

BI.ZONE Secure SD-WAN

Руководство по установке CyberEdge VE

Введение

Данное руководство предназначено для пользователей решения BI.ZONE Secure SD-WAN и описывает процесс первичной установки и активации виртуальной машины CyberEdge VE.

CyberEdge VE представляет собой виртуальную реализацию оборудования CPE, предназначенное для непосредственной обработки трафика (маршрутизация, коммутация, реализация функций безопасности в виде VNF и других задач обработки трафика). В отличие от физических CPE, CyberEdge VE поддерживает работу на виртуализированной серверной инфраструктуре с одним из следующих гипервизоров:

- VMware ESXi версии 6.5 или выше. Примечание: для работы в более старых версиях может потребоваться кастомизация файла описания OVF-шаблона.
- QEMU/KVM.



Комплект поставки

CyberEdge VE в зависимости от типа гипервизора включает в себя:

1. Для гипервизора VMware:
 - а. Образ диска **VMDK** и файл описания **OVF**.
 - б. Альтернативно, файл **OVA**, включающий в себя комплект **VMDK** + **OVF**.
2. Для гипервизора QEMU — образ диска **QCOW2** и файл описания **XML**.



Минимальные требования к вычислительным ресурсам

Требования могут меняться, в зависимости от версии CyberEdge VE. На текущий момент предъявляются следующие минимальные требования:

- ЦПУ — 1 ядро.
- ОЗУ — 2 Гбайт.
- ПЗУ — 64 Гбайт.
- Сетевые интерфейсы — 2 шт.

В процессе работы CPE может потребоваться увеличение ресурсов, выделенных для данной виртуальной машины. Допускается изменения только числа ядер ЦПУ и количества ОЗУ, выделенного для виртуальной машины. Для изменения указанных параметров, виртуальную машину необходимо выключить. После повторного включения, CyberEdge VE самостоятельно определит новые оптимальные параметры работы. В случае, если было изменено количество ядер ЦПУ, то для применения новых настроек необходимо дополнительно выполнить еще один цикл перезагрузки данной виртуальной машины.

Допускаются следующие варианты настроек виртуальной машины с CyberEdge VE:

- ЦПУ: 1, 2, 4, 8 или 16 ядер на одном сокете (не более 1 сокета).
- ОЗУ: 2, 4, 8, 16 или 32 Гбайт (без привязки к числу ядер ЦПУ).

Требования, используемые по умолчанию для образа CyberEdge VE, возможно посмотреть в разделе `VirtualHardwareSection` соответствующего OVF-файла, открыв его в текстовом редакторе:

```
<VirtualHardwareSection ovf:transport="com.vmware.guestInfo">
  <Info>Virtual hardware requirements</Info>
  <System>
    <vssd:ElementName>Virtual Hardware Family</vssd:ElementName>
    <vssd:InstanceID>0</vssd:InstanceID>
    <vssd:VirtualSystemIdentifier>CyberEdgeVE</vssd:VirtualSystemIdentifier>
    <vssd:VirtualSystemType>vmx-13</vssd:VirtualSystemType>
  </System>
  <Item>
    <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
    <rasd:Description>Number of Virtual CPUs</rasd:Description>
    <rasd:ElementName>1 virtual CPU(s)</rasd:ElementName>
    <rasd:InstanceID>1</rasd:InstanceID>
    <rasd:ResourceType>3</rasd:ResourceType>
    <rasd:VirtualQuantity>1</rasd:VirtualQuantity>
  </Item>
  <Item>
    <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
    <rasd:Description>Memory Size</rasd:Description>
```



```
<rasd:ElementName>2048MB of memory</rasd:ElementName>  
<rasd:InstanceID>2</rasd:InstanceID>  
<rasd:ResourceType>4</rasd:ResourceType>  
<rasd:VirtualQuantity>2048</rasd:VirtualQuantity>  
</Item>
```



Предварительная подготовка

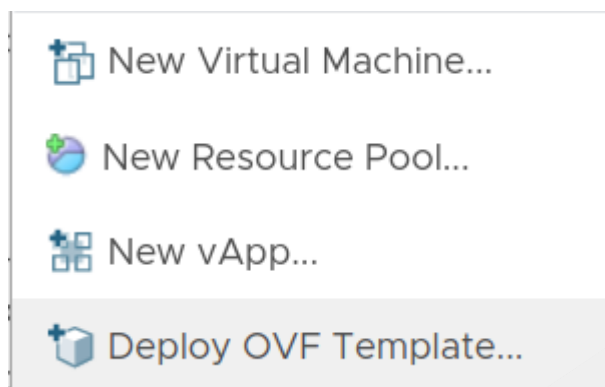
Ознакомьтесь со следующими предварительными рекомендациями для дальнейшей установки CyberEdge VE:

1. Если используемая система виртуализации предполагает ручное назначение IP-адресов, то при создании CPE в UI необходимо прописать IP-адрес как минимум на WAN-интерфейсе CPE. IP-адрес, длина маски и шлюз по умолчанию для WAN-интерфейса:
 - a. Для работы CyberEdge VE в сети интернет рекомендуется назначить публичный IP-адрес на WAN-интерфейс.
 - b. Допускается использование NAT совместно с использованием приватного IP-адреса на CyberEdge VE. При этом для CyberEdge VE в режиме Hub, NAT-правила должны быть статичны, то есть итоговый публичный адрес устройства не должен меняться. Для CyberEdge VE в режиме Spoke допускается использование любого типа NAT.
2. CyberEdge VE в режиме Hub подразумевает возможность устройству быть транзитным для других устройств SD-WAN сети, поэтому для работы в режиме Hub потребуется:
 - a. Канал связи с достаточной пропускной способностью.
 - b. Использование статических IP-адресов либо статической NAT-трансляции.
3. Сетевой доступ — в зависимости от режима работы CPE, необходимо разрешить несколько сетевых подключений к или от CPE.
4. Модель CyberEdge VE:
 - a. При создании CyberEdge VE с одним WAN-портом, необходимо использовать модель **CyberEdge VE (ESXI/QEMU/KVM, 2 ports) [Single WAN]**, при этом общее количество интерфейсов CyberEdge VE должно равняться двум (соответствует OVF-шаблону по умолчанию).
 - b. При необходимости подключения двух WAN-каналов к CPE, необходимо использовать модель **CyberEdge VE (ESXI/QEMU/KVM, 3 ports) [Dual WAN]**, при этом общее количество интерфейсов CyberEdge VE должно быть не менее 3.

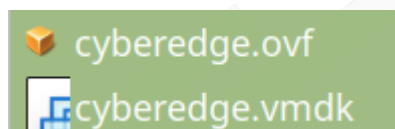
Запуск CyberEdge VE в гипервизоре VMware ESXI

Для запуска CyberEdge VE в гипервизоре VMware ESXI, необходимо выполнить следующие шаги:

1. Осуществите вход в систему управления **VMware vSphere** и выберите опцию установки новой виртуальной машины — **Deploy OVF Template**:



2. Выберите опцию **Local file** и укажите все файлы из комплекта поставки:



3. Укажите предпочитаемое имя виртуальной машины, локацию.
4. Выберите место и тип хранения диска виртуальной машины. Наиболее производительным считается режим **Thick Provision Eager Zeroed**, но он требует немного больше времени на создание:
 - a. **Thick Provision Lazy Zeroed** — всё пространство диска выделяется в момент создания, при этом блоки не очищаются от данных, которые находились там ранее. При первом обращении CyberEdge VE к этому блоку, он обнуляется.
 - b. **Thick Provision Eager Zeroed** — всё пространство диска выделяется в момент создания, при этом блоки очищаются от данных, которые находились там ранее. Далее происходит обычная работа с блоками без очистки.
 - c. **Thin Provision** — диски создаются минимального размера и растут по мере их наполнения данными до выделенного объема. При выделении нового блока — он предварительно очищается.
5. Подключите сетевые интерфейсы CyberEdge VE к сети. При этом к WAN-интерфейсу необходимо подключить внешнюю сеть, к LAN-интерфейсу — внутреннюю сеть:

Select networks

Select a destination network for each source network.

Source Network
WAN
LAN

- Если необходимо подключить к CyberEdge VE дополнительные внутренние сети, то их можно добавить в режиме **802.1Q Trunk** на LAN-интерфейсе.
- Если необходимо подключить к CyberEdge VE дополнительные внешние сети, рекомендуется запросить у производителя другой OVF-шаблон.

6. В заключительном окне введите ссылку активации и сертификата активируемого CyberEdge VE:

- Ссылка активации (**BZ_PROVISION_LINK**) может быть получена в UI Платформы по следующему пути: **Networking** → **Edge CPEs** → **Имя_CPE** → вкладка **General** → блок **Provision**.
- Ссылка с сертификатом (**BZ_CERTS_LINK**) может быть получена в UI Платформы по следующему пути: **Administration** → подраздел **CPE certificates**.

URL	2 settings
BZ_PROVISION_LINK	<input type="text"/>
BZ_CERTS_LINK	<input type="text"/>

7. После активации CyberEdge VE осуществите его запуск кнопкой **Power on** средствами VMware. После включения CyberEdge VE автоматически распознает ссылку активации, расшифрует ее и начнет процесс активации:

- При наличии связи с Платформой, активация завершится успешно, и дальнейшее управление будет осуществляться через UI.
- Если активация будет не успешной, CyberEdge VE вернется к стандартному способу активации и будет ждать ссылку активации на LAN-интерфейсе. Для повторной активации средствами VMware, выключите CyberEdge VE и при необходимости измените значение ссылки активации в настройках **vApp Options**, после чего повторно включите CyberEdge VE.

Запуск CyberEdge VE в гипервизоре QEMU/KVM

Запуск CyberEdge VE в гипервизоре QEMU/KVM производится в соответствии с XML-описанием.

Для запуска CyberEdge VE в гипервизоре QEMU/KVM, необходимо выполнить следующие шаги:

1. Проверка зависимостей (опционально).
2. Проверка сетевых настроек (опционально).
3. Запуск CyberEdge VE.
4. Активация CyberEdge VE.

Проверка зависимостей (опционально)

Аппаратные зависимости. Процессор хост-системы должен поддерживать технологию аппаратного ускорения виртуализации Intel-VT или AMD-V. Следующая команда покажет количество ядер процессора, имеющих поддержку одной из данных технологий:

```
$ egrep -c '(vmx|svm)' /proc/cpuinfo\
```

Подсказка

В случае, если вывод команды показывает значение `0`, то возможности виртуализации не включены. Виртуализацию необходимо включить в настройках виртуальной машины, в случае ее использования или в BIOS (если машина физическая).

Программные зависимости. На хост-системе должен быть установлен следующий набор пакетов (наименования пакетов могут отличаться в зависимости от ОС хоста):

```
qemu-system-x86  
qemu-kvm  
libvirt-clients
```

Может потребоваться установка отдельным пакетом:

```
libvirt-daemon-system
```

Проверка сетевых настроек (опционально)

Поскольку CyberEdge VE является сетевым устройством, ему необходимо иметь хотя бы два интерфейса. В ОС Linux, сетевые интерфейсы виртуальных машин обычно подключают в виртуальные коммутаторы (мосты). Для корректного запуска CyberEdge VE, удостоверьтесь в возможности подключения двух интерфейсов CyberEdge VE в разные Linux-мосты (либо осуществить проброс в виртуальную машину физических портов сервера с использованием технологии SR-IOV).

По умолчанию, некоторые ОС уже имеют настройки для размещения сетевых интерфейсов для виртуальных машин QEMU. Например, для ОС «Ubuntu» настройки интерфейса по умолчанию можно найти в файле **default.xml** по следующему пути: `/etc/libvirt/qemu/networks/`.

При этом, управление виртуализацией QEMU/KVM зачастую осуществляется не напрямую, а с использованием одного или более слоев абстракции. Первым слоем абстракции является библиотека `libvirt` и ее CLI утилита `virsh`. Например, просмотр стандартных сетевых настроек среды виртуализации можно осуществить командами:

```
$ virsh net-list
$ virsh net-info default
```

При необходимости внесения изменений в сетевые настройки хоста, можно воспользоваться следующим шаблоном WAN-сети. Для этого нужно создать в директории `/etc/libvirt/qemu/networks/` файл **wan-net.xml** и прописать в нем следующее:

```
<network>
  <name>wan-net</name>
  <forward mode='nat'/>
  <bridge name='br-wan' stp='on' delay='0'/>
  <ip address='192.168.165.1' netmask='255.255.255.0'>
    <dhcp>
      <range start='192.168.165.100' end='192.168.165.200'/>
    </dhcp>
  </ip>
</network>
```

А также следующим шаблоном LAN-сети. Для этого нужно создать в директории `/etc/libvirt/qemu/networks/` файл **lan-net.xml** и прописать в нем следующее:

```
<network>
  <name>lan-net</name>
  <forward mode='route'/>
  <bridge name='br-lan' stp='off' delay='0'/>
```

```
<ip address='192.168.2.10' netmask='255.255.255.0'/>
</network>
```

Проверьте, что включен `ip forwarding` :

```
$ cat /proc/sys/net/ipv4/ip_forward # (1)!
```

1. если значение `0` , то `ip forwarding` не включен. Если значение `1` , то `ip forwarding` включен

В качестве `forward mode`, могут быть использованы следующие режимы:

- `nat` – подразумевает маршрутизацию трафика виртуальных машин в данной сети на уровне хоста, с последующей подменой IP-адреса исходной виртуальной машины на IP-адрес хоста;
- `route` – подразумевает маршрутизацию трафика виртуальных машин в данной сети на уровне хоста, без изменения IP-заголовков (при этом требуется, чтобы в сети был обратный маршрут на внутреннюю подсеть хоста);
- `bridge` – подразумевает коммутацию трафика виртуальных машин в данной сети на уровне хоста (может потребовать дополнительных настроек на хосте);
- `hostdev` – подразумевает передачу SR-IOV сетевой карты в виртуальную машину напрямую.

Произведите перезагрузку:

```
$ sudo systemctl restart libvirtd
```

Для создания данных сетей из файла, выполните следующие команды:

```
$ virsh net-define wan-net.xml
$ virsh net-define lan-net.xml
$ virsh net-start wan-net
$ virsh net-start lan-net
$ virsh net-autostart wan-net
$ virsh net-autostart lan-net
```

Определение виртуальной машины

Команда `define` загрузит файл с описанием параметров запуска виртуальной машины и создаст ее конфигурацию, но не запустит саму виртуальную машину:

```
$ virsh define cyberedge.xml
```

Настройка автозапуска виртуальной машины

Команда `autostart` настраивает виртуальную машину для автоматического запуска при загрузке хостовой системы:

```
$ virsh autostart cyberedge.xml
```

Запуск CyberEdge VE

В случае, если образ CyberEdge VE представлен в виде архива (имя архива должно быть – `cyberedge.qcow2.tar.gz`), его необходимо предварительно распаковать:

```
$ tar -xvzf cyberedge.qcow2.tar.gz  
$ sudo cp cyberedge.qcow2 /opt/  
$ cd /opt/
```

В случае, если имя архива или путь отличается от команды выше (прописано в **cyberedge.xml**), то нужно либо заменить в команде выше, либо в самом файле на имена, указанные ранее.

Запуск виртуальной машины производится следующей командой (файл с описанием параметров запуска (например: **cyberedge.xml**) присутствует в комплекте поставки):

```
$ virsh start cyberedge.xml # (1)
```

1. Команда `start` запускает виртуальную машину, которая была предварительно определена (`define`).

Активация CyberEdge VE

При использовании гипервизора QEMU, активация CyberEdge VE возможна только в режиме, аналогичном активации физического CPE, то есть через отправку ссылки активации на LAN-интерфейс.

Ссылка активации должна быть получена с использованием UI. Основная рекомендация — получение ссылки в режиме **One-click CPE activation**.

Provision

☐ Verify settings on CPE before activation
 ☒ One-click CPE activation

Provision link

```

/z3pgXgdU1WZ2F0wm17V5Xe75XaFKUqz
/VGUXAKSEyNnA4j3mPfm4pSzMAXCPMRo5ThMudD6f8JOQqrye4r1th5RQGwckL1uCKX2ANDV1cS6fOtS59I5y
AU0ICIQ9T2oAGNRa0bt%2BcPty%2B8GLCfmmVDAg1fCytveS%2Bx3Mk6xjcaDdPQbzA0tNkhrFkHk6
/Kab3oMB72nq7ipS8RF3WS16%2BQ07QJ6%2BXRQ26Zj1doEBQWAT
/vh7WYU2g3Bqbtv9madhHppbEMW4ieypVAAreBAEL%2BUYij4OZOiwMwgHyPfCwvO1eZRk47e%2BM0ldFuDc
8a4YwFHPv5al/vQ9hZj0
/Hp1v04a52RXWMTBMrGKO1nlll5iehDUsSV3ZNRrXL1E%2BmNT4hdthbM2U8DsaMhUAvpQVBHplh3HPq6pln
Az2a2SLWPFITIBVoEOnb7VAPryeLbPhQgAYNuCQ60HrNgXjyBOeKZxNmgMDBU7g76IKm8n6t
/2a/Fsm31uKQ%2BeccFFsrqdZDA4qx2HrEXWB8sqEOeNbDMZEggnHHRp/ti5tbRH
/qkPm9Q0Mt8BcHA2oZMXkc8UTSty0pBqg1ONCHDlglWlUcmLNujk3GmMjplKBYElAxB6UUh31DMYkF0uqVNaq
G6hFytLhJfRA4vAz1AHYpNHgy7
/jf3MK6Pk0uFDEKqf4UvVP3fkhUDsraEVdvrMaxnqj35fU7bGLEfouWL8GQgaMIMXjIL3ZvRKkuQ%2B
/YUARfW5bAO8zgAmP10Cj41s%2BTKONjsLIH1XqnHm8xqPz6nvbEaWlo56TE3KJHT3
/OG4IMmkkdNmNz5zH1XOUD7oA/7JlmHmi7qYtDj6mpkV2VrDAfplBmPc

```

После получения ссылки активации, ее необходимо передать с хоста (гипервизора) на LAN-интерфейс CyberEdge VE с использованием, например, утилиты `curl` :

```
$ curl 'http://...'
```

Successfully store CPE configuration from URL. Starting to apply it...

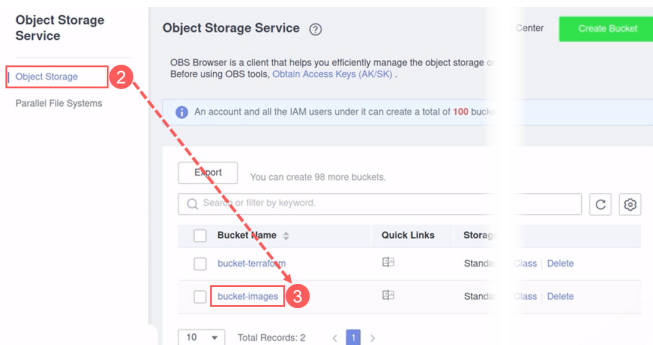
После перехвата ссылки активации, CyberEdge VE подключится к Платформе и далее будет управляться централизованно.



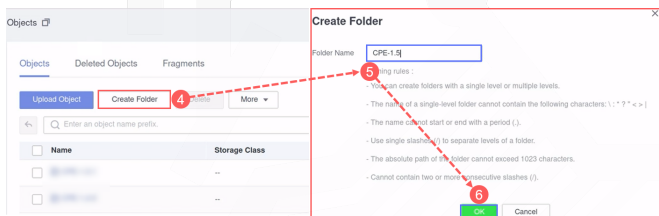
Запуск CyberEdge VE в Cloud.ru

Для запуска CyberEdge VE в Cloud.ru, необходимо выполнить следующие шаги:

1. Зайдите под своей учетной записью на портале cloud.ru.
2. Перейдите в раздел **Storage → Object Storage Service**.
3. Во вкладке **Object Storage**, в колонке **Bucket Name** выберите имя **bucket-images**.

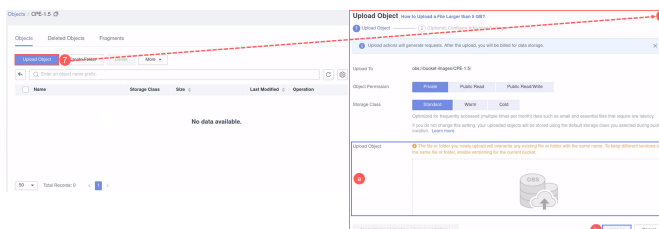


4. В окне **Objects** нажмите на кнопку **Create Folder** для создания директории, где будет храниться образ CyberEdge VE.
5. Опционально. В окне **Create Folder**, в поле **Folder Name** введите имя директории.
6. Опционально. Нажмите кнопку **OK** для создания директории.

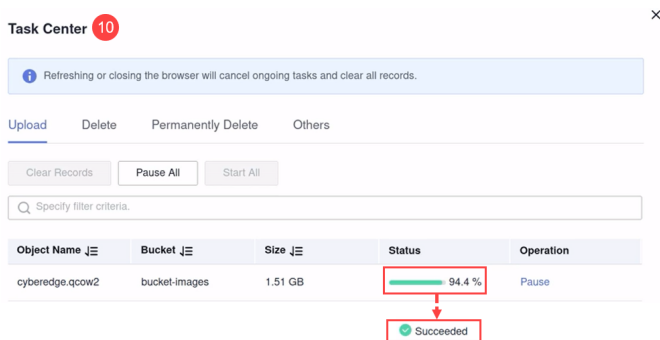


7. Опционально. Перейдите в созданную папку и нажмите на кнопку **Upload Object**.
8. В окне **Upload Object**:

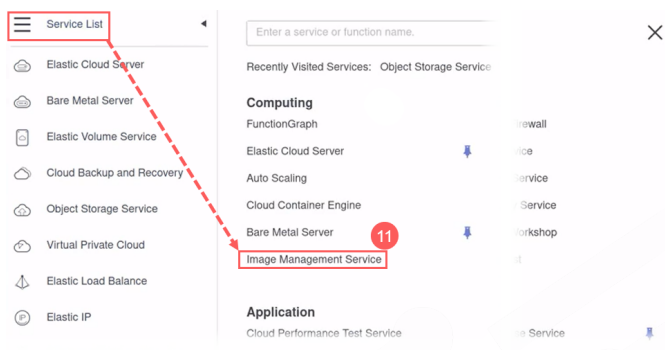
- a. В поле **Upload Object** перетащите файл в формате **.qcow2**.
- b. Нажмите на кнопку **Upload**.



9. Далее сбоку откроется окно **Task Center**, в котором нужно убедиться в том, что образ успешно загружен (колонка — **Status**, статус — **Succeeded**).



10. В боковом меню **Service List** выберите раздел **Image Management Service**.

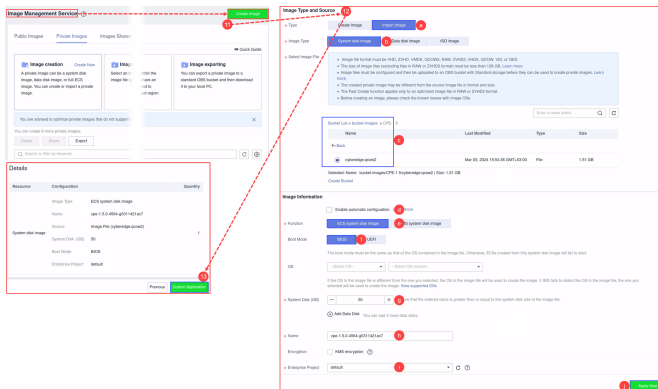


11. В окне **Image Management Service** нажмите на кнопку **Create Image**.

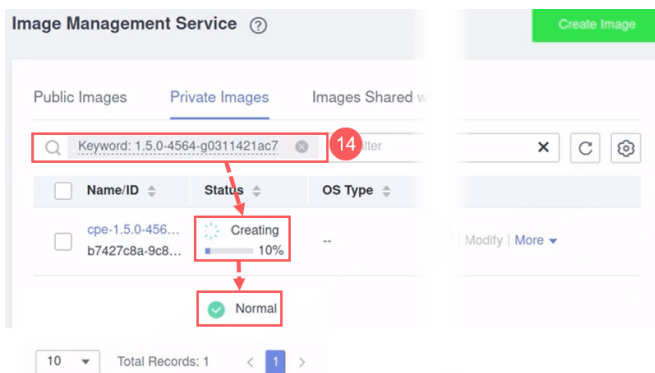
12. В окне **Image Type and Source** выполните следующую настройку:

- В поле **Type** выберите кнопку **Import image**.
- В поле **Image Type** выберите кнопку **System disk image**.
- В поле **Select Image File** выберите путь до файла в формате **.qcow2**, который был ранее загружен.
- В блоке **Image information** отключите флажок **Enable automatic configuration**.
- В поле **Function** выберите кнопку **ECS system disk image**.
- В поле **Boot Mode** выберите кнопку **BIOS**.
- В поле **System Disk (GB)** пропишите **50** Гбайт.
- В поле **Name** пропишите имя образа, например: **cpe-Y.Y.Y-XXX**.
- В поле **Enterprise Project** выберите значение **default**.
- Для применения настроек нажмите кнопку **Apply Now**.

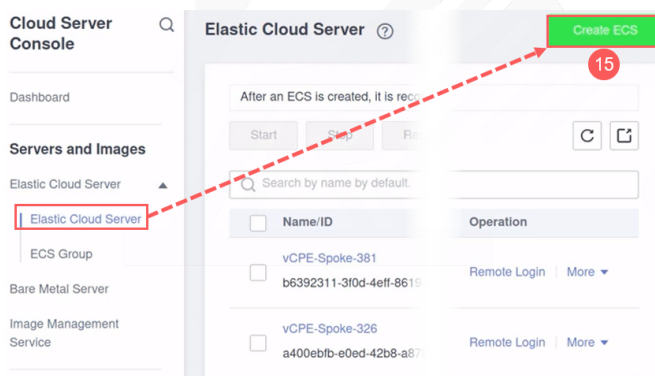
13. В окне **Details** убедитесь в том, что настройки выбраны верные. Нажмите кнопку **Submit Application**.



14. В окне **Image Management Service** в поисковой строке, введите имя образа. Дождитесь, когда он загрузится (👍 **Normal**).



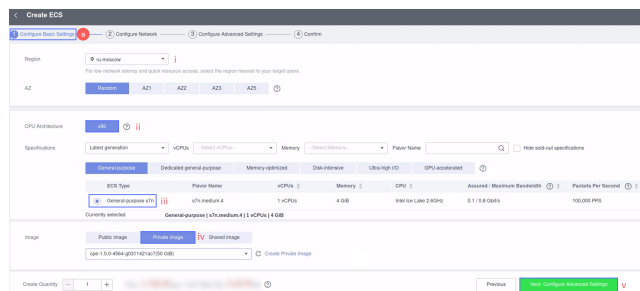
15. Выберите в боковом меню подраздел **Elastic Cloud Server**. Нажмите на кнопку **Create ECS**.



16. В окне **Create ECS**:

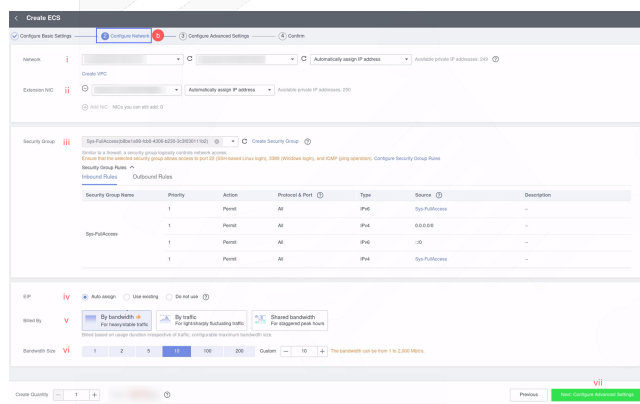
- Во вкладке **Configure Basic Settings**:
 - В поле **Region** выберите пункт **ru-moscow**.
 - В поле **CPU Architecture** выберите кнопку **x86**.
 - В поле **Specification** выберите тип Elastic Cloud Server — **General-purpose s7n**.
 - В поле **Image** выберите кнопку **Private Image**. В нем укажите ранее созданный образ.

v. Нажмите кнопку **Next: Configure Advanced Setting** , чтобы перейти на следующий шаг.



b. Во вкладке **Configure Network**:

- i. В поле **Network** укажите один или несколько IP-адресов VPC.
- ii. В поле **Extension NIC** укажите IP-адрес NIC.
- iii. В поле **Security Group** выберите набор правил контроля доступа к виртуальным машинам ECS.
- iv. В поле **EIP** выберите кнопку **Auto assign** .
- v. В поле **Billed By** выберите кнопку **By bandwidth** .
- vi. В поле **Bandwidth Size** выберите необходимую полосу обрабатываемого трафика.
- vii. Нажмите кнопку **Next: Configure Advanced Setting** , чтобы перейти на следующий шаг.



c. Во вкладке **Configure Advanced Setting**:

- i. В поле **ECS Name** введите имя CyberEdge VE которое ожидает активации в UI, например: **CPE-Hub-Moscow** .
- ii. В поле **Login Mode** выберите кнопку **Inherit Password From Image** .
- iii. В поле **Advanced Options** установите флажок **Configure now**.
- iv. В поле **User Data** выберите кнопку **As text** . В самом поле требуется все значения в одну строку, разделенные символом **;** , следующим образом:



BZ_CERTS_LINK=Ссылка_на_сертификат; BZ_PROVISION_LINK=Ссылка_активации . Для получения ссылок, пройдите в UI BI.ZONE Secure SD-WAN:

- i. Ссылка на сертификат (**BZ_CERTS_LINK**) может быть получена по следующему пути: **Administration** → подраздел **CPE certificates**.
- ii. Ссылка активации (**BZ_PROVISION_LINK**) может быть получена по следующему пути: **Networking** → **Edge CPEs** → **Имя_CPE** → вкладка **General** → блок **Provision**.

v. Нажмите кнопку **Next: Confirm** , чтобы перейти на следующий шаг.

d. Во вкладке **Confirm**:

- i. В блоке **Configuration** проверьте правильность выбранных настроек.
- ii. Во всплывающем списке **Enterprise Project** выберите пункт **default**.
- iii. Нажмите на кнопку **Apply Now** для подтверждения настроек.

17. После завершения установки, осуществите переход в UI BI.ZONE Secure SD-WAN и убедитесь, что vCPE имеет статус **⚡ ONLINE**.

Edge CPEs

+ Add		Delete								
	Name	Type	Stage	Status	Model	Version	VNFs			
<input type="checkbox"/>	ecs-14bc	SPOKE	✓ Operational	⚡ ONLINE	CyberEdge VE	1.5.1-188	firewall			

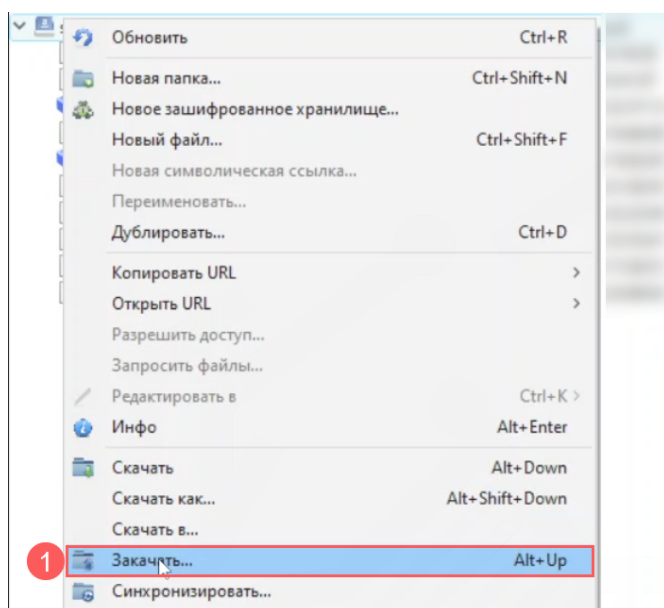
Запуск CyberEdge VE в Yandex Cloud

В процессе запуска CyberEdge VE в Yandex Cloud будет использоваться ПО «Cyberduck» версии 8.8.0. С другими совместимыми клиентами для работы с Yandex Cloud возможно ознакомиться на сайте [Yandex Cloud](#).

Настройка ПО «Cyberduck» выполняется в соответствии с рекомендациями изготовителя: [ссылка](#).

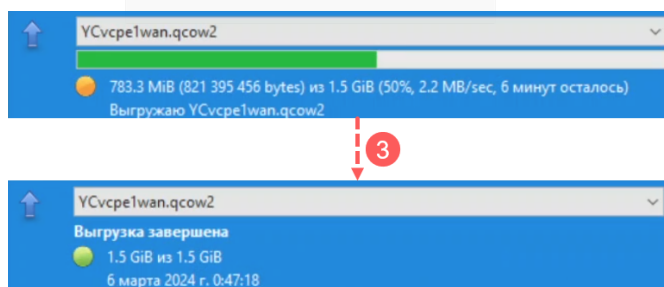
Для запуска CyberEdge VE в Yandex Cloud, необходимо выполнить следующие шаги:

1. Нажмите правой кнопкой на соединение с бакетом и выберите пункт **Закачать....**

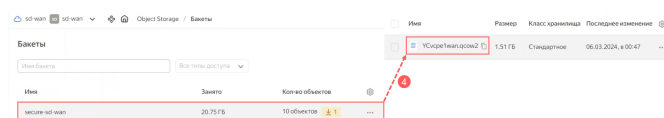


2. В диалоговом окне выгрузки выберите файл с образом диска .qcow2.

3. Дождитесь выгрузки образа диска.



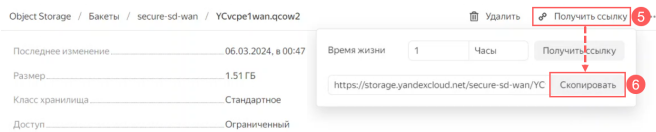
4. В Yandex Cloud пройдите в **Object Storage** в раздел **Бакеты** и выберите бакет.



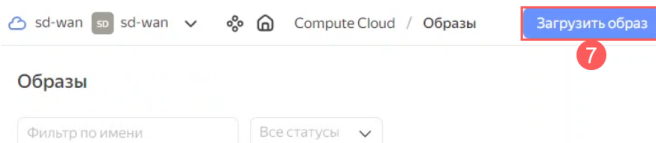


5. В окне просмотра параметров бакета нажмите на кнопку **Получить ссылку**.

6. В строке с ссылкой нажмите кнопку **Скопировать**.



7. Перейдите в **Compute Cloud** в раздел **Образы** и нажмите на кнопку **Загрузить образ**.

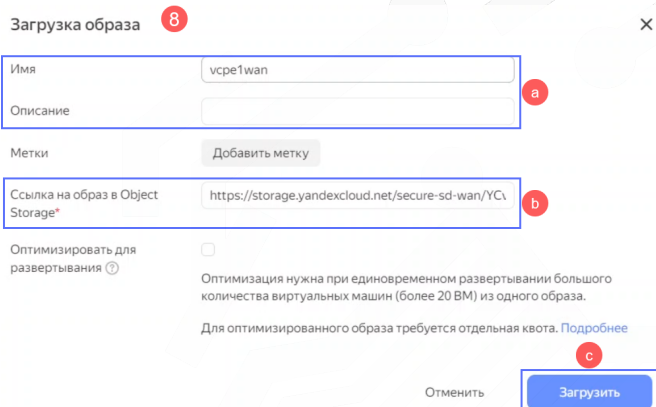


8. В окне **Загрузка образа**:

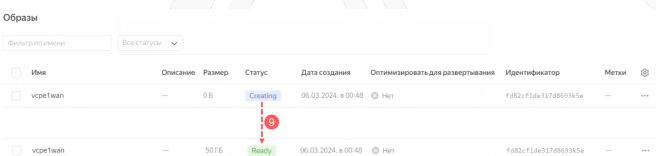
а. Введите имя образа и при необходимости описание.

б. Вставьте ранее скопированную ссылку в поле **Ссылка на образ в Object Storage**.

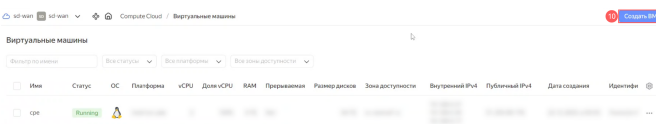
с. Нажмите кнопку **Загрузить**.



9. Дождитесь загрузки образа.



10. Перейдите в раздел **Виртуальные машины** и нажмите на кнопку **Создать VM**.



11. В окне **Создание виртуальной машины**:

а. В блоке **Базовые параметры** пропишите имя виртуальной машины и при необходимости другие поля.

- b. В блоке **Выбор образа/загрузочного диска** выберите вкладку **Свой образ** и в ней нажмите кнопку **Выбрать**.

Создание виртуальной машины ¹¹

Базовые параметры

Имя ¹ ^a


Описание ²

Зона доступности ³

Метки

Выбор образа/загрузочного диска

Операционные системы Container Solution Marketplace **Свой образ** ^b

 Выберите загрузочный диск

В качестве загрузочного диска может быть использован диск, снимок или образ.

- c. В окне **Выберите загрузочный диск** выберите вкладку **Образ**. В списке выберите ранее созданный образ и нажмите кнопку **Применить**.

Выберите загрузочный диск ^c

Диск Снимок **Образ**

Фильтр по имени

Имя	Размер	Дата создания
<input checked="" type="radio"/> vcp1wan	50 ГБ	06.03.2024, в 00:48

☒ Удалять вместе с VM [?]

- d. В блоке **Диски и файловые хранилища** определите параметры ПЗУ. Обязательно выберите тип диска SSD.

Диски и файловые хранилища

Диски 1 **Файловые хранилища**

disk-1709675335634 **Загрузочный** ^d

Тип ¹

Размер ²

Макс. IOPS ³ Чтение 2000 Запись 2000

Макс. bandwidth ⁴ Чтение 30 МБ/с Запись 30 МБ/с

Шифрование

Функциональность находится в стадии Preview. [Запросить доступ.](#)

- e. В блоке **Вычислительные ресурсы** определите параметры ЦПУ и ОЗУ. Обязательно для ОЗУ определите минимум 4 Гбайт памяти.

**Вычислительные ресурсы**

Платформа ⓘ Intel Ice Lake ▾

vCPU 2 2 96

Гарантированная доля vCPU ⓘ 20% 50% 100%

Для решения любых задач, в том числе для высоконагруженных сервисов.

RAM e 4 Гб 2 Гб 32 Гб

Дополнительно ☐ Прерываемая ⓘ

f. В блоке **Сетевые настройки** определите параметры сети:

- i. Для CyberEdge VE работающего в режиме Hub на основном интерфейсе требуется указать белый адрес.
- ii. Определите у дополнительных интерфейсов параметр **Публичный адрес** как **Без адреса**.
- iii. В зависимости от модели CyberEdge VE создайте один или два дополнительных интерфейса. При использовании CyberEdge VE с одним WAN-портом (**CyberEdge VE (ESXI/QEMU/KVM, 2 ports) [Single WAN]**) создайте один дополнительный интерфейс и он будет LAN. При использовании CyberEdge VE с двумя WAN-портами (**CyberEdge VE (ESXI/QEMU/KVM, 3 ports) [Dual WAN]**) создайте два интерфейса: первый созданный дополнительный интерфейс будет WAN, второй созданный дополнительный интерфейс будет LAN.

Сетевые настройки

Подсеть ⓘ default / default-ru-central1-a ▾ X

Публичный адрес Автоматически Список Без адреса

IP-адрес i [] ⓘ

Внутренний IPv4-адрес Автоматически Вручную

Настройки DNS для внутренних адресов ▾

Группы безопасности cpe-sg 1 ▾

Подсеть ⓘ default / default-ru-central1-a ▾ X

Публичный адрес Автоматически Список Без адреса ii

Внутренний IPv4-адрес Автоматически Вручную

Настройки DNS для внутренних адресов ▾

Группы безопасности cpe-sg 1 ▾

Добавить сетевой интерфейс iii

g. В блоке **Доступ**:

- i. В раскрывающемся списке **Сервисный аккаунт** выберите свой аккаунт.



ii. В поле **Логин** пропишите имя учетной записи.

iii. В поле **SSH-ключ** пропишите публичный ключ.

Доступ **g**

Сервисный аккаунт **i** или

Доступ через OS Login **PREVIEW** ☐ Разрешить

Логин* **ii**

SSH-ключ* **iii**

Дополнительно ☒ Разрешить доступ к серийной консоли **?**

h. В блоке **Метаданные**:

i. В поле **Ключ** пропишите значение `user-data`.

ii. В поле **Значение** пропишите ссылку на сертификат и ссылку активации. Значения требуется написать в одну строку, разделенные символом `;`, следующим образом: `BZ_CERTS_LINK=Ссылка_на_сертификат; BZ_PROVISION_LINK=Ссылка_активации`. Для получения ссылок, перейдите в UI BI.ZONE Secure SD-WAN:

i. Ссылка на сертификат (**BZ_CERTS_LINK**) может быть получена по следующему пути: **Administration** → подраздел **CPE certificates**.

ii. Ссылка активации (**BZ_PROVISION_LINK**) может быть получена по следующему пути: **Networking** → **Edge CPEs** → **Имя_CPE** → вкладка **General** → блок **Provision**.

Метаданные **h**

Настройки метаданных могут повлиять на работоспособность виртуальной машины. Меняйте их только если вы точно знаете, что хотите сделать.

Ключ	Значение
i user-data	ii <input type="text"/>

i. Нажмите кнопку .

12. После завершения установки, осуществите переход в UI BI.ZONE Secure SD-WAN и убедитесь, что CyberEdge VE имеет статус **⚡ ONLINE**.



Edge CPEs

+ Add

Delete

12

<input type="checkbox"/>	Name	Type	Stage	Status	Model	Version	VNFs
<input type="checkbox"/>	ecs-14bc	SPOKE	✓ Operational	🟢 ONLINE	CyberEdge VE	1.5.1-188	<div>🔗 firewall</div>

