

vCloud Director 10 HTML5 F.A.Q.

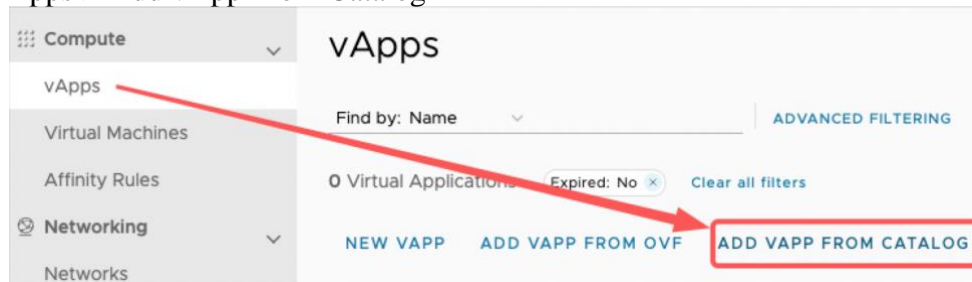
Table of Contents

VIRTUAL MACHINE CREATION FROM TEMPLATE	2
VIRTUAL MACHINE CREATION FROM ISO.....	8
IMPORTING MEDIA	11
EXPORTING VIRTUAL MACHINE.	12
CREATING VM SNAPSHOT	14
HOT ADD CPU/RAM	15
INCREASING/DECREASING VM COMPUTER RESOURCES	17
VM PASSWORD	19
VIRTUAL DATA CENTER RESOURCE INFORMATION	20
REMOTE CONSOLE	21
VMWARE TOOLS INSTALLATION:.....	22
NETWORK: ADDING NETWORK TO VAPP	22
NETWORK: ADDING NETWORK TO VM.....	24
NETWORK: EDGE GATEWAY (NEW VERSION, NSXT).....	25
NETWORK: EDGE GATEWAY (OLDER VERSION, NSXV).....	30
NETWORK: CREATING EDGE GATEWAY VXLAN.....	33
NETWORK: IPSEC CONFIGURATION EXAMPLE (OLDER VERSION, NSXV)	36
CHANGE USER PASSWORD	39

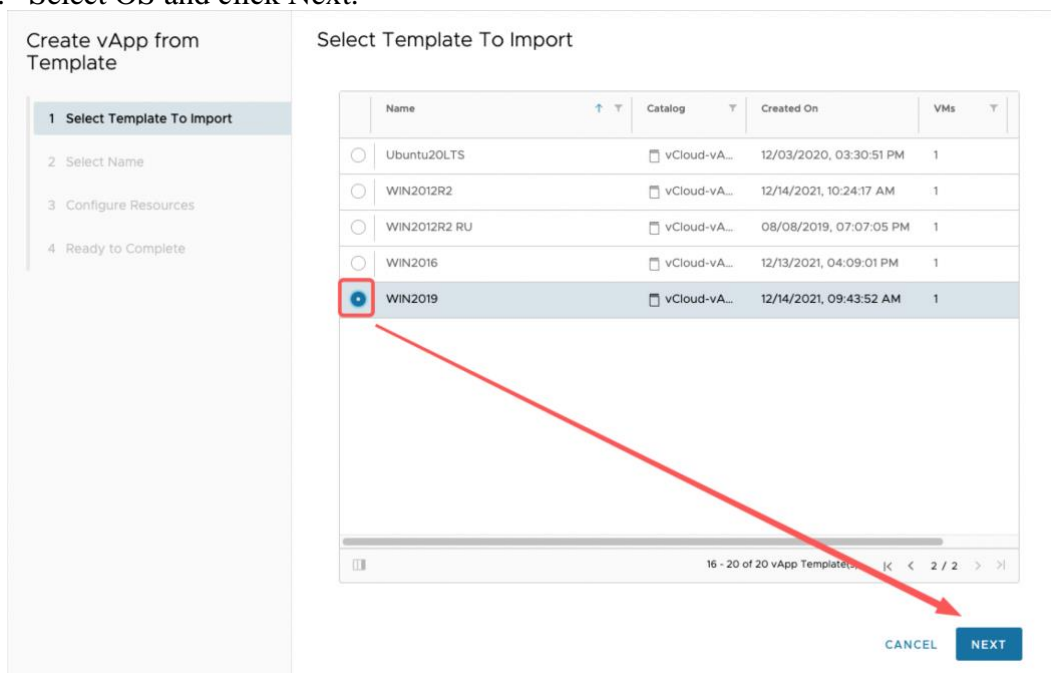
Virtual machine creation from template

Connect to your Cloud Director organization. Select your vDC.

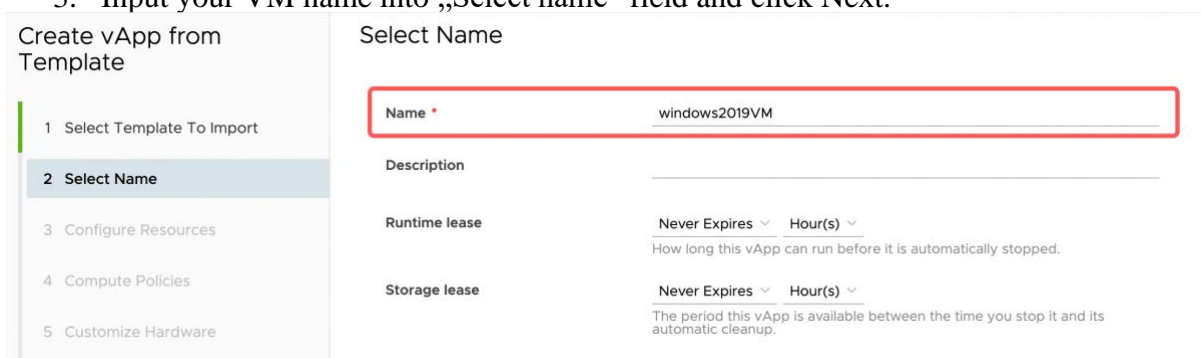
1. vApps > Add vApp From Catalog



2. Select OS and click Next.



3. Input your VM name into „Select name“ field and click Next.



4. In „Configure Resources“ tab, select available storage Policy and click Next.

Create vApp from Template

- 1 Select Template To Import
- 2 Select Name
- 3 Configure Resources
- 4 Compute Policies
- 5 Customize Hardware

Configure Resources

Select the Storage Policies that you want the deployed virtual machines of this vApp to use.

Name	Storage Policy	Default VM Template Storage Policy
Win2019	SAN SSD ▾	-

5. In "Compute Policies" tab, input necessary CPU/RAM count.

Create vApp from Template

- 1 Select Template To Import
- 2 Select Name
- 3 Configure Resources
- 4 Compute Policies
- 5 Customize Hardware
- 6 Configure Networking
- 7 Ready to Complete

Compute Policies

Configure the VM Placement and VM Sizing policies for each VM.

Virtual Machines	VM Placement Policy	VM Sizing Policy
Compute		
Virtual CPUs	2	▾
Cores per socket	1	▾
Number of sockets	2	
Memory	4	GB ▾

1 - 1 of 1 VM template(s)

6. In "Customize Hardware" tab, input disk size.

Create vApp from Template

- 1 Select Template To Import
- 2 Select Name
- 3 Configure Resources
- 4 Compute Policies
- 5 Customize Hardware
- 6 Configure Networking
- 7 Ready to Complete

Customize Hardware

Review the hardware of the virtual machines in this vApp

Virtual Machine	Storage				
Win2019	<p>Hard Disks</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Name</th> <th style="width: 40%;">Size</th> </tr> </thead> <tbody> <tr> <td>Hard disk 1</td> <td style="border: 2px solid red;">40 GB ▾</td> </tr> </tbody> </table>	Name	Size	Hard disk 1	40 GB ▾
Name	Size				
Hard disk 1	40 GB ▾				

7. In "Configure Networking" tab, under "Network" select your network.

Create vApp from Template

- 1 Select Template To Import
- 2 Select Name
- 3 Configure Resources
- 4 Compute Policies
- 5 Customize Hardware
- 6 Configure Networking**
- 7 Ready to Complete

Configure Networking

Select the networks to which you want each virtual machine to connect. You can configure additional properties for virtual machines after you complete this wizard.

Switch to the advanced networking workflow

Virtual Machines	Computer Name	Primary NIC	Network
Win2019	Win2019	● NIC 0	demowiki-vxla P Pool

CANCEL
PREVIOUS
NEXT

8. Click Finish.

Create vApp from Template

- 1 Select Template To Import
- 2 Select Name
- 3 Configure Resources
- 4 Compute Policies
- 5 Customize Hardware
- 6 Configure Networking
- 7 Ready to Complete**

Ready to Complete

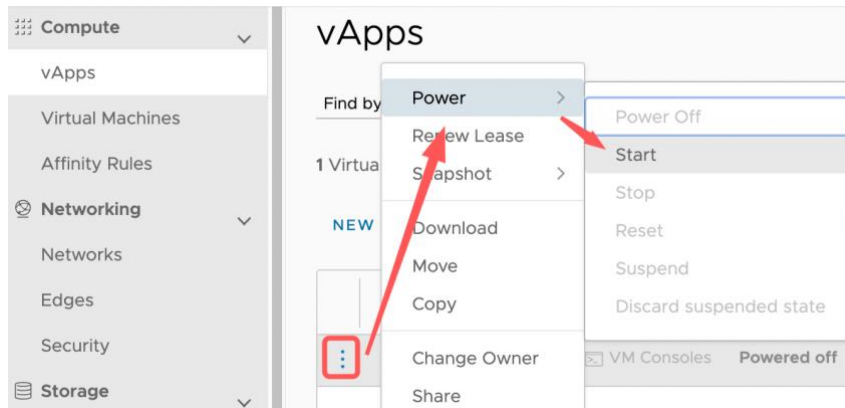
You are about to create a vApp with these specifications. Review the settings and click finish.

vApp Template	WIN2019
VDC	demoWiki_vDC
vApp name	windows2019VM
vApp description	
Runtime lease	Never Expires
Storage lease	Never Expires
Networks	demowiki-vxian

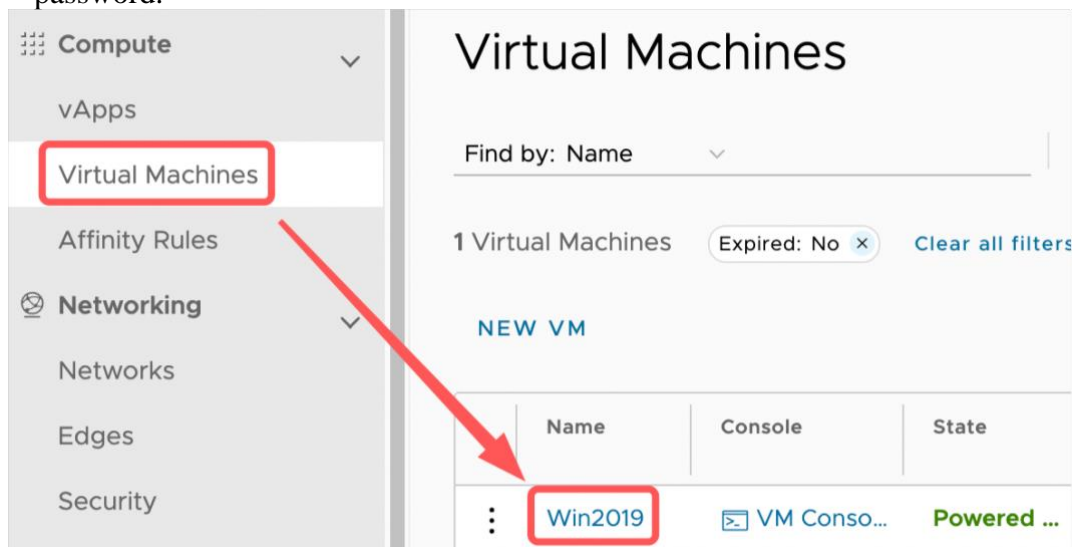
VM

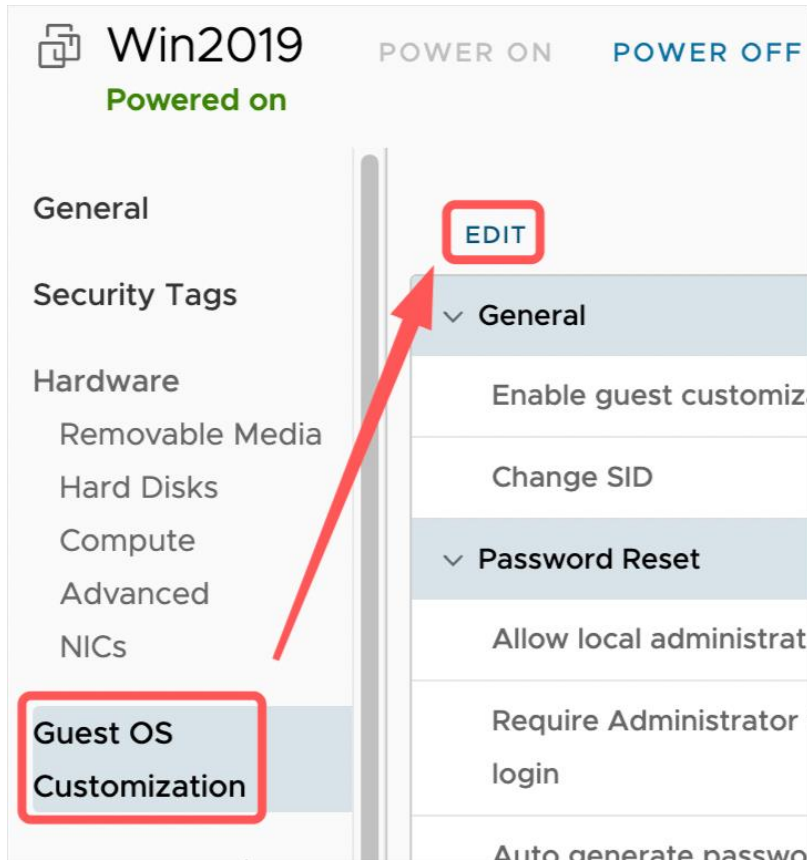
CANCEL
PREVIOUS
FINISH

9. Power on your created vApp by clicking on vApp – Power – Start.



10. You can find auto-generated root/administrator password by going to your VM in “Virtual Machines”, clicking on its name – Guest properties – Edit – Specify password.





Edit Guest Properties

General

Enable guest customization

The computer name and network settings configured for this VM are applied to its Guest OS when the VM is powered on. The following settings are only applied the 1st time the VM is powered on or if "Power on and Force Recustomization" is performed: Change SID, Password Reset, Join Domain and Customization Script. Guest customization should not be enabled if the VM uses Guest Properties for customization.

Change SID

Applicable for Windows VMs and will run Sysprep to change Windows SID. On Windows NT, VMware Cloud Director uses Sidgen. Running sysprep is a prerequisite for completing domain join.

Password Reset

Allow local administrator password

Require Administrator to change password on first login

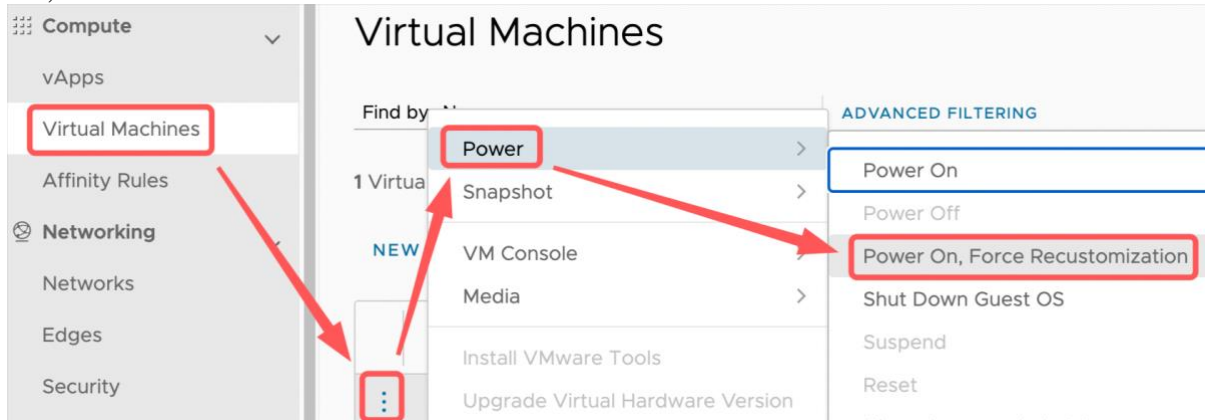
Auto generate password

Specify password

4r44 P

If there's no generated password in the field, make sure that "Enable guest customization", "change SID", "Allow local administrator password" and "Auto generate password" are turned on.

If you want to start customization process again, power off the VM, click on Power – Power On, Force Recustomization.



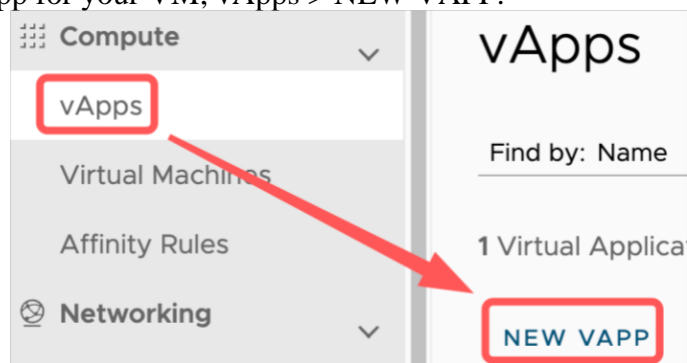
Please change the root/administrator password on the first login (from OS).

Once the VM is fully set-up, we recommend disabling "Enable guest customization".

Virtual machine creation from ISO

First, connect to your organization.

1. Create a vApp for your VM, vApps > NEW VAPP.



2. Input your vApp name, click Add virtual machine.

New vApp

Name *

Description

Power on

Virtual Machines	OS

3. Input your VM name, select “Type” = New, select OS type, ISO, VM resources.

New VM

Name *

Computer Name *

Description

Type New From Template

Operating System

OS family *

Operating System *

Boot image

Compute

Virtual CPUs

Cores per socket

Number of sockets

Memory

Storage [ADD](#)

Disk	Storage Policy	IOPS	Size
1	VM default policy	Not Applicable	<input type="text" value="40"/> GB

4. Select your network, click OK

Networking [< UNDO CHANGES AND GO BACK](#) [ADD](#)

NIC	Network	Network Adapter Type	IP Mode	IP Address	Primary NIC
1	<input type="text" value="demowiki-vxlan"/>	VMXNET3	<input type="text" value="Static - IP Pool"/>	Auto-assigned	<input checked="" type="radio"/>

5. Click Create.

New vApp ×

Name * 🔍

Description

Power on

Virtual Machines	OS	Compute									
vmUnix	Debian GNU/Linux 10 (64-bit)	<table border="1"> <tr> <td>CPU</td> <td>2</td> <td>🗑️</td> </tr> <tr> <td>Memory</td> <td>4 GB</td> <td></td> </tr> <tr> <td>Disk</td> <td>40 GB</td> <td></td> </tr> </table>	CPU	2	🗑️	Memory	4 GB		Disk	40 GB	
CPU	2	🗑️									
Memory	4 GB										
Disk	40 GB										

[ADD VIRTUAL MACHINE](#)

[CANCEL](#) [CREATE](#)

6. Power On your VM.

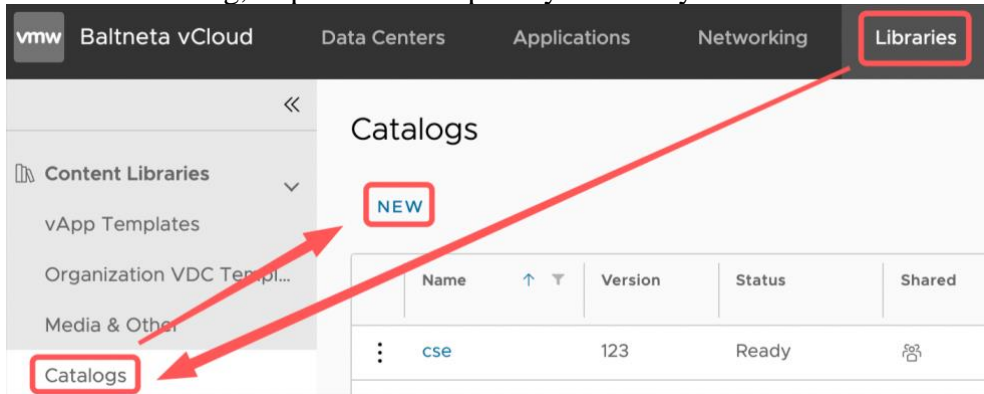
The screenshot shows the 'Virtual Machines' page in the Compute section. The 'Virtual Machines' menu item is highlighted with a red box. A context menu is open over a VM, with 'Power' selected and a sub-menu showing 'Power On' as the active option, also highlighted with a red box. Other options in the sub-menu include Power Off, Power On, Force Recustomization, Shut Down Guest OS, Suspend, Reset, and Discard suspended state.

7. Open VM Console, and proceed to OS installation.

The screenshot shows the 'Virtual Machines' page. The 'Virtual Machines' menu item is highlighted with a red box. A context menu is open over a VM, with 'VM Console' selected and a sub-menu showing 'Launch Web Console' as the active option, also highlighted with a red box. Other options in the sub-menu include Launch Remote Console and Download VM Remote Console. Red arrows point from the 'Virtual Machines' menu item to the context menu and from 'VM Console' to the sub-menu.

Importing media

1. Create new catalog, or proceed to step 2 if you already have one.



Create Catalog

Name this Catalog

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

Name *

Description

Pre-provision on specific storage policy

Subscribed Catalog

A subscribed catalog is a read-only copy of an external published catalog and cannot be modified. Check the box and provide the location URL and an optional password.

Subscribe to an external catalog

Subscription URL *

Example: `https://www.example.com/catalogs/my-catalog/` or `file:///data/catalogs/my-catalog/`

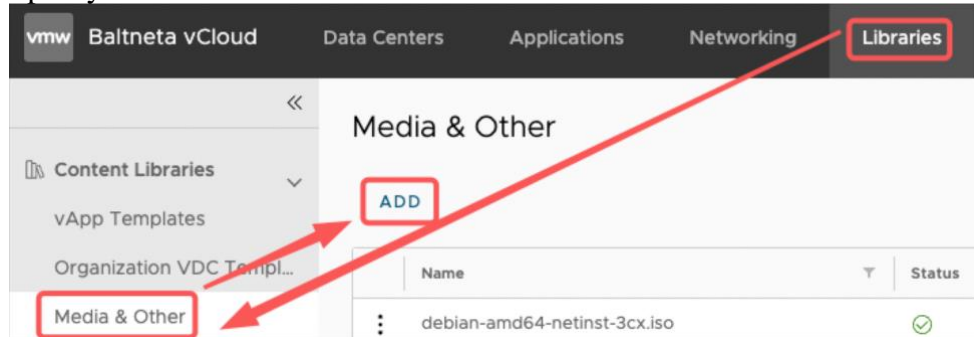
Password

Supply an optional password to access the catalog.

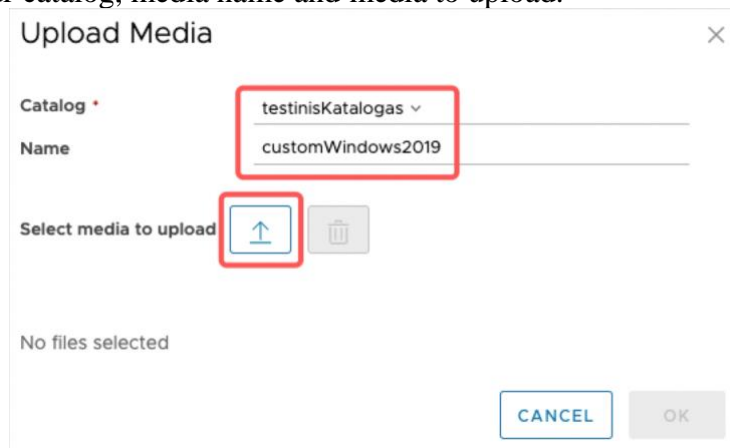
Automatically download the content from an external catalog

If you enable this option, the system performs automatic synchronization of all remote items as part of the catalog sync. If you disable this option, you need to sync manually the individual items in the subscribed catalog.

2. Import your media.

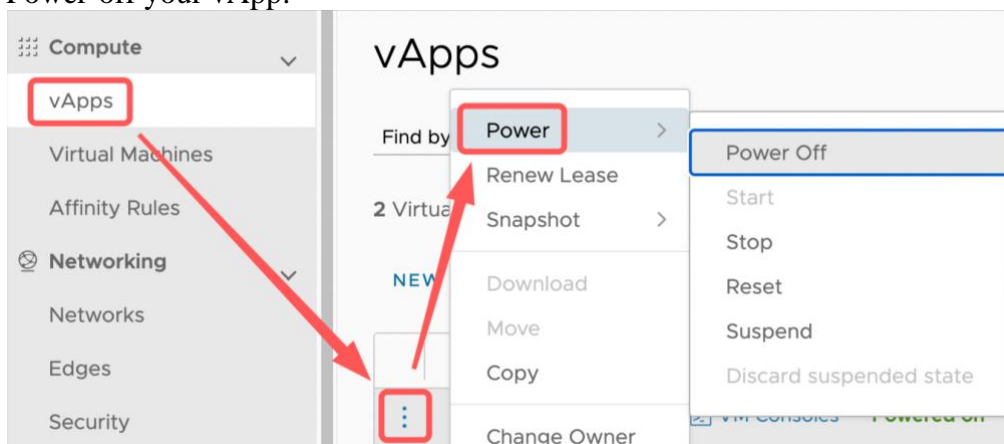


3. Select your catalog, media name and media to upload.

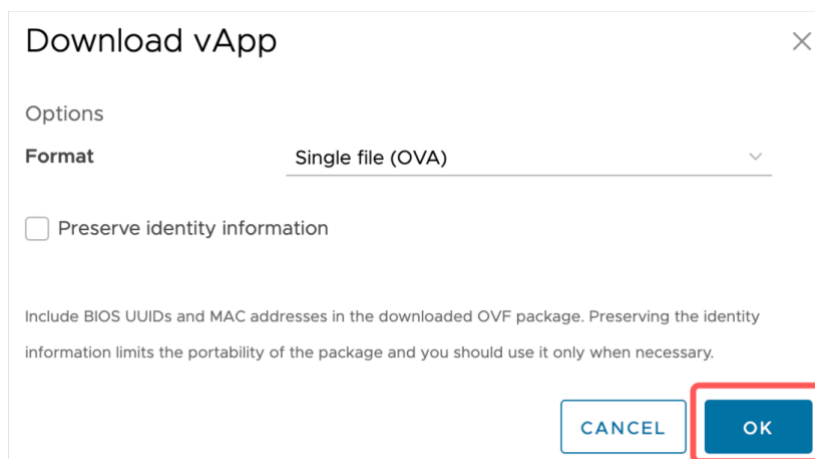
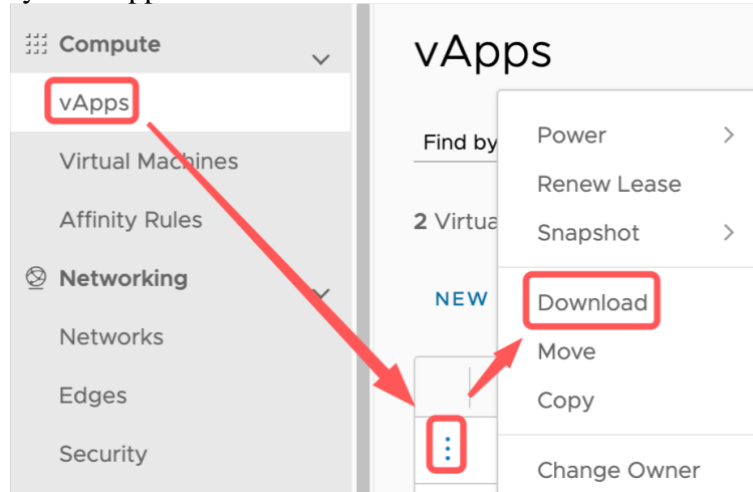


Exporting virtual machine.

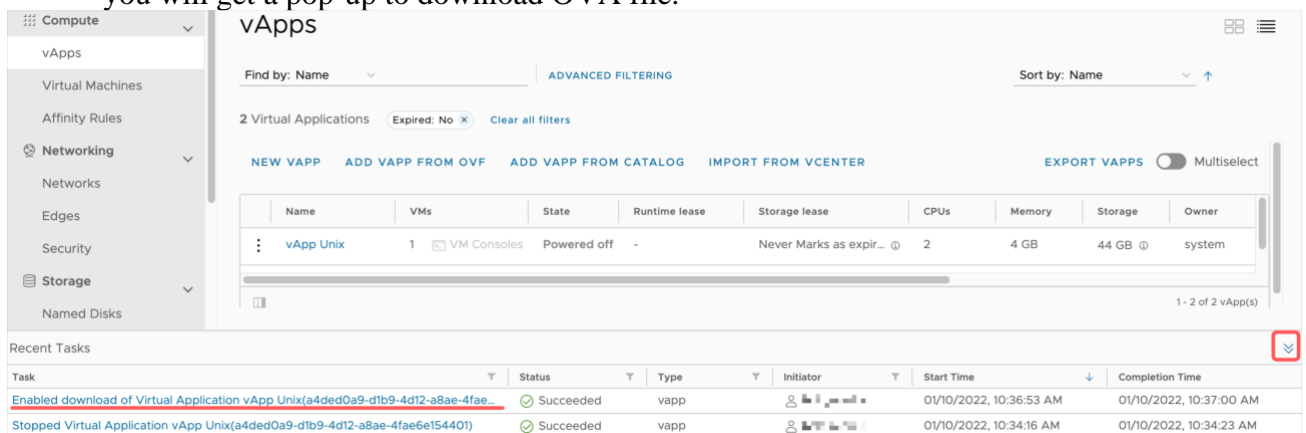
1. Power-off your vApp:



2. Download your vApp:



3. At the bottom of the page, you can see the status of the process. Once it's finished, you will get a pop-up to download OVA file.



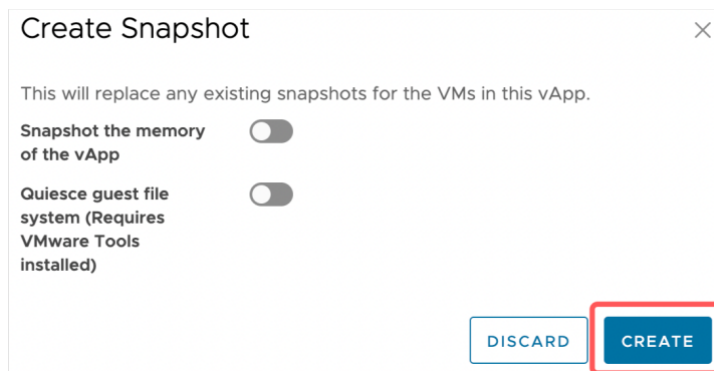
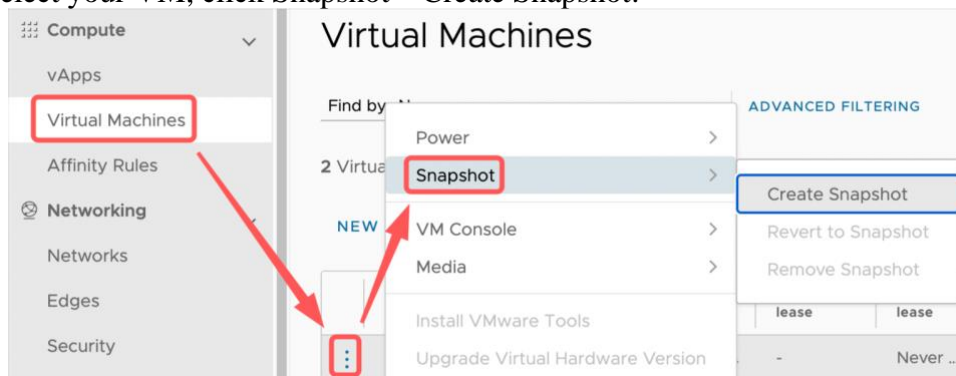
Creating VM Snapshot

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“.

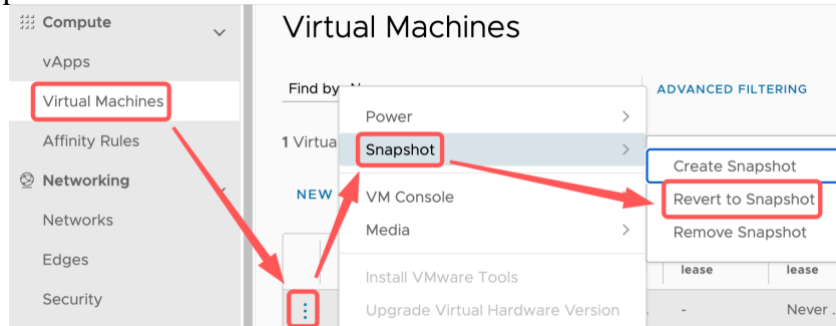
In order to create a VM „Snapshot“ you must have a free space in your virtual data center. E.g., if VM’s disk size is 100 GB, you will need 100 GB space for the snapshot.

Limitations: you can only have one “Snapshot”

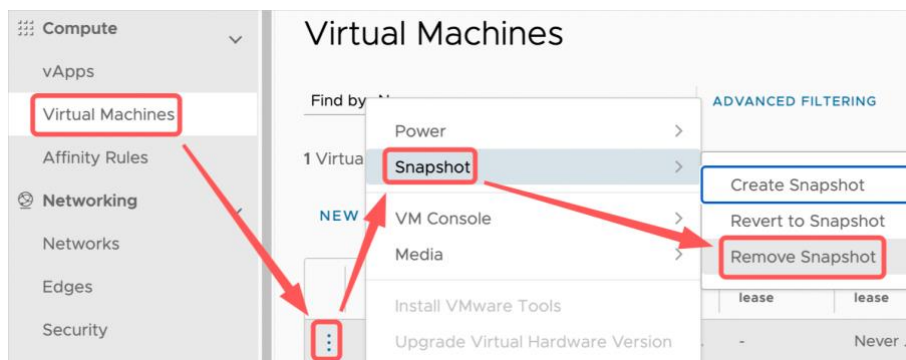
1. Select your VM, click Snapshot – Create Snapshot:



2. If you want to revert the VM to the snapshot, click the VM, select Snapshot – Revert to Snapshot.



3. If the snapshot is no longer needed, click on the VM, select Snapshot – Remove Snapshot.

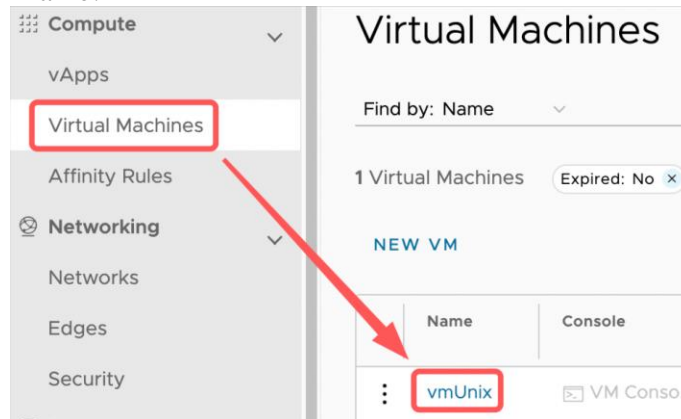


Hot Add CPU/RAM

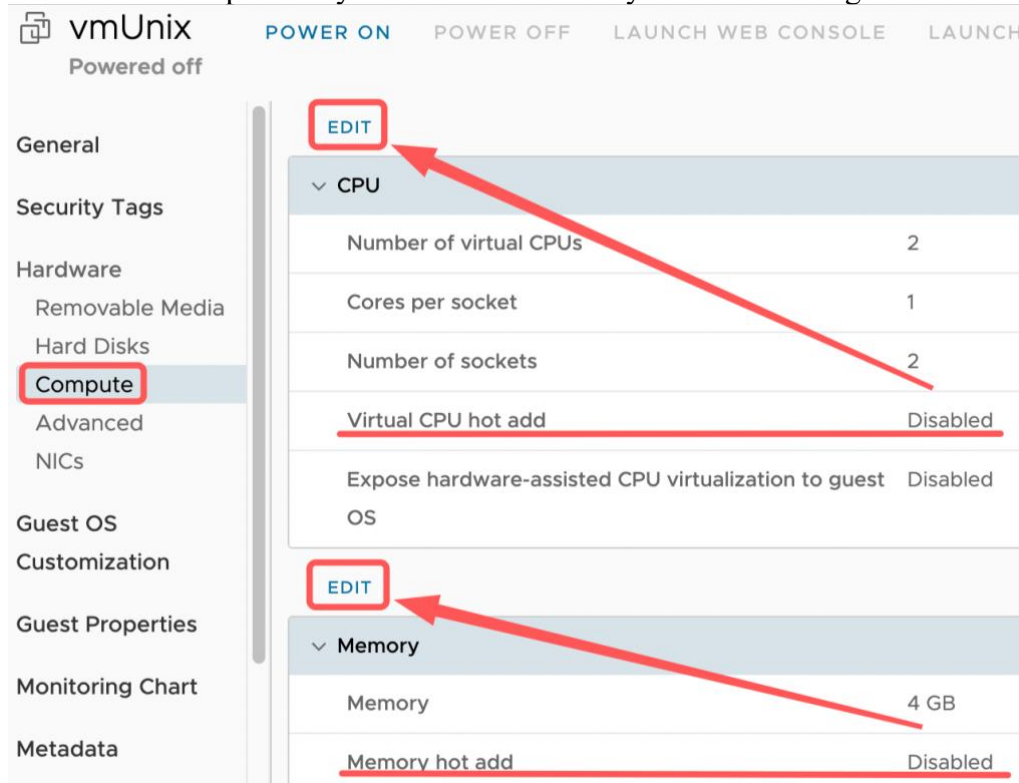
HOT add CPU and RAM technology is used in order to increase virtual machine's CPU and/or RAM without downtime. „Hot add“ can be enabled only while VM is powered off. Some operating systems may not support this technology, therefore it is best to check with the software manufacturer.

To view Hot Add status:

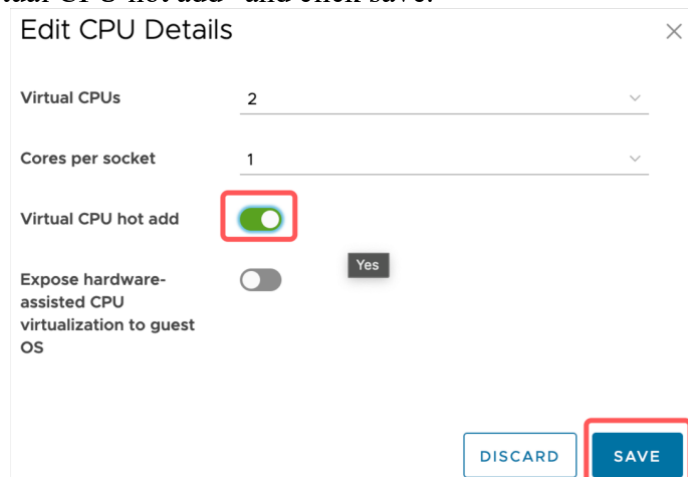
1. Click on VM name:



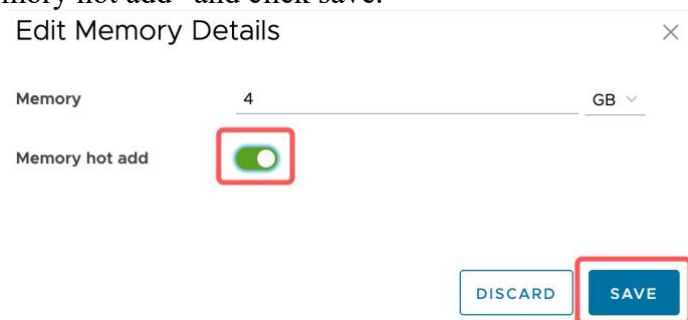
2. On Hardware>Compute tab you'll see its status. If you want to change it click "Edit"



3. Enable “Virtual CPU hot add” and click save.



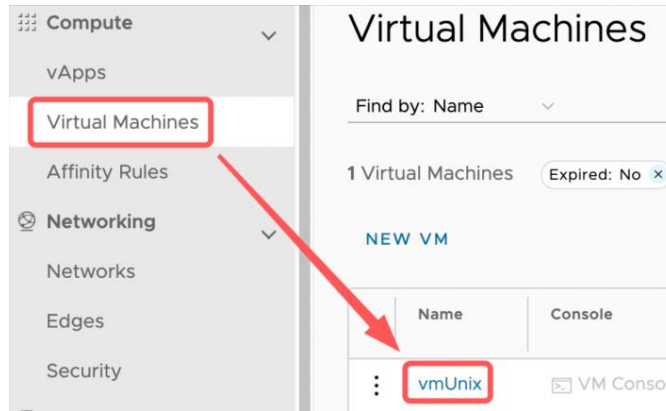
4. Enable “Memory hot add” and click save.



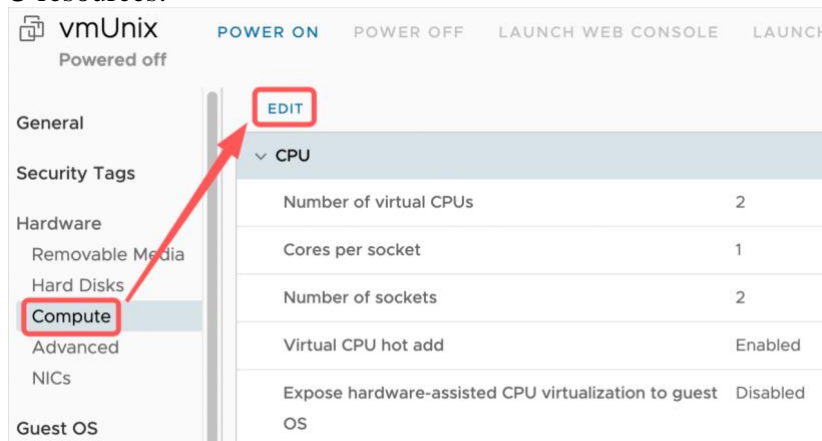
Increasing/decreasing VM computer resources

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 Baltmeta technicians.

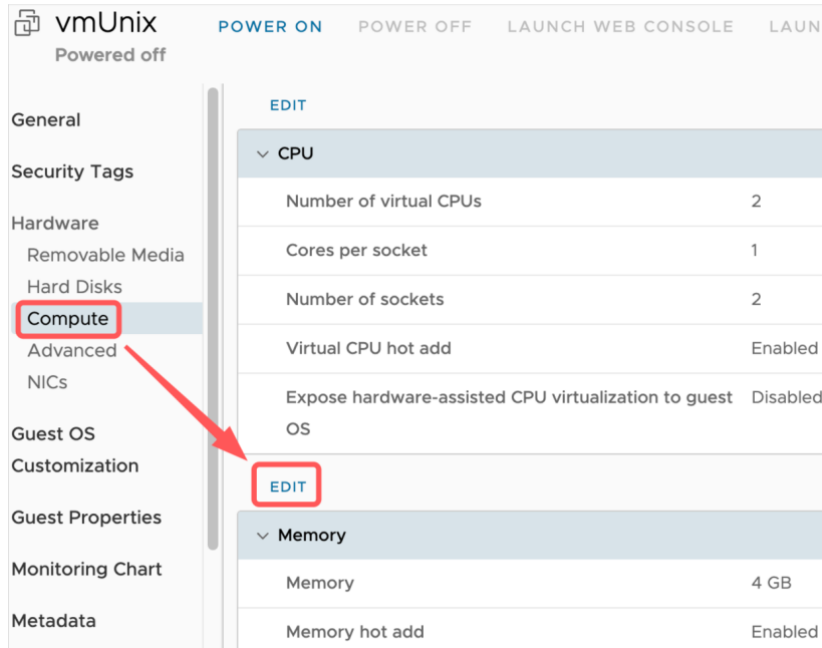
Click on VM name.



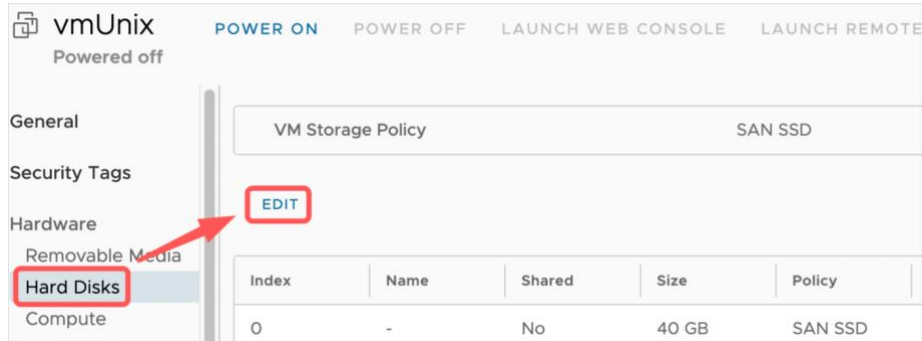
Changing vCPU resources:



Changing RAM resources:

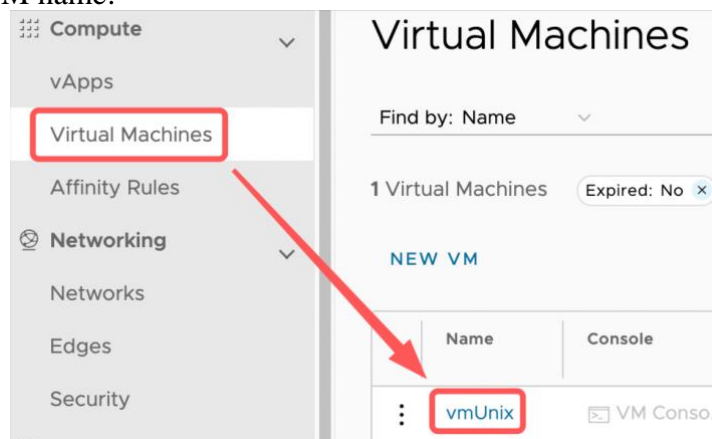


Changing Disk resources:

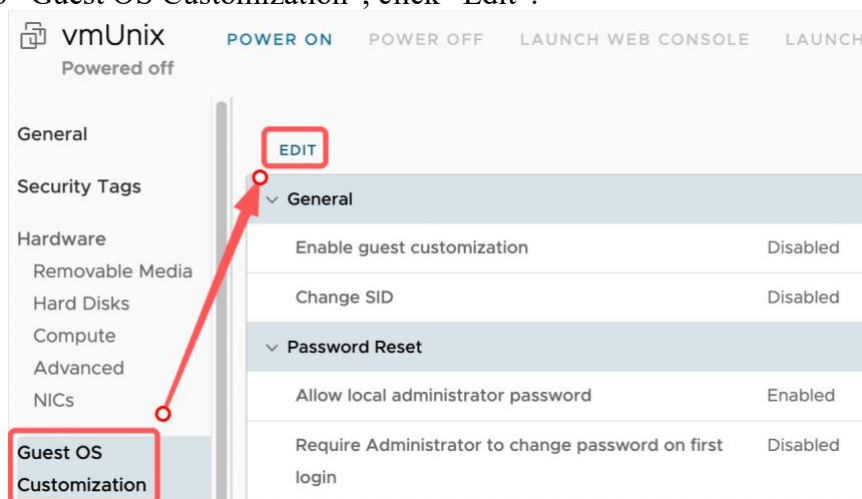


VM password

1. Click on VM name:



2. Go to “Guest OS Customization”, click “Edit”:



- The generated password. Can be seen in “Specify password” field.
Windows default admin user: administrator
Linux default admin user: root

Edit Guest Properties

General

Enable guest customization

The computer name and network settings configured for this VM are applied to its Guest OS when the VM is powered on. The following settings are only applied the 1st time the VM is powered on or if "Power on and Force Recustomization" is performed: Change SID, Password Reset, Join Domain and Customization Script. Guest customization should not be enabled if the VM uses Guest Properties for customization.

Password Reset

Allow local administrator password

Require Administrator to change password on first login

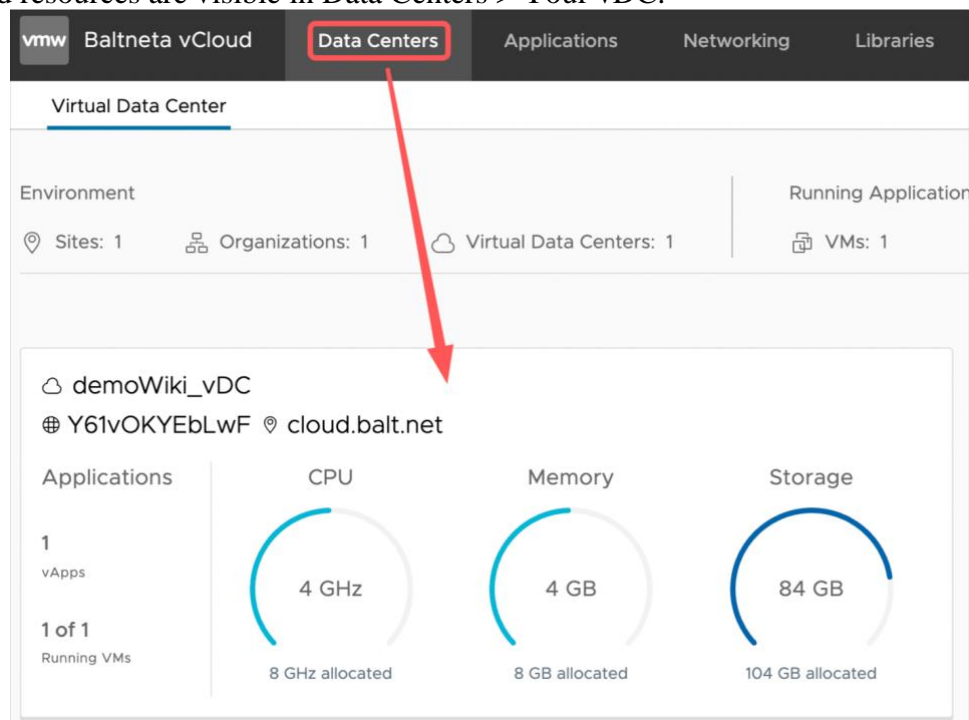
Auto generate password

Specify password

- Please change the root/administrator password on the first login (from OS).
Once the VM is fully set-up, we recommend disabling “Enable guest customization”.

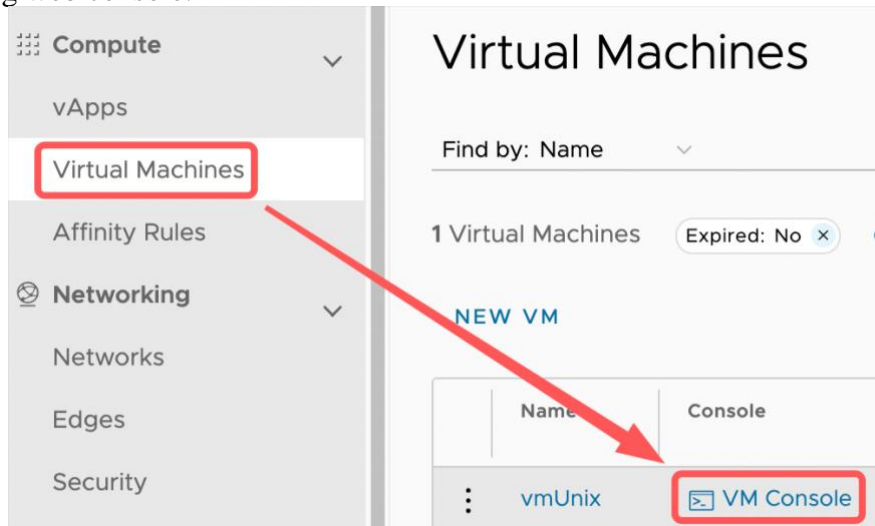
Virtual data center resource information

Allocated resources are visible in Data Centers > Your vDC.



Remote Console

- Using web console:



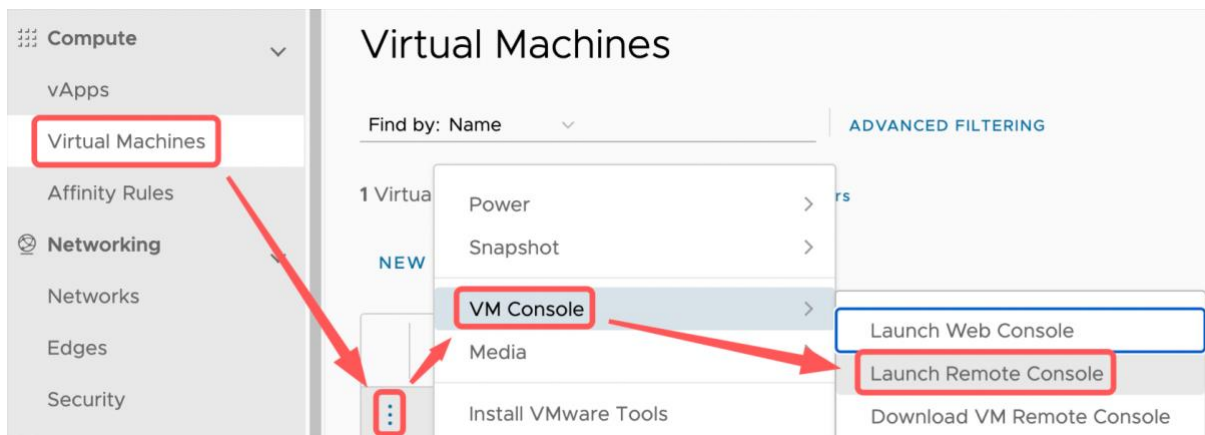
- Using (VMRC) VMware Remote Console application:

Application can be downloaded from:

Windows: <https://pagalba.balt.net/images/a/a1/VMware-VMRC-12.0.1-18113358.zip>

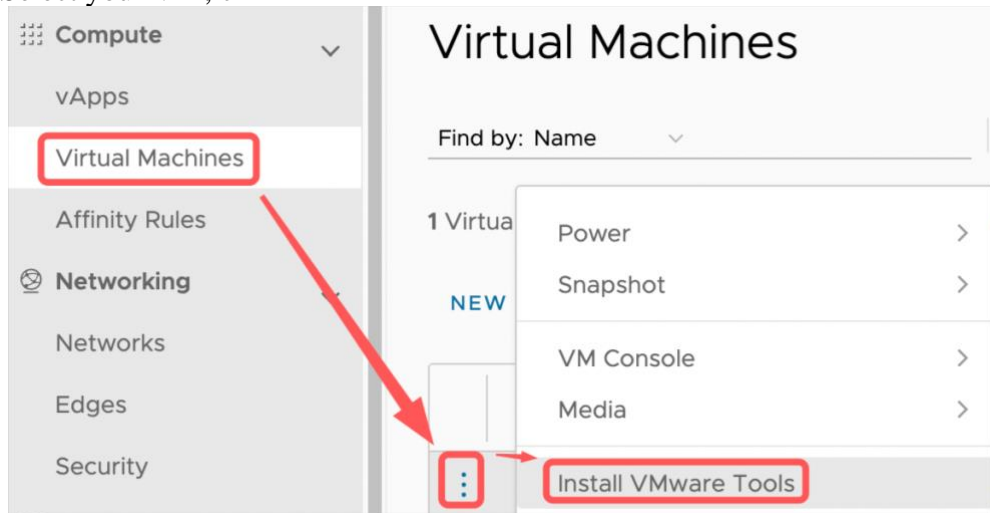
Linux: https://pagalba.balt.net/images/c/c3/VMware-Remote-Console-12.0.1-18113358.x86_64.bundle

OSX: <https://apps.apple.com/us/app/vmware-remote-console/id1230249825>



VMware tools installation:

1. Select your VM, click on “Install VMware Tools”:



2. Launch web or VMRC console and login to the OS. You will find VMware tools CD attached. Install it and reboot VM.
3. Alternative ways to install VMware tools are described in VMware Docs:

Linux: <https://docs.vmware.com/en/VMware-Tools/11.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-08BB9465-D40A-4E16-9E15-8C016CC8166F.html>

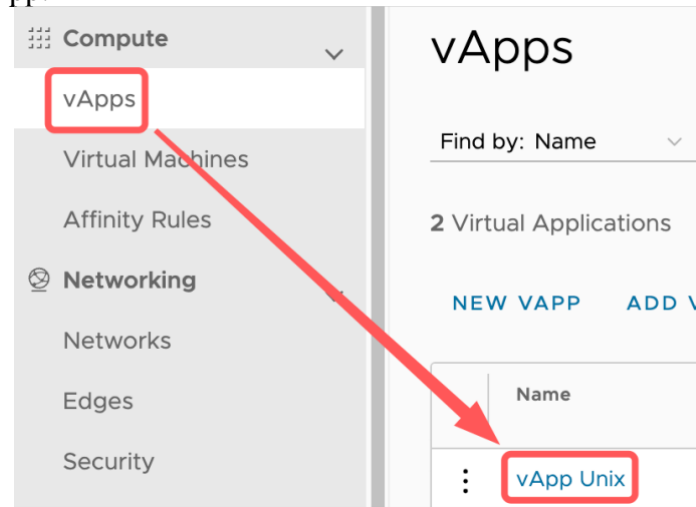
Windows: <https://docs.vmware.com/en/VMware-Tools/11.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html>

Network: adding network to vApp

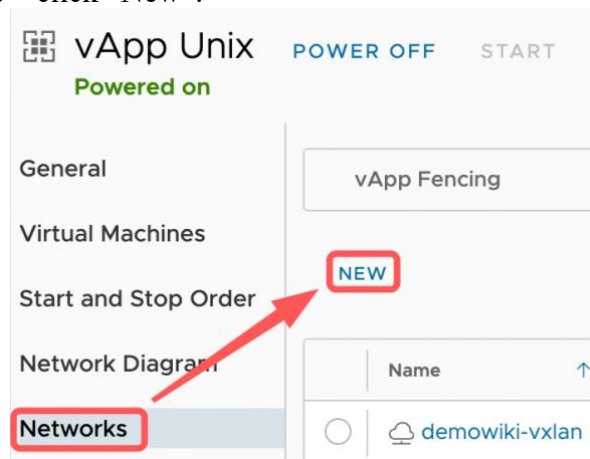
1. You can view organization networks on Networking>Networks.



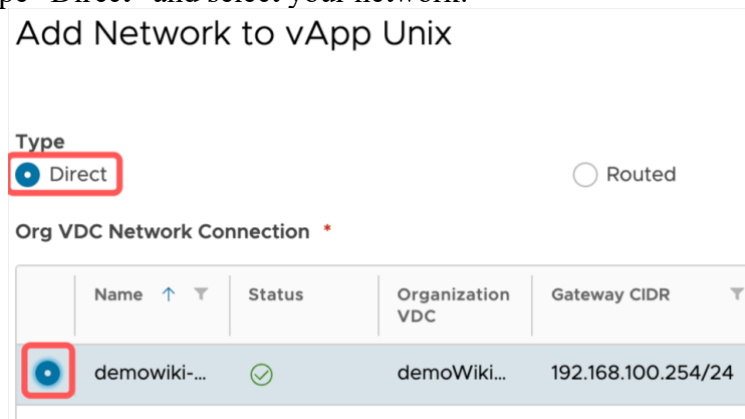
2. Click on vApp:



3. Go to Networks – click “New”:

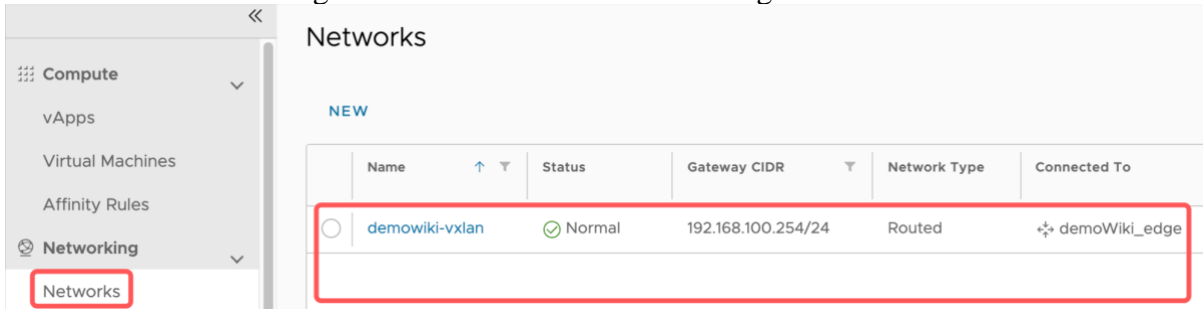


4. Select Type “Direct” and select your network:

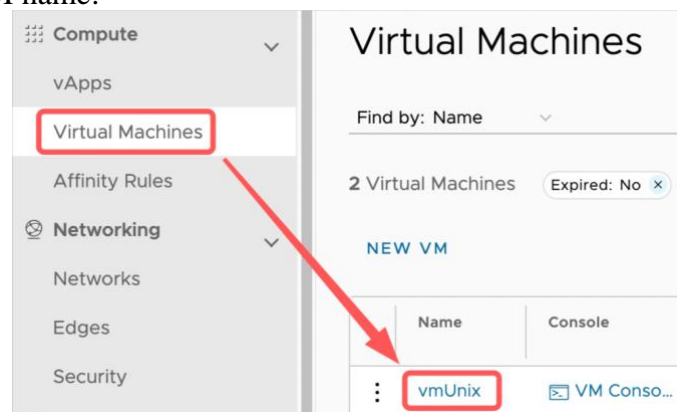


Network: adding network to VM

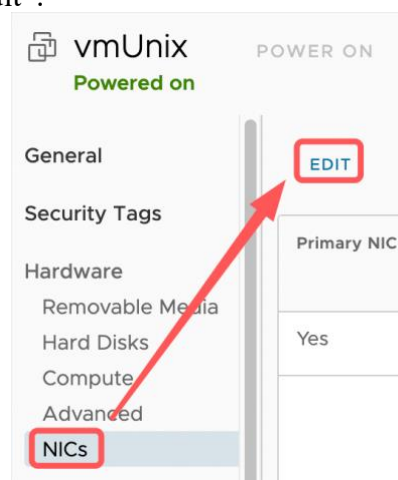
1. You can view organization networks on Networking>Networks.



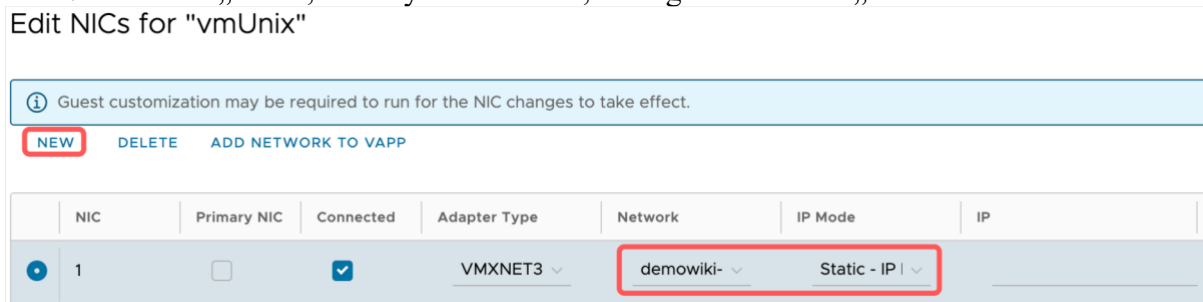
2. Click on VM name:



3. Go to NICs – click „Edit“:



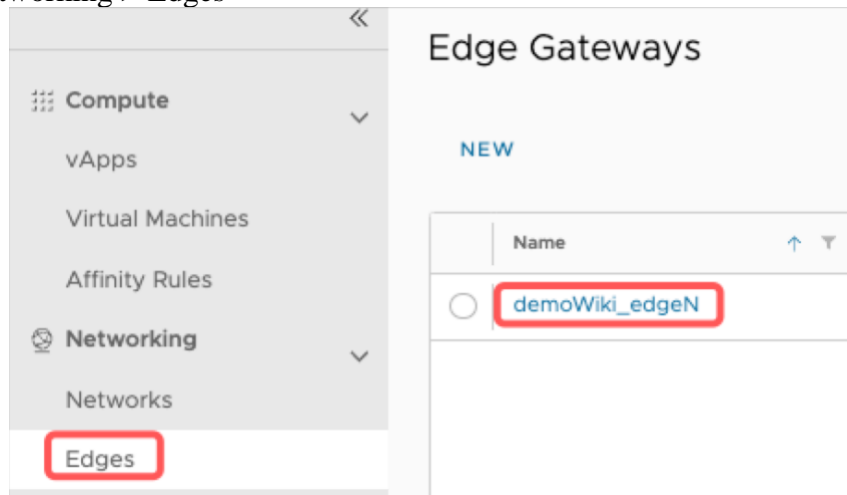
4. Click on „New“, select your Network, Change IP mode to „Static – IP Pool“
 Edit NICs for "vmUnix"



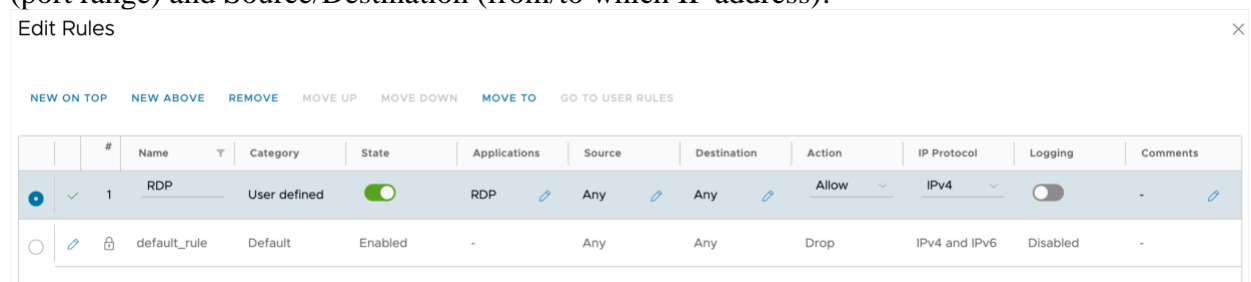
If your network is not in the list, make sure it's added to vApp.

Network: Edge Gateway (new version, nsxt)

Go to Networking > Edges



Firewall Tab – for creating firewall rules. It is important to specify an application (port range) and Source/Destination (from/to which IP address):



If you can't find the necessary application (port range) in the list, you can create your own by going to „Security“ – „Application Port Profiles“:

demoWiki_edgeN [OPEN IN VDC CONTEXT](#) [DELETE](#) [INCREASE SCOPE](#)

Configuration
 General
 Edge Cluster
 Rate Limiting

Services
 Firewall
 NAT
 IPSec VPN
 L2 VPN

Load Balancer
 General Settings

Security
 Static Groups
 IP Sets
Application Port Profiles

Custom Applications ⓘ

NEW

Name	Status	Description
avi-ControllerCluster	Normal	-

Default Applications ⓘ

Name	Status	Description
Active Directory Server	Normal	Active Directory Server
Active Directory Server UDP	Normal	Active Directory Server UDP
AD Server	Normal	AD Server
CIM-HTTP	Normal	CIM-HTTP

New Application Port Profile

Name * My Custom port

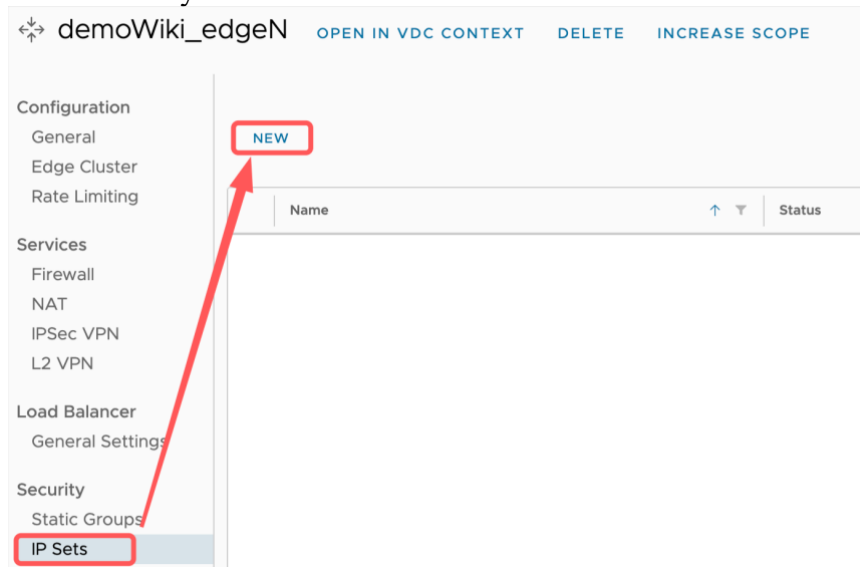
Description
 For spec. application

ADD PORT PROFILE

Protocol TCP

Ports 111,222,333
 Ports separated by comma

If you want to limit access by Source/Destination IP but can't find the one you need on the list, you can create your own on "IP Sets" tab:



New IP Set

Name *

Description

IP Addresses Enter an IPv4 or IPv6 address, range or CIDR [?](#)

1.1.1.1	ADD
	MODIFY
	REMOVE
	UNDO

NAT tab – you can create port forward rules

Edit NAT Rule

Name * ssh

Description

Interface Type * DNAT

External IP * 92.168.101.0/24
Destination IP or CIDR

External Port 22
Destination Port

Internal IP * 192.168.101.101
Translated IP or CIDR

Application SSH

Translated Port

Advanced Settings

State

Logging

Priority 0
If an address has multiple NAT rules, the rule with the highest priority is applied. A lower value means a higher precedence for this rule.

Firewall Match Match External Address
Determines how the firewall matches the address during NATing if firewall stage is not skipped. Below are valid values:

Applied To -
Applies this NAT rule only for the selected Org Vdc network. Only networks with distributed routing disabled can be used.

DISCARD SAVE

Edit NAT Rule

Name * 196609

Description

Interface Type * SNAT

External IP * 92.168.101.0/24
Destination IP or CIDR

Internal IP * 192.168.101.0/24
Source IP or CIDR

Destination IP

Advanced Settings

State

Logging

Priority 0
If an address has multiple NAT rules, the rule with the highest priority is applied. A lower value means a higher precedence for this rule.

Firewall Match Match Internal Address
Determines how the firewall matches the address during NATing if firewall stage is not skipped. Below are valid values:

Applied To -
Applies this NAT rule only for the selected Org Vdc network. Only networks with distributed routing disabled can be used.

DISCARD SAVE

- SNAT interface type – Lets you create internet access for VMs that are using Edge GW.
- DNAT interface type – Lets you create access through a specific port.
- External IP – must be Edge gateway IP, you can find it in „IP Management“ - „IP Allocations“ - „Ips Used“ tab.
- Internal IP - internal IP range.
- Application - Specific port range.

IPSec VPN

When creating IPSec tunnel, choose “Peer Authentication Mode” - “Pre-Shared Key” and enter your own key that you want to use.

“Endpoint Configuration” - “Local Endpoint” – “IP Address” enter Edge router external IP, „Networks“ input your internal networks (for example 192.168.1.0/24) that are connected to the Edge router (vxlan).

„Remote Endpoint“ enter remote network point info to which you want to connect the tunnel, „IP Address“ and „Remote ID“ – external IP, „Networks“ – internal IP range/subnet.

Add IPSec VPN Tunnel

- 1 General Settings
- 2 Peer Authentication Mode
- 3 Endpoint Configuration
- 4 Ready to Complete

Endpoint Configuration

Local Endpoint

IP Address *

Networks *

Comma separated CIDRs (i.e. 192.168.10.0/24, 212.138.0.0/16)

Remote Endpoint

IP Address *

Networks *

Comma separated CIDRs (i.e. 192.168.10.0/24, 212.138.0.0/16)

Remote ID

Once the tunnel is created, we recommend changing security settings to these (or to what your remote point supports):

Configuration

- General
- Edge Cluster
- Rate Limiting

Services

- Firewall
- NAT
- IPSec VPN
- L2 VPN

[NEW](#) [EDIT](#) [VIEW STATISTICS](#) SECURITY PROFILE CUSTOMIZATION [DELETE](#)

	Name	State	Security Profile
+	testIPSec	✔ Enabled	User Defined

Customize Security Profile ✕

IKE Profiles

Version * ▼ IKE v2

Encryption * ▼ AES 256

Digest * ▼ SHA 2 - 256

Diffie-Hellman Group * ▼ Group 14

Association Life Time (seconds) 86400

Tunnel Configuration

Enable Perfect Forward Secrecy

Defragmentation Policy ▼ Copy

Encryption * ▼ AES 256

Digest * ▼ SHA 2 - 256

Diffie-Hellman Group * ▼ Group 14

Association Life Time (seconds) 3600

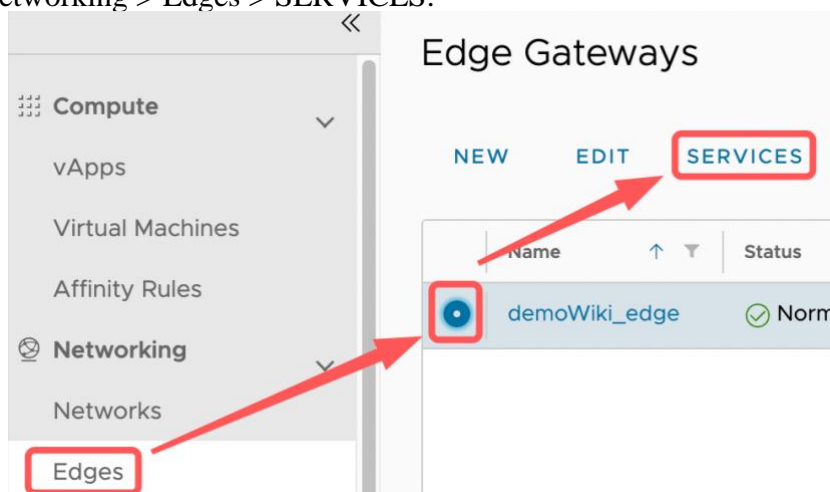
DPD Configuration

Probe Interval (seconds) 60

DISCARD
SAVE

Network: Edge Gateway (older version, nsxv)

1. Go to Networking > Edges > SERVICES.



2. Firewall – for creating firewall rules (if you turn off firewall NAT rules will stop working).

Edge Gateway - demoWiki_edge

Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Certificates Grouping Objects Statistics Edge Settings

Firewall Rules

Enabled

+ × ↑ ↓

Show only user-defined rules

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	firewall	Internal High use		Any	Any	Accept	<input type="checkbox"/>
2	outgoing traffic	User	internal	external	Any	Accept	<input type="checkbox"/>
3	default rule for ingress	Default Policy	Any	Any	Any	Deny	<input type="checkbox"/>

3. NAT – for creating DNAT and SNAT rules.

Edge Gateway - demoWiki_edge

Firewall DHCP NAT Routing Load Balancer

NAT44 Rules

+ DNAT RULE + SNAT RULE [edit] [delete]

Show only user-defined rules

ID	Type	Action	Applied on	Origin

SNAT RULE – Lets you grant internet access for VMs that are using Edge GW.

Original Source IP/Range – internal IP range.

Translated Source IP/Range – external edge GW IP.

Edit SNAT Rule

Applied On: private_vlan_1540_isolated

Original Source IP/Range * 192.168.100.0/24

Protocol Any

Original Port any

ICMP Type

Translated Source IP/Range * 77.241.111.111

SELECT

DISCARD KEEP

DNAT RULE – port forward.

Add DNAT Rule ✕

Applied On: private_vlan_1540_isolated ▾

Original IP/Range * 77.24 ■ ■ ■ [icon]

SELECT

Protocol TCP ▾

Original Port 22 ▾

ICMP Type ▾

Translated IP/Range * 192.168.100.10

DISCARD
KEEP

Original IP/Range – external edge GW IP.

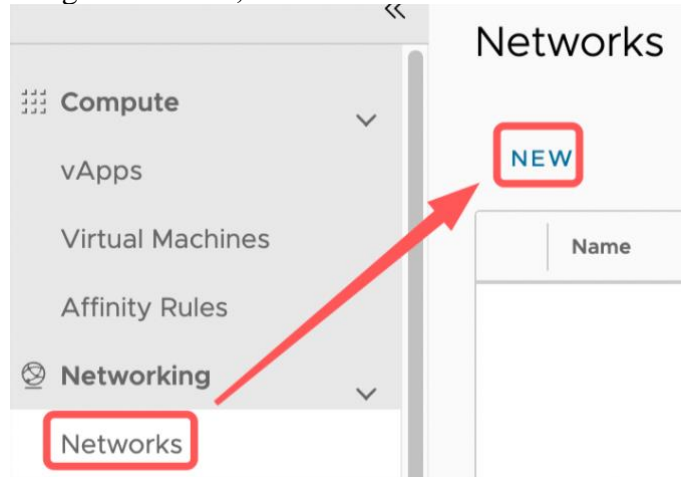
Translated IP/Range – internal IP range.

Source IP Address – client IP that will be trying to reach port, can also be left as “Any”.

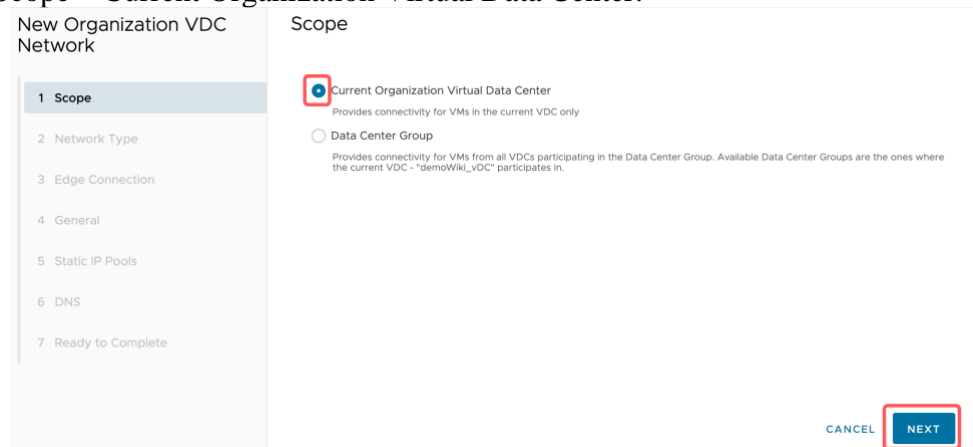
„Protocol“, “Original Port“ and „Translated port“ – port type and port number.

Network: creating Edge Gateway vxlan

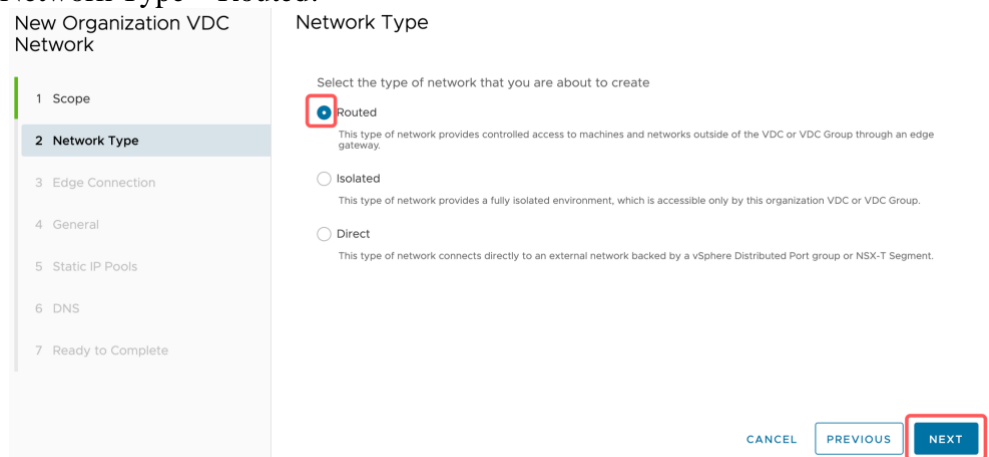
1. Go to Networking – Networks, click “New”:



2. Scope – Current Organization Virtual Data Center:



3. Network Type – Routed:



4. Edge Connection – select your Edge

New Organization VDC Network

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

Edge Connection

Name	External Networks	Org VDC Networks
demoWiki_edge	1	0

1 - 1 of 1 Edge Gateway(s)

Interface Type: Internal Guest VLAN Allowed:

CANCEL PREVIOUS **NEXT**

5. On General tab, input vxlan name and Gateway CIDR:

New Organization VDC Network

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

General

Name *

Description

Dual-Stack Mode

Gateway CIDR *

Shared

CANCEL PREVIOUS **NEXT**

6. On Static IP Pools input your static IP range and click „Add“

7. On DNS, deselect “Use Edge DNS and input your DNS. You can use Baltmeta DNS:
195.14.170.14
195.14.176.14

8. Click “Finish”:

New Organization VDC Network

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

Ready to Complete

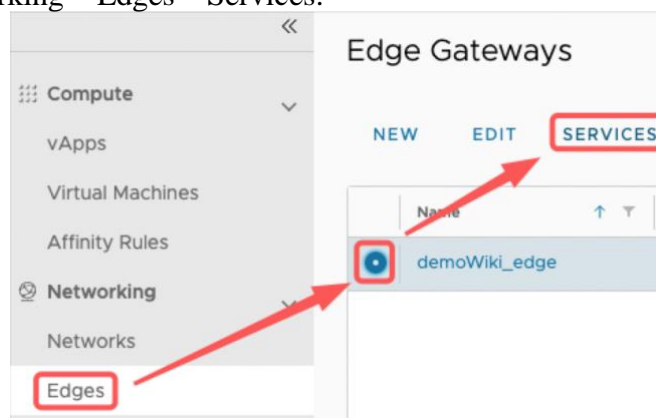
You are about to create an Org VDC Network with these specifications. Review the settings and click Finish.

Scope	demoWiki_vdc
Name	demowiki-vxlan
Description	-
Shared	No
Dual-Stack Mode	No
Gateway CIDR	192.168.100.254/24
Network Type	Routed ⓘ
Connection	demoWiki_edge
Connection Type	Internal
Guest VLAN Allowed	No
Primary DNS	195.14.170.14
Secondary DNS	195.14.176.14

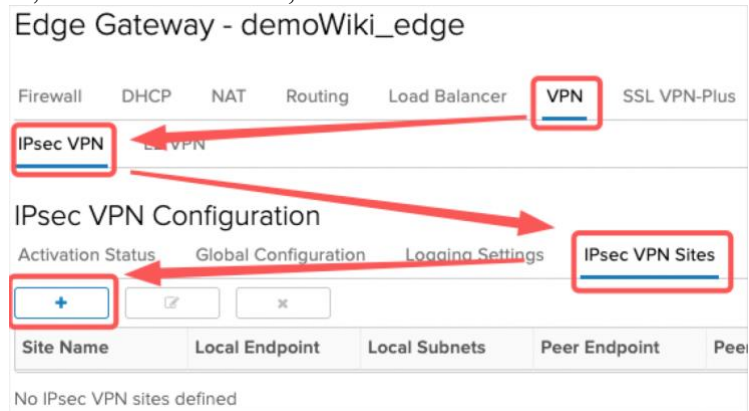
CANCEL PREVIOUS FINISH

Network: IpSec configuration example (older version, nsxv)

1. Go to Networking – Edges – Services.



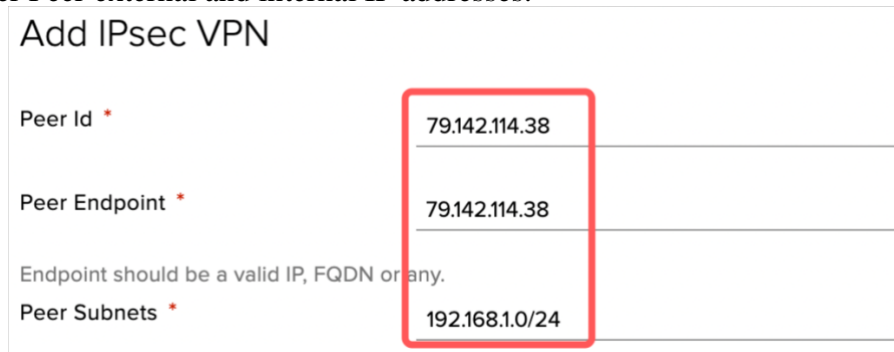
2. On VPN tab, “IPsec VPN Sites”, click “+”:



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.

Add IPsec VPN ✕

Encryption Algorithm AES256 ▾

Authentication PSK ▾

Change Shared Key

Pre-Shared Key * 🔒

Display Shared Key

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.

Diffie-Hellman Group DH14 ▾

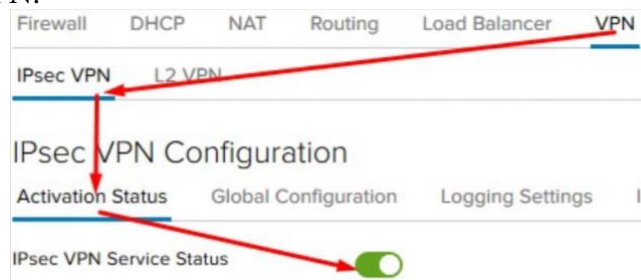
Digest Algorithm SHA1 ▾

IKE Option IKEv1 ▾

IKE Responder Only

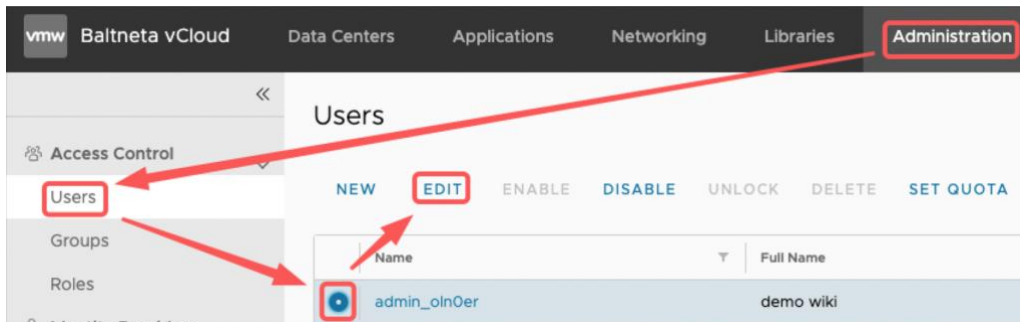
DISCARD
KEEP

6. Enable the VPN.



Change user password

1. Go to Administration – Access Control – Users, select user and click “Edit”:



2. Input new password and click save:

Edit User

Credentials

User name

Password

Confirm password

Enable

Role

Available roles *

Select a role

Contact Info

Full name

Email address