



Российская сервисная платформа виртуализации РУСТЭК

Виртуальный РУСТЭК

Релиз 2.6

Оглавление

1 Развёртывание платформы РУСТЭК в виртуальной среде для организации вложенной виртуализации	3
1.1 Дисклеймер	3
1.2 Требования к среде виртуализации	3
1.2.1 Однородное оборудование	3
1.2.2 Поддержка аппаратной виртуализации	3
1.2.3 Достаточное количество ресурсов	3
1.2.4 Единые наборы инструкций	3
1.2.5 Уникальные VLAN	3
1.2.6 Jumbo frames	4
1.2.7 Согласованность MTU	4
1.2.8 Пропускная способность	4
1.2.9 Низкие задержки записи	4
1.2.10 «Смешанный» режим работы виртуальных коммутаторов	4
1.2.11 Особенности использования VMware vSphere	4
1.3 Ограничения	4
1.3.1 HA не будет выключать вычислительные узлы через IPMI	4
1.3.2 Миграция и эвакуация при разных CPU	5
1.3.3 Клонирование узлов РУСТЭК	5
1.3.4 Уникальные vg_id	5
1.4 Пример конфигурации узла РУСТЭК для VMware vSphere	6
2 Размещение платформы РУСТЭК на платформе РУСТЭК	7
2.1 Подготовка	7
2.2 Создание образа	7
2.3 Подготовка сетевой части	7
2.3.1 Создание родительского порта	7
2.3.2 Создание дочернего порта	8
2.3.3 Создание trunk	8
2.3.4 Добавление дочернего порта	9
2.4 Создание VM	9
2.5 Безопасность портов, ограничения	9

1 Развёртывание платформы РУСТЭК в виртуальной среде для организации вложенной виртуализации

1.1 Дисклеймер

РУСТЭК – это платформа виртуализации оборудования. Это значит, что продукт предназначен для работы прежде всего на физических серверах с СХД. Работа в виртуальной среде не является целевым режимом работы, так как может быть нестабильна из-за влияния другой виртуальной инфраструктуры на этом же оборудовании. Поэтому использование вложенной виртуализации не допускается для промышленной эксплуатации, кроме ряда исключений с соблюдением условий. Например, для демонстрации функционала платформы РУСТЭК в ненагруженном режиме, для обучения работе с платформой РУСТЭК.

1.2 Требования к среде виртуализации

1.2.1 Однородное оборудование

При размещении виртуальных узлов платформы на более чем одном физическом сервере избегайте ситуаций, когда узлы РУСТЭК располагаются на хостах, значительно отличающихся друг от друга по характеристикам. Особенно это относится к CPU, сетевым адаптерам и НВА. Допустимо использовать разные процессоры в рамках одного поколения или сетевые устройства, обеспечивающие схожую пропускную способность и производительность.

1.2.2 Поддержка аппаратной виртуализации

Оборудование виртуальной машины, должно уметь транслировать поддержку аппаратной виртуализации в гостевую ОС.

1.2.3 Достаточное количество ресурсов

Каждая виртуальная машина стенда РУСТЭК должна соответствовать требованиям из официальной документации.

1.2.4 Единые наборы инструкций

Процессоры на хостах, на которых могут располагаться узлы РУСТЭК, должны поддерживать один и тот же набор инструкций. Для этого используйте либо процессоры одного поколения, как говорилось выше, либо технологии типа VMware EVC™ Mode, ограничивающих наборы инструкций процессоров в кластере по минимальному.

1.2.5 Уникальные VLAN

Для менеджмент-сети каждой инсталляции РУСТЭК должен быть выделен отдельный VLAN.

Строго не рекомендуется:

- размещать в одном VLAN несколько инсталляций РУСТЭК;
- использовать одинаковые диапазоны VLAN для внутренних сетей РУСТЭК для разных инсталляций.

1.2.6 Jumbo frames

На всём сетевом оборудовании, объединяющем физические сервера в кластер виртуализации, как физическом, так и виртуальном, должны быть включены Jumbo frames.

1.2.7 Согласованность MTU

При настройке Jumbo frames можно столкнуться с тем, что оборудование по-разному считает размер Jumbo-кадра. Важно соблюдать согласованность на всех уровнях и не допускать ситуаций «бутылочного горлышка».

1.2.8 Пропускная способность

Как и любая информационная система, РУСТЭК работает тем лучше, чем выше скорость передачи информации между его узлами. Рекомендуется использовать сети не ниже 10 Gb/s для сетей передачи данных и не ниже 16 Gbit/s для сетей хранения данных, если используется протокол FibreChannel.

1.2.9 Низкие задержки записи

Доступ к системе хранения данных, на которой лежат диски узлов РУСТЭК, должен быть быстрым: ≤ 20 ms при стандартном блоке в 16 Kb.

1.2.10 «Смешанный» режим работы виртуальных коммутаторов

Все виртуальные коммутаторы, к которым подключены узлы платформы РУСТЭК, должны находиться в «смешанном» режиме работы (promiscuous mode) и поддерживать подмену MAC-адресов.

1.2.11 Особенности использования VMware vSphere

Особенности использования VMware vSphere:

- для всех виртуальных машин РУСТЭК должен быть настроен Custom Attribute `Disk.EnableUUID = True`;
- для всех физических хостов, на которых могут располагаться узлы РУСТЭК, специальный параметр `Net.ReversePathFwdCheckPromisc` должен быть выставлен в значение «1».

1.3 Ограничения

1.3.1 НА не будет выключать вычислительные узлы через IPMI

При установке на физические серверы РУСТЭК позволяет администратору настроить управление питанием вычислительных узлов через IPMI-интерфейсы серверов. В случае с виртуальными серверами это невозможно.

Способ решения: при инсталляции выключать в РУСТЭК.Конфигураторе опцию «Использовать IPMI» в меню «Настройки высокой доступности серверов» — тогда отказавшие узлы будут определять свою изоляцию сами и блокировать операционную систему через kernel panic.

1.3.2 Миграция и эвакуация при разных CPU

Если не соблюдено требование о едином наборе инструкций, вы можете столкнуться с ситуацией, когда не происходит миграция или эвакуация виртуальных машин между вычислительными узлами.

Способ решения: перезапуск вычислительных узлов РУСТЭК на физических хостах с одинаковыми процессорами. Чтобы избежать таких проблем, используйте одинаковые CPU, технологии унификации производительности или правила афинности для размещения всех узлов РУСТЭК на одном физическом сервере или на группе физических серверов, удовлетворяющих требованиям.

1.3.3 Клонирование узлов РУСТЭК

Не клонируйте виртуальные машины с установленной базовой ОС, чтобы увеличить количество узлов. Каждая операционная система обладает набором индивидуальных характеристик, помимо IP- и MAC-адресов, которые при клонировании не меняются. Клонирование VM с операционной системой приведёт к ошибкам при установке.

Способ решения: установка на каждую виртуальную машину своего собственного экземпляра базовой операционной системы РУСТЭК.

1.3.4 Уникальные `vr_id`

`vr_id` — это логическая сущность, целое натуральное число в диапазоне от 1 до 254, используется в качестве идентификатора виртуальных роутеров. В инсталляции РУСТЭК используется три `vr_id`: общий, для службы `cinder` и для службы `keystone`. В рамках одного VLAN, сколько бы инсталляций РУСТЭК в нём ни было, `vr_id` не должны повторяться, иначе могут возникнуть проблемы неясного генеза. `vr_id` настраиваются в файле `/var/lib/rustack-ansible/group_vars/all/user_vars/network.yml`.

Способ решения: размещать не более одной инсталляции РУСТЭК на один VLAN и вести учёт используемых `vr_id`.

1.4 Пример конфигурации узла РУСТЭК для VMware vSphere

VM Hardware ^

- ▼ CPU**

Utilization	32 CPU(s), 698 MHz used
Shares	8000 (Normal)
Reservation	0 MHz
Limit	Unlimited
Hardware virtualization	Enabled
IOMMU	Disabled
Performance counters	Disabled
- > Memory 32 GB, 2.32 GB memory active
- > Hard disk 1 350 GB
- > Network adapter 1 trunk_network (connected)
- ▼ Network adapter 2**

Adapter Type	VMXNET 3
MAC Address	00:50:56:8d:0a:7c
DirectPath I/O	Inactive
Network	trunk_network (connected)
- ▼ CD/DVD drive 1** ⊞ ▼

Connected to	Host image file
File	[distro] rustack-2021.2.4.iso
- > Video card 4 MB
- VMCI device Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
- ▼ Other**

Controllers	PCI controller 0 IDE 0 IDE 1 PS2 controller 0 SIO controller 0
SCSI Adapters	SCSI controller 0 (VMware paravirtual SCSI)
Input Devices	Keyboard Pointing device
Compatibility	ESXi 6.7 and later (VM version 14)

[Edit Settings...](#)

Custom Attributes ^

Attribute	Value
disk.EnableUUID	

1 items

[Edit...](#)

2 Размещение платформы РУСТЭК на платформе РУСТЭК

2.1 Подготовка

Для запуска VM на виртуальном РУСТЭК необходимо на родительском РУСТЭК включить **Nested Virtualization**. Для этого на всех физических узлах замените содержимое файла `/etc/modprobe.d/kvm.conf` на:

```
options kvm-intel nested=y
```

После этого перезагрузите модуль `kvm-intel` (⚠️ при этом на узле не должно быть запущенных VM) и проверьте, что параметр применился:

```
# rmmmod kvm-intel
# modprobe kvm-intel
# ca
t /sys/module/kvm_intel/parameters/nested
Y
```

2.2 Создание образа

Поддержка драйверов virtio появилась в РУСТЭК, начиная с версии 2021.2.5.

- Загрузить iso-образ РУСТЭК с параметрами:
 - контейнер — **bare**;
 - формат диска — **iso**;
 - размер диска, ГБ — **3**.
- Создать VM с диском iso-образа, после создания сразу выключить.
- Создать диск с размером не менее 20 ГБ и подключить его к созданной VM.
- Включить VM, установить ОС РУСТЭК и выключить VM.
- В портале в разделе **Диски** выбрать диск, на который была установлена ОС РУСТЭК, отключить его от VM и нажать на кнопку **Загрузить как образ** .

2.3 Подготовка сетевой части

Создайте trunk порт (trunk) для использования виртуальным узлом РУСТЭК. Также создайте один родительский порт и минимум один дочерний порт.

2.3.1 Создание родительского порта

Если нет сети и подсети, следует их создать (см. Руководство пользователя).

Родительский порт — порт, который нужно будет подключить к одному виртуальному узлу РУСТЭК. Родительский порт будет действовать как нетегированный интерфейс внутри VM.

Порядок создания родительского порта в портале РУСТЭК:

1. В разделе **Сеть** → **Порты** нажать кнопку **Создать**  на панели инструментов.
2. В форме **Создание порта** заполнить поля:
 - a. **Имя** – parent1;
 - b. **Подсеть** – выбрать подсеть subnetwork;
 - c. **Безопасность портов** – выключить чекбокс. Это нужно для возможности присваивания любого IP-адреса, в противном случае на VM необходимо будет указывать IP и MAC-адрес как в свойствах порта.;
Остальные поля оставить по умолчанию или заполнить (см. Руководство пользователя).
3. Нажать кнопку **Создать**.

Аналогично порт можно создать в разделе **Сеть** → **Подсети**, нажав на кнопку **Добавить порт**  на панели инструментов. (подробнее см. в Руководство пользователя).

2.3.2 Создание дочернего порта

Дочерний порт будет связан с trunk, который в свою очередь связан с родительским портом. Внутри VM необходимо создать VLAN-интерфейс с VID таким же как у дочернего порта.

Порядок создания дочернего порта в портале РУСТЭК:

1. В разделе **Сеть** → **Порты** нажать кнопку **Создать**  на панели инструментов.
2. В форме **Создание порта** заполнить поля:
 - a. **Имя** – subport1;
 - b. **Подсеть** – выбрать подсеть subnetwork;
 - c. **Безопасность портов** – выключить чекбокс;
Остальные поля оставить по умолчанию или заполнить.
3. Нажать кнопку **Создать**.

Таким же образом можно создать остальные дочерние порты.

2.3.3 Создание trunk

В Neutron VLAN trunk позволяет нескольким сетям подключаться к VM с помощью одного виртуального сетевого адаптера (vNIC).

Порядок создания trunk в портале РУСТЭК:

1. В разделе **Сеть** → **Trunk-порты** нажать кнопку **Создать**  на панели инструментов.
2. В форме **Создание trunk-порта** заполнить поля:
 - a. **Имя** – trunk1;
 - b. **Родительский порт** – выбрать порт parent1;
 - c. Остальные поля оставить по умолчанию или заполнить (см. Руководство пользователя).
3. Нажать кнопку **Создать**.

2.3.4 Добавление дочернего порта

Порядок добавления дочернего порта в портале РУСТЭК:

1. В разделе **Сеть** → **Trunk-порты** выбрать trunk1 и нажать кнопку  на панели инструментов.
2. В форме **Добавление дочернего порта** заполнить поля:
 - а. **Дочерний порт** – выбрать порт subport1;
 - б. **Тип сегментации** – выбрать VLAN;
 - с. **ID сегмента**– задать необходимое значение VLAN.
3. Нажать кнопку **Создать**.

Таким же образом можно добавить другие дочерние порты.

Поддерживается только тип сегментации VLAN (параметр `segmentation-type`).

2.4 Создание VM

Создайте VM согласно документу Руководство пользователя. В форме **Создание VM** вместо сети подключите порт.

2.5 Безопасность портов, ограничения

Строго не рекомендуется включать безопасность портов в следующих случаях:

- если на узлах виртуального РУСТЭК больше одного сетевого интерфейса, потому что при агрегации в bond сами интерфейсы и интерфейс bond меняют MAC-адрес на MAC-адрес первого сетевого интерфейса;
- при создании дочерних портов для создания сетей, поскольку виртуальный РУСТЭК сам выдаёт этим сетям IP-адреса.

В обоих вариантах сработает правило антиспуфинга и передача трафика заблокируется.

Обратите внимание:

- если в виртуальном РУСТЭК более одного узла, то для каждого узла создайте свой родительский и дочерние порты и trunk;
- при использовании для сети управления должен быть только один подключенный сетевой интерфейс, при этом у интерфейса `bond0.<VLAN ID>` MAC- и IP-адреса должны соответствовать указанному в свойствах порта. Их можно установить вручную через консоль операционной системы:

```
# ip link set dev bond0.<VLAN ID> address <yo:ur:ma:ca:dd:re:ss>
```