

Flexible Computing Advanced

Руководство пользователя

1.	Введение.....	3
2.	Навигатор по опциям и возможностям	3
3.	Архитектура, опции, особенности и рекомендации	3
3.1.	Обзор архитектуры	3
3.2.	DA или DR? Показатели RTO и RPO	6
3.3.	Катастрофоустойчивость (Disaster Avoidance, DA).....	7
3.4.	Аварийное восстановление (Disaster Recovery, DR)	8
3.5.	Подсистема хранения.....	8
3.6.	Резервное копирование на диск (Бэкап на диск)	8
3.7.	Резервное копирование (архивирование) на ленту (Бэкап на ленту).....	8
3.8.	Самостоятельное управление резервным копированием (BETA)	9
3.9.	Выделенные GHz и vCPU.....	9
3.10.	Отказоустойчивый доступ к сетям Интернет и IPVPN	9
3.11.	VMware NSX Edge	12
3.12.	NSX Edge High Availability	13
3.13.	Защита от DDoS-атак.....	14
3.14.	Аренда лицензий на ПО.....	14
3.15.	Активация ПО Microsoft по программе SPLA через KMS	14
3.16.	Как подключить локальную сеть к облаку Orange?.....	15
3.17.	Виртуальный маршрутизатор Cisco CSR1000v.....	16
3.18.	Подключение внешних USB устройств (USB-to-IP).....	16
3.19.	Подключение внешних сетевых устройств/серверов расположенных в iX.....	17
4.	Основные элементы VMware vCloud Director	17
5.	Вход в виртуальный дата-центр	18
6.	Типичные проблемы при подключении и работе с WEB-интерфейсом.....	19
7.	Проверка доступности ресурсов vDC и сетевой связности.....	19
7.1.	Проверка доступности ресурсов	20
7.2.	Проверка сетевых ресурсов	22
8.	Управление учётными записями пользователей	25
9.	Загрузка образов (ISO) и шаблонов VM.....	27
9.1.	Создание каталога.....	27
9.2.	Загрузка через vCloud Director	28
9.3.	Загрузка через FTPS-сервер Orange.....	29
9.4.	Загрузка через ovftool	29
10.	Сети vOrg и vApp	30
10.1.	Создание vOrg сети	30
10.2.	Создание vApp сети.....	31
11.	NSX Edge Gateway.....	33
11.1.	Размеры и производительность NSX Edge Gateway	33
11.2.	Настройка DHCP	34
11.3.	Настройка NAT	36
11.3.1.	Создание правила SNAT	36
11.3.2.	Создание правила DNAT	40
11.4.	Настройка Firewall.....	41
11.5.	Настройка Static routing.....	44

11.6.	Балансировщик нагрузки (Load Balancer).....	44
11.7.	VPN.....	44
11.8.	NSX Edge High Availability	45
12.	Настройка и управление виртуальными машинами и vApp	45
12.1.	Создание нового контейнера vApp.....	45
12.2.	Создание виртуальной машины из шаблона	49
12.3.	Создание виртуальной машины «с нуля»	51
12.4.	Установка ОС на виртуальную машину.....	53
12.5.	Мониторинг ресурсов.....	55
12.6.	Выгрузка шаблона vApp из vCloud Director	56
12.7.	Установка VMware tools на VM	57
12.8.	Выбор типа СХД для VM.....	58
13.	Известные проблемы	60

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 [vCloud 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 vCloud Director версии 10.2.0.17008054.

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 VM (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)	3.18	
Подключение внешних сетевых устройств/серверов расположенных в iX (недоступны в случае аварии в iX)	3.19	
Опции отказоустойчивости		
Архитектура платформы уровня Disaster Avoidance	3.1	
Резервирование ресурсов + приоритетный запуск VM в случае disaster	3.3	
Размещение дисков VM в двух ДЦ (синхронная репликация)	3.5	
Разнесение VM 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 IPVPN (через два ДЦ, разные PE, разные последние мили)		
Edge GW в режиме High Availability	3.11	11.8
Виртуальный маршрутизатор Cisco CSR1000v	3.17	
Защита от DDoS-атак	3.13	
Storage		
Silver (расположено в iX, недоступно в случае аварии в iX)	3.5	12.8
Gold (расположено в iX, недоступно в случае аварии в iX)		
Platinum (расположено в iX, недоступно в случае аварии в iX)		
Platinum DR (синхронная репликация)		
Резервное копирование и архивирование		
Резервное копирование на массив в iX	3.6	
Резервное копирование на массивы в двух ДЦ (асинхронная репликация)		
Архивирование и восстановление на ленту	3.7	
Offsite хранение лент		

3. Архитектура, опции, особенности и рекомендации

3.1. Обзор архитектуры

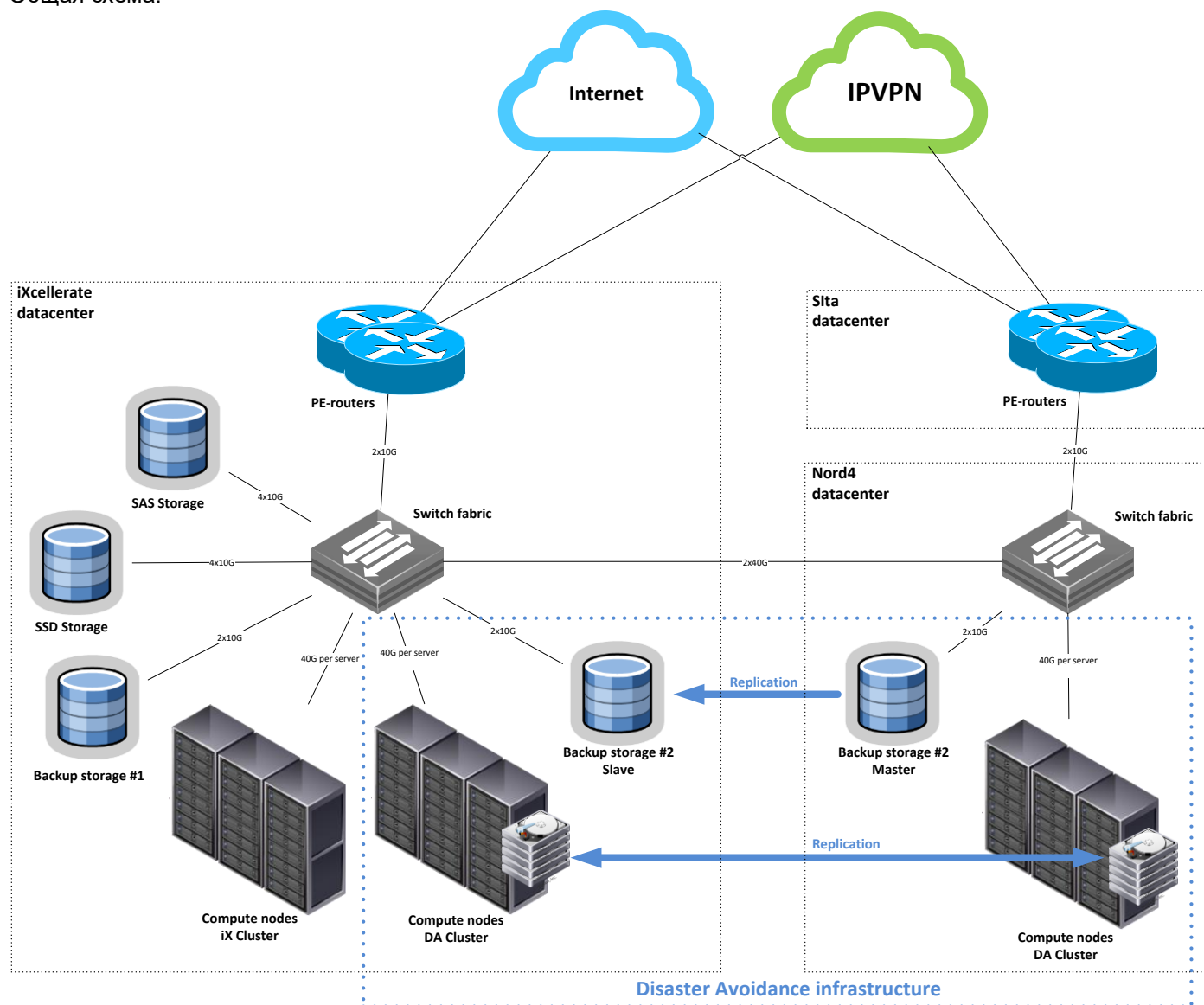
Основным принципом при построении инфраструктуры публичного облака для Orange является отказоустойчивость. Для этого применяется комплексный подход на всех уровнях:

- 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);
- Используется оборудование и ПО только промышленного класса от лидеров рынка: HPE, Juniper, Huawei, VMware, Netapp, Veeam, CheckPoint, ADVA;

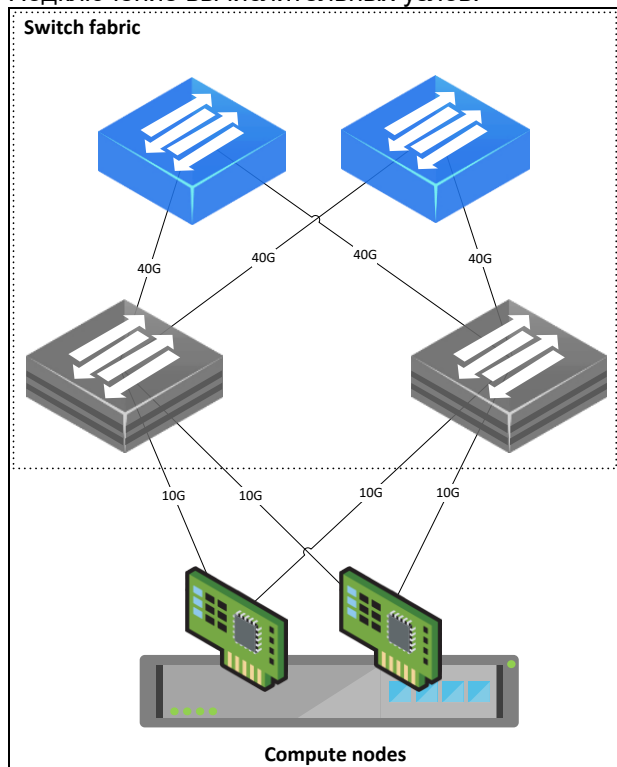
- Активные сервисные контракты по всему оборудованию и ПО;
- Постоянное поддержание и повышение экспертизы инженеров;
- DWDM-каналы между дата-центрами (далее ДЦ) проложены разными маршрутами по городу, входят в ДЦ через разные кабельные коллекторы, внутри ДЦ трассы также не пересекаются на уровне кабельных лотков, работают на двух наборах полностью независимого оборудования;
- Задержка передачи данных между ДЦ: 0,3-0,4мс при измерениях VM<>VM, 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 (Интернет, IPVPN) подаются с двух независимых PE-маршрутизаторов, расположенных в разных ДЦ по разным трассам;
- Все классические СХД имеют 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 кластера iXcellerate:

CPU	2xE5-2680 v3 @ 2.50GHz (12C, Turbo Boost 3,3GHz, Haswell)
RAM	256-768 GB

Характеристики вычислительных узлов кластера DA:

CPU	2xE5-2698 v4 @ 2.20GHz (20C, Turbo Boost 3,6GHz, Broadwell)
RAM	512-704 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 ДЦ iXcellerate и обеспечивают отказоустойчивость только в пределах этого ДЦ. Т.е. в случае катастрофы в ДЦ iXcellerate 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 ДЦ iXcellerate 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 vCloud Director будет указан суммарный объём выделенного дискового пространства (указанный в Бланке заказа + добавленный Orange) и суммарный объём потребленного дискового пространства.

VMware vCloud Director учитывает потребление дискового пространства по следующей формуле (для каждого типа отдельно):

Суммарный объём потребленного 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 ($T > 3$)

- 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 выбрать:

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

3.8. Самостоятельное управление резервным копированием (BETA)

Примечание: данный функционал находится в процессе тестирования и доступен по запросу.

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.

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 VM на каждый vCPU (ядро) выделяется (т.н. Allocation) 1GHz – т.е. максимум может быть включено 48 vCPU в данной ситуации (например: 12 VM по 4 vCPU, или 2 VM по 12 vCPU и 6 VM 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: $48 \times 2,5 = 120\text{GHz}$. 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 VM.

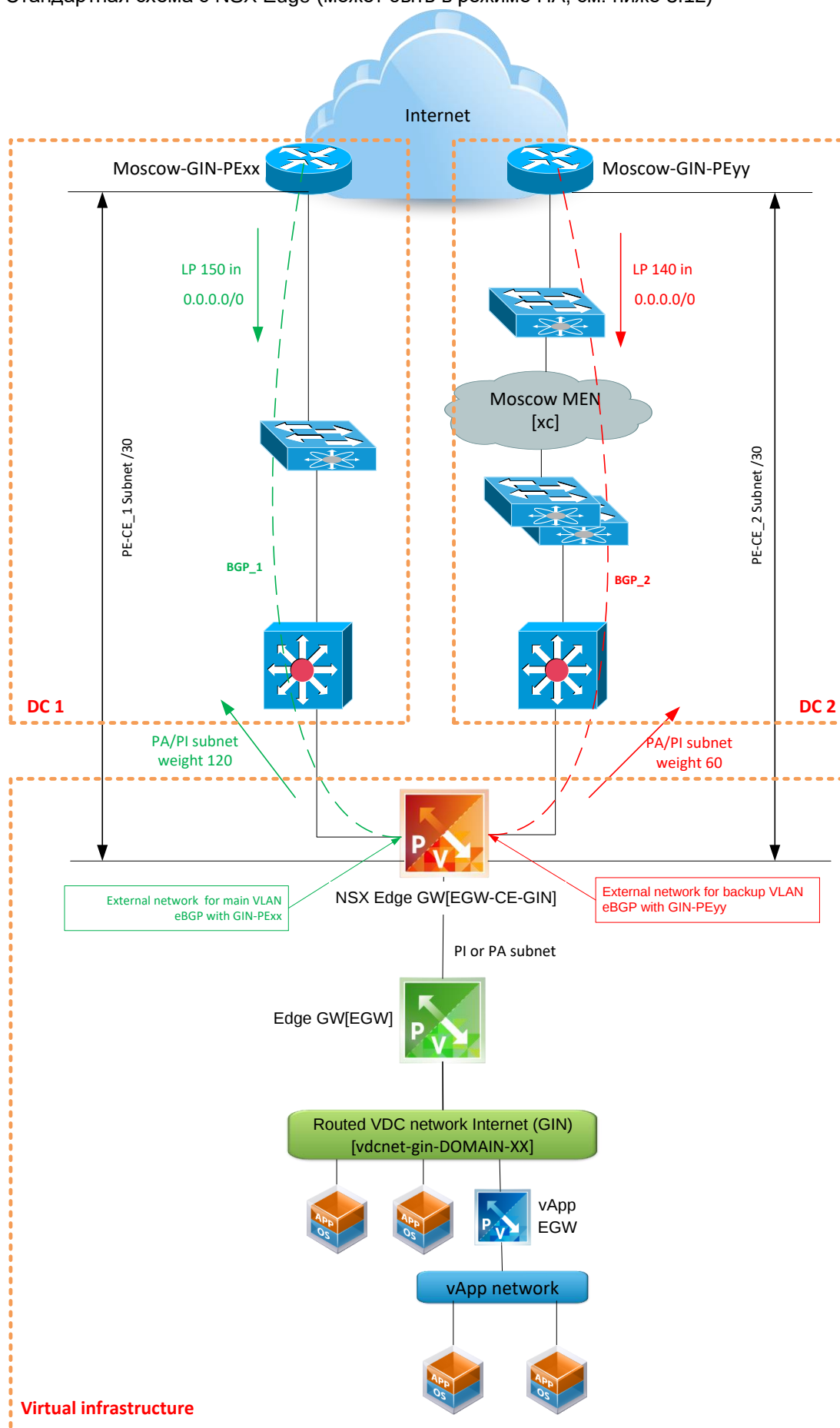
Если нужно избежать потенциальной ситуации ограничения частоты ядер, можно посчитать так: $48\text{GHz} / 2,5\text{GHz} = 19,2$ vCPU – т.е. настроить на VM 19 ядер и они гарантированно не будут ограничиваться.

3.10. Отказоустойчивый доступ к сетям Интернет и IPVPN

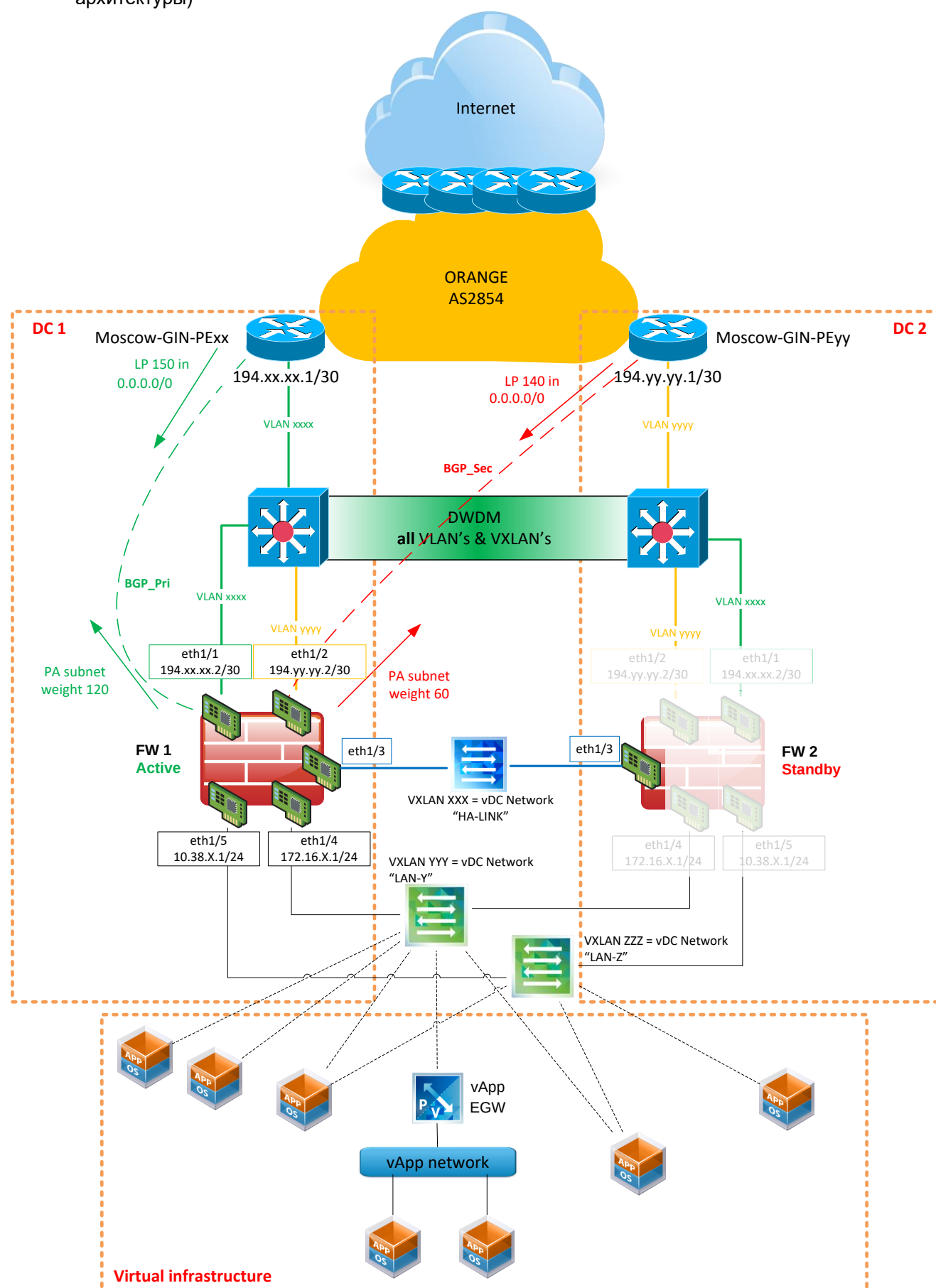
Все внешние сетевые соединения зарезервированы на уровнях физических соединений, физического оборудования, сети MEN, PE-маршрутизаторов и организуются через два датацентра. При этом не имеет значения, по какому маршруту (через какой датацентр) идёт в текущий момент трафик – для виртуальных машин в vDC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

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

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



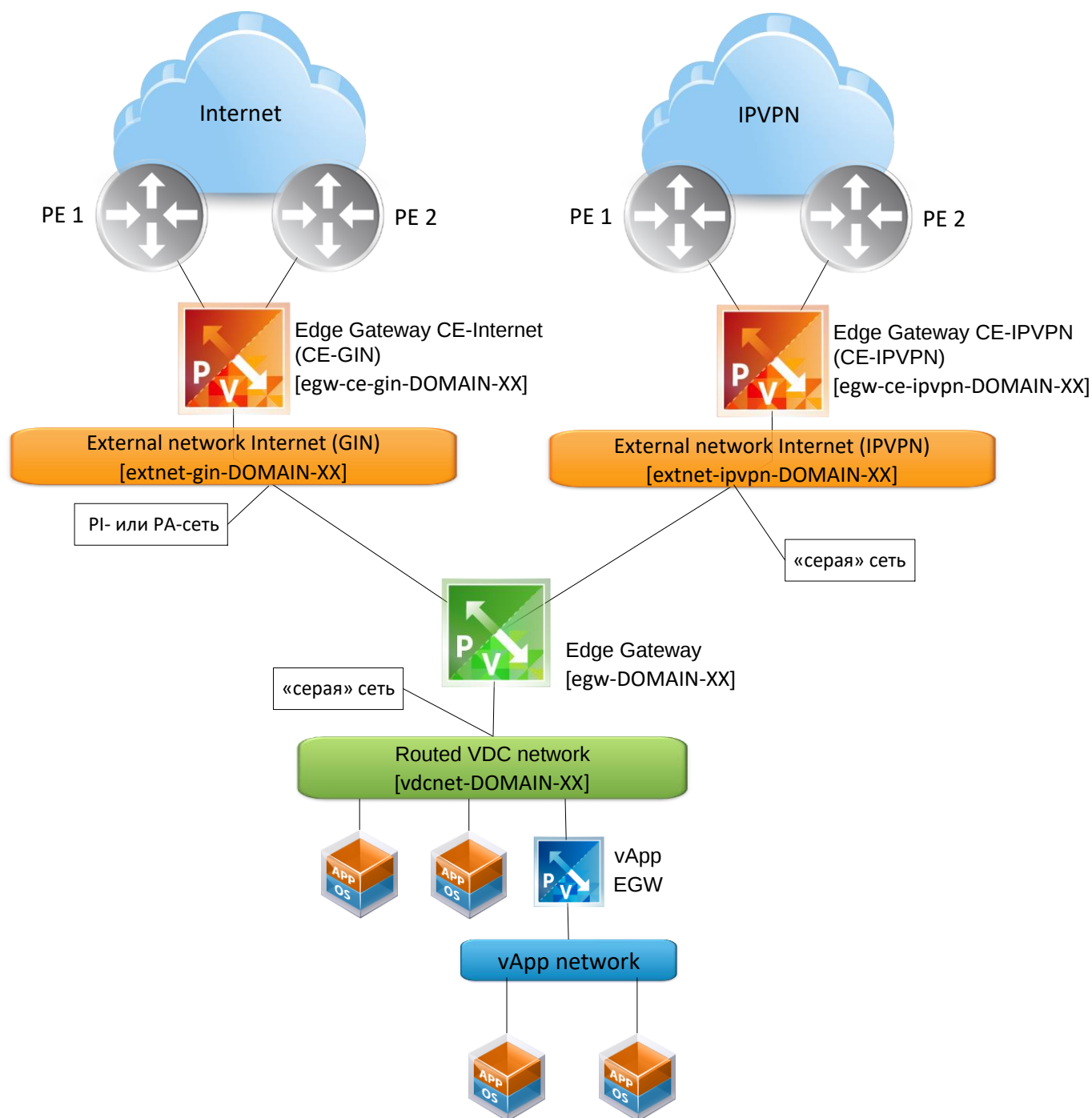
- Использование заказчиком собственного виртуального маршрутизатора (пример возможной архитектуры)



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 IPVPN используются разные EGW-CE. Настройка этих параметров находится в зоне ответственности Orange;
- «EGW» - полностью доступен для управления клиентом из web-интерфейса vCloud 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 IPVPN «Edge Gateway CE-IPVPN (CE-IPVPN) [egw-ce-ipvpn-DOMAIN-XX]» - полностью управляется Orange, выполняет только функции CE и обеспечивает связность с EGW через OSPF. В случае необходимости, EGW CE-IPVPN может быть заменён на Cisco CSR1000v (см. 3.17).

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 IPVPN).

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

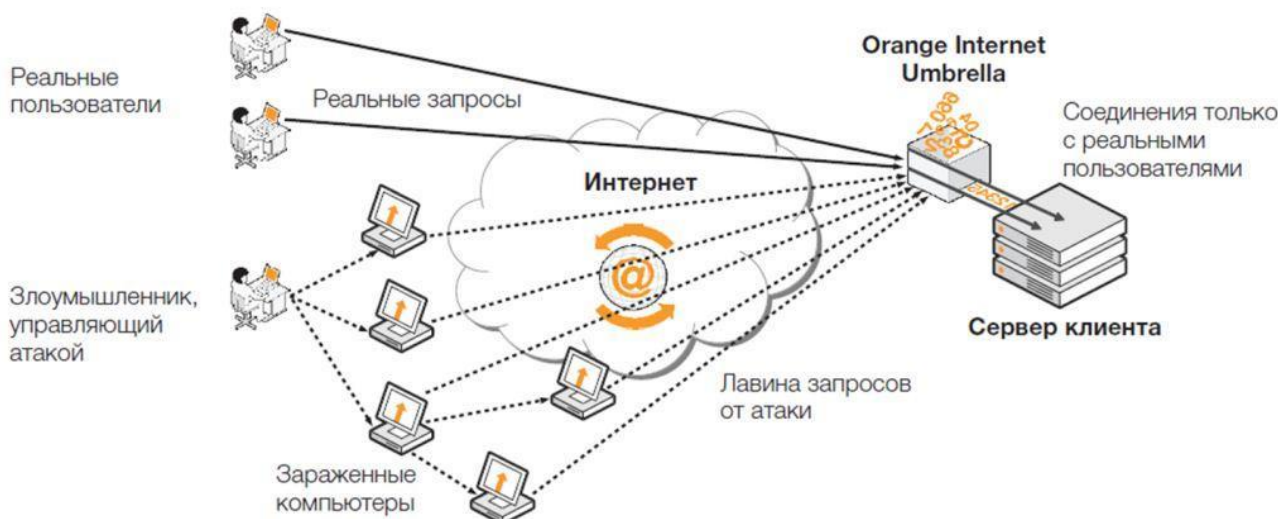
* По специальному запросу может быть уменьшено до 3 сек.

** 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 VM не имеет доступа в Интернет, необходимо обратиться в Orange для активации MAK-ключом.

Процедура активации:

- Проверить, что на EGW открыт порт TCP1688 в Интернет

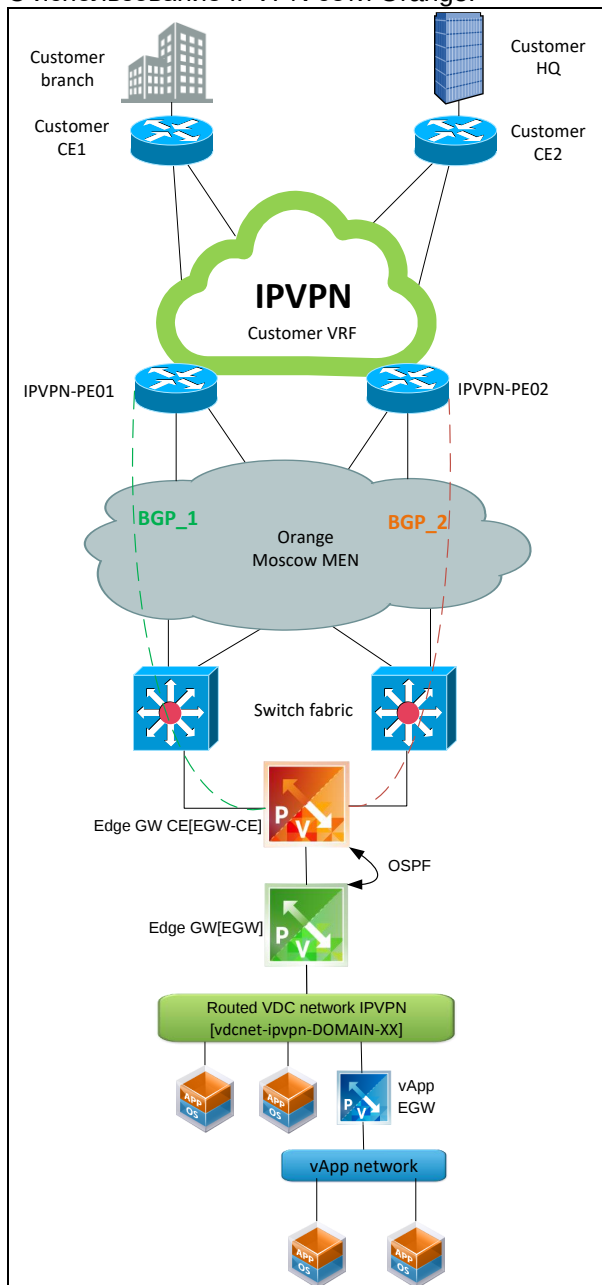
- Проверить, что на ВМ установлено корректно время!
- Установить IP KMS
slmgr -skms 194.84.17.201:1688
- Активировать online
slmgr.vbs /ato
- Проверяем активацию
slmgr /dlv

* 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 IPVPN сети Orange.

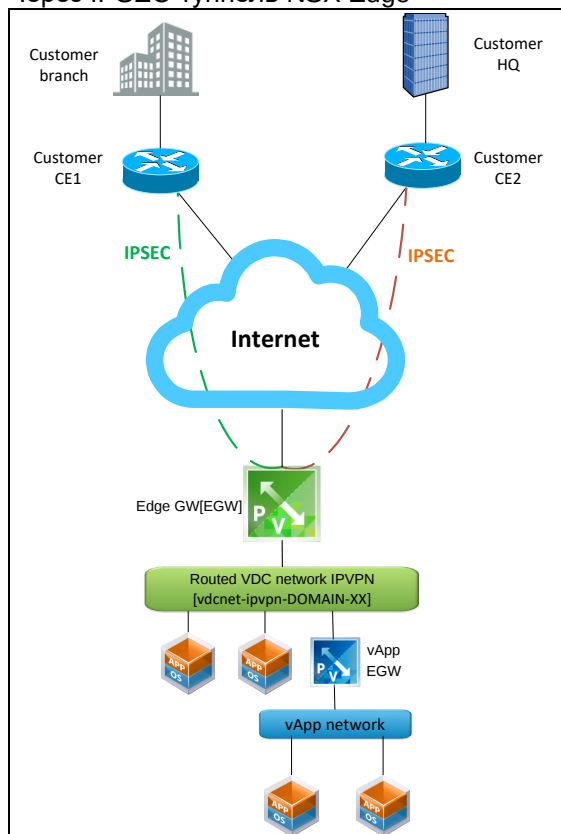


Плюсами такого метода являются:

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

- Опциональный SLA
- Работоспособность канала – 30 Orange
- Опция подключения удалённых сайтов к сети IPVPN через услугу «Internet VPN»(IPSEC до IPVPN-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. Виртуальный маршрутизатор Cisco CSR1000v

В качестве виртуального маршрутизатора в vDC может быть использован Cisco CSR1000v, совместно или заменяя Edge и Edge-CE. Данная конфигурация является нестандартной и прорабатывается совместно с Orange. Cisco CSR1000v может управляться клиентом самостоятельно или силами Orange (услуга «Managed Router»). Orange может предоставить лицензии на CSR нужного уровня функциональности и производительности.

Более подробная информация о CSR доступна [сайте Cisco](https://www.cisco.com).

3.18. 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 VM (к одной VM может быть 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, флеш-накопители и т.п.

3.19. Подключение внешних сетевых устройств/серверов расположенных в iX

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 iXcellerate (услуга «Nethosting»). Также данная опция может быть использована для подключения vDC к стороннему оператору связи, напрямую или через физический маршрутизатор установленный в iX.

В зависимости от требуемой скорости, это может быть:

- Один или два порта(MC-LAG) 1000BASE-T на одно устройство, организуется медный кабсоед до оборудования клиента;
- Один или два порта(MC-LAG) 10GBASE-SR на одно устройство, организуется оптический кабсоед MM LC duplex до оборудования клиента. *Не является стандартным вариантом, требуется проработка.*

4. Основные элементы VMware vCloud Director

Виртуальная организация (organization, vOrg) – самый верхний элемент в иерархии объектов абстракции vCloud 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, контейнеры vApp, сети и пр. Вы можете увеличивать его размеры по мере необходимости, покупая 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 контейнер, в котором размещаются виртуальные машины. Его можно создать пустым или сразу с виртуальными машинами. Благодаря контейнерам 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. vCloud 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 находиться 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-IPVPN	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 IPVPN	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-IPVPN (CE-IPVPN)	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 (IPVPN)	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 IPVPN	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

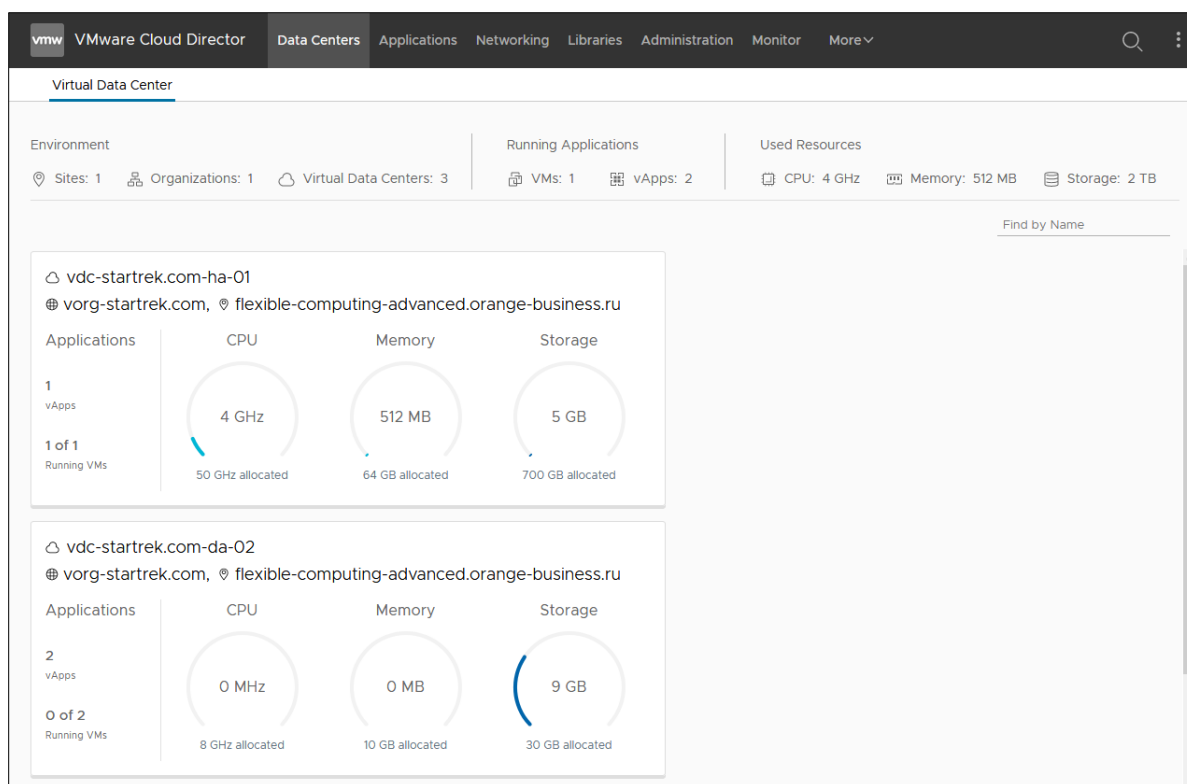
5. Вход в виртуальный дата-центр

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 (старый интерфейс на базе FLASH более недоступен!):

- «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 VM 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:

The screenshot shows the VMware Cloud Director web interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', and several tabs: 'Data Centers' (selected), 'Applications', 'Networking', 'Libraries', 'Administration', and 'Monitor'. Below the navigation bar, the 'Virtual Data Center' section is active. It displays summary statistics: 'Environment' (Sites: 1, Organizations: 1, Virtual Data Centers: 3), 'Running Applications' (VMs: 1, vApps: 2), and 'Used Resources' (CPU: 1). A red arrow points to the 'Data Centers' tab, and another red arrow points to a specific vDC card titled 'vdc-startrek.com-ha-01'. This card shows the vDC's details, including its name, a globe icon, and two domain names: 'vorg-startrek.com' and 'flexible-computing-advanced.orange-business.ru'. Below the details, there are four sections: 'Applications' (showing 1 vApp and 1 of 1 Running VMs), 'CPU' (4 GHz used, 50 GHz allocated), 'Memory' (512 MB used, 64 GB allocated), and 'Storage' (5 GB used, 700 GB allocated). Each resource section is represented by a circular gauge.

Environment	Running Applications	Used Resources
Sites: 1 Organizations: 1 Virtual Data Centers: 3	VMs: 1 vApps: 2	CPU: 1

Applications	CPU	Memory	Storage
1 vApps 1 of 1 Running VMs	4 GHz 50 GHz allocated	512 MB 64 GB allocated	5 GB 700 GB allocated

Слева в меню «General»:

The screenshot displays the VMware Cloud Director interface. The top navigation bar includes 'vmw VMware Cloud Director', 'Data Centers', 'Applications', 'Networking', 'Libraries', 'Administration', and 'Monitor'. The left sidebar contains a tree view with categories: 'Compute' (vApps, Virtual Machines, Affinity Rules), 'Networking' (Networks, Edges, Security), 'Storage' (Named Disks, Storage Policies), and 'Settings' (General, Metadata, Sharing, Kubernetes Policies). The 'General' option under 'Settings' is highlighted with a red box. The main content area is titled 'General' and contains a table with system information, also highlighted with a red box.

General	
▼ Info	
Name	vdc-startrek.com-da-02
Description	-
Status	✓ Enabled
▼ Metrics	
Allocation Model	Allocation pool
vCPU	1 GHz
CPU (Allocation Used/Quota)	0 MHz / 8 GHz (0%)
Memory (Allocation Used/Quota)	0 MB / 10 GB (0%)

Доступные дисковые ресурсы доступны в меню «Storage Policies»:

The screenshot shows the VMware Cloud Director interface. The left sidebar has a menu with categories: Compute, Networking, Storage, and Settings. The 'Storage' category is expanded, and 'Storage Policies' is highlighted. The main panel displays the 'Storage Policies' section with a table of policies.

	Name	Status	Default	Used	Limit	Capabilities
☐	vmstore-cloud-gold	✓	–	4 GB	10 GB	1
☐	vmstore-cloud-platinum-da	✓	✓	5 GB	10 GB	4
☐	vmstore-cloud-silver	✓	–	0 MB	10 GB	1

7.2. Проверка сетевых ресурсов

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

The screenshot shows the VMware Cloud Director interface. The left sidebar has a menu with categories: Compute, Networking, Storage, and Settings. The 'Compute' category is expanded, and 'vApps' is highlighted. The main panel displays the 'vApps' section with a search bar and a list of virtual applications. A specific vApp named 'ATP-1.0' is selected, showing its status and details.

ATP-1.0

Powered off
 Lease Never Suspends ⓘ
 Created On 05/16/2018, 5:56:30 PM
 Owner adm_startrek.com

VMs 1
 VM Consoles

CPU 2
 Storage 2.06 TB ⓘ
 Memory 512 MB
 Networks 1 ⓘ

BADGES

ACTIONS **DETAILS**

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

All vApps > ATP-1.0

ATP-1.0 **Powered on**

POWER OFF START STOP RENEW LEASE CHANGE OWNER ALL ACTIONS ▾

General Virtual Machines Start and Stop Order Network Diagram Networks Guest Properties Sharing

Find by: Name ▾ ADVANCED FILTERING Sort by: Name ▾ ↑

1 Virtual Machines

Multiselect

Name	Console	Status	Lease	Created On	OS
orange-atp	VM Console	Powered on	Never Suspen...	05/16/2018, 5:56:33 PM	Ub

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

All vApps > vapp-ebf18528-ece7-4d7e-83e9-b3e65cf8346a > vm-82834197-c87f-4a3c-8089-ba3a9b3579f0

orange-atp **Powered on**

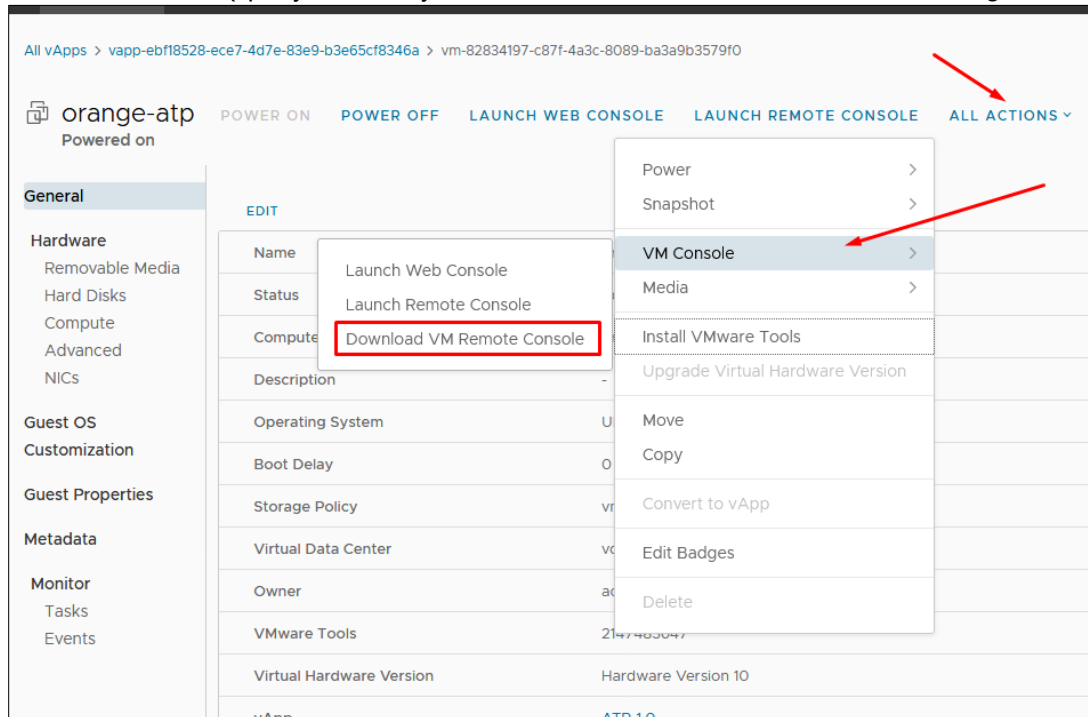
POWER ON POWER OFF LAUNCH WEB CONSOLE LAUNCH REMOTE CONSOLE ALL ACTIONS ▾

General EDIT

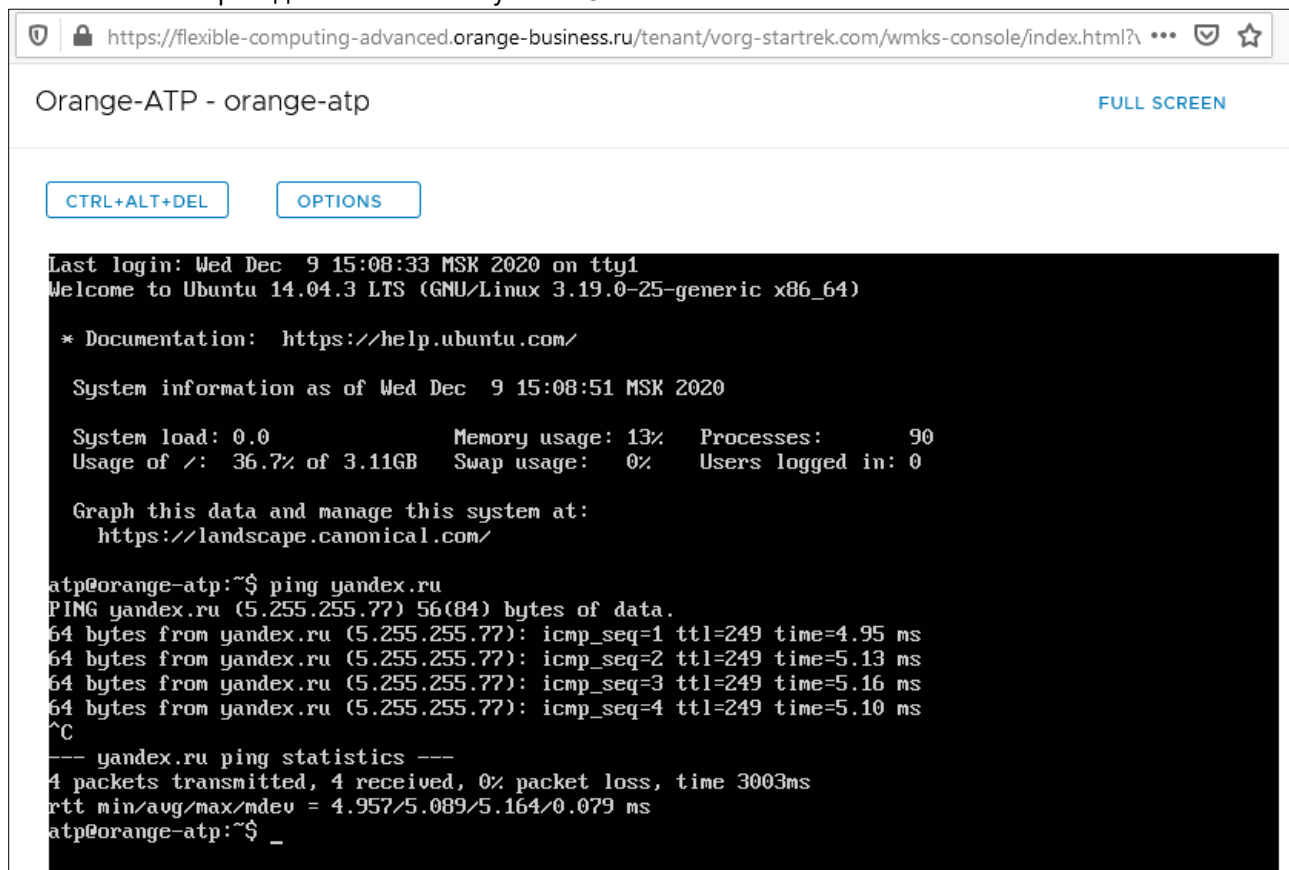
Hardware

Name	orange-atp
Status	Powered on
Computer Name	orange-atp-0
Description	-

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 которой должны быть получены ICMP ответы:



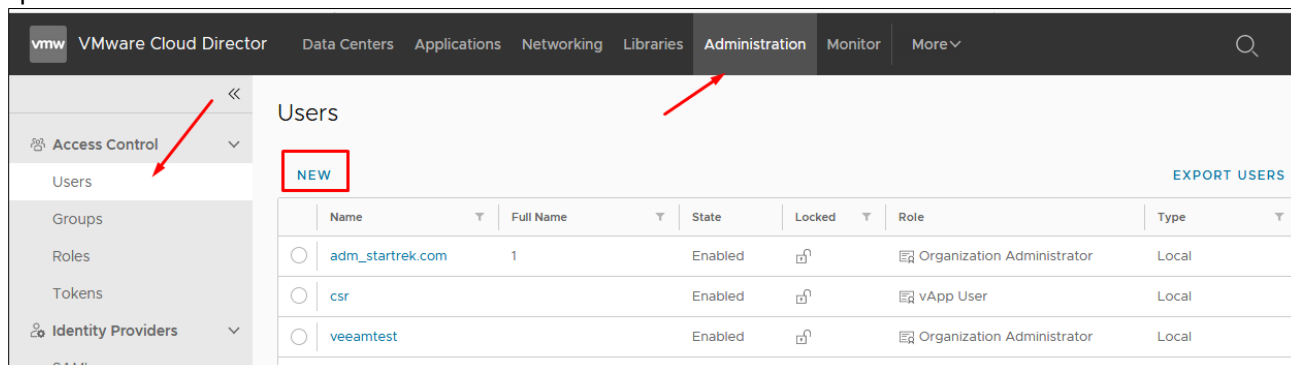
Для сети IPVPN (ВМ atp-ipvpn) процедура аналогична, но проверять следует доступность удалённого хоста в

вашей IPVPN сети.

8. Управление учётными записями пользователей

vCloud 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:

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw VMware Cloud Director', 'Data Centers', 'Applications', 'Networking', 'Libraries', 'Administration', 'Monitor', and 'More'. The left sidebar has 'Compute' expanded, showing 'vApps', 'Virtual Machines', and 'Affinity Rules'. The main area displays 'vApps' with a search bar and filters. A vApp named 'Orange-ATP' is shown with details: Powered on, Lease 52 minutes, Created On 12/09/2020, 3:07:37 PM, Owner system. Below this, a table lists VMs (1) and CPUs (2). A context menu is open over the 'ACTIONS' button, showing options: Power, Renew Lease, Snapshot, Download, Move, Copy, Change Owner, Share (highlighted), and Add. Red arrows point to 'Data Centers', 'vApps', 'ACTIONS', and 'Share'.

The screenshot shows the 'Share' dialog box. The 'Share with' section has 'Specific Users and Groups' selected. The 'Users' tab is active, showing a table with columns 'Name' and 'Access Level'. The table lists 'adm_startrek.com' (Read Only), 'csr' (Read Only), and 'veeamtest' (Read/Write). A dropdown menu is open for 'csr', showing 'Read Only', 'Read/Write', and 'Full Control'. The 'DISCARD' and 'SHARE' buttons are at the bottom right.

9. Загрузка образов (ISO) и шаблонов VM

9.1. Создание каталога

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

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', 'Data Centers', 'Applications', 'Networking', 'Libraries', 'Administration', 'Monitor', and 'More'. The 'Libraries' tab is selected. On the left sidebar, under 'Content Libraries', the 'Catalogs' link is highlighted with a red arrow. The main area displays the 'Catalogs' table with a 'NEW' button in the top left corner, also highlighted with a red arrow. The table lists several catalogs with columns: Name, Version, Status, Shared, External, Owner, Created On, and vApp Templates.

Name	Version	Status	Shared	External	Owner	Created On	vApp Templates
Cisco	23	Ready		-	system	2/16/2017, 3:32:45 PM	1
Cisco IPT	6	Ready		-	system	3/30/2016, 8:53:53 PM	0
Linux Shared	25	Ready		-	system	12/17/2015, 12:36:55 P...	0
Microsoft Shar...	26	Ready		-	system	12/16/2015, 8:58:51 PM	0
Shared catalog	44	Ready		-	system	9/24/2015, 4:28:51 PM	2

Выберите место хранения каталогов:

The 'Create Catalog' dialog box is shown. It has a title bar with a close button. The main content area includes a 'Name this Catalog' section with a text input field containing 'test-catalog'. Below this is a 'Description' section with a text area. A toggle switch for 'Pre-provision on specific storage policy' is turned on, highlighted with a red arrow. Below the toggle is a table titled 'Storage Policy' with a dropdown menu 'Select a storage policy'. The table has two columns: 'Storage Policy' and 'Organization VDC'. It lists five storage policies, each with a radio button. The first two are 'vmstore-cloud-gold' and the last two are 'vmstore-cloud-platinum-da'. The table is highlighted with a red border. At the bottom right of the table, it says '1 - 5 of 9 storage policies'.

Storage Policy	Organization VDC
☐ vmstore-cloud-gold	vdc-startrek.com-01
☐ vmstore-cloud-gold	vdc-startrek.com-da-02
☐ vmstore-cloud-silver	vdc-startrek.com-ha-01
☐ vmstore-cloud-platinum-ha	vdc-startrek.com-ha-01
☐ vmstore-cloud-platinum-da	vdc-startrek.com-da-02

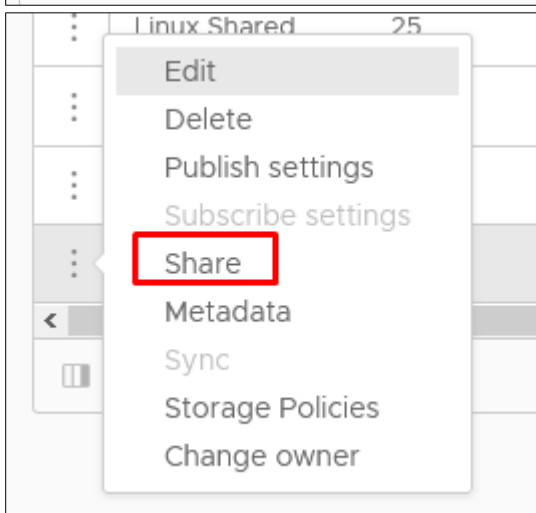
По умолчанию каталог будет доступен всем пользователям вашей организации в режиме только для чтения, в случае необходимости это можно изменить:

Catalogs

NEW

	Name	Version	Status	Shared	External	Owner	Created On	vApp Templates	Media Other
⋮	Cisco	23	Ready	🔒	-	system	2/16/2017, 3:32:45 PM	1	4
⋮	Cisco IPT	6	Ready	🔒	-	system	3/30/2016, 8:53:53 PM	0	2
⋮	Linux Shared	25	Ready	🔒	-	system	12/17/2015, 12:36:55 P...	0	13
⋮	Microsoft Shar...	26	Ready	🔒	-	system	12/16/2015, 8:58:51 PM	0	10
⋮	Shared catalog	44	Ready	🔒	-	system	9/24/2015, 4:28:51 PM	2	2
⋮	test	10	Ready	🔒	-	adm_startrek.co...	6/16/2020, 1:58:14 PM	1	0

1 - 6 of 6 items



Share Catalog 'test'

Users and Groups Organizations

Share with ☒ All Users and Groups ☐ Specific Users and Groups

Access Level Full Control

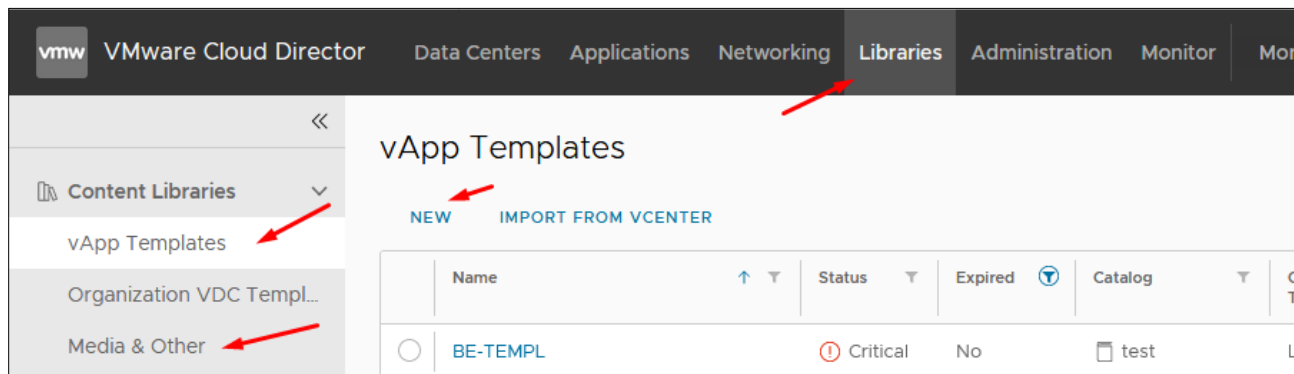
9.2. Загрузка через vCloud Director

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 – 13;
- 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](#).

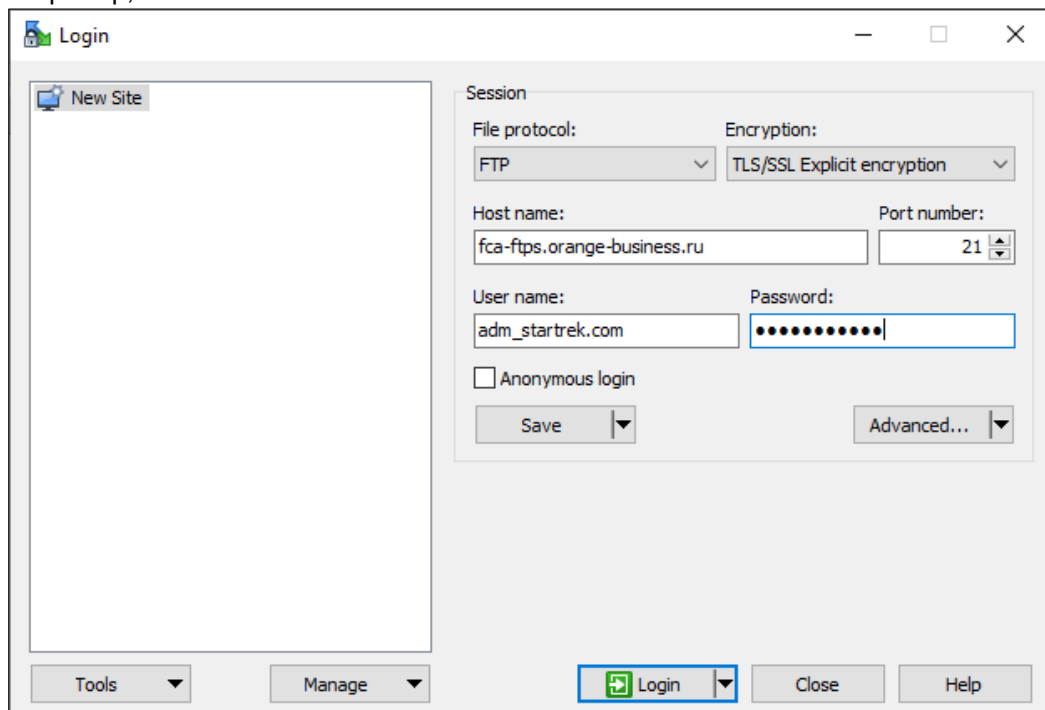


9.3. Загрузка через FTPS-сервер Orange

Альтернативным способом загрузки шаблонов VM является использование FTPS-сервера Orange. Данный вариант более удобен в случае необходимости загрузки большого количества VM или если вы заказали услугу миграции VM силами Orange (в этом случае возможна загрузка файлов VM 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-starttrack.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-starttrack.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-starttrack.com&vdc=vorg-startrack.com-01&catalog=test&media=image"
```

10. Cemu vOrg u vApp

10.1. Создание vOrg cemu

The screenshot shows the VMware Cloud Director interface. The left sidebar has a 'Networking' menu with 'Networks' selected. The main area displays the 'New Organization VDC Network' wizard. The 'Scope' step is active, showing 'Current Organization Virtual Data Center' as the selected scope. Below the wizard, a table lists existing networks:

Name	Status	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared	Route Advertised
Shared-net-test	Normal	192.168.83.1/24	Isolated	-	1%	☒	-

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

The screenshot shows the 'New Organization VDC Network' wizard, 'Network Type' step. The 'Isolated' option is selected, indicating a fully isolated environment accessible only by this organization VDC or VDC Group. The 'Routed' option is also visible, indicating a network providing controlled access to machines and networks outside of the VDC or VDC Group through an edge gateway.

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:

New Organization VDC Network

- Scope
- Network Type
- General**
- Static IP Pools
- DNS
- Ready to Complete

General

Name *

Gateway CIDR * ⓘ

Description

Shared ☐ ⓘ

10.2. Создание vApp сети

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

Name	Status	Gateway CIDR	Connection	Retain the IP/MAC Resources.
Shared-net-te...	✓	192.168.83.1/24	Direct: Shared-net-te...	

1 - 1 of 1 vApp network(s)

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

Add Network to ATP-1.0

Type

☐ OrgVDC Network
 ☐ vApp Network

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

Add Network to Orange-ATP

Type ☐ OrgVDC Network ☒ vApp Network

Name *

Description

Address and DNS

Gateway CIDR *

Primary DNS

Secondary DNS

DNS suffix

Allow Guest VLAN ☐

Static IP Pools
Enter an IP range (format: 192.168.1.2 - 192.168.1.100)

Static IP Pools
Enter an IP range (format: 192.168.1.2 - 192.168.1.100)

Total IP addresses: 0

Connect to an orgVdc network ☒

	Name	Status	Organization VDC	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Sh
☒	Shared-net-test	✓	vdc-startrek.com-ha-...	192.168.83.1/24	Isolated	-	1%	✓
☐	shared-routed	✓	vdc-startrek.com-ha-...	192.168.100.1/25	Routed	-	1%	

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

All vApps > Orange-ATP > test

test DELETE SYNC SYSLOG

General

IP Management

Static Pools

DNS

DHCP

IP Allocations

Services

Routing

EDIT

Firewall Enabled

NAT Enabled

Firewall Rules

#	Name	Enabled	Action	Pro
1	Allow all outgoing traf...	Yes	Allow	An

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.

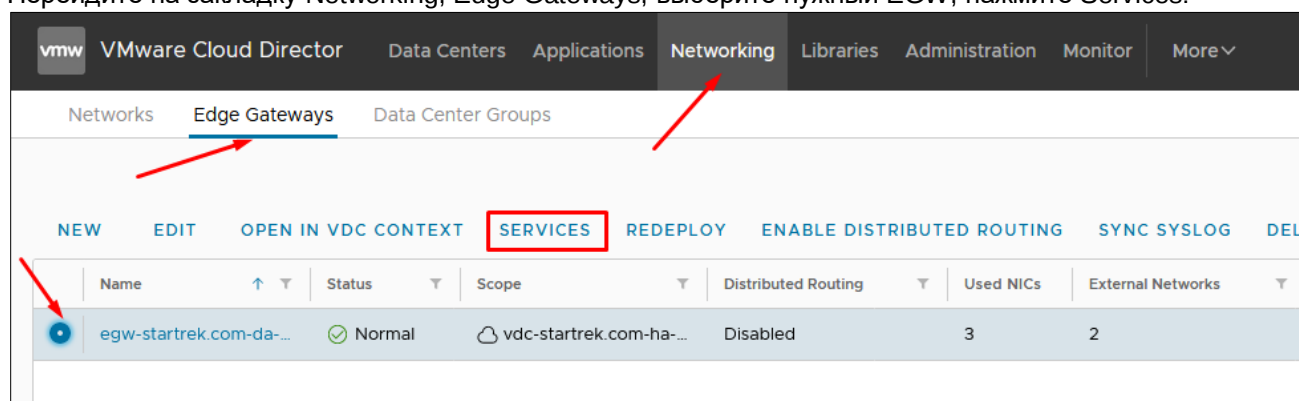
От размера EGW зависит производительность его функций:

	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	1,024	2,048	2,048	2,048
Until Overwrite				
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

Edge Gateway - egw-startrek.com-da-01

Firewall **DHCP** NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings

Pools Bindings Relay

DHCP Pools

 You have unsaved changes.

DHCP Service Status ☒

IP Range	Primary Name Server	Auto Configure DNS	Default Gateway
----------	---------------------	--------------------	-----------------

Задайте параметры пула

Add DHCP Pool ✕

-

IP Range *	16.16.100-172.16.16.200
Domain Name	example.com
Auto Configure DNS	☐
Primary Name Server	172.16.16.1
Secondary Name Server	172.16.16.10
Default Gateway	172.16.16.1
Subnet Mask	255.255.255.0
Lease Never Expires	☐
Lease Time (Seconds)	86400

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

Это можно посмотреть и изменить здесь:

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw VMware Cloud Director', 'Data Centers', 'Applications', 'Networking' (highlighted with a red arrow), 'Libraries', 'Administration', 'Monitor', and 'More'. Below the navigation bar, the 'Networking' section is active, showing 'Networks', 'Edge Gateways', and 'Data Center Groups'. A red arrow points to the 'Networks' tab. The 'NEW' button is visible. A table lists networks:

	Name	Status	Scope	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared
☐	Shared-net-test	Normal	vdc-startrek.com-ha...	192.168.83.1/24	Isolated	-	1%	☒
☐	shared-routed	Normal	vdc-startrek.com-ha...	192.168.100.1/25	Routed	egw-startrek.com-da...	1%	☐

Below the table, the 'shared-routed' network configuration is shown. The 'General' tab is selected. The 'IP Management' section is expanded, showing 'Static IP Pools'. The configuration details are as follows:

Property	Value
Gateway CIDR	192.168.100.1/25
Static IP Pools	192.168.100.2 - 192.168.100.100
Total IP addresses:	99

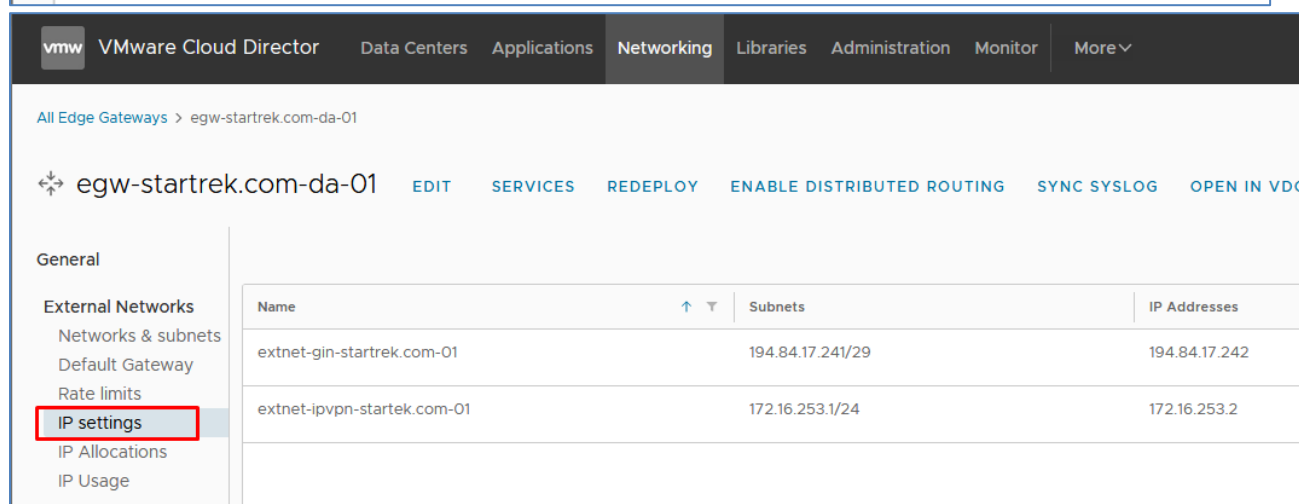
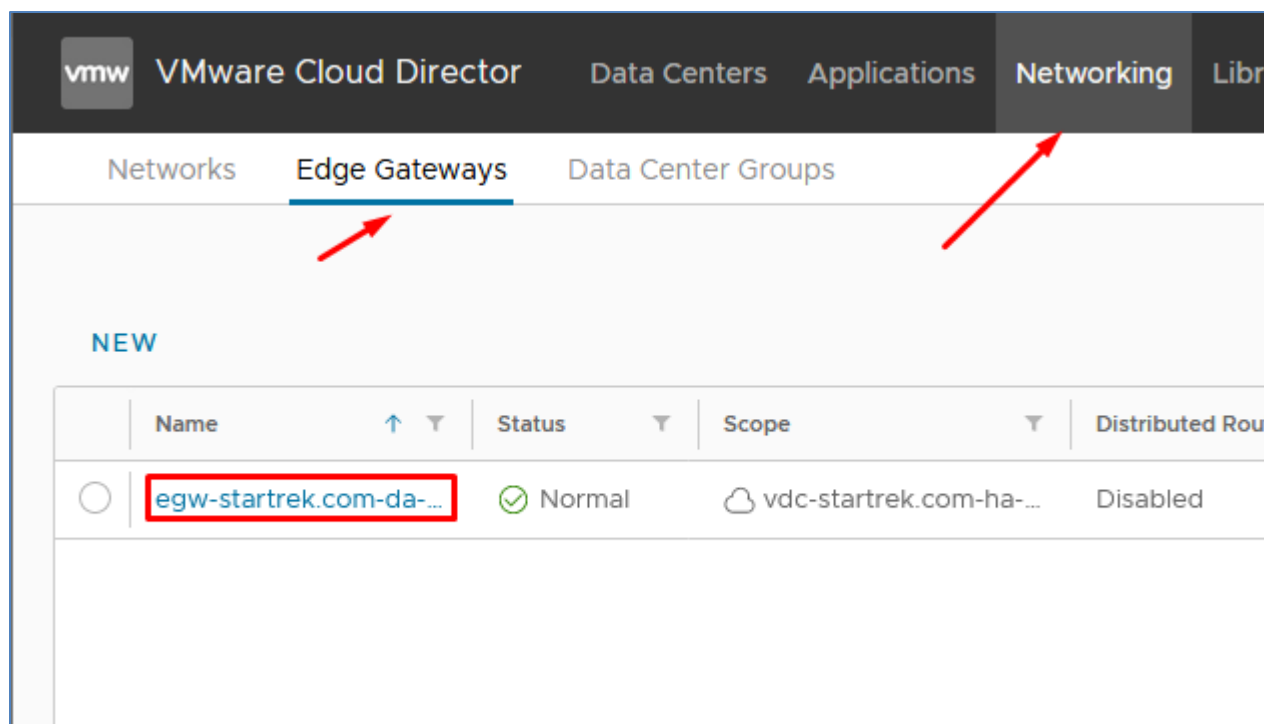
11.3. Настройка NAT

NAT (Network Address Translation) - трансляция частных («серых», RFC1918) IP-адресов во внешние («белые») и наоборот. Благодаря этому процессу ваша виртуальная машина получает доступ в Интернет. Для настройки этого механизма в vCloud 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:

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', 'Data Centers', 'Applications', 'Networking' (selected), 'Libraries', and 'Administration'. Below the navigation bar, the breadcrumb 'All Edge Gateways > egw-startrek.com-da-01' is visible. The main header for the selected Edge Gateway is 'egw-startrek.com-da-01' with buttons for 'EDIT', 'SERVICES', 'REDEPLOY', and 'ENABLE DISTRIBUTED ROUTING'. On the left sidebar, under 'General', the 'IP Allocations' option is highlighted with a red box. The main content area shows a table with the following data:

External network	Sub-allocated IP pools
☐ extnet-gin-startrek.com-01	194.84.17.243 - 194.84.17.243
☐ extnet-ipvpn-startrek.com-01	-

Закройте окно, на нужном EGW выберите пункт Services.

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', 'Data Centers', 'Applications', 'Networking' (selected), 'Libraries', 'Administration', 'Monitor', and 'More'. Below the navigation bar, the breadcrumb 'Networks > Edge Gateways > Data Center Groups' is visible. The main header for the selected Edge Gateway is 'egw-startrek.com-da-01' with buttons for 'NEW', 'EDIT', 'OPEN IN VDC CONTEXT', 'SERVICES' (highlighted with a red box), 'REDEPLOY', 'ENABLE DISTRIBUTED ROUTING', 'SYNC SYSLOG', and 'DELETE'. The main content area shows a table with the following data:

Name	Status	Scope	Distributed Routing	Used NICs	External Networks
egw-startrek.com-da-...	Normal	vdc-startrek.com-ha-...	Disabled	3	2

Перейдите на вкладку NAT, нажимаем кнопку Add SNAT

Edge Gateway - egw-startrek.com-da-01

Firewall DHCP **NAT** Routing Load Balancer VPN Certificates Grouping

NAT Rules

+ DNAT RULE **+ SNAT RULE**    

ID	Type	Action	Applied on	Original	
				IP Address	Port
No NAT rules defined.					

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.

Add SNAT Rule

Applied On: extnet-gin-startrek.com-01 

Original Source IP/Range * 172.16.253.0/24

Translated Source IP/Range * 194.84.17.243

SELECT

Destination IP Address

Destination Port

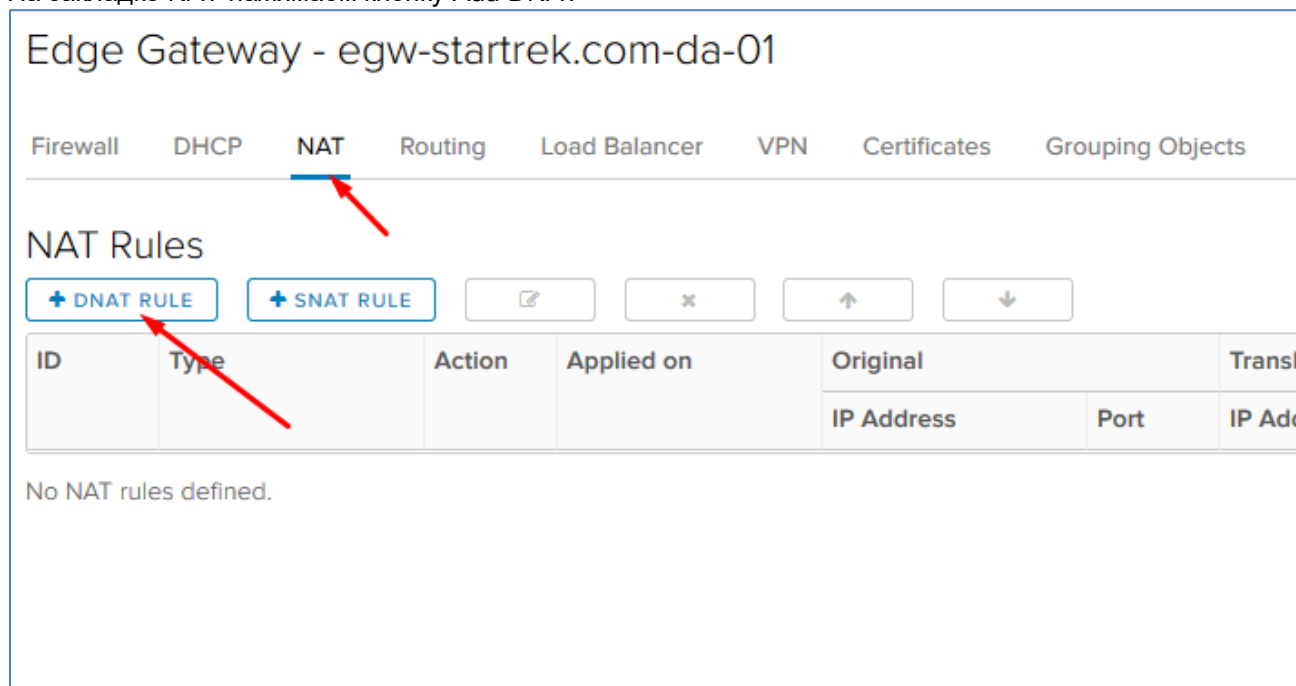
Description

DISCARD **KEEP**

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

Add DNAT Rule

Applied On: extnet-gin-startrek.com-01

Original IP/Range * 194.84.17.243

Protocol TCP

Original Port 443

ICMP Type

Translated IP/Range * 172.16.253.50

Translated Port 443

DISCARD KEEP

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.

VMware Cloud Director | Data Centers | Applications | **Networking** | Libraries | Administration | Monitor | More

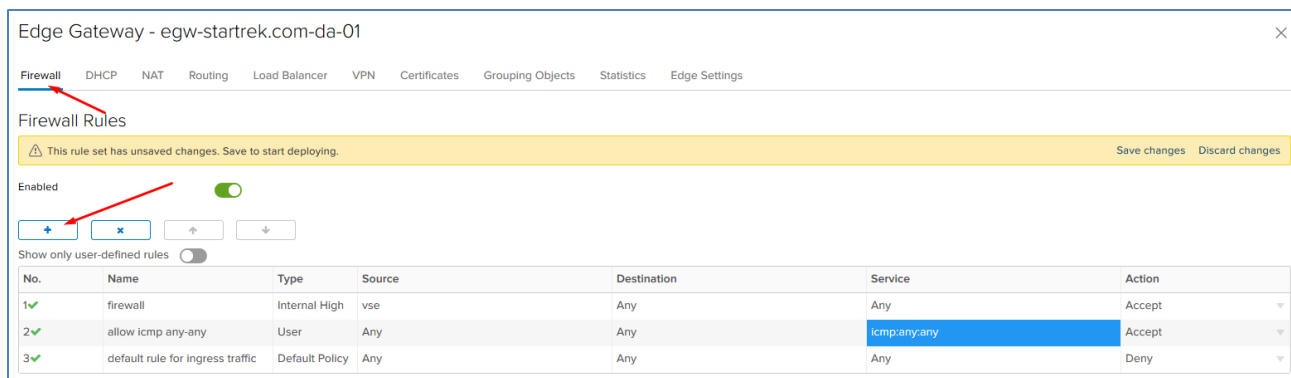
Networks | **Edge Gateways** | Data Center Groups

NEW | EDIT | OPEN IN VDC CONTEXT | **SERVICES** | REDEPLOY | ENABLE DISTRIBUTED ROUTING | SYNC SYSLOG | DEL

Name	Status	Scope	Distributed Routing	Used NICs	External Networks
egw-startrek.com-da-...	Normal	vdc-startrek.com-ha-...	Disabled	3	2

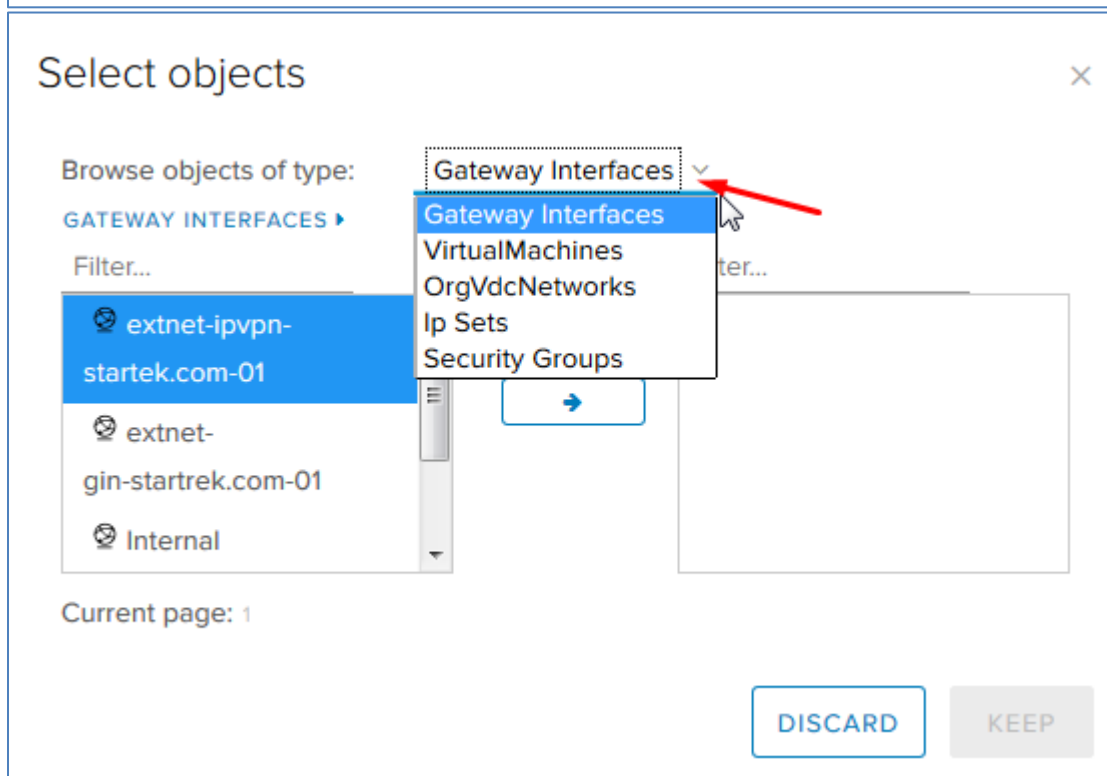
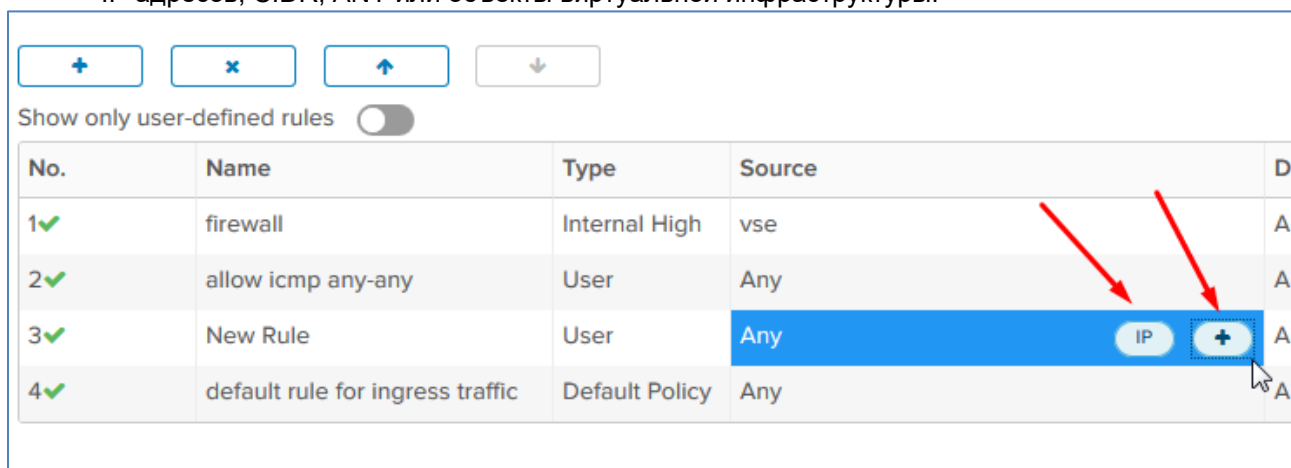
В появившемся окне Services перейдите во вкладку Firewall, нажмите Add.

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: единый 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

Add Service

Protocol

Any

TCP

UDP

ICMP

Any

Source Port

Leaving this field empty will make this rule apply to any port

Destination Port

any

Leaving this field empty will make this rule apply to any port

DISCARD

KEEP

- 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.

Edge Gateway - egw-startrek.com-da-01

Firewall

DHCP

NAT

Routing

Load Balancer

VPN

Certificates

Grouping Objects

Statistics

Edge Settings

Firewall Rules

This rule set has unsaved changes. Save to start deploying.

Save changes Discard changes

Enabled

+

x

↑

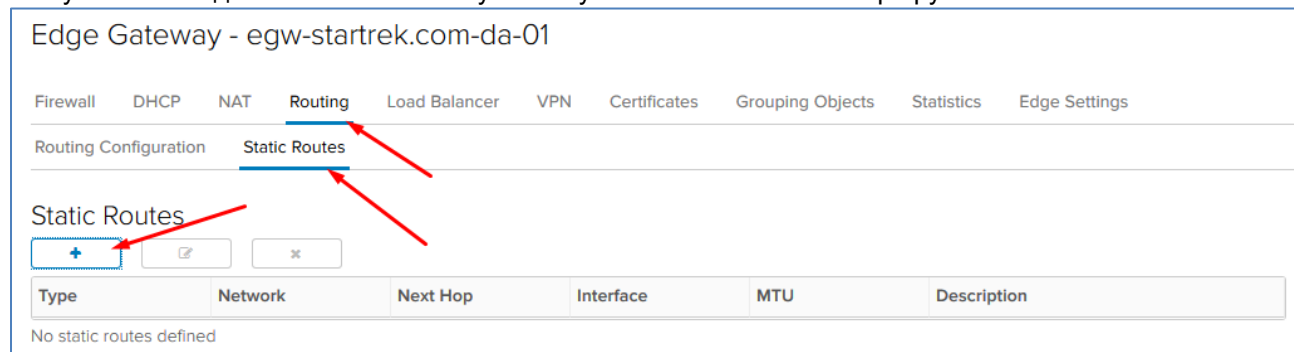
↓

Show only user-defined rules

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal High	vse	Any	Any	Accept
2	allow icmp any-any	User	Any	Any	icmp:any:any	Accept
3	New Rule	User	Any	Any	Any	Accept
4	default rule for ingress traffic	Default Policy	Any	Any	Any	Deny

11.5. Настройка Static routing

В случае необходимости на EGW могут быть указаны статические маршруты.



The 'Add Static Route' dialog box contains the following fields:

- Network ***: A text input field with a hint: 'Network should be entered in CIDR format e.g. 192.169.1.0/24'.
- Next Hop ***: A text input field.
- MTU**: A text input field with the value '1,500'.
- Interface**: A dropdown menu showing 'extnet-gin-startrek.com-01 (extnet-gin-startre...'.
- Description**: A large text area for additional information.

At the bottom right, there are two buttons: 'DISCARD' and 'KEEP'.

11.6. Балансировщик нагрузки (Load Balancer)

Балансировщик является достаточно сложным сервисом, предоставляемым NSX Edge Gateway, поэтому Orange рекомендует ознакомиться 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:

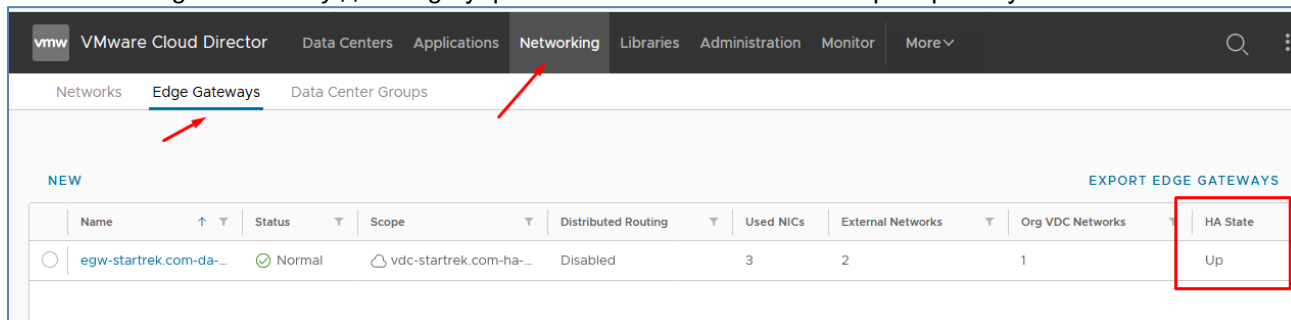
- SSL VPN-Plus, позволяет удаленным пользователям получать доступ к корпоративным приложениям работающим в облаке;

- 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 VT1 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 \(VPN\)](#).

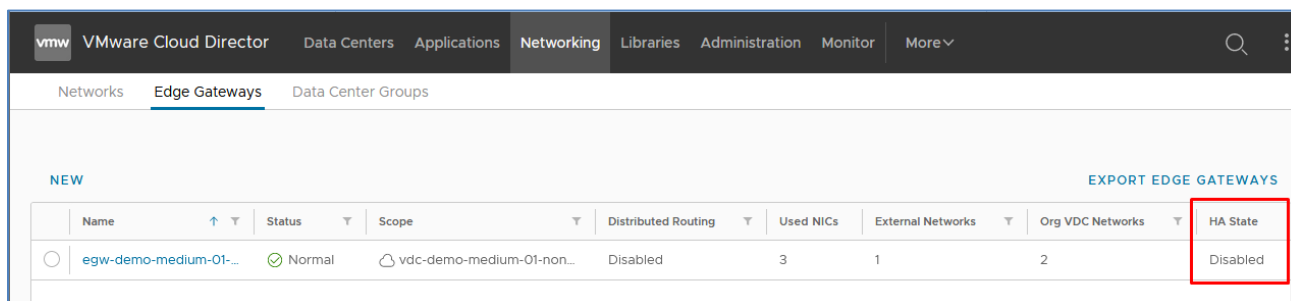
11.8. NSX Edge High Availability

Состояние High Availability для Edge управляемого клиентом можно проверить тут:



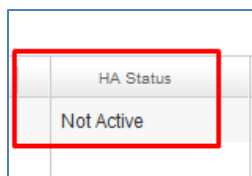
Name	Status	Scope	Distributed Routing	Used NICs	External Networks	Org VDC Networks	HA State
egw-startrek.com-da...	Normal	vdc-startrek.com-ha...	Disabled	3	2	1	Up

«Up» – HA включён.



Name	Status	Scope	Distributed Routing	Used NICs	External Networks	Org VDC Networks	HA State
egw-demo-medium-01...	Normal	vdc-demo-medium-01-non...	Disabled	3	1	2	Disabled

«Disabled» – отключено.



HA Status
Not Active

«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 контейнера vApp

Новый vApp можно создать пустым, из шаблона vApp или с пустой VM (без ОС).

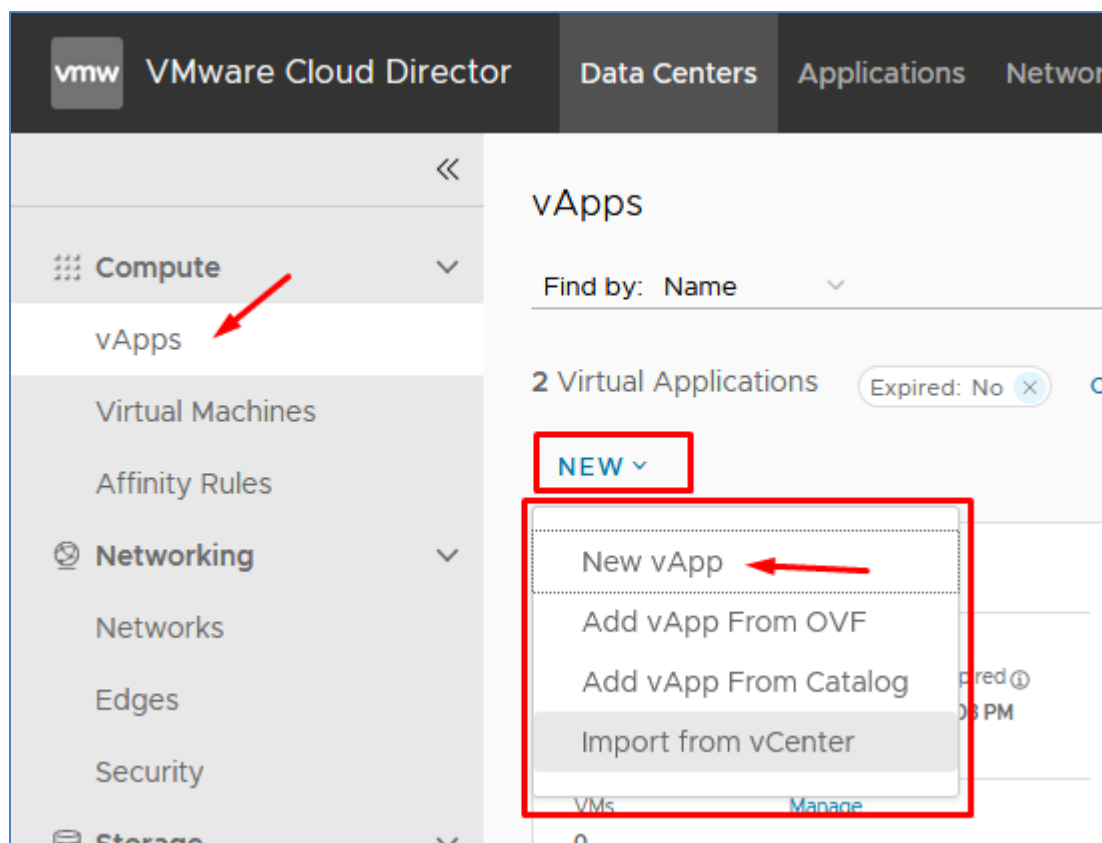
Далее рассмотрим процесс создания vApp с пустой VM.

Выбрать нужный vDC:

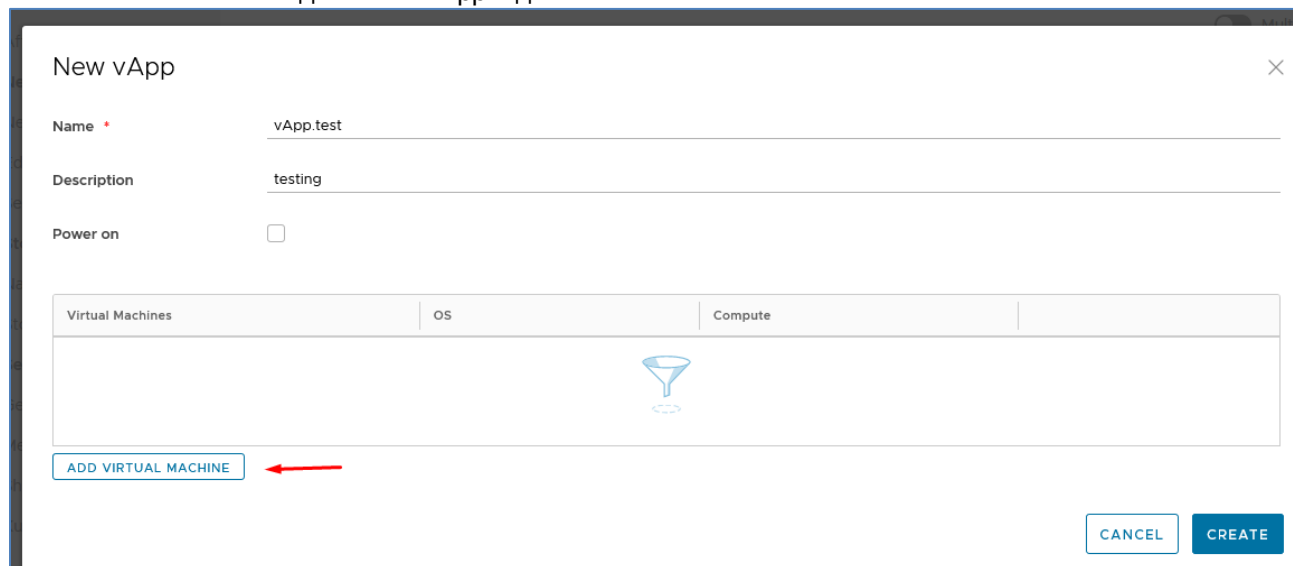
The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'VMware Cloud Director', 'Data Centers', 'Applications', 'Networking', 'Libraries', and 'Administration'. The 'Data Centers' tab is selected, and a red arrow points to it. Below the navigation bar, the 'Virtual Data Center' section is active. It displays a summary of the environment: 1 Site, 1 Organization, 3 Virtual Data Centers, 0 VMs, and 2 vApps. Below this, two vDCs are listed:

- vdc-startrek.com-ha-01**
 - Locations: vorg-startrek.com, flexible-computing-advanced.orange-business.ru
 - Applications: 1 vApps, 0 of 1 Running VMs
 - CPU: 0 MHz (50 GHz allocated)
 - Memory: 0 MB (64 GB allocated)
 - Storage: 512 MB (700 GB allocated)
- vdc-startrek.com-da-02**
 - Locations: vorg-startrek.com, flexible-computing-advanced.orange-business.ru
 - Applications: 2 vApps, 0 of 1 Running VMs
 - CPU: 0 MHz (8 GHz allocated)
 - Memory: 0 MB (10 GB allocated)
 - Storage: 5 GB (30 GB allocated)

Red arrows point to the cloud icon of 'vdc-startrek.com-ha-01' and the cloud icon of 'vdc-startrek.com-da-02'.



В появившемся окне задаем имя vApp и добавляем VM:



В появившемся окне задаем имя vApp и добавляем VM.

New VM

Name *

test-vm

Computer Name *

test-vm

Description

Type

New

From Template

Operating System

OS family *

Select...

Operating System *

Select...

Boot image

Select...

Storage

ADD

Disk	Storage Policy	IOPS	Size

Use custom storage policy:

Networking

CUSTOMIZE

CANCEL

OK

Во вкладке Add Virtual Machines вы можете:

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

12.2. Создание виртуальной машины из шаблона

Выберите уже существующий контейнер vApp, перейдите на вкладку Virtual Machines:

VMware Cloud Director interface showing the vApp 'ATP-DA' and the 'Virtual Machines' tab. The interface includes a left sidebar with navigation options (Compute, Networking, Storage, Settings) and a main panel displaying the vApp details and a table of virtual machines. A red arrow points to the 'vApps' menu item in the left sidebar. Another red arrow points to the 'ALL ACTIONS' dropdown menu, which is open, showing options like 'Power', 'Renew Lease', 'Snapshot', 'Download', 'Move', 'Copy', 'Change Owner', 'Share', 'Add', 'Create Template', 'Convert To VM', 'Edit Badges', and 'Delete'. A third red arrow points to the 'Add' option in this menu. A fourth red arrow points to the 'Add VM' option in a sub-menu that appears when 'Add' is selected. The main panel shows a table with one virtual machine named 'orange-a...'.

Add VMs to Orange-ATP

You can search the catalog for virtual machines to add to this vApp or add a new, blank VM. Once the vApp is created, you can power on the new VM and install an operating system.

Virtual Machines	OS	Compute
🔍		

ADD VIRTUAL MACHINE **CANCEL** **ADD**

Выберите шаблон ВМ из своего или публичного каталога:

New VM

Name *

Computer Name *

Description

Type

☐ New

☒ From Template

Templates

	Name	vApp Name	Catalog	OS	Compute	Storage
☐	ubuntu-test	ubuntu-server-14.04.3	Shared catal...	Ubuntu Linux (64-bit)	CPU 2 Memory 1 GB	Po
☐	orange-atp	Orange-ATP	Shared catal...	Ubuntu Linux (64-bit)	CPU 2 Memory 512 MB	Po
☐	ISE-2.2.0.470-virtual-600GB-SNS34...	ISE-2.2.0.470-virtual-600GB-SNS34...	Cisco	Red Hat Enterprise Linux 7 (64-b...	CPU 4 Memory 16 GB	Po

Storage

Storage Policy

vmstore-cloud-platinum-ha (VDC Default)

CANCEL

OK

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

Storage

Storage Policy

vmstore-cloud-platinum-ha (VDC Default)

Custom Properties

There are no user configurable properties.

End User License Agreements

There are no EULAs to review.

CANCEL

OK

Подключение к сетям:

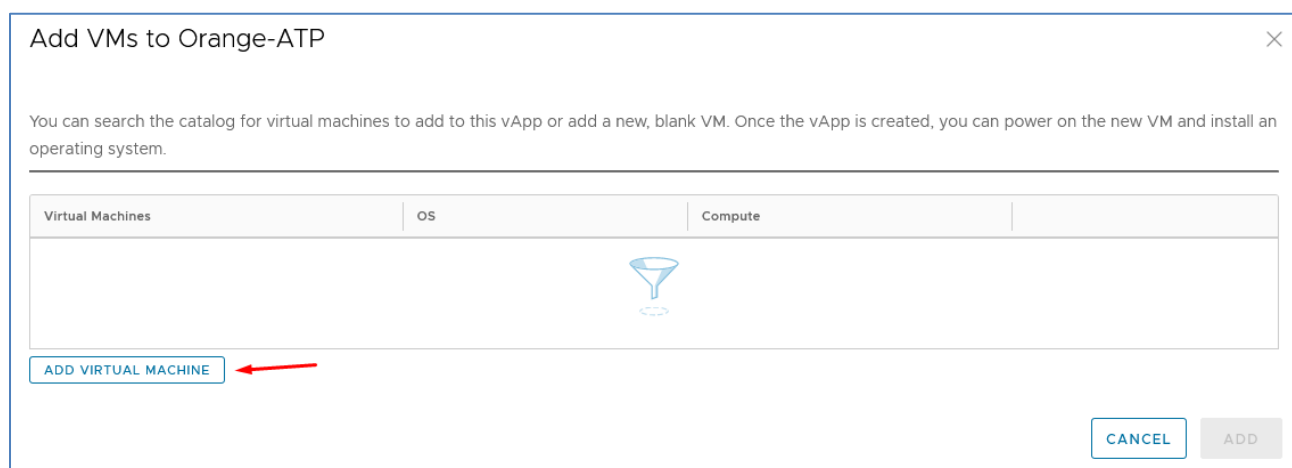
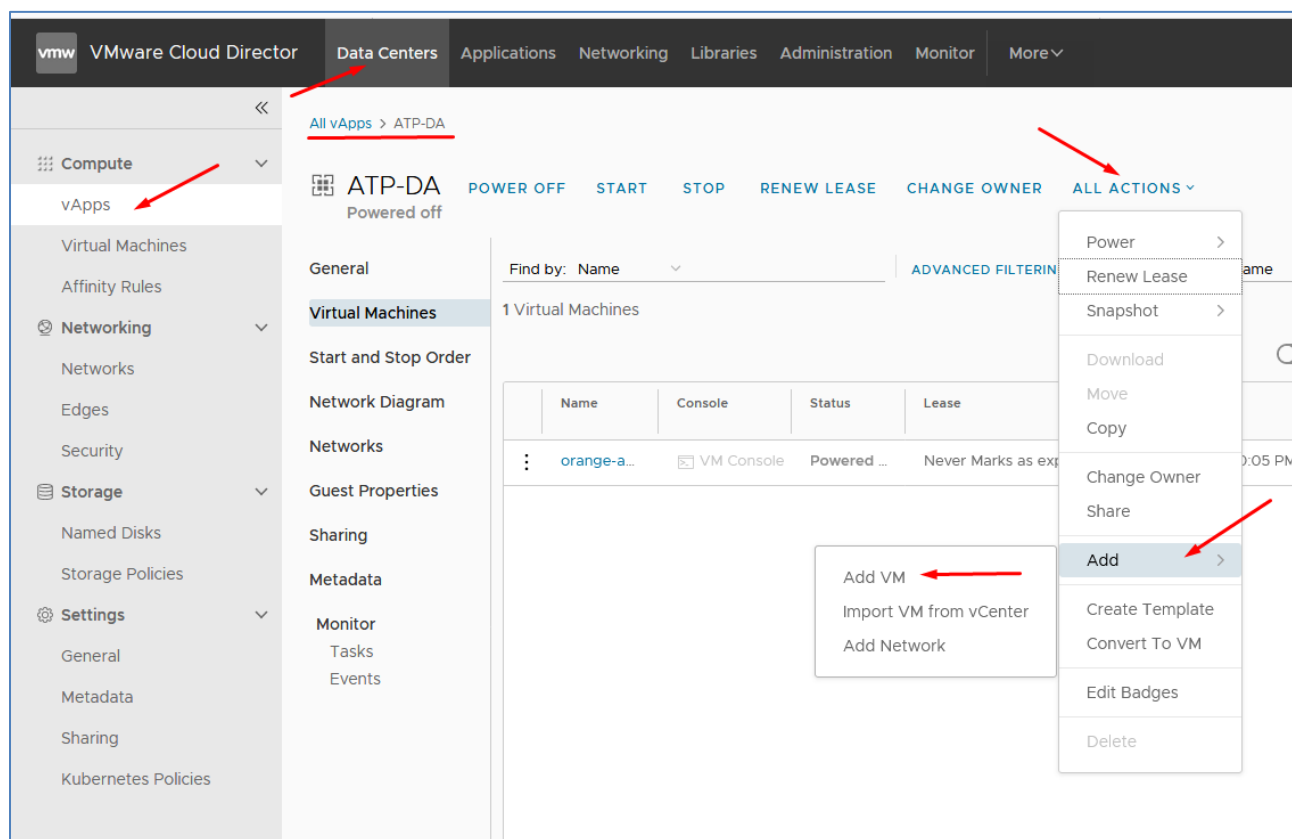
NICs

ADD VAPP NETWORK

Primary NIC	NIC	Connected	Network Adapter Type	Network	IP Mode	IP Address	External IP Address	MAC Address
☐	1	☐	VMXN	None	None		-	00:50:56:01:01
☒	0	☒	VMXN	None	None		-	00:50:56:01:01

Проверьте параметры и завершите создание VM кнопкой Finish.

12.3. Создание виртуальной машины «с нуля»



New VM

Name *

test

Computer Name *

test

Description

Type

New

From Template

Operating System

OS family *

Microsoft Windows

Operating System *

Microsoft Windows Server 2016 (64-bit)

Boot image

Select...

Compute

Select a Size

Small

Medium

Large

Name

↑

↓

Catalog

Bootable_UCSInstall_UCCX_11_0_1_UCOS_11.0.110000-75.sgn.i...

Cisco IPT

Bootable_UCSInstall_UCOS_UNRST_11.0.120000-2.sgn.iso

Cisco IPT

CentOS-7-x86_64-DVD-1511.iso

Linux Share

CheckpointGatewayR80-20.iso

Shared cat

csr1000v-universalk9.03.15.00.S.155-2.S-std.SPA.iso

Cisco

csr1000v-universalk9.03.17.04.S.156-1.S4-std.iso

Cisco

csr1000v-universalk9.16.03.07.iso

Cisco

csr1000v-universalk9.16.06.04.iso

Cisco

DaRT8.1

Shared cat

debian-8.2.0-amd64-DVD-1.iso

Linux Share

debian-8.2.0-amd64-DVD-2.iso

Linux Share

debian-8.2.0-amd64-DVD-3.iso

Linux Share

Fedora-Server-DVD-x86_64-23.iso

Linux Share

OracleLinux-R7-U3-Server-x86_64-dvd.iso

Linux Share

rhel-server-6.6-x86_64-dvd.iso

Linux Share

Storage (GB)

40

80

160

CANCEL

OK

Задайте параметры виртуального оборудования

Compute

Select a Size

Pre-defined Sizing Options

Custom Sizing Options

	CPU	Cores	Memory (MB)	Storage (GB)
Small	1	1	512	40
Medium	2	1	1024	80
Large	4	1	1024	160

Storage

ADD

Disk	Storage Policy	IOPS	Size	
1	VM default policy	Not Applicable	*	GB

Use custom storage policy:

Новая VM появится в списке

Add VMs to Orange-ATP

You can search the catalog for virtual machines to add to this vApp or add a new, blank VM. Once the vApp is created, you can power on the new VM and install an operating system.

Virtual Machines	OS	Compute	
test	Microsoft Windows Server 2016 (64-bit)	CPU2 Memory1 GB Disk100 GB	

ADD VIRTUAL MACHINE

CANCEL

ADD

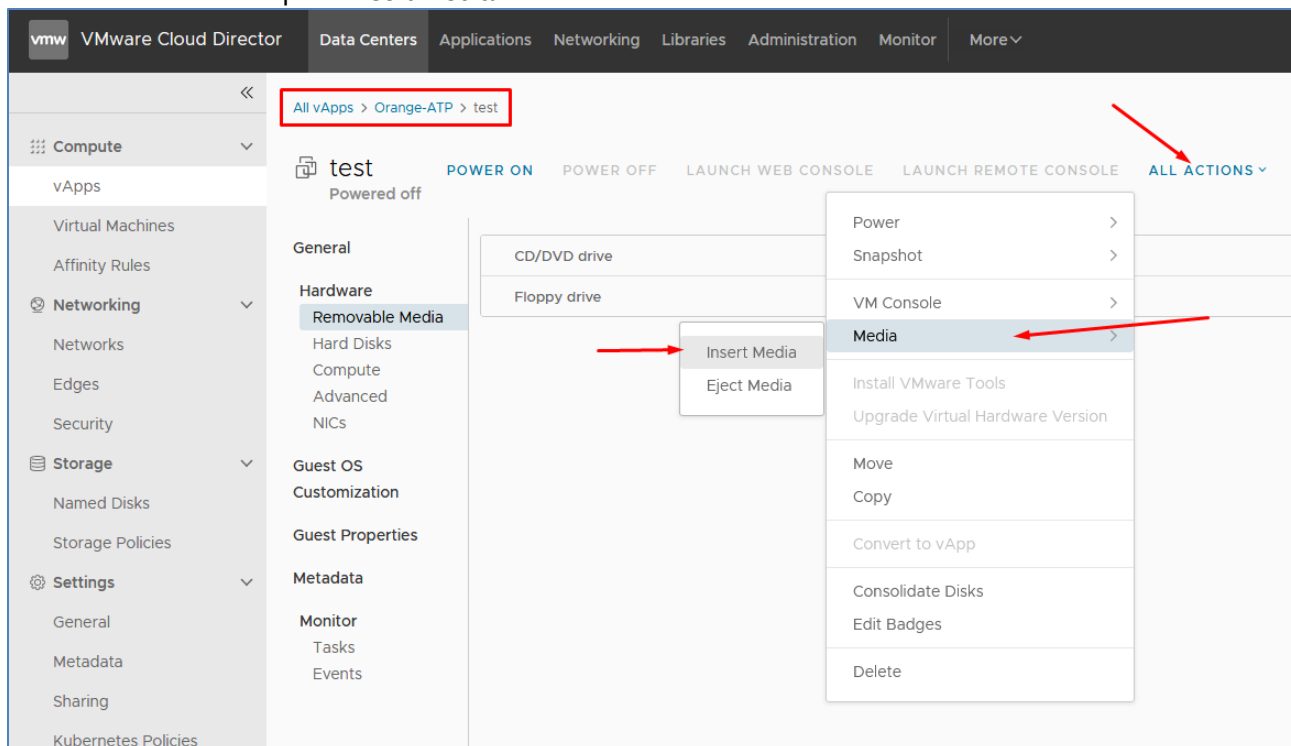
Можно сразу добавить ещё VM.

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 VM выберите Insert Media:



Insert CD

Select the media file to insert in the VM.

Media available now:

Name	Catalog	Owner	Created On	Storage Used
CheckpointGatewayR80-20.iso	Shared catalog	system	4/14/2019, 4:29:26 PM	3248.41 MB
debian-8.2.0-amd64-DVD-2.iso	Linux Shared	system	12/17/2015, 1:37:47 PM	4472.29 MB
OracleLinux-R7-U3-Server-x86_64-dvd.iso	Linux Shared	system	6/6/2017, 3:47:41 PM	4425.00 ...
rhel-server-6.9-x86_64-dvd.iso	Linux Shared	system	5/25/2017, 4:14:53 PM	3707.00 ...
SW_DVD9_SQL_Svr_Standard_Edtn_2008_R2_Russian_MLF_X16-29612.ISO	Microsoft Shar...	system	9/28/2016, 7:00:56 P...	4100.75 MB
debian-8.2.0-amd64-DVD-3.iso	Linux Shared	system	12/17/2015, 1:38:07 PM	4477.71 MB
ubuntu-14.04.3-server-amd64.iso	Linux Shared	system	12/17/2015, 1:39:09 PM	574.00 MB
Bootable_UCSInstall_UCCX_11_0_1_UCOS_11.0.110000-75.sgn.iso	Cisco IPT	system	3/30/2016, 9:13:09 PM	4734.17 MB
csr1000v-universalk9.03.17.04.S.156-1.S4-std.iso	Cisco	system	7/4/2018, 12:42:49 PM	425.41 MB
SW_DVD9_NTRL_SQL_Svr_Standard_Edtn_2016_64Bit_English_OEM_VL_X20-97264.iso	Microsoft Shar...	system	6/21/2018, 6:48:15 PM	2832.65 MB
SW_DVD9_Windows_Svr_Std_and_DataCtr_2012_R2_64Bit_English_-4_MLF_X19-82891.IS...	Microsoft Shar...	system	12/16/2015, 8:59:07 P...	5149.95 MB
SW_DVD9_NTRL_SQL_Svr_Standard_Edtn_2017_64Bit_English_OEM_VL_X21-56945.iso	Microsoft Shar...	system	6/21/2018, 10:49:55 P...	1474.61 MB
SW_DVD5_SA_Win_Ent_7w_SP1_64BIT_English_-2_MLF_X17-58882.ISO	Microsoft Shar...	system	12/29/2016, 5:41:52 PM	3035.17 MB

CANCEL

INSERT

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 BM:

vmw VMware Cloud Director Data Centers Applications Networking Libraries Administration Monitor More ▾

« All vApps > Orange-ATP > test

Compute ▾

vApps

Virtual Machines

Affinity Rules

Networking ▾

Networks

Edges

Security

Storage ▾

Named Disks

Storage Policies

Settings ▾

General

test POWER ON POWER OFF LAUNCH WEB CONSOLE LAUNCH REMOTE CONSOLE ALL ACTIONS ▾

Powered off

General

Hardware

Removable Media

Hard Disks

Compute

Advanced

NICs

Guest OS

Customization

Guest Properties

Metadata

Monitor

EDIT

Name	test
Status	Powered off
Computer Name	test
Description	-
Operating System	Microsoft Windows Server 2016 (64-bit)
Boot Delay	0
Storage Policy	vmstore-cloud-platinum-ha
Virtual Data Center	vdc-startrek.com-ha-01
Owner	system

×

Edit VM test

Name *

test

Computer Name *

test

Description

Operating System Family

Microsoft Windows

Operating System

Microsoft Windows Server 2016 (64-bit)

Boot Delay *

0

Storage Policy

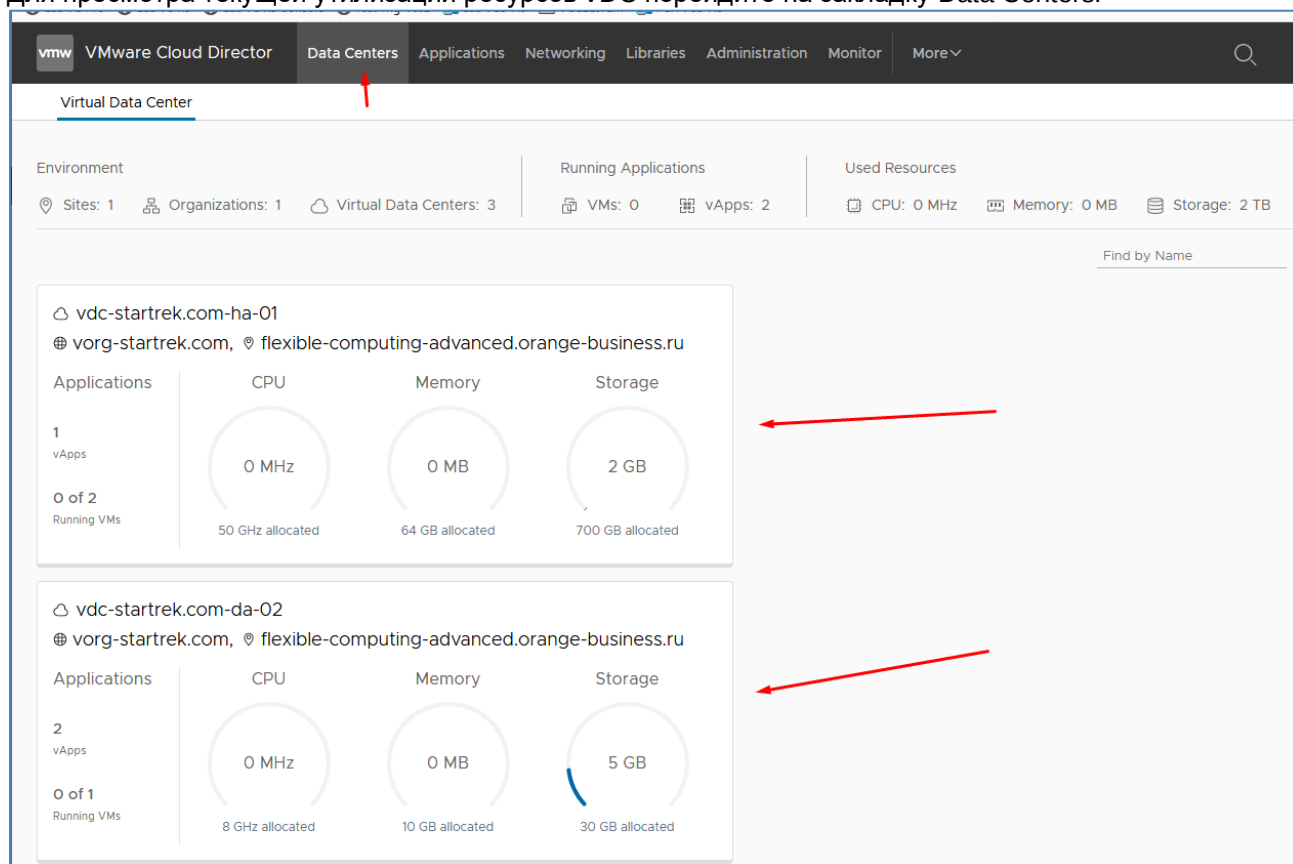
vmstore-cloud-platinum-ha

Enter BIOS Setup

☒

12.5. Мониторинг ресурсов

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



Более подробную информацию можно посмотреть внутри vDC:

General

Info

Name	vdc-startrek.com-ha-01
Description	-
Status	Enabled

Metrics

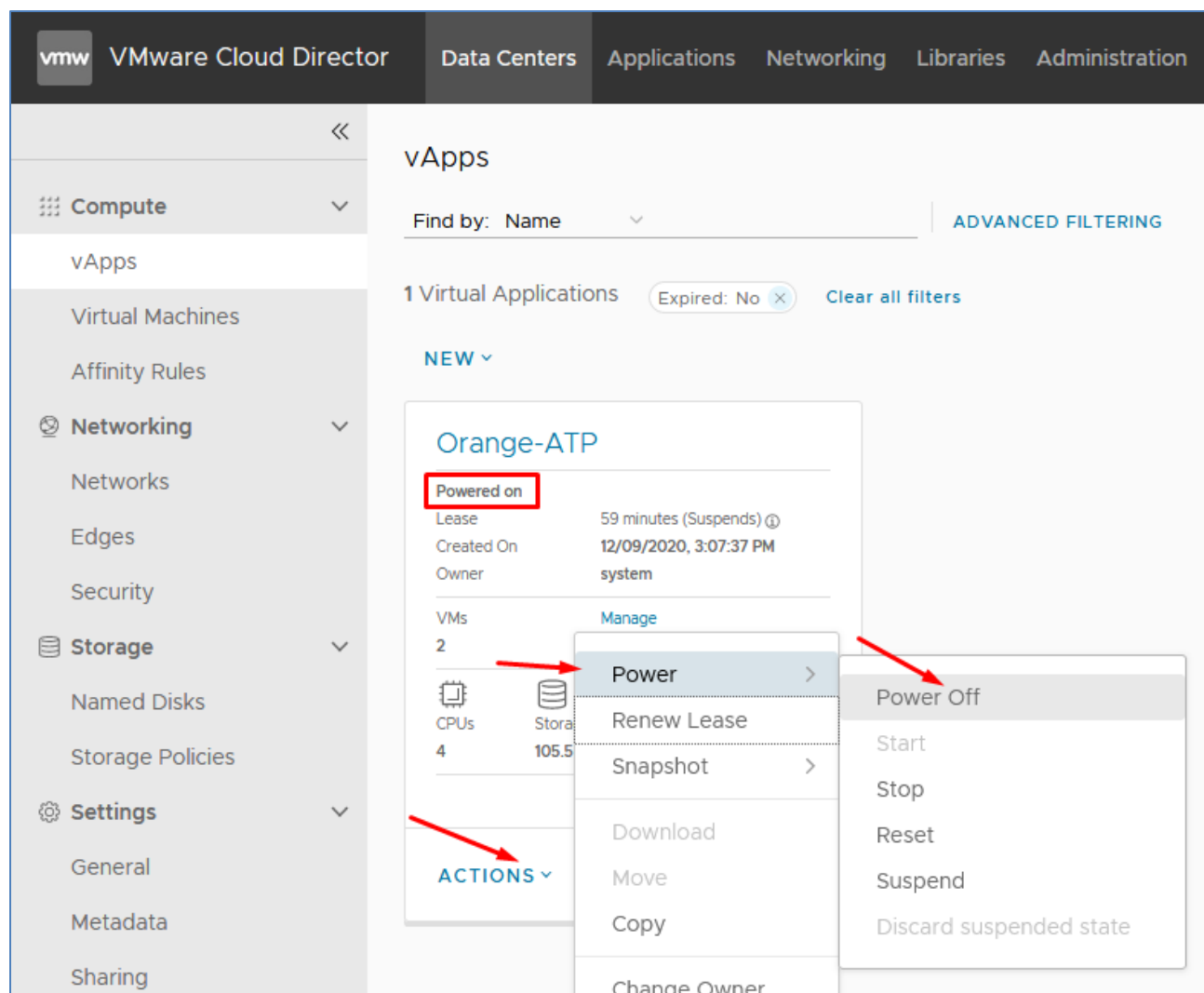
Allocation Model	Allocation pool
vCPU	2.2 GHz
CPU (Allocation Used/Quota)	0 MHz / 50 GHz (0%)
Memory (Allocation Used/Quota)	0 MB / 64 GB (0%)

Storage Policies

	Name	Status	Default	Used	Limit	Capabilities
☐	vmstore-cloud-gold	✓	-	0 MB	100 GB	1
☐	vmstore-cloud-platinum-ha	✓	✓	5.5 GB	500 GB	4
☐	vmstore-cloud-silver	✓	-	100 GB	100 GB	1

12.6. Выгрузка шаблона vApp из vCloud 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 VM

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 VM.

В случае отсутствия установленных (процесс установки завершён, ос перезагружена, образ отмонтирован) и работоспособных (гипервизор имеет возможность подключения) VMware Tools в операционной системы виртуальной машины:

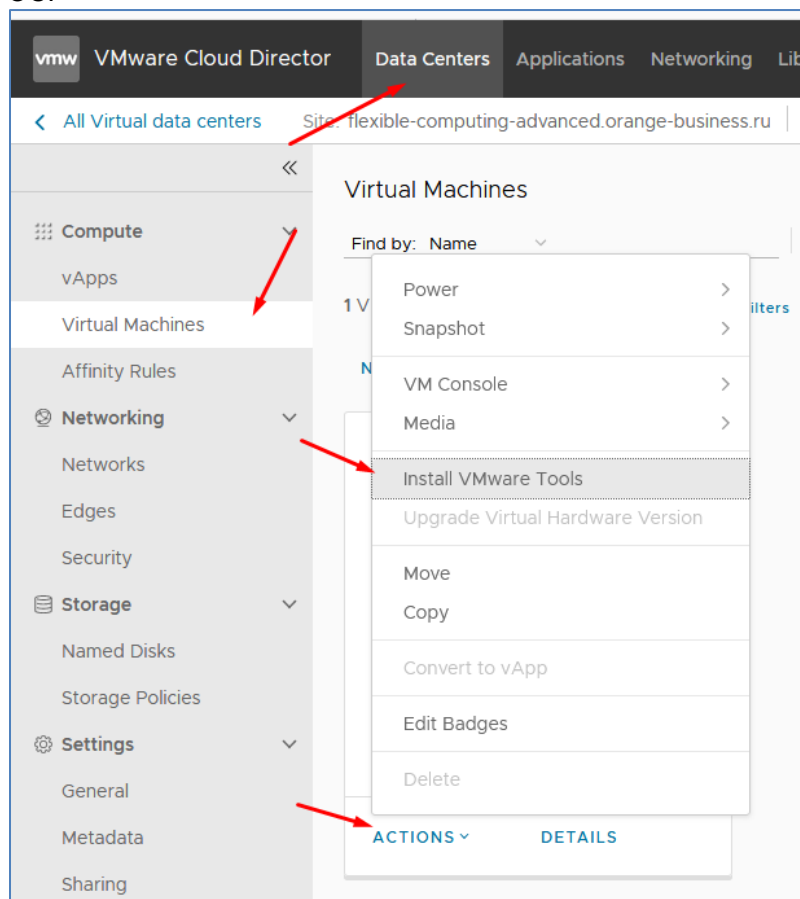
- резервные копии VM могут быть неконсистентными с большей вероятностью;
- в случае если при проведении аварийно-восстановительных работ VM клиента не может быть перемещена на другой гипервизор и этим блокирует работы, VM может быть перезагружена без согласования с клиентом;
- в случае аварии на хосте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

Актуальные и подробные инструкции находятся [здесь](#).

Версия 3.0.4 © Orange Business Services, 2021

57

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 ту-же политику, что и основной диск ВМ.

Из контекста ВМ:

The screenshot displays the VMware Cloud Director interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', and several tabs: 'Data Centers', 'Applications', 'Networking', 'Libraries', 'Administration', 'Monitor', and 'More'. The 'Data Centers' tab is selected, and the breadcrumb path is 'All vApps > ATP-1.0 > orange-atp'. The left sidebar shows a tree view with 'Compute' expanded, and 'vApps' selected. The main area shows the 'orange-atp' vApp, which is 'Powered on'. The 'General' tab is active, and the 'EDIT' button is highlighted. Below the main interface, the 'Edit VM orange-atp' dialog is shown, with the 'Storage Policy' field highlighted.

Name	orange-atp
Status	Powered on
Computer Name	orange-atp-0
Description	-
Operating System	Ubuntu Linux (64-bit)
Boot Delay	0
Storage Policy	vmstore-cloud-platinum
Virtual Data Center	vdc-startrek.com-01
Owner	adm_startrek.com
VMware Tools	2147483647
Virtual Hardware Version	Hardware Version 10
vApp	ATP-1.0

Edit VM orange-atp

Name * orange-atp

Computer Name * orange-atp-0

Description

Operating System Family Linux

Operating System Ubuntu Linux (64-bit)

Boot Delay * 0

Storage Policy vmstore-cloud-platinum

Enter BIOS Setup ☐

Установка политик для дисков ВМ:

VMware Cloud Director Data Centers Applications Networking Libraries Administration Monitor More

All vApps > ATP-1.0 > orange-atp

orange-atp Powered on

General Hardware Removable Media **Hard Disks** Compute Advanced NICs Guest OS Customization Guest Properties

VM Storage Policy vmstore-cloud-platinum

EDIT

Index	Name	Shared	Size	Policy	IOPS	Bus Type
0	-	No	4 GB	vmstore-cloud-silv...	0	LSI Logic Parallel (SC...
1	-	No	2.05 TB	vmstore-cloud-silv...	0	LSI Logic Parallel (SC...

Edit Hard Disks for orange-atp

Some hard drive properties cannot be modified while the virtual machine is powered on

ADD

Index	Name	Shared	Size	Policy	IOPS	Bus Type	Bus Number	Unit Number
0	-	No	4 GB	vmstore-cloud	Not Applicable	LSI Logic Para	0	0
1	-	No	2100 GB	vmstore-cloud-silver	Applicable	LSI Logic Para	0	1

DISCARD SAVE

(Use VM default) – означает ту-же политику, которая назначена для метаданных.

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. <i>Примечание: аналогичные проблемы наблюдались на Windows 7 и Server 2008R2.</i>	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	-