Business Services

Flexible Computing Advanced

Руководство пользователя

1. Введение

Цель настоящего руководства — продемонстрировать порядок выполнения первоначальных шагов и базовых операций на облачной платформе Orange Flexible Computing Advanced.

Более подробную информацию можно получить в руководстве пользователя Cloud Director Tenant Portal Guide.

Для обеспечения безопасности и функциональности платформы, Orange систематически производит установку патчей и обновлений для ПО платформы, что может приводить к изменениям в интерфейсе и появлению нового функционала, не описанного в данном документе. В случае возникновения вопросов рекомендуется обратиться в Orange или к документации VMware по нужной версии ПО.

Данная версия документа основана на Cloud Director версии 10.3.2.

2. Навигатор по опциям и возможностям

	Описание	Настройка
Базовый функционал		
Управление виртуальным ДЦ (vDC) через WEB-интерфейс	4, 5	12
Использование готовых и своих образов ВМ (ISO/vApp template)	9	
Управление виртуальными сетями	10	
Виртуальный firewall NSX Edge Gateway	3.11	
Аренда лицензий на ПО	3.14	
Внешние устройства		
Подключение внешних USB устройств (USB-to-IP)	3.17	
Подключение внешних сетевых устройств/серверов расположенных в ДЦ Orange	3.18	
Опции отказоустойчивости		
Архитектура платформы уровня Disaster Avoidance	3.1	
Резервирование ресурсов + приоритетный запуск ВМ в случае disaster	3.3	
Размещение дисков ВМ в двух ДЦ (синхронная репликация)	3.5	
Разнесение ВМ между ДЦ	3.3	
Сеть		
Отказоустойчивый доступ к сети Интернет (через два ДЦ, разные PE, разные последние мили)	3.10	11.3
Отказоустойчивый доступ к сети BVPN (через два ДЦ, разные PE, разные последние мили)		
Edge GW в режиме High Availability	3.11	11.8
Защита от DDoS-атак	3.13	
Storage		
Silver	3.5	12.8
Gold		
Platinum		
Platinum DR (синхронная репликация)		
Резервное копирование и архивирование		
Резервное копирование на массив в основном ДЦ	3.6	
Архивирование и восстановление на ленту	3.7	
Offsite хранение лент		

3. Архитектура, опции, особенности и рекомендации

3.1. Обзор архитектуры

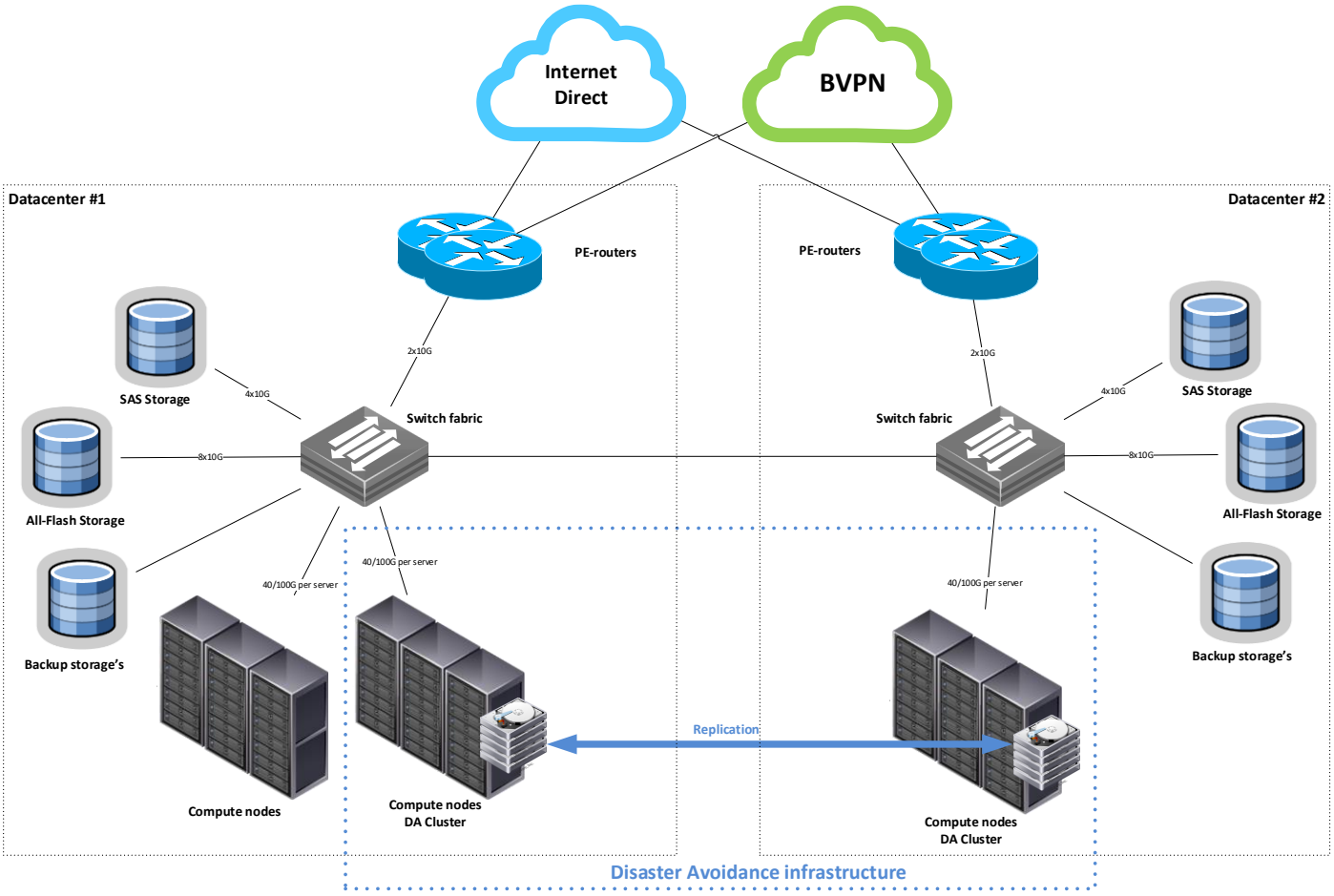
Основным принципом при построении инфраструктуры публичного облака для Orange является отказоустойчивость. Для этого применяется комплексный подход на всех уровнях:

- Основной дата-центр – IXcellerate Moscow One уровня Tier III+ (Москва, Алтуфьевское шоссе, 33Г);
- Второй дата-центр – DataLine Nord4 уровня Tier III (Москва, Коровинское шоссе, 41);
- Третий дата-центр – технический центр Orange «Петровка» (Москва, ул. Петровка, 15/13);
- Используется оборудование и ПО только промышленного класса от лидеров рынка: HPE, Juniper, Huawei, VMware, Netapp, Veeam, CheckPoint, ADVA;
- Постоянное поддержание и повышение экспертизы инженеров;
- DWDM-каналы между дата-центрами (далее ДЦ) проложены разными маршрутами по городу, входят в

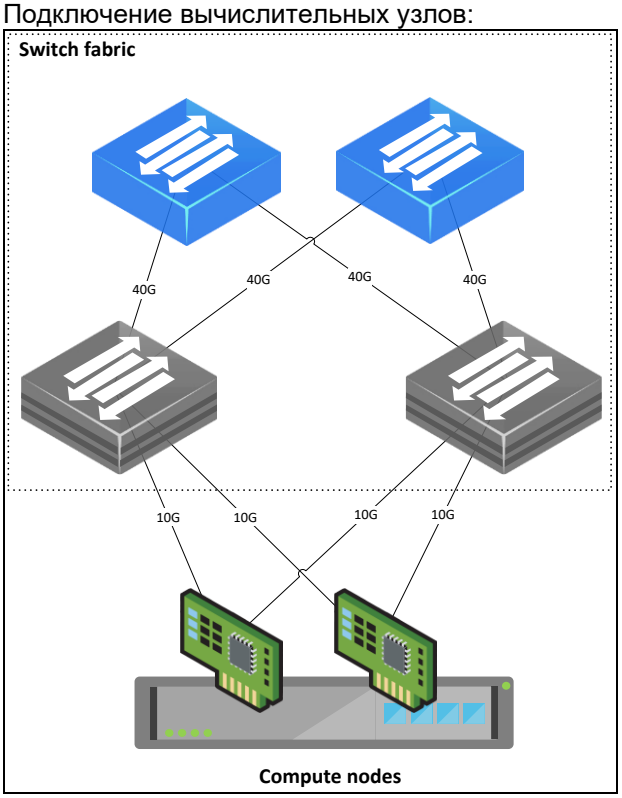
ДЦ через разные кабельные коллекторы, внутри ДЦ трассы также не пересекаются на уровне кабельных лотков, работают на двух наборах полностью независимого оборудования;

- Задержка передачи данных между ДЦ: 0,3-0,4мс при измерениях ВМ<>ВМ, т.е. включая все уровни;
- Все оборудование имеет минимум два блока питания и подключено к разным лучам питания;
- Все сетевые соединения между устройствами выполнены минимум двумя кабельными соединениями и терминируются на разных коммутаторах (MC-LAG);
- Для подключения серверов используются как минимум две физически разные многопортовые сетевые карты;
- Внешние сетевые сервисы (Internet Direct, BVPN) подаются с двух независимых PE-маршрутизаторов, расположенных в разных ДЦ по разным трассам;
- Все классические СХД имеют как минимум два контроллера и резервирование дисков с помощью RAID. SDS СХД DA-кластера помимо резервирования дисков внутри ДЦ хранит полную копию данных во втором ДЦ (при заказе опции DA);
- Используется физически выделенный отдельный кластер управления, построенный по технологии DA в двух ДЦ;
- Все критичные сервисы кластера управления зарезервированы на уровне приложений и разнесены между ДЦ;
- Круглосуточный мониторинг состояния оборудования и доступности сервиса.

Совокупность этих мер позволяет Orange гарантировать высочайший уровень доступности сервиса для конечного заказчика.
Общая схема:



Подключение вычислительных узлов:



Характеристики вычислительных узлов кластеров:

пп	CPU	RAM
1.0	2x E5-2680 v3 @ 2.50GHz (12C, Turbo Boost 3.30GHz, Haswell)	608-768 Gb
2.0	2x E5-2698 v4 @ 2.20GHz (20C, Turbo Boost 3.60GHz, Broadwell)	768 Gb
2.1	2x Xeon Gold 6248 @ 2.50GHz (20C, Turbo Boost 3.90GHz, Cascade Lake)	768 Gb
2.2	2x Xeon Gold 6248R @ 3.00GHz (24C, Turbo Boost 4.00GHz, Cascade Lake)	1536 Gb

Дисковая ёмкость уровней Silver, Gold и Platinum отличается параметрами IOPS на 1 ТБ: 112, 420 и 3000 соответственно. Реальные показатели IOPS зависят от параметров нагрузки и, как правило, больше указанных выше. При самостоятельном синтетическом тестировании производительности дисковой подсистемы необходимо учитывать, что на платформе применяются технологии оптимизации и кеширования, повышающие скорость работы реальных приложений, поэтому рекомендуется использовать тестовые пакеты, эмулирующие реальную нагрузку, и запускать их на время не менее 30 минут.

3.2. DA или DR? Показатели RTO и RPO

Для защиты от природных и техногенных катастроф или терактов и обеспечения непрерывности бизнес-процессов необходимо резервирование основных систем хранения и обработки данных. В случае катастрофы может пострадать здание центра обработки данных, поэтому для обеспечения непрерывности работы сервиса необходимо создание территориально удаленной площадки – резервного дата-центра. Давайте рассмотрим взаимосвязь между аварийным восстановлением (Disaster Recovery, DR) и предотвращением катастроф (Disaster Avoidance, DA) для современного виртуального дата-центра.

В чем разница между предотвращением катастроф и аварийным восстановлением?
Катастрофы могут быть вызваны природными причинами, такими как землетрясение или ураган, они могут быть вызваны несчастным случаем, например, пожаром, а также могут быть искусственными, такими как военные действия или терроризм. Но в каждом случае катастрофа является незапланированным событием, которое неизбежно нарушает работу основного виртуального дата-центра.

Понятие **аварийного восстановления** касается стратегии, используемой для минимизации последствий сбоев и восстановления критически важных бизнес-функций после катастрофы. Стратегия аварийного восстановления обычно включает в себя определение параметров RPO (максимальный период времени, за который могут быть потеряны данные) и RTO (промежуток времени, в течение которого система может оставаться недоступной), а также аппаратное обеспечение, программное обеспечение и методы, необходимые для достижения этих целей.

Например, традиционный план аварийного восстановления может состоять в том, чтобы восстановить пять ключевых бизнес-приложений до нормальной функциональности в течение 60 минут после события катастрофы (это RTO), теряя при этом только до 10 минут данных (RPO). Фактические RPO и RTO будут зависеть от ваших конкретных потребностей бизнеса и соответствующих инвестиций в оборудование, программное обеспечение и персонал. Организации с *множеством* критически важных приложений в условиях коротких требований RPO и RTO обычно должны инвестировать значительно больше в инфраструктуру аппаратного и программного обеспечения для достижения этих целей по сравнению с бизнесом с *несколькими* важными приложениями и более мягкими требованиями RTO/RPO. Простым примером аварийного восстановления (DR) является восстановление резервных копий, где серверы перезагружаются из последнего набора резервных копий, сохраненного на локальных или удаленных СХД.

Для сравнения, стратегия **предотвращения катастроф** (DA) - это усилия, направленные в первую очередь на *предотвращение* сбоев, связанных с катастрофами. DA – это устойчивость, а не только восстановление – т.е. поддержание доступности приложений в свете предсказуемых сбоев. Простым примером предотвращения катастроф является миграция виртуальной машины. Например, виртуальные машины могут быть перенесены на другие хост-сервера, чтобы можно было произвести обслуживание или обновление исходного хост-сервера, что предотвращает аппаратные сбои (небольшие катастрофы). Точно так же, если вы знаете, что ураган опускается на ваш основной центр обработки данных, можно перенести рабочую нагрузку на серверы в другом ДЦ до тех пор, пока не пройдет шторм и не будет произведен ремонт.

Ключевым соображением в обоих примерах является «предсказуемость» катастрофы. Часто невозможно осуществить или экономически не выгодно планировать защиту от всех возможных катастроф, поэтому при планировании всегда стремятся защитить бизнес от наиболее вероятных ситуаций.

Что лучше: DR или DA?
Технологии аварийного восстановления (DR) обычно предлагают самые разнообразные варианты развертывания и ценовые диапазоны и обычно используются организациями, которые могут терпеть некоторый уровень сбоя рабочей нагрузки или потери данных. Тем не менее, восстановление необходимо периодически проверять и практиковать, чтобы гарантировать, что оно работает должным образом - регулярные тренировки минимизируют задержки восстановления, вызванные человеческой ошибкой или неопытными сотрудниками.

В случае когда бизнесу критичен простой сервисов даже в течение 1 минуты необходимо рассматривать вариант с предотвращением катастроф (DA), который является наиболее агрессивной формой готовности к стихийным бедствиям. В данном случае требуется совместное использование нескольких центров обработки данных для распределения вычислительных ресурсов, что повышает не только отказоустойчивость, но и стоимость решения. Поскольку все центры обработки данных постоянно работают, ИТ-персонал регулярно работает со всем оборудованием, и ИТ-администраторы остаются в курсе параметров работы систем.

Поэтому конечный выбор стратегии защиты от катастроф должен основываться на потребностях бизнеса (таких как RTO и RPO) и требованиях соответствия нормативным актам, а не на технологической доступности. Бизнес, который просто не может позволить себе быть оффлайн должен выбирать DA, в то время как менее требовательный бизнес может потенциально сэкономить деньги и упростить инфраструктуру с помощью стратегии DR.

3.3. Катастрофоустойчивость (Disaster Avoidance, DA)

Для поддержания непрерывной работоспособности Виртуального Дата-центра клиента в случае аварии на одном из Дата-центров Orange, клиент может заказать опцию катастрофоустойчивого облака. В случае активации данной опции, ВМ распределяются случайным образом или по настроенным правилам между основной и резервной площадкой. При возникновении аварии в одном из ДЦ Orange, работавшие на нём ВМ автоматически запускаются на втором ДЦ. В обоих ДЦ доступны идентичные наборы внутренних и внешних сетей, что исключает необходимость изменения сетевых параметров ВМ в случае катастрофы.
Для обеспечения минимального времени простоя сервиса, в случае если приложение поддерживает кластеризацию, рекомендуется разместить члены кластера приложения в разных ДЦ с помощью правил (для этого необходимо сообщить Orange списки ВМ для размещения в каждом из ДЦ; ВМ, не вошедшие в списки, размещаются случайным образом).

3.4. Аварийное восстановление (Disaster Recovery, DR)

Облачная инфраструктура Orange может быть использована клиентом как DR-площадка. Технически

вариантов реализации такого сценария достаточно много и выбор конкретного зависит от существующей инфраструктуры и потребностей клиента. Клиент может самостоятельно развернуть такое решение (если не требуется интеграция на уровне системы управления облачной инфраструктурой), или специалисты Orange могут развернуть для клиента решение класса DRaaS (например, Zerto или Veeam Cloud Connect).

3.5. Подсистема хранения

Возможно использование разных типов дисковой ёмкости для одного и того же Виртуального Дата-центра и для одной и той же ВМ.
В случае заказа опции катастрофоустойчивости (DA) виртуальные машины размещаются на распределённой между двумя ДЦ All-Flash СХД (синхронная репликация). Этим обеспечивается доступность данных в случае катастрофы. Но также возможен заказ дискового пространства уровней Silver и Gold со следующими ограничениями:

- СХД для уровней Silver и Gold расположены в основном ДЦ и обеспечивают отказоустойчивость только в пределах этого ДЦ. Т.е. в случае катастрофы в основном ДЦ дисковое пространство уровней Silver и Gold не будет доступно из второго ДЦ. В случае катастрофы во втором ДЦ – доступ будет;
- Дисковое пространство уровней Silver и Gold может быть добавлено только как второй и последующие диски ВМ;
- Автоматический перезапуск ВМ, содержащих диски уровней Silver и Gold, в случае катастрофы в основном ДЦ не гарантируется, для запуска может потребоваться вмешательство инженеров Orange. Для исключения этого риска рекомендуется создать нужное количество ВМ с уровнями Silver и Gold, предоставить доступ к дискам через CIFS/NFS и обращаться к ним с продуктивных ВМ через сеть.

Сверх заказанного дискового пространства (уровней Silver, Gold и Platinum, но не для Platinum-DA), для каждого типа выделяется дополнительное дисковое пространство для своп (swap) ВМ Клиента из расчёта суммарного заказанного объёма ОЗУ, который добавляется Orange к каждому из заказанных типов. В Портале Cloud Director будет указан суммарный объём выделенного дискового пространства (указанный в Бланке заказа + добавленный Orange) и суммарный объём потребленного дискового пространства.
VMware Cloud Director учитывает потребление дискового пространства по следующей формуле (для каждого типа отдельно):
Суммарный объём потреблённого дискового пространства = Объём места на жестком диске, выделенный под ВМ Клиента (сумма объёмов дисков ВМ) + Объём памяти (ОЗУ), выделенный под все ВМ Клиента + Шаблоны и ISO-образы + Служебные файлы ВМ (метаданные) + Снэпшоты.
Использование места на жестком диске сверх того, что указано в Бланке заказа, может вызвать некорректную работу vdc клиента с последующим нарушением работы всех приложений.

3.6. Резервное копирование на диск (Бэкап на диск)

В случае потери или порчи данных Клиента по запросу Клиента Виртуальная машина может быть восстановлена из последней копии. Для активации данной опции необходимо её заказать путем оформления соответствующего бланка заказа на услугу.
Виртуальная машина восстанавливается из резервной копии «как есть». По причине технологических ограничений Orange не несет ответственности за целостность информационных систем и бизнес-приложений. Orange гарантирует восстановление виртуальных машин до уровня ОС внутри виртуальной машины.
Данная опция позволяет хранить полную копию vDC клиента и несколько инкрементных точек восстановления на диске. Клиент выбирает одну из 3-х стандартных схем резервного копирования на диск и количество точек восстановления (Т>3)

- Ежедневное;
- 3 точки в неделю: Понедельник, Среда, Пятница;
- 2 точки в неделю: Вторник, Четверг.

3.7. Резервное копирование (архивирование) на ленту (Бэкап на ленту)

Данный метод позволяет хранить резервные копии данных на съемных носителях (лентах), которые могут быть перемещены на удалённую площадку. Для активации данной опции необходимо её заказать путем оформления соответствующего бланка заказа на услугу.
Восстановление данных с ленты требует значительно больше времени, чем восстановление данных с дисков. Резервное копирование на ленту используется, когда необходимо длительное хранение данных и хранение резервных копий на удалённой площадке, альтернативной двум ДЦ, используемым для оказания Услуги.
Библиотека MSL4048 поддерживает аппаратное шифрование AES 256-bit на уровне ленточной библиотеки. Шифрование бэкапов на ленте опционально.
Клиент выбирает одну из 3-х стандартных схем резервного копирования на ленту и количество точек

восстановления (T>3)

- Ежедневное;
- 3 точки в неделю: Понедельник, Среда, Пятница;
- 2 точки в неделю: Вторник, Четверг.

Каждую неделю по расписанию создаётся полная копия vDC клиента, которая записывается на ленту. Лента вывозится на удалённую площадку на ежемесячной основе, где хранится в огнеупорном шкафу.
Клиент может выбирать:

- Хранить X недельных копий;
- Хранить Y месячных копий.

3.8. Самостоятельное управление резервным копированием (Self Service Backup)

Самостоятельное управление резервным копированием возможно через портал самоуправления Veeam Enterprise Manager.
Данная опция не совместима с РК на ленточные носители и резервным копированием на диск выполняемым Orange.
При заказе данной опции Клиенту необходимо самостоятельно рассчитать требуемый объём дискового пространства для хранения резервных копий исходя из объёма данных ВМ и планируемого расписания.

3.9. Выделенные GHz и vCPU

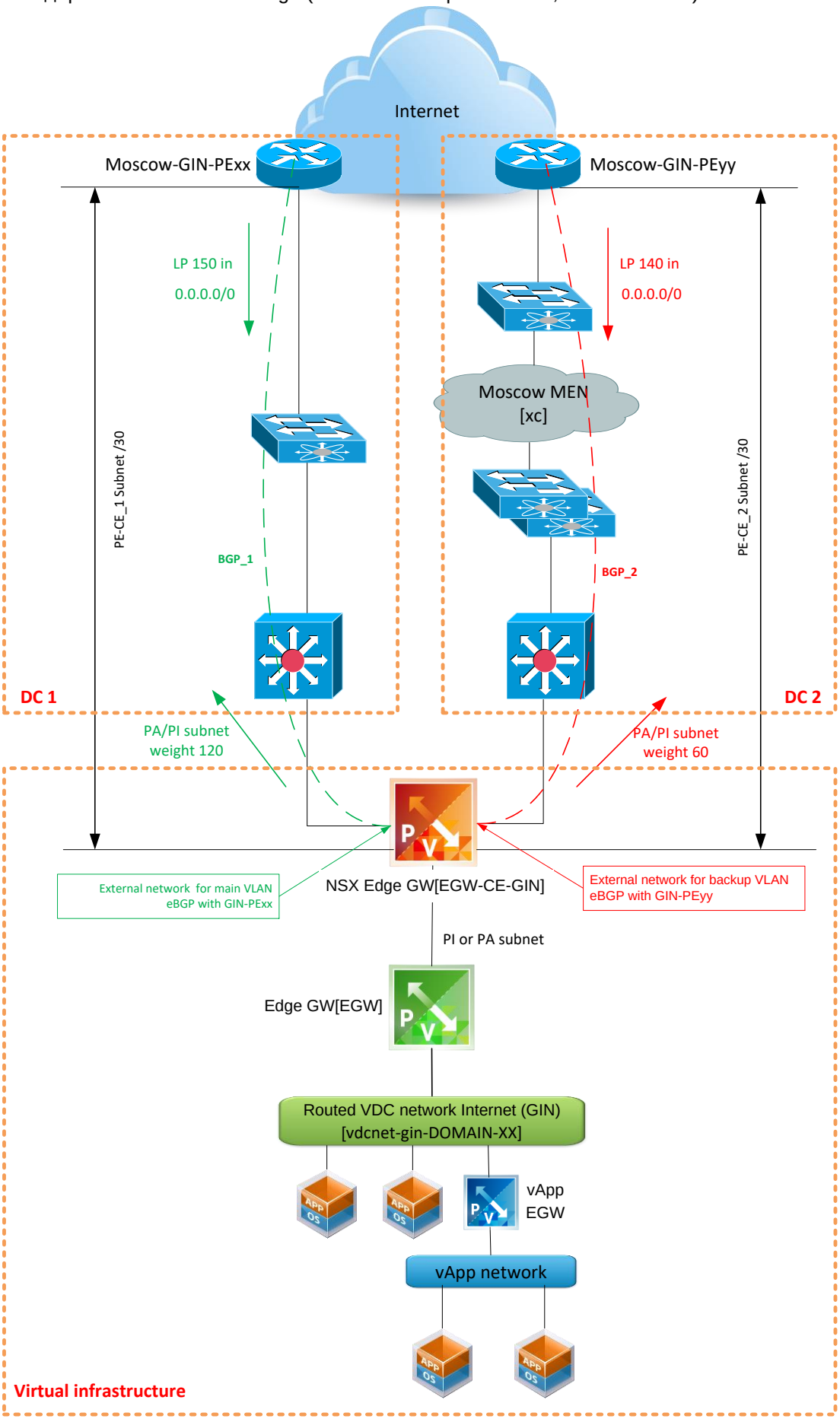
В рамках услуги FCA для Клиента создаётся виртуальный Дата-центр с набором вычислительных ресурсов согласно подписанному бланку заказа. В случае выделения процессорной мощности стоит обратить внимание на отличие между выделяемой процессорной мощностью и количеством ядер (vCPU).
Для примера предположим, что для vDC выделено 48GHz процессорной мощности.
При включении ВМ на каждый vCPU (ядро) выделяется (т.н. Allocation) 1GHz – т.е. максимум может быть включено 48 vCPU в данной ситуации (например: 12 ВМ по 4 vCPU, или 2 ВМ по 12 vCPU и 6 ВМ по 4 vCPU).
В инфраструктуре есть физические процессоры с номинальной частотой 2,2GHz и 2,5GHz, возьмём для дальнейших расчётов 2,5GHz.
Если все vCPU будут работать в полную мощность: 48*2,5=120GHz. Т.к. 120GHz больше выделенных 48GHz, то общее потребление vDC GHz будет ограничиваться до 48GHz – фактически все ядра будут работать на частоте 1GHz. Но такая ситуация крайне редка, как правило большинство vCPU почти простаивают (т.е. реально работающим достанется больше, вплоть до всех физических 2,5) - это даёт дополнительную гибкость в конфигурировании и работе ВМ.
Если нужно избежать потенциальной ситуации ограничения частоты ядер, можно посчитать так: 48GHz / 2.5GHz = 19.2 vCPU – т.е. настроить на ВМ 19 ядер и они гарантированно не будут ограничиваться.

3.10. Отказоустойчивый доступ к сетям Интернет и BVPN

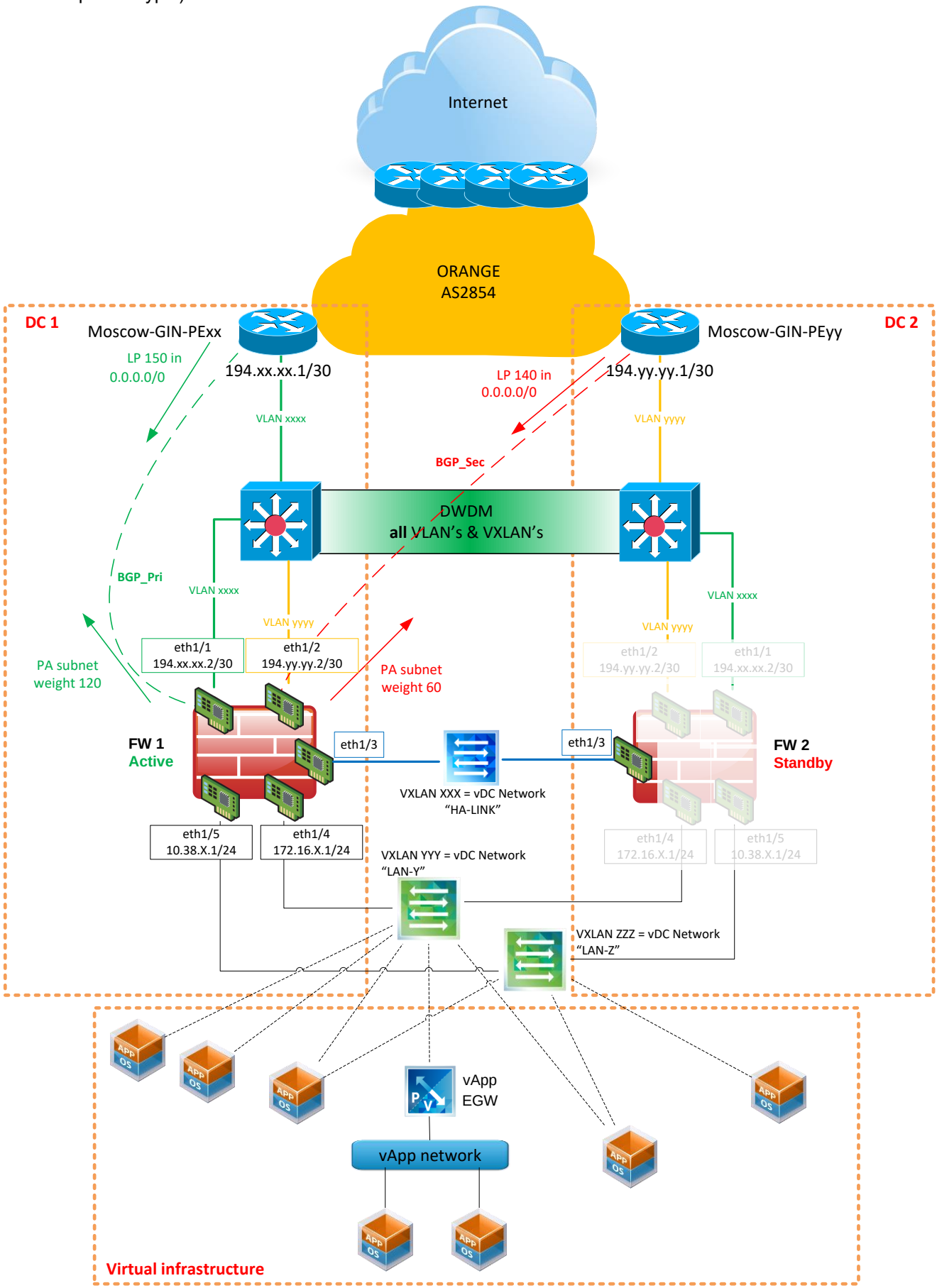
Все внешние сетевые соединения зарезервированы на уровнях физических соединений, физического оборудования, сети MEN, PE-маршрутизаторов и организуются через два датацентра. При этом не имеет значения, по какому маршруту (через какой датацентр) идёт в текущий момент трафик – для виртуальных машин в vDC это прозрачно и не имеет значимых отличий в задержках.

Ниже приведены схемы организации доступа к сети Интернет, для сети BVPN они аналогичны:

- Стандартная схема с NSX Edge (может быть в режиме HA, см. ниже 3.12)



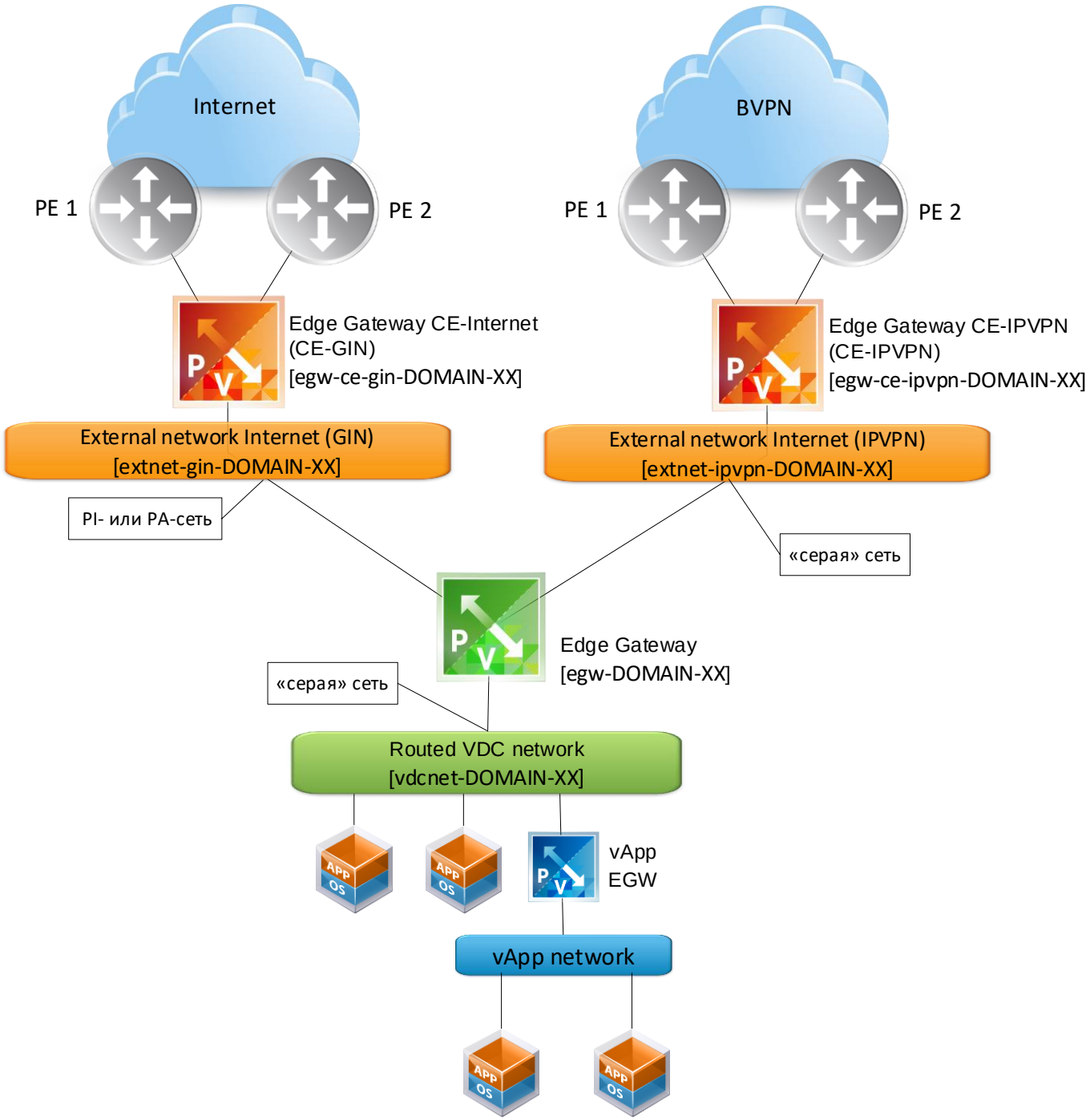
- Использование заказчиком собственного виртуального маршрутизатора (пример возможной архитектуры)



3.11. VMware NSX Edge

VMware NSX Edge – это решение, обеспечивающее для виртуального дата-центра функции маршрутизации, Firewall, NAT, DHCP, Site to Site VPN, SSL VPN-Plus, Load Balancing, High Availability, syslog. В инфраструктуре облака Orange существует два класса VMware NSX Edge Gateway:

- «EGW-**CE**» - выполняет функции классического CE-маршрутизатора. Для доступа в Интернет и BVPN используются разные EGW-CE. Настройка этих параметров находиться в зоне ответственности Orange;
- «EGW» - полностью доступен для управления клиентом из web-интерфейса Cloud Director . Обеспечивает DHCP, NAT, VPN, маршрутизацию, фильтрацию и балансировку нагрузки для внутренних сетей vDC.



Для сети Интернет «Edge Gateway CE-Internet (CE-GIN) [egw-ce-gin-DOMAIN-XX]» - полностью управляется Orange, выполняет только функции CE и предоставляет в сеть «External network Internet (GIN) [extnet-gin-DOMAIN-X]» выделенный префикс.

Для сети BVPN «Edge Gateway CE-BVPN (CE-BVPN) [egw-ce-ipvpn-DOMAIN-XX]» - полностью управляется Orange, выполняет только функции CE и обеспечивает связность с EGW через OSPF.

Edge Gateway [egw-DOMAIN-XX]» полностью доступен для управления клиентом из vCD.

3.12. NSX Edge High Availability

При заказе данной опции создаются active-passive кластеры из двух NSX Edge, автоматически размещающихся на разных хостах, а в случае DA в разных ДЦ:

- Для выбранного EGW управляемого клиентом;
- Для EGW-CE-GIN (в случае наличия доступа в Интернет);
- Для EGW-CE-IPVPN (в случае наличия доступа в сеть BVPN).

Это позволяет минимизировать время простоя сетевого доступа в случае выхода из строя физического хоста, на котором работает NSX Edge, или проблем с BM NSX Edge.

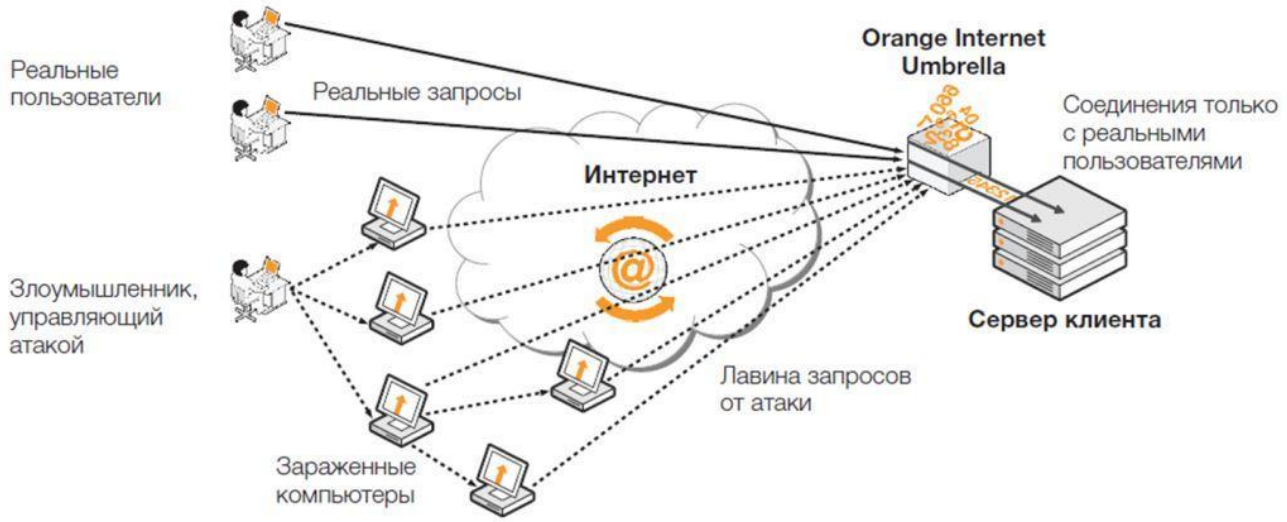
Ориентировочные временные параметры (данные основаны на логике работы технологий, их настройках и проведённых Orange тестах):

Сценарий	Перерыв доступа	Время, секунд
Аварийное переключение с основного канала Интернет или BVPN на резервный	Да	15 *
Штатное переключение (обслуживание) с основного канала Интернет или BVPN на резервный	Да	15 *
Возврат на основной канал Интернет или BVPN	Нет	-
Перезагрузка NSX Edge, после аварии на хосте	Да	45
Переключение на резервный NSX Edge при наличии опции High Availability	Да	15 **

* По специальному запросу может быть уменьшено до 3 сек.
** По специальному запросу может быть уменьшено до 6 сек.

3.13. Защита от DDoS-атак

Для порта Интернет, подключаемого в vDC, может быть заказана услуга защиты от DDoS-атак «Internet Umbrella» имеющая в своей основе комплекс оборудования Arbor и интеграцию с сетью Orange. «Internet Umbrella» – совокупность действий Orange, направленных на противодействие атакам типа DDoS, нацеленных на переполнение паразитным трафиком предоставленных Orange каналов доступа к сети Интернет.



3.14. Аренда лицензий на ПО

В рамках услуги FCA Orange может предоставлять клиенту лицензии по модели Software as a Service. Стандартно предоставляются в аренду лицензии:

- Microsoft Windows Server standard*;
- Microsoft Windows SQL Server standard*;

* К аренде доступны актуальные версии ПО, при этом, как правило, позволяющие использовать более старые версии.

По запросу доступен широкий спектр лицензий на ПО Microsoft.

3.15. Активация ПО Microsoft по программе SPLA через KMS

Для активации ПО Microsoft используется KMS-сервер Orange, доступный через сеть Интернет с адресов, выделяемых клиентам. Если BM не имеет доступа в Интернет, необходимо обратиться в Orange для активации MAK-ключом.

Процедура активации:

- Проверить, что на EGW открыт порт TCP1688 в Интернет
- Проверить, что на BM установлено корректно время!

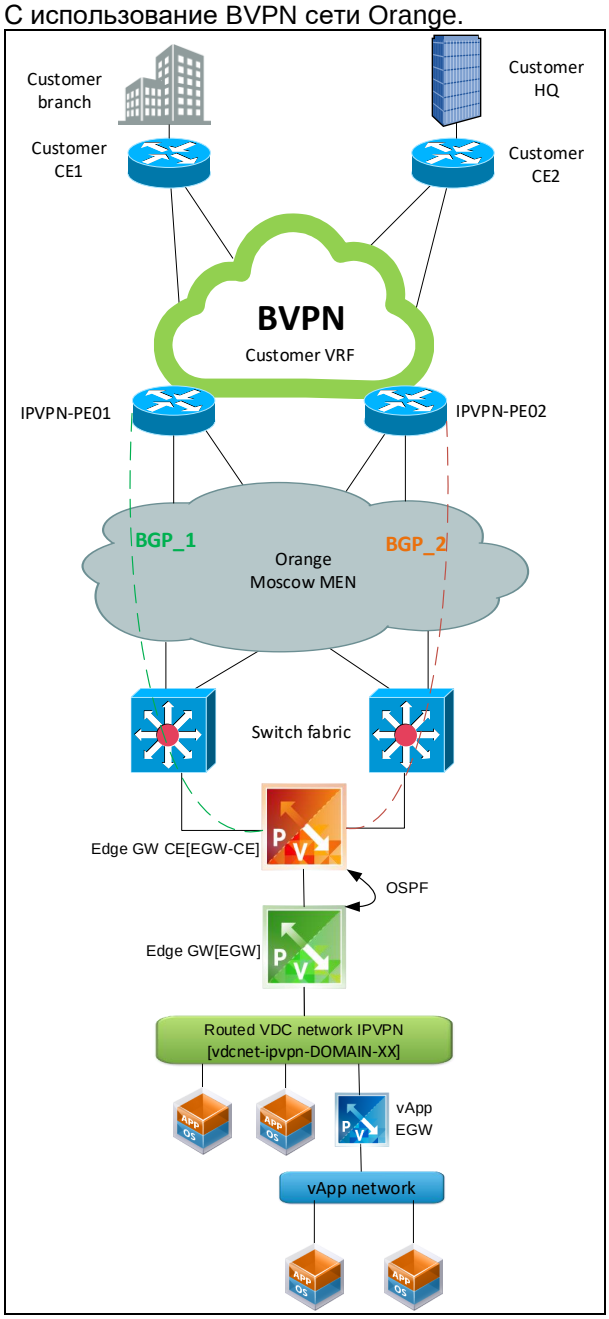
- Установить IP KMS
  slmgr -skms 194.84.17.201:1688
- Активировать online
  slmgr.vbs /ato
- Проверяем активацию
  slmgr /dlv

* Если KMS-сервер недоступен, необходимо обратиться в Orange.

3.16. Как подключить локальную сеть к облаку Orange?

Существует два основных метода подключения:

1. С использование BVPN сети Orange.

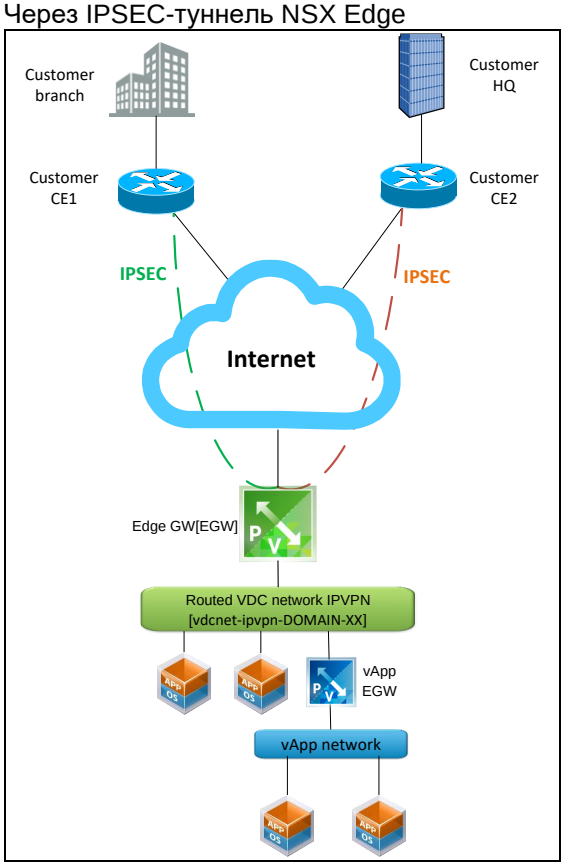


Плюсами такого метода являются:

- Качественные параметры канала (RTD, jitter, PLR) лучше, чем в сети Интернет
- Отказоустойчивое соединение облако-сеть BVPN
- Возможность реализации отказоустойчивого подключения со стороны сети клиента
- Опциональный SLA

- Работоспособность канала – ЗО Orange
- Опция подключения удалённых сайтов к сети BVPN через услугу «Internet VPN»(IPSEC до BVPN-узлов через Интернет)

2. Через IPSEC-туннель NSX Edge



Плюсы:

- Стоимость
- Скорость подключения новых удалённых сайтов

* Другие типы подключений через NSX Edge описаны в разделе 11.7 «VPN».

3.17. Подключение внешних USB устройств (USB-to-IP)

Для обеспечения проброса внешних USB устройств (как правило аппаратных USB ключей защиты ПО), используется оборудование Digi*:

- Digi AW08-G300, 8 USB портов, multihost
- Digi AW24-G300, 24 USB портов, multihost

Каждый из USB-портов привязывается к ВМ (к одной ВМ может быт привязано несколько портов).
Для каждого Заказчика устанавливается отдельное устройство Digi.
Следует отметить, что на текущий момент проброс ключей в виртуальные машины возможен только для гостевых ОС семейства MS Windows. Такое ограничение существует в связи с отсутствием драйверов для Linux ОС у производителя устройств USB-to-IP.
Также не рекомендуется использовать данные устройства для подключения высокоскоростных USB устройств, таких как внешние HDD, флэш-накопители и т.п.
** Производитель и модели могут быть изменены в ходе проработки запроса*

3.18. Подключение внешних сетевых устройств/серверов расположенных в ДЦ Orange

Существует возможность объединения физической сети и виртуальной сети vDC на уровне L2. Это может быть vDC сеть в которой непосредственно находятся виртуальные машины, или отдельный сегмент изолированный Edge.
Это может быть необходимо в случае размещения оборудования клиента в ДЦ Orange (услуга «Nethosting»).

Также данная опция может быть использована для подключения vDC к стороннему оператору связи, напрямую или через физический маршрутизатор.

В зависимости от требуемой скорости, это может быть:

- Один или два порта(MC-LAG) 1000BASE-T на одно устройство, организуется медное кабельное соединение до оборудования клиента;
- Один или два порта(MC-LAG) 10GBASE-SR на одно устройство, организуется оптическое кабельное соединение до оборудования клиента. *Не является стандартным вариантом, требуется проработка.*

4. Основные элементы VMware Cloud Director

Виртуальная организация (organization, vOrg) – самый верхний элемент в иерархии объектов абстракции Cloud Director . Содержит в себе информацию о пользовательских аккаунтах вашей организации и общие параметры.

Виртуальная организация (vOrg) – корневой логический элемент, содержащий в себе все ваши vDC, учётные записи администраторов, параметры аутентификация, уведомлений и т.п.

Виртуальный датацентр (virtual datacenter, vDC) – это совокупность ваших облачных ресурсов (виртуальные процессоры, память, место на диске, сети и т.д.). Это среда, в которой создаются виртуальные машины, наборы виртуальных машин, объединенных в одну группу - vApp, сети и пр. Вы можете увеличивать его размеры по мере необходимости, докупая нужные ресурсы (процессоры, память или диски) путем подписания соответствующего бланка заказа.

В вашей организации vOrg могут быть два (или более) vDC в случае, если, например, одновременно заказаны обычный vDC и с опцией Disaster Avoidance.

vApp – это набор виртуальных машин, объединенных в одну группу. Его можно создать пустым или сразу с виртуальными машинами. Благодаря vApp группой виртуальных машин можно управлять как одной единицей. Это особенно удобно, если вы управляете большой виртуальной инфраструктурой. На основе vApp можно создавать шаблоны. Если у вас есть необходимость периодически создавать однотипные группы виртуальных машин, то это свойство vApp позволит вам сэкономить время. Cloud Director также предоставляет возможность создавать отдельную сеть на уровне vApp, позволяя обеспечивать дополнительную изоляцию между двумя vApp. vApp можно использовать для группировки виртуальных машин, относящихся к одному бизнес-приложению. Также на основе vApp можно разграничивать доступ между администраторами вашей организации.

Виртуальные машины (VM, BM) можно создавать из шаблонов в каталоге (сразу с ОС) или «с нуля», устанавливая нужную ОС из загруженного шаблона или образа.

Каталоги (Catalogs) – это папки, в которых можно хранить шаблоны vApp, виртуальных машин и медиа-файлов (ISO-образы).

Сеть уровня организации (Org VDC Network) – это сеть, доступная по умолчанию для всех vApp. Сеть уровня организации может быть изолированной от внешних сетей (isolated), маршрутизируемой через Edge Gateway (routed) или напрямую соединённой с внешними сетями на L2 (direct).

Помимо сети уровня организации, которая доступна для всех vApp и может быть «растянута» между разными vDC одной организации вы можете создать сеть уровня vApp. По этой сети будут взаимодействовать виртуальные машины только данного vApp: для виртуальных машин из других vApp она не будет доступна. Сеть уровня vApp можно подсоединить к сети уровня организации, тем самым позволив данному vApp взаимодействовать с другими vApp организации или за ее пределами, при этом между сетью vApp и сетью vOrg будет находится специализированный, «маленький», Edge Gateway предоставляющей ограниченный функционал (только FW,NAT и DHCP).

В облаке Orange приняты **стандартные соглашения об именовании объектов**:

Объект	Шаблон имени	Пример для "startrek.com"
Organization	vorg-DOMAIN	vorg-startrek.com
Virtual Datacenter	vdc-DOMAIN-XX	vdc-startrek.com-01
Edge Gateway CE-Internet (CE-GIN)	egw-ce-gin-DOMAIN-XX	egw-ce-gin-startrek.com-01
Edge Gateway Internet (GIN)	egw-gin-DOMAIN-XX	egw-gin-startrek.com-01
Edge Gateway CE-BVPN	egw-ce-ipvpn-DOMAIN-XX	egw-ipvpn-startrek.com-01
Edge Gateway (managed by customer)	egw-DOMAIN-XX	egw-startrek.com-01

Routed VDC network Internet (GIN)	vdcnet-gin-DOMAIN-XX	vdcnet-gin-startrek.com-01
Routed VDC network BVPN	vdcnet-ipvpn-DOMAIN-XX	vdcnet-ipvpn-startrek.com-01
Internal VDC network	vdcnet-DOMAIN-XX	vdcnet-startrek.com-01
Direct connected VDC network L2VPN	vdcnet-l2vpn-DOMAIN-XX	vdcnet-l2vpn-startrek.com-01
Distributed Port Group CE-Internet (CE-GIN)	dpg-ce-gin-DOMAIN	dpg-ce-gin-startrek.com
Distributed Port Group CE-BVPN (CE-BVPN)	dpg-ce-ipvpn-DOMAIN	dpg-ce-ipvpn-startrek.com
Distributed Port Group Internet (GIN)	dpg-gin-DOMAIN-VID	dpg-gin-startrek.com-2925
Distributed Port Group Internet (BVPN)	dpg-ipvpn-DOMAIN-VID	dpg-ipvpn-startrek.com-2924
Distributed Port Group Internet (L2VPN)	dpg-l2vpn-DOMAIN-VID	dpg-l2vpn-startrek.com-2999
External network Internet (GIN)	extnet-gin-DOMAIN-XX	extnet-gin-startrek.com-01
External network BVPN	extnet-ipvpn-DOMAIN-VID	extnet-ipvpn-startrek.com-2924
External network L2VPN	extnet-l2vpn-DOMAIN-VID	extnet-l2vpn-startrek.com-2999
Основной администратор организации	adm_DOMAIN	adm_startrek.com

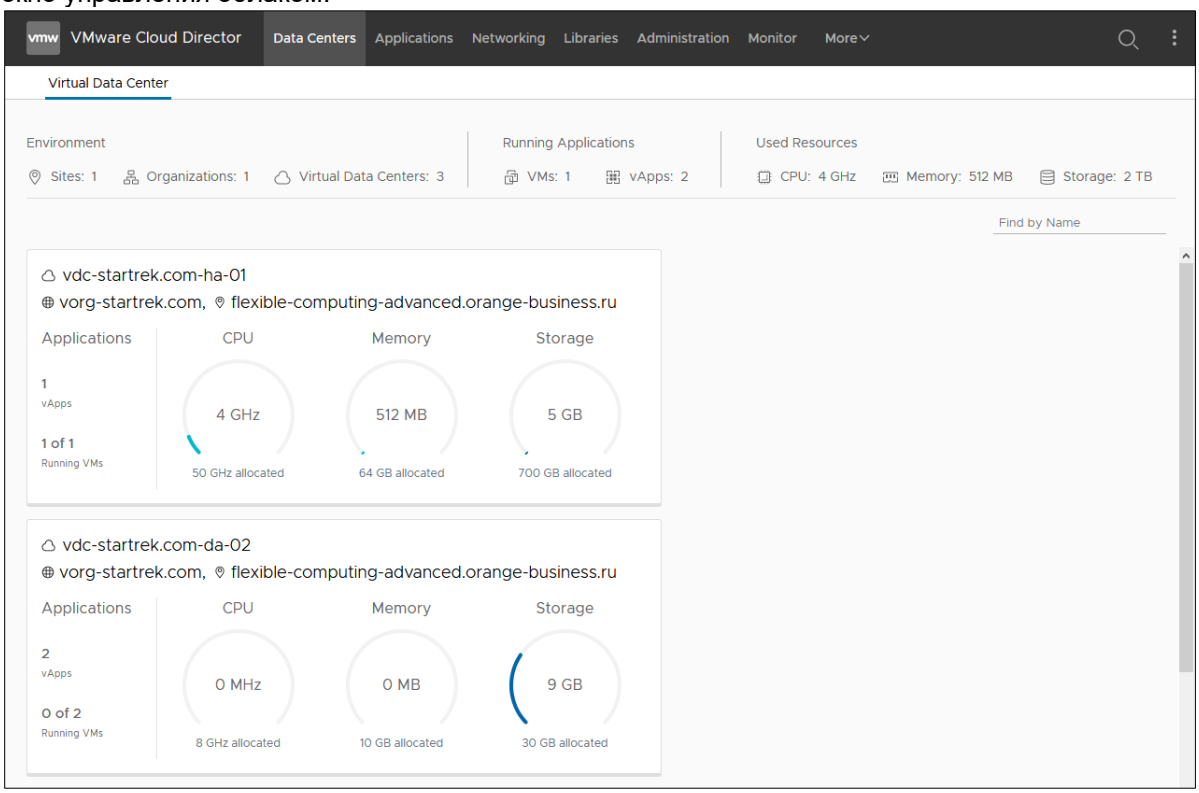
5. *Вход в виртуальный дата-центр*

После окончания создания и настройки вашего виртуального дата-центра (далее vDC – Virtual DataCenter) вы получите от Orange URL и административный аккаунт для доступа к vDC.

На текущий момент доступен только HTML5 WEB-интерфейс:

- «Tenant portal»: полнофункциональный интерфейс на базе HTML5.
  Доступен по адресу вида (в конце необходимо указывать имя своего vorg):
  https://flexible-computing-advanced.orange-business.ru/tenant/**vorg-startrek.com/**

Открываем в браузере URL, вводим в соответствующие поля имя пользователя и пароль, входим в основное окно управления облаком:



6. *Типичные проблемы при подключении и работе с WEB-интерфейсом*

- В случае использования SSL-инспекции при выходе в Интернет, либо при перезаписи корневых

сертификатов (например, через политики AD), может не работать удалённая консоль ВМ и загрузка образов/vApp.
Для решения проблемы необходимо через тот-же браузер зайти по адресу https://proxy.orange-business.ru/ и вручную подтвердить доверие сертификату.

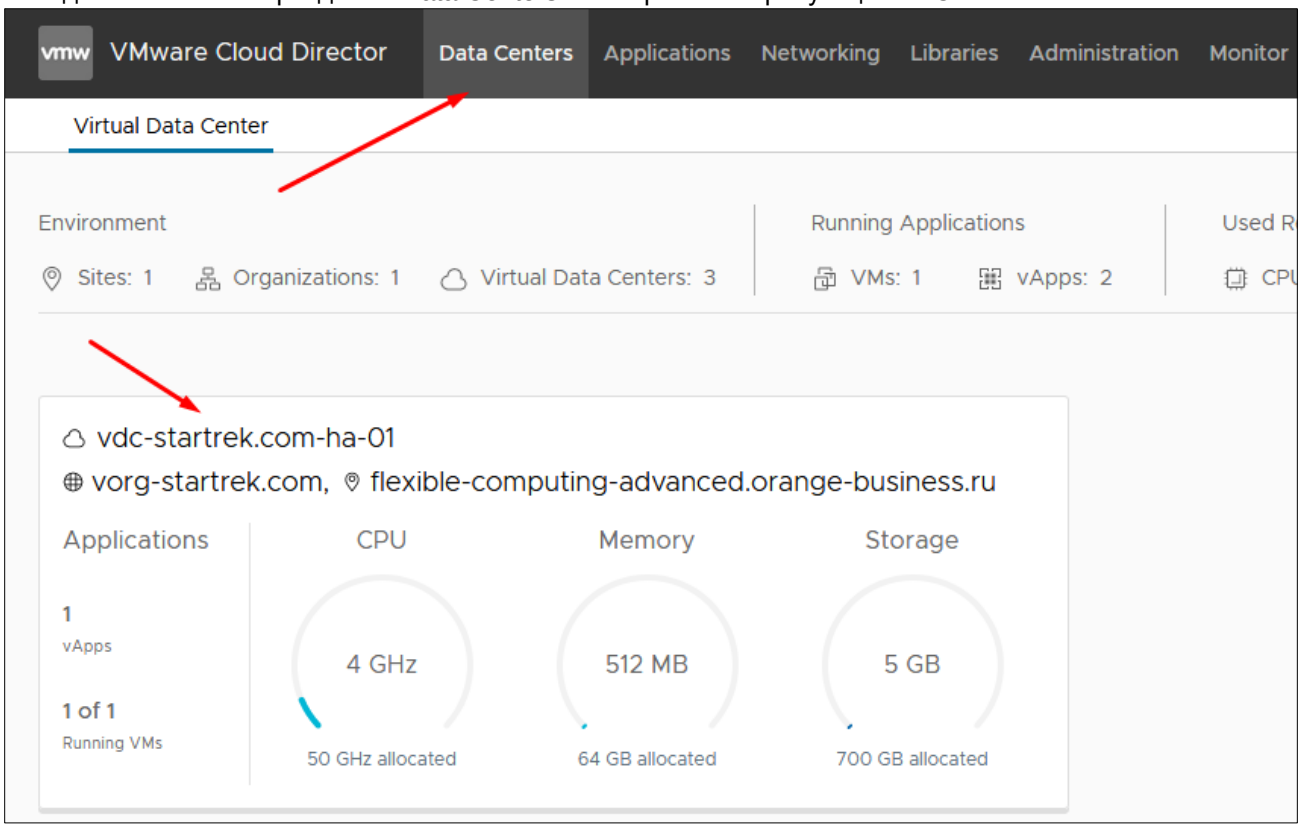
7. Проверка доступности ресурсов vDC и сетевой связности

Завершающим шагом настройки вашего vDC со стороны Orange является фактическая проверка доступности ресурсов и наличия сетевой связности.

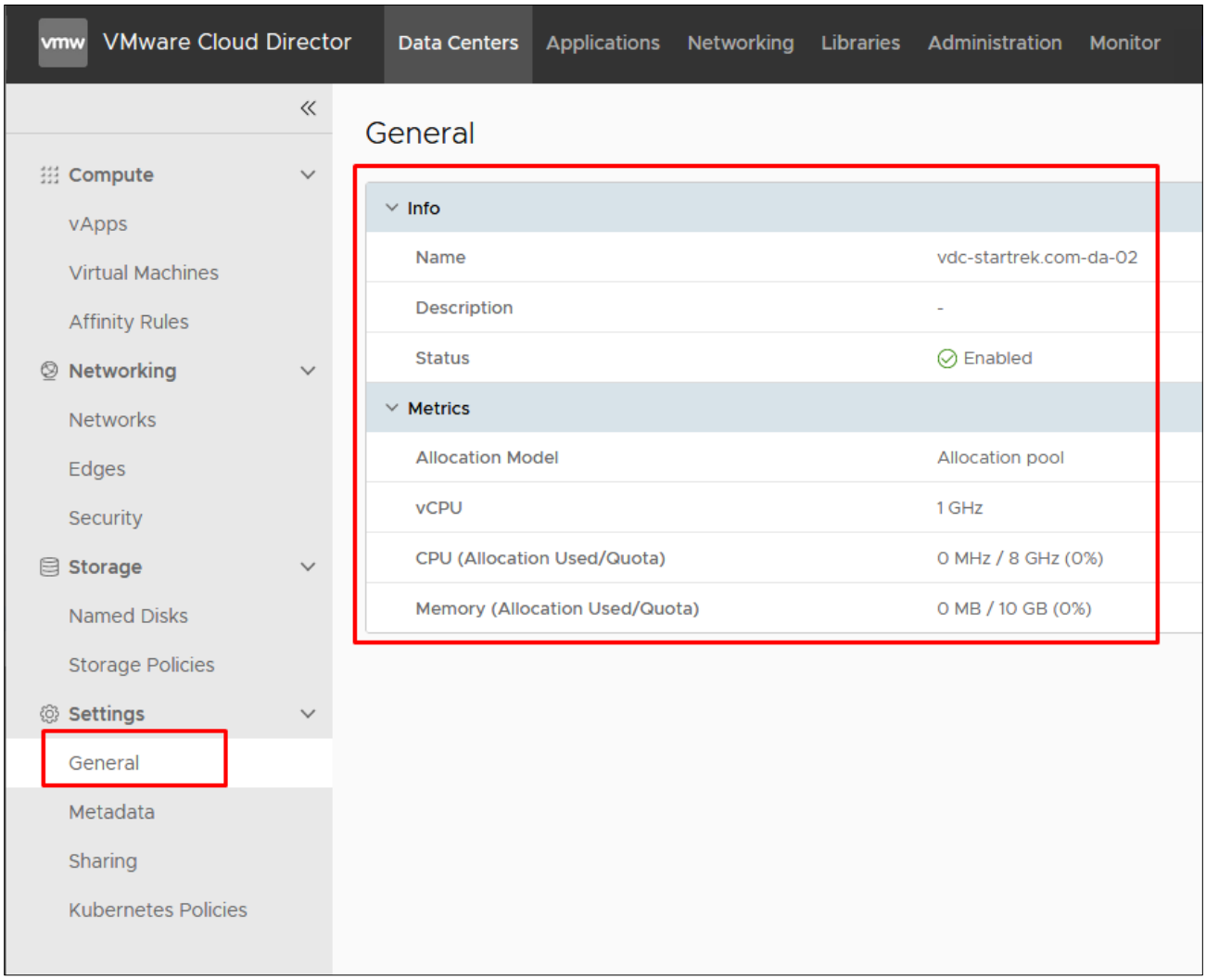
Для этого используется преднастроенный шаблон vApp «Orange-ATP». Мы рекомендуем вам повторить проверку.

7.1. Проверка доступности ресурсов

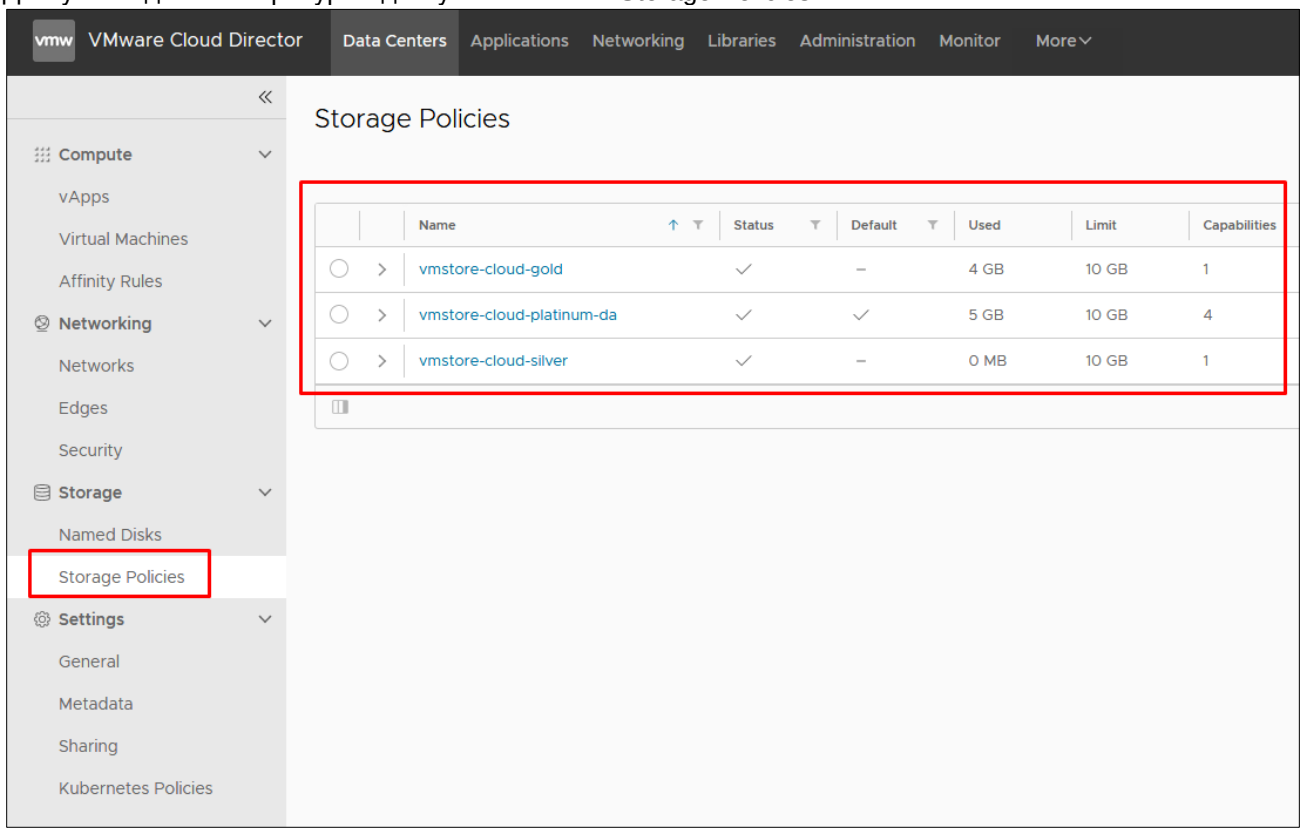
Находясь в основном разделе «Data Centers» выберите интересующий vDC:



Слева в меню «General»:

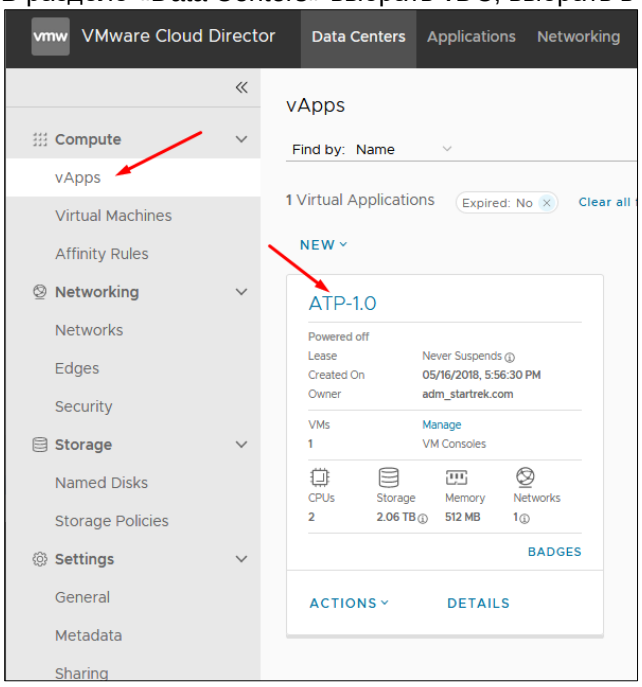


Доступные дисковые ресурсы доступны в меню «Storage Policies»:

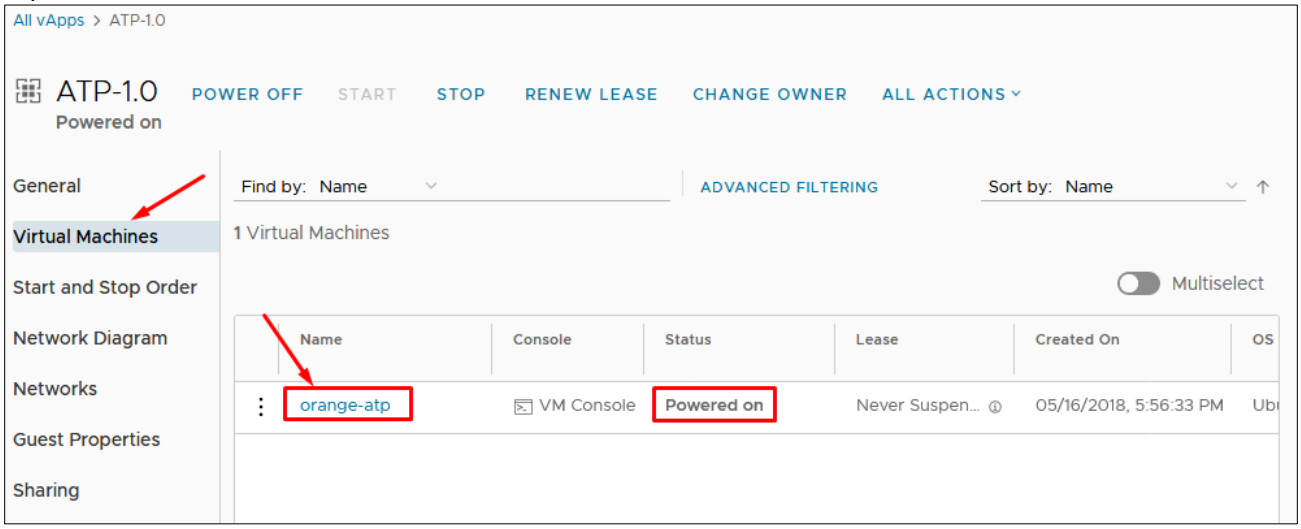


7.2. Проверка сетевых ресурсов

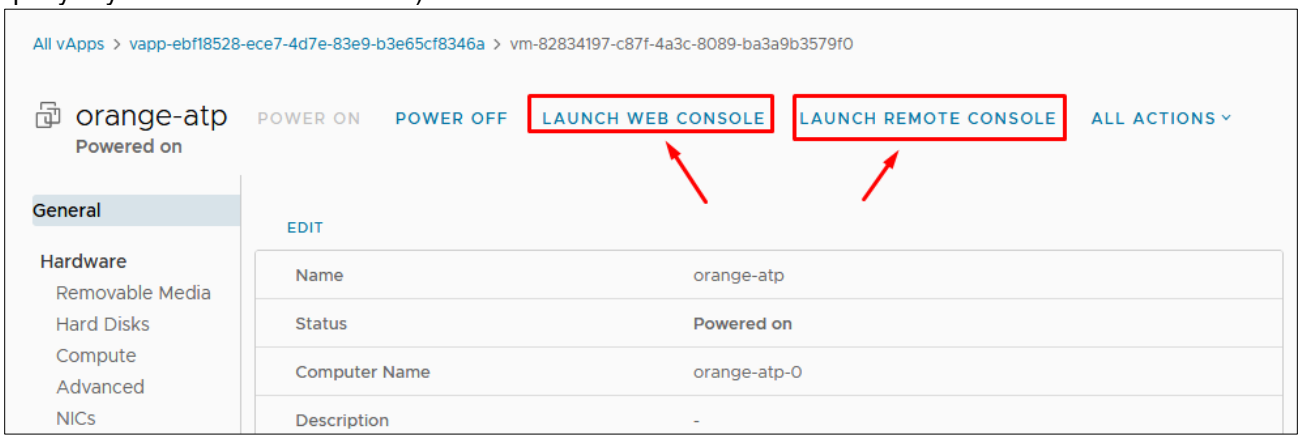
В разделе «Data Centers» выбрать vDC, выбрать в меню слева «vApps», зайти в тестовый vApp:



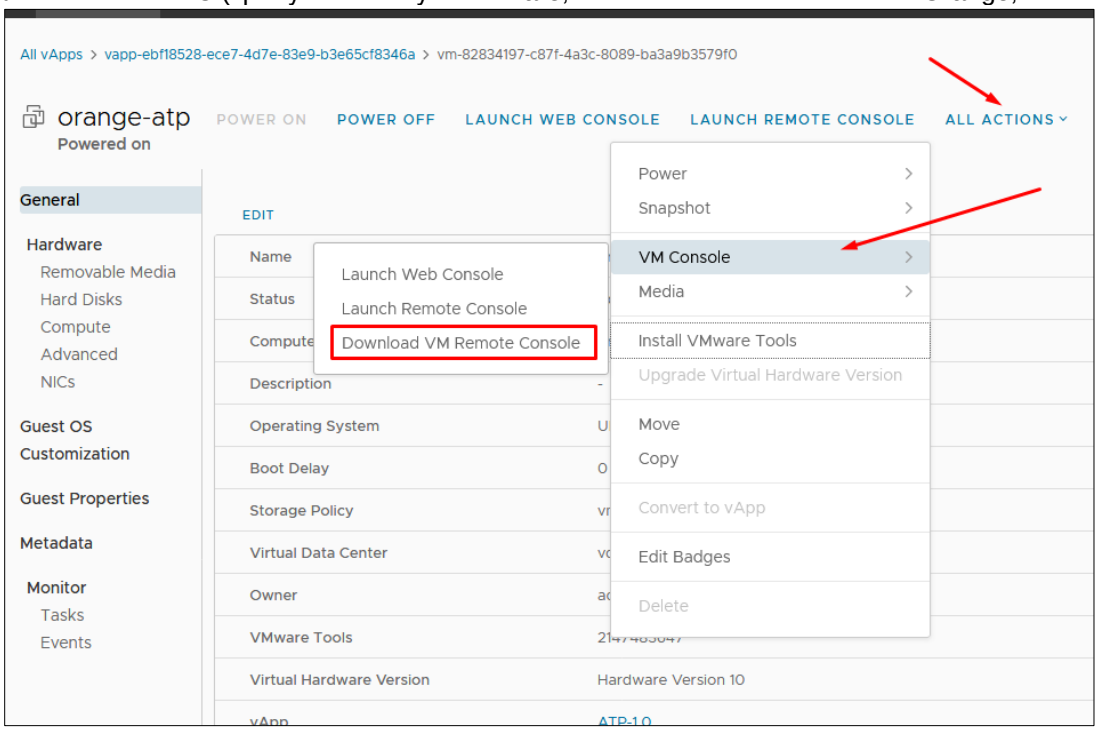
Виртуальная машина "orange-atp" уже должна быть включена, если это не так - запустите vApp целиком, перейдите в ВМ:



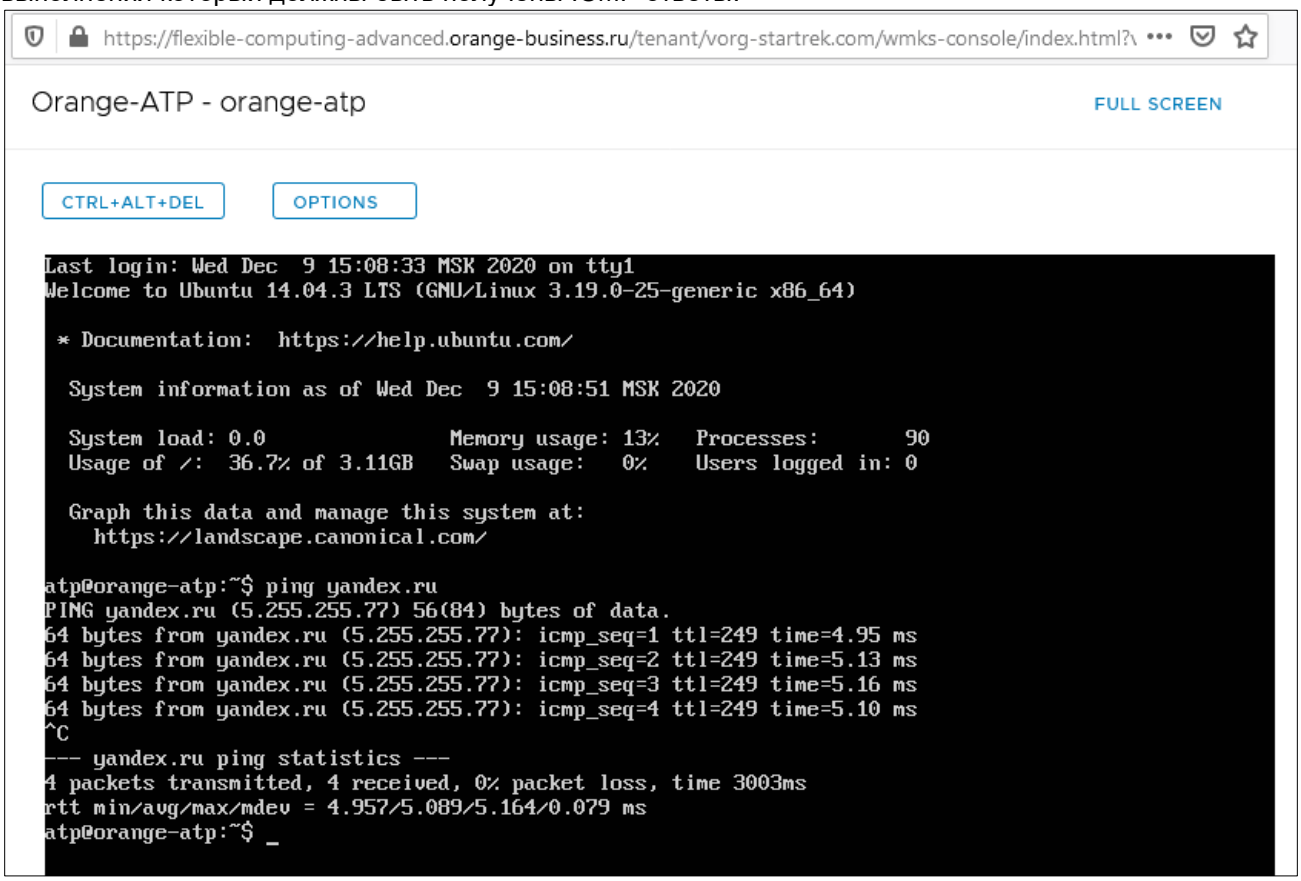
Для доступа в консоль виртуальной машины можно использовать WEB-консоль или VMRC (рекомендуется, но требует установки клиента на ПК):



Установка VMRC (требуется аккаунт VMware, или вы можете связаться с Orange, чтобы получить его):



ВМ из данного vApp автоматически входят в ОС и получают сетевые настройки через VMware Tools. Остаётся проверить доступность сетей, для Интернет это будет, например, команда «ping yandex.ru» в результате выполнения который должны быть получены ICMP ответы:

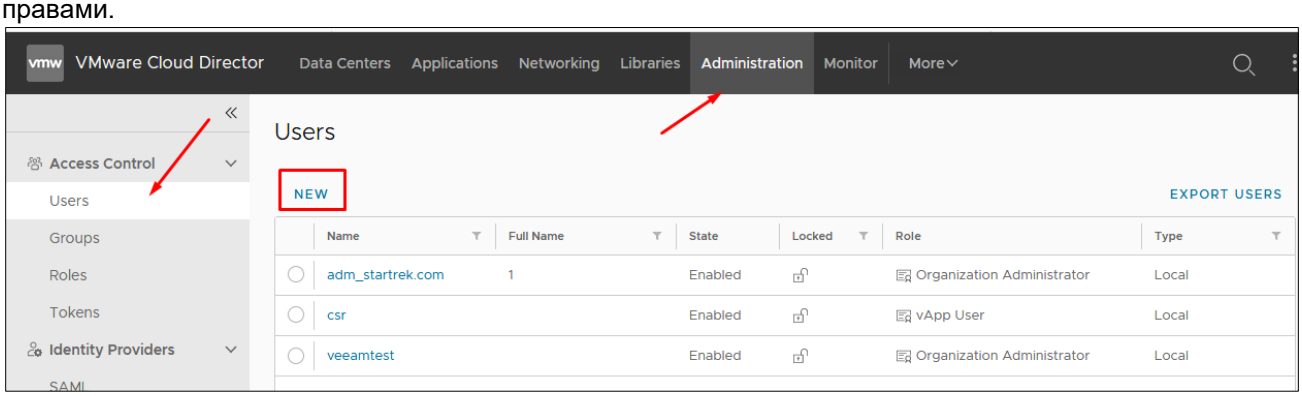


Для сети BVPN (ВМ atp-BVPN) процедура аналогична, но проверять следует доступность удалённого хоста в

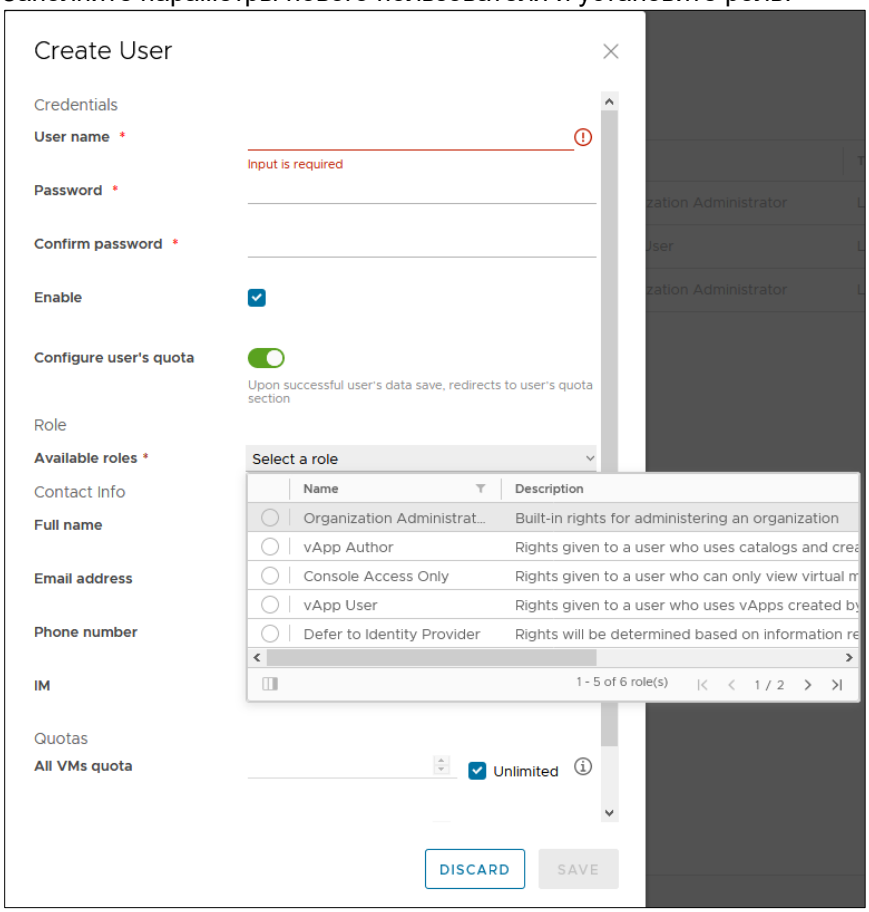
вашей BVPN сети.

8. *Управление учётными записями пользователей*

Cloud Director позволяет управлять правами доступа пользователей к облачным ресурсам. Выбрать нужную роль можно при создании нового пользователя.
При первоначальной настройке вашего облака создаётся один пользователь с полными правами Organization Administrator, в случае необходимости вы можете создать любое количество пользователей с разными правами.



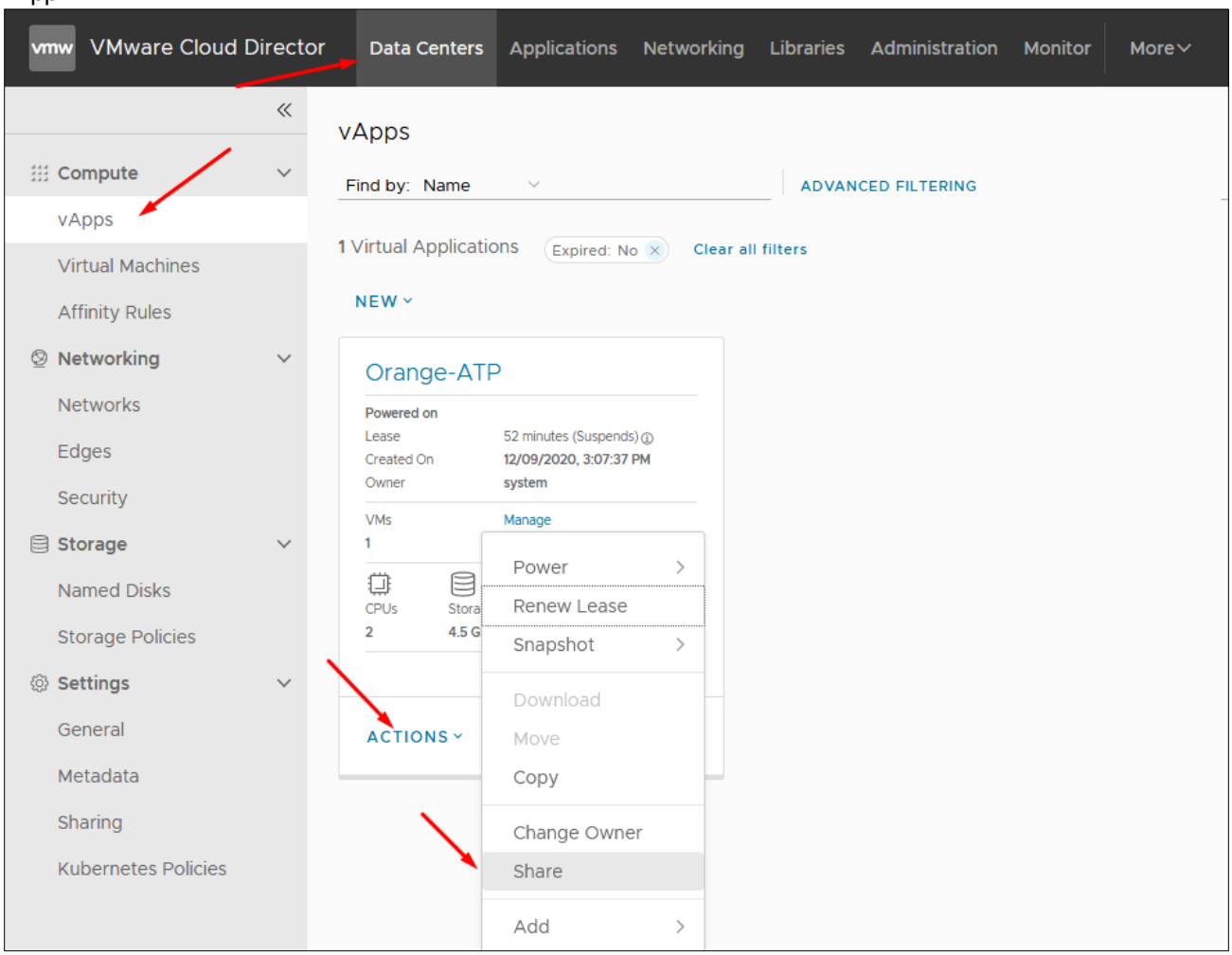
Заполните параметры нового пользователя и установите роль:

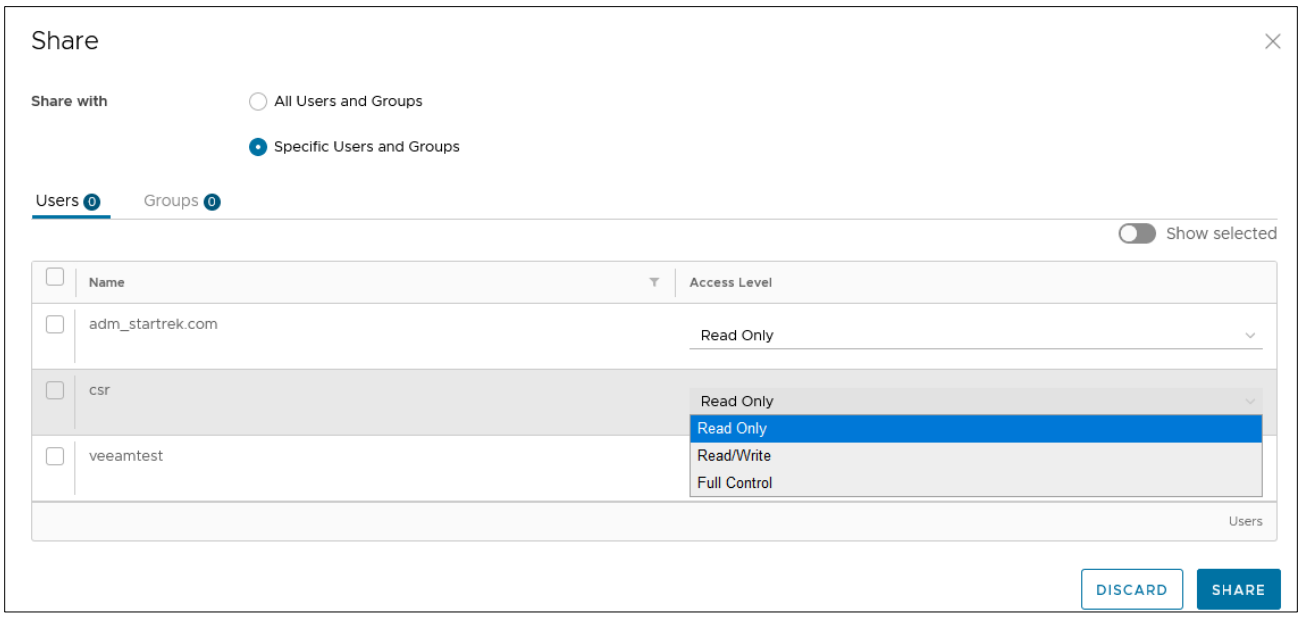


Типы ролей:

- Администратор организации (Organization administrator) – полные права доступа ко всей организации и её иерархии.
- Создатель каталога (Catalog Author) может создавать и публиковать каталоги.
- Создатель vApp (vApp Author) может использовать каталоги и создавать vApp.
- Пользователь vApp (vApp User) может использовать существующие vApp.
- Консольный доступ (Console Access Only) позволит пользователю с такой ролью только просматривать свойства виртуальных машин и пользоваться консолью гостевой ОС (без возможности управления её «питанием»).

Права доступа к определённым vApp для пользователей с ролью vApp User задаются в настройках конкретного vApp:

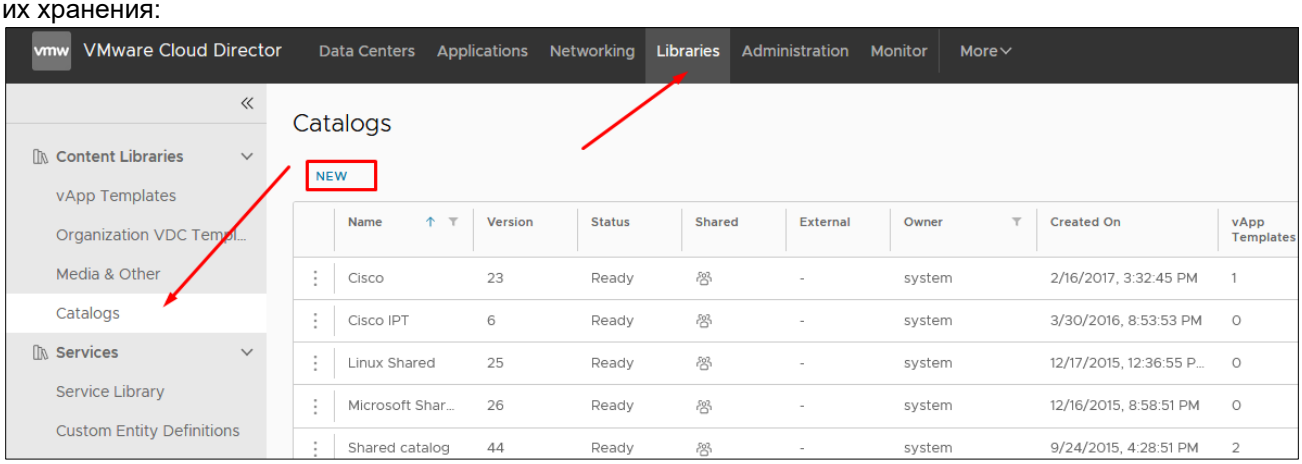




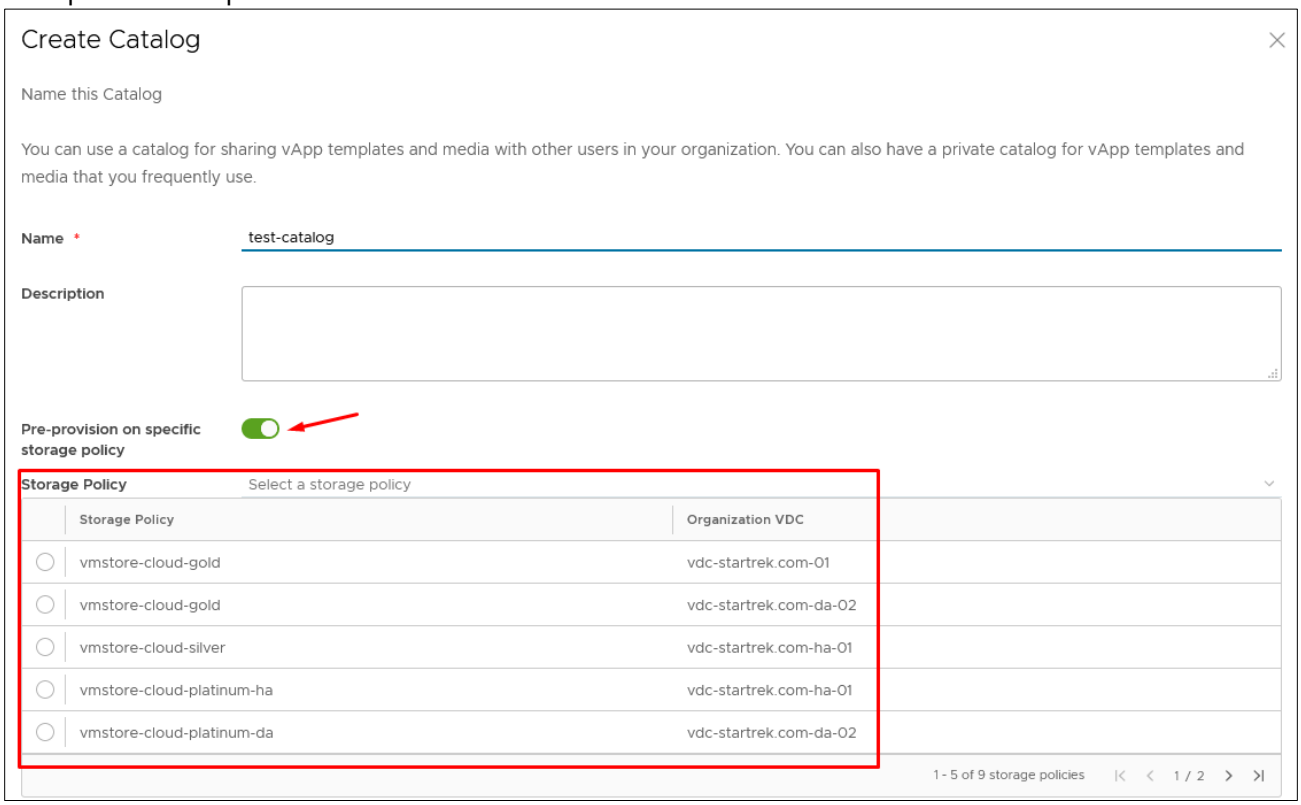
9. Загрузка образов (ISO) и шаблонов ВМ

9.1. Создание каталога

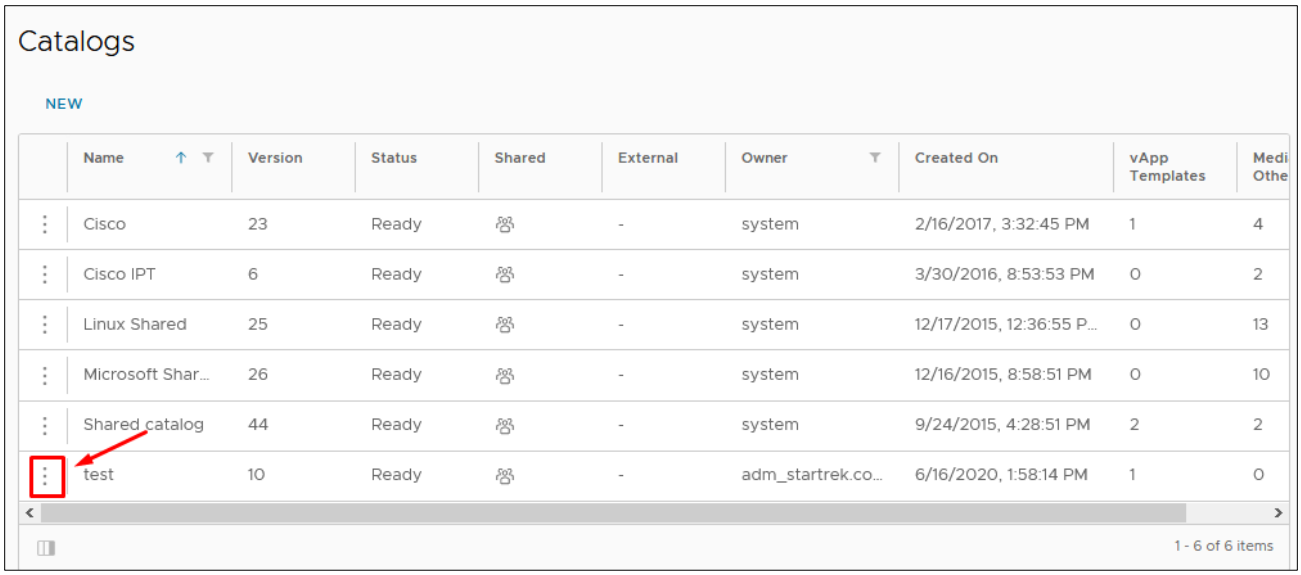
Для получения возможности загрузки любого типа данных, в первую очередь необходимо создать каталог для их хранения:

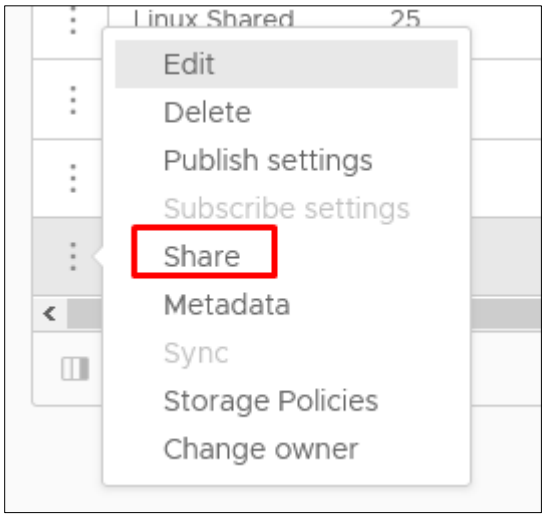


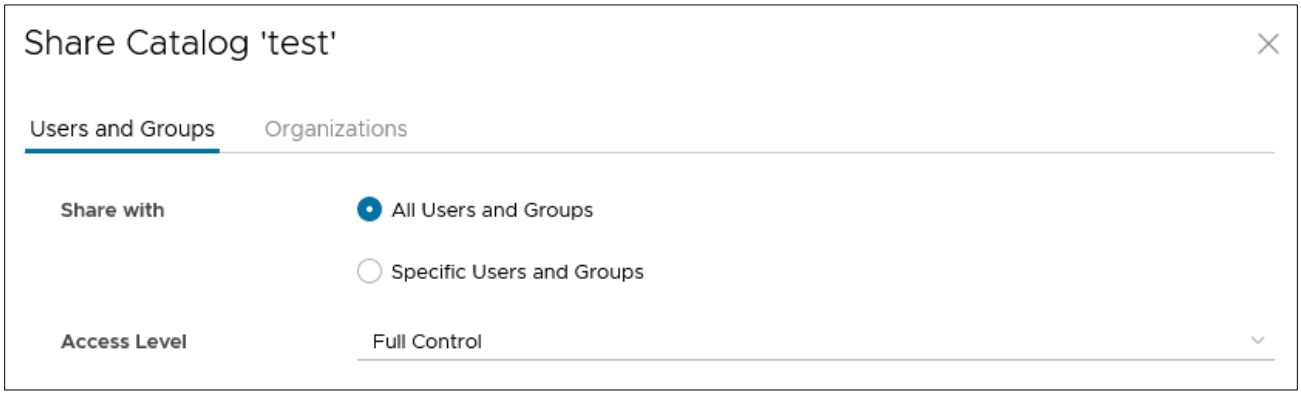
Выберите место хранения каталогов:



По умолчанию каталог будет доступен всем пользователям вашей организации в режиме только для чтения, в случае необходимости это можно изменить:







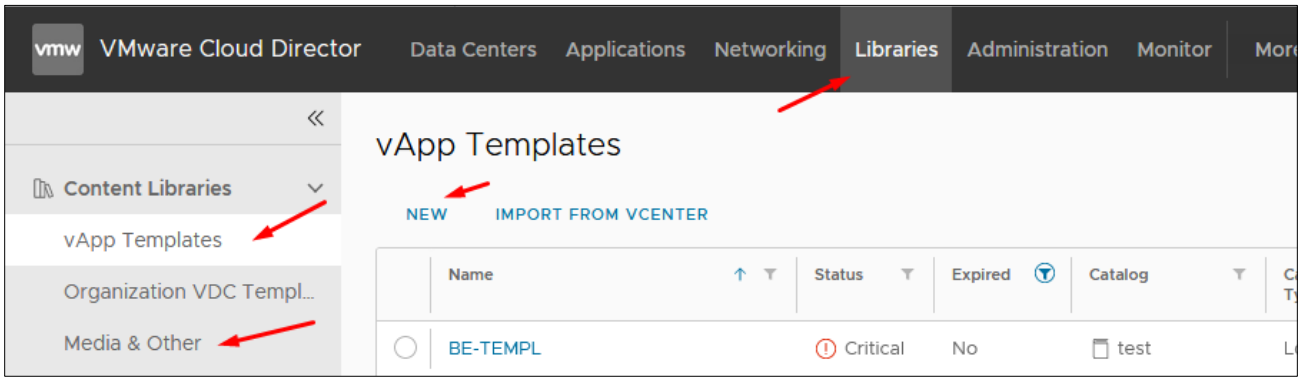
9.2. Загрузка через Cloud Director

После создания каталога появляется возможность загрузить ISO-образы (“Media & Other”) или шаблоны vApp в формате OVA или OVF («vApp Templates»).

Внимание:

- Образы должны быть в формате OVF, либо OVA. Максимальная версия поддерживаемого Virtual Hardware – 19;
- К машине не должны быть подключены дополнительные устройства, кроме SCSI HDD, IDE CD-ROM, VMware Video Card, Network Adapters (использование таких устройств, как звуковые карты, SATA дисковые устройства и др. не поддерживается). Поэтому если у вас есть виртуальная машина в

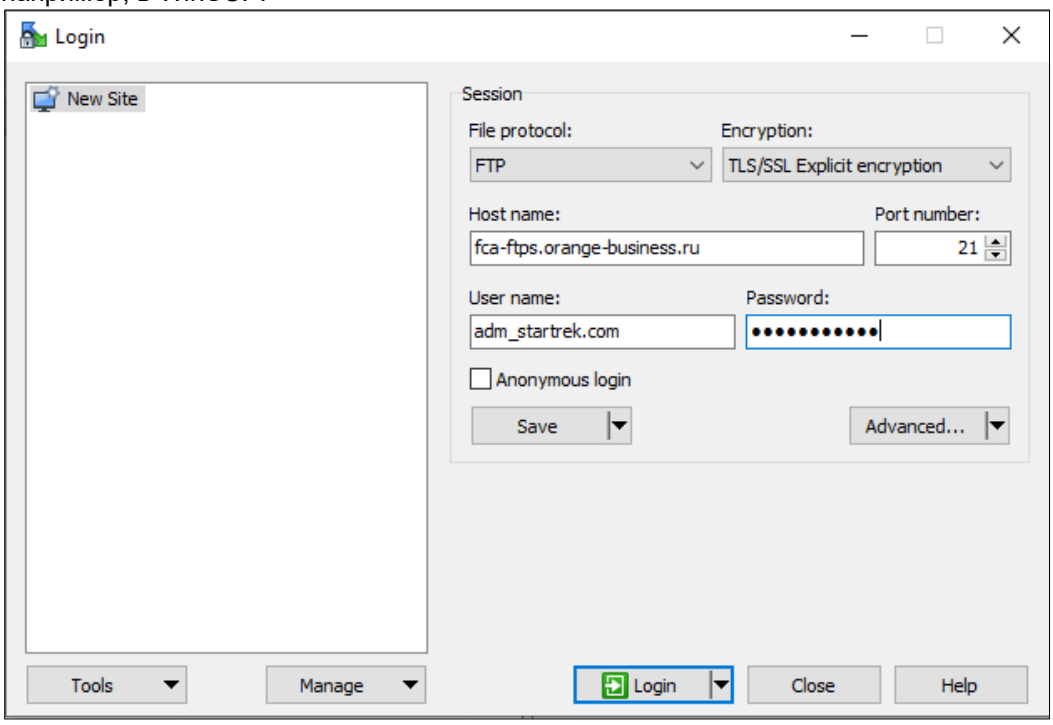
формате VMX (например, из локальной инсталляции vSphere или VMware workstation), то их предварительно необходимо экспортировать в формате OVF/OVA или сконвертировать утилитой ovftool.



9.3. Загрузка через FTPS-сервер Orange

Альтернативным способом загрузки шаблонов ВМ является использование FTPS-сервера Orange. Данный вариант более удобен в случае необходимости загрузки большого количества ВМ или если вы заказали услугу миграции ВМ силами Orange (в этом случае возможна загрузка файлов ВМ без конвертации в OVA/OVF). Реквизиты доступа к FTPS-серверу вы можете получить, обратившись в HelpDesk Orange либо к аккаунт менеджеру.
После окончания загрузки вы должны сообщить об этом в Orange для проведения процедуры импорта.

Примечание: для доступа к ftp серверу нужно использовать режим FTP «**TLS/SSL Explicit encryption**» например, в WinSCP:



9.4. Загрузка через ovftool

Утилита ovftool является крайне удобной при работе с vCloud и показывает большую скорость работы по сравнению с WEB-интерфейсом. Подробную документацию можно получить на странице утилиты.

Ниже приведены несколько примеров синтаксиса:

- Export vApp Template from vCloud

```
ovftool.exe --targetType="OVA"
```

```
"vcloud://USERNAME@flexible-computing-advanced.orange-business.ru?org=vorg-startrack.com&vdc=vorg-startrack.com-01&vapp=vApp_01" "C:/Users/test/Desktop/vm.ova"
```

- Import vApp Template from vCloud

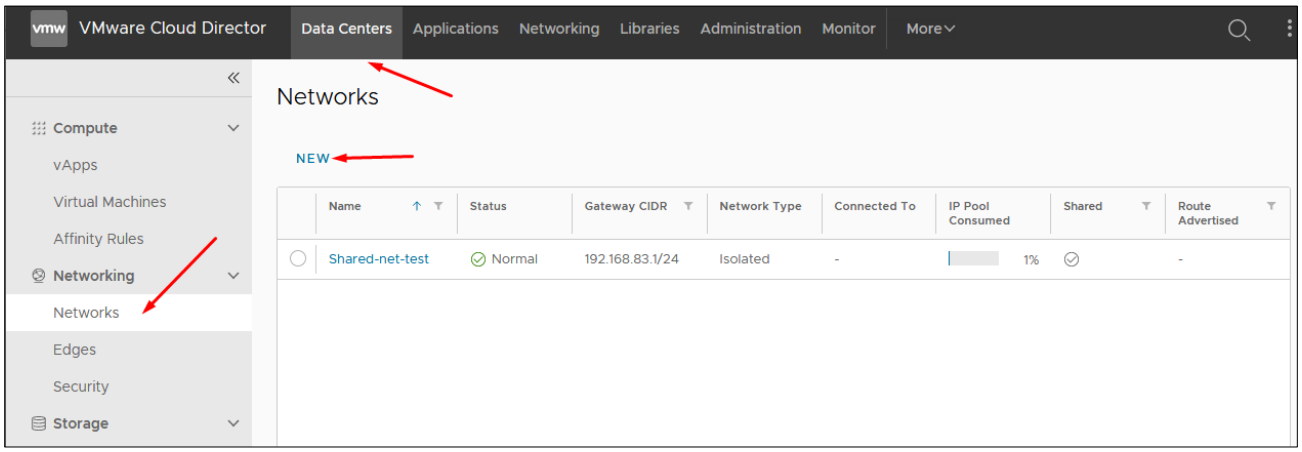
```
ovftool.exe --sourceType="OVA" "C:/Users/test/Desktop/vm.ova"
"vcloud://USERNAME@flexible-computing-advanced.orange-business.ru?org=vorg-startrack.com&vdc=vorg-startrack.com-01&catalog=test&vappTemplate=testtemplate"
```

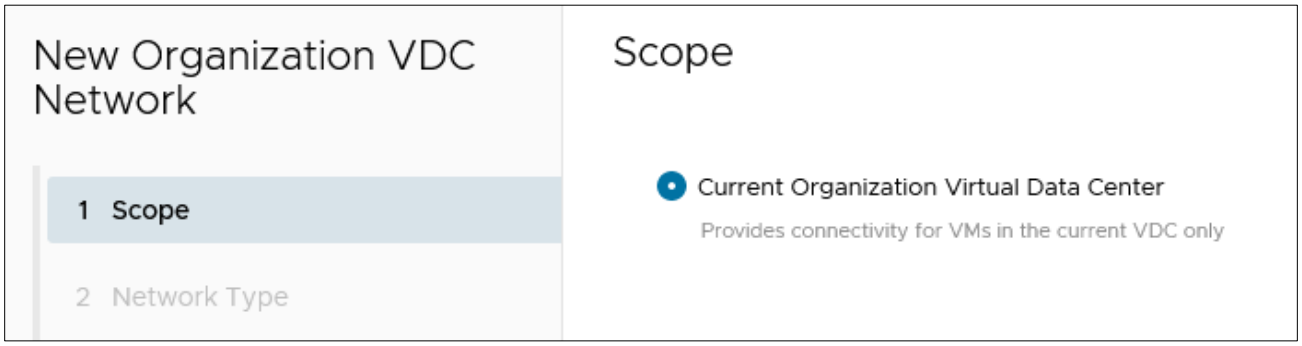
- Upload ISO

```
ovftool.exe --sourceType="ISO" "C:/down-file.iso"
"vcloud://USERNAME@flexible-computing-advanced.orange-business.ru?org=vorg-startrack.com&vdc=vorg-startrack.com-01&catalog=test&media=image"
```

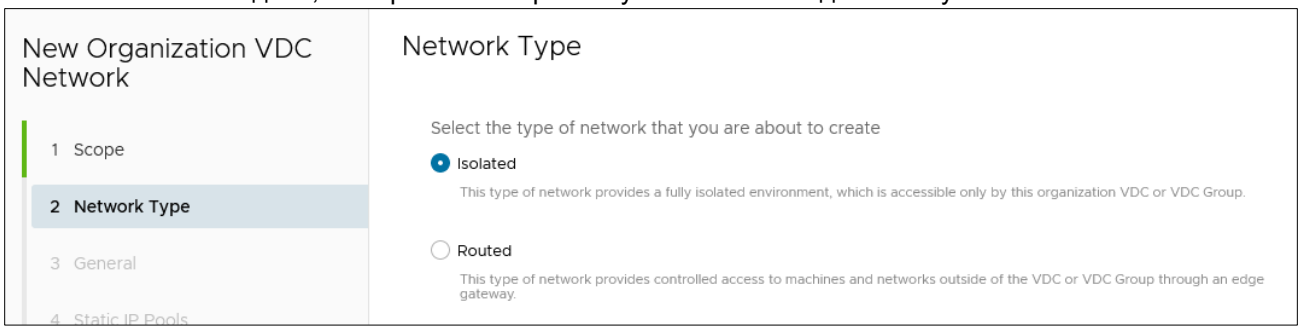
10. Сети vOrg и vApp

10.1. Создание vOrg сети





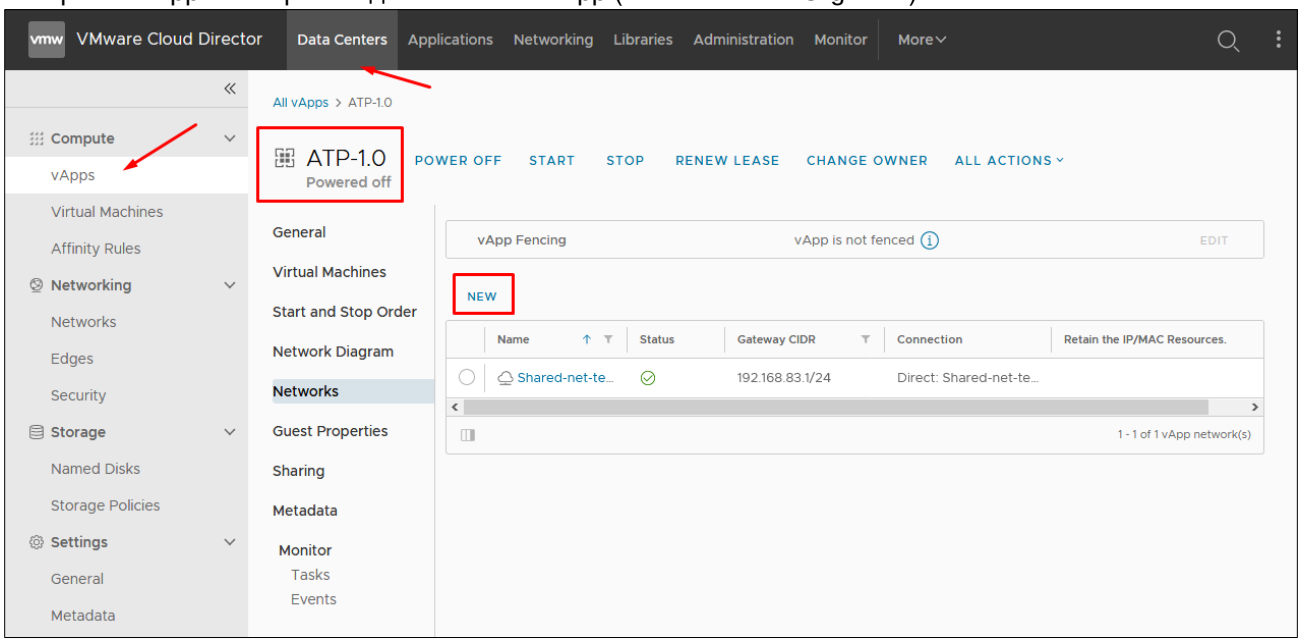
В зависимости от задачи, выбираем изолированную сеть либо подключённую к EGW.



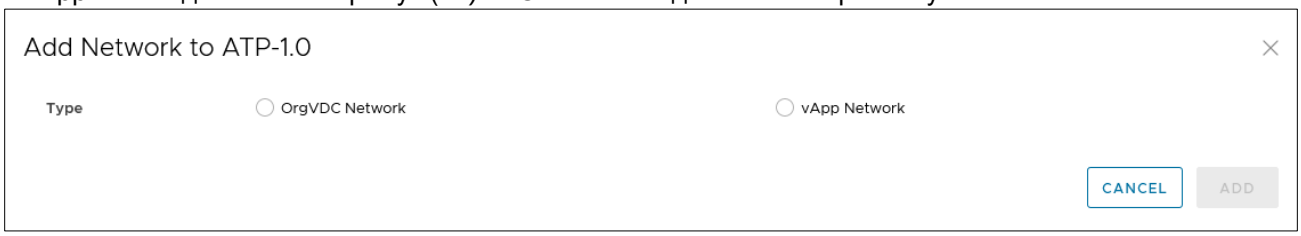
Указываем параметры сети. Если планируется использовать DHCP, необходимо уменьшить на размер пула DHCP-адресов Static IP pool. Если ваша инфраструктура имеет более одного vDC, сеть можно сделать доступной для остальных vDC, для этого необходимо включить параметр:

10.2. Создание vApp сети

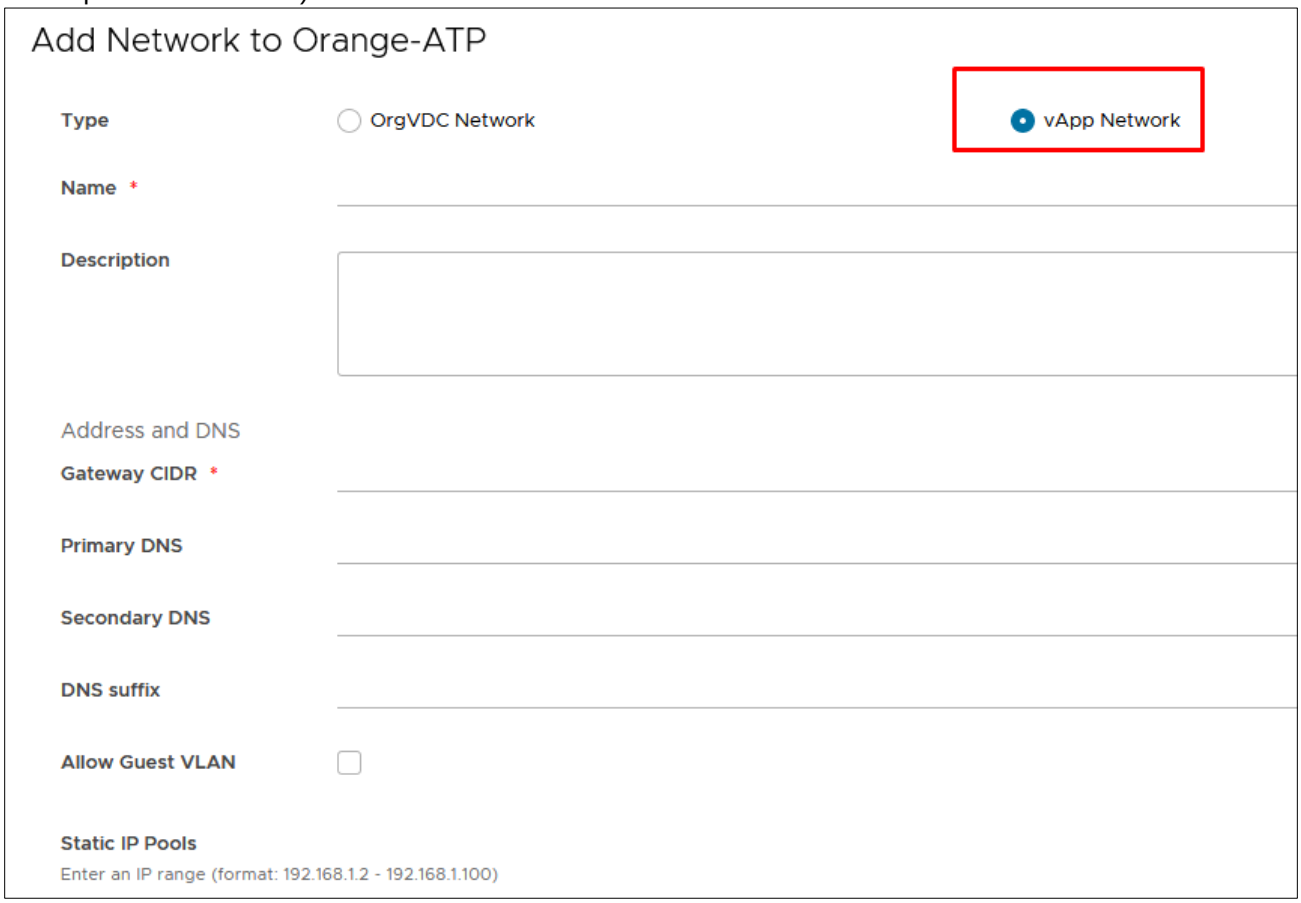
Настройка vApp сети производится из окна vApp (в отличие от vOrg сети).

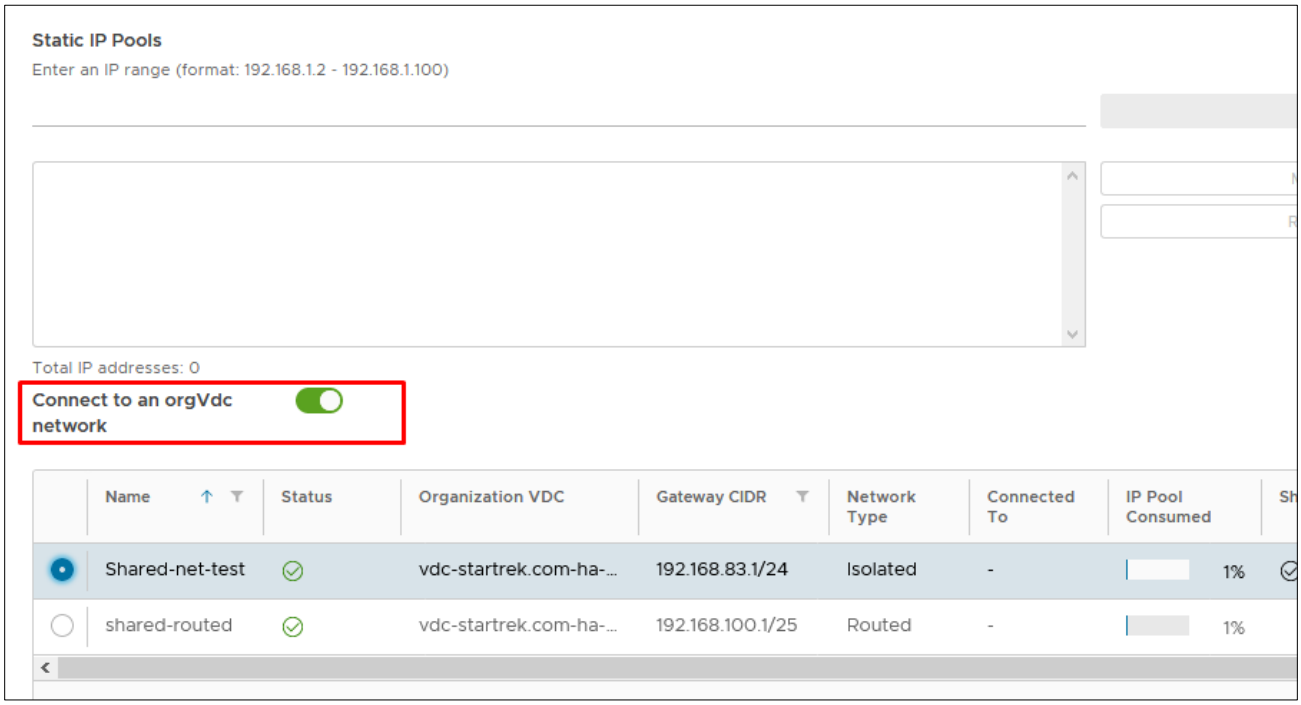


В vApp можно добавить напрямую(L2) vDC сеть или сделать изолированную:

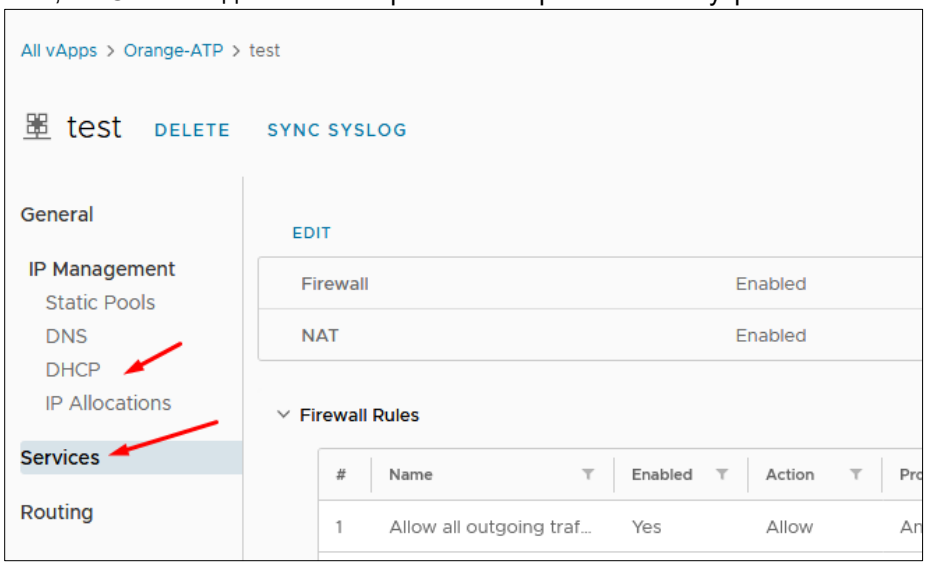


Изолированную сеть vApp можно подключить к сети vOrg сети через «vApp Edge» (добавиться возможность активировать FW и NAT):





NAT, DHCP и FW для такого варианта настраиваются внутри сети:



11. NSX Edge Gateway

11.1. Размеры и производительность NSX Edge Gateway

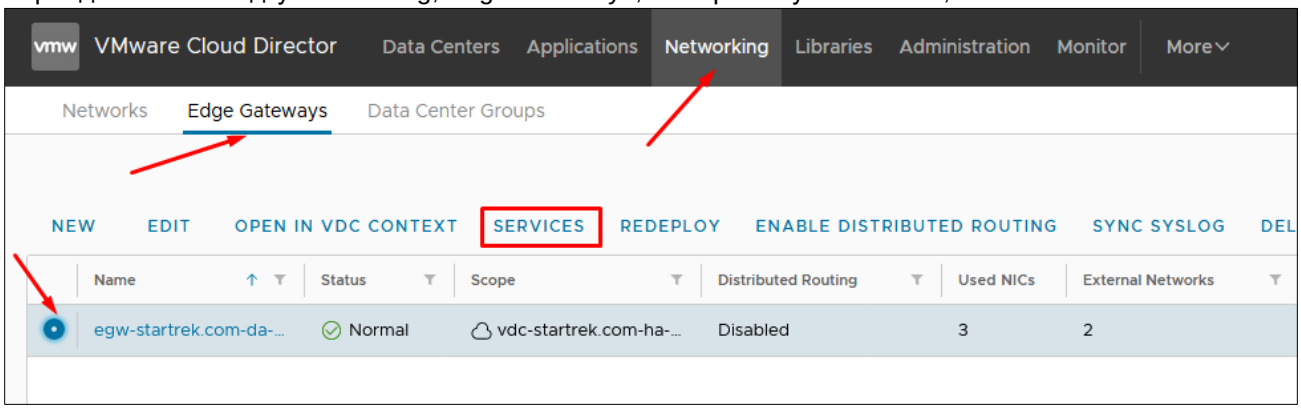
По умолчанию NSX Edge Gateway размер Compact и ограничение на подключение до 5 внутренних клиентских виртуальных сетей. Можно заказать изменение размера NSX Edge Gateway на Large, X-Large и Quad-Large, а также увеличить количество подключаемых сетей и активировать опцию high availability для NSX Edge.
От размера EGW зависит производительность его функций:

	NSX Edge (Compact)	**NSX Edge (Large)**	**NSX Edge (Quad-Large)**	**NSX Edge (X-Large)**
vCPU	1	2	4	6
Memory	512MB	1GB	1GB	8GB
Disk	512MB	512MB	512MB	4.5GB + 4GB
Interfaces	10	10	10	10
Sub Interfaces (Trunk)	200	200	200	200
NAT Rules	2,048	4,096	4,096	8,192
ARP Entries Until Overwrite	1,024	2,048	2,048	2,048
FW Rules	2000	2000	2000	2000
FW Performance	3Gbps	9.7Gbps	9.7Gbps	9.7Gbps
DHCP Pools	20	20,000	20,000	20,000
ECMP Paths	8	8	8	8
Static Routes	2,048	2,048	2,048	2,048
LB Pools	64	64	64	1,024
LB Virtual Servers	64	64	64	1,024
LB Server / Pool	32	32	32	32
LB Health Checks	320	320	320	3,072
LB Application Rules	4,096	4,096	4,096	4,096
L2VPN Clients Hub to Spoke	5	5	5	5
L2VPN Networks per Client/Server	200	200	200	200
IPSec Tunnels	512	1,6	4,096	6
SSLVPN Tunnels	50	100	100	1
SSLVPN Private Networks	16	16	16	16

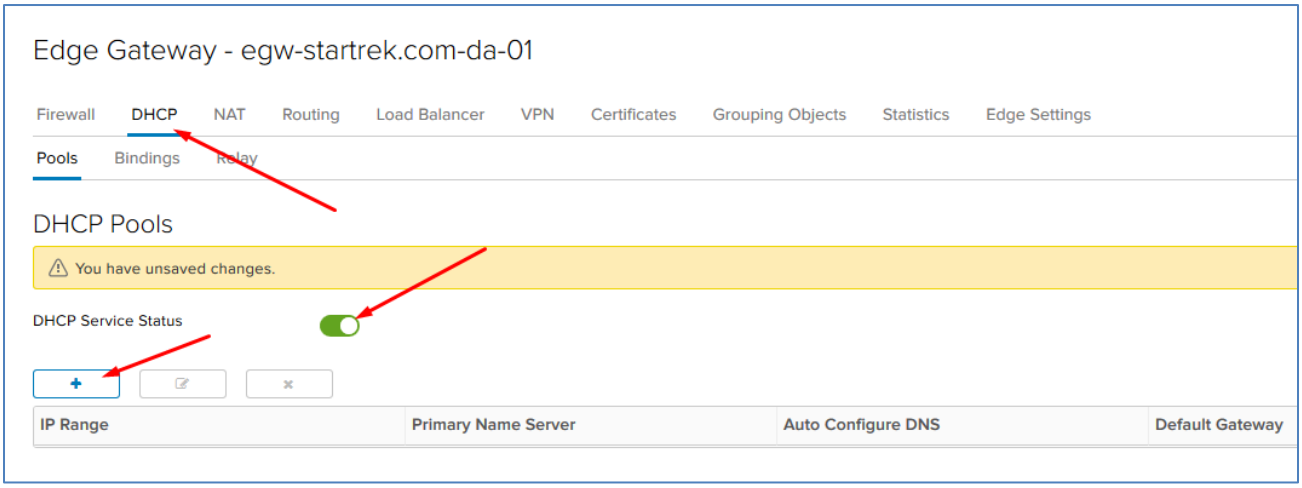
Concurrent Sessions	64	1,000,000	1,000,000	1,000,000
Sessions/Second	8	50	50	50
LB Throughput L7 Proxy)		2.2Gbps	2.2Gbps	3Gbps
LB Throughput L4 Mode)		6Gbps	6Gbps	6Gbps
LB Connections/s (L7 Proxy)		46	50	50
LB Concurrent Connections (L7 Proxy)		8	60	60
LB Connections/s (L4 Mode)		50	50	50
LB Concurrent Connections (L4 Mode)		600	1,000,000	1,000,000
BGP Routes	20	50	250	250
BGP Neighbors	10	20	100	100
BGP Routes Redistributed	No Limit	No Limit	No Limit	No Limit
OSPF Routes	20	50	100	100
OSPF LSA Entries Max 750 Type-1	20	50	100	100
OSPF Adjacencies	10	20	40	40
OSPF Routes Redistributed	2000	5000	20	20
Total Routes	20	50	250	250

11.2. Настройка DHCP

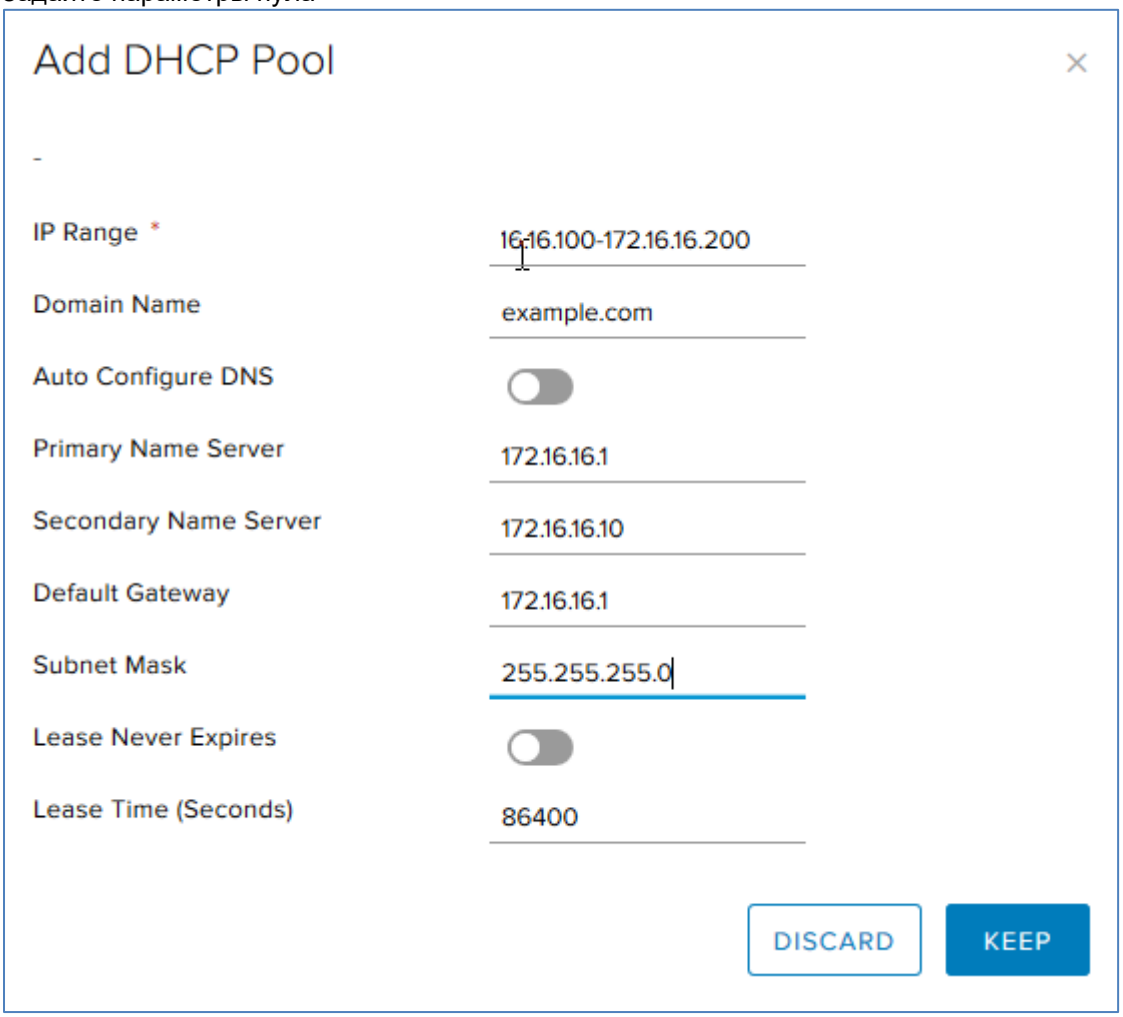
Перейдите на закладку Networking, Edge Gateways, выберите нужный EGW, нажмите Services:



Включите сервис DHCP, нажмите Add

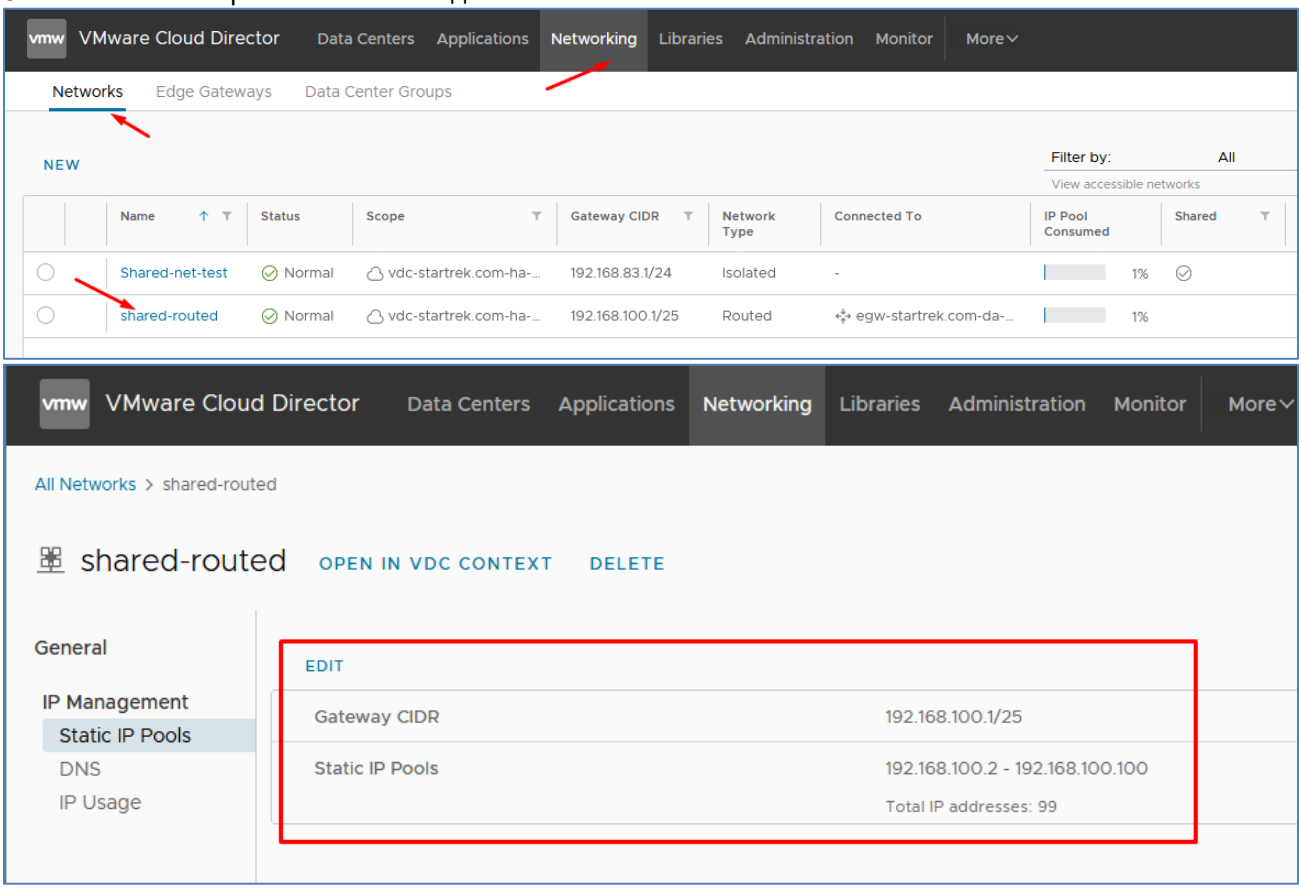


Задайте параметры пула



Внимание: диапазон этих IP адресов не должен пересекаться с Static IP Pool сети уровня организации.

Это можно посмотреть и изменить здесь:

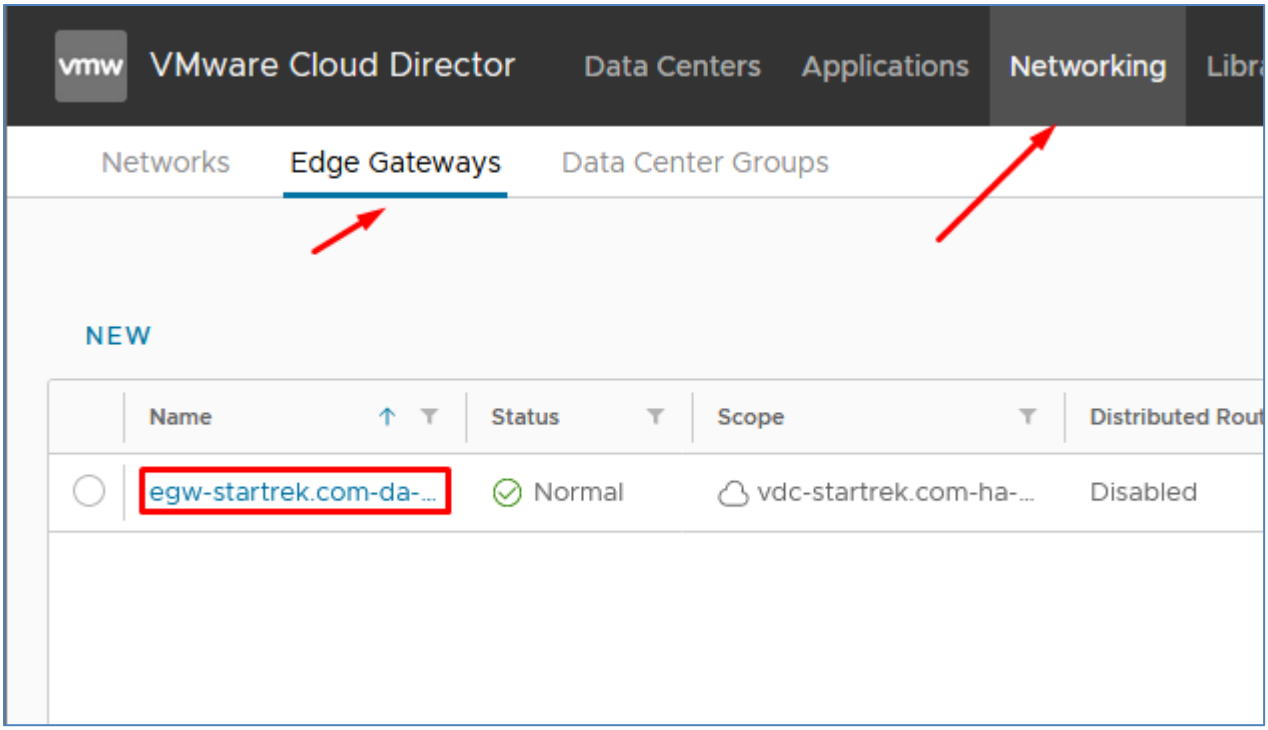


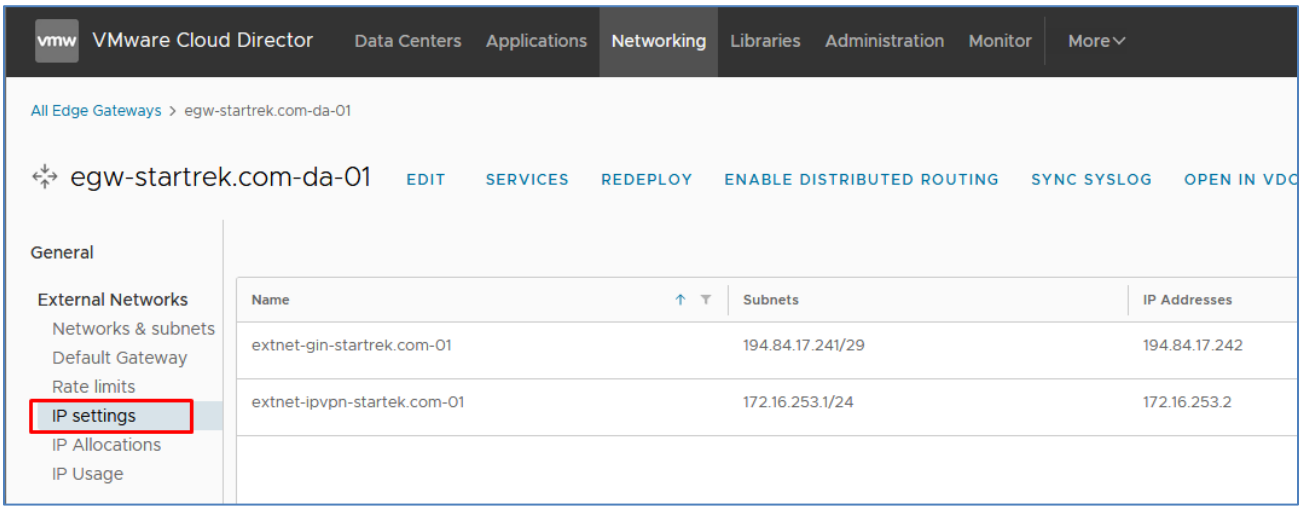
11.3. Настройка NAT

NAT (Network Address Translation) - трансляция приватных («серых», RFC1918) IP-адресов во внешние («белые») и наоборот. Благодаря этому процессу ваша виртуальная машина получает доступ в Интернет. Для настройки этого механизма в Cloud Director нужно настроить правила SNAT и DNAT.

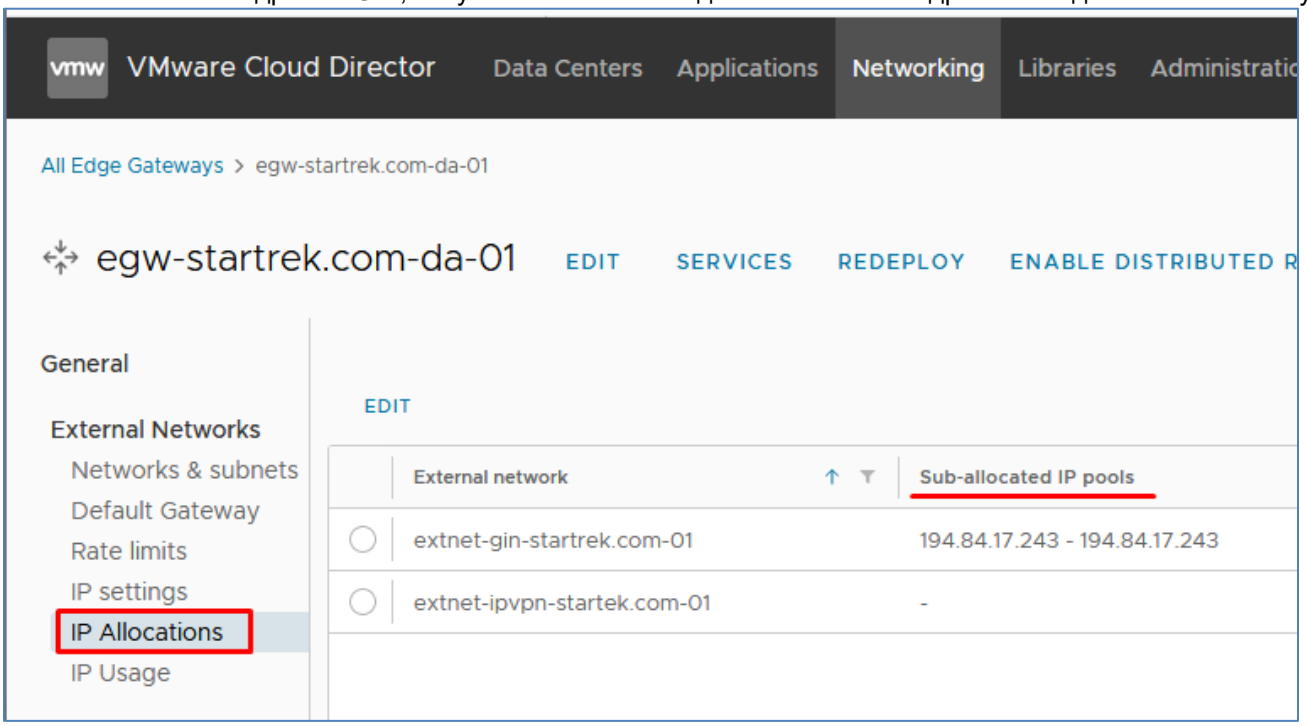
11.3.1. Создание правила SNAT

SNAT (Source Network Address Translation) - механизм, суть которого состоит в замене адреса источника при пересылке пакета.
Перейдите на закладку Administration, выберите свой vDC, вкладка Edge Gateways, нажмите на нужном EGW выберите пункт Edge Gateway Services.

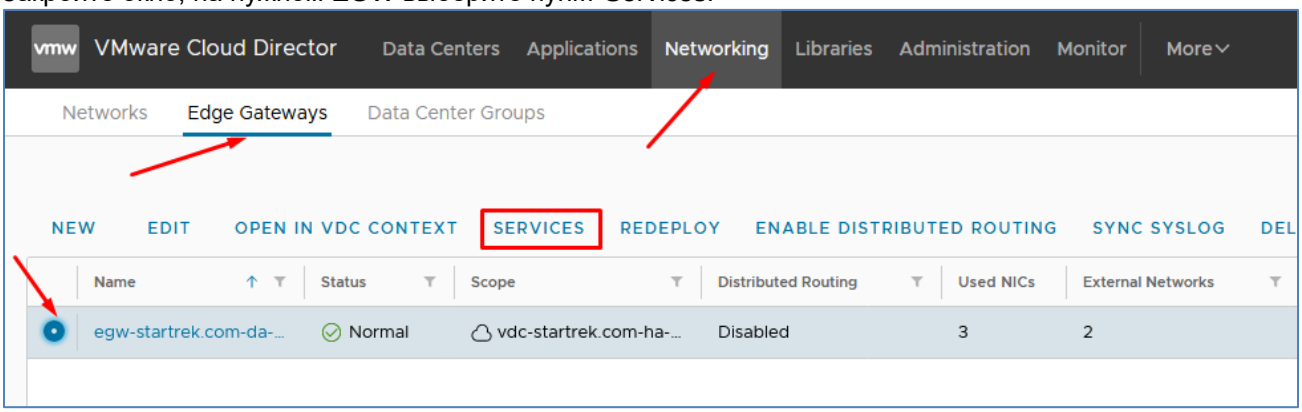




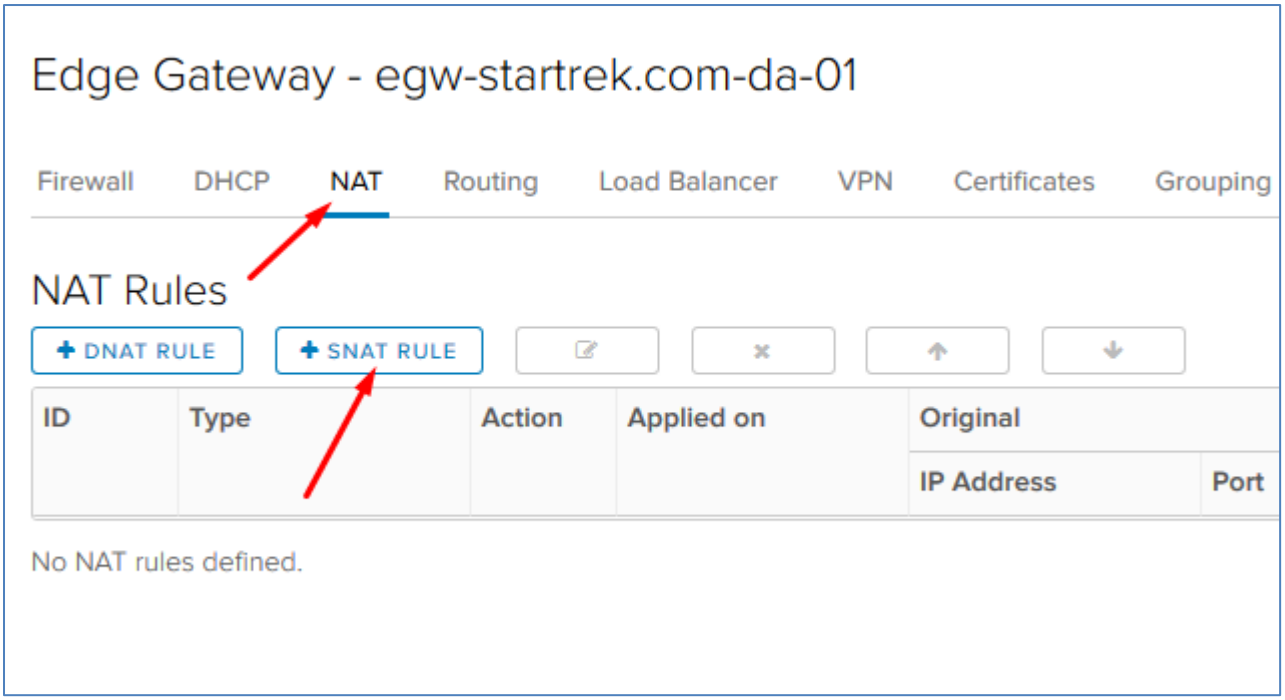
Помимо основного адреса EGW, могут быть назначены дополнительные адреса из подключённых к нему сетей:



Закройте окно, на нужном EGW выберите пункт Services.

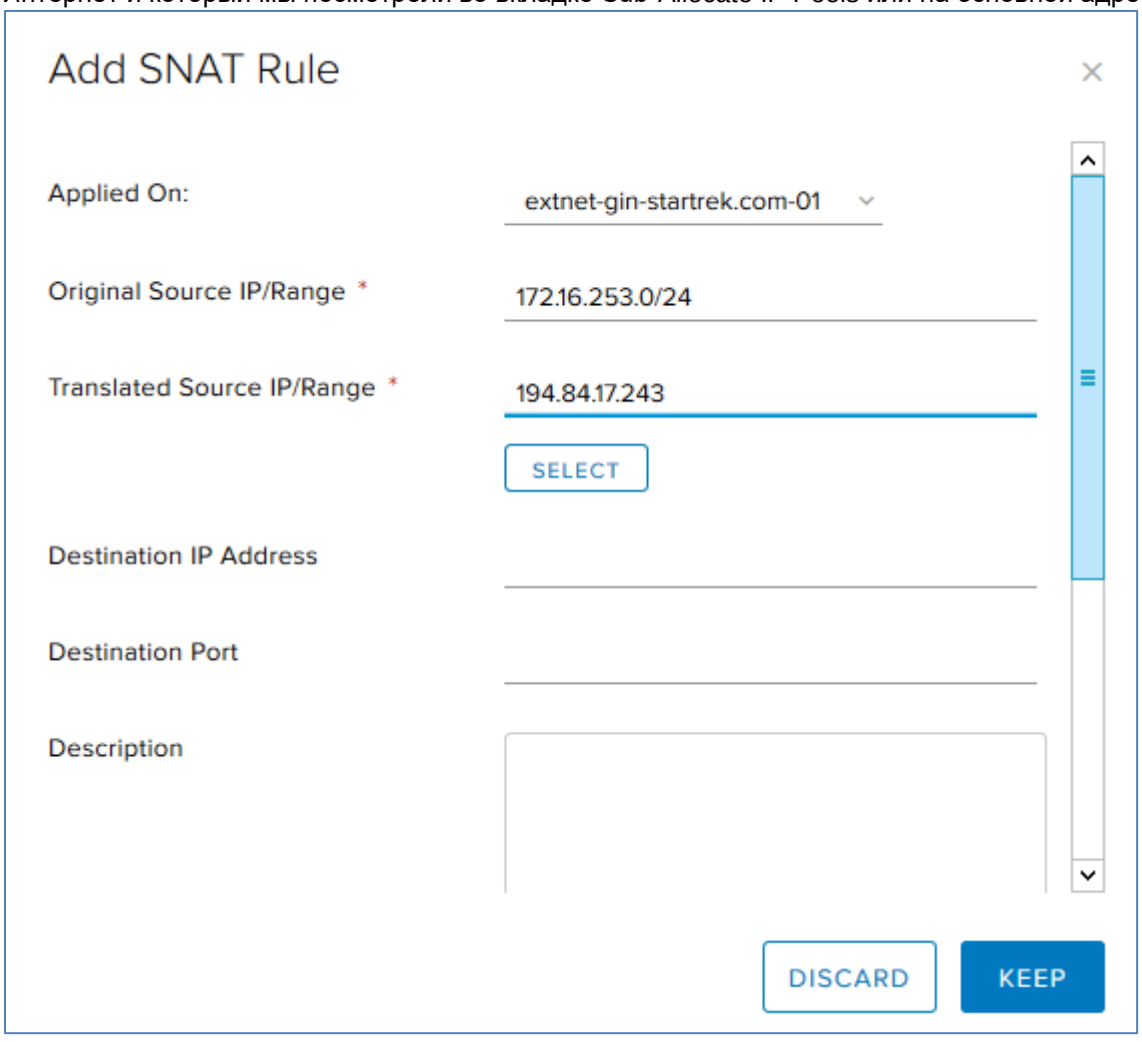


Перейдите на вкладку NAT, нажимаем кнопку Add SNAT



Заполняем параметры

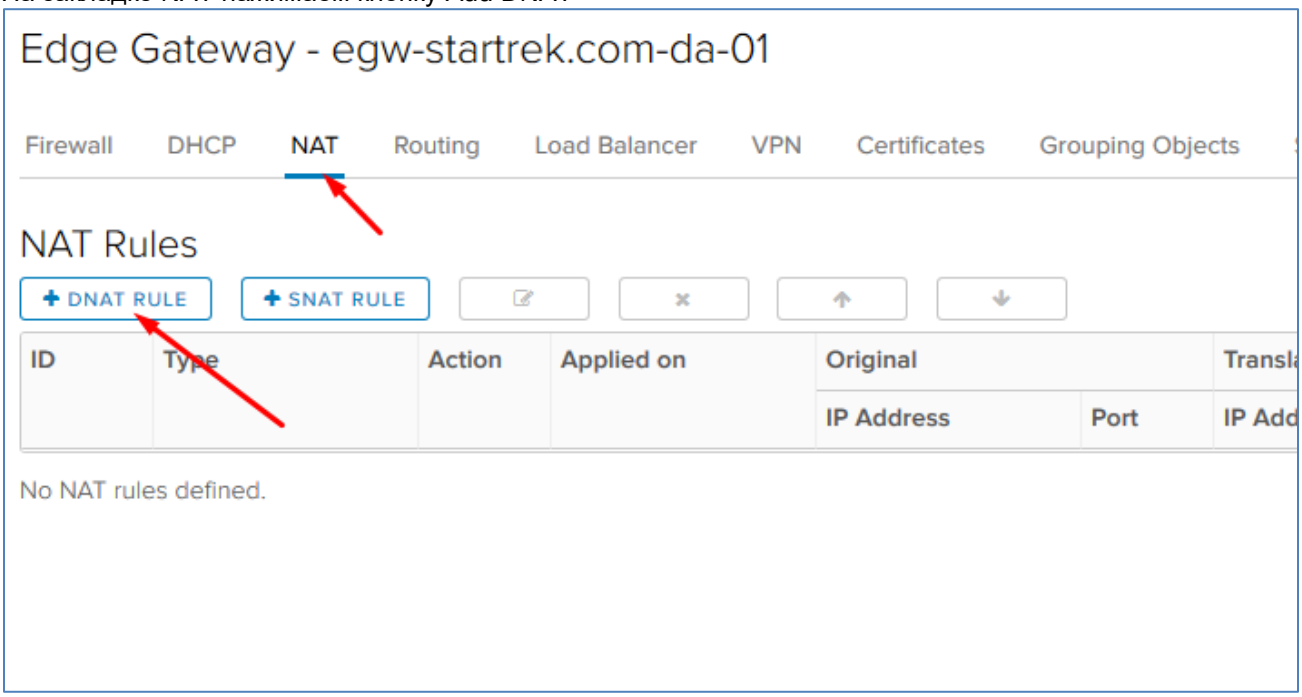
- в поле Applied on указываем внешнюю сеть (вида extnet-gin-DOMAIN-XX);
- в поле Original source IP/range указываем внутренний диапазон адресов, например 172.16.253.0/24;
- в поле Translated source IP/range внешний адрес, через который будет осуществляться выход в Интернет и который мы посмотрели во вкладке Sub-Allocate IP Pools или на основной адрес.



11.3.2. Создание правила DNAT

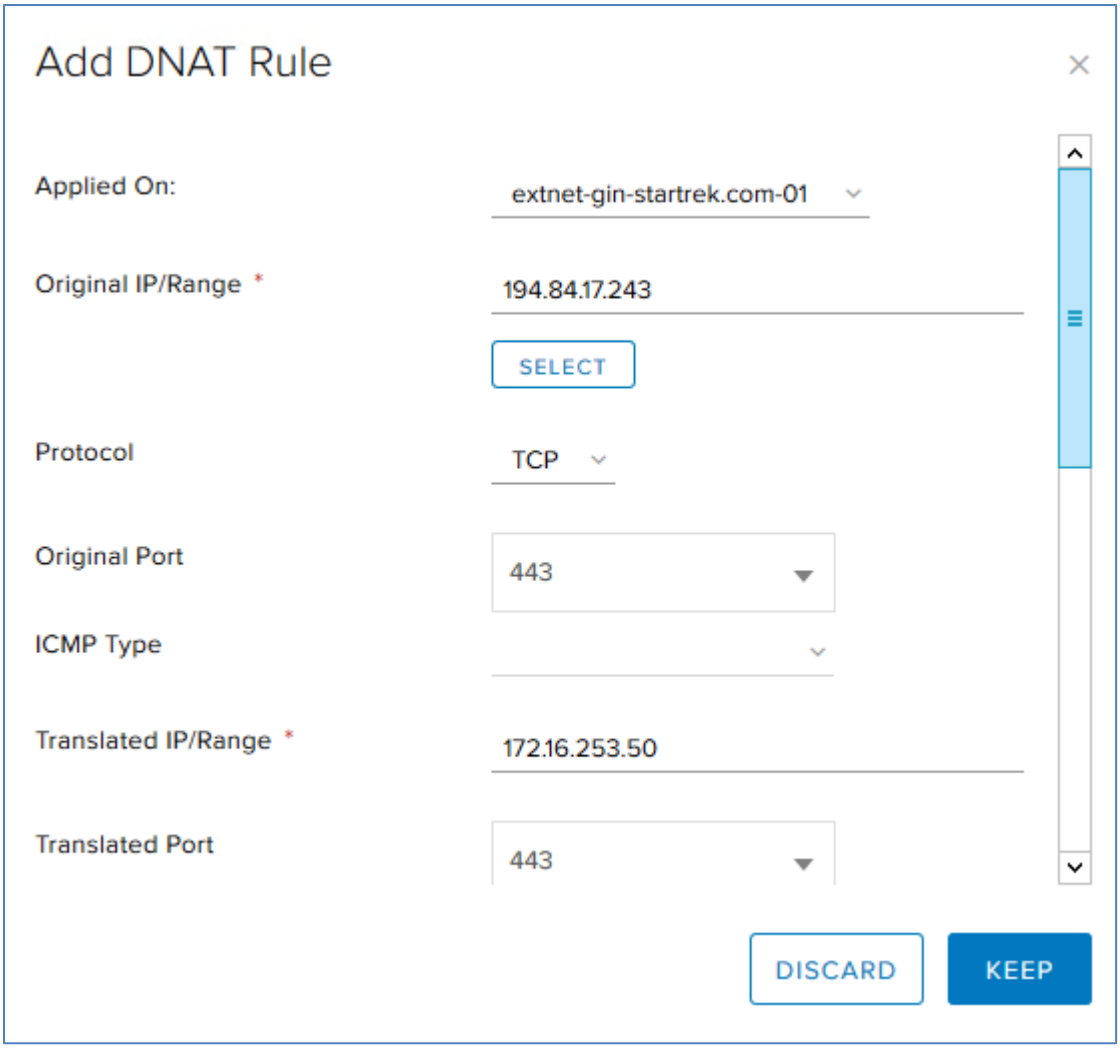
DNAT- механизм, изменяющий адрес назначения пакета, а также порт назначения. Используется для перенаправления входящих пакетов с внешнего адреса/порта на приватный IP-адрес/порт внутри частной сети.

На закладке NAT нажимаем кнопку Add DNAT



Заполняем параметры:

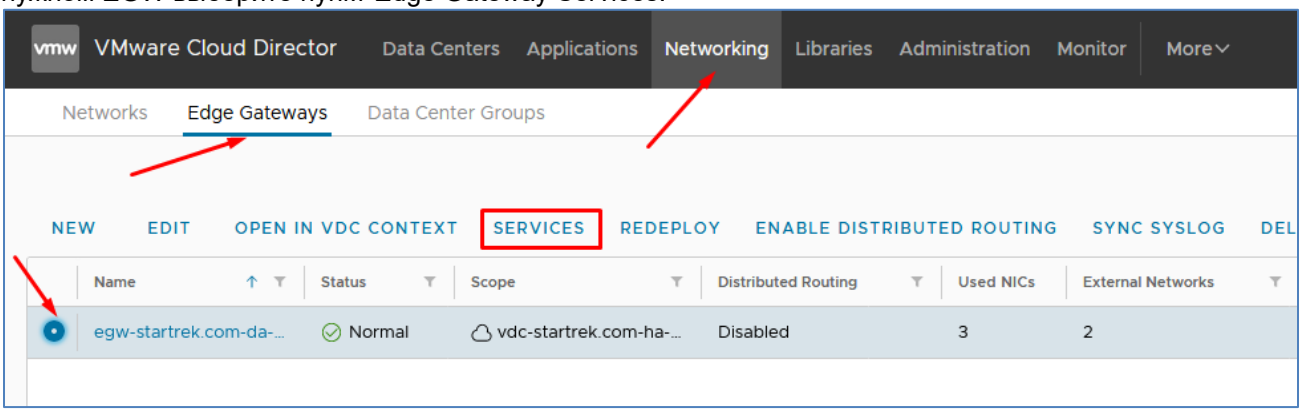
- в поле Applied on указываем внешнюю сеть (вида extnet-gin-DOMAIN-XX);
- в поле Description указываем описание правила DNAT;
- в поле Original IP/range указываем внешний адрес (адрес из диапазона Sub-Allocate IP Pools);
- в поле Protocol - протокол;
- в поле Original Port – порт на внешнем интерфейсе;
- в поле Translated IP/range - укажите внутренний IP-адрес, например 172.16.253.50
- в поле Translated port – порт назначения на внутреннем сервере



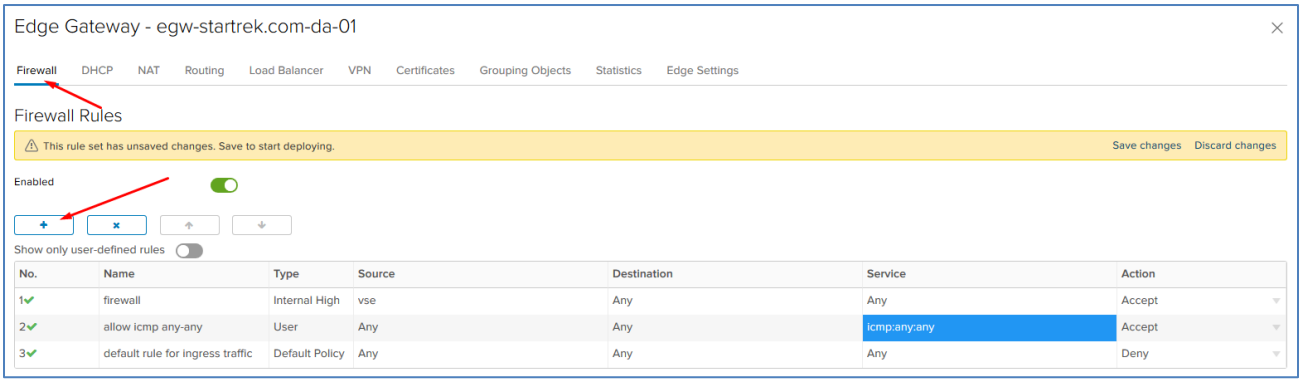
После этого необходимо настроить Firewall на пропуск соответствующих пакетов.

11.4. Настройка Firewall

Перейдите на закладку Administration, выберите свой vDC, вкладка Edge Gateways, нажмите правой кнопкой на нужном EGW выберите пункт Edge Gateway Services.

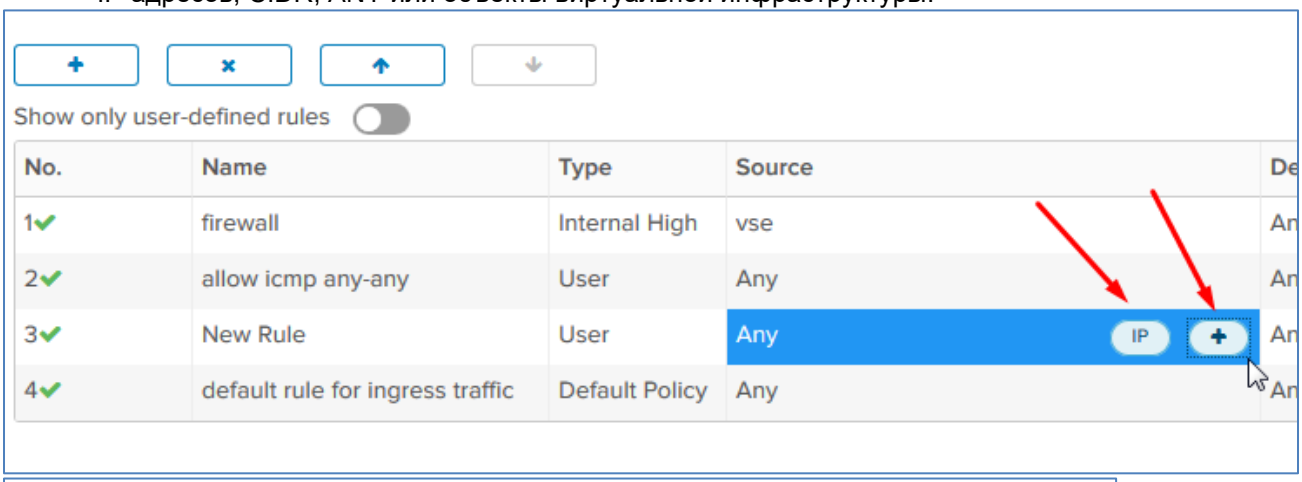


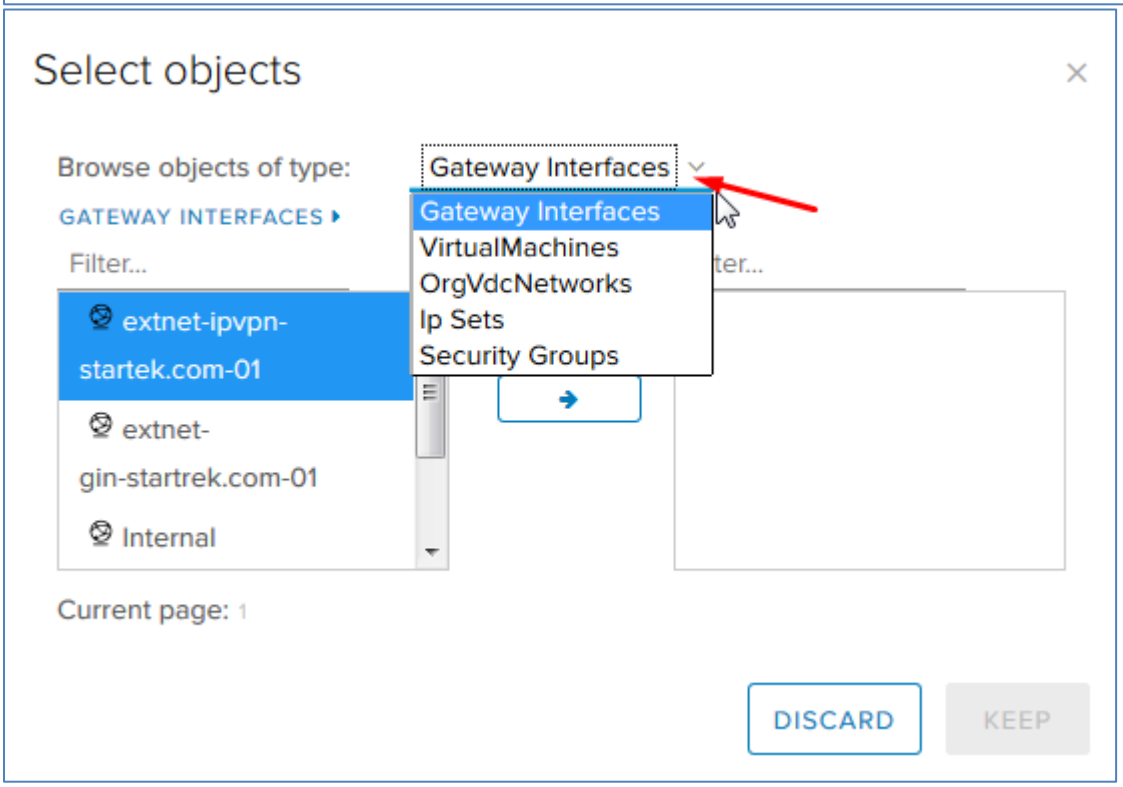
В появившемся окне Services перейдите во вкладку Firewall, нажмите Add.
По умолчанию в пункте Default action выбрана опция Deny, т. е. Firewall будет блокировать весь трафик. Чтобы этого не происходило нужно настроить правила.



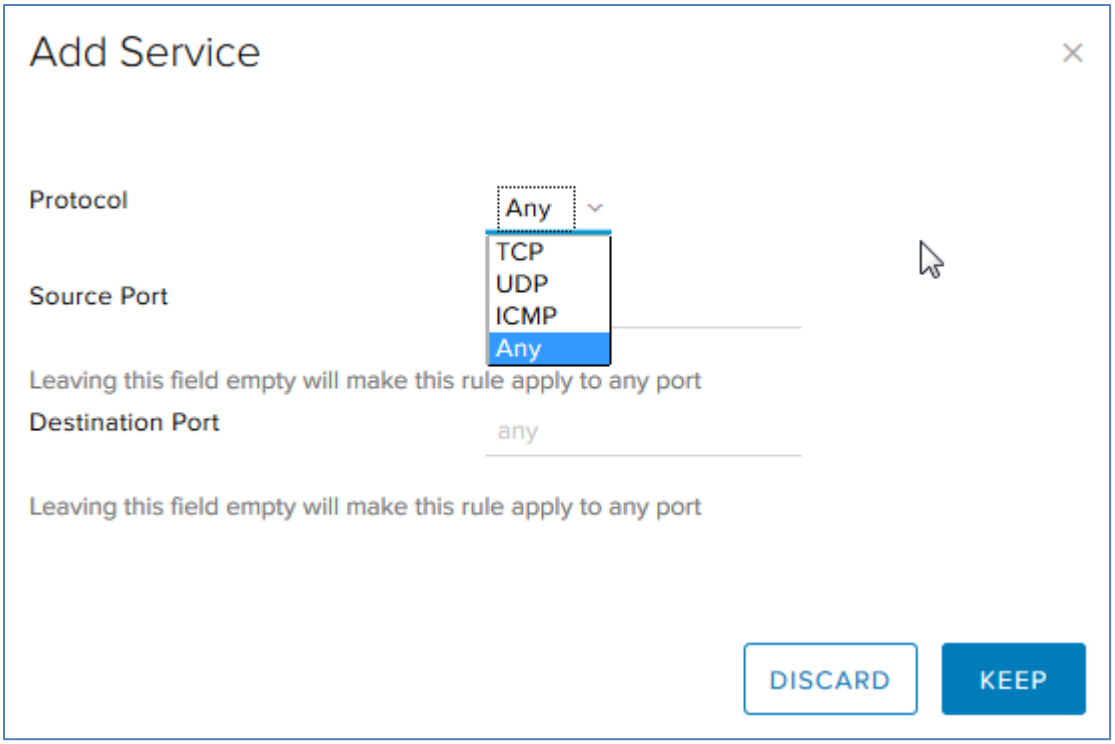
Заполните параметры нового правила:

- в поле Name (Название) задайте название правила;
- в поле Source (Источник) введите необходимые адреса источника: единичный IP-адрес, диапазон IP-адресов, CIDR, ANY или объекты виртуальной инфраструктуры:



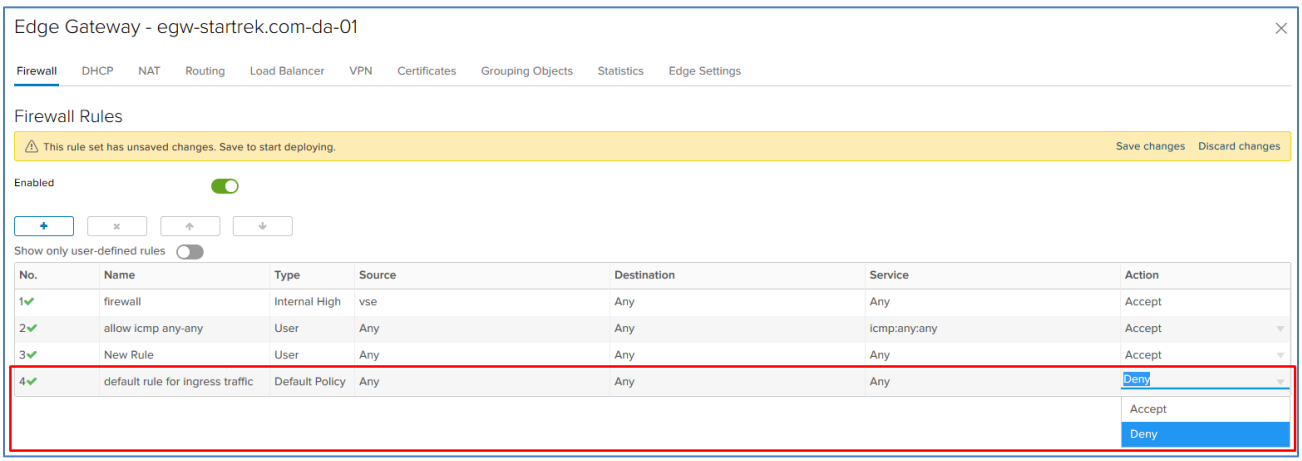


- в поле Destination укажите адрес получателя. В таком же формате, как и для поля Source;
- в поле Service выберите протоколы и порты получателя. Можно оставить Any, например, для 1-1 NAT



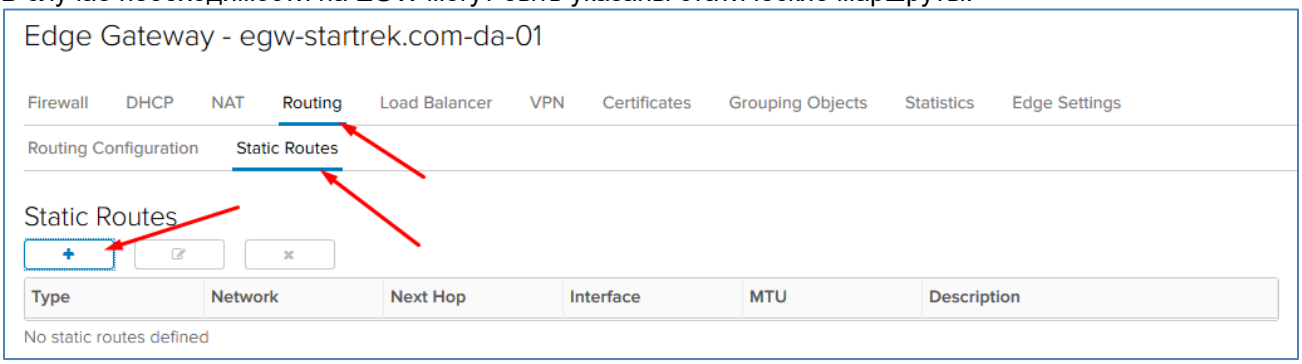
- в поле Action выберите необходимое значение (allow - разрешить, deny - запретить).

Внимание: если в глобальной политике Firewall задано Allow, то в правиле FW задаются параметры сессий, которые Firewall будет блокировать. Для этого в окне правила нужно выбрать опцию Deny. Если в глобальной политике выставлена опция Deny, то в правиле задаются параметры сессий, который Firewall будет пропускать.



11.5. Настройка Static routing

В случае необходимости на EGW могут быть указаны статические маршруты.



11.6. Балансировщик нагрузки (Load Balancer)

Балансировщик является достаточно сложным сервисом, предоставляемым NSX Edge Gateway, поэтому Orange рекомендует ознакомится с документацией VMware и составить план конфигурации LB.

Для начала настройки балансировщика необходимо выбрать внешние IP-адреса (Sub-Allocated IP Pools, см. выше) и внутренние адреса серверов.
Перейдите на закладку Administration, выберите свой vDC, вкладка Edge Gateways, нажмите правой кнопкой на нужном EGW выберите пункт Edge Gateway Services.
Далее следует руководствоваться планом конфигурации и разделом документации «Load Balancing».

11.7. VPN

NSX Edge Gateway предоставляет следующие типы VPN-каналов:

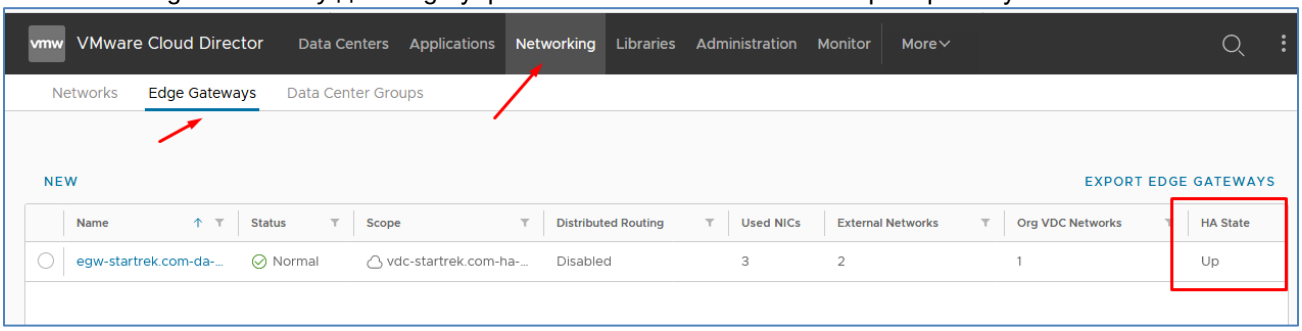
- SSL VPN-Plus, позволяет удаленным пользователям получать доступ к корпоративным приложениям работающим в облаке;

- IPsec VPN, обеспечивает межсетевое соединение между пограничным шлюзом NSX Edge Gateway и удаленными узлами, которые также могут быть NSX Edge Gateway или любым другим аппаратным/программным маршрутизатором или VPN-шлюзом, поддерживающим стандарт IPSEC. Доступны два варианта:
  - Policy-Based IPSec VPN – простой вариант для каналов без резервирования;
  - Route-Based IPSec VPN – позволяет выполнять резервирование каналов IPSec через VTI и BGP.
- L2 VPN, можно использовать для расширения имеющейся физической локальной сети в облако без перенумерации (смены) IP-адресов серверов при переносе между сегментами. L2 VPN туннель устанавливается только между двумя VMware Edge Gateway.

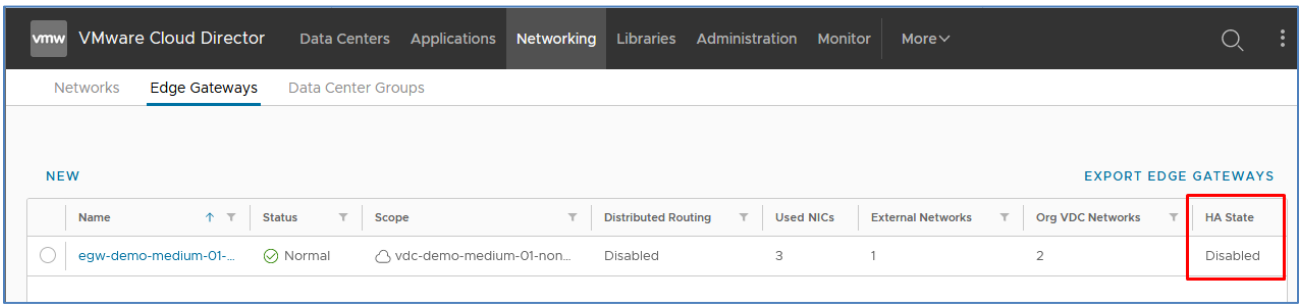
Подробнее можно ознакомиться в разделе документации Virtual Private Networks (VPN).

11.8. NSX Edge High Availability

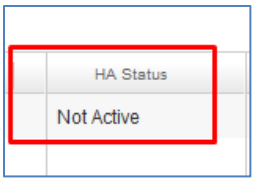
Состояние High Availability для Edge управляемого клиентом можно проверить тут:



«Up» – HA включён.



«Disabled» – отключено.



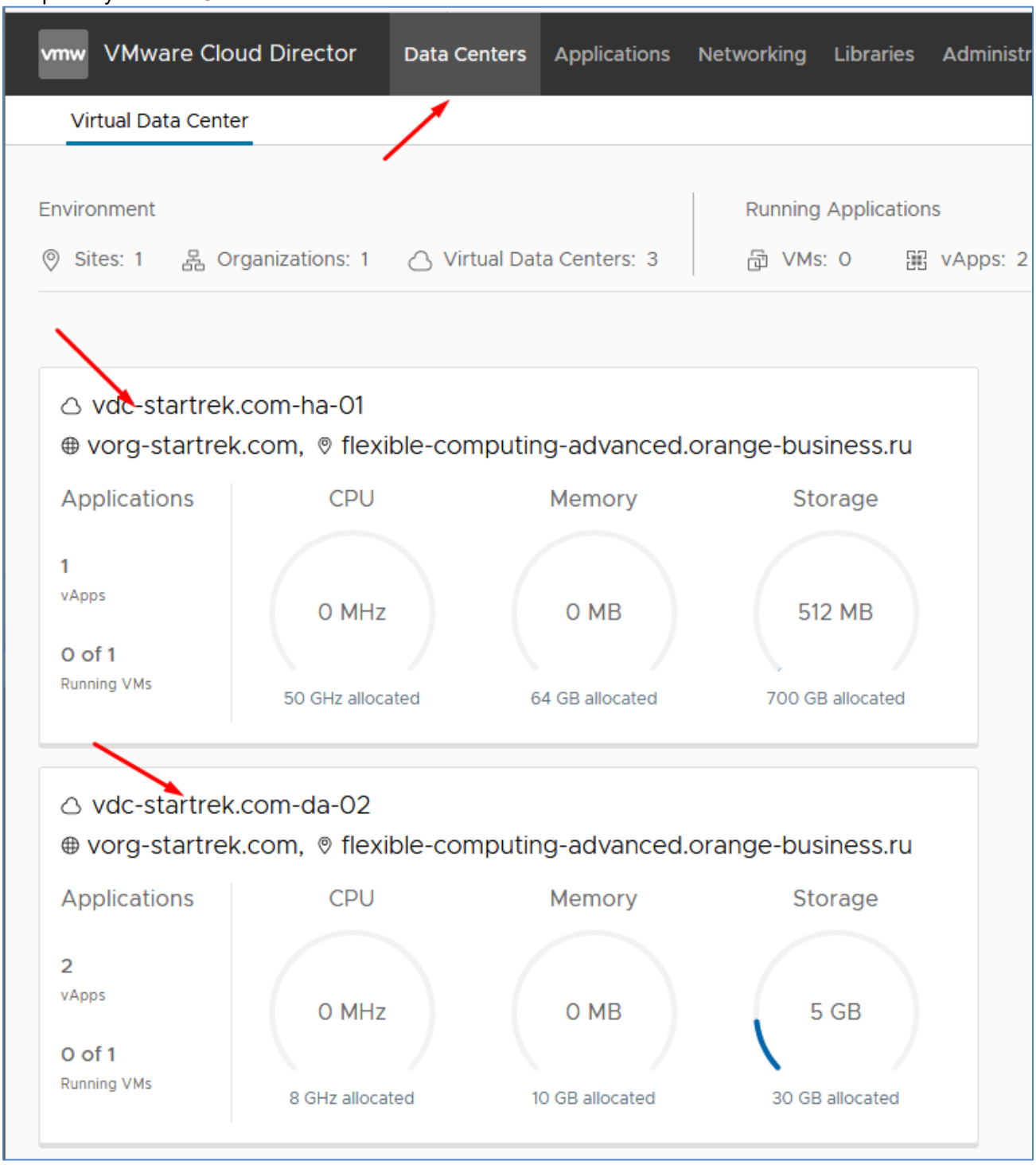
«Not active» – конфигурация HA включена, но не активна.
Примечание: Для включения режима HA, к Edge должна быть подключена хотя-бы одна внутренняя сеть – она будет использоваться для heartbeat.

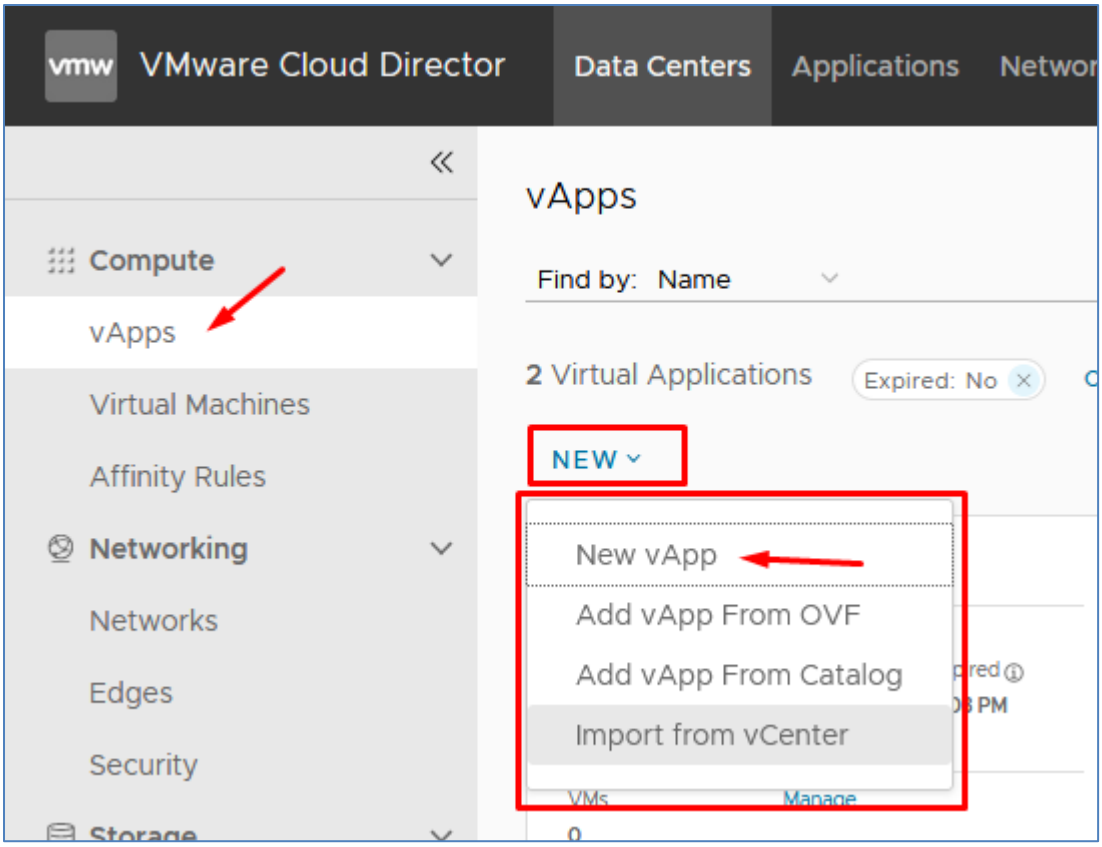
12. Настройка и управление виртуальными машинами и vApp

12.1. Создание нового vApp

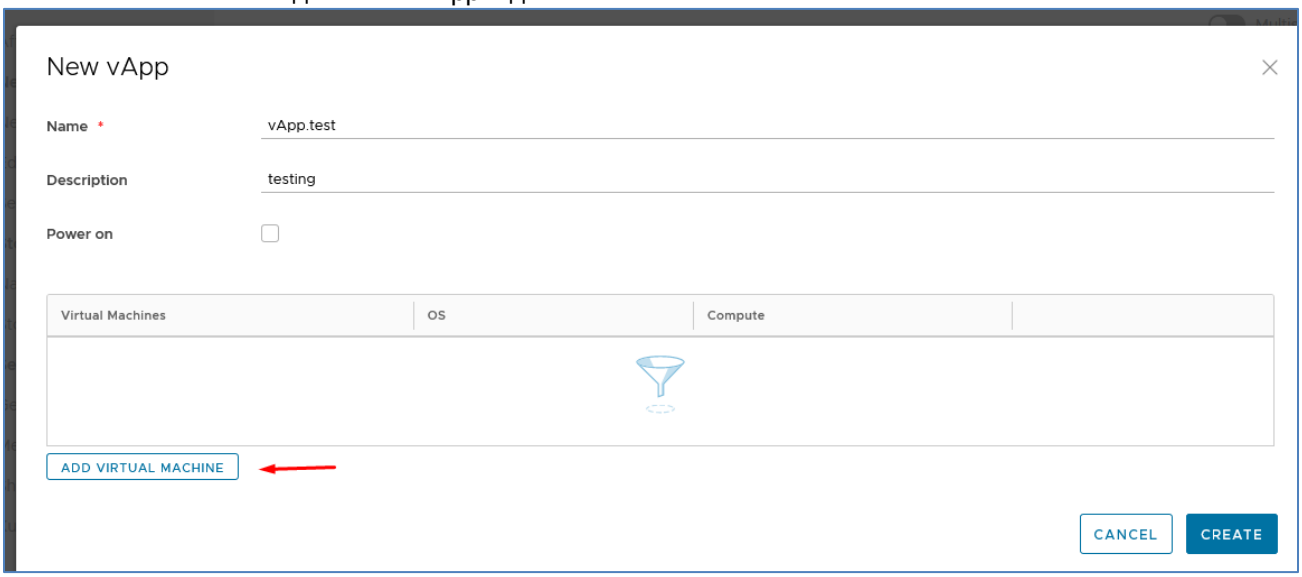
Новый vApp можно создать пустым, из шаблона vApp или с пустой ВМ (без ОС).
Далее рассмотрим процесс создания vApp с пустой ВМ.

Выбрать нужный vDC:

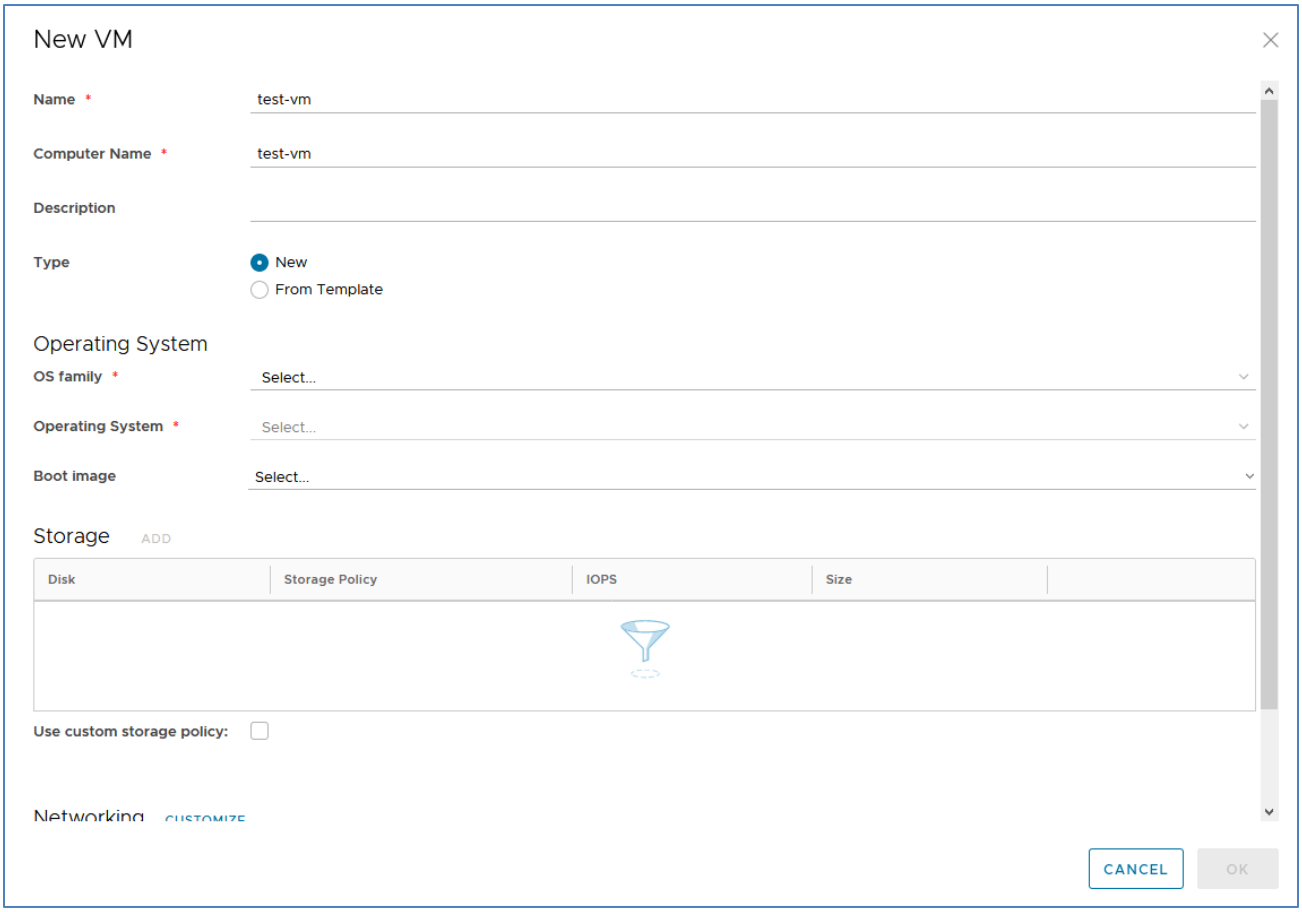




В появившемся окне задаем имя vApp и добавляем ВМ:



В появившемся окне задаем имя vApp и добавляем ВМ.

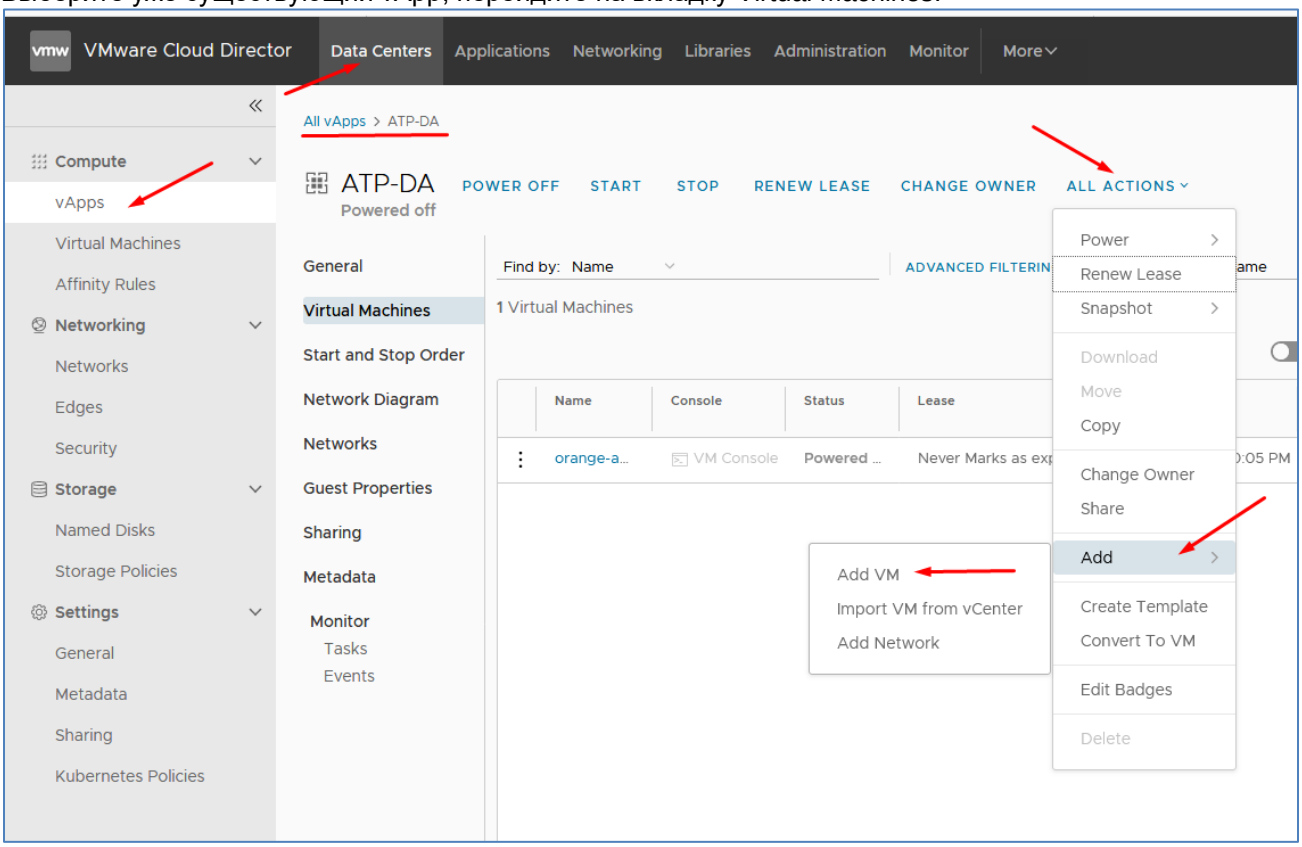


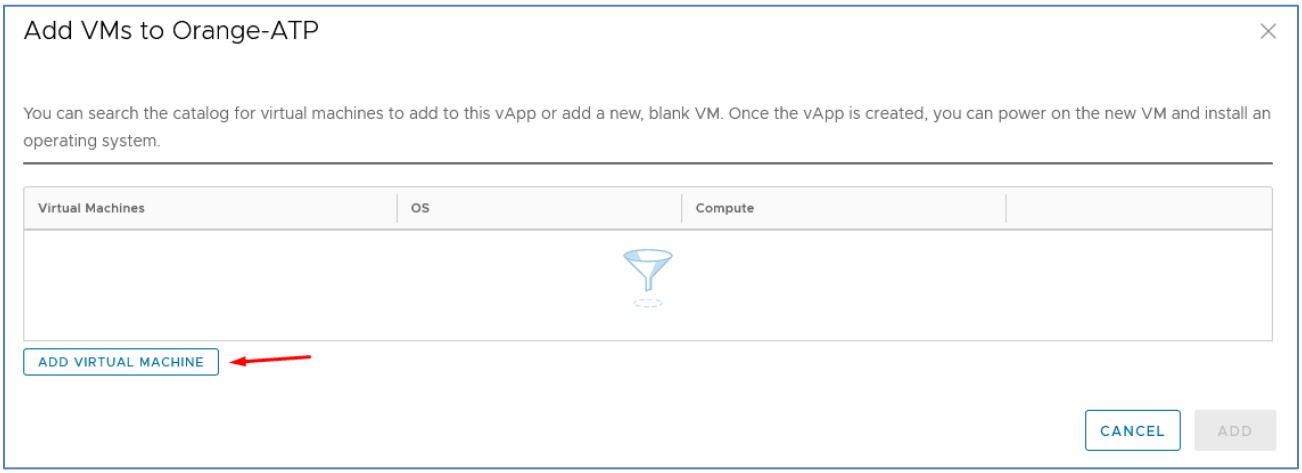
Во вкладке Add Virtual Machines вы можете:

- добавить шаблон виртуальной машины из каталога
- создать виртуальную машину с нуля и указать загрузочный ISO
- оставить vApp пустым и импортировать туда шаблон виртуальной машины или образ позже

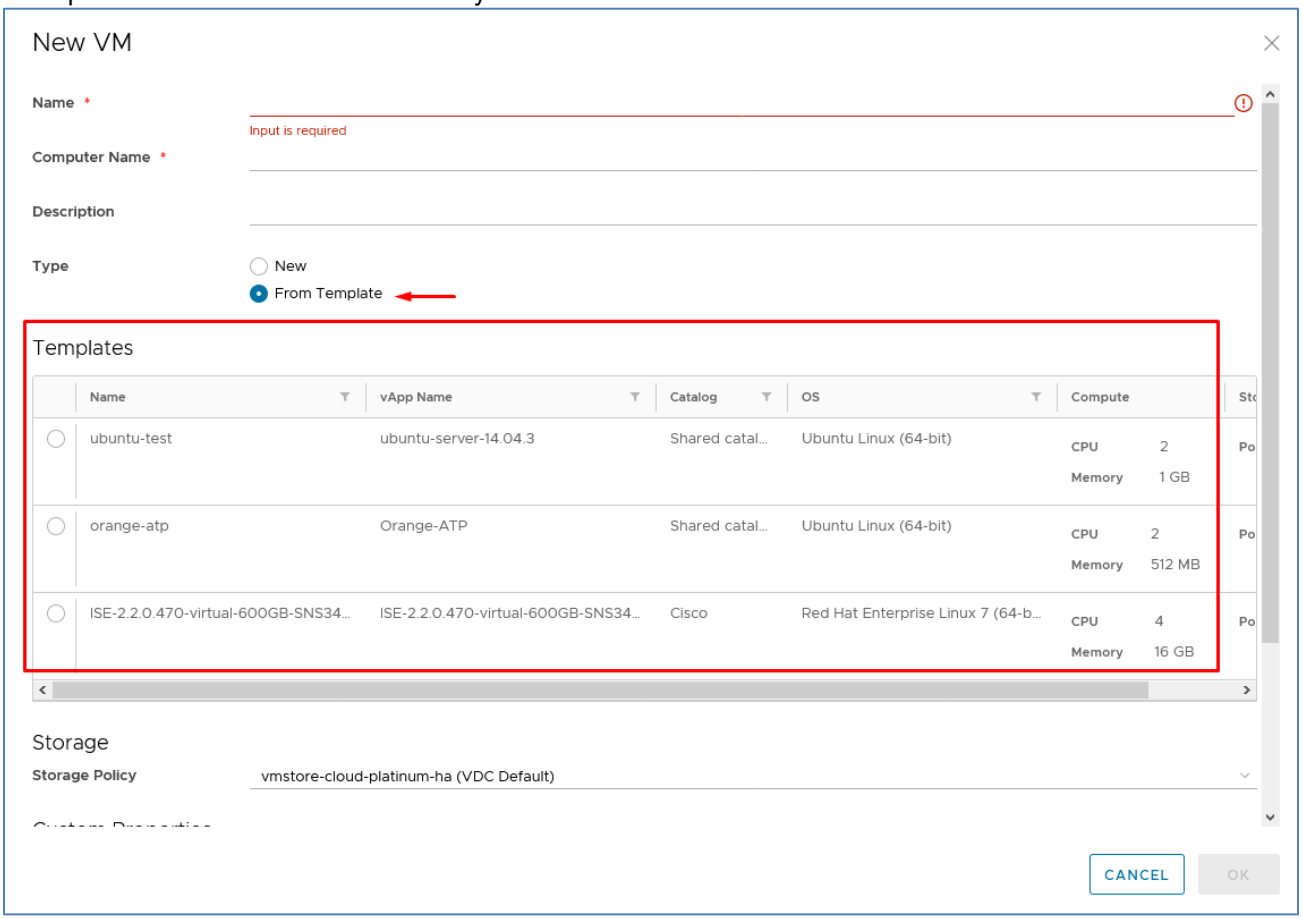
12.2. Создание виртуальной машины из шаблона

Выберите уже существующий vApp, перейдите на вкладку Virtual Machines:

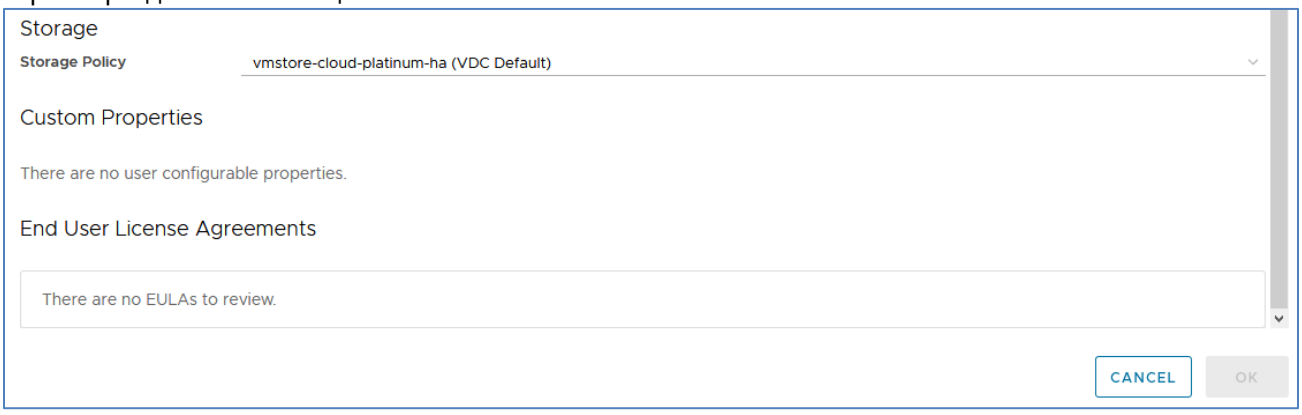




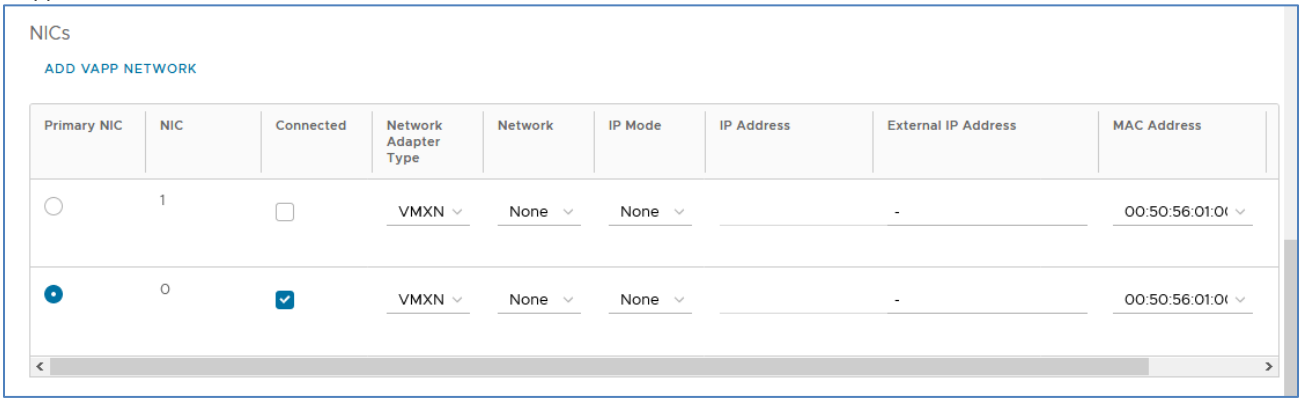
Выберите шаблон ВМ из своего или публичного каталога:



Далее задайте место хранения ВМ и прочие параметры. В зависимости от типа шаблона доступны те или иные параметры для кастомизации ВМ:

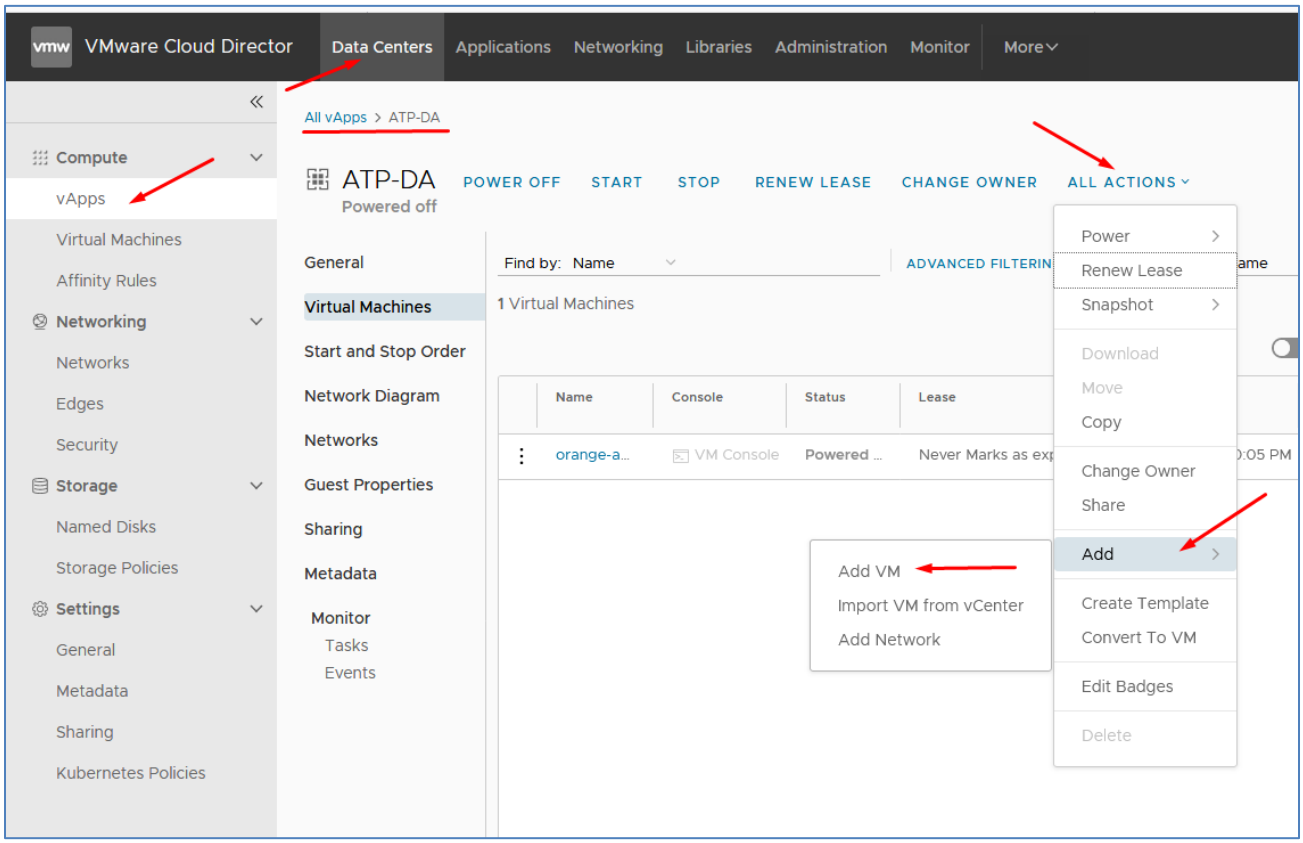


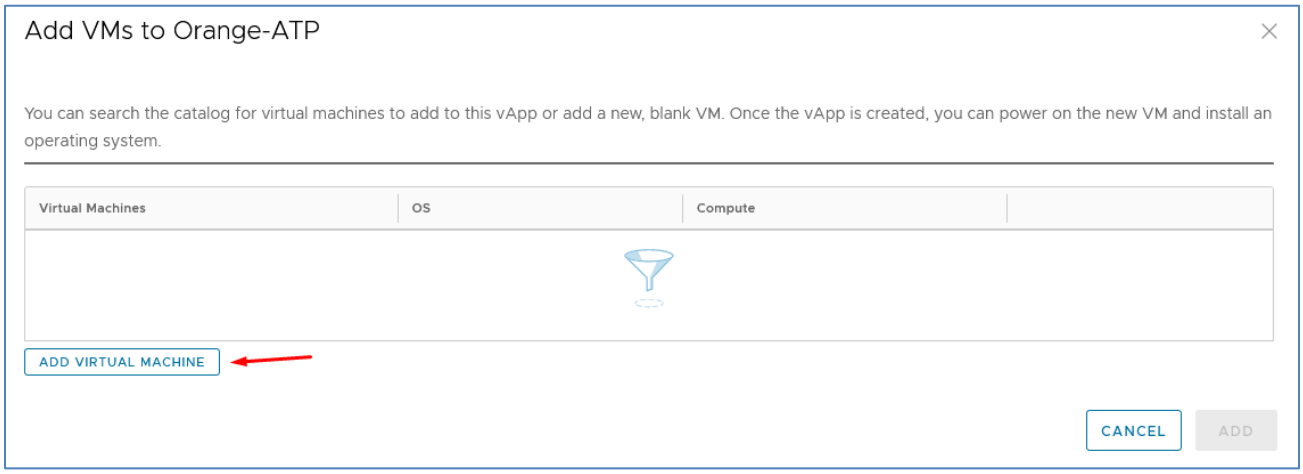
Подключение к сетям:

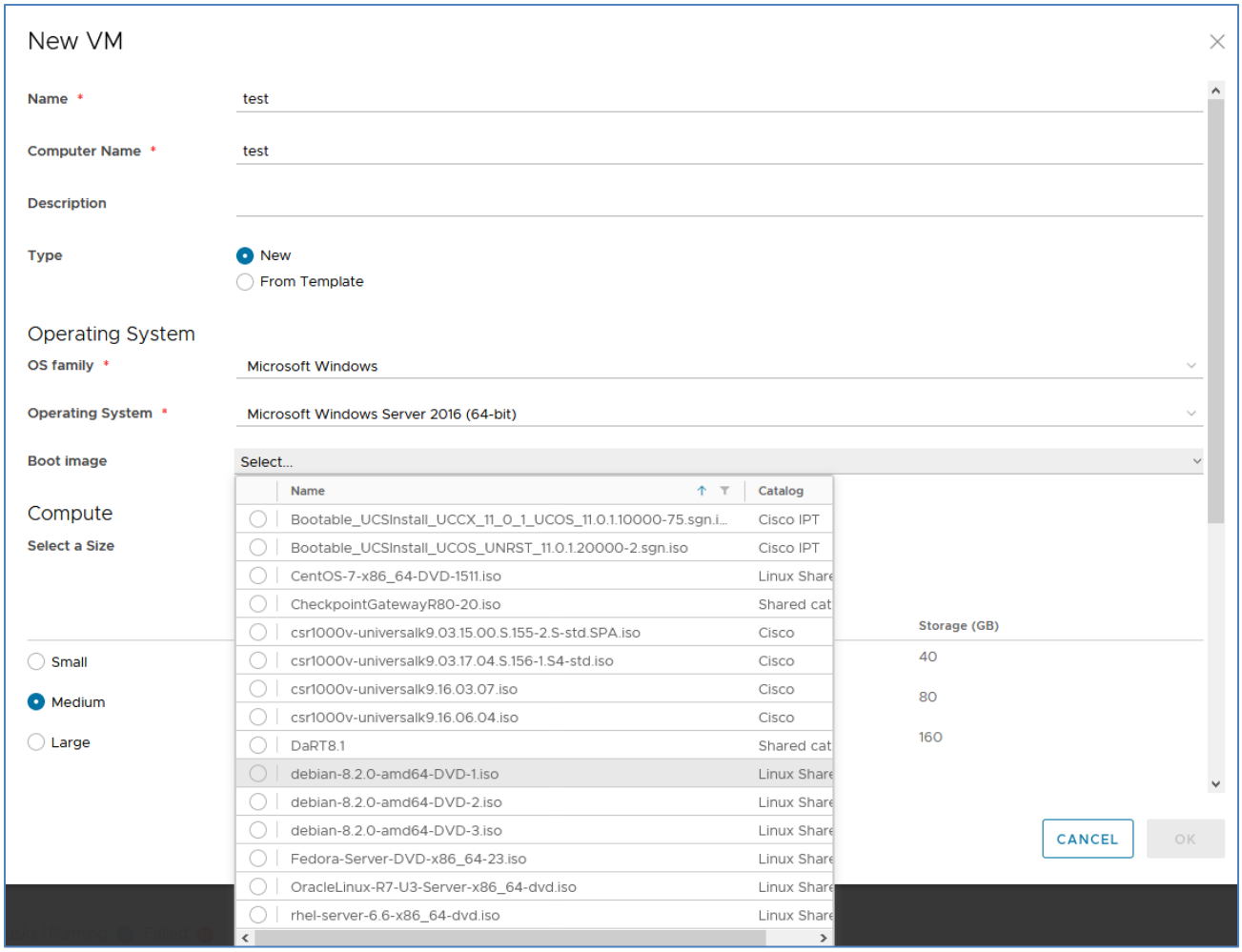


Проверьте параметры и завершите создание ВМ кнопкой Finish.

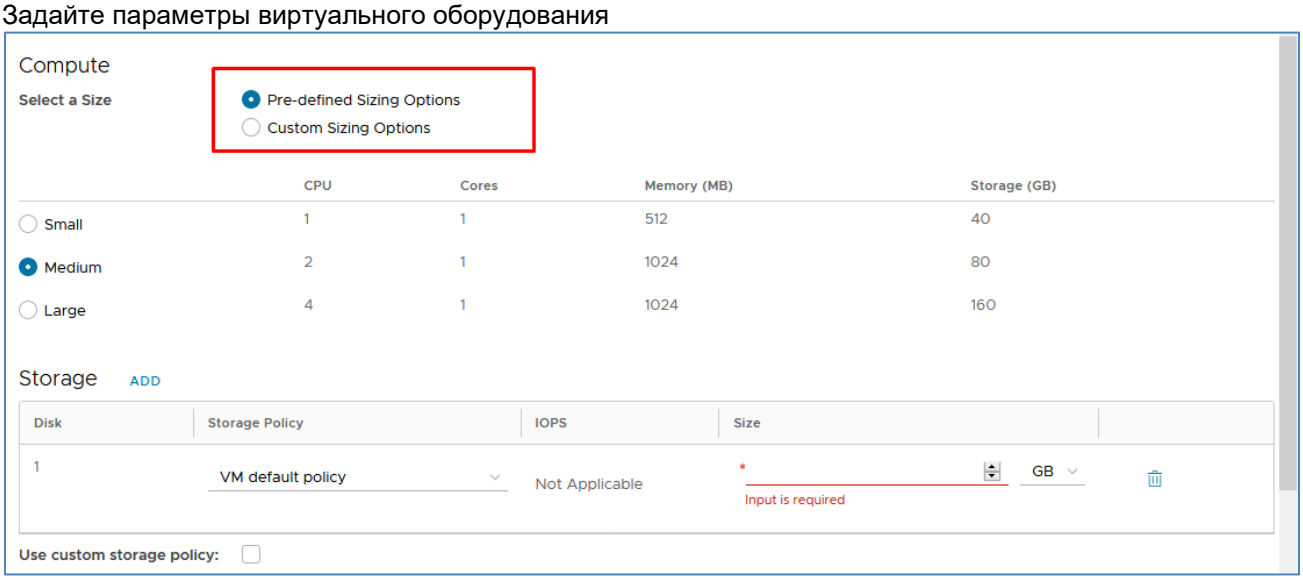
12.3. Создание виртуальной машины «с нуля»



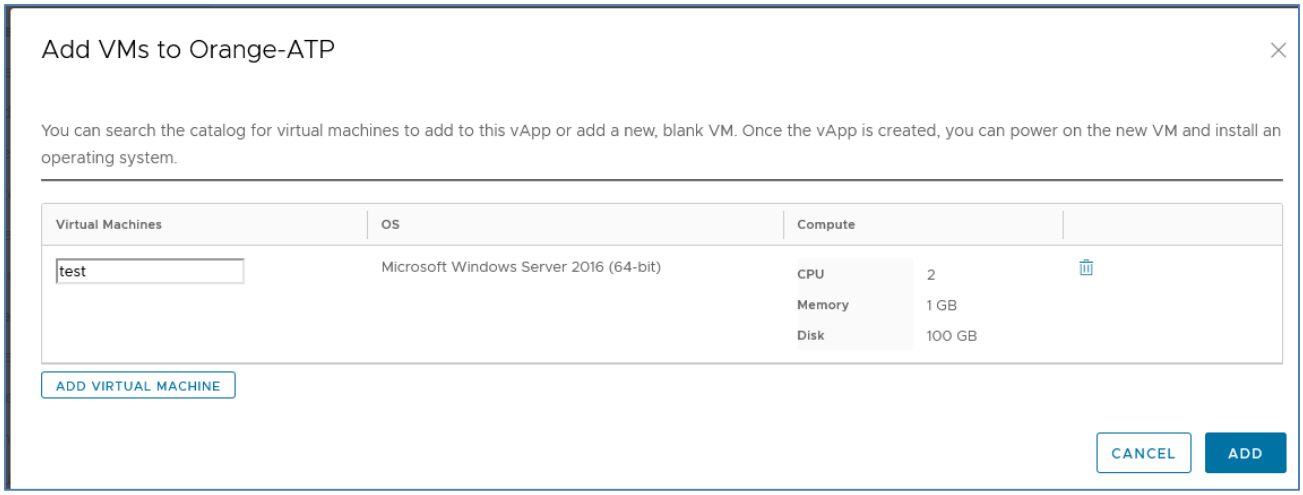




Задайте параметры виртуального оборудования



Новая ВМ появиться в списке



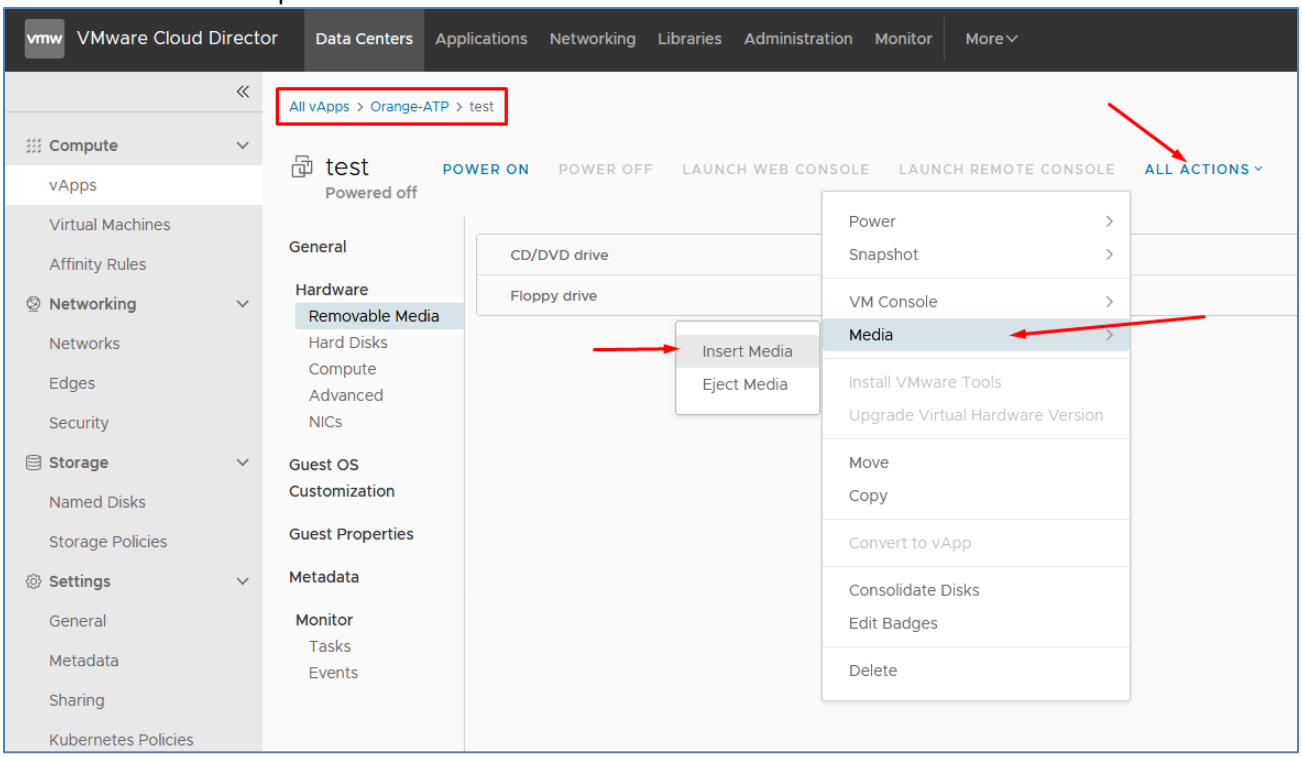
Можно сразу добавить ещё ВМ.

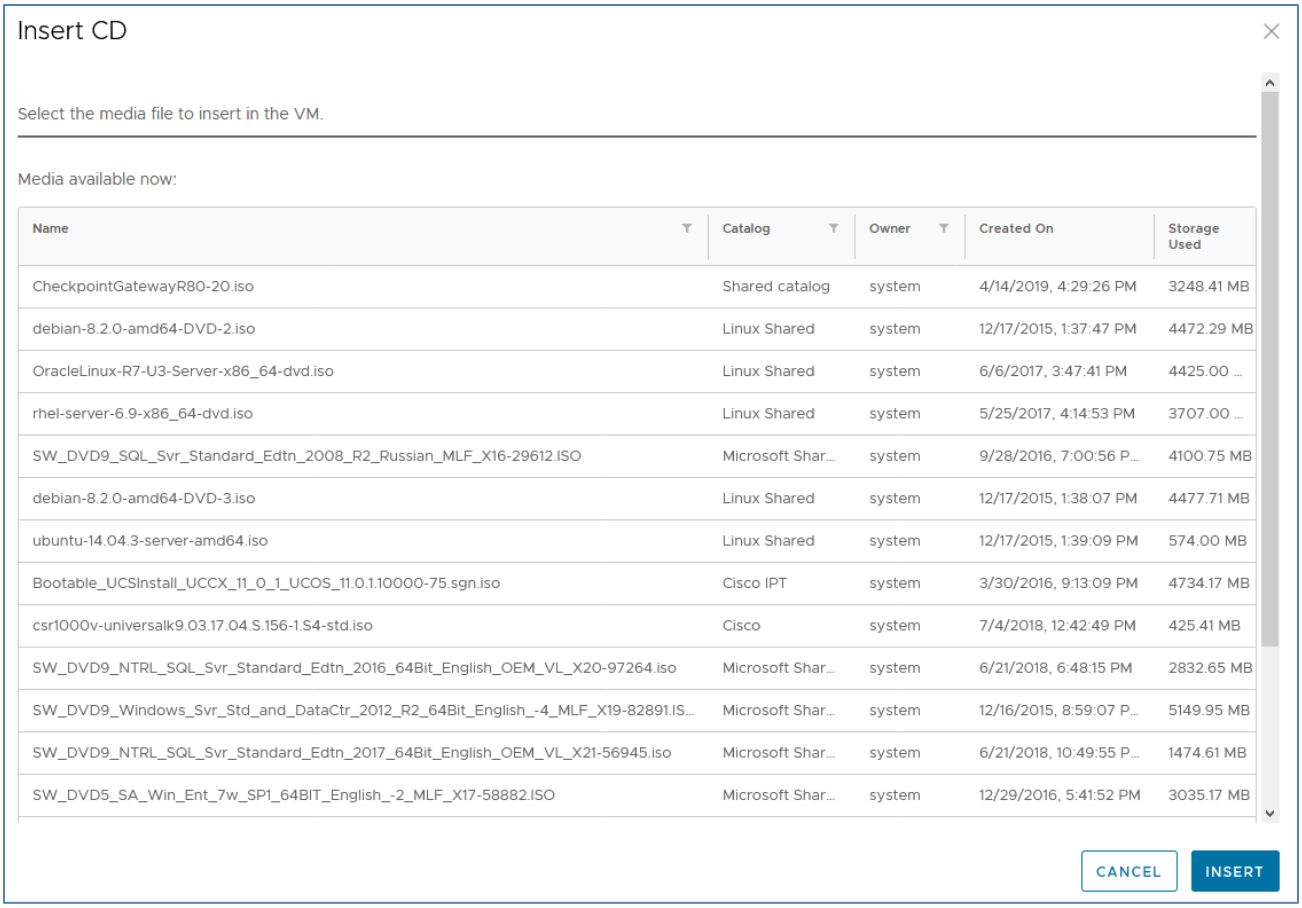
12.4. Установка ОС на виртуальную машину

Чтобы установить ОС на подготовленную виртуальную машину, нужно подключить ISO-образ установочного диска. Это можно сделать с локального диска или из каталога vCD.

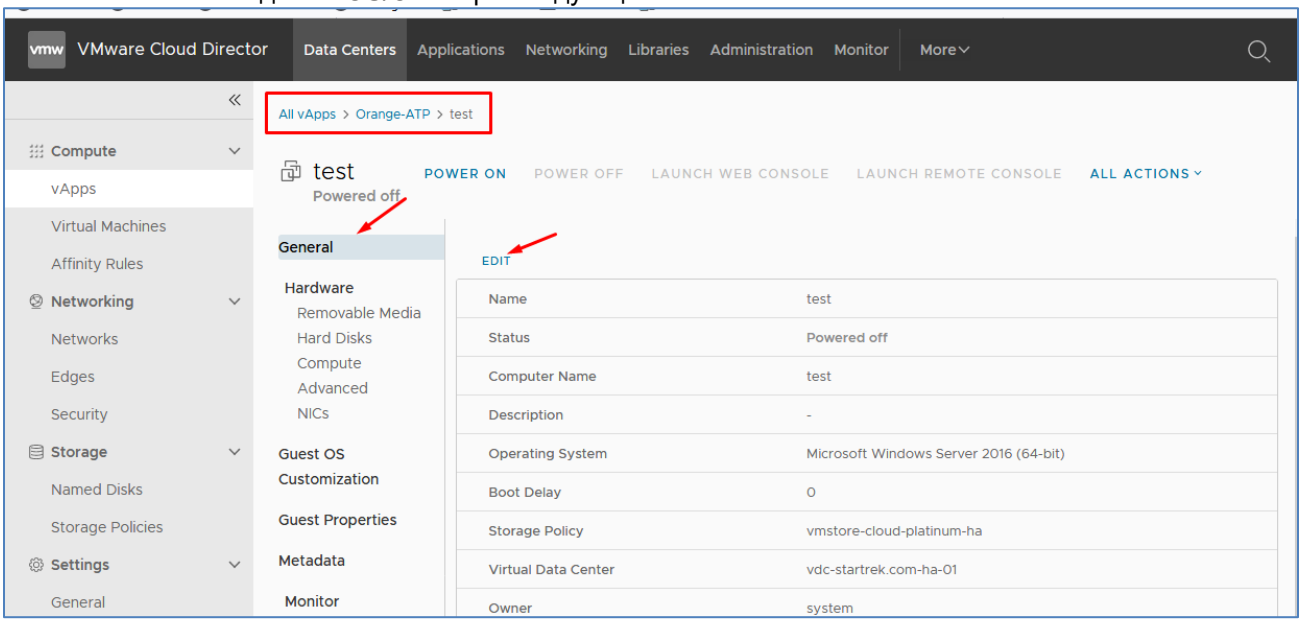
Начиная с версии vCloud 10.0, вследствие удаления старого FLASH интерфейса, нет возможности подключения образов через VMRC или WEB-консоль.

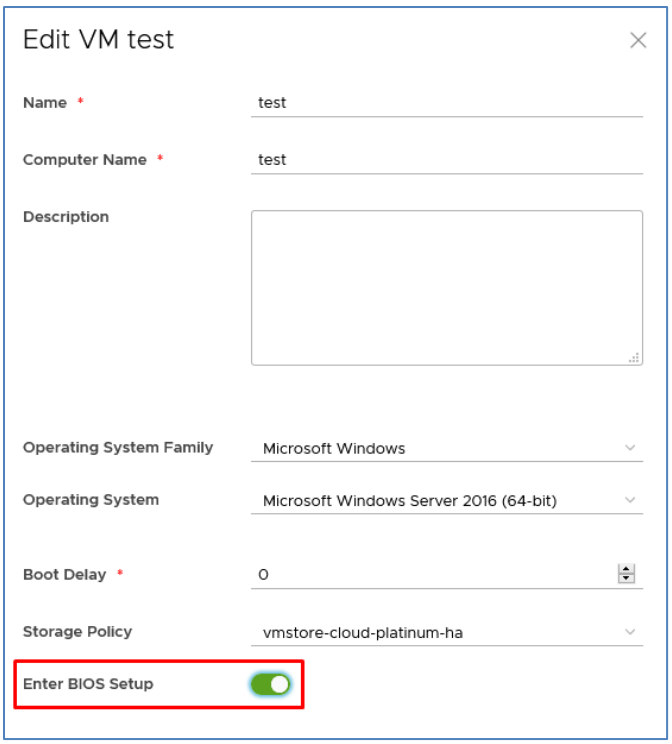
Предполагается, что уже создан каталог и в него загружен нужный ISO-образ установочного диска.
Из контекста ВМ выберите Insert Media:





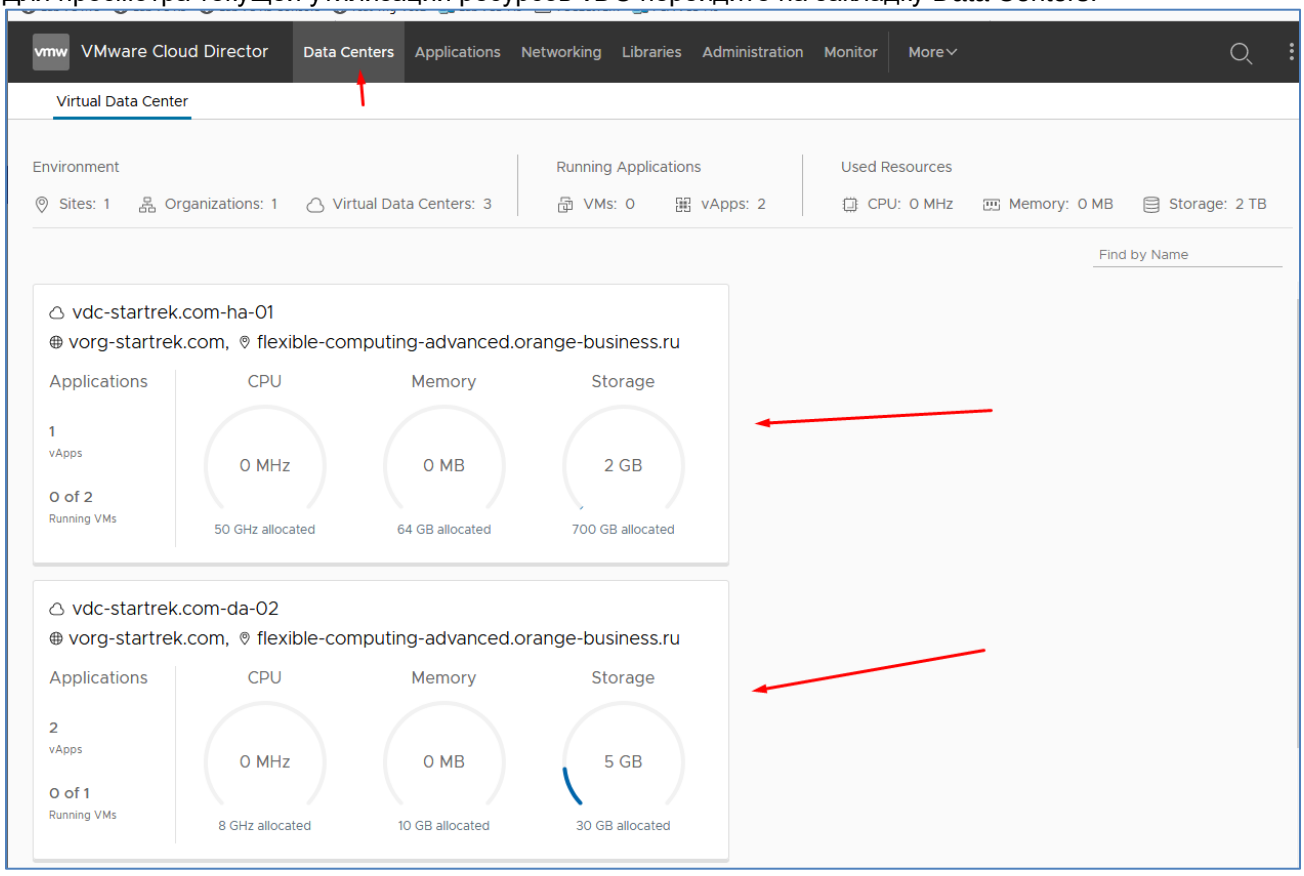
По умолчанию DVD-привод присутствует в списке загрузки, но не первым. Если есть необходимость поменять очередность загрузки – необходимо сделать это через BIOS/UEFI, для этого необходимо установить опцию автоматического входа в BIOS/UEFI при следующем включении ВМ:



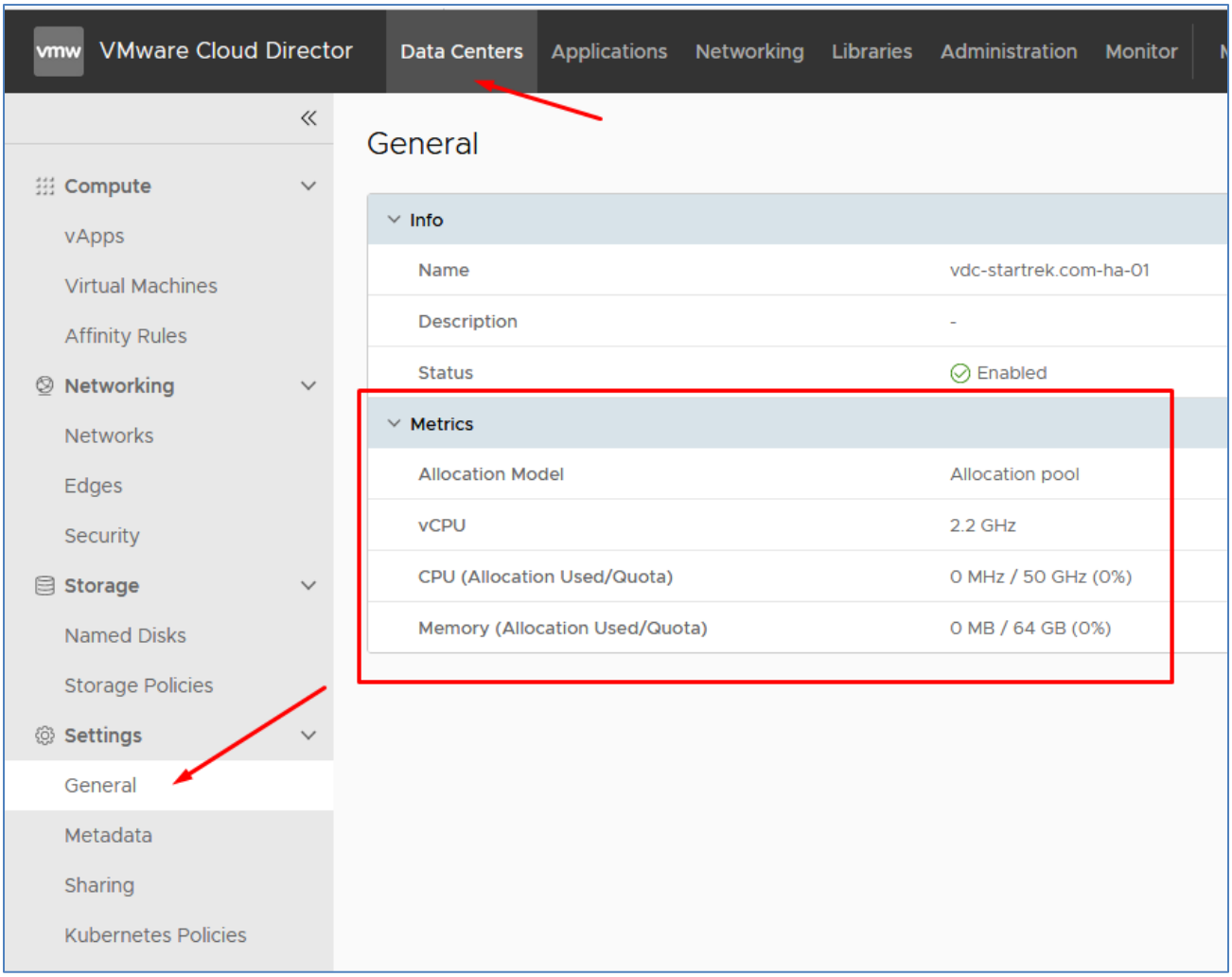


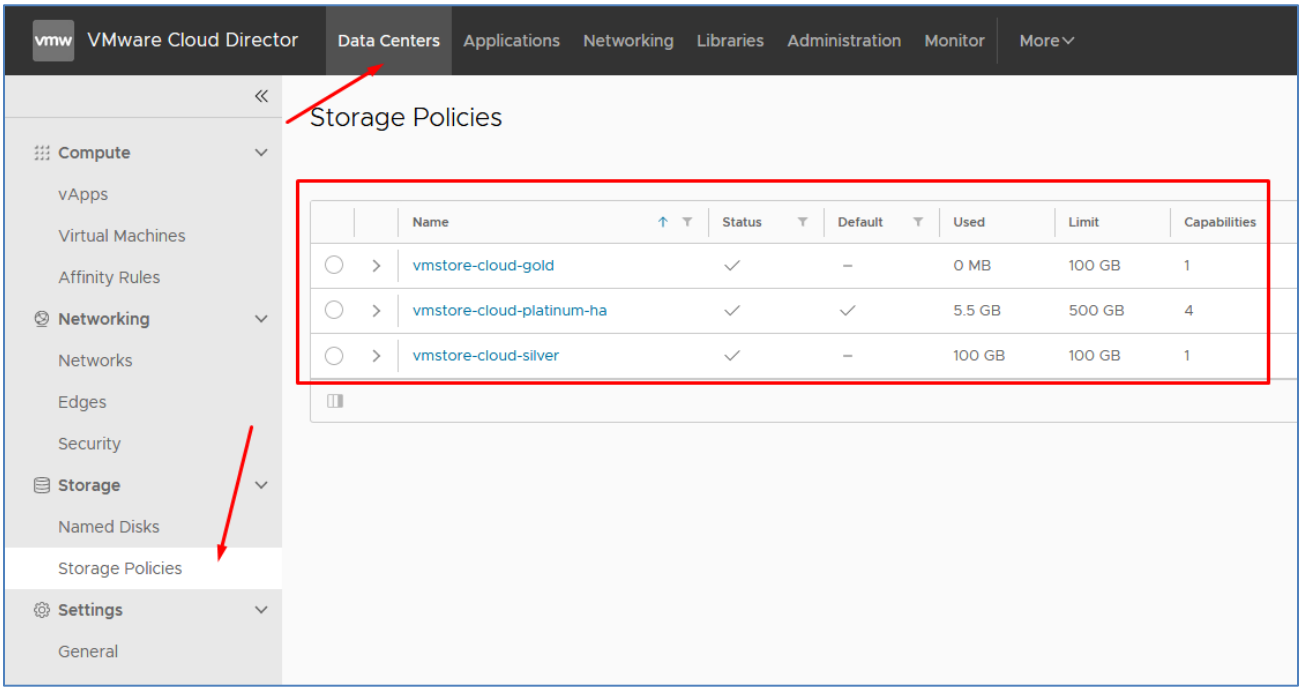
12.5. Мониторинг ресурсов

Для просмотра текущей утилизации ресурсов vDC перейдите на закладку Data Centers:



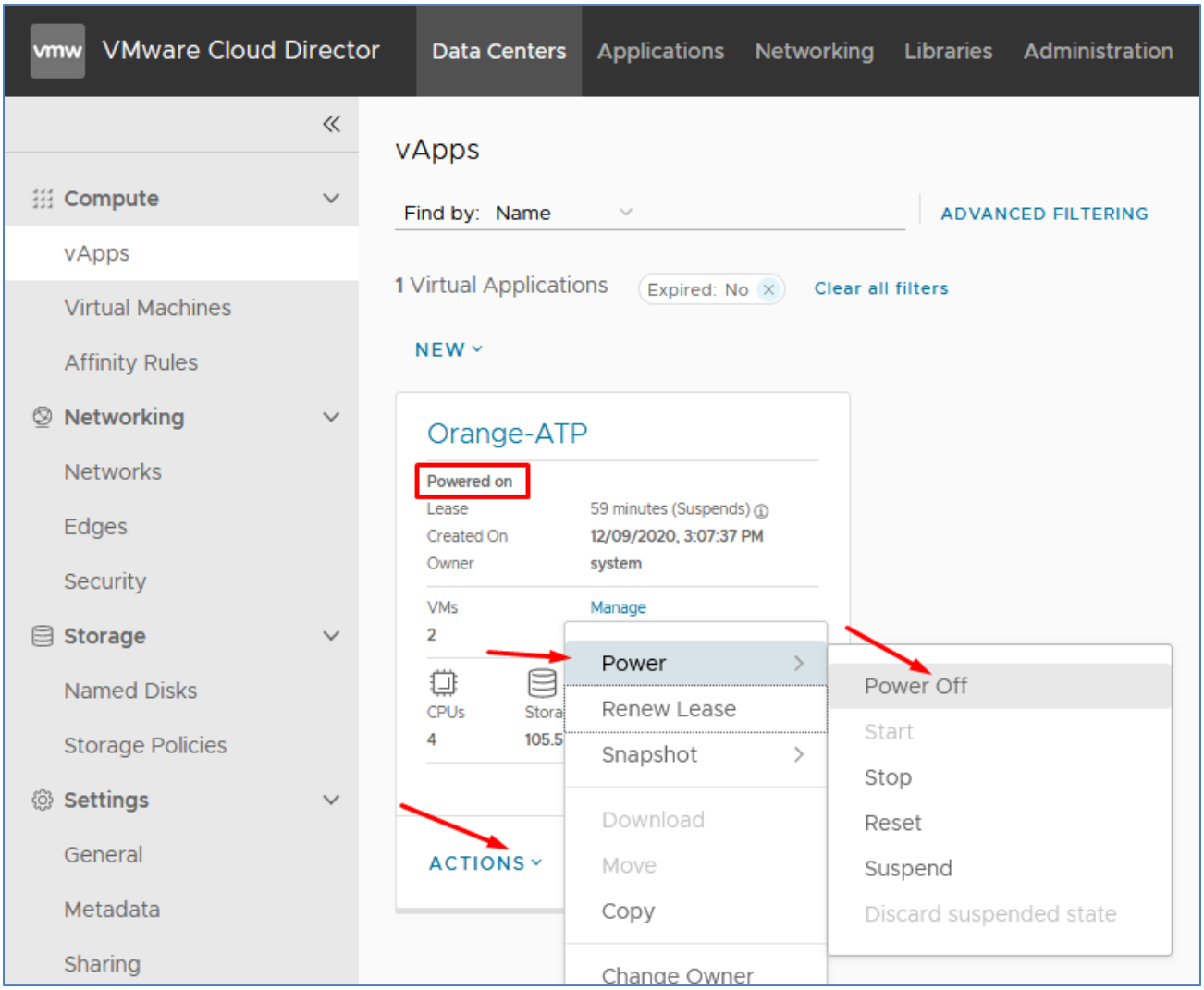
Более подробную информацию можно посмотреть внутри vDC:





12.6. Выгрузка шаблона vApp из Cloud Director

Для экспорта шаблона vApp (ВМ), в первую очередь vApp должен быть остановлен. Даже если все Вм в vApp выключены, сам vApp считается работающим пока не будет специально остановлен.



После остановки станет доступен пункт Download

12.7. Установка VMware tools на ВМ

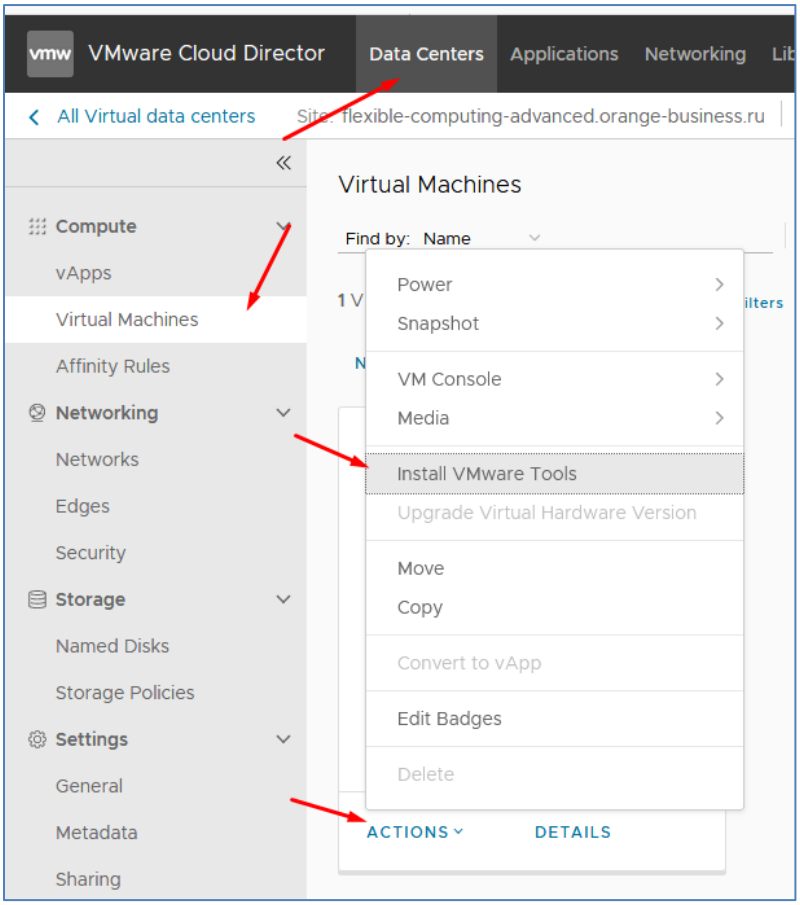
VMware Tools — это набор утилит, который повышает производительность операционной системы виртуальной машины и улучшает управление виртуальной машиной. Если в виртуальной машине не установлен данный набор утилит, то в гостевой операционной системе отсутствуют некоторые важные функции и возможности по интеграции с гипервизором, также отсутствуют оптимизированные драйвера для виртуальных устройств и возможности по управлению питанием (reboot/shutdown) гостевой операционной системы через средства управления VMware

Установка VMware Tools в операционную систему виртуальной машины находится в зоне ответственности клиента и является обязательной. В случае использования специфической ОС для которой нет инструкции по установке или дистрибутива VMware Tools, клиент должен обратиться в Orange для консультации и фиксации факта наличия такой ВМ.
В случае отсутствия установленных (процесс установки завершён, ос перезагружена, образ отмонтирован) и работоспособных (гипервизор имеет возможность подключения) VMware Tools в операционной системы виртуальной машины:

- резервные копии ВМ могут быть неконсистентными с большей вероятностью;
- в случае если при проведении аварийно-восстановительных работ ВМ клиента не может быть перемещена на другой гипервизор и этим блокирует работы, ВМ может быть перезагружена без согласования с клиентом;
- в случае аварии на хосте или в ДЦ, Orange не гарантирует запуск ВМ на другом хосте или перезапуск может занять более продолжительное время.

Актуальные и подробные инструкции находятся здесь.

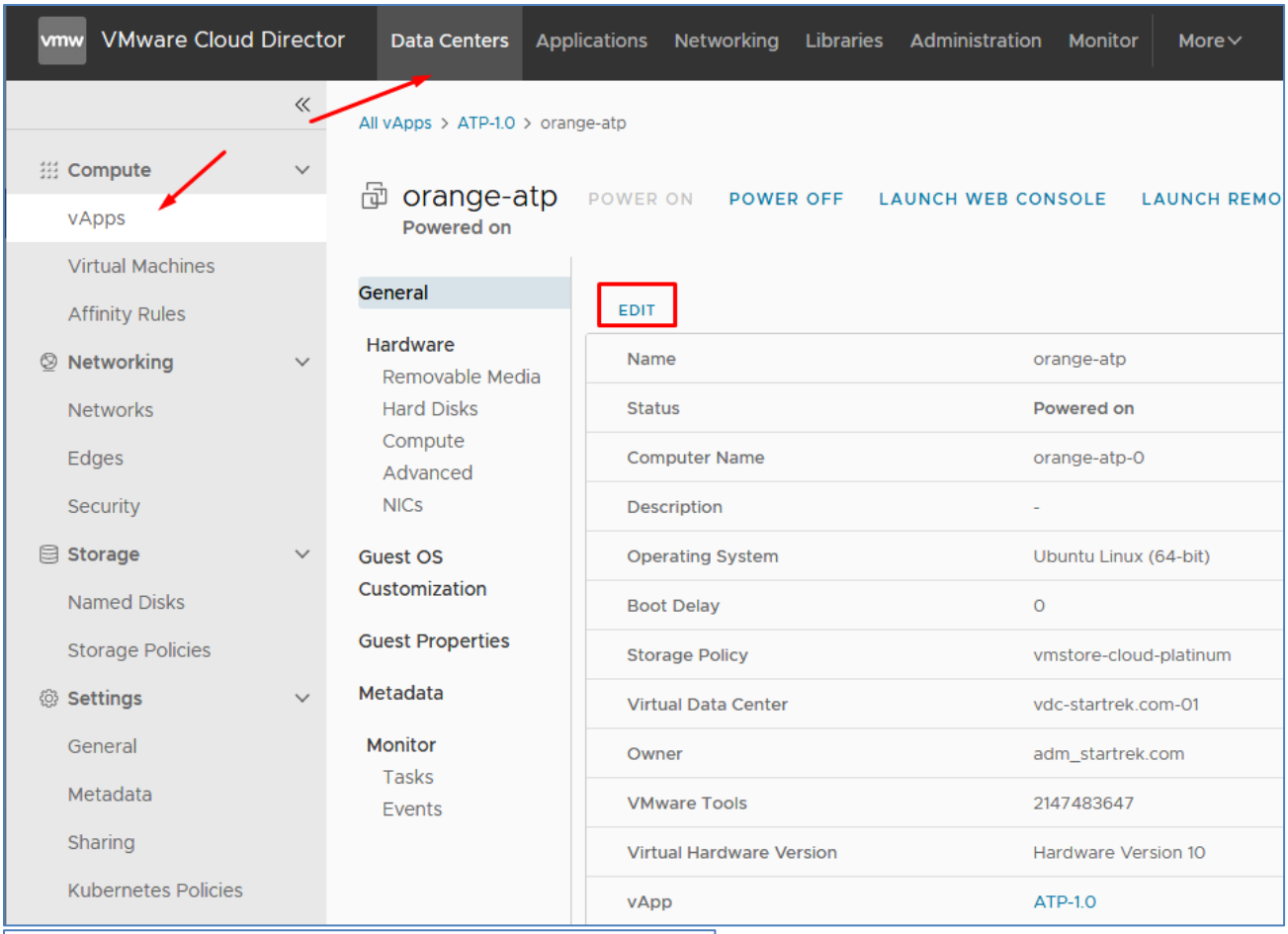
Для подключения ISO-образа с VMware Tools к ВМ нажмите правой кнопкой на ВМ и выберите пункт Install VMware Tools, это приведёт к монтированию ISO-образа к ВМ, после чего необходимо произвести установку в ОС.

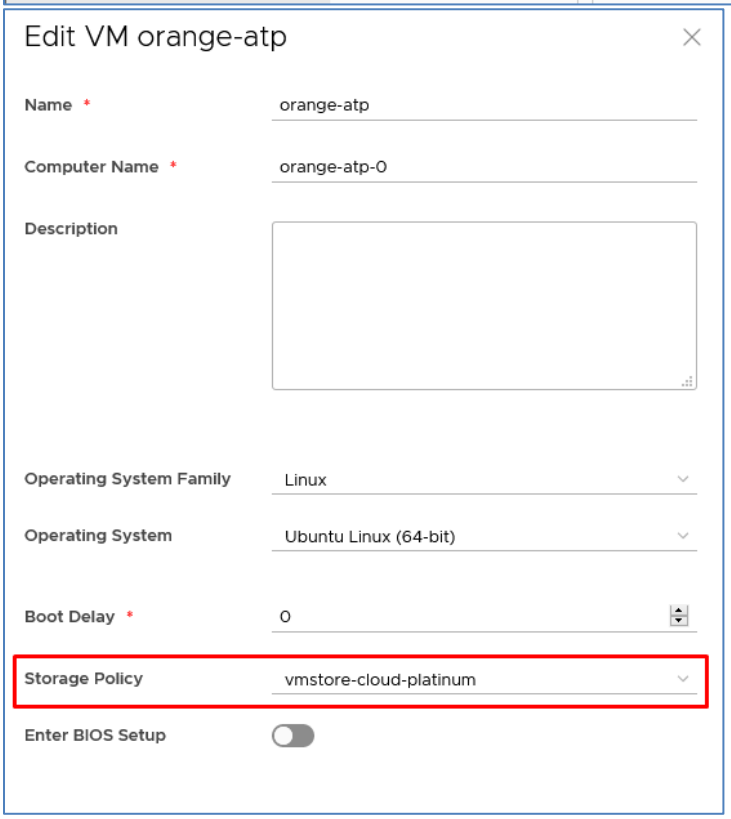


12.8. Выбор типа СХД для ВМ

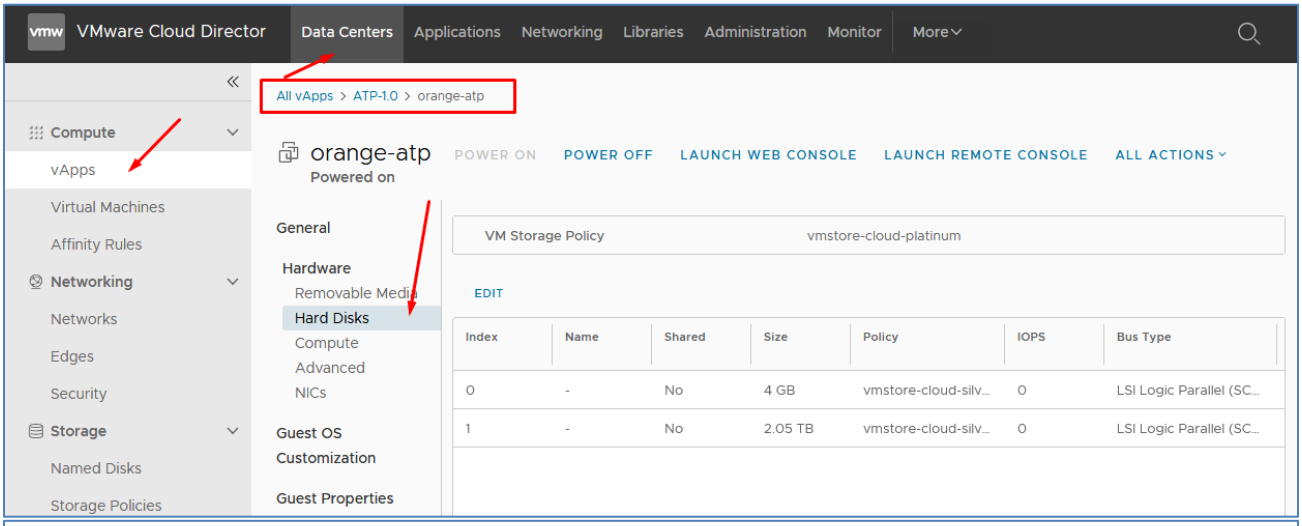
Тип используемого СХД для ВМ задаётся с помощью назначения нужной политики для дисков и для объекта «vm home»(метаданные ВМ). Метаданные должны использовать туже политику, что и основной диск ВМ.

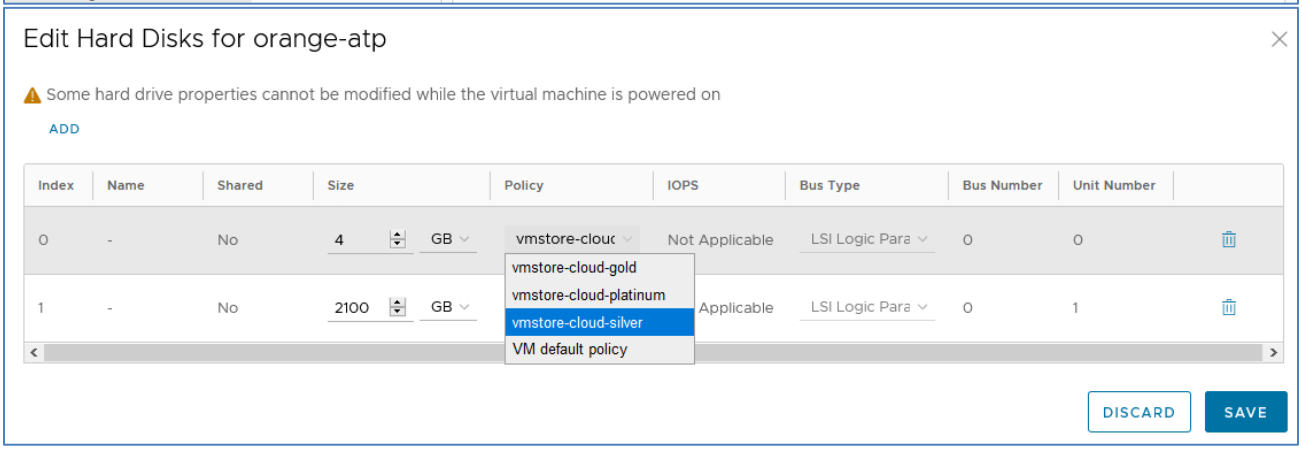
Из контекста ВМ:





Установка политик для дисков ВМ:





(Use VM default) – означает туже политику, которая назначена для метаданных.

12.9. Именованные диски ВМ (Named Disks)

Данный тип дисков создаётся на уровне vDC, а не виртуальной машины, и может быть подключён одновременно к нескольким ВМ.
В основном это необходимо для кластерных решений.
Варианты и описание настройки доступны в документации.
Внимание: для ВМ использующих named disks недоступно создание снэпшотов, и как следствие резервное копирование на уровне гипервизора.

13. Известные проблемы

Описание проблемы	Решение	KB VMware
На ОС Windows Server 2012 и выше пропадает сетевая связность. Доступ восстанавливается после перезагрузки или up/down сетевого интерфейса. *Примечание: аналогичные проблемы наблюдались на Windows 7 и Server 2008R2.*	Использовать тип vNIC – VMXNET3	KB 2109922
Отсутствует/некорректно работает мышь при установке Windows и после	1. При установке использовать VMRC, вместо WEB-консоли 2. Установить VMware tools используя клавиатуру	-