O2 Cloud - Virtuální datové centrum
Tenant portál

Uživatelský manuál verze 13 (říjen 2025)

O2 Czech Republic, a. s.

About VMware Cloud Director

VMware products may be covered by one or more patents listed at:
http://www.vmware.com/go/patents

View the End User License Agreement

OK

Obsah

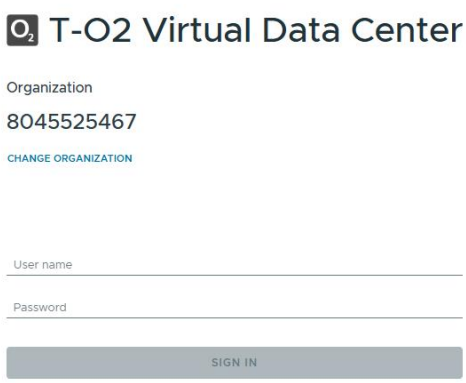
1 Rejstřík pojmů

Pojem	Vysvětlení
Portál O2 Cloud – Tenant Portál	**Portálová aplikace pro ovládání prostředí služby O2 Virtuální datové centrum poskytovaná společností O2 Czech Republic. Správa portálu nevyžaduje žádný doplněk, jedná se o HTML 5)**
IaaS	Infrastruktura jako služba (z „Infrastructure as a Service“) — v tomto případě poskytovatel služeb se zavazuje poskytnout infrastrukturu. Typicky se jedná o virtualizaci. Hlavní výhodou tohoto přístupu je to, že se o veškeré problémy s hardwarem stará poskytovatel.
vDC	Virtuální datové centrum. Představuje množství výpočetního výkonu, paměti a diskového prostoru, které je alokované jednomu zákazníkovi v rámci služby O2 Cloud.
vAPP	Virtuální prostředí (obálka) slučující v sobě několik aplikačních serverů dle jejich určení, účelu a pravidel komunikace.
VM	Virtuální server
Catalog	Katalog pro správu šablon, instalačních médií
Organizace	Soubor prostředků, které má zákazník k dispozici.
vCentrum	Správcovské prostředí pro virtualizační řešení od VMware.
O2 CCU	Jednotka přepočtu procesorového výkonu dle specifikace SPECint
CPU	Zkratka pro fyzický procesor
RAM	Operační paměť
LAN	Místní síť
IP POOL	Rozsah síťových adres
Statická IP adresa	Statická síťová adresa
DHCP	Dynamické přidělování síťových adres bez zásahu administrátora
FIREWALL	Bezpečnostní prvek sloužící k ochraně sití
ROUTER	Směrovač síťového provozu
NAT	Překlad síťových adres
LDAP	Databáze uživatelských účtů a rolí
AD	Active Directory – Microsoftí verze LDAP
URL	Webová adresa
Template	Šablona
OS	Operační systém – WINDOWS, LINUX apod.
APP	Aplikace – web server, CRM a pod
ISO image	Instalační médium pro OS, APP (je to soubor s instalačními zdroji)
IE, FIREFOX, GOOGLE CHROME	Webové prohlížeče
MB, GB	Jednotky velikosti dat
Snapshot	VMware „snapshot“ je kopie souboru na disku virtuálního stroje (VMDK) v daném okamžiku.

2 Přihlášení do prostředí tenant Portálu O2 Cloud

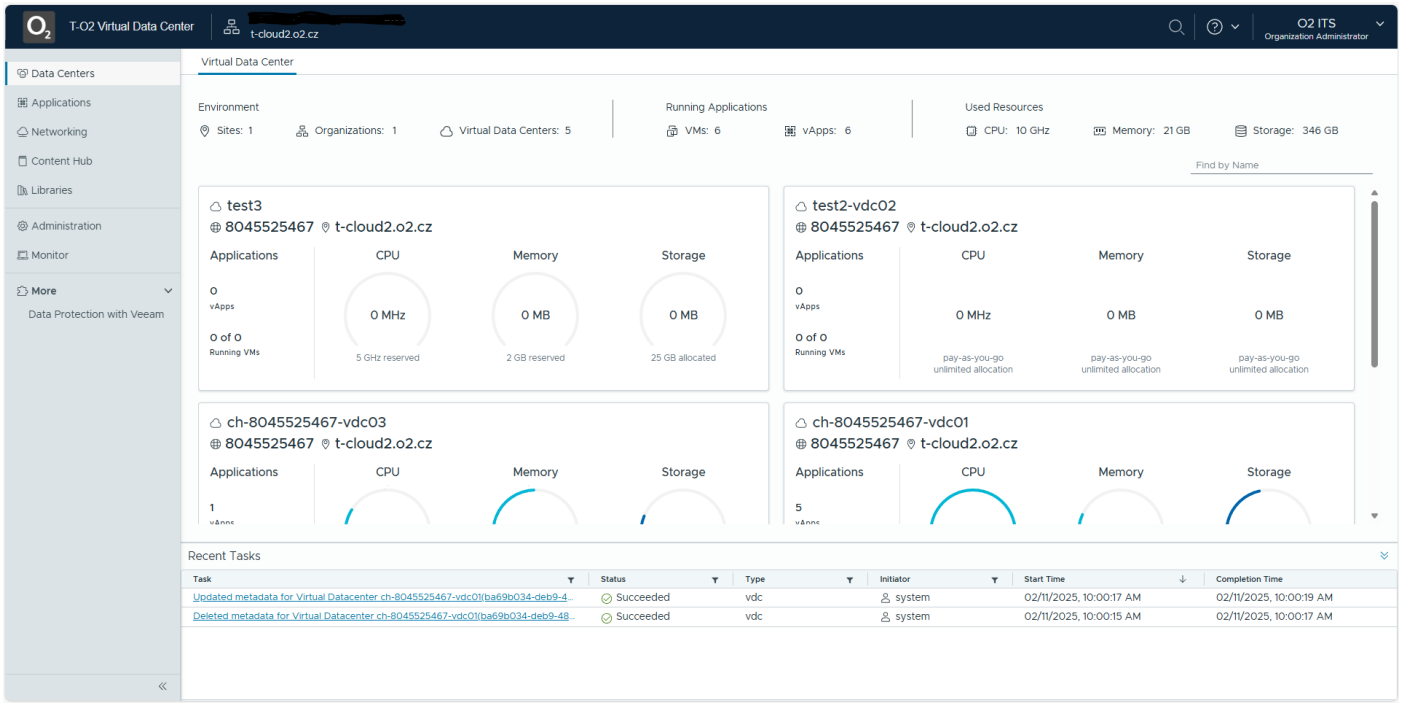
Přihlášení do tenant portálu je na adrese: https://cloud2.o2.cz/tenant/ServiceIDorganizace

Zde zadejte vámi obdržené přihlašovací údaje do organizace.



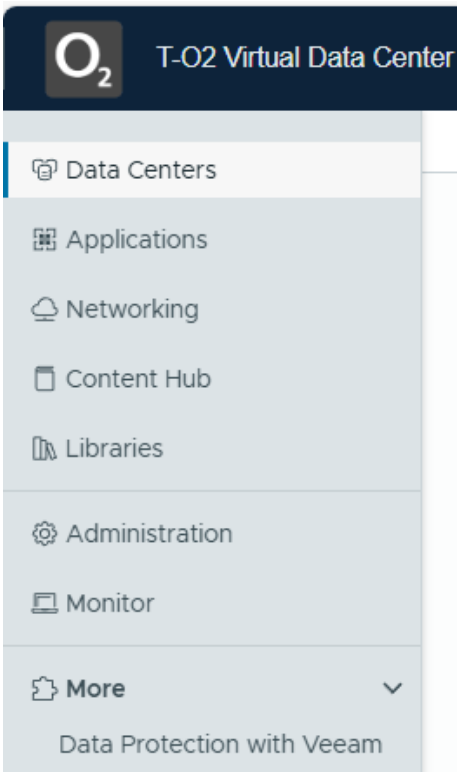
3 Přehled správy

Po přihlášení budete přesměrováni na úvodní stranu, kde je zobrazen přehled vDC (virtuální datové centrum nebo virtuální datová centra ve Vaši organizaci, dále jen vDC) a jejich parametry.



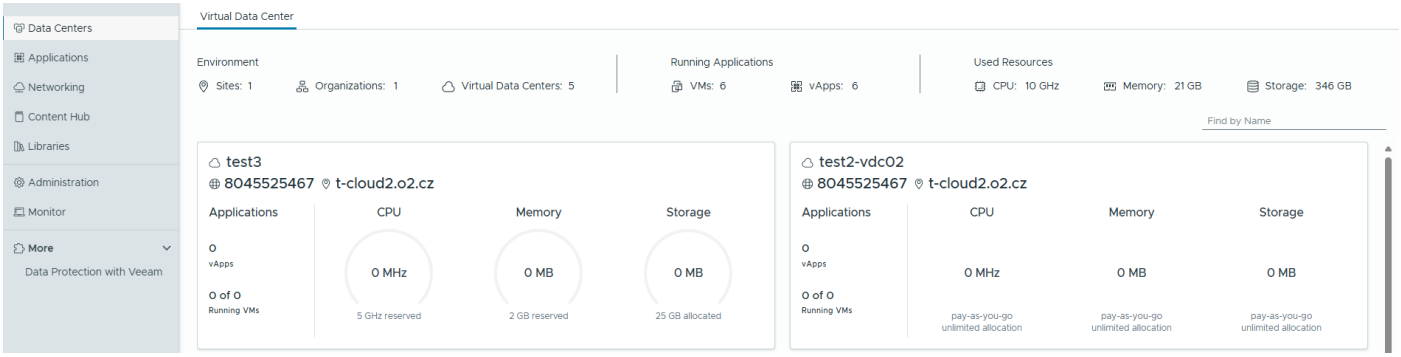
3.1 Správa organizace

Na levé straně se nachází ke správě prostředí následující položky:

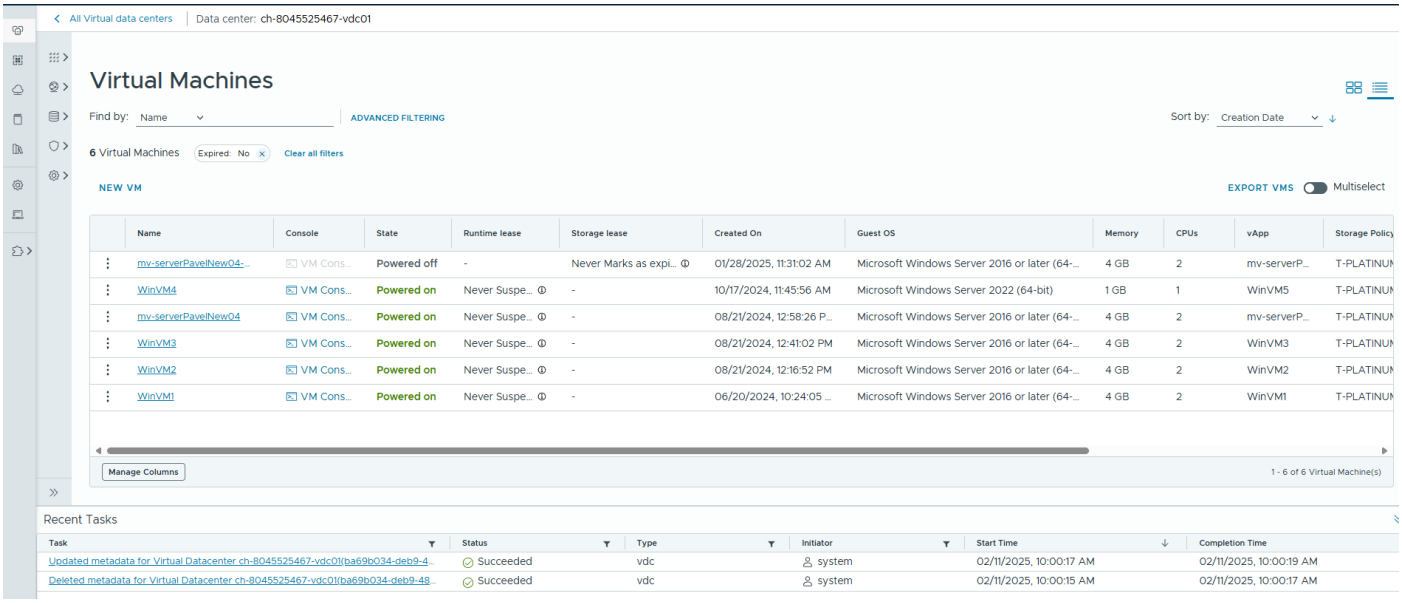


3.1.1 Data Centers (Datacentra)

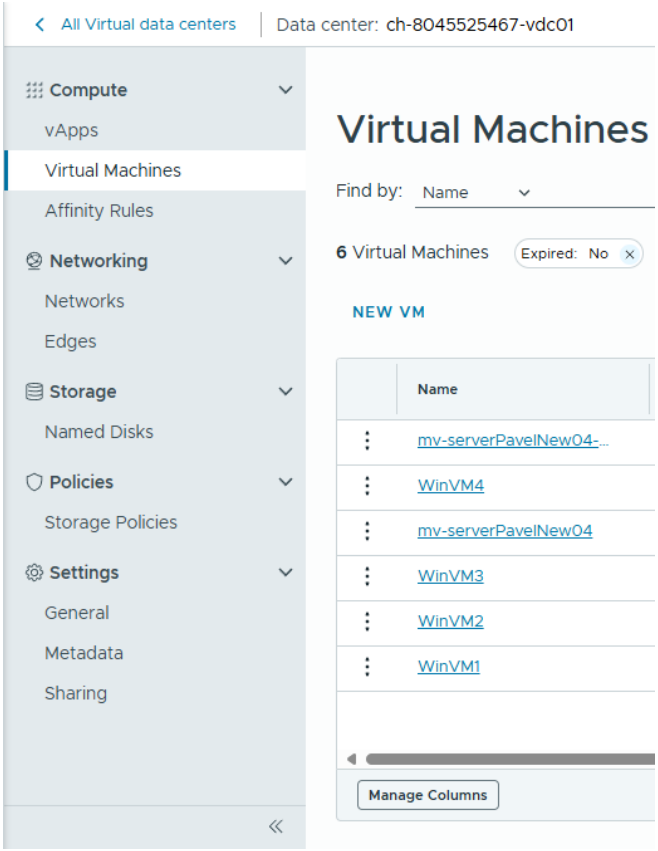
Přehled vDC v organizaci a jejich parametry – po kliknutí na příslušné vDC se proklikneme do vDC, kde je možno provádět správu.



Následně je zobrazen seznam virtuálních serverů



V levém sloupci jsou zobrazeny jednotlivé položky nastavení organizace:



Compute

vApps – přehled vApp ve vDC
Virtual Machines – přehled VM ve vDC
Affinity rules – pravidla

Networking

Networks – přehled sítí ve vDC
Edges – EGW ve vDC

Storage

Named Disks – seznam jmenných disků, které lze připojovat k jednotlivým VMs

Policies

Storage Policies – přehled storage politik přidělených pro vDC
Storage politika daného VM významně ovlivňuje i rychlost zálohování přes síťové rozhraní.

Settings

General – info o vDC
Metadata – metadata vDC
Sharing – informace o režimu sdílení vDC mezi uživateli a skupinami

3.1.2 Applications

Virtual Applications – seznam všech vApp napříč všemi vDC
Virtual Machines – seznam všech VMs napříč všemi vDC

3.1.3 Networking

Networks – seznam všech sítí v organizaci napříč všemi vDC
Edge Gateways – seznam všech EGW (virtuálních routerů) v organizaci napříč všemi vDC
Data Center Groups – seznam DCG v organizaci (DCG zajišťuje sdílení sítí a EGW mezi jednotlivými vDC)

3.1.4 Content Hub

Content

Application images – seznam všech vApp template + ISO images
vApp Templates – seznam všech vApp template, ze kterých lze provést deploy nového VM
Media – seznam všech ISO images (obrazů disku)

Catalogs – seznam všech katalogů

3.1.5 Libraries

Services

Services Library – dlaždicový seznam jednotlivých workflow prostřednictvím kterých si zákazník může zažádat o navýšení zdrojů VDC, aktivaci SPLA licencí, aktivaci IPv6 na novou síť atd.

3.1.6 Administration (administrace)

Users – správa uživatelů a skupin
(V případě potřeby můžete přidat další lokální uživatele do vaší organizace)

- Klikněte na „**NEW**“ (nový uživatel)
- Vyplňte „User name“. Zadejte a potvrďte „Password“
- Přiřaďte uživateli roli ze seznamu rolí (nejčastěji Organization Administrator)
- Vyplňte kontaktní informace pro uživatele
- Klikněte na „**SAVE**“

Groups – správa skupin
Roles – definice rolí

Settings
General – Nastavení URL a popisu organizace
Email – nastavení a popis mailových informací

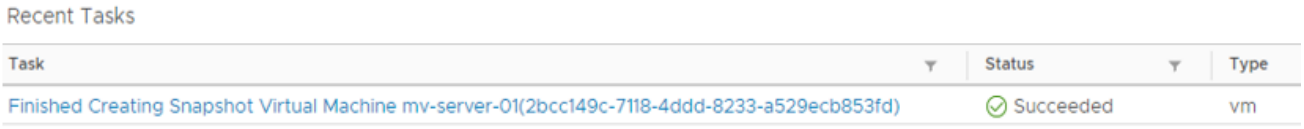
- Po kliknutí na Email můžete provést nastavení SMTP serveru a notifikací.
- O2 Cloud2 vyžaduje SMTP server pro zasílání notifikací a alertů uživatelům. Organizace může použít SMTP server definovaný Administrátorem Portálu O2 Cloudu nebo použít svůj vlastní.
- Klikněte na „Edit“ a na „Use Custom SMTP Server“, kde specifikujete server a uložte tlačítkem „**SAVE**“

Guest Personalizaton – Nastavení domény (AD) a možnosti přiřazení virtuálních serverů do této domény (jedná se o doménu zákazníka)
Metadata – Informace o zákazníkovi (IČO, telefonní kontakt, mailový kontakt aj.)
Policies – nastavení „omezení“ pro virtuální organizaci

3.1.7 Monitor

přehled úloh a událostí

Úplně dole jsou uvedeny Recent Tasks (poslední úlohy).



4 Práce s vlastní organizací

4.1 Správa „prostředků“ (resources) Vaší organizace

Prostředky Vaší organizace včetně vDC přidělené Administrátorem vCloud můžete měnit prostřednictvím vypublikovaných workflow, která naleznete v Libraries -> Services -> Service Library nebo kontaktujte obchodního zástupce O2.

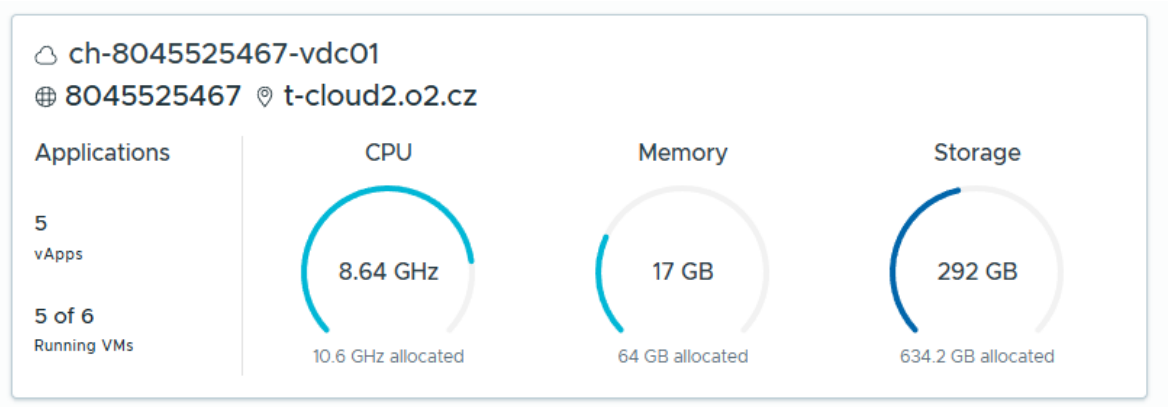
4.2 Správa vDC (virtuálních datacenter)

Virtuální datacentra poskytují procesor(y), paměť, a diskové úložiště, které byly vaší organizaci přidělené administrátorem Portálu O2 Cloudu na základě objednávky. Každá organizace může mít jedno nebo více vDC.

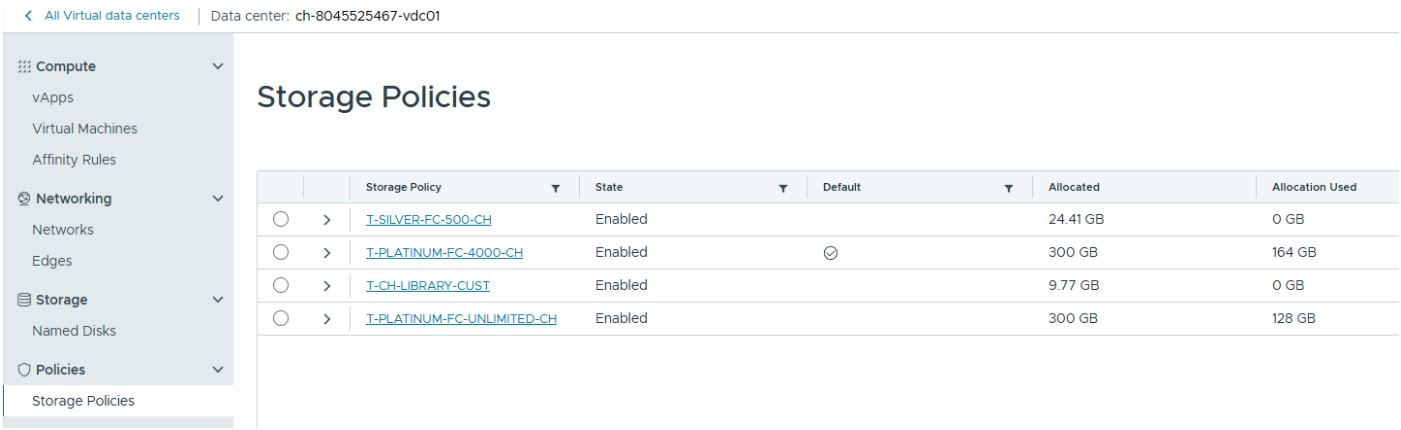
4.2.1 Zobrazení vDC

Zobrazením vDC vaší organizace můžete provádět kontrolu prostředků, které byly nastaveny v rámci organizace.

V přehledu Datacenters naleznete jednotlivá vDC. Zobrazí se další informace o vašem virtuálním datacentru. včetně zakoupené = nastavené kapacity vDC a její obsazení.



Poznámka: Chcete-li vidět rozpad Storage na jednotlivé storage tiery, rozklikněte vDC -> Policies -> Storage Policies Zde pak uvidíte jakou kapacitu aktuálně využíváte (Allocation Used) ze zakoupené (Allocated) u každého storage tieru.



CPU allocation used (na dashboard CPU) = statická hodnota. Nemění se s reálnou CPU utilizací jednotlivých VMs. Ukazuje, kolikrát je 0.96 u SQLaaS VDC přiděleno. Je to tedy "minimální garance", nikoliv součet reálného využití vCPU (GHz) všech serverů. Tato hodnota neukazuje, kolik CPU (GHz) je ve vDC opravdu čerpáno. Ukazuje jen statickou informaci, kolikrát je 0.96 přidělena ve vDC. Pokud bude ve vDC jeden server o 9 CPU, tak tato hodnota bude na Dashboardu vždy 9 x 0.96 GHz = 8.64 GHz.

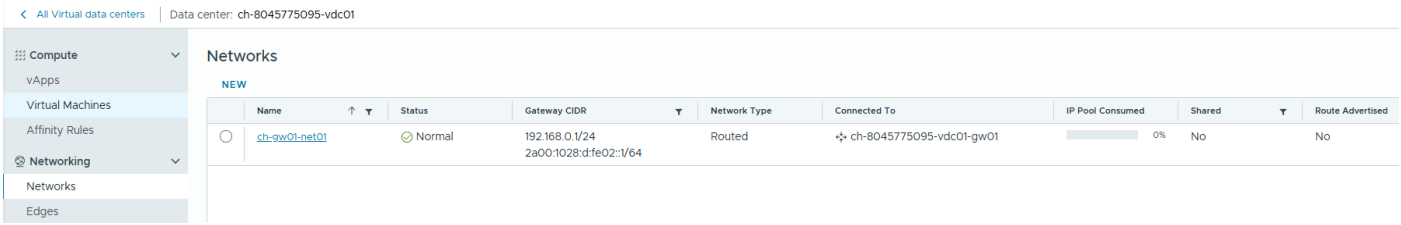
V případě alokačního VDC (nikoliv SQLaaS) platí totéž, akorát konstanta není 0.96, ale 0.78.

Poznámka: U alokačního vDC je maximální frekvence jednoho vCPU 2.66 GHz, u SQLaaS je to 3,6 GHz.

4.2.2 Zobrazení sítí vaší organizace

Pro informaci o sítích, které má vaše organizace k dispozici, klikněte na Networking.
Zobrazí se všechny sítě v celé organizaci, direct sítě i routované sítě připojené do EdgeGW, tj. virtuální router. Více o EdgeGW v kapitole: Kapitola 5, Administrace Edge GW.

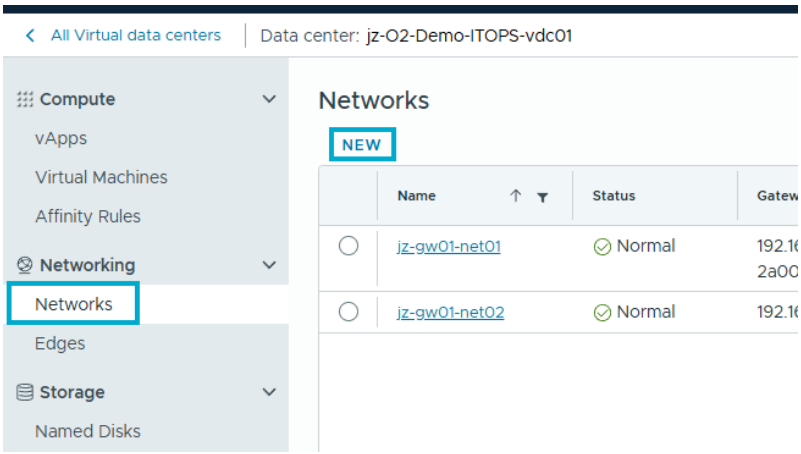
Zobrazení sítí je možné provést i z konkrétního datacentra.
Následně klikněte v levém sloupci v sekci Networking na Networks (sítě) a zobrazí se sítě v daném datacentru.



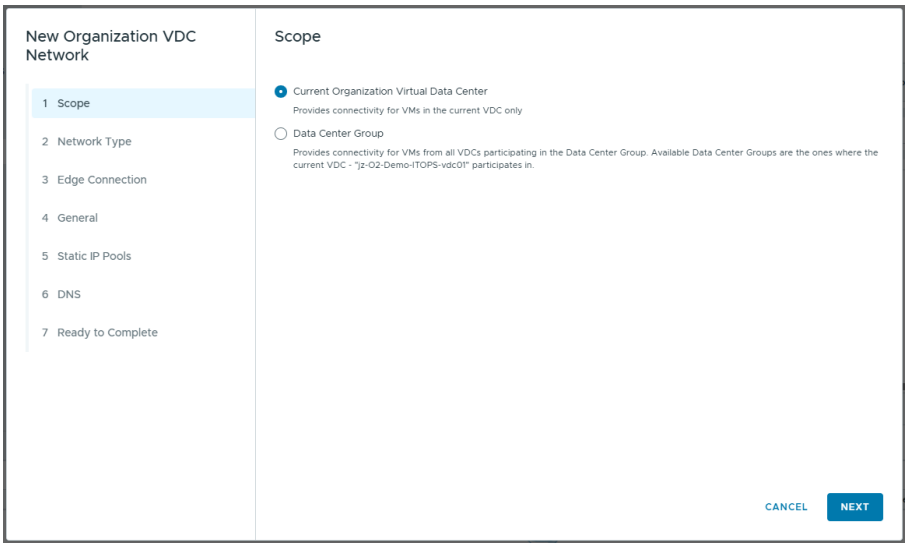
4.2.3 Vytvoření sítě z konkrétního vDC

Pokud již v prostředí máte vytvořenou datacenter group pro sdílení routovaných privátních sítí napříč virtuálními datovými centry na shodné lokalitě, nebudete se řídit postupem níže ale novou routovanou privátní síť si přidáte přímo v datacenter groupě, postup je uveden v kapitole **4.2.6 Sdílení privátních routovaných sítí.**

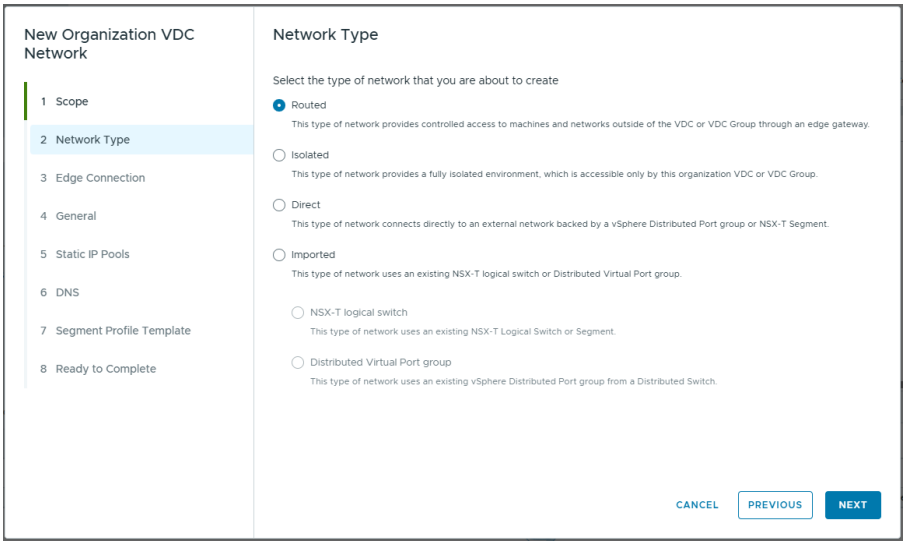
Klikněte na datové centrum, ve kterém požadujete vytvořit novou org síť. V levém sloupci klikněte na Networks a poté na NEW.



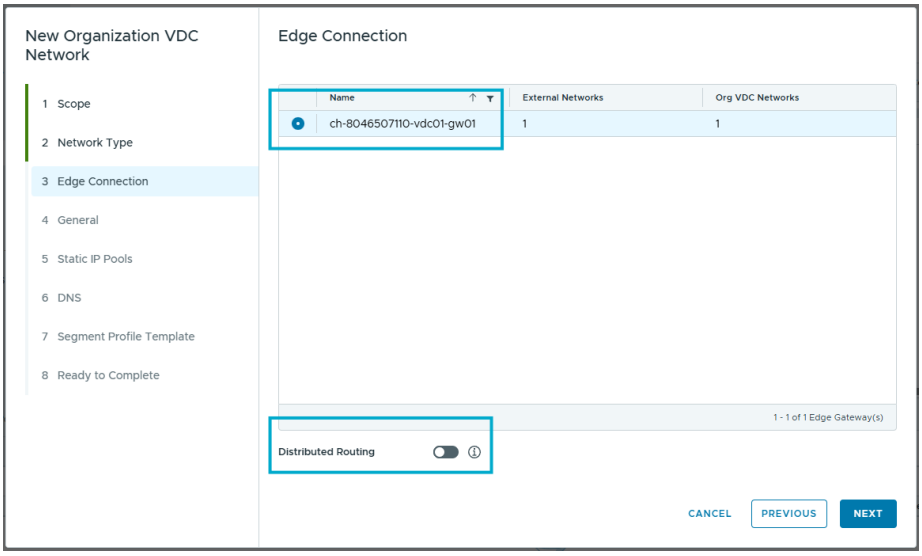
Spustí se původce vytvoření nové org sítě, ve Scope zvolte „Current Organization Virtual Data Center“



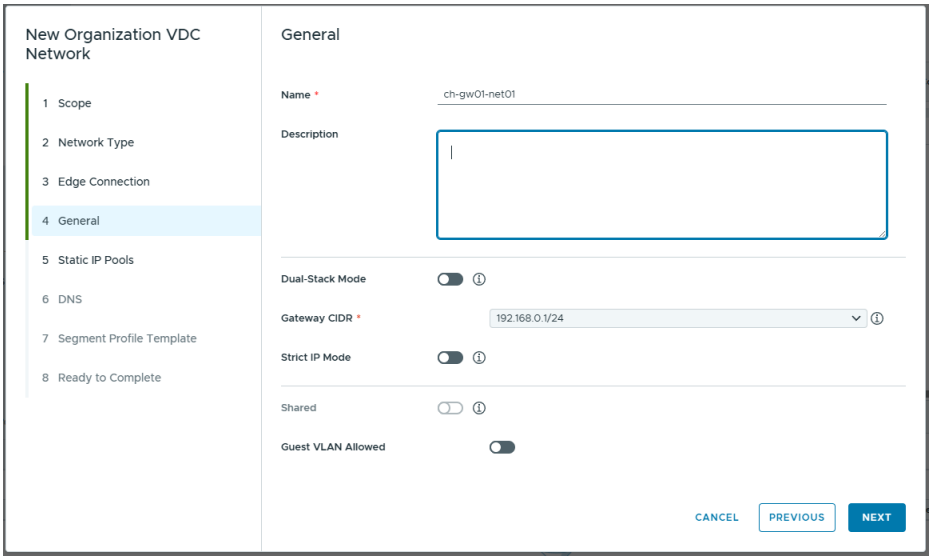
Dále vyberte Routed



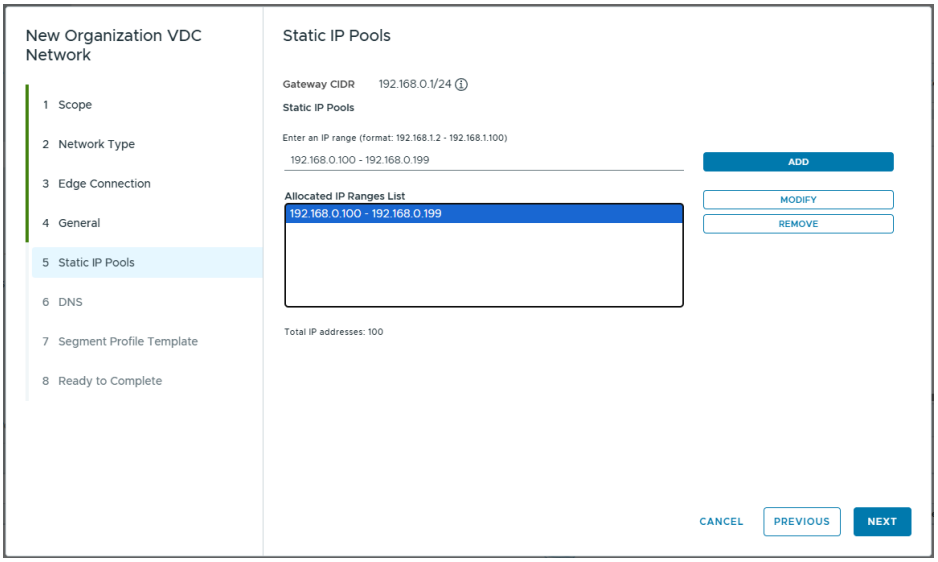
Vyberte Edge Gateway, do které má být nová org síť připojena a níže vypněte distribuovaný routing, který zajistí, že veškerá komunikace bude směrována přes Edge GW včetně firewallu.



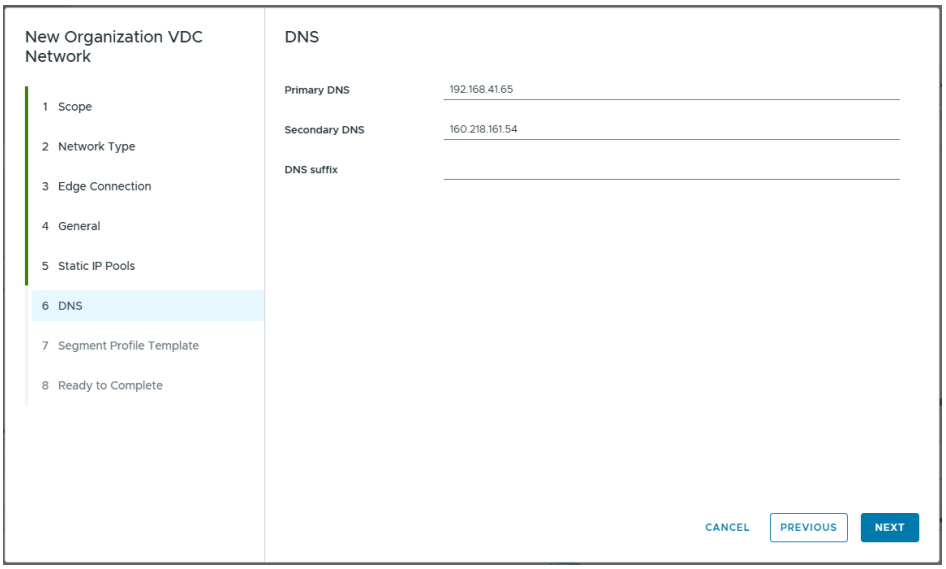
Níže zadejte název sítě a IP adresu Edge GW (příklad 192.168.0.1/24)



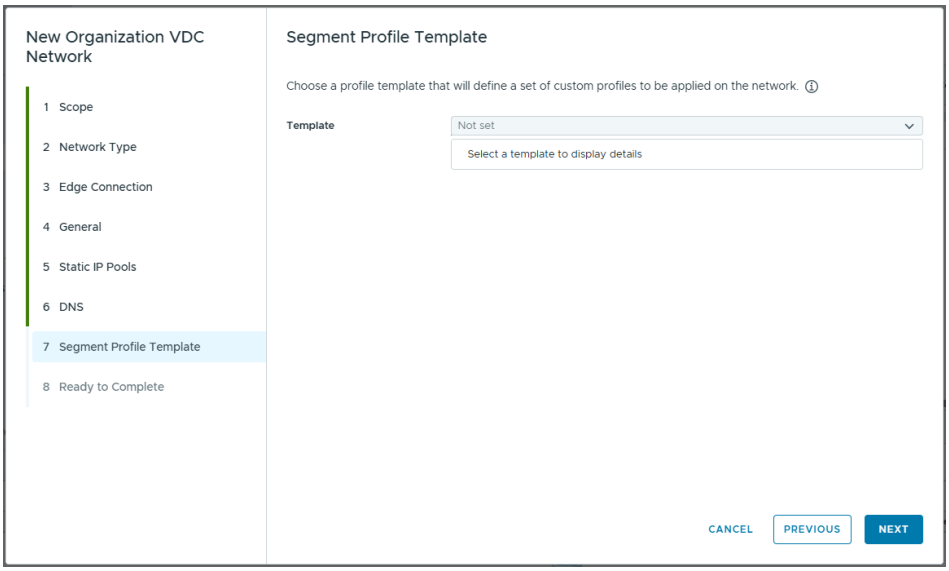
Specifikujte rozsah nové sítě



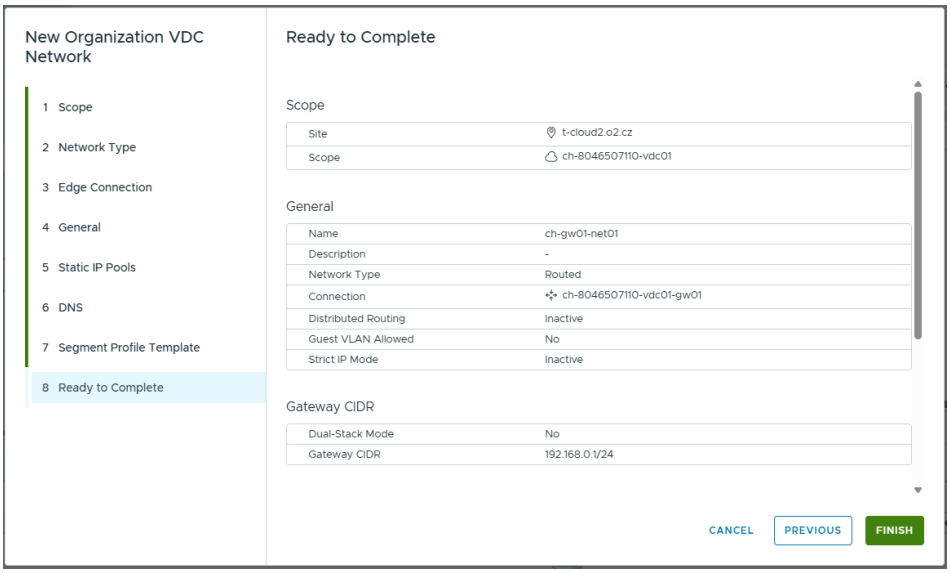
Zadejte DNS servery – 192.168.41.65 a 160.218.161.54 nebo můžete použít vlastní



V této části klikněte na NEXT (není třeba nic nastavovat – ponechte v poli Template hodnotu Not set).



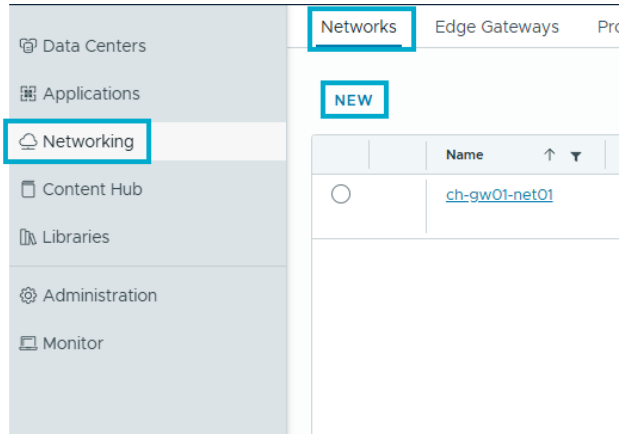
Zobrazí se souhrn vytvářené sítě, pro vytvoření klikněte na FINISH



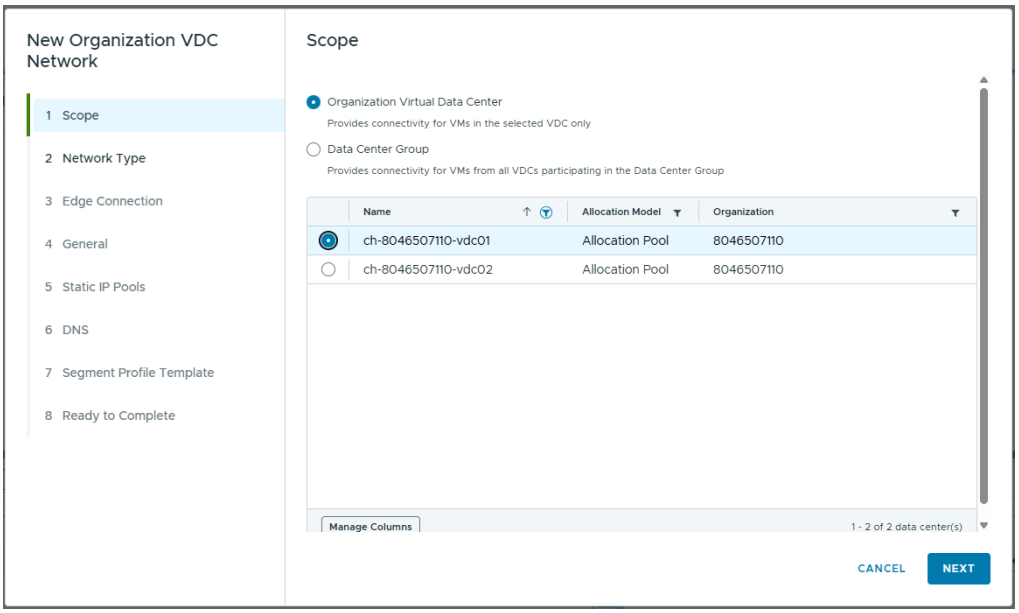
4.2.4 Vytvoření sítě z nabídky Networking

Pokud již v prostředí máte vytvořenou datacenter group pro sdílení routovaných privátních sítí napříč virtuálními datovými centry na shodné lokalitě, nebudete se řídit postupem níže ale novou routovanou privátní síť si přidáte přímo v datacenter groupě, postup je uveden v kapitole **4.2.6 Sdílení privátních routovaných sítí.**

Novou privátní routovanou síť můžete vytvořit ze souhrnného pohledu Tenant portálu.



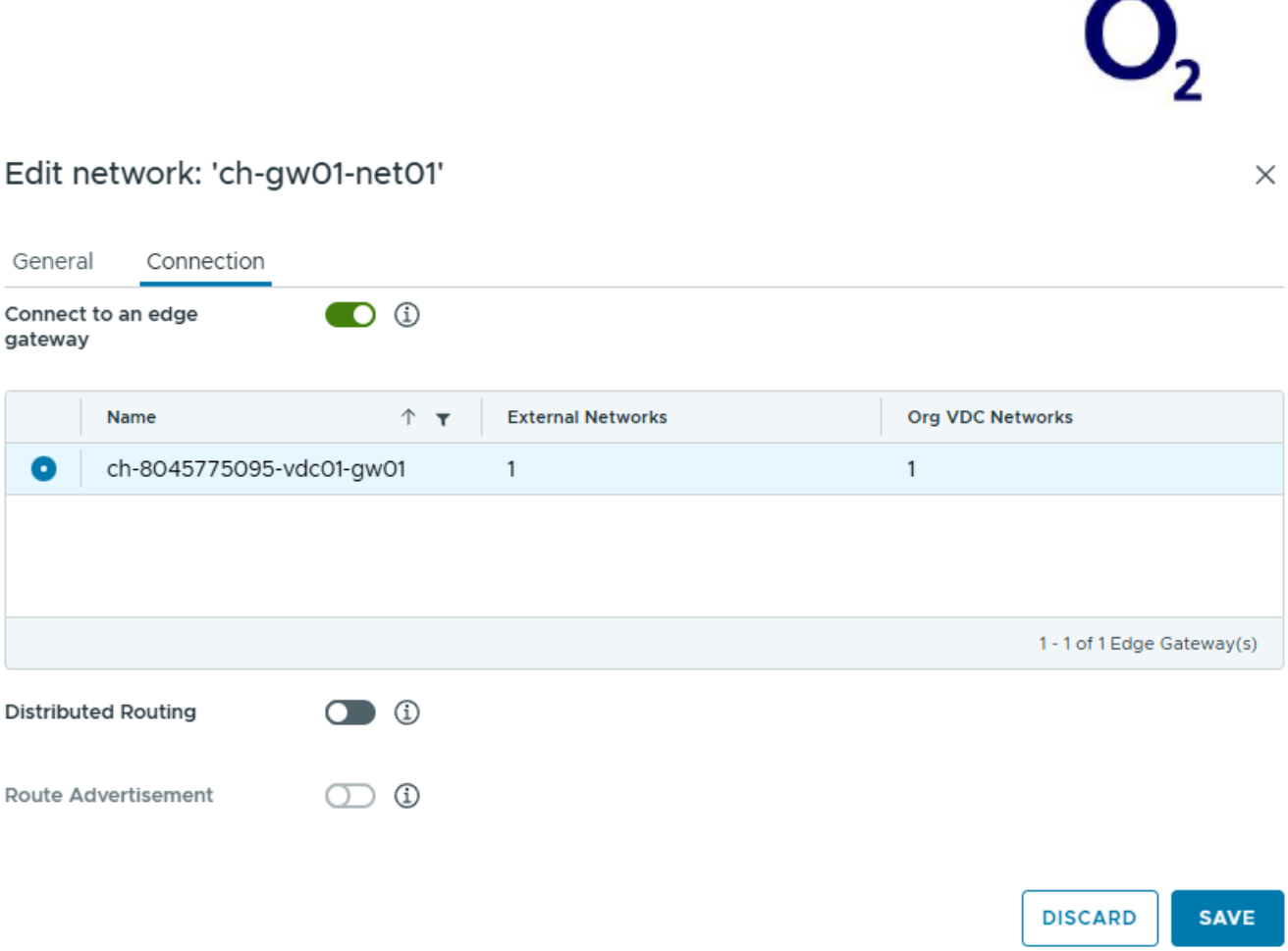
Rozdíl oproti předchozímu postupu je v tom, že v prvním kroku průvodce nové sítě vybíráte virtuální datové centrum (vDC), ve kterém se bude nová privátní routovaná LAN síť využívat.
Po té je již postup na vytvoření nové privátní LAN sítě shodný jako v kapitole předešlé.



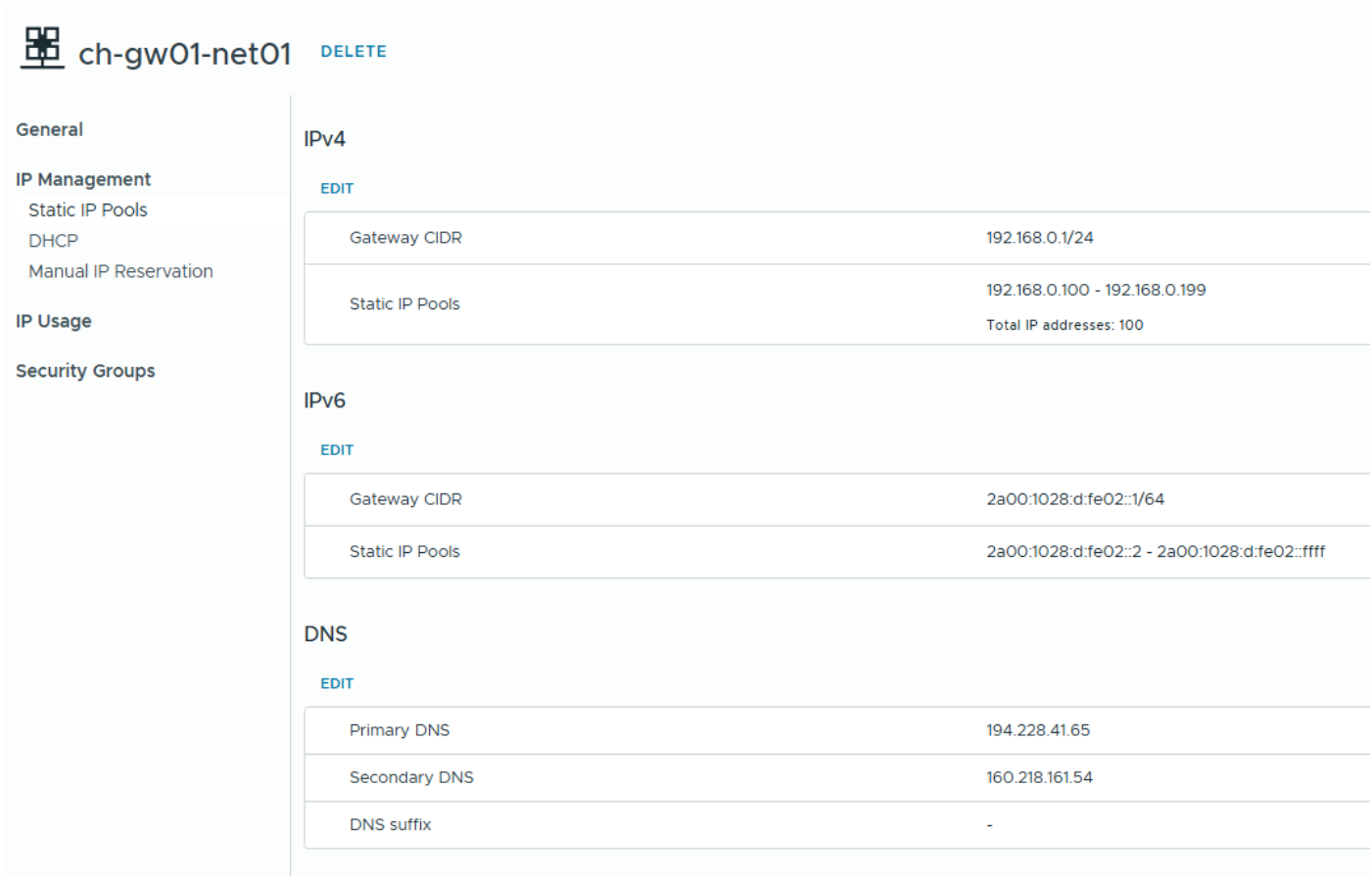
4.2.5 Editace sítě

Po rozkliknutí označení sítě (kliknutím na síť) se níže zobrazí její vlastnosti, které lze možno upravit.

Zde je možno upravit připojení do EdgeGW nebo zapnout funkci Distributed Routing (defaultně je tato funkce vypnutá).



Dále je možno upravovat přidělování IP adres, (jak pro IPv4 tak i pro IPv6), i provést změnu DNS serverů. Doporučujeme ponechat ve výchozím nastavení.



Upozornění:

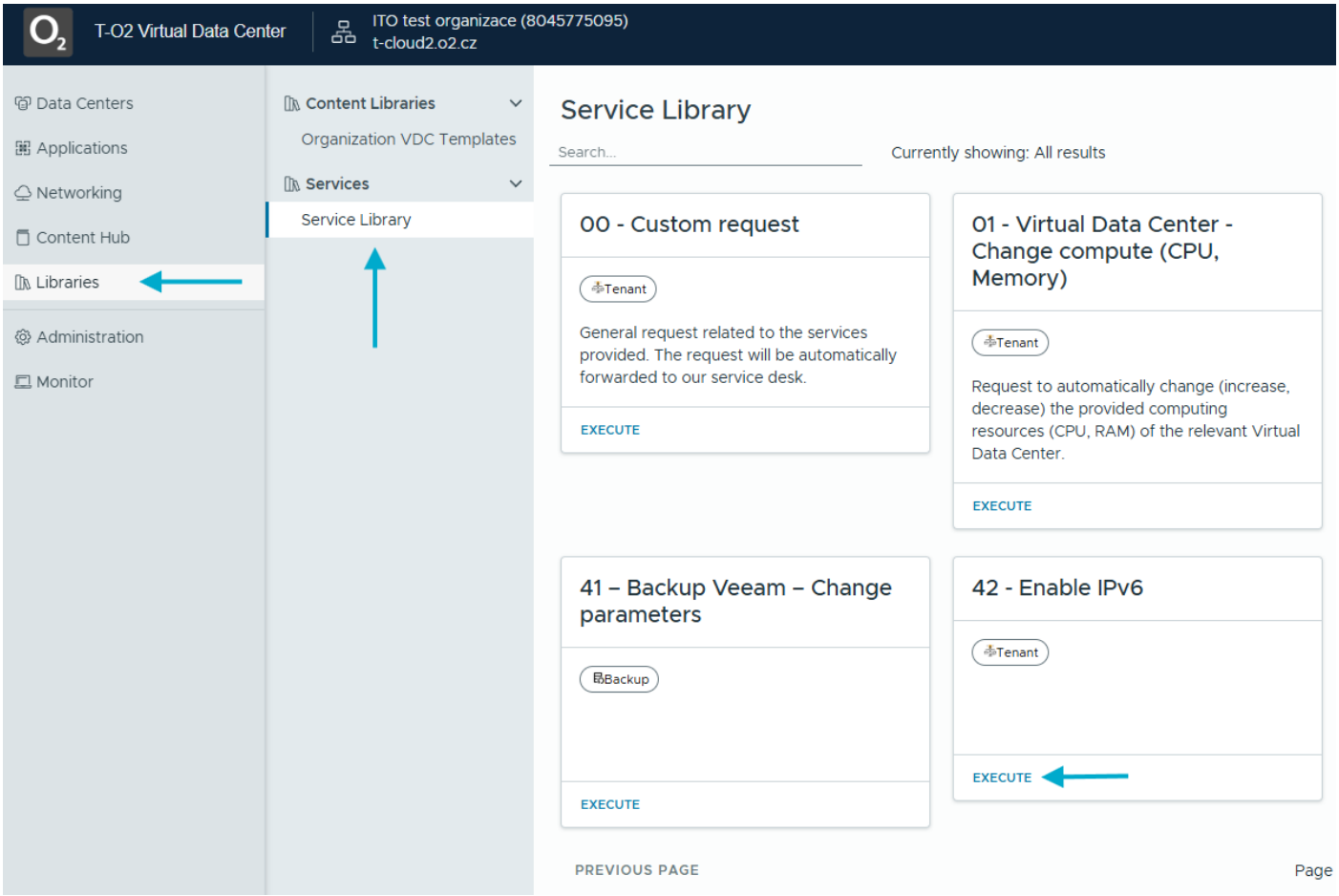
Pokud si vytvoříte novou privátní síť, přidejte si jí v **EdgeGW** do statické groupy **internal_networks** a do statické groupy **o2_backup_internal networks**, více info: Kapitola 5, Administrace Edge GW – virtuální router v organizaci

Direct sítě nejsou připojeny do EdgeGW.

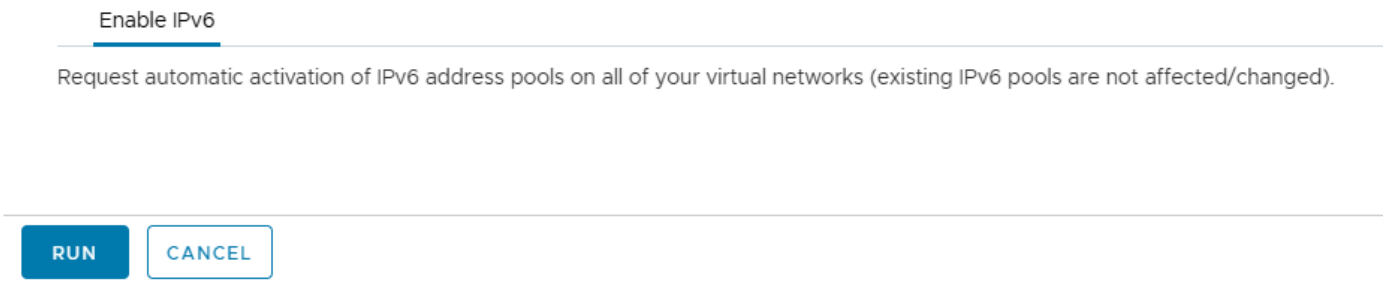
Na síti je možno využívat i IPv6, je-li na síti nastavena – aktivována.

Aktivaci IPv6 je možno provést následujícím způsobem.

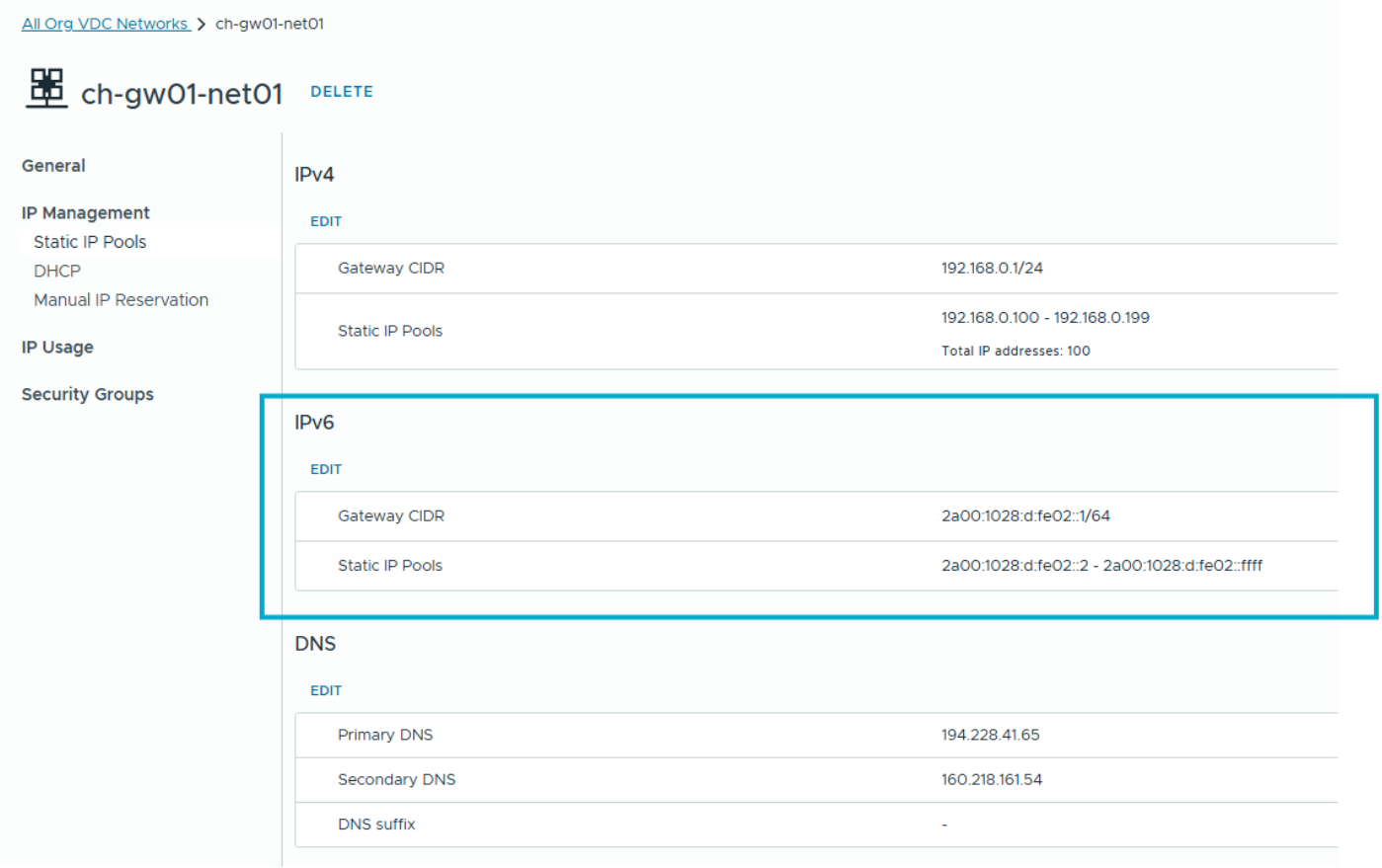
Klikněte na **Libraries**, pak na **Service Library** **a v dlaždici Enable IPv6 na** **EXECUTE**.



Po té potvrďte aktivaci tlačítkem **RUN**



Následně se na org síti zobrazí také IP adresa IPv6, Gateway a Static IP Pools.



Aktivaci IPv6 doporučujeme provést kdykoliv si ručně vytvoříte novou privátní síť. Taková privátní síť je nastavená pouze pro IPv4.

Pokud budete využívat IPv6 IP adresaci, doporučujeme Vám vytvořit nebo upravit IP sety tak, aby v IP Setu, který je následně použit ve FW pravidle (source/destination), byla uvedena jak IPv4 IP adresa tak i IPv6 IP adresa, tudíž jste nemuseli řešit, zda v Destination FW pravidla má být IPv4 IP adresa nebo IPv6. V destination FW pravidla doporučujeme využívat IP sety, které odpovídají názvu virtuálního serveru.

Využíváte-li v prostředí pouze IPv6, tak v IP setu použijte IPv6 IP adresaci.

Všechny IPv6 IP adresy přidělené jsou zároveň veřejné IP adresy (NAT se pro ně nenastavuje).

Níže jsou uvedeny IP adresy DNS serverů

DNS pro IPv4:

Primární: *194.228.41.65*

Sekundární: *160.218.161.54*

DNS pro IPv6:

Primární: *2a00:1028:1:910::1*

Sekundární: *2a00:1028:1:911::1*

4.2.6 Sdílení privátních routovaných sítí

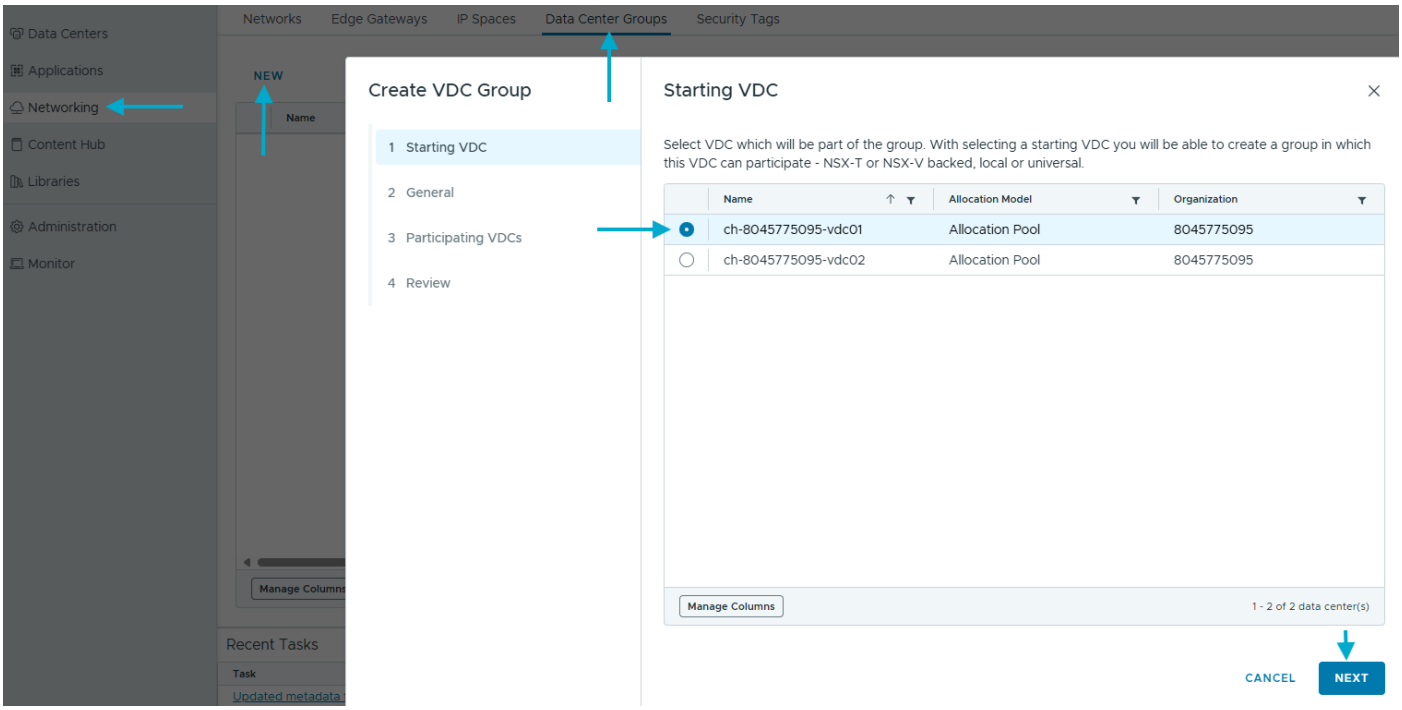
Vytvoření DCG skupiny

V rámci Vaší organizace můžete sdílet jednotlivé routované org sítě (org networks) mezi virtuálními datovými centry v rámci lokality.

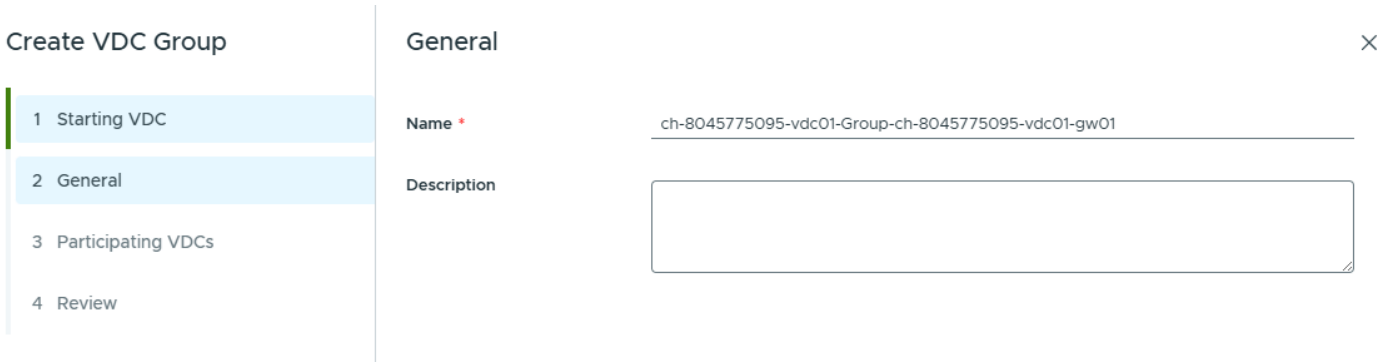
Toto lze nastavit následovně:

Nejprve si vytvořte Data Center Grupu. Provádí se pouze jednou.

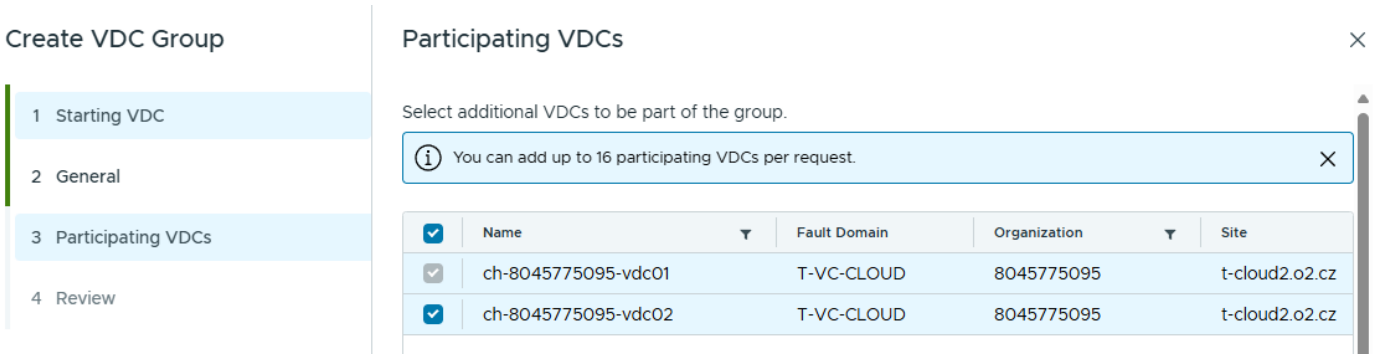
Networking -> Data Center Groups -> NEW -> Vyberete VDC, ve kterém máte umístěnou EdgeGW (většinou vdc01)



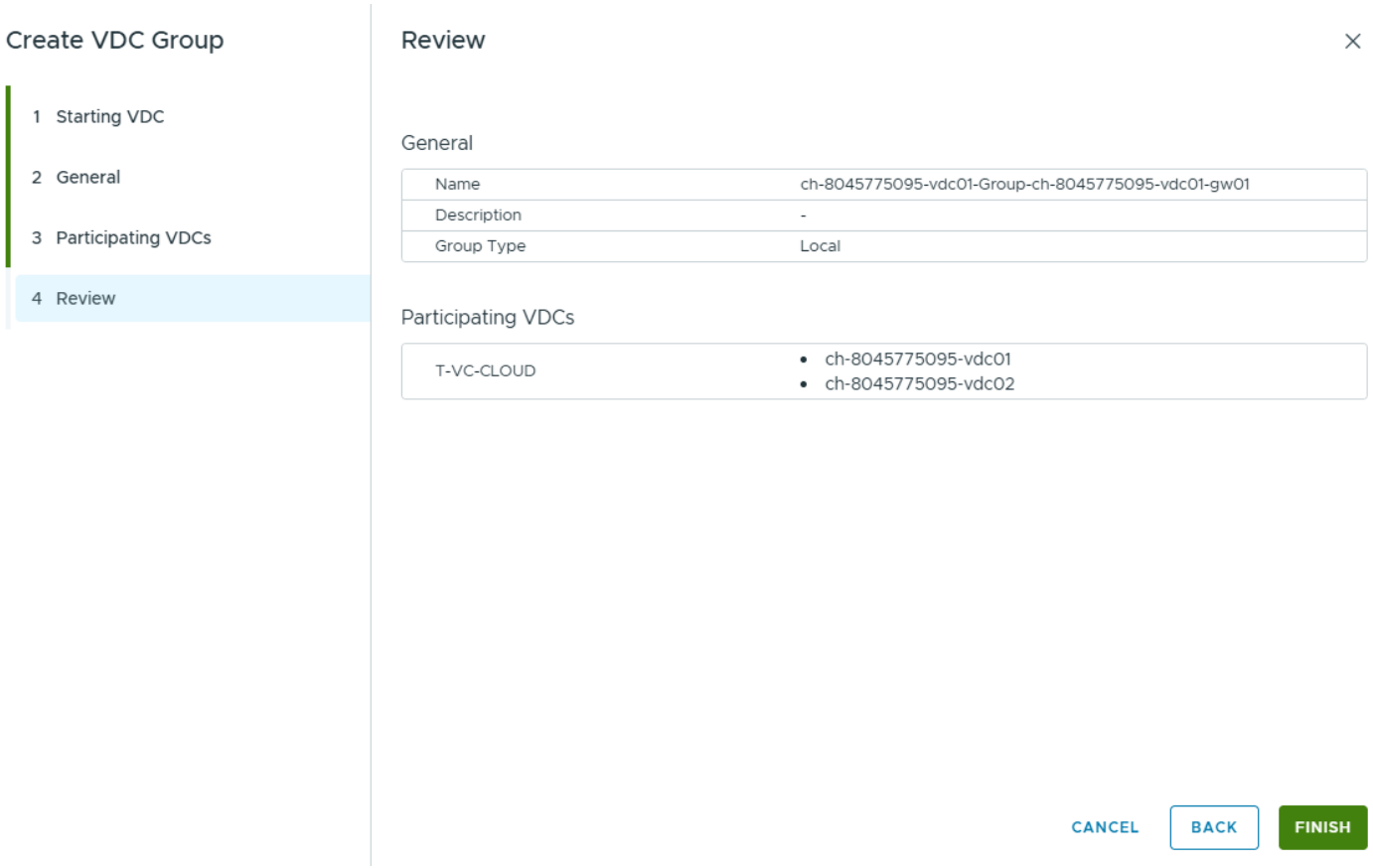
DCG si pojmenujte



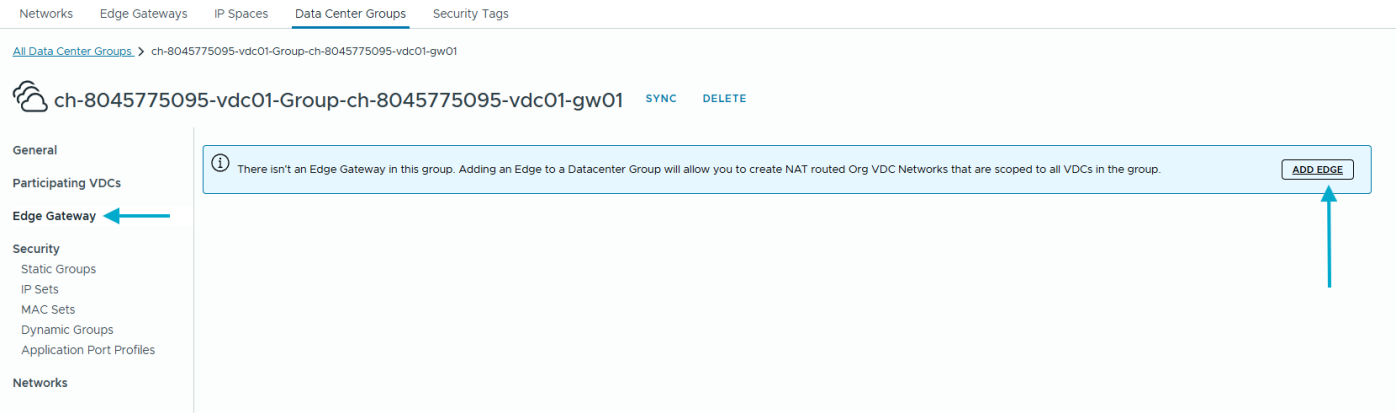
Následně vyberte vDC, které mají být součástí skupiny. Tedy zaškrtněte ty vDC, do kterých se mají nasdílet routované sítě z výchozího vDC01



Potvrďte vytvoření DCG skupiny tlačítkem **Finish**

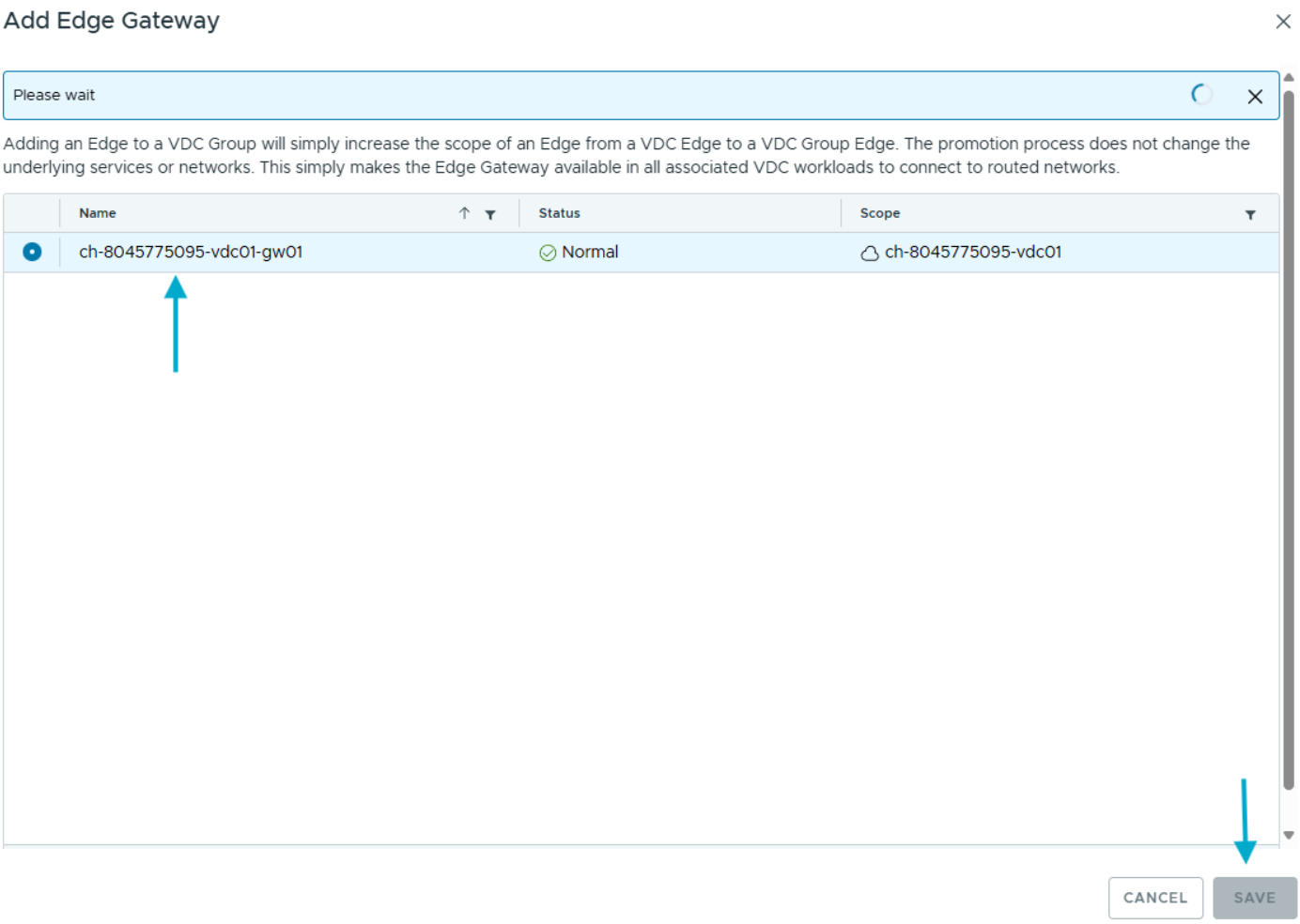


Do nově vytvořené skupiny přidejte Edge, následovně:
(Pokud nastane problém s nedostatečným oprávněním, založte tiket a toto nastaví administrátoři O2 ITS).

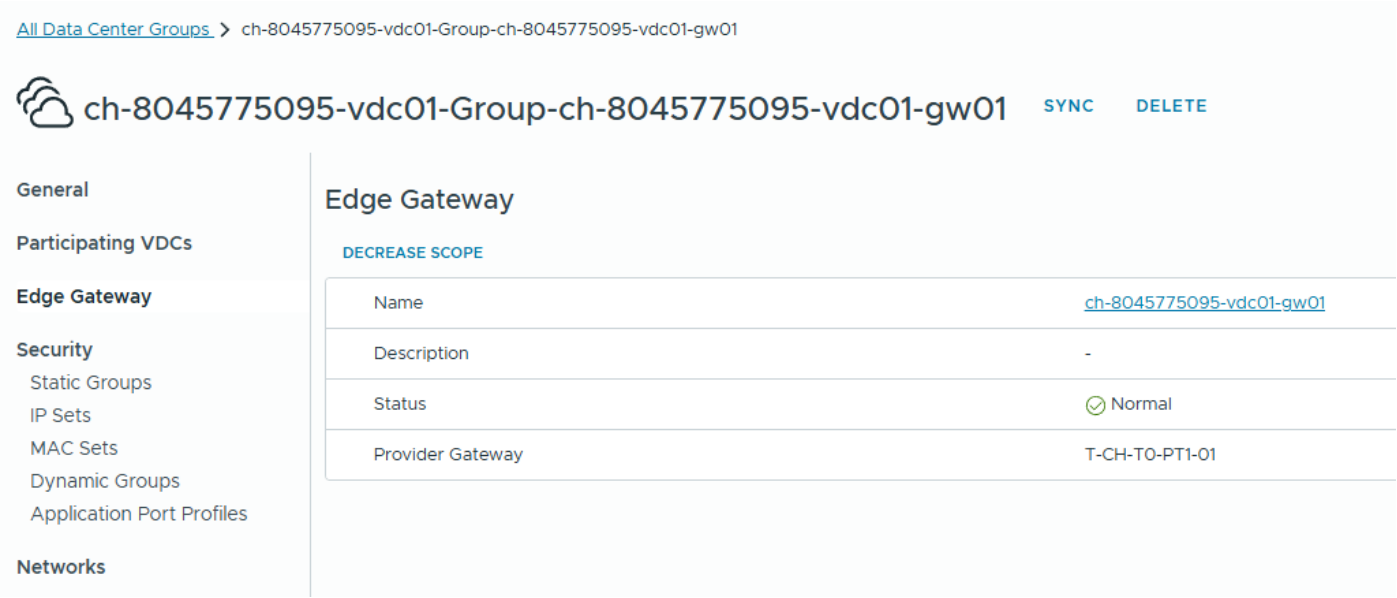


V pravé části klikněte na ADD EDGE

Přidejte EdgeGW do DCG skupiny a potvrďte kliknutím na SAVE (Uložit).



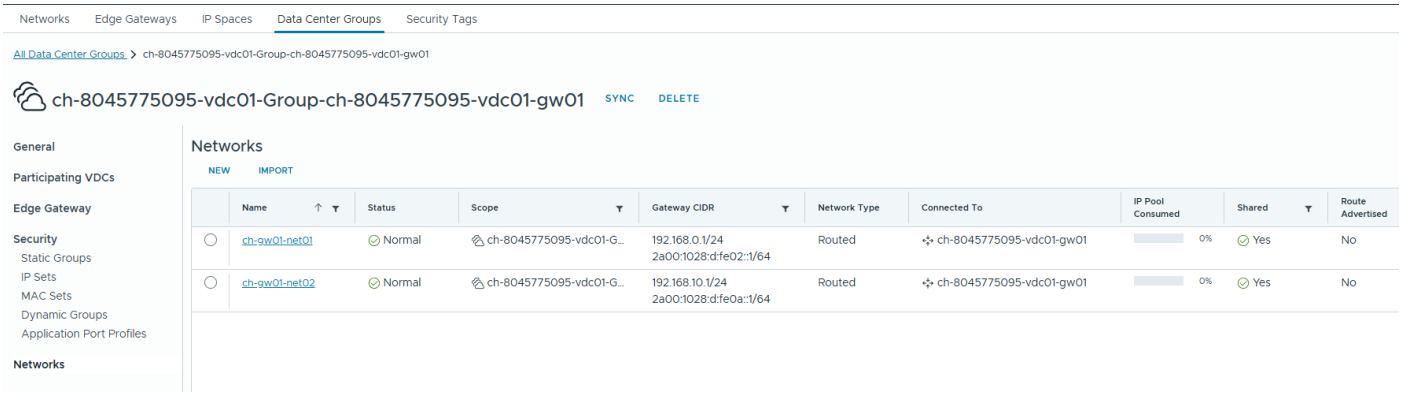
EdgeGW je přidána do DCG skupiny a všechny routované privátní sítě připojené k EdgeGW se tak nasdílí do všech participujících VDC.



Po přidání EdgeGW do skupiny se v Networks zobrazí všechny routované sítě (org networks), které jsou připojené do EdgeGW. (netýká se direct sítí).

Požadujete-li přidat novou privátní routovanou síť, klikněte na Networks a pak na NEW.

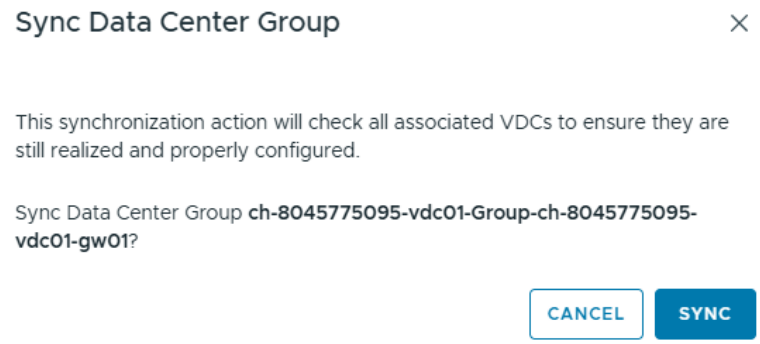
Poznámka: Direct sítě typu PT5 tímto způsobem nelze sdílet – ty se musí připojit ručně ke každému VDC zvlášť.



Tímto je zajištěno, že sítě viditelné v Networks budou dostupné v těch vDC, které jsou nastaveny v sekci Participating VDCs.

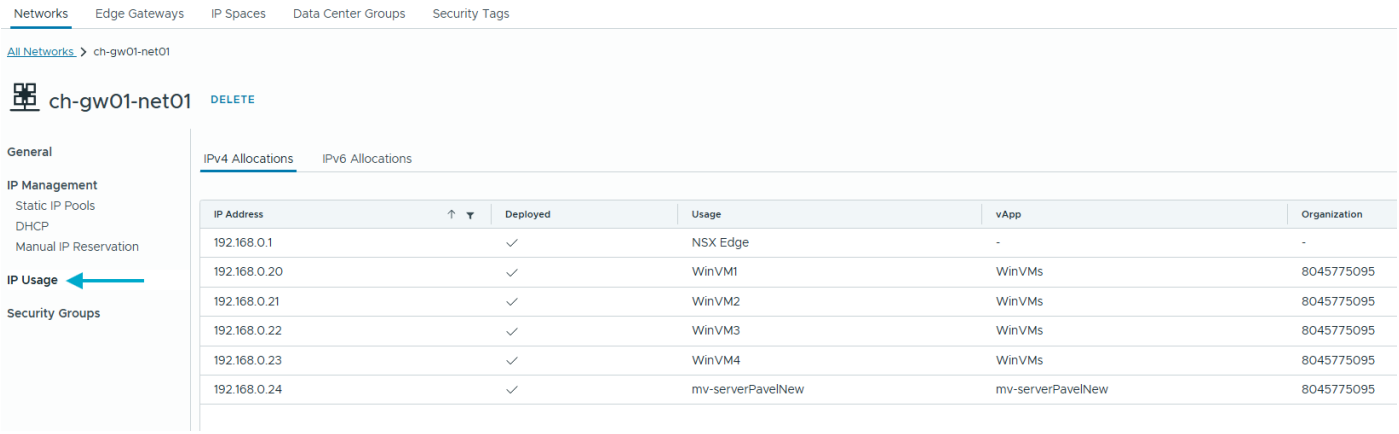
V případě dodatečného vytváření dalších routovaných sítí je nutné do sekce Networks tyto sítě přidat přes NEW proto aby byly viditelné napříč Participating VDCs.

Tlačítkem **Sync** se provede kontrola nasdílených sítí vs VDC.



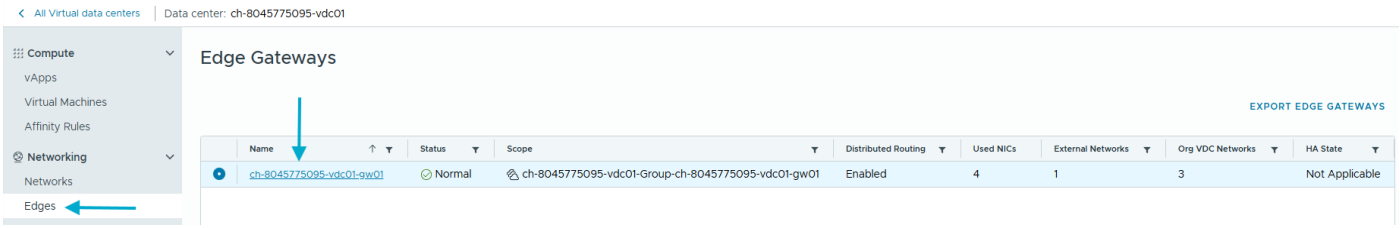
4.2.7 Přehled využití IP adres organizace

Po označení sítě je níže uveden přehled přidělených IP adres z označené sítě.

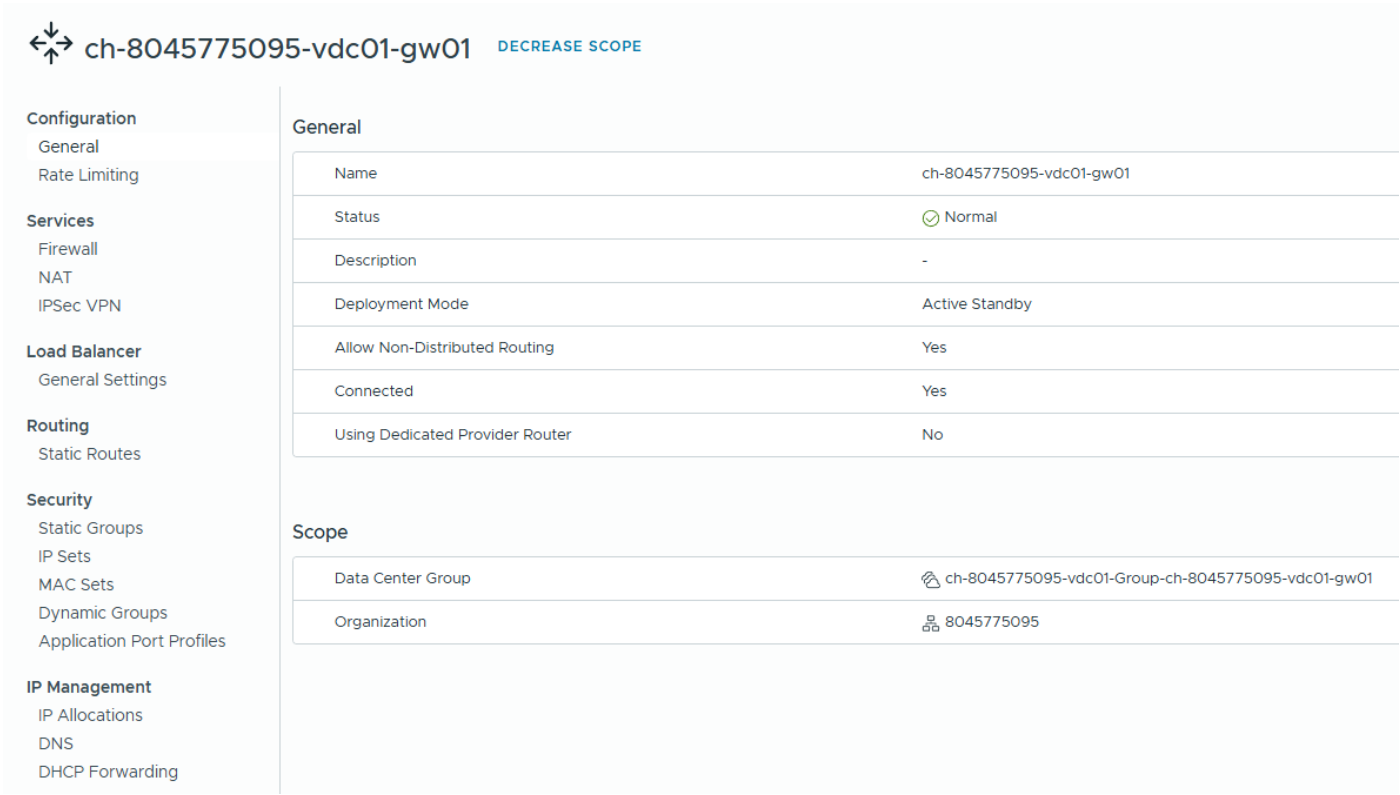


5 Administrace Edge GW – virtuální router v organizaci

5.1.1 Správa EdgeGW – otevření správy virtuálního routeru, dále jen EdgeGW

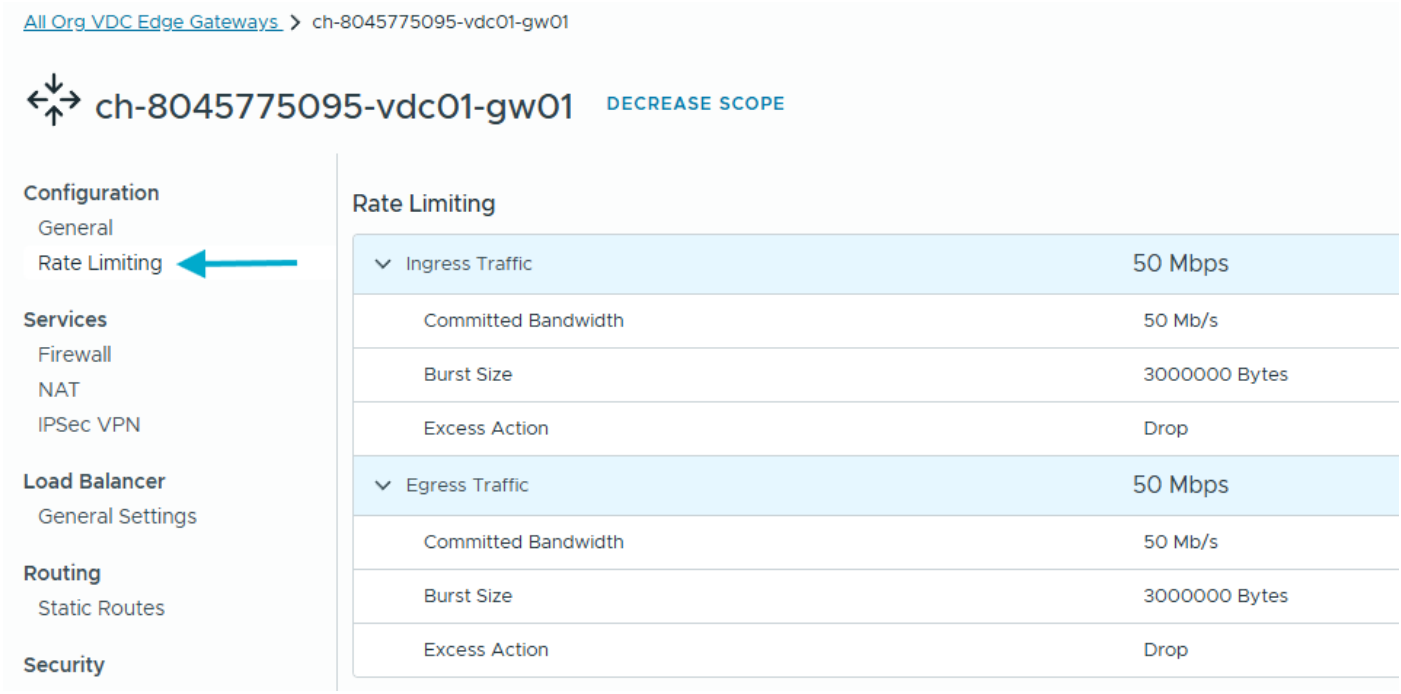


Zobrazí se kompletní správa EdgeGW.



5.1.2 Rate Limiting

Je nastavení, ve kterém je uvedeno, jaká je nastavena propustnost na EdgeGW. Je nastavena tak, jakou máte zakoupenou. ***Tato propustnost ovlivňuje i rychlost zálohování přes síťové rozhraní.***



5.1.3 Konfigurace Firewall

- Klikněte na **Firewall**

Ve výchozím nastavení po zřízení organizace jsou nastavena pravidla:

V pravidlech je podporován jak protocol IPv4 tak IPv6.

V pravidlu NAT neměňte defaultní hodnotu v poli „Applied To“, defaultní hodnota je „-“.

o2_backup – pravidlo nutné pro zálohování/obnova dat přes IPv6. V případě, že používáte snapshotovou zálohu, tak toto pravidlo není využíváno ale doporučujeme ho ponechat pro případ čerpání dalších služeb O2.

icmp - povolení pingu na veřejnou IP adresu EdgeGW

external - pravidlo povolující komunikaci pro jakýkoliv port a protokol do internal networks (internal_networks jsou definovány v IP setech, ve výchozím nastavení je to síť v organizaci, 192.168.0.0/24).

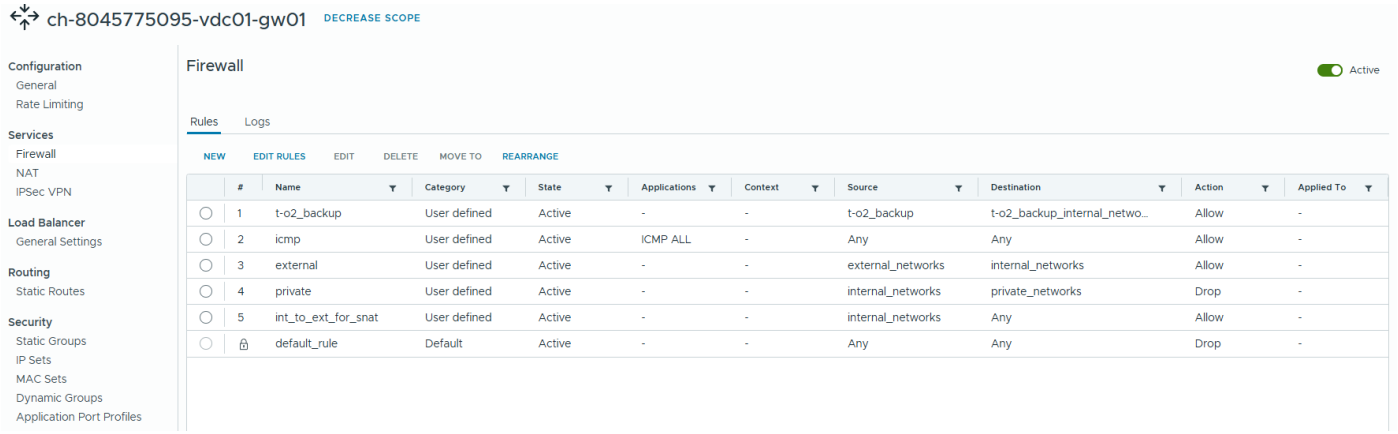
private - pravidlo zakazující komunikaci pro jakýkoliv port a protokol z internal_networks do private networks.
(skupina **internal_networks** je definována ve Static Group, ve výchozím nastavení je to síť v organizaci, 192.168.0.0/24).
(skupina **private_networks** je definována v IP setech, ve výchozím nastavení jsou to privátní rozsahy, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

int_to_ext_for_snat - pravidlo povolující odchozí síťovou komunikaci pro jakýkoliv protokol a port z organizace. například do internetu nebo pro další služby O2, které můžete v budoucnu v případě potřeby čerpat.

default_rule - **defaultní pravidlo zakazující ostatní síťový provoz**.

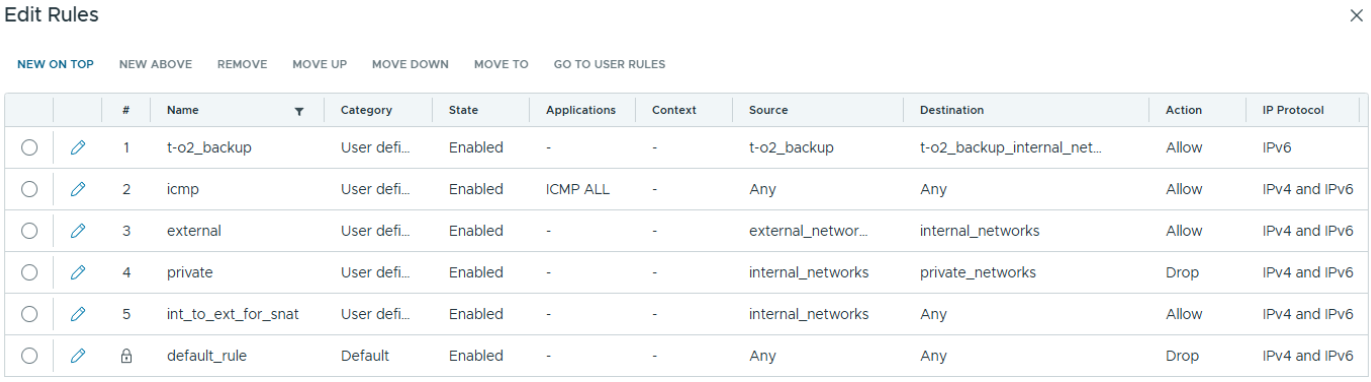
(Ve výchozím nastavení má tedy organizace povolen překlad do internetu, což povoluje v NAT pravidlo int_to_ext_for_snat).

FW PRAVIDLA, přednost pro FW mají vždy pravidla, které jsou nastaveny nejvýše.
Pravidla lze posouvat dolů a nahoru pomocí tlačítek, klikněte na Edit Rules a po té je možno pravidlo posouvat pomocí tlačítek MOVE DOWN A MOVE UP.



Správu pravidel (vytváření, úpravy, mazání nebo změnu pořadí pravidel) lze ve FW provést kliknutím z pohledu **Firewall** a následně na **EDIT RULES**.

FW pravidla



FW v NSX-T podporuje IPv6.

5.1.4 Konfigurace NAT

- Klikněte na **NAT**

Ve výchozím nastavení po zřízení organizace jsou nastavena pravidla:

V pravidlu NAT neměňte defaultní hodnotu v poli „Applied To“, defaultní hodnota je „-“.

no_snat_10 - pravidlo nastavuje, aby se pro cíl v síti 10.0.0.0/8 nepoužíval ze sítí Cloudu překlad.
(pravidlo je předpřipraveno pro případ čerpání dalších služeb O2).

no_snat_172_16 - pravidlo nastavuje, aby se pro cíl v síti 172.16.0.0/12 nepoužíval ze sítí Cloudu překlad.
(pravidlo je předpřipraveno pro případ čerpání dalších služeb O2).

no_snat_192_168 - pravidlo nastavuje, aby se pro cíl v síti 192.168.0.0/16 nepoužíval ze sítí Cloudu překlad.
(pravidlo je předpřipraveno pro případ čerpání dalších služeb O2).

snat_to_external - pravidlo, které nastavuje překlad do internetu, tak že síť v Cloudu bude vystupovat veřejnou IP,
v tomto příkladu pod veřejnou IP 90.183.120.61.

(Ve výchozím nastavení má tedy organizace povolen přístup do internetu, což povoluje ve FW pravidlo int_to_ext_for_snat).

Priority jednotlivých pravidel jsou nastaveny takto:

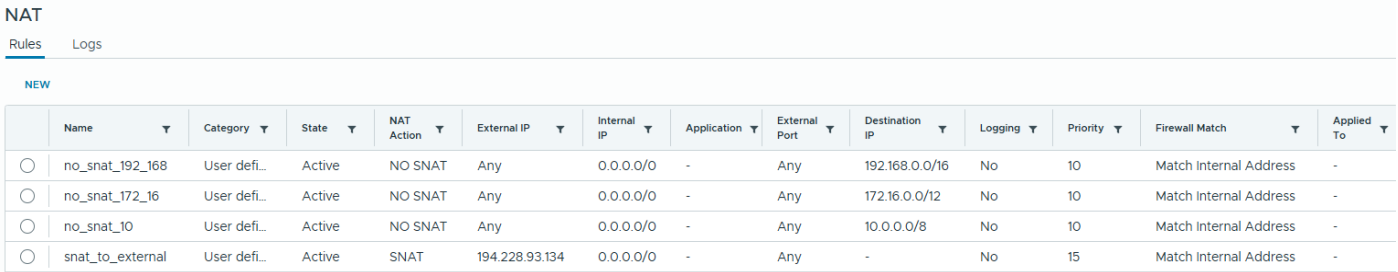
15 pro SNAT

10 pro NO SNAT

Priorita pro DNAT je výchozí hodnota 50. Doporučujeme tuto hodnotu změnit na 0. V případě, že máte dvě a více DNATových pravidel se stejným externím portem, je potřeba tyto pravidla priorizovat (jednomu pravidlu nastavit vyšší prioritu než druhému, aby nedocházelo ke kolizi). 0 je nejvyšší priorita.

Dále u všech pravidel musí být nastaven Firewall Match na Match Internal Adress.

NAT PRAVIDLA, lze nastavovat priority pravidel, čím nižší číslo, tím má pravidlo větší prioritu pro zpracování pravidel.


NAT

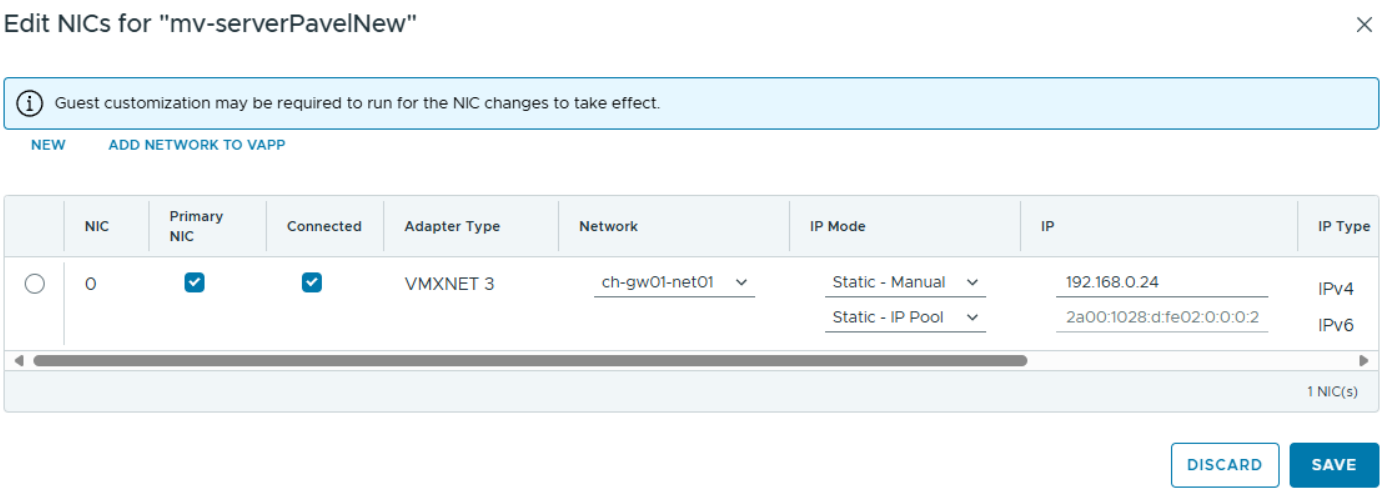
Rules Logs

NEW

	Name	Category	State	NAT Action	External IP	Internal IP	Application	External Port	Destination IP	Logging	Priority	Firewall Match	Applied To
○	no_snat_192_168	User defi...	Active	NO SNAT	Any	0.0.0.0/0	-	Any	192.168.0.0/16	No	10	Match Internal Address	-
○	no_snat_172_16	User defi...	Active	NO SNAT	Any	0.0.0.0/0	-	Any	172.16.0.0/12	No	10	Match Internal Address	-
○	no_snat_10	User defi...	Active	NO SNAT	Any	0.0.0.0/0	-	Any	10.0.0.0/8	No	10	Match Internal Address	-
○	snat_to_external	User defi...	Active	SNAT	194.228.93.134	0.0.0.0/0	-	Any	-	No	15	Match Internal Address	-

Poznámka: NAT pro IPv6 je irelevantní, protože IPv6 adresy jsou všechny veřejné a NAT se pro ně nepoužívá.

U virtuálního serveru je možno v konfiguraci vNIC použít jak **IPv4** tak **IPv6,** viz obrázek



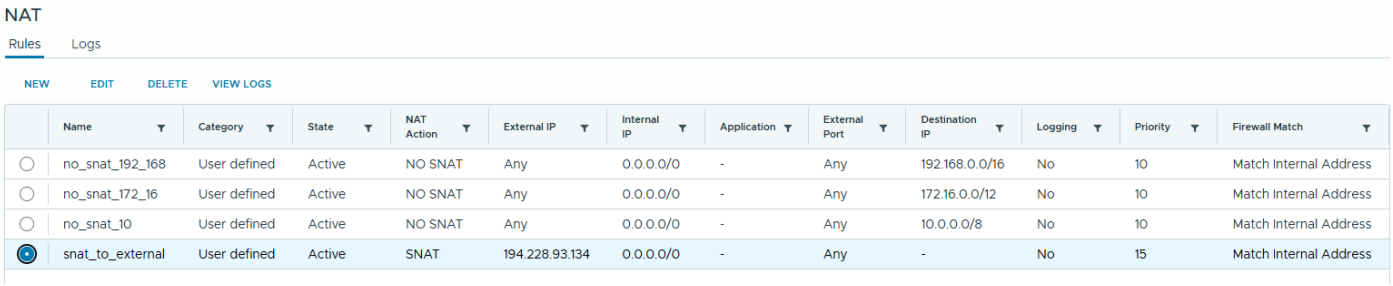
5.1.5 Nastavení prostupu z organizace do internetu

Ve vaši organizaci je ve výchozím nastavení povolen prostup do Internetu. Jsou to dvě níže uvedená pravidla, bod 1) a bod 2 níže) tedy za předpokladu, že existuje EdgeGW - virtuální router, NAT, FW, VPN apod.).

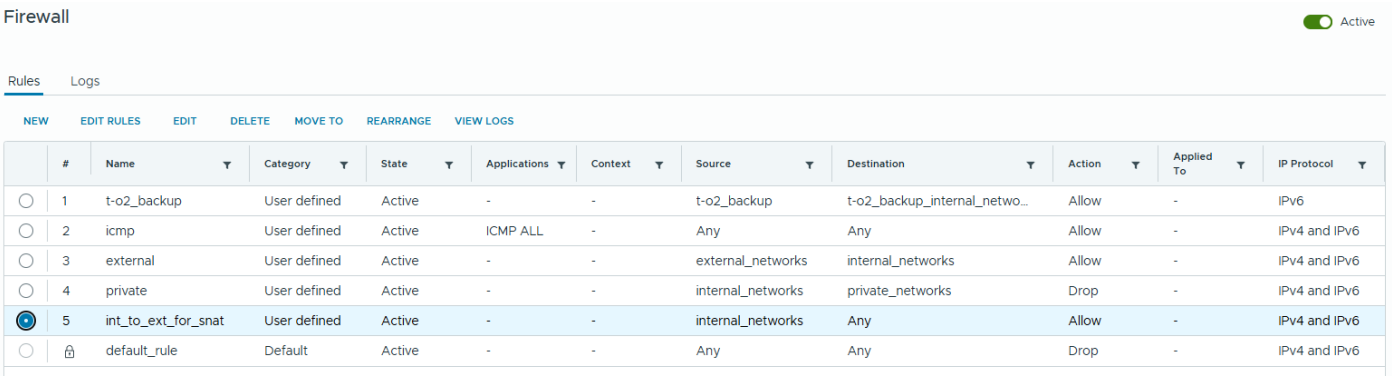
Pokud nemá organizace EdgeGW, tedy ve vaší organizaci jsou pouze **direct sítě** typu PT5 nebo je v EdgeGW v organizaci přítomna, ale má na severní straně připojenou síť PT6 se směrováním provozu do PT6 sítě a prostup do internetu nefunguje, musí tento prostup na základě požadavku nastavit síťoví specialisté v O2 ITS.

Prostup sítě v Cloudu z organizace do internetu je zajištěn dvěma níže uvedenými pravidly:

1) pravidlo SNAT „snat_to_external“ definované v NAT, 0.0.0.0/0 – zápis reprezentuje všechny sítě v Cloudu, které budou překládány na veřejnou IP adresu, případně se mohou v případě většího počtu sítí a veřejných IP adres konkrétně nastavit, která síť či IP adresy mají být překládány na tu či onu veřejnou IP adresu, viz obrázek:



2) pravidlo int_to_ext_for_snat, kde **internal_networks** jako zdroj komunikace, reprezentuje statickou skupinu, ve které je ve výchozím nastavení definována org sít v Cloudu, (může se upravit dle potřeby) a jako cíl **Any**, viz obrázek:



5.1.6 Logování služeb FW a NAT v EdgeGW

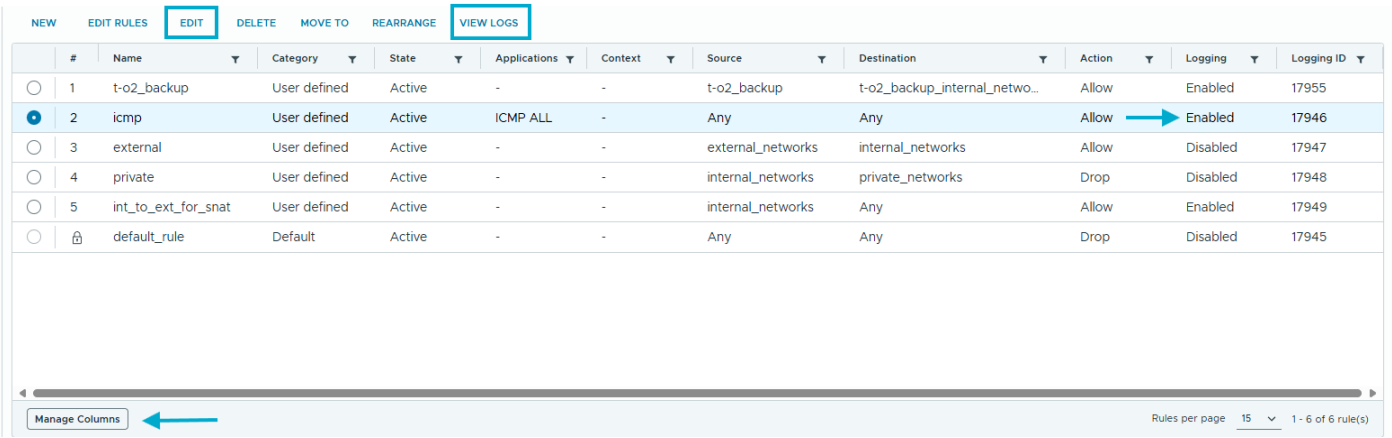
Používá se pro případ, kdy potřebujete detailněji prověřit komunikaci, která prošla skrze FW nebo NAT pravidlo. Logování si zapněte pouze pro konkrétní FW/NAT pravidla, která chcete po určitou dobu sledovat. **Jakmile již logování nebudete potřebovat vypněte jej prosím, aby se nezahlcoval systém, který sbírá logy od všech zákazníků.**

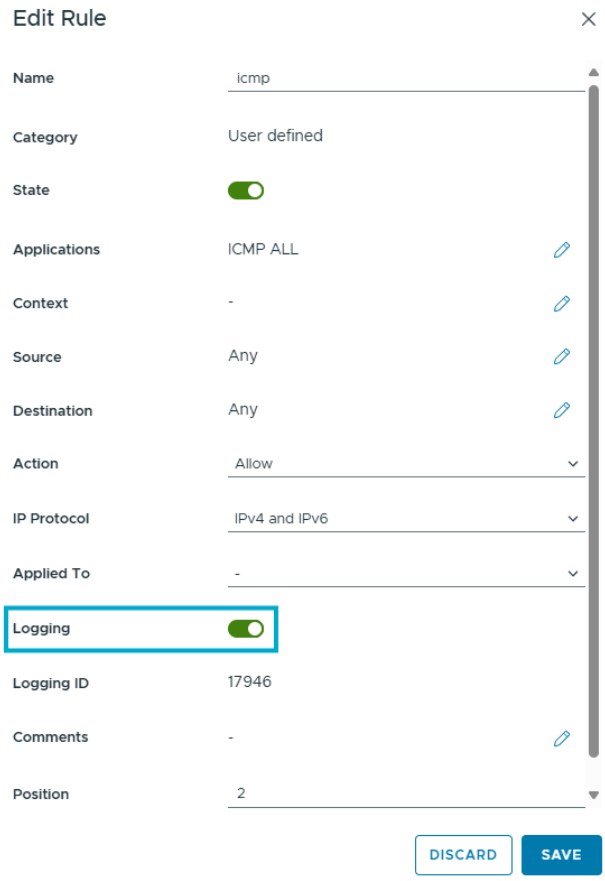
Logování FW pravidel

FW pravidla je možné logovat. Díky tomu lze zpětně dohledat komunikaci, která FW pravidlem prošla.

Zapnutí logování konkrétního FW pravidla se provádí v editaci pravidla:

Vyberete konkrétní FW pravidlo (označené modrou tečkou) -> EDIT -> Logging: ON -> Save

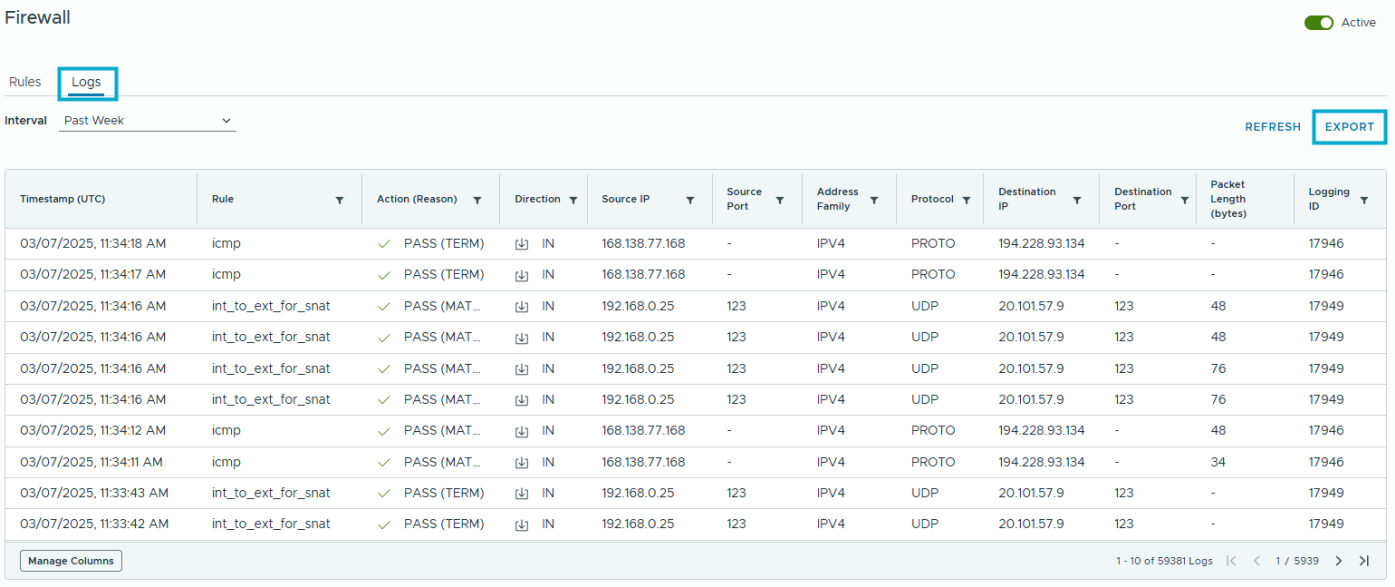




Aby se Vám v seznamu FW pravidel zobrazil sloupec ukazující, jaká pravidla mají logování zapnutá, je potřeba si sloupec zpřístupnit přes tlačítko „Manage Columns“, který je ve výchozím stavu neaktivní.

Přes „VIEW LOGS“ viz obrázek výše následně můžete nahlížet na logy daného FW pravidla.

Požadujete-li export všech logů FW pravidel se zapnutým logování, překliknete se na záložku „Logs“, kde si dále můžete filtrovat dle vašich potřeb, případně provést export do .csv viz obrázek níže.

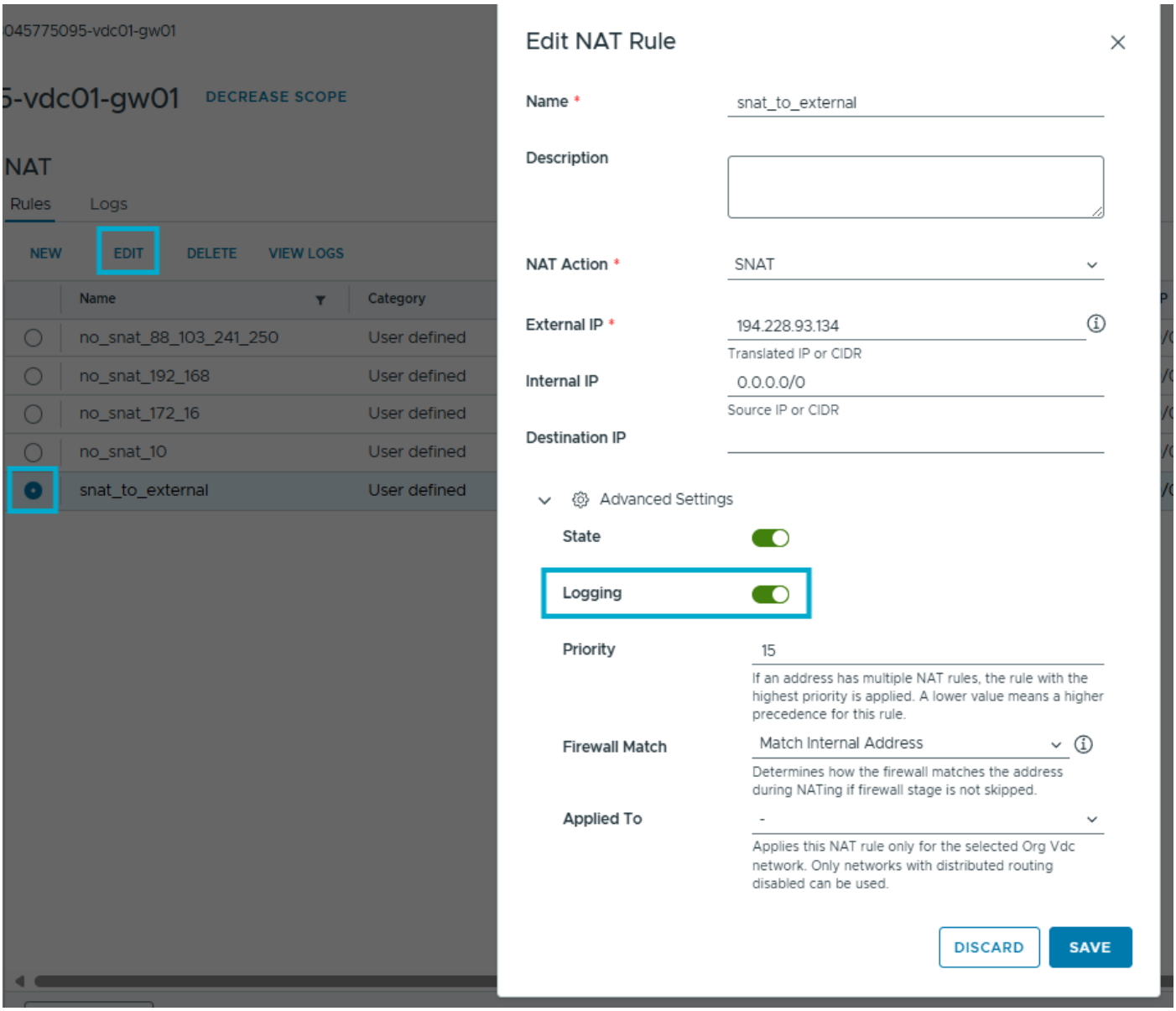


Logování NAT pravidel

NAT pravidla je možné též logovat. Díky tomu lze zpětně dohledat komunikaci, která NAT pravidlem prošla.

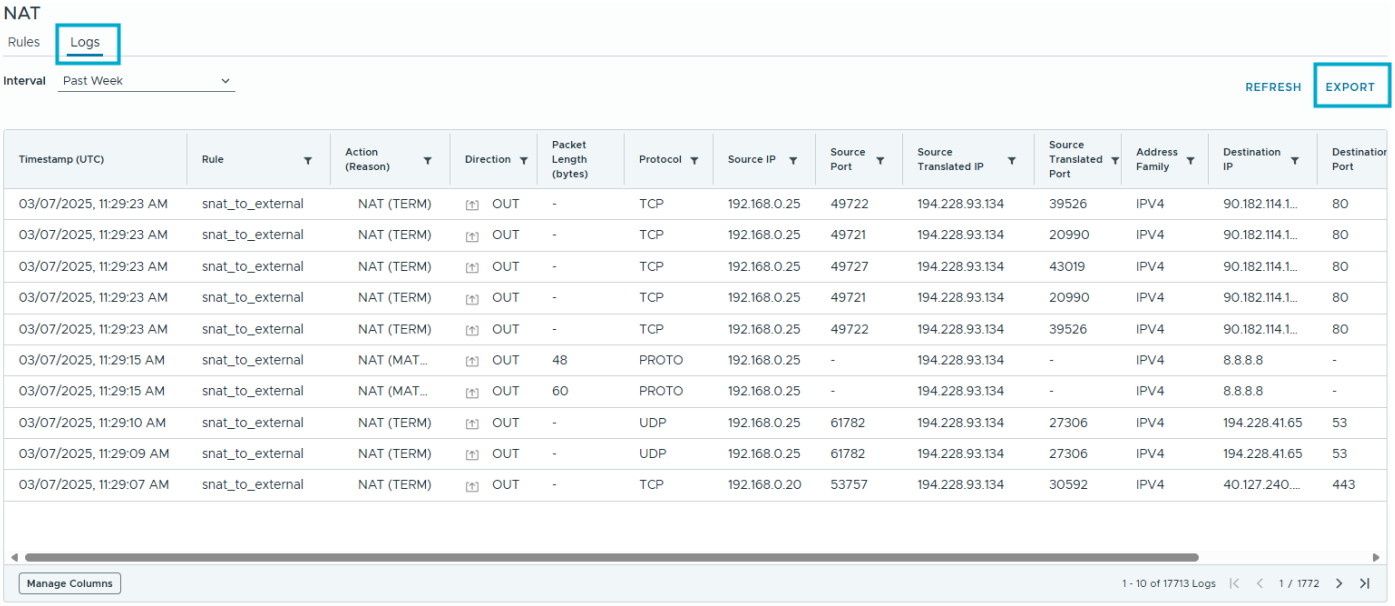
Zapnutí logování konkrétního NAT pravidla se provádí v editaci pravidla:

Vyberete konkrétní FW pravidlo (označené modrou tečkou) -> EDIT -> Logging: ON -> Save



Přes „VIEW LOGS“ viz obrázek výše následně můžete nahlížet na sesbírané logy daného NAT pravidla.

Požadujete-li export logů všech NAT pravidel se zapnutým logování, překlikněte se na záložku „Logs“, kde si dále můžete filtrovat dle vašich potřeb, případně provést export do .csv viz obrázek níže



5.1.7 Nastavení Firewallu a NATu – doporučení nastavení FW pro zvýšení bezpečnosti

Důležité:

Dále důrazně doporučujeme mít v překladech **a zejména v pravidlech firewallu povoleny skutečně jen porty, které potřebujete pro provoz Vaší organizace a další všechny nepotřebné porty, které nevyužíváte tak nepovolovat.** **Mít zapnutý firewall podle všech bezpečnostních doporučení a nastavená jen ty nezbytná pravidla, která zajistí bezpečný provoz Vaší organizace**. (Ostatní nespecifikovaný provoz z nespecifikovaných zdrojů bude tak na FW zahozen z důvodu bezpečnosti, což je žádoucí) a bude tak povolena jen komunikace, která je požadována.

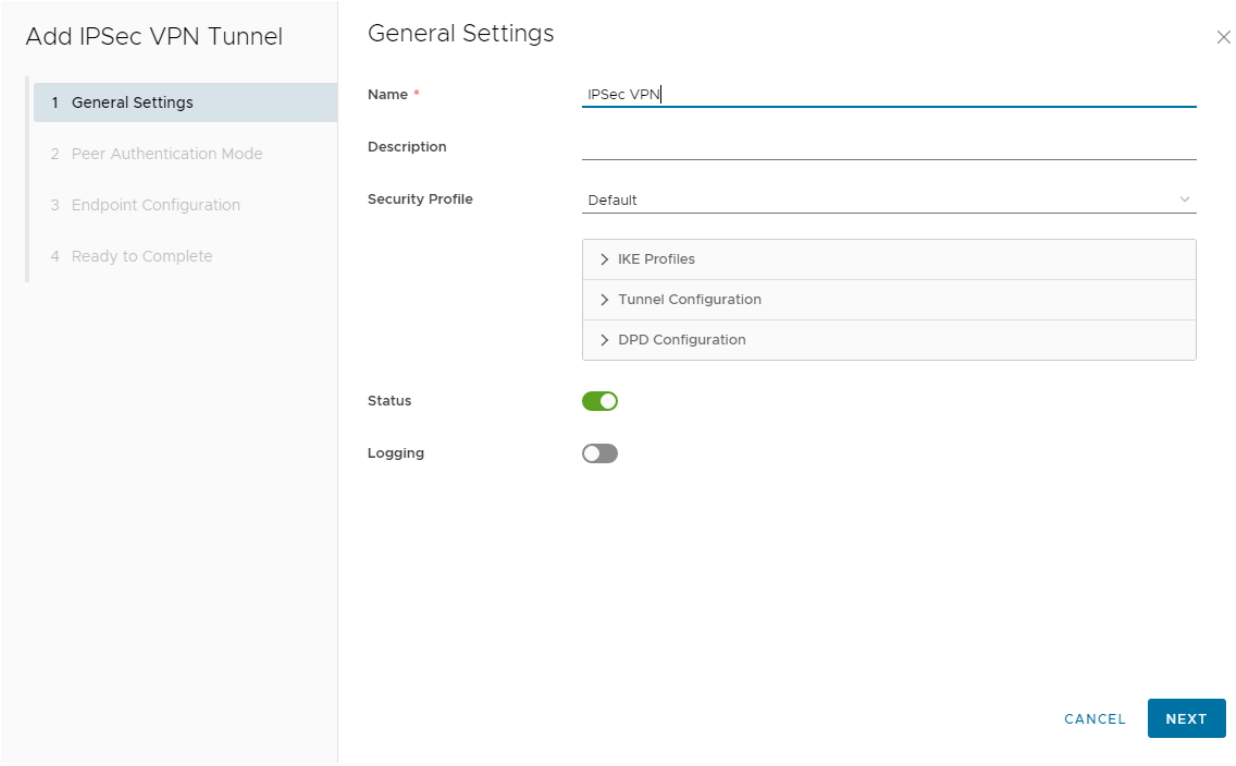
Doporučujeme omezit všechny management porty, pomocí kterých probíhá administrace cílového systému, tak aby v pravidlu ve FW ve zdroji komunikace byly uvedeny jen důvěryhodné IP adresy či sítě, ze kterých se na servery v Cloudu budete připojovat z důvodu bezpečnosti a snížení rizika kompromitace/zneužití serveru.

Příklad: v případě povolení komunikace tcp/3389 a tcp/22 důrazně doporučujeme specifikovat v pravidle ve zdroji komunikaci jasně zdrojové IP adresy nebo sítě, ze kterých je možno se na server(y) připojit, (přes RDP do Windows nebo přes SSH do Linuxu), tak aby bylo možno komunikaci na servery navázat jen z důvěryhodných IP adres či sítí a tím tak zabezpečit celou komunikaci a neumožnit tak navazovat komunikaci z nedůvěryhodných IP adres, ze kterých je možno na servery následně útočit. Následně je nutno pro připojení na server z internetu mít vytvořené pravidlo DNAT, které zajistí překlad veřejné IP adresy na privátní IP adresu serveru aby komunikace fungovala.

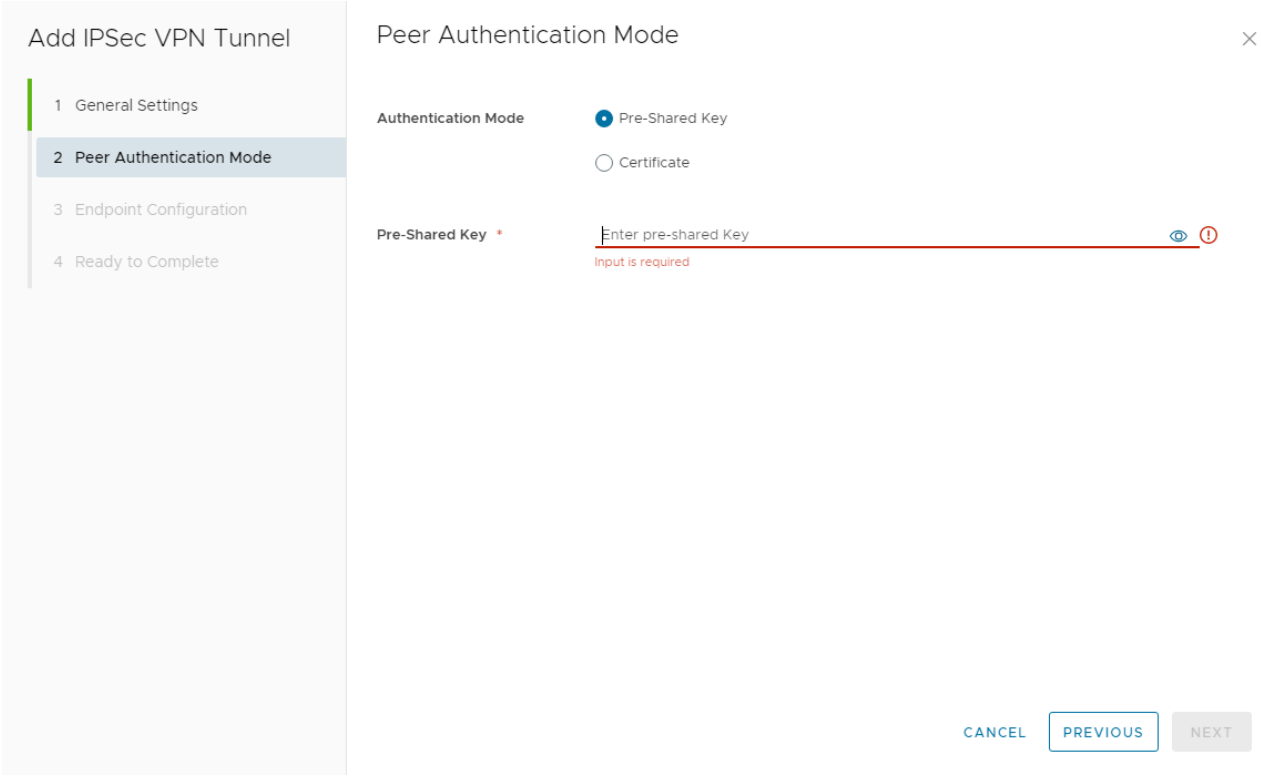
5.1.8 Vytvoření IPSec VPN

- Klikněte na **IPSec VPN -> NEW**

- VPN si pojmenujte



- Zadejte Pre-Shared Key nebo Certificate



Dále specifikujte:

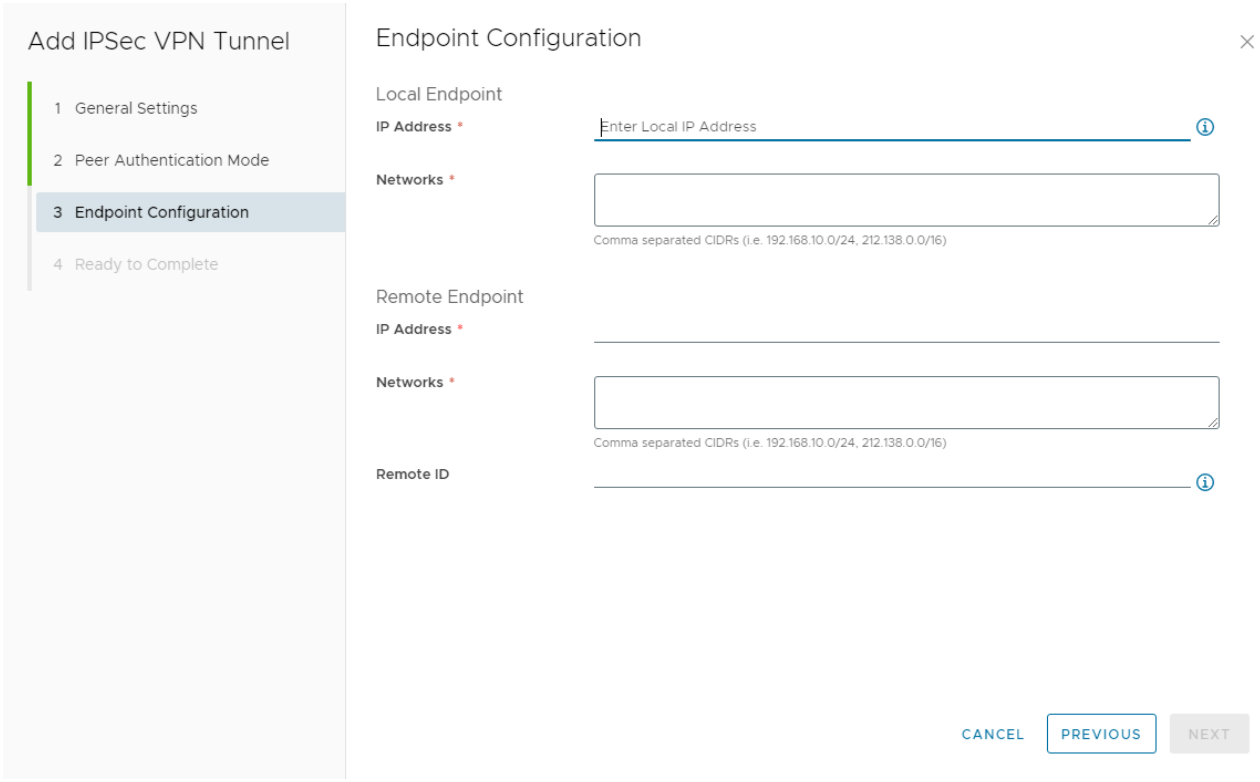
Local Endpoint:

IP Adress: veřejná IP adresa v Cloudu
Networks: privátní rozsah(y) v Cloudu

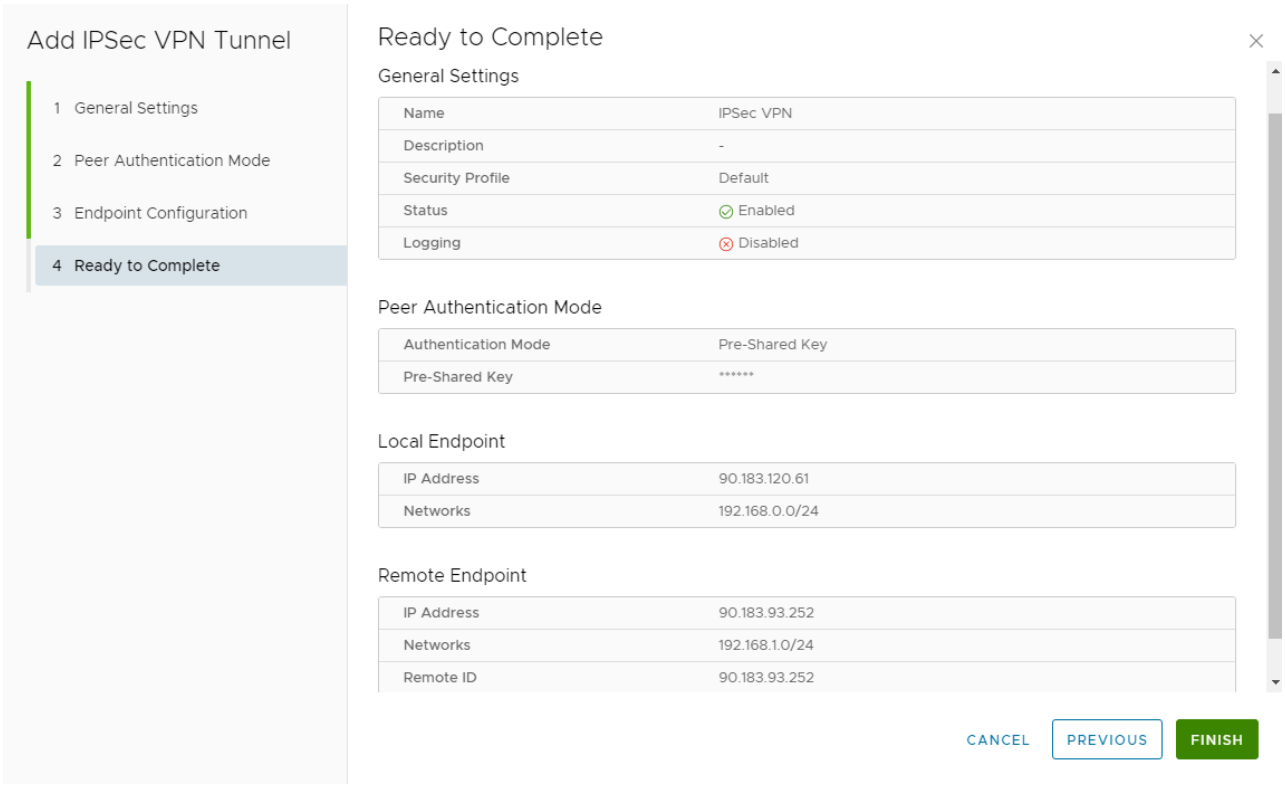
Remote Endpoint

IP Adress: veřejná IP adresa vašeho routeru (ne cloud)
Networks: privátní rozsah(y) za vaším routerem (ne cloud)
Remote ID: veřejná IP adresa vašeho routeru (ne cloud)

Poznámka: Privátní rozsahy musí být na obou stranách jiné (nesmí být na obou stranách shodné), jinak nebude komunikace funkční.

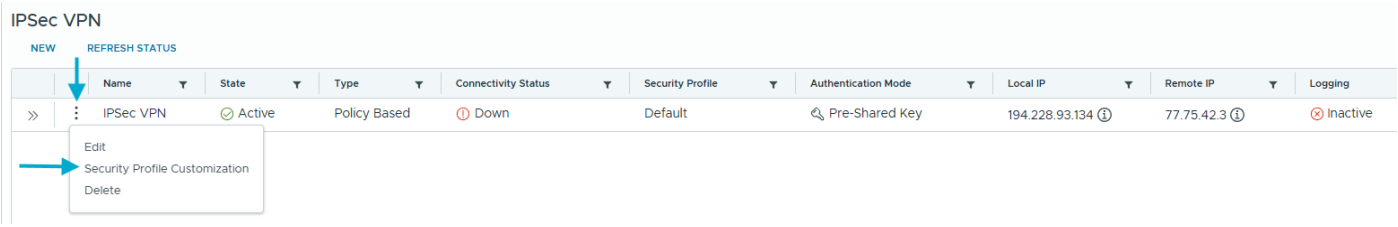


Vytvoření IPSec VPN dokončíte kliknutím na **FINISH.**

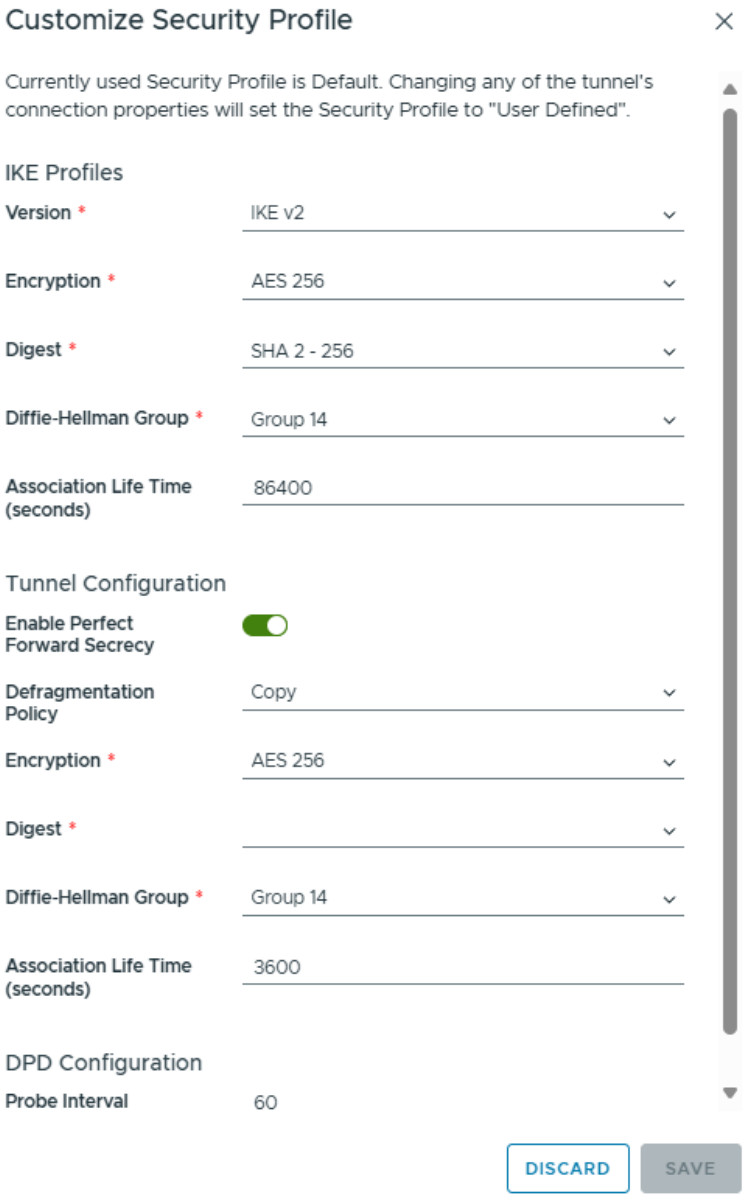


5.1.9 Vytvoření Security profilu – nastavení pro IPSec VPN

Pokud nevyhovuje výchozí konfigurace IP SEC VPN, tak je možno vytvořit Security profil (specifickou konfiguraci) pro IP Sec VPN.



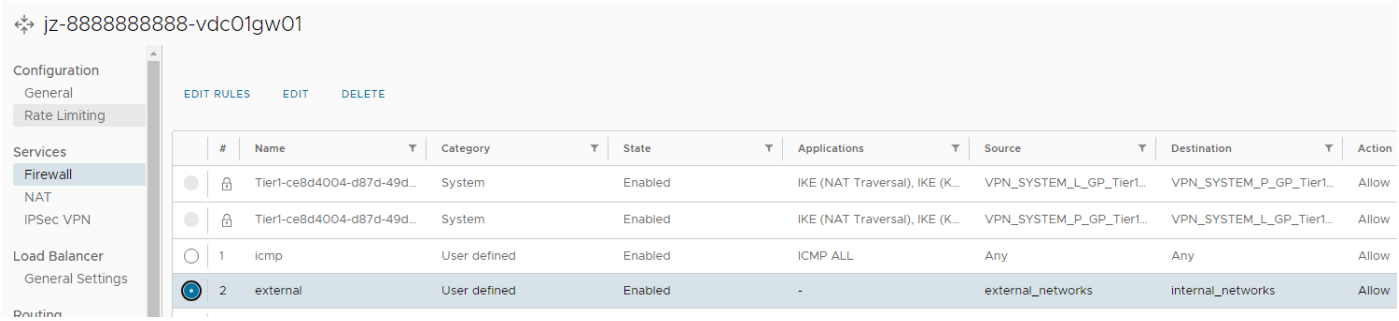
Zobrazí se jednotlivé nastavení IP SEC VPN, které je možno detailně konfigurovat a které musí být shodně nastaveno i na druhé straně (na straně zákaznického routeru). Toto nastavení – security profil se následně použije pro IPSec VPN.



Následně je potřeba nakonfigurovat VPN tunel na vaší straně (na straně zákazníka).

Ve výchozím nastavení při vytvoření organizace je povolena komunikace do internetu, popsáno v kapitole 5.1.5. Dále je ve výchozím nastavení povoleno pravidlo, povolující komunikaci z externích sítí do Cloudu, konkrétně se jedná o pravidlo **external, kde zdroj (source) je external_networks, což je IP set, obsahující externí sítě, pro které chceme povolit komunikaci do všech interních sítí v o2 cloudu. Tedy do IP setu external_networks je potřeba po nakonfigurování vpn vložit všechny lokální remote subnety IPsec vpn – subnety vpn poboček). IP set external_networks je možno upravit o další rozsahy.**

Dále po nastavení IP Sec VPN jsou automaticky vytvořena dvě nejvýše uvedená pravidla, viz obrázek:



Upozornění:

Při konfiguraci IP sec VPN **nesmí** být na obou stranách **shodné rozsahy**

Pokud jsou nastaveny rozsahy ve statických routách, tak mají přednost před rozsahy definovanými v IP SEC VPN.

Následně je VPN nastavena a vpn tunel se úspěšně sestaví.

Poznámka: Status VPN se může změnit na status UP až poté, co začne v tunelu probíhat komunikace.

5.1.10 Konfigurace Routingu

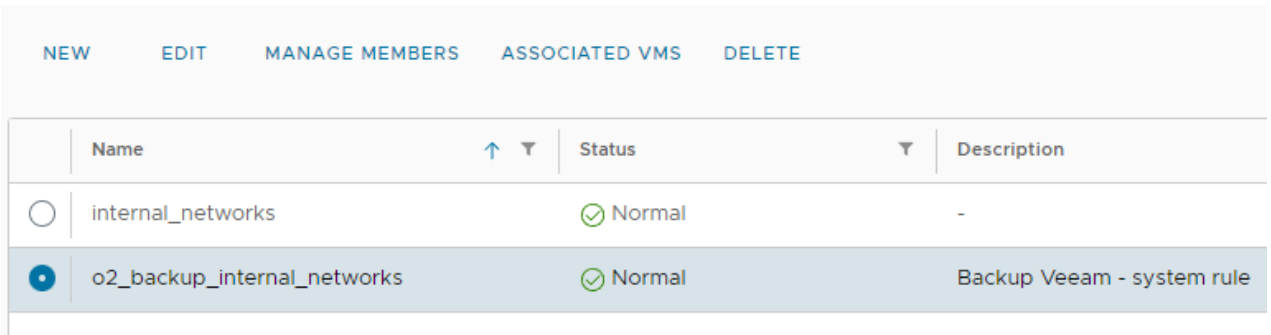
Pokud máte nastaveno více sítí v organizaci, je možné nastavit routing do konkrétních sítí.

5.1.11 Konfigurace Static Groups

- Klikněte na **Static Groups**

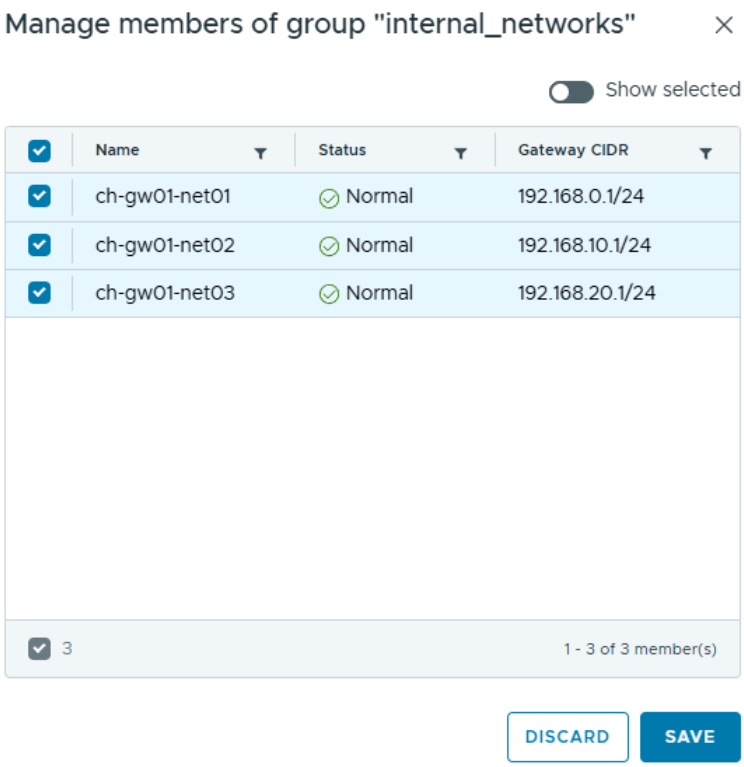
Ve výchozím nastavení po zřízení organizace jsou nastaveny skupiny internal_networks a o2_backup_internal_networks.

Členové těchto skupin jsou všechny interní sítě v daném vDC.



Tyto skupiny pak lze přehledně a jednoduše používat ve FW pravidlech.

Pokud si vytvoříte novou routovanou síť, nezapomeňte ji zahrnout do členů obou skupin.



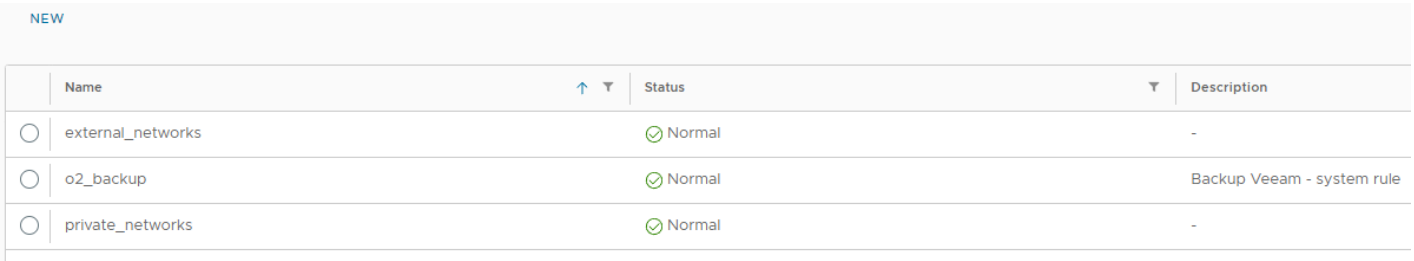
Pokud vytvoříte novou org. síť privátního rozsahu, je nutné ji nastavit jako člena do obou statických skupin **internal_networks** a **o2_backup_internal_networks**. To nastavíte pomocí **MANAGE MEMBERS dané skupiny.**

5.1.12 Konfigurace IP Sets

- Klikněte na **IP Sets**

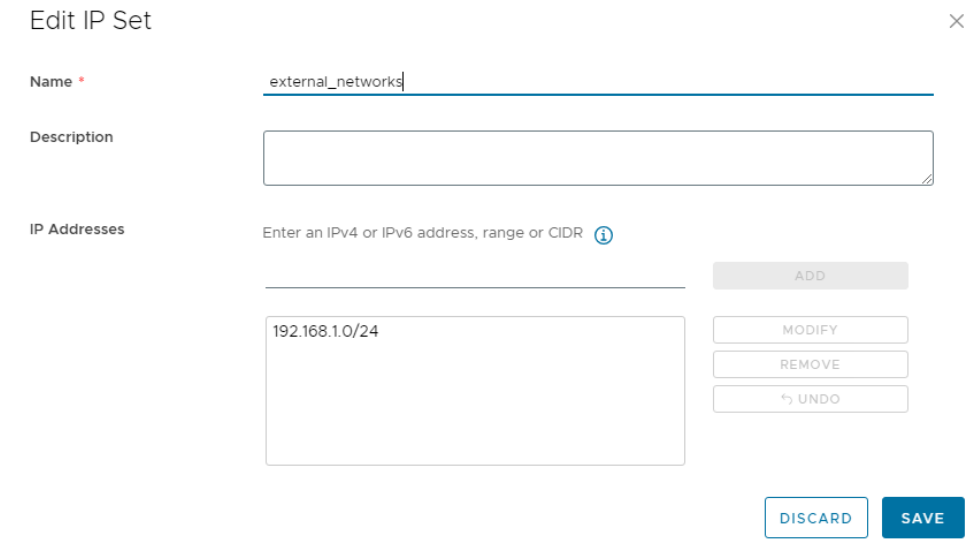
Ve výchozím nastavení po zřízení organizace jsou nastaveny IP Sety:

enternal_networks, private_networks a o2_backup.

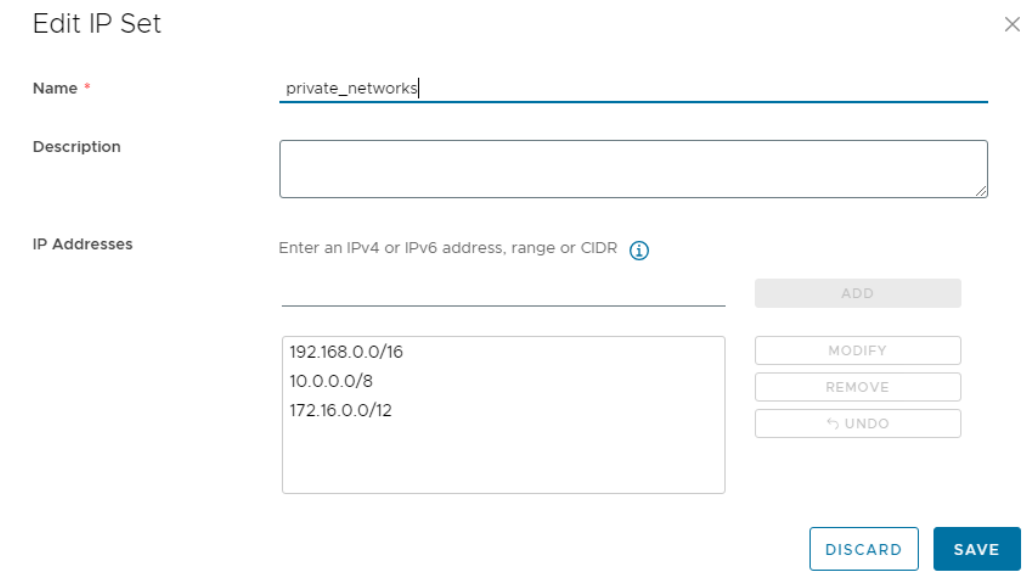


external_networks – IP Set**,** ve kterém je definována externí síť.
Zde definujete IP adresy nebo sítě, které mají mít přístup do privátních rozsahů v O2 Cloudu.
IPv6 je možno také použít.

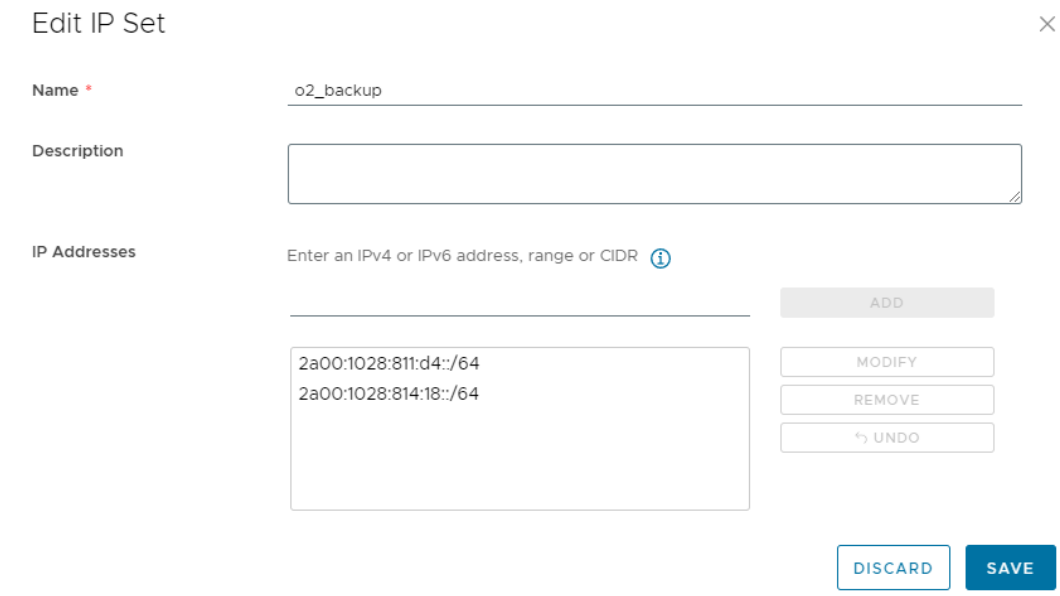
Pro příklad: 192.168.1.0/24, síť, která není v Cloudu ale u zákazníka, např. pro VPN, kde dva shodné rozsahy nemohou být na obou stranách.



private_networks – IP Set, který obsahuje obecně známé privátní rozsahy, viz obrázek
IPv6 je možno také použít.



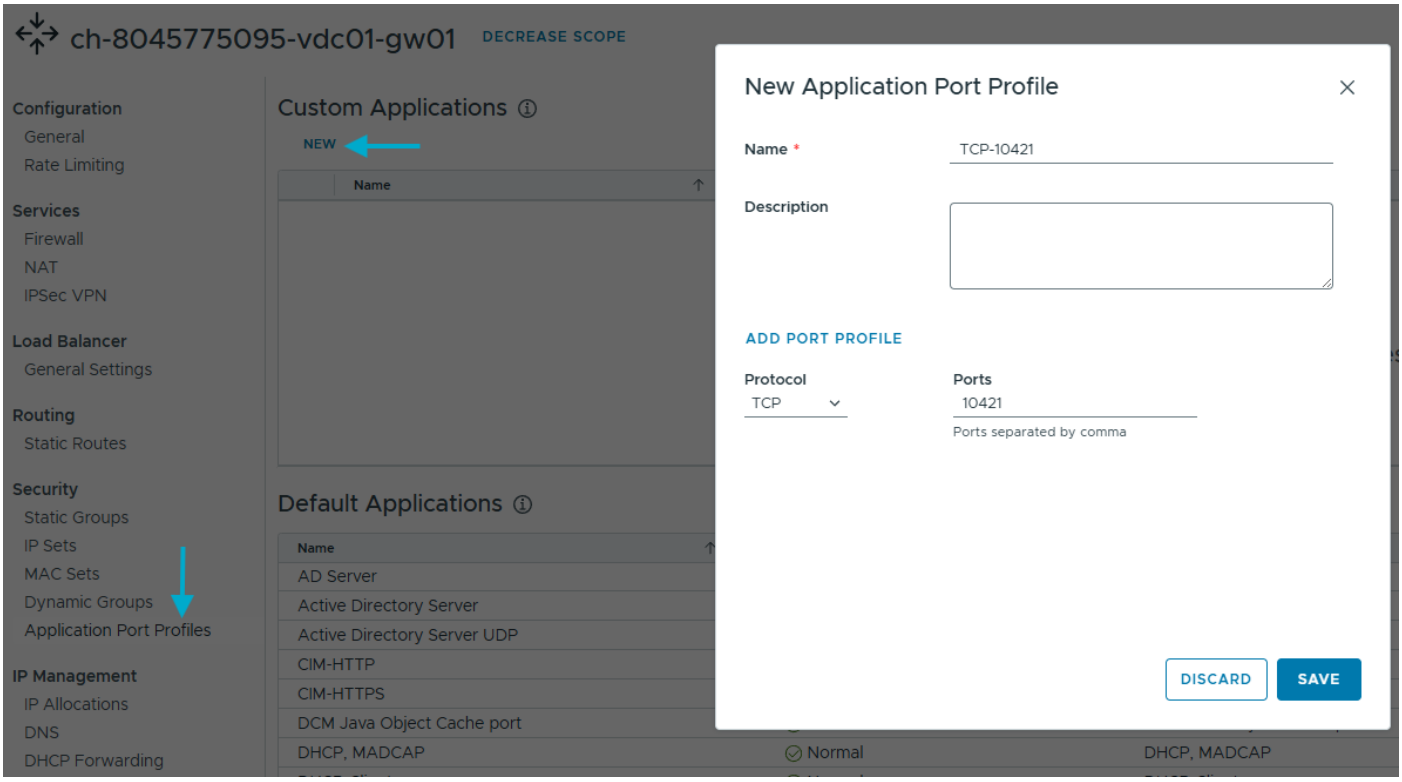
o2_backup – IP Set, který obsahuje IPv6 adresy pro Backup infrastrukturu v O2.
Toto pravidlo prosím neupravujte.
IPv6 je možno také použít.



Je možno vytvářet vlastní IP sety, které je možno následně použít v pravidlech ve FW.

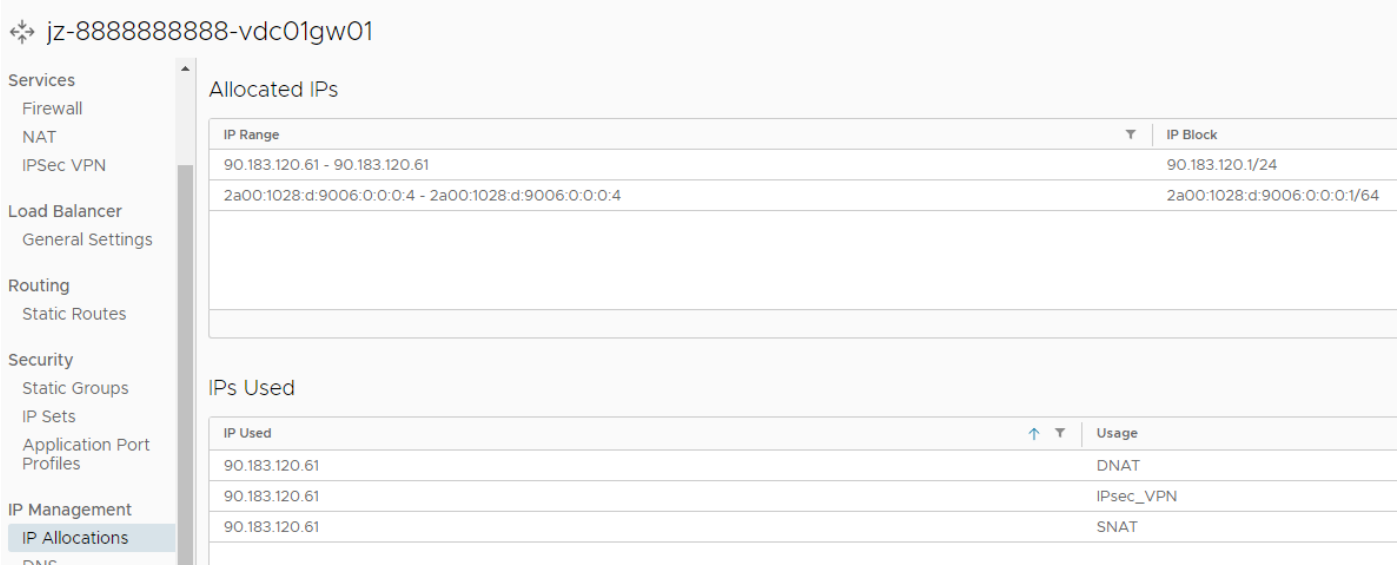
5.1.13 Konfigurace Application Port Profiles

Je možno si vytvořit aplikační profil a ten pak použít ve FW pravidlech. Hodí se pro případ, kdy v defaultních portech nenaleznete Váš požadovaný port.



5.1.14 IP Allocations

V IP Allocations je viditelné, které veřejné IP adresy jsou nastavené ve Vaši organizaci, ty se mohou použít v pravidlech.



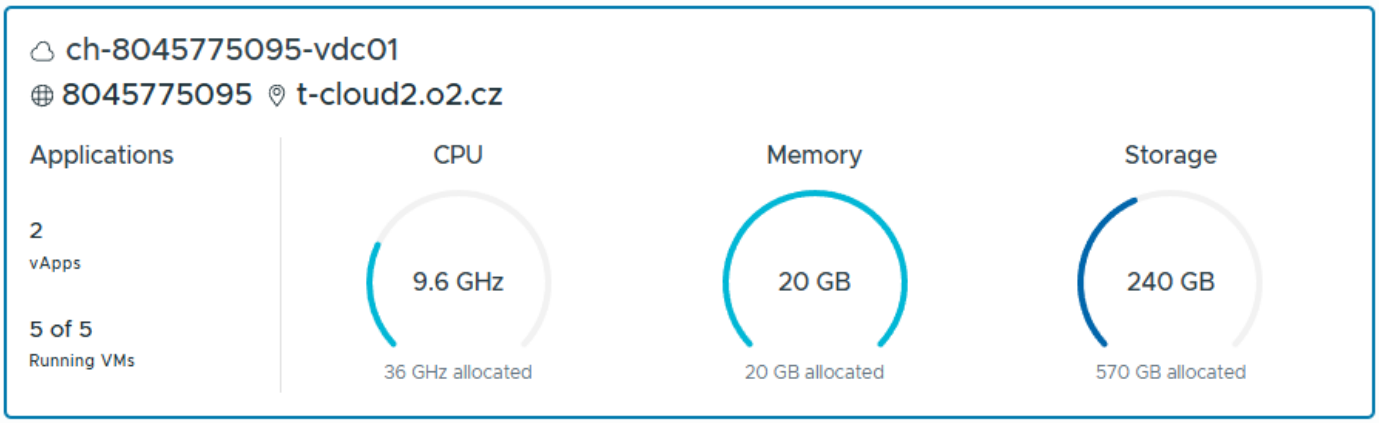
5.1.15 DNS a DHCP Forwarding

Je možno konfigurovat i služby DNS a DHCP Forwarding.

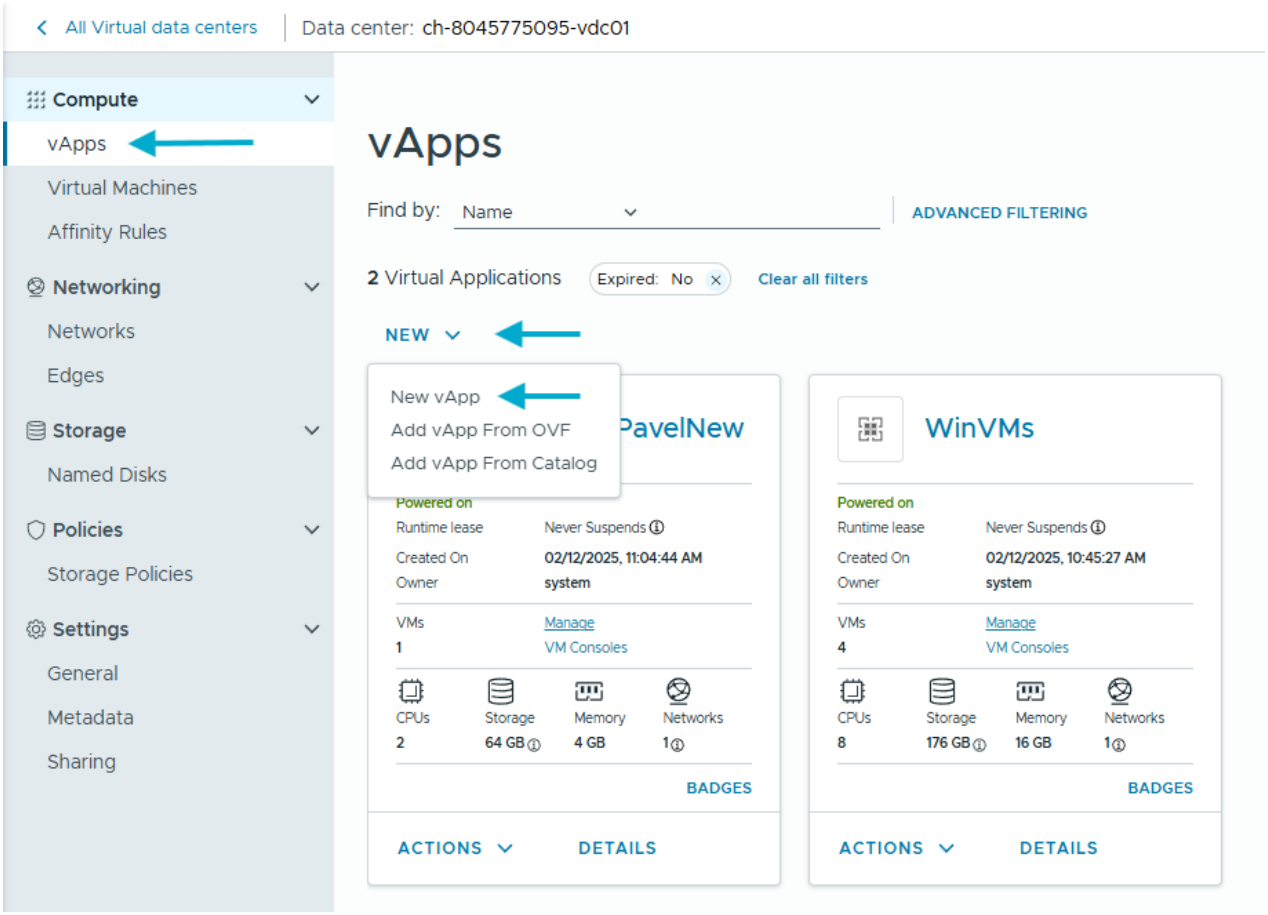
6 Vytvoření vAPP

Tato kapitola popisuje způsob vytvoření vlastní vAppy.

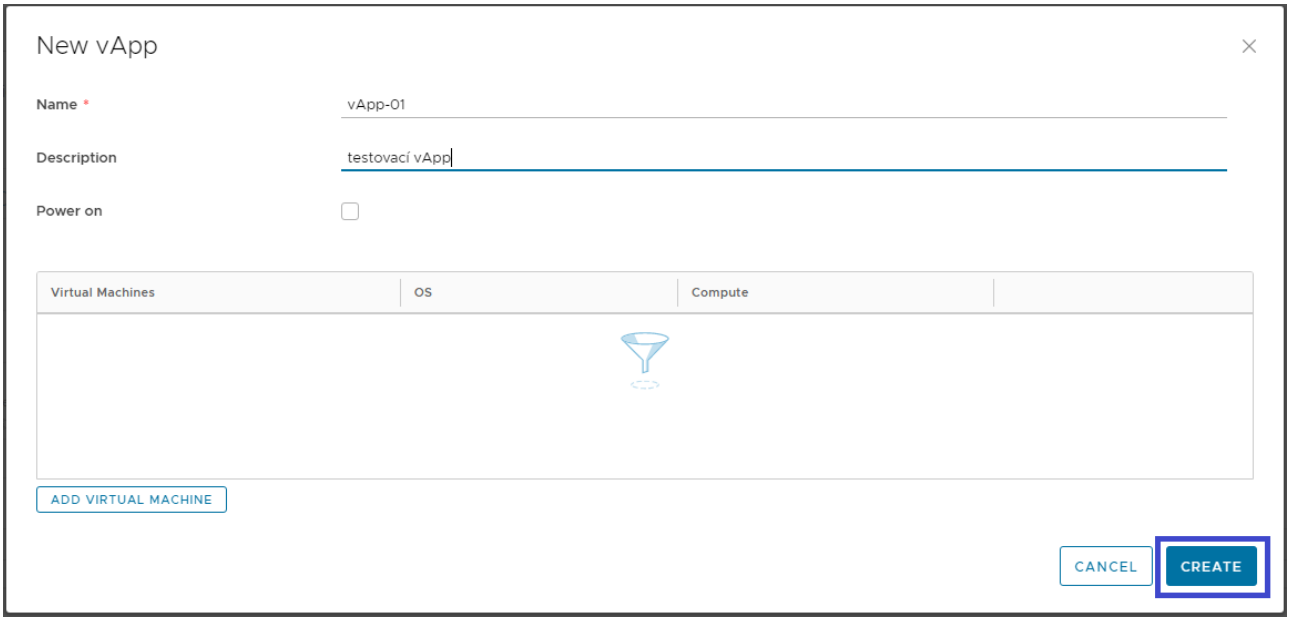
V organizaci se proklikneme do vDC, kde chceme provést vytvoření vAPP.



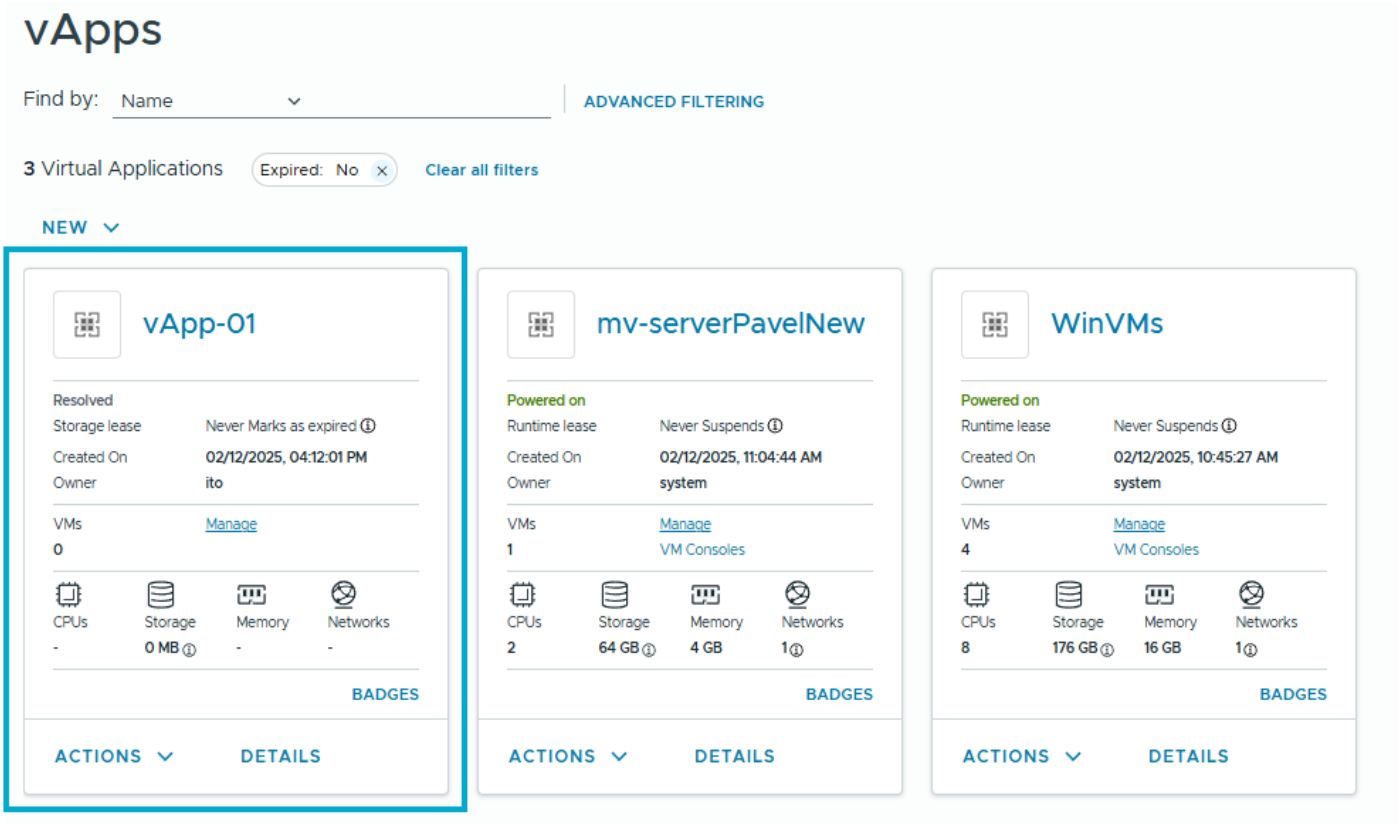
Zde přejdeme v levém sloupci na **vApps** a klikneme na „**New vApp**“.



Do pole „**Name**“ zadejte jméno vApp – mělo by odpovídat účelu vytvářeného vApp a kliknout na „**Create**“
Description (Popis) – popis popisující vAppu.

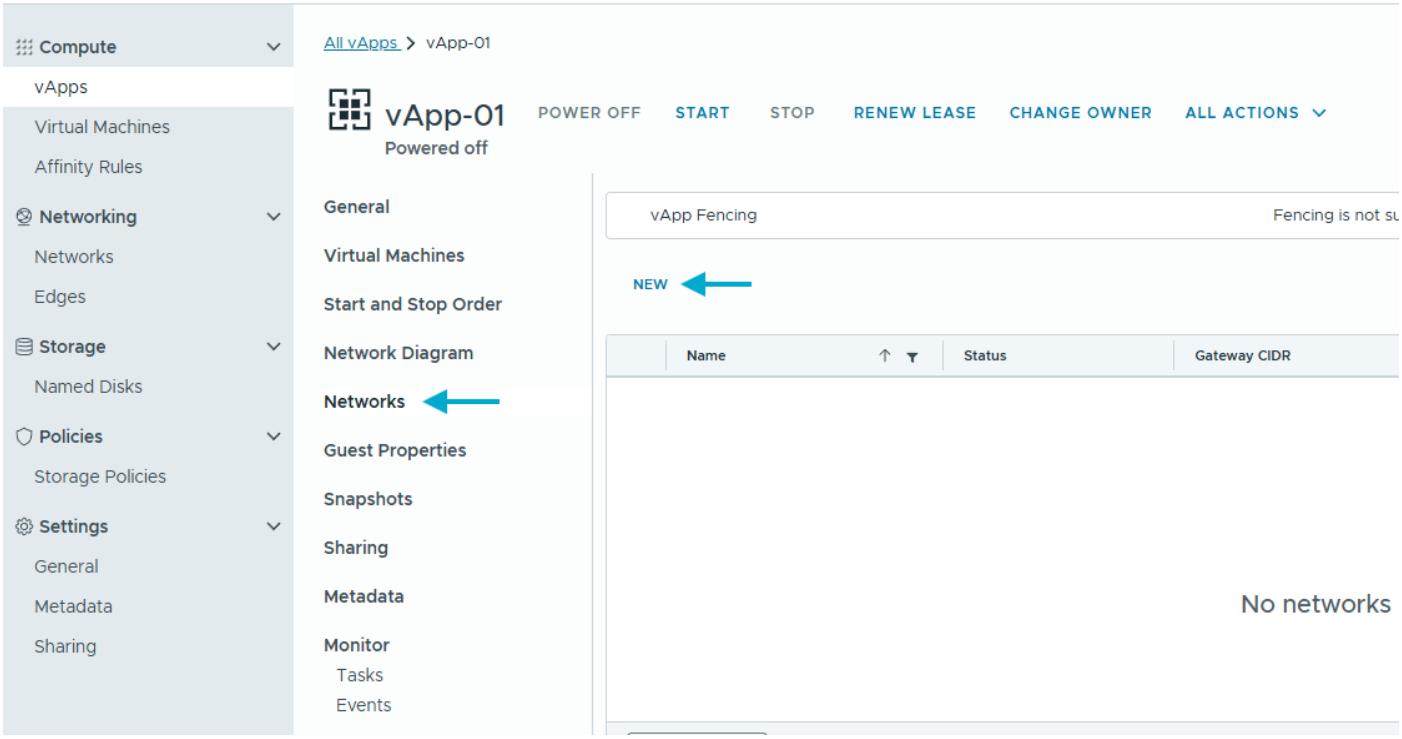


vApp je následně vytvořená. Objeví se v přehledu vApp v příslušném vDC.

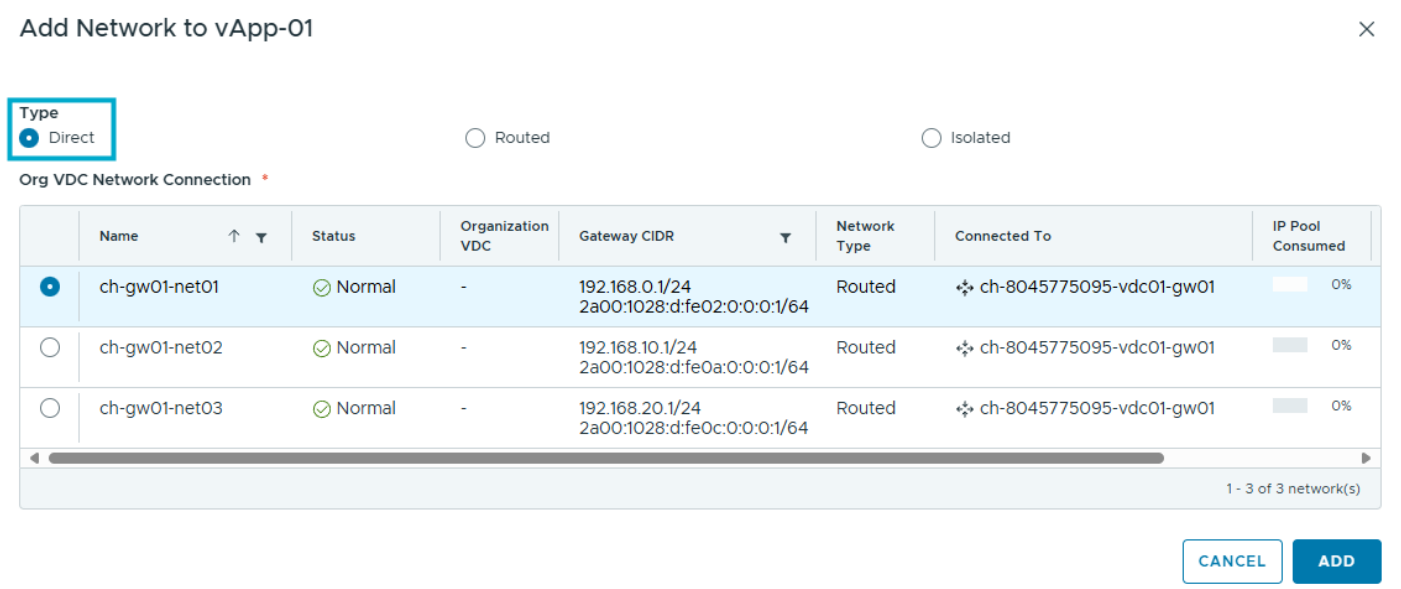


Do nové vAppy je potřeba vždy připojit privátní síť, kterou bude VM využívat:

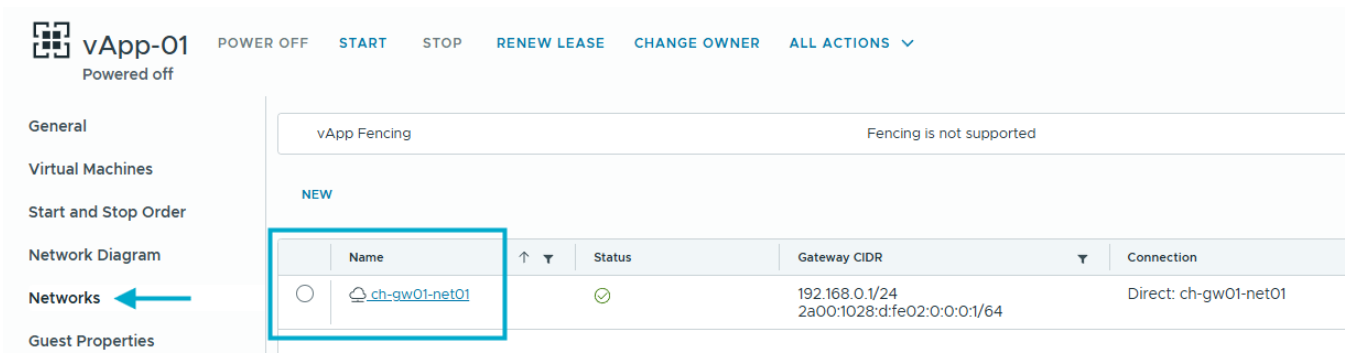
Networks -> NEW -> Type: **Direct** -> vybereme privátní síť -> ADD



Bez ohledu na to, zda se jedná o routovanou privátní síť nebo direct sít, vždy sítě do vAppy připojujeme jako typ Direct



Tímto jsme si připojili privátní síť (v tomto případě síť ch-gw01-net01 s rozsahem 192.168.0.0/24) do vAppy.



Následně můžete provést deploy VM v rámci vytváření vApp – volba „ADD VIRTUAL MACHINE). (není podmínkou).

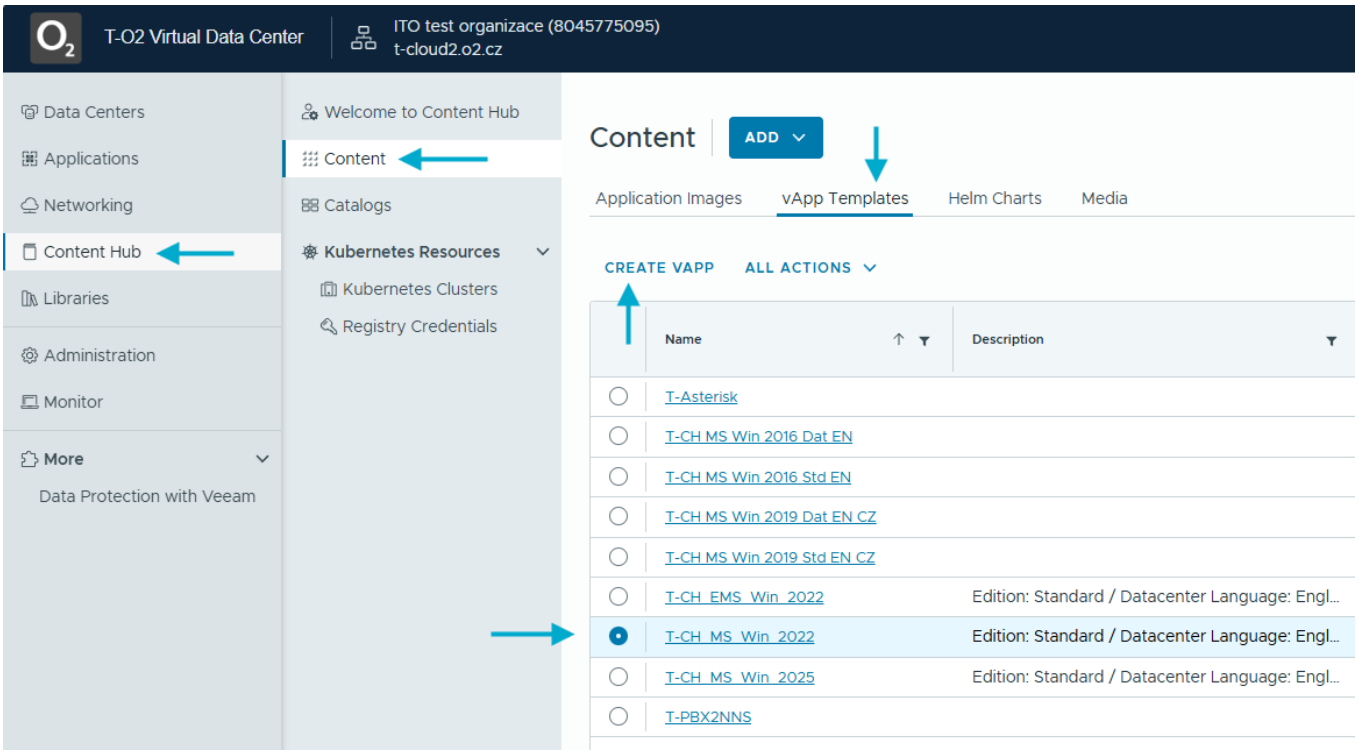
Tlačítka ACTIONS a DETAILS

DETAILS – info o vApp
ACTIONS – Pod rozbalovacím menu ACTIONS na kartě vApp můžeme provádět následující:
Suspend – Suspendovaná vApp zapauzuje všechny VM ve vApp
Power Off – Každé VM v rámci vApp bude vypnuto
Stop – Zastavení
Start – Zapne vApp a všechny VM
Reset – Restartuje vApp
Discard suspended state – zruší stav suspend
Delete – smaže vApp
Create Snapshot – udělá snapshot vApp
Revert to Current – vrátí se k Snapshotu
Remove All – dojde k odmazání snapshotu
Change owner – změní vlastníka vApp
Move – Přesune vApp a odstraní z původního místa
Copy – Zkopíruje vApp a zachová na původním umístění
Renew Lease – prodloužení expirace nad vAppou nebo virtuálním serverem
Create Template – přidá vApp do katalogu
Convert To VM – převede vAppu obsahující 1 VM na samostatný VM bez vAppy (užitečné pokud nechcete používat strukturu vApp tedy provozovat VM bez vAppy – bez obálky)
Edit Badges – umožňuje označení vAppy barevným odznáčkem pro zpřehlednění
Add VM – umožňuje přidat VM do vApp
Add Network – umožňuje přidat síť do vApp
Download – stáhne vApp ve formátu OVA (za předpokladu, že je VM vypnuté)

6.1 Vytvoření vAPP (virtuálního serveru) z katalogu:

vAppu je možné vytvořit i z katalogu. Přejděte v levé nabídce na Content Hub.

Následně klikněte v na **Content**, vyberte **vApp Templates**, zvolte příslušnou Template (šablonu), ze které požadujete vytvořit VM, zvolte „**CREATE VAPP**“ a projděte průvodce vytvořením vAppy.

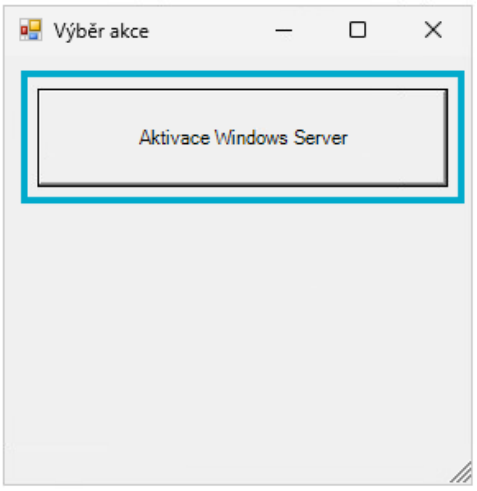


Tímto je vytvoření vApp dokončeno.

6.2 Aktivace operačního systému

Po spuštění serveru a provedení OS Guest Customizace provedete aktivaci operačního systému následovně:
V adresáři **C:\Install\IMAGE_Install_Utilities_v2** je uložen script **MS-ActivateOS-2016-2019-2022-2025-v2.ps1.**
(Script aktivuje Windows OS, verze 2016,2019,2022 a 2025).

Spusťte script MS-ActivateOS-2016-2019-2022-2025-v2.ps1 a zvolte Aktivace Windows Server.

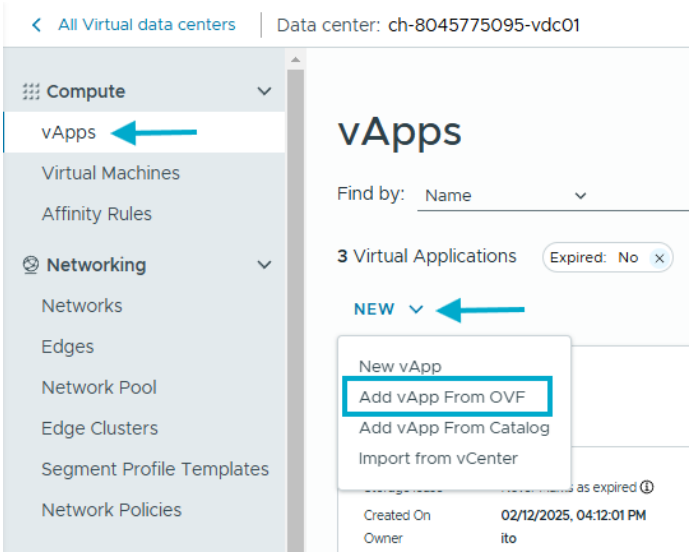


Po spuštění scriptu dojde k ověření prostupu z vaší sítě na KMS server.
Pokud prostup je, tak script nastaví operačnímu systému KMS server a provede aktivaci OS proti KMS serveru.

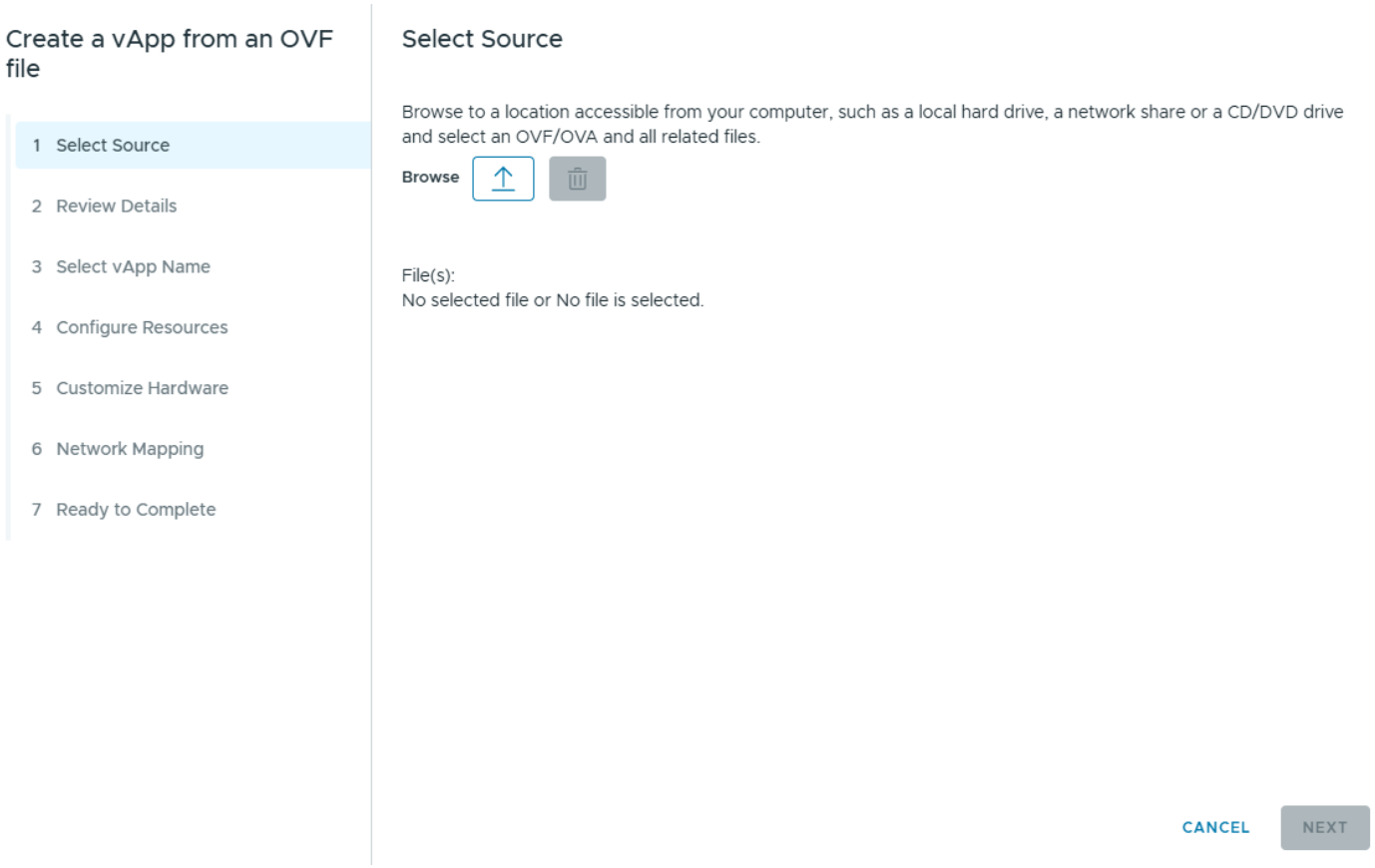
Pokud prostup není, zadejte požadavek přes Servicedesk a prostup z Vaší sítě na KMS server bude nastaven.

6.3 Vytvoření vAPP z OVF:

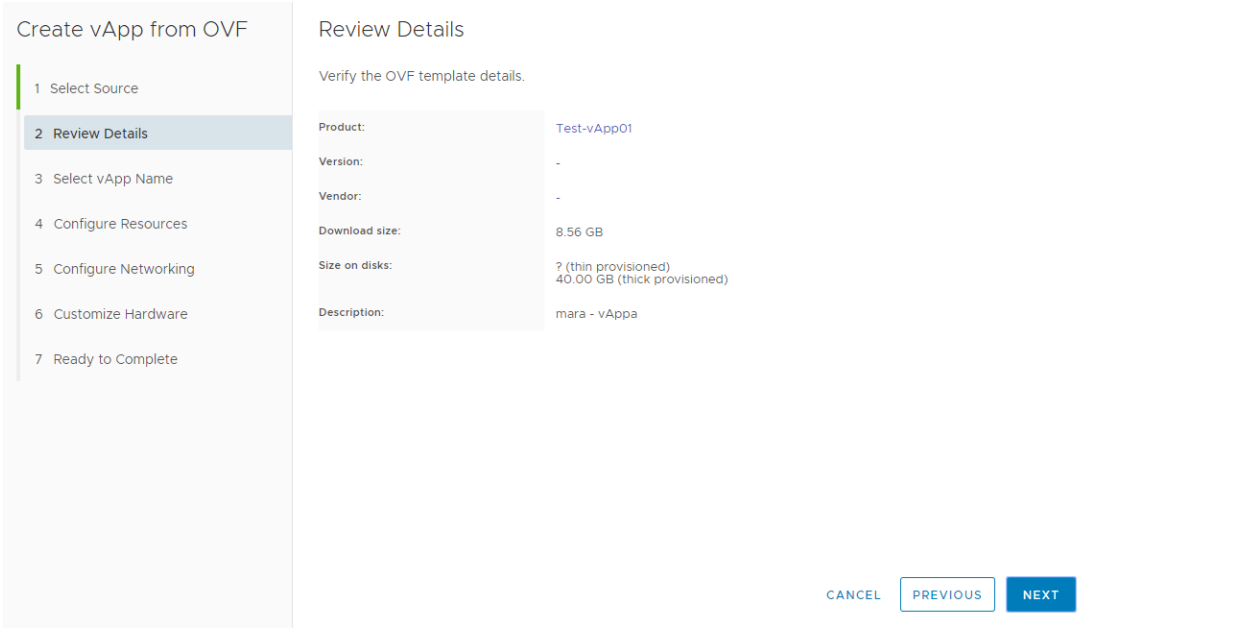
Klikněte na „**vApps“** v levém sloupci a následně na „**Add vApp From OVF**“



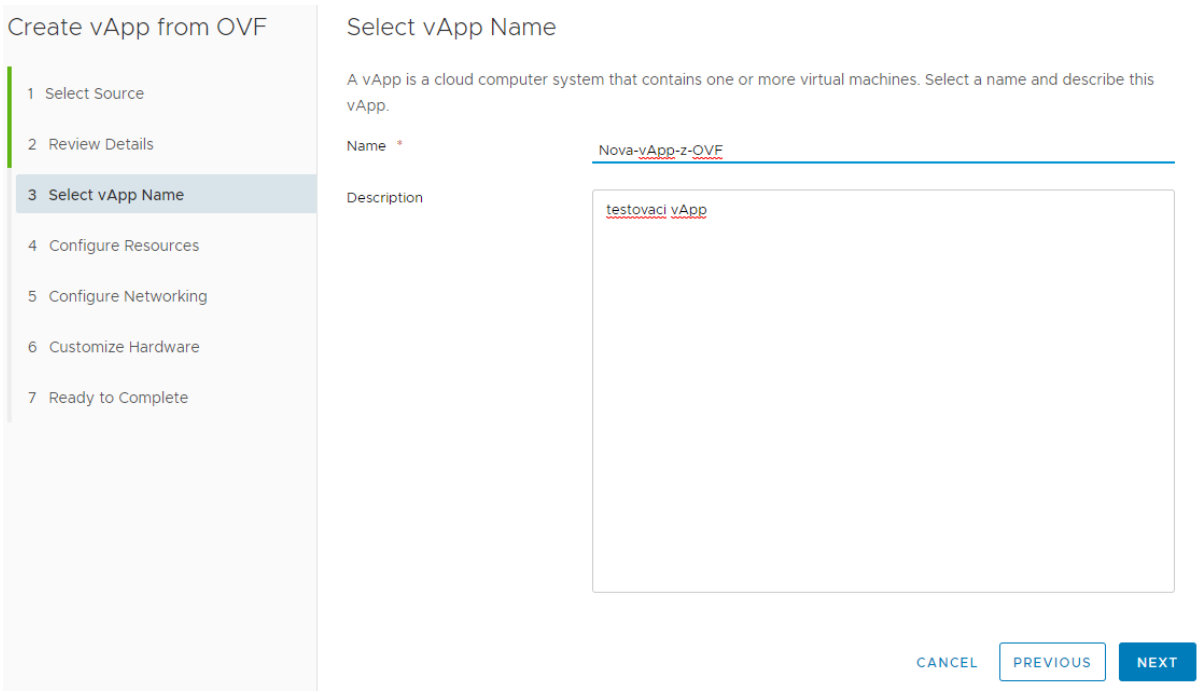
V prvním kroku vyberte soubor *.ova nebo *.ovf z lokálního počítače přes tlačítko Browse a pokračujte kliknutím na „**NEXT**“



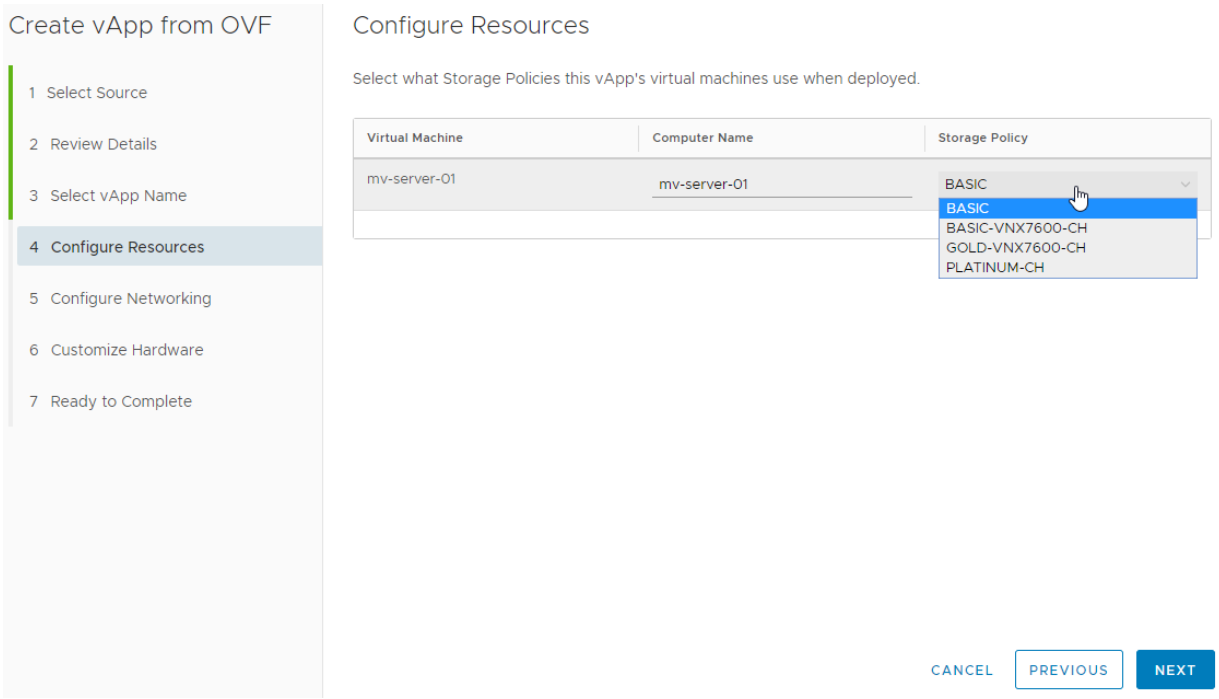
V následujícím okně se zobrazí souhrn informací o vAppě



Vyplňte název vAppy (Name) a pokračujte tlačítkem „**NEXT**“



V následujícím okně můžete pojmenovat server(y) ve vAppě nebo název (názvy) ponechat a dále vybrat uložiště (Storage Policy), na kterou budou uloženy. Pokud máte více uložišť, výběr je možný po kliknutí na Storage Policy.

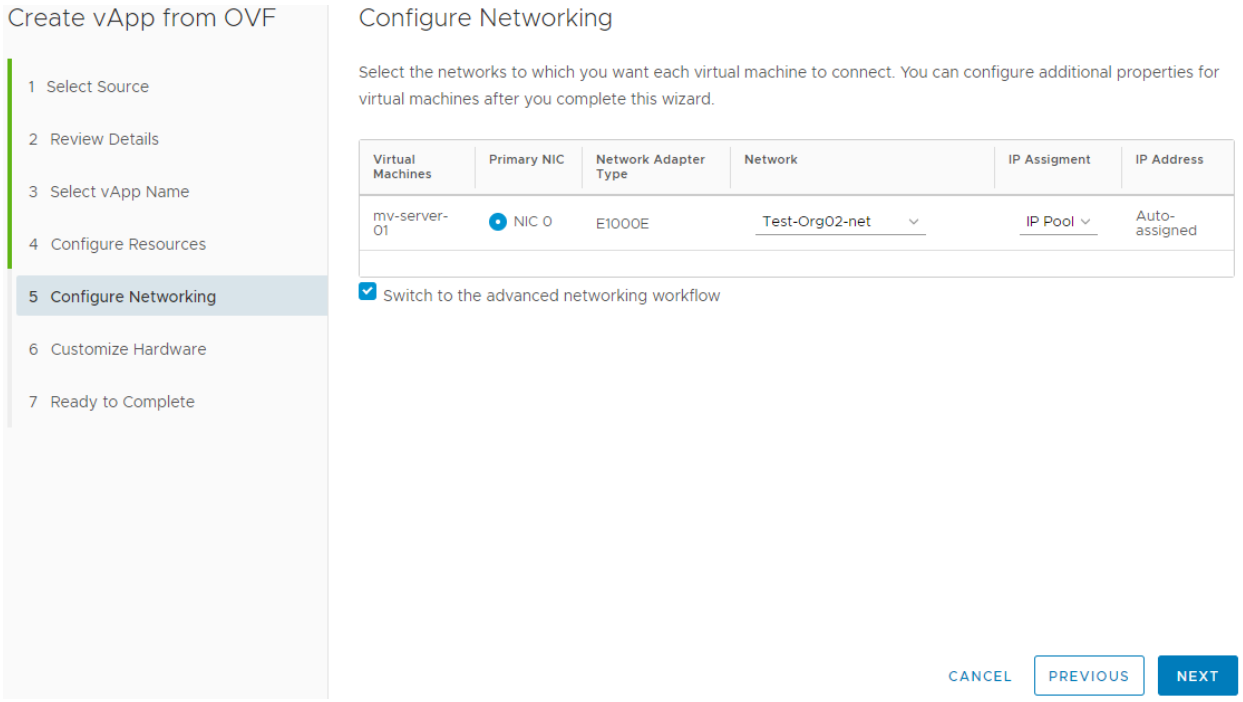


V dalším okně vyberte síť pro danný virtuál (virtuály) při je možno zobrazit rozšířený pohled. (Switch to the advanced networking workflow).

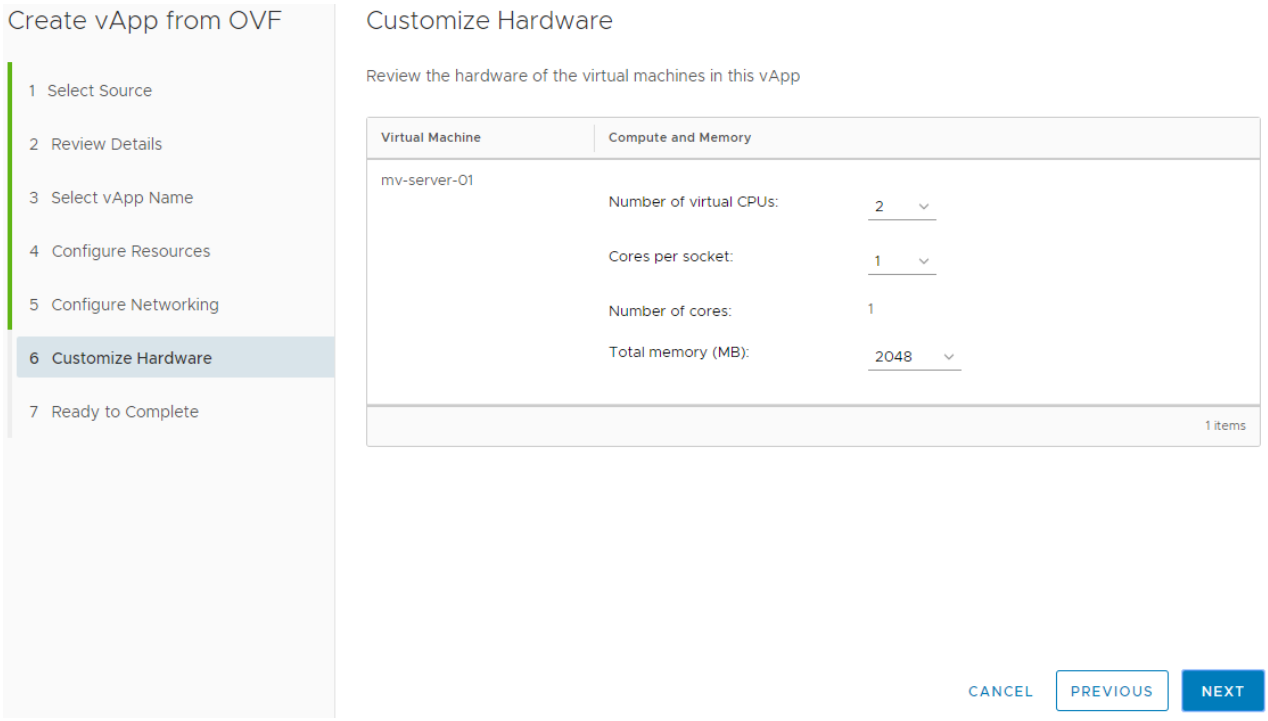
Dále zvolte síť (sítě, pokud má vmko více adaptérů) v organizaci, do které má být virtuální server připojen.

V případě že při výběru nebude možno změnit typ síťového adaptéru na VMXNET3, tak po vytvoření vAppy doporučujeme přejít do vlastností serveru (ACTIONS na kartě serveru a zvolit General) a v sekci sítě změnit typ adaptéru na VMXNET3). Tento adaptér komunikuje rychlostí 10 Gbps v případě že jsou na serveru nainstalovány VMware Tools, které doporučujeme a musí být na serveru nainstalovány za účelem instalace virtuálních ovladačů a efektivního využití virtuální platformy. Síťový adaptér E1000 komunikuje „Jen“ rychlostí 1 Gbps.

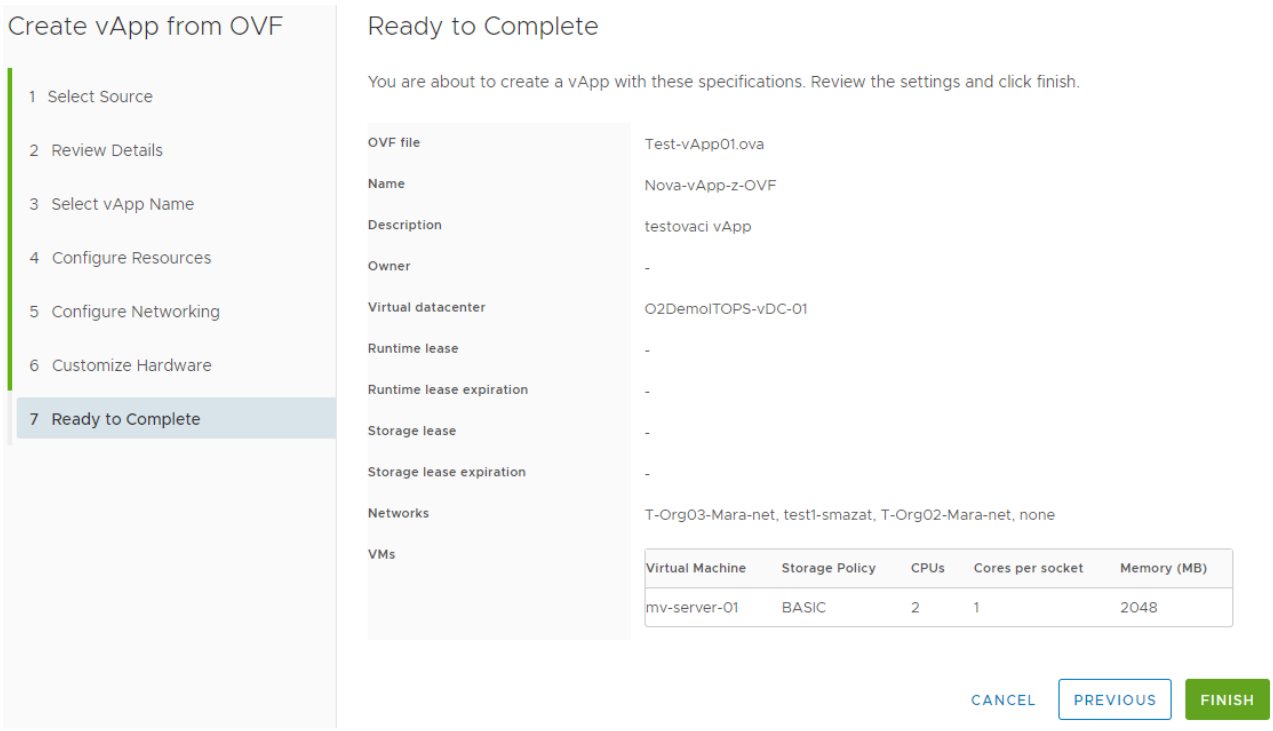
Dále zvolte způsob adresace (IP Assigment):
DHCP – přidělí IP adresu z DHCP. DHCP musí být nastaveno na EdgeGW
IP pool – přidělí + 1 volnou IP adresu se zvolené sítě – **tato volba je DOPORUČENA**
Manual IP – umožňuje v rámci zvolené sítě specifikovat ručně IP adresu



V dalším kroku potvrďte nebo přenastavte výkonové parametry virtuálního serveru s ohledem na celkové parametry Vašeho virtuálního datového centra. (pokračujte na „**NEXT**“)



Tlačítkem „**FINISH**“ potvrdíte vytvoření vApp z OVF do Vaši organizace

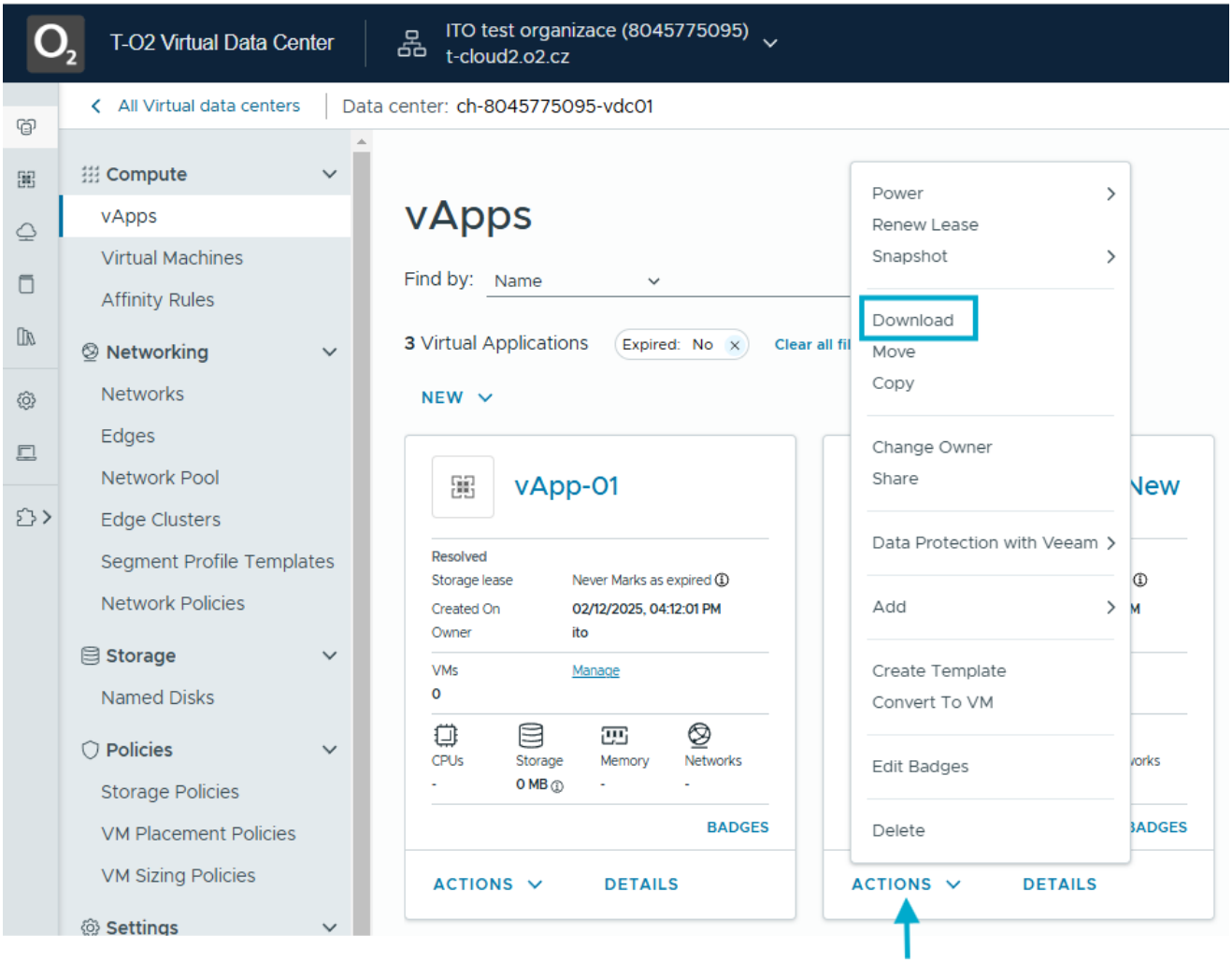


Tímto se vytvoří vApp z OVF

Pokud nastanou jakékoliv problémy s vytvořením vAppy z OVF (nebo z OVA), obraťte se na ServiceDesk nebo zadejte tiket a po té obdržíte přístupy na FTP, kam image nahrajte a my po té provedeme import.

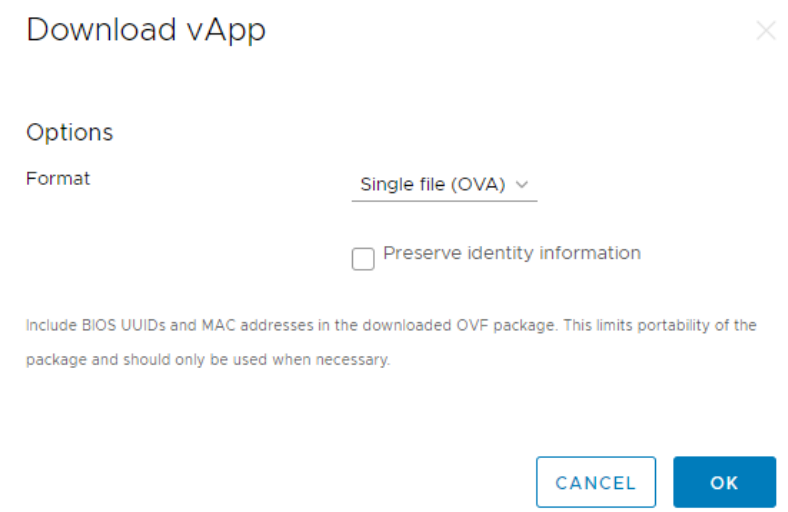
6.4 Stažení vAPP v OVF z organizace do lokálního počítače

Klikněte na „**ACTIONS**“ na kartě virtuálního serveru a vyberte Download

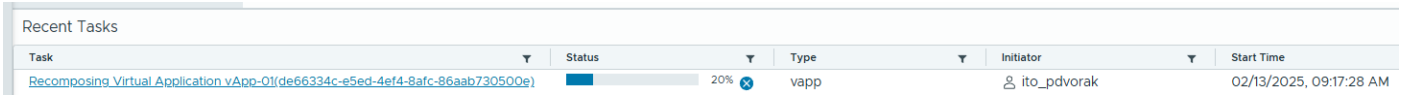


<u>vAppu (s VM servery, které jsou v dané vAppě), je možné stáhnout pouze za vypnutého stavu. V opačném případě budete mít tlačítko Download zašedlé.</u>

V následujícím okně potvrďte tlačítkem „**OK**“ stažení vAppy



Povolení a příprava ke stažení se zobrazí dole v událostech vCentra

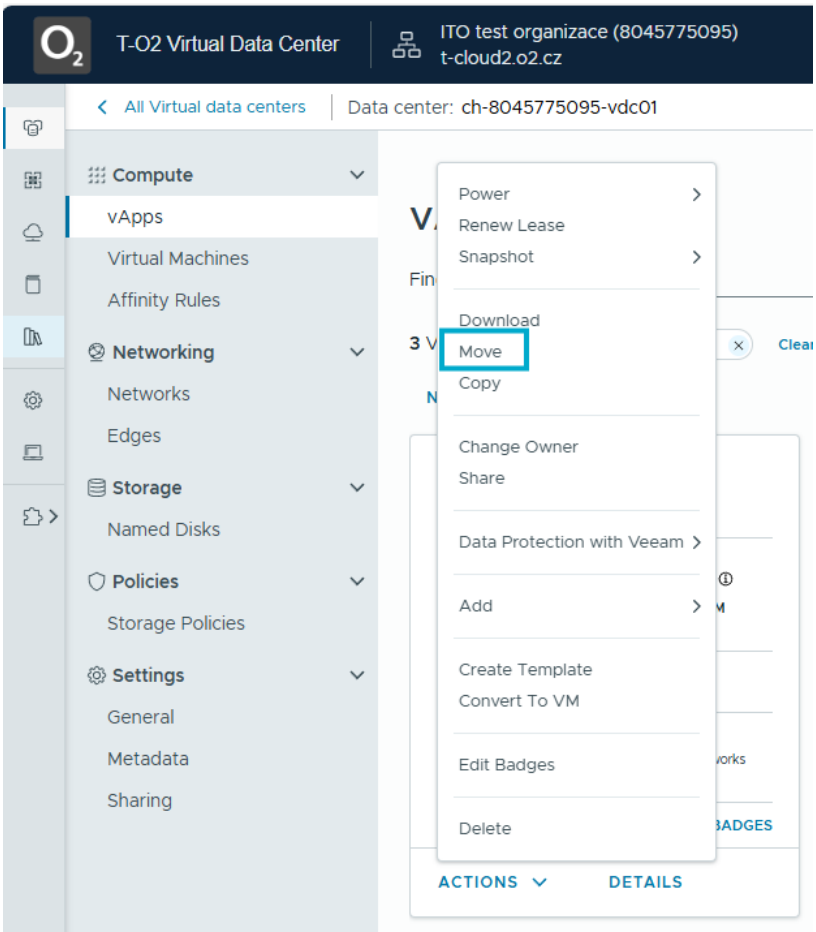


Po dokončení tasku se automaticky začne stahovat soubor k Vám do lokálního počítače (podle nastavení prohlížeče stahování začne automaticky do stažených souborů nebo budete dotázán kam se má soubor *.ova uložit).

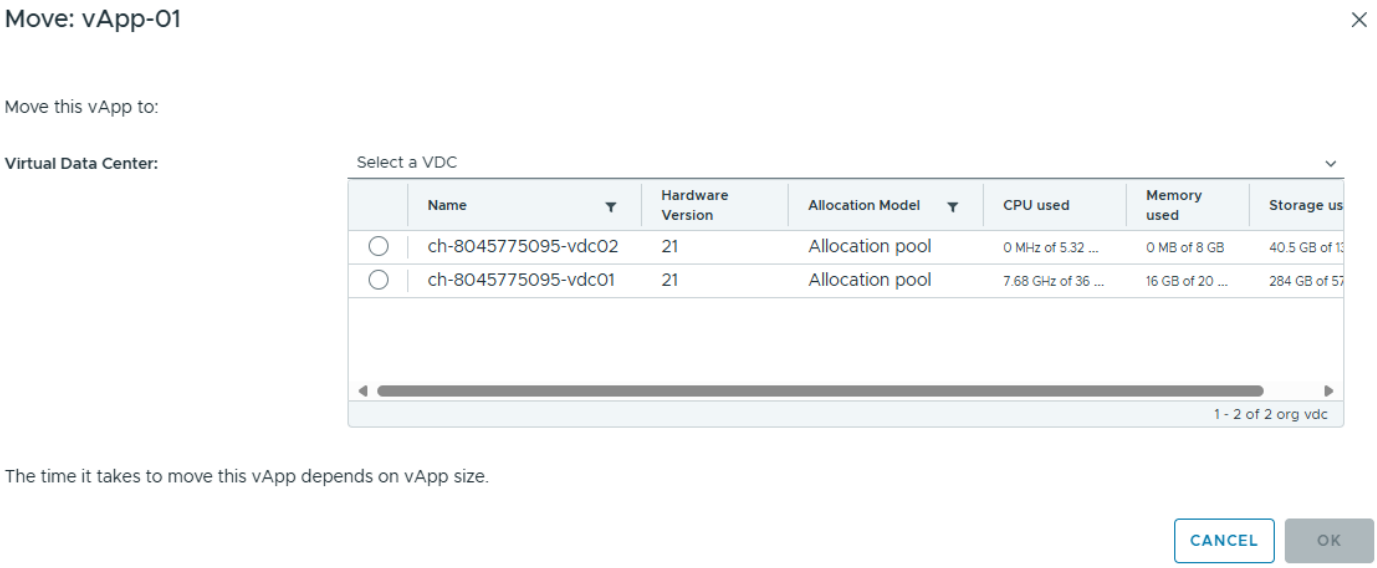
Tímto se provede stažení vAppy do lokálního počítače.

6.5 Přesun vAppy do jiného vDC

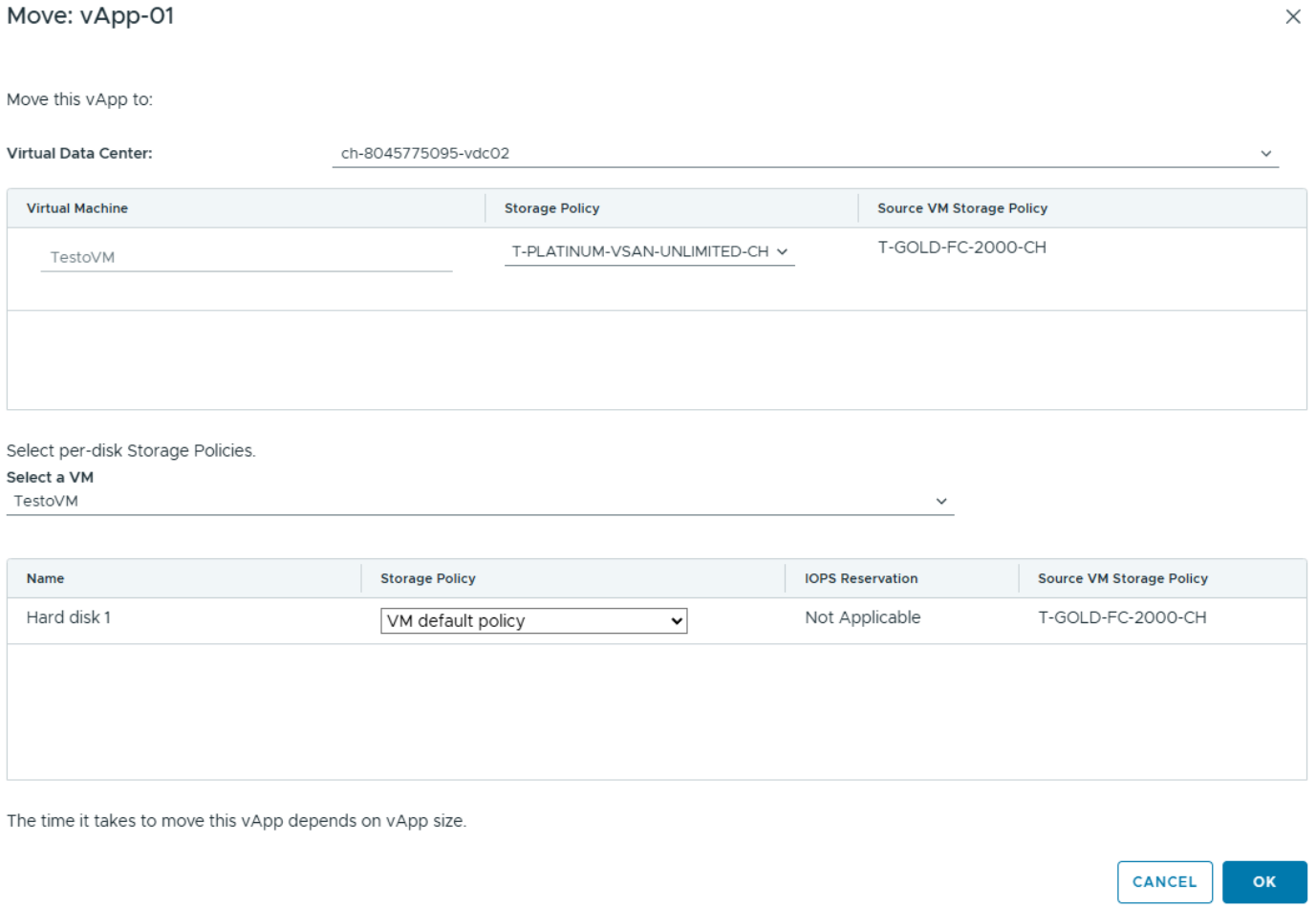
vAppu je možno přesunout, (pouze za vypnutého stavu) do jiného virtuálního datového centra kliknutím **z pohledu vApps** kliknout na **ACTIONS** a **Move**. V detailu vAppy je to možné provést i přes **ALL ACTIONS** a **MOVE**.



Vyberte **cílové vDC**



a **storage politiku** pro celé VM případně můžete každému disku přidělit politiku jinou



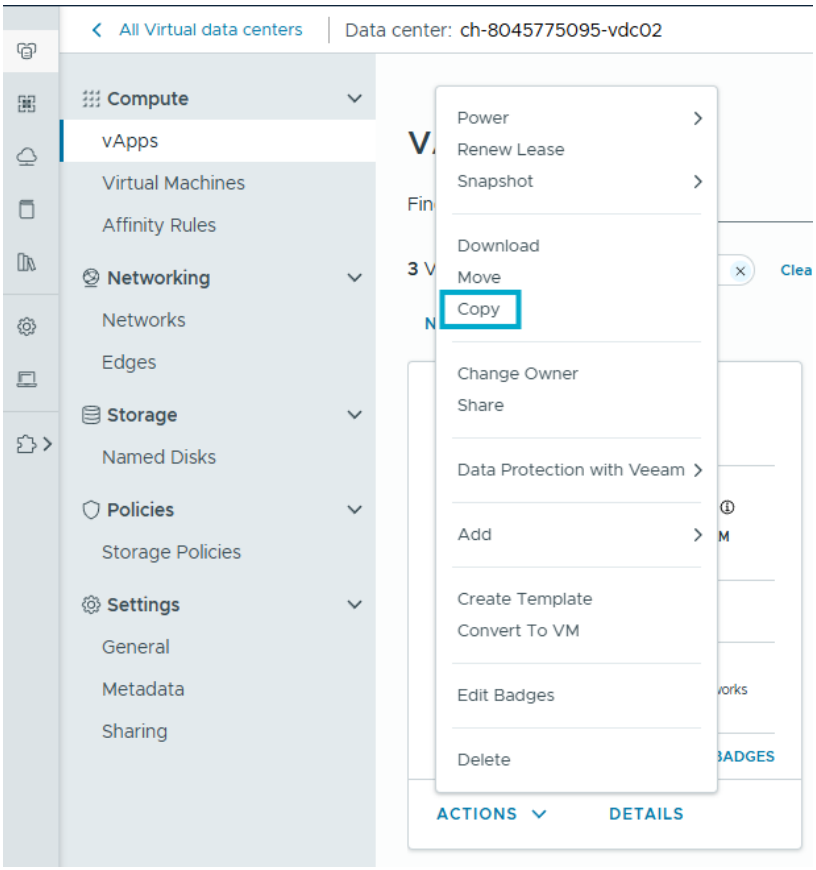
Potvrzením tlačítkem OK se spustí proces přesunu vAppy do jiného vDC.

(Přesun vAppy v rámci stejného datacenta není povoleno).

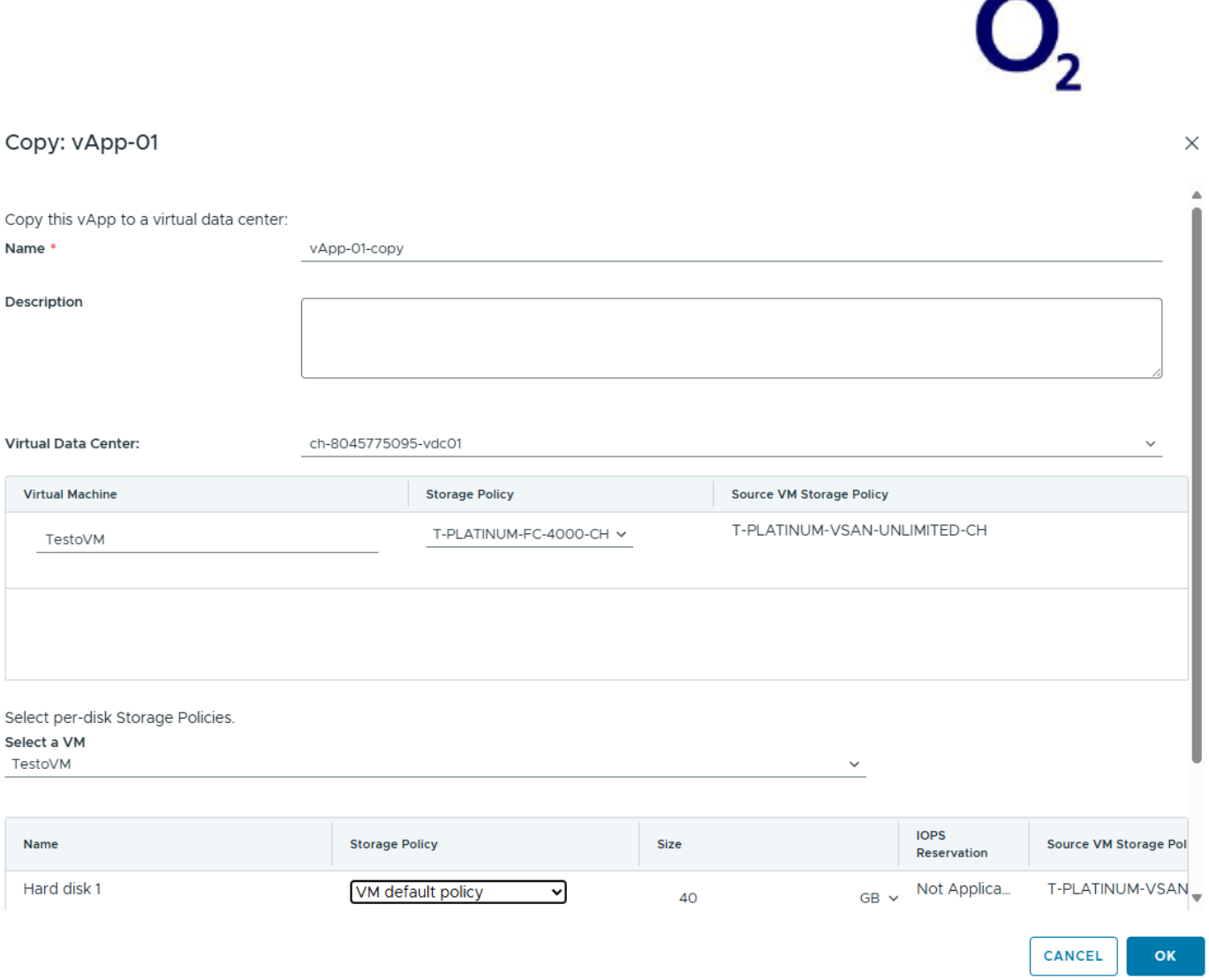
6.6 Clone vAppy do jiného vDC

vAppu je možno zklonovat, do stejného nebo jiného virtuálního datového centra kliknutím **z pohledu vApps** na **ACTIONS** a následně na **Copy**. V detailu vAppy je to možné provést i přes **ALL ACTIONS** a **COPY**.

To je možné provést pouze za vypnutého stavu vAppy. Za zapnutého stavu je „Copy“ zašedlé.



Zvolte **název vAppy** a **storage politiky pro jednotlivá VM** **a potvrďte OK.**



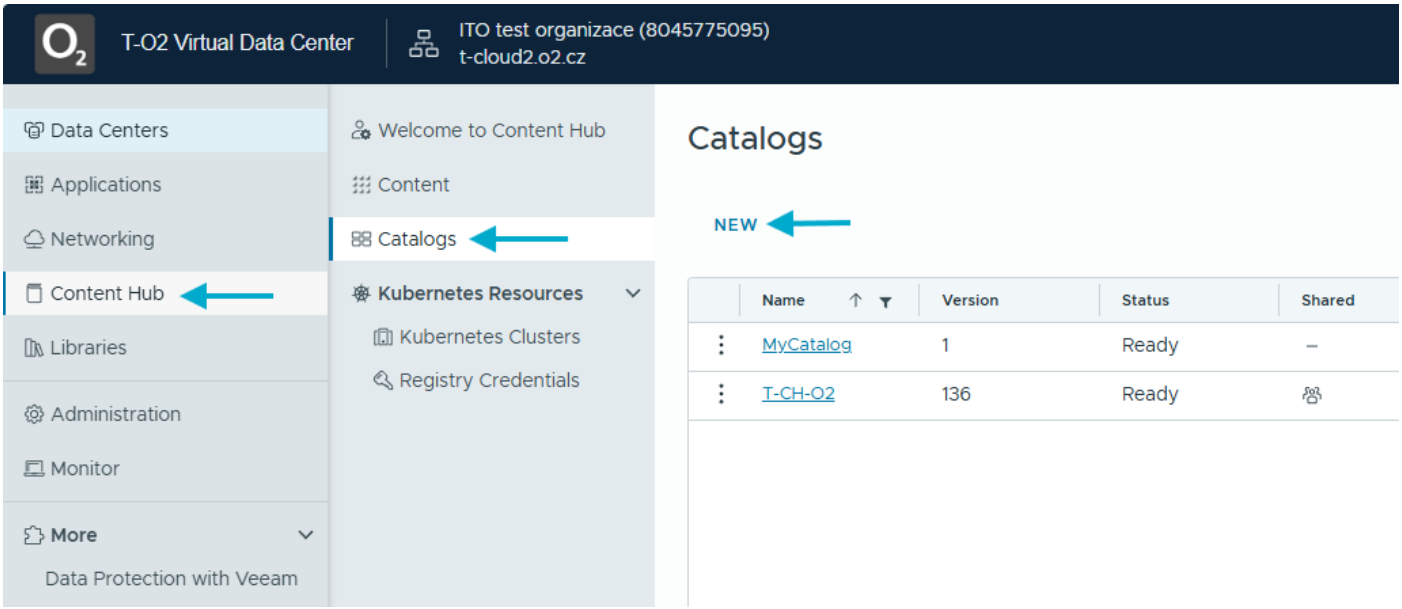
Zklonované servery mají SHODNOU MAC jako původní servery. **Je nutno před zapnutím VM serveru změnit MAC v detailu VM, kliknout na NIC a provést reset. Následně změnit i IP adresu.**

(V prostředí nelze spustit dva virtuální servery se shodnou MAC a IP adresou – kolize MAC/IP adres).

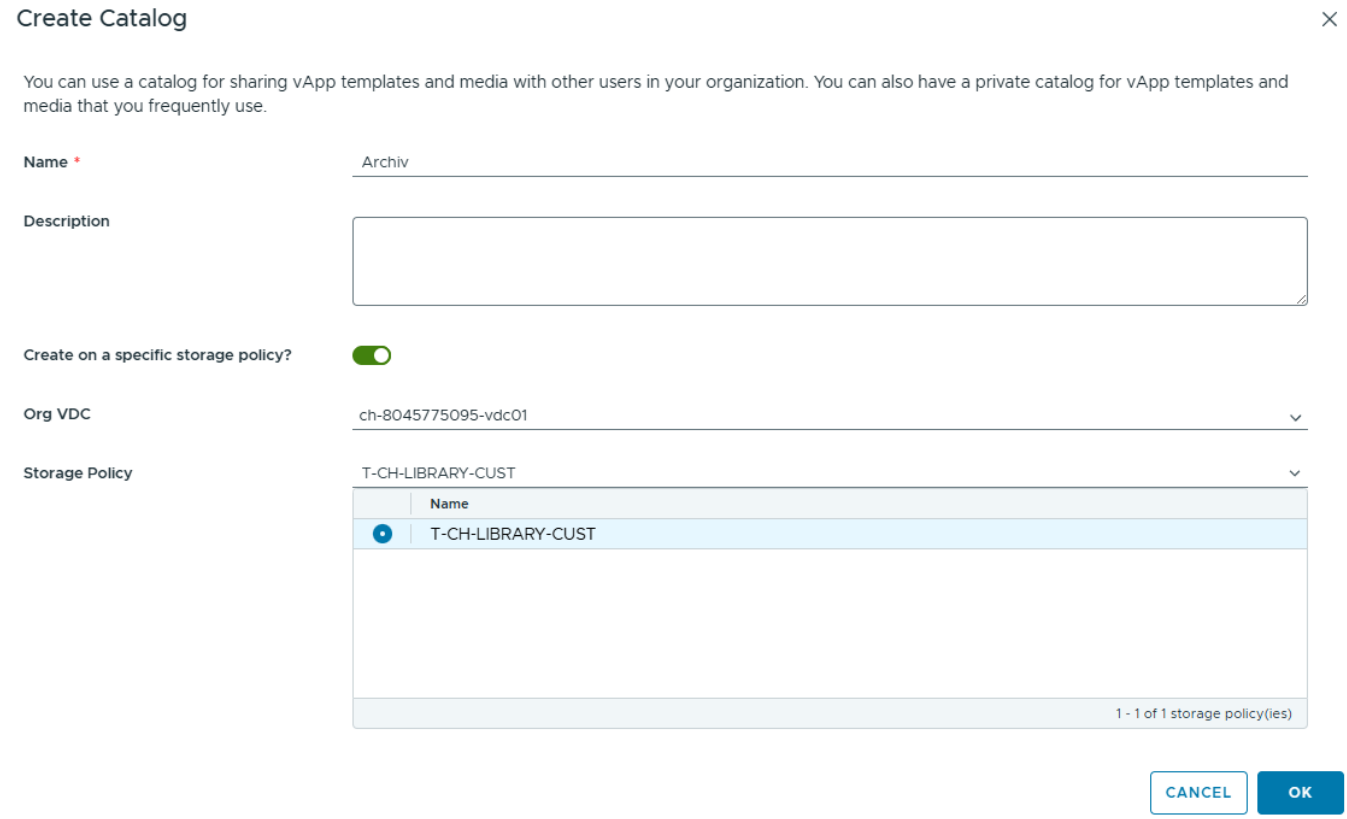
Tím se provedl clone vAppy.

7 Vytvoření katalogu

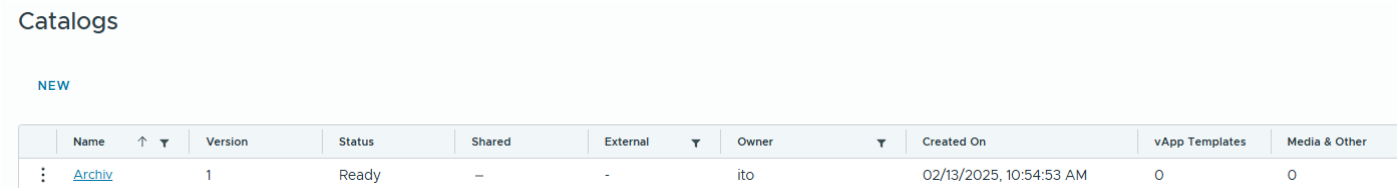
- Vytvořte katalog pro import ISO image – katalogů můžete vytvořit libovolné množství a rozdělit je podle potřeb a použití, nebo můžete vytvořit jeden katalog pro všechny Vaše **Image** a **template (šablony)**.
- Klikněte v portálu v levé nabídce na **Content Hub, poté na Catalogs a poté na NEW**.



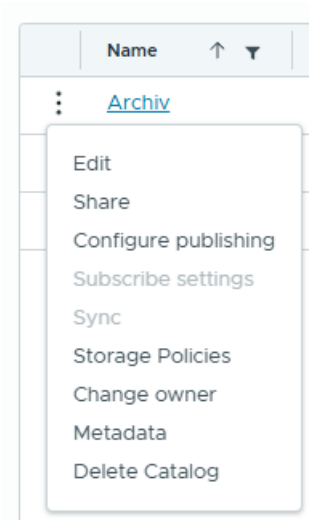
Následně vyplňte název katalogu, popis katalogu. Aktivací přepínače „Create on a specific storage policy“ můžete zvolit vDC, na kterém má být umístěný katalog. Výchozí úložiště pro katalogy je NFS úložiště „*-LIBRARY-CUST“



Následně se katalog vytvoří a je dostupný v přehledu ostatních.



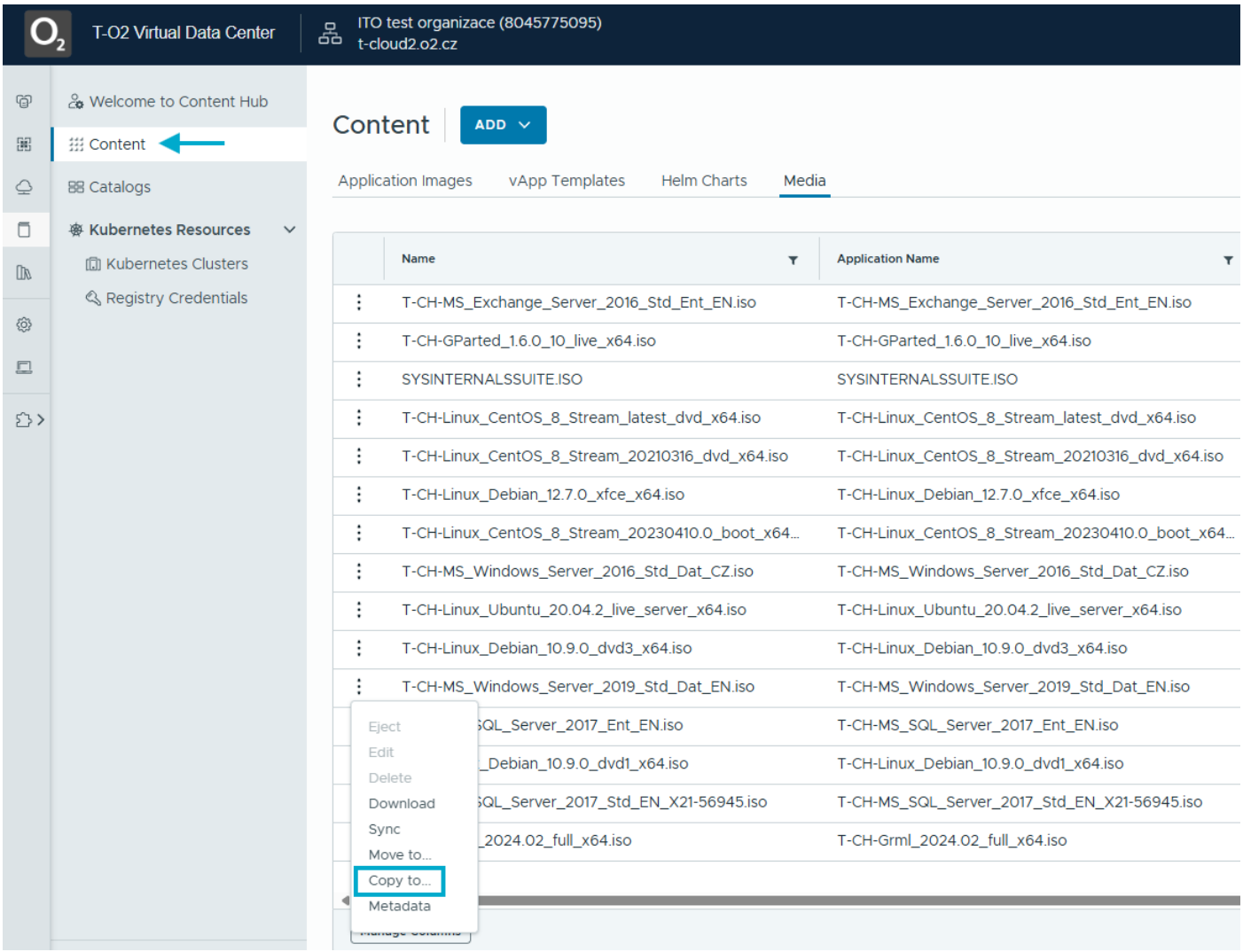
U katalogu je možno upravovat další vlastnosti kliknutím na



Edit – Editace katalogu – umožňuje upravit název a popis
Delete Catalog– smaže katalog
Configure publishing– publikace katalogu
Subscribe settings – není možno použít
Share - sdílení katalogu mezi uživateli a skupinami a přidělování oprávnění (Read Only, Change, Full Control)
Metadata - nepoužívat
Sync - nelze použít
Storage Policies - umožňuje změnit uložení katalogu na NFS úložiště „*-LIBRARY-CUST“ v jiném vDC

V prostředí Cloudu jsou dostupné 2 veřejné catalogy **JZ-O2** a **CH-O2**. Tyto katalogy obsahují jak **vApp Templates (vApp šablony) tak i Media (média – iso soubory)**.

Veřejné vApp templaty a ISO soubory ze sdíleného katalogu je možno překopírovat do vašeho katalogu v organizaci prostřednictvím volby Content -> vApp Templates nebo Media -> „Copy To“.



7.1 Import vlastního ISO image nebo šablony

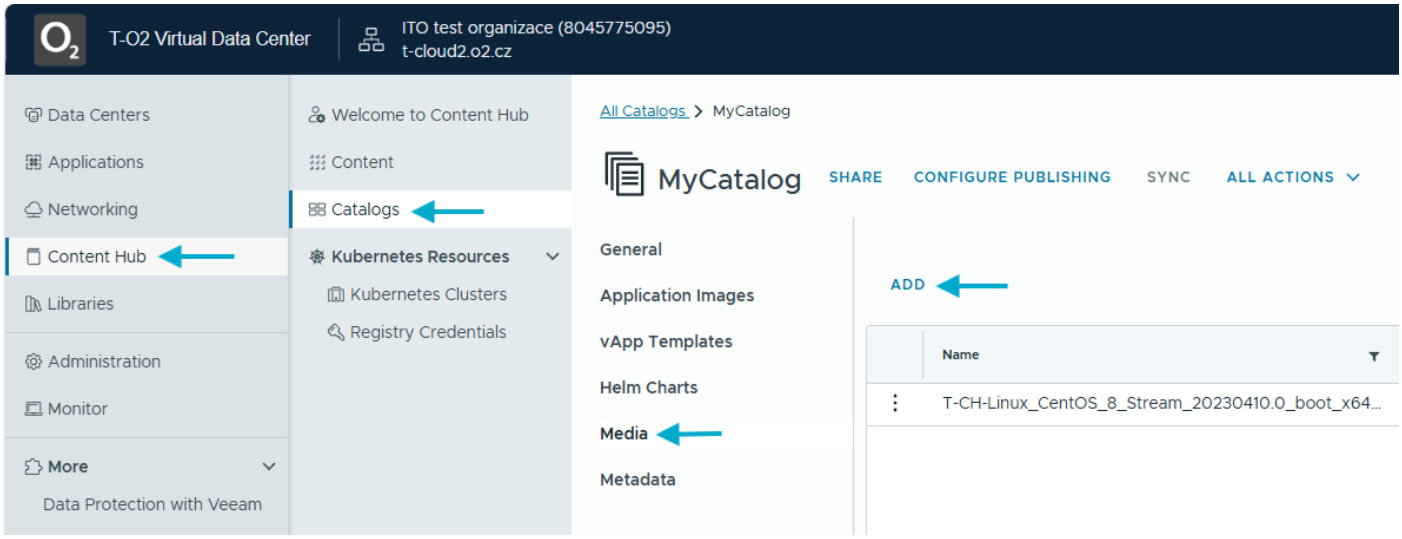
- Importujte ISO image nebo šablony do připraveného katalogu
  - Vlastní
  - Ze sdíleného katalogu
- Vyberte vytvořený katalog nebo katalog kam chcete importovat image a záložku – Template, nebo Media
- Vyberte „Upload“
- Vyberte ISO, které chcete importovat
- Upravte název a popis
- Nastavte požadovaný katalog
- Klikněte na „Upload“ – následně budete vyzvání k potvrzení, zda chcete opravdu danou operaci provést. Po potvrzení se provede nakopírování ISO do připraveného a nastaveného katalogu.

POZOR!: Rychlost je přímo úměrná rychlosti Vašeho připojení a to zejména v hodnotě UPLOAD.

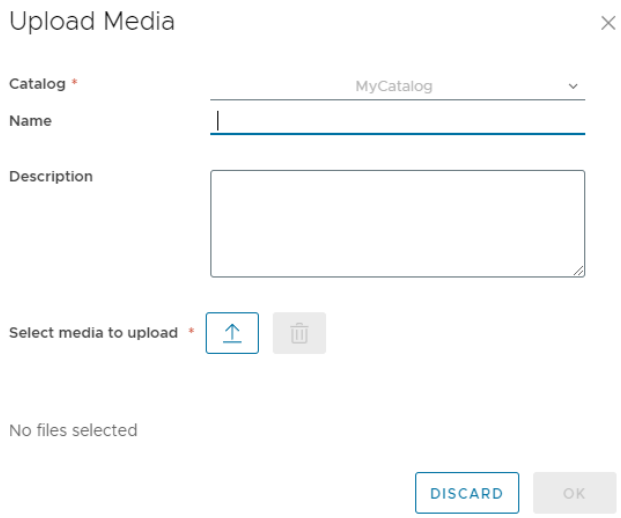
Nejprve povolte komunikaci protokolu https.

- Přejděte na Content Hub, v levém sloupci kliknout na Catalogs, vyberte Váš katalog, zvolte Media

- Klikněte na „**ADD**“



- Vyberte Catalog ve vaši organizaci
- Vyberte ISO z lokálního počítače, které chcete nahrát do katalogu
- Potvrďte OK



ISO bude po nahrání k dispozici v katalogu a lze ho připojit virtuálnímu serveru.

8 Limity virtuálního serveru

Limit vCPU

Maximální počet vCPU pro virtuální server ve standardním vDC (mimo službu SQLaaS) je 18.

Maximální počet vCPU pro virtuální server v SQLaaS vDC je 4.

Limit paměti

Maximální velikost paměti pro virtuální server ve standardním vDC (mimo SQLaaS) je 192 GB.

Maximální velikost paměti pro virtuální server v SQLaaS vDC je 64 GB.

Limit disku

Maximální velikost jednoho disku virtuálního serveru ve standardním vDC (mimo SQLaaS) je 6,5 TB.

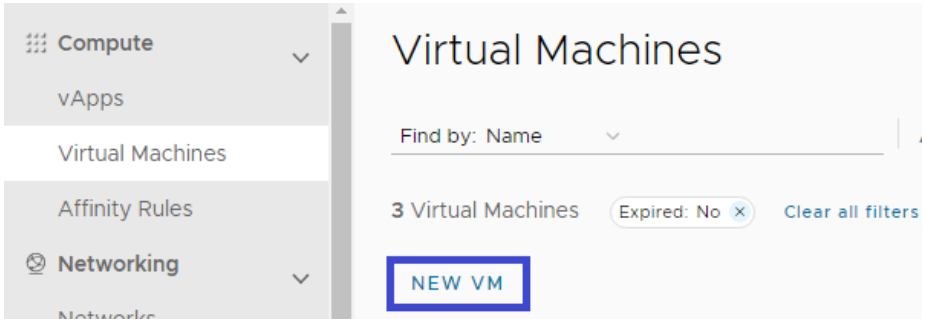
Maximální velikost jednoho disku virtuálního serveru v SQLaaS vDC Cloudu je 6,5 TB.

9 Vytvoření virtuálního serveru

- Virtuální server je možné vytvořit dvěma způsoby:
  - Z katalogu – vlastního, nebo sdíleného
  - Vytvoření nového serveru bez použití katalogu

9.1 Vytvoření nového serveru bez použití katalogu

- v levém sloupci klikněte na „**Virtual Machines**“ a následně klikněte na „**NEW VM**“



Následně se zobrazí formulář pro vytvoření serveru, viz obrázek níže:

NEW VM

- **Name** – Pojmenujte nový virtuální stroj.
- **Computer Name** – jméno pro O.S.
- **Description** – Do popisu popište účel virtuálního stroje
- **Type** – vyberte v tomto případě New (virtuál ze šablony bude popsáno níže)
- **Power on** – zapnutí virtuálního serveru po vytvoření

Operating System

- **Guest OS family** – Vyberte platformu OS, který bude nainstalován na tomto virtuálním stroji:
  - Microsoft Windows
  - Linux
  - Other
- **Guest OS** – ze seznamu vyberte **co nejpřesněji** OS, který bude nainstalován na virtuální stroj. V případě, že nebude OS v seznamu plně odpovídat, zvolte nejbližší podobný nebo zvolte volbu „ostatní“
- **Boot image** – nastavení bootovací image

Boot Options

- **Boot Firmware** – EFI nebo BIOS
- **EFI Secure Boot** – lze aktivovat
- **Enter Boot Setup** – pokud je aktivováno, po spuštění VM nabootuje do BIOSu

COMPUTE

- **CPU** – počet vCPU virtuálního serveru

Limity:

Maximální počet vCPU pro virtuální server ve standardním (mimo službu SQLaaS) Cloudu je 18.

Maximální počet vCPU pro virtuální server v SQLaaS vDC Cloudu je 4.

- **Cores per socket** – počet jader na jeden socket
- **Memory** – velikost paměti – **POZOR!**

Limity:

Maximální velikost paměti pro virtuální server ve standardním (mimo službu SQLaaS) Cloudu je 192 GB.

Maximální velikost paměti pro virtuální server v SQLaaS vDC Cloudu je 64 GB.

  - Paměť reprezentuje soubor uložený na datastoru, je tedy nutné mít ve vDC uložiště s dostatkem kapacity. Příklad: virtuální server, který bude mít disk 100 GB a paměť 8 GB bude na uložišti zabírat 108 GB.
    POZOR! **Je třeba nastavit takovou hodnotu velikosti RAM, která nanejvýš odpovídá požadavku na celé přidělené prostředí vDC** – to jsou parametry které jste požadovali a následně si objednali
    V případě, že nastavíte větší velikost, virtuální stroj nelze spustit Dále je také potřeba počítat s několikaprocentní režijí prostředí, proto bývá obvykle smlouvou každému VDC přiděleno více zdrojů než kolik vaše systémy reálně vyžadují.
- **Storage** – uložiště virtuálního serveru
  - **Storage policy** – vyberte Vaše uložiště v organizaci pro uložení disku virtuální serveru. Pokud ponecháte Storage policy „default“ uloží se disk na výchozí storage policy. Jaká výchozí storage policy je v organizaci nastavena zjistíte kliknutím na **Datacentrum**, v sekci **Policies** kliknout na **Storage Policies**, následně se v pravé části zobrazí dostupná uložiště, která jsou nastavena, včetně výchozího a i jejich kapacit – „**Allocation Used**“ = aktuálně využité místo, **Allocated** = Celková zakoupená kapacita uložiště.
  - **Size** – Specifikace velikosti disku v (GB)
  - (tlačítkem „**ADD**“ je možno přidat další HDD). Ikonkou koše je možno disk odebrat.
    Limity:
    - **POZOR! - Maximální velikost jednoho disku virtuálního serveru je 6,5 TB.**
    - POZOR! - **je nutné nastavit takovou hodnotu velikosti disku, která odpovídá požadavku na celé přidělené prostředí vDC** – to jsou parametry které jste požadovali a následně si objednali. V případě, že nastavíte větší velikost, virtuální stroj nespustíte! Dále je také potřeba počítat s režijí prostředí.

Poznámka: Pokud nezaškrtnete „**Use custom storage policy:**“, vytvoří se VM na defaultním storage tieru (tedy na defaultní storage policy)

- **Networking** – pro daný NIC vyberte v poli Network síť v organizaci a dále IP Mode (způsob adresace).

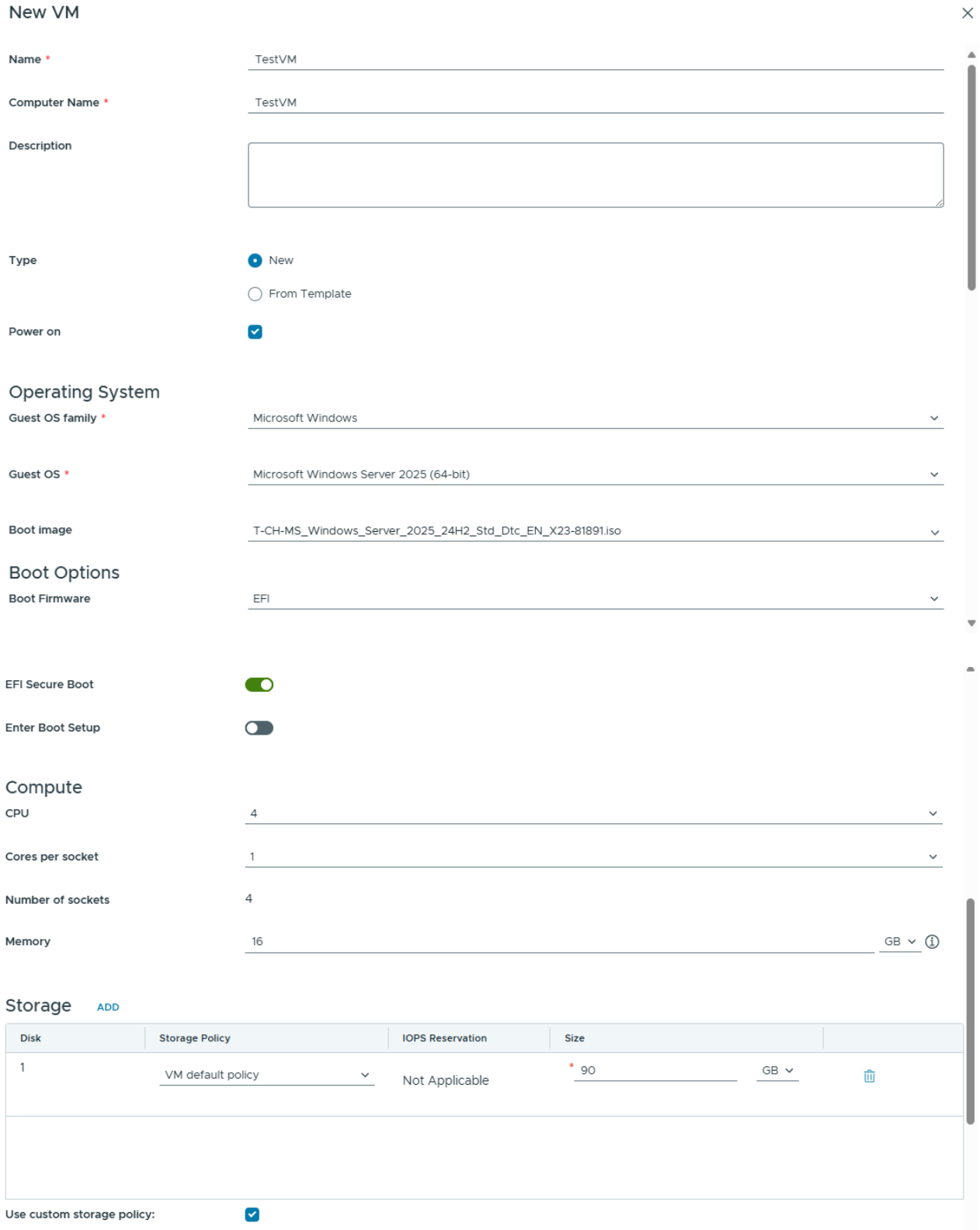
  - **IP Mode**:
    - **DHCP** – přidělí IP adresu z DHCP. DHCP musí být nastaveno na EdgeGW (většinou se nevyužívá)
    - **IP pool** – přidělí + 1 volnou IP adresu se zvolené sítě – **tato volba je DOPORUČENA**
    - **Manual IP** – umožňuje v rámci zvolené sítě specifikovat ručně IP adresu

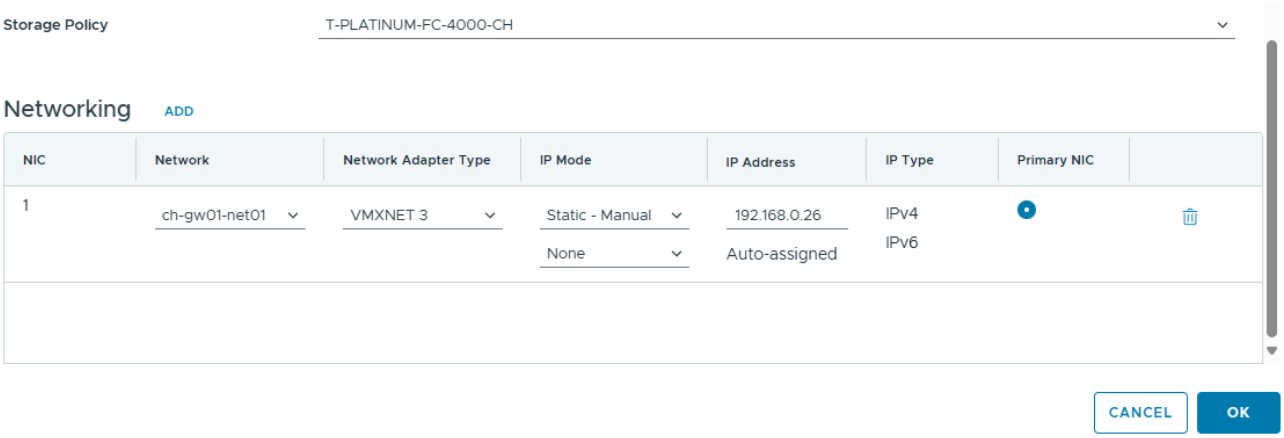
Vytvoření serveru potvrďte tlačítkem „OK“.

Důležité:

Pokud server vytváří O2 nebo O2ITS, po předání serveru VŽDY z důvodu bezpečnosti změňte předaná hesla všech vytvořených účtů.

Příklad vyplněného formuláře s parametry pro vytvoření virtuálního serveru z ISO souboru





Vytvoření serveru je následně provedeno. **Při vytvoření nelze specifikovat konkrétní vAppu**. Server se vytvoří bez vAppy. Virtuální server je možno přesunout do konkrétní vAppy kliknutím u virtuálního serveru na **ALL ACTIONS** a volbou „**Move**“.

9.2 Doporučené dodatečné nastavení virtuálního serveru

Po vytvoření virtuálního serveru doporučujeme provést námi doporučenou konfiguraci virtuálu:

9.2.1 Instalace VMware Tools

Doporučené nastavení: mít nainstalované a aktualizované VMware Tools na virtuálním serveru.

Klikněte na kartě virtuálního serveru na „**ALL ACTIONS“** a zvolte „**Install VMware Tools**“.

(V případě OS Linux lze použít Open-VM-Tools).

Instalátor VMware Tools je připojen do DC/DVD mechaniky a tím je možno instalaci provést v nastavení typical.

Po instalaci bude vyžadován restart serveru, po updatu – aktualizaci může být vyžadován.

Jedná se o virtuální ovladače a nástroje, které zajistí ve virtuálním serveru efektivní využití virtuální platformy. Absence VMware Tools může způsobit nefunkční síťové připojení serveru (chybějící síťová karta). Součástí VMware Tools jsou i ovladače pro síťovou kartu VMXNET3.

9.2.2 Nastavení pojmenování virtuálního serveru v tenant portálu a v operačním systému (OS)

Doporučené nastavení: shodné nastavení pojmenování virtuálního serveru jak v tenant portálu tak v OS.

Virtuální server doporučujeme mít shodně pojmenovaný tak že souhlasí název serveru v tenant portálu, konkrétně v poli „**Computer Name**“ na kartě virtuálního serveru, „**DETAILS**“ v sekci „**General**“– hostname OS v **OS** s názvem. (VMware hostname – vmware název může být shodný nebo odlišný od názvu v OS).

9.2.3 Nastavení IP adresy virtuálního serveru v tenant portálu a v operačním systému

Doporučené nastavení: shodné nastavení IP adresy virtuálního serveru jak v tenant portálu tak v OS.

Virtuální server doporučujeme mít shodně nastaven tak, že souhlasí nastavená IP adresa v tenant portálu, konkrétně v poli „IP Address“ na kartě virtuálního serveru v sekci „**NICs**“ s IP adresou v OS.

9.2.4 Nastavení síťového adaptéru VMXNET3 na virtuálním serveru

Doporučené nastavení: na serveru doporučujeme používat síťový adaptér VMXNET3.

Na serveru doporučujeme mít nastaven typ síťového adaptéru VMXNET3. Síťový adaptér **VMXNET3** umožňuje komunikovat rychlostí **10Gbps**, zatímco síťový adaptér **E1000 „pouze" 1Gbps**.

V případě že virtuální server má více síťových adaptérů, tak doporučujeme **mít u všech shodný typ**, tedy **VMXNET3**.
Síťový adaptér lze měnit zatím pouze z portálu vCloud Director ve vlastnostech virtuálního serveru, záložka Hardware -> NICs -> Network adapter Type.Typ síťového adaptéru nelze měnit za běhu serveru, server se musí vypnout, stávající síťový adaptér odebrat a přidat nový síťový adaptér typu VMXNET3.

Propustnost síťového adaptéru významně ovlivňuje i rychlost zálohování přes síťové rozhraní, proto doporučujeme použít typ síť. Adaptéru VMXNET3 = 10 Gbps.

(Síťový adaptér E1000 má jen propustnost 1 Gbps).

9.2.5 Nastavení disků virtuálního serveru

Doporučené nastavení: pro každý oddíl separátní disk.

V případě, že virtuální server má mít více disků tak doporučujeme mít pro každý oddíl separátní disk. Je to z toho důvodu, aby bylo možno jednoduše navyšovat kapacity jednotlivých disků bez ohledu na umístění jednotlivých oddílů v O.S., které nelze za určitých podmínek vždy navýšit.

POZOR! – zmenšování virtuálních disků není možné a není podporováno.

9.2.6 Ověření, že je vypnuta Guest Customizace

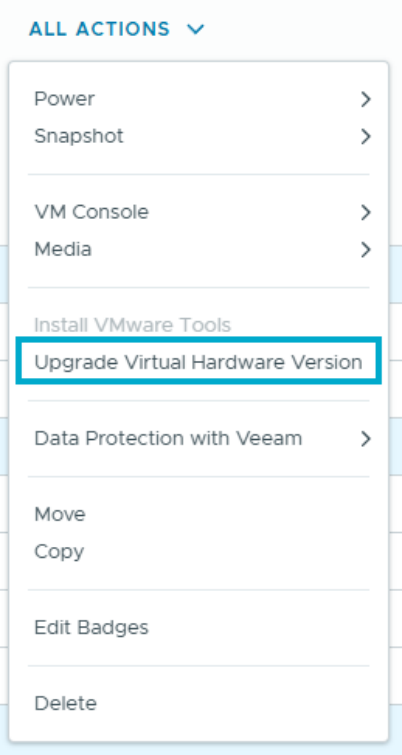
Doporučené nastavení: nezapínat na virtuálním serveru funkci „Guest Customization". Po deploy VM je potřeba ji vždy vypnout. Customizace v případě OS Windows 2025 trvá 15 – 20 minut, neprovádějte žádné změny a prosím vyčkejte.

K ověření tohoto nastavení kliknout na kartě virtuálního serveru na „**Guest OS Customization**" a ověřit, jestli jsou „odnastavené = odškrtnuté volby „**Change SID**" a „**Enable guest Customization**". Ve výchozím nastavení je tato volba zapnutá. Pokud je funkce zapnuta, provede se přepsání nastavení sítě a hodnoty v poli „**ComputerName**" do operačního systému. Pokud je ještě nastavena volba „**Change SID**" tak dojde v OS i ke změně SIDu. (Tato volba se používá zejména v případě instalaci většího počtu serverů a v případě, že je požadováno automaticky propsat nastavení jména počítače a sítě striktně do nového operačního systému serveru). Poté je i tak nutno ověřit, jestli obě volby jsou vypnuty, aby nedošlo v budoucnu k tomuto nastavení, **které by mohlo při změně jména, nastavení sítě a SIDu způsobit nefunkčnost serveru, odpojení z domény apod**.

9.2.7 Ověření, že je nastavena poslední dostupná HW verze virtuálního serveru

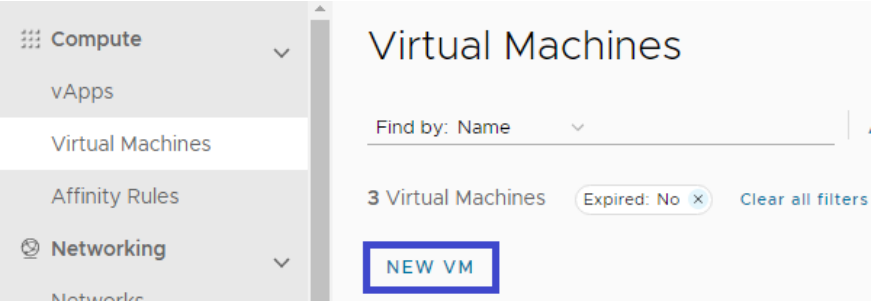
Doporučené nastavení: používat na serveru poslední HW verzi.

Upgrade HW verze serveru na poslední dostupnou. Tím bude zajištěno, že virtuální server bude využívat efektivně všechny možnosti virtuální platformy. Upgrade na HW verzi se provádí pouze za vypnutého stavu serveru. Update na vyšší HW verzi je možné zatím provést pouze z vCloud Directoru.



9.3 Vytvoření nového serveru z katalogu (z Templaty)

- v levém sloupci klikněte na „**Virtual Machines**“ a následně klikněte na „**NEW VM**“

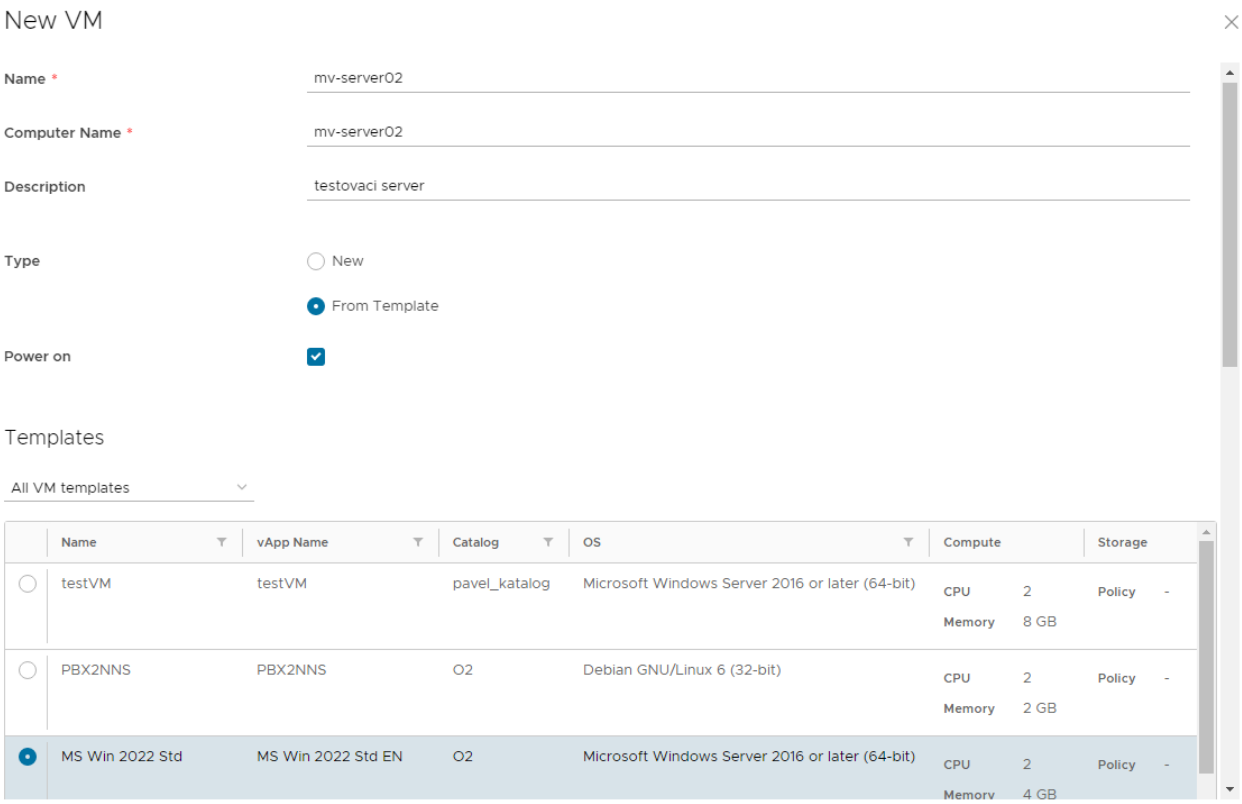


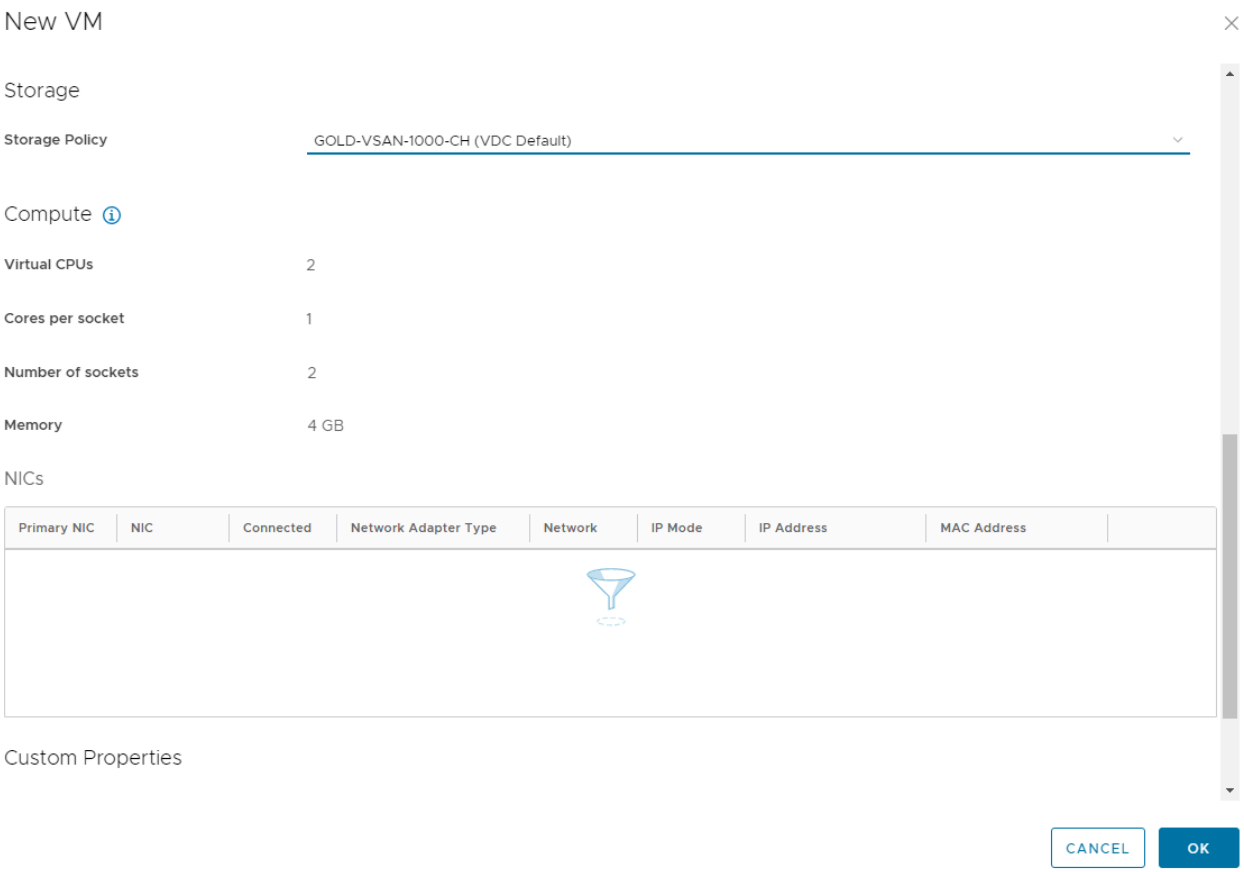
Následně se zobrazí formulář pro vytvoření serveru, viz obrázek níže:

- **Name** – pojmenujte nový virtuální stroj
- **Computer Name** – jméno pro OS
- **Description** – do popisu popište účel virtuálního stroje
- **Type** – zvolte „**From Template**“ (ze šablony)
- **Power on** – v případě že je zaškrtnuto, virtuální server se po vytvoření zapne
- **Templates** – v sekci Templates vyberte šablonu s verzí OS
- **Use custom storage policy** – zaškrtnutím této volby máte možnost uložit virtuální server na konkrétní uložiště v organizaci (používá se v případ, že v organizaci je více uložišť než jedno). Pokud není zaškrtnuto, uloží se na defaultní úložiště (storage tier)
  Tato možnost tak umožňuje v případě, že má organizace více uložišť zvolit například produkční servery na rychlé uložiště například na **PLATINUM-VSAN-UNLIMITED-JZ** (CH nebo JZ v názvu označuje lokalitu dané storage).

Vytvoření serveru potvrďte tlačítkem „OK“.

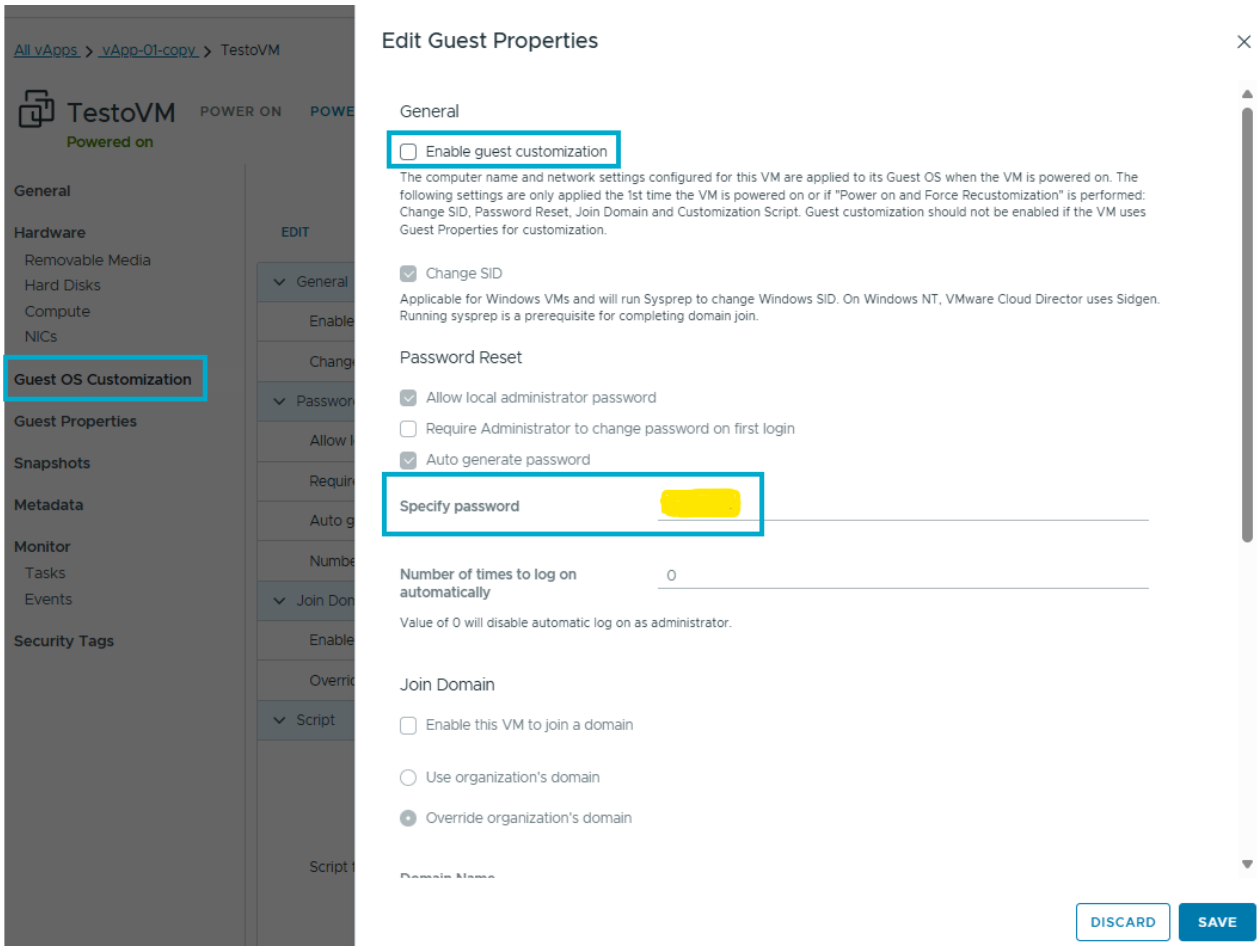
Důležité: Pokud server vytváří O2 nebo O2ITS, po předání serveru VŽDY u důvodu bezpečnosti změňte předaná hesla všech vytvořených účtů.



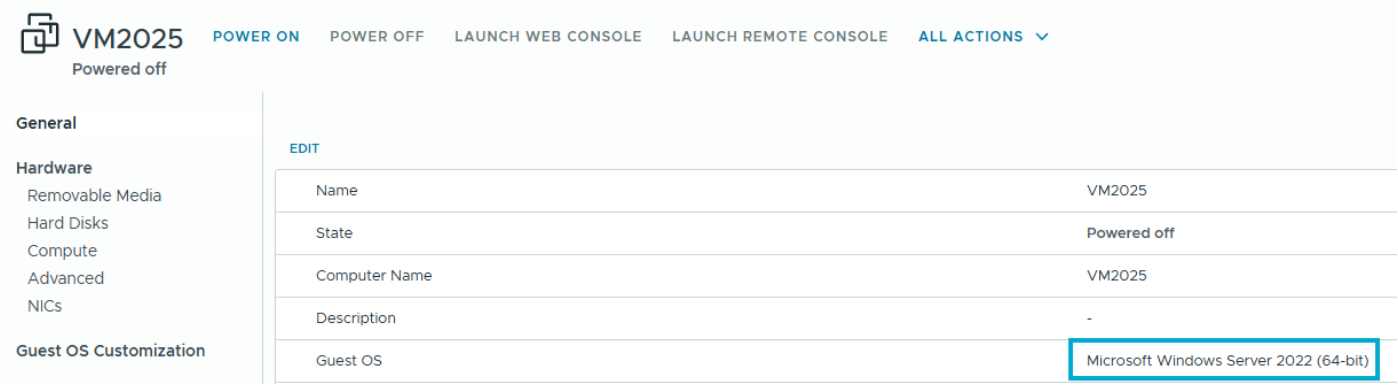


Vytvoření serveru je následně provedeno. Při vytvoření nelze specifikovat konkrétní vAppu. Server se vytvoří bez vAppy. Je možno jej přesunout do konkrétní vAppy kliknutím u virtuálního serveru na **ALL ACTIONS** a volbu **Move.** Případně můžete server vytvářet postupem přidání do existující vAppy, kdy vyberete vAppu -> ALL ACTIONS -> Add VM.

Pokud vytváříte nový server s **OS Windows Server 2022 nebo 2025 z templaty**, po dokončení deploy serveru a jeho zapnutí Vám **nabootuje na logon screen, na kterém bude systém vyžadovat změnu hesla pro lokální účet Administrator. Toto prosím ignorujte a vyčkejte. Customizace v případě OS s Windows 2025 trvá 15 – 20 minut, neprovádějte žádné změny a prosím vyčkejte** (dobu trvání customizace pro OS Windows 2025 nelze urychlit). Pro ostatní operační systémy (OS Windows 2016, Windows 2019 a Windows 2022) **proběhne OS Guest Customizace do cca do 2 minut a po té dojde k automatickému restartu VM.** Následně proběhne nastavení hesla pro účet Administrator z customizace. Přihlašte se do VM defaultním heslem z customizace viz obr. níže, následně si v OS heslo lokálního admin účtu změňte na vlastní a na závěr **customizaci VM v tenantu deaktivujte** (viz obr. níže).

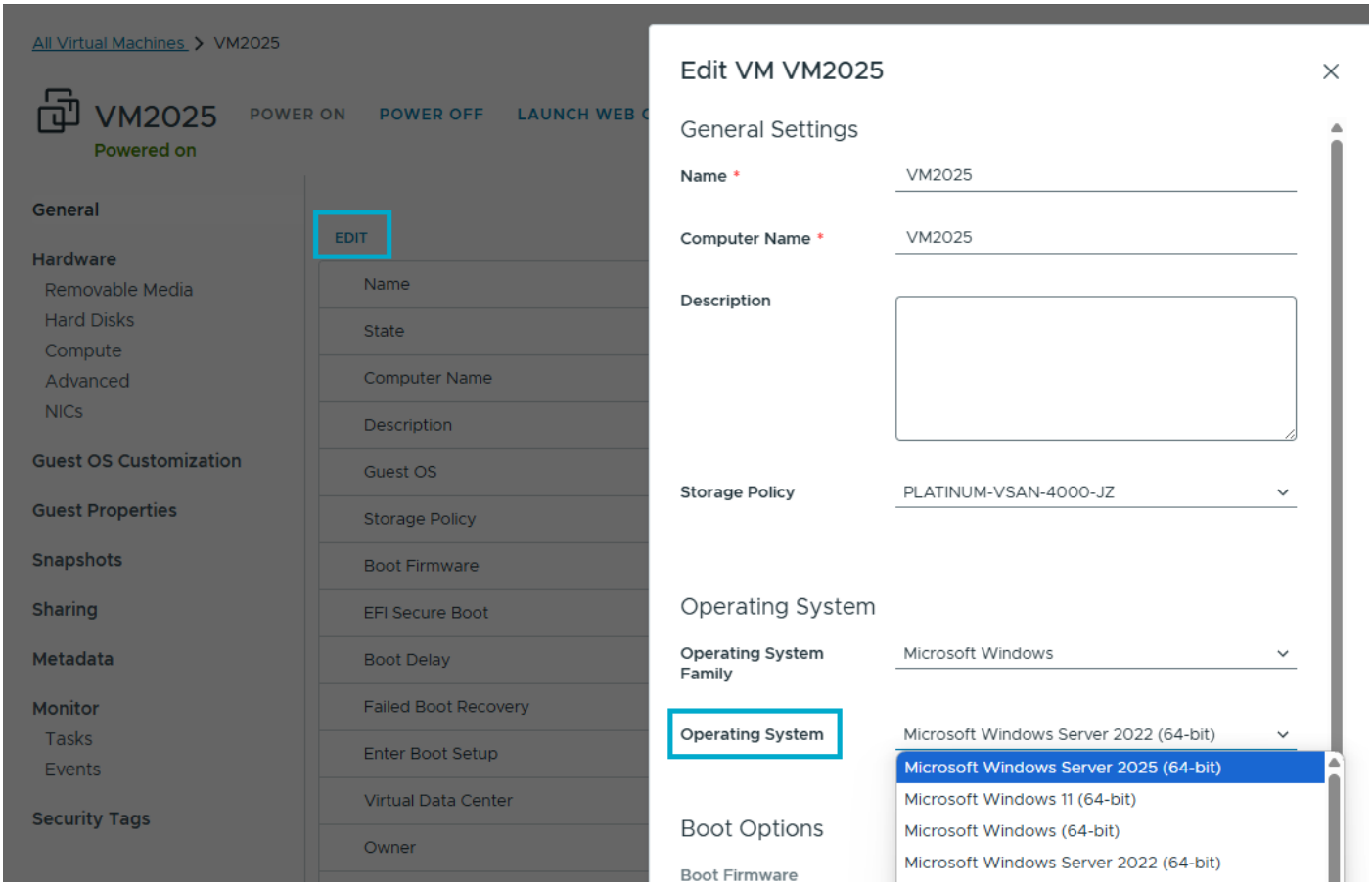


Pokud si vytvoříte nový VM z templaty s OS Window Server 2025, server se Vám vytvoří s Guest OS „Microsoft Windows Server 2022 (64-bit)“.



Je to z toho důvodu, aby se Vám při prvotním spuštění provedla customizace, tedy aby se Vám propsala IP adresa nastavená na serveru z vCD do konfigurace síťové karty v OS a aby se nastavilo defaultní heslo lokálního administrátora. Jakmile se do OS přihlásíte defaultním heslem lokálního administrátora z customizace a následně si jej změníte v OS na vlastní heslo, vypněte Guest customizaci dle obrázku výše, server vypněte a změňte verzi operačního systému z Microsoft Windows Server 2022 (64 bit) na Microsoft Windows Server 2025 (64 bit).

VM -> General -> EDIT -> Operating System



PO VYTVOŘENÍ VIRTUÁLNÍHO SERVERU ZE ŠABLONY PROVĚŘIT JEHO NASTAVENÍ TAK JAKO V PŘÍPADĚ VYTVOŘENÍ NOVÉHO VIRTUÁLNÍHO SERVERU.

VIZ KAPITOLA: 9.2 Doporučené dodatečné nastavení virtuálního serveru.

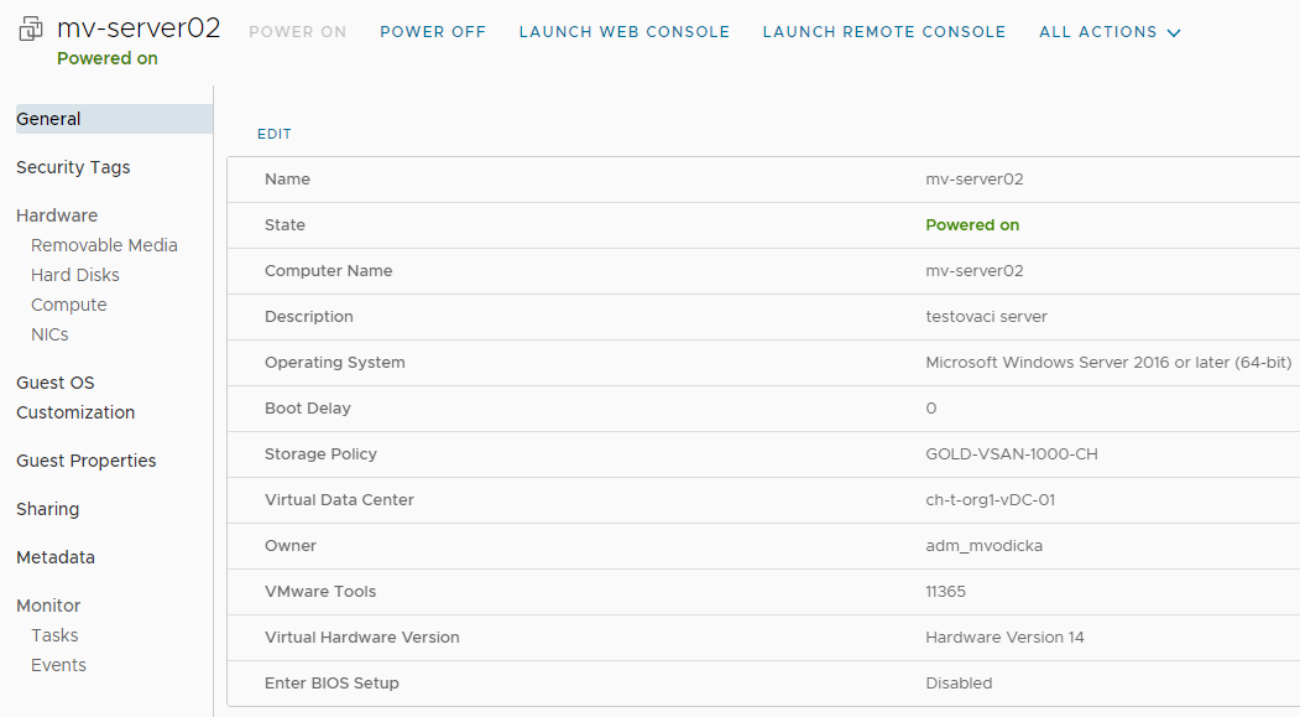
V sekci Hardware daného VM lze možno nastavit „**Memory hot add**“ (přidání paměti virtuálního serveru za běhu serveru) a „**Virtual CPU hot add**“. (přidání vCPU serveru za běhu virtuálního serveru). Doporučujeme ale tyto obě volby **nenastavovat**, neboť je vždy vhodnější virtuální server vypnout, provést navýšení a zapnout. Tyto volby umožňují pouze přidávat vCPU a paměť za běhu serveru a jsou funkční pouze tehdy pokud to daný OS podporuje a umožňují pouze přidávat nikoli odebírat vCPU a paměť serveru.

9.4 Pokročilá nastavení virtuálních serverů

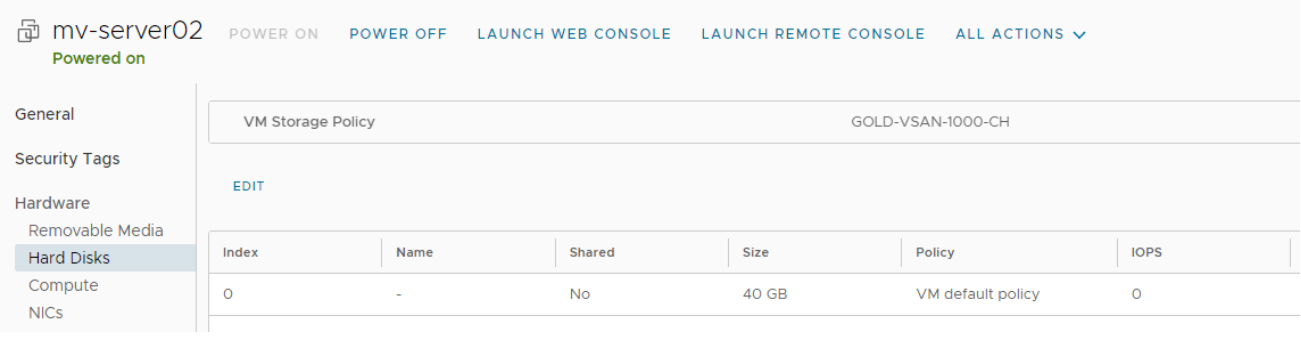
Pokud máte v rámci smlouvy zpřístupněn více jak jeden **Storage Tier**, lze u každého VMka daného OrgVDC definovat/změnit příslušný storage tier na úrovni VM disku (např.: disk0 = **SILVER** tier, disk1 = **GOLD** tier, disk2 = **PLATINUM** tier). Tato změna se provádí na záložce **General** a položka Storage Policy.“ Dále je možno měnit uložiště jednotlivých disků. Opět v záložce General, níže u každého disku je možno měnit Policy.

- Omezení: Pokud v daném storage Tier nemáte volnou diskovou kapacitu, nelze do ní VM umístit.
- **POZOR!** Změna storage tieru má vliv na výkonnost daného VM/disku

Storage policy virtuálního serveru



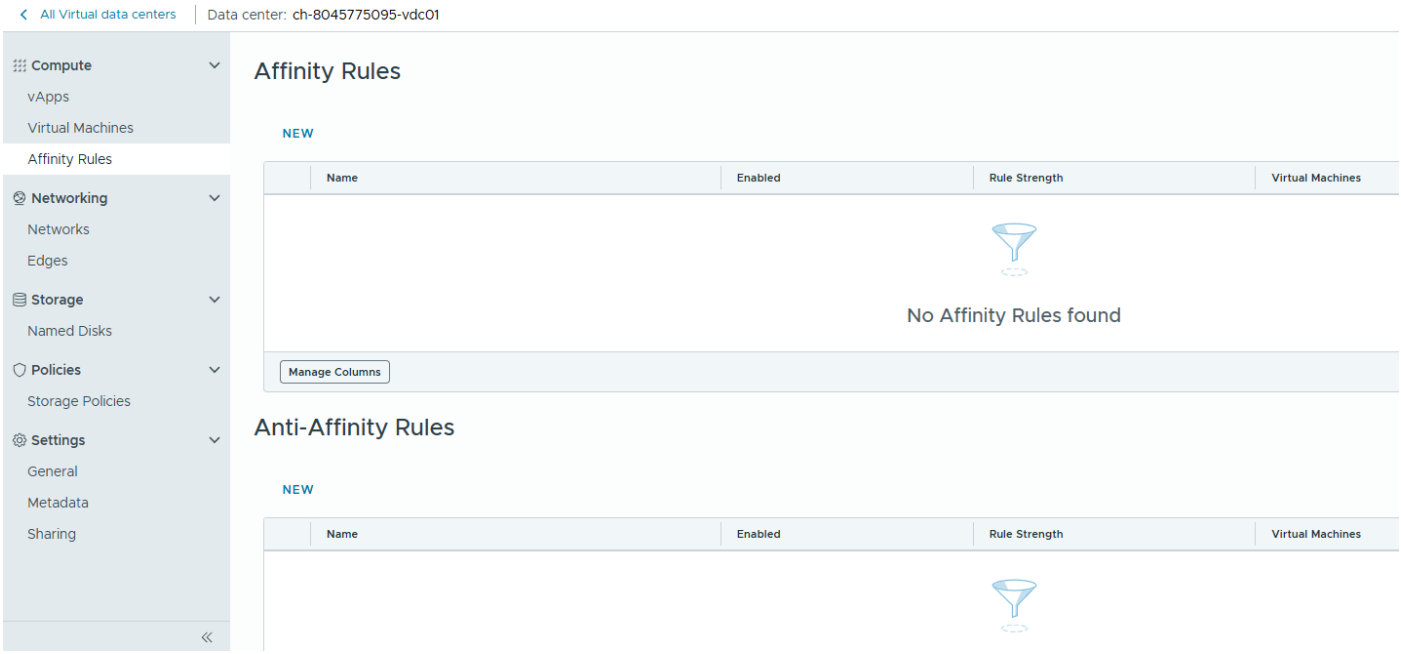
Storage lze měnit i u jednotlivých disků



- Pro jednotlivá VM můžete nastavit i některá DR pravidla z pohledu provázanosti jednotlivých VM pomoci **Affinity rules**. Afinity Rules jsou dostupné v levém sloupci v pohledu konkrétního datacentra. Pomocí nich můžete zadefinovat zda se dvě VM **mohou nebo nemohou spolu vyskytovat na jednom fyzickém HW hostu**. K této funkcionalitě je možné se dostat několika způsoby.

  - Pokud pravidla nenastavíte, je umístění VM určováno automaticky jen na základě disponibilního výkonu
  - „**Affinity Rule**“ – zabezpečuje, že vybrané VMka vždy poběží na stejném hypervizoru/ESXi.
  - „**Anti-Affinity Rule**“ – zabezpečuje, že vybrané VMka nikdy nebudou na stejném hypervizoru/ESXi

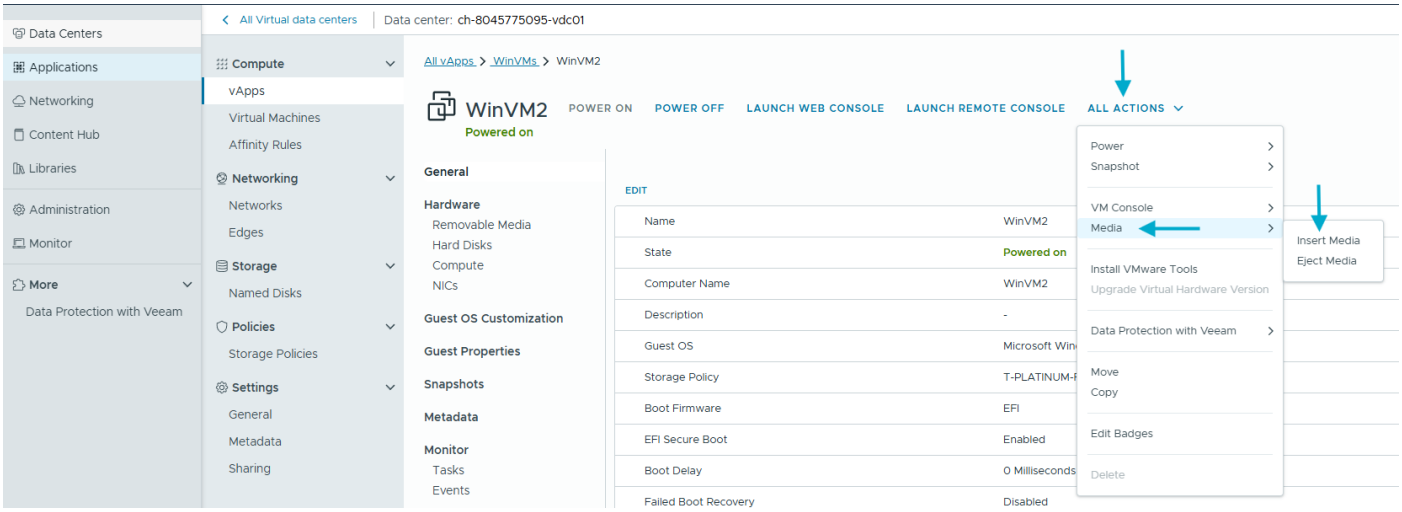
- **POZOR!** Každé VMko může být součástí pouze jednoho afinitní pravidla daného typu (afinitní, anti-afinitní). V případě pokusu o zařazení VMka do jiného pravidla stejného typu se objeví chybová hláška „*There are incorrect or missing values below*“. V případě konfliktu s jinými dříve definovanými pravidly, nelze pravidlo uložit a objeví se hláška „*XY VM Affinity Rule YX conflicts with given set of VMs*“



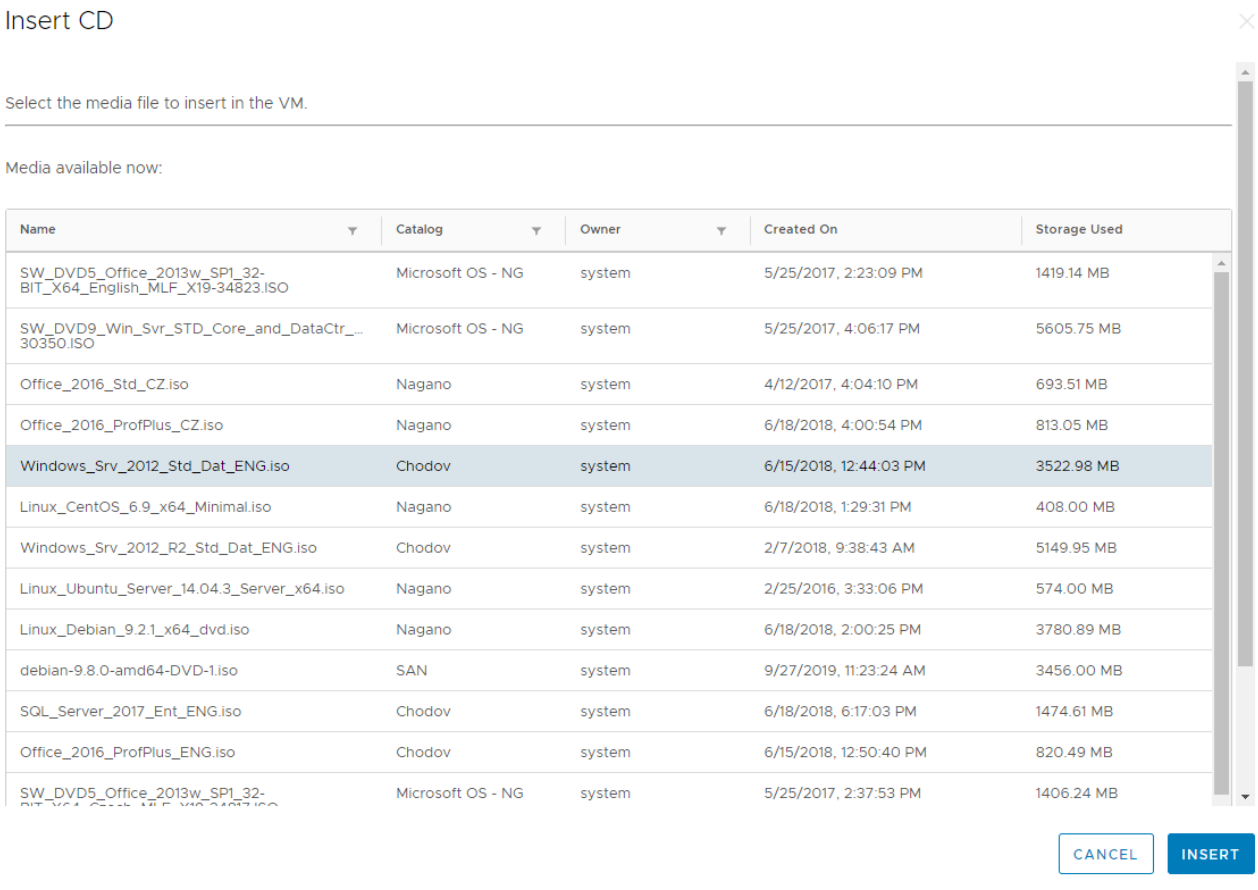
10 Instalace a editace serveru:

10.1 Vytvoření serveru

- Přejděte na **Data Centers**, dále v levém sloupci na **Virtual Machines**
- Vyhledejte kartu serveru a klikněte na **ALL ACTIONS** instalovaný server a vyberte položku **Insert Media**.
- Následně vyberte z katalogu požadovaný image a server spusťe. Proběhne instalace.

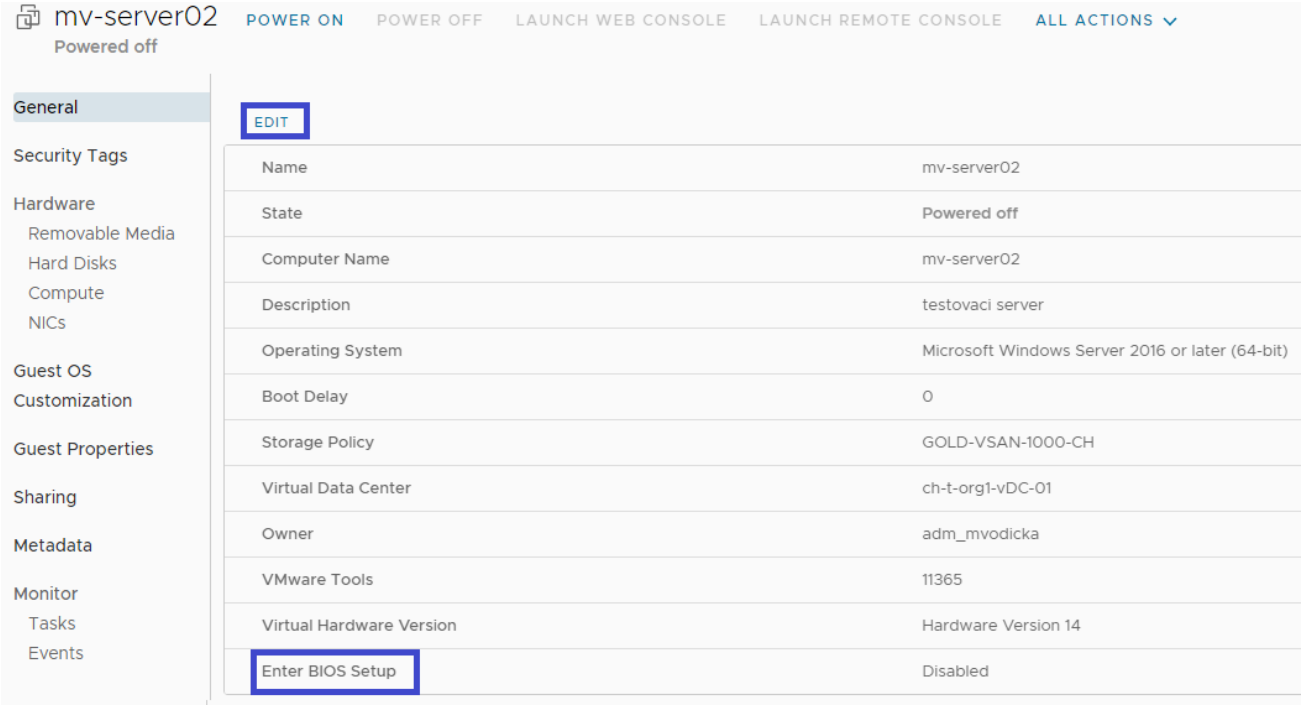


Vyberte požadované ISO a potvrďte tlačítkem **INSERT**



Tím se připojí ISO OS v tomto příkladu do virtuálního serveru. Následně VM spusťte a nainstalujte OS.

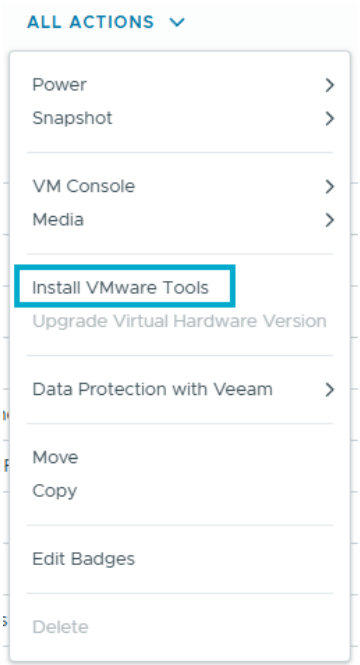
V případě, že server nenabootuje z ISO, tak server vypněte. Klikněte na kartě serveru na záložce General a zaškrtněte volbu „**Enter BIOS Setup**“ a uložte nastavení tlačítkem „**SAVE**“.Toto je další vylepšení prostředí, což ještě „nedávno“ nebylo možné. Po startu virtuálního serveru je spuštěn **BIOS**, ve kterém upravte bootovací pořadí tak, že CD/DVD bude první a nastavení BIOSU uložte. Následně již virtuální server nabootuje z CD/DVD a zvoleného ISO souboru…



Server je následně nainstalován.

Po instalaci serveru je nutno nainstalovat VMware Tools.

Klikněte na kartě virtuálního serveru na **ALL ACTIONS** a vyberte „**Install VMware Tools**.



Následně se (v OS) v mechanice zobrazí instalátor.
Nainstalujte **VMware Tools**. **Po instalaci je vyžadován restart virtuálního serveru.**

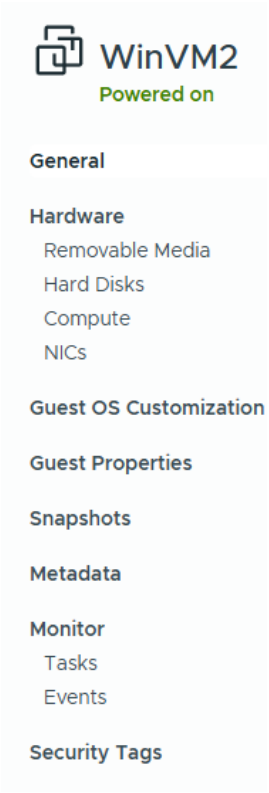
PO VYTVOŘENÍ VIRTUÁLNÍHO SERVERU ZE ŠABLONY PROVĚŘIT JEHO NASTAVENÍ TAK JAKO V PŘÍPADĚ VYTVOŘENÍ NOVÉHO VIRTUÁLNÍHO SERVERU.

VIZ KAPITOLA: 9.2 Doporučené dodatečné nastavení virtuálního serveru.

10.2 Editace serveru

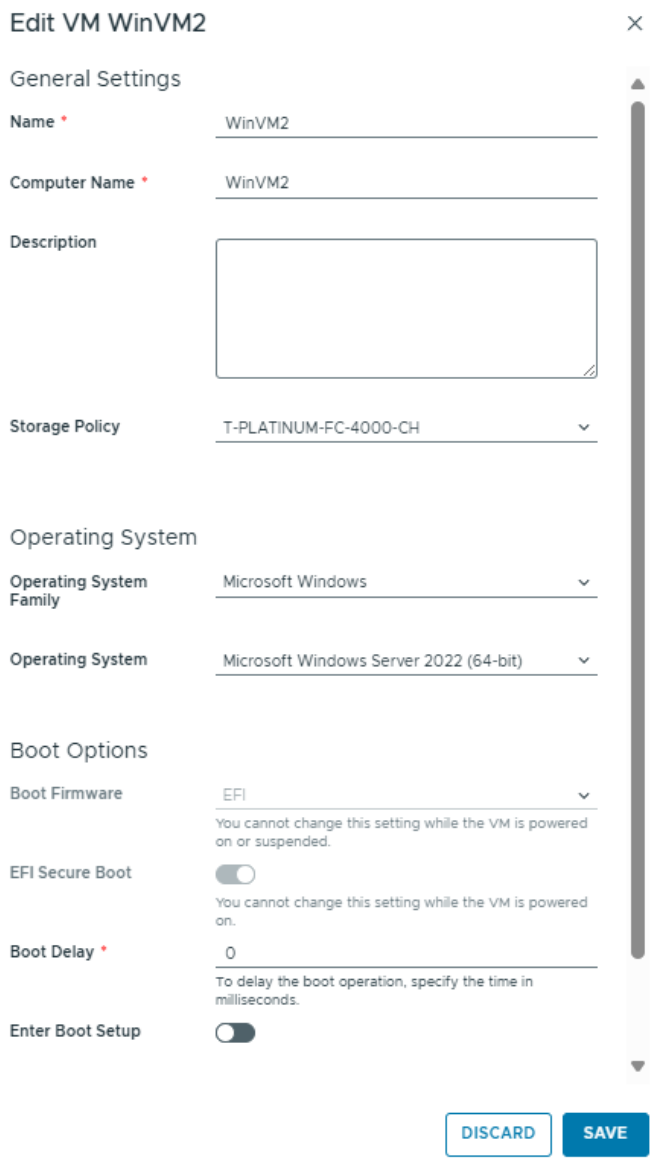
- Po vytvoření serveru a v průběhu provozu serveru je možno provádět editace parametrů serveru. Například je možno přidávat vCPU, (pokud je zapnuto nastavení Virtual CPU hot add), upravovat velikost paměti (pokud je zapnut Memory hot add) a upravovat disky.

Klikněte na kartě virtuálního serveru a zobrazí se následně níže uvedené možnosti:



General – obecné nastavení serveru
(název, operační systém, verze VMware Tools, Virtual Hardware version apod…), detaily níže

Lze nastavit vstup do BIOSU (Enter BIOS Setup) nebo Boot Delay



Hardware – Úprava výkonostních a kapacitních parametrů serveru

Guest OS Customization – customizace

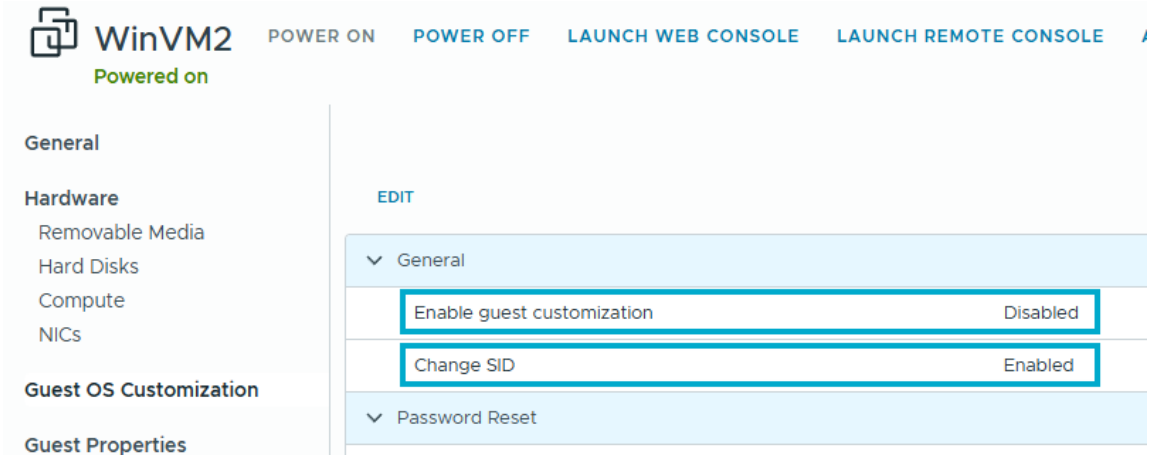
Toto nastavení se používá především pro NOVÉ servery Windows Server 2022 a 2025 vytvářené z Templaty (šablony), kdy ulehčuje konfiguraci s nastavením OS.

Pro stávající servery nedoporučujeme zapínat tuto volbu !!

Pokud zaškrtnete **Enable guest customization**, bude aplikováno pro daný virtuální server nastavení názvu virtuálního serveru a sítě z tohoto rozhraní do operačního systému virtuálního serveru.
Do OS se z tenant portálu aplikuje ComputerName uvedený v tenant portálu a parametry sítě, do které je virtuální server připojen. (IP adresa, maska, GW a DNS Servery). **Toto nastavení PŘEPÍŠE stávající nastavení OS.**

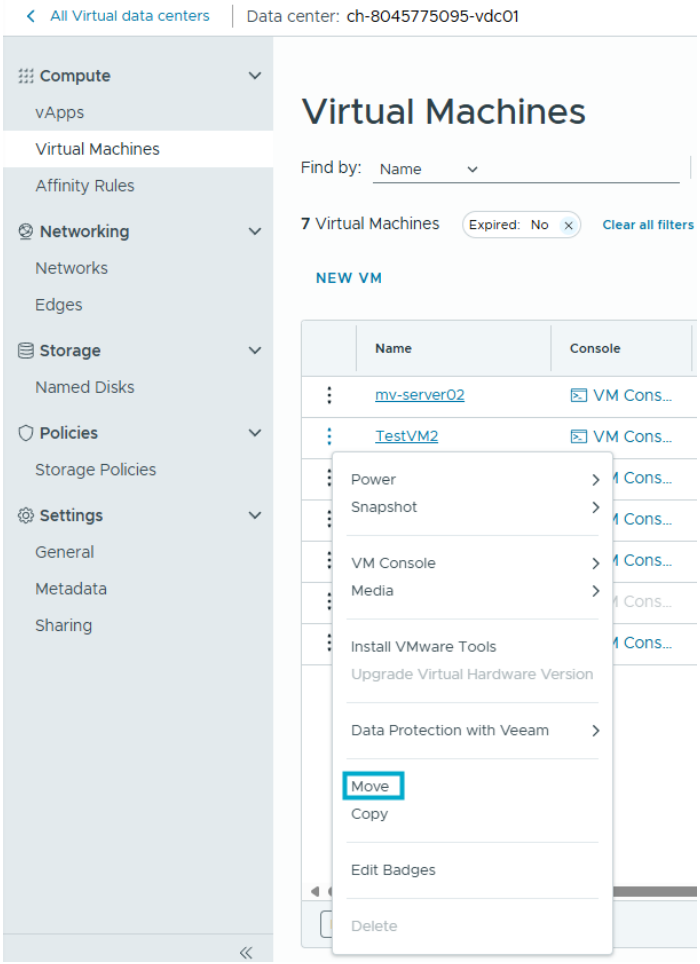
Pokud nevyžadujete provést customizaci serveru v provozu důrazně doporučujeme toto nastavení NEZAPÍNAT. Může to mít za následek odpojení serveru z domény, neboť by mohlo dojít ke změně názvu serveru OS pokud by bylo rozdílné v Tenant portálu

oproti OS a dále i změnu DNS serverů. Pokud je ještě v tomto nastavení zaškrtnuta volba „Change SID“ došlo by i k resetu SID v OS, což by způsobilo odpojení serveru z domény a ohrožení dostupnosti tedy i funkčnosti tohoto serveru ve Vaší organizaci.

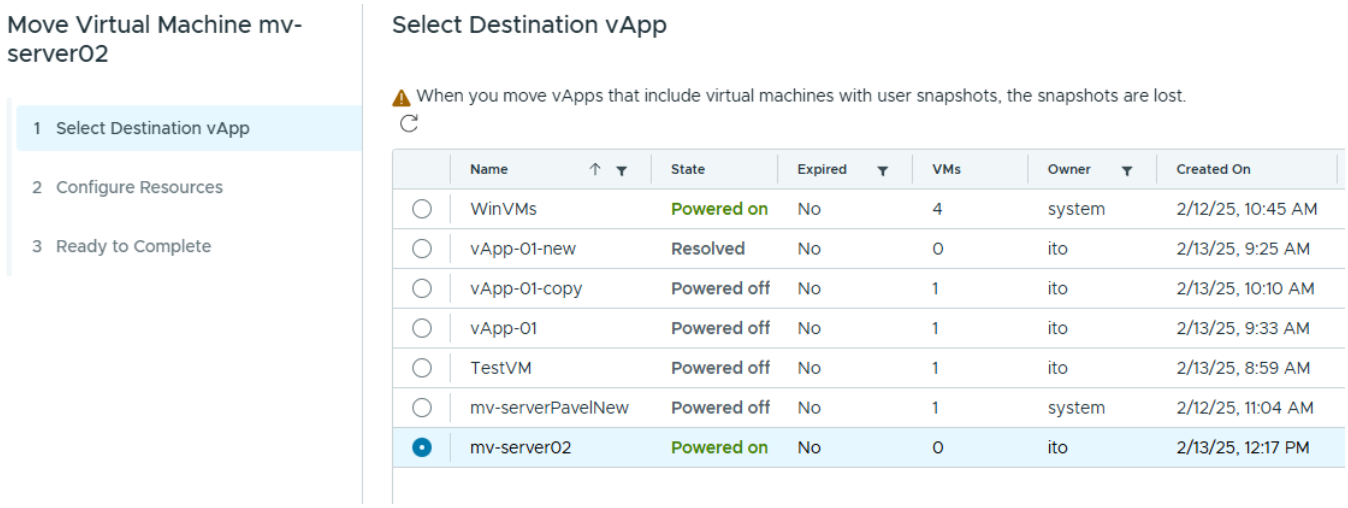


10.3 Přesun virtuálního serveru do jiné vAppy

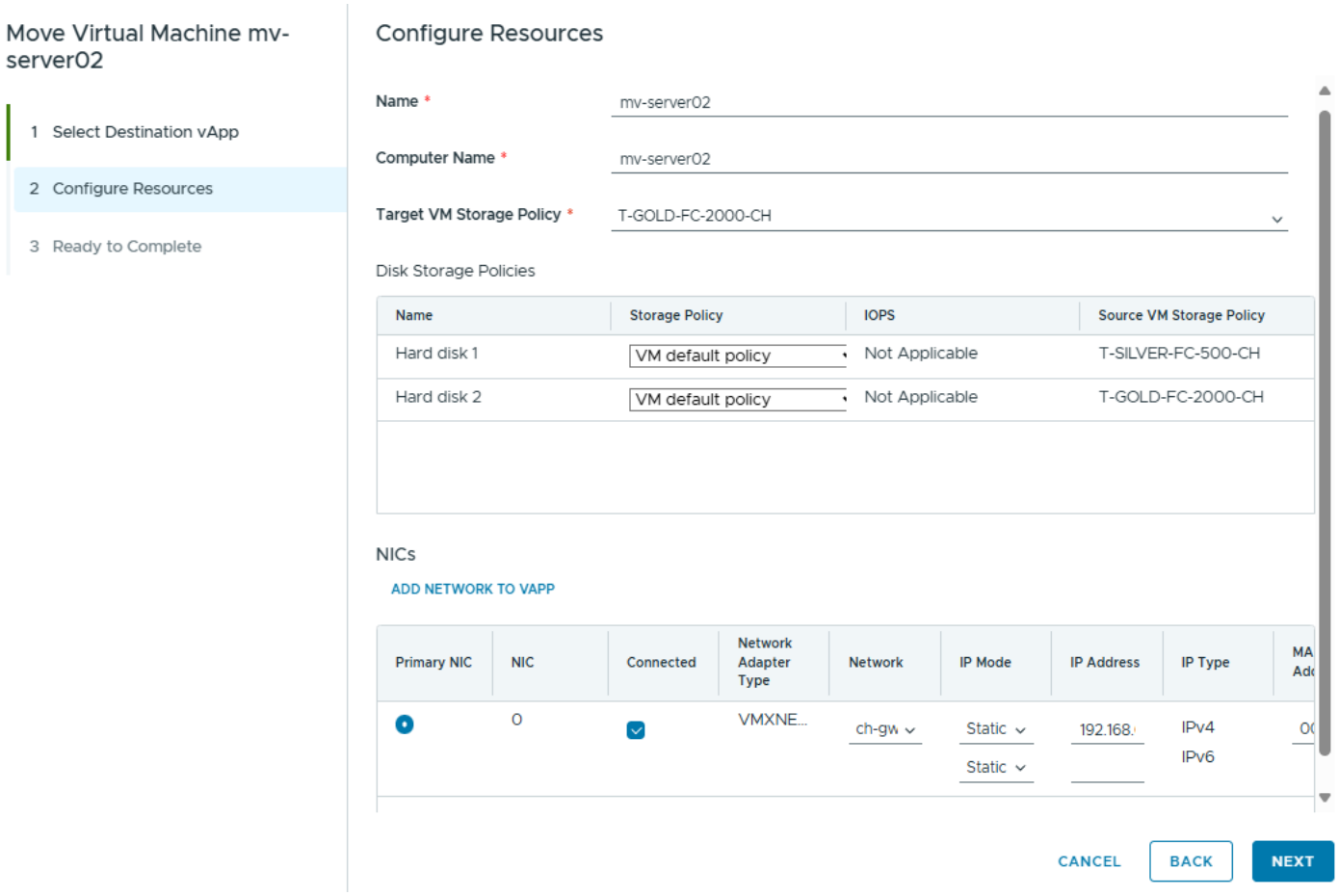
Virtuální server lze přesunout do jiné vAppy kliknutím na **3 tečky u VM** a po té na **Move** z pohledu Virtual Machines a je možné tuto operaci provést za běhu VM. Pokud vAppa neexistuje, kliknutím na vApps a New vApp jí nejprve předem vytvořte, viz kapitola 6. (V detailu virtuálního serveru je možno také zvolit přesun a to prostřednictvím **ALL ACTIONS** a pak **MOVE**).



Zvolte cílovou vApp. Pokud máte k dispozici více datacenter, tak lze tak přesouvat virtuální servery v rámci lokalit JZM a Chodov. **V cílové vAppě musí být shodná síť jako ve stávající, pokud má být u VM serveru zachována IP adresace.**



V dalším kroku vyplňte cílovou **Storage policy** a po té **konfiguraci sítě**, jakou má dané VM.

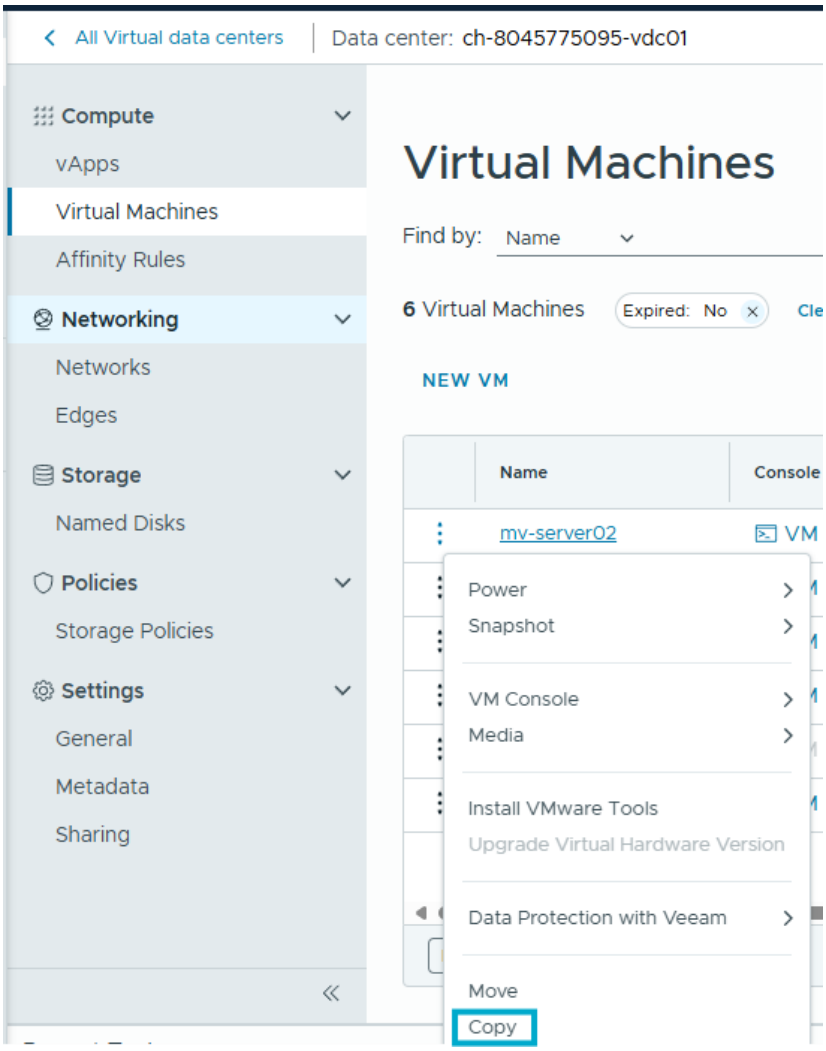


Poté dokončit. Tím se přesune server do zvolené cílové vAppy.

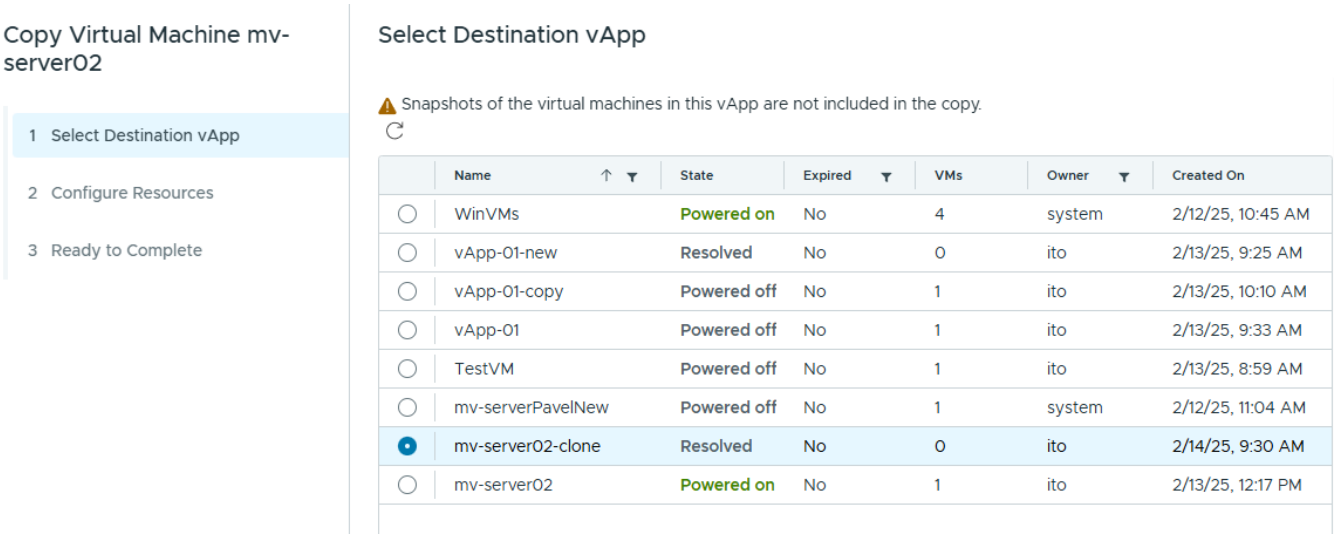
Přesunutý server má STEJNOU MAC jakou měl před přesunem, MAC zůstává zachována.
Tímto postupem se provedl přesun serveru do vAppy.

10.4 Clone virtuálního serveru do jiné vAppy

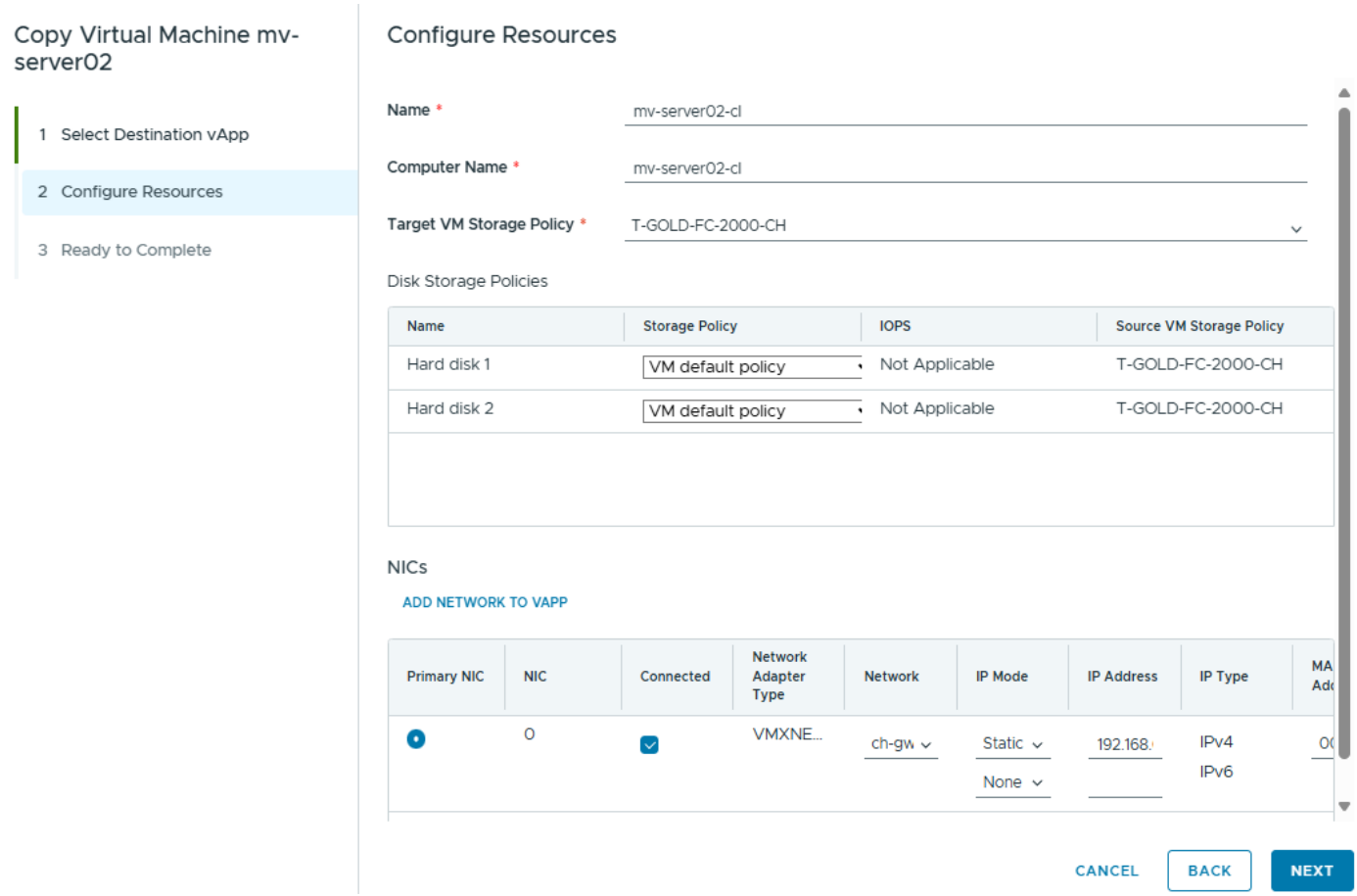
Virtuální server lze zkopírovat do jiné vAppy kliknutím na **3 tečky u VM** a po té na **Move** z pohledu Virtual Machines a je možné tuto operaci provést za běhu VM (v zapnutém stavu).
(V detailu virtuálního serveru je možno také zvolit přesun a to prostřednictvím **ALL ACTIONS** a pak **MOVE**).



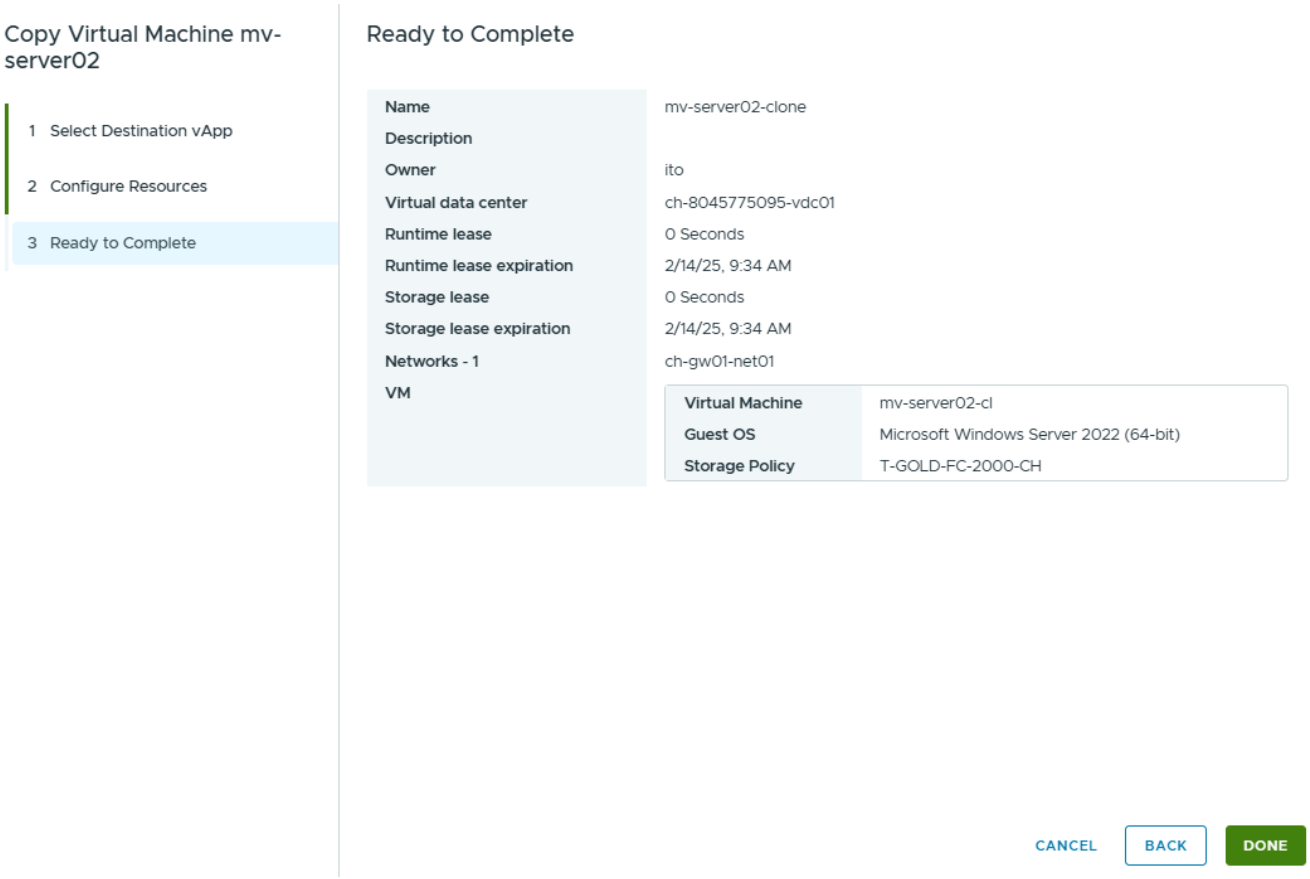
Vyberte cílovou vAppu a pokračujte kliknutím na **NEXT**



Vyberte **cílovou storage** a nastavte **IP adresaci** pro server.



Clone dokončíte kliknutím na **DONE**.



Zklonovaný server má JINOU MAC než původní server, ze kterého se nové VM vytvořilo kopií = clonem.
Tím se provedla kopie = clone serveru.

Před zapnutím zklonovaného VM doporučujeme v o2 cloudu vNIC odpojit, VM spustit, readresovat na úrovni OS a poté vNIC připojit, aby nedošlo ke kolizi IP adresy se zdrojovým VM.

10.5 Práce s BIOS u VM

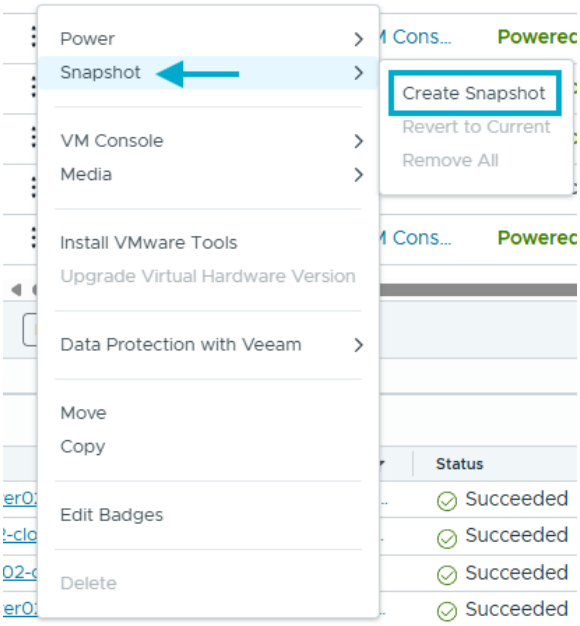
Ve vlastnostech VM je možné se dostat **do BIOSu a používat klávesové zkratky během BOOT procesu.** K této funkcionalitě se lze dostat po kliknutí na kartě virtuálního serveru na v sekci **General.**

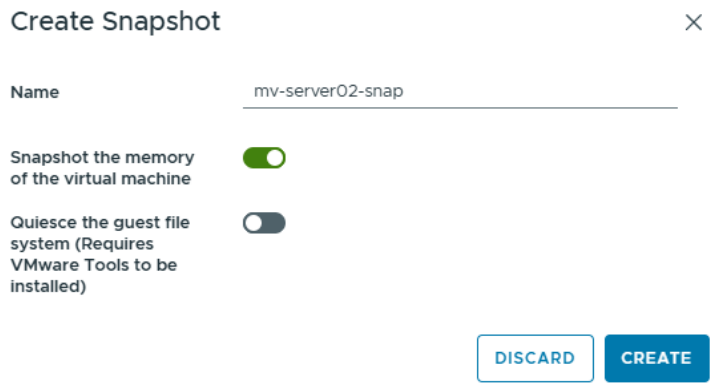
- Lze nastavit pravidla pro bootování VM (například nastavit v jakém pořadí se startují). Funkce **Boot Delay** – je udáván v ms (hodnota 1000 = 1sekunda)
- Lze nastavit aby při následujícím spuštění VM server nejdříve přešel do BIOS. Funkce **Enter BIOS Setup** – při následujícím bootu VM přejde VM do BIOSu.

11 Snapshoty serveru:

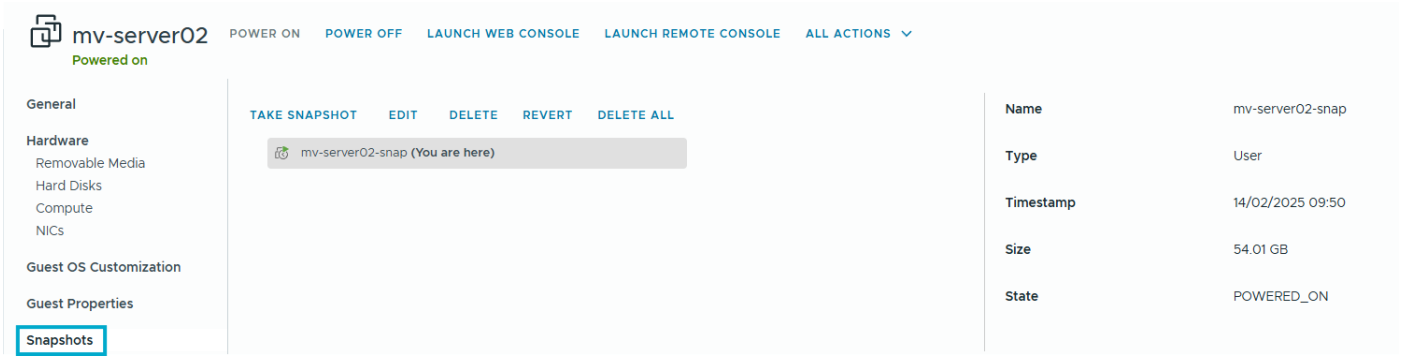
Před případnými aktualizacemi serveru, release verzí apod. je možno provést snapshot (snímek) serveru za účelem uchování funkčního stavu serveru. V případě problému je pak možno se do tohoto snímku (snapshotu) „vrátit“ a opět zajistit bezproblémový provoz serveru před tímto zásahem.

- Klikněte na kartě virtuálního serveru na „**Snapshots**“, zvolte „**Create Snapshot**“ a pojmenujte si jej. Případně můžete zaškrtnout volbu snapshotu včetně vRAM a potvrďte „**CREATE**“.





Vytvořený snapshot s detailními informacemi naleznete na „**Snapshots**“, kde můžete též vytvářet/revertovat/mazat snapshot



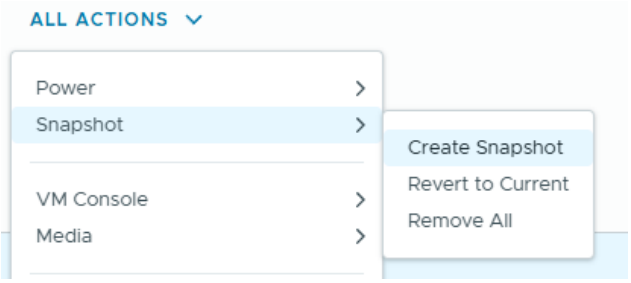
- **POZOR!** **Pro úspěšné vytvoření snapshotu je potřeba mít dostatek diskové kapacity v rámci VDC, ve kterém se VM nachází**

- **Pro příklad:** potřebujete-li provést **snapshot VM včetně obsahu vRAM** pro VM, které má **8 GB vRAM** a jeden disk o velikosti **160 GB**, bude potřeba mít na příslušném úložišti (storage tieru) ve vDC alespoň **160 + 8 GB volného místa**. Pokud se bude provádět **snapshot bez obsahu vRAM**, bude stačit **160 GB volného místa**.

- **POZOR!** V rámci této funkcionality máte vždy možnost vytvořit **vždy pouze jeden snapshot a pokud je již vytvořen starší snapshot tak je tímto přepsán novějším.**

Následně se vytvoří snapshot (snímek) virtuálního serveru.

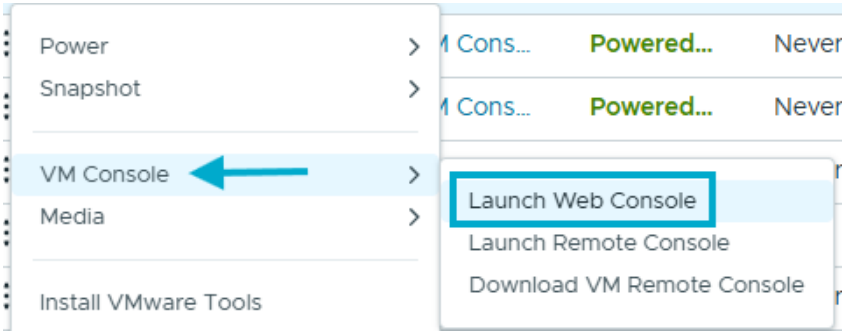
Po kliknutí na „**ALL ACTIONS**“ na kartě virtuálního serveru jsou další možnosti práce se „snapshotem“



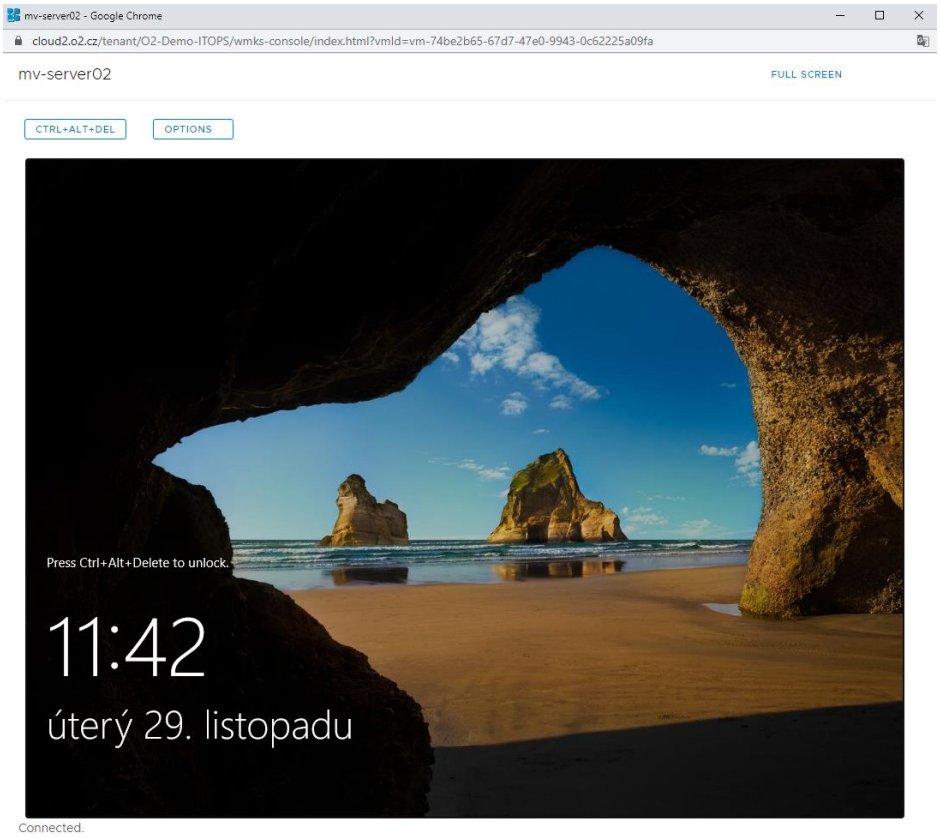
Create Snapshot – vytvoření snapshotu
Revert to Current – vrátit se do stavu doby pořízení snapshotu
Remove All – odstranit snapshot

12 Práce s „konzolí“ virtuálního serveru

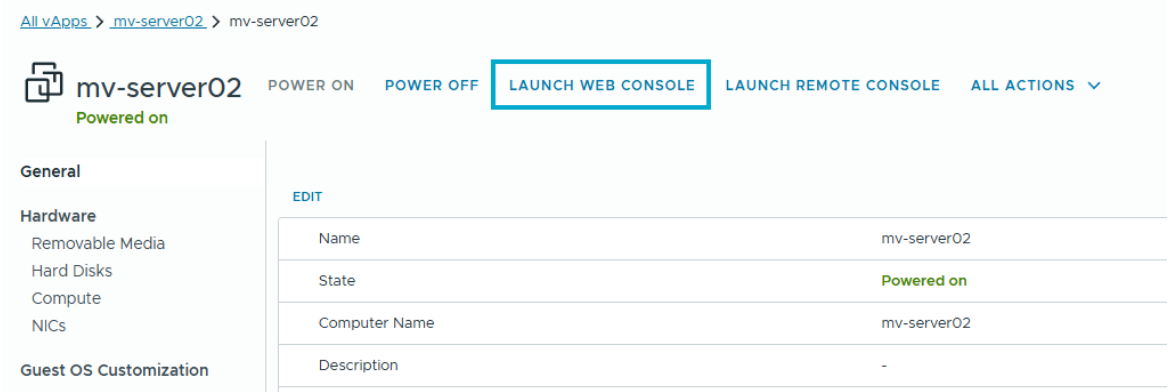
V tenant portálu je dostupná webová konzole virtuálního serveru po kliknutí na VM Console. Nejsou vyžadovány žádné doplňky.



Po kliknutí se zobrazí konzole serveru.

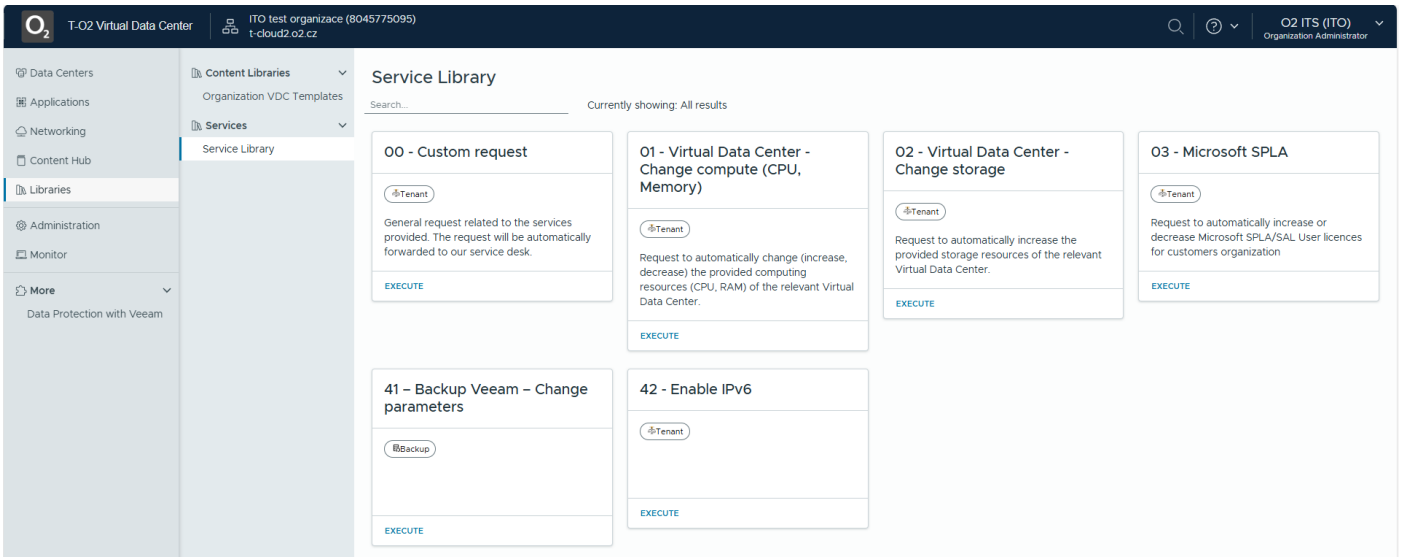


Konzoli lze též vyvolat z karty serveru přes „**LAUNCH WEB CONSOLE**“



13 Service Library

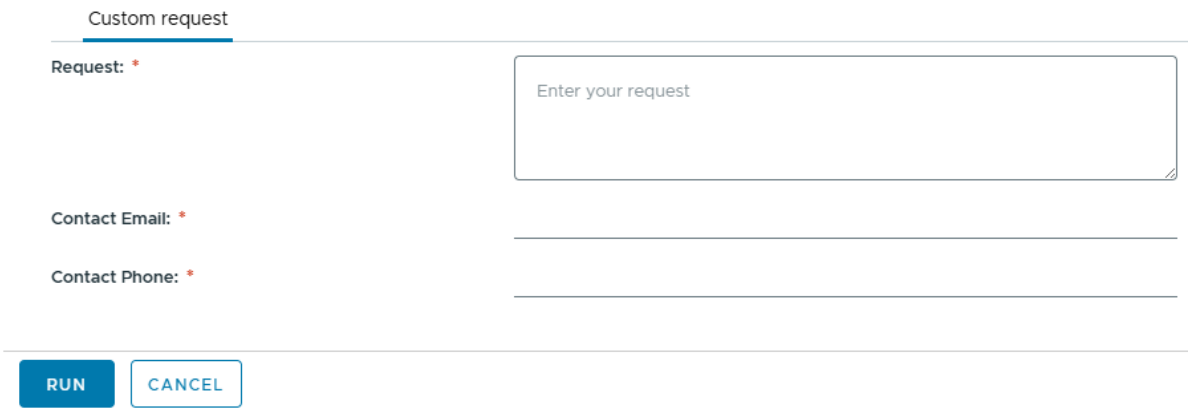
Po kliknutí na **Libraries** -> **Services** -> **Service Library,** můžete provádět úpravy Vašeho virtuálního datového centra prostřednictvím workflow.



00 – Custom request

General request related to the services provided. The request will be automatically sent to our service desk.

Obecný požadavek související s poskytovanými službami. Požadavek bude automaticky odeslán na náš ServiceDesk. (tlačítkem **EXECUTE**) a poté zpracován.

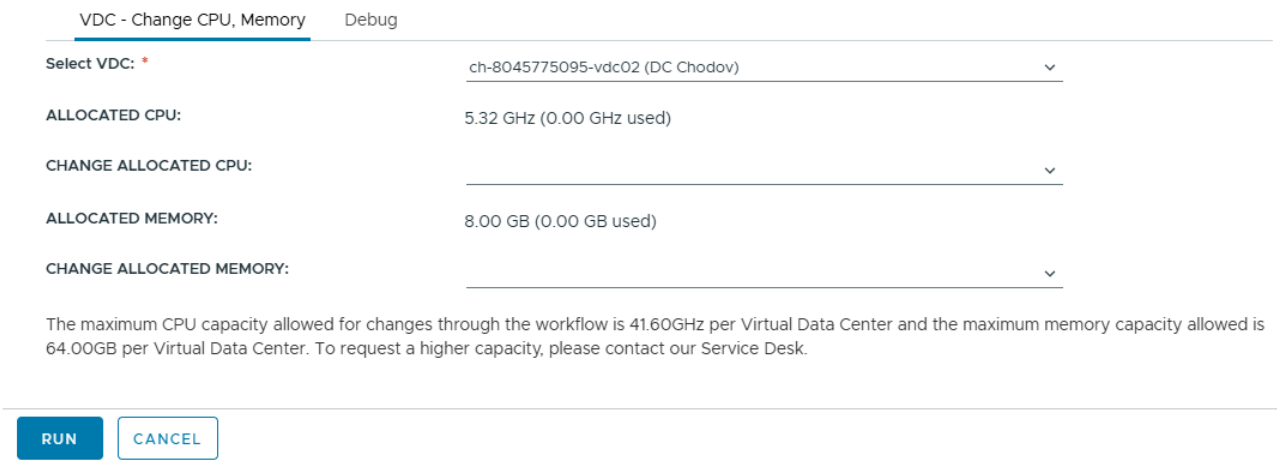


Do pole **Request** – (požadavek), napište požadavek, uveďte kontaktní údaje a WF spusťte stisknutím tlačítka **RUN**.

01 – Virtual Data Center - Change compute (CPU, Memory)

Request to automatically change (increase, decrease) the provided computing resources (CPU, RAM) of the relevant Virtual Data Center.

Žádost o automatickou změnu (zvýšení, snížení) poskytovaných výpočetních zdrojů (vCPU, RAM) příslušného virtuálního datového centra. (tlačítkem **EXECUTE**).



Vyberte o kolik vCPU nebo paměti se má **navýšit nebo snížit** Vámi vybrané vDC a následně klikněte na **RUN**.

Požadujete-li počet vCPU nebo paměti, které nejsou uvedeny v rozbalovací nabídce, je potřeba spustit workflow opakovaně pro dosažení cílového stavu.

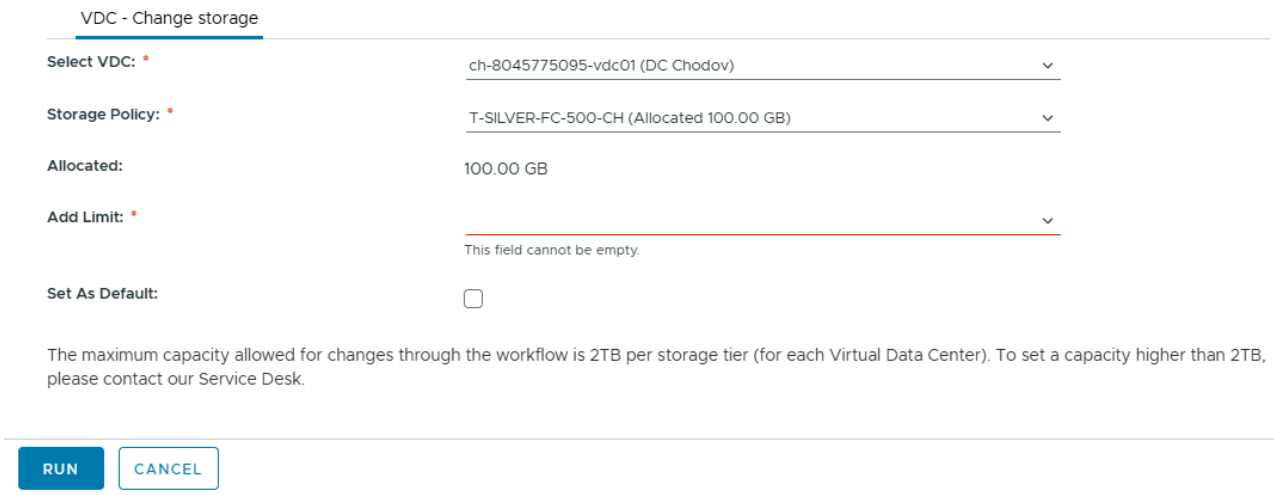
(Příklad: požadujete-li například přidat +6 vCPU do vDC, je potřeba spustit workflow nejprve +2 vCPU a poté přidat +4 vCPU) aby výsledný součet byl 6 vCPU, to samé v případě snížení).

Po spuštění je workflow zobrazeno v seznamu úloh jako běžící úloha, po jejímž dokončení dojde k navýšení zdrojů.

Maximální výpočetní výkon VM je 16 vCPU a 64 GB RAM.

02 – Virtual Data Center – Change storage

Žádost o automatické navýšení poskytovaných uložišť (storage tieru s příslušnou storage policy) vybraného virtuálního datového centra nebo přidání nového úložiště.



Vyberte příslušnou storage, (uložiště), pro kterou chcete provést navýšení a z rozbalovací nabídky vyberte, o kolik se má **navýšit uložiště** ve Vašem vDC a následně klikněte na **RUN**.

(Příklad: požadujete-li například přidat +150 GB do vDC, je potřeba spustit workflow nejprve +100 GB, spustit workflow a poté přidat +50 GB) aby výsledný součet danného uložiště 150 GB).

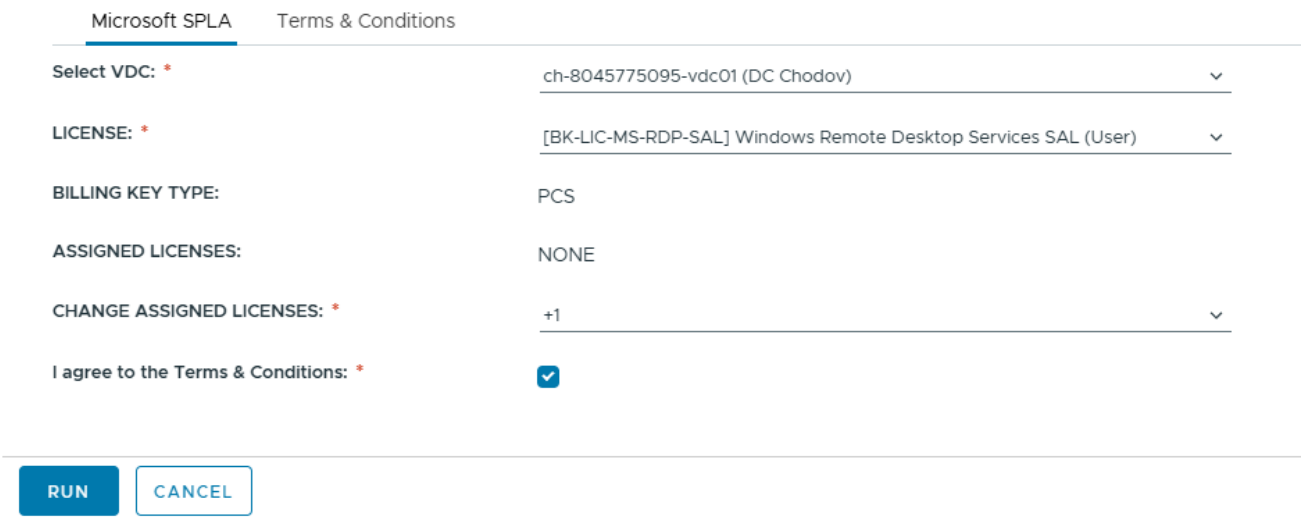
Po spuštění je workflow zobrazeno v seznamu úloh jako běžící úloha, po jejímž dokončení dojde k navýšení zdrojů.

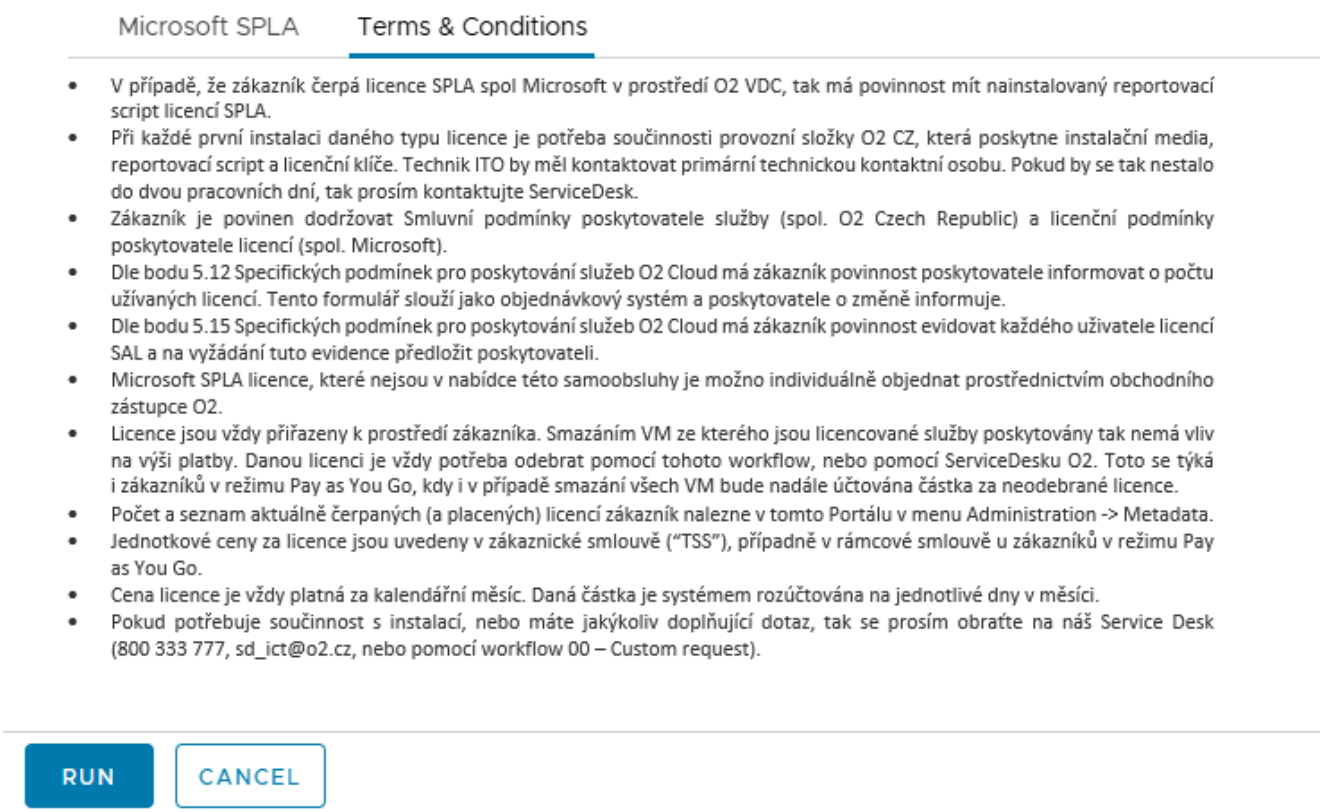
Tímto způsobem můžete navyšovat jednotlivá úložiště (storage tiery) až do kapacity 2 TB per tier (nikoliv v součtu). Pro vyšší kapacitu kontaktujte náš Service Desk.

21 – Microsoft SPLA

Request to automatically increase or decrease Microsoft SPLA/SAL User licences for customers organization

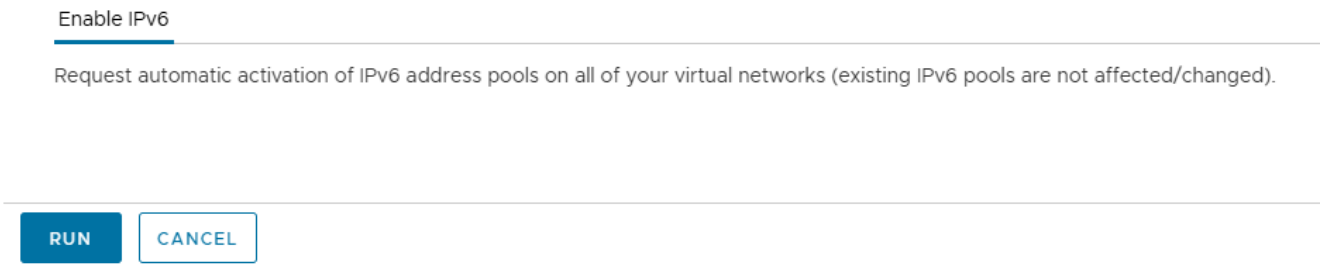
Žádost o automatické zvýšení nebo snížení uživatelských licencí Microsoft SPLA/SAL pro organizaci zákazníků





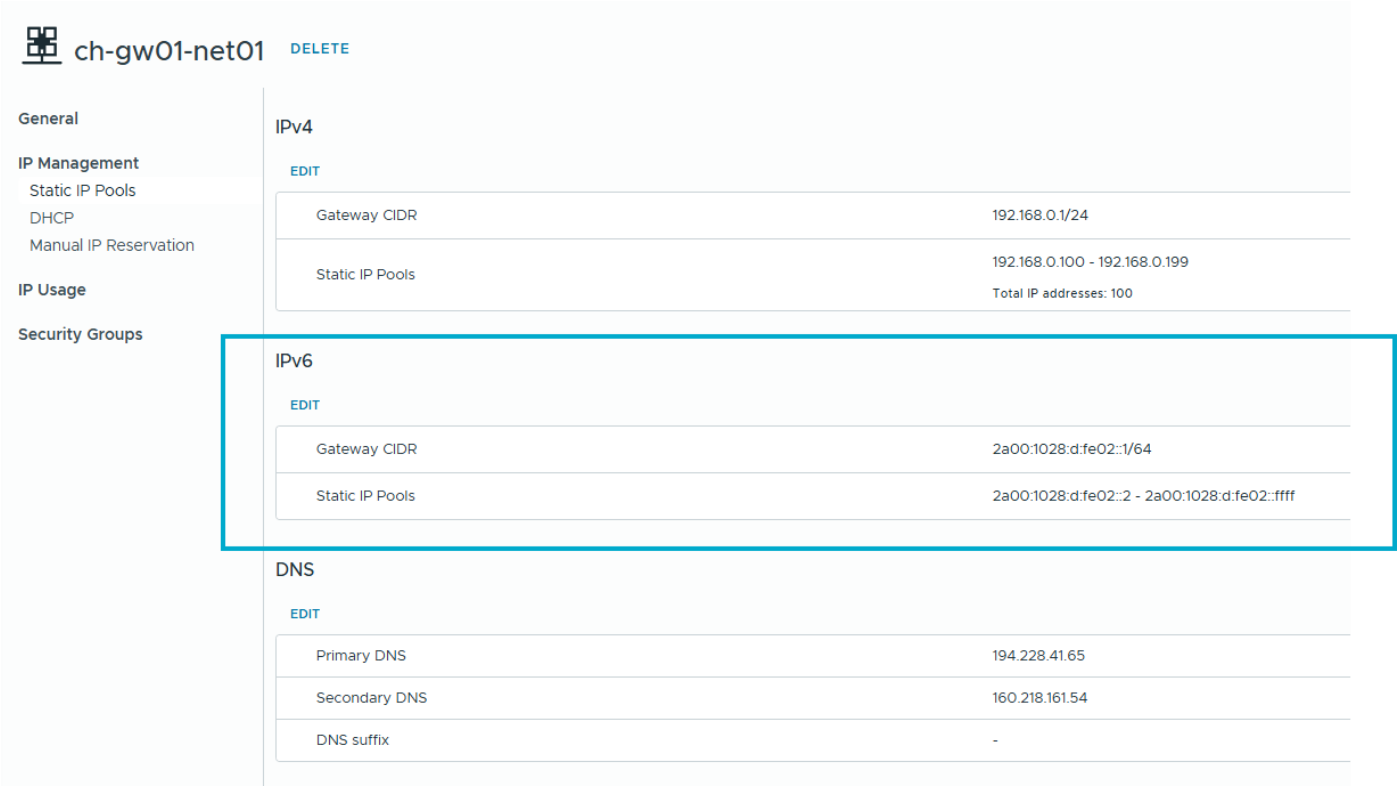
Vyberte vDC, následně v seznamu **LICENSE** vyberte **produkt**, po té v seznamu **CHANGE ASSIGNED LICENCES** **počet** a klikněte na **RUN**.

42 – Enable IPv6



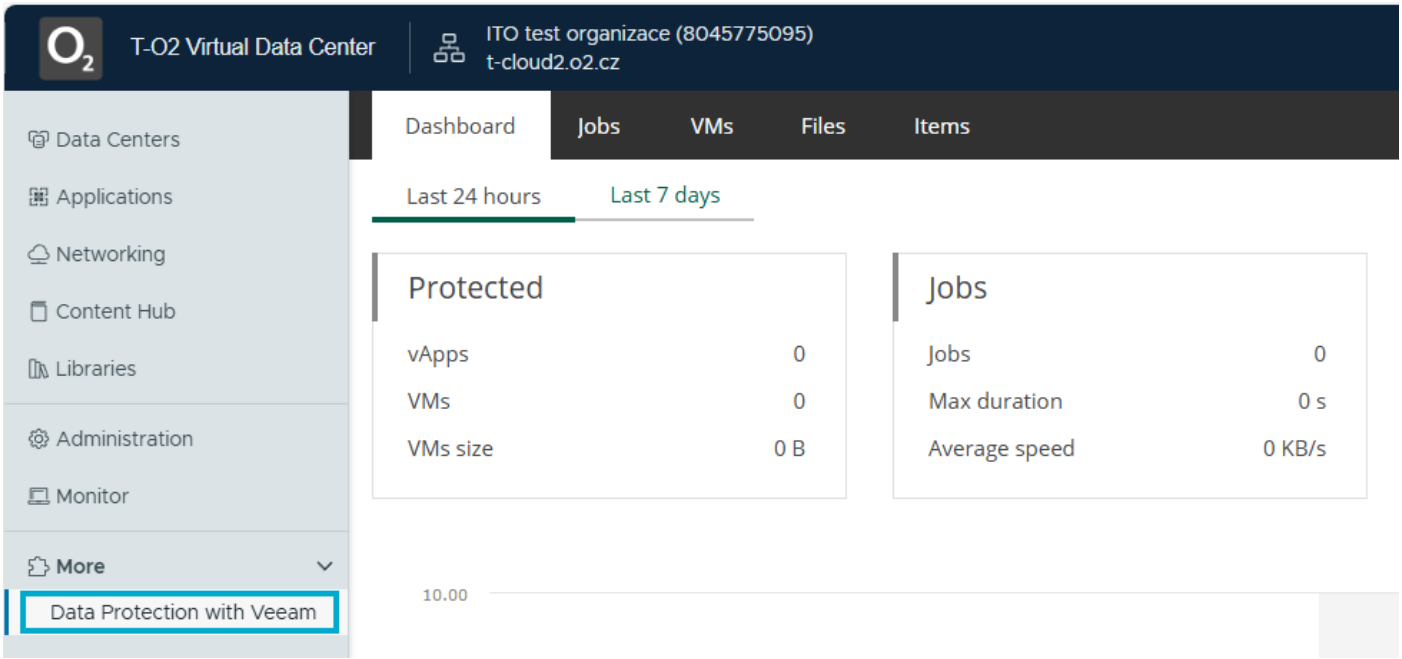
Po spuštení tohoto workflow dojde k automatické aktivaci IPv6 na všech privátních org routed sítích, které IPv6 nastavený nemají.

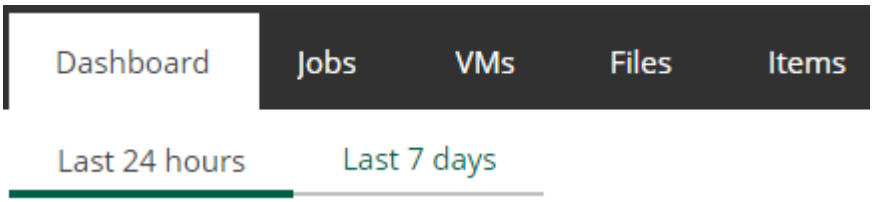
Následně se na routované org síti zobrazí IP adresa IPv6, Gateway a Static IP Pools pro virtuální servery.



14 Zálohy a obnovy Veeam – Data Protection with Veeam

Zálohování a obnovy je možné nastavit prostřednictvím backup modulu **Data Protection with Veeam.** O zpřístupnění backup modulu je potřeba si zažádat přes svého O2 obchodníka. Následně Vám backup modul vypublikujeme a vám se zobrazí v sekci „**More -> Data Protection with Veeam**“





Dashboard – nástěnka a přehled

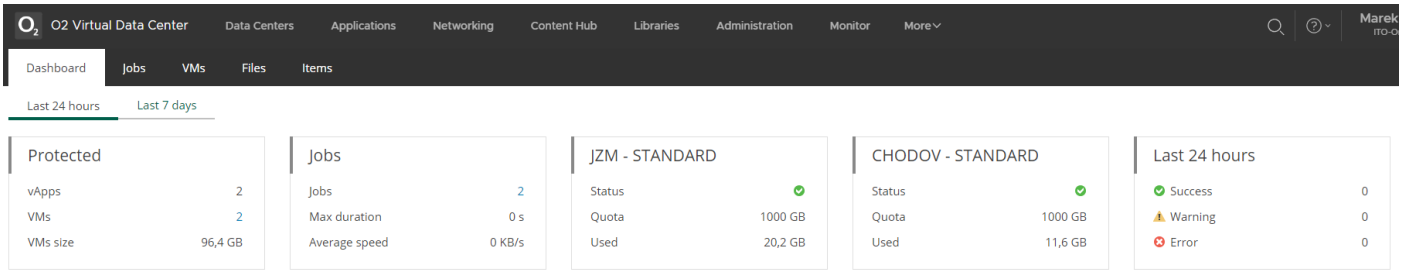
Jobs – seznam zálohovacích úloh

VMs – přehled zálohovaných virtuálních serverů

Files – možno obnovit adresáře a soubory z virtuálních serverů

Items – možno obnovit SQL a Oracle DB.

Na nástěnce (Dashboard) je přehled (za 24 hodin nebo za 7 dní), který zobrazuje informace:



Protected

vApps: počet zálohovaných vApp (obálka nad servery sloužící k logickému zařazení jednotlivých virtuálních serverů).
VMs: počet zálohovaných virtuálních serverů.
VMs size: celková obsazená kapacita na platformě v O2 Cloudu.

Jobs

Jobs: počet zálohovacích úloh
Max duration: doba nejdéle trvající zálohy
Average speed: průměrná rychlost zálohy

Dále, podle lokality je zobrazena karta, ve které jsou informace:

Celkový stav: zobrazuje celkový stav úspěšnosti záloh v dané lokalitě
Quota: maximální kapacita objemu zálohování, po jejímž překročení nebude funkční zálohování, neproběhne záloha
Used: skutečný aktuální objem zálohovaných dat

Last 24 hours nebo 7 dní

Success: počet úspěšných záloh
Warning: počet záloh s upozorněním
Error: počet záloh s chybou

14.1 Nastavení příchozího pravidla ve Firewallu operačního systému zálohovaného serveru

Pravidlo je potřeba vytvořit v případě, kdy využíváte zálohování přes IPv6 pro rychlejší (efektivnější) odzálohovávání transakčních SQL/Oracle logů na DB serveru s aktivním app-aware processingem

V případě, že máte u zálohovaného virtuálního serveru, dále jen VM, aktivní Firewall v operačním systému, je potřeba povolit níže uvedené porty v příchozím pravidle na daném VM.

Vytvořte si tedy ve FW dvě příchozí pravidla, jedno pro TCP, kde vydefinujete TCP porty a druhé pro UDP, kde vydefinujete UDP porty. Remote port není potřeba definovat.
V pravidle není potřeba definovat IP adresy ve zdroji a cíli, (zůstává Any/Any). Níže uvedené porty nastavujete pouze do Local Ports v příchozím pravidle. Odchozí pravidlo není potřeba nastavovat.

Zdroj informací: Veeam KB:

https://helpcenter.veeam.com/docs/backup/explorers/vesql_used_ports.html?ver=120

https://helpcenter.veeam.com/docs/backup/agents/used_ports.html?ver=120

Windows:

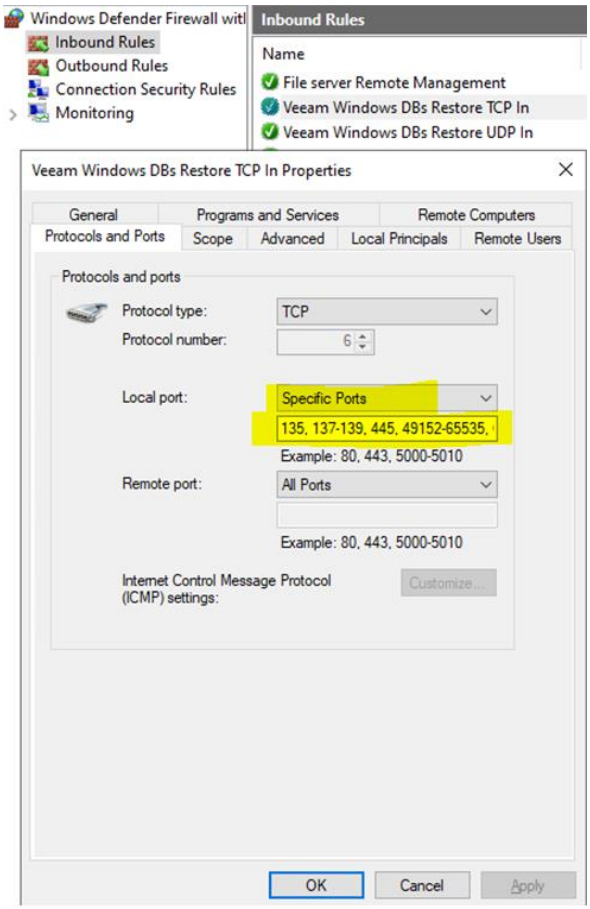
Windows agent (musí být povoleny vždy)
TCP: 10005, 10001, 2500-3300, 6184-6194, 135, 137-139, 445, 6160, 11731, 6211, 11731, 6162, 49152-65535
UDP: 135, 137-139, 445, 6160, 11731
+ navíc dle služby:

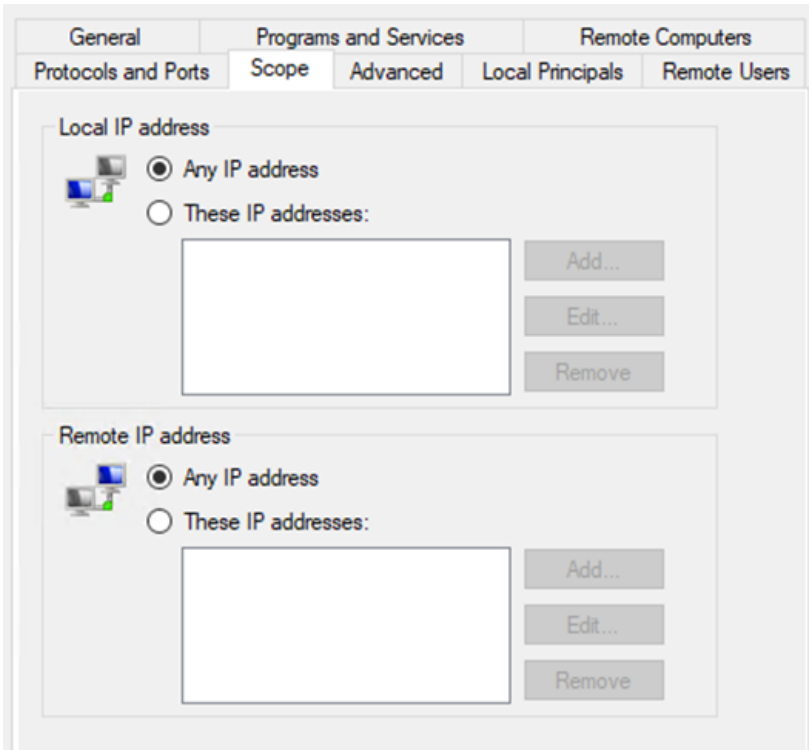
Active Directory
TCP: 389, 636, 3268, 3269
UDP: 389

Microsoft SQL Server
TCP: 1433, 1434, 6167, 1025-1034
UDP: 1434

Oracle
TCP: 6167, 1025-1075

Exchange
TCP: 60005-65535, 443





Linux

Linux agent (musí být povoleny vždy):
TCP: 22, 6160, 6162, 2500-3300

+ navíc dle služby:

Oracle
TCP: 6167

PostgreSQL
shodné s Linux agent

SAP HANA
shodné s Linux agent

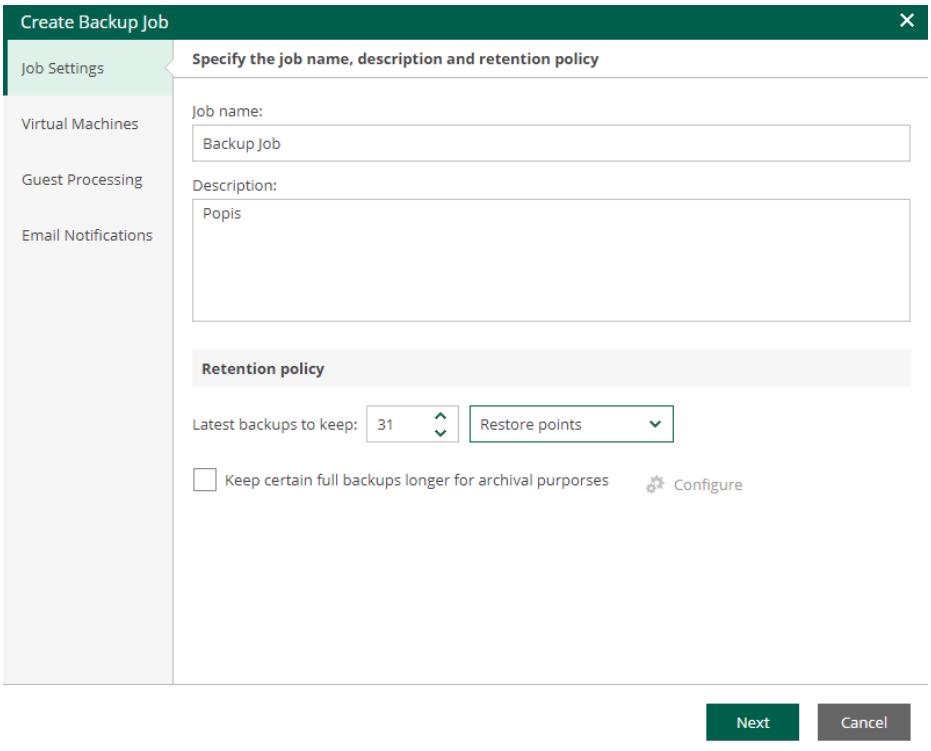
Unix, macOS

Unix,macOS agent (musí být povoleny vždy):
TCP: 10006

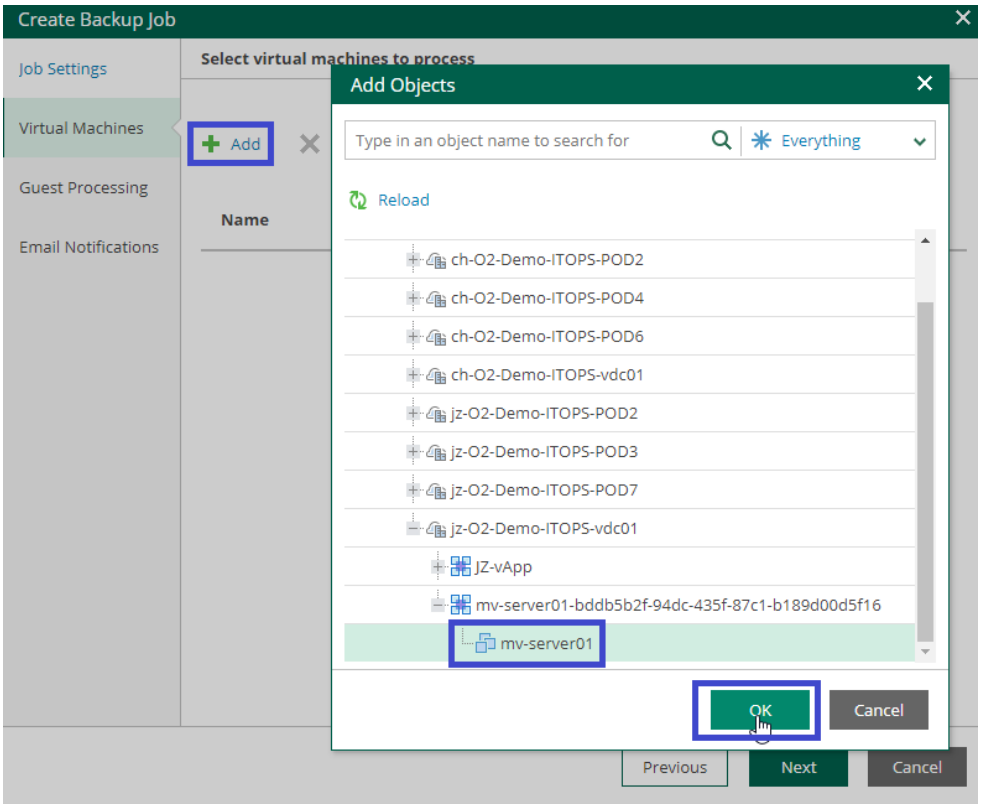
14.2 Vytvoření zálohovací úlohy

Kliknutím na Jobs a následně na Create spustíte průvodce k vytvoření zálohovací úlohy.

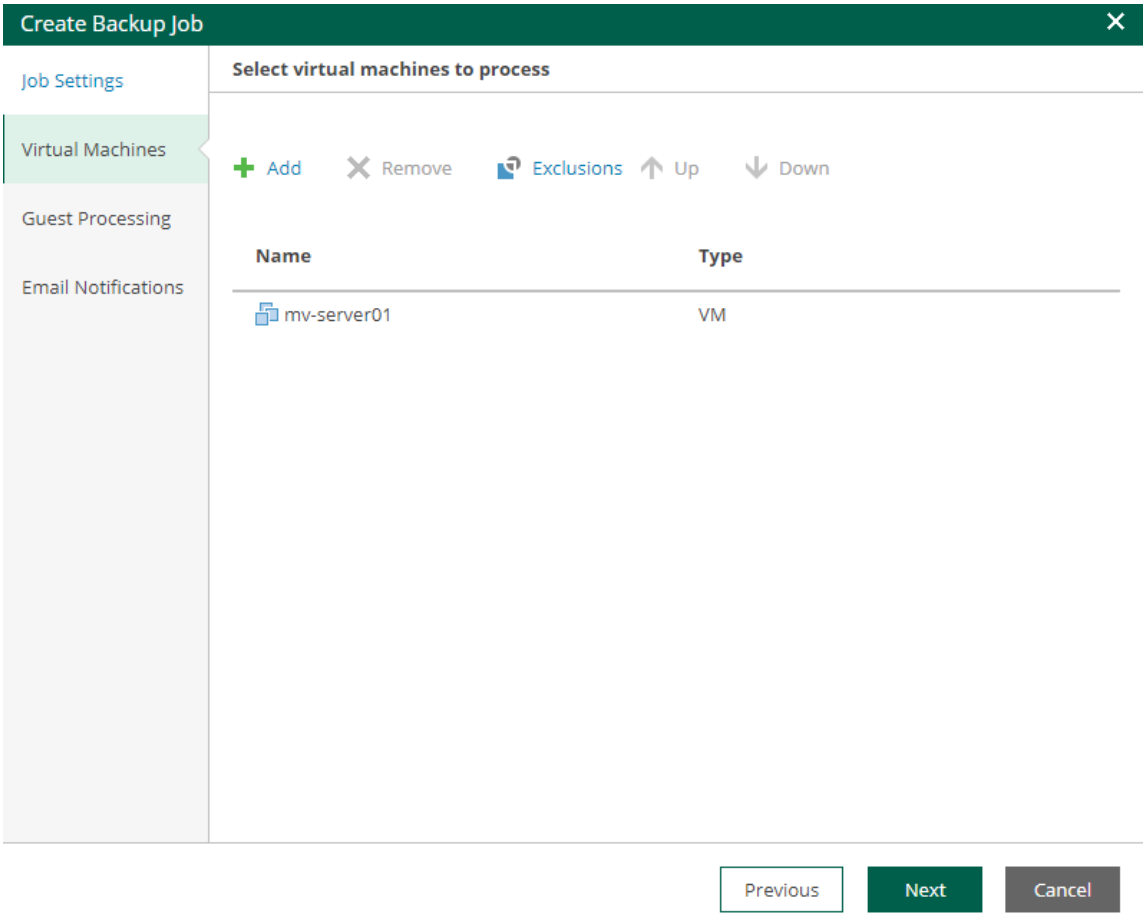
Zadejte název zálohovací úlohy, volitelný je popis, poté nastavte Retenční politiku, dny nebo restore pointy.



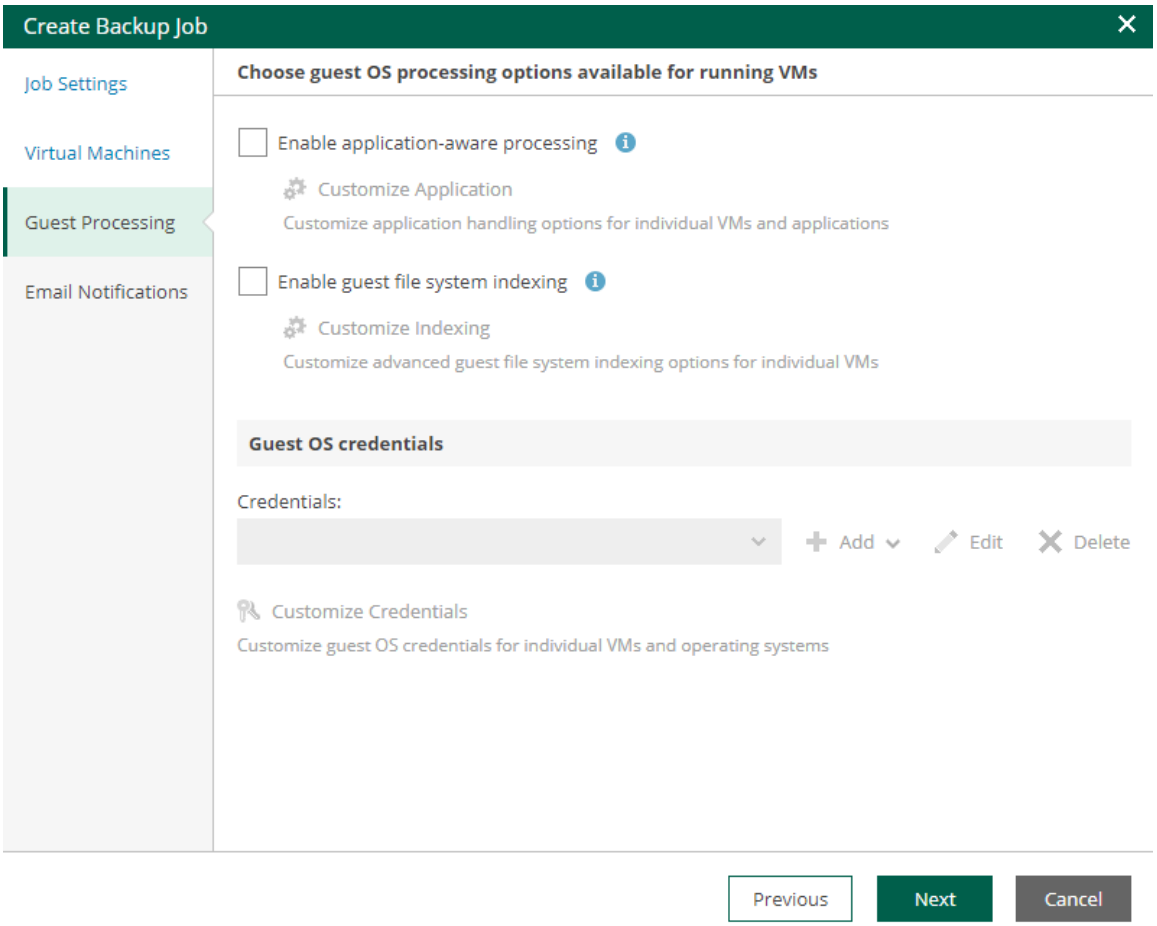
Vyberte vDC, nebo vAppu nebo jednotlivé virtuální servery, podle toho co požadujete zálohovat



Vybrané objekty k zálohování



Dále je možno nastavit **aware processing** nebo **indexaci** – vyžaduje přístup do OS serveru.

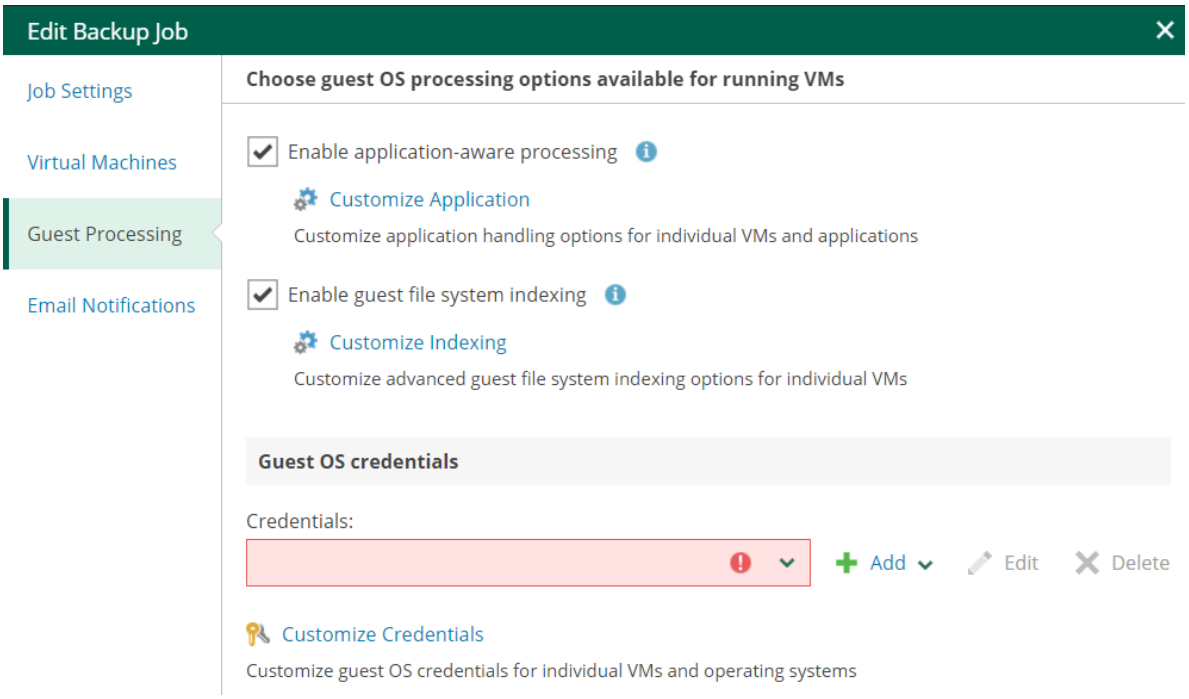


Zapnete-li aware processing nebo indexaci, je potřeba vytvořit servisní Veeam účet například „veeambackup“ (doménový nebo lokální), zavést jej do Credentials ve Veeamu a nastavit jej jako lokálního administrátora zálohovaného serveru + provést další konfiguraci serveru. Nastavení je popsáno v následující kapitole.

Aware processing:

Detects and prepares applications for consistent backup performs transaction logs processing and configures the OS to perform required restore steps upon first boot.

Poznámka: (pouze pro zákazníky migrované z verze Veeam 11 na Veeam 12).
Pokud požadujete v zálohovací úloze změnit notifikační email a zálohovací úloha má aktivní Guest Processingem, tak musíte znovu definovat účet pro Guest Processing, jinak nelze změnu notifikačního emailu dokončit a jsou tak vyžadovány Credentials.



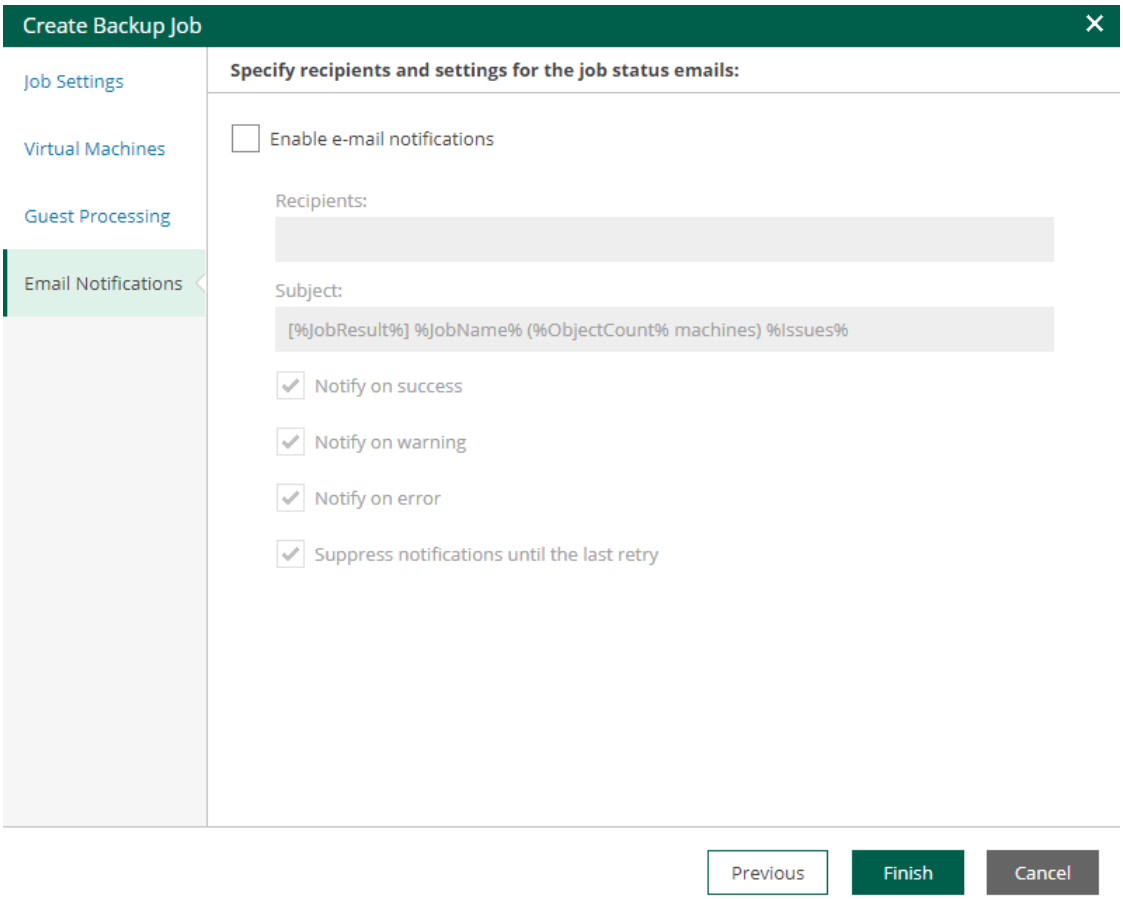
Pokud přístupové jméno a heslo stávajícího servisního účtu neznáte, vytvořte si přes tlačítko „Add“ nový účet, který následně nastavte na všech serverech, kde využíváte Guest Processing.

Indexace:

Indexes guest OS files inside processed VM to enable browsing and searching for guest files in backup. Indexing is completely optional, and not required to be able to perform instant file level recovery.

V dalším kroku je možno specifikovat notifikace zasílané na email(y) o stavu záloh a pak kliknout na Finish.

V případě specifikace více emailových adres, jednotlivé od sebe oddělujte středníkem.



Po vytvoření zálohovací úlohy Veeam přidělí automaticky čas, kdy bude zálohovací úloha spouštěna.

Pokud následně provedete jakoukoliv změnu v existující zálohovací úloze, může dojít k přeplánování času spouštění úlohy.
Tento čas se nezmění do doby další editace zálohovací úlohy. Pokud nebude zálohovací úloha editována, bude zálohování prováděno pravidelně ve stejný čas.

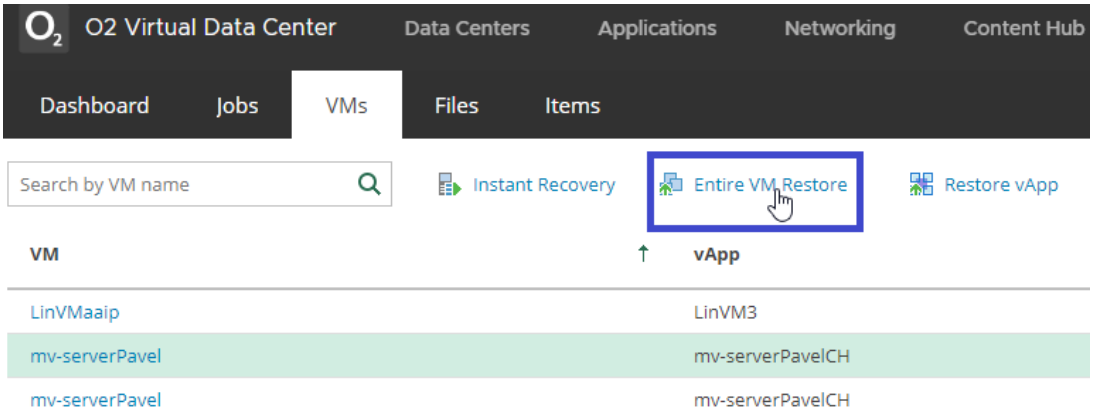
14.3 Obnova virtuálního serveru

Před obnovou serveru zkontrolujte, zda-li máte dostatek volných prostředků (vCPU vDC, vRAM vDC, Storage vDC) pro obnovovaný server v daném vDC, do kterého se má server obnovit.

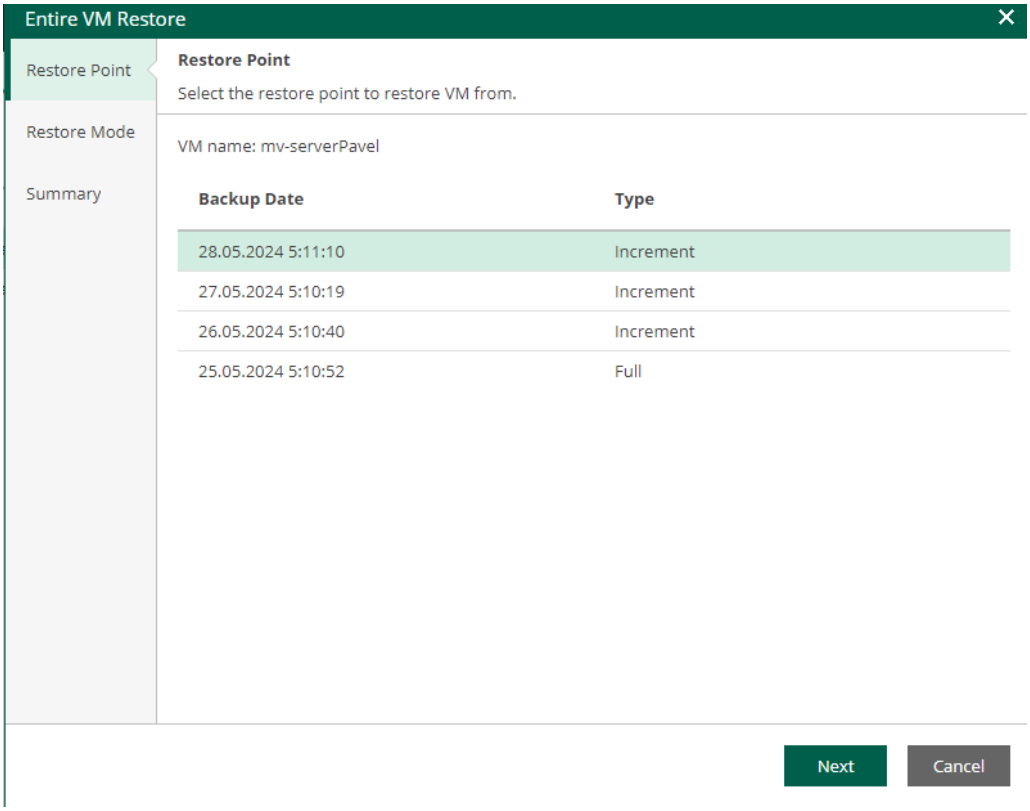
V případě, že není dostatek volných prostředků si je přes Service Library, (kapitola 13), můžete navýšit.

Kliknutím na **VMs** se zobrazí seznam zálohovaných serverů.

Označte server, který požadujete obnovit a zvolte **Entire VM Restore** (obnovit celé VM).



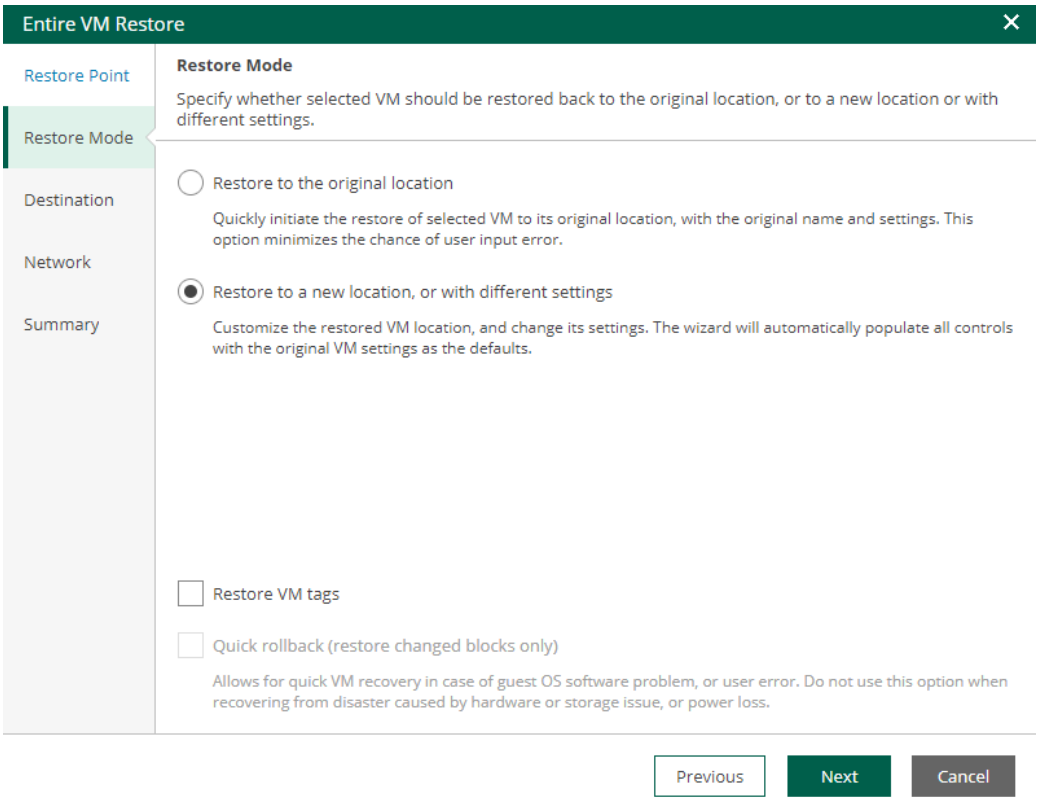
Dále, vyberte k jakému **datu a čas**u požadujete **VM obnovit**



Dále specifikujte mód obnovy.

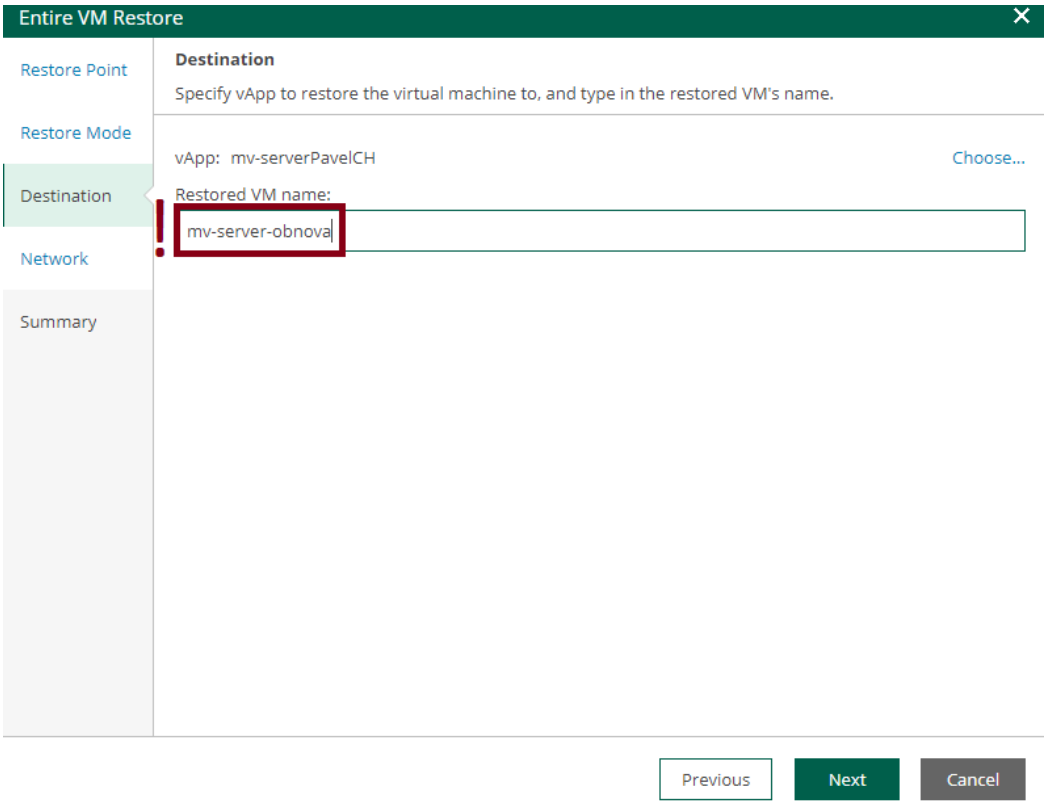
Restore to the original location: obnovovaný server **NAHRADÍ** existující VM server v O2 Cloudu

Restore to new location, or with different settings: obnovovaný server **NENAHRADÍ** existující VM v O2 Cloudu a server bude obnoven vedle stávajícího. (původní server zůstává bezezměny).
(pro příklad volíme obnovu VM vedle stávajícího serveru).

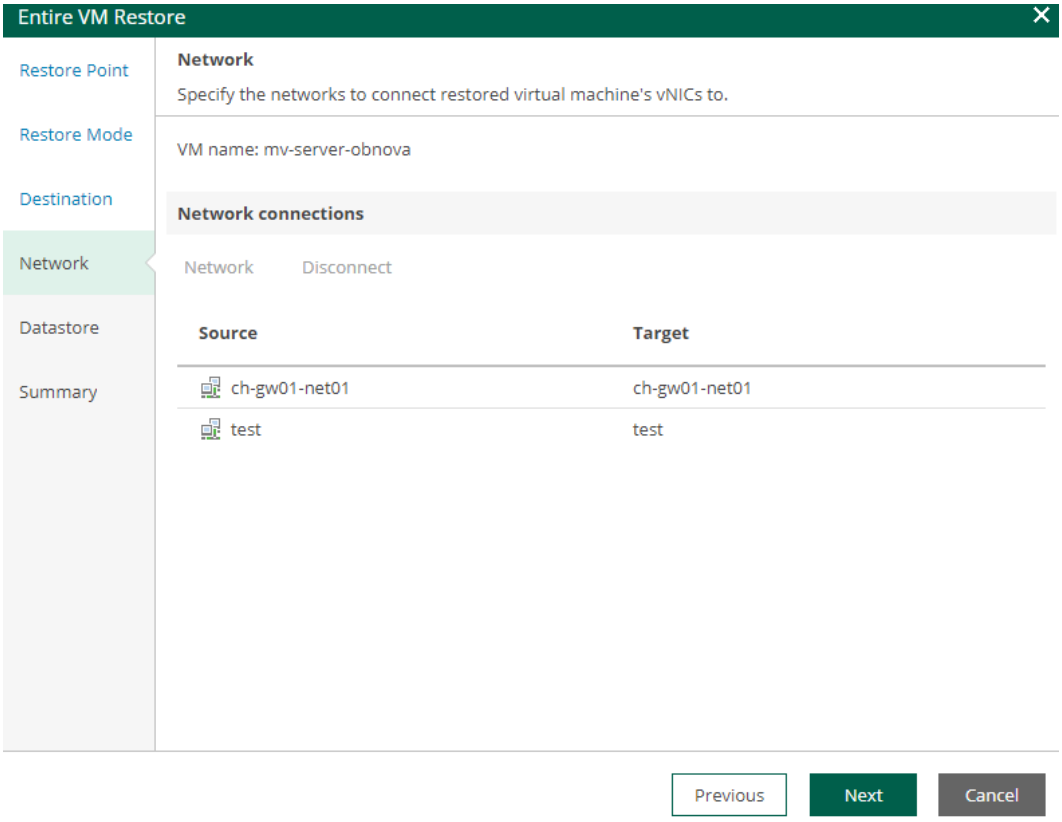


Dále specifikujte název pro obnovené VM. Název se **nesmí shodovat s původním názvem serveru**,

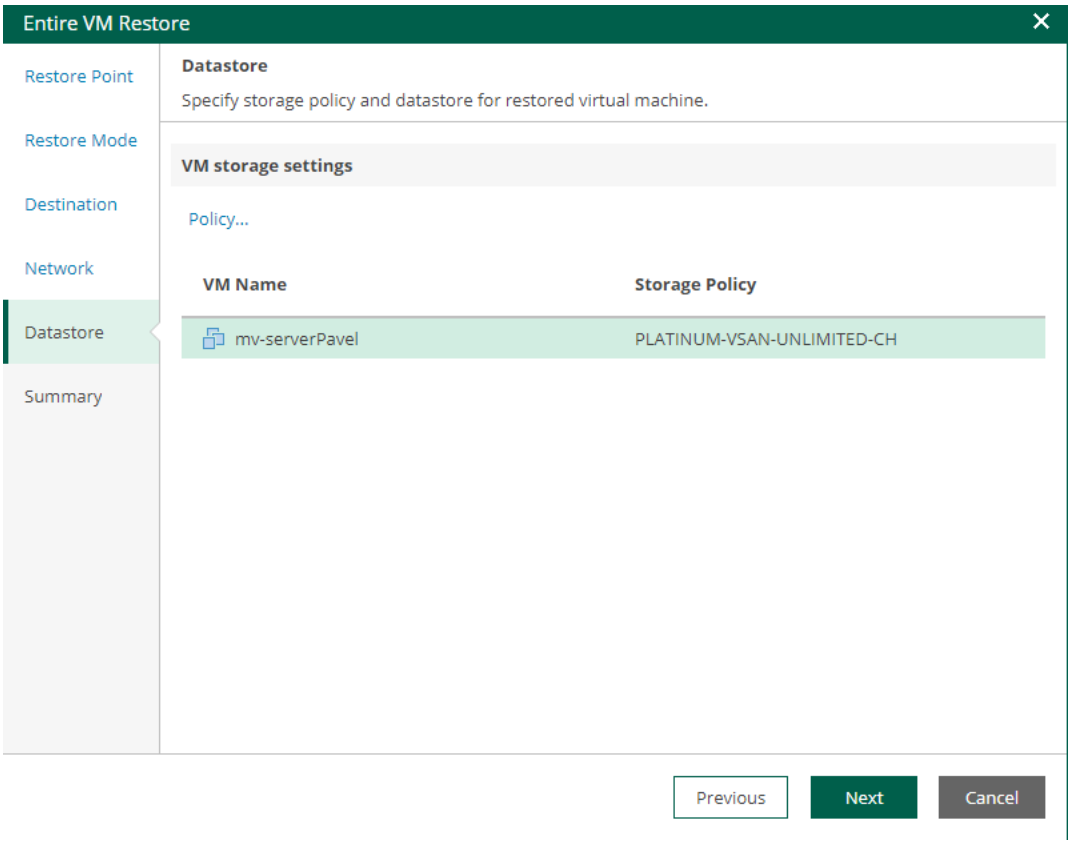
jinak obnovený server nahradí původní.



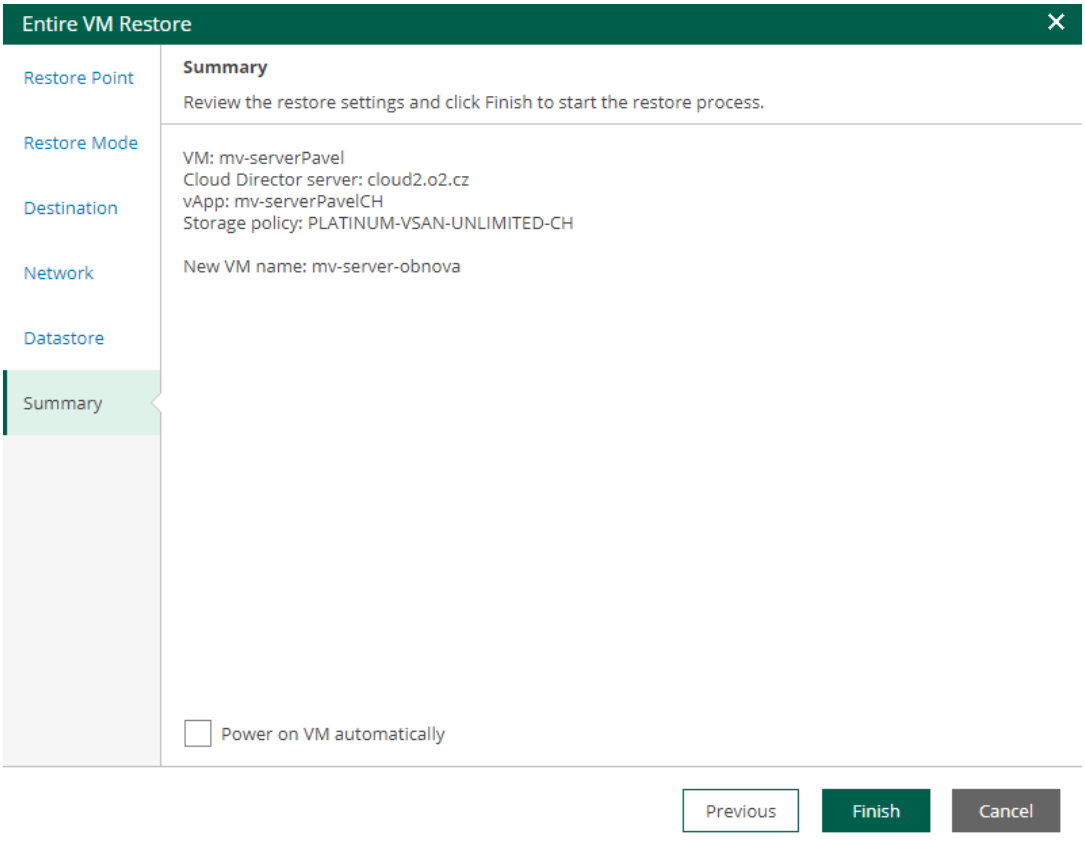
Zde můžete specifikovat jaké sítě mají být k obnovovanému serveru připojeny, případně můžete ponechat sítě odpojené (disconnect) a připojit si je dodatečně po obnově serveru.



Kliknutím na Policy vyberte uložiště pro obnovovaný server.

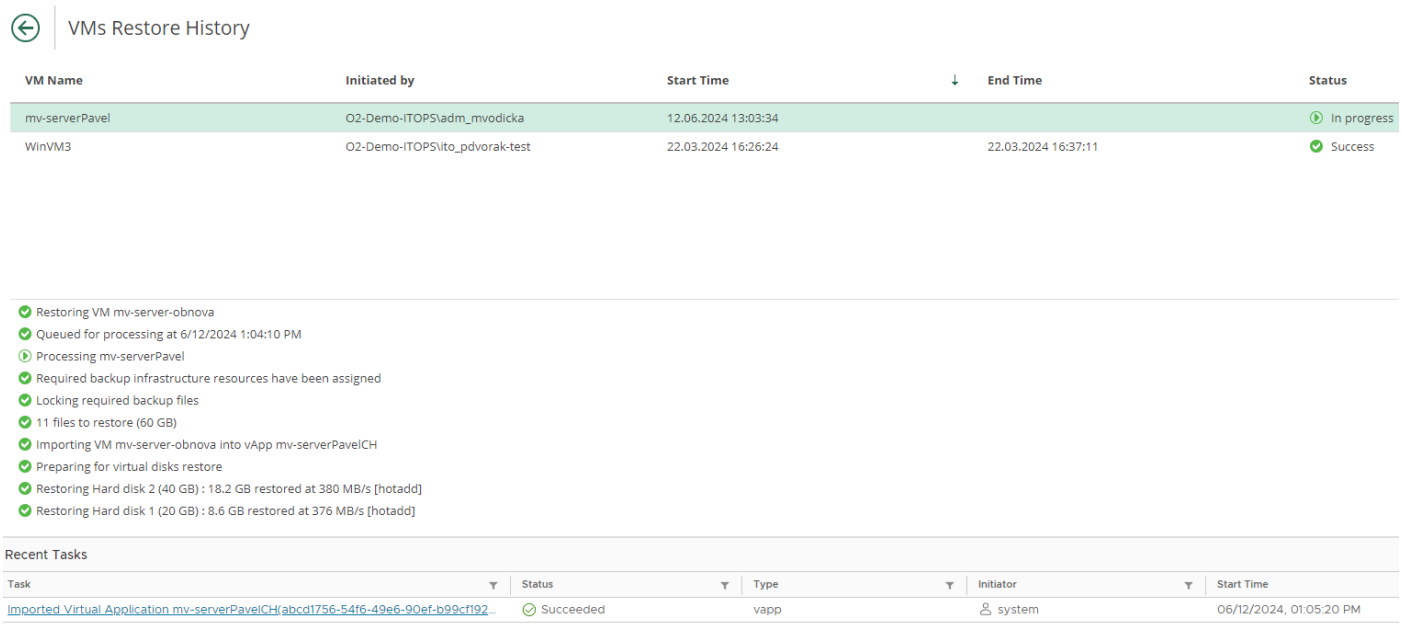


Následně se zobrazí souhrn zvolených nastavení, tlačítkem **Finish** zahájíte obnovu serveru. Níže ještě můžete vybrat, zda-li se má obnovený server po obnově spustit či nikoli.



Kliknutím na **History** můžete sledovat průběh obnovy. Po dokončení obnovy (status **Success**) se Vám server

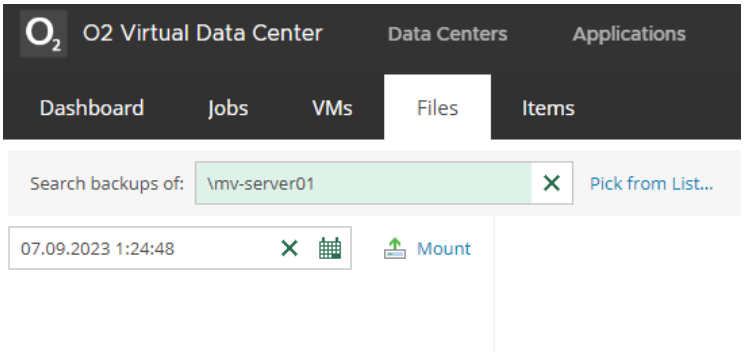
obnoví v prostředí Vaší organizace.



14.4 Obnova adresáře nebo souboru

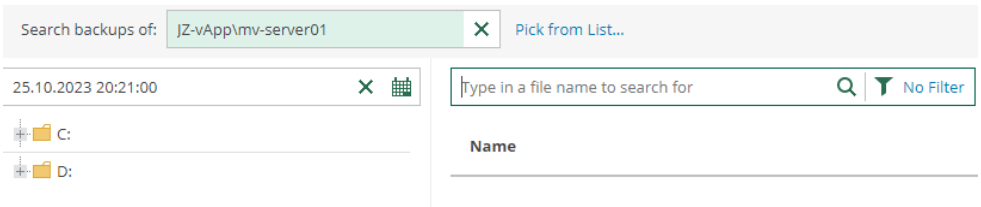
Kliknutím na **Files** a vyhledání názvu serveru a níže prostřednictvím **kalendáře** vyberte **zálohu**

a tlačítkem **Mount** se načte ze zvolené zálohy struktura adresářů a souborů.

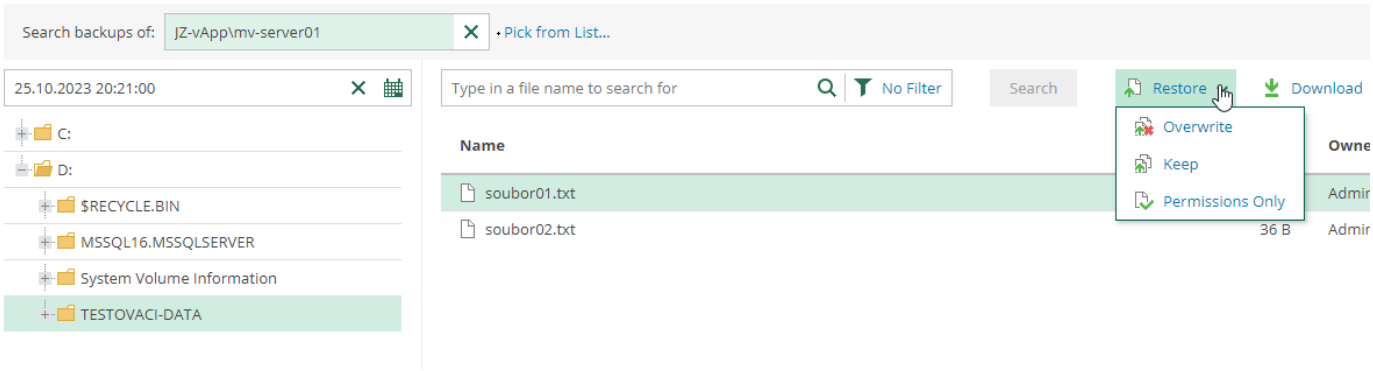


Po načtení zálohy je zobrazen seznam adresářů a souborů.

Adresář nebo soubor je možné vyhledat pomocí vyhledávacího pole:



Vyberte adresář nebo soubor, který požadujete obnovit a klikněte na Restore.



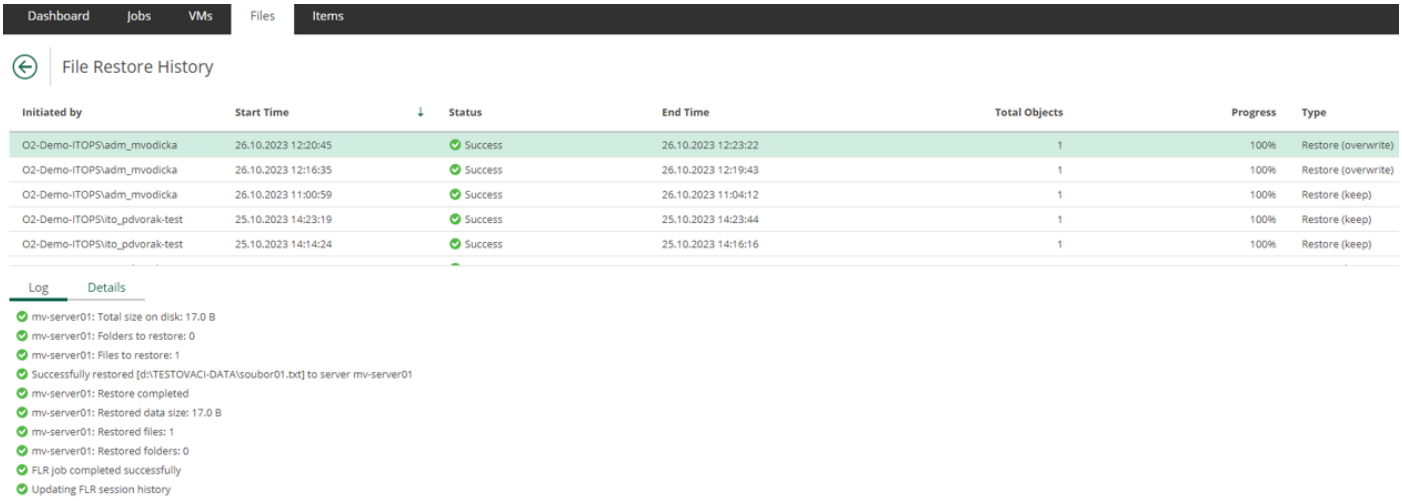
Možnosti obnovy jsou následující:

Overwrite – přepíše ze zálohy obnovovaný objekt (adresář nebo soubor, podle toho, co je vybráno k obnově) na cílovém serveru

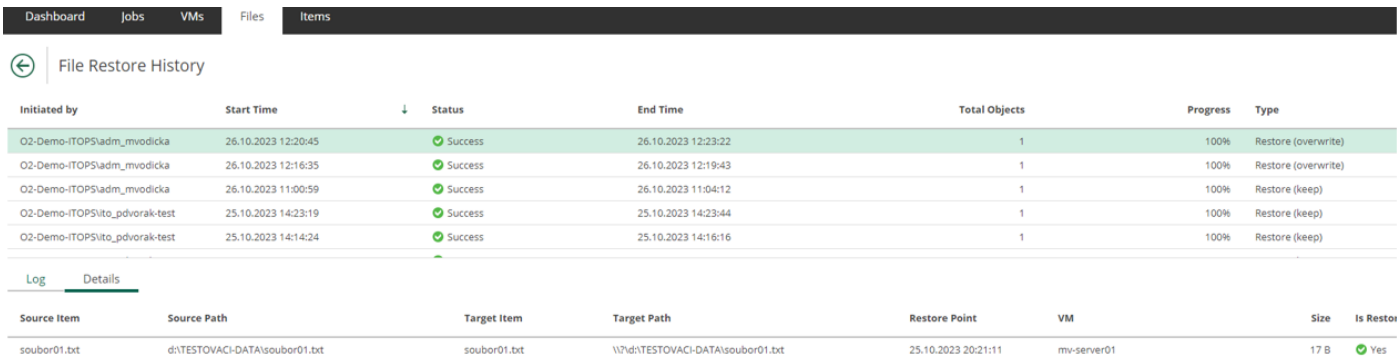
Keep – zachová obnovovaný objekt (adresář nebo soubor, podle toho co je vybráno k obnově) a doplní postfix **RESTORED_DATUM_ZÁLOHY**

Permissions Only – obnoví pouze oprávnění obnovovaného objektu

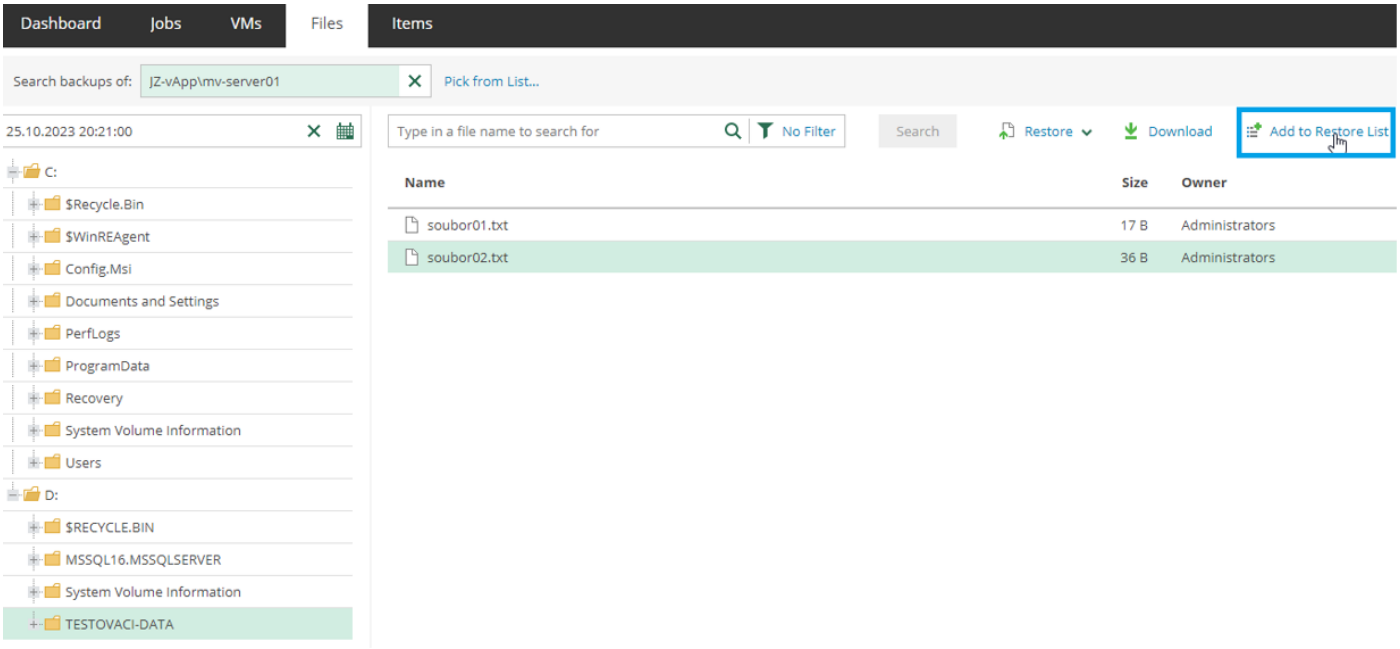
Po vybrání objektu k obnově se zobrazí informace o průběhu obnovy s typem, jaký byl vybrán.



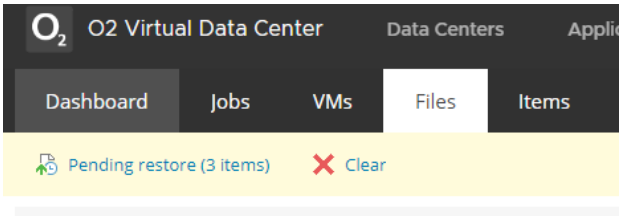
V pohledu **Details** je detailní přehled o tom co bylo **s jakým typem obnovy**, **obnoveno**.



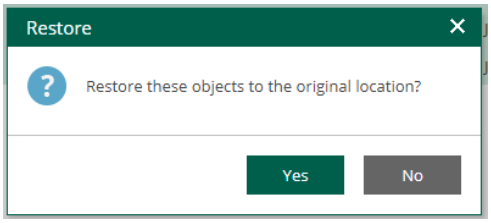
Hromadnou obnovu objektů (adresář nebo soubor), je možno provést označením adresáře nebo souboru a následně kliknutím na **Add to Restore List**.



Následně se zobrazí čekající objekty k obnově:

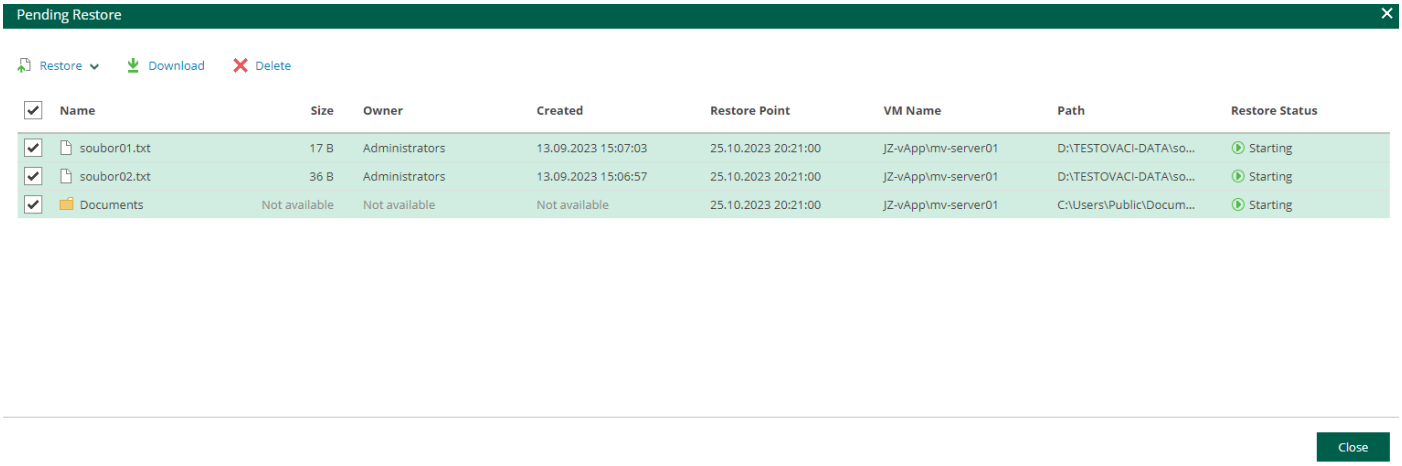


Vyberte **typ obnovy** a potvrďte **YES**.

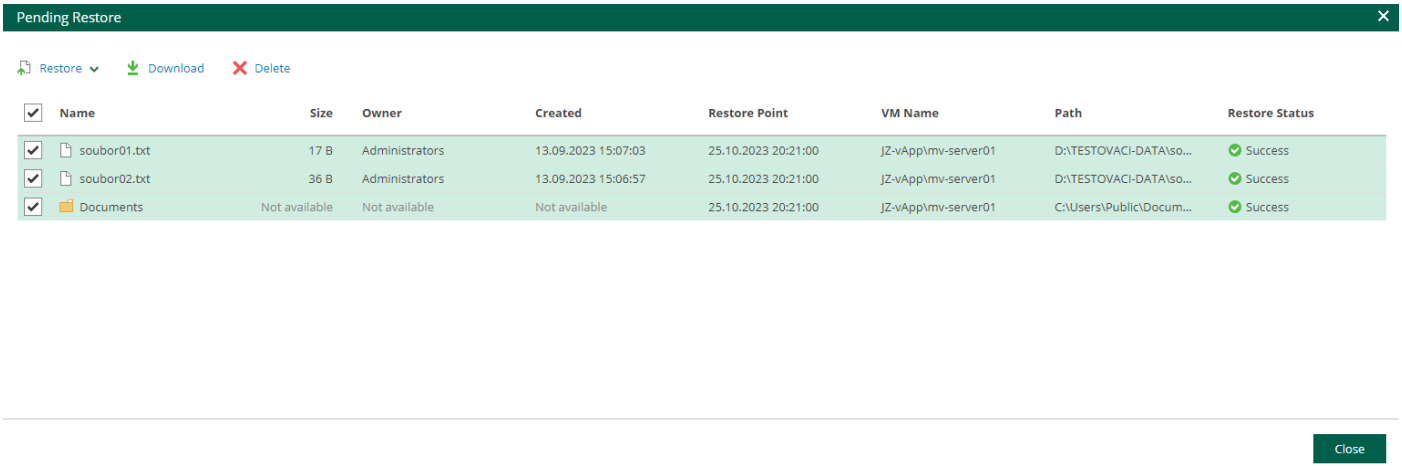


Pro příklad byl vybrán typ obnovy s přepsáním v originálním umístění:

Následně je zobrazen průběh obnovy.

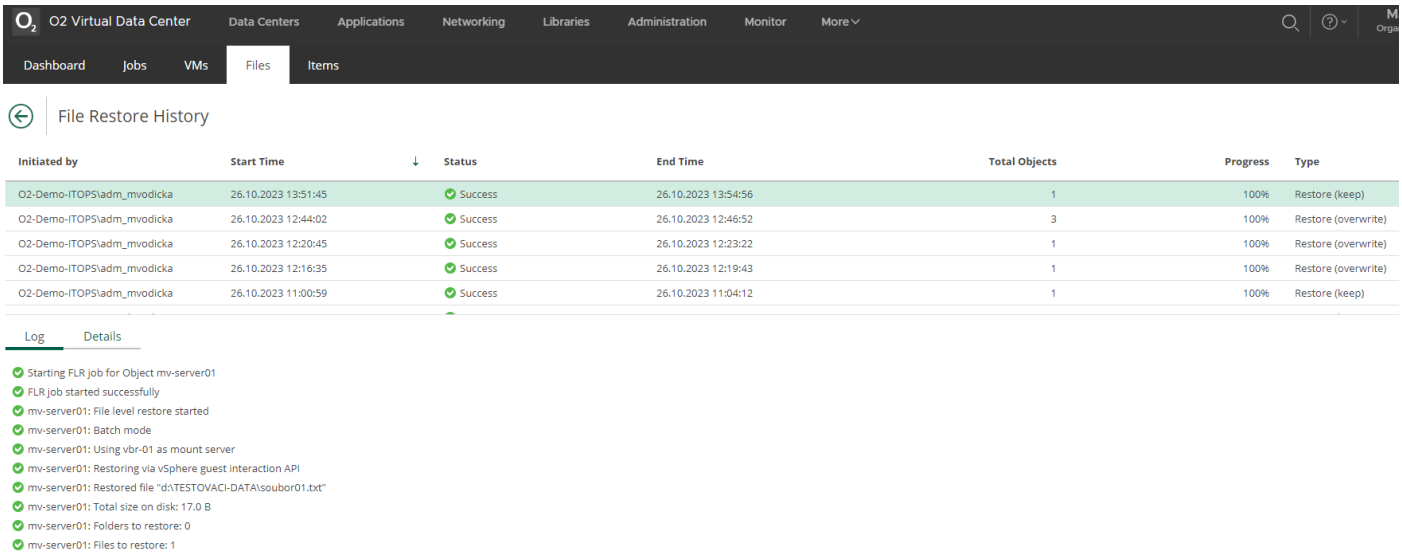


Dokončení obnovovaných objektů



Dále je možno stáhnout obnovovaný objekt do lokálního počítače „k sobě“ kliknutím na **Download**.

Kliknutím na **History** se zobrazí přehled obnov včetně detailního pohledu.



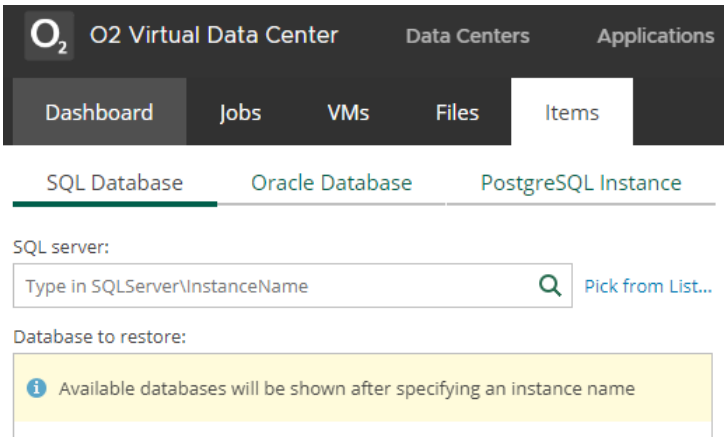
14.5 Obnova databáze

Možnost obnovy databází máte pouze v případě, že jste si aktivoval backup přes IPv6,
viz kapitola 15: Zapnutí backupu na vnic přes IPv6.

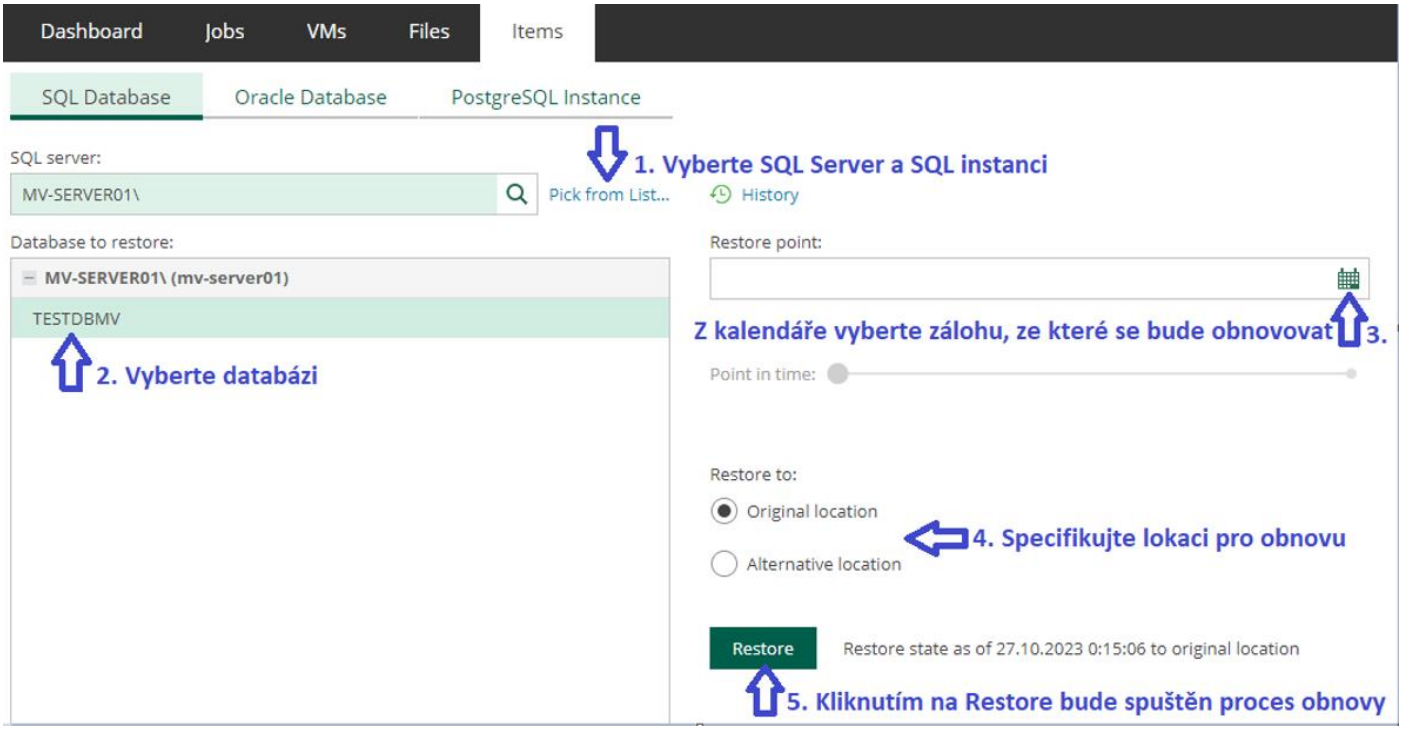
V opačném případě je potřeba, abyste zadal(a) požadavek přes ITSM systém nebo kontaktoval SD.

K obnově databází je zapotřebí mít v datacentru na zálohovaném VM dostupnou backup IPv6 síť, jinak nebude obnova databází na cílový server možná. Pro připojení backup IPv6 sítě do Vašeho datacentra zadejte prosím požadavek.

Kliknutím na **Items** je možno obnovovat databáze **SQL**, **Oracle** a **Postgre**.
Specifikujte název serveru nebo vyberte server z Pick from List …



SQL Database – postup obnovy:



Dále specifikujte níže uvedené nastavení obnovy:

Server Name: **zadejte IPv6 backup adresu cílového serveru**, do kterého požadujete obnovit databázi (nikoliv doménové jméno nebo IPv4 adresu)

User Name: servisní Veeam účet – účet s oprávněním **lokálního administrátora v rámci OS**, který má dále roli **sysadmin** = přístup na všechny DB v rámci MS SQL, takže **není potřeba specifikovat** v poli *„Use the following credentials to access the database“* přístup do DB).

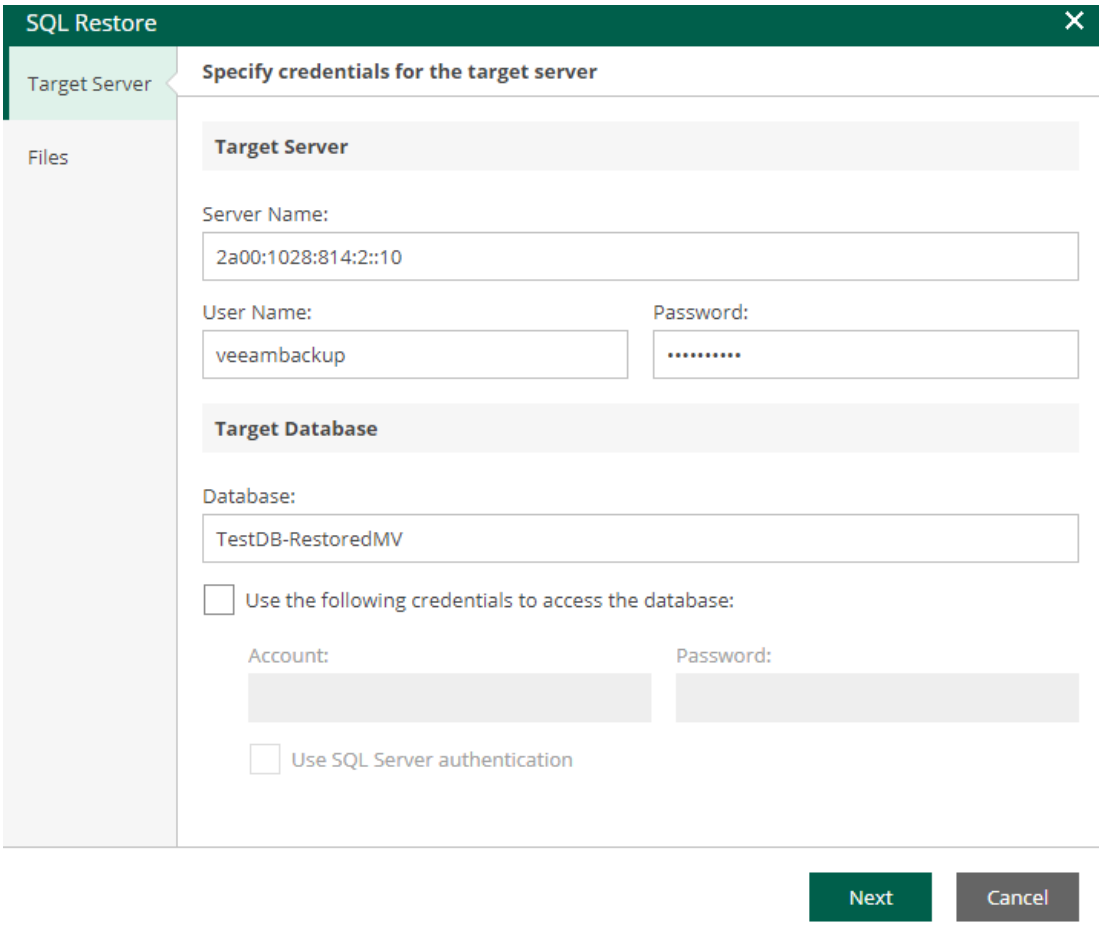
Poznámka:
Pokud je doménový účet, tak specifikujte tvar: d*oména\účet*
Pokud se jedná o lokální účet, tak specifikujte ve tvaru: *účet* nebo název *serveru\účet* nebo *.\účet*

Password: zadejte heslo pro tento účet

Database: název DB po obnově - pokud ponecháte shodný název DB na shodném serveru, **původní DB bude přepsána !**

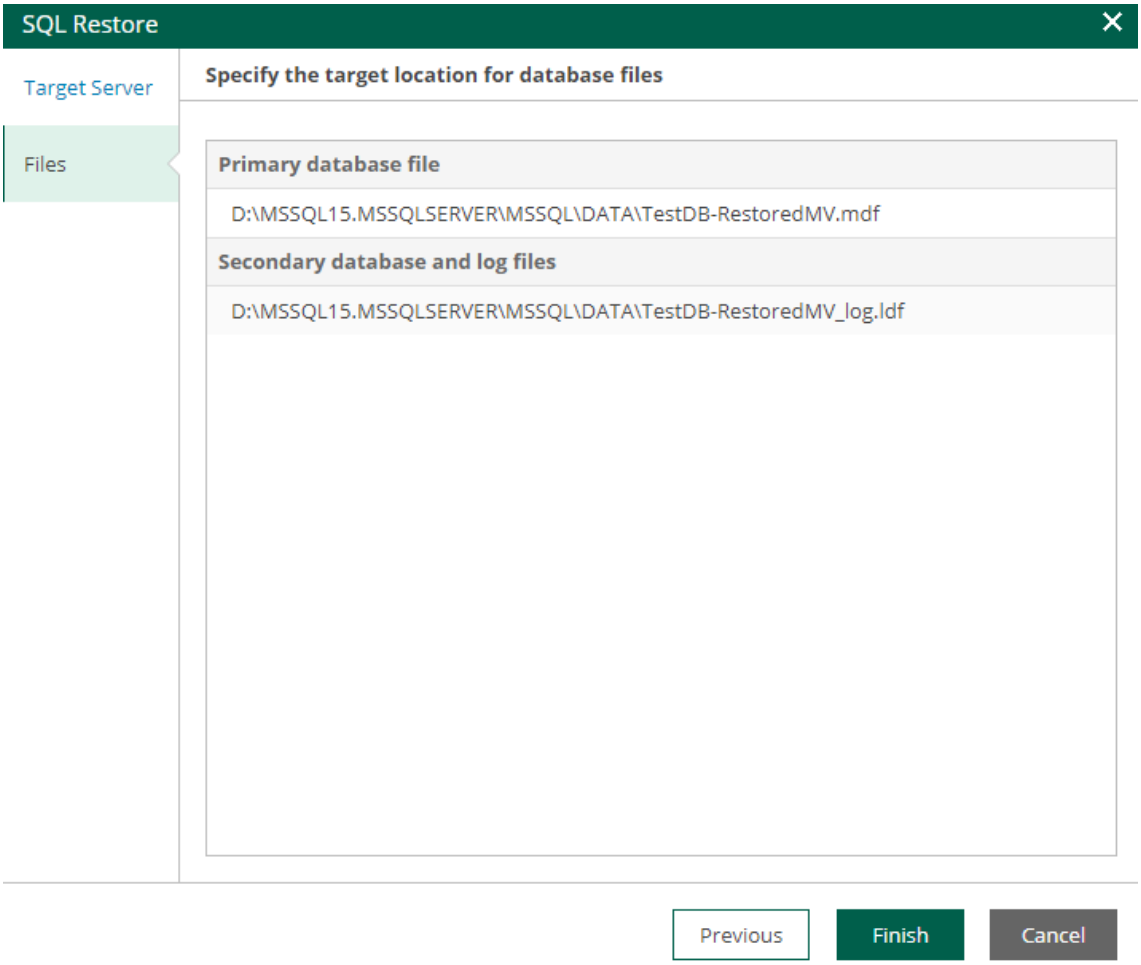
Dále pokračujte tlačítkem **Next**.

Ilustrativní příklad je uveden níže, pokračuje po té tlačítkem **NEXT**



Zobrazí se název datového souboru a název logového souboru databáze k obnově.
Pokud požadujete obnovit DB pod jiným názvem, tak je potřeba změnit název jak datového tak logového souboru na jiný název, než je původní, například „restored“, aby se nepřepsaly původní soubory reprezentující DB.

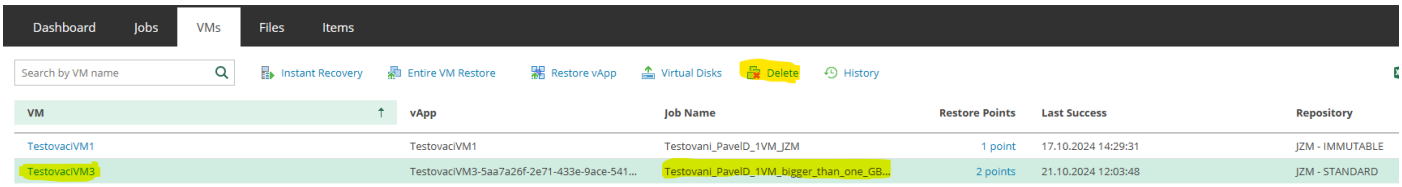
V případě přepisu stávající databáze můžete ponechat původní soubory reprezentující DB.
Kliknutím na FINISH zahájíte process obnovy DB.



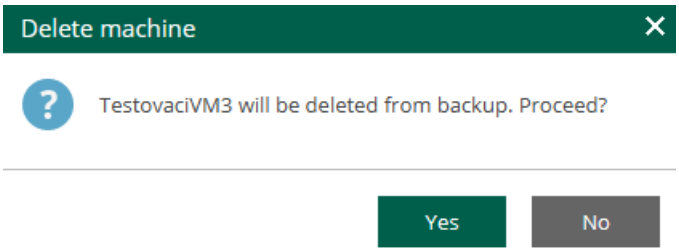
Poté se zobrazí proces obnovy.
Obnovená DB po dokončení obnovy bude k dispozici v MS SQL.

14.6 Smazání zálohy serveru

Vyberete zálohu serveru z odpovídajícího backup jobu -> **Delete**



Zobrazí se dialogové okno pro potvrzení smazání záloh VM -> **Yes**



A záloha daného VM ze seznamu zálohovaných VM zmizí.

Poznámka:

Pokud se bude jednat o VM se zálohou umístěnou na repozitáři “JZM – IMMUTABLE” nebo “CHODOV - IMMUTABLE”, nedojde po smazání záloh k odstranění VM ze seznamu zálohovaných VM okamžitě, ale až po 30 dnech.

15 Zapnutí backupu na vnic přes IPv6

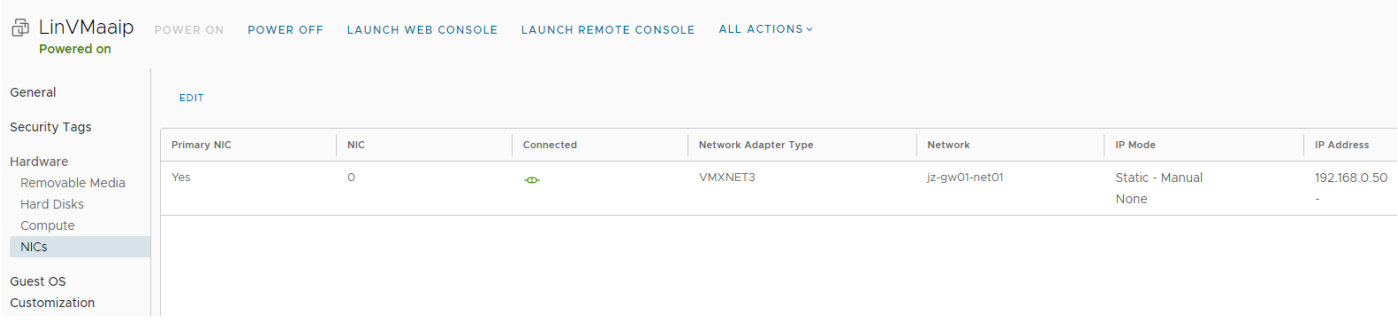
V prostředí O2 Cloud existují dva zálohovací scénáře.

Používá se pro urychlení záloh a obnovu VM s aktivním App-aware processingem nebo indexací, tím je zajištěno, že zálohování neprobíhá pomaleji přes komponentu VIX, ale rychleji přes backup rozhraní. Zároveň vám umožňuje obnovovat databáze přes VBEM (Veeam Backp Enterprise Manager) a to bez součinnosti O2 ITS. V opačném případě je potřeba pro obnovu DB založit požadavek nebo kontaktovat Servicedesk, kontakty jsou uvedeny na poslední straně.

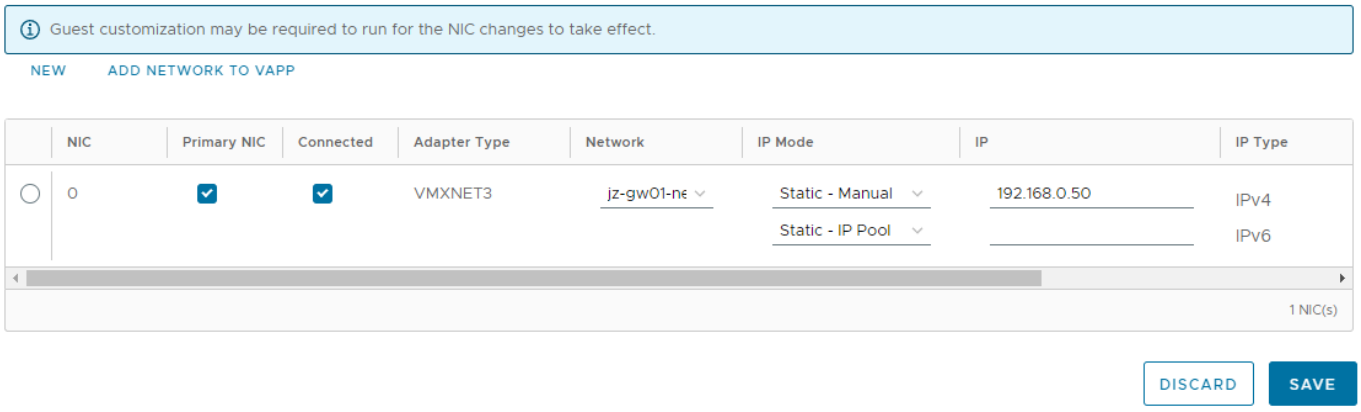
15.1 Virtuální server má jednu síťovou kartu připojenou do privátní sítě, která je připojená jako typ routed do EdgeGW. (nikoli síť typu direct).

Je potřeba provést IP adresaci IPv6 na úrovni vCloud Directoru a OS.

Rozklikněte VM, pak přejděte na NIC, ve výchozím nastavení je přidělena pouze IPv4.

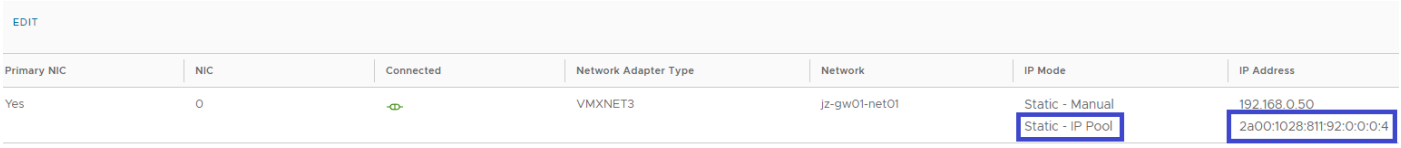


Klikněte na **EDIT** a pro IPv6 zvolte **IP Mode Static IP Pool a klikněte na SAVE.**



Tím se Vám ze statického IPv6 poolu **přidělí IPv6 adresa**, a tuto adresu **musíte ručně zadat pro IPv6 adresaci v OS**. (Automaticky se z vCloud Directoru nepropisuje).

Po uložení se vám IPv6 zobrazí, příklad je uveden níže:



Masku sítě a **Gateway** najdete po kliknutí na **Networks**, rozkliknutí **dané org sítě**, po té klikněte na **Static IP Pools** a v sekci **IPv6** je viditelná **IP adresa Gateway CIDR.**

DNS pro IPv6 jsou:

Primární: *2a00:1028:1:910::1*

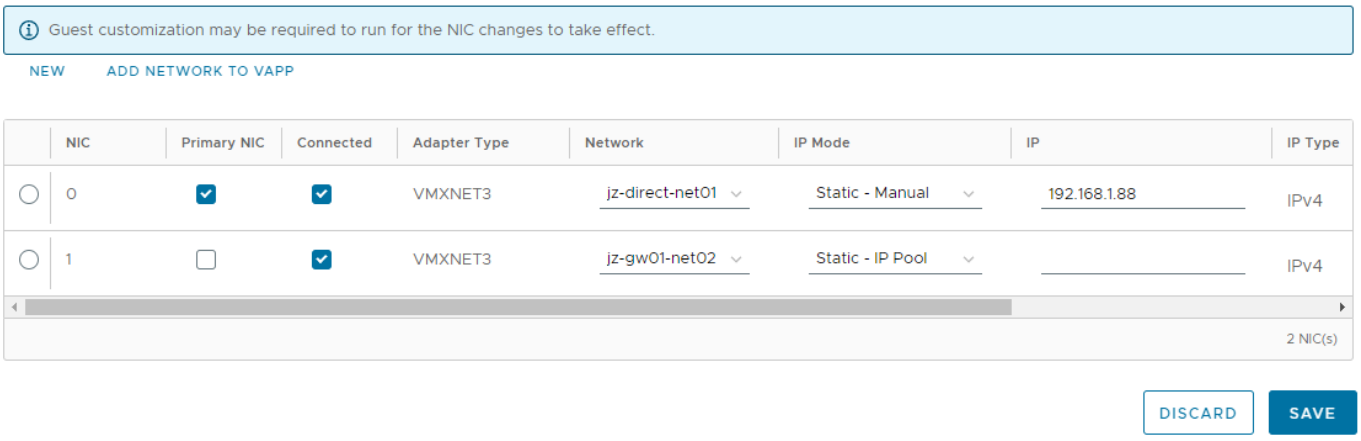
Sekundární: *2a00:1028:1:911::1*

15.2 Scénář, kdy má virtuální server jednu síťovou kartu připojenou do privátní sítě, která není připojená do EdgeGW a je to typ sítě direct (síť PT5, nikoli síť typu routed).

Je potřeba přidat k VM novou síťovou kartu a provést IP adresaci IPv6 na úrovni vCloud Directoru a OS.

Před připojením sítě k VM, je potřeba jí nejprve přidat do vAppy, (ve které se VM nachází) jako typ direct. V opačném případě se vám daná síť nezobrazí v seznamu při konfiguraci NIC.

Rozklikněte VM, pak přejděte na **NIC** a kliknout na tlačítko **EDIT**.
Ke stávající síťové kartě přidejte přes tlačítko **NEW** novou síťovou kartu, vyberte routovanou síť, tj. síť, která je připojená do EdgeGW (nikoliv direct síť typu PT5), IP Mode pro IPv4 zvolte **None** a pro **IPv6** zvolte **Static IP Pool** a typ adaptéru doporučujeme **VMXNET3.**



Po uložení je konfigurace následující:

Pro nově přidanou virtuální síťovou kartu proveďte IPv6 IP adresaci v OS.
(Automaticky se z vCloud Directoru nepropisuje do OS).

EDIT

Primary NIC	NIC	Connected	Network Adapter Type	Network	IP Mode	IP Address
Yes	0		VMXNET3	jz-direct-net01	Static - Manual	192.168.1.88
	1		VMXNET3	jz-gw01-net02	Static - IP Pool	192.168.1.100

Masku sítě a **Gateway** najdete po kliknutí na **Networks**, rozkliknutí **dané org sítě**, po té klikněte na **Static IP Pools** a v sekci **IPv6** je viditelná **IP adresa Gateway CIDR.**

DNS pro IPv6 jsou:

Primární: *2a00:1028:1:910::1*

Sekundární: *2a00:1028:1:911::1*

Pro správnou funkčnost zálohování přes backup IPv6 interface je potřeba, aby bylo nastaveno v EdgeGW definované pravidlo povolující icmp pro IPv6ku. Nestačí jen IPv4.

#	Name	Category	State	Applications	Context	Source	Destination	Action	Applied To	IP Protocol
1	o2_backup	User defined	Active	-	-	o2_backup	o2_backup_internal_networks	Allow	-	IPv6
2	icmp	User defined	Active	ICMP ALL	-	Any	Any	Allow	-	IPv4 and IPv6
3	external	User defined	Active	-	-	external_networks	internal_networks	Allow	-	IPv4 and IPv6
4	private	User defined	Active	-	-	internal_networks	private_networks	Drop	-	IPv4 and IPv6
5	int_to_ext_for_snat	User defined	Active	-	-	internal_networks	Any	Allow	-	IPv4 and IPv6
	default_rule	Default	Active	-	-	Any	Any	Drop	-	IPv4 and IPv6

Zároveň je potřeba, aby byl povolený provoz ze **všech interních routovaných LAN sítí** v **O2 cloudu** reprezentovaných statickou „member grupou“ „**internal_networks**“ kamkoliv.

#	Name	Category	State	Applications	Source	Destination	Action	IP Protocol
1	o2_backup	User defined	Enabled	-	o2_backup	o2_backup_internal_netw...	Allow	IPv6
2	icmp	User defined	Enabled	ICMP ALL	Any	Any	Allow	IPv4 and IPv6
3	int_to_ext_for_snat	User defined	Enabled	-	internal_networks	Any	Allow	IPv4 and IPv6
	default_rule	Default	Enabled	-	Any	Any	Drop	IPv4 and IPv6

Ve statické „groupě“ **Internal Networks** pak musí být uvedené všechny routované sítě, které jsou v daném vDC.

16 Nastavení serveru pro aware processing a indexaci pro Veeam

Tento návod popisuje nutné prerequisites pro správnou funkčnost

- Guest file system indexing (indexace filesystému)

- Application-aware processing (konzistentní backup aplikace, oříznutí logů aplikace)

V první řadě je nutné nadefinovat servisní účet, pod kterým se daná indexace či application processing bude provádět. Nejoptimálnější je doménový uživatel s právy lokálního administrátora.

Pro indexaci fs požadována úroveň administrátora.
Pro backup MS SQL je požadována úroveň administrátora a sysadmin v MS SQL serveru.
Pro backup MS Exchange je požadována úroveň doménového Organization administrátora.
Pro backup Oracle je požadována úroveň sysdba.

AAIP Permissions required

	RPC	VIX
Local built-in administrator	✓	✓
Domain built-in administrator	✓	✓
Domain admin	✓	✗
Domain user with local admin permissions and EnableLUA=0*	✓	✓
Local admin	✗	✗
Local admin with EnableLUA=0* (exact-hostname\username or only username format)	✓	✓
Local admin with LocalAccountTokenFilterPolicy=1*	✓	✗
Domain user with local admin permissions	✓	✗
Domain user with local admin permissions and LocalAccountTokenFilterPolicy=1*	✓	✗

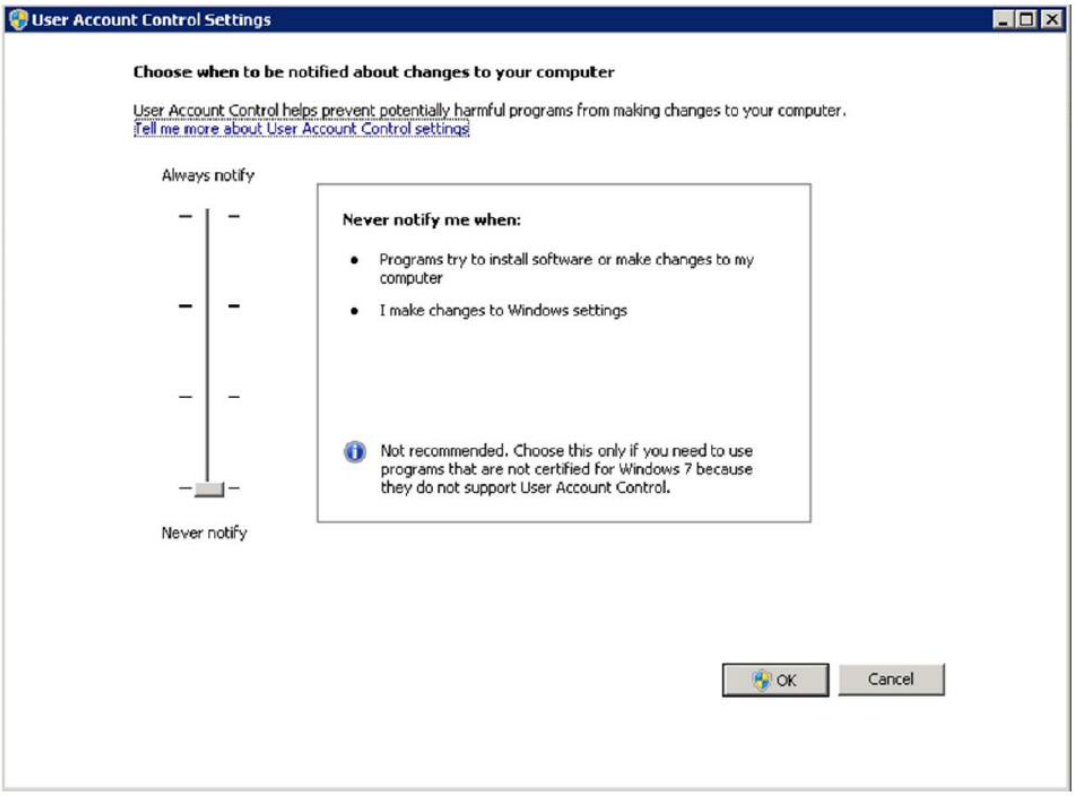
Úprava Windows systému pro eliminaci chyby „Cannot connect to the host's administrative share“:

0. Aktuální VMware Tools ve virtuálních strojích!

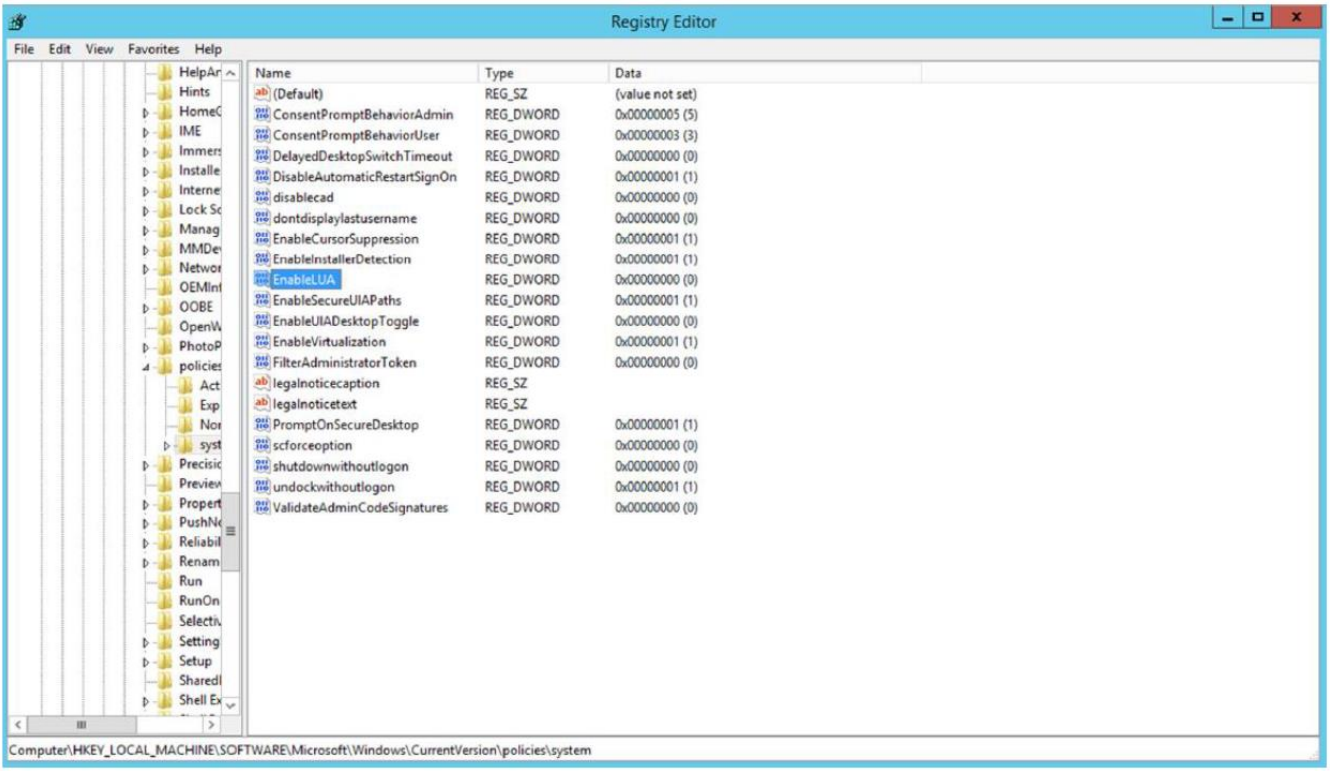
1. Ujistěte se, že je účet použitý softwarem Veeam členem skupiny „Local Administrators“ na Vašem serveru.

2. Pokud je použit účet, který se nejmenuje „Administrator“, vypněte UAC v operačním systému zálohovaného stroje:

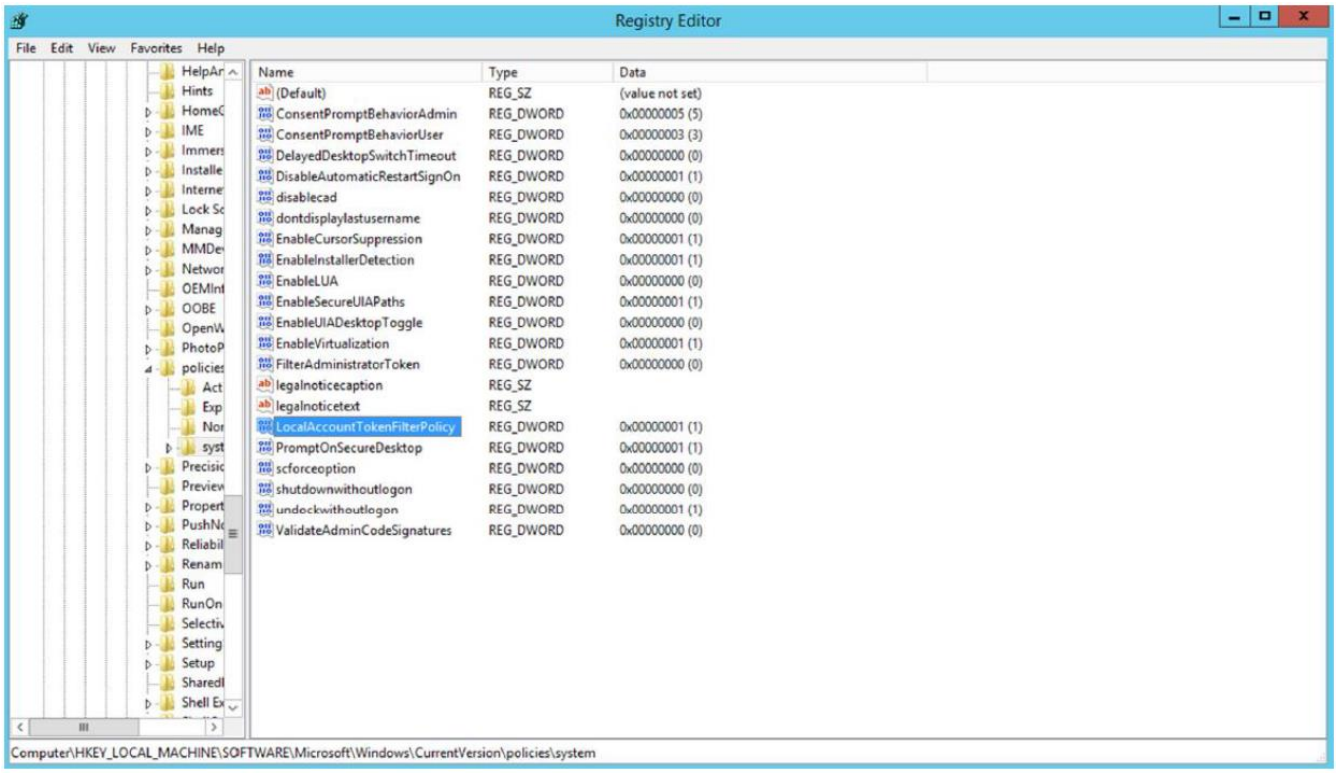
a) pro Windows Server 2008/2008R2/2012/2012R2/2016/2019 nastavte v dialogu „Change User Account Control Settings“ posuvník na „Never Notify“, viz obr.



b) pro Windows Server 2012/2012 R2/2016/2019 změňte v registru v části:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System
hodnotu klíče „EnableLUA“ na 0, viz obr.

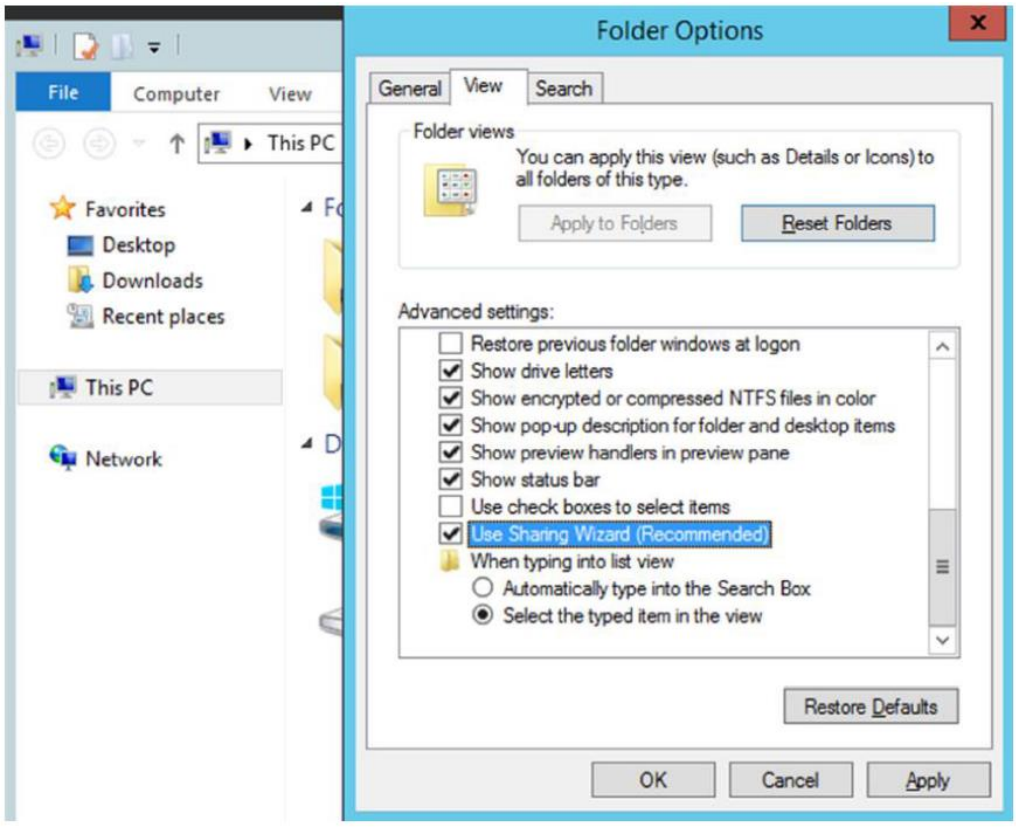


3. Změňte také v části (volitelné – potenciální bezpečnostní riziko – hash útoky):
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System
hodnotu klíče „LocalAccountTokenFilterPolicy“ na 1, viz obr.

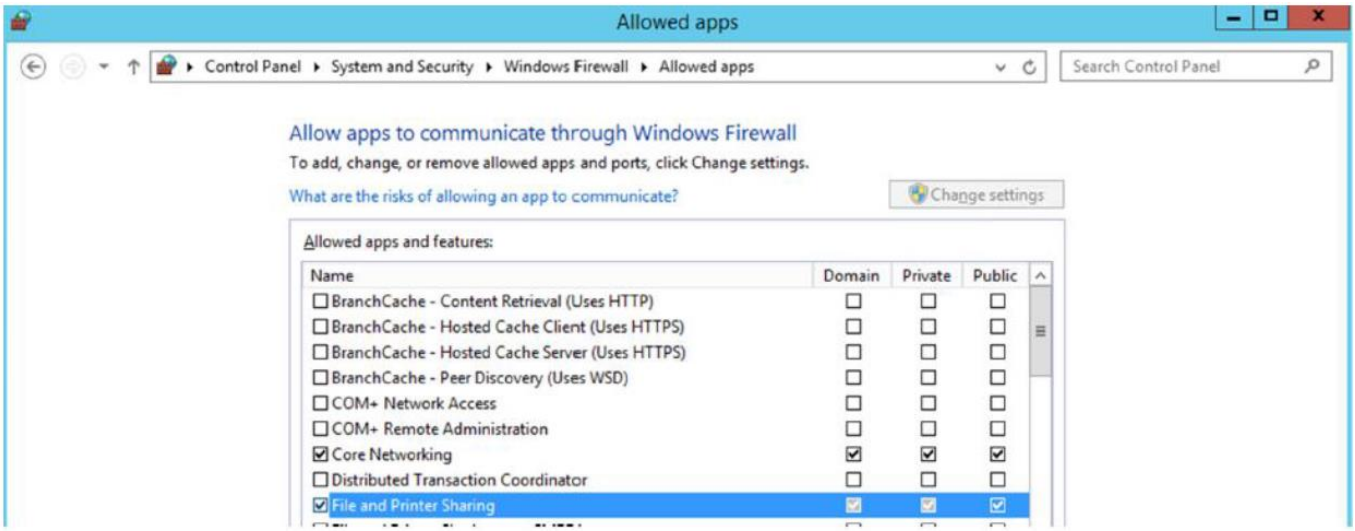


Pokud klíč neexistuje, vytvořte nový: New -> DWORD (32-bit) Value a pojmenujte ho: LocalAccountTokenFilterPolicy poté změňte hodnotu na 1.

4. Ujistěte se, že je v operačním systému povoleno „Use Sharing Wizard“, viz obr.



5. Ujistěte se, že je ve firewallu operačního systému Windows povoleno „File and Printer Sharing“ na sítích: Private a Public, viz obr.



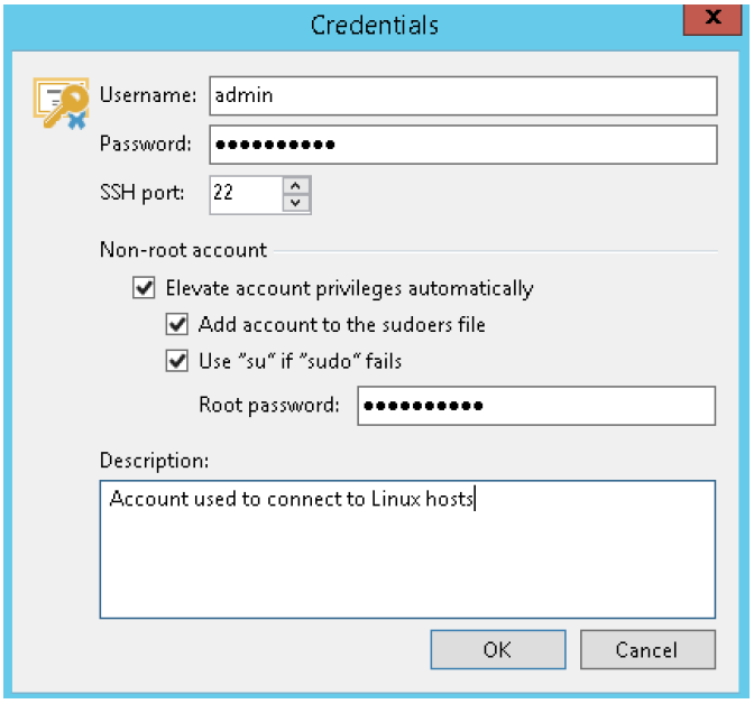
6. Proveďte restart serveru.

Úprava Linux systému pro funkční indexaci:

0. Aktuální VMware Tools ve virtuálních strojích.

1. Přítomnost balíčků openssh, mlocate, gzip a tar.

2. Ujistěte se, že účet použitý softwarem Veeam je root. Pokud chcete použít non-root účet je potřeba nastavit sudo oprávnění pro daný účet a zadat root heslo do Veeam B&R.
Př.



17 Služba O2 Zálohování PRO

17.1 Popis služby

O2 Zálohování PRO je doplňková služba služby O2 Zálohování (v rámci služeb O2 Cloud), která zvyšuje odolnost uložených dat, může přispět k plnění požadavků stanovených právními předpisy v oblasti kybernetické bezpečnosti i ochraně před ransomware útoky.

Tato doplňková služba konkrétně **umožňuje ukládat Vaše zálohovaná data ve dvou geografických lokalitách současně (GEO) a zároveň zpřístupňuje tzv. nepřepisovatelné uložiště (IMU), které znemožňuje jakoukoliv změnu či smazání v něm uložených dat po nastavenou dobu jejich neměnitelnosti, tj. 7, nebo 28 dní**. Je-li stanovená doba uchování (retence) dat kratší, než je nastavená doba jejich neměnitelnosti, jsou tato data uložena po dobu jejich neměnitelnosti a po tuto dobu jsou nepřepisovatelná a nesmazatelná. Pokud je stanovena delší doba uchování dat, než je nastavená doba jejich neměnitelnosti, přecházejí data po uplynutí doby jejich neměnitelnosti do režimu read-write.)

Imutabilní záloha - nezměnitelná po stanovenou dobu. Jakmile je vytvořena, nelze ji upravit ani smazat, což ji chrání před ransomwarem a jinými kybernetickými hrozbami. Je umístěna na nepřepisovatelném úložišti.

Neimutabilní záloha - běžná záloha, kterou lze upravit nebo smazat kdykoliv. Pokud není dostatečně chráněna, může být napadena ransomwarem, který ji zašifruje nebo smaže.

Vysvětlení imutabilní zálohy na příkladu

Pokud je imutabilita nastavena na 7 dnů a retence na 14 dnů, znamená to, že záloha bude nezměnitelná po dobu 7 dnů – během této doby ji nelze upravit ani smazat. Po uplynutí této lhůty se záloha stává editovatelnou, ale stále zůstává uložená díky retenci, která ji uchovává po celkových 14 dnů.

V praxi to znamená, že:

- Prvních 7 dnů jsou data chráněna proti jakýmkoli změnám či smazání.

- Od 8. do 14. dne už mohou být data upravena nebo odstraněna, ale stále jsou dostupná v systému.

- Po 14 dnech se záloha smaže podle nastavené politiky retence.

Po expiraci imutability se záloha stává běžnou zálohou, což znamená, že ji lze upravit nebo smazat podle nastavené politiky retence. V praxi to vypadá takto:

- Během období imutability (např. 7 dní) je záloha nezměnitelná a chráněná proti jakýmkoli úpravám či smazání.

- Po uplynutí této doby se záloha automaticky přepne na běžnou zálohu, která podléhá pravidlům retence.

- Pokud je retence nastavena na 14 dní, záloha zůstane dostupná dalších 7 dní, ale už ji lze upravit nebo odstranit.

- Po 14 dnech se záloha smaže podle nastavené politiky.

Tento model se často používá v kybernetické bezpečnosti, kde imutabilita chrání data před ransomwarem a jinými hrozbami.

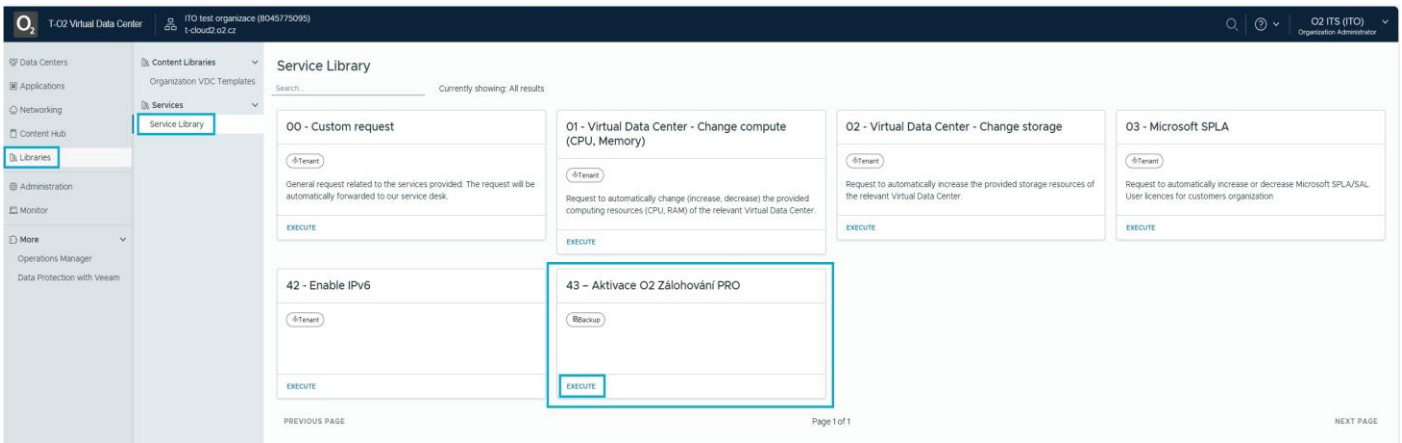
17.2 Princip zpoplatnění služby

- Aktivace služby: Samotná aktivace těchto doplňkových služeb v rozhraní nemění okamžitě stávající cenu za službu Zálohování VDC.
- Změna ceny: Změna (navýšení) ceny služby O2 Zálohování PRO nastane až tehdy, kdy skutečně se nakonfiguruje a bude se aktivně využívat ukládání záloh do více než jedné lokality současně, a to po dobu po kterou budete zálohování dat ve dvou lokalitách využívat.
- Standardní cena: Pokud jsou tyto doplňkové služby pouze aktivované, ale nadále všechny zálohy využívají pouze jednu cílovou lokalitu, bude za službu Zálohování VDC stále účtována standardní (původní) cena dle Smlouvy.
- Nová sazba: Pokud je aktivně využíváno zálohování dat do více lokalit současně, pak se na celkový objem dat zálohovaných v tomto multi-lokačním režimu (tj. na data ukládaná souhrnně do všech lokalit) uplatní nová (vyšší) sazba, a to následovně: cena za službu Zálohování VDC při využívání multi-lokačního režimu se zobrazí v aktivačním Workflow "Cena za každý GB záloh ve více lokalitách". Tato jednotková cena bude následně aplikována na celkový objem GB dat zálohovaných souhrnně ve všech využívaných lokalitách.

17.3 Způsob aktivace

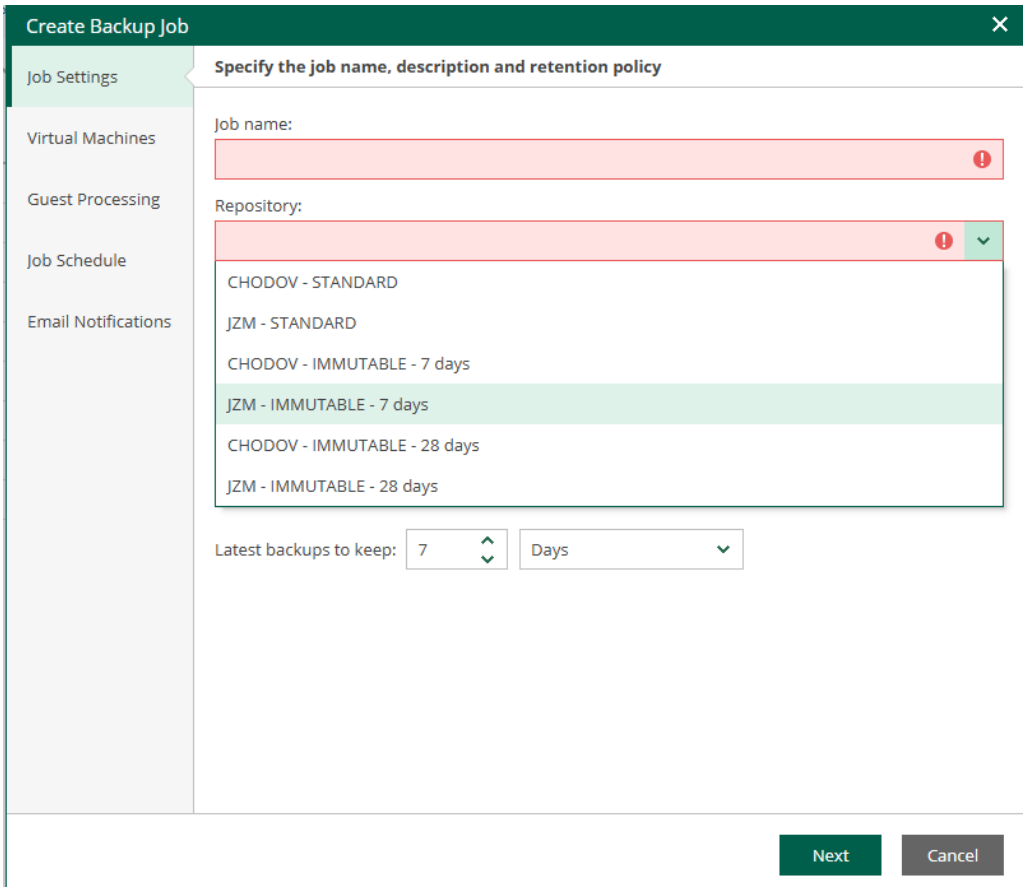
Pro aktivaci doplňkové služby O2 Zálohování PRO (GEO a IMU) se postupuje podle následujících kroků:

1. Přihlášení do vCloud Director: Přihlásit se do svého účtu ve vCloud Director.
2. Libraries -> Services -> Service Library -> 43 – Aktivace O2 Zálohování PRO -> Execute



3. Konfigurace zálohování - nakonfigurovat zálohování dle potřeb viz kapitola 14.2.

   Jedna nebo dvě lokality pro standardní uložiště
   imutabilní nebo standardní uložiště v jedné nebo dvou lokalitách.

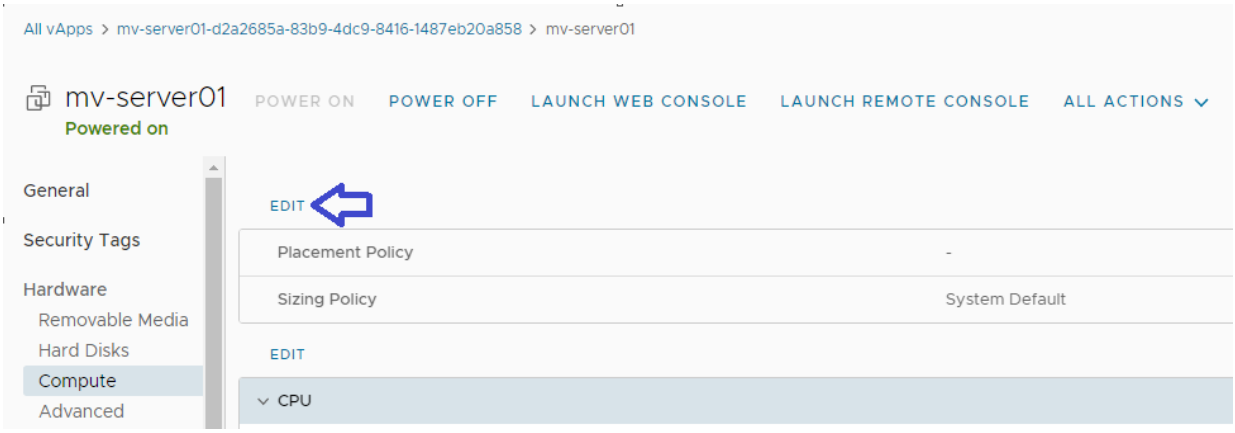

Create Backup Job
Job Settings
Virtual Machines
Guest Processing
Job Schedule
Email Notifications
Specify the job name, description and retention policy
Job name:
Repository:
CHODOV - STANDARD
JZM - STANDARD
CHODOV - IMMUTABLE - 7 days
JZM - IMMUTABLE - 7 days
CHODOV - IMMUTABLE - 28 days
JZM - IMMUTABLE - 28 days
Latest backups to keep:
7
Days
Next
Cancel

18 Cloud Voice politiky

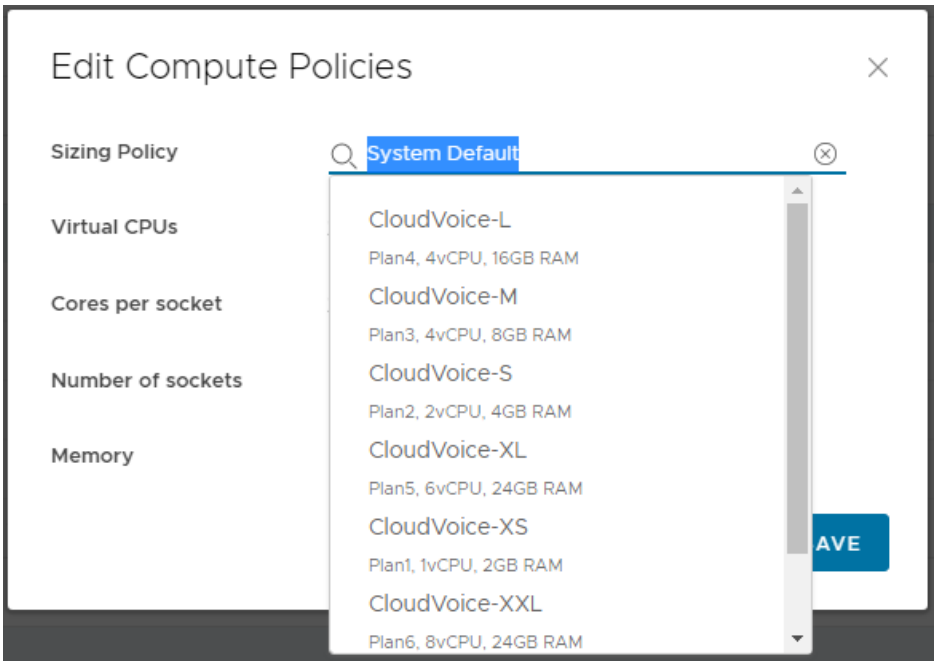
V případě, že máte ve vDC k dispozici **Cloud Voice politiky**, tak je můžete aplikovat na jednotlivé virtuální server(y) dle Vašich požadavků.

Doporučujeme ověřit kapacitu vDC před výběrem **Cloud Voice politiky**.
V případě nedostatečné kapacity vDC je možno pomocí **Service Library** upravovat kapacitu vDC,
viz kapitola 13.

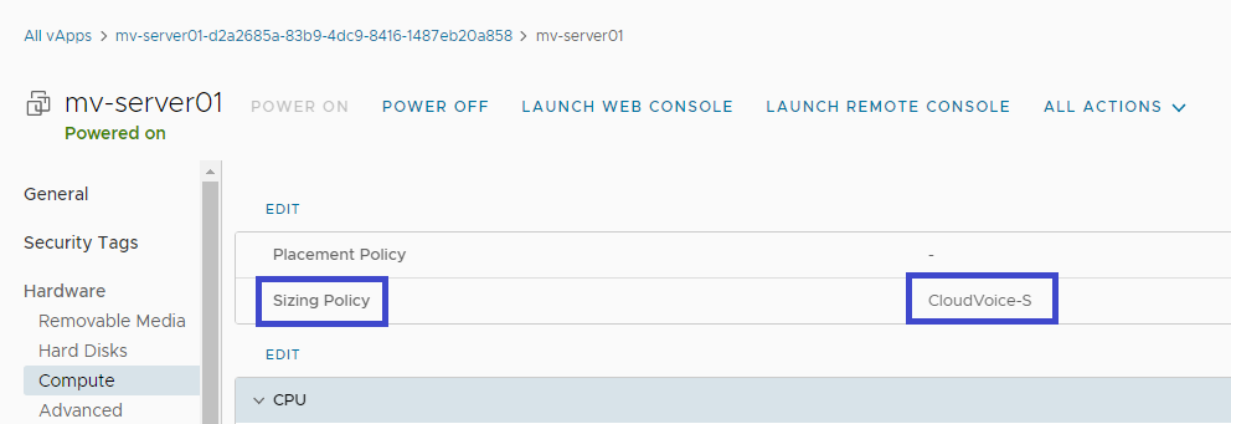
Nastavení Cloud Voice politiky je možno provést kliknutím na virtuální server, následně na **Compute** a **Edit**.



Následně se zobrazí seznam **Cloud Voice politik**, vyberte politiku, kterou požadujete a následně potvrdit tlačítkem **Save** (Uložit).



Tímto se vybraná politika (pro příklad vybrána politika CloudVoice-S), aplikuje na virtuální server a v poli **Sizing Policy** je politika nastavená.



V případě, že je Cloud Voice politika, která se má nastavit, nižšího výpočetního výkonu ve smyslu počtu vCPU a paměti, než je aktuálně nastaveno na virtuálním serveru, doporučujeme zvážit nastavení cílové Cloud Voice politiky za vypnutého stavu serveru.
(Zejména u větších DB systémů a vytížených serverů by mohlo snížení prostředků (vCPU a vRAM), způsobit ztrátu dat).

Pokud vybíráte politiku, která pro server nastavuje více CPU, než kolik má aktuálně daný virtuální server nastaven, je potřeba server vypnout, provést výběr Cloud Voice politiky a server zapnout.
V případě, že má server aktivní funkci **Virtual CPU hot add**, lze změnu Cloud Voice politiky provést za zapnutého stavu serveru bez nutnosti ho vypínat.

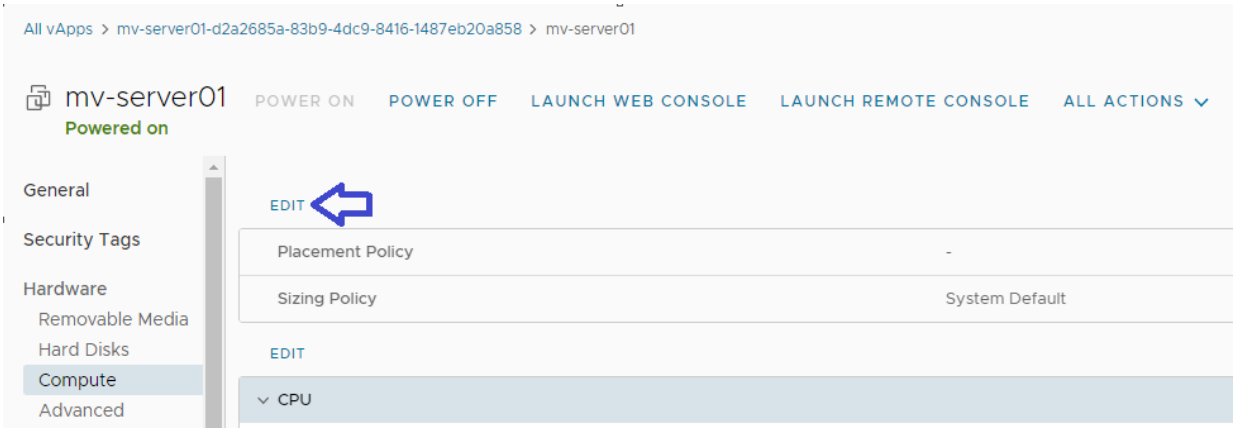
Pokud vybíráte politiku, která pro server nastavuje více paměti, než kolik má aktuálně daný virtuální server nastavenou, je potřeba server vypnout, provést výběr Cloud Voice politiky a server zapnout.
V případě, že má server aktivní funkci **Memory hot add**, lze změnu Cloud Voice politiky provést za zapnutého stavu serveru bez nutnosti ho vypínat.

19 SQLaaS politiky

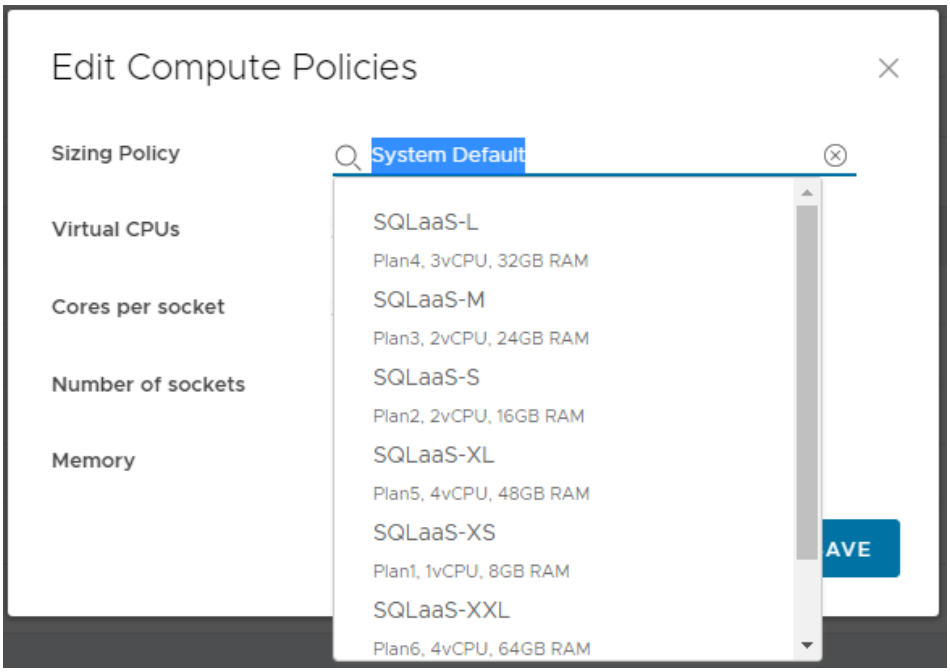
V případě, že máte ve vDC k dispozici **SQLaaS politiky**, tak je můžete aplikovat na jednotlivé virtuální server(y) dle Vašich požadavků.

Doporučujeme ověřit kapacitu vDC před výběrem **SQLaaS politiky**.
V případě nedostatečné kapacity vDC je možno pomocí **Service Library** upravovat kapacitu vDC,
viz kapitola 11.

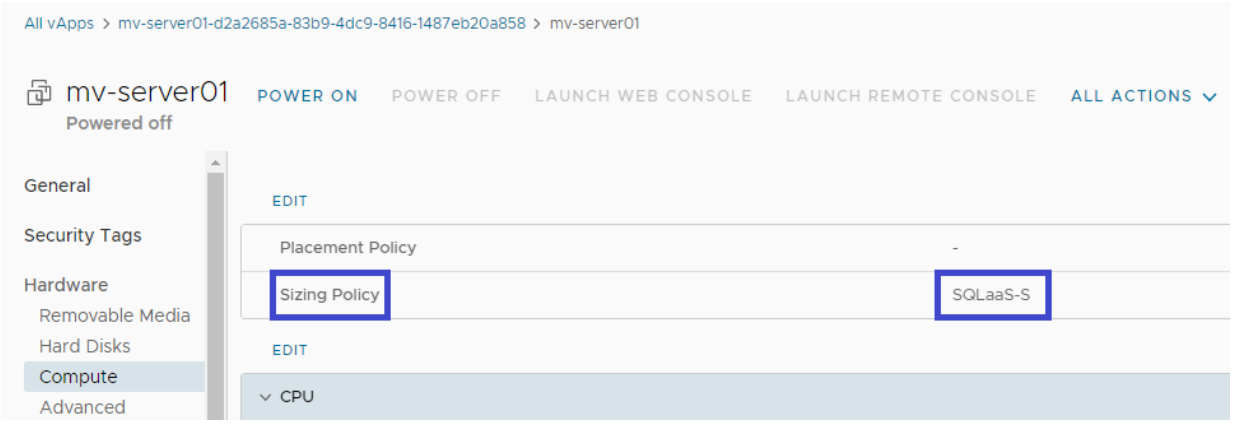
Nastavení SQLaaS politiky je možno provést kliknutím na virtuální server, následně na **Compute** a **Edit**.



Následně se zobrazí seznam **SQLaaS politik**, vyberte politiku, kterou požadujete a následně potvrdit tlačítkem **Save** (Uložit).



Tímto se vybraná politika (pro příklad vybrána politika SQLaaS-S), aplikuje na virtuální server a v poli **Sizing Policy** je politika nastavená.



V případě, že je SQLaaS politika, která se má nastavit, nižšího výpočetního výkonu ve smyslu počtu vCPU a paměti, než je aktuálně nastaveno na virtuálním serveru, doporučujeme zvážit nastavení cílové SQLaaS politiky za vypnutého stavu serveru.
(Zejména u větších DB systémů a vytížených serverů by mohlo snížení prostředků (vCPU a vRAM), způsobit ztrátu dat).

Pokud vybíráte politiku, která pro server nastavuje více CPU, než kolik má aktuálně daný virtuální server nastaven, je potřeba server vypnout, provést výběr SQLaaS politiky a server zapnout.
V případě, že má server aktivní funkci **Virtual CPU hot add**, lze změnu SQLaaS politiky provést za zapnutého stavu serveru bez nutnosti ho vypínat.

Pokud vybíráte politiku, která pro server nastavuje více paměti, než kolik má aktuálně daný virtuální server nastavenou, je potřeba server vypnout, provést výběr SQLaaS politiky a server zapnout.
V případě, že má server aktivní funkci **Memory hot add**, lze změnu SQLaaS politiky provést za zapnutého stavu serveru bez nutnosti ho vypínat.

20 O2 VDC Premium

Služba s důrazem na zvýšenou bezpečnost (šifrované disky) a dostupnost. Výpočetní výkon a diskovou kapacitu je možné čerpat ze dvou nezávislých lokalit s šifrovanými disky nebo z geograficky rozkročeného výpočetního clusteru.

Splňuje vysoké bezpečnostní standardy a SLA plynoucí z požadavků na zápis do katalogu služeb pro dodávky do Státní správy tzv. **eGovernment Cloudu**.

> Řešení O2 Virtuální datové centrum Premium provozujeme v souladu s vyhláškou o cloud computingu, kde je O2 VDC Premium certifikované v bezpečnostní úrovni 3. Prostředí je tedy provozováno s důrazem na zajištění bezpečného, škálovatelného a legislativně kompatibilního prostředí pro provoz eGOV aplikací.

Bezpečnostní úrovně:

BU1 - standardní VDC Standard (v této BÚ se služba O2 VDC Premium neprovozuje)

BU2 - standardní VDC s šifrovanými disky (O2 VDC Premium)

BU3 - vysoce dostupná služba (stretchovaný VMware cluster / vSAN) s šifrovanými disky roztažená přes obě lokality CH a JZM (O2 VDC Premium).

20.1 O2 VDC Premium s BU2 – VDC s šifrovanými disky

Jedná se o klasické VDC Standard s tím rozdílem, že využívá šifrované disky.
Označení diskových storage tierů začíná „ENC“.

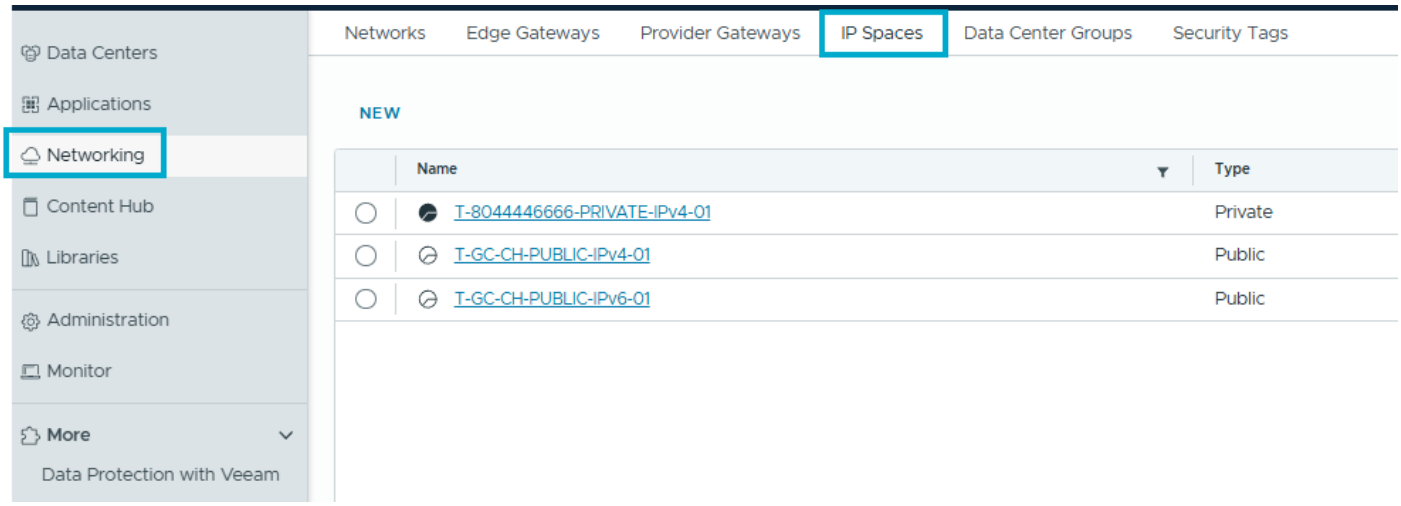
Příklad šifrovaného diskového storage tieru: **ENC**-GOLD-VSAN-1000-JZ

20.2 O2 VDC Premium s BU3 - VDC s šifrovanými disky a vysokou dostupností

Služba poskytovaná z geograficky rozkročeného výpočetního clusteru se **synchronní replikací dat** a automatickým přepnutím provozu při výpadku primární lokality. Poskytuje možnost nadstandardních bezpečnostních standardů. Jedná se o stretchovaný VMware cluster/vSAN přes 2 lokality s vysokou dostupností.

V prostředí tenant portálu se oproti standardnímu VDC využívají pro danou lokalitu 3 logické bloky IP adres tzv. „**IP Spaces**“ (2 veřejné a 1 privátní), ze kterých se čerpají bloky adres pro routované LAN sítě (OrgNetwork) a veřejné IP adresy.

Networking -> IP Spaces



Jakmile si ke standardnímu VDC objednáte také službu O2 VDC Premium ve variantě BU3 geocluster (neplatí pro variantu BU2), bude mít tato služba přesah i do vašeho standardního VDC a to v kontextu drobné změny postupu pro vytváření nových privátních routovaných LAN sítí (OrgNetwork), protože zavádí IP Spaces.

20.2.1 GC-PUBLIC-IPv4-01

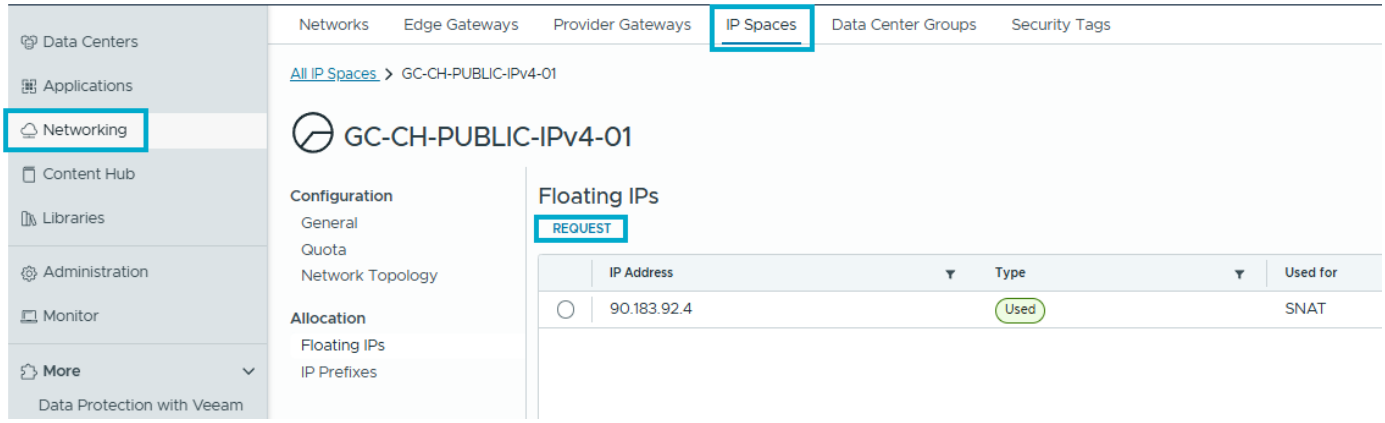
- IP space pro čerpání veřejných IPv4 adres z Internetu
- můžete si sami požádat až o 4 veřejné IPv4 adresy. Pokud byste jich potřebovali více, kontaktujte prosím náš Service Desk.
- 1 veřejná IPv4 adresa může být použita pouze pro 1 službu.

  Příklad:
  Budete-li využívat NAT a IPsec vpn, tak 1 adresa bude využita pro službu NAT, jedna adresa pro IPsec vpn a v případě potřeby si budete moci sami požádat o další 2 adresy bez nutnosti kontaktovat náš Service Desk.

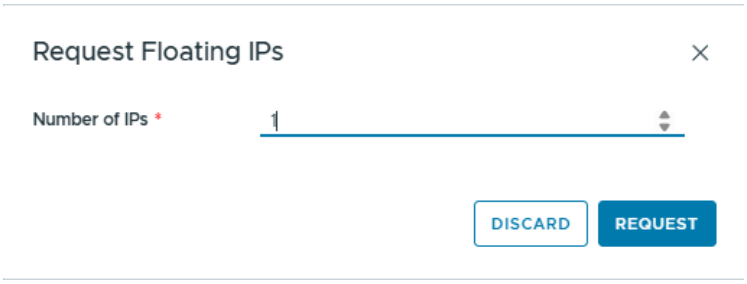
  Na rozdíl od standardního VDC nelze použít 1 IPv4 adresu pro NAT i IPsec vpn zároveň.

20.2.1.1 Žádost o další veřejnou IPv4 adresu

Networking -> IP Spaces -> GC-CH-PUBLIC-IPv4-01 -> REQUEST -> zvolíte počet veřejných IPv4 adres, o které žádáte -> REQUEST



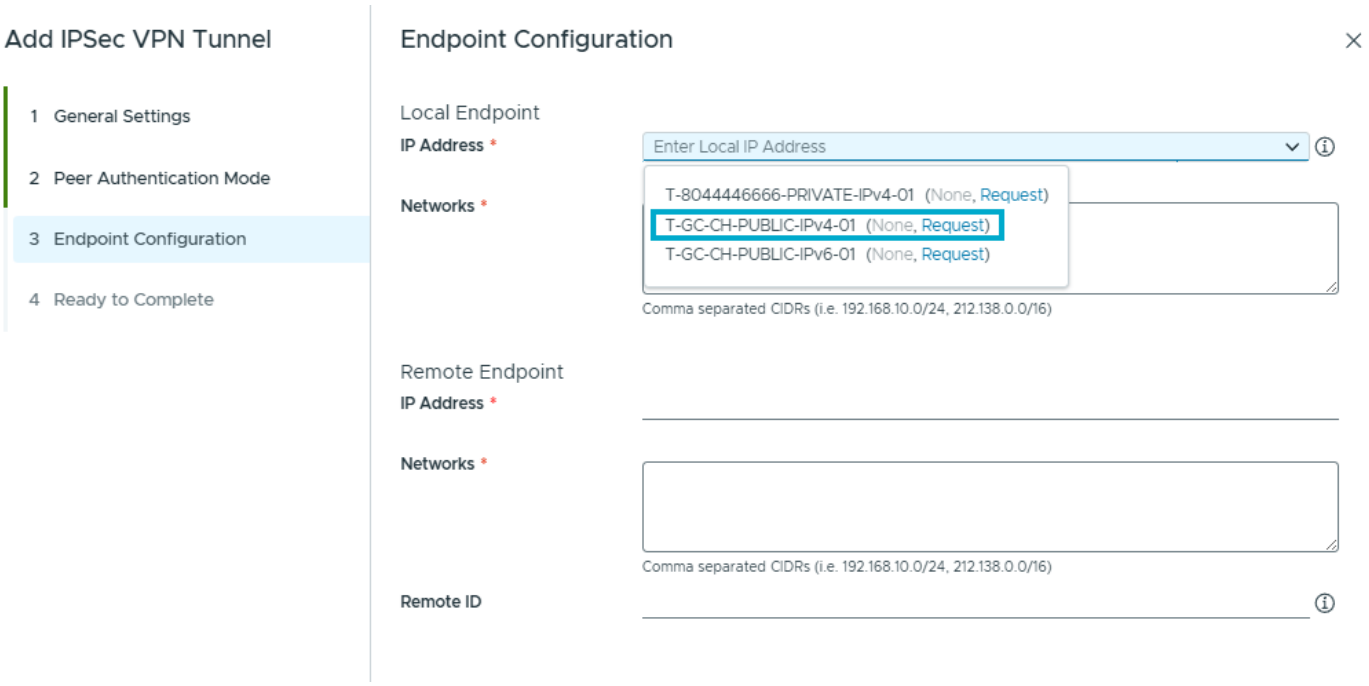
Poznámka: IPv4 adresy uvedené na screenech jsou pouze ilustrativní.



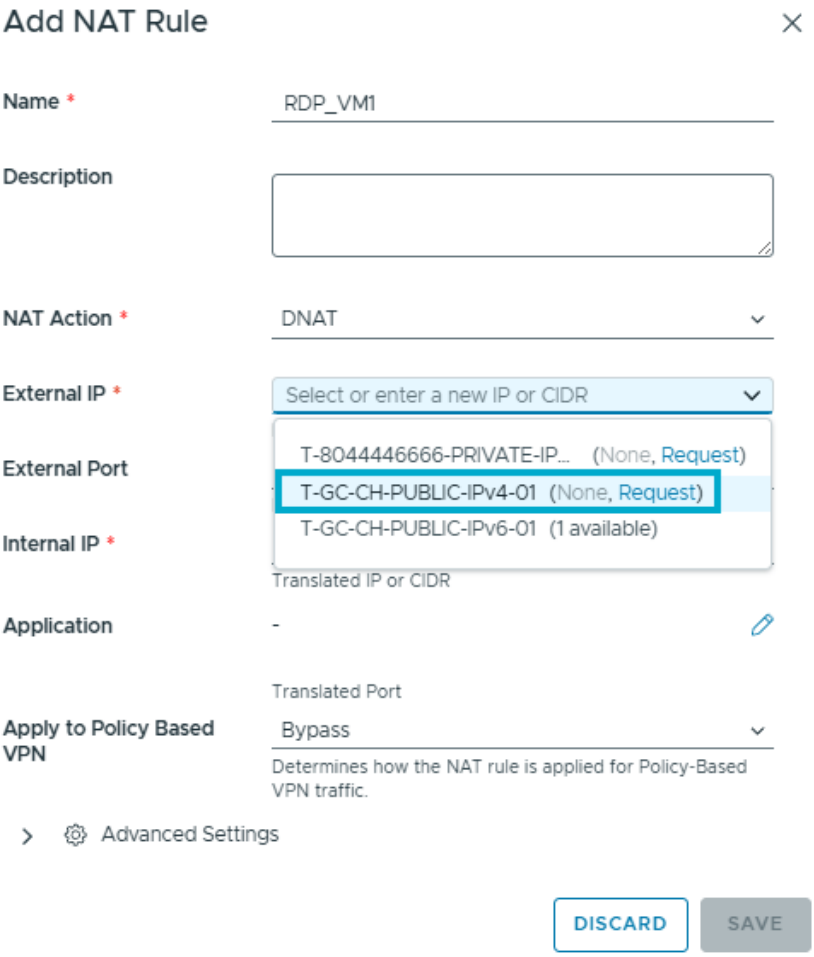
Po stisknutí tlačítka REQUEST je Vám přidělena nová IPv4 adresa, kterou dále můžete využít pro příslušnou službu (NAT, IPsec) u odpovídající geoclusterové EdgeGW tedy EdgeGW jejíž jmenná konvence začíná „**gc-**“.

Druhý způsob, jak si můžete požádat o veřejnou IPv4 adresu z tohoto IP space, je přímo z konkrétní služby (NAT, IPsec) dané geoclusterové EdgeGW

IPsec

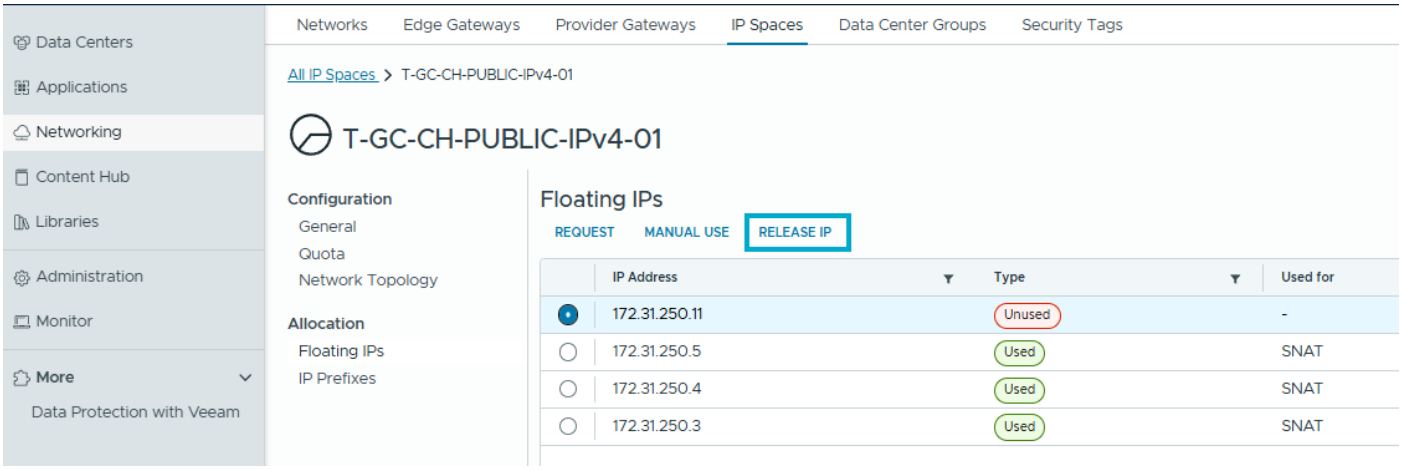

Add IPSec VPN Tunnel
1 General Settings
2 Peer Authentication Mode
3 Endpoint Configuration
4 Ready to Complete
Endpoint Configuration
Local Endpoint
IP Address *
Enter Local IP Address
T-8044446666-PRIVATE-IPv4-01 (None, Request)
T-GC-CH-PUBLIC-IPv4-01 (None, Request)
T-GC-CH-PUBLIC-IPv6-01 (None, Request)
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

NAT:

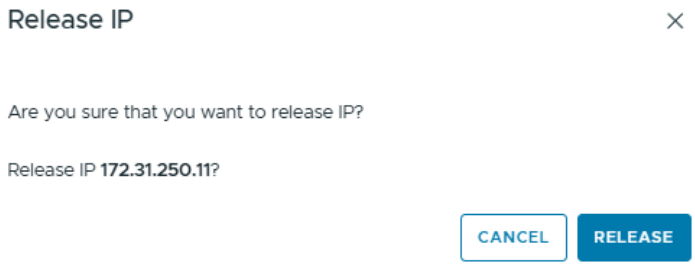

Add NAT Rule
Name *
RDP_VM1
Description
NAT Action *
DNAT
External IP *
Select or enter a new IP or CIDR
T-8044446666-PRIVATE-IP... (None, Request)
T-GC-CH-PUBLIC-IPv4-01 (None, Request)
T-GC-CH-PUBLIC-IPv6-01 (1 available)
External Port
Internal IP *
Translated IP or CIDR
Application
-
Translated Port
Apply to Policy Based VPN
Bypass
Determines how the NAT rule is applied for Policy-Based VPN traffic.
Advanced Settings
DISCARD
SAVE

20.2.1.2 Zrušení nevyužívané veřejné IPv4 adresy

Nebudete-li veřejnou IPv4 adresu již využívat, od nastavte si ji prosím z využívané služby (NAT, IPsec), stav IP adresy se Vám následně změní z Used na Unused viz obrázek níže



a přes tlačítko „**RELEASE IP**“ ji odstraníte



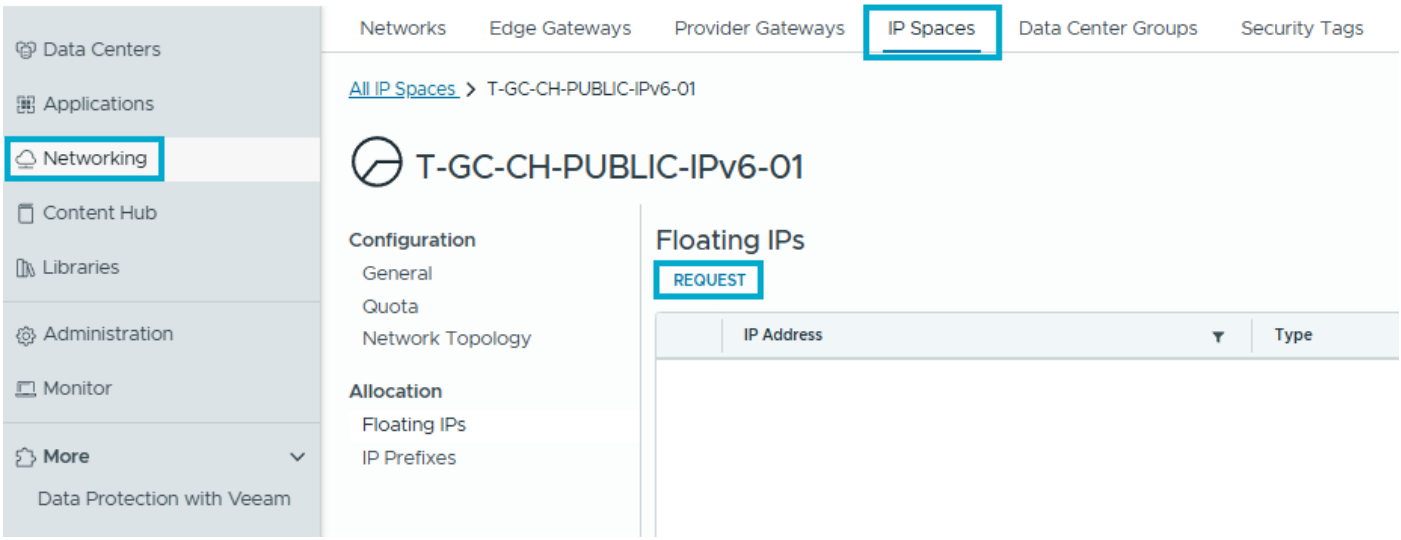
20.2.2 GC-PUBLIC-IPv6-01

- IP space pro čerpání veřejných IPv6 adres a prefixů (bloků IPv6 adres) pro privátní routované LAN sítě (OrgNetworks)
- můžete si sami požádat až o 4 veřejné IPv4 adresy. Pokud byste jich potřebovali více, kontaktujte prosím náš Service Desk.
- 1 veřejná IPv6 adresa může být použita pouze pro 1 službu.

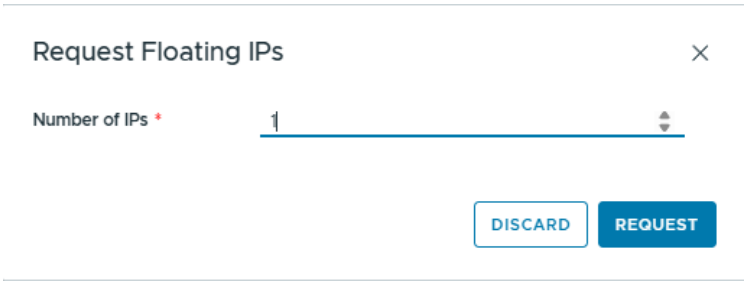
  Příklad:
  Budete-li využívat IPsec vpn, tak 1 adresa bude využita pro službu IPsec vpn a v případě potřeby si budete moci sami požádat o další 3 adresy bez nutnosti kontaktovat náš Service Desk.

20.2.2.1 Žádost o další veřejnou IPv6 adresu

Networking -> IP Spaces -> GC-CH-PUBLIC-IPv6-01 -> REQUEST -> zvolíte počet veřejných IPv6 adres, o které žádáte -> REQUEST



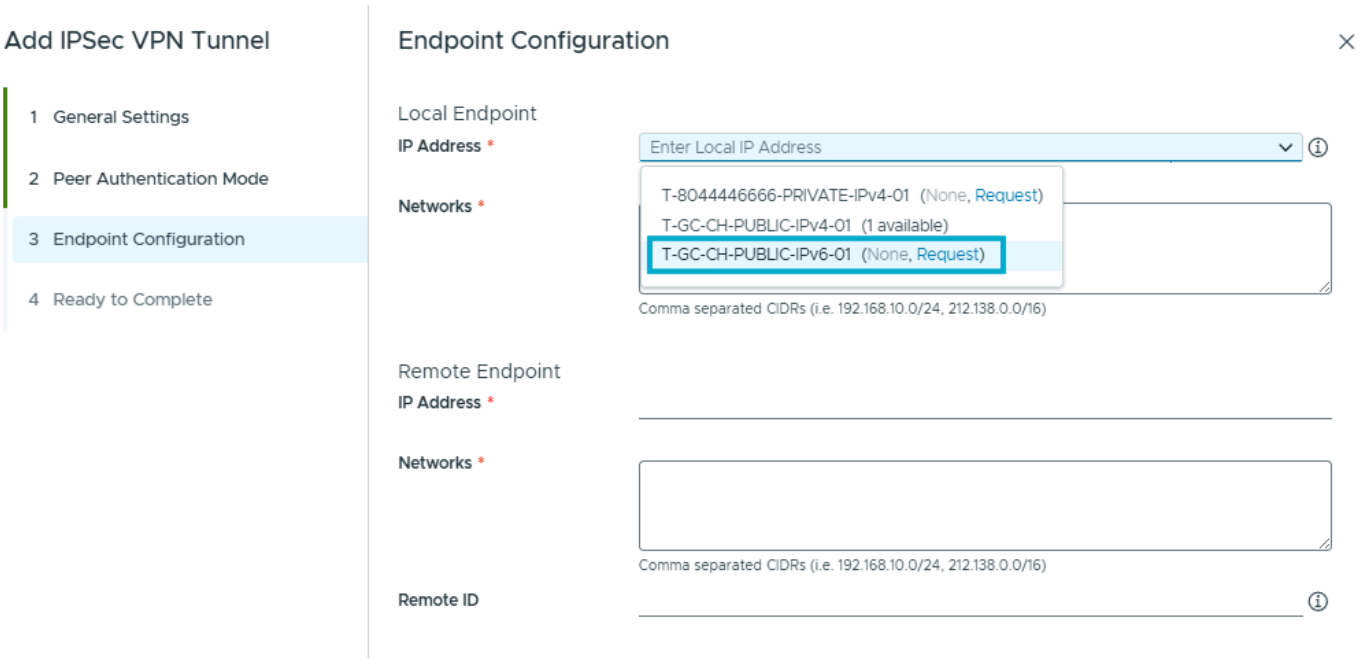
Poznámka: IPv6 adresy uvedené na screenech jsou pouze ilustrativní.



Po stisknutí tlačítka REQUEST je Vám přidělena nová IPv6 adresa, kterou dále můžete využít pro příslušnou službu (IPsec) u odpovídající geoclusterové EdgeGW tedy EdgeGW jejíž jmenná konvence začíná „**gc-**“.

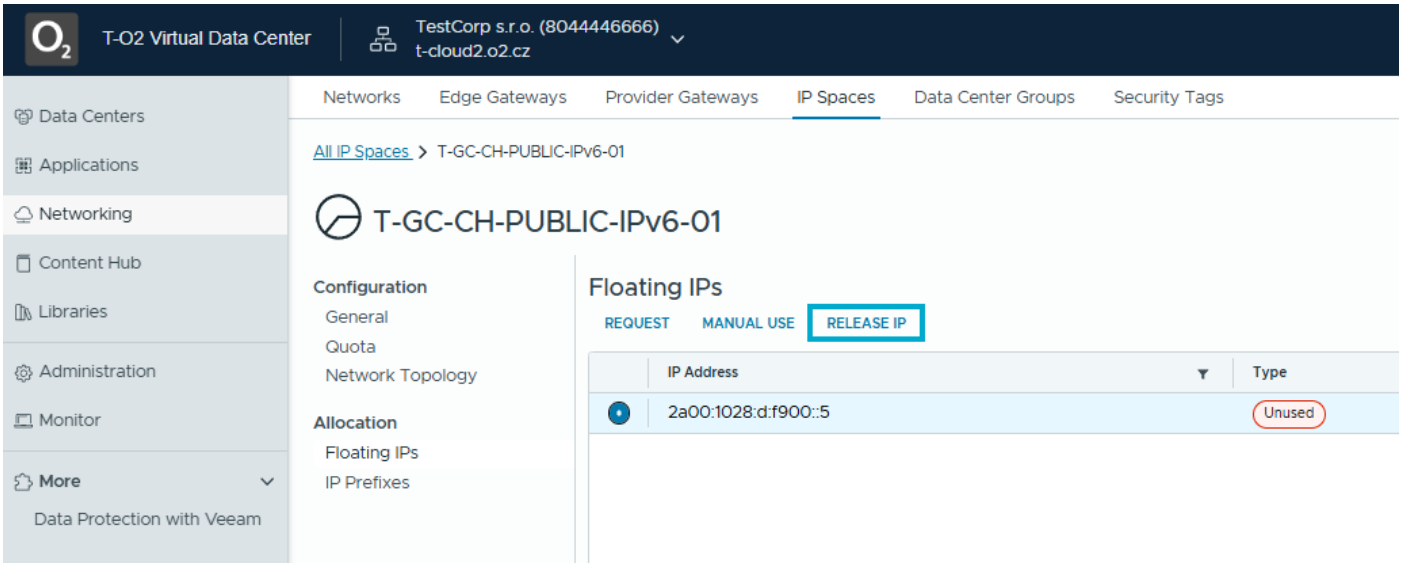
Druhý způsob, jak si můžete požádat o veřejnou IPv6 adresu z tohoto IP space, je přímo z konkrétní služby (IPsec) dané geoclusterové EdgeGW

IPsec

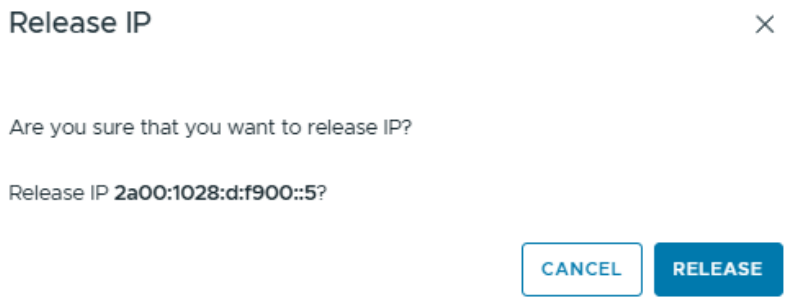


20.2.2.2 Zrušení nevyužívané veřejné IPv6 adresy

Nebudete-li veřejnou IPv6 adresu již využívat, od nastavte si ji prosím z využívané služby (IPsec), stav IP adresy se Vám následně změní z Used na Unused viz obrázek níže



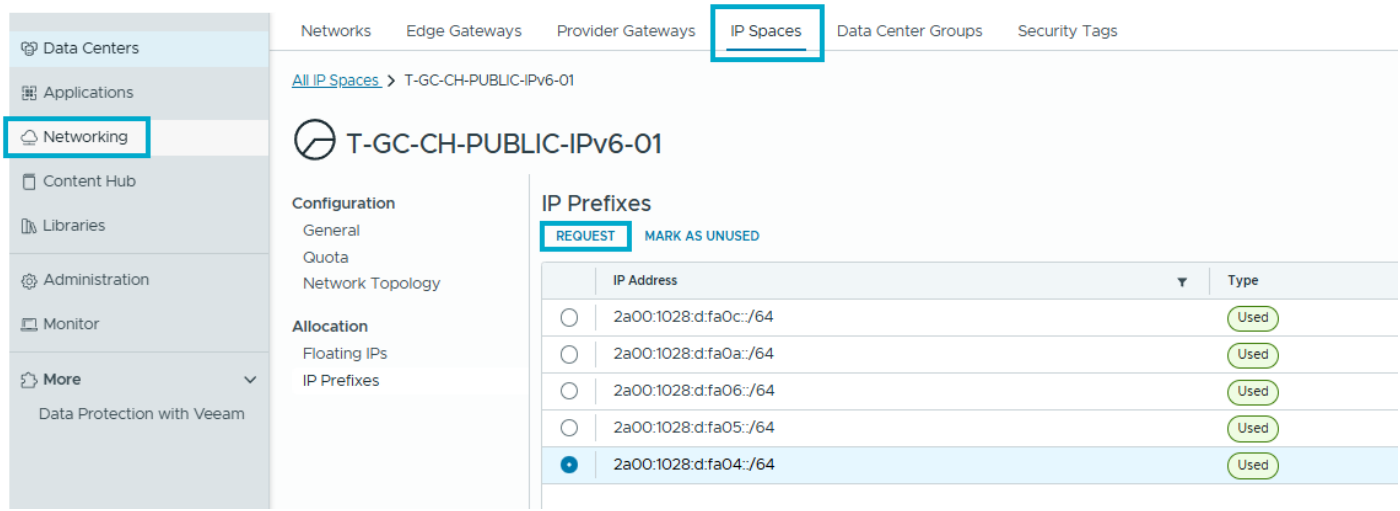
a přes tlačítko „**RELEASE IP**“ ji odstraníte



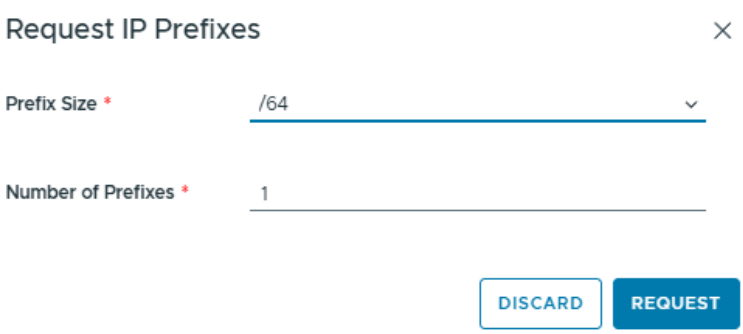
20.2.2.3 Žádost o nový IPv6 blok adres pro privátní routovanou LAN síť (OrgNetwork)

V případě potřeby si můžete na existující nebo nové privátní routované LAN síti (OrgNetwork) aktivovat IPv6 přidáním nového bloku IPv6 adres.

Networking -> IP Spaces -> GC-CH-PUBLIC-IPv6-01 -> REQUEST



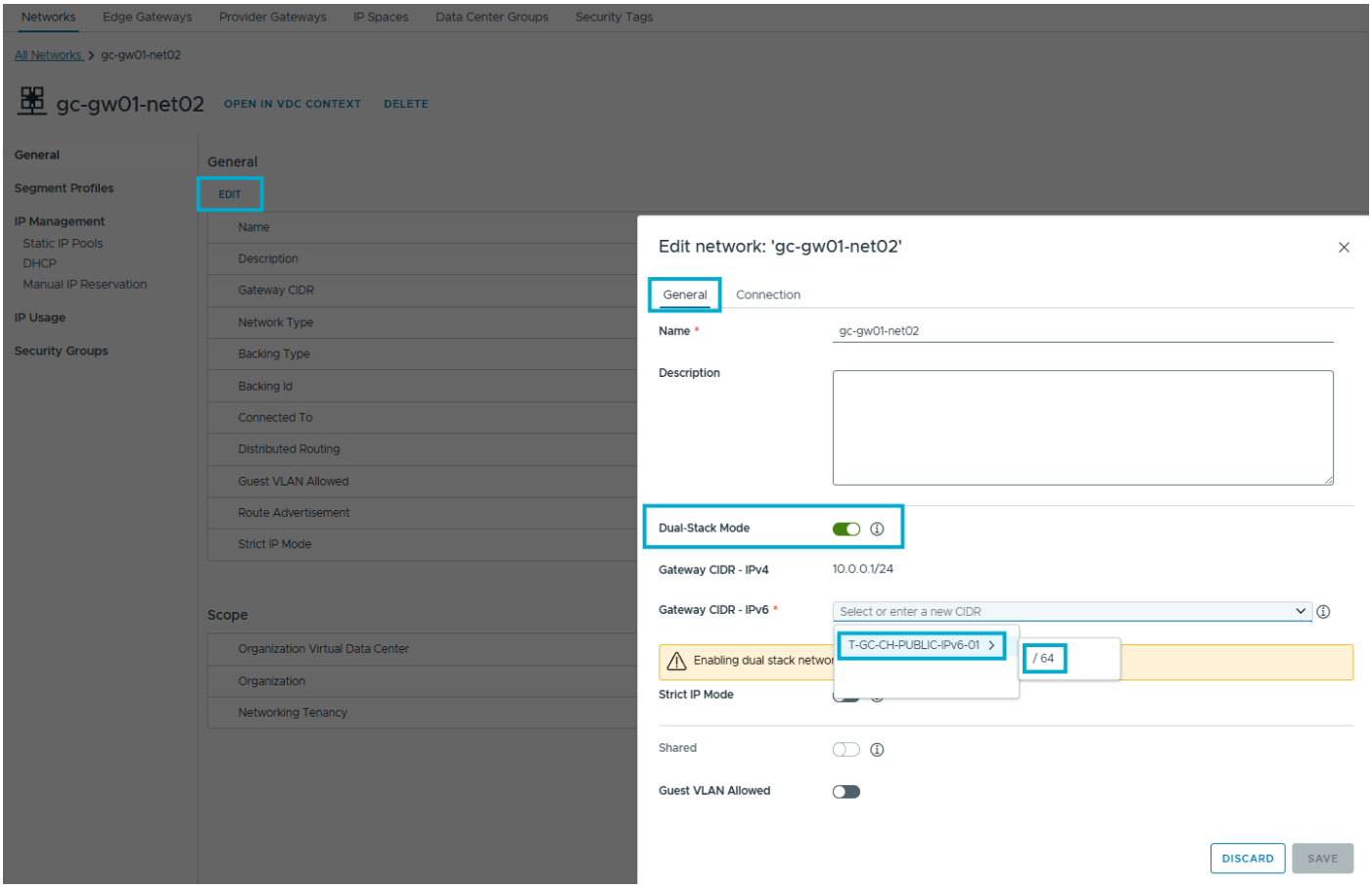
Zvolíte počet veřejných IPv6 bloků (prefixes), o které žádáte (na obrázku jeden) -> REQUEST



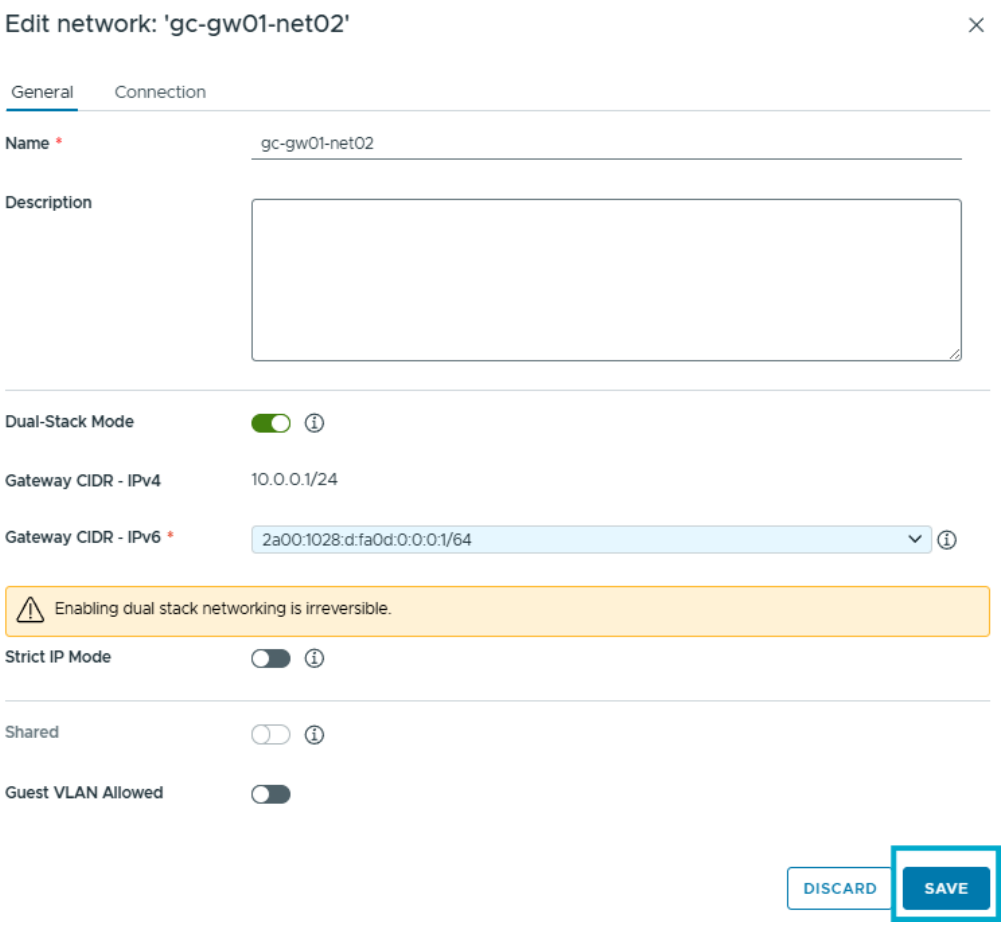
Poznámka: Celkem si můžete požádat až o 16 bloků IPv6 adres (prefixů).

Následně si vyberete privátní routovanou LAN (OrgNetwork), u které chcete aktivovat IPv6 ke stávající IPv4.

EDIT -> General -> aktivujete Dual-Stack Mode -> Gateway CIDR - IPv6 -> zvolíte IP space GC-PUBLIC-IPv6-01 -> /64 -> doplní se Vám IPv6 blok, o který jste si zažádali v předchozím kroku.



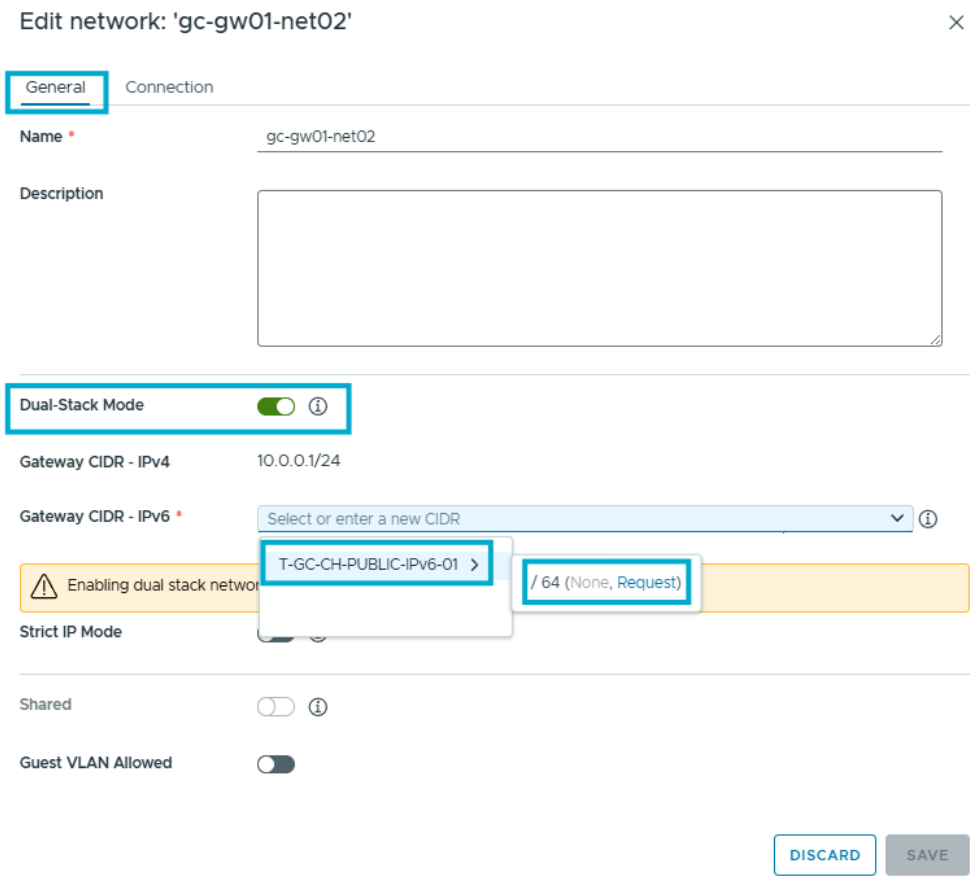
IPv6 blok se Vám automaticky doplní -> SAVE

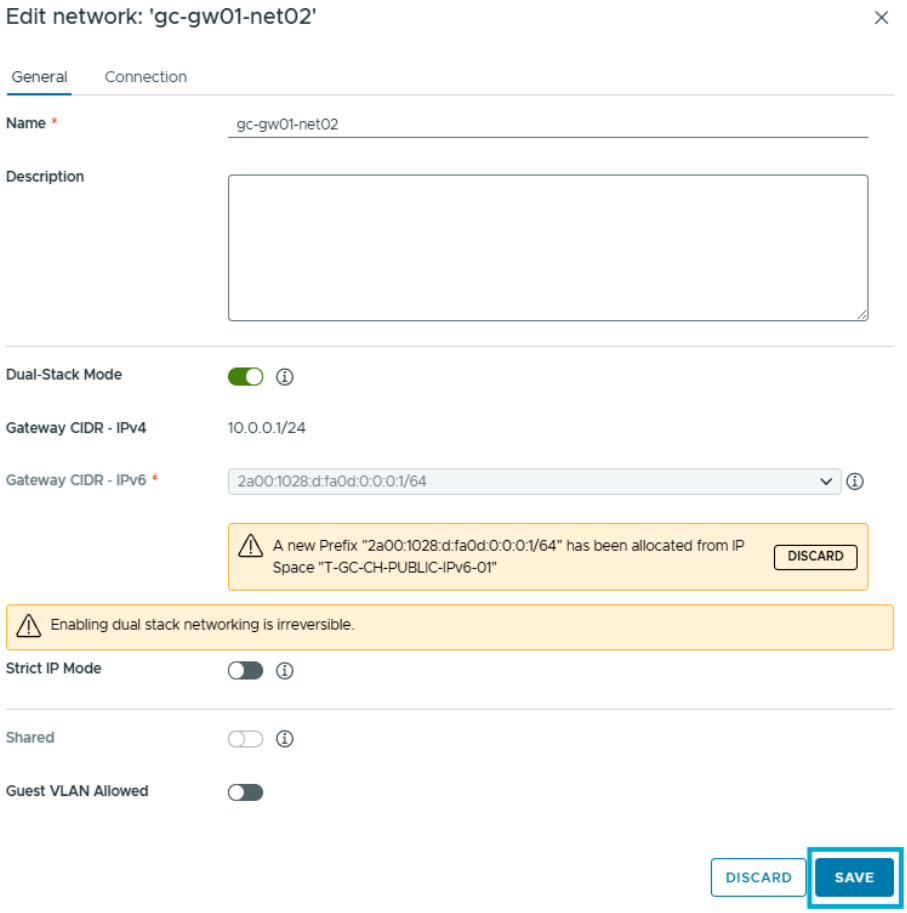


Poznámka: 1 privátní routovaná LAN (OrgNetwork) = 1 blok (prefix) IPv6 adres

Druhý, způsob, jak si můžete požádat o blok IPv6 adres z tohoto IP space, je přímo při aktivaci IPv6 sítě nad danou privátní routovanou LAN sítí (OrgNetwork) připojené ke geoclusterové EdgeGW.

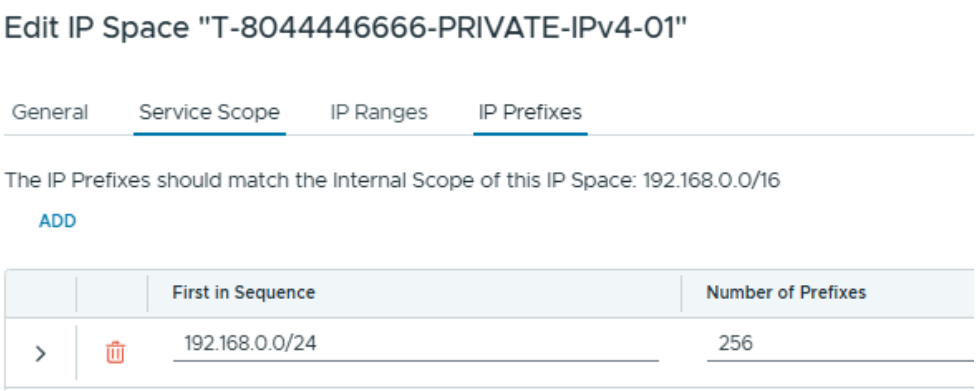
EDIT -> General -> aktivujete Dual-Stack Mode -> Gateway CIDR - IPv6 -> zvolíte IP space GC-PUBLIC-IPv6-01 -> /64 (None, Request)-> tímto si požádáte o nový IPv6 blok, který se vám automaticky doplní do pole “Gateway CIDR - IPv6”.


Edit network: 'gc-gw01-net02'
General
Connection
Name *
gc-gw01-net02
Description
Dual-Stack Mode
Gateway CIDR - IPv4
10.0.0.1/24
Gateway CIDR - IPv6 *
Select or enter a new CIDR
T-GC-CH-PUBLIC-IPv6-01
/ 64 (None, Request)
Enabling dual stack networ
Strict IP Mode
Shared
Guest VLAN Allowed
DISCARD
SAVE


Edit network: 'gc-gw01-net02'
General
Connection
Name *
gc-gw01-net02
Description
Dual-Stack Mode
Gateway CIDR - IPv4
10.0.0.1/24
Gateway CIDR - IPv6 *
2a00:1028:d:fa0d:0:0:0:1/64
A new Prefix "2a00:1028:d:fa0d:0:0:0:1/64" has been allocated from IP Space "T-GC-CH-PUBLIC-IPv6-01"
DISCARD
Enabling dual stack networking is irreversible.
Strict IP Mode
Shared
Guest VLAN Allowed
DISCARD
SAVE

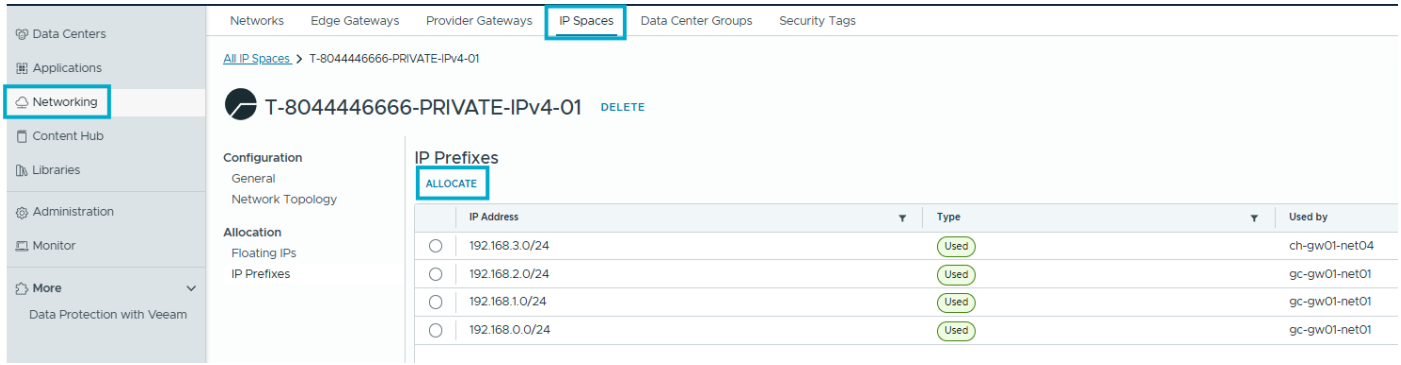
20.2.3 PRIVATE-IPv4-01

- pro čerpání privátních routovaných LAN subnetů (OrgNetworks)
- v IP Prefixes máte předdefinovanou síť 192.168.0.0/24, můžete tedy vytvořit až 256 C sítí



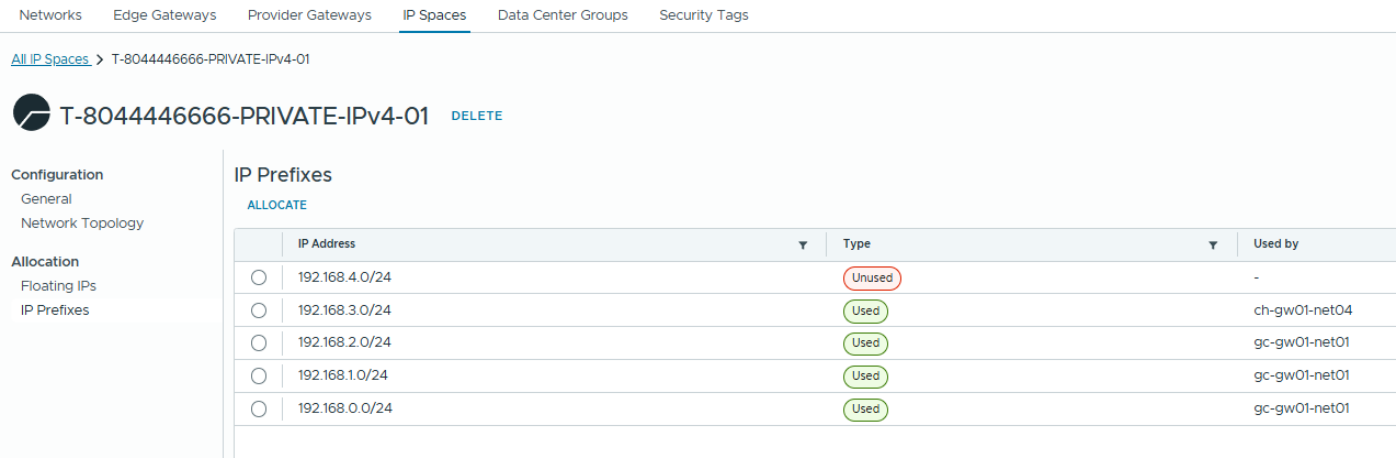
20.2.3.1 Vytvoření nové privátní routované LAN sítě (OrgNetwork) předalokováním subnetu v IP space

Networking -> IP Spaces -> Allocation -> IP Prefixes -> ALLOCATE

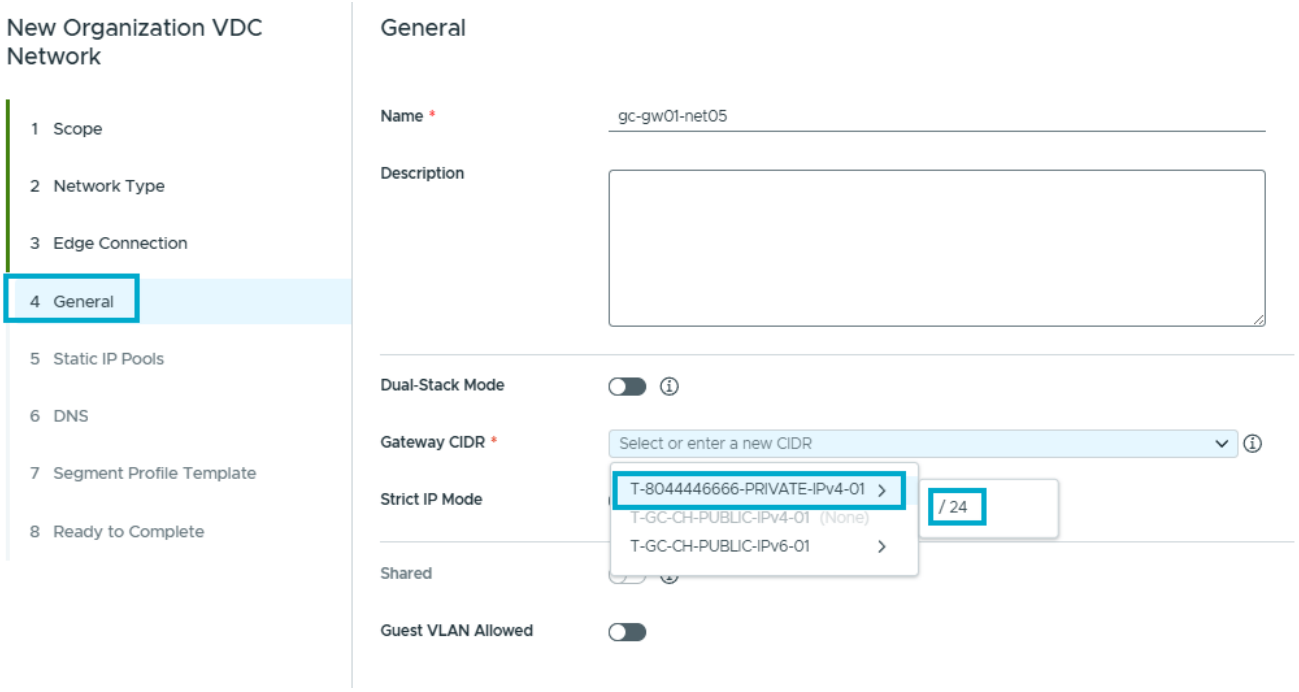


V dalším kroku uvedete počet LAN subnetů, které se mají vytvořit z rozsahu 192.168.0.0/16 (na obrázku jeden) -> ALLOCATE

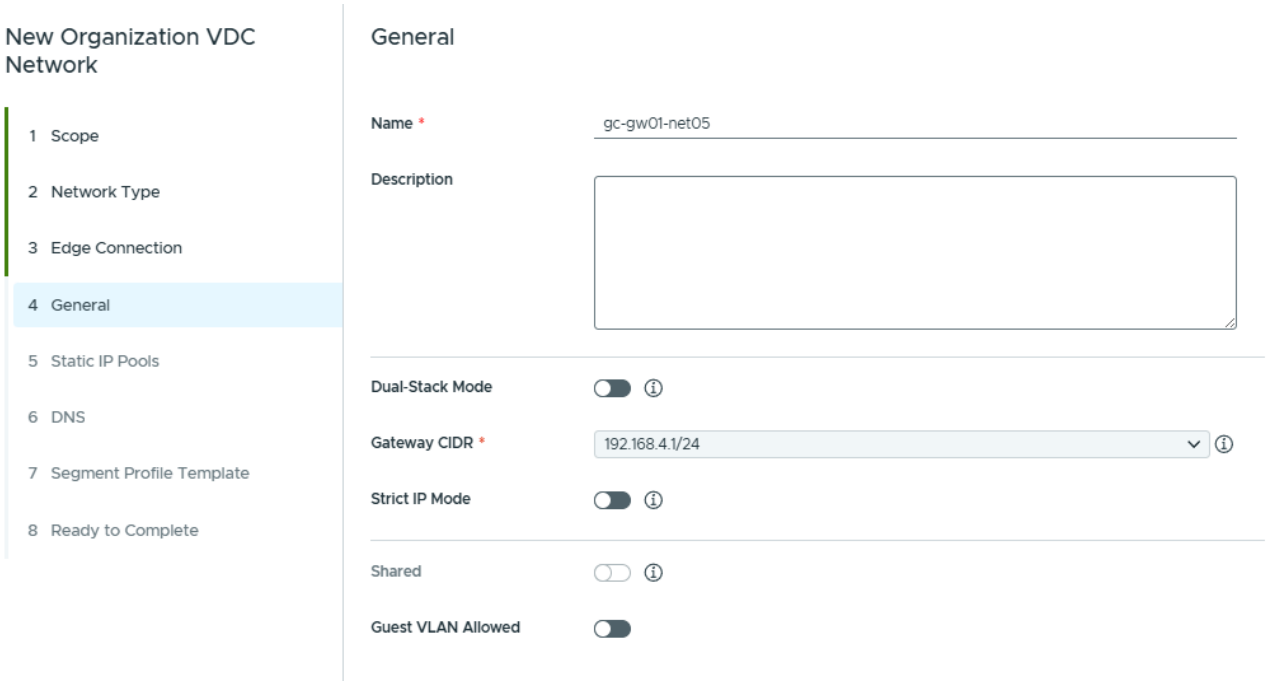
Vytvořený subnet uvidíte ve stavu Unused



Při vytváření nové privátní routované sítě LAN (OrgNetwork) se postupuje stejně viz kapitola **4.2.4 Vytvoření sítě z nabídky Networking** s tím rozdílem, že na kartě General nevyplňujete „Gateway CIDR“ ručně, ale prokliknete přes IP space „PRIVATE-IPv4-01“ -> /24

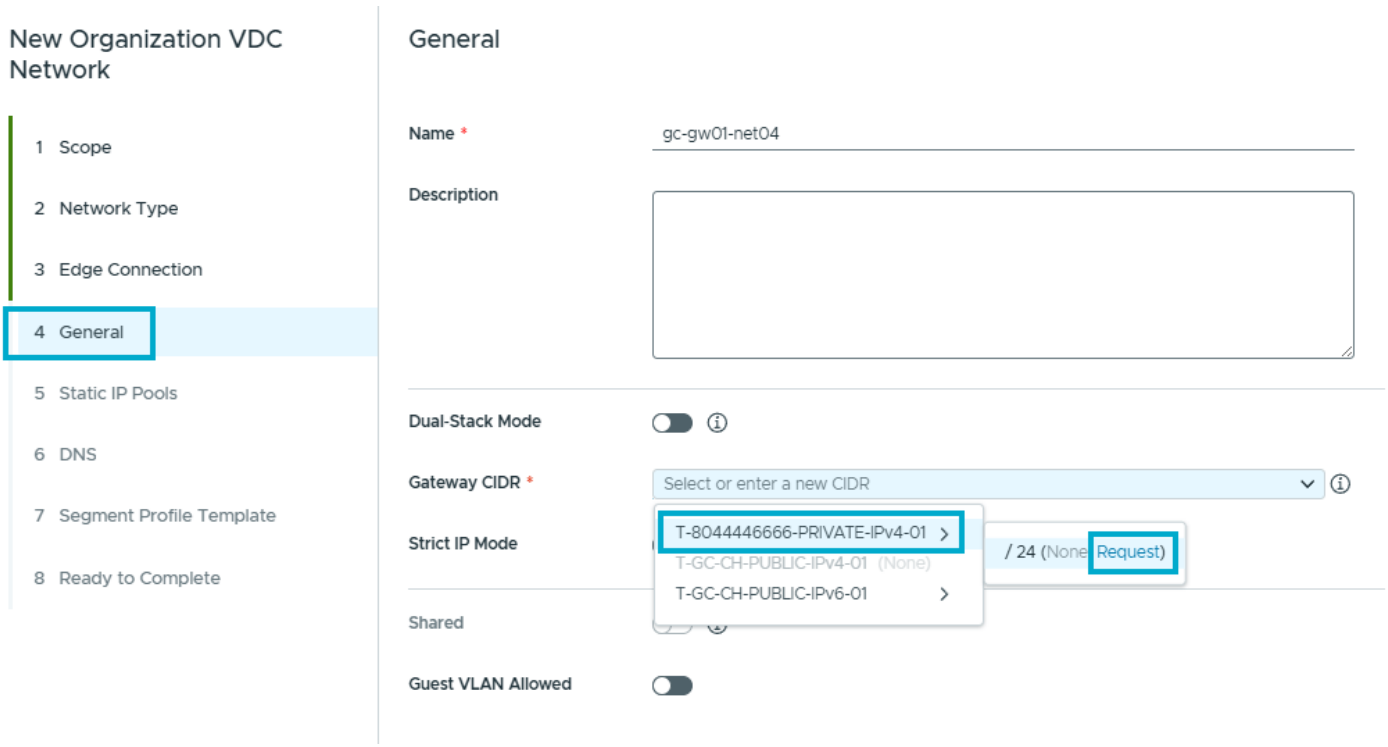


A rozsah subnetu, který jste si předalokovali v IP space v předchozím kroku, se Vám automaticky doplní.

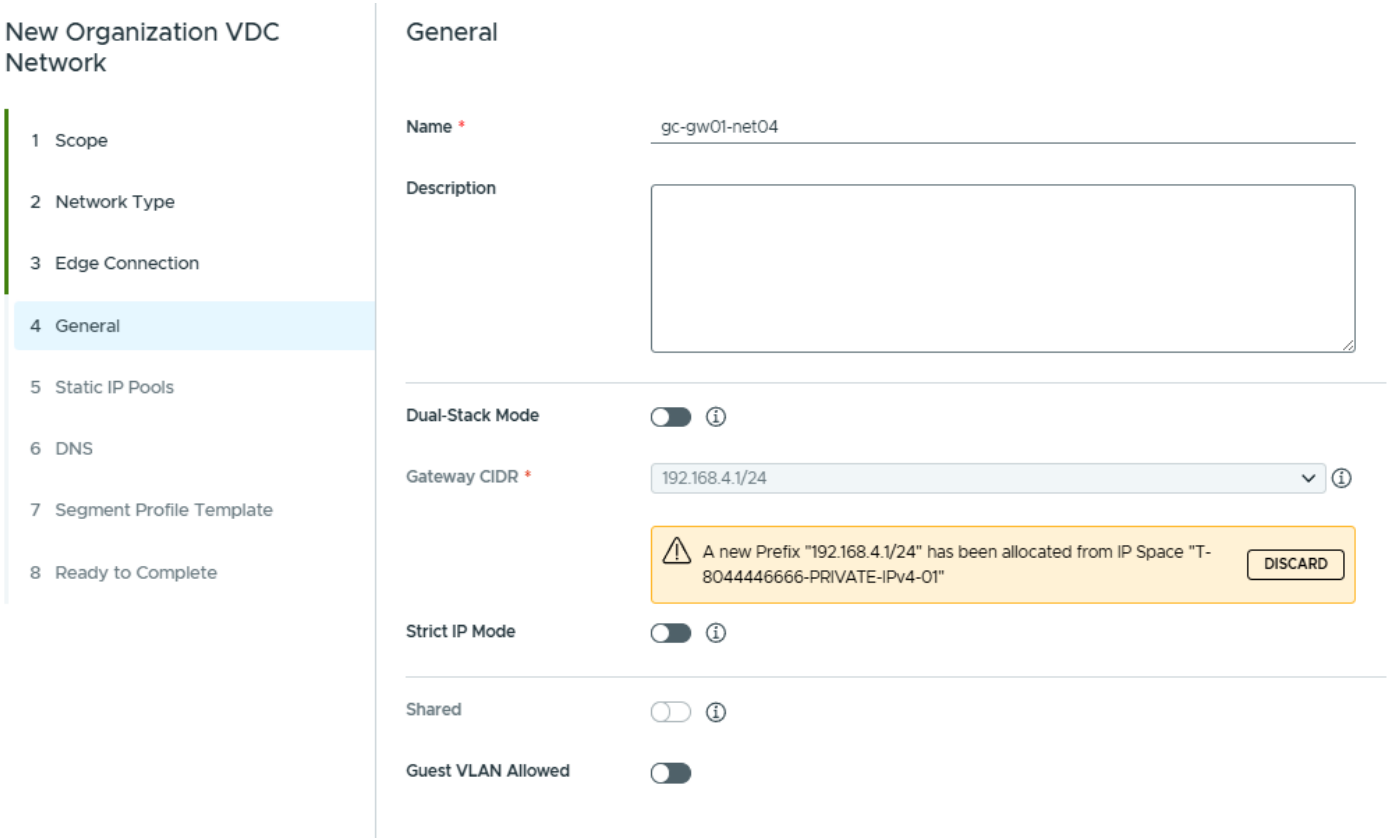


20.2.3.2 Vytvoření nové privátní routované LAN sítě (OrgNetwork) bez nutnosti předalokoce subnetu v IP space

O nový subnet z tohoto IP space si můžete požádat přímo v průvodci při vytváření nové privátní LAN sítě (OrgNetwork) na kartě „General“ přes „Request“.



Tímto se Vám automaticky z IP space přidělí další volný subnet.



Další postup vytváření OrgNetwork je již shodný s kapitolou 4.2.4 Vytvoření sítě z nabídky Networking.

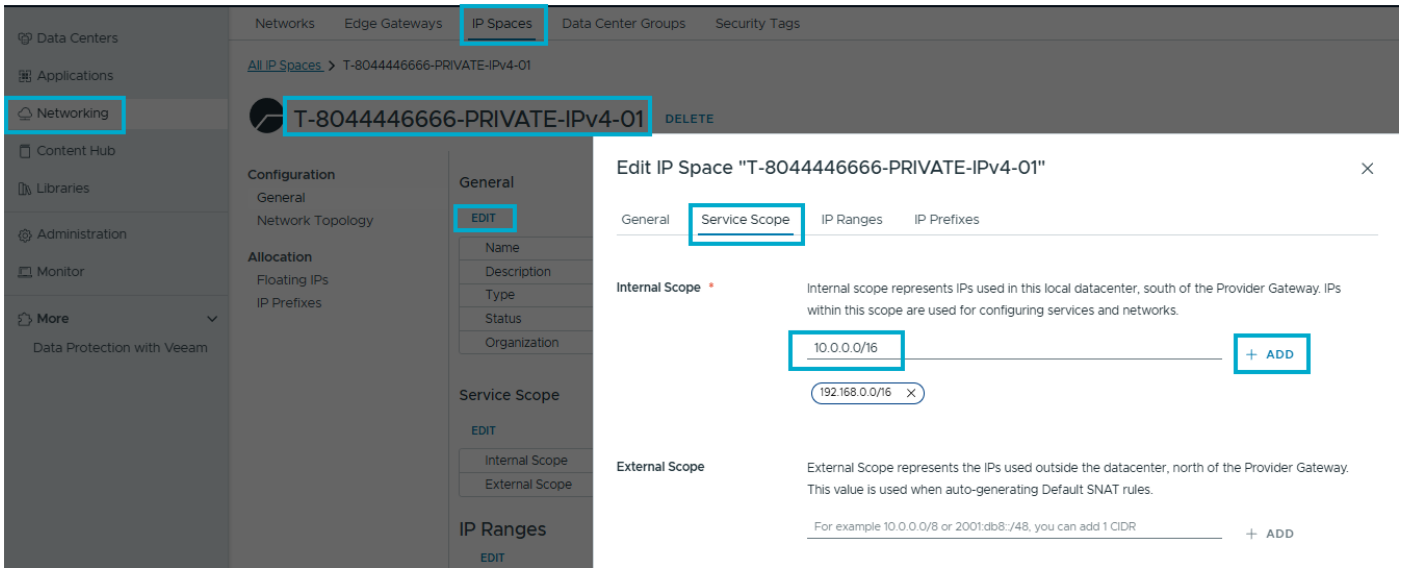
20.2.3.3 Vytvoření nové privátní routované LAN sítě (OrgNetwork) s Vámi definovaným rozsahem

V IP Prefixes máte defaultně předdefinovanou síť 192.168.0.0/24, ze které si můžete vytvořit až 256 C sítí

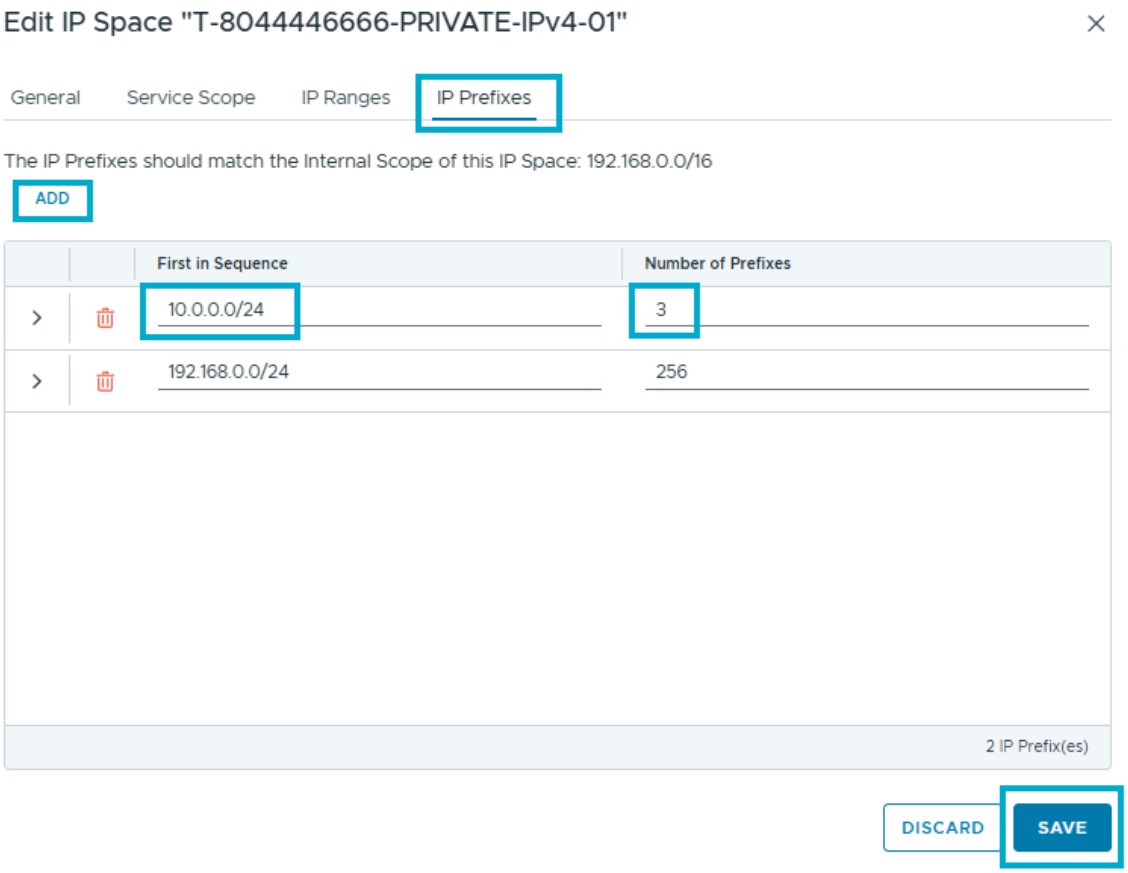
Pokud byste chtěli využívat pro privátní LAN sítě svůj vlastní rozsah (například 10.0.0.0/24) je potřeba provést tyto kroky:

1) Do „Service Scope“ si přidáte vám požadovaný rozsah, ze kterého se budou „krájet“ požadované sítě

Networking -> IP Spaces -> PRIVATE-IPv4-01 -> EDIT -> Service Scope -> Internal Scope: doplníte rozsah -> *ADD*



2) Přidáte ke stávajícímu subnetu 192.168.0.0/24 vámi požadovaný například 10.0.0.0/24 a uložíte (SAVE)



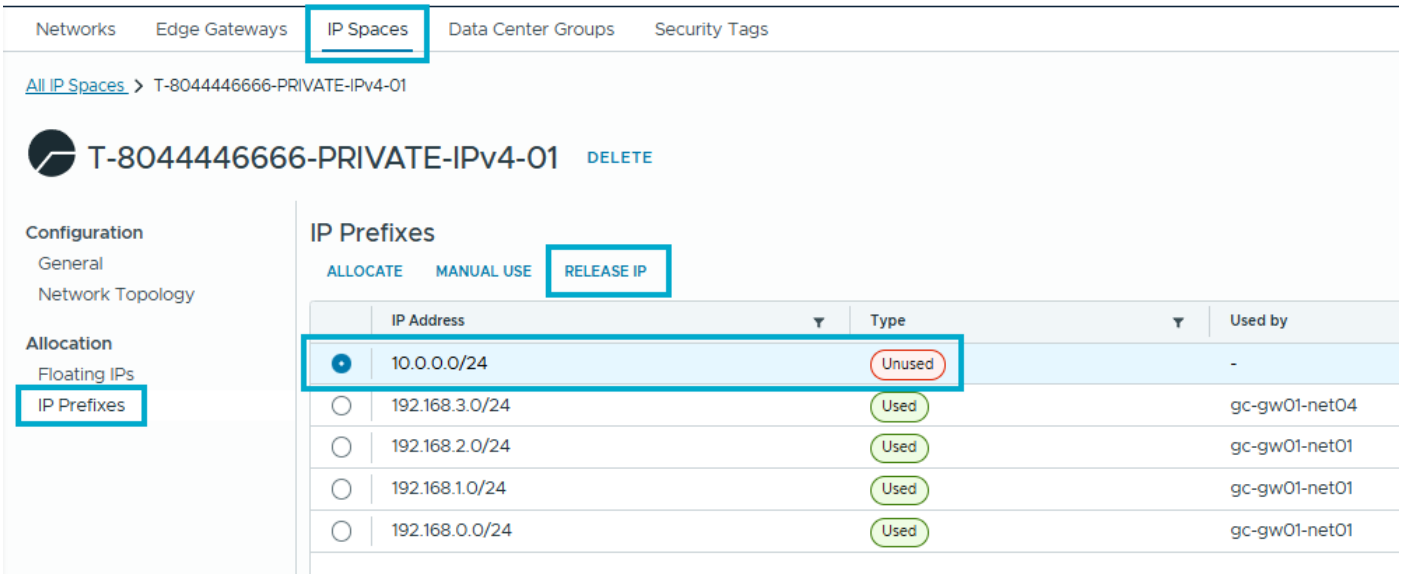
Při vytváření nových privátních sítí je pak princip zcela stejný viz kapitoly 20.2.3.1 a 20.2.3.1 tedy můžete si vybrat, zda si nejprve privátní routovaný LAN subnet předalokujete a následně si jej při vytváření nové sítě zvolíte 20.2.3.1 nebo si rovnou o nový subnet z vámi definovaného rozsahu zažádáte při vytváření nové privátní routované LAN viz 20.2.3.1.

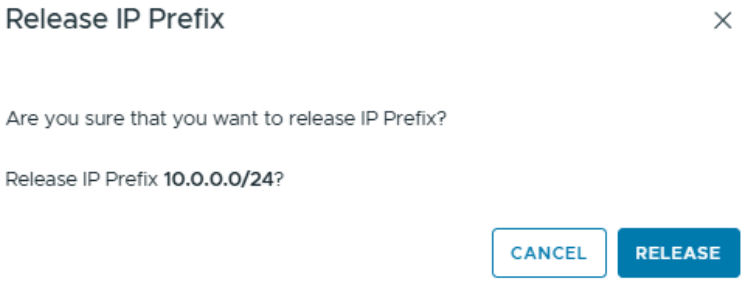
Na obrázku výše jsou pro subnet 10.0.0.0/24 definované 3 prefixy což znamená, že můžete vytvořit až 3 privátní LAN routované sítě (OrgNetwork) tedy 10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24. Jakmile se počet prefixů vyčerpá, začne se u dalších nových sítí čerpat z rozsah 192.168.0.0/24. Samozřejmě si kdykoliv v případě potřeby můžete navýšit počet prefixů u vámi definovaného rozsahu.

20.2.3.4 Uvolnění LAN subnetu po zrušení privátní routované LAN sítě (OrgNetwork)

Pokud si smažete nevyužívanou privátní routovanou LAN síť (OrgNetwork), doporučujeme ji uvolnit i u IP space „PRIVATE-IPv4-01“

Networking -> IP Spaces -> PRIVATE-IPv4-01 -> Allocation -> IP Prefixes -> vyberete rozsah ve stavu *Unused -> RELEASE IP -> RELEASE*





21 O2 DRaaS

Jedná se o službu Disaster Recovery as a Service, doplňková služba k VDC.

Infrastruktura: služba je postavena na technologii Veeam, (Veeam Cloud Connect v kombinaci s VMware Cloud Director (vCD)

Princip služby: Zákazník ukládá repliky serverů z on-premise prostředí do O2 VDC. V případě potřeby (nefunkčnosti původní infrastruktury), aktivuje repliky a provoz jeho prostředí je zajištěn z O2 VDC.

Služba lze provozovat ve třech bezpečnostních úrovní:

Bezpečnostní úrovně:

BU1 - standardní VDC Standard

BU2 - standardní VDC s šifrovanými disky

BU3 - vysoce dostupná služba (stretchovaný VMware cluster / vSAN) s šifrovanými disky roztažená přes obě lokality CH a JZM.

21.1 O2 DRaaS s BU2 – VDC s šifrovanými disky

Jedná se o klasické VDC Standard s tím rozdílem, že využívá šifrované disky.
Označení diskových storage tierů začíná „ENC“.

Příklad šifrovaného diskového storage tieru: **ENC**-GOLD-VSAN-1000-JZ

21.2 O2 DRaaS s BU3 - VDC s šifrovanými disky a vysokou dostupností

Služba poskytovaná z geograficky rozkročeného výpočetního clusteru se **synchronní replikací dat** a automatickým přepnutím provozu při výpadku primární lokality. Poskytuje možnost nadstandardních bezpečnostních standardů. Jedná se o stretchovaný VMware cluster/vSAN přes 2 lokality s vysokou dostupností.

V prostředí tenant portálu se oproti standardnímu VDC využívají pro danou lokalitu 3 logické bloky IP adres tzv. „**IP Spaces**“ (2 veřejné a 1 privátní), ze kterých se čerpají bloky adres pro routované LAN sítě (OrgNetwork) a veřejné IP adresy.

PRINCIPY PRÁCE S IP SPACES JSOU SHODNÉ SE SLUŽBOU VDC PREMIUM BU3, VIZ KAPITOLA:

20.2 O2 VDC Premium s BU3 - VDC s šifrovanými disky a vysokou dostupností

VČETNĚ VŠECH JEJÍCH PODKAPITOL.

22 Známé chyby a jejich řešení

1) **Problém: Server je pomalý a nelze ovládat myší**
   ŘEŠENÍ: ověřte, že jsou na serveru nainstalovány VMware Tools a jsou aktuální. Jak provést jejich instalaci či aktualizaci je popsáno v kapitole 9.2.1. Doporučené dodatečné nastavení virtuálního serveru
   (V případě OS Linux lze použít i Open-VM-Tools).

2) **Problém: Server (y) mají výpadky síťového připojení**
   ŘEŠENÍ: ověřte, že virtuální server používá typ síťového adaptéru VMXNET3 a dále to, že jsou na serveru nainstalovány VMware Tools a jsou aktuální.

3) **Problém: Paměť serveru nelze navýšit i přesto, že jsou prostředky (vDC Memory) ve vDC dostatečné.**
   ŘEŠENÍ: ověřte, že jsou dostatečné prostředky i pro vDC Storage, na které je server uložen. Paměť reprezentuje soubor na datastoru takže je potřeba mít dostatečnou kapacitu i uložiště (vDC Storage), na které je server uložen.

4) **Problém: Nelze sestavit Site-To-Site VPN tunel**
   ŘEŠENÍ: zkontrolujte nastavení VPN. Všechny parametry VPN definované v o2 cloudu musí přesně odpovídat (1:1) parametrům na protistraně - tedy na zákaznickém routeru (vpn GW).

5) **Problém: Nefunkční připojení na server přes RDP nebo SSH**
   ŘEŠENÍ: ověřte, že máte správně nastaven DNAT pravidlo a Firewall (dále jen FW) pravidlo. DNAT pravidlo nastavte překlad veřejná IP adresa na interní IP adresu cílového serveru, port a ve FW pak uveďte zdroj, tj. důvěryhodné IP adresy, ty IP adresy, ze kterých na server budete přistupovat, cíl: IP adresa nebo IP set odpovídající cílovému VM, protocol TCP a port v případě Windows RDP je 3389, v případě SSH je to tcp/21. Port lze ještě z důvodu bezpečnosti změnit na jiný.

6) **Problém: V security logu Windows serveru jsou neúspěšné pokusy o přihlášení na server**
   ŘEŠENÍ: ověřte, že jsou nastaveny ve zdroji pravidla pro připojení na RDP či SSH ve FW jen zdrojové IP adresy, ze kterých se na server připojujete. Source by nemělo být „Any“ z důvodu bezpečnosti.

23 Nahlášení incidentu, nedostupnosti, nebo prověření služby

Pro nahlášení incidentu, nedostupnosti, nebo prověření služby kontaktujte **bezplatnou linku 800 333 777**, kde pod volbou **3 zvolte „ICT“**.
Linka je **dostupná nonstop v režimu 24×7**.

Během hovoru od Vás bude požadováno:

- Název služby, kterou chcete prověřit: **O2 Cloud**, nebo **O2 Virtuální datové centrum**
- **Identifikátor služby:** <na předávacím protokolu>
- **Název společnosti** na kterou je služba vedena: např. Vaše společnost, s. r. o.
- **IČO společnosti** na které je služba vedena: <IČO vaší společnosti>
- Označení vašeho vDC: <jde o poslední část URL> např. VaseFirmaXY

Co by jste si měli poznamenat:

- Evidenční číslo požadavku pod kterým je evidováno – poskytne jej specialista se kterým budete hovořit

Alternativní cesta: kontaktujte **Servicedesk** přes **portál ITSM** na **url adrese**: **https://itsm.o2its.cz**
Na portále máte možnost po přihlášení založit tiket = požadavek, který následně bude předán řešitelům.
Nebo můžete napsat požadavek na **emailovou adresu sd_ict@o2.cz**.

24 Urgence a eskalace požadavku

Pro dotaz na stav nahlášeného požadavku kontaktujte **bezplatnou linku 800 333 777 ***, kde pod volbou **3 zvolte „ICT“**. **Linka je dostupná nonstop v režimu 24×7**.

Během hovoru od Vás bude požadováno:

- Název služby, které se požadavek týká: **O2 Cloud**, nebo **O2 Virtuální datové centrum**
- **Evidenční číslo požadavku**: <dle informace při nahlášení>
- **Název společnosti** na kterou je služba vedena: např. Vaše společnost, s. r. o.
- **IČO společnosti** na které je služba vedena: <IČO vaší společnosti>

**** Pokud máte přiděleného servisního manažera, můžete se s urgencí, či eskalací obrátit na něj.***