

Flexible Computing Advanced

User Guide

1.	Introduction	3
2.	Options and Features Navigator	3
3.	Architecture, options, features and recommendations	3
3.1.	Architecture overview	3
3.2.	DA or DR? RTO and RPO indicators	5
3.3.	Disaster Avoidance (DA)	6
3.4.	Disaster Recovery (DR)	6
3.5.	Storage Subsystem	6
3.5.1.	Available storage levels (storage policies) of VM disks	6
3.5.2.	Общие рекомендации при размещении дисков ВМ	7
3.5.3.	Уровень #SYSTEM	7
3.5.4.	Storage Levels Disaster Avoidance (DA)	8
3.5.5.	Disk consumption in Cloud Director	8
3.5.6.	VM disk testing methodology	8
3.6.	Backup to disk	14
3.7.	Backup (archiving) to tape	14
3.8.	Independent backup management (Self Service Backup)	15
3.9.	Dedicated GHz and vCPUs	15
3.10.	Fault-tolerant access to Internet and BVPN networks	15
3.11.	VMware NSX Edge	17
3.12.	NSX Edge High Availability	19
3.13.	Protection against DDoS attacks	19
3.14.	Rental of software licenses	19
3.15.	Microsoft software activation via the SPLA program using KMS	20
3.16.	How to connect a local network to the Orange cloud?	20
3.17.	Connecting external USB devices (USB-to-IP)	22
3.18.	Connecting external network devices / servers located in the Orange DC's	22
4.	Main elements of VMware Cloud Director	22
5.	Login to the virtual data center	23
6.	Typical problems when connecting to the web interface and using it	24
7.	Checking vDC resource availability and network connectivity	24
7.1.	Checking resource availability	25
7.2.	Checking network resources	27
8.	User account management	29
9.	Uploading images (ISO) and VM templates	32
9.1.	Directory creation	32
9.2.	Uploading via Cloud Director	34
9.3.	Upload via the Orange FTPS server	35
9.4.	Upload via ovftool	35
10.	VOrg and vApp networks	36
10.1.	Creating a vOrg network	36
10.2.	Creating a vApp network	37
11.	NSX Edge Gateway	39
11.1.	NSX Edge Gateway size and performance	39
11.2.	DHCP configuration	40
11.3.	NAT configuration	42
11.3.1.	Creating a SNAT rule	42
11.3.2.	Creating a DNAT rule	46

11.4.	Firewall configuration	47
11.5.	Static Routing configuration	50
11.6.	Load Balancer	50
11.7.	VPN	50
11.8.	NSX Edge High Availability	51
12.	Configuring and managing virtual machines and vApps.....	51
12.1.	Creating a new vApp	51
12.2.	Creating a virtual machine from a template	55
12.3.	Creating a virtual machine from scratch	57
12.4.	Installing an OS on a virtual machine	60
12.5.	Resource monitoring	62
12.7.	Exporting a vApp template from Cloud Director.....	66
12.8.	Installing VMware Tools on a VM	67
12.9.	Selecting storage type for VM	68
12.10.	Named Disks.....	72
12.11.	Hosting of VM in a specific data center	72
12.12.	Affinity и anti-affinity правила ВМ	74
13.	Known Issues.....	75

1. Introduction

The purpose of this guide is to demonstrate how to perform the initial steps and basic operations on the cloud platform Orange Flexible Computing Advanced.

For more information, see the [Cloud Director Documentation Home](#).

To ensure the safety and functionality of the Platform, Orange installs patches on a regular basis and updates for the platform's software, which may lead to changes in the interface and the emergence of new functions not described in this document. If you have any questions, contact your Orange representative or consult the VMware documentation for the corresponding software version.

This version of the document is based on VMware Cloud Director version 10.5.

2. Options and Features Navigator

	Description	Configuration
Basic functionality		
Managing a virtual DC (vDC) via the WEB interface	4, 5	12
Using ready-to-use and custom VM images (ISO/vApp template)	9	
Managing virtual networks	10	
NSX Edge Gateway virtual firewall	3.11	
Rental of software licenses	3.14	
External devices		
Connecting external USB devices (USB-to-IP)	3.17	
Connecting external network devices or servers located in the primary DC	3.18	
Failover options		
Platform architecture of the Disaster Avoidance level	3.1	
Resource reservation + priority VM launch in the event of a disaster	3.3	
Placement of VM disks in two DCs (synchronous replication)	3.5	
Distribution of VMs between DCs	3.3	12.11
Affinity and anti-affinity rules of the VM	12.12	
Network		
Fault-tolerant Internet access (via two DCs, different PEs, different last miles)	3.103.11	11.3
Fault-tolerant access to IVPN (via two DCs, different PEs, different last miles)		
Edge GW in High Availability mode	3.11	11.8
Protection against DDoS attacks	3.13	
Storage		
Silver/Gold/Platinum	3.5	12.9
Silver/Gold/Platinum DA		
Platinum Plus		
Backup and archiving		
Backing up to disk	3.6	
Archiving and restoring to/from tape	3.7	
Offsite tape storage		
Self Service Backup	3.8	

3. Architecture, options, features and recommendations

3.1. Architecture overview

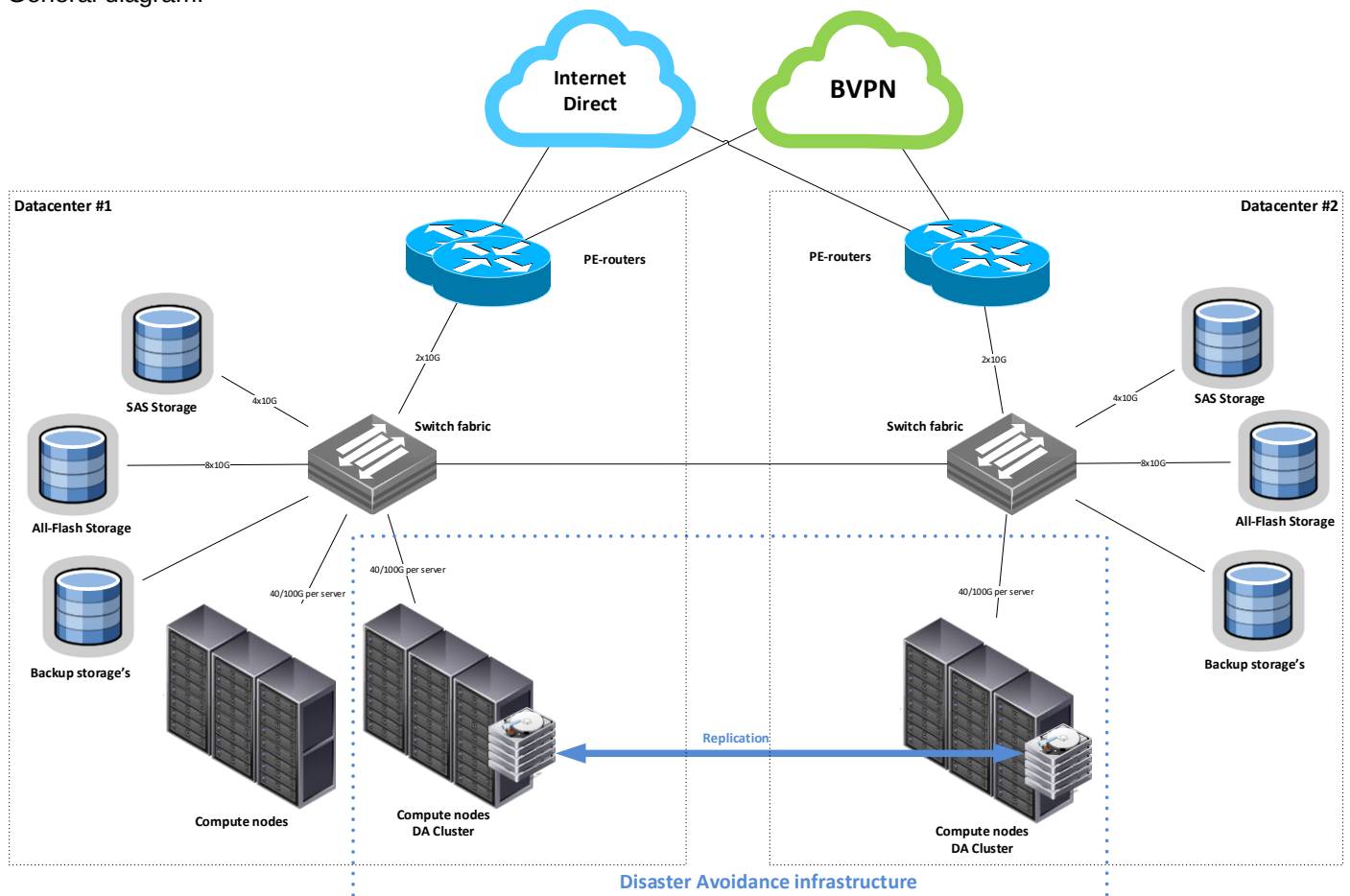
Orange's main goal in building the infrastructure of a public cloud is to ensure fault tolerance. For this, an integrated approach is applied at all levels:

- Depending on the customer's services configuration, different combinations of data centers (hereinafter referred to as DCs) from the list may provide the services:
 - [IXcellerate Moscow One](#) (Tier 3+), 33G Altufevskoe Shosse, Moscow;
 - [Nord4](#) (Tier 3), 41 Korovinskoe Shosse, Moscow;
 - Orange technical center «Petrovka», 15/16 Petrovka street, Moscow;
- ADVA, PacketLight
- The expertise of the engineers is constantly updated and refreshed;

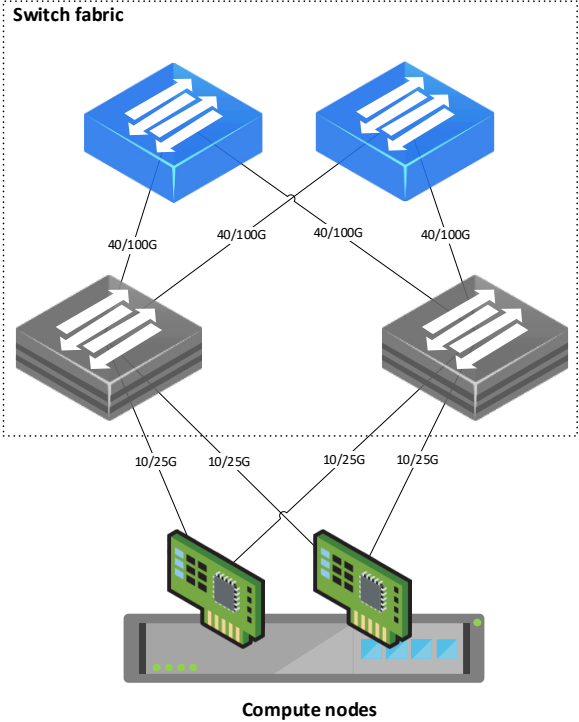
- DWDM communication channels) are laid using different routes around the city, they enter the DCs through different cable collectors. Inside the DC the routes never intersect at the level of cable trays. DWDM channels operate on two completely independent sets of equipment;
- Network latency between DCs: 0.3-1,5 ms when measuring VM<>VM, (depends on the location of the VM);
- All equipment has at least two power supplies and is connected to different power lines;
- All network connections between the devices have at least two cable connections and are terminated at different switches (MC-LAG);
- At least two different physical multi-port network cards are used to connect the servers;
- External network services (Internet Direct, BVPN) are provided using different routes from two independent PE routers in different DCs;
- All traditional storage systems have at least two controllers and RAID-based disk redundancy.
- DA clusters are located in different DCs using synchronous replication
- A physically dedicated control cluster is used, it is built in two DCs using DA technology;
- All mission-critical services of the control cluster are reserved at the application level and distributed between DCs;
- 24/7 monitoring of equipment status and service availability.

The combination of these measures allows Orange to ensure the highest level of service availability for the end customer.

General diagram:



Connecting computing nodes:



Characteristics of the computing nodes of the clusters:

nn	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

3.2. DA or DR? RTO and RPO indicators

To protect against natural and man-made disasters or terrorist attacks and ensure business processes remain uninterrupted, it is necessary to back up the main data storage and processing systems. In the event of a disaster, the data center's building can be damaged, therefore, to ensure the continuity of the service, it is necessary to use a geographically remote site as a backup data center. Let's look at what the relationship between Disaster Recovery (DR) and Disaster Avoidance (DA) is for a modern virtual data center.

What is the difference between disaster avoidance and disaster recovery?

Disasters can be due to natural causes, including earthquakes and hurricanes, or accidents such as a fire, or they can be man-made like military action or terrorism. In all cases, such a disaster is an unplanned event that inevitably disrupts the operation of the main virtual data center.

Disaster recovery refers to the strategy used to minimize the impact of disruptions and recover critical business functions after a disaster. A disaster recovery strategy typically includes a Recovery Point Objective (RPO, the maximum period of time for which data may be lost) and a Recovery Time Objective (RTO, the tolerable period of system unavailability) indicators, as well as the hardware, software, and methods needed to achieve these targets.

For example, a traditional disaster recovery plan might involve restoring five key business applications to normal operation within 60 minutes of a disaster event (RTO), with only up to 10 minutes of lost data (RPO). The actual RPO and RTO values will depend on your specific business needs and the associated hardware, software, and personnel investments. Organizations with *many* mission-critical applications and strict RPO and RTO requirements typically have to invest significantly more in hardware and software infrastructure to achieve these goals in comparison to businesses with *few* mission-critical applications and lighter RTO/RPO requirements. A simple example of disaster recovery (DR) is backup recovery, where servers are rebooted using the latest set of backups stored on local or

remote storage systems.

In comparison, a **Disaster Avoidance (DA)** strategy is an effort primarily aimed at *preventing* any disruptions associated with disasters. DA provides resiliency, not just recovery, i.e., it maintains the availability of applications by taking predictable failures into account. A simple example of disaster avoidance is virtual machine migration. For example, virtual machines can be moved to other host servers so that maintenance or an upgrade of the original host server can be performed while preventing hardware failures (minor disasters). Likewise, if you know that a hurricane is coming toward your main data center, then you can transfer the workload to servers at another data center until the hurricane passes and repairs are made.

The key consideration in both examples is the "predictability" of the disaster. It is often impossible or unprofitable to provide protection against all possible disasters, therefore, when planning, you must always strive to protect the business against the most likely negative factors.

Which is better: DR or DA?

Disaster Recovery (DR) technologies typically offer a wide variety of deployment options and price ranges and are used by organizations that can tolerate workload disruption or data loss to some extent. However, recovery needs to be checked and practiced periodically to ensure that it works as expected. Regular training minimizes recovery delays caused by human error or inexperience.

Where service downtime for even 1 minute is critical for business, Disaster Avoidance (DA) should be considered, as it is the most proactive form of disaster preparedness. In this case, the joint use of several data centers is required for the distribution of computing resources. Although this increases fault tolerance, the cost of the solution will also rise. Since all the data centers are working non-stop, the IT staff regularly works on all the equipment, and the IT administrators are constantly aware of the parameters of the systems.

Therefore, the ultimate selection of a strategy for disaster management should be based on the business's needs (such as RTOs and RPOs) and compliance requirements, rather than technological availability. Businesses that simply cannot afford to be offline should opt for DA, while less demanding businesses can potentially save money and simplify their infrastructure by implementing a DR strategy.

3.3. Disaster Avoidance (DA)

To maintain the continuous operation of the customer's Virtual Data Center in the event of a failure in one of Orange's Data Centers, the Customer has the option to order a disaster-proof cloud. If this option is activated, VMs are distributed between the main and backup sites either randomly or according to customized rules. When there is an incident in one of Orange's DCs, the VMs running on it automatically start in the second DC. In both DCs, there are identical sets of internal and external networks, which eliminates the need for changes in VM network parameters in the event of a disaster.

To minimize service downtime, if the application supports clustering, it is recommended to place the members of the application cluster in different DCs by using rules - VM Placement Policy(client self-defined).

3.4. Disaster Recovery (DR)

The customer can use Orange cloud infrastructure as a DR platform. From a technical point of view, there are many options for implementing such a scenario, and the choice of a particular option depends on the existing infrastructure and the customer's needs. The customer can independently deploy such a solution (if integration at the level of the cloud infrastructure management system is not required), or Orange employees can deploy a DRaaS class solution for the customer (for example - Veeam Cloud Connect, Hystax Acura, VMware Cloud Director Availability).

3.5. Storage Subsystem

3.5.1. Available storage levels (storage policies) of VM disks

It is possible to use different types of disk capacity and storage levels for the same Virtual Data Center (vDC) and for the same VM.

Storage tier options and their performance differences:

- Silver tier, available up to 150 IOPS per 1Tb of capacity, 500 IOPS/disk maximum*
- Gold tier, available up to 500 IOPS per 1Tb capacity, 1500 IOPS/disk maximum*
- Platinum level, available up to 1500 IOPS per 1Tb capacity, 5000 IOPS/disk maximum*
- Platinum-Plus level, available up to 7500 IOPS per 1Tb capacity, 25000 IOPS/disk maximum*

* The IOPS values mentioned are achievable with an OLTP 70/30 load profile with an average block up to 16kb.

Disaster Avoidance (DA) option is available for Silver/Gold/Platinum tiers, see below.

3.5.2.General recommendations for VM disk placement

Disk capacity of different storage tiers has different achievable IOPS and latency. Actual application performance depends on the parameters of the data load they generate: Read/Write profile, block size, and IOPS.

- Do not use the #SYSTEM default policy, which is designed to allocate hypervisor configuration files and system swap files (this is not to be confused with dedicated swap partitions within the VM).
- For optimal performance, place VM boot and system disks at Gold or Platinum levels.
- Cold data/backup/file server disks - Silver or Gold level
- DBMS disks - Platinum level
- Highly loaded DBMS disks – Platinum-Plus level

3.5.3.Level #SYSTEM

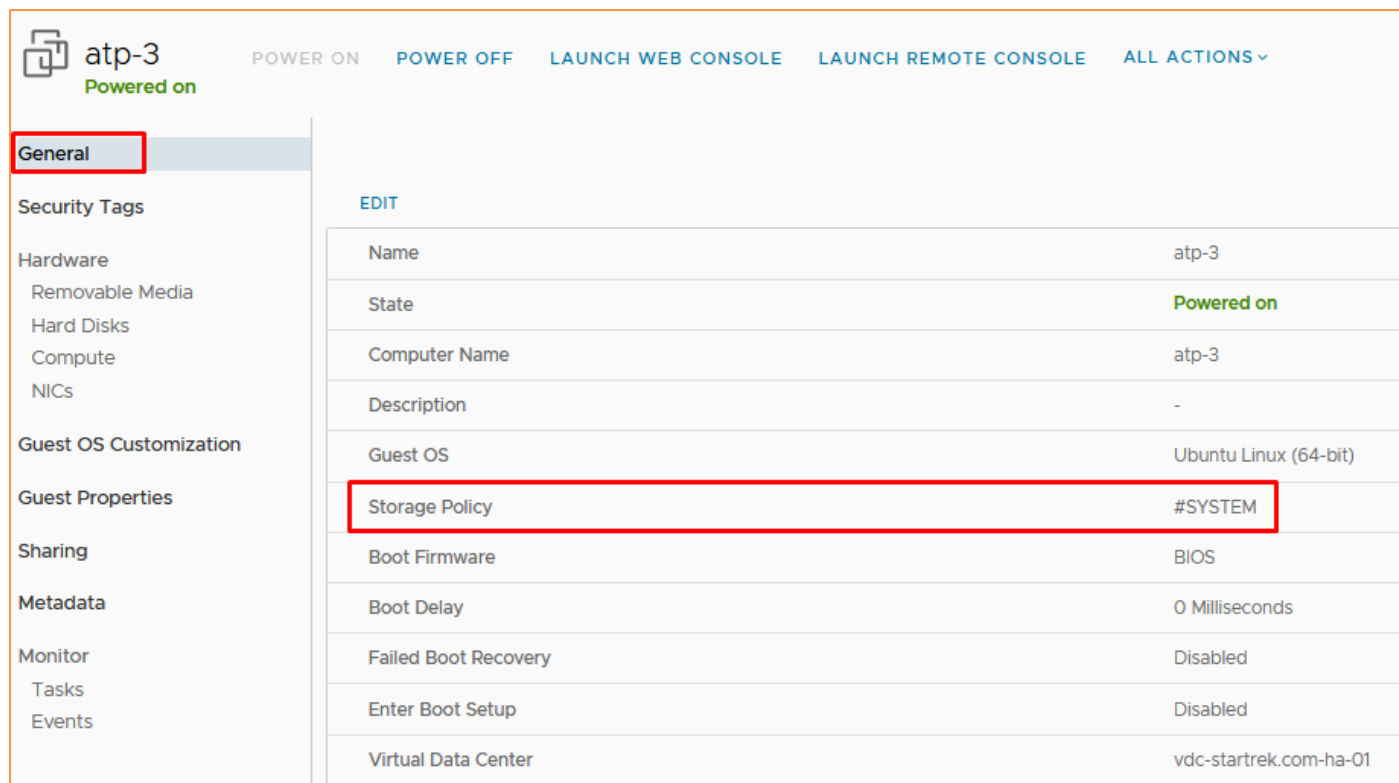
To host service metadata and system swap files, each vDC has a default and non-tariffed #SYSTEM level (including #SYSTEM-site1 and #SYSTEM-site2 variants), which is the default level for VMs.

Placing any user data on these levels is not allowed.

#SYSTEM-site1 and #SYSTEM-site2 are for scenarios with a fixed VM location in one of the DCs.

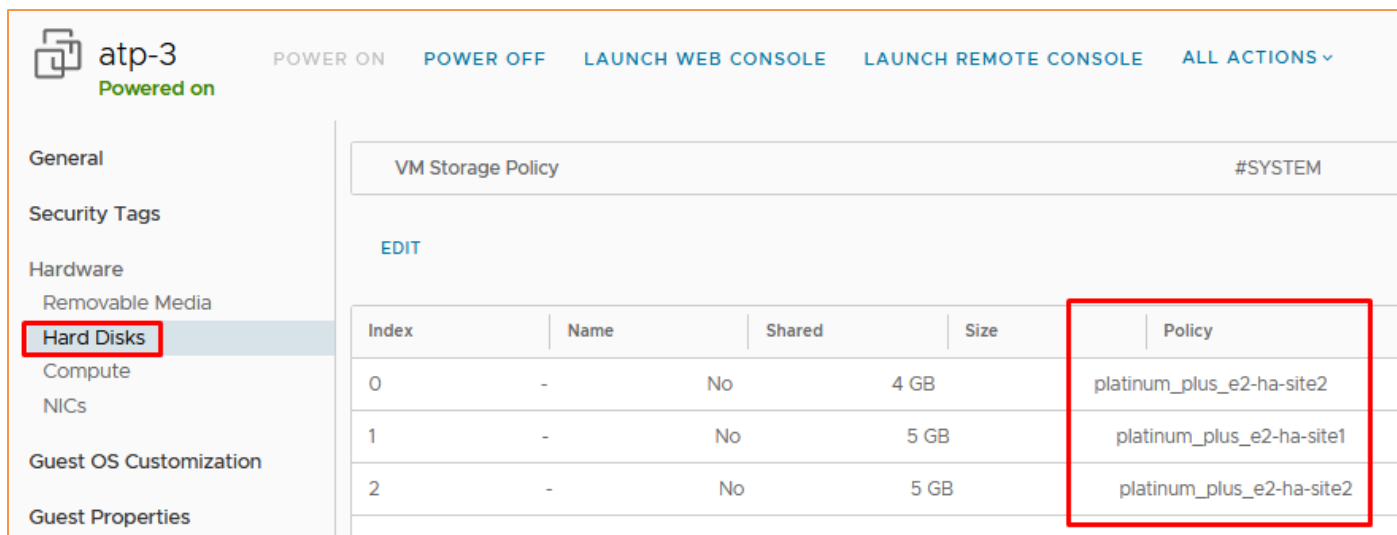
When creating new VM disks (VM deployment), you should manually select the required VM level (instead of the default #SYSTEM) from the list of available for current vDC.

At the same time, do not change the default IOPS values set for the storage level: setting a lower value will result in an artificial limitation, and the system will not allow setting a higher value.



The screenshot shows the configuration page for a VM named 'atp-3'. The 'General' tab is active. The configuration table lists various settings, with 'Storage Policy' highlighted and set to '#SYSTEM'.

EDIT	
Name	atp-3
State	Powered on
Computer Name	atp-3
Description	-
Guest OS	Ubuntu Linux (64-bit)
Storage Policy	#SYSTEM
Boot Firmware	BIOS
Boot Delay	0 Milliseconds
Failed Boot Recovery	Disabled
Enter Boot Setup	Disabled
Virtual Data Center	vdc-startrek.com-ha-01



atp-3
Powered on

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

General

Security Tags

Hardware

Removable Media

Hard Disks

Compute

NICs

Guest OS Customization

Guest Properties

VM Storage Policy #SYSTEM

EDIT

Index	Name	Shared	Size	Policy
0	-	No	4 GB	platinum_plus_e2-ha-site2
1	-	No	5 GB	platinum_plus_e2-ha-site1
2	-	No	5 GB	platinum_plus_e2-ha-site2

3.5.4.Storage Levels Disaster Avoidance (DA)

The solutions allow in the event of a DC level (or storage in the DC) failure to sustain RPO=0 and reduce RTO to within ten seconds - to restart affected VMs and applications on the second site.

In case of ordering the DA option, virtual machines are hosted on the distributed between the two DCs storage system (Synchronized replication is used to protect the data)

Due to additional delay for replication between DCs (about 1ms), Platinum-Plus level is not available in case of ordering DA option.

3.5.5.Disk consumption in Cloud Director

Cloud Director counts disk space consumption according to the following formula (for each type separately):

Total disk space consumed = Hard disk space allocated to the Client's VM (sum of VM disk volumes) + Templates and ISO images + Snapshots.

In case the main policy other than #SYSTEM is selected for a VM, the following is added to this formula: Memory (RAM) allocated for all VMs + VM service files (metadata).

Using hard disk space in addition to what is specified in the order form may cause incorrect operation of the client vDC with subsequent disruption of all applications.

3.5.6.VM disk testing methodology

The purpose of this section is to reduce the number of calls to technical support in case of questions and doubts about the performance of the VM disk subsystem.

- Restrictions on performing stress testing

Long (days, weeks) load synthetic tests, especially multi-threaded (from several disks / VMs), may lead to disruption of the platform hardware and / or software, as well as create difficulties for other users of the platform to receive services, which is unacceptable and is a violation of the related paragraphs of the General Terms of Service.

- Testing tools

For testing it is recommended to use the fio package available for all popular operating systems. Ready builds can be downloaded from the link: https://fio.readthedocs.io/en/latest/fio_doc.html#binary-packages.

At the time of this section writing, version 3.36 under Windows was used.

Installation on Linux - systems with the apt package manager:

```
sudo apt update
sudo apt install fio
```

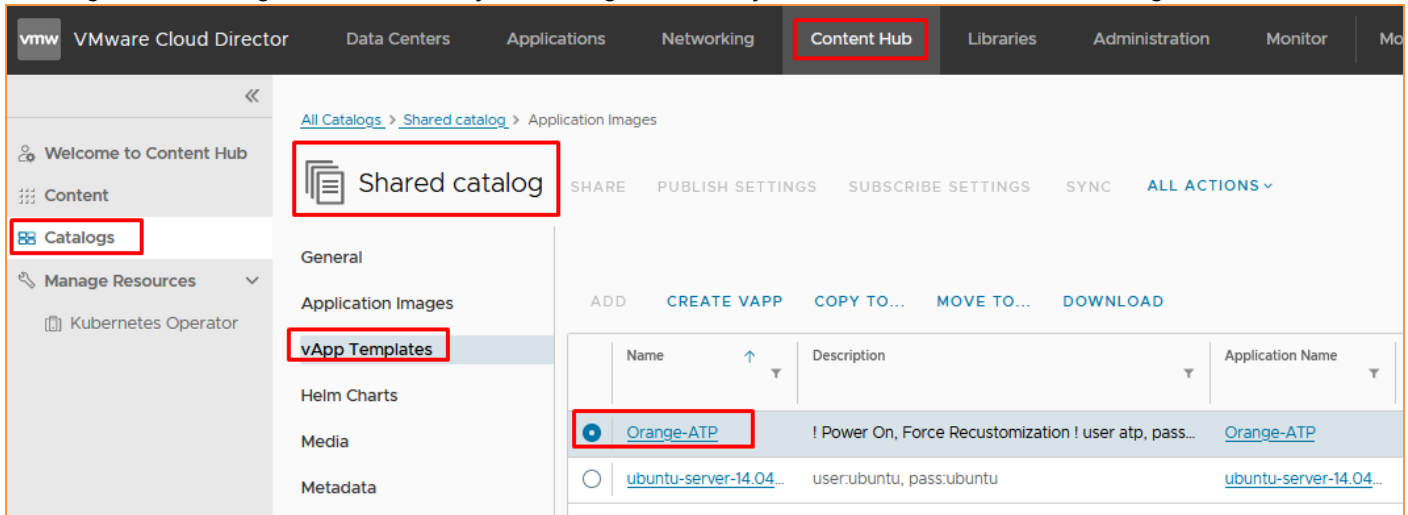
In systems with a batch manager yum/dnf:

```
sudo yum makecache --refresh
sudo yum -y install fio
or
sudo dnf makecache --refresh
sudo dnf -y install fio
```

documentation: https://fio.readthedocs.io/en/latest/fio_doc.html

The VM on which the tests will be performed must be using a “LSI Logic SAS” or “VMware Paravirtual” disk controller, otherwise the results may be incorrect (performance will be limited by the outdated controller type).

An image of the Orange-ATP VM already containing the fio utility is available in the Shared catalog:



• Test Prep

For testing, it is easy to use the template below, which describes several typical disk load profiles.

Edit the template to fit your environment (global section), save it in the folder testing folder as tests.fio:

```
# -----tests.fio start-----
[global]
# test area, cannot be larger than the file system or disk size
size=10G

# test file or device name, e.g. /dev/sdb
# attention, the data will be overwritten!
filename=testfio.tst

# do not use buffering
direct=1
buffered=0

# for Linux ioengine=libaio
# for Windows:
#         ioengine=windowsaio
#         thread=1
ioengine=windowsaio
thread=1

# test time limitation
time_based=1

# test time in seconds (it is not recommended to run the test longer than 10 minutes)
# if it is necessary to run for a longer period of time, please contact Tech team
```

```

runtime=300

# Sequential read, 100%, 250kb block. Assumed storage level is Silver
[seqread-silver]
bs=250k
rw=read
# requested load
rate_IOPS=500

# Sequential write, 100%, 250kb block. Assumed storage level is Silver
[seqwrite-silver]
bs=250k
rw=write
# requested load
rate_IOPS=500

Mixed sequential read 50% read, write 50%, 64kb block. Assumed storage level is Gold
[mixed-gold]
bs=64k
rw=readwrite
iodepth=4
# requested load for write/read
rate_IOPS=750,750

# DBMS - 70% read, random access, 8kb block. Assumed storage level - Platinum
[oltp-platinum]
bs=8K
rw=randrw
iodepth=8
# requested load for write/read
rate_IOPS=3500,1500

# loaded DBMS - 70% read, random access, 8kb block. Assumed storage level - Platinum
Plus [oltp-platinum+]
bs=8K
rw=randrw
iodepth=32
# requested load for write/read
rate_IOPS=17500,7500
# -----tests.fio end-----

```

Mount the required file systems on the VM or define disks for testing.

Before testing, make sure that the disk is not bootable and there is no load on the disk from the operating system. Select a folder for testing.

In the examples below, a separate E disk was allocated, formatted in NTFS and the **fio** folder was created on it.

- Testing

Execute the test by running at the command line in the test folder::

```

# fio -section <test name> tests.fio
where <test name> - one of the values:
seqread-silver
seqwrite-silver
mixed-gold
oltp-platinum
oltp-platinum+

```

(the test can be interrupted at any time by Ctrl-C)

Each section has a parameter that specifies the load in IOPS - “rate_IOPS”, which corresponds to the maximum capabilities of the recommended storage levels.

If this parameter is not used, the test results will probably have atypical values for latency, as the hypervisor will

partially slow down some i/o's to comply with policies. (last example).

- Results Analysis.

Depending on the application, different metrics may be important for performance: bandwidth/IOPS/latency or all together.

The response time (latency) depends on the storage level, block size and load type..

- Typical values for different levels:
- Silver 5-20ms
- Gold 3-10ms
- Platinum 1-5ms
- Platinum-Plus 1-2ms.

The DA option adds about 1.5ms more for all levels

In fio utility tests, you should look at the “avg” result by the “lat” metric (usec - μ s - microseconds, msec - ms - milliseconds, 1000usec=1msec).

- Examples:

- In case of streaming workloads (application-level backups, log collection, etc.), BW is relevant, showing the available disk bandwidth under a given load.

Example fio operation -section seqwrite-silver tests.fio:

```

C:\> Select Command Prompt
E:\fio> fio -section=seq-write tests.fio
seq-write: (g=0): rw=write, bs=(R) 250KiB-250KiB, (W) 250KiB-250KiB, (T) 250KiB-250KiB, ioengine=windowsaio, iodepth=1
fio-3.36
Starting 1 thread
Jobs: 1 (f=1), 0-500 IOPS: [W(1)][100.0%][W=122MiB/s][W=500 IOPS][eta 00m:00s]
seq-write: (groupid=0, jobs=1): err= 0: pid=3748: Thu Dec 14 14:32:41 2023
write: IOPS=500 BW=122MiB/s (128MB/s)(35.8GiB/300001msec); 0 zone resets
slat (usec): min=20, max=21275, avg=49.90, stdev=171.03
clat (nsec): min=11, max=22463k, avg=946468.51, stdev=310198.09
lat (usec): min=52, max=22534, avg=996.37, stdev=354.66
clat percentiles (usec):
| 1.00th=[ 734], 5.00th=[ 766], 10.00th=[ 791], 20.00th=[ 816],
| 30.00th=[ 840], 40.00th=[ 865], 50.00th=[ 889], 60.00th=[ 922],
| 70.00th=[ 955], 80.00th=[ 1004], 90.00th=[ 1106], 95.00th=[ 1254],
| 99.00th=[ 2008], 99.50th=[ 2507], 99.90th=[ 3785], 99.95th=[ 4752],
| 99.99th=[10159]
bw ( KiB/s): min=120741, max=129702, per=100.00%, avg=125123.45, stdev=388.56, samples=596
iops : min= 482, max= 518, avg=500.13, stdev= 1.60, samples=596
lat (nsec) : 20=0.01%
lat (usec) : 4=0.01%, 20=0.01%, 250=0.01%, 500=0.01%, 750=2.16%
lat (msec) : 1000=77.22%
lat (msec) : 2=19.59%, 4=0.93%, 10=0.07%, 20=0.01%, 50=0.01%
cpu : usr=44.67%, sys=2.00%, ctx=0, majf=0, minf=0
IO depths : 1=100.0%, 2=0.0%, 4=0.0%, 8=0.0%, 16=0.0%, 32=0.0%, >=64=0.0%
submit : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
complete : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
issued rwts: total=0,150001,0,0 short=0,0,0,0 dropped=0,0,0,0
latency : target=0, window=0, percentile=100.00%, depth=1

Run status group 0 (all jobs):
WRITE: bw=122MiB/s (128MB/s), 122MiB/s-122MiB/s (128MB/s-128MB/s), io=35.8GiB (38.4GB), run=300001-300001msec
E:\fio>
  
```

Multiplying the average block size of 250Kb by 500 IOPS gives 128MB/s

2. IOPS/latency is interesting for mixed and random loads:
Example fio -section mixed-gold tests.fio:

```

Select Command Prompt
E:\fio>fio -section=mixed-gold tests.fio
mixed-gold: (g=0): rw=rw, bs=(R) 64.0KiB-64.0KiB, (W) 64.0KiB-64.0KiB, (T) 64.0KiB-64.0KiB, ioengine=windowsaio, iodepth=4
fio-3.36
Starting 1 thread
Jobs: 1 (f=0), 0-1500 IOPS: [f(1)][100.0%][r=56.4MiB/s,w=57.5MiB/s][r=902,w=919 IOPS][eta 00m:00s]
mixed-gold: (groupid=0, jobs=1): err= 0: pid=7888: Thu Dec 14 14:52:32 2023
read: IOPS=731, BW=45.7MiB/s (47.9MB/s)(13.4GiB/300035msec)
  slat (usec): min=6, max=976, avg=16.15, stdev= 8.68
  clat (usec): min=184, max=639168, avg=2451.59, stdev=18263.12
  lat (usec): min=254, max=639184, avg=2467.74, stdev=18263.13
  clat percentiles (usec):
    | 1.00th=[ 297], 5.00th=[ 343], 10.00th=[ 367], 20.00th=[ 408],
    | 30.00th=[ 486], 40.00th=[ 758], 50.00th=[ 832], 60.00th=[ 898],
    | 70.00th=[ 988], 80.00th=[ 1139], 90.00th=[ 1483], 95.00th=[ 1942],
    | 99.00th=[ 9372], 99.50th=[173016], 99.90th=[235930], 99.95th=[252707],
    | 99.99th=[450888]
  bw ( KiB/s): min= 126, max=113007, per=100.00%, avg=46867.00, stdev=16726.37, samples=595
  iops: min= 1, max= 1765, avg=731.86, stdev=261.35, samples=595
write: IOPS=731, BW=45.7MiB/s (48.0MB/s)(13.4GiB/300035msec); 0 zone resets
  slat (usec): min=7, max=18865, avg=20.37, stdev=41.37
  clat (usec): min=521, max=440809, avg=2207.28, stdev=16271.26
  lat (usec): min=539, max=440827, avg=2317.65, stdev=16271.33
  clat percentiles (usec):
    | 1.00th=[ 619], 5.00th=[ 652], 10.00th=[ 676], 20.00th=[ 701],
    | 30.00th=[ 725], 40.00th=[ 750], 50.00th=[ 775], 60.00th=[ 807],
    | 70.00th=[ 840], 80.00th=[ 906], 90.00th=[ 1057], 95.00th=[ 1303],
    | 99.00th=[ 6980], 99.50th=[164627], 99.90th=[221250], 99.95th=[240124],
    | 99.99th=[250610]
  bw ( KiB/s): min= 126, max=115401, per=100.00%, avg=46891.95, stdev=16697.00, samples=595
  iops: min= 1, max= 1803, avg=732.26, stdev=260.89, samples=595
  lat (usec) : 250=0.01%, 500=15.45%, 750=24.29%, 1000=39.52%
  lat (msec) : 2=17.23%, 4=2.01%, 10=0.53%, 20=0.08%, 50=0.08%
  lat (msec) : 100=0.08%, 250=0.69%, 500=0.03%, 750=0.01%
  cpu        : usr=1.67%, sys=0.67%, ctx=0, majf=0, minf=0
  IO depths  : 1=6.9%, 2=16.2%, 4=76.9%, 8=0.0%, 16=0.0%, 32=0.0%, >=64=0.0%
  submit     : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
  complete   : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
  issued rwts: total=219511,219612,0,0 short=0,0,0,0 dropped=0,0,0,0
  latency    : target=0, window=0, percentile=100.00%, depth=4

Run status group 0 (all jobs):
  READ: bw=45.7MiB/s (47.9MB/s), 45.7MiB/s-45.7MiB/s (47.9MB/s-47.9MB/s), io=13.4GiB (14.4GB), run=300035-300035msec
  WRITE: bw=45.7MiB/s (48.0MB/s), 45.7MiB/s-45.7MiB/s (48.0MB/s-48.0MB/s), io=13.4GiB (14.4GB), run=300035-300035msec
E:\fio>

```

3. Example for DBMS

fio -section oltp-platinum tests.fio:

```

Command Prompt
E:\fio>fio -section=oltp-platinum tests.fio
oltp-platinum: (g=0): rw=randrw, bs=(R) 8192B-8192B, (W) 8192B-8192B, (T) 8192B-8192B, ioengine=windowsaio, iodepth=8
fio-3.36
Starting 1 thread
Jobs: 1 (f=1), 0-5000 IOPS: [m(1)][100.0%][r=21.7MiB/s,w=9531KiB/s][r=2779,w=1191 IOPS][eta 00m:00s]
oltp-platinum: (groupid=0, jobs=1): err= 0: pid=8224: Thu Dec 14 15:02:36 2023
read: IOPS=3497, BW=27.3MiB/s (28.7MB/s)(8200MiB/300098msec)
  slat (usec): min=5, max=220, avg=11.50, stdev= 7.23
  clat (usec): min=163, max=218866, avg=606.02, stdev=3358.94
  lat (usec): min=185, max=218873, avg=617.52, stdev=3358.95
  clat percentiles (usec):
    | 1.00th=[ 235], 5.00th=[ 265], 10.00th=[ 281], 20.00th=[ 326],
    | 30.00th=[ 453], 40.00th=[ 486], 50.00th=[ 515], 60.00th=[ 553],
    | 70.00th=[ 594], 80.00th=[ 635], 90.00th=[ 701], 95.00th=[ 848],
    | 99.00th=[ 2212], 99.50th=[ 3163], 99.90th=[ 6128], 99.95th=[ 10159],
    | 99.99th=[208667]
  bw ( KiB/s): min=15857, max=40593, per=100.00%, avg=28026.15, stdev=4286.14, samples=595
  iops: min= 1982, max= 5074, avg=3502.88, stdev=535.77, samples=595
write: IOPS=1498, BW=11.7MiB/s (12.3MB/s)(3514MiB/300098msec); 0 zone resets
  slat (usec): min=6, max=278, avg=13.46, stdev= 8.05
  clat (usec): min=198, max=220514, avg=394.84, stdev=962.88
  lat (usec): min=231, max=220524, avg=394.84, stdev=962.90
  clat percentiles (usec):
    | 1.00th=[ 269], 5.00th=[ 289], 10.00th=[ 302], 20.00th=[ 318],
    | 30.00th=[ 330], 40.00th=[ 343], 50.00th=[ 355], 60.00th=[ 367],
    | 70.00th=[ 383], 80.00th=[ 408], 90.00th=[ 445], 95.00th=[ 494],
    | 99.00th=[ 709], 99.50th=[ 955], 99.90th=[ 2704], 99.95th=[ 4359],
    | 99.99th=[10159]
  bw ( KiB/s): min= 7135, max=16993, per=100.00%, avg=12011.18, stdev=1565.68, samples=595
  iops: min= 891, max= 2124, avg=1501.01, stdev=195.71, samples=595
  lat (usec) : 250=1.91%, 500=58.44%, 750=34.16%, 1000=3.05%
  lat (msec) : 2=1.61%, 4=0.62%, 10=0.17%, 20=0.02%, 50=0.01%
  lat (msec) : 100=0.01%, 250=0.02%
  cpu : usr=1.00%, sys=0.67%, ctx=0, majf=0, minf=0
  IO depths : 1=16.6%, 2=32.5%, 4=29.4%, 8=21.5%, 16=0.0%, 32=0.0%, >=64=0.0%
  submit : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
  complete : 0=0.0%, 4=99.8%, 8=0.2%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
  issued rwts: total=1049573,449817,0,0 short=0,0,0,0 dropped=0,0,0,0
  latency : target=0, window=0, percentile=100.00%, depth=8

Run status group 0 (all jobs):
  READ: bw=27.3MiB/s (28.7MB/s), 27.3MiB/s-27.3MiB/s (28.7MB/s-28.7MB/s), io=8200MiB (8598MB), run=300098-300098msec
  WRITE: bw=11.7MiB/s (12.3MB/s), 11.7MiB/s-11.7MiB/s (12.3MB/s-12.3MB/s), io=3514MiB (3685MB), run=300098-300098msec
E:\fio>

```

(Latency values are given in microseconds).

4. Similar to tip 3, but requested 25000 IOPS when the disk is placed at Platinum level (not Platinum-Plus):

fio -section oltp-platinum+ tests.fio:

```

E:\fio>fio -section=oltp-platinum+ tests.fio
oltp-platinum+: (g=0): rw=randrw, bs=(R) 8192B-8192B, (W) 8192B-8192B, (T) 8192B-8192B, ioengine=windowsaio, iodepth=32
fio-3.36
Starting 1 thread
Jobs: 1 (f=1), 0-25000 IOPS: [m(1)][100.0%][r=18.9MiB/s,w=18.3MiB/s][r=2414,w=2345 IOPS][eta 00m:00s]
oltp-platinum+ test group 0, jobs=1): err= 0: pid=4696: Thu Dec 14 15:16:01 2023
read: IOPS=2513, BW=19.6MiB/s (20.6MB/s)(5891MiB/300036msec)
  slat (usec): min=5, max=2174, avg=12.65, stdev=11.24
  clat (usec): min=66, max=400754, avg=6444.36, stdev=18850.80
  lat (usec): min=198, max=400764, avg=6454.00, stdev=18850.39
  clat percentiles (usec):
    | 1.00th=[ 293], 5.00th=[ 367], 10.00th=[ 465], 20.00th=[ 603],
    | 30.00th=[ 766], 40.00th=[ 5800], 50.00th=[ 6063], 60.00th=[ 6325],
    | 70.00th=[ 6456], 80.00th=[ 6587], 90.00th=[ 6783], 95.00th=[ 7111],
    | 99.00th=[109577], 99.50th=[183501], 99.90th=[229639], 99.95th=[235930],
    | 99.99th=[248513]
  bw ( KiB/s): min=12840, max=73980, per=100.00%, avg=20344.42, stdev=4457.87, samples=177
  iops: min= 1605, max= 9247, avg=2542.79, stdev=557.22, samples=177
write: IOPS=2500, BW=19.5MiB/s (20.5MB/s)(5861MiB/300036msec); 0 zone resets
  slat (usec): min=6, max=959, avg=14.19, stdev=11.56
  clat (usec): min=19, max=401496, avg=6215.37, stdev=18293.65
  lat (usec): min=247, max=401529, avg=6229.56, stdev=18293.19
  clat percentiles (usec):
    | 1.00th=[ 318], 5.00th=[ 363], 10.00th=[ 400], 20.00th=[ 469],
    | 30.00th=[ 586], 40.00th=[ 5735], 50.00th=[ 5997], 60.00th=[ 6194],
    | 70.00th=[ 6390], 80.00th=[ 6521], 90.00th=[ 6718], 95.00th=[ 6915],
    | 99.00th=[ 98042], 99.50th=[179307], 99.90th=[229639], 99.95th=[235930],
    | 99.99th=[246416]
  bw ( KiB/s): min=12432, max=38690, per=100.00%, avg=20084.02, stdev=2366.05, samples=177
  iops: min= 1554, max= 4836, avg=2510.24, stdev=295.77, samples=177
lat (usec) : 20=0.01%, 100=0.01%, 250=0.09%, 500=17.70%, 750=13.68%
lat (msec) : 1000=2.40%
lat (msec) : 2=0.77%, 4=1.02%, 10=62.49%, 20=0.36%, 50=0.18%
lat (msec) : 100=0.30%, 250=1.01%, 500=0.01%
cpu        : usr=0.33%, sys=2.00%, ctx=0, majf=0, minf=0
IO depths  : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.8%, 16=68.0%, 32=31.0%, >=64=0.0%
submit     : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
complete  : 0=0.0%, 4=97.6%, 8=1.3%, 16=0.9%, 32=0.2%, 64=0.0%, >=64=0.0%
issued rwts: total=754039,750164,0,0 short=0,0,0,0 dropped=0,0,0,0
latency    : target=0, window=0, percentile=100.00%, depth=32

Run status group 0 (all jobs):
  READ: bw=19.6MiB/s (20.6MB/s), 19.6MiB/s-19.6MiB/s (20.6MB/s-20.6MB/s), io=5891MiB (6177MB), run=300036-300036msec
  WRITE: bw=19.5MiB/s (20.5MB/s), 19.5MiB/s-19.5MiB/s (20.5MB/s-20.5MB/s), io=5861MiB (6145MB), run=300036-300036msec
E:\fio>

```

If the requested I/O operations exceed the capacity of the selected storage level, the system will limit performance by increasing the response time.

3.6. Backup to disk

If the Customer's data is lost or damaged the Customer may require the restoration of a virtual machine from the latest backup. To enable this option, you must order it by filling out the appropriate Service Order Form.

The virtual machine shall be restored from the backup "as is". Due to technical limitations, Orange shall not be held liable for the integrity of information systems and business applications.

Orange ensures recovery of virtual machines to the level of the OS within the virtual machine.

This option allows for a full copy of the customer's vDC and several incremental restore points to be stored on the disk. The customer selects one of 3 standard backup-to-disk schemes and the number of recovery points ($T > 3$)

- Daily;
- 3 points per week: Monday, Wednesday, Friday;
- 2 points per week: Tuesday, Thursday.

Depending on the parameters of the vDC ordered

3.7. Backup (archiving) to tape

This method allows backup copies of data to be stored on removable media (tapes), which can be moved to a remote site. To enable this option, you must order it by filling out the appropriate Service Order Form.

Recovering data from a tape requires significantly more time than data recovery from disks. Backup to tape is used when long-term storage of data and the storage of backup copies at a remote site, rather than to the two DCs used to provide the Service, are necessary. The MSL4048 library supports AES 256-bit hardware encryption at the tape library level. The encryption of backups on tape is optional.

The customer selects one of 3 standard backup to tape schemes and the number of recovery points ($T > 3$)

- Daily;
- 3 points per week: Monday, Wednesday, Friday;
- 2 points per week: Tuesday, Thursday.

Every week according to the schedule, a full copy of the customer's vDC is created and recorded on the tape. The tape is exported to a remote site each month, where it is stored in a fire-resistant cabinet.

The customer can choose:

- To store X weekly copies;
- To store Y monthly copies.

3.8. Independent backup management (Self Service Backup)

A self-service backup is available on the Veeam Self-Service Backup Portal for Cloud Director.

This option is not compatible with Orange's tape and disk backups.

When ordering this option, the Client must calculate the required amount of disk space for storing backups based on the amount of VM data and the planned schedule.

When you order this option, you will receive additional login credentials.

3.9. Dedicated GHz and vCPUs

As part of the FCA service, a virtual Data Center is created for the Customer with a set of computing resources as delineated on the signed Service Order Form. If you are allocating processor power, you should pay attention to the difference between the allocated processor power and the number of cores (vCPUs).

For example, let's assume that a vDC has 48GHz of processor power allocated.

When the VM is turned on, 1GHz is allocated for each vCPU (core), i.e. a maximum of 48 vCPUs can be enabled in this scenario (for example: 12 VMs with 4 vCPUs, or 2 VMs with 12 vCPUs and 6 VMs with 4 vCPUs).

The infrastructure has physical processors with a nominal frequency of 2.2/2.5/3.0 GHz. Let's take 2.5GHz to make our further calculations.

If all vCPUs are using full power: $48 * 2.5 = 120\text{GHz}$. Because 120GHz is more than the allocated 48GHz, then the total consumption for the vDC will be limited to 48GHz, that is, all cores will in fact operate at 1GHz. But this situation is extremely rare, since, as a rule, most vCPUs are nearly idle (i.e., vCPUs that are actually working will get more resources — up to the whole physical 2.5), this ensures additional flexibility in configuring and operating VMs.

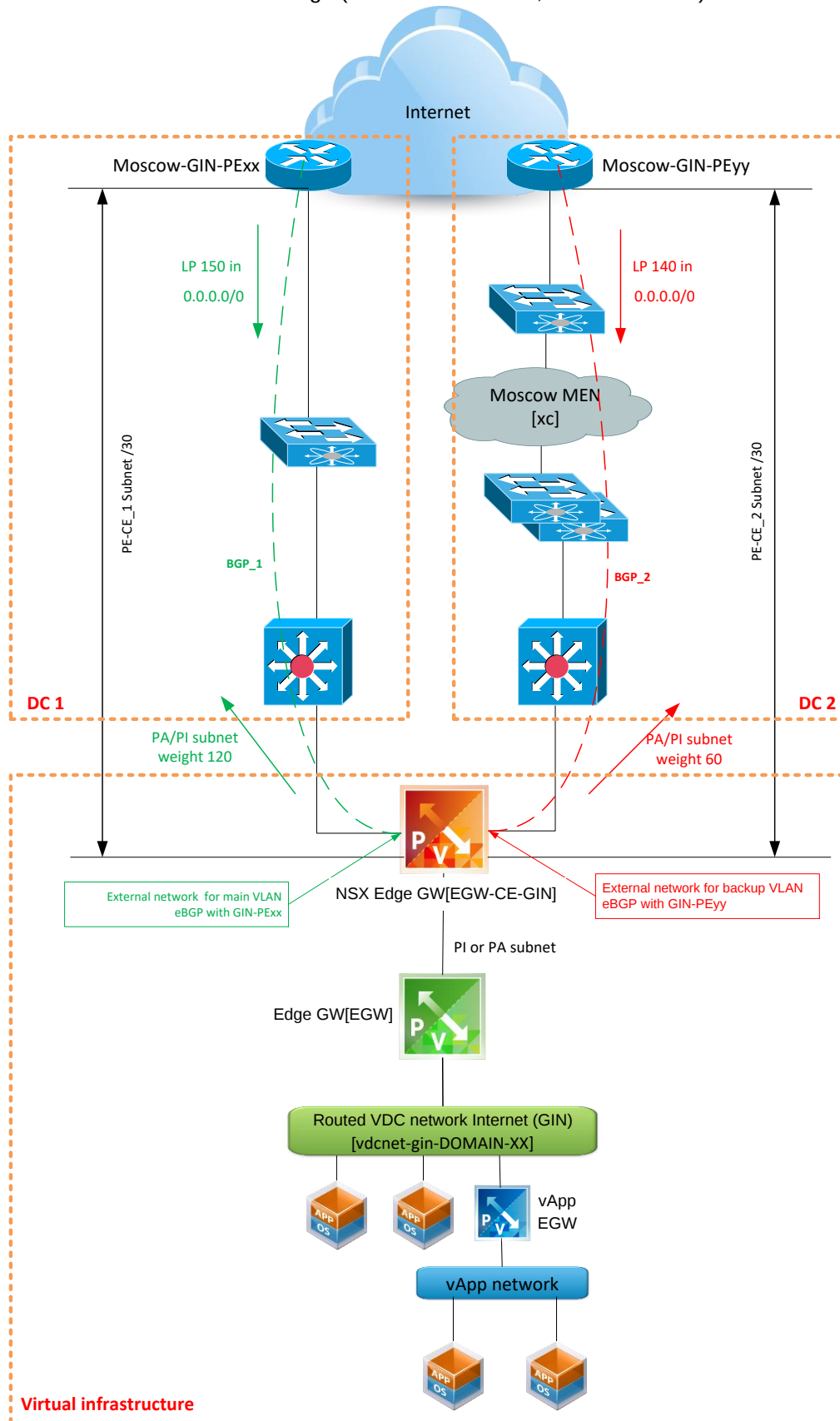
If you need to avoid a potential limitation of the core frequency, you can calculate it like this: $48\text{GHz} / 2.5\text{GHz} = 19.2$ vCPU, i.e. 19 cores can be configured on a VM without getting limited.

3.10. Fault-tolerant access to Internet and BVPN networks

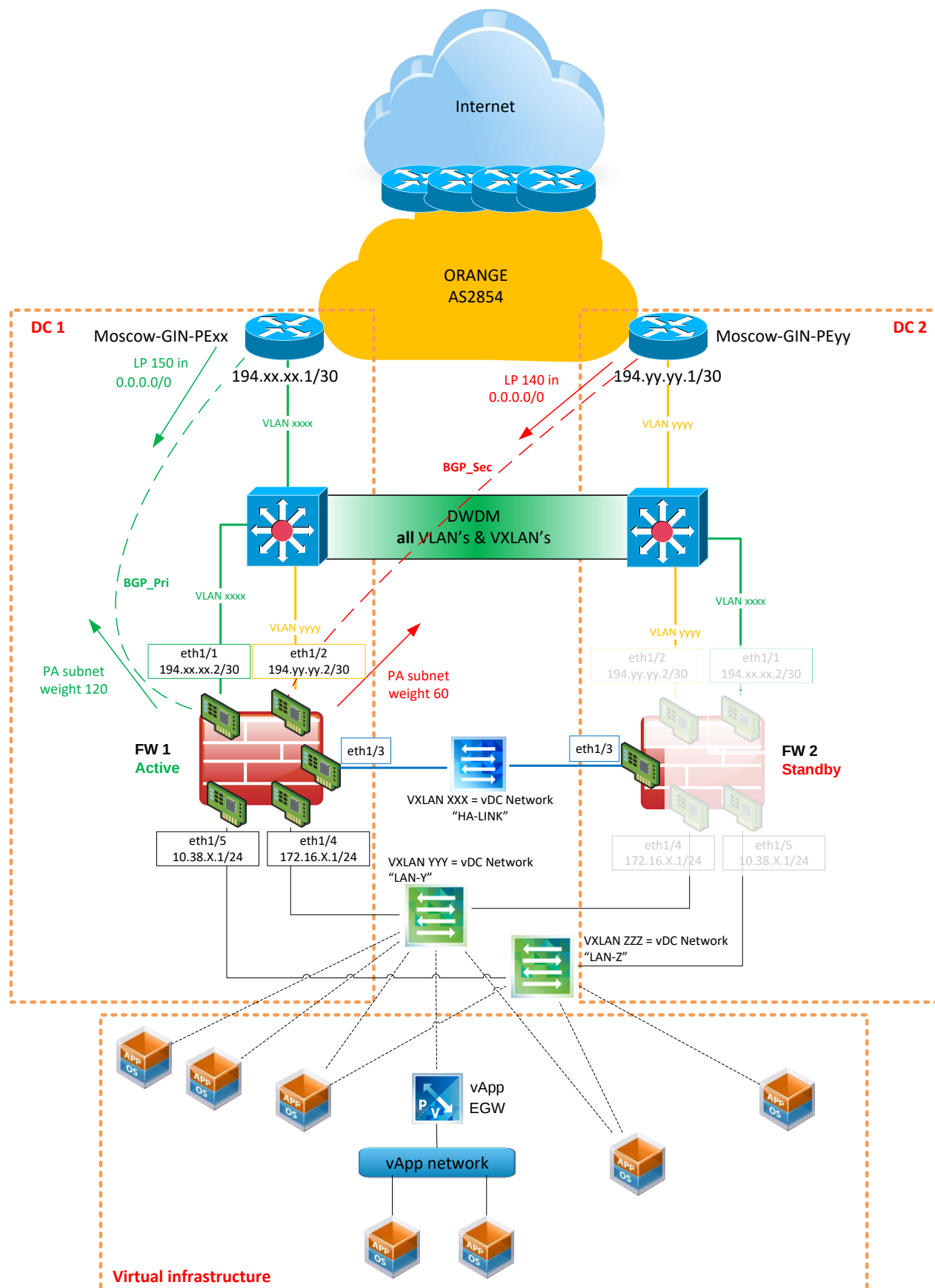
All external network connections are reserved at the levels of physical connections, physical equipment, MEN network, PE-routers and are organized through two data centers. At the same time, it does not matter which route (through which data center) traffic is currently flowing - for virtual machines in vDC this is transparent and does not have significant differences in latencies.

Below are the schemes for organizing access to the Internet, for the BVPN network they are similar:

- Standard scheme with NSX Edge (can be in HA mode, see below 3.12)



- Customer's use of his own virtual router (example of a possible architecture)

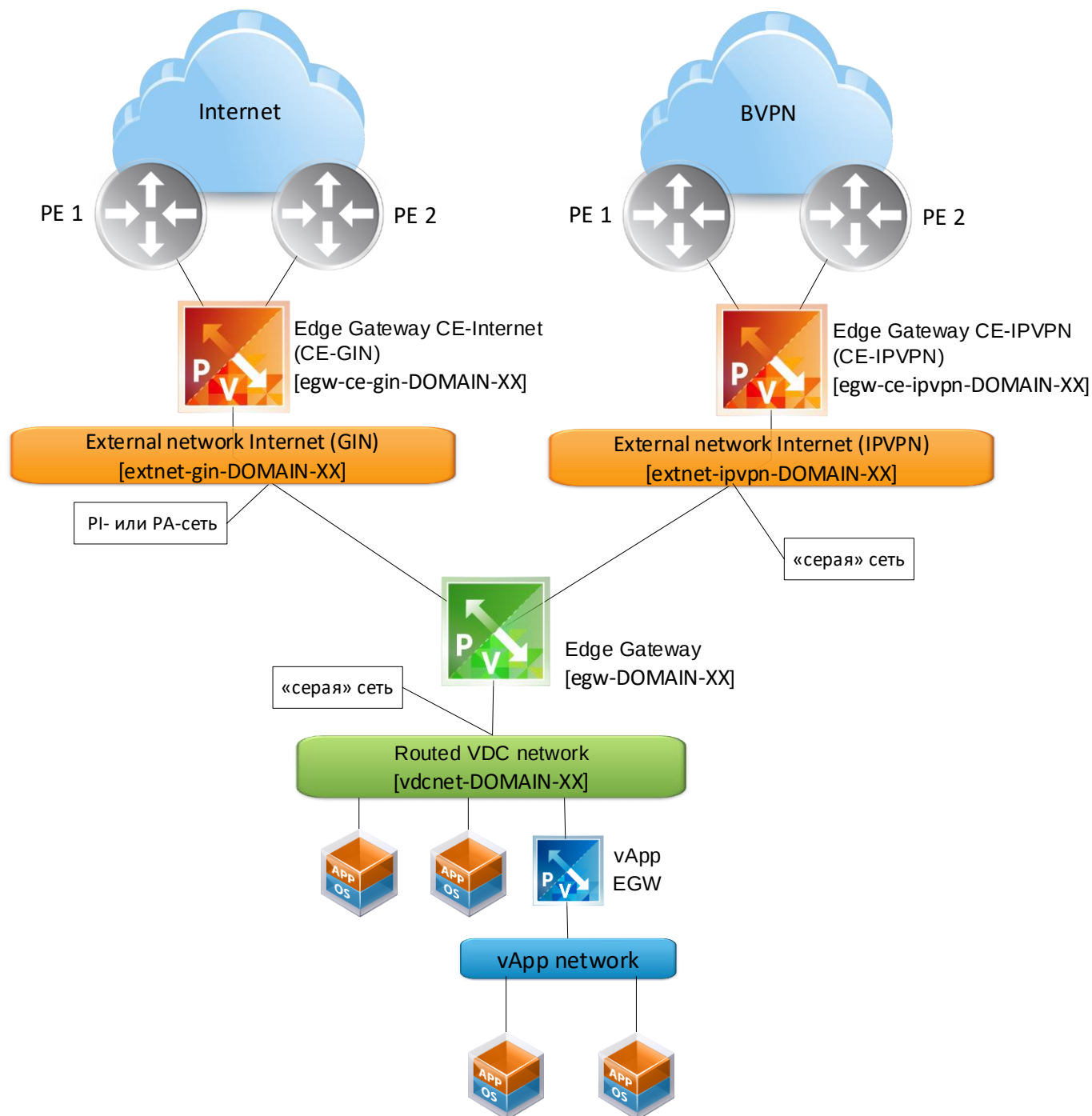


3.11. VMware NSX Edge

VMware NSX Edge is a solution that provides the following functions for the virtual data center: routing, Firewall, NAT, DHCP, Site to Site VPN, SSL VPN-Plus, Load Balancing, High Availability, syslog. There are two classes of VMware Version 4.1.6 © Orange Business Services, 2024

NSX Edge Gateway in the Orange cloud infrastructure:

- An EGW-CE functions as a traditional CE router. All external network connections use two data centers and are reserved at the levels of physical connections, physical equipment, the MEN network, and PE routers. Different EGW-CEs are used for Internet access and BVPN. The configuration of these parameters lies within Orange's area of responsibility.
- EGW is fully available for the customer to manage from the Cloud Director web interface. It provides DHCP, NAT, VPN, routing, filtering, and load balancing for internal vDC networks.



For the Edge Gateway CE-Internet (CE-GIN) [egw-ce-gin-DOMAIN-XX] Internet network, the interface is fully managed by Orange, performs only CE functions and provides a dedicated prefix to the External network Internet (GIN) [extnet-gin-DOMAIN-X].

For the BVPN network Edge Gateway CE-BVPN (CE-IPVPN) [egw-ce-ipvpn-DOMAIN-XX], the interface is fully managed by Orange, performs only CE functions, and provides connectivity to the EGW via OSPF.

Edge Gateway [egw-DOMAIN-XX] is fully available for customer self-service via vCD.

3.12. NSX Edge High Availability

When ordering this option, active-passive clusters of two instances of NSX Edge are created and automatically placed on different hosts. In the case of DA, they are placed in different DCs:

- For the selected customer-managed EGW;
- For the EGW-CE-GIN (if Internet access is available);
- For the EGW-CE-BVPN (if the BVPN network is accessible).

This makes it possible to minimize network access downtime in the event of the failure of the physical host on which NSX Edge runs or in the event of problems with NSX Edge VM.

Estimated time parameters (the data is based on the logic of the technologies, their configuration and Orange tests):

Scenario	Access interruption	Time, seconds
Failover from the main Internet or BVPN channel to the backup one	Yes	15 *
Regular switching (maintenance) from the main Internet or BVPN channel to the backup one	Yes	15 *
Switch back to main Internet or BVPN channel	No	-
Rebooting NSX Edge after a host crash	Yes	45
Switching to a backup instance of NSX Edge with the High Availability option	Yes	15 **

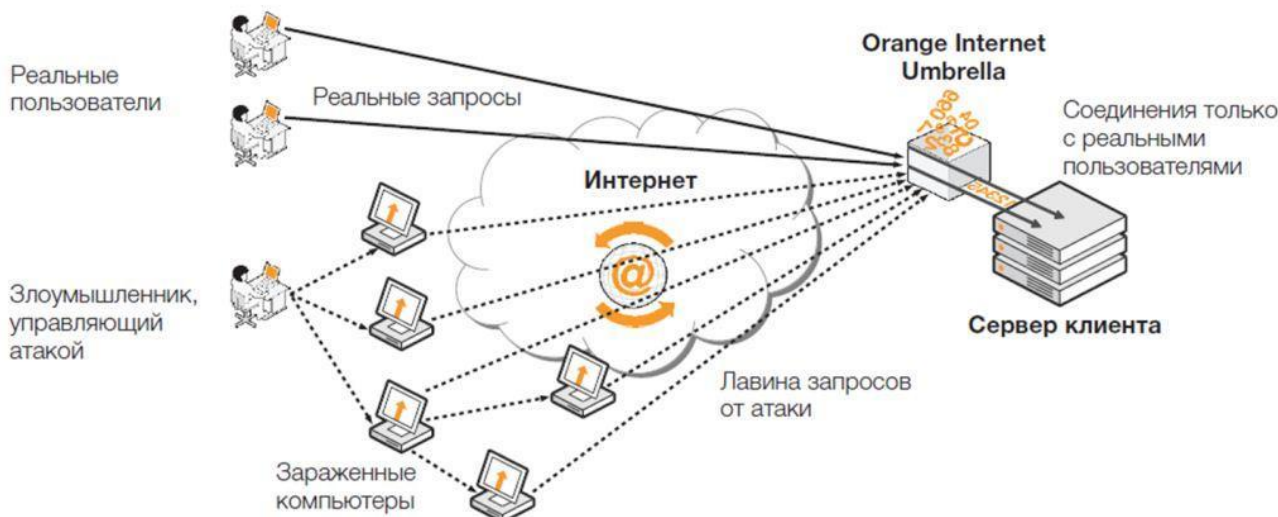
* It can be reduced to 3 seconds upon request.

** It can be reduced to 6 seconds upon request.

3.13. Protection against DDoS attacks

The Internet Umbrella service can be ordered to protect the Internet port connected to vDC against DDoS attacks based on the Mitigator hardware complex and integration with the Orange network.

Internet Umbrella is a set of Orange activities aimed at countering DDoS attacks which are aimed at flooding the Internet access channels provided by Orange.



3.14. Rental of software licenses

As part of the FCA service, Orange can provide licenses to the customer along to the Software as a Service model. The following licenses are rented out by default:

- Microsoft Windows Server sStandard*;
- Microsoft Windows Server Datacenter*;
- Microsoft SQL Server sStandard*;
- Microsoft SQL Server Enterprise*;

* The current versions of the software are available for rent, while, as a rule, allowing the use of older versions.

A wide range of Microsoft software licenses are available upon request.

3.15. *Microsoft software activation via the SPLA program using KMS*

To activate Microsoft software, Orange's KMS server is used, which is accessible via the Internet from the addresses allocated to customers. If the VM does not have access to the Internet, please contact Orange to activate it with a MAC key.

Activation procedure:

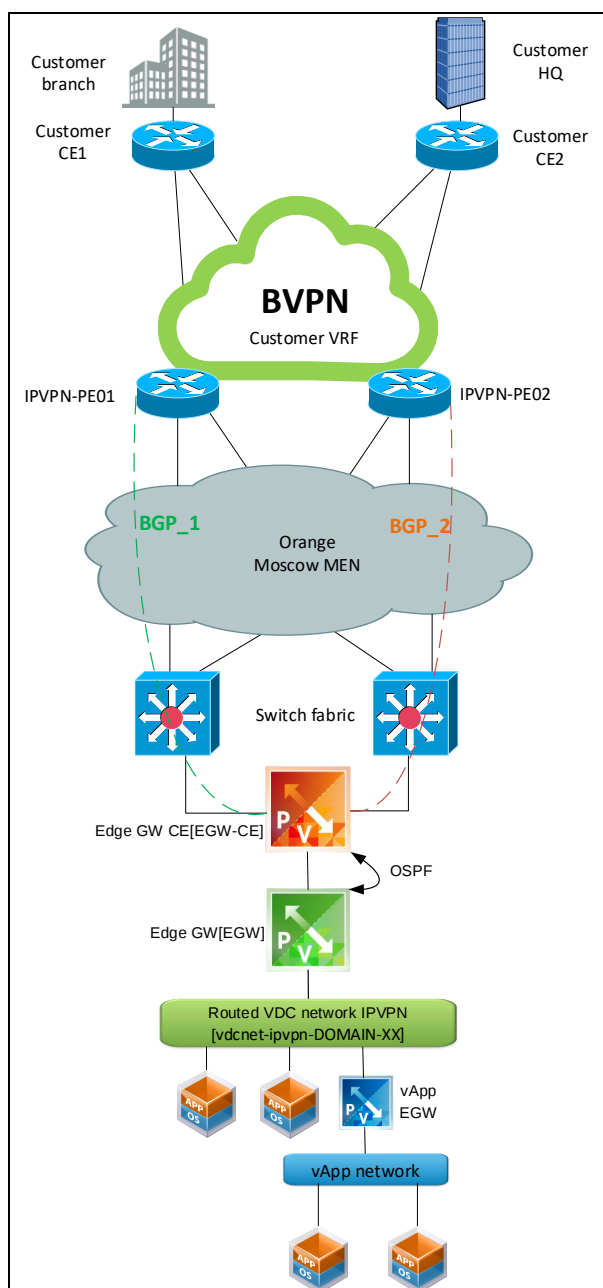
- Check that the TCP1688 port is open on the EGW and accessible from the Internet
- Check that the time in the VM is correct!
- Set IP KMS:
slmgr -skms 194.84.17.201:1688
- Enable online:
slmgr.vbs /ato
- Check activation:
slmgr /dlv

* If the KMS server is not available, please contact Orange.

3.16. *How to connect a local network to the Orange cloud?*

There are two main connection methods:

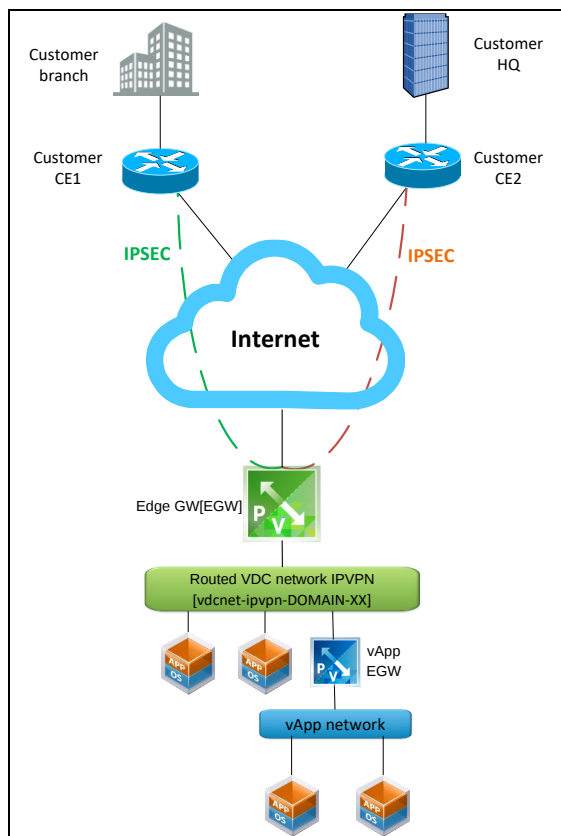
1. Using the BVPN Orange network.



The advantages of this method are:

- The channel parameters (RTD, jitter, PLR) are better than those on the Internet
- A fault-tolerant connection between the cloud and BVPN
- Enabling fault-tolerant connections from the customer's network
- Optional SLA
- Channel performance – Orange
- Optional connection of remote sites to the BVPN network through the Internet VPN service (IPSEC to BVPN nodes over the Internet)

2. Through the IPSEC Tunnel of NSX Edge



Advantages:

- Cost
- Connection speed for new remote sites

* For other connection types through the NSX Edge, see 11.7 «VPN».

3.17. Connecting external USB devices (USB-to-IP)

USB-to-IP devices are used to provide external USB devices (usually hardware USB keys for software protection). The manufacturer and model are specified in the pre-sale stage.

Each USB port is bound to a VM (several ports can be assigned to one VM).

A separate device is installed for each Customer.

It is not recommended to use these devices to connect high-speed USB devices such as external HDDs, flash drives, etc.

3.18. Connecting external network devices / servers located in the Orange DC's

It is possible to combine the physical network and the vDC virtual network at the L2 level. This can be a vDC network in which virtual machines are located, or a separate segment isolated using Edge.

This may be necessary if the customer's equipment is placed in the Orange DC's (the Nethosting service). Also, this option can be used to connect the vDC to a third-party telecom operator directly or through a physical router.

Depending on the required speed, this can be:

- One or two (MC-LAG) 1000BASE-T ports per device and a copper cable to the customer's equipment;
- One or two (MC-LAG) 10GBASE-SR per device and a optical cable to the customer's equipment. *This is not a standard option, additional development is required.*

4. Main elements of VMware Cloud Director

Virtual organization (organization, vOrg) is the top-most element in the hierarchy of Cloud Director abstraction objects. It contains information about your organization's user accounts and general parameters.

Virtual organization (vOrg) is a root logical element that contains all your vDCs, administrator accounts, authentication parameters, notifications, etc.

Virtual Datacenter, vDC is a collection of your cloud resources (virtual processors, memory, disk space, networks, etc.). This is an environment in which virtual machines, vApps, networks, etc. are created. You can increase its size by

purchasing the necessary resources (processors, memory or disks) by signing the corresponding Service Order Form. Your vOrg can have two vDCs if you ordered a regular vDC and the Disaster Avoidance option at the same time.

vApp is a set of virtual machines combined into one group that hosts virtual machines. It can be created empty or with virtual machines already inside. vApps allow for the management of a group of virtual machines as one unit. This is especially useful if you are managing a large virtual infrastructure. Templates can be created using vApp. If you need to periodically create groups of virtual machines of the same type, then a vApp template will save you time. Cloud Director also allows you to create a separate network at the vApp level for additional isolation between two vApps. vApps can be used to group virtual machines that belong to a single business application. Also, vApp allows you to differentiate access between the administrators of your organization.

Virtual machines (VMs) can be created using templates (with an OS) in the directory or from scratch by installing the desired OS from a downloaded template or image.

Catalogs are folders where you can store vApp templates, virtual machines, and media files (ISO images).

Org VDC Network is a network that is available for all vApps by default. An organization-level network can be isolated from external networks (isolated), routed through the Edge Gateway (routed) or directly connected to external networks on the L2 level (direct).

In addition to an organization-level network that is available to all vApps and can be stretched across different vDCs of the same organization, you can create a vApp-level network. This will be a network for interaction between virtual machines of the given vApp only; it will not be available for virtual machines from other vApps. A vApp network can be connected to an organization level network to allow a given vApp to interact with other vApps within the organization or outside it, and there will be a specialized "small" Edge Gateway with limited functionality (FW, NAT and DHCP only) between the vApp network and the vOrg network.

The Orange cloud uses **standard naming conventions for objects**:

Object	Name pattern	Example for 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 (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 BVPN	extnet-ipvpn-DOMAIN-VID	extnet-ipvpn-startrek.com-2924
External network L2VPN	extnet-l2vpn-DOMAIN-VID	extnet-l2vpn-startrek.com-2999
Chief administrator of the organization	adm_DOMAIN	adm_startrek.com

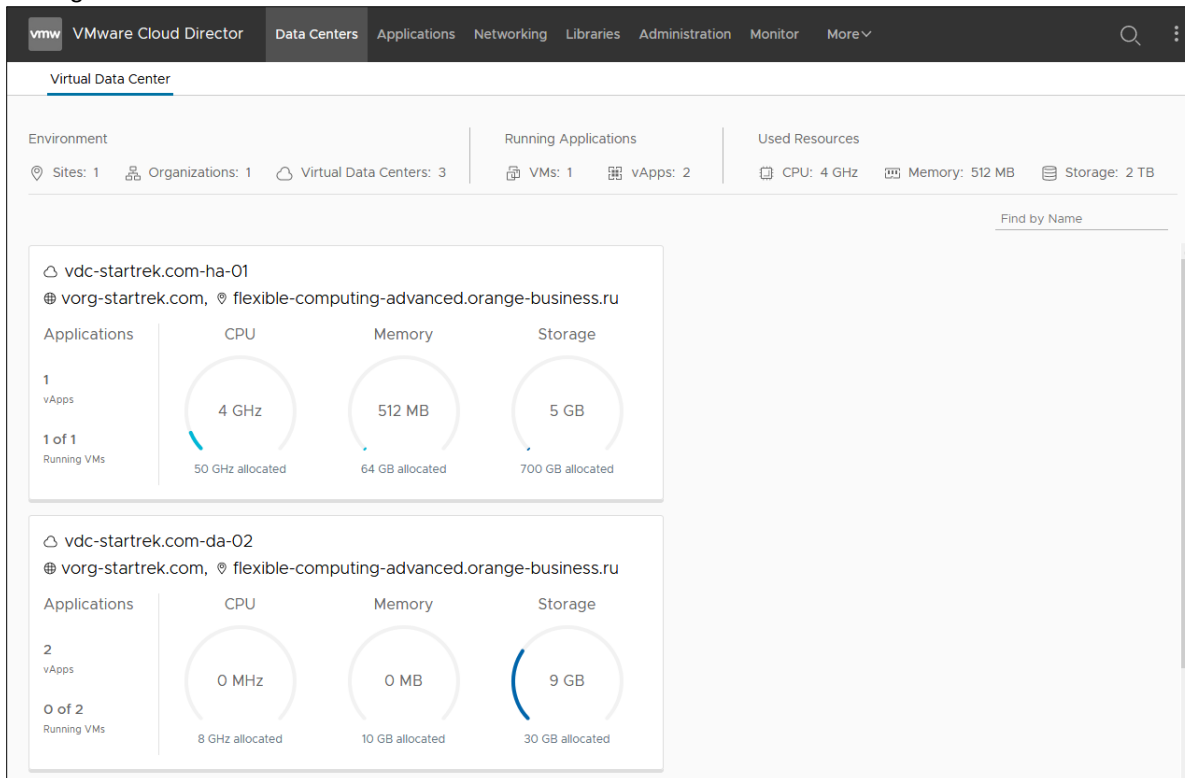
5. Login to the virtual data center

After completing the creation and configuration of your virtual data center (Virtual DataCenter, vDC), you will receive a URL and an administrator account from Orange to access the vDC.

Currently only HTML5 WEB-interface is available:

- Tenant Portal is a fully functional HTML5-based interface.
Available at the following address (you must specify the name of your vorg at the end): <https://flexible-computing-advanced.orange-business.ru/tenant/vorg-startrek.com/>

Open the URL in the browser, enter a username and password in the appropriate fields and enter the main cloud management window:



6. Typical problems when connecting to the web interface and using it

- Access to the management portal is allowed from the IPs specified in the questionnaire or through authorization on the FW. To change the IP or user list, you can use the Change Management procedure (contact Orange Help Desk).

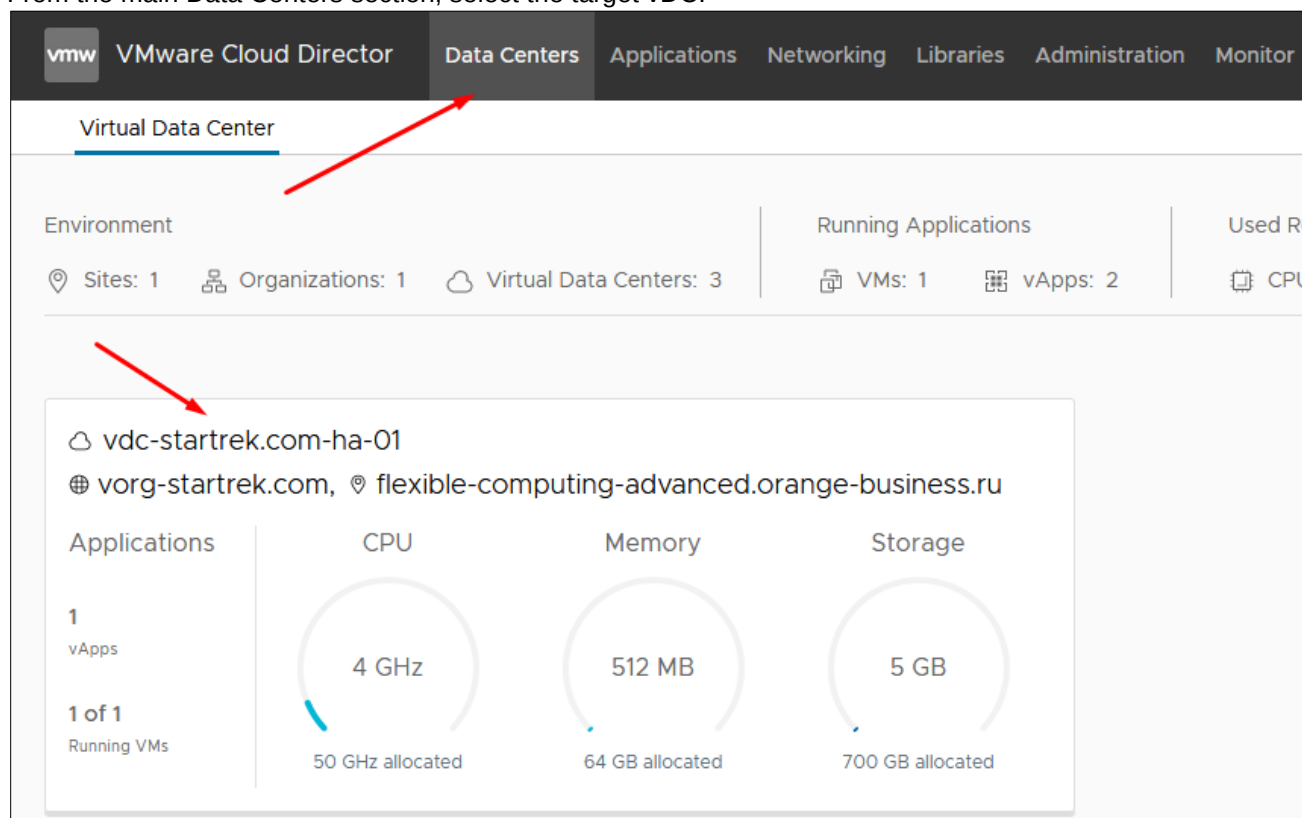
7. Checking vDC resource availability and network connectivity

The final step that Orange has to take in configuring your vDC is checking the resource availability and network connectivity.

For this, the pre-configured Orange-ATP vApp template is used. We recommend that you repeat the check yourself.

7.1. Checking resource availability

From the main Data Centers section, select the target vDC:



The screenshot displays the VMware Cloud Director interface. The top navigation bar includes tabs for 'VMware Cloud Director', 'Data Centers', 'Applications', 'Networking', 'Libraries', 'Administration', and 'Monitor'. The 'Data Centers' tab is selected. Below the navigation bar, the 'Virtual Data Center' section is visible. It shows a summary of the environment: Sites: 1, Organizations: 1, Virtual Data Centers: 3, Running Applications: VMs: 1, vApps: 2, and Used Resources: CPU. A red arrow points to the 'Data Centers' tab. Another red arrow points to the 'vdc-startrek.com-ha-01' vDC entry in the list. The vDC details show 1 vApp and 1 of 1 Running VMs. Resource usage is displayed for CPU (4 GHz used, 50 GHz allocated), Memory (512 MB used, 64 GB allocated), and Storage (5 GB used, 700 GB allocated).

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

On the left in the General menu:

vmw VMware Cloud Director

Data Centers

Applications

Networking

Libraries

Administration

Monitor

<<

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

General

Metadata

Sharing

Kubernetes Policies

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%)

Available disk resources can be found in the Storage Policies menu:

Storage 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. Checking network resources

In the Data Centers section, select vDC, then select vApps from the menu on the left and go to the test vApp:

vApps

Find by: Name

1 Virtual Applications Expired: No Clear all

NEW

ATP-1.0

Powered off
Lease
Created On 05/16/2018, 5:56:30 PM
Owner adm_startrek.com

VMs 1 Manage
VM Consoles

CPU 2
Storage 2.06 TB
Memory 512 MB
Networks 1

BADGES

ACTIONS **DETAILS**

The orange-atp virtual machine should already be running, if it is not, start the entire vApp and go to the VM:

The screenshot shows the vSphere interface for the ATP-1.0 vApp. The left sidebar contains a menu with 'Virtual Machines' highlighted. The main area displays a table of virtual machines. The 'orange-atp' VM is listed with a status of 'Powered on'. Red arrows point to the 'Virtual Machines' menu item and the 'orange-atp' entry in the table.

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

To access the virtual machine console, you can use the web console or VMRC (recommended, but it requires the client to be installed on a PC, Contact Orange to receive a distribution kit):

The screenshot shows the vSphere interface for the 'orange-atp' VM. The 'LAUNCH WEB CONSOLE' and 'LAUNCH REMOTE CONSOLE' buttons are highlighted with red boxes and arrows. The left sidebar shows the 'General' tab selected. The main area displays the VM details table.

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

VMs from this vApp automatically get included in the OS and receive network settings using VMware Tools. Now you should check the availability of networks. As an example, for the Internet this can be done with the "ping yandex.ru" command, as a result of which the following ICMP responses should be received:

```

https://flexible-computing-advanced.orange-business.ru/tenant/vorg-startrek.com/wmks-console/index.html?
Orange-ATP - orange-atp FULL SCREEN

CTRL+ALT+DEL OPTIONS

Last login: Wed Dec  9 15:08:33 MSK 2020 on tty1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Wed Dec  9 15:08:51 MSK 2020

System load: 0.0          Memory usage: 13%    Processes:   90
Usage of /: 36.7% of 3.11GB Swap usage:  0%    Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

atp@orange-atp:~$ ping yandex.ru
PING yandex.ru (5.255.255.77) 56(84) bytes of data:
64 bytes from yandex.ru (5.255.255.77): icmp_seq=1 ttl=249 time=4.95 ms
64 bytes from yandex.ru (5.255.255.77): icmp_seq=2 ttl=249 time=5.13 ms
64 bytes from yandex.ru (5.255.255.77): icmp_seq=3 ttl=249 time=5.16 ms
64 bytes from yandex.ru (5.255.255.77): icmp_seq=4 ttl=249 time=5.10 ms
^C
--- yandex.ru ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 4.957/5.089/5.164/0.079 ms
atp@orange-atp:~$ _

```

For the BVPN network (VM atp-ipvpn), the procedure is the same, but you should check the availability of the remote host in your BVPN network.

8. User account management

Cloud Director allows you to manage user access rights for cloud resources. You can select the required role when creating a new user.

During the initial configuration of your cloud, one user is created with full Organization Administrator rights. If necessary, you can create any number of users with different rights.

VMware Cloud Director Administration

Users

NEW

EXPORT USERS

Name	Full Name	State	Locked	Role	Type
adm_startrek.com	1	Enabled	☐	Organization Administrator	Local
csr		Enabled	☐	vApp User	Local
veeamtest		Enabled	☐	Organization Administrator	Local

Fill in the details of the new user and set the role:

Create User

Credentials

User name *

Input is required

Password *

Confirm password *

Enable☒

Configure user's quota☒

Upon successful user's data save, redirects to user's quota section

Role

Available roles *

Select a role

	Name	Description
☐	Organization Administrat...	Built-in rights for administering an organization
☐	vApp Author	Rights given to a user who uses catalogs and crea
☐	Console Access Only	Rights given to a user who can only view virtual m
☐	vApp User	Rights given to a user who uses vApps created by
☐	Defer to Identity Provider	Rights will be determined based on information re

Contact Info

Full name

Email address

Phone number

IM

Quotas

All VMs quota

☒ Unlimited

DISCARD

SAVE

Types of role:

The Organization Administrator has full access rights to the entire organization and its hierarchy.
Catalog Author can create and publish catalogs.
vApp Author can use directories and create vApps.
vApp User can use existing vApps.
Console Access Only will allow a user with this role to only view the properties of virtual machines and use the guest OS console (without the ability to switch it on/off).

Access rights for a specific vApp for users with the vApp User role are defined in the settings of a specific vApp:

VMware Cloud Director

Data Centers Applications Networking Libraries Administration Monitor More

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

General

Metadata

Sharing

Kubernetes Policies

vApps

Find by: Name

ADVANCED FILTERING

1 Virtual Applications

Expired: No

Clear all filters

NEW

Orange-ATP

Powered on

Lease 52 minutes (Suspends)

Created On 12/09/2020, 3:07:37 PM

Owner system

VMs 1

CPU 2

Storage 4.5 G

Manage

Power

Renew Lease

Snapshot

Download

Move

Copy

Change Owner

Share

Add

ACTIONS

Share

Share with

☐ All Users and Groups

☒ Specific Users and Groups

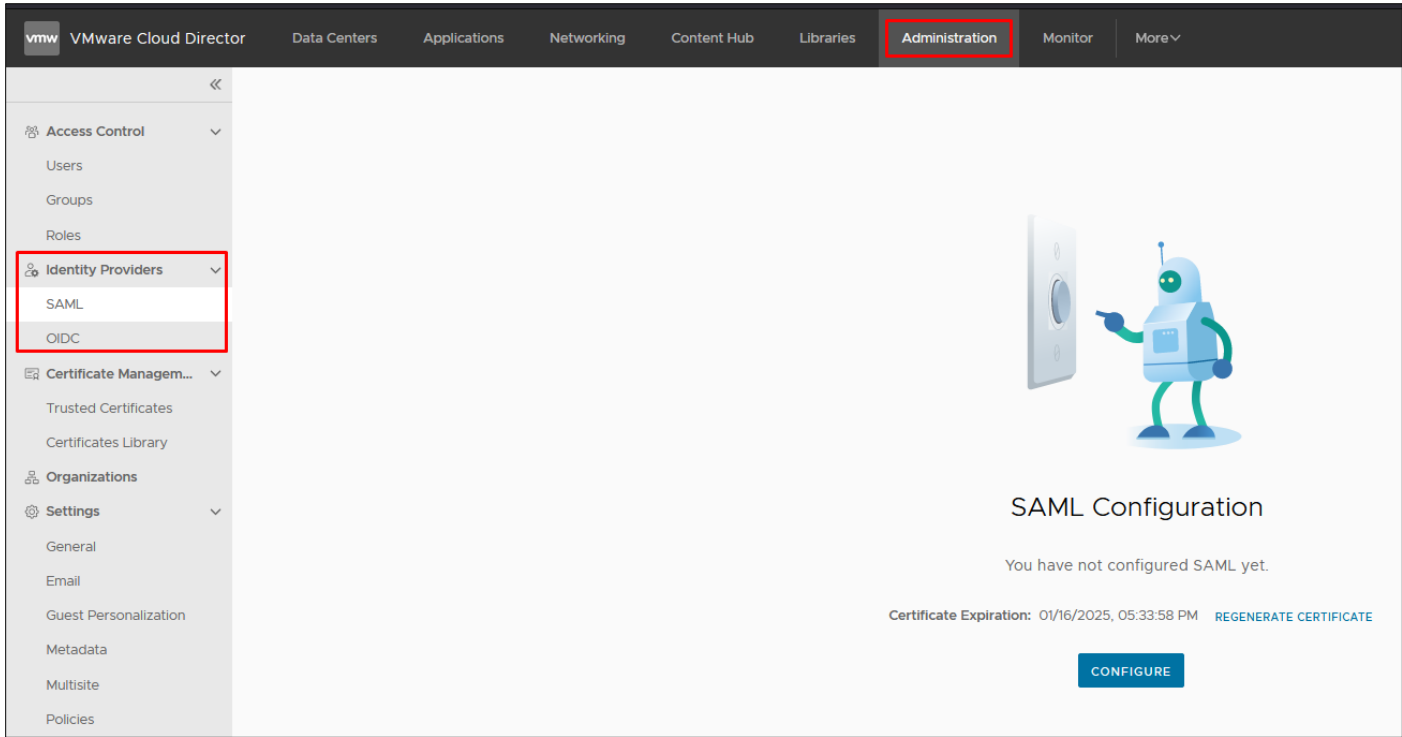
Users 0 Groups 0

Show selected

Name	Access Level
adm_startrek.com	Read Only
csr	Read Only
veeamtest	Read/Write

DISCARD SHARE

If needed, a mechanism for integrating third-party accounts via SAML or OIDC can be used. In this case, the standard Cloud Director login window will be changed, to log in using local accounts it is necessary to use a URL like "https://flexible-computing-advanced.orange-business.ru/tenant/HA3BAHIE-VORG/login" for login

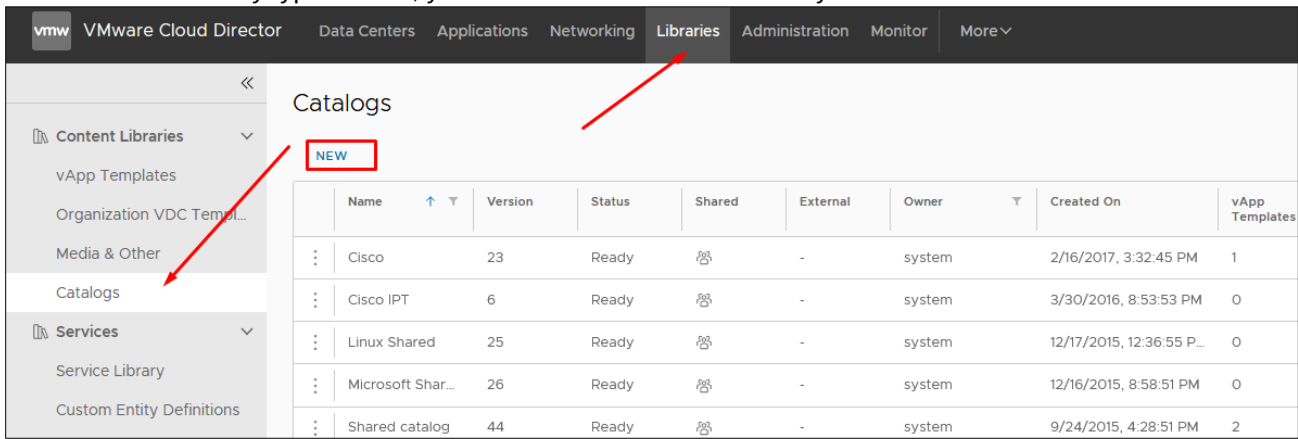


For more information on setup, please refer to the manufacturer's documentation:
<https://docs.vmware.com/en/VMware-Cloud-Director/10.5/VMware-Cloud-Director-Service-Provider-Admin-Guide/GUID-89329614-343E-44AC-9AD3-90A3119D970B.html>

9. Uploading images (ISO) and VM templates

9.1. Directory creation

To be able to load any type of data, you first need to create a directory to store it in:



Select the storage location for the directories:

Create Catalog

Name this Catalog

You can use a catalog for sharing vApp templates and media with other users in your organization. You can also have a private catalog for vApp templates and media that you frequently use.

Name *

test-catalog

Description

Pre-provision on specific storage policy

Storage Policy

Select a storage policy

	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

1 - 5 of 9 storage policies

By default, the directory will be available to all users of your organization in read-only mode. If necessary, this para

vmw

VMware Cloud Director

Data Centers

Applications

Networking

Content Hub

Welcome to Content Hub

Content

Catalogs

Manage Resources

VMware Marketplace

Helm Chart Repository

Kubernetes Operator

Catalogs

NEW

Name	Version	Status
Cisco	24	Ready
Cisco IPT	6	Ready
Linux Shared	44	Ready
Microsoft Shared	39	Ready
Shared catalog	70	Ready
test	21	Ready

Edit

Share

Publish settings

Subscribe settings

Sync

Storage Policies

Change owner

Metadata

Delete Catalog

meter can be changed:

Share Catalog 'test'

Users and Groups

Organizations

Share with

☒ All Principals

Full Control

☐ Specific Principals

Users

Groups

Service Accounts

☐ Show selected

☐	Name	Full Name	Access Level
☐	adm_startrek.com	1	Read Only
☐	csr		Read Only
☐	i.korotovskikh		Read Only
☐	veeam.sa	Veeam Service Account: DO NOT M...	Read Only

Users

1 / 2

DISCARD

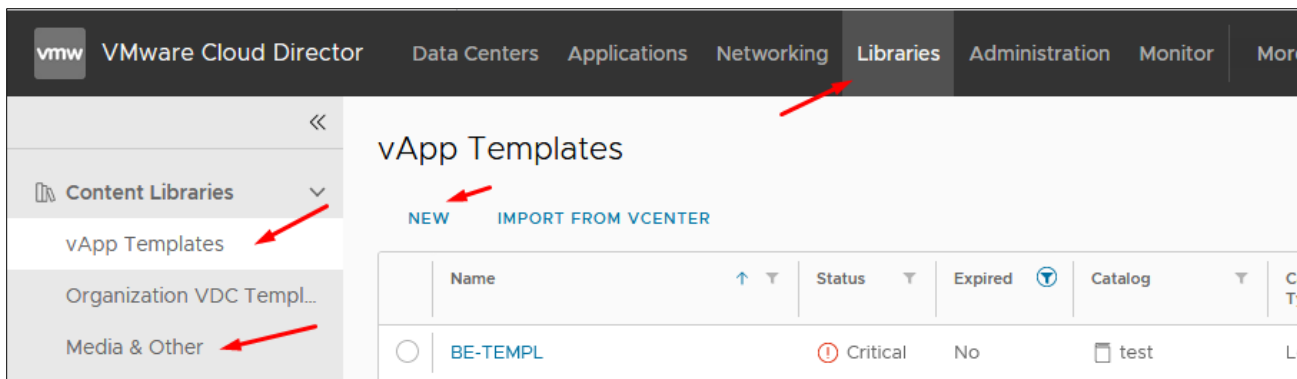
SAVE

9.2. Uploading via Cloud Director

After creating the catalog, it becomes possible to upload ISO images (Media & Other) or vApp templates in the OVA or OVF format (vApp Templates).

Attention:

- Images must be in the OVF or OVA format. The newest supported Virtual Hardware version is 19;
- Additional devices, except for SCSI HDD, IDE CD-ROM, VMware Video Card, and Network Adapters, should not be connected to the machine (such devices as sound cards, SATA disk devices, etc. are not supported). Therefore, if you have a virtual machine in the VMX format (for example, from a local instance of vSphere or VMware workstation), then they must first be exported to the OVF/OVA format or converted using the [ovftool](#) utility.



9.3. Upload via the Orange FTPS server

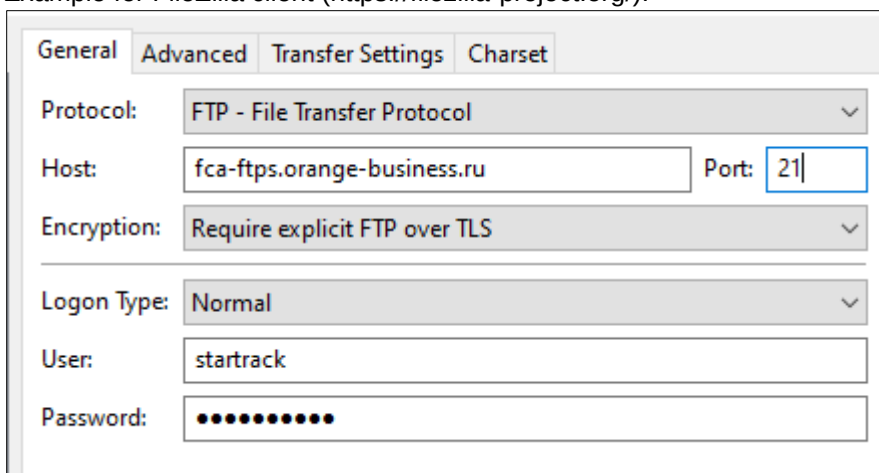
An alternative way to upload VM templates is to use the Orange FTPS server. This option is more useful if you need to upload a large number of VMs or if you ordered the VM migration service provided by Orange (in this case, you can upload VM files without converting them to OVA/OVF).

You can get the access details for the FTPS server by contacting Orange HelpDesk or your account manager. After the upload is complete, you should inform Orange in order to carry out the import procedure.

Connection settings:

- Host: fca-ftp.orange-business.ru
- Port: 21
- Protocol: FTP
- Encryption: FTP over TLS explicit

Example for FileZilla client (<https://filezilla-project.org/>):



9.4. Upload via ovftool

The ovftool utility is extremely convenient when working with vCloud and speeds up work processes in comparison with the web interface. Detailed documentation is available [on the utility page](#).

Version ovftool 4.4.0 is currently required.

Below are some examples of syntax:

- 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. VOrg and vApp networks

10.1. Creating a vOrg network

The screenshot shows the VMware Cloud Director interface. In the left sidebar, the 'Networking' menu is expanded, and 'Networks' is selected. The main panel displays the 'New Organization VDC Network' wizard. The 'Scope' step is active, showing a radio button selected for 'Current Organization Virtual Data Center'. Below this, it states 'Provides connectivity for VMs in the current VDC only'. The 'Networks' table below shows a single network entry: 'Shared-net-test' with a status of 'Normal', gateway '192.168.83.1/24', and network type 'Isolated'.

Depending on the task, we choose an isolated network or a network connected to the EGW.

The screenshot shows the 'New Organization VDC Network' wizard, specifically the 'Network Type' step. The 'Isolated' option is selected with a radio button. Below it, a description states: 'This type of network provides a fully isolated environment, which is accessible only by this organization VDC or VDC Group.' The 'Routed' option is also visible but unselected, with a description: 'This type of network provides controlled access to machines and networks outside of the VDC or VDC Group through an edge gateway.'

Specify the network parameters. If you plan to use DHCP, you must reduce the DHCP address pool by the size of the Static IP pool. If your infrastructure has more than one vDC, the network can be made available to other vDCs by enabling the following parameter:

New Organization VDC Network

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

General

Name *

Gateway CIDR *

Description

Shared

☐

i

10.2. Creating a vApp network

The vApp network is configured from the vApp window (as opposed to the vOrg network).

VMware Cloud Director interface showing the configuration of a vApp network. The left sidebar shows the navigation menu with 'vApps' highlighted. The main panel displays the configuration for 'ATP-1.0' (Powered off). The 'NEW' button is highlighted, and the table below shows the network configuration.

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)

In vApp, you can add an (L2) vDC network directly or make it isolated:

Add Network to ATP-1.0

Type

☐ OrgVDC Network

☐ vApp Network

CANCEL

ADD

An isolated vApp network can be connected to the vOrg network via the vApp Edge (adding the ability to activate FW and 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 and FW for this option are configured within the network:

11. NSX Edge Gateway

11.1. NSX Edge Gateway size and performance

By default, NSX Edge Gateway is sized Compact and limited to connect up to 9 internal client virtual networks (10 primary interfaces, one taken by uplink). Additional interfaces (up to 200 on each primary interface) can be configured using the internal network connection type “Subinterface” on each primary interface.

The NSX Edge Gateway can be resized to Large, X-Large and Quad-Large, as well as the number of connected networks can be increased and the high availability option for NSX Edge can be activated.

The performance of its functions depends on the size of the EGW:

	NSX Edge (Compact)	NSX Edge (Large)	NSX Edge (Quad-Large)	NSX Edge (X-Large)
vCPU	1	2	4	6
Memory	512 MB	1 GB	1 GB	8 GB
Disk	512 MB	512 MB	512 MB	4.5 GB + 4 GB
Interfaces	10	10	10	10
Sub Interfaces (Trunk)	200	200	200	200
NAT Rules	2048	4096	4096	8192
ARP Entries Until overwrite	1024	2048	2048	2048
FW Rules	2,000	2000	2000	2000
FW Performance	3 Gbps	9.7 Gbps	9.7 Gbps	9.7 Gbps
DHCP Pools	20k	20k	20k	20k
ECMP Paths	8	8	8	8
Static Routes	2048	2048	10240	10240
LB Pools	64	64	64	1024
LB Virtual Servers	64	64	64	1024
LB Server / Pool	32	32	32	32
LB Health Checks	320	320	320	3072
LB Application Rules	4096	4096	4096	4096
L2VPN Clients Hub to Spoke	5	5	5	5
L2VPN Networks per Client/Server	200	200	200	200
IPSec Tunnels	512	1600	4096	6000
SSLVPN Tunnels	50	100	100	1000
SSLVPN Private Networks	16	16	16	16

Concurrent Sessions	64k	1000k	1000k	1000k
Sessions/Second	8k	50k	50k	50k
LB Throughput L7 Proxy)	n/a	2.2 Gbps	2.2 Gbps	3 Gbps
LB Throughput (L4 Mode)	n/a	6 Gbps	6 Gbps	6 Gbps
LB Connections/s (L7 Proxy)	n/a	46k	50k	50k
LB Concurrent Connections (L7 Proxy)	n/a	8k	60k	60k
LB Connections/s (L4 Mode)	n/a	50k	50k	50k
LB Concurrent Connections (L4 Mode)	n/a	600k	1000k	1000k
BGP Routes	20k	50k	250k	250k
BGP Neighbors	10	20	100	100
BGP Routes Redistributed	No Limit	No Limit	No Limit	No Limit
OSPF Routes	20k	50k	100k	100k
OSPF LSA Entries Max 750 Type-1	20k	50k	100k	100k
OSPF Adjacencies	10	20	40	40
OSPF Routes Redistributed	2k	5k	20k	20k
Total Routes	20	50	250	250

11.2. DHCP configuration

Go to the Networking tab, Edge Gateways, select the required EGW, and click Services:

The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'vmw', 'VMware Cloud Director', and tabs for 'Data Centers', 'Applications', 'Networking' (selected), 'Libraries', 'Administration', 'Monitor', and 'More'. Below the navigation bar, the 'Edge Gateways' tab is selected. A table lists edge gateways with columns: Name, Status, Scope, Distributed Routing, Used NICs, and External Networks. The first entry is 'egw-startrek.com-da-...' with a status of 'Normal' and 'Disabled' distributed routing. A red box highlights the 'SERVICES' button above the table. A red arrow points to the first entry in the table.

Enable DHCP service and click 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
----------	---------------------	--------------------	-----------------

Set pool parameters

Add DHCP Pool

-

IP Range *

Domain Name

Auto Configure DNS ☐

Primary Name Server

Secondary Name Server

Default Gateway

Subnet Mask

Lease Never Expires ☐

Lease Time (Seconds)

Note: The range of these IP addresses must not overlap with the Static IP Pool of the organization's network.

This can be checked and changed here:

vmw VMware Cloud Director

Data CentersApplicationsNetworkingLibrariesAdministrationMonitorMore

NetworksEdge GatewaysData Center Groups

NEW

Filter by: All

View accessible 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%	

vmw VMware Cloud Director

Data CentersApplicationsNetworkingLibrariesAdministrationMonitorMore

All Networks > shared-routed

shared-routed

OPEN IN VDC CONTEXTDELETE

General

IP Management

Static IP Pools

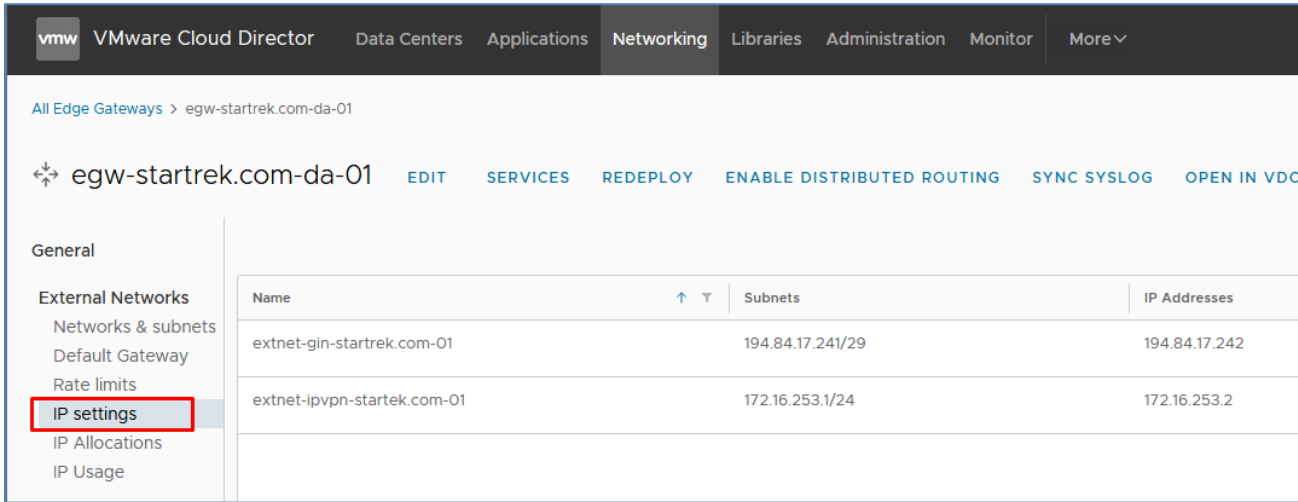
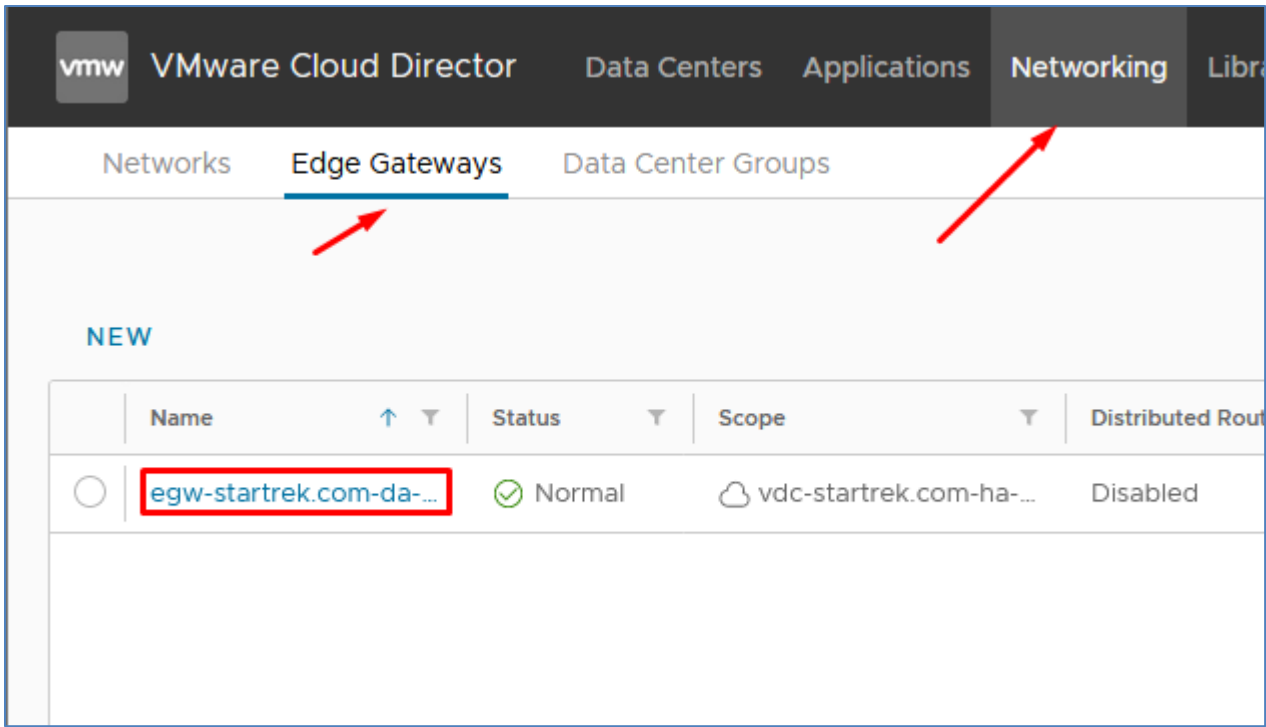
DNS

IP Usage

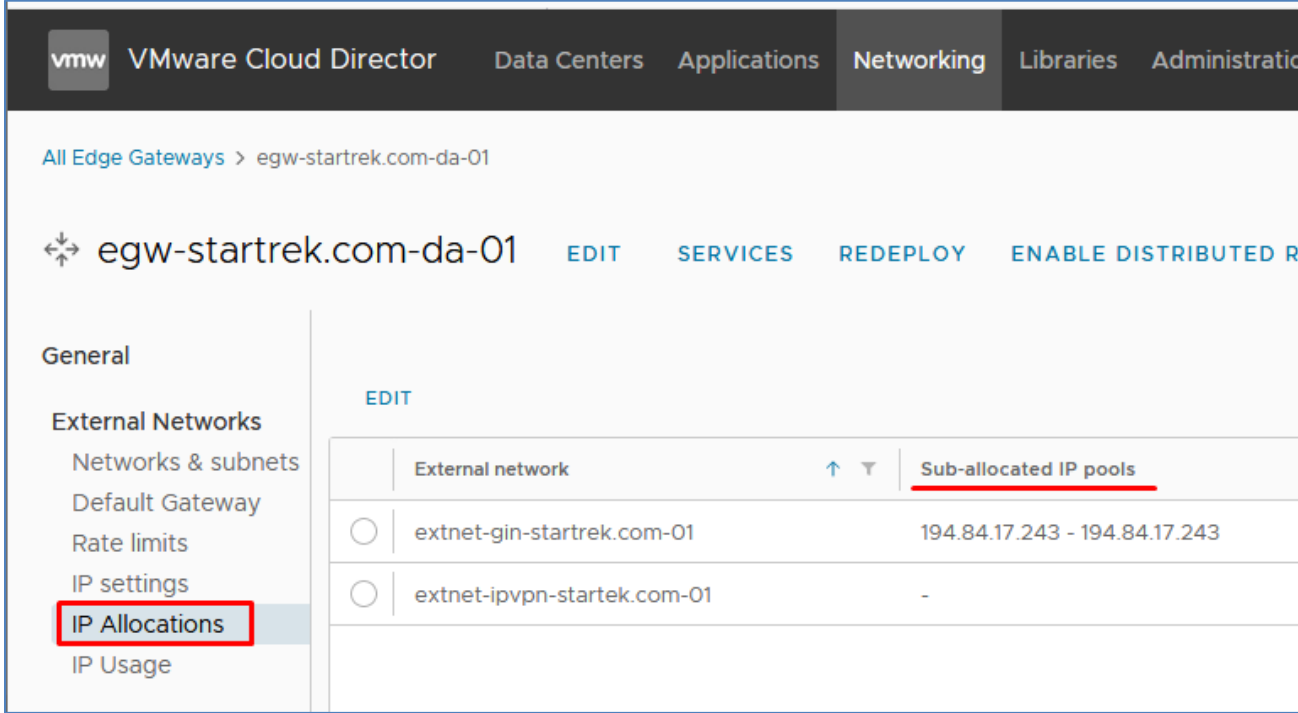
EDIT

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

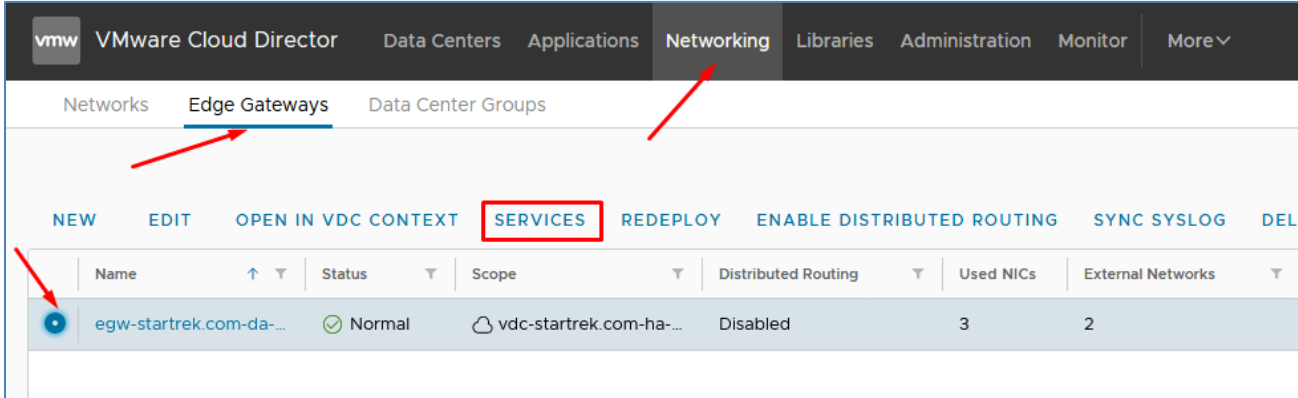
- 11.3. NAT configuration
- NAT (Network Address Translation) is used for the translation of private (gray, RFC1918) IP addresses to external (white) ones and vice versa. In this way, your virtual machine gains access to the Internet. To configure this mechanism in Cloud Director, you need to configure SNAT and DNAT rules.
- 11.3.1. Creating a SNAT rule
- SNAT (Source Network Address Translation) is a mechanism to replace the source address when sending a packet. Go to the Administration tab, select your vDC, open the Edge Gateways tab, right-click on the required EGW and select the Edge Gateway Services item.



In addition to the main EGW address, it can be assigned additional addresses from the networks connected to it:



Close the window and select Services for the required EGW.



Go to the NAT tab and click the Add SNAT button

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.					

Specify parameters

- In the Applied On field, specify the external network (like extnet-gin-DOMAIN-XX);
- In the Original source IP / Range field, specify the internal address range, for example, 172.16.253.0/24;
- In the Translated source IP/range field, specify the external address through which the Internet or the main address will be accessed and which we saw on the Sub-Allocate IP Pools tab.

Add SNAT Rule

Applied On:

Original Source IP/Range *

Translated Source IP/Range *

Destination IP Address

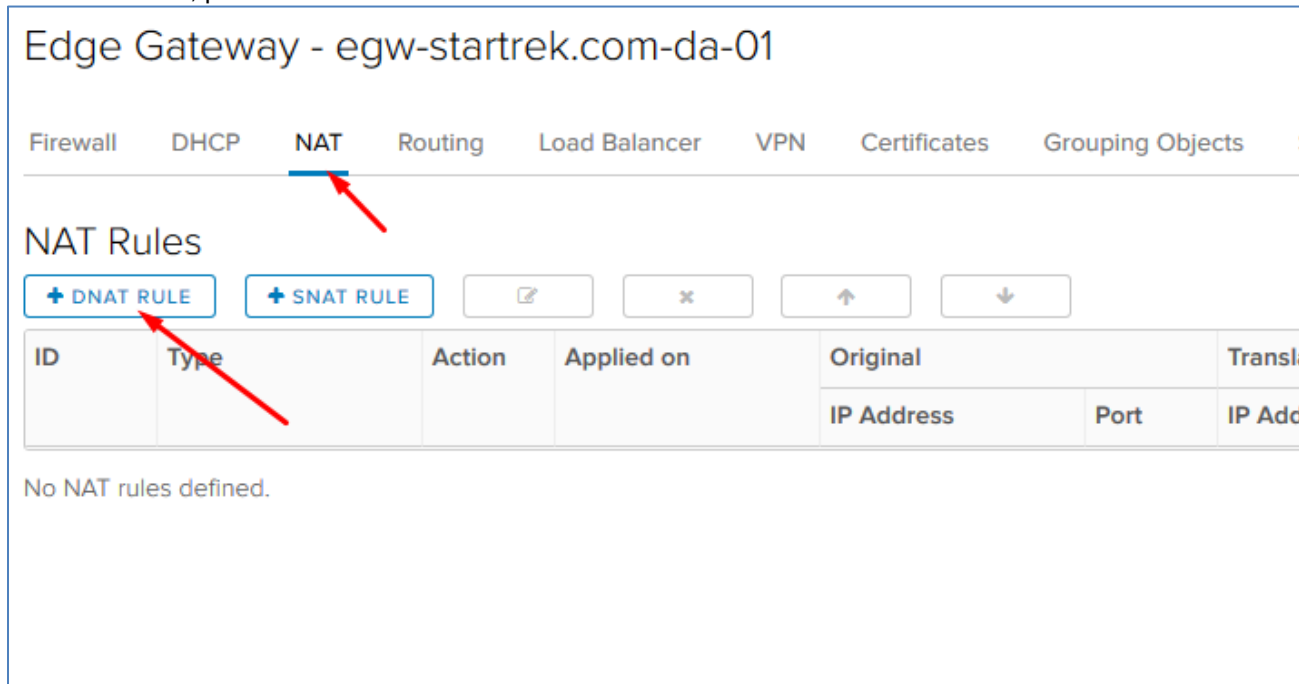
Destination Port

Description

11.3.2. Creating a DNAT rule

DNAT is a mechanism that changes the destination address and destination port of a packet. It is used to redirect incoming packets from an external address / port to a private IP / port within a private network.

On the NAT tab, press the Add DNAT button



Specify parameters:

- In the Applied On field, specify the external network (like extnet-gin-DOMAIN-XX);
- In the Description field, specify the description of the DNAT rule;
- In the Original IP/range field, specify the external address (an address from the Sub-Allocate IP Pools range);
- Fill in the Protocol field;
- In the Original Port field, specify the port on the external interface;
- In the Translated IP/range field, specify the internal IP address, for example, 172.16.253.50
- In the Translated Port field, specify the destination port on the internal server

Add DNAT Rule

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

Original IP/Range * 194.84.17.243

SELECT

Protocol TCP

Original Port 443

ICMP Type

Translated IP/Range * 172.16.253.50

Translated Port 443

DISCARD KEEP

After that, configure the Firewall to let the corresponding packets through.

11.4. Firewall configuration

Go to the Administration tab, select your vDC, open the Edge Gateways tab, right-click on the required EGW and select the Edge Gateway Services item.

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

In the Services window that appears, go to the Firewall tab and click Add.

By default, the Deny option is selected in the Default Action item, meaning that the Firewall will block all traffic. To prevent this, you need to configure the rules.

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✓	default rule for ingress traffic	Default Policy	Any	Any	Any	Deny

Fill in the parameters of the new rule:

- In the Name field, specify a name for the rule;
- In the Source field, enter the source addresses: single IP address, IP address range, CIDR, ANY, or virtual infrastructure objects:

+ 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	Deny
4✓	default rule for ingress traffic	Default Policy	Any	Any	Any	Deny

Select objects

Browse objects of type:

GATEWAY INTERFACES ▶

Filter...

extnet-ipvpn-startrek.com-01

extnet-gin-startrek.com-01

Internal

Gateway Interfaces

VirtualMachines

OrgVdcNetworks

Ip Sets

Security Groups

Current page: 1

DISCARD KEEP

- Specify the recipient's address in the Destination field. The format is the same as for the Source field;
- In the Service field, select the recipient protocols and ports. You can leave Any, for example, for 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

• In the Action field, select the required value (Allow or Deny).

Attention: If the global Firewall policy is set to Allow, then the FW rule sets the parameters of sessions that the Firewall will block. To do this, select the Deny option in the rule's window. If the Deny option is selected in the global policy, then the rule specifies the parameters of sessions that the Firewall will let through.

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

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. Static Routing configuration

If necessary, static routes can be specified on the EGW.

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

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

Routing Configuration **Static Routes**

Static Routes

+ ✎ ✕

Type	Network	Next Hop	Interface	MTU	Description
No static routes defined					

Add Static Route

Network *

Network should be entered in CIDR format e.g. 192.169.1.0/24

Next Hop *

MTU 1,500

Interface extnet-gin-startrek.com-01 (extnet-gin-startrek.com-01)

Description

DISCARD KEEP

11.6. Load Balancer

Load Balancer (LB) is a fairly complex service provided by NSX Edge Gateway, so Orange recommends that you read [VMware's documentation](#) and plan your LB configuration.

To start configuring the Load Balancer, you need to select external IP addresses (Sub-Allocated IP Pools, see above) and internal server addresses.

Go to the Administration tab, select your vDC, open the Edge Gateways tab, right-click on the required EGW and select the Edge Gateway Services item.

Next, you should be guided by the configuration plan and the [Load Balancing section of the documentation](#).

11.7. VPN

NSX Edge Gateway provides the following types of VPN channels:

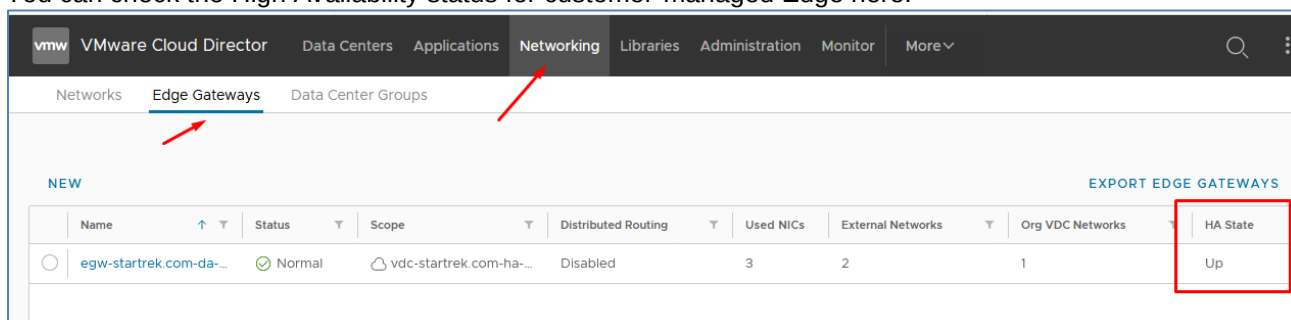
- SSL VPN-Plus, allows remote users to access corporate applications running in the cloud;

- IPsec VPN provides a firewall connection between the NSX Edge Gateway and remote sites, which can also be an NSX Edge Gateway or any other hardware/software router or VPN gateway that supports IPSEC. There are two options:
 - Policy-Based IPsec VPN is a simple option that is configured through the GUI;
 - Route-Based IPsec VPN allows for IPsec channel redundancy and is configured via API.
- L2 VPN can be used to expand an existing physical local network by connecting to the cloud without renumbering (changing) the IP addresses of servers when transferring between segments. L2 VPN tunnel is established only between two VMware Edge Gateways.

For more information, see the [Virtual Private Networks \(VPN\) documentation section](#).

11.8. NSX Edge High Availability

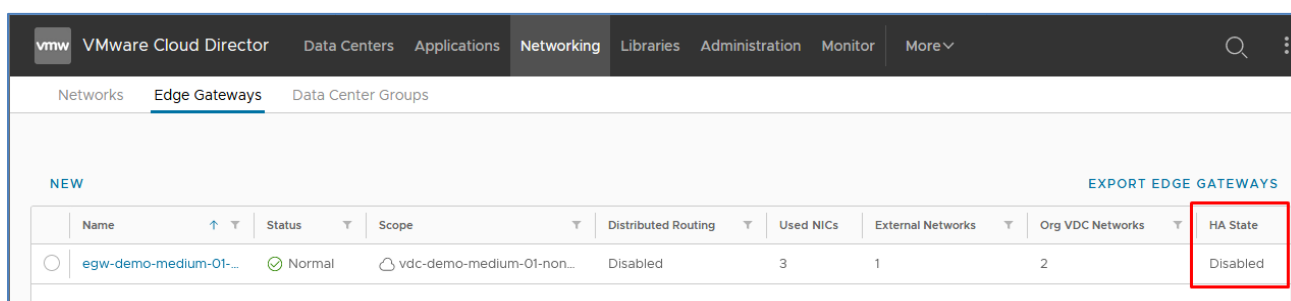
You can check the High Availability status for customer-managed Edge here:



The screenshot shows the VMware Cloud Director interface with the 'Networking' tab selected. Under 'Edge Gateways', a table lists the status of various edge gateways. The 'HA State' column for the gateway 'egw-startrek.com-da...' is 'Up', which is highlighted with a red box. Red arrows point to the 'Networking' tab and the 'Edge Gateways' sub-tab.

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

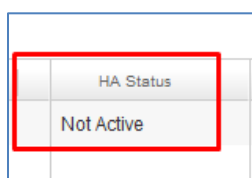
Up means that HA is enabled.



The screenshot shows the VMware Cloud Director interface with the 'Networking' tab selected. Under 'Edge Gateways', a table lists the status of various edge gateways. The 'HA State' column for the gateway 'egw-demo-medium-01...' is 'Disabled', which is highlighted with a red box.

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 means that HA is disabled.



A close-up of the 'HA Status' dropdown menu, showing 'Not Active' as the selected option, highlighted with a red box.

HA Status
Not Active

Not Active means that HA configuration is enabled but not active.

Note: To enable HA mode, at least one internal network must be connected to the Edge, as it will be used for heartbeat.

12. Configuring and managing virtual machines and vApps

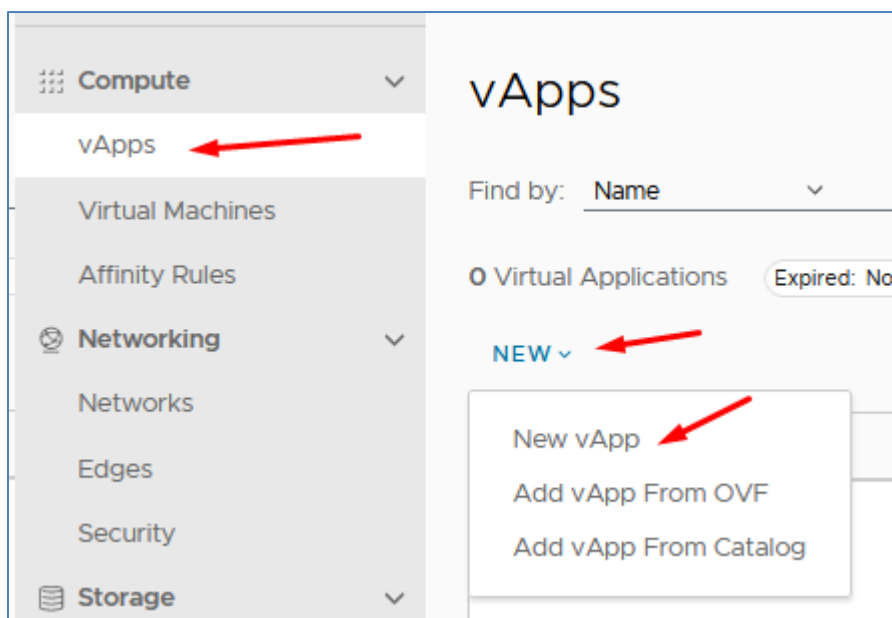
12.1. Creating a new vApp

A new vApp can be created empty using a vApp template or with an empty VM (without OS). Next, let's look at the process of creating a vApp with an empty VM.

Select the required 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 the 'Virtual Data Center' section is active. Below this, there are two vDCs listed:

- vdc-startrek.com-ha-01**:
 - Locations: vrg-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: vrg-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)



In the window that appears, set the vApp name and add the VM:

The 'New vApp' configuration window is shown. It has a title bar with a close button. The form includes: a 'Name' field with the value 'vApp.test'; a 'Description' field with the value 'testing'; a 'Power on' checkbox which is unchecked; a table with columns 'Virtual Machines', 'OS', and 'Compute' containing a funnel icon; an 'ADD VIRTUAL MACHINE' button (highlighted with a red arrow); and 'CANCEL' and 'CREATE' buttons at the bottom right.

In the window that appears, set the vApp name and add the 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

In the Add Virtual Machines tab, you can:

- Add a virtual machine template from the catalog
- Create a virtual machine from scratch and specify the boot ISO
- Leave the vApp empty and import the virtual machine template or image later

12.2. Creating a virtual machine from a template

Select an existing vApp and go to the Virtual Machines tab:

vmw

VMware Cloud Director

Data Centers

Applications

Networking

Content Hub

Libraries

Administration

Monitor

More

All Virtual data centers

Site: flexible-computing-advanced.orange-business.ru

Organization: vorg-startrek.com

Data center: vdc-startrek.com-ha-02

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

Kubernetes Policies

All vApps > Test-vApp-01

Test-vApp-01

Resolved

General

Virtual Machines

Start and Stop Order

Network Diagram

Networks

Guest Properties

Sharing

Metadata

Monitor

Tasks

Events

POWER OFF

START

STOP

RENEW LEASE

CHANGE OWNER

ALL ACTIONS

Power

Renew Lease

Snapshot

Download

Move

Copy

Change Owner

Share

Add

Create Template

Edit Badges

Delete

Add VM

Add Network

EDIT

Info

Name

State

Description

Data center

Owner

Snapshot

EDIT

Lease

Runtime Lease

Never expires

Add VMs to Test-vApp-01

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

Select a VM template from your own or public directory:

New VM

Name *

TestVM

Computer Name *

TestVM

Description

Type

☐ New

☒ From Template

Templates

	vApp Template Name	VM Name	Catalog	OS	Compute	Storage
☐	ubuntu-server-14.04.3	ubuntu-test	Shared catalog	Ubuntu Linux (64-bit)	CPU 2 Memory 1 GB	Policy -
☐	Orange-ATP	orange-atp-tpl	Shared catalog	Ubuntu Linux (64-bit)	CPU 2 Memory 1 GB	Policy -
☐	Orange-ATP	orange-atp-tpl	test	Ubuntu Linux (64-bit)	CPU 2 Memory 1 GB	Policy -

Next, set the VM storage location and other parameters.

Some templates (OVA) do not allow you to specify a storage policy at creation time, in this case it is possible that the default #SYSTEM level does not have enough free space: you must select any policy where there is enough space, after the template is deployed, change the generic to the desired #SYSTEM type.

In any scenario, after deployment, you must change the VM's working disk storage policies to the desired one.

Depending on the type of template, certain parameters are available for customizing the VM:

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

Connecting to networks:

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

Check the parameters and complete the creation of the VM by pressing the Finish button.

12.3. *Creating a virtual machine from scratch*

vmw VMware Cloud Director

Data CentersApplicationsNetworkingContent HubLibrariesAdministrationMonitorMore

All Virtual data centersSite: flexible-computing-advanced.orange-business.ruOrganization: vorg-startrek.comData center: vdc-startrek.com-ha-02

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

Kubernetes Policies

All vApps > Test-vApp-01

Test-vApp-01

Resolved

General

Virtual Machines

Start and Stop Order

Network Diagram

Networks

Guest Properties

Sharing

Metadata

Monitor

Tasks

Events

POWER OFFSTARTSTOPRENEW LEASECHANGE OWNERALL ACTIONS

EDIT

Info

Name

State

Description

Data center

Owner

Snapshot

EDIT

Lease

Runtime Lease

Never expires

Power

Renew Lease

Snapshot

Download

Move

Copy

Change Owner

Share

Add

Create Template

Edit Badges

Delete

Add VM

Add Network

Add VMs to Test-vApp-01

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

New VM

Name *

TestVM

Computer Name *

TestVM

Description

Type

New

From Template

Operating System

Guest OS family *

Linux

Guest OS *

Ubuntu Linux (64-bit)

Boot image

Select...

	Name	Catalog
☐	ubuntu-14.04.3-desktop-amd64.iso	Linux Share
☐	ubuntu-14.04.3-server-amd64.iso	Linux Share
☐	ubuntu-16.04.3-server-amd64.iso	Linux Share
☐	ubuntu-20.04.2-live-server-amd64.iso	Linux Share
☐	ubuntu-22.04.1-live-server-amd64.iso	Linux Share
☐	ubuntu-22.04.2-live-server-amd64.iso	Linux Share
☐	ubuntu-22.04.3-live-server-amd64.iso	Linux Share

Boot Options

Boot Firmware

Enter Boot Setup

Compute

Placement Policy

Version 4.1.6 © Orange Business Services, 2024

58

 **Business**

Orange Restricted

Set virtual hardware parameters

New VM

Boot image

ubuntu-22.04.2-live-server-amd64.iso

Boot Options

Boot Firmware

BIOS

Enter Boot Setup

Compute

Placement Policy

VM placement to Site1

Sizing Policy

None

CPU

8

Cores per socket

8

Number of sockets

1

Memory

128

GB

Storage

ADD

Disk	Storage Policy	IOPS Reservation	Size	
1	platinum_plus_e2-ha-site1	25000	* 10 GB	

It is mandatory to specify one of the “#SYSTEM” as the default storage policy for the VM (with or without site linkage).

Storage

ADD

Disk	Storage Policy	IOPS Reservation	Size	
1	platinum_plus_e2-ha-site1	25000	* 10 GB	

Use custom storage policy:

Storage Policy

#SYSTEM-site1

Networking

ADD

ADD NETWORK TO VAPP

NIC	Network	Network Adapter Type	IP Mode	IP Address	Primary NIC	
1	None	VMXNET3	None	Auto-assigned		

The new VM will appear in the list

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

You can add another VM immediately.

12.4. Installing an OS on a virtual machine

To install the OS on a ready-made virtual machine, you need to connect the ISO image of the installation disc. Only the ISO file previously uploaded to the Cloud Director directory can be connected.

It is assumed that a directory has already been created and the correct ISO image from the installation disc has been loaded into it.

Select Insert Media from the VM context menu:

The screenshot shows the VMware Cloud Director interface. The breadcrumb navigation at the top reads "All vApps > Orange-ATP > test". The left sidebar shows the "Compute" section expanded, with "Virtual Machines" selected. The main panel displays the "test" VM, which is "Powered off". The "Hardware" tab is active, and the "Removable Media" sub-tab is selected. A context menu is open over the "Removable Media" section, showing options: "Insert Media", "Eject Media", "Power", "Snapshot", "VM Console", "Media", "Install VMware Tools", "Upgrade Virtual Hardware Version", "Move", "Copy", "Convert to vApp", "Consolidate Disks", "Edit Badges", and "Delete". Red arrows point to the "Insert Media" option in the context menu and the "Media" option in the "Hardware" sub-menu.

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_11.0.1.10000-75.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

By default, the DVD drive appears in the boot list, but not as the first item. If there is a need to change the boot order, you need to do it through BIOS/UEFI. For this, you need to set the option to automatically enter BIOS/UEFI the next time the VM is turned on:

vmware VMware Cloud Director Data Centers Applications Networking Libraries Administration Monitor More

test

All vApps > Orange-ATP > test

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

General

test

Powered off

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

General

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

✕

Name *

test

Computer Name *

test

Description

Operating System Family

Microsoft Windows

Operating System

Microsoft Windows Server 2016 (64-bit)

Boot Delay *

0

Storage Policy

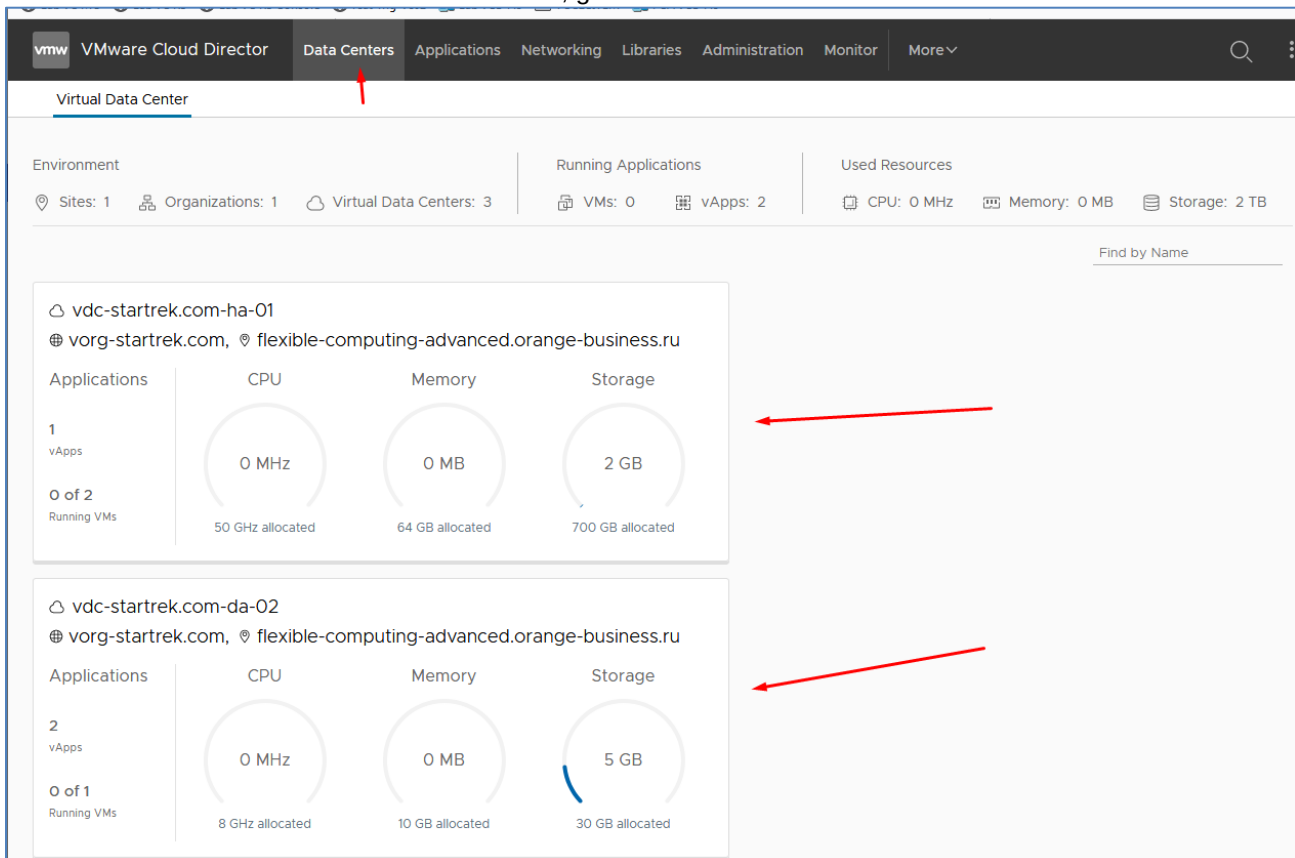
vmstore-cloud-platinum-ha

Enter BIOS Setup

☒

12.5. Resource monitoring

To view the current utilization of vDC resources, go to the Data Centers tab:



More details can be viewed inside the vDC:

vmw

VMware Cloud Director

Data Centers

Applications

Networking

Libraries

Administration

Monitor

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%)

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

General

Metadata

Sharing

Kubernetes Policies

vmw

VMware Cloud Director

Data Centers

Applications

Networking

Libraries

Administration

Monitor

More

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

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

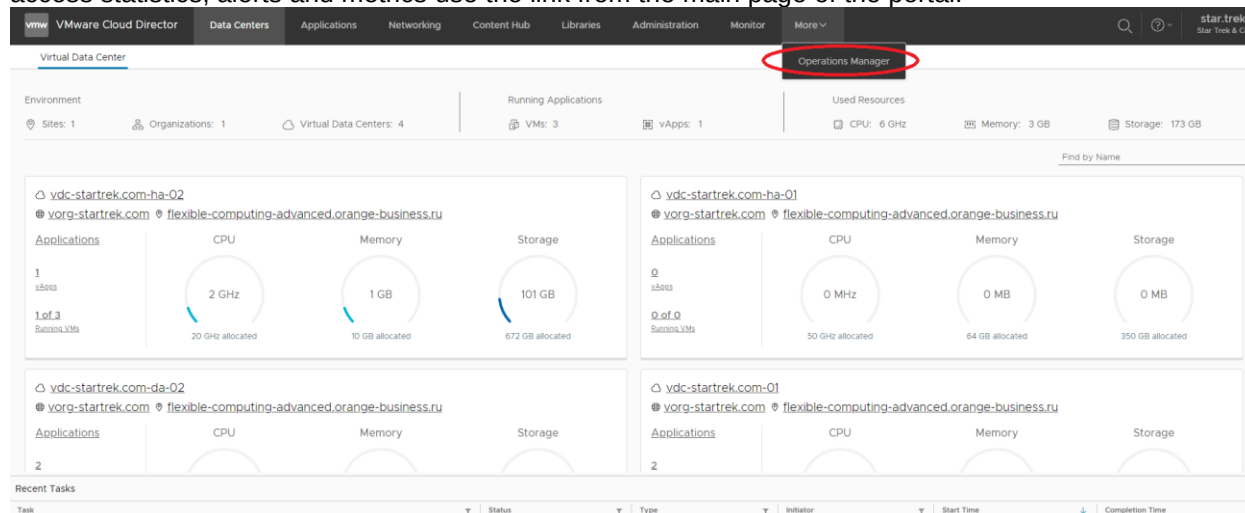
Storage Policies

Settings

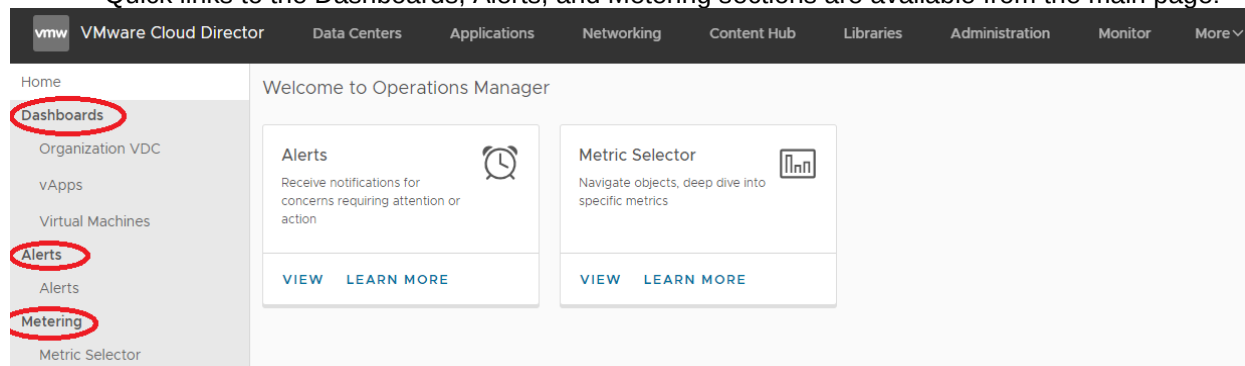
General

12.6. Historical VM metrics

Cloud Director portal users are able to view detailed historical statistics for virtual machines in their vDCs. To access statistics, alerts and metrics use the link from the main page of the portal:



Quick links to the Dashboards, Alerts, and Metering sections are available from the main page:



The Dashboards section allows you to quickly access data about your vDCs, deployed vApps, and virtual machines.

Home

Dashboards

Organization VDC

vApps

Virtual Machines

Alerts

Alerts

Metering

Metric Selector

EXPORT

Type here to apply filters

Name	vAPP	Organization	Organization VDC	Status	Number of vcpu	CPU Utilization	Memory Utilization	Storage Utilization
atp-sp-3-HYWy	atp-sp-3-5ddad4e0-59d3...	vorg-startrek.com	vdc-startrek.com-01	Powered on	2	27.33 MHz	424.59 MB	20 GB
atp-sp-2-JdPQ	atp-sp-2-ast3a4f5-616a-4...	vorg-startrek.com	vdc-startrek.com-01	Powered on	2	27.13 MHz	432.65 MB	20 GB
orange-atp-MIVT	ATP-DA	vorg-startrek.com	vdc-startrek.com-da-02	Powered off	4	-	0 KB	4 GB
orange-atp-HdDN	orange-atp-64940bad-e...	vorg-startrek.com	vdc-startrek.com-ha-02	Powered off	2	-	0 KB	54 GB
orange-atp2-U2tZ	ATP-DA2	vorg-startrek.com	vdc-startrek.com-da-02	Powered off	2	-	0 KB	4 GB
atp-ic-1-FpAM	atp-ic-1-w29b87fc-e553-...	vorg-startrek.com	vdc-startrek.com-ha-02	Powered on	2	30.4 MHz	439.41 MB	33 GB
atp-sp-1-8cTL	tst	vorg-startrek.com	vdc-startrek.com-01	Powered off	2	-	0 KB	20 GB
orange-atp-tpi-JGCP	orange-atp-tpi	vorg-startrek.com	vdc-startrek.com-ha-02	Powered off	2	-	0 KB	10 GB

Alerts review

Alerts section contains a list of current alerts sorted by importance.

VMware Cloud Director

Data CentersApplicationsNetworkingContent HubLibrariesAdministrationMonitorMore

star.trek
Star Trek & Co

Home

Dashboards

Organization VDC

vApps

Virtual Machines

Alerts

Alerts

Metering

Metric Selector

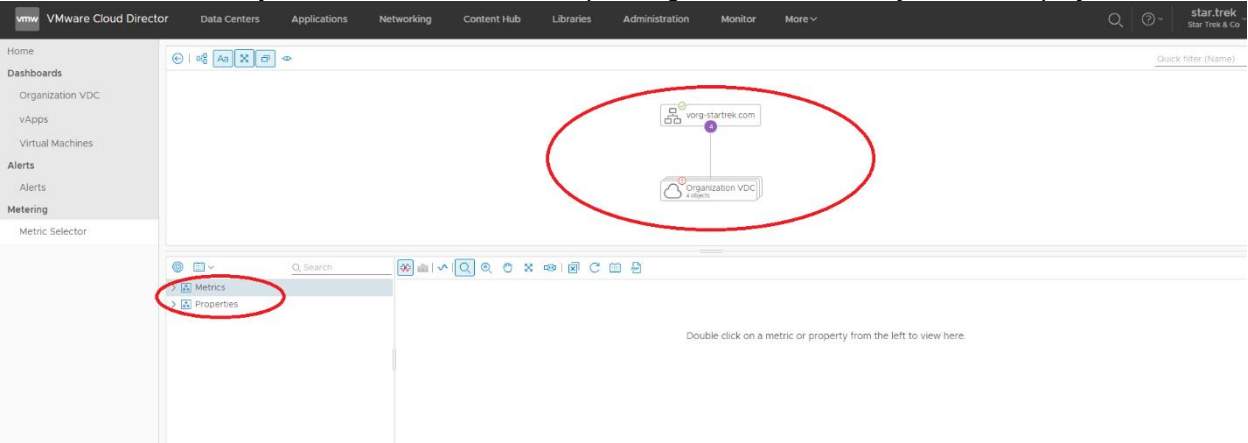
Group ByNone

Status:Active

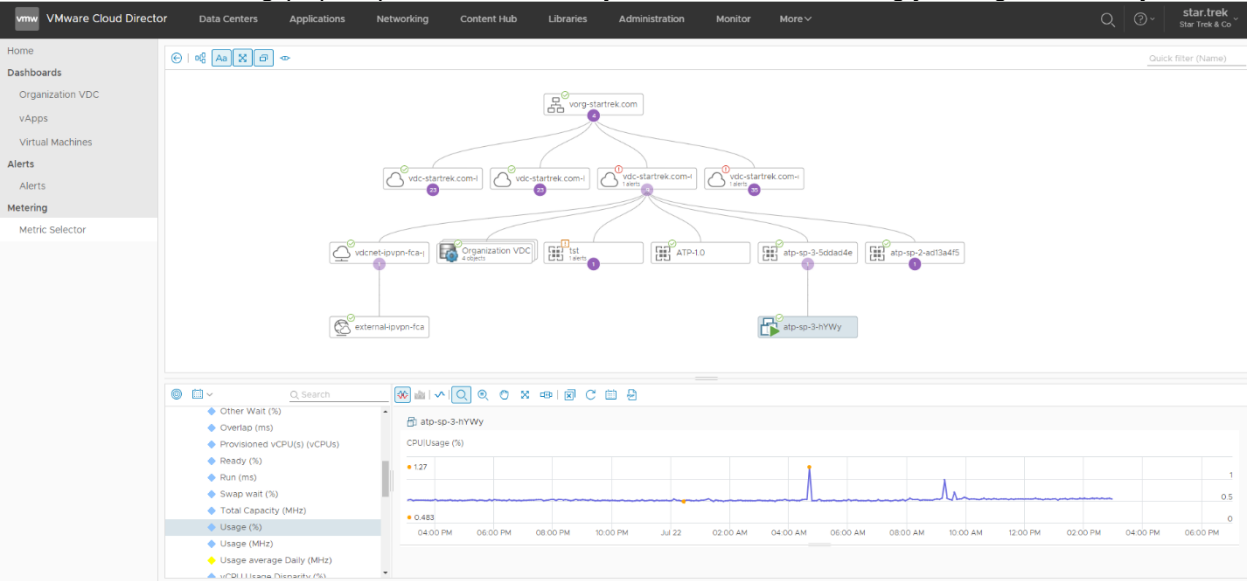
☐	Criticality	Alert	Triggered On	Created On	Status	Alert Type	Importance
☐	★	Organization VDC Storage Policy is running out of storage space	vmstore-cloud-gold-XXC	7/18/24 10:47 AM	Active	Virtualization/Hypervisor	Low (18%)
☐	★	Organization VDC Memory usage reserved is nearing capacity	vdc-startrek.com-01	6/26/24 1:22 PM	Active	Virtualization/Hypervisor	Medium (33%)
☐	★	Organization VDC Memory usage reserved is nearing capacity	vdc-startrek.com-da-02	6/26/24 1:22 PM	Active	Virtualization/Hypervisor	Medium (33%)
☐	★	Organization VDC Storage Policy is running out of storage space	vmstore-cloud-gold-N4	7/18/24 10:47 AM	Active	Virtualization/Hypervisor	Low (18%)
☐	★	vApp is Powered Off	orange-atp-tpi	6/26/24 1:22 PM	Active	Application	Medium (31%)
☐	★	vApp is Powered Off	orange-atp-64940bad-edac-406f-b155-718a3421ae79	6/26/24 1:22 PM	Active	Application	Medium (31%)
☐	★	vApp is Powered Off	ATP-DA2	6/26/24 1:22 PM	Active	Application	Medium (31%)
☐	★	vApp is Powered Off	tst	6/26/24 1:22 PM	Active	Application	Medium (31%)
☐	★	vApp is in Mixed State (One or more vms Powered Off)	ATP-DA	6/26/24 1:22 PM	Active	Application	Medium (34%)

VM metrics review

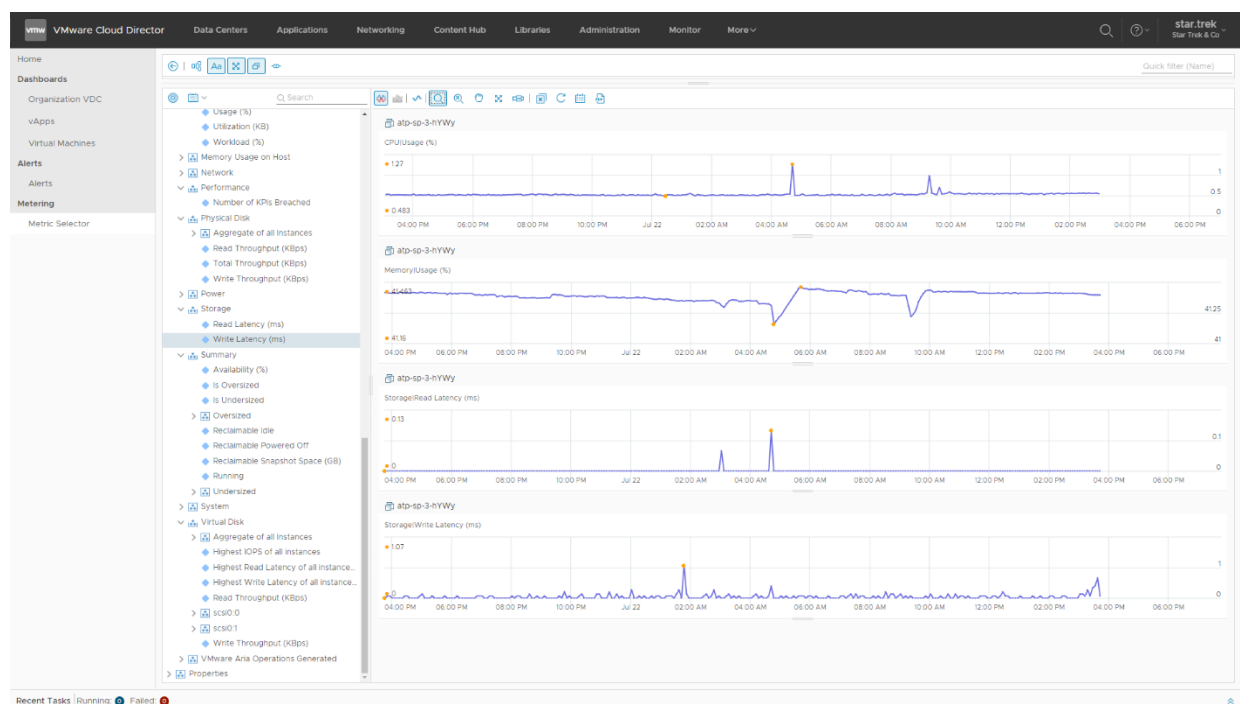
The tree of objects and the metrics corresponding to the selected objects are displayed.



By selecting the desired object on the tree, you can quickly access specific metrics. Double-clicking (expand) reveals nested objects on the tree, allowing you to get to the object of interest:

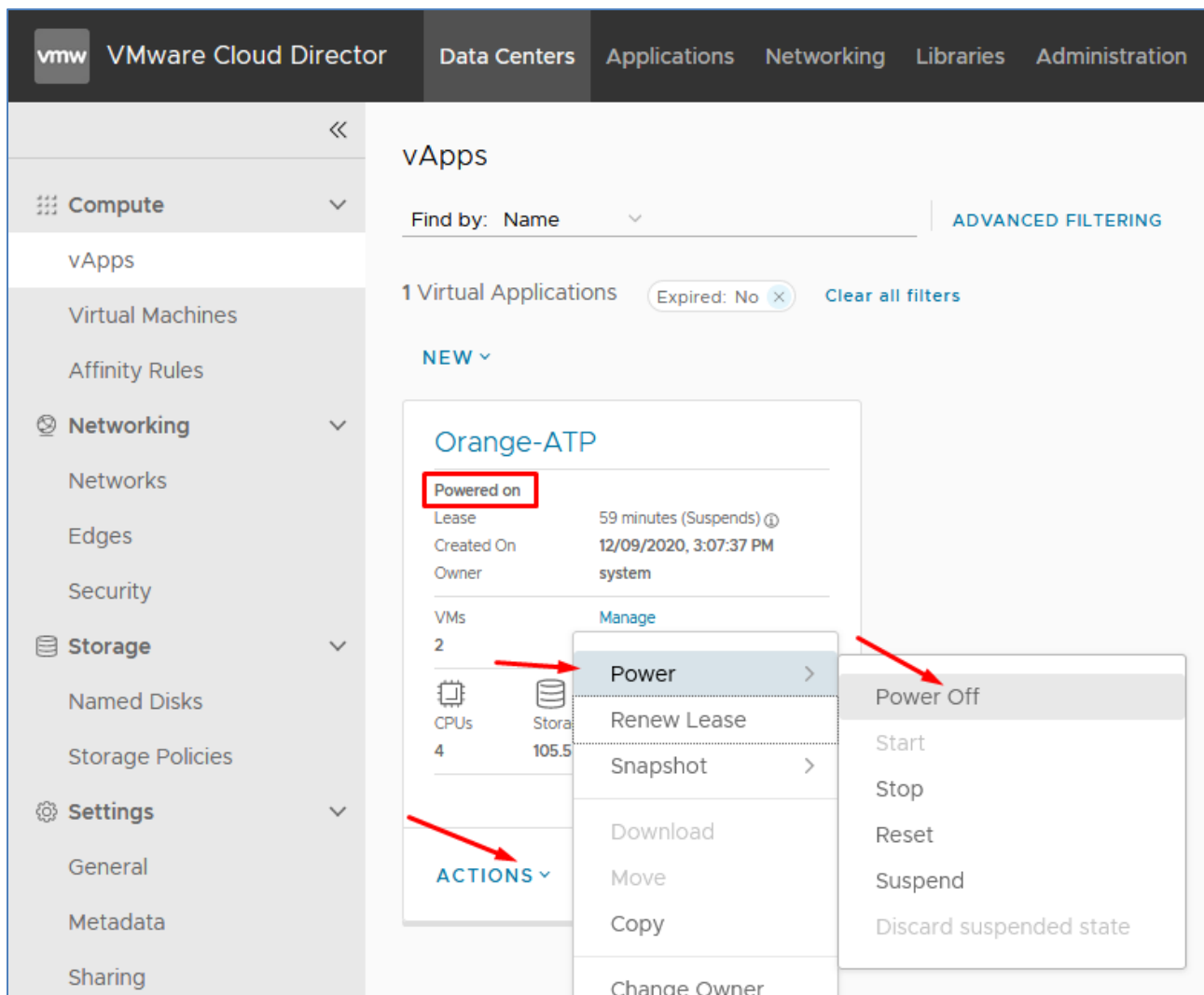


The main types of metrics that affect VM performance are CPU utilization, MEM, and disk subsystem response time:



12.7. Exporting a vApp template from Cloud Director

To export a vApp template (VM), the vApp must first be stopped. Even if all VMs in the vApp are turned off, the vApp itself is considered running until it is intentionally stopped.



After stopping, the Download item will become available

12.8. Installing VMware Tools on a VM

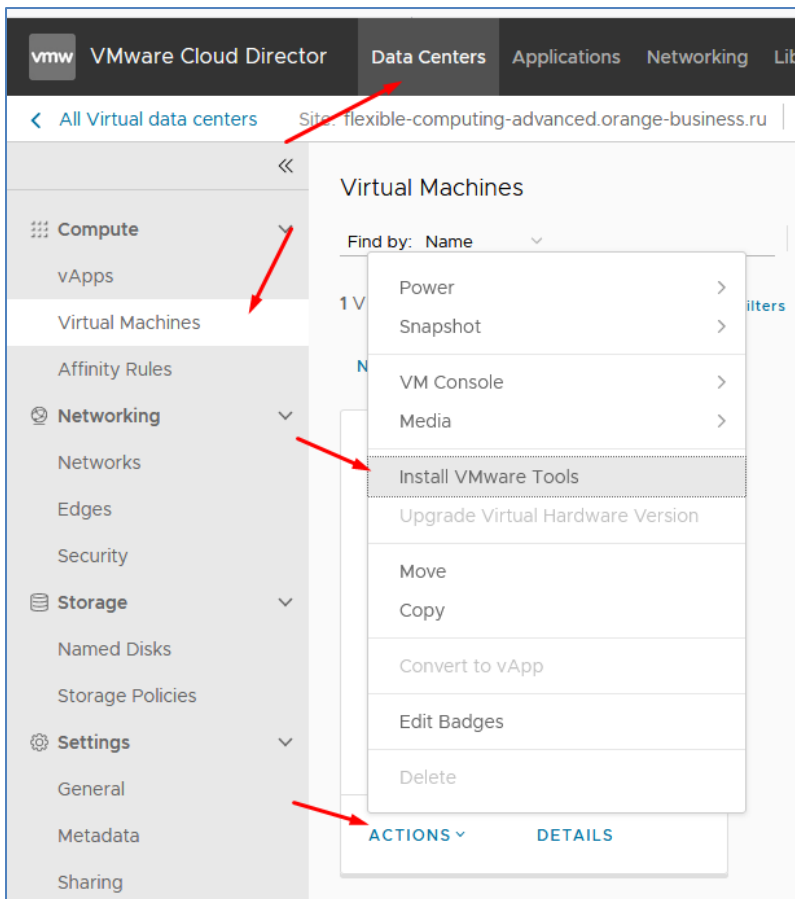
VMware Tools is a set of utilities that improves the performance of the virtual machine's operating system and improves the management of the virtual machine. If the virtual machine does not have this set of utilities installed, the guest operating system will lack some important functions and capabilities for integration with the hypervisor, and there will also be no optimized drivers for virtual devices or power management options (reboot/shutdown) of the guest operating system through VMware management tools.

The installation of VMware Tools on the virtual machine's operating system is within the customer's scope of liability and is mandatory. If a specific operating system is used for which there are no installation instructions or VMware Tools distribution, the customer must contact Orange for consulting and recording of the existence of such VM. If VMware Tools have either not been installed (the installation process is complete, the operating system has been restarted, or the image is mounted) or are not operational (hypervisor has the ability to connect) on the operating system of the virtual machine:

- backup copies of the VM may be more likely to be inconsistent;
- if during the emergency recovery the customer's VM cannot be moved to another hypervisor and thus blocks the recovery efforts, the VM may be restarted without the Customer's approval;
- in the event of an incident at the host or in the DC, Orange does not guarantee the startup of the VM on another host or that restarting will not take an extended period of time.

For up-to-date and detailed instructions, click [here](#).

To mount an ISO image from VMware Tools to a VM, right-click on the VM and select Install VMware Tools. This will mount the ISO image to the VM, after which you need to install it on the OS.



12.9. **Selecting storage type for VM**

The type of storage system used for a VM is set by enabling the necessary policy for disks and for the vm home object (VM metadata). Metadata should use one of the #SYSTEM policies (with or without site linking - as needed).

From the context of the VM, a metadata storage policy is being set:

All Virtual Machines > atp-sp-1

 **atp-sp-1**
Powered on

POWER ONPOWER OFFLAUNCH WEB CONSOLELAUNCH REMOTE CONSOLEALL ACTIONS ▾

General

Security Tags

Hardware

Removable Media

Hard Disks

Compute

NICs

Guest OS Customization

Guest Properties

Sharing

Metadata

Monitor

Tasks

Events

EDIT

Name	atp-sp-1
State	Powered on
Computer Name	atp-sp-1
Description	-
Guest OS	Ubuntu Linux (64-bit)
Storage Policy	#SYSTEM-site1
Boot Firmware	BIOS
Boot Delay	0 Milliseconds
Failed Boot Recovery	Disabled
Enter Boot Setup	Disabled
Virtual Data Center	vdc-startrek.com-01
Owner	system
VMware Tools	12325
Virtual Hardware Version	Hardware Version 18

Edit VM atp-sp-1

General Settings

Name *

atp-sp-1

Computer Name *

atp-sp-1

Description

Storage Policy

#SYSTEM-site1

Operating System

Operating System Family

Linux

Operating System

Ubuntu Linux (64-bit)

Boot Options

Boot Firmware

BIOS

You cannot change this setting while the VM is powered on or suspended.

Boot Delay *

0

To delay the boot operation, specify the time in milliseconds.

Enter Boot Setup

DISCARD

SAVE

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

Enabling policies for VM disks:

vmware

VMware Cloud Director

Data Centers

Applications

Networking

Libraries

Administration

Monitor

More

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

All vApps > ATP-1.0 > orange-atp

orange-atp

Powered on

POWER ON

POWER OFF

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE

ALL ACTIONS

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-platinum	Applicable	LSI Logic Para	0	1

vmstore-cloud-gold

vmstore-cloud-platinum

vmstore-cloud-silver

VM default policy

DISCARD

SAVE

(Use VM default) - means the same policy that is assigned for metadata. The #SYSTEM policies are not designed to accommodate VM disks, the VM will not work with this choice.

12.10. Named Disks

This type of disk is created at the vDC level, not a virtual machine, and can be connected to several VMs at the same time.

This is mainly necessary for cluster solutions.

Configuration options and descriptions are available [in the documentation](#).

Attention: Snapshot creation is not available for VMs using named disks, and as a result, backups at the hypervisor level are not available.

12.11. Hosting of VM in a specific data center

By default, VMs are automatically deployed by the system to a random datacenter based on performance metrics and affinity rules (if any).

It is possible to limit VM placement to one of the data centers. For example, this can be used when creating a fault-tolerant application cluster where the primary set of VMs is bound to one datacenter and the backup set of VMs is bound to a second datacenter.

This parameter must be configured for each VM.

The parameter can be changed at any time without shutting down or interrupting VMs. VMs will be moved using vMotion technology.

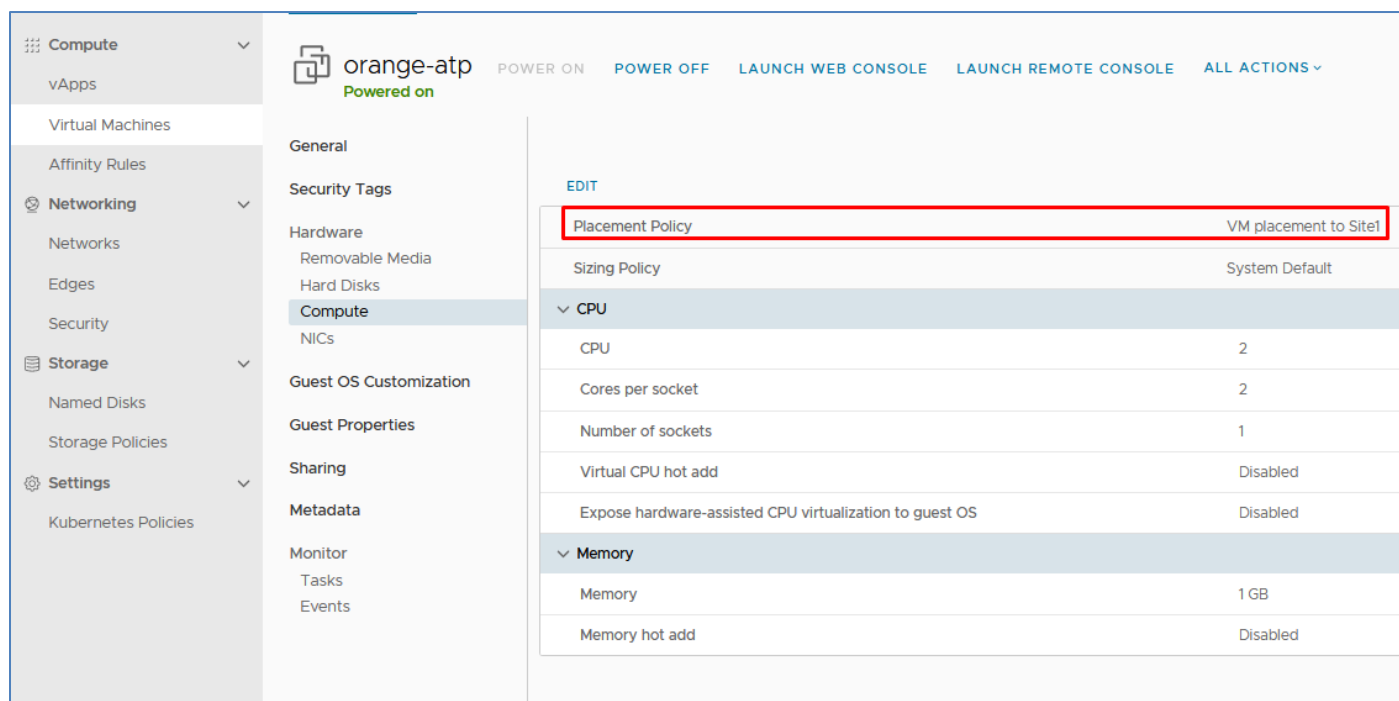
Example 1 - linkage to a data center is not specified:

The screenshot shows the vSphere interface for a virtual machine named 'orange-atp'. The left sidebar contains a navigation tree with categories like Compute, Networking, Storage, and Settings. Under 'Compute', 'Virtual Machines' is selected. The main panel shows the VM's configuration. At the top, there's a breadcrumb 'All Virtual Machines > orange-atp'. Below that, the VM name 'orange-atp' is displayed with a 'Powered on' status. The configuration is divided into sections: General, Security Tags, Hardware, Removable Media, Hard Disks, Compute (selected), Guest OS Customization, Guest Properties, Sharing, Metadata, Monitor, Tasks, and Events. The 'Compute' section is expanded, showing a table of configuration parameters. The 'Placement Policy' is highlighted with a red box and shows a value of '-'. Other parameters include Sizing Policy (System Default), CPU (2 cores), and Memory (1 GB).

EDIT	
Placement Policy	-
Sizing Policy	System Default
▼ CPU	
CPU	2
Cores per socket	2
Number of sockets	1
Virtual CPU hot add	Disabled
Expose hardware-assisted CPU virtualization to guest OS	Disabled
▼ Memory	
Memory	1 GB
Memory hot add	Disabled

Example 2 - linkage to Data Center1 has been established:

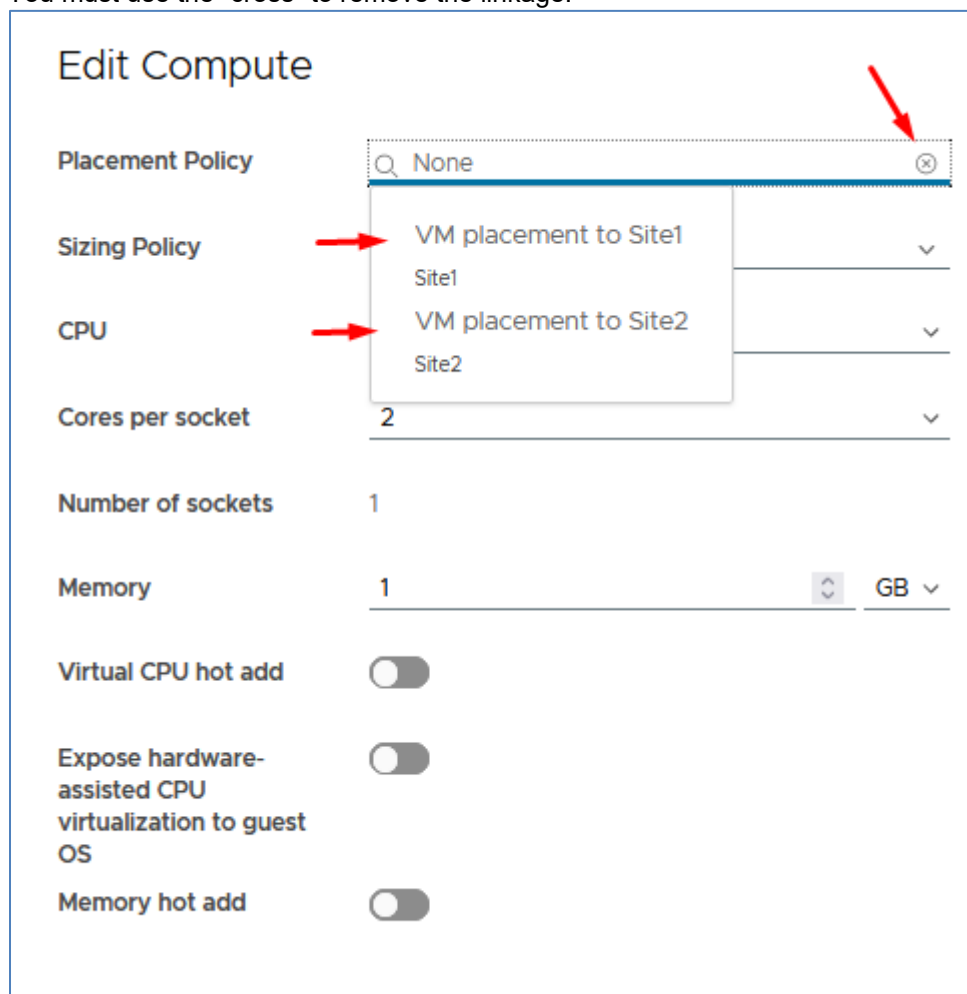
Version 4.1.6 © Orange Business Services, 2024



The screenshot shows the 'orange-atp' virtual machine configuration page. The 'Compute' tab is selected, and the 'Placement Policy' is highlighted with a red box. The 'Placement Policy' is set to 'VM placement to Site1'. The 'Sizing Policy' is set to 'System Default'. The 'CPU' section shows 2 CPU, 2 Cores per socket, 1 Number of sockets, Virtual CPU hot add Disabled, and Expose hardware-assisted CPU virtualization to guest OS Disabled. The 'Memory' section shows 1 GB Memory and Memory hot add Disabled.

Placement Policy	VM placement to Site1
Sizing Policy	System Default
CPU	
CPU	2
Cores per socket	2
Number of sockets	1
Virtual CPU hot add	Disabled
Expose hardware-assisted CPU virtualization to guest OS	Disabled
Memory	
Memory	1 GB
Memory hot add	Disabled

You must use the “cross” to remove the linkage:



The 'Edit Compute' dialog box shows the 'Placement Policy' dropdown menu. The dropdown menu is open, showing 'None', 'VM placement to Site1', and 'Site1'. A red arrow points to the 'cross' icon in the top right corner of the dropdown menu, indicating how to remove the linkage.

Placement Policy	VM placement to Site1
Sizing Policy	System Default
CPU	
CPU	2
Cores per socket	2
Number of sockets	1
Memory	1 GB
Virtual CPU hot add	Disabled
Expose hardware-assisted CPU virtualization to guest OS	Disabled
Memory hot add	Disabled

12.12. Affinity and anti-affinity rules for VMs

Affinity rules is a rule for co-locating VMs on the same hypervisor, that is, on the same physical server. It can be used, for example, if minimal network latency between VMs is required for them to work together.

Anti-affinity rules is the rule of placing VMs on different hypervisors. It is usually used in application-level clustering to avoid the situation when two nodes will run on the same physical server.

vmw VMware Cloud Director

Data CentersApplicationsNetworkingContent HubLibrariesAdministration

< All Virtual data centers

Site: flexible-computing-advanced.orange-business.ru | Organization: vorg-startrek.com | Data center: vdc-startrek.com-01

Compute

vApps

Virtual Machines

Affinity Rules

Networking

Networks

Edges

Security

Storage

Named Disks

Storage Policies

Settings

Kubernetes Policies

Affinity Rules

NEW

Name	Enabled
------	---------

Manage Columns

Anti-Affinity Rules

NEW

Name	Enabled
------	---------

Manage Columns

Create Affinity Rule

×

Rule Metadata

Name *

TestAff

Enabled

☒

Required

☐

VMs in Rule

Show selected

☐	Name	vApp Name
☐	atp-sp-1	atp-sp-1-af4abba0-c653-46d6-b793-e0a0112ef2f1
☐	atp-sp-2	atp-sp-2-ad13a4f5-616a-4272-9c0d-9e0aafb6553a
☐	atp-sp-3	atp-sp-3-5ddad4e0-59d3-4158-99dc-506129e8e4fc

1 - 3 of 3 VM(s)

DISCARD

SAVE

It is not recommended to set the “Required” option, because if for some reason the rule cannot be satisfied - the VM will not be enabled.

13. Known Issues

Description of the problem	Solution	KB VMware
Network connectivity is lost in Windows Server 2012 and higher. Access is restored after rebooting or enabling and disabling the network interface. <i>Note: Similar problems have been observed in Windows 7 and Server 2008R2.</i>	Use the VMXNET3 vNIC type	KB 2109922
Missing/incorrect mouse operation during Windows installation and after it	1. When installing, use VMRC instead of the web console 2. Install VMware Tools using the keyboard	-