /etc/ovirt-engine/aaa/myrootca.jks
pool.default.ssl.truststore.password = password
```

4. Перезапустить службу

```
systemctl restart ovirt-engine
```

4.2. Настройка LDAPS

1. Добавить сертификат центра сертификации или самоподписываемый сертификат контроллера Active Directory. Контроллеру Active Directory должен быть выдан сертификат "Kerberos Authentication".

   Загрузить сертификат в формате .cer(Base 64 encoded X.509) на сервер в каталог /root.

   Добавить сертификат в хранилище доверенных корневых центров сертификации:

```
keytool -importcert -noprompt -trustcacerts -alias MyCer -file
/root/MyCer.cer -keystore /etc/ovirt-engine/aaa/myrootca.jks -storepass
password
```

2. Убедиться, что SRV-записи успешно резолвится:

```
dig _ldaps._tcp.gc._msdcs.example.ru SRV
dig _ldaps._tcp.example.ru SRV
```

3. Добавить в файл `/etc/ovirt-engine/aaa/domain.local.properties` строки:

```
pool.default.serverset.srvrecord.service = ldaps
pool.default.ssl.enable = true
```

   раскоментировать и отредактировать:

```
pool.default.ssl.truststore.file = /etc/ovirt-engine/aaa/myrootca.jks
pool.default.ssl.truststore.password = password
```

4. Перезапустить службу

```
systemctl restart ovirt-engine
```

Настройка политики паролей

1. Использование утилиты ovirt-aaa-jdbc-tool

С версии zVirt 4.1 политики, заданные данным инструментом, применяются также к паролям, которые устанавливаются через портал администрирования.

Утилита **ovirt-aaa-jdbc-tool** позволяет переопределить политику паролей по умолчанию, которая применяется к паролям, задаваемым посредством **ovirt-aaa-jdbc-tool**

Политика паролей может быть задана с помощью параметров, описанных в таблице.

Таблица 1. Параметры, относящиеся к политике паролей

Параметр	**Описание**	**Значение по умолчанию**
MIN_LENGTH	Определяет минимальную длину пароля.	6
PASSWORD_EXPIRATION_DAYS	Определяет срок действия для новых паролей (в днях).	180
PASSWORD_HISTORY_LIMIT	Количество старых паролей, которые не должны повторяться при смене пароля.	3
PASSWORD_EXPIRATION_NOTICE_DAYS	Определяет за сколько дней до истечения срока действия пароля уведомлять пользователя (в днях).	0

Параметр	Описание	Значение по умолчанию
PASSWORD_COMPLEXITY	Шаблон, определяющий сложность пароля в формате: `name:chars=x::min=y::...` где: • **name** - название правила. • **x** - перечисление символов. Символы `\t, \n, \f, \', \"` можно использовать, но в шаблоне их нужно экранировать следующим образом: `\\t, \\n, \\f, \\', \\"`. • **y** - минимальное количество указанных символов в пароле. Значение `min=-1` снимает ограничение на количество соответствующих символов. Все правила должны быть введены в одну строку без пробелов.	***UPPERCASE:chars=ABCDEFGHIJKLMNOPQRSTUVWXYZ::min=1 LOWERCASE:chars=abcdefghijklmnopqrstu-vwxyz::min=1 NUMBERS:chars=0123456789::min=1 SYMBOLS:chars=@#$%^&*()_-=.::min=1***
ALLOW_EXPIRED_PASSWORD_CHANGE	Логическое значение, разрешающее/запрещающее пользователю изменять пароль после истечения срока действия. Если установлено значение `true` - изменение пароля разрешено.	true

1.1. Просмотр текущих значений параметров

Для получения текущего значения нужного параметра используйте следующий синтаксис:

```
ovirt-aaa-jdbc-tool settings show --name=<param-name> ①
```

① - вместо `<param-name>` введите имя параметра.

Например, для просмотра значения параметра `PASSWORD_COMPLEXITY` используйте следующую команду:

```
ovirt-aaa-jdbc-tool settings show --name=PASSWORD_COMPLEXITY

-- setting --
name: PASSWORD_COMPLEXITY
value:
UPPERCASE:chars=ABCDEFGHIJKLMNOPQRSTUVWXYZ::min=1::LOWERCASE:chars=abcdefghijklm
nopqrstuvwxyz::min=1::NUMBERS:chars=0123456789::min=1::SYMBOLS:chars=@#$%^&*()_-
=.::min=1::
type: class java.lang.String
description: complexity groups definition.
format:\n[name:chars=x::min=y::...]\nmin=-1 no limit. following chars should be
escaped: \\t, \\n, \\f, \\', \\" \\\\
```

1.2. Изменение значений параметров

Для изменения значения соответствующего параметра используется следующий синтаксис:

```
ovirt-aaa-jdbc-tool settings set \
    --name=<param-name> \ ①
    --value=<param-value> ②
```

① - вместо `<param-name>` введите имя параметра.

② - вместо `<param-value>` введите значение параметра.

Примеры:

Пример 1. Изменение срока действия пароля

Команда ниже установит срок действия новых паролей на 365 дней.

```
ovirt-aaa-jdbc-tool settings set \
    --name=PASSWORD_EXPIRATION_DAYS \
    --value=365
```

Пример 2. Изменение сложности паролей

```
ovirt-aaa-jdbc-tool settings set \
    --name=PASSWORD_COMPLEXITY \
    --
value=UPPERCASE:chars=ABCDEFGHIJKLMNOPQRSTUVWXYZ::min=1::LOWERCASE:chars=abcd
efghijklmnopqrstuvwxyz::min=1::NUMBERS:chars=0123456789::min=-1::SYMBOLS:char
s=@#$%^&*()_-=.::min=-1::
```

В примере выше устанавливаются следующие правила в отношении сложности паролей:

- В пароле могут присутствовать:
  - заглавные буквы;
  - строчные буквы;
  - цифры;
  - специальные символы из следующего списка: `@#$%^&*()_`.
- Обязательно наличие хотя бы одной заглавной буквы (UPPERCASE…min=1).
- Обязательно наличие хотя бы одной строчной буквы (LOWERCASE…min=1).
- Наличие цифр в пароле не обязательно (NUMBERS…min=-1).
- Наличие специальных символов в пароле не обязательно (SYMBOLS…min=-1).

2. Использование утилиты engine-config

В версиях zVirt 4.0 и старше политики, заданные данным инструментом, применяются только к паролям, которые устанавливаются через портал администрирования.

В версиях zVirt 4.1 и новее для настройки политики паролей используйте утилиту ovirt-aaa-jdbc-tool.

Утилита **engine-config** позволяет переопределить политику паролей по умолчанию, которая применяется в отношении паролей, заданных через портал администрирования.

Политика может быть задана с помощью параметров, описанных в таблице.

Таблица 2. Параметры, относящиеся к политике паролей

Параметр	Описание	Значение по умолчанию

Параметр	Описание	Значение по умолчанию
InternalUserPasswordPattern	Определяет шаблон проверки пароля, используемый при создании внутреннего пользователя. В качестве значения ожидается тип **String**, поэтому при изменении значения указывайте его в двойных кавычках (''…'').	`(?=.[a-z])(?=.[A-Z])(?=.[0-9])(?=.[@#$%^&*()_\-=.]).{6,}` Данный шаблон интерпретируется следующим образом: • Минимальная длина пароля - 6 символов (`{6,}`). • Пароль должен содержать хотя бы одну строчную букву. • Пароль должен содержать хотя бы одну заглавную букву. • Пароль должен содержать хотя бы одну цифру. • Пароль должен содержать хотя бы один спецсимвол из набора `@#$%^&*()_\-=.`
ChangeUserPasswordTimeout	Определяет количество дней, в течение которых пользователь может изменить пароль. Допустимые значения от 0 до 3000.	60

2.1. Просмотр текущих значений параметров

Для получения текущего значения нужного параметра используйте следующий синтаксис:

```
engine-config --get <param-name> ①
```

① - вместо `<param-name>` введите имя параметра.

Например, для просмотра текущего шаблона проверки пароля, используйте следующую команду:

```
engine-config --get InternalUserPasswordPattern

InternalUserPasswordPattern: (?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[@#$%^&*()_\-=.]).{6,} version: general
```

2.2. Изменение значений параметров

Для изменения значения соответствующего параметра используется следующий синтаксис:

```
engine-config --set <param-name>=<param-value> ① ②
```

① - вместо `<param-name>` введите имя параметра.

② - вместо `<param-value>` введите значение параметра.

Пример:

Пример 3. Изменение требования к длине пароля

Команда ниже установит минимальную длину пароля равной 12 символам.

```
engine-config --set InternalUserPasswordPattern="(?=.*[a-z])(?=.*[A-Z])(?=.*
[0-9])(?=.*[@#$%^&*()_\-=.]).{12,}"
```

Изменение длительности сессии пользователя

1. Способы изменения длительности сессии

1.1. При использовании AAA-JDBC

Для настройки пользовательских параметров в системе zvirt можно использовать утилиту **engine-config** (для режима HE необходимо войти в консоль BM Hosted Engine).

Один из настраиваемых параметров - назначение времени сессий для пользователя.

Изменить время сессии для пользователя в системе zvirt можно:

- Глобально для всех пользователей, для этого:
  1. Войдите в консоль Менеджера управления.
  2. С помощью утилиты **engine-config** установите необходимое значение для параметра **UserSessionTimeOutInterval**.

     Параметр устанавливает значение для всех доступов: Пользовательский портал/ Портал администрирования/API.

     Задание значения для параметра **UserSessionTimeOutInterval**:

     ```
     engine-config -s UserSessionTimeOutInterval=20
     ```

     Время пользовательской сессии устанавливается в минутах
  3. Перезапустите службу **ovirt-engine**:

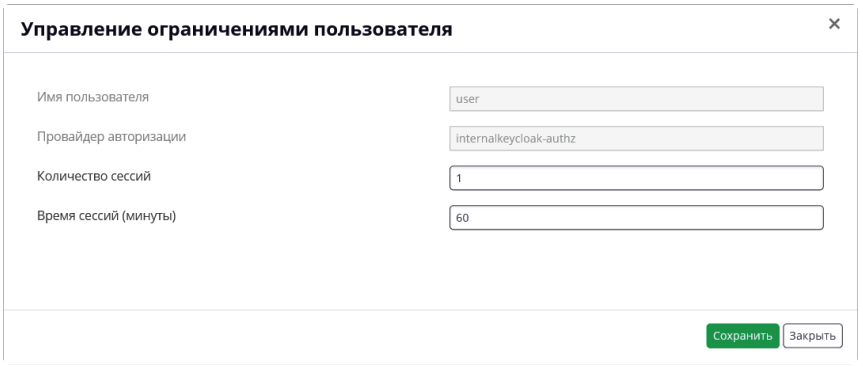
     ```
     systemctl restart ovirt-engine
     ```
  4. Проверьте, что значение сохранено и назначено:

     ```
     engine-config -g UserSessionTimeOutInterval
     ```

     Ожидаемый вывод:

```
UserSessionTimeOutInterval: 20 version: general
```

- Для отдельного пользователя системы посредством UI. Для этого:
  1. На портале администрирования перейдите в **Управление > Пользователи**.
  2. Выделите нужного пользователя и нажмите **[Управление ограничениями]**.
  3. В появившемся окне установите значение для параметра **Время сессий (минуты)**.



  4. Нажмите **[Сохранить]**.
  5. Войдите в консоль Менеджера управления.
  6. Перезапустите службу **ovirt-engine**:

```
systemctl restart ovirt-engine
```

По умолчанию время пользовательской сессии (параметр **UserSessionTimeOutInterval**) равно 30 мин. Значения времени пользовательской сессии устанавливается в пределах от 1 до 100000 минут (`UserSessionTimeOutInterval.validValues=1..100000`).

1.2. При использовании Keycloak

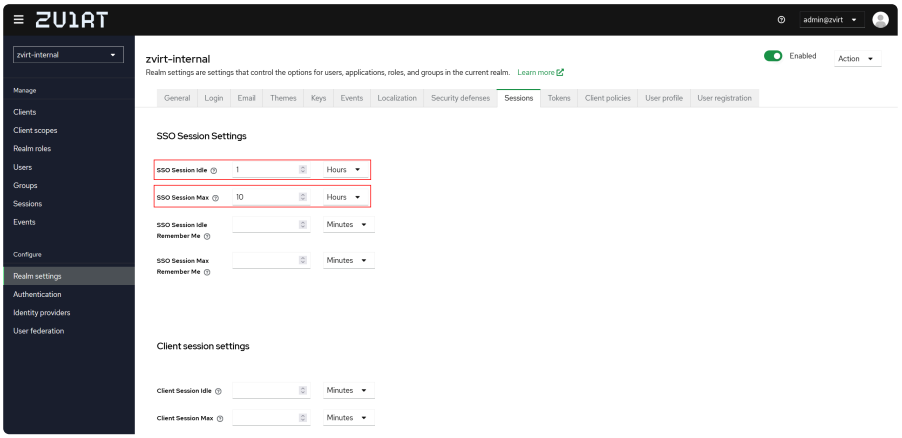
В zVirt 4.4 с интергрированным Keycloak для настройки длительности сессии пользователей необходимо выполнить следующее:

1. Подключитесь к порталу Keycloak с ролью администратора пространства zvirt-internal (по умолчанию admin@zvirt).
2. Перейдите в раздел **Realm settings**.
3. На вкладке **Sessions** настройте необходимые параметры длительности сессии и нажмите **[Save]**:
   - **SSO Session Idle**: определяет максимальное время неактивности сессии Single Sign-On (SSO), после которого она автоматически завершается и пользователь снова будет вынужден пройти аутентификацию. В общем случае для управления длительностью сессии пользователя, необходимо настраивать именно этот параметр.

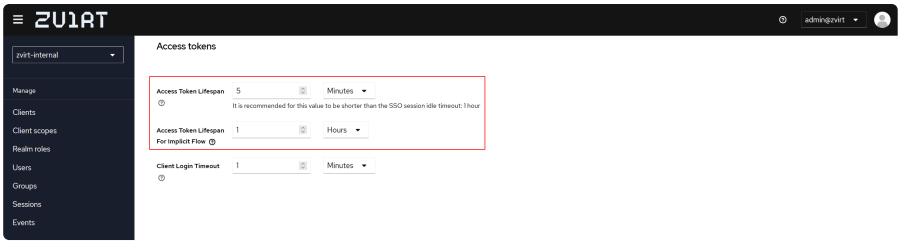
- **SSO Session Max**: определяет максимальную продолжительность жизни сессии Single Sign-On (SSO). Это абсолютная длительность существования сессии независимо от уровня активности пользователя.
- **SSO Session Idle Remember Me**: действует аналогично **SSO Session Idle**, но применяется только к пользователям, которые воспользовались функцией **Remember me**. Если значение не задано, будет использоваться параметр **SSO Session Idle**.
- **SSO Session Max Remember Me**: действует аналогично **SSO Session Max**, но применяется только к пользователям, которые воспользовались функцией **Remember me**. Если значение не задано, будет использоваться параметр **SSO Session Max**.

Функция **Remember me** по умолчанию отключена.

- **Client Session Idle**: действует аналогично **SSO Session Idle**, но применяется к каждой клиентской сессии, установленной с отдельным клиентом (application). Если значение не задано, будет использоваться параметр **SSO Session Idle**.
- **Client Session Max**: действует аналогично **SSO Session Max**, но применяется к каждой клиентской сессии, установленной с отдельным клиентом (application). Если значение не задано, будет использоваться параметр **SSO Session Max**.



4. На вкладке **Tokens** в разделе **Access Tokens** настройте необходимые сроки действия токенов и нажмите **[Save]**:
   - **Access Token Lifespan**: определяет срок действия токенов доступа (access tokens), используемых клиентами для авторизированного доступа к ресурсам (например, для выполнения запросов к API). После истечения указанного времени токен становится недействительным и требуется запрос нового токена. Рекомендуется указывать значение меньшее, чем установленное для параметра **SSO Session Idle**.
   - **Access Token Lifespan For Implicit Flow**: определяет срок действия токенов доступа (access tokens), выданных в рамках протокола OAuth 2.0.



5. Настройте необходимые значения для глобального параметра **UserSessionTimeOutInterval** и для отдельных пользователей.

> Время жизни сессии, настроенное с помощью параметра **UserSessionTimeOutInterval**, должно быть меньше значения **SSO Session Idle** в Keycloak.

2. Приоритеты значений длительности пользовательской сессии

- Для пользователей (включая admin), у которых в настройках **Время сессий** на портале администрирования выставлено значение **0**, применяется глобальная настройка.
- При развертывании Менеджера управления для пользователя admin по умолчанию устанавливается длительность сессии **0**, для остальных пользователей - **60**.
- Если через портал администрирования для пользователя установлено время сессии, отличное от **0**, то оно имеет приоритет над временем, заданным глобально через параметр **UserSessionTimeOutInterval**. При этом порядок ввода значений (для конкретного пользователя или глобально) не имеет значения.

В zVirt 4.4 и выше, при настроенной интеграции с Keycloak необходимо учитывать следующее:

- Время сессии на пользовательском портале соответствует значению, установленному в Keycloak.
- Время сессии на портале администрирования соответствует значению, установленному в глобальном параметре **UserSessionTimeOutInterval** или через портал администрирования.

Дополнительная настройка виртуальных машин

1. Настройка операционных систем с помощью osinfo

zVirt хранит конфигурации операционных систем для виртуальных машин в файле **/etc/ovirt-engine/osinfo.conf.d/00-defaults.properties**, который содержит значения по умолчанию, например:
`os.other.devices.display.protocols.value = spice/qxl,vnc/vga,vnc/qxl`.

Ситуаций, когда эти значения нужно редактировать, довольно мало:

- Добавление ОС, которой нет в списке поддерживаемых гостевых ОС.
- Добавление ключа продукта (например, `os.windows_10x64.productKey.value =`).
- Настройка пути `sysprep` для виртуальной машины Windows (например, `os.windows_10x64.sysprepPath.value = ${ENGINE_USR}/conf/sysprep/sysprep.w10x64`).

Не редактируйте сам файл **00-defaults.properties**. После обновления или восстановления Менеджера управления изменения будут перезаписаны.

Не изменяйте значения, переданные непосредственно из ОС или Менеджера управления, например, максимальный объем памяти.

Чтобы изменить настройки ОС, создайте переопределяющий файл в папке **/etc/ovirt-engine/osinfo.conf.d/**. Имя файла должно начинаться со значения больше `00`, чтобы этот файл следовал за файлом **/etc/ovirt-engine/osinfo.conf.d/00-defaults.properties**, и должно заканчиваться расширением **.properties**.

Например, файл **10-productkeys.properties** переопределит файл **00-defaults.properties**, заданный по умолчанию. Последний файл в списке имеет приоритет над более ранними файлами.

2. Настройка единого входа (Single Sign-On) для виртуальных машин

Настройка единого входа, (альтернативное название — делегированием пароля) , позволяет авторизоваться на виртуальной машине автоматически, используя учетные данные, введенные для авторизации на Пользовательском портале. Единый вход можно использовать как на виртуальных машинах Red Hat Enterprise Linux, так и на виртуальных машинах Windows.

Единый вход не поддерживается для виртуальных машин под управлением Red Hat Enterprise Linux 8.0.

Если включен единый вход на Пользовательский портал, то единый вход на виртуальные машины невозможен. Когда включен единый вход на Пользовательский портал — Пользовательскому порталу не требуется принимать пароль и поэтому невозможно делегировать пароль для входа на виртуальные машины.

2.1. Настройка единого входа для виртуальных машин Red Hat Enterprise Linux с использованием IPA

Чтобы настроить единый вход для виртуальных машин Red Hat Enterprise Linux с использованием графических сред рабочего стола GNOME и KDE и серверов IPA, установите пакет *ovirt-guest-agent* на виртуальную машину и пакеты, связанные с вашим оконным менеджером.

В следующей процедуре предполагается, что конфигурация IPA настроена и работает, домен IPA уже подключен к Менеджеру управления. Кроме того, с помощью NTP обеспечьте синхронизацию времени Менеджера управления, виртуальной машины и системы, осуществляющей хостинг IPA.

Единый вход больше не рекомендуется для виртуальных машин под управлением Red Hat Enterprise Linux 7.0 или более ранних версий Единый вход не поддерживается для виртуальных машин под управлением Red Hat Enterprise Linux 8 или более поздних версий, а также для ОС Windows.

Настройка единого входа для виртуальных машин Red Hat Enterprise Linux.

Порядок действий:

1. Авторизуйтесь на виртуальной машине с Red Hat Enterprise Linux.
2. Включите репозиторий:
    - Для Red Hat Enterprise Linux 6:

```
subscription-manager repos --enable=rhel-6-server-rhv-4-agent-rpms
```

    - Для Red Hat Enterprise Linux 7:

```
subscription-manager repos --enable=rhel-7-server-rh-common-rpms
```

3. Загрузите и установите пакеты гостевого агента, единого входа и IPA:

```
yum install ovirt-guest-agent-common ovirt-guest-agent-pam-module ovirt-guest-agent-gdm-plugin ipa-client
```

4. Выполните следующую команду и следуйте подсказкам, чтобы настроить `ipa-client` и подключить виртуальную машину к домену:

```
ipa-client-install --permit --mkhomedir
```

> В средах, где используется обфускация DNS, команда должна быть следующей:
>
> ```
> ipa-client-install --domain=FQDN --server=FQDN
> ```

5. Для Red Hat Enterprise Linux 7.2 и более поздних версий:

```
authconfig --enablenis --update
```

> В Red Hat Enterprise Linux 7.2 есть новая версия сервиса System Security Services Daemon (SSSD), которая вводит конфигурацию, несовместимую с реализацией единого входа на гостевом агенте Менеджера управления. Эта команда нужна, чтобы единый вход работал.

6. Получите подробную информацию о пользователе IPA:

```
getent passwd ipa-user
```

7. Запишите UID и GID пользователя IPA:

```
ipa-user:*:936600010:936600001::/home/ipa-user:/bin/sh
```

8. Создайте домашний каталог для пользователя IPA:

```
mkdir /home/ipa-user
```

9. Назначьте пользователя IPA владельцем каталога:

```
chown 936600010:936600001 /home/ipa-user
```

Авторизуйтесь на Пользовательском портале, используя имя и пароль пользователя, для которого настроен единый вход, и подключитесь к консоли виртуальной машины. Авторизация произойдет автоматически.

2.2. Настройка единого входа на виртуальных машинах Windows

Чтобы настроить единый вход на виртуальных машинах Windows, на гостевой виртуальной машине должен быть установлен гостевой агент Windows. Этот агент включен в ISO-образ **virtio-win**. Если в вашем домене хранения образ **virtio-win_version.iso** недоступен, свяжитесь с системным администратором.

Порядок действий:

1. Выберите виртуальную машину Windows. Убедитесь, что она включена.
2. Нажмите ⋮ > **[Сменить CD (Change CD)]**.
3. Из списка образов выберите **virtio-win_version.iso**.
4. Нажмите **[OK]**.
5. Нажмите **[Консоль (Console)]** и авторизуйтесь на виртуальной машине.
6. Чтобы получить доступ к содержимому ISO-файла гостевых инструментов, на виртуальной машине найдите CD-привод и запустите **virtio-win_version.iso**. После установки инструментов вам будет предложено перезагрузить машину, чтобы изменения вступили в силу.

Авторизуйтесь на Пользовательском портале, используя имя и пароль пользователя, для которого настроен единый вход, и подключитесь к консоли виртуальной машины. Авторизация произойдет автоматически.

2.3. Отключение единого входа для виртуальных машин

Следующая процедура описывает, как отключить единый вход для виртуальной машины.

Порядок действий:

1. Выберите виртуальную машину и нажмите **[Изменить (Edit)]**.
2. Откройте вкладку **Консоль (Console)**.
3. Установите флажок **Отключить единый вход (Disable Single Sign On)**.
4. Нажмите **[OK]**.

3. Настройка USB-устройств

Виртуальную машину, подключенную по протоколу SPICE, можно настроить на прямое подключение к USB-устройствам клиентской машины.

Чтобы включить автоматическое перенаправление USB-устройства с Пользовательского портала выполните следующие действий:

1. Откройте вкладку **Консоль (Console)** в окне **Новая виртуальная машина (New Virtual Machine)** или в окне **Изменить виртуальную машину (Edit Virtual Machine)**
2. Установите флажок **Включить USB (USB Enabled)**
3. Нажмите **[OK]**.
4. Перезагрузите виртуальную машину для применения этой настройки.
5. Виртуальная машина должна быть активна и находится в активном окне для автоматического перенаправление USB-устройства.

USB-перенаправление можно включать вручную при каждом подключении устройства.

Так же можно настроить автоматическое перенаправление в окне **Параметры консоли (Console Options)** Портала администрирования.

Обратите внимание на различие между клиентской машиной и гостевой машиной. Клиент — это оборудование, используемое для доступа к гостевой машине. Гостевая машина — это виртуальная рабочая станция или виртуальный сервер, доступ к которому осуществляется через Пользовательский портал или Портал администрирования.

Если режим USB-перенаправления **Включен (Enabled)**, то будет разрешено USB-перенаправление KVM/SPICE для виртуальных машин Linux и Windows. Виртуальные (гостевые) машины не требуют установленных гостевых агентов и драйверов для собственных USB-устройств. На клиентах Linux все пакеты, необходимые для USB-перенаправления, входят в пакет **virt-viewer**. На клиентах Windows нужно установить пакет **usbdk**.

В случае ПК с 64-разрядной архитектурой для установки 64-разрядной версии драйвера USB необходимо использовать 64-разрядную версию браузера. USB-перенаправление не будет работать, если 32-разрядная версия драйвера установлена на компьютер с 64-разрядной архитектурой. Если с самого начала установлен драйвер USB-перенаправления с правильной архитектурой, то USB может быть доступно как в 32-, так и в 64-разрядных браузерах.

3.1. Использование USB-устройств на клиенте Windows

Для перенаправления USB-устройства на гостевую машину, на клиентской машине Windows должен быть установлен драйвер `usbdk`. Убедитесь, что версия `usbdk` соответствует архитектуре клиентской машины. Например, на 64-разрядные машины Windows нужно устанавливать 64-разрядную версию `usbdk`.

Автоматическое USB-перенаправление поддерживается, только если виртуальная машина открыта с Пользовательского портала.

Порядок действий (начинается на Портале администрирования):

1. Когда драйвер `usbdk` установлен, нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.
2. Выберите виртуальную машину, настроенную на использование протокола SPICE, и нажмите **[Изменить (Edit)]**. Откроется окно **Изменить виртуальную машину (Edit Virtual Machine)**.
3. Откройте вкладку **Консоль (Console)**.
4. Установите флажок **Включить USB (USB enabled)** и нажмите **[OK]**.
5. Нажмите **Консоль (Console) > Параметры консоли (Console Options)**.
6. Установите флажок **Включить USB Auto-Share (Enable USB Auto-Share)** и нажмите **[OK]**.
7. Запустите виртуальную машину с **Пользовательского портала** и нажмите **[Консоль (Console)]**, чтобы подключиться к этой виртуальной машине.
8. Подключите USB-устройство к клиентской машине, чтобы оно автоматически отобразилось на гостевой машине.

3.2. Использование USB-устройств на клиенте Linux

Пакет `usbredir` включает USB-перенаправление с клиентской машины Linux на виртуальные машины. `usbredir` обычно зависит от пакета *virt-viewer* и автоматически устанавливается вместе с ним (уточните в документации производителя вашего дистрибутива).

USB-перенаправление поддерживается только если виртуальная машина открыта с Пользовательского портала.

Порядок действий (начинается на Портале администрирования):

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.
2. Выберите виртуальную машину, настроенную на использование протокола SPICE, и нажмите **[Изменить (Edit)]**. Откроется окно **Изменить виртуальную машину (Edit Virtual Machine)**.
3. Откройте вкладку **Консоль (Console)**.
4. Установите флажок **Включить USB (USB enabled)** и нажмите **[OK]**.
5. Нажмите **Консоль (Console) > Параметры консоли (Console Options)**.
6. Установите флажок **Включить USB Auto-Share (Enable USB Auto-Share)** и нажмите **[OK]**.
7. Запустите виртуальную машину с Пользовательского портала и нажмите **[Консоль (Console)]**, чтобы подключиться к этой виртуальной машине.

8. Подключите USB-устройство к клиентской машине, чтобы оно автоматически отобразилось на гостевой машине.

4. Настройка нескольких мониторов

Для одной виртуальной машины, подключённой по протоколу SPICE, поддерживается не более четырёх подключенных дисплеев.

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Если виртуальная машина выключена, нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Консоль (Console)**.
4. Выберите количество дисплеев в выпадающем списке **Мониторы (Monitors)**.

> Эта настройка управляет максимальным количеством дисплеев, которые можно подключить к виртуальной машины. Во время работы машины можете добавлять дисплеи, пока не будет достигнут установленный максимум.

5. Нажмите **[OK]**.
6. Начните сеанс SPICE с виртуальной машиной.
7. Откройте выпадающее меню **Представление (View)** в верхней части окна клиента SPICE.
8. Откройте меню **Дисплей (Display)**.
9. Нажмите на имя дисплея, чтобы включить или выключить его.

> По умолчанию Дисплей 1 (Display 1) — это дисплей, включенный в начале сеанса SPICE с виртуальной машиной. Если никакие другие дисплеи дисплеи не подключены/включены, то отключение этого дисплея завершит сеанс SPICE с виртуальной машиной.

5. Настройка параметров консоли

5.1. Параметры консоли

Протоколы подключения — это базовая технология предоставления графических консолей виртуальным машинам, которая позволяет пользователям работать с виртуальными машинами так же, как с физическими машинами. Сейчас в zVirt поддерживаются следующие протоколы подключения:

SPICE

Simple Protocol for Independent Computing Environments (SPICE) рекомендуется как для виртуальных машин Linux, так и Windows. Чтобы открыть консоль виртуальной машины с помощью SPICE, используйте инструмент удаленного просмотра - **Remote Viewer**.

VNC

Virtual Network Computing (VNC) можно использовать для открытия консолей как виртуальных машин Linux, так и Windows. Чтобы открыть консоль виртуальной машины с помощью VNC, используйте инструмент удаленного просмотра **Remote Viewer** или VNC-клиент.

RDP

Remote Desktop Protocol (RDP) можно использовать только для открытия консолей виртуальных машин Windows и только при доступе к виртуальным машинам с клиентской машины Windows с установленным инструментом удаленного просмотра (Remote Desktop). Прежде чем подключиться к виртуальной машине Windows по RDP, настройте на виртуальной машине удаленный общий доступ и разрешите в брандмауэре подключения к удаленному рабочему столу.

5.2. Доступ к параметрам консоли

На Портале администрирования можно настроить несколько вариантов открытия графических консолей виртуальных машин.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите работающую виртуальную машину.
2. Нажмите **Консоль (Console) > Параметры консоли (Console Options)**.

Протоколы подключения и тип видео можно настроить в окне **Изменить виртуальную машину (Edit Virtual Machine)** на вкладке **Консоль (Console)** на Портале администрирования. Для каждого из протоколов подключения можно настроить дополнительные параметры. Например, при использовании протокола подключения VNC можно настроить раскладку клавиатуры. Для получения дополнительной информации см. раздел Описание настроек консоли виртуальной машины.

5.3. Параметры консоли SPICE

Когда выбран протокол подключения SPICE, в окне **Параметры консоли (Console Options)** доступны следующие параметры.

Опции SPICE

- **Изменить комбинацию клавиш Ctrl+Alt+Del на Ctrl+Alt+End (Map ctrl+alt+del short-cut to ctrl+alt+end)**: установите этот флажок, чтобы преобразовать комбинацию `Ctrl`+`Alt`+`Del` в `Ctrl`+`Alt`+`End` внутри виртуальной машины.
- **Включить USB Auto-Share (Enable USB Auto-Share)**: установите этот флажок для автоматического перенаправления USB-устройств на виртуальную машину. Если этот флажок не установлен, USB-устройства будут подключаться к клиентской машине, а не к гостевой виртуальной машине. Чтобы использовать USB-устройство на гостевой машине, когда флажок не установлен, включите устройство вручную в меню клиента SPICE.
- **Открыть в полноэкранном режиме (Open in Full Screen)**: установите этот флажок, чтобы консоль виртуальной машины автоматически открывалась в полноэкранном режиме при подключении к виртуальной машине. Для включения/выключения полноэкранного режима нажмите `Shift`+`F11`.
- **Включить SPICE-прокси (Enable SPICE Proxy)**: установите этот флажок, чтобы включить SPICE-прокси.

5.4. Параметры консоли VNC

Когда выбран протокол подключения VNC, в окне **Параметры консоли (Console Options)** доступны следующие параметры.

Вызов консоли (Console Invocation)

- **Нативный клиент (Native Client)**: при подключении к консоли виртуальной машины, диалоговое окно загрузки предоставляет файл, который открывает консоль виртуальной машины с помощью инструмента удаленного просмотра `Remote Viewer`.
- **noVNC**: при подключении к консоли виртуальной машины, открывается вкладка браузера, выполняющая роль консоли.

Опции VNC

- **Изменить комбинацию клавиш Ctrl+Alt+Del на Ctrl+Alt+End (Map ctrl+alt+del short-cut to ctrl+alt+end)**: Установите этот флажок, чтобы преобразовать комбинацию `Ctrl`+`Alt`+`Del` в `Ctrl`+`Alt`+`End` внутри виртуальной машины.

5.5. Параметры консоли RDP

Когда выбран **Удалённый рабочий стол (Remote Desktop)** в окне **Параметры консоли (Console Options)**, доступны следующие параметры.

Вызов консоли (Console Invocation)

- **Автоматически (Auto)**: менеджер управления автоматически выбирает метод вызова консоли.
- **Нативный клиент (Native client)**: при подключении к консоли виртуальной машины, диалоговое окно загрузки предоставляет файл, который открывает консоль виртуальной машины с помощью инструмента удаленного просмотра `Remote Viewer`.

Опции RDP

- **Использовать локальные диски (Use Local Drives)**: установите этот флажок, чтобы гостевая виртуальная машина смогла обращаться к дискам на клиентской машине.

5.6. Параметры инструмента удаленного просмотра (Remote Viewer)

5.6.1. Параметры инструмента удаленного просмотра Remote Viewer

Если указан параметр вызова консоли **Нативный клиент (Native client)**, то для подключения к виртуальной машине используется инструмент удаленного просмотра **Remote Viewer**. Окно **Remote Viewer** предлагает ряд параметров для взаимодействия с виртуальной машиной, к которой подключен этот инструмент.

Таблица 1. Параметры инструмента удаленного просмотра Remote Viewer

Параметр	Описание
Файл (File)	• **Снимок экрана (Screenshot)**: делает экранный снимок активного окна и сохраняет его в указанном месте. • **Выбор USB-устройства (USB device selection)**: если на виртуальной машине включено USB-перенаправление, то доступ к USB-устройству, подключенному к клиентской машине, можно получить из этого меню. • **Выход (Quit)**: закрывает консоль. Клавишная комбинация для этого параметра: `Shift` + `Ctrl` + `Q`.

Параметр	Описание
Представление (View)	• **Полный экран (Full screen)**: включает и выключает полноэкранный режим. При включении полноэкранного режима виртуальная машина разворачивается на весь экран. При его выключении виртуальная машина отображается в виде окна. Клавишная комбинация для включения/выключения полноэкранного режима: `SHIFT`+`F11`. • **Изменение масштаба (Zoom)**: изменение масштаба окна консоли. `Ctrl`+`+` увеличивает масштаб, `Ctrl`+`-` уменьшает, а `Ctrl`+`0` возвращает экран к изначальному размеру. • **Изменять размер автоматически (Automatically resize)**: выберите этот параметр, чтобы разрешение гостевой системы автоматически подстраивалось под размер окна консоли. • **Дисплеи (Displays)**: позволяет пользователям включать и выключать дисплеи для гостевой виртуальной машины.
Отправить клавишную комбинацию (Send key)	• **Ctrl + Alt + Del**: на виртуальной машине Red Hat Enterprise Linux она отображает диалоговое окно с параметрами приостановки, выключения или перезапуска виртуальной машины. На виртуальной машине Windows она отображает диспетчер задач или диалоговое окно Безопасность Windows (Windows Security). • **Ctrl + Alt + Backspace**: на виртуальной машине Red Hat Enterprise Linux она перезапускает X-сервер. На виртуальной машине Windows она не делает ничего. • **Ctrl + Alt + F1** • **Ctrl + Alt + F2** • **Ctrl + Alt + F3** • **Ctrl + Alt + F4** • **Ctrl + Alt + F5** • **Ctrl + Alt + F6** • **Ctrl + Alt + F7** • **Ctrl + Alt + F8** • **Ctrl + Alt + F9** • **Ctrl + Alt + F10** • **Ctrl + Alt + F11** • **Ctrl + Alt + F12** • **Printscreen**: передает нажатие **Printscreen** на клавиатуре Клиента виртуальной машине.
Справка (Help)	Пункт **О программе (About)** отображает сведения об используемой версии инструмента просмотра виртуальных машин `Virtual Machine Viewer`.

Параметр	Описание
Высвободить курсор из виртуальной машины (Release Cursor from Virtual Machine)	`SHIFT` + `F12`

5.6.2. Клавишные комбинации инструмента удаленного просмотра Remote Viewer

Клавишные комбинации для виртуальной машины доступны как в полноэкранном, так и в оконном режиме. Чтобы в полноэкранном режиме отобразить меню, в котором есть кнопка для клавишных комбинаций, переместите указатель мыши в середину верхней части экрана. В оконном режиме клавишные комбинации доступны через меню **Отправить клавишную комбинацию (Send key)** в строке заголовка окна виртуальной машины.

Если мышь используется внутри виртуальной машины и виртуальная машина не находится в полноэкранном режиме, то мышь может быть заблокирована окном виртуальной машины, так как Vdagent не запущен на клиентском компьютере. Чтобы разблокировать мышь, нажмите `Shift` + `F12`.

6. Настройка сервиса watchdog

6.1. Добавление карты сервиса watchdog в виртуальную машину

В виртуальную машину можно добавить карту сервиса watchdog, чтобы отслеживать работоспособность операционной системы.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Высокая доступность (High Availability)**.
4. Выберите используемую модель сервиса watchdog в выпадающем списке **Модель (Watchdog Model)**.
5. Выберите действие в выпадающем списке **Действие (Watchdog Action)**. Это действие, которое выполняет виртуальная машина при срабатывании сервиса **watchdog**.
6. Нажмите **[OK]**.

6.2. Установка сервиса watchdog

Установите пакет *watchdog* на виртуальную машину и запустите службу **watchdog**, чтобы активировать карту сервиса **watchdog**.

Порядок действий:

1. Авторизуйтесь на виртуальной машине, к которой подключена карта сервиса **watchdog**.
2. Установите пакет *watchdog* и зависимости:

```
dnf install watchdog
```

3. Измените файл `/etc/watchdog.conf` и раскомментируйте следующую строку:

```
watchdog-device = /dev/watchdog
```

4. Сохраните изменения.
5. Запустите службу **watchdog** и убедитесь, что она запускается при загрузке:
   - Red Hat Enterprise Linux 6:

```
service watchdog start
chkconfig watchdog on
```

   - Red Hat Enterprise Linux 7:

```
systemctl start watchdog.service
systemctl enable watchdog.service
```

6.3. Подтверждение функциональности сервиса watchdog

Убедитесь, что карта сервиса **watchdog** подключена к виртуальной машине и служба **watchdog** активна.

Эта процедура предназначена только для проверки функциональности сервисов **watchdog** и не должна выполняться на продуктивных машинах.

Порядок действий:

1. Авторизуйтесь на виртуальной машине, к которой подключена карта сервиса **watchdog**.
2. Убедитесь, что карта сервиса **watchdog** опознана виртуальной машиной:

```
lspci | grep watchdog -i
```

3. Выполните одну из следующих команд, чтобы убедиться в активности сервиса **watchdog**:
    - Инициируйте "панику" ядра:

      ```
      echo c > /proc/sysrq-trigger
      ```

    - Остановите службу **watchdog**:

      ```
      kill -9 pgrep watchdog
      ```

Таймер сервиса **watchdog** больше невозможно сбросить, поэтому счетчик сервиса **watchdog** вскоре досчитает до нуля. Когда это произойдет, будет выполнено действие, выбранное в выпадающем меню **Действие (Watchdog Action)** для данной виртуальной машины.

6.4. Параметры сервиса watchdog в файле watchdog.conf

Ниже приводится список параметров для настройки службы **watchdog**, включенных в файл **/etc/watchdog.conf**. Чтобы настроить параметр, раскомментируйте его, сохраните изменения и перезапустите службу **watchdog**.

> Более подробно о параметрах настройки службы **watchdog** и использовании команды `watchdog` смотрите в справочной системе `man watchdog`.

Таблица 2. Переменные в файле watchdog.conf

Имя переменной	Значение по умолчанию	Примечания
`ping`	—	IP-адрес, на который сервис **watchdog** пытается отправить icmp-запрос, чтобы проверить доступность этого адреса. Можно указать несколько IP-адресов, добавив строки `ping`.
`interface`	—	Сетевой интерфейс, за которым будет следить сервис **watchdog** и на котором он будет проверять наличие сетевого трафика. Можно указать несколько сетевых интерфейсов, добавив строки `interface`.
`file`	/var/log/messages	Файл в локальной системе, изменения в котором будет отслеживать сервис **watchdog**. Можно указать несколько файлов, добавив строки `file`.
`change`	1407	Количество интервалов сервиса **watchdog**, после которого он проверяет наличие изменений в файлах. Строка `change` должна указываться сразу после каждой строки `file` и применяется к строке `file`, находящейся непосредственно над ней.

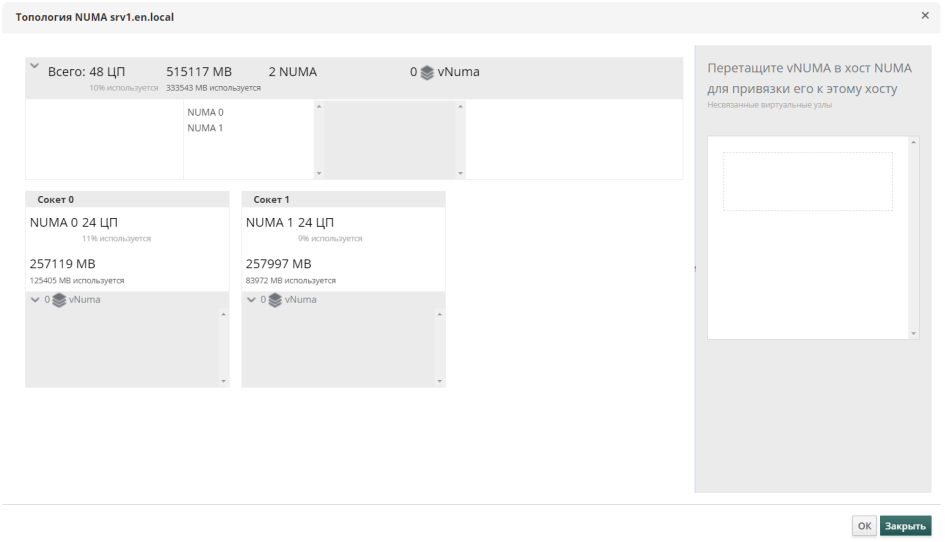
Имя переменной	Значение по умолчанию	Примечания
`max-load-1`	24	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение 1 минуты. При превышении этого среднего значения срабатывает сервис **watchdog**. Значение `0` выключает эту функцию.
`max-load-5`	18	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение 5 минут. При превышении этого среднего значения срабатывает сервис **watchdog**. Значение `0` выключает эту функцию. По умолчанию значение этой переменной равно примерно 3/4 значения `max-load-1`.
`max-load-15`	12	Максимальная средняя нагрузка, которую виртуальная машина может выдержать в течение 15 минут. При превышении этого среднего значения срабатывает сервис **watchdog**. Значение `0` выключает эту функцию. По умолчанию значение этой переменной равно примерно 1/2 значения `max-load-1`.
`min-memory`	1	Минимальный объем виртуальной памяти, который должен оставаться свободным на виртуальной машине. Измеряется в страницах. Значение `0` выключает эту функцию.
`repair-binary`	/usr/sbin/repair	Путь и имя двоичного файла в локальной системе, который будет запускаться при срабатывании сервиса **watchdog**. Если указанный файл устраняет проблемы, не давая **watchdog** сбросить счетчик, то действие сервиса **watchdog** не активируется.
`test-binary`	—	Путь и имя двоичного файла в локальной системе, который сервис **watchdog** будет пытаться запустить в течение каждого интервала. Этот параметр позволяет указать файл для запуска пользовательских тестов.
`test-timeout`	—	Лимит времени (в секундах), в течение которого могут выполняться пользовательские тесты. Значение `0` позволяет выполнять пользовательские тесты без ограничений по времени.
`temperature-device`	—	Путь и имя устройства для проверки температуры машины, на которой запущена служба **watchdog**.
`max-temperature`	120	Максимальная допустимая температура машины, на которой запущена службы **watchdog**. При достижении этой температуры машина будет остановлена. Преобразование единиц измерения не учитывается, поэтому указывайте значение, соответствующее используемой карте сервиса **watchdog**.
`admin`	root	Адрес эл. почты, на который отправляются уведомления.

Имя переменной	Значение по умолчанию	Примечания
`interval`	10	Интервал (в секундах) между обновлениями на устройстве сервиса **watchdog**. Устройство сервиса **watchdog** ожидает, что обновления будут поступать как минимум каждую минуту, и если в течение минуты обновлений нет, то срабатывает сервис **watchdog**. Этот одноминутный интервал жестко задан в драйверах сервиса **watchdog** и не настраивается.
`logtick`	1	Когда для службы **watchdog** включен режим детального журналирования, служба **watchdog** периодически записывает сообщения журнала в локальную систему. Значение `logtick` обозначает количество интервалов сервиса **watchdog**, после которого записывается сообщение.
`realtime`	yes	Указывает, заблокирован ли сервис **watchdog** в памяти. Значение `yes` блокирует сервис **watchdog** в памяти, предотвращая его выгрузку из памяти, а `no` разрешает такую выгрузку. Если сервис **watchdog** выгружается из памяти и не возвращается обратно до обнуления счетчика, то срабатывает сервис **watchdog**.
`priority`	1	Приоритет в графике задач, когда параметр `realtime` установлен в значение `yes`.
`pidfile`	/var/run/sys-logd.pid	Путь и имя PID-файла, за которым следит сервис **watchdog**, чтобы определить, по-прежнему ли активен соответствующий процесс. Если соответствующий процесс **не** активен, то срабатывает сервис **watch-dog**.

7. Настройка виртуальных узлов NUMA

На Портале администрирования можно настроить виртуальные узлы NUMA на виртуальной машине и закрепить их за физическими узлами NUMA на одном или нескольких хостах. Согласно политике хоста по умолчанию, виртуальные машины планируются и запускаются на любых доступных ресурсах хоста. В результате ресурсы, обеспечивающие работу большой виртуальной машины, которая не может поместиться в один сокет хоста, могут быть распределены по нескольким узлам NUMA. Со временем эти ресурсы могут перемещаться, ухудшая производительность и делая ее непредсказуемой. Чтобы избежать этого и повысить производительность, настройте и закрепите виртуальные узлы NUMA.

Для настройки виртуальных узлов NUMA нужен хост с включенным NUMA. Чтобы убедиться, что NUMA на хосте включен, авторизуйтесь на хосте и запустите `numactl --hardware`. В выводе этой команды должны присутствовать минимум два узла NUMA. Можно также просмотреть топологию NUMA хоста на Портале администрирования, выбрав хост на вкладке **Хосты (Hosts)** (**Ресурсы (Compute) > Хосты (Hosts)**) перейдя в его детальное описание, нажав ⋮, и кликнуть по **Поддержка NUMA (NUMA Support)**.



Эта кнопка доступна, только если выбранный хост имеет минимум два узла NUMA.

Если задано Закрепление NUMA (NUMA Pinning), то режимом миграции по умолчанию будет **Разрешить только ручную миграцию (Allow manual migration only)**.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Нажмите **[Показать расширенные настройки (Show Advanced Options)]**.
4. Откройте вкладку **Хост (Host)**.
5. Под **Запустить на: (Start Running On:)** нажмите кнопку-переключатель **Указанном хосте (Specific Host(s))** и выберите хосты из списка. Выбранные хосты должны иметь минимум два узла NUMA.
6. Нажмите **[Привязка NUMA (NUMA Pinning)]**.
7. В окне **Топология NUMA (NUMA Topology)** выберите и перетащите необходимые виртуальные узлы NUMA из блока справа в блок узлов NUMA хоста слева, затем нажмите **[OK]**.
8. На каждом узле NUMA в выпадающем списке **Режим тонкой настройки (Tune Mode)** выберите один из режимов: **Строгий (Strict)**, **Предпочитаемый (Preferred)** или **Интерактивный (Interleave)**. Если выбран **Предпочитаемый (Preferred)** режим, то **Количество хостов NUMA (NUMA Node Count)** должно быть установлено в значение `1`.
9. Можно также задать политику закрепления NUMA автоматически, выбрав в выпадающем списке **Рекомендации по автоматическому закреплению (Auto Pinning Policy)**:
    - **Отсутствует (None)** — не вносит никаких изменений в виртуальную машину.

- **Изменить размер и прикрепить (Resize and Pin)** — устанавливает максимальную топологию ЦП и генерирует конфигурации закрепления ЦП и NUMA.

10. Нажмите **[OK]**.

Если не закрепить виртуальный узел NUMA на узле NUMA хоста, то система по умолчанию использует узел NUMA, который содержит ввод-вывод с отображением памяти (MMIO) устройства хоста, при условии, что имеется одно или несколько устройств хоста и все эти устройства из одного узла NUMA.

8. Настройка фоновых виртуальных машин (Headless Virtual Machines)

Можно настроить фоновую виртуальную машину, когда нет необходимости обращаться к машине через графическую консоль. Такая фоновая машина будет работать без видео- и графических устройств. Это может быть полезно в ситуациях, когда ресурсы хоста ограничены или нужно соблюсти требования к использованию виртуальных машин (например, виртуальных машин реального времени).

Управлять фоновыми виртуальными машинами можно через последовательную консоль, SSH или любую другую службу доступа из командной строки. Применить фоновый режим можно при открытии вкладки **Консоль(Console)** во время создания или изменения виртуальных машин и пулов машин, а также во время изменения шаблонов. Эта возможность также доступна при создании или изменении типов экземпляров.

При создании новой фоновой виртуальной машины можно использовать окно **[Однократный запуск (Run Once)]**, чтобы обратиться к виртуальной машине через графическую консоль, но только для однократного запуска. Для получения дополнительной информации см. раздел Описание настроек в окне "Запустить ВМ (Run Virtual Machine(s))".

Предварительные условия:

- При изменении существующей виртуальной машины и отсутствии установленного гостевого агента zVirt запишите IP-адрес машины, прежде чем выбирать **Режим Headless (Headless Mode)**.
- Перед запуском виртуальной машины в фоновом режиме конфигурацию GRUB для этой машины нужно установить в консольный режим, иначе процесс загрузки гостевой операционной системы зависнет. Чтобы установить консольный режим, закомментируйте флаг splashimage в файле конфигурации меню GRUB:

```
#splashimage=(hd0,0)/grub/splash.xpm.gz serial --unit=0 --speed=9600 --
parity=no --stop=1 terminal --timeout=2 serial
```

После выбора **Режим Headless (Headless Mode)** перезапустите виртуальную машину, если она уже работает.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Консоль (Console)**.
4. Выберите **Режим Headless (Headless Mode)**. Все остальные поля в разделе **Графический адаптер (Graphical Console)** станут неактивны.
5. При желании выберите **Консольный порт VirtIO-serial (Enable VirtIO serial console)**, чтобы включить взаимодействие с виртуальной машиной через последовательную консоль. Рекомендуем это сделать.
6. Если виртуальная машина работает, перезагрузите ее. См. раздел Перезагрузка или сброс виртуальной машины.

9. Настройка высокопроизводительных виртуальных машин, шаблонов и пулов

Виртуальную машину можно настроить на обеспечение высокой производительности, чтобы ее показатели производительности были максимально близки к показателям физической машины. При выборе оптимизации для высокой производительности виртуальная машина конфигурируется с набором автоматических и рекомендуемых ручных настроек, обеспечивающих максимальную эффективность.

Параметр **Высокая производительность** доступен только на Портале администрирования: выберите **Высокая производительность (High Performance)** в выпадающем списке **Профиль нагрузки (Optimized for)** в закладке **"Высокая доступность"** окне **Изменить виртуальную машину (Edit)** или **Создать (New) виртуальную машину**, шаблон или пул. Эта опция недоступна на Пользовательском портале.

Виртуальные машины

Если изменить режим оптимизации работающей виртуальной машины на **Высокая производительность**, то некоторые изменения конфигурации потребуют перезапуска виртуальной машины. Чтобы изменить режим оптимизации новой или существующей виртуальной машины на **Высокая производительность**, может потребоваться сначала вручную внести изменения в кластер и конфигурацию закрепленного хоста.

Высокопроизводительная виртуальная машина имеет определенные ограничения, поскольку повышение производительности приводит к уменьшению гибкости:

- Если для потоков ЦП, потоков ввода/вывода, потоков эмулятора или узлов NUMA установлено закрепление в соответствии с рекомендуемыми настройками, то высокопроизводительной виртуальной машине может быть назначено только подмножество хостов кластера.
- Многие устройства выключаются автоматически, из-за чего использовать виртуальную машину может быть не так удобно.

Шаблоны и пулы

Высокопроизводительные шаблоны и пулы создаются и изменяются так же, как и виртуальные машины. Если для создания новых виртуальных машин используется высокопроизводительный шаблон или пул, то эти виртуальные машины наследуют это свойство и его конфигурации. Однако некоторые настройки не наследуются и должны быть установлены вручную:

- Закрепление ЦП (CPU pinning).
- Виртуальный узел NUMA и топология закрепления NUMA.
- Топология закрепления потоков ввода/вывода и эмулятора.
- Сквозной доступ ЦП хоста (Pass-through Host CPU).

9.1. Создание высокопроизводительной виртуальной машины, шаблона или пула

Чтобы создать высокопроизводительную виртуальную машину, шаблон или пул выполните следующие действия.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите **[Создать (New)]**. Откроется окно **Новая виртуальная машина (New Virtual Machine)**.
3. На вкладке **Общее (General)** выберите **Высокая производительность (High Performance)** в выпадающем меню **Профиль нагрузки (Optimized for)**.

   При выборе этого параметра автоматически выполняются определенные изменения конфигурации этой виртуальной машины, которые можно просмотреть, открывая разные вкладки. Их можно как вернуть в изначальные значения, так и переопределить (подробности см. в разделе Автоматические настройки высокопроизводительной конфигурации). Последнее значение настройки сохраняется после изменении.
4. Нажмите **[OK]**.

   Если ручные настройки не заданы, отобразится экран **Высокопроизводительные параметры виртуальной машины/пула (High Performance Virtual Machine/Pool**

Settings), описывающий рекомендуемые ручные настройки.

Если некоторые ручные настройки заданы, на экране **Высокопроизводительные параметры виртуальной машины/пула (High Performance Virtual Machine/Pool Settings)** отобразятся неустановленные настройки.

Если все ручные настройки заданы, экран **Высокопроизводительные параметры виртуальной машины/пула (High Performance Virtual Machine/Pool Settings)** не появится.

5. Если появляется экран **Высокопроизводительные параметры виртуальной машины/пула (High Performance Virtual Machine/Pool Settings)**, нажмите **[Отменить (Cancel)]**, чтобы вернуться в окно **[Создать (New)]** или **[Изменить (Edit)]** и выполнить ручную настройку. Подробности см. в разделе Конфигурирование рекомендуемых ручных настроек. Либо нажмите **[OK]**, чтобы проигнорировать рекомендации. В результате может снизиться производительность.
6. Нажмите **[OK]**.

   Тип оптимизации можно просмотреть на вкладке **Общие (General)** подробного представления виртуальной машины, пула или шаблона.

Определенные конфигурации могут переопределять настройки высокой производительности. Например, если выбрать тип экземпляра для виртуальной машины до выбора **Высокой производительности (High Performance)** в выпадающем меню **Профиль нагрузки (Optimized for)** и до выполнения ручной настройки, то настройка типа экземпляра не повлияет на высокопроизводительную конфигурацию. Однако это не относится к случаям, когда тип экземпляра выбирается после выбора высокопроизводительной конфигурации, проверьте окончательную конфигурацию на разных вкладках, чтобы убедиться, что высокопроизводительные конфигурации не переопределены типом экземпляра.

Приоритет обычно имеет конфигурация, сохраненная последней.

Поддержка типов экземпляров признана устаревшей и будет удалена в одном из будущих выпусков.

9.1.1. Автоматические настройки высокопроизводительной конфигурации

Автоматические настройки сведены в следующую таблицу. В столбце **Включено (Д/Н) (Enabled (Y/N))** отображаются включенные или выключенные конфигурации. В столбце **Применяется к (Applies to)** отображаются соответствующие ресурсы:

- ВМ — виртуальная машина;
- Ш — шаблон;
- П — пул;

- К — кластер.

Таблица 3. Автоматические настройки высокопроизводительной конфигурации

Параметр	**Включено (Д/Н) (Enabled (Y/N))**	**Применяется к (Applies to)**
Фоновый режим (Headless Mode) (вкладка **Консоль (Console)**)	Д	ВМ, Ш, П
Включить USB (USB Enabled) (вкладка **Консоль (Console)**)	Н	ВМ, Ш, П
Поддержка смарт-карт (Smartcard Enabled) (вкладка **Консоль (Console)**)	Н	ВМ, Ш, П
Включить звуковую карту (Soundcard Enabled) (вкладка **Консоль (Console)**)	Н	ВМ, Ш, П
Консольный порт VirtIO-serial (Enable VirtIO serial console) (вкладка **Консоль (Console)**)	Д	ВМ, Ш, П
Разрешить только ручную миграцию (Allow manual migration only) (вкладка **Хост (Host)**)	Д	ВМ, Ш, П
Сквозной доступ ЦП хоста (Pass-Through Host CPU) (вкладка **Хост (Host)**)	Д	ВМ, Ш, П
Высокая доступность (Highly Available) (вкладка **Высокая доступность (High Availability)**) Высокая доступность не включается автоматически, если выбрать её вручную, то высокая доступность должна быть включена только для закрепленных хостов.	Н	ВМ, Ш, П
Без использования watchdog (No-Watchdog) (вкладка **Высокая доступность (High Availability)**)	Н	ВМ, Ш, П
Включить Balloning (Memory Balloon Device) (вкладка **Выделение ресурсов (Resource Allocation)**)	Н	ВМ, Ш, П
Потоки ввода/вывода (I/O Threads Enabled) (вкладка **Выделение ресурсов (Resource Allocation)**, Количество потоков ввода/вывода = `1`)	Д	ВМ, Ш, П
Устройство Паравиртуализированный генератор случайных чисел PCI (Paravirtualized Random Number Generator PCI) (virtio-rng) (вкладка **Генератор случайных чисел (Random Generator)**)	Д	ВМ, Ш, П
Топология закрепления потоков ввода/вывода и эмулятора	Д	ВМ, Ш
Кэш ЦП третьего уровня	Д	ВМ, Ш, П

9.1.2. Закрепление привязки ввода/вывода и эмуляции потоков (автоматические настройки)

Для закрепления ввода/вывода и эмуляции потоков конфигурации нужно, чтобы потоки ввода-вывода, узлы NUMA и закрепление NUMA были включены и настроены на виртуальной машине, в противном случае в журнале engine отобразится предупреждение.

Автоматическая топология привязки

- Закрепляются первые два ЦП каждого узла NUMA.
- Если все ЦП находятся на одном узле NUMA хоста:
  - Первые два виртуальных ЦП автоматически резервируются/закрепляются.
  - Остальные виртуальные ЦП доступны для ручного закрепления виртуальных ЦП.
- Если виртуальная машина занимает более одного узла NUMA:
  - Первые два ЦП узла NUMA с наибольшим количеством закреплений зарезервированы/закреплены.
  - Остальные закрепленные узлы NUMA предназначены только для закрепления виртуальных ЦП.

Пулы не поддерживают закрепление потоков ввода/вывода и эмулятора.

Если ЦП хоста закреплен как за виртуальным ЦП, так и за потоками ввода-вывода и эмулятора, то в журнале появится предупреждение, и система предложит рассмотреть возможность изменения топологии закрепления ЦП, чтобы избежать этой ситуации.

9.1.3. Значки "Высокая производительность"

На экране **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** следующими значками обозначаются состояния высокопроизводительной виртуальной машины.

Таблица 4. Значки "Высокая производительность"

Значок	Описание
	Высокопроизводительная виртуальная машина
	Высокопроизводительная виртуальная машина с конфигурацией "Следующий запуск (Next Run)"
	Высокопроизводительная виртуальная машина без сохранения состояния
	Высокопроизводительная виртуальная машина без сохранения состояния с конфигурацией "Следующий запуск (Next Run)"
	Виртуальная машина в высокопроизводительном пуле

9.2. Конфигурирование рекомендуемых ручных настроек

Рекомендуемые ручные настройки можно задать в окнах **Новая виртуальная машина (New)** или **Изменить виртуальную машину (Edit)**.

Если рекомендуемая настройка не задана, то на экране **Высокопроизводительные параметры виртуальной машины/пула (High Performance Virtual Machine/Pool Settings)** при сохранении ресурса отображается рекомендуемая настройка.

К рекомендуемыми ручными настройкам относятся:

- Закрепление ЦП.
- Настройка политики закрепления NUMA.
- Конфигурирование больших страниц.
- Выключение KSM.

9.2.1. Ручные настройки высокопроизводительной конфигурации

В таблице ниже приведены все рекомендуемые ручные настройки. В столбце **Включено (да/нет)** показано, какие параметры должны быть включены, а какие — выключены. В столбце **Применяется к** отображаются соответствующие ресурсы:

- ВМ — виртуальная машина;
- Ш — шаблон;
- П — пул;
- К — кластер.

Таблица 5. Ручные настройки высокопроизводительной конфигурации

Параметр	Включено (да/нет)	Применяется к
Количество хостов NUMA (NUMA Node Count) (вкладка **Хост (Host)**)	Д	ВМ
Режим тонкой настройки (Tune Mode) (экран после нажатия **[Закрепление NUMA (NUMA Pinning)]**)	Д	ВМ
Закрепление NUMA (NUMA Pinning) (вкладка **Хост (Host)**)	Д	ВМ
Рекомендации по автоматическому закреплению (Auto Pinning Policy) (вкладка **Хост (Host)**)	Д	ВМ
Топология привязки ЦП (CPU Pinning topology) (вкладка Выделение ресурсов (Resource Allocation))	Д	ВМ, П

Параметр	Включено (да/нет)	Применяется к
Большие страницы (hugepages) (вкладка Пользовательские свойства (Custom Properties))	Д	ВМ, Ш, П
KSM (вкладка Оптимизация (Optimization tab))	Н	К

9.2.2. Закрепление ЦП

Чтобы закрепить виртуальные ЦП за физическим ЦП конкретного хоста:

1. На вкладке **Хост (Host)** в блоке **Запустить на: (Start Running On:)** нажмите кнопку-переключатель **Указанном хосте (Specific Host(s))**.
2. На вкладке **Выделение ресурсов (Resource Allocation)** в меню **Политика Закрепления ЦПУ** выберите подходящую политику.
    - При использовании политики закрепления **Manual** также введите конфигурацию в поле **Топология привязки ЦП (CPU Pinning Topology)** и подтвердите, что такая конфигурация соответствует конфигурации закрепленного хоста.

    > Если в поле **Топология привязки ЦП (CPU Pinning Topology)** задана конфигурация, то режим миграции ВМ (вкладка **Хост**) автоматически меняется на **Разрешить только ручную миграцию**.
    >
    > Это поле заполняется автоматически, а топология ЦП обновляется, когда активируется автоматическое закрепление NUMA.
    >
    > Подробные сведения о синтаксисе этого поля см. в разделе Описание настроек выделения ресурсов виртуальных машин.window=_blank.
3. Проверьте, что конфигурация виртуальной машины совместима с конфигурацией хоста:
    - Количество сокетов виртуальной машины не должно превышать количество сокетов хоста.
    - Количество ядер виртуальной машины на один виртуальный сокет не должно превышать количество ядер хоста.
    - Процессы, сильно загружающие ЦП, лучше всего выполняются, когда на хосте и виртуальной машине ожидается одинаковая загрузка кэша. Чтобы производительность была максимальной, количество потоков на ядро у виртуальной машины не должно превышать количество потоков у хоста.

К закреплению ЦП предъявляются следующие требования:

- Если на хосте включен NUMA, то необходимо учитывать настройки NUMA хоста (память и ЦП), поскольку виртуальная машина должна соответствовать конфигурации NUMA хоста.
- Необходимо учитывать Топологию закрепления потоков ввода-вывода.
- Закрепление ЦП можно настроить только для виртуальных машин и пулов, но не для шаблонов. Поэтому закрепление ЦП необходимо настроить вручную при создании высокопроизводительной виртуальной машины или пула, даже если они основаны на высокопроизводительном шаблоне.

9.2.3. Настройка политики закрепления NUMA

Чтобы настроить политику закрепления NUMA, нужен закрепленный хост с включенным NUMA и как минимум двумя узлами NUMA. Можно настроить топологию NUMA вручную или воспользоваться **Рекомендации по автоматическому закреплению (Auto Pinning Policy)** для автоматической настройки топологии вкладки **Хост (Host)** окна **Создать (New)/ Изменить (Edit)**.

Ручная настройка политики закрепления NUMA

1. Нажмите **[Привязка NUMA (NUMA Pinning)]**.
2. В окне **Топология NUMA (NUMA Topology)** выберите и перетащите необходимые виртуальные узлы из NUMA из блока справа в блок физических узлов NUMA хоста слева.
3. Выберите режим **Строгий (Strict)**, **Предпочтительный (Preferred)** или **С чередованием (Interleave)** из выпадающего списка **Режим тонкой настройки (Tune Mode) для каждого узла NUMA**. Если выбран режим **Предпочтительный (Preferred)**, то Количество узлов NUMA (NUMA Node Count) должно быть установлено в значение `1`.
4. Нажмите **[OK]**.

Автоматическая настройка политики закрепления NUMA

1. На вкладке **Хост (Host)** и блоке **Запустить на: (Start Running On:)** нажмите кнопку-переключатель **Указанном хосте (Specific Host(s))** и выберите хост(ы) из списка. У заданного(ых) хоста(ов) должно быть не менее двух узлов NUMA.
2. В блоке **Настройки NUMA (Configure NUMA)** выберите **Рекомендации по автоматическому закреплению (Auto Pinning Policy)** из выпадающего списка:
   - **Не назначено (None)** - не вносит никаких изменений в виртуальную машину.
   - **Изменить размер и прикрепить (Resize and Pin)** — устанавливает максимальную топологию ЦП и генерирует конфигурации закрепления ЦП и NUMA.
3. Нажмите **[OK]**.

Менеджер управления рассчитывает Топологию закрепления ЦП, обновляет поля топологии ЦП (Общее количество виртуальных ЦП, ядер на виртуальный сокет, потоков на ядро) и вводит строку конфигурации топологии в поле **Топология привязки ЦП (CPU Pinning Topology)** вкладки **Выделение ресурсов (Resource Allocation)** виртуальной машины.

Необходимо учитывать количество указанных виртуальных узлов NUMA и политику закрепления NUMA:

- Настройки NUMA хоста (память и ЦП).
- Узел NUMA, в котором указаны устройства хоста.
- Топология закрепления ЦП.
- Топологию закрепления потоков ввода-вывода.
- Размеры больших страниц.
- Закрепление NUMA можно настроить только для виртуальных машин. Закрепление NUMA нельзя настроить для пулов и шаблонов. Закрепление NUMA необходимо настроить вручную при создании высокопроизводительной виртуальной машины из шаблона.

9.2.4. Конфигурирование больших страниц (Configuring Huge Pages)

При запуске ВМ с настроенным свойством **hugepages** на хосте резервируется необходимое количество страниц оперативной памяти. Данная настройка рекомендована при наличии требований к производительности ОЗУ ВМ.

Количество свободных и занятых страниц можно найти на вкладке **Общее** подробного представления хоста в свойстве **Доступно Huge Pages (размер: количество)**.

Для использования больших страниц памяти на ВМ, предварительно настройте их на необходимых хостах в соответствии с разделом Конфигурация хостов для использования больших страниц руководства администратора.

Конфигурирование больших страниц

1. В окне **Создать… (New)/Изменить… (Edit)** на вкладке **Доп. параметры (Custom Properties)** выберите **hugepages** из списка пользовательских свойств, где по умолчанию отображается **Выберите ключ… (Please select a key…)**.
2. Укажите размер большой страницы в КБ (например, для задания размера страниц равной 1Гб, необходимо установить значение **1048576**).

К размеру большой страницы предъявляются следующие требования:

- Размер большой страницы у виртуальной машины должен быть такой же, что и у закрепленного хоста.

- Объем памяти виртуальной машины должен соответствовать выбранному размеру свободных больших страниц закрепленного хоста.
- Размер узла NUMA должен представлять собой величину, кратную выбранному размеру большой страницы.

При использовании больших страниц на виртуальной машине становится недоступным динамическое добавление или изъятие ОЗУ ВМ.

Данная настройка не влияет на количество и размер больших страниц внутри гостевой операционной системы ВМ.

При необходимости настройки больших страниц внутри гостевой ОС необходимо в дополнение к настройке **hugepages** добавить пользовательское свойство ВМ **extra_cpu_flags** со значением **pdpe1gb**.

9.2.5. Выключение KSM (Disabling KSM)

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)** и выберите кластер.
2. Нажмите **[Изменить (Edit)]**.
3. На вкладке **Оптимизация (Optimization)** снимите флажок **Включить KSM (Enable KSM)**.

10. Настройка часового пояса

Настройки часовых поясов для виртуальных машин хранятся в zVirt в файле **/etc/ovirt-engine/timezones/00-defaults.properties**. В этом файле содержатся значения часовых поясов по умолчанию, например, `Etc/GMT=Greenwich Standard Time`. В нем используются сопоставления, действительные для часовых поясов Windows и других.

Не изменяйте файл `00-defaults.properties`. Обновление или восстановление Менеджера управления приведет к перезаписи изменений.

Не изменяйте значения, которые поступают непосредственно от операционной системы или Менеджера управления.

Порядок действий:

1. Создайте файл переопределения в **/etc/ovirt-engine/timezones/**. Имя файла должно начинаться со значения больше **00**, чтобы этот файл появился после файла **/etc/ovirt-engine/timezones/00-defaults.properties** и должно заканчивался расширением **.properties**. Например, **10-timezone.properties** переопределяет файл по умолчанию **00-defaults.properties**. Последний файл в списке будет иметь приоритет перед предыдущими файлами.

2. Добавьте новые часовые пояса в этот файл. Убедитесь, что каждый ключ — это действительный Общий часовой пояс из базы данных часовых поясов, а значение - действительный часовой пояс Windows:

   Общее

   Часовые пояса, которые используются в операционных системах, отличных от Windows, должны соответствовать стандартному формату часового пояса, например, `Etc/GMT` или `Europe/Moscow`.

   Windows

   Часовые пояса, которые Windows непосредственно поддерживает, например, `GMT Standard Time` или `Israel Standard Time`.

3. Перезапустите службу `zVirt`:

```
systemctl restart ovirt-engine
```

Администрирование виртуальных машин

1. Выключение виртуальной машины

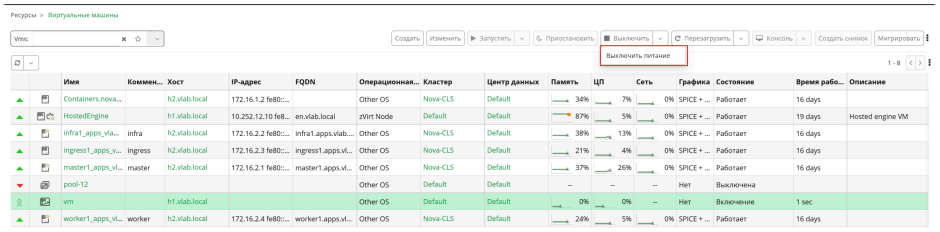
Прекратить работу виртуальной машины можно с помощью кнопки **[Выключить (Shutdown)]** или **[Отключить питание (Power Off)]**. Кнопка **[Выключить (Shutdown)]** позволяет корректно выключить виртуальную машину. Кнопка **[Отключить питание (Power Off)]** позволяет выполнить принудительное выключение. Корректное выключение предпочтительнее, нежели принудительное.

Если рядом с виртуальной машиной появился восклицательный знак, значит, удалить моментальный снимок не удалось, и после выключения невозможно будет повторно запустить виртуальную машину. Попробуйте удалить моментальный снимок снова и убедитесь, что восклицательный знак исчез, перед тем как выключить виртуальную машину. Дополнительную информацию см. в разделе Удаление моментального снимка.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите работающую виртуальную машину.
2. Нажмите **[Выключить (Shutdown)]** или нажмите правой кнопкой мыши на виртуальную машину и выберите **[Выключить (Shutdown)]** из всплывающего контекстного меню.
3. При желании на Портале администрирования в окне подтверждения **Выключить ВМ (Shut down Virtual Machine(s))** введите **Причину (Reason)** выключения виртуальной машины. В нем можно указать причину выключения, которая будет отображаться в журналах и во время следующего включения питания виртуальной машины.
4. В окне подтверждения **Выключить ВМ (Shut down Virtual Machine(s))** нажмите **[OK]**.

При корректном выключении **Состояние (Status)** виртуальной машины изменится на **Выключена (Down)** и будет обозначено значком ▼. Если виртуальную машину нельзя выключить корректно, нажмите стрелку "вниз" рядом с кнопкой **[Выключить (Shutdown)]**, а затем нажмите **[Выключить питание (Power Off)]** для выполнения принудительного выключения или нажмите правой кнопкой мыши на виртуальную машину и выберите **[Выключить питание (Power Off)]** из всплывающего контекстного меню.



2. Приостановка виртуальной машины

Приостановка виртуальной машины то же самое, что и перевод ее в Спящий режим (Hibernate).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите работающую виртуальную машину.
2. Нажмите **[Приостановить (Suspend)]** или нажмите правой кнопкой мыши на виртуальную машину и выберите **[Приостановить (Suspend)]** из всплывающего контекстного меню.

Состояние (Status) виртуальной машины изменится на **Приостановлена (Suspended)** и будет обозначено значком .

3. Перезагрузка или сброс виртуальной машины

Виртуальные машины можно перезапустить двумя способами — используя перезагрузку или сброс.

Перезагрузка виртуальной машины может потребоваться в некоторых случаях, например, после обновления или изменения конфигурации. При перезагрузке консоль виртуальной машины остается открытой, пока гостевая операционная система перезапускается.

Если гостевая операционная система не загружается или не отвечает, то требуется сброс виртуальной машины. При сбросе консоль виртуальной машины остается открытой, пока гостевая операционная система перезапускается.

Сброс виртуальной машины выполняется только с Портала администрирования.

Перезагрузка виртуальной машины

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите работающую виртуальную машину.

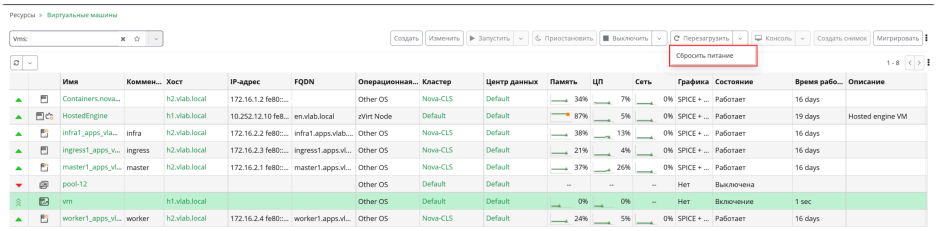
2. Нажмите **[Перезагрузить (Reboot)]** или нажмите правой кнопкой мыши на виртуальную машину и выберите **[Перезагрузить (Reboot)]** из всплывающего контекстного меню.
3. Нажмите **[OK]** в окне подтверждения **Перезагрузить ВМ (Reboot Virtual Machine(s))**.

Сброс виртуальной машины

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите работающую виртуальную машину.
2. Нажмите стрелку "вниз" рядом с кнопкой **[Перезагрузить (Reboot)]**, затем нажмите **[Сбросить питание (Reset)]** или нажмите правой кнопкой мыши на виртуальную машину и выберите **[Сбросить питание (Reset)]** из всплывающего контекстного меню.
3. Нажмите **[OK]** в окне подтверждения **Сбросить питание ВМ (Reset Virtual Machine(s))**.

Состояние (Status) виртуальной машины во время операций по перезагрузке и сбросу сначала изменится на **Перезагрузка в процессе (Reboot In Progress)** со значком , а затем вернется в значение **Работает (Up)** .



4. Удаление виртуальной машины

Кнопка **[Удалить (Remove)]** не активна во время работы виртуальных машин. Чтобы удалить виртуальную машину, ее нужно сначала выключить.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину, которую нужно удалить.
2. Нажмите **[Удалить (Remove)]** в ⋮.
3. При желании установите флажок **Удалить диск(и) (Remove Disk(s))**, чтобы вместе с виртуальной машиной удалить подключенные к ней виртуальные диски. Если флажок **Удалить диск(и) (Remove Disk(s))** снят, то виртуальные диски останутся в среде в качестве плавающих дисков.

4. Нажмите **[OK]**.

5. Клонирование виртуальной машины

Виртуальные машины можно клонировать без предварительного создания шаблона или моментального снимка.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину, которую нужно клонировать.
2. Нажмите **[Клонировать ВМ (Clone VM)]** в ⋮.
3. Введите **Имя (Name)** для новой виртуальной машины.
4. Нажмите **[OK]**.

6. Обновление гостевых агентов и драйверов виртуальных машин

Для обеспечения надежной работы виртуальных машин, рекомендуем выполнять систематическое обновление гостевых дополнений, следуя официальным руководствам от производителей соответствующих операционных систем.

Обратите внимание на следующие важные моменты:

- При поиске установочных пакетов, обязательно используйте официальный репозиторий производителя.
- Для успешной установки и функционирования гостевых дополнений, вам потребуются административные права.

Инструменты и агенты также предоставляют информацию для виртуальных машин, включая:

- Использование ресурсов.
- IP-адреса.
- Установленные приложения.

Гостевые инструменты для операционной систем семейства MS Windows распространяются в виде файла ISO, который можно подключить к виртуальным машинам. Гостевые инструменты для операционных систем семейства Linux распространяются с этими ОС в виде пакета, обычно называемым *qemu-guest-agent-<version>.rpm* или *qemu-guest-agent-<version>.deb*.

6.1. Обновление гостевых агентов и драйверов в Linux

Обновите гостевые агенты и драйверы на виртуальных машинах с Linux, чтобы использовать последнюю версию.

Порядок действий

1. Авторизуйтесь на виртуальной машине с Linux.
2. Обновите пакет `qemu-guest-agent`:
   - Для семейства ОС RedHat:

     ```
     dnf update qemu-guest-agent
     ```

   - Для семейства ОС Debian

     ```
     apt-get upgrade qemu-guest-agent
     ```

3. Перезапустите службу:

   ```
   systemctl restart qemu-guest-agent.service
   ```

6.2. Обновление гостевых агентов и драйверов Windows

Образ ISO с драйверами virtio для Windows, необходимый для выполнения процедур, описанных в этом разделе, можно загрузить в официальном репозитории Orion soft. Рекомендуем скачивать последнюю доступную версию образа.

Обновить драйверы Windows или гостевые агентов Windows можно с помощью ISO-образа `virtio-win`, используя командную строку виртуальной машины. Во время этой процедуры нужно удалить и переустановить драйверы, которые могут привести к нарушению работы сети. После переустановки драйверов настройки восстановятся.

Порядок действий:

1. При обновлении драйверов на виртуальной машине Windows используйте утилиту `netsh`, чтобы сохранить настройки TCP перед удалением драйвера `netkvm`:
   `C:\WINDOWS\system32>netsh dump > filename.txt`
2. Загрузите файл **virtio-win_version.iso** в домен данных.
3. Если виртуальная машина работает, то на **Портале администрирования** или **Пользовательском портале** нажмите ⋮ → **[Сменить CD (Change CD)]**, чтобы подключить файл **virtio-win_version.iso** к виртуальной машине. Если виртуальная

машина выключена, нажмите кнопку **[Однократный запуск(Run Once)]** и подключите файл **virtio-win_version.iso** как CD.

4. Авторизуйтесь на виртуальной машине.
5. Выберите CD-привод (в этом примере - D:\\), содержащий файл **virtio-win_version.iso**.
6. Переустановите гостевые агенты или драйверы:
   - Чтобы переустановить только гостевые агенты, используйте `qemu-ga-x86_64.msi`:

     ```
     C:\WINDOWS\system32>msiexec.exe /i D:\guest-agent\qemu-ga-x86_64.msi
     /passive /norestart
     ```

   - Чтобы переустановить гостевые агенты и драйверы или только драйверы, используйте `virtio-win-gt-x64.msi`:

     ```
     C:\WINDOWS\system32>msiexec.exe /i D:\virtio-win-gt-x64.msi /passive
     /norestart
     ```

7. При обновлении драйверов восстановите настройки, сохраненные с использованием `netsh`:

   ```
   C:\WINDOWS\system32>netsh -f filename.txt
   ```

7. Виртуальные машины и разрешения

7.1. Управление системными разрешениями для виртуальной машины

Администратор с ролью **SuperUser** управляет всеми аспектами Портала администрирования. Другим пользователям могут быть назначены ограниченные административные роли. Ограниченные роли нужны, чтобы предоставить пользователю административные права, которые действуют только в отношении определенного ресурса. Например, администратор с ролью **DataCenterAdmin** имеет права администратора центра данных только на назначенный центр данных (кроме его хранилища), а роль **ClusterAdmin** имеет права администратора кластера только на назначенный кластер.

Пользователь с ролью **UserVmManager** имеет права системного администратора виртуальных машин в центре данных. Эту роль можно применять к конкретным виртуальным машинам, к центру данных или ко всей среде виртуализации, что удобно, т.к. можно разрешать разным пользователям управлять определенными виртуальными ресурсами.

Роль администратора виртуальной машины разрешает пользователю выполнять следующие действия:

- Создавать, изменять и удалять виртуальные машины.
- Запускать, приостанавливать, выключать и останавливать виртуальные машины.

Роли и разрешения могут быть назначены только существующим пользователям.

Многие конечные пользователи связаны только с ресурсами виртуальной машины в среде виртуализации. Поэтому пользователю zVirt предоставляются несколько пользовательских ролей, позволяющих управлять именно виртуальными машинами, а не другими ресурсами центра данных.

7.2. Описание ролей администратора виртуальных машин

В приведенной ниже таблице описаны роли и права администратора, применимые к администрированию виртуальных машин.

Таблица 1. Роли системного администратора zVirt

Роль	Права	Примечания
DataCenterAdmin	Администратор центра данных	Обладает административными разрешениями в отношении всех объектов в конкретном центре данных, за исключением хранилища.
ClusterAdmin	Администратор кластера	Обладает административными разрешениями в отношении всех объектов в конкретном кластере.
NetworkAdmin	Администратор сети	Обладает административными разрешениями в отношении всех операций в конкретной логической сети. Может конфигурировать и управлять сетями, подключенными к виртуальным машинам. Чтобы сконфигурировать зеркалирование портов в сети виртуальных машин, примените роль **NetworkAdmin** к сети и роль **UserVmManager** к виртуальной машине.

7.3. Описание ролей пользователя виртуальных машин

В приведенной ниже таблице описаны пользовательские роли и права, применимые к пользователям виртуальных машин. Эти роли открывают доступ к Пользовательскому порталу, чтобы заходить на виртуальные машины и управлять ими, но не предоставляют никаких разрешений для Портала администрирования.

Таблица 2. Системные роли пользователя zVirt

Роль	Права	Примечания

Роль	Права	Примечания
UserRole	Может получать доступ к виртуальным машинам и пулам и использовать их.	Может авторизовываться на Пользовательском портале и использовать виртуальные машины и пулы.
PowerUserRole	Может создавать виртуальные машины и шаблоны и управлять ими.	В окне **Настройка (Configure)** (**Управление (Administration) > Настройка (Configure)**) назначьте эту роль пользователю для всей среды, либо только для отдельных центров данных или кластеров. Например, если роль **PowerUserRole** применяется на уровне центра данных, то пользователь в этой роли может создавать виртуальные машины и шаблоны в центре данных. Роль **PowerUserRole** эквивалентна ролям: **VmCreator**, **DiskCreator** и **TemplateCreator**.
UserVmManager	Системный администратор виртуальной машины.	Может управлять виртуальными машинами, создавать и использовать моментальные снимки. Пользователю, который создает виртуальную машину через Пользовательский портал, автоматически назначается роль **UserVmManager** для этой машины.
UserTemplateBasedVm	Ограниченные права на использование только Шаблонов.	Уровень прав позволяет создавать виртуальные машины с помощью шаблона.
VmCreator	Может создавать виртуальные машины на Пользовательском портале.	Эта роль применяется не к отдельной виртуальной машине. Применяйте эту роль ко всей среде в окне **Настройка (Configure)**. Применяя эту роль к кластеру, нужно также применить роль **DiskCreator** ко всему центру данных или к конкретным доменам хранения.
VnicProfileUser	Пользователь логической сети и сетевого интерфейса для виртуальных машин.	Если при создании профиля интерфейса логической сети vNIC, была выбрана опция **Разрешить всем пользователям доступ к этому профилю (Allow all users to use this Profile)**, то разрешения **VnicProfileUser** назначаются всем пользователям логической сети. Затем пользователи могут подключать/отключать сетевые интерфейсы виртуальных машин к/от логической сети.

7.4. Назначение виртуальных машин пользователям

Если виртуальные машины создаются для других пользователей, а не для создающего пользователя, то сначала следует назначить роли пользователям, и только потом они смогут использовать виртуальные машины. Обратите внимание, что роли можно назначать только существующим пользователям. Для получения дополнительной информации о

создании учетных записей пользователей см. раздел **Пользователи и роли** в **Руководстве администратора**

Пользовательский портал поддерживает три роли по умолчанию: Пользователь (User), Ключевой пользователь (PowerUser) и Пользователь, управляющий ВМ (UserVmManager). Однако нестандартные роли можно настраивать через Портал администрирования. Роли по умолчанию описаны ниже.

- Пользователь с ролью **UserRole** может подключаться к виртуальным машинам и использовать их. Эта роль подходит конечным пользователям ПК, выполняющим повседневные задачи.
- Пользователь с ролью **PowerUser** может создавать виртуальные машины и просматривать виртуальные ресурсы. Эта роль подходит администраторам или менеджерам, которые хотят предоставить виртуальные ресурсы работникам.
- Пользователь с ролью **UserVmManager** может изменять и удалять виртуальные машины, назначать пользовательские разрешения, использовать моментальные снимки и шаблоны. Роль подходит, если требуется внести изменения конфигурации в виртуальной среде.

Когда создается виртуальная машина, она автоматически наследует права Пользователя, которому назначена роль **UserVmManager** для управления созданной ВМ. Это позволяет вносить изменения в виртуальную машину и назначать пользователям разрешения на управление ею.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к её подробному представлению.
3. Откройте вкладку **Разрешения (Permissions)**.
4. Нажмите **[Добавить (Add)]**.
5. Введите реальное или пользовательское имя или часть имени пользователя в текстовое поле и выберите нужное из списка возможных совпадений в списке результатов. Нажмите **[Поиск (Go)]**
6. Установите флажок напротив пользователя, которому будут назначены разрешения.
7. Из выпадающего списка **Роль для связи: (Role to Assign)** выберите **UserRole**.
8. Нажмите **[OK]**.

Имя и роль пользователя отобразятся в списке пользователей, которым разрешен доступ к этой виртуальной машине.

Если пользователю назначены разрешения только в отношении одной виртуальной машины, то для этой виртуальной машины может быть настроен единый вход (SSO). Когда включен единый вход, пользователь авторизуется на Пользовательском портале, а затем подключается к виртуальной машине, например, через SPICE-консоль, при этом пользователи автоматически авторизуются на виртуальной машине, и им не нужно снова вводить имя пользователя и пароль. Единый вход можно включить или выключить на каждой отдельно взятой виртуальной машине. Подробную информацию о включении и выключении единого входа для виртуальных машин см. в разделе Настройка единого входа (Single Sign-On) для виртуальных машин.

7.5. Лишение пользователей доступа к виртуальным машинам

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите на имя виртуальной машины, чтобы перейти к её подробному представлению.
3. Нажмите **Разрешения (Permissions)**.
4. Выберите разрешения, которые хоте удалить (чтобы выбрать несколько зажмите клавишу `Ctrl` на клавиатуре и щёлкните на разрешениях).
5. Нажмите **[Удалить (Remove)]**. Появится предупреждающее сообщение с просьбой подтвердить удаление выбранных разрешений.
6. Для подтверждения удаления выбранных пользователей нажмите **[OK]**. Для отмены нажмите **[Закрыть (Cancel)]**.

8. Моментальные снимки

8.1. Создание моментального снимка виртуальной машины

Моментальный снимок — это представление операционной системы виртуальной машины, всех ее приложений и данных в конкретный момент времени. Его можно использовать для сохранения настроек виртуальной машины перед обновлением или установкой новых приложений. В случае возникновения проблем, снимок можно использовать для восстановления виртуальной машины до предыдущего состояния.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Снимки (Snapshots)** и нажмите **[Создать (Create)]**.

4. Введите описание моментального снимка.
5. Выберите диски в **Выбрать диски (Disks to include)**, отметив их флажками.

> Если ни один диск не выбран, то будет создан частичный моментальный снимок виртуальной машины (без диска). Доступен предварительный просмотр моментального снимка для проверки конфигурации виртуальной машины. Обратите внимание, что если подтвердить частичный моментальный снимок в процедуре восстановления, то результат процедуры каждый раз будет виртуальная машина без диска.

6. Выберите **Сохранить память (Save Memory)**, чтобы память работающей виртуальной машины была включена в моментальный снимок.
7. Нажмите **[OK]**.

Операционная система и приложения виртуальной машины на выбранном(-ых) диске(-ах) хранятся в моментальном снимке, для которого доступны предварительный просмотр и восстановление. При создании моментального снимка у него будет состояние **Заблокировано (Locked)**, который потом изменится на **Ok**. Если на вкладке **Снимки (Snapshots)** нажать на моментальный снимок, то подробные сведения о нем будут отображаться в выпадающих списках **Общее (General)**, **Диски (Disks)**, **Сетевые интерфейсы (Network Interfaces)** и **Установленные приложения (Installed Applications)** .

8.2. Использование моментальных снимков для восстановления виртуальной машины

С помощью моментального снимка можно восстановить виртуальную машину до предыдущего состояния.

> Процесс восстановления можно начать только при выключенной виртуальной машине.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Снимки (Snapshots)**, чтобы открыть список доступных моментальных снимков.
4. В верхней панели выберите моментальный снимок для восстановления. Подробные сведения о моментальном снимке отображаются в нижней панели.
5. Нажмите кнопку **[Предварительный просмотр (Preview)]** и выберите **Пользовательский (Custom)**.
6. Установите флажки, чтобы выбрать **Память (Memory)** и **Диски (Disks)** , которые хотите восстановить, и нажмите **[OK]**. Так, можно создавать и восстанавливаться с

пользовательского моментального снимка, используя конфигурацию и диск(-и) из нескольких моментальных снимков.

Состояние моментального снимка изменится на **Режим предварительного просмотра (Preview Mode)**. Состояние виртуальной машины ненадолго изменится на **Образ заблокирован (Image Locked)**, а потом вернется в значение **Выключен (Down)** .

7. Включите виртуальную машину; она будет работать на образе диска моментального снимка.
8. Выключите виртуальную машину.
9. Нажмите **[Подтвердить (Commit)]**, чтобы всегда восстанавливать виртуальную машину до состояния этого моментального снимка. Все последующие моментальные снимки будут стерты. Либо нажмите **[Отменить (Undo)]**, чтобы отключить моментальный снимок и вернуть виртуальную машину к предыдущему состоянию.

При наличии нескольких снимков, восстановление состояния виртуальной машины из одного из них, удалит более поздние снимки, а их данные будут потеряны.

8.3. Создание виртуальной машины из моментального снимка

С помощью моментального снимка можно создать виртуальную машину.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Снимки (Snapshots)**, чтобы открыть список доступных моментальных снимков.
4. Выберите моментальный снимок из списка и нажмите **[Клонировать (Clone)]**.
5. Введите **Имя (Name)** виртуальной машины.
6. Нажмите **[OK]**.

Вскоре клонированная виртуальная машина появится на вкладке **Виртуальные машины (Virtual Machines)** на панели навигации в состоянии **Образ заблокирован (Image Locked)**. Состояние виртуальной машины не изменится, пока zVirt не завершит ее создание. Создание виртуальных дисков с динамическим расширением пространства занимает меньше времени, чем создание виртуальных дисков с предварительным выделением.

Когда виртуальная машина готова к использованию, ее состояние в разделе **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** изменится с **Образ заблокирован (Image Locked)** на **Выключен (Down)** .

8.4. Удаление моментального снимка

Моментальный снимок виртуальной машины можно стереть и навсегда удалить из среды zVirt.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Снимки (Snapshots)**, чтобы открыть список моментальных снимков выбранной виртуальной машины.
4. Выберите моментальный снимок, который хотите удалить.
5. Нажмите **[Удалить (Delete)]**.
6. Нажмите **[OK]**.

При неудачной попытке удаления устраните проблему, из-за которой удаление не произошло (например, отказ хоста, недоступное устройство хранения или временные проблемы в работе сети), и попробуйте еще раз.

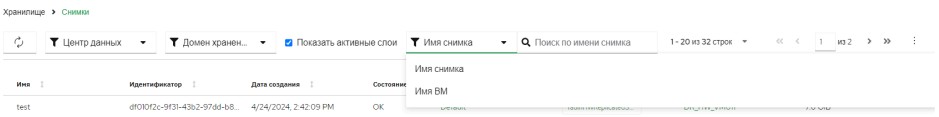
8.5. Просмотр списка всех моментальных снимков

В разделе **Хранилище (Storage)** > **Снимки (Snapshots)** отображаются моментальные снимки из всех доменов хранения.

Моментальные снимки можно:

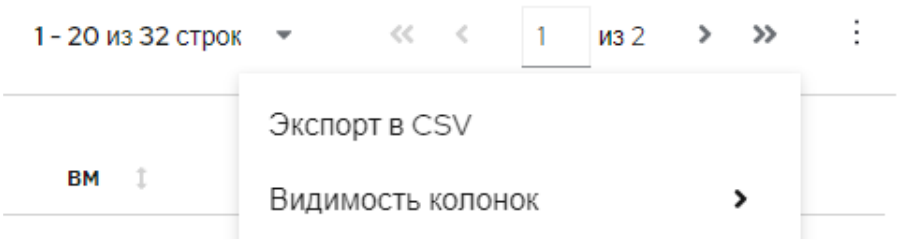
- отфильтровать по:
  - центру данных;
  - домену хранения;
- найти по:
  - имени снимка;
  - имени ВМ.

При необходимости можно включить опцию **Показать активные слои** виртуальной машины.



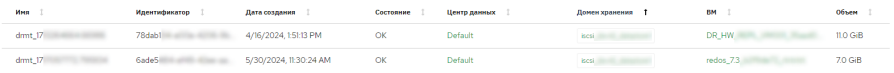
С помощью кнопки ⋮ можно:

- экспортировать в `CSV`;
- настроить видимость колонок.



На странице **Снимки (Snapshots)** при нажатии на имя:

- центра данных будет выполнен переход на страницу администрирования центра данных, к которому относится моментальный снимок;
- домена хранения будет выполнен переход на страницу администрирования домена хранения, на котором располагается моментальный снимок;
- виртуальной машины будет выполнен переход на страницу администрирования виртуальной машины, к которой относится моментальный снимок;



9. Устройства хоста

9.1. Добавление устройства хоста к виртуальной машине

Чтобы повысить производительность, можно подключить устройство хоста к виртуальной машине.

Устройства хоста — это физические устройства, подключенные к определенной машине хоста, например:

- накопители на магнитной ленте, диски и чейнджеры SCSI;
- сетевые карты, графические процессоры, HBA-адаптеры;
- мыши, камеры и диски с USB-интерфейсом;

Добавить устройство хоста к виртуальной машине можно в её подробном представлении через закладку **Устройства хоста (Host Devices)**. Сначала выберите один из хостов кластера и тип устройства. Затем выберите и подключите одно или несколько устройств хоста на этом хосте.

При изменении настройки через кнопку **[Прикрепить к другому хосту (Pin to another host)]** удаляются текущие устройства хоста. Когда эти изменения сохраняются в настройках **Хост (Host)** виртуальной машины, параметр **Запустить на (Start Running On)** переключается в значение **Указанном хосте (Specific Host(s))** и задает хост, который был выбран ранее через настройку **Прикрепить к другому хосту (Pin to another host)**.

После подключения одного или нескольких устройств хоста, запустите виртуальную машину, чтобы изменения вступили в силу. Виртуальная машина запускается на хосте, у которого есть подключенные устройства хоста. Если виртуальная машина не может запуститься на указанном хосте или получить доступ к устройству хоста, то она отменяет операцию запуска и показывает сообщение об ошибке с информацией о причине отмены.

Предварительные условия:

- Статус хоста **Включено (Up)** .
- Хост настроен на прямое назначение устройств.

Порядок действий:

1. На Портале администрирования нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.
2. Выключите виртуальную машину.
3. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
4. Откройте вкладку **Устройства хоста (Host Devices)**.
5. Нажмите **[Добавить устройство (Add device)]**. Откроется окно **Добавить устройства хоста (Add Host Devices)**.
6. Используйте параметр **Хост (Pinned Host)**, чтобы выбрать хост, на котором будет работать виртуальная машина.
7. Используйте параметр **Совместимость (Capability)**, чтобы открыть список устройств `pci`, `scsi`, `nvdimm` или `usb_device`.

   Параметр nvdimm — это предварительная версия функции, представленная для оценки. Дополнительные сведения см. Устройства хоста NVDIMM.

8. Выберите устройства через **Доступные устройства хоста (Available Host Devices)**.
9. Нажмите стрелку вниз , чтобы перенести устройства в **Подключаемые устройства хоста (Host Devices to be attached)**.
10. Нажмите **[OK]**, чтобы подключить эти устройства к виртуальной машине и закрыть окно.
    - Дополнительно: при подключении хост-устройств SCSI настройте наиболее подходящий драйвер.

a. Нажмите **[Изменить (Edit)]**. Откроется окно **Изменить виртуальную машину (Edit Virtual Machine)**.

b. Откройте вкладку **Доп. параметры (Custom Properties)**.

c. Нажмите **[Выберите ключ (Please select a key)]** и выберите **scsi_hostdev** внизу выпадающего списка.

d. В большинстве случаев выбирайте **scsi-hd**. В остальных случаях, а именно для накопителей на магнитной ленте или CD-чейнджеров, выбирайте параметр **scsi_generic**. Дополнительные сведения см. в разделе Описание настроек пользовательских свойств виртуальных машин.

e. Нажмите кнопку **[OK]**.

11. Запустите виртуальную машину.
12. Пока виртуальная машина запускается, посмотрите сообщения об ошибках в **Отмененные операции (Operation Canceled)**.

9.1.1. Поиск и устранение неполадок

Если не получается добавить устройство хоста к виртуальной машине, или виртуальная машина не запускается с подключенными устройствами хоста, то появятся сообщения об ошибках **Отмененные операции (Operation Canceled)**. Например:

```
Operation Canceled
Error while executing action:

<vm name>:
* Cannot run VM. There is no host that satisfies current scheduling constraints.
See below for details:
* The host <first_hostname> did not satisfy internal filter HostDevice because
it does not support host device passthrough.
* The host <second_hostname> did not satisfy internal filter HostDevice because
the host does not provide requested host devices.
```

Ошибку можно устранить, удалив устройство хоста из виртуальной машины или исправив проблемы, о которых говорится в сообщении об ошибке. Например:

- В ответ на сообщение `The host <hostname> did not satisfy internal filter HostDevice because it does not support host device passthrough` (Хост <имя хоста> не прошел внутренний фильтр HostDevice, поскольку он не поддерживает сквозной доступ устройств хоста) настройте сквозной доступ устройств на хосте и перезапустите виртуальную машину.
- В ответ на сообщение `The host <hostname> did not satisfy internal filter HostDevice because the host does not provide requested host devices` (Хост <имя хоста> не прошел внутренний фильтр HostDevice, поскольку хост не предоставляет запрашиваемые устройства хоста) добавьте устройство на хост.

- В ответ на сообщение `Cannot add Host devices because the VM is in Up status` (Невозможно добавить устройства хоста, поскольку виртуальная машина находится во включенном состоянии) выключите виртуальную машину перед добавлением устройства хоста.
- Проверьте, что состояние хоста **Включено (Up)** 🔺.

9.2. Удаление устройств хоста из виртуальной машины

Необязательно удалять все устройства хоста, непосредственно подключенные к виртуальной машине, чтобы добавить устройства с другого хоста. Достаточно добавить устройства с нужного хоста, при этом все устройства, уже подключенные к виртуальной машине, удалятся автоматически.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Устройства хоста (Host Devices)**, чтобы открыть список устройств хоста, подключенных к виртуальной машине.
4. Выберите устройство хоста, которое необходимо отключить от виртуальной машины, или, зажав клавишу `Ctrl`, выберите несколько устройств и нажмите **[Удалить устройство (Remove device)]**. Откроется окно **Удалить устройство(-а) хоста (Remove Host Device(s))**.
5. Нажмите **[OK]**, чтобы подтвердить и удалить выбранные устройства у виртуальной машины.

9.3. Закрепление виртуальной машины на другом хосте

Можно открыть вкладку **Устройства хоста (Host Devices)** в подробном представлении виртуальной машины, чтобы закрепить ее на конкретном хосте. Если к виртуальной машине подключены какие-либо устройства хоста, то при закреплении виртуальной машины на другом хосте эти устройства хоста автоматически удалятся из виртуальной машины.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Нажмите на имя виртуальной машины, чтобы открыть её подробное представление.
3. Откройте вкладку **Устройства хоста (Host Devices)**.
4. Нажмите **Прикрепить к другому хосту (Pin to another host)**. Откроется окно **Прикрепить ВМ к хосту (Pin VM to Host)**.
5. В выпадающем меню **Хост (Host)** выберите хост.

6. Нажмите **[OK]**, чтобы закрепить виртуальную машину на выбранном хосте.

9.4. Устройства хоста NVDIMM

Устройства NVDIMM — это предварительная версия технологии, представленная только для оценки (Technology Preview) и не обеспечиваются технической поддержкой. Orion soft не рекомендует использовать их в продуктивной среде.

Можно добавить эмулируемые устройства NVDIMM к виртуальным машинам. Этот тип памяти также известен под названием **виртуальный NVDIMM (virtual NVDIMM)** или **vNVDIMM**. Работу эмулируемого устройства NVDIMM, которое можно подключить к виртуальной машине, обеспечивает реальное устройство NVDIMM на том хосте, где работает виртуальная машина. Поэтому, прикрепление NVDIMM к виртуальной машине также привязывает виртуальную машину к определенному хосту. Можно перенастроить режим, разбиение на разделы и другие свойства эмулируемого устройства NVDIMM в виртуальной машине, не затрагивая настройки физического NVDIMM на устройстве хоста. Чтобы добавить эмулируемое устройство NVDIMM к виртуальной машине, см. раздел Добавление устройства хоста к виртуальной машине.

Ограничения

- Моментальные снимки памяти отключены, когда устройство NVDIMM находится в виртуальной машине. Невозможно сделать моментальный снимок содержимого NVDIMM, а моментальный снимок памяти не может работать корректно без соответствующих данных NVDIMM.
- В zVirt у каждого устройства NVDIMM, переданного на виртуальную машину, есть автоматически назначенная зона меток с фиксированным размером 128 КБ на оборудовании IBM POWER и, кроме того, 128 КБ — это минимальный размер метки, допустимый в QEMU.
- По умолчанию виртуальная машина использует все устройство NVDIMM. Нельзя настроить размер NVDIMM через виртуальную машину. Для настройки размера необходимо на хосте разбить устройство NVDIMM на разделы и добавить раздел к виртуальной машине.
- Размер устройства NVDIMM на виртуальной машине может быть несколько меньше, чем на хосте, чтобы подходить под скорректированные размер и соотношение libvirt и QEMU. Необходимо также очень точно подбирать размер, чтобы горячее подключение памяти нормально выполнялось.
- libvirt и QEMU корректируют свой размер и размещение меток. Изменение этих внутренних соотношений может привести к потере данных.
- Платформа не поддерживает горячее подключение NVDIMM.

- Виртуальные машины с устройствами NVDIMM не могут мигрировать, потому что они закреплены на хосте.
- SELinux на данный момент блокирует доступ к устройствам NVDIMM в режиме devdax.

Дополнительные ресурсы

- Документация QEMU NVDIMM

10. Группы сходства

10.1. Группы сходства

Группы сходства (Affinity) помогают определить место работы выбранных виртуальных машин относительно друг друга и указанных хостов. Эта функциональность помогает управлять сценариями разных процессов, чтобы соблюдать лицензионные требования, обеспечивать высокую доступность и аварийное восстановление.

Правило сходства ВМ

Когда создается группу сходства, выбираются виртуальные машины, которые входят в эту группу. Чтобы задать место работы этих виртуальных машин относительно друг друга, включите **Правило сходства ВМ (VM Affinity Rule)**:

- **Положительное** — правило пытается запускать виртуальные машины вместе на одном хосте;
- **Отрицательное** — правило пытается запускать виртуальные машины отдельно на разных хостах.

Если правило не может быть выполнено, результат зависит от того, включен ли модуль веса или фильтра.

Правило сходства хостов

При желании можно добавить хосты к группе сходства. Чтобы задать место работы виртуальных машин в такой группе относительно хостов в этой группе, включите **Правило сходства хоста (Host Affinity Rule)**:

- **Положительное** — правило пытается запускать виртуальные машины на хостах в группе сходства;
- **Отрицательное** — правило пытается запускать виртуальные машины на хостах, которые не входят в группу сходства.

Если правило не может быть выполнено, результат зависит от того, включен ли модуль веса или фильтра.

Вес модулей по умолчанию

По умолчанию оба правила сходства обращаются к весу модулей в политике планирования кластера. Используя веса модулей, планировщик стремится выполнить правило, но в любом случае разрешает виртуальным машинам в группе сходства работать, если правило не может быть выполнено.

Например, при положительном **Правиле сходства ВМ (VM Affinity Rule)** и включенных весах модулей планировщик стремится запустить все виртуальные машины группы сходства на одном хосте. Однако если у одного хоста недостаточно ресурсов для этого, планировщик запускает виртуальные машины на нескольких хостах.

Чтобы этот модуль работал, в разделе **Вес модулей (Weights Modules)** политик планирования должны быть ключевые слова `VmAffinityGroups` и `VmToHostsAffinityGroups`.

Функция принудительного исполнения и модули фильтров

Оба правила сходства предусматривают возможность **Принудительного исполнения (Enforcing)**, которая применяет модуль фильтра в политике планирования кластера. Модули фильтров переопределяют веса модулей. При включенных модулях фильтров планировщик требует выполнения правила. Если правило не может быть выполнено, модули фильтров не дают запуститься виртуальным машинам в группе сходства.

Например, при положительном **Правиле связности хостов (Host Affinity Rule)** и включенной функции **Принудительного исполнения (Enforcing)** (модули фильтра включены) планировщик обязательно будет делать так, чтобы виртуальные машины группы сходства запускались на хостах из группы сходства. Однако если эти хосты выключены, то планировщик **не** запускает виртуальные машины.

Чтобы этот модуль работал, в разделе **Модули фильтров (Filter Modules)** политик планирования должны быть ключевые слова `VmAffinityGroups` и `VmToHostsAffinityGroups`.

Дополнительные сведения о том, как эти правила и параметры можно сочетать, см. в разделе Примеры групп сходства.

- По своей функции метка сходства аналогична группе сходства с положительным **Правилом связности хостов (Host Affinity Rule)** и включенной функцией **Принудительно (Enforcing)**.
- Чтобы метки сходства работали, в разделе **Модули фильтров (Filter Modules)** политик планирования должен быть включен хотя бы один фильтр.
- Если между группой сходства и меткой сходства возникают противоречия, то затрагиваемые виртуальные машины не запускаются. Сведения о предотвращении, устранении и разрешении противоречий см. в разделе Поиск и устранение неполадок в группах сходства.

Веса модулей и Модули фильтров влияют на каждое правило в политике планирования кластера.

- Чтобы **Правило сходства ВМ (VM Affinity Rule)** работало, в политике планирования должно быть ключевое слово `VmAffinityGroups` в разделах **Вес модулей (Weights Modules)** и **Модули фильтров (Filter modules)**.
- Чтобы **Правило связности хостов (Host Affinity Rule)** работало, в политике планирования должно быть ключевое слово `VmToHostsAffinityGroups` в разделах **Вес модулей (Weights Modules)** и **Модули фильтра (Filter Modules)**.

- Группы сходства применяются к виртуальным машинам в кластере. Перемещение виртуальной машины из одного кластера в другой удаляет ее из групп сходства в исходном кластере.
- Виртуальные машины не нужно перезапускать, чтобы правила групп сходства вступили в силу.

10.2. Создание группы сходства

Новые группы сходства можно создавать на Портале администрирования.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к её подробному представлению.
3. Откройте вкладку **Группы сходства (Affinity Groups)**.
4. Нажмите **[Новая (New)]**.
5. Введите **Имя (Name)** и **Описание (Description)** для группы сходства.
6. Из выпадающего списка **Правило ВМ (VM Affinity Rule)** выберите **Положительно (Positive)** для применения положительного правила сходства или **Отрицательно (Negative)** для применения отрицательного. Выберите **Отключено (Disable)**, чтобы выключить правило сходства.
   - Установите флажок **Принудительно (Enforcing)**, чтобы обеспечить принудительное исполнение, или убедитесь, что флажок снят, чтобы принудительное исполнение не применялось.
7. Из выпадающего списка выберите виртуальные машины, которые нужно добавить в группу сходства. Чтобы добавить или удалить дополнительные виртуальные машины, используйте кнопки [+] и [−].
8. Из выпадающего списка **Правило сходства хоста (Host Affinity Rule)** выберите **Положительно (Positive)** для применения положительного правила сходства или

Отрицательно (Negative) для применения отрицательного. Выберите **Отключено (Disable)**, чтобы выключить правило сходства.

- Установите флажок **Принудительно (Enforcing)**, чтобы обеспечить принудительное исполнение, или убедитесь, что флажок снят, чтобы принудительное исполнение не применялось.

9. Из выпадающего списка выберите хосты, которые нужно добавить в группу сходства. Чтобы добавить или удалить дополнительные хосты, используйте кнопки + и −.
10. Нажмите **[OK]**.

10.3. Изменение группы сходства

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к её подробному представлению.
3. Откройте вкладку **Группы сходства (Affinity Groups)**.
4. Нажмите **[Изменить (Edit)]**.
5. Установите желаемые значения, используя выпадающие списки **Правило сходства ВМ (VM Affinity Rule)** и флажки **Принудительно (Enforcing)**, и с помощью кнопок + и − добавляйте или удаляйте виртуальные машины и/или хосты в или из группы сходства.
6. Нажмите **[OK]**.

10.4. Удаление группы сходства

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите на имя виртуальной машины, чтобы перейти к её подробному представлению.
3. Откройте вкладку **Группы сходства (Affinity Groups)**.
4. Нажмите **[Удалить (Remove)]**.
5. Нажмите **[OK]**.

Политика сходства, применявшаяся к виртуальным машинам, которые входили в эту группу сходства, больше не применяется.

10.5. Примеры групп сходства

На примерах ниже показано, как применять правила сходства для разных сценариев, используя разные возможности групп сходства, описанные в этой главе.

Пример 1. Высокая доступность

Евгения работает инженером DevOps в стартапе. Для обеспечения высокой доступности две виртуальные машины должны работать на разных хостах в кластере.

Евгения создает группу сходства с именем "high availability ABC" и делает следующее:

- Добавляет эти две виртуальные машины: `VM01` и `VM02` в группу сходства.
- Задает **Правило сходства ВМ (VM Affinity Rule)** как **Отрицательно (Negative)**, чтобы виртуальные машины старались запускаться на разных хостах.
- Оставляет флажок **Принудительно (Enforcing)** снятым (отключенным), чтобы обе виртуальные машины могли продолжить работу, если во время сбоя будет доступен только один хост.
- Оставляет список **Хосты (Hosts)** пустым, чтобы виртуальные машины запускались на любом хосте в кластере.

Пример 2. Производительность

Сидор разрабатывает ПО и использует две виртуальные машины для сборки ПО и его многократного ежедневного тестирования. Между этими двумя виртуальными машинами идет интенсивный сетевой трафик. Благодаря работе машин на одном и том же хосте снижается сетевой трафик и влияние задержки сети на процесс сборки и тестирования. Использование хостов с лучшими характеристиками (ЦП с более высокой скоростью, SSD, больший объем памяти) позволяет ускорить процесс.

Сидор создает группу сходства с именем "build and testing ABC" и делает следующее:

- Добавляет виртуальные машины для сборки и тестирования `VM01` и `VM02` в группу сходства.
- Добавляет хосты с лучшими характеристиками `host03`, `host04` и `host05` в группу сходства.
- Задает **Правило сходства ВМ (VM Affinity Rule)** как **Положительно (Positive)**, чтобы виртуальные машины старались запускаться на одном и том же хосте, что снизит сетевой трафик и влияние задержки.
- Задает **Правило сходства хоста (Host Affinity Rule)** как **Положительно (Positive)**, чтобы виртуальные машины старались запускаться на хостах с лучшими характеристиками для ускорения процесса.
- Оставляет флажок **Принудительно (Enforcing)** снятым (отключенным) для обоих правил, чтобы виртуальные машины могли запускаться, если хосты с лучшими

характеристиками не доступны.

Пример 3. Лицензирование

Афанасий — менеджер по программным активам, который помогает своей организации соблюдать требования вендорской ограничительной лицензии на ПО для 3D-визуализации. По условиям лицензии, виртуальные машины для сервера лицензий `VM-LS` и рабочие станции визуализации `VM-WS#` должны работать на одном и том же хосте. Кроме того, физическим ЦП, согласно модели лицензирования ПО требуется, чтобы рабочие станции работали на одном из двух GPU-хостов: основном `host-gpu-primary` или резервном `host-gpu-backup`.

Для удовлетворения этих требований Афанасий создает группу сходства с именем "seismic 3D images ABC" и делает следующее:

- Добавляет ранее упомянутые виртуальные машины и хосты в группу сходства.
- Задает **Правило сходства ВМ (VM Affinity Rule)** как **Положительно (Positive)** и ставит флажок **Принудительно (Enforcing)**, чтобы сервер лицензий и рабочие станции обязательно запускались вместе на одном из хостов, а не на разных хостах.
- Задает **Правило сходства хоста (Host Affinity Rule)** как **Положительно (Positive)** и ставит флажок **Принудительно (Enforcing)**, чтобы виртуальные машины обязательно запускались на одном из двух GPU-хостов, а не на других хостах в кластере.

10.6. Поиск и устранение неполадок в группах сходства

Чтобы предотвратить возникновение проблем с группами сходства:

- Спланируйте и задокументируйте ожидаемые сценарии и результаты от использования групп сходства.
- Проверьте и протестируйте результаты при разных условиях.
- Применяйте передовые методы управления изменениями.
- Используйте опцию **Принудительно (Enforcing)**, если требуется.

При обнаружении остановки виртуальных машин:

- Проверьте, что в кластере есть политика планирования, где разделы **Вес модулей (Weights Modules)** и **Модули фильтров (Filter Modules)** содержат `VmAffinityGroups` и `VmToHostsAffinityGroups`.
- Проверьте наличие конфликтов между метками сходства и группами сходства.

При возможных конфликтах между метками сходства и группами сходства:

- Учитывайте, что метка сходства — это эквивалент группы сходства, у которой **Правило сходства хоста (Host Affinity Rule)** установлено как **Положительно (Positive)** и включена опция **Принудительно (Enforcing)** .
- Учитывайте, что при конфликте между меткой сходства и группой сходства пересекающийся набор виртуальных машин работать не будет.
- Определите, возможен ли конфликт:
  - Изучите раздел **Модули фильтров (Filter Modules)** в политиках планирования кластера. Они должны содержать ключевое слово `VmAffinityGroups` ИЛИ `VmToHostsAffinityGroups` . В противном случае конфликт невозможен. (Наличие `VmAffinityGroups` и `VmToHostsAffinityGroups` в разделе **Вес модулей (Weights Modules)** не имеет значения, так как ключевые слова в разделе **Модули фильтров (Filter Modules)** переопределят их).
  - Изучите группы сходства. В них должно содержаться правило с включенной опцией **Принудительно (Enforcing)**. В противном случае конфликт невозможен.
- Если конфликт возможен, определите набор виртуальных машин, которые могут быть вовлечены:
  - Изучите метки сходства и группы сходства. Составьте список виртуальных машин, которые входят и в метку сходства, и в группу сходства, где включена опция **Принудительное исполнение (Enforcing)**.
  - Для каждого хоста и каждой виртуальной машины в пересекающемся наборе проанализируйте условия, при которых может произойти конфликт.
- Определите, совпадают ли неработающие виртуальные машины с виртуальными машинами в анализе.
- Наконец, реструктурируйте группы сходства и метки сходства, чтобы избежать непреднамеренных конфликтов.
- Проверьте, что любые изменения приводят к ожидаемым результатам в разных условиях.
- При наличии перекрывающихся групп сходства и меток сходства их проще просматривать в одном месте как группы сходства. Рассмотрите возможность преобразования метки сходства в эквивалентную группу сходства, где **Правило сходства хоста (Host Affinity Rule)** задано как **Положительно (Positive)** и включена опция **Принудительно (Enforcing)**.

11. Метки сходства

11.1. О метках сходства

Метки сходства можно создавать и модифицировать на Портале администрирования.

Метки сходства (Affinity Labels) используются вместе с **Группами сходства (Affinity Groups)** для установки любого вида сходства между виртуальными машинами и хостами (положительное, отрицательное). Смотрите раздел Группы сходства для получения больше информации о степени сходства.

Метки сходства являются подмножеством групп сходства и могут с ними конфликтовать. В случае конфликта виртуальная машина не запустится.

11.2. Создание метки сходства

Метки сходства можно создать из подробного представления виртуальной машины, хоста или кластера. В данном конкретном случае используется подробное представление кластера.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)** и выберите соответствующий кластер.
2. Нажмите на имя кластера, чтобы перейти к его подробному представлению.
3. Откройте вкладку **Метки сходства (Affinity Labels)**.
4. Нажмите **[Новый (New)]**.
5. Введите **Имя (Name)** для метки сходства.
6. Из выпадающих списков выберите виртуальные машины и хосты, которые будут ассоциированы с меткой. Для добавления дополнительных виртуальных машин и хостов используйте кнопку +.
7. Нажмите **[OK]**.

11.3. Изменение метки сходства

Метки сходства можно изменить из подробного представления виртуальной машины, хоста или кластера. В данном конкретном случае используется подробное представление кластера.

Порядок действий (для кластера):

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)** и выберите соответствующий кластер.
2. Нажмите на имя кластера, чтобы перейти к его подробному представлению.
3. Откройте вкладку **Метки сходства (Affinity Labels)**.
4. Выберите метку, которую хотите изменить.
5. Нажмите **[Изменить (Edit)]**.

6. Для добавления или удаления виртуальных машин и хостов в или из метки сходства используйте кнопки + и −.
7. Нажмите **[OK]**.

11.4. Удаление метки сходства

Метки сходства можно удалить только из подробного представления кластера.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Кластеры (Clusters)** и выберите соответствующий кластер.
2. Нажмите на имя кластера, чтобы перейти к его подробному представлению.
3. Откройте вкладку **Метки сходства (Affinity Labels)**.
4. Выберите метку, которую хотите удалить.
5. Нажмите **[Изменить (Edit)]**.
6. Для удаления всех виртуальных машин и хостов из метки сходства используйте кнопку −.
7. Нажмите **[OK]**.
8. Нажмите **[Удалить (Delete)]**.
9. Нажмите **[OK]**.

12. Экспортирование и импортирование виртуальных машин и шаблонов

Сущность "экспорт-домен" считается устаревшей. Экспорт-домены можно отключить от центра данных и импортировать в другой центр данных в той же или другой среде. Затем виртуальные машины, "плавающие" виртуальные диски и шаблоны можно выгрузить из импортированного домена хранения в подключенный центр данных.

Виртуальные машины и шаблоны можно экспортировать или импортировать в центр данных в той же или другой среде zVirt. Экспорт и импорт выполняются с помощью домена экспорта, домена данных или хоста zVirt. При экспортировании или импортировании виртуальной машины или шаблона сохраняются свойства и основные сведения такие: имя и описание, выделение ресурсов и настройки высокой доступности виртуальной машины или шаблона.

Разрешения и роли пользователей виртуальных машин и шаблонов включены в OVF-файлы. Виртуальные машины и шаблоны могут быть импортированы со своими изначальными

разрешениями и ролями пользователей, когда домен хранения отключается от одного центра данных и подключается к другому. Чтобы разрешения были успешно зарегистрированы, пользователи и роли, связанные с разрешениями виртуальных машин или шаблонов, должны существовать в центре данных до начала процесса регистрации.

Функцию V2V можно использовать для импорта виртуальных машин от других провайдеров сервисов виртуализации (Xen или VMware) или импорта виртуальных машин Windows. Функция V2V преобразует виртуальные машины, обеспечивая возможность их размещения на хостах zVirt.

Виртуальные машины необходимо выключить перед импортированием.

12.1. Экспортирование виртуальной машины в домен экспорта

Экспортируйте виртуальную машину в домен экспорта, для импорта в другой центр данных. Сначала обязательно убедитесь, что домен экспорта подключен к центру данных, в котором находится экспортируемая виртуальная машина.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите ⋮ и затем **[Экспорт в экспорт-домен (Export to Export Domain)]**.
3. При желании установите следующие флажки в окне **Экспорт ВМ (Export Virtual Machine)**:
    - **Перезаписать принудительно (Force Override)**: перезаписывает существующие образы виртуальной машины в домене экспорта.
    - **Свернуть снимки (Collapse Snapshots)**: создает единый том экспорта на каждый диск. Эта функция удаляет точки для восстановления с моментальных снимков и добавленные шаблоны в виртуальную машину, созданную на базе шаблона, а также удаляет любые зависимости виртуальной машины от шаблона. Если виртуальная машина зависела от шаблона:
        - выберите эту функцию и экспортируйте шаблон вместе с виртуальной машиной;
        - либо убедитесь, что шаблон являющемся приемником, существует в центре данных.

Создавая виртуальную машину из шаблона через **Ресурсы (Compute) > Шаблоны (Templates)** и **Новая ВМ (New VM)**, появится две опции выделения хранилища в разделе **Тип диска (Storage Allocation)** на вкладке **Выделение ресурсов (Resource Allocation)**:

- Если выбрана опция **Клонированный (Clone)**, то виртуальная машина не зависит от шаблона. Шаблон не обязательно должен существовать в центре данных, являющемся приемником.
- Если выбрана опция **Тонкий (Thin)**, то виртуальная машина зависит от шаблона, поэтому шаблон должен существовать в центре данных, являющемся приемником, или быть экспортирован с виртуальной машиной. Либо установите флажок **Свернуть снимки (Collapse Snapshots)**, чтобы свернуть диск шаблона и виртуальный диск в единый диск.

Чтобы посмотреть, какая опция была выбрана, нажмите на имя виртуальной машины и откройте вкладку **Общие (General)** в подробном представлении.

4. Нажмите **[OK]**.

Начнется экспорт виртуальной машины. Во время экспортирования виртуальная машина отображается в **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** в состоянии **Образ заблокирован (Image Locked)** 🔏. Процесс может длиться до часа в зависимости от размера образов жесткого диска виртуальной машины и оборудования хранилища. Откройте вкладку **События (Events)** для просмотра прогресса. После завершения процесса виртуальная машина экспортирована в домен экспорта и и будет отображена на вкладке **Импортировать ВМ (VM Import)** подробного представления домена экспорта.

12.2. Экспортирование виртуальной машины в домен данных

Виртуальную машину можно экспортировать в домен данных для хранения клона виртуальной машины в качестве резервной копии.

При экспортировании виртуальной машины, зависимой от шаблона, в целевом домене хранения должен быть этот шаблон.

При создании виртуальной машины из шаблона через **Ресурсы (Compute) > Шаблоны (Templates)** и **Новая ВМ (New VM)**, на вкладке **Выделение ресурсов (Resource Allocation)** в разделе **Тип диска (Storage Allocation)** появятся две опции выделения хранилища :

- Если выбрана опция **Клонированный (Clone)**, то виртуальная машина не зависит от шаблона. Шаблон не обязательно должен существовать в центре данных, являющемся приемником.
- Если выбрана опция **Тонкий (Thin)**, то виртуальная машина зависит от шаблона, поэтому шаблон должен существовать в центре данных, являющемся приемником, или быть экспортирован с виртуальной машиной. Либо установите флажок **Свернуть снимки (Collapse Snapshots)**, чтобы свернуть диск шаблона и виртуальный диск в единый диск.

Чтобы посмотреть, какая опция была выбрана, нажмите на имя виртуальной машины и откройте вкладку **Общие (General)** в подробном представлении.

Предварительные условия:

- Домен данных подключен к центру данных.
- Виртуальная машина выключена.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Экспортировать (Export)]**.
3. Укажите имя экспортируемой виртуальной машины.
4. Выберите **Домен хранения (Storage domain)** из списка.
    - При желании установите флажок **Свернуть снимки (Collapse snapshots)**, чтобы экспортировать виртуальную машину без моментальных снимков.
5. Нажмите **[OK]**.

Менеджер управления клонирует виртуальную машину, включая все ее диски, в целевой домен.

При перемещении диска из домена данных одного типа в домен данных другого формат диска меняется соответственно. Например, если диск в домене данных NFS и в формате динамического выделения/Тонкий (thin) перемещается в домен iSCSI, то его формат поменяется на предварительно размеченный. Процедура отличается от использования домена экспорта, так как домен экспорта имеет тип NFS.

Во время экспортирования виртуальная машина отображается в состоянии **Образ заблокирован (Image Locked)**  . Процесс может длиться до часа в зависимости от размера образов жесткого диска виртуальной машины и оборудования хранилища. Откройте вкладку `События (Events)` для просмотра прогресса. По завершении процесса виртуальная машина экспортирована в домен данных и отобразится в списке виртуальных машин.

Дополнительные ресурсы:

- Создание виртуальной машины на основе шаблона.

12.3. Импортирование виртуальной машины из домена экспорта

В домене экспорта находится виртуальная машина. Прежде чем виртуальную машину можно будет импортировать в новый центр данных, домен экспорта должен быть подключен к центру данных, являющемуся приемником.

Порядок действий:

1. Нажмите **Хранилище (Storage)** > **Домены (Domains)** и выберите домен экспорта. У домена экспорта должно быть состояние **Активный (Active)**.
2. Нажмите на имя домена экспорта, чтобы перейти к его подробному представлению.
3. Откройте вкладку **Импортировать ВМ (VM Import)**, чтобы вывести список виртуальных машин, доступных для импорта.
4. Выберите одну или несколько виртуальных машин для импорта. При обнаружении в среде виртуализации виртуальных машин с такими же именами, одноимённые импортируемые виртуальные машины будут обозначены значком ⚠️ рядом с именем. Введите уникальные имена для каждой из них.
5. Выберите **Целевой кластер (Target Cluster)**.
6. Установите флажок **Свернуть снимки (Collapse Snapshots)**, чтобы удалить точки для восстановления с моментальных снимков и добавить шаблоны в виртуальную машину, созданную на основе шаблона.
7. Нажмите на виртуальную машину, которую нужно импортировать, и откройте вложенную вкладку **Диски (Disks)**. На этой вкладке можно использовать выпадающие списки:
    - **Политика выделения (Allocation Policy)** — выделение пространства для диска, используемого виртуальной машиной: динамическое или предварительное. Также отображается значок, обозначающий, какой из дисков на импорт ведет себя как загрузочный диск для виртуальной машины.
    - **Домен хранения (Storage Domain)** — домен хранения на котором будет храниться диск.
8. Нажмите **[OK]** , чтобы импортировать виртуальные машины.

За одну операцию можно импортировать только виртуальные машины, у которых одна и та же архитектура. Если среди виртуальных машин, которые нужно импортировать, хотя бы у одной из них отличается архитектура, то появится предупреждение в котором система предложит изменить выбор, чтобы импортировались только виртуальные машины с одной и той же архитектурой.

12.4. Импортирование виртуальной машины из домена данных

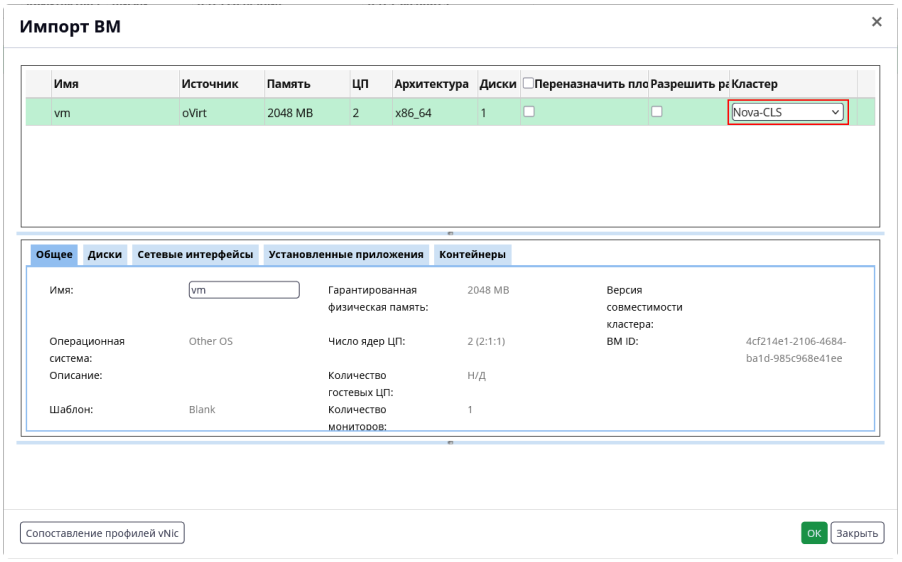
Виртуальную машину можно импортировать в один или несколько кластеров из домена хранения данных.

Предварительное условие:

- Домен хранения данных, из которого импортируется виртуальная машина, должен быть подключен к центру данных и активирован.

Порядок действий:

1. Нажмите **Хранилище (Storage)** > **Домены (Domains)**.
2. Нажмите на имя импортированного домена хранения, чтобы открыть его подробное представление.
3. Откройте вкладку **Импортировать ВМ (VM Import)**.
4. Выберите одну или несколько виртуальных машин для импорта. При обнаружении в среде виртуализации виртуальных машин с такими же именами, одноимённые импортируемые виртуальные машины будут обозначены значком ⚠ рядом с именем. Введите уникальные имена для каждой из них.
5. При обнаружении конфликта с MAC-адресом появится восклицательный знак ⚠ рядом с именем виртуальной машины. Наведите указатель мыши на значок для просмотра подсказки, которая отображает тип возникшей ошибки.
6. Убедитесь, что для каждой виртуальной машины в окне **Импорт ВМ (Import Virtual Machine(s))** в списке **Кластер (Cluster)** выбран правильный целевой кластер.



7. Сопоставьте внешние vNIC-профили виртуальных машин с профилями в целевом кластере (кластерах):
    a. Нажмите **[Сопоставление vNIC-профилей (vNic Profiles Mapping)]**.

b. Выберите vNIC-профиль в выпадающем списке **Целевой профиль vNIC (Target vNic Profile)**.

c. Если в окне **Импортировать виртуальную(ые) машину(ы) (Import Virtual Machine(s))** выбрано несколько целевых кластеров, то выберите каждый целевой кластер в выпадающем списке **Целевой кластер (Target Cluster)** и убедитесь в корректности сопоставления.

8. Нажмите **[OK]**.

> Если доступных адресов для переназначения нет, то выполнить операцию импортирования не удастся. Однако в случае с MAC-адресами, находящимися вне диапазона пула MAC-адресов кластера, виртуальную машину можно импортировать без повторного назначения нового MAC-адреса.

9. Нажмите **[OK]**.

12.5. Импортирование виртуальной машины из провайдера VMware

Во время импорта из провайдера VMware в процессе каждой операции импорта необходимо вводить данные в окне **Импорт ВМ (Import Virtual Machine(s))**. Или можно добавить провайдера VMware в качестве внешнего провайдера и выбрать предварительно сконфигурированного провайдера во время операций импорта.

zVirt использует инструмент v2v для импорта виртуальных машин VMware (предоставляется пакетом virt-v2v). Для файлов OVA zVirt поддерживает диски только в формате VMDK.

> При неудачной попытке импорта см. подробные сведения в соответствующем файле журналов **/var/log/vdsm/import/** и **/var/log/vdsm/vdsm.log** на прокси-хосте.

Предварительные условия:

- Как минимум один домен данных должен быть подключен к центру данных.

  > Мигрировать можно только в общие хранилища, например, NFS, iSCSI или FCP.
  > Локальные хранилища не поддерживаются.

- Файл образа **virtio-win_version.iso** для виртуальных машин Windows выгружен в домен хранения. Этот образ включает в себя гостевые инструменты, необходимые для миграции виртуальных машин Windows.
- Виртуальную машина выключена перед импортом. Запуск виртуальной машины VMware в процессе импорта может привести к повреждению данных.
- Импортировать можно только виртуальные машины с одинаковой архитектурой. Если среди виртуальных машин, которые нужно импортировать, хотя бы у одной из них

отличается архитектура, то появится предупреждение в котором система предложит изменить выбор, чтобы импортировались только виртуальные машины с одной и той же архитектурой.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)**.
2. Нажмите ⋮ и выберите **[Импортировать (Import)]**. Откроется окно **Импорт ВМ (Import Virtual Machine(s))**.
3. Выберите VMware из списка **Источник (Source)**.
    - Если провайдер VMware настроен в качестве внешнего провайдера, то выберите его из списка **Внешний провайдер (External Provider)**. Убедитесь, что учетные данные провайдера верны. Если при настройке внешнего провайдера вы не указали центр данных, являющийся приемником, или прокси-хост, то выберите эти параметры сейчас.
    - Если провайдер VMware еще не настроен или данные импортируются из нового провайдера VMware, введите следующую информацию:
        a. Выберите из списка **Центр данных (Data Center)**, в котором будет доступна виртуальная машина.
        b. Введите IP-адрес или FQDN экземпляра VMware vCenter в поле **vCenter**.
        c. Введите IP-адрес или FQDN хоста, из которого будут импортироваться виртуальные машины, в поле **ESXi**.
        d. Введите имя центра данных и кластера, в которых находится указанный хост ESXi, в поле **Центр данных (Data Center)**.
        e. Если происходил обмен SSL-сертификатом между хостом ESXi и Менеджером управления, то оставьте флажок **Проверка SSL-сертификата сервера** (Verify server's SSL certificate) установленным, чтобы проверять сертификат хоста ESXi. В противном случае снимите флажок.
        f. Введите **Имя пользователя (Username)** и **Пароль (Password)** для экземпляра VMware vCenter. Пользователь должен иметь доступ к центру данных VMware и хосту ESXi, на котором находятся виртуальные машины.
        g. Выберите хост в выбранном центре данных с установленным пакетом virt-v2v, который будет служить **Прокси-хостом (Proxy Host)** во время операций импорта виртуальных машин. Этот хост также должен быть способен подключаться к сети внешнего провайдера VMware vCenter.
4. Нажмите **[Загрузить (Load)]**, чтобы открыть список виртуальных машин на провайдере VMware, которые можно импортировать.
5. Выберите одну или несколько виртуальных машин из списка **Виртуальные машины на источнике (Virtual Machines on Source)** и с помощью стрелок переместите их в список

Виртуальные машины для импорта (Virtual Machines to Import). Нажмите **[Далее (Next)]**.

Если сетевое устройство виртуальной машины использует тип драйвера e1000 или rtl8139, то виртуальная машина будет использовать тот же тип драйвера после импорта в zVirt.

При необходимости после импорта можно вручную изменить тип драйвера на VirtIO. Сведения о том, как изменить тип драйвера после импорта виртуальной машины, см. в разделе Изменение сетевого интерфейса. Если сетевое устройство использует другой тип драйвера (не e1000 или rtl8139), то этот тип драйвера автоматически меняется на VirtIO во время импорта. Параметр **Подключить CD (Attach VirtIO-drivers)** позволяет внедрить драйверы VirtIO в файлы импортированной виртуальной машины, чтобы при смене драйвера на VirtIO операционная система правильно обнаружила устройство.

6. Выберите **Целевой кластер (Target Cluster)**, на котором будут находиться виртуальные машины.
7. Выберите **Профиль ЦП (CPU Profile)** для виртуальных машин.
8. Установите флажок **Свернуть снимки (Collapse Snapshots)**, чтобы убрать точки для восстановления с моментальных снимков и добавить шаблоны в виртуальные машины, созданные на основе шаблонов.
9. Установите флажок **Клонировать (Clone)**, чтобы изменить имена и MAC-адреса виртуальных машин, клонировать все диски и удалить все моментальные снимки. Если рядом с именем виртуальной машины появится знак предупреждения, необходимо клонировать виртуальную машину и изменить ее имя.
10. Нажмите на каждую виртуальную машину, которую хотите импортировать и в списках **Политика выделения (Allocation Policy)** и **Домен хранения (Storage Domain)** выберите, какой диск будет использовать виртуальная машина: с динамическим или предварительным выделением пространства, а также выберите домен хранения, на котором будет храниться диск. Кроме того, во вложенной вкладке **Диски (Disks)** можно посмотреть какой из импортируемых дисков является загрузочным для выбранной виртуальной машины.
11. Если установлен флажок **Клонировать (Clone)**, измените имя виртуальной машины на вложенной вкладке **Общее (General)**.
12. Нажмите **[OK]**, чтобы импортировать виртуальные машины.

Тип ЦП виртуальной машины должен совпадать с типом ЦП кластера, на который ее импортируют. Чтобы посмотреть Тип ЦП (CPU Type) кластера на Портале администрирования:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Выберите кластер.
3. Нажмите **[Изменить (Edit)]**.

4. Откройте вкладку **Общее (General)**.

Если тип ЦП виртуальной машины отличается, настройте тип ЦП импортируемой виртуальной машины:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Выберите виртуальную машину.
3. Нажмите **[Изменить (Edit)]**.
4. Откройте вкладку **Система (System)**.
5. Нажмите на стрелку **Дополнительные параметры (Advanced Parameters)**.
6. Выберите нужный тип ЦП из списка **Тип ЦП (Custom CPU)**.
7. Нажмите **[OK]**.

12.6. Экспортирование виртуальной машины на хост

Виртуальную машину можно экспортировать по конкретно заданному пути или в смонтированное общее NFS-хранилище на хосте в центре данных zVirt. В результате экспорта будет создан пакет открытого виртуального устройства (OVA).

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите Дополнительные действия ⋮, а затем **[Экспорт в OVA (Export as OVA)]**.
3. Выберите хост в выпадающем списке **Хост (Host)**.
4. Введите абсолютный путь к каталогу экспорта в поле **Путь (Directory)**, поставив в конце завершающий слэш. Например: **/images2/ova/**.
5. При желании можно изменить имя файла по умолчанию в поле **Имя (Name)**.
6. Нажмите **[OK]**.

Статус экспорта можно посмотреть во вкладке **События (Events)**.

12.7. Импортирование виртуальной машины из хоста

Импортируйте файл виртуальной машины OVA в среду zVirt. Файл можно импортировать из любого хоста zVirt в центре данных.

На текущий момент можно импортировать только файлы zVirt и OVA, созданные VMware. KVM и Xen не поддерживаются. Расположение файла может быть локальным каталогом или удаленным подключением NFS, если оно не находится в каталоге "/root" или подкаталогах. Убедитесь, что достаточно места для размещения файла. Процесс импорта использует `virt-v2v`.
Успешно импортировать можно только те виртуальные машины, которые работают на операционных системах, совместимых с `virt-v2v`.

Порядок действий:

1. Скопируйте файл OVA на хост на вашем кластере в расположение файловой системы, например, **/var/tmp**.
2. Убедитесь, что файл OVA имеет разрешения на чтение/запись для пользователя vdsm (UID 36) и группы kvm (GID 36) или установите владельцев:

   ```
   chown 36:36 path_to_OVA_file/file.OVA
   ```

3. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
4. Нажмите ⋮ и выберите **[Импортировать (Import)]**. Откроется окно **Импорт ВМ (Import Virtual Machine(s))**.
   a. Выберите **Virtual Appliance (OVA)** из списка **Источник (Source)**.
   b. Выберите хост в списке **Хост (Host)**.
   c. В поле **Путь (Path)** укажите абсолютный путь файла OVA.
   d. Нажмите **[Загрузить (Load)]**, чтобы открыть список виртуальных машин для импорта.
   e. Выберите виртуальную машину из списка **Виртуальные машины на источнике (Virtual Machines on Source)** и с помощью стрелки переместите ее в список **Виртуальные машины для импорта (Virtual Machines to Import)**.
5. Нажмите **[Далее (Next)]**.
   a. Выберите **Домен хранения (Storage Domain)** для виртуальной машины.
   b. Выберите **Целевой кластер (Target Cluster)**, на котором будут находиться виртуальные машины.
   c. Выберите **Профиль ЦП (CPU Profile)** для виртуальных машин.
   d. Выберите **Политику выделения (Allocation Policy)** для виртуальных машин.
   e. При желании можно установить флажок **Подключить CD (Attach VirtIO-drivers)** и выбрать подходящий образ из списка, чтобы добавить драйверы VirtIO.
   f. Выберите виртуальную машину и на вкладке **Общее (General)** выберите **Операционную систему (Operating System)**.
   g. На вкладке **Сетевые интерфейсы (Network Interfaces)** выберите **Имя сети (Network Name)** и **Имя профиля (Profile Name)**.

h. Откройте вкладку **Диски (Disks)**, чтобы посмотреть **Имя (Alias)**, **Виртуальный размер (Virtual Size)** и **Фактический размер (Actual Size)** виртуальной машины.

6. Нажмите **[OK]**.

12.8. Импортирование виртуальной машины из хоста KVM

zVirt конвертирует виртуальные машины хоста KVM в корректный формат перед их импортом. Необходимо включить аутентификацию по открытому ключу между хостом KVM и как минимум одним хостом в центре данных, являющимся приемником (этот хост в следующей процедуре называется прокси-хостом).

Виртуальную машину необходимо выключить перед импортом. Запуск виртуальной машины KVM в процессе импорта может привести к повреждению данных.

Импортировать можно только виртуальные машины с одинаковой архитектурой. Если у какой-либо импортируемой виртуальной машины другая архитектура, то появится предупреждение, и система предложит изменить выборку, чтобы в ней были только виртуальные машины с одинаковой архитектурой.

При неудачной попытке импорта см. подробные сведения в соответствующем файле журналов **/var/log/vdsm/import/** и **/var/log/vdsm/vdsm.log** на прокси-хосте.

Порядок действий:

1. Включите аутентификацию с открытым ключом между прокси-хостом и хостом KVM:

   a. Авторизуйтесь на прокси-хосте и сгенерируйте SSH-ключи для пользователя vdsm.

   ```
   sudo -u vdsm ssh-keygen
   ```

   b. Скопируйте открытый ключ пользователя vdsm на хост KVM. Файл `known_hosts` на прокси-хосте также обновится, и в нем появится хост-ключ хоста KVM.

   ```
   sudo -u vdsm ssh-copy-id root@kvmhost.example.com
   ```

   c. Авторизуйтесь на хосте KVM, чтобы убедиться, что вход в систему работает корректно.

   ```
   sudo -u vdsm ssh root@kvmhost.example.com
   ```

2. Авторизуйтесь на Портале администрирования.

3. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.

4. Нажмите ⋮ и выберите **[Импортировать (Import)]**. Откроется окно **Импорт ВМ (Import Virtual Machine(s))**.
5. Выберите **Центр данных (Data Center)**, на котором содержится прокси-хост.
6. Выберите **KVM (через Libvirt) (KVM (via Libvirt))** из выпадающего списка **Источник (Source)**.
7. При желании можно выбрать провайдер KVM из выпадающего списка **Внешний провайдер (External Provider)**. Корректный идентификатор URI будет уже проставлен. Дополнительные сведения см. в разделе Добавление хоста KVM в качестве провайдера виртуальных машин в **Руководстве администратора**.
8. Введите **URI** хоста KVM в следующем формате:

```
qemu+ssh://root@kvmhost.example.com/system
```

9. Оставьте флажок **Требуется авторизация (Requires Authentication)** установленным.
10. Введите `root` в поле **Имя пользователя (Username)**.
11. Введите **Пароль (Password)** пользователя *root* хоста KVM.
12. Выберите **Хост прокси (Proxy Host)** в выпадающем списке.
13. Нажмите **[Загрузить (Load)]**, чтобы открыть список виртуальных машин на хосте KVM, которые можно импортировать.
14. Выберите одну или несколько виртуальных машин из списка **Виртуальные машины на источнике (Virtual Machines on Source)** и с помощью стрелок ▶ и ◀ поместите их в список **Виртуальные машины для импорта (Virtual Machines to Import)**.
15. Нажмите **[Далее (Next)]**.
16. Выберите **Кластер (Cluster)**, на котором будут находиться виртуальные машины.
17. Выберите **Профиль ЦП (CPU Profile)** для виртуальных машин.
18. При желании установите флажок **Свернуть снимки (Collapse Snapshots)**, чтобы убрать точки для восстановления с моментальных снимков и добавить шаблоны в виртуальные машины, созданные на основе шаблонов.
19. При желании установите флажок **Клонировать (Clone)**, чтобы изменить имена и MAC-адреса виртуальных машин, клонировать все диски и удалить все моментальные снимки. Если рядом с именем виртуальной машины появится знак предупреждения ⚠ или в место для флажка в столбце **ВМ в системе (VM in System)**, необходимо клонировать виртуальную машину и изменить ее имя.
20. Нажмите на каждую виртуальную машину, которую хотите импортировать, и откройте вложенную вкладку **Диски (Disks)**. На этой вкладке можно использовать выпадающие списки:
    - **Политика выделения (Allocation Policy)** — выделение пространства для диска, используемого виртуальной машиной: динамическое или предварительное. Также

отображается значок, обозначающий, какой из дисков на импорт ведет себя как загрузочный диск для виртуальной машины.

- **Домен хранения (Storage Domain)** — домен хранения на котором будет храниться диск.

21. Если установлен флажок **Клонировать (Clone)**, измените имя виртуальной машины на вкладке **Общее (General)**.
22. Нажмите **[OK]**.

Тип ЦП виртуальной машины должен совпадать с типом ЦП кластера, на который ее импортируют. Чтобы посмотреть **Тип ЦП (CPU Type)** кластера на Портале администрирования:

1. Нажмите **Ресурсы (Compute)** > **Кластеры (Clusters)**.
2. Выберите кластер.
3. Нажмите **[Изменить (Edit)]**.
4. Откройте вкладку **Общее (General)**.

Если тип ЦП виртуальной машины отличается, настройте тип ЦП импортируемой виртуальной машины:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)**.
2. Выберите виртуальную машину.
3. Нажмите **[Изменить (Edit)]**.
4. Откройте вкладку **Система (System)**.
5. Нажмите на стрелку **Дополнительные параметры (Advanced Parameters)**.
6. Выберите нужный тип ЦП из списка **Тип ЦП (CPU Type)**.
7. Нажмите **[OK]**.

13. Миграция виртуальных машин между хостами

Живая миграция дает возможность перемещать работающую виртуальную машину между физическими хостами без прерывания на обслуживание. Виртуальная машина остается включенной, а пользовательские приложения продолжают работать, пока виртуальная машина перемещается на новый физический хост. Оперативная память виртуальной машины копируется в фоновом режиме с хоста-источника на хост-приемник. Хранилище и сетевое подключение при этом не меняются.

Виртуальную машину, которая использует виртуальный графический процессор (vGPU), нельзя переместить на другой хост.

13.1. Предварительные условия для живой миграции

Живая миграция используется для плавного перемещения виртуальных машин в рамках ряда типовых задач обслуживания. Среда zVirt должна быть заранее правильно настроена на поддержку живой миграции виртуальных машин. Для успешной живой миграции виртуальных машин должны быть выполнены как минимум следующие предварительные условия:

- Состояние хоста-источника и хоста-приемника: **Включено (Up)** .
- У хоста-источника и хоста-приемника есть доступ к одним и тем же виртуальным сетям и VLAN.
- У хоста-источника и хоста-приемника есть доступ к домену хранения данных, в котором находится виртуальная машина.
- Хост-источник и хост-приемник имеют ЦП одного производителя.
- Мощности ЦП хоста-приемника достаточно для обеспечения работы виртуальной машины.
- У хоста-приемника достаточно неиспользуемой оперативной памяти для обеспечения работы виртуальной машины.
- На перемещаемой виртуальной машине не установлено пользовательское свойство `viodiskcache` (вкладка **Доп. параметры** в окне создания/изменения ВМ).
- При наличии плавающих адресов у мигрируемой ВМ необходимо, чтобы кластер назначения был в составе SDN.

> Если кластер назначения имеет "Тип коммутатора" — "Мост", то миграция ВМ будет выполнена, но плавающий адрес не будет перенесен.

Живая миграция выполняется с помощью сети и предполагает передачу больших объемов данных между хостами. Одновременные миграции могут привести к перегрузке сети управления. Для достижения наилучшей производительности создайте отдельные логические сети для управления, хранения, отображения и миграции данных виртуальных машин, чтобы минимизировать риск перегрузки сети.

13.2. Настройка виртуальных машин с виртуальными сетевыми картами с включенным SR-IOV для уменьшения времени неработоспособности сети во время миграции

Виртуальные машины с виртуальными сетевыми картами, которые напрямую подключены к виртуальной функции сетевой карты хоста с включенным SR-IOV, можно дополнительно настроить для уменьшения времени неработоспособности сети во время живой миграции:

1. Убедитесь, что у хоста-приемника есть доступная виртуальная функция.
2. Установите параметры **Passthrough** и **Мигрируемый (Migratable)** в vNIC-профиле со сквозным доступом.
3. Включите горячее подключение для сетевого интерфейса виртуальной машины.
4. Убедитесь, что у виртуальной машины есть резервная виртуальная сетевая карта VirtIO в дополнение к виртуальной сетевой карте со сквозным доступом, чтобы поддерживать сетевое подключение виртуальной машины во время миграции.
5. Перед настройкой bond-интерфейса установите параметр виртуальной сетевой карты VirtIO **Без сетевых фильтров (No Network Filter)** . См. раздел Описание настроек в окне "Профиль интерфейса (Interface Profile)" в Руководстве по администрированию ресурсов zVirt.
6. Добавьте обе виртуальные сетевые карты в качестве ведомых в bond-интерфейс active-backup на виртуальной машине, при этом виртуальная сетевая карта со сквозным доступом будет основным интерфейсом.

   Профили bond-интерфейсов и виртуальных сетевых карт можно настроить одним из следующих способов:

   - На bond-интерфейсе не настроен `fail_over_mac=active`, а виртуальная функция виртуальной сетевой карты — **основной ведомый (slave)** (рекомендуется). Отключите фильтр спуфинга MAC-адресов в vNIC-профиле VirtIO, чтобы трафик, проходящий через виртуальную сетевую карту VirtIO, не отбрасывался из-за использования MAC-адреса виртуальной функции виртуальной сетевой карты.
   - На bond-интерфейсе настроено `fail_over_mac=active`. Такая политика обработки отказа гарантирует, что MAC-адрес bond-интерфейса всегда будет MAC-адресом активного ведомого. При обработке отказа MAC-адрес виртуальной машины меняется, что приводит к небольшому нарушению трафика.

13.3. Настройка виртуальных машин с виртуальными сетевыми картами с включенным SR-IOV и минимальным временем простоя

Чтобы настроить виртуальные машины для миграции с виртуальными сетевыми картами с включенным SR-IOV и минимальным временем простоя, следуйте описанной ниже процедуре.

Следующие шаги — это предварительная версия технологии, представленная только для оценки (Technology Preview).

1. Создайте vNIC-профиль с виртуальными сетевыми картами с включенным SR-IOV. См. Создание или изменение профилей vNIC и Установка и настройка SR-IOV в

руководстве администратора.

2. На Портале администрирования перейдите в раздел **Сеть (Network) > VNIC-профили (VNIC profiles)**, выберите vNIC-профиль, нажмите **[Изменить (Edit)]** и выберите **vNIC-профиль аварийного переключения (Failover vNIC profile)** из выпадающего списка.
3. Нажмите **[OK]**, чтобы сохранить настройки профиля.
4. Выполните горячее подключение сетевого интерфейса с созданным vNIC-профилем аварийного переключения к виртуальной машине или запустите виртуальную машину с подключенным сетевым интерфейсом.

> У виртуальной машины есть три сетевых интерфейса: интерфейс контроллера и два вспомогательных интерфейса. Интерфейс контроллера должен быть активным и подключенным, чтобы миграция прошла успешно.

5. Для автоматического развертывания виртуальных машин с такой конфигурацией используйте следующее правило `udev`:

```
SUBSYSTEM=="net",
ACTION=="add|change",
ENV{ID_NET_DRIVER}!="net_failover",
NM_UNMANAGED}="1",
RUN+="/bin/sh -c '/sbin/ip link set up $INTERFACE'"
```

   Это правило `udev` работает только в системах, которые управляют интерфейсами с помощью **Менеджера сети (NetworkManager)**. Это правило гарантирует, что активирован только интерфейс контроллера.

13.4. Автоматическая миграция виртуальных машин

Когда хост переводят в режим обслуживания, Менеджер управления автоматически инициирует живую миграцию для всех работающих на этом хосте виртуальных машин. Хост-приемник оценивается для каждой виртуальной машины по мере ее миграции, чтобы распределить нагрузку по кластеру. Однако для высокопроизводительных и/или закрепленных виртуальных машин появляется окно **Хост обслуживания (Maintenance Host)** с запросом подтвердить действие, поскольку производительность целевого хоста может быть ниже производительности текущего хоста.

Менеджер управления автоматически инициирует живую миграцию виртуальных машин для поддержания уровней балансировки нагрузки или энергосбережения в соответствии с политикой планирования. Укажите политику планирования, которая наилучшим образом отвечает потребностям вашей среды. При необходимости для конкретных виртуальных машин можно отключить автоматическую или даже ручную живую миграцию. Если виртуальные машины настроены на высокую производительность, и/или если они были закреплены (**Passthrough ЦП хоста (Pass-Through Host CPU)**, **Привязкой ЦП (CPU Pinning)**

или **Привязкой NUMA (NUMA Pinning)**), режим миграции установлен в значение **Разрешить только ручную миграцию (Allow manual migration only)**. Однако при необходимости его можно изменить на режим **Разрешить ручную и автоматическую миграцию(Allow manual and automatic migration)**. Следует соблюдать особую осторожность при изменении параметров миграции по умолчанию, чтобы не выполнить миграцию виртуальной машины на хост, который не поддерживает высокую производительность или закрепление.

13.5. Блокировка автоматической миграции виртуальной машины

В Менеджере управления можно отключить автоматическую миграцию виртуальных машин. Кроме того, можно отключить ручную миграцию виртуальных машин, настроив виртуальную машину так, чтобы она работала только на определенном хосте.

Возможность отключить автоматическую миграцию и обязать виртуальную машину работать на определенном хосте пригодится при использовании прикладных продуктов с признаком высокой доступности.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Хост (Host)**.
4. В разделе **Запустить на (Start Running On)** выберите **Любом хосте в кластере (Any Host in Cluster)** или **Указанном хосте (Specific Host(s))**, что позволяет выбрать несколько хостов.

   В режиме высокой доступности прямое назначение виртуальной машины конкретному хосту и отключение миграции взаимно исключают друг друга при работе zVirt.

   Если к виртуальной машине напрямую подключены устройства хоста, но указан другой хост, то устройства хоста предыдущего хоста будут автоматически удалены из виртуальной машины.

5. Выберите **Разрешить только ручную миграцию (Allow manual migration only)** или **Не разрешать миграцию (Do not allow migration)** в выпадающем списке **Параметры миграции (Migration Options)**.
6. Нажмите **[OK]**.

13.6. Ручная миграция виртуальных машин

Работающую виртуальную машину можно перенести на любой хост в центре данных без прерываний работы сервисов. Миграция виртуальных машин на другой хост особенно полезна при чрезмерной нагрузке на определенный хост. Предварительные условия для живой миграции см. в разделе Предварительные условия для живой миграции. У высокопроизводительных виртуальных машин и/или виртуальных машин с **Passthrough ЦП хоста (Pass-Through Host CPU)**, **Привязкой ЦП (CPU Pinning)** или **Привязкой NUMA (NUMA Pinning)**, режим миграции по умолчанию установлен в значение **Разрешить только ручную миграцию (Allow manual mirgation only)**. Выберите **Выбрать хост автоматически (Select Host Automatically)**, чтобы виртуальная машина мигрировала на хост с максимальной производительностью.

При переводе хоста в режим обслуживания виртуальные машины, работающие на этом хосте, автоматически переносятся на другие хосты в том же кластере. Переносить эти виртуальные машины вручную не требуется.

В zVirt 4.3 и выше для ручной миграции виртуальных машин используется визард миграции. Визард предоставляет следующие функции:

- Живая миграция только виртуальных машин между хостами в пределах одного центра данных.
- Миграция только дисков виртуальных машин между доменами хранения в пределах одного центра данных. (перед началом миграции внимательно изучите особенности миграции дисков.)
- Миграция виртуальных машин и их дисков в пределах одного центра данных.

Порядок действий:

1. Нажмите **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** и выберите одну или несколько работающих виртуальных машин.
2. В панели управления нажмите **[Мигрировать (Migrate)]**.
3. В открывшемся визарде:

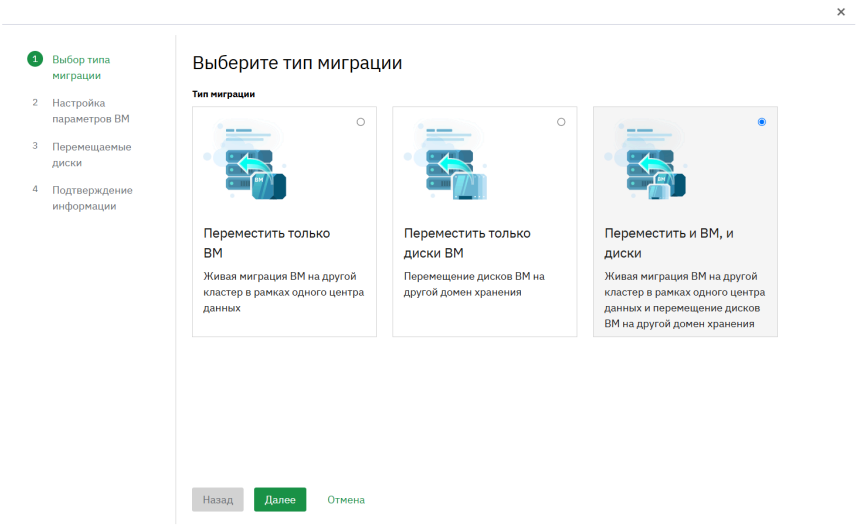
    a. Выберите тип миграции:

    Типы миграции **Переместить только диски ВМ** и **Переместить и ВМ, и диски** недоступны в случае:

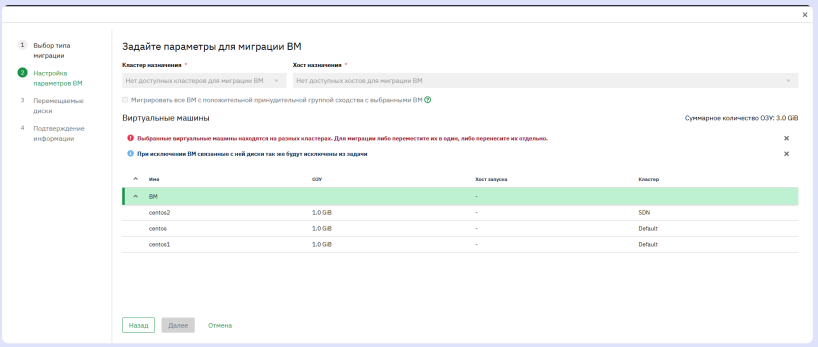
    - Если пользователь не имеет прав на домен хранения;
    - Если домен хранения в кластере один.

    - При необходимости перемещения только виртуальной машины на другой хост, выберите **Переместить только ВМ**.
    - При необходимости перемещения виртуальной машины на другой хост и её дисков в другой домен хранения, выберите **Переместить и ВМ, и диски**.



b. Нажмите **[Далее]** и на следующем этапе задайте параметры для миграции ВМ:

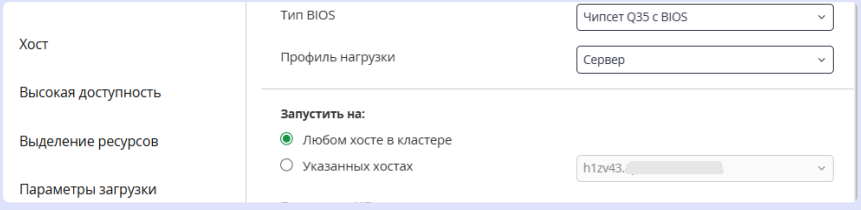
Если выбранные виртуальные машины находятся на разных кластерах, то для миграции переместите их в один кластер или переносите отдельно.



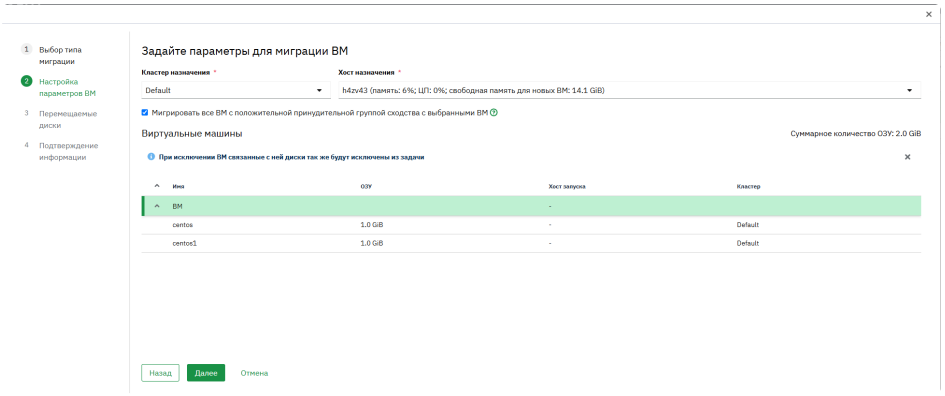
Для исключения ВМ из задачи на миграцию нажмите 🗑 в строке соответствующей ВМ.

- Укажите **кластер назначения**.

При выполнении миграции между кластерами настройка запуска ВМ на определенных хостах кластера сбрасывается на значение **"Любом хосте кластера"**.

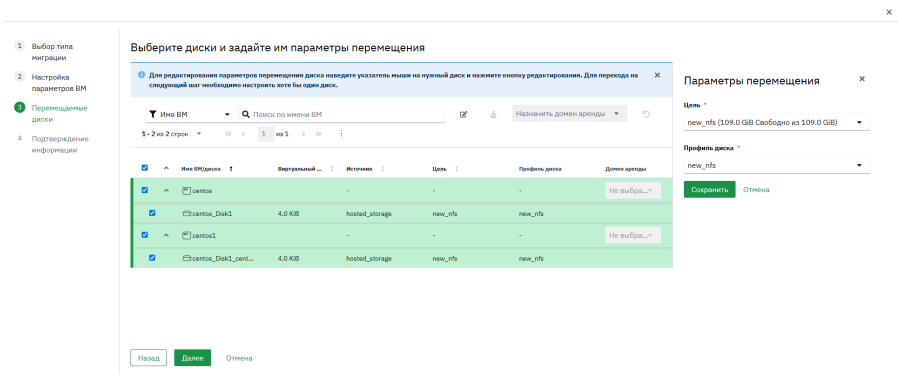


- Укажите **хост назначения**.
- Если необходимо **мигрировать все ВМ с положительной принудительной группой сходства с выбранными виртуальными машинами**, активируйте соответствующую опцию.
- Убедитесь, что список содержит все необходимые виртуальные машины.



a. Нажмите **[Далее]**. Если был выбран тип миграции **Переместить и ВМ, и диски**, на следующем этапе выберите необходимые диски и укажите параметры их перемещения:

   - При необходимости установите или измените домен аренды для высокодоступных виртуальных машин в столбце **Домен аренды**. Если необходимо назначить одинаковый домен аренды для всех выбранных виртуальных машин, воспользуйтесь соответствующим меню в верхней панели.
   - В строке нужного диска нажмите . Если целевой домен хранения и профиль одинаковый для нескольких дисков, выделите их и нажмите на в верхней панели.
   - В открывшейся панели укажите целевой домен хранения и профиль диска(ов). Нажмите **[Сохранить]**.



При наличии большого количества дисков, можно воспользоваться формой поиска в верхней панели. Она позволяет фильтровать диски по:

- Имени диска.
- Имени виртуальной машины.

Если заданы ошибочные параметры перемещения их можно удалить. Для этого нажмите в строке соответствующего диска или в верхней панели, предварительно выделив нужные диски.

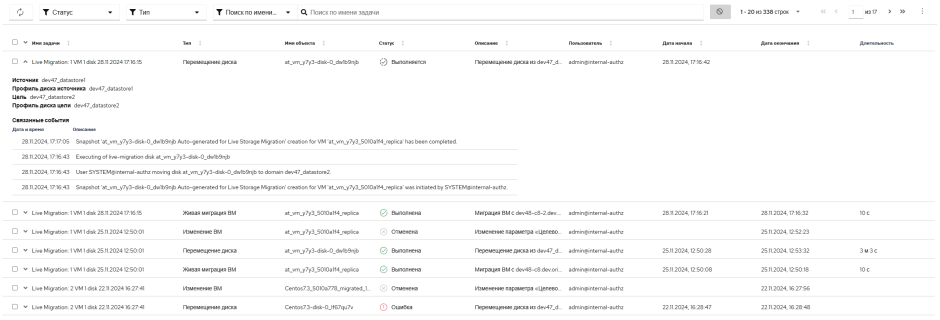
b. На этапе подтверждения информации убедитесь, что задание на миграцию содержит корректный список ВМ и/или дисков, для ВМ указаны правильные кластер и хост назначения, а для дисков целевой домен хранения и профиль.

c. Нажмите **[Мигрировать]**.

13.6.1. Мониторинг задач на миграцию

Для мониторинга созданных задач на миграцию используется страница **Управление › Задачи на миграцию**.

Страница содержит табличное представление списка операций, входящих в задачи на миграцию, с подробным описанием.



Каждая запись в списке содержит следующие параметры:

- **Имя задачи**: имя формируется автоматически исходя из типа и количества мигрируемых компонентов (диски/ВМ) и времени запуска процедуры миграции. В списке может присутствовать несколько записей с одинаковым именем. Это указывает на то, что записи описывают разные этапы одной задачи на миграции.
- **Тип**: тип задачи на миграцию. Возможны следующие значения:
  - **Живая миграция ВМ** — запись содержит сведения о миграции ВМ между хостами. Одна задача может содержать несколько записей такого типа, по одной записи на каждую мигрирующую ВМ.
  - **Перемещение диска** — запись содержит сведения о миграции диска между доменами хранения. Одна задача может содержать несколько записей такого типа, по одной записи на каждый мигрирующий диск.
  - **Изменение ВМ** — запись содержит сведения об изменении домена аренды ВМ. Одна задача может содержать несколько записей такого типа, по одной записи на каждую ВМ, для которой изменяется домен аренды.
- **Имя объекта**: содержит имя связанного объекта (диска/ВМ).
- **Статус**: указывает на статус операции. Возможны следующие значения:
  - **Выполнена** — операция успешно завершена.
  - **Отменена** — операция отменена пользователем.
  - **Ошибка** — операция завершилась ошибкой.
  - **Выполняется** — операция находится в стадии выполнения.
  - **Создана** — задание на выполнение создано, но операция еще не выполняется. На этом этапе операцию можно отменить (см. ниже).

- **Описание**: содержит подробное описание операции.
- **Пользователь**: указывает полное имя пользователя, который инициировал соответствующую задачу на миграцию.
- **Дата начала**: дата и время начала операции. Значение может быть пустым в случае отмены операции пользователем.
- **Дата окончания**: дата и время окончания операции.
- **Длительность**: длительность операции. Указывается только для операций со статусом **Выполнена**.

Каждая запись в таблице содержит подробное описание операции, а также список связанных событий. Для просмотра описания нажмите ⌄ в строке с нужной записью.

Информация в подробном описании зависит от типа операции:

- Для типа **Живая миграция ВМ**:
  - Кластер источник.
  - Хост источник.
  - Кластер назначения.
  - Хост назначения.
- Для типа **Перемещение диска**:
  - Домен хранения источник.
  - Профиль диска источник.
  - Целевой домен хранения.
  - Целевой профиль диска.
- Для типа **Изменение ВМ**:
  - Домен хранения для аренды ВМ источник.
  - Целевой домен хранения для аренды ВМ.

На странице просмотра задач на миграцию можно отменить операции, которые не начали выполняться. Для этого нажмите ⃠ в строке соответствующей записи или выделите несколько записей и нажмите на кнопку отмены в верхней панели.

Отмененные операции невозможно восстановить в очереди задач.

Для облегчения поиска нужных записей в верхней панели доступны различные способы фильтрации:

- По статусу операции.
- По типу операции.

- По имени задачи или объекта.

13.7. Настройка приоритета миграции

Менеджер управления ставит в очередь параллельные запросы на миграцию виртуальных машин с заданного хоста. Процесс балансировки нагрузки выполняется каждую минуту. Хосты, уже задействованные в миграции, не включаются в цикл миграции до тех пор, пока их событие миграции не завершится. Событие миграции запускается в соответствии с политикой балансировки нагрузки для кластера, когда в очереди есть запрос на миграцию, а в кластере доступные хосты для выполнения.

Порядок очереди миграции можно изменить, назначив приоритет каждой виртуальной машине. Например, установить, что критически важные виртуальные машины будут перенесены раньше других. Миграции будут упорядочены по приоритету: виртуальные машины с наивысшим приоритетом будут перенесены в первую очередь.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Высокая доступность (High Availability)**.
4. Выберите из выпадающего списка **Приоритет (Priority)** значение **Низкий (Low)**, **Средний (Medium)** или **Высокий (High)**.
5. Нажмите **[OK]**.

13.8. Настройка параллельных соединений для миграции

libvirt и QEMU позволяют использовать несколько параллельных соединений для одной миграции (QEMU называет эту функцию multifd). При наличии одного соединения для миграции и достаточной пропускной способности сети один поток миграции может стать узким местом из-за ограниченной мощности одного процессора. Чтобы использовать всю мощность сети, можно задействовать несколько соединений, которые обслуживаются несколькими потоками на нескольких процессорах. Например, 8-16 соединений могут задействовать пропускную способность сети 100 Гбит/с.

Кроме того, реализация передачи данных multifd проще и эффективнее, чем традиционный механизм миграции, и может работать быстрее даже при более низкой пропускной способности сети.

- Поскольку пропускную способность сети легче перегрузить несколькими соединениями, не рекомендуется одновременно переносить несколько виртуальных машин с одного хоста.
- Закрепление ЦП виртуальной машины может ограничить количество ЦП, доступных для процесса QEMU, и наложить ограничение на значимое количество параллельных соединений.
- Если указано одно соединение, то реализация параллельной миграции может быть недостаточно надежной. Рекомендуется всегда использовать как минимум два соединения. В худшем случае один из потоков будет простаивать, вызывая при этом лишь небольшие накладные расходы.

Параллельные миграции можно настроить как на уровне Кластера (**Изменить кластер** > **Политика миграции** > **Дополнительные свойства** > **Параллельные миграции**), так и на уровне ВМ (**Изменить/Новая ВМ** > **Хост** > **Параметры миграции** > **Параллельные миграции**). По умолчанию правила параллельных миграций наследуются виртуальными машинами от кластера. Установка необходимых правил на уровне ВМ, позволяет переопределить наследуемые параметры.

Таблица 3. Описание значений параметра "Параллельные миграции"

Значение	Описание
Auto	Использование параллельных соединений миграции и их количество определяется автоматически в зависимости от доступных ресурсов (пропускная способность сети и мощность процессора).
Auto Parallel	Параллельные соединения миграции используются всегда. Количество соединений определяется автоматически в зависимости от доступных ресурсов (пропускная способность сети и мощность процессора).
Disabled (значение по умолчанию для кластеров)	Параллельные соединения миграции не используются.
Custom	Параллельные соединения миграции используются всегда. Количество соединений устанавливается пользователем в поле **Количество соединений ВМ миграций**. Минимальное количество соединений — `2`. Максимальное количество — `255`, но не рекомендуется использовать более `16`. Фактическое количество соединений, используемых для конкретной миграции, ограничивается количеством потоков на исходном и целевом хостах и определяется меньшим значением количества потоков.
Использовать кластер по умолчанию (только в окне создание/редактирование ВМ)	Использовать параллельные соединения, как указано в настройках кластера.

13.9. Миграция очень больших виртуальных машин

В zVirt 4.0 появилась новая функция — миграция без копирования.

Миграция без копирования еще больше повышает скорость миграции и может позволить мигрировать большие виртуальные машины (более 1ТБ ОЗУ).

Для использования данной функции внедрена новая политика миграции — **Очень большие ВМ (Very large VMs)**.

Текущая реализация миграции без копирования в QEMU имеет некоторые ограничения:

- Её можно использовать только с параллельной миграцией.
- Её нельзя использовать с шифрованием миграции.
- Функция доступна только в кластере с версией совместимости **4.7**.
- Vdsm, libvirt и QEMU на хосте-источнике миграции должны поддерживать эту функцию.
- Это новая функция в QEMU/libvirt, которая может содержать ошибки. В данный момент рекомендуется использовать её, только если это действительно необходимо.

Для активации данной функции:

1. На портале администрирования перейдите в **Ресурсы > Кластеры**.
2. Выделите подходящий кластер (с версией совместимости **4.7**) и нажмите **[Изменить]**.
3. На вкладке **Политика миграции** в меню **Политика миграции** выберите *Очень большие ВМ (Very large VMs)*.
4. Настройте необходимые параметры для поддержки функции миграции без копирования:
    a. В дополнительных свойствах отключите шифрование при миграции.
    b. Настройте Параллельные миграции.
5. Нажмите **[OK]**.

Эта политика предназначена для очень больших виртуальных машин, для которых короткое время простоя может быть недостаточным. Политика устанавливает более длительное первоначальное время простоя.

Если эта политика выбрана, а вышеуказанные ограничения не соблюдены, то:

- Если параллельные миграции отключены или включены в режиме **Auto**, то они используются с автоматическим количеством параллельных соединений.
- Если включено шифрование при миграции, то функция миграции без копирования не работает.

Если политика выбрана, а хост не поддерживает эту функцию, то:

- Если Vdsm не поддерживает эту функцию, регистрируется несоответствие вызовов API и функция миграции без копирования не запускается.

Это возможно в том случае, если в конфигурации Менеджера были включены параллельные миграции (на уровне кластера), а хост, находящийся в кластере, не обновлен.

Во всех указанных случаях миграция ВМ продолжается, хотя и с разными параметрами.

13.10. Отмена начатых миграций виртуальных машин

Миграция виртуальной машины занимает больше времени, чем ожидалось. Прежде чем вносить какие-либо изменения в среду, проверьте, где запущены все виртуальные машины.

Порядок действий:

1. Выберите мигрирующую виртуальную машину. Она отображается в разделе **Ресурсы (Compute) > Виртуальные машины (Virtual Machines)** в состоянии **Миграция с (Migrating from)** и обозначается значком мигрирует .
2. Нажмите ⋮, затем — **[Отменить миграцию (Cancel Migration)]**.

Состояние виртуальной машины изменится со значения **Миграция с (Migrating from)** на значение **Работает (Up)** и значок .

13.11. Уведомление о событиях и журнале при автоматической миграции виртуальных серверов с признаком высокой доступности

Когда из-за присвоенного признака высокой доступности виртуальный сервер переносится автоматически, подробные сведения об автоматической миграции записываются на вкладке **События (Events)** и в журнале Менеджера в ВМ. Это помогает быстрее находить и исправлять ошибки. Ниже приведены примеры таких записей:

Пример 4. Уведомление на вкладке "События (Events)" на Портале администрирования

```
Highly Available Virtual_Machine_Name failed. It will be restarted
automatically.
Virtual_Machine_Name was restarted on Host Host_Name
```

Пример 5. Уведомление в журнале Менеджера управления engine.log

Этот журнал находится в Менеджере управления по пути `/var/log/ovirt-engine/engine.log` :

```
Failed to start Highly Available VM. Attempting to restart. VM Name:
Virtual_Machine_Name, VM Id:Virtual_Machine_ID_Number
```

14. Увеличение времени непрерывной работы с помощью высокой доступности виртуальной машины

14.1. Что такое высокая доступность?

Высокая доступность рекомендована для виртуальных машин, на которых запущены критически важные процессы. Виртуальная машина с признаком высокой доступности перезапускается автоматически в случае если процесс прерван: либо на своем изначальном хосте, либо на другом хосте в кластере. Например, перезапуск виртуальной машины может произойти в одной из следующих ситуаций:

- Хост перестает работать из-за отказа оборудования.
- Хост переведен в режим обслуживания на период плановой неработоспособности.
- Хост становится недоступен из-за потери связи с внешним хранилищем.

Виртуальная машина с признаком высокой доступности не перезапускается, если она была прямо выключена, например, как в следующих ситуациях:

- Виртуальная машина выключена с гостевой машины.
- Виртуальная машина выключена из Менеджера управления.
- Хост выключен администратором без предварительного перевода в режим обслуживания.

У виртуальных машин есть дополнительная возможность получить в аренду пространство на специальном томе хранилища, что позволяет виртуальной машине запуститься на другом хосте даже при отсутствии питания у изначального хоста. Функциональность также не позволяет виртуальной машине запуститься на двух разных хостах, что может привести к повреждению ее дисков.

В режиме высокой доступности перебои в работе сервиса минимальны, так как виртуальные машины перезапускаются в течение нескольких секунд без участия пользователя. В режиме высокой доступности сохраняется баланс ресурсов, так как гостевые машины запускаются на хосте с низким текущим потреблением ресурсов или в соответствии с настроенными политиками балансировки нагрузки или энергосбережения — таким образом, обеспечивается необходимая мощность, для перезапуска виртуальные машины в любой момент.

Высокая доступность и ошибки ввода/вывода хранилища

При возникновении ошибки ввода/вывода хранилища виртуальная машина приостанавливается. Можно настроить действия хоста с виртуальными машинами с признаком высокой доступности после того, как подключение к домену хранения будет восстановлено: хост может вновь их запустить, некорректно выключить (сбросить питание), или оставить на паузе.
Дополнительную информацию об этих опциях см. в разделе Описание настроек высокой доступности виртуальной машины.

14.2. Пояснения относительно высокой доступности

Для хоста с признаком высокой доступности требуется устройство управления питанием и параметры изоляции. Чтобы виртуальная машина работала в режиме высокой доступности, когда ее хост перестает работать, виртуальную машину нужно запустить на другом доступном хосте в кластере.

Чтобы обеспечить миграцию виртуальных машин с признаком высокой доступности:

- Для хостов, на которых работают виртуальные машины с признаком высокой доступности, должно быть настроено управление питанием.
- Хост, на котором работает виртуальная машина с признаком высокой доступности, должен входить в кластер, в котором есть и другие доступные хосты.
- Хост-приемник должен быть запущен.
- У хоста-источника и хоста-приемника должен быть доступ к домену данных, на котором находится виртуальная машина.
- У хоста-источника и хоста-приемника должен быть доступ к одним и тем же виртуальным сетям и сетям VLAN.
- На хосте-приемнике должно быть достаточно ресурсов ЦП, которые не используются для обеспечения работы виртуальной машины.
- На хосте-приемнике должен быть достаточный объем ОЗУ, который не используется для обеспечения работы виртуальной машины.

14.3. Конфигурирование виртуальной машины с признаком высокой доступности

Высокая доступность настраивается отдельно для каждой виртуальной машины.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.

2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Высокая доступность (High Availability)**.
4. Установите флажок **Высокая доступность (Highly Available)** для включения высокой доступности для виртуальной машины.
5. В выпадающем списке **Целевой домен хранения для аренды ВМ (Target Storage Domain for VM Lease)** выберите домен хранения для сохранения аренды виртуальной машины или выберите **Домен хранения не выбран (No VM Lease)**, чтобы отключить эту функциональность. Для получения дополнительной информации об аренде виртуальных машин см. раздел Что такое высокая доступность?.
6. В выпадающем списке **Действие (Resume Behavior)** выберите **Автовозобновление (Auto Resume)**, **Оставить на паузе (Leave Paused)** или **Принудительно завершить (Kill)**. Если указана аренда виртуальной машины, то единственная доступная опция - **Принудительно завершить (KILL)**. Дополнительную информацию см. в разделе Описание настроек высокой доступности виртуальной машины.
7. Из выпадающего списка **Приоритет (Priority)** выберите значение **Низкий (Low)**, **Средний (Medium)** или **Высокий (High)** . В момент инициации миграции создается очередь, согласно которой сначала переносятся виртуальные машины с высоким приоритетом. Если у кластера мало ресурсов, то переносятся только виртуальные машины с высоким приоритетом.
8. Нажмите **[OK]**.

15. Другие задачи, касающиеся виртуальных машин

15.1. Включение SAP-мониторинга

Включите SAP-мониторинг на виртуальной машине через Портал администрирования.

Порядок действий:

1. Нажмите **Ресурсы (Compute)** > **Виртуальные машины (Virtual Machines)** и выберите виртуальную машину.
2. Нажмите **[Изменить (Edit)]**.
3. Откройте вкладку **Доп. параметры (Custom Properties)**.
4. Выберите `sap_agent` из выпадающего списка. Убедитесь, что во вторичном выпадающем меню установлено значение **True**.

   Если свойства уже были заданы, выберите знак + для добавления нового правила свойства и выберите `sap_agent`.
5. Нажмите **[OK]**.

15.2. Конфигурирование виртуальных машин Linux на использование SPICE

SPICE — протокол подключения удаленного дисплея, предназначенный для виртуальных сред и позволяющий просматривать рабочее место или сервер виртуализации.

SPICE обеспечивает удобство использования, низкое потребление ресурсов ЦП и передача потокового видео в высоком качестве. Использование SPICE на машине, работающей на Linux, значительно улучшает перемещение курсора мыши по консоли виртуальной машины. Чтобы использовать SPICE, системе X-Windows требуются дополнительные QXL-драйверы. QXL-драйверы распространяются производителями дистрибутивов, на виртуальные машины с ОС семейства Red Hat Enterprise Linux QXL-драйверы устанавливаются по умолчанию. После установки SPICE на виртуальной машине, производительность графического интерфейса пользователя значительно увеличивается.

Как правило, наиболее полезной эта функция оказывается, когда нужно задействовать графический интерфейс пользователя. Системные администраторы, создающие виртуальные серверы, могут и не настраивать SPICE, если обращаются к графическому интерфейсу пользователя по минимуму.

15.3. Добавление устройства доверенного платформенного модуля (TPM)

Устройства доверенного платформенного модуля (TPM-устройства) предоставляют безопасный криптопроцессор, предназначенный для выполнения криптографических операций:

- генерирование криптографических ключей, случайных чисел и хэшей;
- хранение данных, которые можно использовать для безопасной проверки конфигураций ПО.

TPM-устройства обычно используются для шифрования дисков.

QEMU и libvirt реализуют совместимость с эмулируемыми TPM-устройствами версии 2.0.zVirt добавляет эмулируемое TPM-устройство на виртуальные машины.

После того, как эмулируемое TPM-устройство добавлено на виртуальную машину, его можно использовать в гостевой ОС как обычное TPM-устройство версии 2.0.

Если имеются TPM-данные, которые хранятся для виртуальной машины, а TPM-устройство отключено на виртуальной машине, то TPM-данные удаляются без возможности восстановления.

Порядок действий:

1. На экране **Новая виртуальная машина (New Virtual Machine)** или **Изменить виртуальную машину (Edit Virtual Machine)** нажмите **[Показать расширенные настройки (Show Advanced Options)]**.
2. На вкладке **Выделение ресурсов (Resource Allocation)** установите флажок **Включить TPM (TPM Device Enabled)**.

Применяются следующие ограничения:

- TPM-устройства можно использовать только на 64-разрядных машинах x86 с прошивкой UEFI.
- У виртуальных машин с TPM-устройствами не может быть моментальных снимков с состоянием памяти.
- Если Менеджер управления периодически извлекает и хранит TPM-данные, то нет гарантии, что у него всегда будет последняя версия TPM-данных.

  Процесс может занять 120 секунд и более, поэтому нужно дождаться окончания процесса, прежде чем работающую виртуальную машину можно будет клонировать, перенести или снять с нее моментальный снимок.

- TPM-устройства можно включить только на виртуальных машинах Linux с ядром 4.0 или более поздней версии и на Windows 8.1 или более поздней версии.
- Виртуальные машины и шаблоны с TPM-данными нельзя экспортировать или импортировать.