Business Services

Flexible Computing Advanced

User Guide

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 vCloud Director Tenant Portal Guide.

To ensure the safety and functionality of the Platform, Orange periodically installs patches 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 vCloud Director version 10.2.0.17008054.

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)	3.18	
Connecting external network devices or servers located in the iX (not available in the event of an iX failure)	3.19	
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 several DCs	3.3	
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
Cisco CSR1000v virtual router	3.17	
Protection against DDoS attacks	3.13	
Storage		
Silver (located in iX, not available in the event of failure in iX)	3.5	12.8
Gold (located in iX, not available in the event of failure in iX)		
Platinum (located in iX, not available in the event of failure in iX)		
Platinum DR (synchronous replication)		
Backup and archiving		
Backing up to an array in iX	3.6	
Backing up to arrays in two DCs (asynchronous replication)		
Archiving and restoring to/from tape	3.7	
Offsite tape storage		

3. Architecture, options, features and recommendations

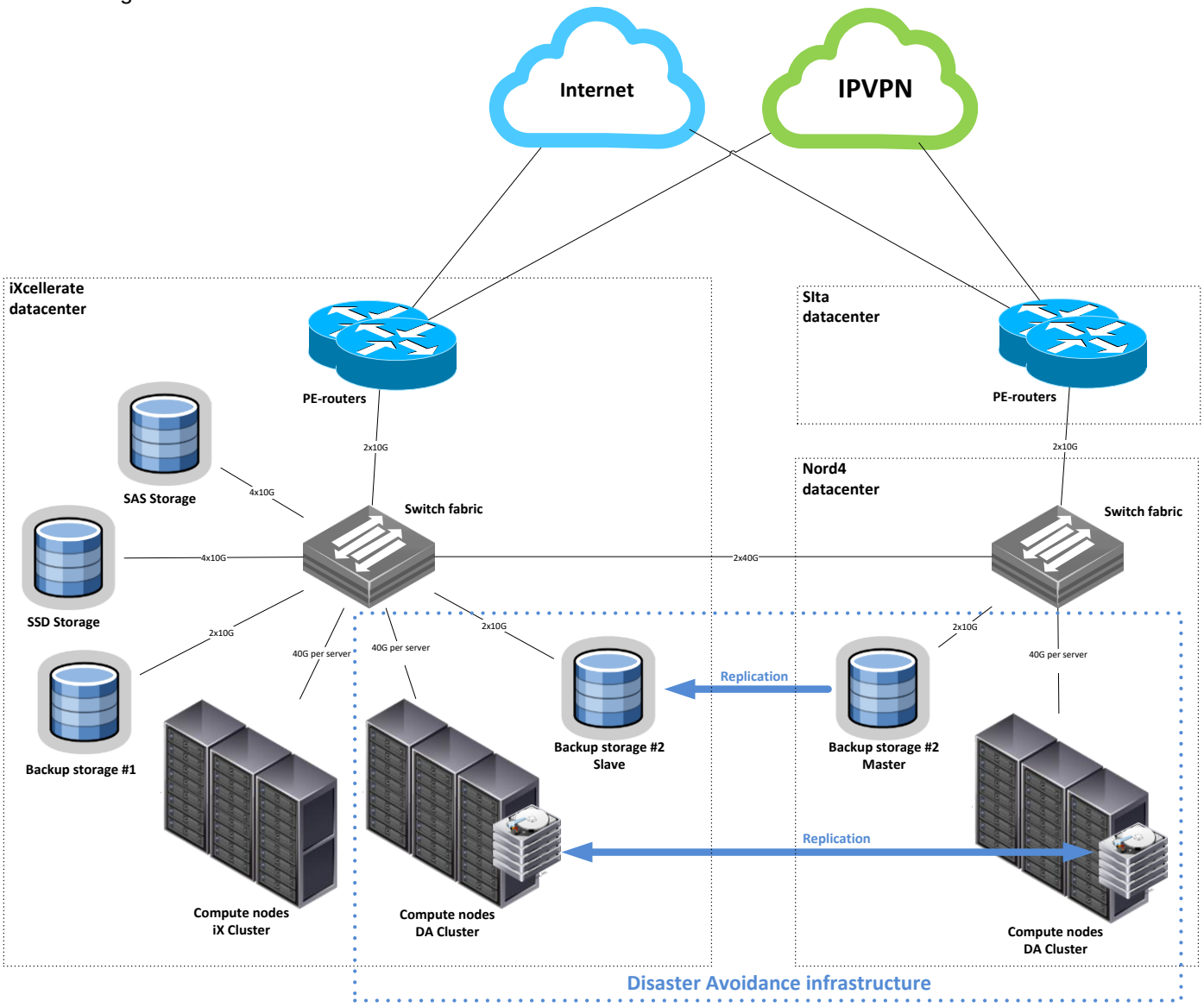
3.1. Architecture overview

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:

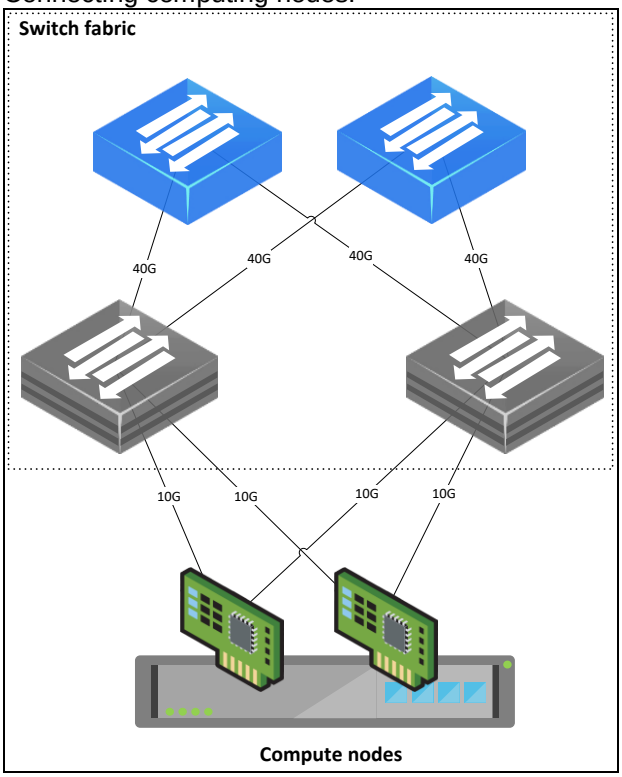
- The main data center is IXcellerate Moscow One (Tier 3+), 33G Altufevskoe Shosse, Moscow;
- The secondary data center is DataLine Nord4 (Tier 3), 41 Korovinskoe Shosse, Moscow;
- Only enterprise-class equipment and software from market leaders is used: HPE, Juniper, Huawei, VMware, Netapp, Veeam, CheckPoint, ADVA;
- Valid service contracts for all hardware and software;
- The expertise of the engineers is constantly updated and refreshed;

- DWDM communication channels between data centers (hereinafter referred to as DCs) 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: 0.3-0.4ms when measuring VM<>VM, including all network levels;
- 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, IPVPN) are provided using different routes from two independent PE routers in different DCs;
- All traditional storage systems have two controllers and RAID-based disk redundancy. The SDS storage system of the DA cluster stores a full copy of the data in the secondary DC in addition to backing up disks inside the main DC (when ordering the DA option);
- 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 iXcellerate cluster:

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

Characteristics of computing nodes of the DA cluster:

CPU	2xE5-2698 v4 @ 2.20GHz (20C, Turbo Boost 3.6GHz, Broadwell)
RAM	512-704 GB

The disk capacity of the Silver, Gold and Platinum levels differs in IOPS per 1 TB: 112, 420 and 3,000, respectively. The actual IOPS value depends on the load parameters and is usually higher than those indicated above. When independently testing the performance of the disk subsystem, you should take into account that the Platform uses optimization and caching technologies that increase the speed of real applications, therefore it is recommended to use test packages that emulate a real load and run them for at least 30 minutes.

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 (for this, you need to inform Orange about the VM lists to be placed in each DC; VMs that are not on the lists are placed randomly).

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, Zerto or Veeam Cloud Connect).

3.5. Storage Subsystem

It is possible to use different types of disk capacity for the same Virtual Data Center and the same VM.
If the disaster avoidance option is ordered, virtual machines are located on an All-Flash DSS distributed between two

DCs (synchronous replication), thus ensuring the availability of data in the event of a disaster. However, it is also possible to order Silver and Gold level disk space with the following restrictions:

- DSSs for Silver and Gold levels are located in the iXcellerate DC, and they only provide fault tolerance within the limits of this DC. I.e., in the event of a disaster in the iXcellerate DC, Silver and Gold level disk space will not be available from the second DC. There will be access in the event of a disaster in the second DC;
- Silver and Gold level disk space can be added only as a second VM disk and subsequent VM disks;
- Automatic restarting of VMs containing Silver and Gold level disks in the event of a disaster in the iXcellerate DC is not guaranteed, Orange engineers may need to intervene. To eliminate this risk, it is recommended to create the necessary number of VMs with Silver and Gold levels, provide access to the disks through CIFS/NFS, and access them from productive VMs via the network.

In addition to the disk space ordered (Silver, Gold and Platinum levels, but not Platinum-DA), additional disk space is allocated for each type for the swap of the Customer's VM based on the total amount of RAM that has been ordered and added by Orange to each of the types ordered. The vCloud Director Portal will show the total amount of allocated disk space (specified in the Service Order Form + added by Orange) and the total amount of disk space consumed. VMware vCloud Director calculates the consumption of disk space according to the following formula (separately for each type):
Total amount of disk space consumed = amount of hard drive space allocated for the Customer's VM (the sum of VM disk capacities) + memory size (RAM) allocated for all Customer VMs + Templates and ISO images + VMs service files (metadata) + Snapshots.
The use of space on the hard drive above that indicated in the Service Order Form can lead to improper functioning of the Customer's vDC, and subsequently, the failure of all applications.

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 (BETA)

Note: This functionality is undergoing testing and is available upon request.

A self-service backup is available on the Veeam Enterprise Manager self-service portal.
This option is not compatible with Orange's tape and disk backups.

3.9. Dedicated GHz and vCPUs

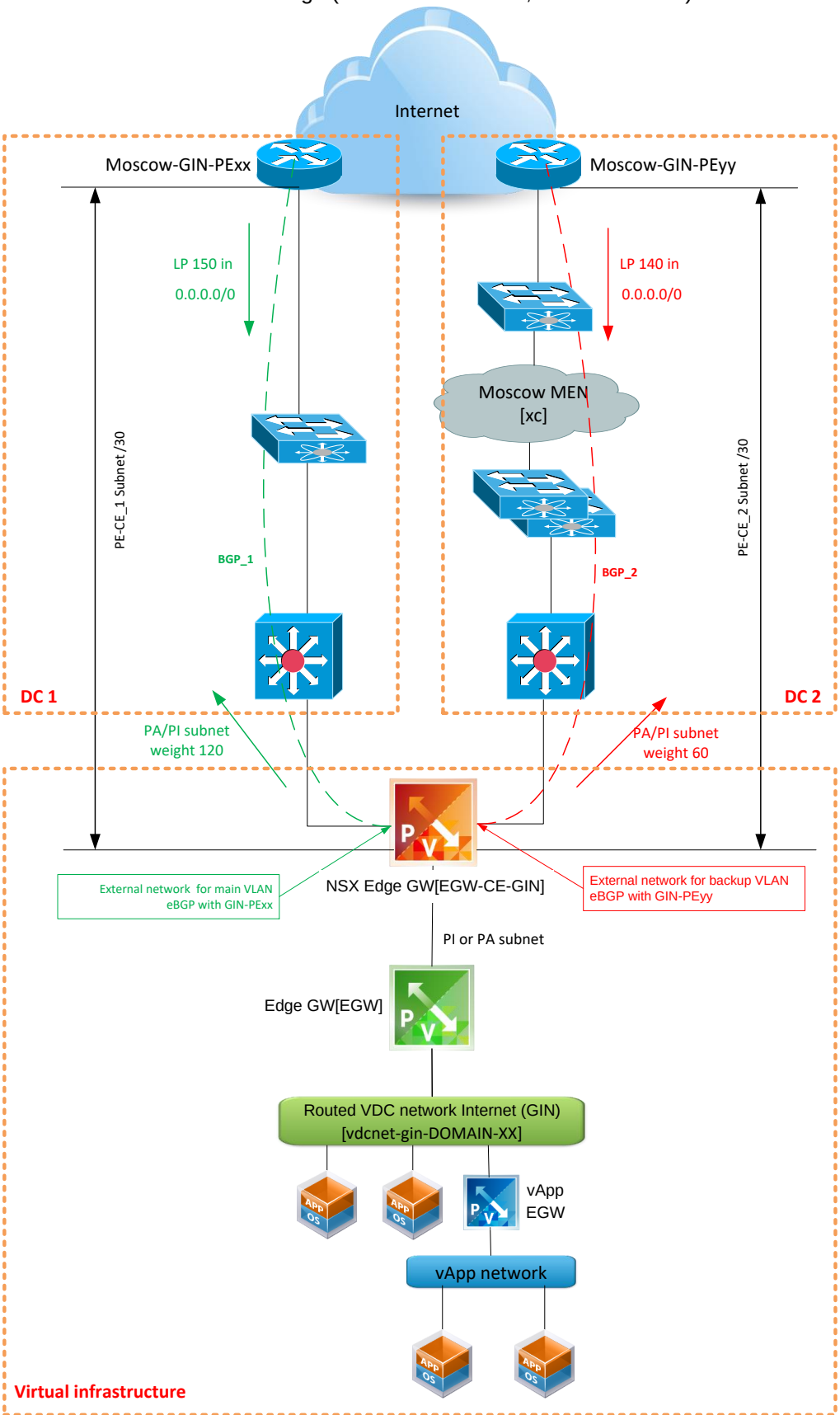
As part of the FCA service, a virtual Data Center is created for the Customer with a set of computing resources as delineated on the signed Service Order Form. If you are allocating processor power, you should pay attention to the difference between the allocated processor power and the number of cores (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 2.2GHz or 2.5GHz. Let's take 2.5GHz to make our further calculations.
If all vCPUs are using full power: 48 * 2.5 = 120GHz. 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: 48GHz / 2.5GHz = 19.2 vCPU, i.e. 19 cores can be configured on a VM without getting limited.

3.10. Fault-tolerant access to Internet and IPVPN networks

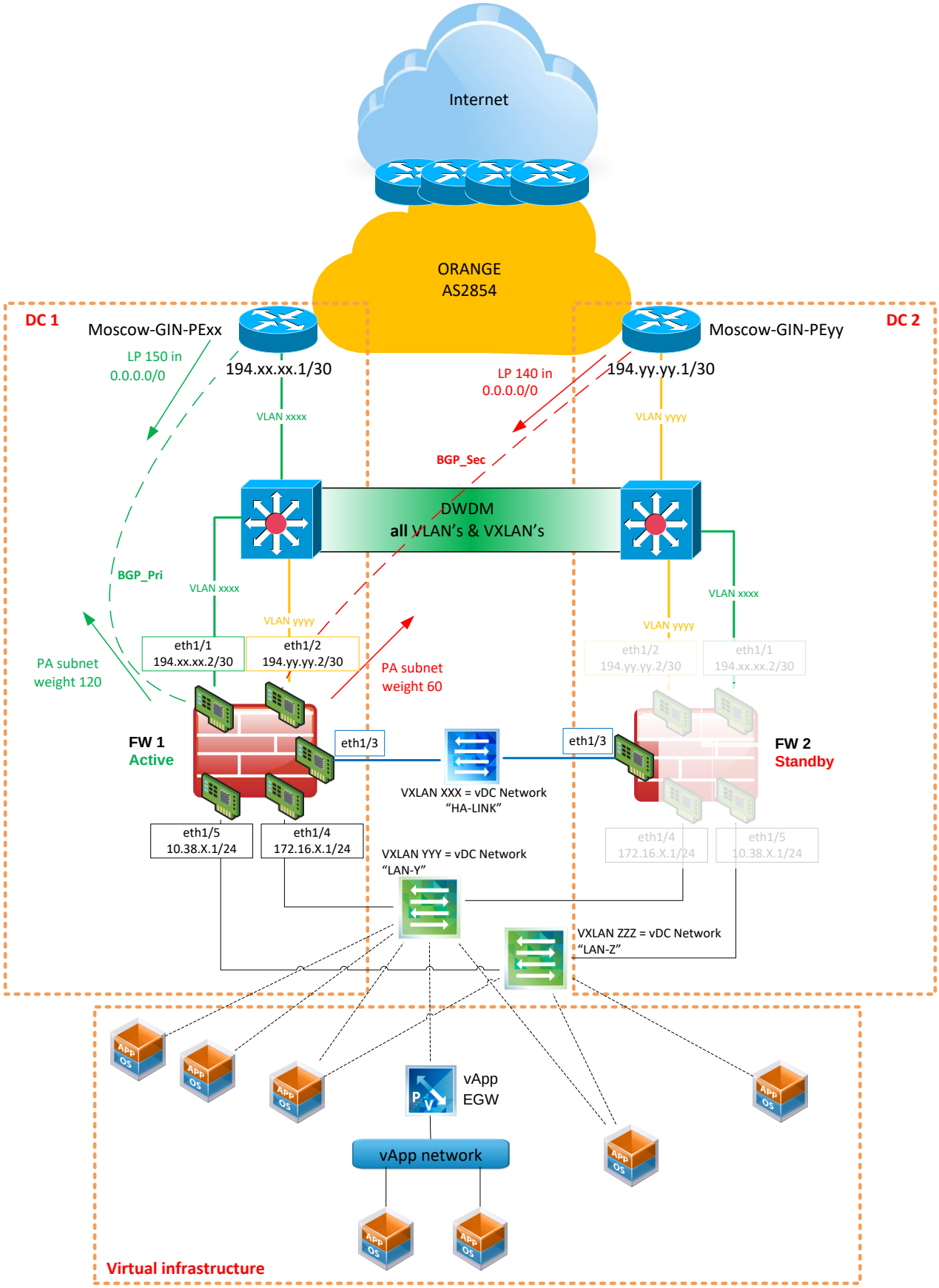
All external network connections are reserved at the levels of physical connections, physical equipment, MEN network, PE-routers and are organized through two data centers. At the same time, it does not matter which route (through which data center) traffic is currently flowing - for virtual machines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

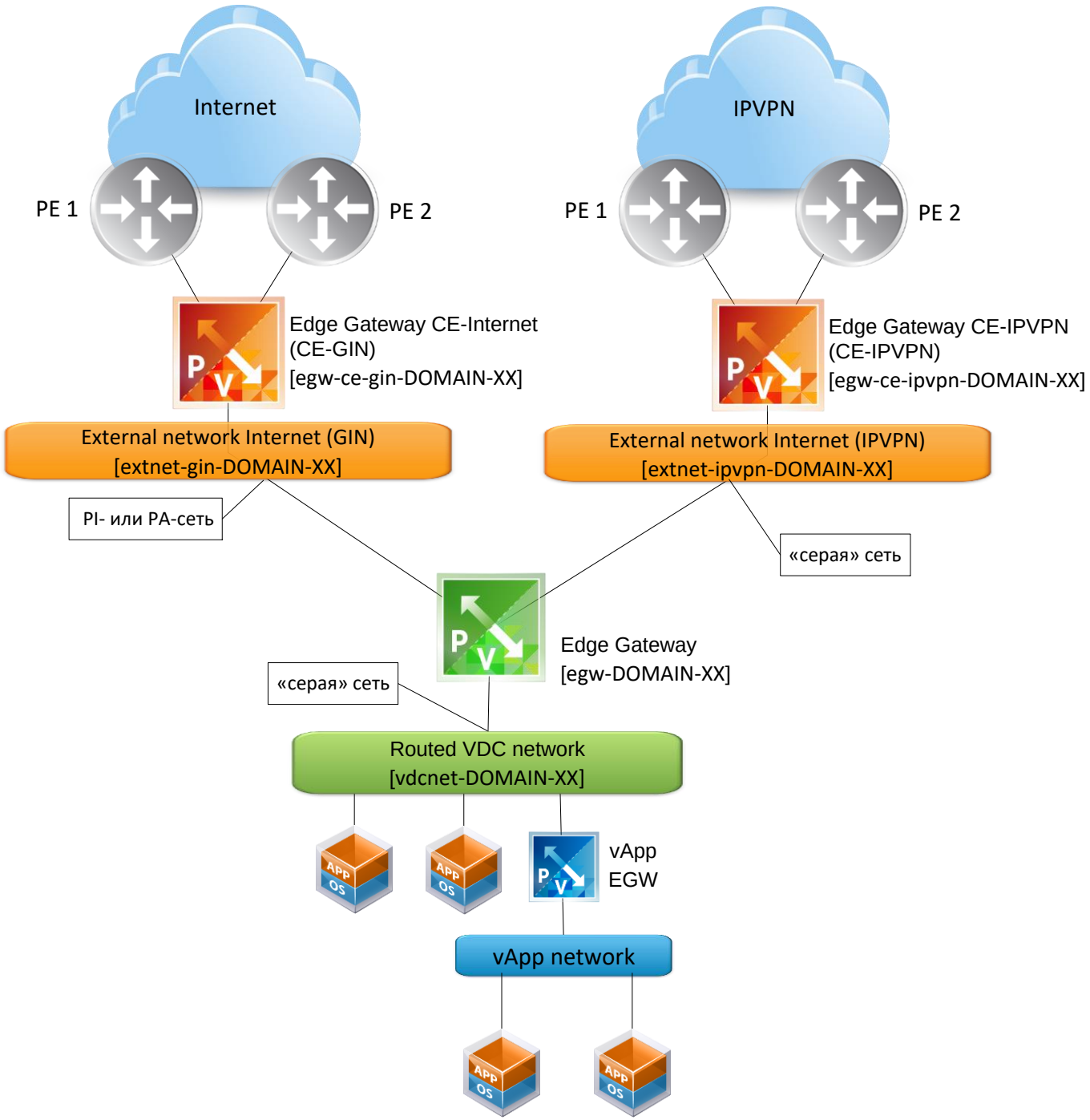


3.11. VMware NSX Edge

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

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 IPVPN. The configuration of these parameters lies within Orange's area of responsibility;
- EGW is fully available for the customer to manage from the vCloud 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 IPVPN network Edge Gateway CE-IPVPN (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. If necessary, the

EGW CE-IPVPN can be replaced with the Cisco CSR1000v (see 3.17).

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-IPVPN (if the IPVPN 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.

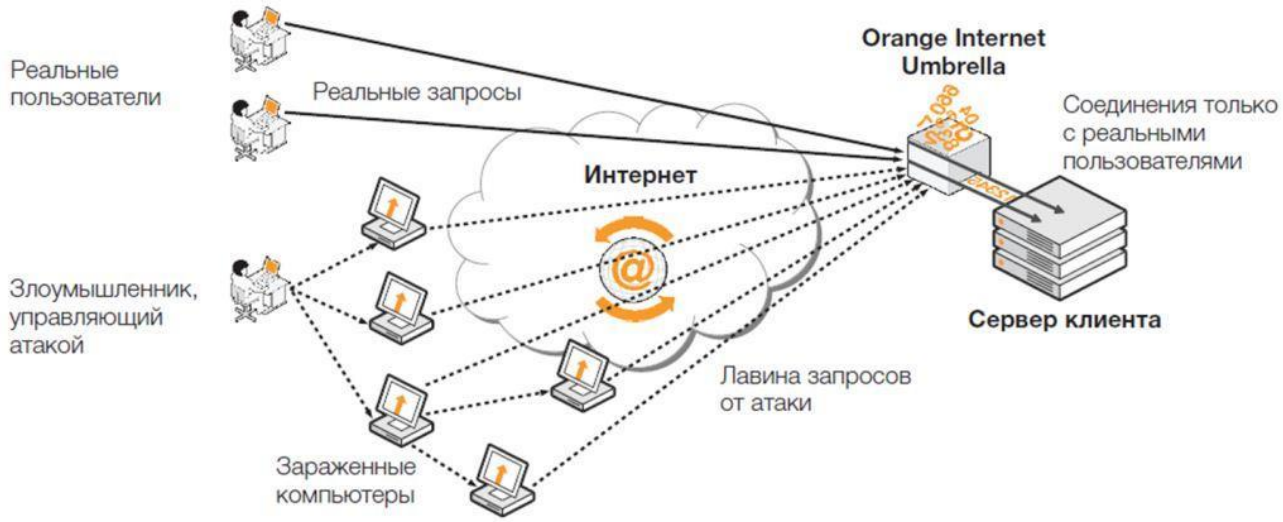
Estimated time parameters (the data is based on the logic of the technologies, their configuration and Orange tests):

Scenario	Access interruption	Time, seconds
Failover from the main Internet or IPVPN channel to the backup one	Yes	15 *
Regular switching (maintenance) from the main Internet or IPVPN channel to the backup one	Yes	15 *
Switch back to main Internet or IPVPN 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 Arbor 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 standard*;
- Microsoft Windows SQL Server standard*;

* 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:

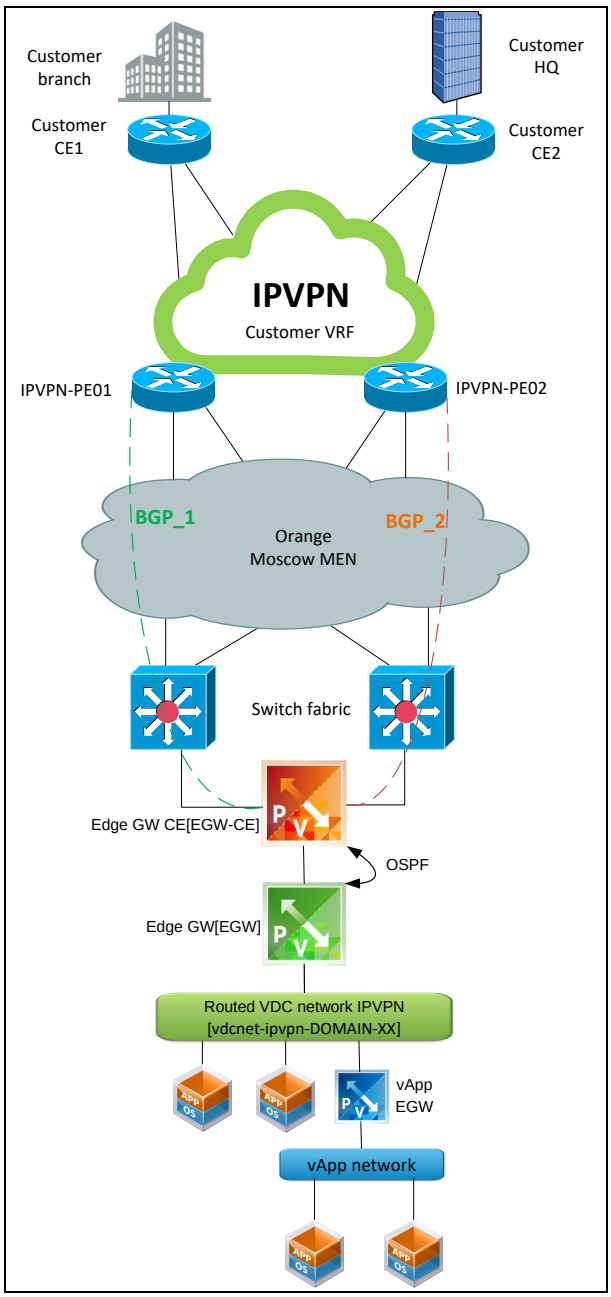
- Check that the TCP1688 port is open on the EGW and accessible from the Internet
- Check that the time in the VM is correct!
- Set IP KMS:
  slmgr -skms 194.84.17.201:1688
- Enable online:
  slmgr.vbs /ato
- Check activation:
  slmgr /dlv

* 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:

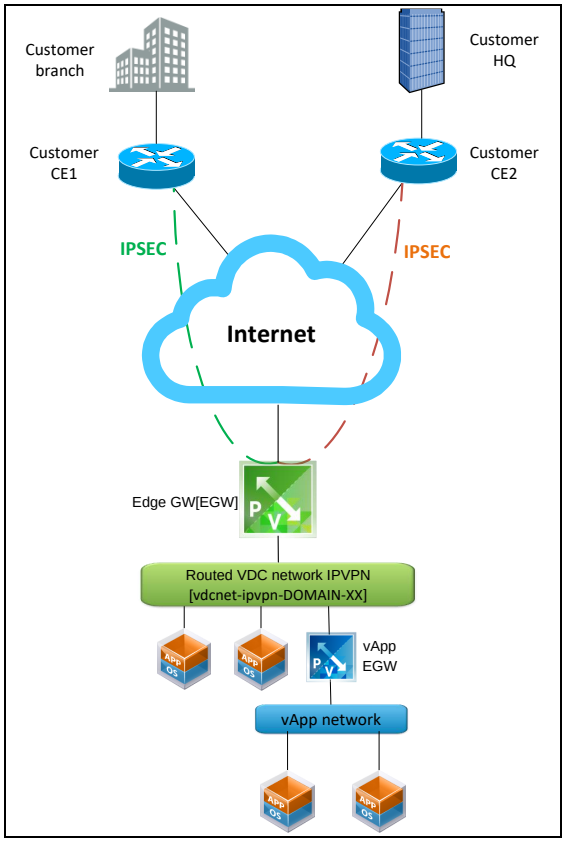
1. Using the IPVPN Orange network.



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 IPVPN
- Enabling fault-tolerant connections from the customer's network
- Optional SLA
- Channel performance – Orange
- Optional connection of remote sites to the IPVPN network through the Internet VPN service (IPSEC to IPVPN 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. Cisco CSR1000v virtual router

Cisco CSR1000v can be used as a virtual router in vDC in addition to, or replacing, Edge and Edge-CE. This configuration is non-standard and is being developed in collaboration with Orange. Cisco CSR1000v can be managed by the customer independently or by Orange (Managed Router service). Orange can provide licenses for a CSR of the desired level of functionality and performance.
More information on CSR is available on the Cisco website.

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

To ensure passthrough of external USB devices (as a rule, these are hardware USB keys for software protection), Digi equipment is used:

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

Each of the USB ports is linked to a VM (several ports can be linked to one VM).
A separate Digi device is installed for each customer.
It should be noted that at present, forwarding keys to virtual machines is only possible for MS Windows guest operating systems. This limitation is due to the fact that USB-to-IP device manufacturers do not provide drivers for Linux OS.
It is also not recommended to use such devices to connect high-speed USB devices such as external HDDs, flash drives, etc.

3.19. Connecting external network devices / servers located in the iX

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 iXcellerate DC (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 installed in the iX.

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 MM LC duplex optical cable to the customer's equipment. *This is not a standard option, additional fine tuning is required.*

4. Main elements of VMware vCloud Director

Virtual organization (organization, vOrg) is the top-most element in the hierarchy of vCloud 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, vApp containers, 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 container that hosts virtual machines. It can be created empty or with virtual machines already inside. Containers 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. vCloud 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-IPVPN	egw-ce-ipvpn-DOMAIN-XX	egw-ipvpn-startrek.com-01
Edge Gateway (managed by customer)	egw-DOMAIN-XX	egw-startrek.com-01
Routed VDC network Internet (GIN)	vdcnet-gin-DOMAIN-XX	vdcnet-gin-startrek.com-01
Routed VDC network IPVPN	vdcnet-ipvpn-DOMAIN-XX	vdcnet-ipvpn-startrek.com-01
Internal VDC network	vdcnet-DOMAIN-XX	vdcnet-startrek.com-01
Direct connected VDC network L2VPN	vdcnet-l2vpn-DOMAIN-XX	vdcnet-l2vpn-startrek.com-01
Distributed Port Group CE-Internet (CE-GIN)	dpg-ce-gin-DOMAIN	dpg-ce-gin-startrek.com
Distributed Port Group CE-IPVPN (CE-IPVPN)	dpg-ce-ipvpn-DOMAIN	dpg-ce-ipvpn-startrek.com
Distributed Port Group Internet (GIN)	dpg-gin-DOMAIN-VID	dpg-gin-startrek.com-2925
Distributed Port Group Internet (IPVPN)	dpg-ipvpn-DOMAIN-VID	dpg-ipvpn-startrek.com-2924

Distributed Port Group Internet (L2VPN)	dpg-l2vpn-DOMAIN-VID	dpg-l2vpn-startrek.com-2999
External network Internet (GIN)	extnet-gin-DOMAIN-XX	extnet-gin-startrek.com-01
External network IPVPN	extnet-ipvpn-DOMAIN-VID	extnet-ipvpn-startrek.com-2924
External network L2VPN	extnet-l2vpn-DOMAIN-VID	extnet-l2vpn-startrek.com-2999
Chief administrator of the organization	adm_DOMAIN	adm_startrek.com

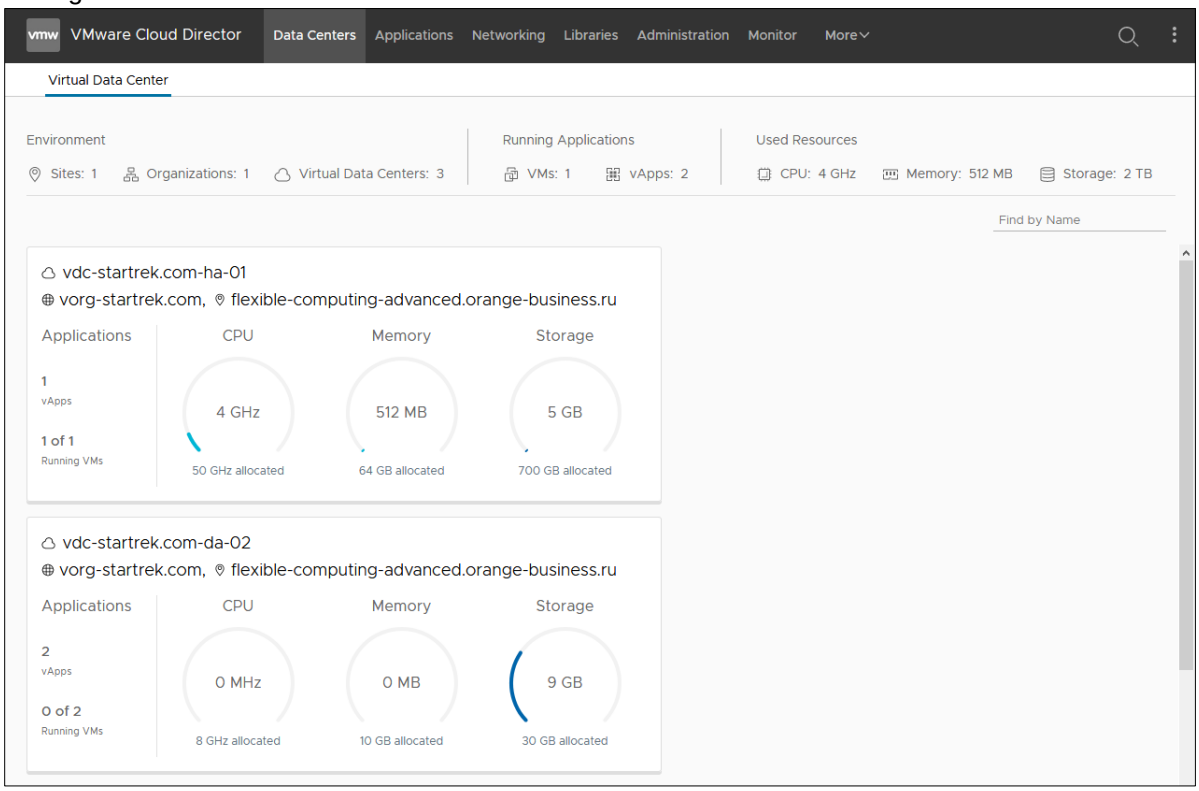
5. Login to the virtual data center

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, two web interfaces for management are 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/**
- The old FLASH-based interface is no longer available!

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

- If you use SSL inspection when accessing the Internet, or overwrite root certificates (for example, through AD policies), the remote VM console and the function for loading images/vApps may not work.
  To solve this problem, you need to go to https://proxy.orange-business.ru/ through the same browser and manually confirm your trust in the certificate.

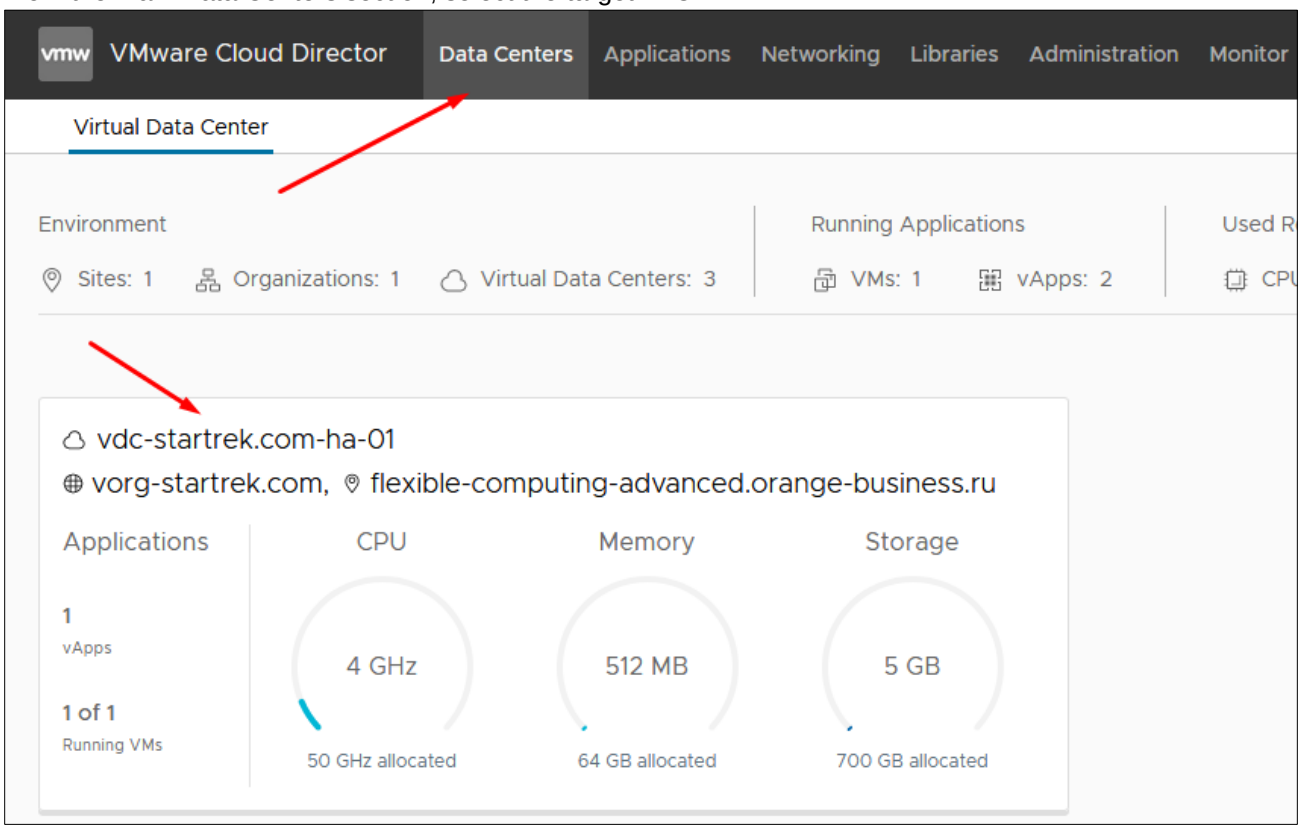
7. Checking vDC resource availability and network connectivity

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

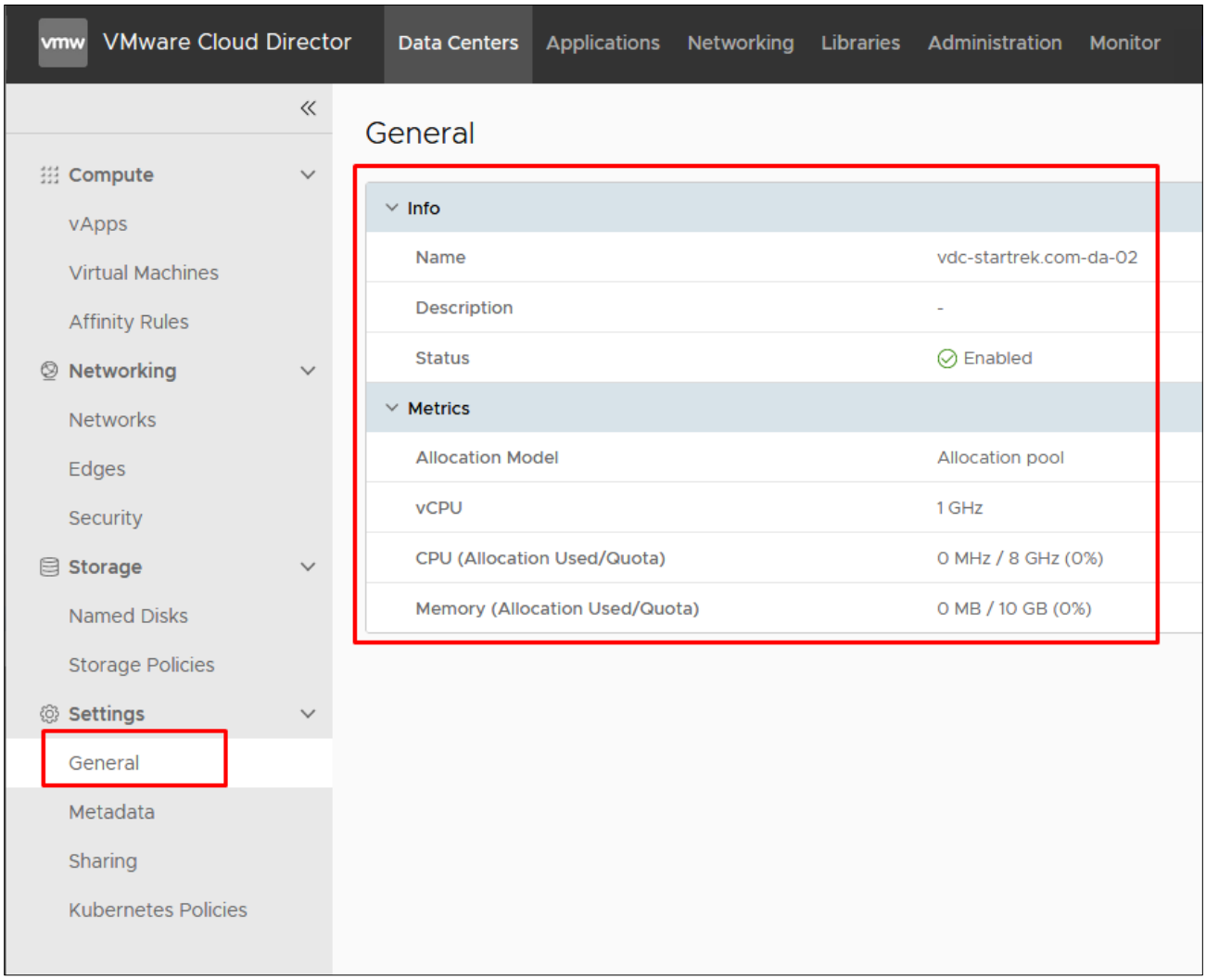
For this, the pre-configured Orange-ATP vApp template is used. We recommend that you repeat the check yourself.

7.1. Checking resource availability

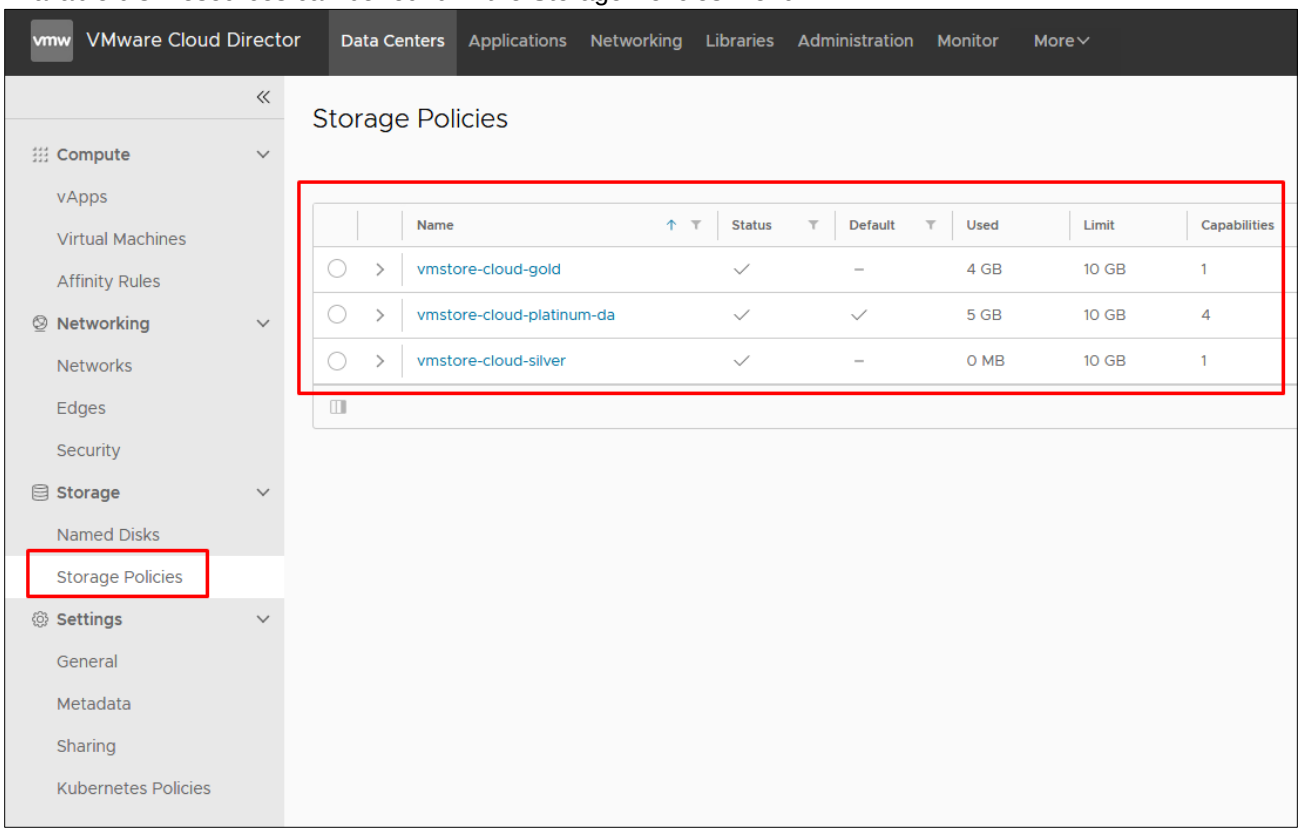
From the main Data Centers section, select the target vDC:



On the left in the General menu:

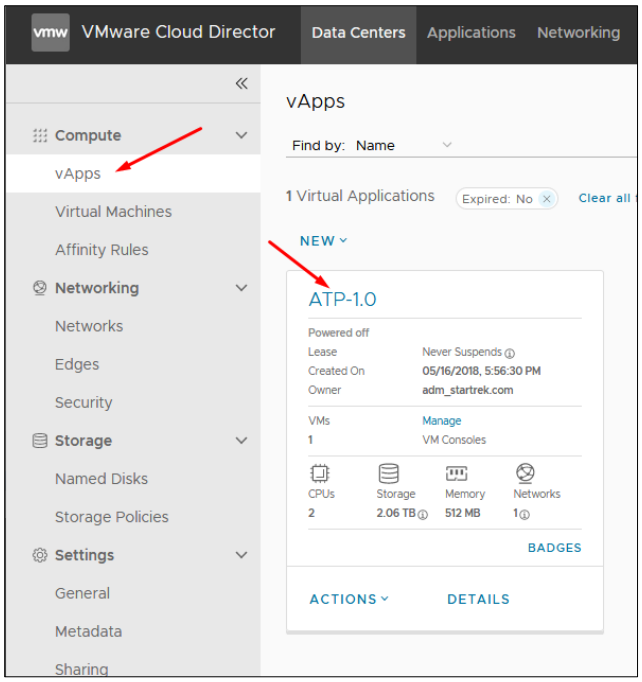


Available disk resources can be found in the Storage Policies menu:

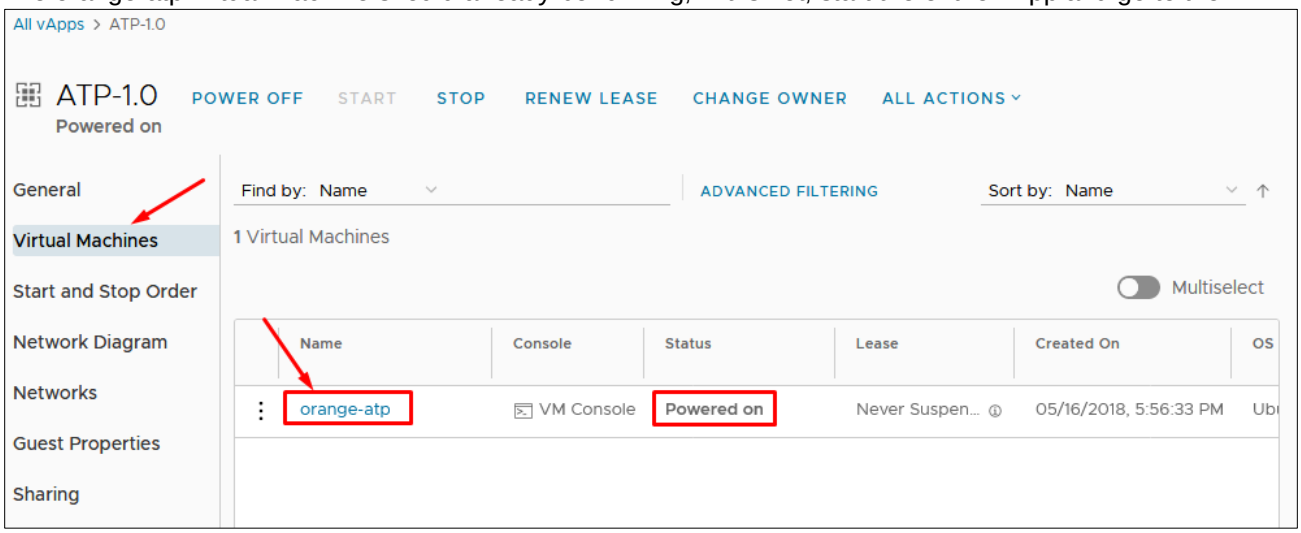


7.2. Checking network resources

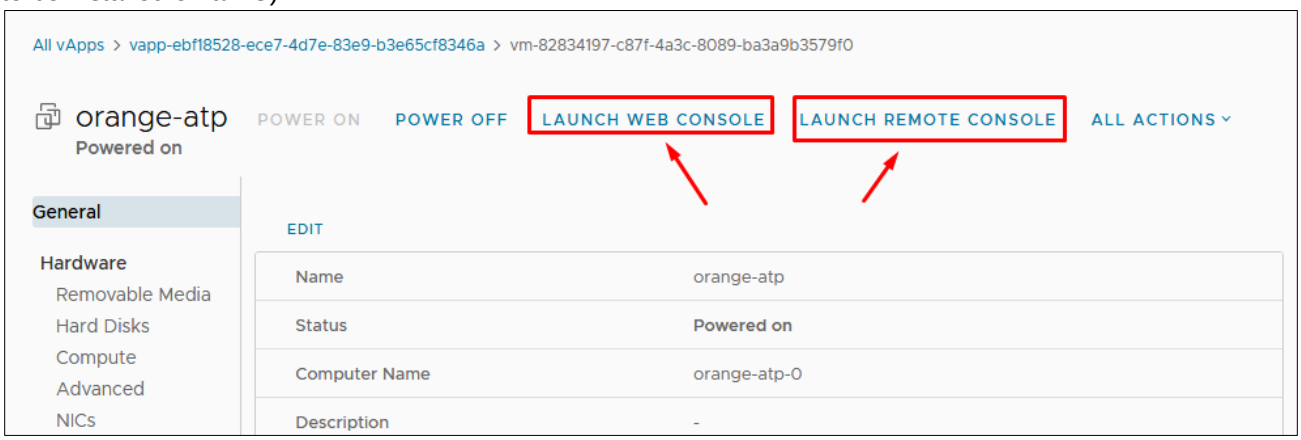
In the Data Centers section, select vDC, then select vApps from the menu on the left and go to the test vApp:



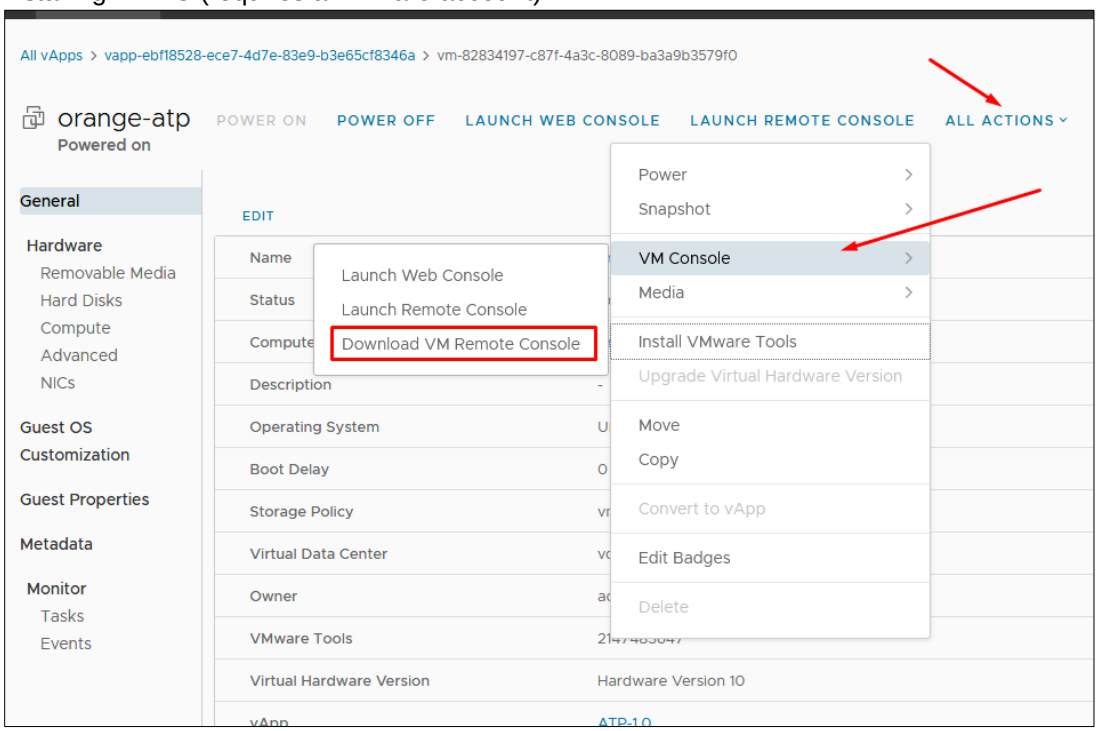
The orange-atp virtual machine should already be running, if it is not, start the entire vApp and go to the VM:



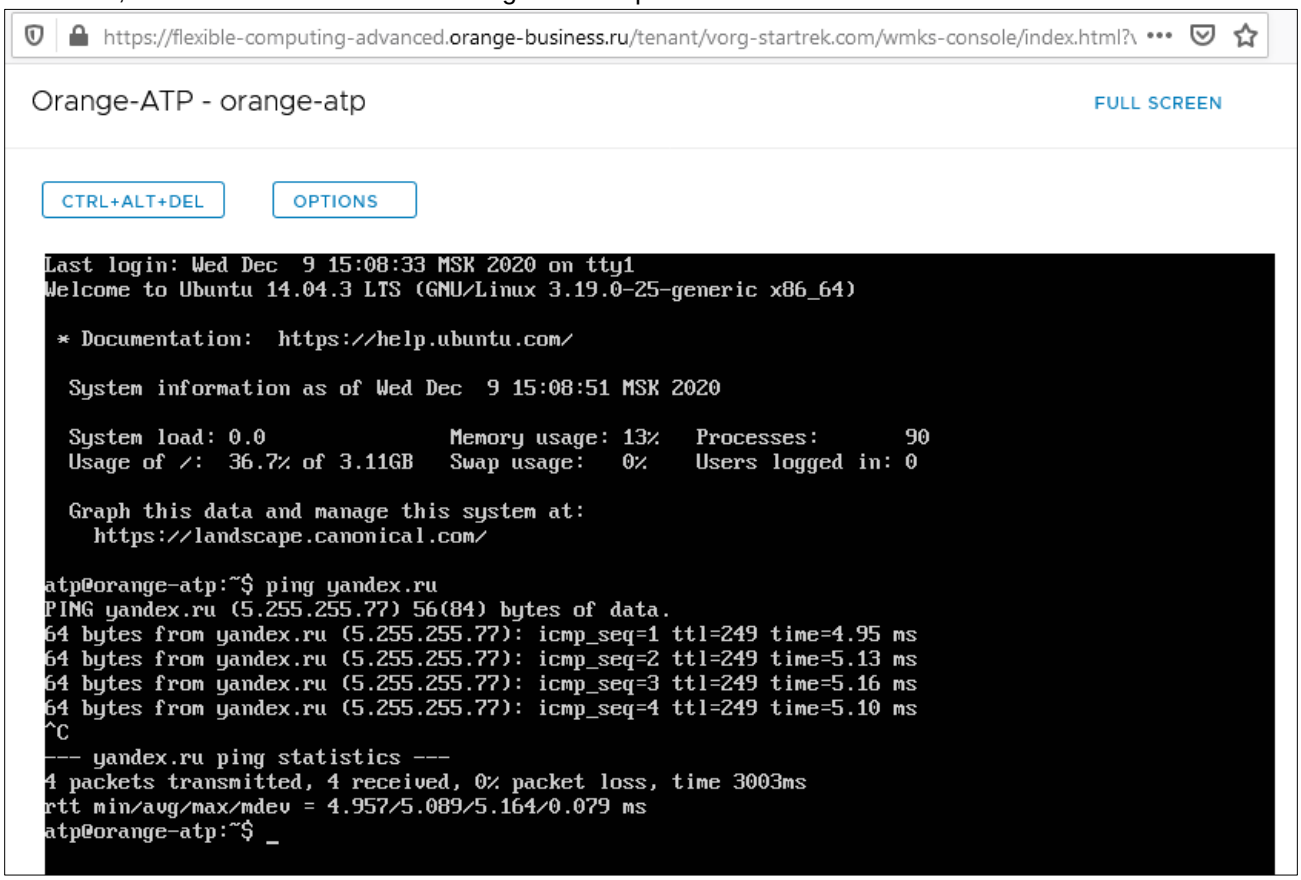
To access the virtual machine console, you can use the web console or VMRC (recommended, but it requires the client to be installed on a PC):



Installing VMRC (requires a VMware account):



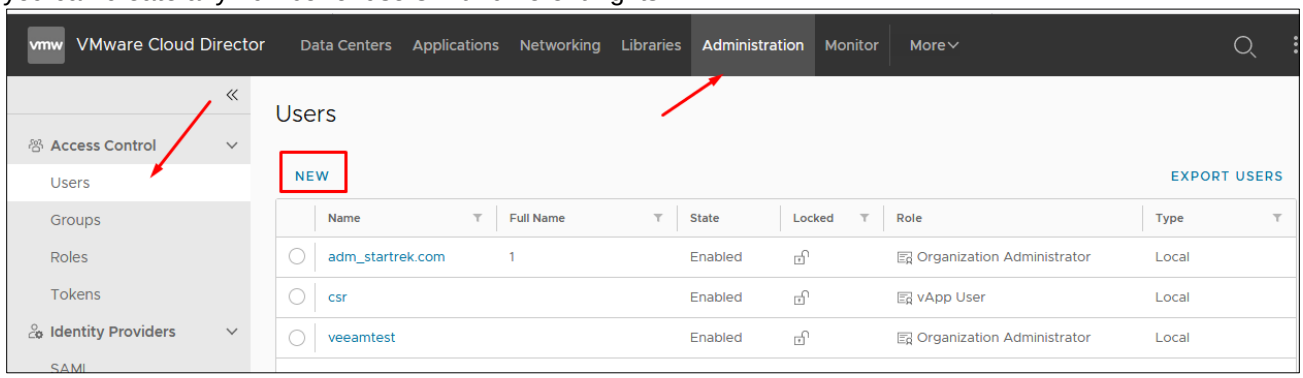
VMs from this vApp automatically get included in the OS and receive network settings using VMware Tools. Now you should check the availability of networks. As an example, for the Internet this can be done with the "ping yandex.ru" command, as a result of which the following ICMP responses should be received:



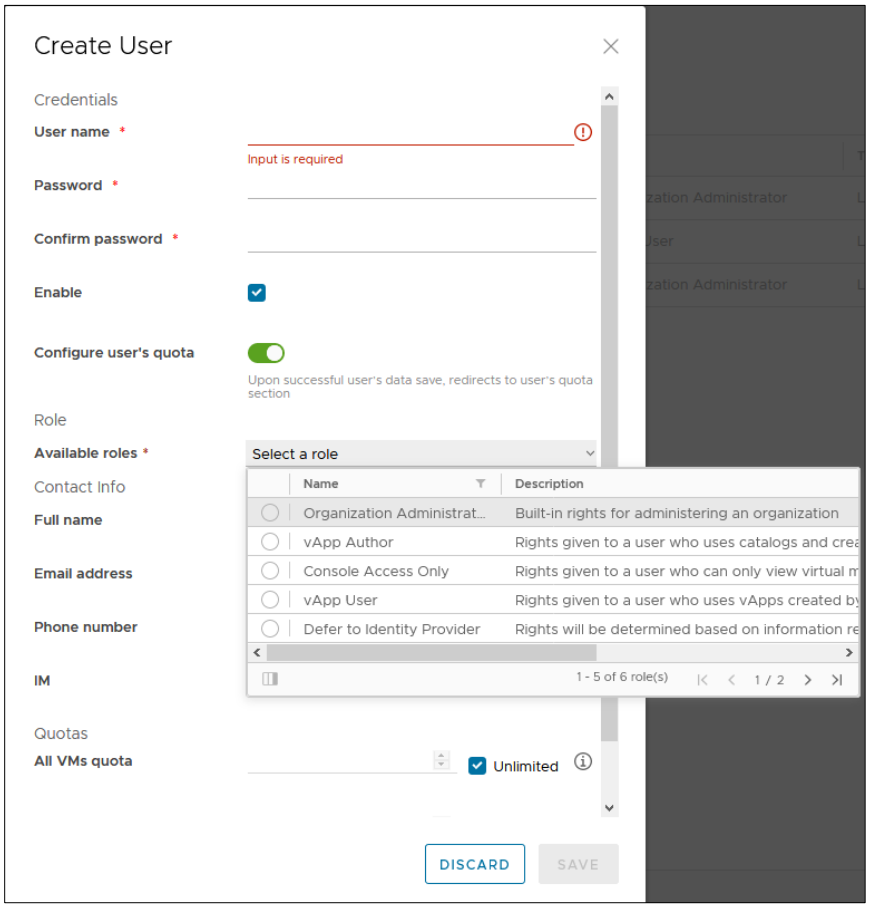
For the IPVPN network (VM atp-ipvpn), the procedure is the same, but you should check the availability of the remote host in your IPVPN network.

8. User account management

vCloud 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.

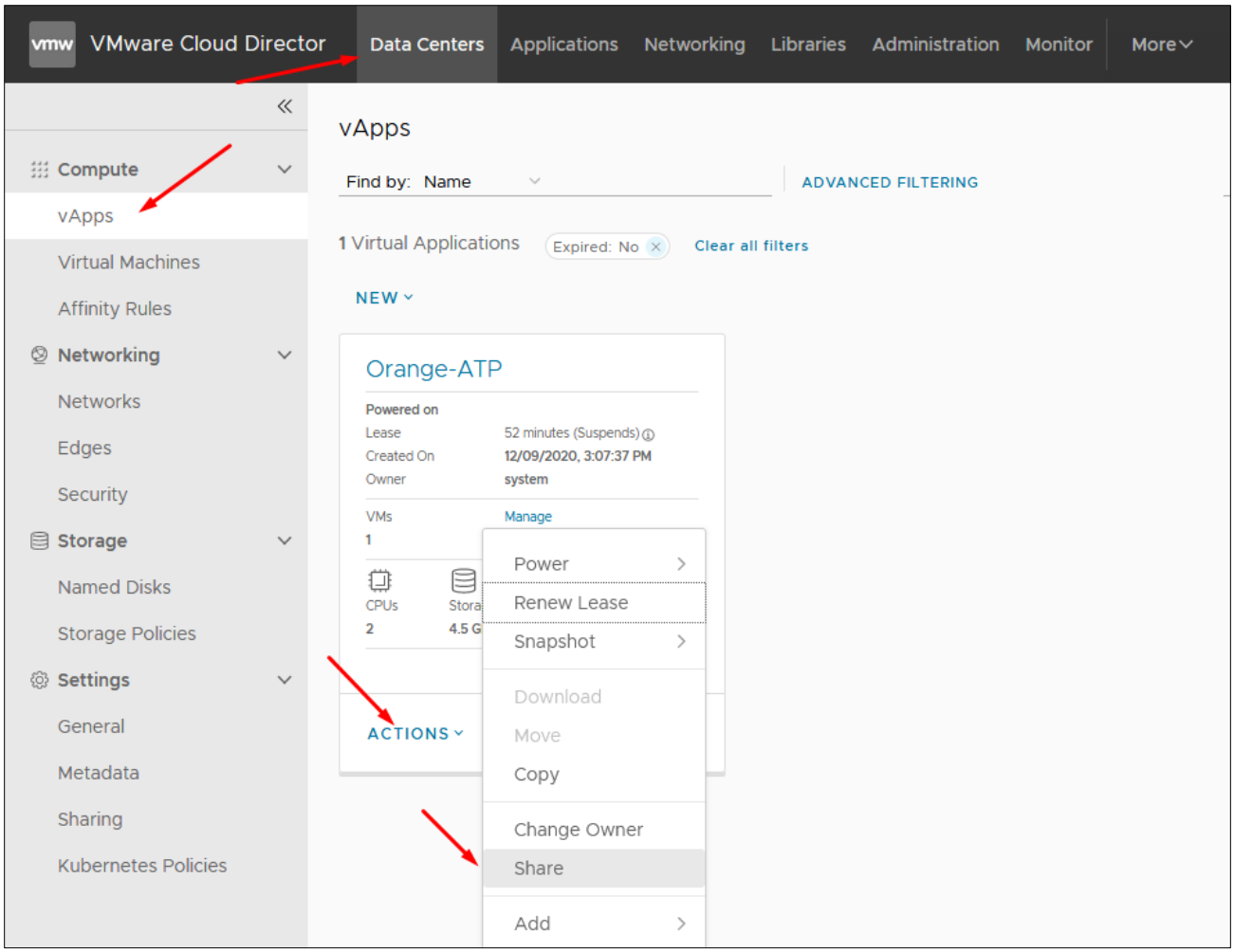


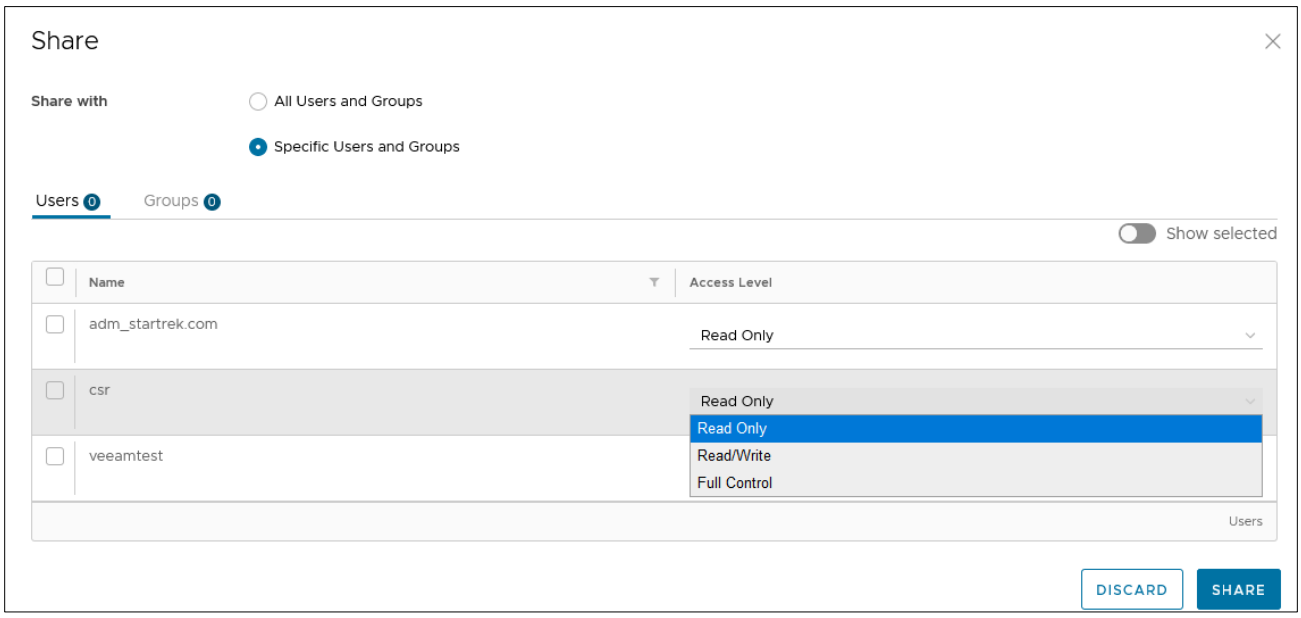
Fill in the details of the new user and set the role:



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:

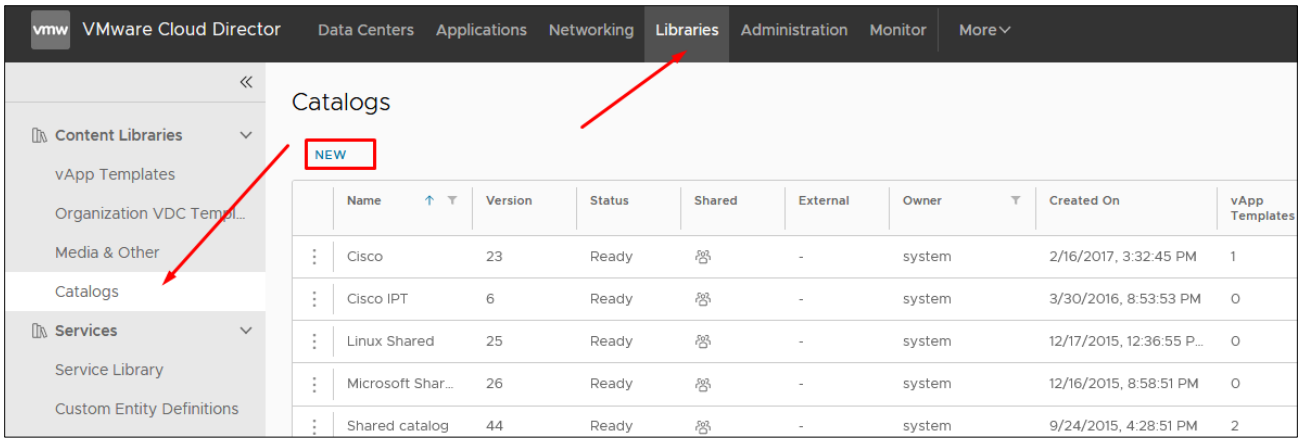




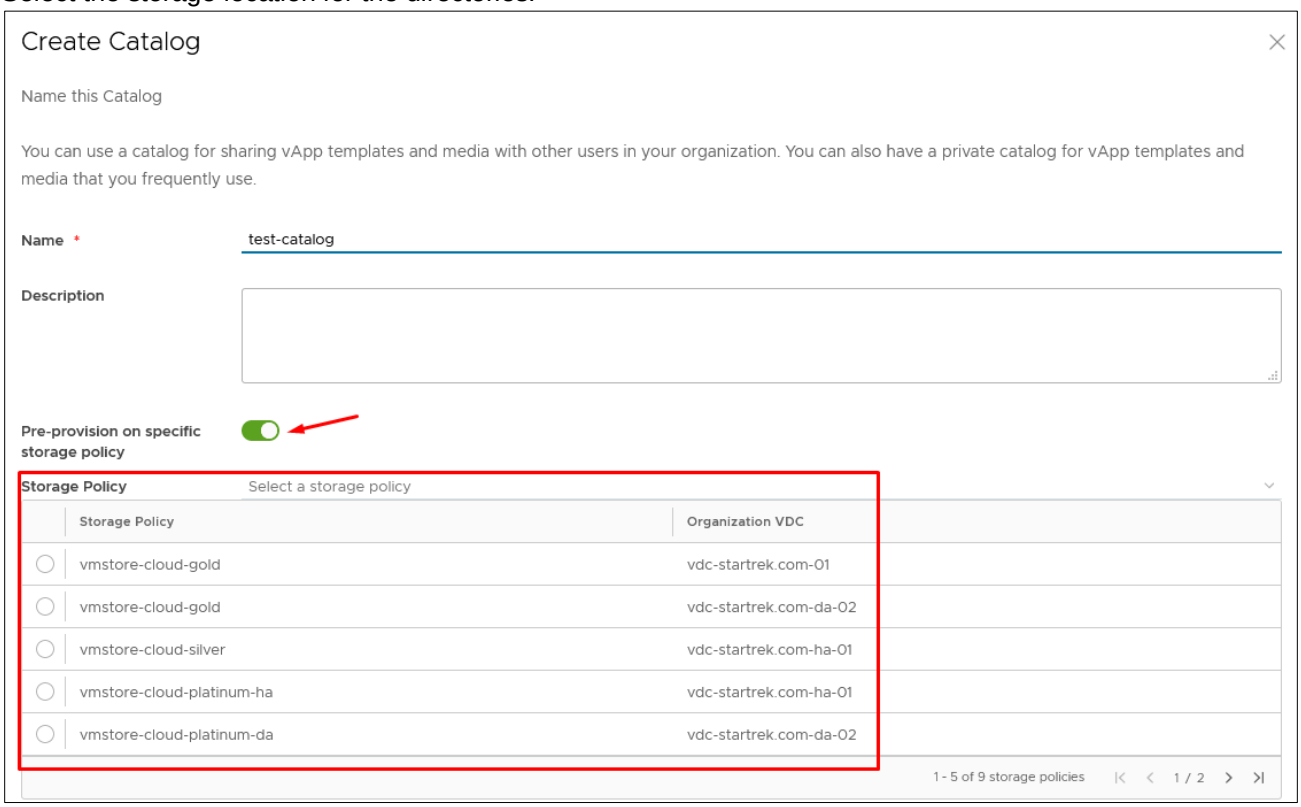
9. *Uploading images (ISO) and VM templates*

9.1. Directory creation

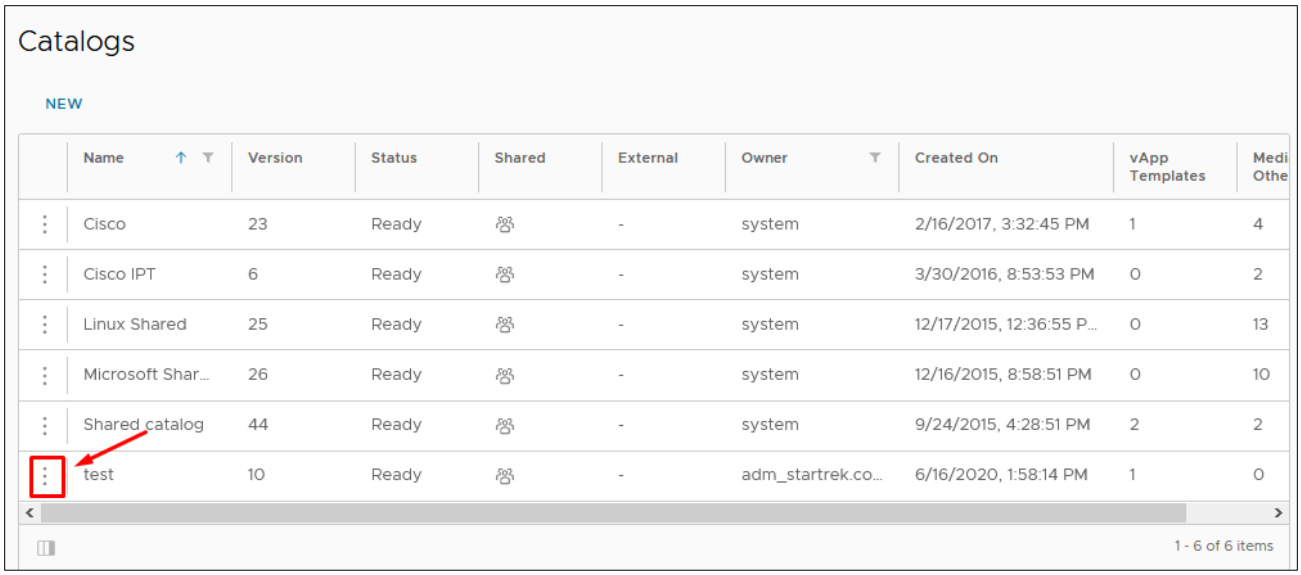
To be able to load any type of data, you first need to create a directory to store it in:

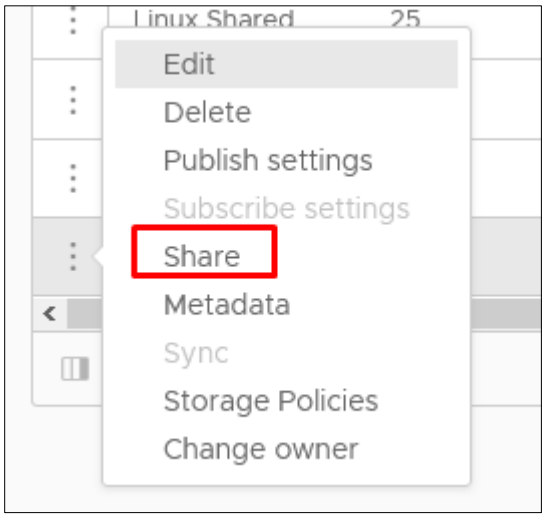


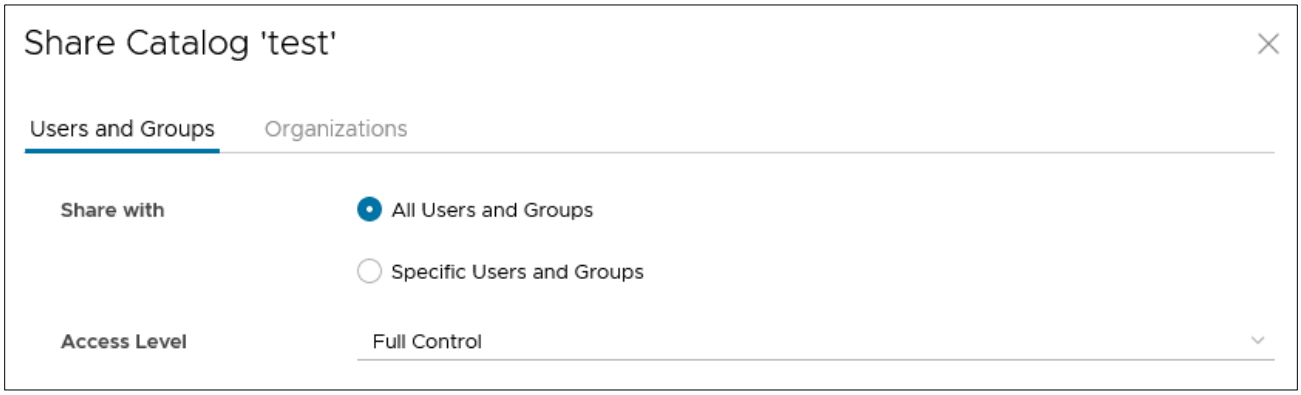
Select the storage location for the directories:



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







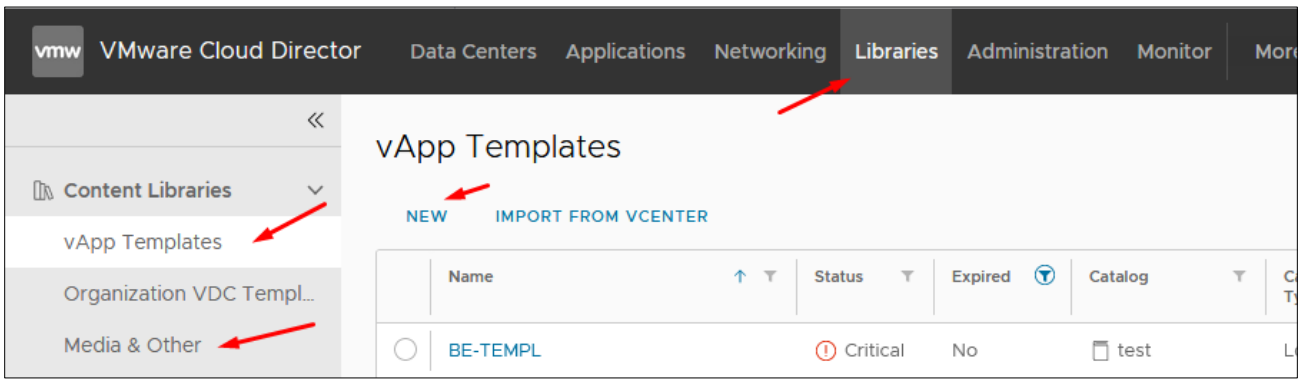
9.2. Uploading via vCloud Director

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 13;
- 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

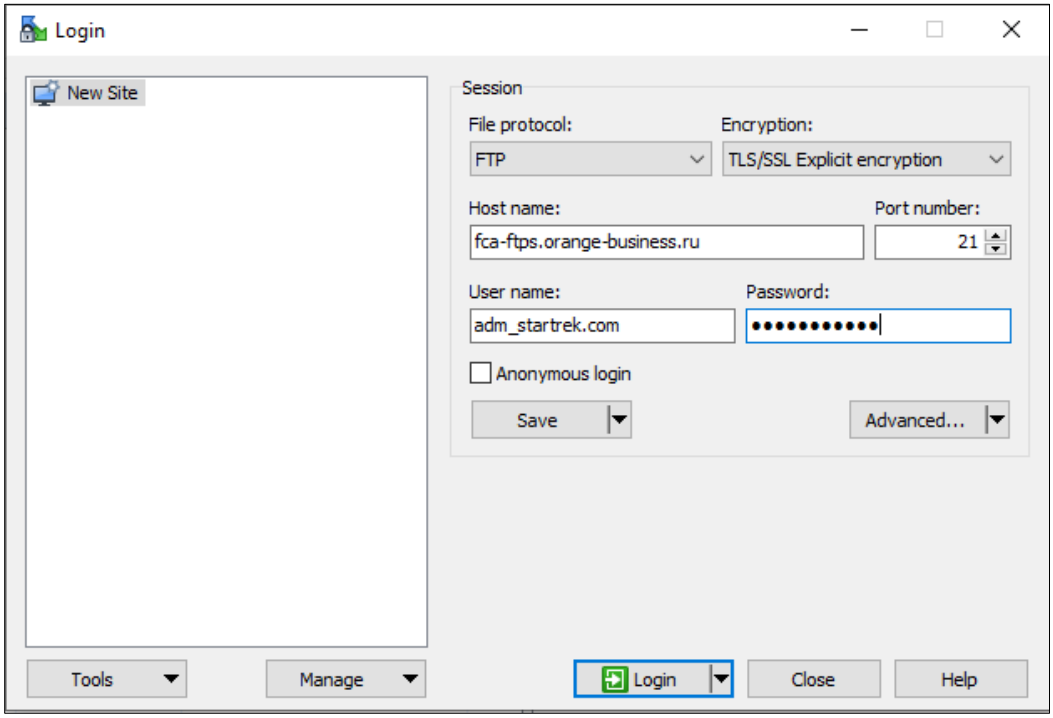
utility.



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.

Note: *to access ftp server you need to use FTP mode* ***"TLS/SSL Explicit encryption"*** *for example, in WinSCP:*



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.

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

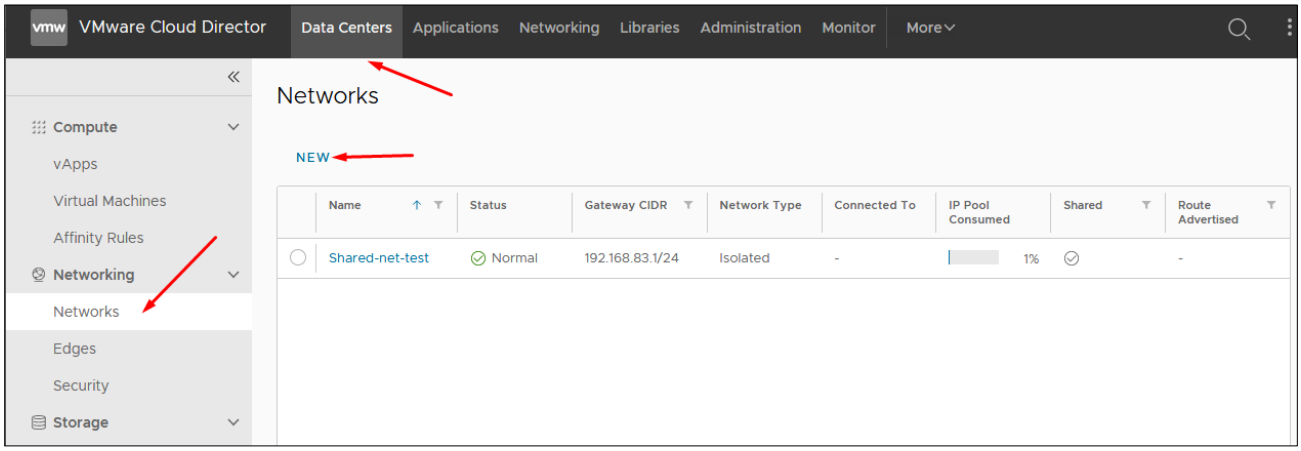
```
ovftool.exe --sourceType="OVA" "C:/Users/test/Desktop/vm.ova"
"vcloud://USERNAME@flexible-computing-advanced.orange-business.ru?org=vorg-startrack.com&vdc=vorg-startrack.com-01&catalog=test&vappTemplate=testtemplate"
```

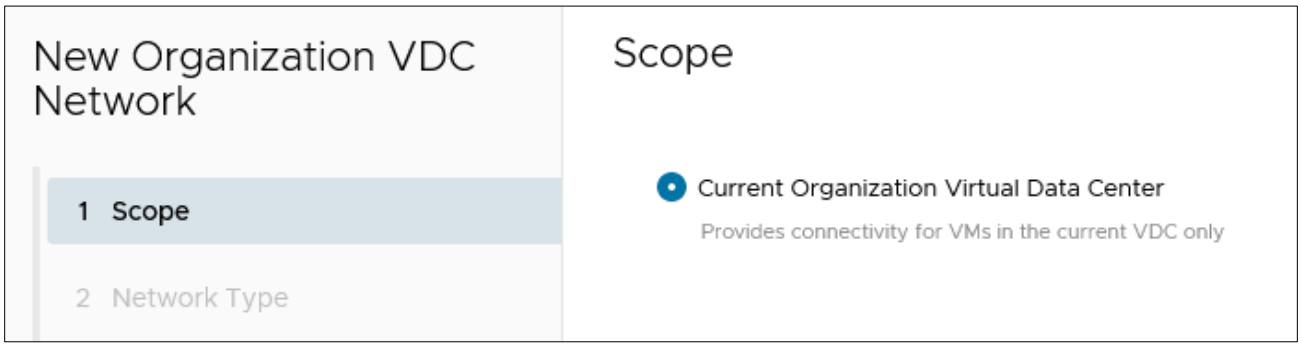
- Upload ISO

```
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"
```

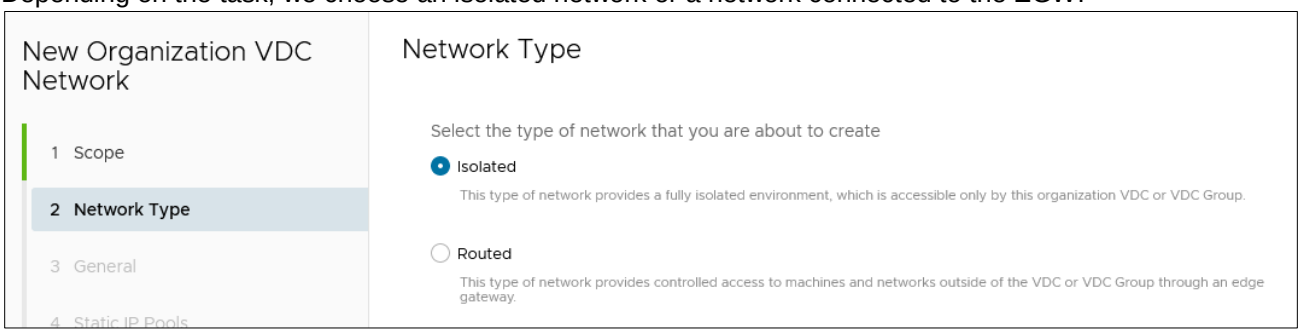
10. VOrg and vApp networks

10.1. Creating a vOrg network





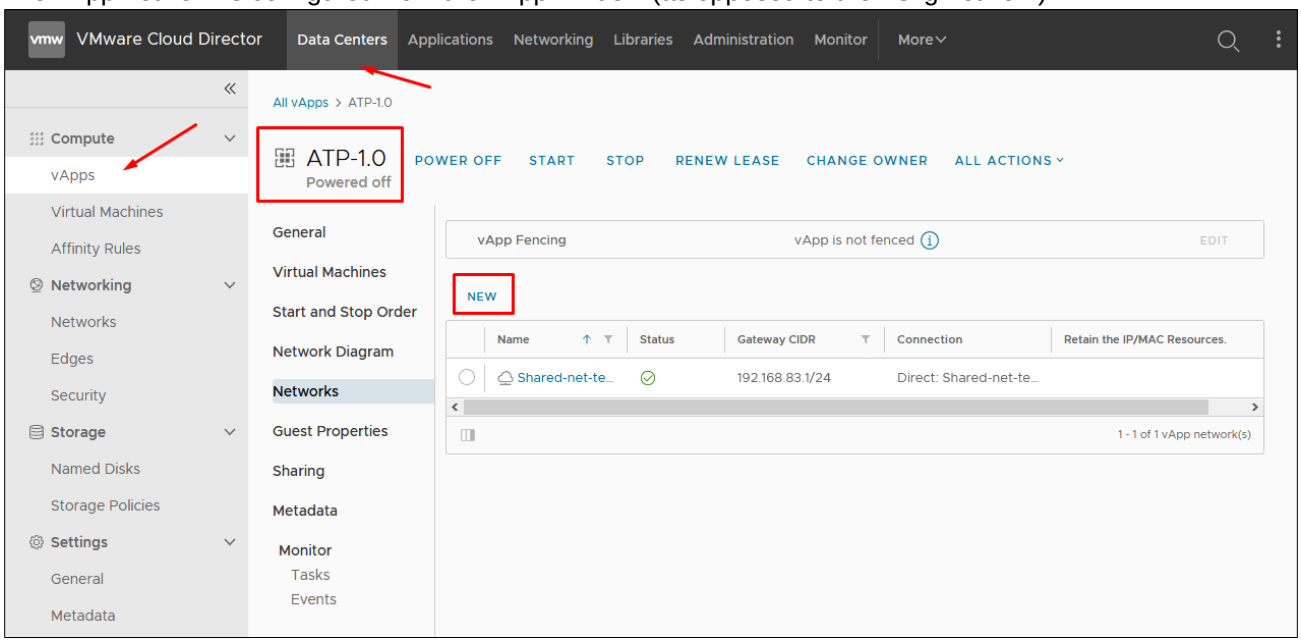
Depending on the task, we choose an isolated network or a network connected to the EGW.



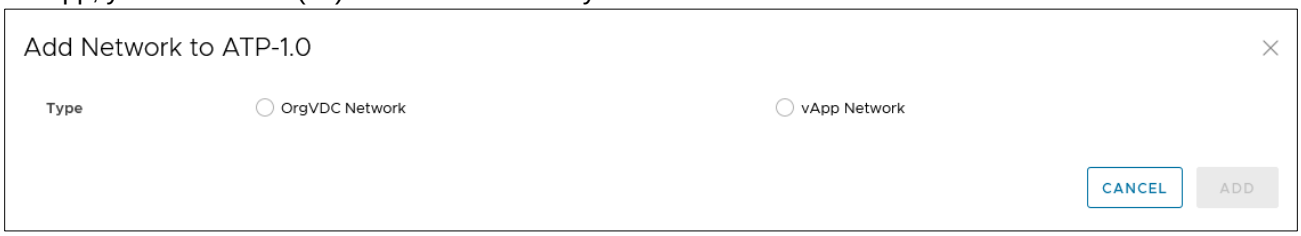
Specify the network parameters. If you plan to use DHCP, you must reduce the DHCP address pool by the size of the Static IP pool. If your infrastructure has more than one vDC, the network can be made available to other vDCs by enabling the following parameter:

10.2. Creating a vApp network

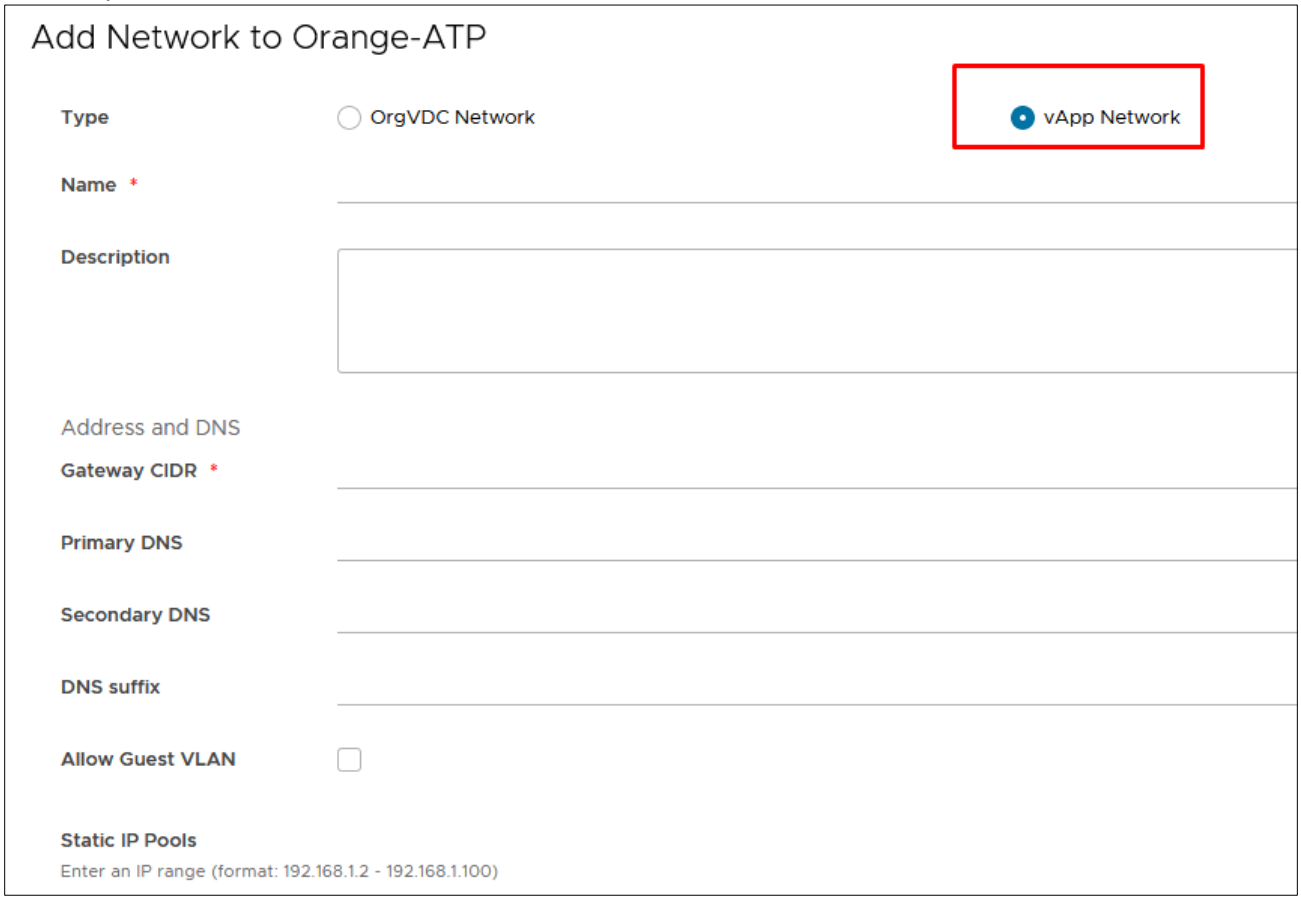
The vApp network is configured from the vApp window (as opposed to the vOrg network).

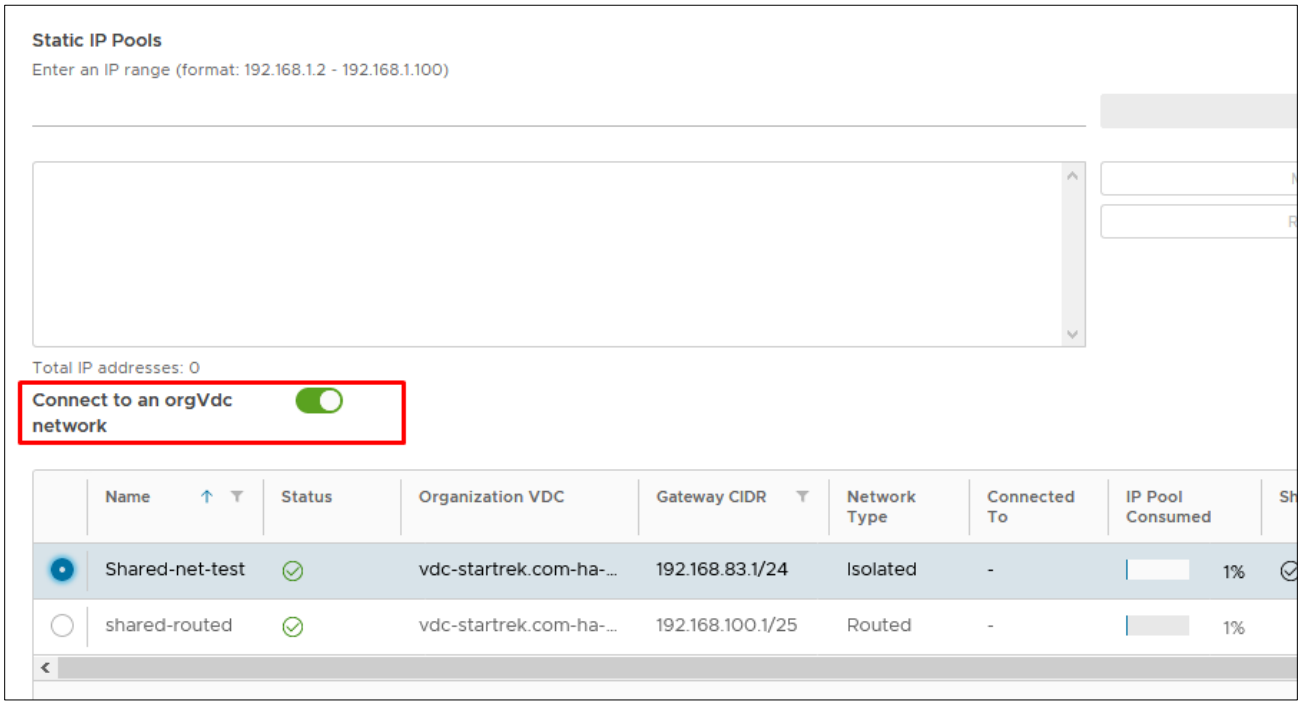


In vApp, you can add an (L2) vDC network directly or make it isolated:

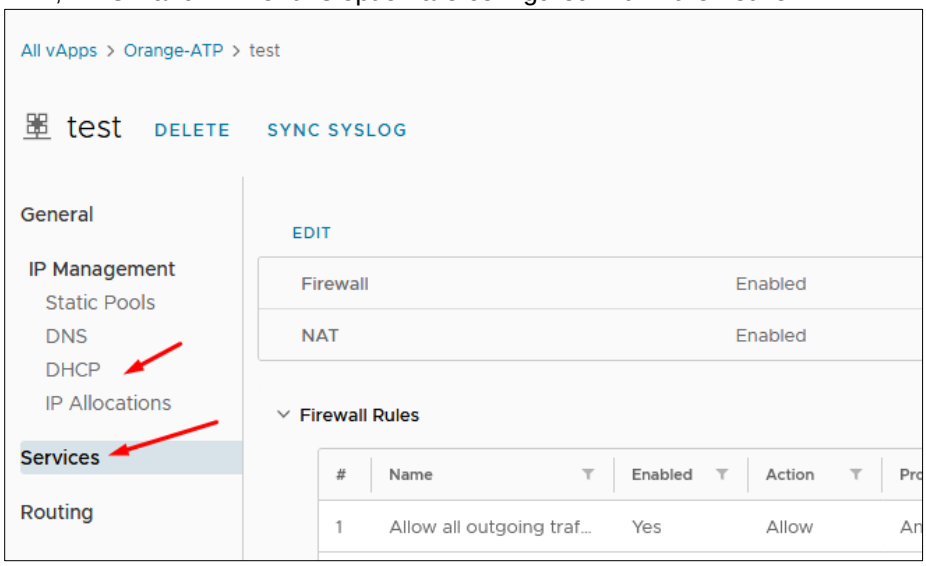


An isolated vApp network can be connected to the vOrg network via the vApp Edge (adding the ability to activate FW and NAT):





NAT, DHCP and FW for this option are configured within the network:



11. NSX Edge Gateway

11.1. NSX Edge Gateway size and performance

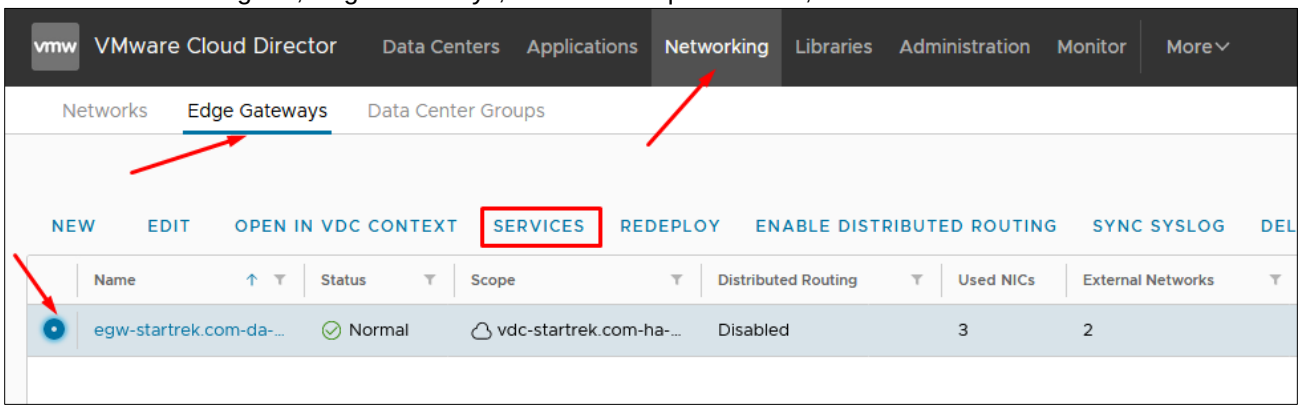
By default the NSX Edge Gateway size is Compact and the connection is limited to 5 internal client VLANs. The Customer can also order an NSX Edge Gateway size change to Large, X-Large, and Quad-Large, increase the number of connected networks, and activate the high availability option for NSX Edge.
The 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	2,048	4,096	4,096	8,192
ARP Entries Until Overwrite	1,024	2,048	2,048	2,048
FW Rules	2,000	2,000	2,000	2,000
FW Performance	3 Gbps	9.7 Gbps	9.7 Gbps	9.7 Gbps
DHCP Pools	20	20,000	20,000	20,000
ECMP Paths	8	8	8	8
Static Routes	2,048	2,048	2,048	2,048
LB Pools	64	64	64	1,024
LB Virtual Servers	64	64	64	1,024
LB Server / Pool	32	32	32	32
LB Health Checks	320	320	320	3,072
LB Application Rules	4,096	4,096	4,096	4,096
L2VPN Clients Hub to Spoke	5	5	5	5
L2VPN Networks per Client/Server	200	200	200	200
IPSec Tunnels	512	1.6	4,096	6
SSLVPN Tunnels	50	100	100	1
SSLVPN Private Networks	16	16	16	16

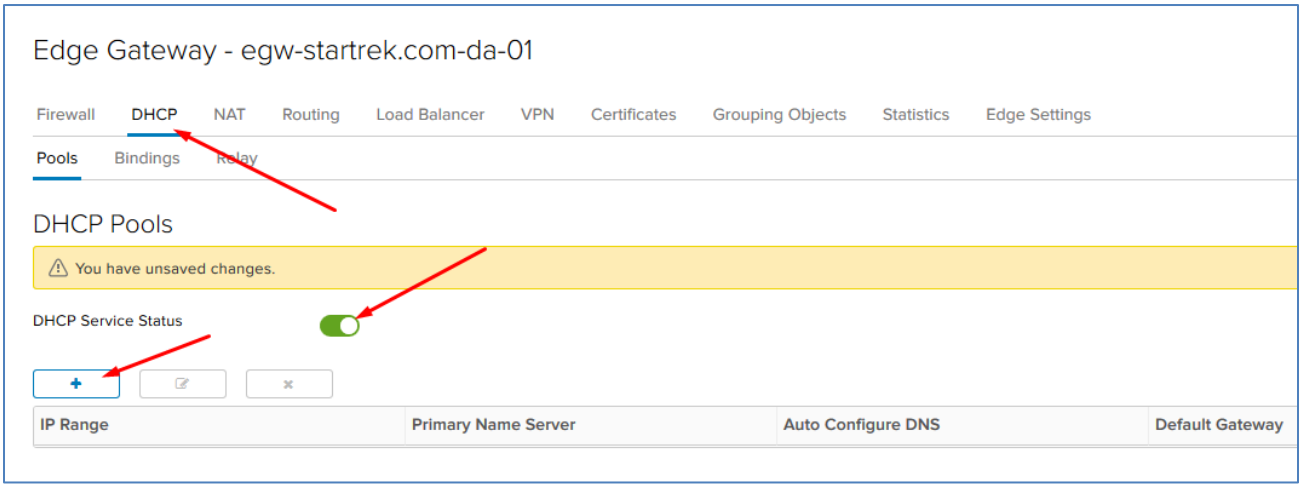
Concurrent Sessions	64	1,000,000	1,000,000	1,000,000
Sessions/Second	8	50	50	50
LB Throughput L7 Proxy)		2.2 Gbps	2.2 Gbps	3 Gbps
LB Throughput (L4 Mode)		6 Gbps	6 Gbps	6 Gbps
LB Connections/s (L7 Proxy)		46	50	50
LB Concurrent Connections (L7 Proxy)		8	60	60
LB Connections/s (L4 Mode)		50	50	50
LB Concurrent Connections (L4 Mode)		600	1,000,000	1,000,000
BGP Routes	20	50	250	250
BGP Neighbors	10	20	100	100
BGP Routes Redistributed	No Limit	No Limit	No Limit	No Limit
OSPF Routes	20	50	100	100
OSPF LSA Entries Max 750 Type-1	20	50	100	100
OSPF Adjacencies	10	20	40	40
OSPF Routes Redistributed	2,000	5,000	20	20
Total Routes	20	50	250	250

11.2. DHCP configuration

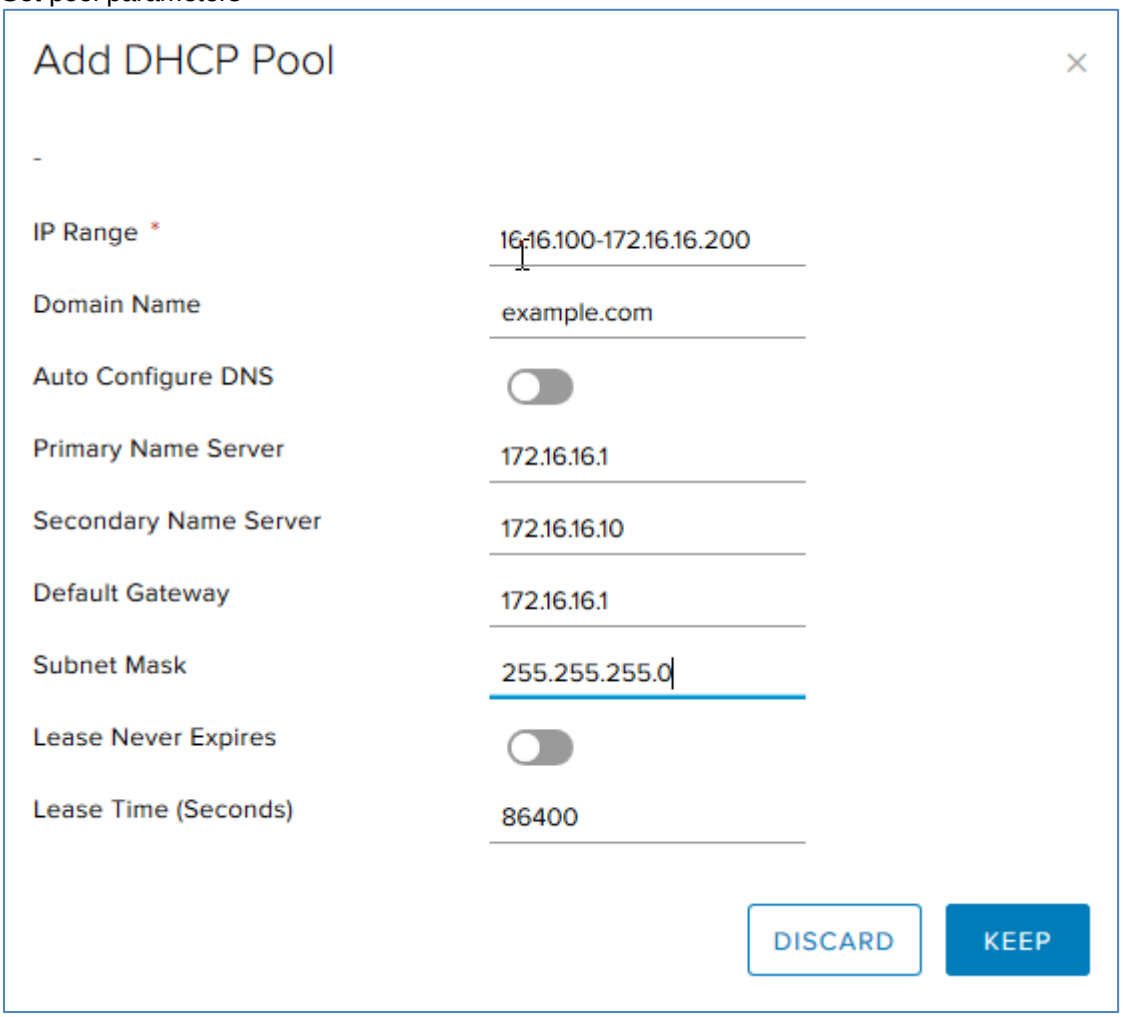
Go to the Networking tab, Edge Gateways, select the required EGW, and click Services:



Enable DHCP service and click Add

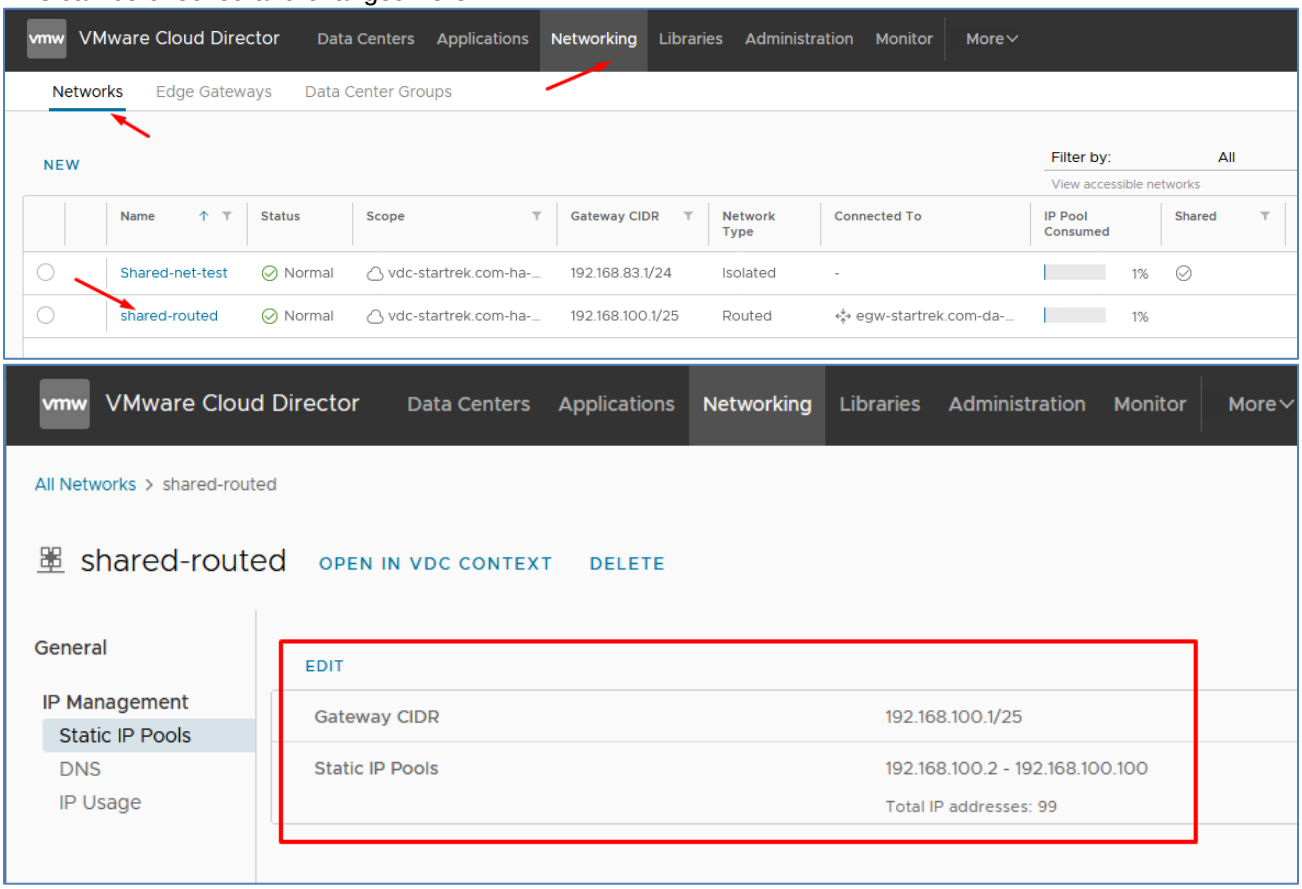


Set pool parameters



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:

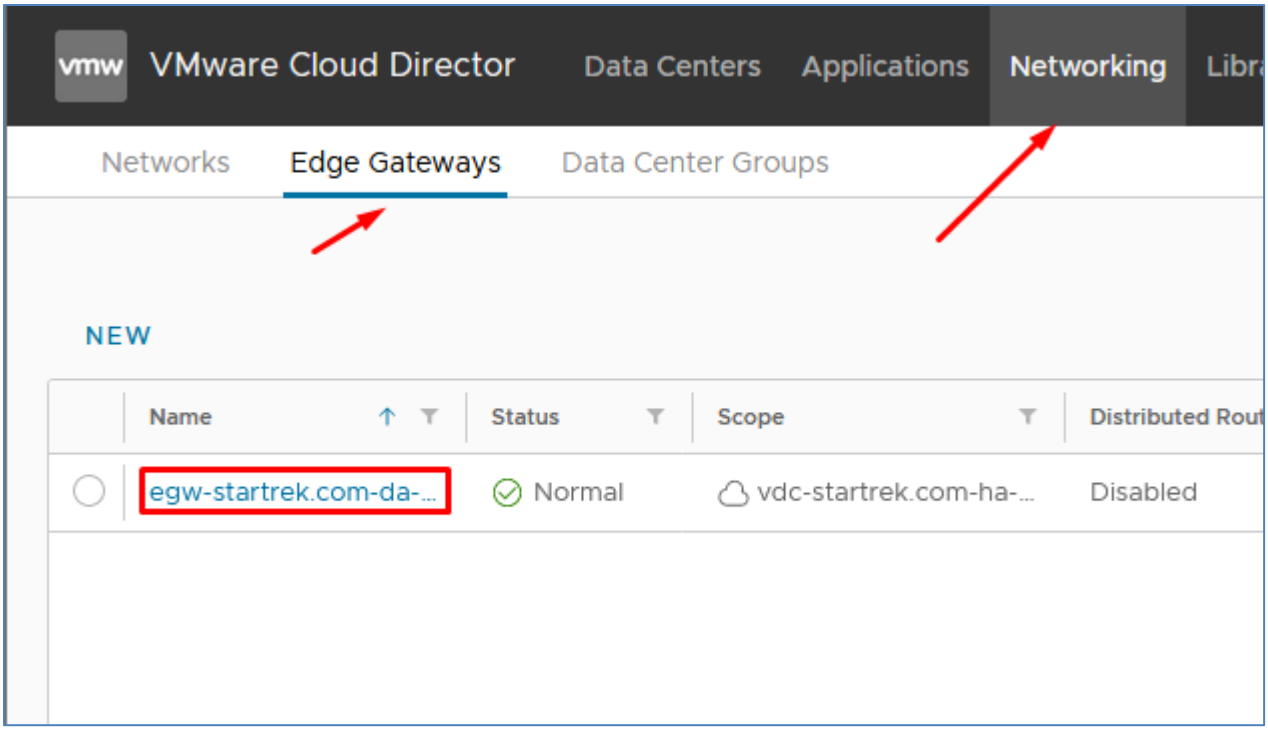


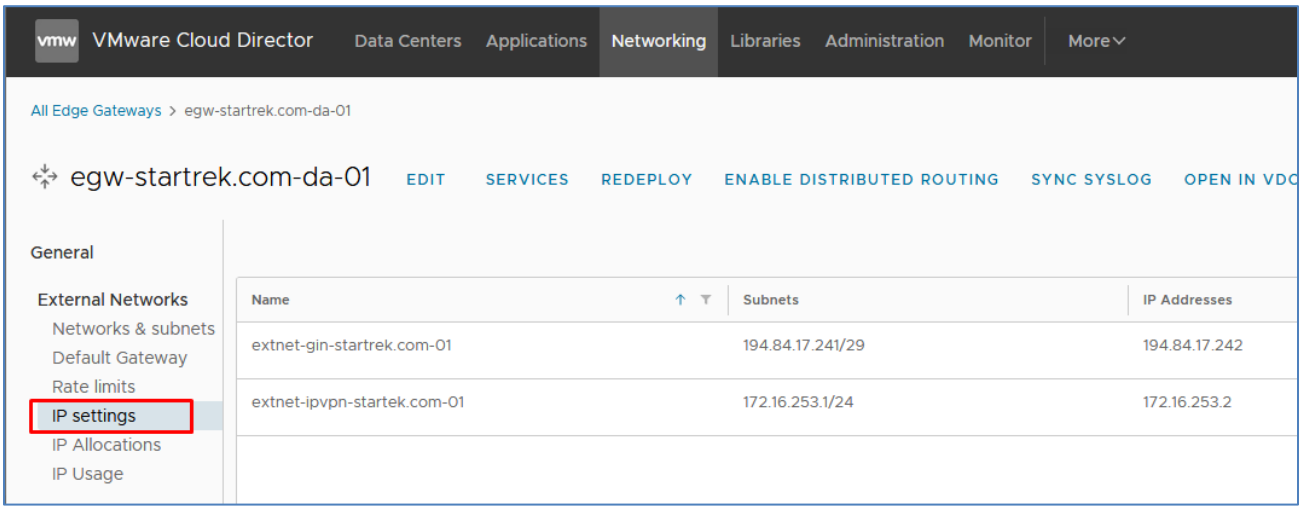
11.3. NAT configuration

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 vCloud Director, you need to configure SNAT and DNAT rules.

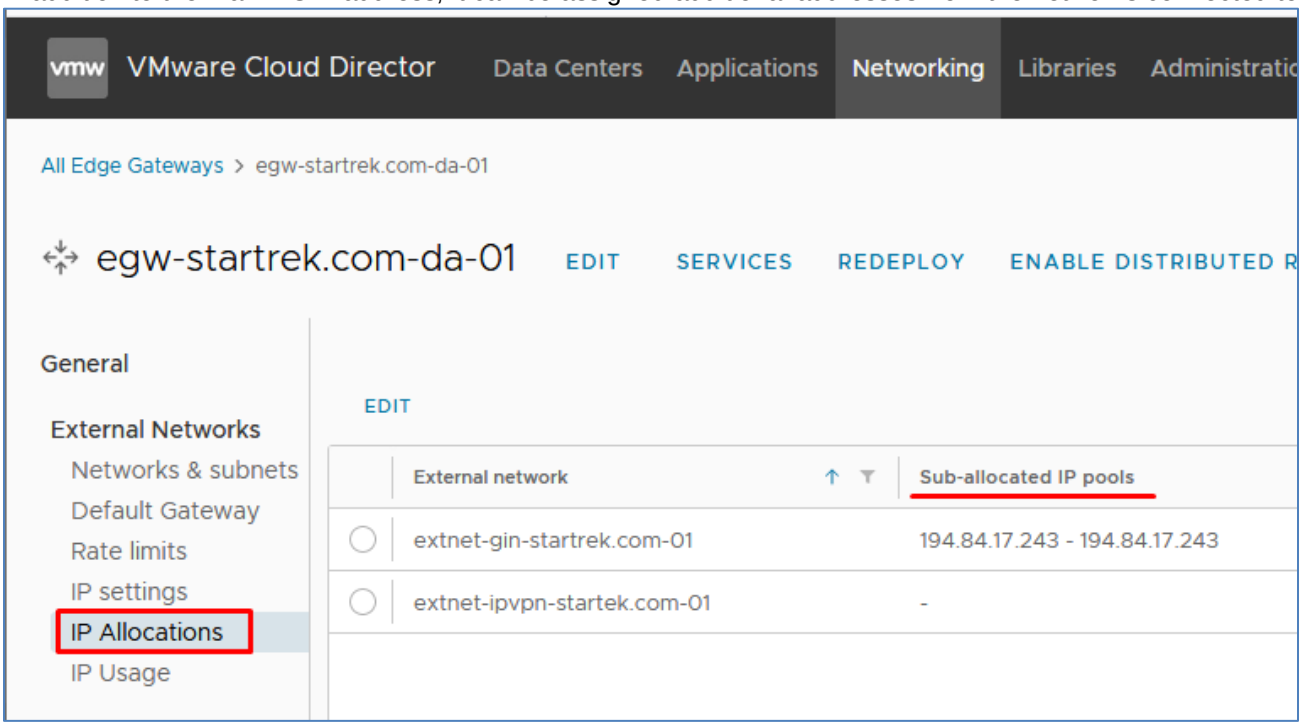
11.3.1. Creating a SNAT rule

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.

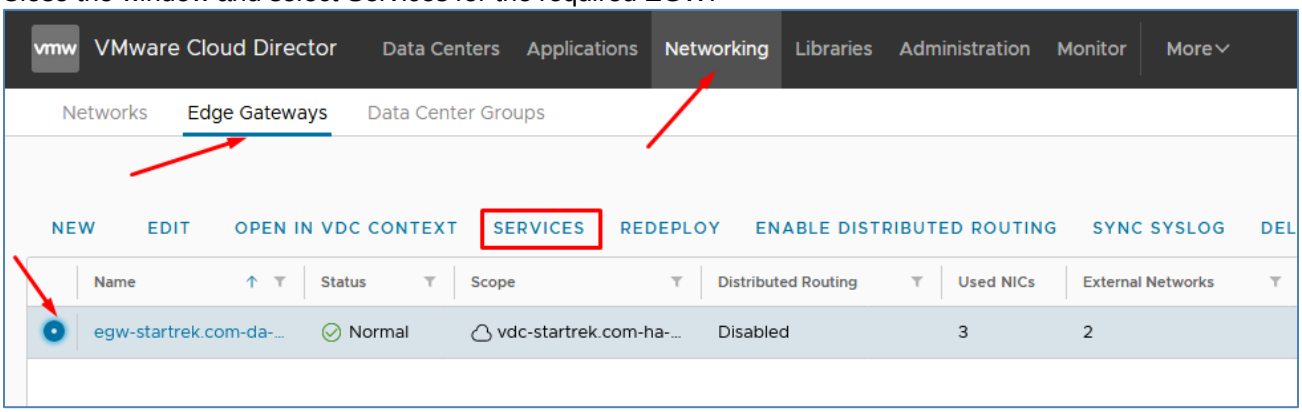




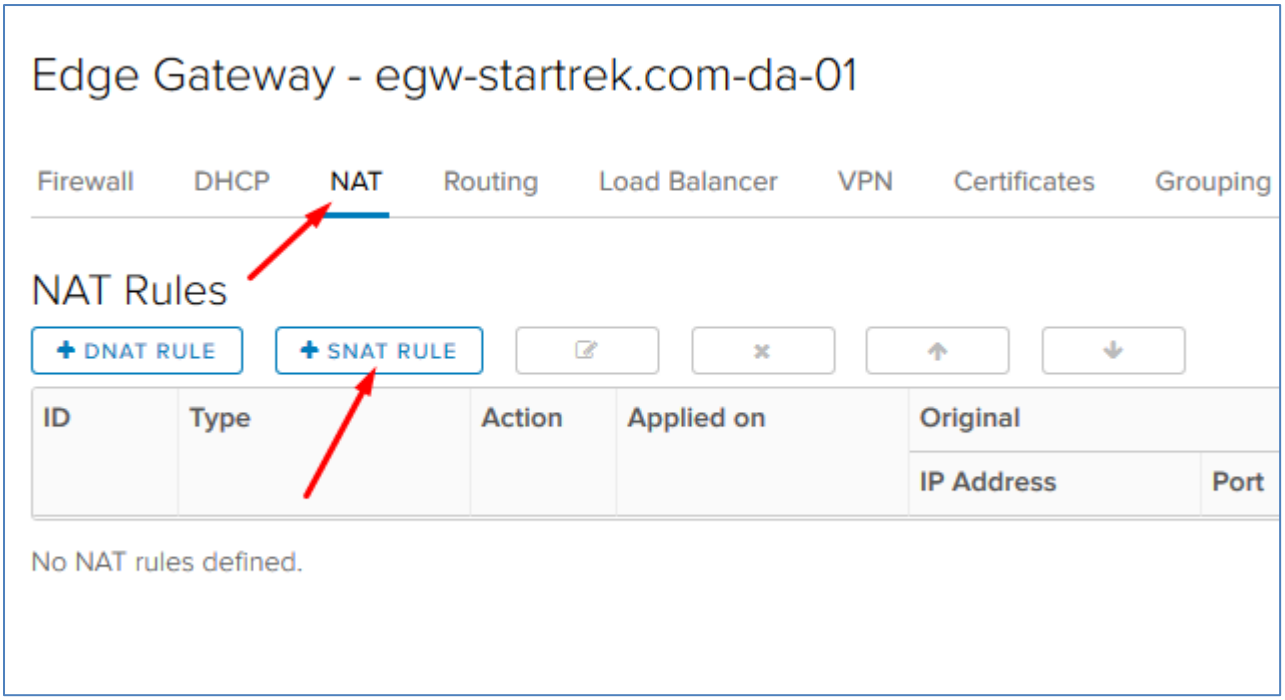
In addition to the main EGW address, it can be assigned additional addresses from the networks connected to it:



Close the window and select Services for the required EGW.

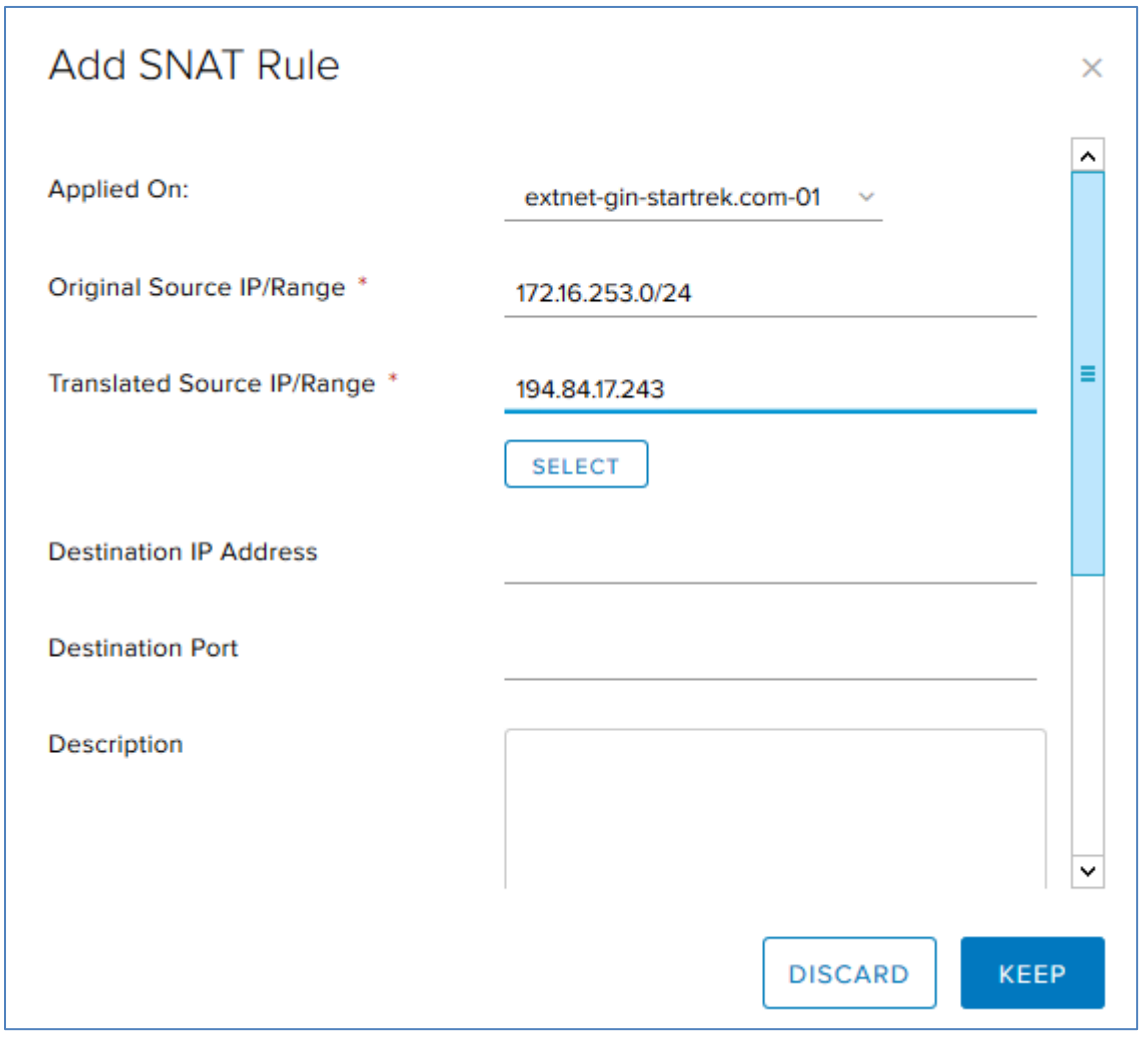


Go to the NAT tab and click the Add SNAT button



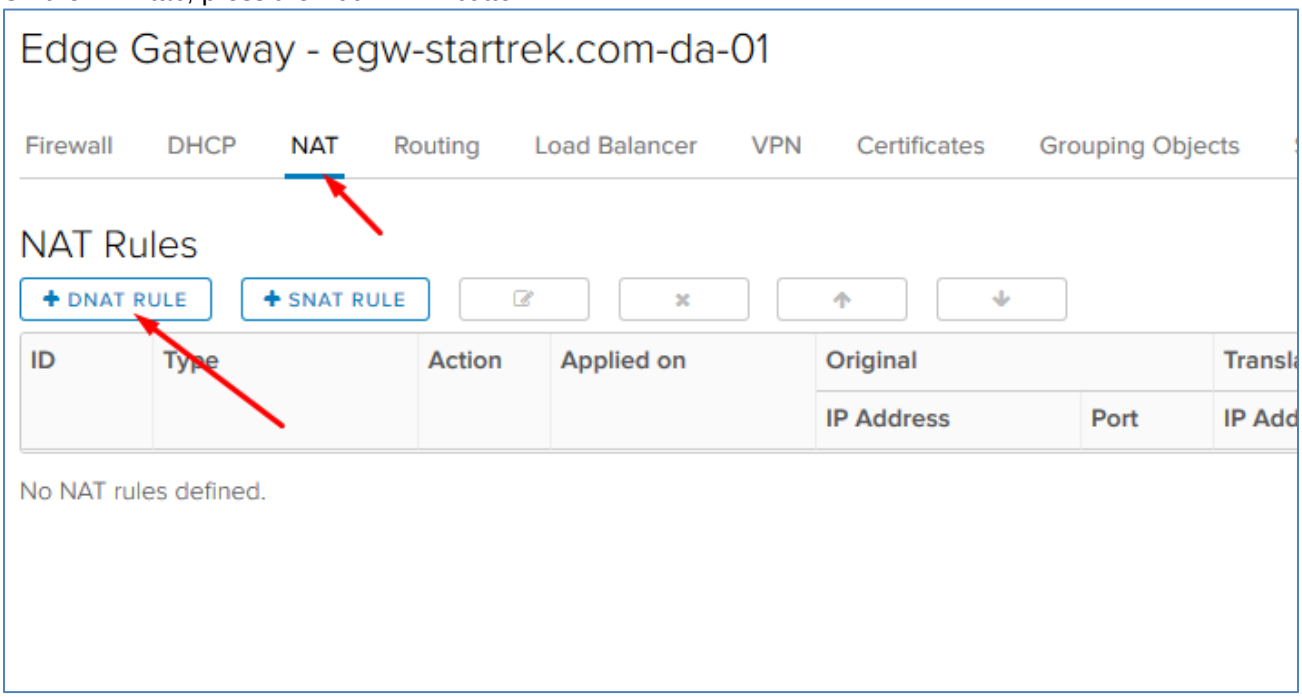
Specify parameters

- 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.



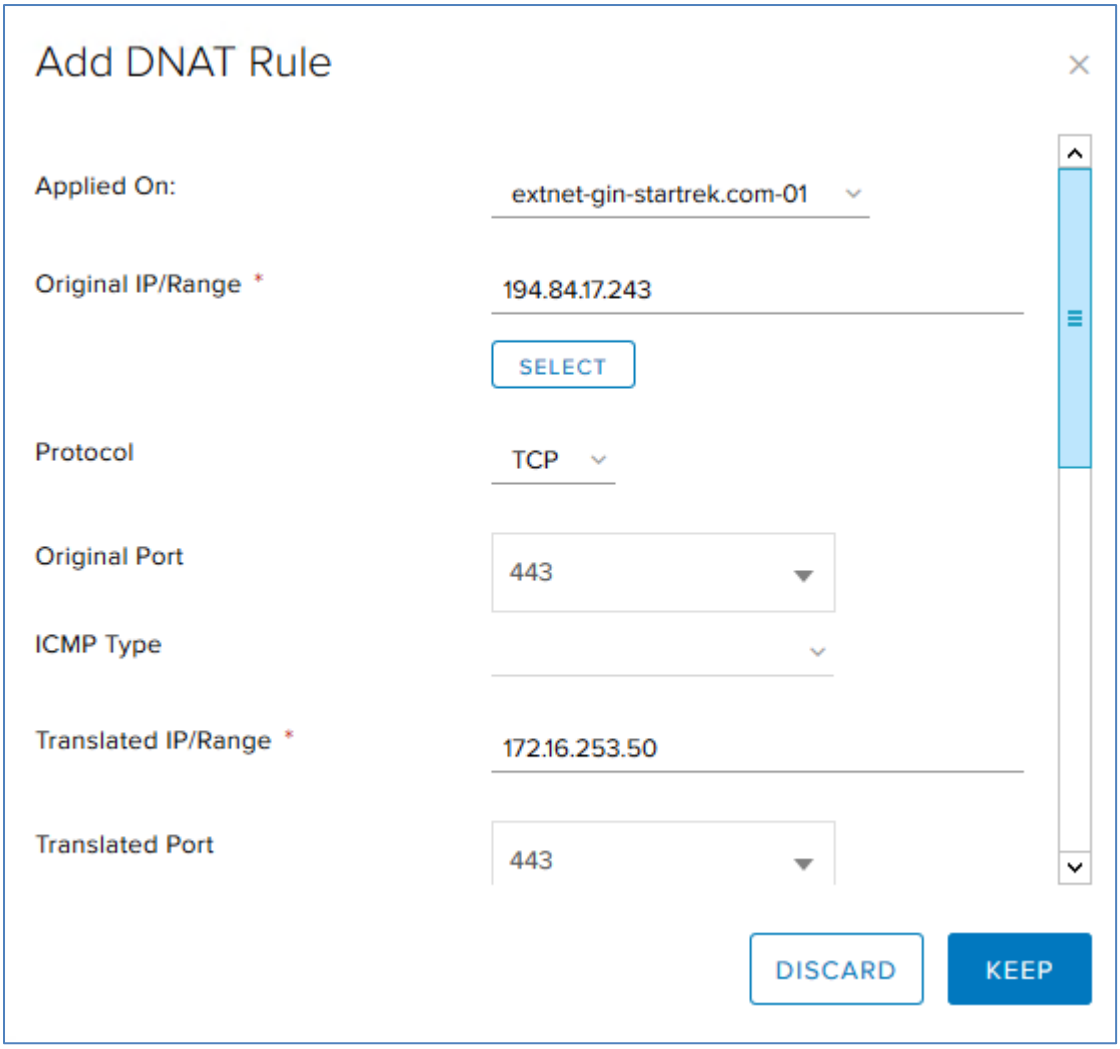
11.3.2. Creating a DNAT rule

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:

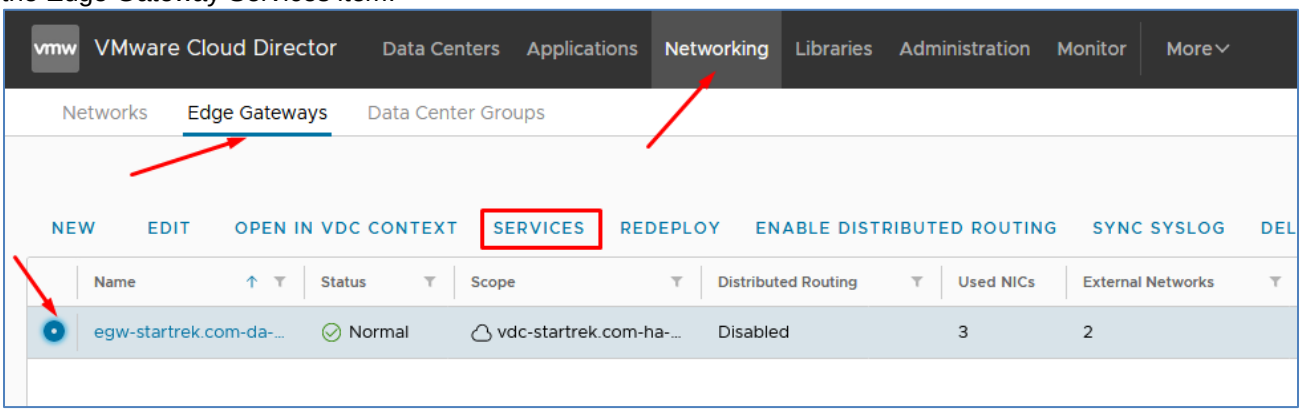
- In the Applied On field, specify the external network (like extnet-gin-DOMAIN-XX);
- In the Description field, specify the description of the DNAT rule;
- In the Original IP/range field, specify the external address (an address from the Sub-Allocate IP Pools range);
- Fill in the Protocol field;
- 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



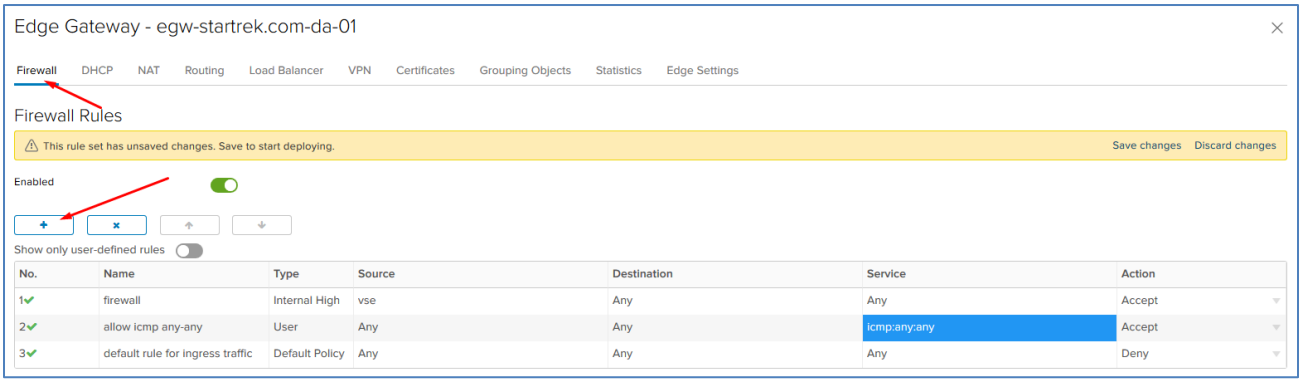
After that, configure the Firewall to let the corresponding packets through.

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.

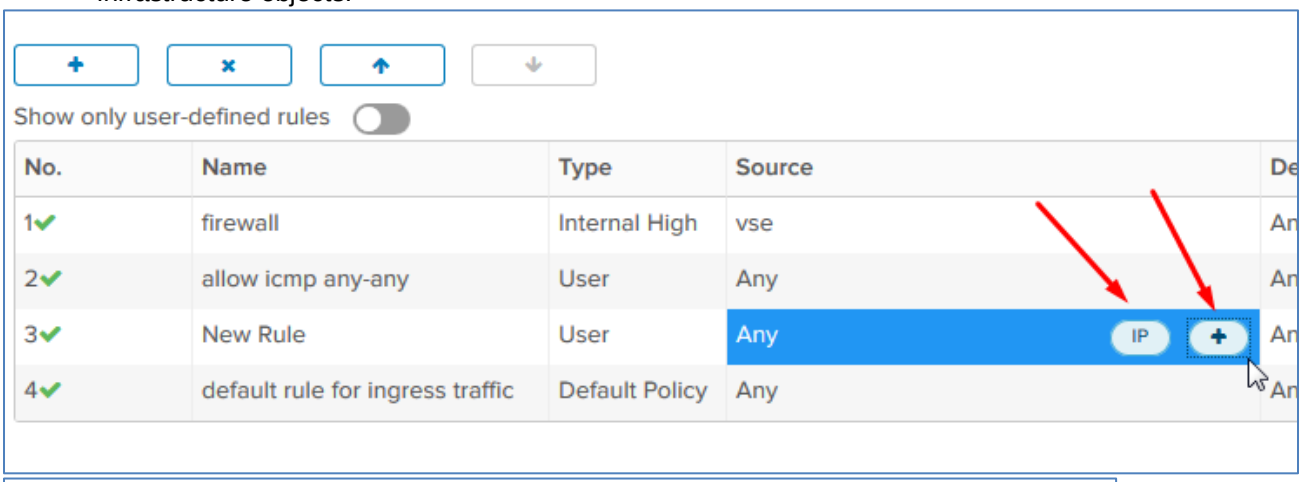


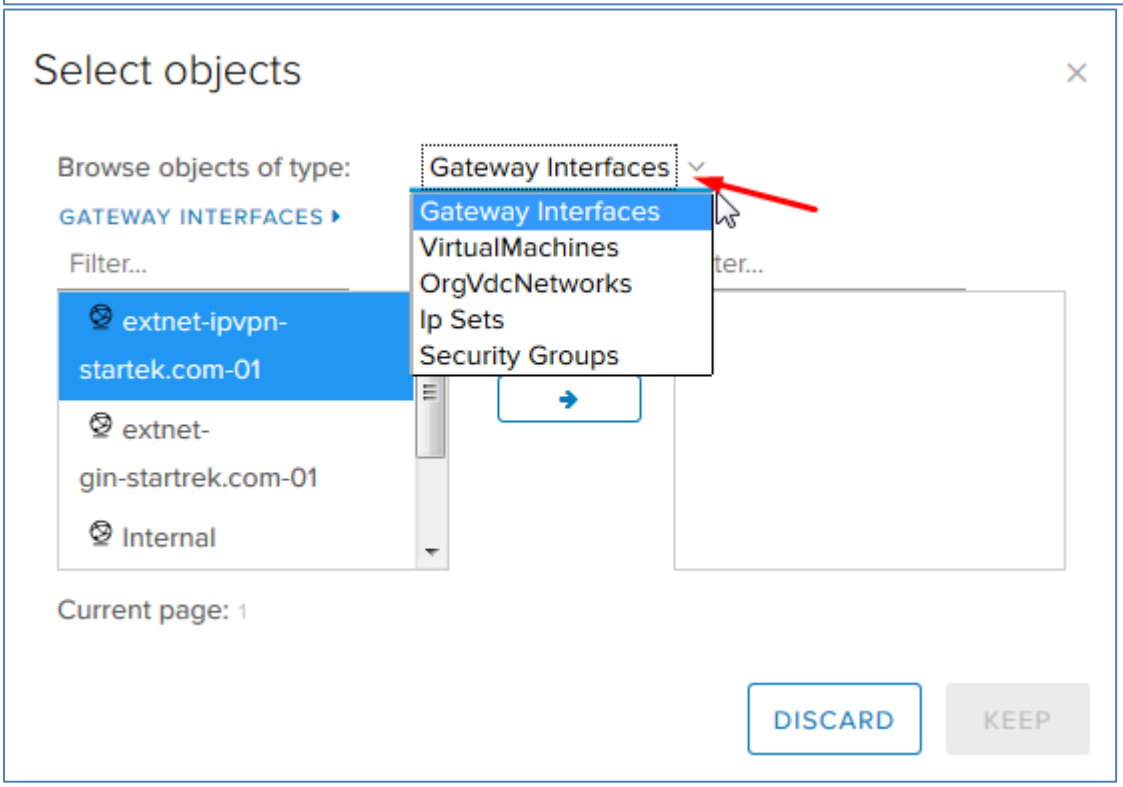
In the Services window that appears, go to the Firewall tab and click Add.
By default, the Deny option is selected in the Default Action item, meaning that the Firewall will block all traffic. To prevent this, you need to configure the rules.



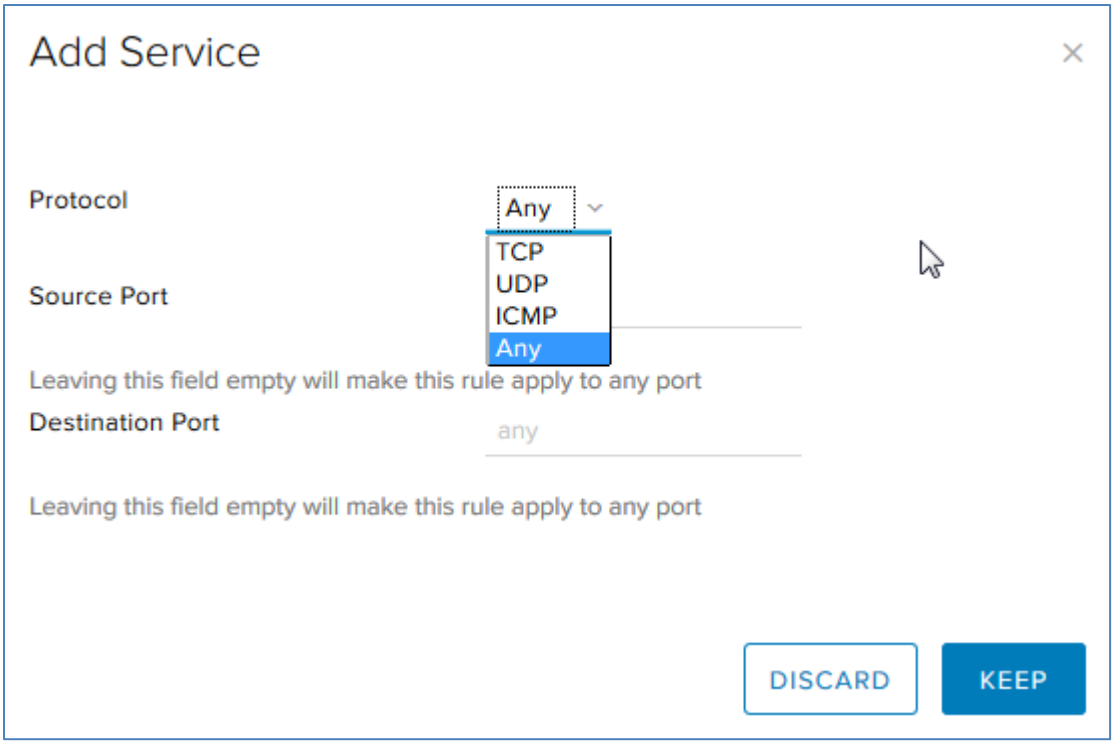
Fill in the parameters of the new rule:

- 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:



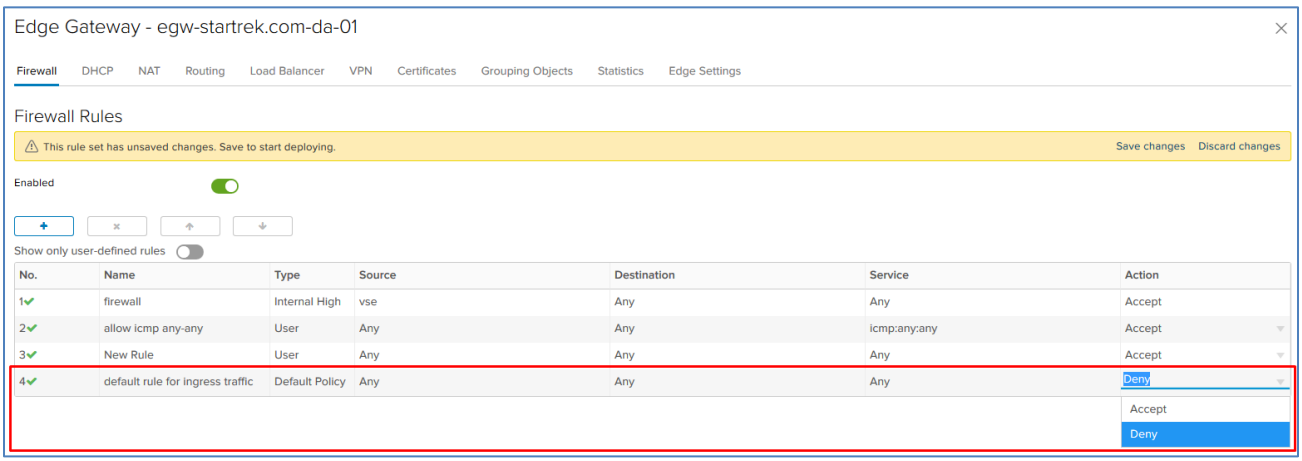


- Specify the recipient's address in the Destination field. The format is the same as for the Source field;
- In the Service field, select the recipient protocols and ports. You can leave Any, for example, for 1-1 NAT



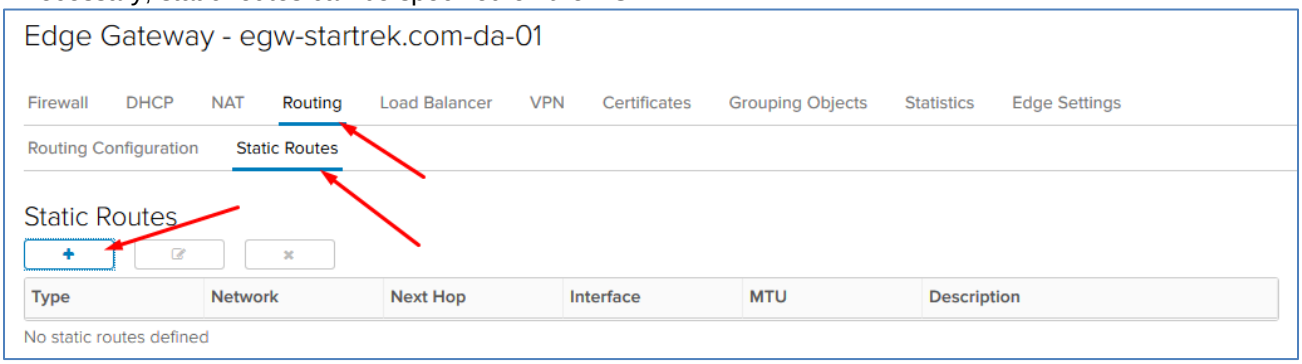
- In the Action field, select the required value (Allow or Deny).

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.



11.5. Static Routing configuration

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



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:

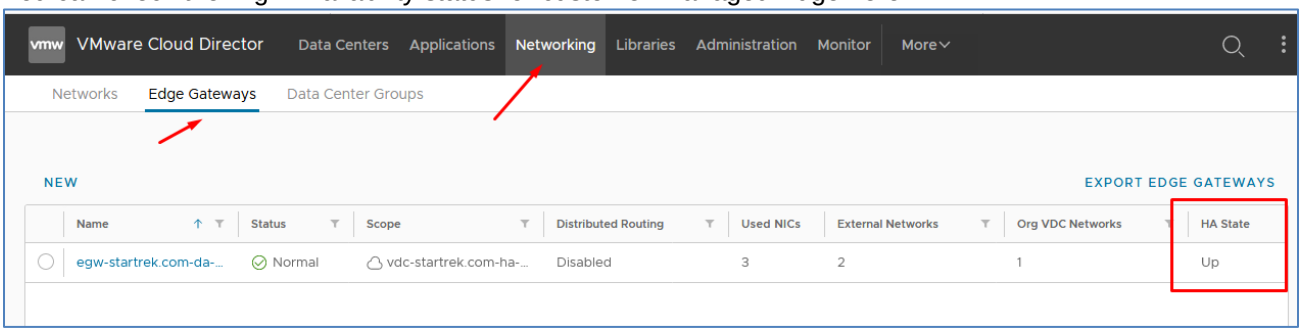
- SSL VPN-Plus, allows remote users to access corporate applications running in the cloud;

- 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.

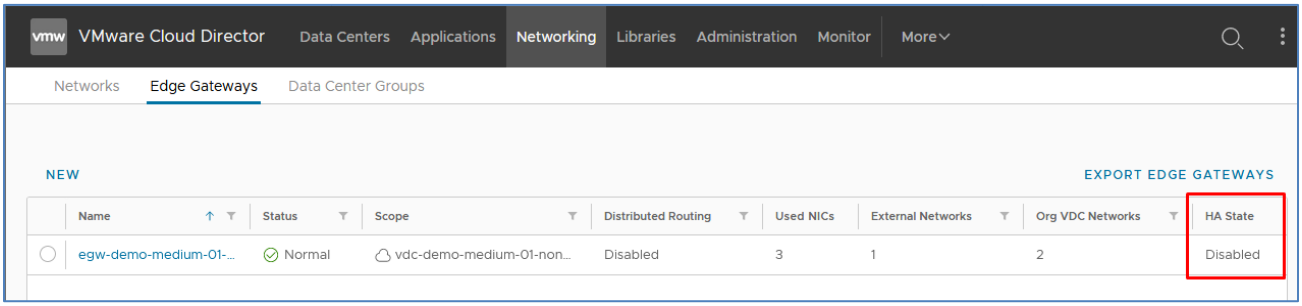
For more information, see the Virtual Private Networks (VPN) documentation section.

11.8. NSX Edge High Availability

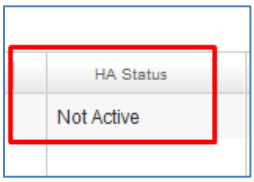
You can check the High Availability status for customer-managed Edge here:



Up means that HA is enabled.



Disabled means that HA is disabled.



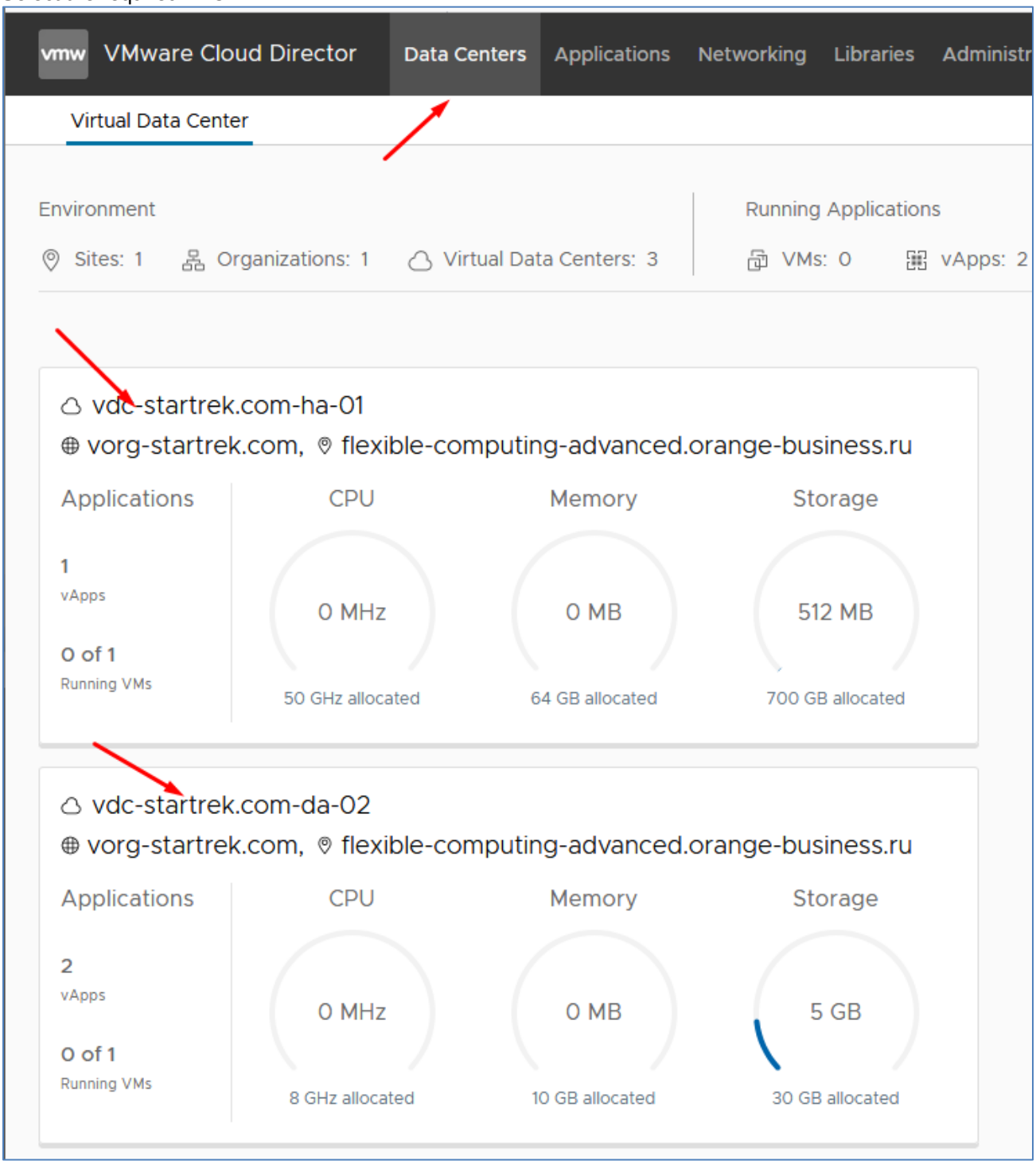
Not Active means that HA configuration is enabled but not active.
Note: To enable HA mode, at least one internal network must be connected to the Edge, as it will be used for heartbeat.

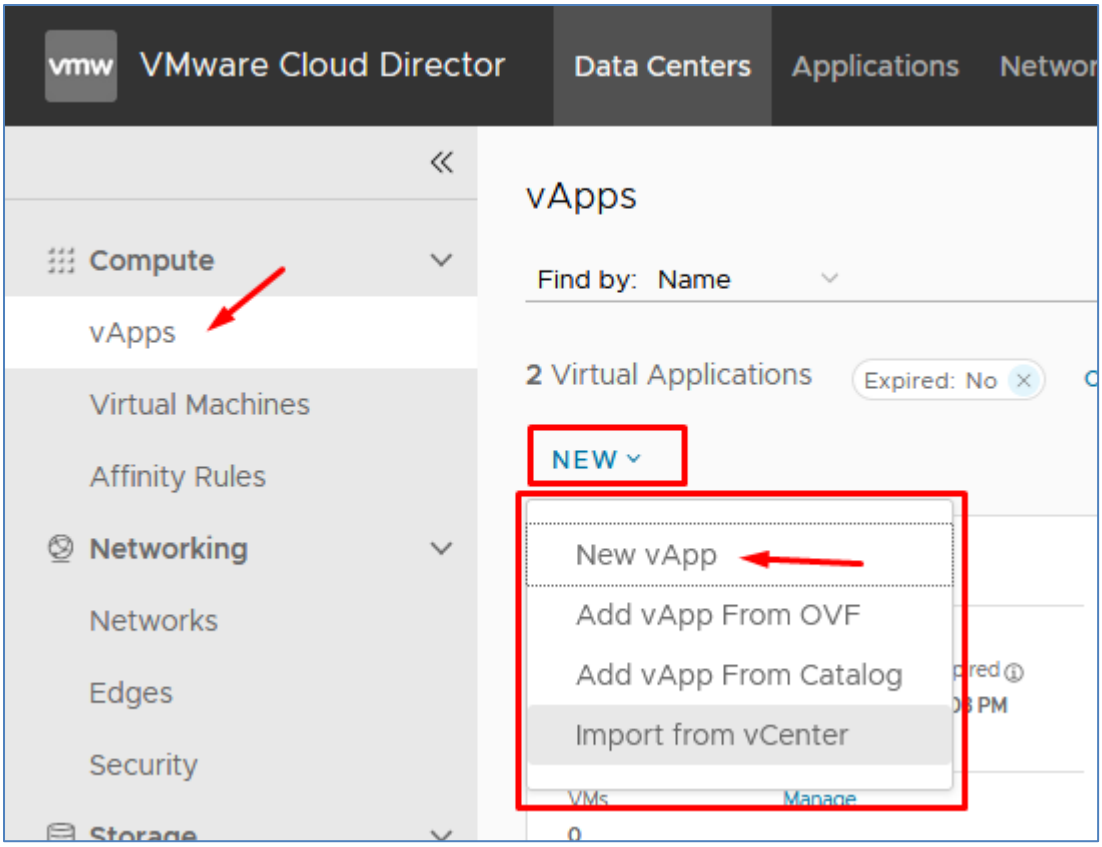
12. Configuring and managing virtual machines and vApps

12.1. Creating a new vApp container

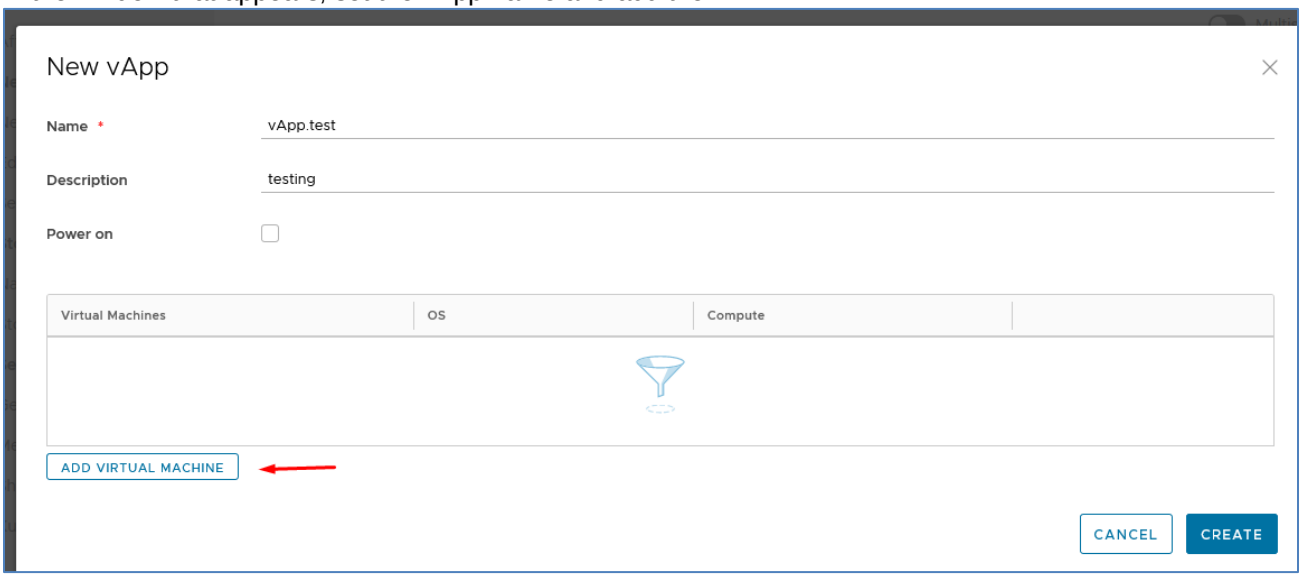
A new vApp can be created empty using a vApp template or with an empty VM (without OS).
Next, let's look at the process of creating a vApp with an empty VM.

Select the required vDC:

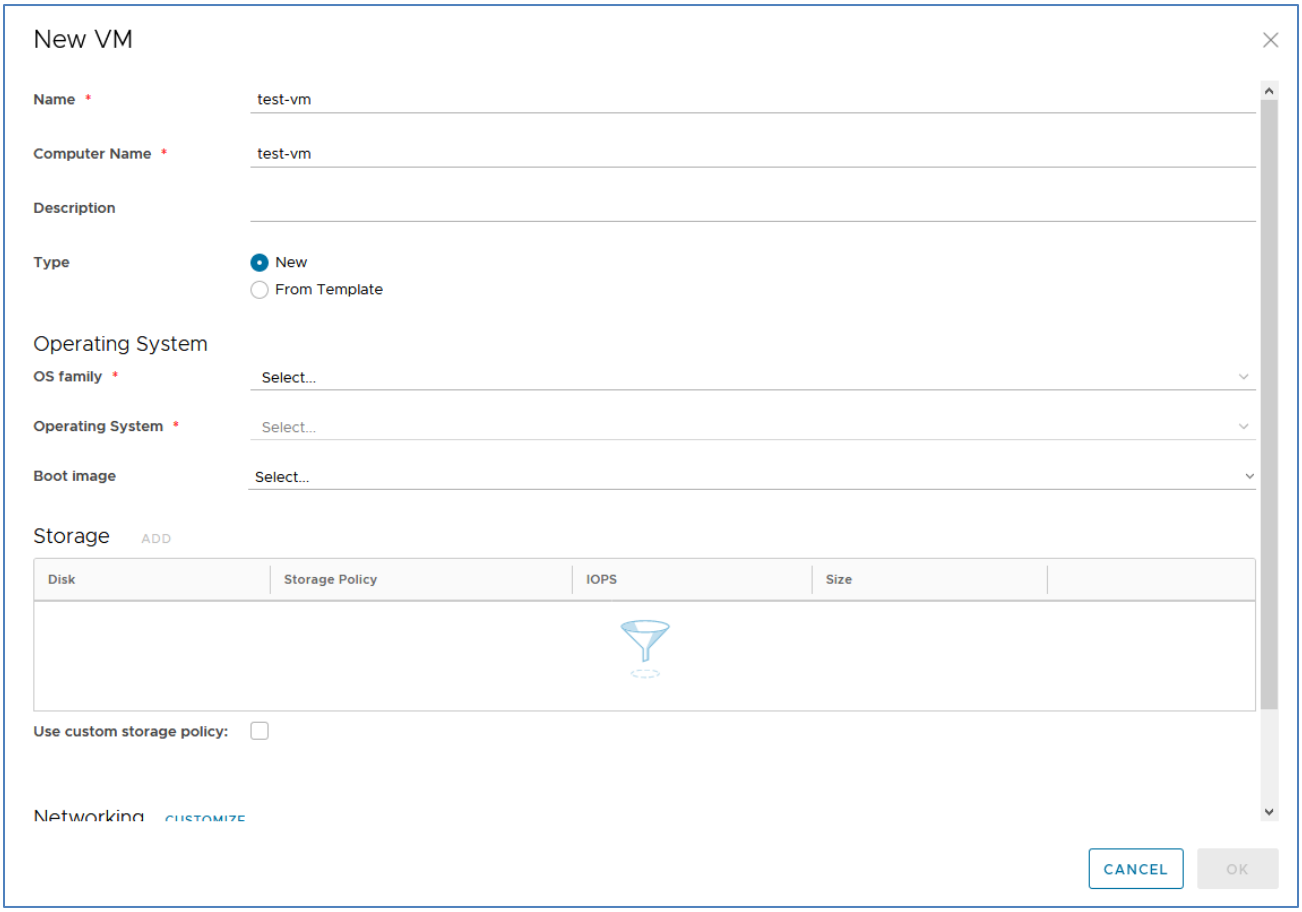




In the window that appears, set the vApp name and add the VM:



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

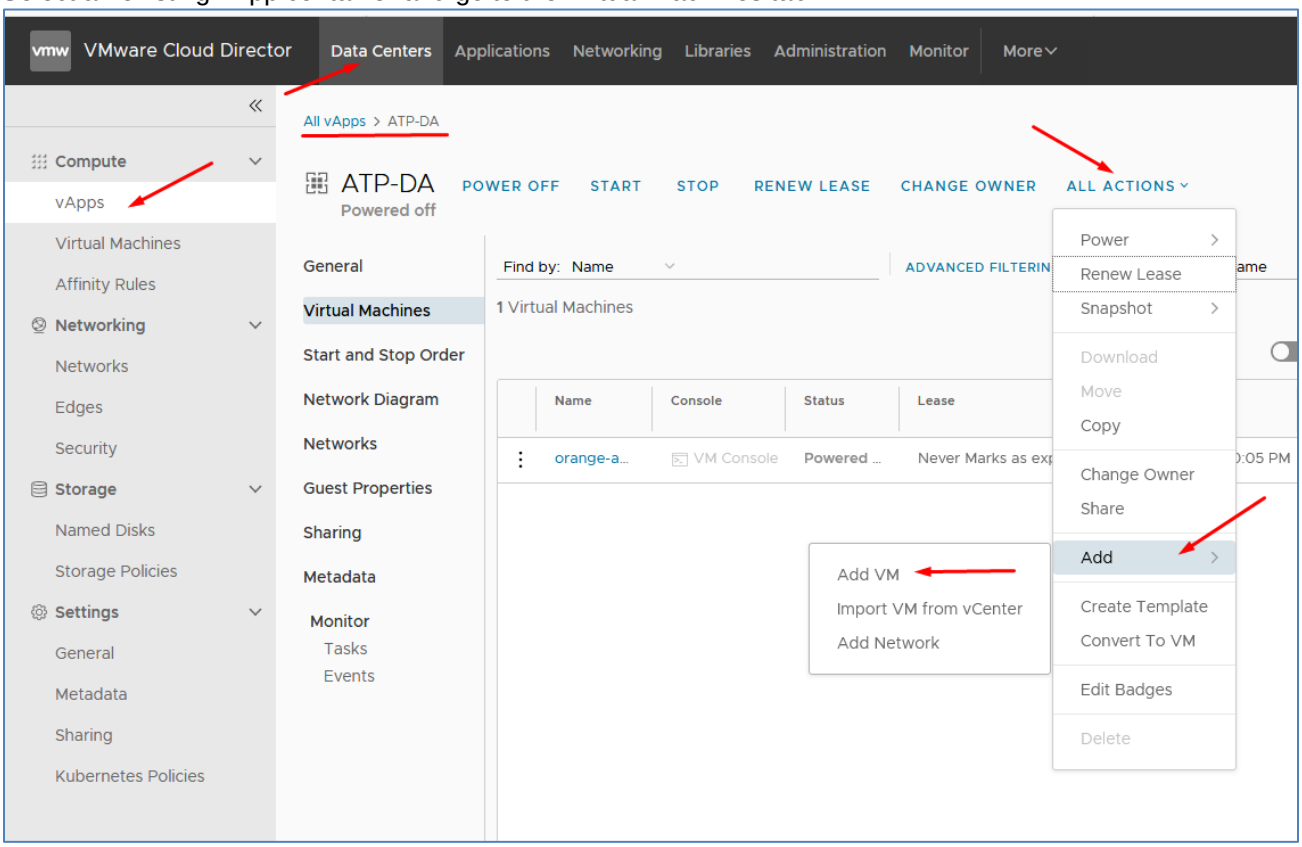


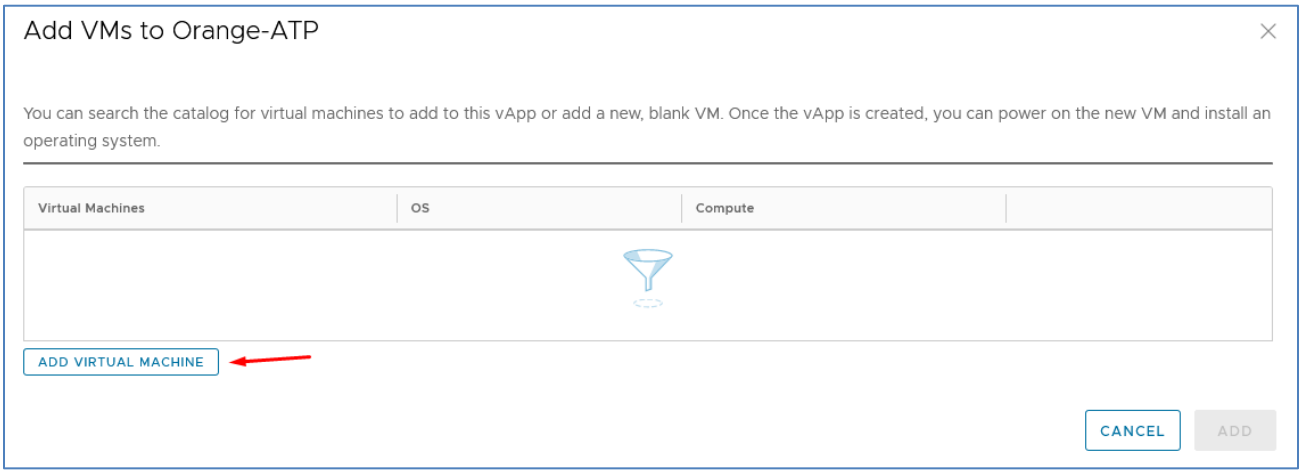
In the Add Virtual Machines tab, you can:

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

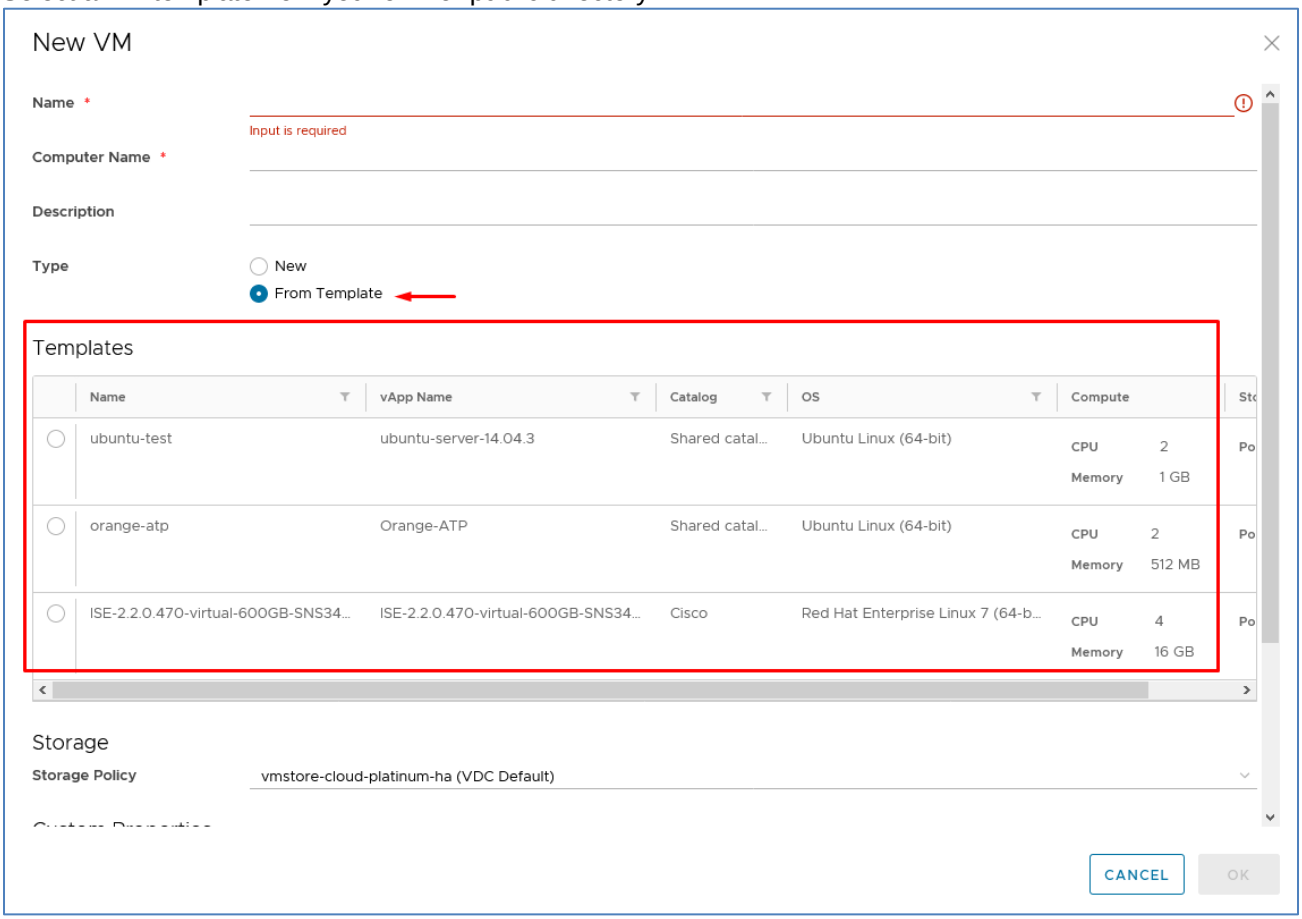
12.2. Creating a virtual machine from a template

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

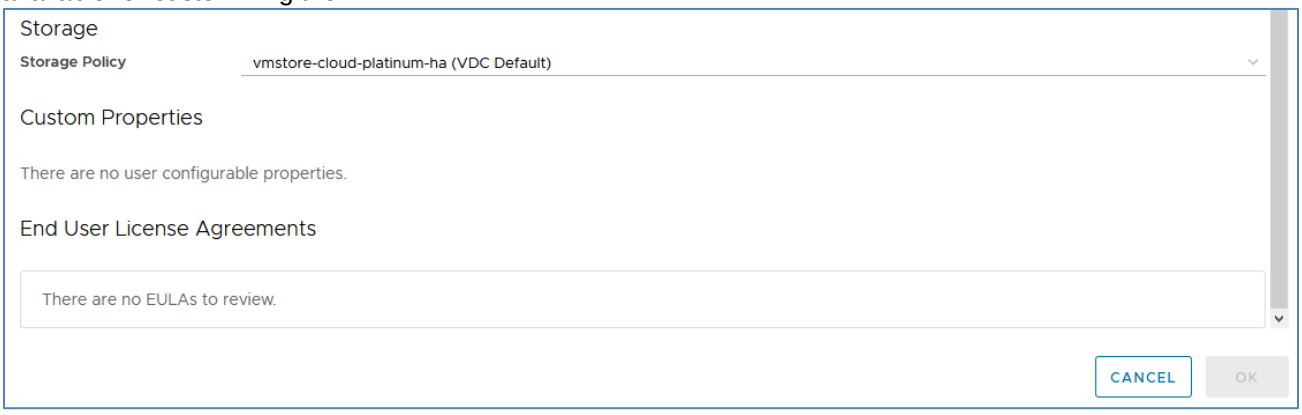




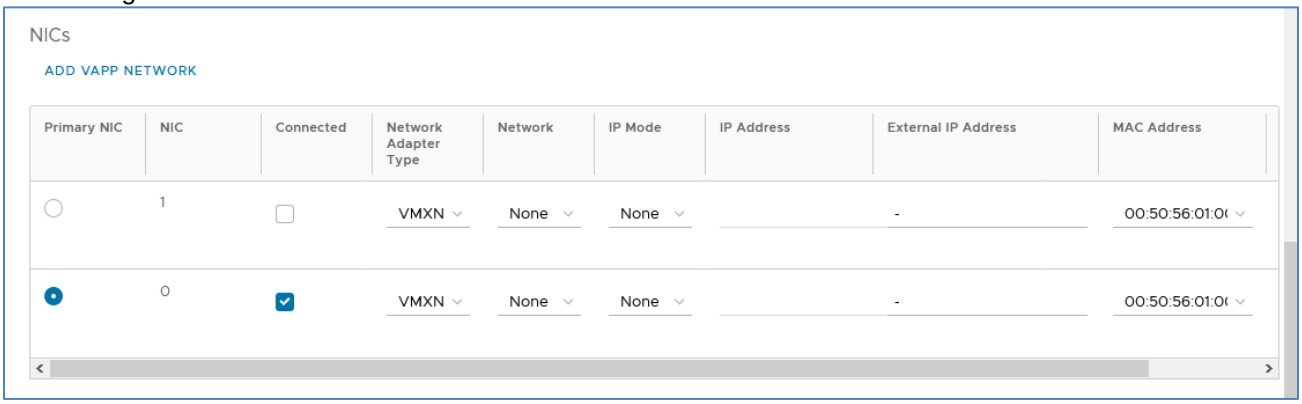
Select a VM template from your own or public directory:



Next, set the VM storage location and other parameters. Depending on the type of template, certain parameters are available for customizing the VM:

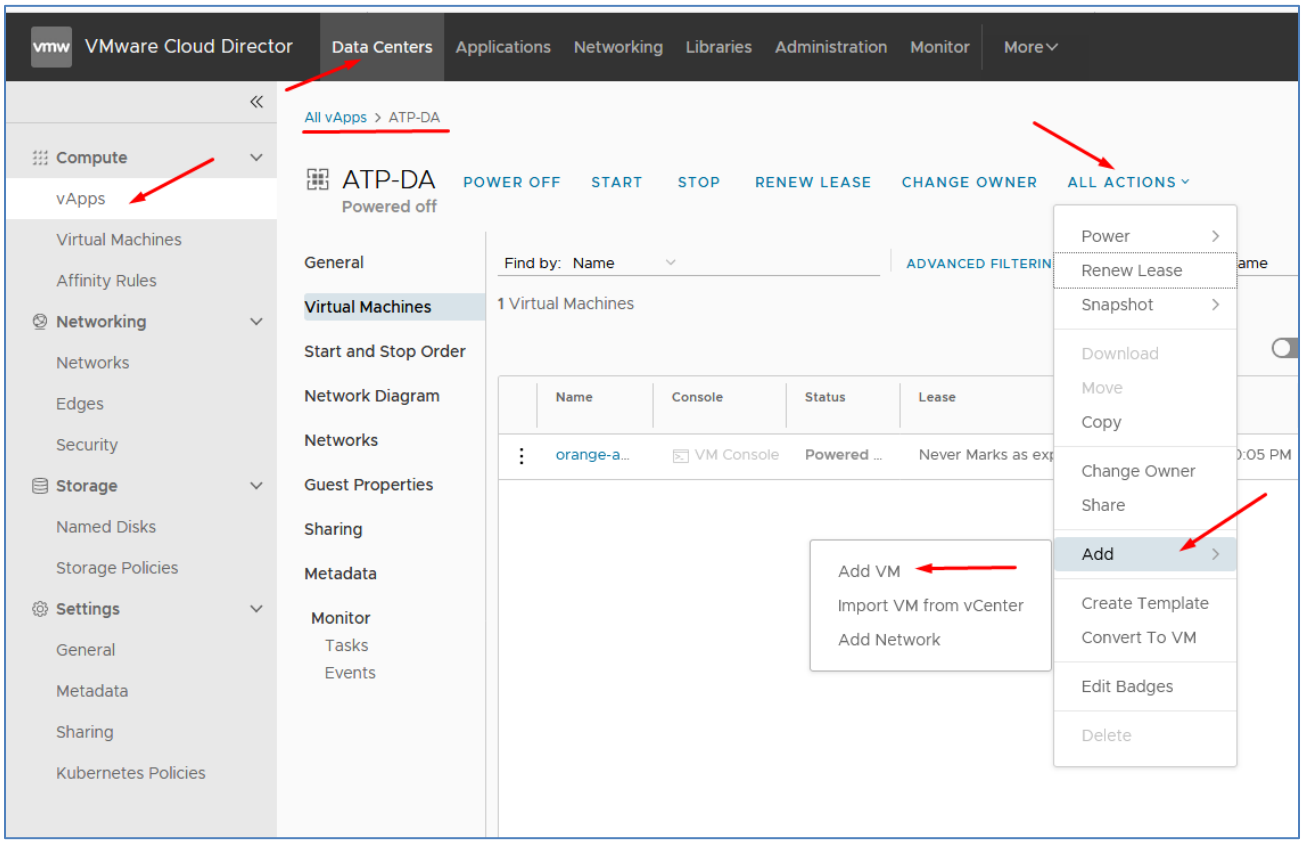


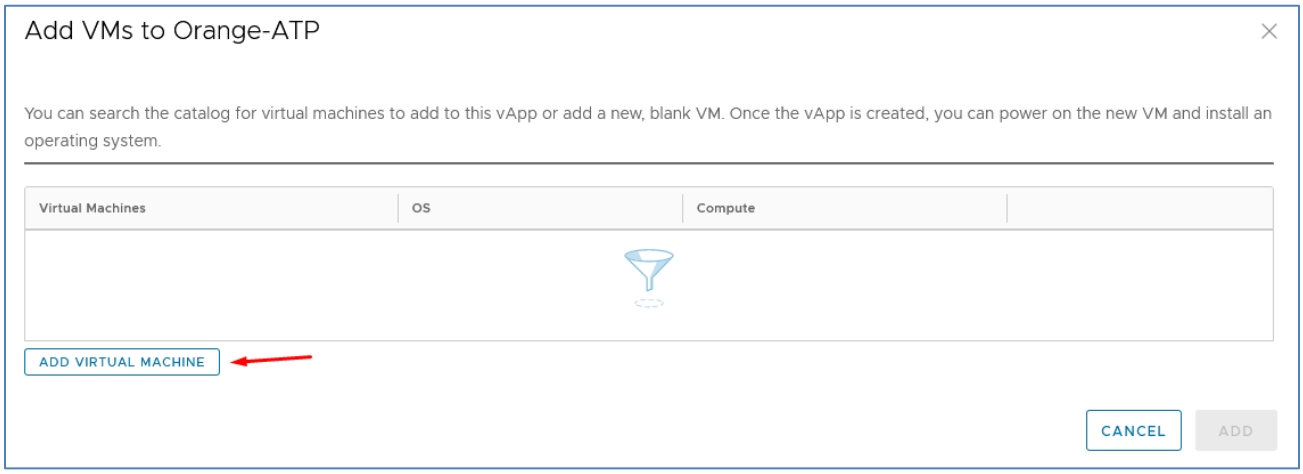
Connecting to networks:

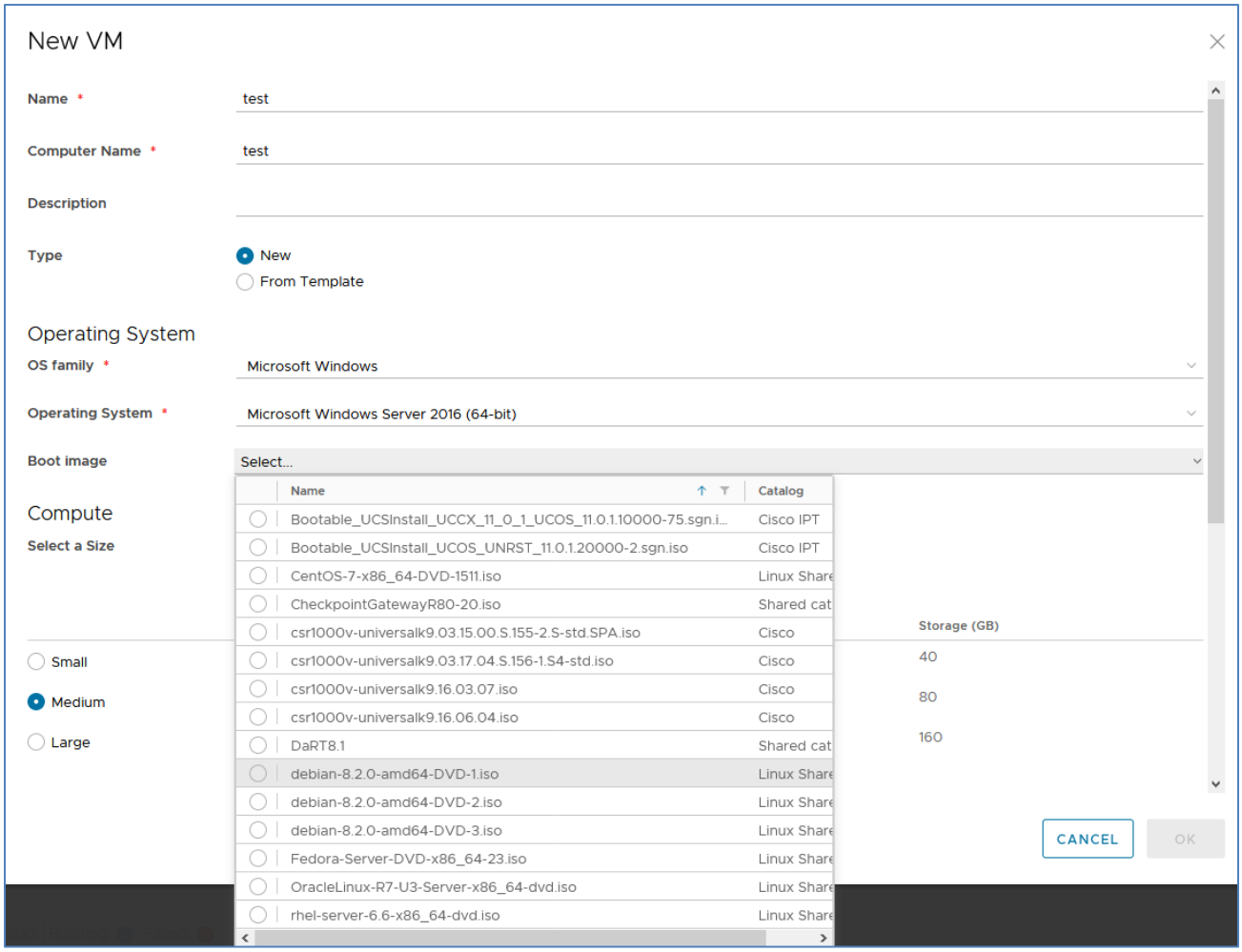


Check the parameters and complete the creation of the VM by pressing the Finish button.

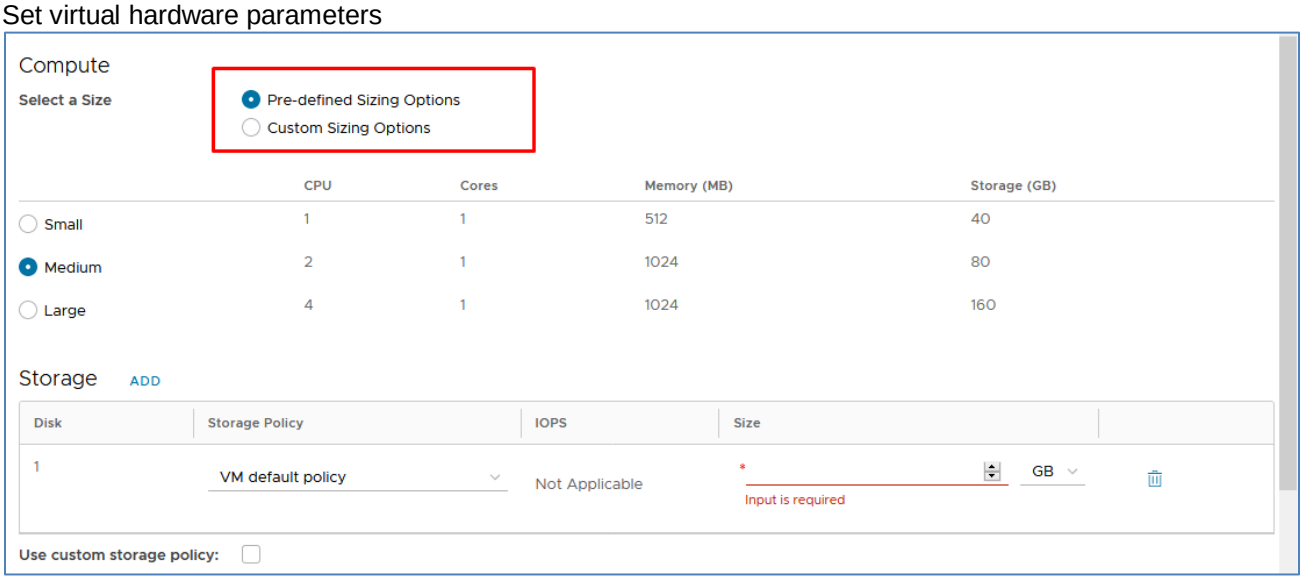
12.3. Creating a virtual machine from scratch



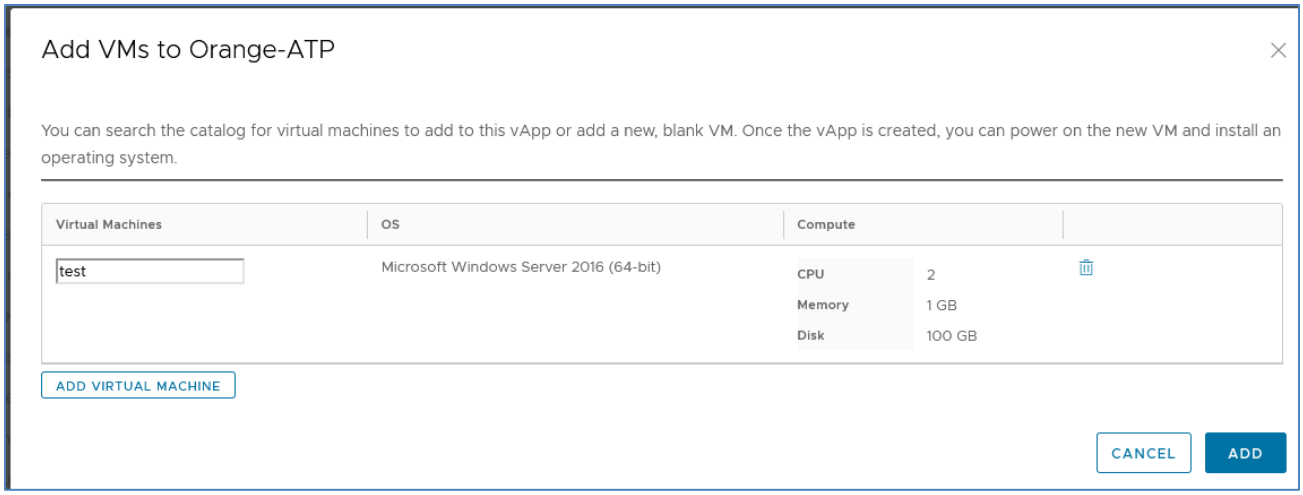




Set virtual hardware parameters



The new VM will appear in the list



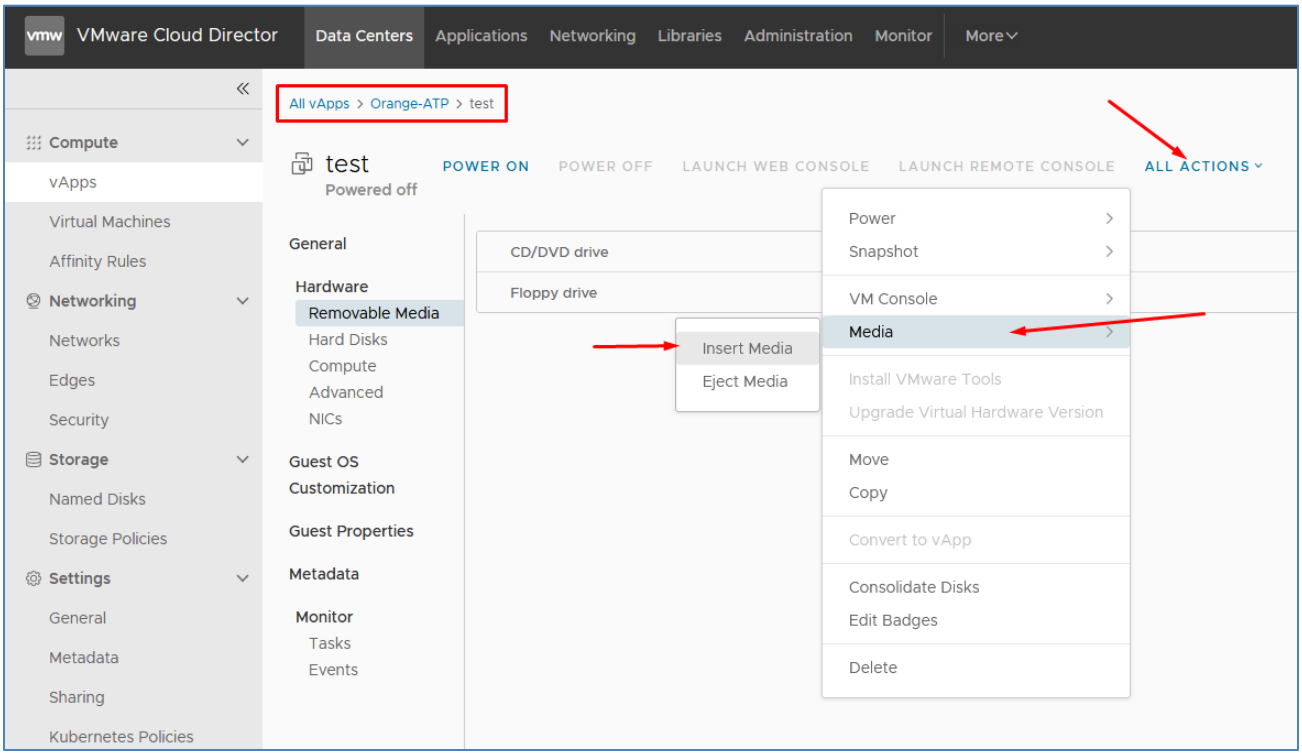
You can add another VM immediately.

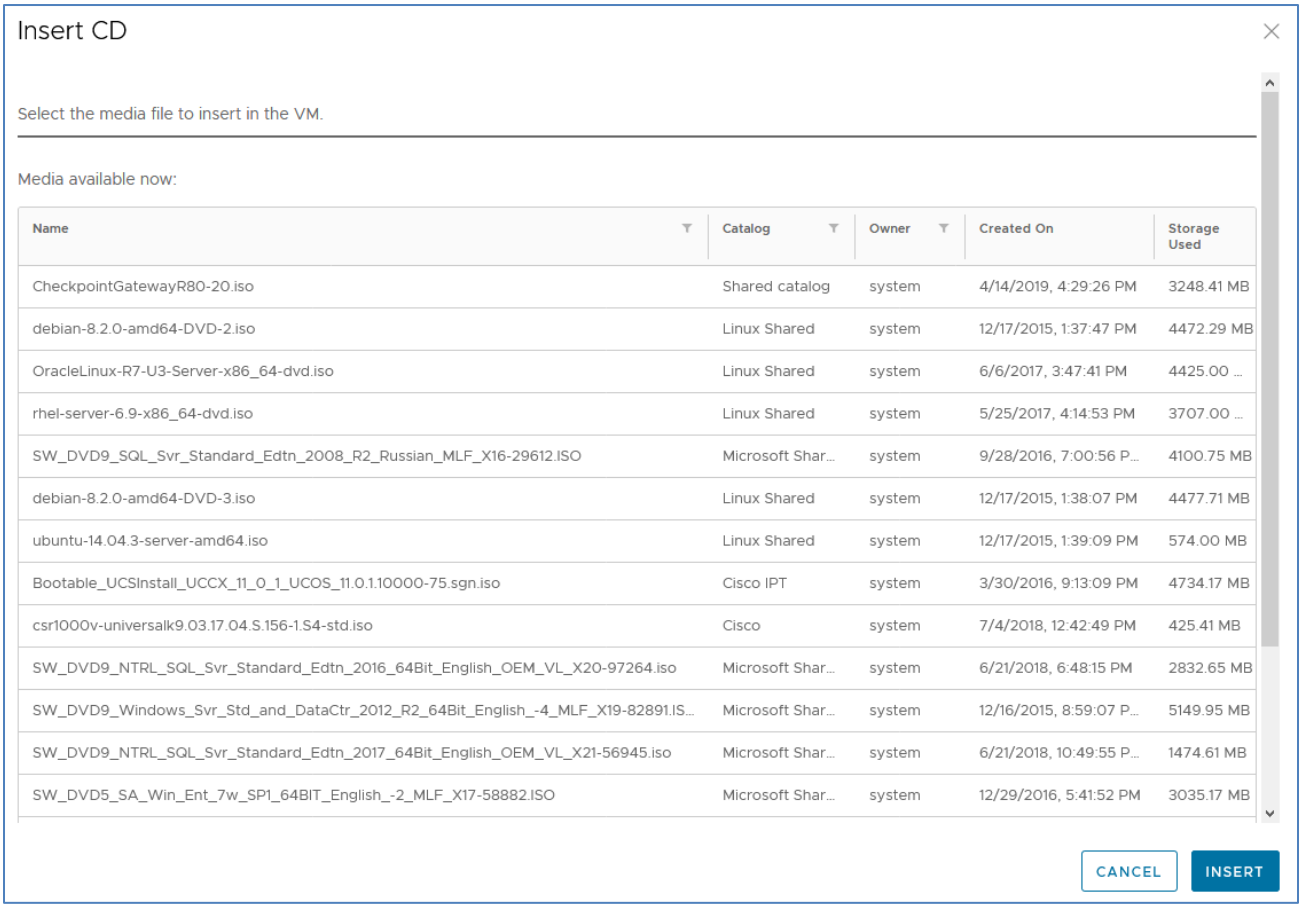
12.4. Installing an OS on a virtual machine

To install the OS on a ready-made virtual machine, you need to connect the ISO image of the installation disc. This can be done from a local disk or a vCD directory.

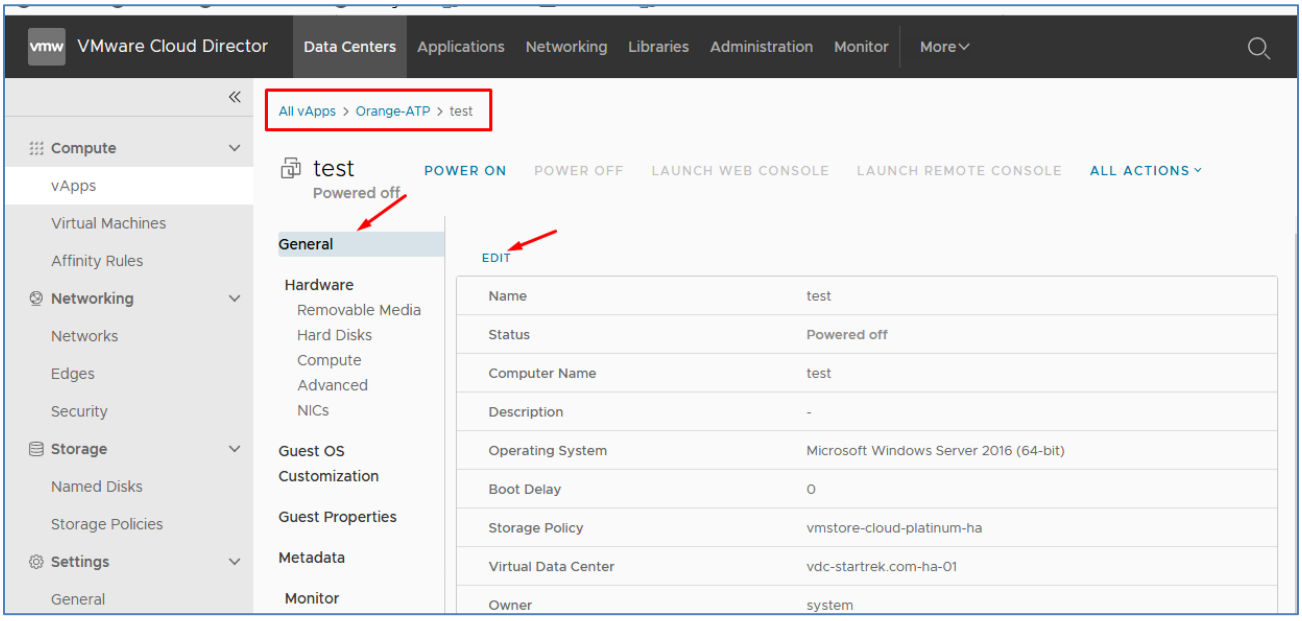
Starting from vCloud 10.0, there is no way to connect images via VMRC or a web console, as the old FLASH interface was removed.

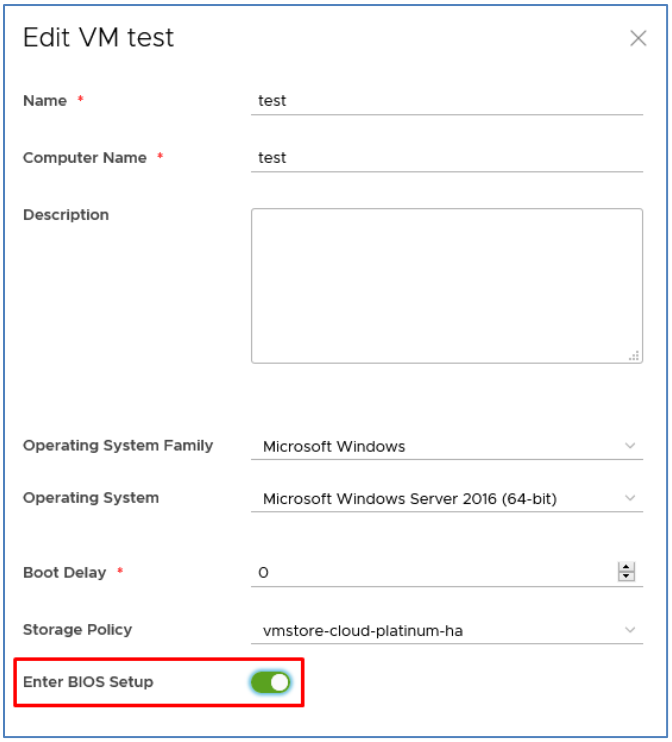
It is assumed that a directory has already been created and the correct ISO image from the installation disc has been loaded into it.
Select Insert Media from the VM context menu:





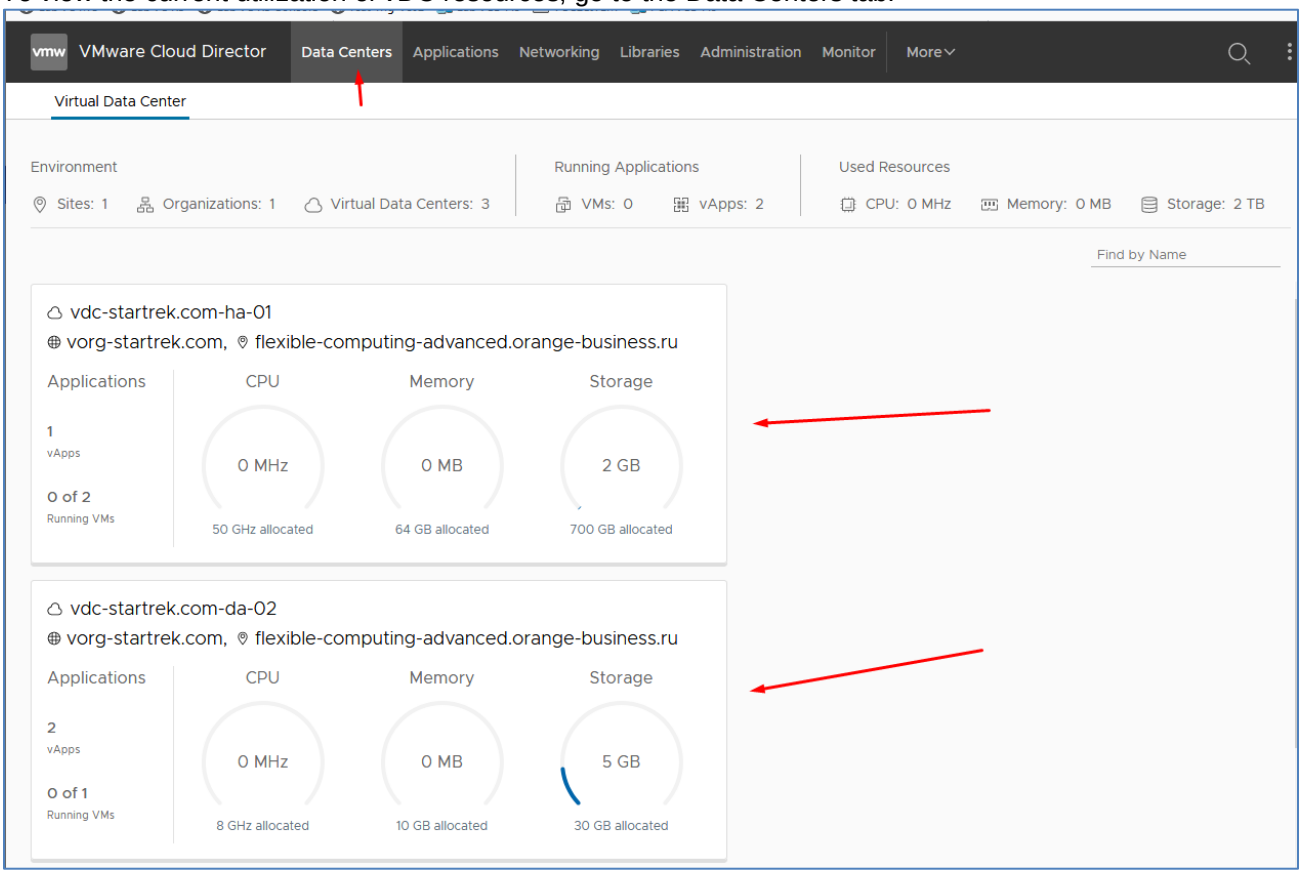
By default, the DVD drive appears in the boot list, but not as the first item. If there is a need to change the boot order, you need to do it through BIOS/UEFI. For this, you need to set the option to automatically enter BIOS/UEFI the next time the VM is turned on:



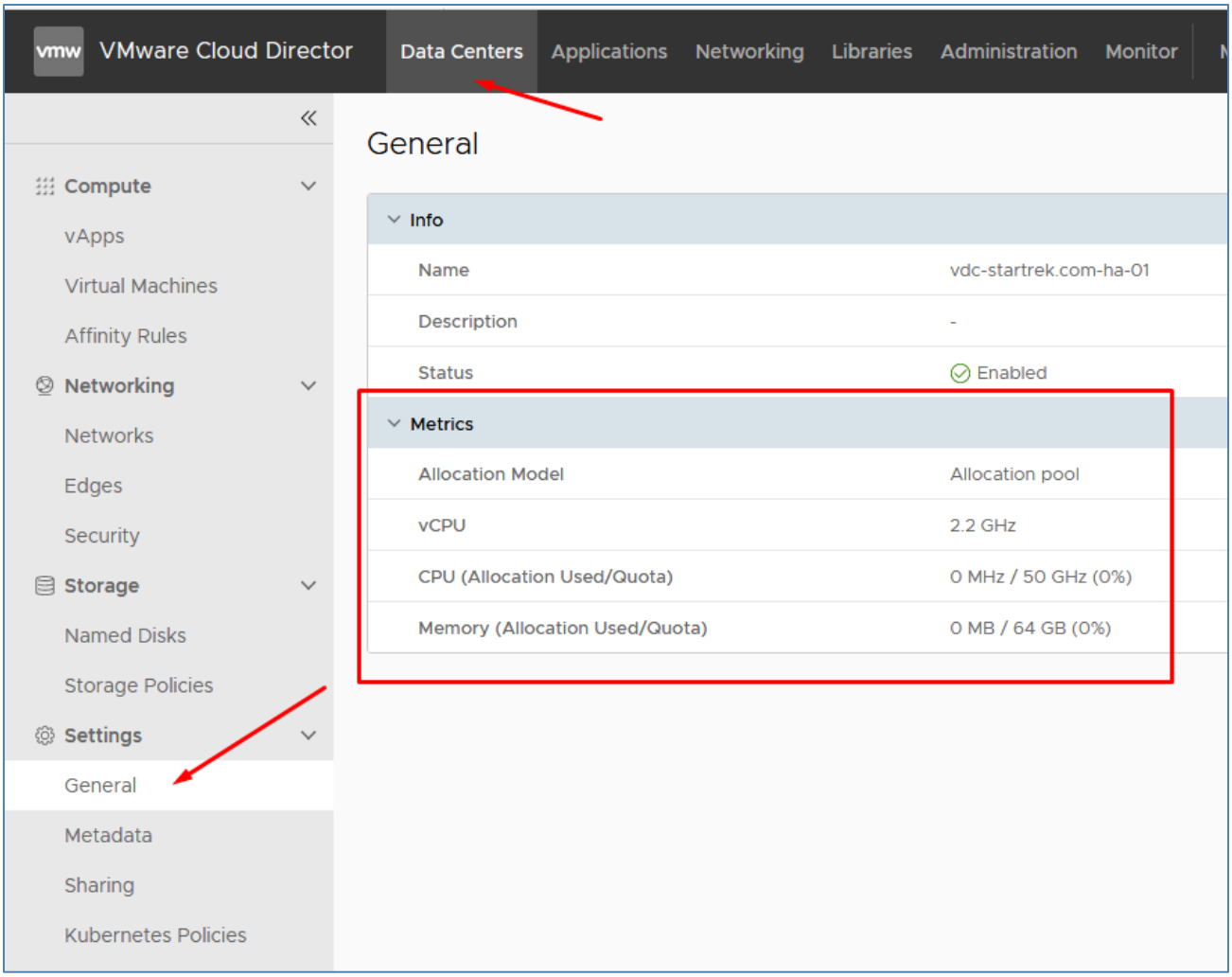


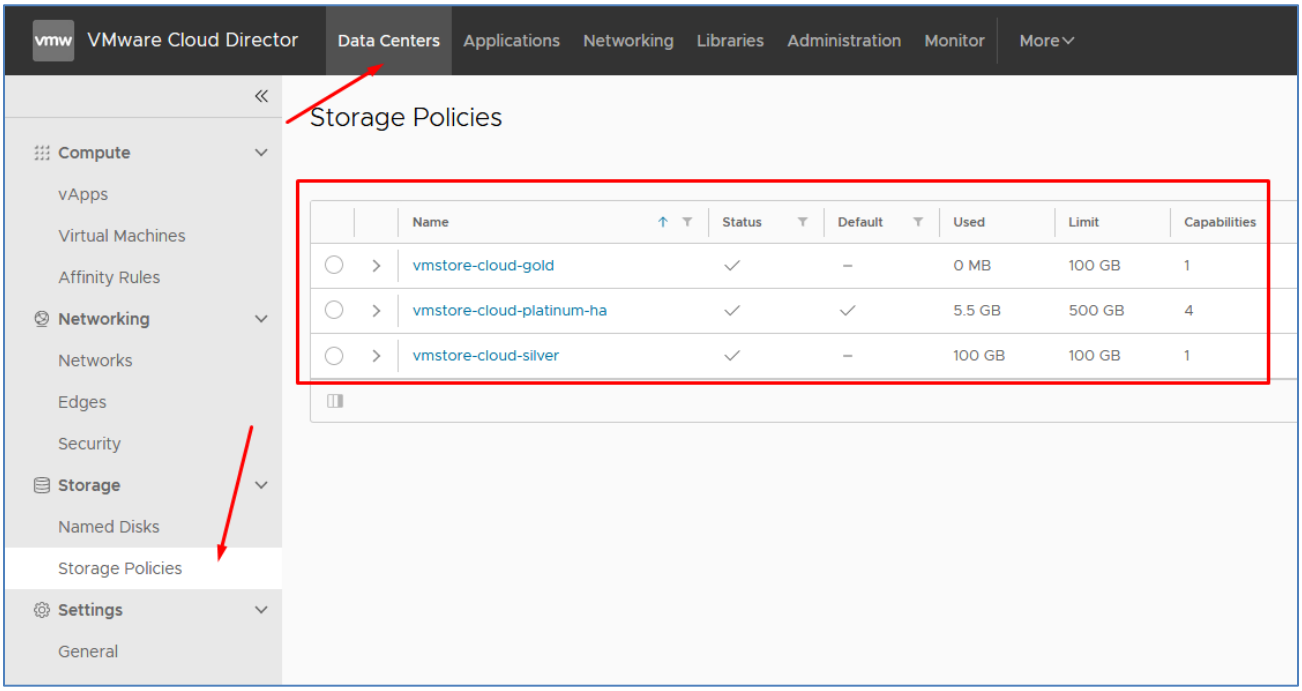
12.5. Resource monitoring

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



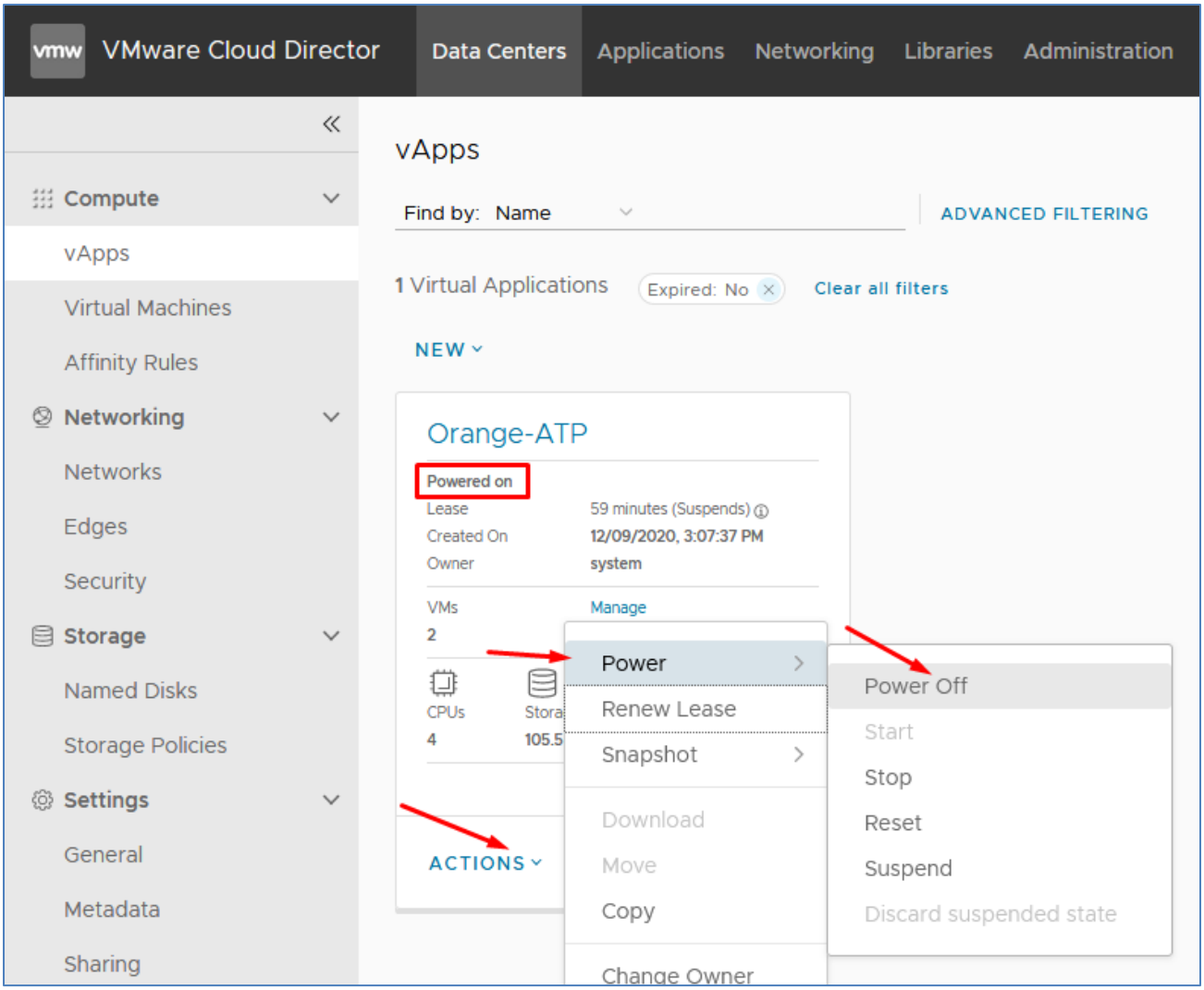
More details can be viewed inside the vDC:





12.6. Exporting a vApp template from vCloud 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

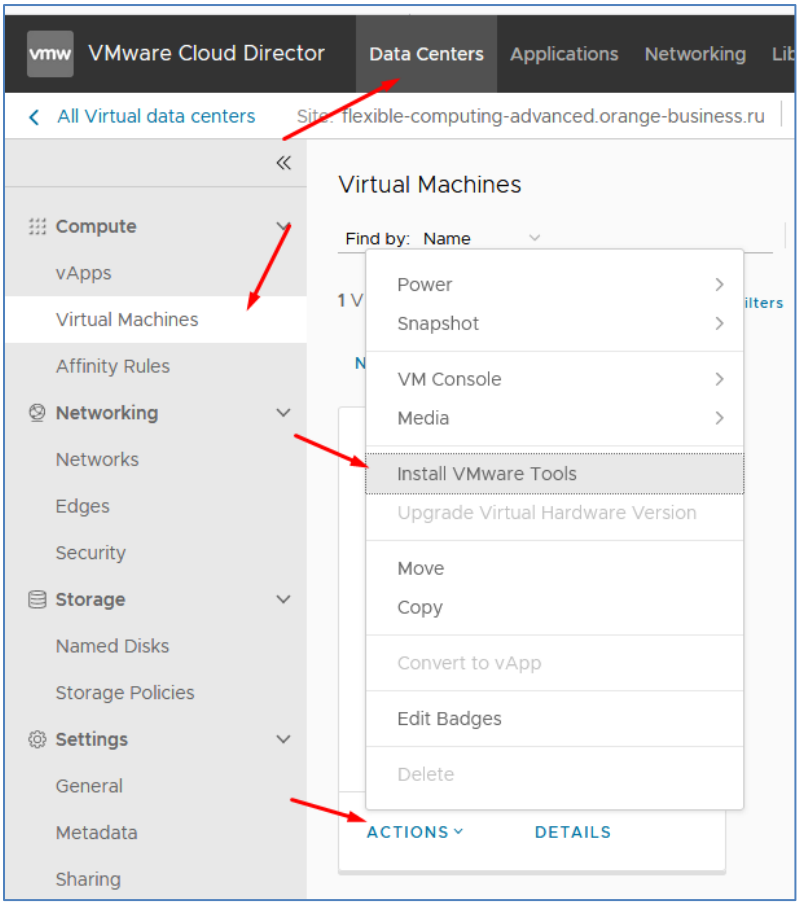
12.7. Installing VMware Tools on a VM

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.

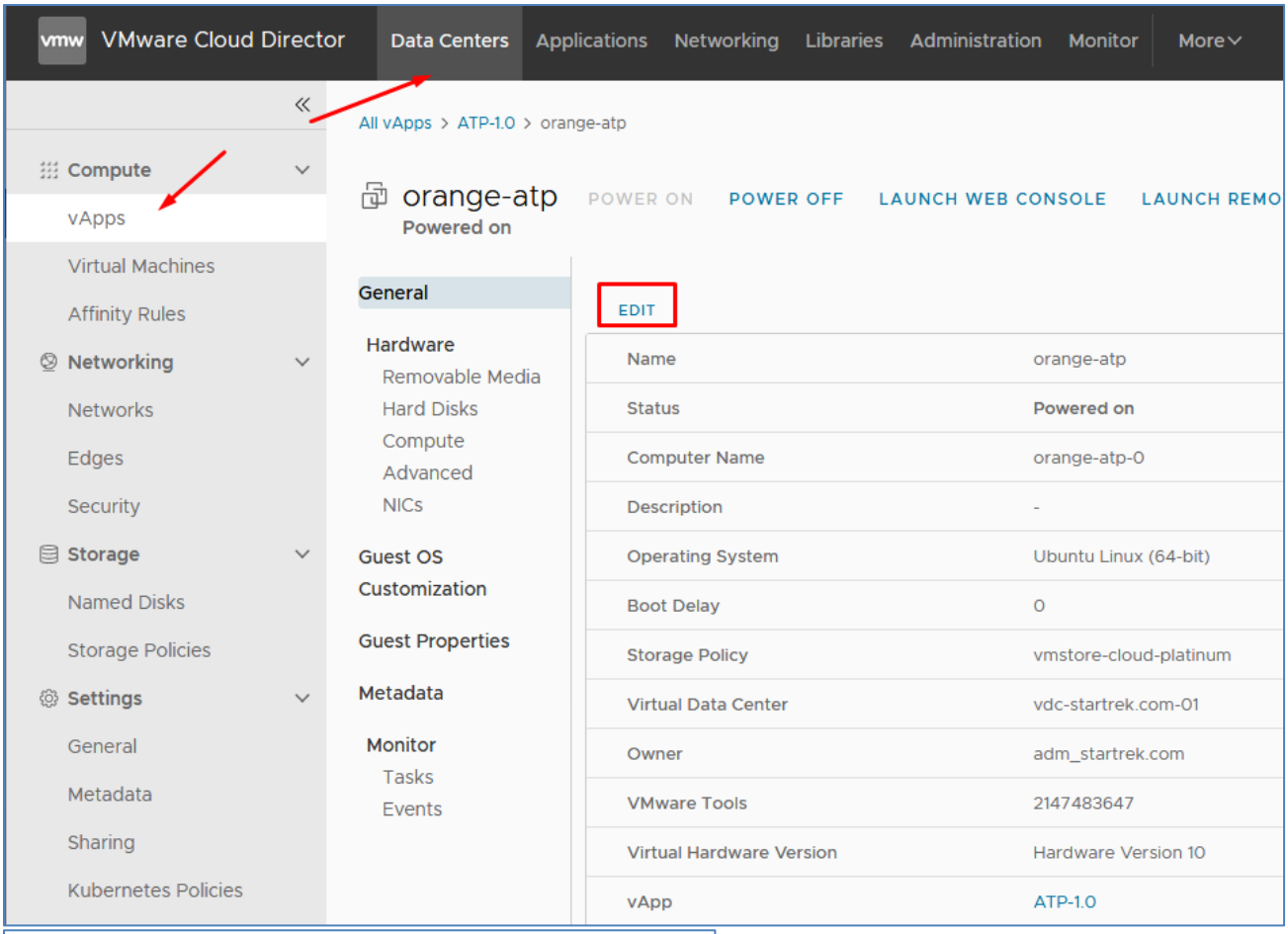
For up-to-date and detailed instructions, click here.
To mount an ISO image from VMware Tools to a VM, right-click on the VM and select Install VMware Tools. This will mount the ISO image to the VM, after which you need to install it on the OS.

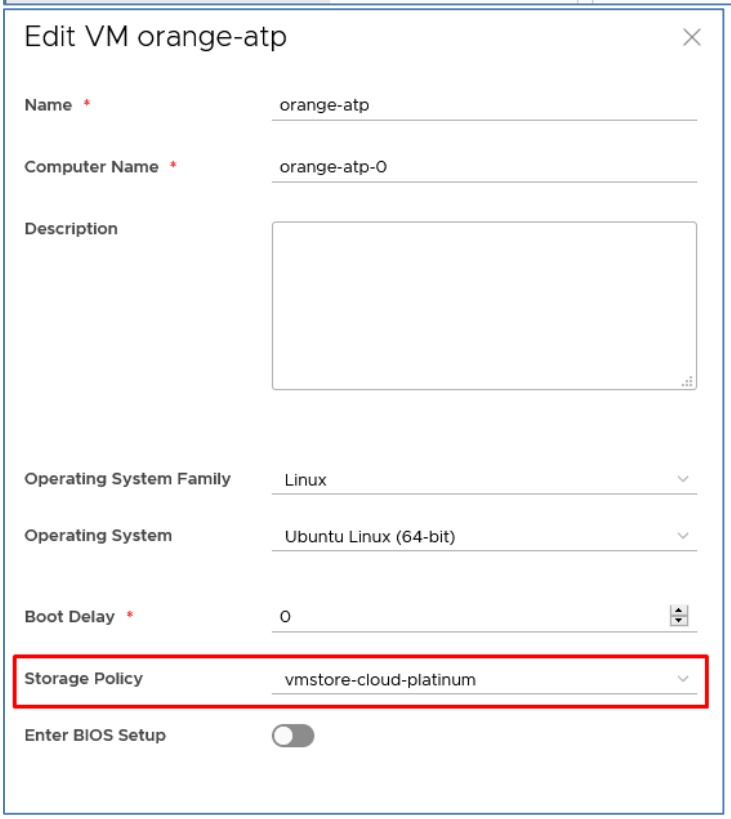


12.8. Selecting storage type for VM

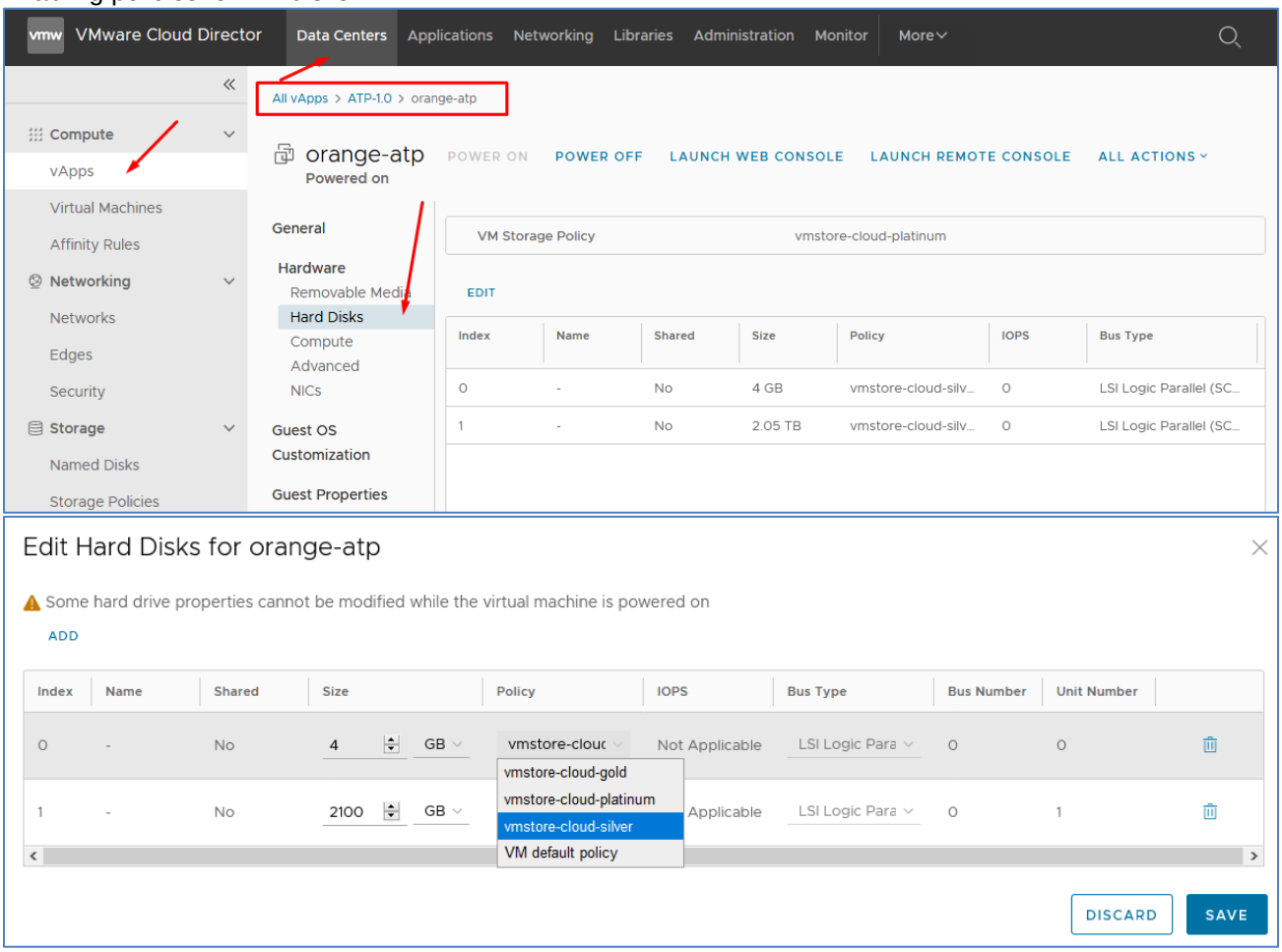
The type of storage system used for a VM is set by enabling the necessary policy for disks and for the vm home object (VM metadata). Metadata must use the same policy as the main VM disk.

From the VM context menu:





Enabling policies for VM disks:



(Use VM default) means the same policy as for metadata.

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. *Note: Similar problems have been observed in Windows 7 and Server 2008R2.*	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	-