

vCloud Director 10 HTML5 F.A.Q.

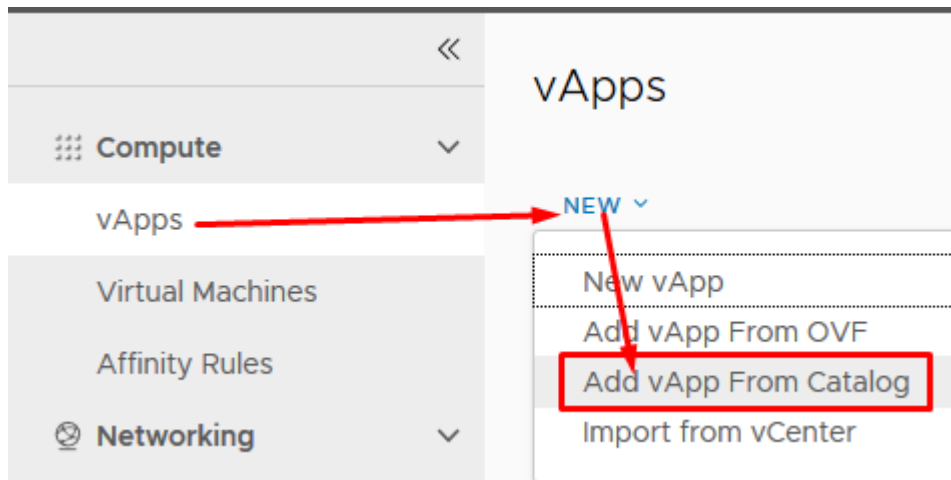
Content

Virtual machine creation from template.....	3
Virtual machine installation using ISO	5
Importing media to a catalog.....	8
Exporting virtual machine.....	9
Create virtual machine snapshot	11
Hot Add CPU/RAM	14
Increasing virtual machine compute resources	16
Virtual machine password.....	18
Virtual data center resource information.....	19
Remote Console	19
VMware Tools	20
Networking: adding network to a virtual machine	21
Networking: Edge Gateway.....	24
Networking: creating Edge Gateway vxlan.....	27
Networking: IpSec configuration example.....	28

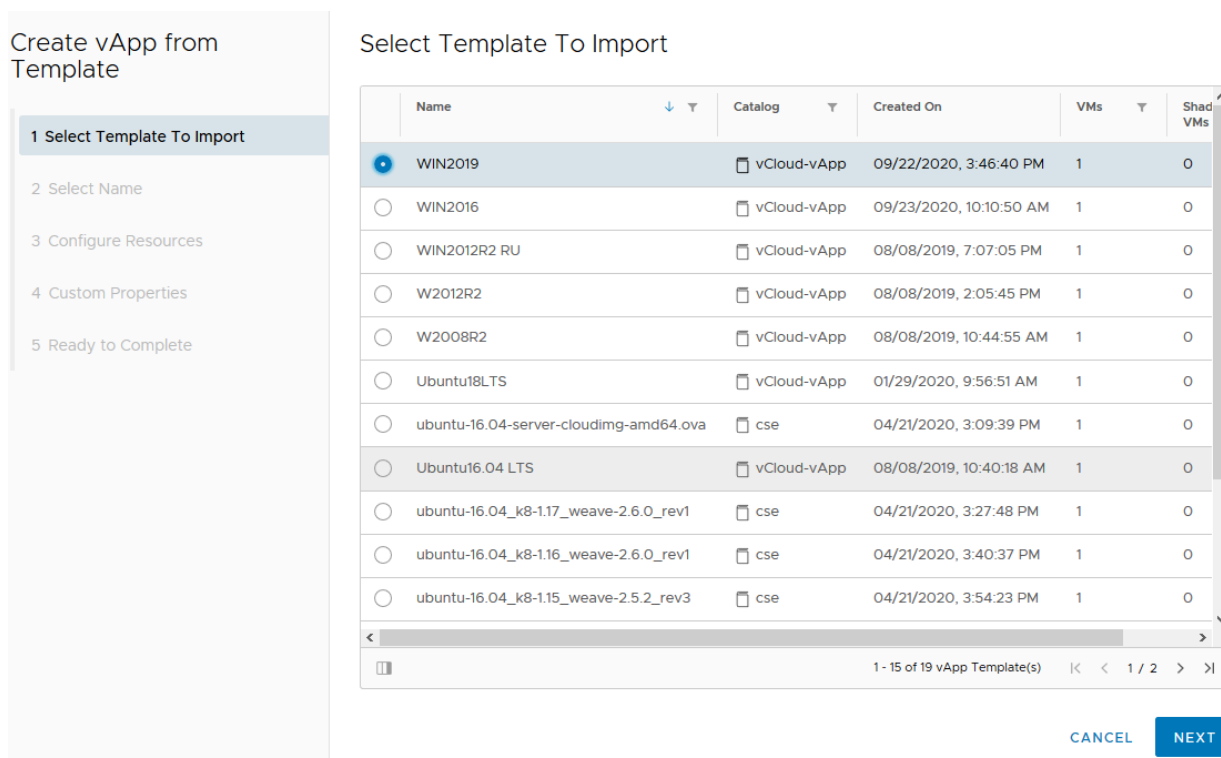
Virtual machine creation from template

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 > Add vApp From Catalog



2. Choose operating system and press next.



3. „Select name“ Enter VM name and press Next.
4. „Configure Resources“ Choose storage Policy and press Next.
5. "Compute Policies" Choose VM resources and press Next.
6. "Customize Hardware" Choose disk size and press Next.
7. "Configure Networking" In the Network tab choose your network. Press Next and Finish. Please wait when vApp with virtual machine is created.
8. Power On created vApp.
9. In Guest properties "Specify password" you can see Administrator or root user password.

All vApps > vApp_Windows > VM1

VM1 | ACTIONS

General

Hardware

- Removable Media
- Hard Disks
- Compute
- Advanced
- NICs

Guest OS Customization

Guest Properties

Monitoring Chart

Metadata

Monitor

- Tasks
- Events

EDIT

General

- Enable guest customization Enabled
- Change SID Enabled

Password Reset

- Allow local administrator password Enabled
- Require Administrator to change password on first login Disabled
- Auto generate password Enabled
- Number of times to log on automatically 0

Join Domain

- Enable this VM to join a domain Disabled
- Override organization's domain Enabled

Script

- Script file -

Edit Guest Properties

Automatic guest customization is not supported on this Guest OS. You can use custom scripts to configure the Guest OS.

General

Enable guest customization

The computer name and network settings configured for this VM are applied the 1st time the VM is powered on or if "Power on", "Password Reset", "Join Domain" and "Customization Script". Guest customization is not supported on this Guest OS.

Change SID

Applicable for Windows VMs and will run Sysprep to change Windows SID. Running sysprep is a prerequisite for completing domain join.

Password Reset

Allow local administrator password

Require Administrator to change password on first login

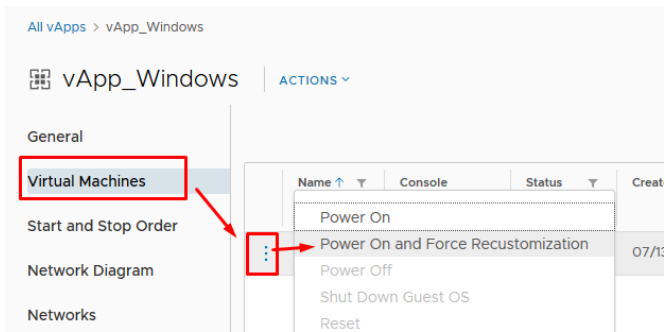
Auto generate password

Specify password

Number of times to log on automatically

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".

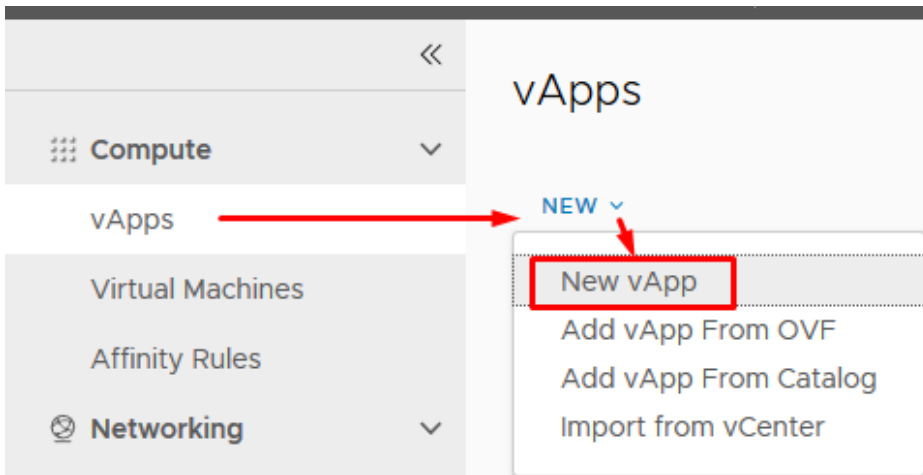


10. When VM is ready we recommend you to change administrator password in your OS and turn off „Guest OS customization“ from VM.

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“.

New vApp

Name *

Description

Power on

Virtual Machines	OS	Compute
		

[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.

New VM



Name * VM1

Computer Name * VM1

Description

Type New From Template

Operating System

OS family * Microsoft Windows

Operating System * Microsoft Windows Server 2016 (64-bit)

Boot image Win2016.ISO

Compute

Virtual CPUs 2

Cores per socket 1

Number of sockets 2

Memory 4 GB

Storage [ADD](#)

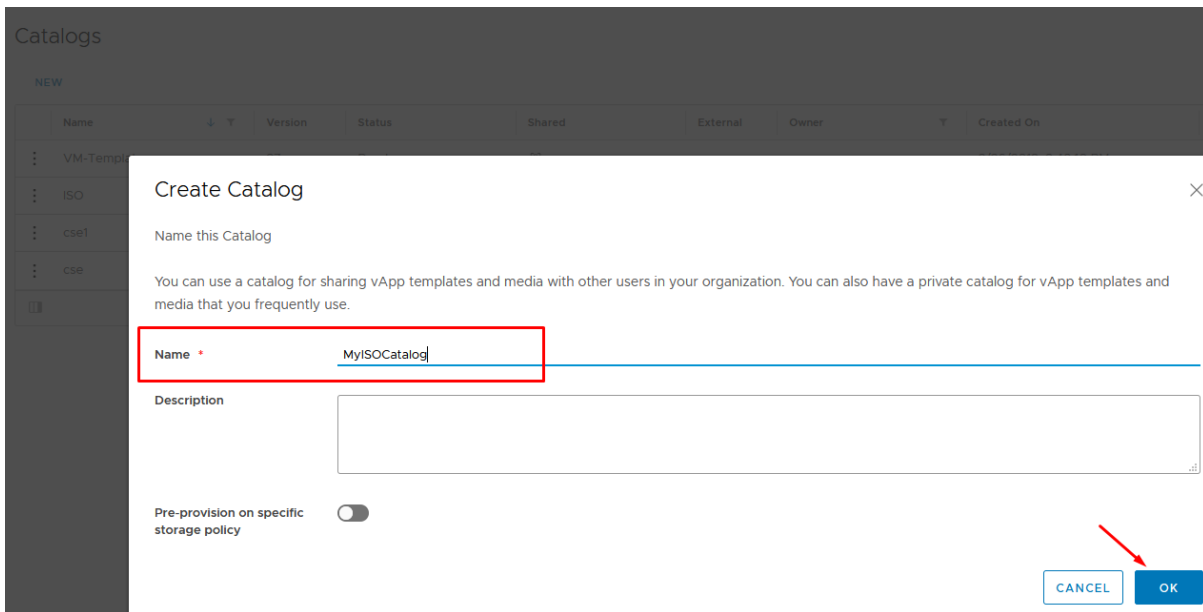
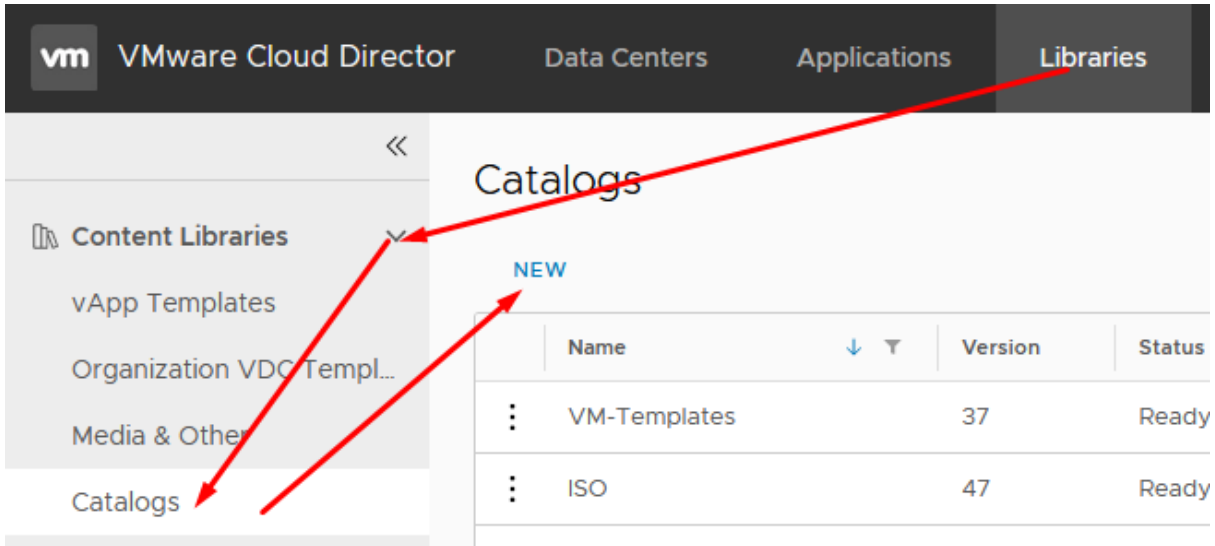
Disk	Storage Policy	IOPS	Size
------	----------------	------	------

[CANCEL](#) [OK](#)

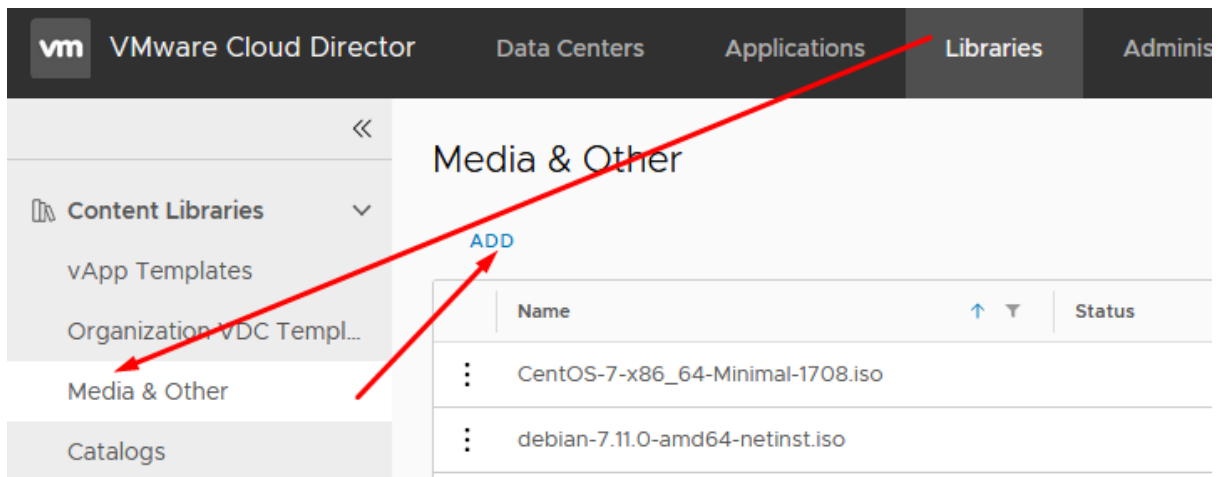
4. Open virtual machine console and follow OS installation wizard.

Importing media to a catalog

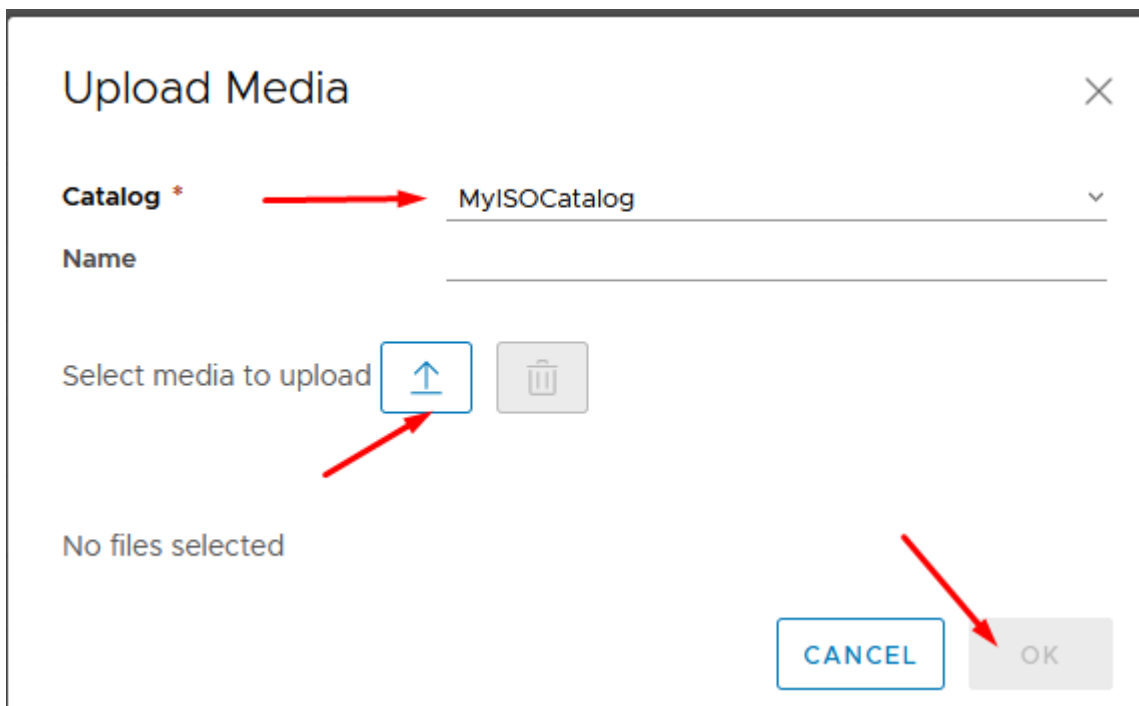
1. Create a new catalog and go to step 2 in case you want to import a media.



2. Import media.

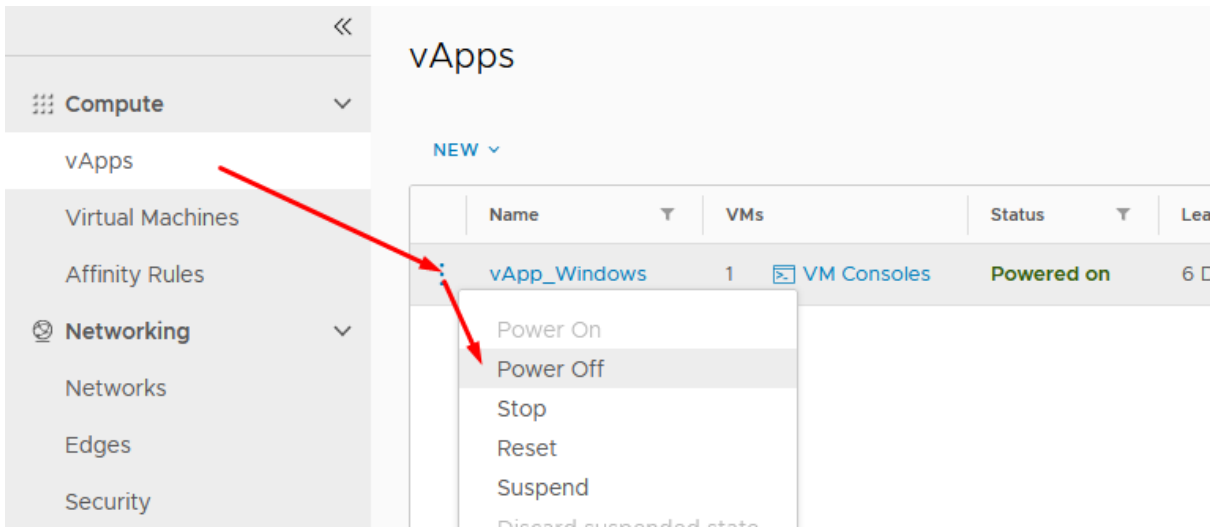


3. Select catalog for media import and press Upload. Enter media „Name“ and press OK.

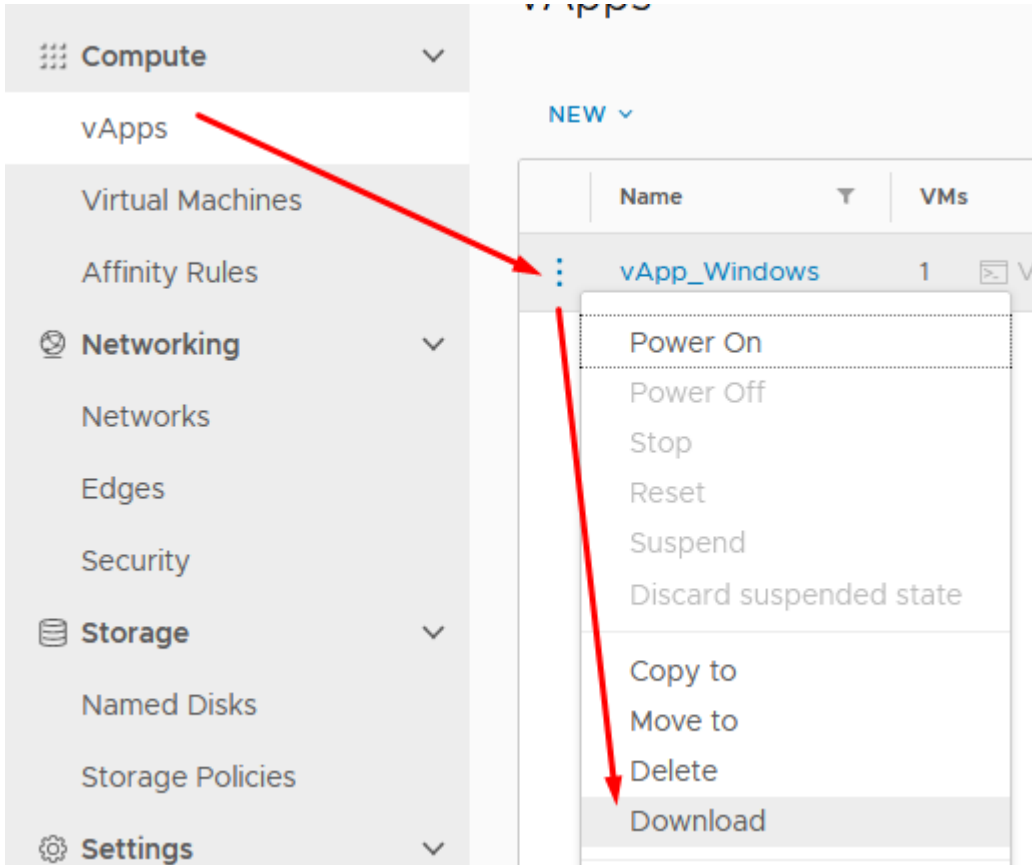


Exporting virtual machine

1. Power off vApp.



2. Select Download.



Download vApp



Options

Format

Single file (OVA)



Preserve identity information

Include BIOS UUIDs and MAC addresses in the downloaded OVF package. Preserving the identity information limits the portability of the package and you should use it only when necessary.

CANCEL

OK

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

The screenshot shows the vApp management interface. At the top, there's a 'vApps' header with a 'NEW' button and a 'Multiselect' toggle. Below is a table with columns: Name, VMs, Status, Lease, CPUs, Memory, Storage, Owner, and Created On. The table contains one entry: 'vApp_Windows' with 1 VM, Power... status, 29 Days lease, 1 CPU, 2 GB memory, 42 GB storage, system owner, and created on 09/02/2020. Below the table is a 'Recent Tasks' section with a table of tasks. A red arrow points from the 'OK' button in the 'Download vApp' dialog to the 'Recent Tasks' section.

Task	Status	Type	Initiator	Start Time	Completion Time
Enabling download of Virtual Application vApp_Windows(d32a7ebb-2f1a-40a4-a71e-427b754f29...	42%	vapp	system	09/02/20...	-
Stopped Virtual Application vApp_Windows(d32a7ebb-2f1a-40a4-a71e-427b754f29...	Succeeded	vapp	system	09/02/20...	09/02/2020, 10:40:33 AM

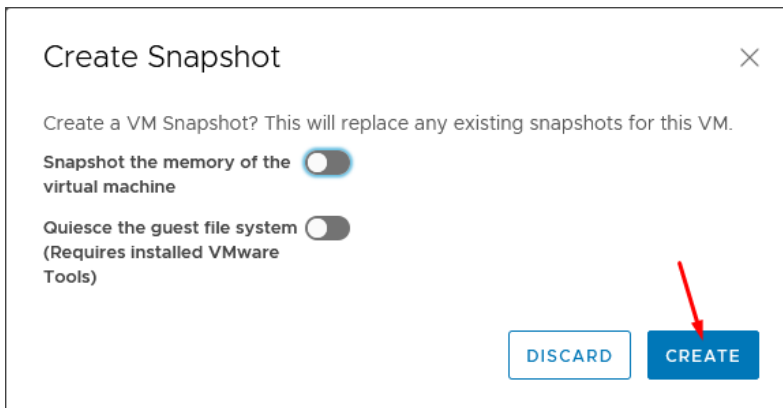
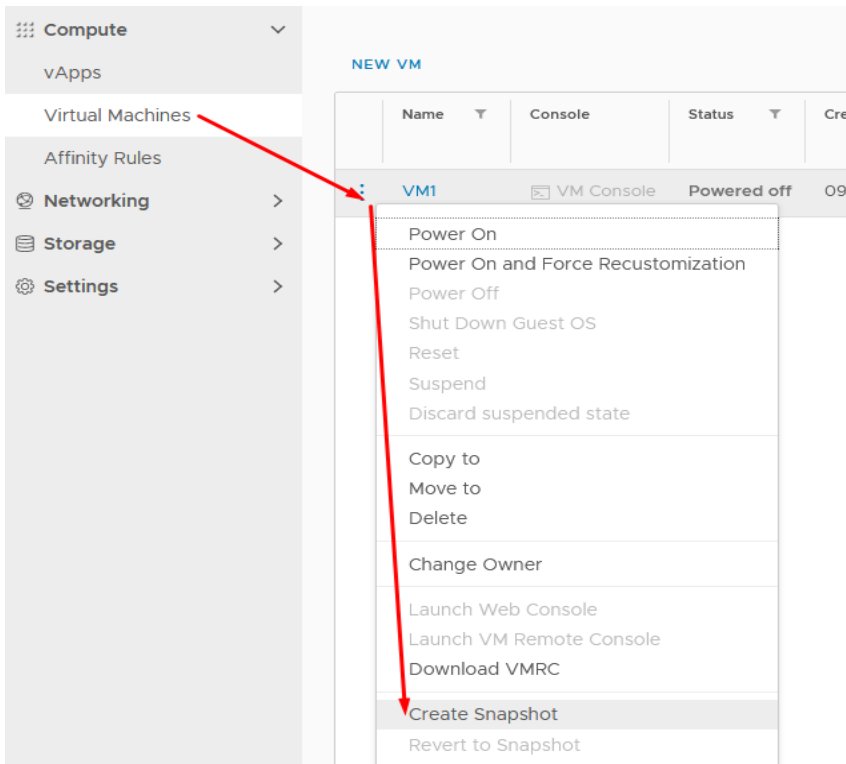
Create virtual machine snapshot

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“.

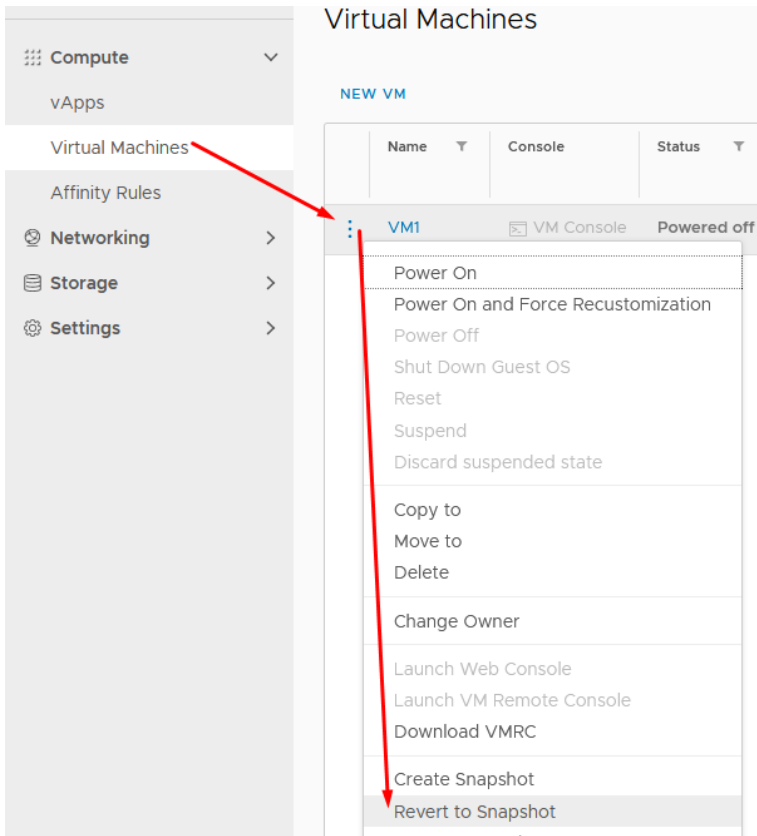
In order to create a VM „Snapshot“ you must have a free space in your virtual data center. E.g., if VM's disk size is 100 GB, you will need 100 GB space for the snapshot.

Limitations: you can only have one „Snapshot“

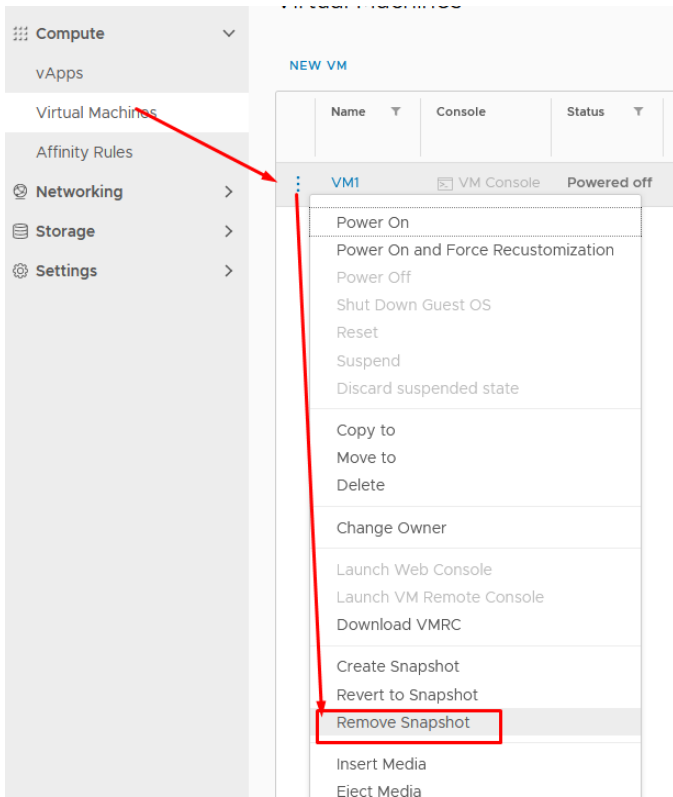
1. Select virtual machine and press „Create Snapshot“.



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



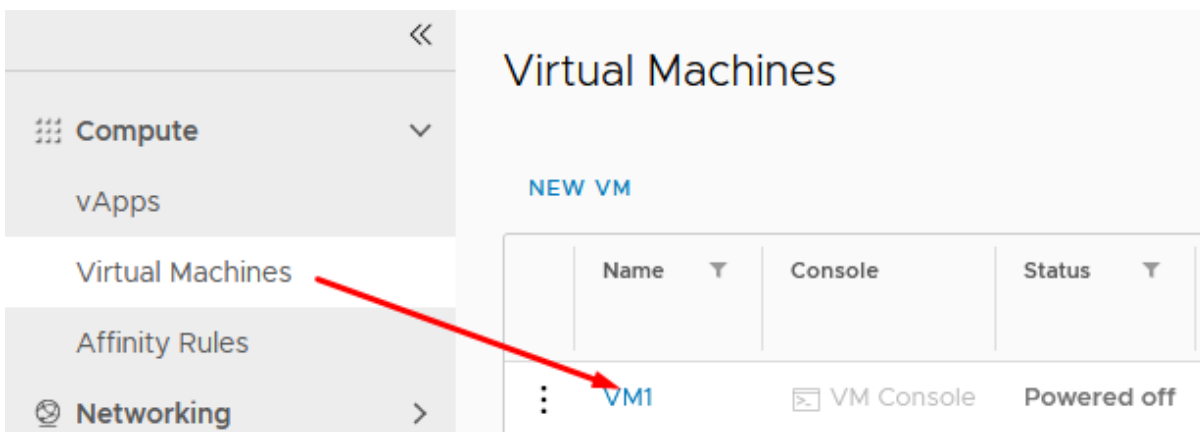
3. If you no longer need the snapshot, delete it, because it can affect virtual machine disk performance.



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.

All vApps > vApp_Windows > VM1

VM1 | ACTIONS ▾

General

Hardware

Removable Media

Hard Disks

Compute

Advanced

NICs

Guest OS

Customization

Guest Properties

Monitoring Chart

Metadata

Monitor

Tasks

Events

EDIT

Placement Policy	-
Sizing Policy	System Default

EDIT

✓ CPU

Number of virtual CPUs	1
Cores per socket	1
Number of sockets	1
Virtual CPU hot add	Disabled
Expose hardware-assisted CPU virtualization to guest OS	Disabled

EDIT

✓ Memory

Memory	2 GB
Memory hot add	Disabled

3. Enable Virtual CPU hot add and press Save.

Edit CPU Details

Virtual CPUs 1 ▾

Cores per socket 1 ▾

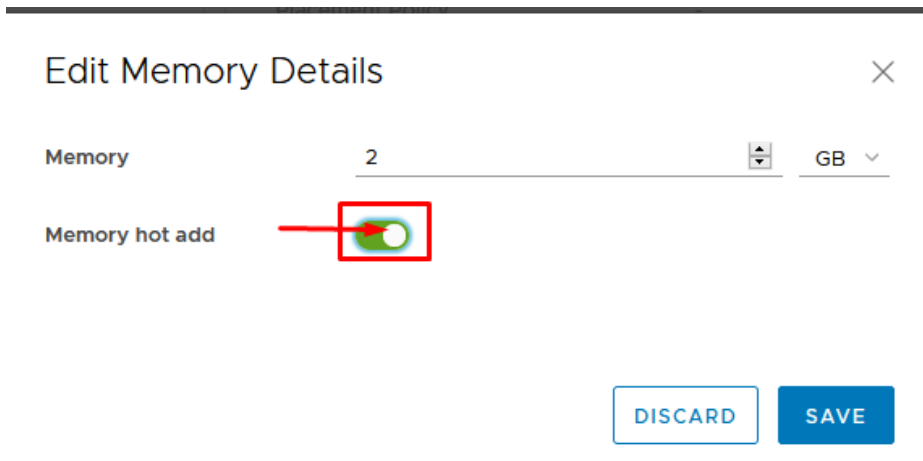
Virtual CPU hot add

Expose hardware-assisted CPU virtualization to guest OS Yes

DISCARD

SAVE

4. Enable Memory hot add and press Save.

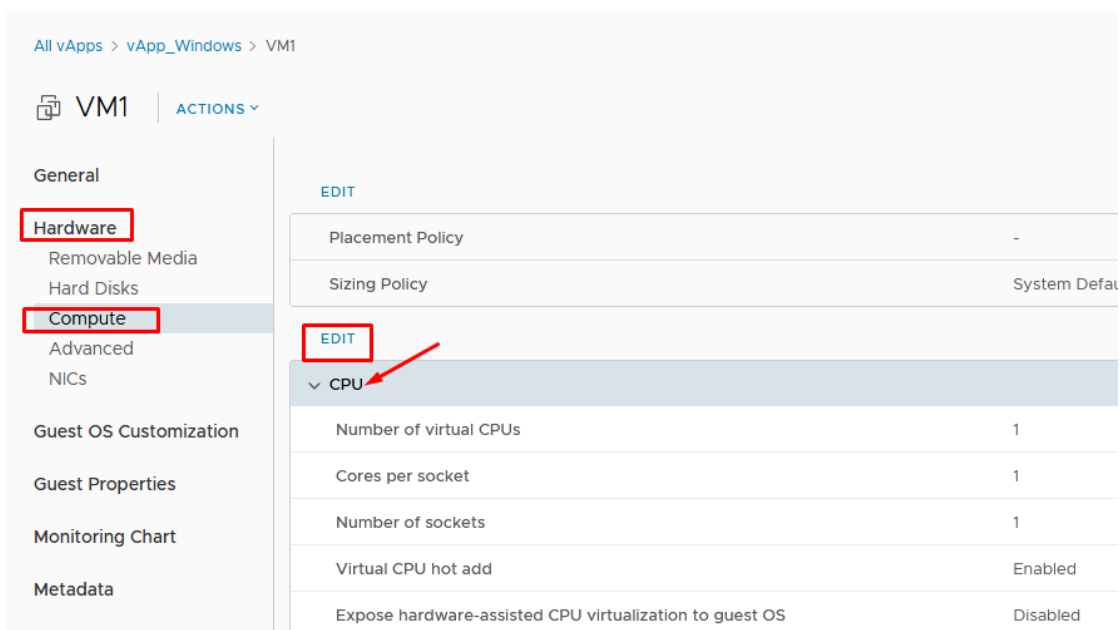


Increasing virtual machine compute resources

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.

The screenshot shows the configuration page for VM1. The left-hand navigation pane has 'Hardware' and 'Compute' highlighted with red boxes. The 'Compute' section is expanded, showing 'CPU' and 'Memory' options. The 'Memory' option is highlighted with a blue bar, and its 'EDIT' button is also highlighted with a red box. A red arrow points from the 'EDIT' button to the 'Memory' option. The right-hand pane shows the 'EDIT' section for the Memory configuration, with options for 'Memory' and 'Memory hot add'.

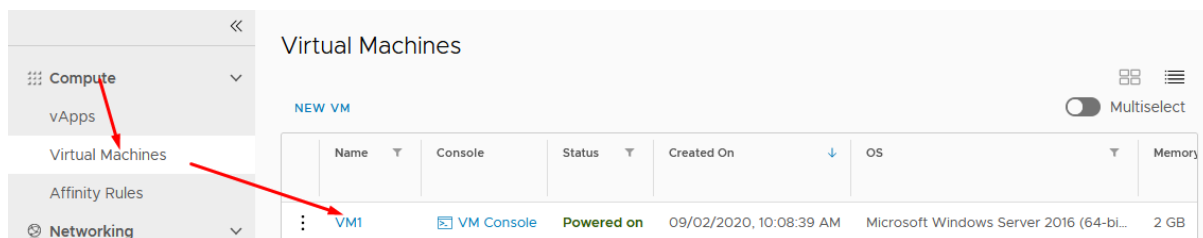
3. Increasing SSD and HDD disk size.

The screenshot shows the configuration page for VM1. The left-hand navigation pane has 'Hardware' and 'Hard Disks' highlighted with red boxes. The 'Hard Disks' section is expanded, showing a table of disks. The 'EDIT' button for the first disk is highlighted with a red box, and a red arrow points from it to the 'Size' column of the table. The 'Size' column shows '40 GB', and another red arrow points to this value. The table has columns for 'Index', 'Name', 'Size', and 'Policy'.

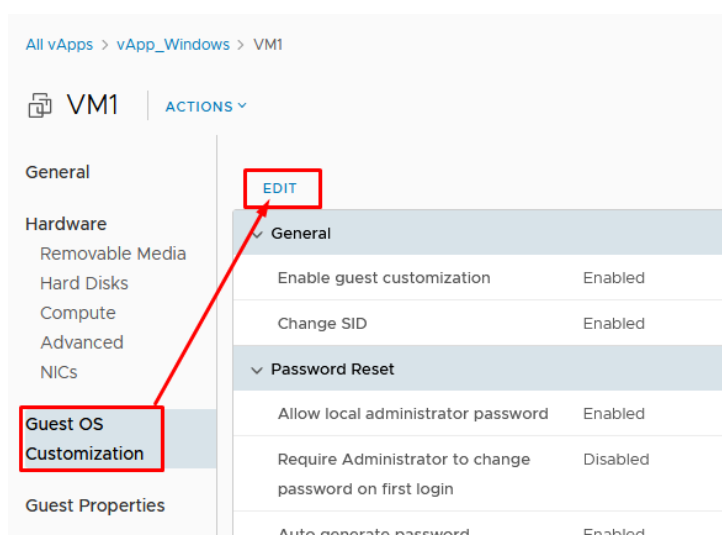
Index	Name	Size	Policy
0	-	40 GB	VM default

Virtual machine password

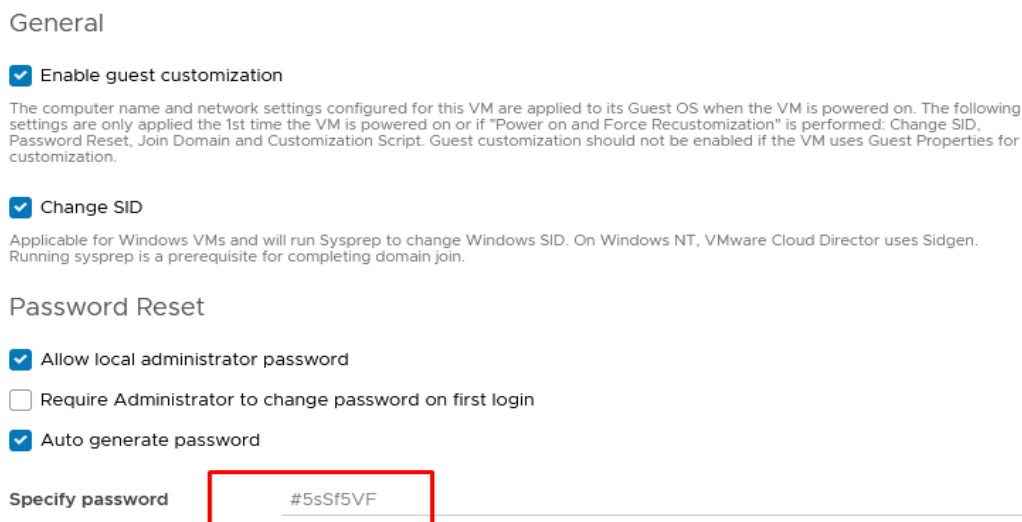
1. Press virtual machine's name



2. Go to Guest OS Customization and select Edit



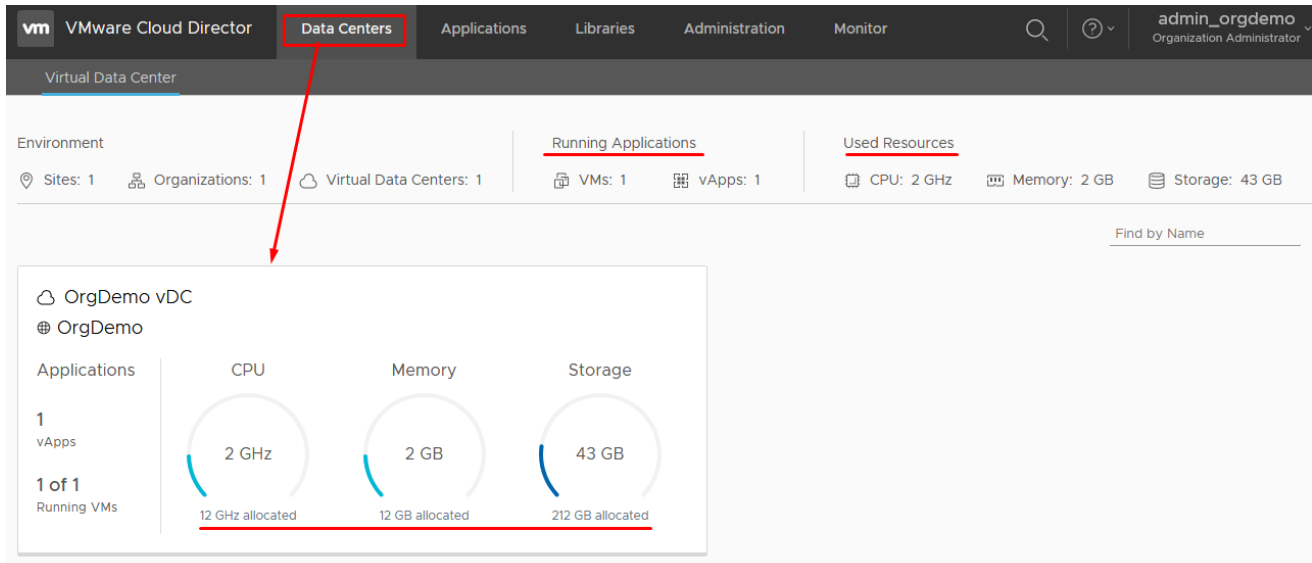
3. Generated password can be seen in „Specify password“.
Windows default admin user: administrator
Linux default admin user: root



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.

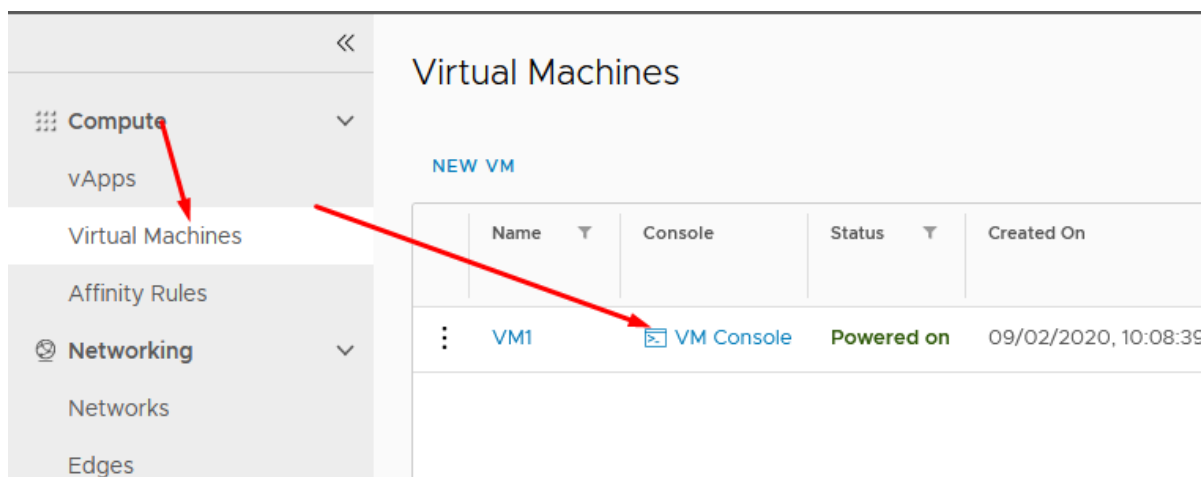
Virtual data center resource information

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



Remote Console

1. Using web console.

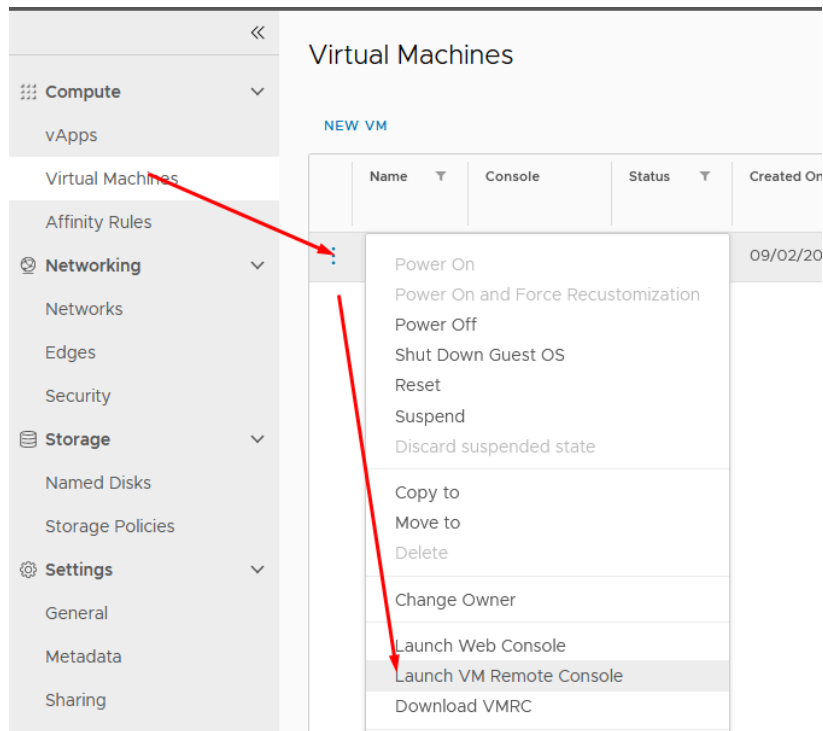


2. VMRC (VMware Remote Console) enables to login to VM console using VMRC client application. In order to use that you need to download VMRC client:

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

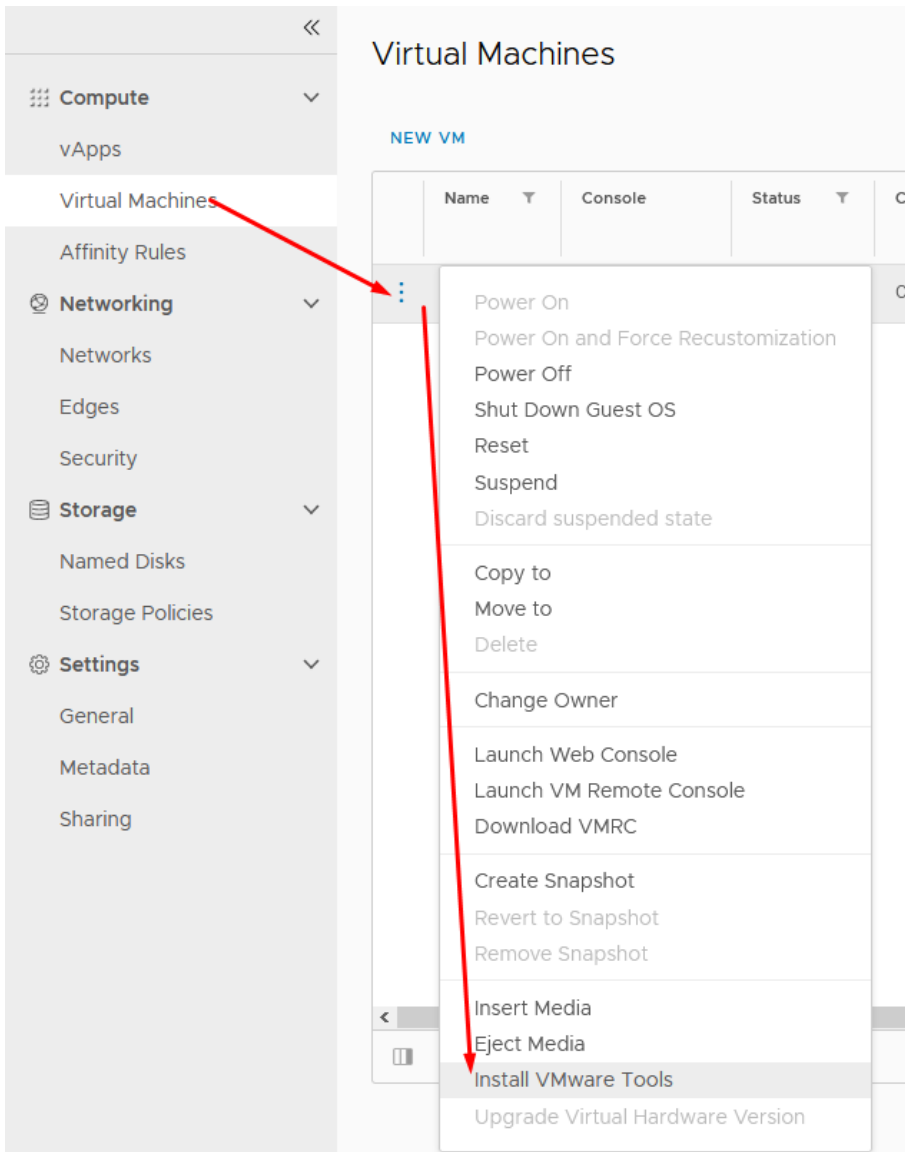
VMware Remote Console 11.1.0 for **Mac**: <https://pagalba.balt.net/images/4/45/VMware-Remote-Console-11.1.0-15913118.dmg.zip>

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“.

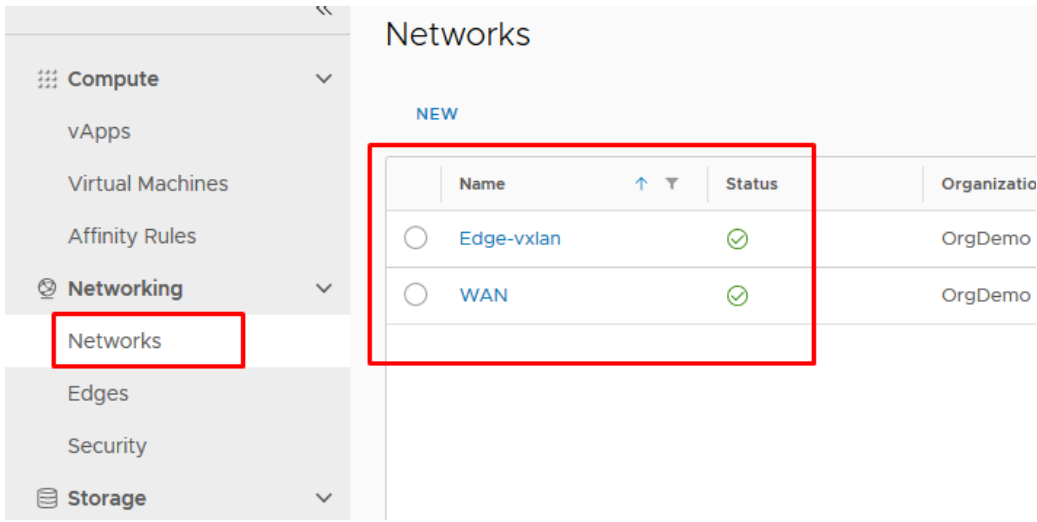


2. Launch web or VMRC console and login to the Windows OS. You will find VMware tools CD attached. Install it and reboot virtual server.
3. Alternative ways to install VMware tools are described in VMware Docs:
 Linux: <https://docs.vmware.com/en/VMware-Tools/11.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-08BB9465-D40A-4E16-9E15-8C016CC8166F.html>

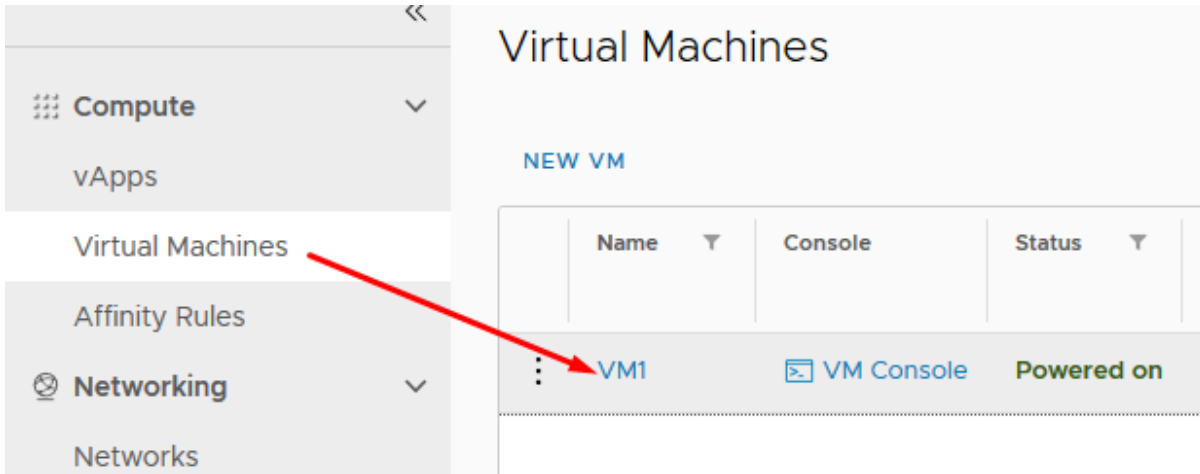
 Windows: <https://docs.vmware.com/en/VMware-Tools/11.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html>

Networking: adding network to a virtual machine

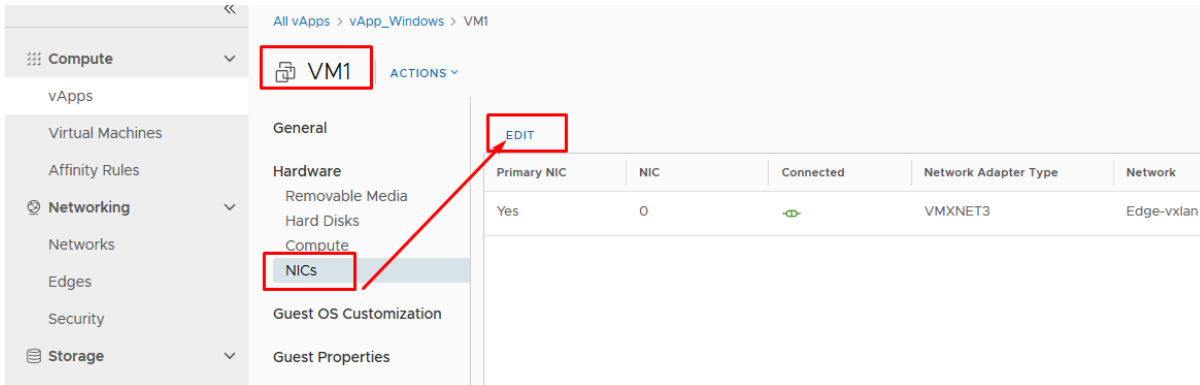
1. Organization networks can be found at Networking>Networks.



2. Press virtual machine name.



3. NICs>Edit.



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

Edit NICs for "VM1"

Guest customization may be required to run for the NIC changes to take effect.

NEW **ADD VAPP NETWORK**

NIC	Primary NIC	Connected	Adapter Type	Network	IP Mode
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	VMXNET3	Edge-vxlan	Static

5. Select OrgVDC Network, press ADD and Save.

Add Network to vApp_Windows

Type **OrgVDC Network**

Name	Status	Organization VDC	Gateway CIDR	Network Type
WAN	<input checked="" type="checkbox"/>	OrgDemo vDC	92.62.135...	Direct

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

All vApps > vApp_Windows > VM1

Compute > VM1

EDIT

Primary NIC	NIC	Connected	Network Adapter Type	Network
Yes	0	<input checked="" type="checkbox"/>	VMXNET3	Edge-vxlan

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.

Edit NICs for "VM1"

Guest customization may be required to run for the NIC changes to take effect.

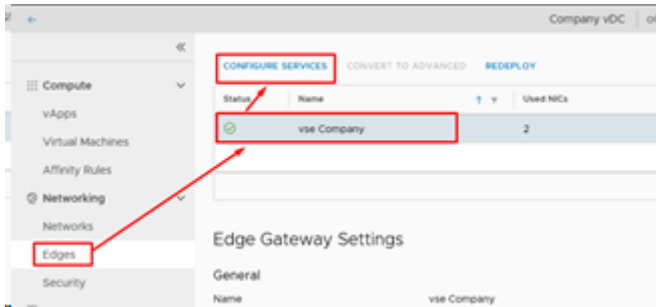
NEW **DELETE** ADD VAPP NETWORK

NIC	Primary NIC	Connected	Adapter Type	Network	IP Mode	IP	External IP
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VMXNET3	WAN	Static - IP Pool		-
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	VMXNET3	Edge-vxlan	Static - IP Pool	192.168.100.1	-

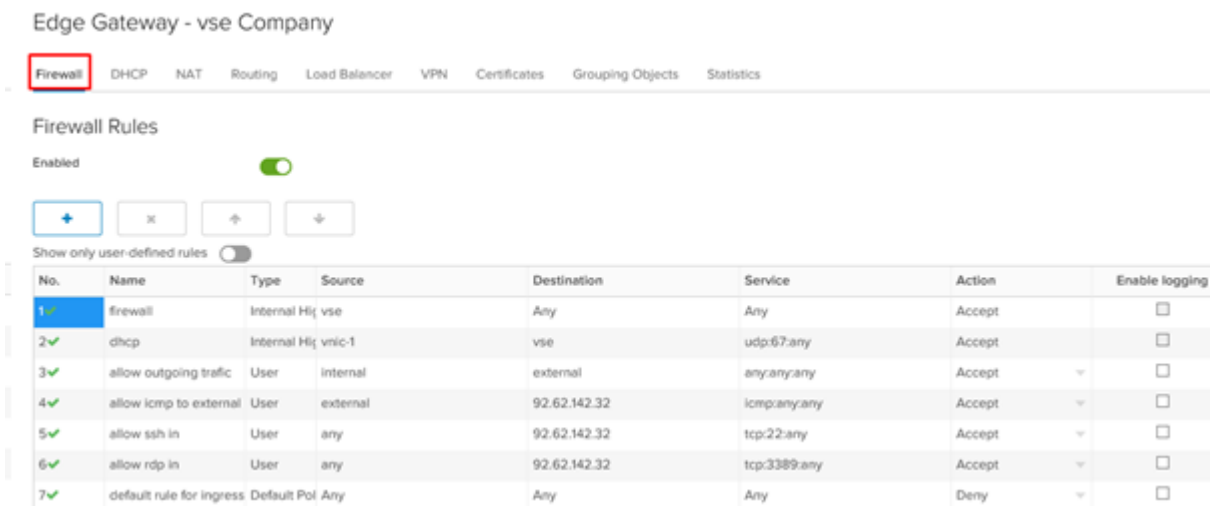
DISCARD **SAVE**

Networking: Edge Gateway

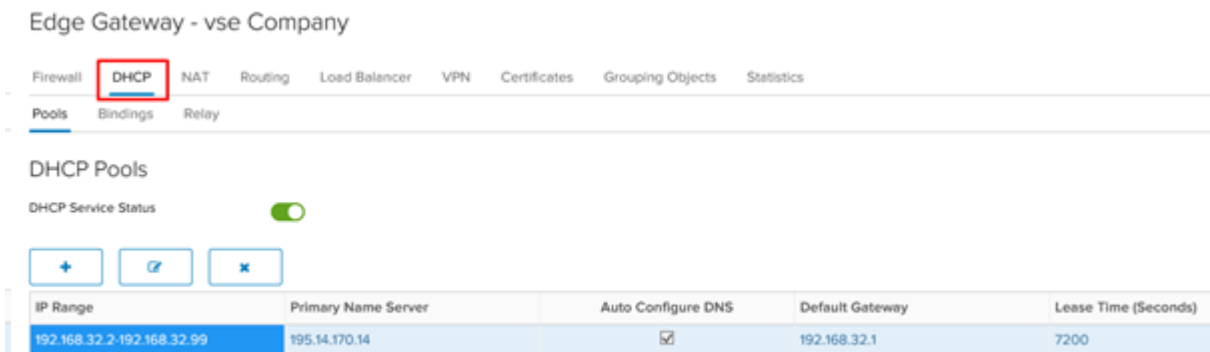
1. Edge gateway services can be configured at Networking > Edges > CONFIGURE SERVICES.



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.

Edge Gateway - vse Company

Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics

NAT Rules

+ DNAT RULE + SNAT RULE

Show only user-defined rules

ID	Type	Action	Applied on	Original		Translated		Protocol	Enabled	Logging	Description
				IP Address	Port	IP Address	Port				
196609	User-defined	SNAT	private_vlan_1521_isolated	192.168.32.0/24	Any	92.62.142.32	Any	Any	✓	✗	
196610	User-defined	DNAT	private_vlan_1521_isolated	92.62.142.32	22	192.168.32.100	22	Tcp	✓	✗	
196611	User-defined	DNAT	private_vlan_1521_isolated	92.62.142.32	3389	192.168.32.100	3389	Tcp	✓	✗	

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.

Edit SNAT Rule



Applied On: private_vlan_1521_isolated

Original Source IP/Range * 192.168.32.0/24

Translated Source IP/Range * 92.62.142.32

Description

Enabled

Enable logging



DISCARD KEEP

DNAT RULE – port forward.

EDIT DNAT Rule

Applied On: private_vlan_1521_isolated

Original IP/Range: 92.62.142.32

Protocol: TCP

Original Port: 22

ICMP Type: Any

Translated IP/Range: 192.168.32.100

Translated Port: 22

Description:

Enabled:

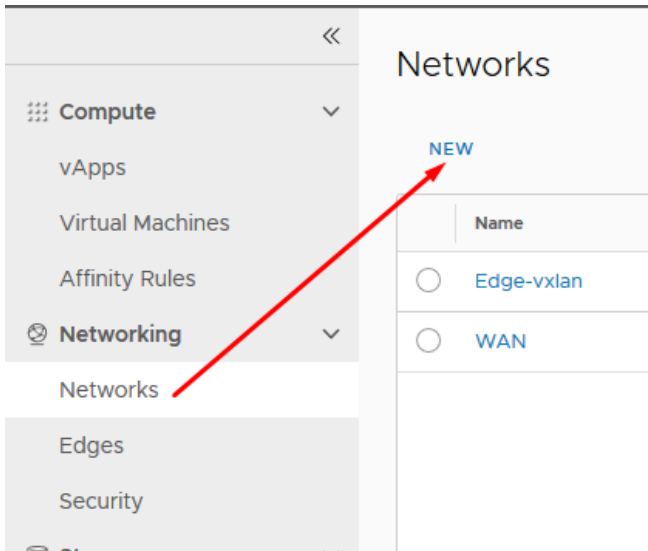
Enable logging:

DISCARD KEEP

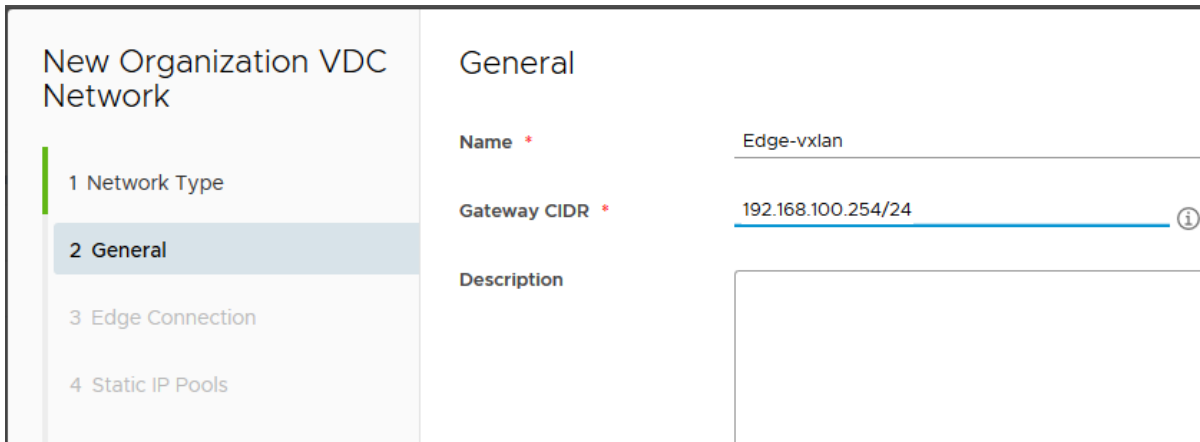
- Applied on – external network should be selected.
- Original IP/Range – external IP, usually the IP of the Edge Gateway.
- Translated – internal IP.
- Appropriate „Protocol“, „Original Port“ and „Translated port“ should be selected.

Networking: creating Edge Gateway vxlan

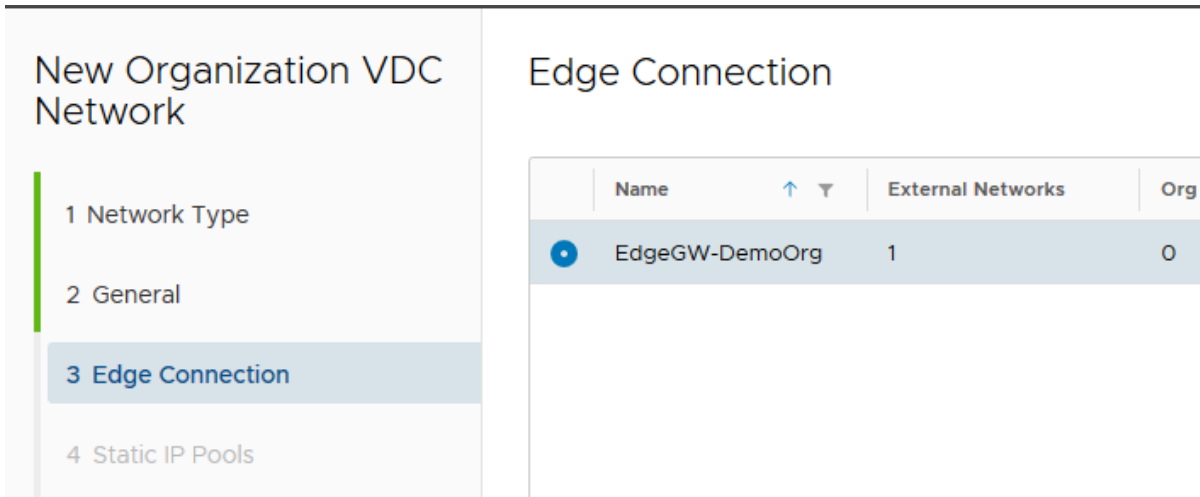
1. Select Networking > Networks, choose „NEW“.



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.

New Organization VDC Network

1 Network Type
2 General
3 Edge Connection
4 Static IP Pools
5 DNS
6 Ready to Complete

Static IP Pools

Gateway CIDR 192.168.100.254/24 ⓘ

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

192.168.100.10 - 192.168.100.100 ADD

192.168.100.10 - 192.168.100.100	MODIFY	REMOVE
----------------------------------	--------	--------

Total IP addresses: 91

6. DNS > enter desired DNS. Baltmeta 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.

< All datacenters

Edge Gateways

NEW EDIT DELETE SERVICES

Name	Status
vse DemoEdge	Normal

2. Add IPsec Sites.

Edge Gateway - vse DemoEdge

Firewall DHCP NAT Routing Load Balancer **VPN** SSL VPN-Plus

IPsec VPN L2 VPN

IPsec VPN Configuration

Activation Status Global Configuration Logging Settings **IPsec VPN Sites**

+

Site Name	Local Endpoint	Local Subnets	Peer Endpoint	Peer Subnets
No IPsec VPN sites defined				

3. Enter Edge external and internal IP addresses.

Add IPsec VPN

Enabled

Enable perfect forward secrecy (PFS)

Name	ipSecSite1
Local Id *	92.62.138.72
Local Endpoint *	92.62.138.72
	<input type="button" value="SELECT"/>
Local Subnets *	192.168.72.0/24

4. Enter Peer external and internal IP addresses.

Add IPsec VPN

Subnets should be entered in CIDR format with comma as separator.

Peer Id *	79.142.114.38
Peer Endpoint *	79.142.114.38
Peer Subnets *	192.168.1.0/24

Endpoint should be a valid IP, FQDN or any.

Subnets should be entered in CIDR format with comma as separator.

Extension

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

Add IPsec VPN

Encryption Algorithm	<input type="text" value="AES256"/>
Authentication	<input type="text" value="PSK"/>
Change Shared Key	<input type="checkbox"/>
Pre-Shared Key *	<input type="text" value="....."/>
Display Shared Key	<input type="checkbox"/>
<p>The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.</p>	
Diffie-Hellman Group	<input type="text" value="DH14"/>
Digest Algorithm	<input type="text" value="SHA1"/>
IKE Option	<input type="text" value="IKEv1"/>
IKE Responder Only	<input type="checkbox"/>

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.

