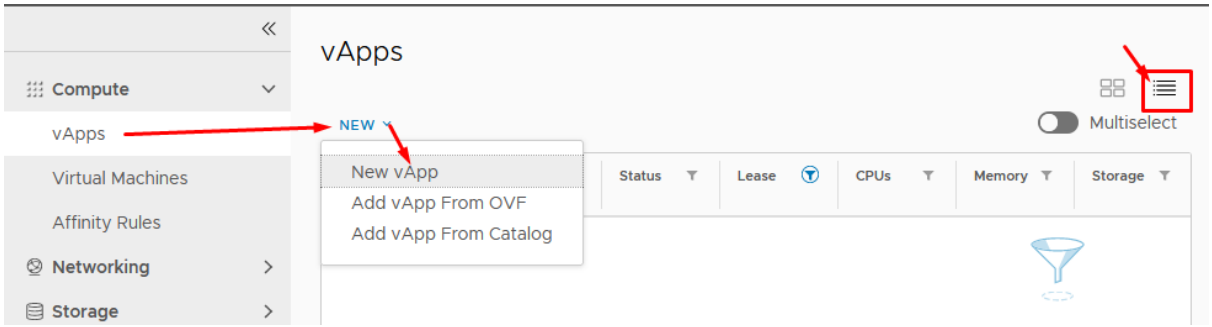
vCloud Director 10 HTML5 F.A.Q.

Content

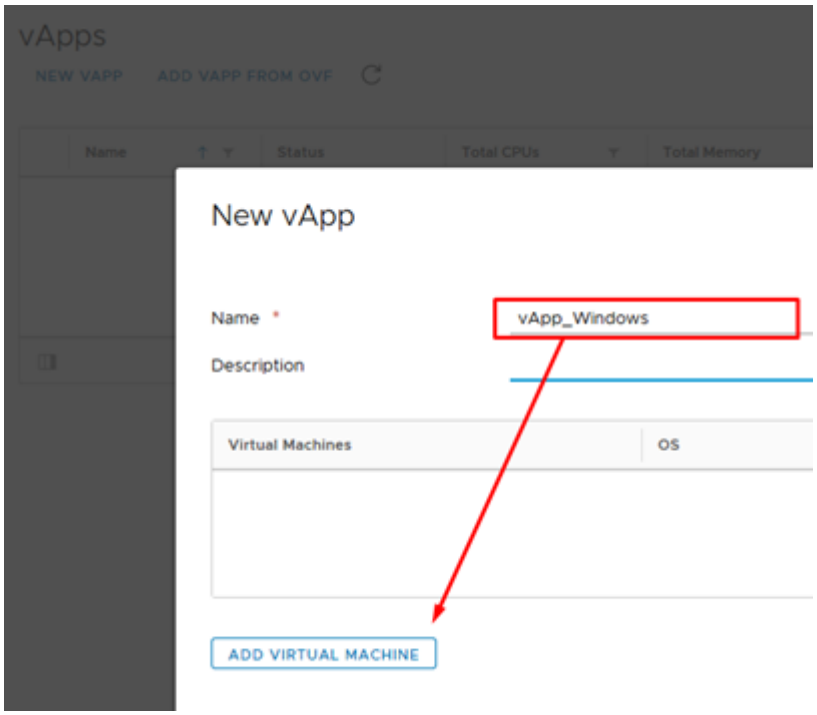
Virtual machine creation from template

If you want to create a virtual machine, please login to your cloud organization. Go to your vDC.

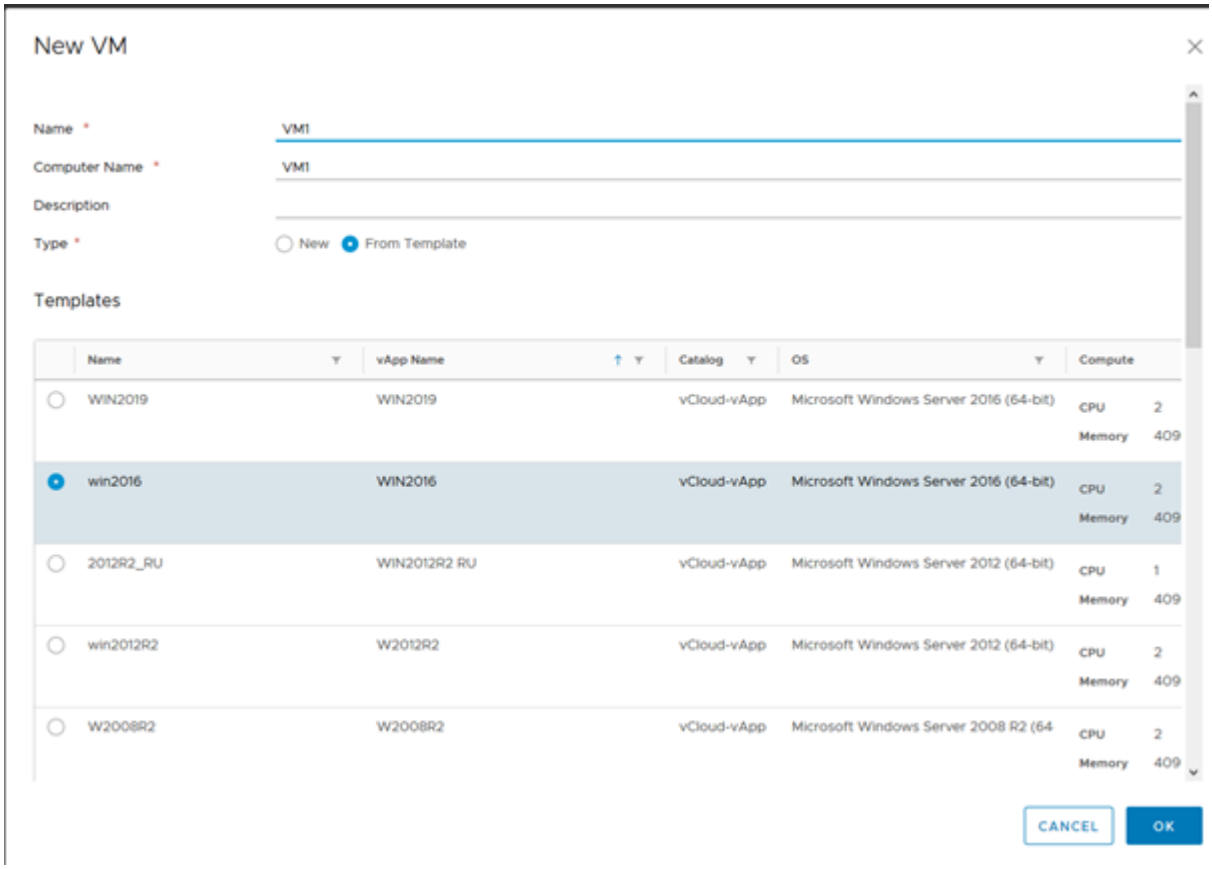
1. Create a catalog for virtual machine, vApps > NEW VAPP.



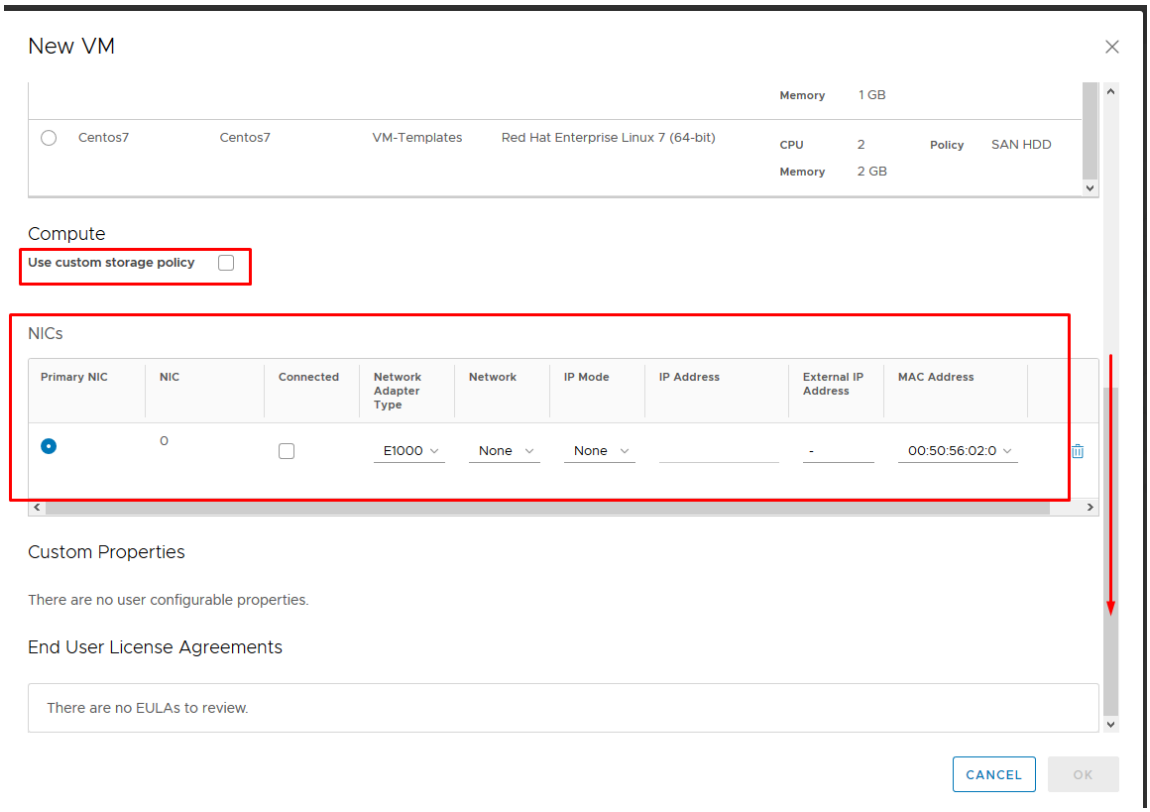
2. Enter catalog name. Add virtual machines from our templates to the catalog - select ADD Virtual Machine.



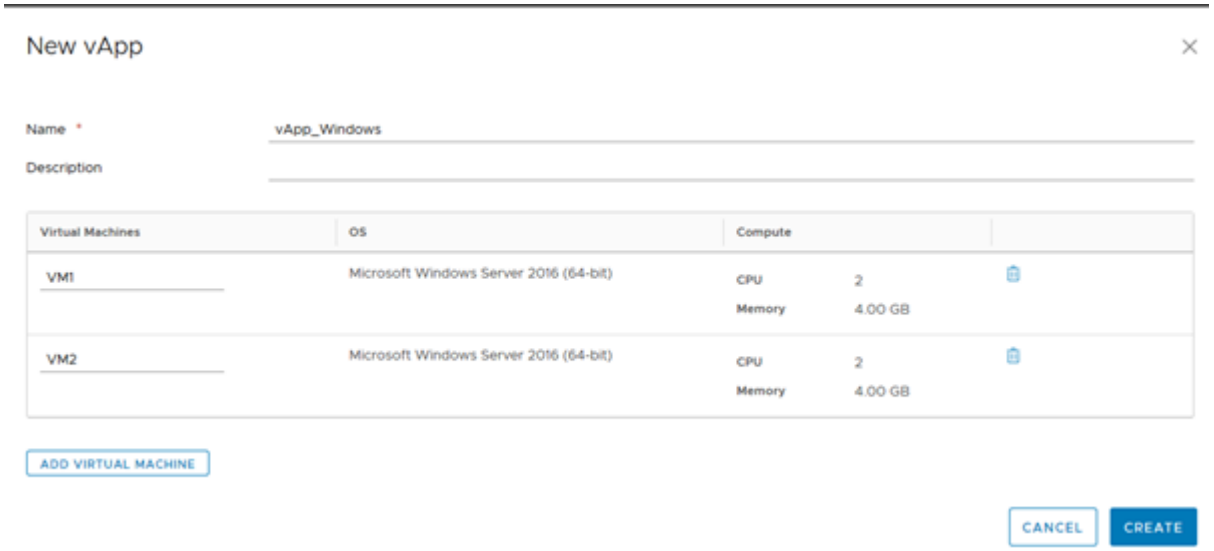
3. Select „From Template“, enter mandatory information.



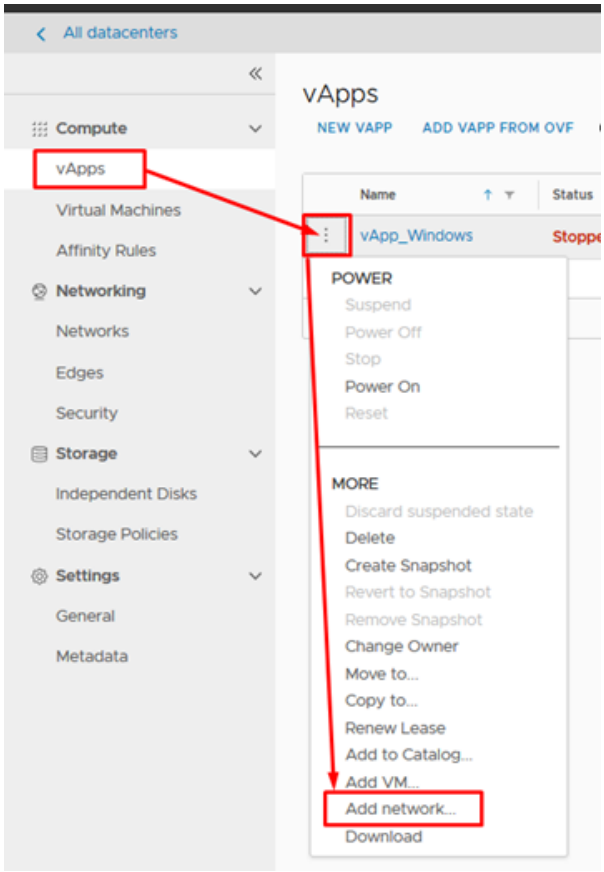
At the bottom of the window you can choose Storage policy -> „Use custom storage policy“. You can add network to a virtual machine. Press Ok.



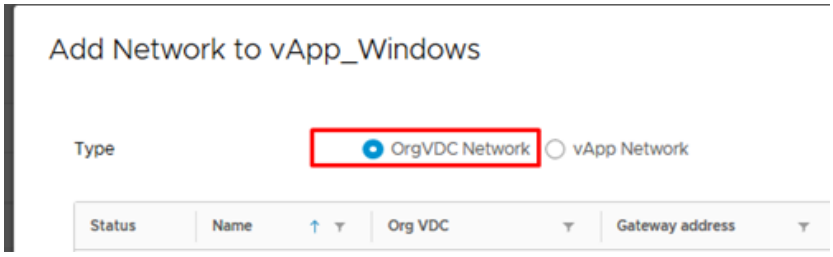
4. Press Create after adding all the needed virtual machines.



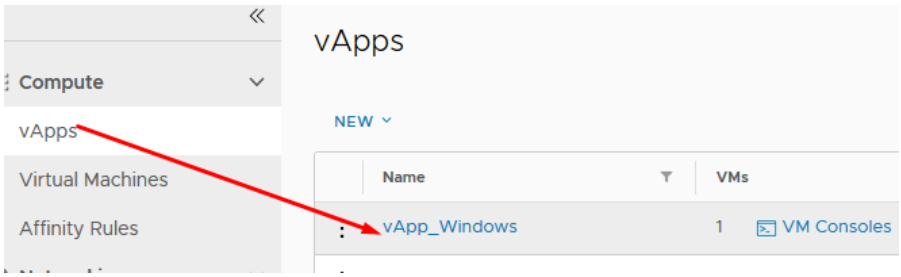
5. Add a network to vApp for virtual machines.

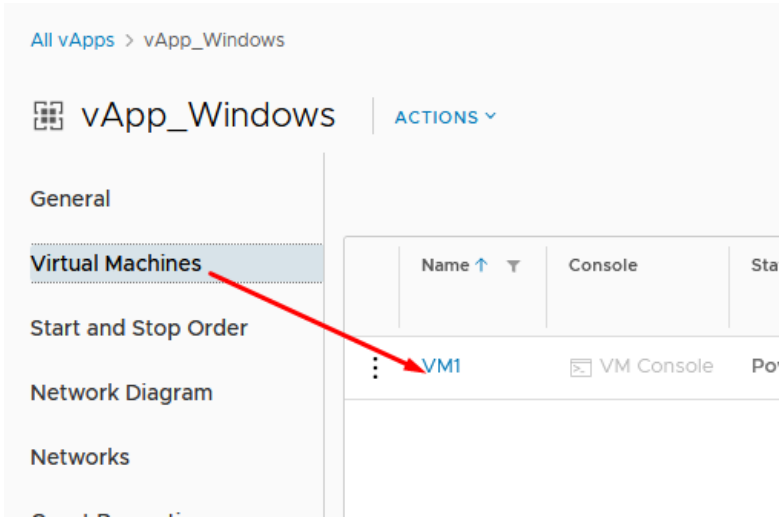


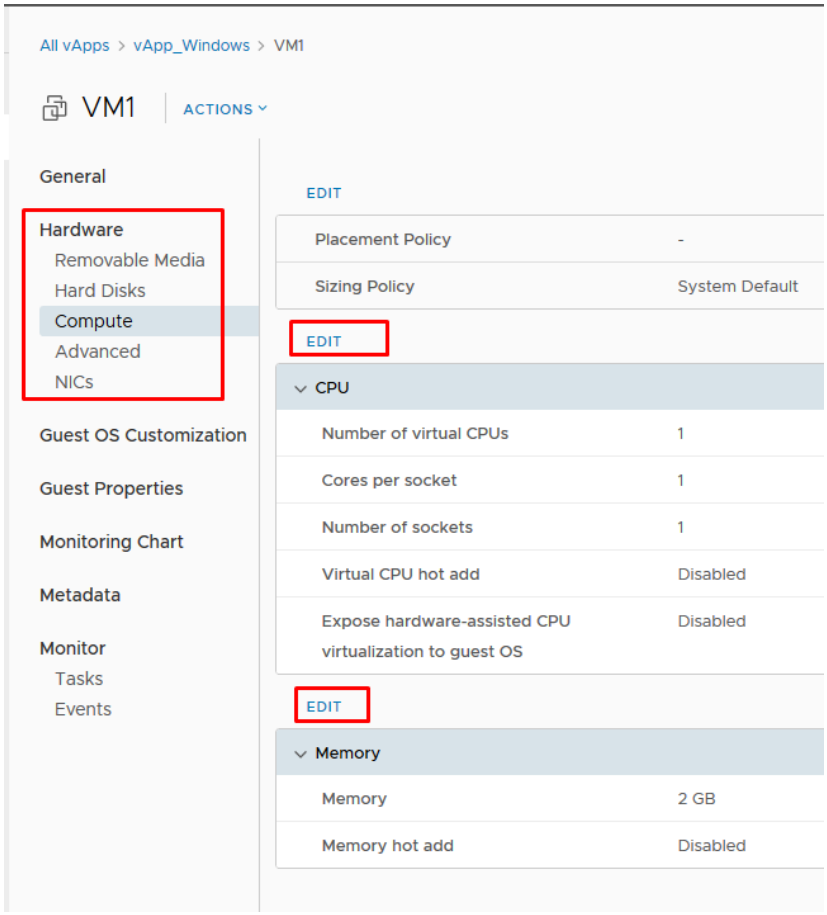
Select OrgVDC Network and add desired network.



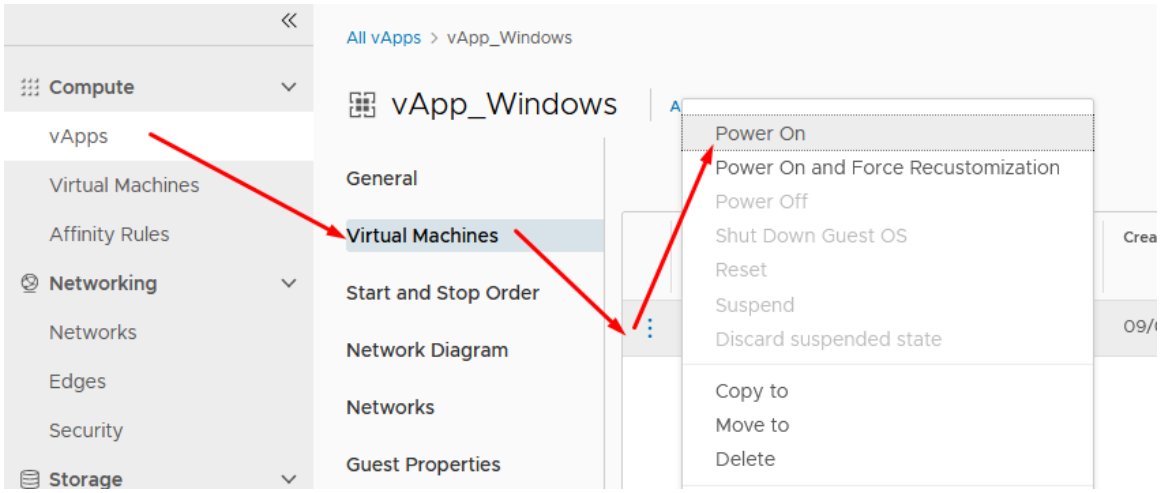
6. You will be able to see the created VMs in the vApp. If you go to virtual machine „Details", there you can change VM resources, add additional network and connect it. Also you can see initial virtual machine password there (we recommend changing administrator password from OS).



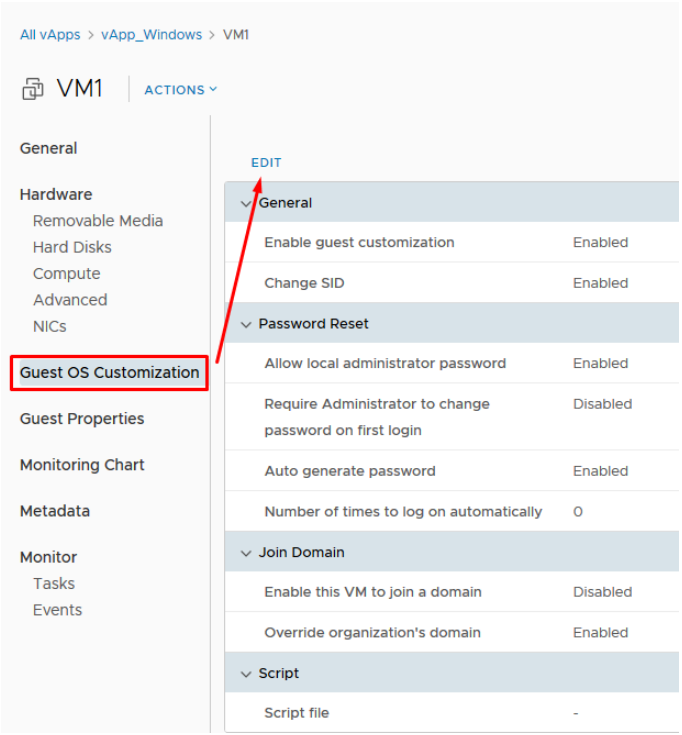


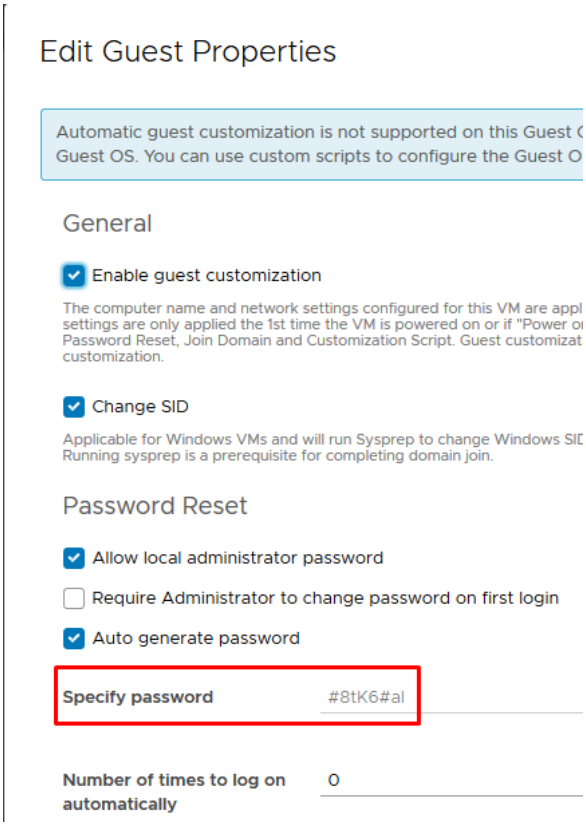


7. Power on the virtual machine.



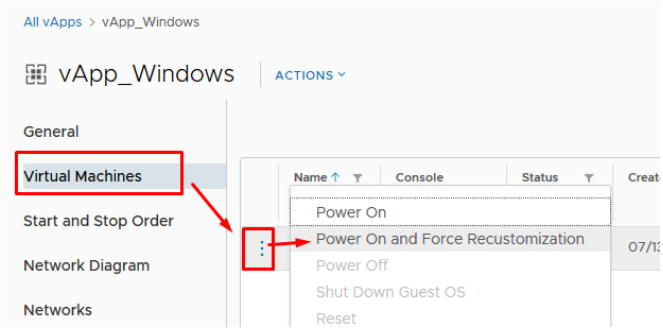
8. In Guest properties “Specify password” you can see Administrator or root user password.





If you cannot see a generated password, please make sure that in “Edit Guest Properties” you can see these attributes as marked: “Enable guest customization”, “Change SID”, “Allow local administrator password”,”Auto generate password”. After that press Save.

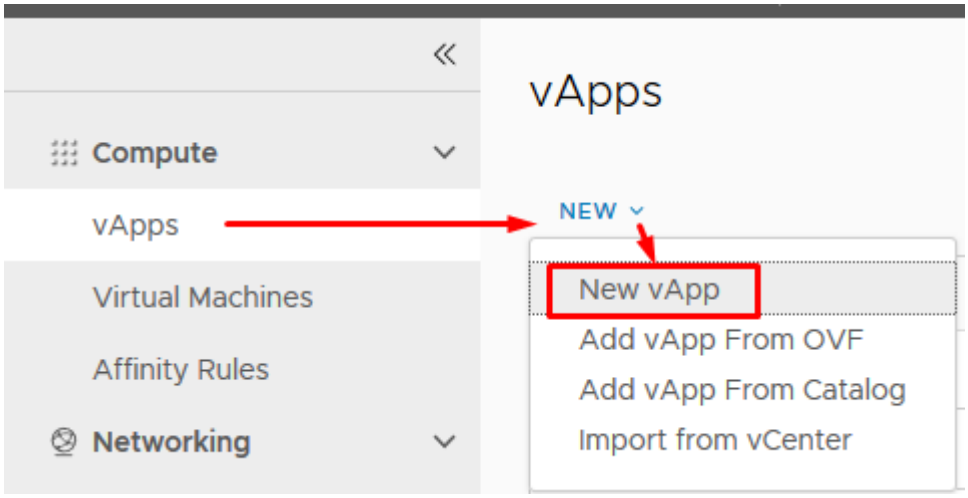
You may want to manually run “customization” process in order to generate and set a new password, then please turn off the virtual machine and press „Power On and Force recustomization“. After customization process is done, we recommend unmarking the attribute “Enable guest os customization”.



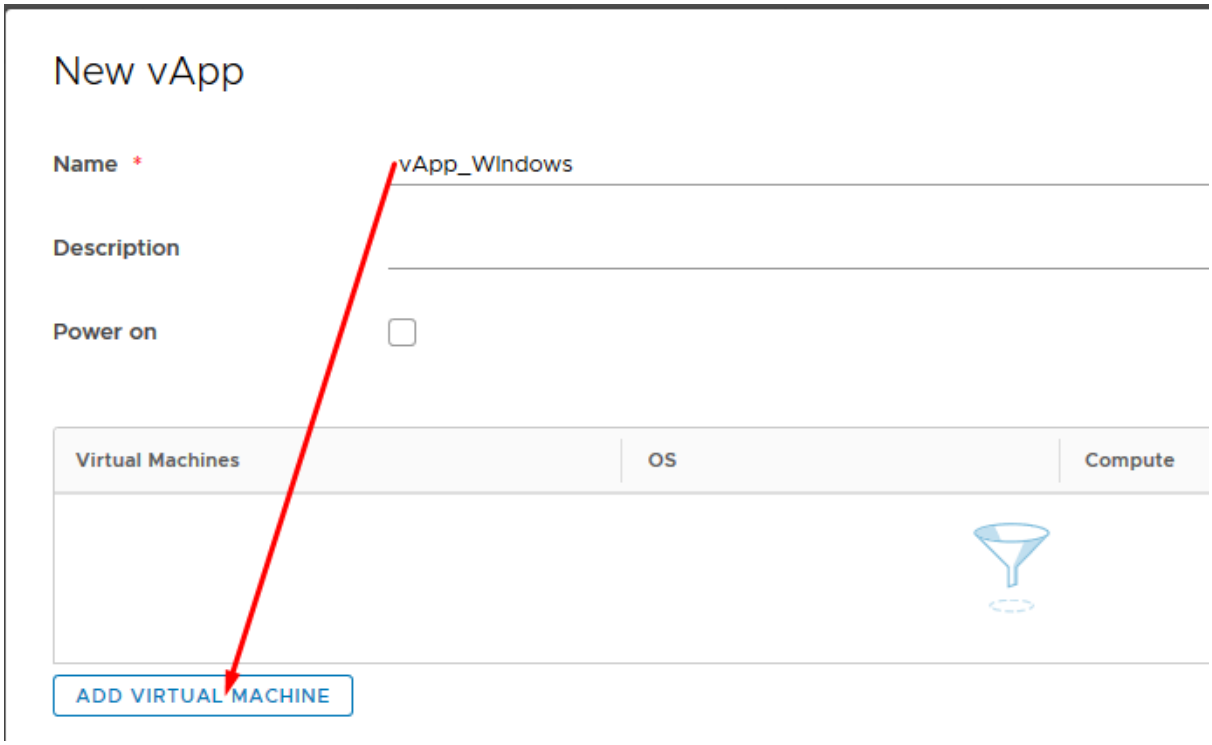
Virtual machine installation using ISO

To install a virtual machine using ISO, please connect to your cloud organization.

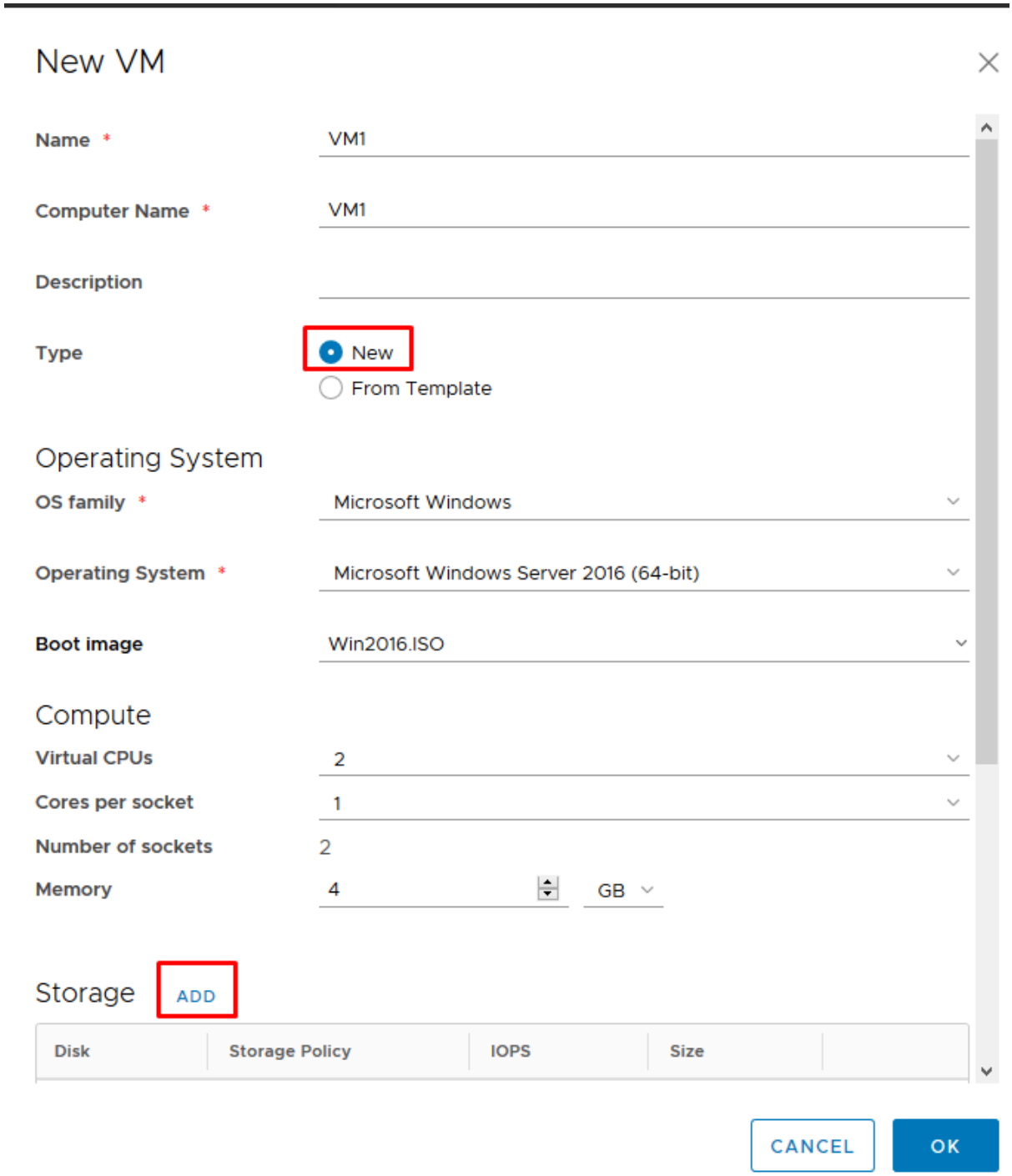
1. Create a catalog for your virtual machine, vApps > NEW VAPP.



2. Enter catalog name and press „Add virtual machine".



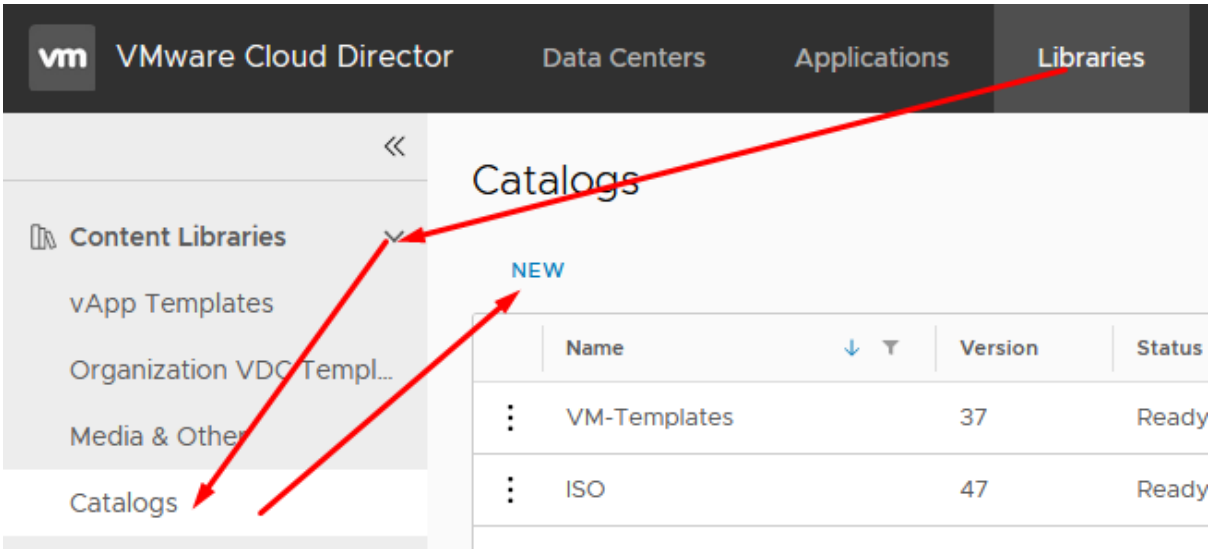
3. Enter mandatory fields, select type New, select OS type, choose desired resources, add Storage, choose an organization network and press Ok.

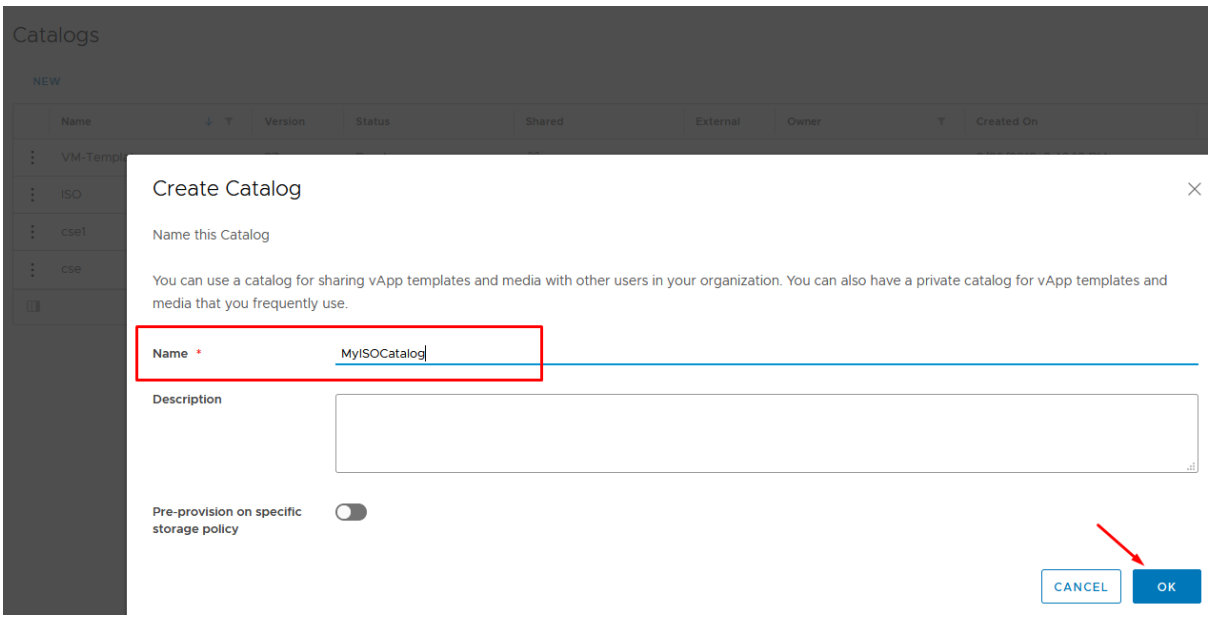


4. Open virtual machine console and follow OS installation wizard.

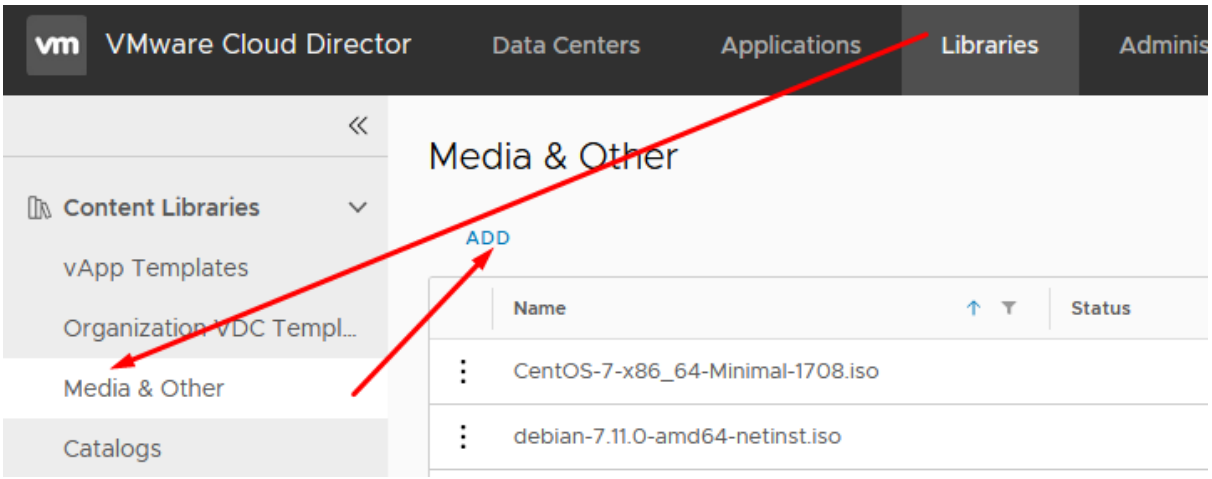
Importing media to a catalog

1. Create a new catalog and go to step 2 in case you want to import a media.

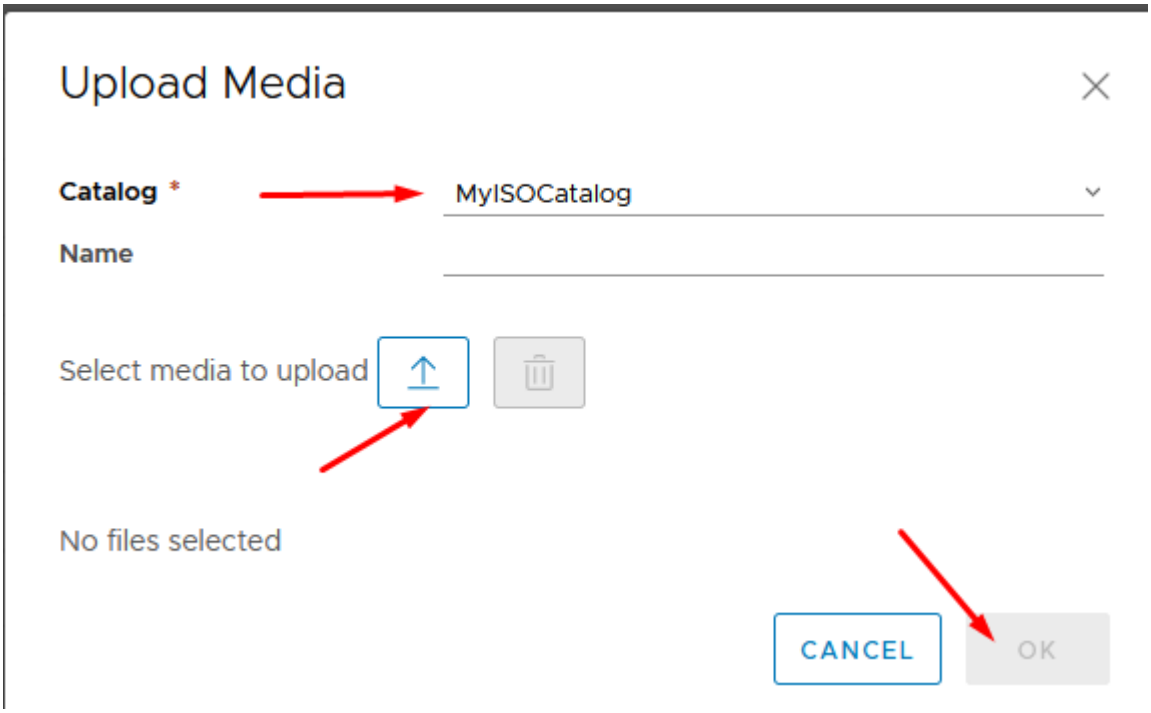




2. Import media.

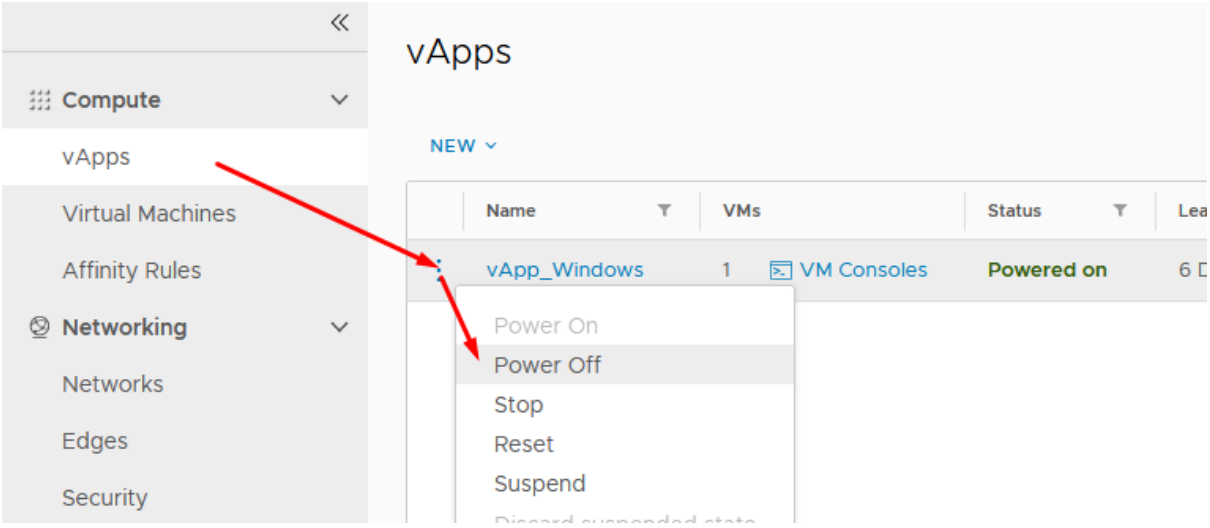


3. Select catalog for media import and press Upload. Enter media „Name" and press OK.

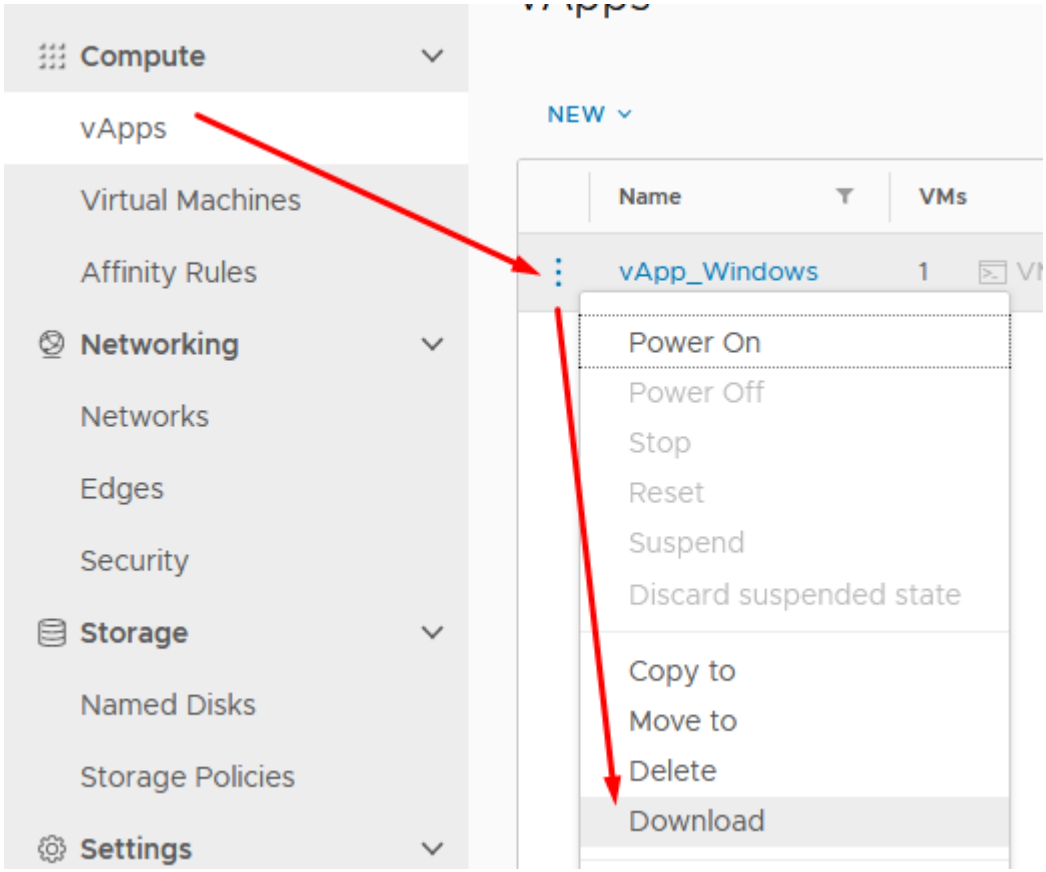


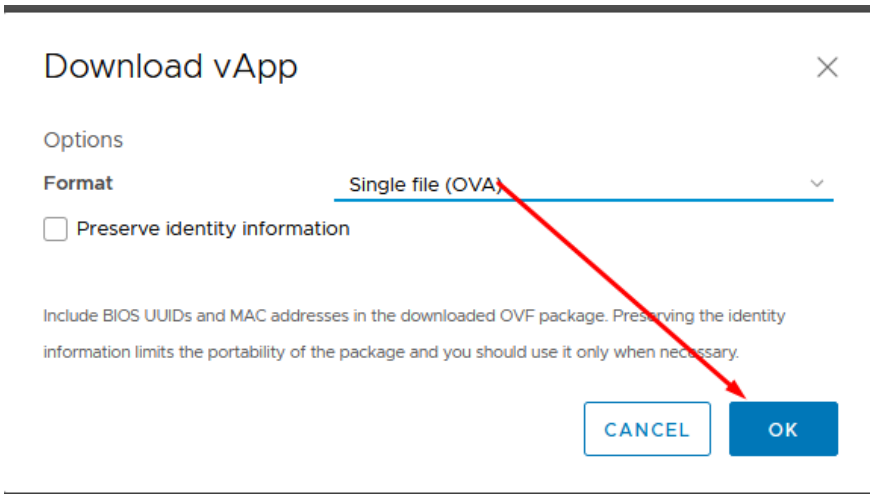
Exporting virtual machine

1. Power off vApp.

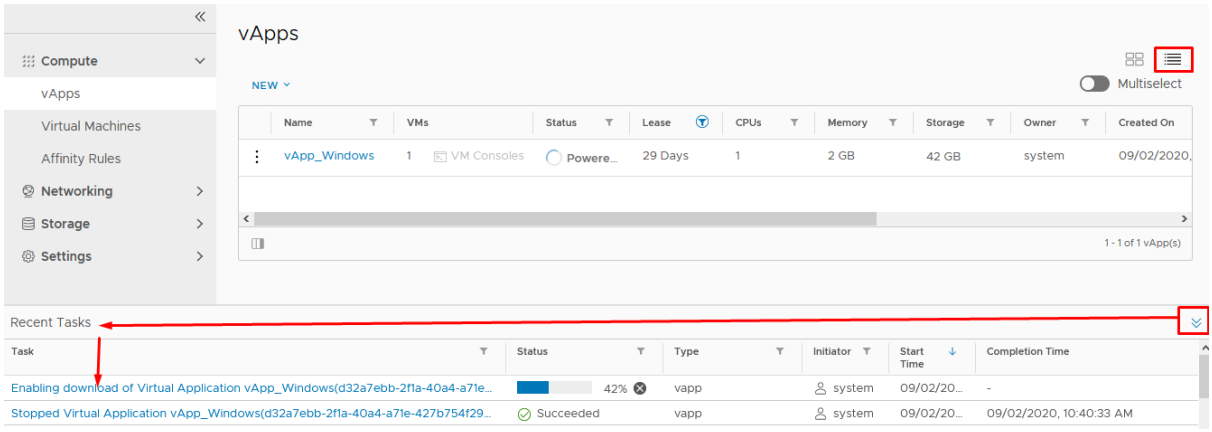


2. Select Download.





3. You can see OVA file status at the bottom of the window. When the file is ready to download, you will be notified.



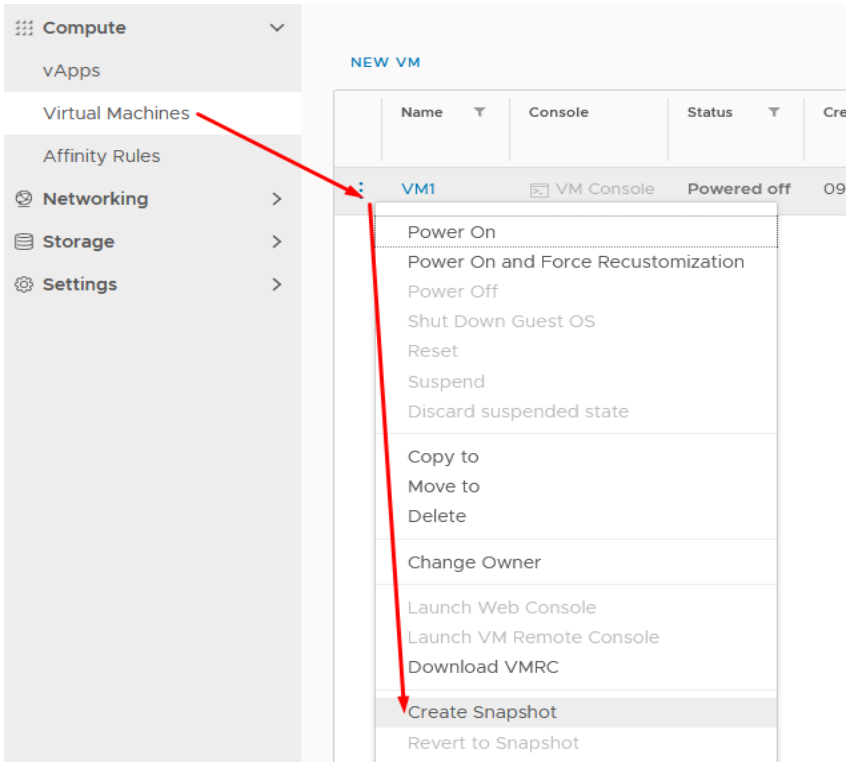
Create virtual machine snapshot

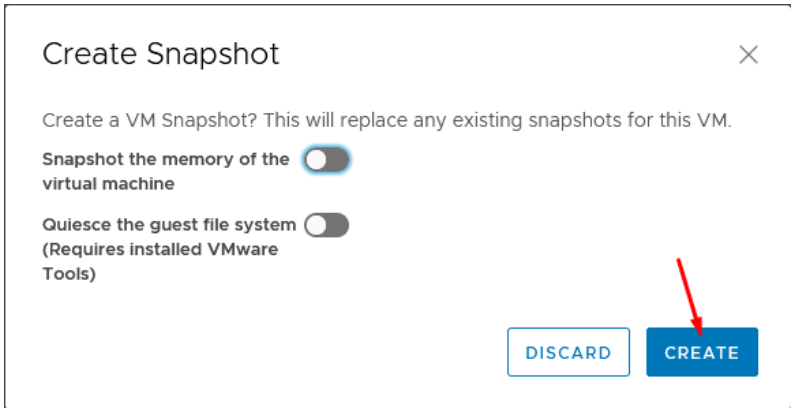
Snapshot is a virtual machine state and data at the snapshot creation moment. „Snapshot" is not intended to replace backups. Most common snapshot usage scenario: you can create it before updating an operating system so in case an OS runs incorrectly, you can load the VM to the state before OS update by selecting "Revert to Snapshot".

In order to create a VM „Snapshot" you must have a free space in your virtual data center. E.g., if VM's disk size is 100 GB, you will need 100 GB space for the snapshot.

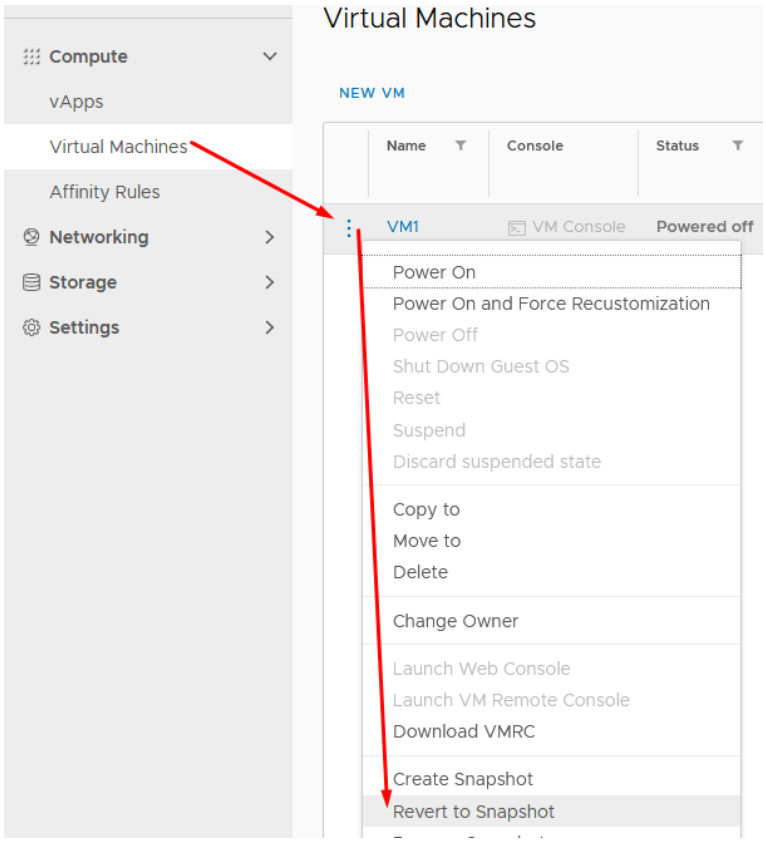
Limitations: you can only have one "Snapshot"

1. Select virtual machine and press „Create Snapshot".

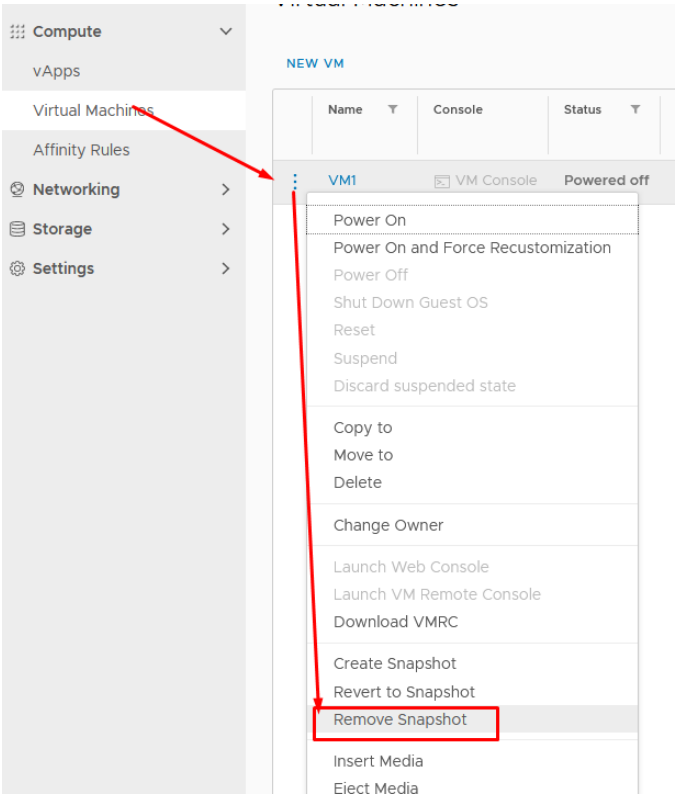




2. If you want to load the VM to the time when snapshot was created, select the VM and press „Revert to Snapshot".



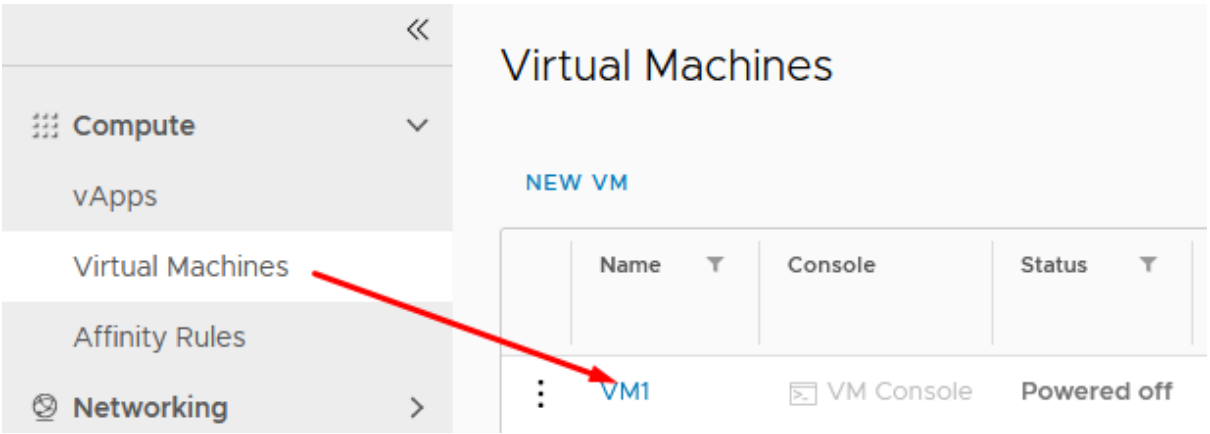
3. If you no longer need the snapshot, delete it, because it can affect virtual machine disk performance.



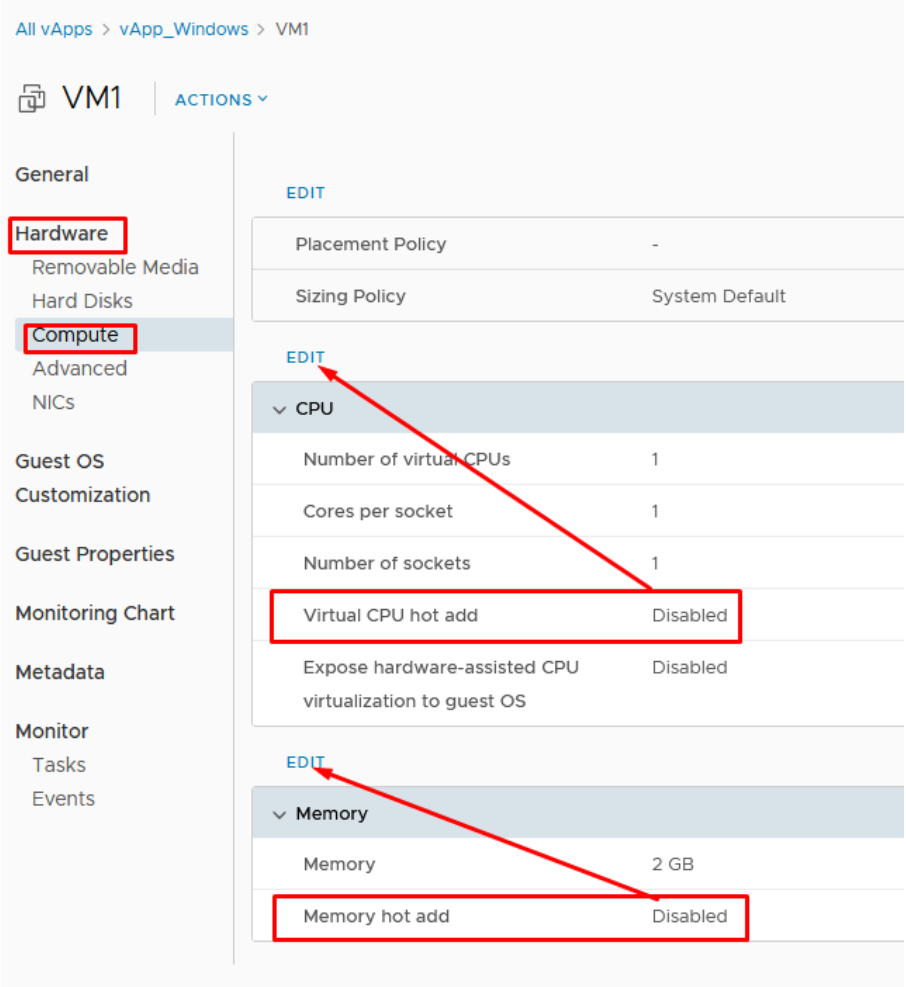
Hot Add CPU/RAM

HOT add CPU and RAM technology is used in order to increase virtual machine's CPU and/or RAM without downtime. „Hot add" can be enabled only while VM is powered off. Some operating systems may not support this technology, therefore it is best to check with the software manufacturer.

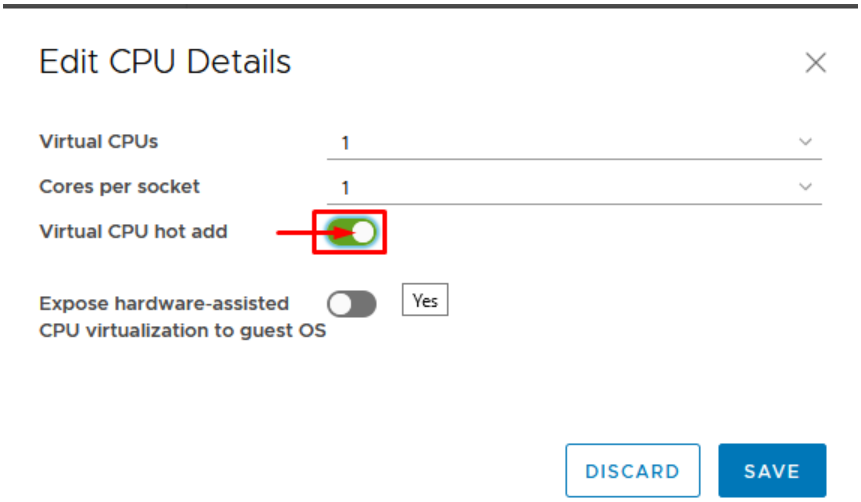
1. Press virtual machine name.



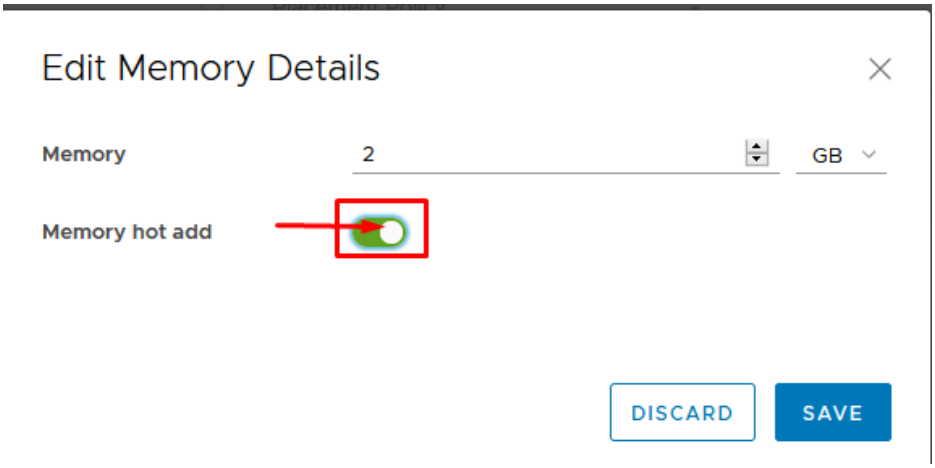
2. In Hardware>Compute you can see Hot Add status. Press Edit to change it.



3. Enable Virtual CPU hot add and press Save.



4. Enable Memory hot add and press Save.

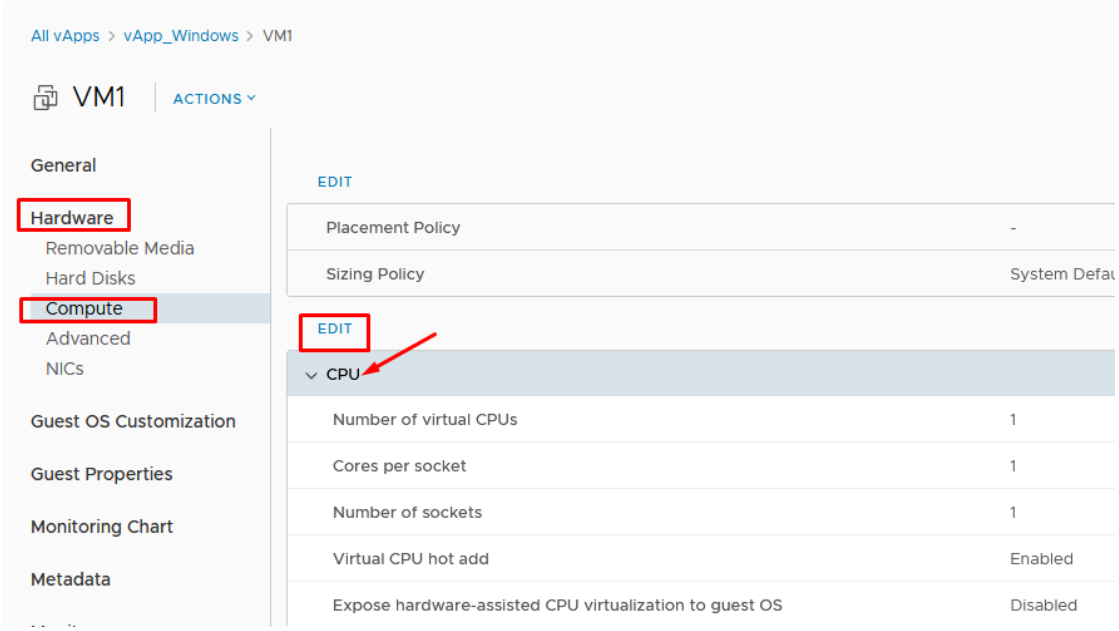


Increasing virtual machine compute resources

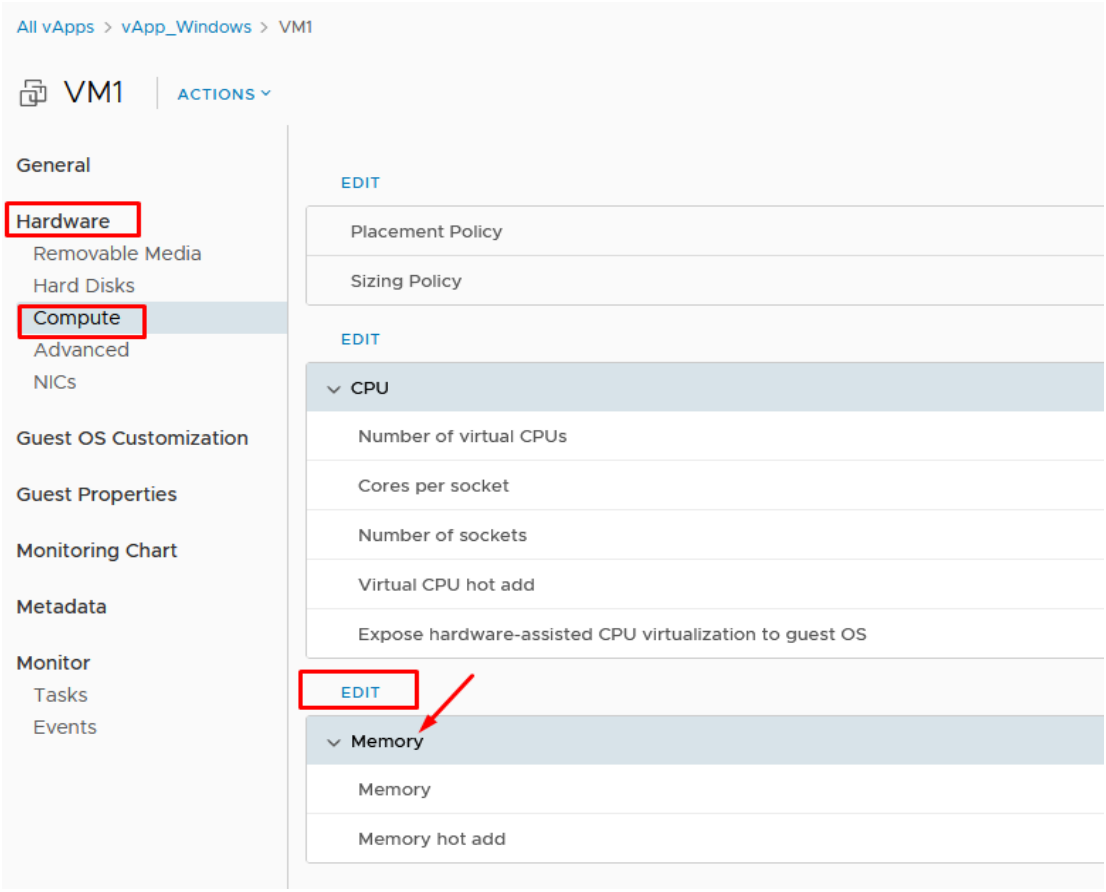
Virtual machine vCPU/RAM can be increased without downtime if CPU/RAM Hot Add is enabled. Compute resources can be decreased only while VM is powered off.

SSD and HDD disks can be increased both for powered on and powered off virtual machines in case they do not contain snapshots. If snapshot is present, you will need to delete it in order to increase disk's size. You cannot decrease disk's size as it is not possible in vCloud Director and also requires specific technical knowledge, however it can be done by Baltneta technicians.

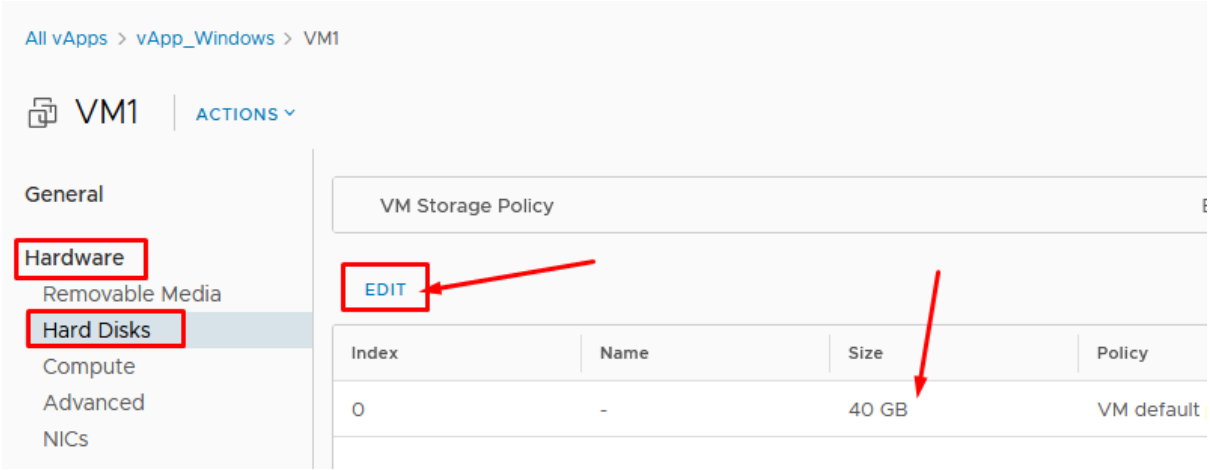
1. Changing vCPU resources.



2. Changing RAM resources.

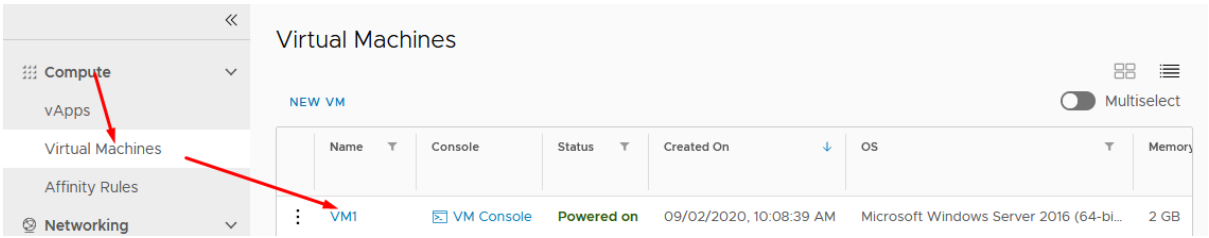


3. Increasing SSD and HDD disk size.

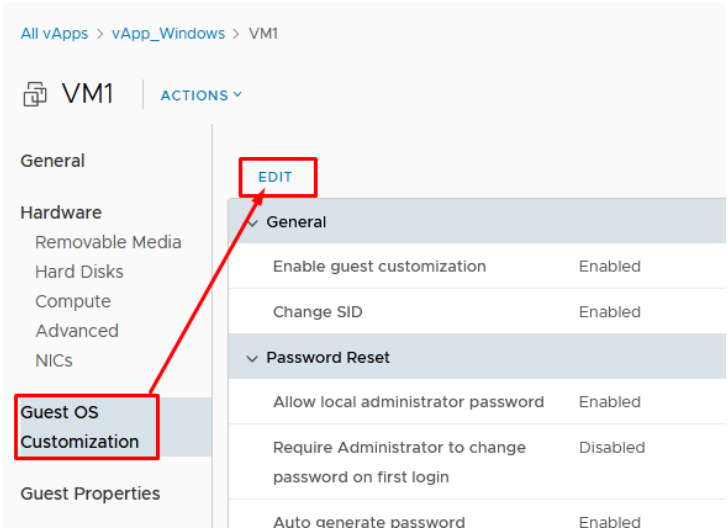


Virtual machine password

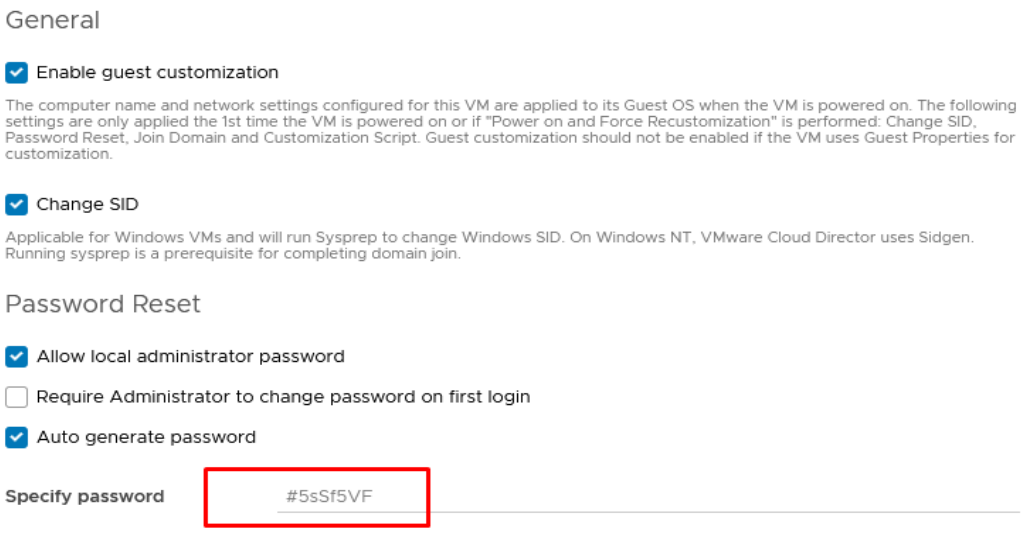
1. Press virtual machine‘s name



2. Go to Guest OS Customization and select Edit



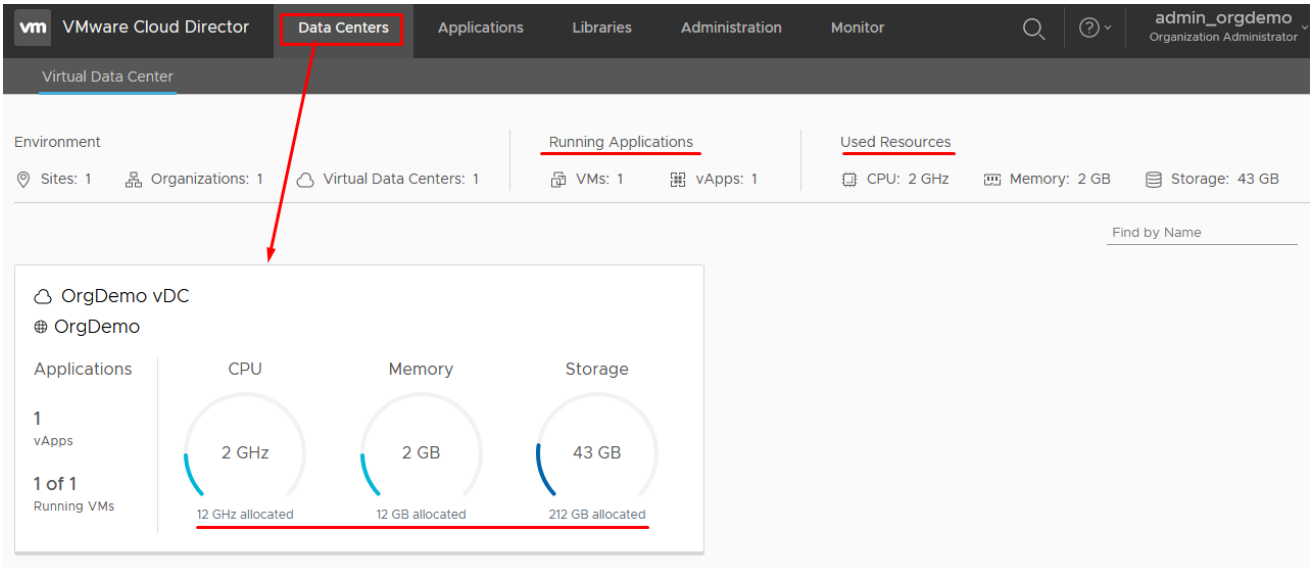
3. Generated password can be seen in „Specify password“.
   Windows default admin user: administrator
   Linux default admin user: root



4. We recommend changing Administrator or root password when you login to the virtual server. Also it is advisable to unmark „Enable Guest OS Customization“ in VM properties after customization processes are done.

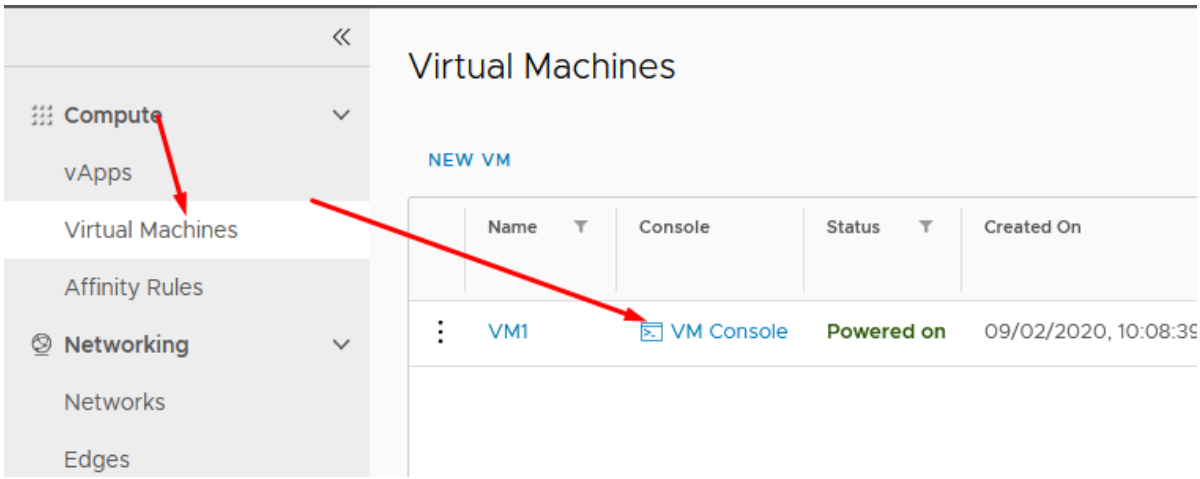
Virtual data center resource information

1. Allocated resources are visible in Data Centers > Your vDC.



Remote Console

1. Using web console.

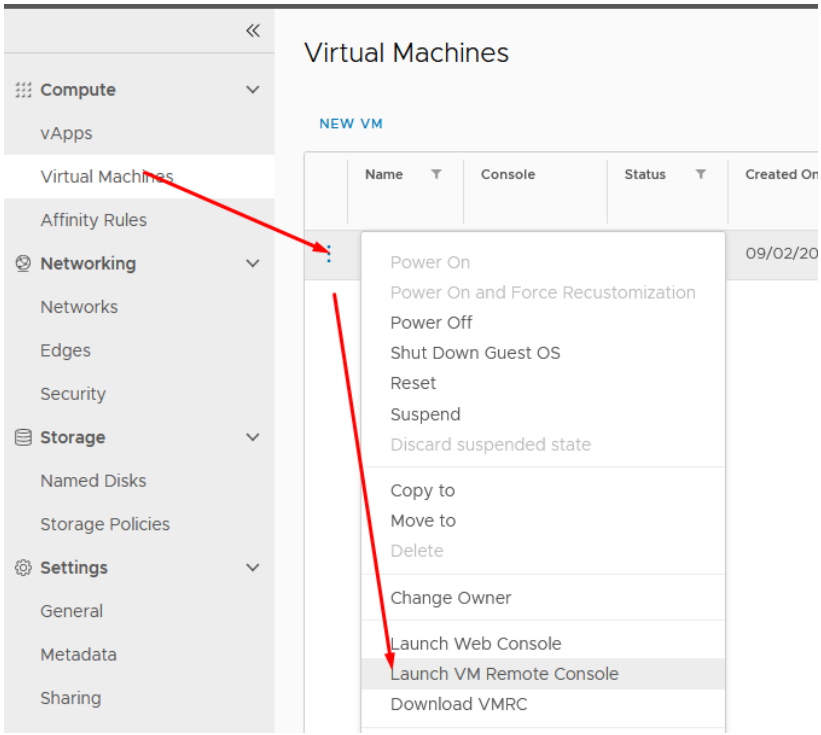


2. VMRC (VMware Remote Console) enables to login to VM console using VMRC client application. In order to use that you need to download VMRC client:

VMware Remote Console 11.1.0 for **Windows** https://pagalba.balt.net/images/e/ea/VMware-VMRC-11.1.0-15913118.zip

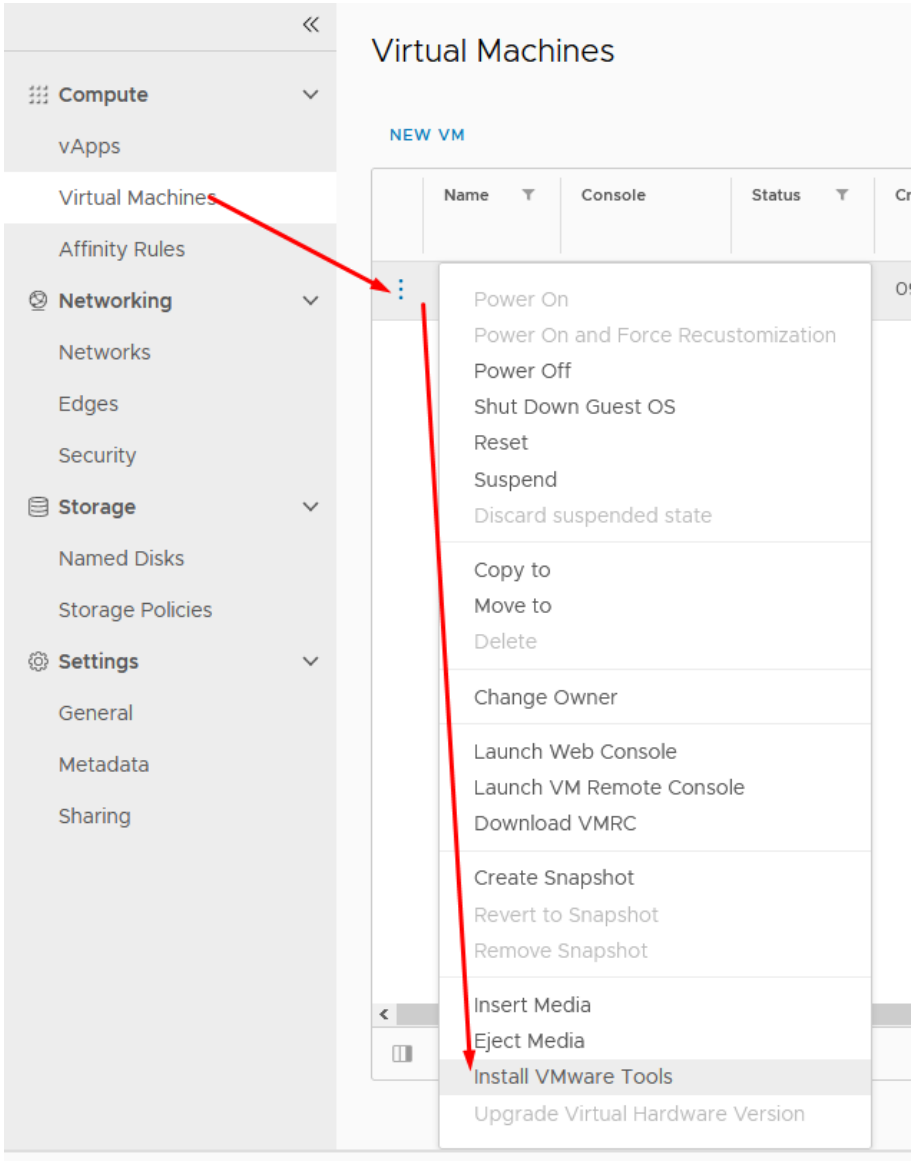
VMware Remote Console 11.1.0 for **Mac**: https://pagalba.balt.net/images/4/45/VMware-Remote-Console-11.1.0-15913118.dmg.zip

VMware Remote Console 11.1.0 for **Linux**: https://pagalba.balt.net/images/9/91/VMware-Remote-Console-11.1.0-15913118.x86_64.zip



VMware Tools

1. Select virtual machine and press „Install VMware Tools“.

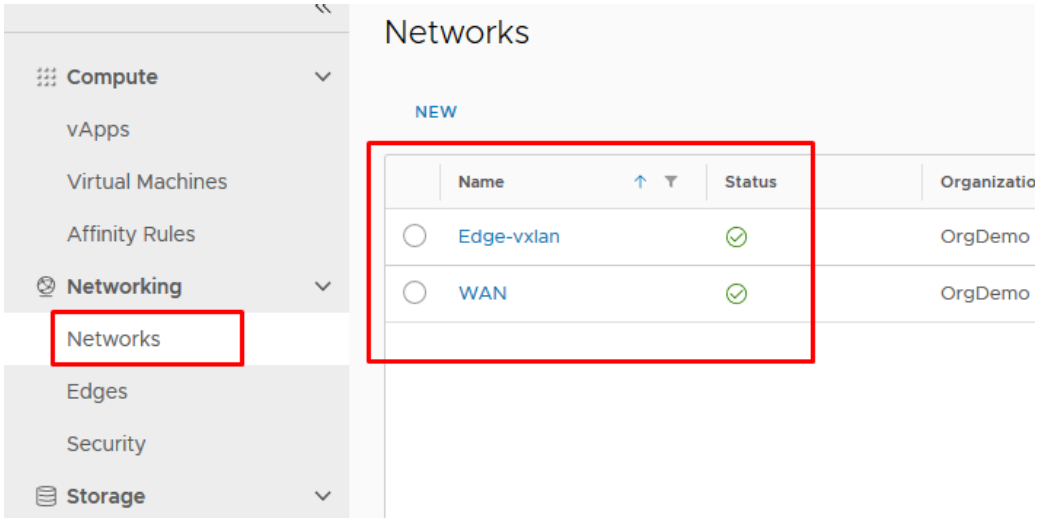


2. Launch web or VMRC console and login to the Windows OS. You will find VMware tools CD attached. Install it and reboot virtual server.
3. Alternative ways to install VMware tools are described in VMware Docs:
   Linux: https://docs.vmware.com/en/VMware-Tools/11.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-08BB9465-D40A-4E16-9E15-8C016CC8166F.html

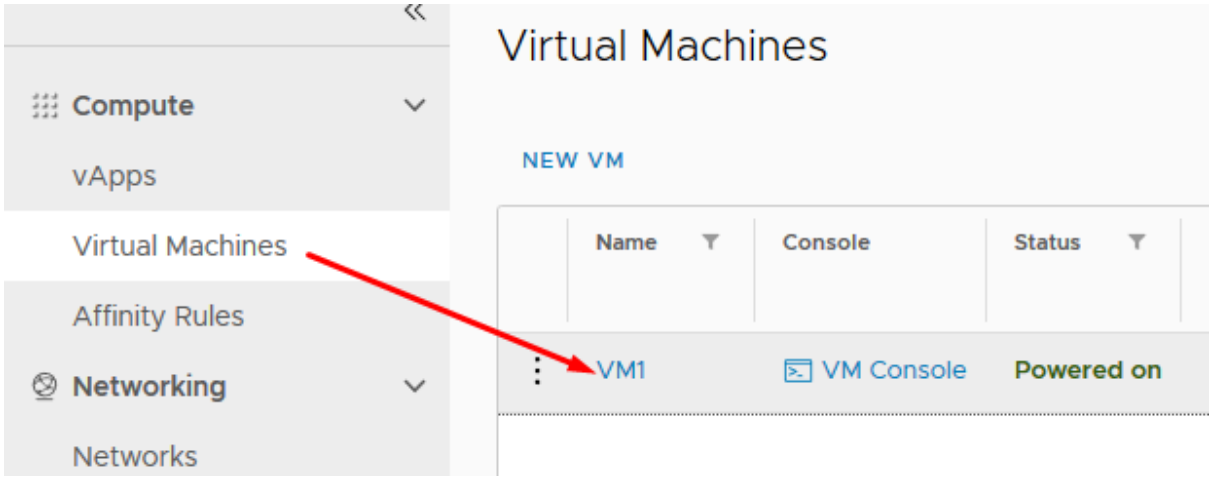
   Windows: https://docs.vmware.com/en/VMware-Tools/11.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html

Networking: adding network to a virtual machine

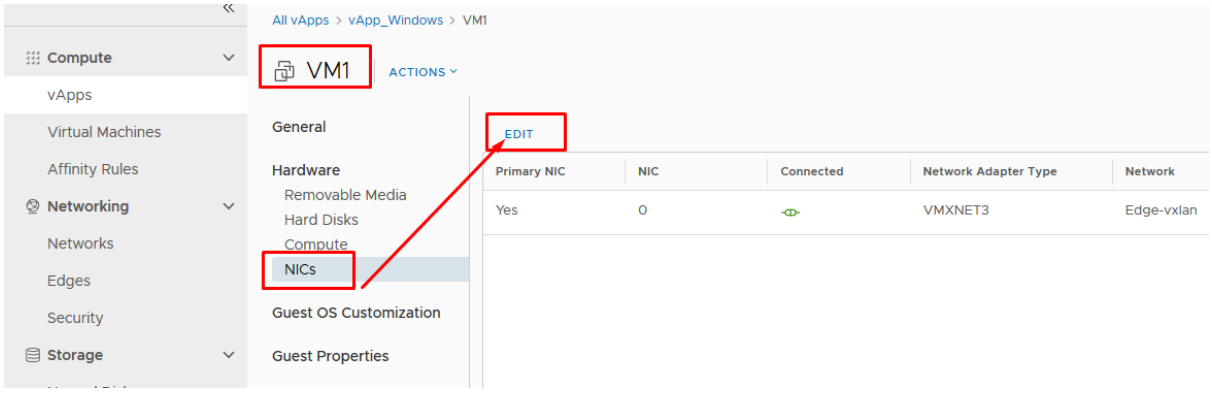
1. Organization networks can be found at Networking>Networks.



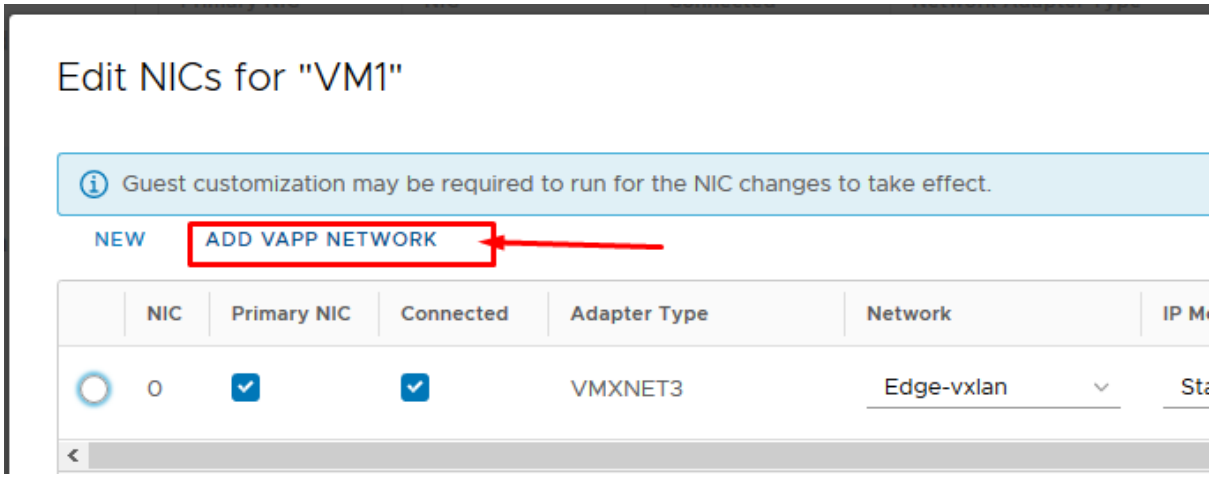
2. Press virtual machine name.



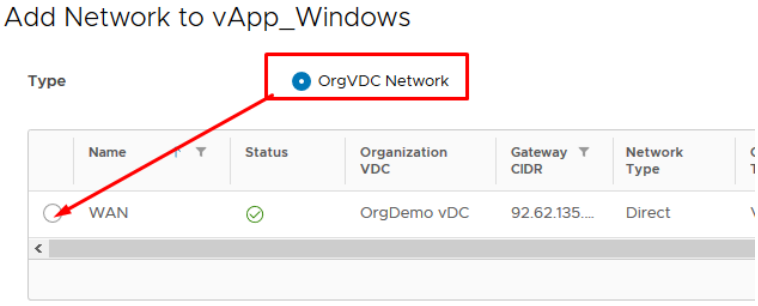
3. NICs>Edit.



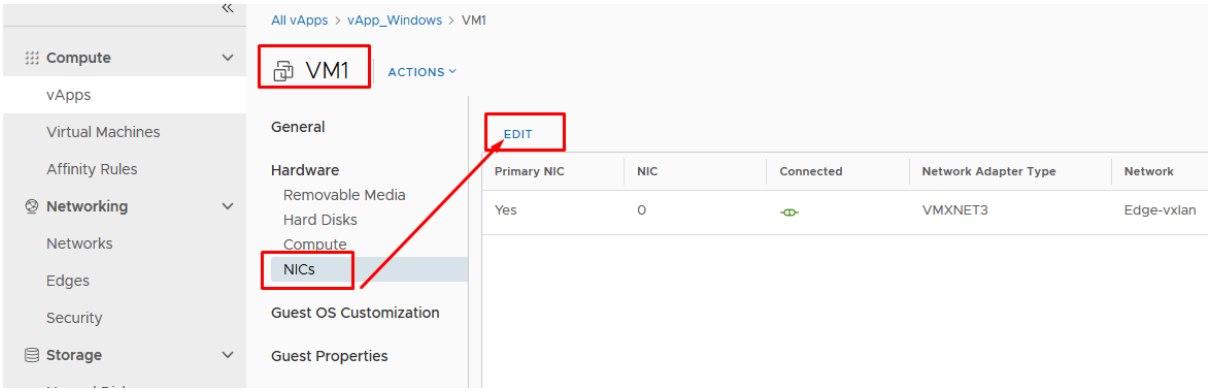
4. Adding network to vApp. Press ADD VAPP NETWORK.



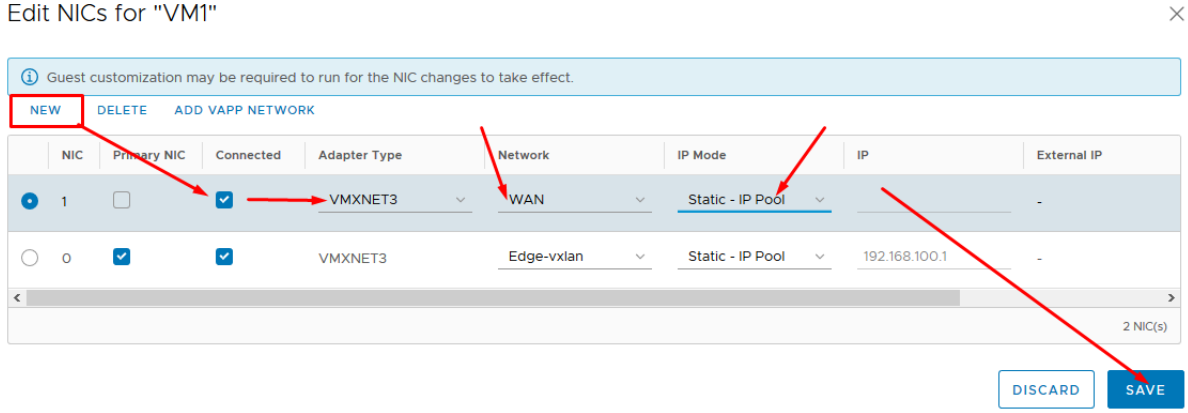
5. Select OrgVDC Network, press ADD and Save.



6. Now we add network adapter to a VM. Again press Edit.

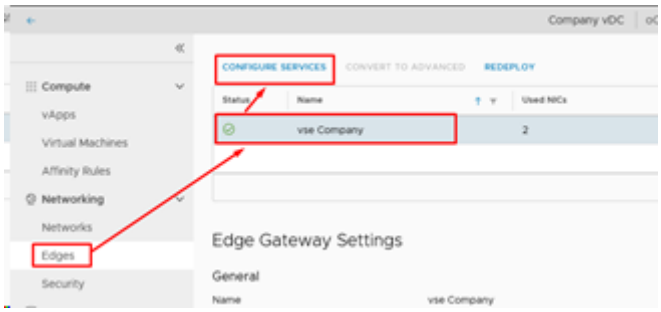


7. Select vmxnet3 or E1000E network adapter type, select network, select Static IP Pool. Press Save. You will be able to see the allocated IP address in the VM NICs page.

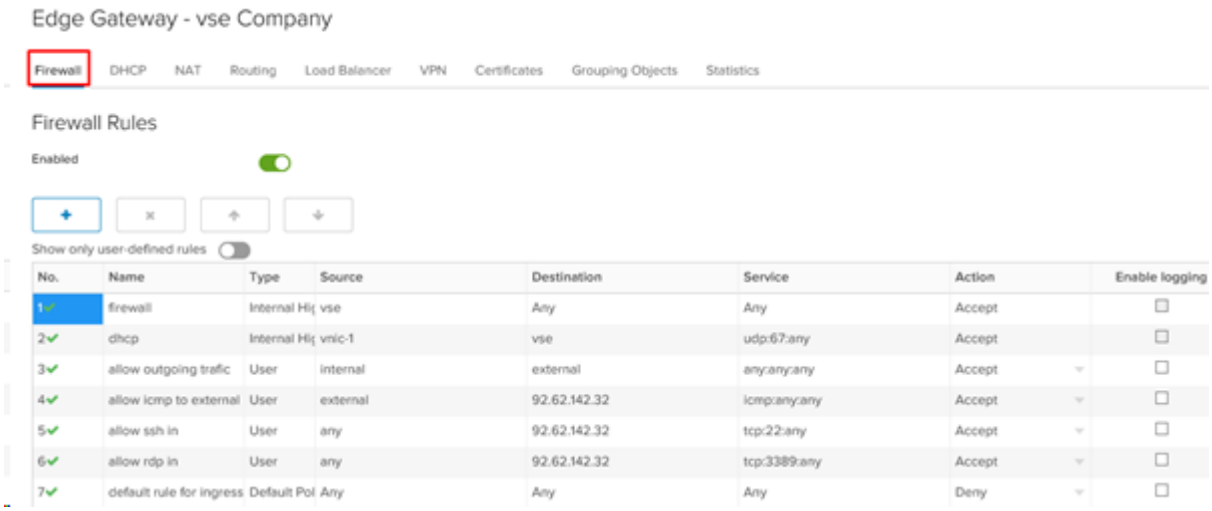


Networking: Edge Gateway

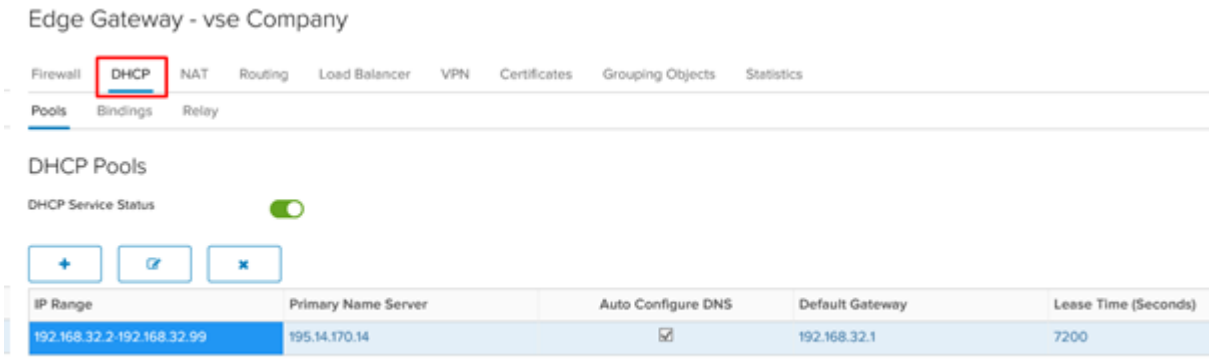
1. Edge gateway services can be configured at Networking > Edges > CONFIGURE SERVICES.



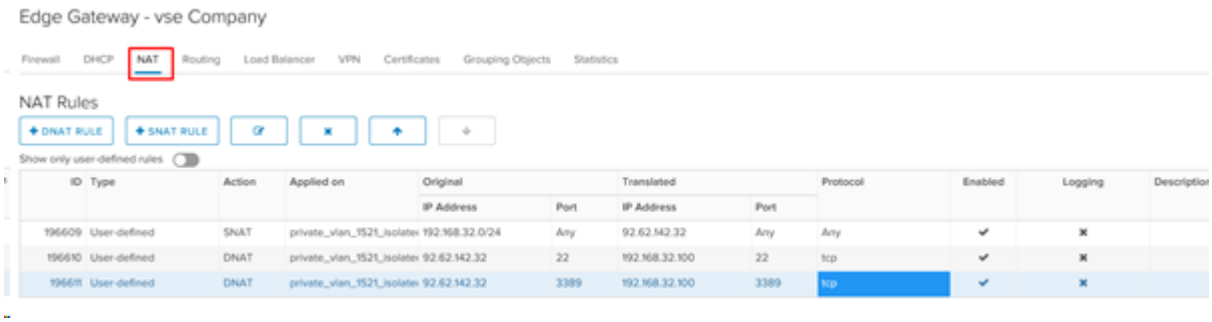
2. Firewall – you can create new rules and enable/disable Firewall (NAT rules do not work while Firewall is disabled).



3. DHCP – it is possible to create IP range which can be used for virtual machines which are connected to Edge Gateway via vxlan (virtual network) and need DHCP.



4. NAT – it is possible to create source NAT and destination NAT (port forward) rules.

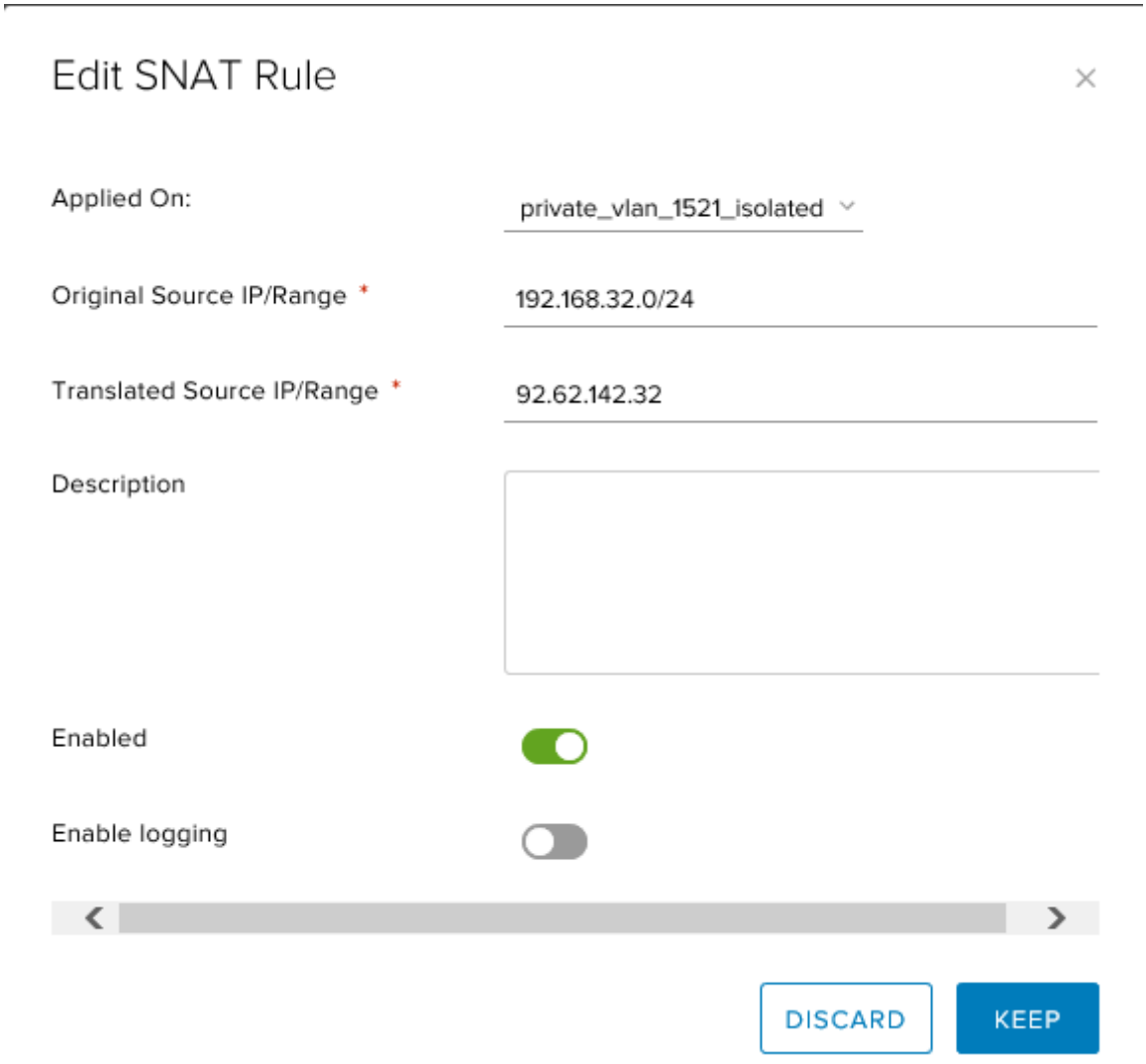


SNAT RULE – source NAT lets virtual machines to reach internet via Edge Gateway.

Applied on – external network should be selected.

Original Source IP/Range – internal IP range (subnet).

Translated Source IP/Range – external IP, usually the IP of the Edge Gateway.

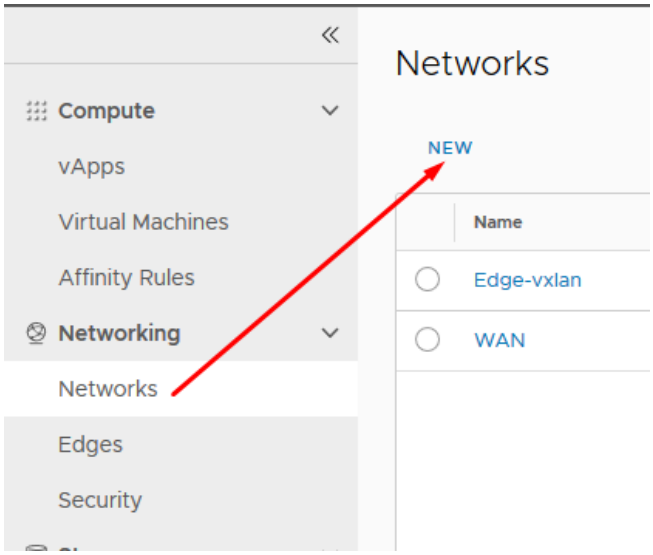


DNAT RULE – port forwad.

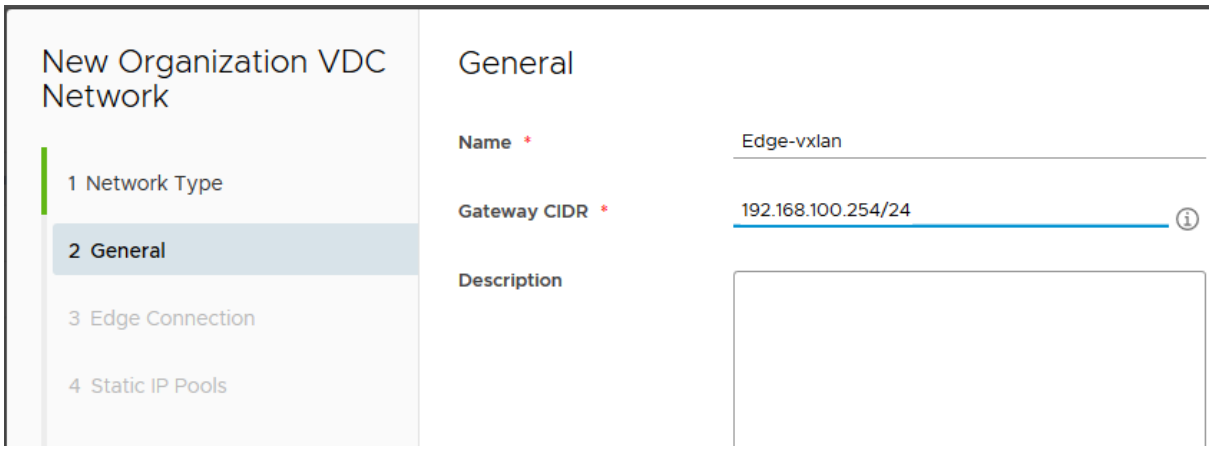
- Applied on – external network should be selected.
- Original IP/Range – external IP, usually the IP of the Edge Gateway.
- Translated – internal IP.
- Appropriate „Protocol", "Original Port" and „Translated port" should be selected.

Networking: creating Edge Gateway vxlan

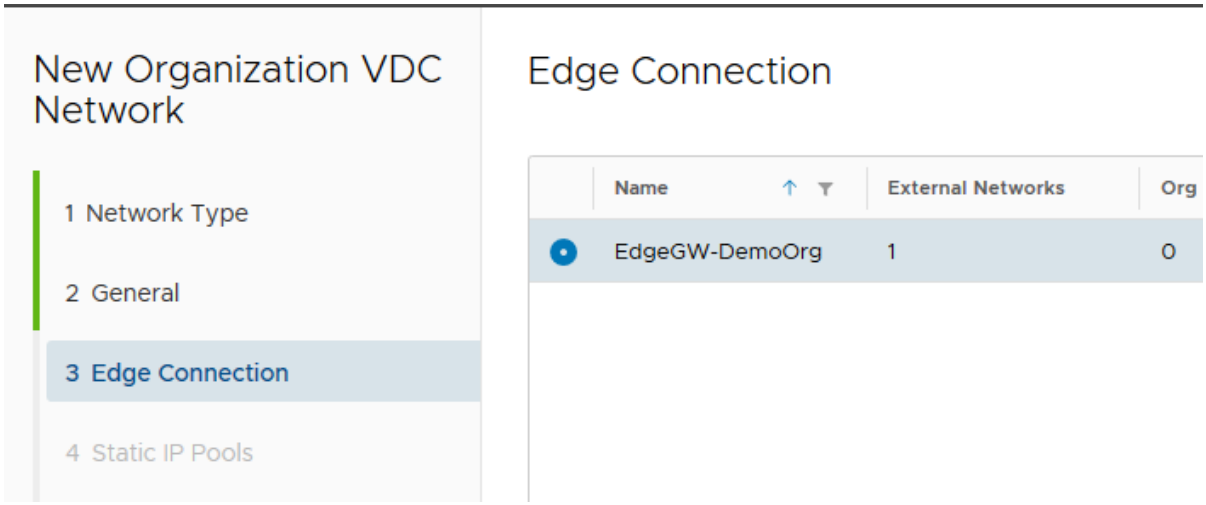
1. Select Networking > Networks, choose „NEW".



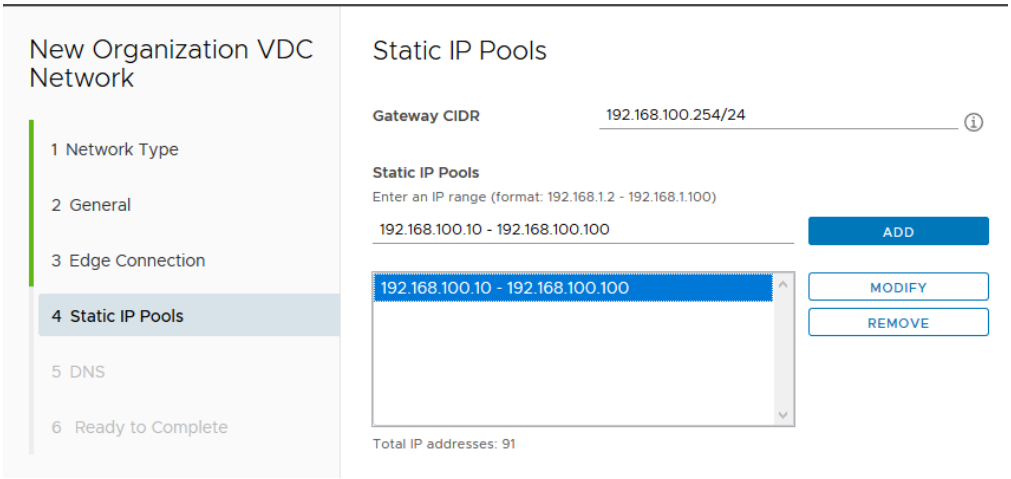
2. Set Network Type > Routed.
3. Enter vxlan name and Gateway CIDR.



4. Edge Connection > select your Edge Gateway.



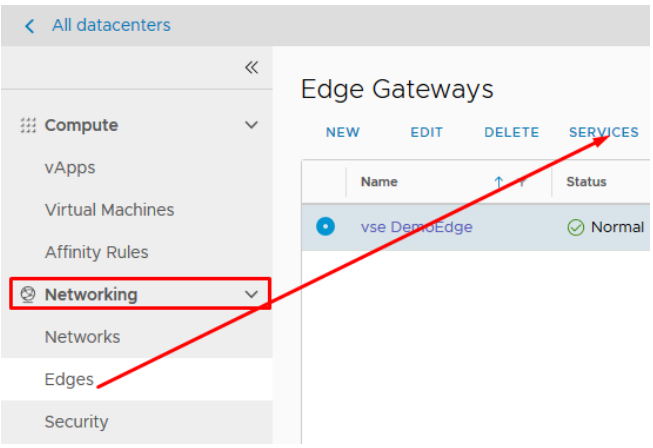
5. Enter desired static IP pool.



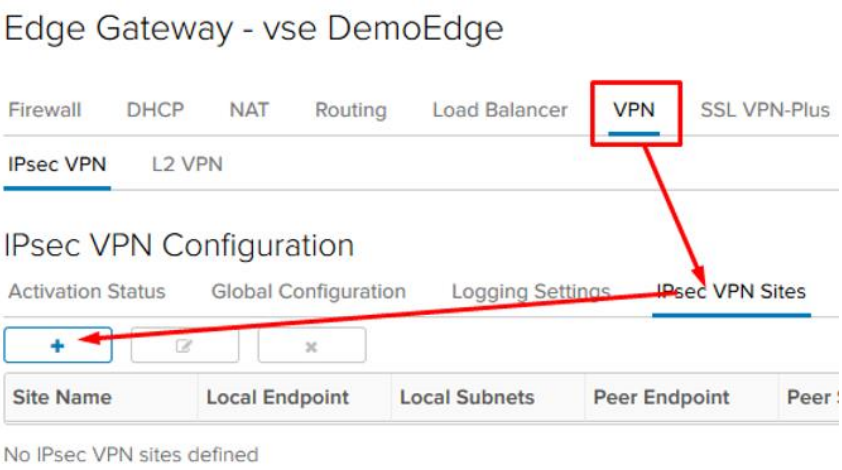
6. DNS > enter desired DNS. Baltneta DNS servers can be used: 195.14.170.14 and 195.14.176.14. Press Next>Finish.

Networking: IpSec configuration example

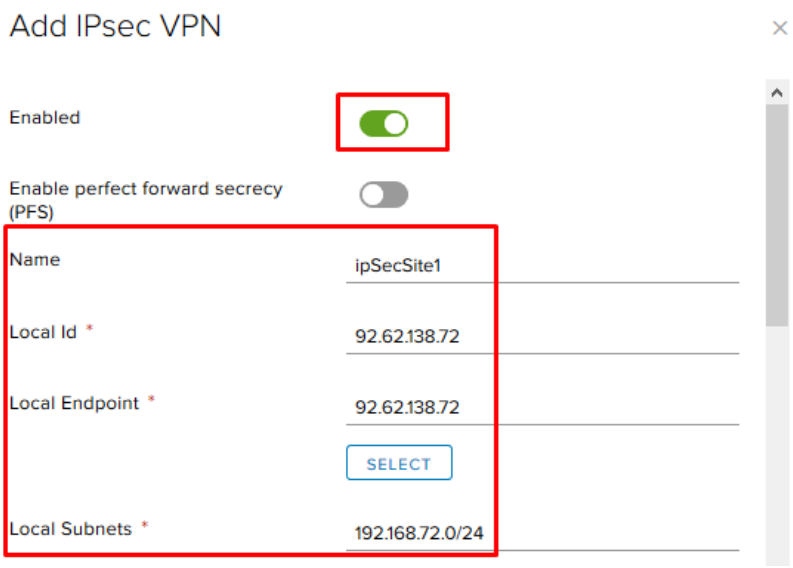
1. Go to Edge gateway services.



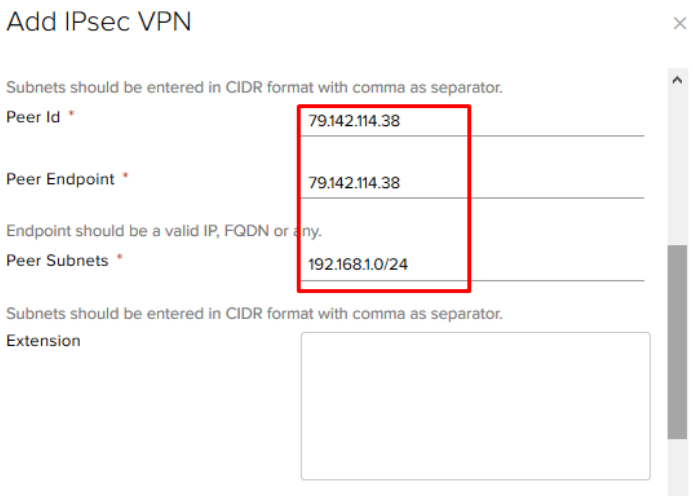
2. Add IPsec Sites.



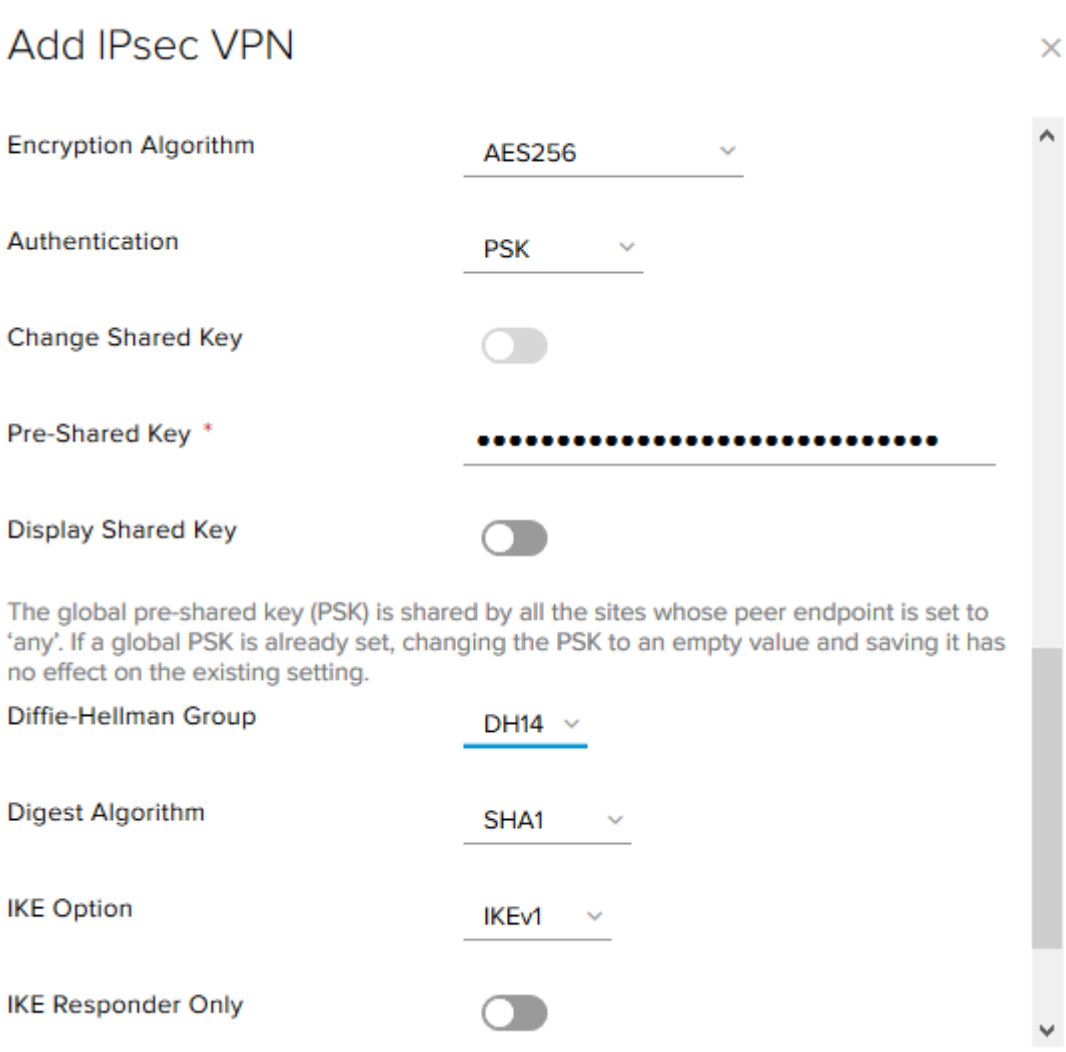
3. Enter Edge external and internal IP addresses.



4. Enter Peer external and internal IP addresses.



5. Enter security information. This configuration must match your Peer site configuration.



6. Table – example of your configuration parameters which must match Peer's configuration.

Baltneta		**Client**
IPSec device model		
Vmware edge		Enter information here
IPsec peer IP (IPSec termination)		
Baltneta Edge IP		Enter information here
Protected networks (traffic that will be protected by IPSec)		
Level	**Baltneta network/host IP**	**Client network/host IP**
	192.168.33.0/24	Enter information here

Attributes	**Baltneta**	(If attributes are OK by your security policy, leave it as it is).
	ISAKMP attributes (phase 1)	
Authentication: ***Preshared-key***	***EsoXahCh0peGheu1AexbiLaighfe1Eik***	
Hash	**sha1**	
Encryption	**aes256**	
DH Group	**14**	
Lifetime	**86400sec**	
	IPSec attributes (phase 2)	
IPSec mode	**Tunnel Mode**	
Transform set	**ESP-AES-256-SHA**	
SA lifetime seconds	**3600**	
Compression	**NO**	
PFS	**DF 14**	

7. Enable VPN.