NetScaler VPX 14.1

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Matrice de prise en charge de NetScaler VPX

October 17, 2024

Ce document répertorie les différents hyperviseurs et fonctionnalités pris en charge sur une instance NetScaler VPX. Le document décrit également leurs consignes d'utilisation et leurs limitations connues.

Instance VPX sur l'hyperviseur VMware ESX

Version ESXi	Date de sortie d'ESXi (AAAA/MM/JJ)	Numéro de build ESXi	Version de NetScaler VPX	Gamme de performances
———————-	———————————-	——————	——————————	——————
ESXi 8.0 mise à jour 3	2024/06/25	24022510	Versions 14.1-17.x et supérieures	10 Mbps à 100 Gbps
ESXi 8.0 mise à jour 2b	2024/03/05	23825572	Versions 14.1-17.x et supérieures	^^
ESXi 8.0 mise à jour 2	2024/02/29	23305546	Versions 14.1-4.x et supérieures	^^
ESXi 8.0 mise à jour 2	2023/09/21	22380479	Versions 14.1-4.x et supérieures	^^
ESXi 8.0 mise à jour 1	2023/04/18	21495797	Versions 14.1-4.x et supérieures	^^
ESXi 8.0 c	2023/03/30	21493926	Versions 14.1-4.x et supérieures	^^
ESXi 8.0	10/2022/11	20513097	Versions 14.1-4.x et supérieures	^^
ESXi 7.0 mise à jour 3o	2024/03/05	23794027	Versions 14.1-17.x et supérieures	^^
Mise à jour 3n d'ESXi 7.0	Navigateurs pris en charge	23307199	Versions 14.1-4.x et supérieures	^^
Mise à jour ESXi 7.0 3m	2023/09/28	22348816	Versions 14.1-4.x et supérieures	^^
Mise à jour 3n d'ESXi 7.0	2023/07/06	21930508	Versions 14.1-8.x et supérieures	^^
Mise à jour ESXi 7.0 3m	2023/05/03	21686933	Versions 14.1-4.x et supérieures	^^

> **Remarque :**
>
> La prise en charge de chaque correctif ESXi est validée sur la version de NetScaler VPX spécifiée dans le tableau précédent et s'applique à toutes les versions supérieures de la version NetScaler VPX 14.1.

Pour plus d'informations sur les directives d'utilisation, consultez la section Directives d'utilisation de l'hyperviseur VMware ESXi.

Instance VPX sur XenServer ou Citrix Hypervisor

Version XenServer ou Citrix Hypervisor	SysID	Gamme de performances
8.4, pris en charge à partir de NetScaler VPX version 14.1 build 17.x 8.2, prise en charge à partir de NetScaler VPX version 13.0 build 64.x 8.0, 7.6, 7.1	450000	10 Mbps à 40 Gbps

Instance VPX sur Microsoft Hyper-V

Version Hyper-V	SysID	Gamme de performances
2016, 2019	450020	10 Mbps à 3 Gbps

Instance VPX sur Nutanix AHV

NetScaler VPX est pris en charge sur Nutanix AHV dans le cadre du partenariat Citrix Ready. Citrix Ready est un programme de partenariat technologique qui aide les fournisseurs de logiciels et de matériel à développer et à intégrer leurs produits avec la technologie NetScaler pour les espaces de travail numériques, les réseaux et les analyses. Citrix Ready est un programme de partenariat technologique qui aide les fournisseurs de logiciels et de matériel à développer et à intégrer leurs produits avec la technologie NetScaler pour l'espace de travail numérique, la mise en réseau et l'analyse.

Pour plus d'informations sur la méthode étape par étape permettant de déployer une instance NetScaler VPX sur Nutanix AHV, consultez Déploiement d'un NetScaler VPX sur Nutanix AHV.

Assistance par des tiers :

Si vous rencontrez des problèmes lors de l'intégration d'un tiers en particulier (Nutanix AHV) dans un environnement NetScaler, signalez un incident de support directement auprès du partenaire tiers (Nutanix).

Si le partenaire détermine que le problème semble provenir de NetScaler, il peut contacter le support NetScaler pour obtenir une assistance supplémentaire. Une ressource technique dédiée provenant de partenaires travaille avec l'équipe de support de NetScaler jusqu'à ce que le problème soit résolu.

Instance VPX sur KVM générique

Version KVM générique	SysID	Gamme de performances
RHEL 7.6, RHEL 8.0, RHEL 9.3 Ubuntu 16.04, Ubuntu 18.04, Ubuntu 22.04	450070	10 Mbps à 100 Gbps

Points à noter :

Lorsque vous utilisez les hyperviseurs KVM, tenez compte des points suivants.

- L'instance VPX est qualifiée pour les versions de version de l'Hypervisor mentionnées dans le tableau 1—4, et non pour les versions de correctifs dans une version. Toutefois, l'instance VPX devrait fonctionner de manière transparente avec les versions de correctifs d'une version prise en charge. Si ce n'est pas le cas, consignez un dossier de support pour le dépannage et le débogage.
- Avant d'utiliser RHEL 7.6, effectuez les étapes suivantes sur l'hôte KVM :
  1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
  2. Régénérez le fichier grub.cfg à l'aide de la commande `"# grub2-mkconfig -o /boot/grub2/grub.cfg"`.
  3. Redémarrez la machine hôte.
- Avant d'utiliser Ubuntu 18.04, effectuez les étapes suivantes sur l'hôte KVM :
  1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
  2. Régénérez le fichier grub.cfg à l'aide de la commande `"# grub-mkconfig -o /boot/grub/grub.cfg "`.
  3. Redémarrez la machine hôte.

Instance VPX sur les clouds publics

Cloud public	SysID	Gamme de performances
AWS	450040	10 Mbps à 30 Gbps
Azure	450020	10 Mbps à 10 Gbps

Cloud public	SysID	Gamme de performances
GCP	450070	10 Mbps à 10 Gbps

Fonctionnalités VPX prises en charge sur les hyperviseurs

Hyperviseurs →	VPX sur XenServer				VPX sur VMware ESX					
^^Caractéristiques ↓	^^		^^				^^	^^		
Interfaces →	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Émulé**	**Passage PCI**	**PV**	**PV**	**SR-IOV**	**Passage PCI**
Prise en charge multi-PE	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Prise en charge du clus-tering	Oui	Oui[1]	Oui	Oui[1]	Oui	Oui	Oui	Oui	Oui[1]	Oui
Balisage VLAN	Oui	Oui	Oui	Oui	Oui	Oui	Oui (unique-ment sur 2012R2)	Oui	Oui	Oui
Détection des événe-ments de lien/HA-Mon	Non[2]	Oui[3]	Non[2]	Oui[3]	Non[2]	Oui[3]	Non[2]	Non[2]	Oui[3]	Oui[3]

^^Caractéristiques ↓	^^		^^				^^	^^		
Configuration des paramètres d'interface	Non	Non	Non	Non	Non	Oui	Non	Non	Non	Oui
LA statique	Oui[2]	Oui[3]	Oui[2]	Non	Oui[2]	Oui[3]	Oui[2]	Oui[2]	Oui[3]	Oui[3]
LACP	Non	Oui[3]	Oui[2]	Non	Oui[2]	Oui[3]	Non	Oui[2]	Oui[3]	Oui[3]
CLAG statique	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
CLAG de la C.A.L.P.	Non	Non	Oui[2]	Non	Oui[2]	Oui[3]	Non	Oui[2]	Oui[3]	Oui[3]
Branchement à chaud	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non

Fonctionnalités VPX prises en charge sur les clouds publics

Clouds publics →	VPX sur AWS	VPX sur Azure	VPX sur GCP
^^Caractéristiques ↓	^^	^^	^^
Prise en charge multi-PE	Oui	Oui	Oui
Prise en charge du clustering	Non	Non	Non
Balisage VLAN	Non	Non	Non

^^Caractéristiques ↓	^^	^^	^^
Détection des événements de lien/HAMon	Non[2]	Non[2]	Non[2]
Configuration des paramètres d'interface	Non	Non	Non
LA statique	Non	Non	Non
LACP	Non	Non	Non
CLAG statique	Non	Non	Non
CLAG de la C.A.L.P.	Non	Non	Non
Branchement à chaud	Oui	Non	Non

Les numéros en exposant (1, 2, 3) utilisés dans les deux tableaux précédents font référence aux points suivants avec leur numérotation respective :

1. La prise en charge du clustering est disponible sur SRIOV pour les interfaces côté client et côté serveur, et non pour le fond de panier.
2. Les événements Interface DOWN ne sont pas enregistrés dans les instances NetScaler VPX.
3. Pour LA statique, le trafic peut toujours être envoyé sur l'interface dont l'état physique est DOWN.

Les points suivants s'appliquent aux caractéristiques respectives capturées dans les deux tableaux précédents :

- Pour LACP, le périphérique homologue connaît l'événement DOWN de l'interface basé sur le mécanisme de délai d'expiration LACP.
  - Délai d'expiration court : 3 secondes
  - Délai d'attente long : 90 secondes
- Pour LACP, ne partagez pas les interfaces entre les machines virtuelles.
- Pour le routage dynamique, le temps de convergence dépend du protocole de routage car les événements de liaison ne sont pas détectés.
- La fonctionnalité Routage statique surveillé échoue si vous ne liez pas les moniteurs à des routes statiques, car l'état de l'itinéraire dépend de l'état du VLAN. L'état du VLAN dépend de l'état de la liaison.

- La détection de défaillance partielle ne se produit pas en haute disponibilité en cas de défaillance de liaison. Une condition cérébrale divisée à haute disponibilité peut se produire en cas de défaillance de liaison.
  - Lorsqu'un événement de lien (désactiver/activer, réinitialiser) est généré à partir d'une instance VPX, l'état physique du lien ne change pas. Pour LA statique, tout trafic initié par le pair est supprimé sur l'instance.
  - Pour que la fonctionnalité de balisage VLAN fonctionne, sur VMware ESX, définissez l'ID VLAN du groupe de ports sur 1–4095 sur le vSwitch du serveur VMware ESX.
- Le branchement à chaud n'est pas pris en charge sur les instances VPX dotées d'interfaces ENA, et le comportement des instances peut être imprévisible en cas de tentative de branchement à chaud. L'ajout à chaud n'est pris en charge que pour les interfaces PV et SRIOV avec NetScaler sur AWS.
- La suppression à chaud via la console Web AWS ou l'interface CLI AWS n'est pas prise en charge avec les interfaces PV, SRIOV et ENA pour NetScaler. Le comportement des instances peut être imprévisible si la suppression à chaud est tentée.

Navigateurs pris en charge

Système d'exploitation	Navigateur et versions
Windows 7	Internet Explorer - 8, 9, 10 et 11 ; Mozilla Firefox 3.6.25 et versions ultérieures ; Google Chrome - 15 et versions ultérieures
Windows 64 bits	Internet Explorer - 8, 9 ; Google Chrome - 15 et versions ultérieures
MAC	Mozilla Firefox - 12 et versions ultérieures ; Safari - 5.1.3 ; Google Chrome - 15 et versions ultérieures

Prise en charge des processeurs AMD pour les instances VPX

À partir de la version 13.1 de NetScaler, l'instance VPX prend en charge à la fois les processeurs Intel et AMD. Les appliances virtuelles VPX peuvent être déployées sur n'importe quel type d'instance doté d'au moins deux cœurs virtualisés et de plus de 2 Go de mémoire. Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

Plateforme VPX vs. Tableau de matrice NIC

Le tableau suivant répertorie les cartes réseau prises en charge sur une plate-forme VPX ou un cloud.

Cartes réseau →	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/XL710 SRIOV VF	Mode de transfert PCI Intel X710/XL710/XXV710
^^Plateformes ↓	^^	^^	^^	^^	^^	^^
VPX (ESXi)	Non	Oui	Non	Oui	Non	Oui
VPX (Citrix Hypervi-sor)	S/O	S/O	S/O	Oui	Oui	Non
VPX (KVM)	Non	Oui	Oui	Oui	Oui	Non
VPX (Hyper-V)	S/O	S/O	S/O	Non	Non	Non
VPX (AWS)	S/O	S/O	S/O	Oui	S/O	S/O
VPX (Azure)	Oui	Oui	Oui	S/O	S/O	S/O
VPX (GCP)	S/O	S/O	S/O	S/O	S/O	S/O

Autres références

- Pour les produits Citrix Ready, visitez Citrix Ready Marketplace.
- Pour obtenir le support produit Citrix Ready, consultez la page FAQ.
- Pour les versions matérielles VMware ESX, consultez Mise à niveau de VMware Tools.

Optimisez les performances de NetScaler VPX sur VMware ESX, Linux KVM et Citrix Hypervisors

October 17, 2024

Les performances de NetScaler VPX varient considérablement en fonction de l'hyperviseur, des ressources système allouées et des configurations de l'hôte. To achieve the desired performance, first follow the recommendations in the VPX data sheet, and then further optimize it using the best practices provided in this document.

Instance NetScaler VPX sur des hyperviseurs VMware ESX

Cette section contient des détails sur les options et les paramètres configurables, ainsi que d'autres suggestions qui vous aideront à optimiser les performances de l'instance NetScaler VPX sur les hyperviseurs VMware ESX.

- Recommended configuration on ESX hosts
- NetScaler VPX avec interfaces réseau E1000
- NetScaler VPX avec interfaces réseau VMXNET3
- NetScaler VPX avec interfaces réseau relais SR-IOV et PCI

Recommended configuration on ESX hosts

To achieve high performance for VPX with E1000, VMXNET3, SR-IOV, and PCI passthrough network interfaces, follow these recommendations:

- The total number of virtual CPUs (vCPUs) provisioned on the ESX host must be less than or equal to the total number of physical CPUs (pCPUs) on the ESX host.
- Non-uniform Memory Access (NUMA) affinity and CPU affinity must be set for the ESX host to achieve good results.

  –To find the NUMA affinity of a Vmnic, log in to the host locally or remotely, and type:

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA
Device NUMA Node: 0
```

  - To set NUMA and vCPU affinity for a VM, see VMware documentation.

NetScaler VPX avec interfaces réseau E1000

Perform the following settings on the VMware ESX host:

- On the VMware ESX host, create two vNICs from one pNIC vSwitch. Plusieurs vNIC créent plusieurs threads de réception (Rx) sur l'hôte ESX. This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.

- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX command:
  - For ESX version 5.5:

```
esxcli system settings advanced set –o /Net/NetTxWorldlet
    –i
```

  - For ESX version 6.0 onwards:

```
esxcli system settings advanced set -o /Net/NetVMTxType –i
    1
```

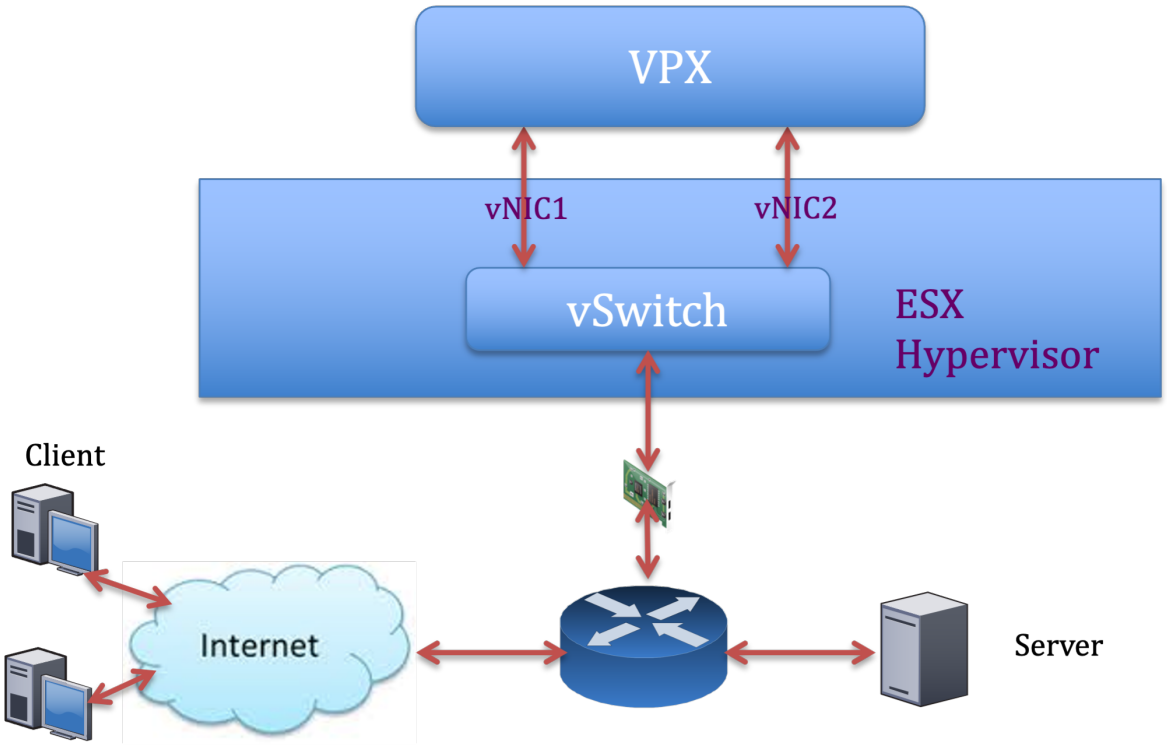
- To further increase the vNIC Tx throughput, use a separate Tx completion thread and Rx threads per device (NIC) queue. Use the following ESX command:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
```

> **Remarque :**
>
> Make sure that you reboot the VMware ESX host to apply the updated settings.

Two vNICs per pNIC deployment

The following is a sample topology and configuration commands for the **Two vNICs per pNIC** model of deployment that delivers better network performance.



Exemple de configuration de NetScaler VPX :

Pour réaliser le déploiement illustré dans l'exemple de topologie précédent, effectuez la configuration suivante sur l'instance NetScaler VPX :

- On the client side, bind the SNIP (1.1.1.2) to network interface 1/1 and enable the VLAN tag mode.

```
1    bind vlan 2 -ifnum 1/1 – tagged
2    bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
```

- On the server side, bind the SNIP (2.2.2.2) to network interface 1/1 and enable the VLAN tag mode.

```
1    bind vlan 3 -ifnum 1/2 – tagged
2    bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
```

- Add an HTTP virtual server (1.1.1.100) and bind it to a service (2.2.2.100).

```
1    add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
        Listenpolicy None -cltTimeout 180
2    add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -
        maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -
        cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
3    bind lb vserver v1 s1
```


> **Remarque :**
>
> Make sure that you include the following two entries in the route table:
>
> - 1.1.1.0/24 subnet with gateway pointing to SNIP 1.1.1.2
> - 2.2.2.0/24 subnet with gateway pointing to SNIP 2.2.2.2

NetScaler VPX avec interfaces réseau VMXNET3

To achieve high performance for VPX with VMXNET3 network interfaces, do the following settings on the VMware ESX host:

- Create two vNICs from one pNIC vSwitch. Multiple vNICs create multiple Rx threads in the ESX host. This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX commands:
  - For ESX version 5.5:

```
esxcli system settings advanced set –o /Net/NetTxWorldlet –i
```

  - For ESX version 6.0 onwards:

```
esxcli system settings advanced set -o /Net/NetVMTxType –i 1
```

On the VMware ESX host, perform the following configuration:

- On the VMware ESX host, create two vNICs from 1 pNIC vSwitch. Multiple vNICs create multiple Tx and Rx threads in the ESX host. This increases the Tx and Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase Tx throughput of a vNIC, use a separate Tx completion thread and Rx threads per device (NIC) queue. Utilisez la commande suivante :

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
```

- Configure a VM to use one transmit thread per vNIC, by adding the following setting to the VM's configuration:

```
ethernetX.ctxPerDev = "1"
```

- Configurez une machine virtuelle pour utiliser jusqu'à 8 threads de transmission par vNIC, en ajoutant le paramètre suivant à la configuration de la machine virtuelle :


```
ethernetX.ctxPerDev = "3"
```

> **Remarque :**
>
> L'augmentation du nombre de threads de transmission par vNIC nécessite davantage de ressources CPU (jusqu'à 8) sur l'hôte ESX. Assurez-vous que des ressources CPU suffisantes sont disponibles avant de définir les paramètres précédents.

> **Remarque :**
>
> Make sure that you reboot the VMware ESX host to apply the updated settings.

You can configure VMXNET3 as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment.

Configuration de la prise en charge des files d'attente multiples et du flux RSS sur les appareils VMware ESX pour VMXNET3 Par défaut, le périphérique VMXNET3 ne prend en charge que 8 files d'attente Rx et Tx. Lorsque le nombre de vCPU sur le VPX dépasse 8, le nombre de files d'attente Rx et Tx configurées pour une interface VMXNET3 passe à 1 par défaut. Vous pouvez configurer jusqu'à 19 files d'attente Rx et Tx pour les périphériques VMXNET3 en modifiant certaines configurations sur ESX. Cette option augmente les performances et la distribution uniforme des paquets sur les vCPU de l'instance VPX.

> **Remarque :**
>
> À partir de la version 13.1 build 48.x de NetScaler, le NetScaler VPX prend en charge jusqu'à 19 files d'attente Rx et Tx sur ESX pour les appareils VMXNET3.

Pré-requis :

Pour configurer jusqu'à 19 files d'attente Rx et Tx sur les appareils ESX pour VMXNET3, assurez-vous que les conditions préalables suivantes sont remplies :

- La version de NetScaler VPX est 13.1 build 48.X et versions ultérieures.
- NetScaler VPX est configuré avec une machine virtuelle de version matérielle 17 ou ultérieure, prise en charge par VMware ESX 7.0 et versions ultérieures.

Configurez les interfaces VMXNET3 pour prendre en charge plus de 8 files d'attente Rx et Tx :

1. Ouvrez le fichier de configuration de la machine virtuelle (.vmx).
2. Spécifiez le nombre de files d'attente Rx et TX en configurant les valeurs `ethernetX.maxTxQueues` et `ethernetX.maxRxQueues` (X étant le nombre de cartes réseau virtuelles à configurer). Le nombre maximum de files d'attente configurées ne doit pas être supérieur au nombre de vCPU de la machine virtuelle.

> **Remarque :**
>
> L'augmentation du nombre de files d'attente augmente également la surcharge du processeur sur l'hôte ESX. Par conséquent, assurez-vous que des ressources CPU suffisantes sont disponibles sur l'hôte ESX avant d'augmenter les files d'attente. Vous pouvez augmenter le nombre maximum de files d'attente prises en charge, dans les scénarios où le nombre de files d'attente est considéré comme un obstacle aux performances. Dans ces situations, nous recommandons d'augmenter progressivement le nombre de files d'attente. Par exemple, de 8 à 12, puis à 16, puis à 20, et ainsi de suite. Évaluez les performances à chaque réglage, plutôt que de les augmenter directement jusqu'à la limite maximale.

NetScaler VPX avec interfaces réseau relais SR-IOV et PCI

Pour obtenir des performances élevées pour NetScaler VPX avec des interfaces réseau SR-IOV et PCI passthrough, consultez Configuration recommandée sur les hôtes ESX.

Consignes d'utilisation de l'hyperviseur VMware ESXi

- Nous vous recommandons de déployer une instance NetScaler VPX sur des disques locaux du serveur ou des volumes de stockage basés sur SAN.

  Consultez la section **Considérations relatives au processeur VMware ESXi** dans le document Meilleures pratiques en matière de performances pour VMware vSphere 6.5. Voici un extrait :
- Il n'est pas recommandé de déployer des machines virtuelles sollicitant beaucoup de CPU ou de mémoire sur un hôte ou un cluster surchargé.
- Dans la plupart des environnements, ESXi permet des niveaux significatifs de surcharge du processeur sans affecter les performances des machines virtuelles. Sur un hôte, vous pouvez exécuter plus de processeurs virtuels que le nombre total de cœurs de processeur physiques de cet hôte.
- Si un hôte ESXi devient saturé en processeur, c'est-à-dire que les machines virtuelles et les autres charges sur l'hôte exigent toutes les ressources CPU dont dispose l'hôte, les charges de travail sensibles à la latence risquent de ne pas fonctionner correctement. Dans ce cas, réduisez la charge du processeur, par exemple, en éteignant certaines machines virtuelles ou en les migrant vers un autre hôte (ou en autorisant DRS à les migrer automatiquement).
- NetScaler recommande d'utiliser la dernière version de compatibilité matérielle pour bénéficier des derniers ensembles de fonctionnalités de l'hyperviseur ESXi pour la machine virtuelle. Pour plus d'informations sur la compatibilité entre le matériel et les versions d'ESXi, consultez la documentation VMware.

- Le NetScaler VPX est une appliance virtuelle haute performance sensible à la latence. Pour atteindre les performances attendues, l'appliance nécessite la réservation du processeur virtuel, la réservation de la mémoire et l'épinglage du processeur virtuel sur l'hôte. En outre, l'hyper thread doit être désactivé sur l'hôte. Si l'hôte ne répond pas à ces exigences, les problèmes suivants peuvent survenir :

  - Basculement à haute disponibilité
  - Pic de processeur au sein de l'instance VPX
  - Lenteur lors de l'accès à la CLI VPX
  - Crash du démon Pit Boss
  - Gouttes de paquets
  - Débit faible

- Un Hypervisor est considéré comme surapprovisionné si l'une des deux conditions suivantes est remplie :

  - Le nombre total de cœurs virtuels (vCPU) provisionnés sur l'hôte est supérieur au nombre total de cœurs physiques (PCPU).
  - Le nombre total de machines virtuelles provisionnées consomme plus de vCPU que le nombre total de processeurs physiques.

    Si une instance est surapprovisionnée, il se peut que l'hyperviseur ne garantisse pas les ressources réservées (telles que le processeur, la mémoire et autres) pour l'instance en raison des surcharges de planification de l'hyperviseur, des bogues ou des limitations avec l'hyperviseur. Ce comportement peut entraîner un manque de ressources CPU pour NetScaler et peut entraîner les problèmes mentionnés au premier point de la section **Directives d'utilisation**. Nous recommandons aux administrateurs de réduire la location de l'hôte afin que le nombre total de processeurs virtuels provisionnés sur l'hôte soit inférieur ou égal au nombre total de processeurs virtuels.

    Exemple

    Pour l'hyperviseur ESX, si le paramètre %RDY% d'un processeur virtuel VPX est supérieur à 0 dans la sortie de commande `esxtop`, l'hôte ESX est réputé avoir des frais de planification, ce qui peut entraîner des problèmes liés à la latence pour l'instance VPX.

    Dans ce cas, réduisez la location sur l'hôte afin que %RDY% revienne toujours à 0. Vous pouvez également contacter le fournisseur de l'hyperviseur pour déterminer les raisons pour lesquelles la réservation de ressources n'a pas été honorée.

Commandes pour contrôler l'utilisation du processeur du moteur de paquets

Vous pouvez utiliser deux commandes (`set ns vpxparam` et `show ns vpxparam`) pour contrôler le comportement d'utilisation du processeur du moteur de paquets (hors gestion) des instances VPX dans les environnements d'hyperviseur et de cloud :

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Autorisez chaque machine virtuelle à utiliser les ressources du processeur allouées à une autre machine virtuelle mais qui ne sont pas utilisées.

  Paramètres `Set ns vpxparam` :

  -cpuyield : libère ou ne libère pas des ressources CPU allouées mais inutilisées.

  - **OUI** : autorise l'utilisation des ressources CPU allouées mais inutilisées par une autre machine virtuelle.
  - **NON** : réservez toutes les ressources du processeur pour la machine virtuelle à laquelle elles ont été allouées. Cette option affiche un pourcentage plus élevé dans les environnements d'hyperviseur et de cloud pour l'utilisation du processeur VPX.
  - **DEFAULT** : Non.

  > **Remarque :**
  >
  > Sur toutes les plateformes NetScaler VPX, l'utilisation du processeur virtuel sur le système hôte est de 100 %. Utilisez la commande `set ns vpxparam –cpuyield YES` pour annuler cette utilisation.

  Si vous souhaitez définir les nœuds du cluster sur « rendement », vous devez effectuer les configurations supplémentaires suivantes sur CCO :

  - Si un cluster est formé, tous les nœuds sont définis sur « YIELD=default ».
  - Si un cluster est formé à l'aide des nœuds déjà définis sur « Yield=YES », les nœuds sont ajoutés au cluster en utilisant le rendement « DEFAULT ».

  > **Remarque :**
  >
  > Si vous souhaitez définir les nœuds du cluster sur « YIELD=YES », vous pouvez configurer uniquement après la formation du cluster, mais pas avant la formation du cluster.

  -masterclockcpu1 : Vous pouvez déplacer la source d'horloge principale de CPU0 (CPU de gestion) vers CPU1. Ce paramètre a les options suivantes :

  - **OUI** : Autorisez la machine virtuelle à déplacer la source d'horloge principale de CPU0 vers CPU1.

  - **NON** : VM utilise CPU0 pour la source d'horloge principale. Par défaut, CPU0 est la principale source d'horloge.

- `show ns vpxparam`

  Cette commande affiche les paramètres `vpxparam` actuels.

Instance NetScaler VPX sur la plateforme Linux-KVM

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aideront à optimiser les performances de l'instance NetScaler VPX sur la plate-forme Linux-KVM.

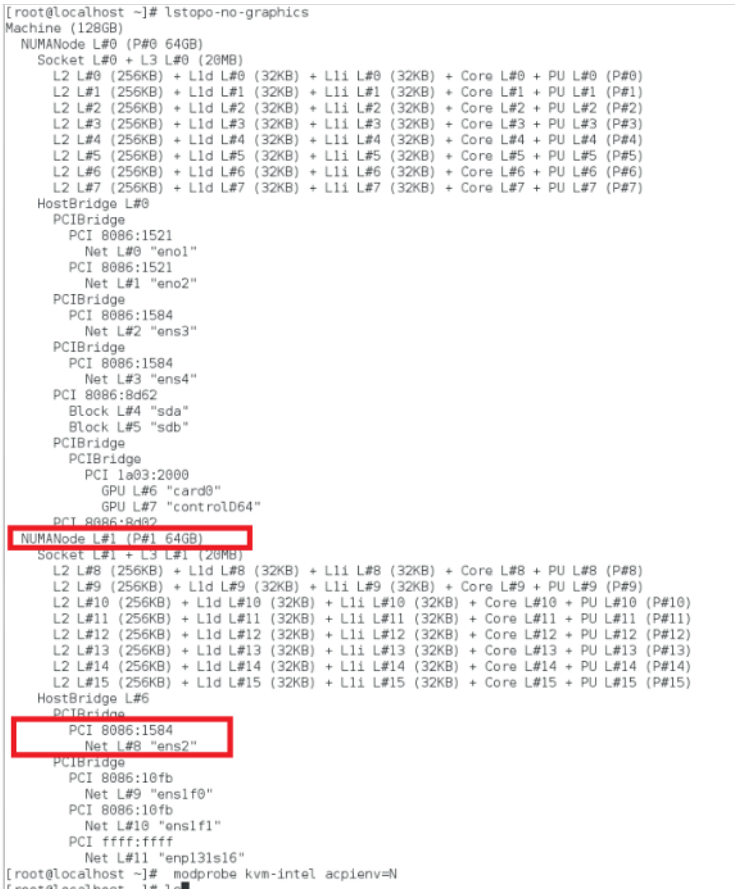
- Paramètres de performance pour KVM
- NetScaler VPX avec interfaces réseau photovoltaïque
- NetScaler VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

Paramètres de performance pour KVM

Perform the following settings on the KVM host:

Find the NUMA domain of the NIC using the `lstopo` command:

Make sure that memory for the VPX and the CPU is pinned to the same location. In the following output, the 10G NIC "ens2"is tied to NUMA domain #1.



Allocate the VPX memory from the NUMA domain.

The `numactl` command indicates the NUMA domain from which the memory is allocated. In the following output, around 10 GB RAM is allocated from NUMA node #0.

```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 55854 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 52388 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

To change the NUMA node mapping, follow these steps.

1. Modifiez le .xml du VPX sur l'hôte.

```
1    /etc/libvirt/qemu/<VPX_name>.xml
```


2. Ajoutez la balise suivante :

```
<numatune>
<memory mode="strict" nodeset="1"/>    This is the NUMA domain name
</numatune>
```

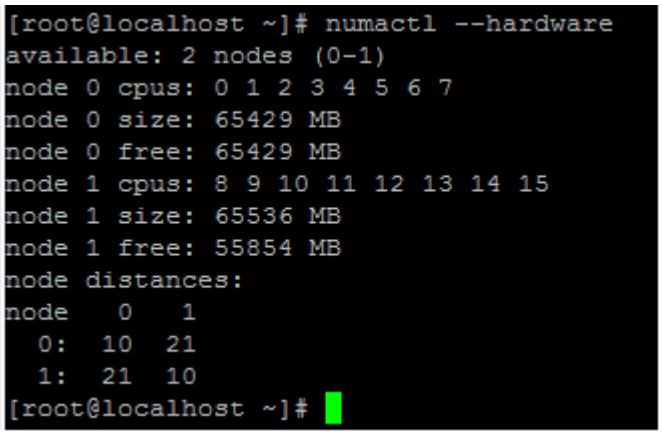
3. Arrêtez le VPX.

4. Exécutez la commande suivante :

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
```

   Cette commande met à jour les informations de configuration de la machine virtuelle avec les mappages de nœuds NUMA.

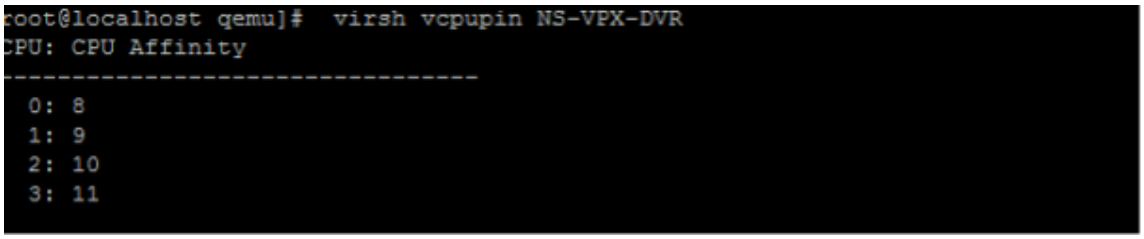
5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `numactl –hardware` commande sur l'hôte pour voir les allocations de mémoire mises à jour pour le VPX.



Pin vCPUs of VPX to physical cores.

- Pour afficher les mappages vCPU vers PCPU d'un VPX, tapez la commande suivante

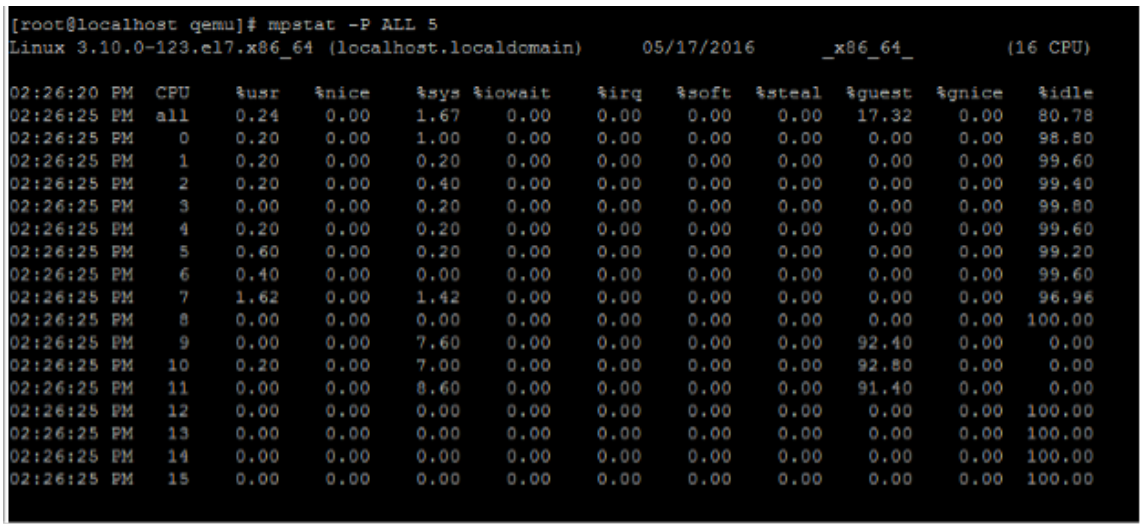
```
virsh vcpupin <VPX name>
```



  Les vCPU 0—4 sont mappés sur les cœurs physiques 8 à 11.

- Pour afficher l'utilisation actuelle du PCPU, tapez la commande suivante :

```
mpstat -P ALL 5
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

Dans cette sortie, 8 correspond au processeur de gestion et 9 à 11 aux moteurs de paquets.

- Pour changer le vCPU en épinglage PCPU, il existe deux options.
  - Modifiez-le au moment de l'exécution après le démarrage du VPX à l'aide de la commande suivante :

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
```

  - Pour apporter des modifications statiques au VPX, modifiez le `.xml` fichier comme précédemment avec les balises suivantes :
    1. Modifiez le fichier .xml du VPX sur l'hôte

```
/etc/libvirt/qemu/<VPX_name>.xml
```

    2. Ajoutez la balise suivante :

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
```

    3. Arrêtez le VPX.
    4. Mettez à jour les informations de configuration de la machine virtuelle avec les map-pages de nœuds NUMA à l'aide de la commande suivante :

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
```


5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `virsh vcpupin <VPX name>` commande sur l'hôte pour voir l'épinglage du processeur mis à jour.

Eliminate host interrupt overhead.

- Détectez VM_EXITS à l'aide de la `kvm_stat` commande.

  Au niveau de l'hyperviseur, les interruptions de l'hôte sont mappées sur les mêmes processeurs sur lesquels les vCPU du VPX sont épinglés. Cela peut entraîner le retrait périodique des processeurs virtuels sur le VPX.

  Pour trouver les sorties de machine virtuelle effectuées par les machines virtuelles exécutant l'hôte, utilisez la `kvm_stat` commande.

  ```
  [root@localhost ~]# kvm_stat -1  | grep EXTERNAL
  kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
  [root@localhost ~]#
  ```

  Une valeur supérieure de l'ordre de 1+M indique un problème.

  Si une seule VM est présente, la valeur attendue est de 30 à 100 K. Tout ce qui dépasse cela peut indiquer qu'il existe un ou plusieurs vecteurs d'interruption d'hôte mappés sur le même pCPU.

- Détectez les interruptions de l'hôte et migrez les interruptions de l'hôte.

  Lorsque vous exécutez la `concatenate` commande pour le fichier « /proc/interrupts », elle affiche tous les mappages d'interruption de l'hôte. Si un ou plusieurs IRQ actifs sont mappés sur le même PCPU, le compteur correspondant est incrémenté.

  Déplacez toutes les interruptions qui se chevauchent avec les processeurs de votre NetScaler VPX vers les processeurs non utilisés :

  ```
  echo 0000000f > /proc/irq/55/smp_affinity
  0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
     only be scheduled on pCPUs 0 – 3
  ```

- Désactivez la balance IRQ.

  Désactivez le démon d'équilibrage de l'IRQ, de sorte qu'aucune replanification ne se produise à la volée.

  ```
  service irqbalance stop
  service irqbalance show - To check the status
  service irqbalance start - Enable if needed
  ```

  Assurez-vous d'exécuter la commande `kvm_stat` pour vous assurer qu'il n'y a pas beaucoup de compteurs.

NetScaler VPX avec interfaces réseau photovoltaïque

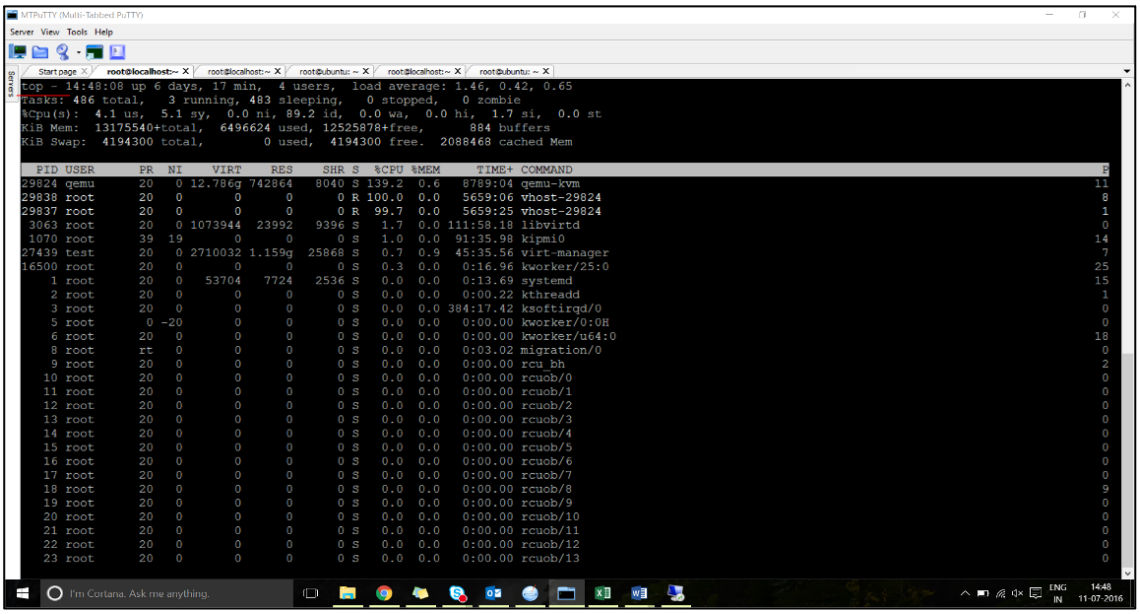
You can configure para-virtualization (PV), SR-IOV, and PCIe passthrough network interfaces as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment.

For optimal performance of PV (virtio) interfaces, follow these steps:

- Identifiez le domaine NUMA auquel appartient le slot/NIC PCIe.
- La mémoire et le processeur virtuel du VPX doivent être épinglés au même domaine NUMA.
- Le thread Vhost doit être lié aux processeurs du même domaine NUMA.

Bind the virtual host threads to the corresponding CPUs:

1. Une fois le trafic démarré, exécutez la `top` commande sur l'hôte.



2. Identifiez l'affinité du processus hôte virtuel (nommé sous le nom `vhost-<pid-of-qemu>`).
3. Liez les processus vHost aux cœurs physiques du domaine NUMA identifié précédemment à l'aide de la commande suivante :

```
taskset –pc <core-id> <process-id>
```

Exemple

```
taskset –pc 12 29838
```

4. Les cœurs de processeur correspondant au domaine NUMA peuvent être identifiés à l'aide de la commande suivante :

```
[root@localhost ~]# virsh capabilities | grep cpu
```



```
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>

        <cpus num='8'>
        <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
        <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
        <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
        <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
        <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
        <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
        <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
        <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
        </cpus>

    <cpuselection/>
    <cpuselection/>
```

Bind the QEMU process to the corresponding physical core:

1. Identifiez les cœurs physiques sur lesquels le processus QEMU est exécuté. Pour plus d'informations, reportez-vous à la sortie précédente.
2. Liez le processus QEMU aux mêmes cœurs physiques auxquels vous liez les vCPU, à l'aide de la commande suivante :

```
taskset -pc 8-11 29824
```

NetScaler VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

For optimal performance of the SR-IOV and Fortville PCIe passthrough network interfaces, follow these steps:

- Identifiez le domaine NUMA auquel appartient le slot/NIC PCIe.
- La mémoire et le vCPU de NetScaler VPX doivent être épinglés au même domaine NUMA.

Sample VPX XML file for vCPU and memory pinning for Linux KVM:

```
    <domain type='kvm'>
        <name>NetScaler-VPX</name>
        <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
```



```
<memory unit='KiB'>8097152</memory>
<currentMemory unit='KiB'>8097152</currentMemory>
<vcpu placement='static'>4</vcpu>

<cputune>
<vcpupin vcpu='0' cpuset='8'/>
<vcpupin vcpu='1' cpuset='9'/>
<vcpupin vcpu='2' cpuset='10'/>
<vcpupin vcpu='3' cpuset='11'/>
</cputune>

<numatune>
<memory mode='strict' nodeset='1'/>
</numatune>

</domain>
```

Instance NetScaler VPX sur Citrix Hypervisors

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aident à optimiser les performances de l'instance NetScaler VPX sur les hyperviseurs Citrix.

- Paramètres de performance pour Citrix Hypervisors
- NetScaler VPX avec interfaces réseau SR-IOV
- NetScaler VPX avec interfaces para-virtualisées

Paramètres de performance pour Citrix Hypervisors

Find the NUMA domain of the NIC using the "xl"command:

```
xl info -n
```

Pin vCPUs of VPX to physical cores.

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
```

Check binding of vCPUs.

```
xl vcpu-list
```

Allouez plus de 8 processeurs virtuels aux machines virtuelles NetScaler.

For configuring more than 8 vCPUs, run the following commands from the Citrix Hypervisor console:

```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
```


NetScaler VPX avec interfaces réseau SR-IOV

For optimal performance of the SR-IOV network interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot or NIC is tied to.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant.

NetScaler VPX avec interfaces para-virtualisées

For optimal performance, two vNICs per pNIC and one vNIC per pNIC configurations are advised, as in other PV environments.

To achieve optimal performance of para-virtualized (netfront) interfaces, follow these steps:

- Identifiez le domaine NUMA auquel appartient le slot PCIe ou la carte réseau.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant du même domaine NUMA.
- Épinglez les threads Rx/Tx hôtes de vNIC aux vCPU du domaine 0.

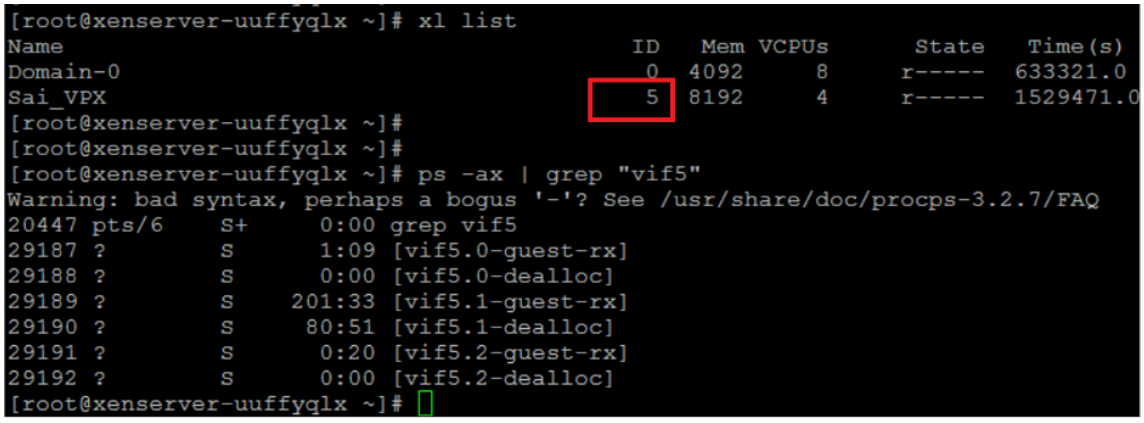
Pin host threads to Domain-0 vCPUs:

1. Recherchez l'ID Xen de NetScaler VPX en utilisant la commande `xl list` sur le shell de l'hôte Citrix Hypervisor.
2. Identifiez les threads hôtes à l'aide de la commande suivante :

   ```
   1    ps -ax | grep vif <Xen-ID>
   ```

   Dans l'exemple suivant, ces valeurs indiquent :

   - **vif5.0** - Les threads de la première interface allouée à VPX dans XenCenter (interface de gestion).
   - **vif5.1** - Les threads de la deuxième interface assignée à VPX, etc.



3. Épinglez les threads aux vCPU du domaine 0 à l'aide de la commande suivante :

```
taskset –pc <core-id> <process-id>
```

Exemple

```
taskset -pc 1 29189
```

Appliquez les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud

October 17, 2024

Vous pouvez appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans un environnement cloud. Cette étape est abordée comme étape de **pré-démarrage** dans ce document. Par conséquent, dans certains cas, comme les licences groupées ADC, une instance VPX spécifique est mise en place en beaucoup moins de temps. Cette fonctionnalité est disponible dans Microsoft Azure, Google Cloud Platform et AWS Clouds.

Qu'est-ce que les données utilisateur

Lorsque vous provisionnez une instance VPX dans un environnement cloud, vous avez la possibilité de transmettre des données utilisateur à l'instance. Les données utilisateur vous permettent d'effectuer des tâches de configuration automatisées courantes, de personnaliser les comportements de démarrage des instances et d'exécuter des scripts après le démarrage de l'instance. Au premier démarrage, l'instance NetScaler VPX exécute les tâches suivantes :

- Lit les données utilisateur.
- Interpréte la configuration fournie dans les données utilisateur.
- Applique la configuration nouvellement ajoutée au démarrage.

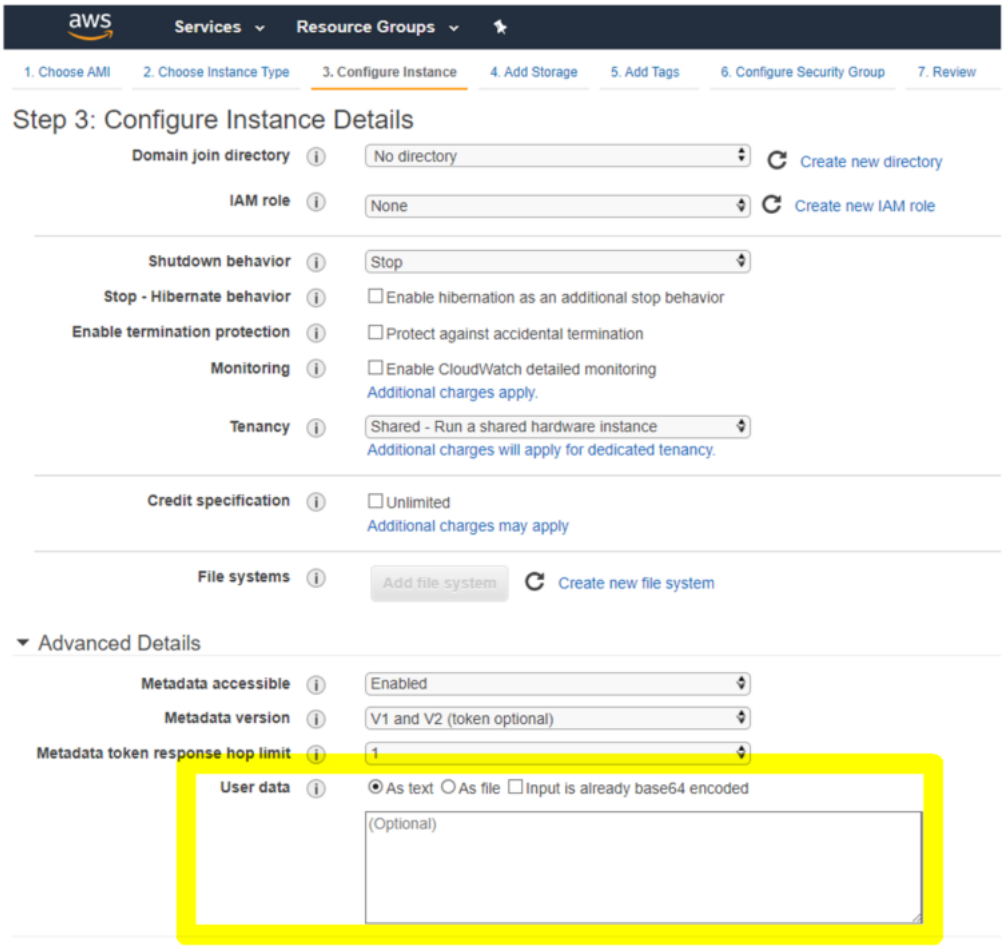
Comment fournir des données utilisateur de pré-démarrage dans une instance cloud

Vous pouvez fournir des données utilisateur de pré-démarrage à l'instance cloud au format XML. Différents clouds ont des interfaces différentes pour fournir des données utilisateur.

Fournir des données utilisateur de pré-démarrage à l'aide de la console AWS

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console AWS, accédez à Configurer les détails de l'instance > Détails avancés, puis**fournissez la configuration des données utilisateur avant le démarrage dans le champ Données utilisateur.**

Pour obtenir des instructions détaillées sur chacune des étapes, consultez Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS. Pour plus d'informations, consultez la documentation AWS sur le lancement d'une instance.



> **Remarque :**
>
> Le mode AWS IMDSv2 uniquement pour la fonctionnalité de données utilisateur avant le démarrage est pris en charge à partir de NetScaler VPX version 13.1.48.x et versions ultérieures.

Fournir des données utilisateur de pré-démarrage à l'aide de l'AWS CLI

Saisissez la commande suivante dans l'interface de ligne de commande AWS :

```
aws ec2 run-instances \
```



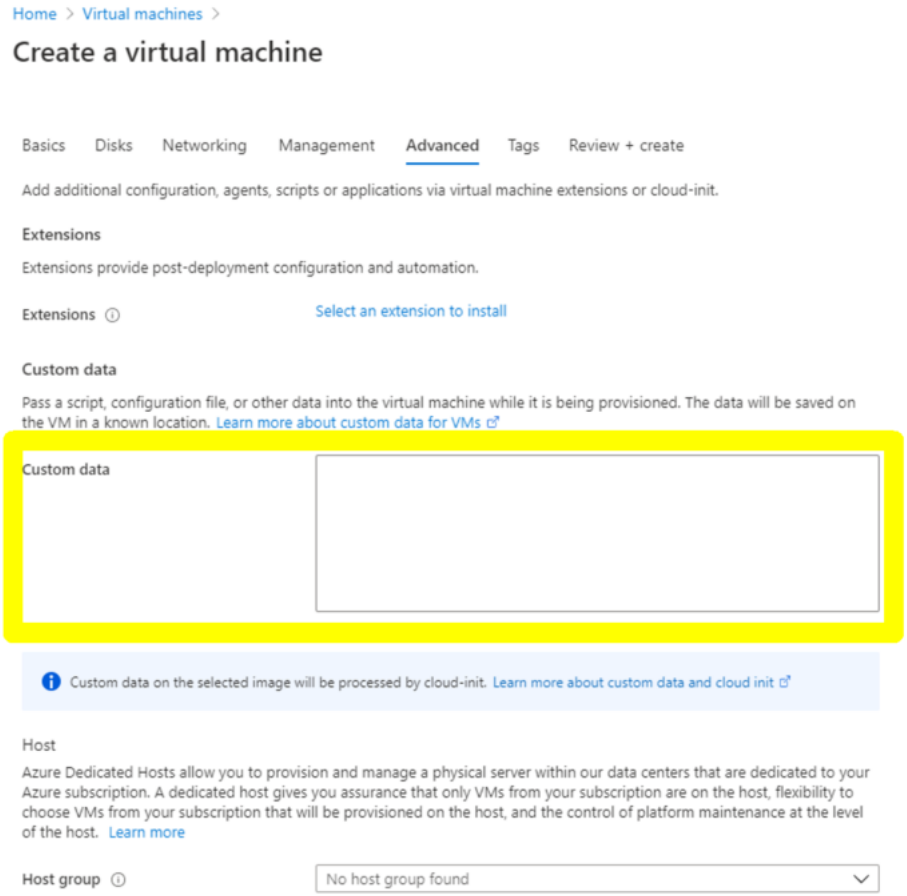
```
        --image-id ami-0abcdef1234567890 \
        --instance-type t2.micro \
        --count 1 \
        --subnet-id subnet-08fc749671b2d077c \
        --key-name MyKeyPair \
        --security-group-ids sg-0b0384b66d7d692f9 \
        --user-data file://my_script.txt
```

Pour plus d'informations, consultez la documentation AWS sur les instances en cours d'exécution.

Pour plus d'informations, consultez la documentation AWS sur l'utilisation des données utilisateur d'instance.

Fournir des données utilisateur de pré-démarrage à l'aide de la console Azure

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console Azure, accédez à l'onglet **Créer une machine virtuelle > Avancé** . Dans le champ **Données personnalisées**, indiquez la configuration des données utilisateur avant le démarrage.



Fournir des données utilisateur de pré-démarrage à l'aide de l'interface de ligne de commande Azure

Saisissez la commande suivante dans l'interface de ligne de commande Azure :

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
```

Exemple

```
az vm create --resource-group MyResourceGroup -name MyVm --image
   debian --custom-data MyCloudInitScript.txt
```

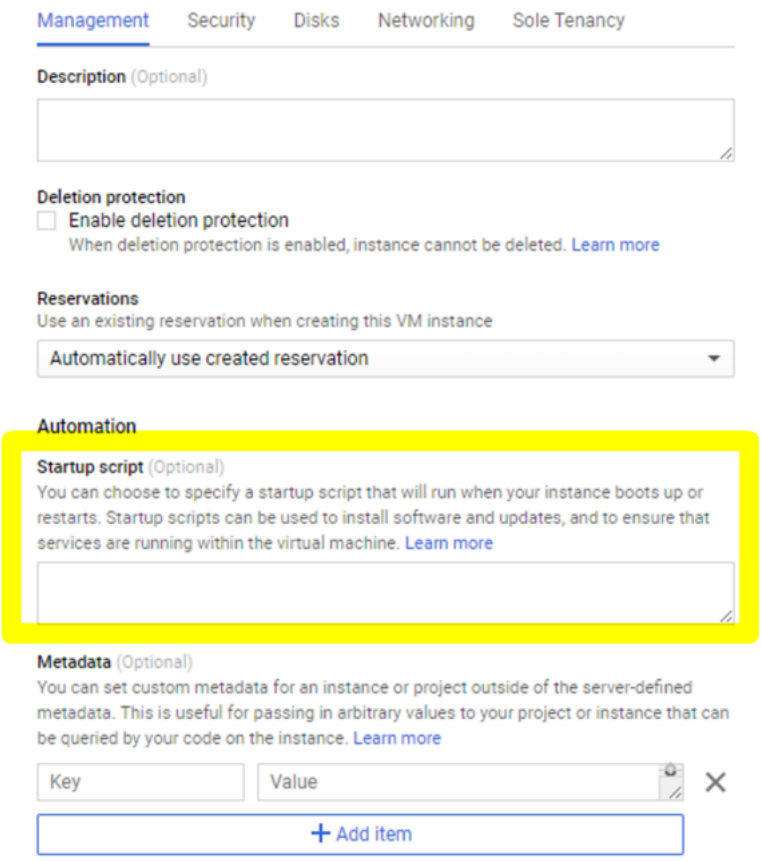
Vous pouvez transmettre vos données personnalisées ou votre configuration de prédémarrage sous forme de fichier au paramètre « —custom-data ». Dans cet exemple, le nom de fichier est **MyCloudInitScript.txt**.

Pour plus d'informations, consultez la documentation Azure CLI.

Fournir des données utilisateur de pré-démarrage à l'aide de la console GCP

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console GCP, renseignez les propriétés de l'instance. Développez **la gestion, la sécurité, les disques, la mise en réseau et la location exclusive**. Accédez à l'onglet **Gestion** . Dans la section **Automation**, indiquez la configuration des données utilisateur de **pré-démarrage dans le champ Script** de démarrage.

Pour obtenir des informations détaillées sur la création de l'instance VPX à l'aide de GCP, consultez Déployer une instance NetScaler VPX sur Google Cloud Platform.



Fournir des données utilisateur de pré-démarrage à l'aide de la CLI gcloud

Saisissez la commande suivante dans l'interface de ligne de commande GCP :

```
gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
   startup-script=LOCAL_FILE_PATH
```

metadata-from-file - Lit la valeur ou les données utilisateur à partir d'un fichier stocké dans le <LOCAL_FILE_PATH>. .

Pour plus d'informations, consultez la documentation de l'interface de ligne de commande gcloud

Format de données utilisateur de prédémarrage

Les données utilisateur de pré-démarrage doivent être fournies à l'instance cloud au format XML. Les données utilisateur de NetScaler avant le démarrage que vous fournissez via l'infrastructure cloud lors du démarrage peuvent comprendre les quatre sections suivantes :

- Configuration de NetScaler représentée par la balise. <NS-CONFIG>

- Démarrage personnalisé du NetScaler représenté par la balise <NS-BOOTSTRAP>.
- Stockage des scripts utilisateur dans NetScaler représentés par la balise. <NS-SCRIPTS>
- Configuration des licences regroupées représentée par la <NS-LICENSE-CONFIG> balise.

Vous pouvez fournir les quatre sections précédentes dans n'importe quel ordre dans la configuration de prédémarrage ADC. Assurez-vous de suivre strictement la mise en forme affichée dans les sections suivantes tout en fournissant les données utilisateur de pré-démarrage.

> **Remarque :**
>
> La configuration complète des données utilisateur de pré-démarrage doit être incluse dans la <NS-PRE-BOOT-CONFIG> balise, comme illustré dans les exemples suivants.

Exemple 1 :

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>           </NS-CONFIG>
     <NS-BOOTSTRAP>        </NS-BOOTSTRAP>
     <NS-SCRIPTS>          </NS-SCRIPTS>
     <NS-LICENSE-CONFIG>   </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
```

Exemple 2 :

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>
    <NS-CONFIG>         </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
```

Utilisez la <NS-CONFIG> balise pour fournir les configurations NetScaler VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> **Remarque :**
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

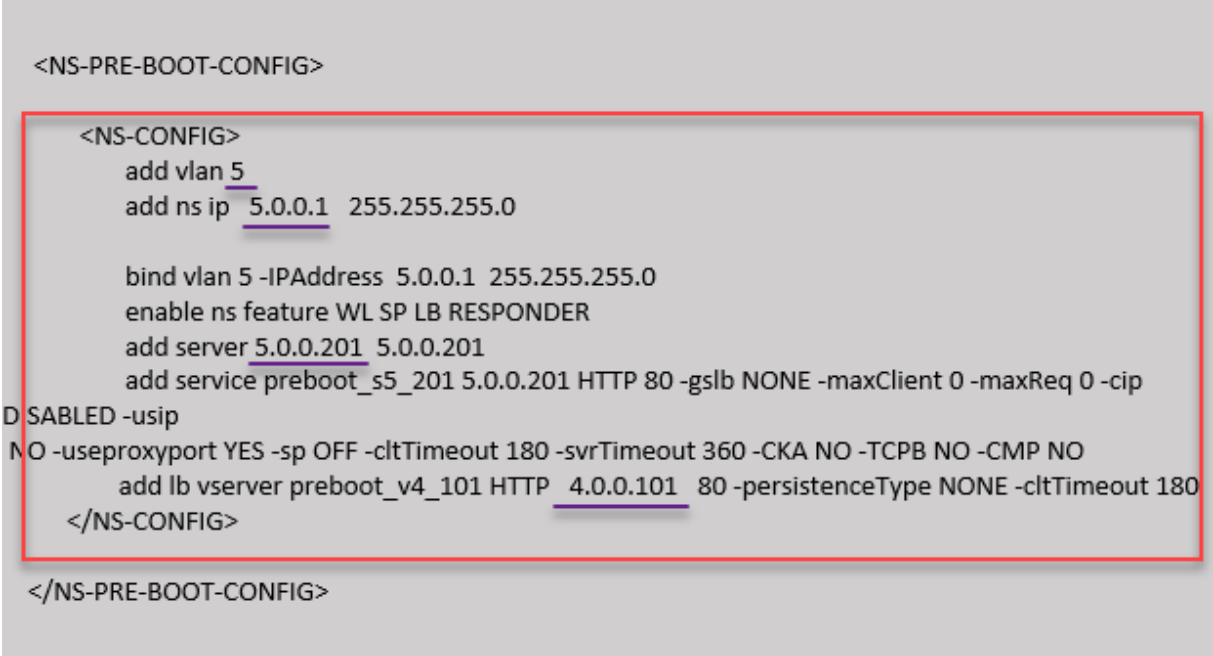
Configurations NetScaler

Utilisez la <NS-CONFIG> balise pour fournir les configurations NetScaler VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> **Remarque :**
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

Exemple

Dans l'exemple suivant, la <NS-CONFIG> section contient les détails des configurations. Un VLAN de l'ID « 5 » est configuré et lié au SNIP (5.0.0.1). Un serveur virtuel d'équilibrage de charge (4.0.0.101) est également configuré.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add vlan 5
        add ns ip 5.0.0.1 255.255.255.0
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO
     -TCPB NO -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180
    </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
```

L'instance NetScaler VPX propose la configuration appliquée dans la <NS-CONFIG> section, comme indiqué dans les illustrations suivantes.


```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -------
1)      10.160.0.72      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      5.0.0.1          0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:48/64
        Interfaces : 1/1 1/2 LO/1

2)      VLAN ID: 5      VLAN Alias Name:
        IPs :
             5.0.0.1    Mask: 255.255.255.0

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 0/1
        IPs :
             10.160.0.72        Mask: 255.255.240.0
 Done
```

```
> sh server
1)      Name:          5.0.0.201       State:ENABLED
        IPAddress:        5.0.0.201
2)      Name:    169.254.169.254       State:ENABLED
        IPAddress: 169.254.169.254
 Done
> stat service

Service(s) Summary
                           IP  port         Type        State    Req/s
preb...5_201        5.0.0.201    80         HTTP         DOWN      0/s
gcpl...vice0 169.254.169.254    53          DNS           UP      0/s
 Done
> sh service preboot_s5_201
        preboot_s5_201 (5.0.0.201:80) - HTTP
        State: DOWN
        Last state change was at Tue Dec 29 07:18:28 2020
        Time since last state change: 0 days, 00:05:02.820
        Server Name: 5.0.0.201
        Server ID : None        Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Monitoring Owner: 0
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
        Monitor Connection Close : NONE
        Appflow logging: ENABLED
        Process Local: DISABLED
```


Scripts utilisateur

Utilisez la <NS-SCRIPTS> balise pour fournir tout script qui doit être stocké et exécuté dans l'instance NetScaler VPX.

Vous pouvez inclure de nombreux scripts dans la <NS-SCRIPTS> balise. Chaque script doit être inclus dans la <SCRIPT> balise. Chaque <SCRIPT> section correspond à un script et contient tous les détails du script à l'aide des sous-balises suivantes.

- **<SCRIPT-NAME>:** Indique le nom du fichier de script qui doit être stocké.
- **<SCRIPT-CONTENT>:** Indique le contenu du fichier qui doit être stocké.
- **<SCRIPT-TARGET-LOCATION>:** Indique l'emplacement cible désigné où ce fichier doit être stocké. Si l'emplacement cible n'est pas fourni, par défaut, le fichier ou le script est enregistré dans le répertoire « /nsconfig ».
- **<SCRIPT-NS-BOOTUP>:** Spécifiez les commandes que vous utilisez pour exécuter le script.
  - Si vous utilisez <SCRIPT-NS-BOOTUP> cette section, les commandes fournies dans la section sont stockées dans « /nsconfig/nsafter.sh » et les commandes sont exécutées après le démarrage du moteur de paquets dans le cadre de l'exécution de « nsafter.sh ».
  - Si vous n'utilisez pas la <SCRIPT-NS-BOOTUP> section, le fichier de script est stocké à l'emplacement cible que vous spécifiez.

Exemple 1 :

Dans cet exemple, la <NS-SCRIPTS> balise contient des détails sur un seul script : script-1.sh. Le script « script-1.sh » est enregistré dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.

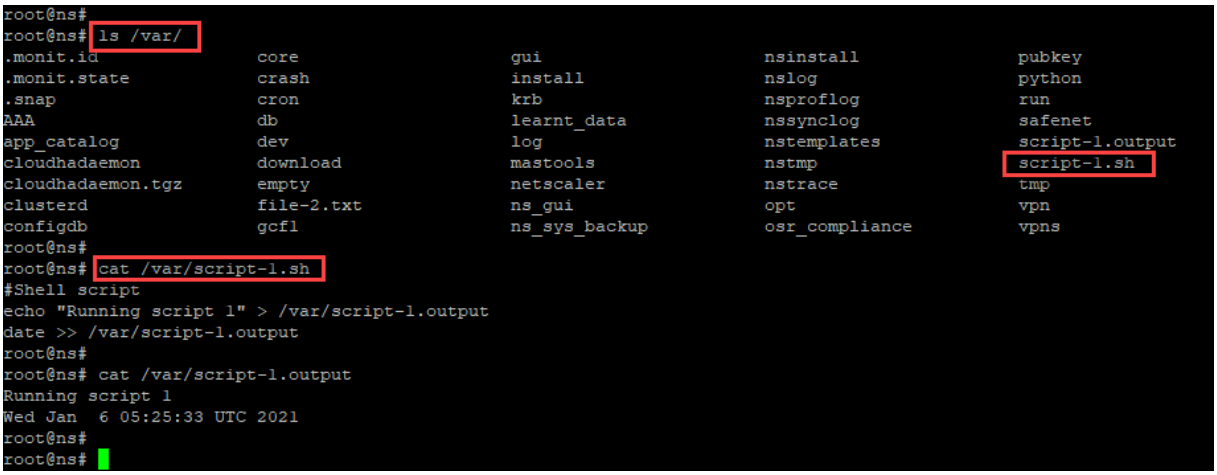
```
<NS-PRE-BOOT-CONFIG>
  <NS-SCRIPTS>
    <SCRIPT>
      <SCRIPT-CONTENT>
        #Shell script
        echo "Running script 1" > /var/script-1.output
        date >> /var/script-1.output
      </SCRIPT-CONTENT>
    <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
    <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION>
    <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
    </SCRIPT>
  </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
```


Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-
                    LOCATION>
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-
                    BOOTUP>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
```

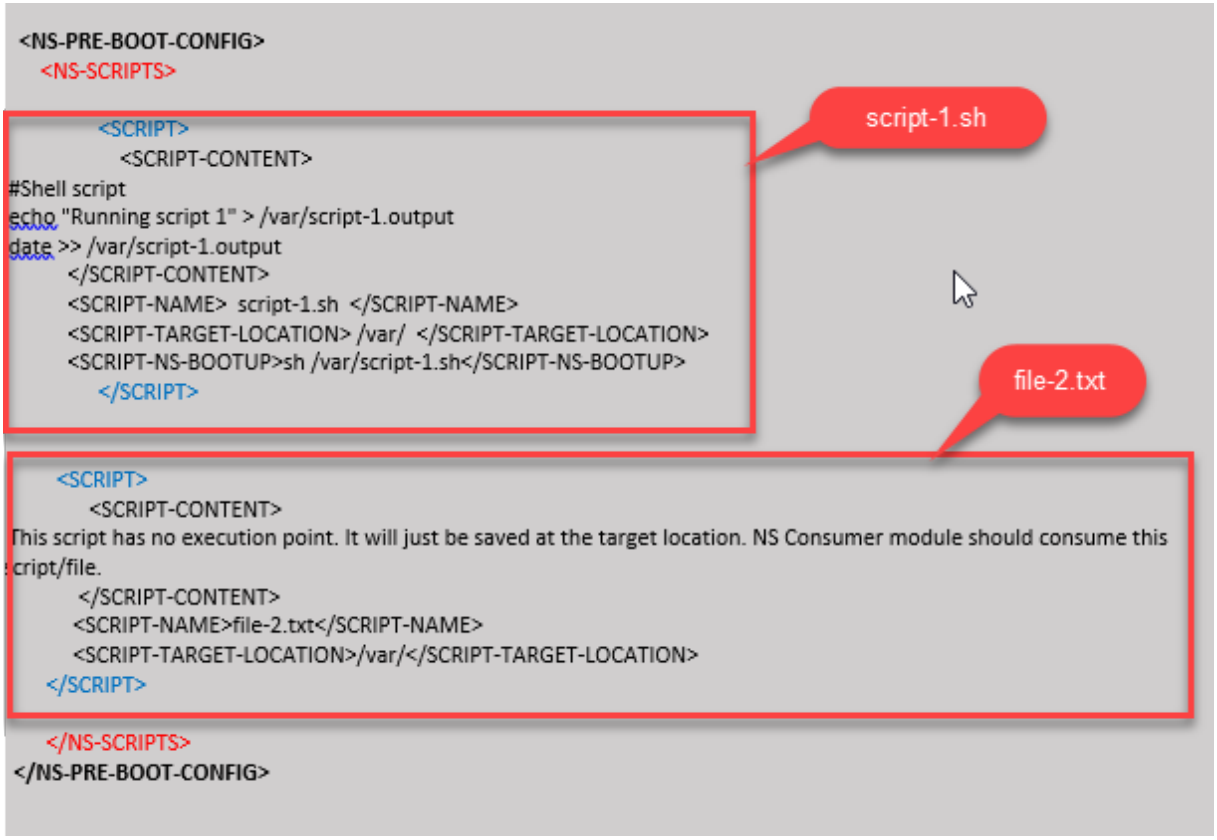
Dans l'instantané suivant, vous pouvez vérifier que le script « script-1.sh » est enregistré dans le répertoire « /var/ ». Le script « Script-1.sh » est exécuté et le fichier de sortie est créé de manière appropriée.



Exemple 2 :

Dans l'exemple suivant, la <NS-SCRIPTS> balise contient des détails sur deux scripts.

- Le premier script est enregistré sous le nom « script-1.sh » dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.
- Le deuxième script est enregistré sous le nom « file-2.txt » dans le répertoire « /var ». Ce fichier contient le contenu spécifié. Mais il n'est pas exécuté car la commande d'exécution de démarrage n'<SCRIPT-NS-BOOTUP> est pas fournie.



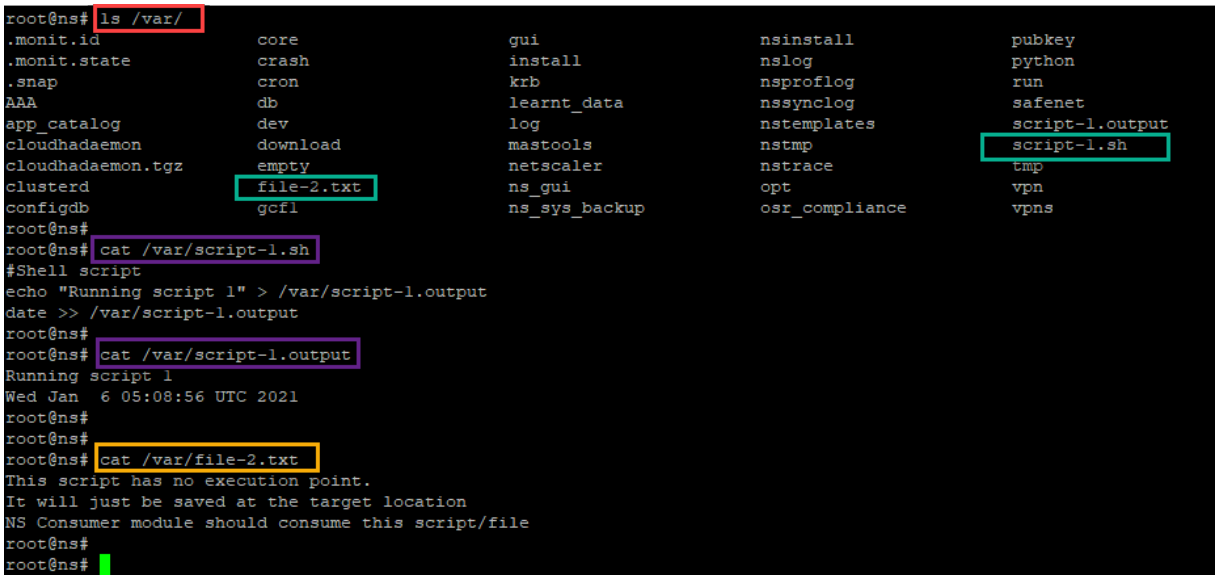
Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo "Running script 1" > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
            </SCRIPT-CONTENT>
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
```


Dans l'instantané suivant, vous pouvez vérifier que script-1.sh et file-2.txt sont créés dans le répertoire « /var/ ». Le fichier Script-1.sh est exécuté et le fichier de sortie est créé de manière appropriée.



Système de licences

Utilisez la balise <NS-LICENSE-CONFIG> pour appliquer les licences groupées NetScaler lors du démarrage de l'instance VPX. Utilisez la <LICENSE-COMMANDS> balise dans <NS-LICENSE-CONFIG> la section pour fournir les commandes de licence regroupées. Ces commandes doivent être valides syntaxiquement.

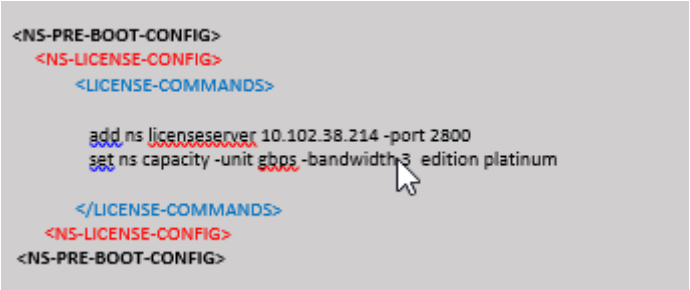
Vous pouvez spécifier les détails de licence regroupés tels que le type de licence, la capacité et le serveur de licences dans la <LICENSE-COMMANDS> section à l'aide des commandes de licences groupées standard. Pour plus d'informations, consultez la section Configurer les licences de capacité groupées NetScaler.

Après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition demandée au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences.

- Si la récupération de la licence est réussie, la bande passante configurée est appliquée à VPX.
- Si la récupération des licences échoue, la licence n'est pas extraite du serveur de licences dans les 10 à 12 minutes environ. Par conséquent, le système redémarre et entre dans un état sans licence.

Exemple

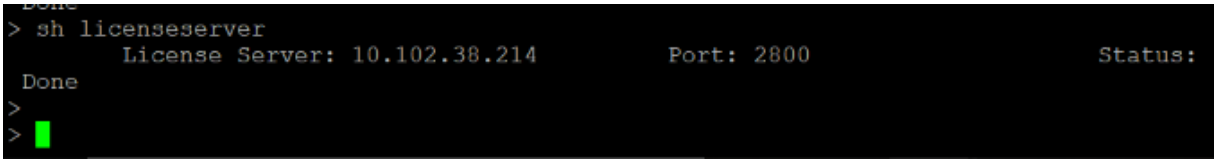
Dans l'exemple suivant, après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition Premium au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences (10.102.38.214).



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
```

Comme illustré dans l'illustration suivante, vous pouvez exécuter la commande « show license server » et vérifier que le serveur de licences (10.102.38.214) est ajouté au VPX.



Bootstrapping

Utilisez la <NS-BOOTSTRAP> balise pour fournir les informations de démarrage personnalisées. Vous pouvez utiliser les <NEW-BOOTSTRAP-SEQUENCE> balises <SKIP-DEFAULT-BOOTSTRAP> et dans la <NS-BOOTSTRAP> section. Cette section indique à l'appliance NetScaler s'il faut éviter ou non le bootstrap par défaut. Si le démarrage par défaut est évité, cette section vous offre la possibilité de fournir une nouvelle séquence de démarrage.

Configuration d'amorçage par défaut

La configuration d'amorçage par défaut de l'appliance NetScaler suit les attributions d'interface suivantes :

- **Eth0** - Interface de gestion avec une certaine adresse NSIP.
- **Eth1** - Interface client avec une certaine adresse VIP.
- **Eth2** - Interface serveur avec une certaine adresse SNIP.

Personnalisation de la configuration de bootstrap

Vous pouvez ignorer la séquence d'amorçage par défaut et fournir une nouvelle séquence d'amorçage pour l'instance NetScaler VPX. Utilisez la <NS-BOOTSTRAP> balise pour fournir les informations de démarrage personnalisées. Par exemple, vous pouvez modifier le démarrage par défaut, où l'interface de gestion (NSIP), l'interface VIP et l'interface orientée serveur (SNIP) sont toujours fournies dans un certain ordre.

Le tableau suivant indique le comportement d'amorçage avec les différentes valeurs autorisées pour <SKIP-DEFAULT-BOOTSTRAP> et les <NEW-BOOTSTRAP-SEQUENCE> balises.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Comportement Bootstrap
OUI	OUI	Le comportement d'amorçage par défaut est ignoré et une nouvelle séquence d'amorçage personnalisée fournie dans la <NS-BOOTSTRAP> section est exécutée.
OUI	NON	Le comportement d'amorçage par défaut est ignoré. Le comportement de démarrage par défaut est ignoré, les commandes d'amorçage fournies dans la <NS-CONFIG> section sont exécutées.

Vous pouvez personnaliser la configuration d'amorçage à l'aide des trois méthodes suivantes :

- Fournissez uniquement les détails de l'interface
- Fournir les détails de l'interface ainsi que les adresses IP et le masque de sous-réseau
- Fournir des commandes liées au bootstrap dans la <NS-CONFIG> section

Méthode 1 : amorçage personnalisé en spécifiant uniquement les détails de l'interface

Vous spécifiez les interfaces de gestion, orientées client et orientées serveur, mais pas leurs adresses IP et masques de sous-réseau. Les adresses IP et les masques de sous-réseau sont renseignés en interrogeant l'infrastructure cloud.

Exemple d'amorçage personnalisé pour AWS

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth2 est assignée en tant qu'interface de gestion (NSIP), Eth1 comme interface client (VIP) et interface Eth0 en tant qu'interface serveur (SNIP). La <NS-BOOTSTRAP> section contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

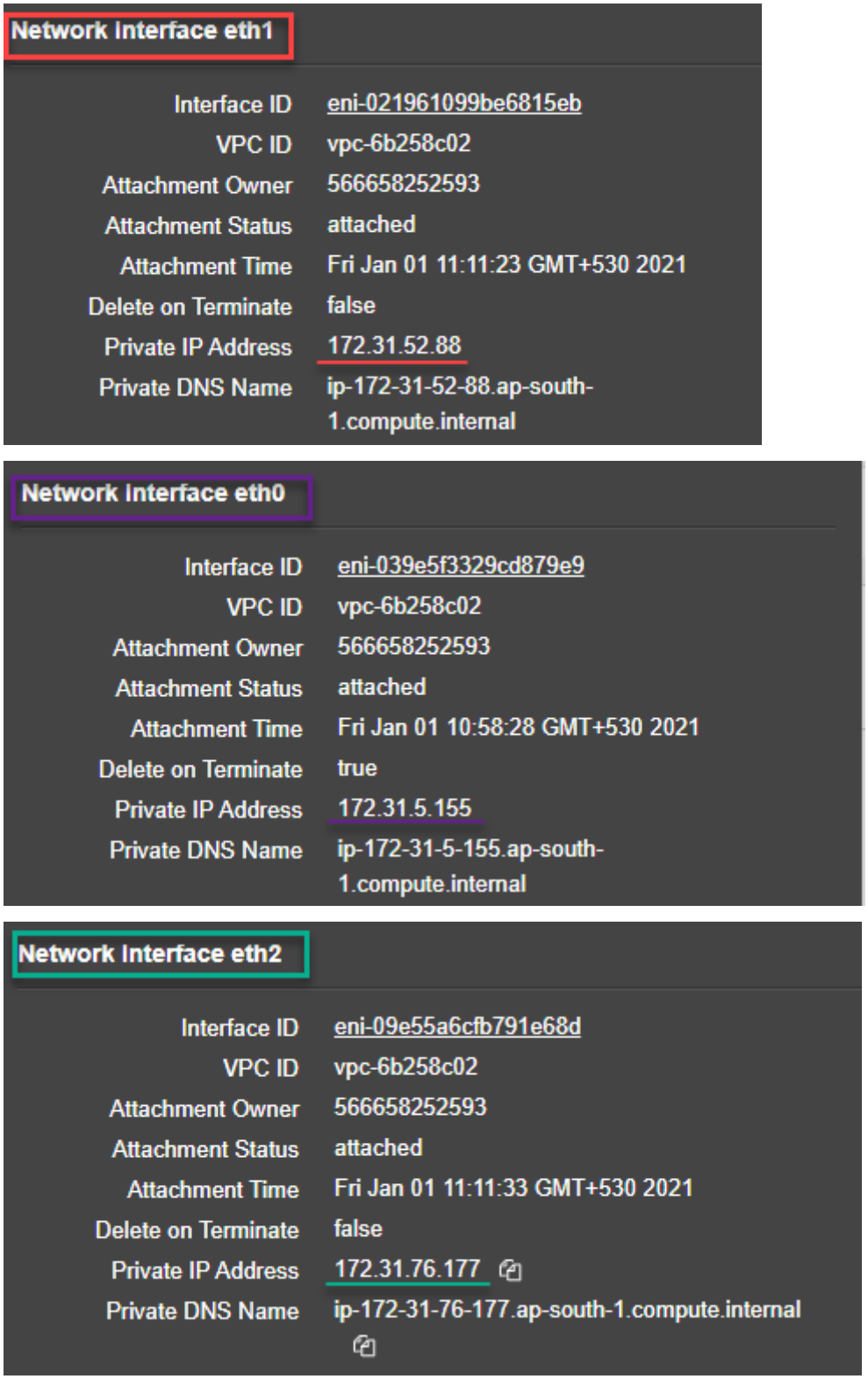
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

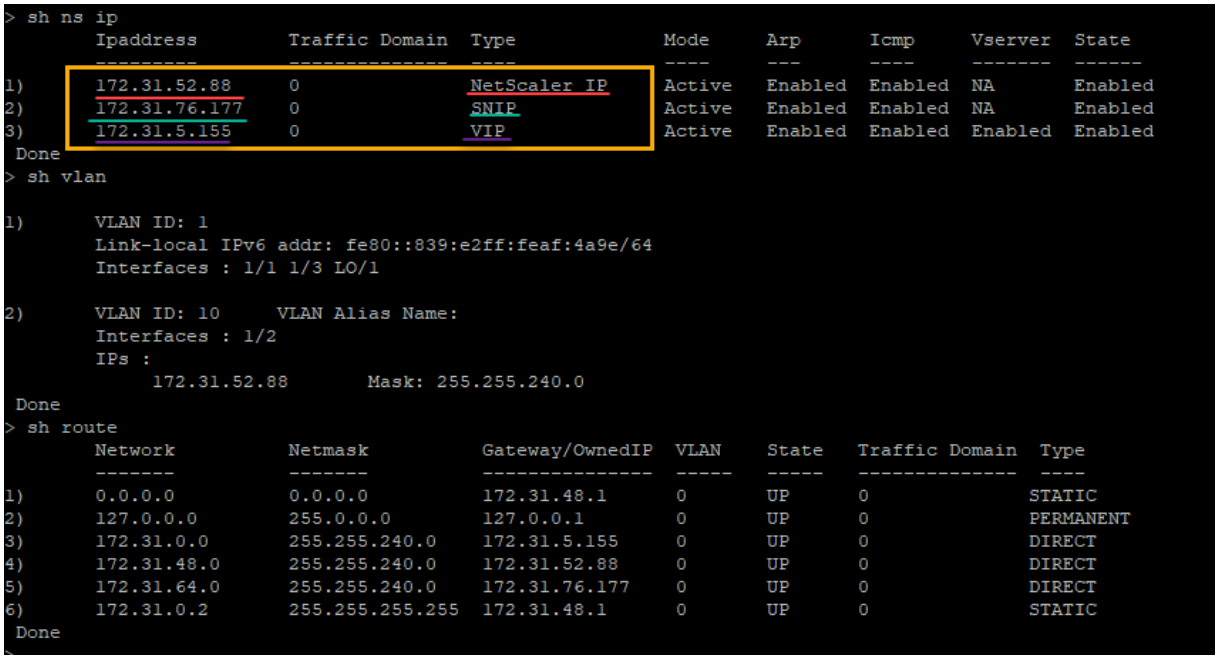
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.



Exemple de bootstrap personnalisé pour Azure

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth1 est assignée en tant qu'interface de gestion (NSIP), Eth0 comme interface client (VIP) et interface Eth2 en tant qu'interface serveur (SNIP). La <NS-BOOTSTRAP> section contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

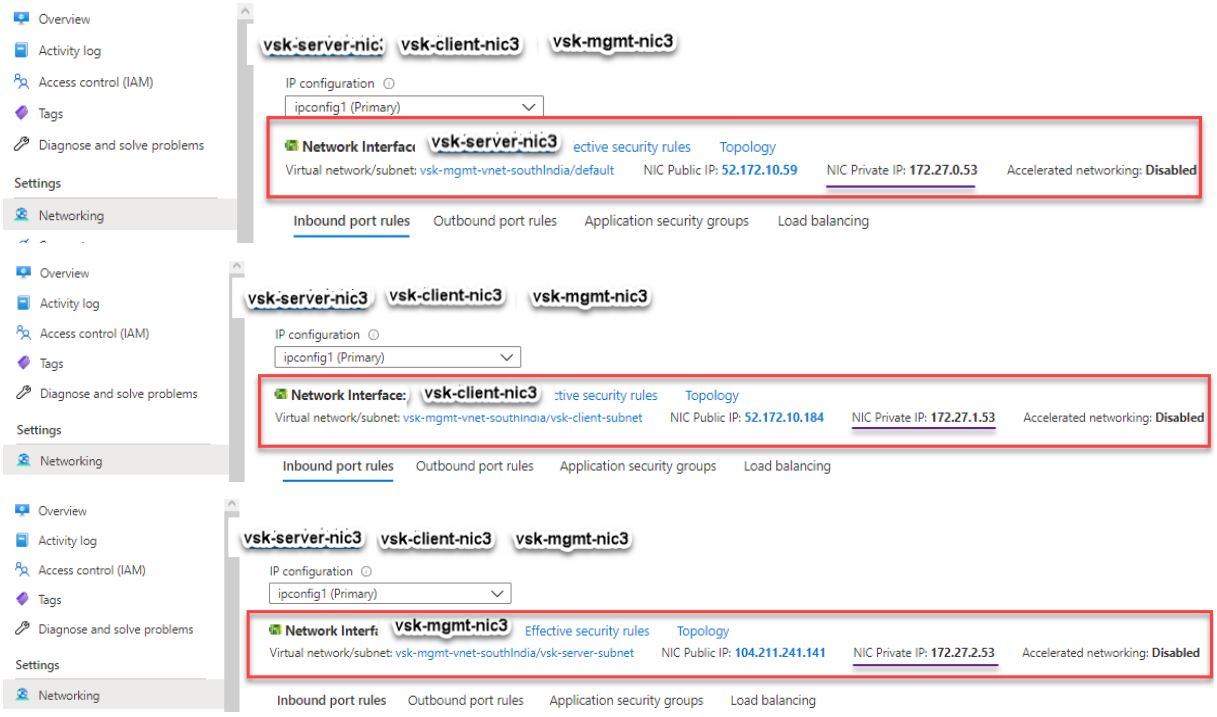
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

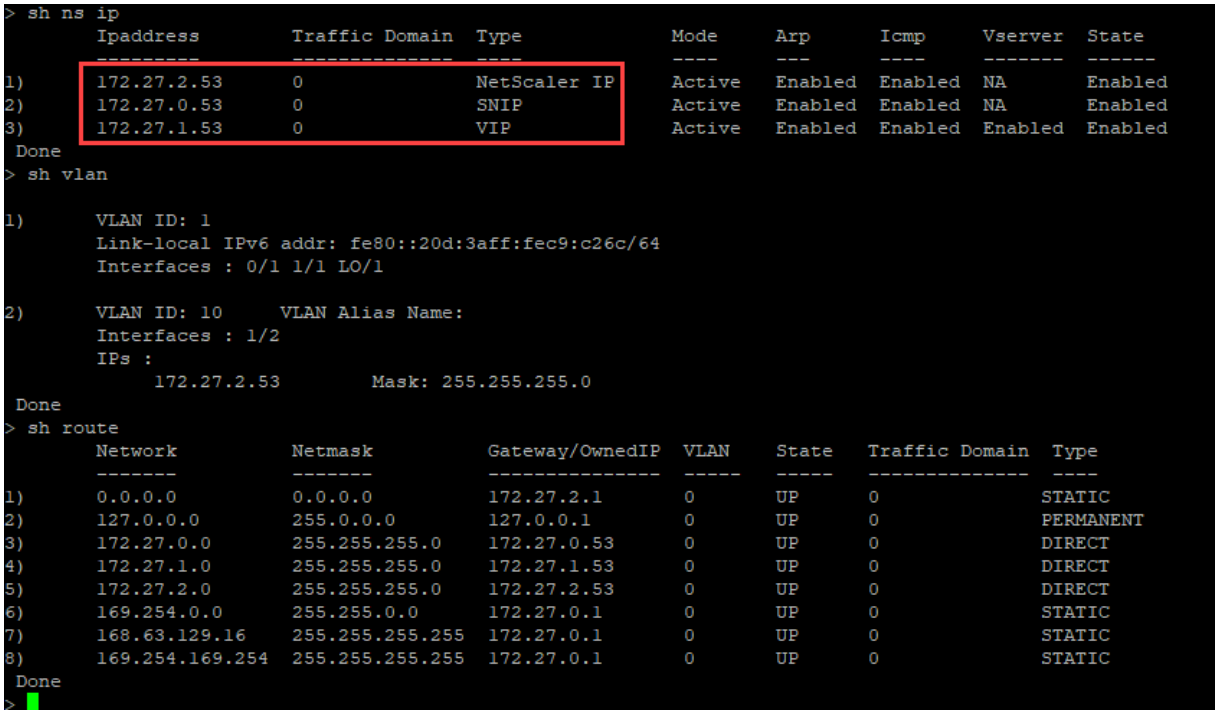
</NS-PRE-BOOT-CONFIG>
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande « show nsip » dans l'ADC CLI et vérifier que la nouvelle séquence d'

amorçage spécifiée dans la <NS-BOOTSTRAP> section est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



Exemples de bootstrap personnalisés pour GCP

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth2 est assignée en tant qu'interface de gestion (NSIP), Eth1 comme interface client (VIP) et interface Eth0 en tant qu'interface serveur (SNIP). La <NS-BOOTSTRAP> section contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée dans le portail GCP, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

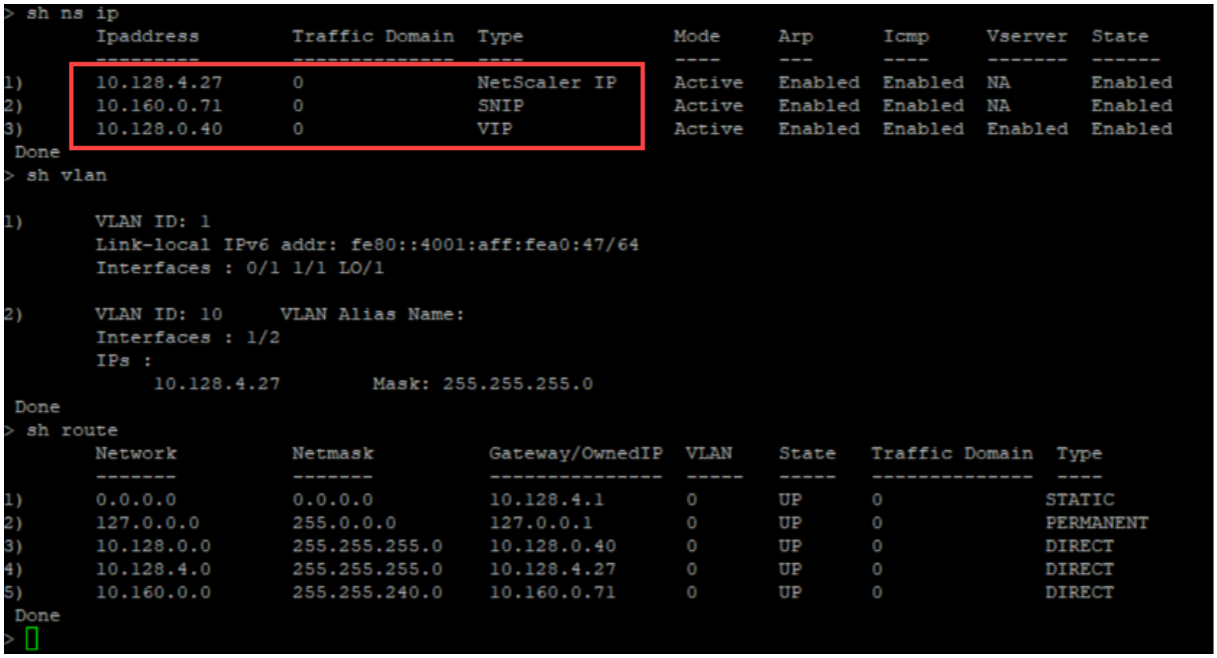
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit :

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.160.0.71	–	35.244.56.180 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	10.128.0.40	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.27	–	34.93.241.147 (ephemeral)	Premium		View details

Public DNS PTR Record
None

Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.



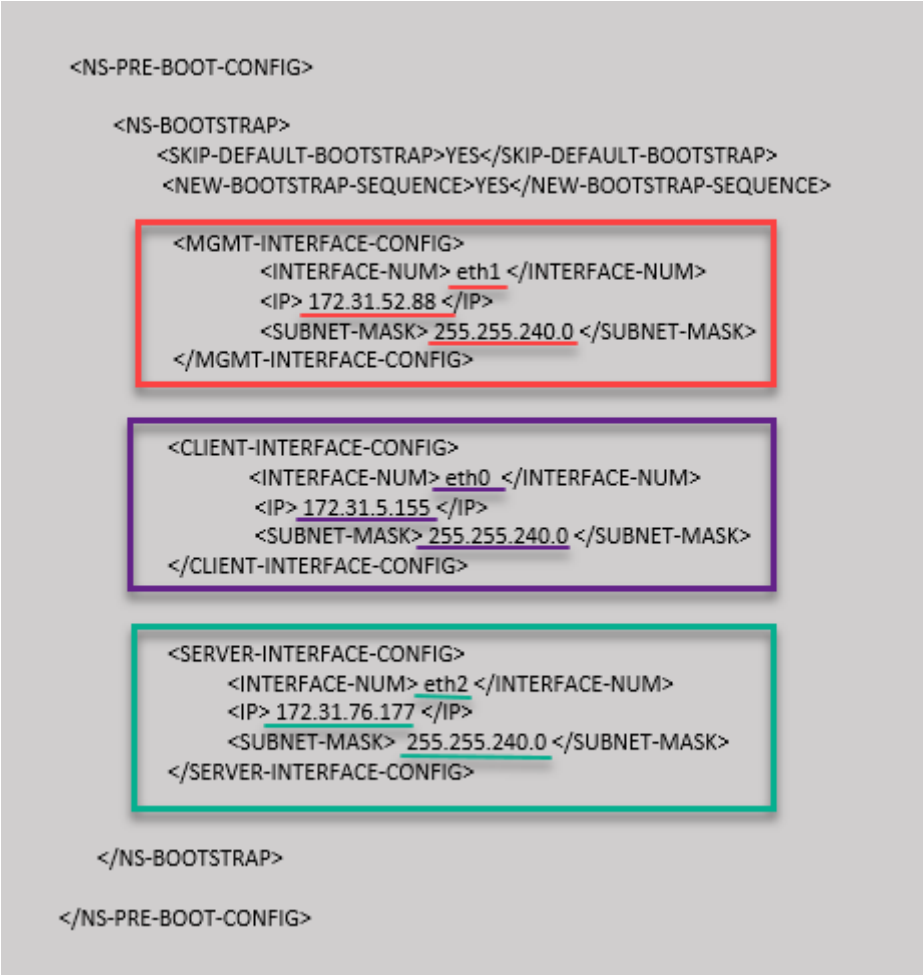
Méthode 2 : amorçage personnalisé en spécifiant les interfaces, adresses IP et masques de sous-réseau

Vous spécifiez les interfaces de gestion, orientées client et serveur, ainsi que leurs adresses IP et leur masque de sous-réseau.

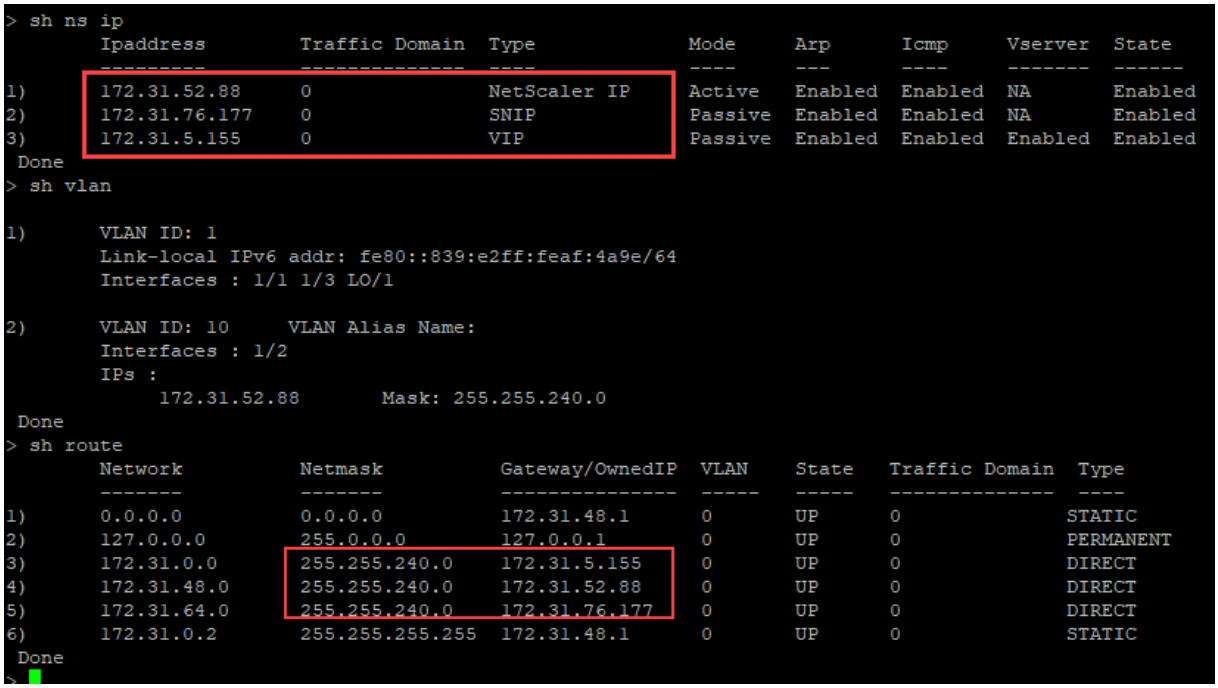
Exemples de bootstrap personnalisés pour AWS

Dans l'exemple suivant, vous ignorez le bootstrap par défaut et exécutez une nouvelle séquence d'amorçage pour l'appliance NetScaler. Pour la nouvelle séquence d'amorçage, vous spécifiez les détails suivants :

- **Interface de gestion :** Interface - Eth1, NSIP - 172.31.52.88 et masque de sous-réseau - 255.255.240.0
- **Interface client :** Interface - Eth0, VIP - 172.31.5.155 et masque de sous-réseau - 255.255.240.0.
- **Interface serveur :** Interface - Eth2, SNIP - 172.31.76.177 et masque de sous-réseau - 255.255.240.0.



Vous pouvez exécuter la `show nsip` commande dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la `<NS-BOOTSTRAP>` section est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



Exemple de bootstrap personnalisé pour Azure

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (172.27.2.53) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (172.27.1.53) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (172.27.0.53) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

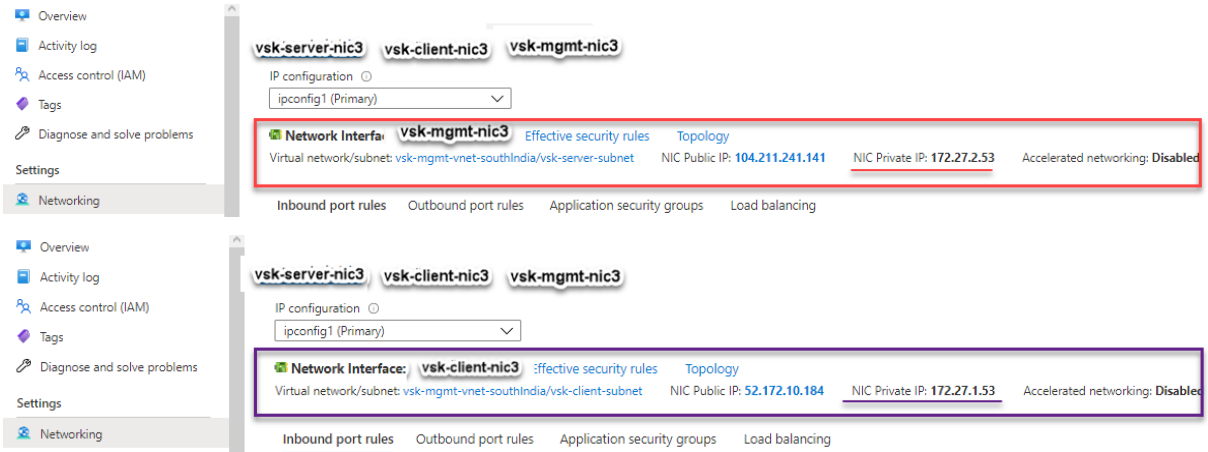
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

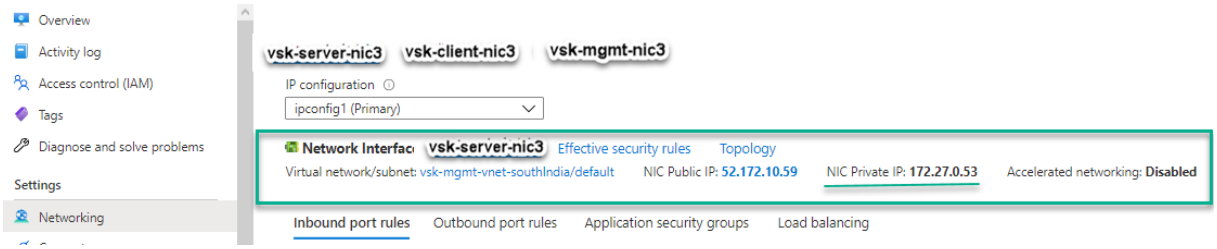
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.





Vous pouvez exécuter la `show nsip` commande dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la `<NS-BOOTSTRAP>` section est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour GCP

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (10.128.4.31) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (10.128.0.43) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (10.160.0.75) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
   <NS-BOOTSTRAP>
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
         <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
          <MGMT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth2 </INTERFACE-NUM>
               <IP> 10.128.4.31 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
           </MGMT-INTERFACE-CONFIG>

          <CLIENT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth1 </INTERFACE-NUM>
               <IP> 10.128.0.43 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </CLIENT-INTERFACE-CONFIG>

          <SERVER-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth0 </INTERFACE-NUM>
               <IP> 10.160.0.75 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </SERVER-INTERFACE-CONFIG>

   </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

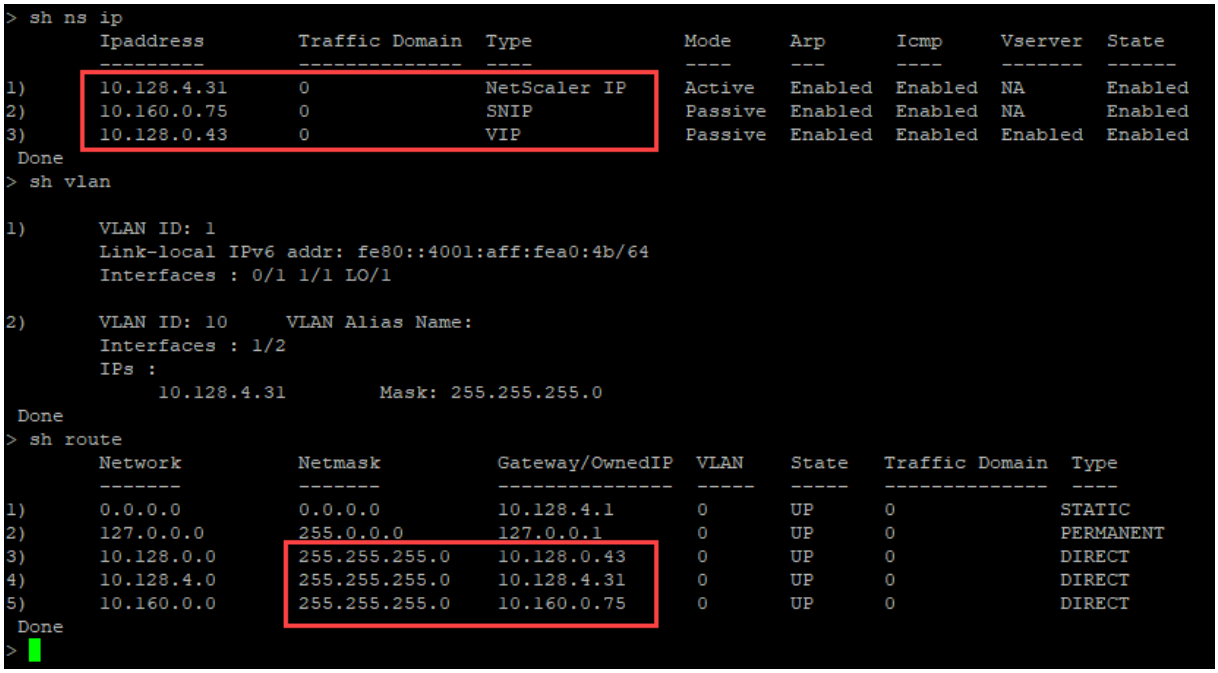
Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Vous pouvez exécuter la `show nsip` commande dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la `<NS-BOOTSTRAP>` section est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



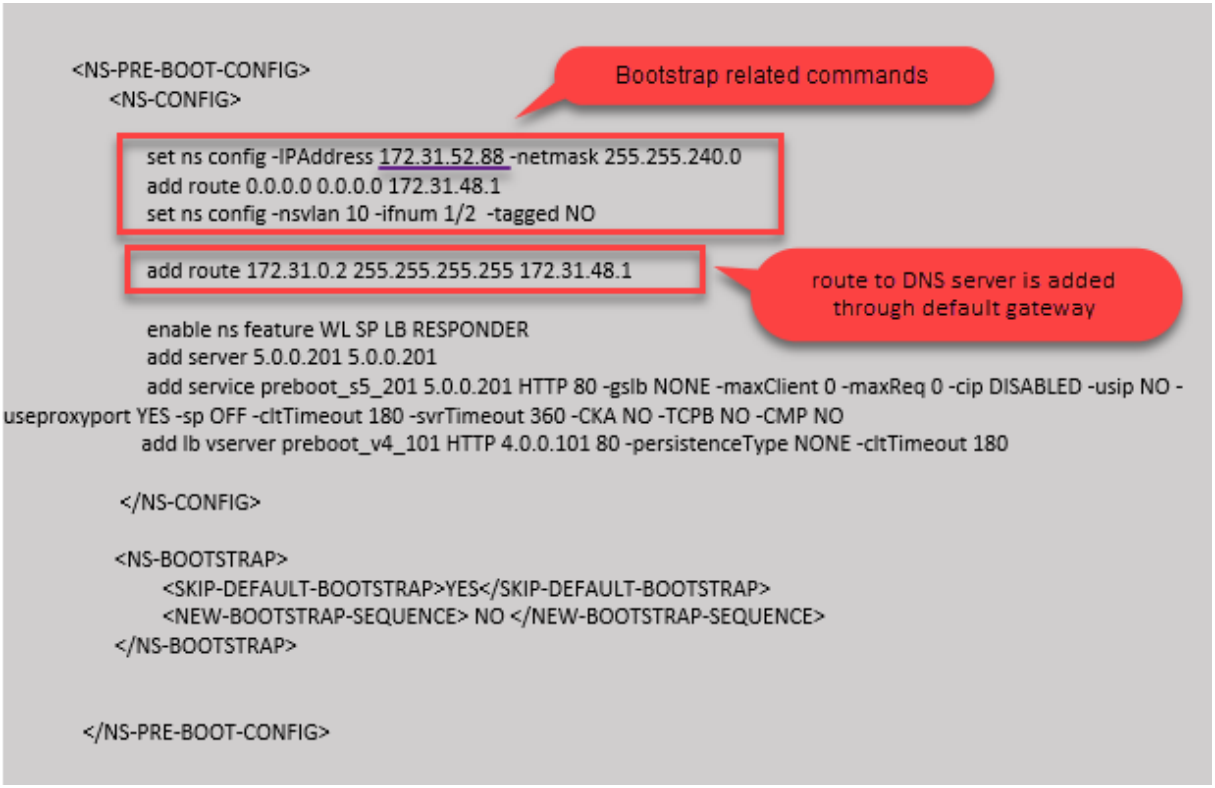
Méthode 3 : Bootstrap personnalisé en fournissant des commandes liées au bootstrap dans la <NS-CONFIG> section

Vous pouvez fournir les commandes associées au bootstrap dans la <NS-CONFIG> section. Dans la <NS-BOOTSTRAP> section, vous devez spécifier « Non » pour exécuter les commandes d'amorçage de la <NS-CONFIG> section. <NEW-BOOTSTRAP-SEQUENCE> Vous devez également fournir les commandes pour attribuer NSIP, routage par défaut et NSVLAN. En outre, fournissez les commandes pertinentes pour le cloud que vous utilisez.

Avant de fournir un bootstrap personnalisé, assurez-vous que votre infrastructure cloud prend en charge une configuration d'interface particulière.

Exemple d'amorçage personnalisé pour AWS

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la <NS-CONFIG> section. La <NS-BOOTSTRAP> section indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la <NS-CONFIG> section sont exécutées. Vous devez également fournir les commandes permettant de créer NSIP, d'ajouter un itinéraire par défaut et d'ajouter un NSVLAN.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
           maxClient 0 -maxReq 0 -cip DISABLED -usip NO -
           useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -
           CKA NO -TCPB NO -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
           persistenceType NONE -cltTimeout 180

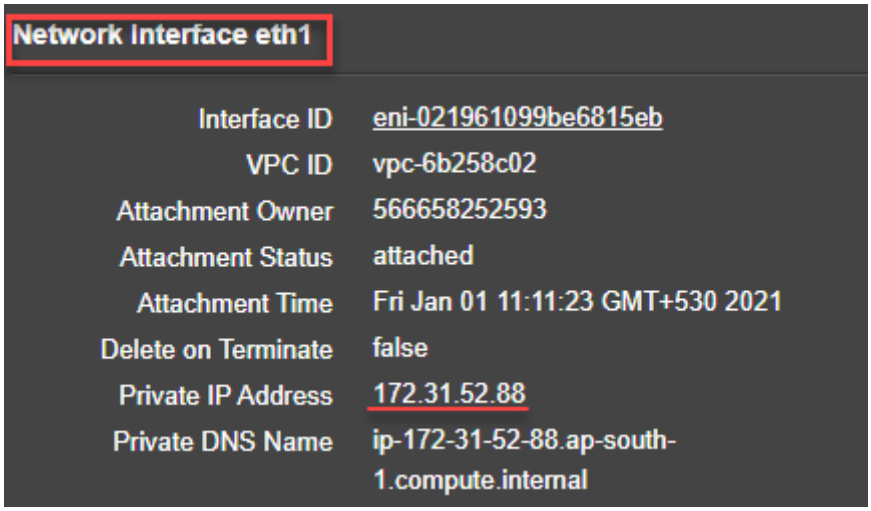
    </NS-CONFIG>

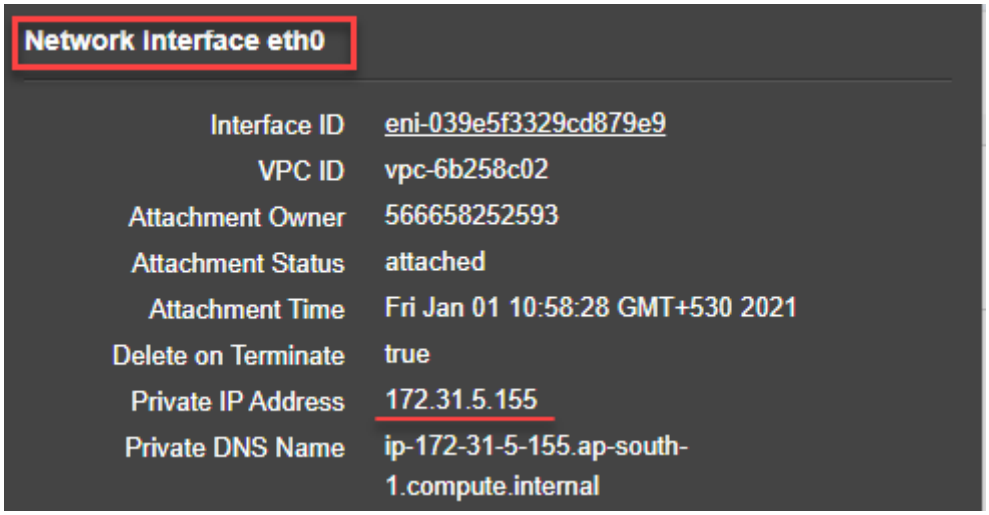
    <NS-BOOTSTRAP>
     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>

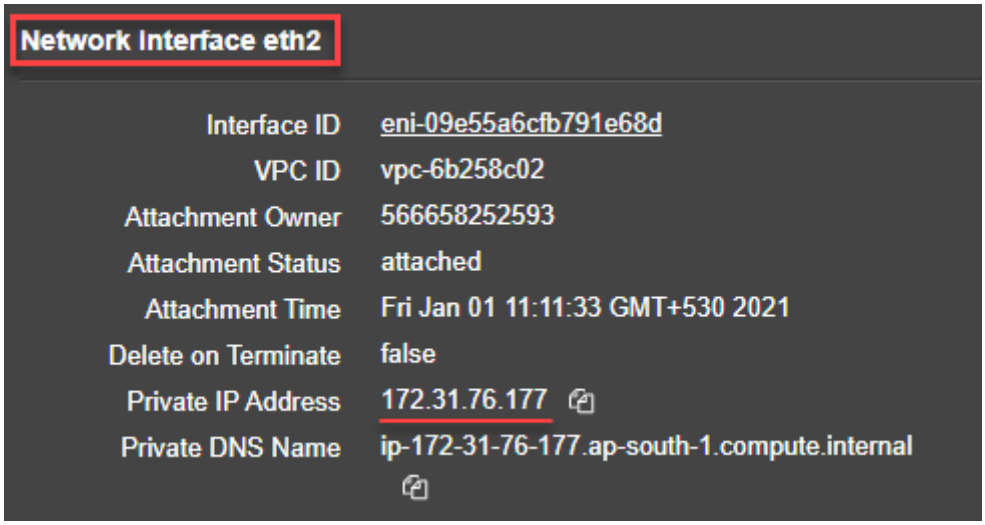

</NS-PRE-BOOT-CONFIG>
```


Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.







Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

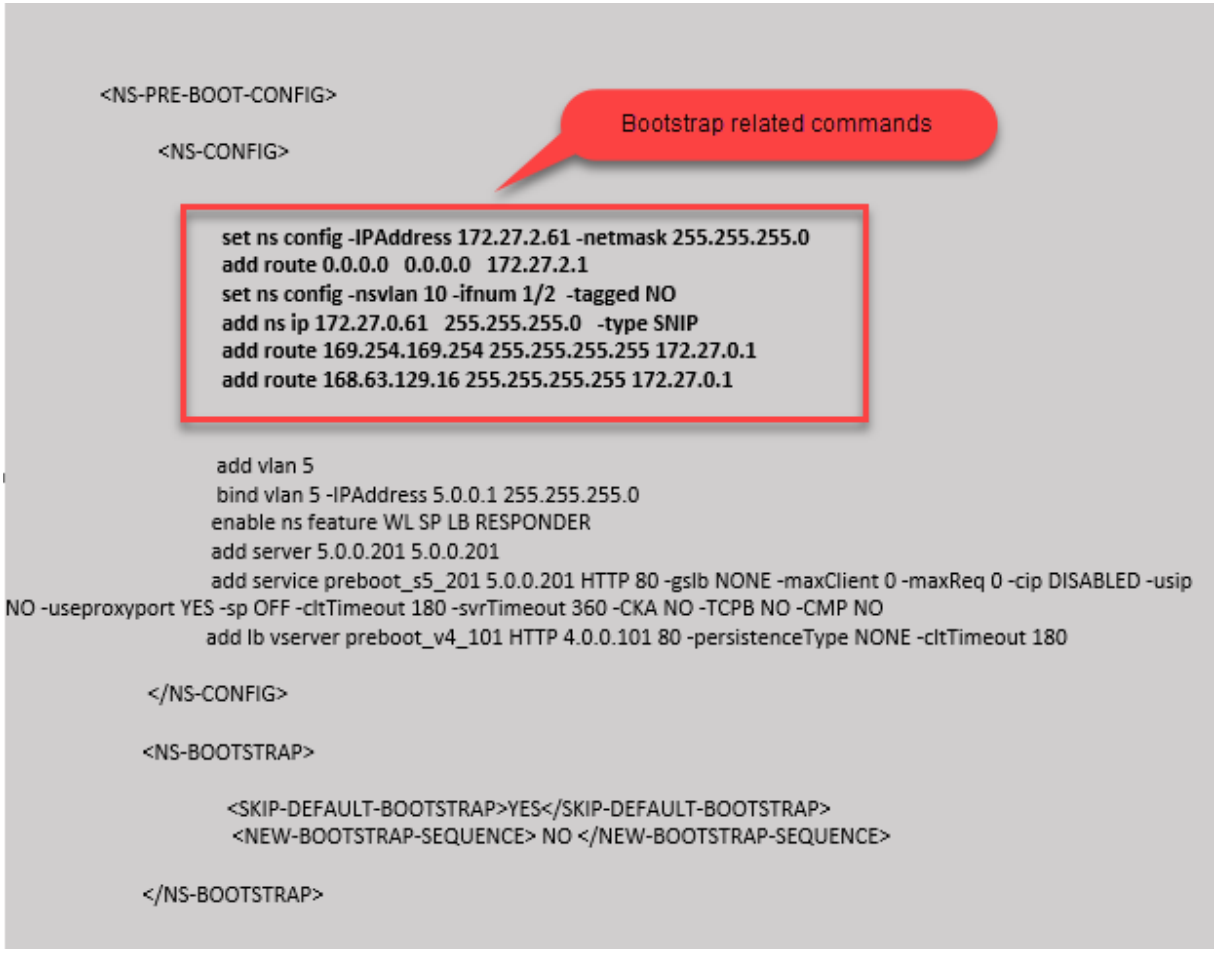
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Exemple de bootstrap personnalisé pour Azure

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la <NS-CONFIG> section. La <NS-BOOTSTRAP> section indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la <NS-CONFIG> section sont exécutées.

> **Remarque :**
>
> Pour le cloud Azure, le serveur de métadonnées d'instance (IMDS) et les serveurs DNS sont accessibles uniquement via l'interface principale (Eth0). Par conséquent, si l'interface Eth0 n'est pas utilisée comme interface de gestion (NSIP), l'interface Eth0 doit au moins être configurée comme SNIP pour l'accès IMDS ou DNS pour fonctionner. La route vers le point de terminaison IMDS (169.254.169.254) et le point de terminaison DNS (168.63.129.16) via la passerelle d'Eth0 doit également être ajoutée.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

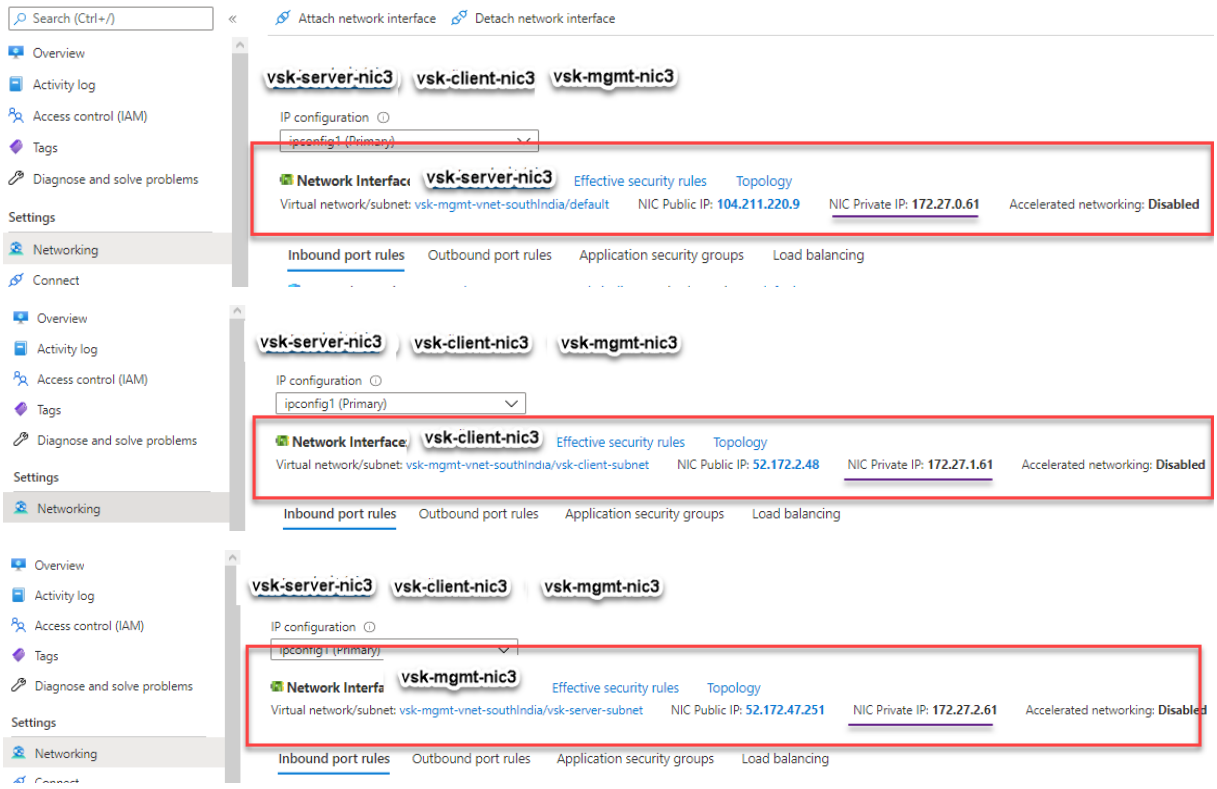
        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

```



```
12            add vlan 5
13            bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
14            enable ns feature WL SP LB RESPONDER
15            add server 5.0.0.201 5.0.0.201
16            add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
                 maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
                  YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
                  NO -CMP NO
17            add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
                 persistenceType NONE -cltTimeout 180
18
19        </NS-CONFIG>
20
21        <NS-BOOTSTRAP>
22
23        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26        </NS-BOOTSTRAP>
27
28    </NS-PRE-BOOT-CONFIG>
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la `show nsip` commande dans l'interface de ligne de commande ADC et

vérifier que la nouvelle séquence d'amorçage spécifiée dans la <NS-BOOTSTRAP> section est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.61      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

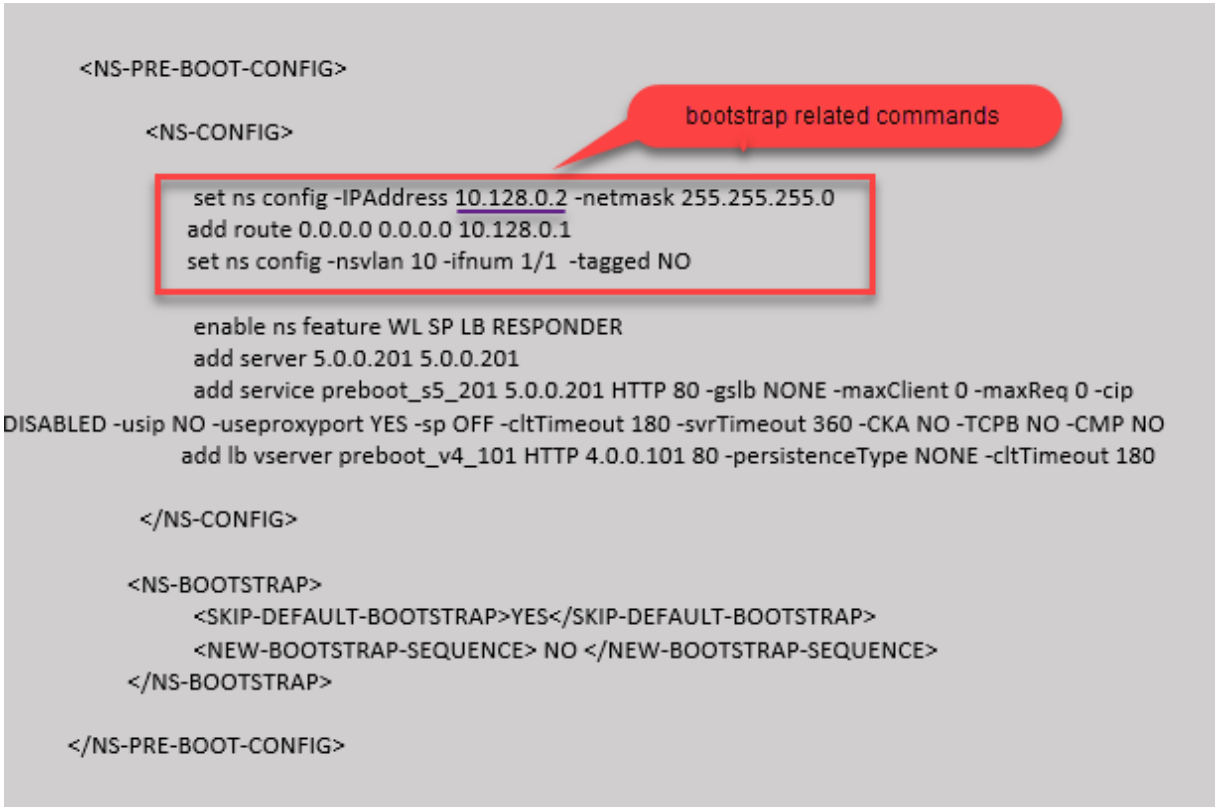
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour GCP

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la <NS-CONFIG> section. La <NS-BOOTSTRAP> section indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la <NS-CONFIG> section sont appliquées.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
             YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
             NO -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

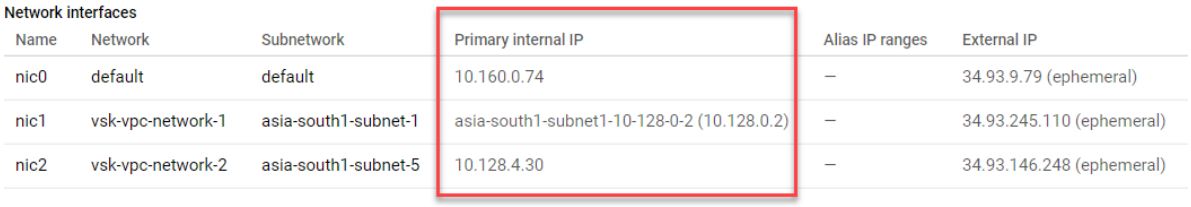
    </NS-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```


Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

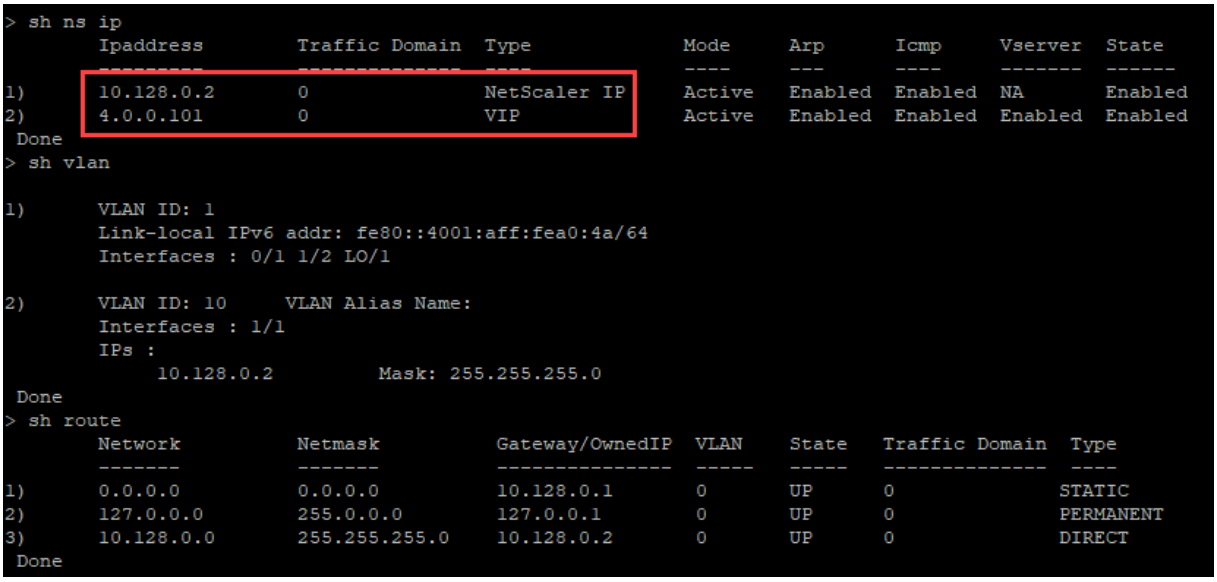
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau, comme indiqué dans l'illustration.



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	—	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	—	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	—	34.93.146.248 (ephemeral)

Vous pouvez exécuter la `show nsip` commande dans **ADC CLI**et vérifier que les configurations fournies dans la `<NS-CONFIG>` section précédente sont appliquées au premier démarrage de l'appliance ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Impact de l'attachement et du détachement de cartes réseau dans AWS et Azure

AWS et Azure permettent d'attacher une interface réseau à une instance et de détacher une interface réseau d'une instance. La fixation ou le détachement d'interfaces peuvent modifier la position de l'interface. Citrix vous recommande donc de ne pas détacher les interfaces de l'instance NetScaler VPX. Si vous détachez ou attachez une interface lorsque le bootstrap personnalisé est configuré, l'instance NetScaler VPX réattribue l'adresse IP principale de l'interface nouvellement disponible à la position de l'interface de gestion en tant que NSIP. Si aucune autre interface n'est disponible après celle que vous avez détachée, la première interface devient l'interface de gestion de l'instance NetScaler VPX.

Par exemple, une instance NetScaler VPX est proposée avec 3 interfaces : Eth0 (SNIP), Eth1 (NSIP) et Eth2 (VIP). Si vous détachez l'interface Eth1 de l'instance, qui est une interface de gestion, ADC configure la prochaine interface disponible (Eth2) comme interface de gestion. Ainsi, l'instance NetScaler VPX est toujours accessible via l'adresse IP principale de l'interface Eth2. Si Eth2 n'est pas non plus disponible, l'interface restante (Eth0) devient l'interface de gestion. Par conséquent, l'accès à l'instance NetScaler VPX continue d'exister.

Considérons une attribution différente des interfaces comme suit : Eth0 (SNIP), Eth1 (VIP) et Eth2 (NSIP). Si vous détachez Eth2 (NSIP), car aucune nouvelle interface n'est disponible après Eth2, la première interface (Eth0) devient l'interface de gestion.

Améliorez les performances SSL-TPS sur les plateformes de cloud public

October 17, 2024

Vous pouvez obtenir de meilleures performances SSL-TPS sur les nuages AWS et GCP en répartissant les poids du moteur de paquets (PE) de manière égale. L'activation de cette fonctionnalité peut entraîner une légère baisse du débit HTTP d'environ 10 à 12 %.

Sur les clouds AWS et GCP, les instances NetScaler VPX dotées de 10 à 16 processeurs virtuels ne présentent aucune amélioration des performances car les poids des PE sont répartis de manière égale par défaut.

> **Remarque :**
>
> Dans le cloud Azure, les poids PE sont également distribués par défaut. Cette fonctionnalité n'améliore aucune performance pour les instances Azure.

Configurer le mode PE à l'aide de l'interface de ligne de commande NetScaler

Après avoir défini le mode PE, vous devez redémarrer le système pour que les modifications de configuration prennent effet.

À l'invite de commande, tapez :

```
1   set cpuparam pemode [CPUBOUND | Default]
```

Lorsque le mode PE est réglé sur CPUBOUND, les poids PE sont également répartis. Lorsque le mode PE est défini sur DEFAULT, les pondérations PE sont définies sur les valeurs par défaut.

> **Remarque :**
>
> Cette commande est spécifique au nœud. Dans une configuration de haute disponibilité ou de

> cluster, vous devez exécuter la commande sur chaque nœud. Si vous exécutez la commande sur CLIP, l'erreur suivante se produit : `Opération non autorisée sur CLIP`

Pour afficher l'état du mode PE configuré, exécutez la commande suivante :

```
1   show cpuparam
```

Exemple

```
1   > show cpuparam
2       Pemode:  CPUBOUND
3    Done
```

Appliquer la configuration du mode PE au premier démarrage de l'appliance NetScaler dans le cloud

Pour appliquer la configuration du mode PE lors du premier démarrage de l'appliance NetScaler dans le cloud, vous devez créer un `/nsconfig/.cpubound.conf` fichier à l'aide du script personnalisé. Pour plus d'informations, consultez Appliquer les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler dans le cloud.

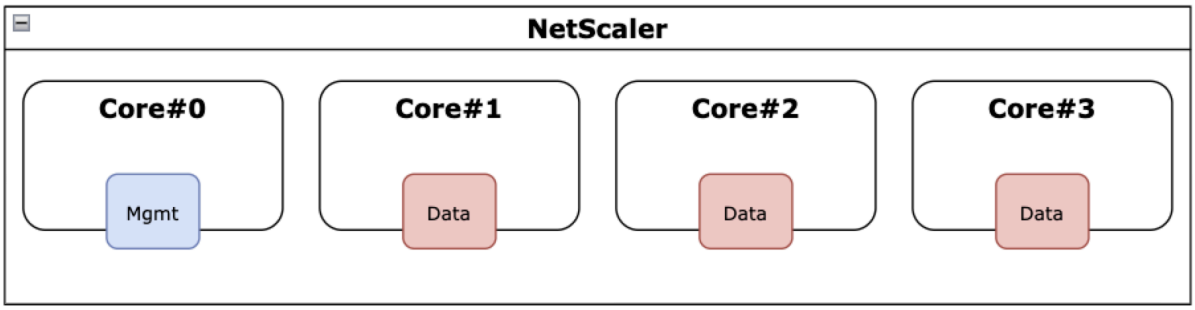
Configurer le multithreading simultané pour NetScaler VPX sur les clouds publics

October 17, 2024

NetScaler utilise différents cœurs dédiés pour ses fonctions de gestion et de plan de données. Un cœur est généralement affecté aux fonctions du plan de gestion. Les autres cœurs disponibles sont affectés aux fonctions du plan de données.

L'image suivante montre une illustration simplifiée d'un NetScaler VPX à 4 cœurs.

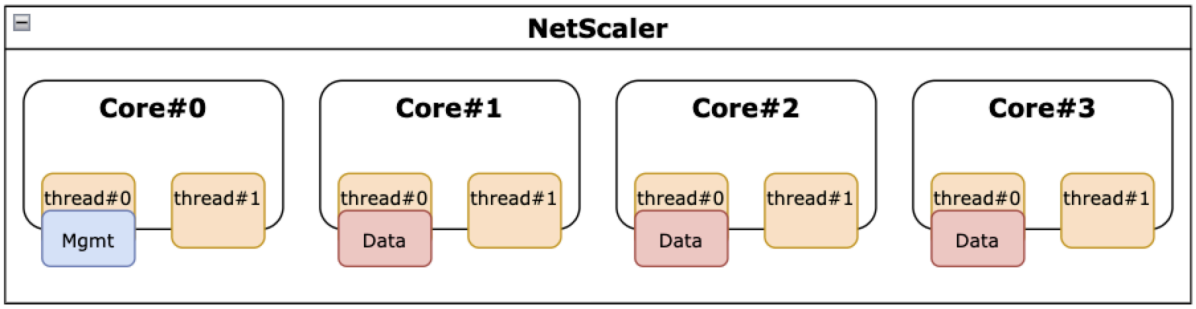
Figure 1. Gestion NetScaler et charge de travail du plan de données sur un système à 4 cœurs



Bien que l'image précédente montre la distribution des fonctions NetScaler sur les cœurs disponibles, il ne s'agit pas nécessairement d'une représentation précise du matériel sous-jacent. La plupart des processeurs x86 modernes fournissent deux cœurs logiques par cœur physique, grâce à des fonctionnalités commercialement connues sous le nom d'Intel Hyperthreading (HT) ou de multithreading simultané (SMT) d'AMD.

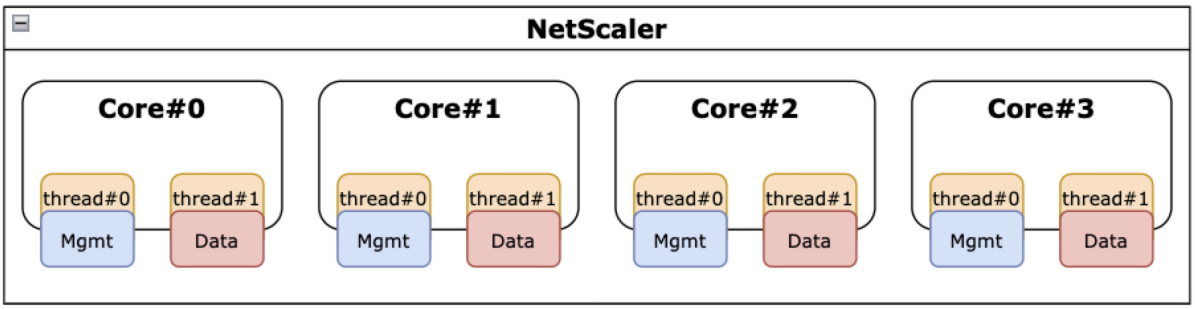
L'image suivante montre NetScaler VPX s'exécutant sur un processeur moderne avec SMT désactivé. Chaque cœur de processeur est divisé en deux ou plusieurs processeurs logiques, communément appelés threads. Chaque thread possède son propre ensemble de ressources répliquées, une partie des ressources partitionnées, et est en concurrence avec ses fils frères pour les ressources partagées.

Figure 2. Gestion NetScaler et charge de travail du plan de données sur un système à 4 cœurs/8 threads avec SMT désactivé



L'image suivante montre NetScaler VPX s'exécutant sur un processeur moderne avec SMT activé.

Figure 3. Gestion NetScaler et charge de travail du plan de données sur un système à 4 cœurs avec SMT activé



L'activation de SMT améliore les performances de NetScaler en :

- Exécution des fonctions du plan de données sur tous les cœurs physiques.
- Déplacer les fonctions du plan de gestion vers le thread frère.
- Introduction d'un mécanisme flexible de limitation des ressources pour empêcher les fonctions du plan de gestion de compromettre les performances des fonctions du plan de données.

Matrice de support SMT

Les plates-formes VPX, les types d'instances cloud et les versions de NetScaler qui prennent en charge le SMT sont répertoriés dans le tableau suivant.

Plateforme VPX	Types d'instances	Version de NetScaler VPX
———————	———————————————————————-	———————————————
AWS	M5, m5n, c5, c5n	14.1-12.x et versions ultérieures
Azure	Toute famille d'instances avec hyperthreading, par exemple DS_v4	14.1-12.x et versions ultérieures
GCP	instances e2	14.1-12.x et versions ultérieures

> **Remarque :**
>
> En activant la fonctionnalité SMT, les performances de NetScaler VPX sont améliorées sur les types pris en charge.

Limitations

La fonctionnalité SMT double efficacement le nombre de vCPU disponibles pour une appliance NetScaler. Les limites de licence doivent être prises en compte pour permettre à l'appliance NetScaler de les utiliser.

Prenons l'exemple de NetScaler VPX illustré à la Figure 3. Si une licence basée sur le débit est utilisée, une licence de 10 Gbit/s ou plus est requise avec la fonction SMT pour activer 8 vCPU. Auparavant, une licence de 1 Gbit/s était suffisante pour activer 4 vCPU. Si une licence vCPU est utilisée, NetScaler VPX doit être configuré pour extraire des licences correspondant au double du nombre de vCPU pour un fonctionnement correct. Contactez le support technique de NetScaler pour obtenir de plus amples informations à ce sujet.

Configurer SMT

Avant d'activer la fonctionnalité SMT, assurez-vous que votre plateforme prend en charge cette fonctionnalité. Consultez le tableau des matrices de support dans la section précédente.

Pour activer la fonction SMT, procédez comme suit :

1. Créez un fichier vide nommé `.smt_handling` dans le répertoire « /nsconfig ».
2. Enregistrez la configuration actuelle.
3. Redémarrez l'instance NetScaler VPX.

```
nscli> shell touch /nsconfig/.smt_handling
  Done
```



```
3   nscli> reboot
4   Are you sure you want to restart NetScaler (Y/N)?   [N]:Y
5   Done
```

4. Après le redémarrage, NetScaler indique que la fonctionnalité est à la fois disponible et activée.

```
1   smt_handling and smt_handling_active are set to " 1 "
2
3   > shell sysctl -a | grep smt_handling
4   netscaler.smt_handling_platform: 1
5   netscaler.smt_handling: 1
6   netscaler.smt_handling_active: 1
```

Pour désactiver la fonction SMT, procédez comme suit :

1. Supprimez le fichier `.smt_handling`.
2. Redémarrez l'instance NetScaler VPX.

```
1   shell rm -f /nsconfig/.smt_handling
2     Done
3
4   reboot
5
6   Are you sure you want to restart NetScaler (Y/N)?   [N]:Y
7   Done
```

3. Après le redémarrage, NetScaler indique que la fonctionnalité est disponible mais désactivée.

```
1   > shell sysctl -a | grep smt_handling
2   netscaler.smt_handling_platform: 1
3   netscaler.smt_handling: 0
4   netscaler.smt_handling_active: 0
```

Dépannage

Exécutez la commande shell `sysctl` pour vérifier l'état de la fonctionnalité SMT.

```
1   ```
2     > shell sysctl -a | grep smt_handling
3     >
4   ```
```

La commande peut renvoyer n'importe laquelle des sorties suivantes.

- La fonction SMT est absente.

  La commande `sysctl` ne renvoie aucune sortie.

- La fonction SMT n'est pas prise en charge.

  La fonctionnalité SMT n'est pas prise en charge pour l'une des raisons suivantes :

- Votre NetScaler VPX est antérieur à 13.1-48.x ou 14.1-12.x.
- Votre cloud ne prend pas en charge le SMT.
- Le type d'instance de votre machine virtuelle ne prend pas en charge le SMT. Par exemple, le nombre de processeurs virtuels est supérieur à 8.

```
> shell sysctl -a | grep smt_handling
netscaler.smt_handling_platform: 0(indicates not supported)
netscaler.smt_handling: 0 (indicates not enabled)
netscaler.smt_handling_active: 0 (indicates not active)
```

- La fonctionnalité SMT est prise en charge mais elle n'est pas activée.

```
> shell sysctl -a | grep smt_handling
netscaler.smt_handling_platform: 1 (available)
netscaler.smt_handling: 0          (not enabled)
netscaler.smt_handling_active: 0   (not active)
```

Installation d'une instance NetScaler VPX sur un serveur bare metal

October 17, 2024

Un bare metal est un serveur physique entièrement dédié qui offre une isolation physique, entièrement intégré dans l'environnement cloud. Il est également connu sous le nom de serveur à locataire unique. La location unique vous permet d'éviter l'effet de voisin bruyant. Avec le métal nu, vous n'êtes pas témoin de l'effet voisin bruyant parce que vous êtes le seul utilisateur.

Un serveur nu installé avec un hyperviseur fournit une suite de gestion pour créer des machines virtuelles sur le serveur. L'hyperviseur n'exécute pas les applications nativement. Son but est de virtualiser vos charges de travail en machines virtuelles distinctes afin d'obtenir la flexibilité et la fiabilité de la virtualisation.

Conditions préalables à l'installation d'une instance NetScaler VPX sur des serveurs bare metal

Un serveur nue doit être obtenu auprès d'un fournisseur de cloud qui répond à toutes les exigences système requises pour l'hyperviseur concerné.

Installation de l'instance NetScaler VPX sur des serveurs bare metal

Pour installer des instances NetScaler VPX sur un serveur bare metal, vous devez d'abord vous procurer un serveur bare metal doté de ressources système adéquates auprès d'un fournisseur de cloud.

Sur ce serveur bare metal, tous les hyperviseurs pris en charge tels que Linux KVM, VMware ESX, Citrix Hypervisor ou Microsoft Hyper-V doivent être installés et configurés avant de déployer l'instance NetScaler VPX.

Pour plus d'informations sur la liste des différents hyperviseurs et fonctionnalités pris en charge sur une instance NetScaler VPX, consultez Matrice de support et directives d'utilisation.

Pour plus d'informations sur l'installation des instances NetScaler VPX sur différents hyperviseurs, consultez la documentation correspondante.

- **Citrix Hypervisor :** Voir Installer une instance NetScaler VPX sur Citrix Hypervisor.
- **VMware ESX :** Voir Installer une instance NetScaler VPX sur VMware ESX.
- **Microsoft Hyper-V :** Voir Installer une instance NetScaler VPX sur un serveur Microsoft Hyper-V.
- **Plateforme Linux KVM :** Voir Installer une instance NetScaler VPX sur la plateforme Linux-KVM.

Installation d'une instance NetScaler VPX sur Citrix Hypervisor

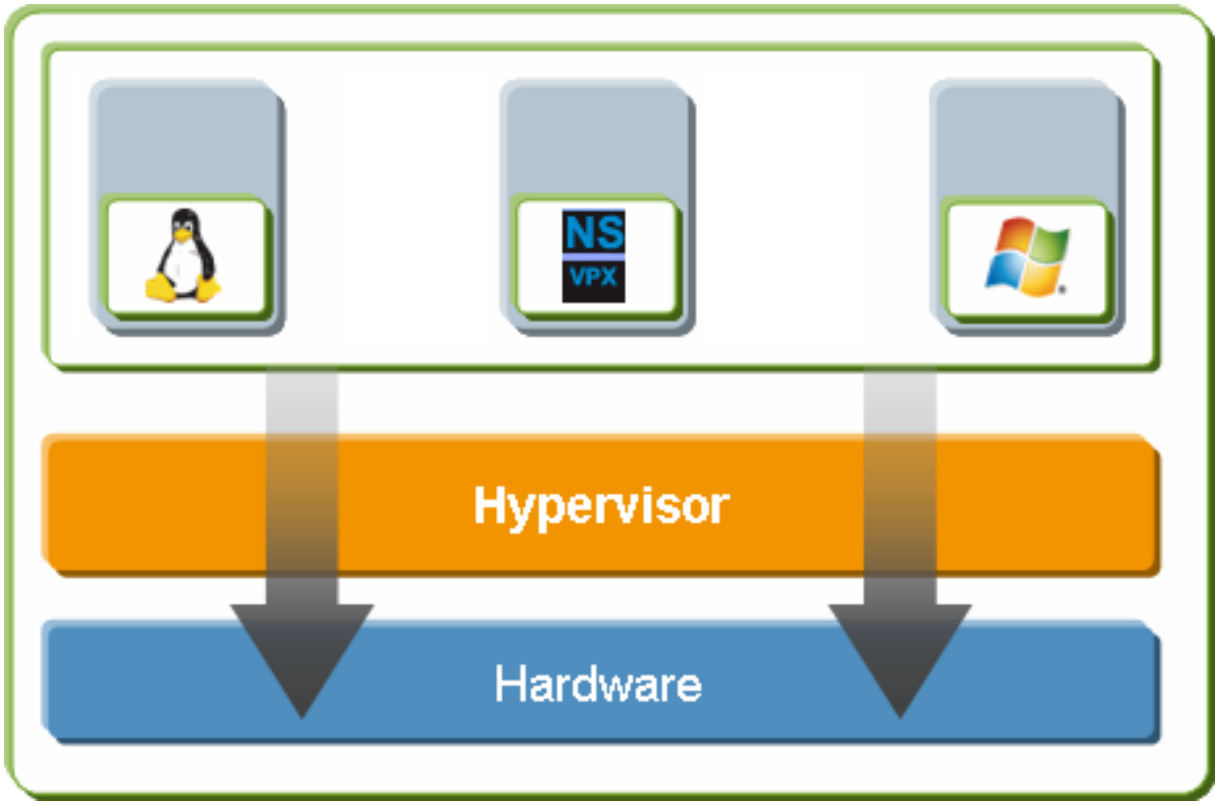
October 17, 2024

Pour installer des instances VPX sur Citrix Hypervisor, vous devez d'abord installer l'hyperviseur sur une machine disposant de ressources système adéquates. Pour effectuer l'installation de l'instance NetScaler VPX, vous utilisez Citrix XenCenter, qui doit être installé sur une machine distante pouvant se connecter à l'hôte Hypervisor via le réseau.

Pour plus d'informations sur Hypervisor, consultez la documentation de Citrix Hypervisor.

La figure suivante montre l'architecture de solution « bare metal » de l'instance NetScaler VPX sur Hypervisor.

Chiffre. Une instance NetScaler VPX sur Citrix Hypervisor



Conditions préalables à l'installation d'une instance NetScaler VPX sur Hypervisor

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez Hypervisor version 6.0 ou ultérieure sur du matériel répondant à la configuration minimale requise.
- Installez XenCenter sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Obtenez les fichiers de licence du dispositif virtuel. Pour plus d'informations sur les licences d'appliance virtuelle, consultez le Guide de licence NetScaler.

Configuration matérielle requise pour l'hyperviseur

Le tableau suivant décrit la configuration matérielle minimale requise pour une plate-forme Hypervisor exécutant une instance NetScaler VPX.

Tableau 2. **Tableau 1** Configuration système minimale requise pour l'hyperviseur exécutant une instance VPX nCore

Composant	Exigences
UC	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter l'instance NetScaler VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte de l'hyperviseur. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus de détails, consultez la documentation du BIOS.
RAM	3 Go
Espace disque	Stockage connecté localement (PATA, SATA, SCSI) avec 40 Go d'espace disque. Remarque : L'installation de l'hyperviseur crée une partition de 4 Go pour le domaine de contrôle de l'hôte de l'hyperviseur. L'espace restant est disponible pour l'instance NetScaler VPX et d'autres machines virtuelles.
Carte d'interface réseau	Une carte réseau 1 Gbit/s ; recommandé : deux cartes réseau 1 Gbit/s

Pour plus d'informations sur l'installation de l'hyperviseur, consultez la documentation sur l'hyperviseur à l'adresse http://support.citrix.com/product/xens/.

Le tableau suivant répertorie les ressources informatiques virtuelles que l'hyperviseur doit fournir pour chaque dispositif virtuel VPX nCore.

Tableau 2. **Tableau 2** Ressources informatiques virtuelles minimales requises pour exécuter une instance nCore VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	2

> **Remarque :**
>
> Pour l'utilisation en production de l'instance NetScaler VPX, Citrix recommande de définir la priorité du processeur (dans les propriétés de la machine virtuelle) au niveau le plus élevé, afin d'améliorer le comportement de planification et la latence du réseau.

Configuration système requise pour XenCenter

XenCenter est une application cliente Windows. Il ne peut pas être exécuté sur la même machine que l'hôte de l'hyperviseur. Pour plus d'informations sur la configuration système minimale requise et l'installation de XenCenter, consultez les documents Hypervisor suivants :

- Configuration système requise
- Installer

Installez les instances NetScaler VPX sur Hypervisor à l'aide de XenCenter

Après avoir installé et configuré Hypervisor et XenCenter, vous pouvez utiliser XenCenter pour installer des dispositifs virtuels sur l'hyperviseur. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute l'hyperviseur.

Pour installer des instances NetScaler VPX sur Hypervisor à l'aide de XenCenter, procédez comme suit :

1. Démarrez **XenCenter** sur votre poste de travail.
2. Dans le menu **Serveur**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un nouveau serveur**, dans la zone de texte du nom d'hôte, tapez l'adresse IP ou le nom DNS de l'hyperviseur auquel vous souhaitez vous connecter.
4. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur, puis cliquez sur **Se connecter**. Le nom de l'hyperviseur apparaît dans le volet de navigation avec un cercle vert, ce qui indique que l'hyperviseur est connecté.
5. Dans le volet de navigation, cliquez sur le nom de l'hyperviseur sur lequel vous souhaitez installer l'instance NetScaler VPX.
6. Dans le menu **VM**, cliquez sur **Importer**.
7. Dans la boîte de dialogue **Importer**, dans le nom du fichier d'importation, accédez à l'emplacement où vous avez enregistré le fichier image de l'instance `.xva` NetScaler VPX. Assurez-vous que l'option VM exportée est sélectionnée, puis cliquez sur **Suivant**.
8. Sélectionnez l'hyperviseur sur lequel vous souhaitez installer le dispositif virtuel, puis cliquez sur **Suivant**.
9. Sélectionnez le référentiel de stockage local dans lequel stocker l'appliance virtuelle, puis cliquez sur **Importer** pour commencer le processus d'importation.
10. Vous pouvez ajouter, modifier ou supprimer les interfaces réseau virtuelles si nécessaire. Lorsque vous avez terminé, cliquez sur **Suivant**.
11. Cliquez sur **Terminer** pour terminer le processus d'importation.

> **Remarque :**
>
> Pour afficher l'état du processus d'importation, cliquez sur l'onglet **Journal**.

12. Si vous souhaitez installer un autre dispositif virtuel, répétez les étapes 5 à 11.

> **Remarque :**
>
> Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, reportez-vous à la section Mise à niveau ou rétrogradation du logiciel système.

Configurer les instances VPX pour utiliser les interfaces réseau de virtualisation des E/S racine unique (SR-IOV)

October 17, 2024

Après avoir installé et configuré une instance NetScaler VPX sur Citrix Hypervisor, vous pouvez configurer l'appliance virtuelle pour utiliser les interfaces réseau SR-IOV.

Les cartes réseau suivantes sont prises en charge :

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G

Limitations

Citrix Hypervisor ne prend pas en charge certaines fonctionnalités des interfaces SR-IOV. Les limitations des cartes réseau Intel 82599, Intel X710 et Intel XL710 sont répertoriées dans les sections suivantes.

Limitations pour la carte réseau Intel 82599

La carte réseau Intel 82599 ne prend pas en charge les fonctionnalités suivantes :

- Commutation de mode L2
- Mise en cluster
- Partitionnement d'administrateur [mode VLAN partagé]
- Haute disponibilité [Actif - Mode actif]

- Cadres Jumbo
- Protocole IPv6 dans un environnement Cluster

Limitations pour les cartes réseau Intel X710 10G et Intel XL710 40G

Les cartes réseau Intel X710 10G et Intel XL710 40G présentent les limitations suivantes :

- Le mode L2 n'est pas pris en charge.
- Le partitionnement administrateur (mode VLAN partagé) n'est pas pris en charge.
- Dans un cluster, les trames Jumbo ne sont pas prises en charge lorsque la carte réseau XL710 est utilisée comme interface de données.
- La liste des interfaces réordonne lorsque les interfaces sont déconnectées et reconnectées.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.
- Pour les cartes réseau Intel X710 10G et Intel XL710 40G, l'interface se présente comme une interface 40/x.
- Seules 16 interfaces Intel X710/XL710 SR-IOV peuvent être prises en charge sur une instance VPX.

> **Remarque :**
>
> Pour que les cartes réseau Intel X710 10G et Intel XL710 40G prennent en charge IPv6, activez le mode de confiance sur les fonctions virtuelles (VF) en tapant la commande suivante sur l'hôte Citrix Hypervisor :
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> **Exemple**
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```

Prérequis pour la carte réseau Intel 82599

Sur l'hôte Citrix Hypervisor, assurez-vous de :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Bloquez la liste du pilote `ixgbevf` en ajoutant l'entrée suivante au fichier **/etc/modprobe.d/blacklist.conf** :

  liste noire ixgbevf
- Activez les fonctions virtuelles (VF) SR-IOV en ajoutant l'entrée suivante au **fichier /etc/modprobe.d/ixgbe** :

  options ixgbe max_vfs =* <number_of_VFs>*

  où ** <number_VFs>représente le nombre de VF SR-IOV que vous souhaitez créer.

- Vérifiez que SR-IOV est activé dans le BIOS.

> **Remarque :**
>
> La version 3.22.3 du pilote IXGBE est recommandée.

Attribuez des vF Intel 82599 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Pour attribuer un vFS Intel 82599 SR-IOV à une instance NetScaler VPX, procédez comme suit :

1. Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour attribuer les vF SR-IOV à l'instance NetScaler VPX :

   xe host-call-plugin plugin=iovirt host-uuid=<*Xen host UUID*> **fn=assign_free_vf args:uuid**=<*NetScaler VM UUID*> **args:ethdev**=<*interface name*> **args:mac=***<Mac addr>*

   Où :

   - <*Xen host UUID*> est l'UUID de l'hôte Citrix Hypervisor.
   - <*NetScaler VM UUID*> est l'UUID de l'instance NetScaler VPX.
   - <*interface name*> est l'interface pour les VF SR-IOV.
   - <*MAC address*> est l'adresse MAC du SR-IOV VF.

   > **Remarque :**
   >
   > Spécifiez l'adresse MAC que vous souhaitez utiliser dans le paramètre Args:Mac=. S'il n'est pas spécifié, le script `iovirt` génère et attribue une adresse MAC de manière aléatoire. De plus, si vous souhaitez utiliser les VF SR-IOV en mode Agrégation de liens, assurez-vous de spécifier l'adresse MAC 00:00:00:00:00:00.

2. Démarrez l'instance NetScaler VPX.

Annulez l'attribution des vF Intel 82599 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Si vous avez attribué une VF SR-IOV incorrecte ou si vous souhaitez modifier une VF SR-IOV attribuée, vous devez annuler l'attribution et réattribuer les VF SR-IOV à l'instance NetScaler VPX.

Pour annuler l'attribution de l'interface réseau SR-IOV attribuée à une instance NetScaler VPX, procédez comme suit :

1. Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour attribuer les vF SR-IOV à l'instance NetScaler VPX et redémarrer l'instance NetScaler VPX :

   xe host-call-plugin plugin=iovirt **host-uuid**=<*Xen_host_UUID*> **fn**=unassign_all **args:uuid**=<*Netscaler_VM_U*

   Où :

   - <*Xen_host_UUID*> - L'UUID de l'hôte Citrix Hypervisor.
   - <*Netscaler_VM_UUID*> : UUID de l'instance NetScaler VPX

2. Démarrez l'instance NetScaler VPX.

Attribuez des vF Intel X710/XL710 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Pour attribuer une VF Intel X710/XL710 SR-IOV à l'instance NetScaler VPX, procédez comme suit :

1. Exécutez la commande suivante sur l'hôte Citrix Hypervisor pour créer un réseau.

```
xe network-create name-label=<network-name>
```

   Exemple

```
xe network-create name-label=SR-IOV-NIC-18 8ee59b73-7319-6998-
   cd69-b9fa3e8d7503
```

2. Déterminez l'identifiant unique universel (UUID) PIF de la carte réseau sur laquelle le réseau SR-IOV doit être configuré.

```
xe pif-list

            uuid ( RO)  : e2874343-f1de-1fa7-8fef-98547c348783
            device ( RO): eth18
currently-attached ( RO): true
              VLAN ( RO): -1
      network-uuid ( RO): f865bd85-44dd-b865-ab65-dcd6ae28c16e
```

3. Configurez le réseau en tant que réseau SR-IOV. La commande suivante renvoie également l'UUID du réseau SR-IOV nouvellement créé :

```
xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<
   physical-pif-uuid>
```

   Exemple

```
xe network-sriov-create network-uuid=8ee59b73-7319-6998-cd69-
   b9fa3e8d7503 pif-uuid=e2874343-f1de-1fa7-8fef-98547
   c3487831629b44f-832a-084e-d67d-5d6d314d5e0f
```


Pour obtenir plus d'informations sur les paramètres réseau SR-IOV, exécutez la commande suivante :

```
[root@citrix-XS82-TOPO ~]# xe network-sriov-param-list uuid=1629b44f-832a-084e-d67d-5d6d314d5e0f

                uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f
       physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783
        logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff
     requires-reboot ( RO): false
remaining-capacity ( RO): 32
```

4. Créez une interface virtuelle (VIF) et attachez-la à la machine virtuelle cible.

```
xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-uuid=8ee59b73-7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-f5ca-18eb-561d-308218a9dd68
3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
```

> **Remarque :**
>
> Le numéro d'index de la carte réseau de la machine virtuelle doit commencer par 0.

Utilisez la commande suivante pour rechercher l'UUID de la machine virtuelle :

```
[root@citrix-XS82-TOPO ~]# xe vm-list
uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68
 name-label ( RW): sai-vpx-1
power-state ( RO): halted
```

Supprimez les vF Intel X710/XL710 SR-IOV de l'instance NetScaler à l'aide de l'hôte Citrix Hypervisor

Pour supprimer un processeur Intel X710/XL710 SR-IOV VF d'une instance NetScaler VPX, procédez comme suit :

1. Copiez l'UUID du VIF que vous souhaitez détruire.
2. Exécutez la commande suivante sur l'hôte Citrix Hypervisor pour détruire le VIF.

```
xe vif-destroy uuid=<vif-uuid>
```

Exemple

```
[root@citrix-XS82-TOPO ~]# xe vif-destroy uuid=3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
```


Configuration de l'agrégation de liens sur l'interface SR-IOV

Pour utiliser les fonctions virtuelles (VF) du SR-IOV en mode d'agrégation de liens, vous devez désactiver la vérification des usurpations pour les fonctions virtuelles que vous avez créées.

Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour désactiver la vérification des usurpations :

ip link set <*interface_name*> **vf** <*VF_id*> **spoofchk** off

Où :

- <interface_name> est le nom de l'interface.
- <VF_id> est l'ID de la fonction virtuelle.

Après avoir désactivé la vérification des usurpations pour toutes les fonctions virtuelles que vous avez créées, redémarrez l'instance NetScaler VPX et configurez l'agrégation de liens. Pour obtenir des instructions, voir Configurer l'agrégation de liens.

> **Important :**
>
> Lorsque vous attribuez les VF SR-IOV à l'instance NetScaler VPX, assurez-vous de spécifier l'adresse MAC 00:00:00:00:00:00 pour les VF.

Configurer VLAN sur l'interface SR-IOV

Vous pouvez configurer le VLAN sur les fonctions virtuelles du SR-IOV. Pour obtenir des instructions, consultez la section Configuration d'un VLAN.

> **Important :**
>
> Assurez-vous que l'hôte Citrix Hypervisor ne contient pas de paramètres VLAN pour l'interface VF.

Installation d'une instance NetScaler VPX sur VMware ESX

October 17, 2024

Avant d'installer des instances NetScaler VPX sur VMware ESX, assurez-vous que VMware ESX Server est installé sur une machine disposant de ressources système adéquates. Pour installer une instance NetScaler VPX sur VMware ESXi, vous utilisez le client VMware vSphere. Le client ou l'outil doit être installé sur une machine distante pouvant se connecter à VMware ESX via le réseau.

Cette section comprend les rubriques suivantes :

- Conditions préalables
- Installation d'une instance NetScaler VPX sur VMware ESX

> **Important :**
>
> Vous ne pouvez pas installer VMware Tools standard ni mettre à niveau la version de VMware Tools disponible sur une instance NetScaler VPX. Les outils VMware pour une instance NetScaler VPX sont fournis dans le cadre de la version logicielle NetScaler.

Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez VMware ESX sur du matériel qui répond à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez un commutateur virtuel et connectez la carte réseau physique au commutateur virtuel.
- Ajoutez un groupe de ports et connectez-le au commutateur virtuel.
- Attachez le groupe de ports à la machine virtuelle.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez la section Vue d'ensemble des licences.

Configuration matérielle requise pour VMware ESX

Le tableau suivant décrit la configuration système minimale requise pour les serveurs VMware ESX exécutant l'appliance virtuelle NetScaler VPX nCore.

Tableau 1. Configuration système minimale requise pour un serveur VMware ESX exécutant une instance NetScaler VPX

Composant	Exigences
UC	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter une instance NetScaler VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte VMware ESX. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus d'informations, consultez la documentation de votre BIOS. À partir de la version 13.1 de NetScaler, l'instance NetScaler VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD.
RAM	2 Go VPX. Pour les déploiements critiques, nous ne recommandons pas 2 Go de RAM pour VPX car le système fonctionne dans un environnement où la mémoire est limitée. Cela peut entraîner des problèmes liés à l'échelle, aux performances ou à la stabilité. 4 Go de RAM ou 8 Go de RAM sont recommandés.
Espace disque	20 Go de plus que la configuration serveur minimale requise par VMware pour configurer ESXi. Consultez la documentation VMware pour connaître la configuration minimale requise pour les serveurs.
Réseau	Une carte réseau (NIC) 1 Gbit/s ; deux cartes réseau 1 Gbit/s recommandées

Pour plus d'informations sur l'installation de VMware ESX, reportez-vous à la section http://www.vmware.com/.

Pour l'interface réseau SR-IOV ou la prise en charge du relais PCI, assurez-vous que les processeurs et paramètres suivants sont activés :

- Processeurs Intel compatibles avec Intel-VT
- Processeurs AMD compatibles avec AMD-V
- L'unité de gestion de la mémoire I/O (IOMMU) ou SR-IOV est activée dans le BIOS

Les cartes réseau suivantes sont prises en charge en mode SR-IOV :

- Carte réseau Mellanox ConnectX-4, à partir de la version 13.1-42.x de NetScaler

- Carte réseau Intel 82599

Le tableau suivant répertorie les ressources informatiques virtuelles que le serveur VMware ESX doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 2. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	4 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans ESX, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> **Remarque :**
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production du dispositif virtuel VPX, l'allocation de mémoire complète doit être réservée. Des cycles de processeur (en MHz) égaux au moins à la vitesse d'un cœur de processeur de l'ESX doivent être réservés.

Configuration système requise pour VMware vSphere Client

VMware vSphere est une application cliente qui peut s'exécuter sur les systèmes d'exploitation Windows et Linux. Il ne peut pas être exécuté sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 4. Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « Matrices de compatibilité vSphere » à l'adresse http://kb.vmware.com/.
UC	750 MHz ; 1 gigahertz (GHz) ou plus rapide recommandé
RAM	1 Go. 2 Go recommandés
NIC (NIC)	Carte réseau 100 Mbit/s ou plus rapide

Composant	Exigences

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Il ne peut pas être exécuté sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 4. Tableau 2 Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
NIC (NIC)	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous ne possédez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com, cliquez sur le **lien Nouveaux utilisateurs** et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)

- NSVPX-ESX-<release number>-<build number>.ovf (par exemple, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (par exemple, NSVPX-ESX-13.0-71.44_nc_64.mf)

Installation d'une instance NetScaler VPX sur VMware ESX

Après avoir installé et configuré VMware ESX, vous pouvez utiliser le client VMware vSphere pour installer des dispositifs virtuels sur le serveur VMware ESX. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute VMware ESX.

Pour installer des instances NetScaler VPX sur VMware ESX à l'aide de VMware vSphere Client, procédez comme suit :

1. Démarrez le client VMware vSphere sur votre station de travail.
2. Dans la zone de texte **Adresse IP/Nom**, tapez l'adresse IP du serveur VMware ESX auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot** de passe, tapez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**
6. Mappez les réseaux affichés dans le modèle OVF du dispositif virtuel aux réseaux que vous avez configurés sur l'hôte ESX. Cliquez sur **Suivant** pour commencer à installer un dispositif virtuel sur VMware ESX. Une fois l'installation terminée, une fenêtre contextuelle vous informe de la réussite de l'installation.
7. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.**
8. Une fois la machine virtuelle démarrée, à partir de la console, configurez les adresses IP, Netmask et Gateway de NetScaler. Lorsque vous avez terminé la configuration, sélectionnez l'option **Enregistrer et quitter** dans la console.
9. Pour installer un autre dispositif virtuel, répétez les étapes 6 à 8.

> **Remarque :**
>
> Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000.
>
> Après l'installation, vous pouvez utiliser le client vSphere ou vSphere Web Client pour gérer les dispositifs virtuels sur VMware ESX.
>
> Pour activer le balisage VLAN sur VMware ESX, configurez l'ID VLAN du groupe de ports sur Tous

> (4095) sur le vSwitch. Pour obtenir des instructions détaillées sur la définition d'un ID VLAN sur le vSwitch, reportez-vous à la documentation VMware.

Migrer une instance NetScaler VPX à l'aide de VMware vMotion

Vous pouvez migrer une instance NetScaler VPX à l'aide de VMware vSphere vMotion.

Suivez ces instructions d'utilisation :

- VMware ne prend pas en charge la fonctionnalité VMotion sur les machines virtuelles configurées avec les interfaces PCI Passthrough et SR-IOV.
- Les interfaces prises en charge sont E1000 et VMXNET3. Pour utiliser vMotion sur votre instance VPX, assurez-vous que l'instance est configurée avec une interface prise en charge.
- Pour plus d'informations sur la façon de migrer une instance à l'aide de VMware VMotion, consultez la documentation VMware.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau VMXNET3

October 17, 2024

Après avoir installé et configuré l'instance NetScaler VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle afin qu'elle utilise les interfaces réseau VMXNET3.

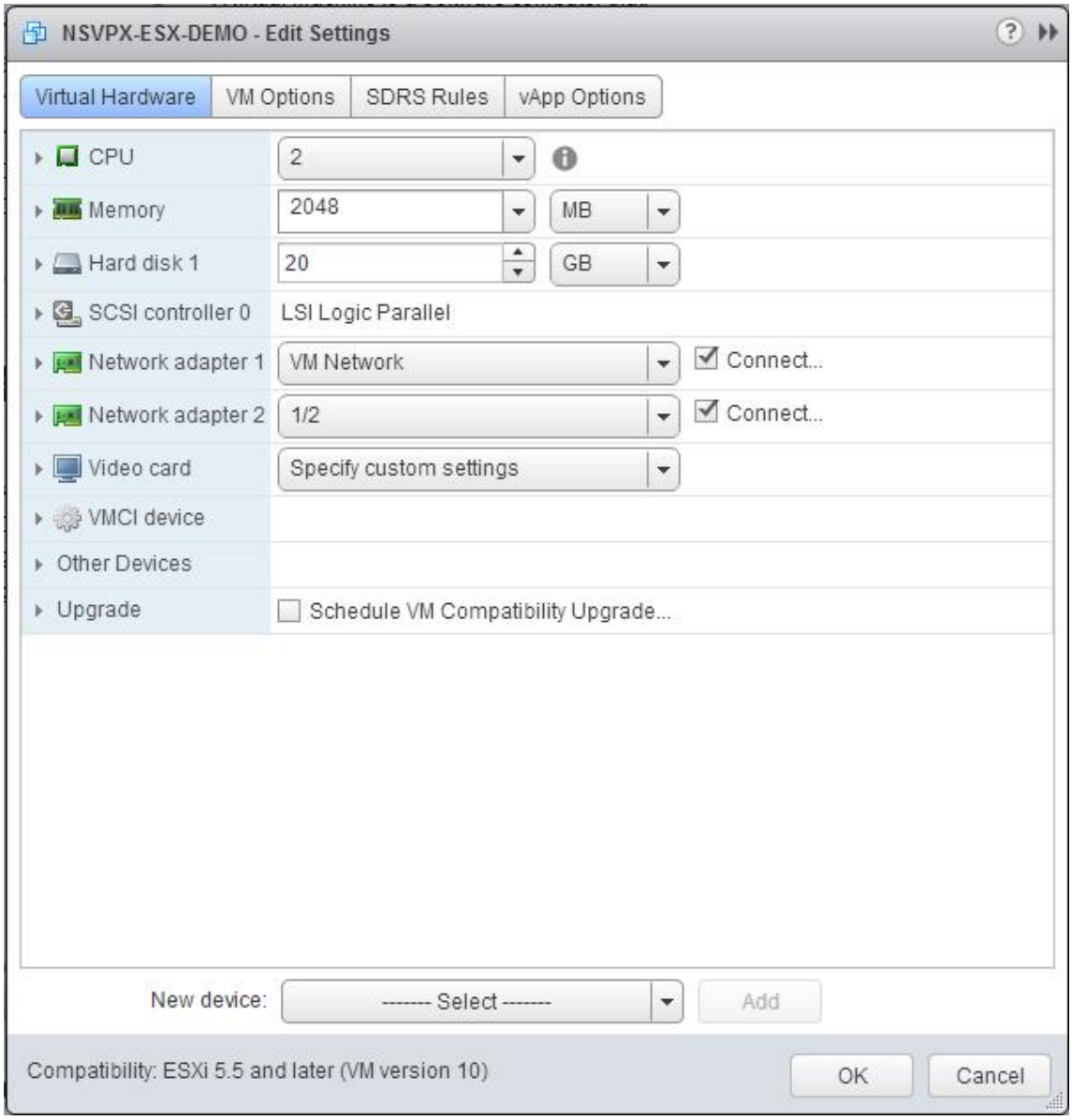
Pour configurer les instances NetScaler VPX afin qu'elles utilisent les interfaces réseau VMXNET3 à l'aide du client Web VMware vSphere :

1. Dans vSphere Web Client, sélectionnez Hôtes et clusters.
2. Mettez à niveau le paramètre de compatibilité de l'instance NetScaler VPX vers ESX, comme suit :

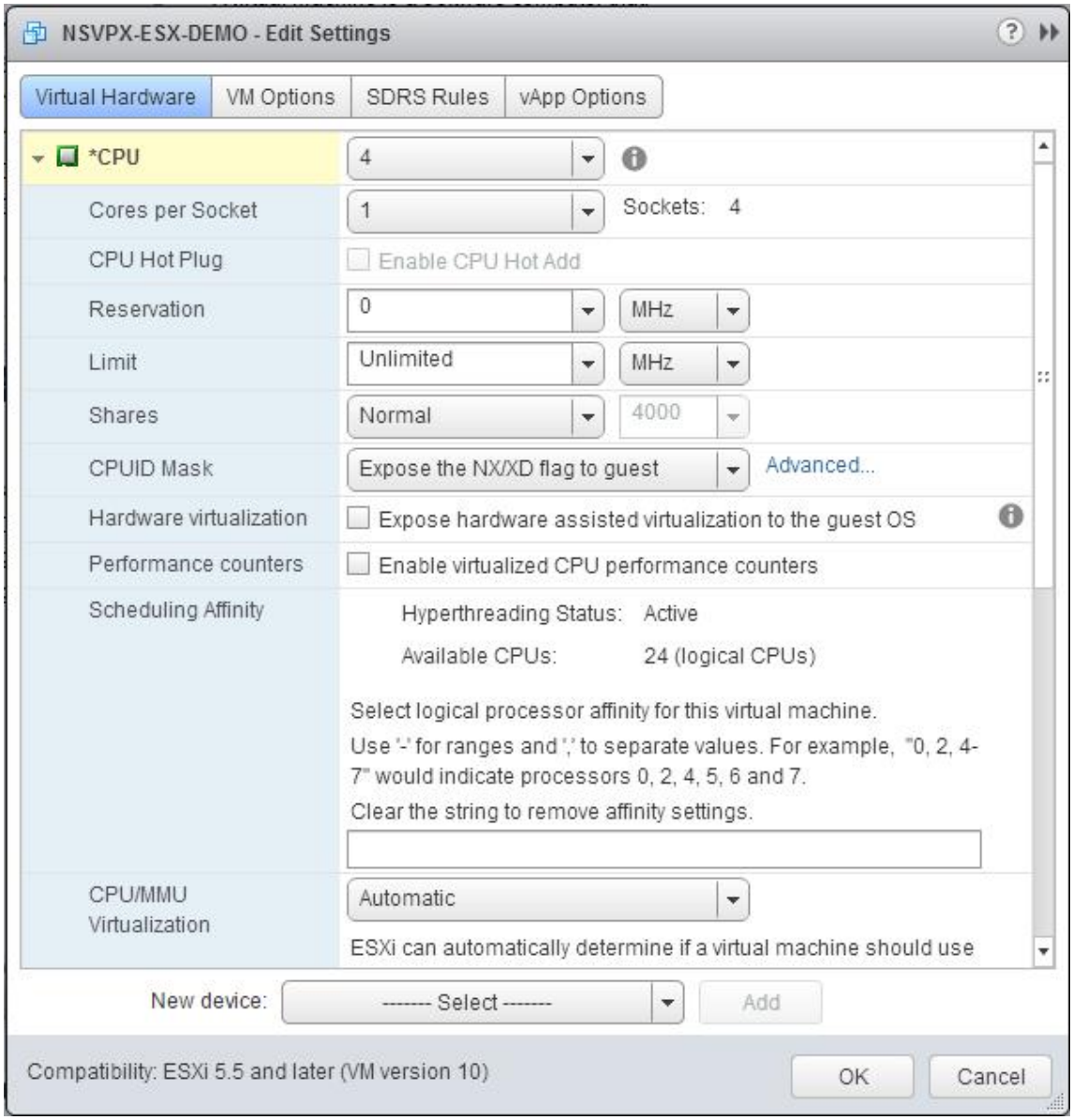
   a. Éteignez l'instance NetScaler VPX.

   b. Cliquez avec le bouton droit sur l'instance NetScaler VPX et sélectionnezCompatibilité > Mettre à niveau la compatibilité des machines virtuelles.

   c. Dans la boîte de dialogue Configurer la compatibilité des machines virtuelles, sélectionnez ESXi 5.5 et versions ultérieures dans la liste déroulante Compatible avec, puis cliquez sur OK.
3. Cliquez avec le bouton droit sur l'instance NetScaler VPX, puis cliquez sur Modifier les paramètres.



4. Dans la boîte de dialogue <virtual_appliance> - Edit Settings, cliquez sur la section CPU.



5. Dans la section CPU, mettez à jour les éléments suivants :

   - Nombre de processeurs
   - Nombre de sockets
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

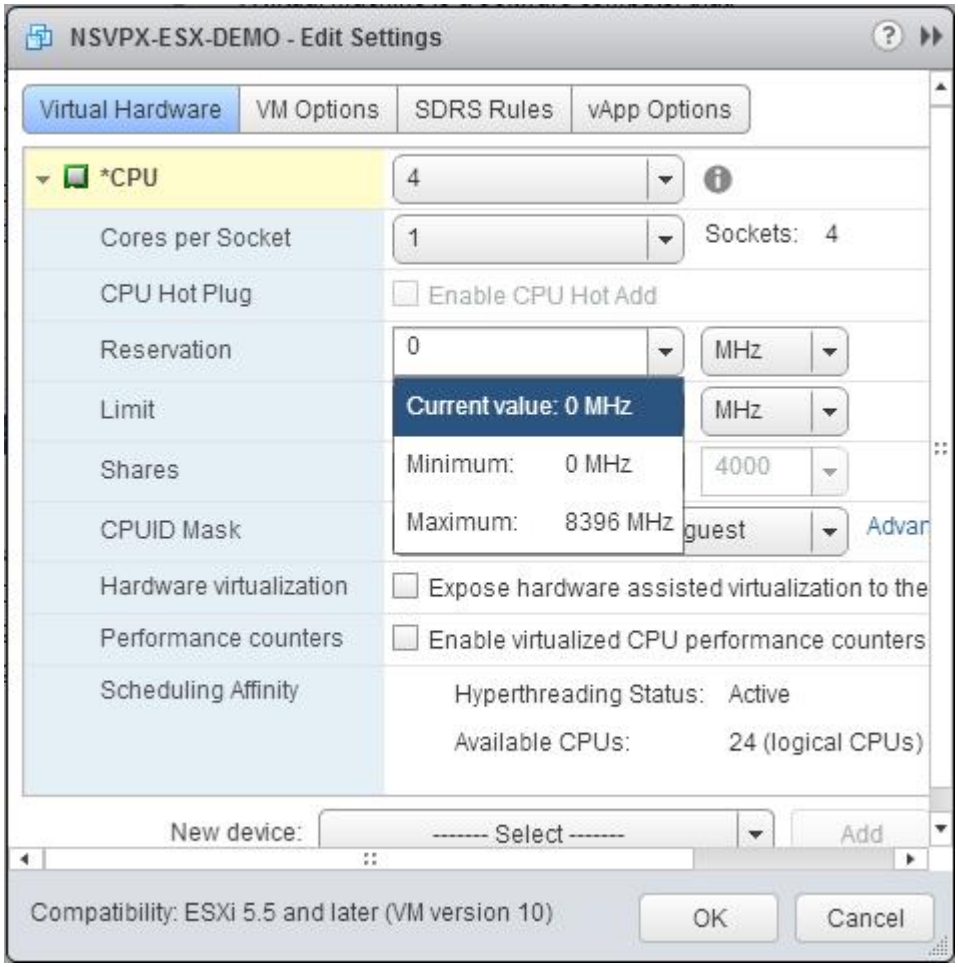
   a. Dans la liste déroulante CPU, sélectionnez le nombre de CPU à affecter à l'appliance virtuelle.

   b. Dans la liste déroulante Cœurs par socket, sélectionnez le nombre de sockets.

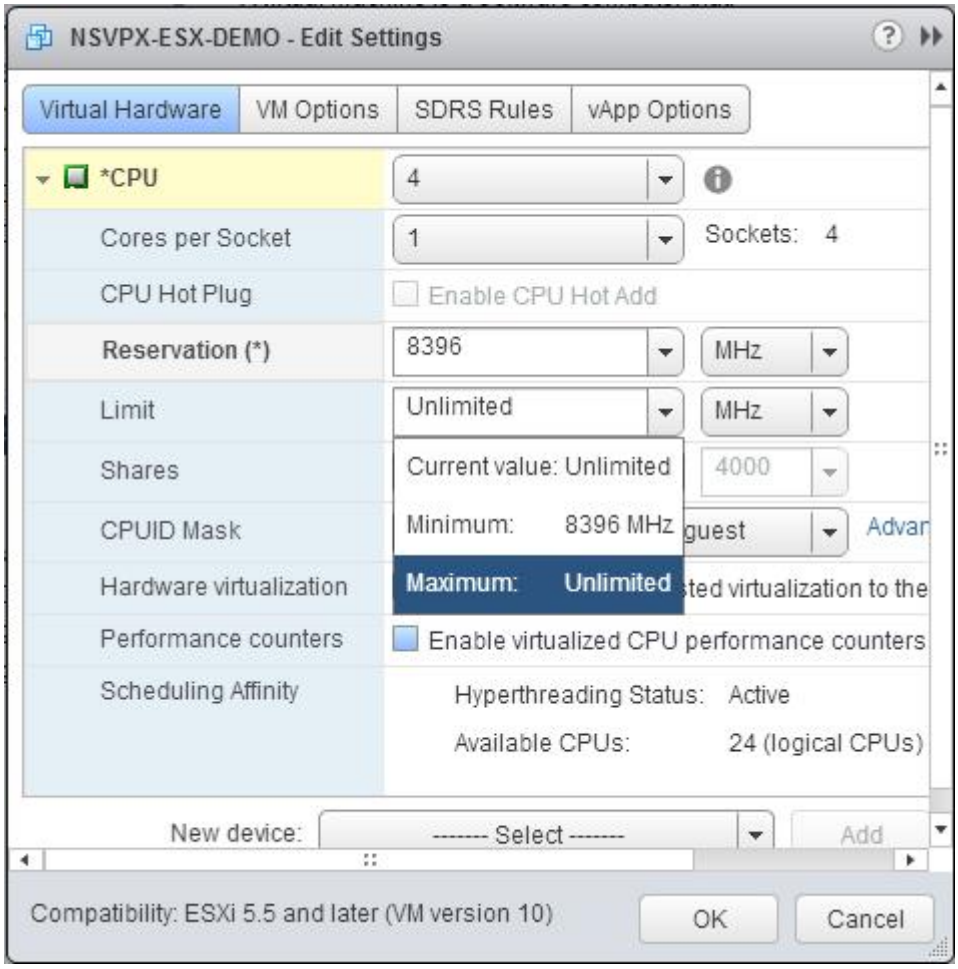
c. (Facultatif) Dans le champ CPU Hot Plug, activez ou désactivez la case à cocher Activer l'ajout à chaud du processeur.

> **Remarque :**
>
> Citrix recommande d'accepter la valeur par défaut (désactivé).

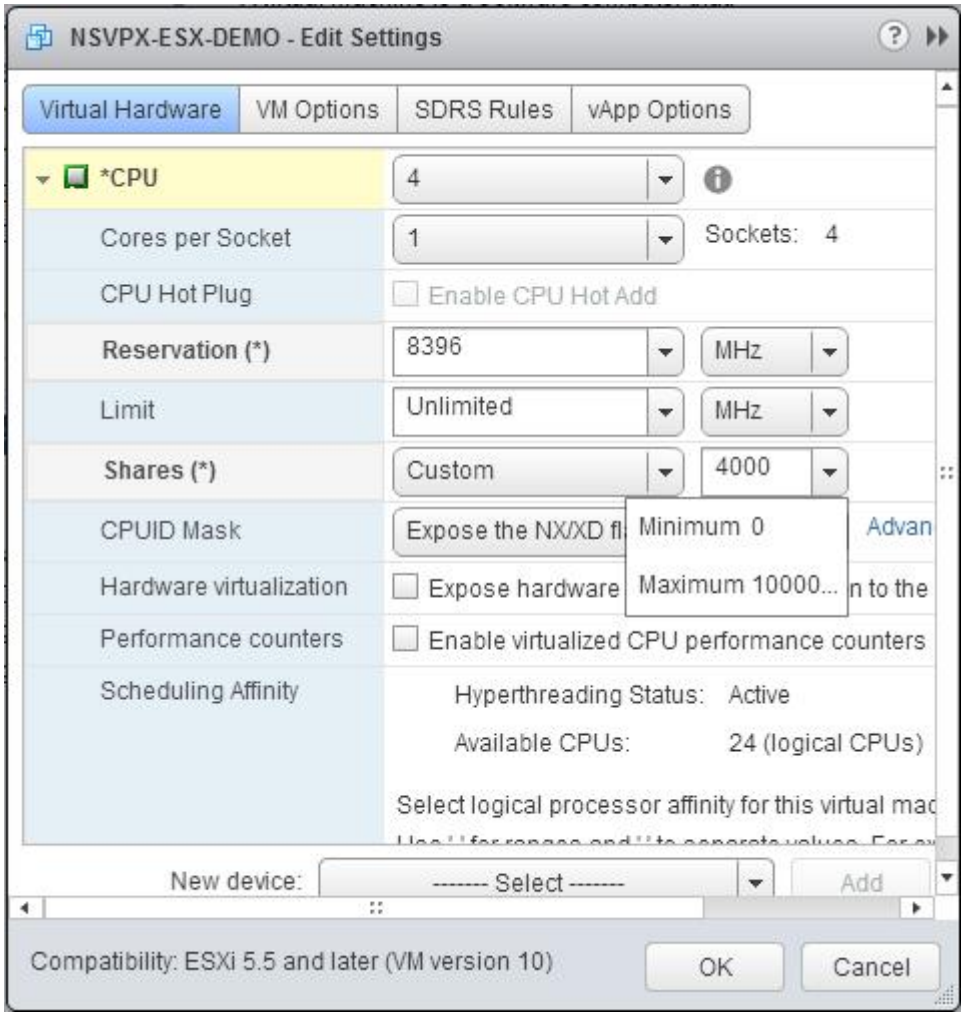
d. Dans la liste déroulante Réservation, sélectionnez le nombre qui est affiché comme valeur maximale.



e. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes Partages, sélectionnez Personnalisé et le nombre qui s'affiche comme valeur maximale.



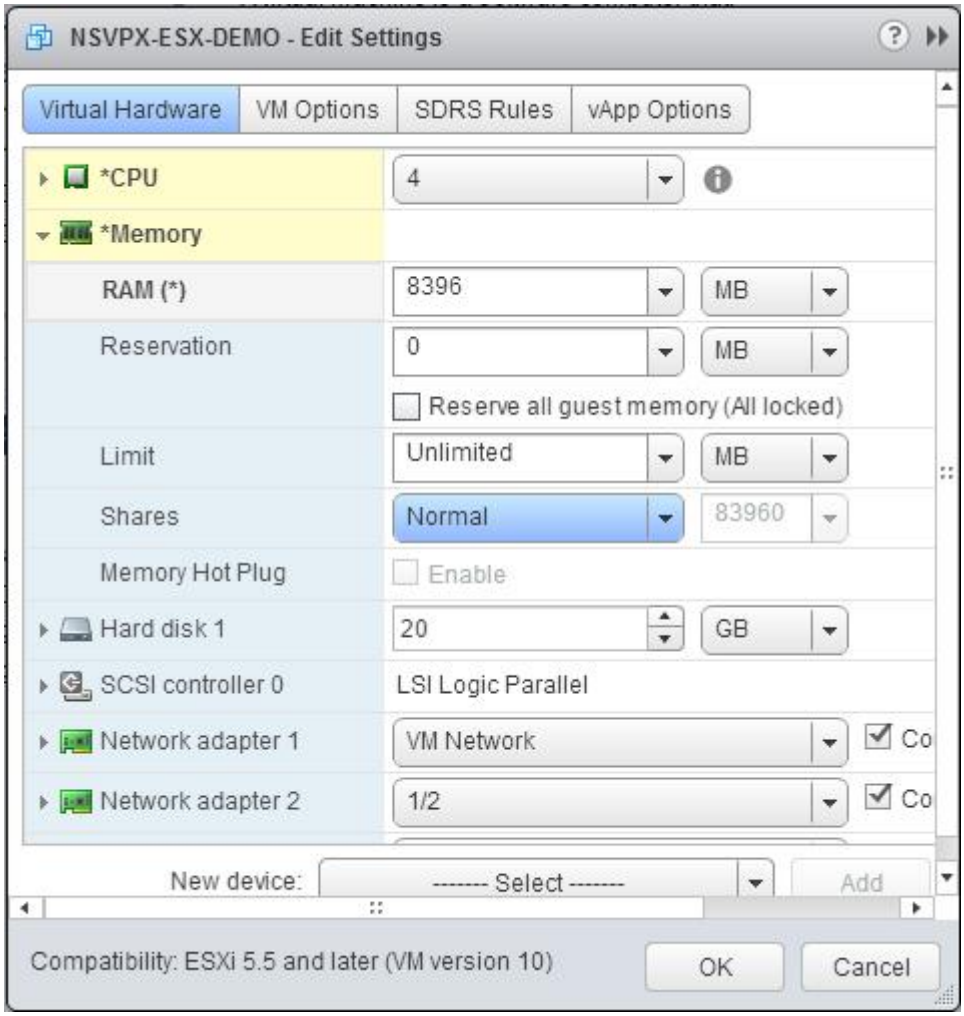
6. Dans la section Mémoire, mettez à jour les éléments suivants :

   - Taille de la RAM
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

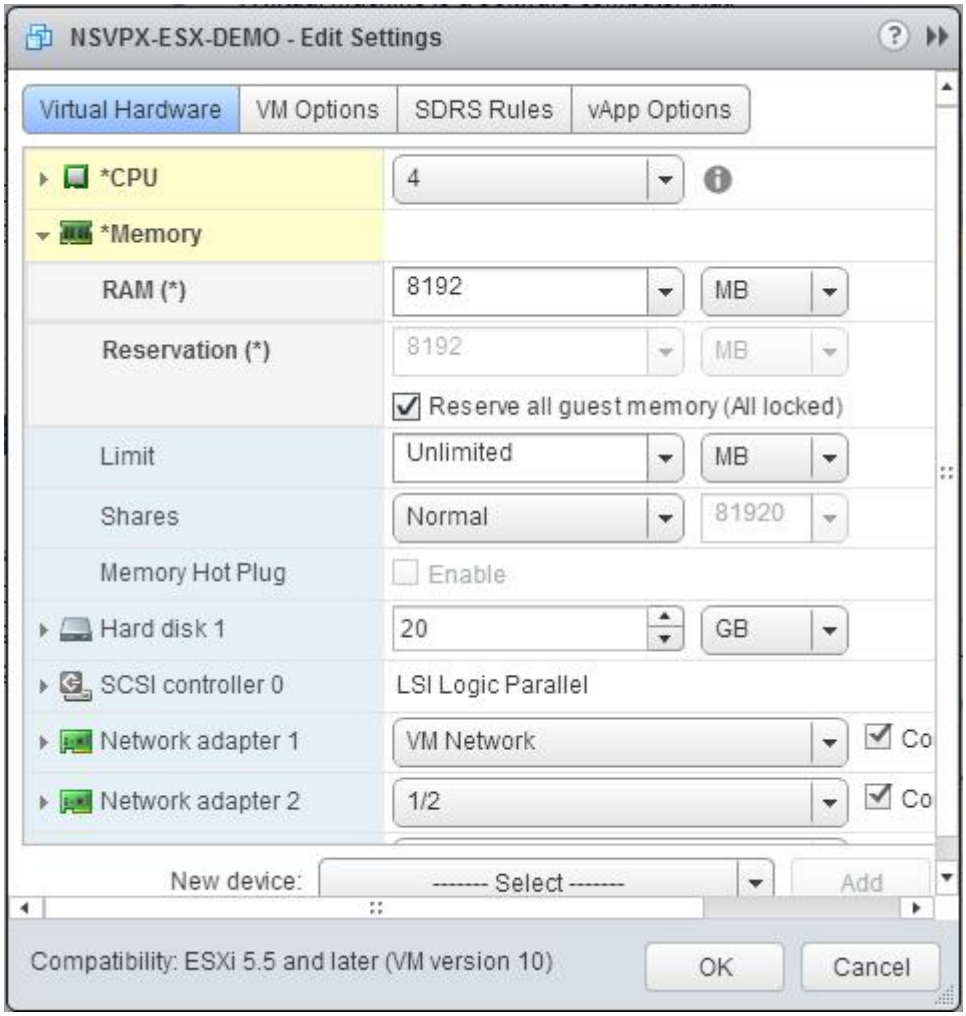
   a. Dans la liste déroulante RAM, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la RAM doit être de 4 x 2 Go = 8 Go.

   > **Remarque :**
   >
   > Pour une édition Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

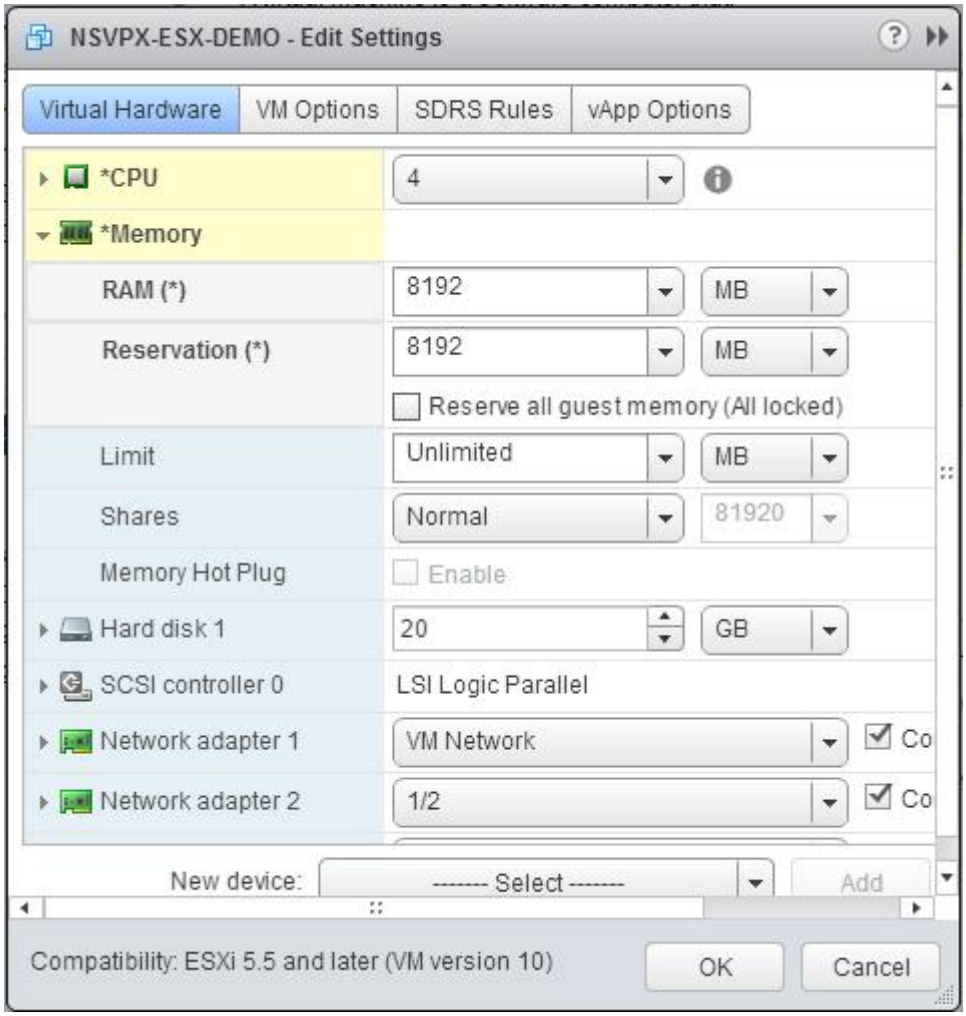


b. Dans la liste déroulante Réservation, entrez la valeur de la réservation mémoire et activez la case à cocher Réserver toute la mémoire invitée (Tout verrouillé). La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

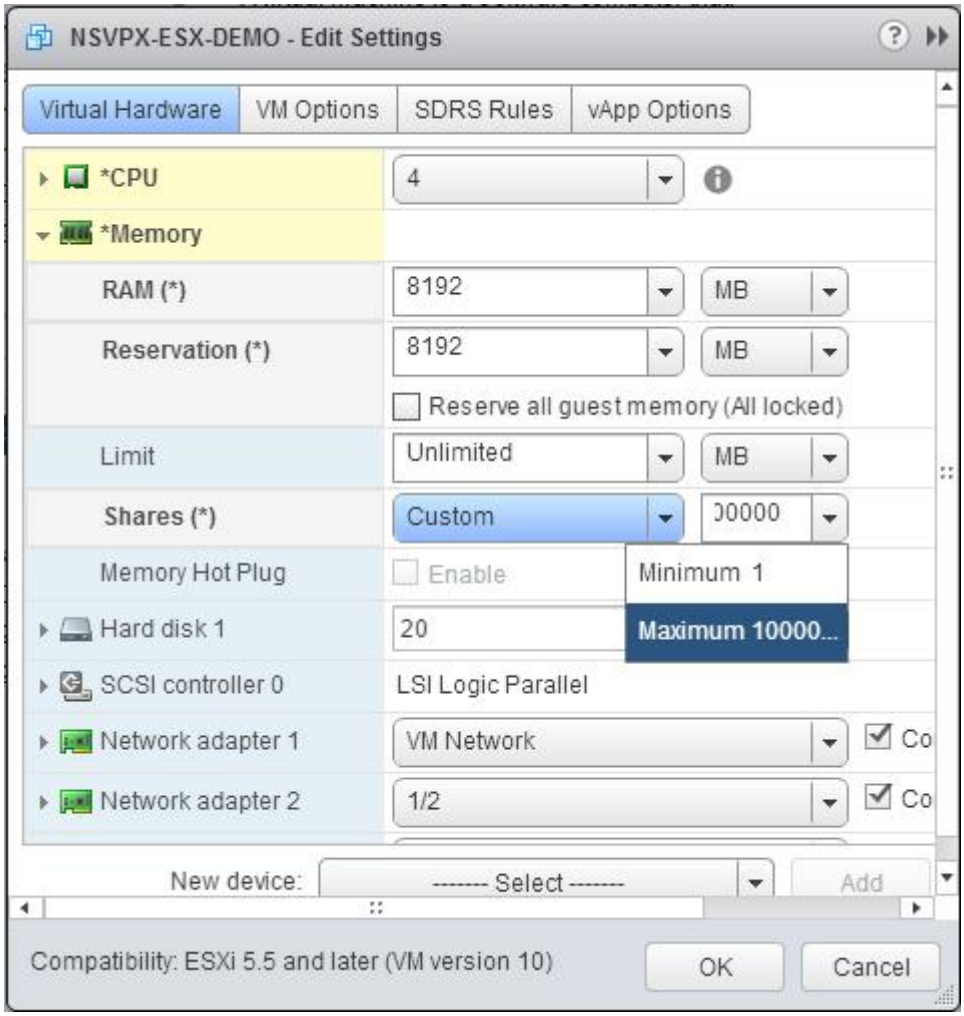
> **Remarque :**
>
> Pour une édition Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



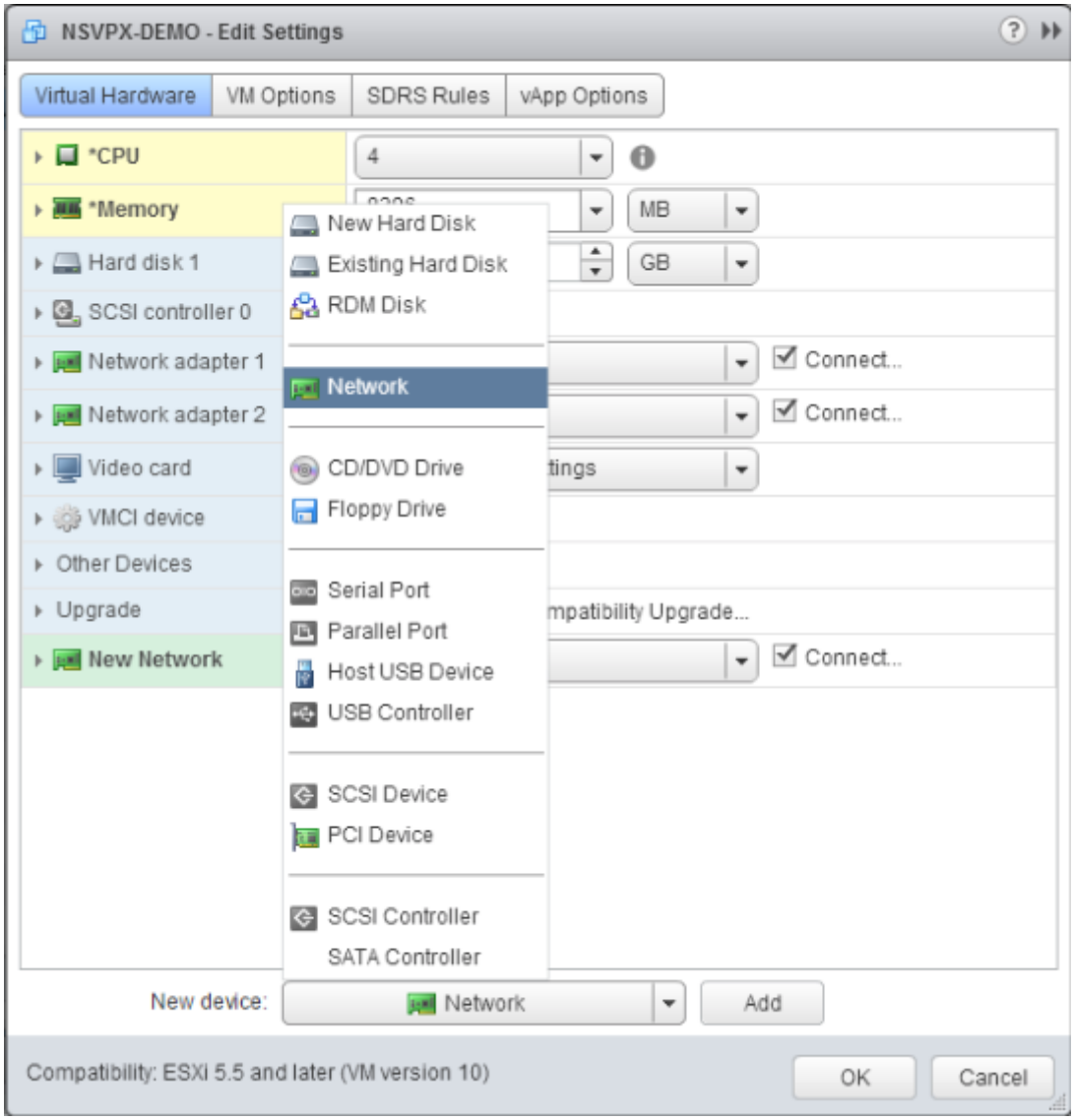
c. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes Partages, sélectionnez Personnalisé et le nombre qui s'affiche comme valeur maximale.



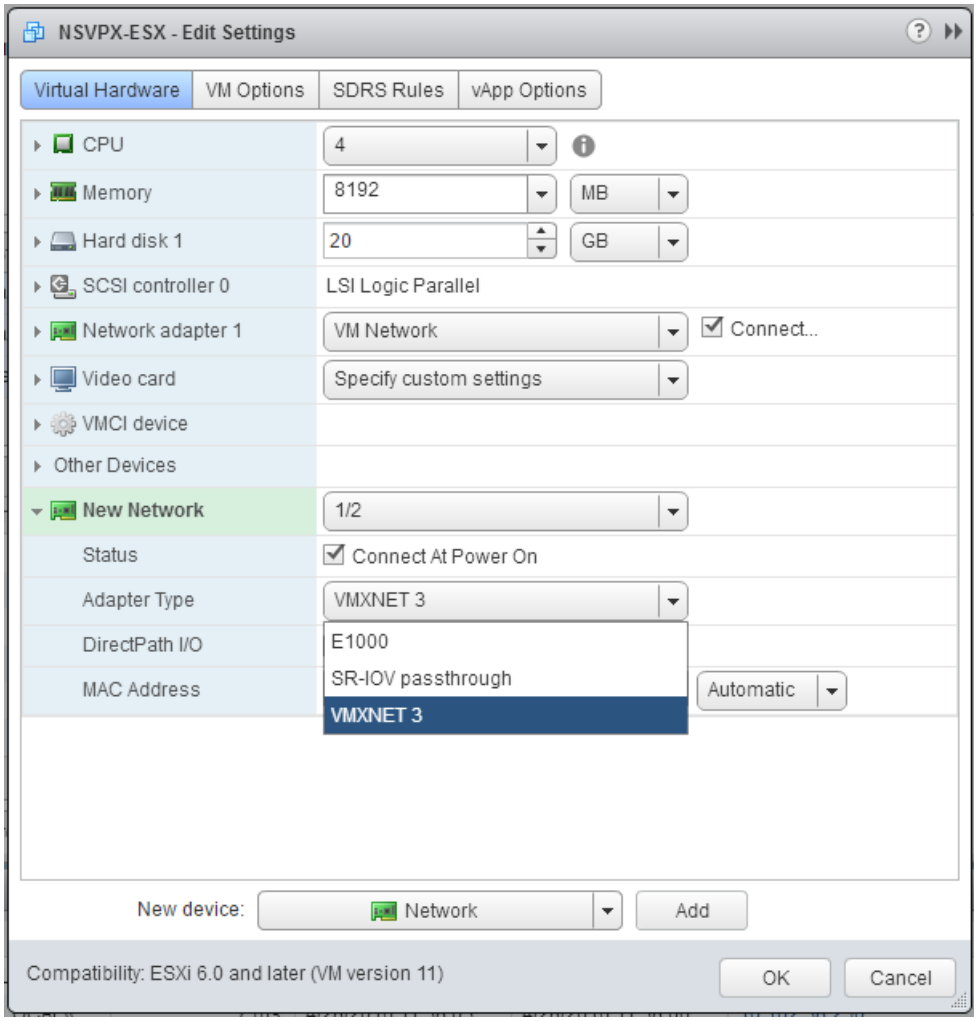
7. Ajoutez une interface réseau VMXNET3. Dans la liste déroulante Nouveau périphérique, sélectionnez Réseau et cliquez sur Ajouter.



8. Dans la section Nouveau réseau, dans la liste déroulante, sélectionnez l'interface réseau et procédez comme suit :

   a. Dans la liste déroulante Type d'adaptateur, sélectionnez VMXNET3.

   > **Important :**
   >
   > L'interface réseau E1000 par défaut et VMXNET3 ne peuvent pas coexister, assurez-vous de supprimer l'interface réseau E1000 et d'utiliser VMXNET3 (0/1) comme interface de gestion.



9. Cliquez sur **OK**.
10. Allumez l'instance NetScaler VPX.
11. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

> Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
> show interface summary
-------------------------------------------------------------------------------

      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------

1     0/1        1500       00:0c:29:89:1d:0e  NetScaler Vir...
   rface, VMXNET3
2     1/1        9000       00:0c:29:89:1d:18  NetScaler Vir...
   rface, VMXNET3
```



```
7    3     1/2        9000       00:0c:29:89:1d:22    NetScaler Vir...
     rface, VMXNET3
8    4     LO/1       9000       00:0c:29:89:1d:0e    Netscaler Loopback
     interface
```

> **Remarque :**
>
> Après avoir ajouté une interface VMXNET3 et redémarré l'appliance NetScaler VPX, l'hyperviseur VMware ESX peut modifier l'ordre dans lequel la carte réseau est présentée à l'appliance VPX. Par conséquent, la carte réseau 1 peut ne pas toujours rester 0/1, ce qui entraîne une perte de connectivité de gestion à l'appliance VPX. Pour éviter ce problème, modifiez le réseau virtuel de la carte réseau en conséquence.
>
> Il s'agit d'une limitation de l'hyperviseur VMware ESX.

Définir la taille de l'anneau de réception pour l'interface réseau VMXNET3

Vous pouvez augmenter la taille de l'anneau de réception pour les interfaces réseau VMXNET3 sur VMware ESX. Une taille d'anneau plus élevée réduit les pertes de paquets en cas d'augmentation soudaine du trafic.

> **Remarque :**
>
> Cette fonctionnalité est disponible dans la version 14.1 build 14.x et les versions ultérieures.

Pour définir la taille de l'anneau sur une interface réseau VMXNET3

À l'invite de commande, tapez :

définir l'*identifiant* de l'interface [-ringsize *positive_integer*]

La taille maximale que vous pouvez définir pour l'anneau d'une interface VMXNET3 est de 2048. Seul le type d'anneau fixe est pris en charge. Vous devez enregistrer la configuration et redémarrer l'instance NetScaler VPX pour que les paramètres soient pris en compte.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

October 17, 2024

Après avoir installé et configuré l'instance NetScaler VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau d'E/S à racine unique et de virtualisation (SR-IOV).

Limitations

Un NetScaler VPX configuré avec l'interface réseau SR-IOV présente les limites suivantes :

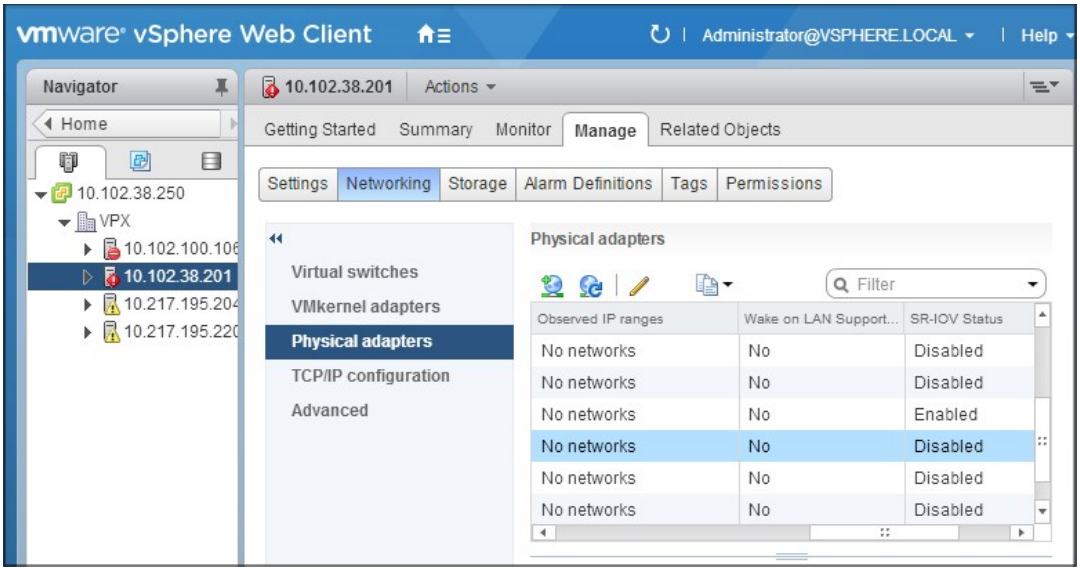
- Les fonctionnalités suivantes ne sont pas prises en charge sur les interfaces SR-IOV utilisant la carte réseau Intel 82599 10G sur ESX VPX :
  - Commutation de mode L2
  - Agrégation de liens statiques et LACP
  - Mise en cluster
  - Partitionnement d'administrateur [mode VLAN partagé]
  - Haute disponibilité [Actif - Mode actif]
  - Cadres Jumbo
  - IPv6
- Les fonctionnalités suivantes ne sont pas prises en charge sur l'interface SR-IOV avec une carte réseau Intel 82599 10G sur KVM VPX :
  - Agrégation de liens statiques et LACP
  - Commutation de mode L2
  - Mise en cluster
  - Partitionnement d'administrateur [mode VLAN partagé]
  - Haute disponibilité [Actif —Mode actif]
  - Cadres Jumbo
  - IPv6
  - La configuration VLAN sur l'interface Hypervisor for SR-IOV VF via `ip link` commande n'est pas prise en charge

Conditions préalables

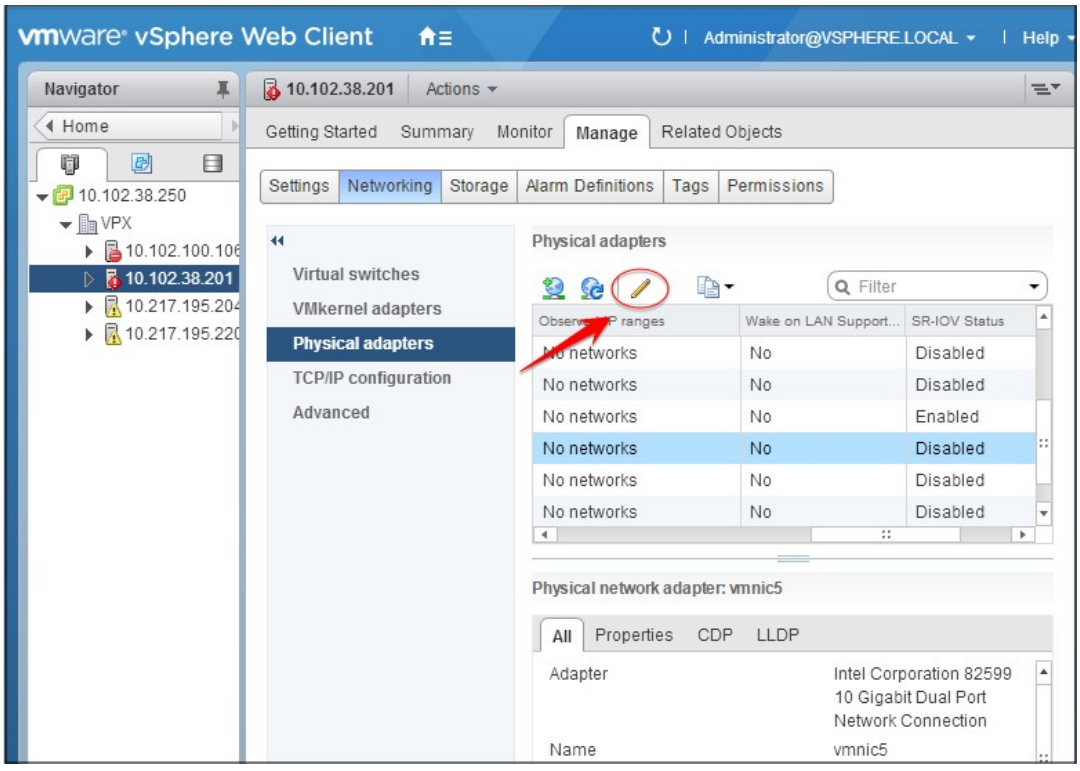
- Assurez-vous d'ajouter l'une des cartes réseau suivantes à l'hôte ESX :
  - Carte réseau Intel 82599, pilote IXGBE version 3.7.13.7.14iov ou ultérieure est recommandée.
  - Carte réseau Mellanox ConnectX-4
- Activez SR-IOV sur l'adaptateur physique de l'hôte.

  Suivez cette procédure pour activer SR-IOV sur l'adaptateur physique hôte :

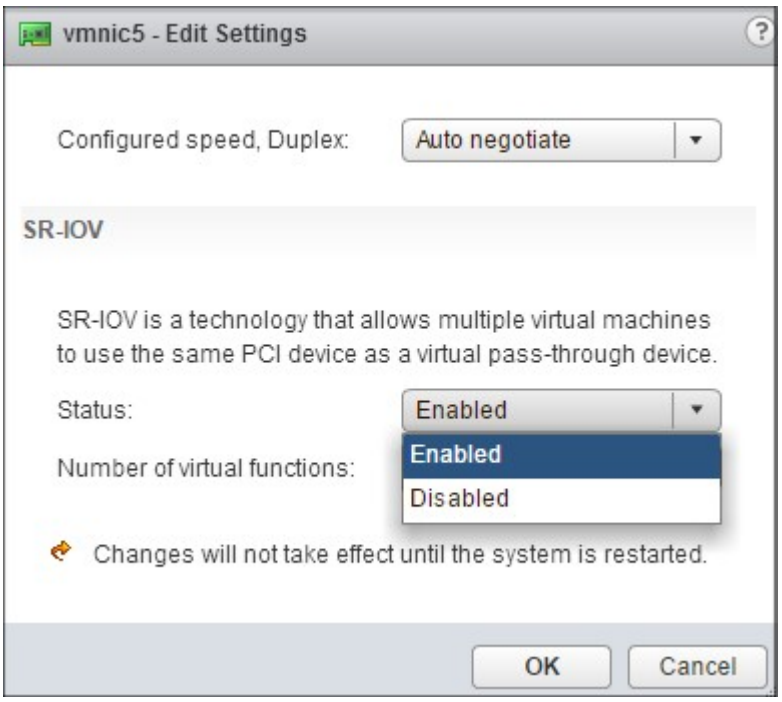
  1. Dans vSphere Web Client, accédez à l'hôte.
  2. Dans l'onglet **Gérer > Réseau**, sélectionnez **Adaptateurs physiques**. Le champ Statut SR-IOV indique si une carte physique prend en charge SR-IOV.



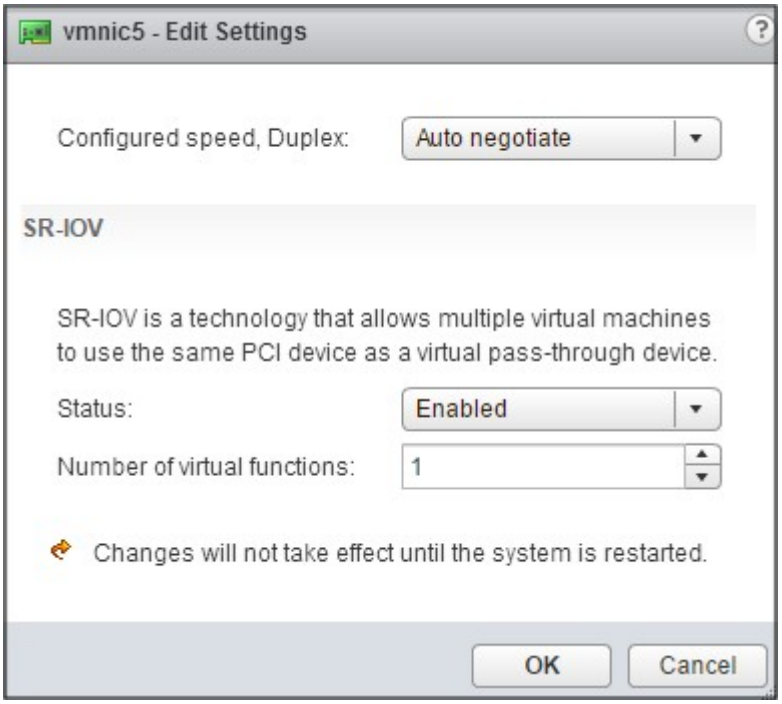
3. Sélectionnez l'adaptateur physique, puis cliquez sur l'icône en forme de crayon pour ouvrir la boîte de dialogue **Modifier les paramètres** .



4. Sous SR-IOV, sélectionnez **Activé** dans la liste déroulante **Statut** .



5. Dans le champ **Nombre de fonctions virtuelles**, entrez le nombre de fonctions virtuelles que vous souhaitez configurer pour la carte.



6. Cliquez sur **OK**.
7. Redémarrez l'hôte.

- Créez un commutateur virtuel distribué (DVS) et `Portgroups`. Pour obtenir des instructions,

reportez-vous à la documentation VMware.

> **Remarque :**
>
> Citrix a qualifié la configuration SR-IOV sur DVS et `Portgroups` uniquement.

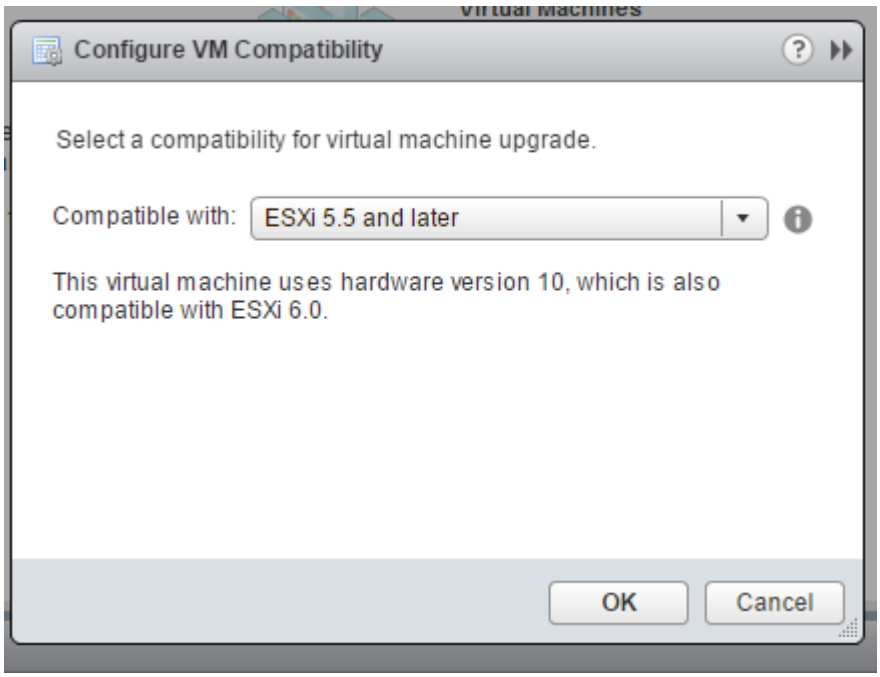
Pour configurer les instances NetScaler VPX afin qu'elles utilisent l'interface réseau SR-IOV à l'aide de VMware vSphere Web Client :

1. Dans vSphere Web Client, sélectionnez **Hôtes et clusters**.
2. Mettez à niveau le paramètre de compatibilité de l'instance NetScaler VPX vers ESX 5.5 ou version ultérieure, comme suit :

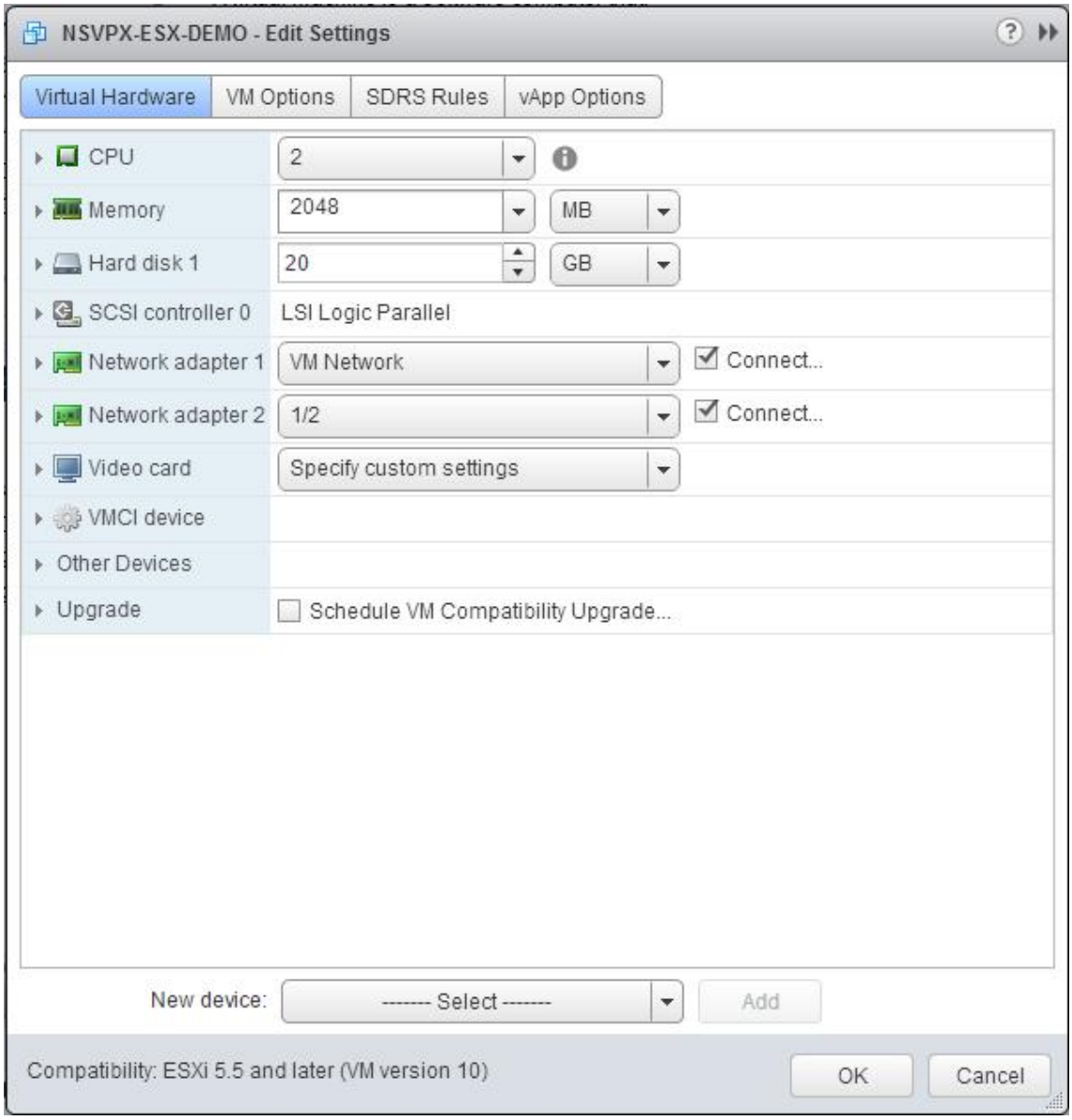
   a. Éteignez l'instance NetScaler VPX.

   b. Cliquez avec le bouton droit sur l'instance NetScaler VPX et sélectionnez **Compatibilité > Mettre à niveau la compatibilité**des machines virtuelles.

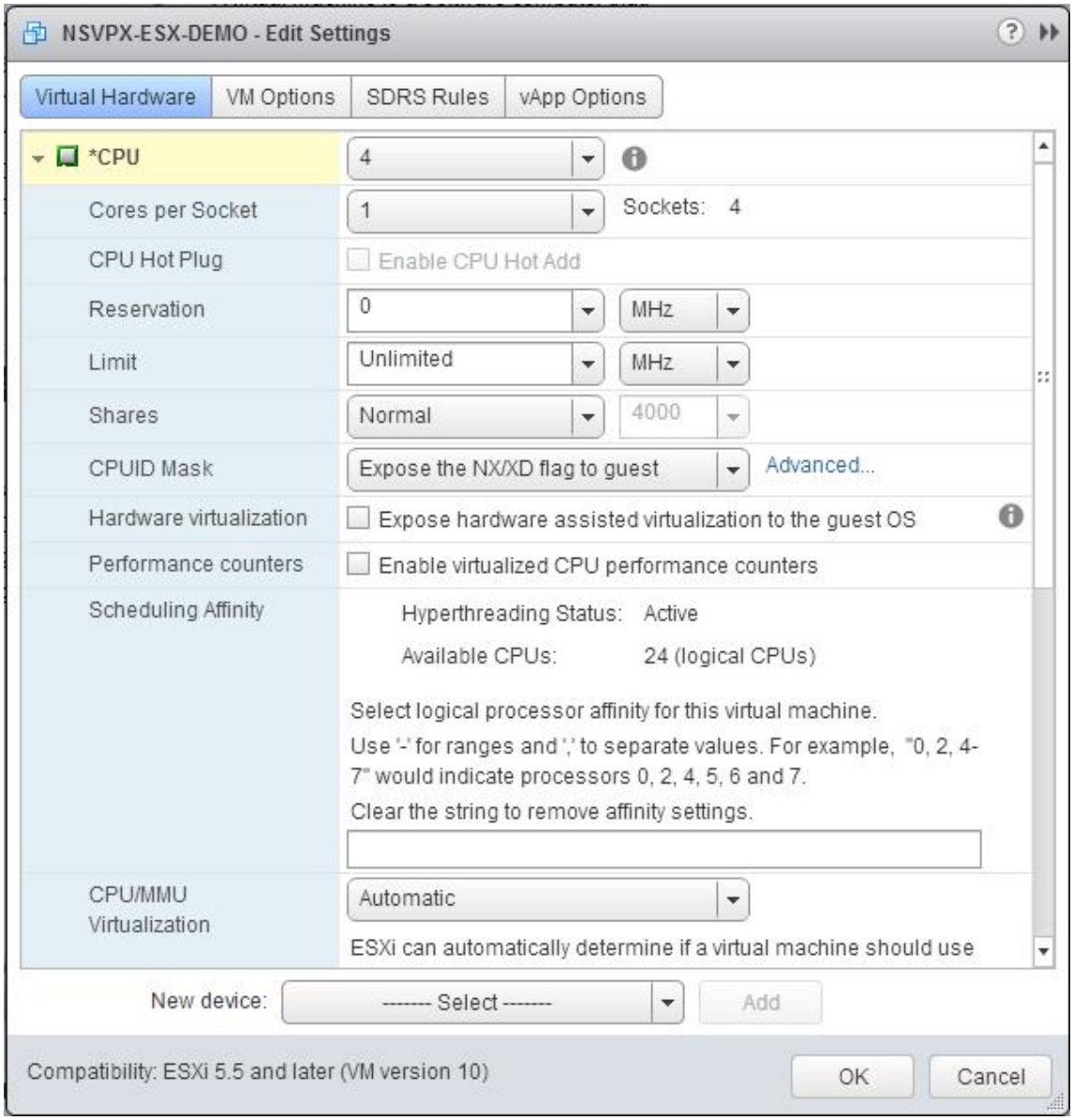
   c. Dans la boîte de dialogue **Configurer la compatibilité des machines virtuelles**, sélectionnez **ESXi 5.5 et versions ultérieures** dans la liste déroulante **Compatible avec**, puis cliquez sur **OK**.



3. Cliquez avec le bouton droit sur l'instance NetScaler VPX et cliquez sur Modifier les paramètres.



4. Dans la <virtual_appliance>boîte de dialogue **- Modifier les paramètres**, cliquez sur la section **CPU** .



5. Dans la section **CPU**, mettez à jour les paramètres suivants :

   - Nombre de processeurs
   - Nombre de sockets
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

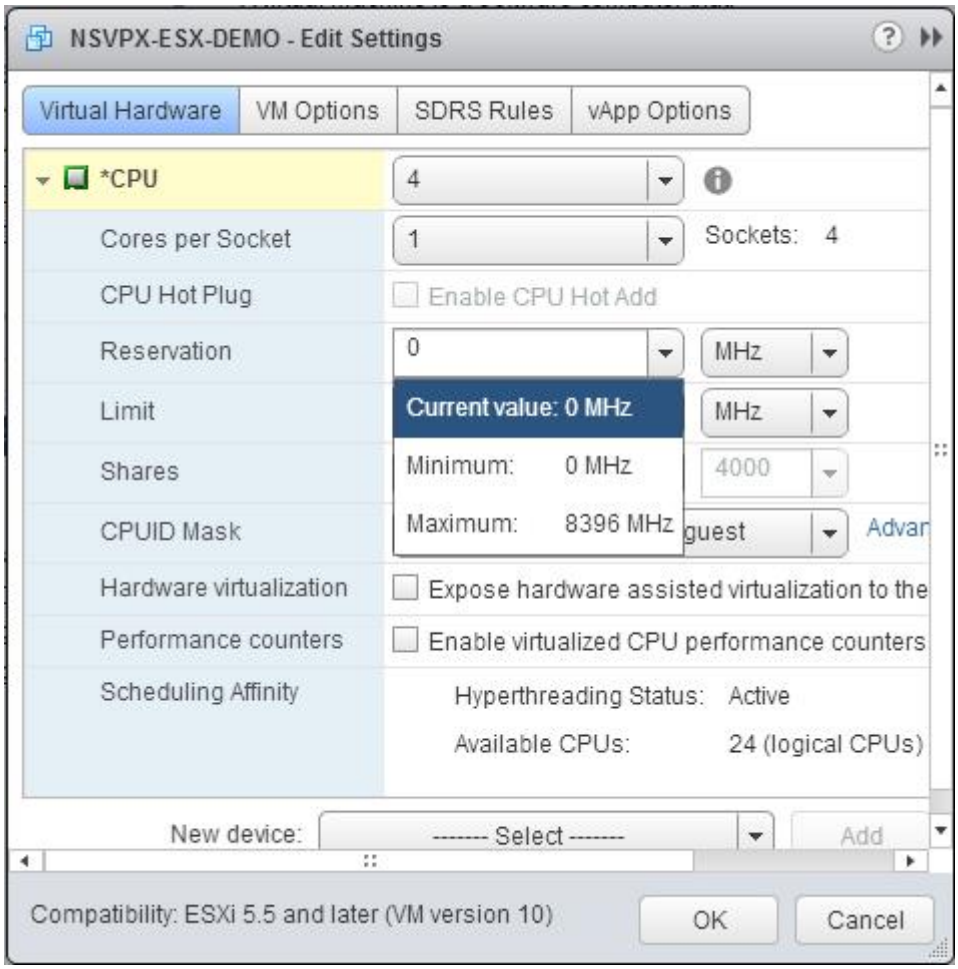
   a. Dans la liste déroulante **CPU**, sélectionnez le nombre de CPU à attribuer à l'appliance virtuelle.

   b. Dans la liste déroulante **Cores par socket**, sélectionnez le nombre de sockets.

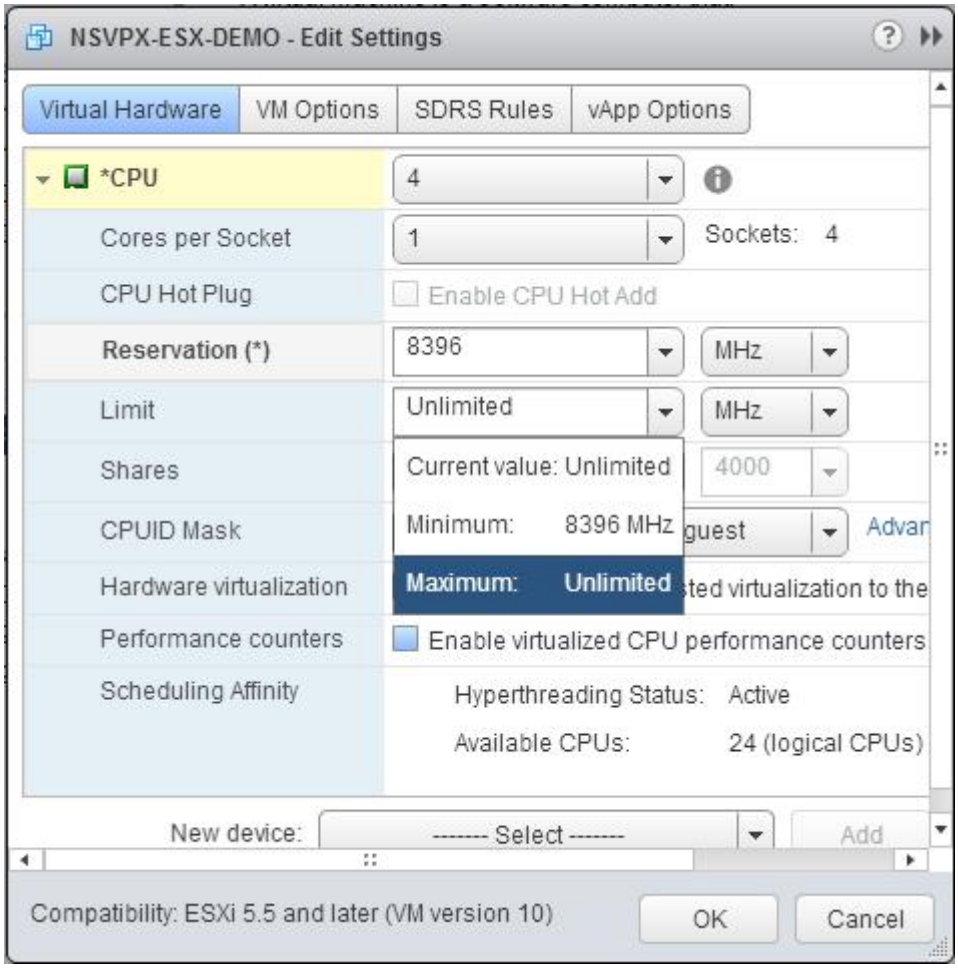
c. (Facultatif) Dans le champ **CPU Hot Plug**, cochez ou décochez la case **Activer l'ajout à chaud du processeur** .

> **Remarque :**
>
> Citrix recommande d'accepter la valeur par défaut (désactivé).

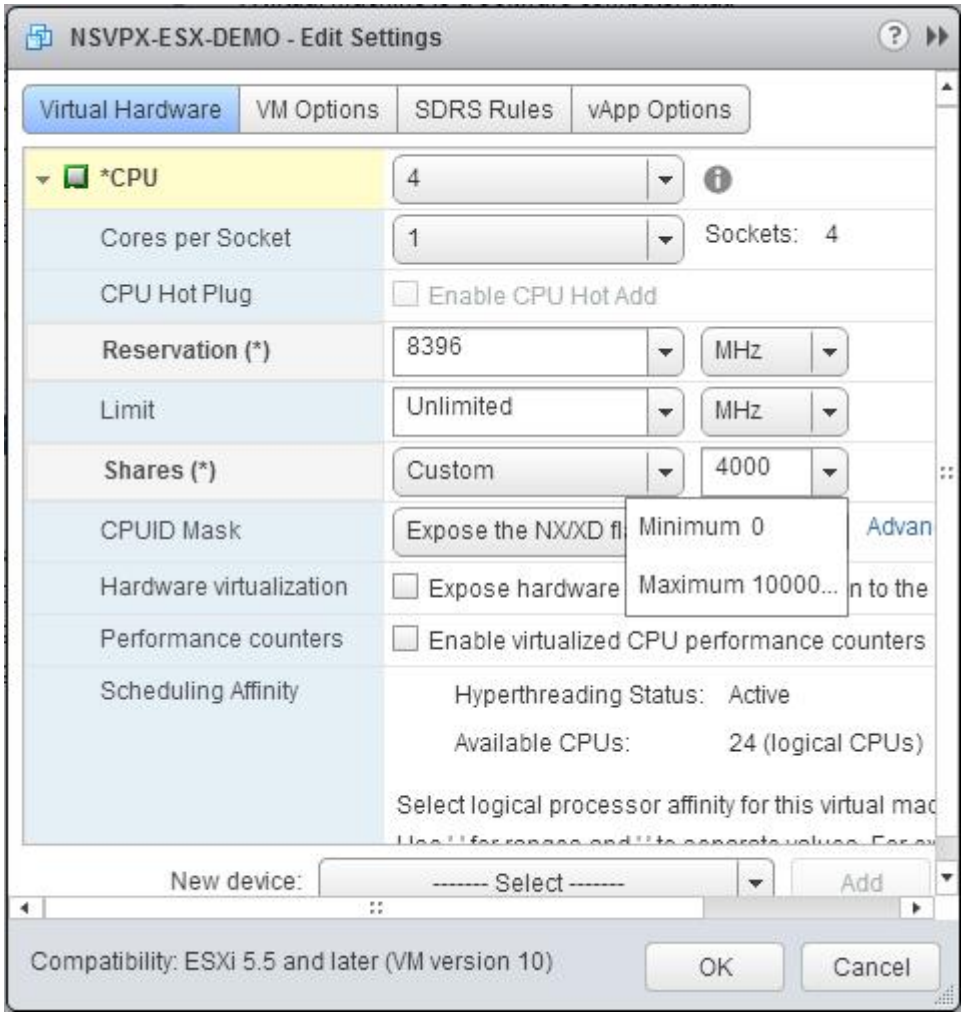
d. Dans la liste déroulante **Réservation**, sélectionnez le nombre affiché comme valeur maximale.



e. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes **Partages**, sélectionnez **Personnalisé** et le nombre affiché comme valeur maximale.



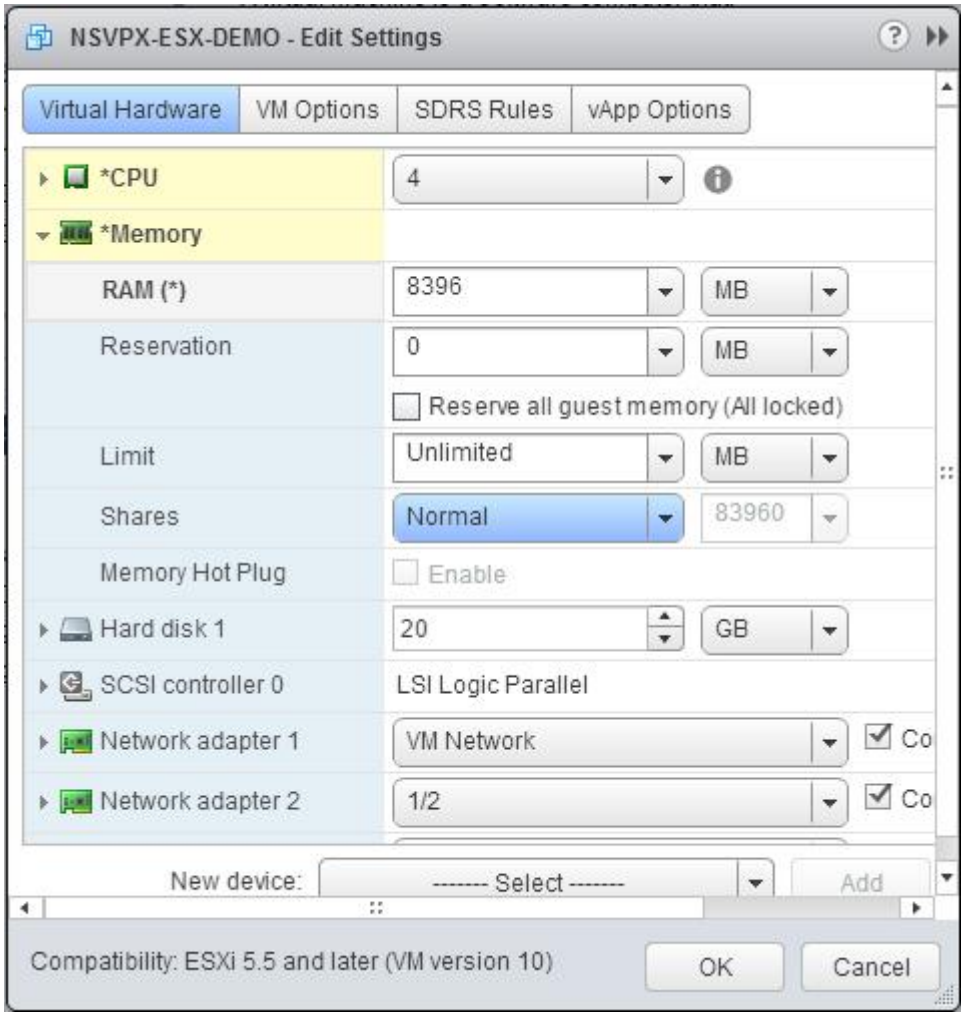
6. Dans la section **Mémoire**, mettez à jour les paramètres suivants :

   - Taille de la RAM
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

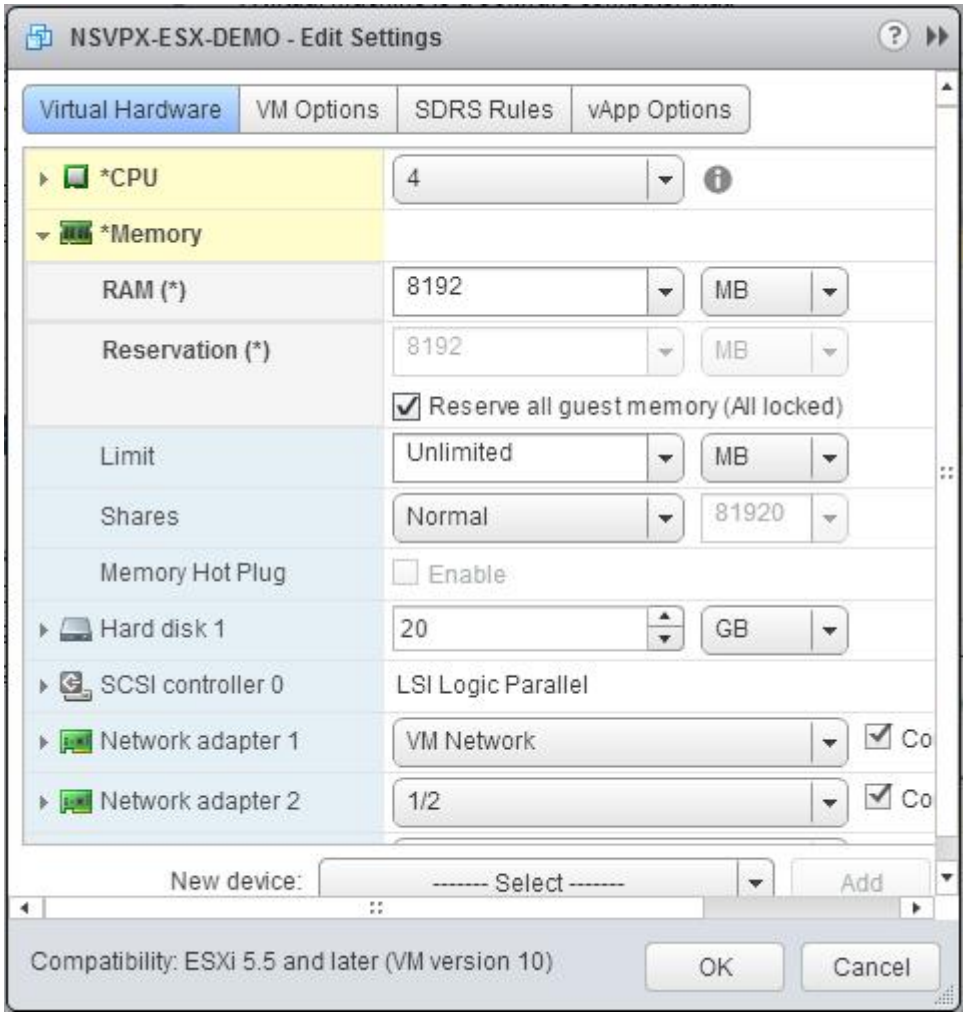
   a. Dans la liste déroulante **RAM**, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 2 Go = 8 Go.

   > **Remarque :**
   >
   > Pour l'édition Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

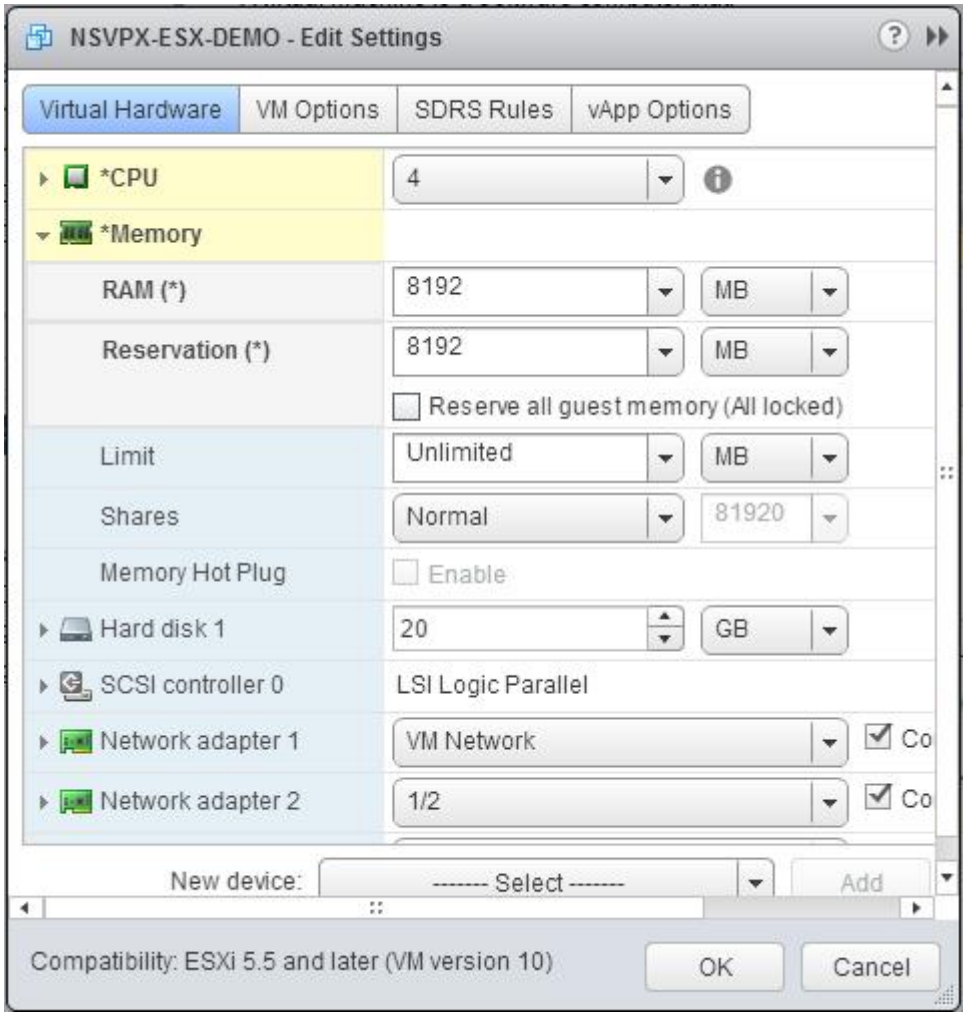


b. Dans la liste déroulante **Réservation**, entrez la valeur de la réservation de mémoire et cochez la case **Réserver toute la mémoire client (Tout est verrouillé)** . La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

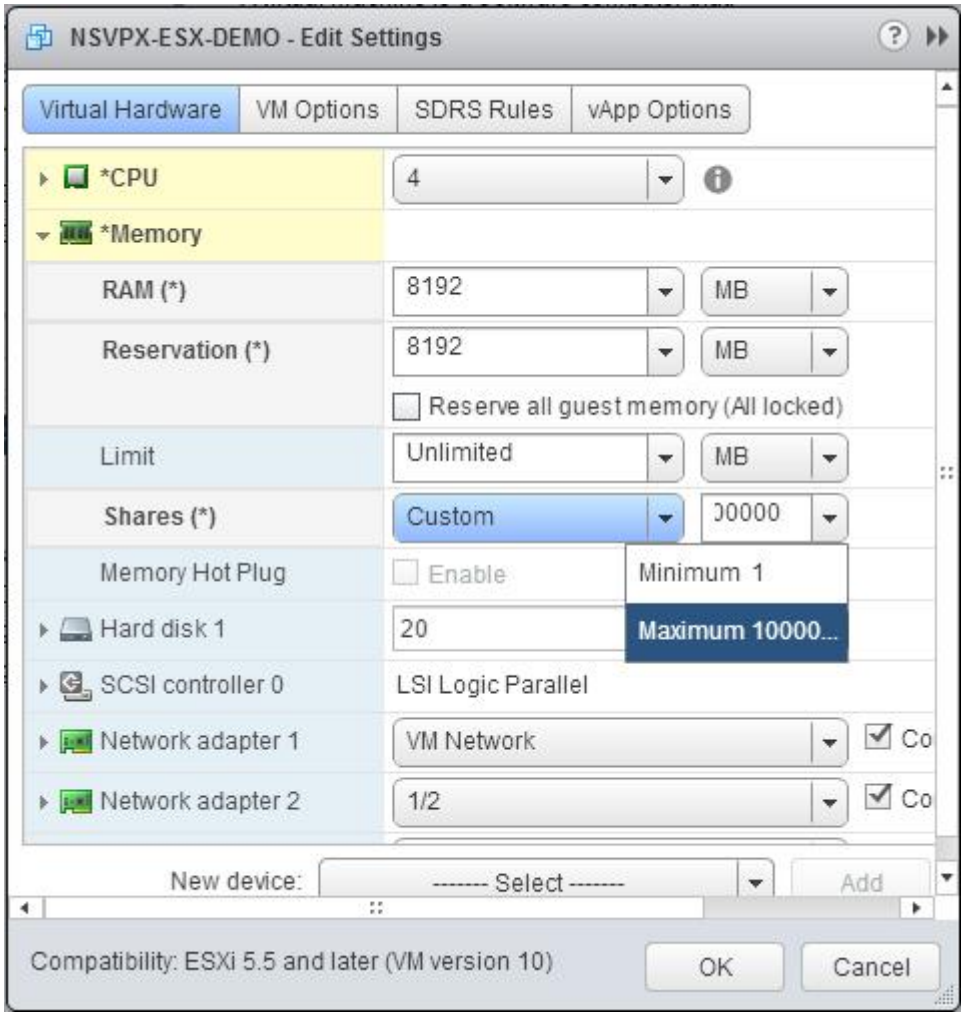
> **Remarque :**
>
> Pour l'édition Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



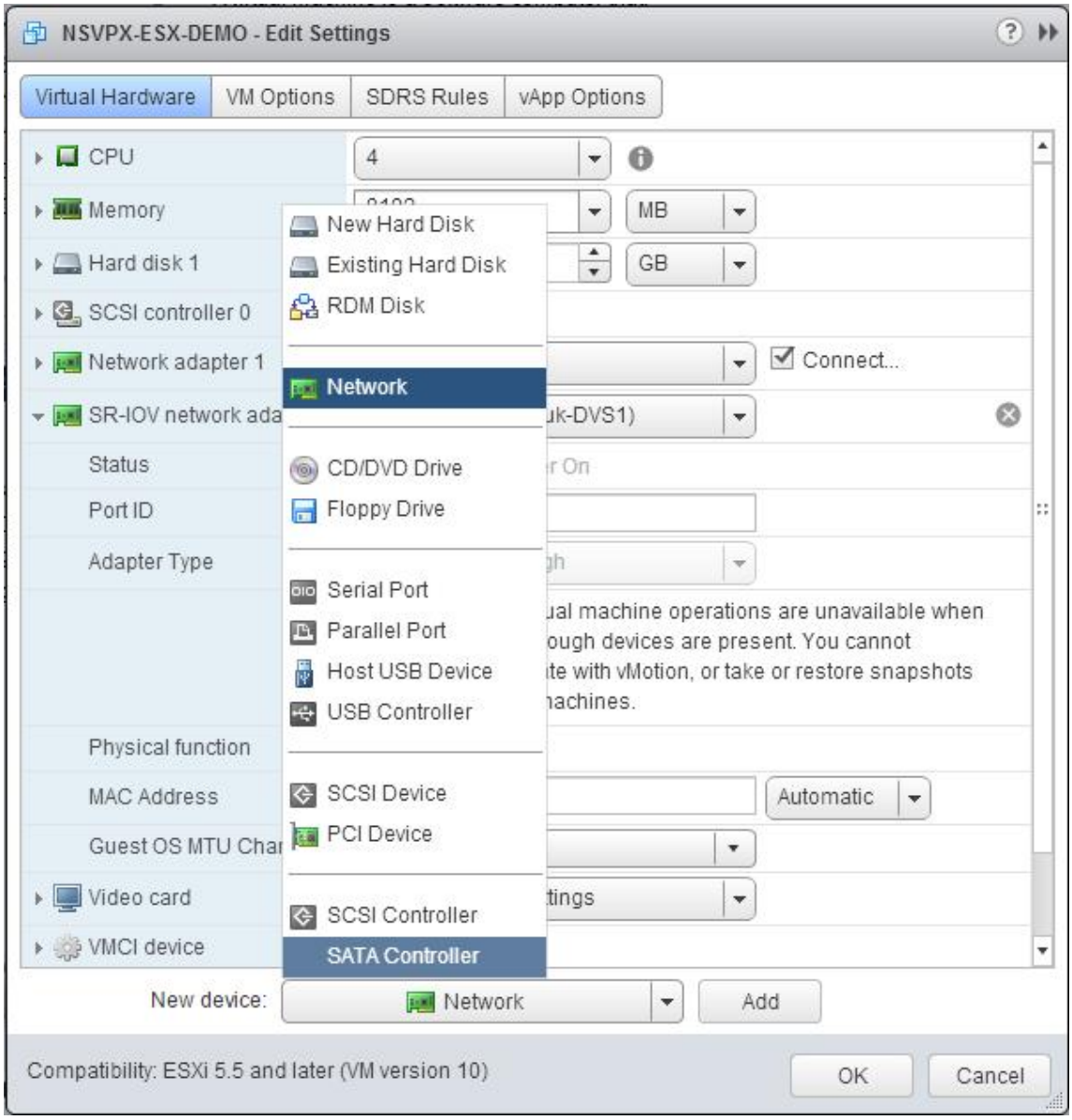
c. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes **Parts**, sélectionnez **Personnalisé**, puis sélectionnez le nombre affiché comme valeur maximale.

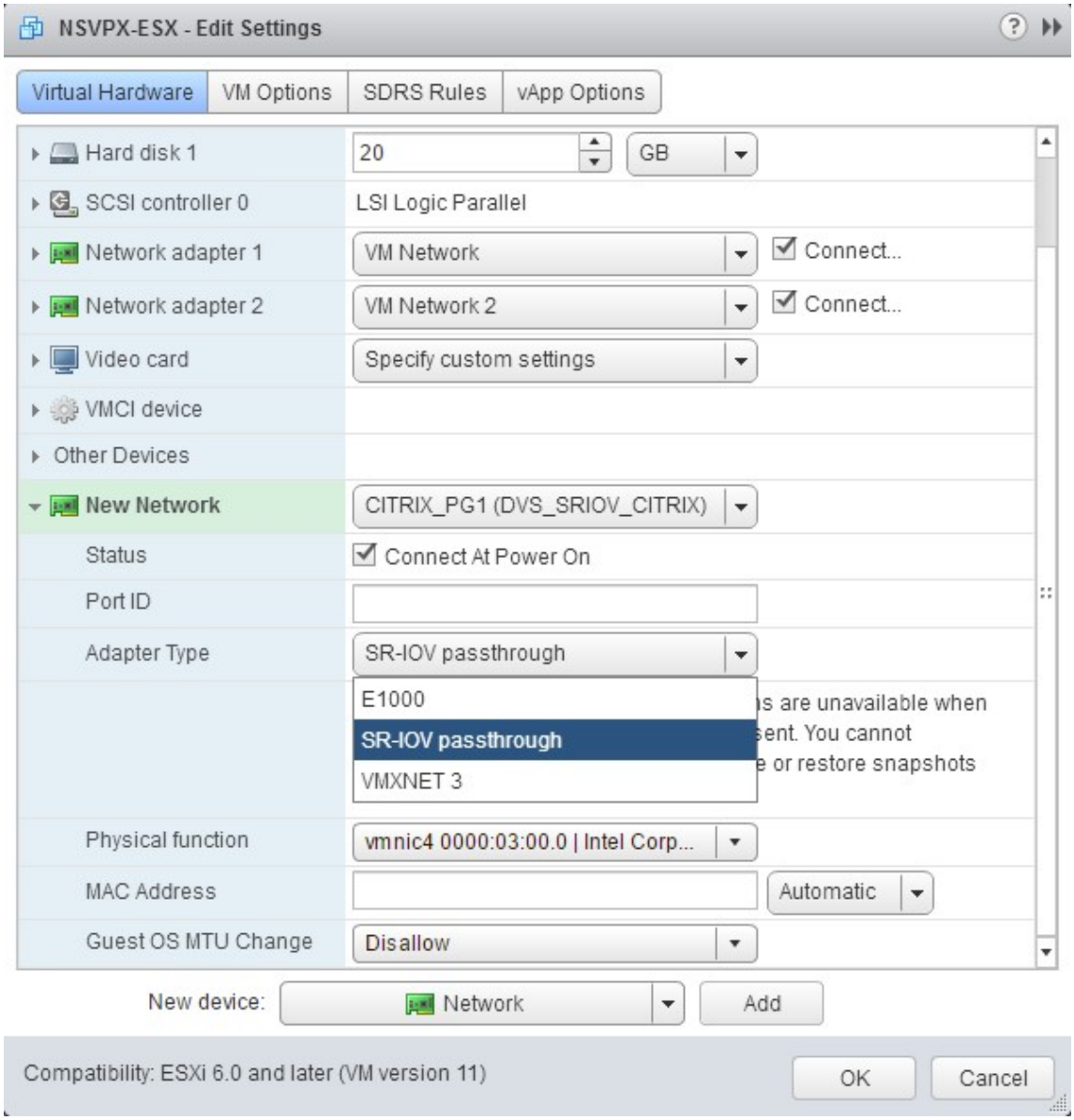


7. Ajouter une interface réseau SR-IOV. Dans la liste déroulante **Nouvel appareil**, sélectionnez **Réseau**, puis cliquez sur **Ajouter**.

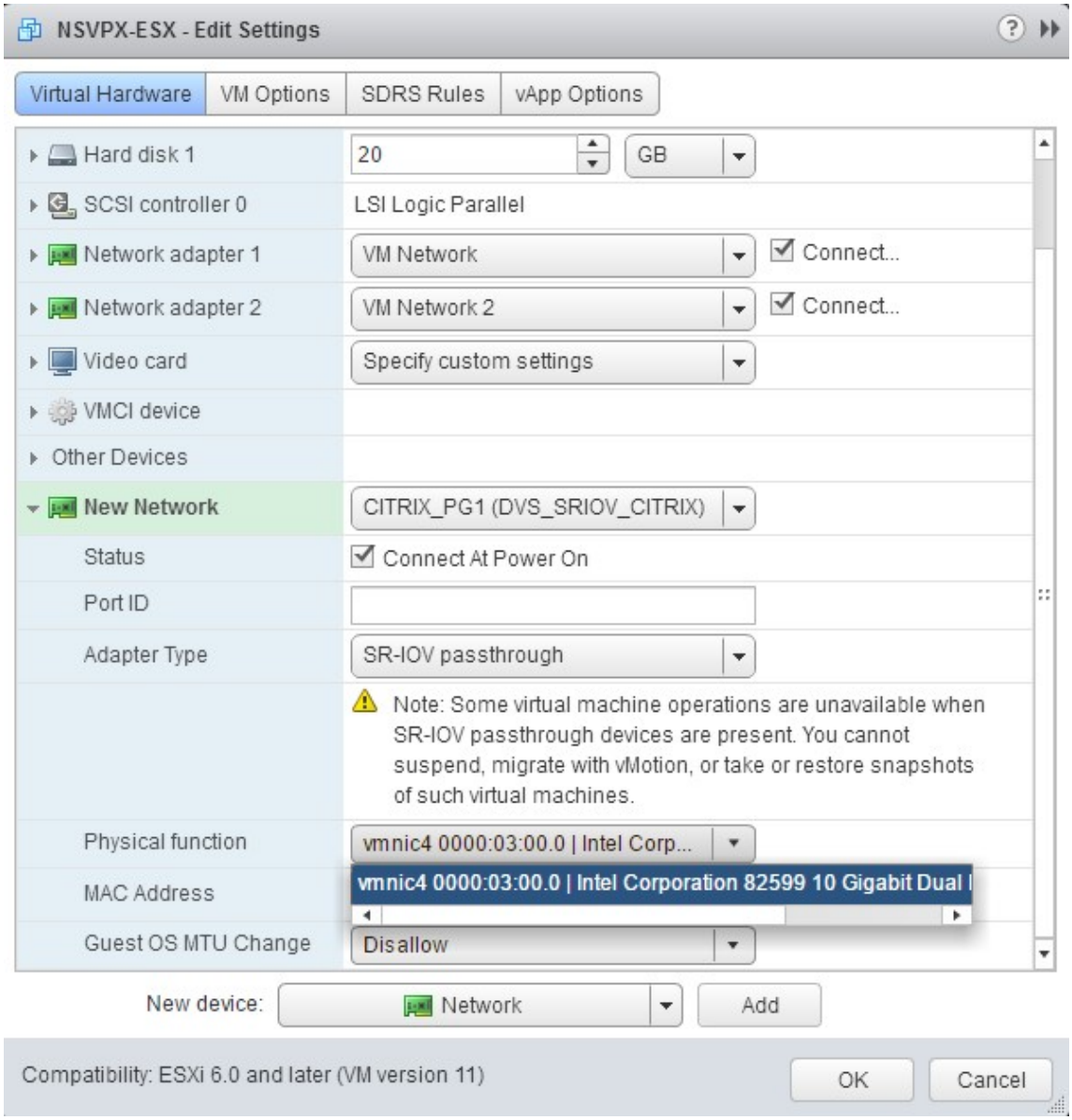


8. Dans la section **Nouveau réseau**. Dans la liste déroulante, sélectionnez celui `Portgroup` que vous avez créé, puis procédez comme suit :

   a. Dans la liste déroulante **Type d'adaptateur**, sélectionnez **Passthrough SR-IOV** .

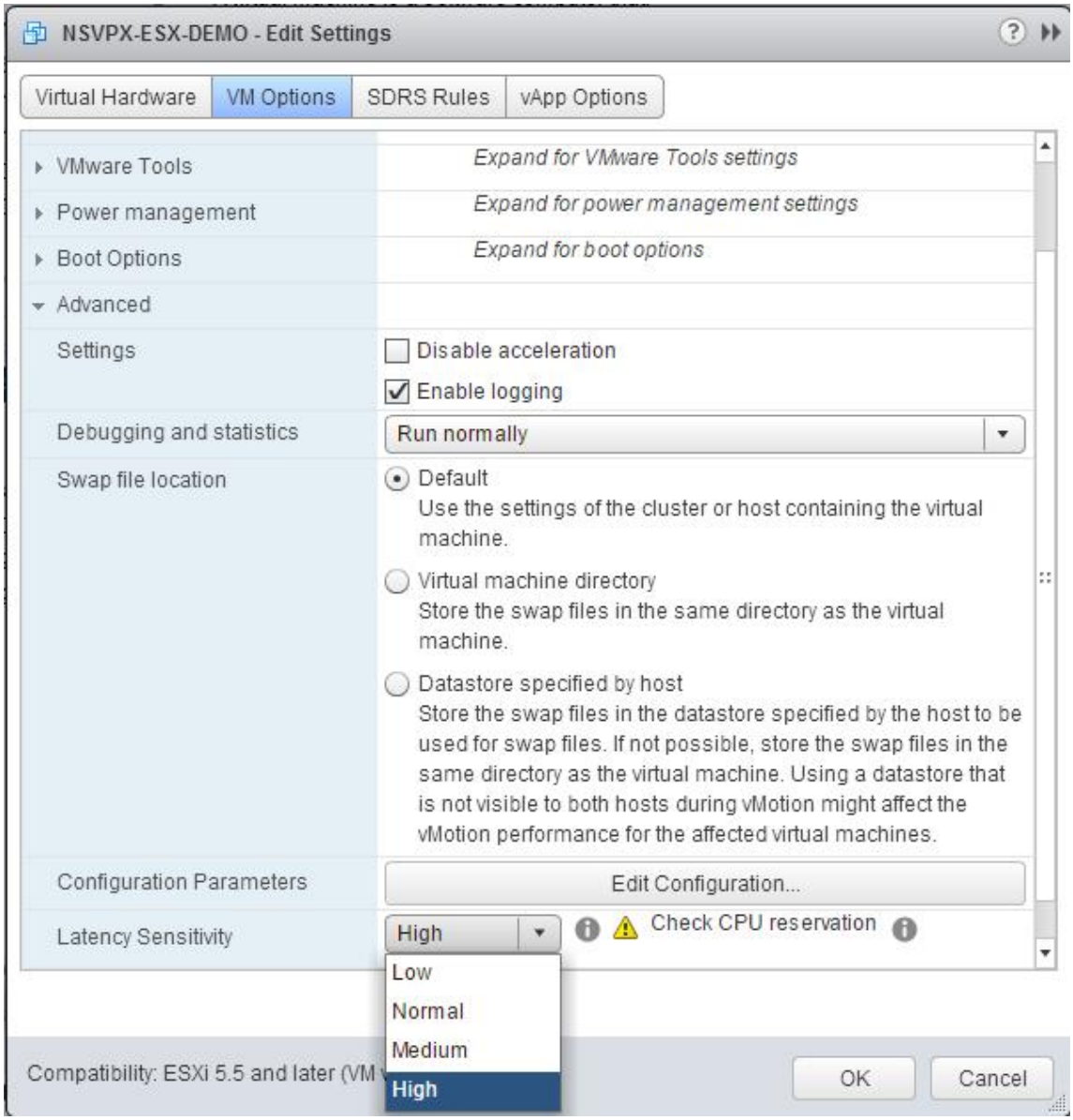


b. Dans la liste déroulante **Fonction physique**, sélectionnez l'adaptateur physique mappé avec le `Portgroup`.



c. Dans la liste déroulante **Guest OS MTU Change**, sélectionnez Interdire **.**

9. Dans la <virtual_appliance>boîte de dialogue **- Modifier les paramètres**, cliquez sur l'onglet **Options de la machine virtuelle** .
10. Dans l'onglet **Options de la machine virtuelle**, sélectionnez la section **Avancé** . Dans la liste déroulante **Sensibilité à la latence**, sélectionnez **Élevé** .



11. Cliquez sur **OK**.
12. Allumez l'instance NetScaler VPX.
13. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

    > Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
1   > show interface summary
2   ---------------------------------------------------------------------------------

3         Interface  MTU        MAC                Suffix
```



```
4   ----------------------------------------------------------------------------

5   1     0/1         1500        00:0c:29:1b:81:0b    NetScaler Virtual
       Interface
6   2     10/1        1500        00:50:56:9f:0c:6f    Intel 82599 10G VF
       Interface
7   3     10/2        1500        00:50:56:9f:5c:1e    Intel 82599 10G VF
       Interface
8   4     10/3        1500        00:50:56:9f:02:1b    Intel 82599 10G VF
       Interface
9   5     10/4        1500        00:50:56:9f:5a:1d    Intel 82599 10G VF
       Interface
10  6     10/5        1500        00:50:56:9f:4e:0b    Intel 82599 10G VF
       Interface
11  7     LO/1        1500        00:0c:29:1b:81:0b    Netscaler Loopback
       interface
12   Done
13  > show inter 10/1
14  1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15          flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16          MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17          Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18          LLDP Mode: NONE,                LR Priority: 1024
19
20          RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21          TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0)
               Stalls(0)
22          NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
               (0)
23          Bandwidth thresholds are not set.
24   Done
```

Configurer un hyperviseur NetScaler VPX sur ESX pour utiliser Intel QAT pour l'accélération SSL en mode SR-IOV

October 17, 2024

L'instance NetScaler VPX de l'hyperviseur VMware ESX peut utiliser la technologie Intel QuickAssist (QAT) pour accélérer les performances SSL de NetScaler. Grâce à Intel QAT, tous les traitements cryptographiques à latence élevée peuvent être déchargés sur la puce, libérant ainsi un ou plusieurs processeurs hôtes pour effectuer d'autres tâches.

Auparavant, tout le traitement cryptographique des chemins de données NetScaler était effectué dans le logiciel à l'aide de processeurs virtuels hôtes.

> **Remarque :**
>
> Actuellement, NetScaler VPX ne prend en charge que le modèle de puce C62x de la famille Intel QAT. Cette fonctionnalité est prise en charge à partir de la version 14.1 build 8.50 de NetScaler.

Conditions préalables

- L'hôte ESX est approvisionné avec une ou plusieurs puces Intel C62x (QAT).
- NetScaler VPX répond à la configuration matérielle requise pour VMware ESX. Pour plus d'informations, voir Installer une instance NetScaler VPX sur VMware ESX.

Limitations

Aucune disposition n'est prévue pour réserver des unités cryptographiques ou de la bande passante pour des machines virtuelles individuelles. Toutes les unités cryptographiques disponibles de tout matériel Intel QAT sont partagées entre toutes les machines virtuelles utilisant le matériel QAT.

Configuration de l'environnement hôte pour utiliser Intel QAT

1. Téléchargez et installez le pilote VMware fourni par Intel pour le modèle de puce de la série C62x (QAT) sur l'hôte VMware. Pour plus d'informations sur les téléchargements des packages Intel et les instructions d'installation, voir le pilote technologique Intel QuickAssist pour VMware.
2. Activez SR-IOV sur l'hôte ESX.
3. Créez des machines virtuelles. Lors de la création d'une machine virtuelle, attribuez le nombre approprié de périphériques PCI pour répondre aux exigences de performances.

> **Remarque :**
>
> Chaque puce C62x (QAT) peut comporter jusqu'à trois points de terminaison PCI distincts. Chaque point de terminaison est un ensemble logique de VF et partage la bande passante de manière égale avec les autres points de terminaison PCI de la puce. Chaque terminal peut avoir jusqu'à 16 VF qui apparaissent sous la forme de 16 périphériques PCI. Vous pouvez ajouter ces appareils à la machine virtuelle pour effectuer l'accélération cryptographique à l'aide de la puce QAT.

Points à noter

- Si l'exigence de chiffrement de la machine virtuelle est d'utiliser plusieurs points de terminaison ou puce PCI QAT, il est recommandé de sélectionner les périphériques PCI ou VF correspondants de manière circulaire afin d'obtenir une distribution symétrique.

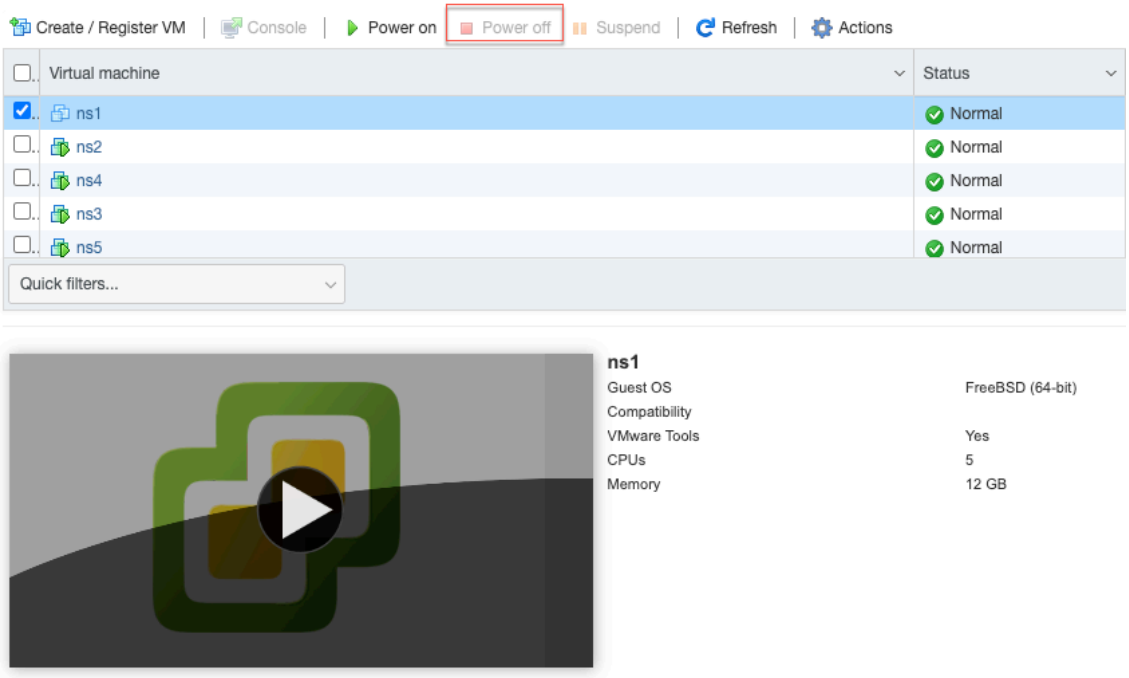
- Il est recommandé que le nombre de périphériques PCI sélectionnés soit égal au nombre de processeurs virtuels sous licence (sans inclure le nombre de processeurs virtuels de gestion). L'ajout d'un nombre de périphériques PCI supérieur au nombre de vCPU disponibles n'améliore pas nécessairement les performances.

  Exemple

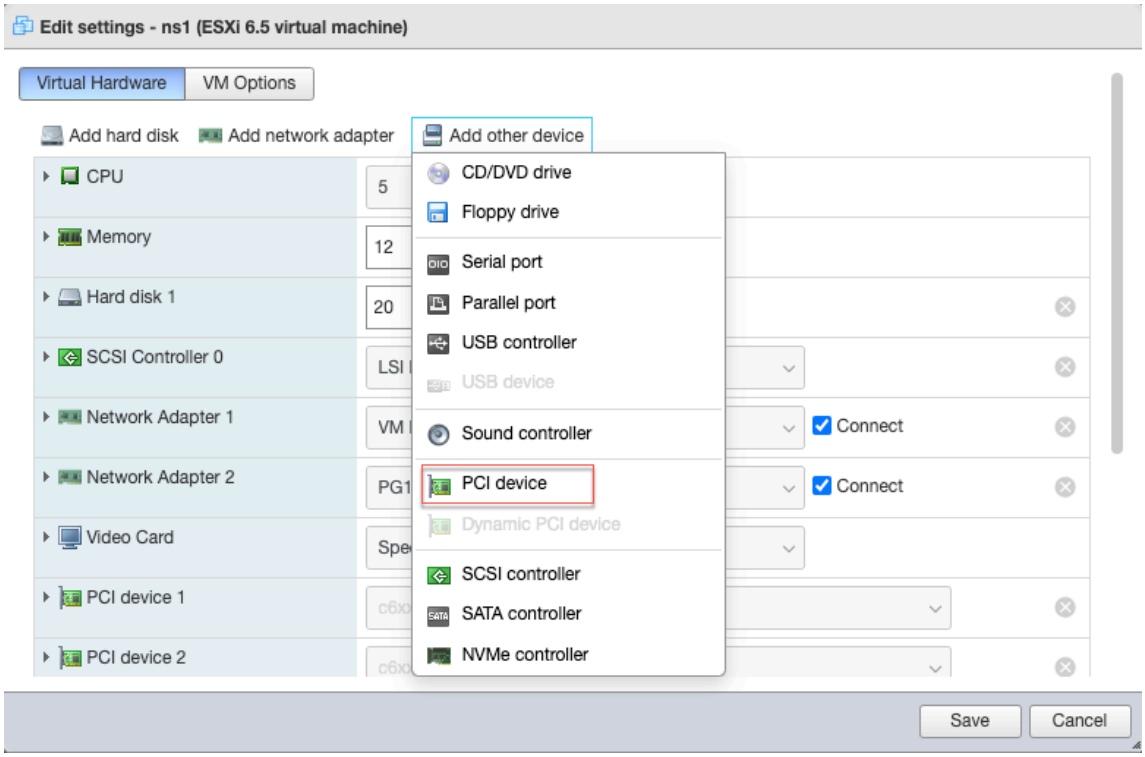
  Prenons l'exemple d'un hôte ESX doté d'une puce Intel C62x dotée de 3 terminaux. Lors du provisionnement d'une machine virtuelle avec 6 vCPU, choisissez 2 VF sur chaque point de terminaison et attribuez-les à la machine virtuelle. Ce type d'affectation garantit une distribution efficace et égale des unités cryptographiques pour la machine virtuelle. Parmi le total des vCPU disponibles, par défaut, un vCPU est réservé au plan de gestion, et les autres vCPU sont disponibles pour les PE du plan de données.

Attribuer des QAT VF à VPX à l'aide du client Web vSphere

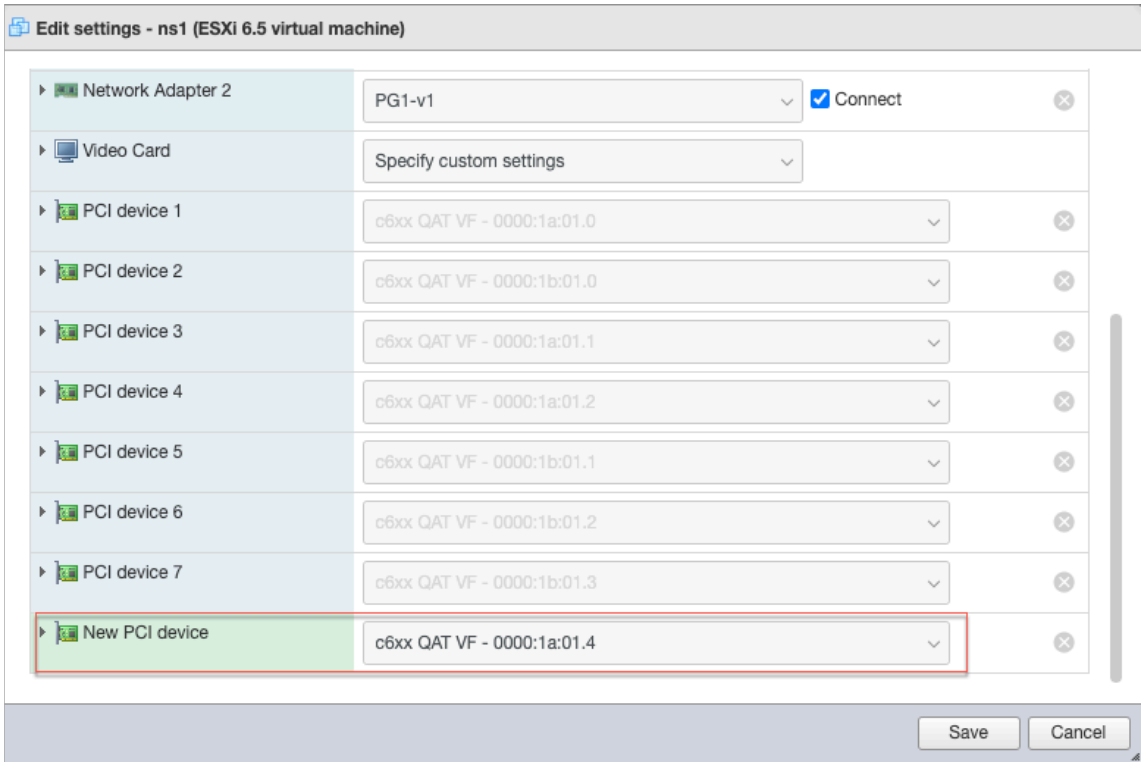
1. Dans le client Web vSphere, accédez à l'hôte ESX sur lequel se trouve la machine virtuelle et cliquez sur **Éteindre**.



2. Accédez à **Actions > Modifier les paramètres > Ajouter un autre périphérique**, puis sélectionnez un périphérique PCI.



3. Pour le périphérique PCI récemment ajouté, attribuez le c6xx QAT VF et enregistrez la configuration.



4. Allumez à nouveau la machine virtuelle.

5. Exécutez la commande `stat ssl` dans la CLI NetScaler pour afficher le résumé SSL et vérifiez les cartes SSL après avoir attribué des QAT VF à VPX.

À propos du déploiement

Ce déploiement a été testé avec les spécifications des composants suivantes :

- Version et version de**NetScaler VPX** : 14.1 à 8.50
- **Version de VMware ESXi : 7.0.3 (build** 20036589)
- **Version du pilote Intel C62x QAT pour VMware** : 1.5.1.54

Migration du NetScaler VPX de l'E1000 vers les interfaces réseau SR-IOV ou VMXNET3

October 17, 2024

24 mai 2018

Vous pouvez configurer vos instances NetScaler VPX existantes qui utilisent les interfaces réseau E1000 pour utiliser les interfaces réseau SR-IOV ou VMXNET3.

Pour configurer une instance NetScaler VPX existante pour utiliser les interfaces réseau SR-IOV, consultez Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV.

Pour configurer une instance NetScaler VPX existante pour utiliser les interfaces réseau VMXNET3, voir Configurer une instance NetScaler VPX pour utiliser l'interface réseau VMXNET3.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau PCI passthrough

October 17, 2024

Vue d'ensemble

Après avoir installé et configuré une instance NetScaler VPX sur VMware ESX Server, vous pouvez utiliser vSphere Web Client pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau PCI passthrough.

La fonction PCI passthrough permet à une machine virtuelle invitée d'accéder directement aux périphériques PCI et PCIe physiques connectés à un hôte.

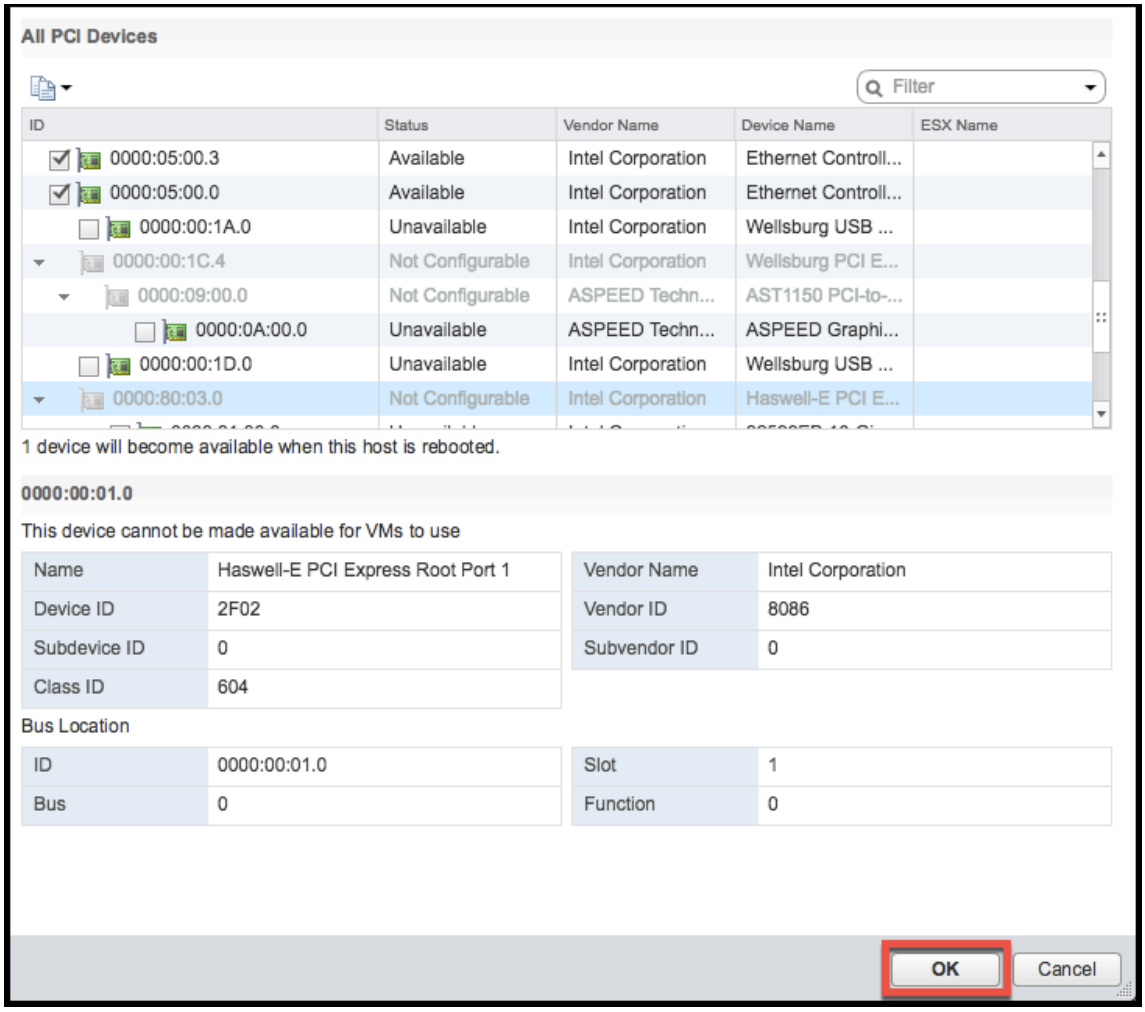
Conditions préalables

- La version du microprogramme de la carte réseau Intel XL710 sur l'hôte est 5.04.
- Périphérique PCI connecté à l'hôte et configuré sur celui-ci
- NIC prises en charge :
  - Carte réseau Intel X710 10G
  - Carte réseau Intel XL710 à deux ports 40G
  - Carte réseau Intel XL710 à port unique 40G
  - Carte réseau Intel XXV710 à deux ports 25G

Configurer les périphériques passthrough sur un hôte

Avant de configurer un périphérique PCI passthrough sur une machine virtuelle, vous devez le configurer sur la machine hôte. Procédez comme suit pour configurer les périphériques passthrough sur un hôte.

1. Sélectionnez l'hôte dans le panneau Navigateur de vSphere Web Client.
2. Cliquez sur **Gérer** > **Paramètres** > **Périphériques PCI** . Tous les périphériques passthrough disponibles s'affichent.
3. Cliquez avec le bouton droit sur le périphérique que vous souhaitez configurer, puis cliquez sur **Modifier**.
4. La fenêtre **Modifier la disponibilité des périphériques PCI** s'affiche.
5. Sélectionnez les périphériques à utiliser pour la transmission, puis cliquez sur **OK**.

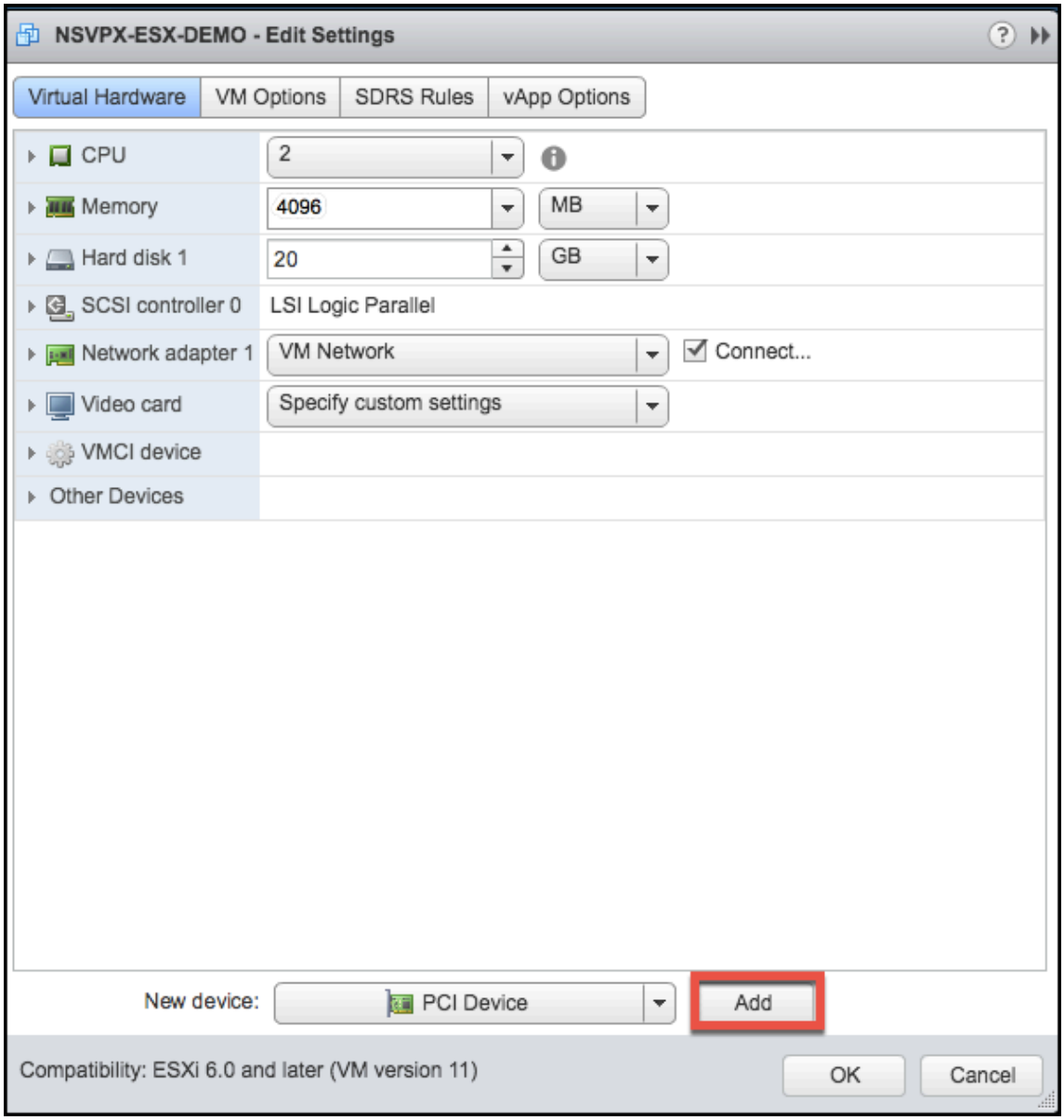


6. Redémarrez la machine hôte.

Configurer des appareils relais sur une instance NetScaler VPX

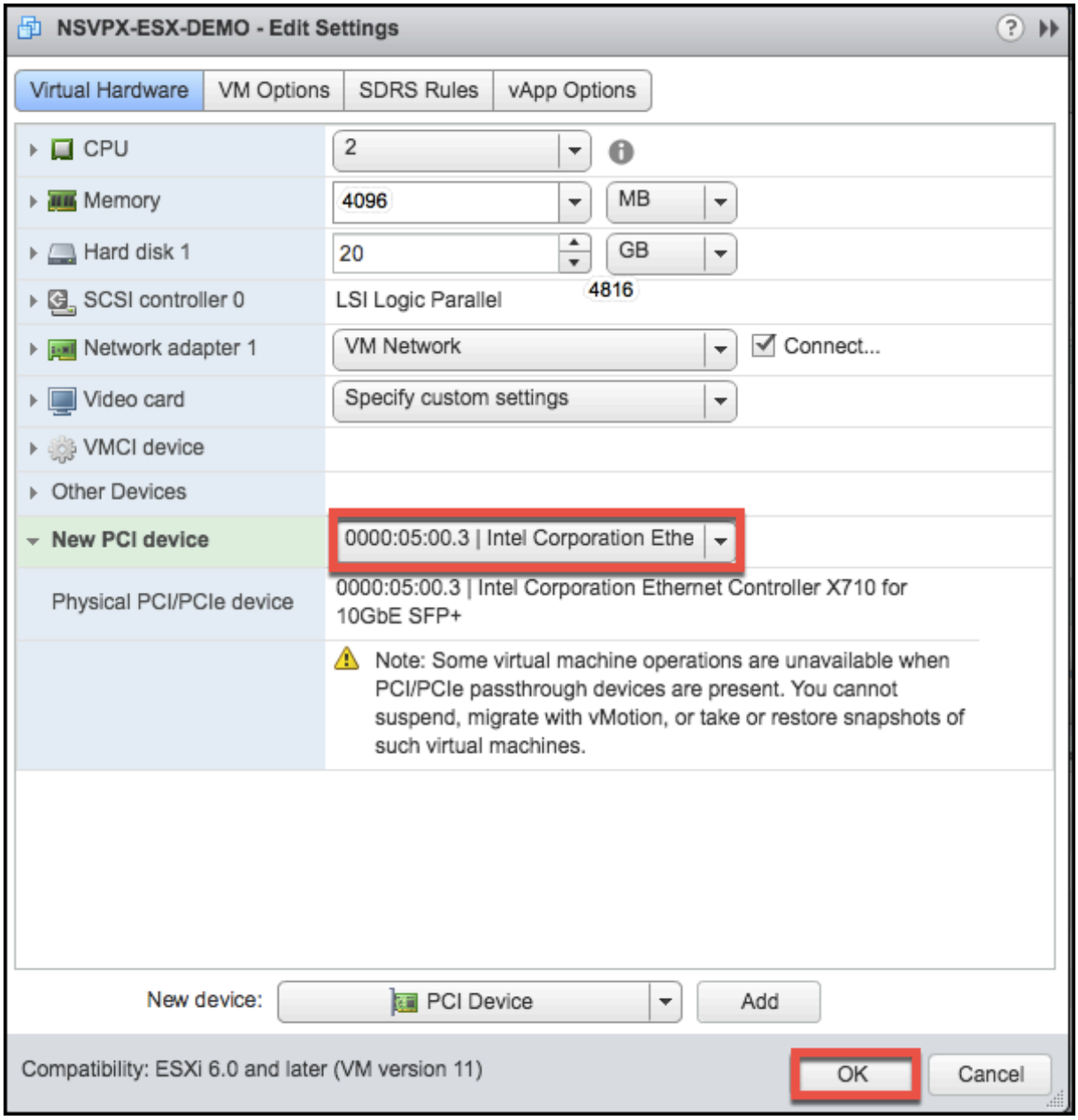
Suivez ces étapes pour configurer un périphérique PCI relais sur une instance NetScaler VPX.

1. Mettez hors tension la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Sous l'onglet **Matériel virtuel**, sélectionnez **Périphérique PCI** dans le menu déroulant **Nouveau périphérique**, puis cliquez sur **Ajouter** .



4. Développez **Nouveau périphérique PCI** et sélectionnez le périphérique de transmission à connecter à la machine virtuelle dans la liste déroulante, puis cliquez sur **OK** .

> **Remarque :**
>
> L'interface réseau VMXNET3 et l'interface réseau PCI ne peuvent pas coexister.



1. Mettez sous tension la machine virtuelle invitée.

Vous avez terminé les étapes de configuration de NetScaler VPX pour utiliser les interfaces réseau PCI passthrough.

Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX

October 17, 2024

Vous pouvez appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX. Therefore in certain cases, a specific setup or VPX instance is brought up in much lesser time.

Pour plus d'informations sur les données utilisateur avant le démarrage et leur format, voir Appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud.

> **Remarque :**
>
> To bootstrap using preboot user data in ESX, default gateway config must be passed in <NS-CONFIG> section. For more information on the content of the <NS-CONFIG> tag, see Sample-<NS-CONFIG>-section.

Sample <NS-CONFIG> section:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

How to provide preboot user data on ESX hypervisor

Vous pouvez fournir des données utilisateur avant le démarrage sur l'hyperviseur ESX à partir d'un client Web ou d'un client vSphere des deux manières suivantes :

- Using CD/DVD ISO
- Using OVF Property

Provide user data using CD/DVD ISO

Vous pouvez utiliser le client VMware vSphere pour injecter des données utilisateur dans la machine virtuelle sous forme d'image ISO à l'aide du lecteur de CD/DVD.

Pour fournir des données utilisateur à l'aide de l'ISO du CD/DVD, procédez comme suit :

1. Créez un fichier dont le nom contient `userdata` le contenu des données utilisateur avant le démarrage. For more information on the content of the `<NS-CONFIG>` tag, see Sample `<NS-CONFIG>` section.

   > **Remarque :**
   >
   > Le nom de fichier doit être strictement utilisé comme `userdata`.

2. Store the `userdata` file in a folder, and build an ISO image using the folder.

   You can build an ISO image with `userdata` file by the following two methods:

   - Using any image processing tool such as PowerISO.
   - Using `mkisofs` command in Linux.

   The following sample configuration shows how to generate an ISO image using the `mkisofs` command in Linux.

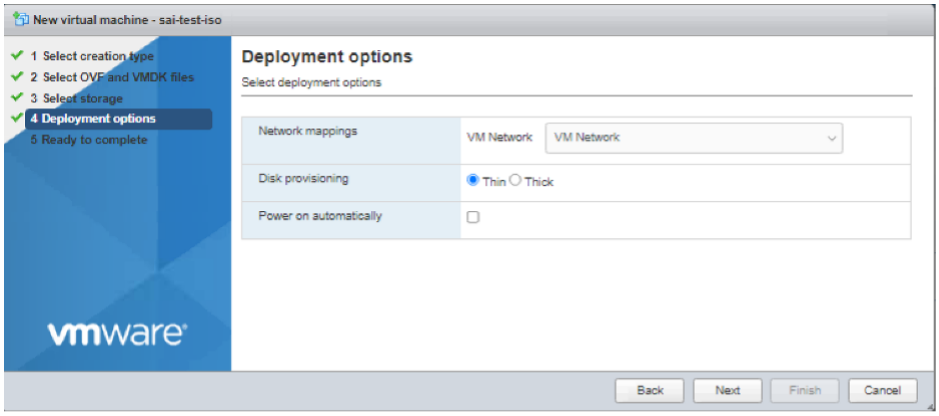
```
root@ubuntu:~/sai/14jul2021# ls -l total 4
drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
    ./esx_preboot_userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@ubuntu:~/sai/14jul2021# ls -lh
total 356K
drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.
    iso

root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
```

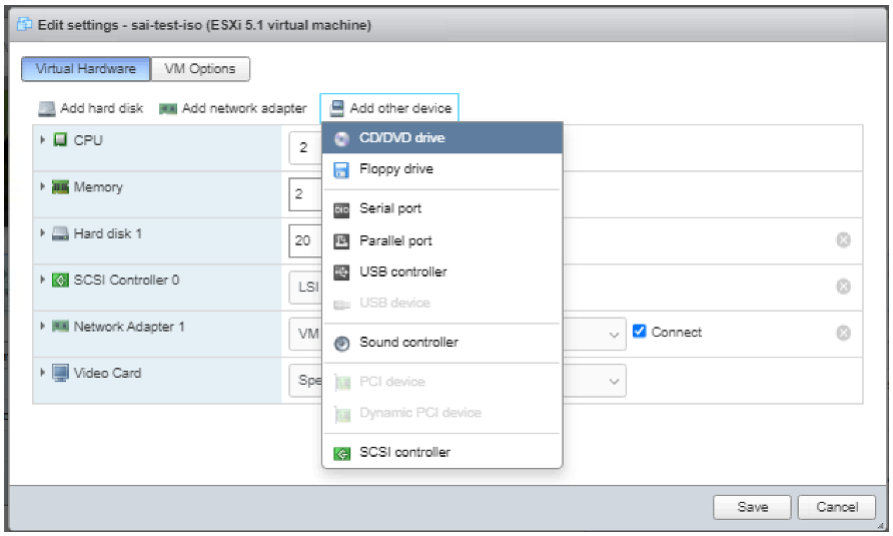


```
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
```

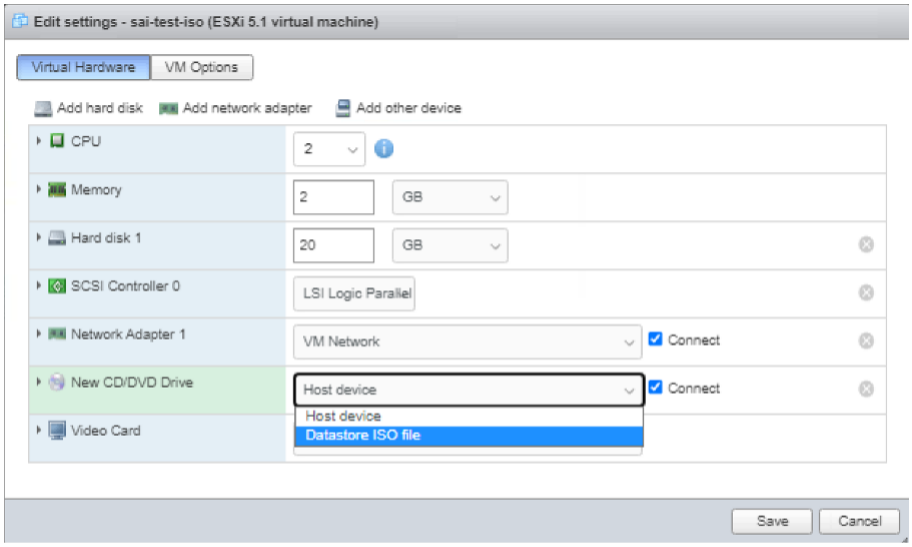
3. Provisionnez l'instance NetScaler VPX à l'aide du processus de déploiement standard pour créer la machine virtuelle. But do not power on the VM automatically.



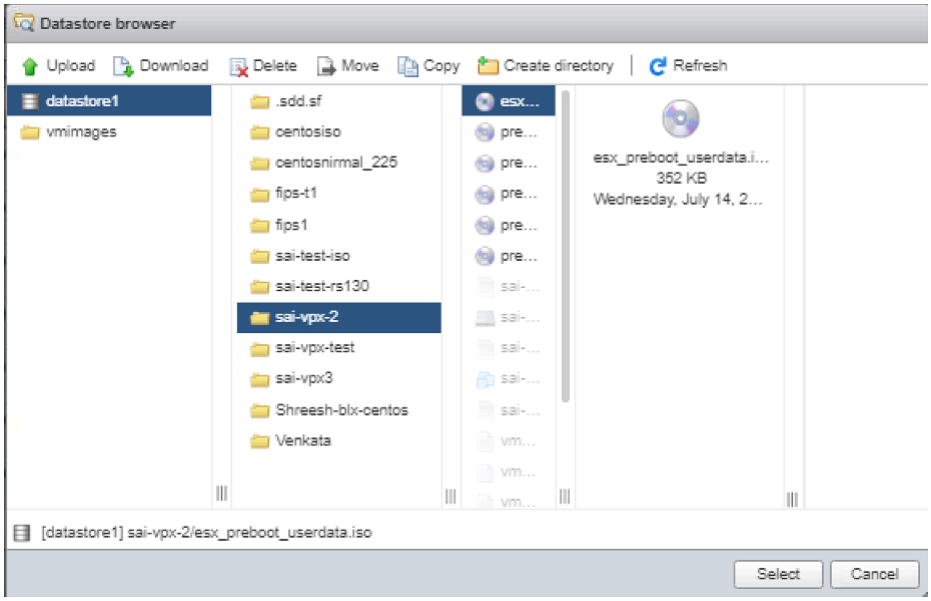
4. After the VM is successfully created, attach the ISO file as CD/DVD drive to the VM.



5. Navigate to **New CD/DVD Drive** and choose **Datastore ISO file** from the drop-down menu.



6. Select a Datastore in the vSphere Client.



7. Power on the VM.

Fourniture de données utilisateur à l'aide de la propriété OVF du client Web ESX

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

     ```
     base64 <userdata-filename>  >   <outuput-file>
     ```

     Exemple

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     ```

     ```
     root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
     PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
     U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - Use online tools to encode user data content, for example, Base64 Encode and Decode.

3. Incluez une section **Produit** dans le modèle OVF d'une instance NetScaler VPX sur l'hyperviseur ESX.

   Sample Product section:

   ```
   <ProductSection>

     <Info>Information about the installed software</Info>
     <Product>NSVPX-VSK Template</Product>
     <Vendor>Citrix</Vendor>
     <VendorUrl>www.citrix.com</VendorUrl>
     <Category> Preboot Userdata </Category>
   ```



```
8
9       <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
            userConfigurable="true" ovf:value="">
10
11        <Label>Userdata</Label>
12        <Description> Userdata for ESX VPX </Description>
13      </Property>
14
15    </ProductSection>
```

4. Provide the base64 encoded user data as the `ovf:value` for `guestinfo.userdata` property in the Product section.

```
1     <ProductSection>
2
3       <Info>Information about the installed software</Info>
4       <Product>NSVPX-VSK Template</Product>
5       <Vendor>Citrix</Vendor>
6       <VendorUrl>www.citrix.com</VendorUrl>
7       <Category> Preboot Userdata </Category>
8       <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
            userConfigurable="true"
9         ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
              CglhZGQgcm91dGUgMC4wLjAuMCAw
10        LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUk
11        ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC
12        U1RSQVA+
              CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1R
13        VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgIC
14        ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgIC
15        ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk
16        QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
              CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
17        RS1DT05GSUc+
              CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+
              Cg==">
18
19        <Label>Userdata</Label>
20        <Description> Userdata for ESX VPX </Description>
21      </Property>
22
23    </ProductSection>
```

5. Use the modified OVF template with Product section for the VM deployment.


```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----            ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP    Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP      0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP      0               DIREC
T
 Done
```

Fourniture de données utilisateur à l'aide de la propriété OVF du client ESX vSphere

Suivez ces étapes pour fournir des données utilisateur à l'aide de la propriété OVF du client ESX vSphere.

1. Create a file with user data content.

```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

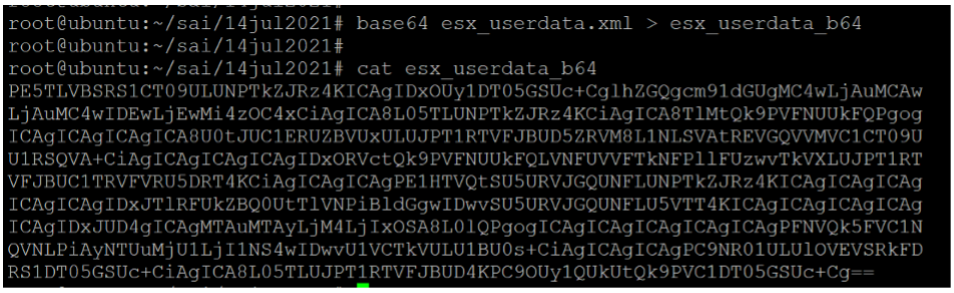
2. Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

     ```
     base64 <userdata-filename>  >  <outuput-file>
     ```

     Exemple


```
base64 esx_userdata.xml  > esx_userdata_b64
```



- Use online tools to encode user data content, for example, Base64 Encode and Decode.

3. Incluez une section **Produit** dans le modèle OVF d'une instance NetScaler VPX sur l'hyperviseur ESX.

   Sample Product section:

```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true" ovf:value="">

    <Label>Userdata</Label>
    <Description> Userdata for ESX VPX </Description>
  </Property>

</ProductSection>
```

4. Provide the base64 encoded user data as the `ovf:value` for `guestinfo.userdata` property in the Product section.

```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.Citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>
  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true"
    ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
       CglhZGQgcm91dGUgMC4wLjAuMCAw
    LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KICAgICA8TlMtQk9PVFNUUk
```



```
11        ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC
12        U1RSQVA+
             CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1R
13        VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgIC
14        ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgIC
15        ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk
16        QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
             CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
17        RS1DT05GSUc+
             CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+
             Cg==">
18
19        <Label>Userdata</Label>
20        <Description> Userdata for ESX VPX </Description>
21      </Property>
22
23    </ProductSection>
```

5. Ajoutez la propriété `ovf:transport="com.vmware.guestInfo"` à VirtualHardwareSection comme suit :

```
1    <VirtualHardwareSection  ovf:transport="com.vmware.guestInfo">
```

6. Use the modified OVF template with Product section for the VM deployment.

```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----             ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP     Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP      0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP      0               DIREC
T
 Done
```


Installation d'une instance NetScaler VPX sur le cloud VMware sur AWS

October 17, 2024

VMware Cloud (VMC) sur AWS vous permet de créer des centres de données définis par logiciel cloud (SDDC) sur AWS avec le nombre souhaité d'hôtes ESX. La VMC sur AWS prend en charge les déploiements NetScaler VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Un SDDC VMware doit être présent avec au moins un hôte.
- Téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau appropriés sur VMware SDDC auxquels les machines virtuelles se connectent.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez le *Guide de licence NetScaler VPX* à </en-us/licensing/licensing-guide-for-netscaler.html>.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> **Remarque :**
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration minimale requise.

Tableau 2. Tableau 2 Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-79.64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-79.64.mf)

Installation d'une instance NetScaler VPX sur le cloud VMware

Après avoir installé et configuré VMware SDDC, vous pouvez utiliser le SDDC pour installer des appliances virtuelles sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

Pour installer des instances NetScaler VPX sur le cloud VMware, procédez comme suit :

1. Ouvrez VMware SDDC sur votre station de travail.
2. Dans les zones de texte **Nom d'utilisateur** et **Mot** de passe, tapez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
3. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
4. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**

   > **Remarque :** Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000.

5. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **Suivant** pour démarrer l'installation d'une appliance virtuelle sur VMware SDDC.
6. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Console** pour émuler un port de console. Cliquez sur l'onglet **Console** pour émuler un port de console.
7. Si vous souhaitez installer un autre dispositif virtuel, répétez l'opération à partir de l'étape 6.
8. Spécifiez l'adresse IP de gestion du même segment que celui sélectionné pour être le réseau de gestion. Le même sous-réseau est utilisé pour la passerelle.
9. Le SDDC VMware exige que les règles NAT et pare-feu soient créées explicitement pour toutes les adresses IP privées appartenant à des segments réseau.

Installation d'une instance NetScaler VPX sur un serveur Microsoft Hyper-V

October 17, 2024

Pour installer des instances NetScaler VPX sur Microsoft Windows Server, vous devez d'abord installer Windows Server avec le rôle Hyper-V activé, sur un ordinateur disposant des ressources système adéquates. Lors de l'installation du rôle Hyper-V, assurez-vous de spécifier les cartes d'interface réseau sur le serveur qui sera utilisé par Hyper-V pour créer les réseaux virtuels. Vous pouvez réserver certaines cartes d'interface réseau pour l'hôte. Utilisez le gestionnaire Hyper-V pour effectuer l'installation de l'instance NetScaler VPX.

L'instance NetScaler VPX pour Hyper-V est fournie au format de disque dur virtuel (VHD). Il inclut la configuration par défaut pour des éléments tels que le CPU, les interfaces réseau, ainsi que la taille et le format du disque dur. Après avoir installé l'instance NetScaler VPX, vous pouvez configurer les adaptateurs réseau sur une appliance virtuelle, ajouter des cartes réseau virtuelles, puis attribuer l'adresse IP NetScaler, le masque de sous-réseau et la passerelle, et terminer la configuration de base de l'appliance virtuelle.

Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, voir Mettre à niveau une appliance autonome NetScalerVPX

> **Remarque :**
>
> Le protocole ISIS (Intermediate System-to-Intermediate System) n'est pas pris en charge sur l'appliance virtuelle NetScaler VPX hébergée sur la plateforme HyperV-2012.

Conditions préalables à l'installation de l'instance NetScaler VPX sur des serveurs Microsoft

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Activez le rôle Hyper-V sur les serveurs Windows. Pour plus d'informations, consultez http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Téléchargez les fichiers de configuration de l'appliance virtuelle.
- Obtenez les fichiers de licence des instances NetScaler VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez le *Guide des licences NetScaler ADC VPX* à l'adresse https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US.

Configuration matérielle requise pour les serveurs Microsoft

Le tableau suivant décrit la configuration minimale requise pour les serveurs Microsoft.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
UC	Processeur 64 bits 1,4 GHz
RAM	8 GB
Disk Space	32 Go ou plus

Le tableau suivant répertorie les ressources informatiques virtuelles pour chaque Instance NetScaler VPX.

Tableau 2. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
RAM	4 Go
CPU virtuel	2
Disk Space	20 Go
Interfaces réseau virtuelles	1

Téléchargez les fichiers de configuration de NetScaler VPX

L'instance NetScaler VPX pour Hyper-V est fournie au format de disque dur virtuel (VHD). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com, cliquez sur **Connexion > Mon compte > Créer un compte Citrix**, puis suivez les instructions pour créer un compte Citrix.

Pour télécharger les fichiers de configuration de l'instance NetScaler VPX, procédez comme suit :

1. Depuis un navigateur Web, accédez à http://www.citrix.com/.
2. Connectez-vous avec votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Téléchargements**.

4. Dans le menu déroulant **Sélectionner un produit**, sélectionnez **NetScaler (NetScaler**ADC).
5. Sous **NetScaler Release X.X > Appliances virtuelles**, cliquez sur **NetScaler**VPX Release X.X
6. Téléchargez le fichier compressé sur votre serveur.

Installation de l'instance NetScaler VPX sur les serveurs Microsoft

Après avoir activé le rôle Hyper-V sur Microsoft Server et extrait les fichiers du dispositif virtuel, vous pouvez utiliser le gestionnaire Hyper-V pour installer l'instance NetScaler VPX. Après avoir importé la machine virtuelle, vous devez configurer les cartes réseau virtuelles en les associant aux réseaux virtuels créés par Hyper-V.

Vous pouvez configurer un maximum de huit cartes réseau virtuelles. Même si la carte réseau physique est hors service, l'appliance virtuelle suppose que la carte réseau virtuelle est active, car elle peut toujours communiquer avec les autres dispositifs virtuels sur le même hôte (serveur).

> **Remarque :**
>
> Vous ne pouvez modifier aucun paramètre pendant que l'appliance virtuelle est en cours d'exécution. Arrêtez l'appliance virtuelle, puis apportez des modifications.

Pour installer une instance NetScaler VPX sur Microsoft Server à l'aide du gestionnaire Hyper-V :

1. Pour démarrer Hyper-V Manager, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le volet de navigation, sous **Hyper-V Manage**r, sélectionnez le serveur sur lequel vous souhaitez installer l'instance NetScaler VPX.
3. Dans le menu **Action**, cliquez sur **Importer une machine virtuelle**.
4. Dans la boîte de dialogue **Importer une machine virtuelle**, dans **Emplacement**, spécifiez le chemin du dossier contenant les fichiers logiciels de l'instance NetScaler VPX, puis **sélectionnez Copier la machine virtuelle (créez un**nouvel identifiant unique). Ce dossier est le dossier parent qui contient les dossiers Snapshots, Virtual Hard Disks et Virtual Machines.

> **Remarque :**
>
> Si vous avez reçu un fichier compressé, assurez-vous d'extraire les fichiers dans un dossier avant de spécifier le chemin d'accès au dossier.

1. Cliquez sur **Importer**.
2. Vérifiez que le dispositif virtuel que vous avez importé est répertorié sous **Machines virtuelles**.
3. Pour installer un autre dispositif virtuel, répétez les étapes **2** à **6**.

> **Important :**
>
> Assurez-vous d'extraire les fichiers vers un autre dossier à l'étape **4**.

Provisionner automatiquement une instance NetScaler VPX sur Hyper-V

Le provisionnement automatique de l'instance NetScaler VPX est facultatif. Si le provisionnement automatique n'est pas effectué, l'appliance virtuelle propose une option permettant de configurer l'adresse IP, etc.

Pour provisionner automatiquement une instance NetScaler VPX sur Hyper-V, procédez comme suit.

1. Créez une image ISO conforme à la norme ISO9660 à l'aide du fichier XML, comme illustré dans l'exemple. Assurez-vous que le nom du fichier XML est **userdata**.

   Vous pouvez créer un fichier ISO à partir d'un fichier XML en utilisant :

   • Tout outil de traitement d'image tel que PowerISO.

   • `mkisofs` commande sous Linux.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment
    /1`"

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""

xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
    1.0"/>

```



```
27    <Property oe:key="com.citrix.netscaler.platform" oe:value="
          NS1000V"/>
28
29    <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="
          cisco-orch-env"/>
30
31    <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
          10.102.100.122"/>
32
33    <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
          255.255.255.128"/>
34
35    <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
          10.102.100.67"/></PropertySection>
36
37    </Environment>
```

2. Copiez l'image ISO sur le serveur Hyper-V.
3. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**. Vous pouvez également sélectionner l'appliance virtuelle, puis cliquer avec le bouton droit de la souris et sélectionner **Paramètres**. La fenêtre **Paramètres** de l'appliance virtuelle sélectionnée s'affiche.
4. Dans la fenêtre **Paramètres**, sous la section Matériel, cliquez sur **Contrôleur IDE** .
5. Dans le volet de droite, sélectionnez **Lecteur DVD** et cliquez sur **Ajouter**. Le lecteur DVD est ajouté dans la section **IDE Controller** dans le volet gauche de la fenêtre.
6. Sélectionnez le **lecteur DVD** ajouté à l'étape 5. Dans le volet droit de la fenêtre, sélectionnez le bouton **radio Fichier image**, cliquez sur **Parcourir** et sélectionnez l'image ISO que vous avez copiée sur le serveur Hyper-V, à l'étape 2.
7. Cliquez sur **Appliquer**.

> **Remarque :**
>
> L'instance d'appliance virtuelle apparaît à l'adresse IP par défaut, lorsque :

- Le lecteur de DVD est joint et le fichier ISO n'est pas fourni.
- Le fichier ISO n'inclut pas le fichier de données utilisateur.
- Le nom ou le format du fichier de données utilisateur n'est pas correct.

Pour configurer des cartes réseau virtuelles sur l'instance NetScaler VPX, procédez comme suit :

1. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**.
2. Dans la boîte de dialogue **Paramètres pour <virtual appliance name>**, cliquez sur **Ajouter du matériel** dans le volet gauche.
3. Dans le volet droit, dans la liste des appareils, sélectionnez **Adaptateur réseau**.

4. Cliquez sur **Ajouter**.
5. Vérifiez que **l'adaptateur réseau (non connecté)** apparaît dans le volet de gauche.
6. Sélectionnez l'adaptateur réseau dans le volet de gauche.
7. Dans le volet droit, dans le menu **Réseau**, sélectionnez le réseau virtuel auquel connecter la carte.
8. Pour sélectionner le réseau virtuel pour les autres adaptateurs réseau que vous souhaitez utiliser, répétez les étapes **6** et **7**.
9. Cliquez sur **Appliquer**, puis sur **OK**.

Pour configurer l'instance NetScaler VPX :

1. Cliquez avec le bouton droit sur l'appliance virtuelle que vous avez précédemment installée, puis sélectionnez **Démarrer**.
2. Accédez à la console en double-cliquant sur l'appliance virtuelle.
3. Tapez l'adresse IP NetScaler, le masque de sous-réseau et la passerelle de votre appliance virtuelle.

Vous avez terminé la configuration de base de votre appliance virtuelle. Entrez l'adresse IP dans un navigateur Web pour accéder à l'appliance virtuelle.

> **Remarque :**
>
> Vous pouvez également utiliser un modèle de machine virtuelle (VM) pour provisionner une instance NetScaler VPX à l'aide de SCVMM.
>
> Si vous utilisez la solution d'association de cartes réseau Microsoft Hyper-V avec des instances NetScaler VPX, consultez l'article CTX224494 pour plus d'informations.

Installation d'une instance NetScaler VPX sur la plateforme Linux-KVM

October 17, 2024

Pour configurer un NetScaler VPX pour la plate-forme Linux-KVM, vous pouvez utiliser l'application graphique Virtual Machine Manager (Virtual Manager). Si vous préférez la ligne de commande Linux-KVM, vous pouvez utiliser le `virsh` programme.

Le système d'exploitation Linux hôte doit être installé sur du matériel approprié à l'aide d'outils de virtualisation tels que le module KVM et QEMU. Le nombre de machines virtuelles pouvant être déployées sur l'Hypervisor dépend des besoins de l'application et du matériel choisi.

Après avoir provisionné une instance NetScaler VPX, vous pouvez ajouter d'autres interfaces.

Limitations et directives d'utilisation

Recommandations générales

Pour éviter tout comportement imprévisible, appliquez les recommandations suivantes :

- Ne modifiez pas le MTU de l'interface VNet associée à la machine virtuelle VPX. Arrêtez la machine virtuelle VPX avant de modifier les paramètres de configuration, tels que les modes d'interface ou le processeur.
- Ne forcez pas l'arrêt de la machine virtuelle VPX. Autrement dit, n'utilisez pas la commande **Force off** .
- Toutes les configurations effectuées sur l'hôte Linux peuvent ou non être persistantes, en fonction de vos paramètres de distribution Linux. Vous pouvez choisir de rendre ces configurations persistantes afin d'assurer un comportement cohérent lors des redémarrages du système d'exploitation Linux hôte.
- Le package NetScaler doit être unique pour chacune des instances NetScaler VPX provisionnées.

Limitations

- La migration en direct d'une instance VPX exécutée sur KVM n'est pas prise en charge.

Conditions préalables à l'installation d'une instance NetScaler VPX sur une plateforme Linux-KVM

October 17, 2024

Vérifiez la configuration minimale requise pour un serveur Linux-KVM s'exécutant sur une instance NetScaler VPX.

Exigence du processeur :

- Processeurs x86 64 bits dotés de la fonctionnalité de virtualisation matérielle incluse dans les processeurs Intel VT-X.

Pour vérifier si votre processeur prend en charge l'hôte Linux, entrez la commande suivante à l'invite de commandes Linux de l'hôte :

```
1   *.egrep '^flags.*(vmx|svm)' /proc/cpuinfo*
```

Si les paramètres du **BIOS** de l'extension précédente sont désactivés, vous devez les activer dans le BIOS.

- Fournir au moins 2 cœurs CPU à Host Linux.
- Il n'y a pas de recommandation spécifique pour la vitesse du processeur, mais plus la vitesse est élevée, meilleures sont les performances de l'application VM.

Mémoire requise (RAM) :

Minimum 4 Go pour le noyau Linux hôte. Ajoutez davantage de mémoire selon les besoins des machines virtuelles.

Disque dur requis :

Calculez l'espace requis pour le noyau Host Linux et les machines virtuelles. Une seule machine virtuelle NetScaler VPX nécessite 20 Go d'espace disque.

Configuration logicielle requise

Le noyau hôte utilisé doit être un noyau Linux 64 bits, version 2.6.20 ou ultérieure, avec tous les outils de virtualisation. Citrix recommande des noyaux plus récents, tels que 3.6.11-4 et versions ultérieures.

De nombreuses distributions Linux telles que Red Hat, CentOS et Fedora ont testé les versions du noyau et les outils de virtualisation associés.

Configuration matérielle requise pour les machines virtuelles invitées

NetScaler VPX prend en charge les types de disque dur IDE et VirtIO. Le type de disque dur a été configuré dans le fichier XML, qui fait partie du package NetScaler.

Exigences de mise en réseau

NetScaler VPX prend en charge les interfaces réseau VirtIO para-virtualisées, SR-IOV et PCI Passthrough.

Pour plus d'informations sur les interfaces réseau prises en charge, voir :

- Provisionnez l'instance NetScaler VPX à l'aide du Virtual Machine Manager
- Configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV
- Configurer une instance NetScaler VPX pour utiliser des interfaces réseau PCI passthrough

Interface source et modes

Le type de périphérique source peut être Bridge ou MacVTap. Dans MacVTAP, quatre modes sont possibles : VEPA, Bridge, Private et Pass-Through. Vérifiez les types d'interfaces que vous pouvez utiliser et les types de trafic pris en charge, comme suit :

Pont :

- Pont Linux.
- `Ebtables` et `iptables` les paramètres sur l'hôte Linux peuvent filtrer le trafic sur le pont si vous ne choisissez pas le bon paramètre ou si vous ne désactivez pas les `IPtable` services.

MacVTap (mode VEPA) :

- Meilleure performance qu'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- Communication inter-VM utilisant la même
- l'appareil inférieur n'est possible que si le commutateur en amont ou en aval prend en charge le mode VEPA.

MacVTap (mode privé) :

- Meilleure performance qu'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- La communication inter-VM utilisant le même périphérique inférieur n'est pas possible.

MacVTap (mode pont) :

- Meilleur comparativement au pont.
- Les interfaces situées sur le même appareil inférieur peuvent être partagées entre les machines virtuelles.
- La communication entre machines virtuelles utilisant le même périphérique inférieur est possible si la liaison inférieure du périphérique est UP.

MacVTap (mode Pass-through) :

- Meilleur comparativement au pont.
- Les interfaces hors du même appareil inférieur ne peuvent pas être partagées entre les machines virtuelles.
- Une seule machine virtuelle peut utiliser le périphérique inférieur.

> **Remarque :**
>
> Pour des performances optimales de l'instance VPX, assurez-vous que les capacités `gro` et `lro` sont désactivées sur les interfaces sources.

Propriétés des interfaces source

Assurez-vous de désactiver les fonctions generic-receve-offload (`gro`) et large receve-offload (`lro`) des interfaces source. Pour désactiver les `lro` fonctionnalités `gro` et, exécutez les commandes suivantes à l'invite du shell Linux hôte.

`ethtool -K eth6 gro désactivé ethool -K eth6 lro désactivé`

Exemple :

```
[root@localhost ~]# ethtool -K eth6

                    Offload parameters for eth6:

                                        rx-checksumming: on

                                        tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

[root@localhost ~]#
```

Exemple :

Si le pont Linux hôte est utilisé comme périphérique source, comme dans l'exemple suivant, et que les `lro` fonctionnalités doivent être désactivées sur les interfaces VNet, qui sont les interfaces virtuelles connectant l'hôte aux machines virtuelles invitées.


```
[root@localhost ~]# brctl show eth6_br

bridge name     bridge  id               STP enabled interfaces

eth6_br         8000.00e0ed1861ae          no         eth6

                                                      vnet0

                                                      vnet2

[root@localhost ~]#
```

Dans l'exemple précédent, les deux interfaces virtuelles sont dérivées de eth6_br et sont représentées par vnet0 et vnet2. Exécutez les commandes suivantes pour désactiver `gro` et désactiver `lro` les fonctionnalités de ces interfaces.

```
ethtool -K vnet0 gro off
        ethtool -K vnet2 gro off
        ethtool -K vnet0 lro off
                 ethtool -K vnet2 lro off
```

Mode promiscuité

Le mode promiscuous doit être activé pour que les fonctionnalités suivantes fonctionnent :

- Mode L2
- Traitement du trafic multidiffusion
- Diffuser
- Trafic IPV6
- MAC virtuel
- Routage dynamique

Utilisez la commande suivante pour activer le mode promiscuité.

```
[root@localhost ~]# ifconfig eth6 promisc
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
           inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
           UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric
               :1
           RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2895843 errors:0 dropped:0 overruns:0 carrier
               :0
           collisions:0 txqueuelen:1000
           RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
```


Module requis

Pour de meilleures performances réseau, assurez-vous que le module vhost_net est présent dans l'hôte Linux. Pour vérifier l'existence du module vhost_net, exécutez la commande suivante sur l'hôte Linux :

```
lsmod | grep "vhost\_net"
```

Si vhost_net n'est pas encore en cours d'exécution, entrez la commande suivante pour l'exécuter :

```
modprobe vhost\_net
```

Provisionner l'instance NetScaler VPX à l'aide d'OpenStack

October 17, 2024

Vous pouvez provisionner une instance NetScaler VPX dans un environnement OpenStack à l'aide de la commande **Nova boot** (OpenStack CLI) ou d'Horizon (tableau de bord OpenStack).

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se fixe à l'instance en tant que périphérique de CD-ROM lorsqu'il démarre. Ce lecteur de configuration peut être utilisé pour transmettre la configuration réseau telle que l'adresse IP de gestion, le masque réseau, la Gateway par défaut et pour injecter des scripts client.

Dans une appliance NetScaler, le mécanisme d'authentification par défaut est basé sur un mot de passe. Le mécanisme d'authentification par paire de clés SSH est désormais pris en charge pour les instances NetScaler VPX dans l'environnement OpenStack.

La paire de clés (clé publique et clé privée) est générée avant d'utiliser le mécanisme de cryptographie à clé publique. Vous pouvez utiliser différents mécanismes, tels que Horizon, Puttygen.exe pour Windows et `ssh-keygen` pour l'environnement Linux, pour générer la paire de clés. Reportez-vous à la documentation en ligne des mécanismes respectifs pour plus d'informations sur la génération de paires de clés.

Une fois qu'une paire de clés est disponible, copiez la clé privée dans un emplacement sécurisé auquel les personnes autorisées ont accès. Dans OpenStack, la clé publique peut être déployée sur une instance VPX à l'aide de la commande Horizon ou Nova boot. Lorsqu'une instance VPX est provisionnée à l'aide d'OpenStack, elle détecte d'abord que l'instance démarre dans un environnement OpenStack en lisant une chaîne BIOS spécifique. Cette chaîne est « OpenStack Foundation » et pour les distributions Red Hat Linux, elle est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plateforme d'hyperviseur KVM. Le disque doit comporter une étiquette OpenStack spécifique.

Si le lecteur de configuration est détecté, l'instance tente de lire la configuration réseau, les scripts personnalisés et la paire de clés SSH si elle est fournie.

Fichier de données utilisateur

L'instance NetScaler VPX utilise un fichier OVF personnalisé, également appelé fichier de données utilisateur, pour injecter la configuration réseau et des scripts personnalisés. Ce fichier est fourni dans le cadre du lecteur de configuration. Voici un exemple de fichier OVF personnalisé.

```
```
  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
  <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  oe:id=""
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:cs="http://schemas.citrix.com/openstack">
  <PlatformSection>
  <Kind></Kind>
  <Version>2016.1</Version>
  <Vendor>VPX</Vendor>
  <Locale>en</Locale>
  </PlatformSection>
  <PropertySection>
  <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
  <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
  <Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
     orch-env"/>
  <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
     />
  <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
     255.255.255.0"/>
  <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
     10.1.2.1"/>
  </PropertySection>
   <cs:ScriptSection>
     <cs:Version>1.0</cs:Version>
       <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack
          " xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
           <Scripts>
             <Script>
                   <Type>shell</Type>
                   <Parameter>X Y</Parameter>
                  <Parameter>Z</Parameter>
                  <BootScript>before</BootScript>
                    <Text>
                          #!/bin/bash
                          echo "Hi, how are you" $1 $2 >> /var/sample.
                             txt
                    </Text>
             </Script>
             <Script>
```

 
```

```
                    <Type>python</Type>
                    <BootScript>after</BootScript>
                     <Text>
                          #!/bin/python
    print("Hello");
                     </Text>
               </Script>
      <Script>
                    <Type>perl</Type>
                    <BootScript>before</BootScript>
                     <Text>
                          !/usr/bin/perl
    my $name = "VPX";
    print "Hello, World $name !\n" ;
                     </Text>
               </Script>
               <Script>
                    <Type>nscli</Type>
                    <BootScript>after</BootScript>
                    <Text>
                     add vlan 33
    bind vlan 33 -ifnum 1/2
                    </Text>
               </Script>
            </Scripts>
        </ScriptSettingSection>
    </cs:ScriptSection>
  </Environment>
``` Dans le fichier OVF qui précède, « PropertySection » est utilisé pour la configuration réseau de NetScaler tandis que \ <cs:ScriptSection\> est utilisé pour inclure tous les scripts. Les balises <Scripts\> \ \ </Scripts\> sont utilisées pour regrouper tous les scripts. Chaque script est défini entre des balises <Script\\> \ \ </Script\>. Chaque balise de script comporte les champs/balises suivants :
```

a) \ <Type> : Spécifie la valeur du type de script. Valeurs possibles : Shell/Perl/Python/NSLCI (pour les scripts CLI NetScaler)

b) \ <Parameter> : Fournit des paramètres au script. Chaque script peut comporter plusieurs \ <Parameter> tags.

c) \ <BootScript> : Spécifie le point d'exécution du script. Valeurs possibles pour cette balise : avant/après. « avant » indique que le script est exécuté avant l'apparition de PE. « after » indique que le script sera exécuté après l'arrivée de PE.

d) \ <Text> : Colle le contenu d'un script.

> **Remarque :**
>
> Actuellement, l'instance VPX ne prend pas en charge la désinfection des scripts. En tant qu'ad-


```

> ministrateur, vous devez vérifier la validité du script.
>
> Toutes les sections ne doivent pas être présentes. Utilisez une « PropertySection » vide pour définir uniquement les scripts à exécuter au premier démarrage ou une fenêtre vide
>
> Une fois que les sections requises du fichier OVF (fichier de données utilisateur) sont remplies, utilisez ce fichier pour provisionner l'instance VPX.

### Configuration réseau

Dans le cadre de la configuration réseau, l'instance VPX lit :

- Adresse IP de gestion
- Masque réseau
- Gateway par défaut

Une fois les paramètres lus avec succès, ils sont renseignés dans la configuration NetScaler, afin de permettre la gestion à distance de l'instance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- Si DHCP échoue ou s'arrête, l'instance présente la configuration réseau par défaut (192.168.100.1/16).

### Script client

L'instance VPX permet d'exécuter un script personnalisé pendant le provisionnement initial. L'appliance prend en charge les scripts de type Shell, Perl, Python et les commandes CLI NetScaler.

### Authentification par paire de clés SSH

L'instance VPX copie la clé publique, disponible dans le lecteur de configuration dans le cadre des métadonnées d'instance, dans son fichier « authorized_keys ». Cela permet à l'utilisateur d'accéder à l'instance avec une clé privée.

> **Remarque :**
>
> Lorsqu'une clé SSH est fournie, les informations d'identification par défaut (nsroot/nsroot) ne fonctionnent plus. Si un accès par mot de passe est nécessaire, ouvrez une session avec la clé privée SSH respective et définissez manuellement un mot de passe.

### Avant de commencer

Avant de provisionner une instance VPX sur un environnement OpenStack, extrayez le `.qcow2` fichier du fichier .tgz et générez

Une image OpenStack de l'image qcow2. Procédez comme suit :

1. Extrayez le `.qcow2` fichier du `.tqz` fichier en tapant la commande suivante

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante.

```
openstack image create --container-format bare --property
   hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2
   file> --public <name of the OpenStack image>

glance image-create --name="NS-VPX-12-0-26-2" --property
   hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
   -12.0-26.2_nc.qcow2
```

Figure 1 : L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

```
+------------------+--------------------------------------------------------+
| Field            | Value                                                  |
+------------------+--------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                       |
| container_format | bare                                                   |
| created_at       | 2017-03-13T08:52:31Z                                   |
| disk_format      | qcow2                                                  |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file   |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                   |
| min_disk         | 0                                                      |
| min_ram          | 0                                                      |
| name             | VPX-KVM-12.0-26.2
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                       |
| properties       | hw_disk_bus='ide'                                      |
| protected        | False                                                  |
| schema           | /v2/schemas/image                                      |
| size             | 784338944                                              |
| status           | active                                                 |
| updated_at       | 2017-03-13T08:52:43Z                                   |
| virtual_size     | None                                                   |
| visibility       | public                                                 |
+------------------+--------------------------------------------------------+
```


Provisionnement de l'instance VPX

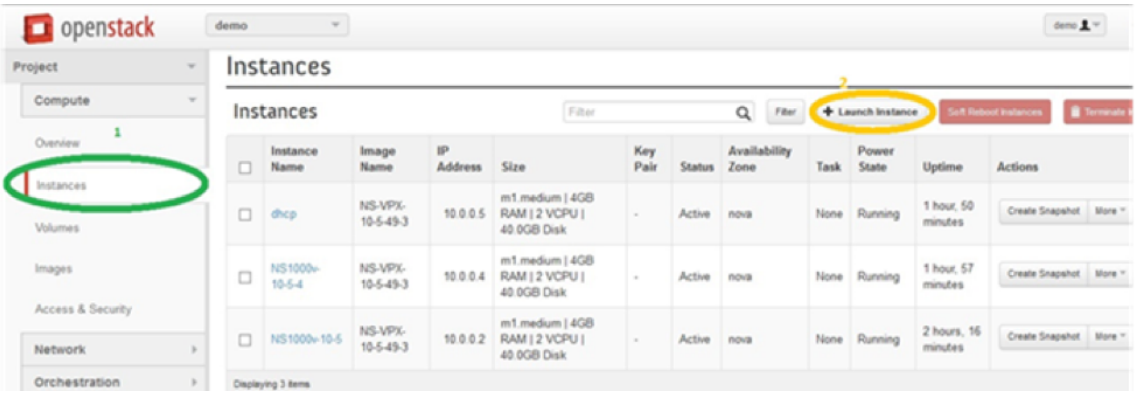
Vous pouvez provisionner une instance VPX de deux façons en utilisant l'une des options suivantes :

- Horizon (tableau de bord OpenStack)
- Commande de démarrage Nova (CLI OpenStack)

Provisionner une instance VPX à l'aide du tableau de bord OpenStack

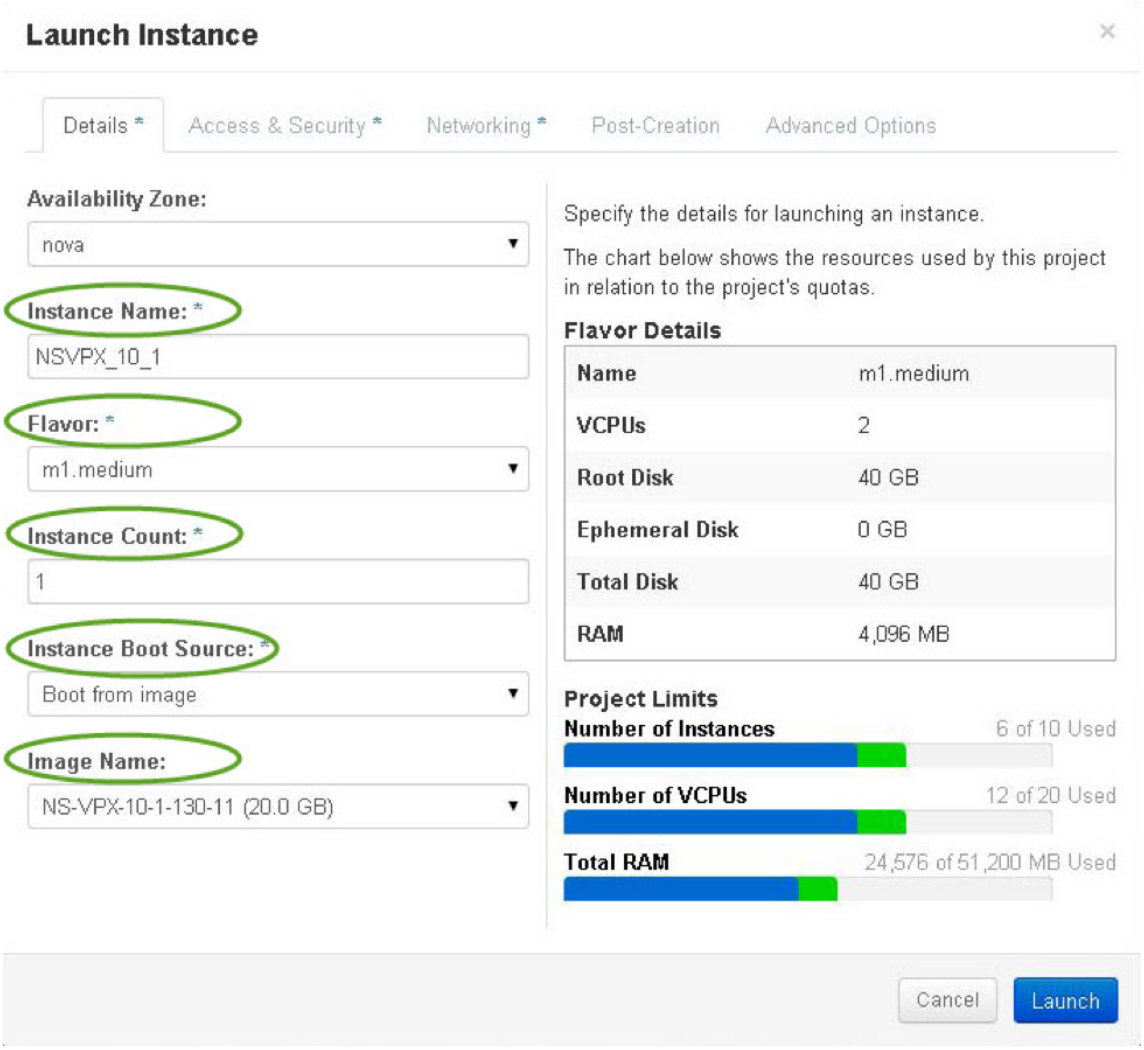
Procédez comme suit pour provisionner l'instance VPX à l'aide d'Horizon :

1. Connectez-vous au tableau de bord OpenStack.
2. Dans le panneau Projet situé à gauche du tableau de bord, sélectionnez **Instances**.
3. Dans le panneau Instances, cliquez sur **Lancer une instance** pour ouvrir l'Assistant Lancement d'instance.



4. Dans l'assistant de lancement d'instance, entrez les détails, tels que :

   a) Nom de l'instance
   b) Saveur d'instance
   c) Nombre d'instances
   d) Source de démarrage d'instance
   e) Nom de l'image



5. Déployez une nouvelle paire de clés ou une paire de clés existante via Horizon en procédant comme suit :

   a) Si vous n'avez pas de paire de clés existante, créez la clé à l'aide des mécanismes existants. Si vous avez une clé existante, ignorez cette étape.

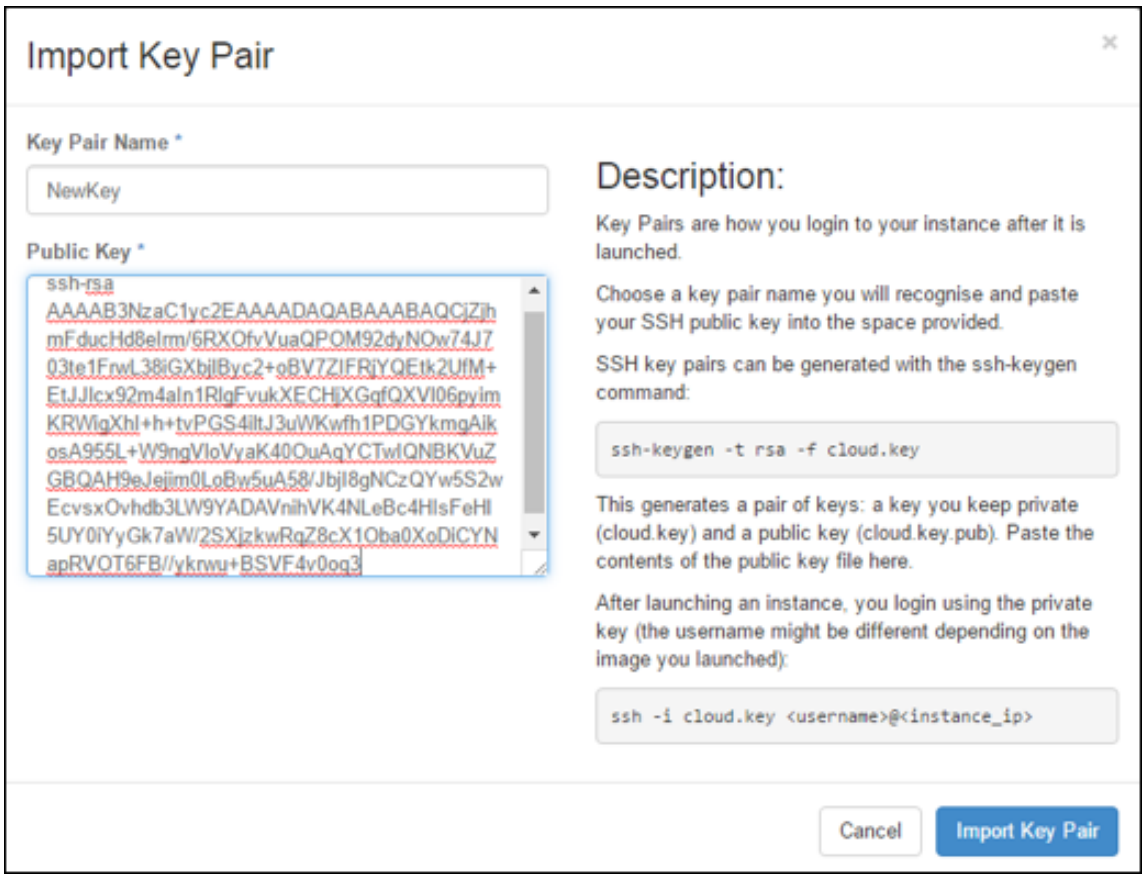
   b) Copier le contenu de la clé publique.

   c) Accédez à **Horizon > Instances > Créer de nouvelles instances**.

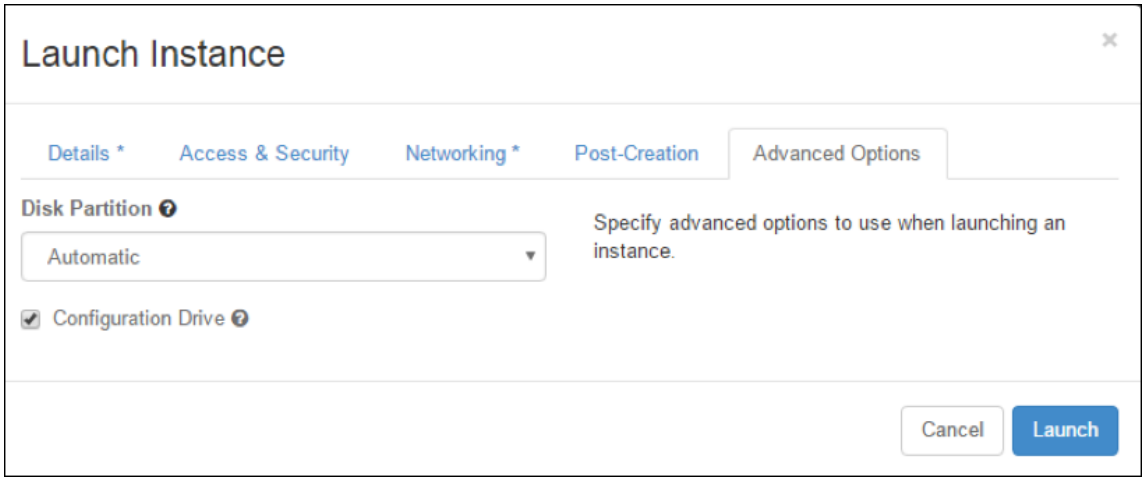
   d) Cliquez sur **Accès et sécurité**.

   e) Cliquez sur le signe+ en regard du menu déroulant **Paire de clés** et indiquez les valeurs des paramètres affichés.

   f) Collez le contenu de la *clé publique dans la zone Clé publique*, donnez un nom à la clé et cliquez sur **Importer la paire de clés** .



6. Cliquez sur l'onglet **Création de publications** dans l'Assistant. Dans le script de personnalisation, ajoutez le contenu du fichier de données utilisateur. Le fichier de données utilisateur contient l'adresse IP, les détails du masque réseau et de la passerelle, ainsi que les scripts client de l'instance VPX.
7. Une fois qu'une paire de clés est sélectionnée ou importée, cochez l'option config-drive et cliquez sur **Launch**.



Provisionner l'instance VPX à l'aide de l'interface de ligne de commande OpenStack

Procédez comme suit pour provisionner une instance VPX à l'aide de l'interface de ligne de commande OpenStack.

1. Pour créer une image à partir de qcow2, tapez la commande suivante :

   ```
   openstack image create --container-format bare --property hw_disk_bus
   =ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX
   -ToT-Image
   ```

2. Pour sélectionner une image pour créer une instance, tapez la commande suivante :

   ```
   openstack image list | more
   ```

3. Pour créer une instance d'une saveur particulière, tapez la commande suivante pour choisir un ID de saveur dans une liste :

   ```
   openstack flavor list
   ```

4. Pour attacher une carte réseau à un réseau particulier, tapez la commande suivante pour choisir un ID réseau dans une liste réseau :

   ```
   openstack network list
   ```

5. Pour créer une instance, tapez la commande suivante :

   ```
   1  openstack server create --flavor FLAVOR_ID --image IMAGE_ID --
      key-name KEY_NAME
   2  --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id
      =net-uuid
   3  INSTANCE_NAME
   4  openstack server create --image VPX-ToT-Image --flavor m1.medium
       --user-data
   5  ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6
      -3efd44b761b9
   6  VPX-ToT
   ```

Figure 2 : L'illustration suivante fournit un exemple de sortie.

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

Provisionnez l'instance NetScaler VPX à l'aide du Virtual Machine Manager

October 17, 2024

Virtual Machine Manager est un outil de bureau pour gérer les invités de machines virtuelles. Il vous permet de créer de nouveaux invités VM et différents types de stockage, et de gérer des réseaux virtuels. Vous pouvez accéder à la console graphique des invités de machines virtuelles à l'aide de la visionneuse VNC intégrée et afficher les statistiques de performances, localement ou à distance.

Après avoir installé votre distribution Linux préférée, avec la virtualisation KVM activée, vous pouvez procéder au Provisioning des machines virtuelles.

Lorsque vous utilisez le Virtual Machine Manager pour provisionner une instance NetScaler VPX, deux options s'offrent à vous :

- Entrez manuellement l'adresse IP, la Gateway et le masque de réseau
- Attribuer automatiquement l'adresse IP, la Gateway et le masque de réseau (provisionnement automatique)

Vous pouvez utiliser deux types d'images pour provisionner une instance NetScaler VPX :

- CRU

- QCOW2

Vous pouvez convertir une image RAW NetScaler VPX en image QCOW2 et provisionner l'instance NetScaler VPX. Pour convertir l'image RAW en une image QCOW2, tapez la commande suivante :

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Par exemple :

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5
_nc.qcow
```

Un déploiement standard de NetScaler VPX sur KVM comprend les étapes suivantes :

- Vérification des prérequis pour le Provisioning automatique d'une instance NetScaler VPX
- Provisioning de l'instance NetScaler VPX à l'aide d'une image RAW
- Provisioning de l'instance NetScaler VPX à l'aide d'une image QCOW2
- Ajout d'interfaces supplémentaires à une instance VPX à l'aide de Virtual Machine Manager

Vérifiez les conditions requises pour le provisionnement automatique d'une instance NetScaler VPX

Le provisionnement automatique est une fonctionnalité facultative qui implique l'utilisation de données provenant du lecteur de CD-ROM. Si cette fonctionnalité est activée, il n'est pas nécessaire de saisir l'adresse IP de gestion, le masque réseau et la passerelle par défaut de l'instance NetScaler VPX lors de la configuration initiale.

Vous devez effectuer les tâches suivantes avant de pouvoir provisionner automatiquement une instance VPX :

1. Créez un fichier XML OVF (Open Virtualization Format) personnalisé ou un fichier de données utilisateur.
2. Convertissez le fichier OVF en image ISO à l'aide d'une application en ligne (par exemple PowerISO).
3. Montez l'image ISO sur l'hôte KVM à l'aide de n'importe quel outil SCP (Secure Copy).

Exemple de fichier XML OVF :

Voici un exemple de contenu d'un fichier XML OVF, que vous pouvez utiliser comme exemple pour créer votre fichier.

```
1  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
3  <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`
4
5  xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`
6
```



```
7    oe:id=""
8
9    xmlns="`http://schemas.dmtf.org/ovf/environment/1"`
10
11   xmlns:cs="`http://schemas.citrix.com/openstack">`
12
13   <PlatformSection>
14
15   <Kind></Kind>
16
17   <Version>2016.1</Version>
18
19   <Vendor>VPX</Vendor>
20
21   <Locale>en</Locale>
22
23   </PlatformSection>
24
25   <PropertySection>
26
27   <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
28
29   <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
30
31   <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>
32
33   <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
        />
34
35   <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
        255.255.255.0"/>
36
37   <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
        10.1.2.1"/>
38
39   </PropertySection>
40
41   </Environment>
```

Dans le fichier XML OVF précédent, « PropertySection » est utilisé pour la configuration réseau NetScaler. Lorsque vous créez le fichier, spécifiez les valeurs des paramètres qui sont mis en surbrillance à la fin de l'exemple :

- Adresse IP de gestion
- Masque réseau
- Gateway

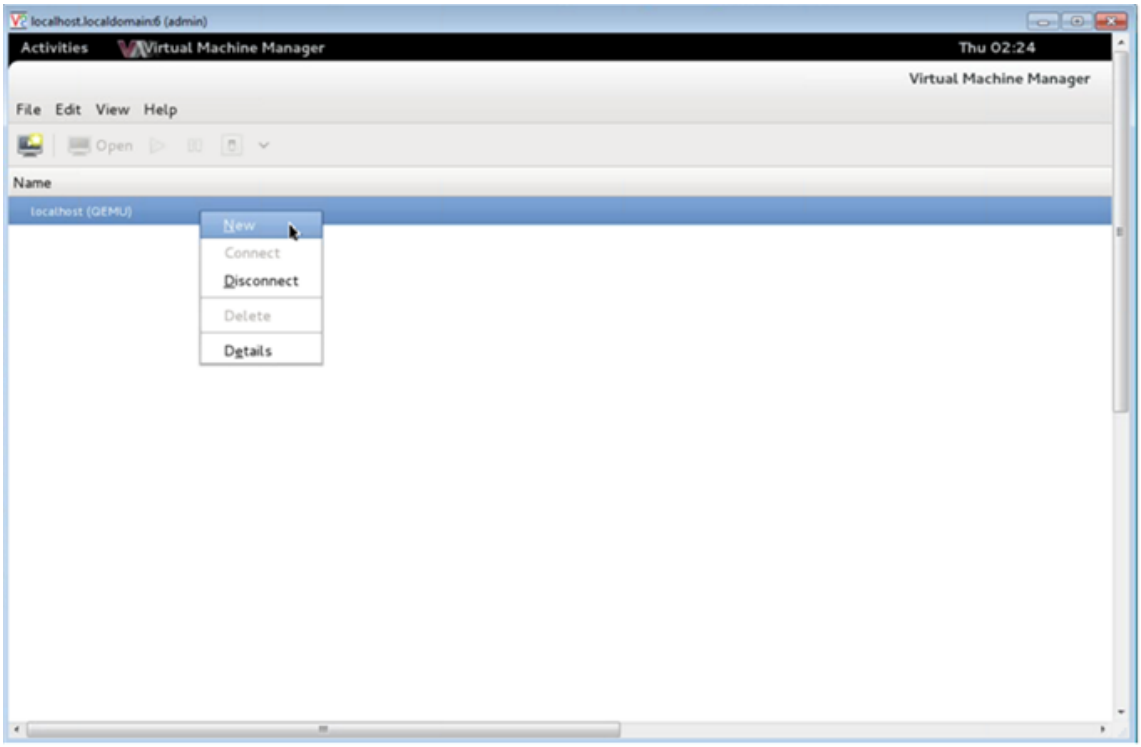
> **Important**
>
> Si le fichier OVF n'est pas correctement formaté XML, l'instance VPX se voit attribuer la configuration réseau par défaut, et non les valeurs spécifiées dans le fichier.

Provisionnez l'instance NetScaler VPX à l'aide d'une image RAW

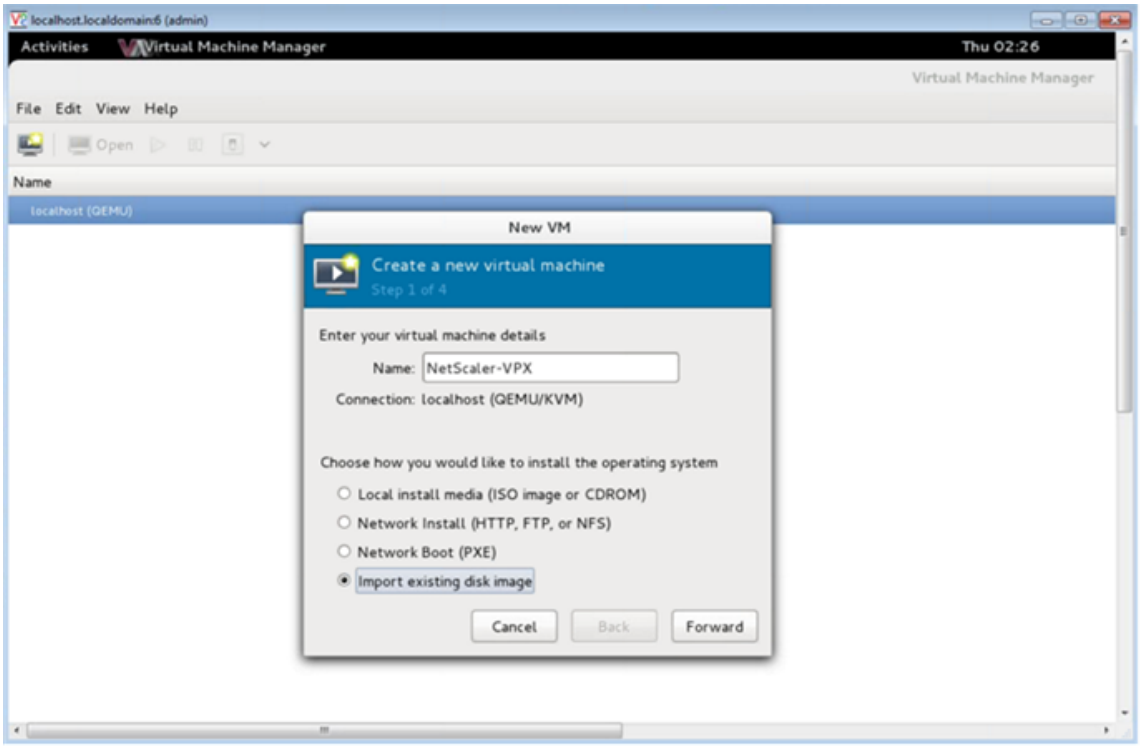
Le Virtual Machine Manager vous permet de provisionner une instance NetScaler VPX à l'aide d'une image RAW.

Pour provisionner une instance NetScaler VPX à l'aide du Virtual Machine Manager, procédez comme suit :

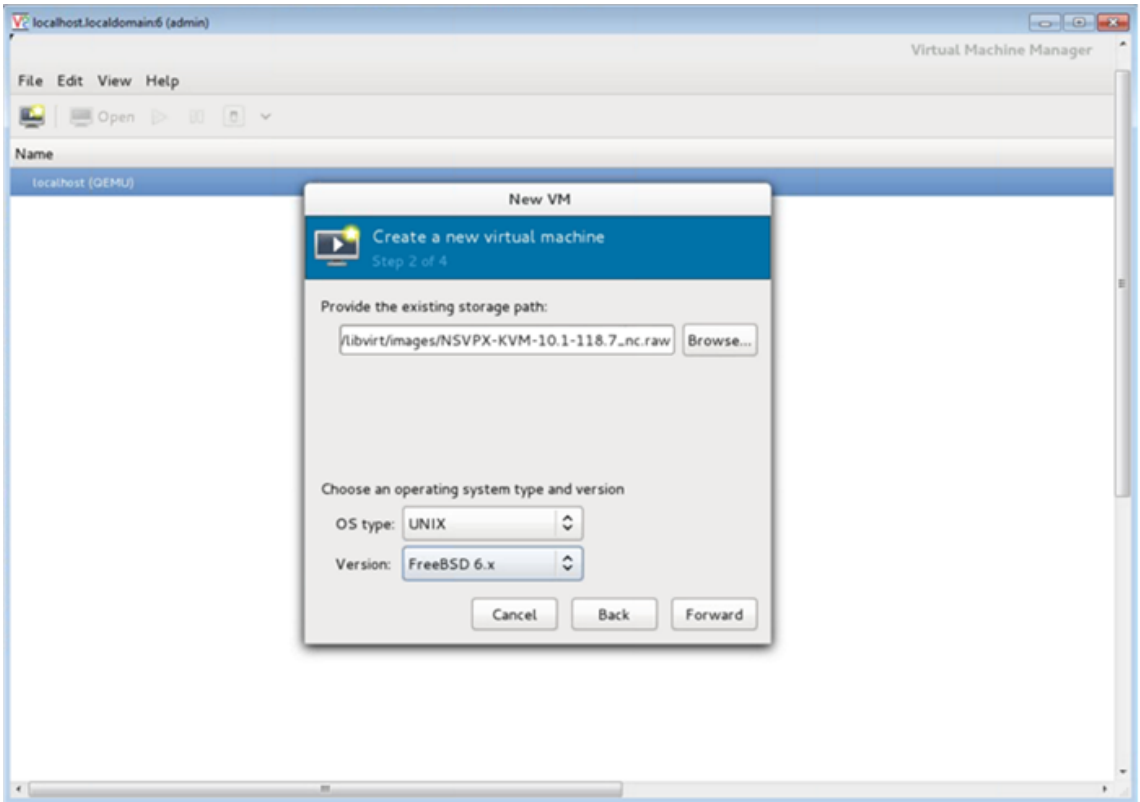
1. Ouvrez Virtual Machine Manager (**Application** > **Outils système** > **Virtual Machine Manager**) et entrez les informations d'identification d'ouverture de session dans la fenêtre **Authentifier** .
2. Cliquez sur l'icône  ou cliquez avec le bouton droit sur **localhost (QEMU)** pour créer une nouvelle instance NetScaler VPX.



3. Dans la zone de texte **Nom**, entrez le nom de la nouvelle machine virtuelle (par exemple, Netscaler-VPX).
4. Dans la fenêtre **Nouvelle machine virtuelle**, sous « Choisissez la manière dont vous souhaitez installer le système d'exploitation », sélectionnez **Importer une image disque existante**, puis cliquez sur **Suivant**.

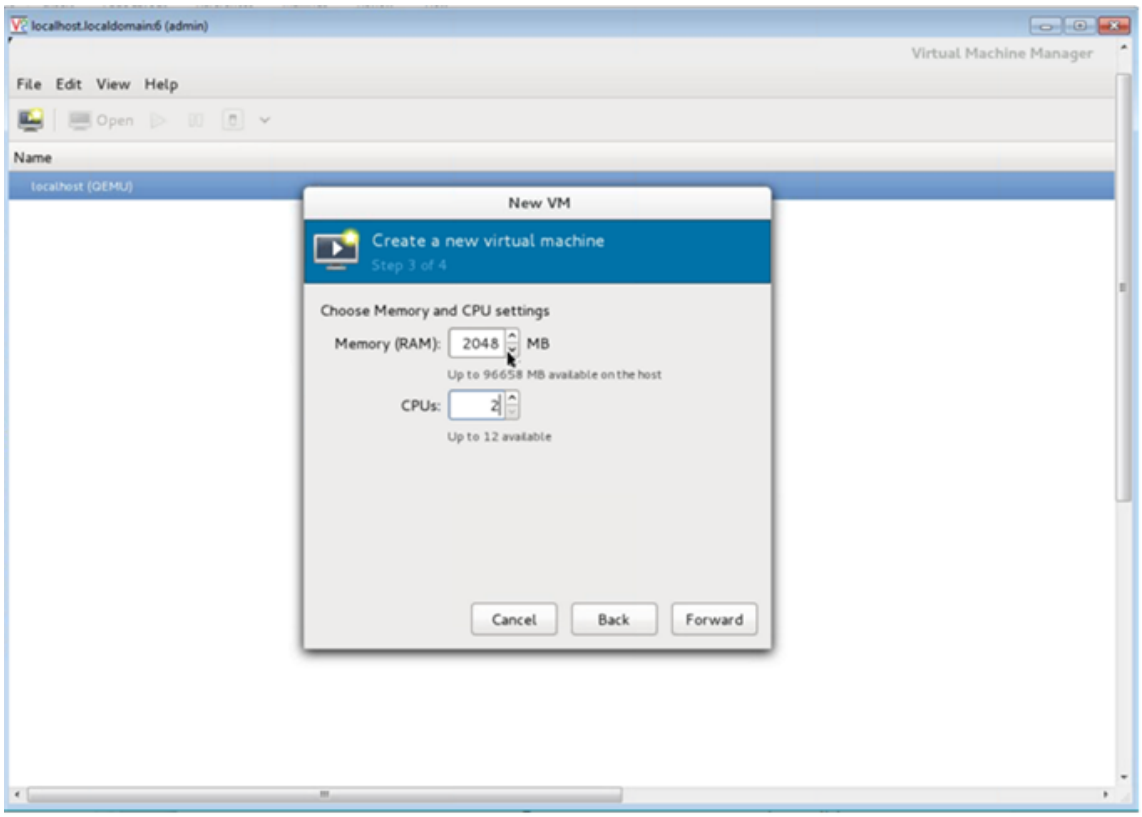


5. Dans le champ **Fournir le chemin de stockage existant**, parcourez le chemin d'accès à l'image. Choisissez le type d'OS sous UNIX et la version sous FreeBSD 6.x. Cliquez ensuite sur **Transférer**.

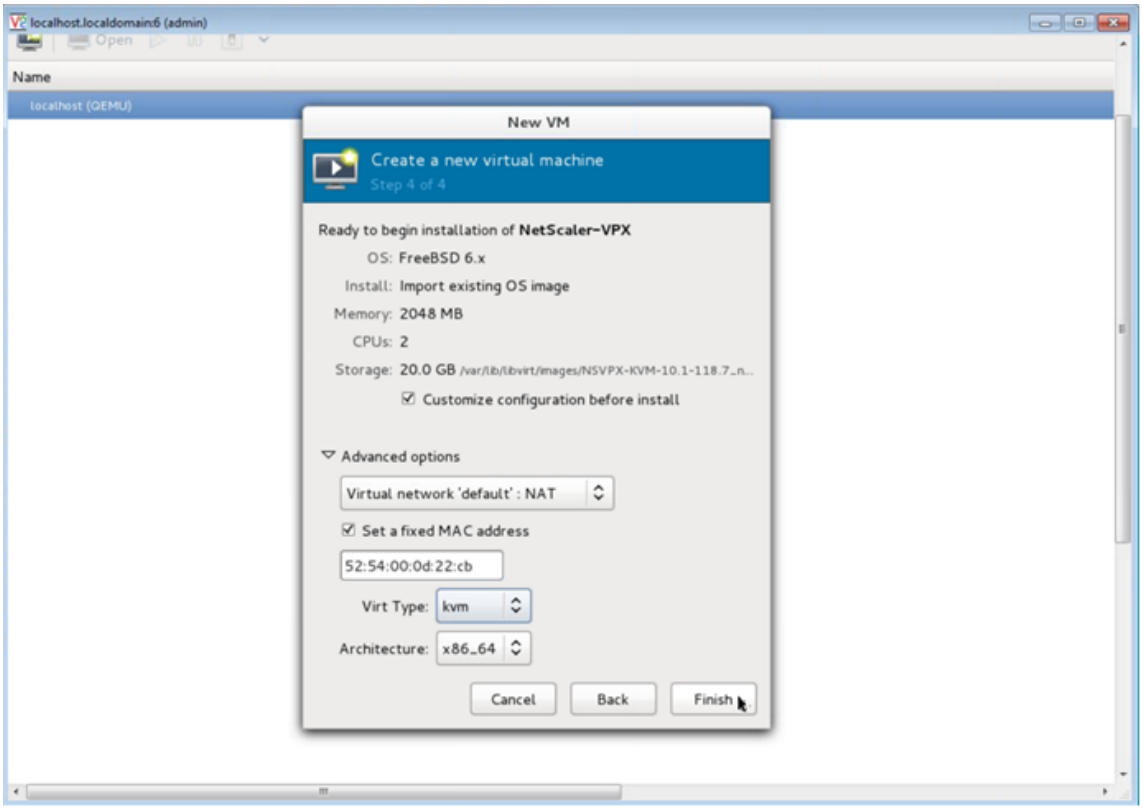


6. Sous **Choisir les paramètres de mémoire et de processeur**, sélectionnez les paramètres suivants, puis cliquez sur **Suivant** :

   - Mémoire vive (RAM) —2048 Mo
   - CPU —2

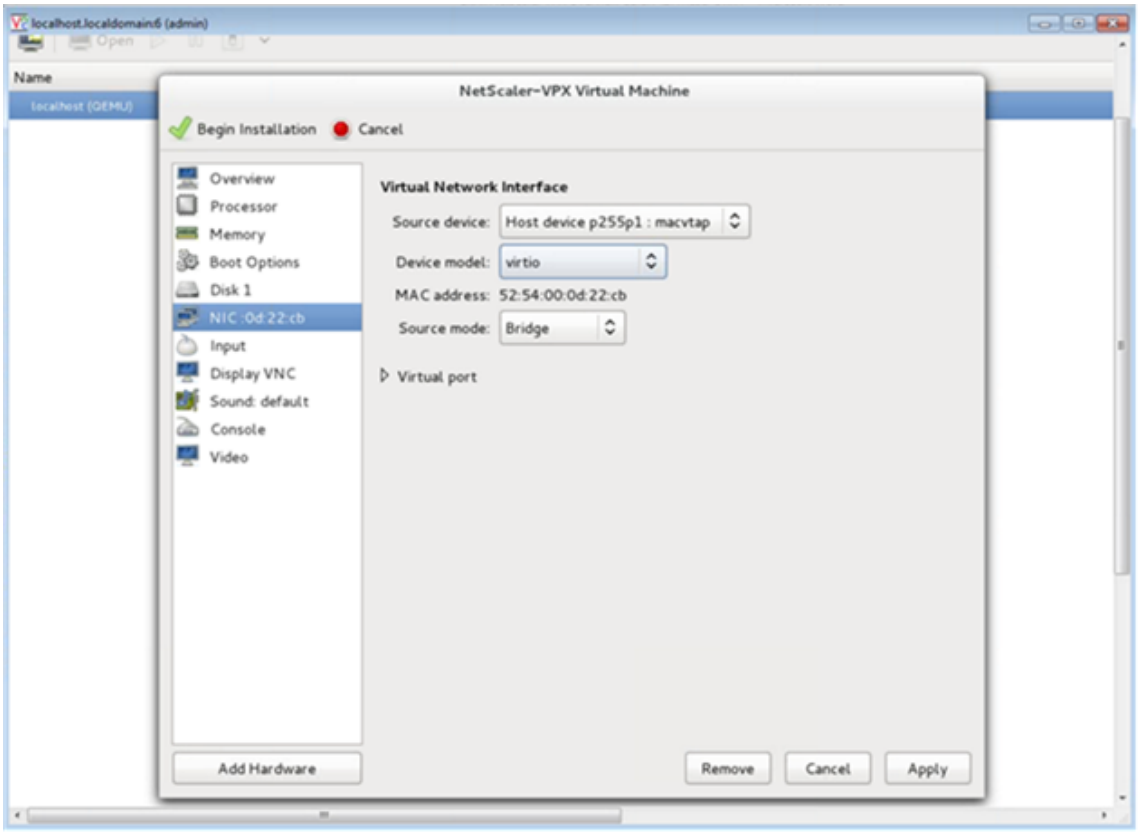


7. Activez la case à cocher **Personnaliser la configuration avant l'installation** . Le cas échéant, sous **Options avancées**, vous pouvez personnaliser l'adresse MAC. Assurez-vous que le **type Virt** sélectionné est KVM et que l'architecture sélectionnée est x86_64. Cliquez sur **Terminer**.



8. Sélectionnez une carte réseau et fournissez la configuration suivante :

   - Périphérique source `ethX macvtap` ou Bridge
   - Modèle d'appareil—`virtio`
   - Mode source : Bridge



9. Cliquez sur **Appliquer**.
10. Si vous souhaitez configurer automatiquement l'instance VPX, consultez la section **Activation de l'auto-provisioning en attachant un lecteur de CDROM** dans ce document. Sinon, cliquez sur **Commencer l'installation**. Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter d'autres interfaces.

Provisionnez l'instance NetScaler VPX à l'aide d'une image QCOW2

À l'aide du Virtual Machine Manager, vous pouvez provisionner l'instance NetScaler VPX à l'aide d'une image QCOW2.

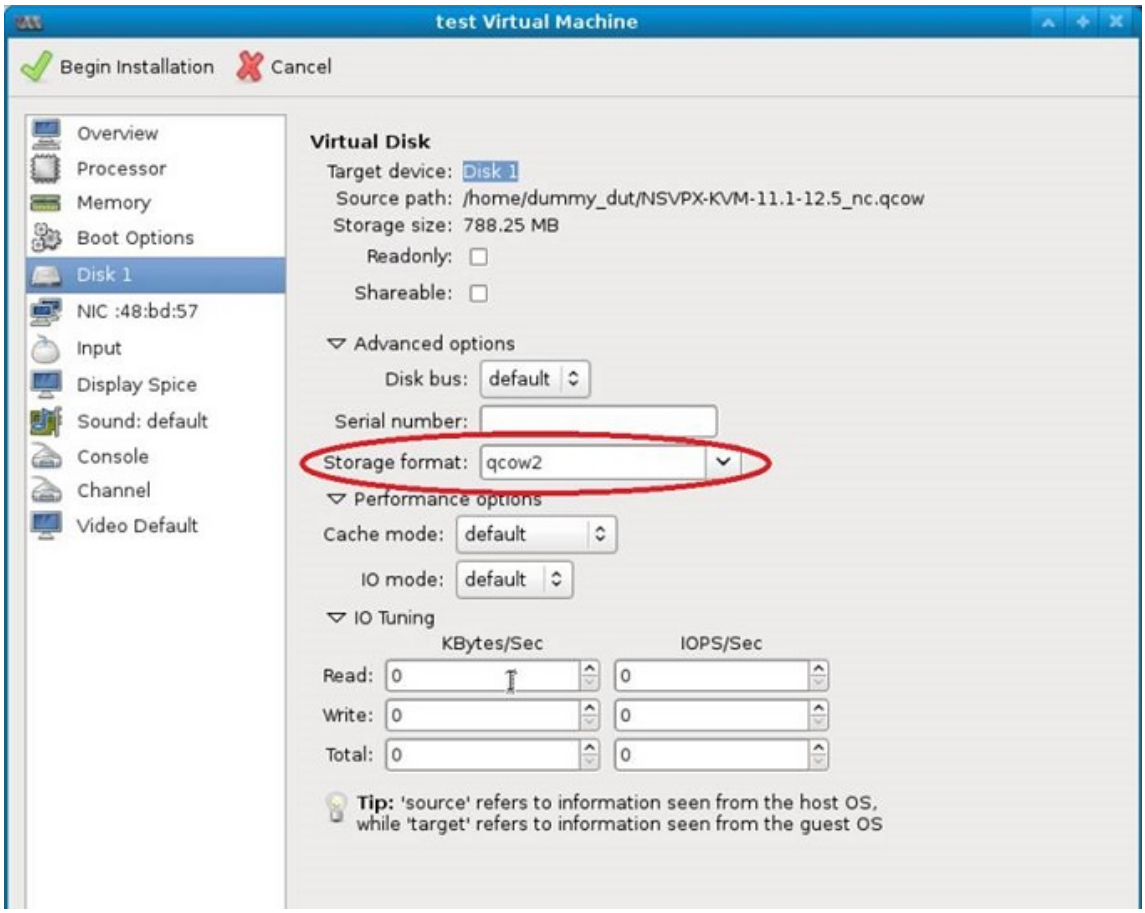
Pour provisionner une instance NetScaler VPX à l'aide d'une image QCOW2, procédez comme suit :

1. Suivez les **étapes 1** à **8 de la section Provisionner**l'instance NetScaler VPX à l'aide d'uneimage RAW.

   > **Remarque :**
   >
   > Assurez-vous de sélectionner l'image **qcow2** à l'étape **5**.

2. Sélectionnez **Disque 1** et cliquez sur **Options avancées** .

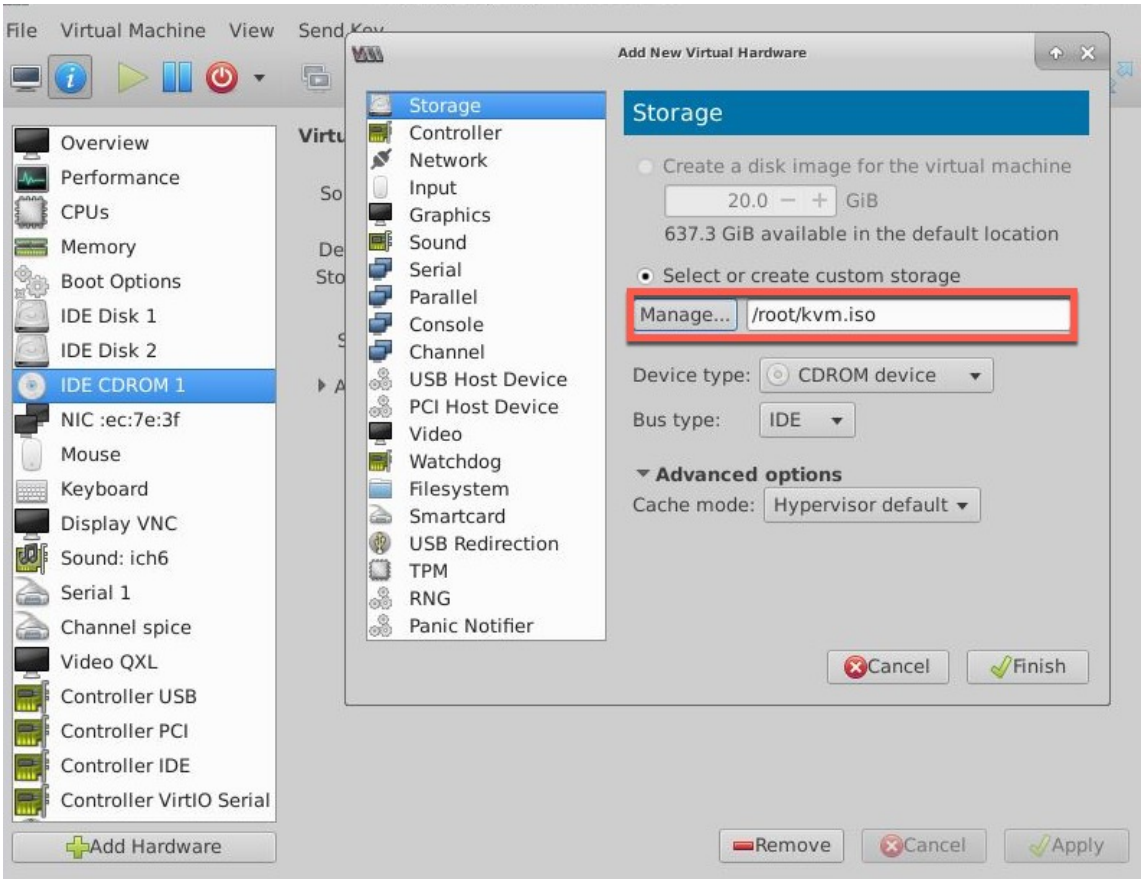
3. Sélectionnez **qcow2** dans la liste déroulante Format de stockage.



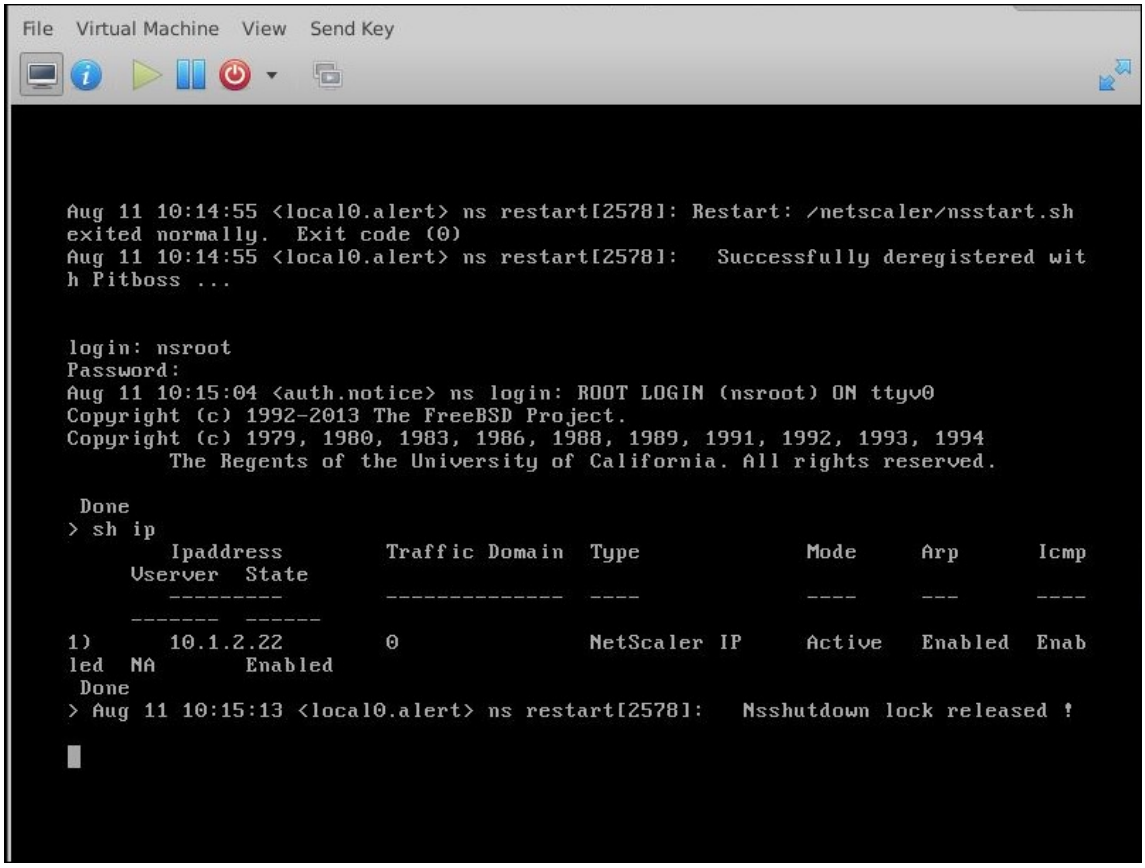
4. Cliquez sur **Appliquer**, puis sur **Commencer l'installation**. Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter d'autres interfaces.

Activer le provisioning automatique en attachant un lecteur de CD-ROM

1. Cliquez sur Ajouter **du matériel > Stockage > Type de périphérique > Lecteur de CD-ROM**.
2. **Cliquez sur**Gérer**et sélectionnez le fichier ISO approprié que vous avez monté dans la section « Conditions requises pour le Provisioning automatique d'une instance NetScaler VPX », puis cliquez sur Terminer.** Un nouveau CDROM est créé sous Ressources sur votre instance NetScaler VPX. Un nouveau CDROM sous Ressources sur votre instance NetScaler VPX est créé.



3. Mettez l'instance VPX sous tension, et il provisionnera automatiquement avec la configuration réseau fournie dans le fichier OVF, comme indiqué dans l'exemple de capture d'écran.



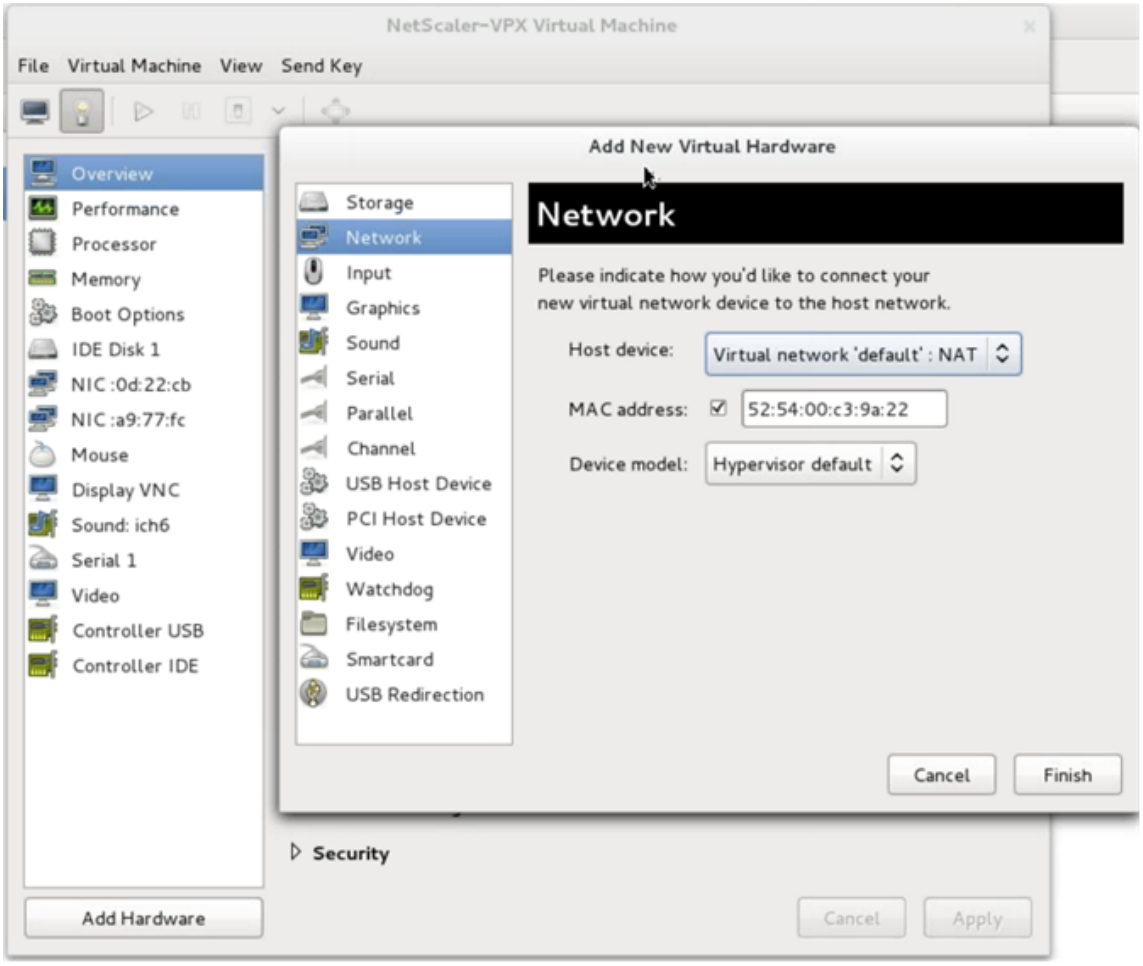
4. Si la mise en service automatique échoue, l'instance affiche l'adresse IP par défaut (192.168.100.1). Dans ce cas, vous devez terminer la configuration initiale manuellement. Pour plus d'informations, voir Configurer l'ADC pour la première fois.

Ajoutez d'autres interfaces à l'instance NetScaler VPX à l'aide du Virtual Machine Manager

Après avoir provisionné l'instance NetScaler VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit.

1. Arrêtez l'instance NetScaler VPX exécutée sur le KVM.
2. Cliquez avec le bouton droit sur l'instance VPX et choisissez **Ouvrir** dans le menu contextuel.
3. Cliquez sur l'icône de  dans l'en-tête pour afficher les détails du matériel virtuel.
4. Cliquez sur **Ajouter du matériel**. Dans la **fenêtre Ajouter un nouveau matériel virtuel**, sélectionnez **Réseau**dans le menu de navigation.



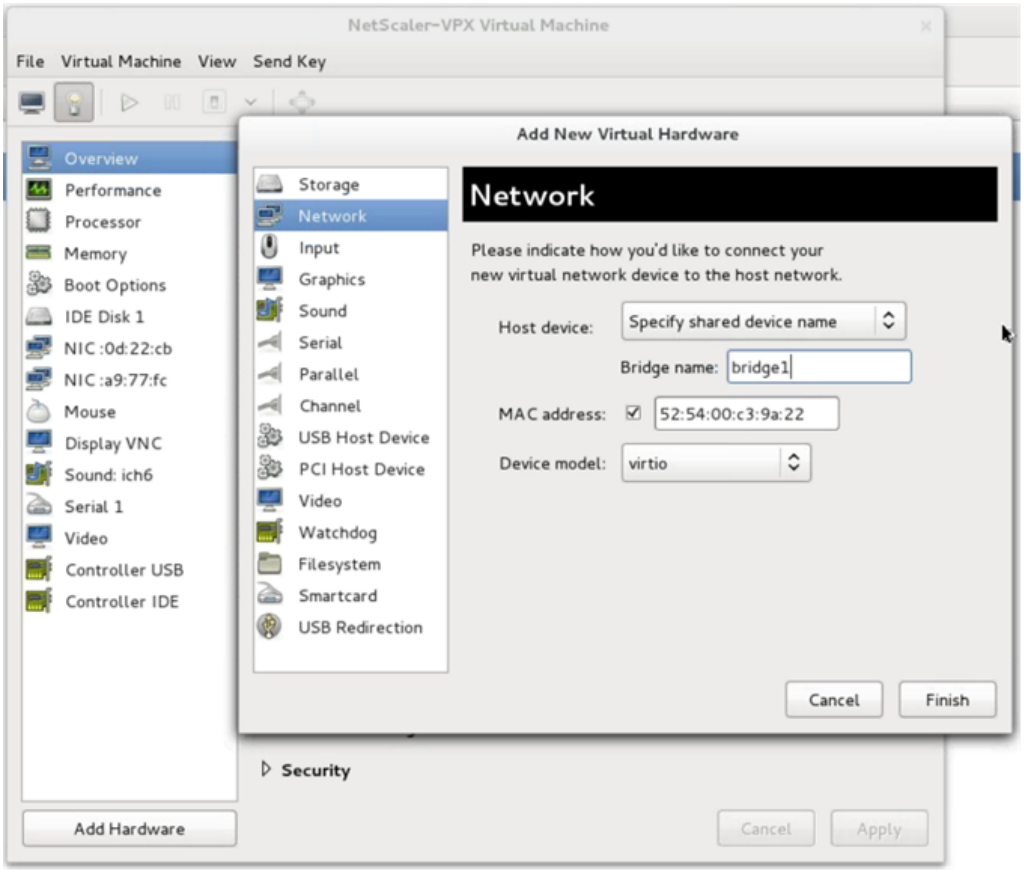
5. Dans le champ **Appareil hôte**, sélectionnez le type d'interface physique. Le type de périphérique hôte peut être Bridge ou MacVTap. Dans le cas d'un MacVTAP, quatre modes possibles sont VEPA, Bridge, Private et Pass-Through.

   a) Pour Bridge

      i. Périphérique hôte : sélectionnez l'option « Spécifier le nom de périphérique partagé ».

      ii. Indiquez le nom du pont configuré dans l'hôte KVM.

      > **Remarque :**
      >
      > Assurez-vous d'avoir configuré un pont Linux dans l'hôte KVM, lié l'interface physique au pont et mis le pont dans l'état UP.



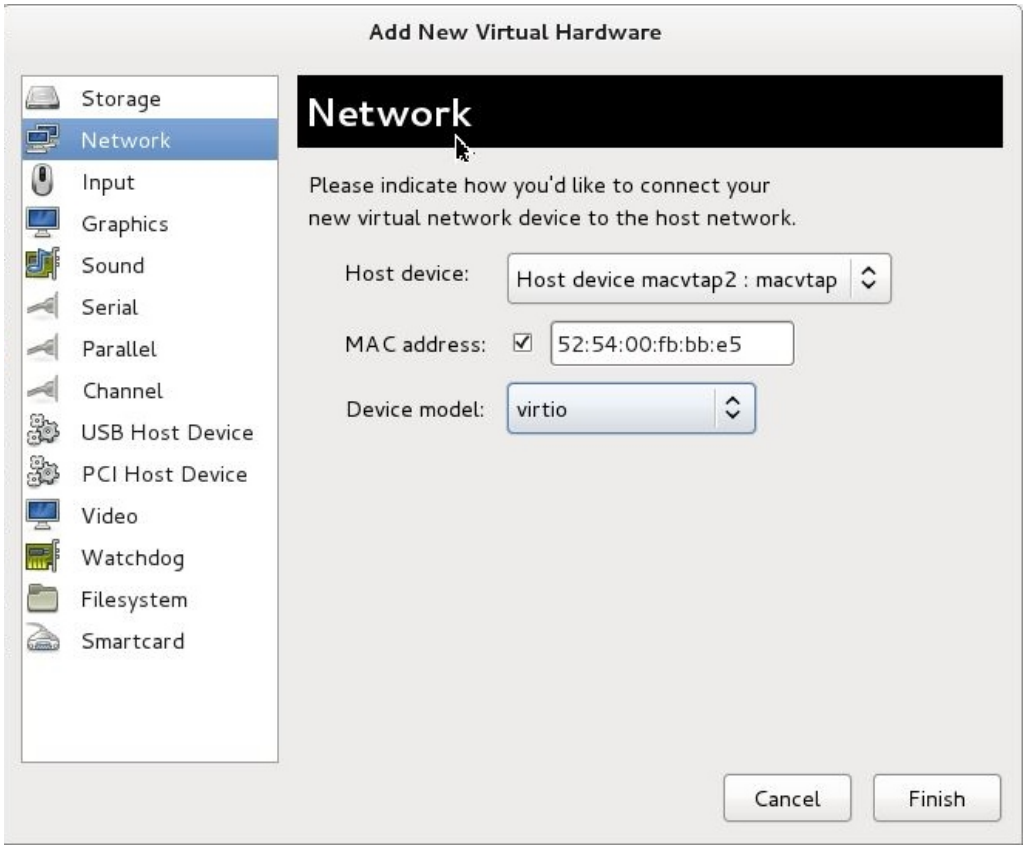
iii. Modèle d'appareil—`virtio`.

iv. Cliquez sur **Terminer**.

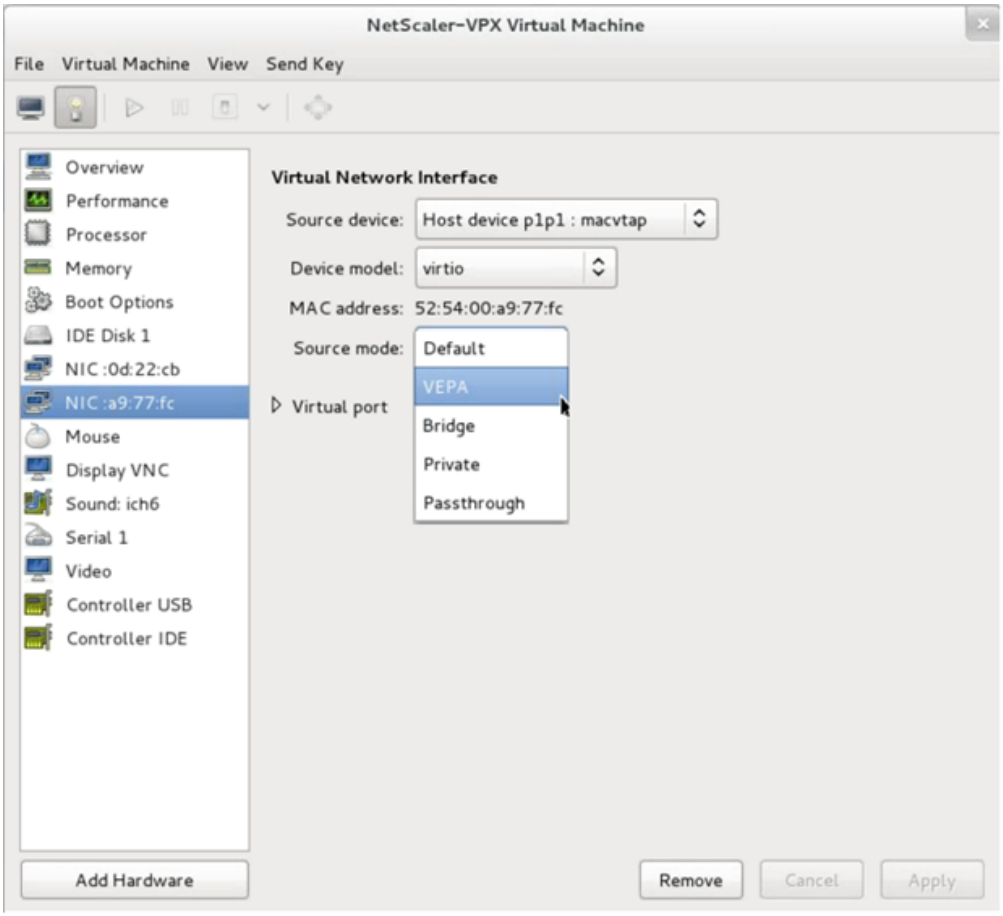
b) Pour MacVTap

i. Périphérique hôte : sélectionnez l'interface physique dans le menu.

ii. Modèle d'appareil—`virtio`.



iii. Cliquez sur **Terminer**. Vous pouvez afficher la carte réseau nouvellement ajoutée dans le volet de navigation.



iv. Sélectionnez la carte réseau nouvellement ajoutée et sélectionnez le mode Source pour cette carte réseau. Les modes disponibles sont VEPA, Pont, Privé et Passthrough. Pour plus de détails sur l'interface et les modes, voir Interface source et modes.

v. Cliquez sur **Appliquer**.

6. Si vous souhaitez configurer automatiquement l'instance VPX, consultez la section « Ajout d'un lecteur de configuration pour activer le provisionnement automatique » dans ce document. Sinon, mettez l'instance VPX sous tension pour terminer manuellement la configuration initiale.

> **Important :**
>
> Les configurations de paramètres d'interface telles que la vitesse, le duplex et la négociation automatique ne sont pas prises en charge.

Configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV

October 17, 2024

Vous pouvez configurer une instance NetScaler VPX exécutée sur la plate-forme Linux-KVM à l'aide de la virtualisation des E/S à racine unique (SR-IOV) avec les cartes réseau suivantes :

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

Cette section décrit comment :

- Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV
- Configurer l'interface LA/LACP statique sur l'interface SR-IOV
- Configurer VLAN sur l'interface SR-IOV

Limitations

Gardez à l'esprit les limitations lors de l'utilisation des cartes réseau Intel 82599, X710, XL710 et X722. Les fonctionnalités suivantes ne sont pas prises en charge.

Limitations pour la carte réseau Intel 82599 :

- Commutation de mode L2.
- Partitionnement administrateur (mode VLAN partagé).
- Haute disponibilité (mode actif-actif).
- Cadres Jumbo.
- IPv6 : Vous ne pouvez configurer que 30 adresses IPv6 uniques dans une instance VPX si vous disposez d'au moins une interface SR-IOV.
- La configuration VLAN sur l'interface Hypervisor for SRIOV VF via `ip link` commande n'est pas prise en charge.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.

Limitations pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G :

- Commutation de mode L2.
- Partitionnement administrateur (mode VLAN partagé).

- Dans un cluster, les trames Jumbo ne sont pas prises en charge lorsque la carte réseau XL710 est utilisée comme interface de données.
- La liste des interfaces réordonne lorsque les interfaces sont déconnectées et reconnectées.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.
- Le nom de l'interface est 40/X pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G
- Jusqu'à 16 interfaces relais Intel XL710/X710/X722 SRIOV ou PCI peuvent être prises en charge sur une instance VPX.

> **Remarque :**
>
> Pour que les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G prennent en charge IPv6, vous devez activer le mode de confiance sur les fonctions virtuelles (VF) en saisissant la commande suivante sur l'hôte KVM :
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> Exemple
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```

Conditions préalables

Avant de configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV, effectuez les tâches préalables suivantes. Reportez-vous à la colonne NIC pour plus d'informations sur la façon d'effectuer les tâches correspondantes.

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
1. Ajoutez la carte réseau à l'hôte KVM.	-	-
1. Téléchargez et installez le dernier pilote Intel.	Pilote IXGBE	Pilote I40E
1. Bloquer le pilote sur l'hôte KVM.	Ajoutez l'entrée suivante dans le fichier /etc/mod-probe.d/blacklist.conf : `blacklist ixgbevf`. Utilisez le pilote IXGBE version 4.3.15 (recommandé).	Ajoutez l'entrée suivante dans le fichier /etc/mod-probe.d/blacklist.conf : `blacklist i40evf`. Utilisez le pilote i40e version 2.0.26 (recommandé).

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
4.Activez SR-IOV Virtual Functions (VF) sur l'hôte KVM. Dans les deux commandes des deux colonnes suivantes : `number_of_VFs` = le nombre de VF virtuels que vous souhaitez créer. `device_name` = le nom de l'interface.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/ixgbe et redémarrez l'hôte KVM : `options ixgbe max_vfs =<number_of_VFs>`. Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo < number_of_VFs> &gt ; /sys/class/net/< device_name>/ device/sriov_numvfs`. Voir l'exemple de la figure 1.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/i40e.conf et redémarrez l'hôte KVM : `options i40e max_vfs =<number_of_VFs>`. Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo<number_of_VFs > > /sys/class/ net/<device_name& gt;/device/ sriov_numvfs`. Voir l'exemple de la figure 2.
1. Rendez les VF persistants en ajoutant les commandes que vous avez utilisées pour créer les VF au fichier rc.local.	Voir l'exemple de la figure 3.	Voir l'exemple de la figure 3.

> **Important :**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

Figure 1 : activer les VF SR-IOV sur l'hôte KVM pour la carte réseau Intel 82599 10G.

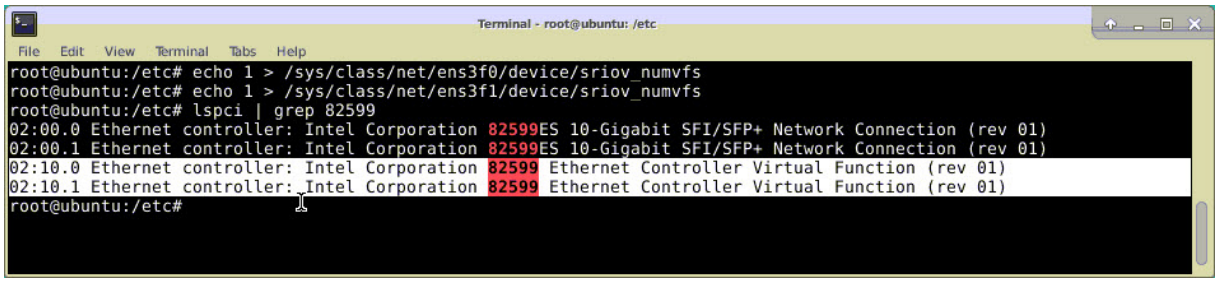


Figure 2 : activer les VF SR-IOV sur l'hôte KVM pour les cartes réseau Intel X710 10G et XL710 40G.

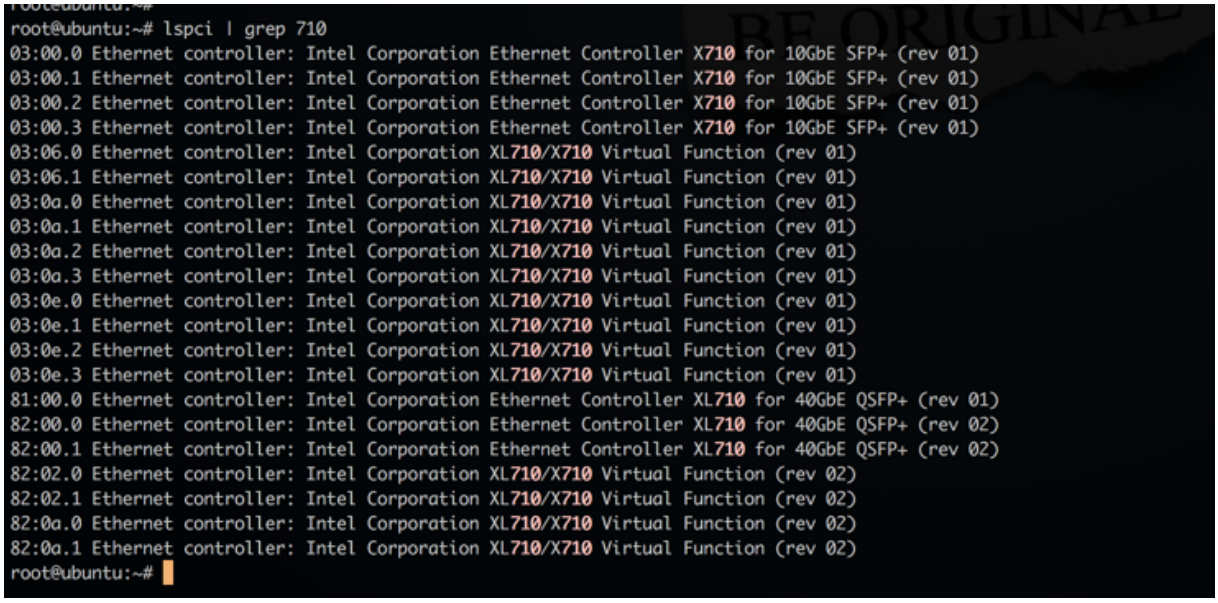


Figure 3 : activer les VF SR-IOV sur l'hôte KVM pour la carte réseau Intel X722 10G.

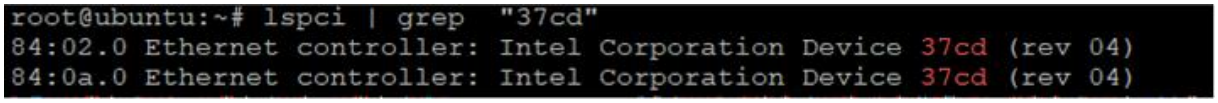
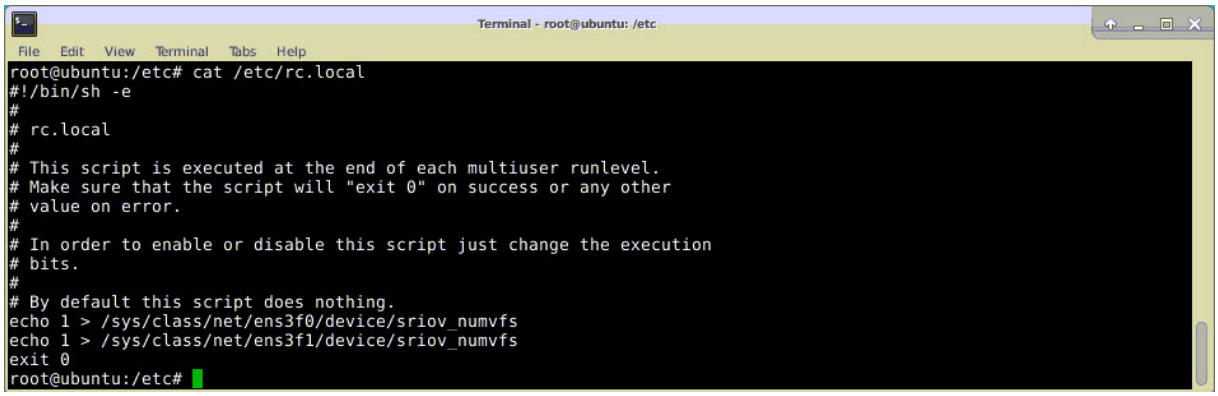


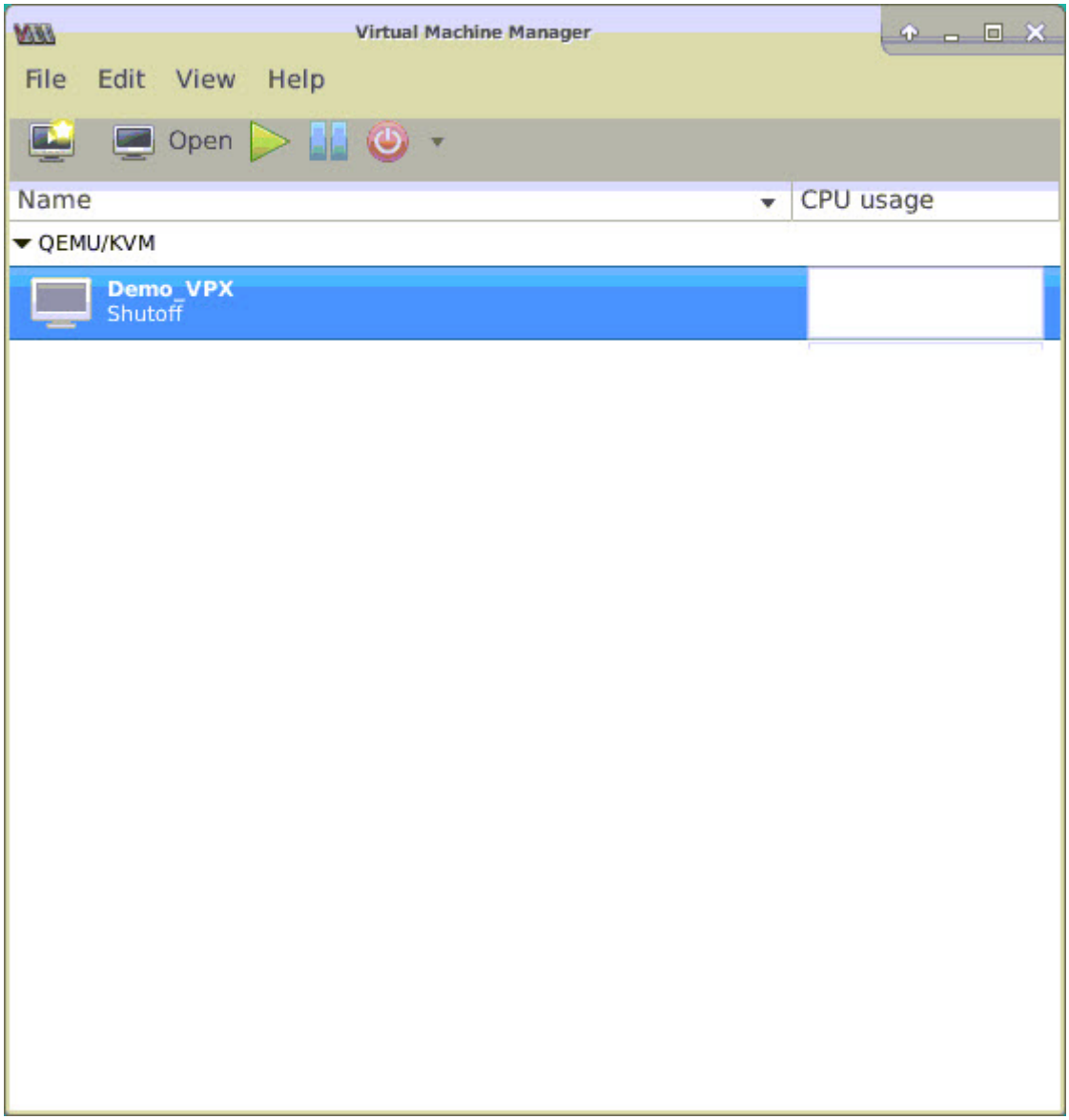
Figure 4 : Rendre les VF persistants.



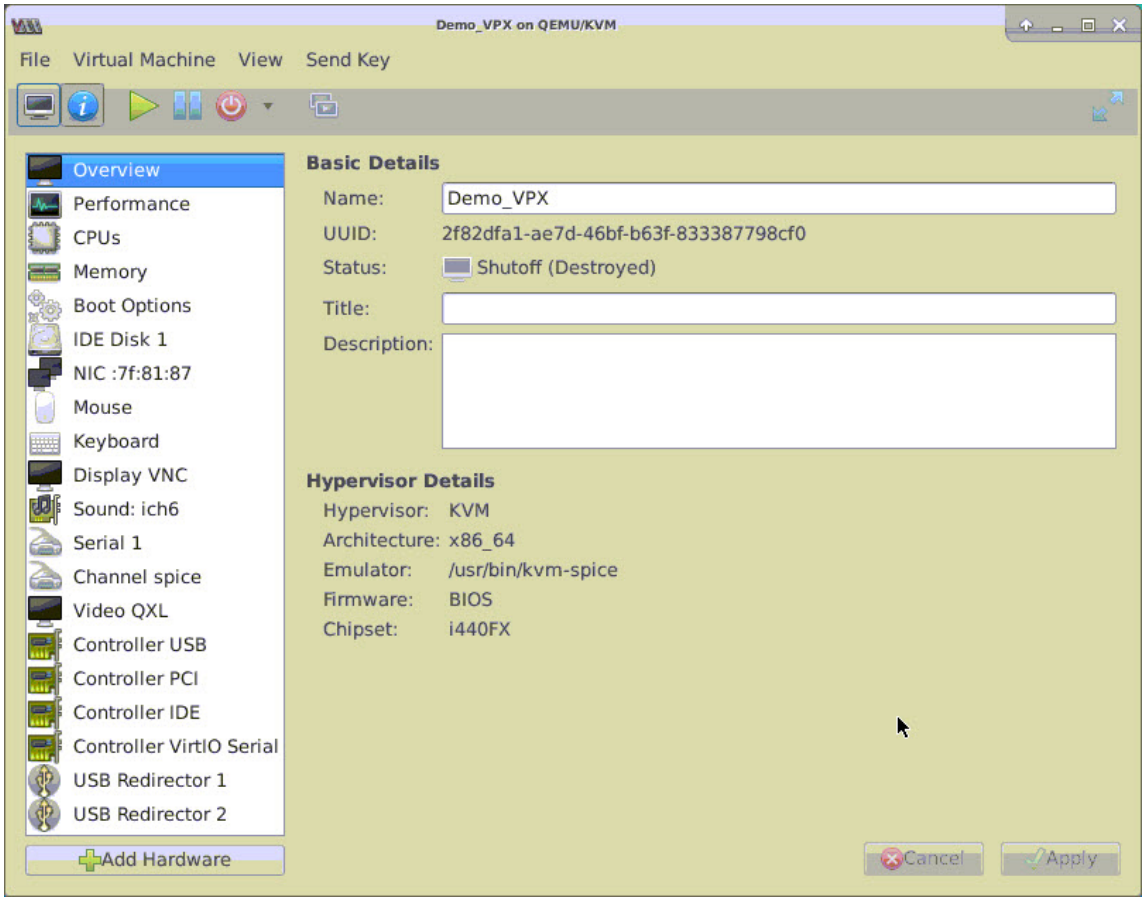
Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

Pour configurer l'instance NetScaler VPX afin qu'elle utilise l'interface réseau SR-IOV à l'aide de Virtual Machine Manager, procédez comme suit :

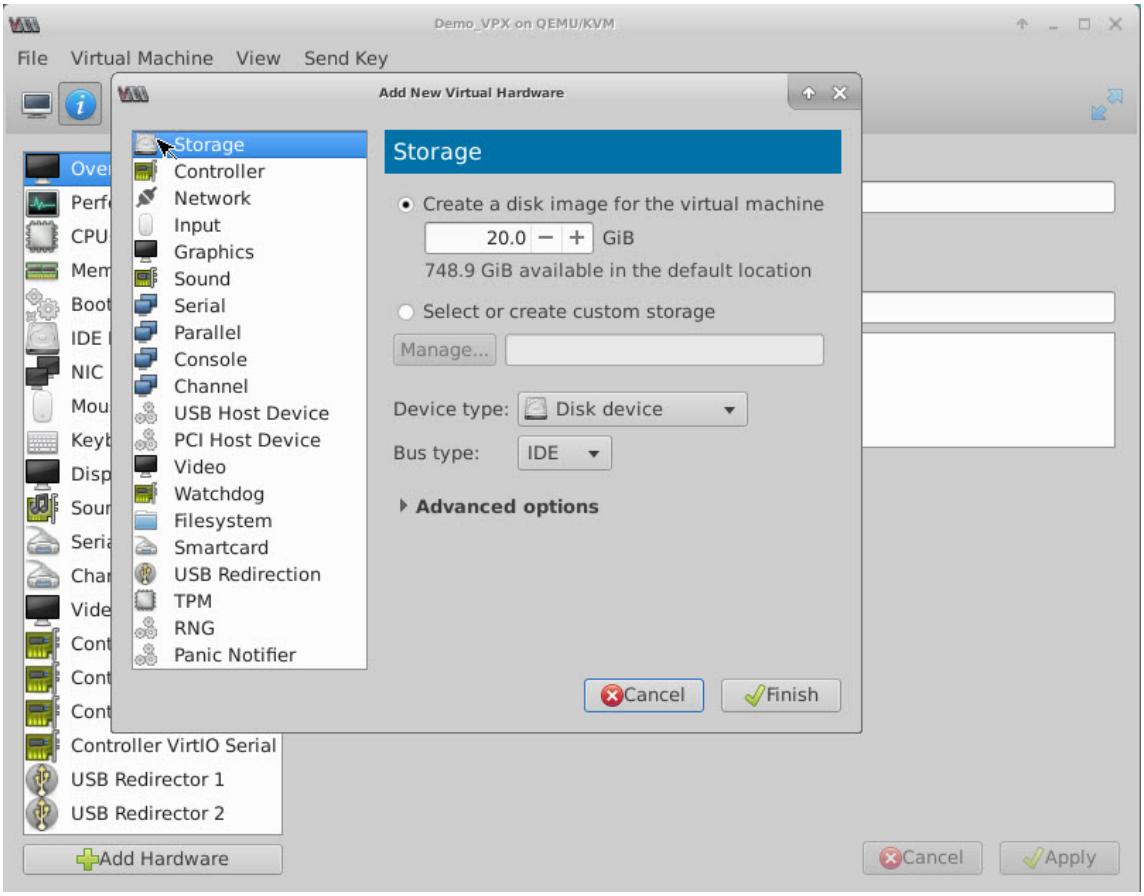
1. Éteignez l'instance NetScaler VPX.
2. Sélectionnez l'instance NetScaler VPX, puis sélectionnez Ouvrir.



3. Dans la <virtual machine on KVM>fenêtre, sélectionnez l'icône **i** .



4. Sélectionnez **Ajouter du matériel**.



5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a) Sélectionnez PCI Host Device.
   b) Dans la section Appareil hôte, sélectionnez le VF que vous avez créé et cliquez sur Terminer.

Figure 4 : VF pour carte réseau Intel 82599 10G

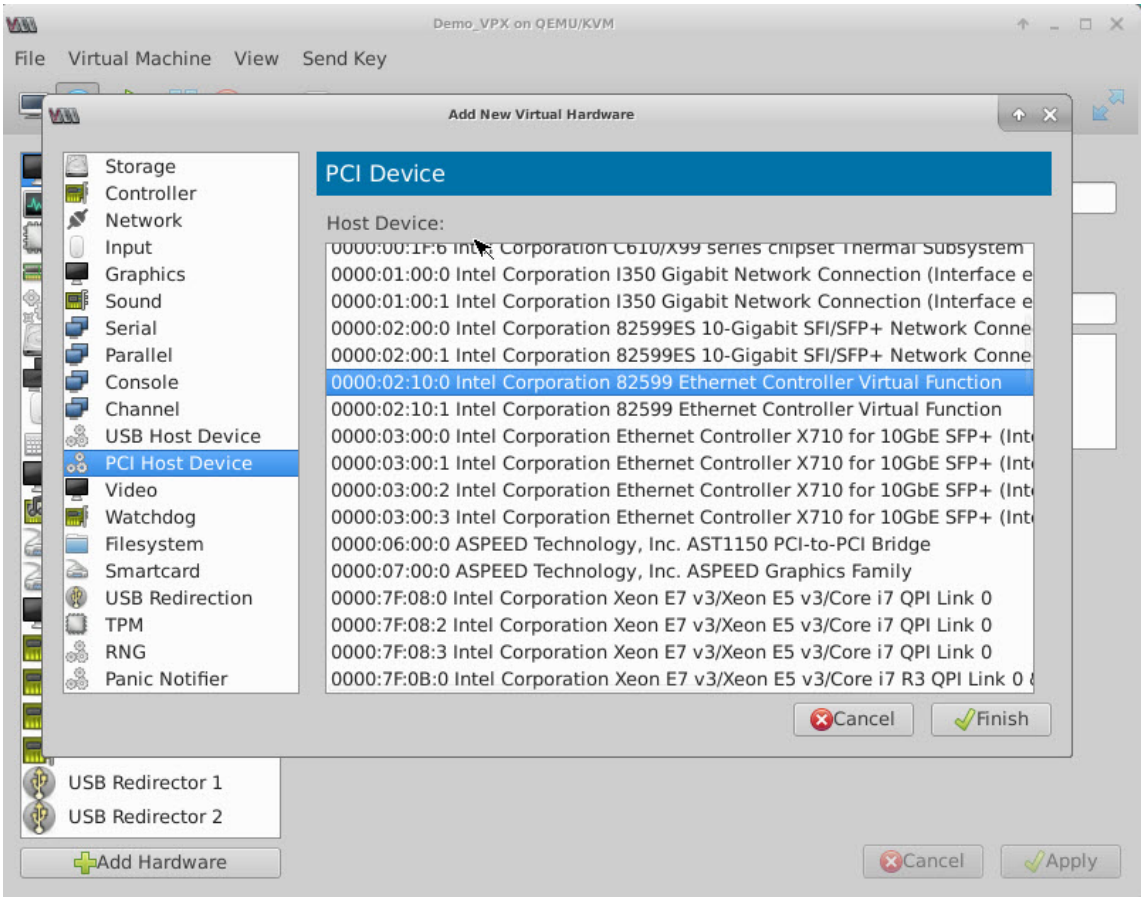


Figure 5 : VF pour carte réseau Intel XL710 40G

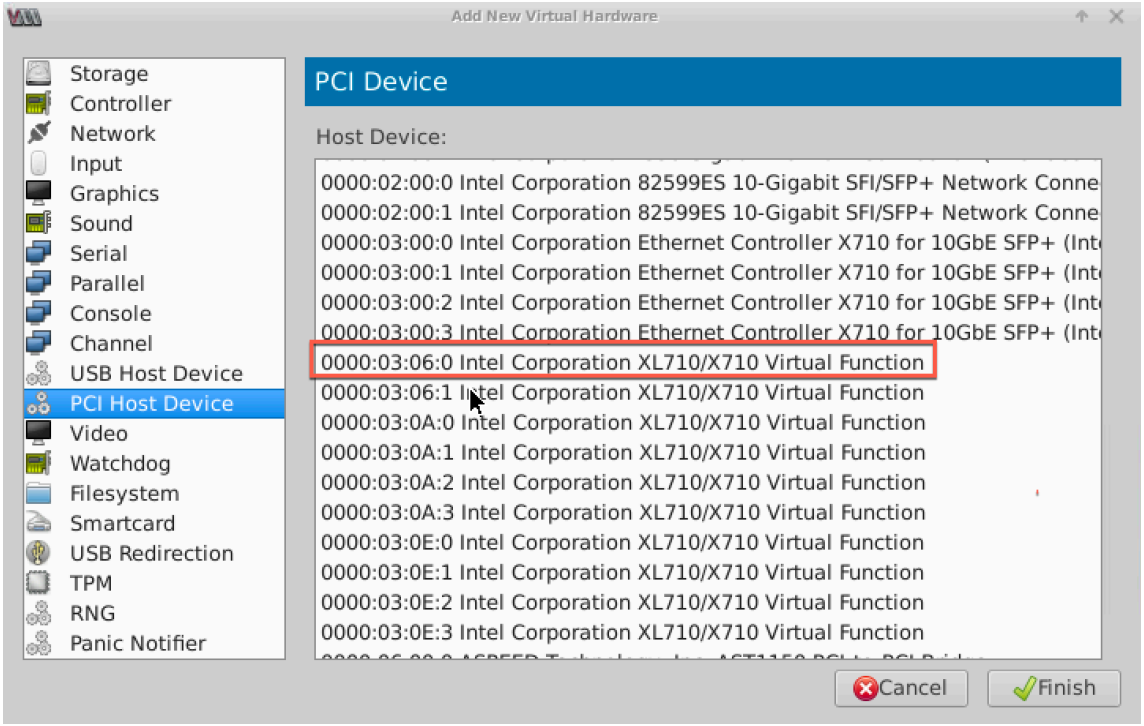
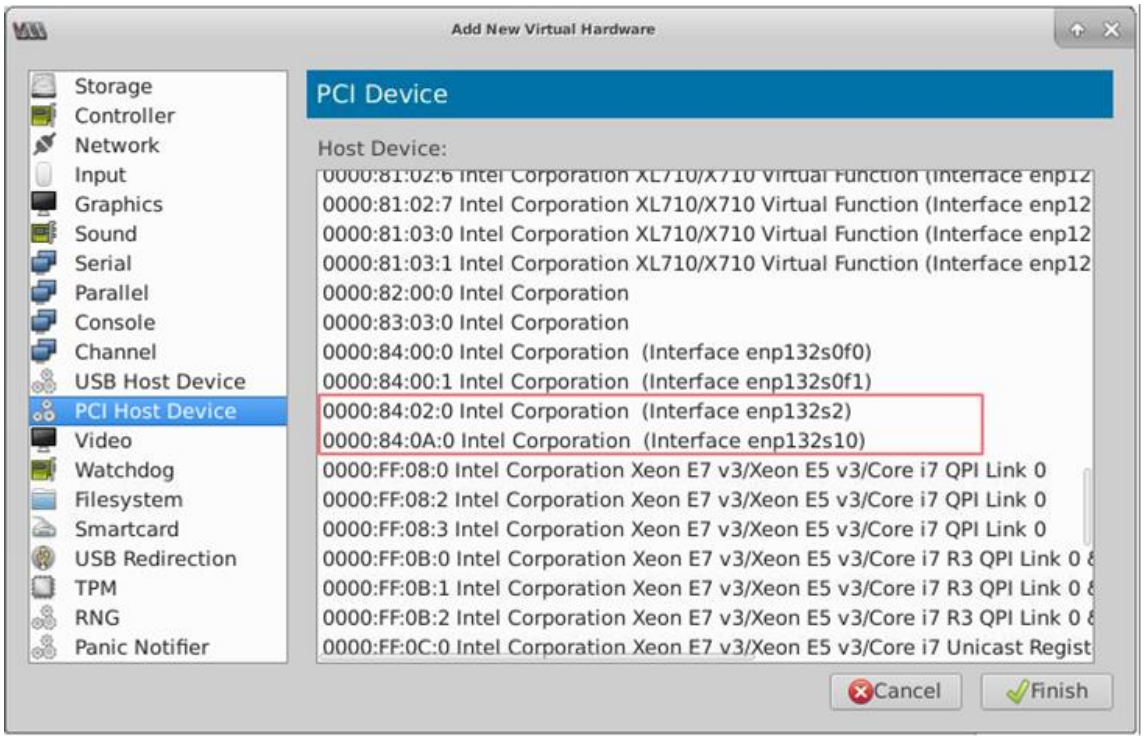


Figure 6 : VF pour carte réseau Intel X722 10G



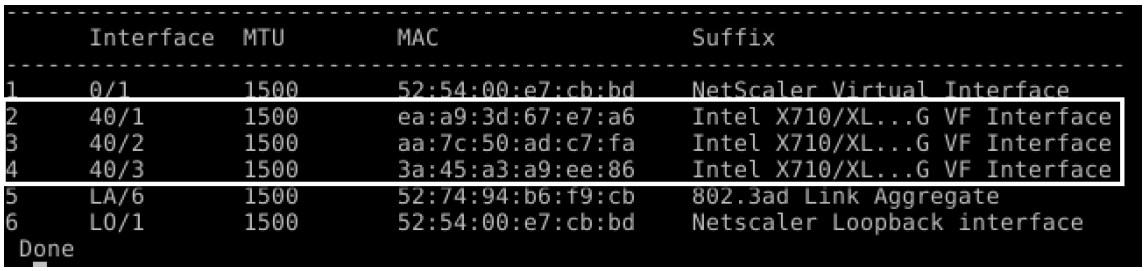
6. Répétez les étapes 4 et 5 pour ajouter les VF que vous avez créées.
7. Allumez l'instance NetScaler VPX.
8. Une fois l'instance NetScaler VPX activée, utilisez la commande suivante pour vérifier la configuration :

```
1    show interface summary
```

La sortie affiche toutes les interfaces que vous avez configurées.

Figure 6 : récapitulatif de sortie pour la carte réseau Intel 82599.

Figure 7. Résumé de la sortie pour les cartes réseau Intel X710 et XL710.



Configurer l'interface LA/LACP statique sur l'interface SR-IOV

> **Important :**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

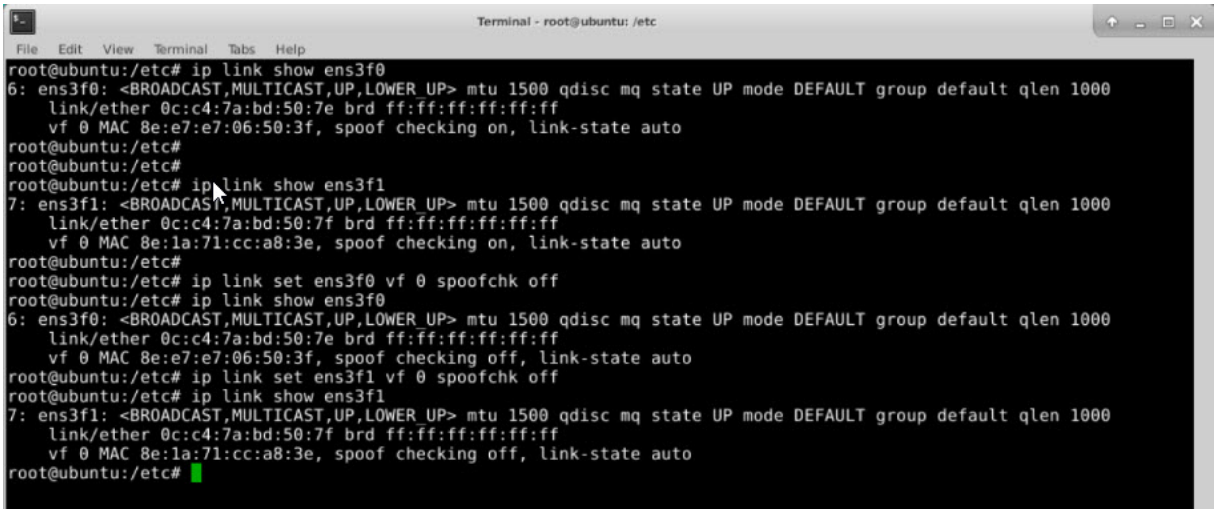
Pour utiliser les VF SR-IOV en mode d'agrégation de liens, désactivez la vérification d'usurpation des VF que vous avez créées. Sur l'hôte KVM, utilisez la commande suivante pour désactiver la vérification d'usurpation :

```
*ip link set \\&#060;interface\\_name\\&#062; vf \\&#060;VF\\_id
\\&#062; spoofchk off*
```

Où :

- Interface_name : est le nom de l'interface.
- vf_id —est l'id de la fonction virtuelle.

Exemple :



Après avoir désactivé la vérification d'usurpation pour toutes les VF que vous avez créées. Redémarrez l'instance NetScaler VPX et configurez l'agrégation de liens. Pour obtenir des instructions détaillées, voir Configuration de l'agrégation de liens.

Configuration du VLAN sur l'interface SR-IOV

Vous pouvez configurer VLAN sur les VF SR-IOV. Pour obtenir des instructions détaillées, reportez-vous à la section Configuration d'un VLAN.

> **Important :**
>
> Assurez-vous que l'hôte KVM ne contient pas de paramètres VLAN pour l'interface VF.

Configurer un NetScaler VPX sur l'hyperviseur KVM pour utiliser Intel QAT pour l'accélération SSL en mode SR-IOV

October 17, 2024

L'instance NetScaler VPX de l'hyperviseur KVM Linux peut utiliser la technologie Intel QuickAssist (QAT) pour accélérer les performances SSL de NetScaler. Grâce à Intel QAT, tous les traitements cryptographiques à latence élevée peuvent être déchargés sur la puce, libérant ainsi un ou plusieurs processeurs hôtes pour effectuer d'autres tâches.

Auparavant, tout le traitement cryptographique des chemins de données NetScaler était effectué dans le logiciel à l'aide de processeurs virtuels hôtes.

> **Remarque :**
>
> Actuellement, NetScaler VPX ne prend en charge que le modèle de puce C62x de la famille Intel QAT. Cette fonctionnalité est prise en charge à partir de la version 14.1 build 8.50 de NetScaler.

Conditions préalables

- L'hôte Linux est équipé d'une puce Intel QAT C62x, soit intégrée directement à la carte mère, soit ajoutée sur une carte PCI externe.

  Modèles de la série Intel QAT C62x : C625, C626, C627, C628. Seuls ces modèles C62x incluent la capacité de cryptage à clé publique (PKE). Les autres variantes C62x ne prennent pas en charge PKE.

- Le NetScaler VPX répond aux exigences matérielles de VMware ESX. Pour plus d'informations, voir Installer une instance NetScaler VPX sur la plate-forme Linux KVM.

Limitations

Aucune disposition n'est prévue pour réserver des unités cryptographiques ou de la bande passante pour des machines virtuelles individuelles. Toutes les unités cryptographiques disponibles de tout matériel Intel QAT sont partagées entre toutes les machines virtuelles utilisant le matériel QAT.

Configuration de l'environnement hôte pour utiliser Intel QAT

1. Téléchargez et installez le pilote fourni par Intel pour le modèle de puce de la série C62x (QAT) sur l'hôte Linux. Pour plus d'informations sur les téléchargements des packages Intel et les instructions d'installation, consultez le pilote de la technologie Intel QuickAssist pour Linux. Un fichier Lisez-moi est disponible dans le package de téléchargement. Un fichier readme est disponible dans le package de téléchargement. Ce fichier fournit des instructions relatives à la compilation et à l'installation du package sur l'hôte.

   Après avoir téléchargé et installé le pilote, effectuez les vérifications d'intégrité suivantes :

   - Notez le nombre de puces C62x. Chaque puce C62x possède jusqu'à 3 terminaux PCIe.
   - Assurez-vous que tous les points de terminaison sont actifs. Exécutez la commande `adf_ctl status` pour afficher l'état de tous les points de terminaison PF (jusqu'à 3).

     ```
     root@Super-Server:~# adf_ctl status

     Checking status of all devices.
     There is 51 QAT acceleration device(s) in the system
     ```

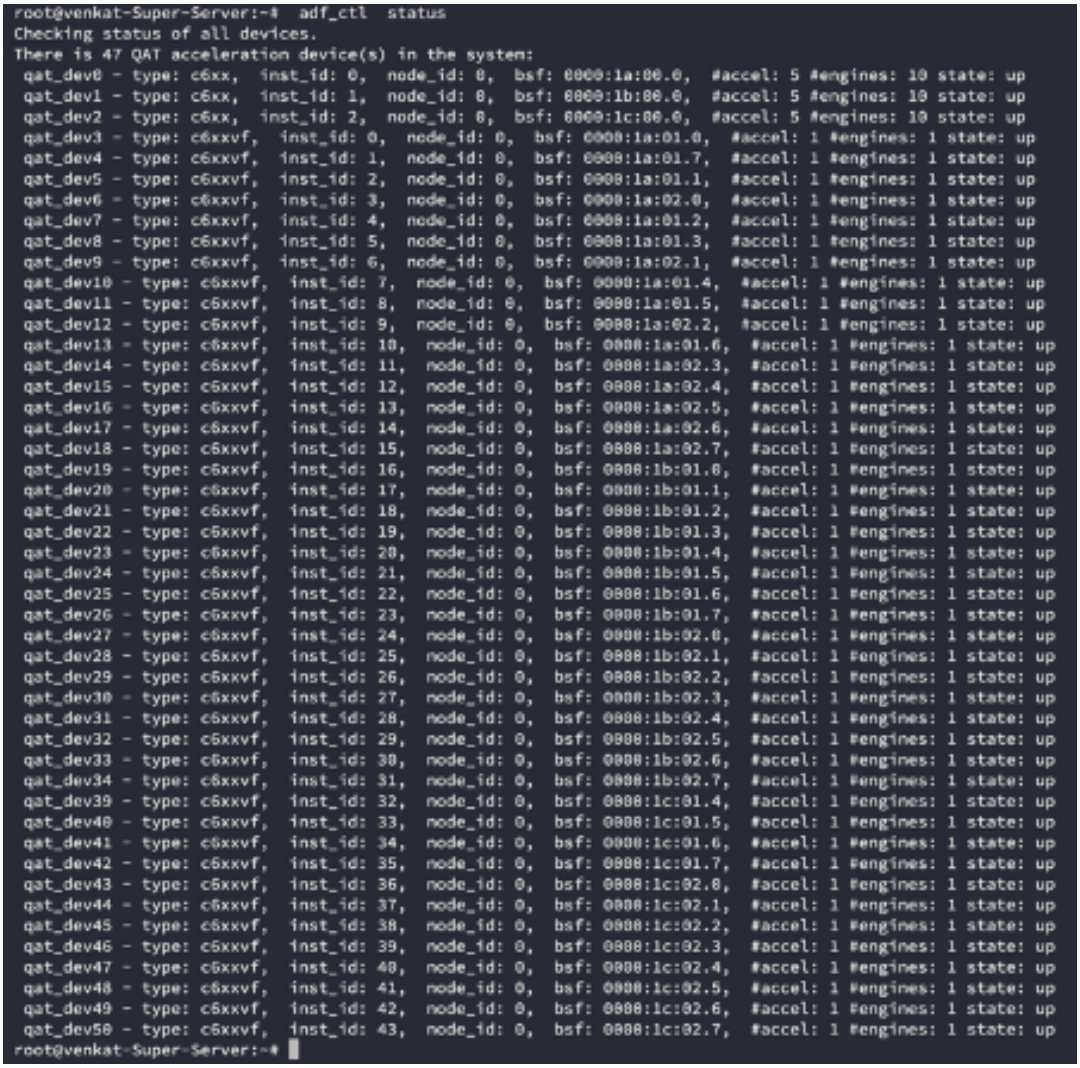


```
5    qat_dev0 - type: c6xx,  inst_id: 0,  node_id: 0,  bsf:
        0000:1a:00.0,  #accel: 5 #engines: 10 state: up
6    qat_dev1 - type: c6xx,  inst_id: 1,  node_id: 0,  bsf:
        0000:1b:00.0,  #accel: 5 #engines: 10 state: up
7    qat_dev2 - type: c6xx,  inst_id: 2,  node_id: 0,  bsf:
        0000:1c:00.0,  #accel: 5 #engines: 10 state: up
```

- Activez SRIOV (support VF) pour tous les terminaux QAT.

```
1    root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1a
        \:00.0/sriov_numvfs
2    root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1b
        \:00.0/sriov_numvfs
3    root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1c
        \:00.0/sriov_numvfs
```

- Assurez-vous que tous les VF sont affichés (16 VF par terminal, soit un total de 48 VF).
- Exécutez la commande adf_ctl status pour vérifier que tous les points de terminaison PF (jusqu'à 3) et les VF de chaque puce Intel QAT sont actifs. Dans cet exemple, le système ne possède qu'une seule puce C62x. Il a donc 51 points de terminaison (3 + 48 VF) au total.



2. Activez SR-IOV sur l'hôte Linux.
3. Créez des machines virtuelles. Lors de la création d'une machine virtuelle, attribuez le nombre approprié de périphériques PCI pour répondre aux exigences de performances.

> **Remarque :**
>
> Chaque puce C62x (QAT) peut comporter jusqu'à trois points de terminaison PCI distincts. Chaque point de terminaison est un ensemble logique de VF et partage la bande passante de manière égale avec les autres points de terminaison PCI de la puce. Chaque terminal peut avoir jusqu'à 16 VF qui apparaissent sous la forme de 16 périphériques PCI. Ajoutez ces appareils à la machine virtuelle pour effectuer l'accélération cryptographique à l'aide de la puce QAT.

Points à noter

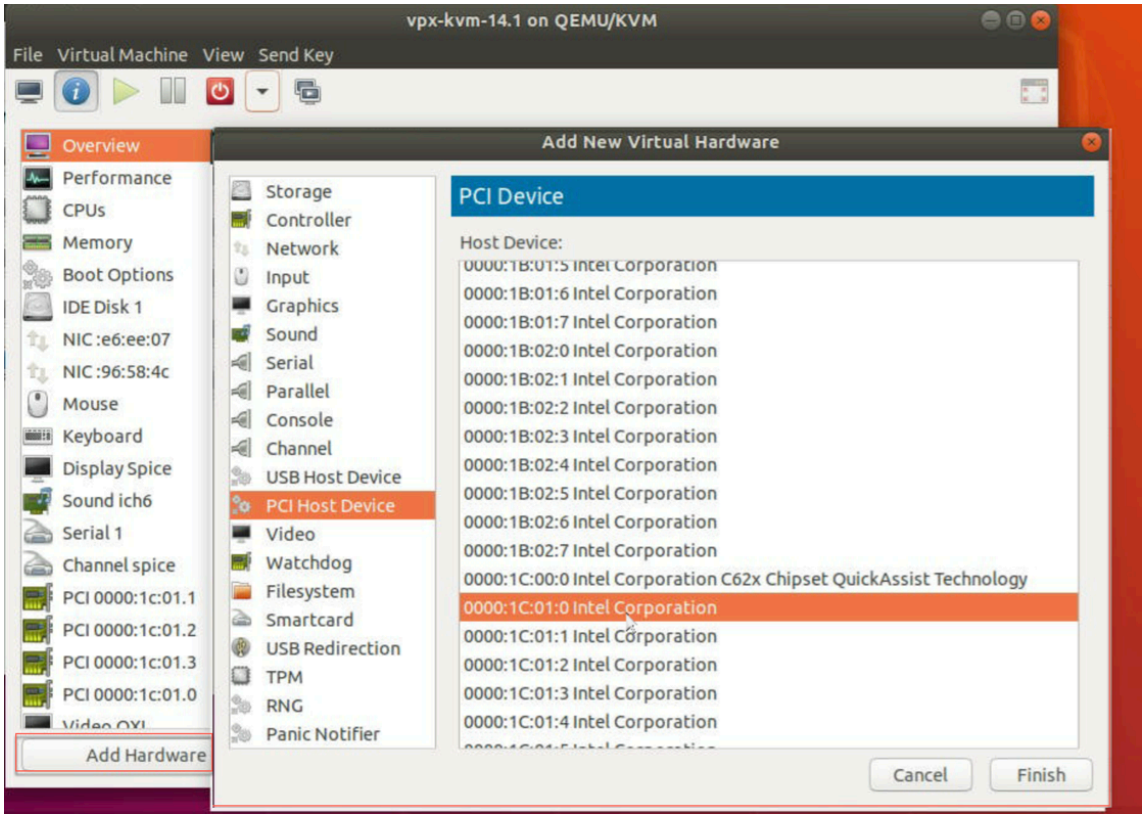
- Si l'exigence de chiffrement des machines virtuelles est d'utiliser plus d'un point de terminaison/puce PCI QAT, nous vous recommandons de sélectionner les dispositifs/VF PCI correspondants de manière circulaire pour obtenir une distribution symétrique.
- Nous recommandons que le nombre de périphériques PCI sélectionnés soit égal au nombre de processeurs virtuels sous licence (sans compter le nombre de processeurs virtuels de gestion). L'ajout d'un nombre de périphériques PCI supérieur au nombre de vCPU disponibles n'améliore pas nécessairement les performances.

  Exemple

  Prenons l'exemple d'un hôte Linux doté d'une puce Intel C62x dotée de 3 terminaux. Lors du provisionnement d'une machine virtuelle avec 6 vCPU, choisissez 2 VF sur chaque point de terminaison et attribuez-les à la machine virtuelle. Cette attribution garantit une distribution efficace et égale des unités cryptographiques pour la machine virtuelle. Parmi le total des vCPU disponibles, par défaut, un vCPU est réservé au plan de gestion, et les autres vCPU sont disponibles pour les PE du plan de données.

Attribuez des VF QAT à NetScaler VPX déployé sur un hyperviseur KVM Linux

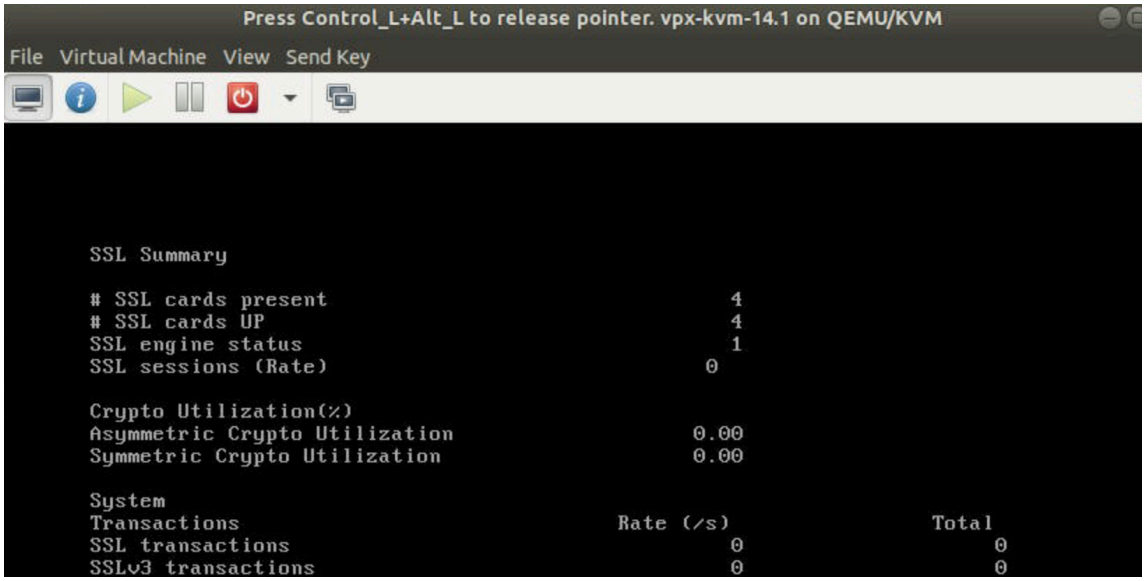
1. Dans le gestionnaire de machines virtuelles Linux KVM, assurez-vous que la machine virtuelle (NetScaler VPX) est hors tension.
2. Accédez à **Ajouter du matériel > Périphérique hôte PCI**.
3. Assignez Intel QAT VF au périphérique PCI.



4. Cliquez sur **Terminer**.
5. Répétez les étapes précédentes pour attribuer un ou plusieurs Intel QAT VF à l'instance NetScaler VPX dans la limite d'un de moins que le nombre total de vCPU. Parce qu'un seul processeur virtuel est réservé au processus de gestion.

   Nombre de VF QAT par machine virtuelle = nombre de processeurs virtuels - 1
6. Power on the VM.
7. Exécutez la commande `stat ssl` dans la CLI NetScaler pour afficher le résumé SSL et vérifiez les cartes SSL après avoir attribué des VF QAT à NetScaler VPX.

   Dans cet exemple, nous avons utilisé 5 vCPU, ce qui implique 4 moteurs de paquets (PE).



À propos du déploiement

Ce déploiement a été testé avec les spécifications des composants suivantes :

- **Version et build de NetScaler VPX** : 14,1—8,50
- **Version d'Ubuntu :** 18.04, noyau 5.4.0-146
- **Version du pilote Intel C62x QAT pour Linux** : L.4.21.0-00001

Configurer une instance NetScaler VPX pour utiliser des interfaces réseau PCI passthrough

October 17, 2024

Après avoir installé et configuré une instance NetScaler VPX sur la plate-forme Linux-KVM, vous pouvez utiliser le Virtual Machine Manager pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau PCI passthrough.

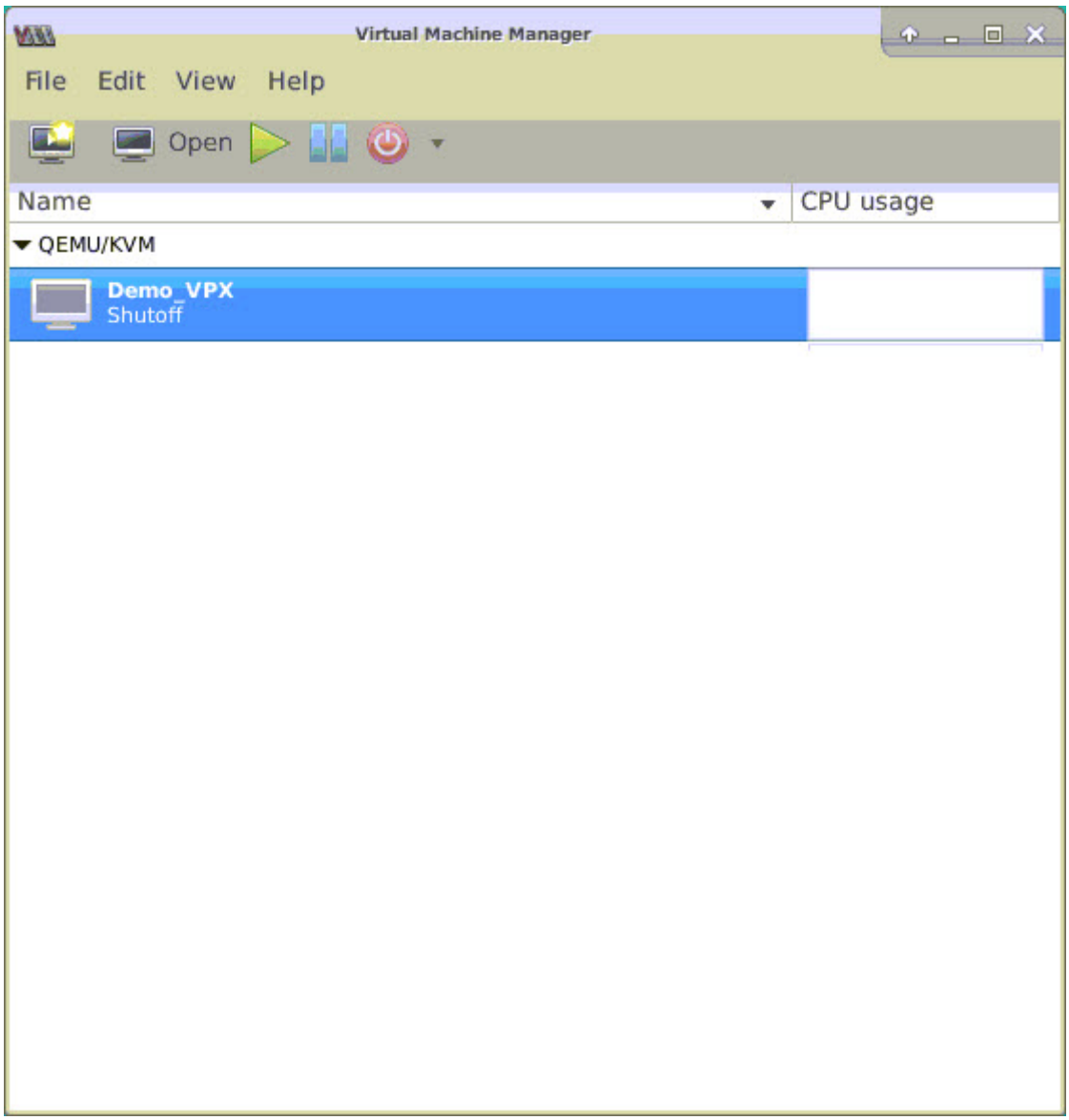
Conditions préalables

- La version du microprogramme de la carte réseau (NIC) Intel XL710 sur l'hôte KVM est 5.04.
- L'hôte KVM prend en charge l'unité de gestion de la mémoire d'entrée-sortie (IOMMU) et Intel VT-d, et ils sont activés dans le BIOS de l'hôte KVM. Sur l'hôte KVM, pour activer IOMMU, ajoutez l'entrée suivante au fichier **/boot/grub2/grub.cfg**:**intel_iommu=1**

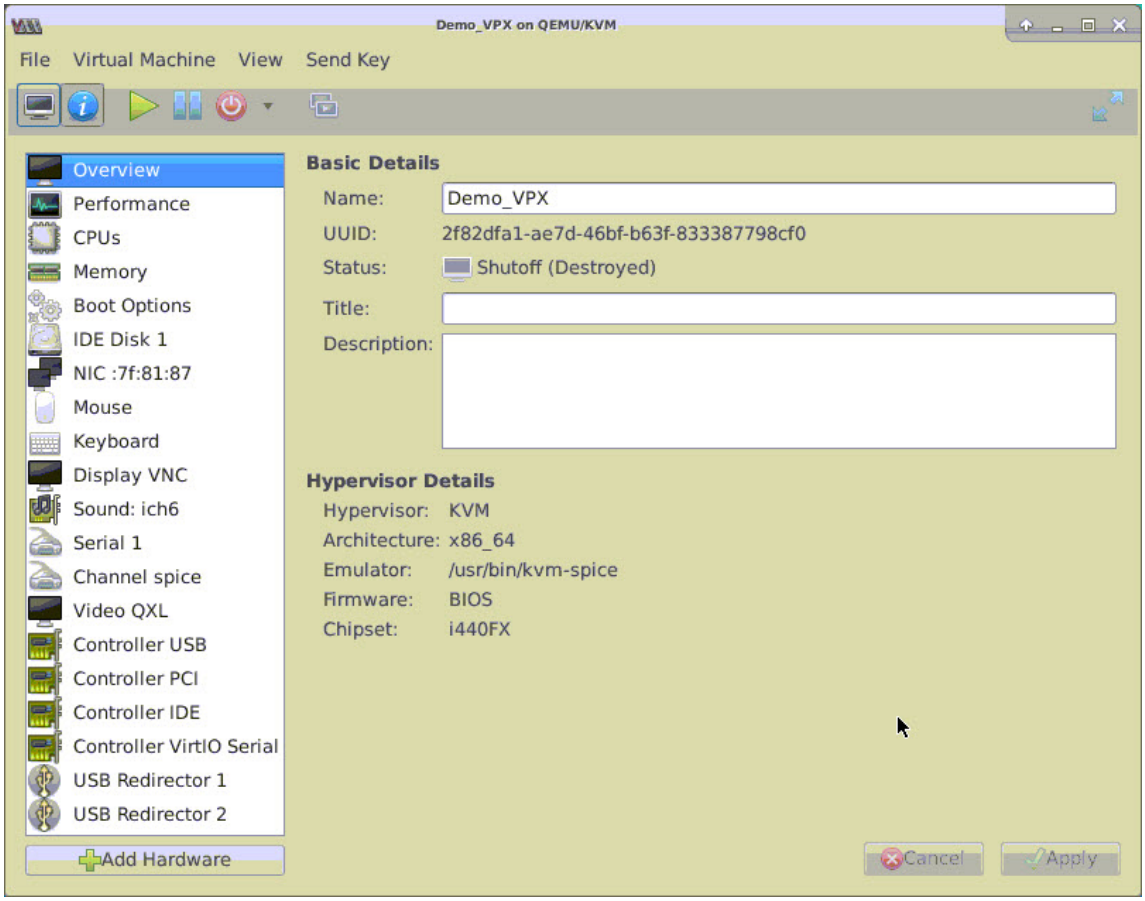
- Exécutez la commande suivante et redémarrez l'hôte KVM : **GRUB2-MKConfig —o /boot/-grub2/grub.cfg**

Pour configurer les instances NetScaler VPX afin qu'elles utilisent des interfaces réseau passthrough PCI à l'aide du Virtual Machine Manager :

1. Éteignez l'instance NetScaler VPX.
2. Sélectionnez l'instance NetScaler VPX et cliquez sur Ouvrir.



3. Dans la fenêtre **Virtual_machine sur KVM**, cliquez sur l'icône **i.**

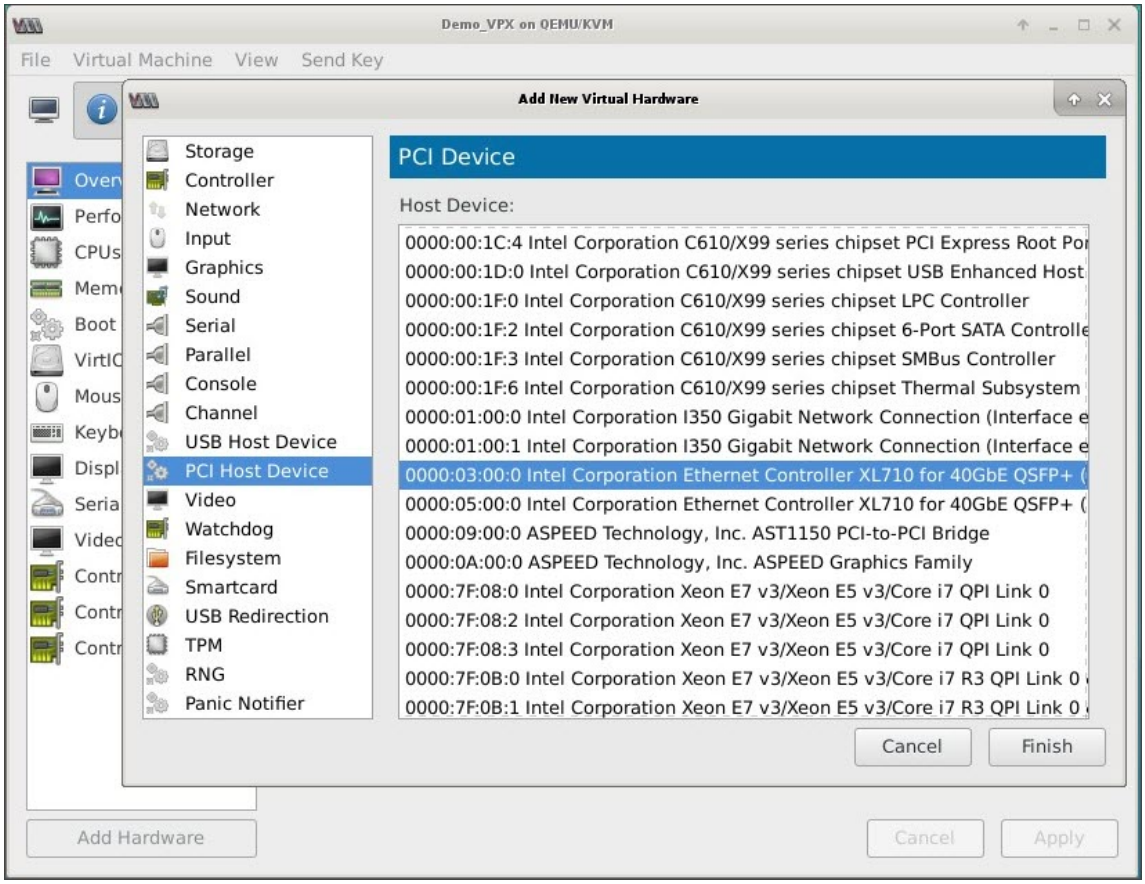


4. Cliquez sur **Ajouter du matériel**.
5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a. Sélectionnez un **périphérique hôte PCI**.

   b. Dans la section **Appareil hôte**, sélectionnez la fonction physique du processeur Intel XL710.

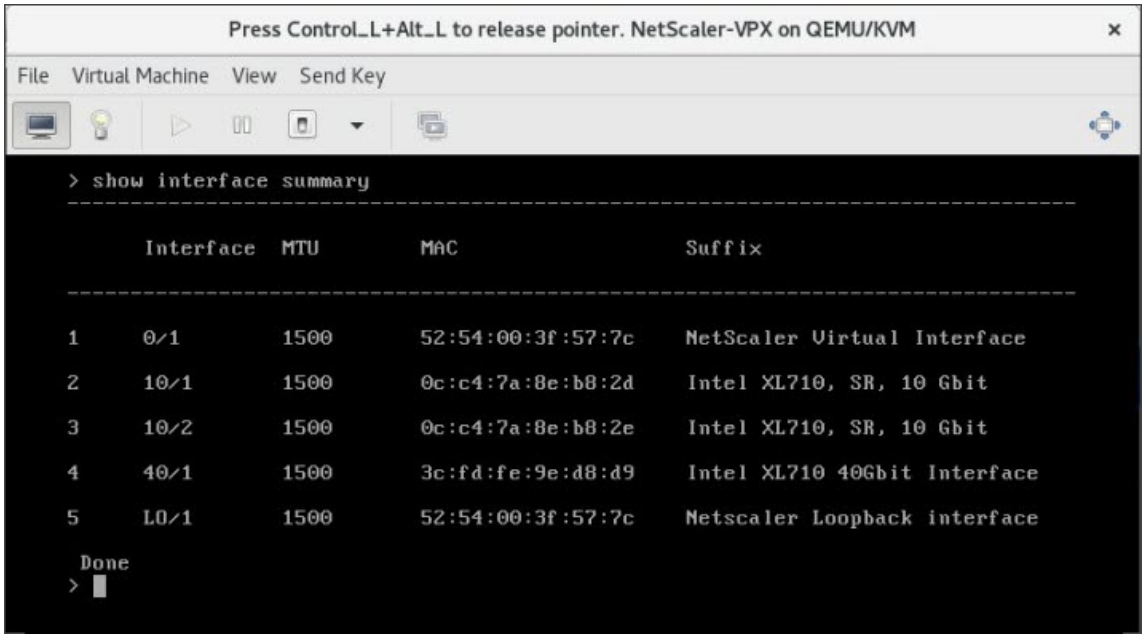
   c. Cliquez sur **Terminer**.



6. Répétez les étapes **4** et **5** pour ajouter d'autres fonctions physiques Intel XL710.
7. Allumez l'instance NetScaler VPX.
8. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

```
COMMAND
> show interface summary
```

La sortie doit afficher toutes les interfaces que vous avez configurées :



Provisionnez l'instance NetScaler VPX à l'aide du programme virsh

October 17, 2024

Le `virsh` programme est un outil de ligne de commande permettant de gérer les invités de machines virtuelles. Sa fonctionnalité est similaire à celle de Virtual Machine Manager. Il vous permet de modifier l'état d'un invité VM (démarrage, arrêt, pause, etc.), de configurer de nouveaux invités et appareils et de modifier les configurations existantes. Le `virsh` programme est également utile pour le script des opérations de gestion des invités de machines virtuelles.

Pour provisionner NetScaler VPX à l'aide du `virsh` programme, procédez comme suit :

1. Utilisez la commande tar pour décompresser le package NetScaler VPX. Le package NSVPX-KVM-*_NC.tgz contient les composants suivants :

   - Fichier XML de domaine spécifiant les attributs VPX [NSVPX-KVM-*_NC.xml]
   - Vérifiez la somme des images de disque NS-VM [Checksum.txt]
   - Image de disque NS-VM [NSVPX-KVM-*_NC.raw]

   Exemple

   ```
   tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
   NSVPX-KVM-10.1-117_nc.xml
   NSVPX-KVM-10.1-117_nc.raw
   checksum.txt
   ```


2. Copiez le fichier XML NSVPX-KVM-*_nc.xml dans un fichier nommé \\<DomainName\\>-NSVPX-KVM-*_nc.xml. Le <DomainName> est également le nom de la machine virtuelle. Exemple

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.xml
```

3. Modifiez le fichier \\<DomainName\\>-NSVPX-KVM-*_nc.xml pour spécifier les paramètres suivants :

   - name (name) : spécifiez le nom.
   - Mac : spécifiez l'adresse MAC.

     > **Remarque :**
     >
     > Le nom de domaine et l'adresse MAC doivent être uniques.

   - fichier source : spécifiez le chemin absolu de la source de l'image disque. Le chemin du fichier doit être absolu. Vous pouvez spécifier le chemin du fichier image RAW ou d'un fichier image QCOW2.

     Si vous souhaitez spécifier un fichier image RAW, spécifiez le chemin source de l'image disque comme indiqué dans l'exemple suivant :

     Exemple

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
```

     Spécifiez le chemin source absolu de l'image disque QCOW2 et définissez le type de pilote comme **qcow2**, comme indiqué dans l'exemple suivant :

     Exemple

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<driver name ='qemu' type='qcow2'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
```

4. Modifiez le fichier \\<DomainName\\>-NSVPX-KVM-*_nc.xml pour configurer les détails du réseau :

   - source dev : spécifiez l'interface.
   - mode : spécifiez le mode. L'interface par défaut est **Macvtap Bridge**.

   Exemple : Mode : MacVTap Bridge Définissez l'interface cible comme ethx et le mode comme pont Type de modèle comme virtio


```
    <interface type='direct'>
        <mac address='52:54:00:29:74:b3'/>
        <source dev='eth0' mode='bridge'/>
        <target dev='macvtap0'/>
        <model type='virtio'/>
        <alias name='net0'/>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
            function='0x0'/>
      </interface>
```

Ici, eth0 est l'interface physique attachée à la machine virtuelle.

5. Définissez les attributs de la VM dans le fichier \\<DomainName\\>-NSVPX-KVM-*_nc.xml en utilisant la commande suivante :

```
virsh define \<DomainName\>-NSVPX-KVM-\*\_nc.xml
```

Exemple

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

6. Démarrez la VM en entrant la commande suivante :

```
virsh start \[\<DomainName\> | \<DomainUUID\>\]
```

Exemple

```
virsh start NetScaler-VPX
```

7. Connectez la machine virtuelle invitée via la console:

```
virsh console \[\<DomainName\> | \<DomainUUID\> |\<DomainID\> \]
```

Exemple

```
virsh console NetScaler-VPX
```

Ajouter d'autres interfaces à l'instance NetScaler VPX à l'aide du programme `virsh`

Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit :

1. Arrêtez l'instance NetScaler VPX exécutée sur le KVM.
2. Modifiez le fichier \\<DomainName\\>-NSVPX-KVM-*_nc.xml à l'aide de la commande :


```
virsh edit \[\<DomainName\> | \<DomainUUID\>\]
```

3. Dans le fichier \\<DomainName\\>-NSVPX-KVM-*_nc.xml , ajoutez les paramètres suivants :

   a) **Pour MacVTap**

   - Type d'interface : spécifiez le type d'interface comme « direct ».
   - Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
   - source dev : spécifiez le nom de l'interface.
   - mode : spécifiez le mode. Les modes pris en charge sont : Bridge, VEPA, Private et Pass-Through
   - type de modèle : spécifiez le type de modèle comme `virtio`

   Exemple

   Mode : Pass-through MacVTap

   Définir l'interface cible comme `ethx`, Mode comme pont et type de modèle comme `virtio`

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
```

   Ici eth1 est l'interface physique attachée à la machine virtuelle.

   b) **Pour le mode Bridge**

   > **Remarque :**
   >
   > Assurez-vous d'avoir configuré un pont Linux dans l'hôte KVM, lié l'interface physique au pont et mis le pont dans l'état UP.

   - Type d'interface : spécifiez le type d'interface comme « pont ».
   - Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
   - pont source : spécifiez le nom du pont.
   - type de modèle : spécifiez le type de modèle comme `virtio`

   Exemple : Mode Pont

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
```



```
5     </interface>
```

Gérer les machines virtuelles clientes NetScaler VPX

October 17, 2024

Vous pouvez utiliser Virtual Machine Manager et le `virsh` programme pour effectuer des tâches de gestion telles que le démarrage ou l'arrêt d'un invité de machine virtuelle, la configuration de nouveaux invités et de nouveaux périphériques, la modification de configurations existantes et la connexion à la console graphique via Virtual Network Computing (VNC).

Gérer les machines virtuelles invitées VPX à l'aide de Virtual Machine Manager

- Lister les invités de la machine virtuelle

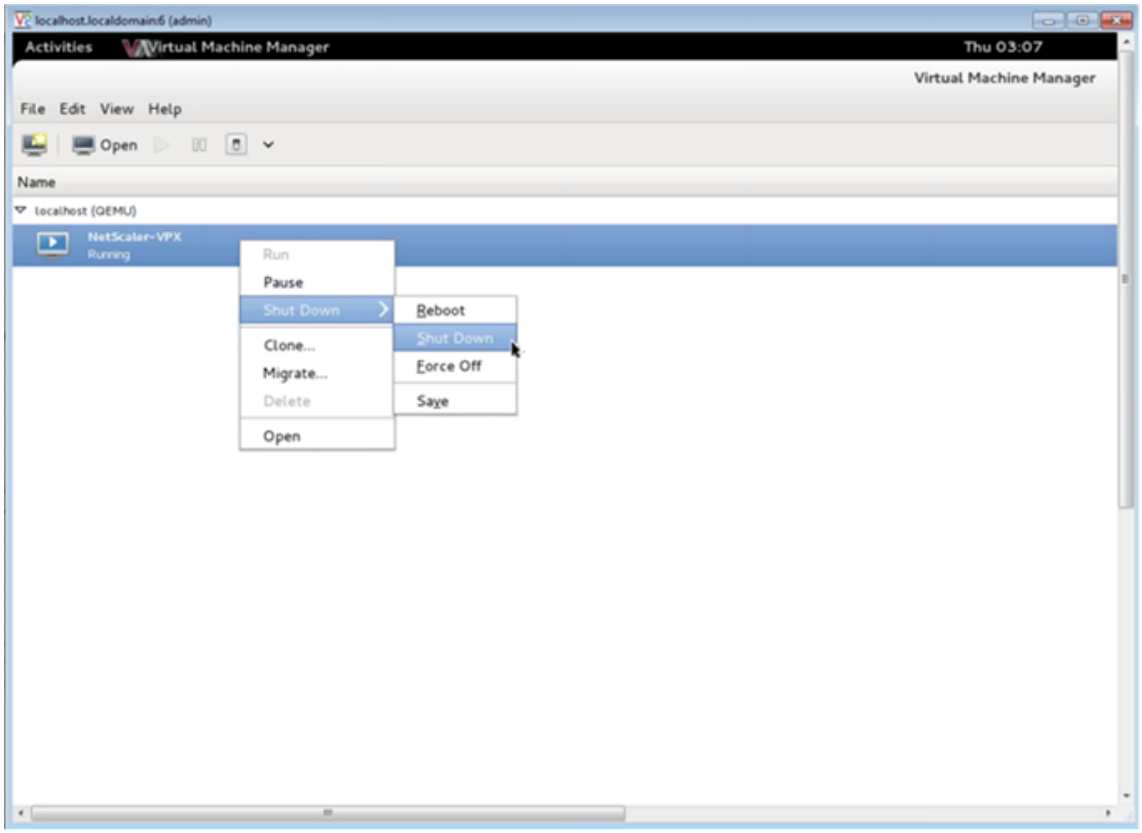
  La fenêtre principale du Virtual Machine Manager affiche une liste de tous les invités de machine virtuelle pour chaque serveur hôte de machine virtuelle auquel il est connecté. Chaque entrée Invité de machine virtuelle contient le nom de la machine virtuelle, ainsi que son état (en cours d'exécution, pause ou arrêt) affiché comme dans l'icône.

- Ouvrir une console graphique

  L'ouverture d'une console graphique à une machine virtuelle invitée vous permet d'interagir avec la machine comme vous le feriez avec un hôte physique via une connexion VNC. Pour ouvrir la console graphique dans Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez l'option Ouvrir dans le menu contextuel.

- Démarrage et arrêt d'un invité

  Vous pouvez démarrer ou arrêter un invité de machine virtuelle à partir du Virtual Machine Manager. Pour modifier l'état de la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez Exécuter ou l'une des options d'arrêt dans le menu contextuel.



- Redémarrer un invité

  Vous pouvez redémarrer une machine virtuelle invitée à partir du Virtual Machine Manager. Pour redémarrer la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest, puis sélectionnez Arrêter > Redémarrer dans le menu contextuel.

- Supprimer un invité

  La suppression d'un invité de machine virtuelle entraîne la suppression de sa configuration XML par défaut. Vous pouvez également supprimer les fichiers de stockage d'un invité. Cela efface complètement l'invité.

  1. Dans le Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest.
  2. Sélectionnez Supprimer dans le menu contextuel. Une fenêtre de confirmation s'ouvre.

     > **Remarque :**
     >
     > L'option Supprimer est activée uniquement lorsque l'invité VM est arrêté.

  3. Cliquez sur **Delete**.
  4. Pour effacer complètement l'invité, supprimez le fichier .raw associé en cochant la case Supprimer les fichiers de stockage associés.

Gérez les machines virtuelles clientes NetScaler VPX à l'aide du programme `virsh`

- Répertorier les invités VM et leurs états actuels.

  Pour utiliser `virsh` pour afficher des informations sur les invités

  ```
  virsh list --all
  ```

  La sortie de la commande affiche tous les domaines avec leurs états. Exemple de sortie :

  ```
  Id Name                 State
  ----------------------------------
    0 Domain-0            running
    1 Domain-1            paused
    2 Domain-2            inactive
    3 Domain-3            crashed
  ```

- Ouvrez une console `virsh`.

  Connectez la machine virtuelle invitée via la console

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple

  ```
  virsh console NetScaler-VPX
  ```

- Démarrez et arrêtez un invité.

  Les invités peuvent être créés à l'aide du nom de domaine ou de l'UUID du domaine.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Exemple

  ```
  virsh start NetScaler-VPX
  ```

  Pour arrêter un invité :

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple

  ```
  virsh shutdown NetScaler-VPX
  ```

- Redémarrer un invité

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple

  ```
  virsh reboot NetScaler-VPX
  ```

  Supprimer un invité

  Pour supprimer une machine virtuelle invitée, vous devez arrêter l'hôte et annuler la définition du fichier <DomainName>-NSVPX-KVM-*_nc.xml avant d'exécuter la commande delete.


```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
```

Exemple

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
```

> **Remarque :**
>
> La commande de suppression ne supprime pas le fichier image disque qui doit être supprimé manuellement.

Provisionner l'instance NetScaler VPX avec SR-IOV, sur OpenStack

October 17, 2024

Vous pouvez déployer des instances NetScaler VPX hautes performances qui utilisent la technologie de virtualisation des E/S à racine unique (SR-IOV) sur OpenStack.

Vous pouvez déployer une instance NetScaler VPX qui utilise la technologie SR-IOV, sur OpenStack, en trois étapes :

- Activez SR-IOV Virtual Functions (VF) sur l'hôte.
- Configurez et rendez les VFS disponibles pour OpenStack.
- Provisionnez le NetScaler VPX sur OpenStack.

Conditions préalables

Assurez-vous que vous :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Téléchargez et installez le dernier pilote IXGBE d'Intel.
- Liste de blocage du pilote IXGBEVF sur l'hôte. Ajoutez l'entrée suivante dans le fichier /etc/modprobe.d/blacklist.conf : Liste des blocs `ixgbevf`

> **Remarque :**
>
> La version du `ixgbe` pilote doit être minimale 5.0.4.

Activer les VF SR-IOV sur l'hôte

Pour activer les VF SR-IOV, effectuez l'une des opérations suivantes :

- <number_of_VFs>Si vous utilisez une version du noyau antérieure à 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/ixgbe et redémarrez l'hôte : options ixgbe max_vfs=
- Si vous utilisez le noyau 3.8 version ou ultérieure, créez des VF à l'aide de la commande suivante :

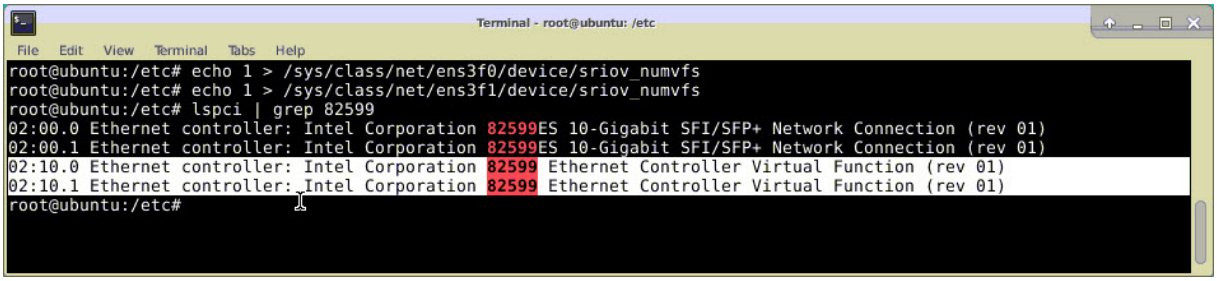
```
1        echo <number_of_VFs> > /sys/class/net/<device_name>/device/
            sriov_numvfs
```

Où :

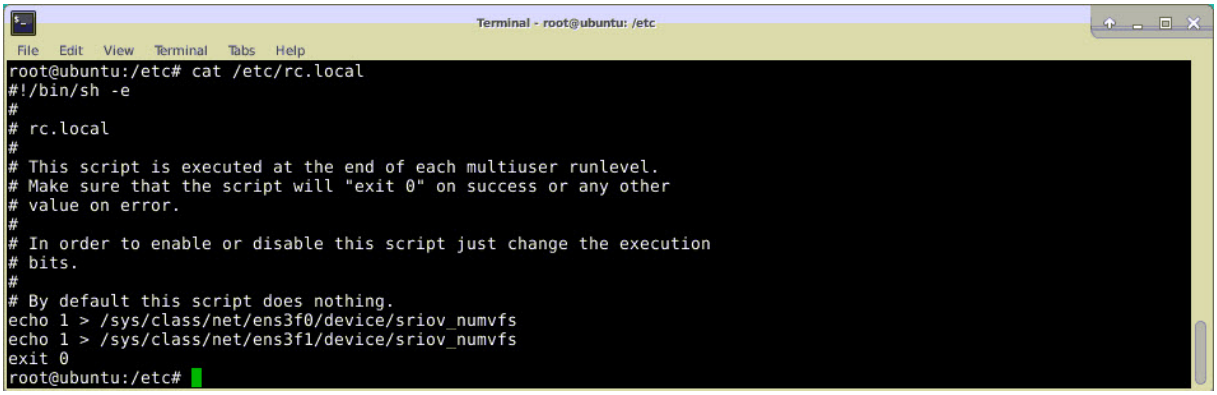
- Number_of_VFS est le nombre de fonctions virtuelles que vous souhaitez créer.
- nom_périphérique est le nom de l'interface.

> **Important :**
>
> Lorsque vous créez les VF SR-IOV, assurez-vous que vous n'attribuez pas d'adresses MAC aux VF.

Voici un exemple de quatre VF en cours de création.



Rendez les VFS persistants, ajoutez les commandes que vous avez utilisées pour créer des VFS au fichier **rc.local** . Voici un exemple montrant le contenu du fichier rc.local.



Pour plus d'informations, consultez ce guide de configuration Intel SR-IOV.

Configurer et rendre les VFS disponibles pour OpenStack

Suivez les étapes indiquées sur le lien ci-dessous pour configurer SR-IOV sur OpenStack :https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking.

Provisionner l'instance NetScaler VPX sur OpenStack

Vous pouvez provisionner une instance NetScaler VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack.

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se fixe à l'instance lors du démarrage. Ce lecteur de configuration peut être utilisé pour transmettre des informations de configuration réseau telles que l'adresse IP de gestion, le masque réseau et la passerelle par défaut, etc., à l'instance avant de configurer les paramètres réseau de l'instance.

Lorsque OpenStack provisionnera une instance VPX, il détecte d'abord que l'instance démarre dans un environnement OpenStack, en lisant une chaîne de BIOS spécifique (OpenStack Foundation) qui indique OpenStack. Pour les distributions Red Hat Linux, la chaîne est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plate-forme hyper-viseur KVM. Le disque doit comporter une étiquette OpenStack spécifique. Si le lecteur de configuration est détecté, l'instance tente de lire les informations suivantes à partir du nom de fichier spécifié dans la commande de nova démarrage. Dans les procédures ci-dessous, le fichier est appelé « userdata.txt ».

- Adresse IP de gestion
- Masque réseau
- Gateway par défaut

Une fois les paramètres lus avec succès, ils sont remplis dans la pile NetScaler. Cela aide à gérer l'instance à distance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- Si DHCP échoue ou temporisation, l'instance affiche la configuration réseau par défaut (192.168.100.1/16).

Provisionner l'instance NetScaler VPX sur OpenStack via l'interface de ligne de commande

Vous pouvez provisionner une instance VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack. Voici le résumé des étapes à suivre pour provisionner une instance NetScaler VPX sur OpenStack :

1. Extraction du `.qcow2` fichier du fichier .tgz
2. Création d'une image OpenStack à partir de l'image qcow2
3. Provisionnement d'une instance VPX

Pour provisionner une instance VPX dans un environnement OpenStack, procédez comme suit.

1. Extrayez le. `qcow2` fichier à partir du `.tqz` fichier en tapant la commande :

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante :

```
glance image-create --name="<name of the OpenStack image>" --
   property hw_disk_bus=ide --is-public=true --container-format=
   bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
   hw_disk_bus=ide --is-public= true --container-format=bare --
   disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
```

L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.


```
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| checksum         | 735dae4ea6e46e39ed3f0acfba02e755     |
| container_format | bare                                 |
| created_at       | 2017-02-16T10:03:29Z                 |
| disk_format      | qcow2                                |
| hw_disk_bus      | ide                                  |
| id               | aeaa13e9-b49b-411c-ab54-c61820a8e2f3 |
| min_disk         | 0                                    |
| min_ram          | 0                                    |
| name             | NSVPX-KVM-12.0-26.2                  |
| owner            | 06c41a73b32f4b48af55359fd7d3502c     |
| protected        | False                                |
| size             | 717946880                            |
| status           | active                               |
| tags             | []                                   |
| updated_at       | 2017-02-16T10:03:38Z                 |
| virtual_size     | None                                 |
| visibility       | private                              |
+------------------+--------------------------------------+
```

3. Une fois qu'une image OpenStack est créée, provisionnez l'instance NetScaler VPX.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1.   medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
```

Dans la commande précédente, userdata.txt est le fichier qui contient les détails tels que l'adresse IP, le masque de réseau et la passerelle par défaut de l'instance VPX. Le fichier de données utilisateur est un fichier personnalisable par l'utilisateur. NSVPX-KVM-12.0-26.2 est le nom de l'appliance virtuelle que vous souhaitez provisionner. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 est le VF OpenStack.

L'illustration suivante donne un exemple de sortie de la commande nova boot.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

L'illustration suivante montre un exemple du fichier userdata.txt. Les valeurs contenues dans les\

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
    "
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
    1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"
    />
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
```



```
    oe:value="10.1.0.1"/>
    </PropertySection>
    </Environment>
```

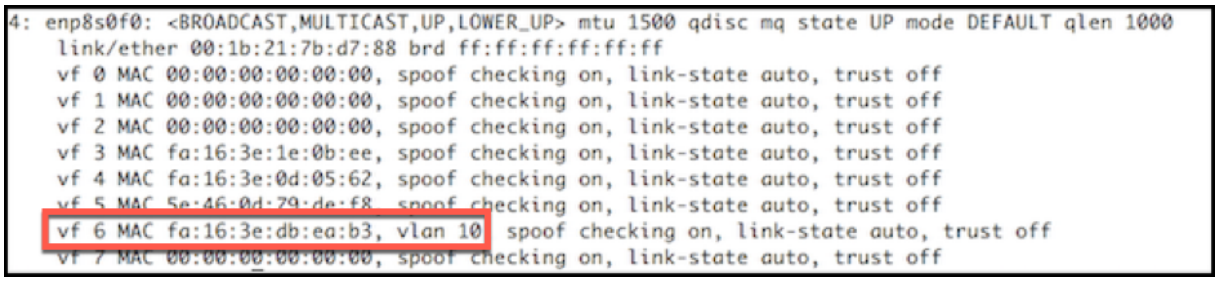
Configurations supplémentaires prises en charge : création et suppression de VLAN sur des VF SR-IOV de l'hôte

Tapez la commande suivante pour créer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 10
```

Dans la commande précédente, « enp8s0f0"est le nom de la fonction physique.

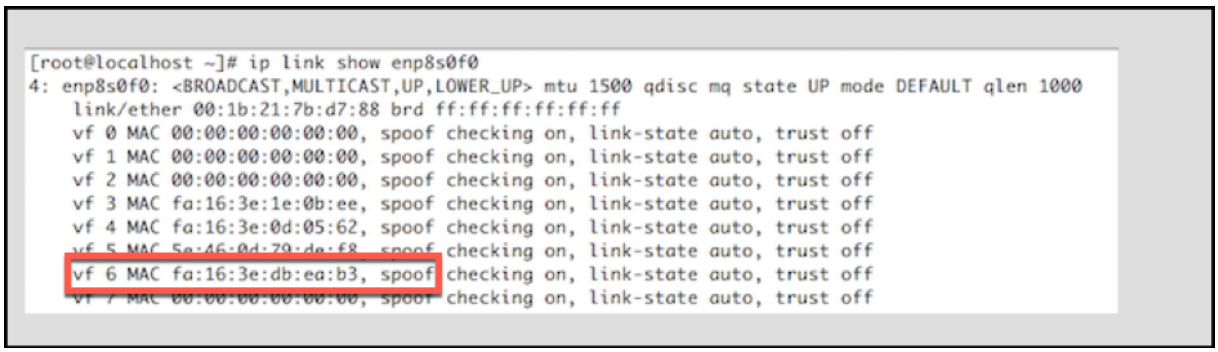
Exemple : VLAN 10, créé sur vf 6



Tapez la commande suivante pour supprimer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 0
```

Exemple : VLAN 10, supprimé de vf 6



Ces étapes complètent la procédure de déploiement d'une instance NetScaler VPX qui utilise la technologie SRIOV sur OpenStack.

Configurer une instance NetScaler VPX sur KVM pour utiliser les interfaces hôtes basées sur OVS DPDK

October 17, 2024

Vous pouvez configurer une instance NetScaler VPX exécutée sur KVM (Fedora et RHOS) pour utiliser Open vSwitch (OVS) avec le kit de développement Data Plane (DPDK) afin d'améliorer les performances du réseau. Ce document explique comment configurer l'instance NetScaler VPX pour qu'elle fonctionne sur les `vhost-user` ports exposés par OVS-DPDK sur l'hôte KVM.

OVS est un commutateur virtuel multicouche sous licence Apache 2.0 open source. DPDK est un ensemble de bibliothèques et de pilotes permettant un traitement rapide des paquets.

Les versions suivantes de Fedora, RHOS, OVS et DPDK sont qualifiées pour configurer une instance NetScaler VPX :

Fedora	RHOS
Fedora 25	RHOS 7,4
OS 2.7.0	VERSION 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Conditions préalables

Avant d'installer DPDK, assurez-vous que l'hôte dispose de pages gigantesques de 1 Go.

Pour plus d'informations, consultez cette documentation relative à la configuration système requise pour DPDK. Voici un résumé des étapes requises pour configurer une instance NetScaler VPX sur KVM afin d'utiliser des interfaces hôtes basées sur OVS DPDK :

- Installez DPDK.
- Créez et installez OVS.
- Créez un pont OVS.
- Attachez une interface physique au pont OVS.
- Connectez des `vhost-user` ports au chemin de données OVS.
- Provisionnez un KVM-VPX avec des `vhost-user` ports OVS-DPDK.

Installer DPDK

Pour installer DPDK, suivez les instructions données dans ce document Open vSwitch with DPDK .

Construire et installer OVS

Téléchargez OVS depuis la page de téléchargementd'OVS. Ensuite, créez et installez OVS à l'aide d'un chemin de données DPDK. Suivez les instructions fournies dans le document Installer Open vSwitch .

Pour plus d'informations, consultez DPDK Getting Started Guide for Linux.

Créer un pont OVS

Selon vos besoins, tapez la commande Fedora ou RHOS pour créer un pont OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
   datapath_type=netdev
```

Commande RHOS :

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

Raccorder l'interface physique au pont OVS

Liez les ports à DPDK, puis connectez-les au pont OVS en saisissant les commandes Fedora ou RHOS suivantes :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set
   Interface dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set
   Interface dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
   options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
   options:dpdk-devargs=0000:03:00.1
```

Le `dpdk-devargs` indiqué dans les options spécifie le BDF PCI de la carte réseau physique respective.

Connectez des vhost-user ports au chemin de données OVS

Tapez les commandes Fedora ou RHOS suivantes pour attacher des vhost-user ports au chemin de données OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
```

Provisionner un KVM-VPX avec des vhost-user ports OVS-DPDK

Vous pouvez provisionner une instance VPX sur Fedora KVM avec des ports vhost-user basés sur OVS-DPDK uniquement à partir de la CLI en utilisant les commandes QEMU suivantes : **Commande Fedora** :

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \

-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,bus=pci.0,addr=0x3 \

```



```
-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

--nographic
```

Pour RHOS, utilisez l'exemple de fichier XML suivant pour provisionner l'instance NetScaler VPX, en utilisant. `virsh`

```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>

  <cputune>

    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>

```



```
35        <emulatorpin cpuset='0,2,4,6'/>
36
37      </cputune>
38
39      <numatune>
40
41        <memory mode='strict' nodeset='0'/>
42
43      </numatune>
44
45      <resource>
46
47        <partition>/machine</partition>
48
49      </resource>
50
51      <os>
52
53        <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55        <boot dev='hd'/>
56
57      </os>
58
59      <features>
60
61        <acpi/>
62
63        <apic/>
64
65      </features>
66
67      <cpu mode='custom' match='minimum' check='full'>
68
69        <model fallback='allow'>Haswell-noTSX</model>
70
71        <vendor>Intel</vendor>
72
73        <topology sockets='1' cores='6' threads='1'/>
74
75        <feature policy='require' name='ss'/>
76
77        <feature policy='require' name='pcid'/>
78
79        <feature policy='require' name='hypervisor'/>
80
81        <feature policy='require' name='arat'/>
82
83    <domain type='kvm'>
84
85      <name>dpdk-vpx1</name>
86
87      <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
```



```
88
89      <memory unit='KiB'>16777216</memory>
90
91      <currentMemory unit='KiB'>16777216</currentMemory>
92
93      <memoryBacking>
94
95        <hugepages>
96
97          <page size='1048576' unit='KiB'/>
98
99        </hugepages>
100
101     </memoryBacking>
102
103     <vcpu placement='static'>6</vcpu>
104
105     <cputune>
106
107       <shares>4096</shares>
108
109       <vcpupin vcpu='0' cpuset='0'/>
110
111       <vcpupin vcpu='1' cpuset='2'/>
112
113       <vcpupin vcpu='2' cpuset='4'/>
114
115       <vcpupin vcpu='3' cpuset='6'/>
116
117       <emulatorpin cpuset='0,2,4,6'/>
118
119     </cputune>
120
121     <numatune>
122
123       <memory mode='strict' nodeset='0'/>
124
125     </numatune>
126
127     <resource>
128
129       <partition>/machine</partition>
130
131     </resource>
132
133     <os>
134
135       <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
136
137       <boot dev='hd'/>
138
139     </os>
140
```



```
141     <features>
142
143       <acpi/>
144
145       <apic/>
146
147     </features>
148
149     <cpu mode='custom' match='minimum' check='full'>
150
151       <model fallback='allow'>Haswell-noTSX</model>
152
153       <vendor>Intel</vendor>
154
155       <topology sockets='1' cores='6' threads='1'/>
156
157       <feature policy='require' name='ss'/>
158
159       <feature policy='require' name='pcid'/>
160
161       <feature policy='require' name='hypervisor'/>
162
163       <feature policy='require' name='arat'/>
164
165       <feature policy='require' name='tsc\_adjust'/>
166
167       <feature policy='require' name='xsaveopt'/>
168
169       <feature policy='require' name='pdpe1gb'/>
170
171       <numa>
172
173         <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess=
              'shared'/>
174
175       </numa>
176
177     </cpu>
178
179     <clock offset='utc'/>
180
181     <on\_poweroff>destroy</on\_poweroff>
182
183     <on\_reboot>restart</on\_reboot>
184
185     <on\_crash>destroy</on\_crash>
186
187     <devices>
188
189       <emulator>/usr/libexec/qemu-kvm</emulator>
190
191       <disk type='file' device='disk'>
192
```



```
193           <driver name='qemu' type='qcow2' cache='none'/>
194
195           <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>
196
197           <target dev='vda' bus='virtio'/>
198
199           <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
                 function='0x0'/>
200
201         </disk>
202
203         <controller type='ide' index='0'>
204
205           <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
                 function='0x1'/>
206
207         </controller>
208
209         <controller type='usb' index='0' model='piix3-uhci'>
210
211           <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
                 function='0x2'/>
212
213         </controller>
214
215         <controller type='pci' index='0' model='pci-root'/>
216
217         <interface type='direct'>
218
219           <mac address='52:54:00:bb:ac:05'/>
220
221           <source dev='enp129s0f0' mode='bridge'/>
222
223           <model type='virtio'/>
224
225           <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
                 function='0x0'/>
226
227         </interface>
228
229         <interface type='vhostuser'>
230
231           <mac address='52:54:00:55:55:56'/>
232
233           <source type='unix' path='/var/run/openvswitch/vhost-user1'
                 mode='client'/>
234
235           <model type='virtio'/>
236
237           <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
                 function='0x0'/>
238
239         </interface>
```



```
240
241         <interface type='vhostuser'>
242
243           <mac address='52:54:00:2a:32:64'/>
244
245           <source type='unix' path='/var/run/openvswitch/vhost-user2'
                 mode='client'/>
246
247           <model type='virtio'/>
248
249           <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
                 function='0x0'/>
250
251         </interface>
252
253         <interface type='vhostuser'>
254
255           <mac address='52:54:00:2a:32:74'/>
256
257           <source type='unix' path='/var/run/openvswitch/vhost-user3'
                 mode='client'/>
258
259           <model type='virtio'/>
260
261           <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
                 function='0x0'/>
262
263         </interface>
264
265         <interface type='vhostuser'>
266
267           <mac address='52:54:00:2a:32:84'/>
268
269           <source type='unix' path='/var/run/openvswitch/vhost-user4'
                 mode='client'/>
270
271          <model type='virtio'/>
272
273           <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
                 function='0x0'/>
274
275         </interface>
276
277         <serial type='pty'>
278
279           <target port='0'/>
280
281         </serial>
282
283         <console type='pty'>
284
285           <target type='serial' port='0'/>
286
```



```
287         </console>
288
289         <input type='mouse' bus='ps2'/>
290
291         <input type='keyboard' bus='ps2'/>
292
293         <graphics type='vnc' port='-1' autoport='yes'>
294
295           <listen type='address'/>
296
297         </graphics>
298
299         <video>
300
301           <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303           <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
                function='0x0'/>
304
305         </video>
306
307         <memballoon model='virtio'>
308
309           <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
                function='0x0'/>
310
311         </memballoon>
312
313       </devices>
314
315     </domain
```

Points à noter

Dans le fichier XML, la hugepage taille doit être de 1 Go, comme indiqué dans le fichier exemple.

```
1     <memoryBacking>
2
3         <hugepages>
4
5           <page size='1048576' unit='KiB'/>
6
7         </hugepages>
```

En outre, dans le fichier exemple, vhost-user1 est le port vhost utilisateur lié à ovs-br0.

```
1     <interface type='vhostuser'>
2
3           <mac address='52:54:00:55:55:56'/>
4
5           <source type='unix' path='/var/run/openvswitch/vhost-user1'
              mode='client'/>
```



```
6
7          <model type='virtio'/>
8
9          <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
               function='0x0'/>
10
11       </interface>
```

Pour faire apparaître l'instance NetScaler VPX, commencez à utiliser la commande. `virsh`

Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur KVM

October 17, 2024

Vous pouvez appliquer les configurations NetScaler VPX sur l'hyperviseur KVM lors du premier démarrage de l'appliance NetScaler. Par conséquent, une configuration client sur une instance VPX peut être configurée en beaucoup moins de temps.

Pour plus d'informations sur les données utilisateur de pré-démarrage et leur format, consultez Appliquer les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler dans le cloud.

> **Remarque :**
>
> Pour amorcer à l'aide des données utilisateur avant le démarrage dans l'hyperviseur KVM, la configuration de passerelle par défaut doit être transmise dans la section `<NS-CONFIG>`. Pour plus d'informations sur le contenu de la balise `<NS-CONFIG>`, reportez-vous à la section `<NS-CONFIG>` Exemple suivante.

Sample `<NS-CONFIG>` section:

```
1   <NS-PRE-BOOT-CONFIG>
2
3       <NS-CONFIG>
4           add route 0.0.0.0 0.0.0.0  10.102.38.1
5       </NS-CONFIG>
6
7       <NS-BOOTSTRAP>
8               <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
9               <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
10
11          <MGMT-INTERFACE-CONFIG>
12                  <INTERFACE-NUM> eth0 </INTERFACE-NUM>
13                  <IP> 10.102.38.216 </IP>
14                  <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
15          </MGMT-INTERFACE-CONFIG>
```



```
16        </NS-BOOTSTRAP>
17
18    </NS-PRE-BOOT-CONFIG>
```

Comment fournir des données utilisateur avant le démarrage sur l'hyperviseur KVM

Vous pouvez fournir des données utilisateur avant le démarrage sur l'hyperviseur KVM via un fichier ISO, qui est joint à l'aide d'un périphérique CDROM.

Fournir des données utilisateur à l'aide du fichier ISO du CD-ROM

Vous pouvez utiliser Virtual Machine Manager (VMM) pour injecter des données utilisateur dans la machine virtuelle (VM) en tant qu'image ISO à l'aide du périphérique CDROM. KVM prend en charge les CD-ROM dans VM Guest, soit en accédant directement à un lecteur physique sur le serveur hôte de la machine virtuelle, soit en accédant aux images ISO.

Les étapes suivantes vous permettent de fournir des données utilisateur à l'aide du fichier ISO du CD-ROM :

1. Créez un fichier dont le nom de fichier `userdata` contient le contenu des données utilisateur avant le démarrage.

   > **Remarque :**
   >
   > Le nom de fichier doit être strictement utilisé comme `userdata`.

2. Store the `userdata` file in a folder, and build an ISO image using the folder.

   You can build an ISO image with `userdata` file by the following two methods:

   - Using any image processing tool such as PowerISO.
   - Using `mkisofs` command in Linux.

   The following sample configuration shows how to generate an ISO image using the `mkisofs` command in Linux.

```
1   root@ubuntu:~/sai/19oct# ls -lh
2   total 4.0K
3   -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
4   root@ubuntu:~/sai/19oct#
5   root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
6   I: -input-charset not specified, using utf-8 (detected in locale
        settings)
7   Total translation table size: 0
8   Total rockridge attributes bytes: 0
9   Total directory bytes: 0
10  Path table size(bytes): 10
```



```
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
```

3. Provisionnez l'instance NetScaler VPX à l'aide du processus de déploiement standard pour créer la machine virtuelle. But do not power on the VM automatically.
4. Ajoutez un lecteur de CD-ROM avec Virtual Machine Manager en suivant les étapes suivantes :
   a) Double-cliquez sur une entrée d'invité de machine virtuelle dans Virtual Machine Manager pour ouvrir sa console, puis passez à la vue Détails avec **Afficher > Détails**.
   b) Cliquez sur **Ajouter du matériel > Stockage > Type de périphérique > périphérique CDROM**.
   c) Cliquez sur **Gérer** et sélectionnez le bon fichier ISO, puis cliquez sur **Terminer**. Un nouveau CDROM sous **Ressources** sur votre instance NetScaler VPX est créé.
5. Power on the VM.

NetScaler VPX sur AWS

October 17, 2024

Vous pouvez lancer une instance NetScaler VPX sur Amazon Web Services (AWS). L'appliance NetScaler VPX est disponible sous forme d'Amazon Machine Image (AMI) sur AWS Marketplace. Une instance NetScaler VPX sur AWS vous permet d'utiliser les fonctionnalités de cloud computing d'AWS et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic de NetScaler pour répondre à leurs besoins commerciaux. L'instance VPX prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance NetScaler physique et peut être déployée en tant qu'instances autonomes ou en paires HA. Pour plus d'informations sur les fonctionnalités de VPX, consultez la fiche technique VPX.

Mise en route

Avant de commencer votre déploiement VPX, vous devez connaître les informations suivantes :

- Terminologie AWS
- Matrice de prise en charge AWS-VPX
- Limitations et directives d'utilisation

- Conditions préalables
- Comment fonctionne une instance NetScaler VPX sur AWS

Déployer une instance NetScaler VPX sur AWS

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Standalone
- Haute disponibilité (actif-passif)
  - Haute disponibilité dans la même zone
  - Haute disponibilité dans différentes zones grâce à Elastic IP
  - Haute disponibilité dans différentes zones grâce à une adresse IP privée
- GSLB actif-actif
- Mise à l'échelle automatique (actif-actif) à l'aide d'ADM

Déploiements hybrides

- Déployer NetScaler dans AWS Outpost
- Déployer NetScaler dans VMC dans AWS

Système de licences

Une instance NetScaler VPX sur AWS nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur AWS :

- Gratuit (illimité)
- Horaire
- Annuel
- BYOL
- Essai gratuit (toutes les offres d'abonnement NetScaler VPX-AWS pendant 21 jours gratuits sur AWS Marketplace.)

Automatisation

- NetScaler ADM : Déploiement intelligent
- GitHub CFT : modèles et scripts NetScaler pour le déploiement d'AWS
- GitHub Ansible : modèles et scripts NetScaler pour le déploiement d'AWS

- GitHub Terraform : modèles et scripts NetScaler pour le déploiement d'AWS
- Bibliothèque de modèles AWS (PL) : NetScaler VPX

Blogs

- Comment NetScaler sur AWS aide les clients à fournir des applications en toute sécurité
- Livraison d'applications dans un cloud hybride avec NetScaler et AWS
- Citrix est un partenaire de compétence réseau AWS
- NetScaler : toujours prêt pour les clouds publics
- Évoluez ou évoluez facilement dans les clouds publics grâce à NetScaler
- Citrix élargit le choix de déploiement ADC avec AWS Outposts
- Utilisation de NetScaler avec le routage d'entrée Amazon VPC
- Citrix offre un choix, des performances et un déploiement simplifié dans AWS
- La sécurité du pare-feu NetScaler Web App, désormais disponible sur AWS Marketplace
- Comment Aria Systems utilise le pare-feu NetScaler Web App sur AWS

Mes vidéos

- Simplification des déploiements NetScaler dans le cloud public grâce à ADM
- Provisioning et configuration de NetScaler VPX dans AWS à l'aide de scripts Terraform prêts à l'emploi
- Déployer NetScaler HA dans AWS à l'aide du modèle CloudFormation
- Déployez NetScaler HA dans les zones de disponibilité à l'aide d'AWS QuickStart
- NetScaler Autoscale à l'aide d'ADM

Études de cas clients

- Solution technologique - Xenit AB
- Une meilleure façon de faire des affaires avec Citrix et le cloud AWS —Aria
- Découvrez les avantages de NetScaler et d'AWS
- Rain for Rent - Témoignage client

Solutions

- Déployez une plateforme de publicité numérique sur AWS avec NetScaler
- Améliorer l'analyse du flux de clics dans AWS à l'aide de NetScaler

Assistance

- Ouvrir un dossier de support
- Pour l'offre d'abonnement NetScaler, consultez Résoudre les problèmes d'une instance VPX sur AWS. Pour déposer une demande d'assistance, recherchez votre numéro de compte AWS et votre code PIN d'assistance, puis appelez le support NetScaler.
- Pour l'offre NetScaler Customer Licensed ou BYOL, assurez-vous que vous disposez d'un contrat de support et de maintenance valide. Si vous n'avez pas conclu d'accord, contactez votre représentant NetScaler.

Références supplémentaires

- Webinaire à la demande AWS - NetScaler sur AWS
- Fiche technique de NetScaler VPX
- NetScaler sur AWS Marketplace
- NetScaler fait partie des solutions de mise en réseau des partenaires AWS (équilibreurs de charge)
- Questions fréquentes sur AWS

Terminologie AWS

October 17, 2024

Cette section décrit la liste des termes et expressions AWS couramment utilisés. Pour plus d'informations, consultez AWS Glossary.

Terme	Définition
Image de machine Amazon (AMI)	Une image de machine, qui fournit les informations requises pour lancer une instance, qui est un serveur virtuel dans le cloud.

Terme	Définition
Elastic Block Store	Fournit des volumes de stockage par blocs persistants à utiliser avec les instances Amazon EC2 dans le cloud AWS.
Service de stockage simple (S3)	Stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle du Web pour les développeurs.
Elastic Compute Cloud (EC2)	Service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter le cloud computing à l'échelle du Web pour les développeurs.
Équilibrage de charge élastique (ELB)	Répartit le trafic applicatif entrant sur plusieurs instances EC2, dans plusieurs zones de disponibilité. Cela augmente la tolérance aux pannes de vos applications.
Interface réseau élastique (ENI)	Interface réseau virtuelle que vous pouvez associer à une instance dans un Virtual Private Cloud (VPC).
Adresse IP élastique (EIP)	Adresse IPv4 publique statique que vous avez allouée dans Amazon EC2 ou Amazon VPC, puis attachée à une instance. Les adresses IP Elastic sont associées à votre compte, et non à une instance spécifique. Ils sont élastiques car vous pouvez facilement les répartir, les attacher, les détacher et les libérer en fonction de l'évolution de vos besoins.
Type d'instance	Amazon EC2 propose une large sélection de types d'instances optimisés pour s'adapter à différents cas d'utilisation. Les types d'instance comprennent différentes combinaisons de processeur, de mémoire, de stockage et de capacité réseau et vous permettent de choisir la combinaison de ressources appropriée pour vos applications.

Terme	Définition
Identity and Access Management (IAM)	Identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. Vous pouvez utiliser un rôle IAM pour permettre aux applications exécutées sur une instance EC2 d'accéder en toute sécurité à vos ressources AWS. Le rôle IAM est requis pour déployer des instances VPX dans une configuration haute disponibilité.
Passerelle Internet	Connecte un réseau à Internet. Vous pouvez acheminer le trafic pour les adresses IP situées en dehors de votre VPC vers la passerelle Internet.
Paire de clés	Ensemble d'identifiants de sécurité que vous utilisez pour prouver votre identité par voie électronique. Une paire de clés se compose d'une clé privée et d'une clé publique.
Tables de routage	Ensemble de règles de routage qui contrôle le trafic quittant tout sous-réseau associé à la table de routage. Vous pouvez associer plusieurs sous-réseaux à une seule table de routage, mais un sous-réseau ne peut être associé qu'à une seule table de routage à la fois.
Groupes de sécurité	Un ensemble nommé de connexions réseau entrantes autorisées pour une instance.
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel les instances EC2 peuvent être attachées. Vous pouvez créer des sous-réseaux pour regrouper les instances en fonction des besoins opérationnels et de sécurité.
Cloud privé virtuel (VPC)	Service Web permettant de Provisioning une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.
Mise à l'échelle automatique	Service Web permettant de lancer ou de résilier automatiquement des instances Amazon EC2 en fonction de stratégies, de calendriers et de bilans d'intégrité définis par l'utilisateur.

Terme	Définition
CloudFormation	Service permettant d'écrire ou de modifier des modèles qui créent et suppriment des ressources AWS associées en tant qu'unité.

Matrice de prise en charge AWS-VPX

October 17, 2024

Les tableaux suivants répertorient le modèle VPX et les régions AWS, les types d'instance et les services pris en charge.

Tableau 1 : modèles VPX pris en charge sur AWS

Modèle VPX pris en charge
NetScaler VPX Advanced - 200 Mbits/s
NetScaler VPX Premium - 1 Gbit/s
NetScaler VPX Premium - 5 Gbit/s
NetScaler VPX Express - 20 Mbps
NetScaler VPX –Licence client
NetScaler VPX FIPS - Licence client
NetScaler VPX FIPS ENA - Licence client

Tableau 2 : régions AWS prises en charge

régions AWS prises en charge
Ouest des États-Unis (Oregon)
USA West (Californie du Nord) Californie)
Est des États-Unis (Ohio)
USA Est (Virginie du Nord) Virginie)
Asie-Pacifique (Mumbai)
Asie-Pacifique (Séoul)
Asie-Pacifique (Singapour)

Asie-Pacifique (Sydney)
Asie-Pacifique (Tokyo)
Asie-Pacifique (Hong Kong)
Asie-Pacifique (Osaka)
Asie-Pacifique (Jakarta)
Asie-Pacifique (Hyderabad)
Canada (Centre)
UE (Francfort)
UE (Irlande)
UE (Londres)
UE (Paris)
UE (Milan)
Amérique du Sud (São Paulo)
AWS GovCloud (États-Unis et Est)
AWS GovCloud (USA Ouest)
Très secret d'AWS (C2S)
Moyen-Orient (Bahreïn)
Afrique (Le Cap)
C2S

> **Remarque :**
>
> Pour la région AWS de Hong Kong, le support NetScaler VPX est disponible uniquement avec les licences BYOL.

Tableau 3 : types d'instance AWS pris en charge

Types d'instance AWS pris en charge
c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge
C5.large, c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.18xlarge, c5.24xlarge
c5n.large, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge
d2.xlarge, d2.2 x large, d2.4 x large, d2.8 x large
m3.large, m3.xlarge, m3.2xlarge
m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge
m5.large, m5.xlarge, m5.2 x large, m5,4 x large, m5,8 x large, m5,12 x large, m5,16 x large, m5.24 x large
m5a. large, m5a. x large, m5a. 2 x large, m5a. 4 x large, m5 a.8 x large, m5a.
m5n.large, m5n.xlarge, m5n.2xlarge, m5n.4xlarge, m5n.8xlarge, m5n.12xlarge, m5n.16xlarge, m5n.24xlarge
m6i.large, m6i.xlarge, m6i.2xlarge, m6i.4xlarge, m6i.8xlarge, m6i.12xlarge, m6i.16xlarge, m6i.24xlarge, m6i.32xlarge

| r7iz.large, r7iz.xlarge, r7iz.2xlarge, r7iz.4xlarge, r7iz.8xlarge, r7iz.12xlarge, r7iz.16xlarge, r7iz.32xlarge |
| t2.medium, t2.large, t2.xlarge, t2.2xlarge |
| t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge |

> **Remarque :**
>
> NetScaler VPX provisionné sur les types d'instance AWS m6i et r7iz ne prend pas en charge la fonctionnalité de file d'attente à faible latence (LLQ) ENA.

Tableau 4 : Services AWS pris en charge

Services AWS pris en charge
EC2 : lance des instances ADC.
Lambda : invoque les API NetScaler VPX NITRO lors du provisionnement d'instances NetScaler VPX depuis CFT.
Routage d'entrée VPC et VPC : Le VPC crée des réseaux isolés dans lesquels l'ADC peut être lancé. Le routage d'
Route53 : distribue le trafic sur tous les nœuds NetScaler VPX de la solution NetScaler Autoscale.
ELB : distribue le trafic sur tous les nœuds NetScaler VPX de la solution NetScaler Autoscale.
Cloudwatch : surveille les performances et les paramètres système de l'instance NetScaler VPX.
AWS Autoscaling : utilisé pour la mise à l'échelle automatique du serveur principal.
Formation dans le cloud : les modèles CloudFormation sont utilisés pour déployer des instances NetScaler VPX.
Service de file d'attente simple (SQS) : surveille les événements de mise à l'échelle et de réduction de la taille d
Simple Notification Service (SNS) : surveille les événements de mise à l'échelle et de réduction de l'échelle dan
Gestion des identités et des accès (IAM) : permet d'accéder aux services et aux ressources AWS.
AWS Outposts : provisionne des instances NetScaler VPX dans AWS Outposts.

NetScaler recommande les types d'instances AWS suivants :

- Séries M5 et C5n pour les éditions Marketplace ou les licences de pool basées sur la bande passante.
- Série C5n pour les licences de pool basées sur VCPU.

Offre VPX sur AWS Marketplace	Recommandation d'instance AWS
VPX Express 20, VPX 200	M5.xLarge
VPX 1 G, VPX 5 G	M5.2xLarge

NetScaler recommande les types d'instances AWS suivants en fonction du débit.

VPX avec licences groupées (licences de bande passante)	Recommandation d'instance AWS
VPX 8 G	C5n.4xLarge
VPX 10 G, VPX 15 G, VPX 25 G	C5n.9xLarge

> **Remarque :**
>
> L'offre VPX 25G n'offre pas le débit 25G souhaité dans AWS mais peut offrir un taux de transactions SSL plus élevé.

Pour atteindre un débit supérieur à la 5G, procédez comme suit :

- Choisissez l'**offre NetScaler VPX - Customer Licensed (BYOL**) sur AWS Marketplace.
- Sélectionnez Licences **groupées (licences de bande passante)** dans l'interface graphique ou l'interface de ligne de commande NetScaler.

Pour déterminer votre instance en fonction de différents indicateurs tels que le nombre de paquets par seconde ou le taux de transactions SSL, contactez votre contact NetScaler pour obtenir des conseils. Pour obtenir des conseils sur les licences et le dimensionnement des pools basés sur des processeurs virtuels, contactez le support NetScaler.

Limitations et directives d'utilisation

October 17, 2024

Les limites et directives d'utilisation suivantes s'appliquent lors du déploiement d'une instance NetScaler VPX sur AWS :

- Avant de commencer, lisez la section terminologie AWS dans Déployer une instance NetScaler VPX sur AWS.
- La fonctionnalité de clustering n'est pas prise en charge pour VPX.
- Pour que la configuration haute disponibilité fonctionne efficacement, associez un périphérique NAT dédié à l'interface de gestion ou associez EIP à NSIP. Pour plus d'informations sur NAT, dans la documentation AWS, consultez Instances NAT.
- Le trafic de données et le trafic de gestion doivent être séparés par les ENIs appartenant à différents sous-réseaux.

- Seule l'adresse NSIP doit être présente sur l'ENI de gestion.
- Si une instance NAT est utilisée pour la sécurité au lieu d'affecter un EIP au NSIP, des modifications appropriées de routage au niveau du VPC sont requises. Pour obtenir des instructions sur la modification du routage au niveau du VPC, dans la documentation AWS, voir Scénario 2 : VPC with Public and Private Subnets.
- Une instance VPX peut être déplacée d'un type d'instance EC2 à un autre (par exemple, de m3.large à m3.xlarge).
- Pour les options de stockage pour VPX sur AWS, Citrix recommande EBS, car il est durable et les données sont disponibles même après leur détachement de l'instance.
- L'ajout dynamique d'ENI à VPX n'est pas pris en charge. Redémarrez l'instance VPX pour appliquer la mise à jour. Citrix vous recommande d'arrêter l'instance autonome ou HA, d'attacher la nouvelle ENI, puis de redémarrer l'instance.
- Vous pouvez attribuer plusieurs adresses IP à un ENI. Le nombre maximal d'adresses IP par ENI est déterminé par le type d'instance EC2, voir la section « Adresses IP par interface réseau par type d'instance » dans Elastic Network Interfaces. Vous devez allouer les adresses IP dans AWS avant de les affecter à des ENI. Pour plus d'informations, voir Interfaces réseau Elastic.
- Citrix vous recommande d'éviter d'utiliser les commandes d'interface d'activation et de désactivation sur les interfaces NetScaler VPX.
- NetScaler `set ha node \\<NODE\\_ID\\> -haStatus STAYPRIMARY` et `set ha node \\<NODE\\_ID\\> -haStatus STAYSECONDARY` les commandes sont désactivés par défaut.
- IPv6 n'est pas pris en charge pour VPX.
- En raison des limitations AWS, ces fonctionnalités ne sont pas prises en charge :
  - Gratuitous ARP (GARP)
  - Mode L2
  - VLAN balisé
  - Routage dynamique
  - MAC virtuel
- Pour que RNAT fonctionne, assurez-vous que la **vérification de la source/destination** est désactivée. Pour plus d'informations, voir « Modification de la vérification source/destination » dans Elastic Network Interfaces.
- Lors d'un déploiement NetScaler VPX sur AWS, dans certaines régions AWS, l'infrastructure AWS peut ne pas être en mesure de résoudre les appels d'API AWS. Cela se produit si les appels d'API sont émis via une interface non administrative sur l'instance NetScaler VPX. Comme solution de contournement, limitez les appels d'API à l'interface de gestion uniquement. Pour ce

faire, créez un NSVLAN sur l'instance VPX et liez l'interface de gestion au NSVLAN à l'aide de la commande appropriée. Par exemple : définir ns config -nsvlan <vlan id > -ifnum 1/1 -tagged NON enregistrer la configuration Redémarrez l'instance VPX à l'invite. Pour plus d'informations sur la configuration nsvlan, reportez-vous à la section Configuration de NSVLAN.

- Dans la console AWS, l'utilisation du vCPU affichée pour une instance VPX sous l'onglet **Surveillance** peut être élevée (jusqu'à 100 %), même lorsque l'utilisation réelle est beaucoup plus faible. Pour voir l'utilisation réelle du vCPU, accédez à **Afficher toutes les mesures CloudWatch**. Pour plus d'informations, consultez Surveillez vos instances à l'aide d'Amazon CloudWatch.
- L'ajout à chaud n'est pris en charge que pour les interfaces PV et SRIOV avec NetScaler sur AWS. Les instances VPX avec interfaces ENA ne prennent pas en charge le branchement à chaud, et le comportement des instances peut être imprévisible en cas de tentative de connexion à chaud.
- La suppression à chaud via la console Web AWS ou l'interface CLI AWS n'est pas prise en charge avec les interfaces PV, SRIOV et ENA pour NetScaler. Le comportement des instances peut être imprévisible si la suppression à chaud est tentée.

Conditions préalables

October 17, 2024

Avant de tenter de créer une instance VPX dans AWS, assurez-vous de disposer des éléments suivants :

- **Un compte AWS** : pour lancer une AMI NetScaler VPX dans un cloud privé virtuel (VPC) AWS. Vous pouvez créer un compte AWS gratuitement sur www.aws.amazon.com.
- **Un compte d'utilisateur AWS Identity and Access Management (IAM)** : pour contrôler en toute sécurité l'accès aux services et ressources AWS pour vos utilisateurs. Pour plus d'informations sur la façon de créer un compte d'utilisateur IAM, consultez Création d'utilisateurs IAM (console). Un rôle IAM est obligatoire pour les déploiements autonomes et haute disponibilité.

  Le rôle IAM associé à votre compte AWS doit disposer des autorisations IAM suivantes pour différents scénarios.

  Paire HA avec des adresses IPv4 dans la même zone AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:AssignPrivateIpAddresses",
3     "iam:SimulatePrincipalPolicy",
4     "iam:GetRole",
```



```
5     "ec2:CreateTags"
```

Paire HA avec des adresses IPv6 dans la même zone AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:AssignIpv6Addresses",
3     "ec2:UnassignIpv6Addresses",
4     "iam:SimulatePrincipalPolicy",
5     "iam:GetRole",
6     "ec2:CreateTags"
```

Couplage HA avec des adresses IPv4 et IPv6 dans la même zone AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:AssignPrivateIpAddresses",
3     "ec2:AssignIpv6Addresses",
4     "ec2:UnassignIpv6Addresses",
5     "iam:SimulatePrincipalPolicy",
6     "iam:GetRole",
7     "ec2:CreateTags"
```

Paire HA avec des adresses IP élastiques dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeAddresses",
3     "ec2:AssociateAddress",
4     "ec2:DisassociateAddress",
5     "iam:SimulatePrincipalPolicy",
6     "iam:GetRole",
7     "ec2:CreateTags"
```

Paire HA avec des adresses IP privées dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeRouteTables",
3     "ec2:DeleteRoute",
4     "ec2:CreateRoute",
5     "ec2:ModifyNetworkInterfaceAttribute",
6     "iam:SimulatePrincipalPolicy",
7     "iam:GetRole",
8     "ec2:CreateTags"
```

Couplage HA avec des adresses IP privées et des adresses IP élastiques dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeAddresses",
3     "ec2:AssociateAddress",
4     "ec2:DisassociateAddress",
5     "ec2:DescribeRouteTables",
6     "ec2:DeleteRoute",
7     "ec2:CreateRoute",
8     "ec2:ModifyNetworkInterfaceAttribute",
```



```
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "ec2:CreateTags"
```

Autoscaling du backend AWS :

```
    "ec2:DescribeInstances",
    "autoscaling:*",
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sqs:CreateQueue",
    "sqs:ListQueues",
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "ec2:CreateTags"
```

> **Remarque :**
>
> - Si vous utilisez une combinaison des fonctionnalités précédentes, utilisez la combinaison d'autorisations IAM pour chacune des fonctionnalités.
> - Si vous utilisez le modèle Citrix CloudFormation, le rôle IAM est automatiquement créé. Le modèle ne permet pas de sélectionner un rôle IAM déjà créé.
> - Lorsque vous vous connectez à l'instance VPX par le biais de l'interface graphique, une invite vous demandant de configurer les privilèges requis pour le rôle IAM s'affiche. Ignorez l'invite si vous avez déjà configuré les privilèges.

- **CLI AWS** : Pour utiliser toutes les fonctionnalités fournies par AWS Management Console à partir de votre programme terminal. Pour plus d'informations, consultez le guide de l'utilisateur de l'AWS CLI. Vous avez également besoin de l'interface de ligne de commande AWS pour changer le type d'interface réseau en SR-IOV.
- **Elastic Network Adapter (ENA)** : pour le type d'instance activé par le pilote ENA, par exemple les instances M5, C5, la version du microprogramme doit être 13.0 et supérieure.
- Vous devez configurer le service de métadonnées d'instance (IMDS) sur l'instance EC2 pour NetScaler VPX. IMDSv1 et IMDSv2 sont deux modes disponibles pour accéder aux métadonnées d'instance à partir d'une instance AWS EC2 en cours d'exécution. L'IMDSv2 est plus sécurisé que l'IMDSv1. Vous pouvez configurer l'instance pour utiliser les deux méthodes (option par défaut) ou uniquement le mode IMDSv2 (en désactivant IMDSv1). Citrix ADC VPX prend en charge le mode IMDSv2 uniquement à partir de la version 13.1.48.x de NetScaler VPX.

Configurer les rôles AWS IAM sur une instance NetScaler VPX

October 17, 2024

Les applications qui s'exécutent sur une instance Amazon EC2 doivent inclure des informations d'identification AWS dans les demandes d'API AWS. Vous pouvez stocker les informations d'identification AWS directement dans l'instance Amazon EC2 et autoriser les applications de cette instance à utiliser ces informations d'identification. Mais vous devez ensuite gérer les informations d'identification et vous assurer qu'elles sont transmises en toute sécurité à chaque instance et mettre à jour chaque instance Amazon EC2 au moment de la rotation des informations d'identification. Cela représente beaucoup de travail supplémentaire.

Vous pouvez et devez plutôt utiliser un rôle de gestion des identités et des accès (IAM) pour gérer les informations d'identification temporaires pour les applications exécutées sur une instance Amazon EC2. Lorsque vous utilisez un rôle, vous n'avez pas besoin de distribuer des informations d'identification à long terme (telles qu'un nom d'utilisateur et un mot de passe ou des clés d'accès) à une instance Amazon EC2. Le rôle fournit plutôt des autorisations temporaires que les applications peuvent utiliser lorsqu'elles effectuent des appels vers d'autres ressources AWS. Lorsque vous lancez une instance Amazon EC2, vous spécifiez un rôle IAM à associer à l'instance. Les applications qui s'exécutent sur l'instance peuvent ensuite utiliser les informations d'identification temporaires fournies par le rôle pour signer les demandes d'API.

Le rôle IAM associé à votre compte AWS doit disposer des autorisations IAM suivantes pour différents scénarios.

Paire HA avec des adresses IPv4 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
```

Paire HA avec des adresses IPv6 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
```

Couplage HA avec des adresses IPv4 et IPv6 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
```



```
6     "iam:GetRole"
```

Paire HA avec des adresses IP élastiques dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeAddresses",
3     "ec2:AssociateAddress",
4     "ec2:DisassociateAddress",
5     "iam:SimulatePrincipalPolicy",
6     "iam:GetRole"
```

Paire HA avec des adresses IP privées dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeRouteTables",
3     "ec2:DeleteRoute",
4     "ec2:CreateRoute",
5     "ec2:ModifyNetworkInterfaceAttribute",
6     "iam:SimulatePrincipalPolicy",
7     "iam:GetRole"
```

Couplage HA avec des adresses IP privées et des adresses IP élastiques dans différentes zones AWS :

```
1     "ec2:DescribeInstances",
2     "ec2:DescribeAddresses",
3     "ec2:AssociateAddress",
4     "ec2:DisassociateAddress",
5     "ec2:DescribeRouteTables",
6     "ec2:DeleteRoute",
7     "ec2:CreateRoute",
8     "ec2:ModifyNetworkInterfaceAttribute",
9     "iam:SimulatePrincipalPolicy",
10    "iam:GetRole"
```

Autoscaling du backend AWS :

```
1     "ec2:DescribeInstances",
2     "autoscaling:*",
3     "sns:CreateTopic",
4     "sns:DeleteTopic",
5     "sns:ListTopics",
6     "sns:Subscribe",
7     "sqs:CreateQueue",
8     "sqs:ListQueues",
9     "sqs:DeleteMessage",
10    "sqs:GetQueueAttributes",
11    "sqs:SetQueueAttributes",
12    "iam:SimulatePrincipalPolicy",
13    "iam:GetRole"
```

Points à noter :

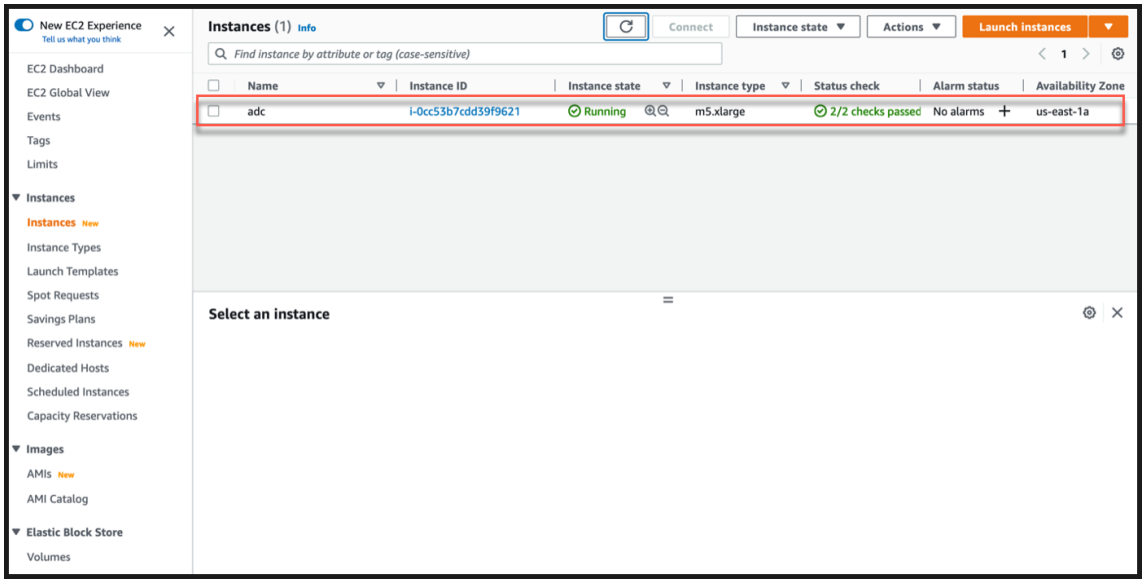
- Si vous utilisez une combinaison des fonctionnalités précédentes, utilisez la combinaison d'autorisations IAM pour chacune des fonctionnalités.
- Si vous utilisez le modèle Citrix CloudFormation, le rôle IAM est automatiquement créé. Le modèle ne permet pas de sélectionner un rôle IAM déjà créé.
- Lorsque vous vous connectez à l'instance VPX par le biais de l'interface graphique, une invite vous demandant de configurer les privilèges requis pour le rôle IAM s'affiche. Ignorez l'invite si vous avez déjà configuré les privilèges.
- Un rôle IAM est obligatoire pour les déploiements autonomes et haute disponibilité.

Créer un rôle IAM

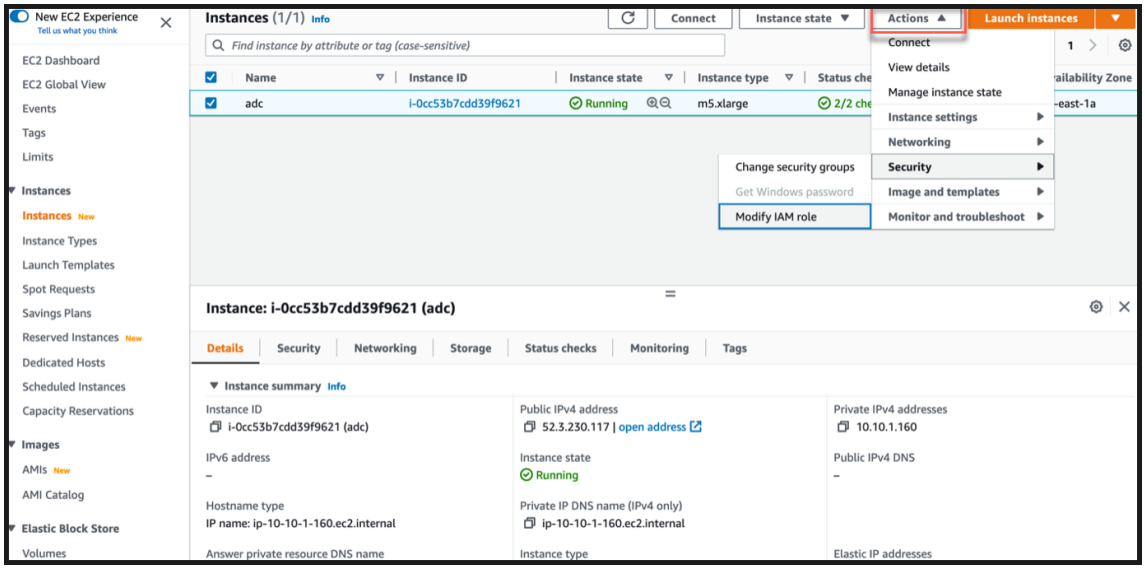
Cette procédure explique comment créer un rôle IAM pour la fonctionnalité de dimensionnement automatique du back-end d'AWS.

> **Remarque :**
>
> Vous pouvez suivre la même procédure pour créer tous les rôles IAM correspondant à d'autres fonctionnalités.

1. Connectez-vous à la console de gestion AWS pour EC2.
2. Accédez à la page de l'instance EC2 et sélectionnez votre instance ADC.

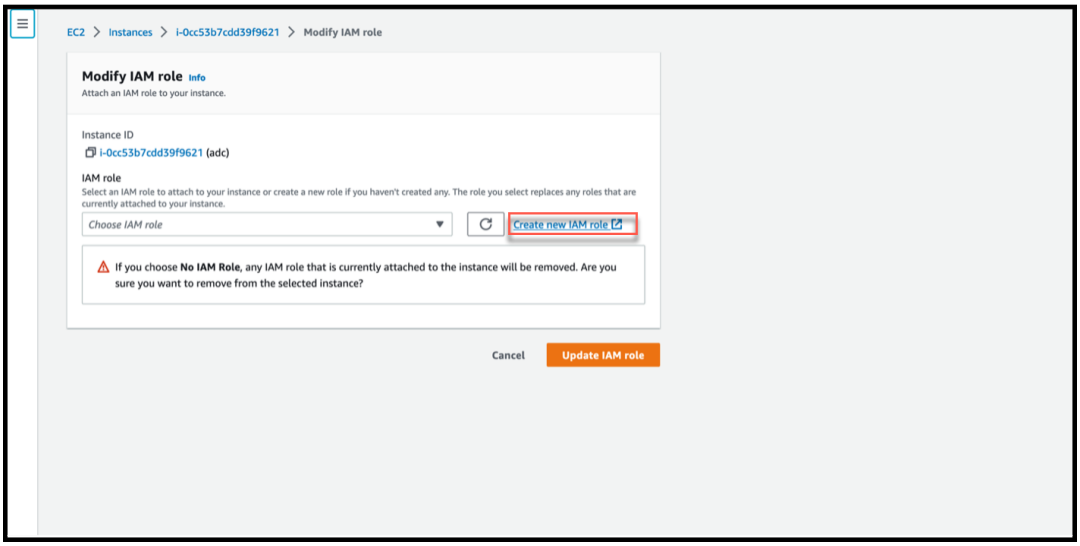


3. Accédez à **Actions > Sécurité > Modifier le rôle IAM**.

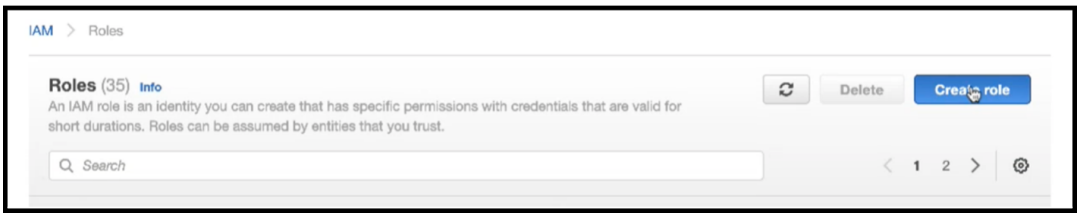


4. Sur la page **Modifier le rôle IAM**, vous pouvez choisir un rôle IAM existant ou créer un rôle IAM.
5. Pour créer un rôle IAM, procédez comme suit :

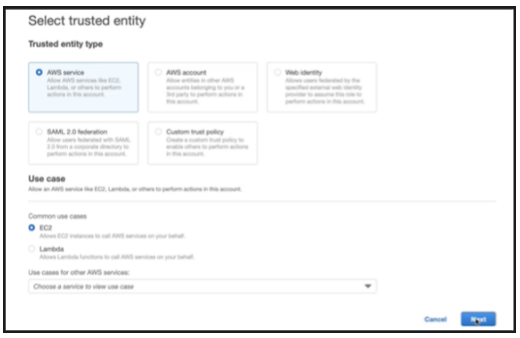
   a) Sur la page **Modifier le rôle IAM**, cliquez sur **Créer un nouveau rôle IAM**.



   b) Sur la page **Rôles**, cliquez sur **Créer un rôle**.



   c) Sélectionnez le **service AWS** sous **Type d'entité de confiance** et **EC2** sous **Cas d'utilisation courants**, puis cliquez sur **Suivant**.



d) Sur la page **Ajouter des autorisations**, cliquez sur **Créer une politique**.

e) Cliquez sur l'onglet **JSON** pour ouvrir l'éditeur JSON.

f) Dans l'éditeur JSON, supprimez tout et collez les autorisations IAM pour la fonctionnalité que vous souhaitez utiliser.

Par exemple, collez les autorisations IAM suivantes pour la fonctionnalité de mise à l'échelle automatique du back-end d'AWS :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
```



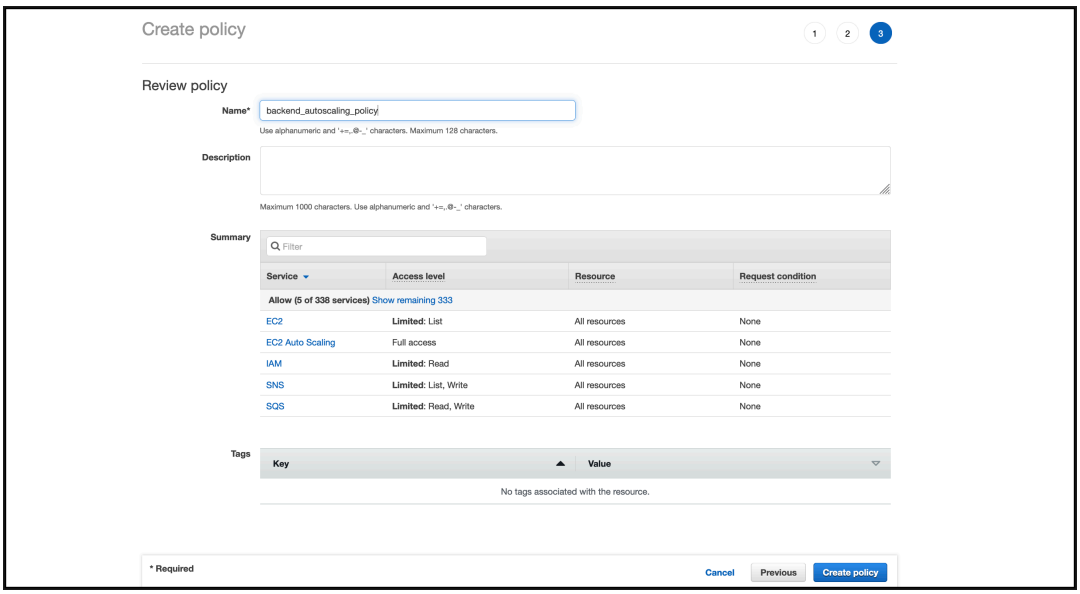
```
                "Action": [
                    "ec2:DescribeInstances",
                    "autoscaling:*",
                    "sns:CreateTopic",
                    "sns:DeleteTopic",
                    "sns:ListTopics",
                    "sns:Subscribe",
                    "sqs:CreateQueue",
                    "sqs:ListQueues",
                    "sqs:DeleteMessage",
                    "sqs:GetQueueAttributes",
                    "sqs:SetQueueAttributes",
                    "iam:SimulatePrincipalPolicy",
                    "iam:GetRole"
                ],
                "Resource": "*"
            }

        ]
    }
```

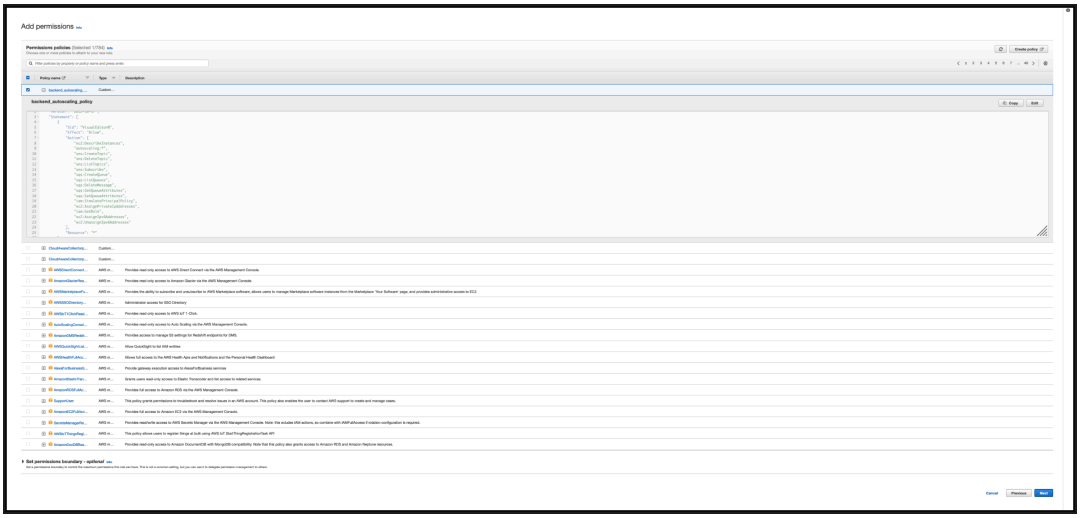
Assurez-vous que la paire clé-valeur « Version » que vous fournissez est identique à celle générée automatiquement par AWS.

g) Cliquez sur **Suivant : Réviser**.

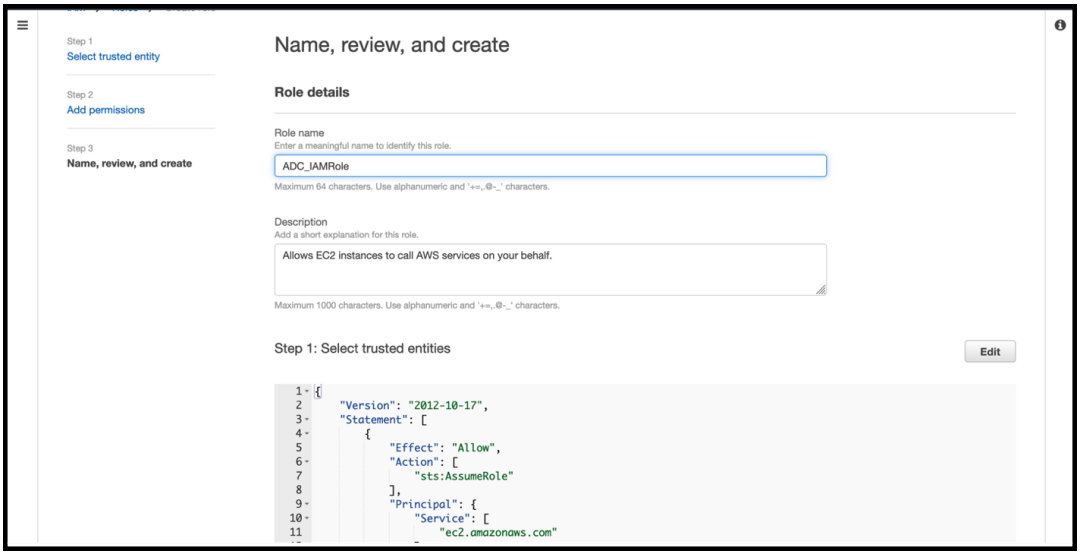
h) Dans l'onglet **Révision de la politique**, donnez un nom valide à la politique, puis cliquez sur **Créer une politique**.



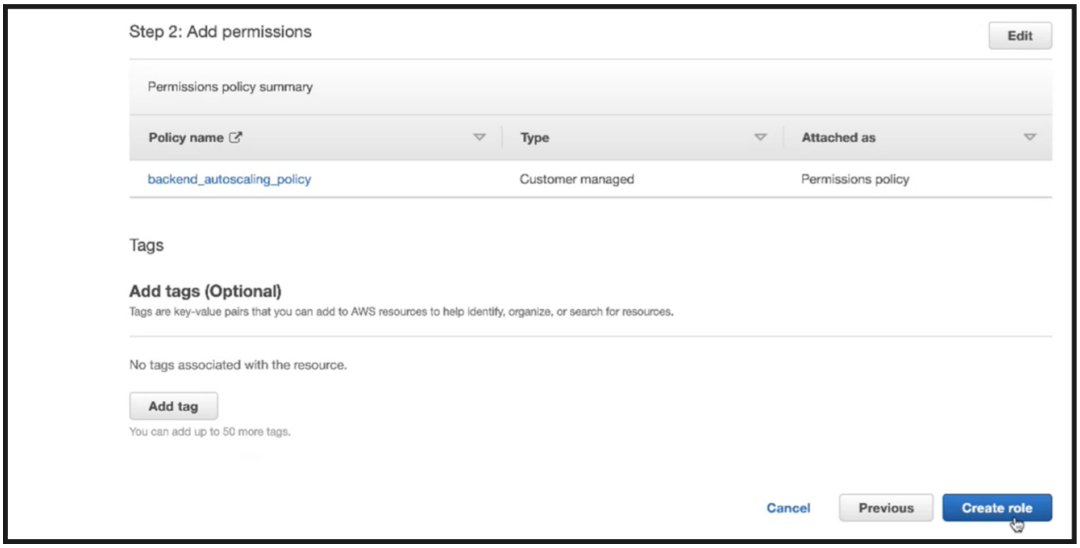
i) Sur la page **Identity Access Management**, cliquez sur le nom de la politique que vous avez créée. Développez la politique pour vérifier l'intégralité du JSON, puis cliquez sur **Suivant**.



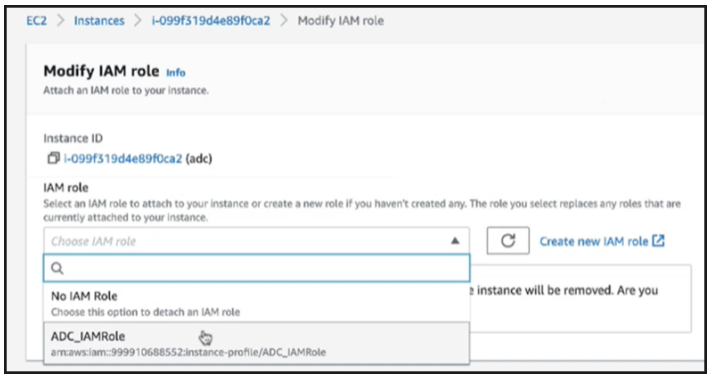
j) Dans la page **Nom, révision et création**, attribuez un nom valide au rôle.



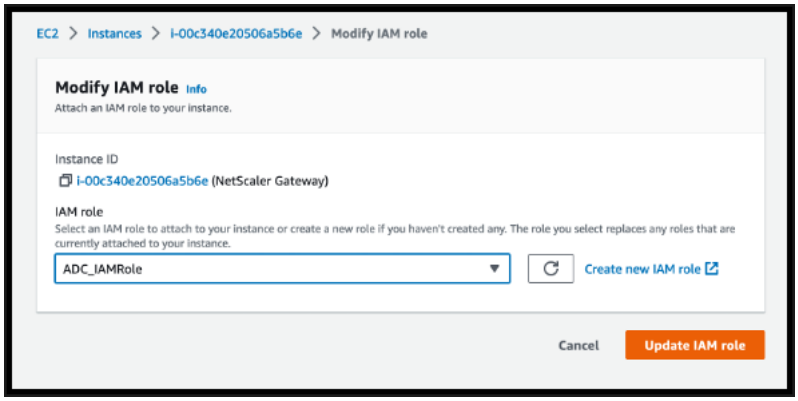
k) Cliquez sur **Créer un rôle**.



6. Répétez les étapes 1, 2 et 3. Cliquez sur le bouton **Actualiser** et sélectionnez le menu déroulant pour voir le rôle que vous avez créé.



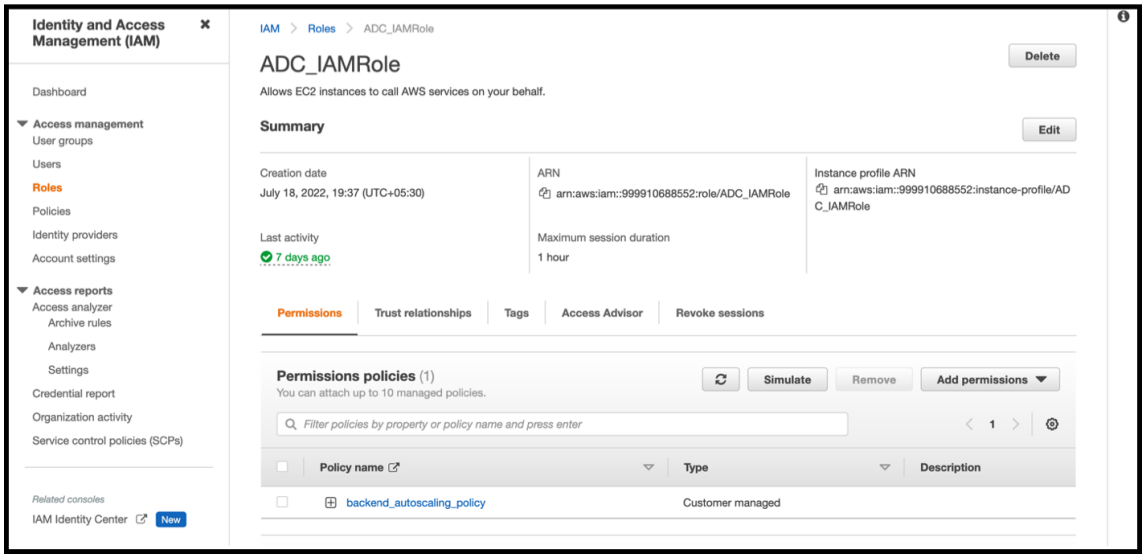
7. Cliquez sur **Mettre à jour le rôle IAM**.



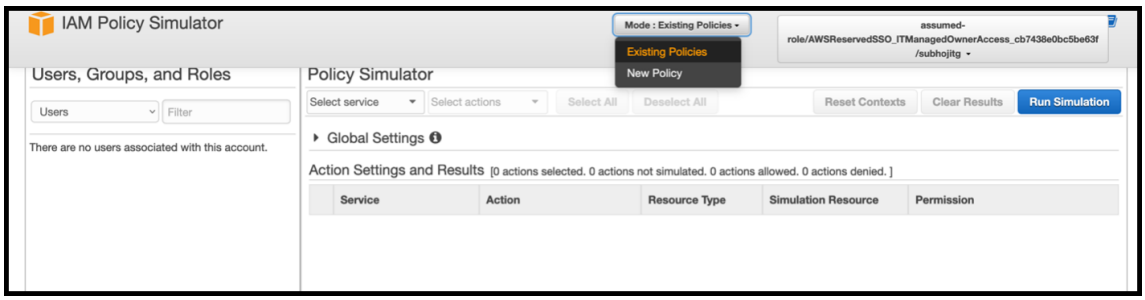
Testez les politiques IAM avec le simulateur de politiques IAM

Le simulateur de politiques IAM est un outil qui vous permet de tester les effets des politiques de contrôle d'accès IAM avant de les mettre en production. Il est plus facile de vérifier et de résoudre les problèmes liés aux autorisations.

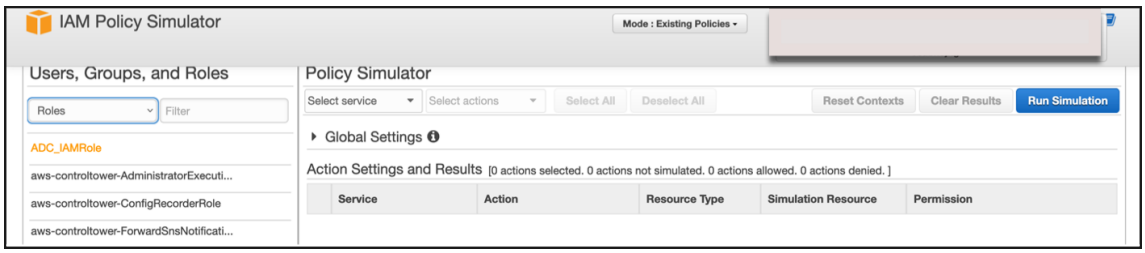
1. **Sur la page**IAM**, sélectionnez le rôle IAM que vous souhaitez tester, puis cliquez sur Simuler.** Dans l'exemple suivant, « ADC_IAMRole » est le rôle IAM. Dans l'exemple suivant, « ADC_IAMRole » est le rôle IAM.



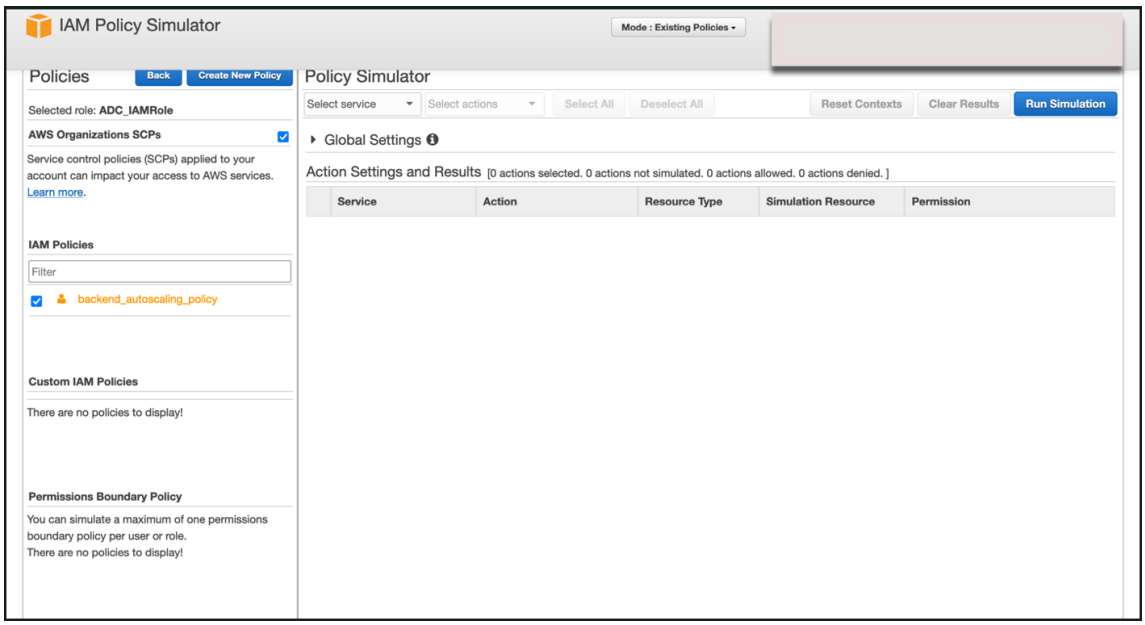
2. Dans la console du **simulateur de politiques IAM**, sélectionnez **Politiques existantes** comme **mode.**



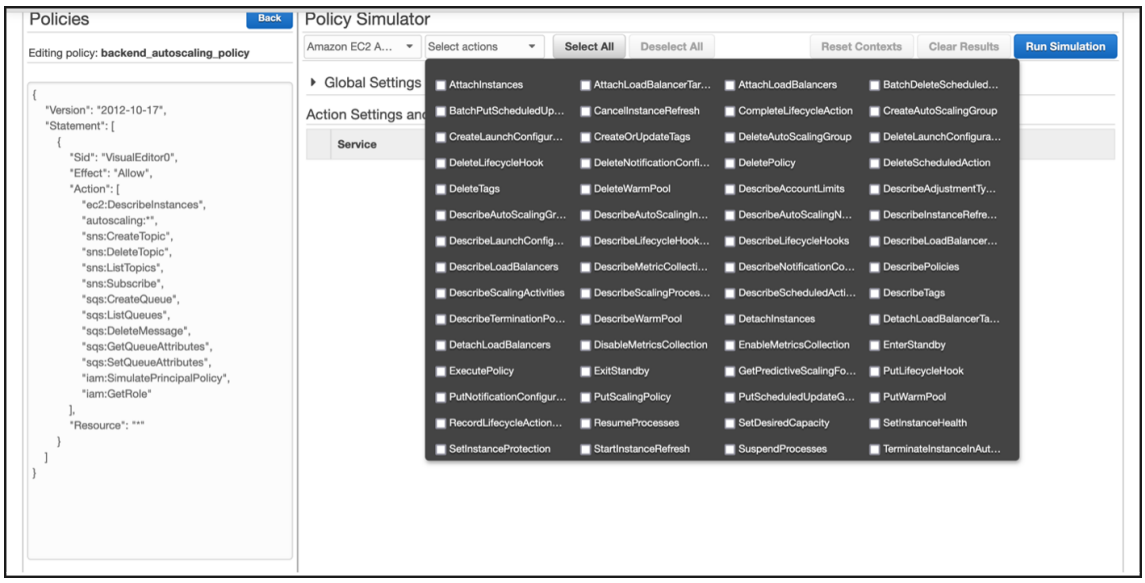
3. Dans l'onglet **Utilisateurs, groupes et rôles**, sélectionnez **Rôles** dans le menu déroulant et choisissez un rôle existant.



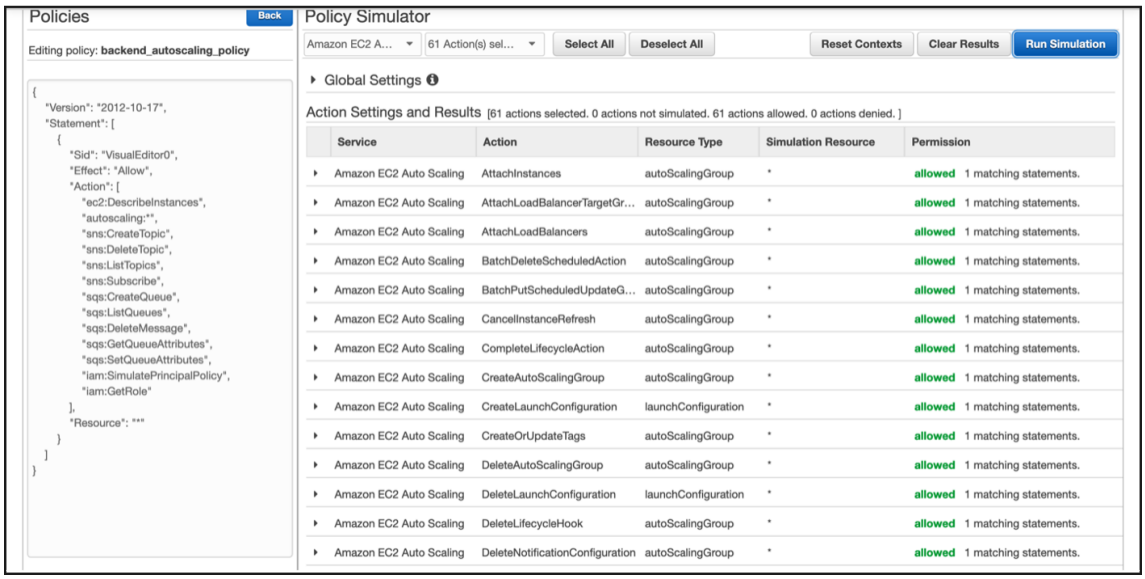
4. Après avoir sélectionné le rôle existant, sélectionnez la politique existante en dessous de celui-ci.



5. Après avoir sélectionné la politique, vous pouvez voir le JSON exact sur le côté gauche de l'écran. Sélectionnez les actions souhaitées dans le menu déroulant **Sélectionner les actions** .



6. Cliquez sur **Exécuter la simulation**.



Pour des informations détaillées, consultez la documentation AWS IAM.

Autres références

Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des instances Amazon EC2

Comment fonctionne une instance NetScaler VPX sur AWS

October 17, 2024

L'instance NetScaler VPX est disponible en tant qu'AMI sur AWS Marketplace et peut être lancée en tant qu'instance EC2 au sein d'un AWS VPC. L'instance AMI NetScaler VPX nécessite au moins 2 processeurs virtuels et 2 Go de mémoire. Une instance EC2 lancée dans un VPC AWS peut également fournir les multiples interfaces, plusieurs adresses IP par interface et les adresses IP publiques et privées nécessaires à la configuration VPX. Chaque instance VPX nécessite au moins trois sous-réseaux IP :

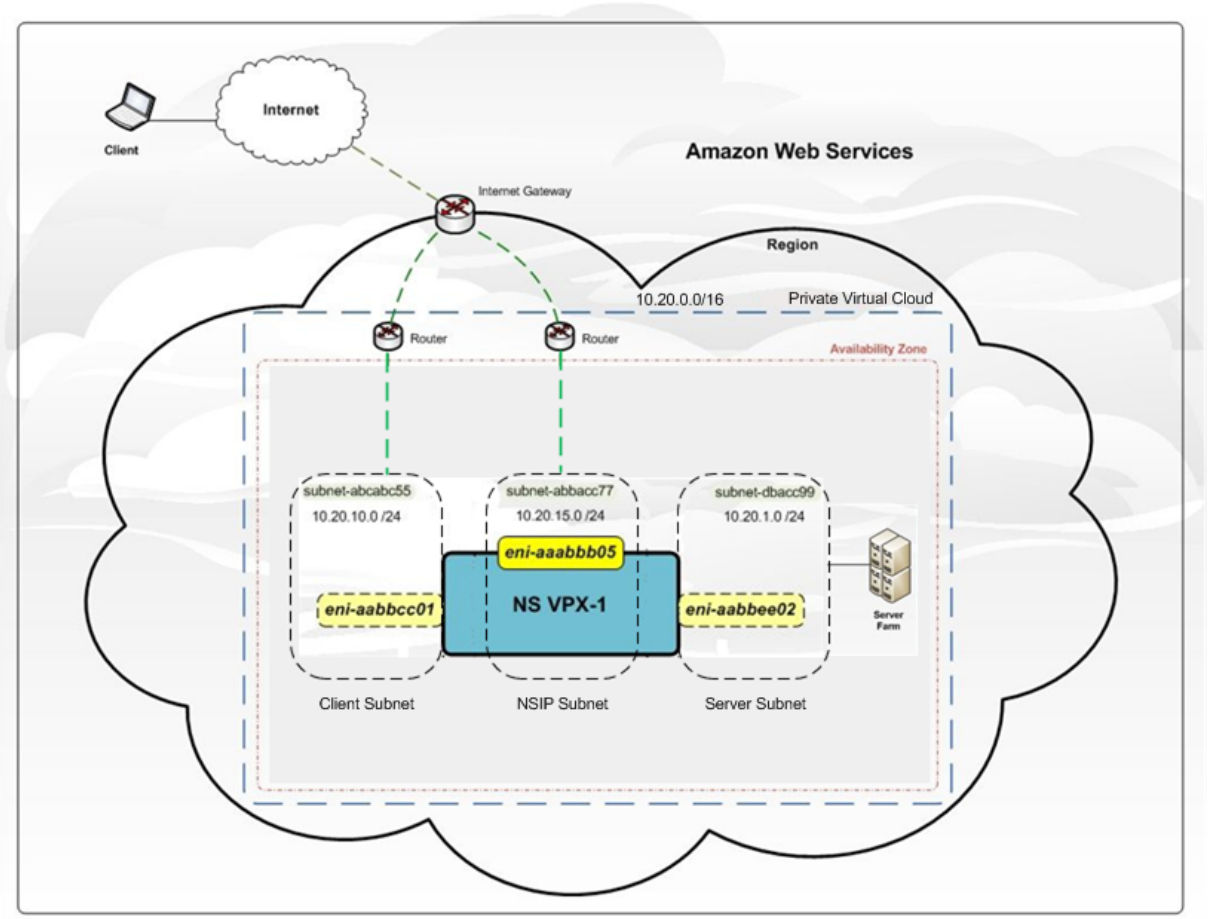
- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le serveur principal (SNIP, MIP, etc.)

Citrix recommande trois interfaces réseau pour une instance VPX standard sur l'installation AWS.

AWS rend actuellement la fonctionnalité multi-IP disponible uniquement pour les instances exécutées au sein d'un VPC AWS. Une instance VPX dans un VPC peut être utilisée pour équilibrer la charge des serveurs exécutant dans des instances EC2. Un Amazon VPC vous permet de créer et de contrôler un environnement réseau virtuel, y compris votre propre plage d'adresses IP, vos sous-réseaux, vos tables de routage et vos passerelles réseau.

> **Remarque :**
>
> Par défaut, vous pouvez créer jusqu'à 5 instances VPC par région AWS pour chaque compte AWS. Vous pouvez demander des limites de VPC plus élevées en soumettant le formulaire http://aws.amazon.com/contact-us/vpc-requestde demande d'Amazon.

Figure 1. Exemple de déploiement d'instance NetScaler VPX sur l'architecture AWS



La figure 1 montre une topologie simple d'un AWS VPC avec un Déploiement de NetScaler VPX. Le VPC AWS comprend :

1. Une passerelle Internet unique pour acheminer le trafic entrant et sortant du VPC.
2. Connectivité réseau entre la passerelle Internet et Internet.
3. Trois sous-réseaux, un pour la gestion, un pour le client et un pour le serveur.
4. Connectivité réseau entre la passerelle Internet et les deux sous-réseaux (gestion et client).
5. Une instance NetScaler VPX autonome déployée au sein du VPC. L'instance VPX a trois ENI, un attaché à chaque sous-réseau.

Déployer une instance autonome NetScaler VPX sur AWS

October 17, 2024

Vous pouvez déployer une instance autonome NetScaler VPX sur AWS à l'aide des options suivantes :

- console Web AWS
- Modèle CloudFormation créé par Citrix
- CLI AWS

Cette rubrique décrit la procédure de déploiement d'une instance NetScaler VPX sur AWS.

Avant de commencer votre déploiement, lisez les rubriques suivantes :

- Conditions préalables
- Directives de limitation et d'utilisation

Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS

Vous pouvez déployer une instance NetScaler VPX sur AWS via la console Web AWS. Le processus de déploiement comprend les étapes suivantes :

1. Créer une paire de clés
2. Créer un cloud privé virtuel (VPC)
3. Ajouter d'autres sous-réseaux
4. Créer des groupes de sécurité et des règles de sécurité
5. Ajouter des tables de routage
6. Créer une passerelle Internet
7. Création d'une instance NetScaler VPX
8. Créez et connectez d'autres interfaces réseau
9. Attachez des adresses IP élastiques à la carte réseau de gestion
10. Se connecter à l'instance VPX

Étape 1 : Créez une paire de clés.

Amazon EC2 utilise une paire de clés pour chiffrer et déchiffrer les informations de connexion. Pour vous connecter à votre instance, vous devez créer une paire de clés, spécifier le nom de la paire de clés lorsque vous lancez l'instance et fournir la clé privée lorsque vous vous connectez à l'instance.

Lorsque vous consultez et lancez une instance à l'aide de l'assistant AWS Launch Instance, vous êtes invité à utiliser une paire de clés existante ou à créer une nouvelle paire de clés. Pour plus d'informations sur la création d'une paire de clés, consultez Paires de clés Amazon EC2.

Étape 2 : Créer un VPC.

Une instance NetScaler VPC est déployée au sein d'un VPC AWS. Un VPC vous permet de définir le réseau virtuel dédié à votre compte AWS. Pour plus d'informations sur AWS VPC, voir Démarrage avec Amazon VPC.

Lors de la création d'un VPC pour votre instance NetScaler VPX, tenez compte des points suivants.

- Utilisez l'option VPC avec un seul sous-réseau public uniquement pour créer un VPC AWS dans une zone de disponibilité AWS.
- Citrix vous recommande de créer au moins **trois sous-réseaux**, des types suivants :
  - Un sous-réseau pour le trafic de gestion. Vous placez l'adresse IP de gestion (NSIP) sur ce sous-réseau. Par défaut, l'interface réseau élastique (ENI) eth0 est utilisée pour l'adresse IP de gestion.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès client (utilisateur vers NetScaler VPX), via lesquels les clients se connectent à une ou plusieurs adresses IP virtuelles (VIP) attribuées aux serveurs virtuels d'équilibrage de charge NetScaler.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès au serveur (VPX vers serveur), via lesquels vos serveurs se connectent aux adresses IP des sous-réseaux appartenant à VPX (SNIP). Pour plus d'informations sur l'équilibrage de charge NetScaler et les serveurs virtuels, les adresses IP virtuelles (VIP) et les adresses IP de sous-réseau (SNIP), consultez :
  - Tous les sous-réseaux doivent se trouver dans la même zone de disponibilité.

Étape 3 : Ajoutez des sous-réseaux.

Lorsque vous avez utilisé l'assistant VPC, un seul sous-réseau a été créé. Selon vos besoins, vous pouvez créer d'autres sous-réseaux. Pour plus d'informations sur la création d'autres sous-réseaux, voir Ajout d'un sous-réseau à votre VPC.

Étape 4 : Créer des groupes de sécurité et des règles de sécurité.

Pour contrôler le trafic entrant et sortant, créez des groupes de sécurité et ajoutez des règles aux groupes. Pour plus d'informations sur la création de groupes et l'ajout de règles, voir Groupes de sécurité pour votre VPC.

Pour les instances NetScaler VPX, l'assistant EC2 fournit des groupes de sécurité par défaut, qui sont générés par AWS Marketplace et sont basés sur les paramètres recommandés par Citrix. Vous pouvez toutefois créer d'autres groupes de sécurité en fonction de vos besoins.

> **Remarque :**
>
> Les ports 22, 80 et 443 doivent être ouverts sur le groupe de sécurité pour les accès SSH, HTTP et HTTPS respectivement.

Étape 5 : Ajoutez des tables de routage.

La table de routage contient un ensemble de règles, appelées routes, qui sont utilisées pour déterminer où le trafic réseau est dirigé. Chaque sous-réseau de votre VPC doit être associé à une table de routage. Pour plus d'informations sur la création d'une table de routage, consultez Tables de routage.

Étape 6 : Créer une Gateway Internet.

Une passerelle Internet a deux objectifs : fournir une cible dans les tables de routage de votre VPC pour le trafic routable sur Internet et effectuer la traduction d'adresses réseau (NAT) pour les instances auxquelles des adresses IPv4 publiques ont été attribuées.

Créez une Gateway Internet pour le trafic Internet. Pour plus d'informations sur la création d'une passerelle Internet, reportez-vous à la section Attachement d'une passerelle Internet.

Étape 7 : Créez une instance NetScaler VPX à l'aide du service AWS EC2.

Pour créer une instance NetScaler VPX à l'aide du service AWS EC2, procédez comme suit.

1. Dans le tableau de bord AWS, accédez à **Calcul > EC2 > Launch Instance > AWS Marketplace**.

   Avant de cliquer sur **Launch Instance**, assurez-vous que votre région est correcte en consultant la note qui apparaît sous **Launch Instance**.

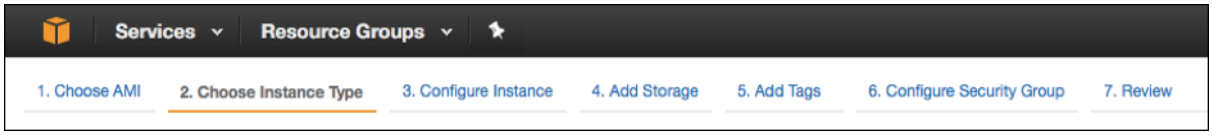
   

2. Dans la barre de recherche sur AWS Marketplace, effectuez une recherche à l'aide du mot clé NetScaler VPX.
3. Sélectionnez la version à déployer, puis cliquez sur **Sélectionner**. Pour la version NetScaler VPX, vous disposez des options suivantes :

   - Une version sous licence
   - Appliance NetScaler VPX Express (Il s'agit d'une appliance virtuelle gratuite, disponible depuis NetScaler 12.0 56.20.)
   - Apportez votre propre appareil

L'assistant de lancement d'instance démarre. Suivez l'assistant pour créer une instance. L'assistant vous invite à :

- Choisir le type d'instance
- Configurer l'instance
- Ajouter un espace de stockage
- Ajouter des balises
- Configurer le groupe de sécurité
- Critique



Étape 8 : Créez et connectez d'autres interfaces réseau.

Créez deux interfaces réseau supplémentaires pour VIP et SNIP. Pour plus d'informations sur la création d'autres interfaces réseau, reportez-vous à la section Création d'une interface réseau .

Après avoir créé les interfaces réseau, vous devez les attacher à l'instance VPX. Avant de joindre l'interface, arrêtez l'instance VPX, connectez l'interface et mettez l'instance sous tension. Pour plus d'informations sur la connexion d'interfaces réseau, consultez la section Attachement d'une interface réseau lors du lancement d'une instance .

Étape 9 : Allouer et associer des IP élastiques.

Si vous attribuez une adresse IP publique à une instance EC2, elle reste attribuée uniquement jusqu'à ce que l'instance soit arrêtée. Après cela, l'adresse est libérée dans le pool. Lorsque vous redémarrez l'instance, une nouvelle adresse IP publique est attribuée.

En revanche, une adresse IP élastique (EIP) reste affectée jusqu'à ce que l'adresse soit dissociée d'une instance.

Allouer et associer une IP élastique pour la carte réseau de gestion. Pour plus d'informations sur la façon d'allouer et d'associer des adresses IP élastiques, consultez les rubriques suivantes :

- Allocation d'une adresse IP élastique
- Associer une adresse IP Elastic à une instance en cours d'exécution

Ces étapes complètent la procédure de création d'une instance NetScaler VPX sur AWS. Cela peut prendre quelques minutes avant que l'instance soit prête. Vérifiez que votre instance a passé avec succès ses contrôles d'état. Vous pouvez consulter ces informations dans la colonne **Contrôles d'état** de la page Instances.

Étape 10 : Se connecter à l'instance VPX.

Après avoir créé l'instance VPX, vous connectez l'instance à l'aide de l'interface graphique et d'un client SSH.

- GUI

Les informations d'identification d'administrateur par défaut pour accéder à une instance NetScaler VPX sont les suivantes :

Nom d'utilisateur : `nsroot`

Mot de passe : le mot de passe par défaut du compte root ns est défini sur l'ID d'instance AWS de l'instance NetScaler VPX. Lors de votre première connexion, vous êtes invité à modifier le mot de passe

pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez vous connecter avec le mot de passe par défaut. Modifiez à nouveau le mot de passe lorsque vous y êtes invité.

- Client SSH

Dans la console de gestion AWS, sélectionnez l'instance NetScaler VPX et cliquez sur Connect. Suivez les instructions données sur la page **Connexion à votre instance** . Suivez les instructions données sur la page **Se connecter à votre instance** .

Pour plus d'informations sur le déploiement d'une instance autonome NetScaler VPX sur AWS à l'aide de la console Web AWS, consultez Scénario : instance autonome

Configurer une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation

Vous pouvez utiliser le modèle CloudFormation fourni par Citrix pour automatiser le lancement d'une instance VPX. Le modèle fournit des fonctionnalités permettant de lancer une seule instance NetScaler VPX ou de créer un environnement de haute disponibilité avec deux instances NetScaler VPX.

Vous pouvez lancer le modèle depuis AWS Marketplace ou GitHub.

Le modèle CloudFormation nécessite un environnement VPC existant et lance une instance VPX avec trois interfaces réseau élastiques (ENI). Avant de démarrer le modèle CloudFormation, assurez-vous de remplir les conditions suivantes :

- Un cloud privé virtuel (VPC) AWS
- Trois sous-réseaux au sein du VPC : un pour la gestion, un pour le trafic client et un pour les serveurs principaux
- Une paire de clés EC2 pour activer l'accès SSH à l'instance
- Un groupe de sécurité avec des ports UDP 3003, TCP 3009—3010, HTTP et SSH ouverts

Consultez la section « Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS » ou la documentation AWS pour plus d'informations sur la manière de remplir les conditions préalables.

Regardez cette vidéo pour découvrir comment configurer et lancer une instance autonome NetScaler VPX à l'aide du modèle Citrix CloudFormation disponible sur AWS Marketplace.

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Un rôle IAM n'est pas obligatoire pour un déploiement autonome. Citrix vous recommande toutefois de créer et d'associer un rôle IAM doté des privilèges requis à l'instance, en cas de besoin futur. Le rôle IAM garantit que l'instance autonome est facilement convertie en nœud haute disponibilité avec SR-IOV, si nécessaire.

Pour plus d'informations sur les privilèges requis, consultez Configuration des instances NetScaler VPX pour utiliser l'interface réseau SR-IOV.

> **Remarque :**
>
> Si vous déployez une instance NetScaler VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut. Si vous déployez une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est « Oui ». Si vous souhaitez désactiver le service CloudWatch, sélectionnez « Non ». Pour plus d'informations, consultez Surveillez vos instances à l'aide d'Amazon CloudWatch

Configurer une instance NetScaler VPX à l'aide de l'AWS CLI

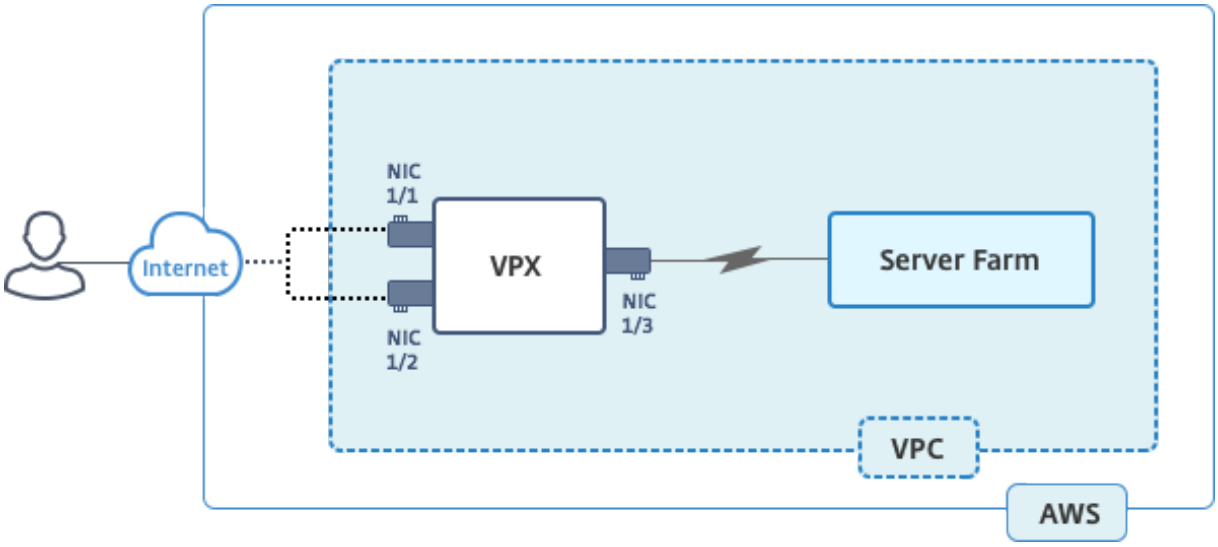
Vous pouvez utiliser l'interface de ligne de commande AWS pour lancer des instances. Pour plus d'informations, consultez la documentation de l'interface de ligne de commande AWS.

Scénario : instance autonome

October 17, 2024

Ce scénario montre comment déployer une instance EC2 autonome NetScaler VPX dans AWS à l'aide de l'interface graphique AWS. Créez une instance VPX autonome avec trois cartes réseau. L'instance, qui est configurée comme un serveur virtuel d'équilibrage de charge, communique avec les serveurs principaux (le parc de serveurs). Pour cette configuration, configurez les routes de communication requises entre l'instance et les serveurs dorsaux, et entre l'instance et les hôtes externes sur Internet public.

Pour plus de détails sur la procédure de déploiement d'une instance VPX, consultez Déployer une instance autonome NetScaler VPX sur AWS.

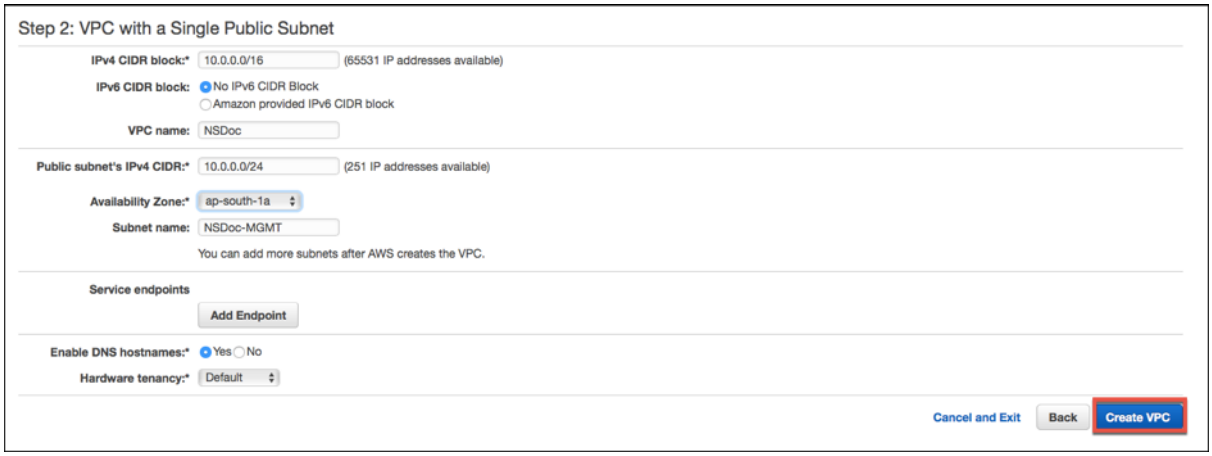


Créez trois cartes réseau. Chaque carte réseau peut être configurée avec une paire d'adresses IP (publique et privée). Les cartes réseau répondent aux objectifs suivants.

Carte d'interface réseau	Motif	Associé à
eth0	Sert le trafic de gestion (NSIP)	Une adresse IP publique et une adresse IP privée
eth1	Sert le trafic côté client (VIP)	Une adresse IP publique et une adresse IP privée
eth2	Communication avec les serveurs back-end (SNIP)	Une adresse IP publique (l'adresse IP privée n'est pas obligatoire)

Étape 1 : Créer un VPC.

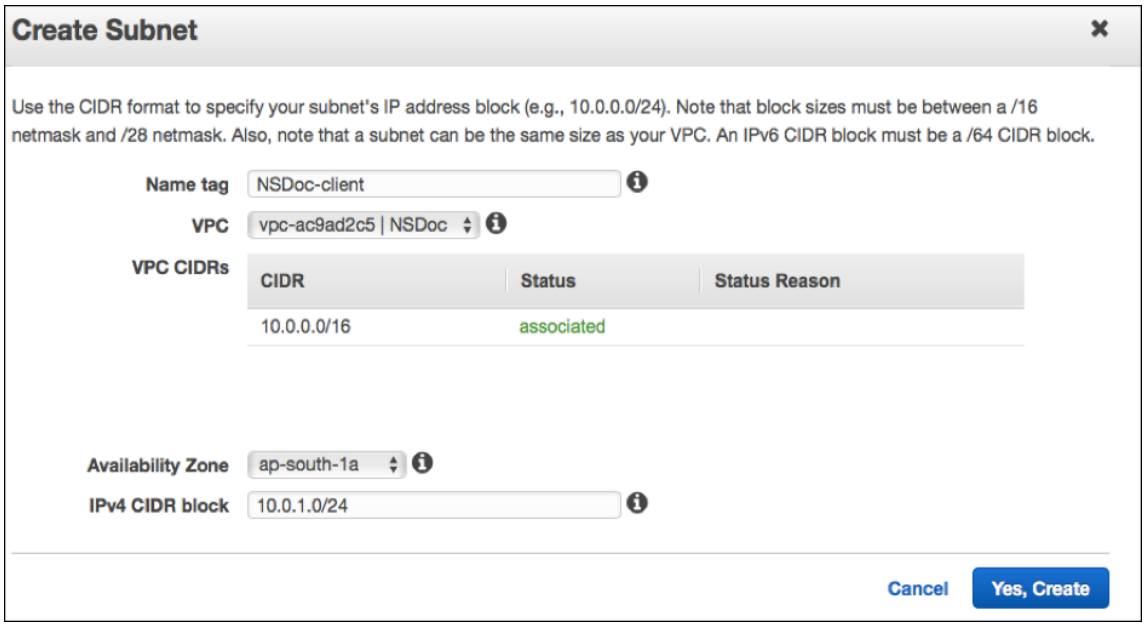
1. Connectez-vous à la console Web AWS et accédez à **Networking & Content Delivery** > **VPC.** Cliquez sur **Démarrer l'assistant VPC**. Cliquez sur **Démarrer l'Assistant VPC**.
2. **Sélectionnez**VPC avec un seul sous-réseau public**et cliquez sur Sélectionner.**
3. Définissez le bloc d'adresse IP sur 10.0.0.0/16, pour ce scénario.
4. Donnez un nom au VPC.
5. Définissez le sous-réseau public sur 10.0.0.0/24. (Il s'agit du réseau de gestion).
6. Sélectionnez une zone de disponibilité.
7. Donnez un nom au sous-réseau.
8. Cliquez sur Créer un **VPC**.



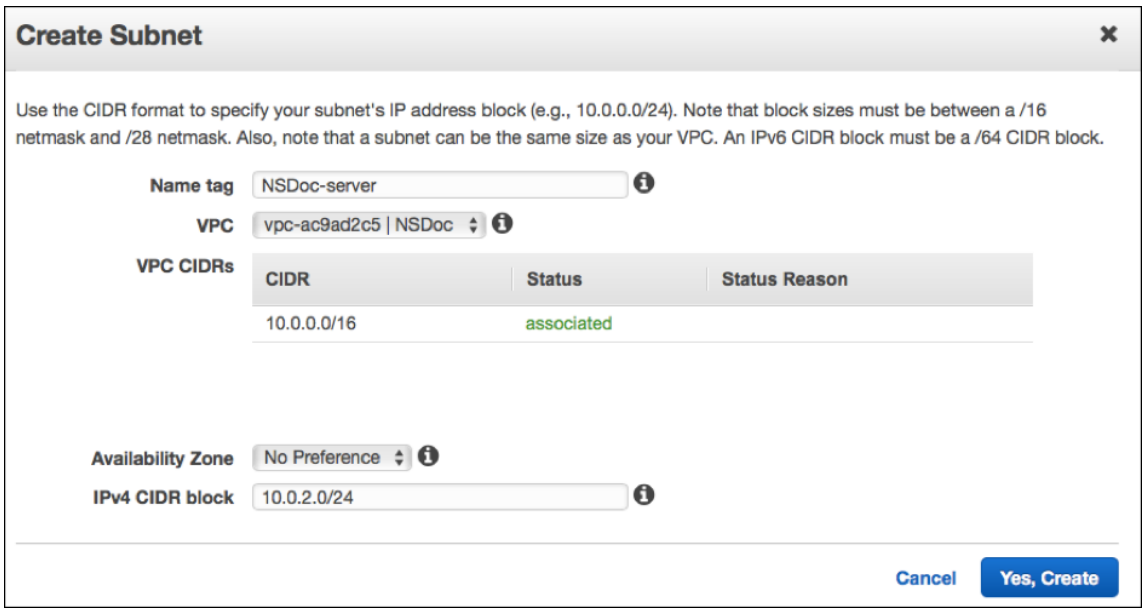
Étape 2 : Création de sous-réseaux supplémentaires

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets, Create Subnet après avoir saisi les informations suivantes.

   - Nom tag : indiquez un nom pour votre sous-réseau.
   - VPC : choisissez le VPC pour lequel vous créez le sous-réseau.
   - Zone de disponibilité : choisissez la zone de disponibilité dans laquelle vous avez créé le VPC à l'étape 1.
   - Bloc d'adresse CIDR IPv4 : Spécifiez un bloc d'adresse CIDR IPv4 pour votre sous-réseau. Pour ce scénario, choisissez 10.0.1.0/24.

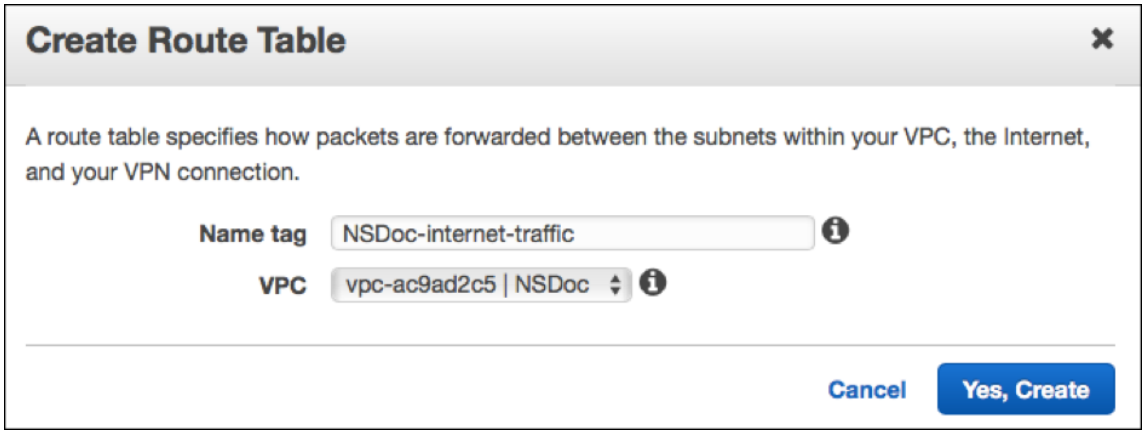


3. Répétez les étapes pour créer un sous-réseau supplémentaire pour les serveurs principaux.



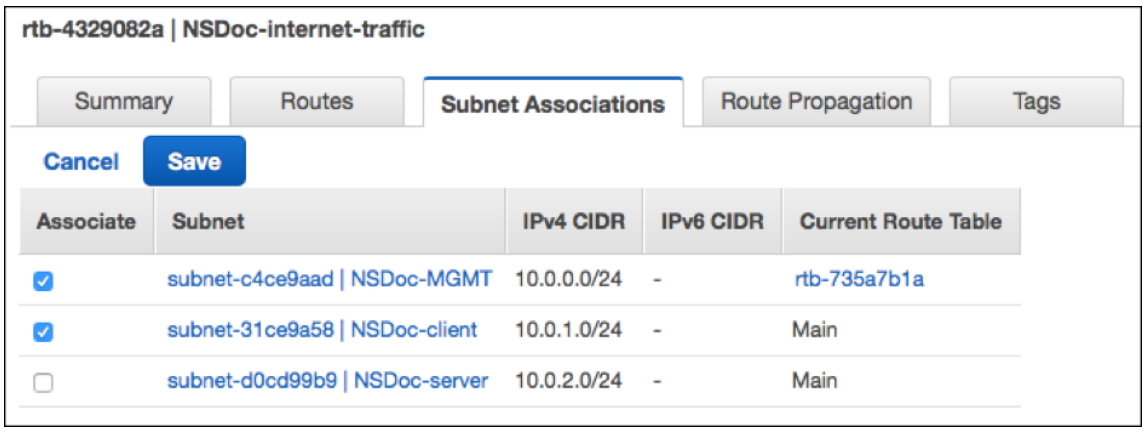
Étape 3 : Création d'une table de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez **Tables de routage** > **Créer une table de routage.**
3. Dans la fenêtre Créer une table de routage, ajoutez un nom et sélectionnez le VPC que vous avez créé à l'étape 1.
4. Cliquez sur **Yes, Create**.

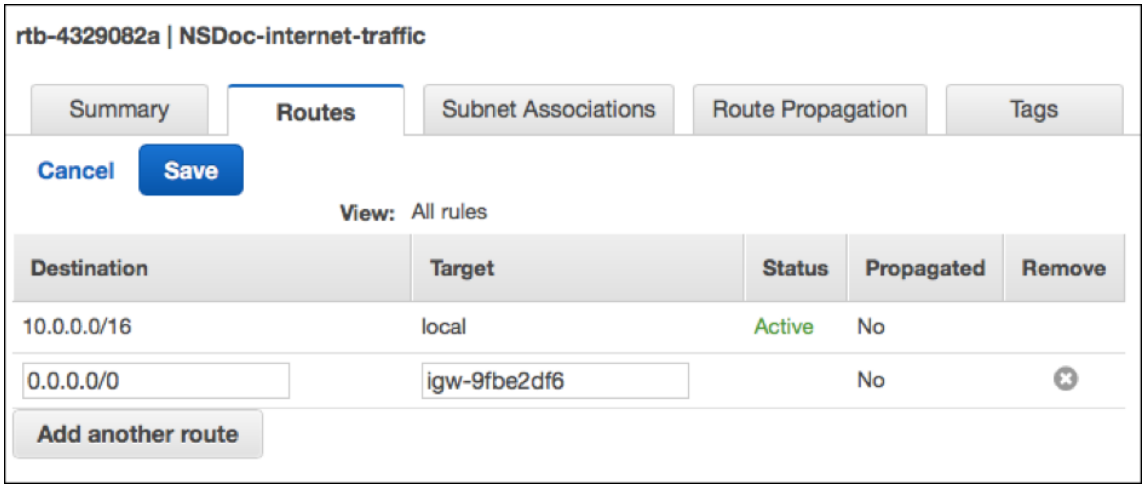


   La table de routage est affectée à tous les sous-réseaux que vous avez créés pour ce VPC, de sorte que le routage du trafic à partir d'une instance d'un sous-réseau peut atteindre une instance d'un autre sous-réseau.

5. Cliquez sur **Associations de sous-réseaux**, puis cliquez sur **Modifier**.
6. Cliquez sur le sous-réseau client et de gestion, puis sur Enregistrer. Cela crée une table de routage pour le trafic Internet uniquement.



7. Cliquez sur **Itinéraires > Modifier > Ajouter un autre itinéraire**.
8. Dans le champ Destination, ajoutez 0.0.0.0/0, puis cliquez sur le champ Cible pour sélectionner igw- \ <xxxx> la passerelle Internet créée automatiquement par l'assistant VPC.
9. Cliquez sur **Enregistrer**.

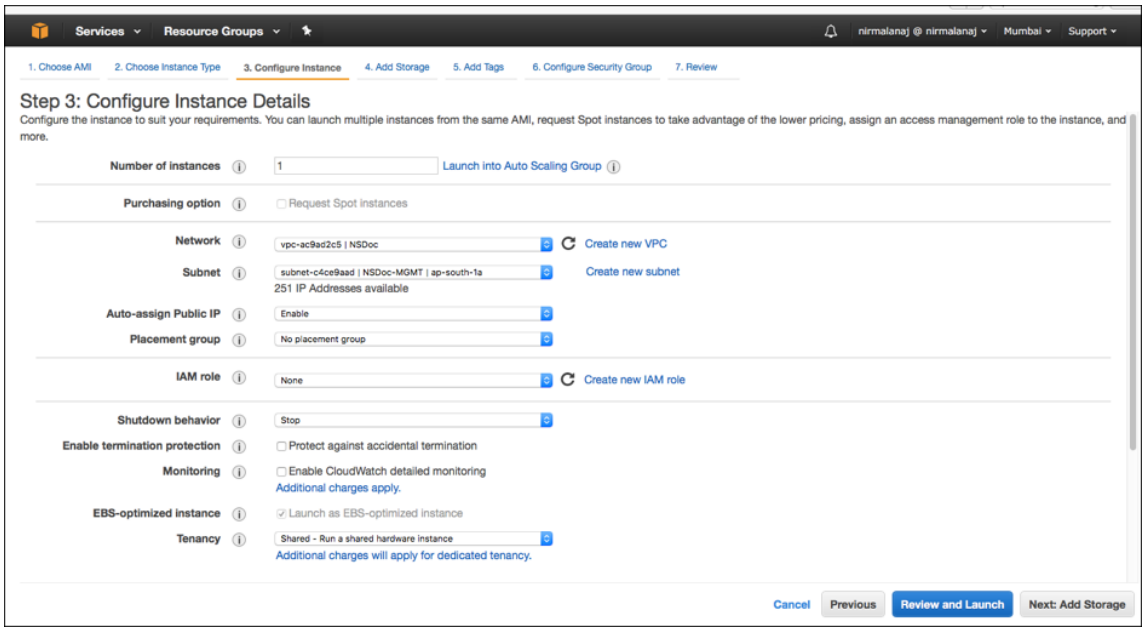


10. Suivez les étapes pour créer une table de routage pour le trafic côté serveur.

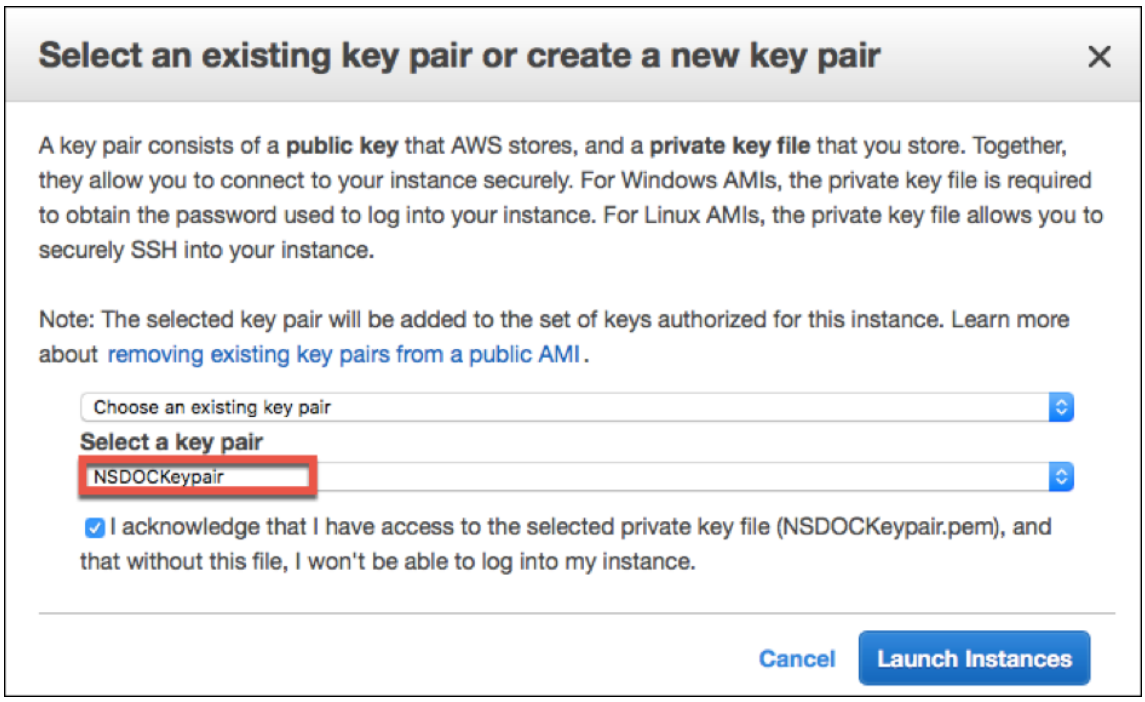
Étape 4 : Création d'une instance NetScaler VPX

1. Connectez-vous à la console de gestion AWS et cliquez sur **EC2** sous **Compute**.
2. Cliquez sur AWS Marketplace. Dans la barre de recherche sur AWS Marketplace, tapez NetScaler VPX et appuyez sur Entrée. Les éditions NetScaler VPX disponibles s'affichent.
3. Cliquez sur **Sélectionner** pour choisir l'édition NetScaler VPX souhaitée. L'assistant d'instance EC2 démarre.
4. Sur la page **Choisir le type d'instance**, sélectionnez **m4. Xlarge** (recommandé) et cliquez sur **Suivant : Configurer les détails de l'instance**.
5. Dans la page Configurer les détails de l'instance, sélectionnez les éléments suivants, puis cliquez sur **Suivant : Ajouter un stockage**.

- Nombre d'instances : 1
- Réseau : le VPC créé à l'étape 1
- Sous-réseau : le sous-réseau de gestion
- Attribuer automatiquement une adresse IP publique : activer



6. Dans la page Ajouter un stockage, sélectionnez l'option par défaut et cliquez sur **Suivant : Ajouter des balises**.
7. Dans la page Ajouter des balises, ajoutez un nom pour l'instance et cliquez sur **Suivant : Configurer le groupe de sécurité**.
8. Sur la page Configurer le groupe de sécurité, sélectionnez l'option par défaut (générée par AWS Marketplace et basée sur les paramètres recommandés par Citrix Systems), puis cliquez sur **Vérifier et lancer > Lancer**.
9. Vous êtes invité à sélectionner une paire de clés existante ou à créer une nouvelle paire de clés. Dans la liste déroulante Sélectionner une paire de clés, sélectionnez la paire de clés que vous avez créée comme condition préalable (voir la section Prérequis).
10. Cochez la case pour reconnaître la paire de clés et cliquez sur **Lancer les instances**.



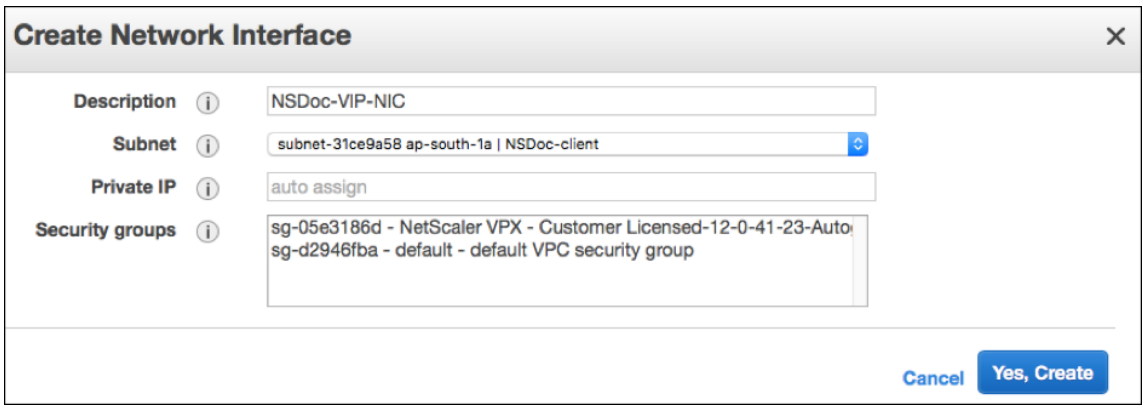
L'assistant de lancement de l'instance affiche l'état du lancement et l'instance apparaît dans la liste des instances lorsqu'elle est complètement lancée.

Pour vérifier l'instance, accédez à la console AWS et cliquez sur **EC2 > Instances en cours d'exécution**. Sélectionnez l'instance et ajoutez un nom. Assurez-vous que l'état de l'instance est en cours d'exécution et que les contrôles d'état sont terminés.

Étape 5 : Créez et connectez d'autres interfaces réseau.

Lorsque vous avez créé le VPC, une seule interface réseau lui était associée. Ajoutez maintenant deux autres interfaces réseau au VPC, pour le VIP et le SNIP.

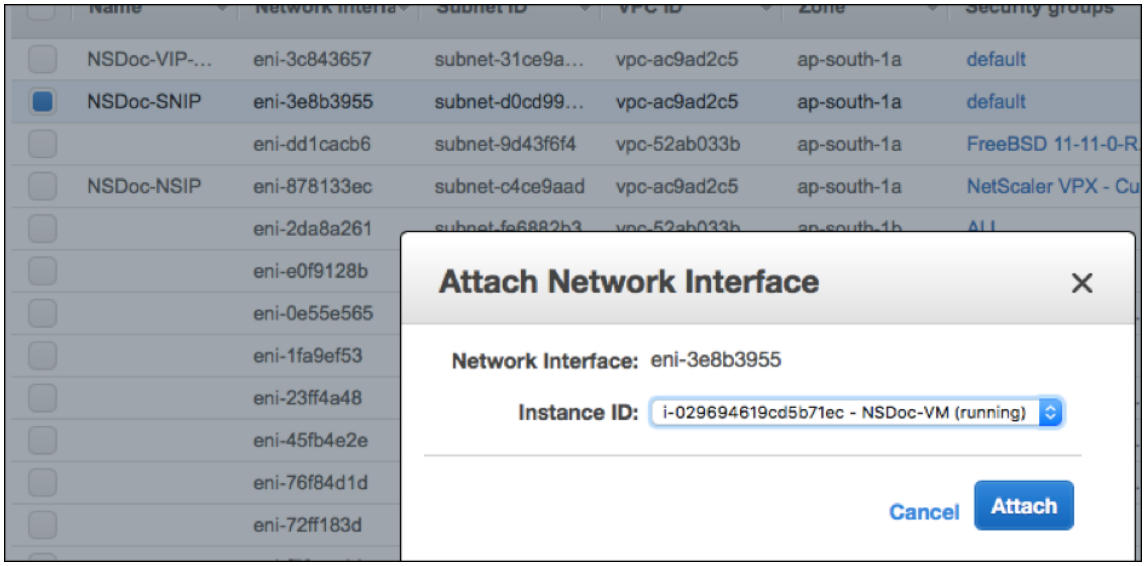
1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Interfaces réseau.
3. Choisissez Create Network Interface.
4. Pour **Description**, entrez un nom descriptif.
5. Pour **Sous-réseau**, sélectionnez le sous-réseau que vous avez créé précédemment pour le VIP.
6. Pour **IP privée**, laissez l'option par défaut.
7. Pour les groupes de sécurité **, sélectionnez le groupe.
8. Cliquez sur **Yes, Create**.



9. Une fois l'interface réseau créée, attribuez-lui un nom.
10. Répétez les étapes pour créer une interface réseau pour le trafic côté serveur.

Connectez les interfaces réseau :

1. Dans le volet de navigation, choisissez Interfaces réseau.
2. Sélectionnez l'interface réseau et cliquez sur **Attacher**.
3. Dans la boîte de dialogue Attacher une interface réseau, sélectionnez l'instance et cliquez sur **Attacher**.



Étape 6 : attachez une adresse IP élastique au NSIP.

1. Depuis la console de gestion AWS, accédez à **RÉSEAU ET SÉCURITÉ > Elastic IPs**.
2. Vérifiez s'il existe un EIP gratuit à joindre. Si ce n'est pas le cas, cliquez sur **Attribuer une nouvelle adresse**.
3. Sélectionnez l'adresse IP nouvellement attribuée et choisissez **Actions > Adresse associée**.

4. Cliquez sur le bouton radio de **l'interface réseau** .
5. Dans la liste déroulante Interface réseau, sélectionnez la carte réseau de gestion.
6. Dans le menu déroulant **Private IP**, sélectionnez l'adresse IP générée par AWS.
7. Cochez la case **Réassociation** .
8. Cliquez sur **Associer**.

Accédez à l'instance VPX :

Après avoir configuré une instance NetScaler VPX autonome avec trois cartes réseau, connectez-vous à l'instance VPX pour terminer la configuration côté NetScaler. Utilisation des options suivantes :

- GUI : saisissez l'adresse IP publique de la carte réseau de gestion dans le navigateur. Ouvrez une session en utilisant `nsroot` comme nom d'utilisateur et l'ID d'instance (i-0c1ffe1d987817522) comme mot de passe.

> **Remarque :**
>
> Lors de votre première connexion, vous êtes invité à modifier le mot de passe pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez vous connecter avec le mot de passe par défaut. Modifiez à nouveau le mot de passe à l'invite et enregistrez la configuration.

- SSH : ouvrez un client SSH et tapez :

```
ssh -i \\&#060;location of your private key\\&#062; ns root@\\&#060;
public DNS of the instance\\&#062;
```

Pour trouver le DNS public, cliquez sur l'instance, puis sur **Connect**.

Informations connexes :

- Pour configurer les adresses IP appartenant à NetScaler (NSIP, VIP et SNIP), consultez la section Configuration des adresses IP appartenant à NetScaler.

- Vous avez configuré une version BYOL de l'appliance NetScaler VPX. Pour plus d'informations, consultez le Guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426

Télécharger une licence NetScaler VPX

October 17, 2024

Après le lancement de l'instance sous licence NetScaler VPX-Customer depuis la place de marché AWS, une licence est requise. Pour plus d'informations sur les licences VPX, reportez-vous à la section Présentation des licences.

Vous devez :

1. Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
2. Télécharger la licence sur l'instance.

S'il s'agit d'une instance de marketplace **payante**, vous n'avez pas besoin d'installer une licence. Le jeu de fonctionnalités et les performances corrects s'activent automatiquement.

Si vous utilisez une instance NetScaler VPX dont le numéro de modèle est supérieur à VPX 5000, le débit réseau peut ne pas être le même que celui spécifié par la licence de l'instance. Toutefois, d'autres fonctionnalités, telles que le débit SSL et les transactions SSL par seconde, peuvent s'améliorer.

La bande passante réseau de 5 Gbit/s est observée dans le type d'`c4.8xlarge` instance.

Comment migrer l'abonnement AWS vers BYOL

Cette section décrit la procédure de migration de l'abonnement AWS vers Bring your own license (BYOL), et inversement.

Procédez comme suit pour migrer un abonnement AWS vers BYOL :

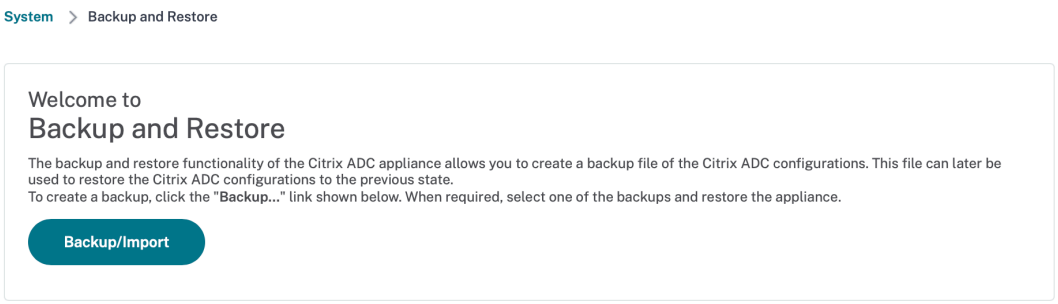
> **Remarque :**
>
> Les **étapes 2** et **3** sont effectuées sur l'instance NetScaler VPX, et toutes les autres étapes sont effectuées sur le portail AWS.

1. Créez une instance BYOL EC2 à l'aide de NetScaler VPX - Customer Licensed dans la même zone de disponibilité que l'ancienne instance EC2 qui possède le même groupe de sécurité, le même rôle IAM et le même sous-réseau. La nouvelle instance EC2 ne doit avoir qu'une seule interface ENI.

2. Pour sauvegarder les données de l'ancienne instance EC2 à l'aide de l'interface graphique NetScaler, procédez comme suit.

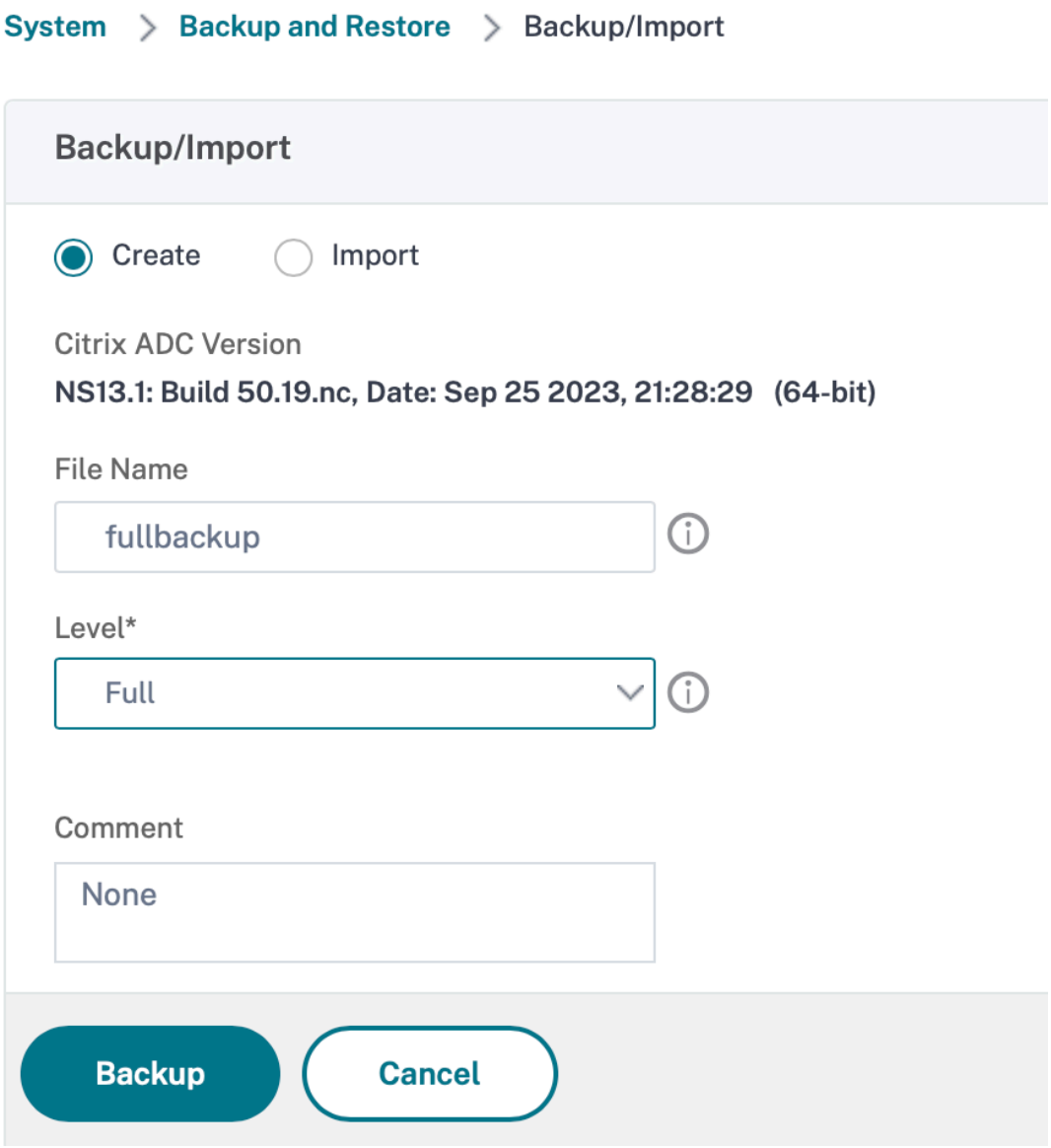
   a) Accédez à **Système > Sauvegarde et restauration**.

   b) Dans la page **Bienvenue**, cliquez sur **Sauvegarde/Importation** pour démarrer le processus.

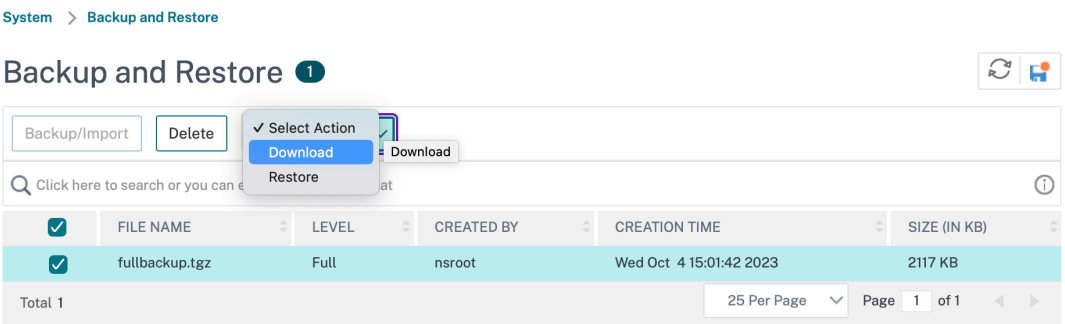


   c) Dans la page **Sauvegarde/Importation**, renseignez les informations suivantes :

   - **Nom** : nom du fichier de sauvegarde.
   - **Niveau** : sélectionnez le niveau de sauvegarde **complet**.
   - **Commentaire** : fournissez une brève description de la sauvegarde.



d) Cliquez sur **Sauvegarde**. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et le télécharger sur votre machine locale.



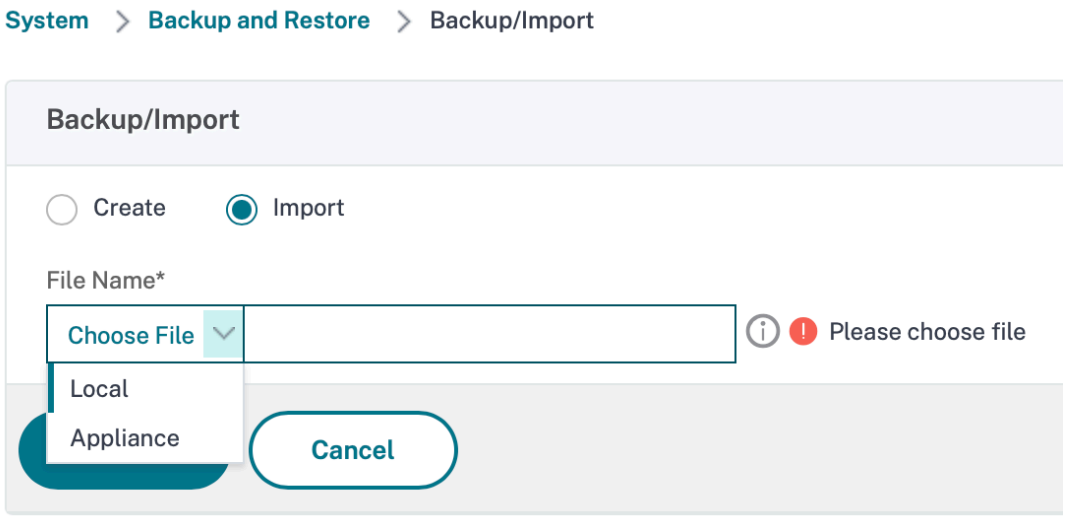
3. Pour restaurer les données sur la nouvelle instance EC2 à l'aide de l'interface graphique

NetScaler, procédez comme suit :

a) Accédez à **Système > Sauvegarde et restauration**.

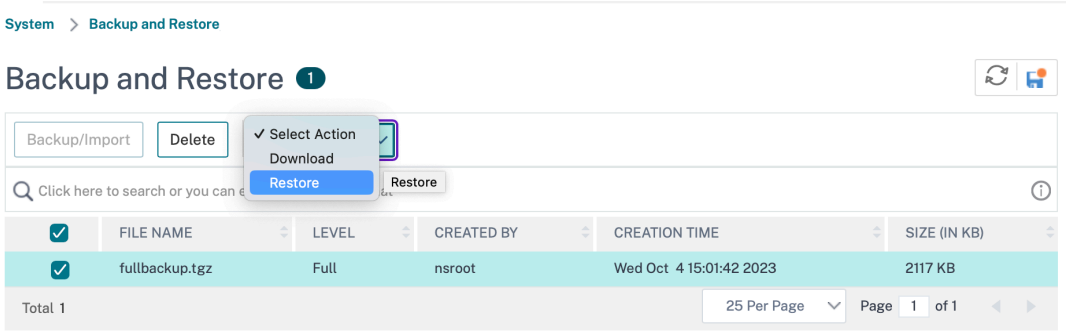
b) Cliquez sur **Sauvegarde/Importer** pour démarrer le processus.

c) Sélectionnez l'option **Importer** et téléchargez le fichier de sauvegarde.

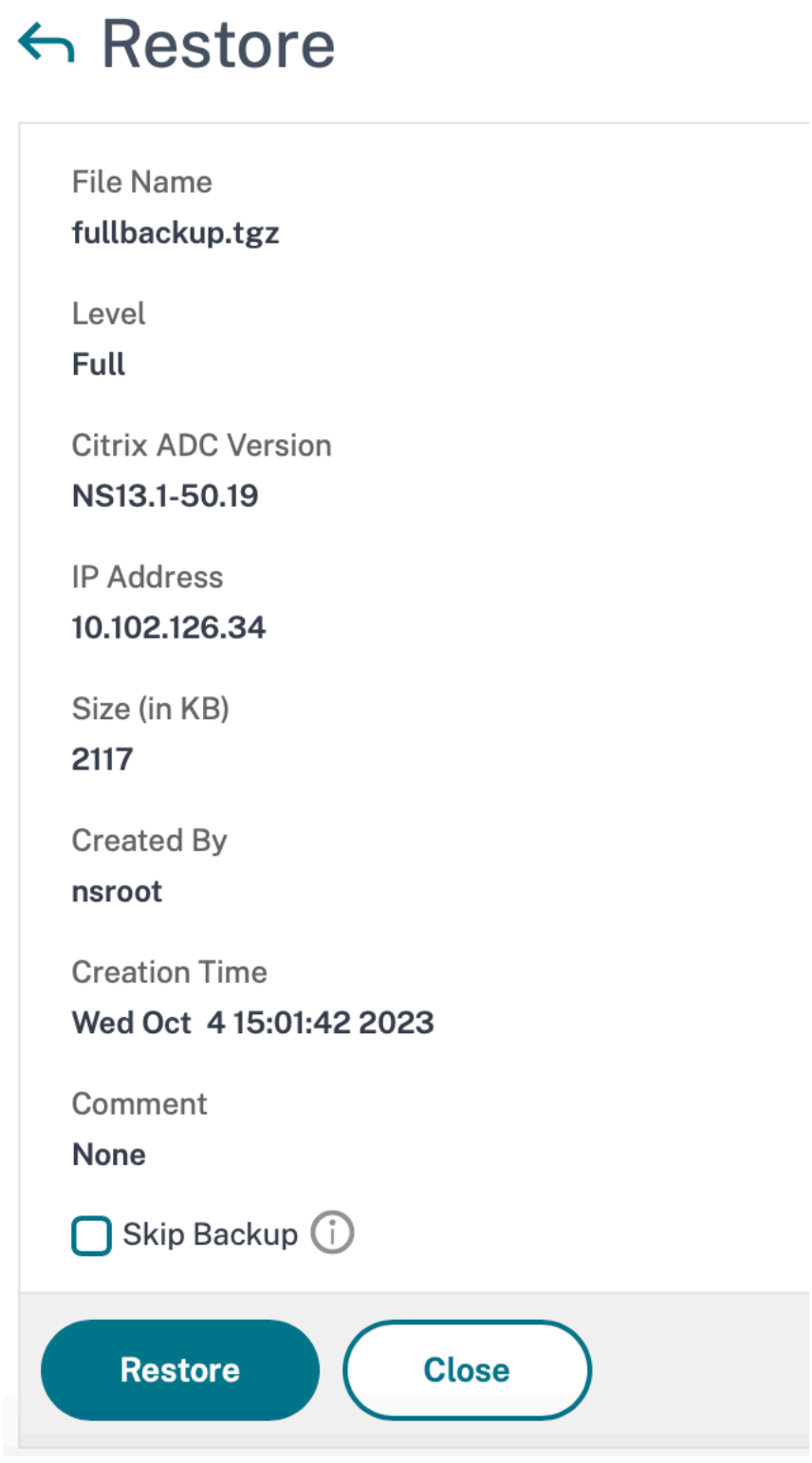


d) Sélectionnez le fichier.

e) **Dans le menu déroulant Sélectionner une action**, sélectionnez **Restaurer**.



f) Sur la page **Restaurer**, vérifiez les détails du fichier, puis cliquez sur **Restaurer**.



g) Après la restauration, redémarrez l'instance EC2.

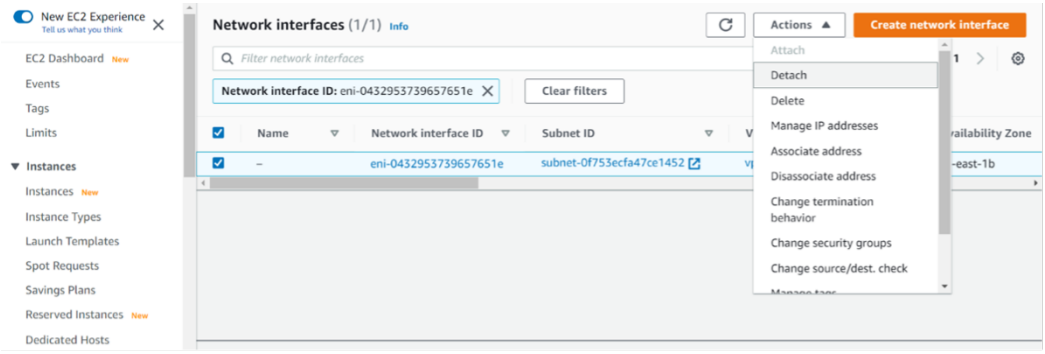
4. Déplacez toutes les interfaces (à l'exception de l'interface de gestion à laquelle l'adresse NSIP

est liée) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une interface réseau d'une instance EC2 à une autre, procédez comme suit :

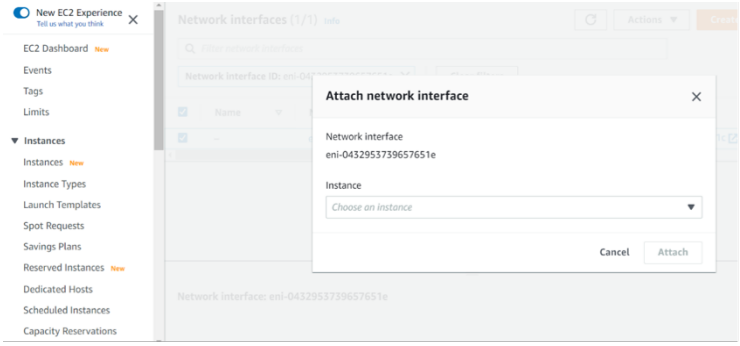
a) Dans le **portail AWS**, arrêtez les anciennes et nouvelles instances EC2.

b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau attachée à l'ancienne instance EC2.

c) Détachez l'instance EC2 en cliquant sur **Actions > Détacher**.



d) Connectez l'interface réseau à la nouvelle instance EC2 en cliquant sur **Actions > Attacher**. Entrez le nom de l'instance EC2 auquel l'interface réseau doit être connectée.



e) Faites les **étapes 1** à **4** pour toutes les autres interfaces connectées. Assurez-vous de suivre la séquence et de conserver l'ordre de l'interface. C'est-à-dire, détachez d'abord l'interface 2 et attachez-la, puis détachez l'interface 3 et attachez-la, etc.

5. Vous ne pouvez pas détacher l'interface de gestion d'une ancienne instance EC2. Déplacez donc toutes les adresses IP secondaires (le cas échéant) de l'interface de gestion (interface réseau principale) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une adresse IP d'une interface à une autre, procédez comme suit :

a) Dans le **portail AWS**, assurez-vous que les anciennes et nouvelles instances EC2 sont à l'état **Stop** .

b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau de gestion attachée à l'ancienne instance EC2.

c) Cliquez sur **Actions > Gérer l'adresse IP**et notez toutes les adresses IP secondaires attribuées (le cas échéant).

d) Accédez à l'interface réseau de gestion ou à l'interface principale de la nouvelle instance EC2.

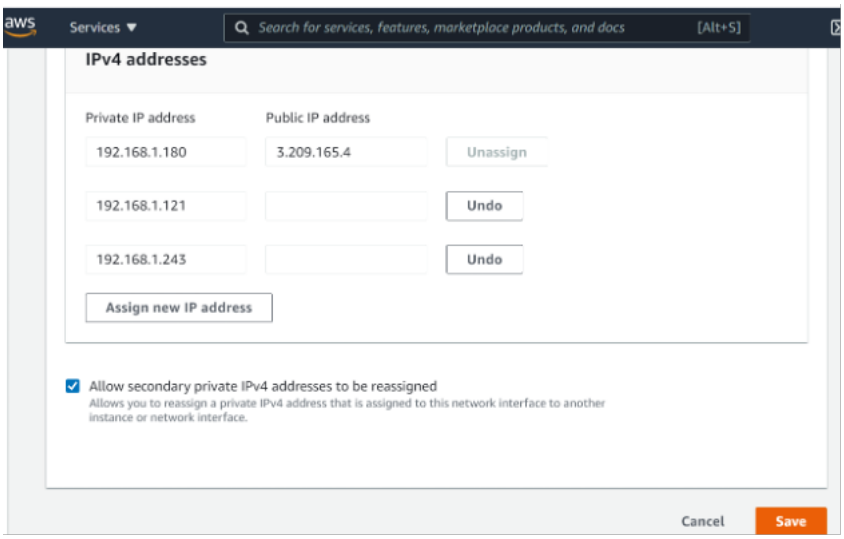
e) Cliquez sur **Actions > Gérer les adresses IP**.

f) Sous **Adresses IPv4**, cliquez sur **Attribuer une nouvelle adresse IP**.

g) Saisissez les adresses IP indiquées à l'**étape 3**.

h) Activez la case à cocher **Autoriser la réaffectation des adresses IP privées secondaires** .

i) Cliquez sur **Enregistrer**.



6. Démarrez la nouvelle instance EC2 et vérifiez la configuration. Une fois que toute la configuration est déplacée, vous pouvez supprimer ou conserver l'ancienne instance EC2 selon vos besoins.
7. Si une adresse EIP est attachée à l'adresse NSIP de l'ancienne instance EC2, déplacez l'adresse NSIP de l'ancienne instance vers la nouvelle adresse NSIP de l'instance.
8. Si vous souhaitez revenir à l'ancienne instance, suivez les mêmes étapes de la manière opposée entre l'ancienne et la nouvelle instance.
9. Une fois que vous passez d'une instance d'abonnement à une instance BYOL, une licence est requise. Pour installer une licence, procédez comme suit :
   - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
   - Télécharger la licence sur l'instance.

> **Remarque :**
>
> Lorsque vous déplacez une instance BYOL vers une instance d'abonnement (instance de marché payante), vous n'avez pas besoin d'installer la licence. Le jeu de fonctionnalités et les performances corrects sont automatiquement activés.

Limitations

L'interface de gestion ne peut pas être déplacée vers la nouvelle instance EC2. Citrix vous recommande donc de configurer manuellement l'interface de gestion. Pour plus d'informations, reportez-vous à l'**étape 5** de la procédure précédente. Une nouvelle instance EC2 est créée avec le réplica exact de l'ancienne instance EC2, mais seule l'adresse NSIP possède une nouvelle adresse IP.

Serveurs d'équilibrage de charge dans différentes zones de disponibilité

October 17, 2024

Une instance VPX peut être utilisée pour équilibrer la charge des serveurs s'exécutant dans la même zone de disponibilité, ou dans :

- Une zone de disponibilité différente (AZ) dans le même VPC AWS
- Une autre région AWS
- AWS EC2 dans un VPC

Pour permettre à une instance VPX d'équilibrer la charge des serveurs exécutés en dehors du VPC AWS que le L'instance VPX est activée, configurez l'instance pour utiliser les EIP pour acheminer le trafic via la passerelle Internet, comme suit :

1. Configurez un SNIP sur l'instance NetScaler VPX à l'aide de la CLI NetScaler ou de l'interface graphique.
2. Activez l'acheminement du trafic hors de l'AZ en créant un sous-réseau public pour le trafic côté serveur.
3. Ajoutez une route de Gateway Internet à la table de routage, à l'aide de la console AWS GUI.
4. Associez la table de routage que vous avez mise à jour au sous-réseau côté serveur.
5. Associez un EIP à l'adresse IP privée côté serveur mappée à une adresse SNIP NetScaler.

Comment fonctionne la haute disponibilité sur AWS

October 17, 2024

Vous pouvez configurer deux instances NetScaler VPX sur AWS sous la forme d'une paire active-passive à haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Haute disponibilité dans la même zone
- Haute disponibilité dans différentes zones

> **Remarque :**
>
> Pour que la haute disponibilité fonctionne, assurez-vous que les deux instances NetScaler VPX sont associées à des rôles IAM et que l'adresse IP Elastic (EIP) est attribuée au NSIP. Vous n'avez pas besoin d'attribuer un EIP au NSIP si le NSIP peut accéder à Internet via l'instance NAT.

Haute disponibilité dans les mêmes zones

Dans un déploiement haute disponibilité dans les mêmes zones, les deux instances VPX doivent avoir des configurations réseau similaires.

Suivez ces deux règles :

Règle 1. Règle 1 Toute carte réseau d'une instance VPX doit se trouver dans le même sous-réseau que la carte réseau correspondante de l'autre VPX. Les deux instances doivent avoir :

- Interface de gestion sur le même sous-réseau (appelé sous-réseau de gestion)
- Interface client sur le même sous-réseau (appelé sous-réseau client)
- Interface serveur sur le même sous-réseau (appelé sous-réseau du serveur)

Article 2. La séquence de carte réseau de gestion, de carte réseau client et de carte réseau serveur sur les deux instances doit être la même. Par exemple, le scénario suivant n'est pas pris en charge.

Instance VPX 1

NIC 0 : gestion Carte réseau 1 : client NIC 2 : Serveur

Instance VPX 2

NIC 0 : gestion

NIC 1 : serveur

Carte réseau 2 : client

Dans ce scénario, la carte réseau 1 de l'instance 1 est dans le sous-réseau client tandis que la carte réseau 1 de l'instance 2 est dans le sous-réseau du serveur. Pour que HA fonctionne, la carte réseau 1 des deux instances doit être soit dans le sous-réseau client, soit dans le sous-réseau du serveur.

À partir de 13.0 41.xx, la haute disponibilité peut être obtenue en migrant des adresses IP privées secondaires attachées aux cartes réseau (cartes réseau client et côté serveur) du nœud HA principal vers le nœud HA secondaire après le basculement. Dans ce déploiement :

- Les deux instances VPX ont le même nombre de cartes réseau et de mappage de sous-réseau selon l'énumération de carte réseau.
- Chaque carte réseau VPX possède une adresse IP privée supplémentaire, à l'exception de la première carte réseau, qui correspond à l'adresse IP de gestion. L'adresse IP privée supplémentaire apparaît comme l'adresse IP privée principale dans la console Web AWS. Dans notre document, nous appelons cette adresse IP supplémentaire l'adresse IP fictive).
- Les adresses IP fictives ne doivent pas être configurées sur l'instance NetScaler en tant que VIP et SNIP.
- D'autres adresses IP privées secondaires doivent être créées, selon les besoins, et configurées en tant que VIP et SNIP.
- Lors du basculement, le nouveau nœud principal recherche les SNIP et les VIP configurés et les déplace des cartes réseau attachées à la précédente principale vers les cartes réseau correspondantes sur la nouvelle interface principale.
- Les instances NetScaler nécessitent des autorisations IAM pour que HA fonctionne. Ajoutez les privilèges IAM suivants à la stratégie IAM ajoutée à chaque instance.

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeNetworkInterfaces"` `"ec2:AssignPrivateIpAddresses"`

> **Remarque :**
>
> `unassignPrivateIpAddress` n'est pas requis.

Cette méthode est plus rapide que l'ancienne méthode. Dans l'ancienne méthode, HA dépend de la migration des interfaces réseau élastiques AWS du nœud principal vers le nœud secondaire.

Pour une méthode héritée, les stratégies suivantes sont requises :

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeAddresses"` `"ec2:AssociateAddress"` `"ec2:DisassociateAddress"`

Pour plus d'informations, consultez Déployer une paire haute disponibilité sur AWS.

Haute disponibilité dans différentes zones

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, sous la forme d'une paire active-passive à haute disponibilité en mode Independent Network Configuration (INC). Lors du basculement, l'EIP (Elastic IP) du VIP de l'instance principale migre vers le secondaire, qui prend le relais en tant que nouveau principal. Dans le processus de basculement, l'API AWS :

- Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
- Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. L'un qui est directement connecté au serveur virtuel et l'autre qui est connecté via l'ensemble d'adresses IP.
- Réassocie l'adresse IP publique (EIP) à l'adresse IP privée appartenant au nouveau VIP principal.

Pour les HA dans différentes zones, les stratégies suivantes sont requises :

`"iam:GetRole" "ec2:DescribeInstances" "ec2:DescribeAddresses" "ec2:AssociateAddress" "ec2:DisassociateAddress"`

Pour plus d'informations, consultez Haute disponibilité dans les zones de disponibilité AWS.

Avant de commencer votre déploiement

Avant de commencer un déploiement HA sur AWS, lisez le document suivant :

- Conditions préalables
- Limitations et directives d'utilisation
- Déployer une instance NetScaler VPX sur AWS
- Haute disponibilité

Dépannage

Pour résoudre toute défaillance lors d'un basculement en mode HA d'une instance NetScaler VPX sur le cloud AWS, consultez le `cloud-ha-daemon.log` fichier stocké à cet emplacement.

Déployer une paire HA VPX dans la même zone de disponibilité AWS

October 17, 2024

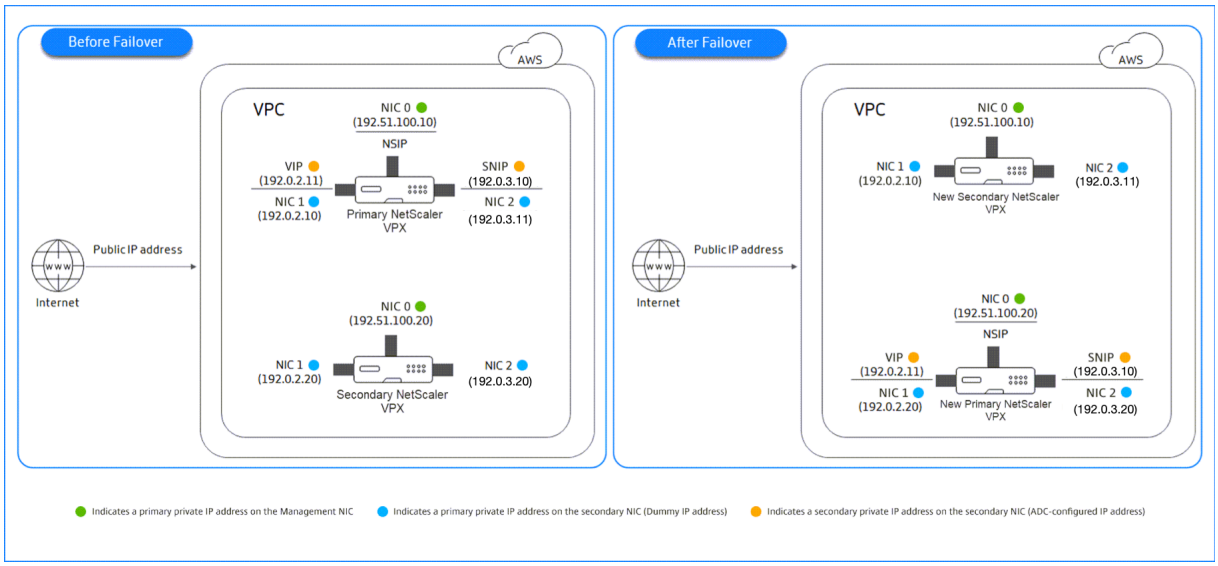
> **Remarque :**
>
> À partir de la version 13.1 build 27.x de NetScaler, la paire VPX HA située dans la même zone de disponibilité AWS prend en charge les adresses IPv6.

Vous pouvez configurer deux instances NetScaler VPX sur AWS en tant que paire HA, dans la même zone AWS où les deux instances VPX se trouvent sur le même sous-réseau. La haute disponibilité est obtenue en migrant les adresses IP privées secondaires attachées aux cartes réseau (cartes réseau côté client et côté serveur) du nœud HA principal vers le nœud HA secondaire après basculement. Toutes les adresses IP Elastic associées aux adresses IP privées secondaires sont également migrées.

La paire NetScaler VPX HA prend en charge les adresses IPv4 et IPv6 dans la même zone de disponibilité AWS.

L'illustration suivante illustre un scénario de basculement HA par migration d'adresses IP privées secondaires.

Figure 1. Une paire NetScaler VPX HA sur AWS, à l'aide d'une migration IP privée



Avant de commencer votre document, lisez les documents suivants :

- Conditions préalables
- Limitations et directives d'utilisation
- Déployer une instance NetScaler VPX sur AWS
- Haute disponibilité

Comment déployer une paire VPX HA dans la même zone

Voici le résumé des étapes pour déployer une paire VPX HA dans la même zone :

1. Créez deux instances VPX sur AWS, chacune dotée de trois cartes réseau.
2. Attribuez une adresse IP privée secondaire AWS au VIP et au SNIP du nœud principal.
3. Configurez VIP et SNIP sur le nœud principal à l'aide des adresses IP privées secondaires AWS.
4. Configurez HA sur les deux nœuds.

Étape 1. Créez deux instances VPX (nœuds primaires et secondaires) à l'aide du même VPC, chacune avec trois cartes réseau (Ethernet 0, Ethernet 1, Ethernet 2)

Suivez les étapes décrites dans Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS.

Étape 2. Sur le nœud principal, attribuez des adresses IP privées pour Ethernet 1 (IP client ou VIP) et Ethernet 2 (IP du serveur principal ou SNIP)

La console AWS attribue automatiquement des adresses IP privées principales aux cartes réseau configurées. Affectez davantage d'adresses IP privées à VIP et SNIP, appelées adresses IP privées secondaires.

Pour attribuer une adresse IP privée à une interface réseau, procédez comme suit :

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez **Network Interfaces**, puis sélectionnez l'interface réseau connectée à l'instance.
3. Choisissez **Actions > Gérer les adresses IP**.
4. Sélectionnez Adresses **IPv4 ou AdressesIPv6 en** fonction de vos besoins.
5. Pour les adresses IPv4 :
    a) Choisissez **Assign new IP**.
    b) Entrez une adresse IPv4 spécifique comprise dans la plage de sous-réseau de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une adresse IP pour vous.
    c) (Facultatif) Choisissez **Autoriser la réaffectation** pour autoriser la réaffectation de l'adresse IP privée secondaire si elle est déjà attribuée à une autre interface réseau.
6. Pour les adresses IPv6 :
    a) Choisissez **Assign new IP**.
    b) Entrez une adresse IPv6 spécifique comprise dans la plage de sous-réseaux de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une adresse IP pour vous.

c) (Facultatif) Choisissez **Autoriser la réaffectation** pour autoriser la réaffectation de l'adresse IP privée principale ou secondaire si elle est déjà attribuée à une autre interface réseau.

7. Choisissez **Oui > Mettre à jour**.

Sous la **description de l'instance**, les adresses IP privées attribuées apparaissent.

> **Remarque :**
>
> Dans un déploiement de paires HA IPv4, vous pouvez attribuer uniquement les adresses IPv4 secondaires sur l'interface et les utiliser comme adresses VIP et SNIP. Mais dans un déploiement de paires HA IPv6, vous pouvez attribuer les adresses IPv6 principales ou IPv6 secondaires sur l'interface et les utiliser comme adresses VIP et SNIP.

Étape 3. Configurez VIP et SNIP sur le nœud principal, à l'aide d'adresses IP privées secondaires

Accédez au nœud principal via SSH. Ouvrez un client SSH et tapez :

```
ssh -i <location of your private key> nsroot@<public DNS of the instance>
```

Ensuite, configurez VIP et SNIP.

Pour les VIP, tapez :

```
add ns ip <IPAddress> <netmask> -type <type>
```

Pour SNIP, tapez :

```
add ns ip <IPAddress> <netmask> -type SNIP
```

Tapez `save config` pour enregistrer.

Pour voir les adresses IP configurées, tapez la commande suivante :

```
show ns ip
```

Pour plus d'informations, consultez les rubriques suivantes :

- Configuration et gestion des adresses IP virtuelles (VIP)
- Configuration de l'adresse NSIP

Étape 4 : Configurer la haute disponibilité sur les deux instances

Sur le nœud principal, ouvrez un client Shell et tapez la commande suivante :


```
add ha node <id> <private IP address of the management NIC of the
   secondary node>
```

Sur le nœud secondaire, tapez la commande suivante :

```
add ha node <id> <private IP address of the management NIC of the
   primary node>
```

Tapez `save config` pour enregistrer la configuration.

Pour voir les nœuds HA configurés, tapez `show ha node`.

Lors du basculement, les adresses IP privées secondaires configurées en tant que VIP et SNIP sur le nœud principal précédent sont migrées vers le nouveau nœud principal.

Pour forcer un basculement sur incident sur un nœud, tapez `force HA`Basculement.

Migrer une ancienne paire HA vers une nouvelle paire HA sur la base d'une migration IP privée secondaire

> **Remarque :**
>
> L'ancienne méthode de déploiement de la paire VPX HA qui fonctionne sur la base de la migration ENI est obsolète. Par conséquent, nous vous recommandons d'utiliser le déploiement de paires HA en fonction de la migration d'une adresse IP privée secondaire.

Pour permettre une migration fluide de l'ancienne paire HA vers une nouvelle paire HA sur la base d'une migration IP privée secondaire, assurez-vous de ce qui suit :

1. Les nœuds principal et secondaire doivent avoir le même nombre d'interfaces, et ces interfaces doivent se trouver dans les mêmes sous-réseaux.
2. Le VIP et le SNIP configurés comme adresse IP privée principale dans l'ancienne méthode doivent être migrés vers une adresse IP privée secondaire dans la nouvelle méthode.
3. Les autorisations IAM requises pour le nouveau déploiement HA doivent être ajoutées aux instances NetScaler principale et secondaire.
4. Redémarrez les instances NetScaler principale et secondaire.

Pour plus d'informations, consultez la section Haute disponibilité dans les mêmes zones.

Déployer une paire haute disponibilité à l'aide du modèle Citrix CloudFormation

Avant de démarrer le modèle CloudFormation, assurez-vous de répondre aux exigences suivantes :

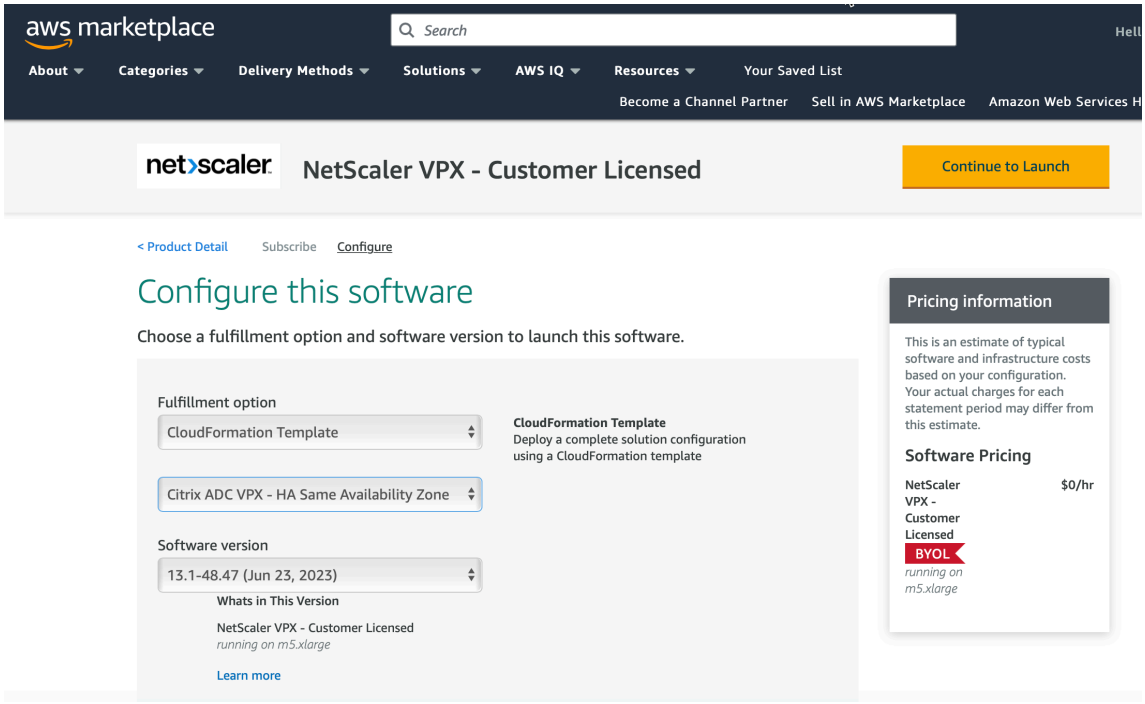
- Un VPC
- Trois sous-réseaux au sein du VPC

- Un groupe de sécurité avec des ports UDP 3003, TCP 3009—3010, HTTP et SSH ouverts
- Une paire de clés
- Créer une passerelle Internet
- Modifier les tables de routage pour les réseaux de clients et de gestion afin qu'ils pointent vers la passerelle Internet

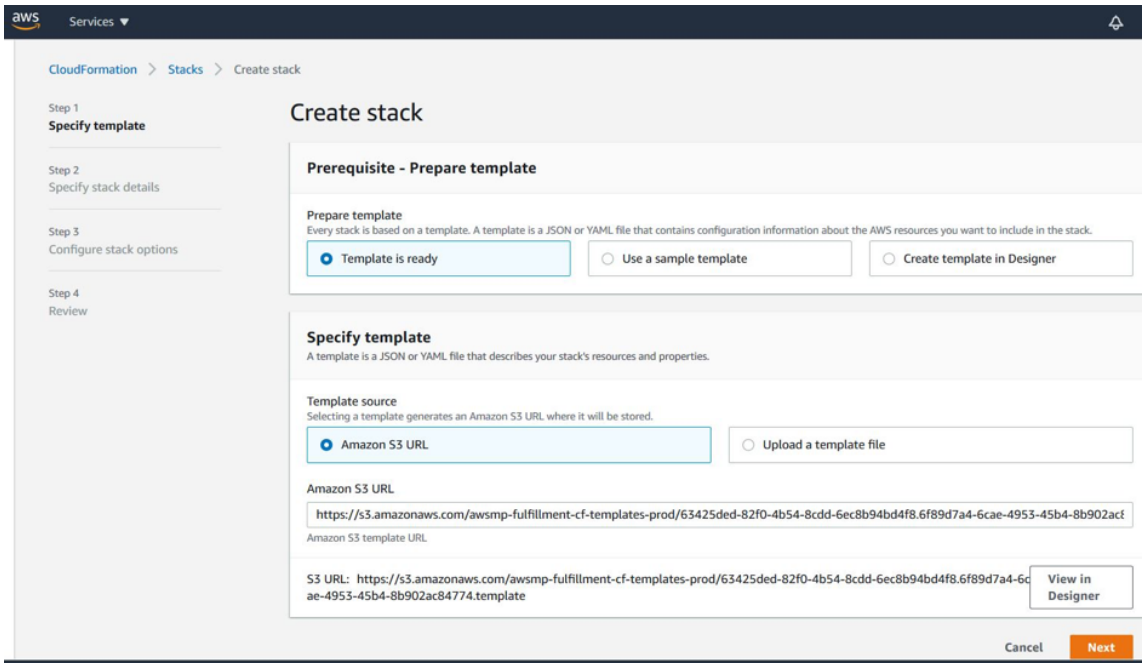
> **Remarque :**
>
> Le modèle Citrix CloudFormation crée automatiquement un rôle IAM. Les rôles IAM existants n' apparaissent pas dans le modèle.

Pour lancer le modèle Citrix CloudFormation :

1. Connectez-vous à AWS Marketplace en utilisant vos informations d'identification AWS.
2. Dans le champ de recherche, tapez **NetScaler VPX** pour rechercher l'AMI NetScaler, puis cliquez sur **OK**.
3. Sur la page des résultats de recherche, cliquez sur l'offre NetScaler VPX souhaitée.
4. Cliquez sur l'onglet **Tarification**, pour accéder à **Informations sur la tarification**.
5. Sélectionnez la région et l'**option d'expédition** comme **NetScaler VPX** —**Customer Licensed**.
6. Cliquez sur **Continuer pour vous abonner**.
7. Consultez les détails sur la page **S'abonner** et cliquez sur **Continuer vers la configuration**.
8. Sélectionnez **Méthode de livraison** comme **modèle CloudFormation**.
9. Sélectionnez le modèle CloudFormation requis.
10. Sélectionnez **Version et**région**du logiciel**, puis cliquez sur **Continuer vers le lancement**.



11. Sous **Choisir une action**, sélectionnez **Lancer CloudFormation**, puis cliquez sur **Lancer**. La page **Créer une pile** s'affiche.
12. Cliquez sur **Suivant**.

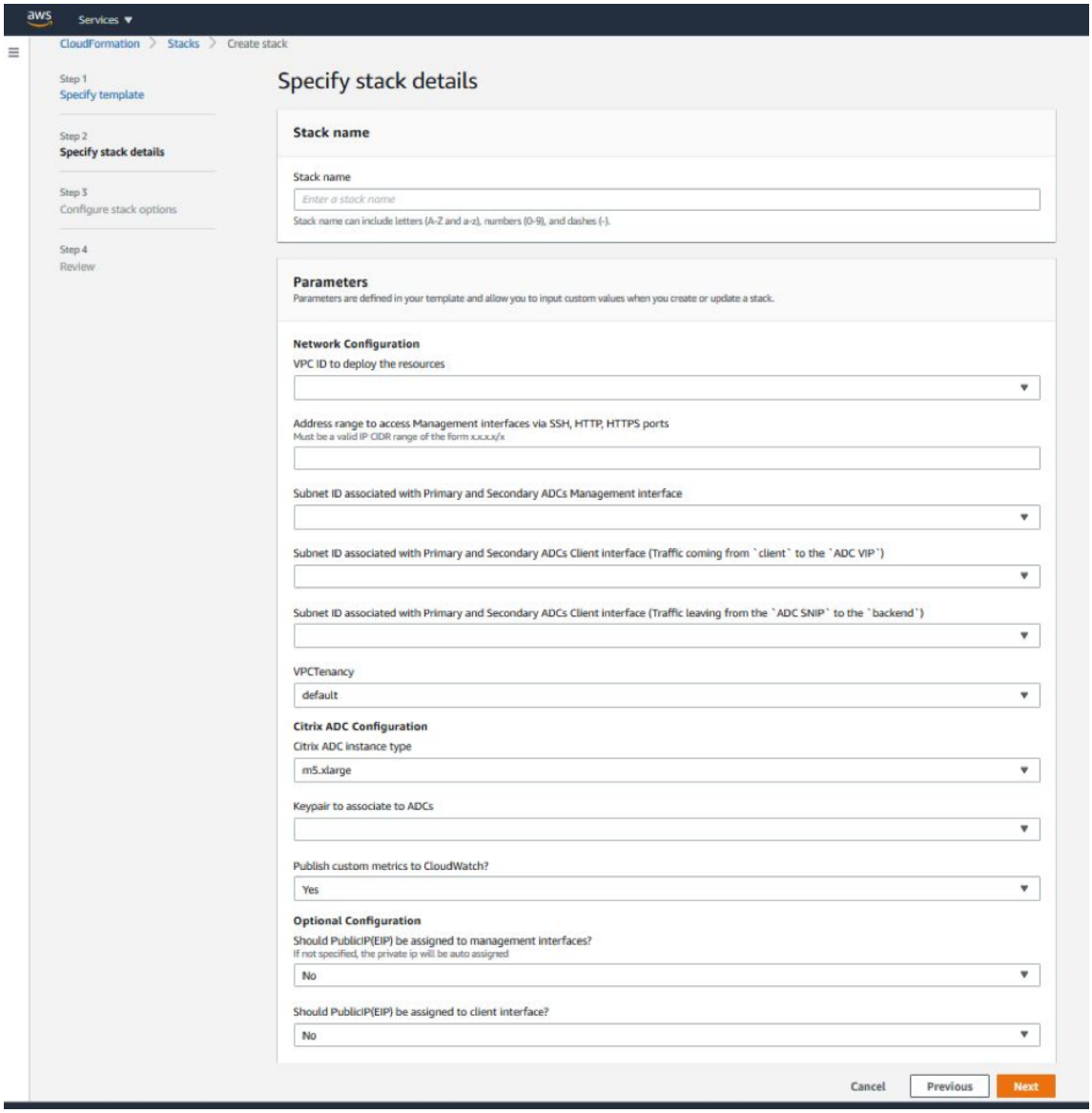


13. La page **Spécifier les détails de la pile** apparaît. Entrez les détails suivants.

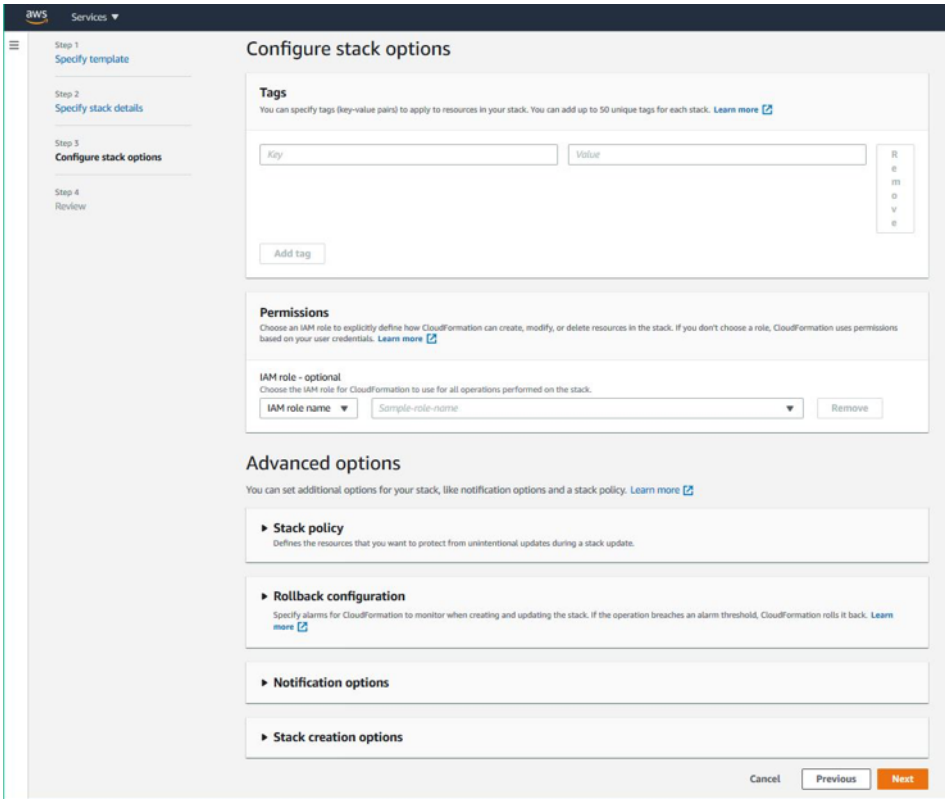
    - Saisissez un **nom de pile**. Le nom doit contenir 25 caractères.
    - Sous **Configuration réseau**, effectuez les opérations suivantes :

- Sélectionnez **Sous-réseau de gestion**, **Sous-réseau client**et **Sous-réseau de serveur**. Assurez-vous de sélectionner les sous-réseaux appropriés que vous avez créés dans le VPC que vous avez sélectionné sous ID du VPC.
- Ajoutez l'**adresse IP de gestion principale**, l'**adresse IP de gestion secondaire**, l'**adresse IP client**et l'**adresse IP du serveur** Les adresses IP doivent appartenir aux mêmes sous-réseaux des sous-réseaux respectifs. Les adresses IP doivent appartenir aux mêmes sous-réseaux des sous-réseaux respectifs. Vous pouvez également laisser le modèle attribuer automatiquement les adresses IP.
- Sélectionnez **par défaut** pour **VPCTenancy**.

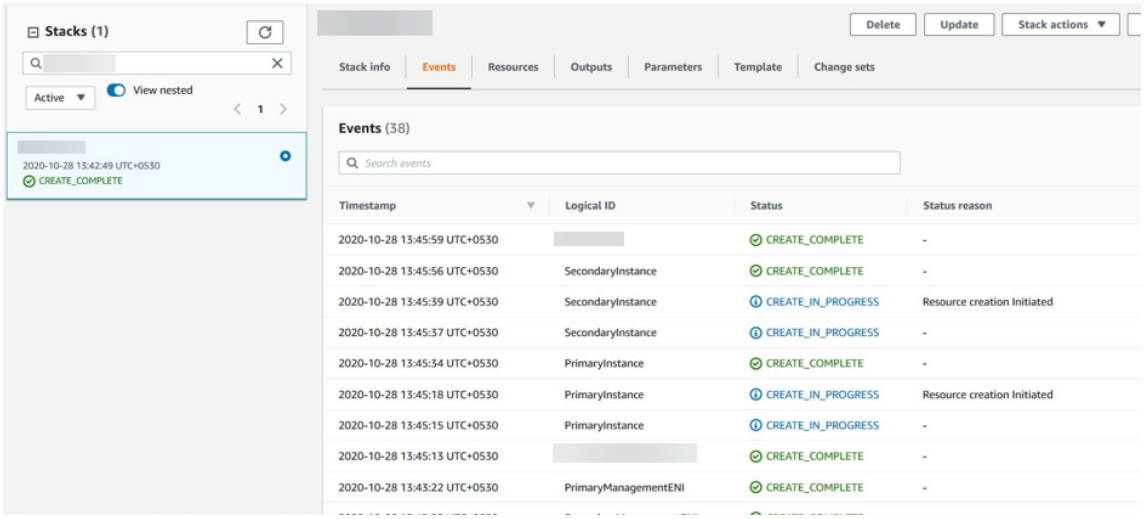
- Sous **Configuration de NetScaler**, effectuez les opérations suivantes :
  - Sélectionnez **m5.xlarge** pour le **type d'instance**.
  - Sélectionnez la paire de clés que vous avez déjà créée dans le menu de **Paire de clés**.
  - Par défaut, **Publier des métriques personnalisées sur CloudWatch ?** l'option est définie sur **Oui**. Si vous souhaitez désactiver cette option, sélectionnez **Non**.
    Pour plus d'informations sur les métriques CloudWatch, consultez [Surveillez vos instances à l'aide d'Amazon CloudWatch] (#monitor-your-instances-using-amazon-cloudWatch).
- Sous **Configuration facultative**, procédez comme suit :
  - Par défaut, **L'adresse IP publique (EIP) doit-elle être attribuée aux interfaces de gestion ?** l'option est définie sur **Non**.
  - Par défaut, **L'adresse IP publique (EIP) doit-elle être attribuée à l'interface client ?** l'option est définie sur **Non**.



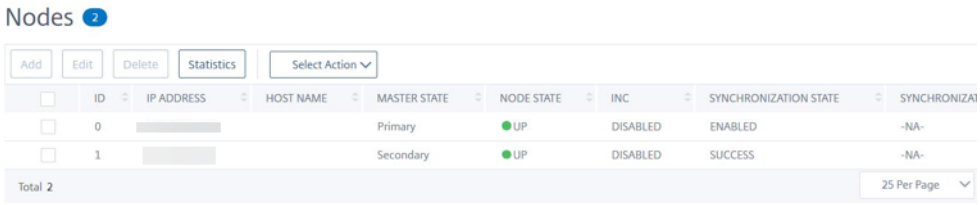
14. Cliquez sur **Suivant**.
15. La page **Configurer les options de la pile** apparaît. Il s'agit d'une page facultative.



16. Cliquez sur **Suivant**.
17. La page **Options** s'affiche. (Cette page est facultative.). Cliquez sur **Suivant**.
18. La page **Révision** s'affiche. Prenez quelques instants pour revoir les paramètres et apporter des modifications éventuelles, si nécessaire.
19. Sélectionnez **Je reconnais qu'AWS CloudFormation peut créer des ressources IAM.** case à cocher, puis cliquez sur **Créer une pile**.
20. Le statut **CREATE-IN-PROGRESS** apparaît. Attendez que le statut soit **CREATE-COMPLETE**. Si le statut ne passe pas à **COMPLETE**, vérifiez la raison de l'échec dans l'onglet **Événements** et recréez l'instance avec les configurations appropriées.



21. Une fois qu'une ressource IAM est créée, accédez à **EC2 Management Console > Instances**. Vous trouvez deux instances VPX créées avec le rôle IAM. Les nœuds principaux et secondaires sont créés chacun avec trois adresses IP privées et trois interfaces réseau.
22. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe. Depuis l'interface graphique, accédez à **Système > Haute disponibilité > Nœuds**. Le NetScaler VPX est déjà configuré en paire HA par le modèle CloudFormation.
23. La paire NetScaler VPX HA s'affiche.



Surveillez vos instances à l'aide d'Amazon CloudWatch

Vous pouvez utiliser le service Amazon CloudWatch pour surveiller un ensemble de mesures NetScaler VPX, telles que l'utilisation du processeur et de la mémoire, ainsi que le débit. CloudWatch surveille les ressources et les applications qui s'exécutent sur AWS, en temps réel. Vous pouvez accéder au tableau de bord Amazon CloudWatch à l'aide de la console AWS Management. Pour plus d'informations, consultez Amazon CloudWatch.

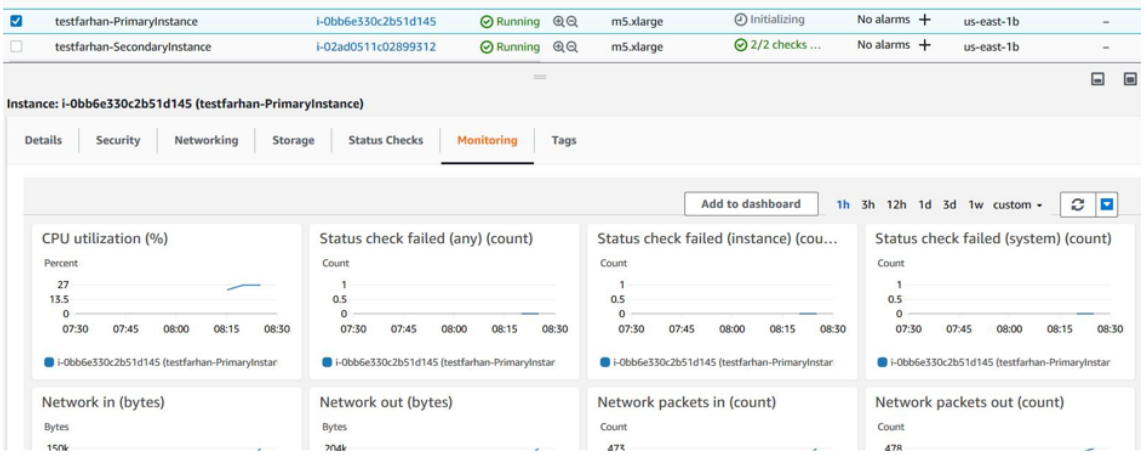
Points à noter

- Si vous déployez une instance NetScaler VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut.
- Si vous déployez une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est « Oui ». Si vous souhaitez désactiver le service CloudWatch, sélectionnez « Non ».
- Les métriques sont disponibles pour le processeur (gestion et utilisation du processeur par paquets), la mémoire et le débit (entrant et sortant).

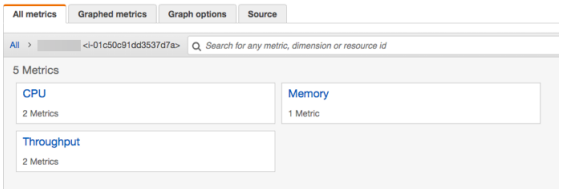
Comment afficher les métriques CloudWatch

Pour afficher les métriques CloudWatch pour votre instance, procédez comme suit :

1. Ouvrez une session sur **AWS Management Console > EC2 > Instances**.
2. Sélectionnez l'instance.
3. Cliquez sur **Surveillance**.
4. Cliquez sur **Afficher toutes les métriques CloudWatch**.

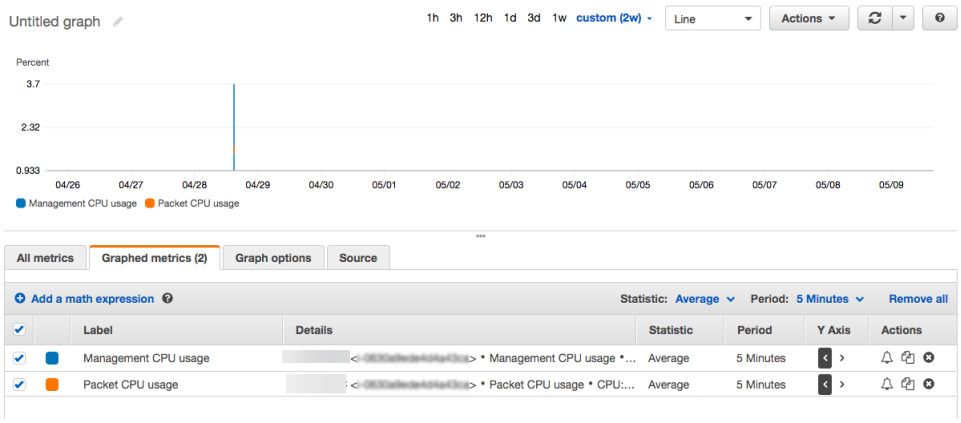


5. Sous Toutes les mesures, cliquez sur votre ID d'instance.



6. Cliquez sur les mesures que vous souhaitez afficher, définissez la durée (en minutes, heures, jours, semaines, mois).
7. Cliquez sur **Mesures graphiques** pour afficher les statistiques d'utilisation. Utilisez les **options de graphique** pour personnaliser votre graphique.

Figure. Mesures graphiques pour l'utilisation du processeur



Configuration de SR-IOV sur une configuration haute disponibilité

La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de NetScaler version 12.0 57.19. Pour plus d'informations sur la configuration de SR-IOV, consultez Configuration des instances NetScaler VPX pour utiliser l'interface réseau SR-IOV.

Ressources connexes

Comment fonctionne la haute disponibilité sur AWS

Haute disponibilité dans différentes zones de disponibilité AWS

October 17, 2024

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, sous la forme d'une paire active-passive à haute disponibilité en mode Independent Network Configuration (INC). Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Points à noter

- Lisez les documents suivants avant de commencer votre déploiement :
  - Terminologie AWS

  - Conditions préalables
  - Limitations et directives d'utilisation

- La paire haute disponibilité VPX peut résider dans la même zone de disponibilité dans un sous-réseau différent ou dans deux zones de disponibilité AWS différentes.
- Citrix vous recommande d'utiliser différents sous-réseaux pour la gestion (NSIP), le trafic client (VIP) et le serveur principal (SNIP).
- La haute disponibilité doit être définie en mode de configuration réseau indépendante (INC) pour qu'un basculement fonctionne.
- Le port 3003 des deux instances doit être ouvert pour le trafic UDP, car il est utilisé pour les pulsations cardiaques.
- Les sous-réseaux de gestion des deux nœuds doivent avoir accès à Internet ou au serveur API AWS via NAT interne afin que les autres API soient fonctionnelles.
- Le rôle IAM doit posséder l'autorisation E2 pour la migration IP publique ou Elastic IP (EIP) et les autorisations de table de routage EC2 pour la migration IP privée.

Vous pouvez déployer la haute disponibilité dans les zones de disponibilité AWS de la manière suivante :

- Utilisation d'adresses IP Elastic
- Utilisation d'adresses IP privées

Références supplémentaires

Pour plus d'informations sur NetScaler Application Delivery Management (ADM) pour AWS, consultez Installer l'agent NetScaler ADM sur AWS.

Déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

October 17, 2024

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP élastiques (EIP) en mode INC.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Comment fonctionne la haute disponibilité avec des adresses EIP dans différentes zones AWS

Lors du basculement, l'EIP du VIP de l'instance principale migre vers l'instance secondaire, qui prend le relais en tant que nouveau serveur principal. Dans le processus de basculement, l'API AWS :

1. Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
2. Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. L'un qui est directement connecté au serveur virtuel et celui qui est connecté via l'ensemble d'adresses IP.
3. Réassocie l'adresse IP publique (EIP) à l'adresse IP privée appartenant au nouveau VIP principal.

> **Remarque :**
>
> Pour protéger votre réseau contre les attaques telles que le déni de service (DoS), lorsque vous utilisez un EIP, vous pouvez créer des groupes de sécurité dans AWS pour restreindre l'accès IP. Pour une haute disponibilité, vous pouvez passer d'EIP à une solution de déplacement IP privée selon vos déploiements.

Comment déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

Voici le résumé des étapes à suivre pour déployer une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents.
3. Configurer la haute disponibilité
    a) Configurez la haute disponibilité en mode INC dans les deux instances.
    b) Ajoutez un ensemble d'adresses IP dans les deux instances.
    c) Liez l'ensemble d'adresses IP dans les deux instances au VIP.
    d) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1 et 2, utilisez la console AWS. Pour les étapes 3, utilisez l'interface graphique NetScaler VPX ou la CLI.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents. Attachez un EIP au VIP du VPX principal.

Pour plus d'informations sur la création d'un VPC et le déploiement d'une instance VPX sur AWS, consultez Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome

Étape 3. Configurer la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande NetScaler VPX ou l'interface graphique pour configurer la haute disponibilité.

Configuration de la haute disponibilité à l'aide de la CLI

1. Configurez la haute disponibilité en mode INC dans les deux instances.

   Sur le nœud principal :

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   Sur le nœud secondaire :

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire

   <prim_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal

2. Ajoutez le jeu d'adresses IP dans les deux instances.

   Tapez la commande suivante sur les deux instances.

   ```
   add ipset <ipsetname>
   ```

3. Liez l'ensemble d'adresses IP à l'ensemble d'adresses IP virtuelles sur les deux instances.

   Tapez la commande suivante sur les deux instances :

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Remarque :**
   >
   > Vous pouvez lier l'ensemble d'adresses IP au VIP principal ou au VIP secondaire. Toutefois, si vous liez l'IP définie au VIP principal, utilisez le VIP secondaire pour ajouter au serveur virtuel, et inversement.

4. Ajoutez un serveur virtuel sur l'instance principale.

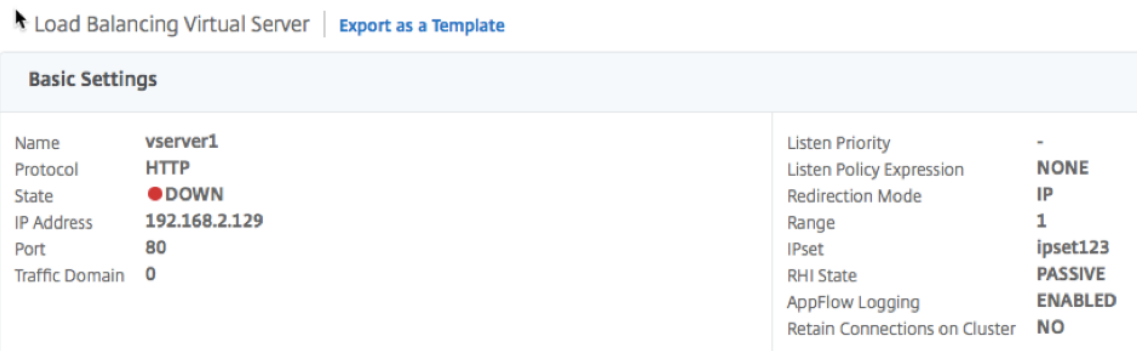
   Entrez la commande suivante :

   ```
   add &#060;server_type&#062; vserver &#060;vserver_name&#062;
   &#060;protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -
   ipset \\&#060;ipset_name&#062;
   ```


Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configuration de la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe.
3. Dans l'interface graphique, accédez à **Configuration** > **Système** > **Haute disponibilité**. Cliquez sur **Ajouter**.
4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur le nœud automatique.
6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire et cliquez sur **Créer**.
7. Répétez les étapes du nœud secondaire.
8. Liez l'IP définie à l'ensemble VIP sur les deux instances.
9. À partir de l'interface graphique, accédez à **Système** > **Réseau** > **IP** > **Ajouter**.
10. Ajoutez les valeurs requises pour l'adresse IP, le masque de réseau, le type d'IP (adresse IP virtuelle) et cliquez sur **Créer**.
11. Accédez à **Système** > **Réseau** > **Ensembles d'adresses IP** > **Ajouter**. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
12. Sur la page IPv4, sélectionnez l'adresse IP virtuelle et cliquez sur **Insérer**. Cliquez sur **Créer** pour créer le jeu d'adresses IP.
13. Ajouter un serveur virtuel dans l'instance principale

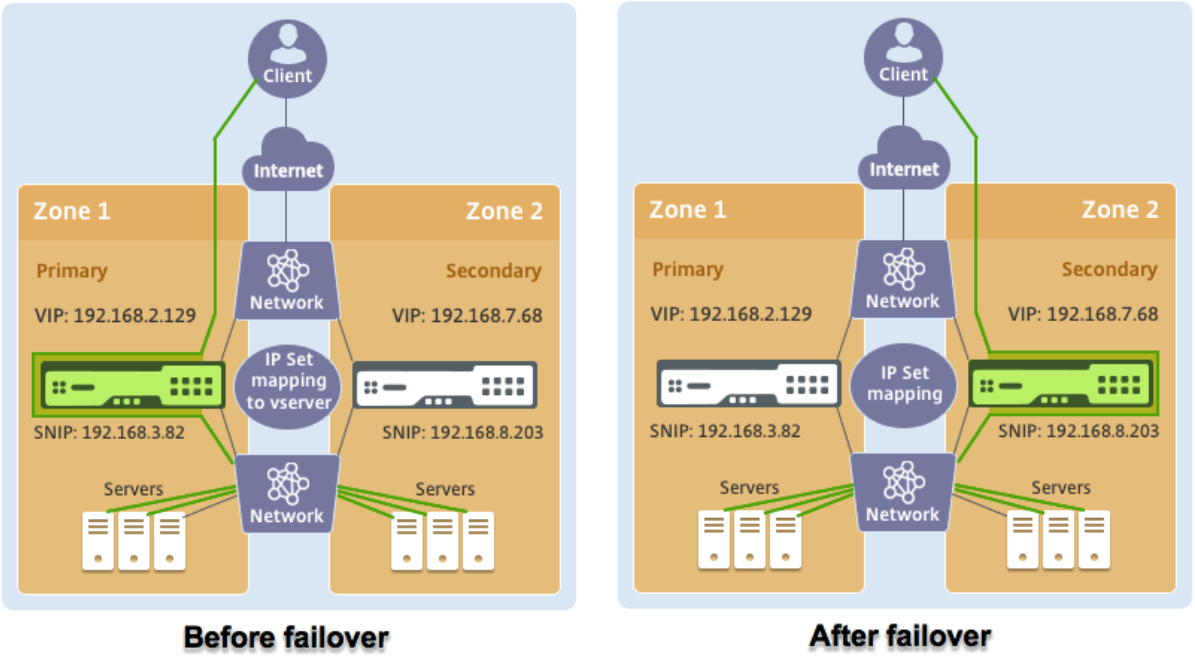
    Dans l'interface graphique, accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter**.



Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance comporte trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal. Un EIP est attaché à l'adresse IP virtuelle du nœud principal.

Schéma : Ce schéma illustre la configuration de haute disponibilité de NetScaler VPX en mode INC, sur AWS



Pour ce scénario, utilisez l'interface de ligne de commande pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds principal et secondaire.

   Sur le primaire :

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Ici, 192.168.6.82 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Sur le secondaire :

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Ici, 192.168.1.108 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un ensemble d'adresses IP et liez l'ensemble d'adresses IP au VIP sur les deux instances

   Au primaire :


```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bindipset ipset123 192.168.7.68
```

Sur le secondaire :

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bind ipset ipset123 192.168.7.68
```

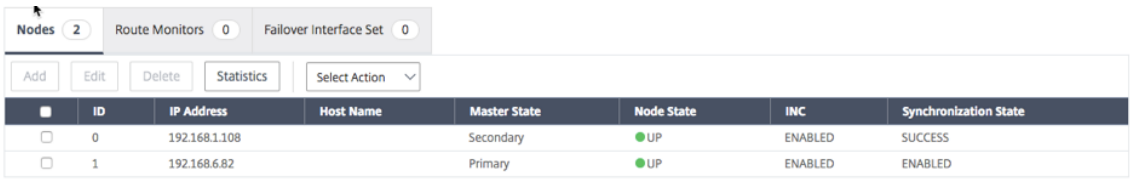
3. Ajoutez un serveur virtuel sur l'instance principale.

   La commande suivante :

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Enregistrez la configuration.

5. Après un basculement forcé, le secondaire devient le nouveau principal.



Déployez une paire VPX haute disponibilité avec des adresses IP privées dans différentes zones AWS

October 17, 2024

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées en mode INC. Cette solution peut être facilement intégrée à la paire haute disponibilité VPX multizone existante avec des adresses IP élastiques. Par conséquent, vous pouvez utiliser les deux solutions ensemble.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

> **Remarque :**
>
> Ce déploiement est pris en charge à partir de la version 13.0 de NetScaler build 67.39. Ce déploiement est compatible avec AWS Transit Gateway.

Paire haute disponibilité avec des adresses IP privées à l'aide d'un VPC non partagé AWS

Conditions préalables

Assurez-vous que le rôle IAM associé à votre compte AWS dispose des autorisations IAM suivantes :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }
```

Déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC non partagé AWS

Voici un résumé des étapes de déploiement d'une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes.

3. Configurer la haute disponibilité

    a) Configurez la haute disponibilité en mode INC dans les deux instances.
    b) Ajoutez les tables de routage respectives dans le VPC qui pointe vers l'interface client.
    c) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1, 2 et 3b, utilisez la console AWS. Pour les étapes 3a et 3c, utilisez l'interface graphique ou l'interface de ligne de commande NetScaler VPX.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes avec le même nombre d'ENI (interface réseau).

Pour plus d'informations sur la création d'un VPC et le déploiement d'une instance VPX sur AWS, consultez Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome

Étape 3. Configurez les adresses VIP ADC en choisissant un sous-réseau qui ne chevauche pas les sous-réseaux Amazon VPC. Si votre VPC est 192.168.0.0/16, pour configurer les adresses VIP ADC, vous pouvez choisir n'importe quel sous-réseau parmi les plages d'adresses IP suivantes :

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

Dans cet exemple, le sous-réseau 10.10.10.0/24 choisi et créé des VIP dans ce sous-réseau. Vous pouvez choisir n'importe quel sous-réseau autre que le sous-réseau VPC (192.168.0.0/16).

Étape 4. Ajoutez une route qui pointe vers l'interface client (VIP) du nœud principal à partir de la table de routage VPC.

À partir de l'interface de ligne de commande AWS, tapez la commande suivante :

```
aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-block 10.10.10.0/24 --gateway-id <eni-client-primary>
```

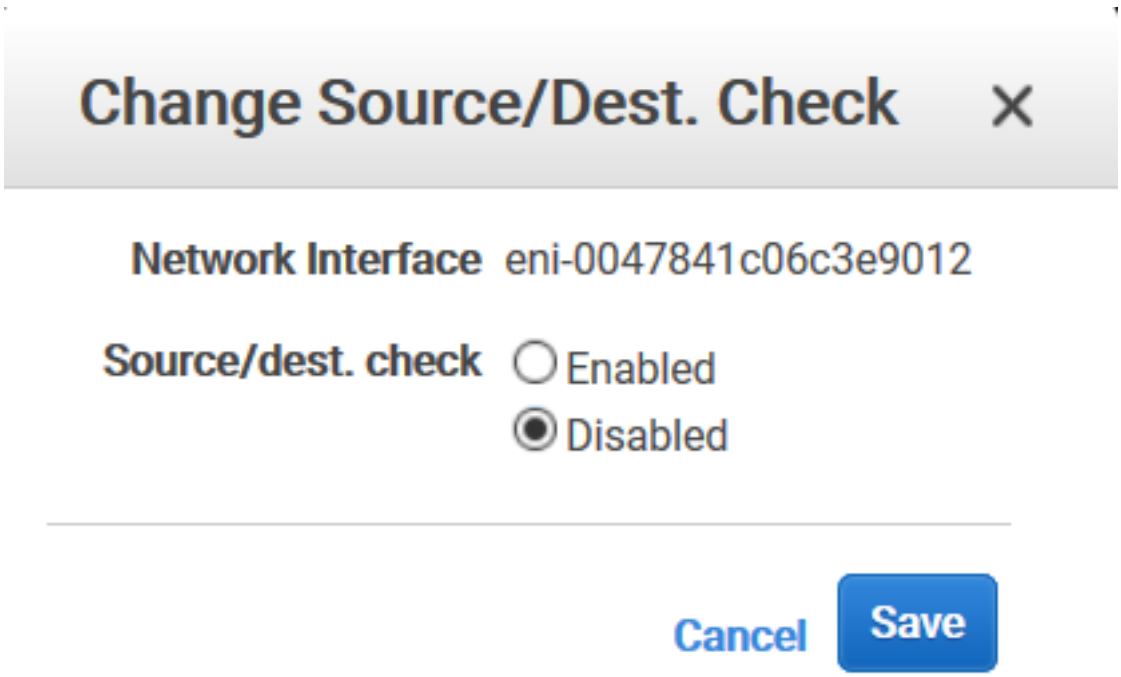
À partir de l'interface graphique AWS, effectuez les étapes suivantes pour ajouter un itinéraire :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Tables de routage**et sélectionnez la table de routage.
3. Choisissez **Actions**, puis cliquez sur **Modifier les itinéraires**.
4. Pour ajouter un itinéraire, choisissez **Ajouter un itinéraire**. Pour **Destination**, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes. Pour ID de passerelle, sélectionnez l'ENI d'une interface client du nœud principal.

> **Remarque :**
>
> Vous devez désactiver la **vérification source/dest** sur l'ENI client de l'instance principale.

Pour désactiver la vérification source/destination d'une interface réseau à l'aide de la console, effectuez les opérations suivantes :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Interfaces réseau**.
3. Sélectionnez l'interface réseau d'une interface client principale, puis choisissez **Actions**, puis cliquez sur **Modifier la source/Dest. Vérifie**.
4. Dans la boîte de dialogue, choisissez **Désactivé**, puis cliquez sur **Enregistrer**.



Étape 5. Configurer la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande NetScaler VPX ou l'interface graphique pour configurer la haute disponibilité.

Configuration de la haute disponibilité à l'aide de la CLI

1. Configurez la haute disponibilité en mode INC dans les deux instances.

   Sur le nœud principal :

   ```
   1   add ha node 1 \<sec\_ip\> -inc ENABLED
   ```

   Sur le nœud secondaire :

   ```
   1   add ha node 1 \<prim\_ip\> -inc ENABLED
   ```

   <sec_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   <prim_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale. Vous devez l'ajouter à partir du sous-réseau choisi, par exemple 10.10.10.0/24.

   Entrez la commande suivante :

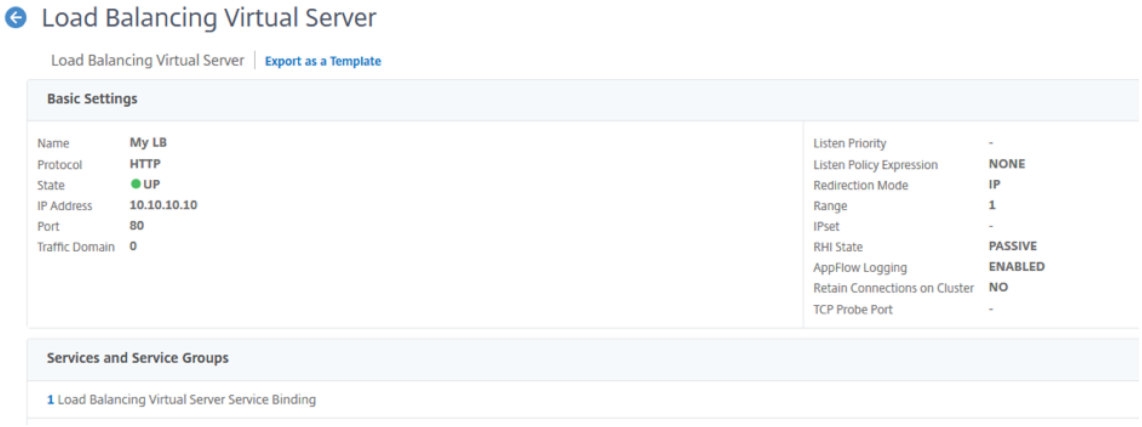
   ```
   1   add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
          primary\_vip\> \<port\>
   ```

Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configuration de la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe.
3. Accédez à **Configuration** > **Système** > **Haute disponibilité**, puis cliquez sur **Ajouter**.
4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur le nœud automatique.
6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire et cliquez sur **Créer**.
7. Répétez les étapes du nœud secondaire.

8. Ajouter un serveur virtuel dans l'instance principale

   Accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter**.



Déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC partagé AWS

Dans un modèle de VPC partagé AWS, le compte propriétaire du VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants). Par conséquent, vous disposez d'un compte propriétaire d'un VPC et d'un compte de participant. Une fois qu'un sous-réseau est partagé, les participants peuvent afficher, créer, modifier et supprimer leurs ressources d'application dans les sous-réseaux partagés avec eux. Les participants ne peuvent pas afficher, modifier ou supprimer des ressources appartenant à d'autres participants ou au propriétaire du VPC.

Pour plus d'informations sur le VPC partagé AWS, consultez la documentation AWS.

> **Remarque :**
>
> Les étapes de configuration pour déployer une paire VPX HA avec des adresses IP privées à l'aide d'un VPC partagé AWS sont les mêmes que pour déployer une paire VPX HA avec des adresses IP privées à l'aide d'un VPC non partagé AWS, à l'exception suivante :
>
> - Les tables de routage du VPC qui pointe vers l'interface client doivent être ajoutées à partir du *compte propriétaire du VPC*.

Conditions préalables

- Assurez-vous que le rôle IAM associé à l'instance NetScaler VPX dans le compte du participant AWS possède les autorisations IAM suivantes :

```
1     "Version": "2012-10-17",
2         "Statement": [
3             {
4
```



```
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "ec2:DisassociateAddress",
                    "iam:GetRole",
                    "iam:SimulatePrincipalPolicy",
                    "ec2:DescribeInstances",
                    "ec2:DescribeAddresses",
                    "ec2:ModifyNetworkInterfaceAttribute",
                    " ec2:AssociateAddress " ,
                    "sts:AssumeRole"
            ],
                "Resource": "*"
             }

        ]
    }
```

> **Remarque :**
>
> Le **rôle AssumeRole** permet à l'instance NetScaler VPX d'assumer le rôle IAM multicompte, qui est créé par le compte propriétaire du VPC.

- Assurez-vous que le compte propriétaire du VPC fournit les autorisations IAM suivantes au compte du participant à l'aide du rôle IAM entre comptes :

```
    {

        "Version": "2012-10-17",
        "Statement": [
            {

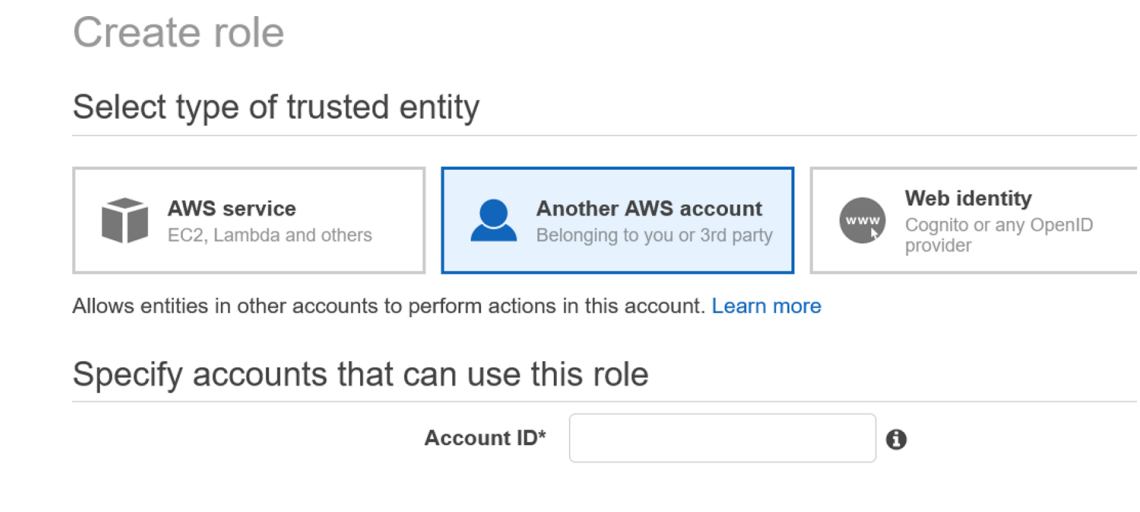
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "ec2:CreateRoute",
                    "ec2:DeleteRoute",
                    "ec2:DescribeRouteTables"
                ],
                "Resource": "*"
             }

        ]
    }
```

Créer un rôle IAM entre comptes

1. Connectez-vous à la console Web AWS.
2. Dans l'onglet **IAM**, accédez à **Roles,** puis choisissez **Create Role**.

3. Choisissez **un autre compte AWS**.



4. Entrez le numéro d'identification de compte à 12 chiffres du compte du participant auquel vous souhaitez accorder l'accès administrateur.

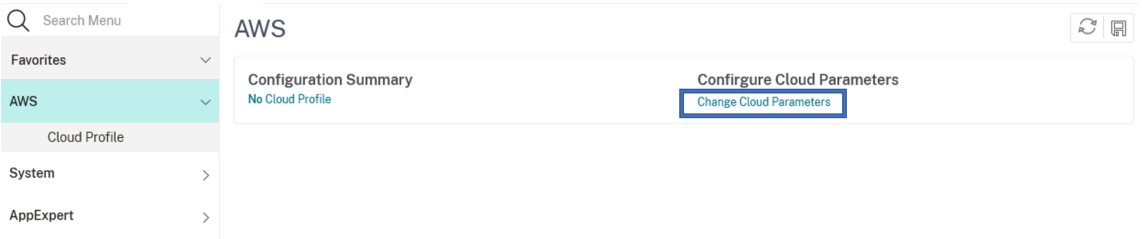
Définissez le rôle IAM multicompte à l'aide de l'interface de ligne de commande NetScaler

La commande suivante permet à l'instance NetScaler VPX d'assumer le rôle IAM intercomptes qui existe dans le compte propriétaire du VPC.

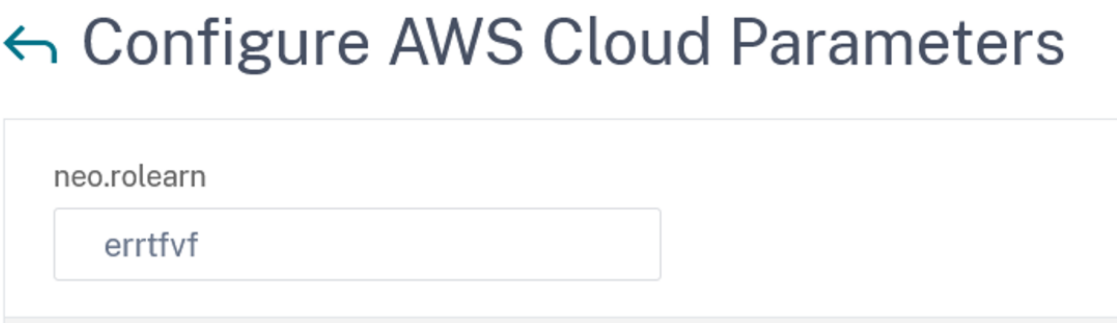
```
set cloud awsParam -roleARN <string>
```

Définissez le rôle IAM multicompte à l'aide de l'interface graphique NetScaler

1. Connectez-vous à l'appliance NetScaler et accédez à **Configuration > AWS > Modifier les paramètres du cloud**.



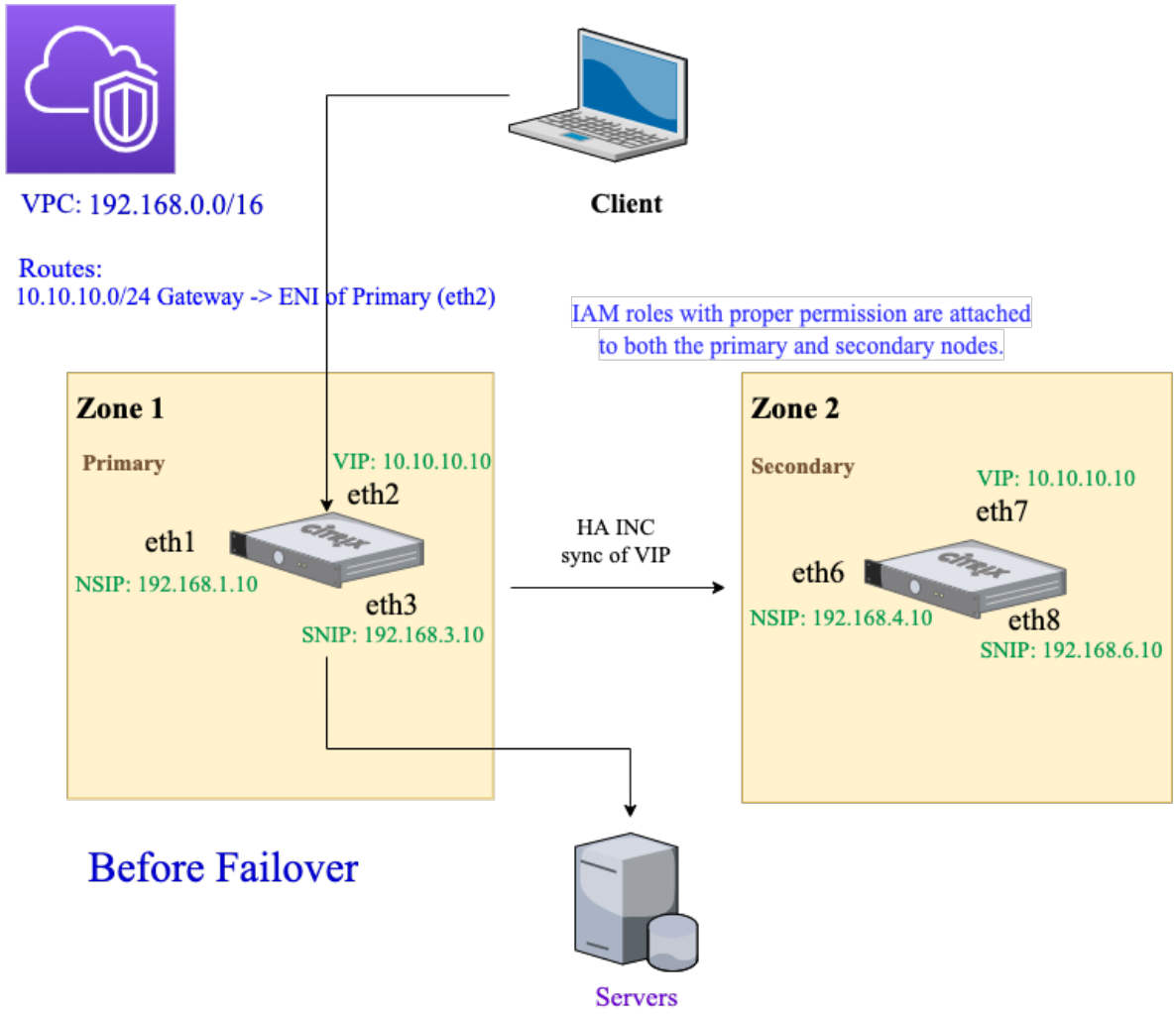
2. Sur la page **Configurer les paramètres du cloud AWS**, entrez la valeur du champ **ROLearn** .

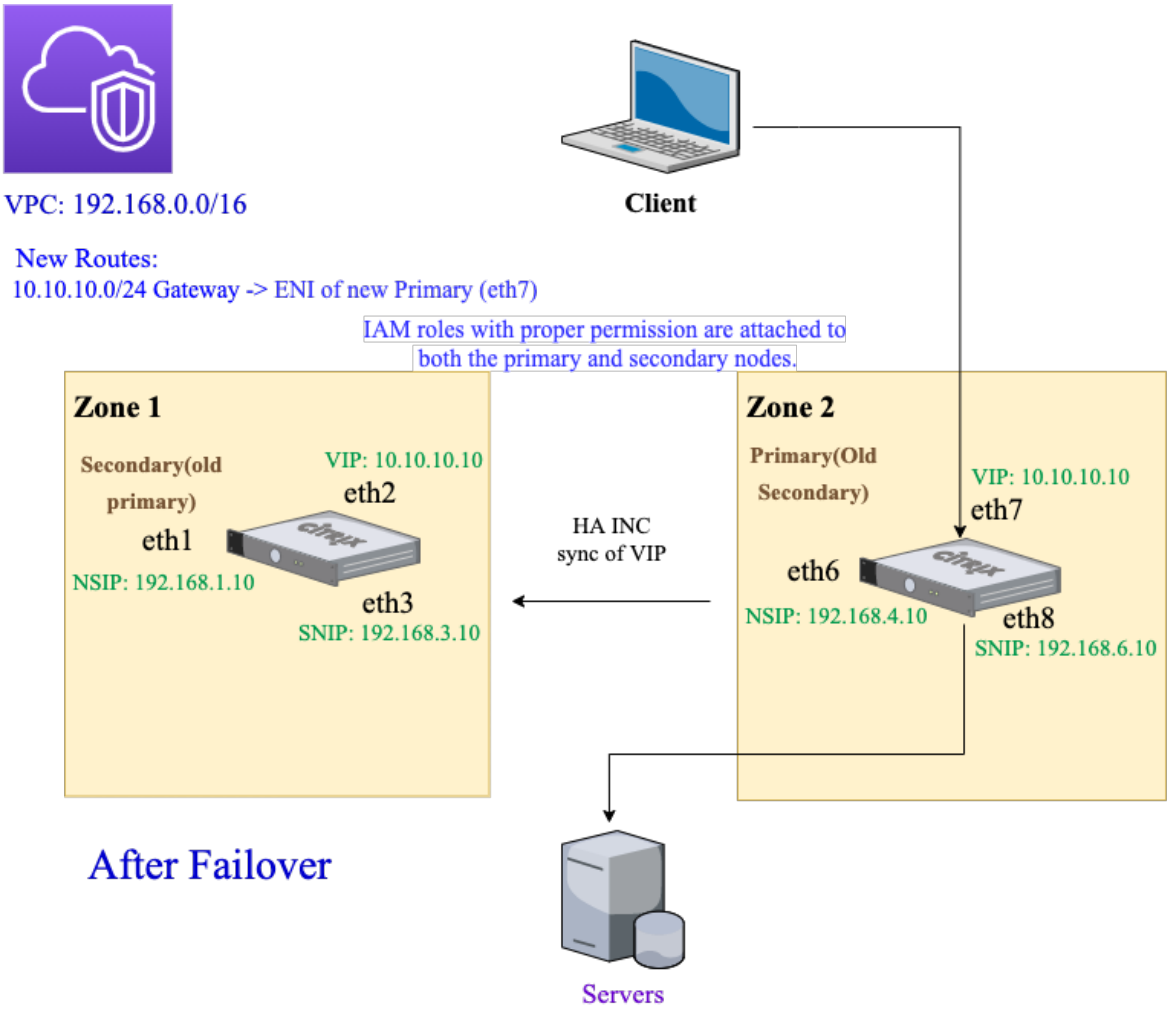


Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance comporte trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal.

Les diagrammes suivants illustrent la configuration de haute disponibilité de NetScaler VPX en mode INC, sur AWS. Le sous-réseau 10.10.10.10 personnalisé, qui ne fait pas partie du VPC, est utilisé comme VIP. Par conséquent, le sous-réseau 10.10.10.10 peut être utilisé dans toutes les zones de disponibilité.





Pour ce scénario, utilisez l'interface de ligne de commande pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds principal et secondaire.

   Sur le nœud principal :

   ```
   add ha node 1 192.168.4.10 -inc enabled
   ```

   Ici, 192.168.4.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Sur le nœud secondaire :

   ```
   add ha node 1 192.168.1.10 -inc enabled
   ```

   Ici, 192.168.1.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale.

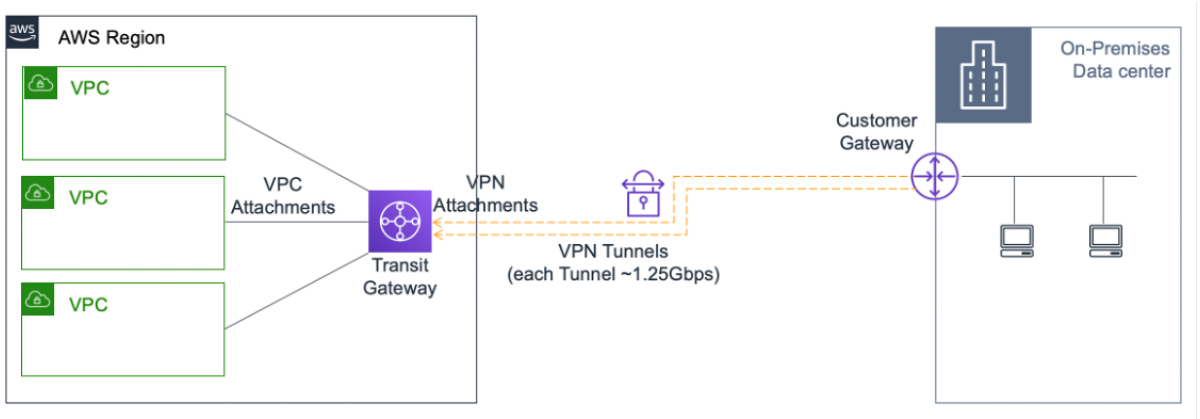
Entrez la commande suivante :

```
1    add lbvserver vserver1 http 10.10.10.10 80
```

3. Enregistrez la configuration.
4. Après un basculement forcé :
   - L'instance secondaire devient la nouvelle instance principale.
   - La route du VPC pointant vers l'ENI principale migre vers l'ENI du client secondaire.
   - Le trafic client reprend vers la nouvelle instance principale.

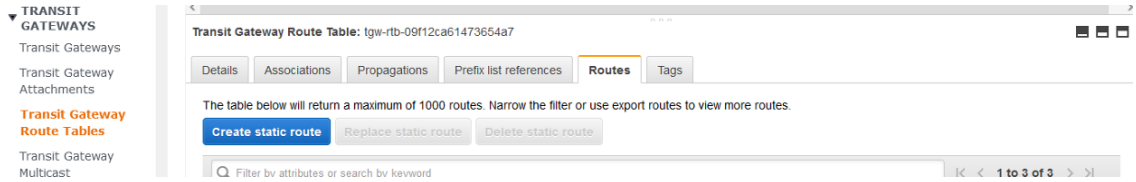
Configuration d'AWS Transit Gateway pour la solution IP privée HA

Vous avez besoin d'AWS Transit Gateway pour que le sous-réseau VIP privé soit routable au sein du réseau interne, sur les VPC AWS, les régions et les réseaux locaux. Le VPC doit se connecter à AWS Transit Gateway. Une route statique pour le sous-réseau VIP ou le pool IP à l'intérieur de la table de routage AWS Transit Gateway est créée et pointée vers le VPC.

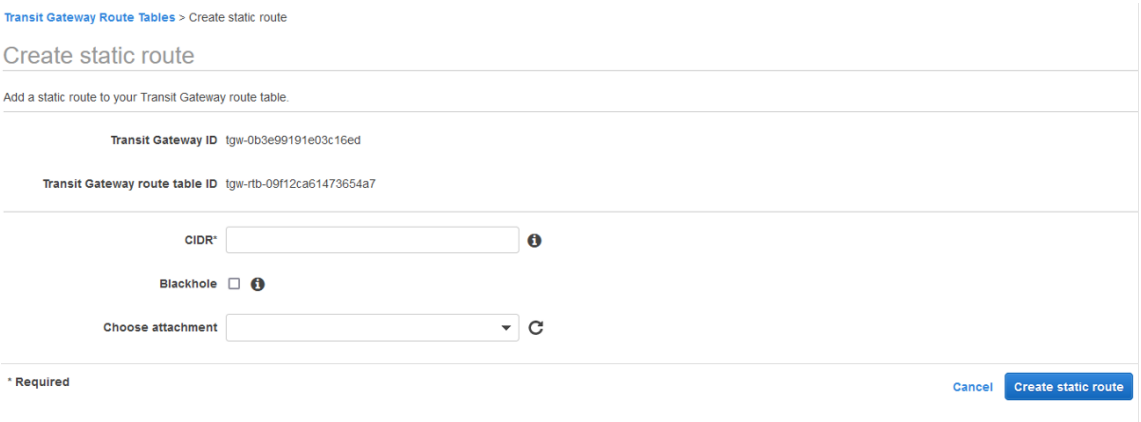


Pour configurer AWS Transit Gateway, procédez comme suit :

1. Ouvrez la console Amazon VPC.
2. Dans le volet de navigation, sélectionnez **Tables de routage Transit Gateway**.
3. Sélectionnez l'onglet **Itinéraires**, puis cliquez sur **Créer un itinéraire statique**.



4. Créez un itinéraire statique où le CIDR pointe vers votre sous-réseau VIPS privé et des points de rattachement vers le VPC doté de NetScaler VPX.



5. Cliquez sur **Créer un itinéraire statique**, puis choisissez **Fermer**.

Dépannage

Si vous rencontrez des problèmes lors de la configuration d'une solution IP privée HA sur une haute disponibilité multizone, vérifiez les points clés suivants pour résoudre les problèmes :

- Les nœuds principal et secondaire disposent du même ensemble d'autorisations IAM.
- Le mode INC est activé à la fois sur les nœuds principal et secondaire.
- Les nœuds principaux et secondaires possèdent le même nombre d'interfaces.
- Lors de la création d'une instance, suivez la même séquence d'attachement d'interfaces sur les nœuds principal et secondaire en fonction du numéro d'index de l'appareil. Supposons que sur un nœud principal, l'interface client soit attachée en premier et l'interface serveur soit attachée en second. Suivez également la même séquence sur le nœud secondaire. En cas de discordance, détachez et reconnectez les interfaces dans le bon ordre.
- Vous pouvez vérifier la séquence des interfaces en suivant ce chemin de navigation : **console AWS > Réseau et sécurité > ENI > Numéro d'index des appareils**. Par défaut, les numéros d'index des appareils suivants sont attribués à ces interfaces : - Interface de gestion —0 - Interface client —1 - Interface serveur —2

  - Interface de gestion –0
  - Interface client –1
  - Interface du serveur –2

- Si la séquence des numéros d'index des appareils sur l'ENI principal est : 0, 1, 2. L'ENI secondaire doit également suivre la même séquence de numéros d'index des appareils : 0, 1, 2.

  En cas de non-concordance dans la séquence des numéros d'index de l'appareil, toutes les routes non concordantes sont transférées vers l'index 0, l'interface de gestion, pour éviter toute

perte de routes. Mais vous devez tout de même détacher les interfaces et les rattacher à nouveau dans le bon ordre pour éviter le déplacement des itinéraires vers l'interface de gestion, car cela peut entraîner des embouteillages.

- Si le trafic ne circule pas, assurez-vous que « Source/DEST ». Check » est désactivé pour la première fois sur l'interface client du nœud principal.
- Assurez-vous que la `cloudhadaemon` commande (`ps -aux | grep cloudha`) est exécutée dans Shell.
- Assurez-vous que la version du microprogramme NetScaler est 13.0 build 70.x ou ultérieure.
- Pour les problèmes liés au processus de basculement, consultez le fichier journal disponible à l'adresse : `/var/log/cloud-ha-daemon.log`

Déployer une instance NetScaler VPX sur AWS Outposts

October 17, 2024

AWS Outposts est un pool de capacités de calcul et de stockage AWS déployées sur votre site. Outposts fournit l'infrastructure et les services AWS sur site. AWS exploite, surveille et gère cette capacité dans le cadre d'une région AWS. Vous pouvez utiliser les mêmes instances NetScaler VPX, les mêmes API AWS, les mêmes outils et la même infrastructure sur site et dans le cloud AWS pour bénéficier d'une expérience hybride cohérente.

Vous pouvez créer des sous-réseaux sur vos Outposts et les spécifier lorsque vous créez des ressources AWS telles que des instances EC2, des volumes EBS, des clusters ECS et des instances RDS. Les instances des sous-réseaux Outposts communiquent avec d'autres instances de la région AWS à l'aide d'adresses IP privées, toutes au sein du même Amazon Virtual Private Cloud (VPC).

Pour plus d'informations, consultez le guide de l'utilisateur AWS Outposts.

Fonctionnement de AWS Outposts

AWS Outposts est conçu pour fonctionner avec une connexion constante et cohérente entre vos Outposts et une région AWS. Pour établir cette connexion à la région et aux charges de travail locales de votre environnement sur site, vous devez connecter votre Outpost à votre réseau local. Votre réseau local doit fournir un accès WAN à la région et à Internet. Internet doit également fournir un accès LAN ou WAN au réseau local sur lequel résident vos charges de travail ou applications sur site.

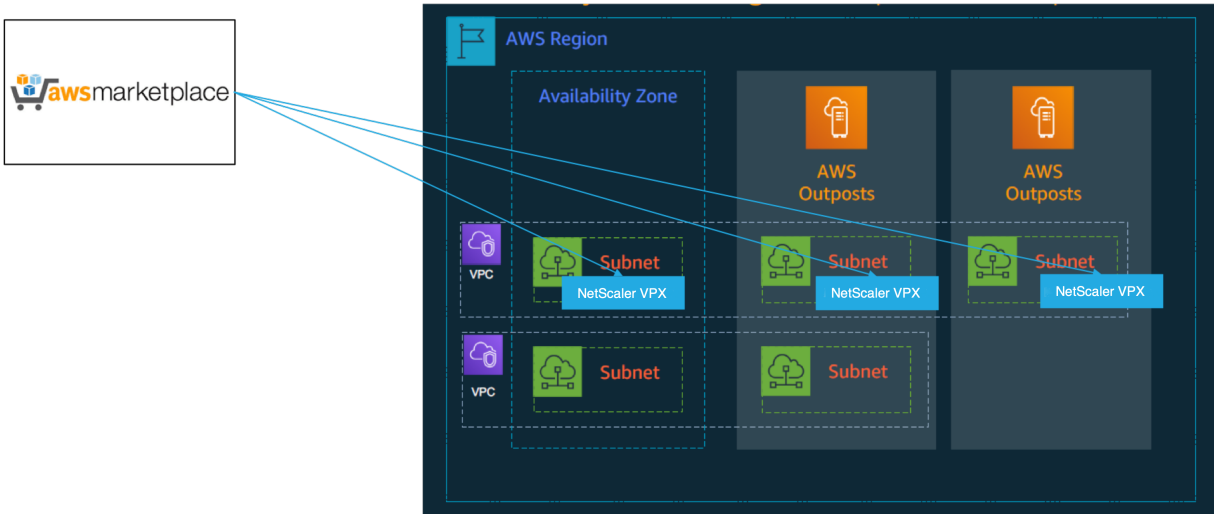
Conditions préalables

- Vous devez installer AWS Outposts sur votre site.
- La capacité de calcul et de stockage d'AWS Outposts doit être disponible pour être utilisée.

Pour plus d'informations sur la manière de passer une commande pour AWS Outposts, consultez la documentation AWS suivante : https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

Déployez une instance NetScaler VPX sur AWS Outposts à l'aide de la console Web AWS

La figure suivante décrit un déploiement simple d'instances NetScaler VPX sur les Outposts. L'AMI NetScaler présente sur AWS Marketplace est également déployée dans les Outposts.



Connectez-vous à la console Web AWS et effectuez les étapes suivantes pour déployer des instances NetScaler VPX EC2 sur vos AWS Outposts.

1. Créez une paire de clés.
2. Créez un cloud privé virtuel (VPC).
3. Ajoutez d'autres sous-réseaux.
4. Créez des groupes de sécurité et des règles de sécurité.
5. Ajoutez des tables de routage.
6. Créez une passerelle Internet.
7. Créez une instance NetScaler VPX à l'aide du service AWS EC2. Depuis le tableau de bord AWS, accédez à **Compute > EC2 > Launch Instance > AWS Marketplace**.
8. Créez et connectez davantage d'interfaces réseau.
9. Attachez des adresses IP élastiques à la carte réseau de gestion.
10. Connectez-vous à l'instance VPX.

Pour obtenir des instructions détaillées sur chacune des étapes, consultez Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS.

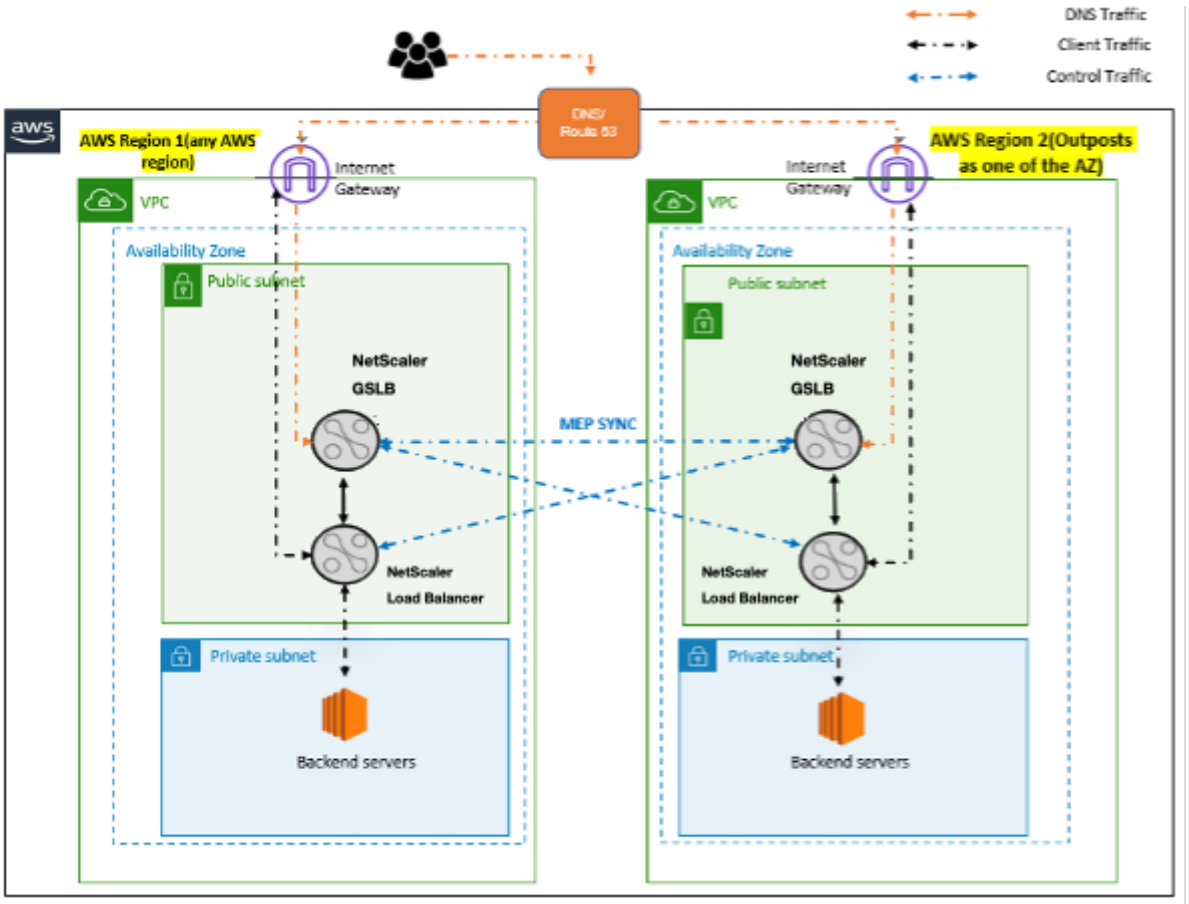
Pour un déploiement haute disponibilité dans la même zone de disponibilité, consultez Déployer une paire haute disponibilité sur AWS.

Déployez une instance NetScaler VPX sur un cloud hybride avec AWS Outposts

Vous pouvez déployer une instance NetScaler VPX sur un cloud hybride dans un environnement AWS qui contient des avant-postes AWS. Vous pouvez simplifier le mécanisme de diffusion des applications à l'aide de la solution d'équilibrage de charge globale des serveurs (GSLB) de NetScaler. La solution GSLB distribue le trafic des applications entre plusieurs centres de données dans des clouds hybrides conçus à l'aide des régions AWS et de l'infrastructure AWS Outposts.

NetScaler GSLB prend en charge les types de déploiement actif-actif et actif-passif pour répondre à différents cas d'utilisation. Outre ces options de déploiement flexibles et ces mécanismes de fourniture d'applications, NetScaler sécurise l'ensemble du réseau et du portefeuille d'applications, que les applications soient déployées de manière native sur AWS Cloud ou AWS Outposts.

Le schéma suivant illustre la mise à disposition d'une application avec l'appliance NetScaler dans un cloud hybride avec AWS.



Dans un déploiement actif-actif, NetScaler dirige le trafic à l'échelle mondiale dans un environnement distribué. Tous les sites de l'environnement échangent des mesures concernant la disponibilité et l'état de santé des ressources via le Metrics Exchange Protocol (MEP). L'appliance NetScaler utilise ces informations pour équilibrer la charge du trafic entre les sites et envoie les demandes des clients au site GSLB le plus approprié, selon la méthode définie (round robin, connexion minimale et proximité statique) spécifiée dans la configuration GSLB.

Vous pouvez utiliser le déploiement GSLB actif-actif pour :

- Optimisez l'utilisation des ressources avec tous les nœuds actifs.
- Améliorez l'expérience utilisateur en dirigeant les demandes vers le site le plus proche de chaque utilisateur.
- Migrez les applications vers le cloud à un rythme défini par l'utilisateur.

Vous pouvez utiliser le déploiement GSLB actif-passif pour :

- Récupération d'urgence
- Explosion de nuages

Références

- Déployer une instance NetScaler VPX sur AWS
- Déployez une instance NetScaler VPX sur AWS Outposts à l'aide de la console Web AWS
- Configurer GSLB sur des instances NetScaler VPX

Protégez AWS API Gateway à l'aide du pare-feu NetScaler Web App Firewall

October 17, 2024

Vous pouvez déployer une appliance NetScaler devant votre AWS API Gateway et sécuriser la passerelle d'API contre les menaces externes. NetScaler Web App Firewall (WAF) peut protéger votre API contre les 10 principales menaces de l'OWASP et les attaques de type « jour zéro ». NetScaler Web App Firewall utilise une base de code unique pour tous les formats ADC. Par conséquent, vous pouvez appliquer et appliquer des stratégies de sécurité de manière cohérente dans n'importe quel environnement. NetScaler Web App Firewall est facile à déployer et est disponible sous forme de licence unique. Le pare-feu NetScaler Web App fournit les fonctionnalités suivantes :

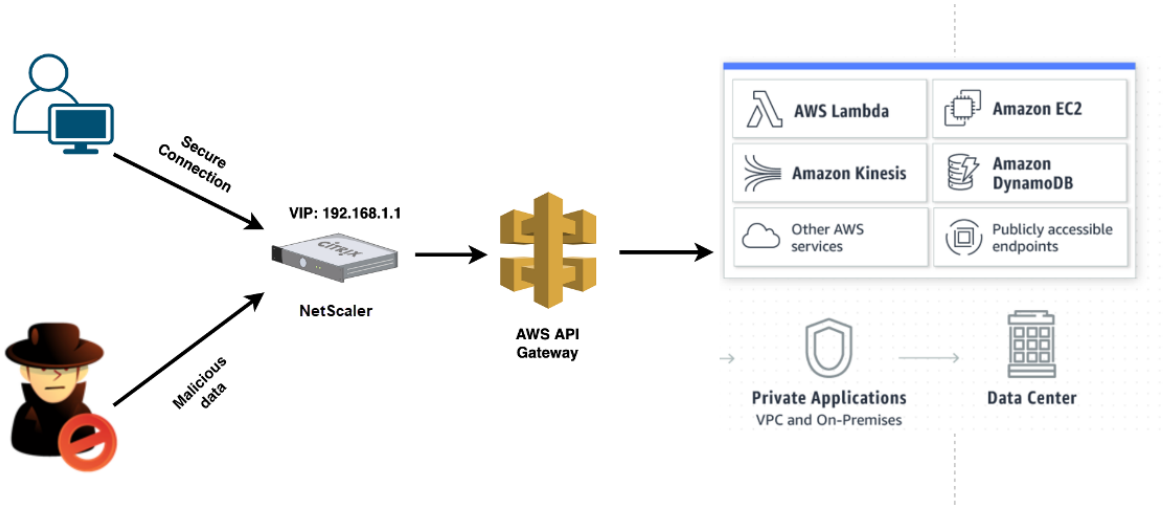
- Configuration simplifiée
- Gestion des robots
- Visibilité holistique
- Rassemblez des données provenant de plusieurs sources et affichez les données sur un écran unifié

Outre la protection de la passerelle d'API, vous pouvez également utiliser les autres fonctionnalités de NetScaler. Pour plus d'informations, consultez la documentation de NetScaler. Pour plus d'informations, consultez la documentation de NetScaler. En plus d'éviter les basculements du centre de données et de minimiser le temps d'arrêt, vous pouvez placer ADC en haute disponibilité au sein ou entre les zones de disponibilité. Vous pouvez également utiliser ou configurer le clustering avec la fonction Autoscale.

Auparavant, AWS API Gateway ne prenait pas en charge les protections nécessaires pour sécuriser les applications sous-jacentes. Sans les protections du Web Application Firewall (WAF), les API étaient sujettes à des menaces de sécurité.

Déployez l'appliance NetScaler devant la passerelle d'API AWS

Dans l'exemple suivant, une appliance NetScaler est déployée devant la passerelle d'API AWS.



Supposons qu'il existe une véritable demande d'API pour le service AWS Lambda. Cette demande peut concerner n'importe lequel des services d'API mentionnés dans la documentation Amazon API Gateway. Comme le montre le schéma précédent, le flux de trafic est le suivant :

1. Le client envoie une demande à la fonction AWS Lambda (XYZ). Cette demande du client est envoyée au serveur virtuel NetScaler (192.168.1.1).
2. Le serveur virtuel inspecte le paquet et recherche tout contenu malveillant.
3. L'appliance NetScaler déclenche une stratégie de réécriture pour modifier le nom d'hôte et l'URL d'une demande client. Par exemple, vous souhaitez changer `https://restapi.citrix.com/default/LamdaFunctionXYZ` sur`https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ`.
4. L'appliance NetScaler transmet cette demande à la passerelle d'API AWS.
5. AWS API Gateway envoie ensuite la demande au service Lambda et appelle la fonction Lambda « XYZ ».
6. Dans le même temps, si un attaquant envoie une demande d'API contenant du contenu malveillant, la demande malveillante atterrit sur l'appliance NetScaler.
7. L'appliance NetScaler inspecte les paquets et les supprime en fonction de l'action configurée.

Configurer l'appliance NetScaler avec WAF activé

Pour activer WAF sur une appliance NetScaler, procédez comme suit :

1. Ajoutez un commutateur de contenu ou un serveur virtuel d'équilibrage de charge. Supposons que l'adresse IP du serveur virtuel soit 192.168.1.1, qui se résout en un nom de domaine (restapi.citrix.com).
2. Activez la stratégie WAF sur le serveur virtuel NetScaler. Pour plus d'informations, consultez Configuration du Web App Firewall.

3. Activez la stratégie de réécriture pour modifier le nom de domaine. Supposons que vous souhaitiez modifier la demande entrante de l'équilibreur de charge sur le nom de domaine « restapi.citrix.com » afin qu'elle soit réécrite sur le serveur principal AWS API Gateway à l'adresse « citrix.execute-api.<region> Nom de domaine .amazonaws ».
4. Activez le mode L3 sur l'appliance NetScaler pour qu'elle agisse en tant que proxy. Utilisez la commande suivante :

```
enable ns mode L3
```

À l'étape 3 de l'exemple précédent, supposons que l'administrateur du site Web souhaite que l'appliance NetScaler remplace le nom de domaine « restapi.citrix.com » par « citrix.execute-api ».<region>.amazonaws.com » et l'URL avec « Default/Lambda/xyz ».

La procédure suivante explique comment modifier le nom d'hôte et l'URL dans une demande client à l'aide de la fonction de réécriture :

1. Connectez-vous à l'appliance NetScaler via SSH.
2. Ajoutez des actions de réécriture.

```
add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER
    (\"Host\")" "\"citrix.execute-api.<region>.amazonaws.com\""

add rewrite action rewrite_url_act replace HTTP.REQ.URL.
    PATH_AND_QUERY "\"/default/lambda/XYZ\""
```

3. Ajoutez des stratégies de réécriture pour les actions de réécriture.

```
add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER(\"Host
    \").CONTAINS(\"restapi.citrix.com\") "rewrite_host_hdr_act

add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER(\"Host\").
    CONTAINS(\"restapi.citrix.com\") "rewrite_url_act
```

4. Liez les stratégies de réécriture à un serveur virtuel.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol
    -priority 10 -gotoPriorityExpression 20 -type REQUEST

bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
    priority 20 -gotoPriorityExpression END -type REQUEST
```

Pour plus d'informations, voir Configurer la réécriture pour modifier le nom d'hôte et l'URL dans la demande du client sur l'appliance NetScaler.

Fonctionnalités et fonctionnalités de NetScaler

Outre la sécurisation du déploiement, l'appliance NetScaler peut également améliorer la demande en fonction des besoins de l'utilisateur. L'appliance NetScaler fournit les fonctionnalités clés suivantes.

- **Équilibrage de la charge de la passerelle d'API :** si vous possédez plusieurs passerelles d'API, vous pouvez équilibrer la charge de plusieurs passerelles d'API à l'aide de l'appliance NetScaler et définir le comportement de la demande d'API.
  - Différentes méthodes d'équilibrage de charge sont disponibles. Par exemple, la méthode de connexion Least évite de surcharger la limite API Gateway, la méthode de chargement personnalisé conserve une charge spécifique sur une passerelle API particulière, etc. Pour plus d'informations, voir Algorithmes d'équilibrage de charge.
  - Le déchargement SSL est configuré sans interrompre le trafic.
  - Le mode Use Source IP (USIP) est activé pour conserver l'adresse IP du client.
  - Paramètres SSL définis par l'utilisateur : vous pouvez disposer de votre propre serveur virtuel SSL avec vos propres certificats et algorithmes signés.
  - Serveur virtuel de sauvegarde : si la passerelle API n'est pas accessible, vous pouvez envoyer la demande à un serveur virtuel de sauvegarde pour d'autres actions.
  - De nombreuses autres fonctionnalités d'équilibrage de charge sont disponibles. Pour plus d'informations, consultez la section Trafic d'équilibrage de charge sur une appliance NetScaler.
- **Authentification, autorisation et audit :** vous pouvez définir vos propres méthodes d'authentification telles que LDAP, SAML, RADIUS, et autoriser et auditer les demandes d'API.
- **Répondeur :** vous pouvez rediriger les demandes d'API vers une autre API Gateway pendant le temps d'arrêt.
- **Limitation du débit :** vous pouvez configurer la fonctionnalité de limitation de débit pour éviter la surcharge d'une passerelle API.
- **Meilleure disponibilité :** vous pouvez configurer une appliance NetScaler dans une configuration haute disponibilité ou une configuration en cluster pour améliorer la disponibilité de vos trafics d'API AWS.
- **API REST :** prend en charge l'API REST, qui peut être utilisée pour automatiser le travail dans les environnements de production cloud.
- **Surveiller les données :** Surveille et enregistre les données pour référence.

L'appliance NetScaler fournit de nombreuses fonctionnalités supplémentaires, qui peuvent être intégrées à la passerelle d'API AWS. Pour plus d'informations, consultez la documentation de NetScaler.

Ajouter le service principal AWS Autoscaling

October 17, 2024

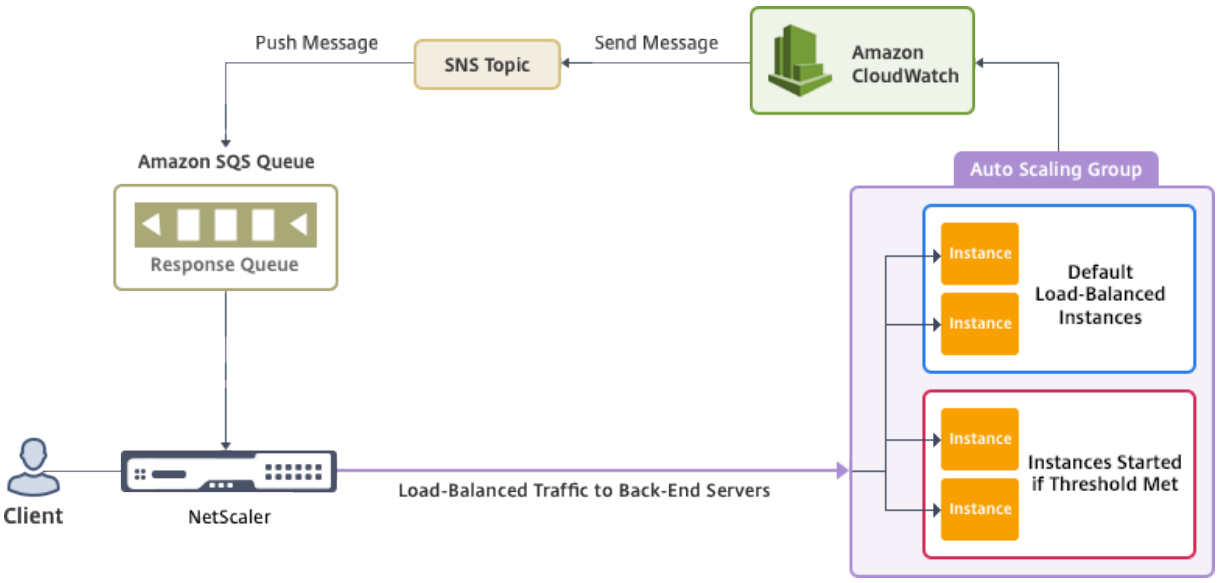
L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources réseau. Lorsque la demande diminue, vous devez réduire votre consommation pour éviter le coût inutile des ressources inutilisées. Vous pouvez minimiser le coût d'exécution des applications en déployant uniquement le nombre d'instances nécessaires à un moment donné. Pour ce faire, vous devez constamment surveiller le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement applicatif puisse évoluer à la hausse ou à la baisse de manière dynamique, vous devez automatiser les processus de surveillance du trafic et d'augmentation et de diminution des ressources chaque fois que cela est nécessaire.

Intégrée au service AWS Auto Scaling, l'instance NetScaler VPX offre les avantages suivants :

- **Équilibrage et gestion de la charge** : configure automatiquement les serveurs pour qu'ils puissent évoluer vers le haut et vers le bas, en fonction de la demande. L'instance VPX détecte automatiquement les groupes Autoscale dans le sous-réseau principal et permet à l'utilisateur de sélectionner les groupes Autoscale pour équilibrer la charge. Tout cela se fait en configurant automatiquement les adresses IP virtuelles et de sous-réseau sur l'instance VPX.
- **Haute disponibilité** : détecte les groupes Autoscale qui couvrent plusieurs zones de disponibilité et serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs dorsaux sur différents VPC, en utilisant le peering VPC
  - Serveurs principaux appartenant aux mêmes groupes de placement
  - Serveurs dorsaux situés dans différentes zones de disponibilité
- **Résiliation progressive de la connexion** : supprime les serveurs Autoscale de manière harmonieuse, évitant ainsi la perte de connexions client en cas de réduction de capacité, à l'aide de la fonction Graceful Timeout.
- **Épuisement des connexions pour les serveurs de secours** : empêche l'envoi de nouvelles connexions client au serveur en mode veille. Cependant, les serveurs Standby font toujours partie du groupe Autoscaling et continuent à gérer les connexions client existantes jusqu'à leur fermeture. Lorsque le serveur revient à l'état InService, il recommence à gérer les nouvelles

connexions. Vous pouvez utiliser l'état Standby pour mettre à jour, modifier ou dépanner les serveurs, ou pour les réduire en fonction des besoins. Pour plus d'informations, consultez la documentation AWS.

Schéma : service AWS Autoscaling avec une instance NetScaler VPX



Ce schéma illustre la compatibilité du service AWS Autoscaling avec une instance NetScaler VPX (serveur virtuel d'équilibrage de charge). Pour plus d'informations, consultez les rubriques AWS suivantes.

- Groupes de mise à l'échelle automatique
- CloudWatch
- Service de notification simple (SNS)
- Service de file d'attente simple (Amazon SQS)

Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance NetScaler VPX, vous devez effectuer les tâches suivantes.

- Lisez les rubriques suivantes :
  - Conditions préalables
  - Directives de limitation et d'utilisation
- Créez une instance NetScaler VPX sur AWS selon vos besoins.
  - Pour plus d'informations sur la création d'une instance autonome NetScaler VPX, consultez Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome

- Pour plus d'informations sur le déploiement d'instances VPX en mode HA, consultez Déployer une paire haute disponibilité sur AWS.

> **Remarque :**
>
> Nous recommandons les paramètres suivants :
>
> - Utilisez le modèle CloudFormation pour créer des instances NetScaler VPX sur AWS.
> - Créez trois interfaces distinctes : une pour la gestion (NSIP), une pour le serveur virtuel LB (VIP) orienté client et une pour l'IP de sous-réseau (NSIP).

- Créez un groupe AWS Autoscale. Si vous ne disposez pas d'une configuration Autoscaling existante, vous devez :

  1. Création d'une configuration de lancement
  2. Création d'un groupe de mise à l'échelle automatique
  3. Vérifiez le groupe Autoscaling

  Pour plus d'informations, consultez http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

- À partir de la version 14.1-12.x de NetScaler, dans un groupe AWS Autoscale, vous devez spécifier une stratégie de réduction de la taille uniquement si vous avez activé l'option Graceful. Dans les versions de NetScaler antérieures à 14.1-12.x, vous deviez spécifier au moins une stratégie de réduction, que l'option Graceful soit activée ou non.

  L'instance NetScaler VPX ne prend en charge que la stratégie de dimensionnement par étapes. La stratégie de dimensionnement simple et la stratégie de mise à l'échelle de suivi des cibles ne sont pas prises en charge pour le groupe Autoscale.

- Assurez-vous que votre compte AWS dispose des autorisations IAM suivantes :

```
1    {
2
3        "Version": "2012-10-17",
4        "Statement": \[
5         {
6
7                "Action": \[
8                    "ec2:DescribeInstances",
9                    "ec2:DescribeNetworkInterfaces",
10                   "ec2:DetachNetworkInterface",
11                   "ec2:AttachNetworkInterface",
12                   "ec2:StartInstances",
13                   "ec2:StopInstances",
14                   "ec2:RebootInstances",
15                   "autoscaling:\*",
16                   "sns:\*",
17                   "sqs:\*"
```



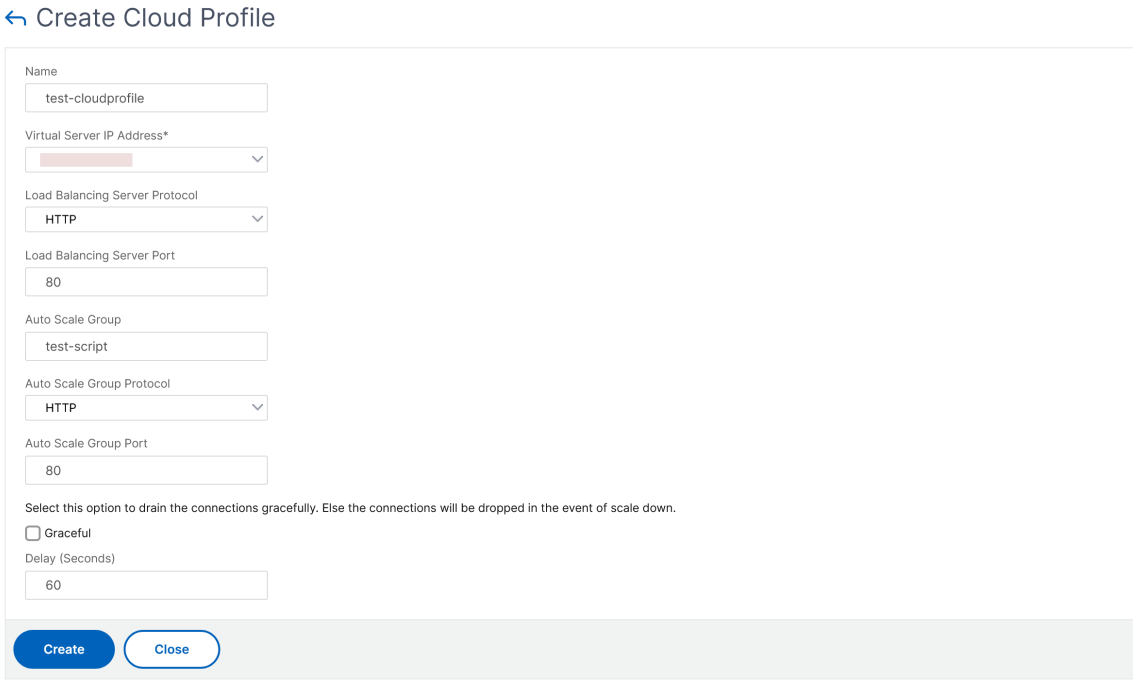
```
18
19                  “ iam: SimulatePrincipalPolicy ”
20                  “ iam: GetRole ”
21                 \],
22                 "Resource": "\*",
23                 "Effect": "Allow"
24              }
25
26          \]
27      }
```

Ajouter le service AWS Autoscaling à une instance NetScaler VPX

Procédez comme suit pour ajouter le service Autoscaling à une instance VPX :

1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour `nsroot`.
2. Accédez à **Système > AWS > Profil cloud** et cliquez sur **Ajouter**.

   La page de configuration de **Create Cloud Profile** s'affiche.



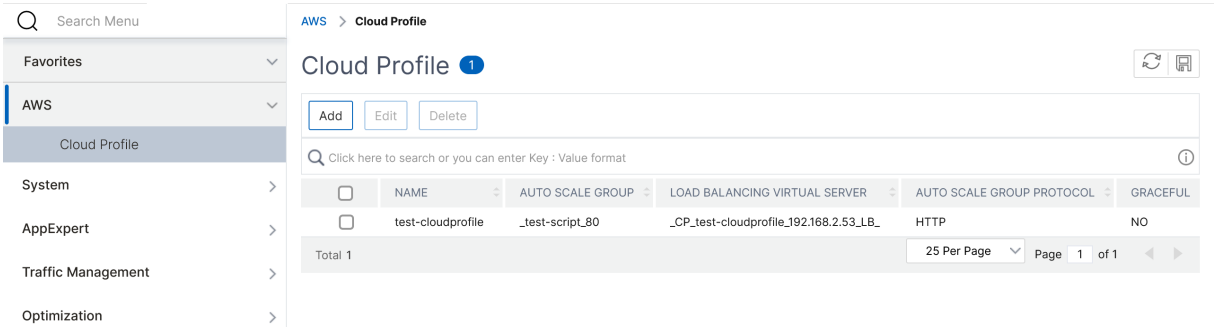
Points à noter lors de la création d'un profil cloud :

- L'adresse IP du serveur virtuel est automatiquement renseignée à partir de l'adresse IP gratuite disponible pour l'instance VPX. Pour plus d'informations, voir Gérer plusieurs adresses IP.
- Tapez le nom exact du groupe Autoscale que vous avez configuré sur votre compte AWS. Pour plus d'informations, consultez la section Groupes AWS Auto Scaling.

- Lors de la sélection du protocole et du port du groupe Autoscaling, assurez-vous que vos serveurs écoutent ces protocoles et ports et que vous liez le bon moniteur au groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour le type de protocole SSL Autoscaling, une fois que vous avez créé le profil cloud, le serveur virtuel ou le groupe de services d'équilibrage de charge semble être en panne en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.
- Sélectionnez **Graceful** et spécifiez une valeur de délai dans le champ **Delay** pour supprimer les serveurs Autoscale de manière élégante. Cette option déclenche un événement de réduction d'échelle. L'instance VPX ne supprime pas le serveur immédiatement mais marque l'un des serveurs pour une suppression progressive. Pendant cette période, l'instance VPX n'autorise pas de nouvelles connexions à ce serveur. Les connexions existantes sont desservies jusqu'à expiration du délai imparti. Une fois le délai expiré, l'instance VPX supprime le serveur.

  Si vous ne sélectionnez pas l'option **Graceful**, le serveur du groupe Autoscale est supprimé immédiatement après la baisse de la charge. Cela peut entraîner une interruption de service pour les clients connectés existants.

Après avoir créé le profil cloud, un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services dont les membres constituent les serveurs du groupe Autoscaling sont créés. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.



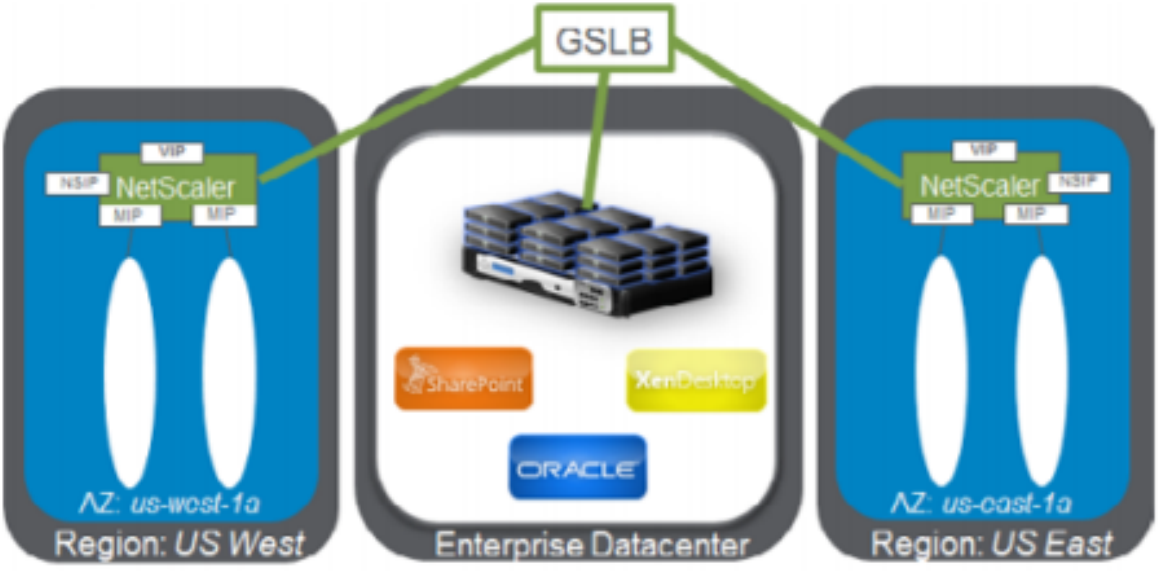
Remarque :

- Pour consulter les informations relatives à AutoScale dans la console AWS, accédez à **EC2** > **Tableau de bord** > **Auto Scaling** > **Auto Scaling Group**.
- Vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même groupe Autoscaling (ASG) dans AWS. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.

Déployez NetScaler GSLB sur AWS

October 17, 2024

La configuration de GSLB pour NetScaler sur AWS consiste essentiellement à configurer NetScaler pour équilibrer la charge du trafic vers les serveurs situés en dehors du VPC auquel NetScaler appartient, par exemple au sein d'un autre VPC dans une autre région de disponibilité ou dans un centre de données sur site.



Présentation de DBS

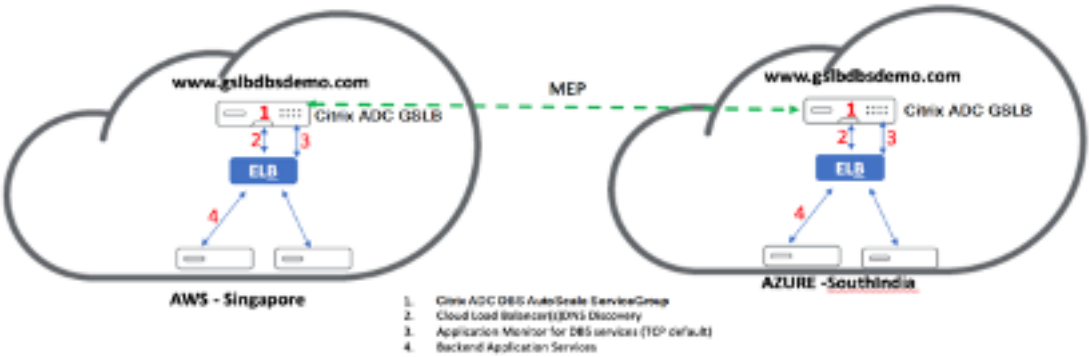
La prise en charge de NetScaler GSLB à l'aide de services basés sur les noms de domaine (DBS) pour les équilibreurs de charge cloud permet la découverte automatique de services cloud dynamiques à l'aide d'une solution d'équilibrage de charge cloud. Cette configuration permet à NetScaler d'implémenter l'équilibrage de charge global du serveur (GSLB DBS) dans un environnement actif-actif. DBS permet de dimensionner les ressources back-end dans les environnements AWS à partir de la découverte DNS.

Cette section couvre les intégrations entre NetScaler dans les environnements AWS AutoScaling. La dernière section du document détaille la possibilité de configurer une paire HA de NetScaler ADC couvrant deux zones de disponibilité (AZ) différentes spécifiques à une région AWS.

DBS avec ELB

GSLB DBS utilise le nom de domaine complet de l'utilisateur Elastic Load Balancer (ELB) pour mettre à jour dynamiquement les groupes de services GSLB afin d'inclure les serveurs principaux créés et supprimés dans AWS. Les serveurs et instances principaux d'AWS peuvent être configurés pour évoluer en fonction de la demande du réseau ou de l'utilisation du processeur. Pour configurer cette fonctionnalité, pointez NetScaler vers l'ELB pour effectuer un routage dynamique vers différents serveurs dans AWS sans avoir à mettre à jour NetScaler manuellement chaque fois qu'une instance est créée et supprimée dans AWS. La fonctionnalité NetScaler DBS pour les groupes de services GSLB utilise la découverte de services prenant en charge DNS pour déterminer les ressources de service membres de l'espace de noms DBS identifié dans le groupe Autoscale.

Composants NetScaler GSLB DBS Autoscale avec équilibreurs de charge cloud :



Configuration des composants AWS

Groupes de sécurité

> **Remarque :**
>
> Nous vous recommandons de créer différents groupes de sécurité pour ELB, l'instance NetScaler GSLB et l'instance Linux, car l'ensemble de règles requis pour chacune de ces entités est différent. Cet exemple comporte une configuration consolidée du groupe de sécurité par souci de brièveté.

Pour garantir la configuration correcte du pare-feu virtuel, consultez Groupes de sécurité pour votre VPC.

1. Connectez-vous au **groupe de ressources AWS** utilisateur et accédez à **EC2 > NETWORK & SECURITY > Security Groups**.
2. Cliquez sur **Créer un groupe de sécurité** et saisissez un nom et une description. Ce groupe de sécurité englobe les serveurs Web principaux NetScaler et Linux.

3. Ajoutez les règles de port entrant à partir de la capture d'écran suivante.

> **Remarque :**
>
> Il est recommandé de limiter l'accès IP source pour le durcissement granulaire. Pour plus d'informations, voir Règles du serveur Web.

1. Services Web principaux Amazon Linux

   a) Connectez-vous au **groupe de ressources AWS** utilisateur et accédez à **EC2 > Instances**.

   b) Cliquez sur**Lancer l'instance** en utilisant les informations qui suivent pour configurer l'instance**Amazon Linux** .

   Saisissez les détails concernant la configuration d'un serveur Web ou d'un service back-end sur cette instance.

2. Configuration de NetScaler

   a) Connectez-vous au **groupe de ressources AWS** utilisateur et accédez à **EC2 > Instances**.

   b) Cliquez sur **Launch Instance** et utilisez les informations suivantes pour configurer l'instance**Amazon AMI**.

3. Configuration IP Elastic

> **Remarque :**
>
> NetScaler peut également être configuré pour fonctionner avec une seule adresse IP élastique si nécessaire pour réduire les coûts, en ne disposant pas d'une adresse IP publique pour le NSIP. Au lieu de cela, attachez une adresse IP élastique au SNIP qui peut couvrir l'accès de gestion au boîtier, en plus de l'adresse IP du site GSLB et de l'adresse IP ADNS.

```
1. Connectez-vous au **groupe de ressources AWS**utilisateur et accédez à **EC2 > NETWORK & SECURITY > Elastic IPs**.

1. Cliquez sur**Attribuer une nouvelle adresse**pour créer une adresse IP élastique.

1. Configurez l'adresse IP élastique pour qu'elle pointe vers l'utilisateur qui exécute l'instance NetScaler dans AWS.

1. Configurez une deuxième adresse IP Elastic et redirigez-la vers l'utilisateur qui exécute l'instance NetScaler.
```

1. Équilibreur de charge élastique

   a) Connectez-vous au **groupe de ressources AWS**utilisateur et accédez à**EC2 > LOAD BALANCING > Load Balancers**.

b) Cliquez sur **Créer un équilibreur de charge** pour configurer un équilibreur de charge classique.

Les équilibreurs de charge élastiques permettent aux utilisateurs d'équilibrer la charge de leurs instances Amazon Linux principales tout en étant en mesure d'équilibrer la charge d'autres instances qui sont lancées en fonction de la demande.

Configuration des services basés sur les noms de domaine d'équilibrage de charge global des serveurs

Pour les configurations de gestion du trafic, voir Configurer le service basé sur le domaine NetScaler GSLB.

Types de déploiement

Déploiement de trois cartes réseau

- Déploiements typiques
  - StyleBook GSLB
  - Avec ADM
  - Avec GSLB (Route53 avec enregistrement de domaine)
  - Licences - Pooled/Marketplace
- Cas d'utilisation
  - Les déploiements à trois cartes réseau sont utilisés pour obtenir une véritable isolation des données et du trafic de gestion.
  - Les déploiements à trois cartes réseau améliorent également l'évolutivité et les performances de l'ADC.
  - Les déploiements à trois cartes réseau sont utilisés dans les applications réseau où le débit est généralement de 1 Gbit/s ou plus et où un déploiement à trois cartes réseau est recommandé.

Déploiement du CFT

Les clients peuvent déployer à l'aide de modèles CloudFormation s'ils personnalisent leurs déploiements ou s'ils automatisent leurs déploiements.

Étapes de déploiement

Voici les étapes de déploiement :

1. Déploiement de trois cartes réseau pour GSLB
2. Système de licences
3. options de déploiement

Déploiement de trois cartes réseau pour GSLB L'instance NetScaler VPX est disponible en tant qu'Amazon Machine Image (AMI) sur la place de marché AWS, et elle peut être lancée en tant qu'instance Elastic Compute Cloud (EC2) au sein d'un AWS VPC. Le type d'instance EC2 minimum autorisé en tant qu'AMI prise en charge sur NetScaler VPX est m4.large. L'instance NetScaler VPX AMI nécessite au moins 2 processeurs virtuels et 2 Go de mémoire. Une instance EC2 lancée dans un VPC AWS peut également fournir les multiples interfaces, plusieurs adresses IP par interface et les adresses IP publiques et privées nécessaires à la configuration VPX. Chaque instance VPX nécessite au moins trois sous-réseaux IP :

- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le back-end (SNIP)

NetScaler recommande trois interfaces réseau pour une installation VPX standard sur AWS.

AWS rend actuellement la fonctionnalité multi-IP disponible uniquement pour les instances exécutées au sein d'un VPC AWS. Une instance VPX dans un VPC peut être utilisée pour équilibrer la charge des serveurs exécutant dans des instances EC2. Un Amazon VPC permet aux utilisateurs de créer et de contrôler un environnement réseau virtuel, y compris leur propre plage d'adresses IP, des sous-réseaux, des tables de routage et des passerelles réseau.

> **Remarque :**
>
> Par défaut, les utilisateurs peuvent créer jusqu'à 5 instances VPC par région AWS pour chaque compte AWS. Les utilisateurs peuvent demander des limites de VPC plus élevées en soumettant le formulaire de demande d'Amazon ici : Amazon VPC Request.

Système de licences Une instance NetScaler VPX sur AWS nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur AWS :

- Gratuit (illimité)
- Horaire
- Annuel
- Apportez votre propre licence

- Essai gratuit (toutes les offres d'abonnement NetScaler VPX-AWS pendant 21 jours gratuits sur AWS Marketplace).

Options de déploiement Les utilisateurs peuvent déployer une instance autonome NetScaler VPX sur AWS. Pour plus d'informations, consultez Déployer une instance autonome NetScaler VPXsur AWS

Équilibrage de charge global du serveur NetScaler pour les déploiements hybrides et multicloud

La solution GSLB (Global Server Load Balancing) hybride et multicloud de NetScaler permet aux utilisateurs de répartir le trafic applicatif entre plusieurs centres de données dans des clouds hybrides, des clouds multiples et des déploiements sur site. La solution GSLB hybride et multicloud NetScaler aide les utilisateurs à gérer leur configuration d'équilibrage de charge dans des environnements hybrides ou multicloud sans modifier la configuration existante. De plus, si les utilisateurs disposent d'une configuration sur site, ils peuvent tester certains de leurs services dans le cloud à l'aide de la solution GSLB hybride et multicloud NetScaler avant de migrer complètement vers le cloud. Par exemple, les utilisateurs ne peuvent acheminer qu'un faible pourcentage de leur trafic vers le cloud et gérer la majeure partie du trafic sur site. La solution GSLB hybride et multicloud NetScaler permet également aux utilisateurs de gérer et de surveiller les instances NetScaler sur différents sites géographiques à partir d'une console unifiée unique.

Une architecture hybride et multicloud peut également améliorer les performances globales de l'entreprise en évitant le « verrouillage du fournisseur » et en utilisant une infrastructure différente pour répondre aux besoins des partenaires utilisateurs et des clients. Avec l'architecture multi-cloud, les utilisateurs peuvent mieux gérer leurs coûts d'infrastructure car ils doivent désormais payer uniquement pour ce qu'ils utilisent. Les utilisateurs peuvent également améliorer la mise à l'échelle de leurs applications puisqu'ils utilisent désormais l'infrastructure à la demande. Il permet également de passer rapidement d'un cloud à un autre pour profiter des meilleures offres de chaque fournisseur.

Les nœuds NetScaler GSLB gèrent la résolution du nom DNS. N'importe lequel de ces nœuds GSLB peut recevoir des requêtes DNS depuis n'importe quel emplacement client. Le nœud GSLB qui reçoit la demande DNS renvoie l'adresse IP du serveur virtuel d'équilibrage de charge sélectionnée par la méthode d'équilibrage de charge configurée. Les métriques (métriques de site, de réseau et de persistance) sont échangées entre les nœuds GSLB à l'aide du protocole d'échange de métriques (MEP), qui est un protocole propriétaire NetScaler. Pour plus d'informations sur le protocole MEP, voirConfigurer le protocole d'échange de métriques.

Le moniteur configuré dans le nœud GSLB surveille l'état de santé du serveur virtuel d'équilibrage de charge dans le même centre de données. Dans une topologie parent-enfant, les métriques entre les nœuds GSLB et NetScaler sont échangées à l'aide de MEP. Toutefois, la configuration de sondes de

surveillance entre un nœud GSLB et un nœud NetScaler LB est facultative dans une topologie parent-enfant.

L'agent NetScaler permet la communication entre NetScaler ADM et les instances gérées dans le centre de données utilisateur. Pour plus d'informations sur les agents NetScaler et comment les installer, consultezMise en route.

> **Remarque :**
>
> Le présent document formule les hypothèses suivantes :
>
> - Si les utilisateurs disposent déjà d'une configuration d'équilibrage de charge, celle-ci est opérationnelle.
> - Une adresse SNIP ou une adresse IP de site GSLB est configurée sur chacun des nœuds NetScaler GSLB. Cette adresse IP est utilisée comme adresse IP source du centre de données lors de l'échange de mesures avec d'autres centres de données.
> - Un service ADNS ou ADNS-TCP est configuré sur chacune des instances NetScaler GSLB pour recevoir le trafic DNS.
> - Les groupes de pare-feu et de sécurité requis sont configurés dans les fournisseurs de services cloud.

Configuration des groupes de sécurité

Les utilisateurs doivent configurer la configuration de pare-feu/groupes de sécurité requise dans les fournisseurs de services cloud. Pour plus d'informations sur les fonctionnalités de sécurité AWS, consultez AWS/Documentation/Amazon VPC/User Guide/Security.

De plus, sur le nœud GSLB, les utilisateurs doivent ouvrir le port 53 pour l'adresse IP du service ADNS/serveur DNS et le port 3009 pour l'adresse IP du site GSLB pour l'échange de trafic MEP. Sur le nœud d'équilibrage de charge, les utilisateurs doivent ouvrir les ports appropriés pour recevoir le trafic de l'application. Par exemple, les utilisateurs doivent ouvrir le port 80 pour recevoir le trafic HTTP et ouvrir le port 443 pour recevoir le trafic HTTPS. Ouvrez le port 443 pour la communication NITRO entre l'agent NetScaler et NetScaler ADM.

Pour la méthode GSLB à temps aller-retour dynamique, les utilisateurs doivent ouvrir le port 53 pour autoriser les sondes UDP et TCP en fonction du type de sonde LDNS configuré. Les sondes UDP ou TCP sont initiées à l'aide de l'un des SNIP. Ce paramètre doit donc être effectué pour les groupes de sécurité liés au sous-réseau côté serveur.

Fonctionnalités de la solution GSLB hybride et multicloud NetScaler

Certaines fonctionnalités de la solution GSLB hybride et multicloud NetScaler sont décrites dans cette section.

Compatibilité avec d'autres solutions d'équilibrage de charge

La solution GSLB hybride et multicloud NetScaler prend en charge diverses solutions d'équilibrage de charge telles que l'équilibreur de charge NetScaler, NGINX, HAProxy et d'autres équilibreurs de charge tiers.

> **Remarque :**
>
> les solutions d'équilibrage de charge autres que NetScaler ne sont prises en charge que si des méthodes GSLB basées sur la proximité et non métriques sont utilisées et si la topologie parent-enfant n'est pas configurée.

Méthodes GSLB

La solution GSLB hybride et multicloud NetScaler prend en charge les méthodes GSLB suivantes.

- Méthodes GSLB basées sur des métriques. Les méthodes GSLB basées sur des métriques collectent des métriques à partir des autres nœuds NetScaler via le protocole d'échange de métriques.
  - Connexion minimale : la demande du client est acheminée vers l'équilibreur de charge qui a le moins de connexions actives.
  - Bande passante minimale : la demande du client est acheminée vers l'équilibreur de charge qui dessert actuellement le moins de trafic.
  - Moins de paquets : La demande du client est acheminée vers l'équilibreur de charge qui a reçu le moins de paquets au cours des 14 dernières secondes.
- Méthodes GSLB non métriques
  - Round Robin : La demande du client est acheminée vers l'adresse IP de l'équilibreur de charge qui figure en haut de la liste des équilibreurs de charge. Cet équilibreur de charge se déplace ensuite vers le bas de la liste.
  - Hachage IP source : Cette méthode utilise la valeur hachée de l'adresse IP du client pour sélectionner un équilibreur de charge.
- Méthodes GSLB basées sur la proximité

- Proximité statique : La demande du client est acheminée vers l'équilibreur de charge le plus proche de l'adresse IP du client.
- Round-Trip Time (RTT) : Cette méthode utilise la valeur RTT (le délai de connexion entre le serveur DNS local du client et le centre de données) pour sélectionner l'adresse IP de l'équilibreur de charge le plus performant.

Pour plus d'informations sur les méthodes d'équilibrage de charge, voir load balancingAlgorithms.

Topologies GSLB

La solution GSLB hybride et multicloud NetScaler prend en charge la topologie active-passive et la topologie parent-enfant.

- Topologie active-passive : assure la reprise après sinistre et garantit la disponibilité continue des applications en les protégeant contre les points de défaillance. Si le centre de données principal tombe en panne, le centre de données passif devient opérationnel. Pour plus d'informations sur la topologie active-passive GSLB, voir Configurer GSLB pour la reprise après sinistre.
- Topologie parent-enfant –Peut être utilisée si les clients utilisent les méthodes GSLB basées sur des métriques pour configurer les nœuds GSLB et d'équilibrage de charge et si les nœuds d'équilibrage de charge sont déployés sur une autre instance NetScaler. Dans une topologie parent-enfant, le nœud LB (site enfant) doit être une appliance NetScaler car l'échange de métriques entre le site parent et le site enfant se fait via le protocole d'échange de métriques (MEP).

Pour plus d'informations sur la topologie parent-enfant, consultez Déploiement de la topologie parent-enfant à l'aide du protocole MEP.

Prise en charge IPv6

La solution GSLB hybride et multicloud NetScaler prend également en charge IPv6.

Surveillance

La solution GSLB hybride et multicloud NetScaler prend en charge les moniteurs intégrés avec une option permettant d'activer la connexion sécurisée. Toutefois, si les configurations LB et GSLB se trouvent sur la même instance NetScaler ou si la topologie parent-enfant est utilisée, la configuration des moniteurs est facultative.

Persistance

La solution GSLB hybride et multicloud NetScaler prend en charge les éléments suivants :

- Sessions de persistance basées sur IP source, de sorte que plusieurs demandes provenant du même client sont dirigées vers le même service si elles arrivent dans la fenêtre de délai d'expiration configurée. Si la valeur de délai expire avant que le client n'envoie une autre demande, la session est abandonnée et l'algorithme d'équilibrage de charge configuré est utilisé pour sélectionner un nouveau serveur pour la prochaine demande du client.
- Persistance de débordement afin que le serveur virtuel de sauvegarde continue à traiter les demandes qu'il reçoit, même après que la charge sur le principal tombe en dessous du seuil. Pour plus d'informations, voir Configurer Spillover.
- Persistance du site de telle sorte que le nœud GSLB sélectionne un centre de données pour traiter une demande client et transfère l'adresse IP du centre de données sélectionné pour toutes les requêtes DNS suivantes. Si la persistance configurée s'applique à un site en panne, le nœud GSLB utilise une méthode GSLB pour sélectionner un nouveau site, et le nouveau site devient persistant pour les demandes suivantes du client.

Configuration à l'aide de NetScaler ADM StyleBooks

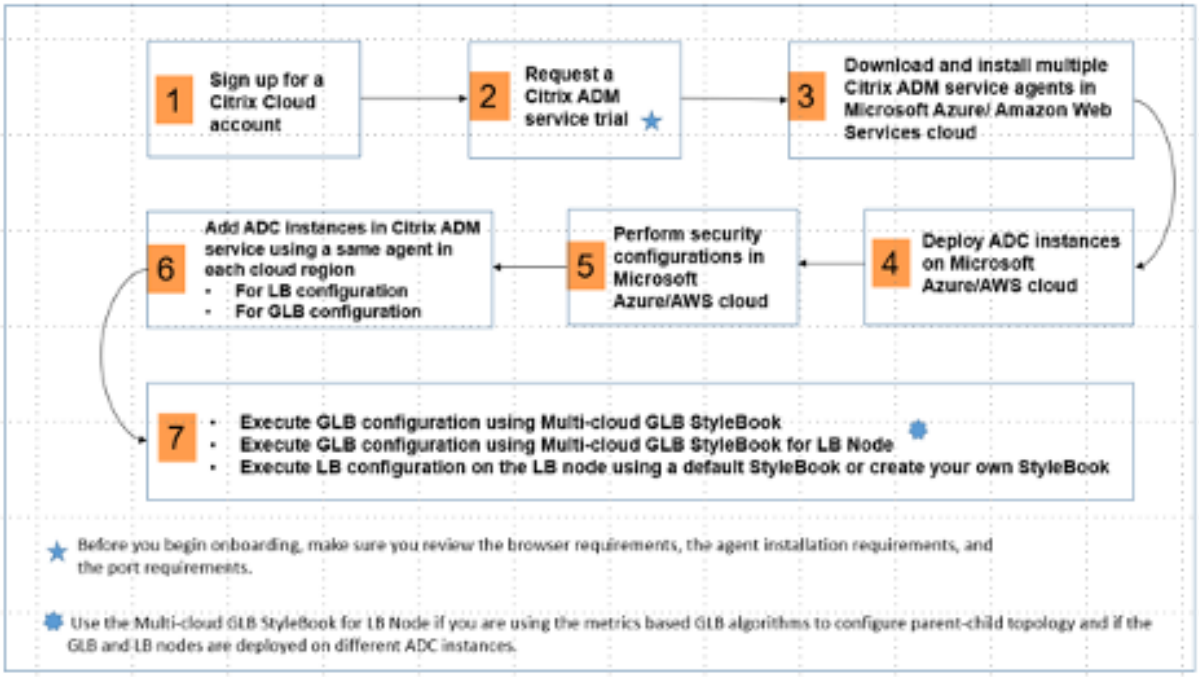
Les clients peuvent utiliser le StyleBook GSLB multicloud par défaut sur NetScaler ADM pour configurer des instances NetScaler avec des configurations GSLB hybrides et multicloud.

Les clients peuvent utiliser le StyleBook GSLB multicloud par défaut pour le StyleBook de nœud d'équilibrage de charge afin de configurer les nœuds d'équilibrage de charge NetScaler qui sont les sites enfants dans une topologie parent-enfant qui gèrent le trafic d'application. Utilisez ce StyleBook uniquement si les utilisateurs souhaitent configurer des nœuds d'équilibrage de charge dans une topologie parent-enfant. Toutefois, chaque nœud LB doit être configuré séparément à l'aide de ce StyleBook.

Flux de travail de configuration de la solution GSLB hybride et multicloud NetScaler

Les clients peuvent utiliser le StyleBook GSLB multicloud fourni sur NetScaler ADM pour configurer des instances NetScaler avec des configurations GSLB hybrides et multicloud.

Le schéma suivant montre le flux de travail pour configurer une solution GSLB hybride et multicloud NetScaler. Les étapes du diagramme de workflow sont expliquées plus en détail après le diagramme.



Effectuez les tâches suivantes en tant qu'administrateur de cloud :

1. Ouvrez un compte NetScaler Cloud.

   Pour commencer à utiliser NetScaler ADM, créez un compte d'entreprise NetScaler Cloud ou rejoignez un compte existant créé par une personne de votre entreprise.

2. Une fois que les utilisateurs se sont connectés à NetScaler Cloud,**cliquez** sur Gérer dans la vignette**NetScaler Application Delivery Management pour configurer le service**ADM pour la première fois.

3. Téléchargez et installez plusieurs agents de service NetScaler ADM.

   Les utilisateurs doivent installer et configurer l'agent de service NetScaler ADM dans leur environnement réseau pour permettre la communication entre NetScaler ADM et les instances gérées dans leur centre de données ou leur cloud. Installez un agent dans chaque région afin qu'il puisse configurer les configurations LB et GSLB sur les instances gérées. Les configurations LB et GSLB peuvent partager un seul agent. Pour plus d'informations sur les trois tâches ci-dessus, consultez Mise en route.

4. Déployez des équilibreurs de charge sur les centres de données cloud et locaux Microsoft AWS.

   En fonction du type d'équilibreurs de charge que les utilisateurs déploient sur le cloud et sur site, provisionnez-les en conséquence. Par exemple, les utilisateurs peuvent provisionner des instances NetScaler VPX dans un cloud privé virtuel Amazon Web Services (AWS) et dans des centres de données sur site. Configurez les instances NetScaler pour qu'elles fonctionnent comme des nœuds LB ou GSLB en mode autonome, en créant les machines virtuelles et en configurant

d'autres ressources. Pour plus d'informations sur le déploiement d'instances NetScaler VPX, consultez les documents suivants :

- NetScaler VPX sur AWS.
- Configurez une instance autonome NetScaler VPX.

5. Effectuer des configurations de sécurité.

   Configurez des groupes de sécurité réseau et des listes ACL réseau dans ARM et dans AWS afin de contrôler le trafic entrant et sortant pour les instances utilisateur et les sous-réseaux.

6. Ajoutez des instances NetScaler dans NetScaler ADM.

   Les instances NetScaler sont des dispositifs réseau ou des dispositifs virtuels que les utilisateurs souhaitent découvrir, gérer et surveiller à partir de NetScaler ADM. Pour gérer et surveiller ces instances, les utilisateurs doivent les ajouter au service et enregistrer les instances LB (si les utilisateurs utilisent NetScaler pour LB) et GSLB. Pour plus d'informations sur la façon d'ajouter des instances NetScaler dans NetScaler ADM, voirMise en route

7. Implémentez les configurations GSLB et LB à l'aide des StyleBooks NetScaler ADM par défaut.

   - Utilisez le StyleBook GSLB multicloud pour exécuter la configuration GSLB sur les instances GSLB NetScaler sélectionnées.
   - Implémentez la configuration d'équilibrage de charge. (Les utilisateurs peuvent ignorer cette étape s'ils disposent déjà de configurations LB sur les instances gérées.) Les utilisateurs peuvent configurer des équilibreurs de charge sur les instances NetScaler de deux manières :
   - Configurez manuellement les instances pour l'équilibrage de charge des applications. Pour plus d'informations sur la configuration manuelle des instances, consultez Configurer l'équilibrage de charge de base.
   - Utilisez StyleBooks. Les utilisateurs peuvent utiliser l'un des StyleBooks NetScaler ADM (StyleBook d'équilibrage de charge HTTP/SSL ou StyleBook d'équilibrage de charge HTTP/SSL (avec moniteurs)) pour créer la configuration de l'équilibreur de charge sur l'instance NetScaler sélectionnée. Les utilisateurs peuvent également créer leurs propres StyleBooks. Pour plus d'informations sur StyleBooks, voir StyleBooks.

8. Utilisez le StyleBook GSLB multicloud pour LB Node pour configurer la topologie parent-enfant GSLB dans l'un des cas suivants :

   - Si les utilisateurs utilisent les algorithmes GSLB basés sur des métriques (moins de paquets, moins de connexions, moins de bande passante) pour configurer les nœuds GSLB et d'équilibrage de charge et si les nœuds d'équilibrage de charge sont déployés sur une autre instance NetScaler.
   - Si la persistance du site est requise.

Utilisation de StyleBooks pour configurer GSLB sur les nœuds d'équilibrage de charge NetScaler

Les clients peuvent utiliser le**Multi-cloud GSLB StyleBook pour le nœud LB**s'ils utilisent les algorithmes GSLB basés sur des métriques (moins de paquets, moins de connexions, moins de bande passante) pour configurer les nœuds GSLB et d'équilibrage de charge et si les nœuds d'équilibrage de charge sont déployés sur une autre instance NetScaler.

Les utilisateurs peuvent également utiliser ce StyleBook pour configurer davantage de sites enfants pour un site parent existant. Ce StyleBook configure un site enfant à la fois. Créez donc autant de configurations (packs de configuration) à partir de ce StyleBook qu'il y a de sites enfants. Le StyleBook applique la configuration GSLB sur les sites enfants. Les utilisateurs peuvent configurer un maximum de 1 024 sites enfants.

> **Remarque :**
>
> Utilisez le StyleBook multicloud GSLB pour configurer les sites parents.

Ce StyleBook formule les hypothèses suivantes :

- Une adresse SNIP ou une adresse IP de site GSLB est configurée.
- Les groupes de pare-feu et de sécurité requis sont configurés dans les fournisseurs de services cloud.

Configuration d'un site enfant dans une topologie parent-enfant à l'aide du StyleBook GSLB multicloud pour le nœud LB

1. Accédez à**Applications > Configuration > Créer un nouveau**.
2. Accédez à **Applications** > **Configuration**, puis cliquez sur**Créer un nouveau**.

   Le StyleBook apparaît sous la forme d'une page d'interface utilisateur sur laquelle les utilisateurs peuvent entrer les valeurs de tous les paramètres définis dans ce StyleBook.

> **Remarque :**
>
> Les termes centre de données et sites sont utilisés de manière interchangeable dans ce document.

1. Définissez les paramètres suivants :

   - **Nom de l'application**. Entrez le nom de l'application GSLB déployée sur les sites GSLB pour lesquels vous souhaitez créer des sites enfants.
   - **Protocole**. Sélectionnez le protocole d'application de l'application déployée dans la zone de liste déroulante.

- **Bilan de santé LB** (facultatif)
- **Type de bilan de santé**. Dans la zone de liste déroulante, sélectionnez le type de sonde utilisée pour vérifier l'état de santé de l'adresse VIP de l'équilibreur de charge qui représente l'application sur un site.
- **Mode sécurisé**. (Facultatif) Sélectionnez **Oui** pour activer ce paramètre si des contrôles de santé basés sur SSL sont requis.
- **Demande HTTP**. (Facultatif) Si les utilisateurs ont sélectionné HTTP comme type de contrôle de santé, entrez la requête HTTP complète utilisée pour sonder l'adresse VIP.
- **Liste des codes de réponse d'état HTTP**. (Facultatif) Si les utilisateurs ont sélectionné HTTP comme type de contrôle de santé, entrez la liste des codes d'état HTTP attendus dans les réponses aux requêtes HTTP lorsque le VIP est sain.

2. Configuration du site parent.
   - Fournissez les détails du site parent (nœud GSLB) sous lequel vous souhaitez créer le site enfant (nœud LB).
     - **Nom du site**. Entrez le nom du site parent.
     - **Adresse IP du site**. Entrez l'adresse IP que le site parent utilise comme adresse IP source lors de l'échange de mesures avec d'autres sites. Cette adresse IP est supposée être déjà configurée sur le nœud GSLB de chaque site.
     - **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site parent qui est utilisée pour échanger des métriques, si l'adresse IP de ce site est NAT'ed.
3. Configuration du site enfant.
   - Fournissez les détails du site enfant.
     - **Nom du site**. Entrez le nom du site.
     - **Adresse IP du site**. Entrez l'adresse IP du site enfant. Ici, utilisez l'adresse IP privée ou le SNIP du nœud NetScaler qui est configuré en tant que site enfant.
     - **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site enfant qui est utilisée pour échanger des métriques, si l'adresse IP de ce site est NAT'ed.
4. Configuration des services GSLB actifs (facultatif)
   - Configurez les services GSLB actifs uniquement si l'adresse IP du serveur virtuel LB n'est pas une adresse IP publique. Cette section permet aux utilisateurs de configurer la liste des services GSLB locaux sur les sites où l'application est déployée.
     - **Adresse IP du service**. Entrez l'adresse IP du serveur virtuel d'équilibrage de charge sur ce site.

- **Adresse IP publique du service**. Si l'adresse IP virtuelle est privée et possède une adresse IP publique qui lui est associée, spécifiez l'adresse IP publique.
- **Port de service**. Entrez le port du service GSLB sur ce site.
- **Nom du site**. Entrez le nom du site sur lequel se trouve le service GSLB.

5. Cliquez sur**Instances cibles** et sélectionnez les instances NetScaler configurées en tant qu'instances GSLB sur chaque site sur lequel déployer la configuration GSLB.
6. Cliquez sur**Créer** pour créer la configuration LB sur l'instance NetScaler sélectionnée (nœud LB). Les utilisateurs peuvent également cliquer sur**Exécution à sec**pour vérifier les objets qui seraient créés dans les instances cibles. La configuration StyleBook que les utilisateurs ont créée apparaît dans la liste des configurations sur la page Configurations. Les utilisateurs peuvent examiner, mettre à jour ou supprimer cette configuration à l'aide de l'interface graphique utilisateur NetScaler ADM.

Déploiement du modèle CloudFormation

NetScaler VPX est disponible en tant qu'Amazon Machine Images (AMI) sur AWS Marketplace. Avant d'utiliser un modèle CloudFormation pour provisionner un NetScaler VPX dans AWS, l'utilisateur AWS doit accepter les conditions et s'abonner au produit AWS Marketplace. Cette étape est requise pour chaque édition de NetScaler VPX disponible sur Marketplace.

Chaque modèle du référentiel CloudFormation possède une documentation colocalisée décrivant l'utilisation et l'architecture du modèle. Les modèles tentent de codifier l'architecture de déploiement recommandée de NetScaler VPX, ou de présenter NetScaler à l'utilisateur ou de démontrer une fonctionnalité, une édition ou une option particulière. Les utilisateurs peuvent réutiliser, modifier ou améliorer les modèles en fonction de leurs besoins spécifiques en matière de production et de test. La plupart des modèles nécessitent des autorisations EC2 complètes en plus des autorisations pour créer des rôles IAM.

Les modèles CloudFormation contiennent des ID AMI spécifiques à une version particulière de NetScaler VPX (par exemple, version 12.0-56.20) et à une édition (par exemple, NetScaler VPX Platinum Edition - 10 Mbps) OU NetScaler BYOL. Pour utiliser une version ou une édition différente de NetScaler VPX avec un modèle CloudFormation, l'utilisateur doit modifier le modèle et remplacer les ID AMI.

Les derniers AMI-ID NetScaler AWS-se trouvent ici : NetScaler AWS CloudFormation Master.

Déploiement de trois cartes réseau CFT

Ce modèle déploie un VPC, avec 3 sous-réseaux (gestion, client, serveur) pour 2 zones de disponibilité. Il déploie une passerelle Internet, avec une route par défaut sur les sous-réseaux publics. Ce modèle

crée également une paire HA dans les zones de disponibilité avec deux instances de NetScaler : 3 ENI associées à 3 sous-réseaux VPC (gestion, client, serveur) sur le réseau principal et 3 ENI associées à 3 sous-réseaux VPC (gestion, client, serveur) sur le réseau secondaire. Tous les noms de ressources créés par ce CFT sont préfixés par un TagName du nom de la pile.

La sortie du modèle CloudFormation inclut :

- PrimaryCitrixADCManagementURL : URL HTTPS vers l'interface graphique de gestion du VPX principal (utilise un certificat auto-signé)
- PrimaryCitrixADCManagementUrl2 : URL HTTP vers l'interface graphique de gestion du VPX principal
- PrimaryCitrixADCINstanceId : ID d'instance de l'instance VPX primaire nouvellement créée
- PrimaryCitrixADCPublicVIP : adresse IP Elastic de l'instance VPX principale associée au VIP
- PrimaryCitrixADCPrivateNSIP - IP privée (IP NS) utilisée pour la gestion du VPX primaire
- PrimaryCitrixADCPublicNSIP - IP publique (IP NS) utilisée pour la gestion du VPX primaire
- PrimaryCitrixADCPrivateVIP : adresse IP privée de l'instance VPX principale associée au VIP
- PrimaryCitrixADCSnip : adresse IP privée de l'instance VPX principale associée au SNIP
- SecondaryCitrixADCManagementURL - URL HTTPS vers l'interface graphique de gestion du VPX secondaire (utilise un certificat auto-signé)
- SecondaryCitrixADCManagementUrl2 - URL HTTP vers l'interface graphique de gestion du VPX secondaire
- SecondaryCitrixADCINstanceId : ID d'instance de l'instance VPX secondaire nouvellement créée
- SecondaryCitrixADCPrivateNSIP - IP privée (IP NS) utilisée pour la gestion du VPX secondaire
- SecondaryCitrixADCPublicNSIP - IP publique (IP NS) utilisée pour la gestion du VPX secondaire
- SecondaryCitrixADCPrivateVIP : adresse IP privée de l'instance VPX secondaire associée au VIP
- SecondaryCitrixADCSnip : adresse IP privée de l'instance VPX secondaire associée au SNIP
- SecurityGroup : identifiant du groupe de sécurité auquel appartient le VPX

Lors de la saisie du CFT, le paramètre * par rapport à n'importe quel paramètre du CFT implique qu'il s'agit d'un champ obligatoire. Par exemple, `VPC ID*` est un champ obligatoire.

Les conditions préalables suivantes doivent être remplies. Le modèle CloudFormation nécessite des autorisations suffisantes pour créer des rôles IAM, au-delà des privilèges complets EC2 normaux. L'utilisateur de ce modèle doit également accepter les conditions et s'abonner au produit AWS Marketplace avant d'utiliser ce modèle CloudFormation.

Les éléments suivants doivent également être présents :

- Paire de clés
- 3 EIP non alloués
- Gestion principale
- VIP client
- Gestion secondaire

Pour plus d'informations sur le provisionnement des instances NetScaler VPX sur AWS, les utilisateurs peuvent visiter : Provisionnement des instances NetScaler VPX sur AWS.

Pour plus d'informations sur la configuration de GSLB à l'aide de StyleBooks, visitez Utilisation de StyleBooks pour configurer GSLB

Reprise après sinistre (DR)

La catastrophe est une perturbation soudaine des fonctions commerciales causée par des catastrophes naturelles ou des événements d'origine humaine. Les catastrophes affectent les opérations des centres de données, après quoi les ressources et les données perdues sur le site du sinistre doivent être entièrement reconstruites et restaurées. La perte de données ou les temps d'arrêt dans le datacenter sont critiques et réduit la continuité de l'activité.

L'un des défis auxquels les clients sont confrontés aujourd'hui est de décider où placer leur site de reprise après sinistre. Les entreprises recherchent la cohérence et les performances indépendamment des défaillances de l'infrastructure sous-jacente ou du réseau.

Pour déployer GSLB pour la récupération après sinistre, voir Déployer une instance autonome NetScaler VPX sur AWS

Autres ressources

NetScaler ADM GSLB pour les déploiements hybrides et multi-cloud.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

October 17, 2024

> **Remarque :**
>
> La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de NetScaler version 12.0 57.19.

Après avoir créé une instance NetScaler VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour qu'elle utilise les interfaces réseau SR-IOV à l'aide de l'interface de ligne de commande AWS.

Dans tous les modèles NetScaler VPX, à l'exception des éditions NetScaler VPX AWS Marketplace 3G et 5G, le SR-IOV n'est pas activé dans la configuration par défaut d'une interface réseau.

Avant de démarrer la configuration, lisez les rubriques suivantes :

- Conditions préalables
- Limitations et directives d'utilisation

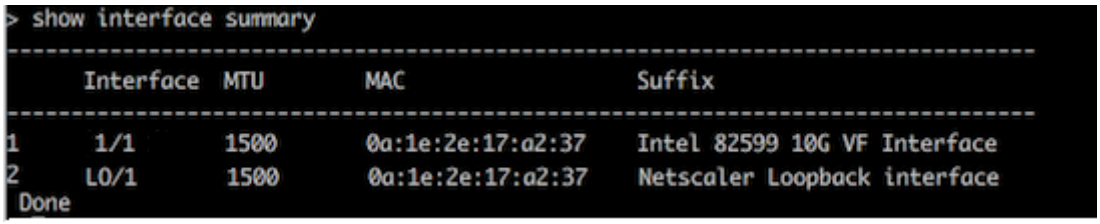
Cette section comprend les rubriques suivantes :

- Modifier le type d'interface en SR-IOV
- Configurer SR-IOV sur une configuration haute disponibilité

Modifier le type d'interface en SR-IOV

Vous pouvez exécuter la commande show interface summary pour vérifier la configuration par défaut d'une interface réseau.

Exemple 1 : La capture d'écran CLI suivante montre la configuration d'une interface réseau dans laquelle le SR-IOV est activé par défaut sur les éditions 3G et 5G de NetScaler VPX AWS Marketplace.



Exemple 2 : La capture d'écran CLI suivante montre la configuration par défaut d'une interface réseau où SR-IOV n'est pas activée.


```
 Done
> sh int s
-----------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-----------------------------------------------------------------------------
1     1/1        1500       12:fc:04:c5:d0:12  NetScaler Virtual Interface
2     LO/1       1500       12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Pour plus d'informations sur la modification du type d'interface en SR-IOV, voir http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Pour changer le type d'interface en SR-IOV

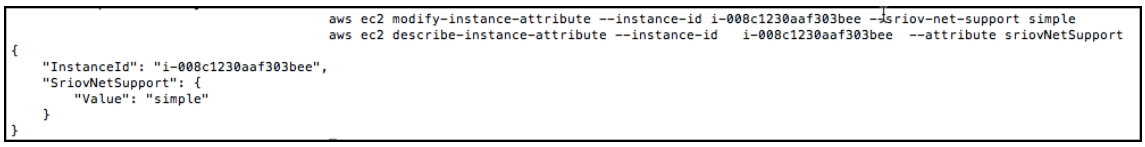
1. Arrêtez l'instance NetScaler VPX exécutée sur AWS.
2. Pour activer SR-IOV sur l'interface réseau, tapez la commande suivante dans l'interface de ligne de commande AWS.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \\&#060;instance\\_id\\&#062; --sriov-net-support simple
   ```

3. Pour vérifier si SR-IOV a été activé, tapez la commande suivante dans l'interface de ligne de commande AWS.

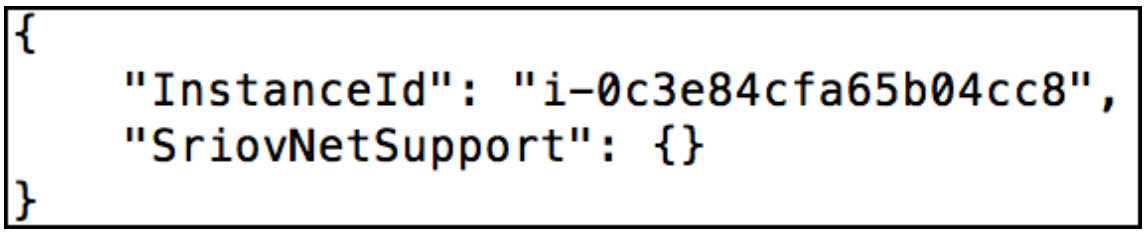
   ```
   $ aws ec2 describe-instance-attribute --instance-id \\&#060;instance\\_id\\&#062; --attribute sriovNetSupport
   ```

   Exemple 3 : Le type d'interface réseau est passé à SR-IOV, à l'aide de l'interface de ligne de commande AWS.

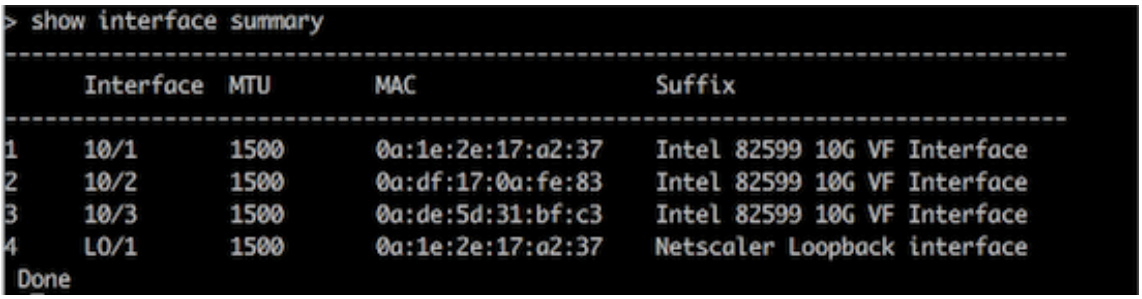
   Si SR-IOV n'est pas activé, la valeur de SriovNetSupport est absente.

   Exemple 4 : Dans l'exemple suivant, la prise en charge SR-IOV n'est pas activée.

4. Mettez l'instance VPX sous tension. Pour voir le statut modifié de l'interface réseau, tapez « show interface summary » dans l'interface de ligne de commande.

   Exemple 5 : La capture d'écran suivante montre les interfaces réseau avec SR-IOV activée. Les interfaces 10/1, 10/2, 10/3 sont activées SR-IOV.



```
> show interface summary
---------------------------------------------------------------------------
      Interface  MTU       MAC                Suffix
---------------------------------------------------------------------------
1     10/1       1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2     10/2       1500      0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3     10/3       1500      0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4     LO/1       1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Ces étapes complètent la procédure de configuration des instances VPX pour utiliser les interfaces réseau SR-IOV.

Configurer SR-IOV sur une configuration haute disponibilité

La haute disponibilité est prise en charge par les interfaces SR-IOV à partir de NetScaler version 12.0 build 57.19.

Si la configuration haute disponibilité a été déployée manuellement ou à l'aide du modèle Citrix CloudFormation pour NetScaler version 12.0 56.20 et versions antérieures, le rôle IAM associé à la configuration haute disponibilité doit disposer des privilèges suivants :

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- SNS : *
- sqs:*
- IAM : Simuler la politique principale
- Je suis : obtenir un rôle

Par défaut, le modèle Citrix CloudFormation pour NetScaler version 12.0 57.19 ajoute automatiquement les privilèges requis au rôle IAM.

> **Remarque :**
>
> Une configuration haute disponibilité avec interfaces SR-IOV prend environ 100 secondes d'arrêt.

Ressources connexes :

Pour plus d'informations sur les rôles IAM, consultez la documentation AWS.

Configurer une instance NetScaler VPX pour utiliser la mise en réseau améliorée avec AWS ENA

October 17, 2024

Après avoir créé une instance NetScaler VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour utiliser la mise en réseau améliorée avec AWS Elastic Network Adapter (ENA), à l'aide de l'interface de ligne de commande AWS.

Associé à AWS ENA, la mise en réseau améliorée offre une bande passante plus élevée, des performances PPS (paquet par seconde) plus élevées et des latences inter-instances toujours plus faibles.

Avant de démarrer la configuration, lisez les rubriques suivantes :

- Conditions préalables
- Limitations et directives d'utilisation

Les configurations HA suivantes sont prises en charge pour les instances compatibles ENA :

- Les adresses IP privées peuvent être déplacées au sein de la même zone de disponibilité.
- Les adresses IP élastiques peuvent être déplacées entre les zones de disponibilité.

Mettre à niveau une instance NetScaler VPX sur AWS

October 17, 2024

Vous pouvez mettre à niveau le type d'instance EC2, le débit, l'édition logicielle et le logiciel système d'un NetScaler VPX s'exécutant sur AWS. Pour certains types de mises à niveau, Citrix recommande d'utiliser la méthode de configuration haute disponibilité pour minimiser les temps d'arrêt.

> **Remarque :**
>
> - La version 10.1.e-124.1308.e ou ultérieure du logiciel NetScaler pour une AMI NetScaler VPX

(y compris la licence utilitaire et la licence client) ne prend pas en charge les familles d'instances M1 et M2.
- En raison des modifications apportées à la prise en charge des instances VPX, la rétrogradation de 10.1.e-124 ou une version ultérieure vers 10.1.123.x ou une version antérieure n'est pas prise en charge.
- La plupart des mises à niveau ne nécessitent pas le lancement d'une nouvelle AMI et la mise à niveau peut être effectuée sur l'instance NetScaler AMI actuelle. Si vous souhaitez effectuer une mise à niveau vers une nouvelle instance NetScaler AMI, utilisez la méthode de configuration haute disponibilité.

Modifier le type d'instance EC2 d'une instance NetScaler VPX sur AWS

Si vos instances NetScaler VPX exécutent la version 10.1.e-124.1308.e ou ultérieure, vous pouvez modifier le type d'instance EC2 depuis la console AWS comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 à partir de la console AWS.
3. Démarrez l'instance.

Vous pouvez également utiliser la procédure ci-dessus pour modifier le type d'instance EC2 pour une version antérieure à 10.1.e-124.1308.e, sauf si vous souhaitez modifier le type d'instance en M3. Dans ce cas, vous devez d'abord suivre la procédure de mise à niveau standard de NetScaler, à l'adresse, pour mettre à niveau le logiciel NetScaler vers la version 10.1.e-124 ou une version ultérieure, puis suivre les étapes ci-dessus.

Mettre à niveau le débit ou l'édition logicielle d'une instance NetScaler VPX sur AWS

Pour mettre à niveau l'édition logicielle (par exemple, pour passer de l'édition Standard à Premium) ou le débit (par exemple, pour passer de 200 Mbps à 1000 Mbps), la méthode dépend de la licence de l'instance.

Utilisation d'une licence client (Bring-Your-Own-License)

Si vous utilisez une licence client, vous pouvez acheter et télécharger la nouvelle licence à partir du site Web Citrix, puis installer la licence sur l'instance VPX. Pour plus d'informations sur le téléchargement et l'installation d'une licence à partir du site Web Citrix, consultez le Guide des licences VPX.

Utilisation d'une licence d'utilitaire (licence d'utilitaire avec frais horaires)

AWS ne prend pas en charge les mises à niveau directes pour les instances payantes. Pour mettre à niveau l'édition logicielle ou le débit d'une instance NetScaler VPX payante, lancez une nouvelle AMI avec la licence et la capacité souhaitées et migrez l'ancienne configuration d'instance vers la nouvelle instance. Cela peut être réalisé en utilisant une configuration de haute disponibilité NetScaler comme décrit dans la sous-section [Mise à niveau vers une nouvelle instance NetScaler AMI en utilisant une configuration de haute disponibilité NetScaler] (#upgrade-to-a-new-citrix-adc-ami-instance-by-using-a-citrix-adc-high-availability-configuration) de cette page.

Mettre à niveau le logiciel système d'une instance NetScaler VPX sur AWS

Si vous devez mettre à niveau une instance VPX exécutant la version 10.1.e-124.1308.e ou une version ultérieure, suivez la procédure de mise à niveau standard de NetScaler dans la section Mettre à niveau et rétrograder une appliance NetScaler.

Si vous devez mettre à niveau une instance VPX exécutant une version antérieure à 10.1.e-124.1308.e vers 10.1.e-124.1308.e ou une version ultérieure, mettez d'abord à niveau le logiciel système, puis modifiez le type d'instance en M3 comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 à partir de la console AWS.
3. Démarrez l'instance.

Effectuez une mise à niveau vers une nouvelle instance NetScaler AMI à l'aide d'une configuration NetScaler haute disponibilité

Pour utiliser la méthode de haute disponibilité de mise à niveau vers une nouvelle instance NetScaler AMI, effectuez les tâches suivantes :

- Créez une nouvelle instance avec le type d'instance EC2 souhaité, l'édition logicielle, le débit ou la version logicielle à partir du marché AWS.
- Configurez la haute disponibilité entre l'ancienne instance (à mettre à niveau) et la nouvelle instance. Une fois la haute disponibilité configurée entre l'ancienne et la nouvelle instance, la configuration de l'ancienne instance est synchronisée avec la nouvelle instance.
- Forcer un basculement HA de l'ancienne instance vers la nouvelle instance. Par conséquent, la nouvelle instance devient principale et commence à recevoir du trafic.
- Arrêtez et reconfigurez ou supprimez l'ancienne instance d'AWS.

Prérequis et points à considérer

- Assurez-vous de comprendre comment fonctionne la haute disponibilité entre deux instances NetScaler VPX sur AWS. Pour plus d'informations sur la configuration de haute disponibilité entre deux instances NetScaler VPX sur AWS, consultez Déployer une paire haute disponibilité sur AWS.
- Vous devez créer la nouvelle instance dans la même zone de disponibilité que l'ancienne instance, avec exactement le même groupe de sécurité et sous-réseau.
- La configuration de haute disponibilité nécessite des clés d'accès et secrètes associées au compte AWS Identity and Access Management (IAM) de l'utilisateur pour les deux instances. Si les informations de clé correctes ne sont pas utilisées lors de la création d'instances VPX, la configuration HA échoue. Pour plus d'informations sur la création d'un compte IAM pour une instance VPX, consultez Prérequis.
  - Vous devez utiliser la console EC2 pour créer la nouvelle instance. Vous ne pouvez pas utiliser le lancement d'AWS 1-Click, car il n'accepte pas les clés d'accès et les clés secrètes comme entrée.
  - La nouvelle instance ne doit avoir qu'une seule interface ENI.

Pour mettre à niveau une instance NetScaler VPX à l'aide d'une configuration haute disponibilité, procédez comme suit :

1. Configurez la haute disponibilité entre l'ancienne et la nouvelle instance. Pour configurer la haute disponibilité entre deux instances NetScaler VPX, à l'invite de commande de chaque instance, tapez :

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Exemple :

   À l'invite de commandes de l'ancienne instance, tapez :

   ```
   1  add ha node 30 192.0.2.30
   2  Done
   ```

   À l'invite de commande de la nouvelle instance, tapez :

   ```
   1  add ha node 10 192.0.2.10
   2  Done
   ```

   Notez les points suivants :

   - Dans la configuration HA, l'ancienne instance est le nœud principal et la nouvelle instance est le nœud secondaire.

- L'adresse IP NSIP n'est pas copiée de l'ancienne instance vers la nouvelle instance. Par conséquent, après la mise à niveau, votre nouvelle instance a une adresse IP de gestion différente de la précédente.
- Le mot de passe du `nsroot` compte de la nouvelle instance est défini sur celui de l'ancienne instance après la synchronisation HA.

Pour plus d'informations sur la configuration de haute disponibilité entre deux instances NetScaler VPX sur AWS, consultez Déployer une paire haute disponibilité sur AWS.

2. Forcer un basculement HA. Pour forcer un basculement dans une configuration haute disponibilité, à l'invite de commandes de l'une ou l'autre des instances, tapez :

```
force HA failover
```

À la suite d'un basculement forcé, les ENI de l'ancienne instance sont migrés vers la nouvelle instance et le trafic circule à travers la nouvelle instance (le nouveau nœud principal). L'ancienne instance (le nouveau nœud secondaire) redémarre.

Si le message d'avertissement suivant s'affiche, tapez N pour annuler l'opération :

```
[WARNING]:Force Failover may cause configuration loss, peer
   health not optimum.   Reason(s):
HA version mismatch
HA heartbeats not seen on some interfaces
Please confirm whether you want force-failover (Y/N)?
```

Le message d'avertissement s'affiche car le logiciel système des deux instances VPX n'est pas compatible HA. Par conséquent, la configuration de l'ancienne instance ne peut pas être synchronisée automatiquement avec la nouvelle instance lors d'un basculement forcé.

Voici la solution de contournement pour ce problème :

a) À l'invite du shell NetScaler de l'ancienne instance, saisissez la commande suivante pour créer une sauvegarde du fichier de configuration (`ns.conf`) :

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Supprimez la ligne suivante du fichier de configuration de sauvegarde (`ns.conf.bkp`):

- `set ns config -IPAddress <IP> -netmask <MASK>`

Par exemple, `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Copiez le fichier de configuration de sauvegarde de l'ancienne instance (`ns.conf.bkp`) dans le répertoire `/nsconfig` de la nouvelle instance.

d) À l'invite du shell NetScaler de la nouvelle instance, saisissez la commande suivante pour charger le fichier de configuration de l'ancienne instance (`ns.conf.bkp`) sur la nouvelle instance :

- batch -f /nsconfig/ns.conf.bkp

e) Enregistrez la configuration sur la nouvelle instance.

- save conifg

f) À l'invite de commandes de l'un des nœuds, tapez la commande suivante pour forcer un basculement, puis tapez Y pour le message d'avertissement pour confirmer l'opération de basculement forcé :

- force ha failover

Exemple :

```
1           > force ha failover
2
3   WARNING]:Force Failover may cause configuration loss, peer
       health not optimum.
4           Reason(s):
5           HA version mismatch
6           HA heartbeats not seen on some interfaces
7           Please confirm whether you want force-failover (Y/N)?
               Y
```

3. Supprimez la configuration HA afin que les deux instances ne soient plus dans une configuration HA. Supprimez d'abord la configuration HA du nœud secondaire, puis supprimez la configuration HA du nœud principal.

   Pour supprimer une configuration HA entre deux instances NetScaler VPX, à l'invite de commande de chaque instance, tapez :

   ```
   1        > remove ha node \<nodeID\>
   2        >  save config
   ```

   Pour plus d'informations sur la configuration de haute disponibilité entre deux instances VPX sur AWS, consultez Déployer une paire haute disponibilité sur AWS.

   Exemple :

À l'invite de commandes de l'ancienne instance (nouveau nœud secondaire), tapez :

```
1           > remove ha node 30
2             Done
3           > save config
4             Done
```

À l'invite de commande de la nouvelle instance (nouveau nœud principal), tapez :

```
1           > remove ha node 10
2             Done
3           > save config
4             Done
```

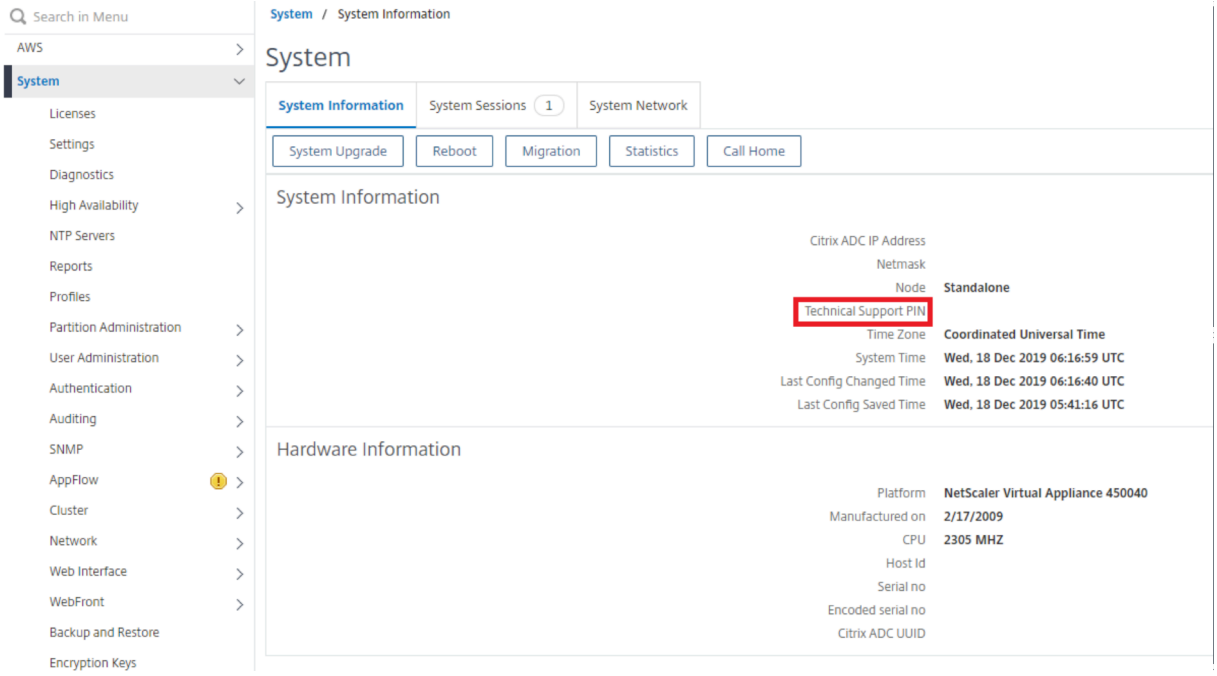

Dépannage d'une instance VPX sur AWS

October 17, 2024

Amazon ne fournit pas d'accès console à une instance NetScaler VPX. Pour résoudre les problèmes, vous devez utiliser l'interface graphique AWS pour afficher le journal d'activité. Vous ne pouvez déboguer que si le réseau est connecté. Pour afficher le journal système d'une instance, cliquez avec le bouton droit sur l'instance et sélectionnez Journal système.

NetScaler fournit un support pour les instances NetScaler VPX sous licence AWS Marketplace (licence utilitaire avec frais horaires) sur AWS. Pour déposer une demande d'assistance, recherchez votre numéro de compte AWS et votre code PIN d'assistance, puis appelez le support NetScaler. Vous serez également invité à indiquer votre nom et votre adresse e-mail. Pour trouver le code PIN d'assistance, connectez-vous à l'interface graphique VPX et accédez à la page Système.

Voici un exemple de page système montrant le code PIN de support.



Questions fréquentes sur AWS

October 17, 2024

- **Une instance NetScaler VPX prend-elle en charge les volumes chiffrés dans AWS ?**

Le chiffrement et le déchiffrement se produisent au niveau de l'hyperviseur, et donc il fonctionne parfaitement avec n'importe quelle instance. Pour plus d'informations sur les volumes chiffrés, consultez le document AWS suivant :

https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Quel est le meilleur moyen de provisionner une instance NetScaler VPX sur AWS ?**

  Vous pouvez mettre en service une instance NetScaler VPX sur AWS de l'une des manières suivantes :

  - Modèle AWS CloudFormation (CFT) dans AWS marketplace
  - NetScaler ADM
  - Démarrages rapides AWS
  - CFT Citrix AWS dans GitHub
  - Scripts Citrix Terraform dans GitHub
  - Playbooks Citrix Ansible dans GitHub
  - Workflow de lancement AWS EC2

  Vous pouvez choisir l'une des options répertoriées en fonction de l'outil d'automatisation que vous utilisez.

  Pour plus de détails sur les options, voir NetScaler VPX sur AWS.

- **Comment mettre à niveau une instance NetScaler VPX dans AWS ?**

  Pour mettre à niveau l'instance NetScaler VPX dans AWS, vous pouvez mettre à niveau le logiciel système ou effectuer une mise à niveau vers une nouvelle image machine Amazon (AMI) NetScaler VPX en suivant la procédure décrite dans Mettre à niveau une instance NetScaler VPX sur AWS.

  La méthode recommandée pour mettre à niveau une instance NetScaler VPX consiste à utiliser le service ADM en suivant la procédure décrite dans Utiliser des tâches pourmettre à niveau les instances NetScaler.

- **Quel est le délai de basculement en mode HA pour NetScaler VPX dans AWS ?**

  - Le basculement en mode HA de NetScaler VPX dans la zone de disponibilité AWS prend environ 3 secondes.
  - Le basculement en mode HA de NetScaler VPX entre les zones de disponibilité AWS prend environ 5 secondes.

- **Quel niveau de support est fourni aux clients abonnés à NetScaler VPX Marketplace qui fournissent le code PIN du support technique ?**

  Par défaut, le service « Sélectionner pour le logiciel » est fourni aux clients qui fournissent le code PIN du support technique.

- **Dans Haute disponibilité sur différentes zones à l'aide du déploiement Elastic IP , devons-nous créer plusieurs IPSets pour chaque application ?**

  Oui. S'il existe plusieurs applications avec plusieurs VIP mappés à plusieurs adresses IP, plusieurs IPsets sont nécessaires. Par conséquent, pendant le basculement HA, tous les mappages VIP principaux des EIP sont remplacés par des VIP secondaires (nouveaux VIP principaux).

- **Pourquoi le mode INC est-il activé en haute disponibilité dans différents déploiements de zones ?**

  Les paires HA dans toutes les zones de disponibilité se trouvent dans différents réseaux. Pour la synchronisation HA, la configuration réseau ne doit pas être synchronisée. Ceci est obtenu en activant le mode INC sur la paire HA.

- **Le nœud HA d'une zone de disponibilité peut-il communiquer avec les serveurs principaux d'une autre zone de disponibilité, à condition que ces zones de disponibilité se trouvent dans le même VPC ?**

  Oui, les sous-réseaux situés dans différentes zones de disponibilité du même VPC sont accessibles en ajoutant un itinéraire supplémentaire pointant vers le sous-réseau du serveur principal via SNIP. Par exemple, si le sous-réseau SNIP d'ADC dans AZ1 est 192.168.3.0/24 et que le sous-réseau du serveur principal dans AZ2 est 192.168.6.0/24, une route doit être ajoutée dans l'appliance NetScaler présente dans AZ1 sous la forme 192.168.6.0 255.255.255.0 192.168.3.1.

- **Les déploiements Haute disponibilité sur différentes zones à l'aide d'Elastic IP et Haute disponibilité sur différentes zones à l'aide d'IP privée peuvent-ils fonctionner ensemble ?**

  Oui, les deux configurations peuvent être appliquées sur la même paire HA.

- **Dans le déploiement Haute disponibilité sur différentes zones à l'aide d'une adresse IP privée , s'il existe plusieurs sous-réseaux avec plusieurs tables de routage dans un VPC, comment un nœud secondaire dans une paire HA connaît-il la table de routage à vérifier lors du basculement HA ?**

  Le nœud secondaire connaît les cartes réseau principales et effectue des recherches dans toutes les tables de routage d'un VPC.

- **Quelle est la taille de la `/var` partition lorsque vous utilisez l'image par défaut pour VPX sur AWS ? Comment augmenter l'espace disque ?**

  La taille du disque racine est limitée à 20 Go pour garder l'image disque petite.

  Si vous souhaitez augmenter l'espace `/var/core/` ou l'espace de `/var/crash/` répertoire, attachez un disque supplémentaire. Pour augmenter la `/var` taille, vous devez actuellement attacher un disque supplémentaire et créer un lien symbolique vers `/var`, après avoir copié le contenu critique sur le nouveau disque.

- **Combien de moteurs de paquets sont activés et alloués aux processeurs virtuels ?**

  Les moteurs de paquets (PE) sont limités par le nombre de processeurs virtuels sous licence. Les démons NetScaler ne sont liés à aucun processeur virtuel en particulier et peuvent s'exécuter sur n'importe quel processeur virtuel autre que PE. Selon AWS, le C5.9XLarge est une instance de 36 processeurs virtuels avec 72 Go de mémoire. Avec les licences groupées, l'instance NetScaler VPX se déploie avec le nombre maximum de PE. Dans ce cas, 19 PE fonctionnent sur les cœurs 1 à 19. Toutefois, les processus de gestion ADC s'exécutent à partir des processeurs 20 à 31.

- **Comment décider de la bonne instance AWS pour ADC ?**

  1. Comprenez votre cas d'utilisation et vos exigences telles que le débit, le PPS, les exigences SSL et la taille moyenne des paquets.
  2. Choisissez l'offre ADC et les licences appropriées qui répondent à vos exigences, telles que les offres de bande passante VPX ou les licences basées sur des processeurs virtuels.
  3. En fonction de l'offre choisie, décidez de l'instance AWS.

  Exemple

  Une licence de 5 Gbit/s permet 5 moteurs de paquets de données. Par conséquent, l'exigence du processeur virtuel est de 6 (5+1 pour la gestion). Mais l'instance 6 vCPU n'est pas disponible. Un processeur virtuel 8 est donc suffisant pour atteindre ce débit à condition que vous choisissiez un réseau qui prend en charge la bande passante de 5 Gbps. Par exemple, vous devez choisir m5.2xlarge pour une licence de bande passante de 5 Gbps afin d'activer l'allocation PE maximale pour une licence de 5 Gbps. Mais si vous utilisez une licence vCPU qui n'est pas limitée par le débit, vous pouvez obtenir un débit de 5 Gbit/s à l'aide de l'instance m5.xlarge elle-même.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **Le déploiement de trois sous-réseaux NIC et trois sous-réseaux est-il obligatoire pour ADC dans AWS ?**

  Three NICs-three subnets est le déploiement recommandé, où chacun est destiné à la gestion, au réseau client et serveur. Ce déploiement offre une meilleure isolation du trafic et des performances VPX. Deux sous-réseaux NIC, deux et un sous-réseau NIC-One sont les autres options disponibles. Il n'est pas recommandé d'avoir plusieurs cartes réseau partageant un sous-réseau dans AWS, comme dans le cas d'un déploiement de deux cartes réseau sur un sous-réseau. Ce scénario peut entraîner des problèmes de réseau tels qu'un routage asymétrique.

Pour plus d'informations, voir Meilleures pratiques de configuration des interfaces réseau dans AWS.

- **Pourquoi un pilote ENA sur AWS indique-t-il toujours une vitesse de liaison de 1 Gbit/s (1/1), quelles que soient les capacités réseau de l'instance ?**

  La vitesse signalée d'un adaptateur réseau élastique AWS (ENA) est souvent affichée sous la forme de 1 Gbit/s (1/1), quel que soit le type d'instance sélectionné. Cela est dû au fait que la vitesse indiquée ne reflète pas directement les performances réelles du réseau. Contrairement aux interfaces réseau traditionnelles, les vitesses ENA peuvent évoluer de manière dynamique en fonction des exigences et de la charge de travail de l'instance. Les véritables performances du réseau sont principalement déterminées par le type et la taille de l'instance. Par conséquent, le débit réel du réseau peut varier considérablement en fonction du type d'instance spécifique et de la charge réseau actuelle.

Déployer une instance NetScaler VPX sur Microsoft Azure

October 17, 2024

Lorsque vous déployez une instance NetScaler VPX sur Microsoft Azure Resource Manager (ARM), vous pouvez utiliser les deux ensembles de fonctionnalités suivants pour répondre aux besoins de votre entreprise :

- Fonctionnalités de cloud computing Azure
- Fonctionnalités d'équilibrage de charge et de gestion du trafic de NetScaler

Vous pouvez déployer des instances NetScaler VPX sur ARM en tant qu'instances autonomes ou en tant que paires haute disponibilité en modes de veille active.

Vous pouvez déployer une instance NetScaler VPX sur Microsoft Azure de deux manières :

- via la Place de marché Azure. L'appliance virtuelle NetScaler VPX est disponible sous forme d'image sur Microsoft Azure Marketplace.
- À l'aide du modèle json NetScaler Azure Resource Manager (ARM) disponible sur GitHub. Pour plus d'informations, consultez le référentiel GitHub pour les modèles de solutions NetScaler.

La pile Microsoft Azure est une plateforme intégrée de matériel et de logiciels qui fournit les services de cloud public Microsoft Azure dans un centre de données local pour permettre aux organisations de construire des clouds hybrides. Vous pouvez désormais déployer les instances NetScaler VPX sur la pile Microsoft Azure.

> **Remarque :**
>
> Azure restreint l'accès au trafic provenant de l'extérieur d'Azure et le bloque. Pour fournir un accès, activez le service ou le port en ajoutant une règle entrante dans le groupe de sécurité réseau attaché à la carte réseau de la machine virtuelle à laquelle une adresse IP publique est attachée. Pour plus d'informations, consultez la documentation Azure sur les règles NAT entrantes.

Conditions préalables

Vous devez disposer de certaines connaissances préalables avant de déployer une instance NetScaler VPX sur Azure.

- Familiarité avec la terminologie Azure et les détails du réseau. Pour plus d'informations, voir Terminologie Azure.
- Connaissance d'une appliance NetScaler. Pour des informations détaillées sur l'appliance NetScaler, voir NetScaler
- Connaissance du réseau NetScaler. Consultez la rubrique Mise en réseau.

Fonctionnement d'une instance NetScaler VPX sur Azure

Dans un déploiement sur site, une instance NetScaler VPX nécessite au moins trois adresses IP :

- Adresse IP de gestion, appelée adresse NSIP
- Adresse IP du sous-réseau (SNIP) pour communiquer avec la batterie de serveurs
- Adresse IP du serveur virtuel (VIP) pour accepter les demandes des clients

Pour plus d'informations, consultez Architecture réseau pour les instances NetScaler VPX sur Microsoft Azure.

> **Remarque :**
>
> L'instance NetScaler VPX prend en charge les processeurs Intel et AMD. Les appliances virtuelles VPX peuvent être déployées sur n'importe quel type d'instance doté d'au moins deux cœurs virtualisés et de plus de 2 Go de mémoire. Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

Dans un déploiement Azure, vous pouvez provisionner une instance NetScaler VPX sur Azure de trois manières :

- Architecture multi-NIC Multi-IP
- Architecture multi-IP de carte réseau unique
- Carte d'interface réseau unique, IP unique

En fonction de vos besoins, vous pouvez utiliser n'importe lequel de ces types d'architecture pris en charge.

Architecture multi-NIC Multi-IP

Dans ce type de déploiement, plusieurs interfaces réseau (NIC) peuvent être attachées à une instance VPX. Toute carte réseau peut avoir une ou plusieurs configurations IP (adresses IP publiques et privées statiques ou dynamiques) qui lui sont attribuées.

Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau
- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

> **Remarque :**
>
> Pour éviter les déplacements du MAC et les désactivations d'interface dans les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de l'instance NetScaler VPX et de lier l'adresse IP principale de la carte réseau dans Azure. Pour plus d'informations, consultez l'article CTX224626 .

Architecture multi-IP de carte réseau unique

Dans ce type de déploiement, une interface réseau (NIC) associée à plusieurs configurations IP - adresses IP publiques et privées statiques ou dynamiques qui lui sont attribuées. Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX
- Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX à l'aide des commandes PowerShell

Carte d'interface réseau unique, IP unique

Dans ce type de déploiement, une interface réseau (NIC) associée à une seule adresse IP, qui est utilisée pour exécuter les fonctions NSIP, SNIP et VIP.

Pour plus d'informations, voir Configurer une instance autonome NetScaler VPX.

> **Remarque :**
>
> Le mode IP unique est disponible uniquement dans les déploiements Azure. Ce mode n'est pas disponible pour une instance NetScaler VPX dans vos locaux, sur AWS ou dans le cadre d'autres

> types de déploiement.

Licence NetScaler VPX

Une instance NetScaler VPX sur Azure nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur Azure.

- **Licences basées sur un abonnement** : les appliances NetScaler VPX sont disponibles sous forme d'instances payantes sur Azure Marketplace. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure.

  > **Remarque :**
  >
  > Pour les instances de licence par abonnement, la facturation de votre abonnement s'applique tout au long de la période de licence pour un modèle de licence particulier. En raison des restrictions liées au cloud, Azure ne prend pas en charge la modification ou la suppression du modèle de licence applicable à votre abonnement. Pour modifier ou supprimer une licence d'abonnement, supprimez la machine virtuelle ADC existante et recréez une nouvelle machine virtuelle ADC avec la licence requise.

  NetScaler fournit un support technique pour les instances de licence par abonnement. Pour déposer un dossier de support, consultez Support pour NetScaler sur Azure —Licence d'abonnement avec prix horaire.

- **Apportez votre propre licence (BYOL)** : Si vous apportez votre propre licence (BYOL), consultez le guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :

  - Utilisez le portail de licences du site Web NetScaler pour générer une licence valide.
  - Télécharger la licence sur l'instance.

  > **Remarque La**
  >
  > Dans un environnement Azure Stack, **BYOL** est la seule option de licence disponible.

- **Licences NetScaler VPX Check-In/Check-Out : pour plus d'informations, voir Licences NetScaler VPX Check-In/Check-Out**.

  À partir de la version 12.0 56.20 de NetScaler, NetScaler VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur NetScaler VPX Express, consultez la section « Licence NetScaler VPX Express » dans la vue d'ensemble des licences NetScaler.

Performances VPX et types d'instances Azure recommandés

Pour obtenir les performances VPX souhaitées, les types d'instances Azure suivants sont recommandés.

Performances VPX	Types d'instances Azure		
	Carte réseau VPX 1/2 cartes réseau	Carte réseau VPX 3	VPX jusqu'à 8 cartes réseau
Jusqu'à 200 Mbits/s	Standard_D2_v4 Standard_DS3_v2 Standard_DS4_v2 Norme_DS3_v2 Norme_DS4_v2		
Jusqu'à 1 Gbit/s	Standard_D4_v4 Standard_DS3_v2 Standard_DS4_v2 Norme_DS3_v2 Norme_DS4_v2		
Jusqu'à 5 Gbit/s	Standard_D8s_v5 Standard_D8_v5 Standard_DS3_v2 Standard_DS4_v2 Standard_D8s_v5 Standard_D8_v5 Standard_DS4_v2 Norme_DS4_v2		
Jusqu'à 10 Gbit/s	Norme_D2_v5 Norme_D8_v5 Norme_D16_v5		

Points à noter

- Pour obtenir des performances optimales sur les instances NetScaler VPX avec un débit de 1 Gbit/s et 5 Gbit/s, vous devez activer la mise en réseau accélérée Azure.

  Pour plus d'informations sur la configuration de la mise en réseau accélérée, consultez Configurer une instance NetScaler VPX pour utiliser la mise en réseau accélérée Azure.
- Quelle que soit la licence horaire basée sur un abonnement achetée sur Azure Marketplace, dans de rares cas, l'instance NetScaler VPX déployée sur Azure peut proposer une licence NetScaler par défaut. Cela est dû à des problèmes avec Azure Instance Metadata Service (IMDS).
- Redémarrez à chaud avant de modifier la configuration de l'instance NetScaler VPX pour activer la licence NetScaler VPX appropriée.

Support IPv6 pour l'instance NetScaler VPX dans Azure

À partir de la version 13.1-21.x, l'instance autonome NetScaler VPX prend en charge les adresses IPv6 dans Azure. Vous pouvez configurer les adresses IPv6 en tant qu'adresses VIP et SNIP sur l'instance autonome NetScaler VPX dans le cloud Azure.

Pour plus d'informations sur la façon d'activer IPv6 sur Azure, consultez la documentation Azure suivante :

- Qu'est-ce que IPv6 pour le réseau virtuel Azure ?
- Ajouter IPv6 à une application IPv4 dans le réseau virtuel Azure - Azure CLI
- Types d'adresses

Pour plus d'informations sur la manière dont l'appliance NetScaler prend en charge IPv6, consultez Protocole Internet version 6.

Limites d'IPv6 :

- Les déploiements IPv6 dans NetScaler ne prennent actuellement pas en charge le dimensionnement automatique du backend Azure.
- IPv6 n'est pas pris en charge pour le déploiement de NetScaler VPX HA.

Limitations

L'exécution de la solution d'équilibrage de charge NetScaler VPX sur ARM impose les limites suivantes :

- L'architecture Azure ne prend pas en charge les fonctionnalités NetScaler suivantes :
  - ARP gratuit (GARP)
  - Mode L2
  - VLAN balisé
  - Routage dynamique
  - MAC virtuel
  - USIP
  - Mise en cluster

  > **Remarque :**
  >
  > Grâce à la fonctionnalité Autoscale de NetScaler Application Delivery Management (ADM) (déploiement dans le cloud), les instances ADC prennent en charge le clustering sur toutes les licences. Pour plus d'informations, consultez Mise à l'échelle automatique de NetScaler VPX dans Microsoft Azure à l'aide de NetScaler ADM.

- Si vous pensez devoir arrêter et désallouer temporairement la machine virtuelle NetScaler VPX à tout moment, attribuez une adresse IP interne statique lors de la création de la machine virtuelle. Si vous n'attribuez pas d'adresse IP interne statique, Azure peut attribuer à la machine virtuelle une adresse IP différente chaque fois qu'elle redémarre, et la machine virtuelle risque de devenir inaccessible.

- Azure prend en charge un débit VPX jusqu'à 10 Gbit/s. Pour plus d'informations, consultez la fiche technique de NetScaler VPX.
- Lorsque vous utilisez une instance NetScaler VPX avec un débit supérieur à 3 Gbit/s, le débit réel du réseau peut ne pas correspondre au débit spécifié dans la licence de l'instance. Cependant, d'autres fonctionnalités telles que le débit SSL et les transactions SSL par seconde peuvent s'améliorer.
- L'ID de déploiement généré par Azure lors du provisionnement de la machine virtuelle n'est pas visible par l'utilisateur dans ARM. Vous ne pouvez pas utiliser l'ID de déploiement pour déployer l'appliance NetScaler VPX sur ARM.
- L'instance NetScaler VPX prend en charge un débit de 20 Mbit/s et des fonctionnalités d'édition standard lors de son initialisation.
- Les instances NetScaler VPX sur Azure avec la mise en réseau accélérée activée offrent de meilleures performances. La mise en réseau accélérée Azure est prise en charge sur les instances NetScaler VPX à partir de la version 13.0 build 76.x. Pour activer la mise en réseau accélérée sur NetScaler VPX, Citrix vous recommande d'utiliser un type d'instance Azure qui prend en charge la mise en réseau accélérée.
- Pour le déploiement de Citrix Virtual Apps and Desktops, un serveur virtuel VPN sur une instance VPX peut être configuré dans les modes suivants :
  - Mode de base, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur ON. Le mode Basic fonctionne pleinement sur une instance NetScaler VPX sans licence.
  - Mode SmartAccess, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur OFF. Le mode SmartAccess ne fonctionne que pour cinq utilisateurs de session NetScaler AAA sur une instance NetScaler VPX sans licence.

> **Remarque :**
>
> Pour configurer la fonctionnalité SmartControl, vous devez appliquer une licence Premium à l'instance NetScaler VPX.

Terminologie Azure

October 17, 2024

Certains des termes Azure utilisés dans la documentation Azure de NetScaler VPX sont répertoriés ci-dessous.

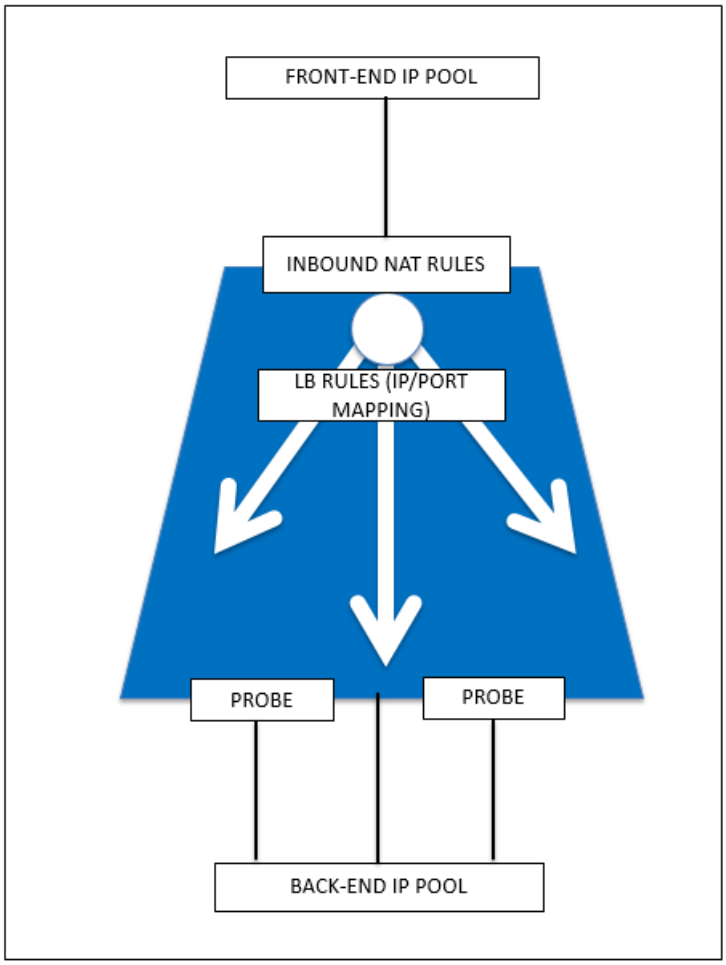
1. Azure Load Balancer —L'équilibreur de charge Azure est une ressource qui distribue le trafic entrant entre les ordinateurs d'un réseau. Le trafic est réparti entre les machines virtuelles définies

dans un ensemble d'équilibreurs de charge. Un équilibreur de charge peut être externe ou connecté à Internet, ou il peut être interne.

2. Azure Resource Manager (ARM) —ARM est le nouveau framework de gestion des services dans Azure. Azure Load Balancer est géré à l'aide d'API et d'outils ARM.
3. Pool d'adresses back-end : il s'agit d'adresses IP associées à la carte réseau (NIC) de la machine virtuelle vers laquelle la charge sera distribuée.
4. BLOB - Binary Large Object —Tout objet binaire tel qu'un fichier ou une image qui peut être stocké dans le stockage Azure.
5. Configuration IP frontale : un équilibreur de charge Azure peut inclure une ou plusieurs adresses IP frontales, également appelées adresses IP virtuelles (VIP). Ces adresses IP servent d'entrée pour le trafic.
6. IP publique au niveau de l'instance (ILPIP) : une ILPIP est une adresse IP publique que vous pouvez attribuer directement à votre machine virtuelle ou à votre instance de rôle, plutôt qu'au service cloud dans lequel réside votre machine virtuelle ou votre instance de rôle. Cela ne remplace pas le VIP (IP virtuelle) attribué à votre service cloud. Il s'agit plutôt d'une adresse IP supplémentaire que vous pouvez utiliser pour vous connecter directement à votre machine virtuelle ou instance de rôle.

   > **Remarque :**
   >
   > Dans le passé, un ILPIP était appelé PIP, ce qui signifie IP publique.

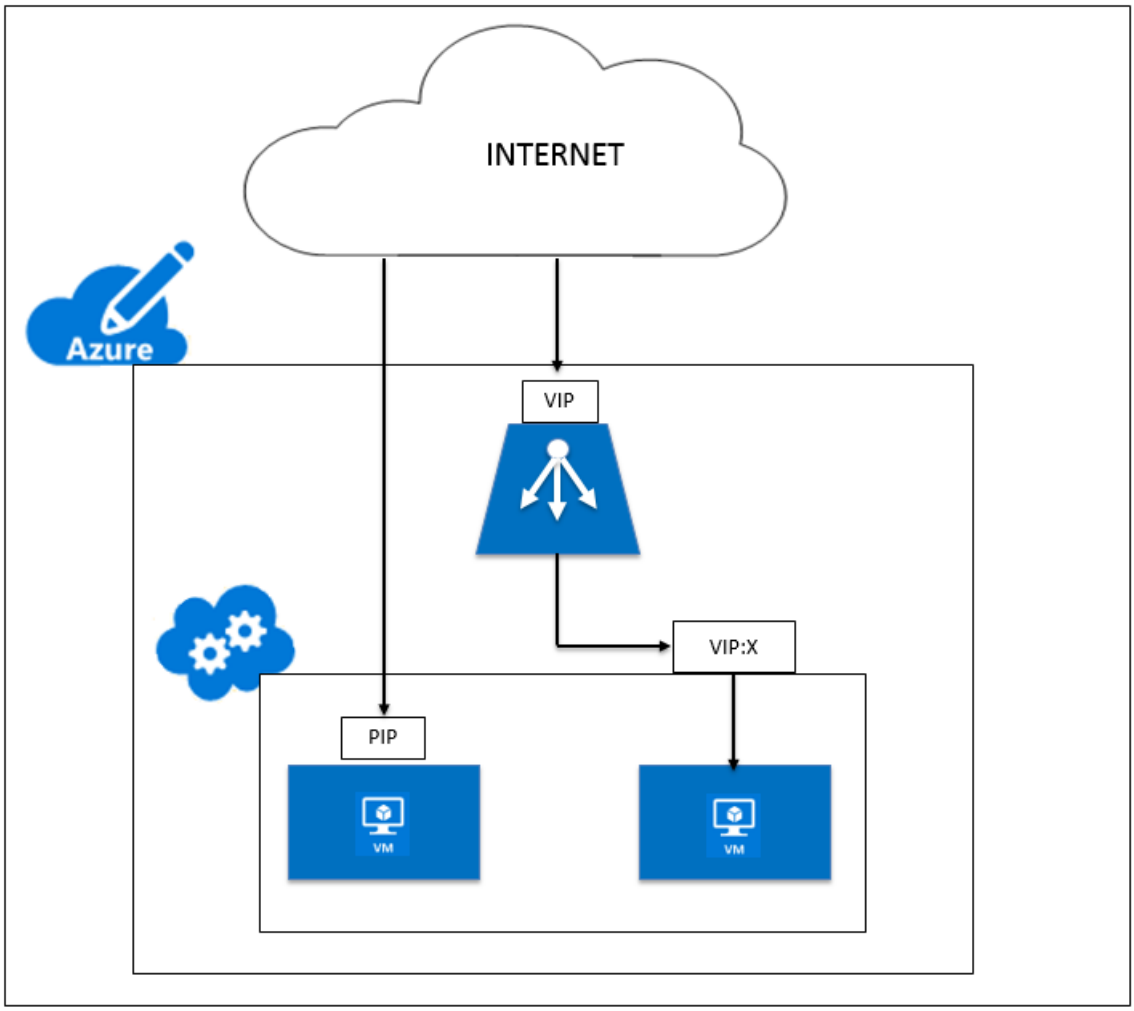
7. Règles NAT entrantes : elles contiennent des règles mappant un port public sur l'équilibreur de charge à un port pour une machine virtuelle spécifique dans le pool d'adresses principal.
8. IP-Config - Il peut être défini comme une paire d'adresses IP (IP publique et IP privée) associée à une carte réseau individuelle. Dans une configuration IP, l'adresse IP publique peut être NULL. Chaque carte réseau peut être associée à plusieurs configurations IP, qui peuvent atteindre 255.
9. Règles d'équilibrage de charge : propriété de règle qui mappe une combinaison IP et port frontaux donnée à un ensemble d'adresses IP et de combinaisons de ports back-end. Avec une définition unique d'une ressource d'équilibrage de charge, vous pouvez définir plusieurs règles d'équilibrage de charge, chaque règle reflétant une combinaison d'une adresse IP et d'un port frontaux et d'une adresse IP principale et d'un port associés aux machines virtuelles.



10. Groupe de sécurité réseau : contient une liste de règles de liste de contrôle d'accès (ACL) qui autorisent ou refusent le trafic réseau vers vos instances de machine virtuelle dans un réseau virtuel. Les NSG peuvent être associés à des sous-réseaux ou à des instances de machine virtuelle individuelles au sein de ce sous-réseau. Lorsqu'un groupe de sécurité réseau est associé à un sous-réseau, les règles ACL s'appliquent à toutes les instances de machines virtuelles de ce sous-réseau. En outre, le trafic vers une machine virtuelle individuelle peut être restreint davantage en associant un groupe de sécurité réseau directement à cette machine virtuelle.
11. Adresses IP privées —Utilisées pour la communication au sein d'un réseau virtuel Azure et de votre réseau local lorsque vous utilisez une Gateway VPN pour étendre votre réseau à Azure. Les adresses IP privées permettent aux ressources Azure de communiquer avec d'autres ressources dans un réseau virtuel ou un réseau local via une Gateway VPN ou un circuit ExpressRoute, sans utiliser d'adresse IP accessible par Internet. Dans le modèle de déploiement Azure Resource Manager, une adresse IP privée est associée aux types de ressources Azure suivants : machines virtuelles, équilibreurs de charge internes (ILB) et passerelles d'application.
12. Sondes : elles contiennent des sondes d'intégrité utilisées pour vérifier la disponibilité des in-

stances de machines virtuelles dans le pool d'adresses principal. Si une machine virtuelle particulière ne répond pas aux sondes d'intégrité pendant un certain temps, elle est retirée du service de trafic. Les sondes vous permettent de suivre l'état de santé des instances virtuelles. En cas d'échec d'une sonde de santé, l'instance virtuelle sera automatiquement retirée de la rotation.

13. Adresses IP publiques (PIP) : PIP est utilisé pour la communication avec Internet, y compris les services publics Azure et est associé aux machines virtuelles, aux équilibreurs de charge connectés à Internet, aux passerelles VPN et aux passerelles d'application.
14. Région - Zone au sein d'une géographie qui ne franchit pas les frontières nationales et qui contient un ou plusieurs centres de données. Les tarifs, les services régionaux et les types d'offres sont exposés au niveau régional. Une région est généralement associée à une autre région, qui peut être distante de plusieurs centaines de kilomètres, pour former une paire régionale. Les paires régionales peuvent être utilisées comme mécanisme pour les scénarios de reprise après sinistre et de haute disponibilité. Aussi appelé généralement lieu.
15. Groupe de ressources : un conteneur du Gestionnaire de ressources contient les ressources associées à une application. Le groupe de ressources peut inclure toutes les ressources d'une application ou uniquement les ressources qui sont regroupées de manière logique
16. Compte de stockage : un compte de stockage Azure vous donne accès au blob, à la file d'attente, à la table et aux services de fichiers Azure dans Azure Storage. Votre compte de stockage fournit l'espace de noms unique pour vos objets de données de stockage Azure.
17. Machine virtuelle : implémentation logicielle d'un ordinateur physique qui exécute un système d'exploitation. Plusieurs machines virtuelles peuvent s'exécuter simultanément sur le même matériel. Dans Azure, les machines virtuelles sont disponibles dans différentes tailles.
18. Réseau virtuel : un réseau virtuel Azure est une représentation de votre propre réseau dans le cloud. Il s'agit d'une isolation logique du cloud Azure dédié à votre abonnement. Vous pouvez contrôler entièrement les blocs d'adresses IP, les paramètres DNS, les politiques de sécurité et les tables de routage au sein de ce réseau. Vous pouvez également segmenter davantage votre réseau virtuel en sous-réseaux et lancer des machines virtuelles Azure IaaS et des services cloud (instances de rôle PaaS). En outre, vous pouvez connecter le réseau virtuel à votre réseau local à l'aide de l'une des options de connectivité disponibles dans Azure. Essentiellement, vous pouvez étendre votre réseau à Azure, avec un contrôle complet sur les blocs d'adresses IP avec l'avantage d'Azure à l'échelle de l'entreprise.



Architecture réseau pour les instances NetScaler VPX sur Microsoft Azure

October 17, 2024

Dans Azure Resource Manager (ARM), une machine virtuelle (VM) NetScaler VPX réside dans un réseau virtuel. Une interface réseau unique peut être créée dans un sous-réseau donné du réseau virtuel et peut être attachée à l'instance VPX. Vous pouvez filtrer le trafic réseau vers et depuis une instance VPX dans un réseau virtuel Azure avec un groupe de sécurité réseau. Un groupe de sécurité réseau contient des règles de sécurité qui autorisent ou refusent le trafic réseau entrant vers ou le trafic réseau sortant à partir d'une instance VPX. Pour plus d'informations, voir Groupes de sécurité.

Le groupe de sécurité réseau filtre les demandes adressées à l'instance NetScaler VPX, qui les envoie aux serveurs. La réponse d'un serveur suit le même chemin à l'envers. Le groupe de sécurité réseau

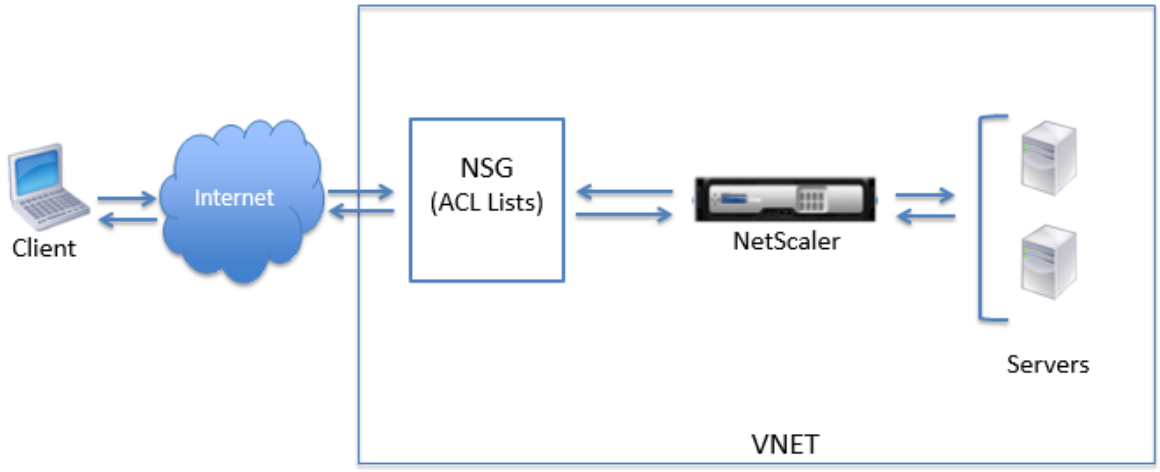
peut être configuré pour filtrer une seule VM VPX ou, avec des sous-réseaux et des réseaux virtuels, peut filtrer le trafic lors du déploiement de plusieurs instances VPX.

La carte réseau contient des détails de configuration réseau tels que le réseau virtuel, les sous-réseaux, l'adresse IP interne et l'adresse IP publique.

Sur ARM, il est bon de connaître les adresses IP suivantes qui sont utilisées pour accéder aux machines virtuelles déployées avec une seule carte réseau et une seule adresse IP :

- L'adresse IP publique (PIP) est l'adresse IP connectée à Internet configurée directement sur la carte réseau virtuelle de la machine virtuelle NetScaler. Cela vous permet d'accéder directement à une machine virtuelle à partir du réseau externe.
- L'adresse IP NetScaler (également appelée NSIP) est l'adresse IP interne configurée sur la machine virtuelle. Il n'est pas routable.
- L'adresse IP virtuelle (VIP) est configurée à l'aide du NSIP et d'un numéro de port. Les clients accèdent aux services NetScaler via l'adresse PIP et lorsque la demande atteint la carte réseau de la machine virtuelle NetScaler VPX ou de l'équilibreur de charge Azure, le VIP est traduit en IP interne (NSIP) et en numéro de port interne.
- L'adresse IP interne est l'adresse IP interne privée de la machine virtuelle à partir du pool d'espace d'adressage du réseau virtuel. Cette adresse IP ne peut pas être atteinte à partir du réseau externe. Cette adresse IP est dynamique par défaut, sauf si vous la définissez sur statique. Le trafic d'Internet est acheminé vers cette adresse selon les règles créées sur le groupe de sécurité réseau. Le groupe de sécurité réseau s'intègre à la carte réseau pour envoyer de manière sélective le bon type de trafic vers le bon port de la carte réseau, qui dépend des services configurés sur la machine virtuelle.

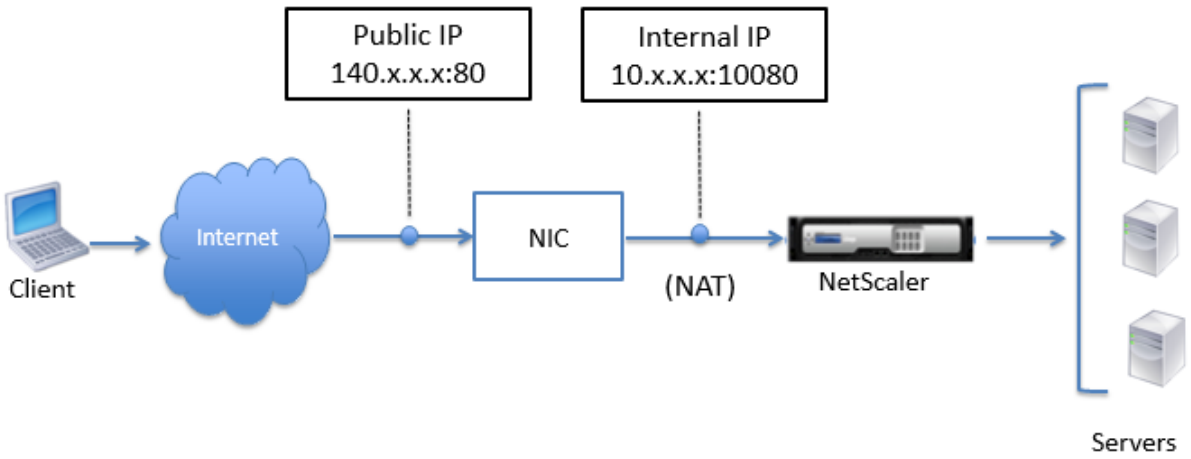
La figure suivante montre comment le trafic circule d'un client vers un serveur via une instance NetScaler VPX provisionnée dans ARM.



Flux de trafic via la traduction d'adresses réseau

Vous pouvez également demander une adresse IP publique (PIP) pour votre instance NetScaler VPX (niveau instance). Si vous utilisez ce PIP direct au niveau de la machine virtuelle, vous n'avez pas besoin de définir des règles entrantes et sortantes pour intercepter le trafic réseau. La demande entrante d'Internet est reçue directement sur la machine virtuelle. Azure effectue la traduction d'adresses réseau (NAT) et transfère le trafic à l'adresse IP interne de l'instance VPX.

La figure suivante montre comment Azure effectue la traduction d'adresses réseau pour mapper l'adresse IP interne NetScaler.



Dans cet exemple, l'adresse IP publique attribuée au groupe de sécurité réseau est 140.x.x.x et l'adresse IP interne est 10.x.x.x. Lorsque les règles entrantes et sortantes sont définies, le port HTTP public 80 est défini comme le port sur lequel les demandes du client sont reçues, et le port privé correspondant, 10080, est défini comme le port sur lequel l'instance NetScaler VPX écoute. La demande du client est reçue sur l'adresse IP publique (140.x.x). Azure effectue la traduction d'adresse réseau pour mapper le PIP à l'adresse IP interne 10.x.x.x sur le port 10080, et transmet la demande du client.

> **Remarque :**
>
> Les machines virtuelles NetScaler VPX en haute disponibilité sont contrôlées par des équilibreurs de charge externes ou internes sur lesquels des règles entrantes sont définies pour contrôler le trafic d'équilibrage de charge. Le trafic externe est d'abord intercepté par ces équilibreurs de charge et le trafic est détourné selon les règles d'équilibrage de charge configurées, qui ont des pools back-end, des règles NAT et des sondes d'intégrité définies sur les équilibreurs de charge.

Instructions relatives à l'utilisation des ports

Vous pouvez configurer davantage de règles entrantes et sortantes dans un groupe de sécurité réseau lors de la création de l'instance NetScaler VPX ou après le provisionnement de la machine virtuelle.

Chaque règle entrante et sortante est associée à un port public et à un port privé.

Avant de configurer les règles de groupe de sécurité réseau, notez les instructions suivantes concernant les numéros de port que vous pouvez utiliser :

1. L'instance NetScaler VPX réserve les ports suivants. Vous ne pouvez pas les définir en tant que ports privés lors de l'utilisation de l'adresse IP publique pour les demandes provenant d'Internet.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Toutefois, si vous souhaitez que les services Internet tels que le VIP utilisent un port standard (par exemple, le port 443), vous devez créer un mappage de ports à l'aide du groupe de sécurité réseau. Le port standard est ensuite mappé à un autre port configuré sur NetScaler pour ce service VIP.

   Par exemple, un service VIP peut s'exécuter sur le port 8443 sur l'instance VPX mais être mappé sur le port public 443. Ainsi, lorsque l'utilisateur accède au port 443 via l'IP publique, la requête est dirigée vers le port privé 8443.
2. L'adresse IP publique ne prend pas en charge les protocoles dans lesquels le mappage de ports est ouvert dynamiquement, tels que FTP passif ou ALG.
3. La haute disponibilité ne fonctionne pas pour le trafic qui utilise une adresse IP publique (PIP) associée à une instance VPX, au lieu d'un PIP configuré sur l'équilibreur de charge Azure.

> **Remarque :**
>
> Dans Azure Resource Manager, une instance NetScaler VPX est associée à deux adresses IP : une adresse IP publique (PIP) et une adresse IP interne. Pendant que le trafic externe se connecte au PIP, l'adresse IP interne ou le NSIP n'est pas routable. Pour configurer VIP dans VPX, utilisez l'adresse IP interne et l'un des ports libres disponibles. N'utilisez pas le PIP pour configurer VIP.

Configurer une instance autonome NetScaler VPX

October 17, 2024

Vous pouvez provisionner une seule instance NetScaler VPX dans le portail Azure Resource Manager (ARM) en mode autonome en créant la machine virtuelle et en configurant d'autres ressources.

Avant de commencer

Assurez-vous que vous disposez de la configuration suivante :

- Un compte d'utilisateur Microsoft Azure
- Accès au Gestionnaire de ressources Microsoft Azure
- Kit de développement logiciel Microsoft Azure
- Microsoft Azure PowerShell

Sur la page Microsoft Azure Portal, connectez-vous au portail Azure Resource Manager en fournissant votre nom d'utilisateur et votre mot de passe.

> **Remarque :**
>
> Dans le portail ARM, le fait de cliquer sur une option dans un volet ouvre un nouveau volet sur la droite. Naviguez d'un volet à l'autre pour configurer votre appareil.

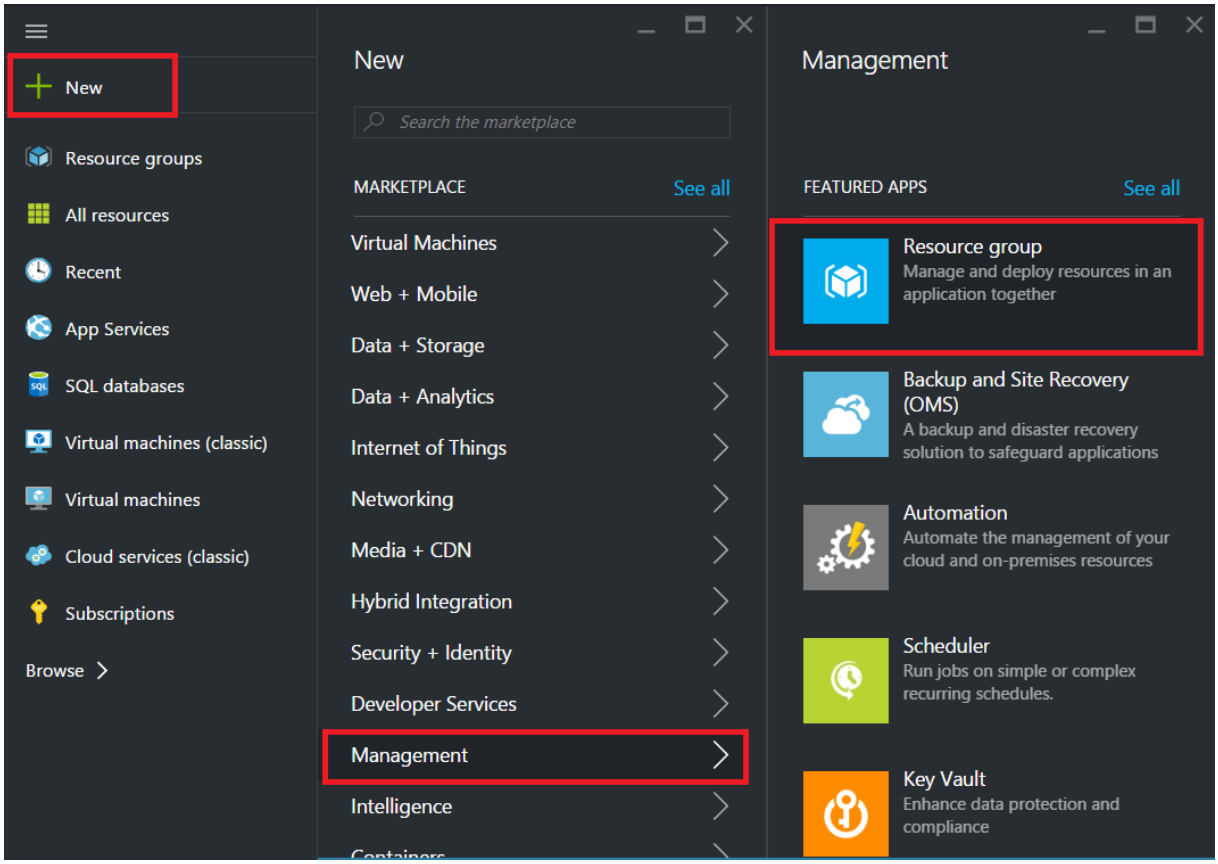
Résumé des étapes de configuration

1. Configuration d'un groupe de ressources
2. Configurer un groupe de sécurité réseau
3. Configuration du réseau virtuel et de ses sous-réseaux
4. Configurer un compte de stockage
5. Configurer un jeu de disponibilité
6. Configurez une instance NetScaler VPX.

Configuration d'un groupe de ressources

Créez un nouveau groupe de ressources qui est un conteneur pour toutes vos ressources. Utilisez le groupe de ressources pour déployer, gérer et surveiller vos ressources en tant que groupe.

1. Cliquez sur **Nouveau** > **Gestion** > **Groupe de ressources**.
2. Dans le volet **Groupe de ressources**, entrez les informations suivantes :
    - Nom du groupe de ressources
    - Emplacement du groupe de ressources
3. Cliquez sur **Créer**.

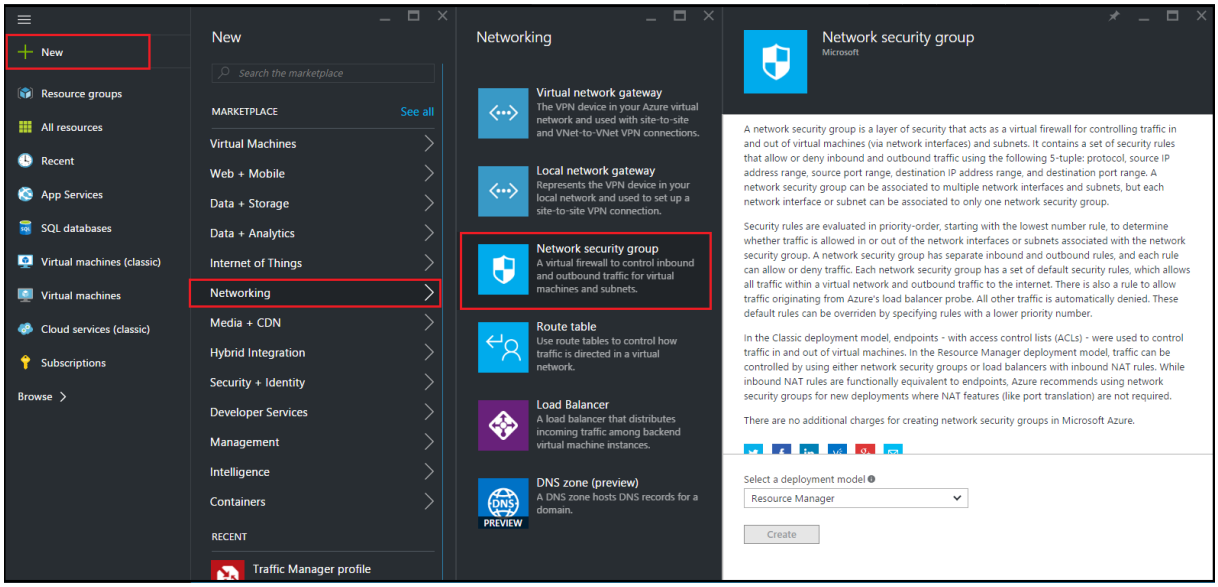


Configurer un groupe de sécurité réseau

Créez un groupe de sécurité réseau pour affecter des règles entrantes et sortantes pour contrôler le trafic entrant et sortant au sein du réseau virtuel. Le groupe de sécurité réseau vous permet de définir des règles de sécurité pour une seule machine virtuelle et de définir des règles de sécurité pour un sous-réseau virtuel.

1. Cliquez sur **Nouveau** > **Mise enréseau > Groupe de sécurité réseau** .
2. Dans le volet **Créer un groupe de sécurité réseau**, entrez les informations suivantes, puis cliquez sur **Créer**.
    - Nom : entrez le nom du groupe de sécurité
    - Groupe de ressources : sélectionnez le groupe de ressources dans la liste déroulante

> **Remarque :**
>
> Assurez-vous d'avoir sélectionné le bon emplacement. La liste des ressources qui apparaissent dans la liste déroulante est différente selon les emplacements.

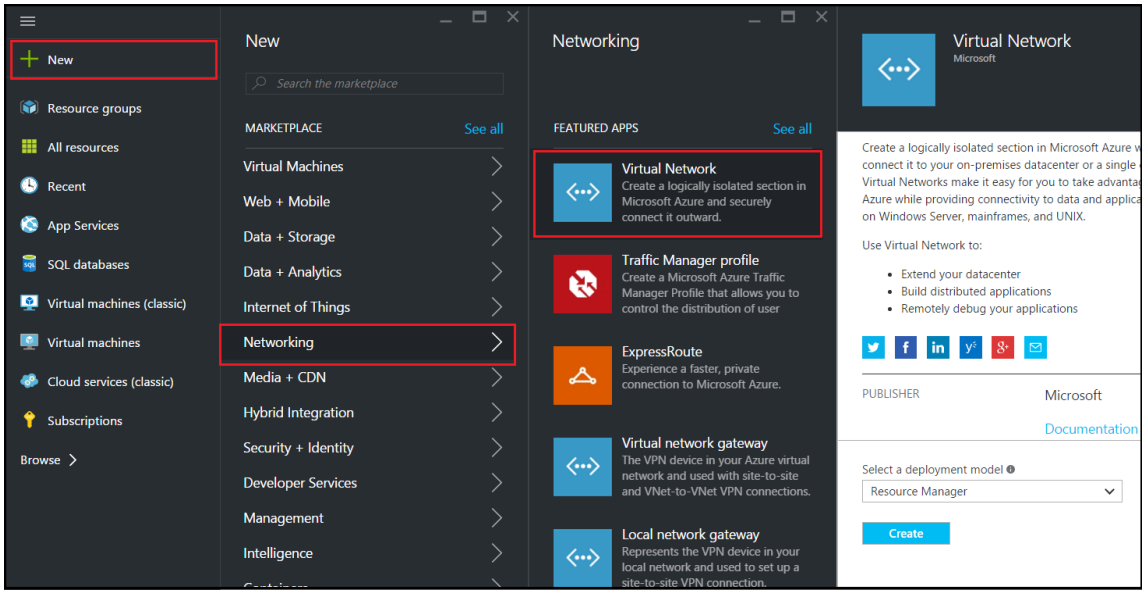


Configurer un réseau virtuel et des sous-réseaux

Les réseaux virtuels d'ARM fournissent un niveau de sécurité et d'isolation à vos services. Les machines virtuelles et les services qui font partie du même réseau virtuel peuvent accéder les uns aux autres.

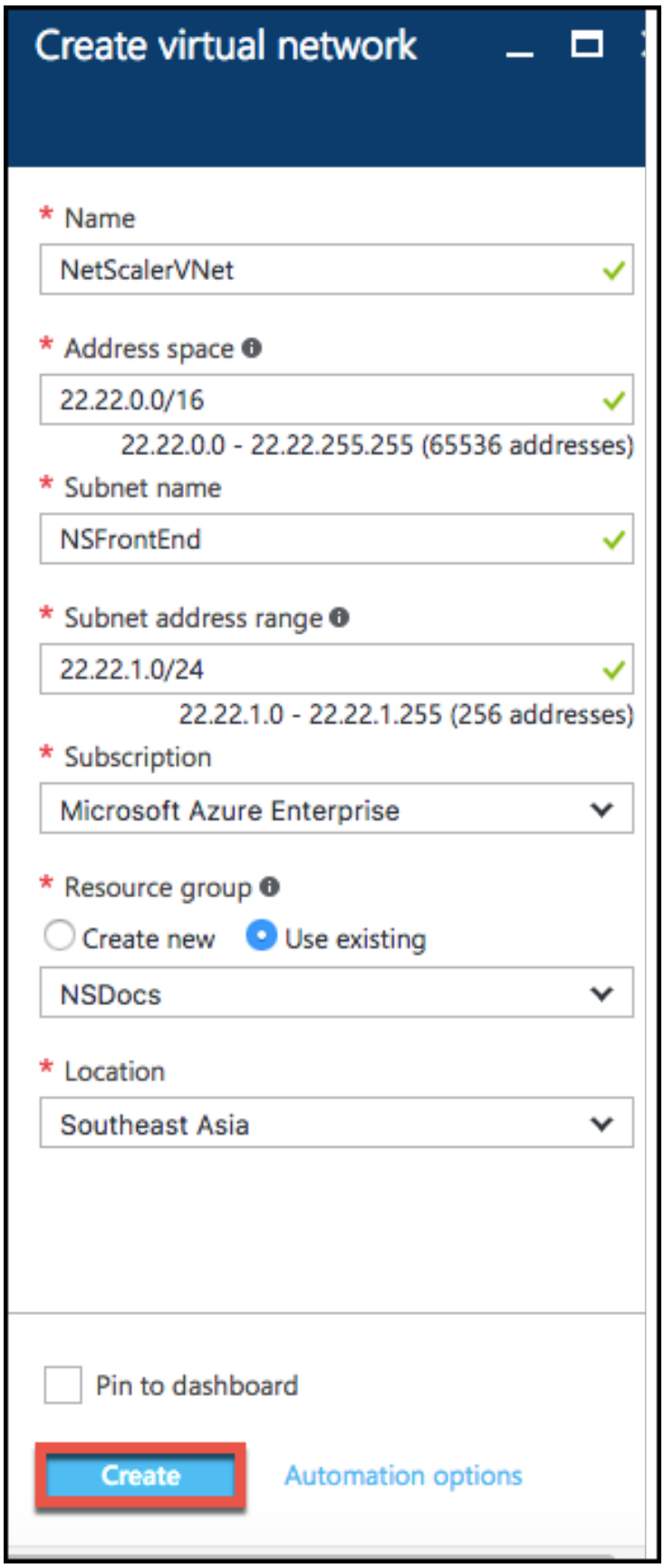
Pour suivre ces étapes pour créer un réseau virtuel et des sous-réseaux.

1. Cliquez sur **Nouveau** > **Réseau** > **Réseau virtuel**.
2. Dans le volet **Réseau virtuel**, assurez-vous que le mode de déploiement est **Gestionnaire de ressources** et cliquez sur **Créer**.



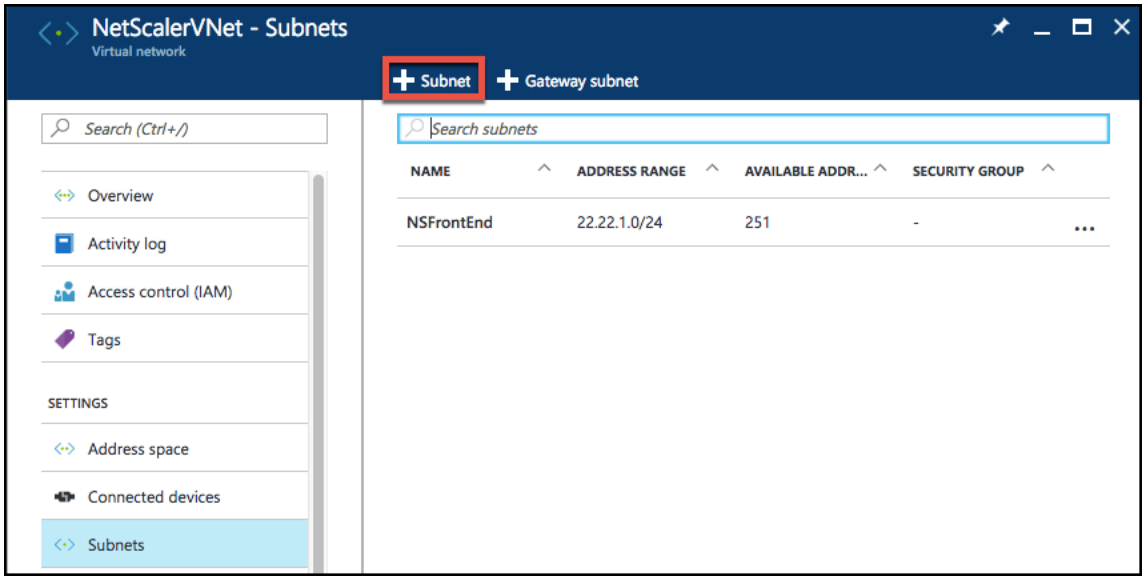
3. Dans le volet **Créer un réseau virtuel**, entrez les valeurs suivantes, puis cliquez sur **Créer** .

    - Nom du réseau virtuel
    - Espace d'adressage : saisissez le bloc d'adresses IP réservé pour le réseau virtuel
    - Sous-réseau : saisissez le nom du premier sous-réseau (vous créerez le second sous-réseau plus tard dans cette étape)
    - Plage d'adresses de sous-réseau : saisissez le bloc d'adresses IP réservé du sous-réseau
    - Groupe de ressources : sélectionnez le groupe de ressources créé précédemment dans la liste déroulante



Configurer le deuxième sous-réseau

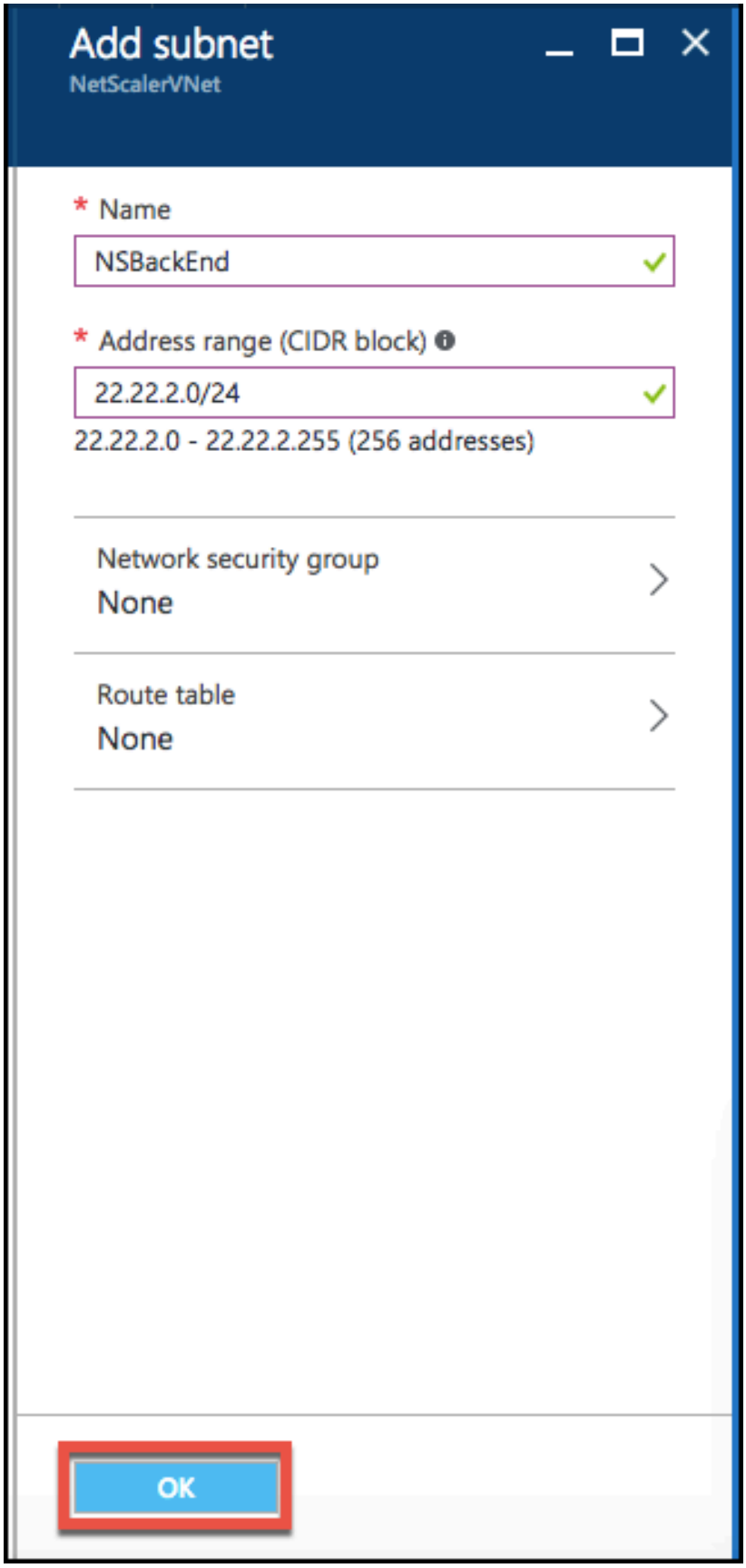
1. Sélectionnez le réseau virtuel nouvellement créé dans le volet **Toutes les ressources** et dans le volet **Paramètres**, cliquez sur **Sous-réseaux** .



2. Cliquez sur **+ Sous-réseau** et créez le second sous-réseau en entrant les détails suivants.

   - Nom du deuxième sous-réseau
   - Plage d'adresses - tapez le bloc d'adresse IP réservé du deuxième sous-réseau
   - Groupe de sécurité réseau : sélectionnez le groupe de sécurité réseau dans la liste déroulante.

3. Cliquez sur **Créer**.

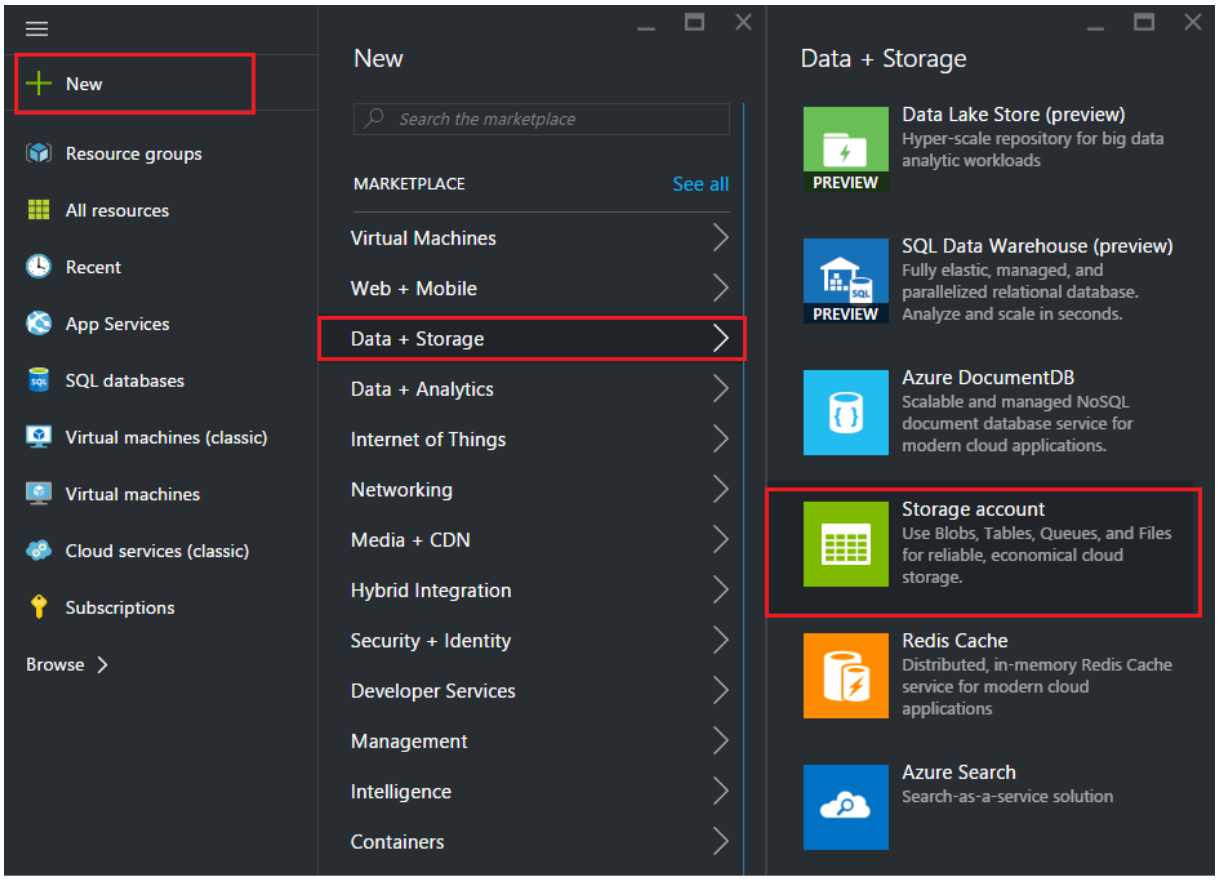


Configurer un compte de stockage

L'infrastructure de stockage ARM IaaS inclut tous les services dans lesquels nous pouvons stocker des données sous forme de blobs, de tables, de files d'attente et de fichiers. Vous pouvez également créer des applications à l'aide de ces formes de données de stockage dans ARM.

Créez un compte de stockage pour stocker toutes vos données.

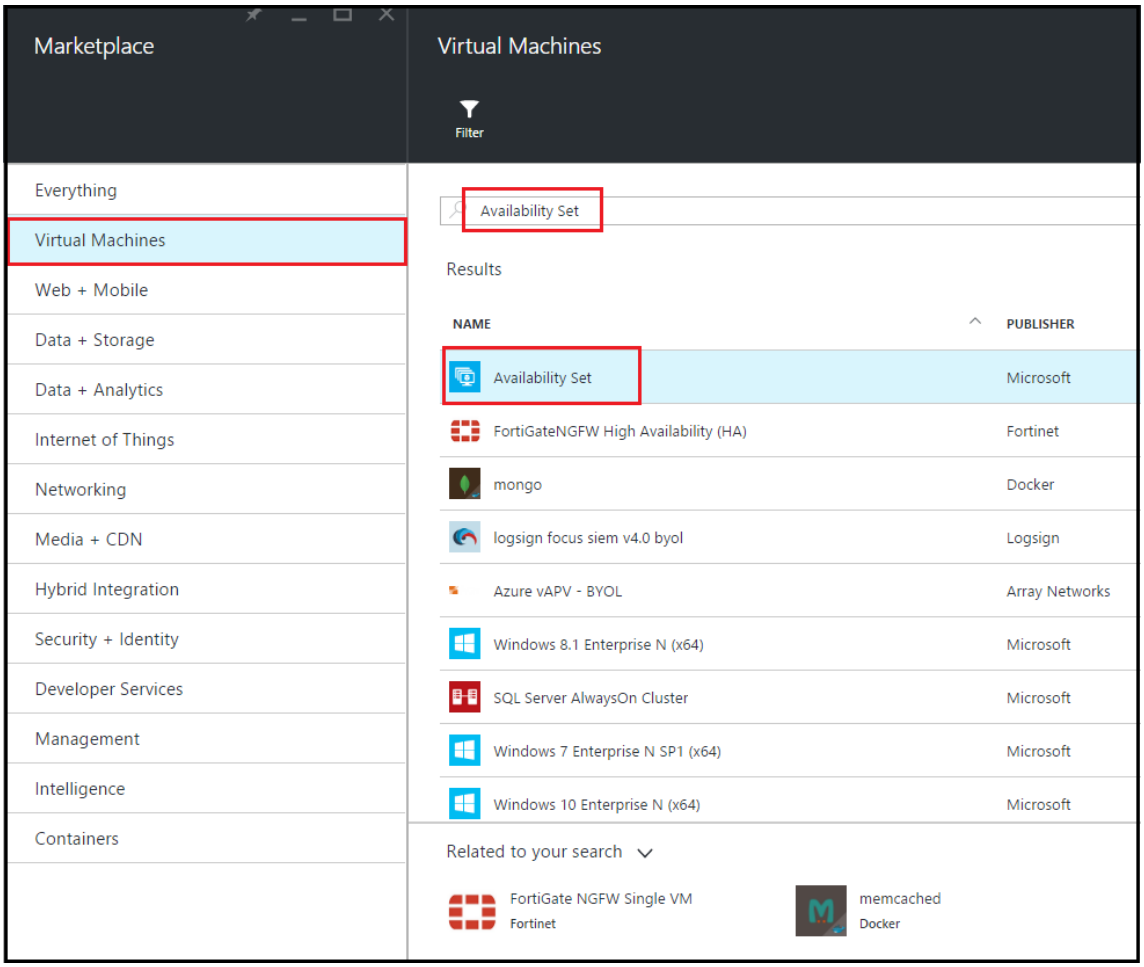
1. Cliquez sur **+Nouveau** > **Données + Stockage** > **Compte de stockage.**
2. Dans le volet **Créer un compte de stockage**, entrez les informations suivantes :
    - Nom du compte
    - Mode de déploiement : assurez-vous de sélectionner **Resource Manager**
    - Type de compte : sélectionnez **Usage général** dans la liste déroulante
    - Réplication : sélectionnez **Stockage localement redondant** dans la liste déroulante
    - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
3. Cliquez sur **Créer**.



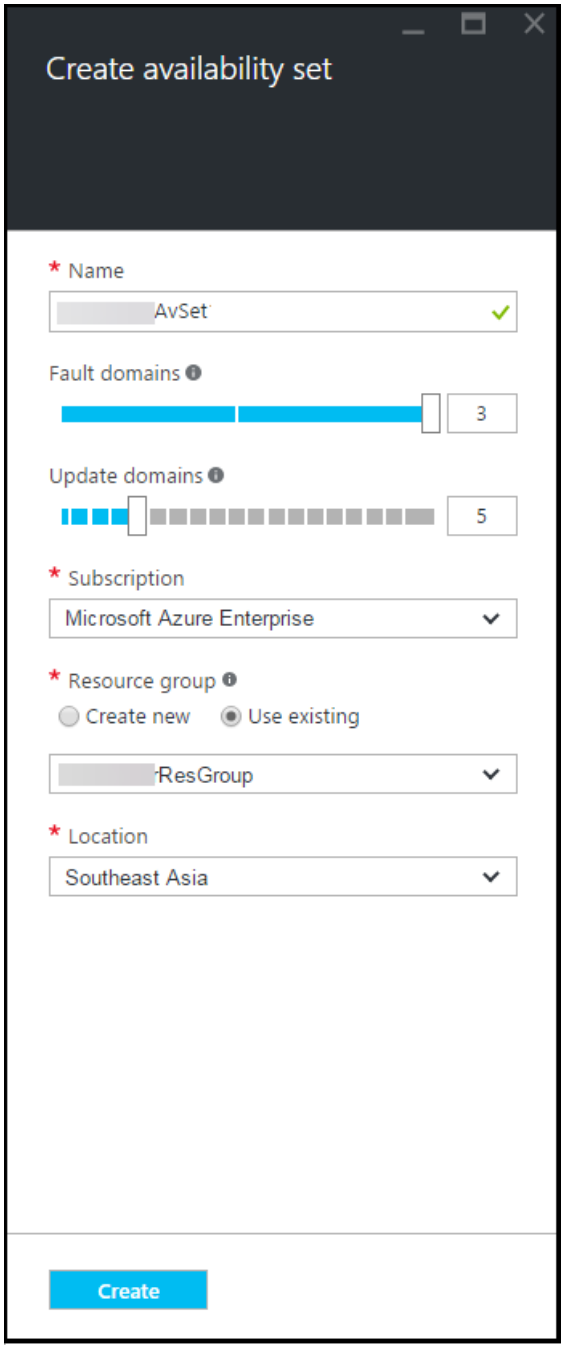
Configurer un jeu de disponibilité

Un ensemble de disponibilité garantit qu'au moins une machine virtuelle reste opérationnelle en cas de maintenance planifiée ou imprévue. Deux machines virtuelles ou plus appartenant au même « ensemble de disponibilité » sont placées sur des domaines de défaillance différents pour fournir des services redondants.

1. Cliquez sur **+Nouveau**.
2. Cliquez sur **Tout afficher** dans le volet MARKETPLACE, puis sur **Machines virtuelles**.
3. Recherchez le jeu de disponibilité, puis sélectionnez Entité de **jeu de disponibilité** dans la liste affichée.



4. Cliquez sur **Créer et,** dans le volet **Créer un jeu de disponibilité**, entrez les détails suivants :
   - Nom du set
   - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
5. Cliquez sur **Créer**.



Configuration d'une instance NetScaler VPX

Créez une instance de NetScaler VPX dans le réseau virtuel. Obtenez l'image NetScaler VPX sur Azure Marketplace, puis utilisez le portail Azure Resource Manager pour créer une instance NetScaler VPX.

Avant de commencer à créer l'instance NetScaler VPX, assurez-vous d'avoir créé un réseau virtuel avec les sous-réseaux requis dans lesquels l'instance réside. Vous pouvez créer des réseaux virtuels pendant le provisioning de machines virtuelles, mais sans la possibilité de créer différents sous-réseaux.

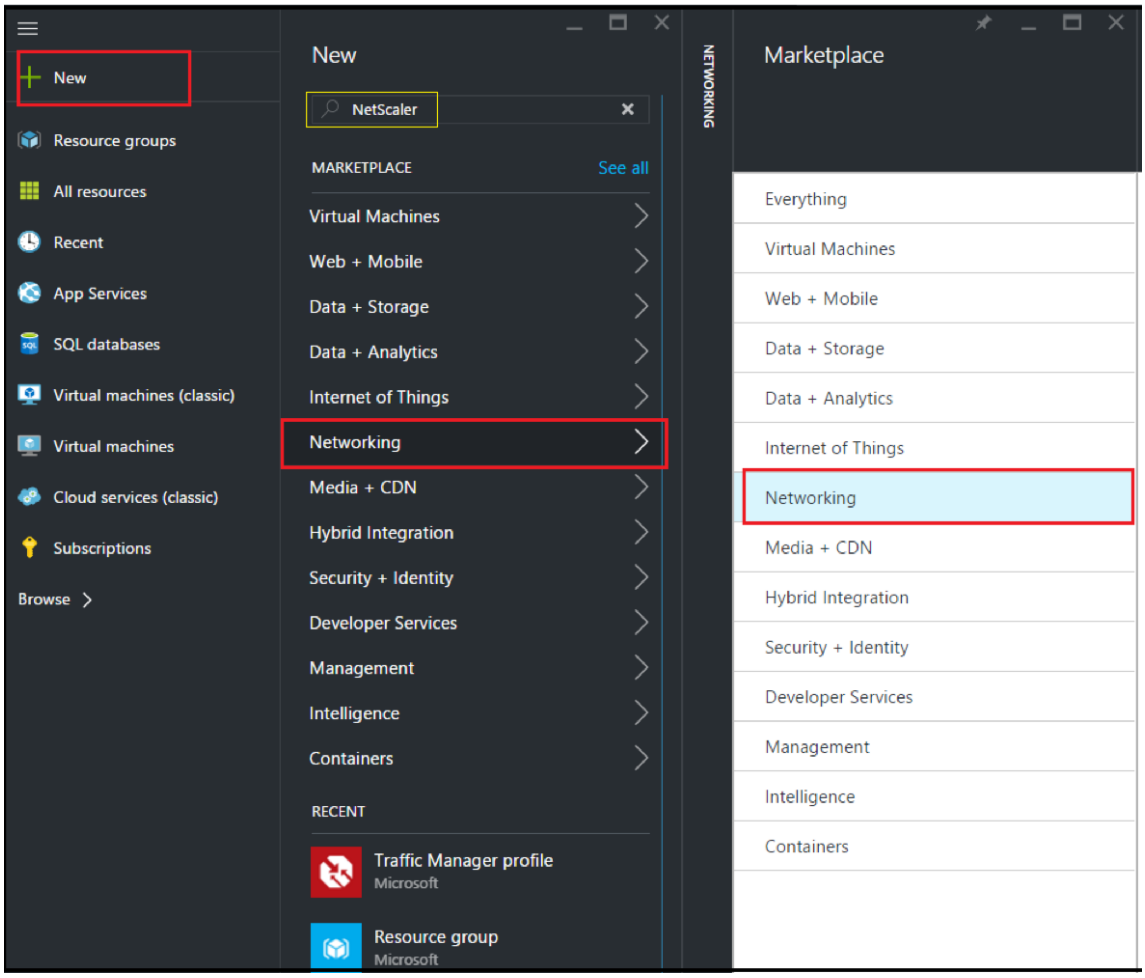
Pour plus d'informations sur la création de réseaux virtuels, consultez http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Configurez éventuellement la connectivité du serveur DNS et du VPN pour permettre à une machine virtuelle d'accéder aux ressources Internet.

> **Remarque :**
>
> Citrix vous recommande de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités avant de provisionner la machine virtuelle NetScaler VPX, afin que les informations réseau soient disponibles lors du provisionnement.

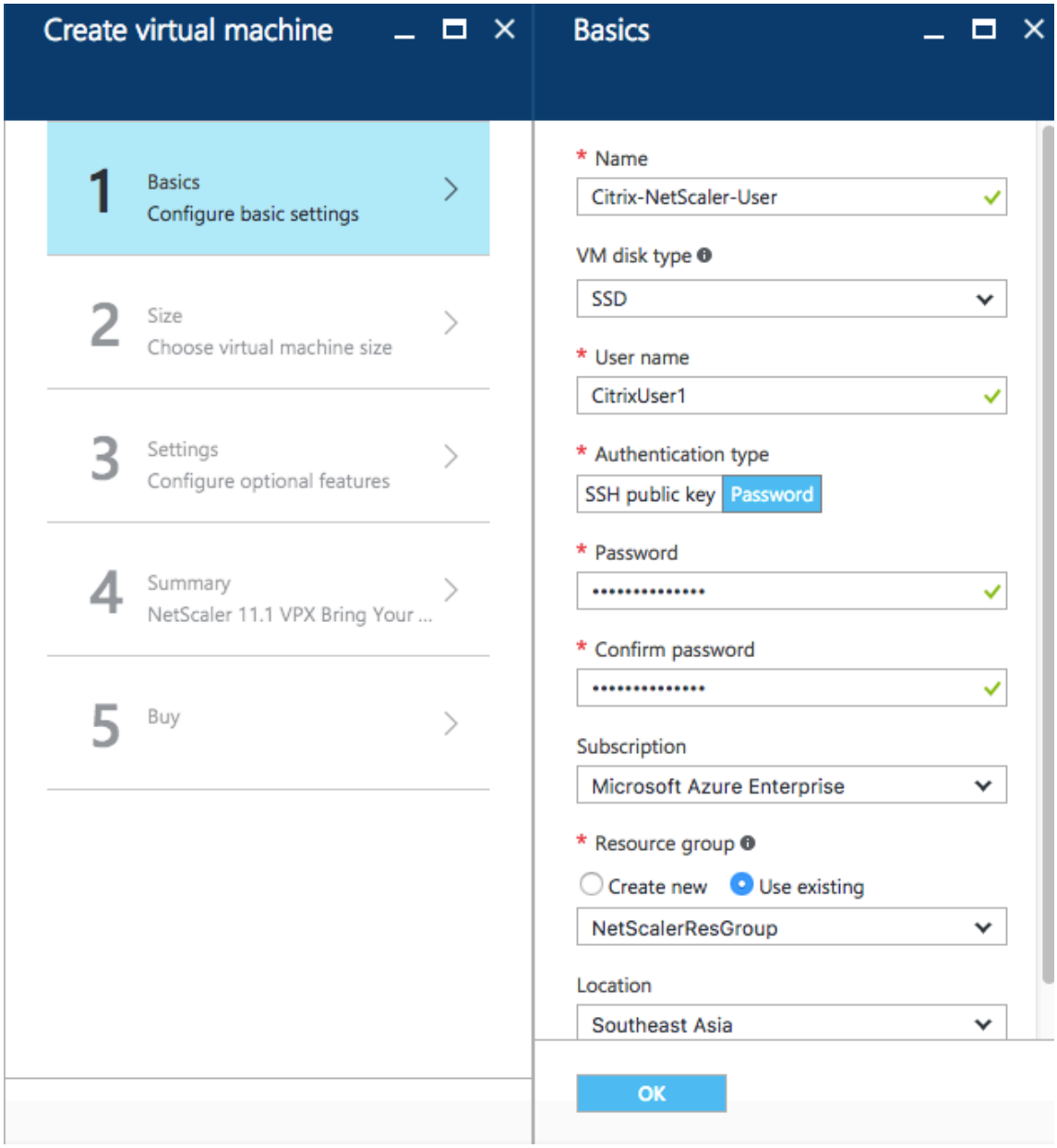
1. Cliquez sur **+Nouveau** > **Réseau**.
2. Cliquez sur **Afficher tout** et dans le volet Réseau, cliquez sur **NetScaler 13.0.**
3. Sélectionnez **NetScaler 13.0 VPX Bring Your Own License** dans la liste des offres logicielles.

   Pour trouver rapidement une entité sur le portail ARM, vous pouvez également taper le nom de l'entité dans le champ de recherche Azure Marketplace et appuyer sur \ <Enter>. Tapez NetScaler dans la zone de recherche pour trouver les images NetScaler.



> **Remarque :**
>
> Assurez-vous de sélectionner la dernière image. Le numéro de version de votre image NetScaler figure peut-être dans le nom.

4. Sur la page **NetScaler VPX Bring Your Own License**, dans la liste déroulante, sélectionnez **Gestionnaire de ressources** et cliquez sur **Créer** .



5. Dans le volet **Créer une machine virtuelle**, spécifiez les valeurs requises dans chaque section pour créer une machine virtuelle. Cliquez sur **OK** dans chaque section pour enregistrer votre configuration.

Basique :

- Nom : spécifiez un nom pour l'instance NetScaler VPX
- Type de disque de machine virtuelle : sélectionnez SSD (valeur par défaut) ou HDD dans le menu déroulant
- Nom d'utilisateur et mot de passe : spécifiez un nom d'utilisateur et un mot de passe pour accéder aux ressources du groupe de ressources que vous avez créé
- Type d'authentification : sélectionnez la clé publique ou le mot de passe SSH
- Groupe de ressources : sélectionnez le groupe de ressources que vous avez créé dans la liste déroulante

Vous pouvez créer un groupe de ressources ici, mais Citrix vous recommande de créer un groupe de ressources à partir des groupes de ressources dans Azure Resource Manager, puis de sélectionner le groupe dans la liste déroulante.

> **Remarque :**
>
> Dans un environnement Azure Stack, en plus des paramètres de base, spécifiez les paramètres suivants :
>
> - Domaine Azure Stack
> - Client Azure Stack (facultatif)
> - Client Azure (facultatif)
> - Secret du client Azure (facultatif)

Taille :

Selon le type de disque de machine virtuelle, SDD ou HDD que vous avez sélectionné dans les paramètres de base, les tailles de disque sont affichées.

- Sélectionnez une taille de disque en fonction de vos besoins et cliquez sur **Sélectionner**.

Paramètres :

- Sélectionnez le type de disque par défaut (Standard)
- Compte de stockage : sélectionnez le compte de stockage
- Réseau virtuel : sélectionnez le réseau virtuel
- Sous-réseau : définissez l'adresse du sous-réseau
- Adresse IP publique : sélectionnez le type d'attribution d'adresse IP
- Groupe de sécurité réseau : sélectionnez le groupe de sécurité que vous avez créé. Assurez-vous que les règles entrantes et sortantes sont configurées dans le groupe de sécurité.
- Ensemble de disponibilité : sélectionnez le jeu de disponibilité dans le menu déroulant

Résumé :

Les paramètres de configuration sont validés et la page Résumé affiche le résultat de la validation. Si la validation échoue, la page Résumé affiche la raison de l'échec. Retournez à la section particulière et apportez les modifications nécessaires. Si la validation réussit, cliquez sur **OK**.

Acheter :

Consultez les détails de l'offre et les conditions légales sur la page d'achat, puis cliquez sur **Acheter**.

Pour un déploiement à haute disponibilité, créez deux instances indépendantes de NetScaler VPX dans le même ensemble de disponibilité et dans le même groupe de ressources pour les déployer dans une configuration de veille active.

Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX

October 17, 2024

Cette section explique comment configurer une instance NetScaler VPX autonome avec plusieurs adresses IP, dans Azure Resource Manager (ARM). Une ou plusieurs cartes réseau peuvent être associées à l'instance VPX, et une ou plusieurs adresses IP publiques et privées statiques ou dynamiques peuvent lui être attribuées à chaque carte réseau. Vous pouvez attribuer plusieurs adresses IP en tant que NSIP, VIP, SNIP, etc.

Pour plus d'informations, consultez la documentation Azure Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.

Si vous souhaitez utiliser les commandes PowerShell, consultez Configuration de plusieurs adresses IP pour une instance NetScaler VPX en mode autonome à l'aide des commandes PowerShell.

Cas d'utilisation

Dans ce cas d'utilisation, une appliance NetScaler VPX autonome est configurée avec une seule carte réseau connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP (ipconfig), chaque serveur ayant une fonction différente, comme le montre le tableau.

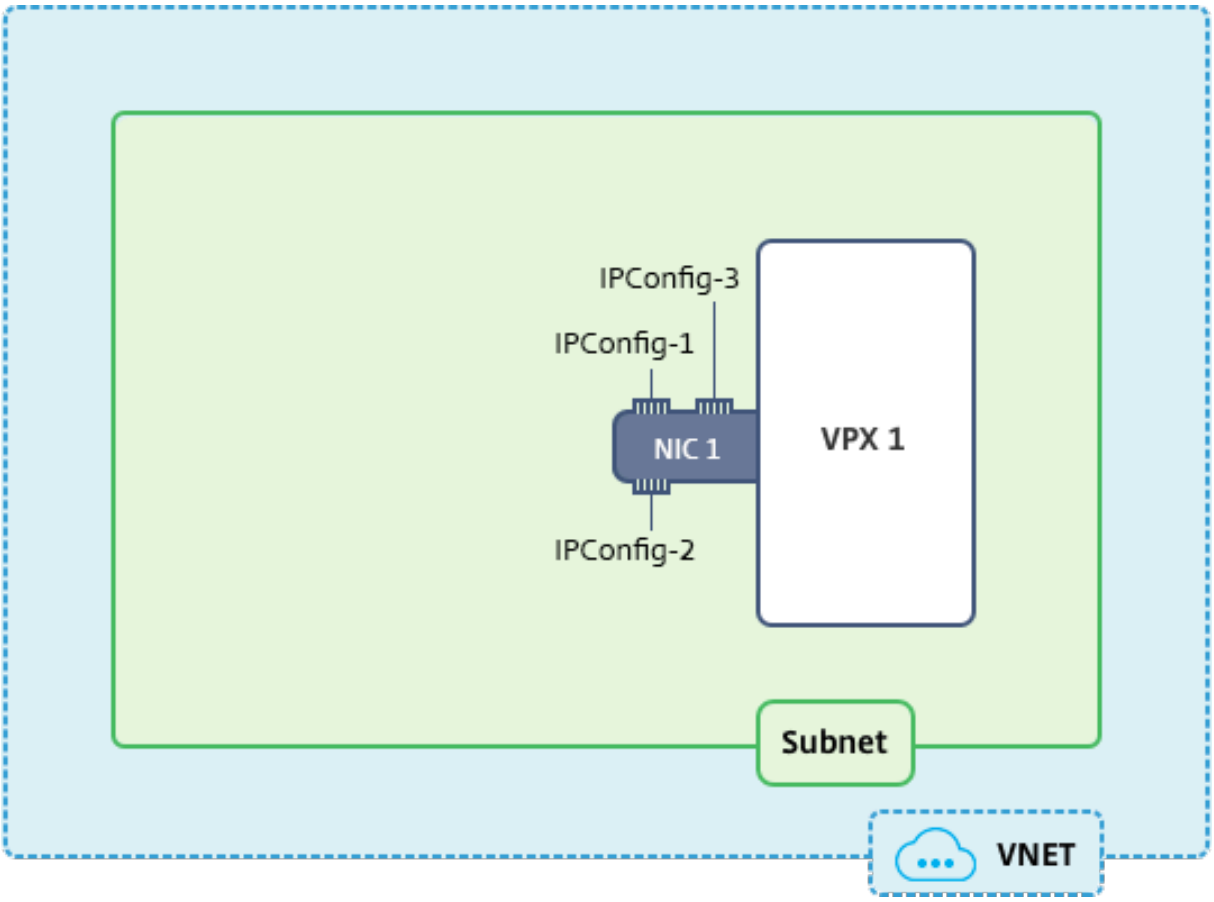
Configuration IP	Associé à	Motif
ipconfig1	Adresse IP publique statique ; adresse IP privée statique	Sert le trafic de gestion
ipconfig2	Adresse IP publique statique ; adresse privée statique	Sert le trafic côté client

Configuration IP	Associé à	Motif
ipconfig3	Adresse IP privée statique	Communication avec les serveurs back-end

> **Remarque :**
>
> `IPConfig-3` n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque :**
>
> Dans un déploiement Azure NetScaler VPX multi-NIC et multi-IP, l'adresse IP privée associée à la principale (première) `IPConfig` de la carte réseau principale (première) est automatiquement ajoutée en tant que NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, selon vos besoins.

Avant de commencer

Avant de commencer, créez une instance VPX en suivant les étapes indiquées sur ce lien :

Configurer une instance autonome NetScaler VPX

Dans ce cas d'utilisation, l'instance VPX NSDoc0330vm est créée.

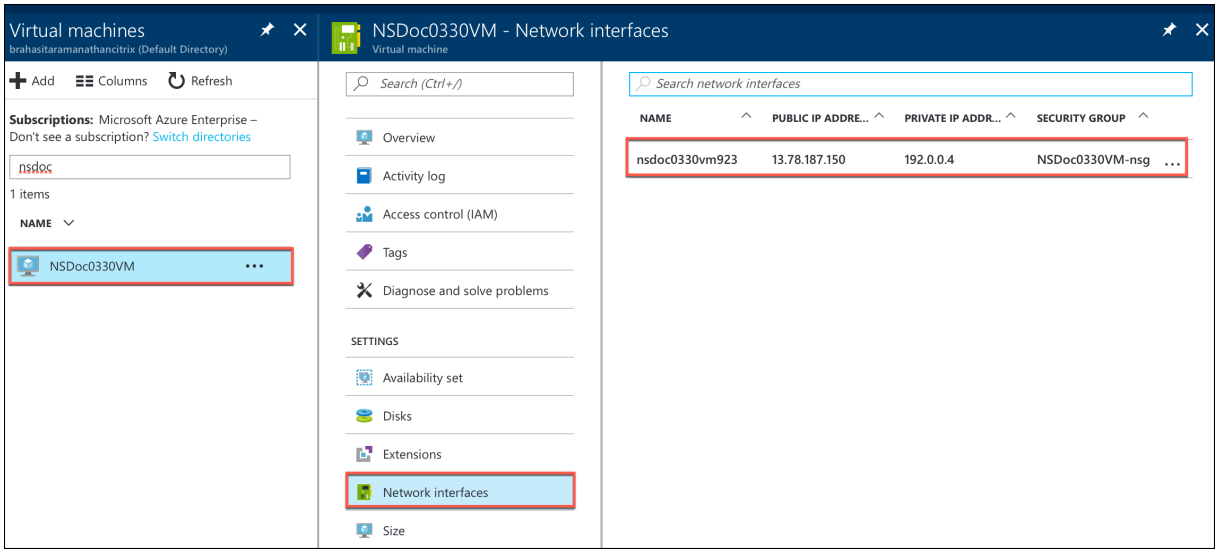
Procédure de configuration de plusieurs adresses IP pour une instance NetScaler VPX en mode autonome.

Pour configurer plusieurs adresses IP pour une appliance NetScaler VPX en mode autonome :

1. Ajouter des adresses IP à la machine virtuelle
2. Configurer les adresses IP appartenant à NetScaler

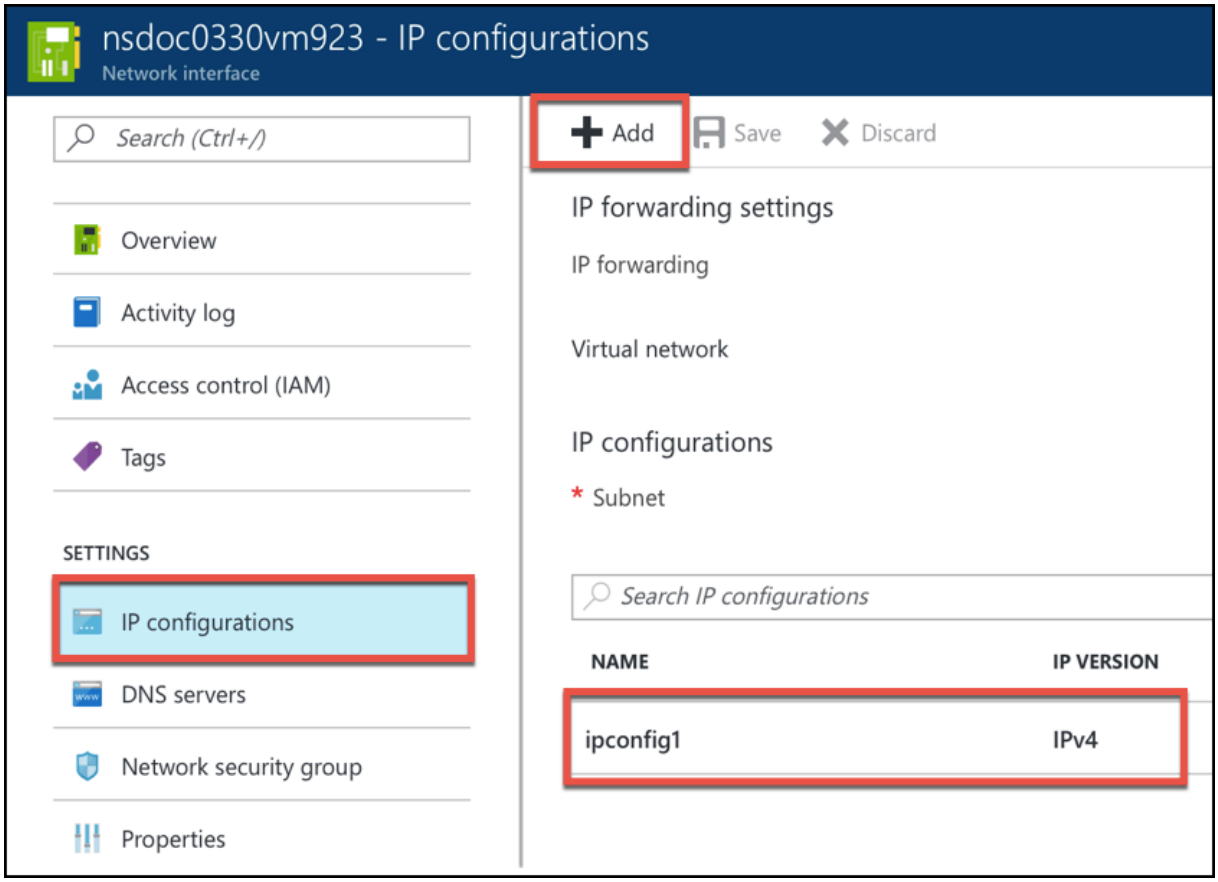
Étape 1 : ajouter des adresses IP à la machine virtuelle

1. Dans le portail, cliquez sur **Plus de services > tapez machines virtuelles** dans la zone de filtre, puis cliquez sur **Machines virtuelles**.
2. Dans le **volet Machines virtuelles**, cliquez sur la machine virtuelle à laquelle vous souhaitez ajouter des adresses IP. Cliquez sur **Interfaces réseau** dans la lame de machine virtuelle qui apparaît, puis sélectionnez l'interface réseau.



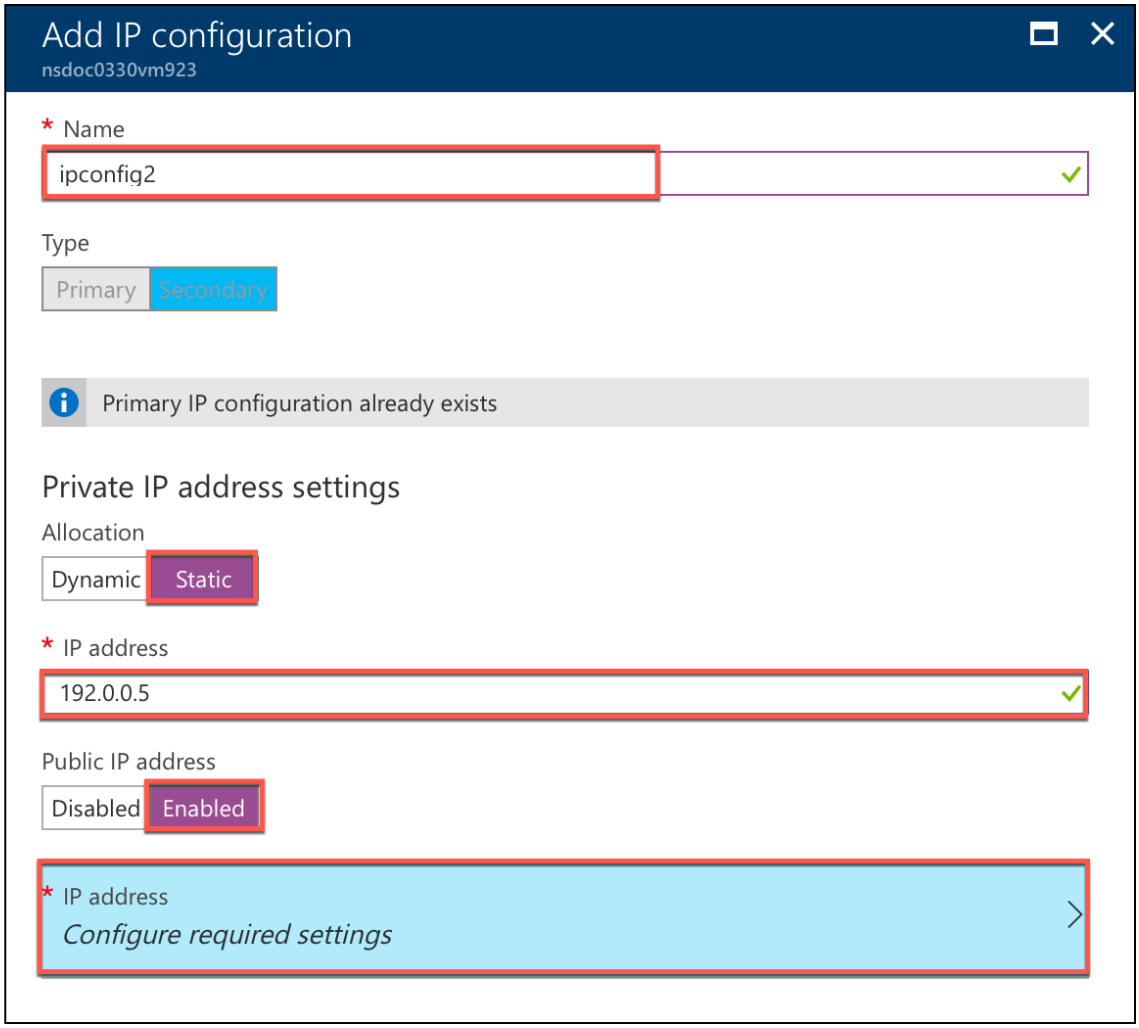
Dans la lame qui apparaît pour la carte réseau sélectionnée, cliquez sur **Configurations IP**. La configuration IP existante qui a été attribuée lors de la création de la machine virtuelle, **ipconfig1**, s'affiche. Dans ce cas d'utilisation, assurez-vous que les adresses IP associées à ipconfig1 sont statiques. Ensuite, créez deux configurations IP supplémentaires : ipconfig2 (VIP) et ipconfig3 (SNIP).

Pour en créer plus `ipconfigs`, créez **Ajouter**.



Dans la fenêtre **Ajouter une configuration IP**, entrez un **nom**, spécifiez la méthode d'allocation comme **statique**, entrez une adresse IP (192.0.0.5 pour ce cas d'utilisation) et activez **l'adresse IP publique** .

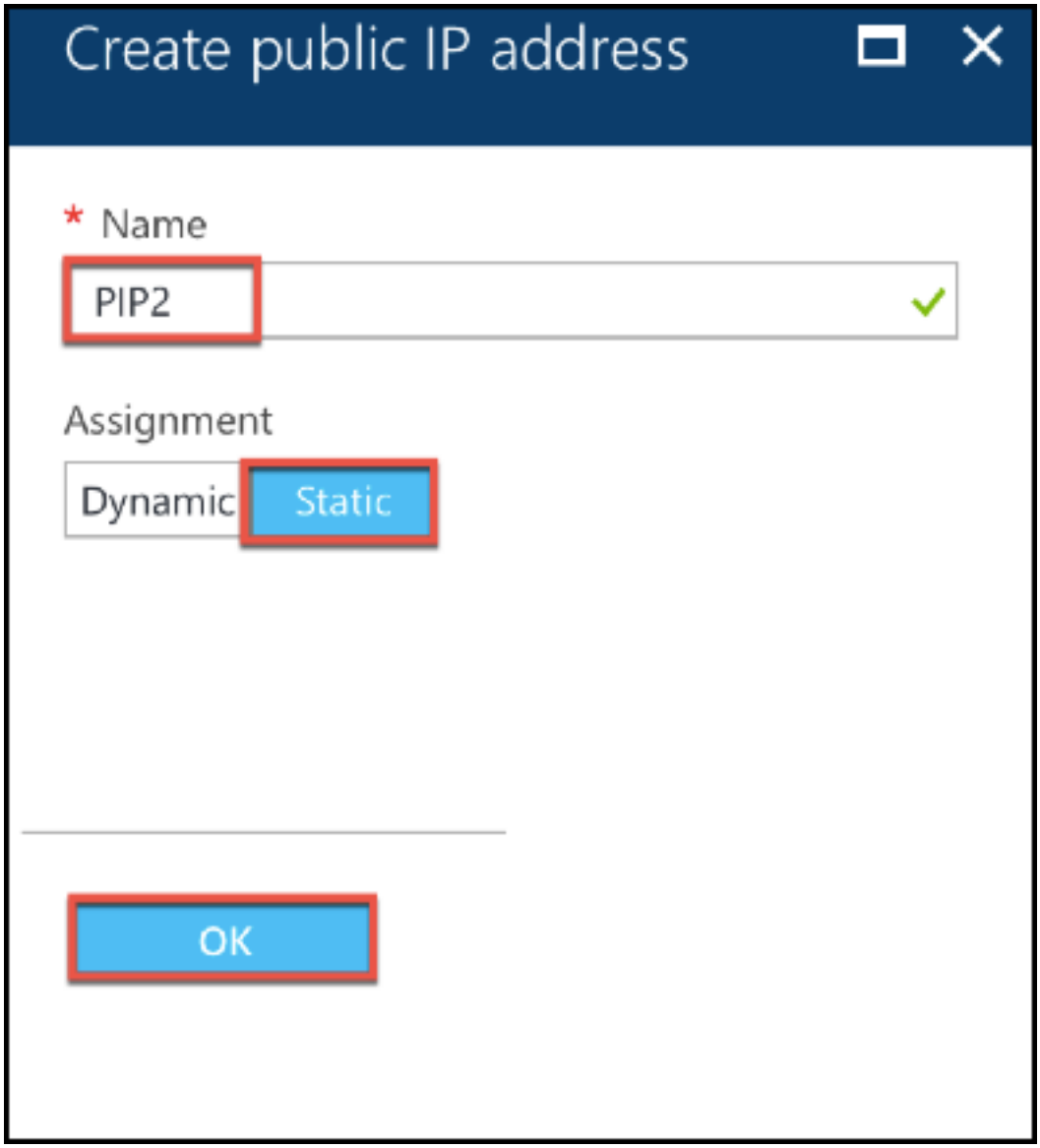
> **Remarque :**
>
> Avant d'ajouter une adresse IP privée statique, vérifiez la disponibilité de l'adresse IP et assurez-vous que l'adresse IP appartient au même sous-réseau auquel la carte réseau est attachée.



Ensuite, cliquez sur **Configurer les paramètres requis** pour créer une adresse IP publique statique pour ipconfig2.

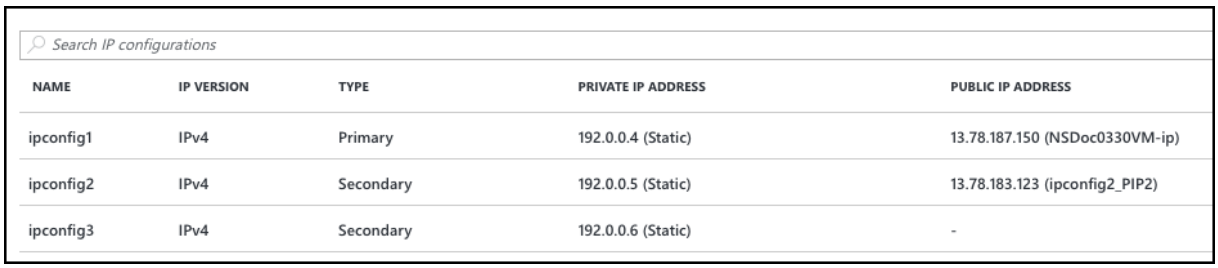
Par défaut, les adresses IP publiques sont dynamiques. Pour vous assurer que la machine virtuelle utilise toujours la même adresse IP publique, créez une adresse IP publique statique.

Dans le volet Créer une adresse IP publique, ajoutez un nom. Sous Attribution, cliquez sur **Statique**. Puis cliquez sur **OK**.



> **Remarque :**
>
> Même lorsque vous définissez la méthode d'allocation sur statique, vous ne pouvez pas spécifier l'adresse IP réelle attribuée à la ressource IP publique. Elle est plutôt allouée à partir d'un pool d'adresses IP disponibles dans l'emplacement Azure où la ressource est créée.

Suivez les étapes pour ajouter une configuration IP supplémentaire pour ipconfig3. La propriété intellectuelle publique n'est pas obligatoire.



Étape 2 : Configuration des adresses IP appartenant à NetScaler

Configurez les adresses IP appartenant à NetScaler à l'aide de l'interface graphique ou de la commande. `add ns ip` Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau

October 17, 2024

Dans un déploiement Microsoft Azure, une configuration à haute disponibilité de deux instances NetScaler VPX est obtenue à l'aide de l'Azure Load Balancer (ALB). Pour ce faire, vous pouvez configurer une sonde de santé sur ALB, qui surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes aux instances principales et secondaires.

Dans cette configuration, seul le nœud principal répond aux sondes de santé et le nœud secondaire ne le fait pas. Une fois que le principal envoie la réponse à la sonde d'intégrité, l'ALB commence à envoyer le trafic de données à l'instance. Si l'instance principale rate deux tests d'intégrité consécutifs, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps total de basculement que peut prendre le changement de trafic peut être de 13 secondes maximum.

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

Les options suivantes sont disponibles pour un déploiement de haute disponibilité multi-cartes réseau :

- Haute disponibilité à l'aide du jeu de disponibilité Azure
- Haute disponibilité à l'aide des zones de disponibilité Azure

Pour plus d'informations sur Azure Availability Set et Availability Zones, consultez la documentation Azure Gérer la disponibilité des machines virtuelles Linux.

Haute disponibilité en utilisant le jeu de disponibilité

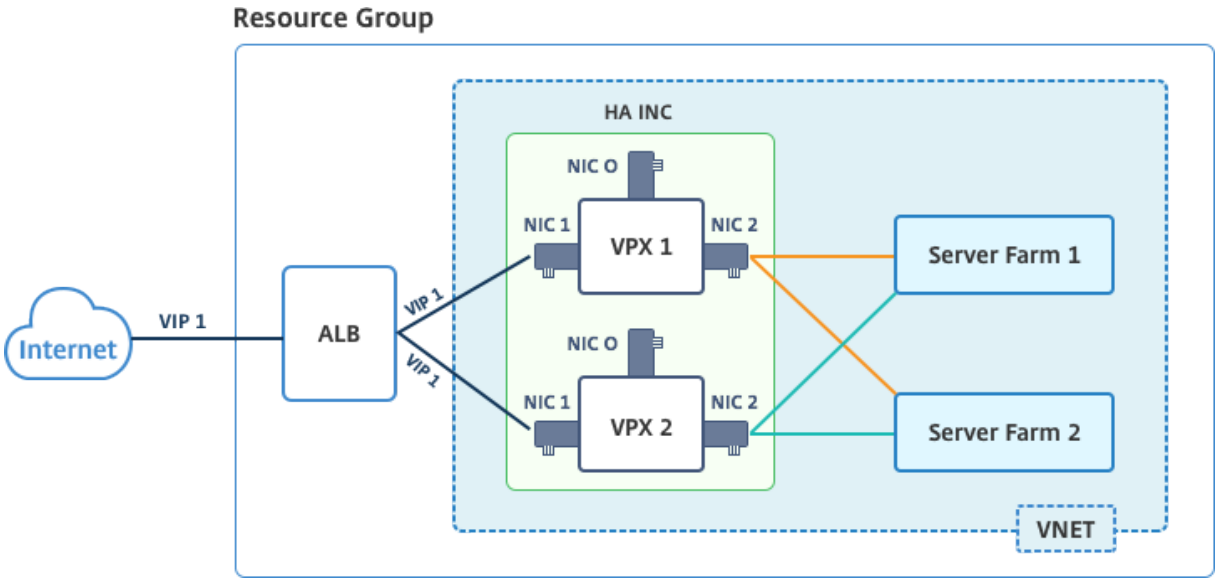
Une configuration haute disponibilité utilisant un jeu de disponibilité doit répondre aux exigences suivantes :

- Configuration de réseau indépendant HA (Independent Network Configuration)
- Azure Load Balancer (ALB) en mode Direct Server Return (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque :**
>
> Pour qu'un déploiement de haute disponibilité de NetScaler VPX sur le cloud Azure fonctionne, vous avez besoin d'une adresse IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds VPX. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Schéma : Exemple d'architecture de déploiement à haute disponibilité utilisant Azure Availability Set



Dans un déploiement actif-passif, les adresses IP publiques frontales (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

Vous pouvez déployer une paire VPX en mode haute disponibilité actif-passif de deux manières en utilisant :

- **Modèle de haute disponibilité standard NetScaler VPX** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.
- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonction des exigences de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA actif-passif à l'aide du modèle Citrix. Si vous souhaitez utiliser les commandes PowerShell, consultez Configuration d'une configuration HA avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell.

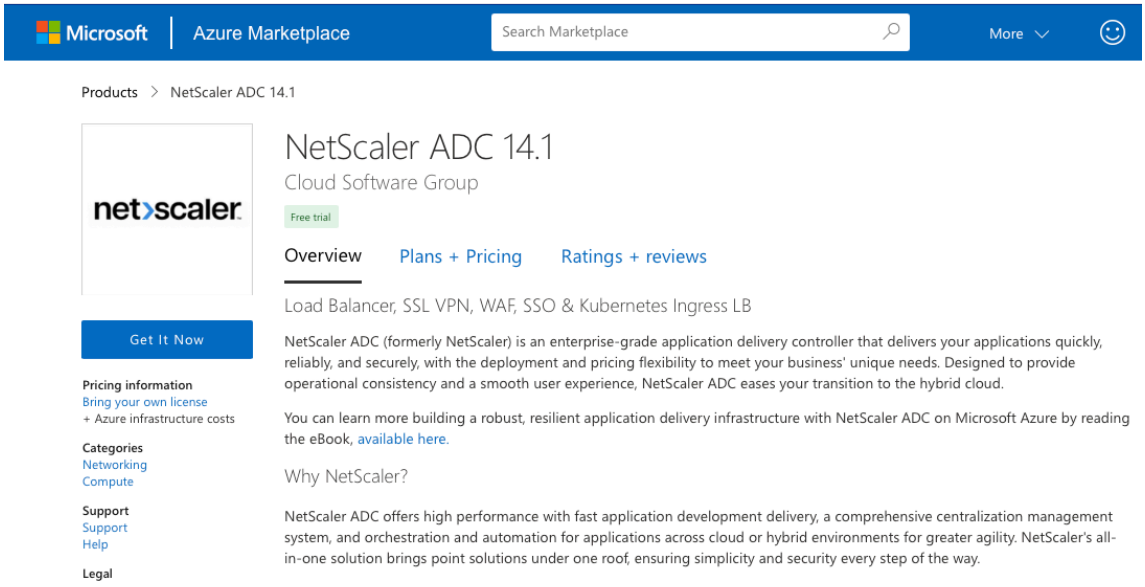
Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler

Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés au trafic de gestion, client et côté serveur, et chaque sous-réseau dispose de deux cartes réseau pour les deux instances VPX.

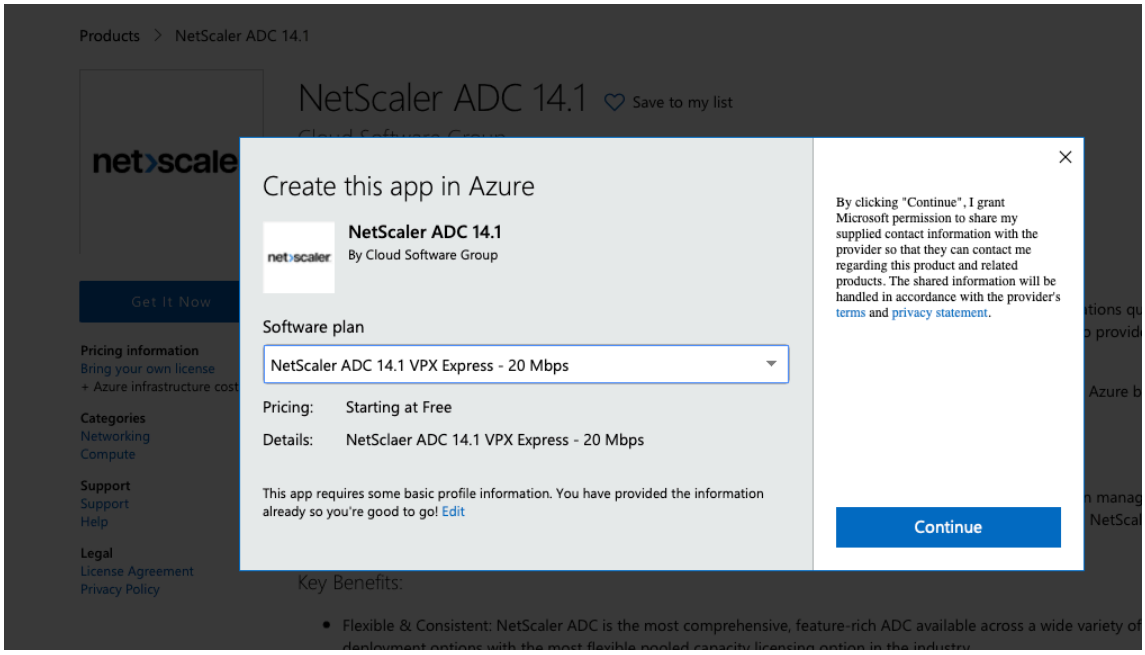
Vous pouvez obtenir le modèle NetScaler HA Pair sur AzureMarketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des jeux de disponibilité Azure.

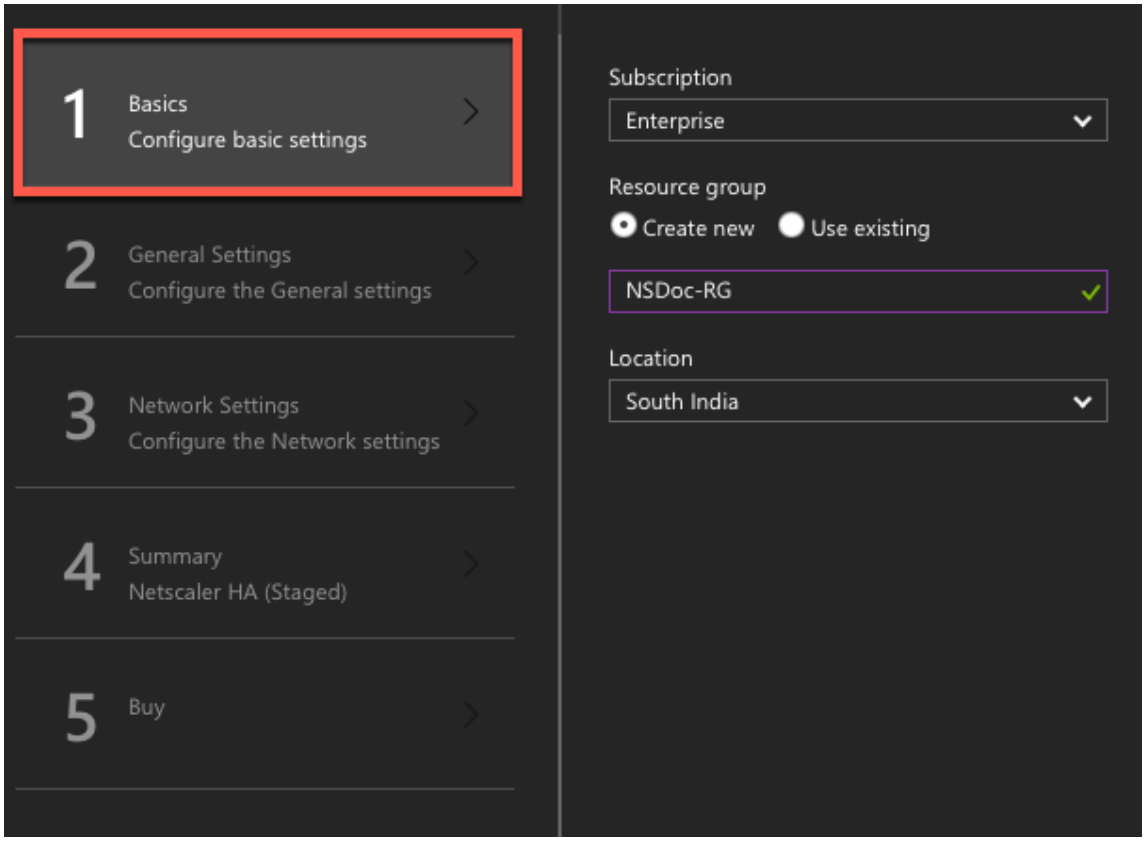
1. Sur Azure Marketplace, recherchez **NetScaler**.



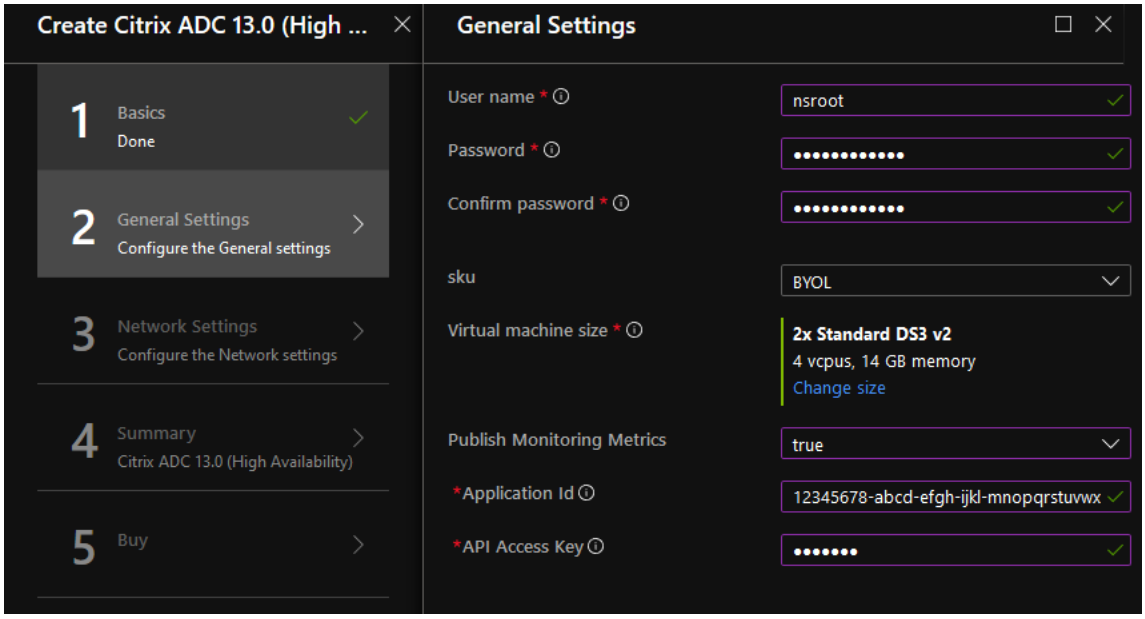
2. Cliquez sur **GET IT NOW**.
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



4. La page **Principes** de base s'affiche. Créez un groupe de ressources et sélectionnez **OK**.

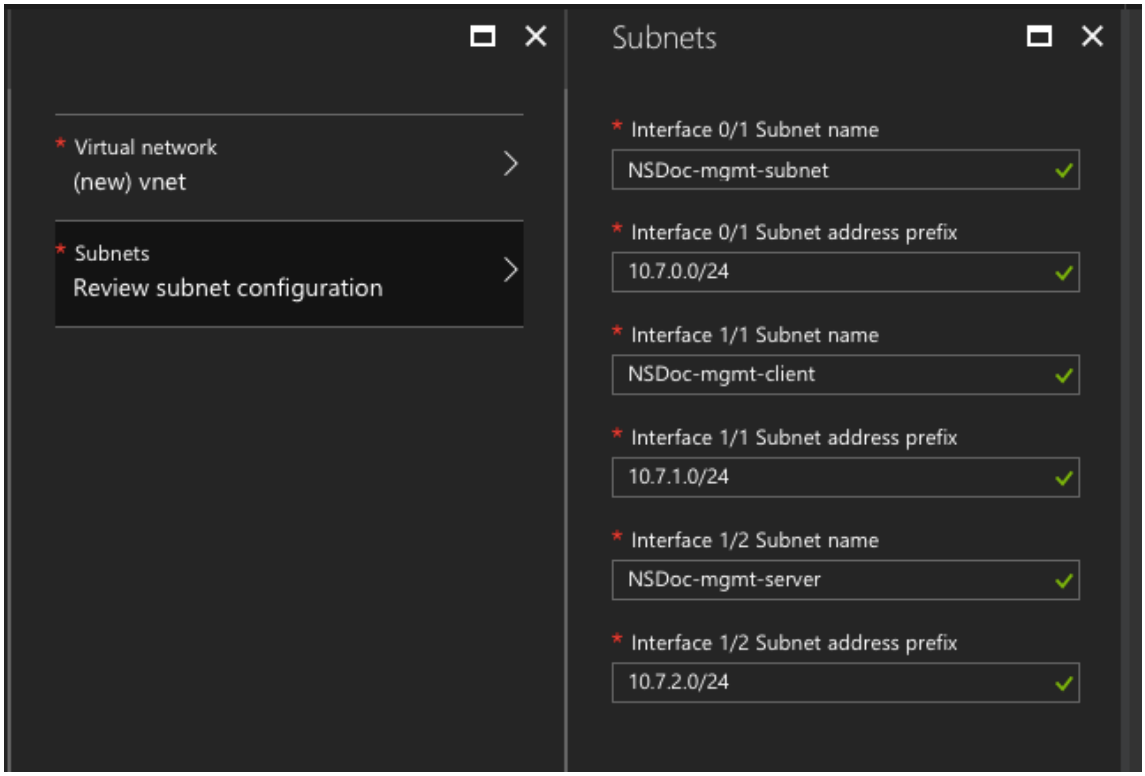


5. La page **Paramètres généraux** s'affiche. Entrez les détails et sélectionnez **OK**.



> **Remarque :**
>
> Par défaut, l'option **Publishing Monitoring Metrics** est définie sur **false**. Si vous souhaitez activer cette option, sélectionnez **vrai**. Créez une application Azure Active Directory (ADD) et un principal de service pouvant accéder aux ressources. Attribuez un rôle de contributeur à l'application AAD nouvellement créée. Pour plus d'informations, voir Utiliser le portail pour créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources.

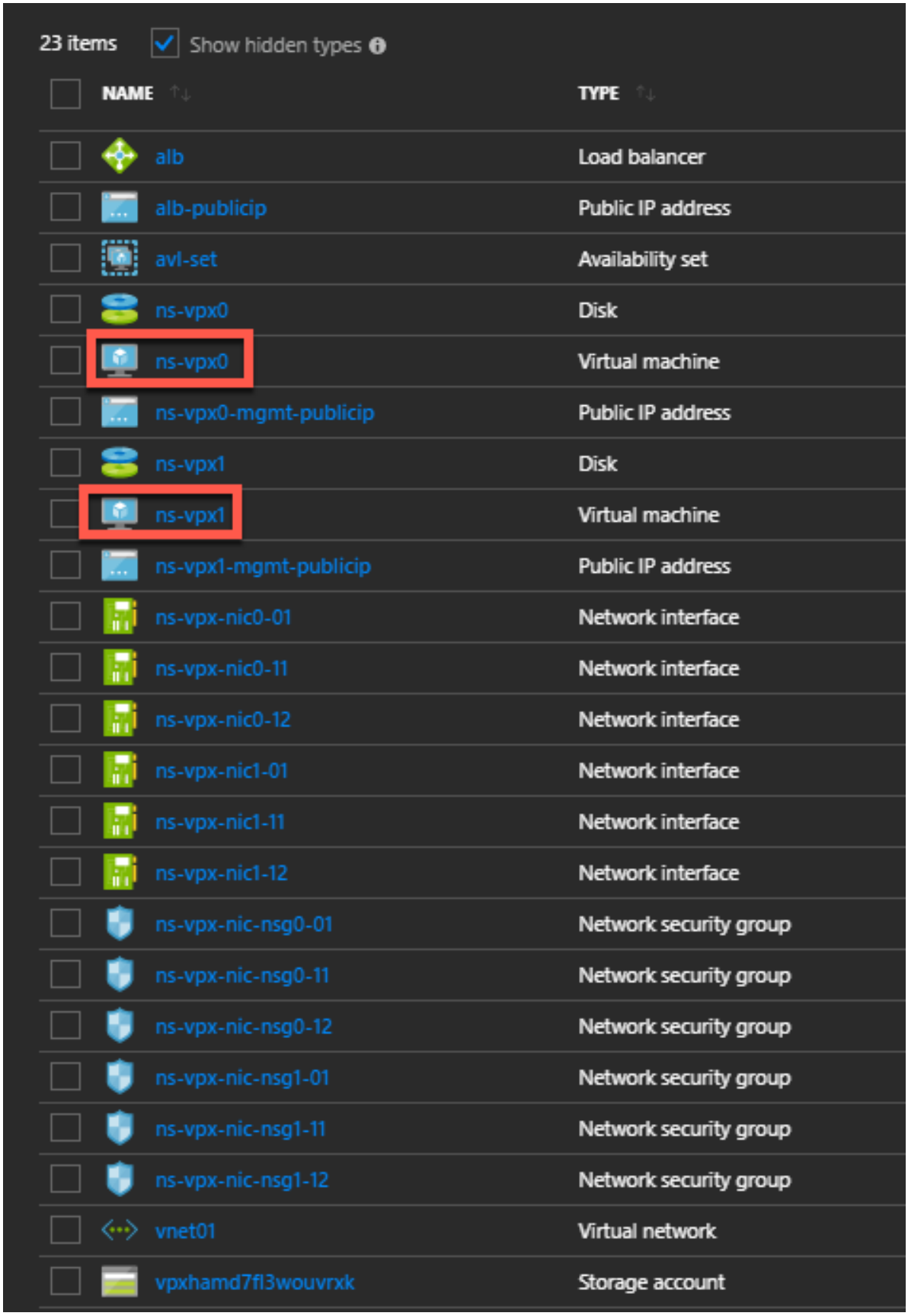
6. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.



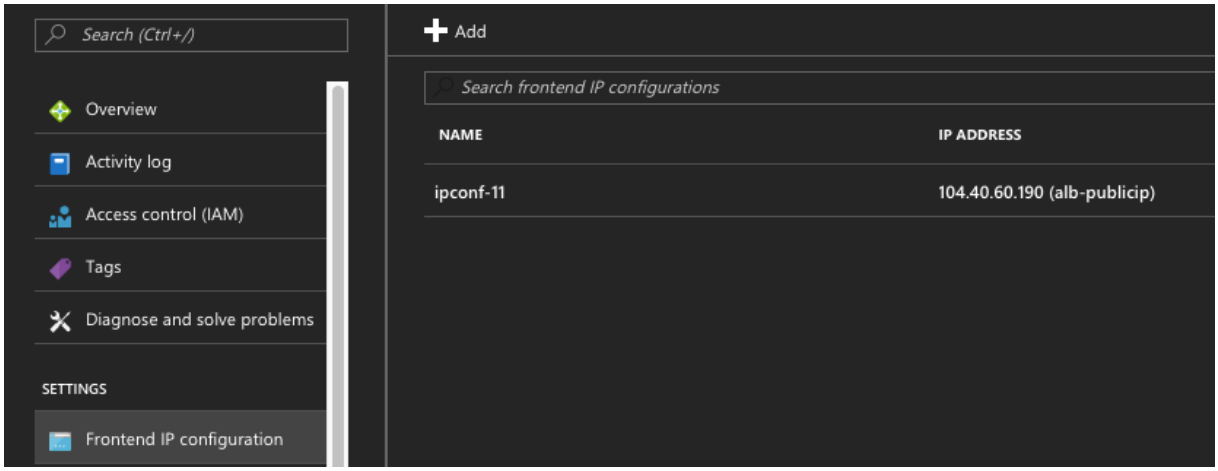
7. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez-la en conséquence. Sélectionnez **OK** pour confirmer.
8. La page **Acheter** s'affiche. Sélectionnez **Acheter** pour terminer le déploiement.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le **groupe de ressources** sur le portail Azure pour afficher les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.



Ensuite, vous devez configurer le serveur virtuel d'équilibrage de charge avec l'**adresse IP publique (PIP) de l'ALB**, sur le nœud principal. Pour trouver le PIP ALB, sélectionnez ALB > Configuration IP du **frontend**.



Consultez la section **Ressources** pour plus d'informations sur la façon de configurer le serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Configuration de nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

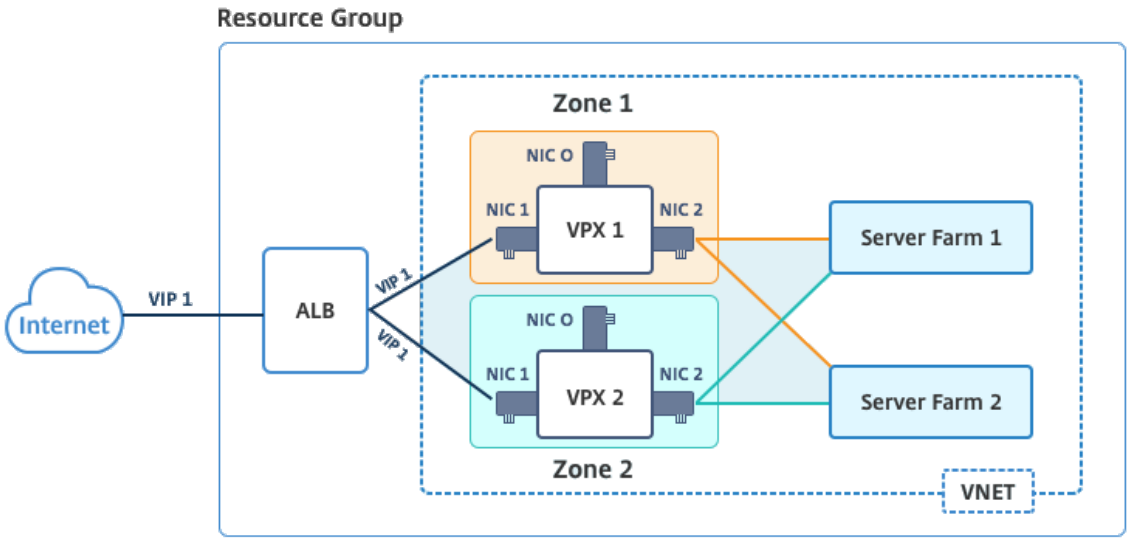
Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Haute disponibilité grâce aux zones de disponibilité

Les zones de disponibilité Azure sont des emplacements isolés de pannes dans une région Azure, fournissant une alimentation, un refroidissement et une mise en réseau redondantes et augmentant la résilience. Seules les régions Azure spécifiques prennent en charge les zones de disponibilité. Pour plus d'informations sur les régions prenant en charge les zones de disponibilité, consultez la documentation Azure Qu'est-ce que les zones de disponibilité dans Azure ?.

Diagramme : Exemple d'architecture de déploiement haute disponibilité, à l'aide de zones de disponibilité Azure



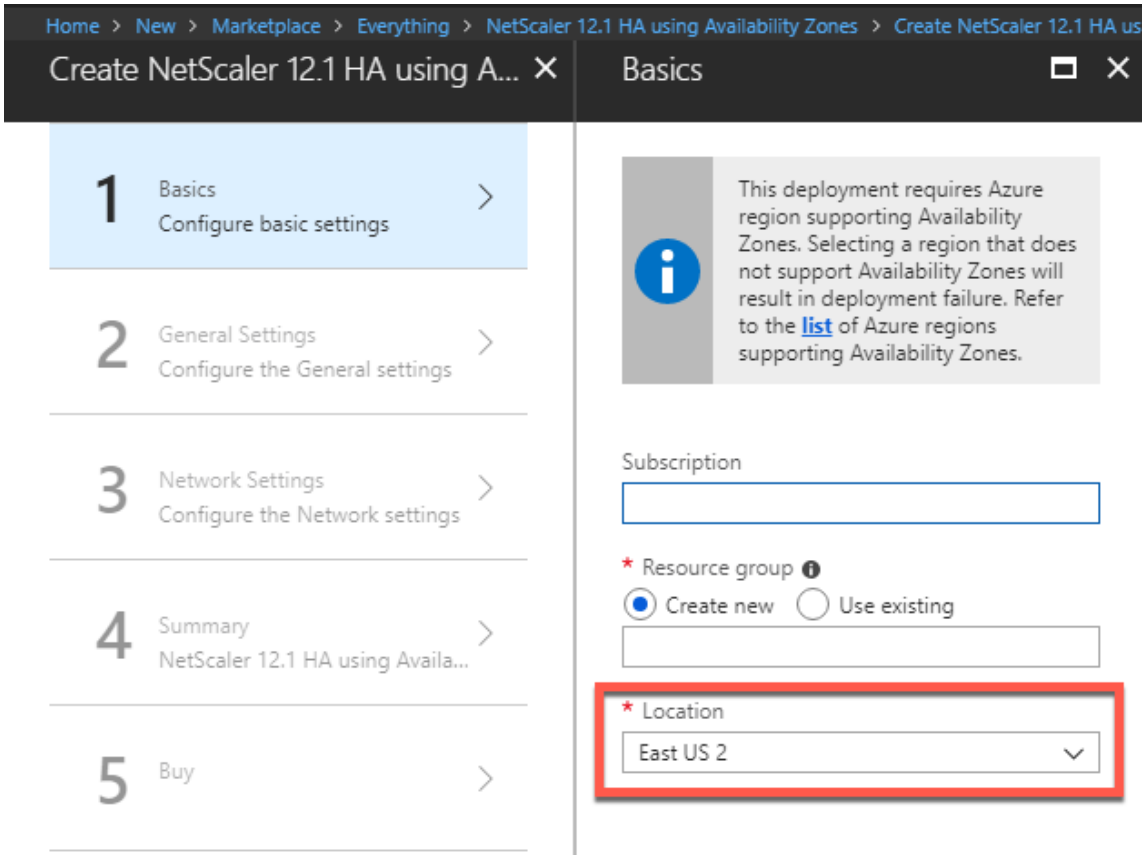
Vous pouvez déployer une paire VPX en mode haute disponibilité à l'aide du modèle intitulé « NetScaler 13.0 HA using Availability Zones », disponible sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des zones de disponibilité Azure.

1. À partir de la Place de marché Azure, sélectionnez et lancez le modèle de solution Citrix.

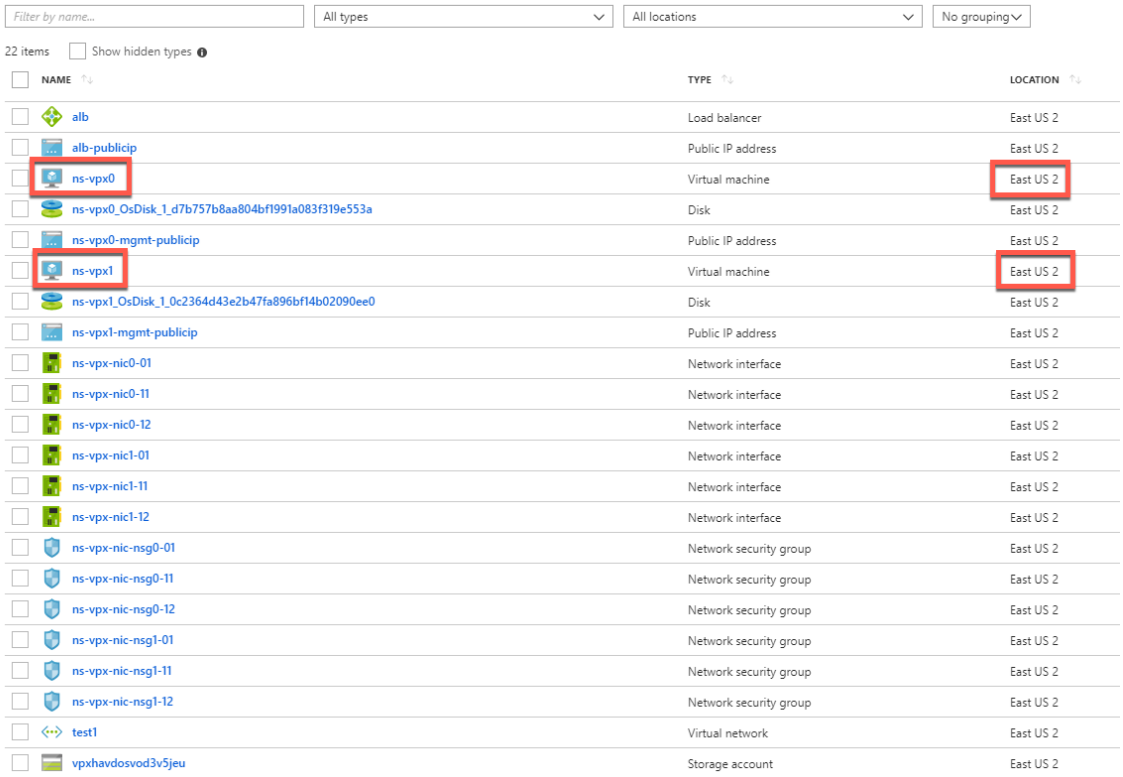
2. Assurez-vous que le type de déploiement est Resource Manager et sélectionnez **Créer**.
3. La page **Principes** de base s'affiche. Entrez les détails et cliquez sur **OK**.

> **Remarque :**
>
> Assurez-vous de sélectionner une région Azure qui prend en charge les zones de disponibilité. Pour plus d'informations sur les régions prenant en charge les zones de disponibilité, consultez la documentation Azure Qu'est-ce que les zones de disponibilité dans Azure ?



4. La page **Paramètres généraux** s'affiche. Entrez les détails et sélectionnez **OK**.
5. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.
6. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez-la en conséquence. Sélectionnez **OK** pour confirmer.
7. La page **Acheter** s'affiche. Sélectionnez **Acheter** pour terminer le déploiement.

   Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois l'opération terminée, sélectionnez le **groupe de ressources** pour voir les détails de configuration, tels que les règles LB, les pools principaux, les sondes de santé, etc., sur le portail Azure. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1. Vous pouvez également voir l'emplacement dans la colonne **Emplacement** .



Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Surveillez vos instances à l'aide de mesures dans Azure Monitor

Vous pouvez utiliser les métriques de la plateforme de données Azure Monitor pour surveiller un ensemble de ressources NetScaler VPX telles que le processeur, l'utilisation de la mémoire et le débit. Le service Metrics surveille les ressources NetScaler VPX qui s'exécutent sur Azure, en temps réel. Vous pouvez utiliser **Metrics Explorer** pour accéder aux données collectées. Pour plus d'informations, reportez-vous à la section Présentation des mesures Azure Monitor.

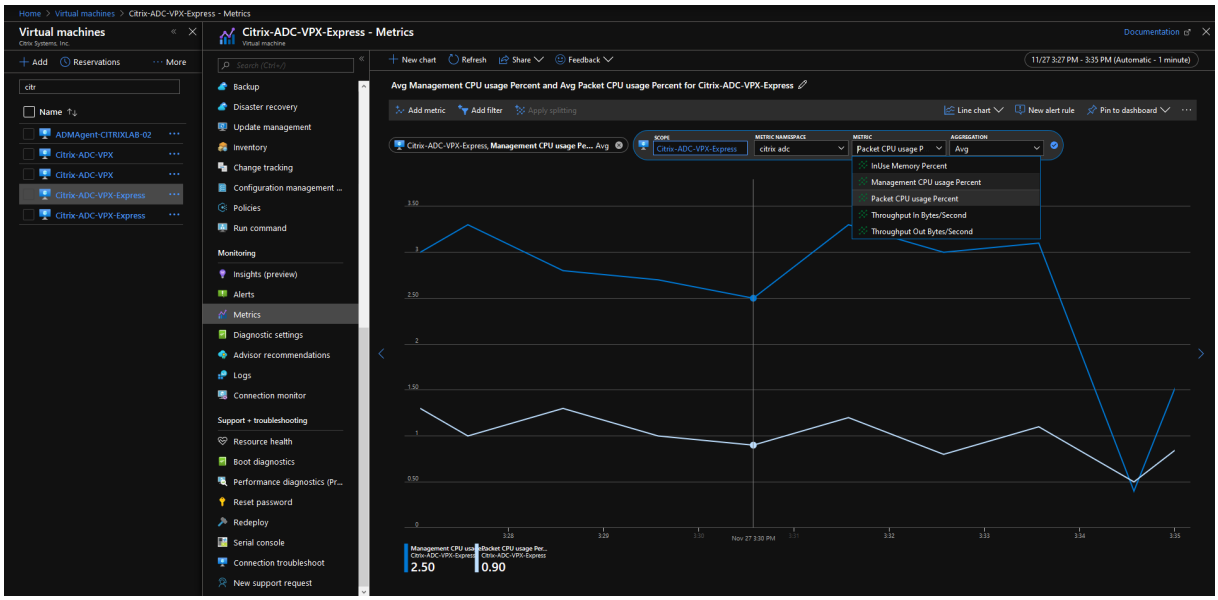
Points à noter

- Si vous déployez une instance NetScaler VPX sur Azure à l'aide de l'offre Azure Marketplace, le service Metrics est désactivé par défaut.
- Le service Metrics n'est pas pris en charge dans Azure CLI.
- Les métriques sont disponibles pour le processeur (gestion et utilisation du processeur par paquets), la mémoire et le débit (entrant et sortant).

Comment afficher les mesures dans Azure Monitor

Pour afficher les mesures dans Azure Monitor pour votre instance, effectuez les opérations suivantes :

1. Connectez-vous à **Azure Portal > Machines virtuelles**.
2. Sélectionnez la machine virtuelle qui est le nœud principal.
3. Dans la section **Surveillance**, cliquez sur **Mesures**.
4. Dans le menu déroulant **Metric Namespace**, cliquez sur **NetScaler**.
5. Sous **Toutes les mesures** dans le menu déroulant **Mesures**, cliquez sur les mesures que vous souhaitez afficher.
6. Cliquez sur **Ajouter une mesure** pour afficher une autre mesure sur le même graphique. Utilisez les options du graphique pour personnaliser votre graphique.



Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

October 17, 2024

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

Un déploiement actif-passif nécessite :

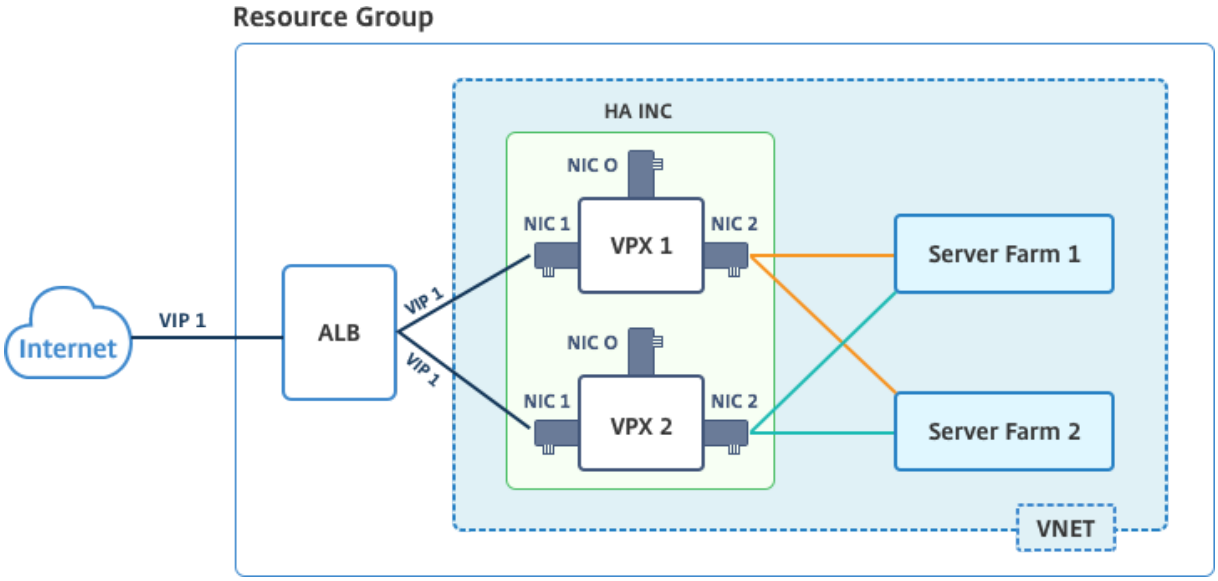
- Configuration de réseau indépendant HA (Independent Network Configuration)

- Azure Load Balancer (ALB) en mode Direct Server Return (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque :**
>
> Pour qu'un déploiement de haute disponibilité de NetScaler VPX sur un cloud Azure fonctionne, vous avez besoin d'une adresse IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds de haute disponibilité. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Schéma : Exemple d'architecture de déploiement actif-passif



Dans un déploiement actif-passif, les adresses IP publiques flottantes (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

ALB surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes et redirige le trafic vers cette instance uniquement qui envoie la réponse des sondes de santé à intervalles réguliers. Ainsi, dans une configuration HA, le nœud principal répond aux sondes d'intégrité et le nœud secondaire ne le fait pas. Si les instances principales manquent deux sondes de santé consécutives, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps de basculement total qui peut prendre pour la commutation de trafic peut être de 13 secondes maximum.

Vous pouvez déployer une paire VPX dans une configuration HA actif-passif de deux façons à l'aide de :

- **Modèle de haute disponibilité standard NetScaler VPX** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.
- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonction des exigences de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA active-passive à l'aide des commandes PowerShell. Si vous souhaitez utiliser le modèle NetScaler VPX Standard HA, consultez Configuration d'une configuration HA avec plusieurs adresses IP et cartes réseau.

Configurer les nœuds HA-INC à l'aide des commandes PowerShell

Scénario : déploiement PowerShell HA-INC

Dans ce scénario, vous déployez une paire NetScaler VPX en utilisant la topologie indiquée dans le tableau. Chaque instance VPX contient trois cartes réseau, chaque carte réseau étant déployée dans un sous-réseau différent. Une configuration IP est attribuée à chaque carte réseau.

ALB	VPX1	VPX2
ALB est associé à l'IP publique 3 (pip3)	L'adresse IP de gestion est configurée avec IPConfig1, qui inclut une adresse IP publique (pip1) et une adresse IP privée (12.5.2.24) ; nic1 ; Mgmtsubnet=12.5.2.0/24	L'adresse IP de gestion est configurée avec IPConfig5, qui inclut une adresse IP publique (pip3) et une adresse IP privée (12.5.2.26) ; nic4 ; Mgmtsubnet=12.5.2.0/24
Les règles LB et le port configurés sont HTTP (80), SSL (443), sonde d'intégrité (9000)	L'adresse IP côté client est configurée avec IPConfig3, qui inclut une adresse IP privée (12.5.1.27) ; nic2 ; FrontendSubet=12.5.1.0/24	L'adresse IP côté client est configurée avec IPConfig7, qui inclut une adresse IP privée (12.5.1.28) ; nic5 ; FrontendSubet=12.5.1.0/24
-	L'adresse IP côté serveur est configurée avec IPConfig4, qui inclut une adresse IP privée (12.5.3.24) ; nic3 ; BackEndSubnet=12.5.3.0/24	L'adresse IP côté serveur est configurée avec IPConfig8, qui inclut une adresse IP privée (12.5.3.28) ; nic6 ; BackEndSubnet=12.5.3.0/24
-	Les règles et les ports pour NSG sont SSH (22), HTTP (80), HTTPS (443)	-

Paramètres des paramètres

Les paramètres suivants sont utilisés dans ce scénario.

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$publisher = « Citrix »

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=”dernière »

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”VPXMultiIPALB”

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$lbName= “MultiIPALB”

$frontEndConfigName1= “FrontEndIP”

$backendPoolName1= “BackendPoolHttp”

$lbRuleName1= “LBRuleHttp”

$healthProbeName= “HealthProbe”

$nsgName=”NSG-MultiIP-ALB”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Pour terminer le déploiement, procédez comme suit à l’aide des commandes PowerShell :

1. Créer un groupe de ressources, un compte de stockage et un jeu de disponibilité
2. Créer un groupe de sécurité réseau et ajouter des règles
3. Créer un réseau virtuel et trois sous-réseaux
4. Créer des adresses IP publiques
5. Créer des configurations IP pour VPX1
6. Créer des configurations IP pour VPX2
7. Créer des cartes réseau pour VPX1
8. Créer des cartes réseau pour VPX2
9. Créer VPX1
10. Créer VPX2
11. Créer ALB

Créez un groupe de ressources, un compte de stockage et un jeu de disponibilité.

```
1   New-AzureRmResourceGroup -Name $rgName -Location $locName
2
3
4   $prmStorageAccount=New-AzureRMStorageAccount -Name
       $prmStorageAccountName -ResourceGroupName $rgName -Type
       Standard_LRS -Location $locName
5
6
```



```
7   $avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
        $rgName -Location $locName
```

Créez un groupe de sécurité réseau et ajoutez des règles.

```
1   $rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
        Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 101
2
3
4   -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 80
5
6
7   $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
        Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 110
8
9
10  -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 443
11
12
13  $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
        Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 120
14
15
16  -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 22
17
18
19  $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
        Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
        $rule3
```

Créez un réseau virtuel et trois sous-réseaux.

```
1   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
        parameter value should be as per your requirement)
2
3
4   $mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        $mgmtSubnetName -AddressPrefix $mgmtSubnetRange
5
6
7   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10  $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
        $rgName -Location $locName -AddressPrefix $vNetAddressRange -
```



```
        Subnet $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13   $subnetName ="frontEndSubnet"
14
15
16   \$subnet1=\$vnet.Subnets|?{
17  \$\_.Name -eq \$subnetName }
18
19
20
21   $subnetName="backEndSubnet"
22
23
24   \$subnet2=\$vnet.Subnets|?{
25  \$\_.Name -eq \$subnetName }
26
27
28
29   $subnetName="mgmtSubnet"
30
31
32   \$subnet3=\$vnet.Subnets|?{
33  \$\_.Name -eq \$subnetName }
```

Créez des adresses IP publiques.

```
1    $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
         $rgName -DomainNameLabel $domName1 -Location $locName -
        AllocationMethod Dynamic
2
3    $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
         $rgName -DomainNameLabel $domName2 -Location $locName -
        AllocationMethod Dynamic
4
5    $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
         $rgName -DomainNameLabel $domName3 -Location $locName -
        AllocationMethod Dynamic
```

Créez des configurations IP pour VPX1.

```
1    $IpConfigName1 = "IPConfig1"
2
3
4    $IPAddress = "12.5.2.24"
5
6
7    $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
        Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
        $pip1 -Primary
8
9
10   $IPConfigName3="IPConfig-3"
```



```
11
12
13    $IPAddress="12.5.1.27"
14
15
16    $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
          Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19    $IPConfigName4 = "IPConfig-4"
20
21
22    $IPAddress = "12.5.3.24"
23
24
25    $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
          -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des configurations IP pour VPX2.

```
1     $IpConfigName5 = "IPConfig5"
2
3
4     $IPAddress="12.5.2.26"
5
6
7     $IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
          Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
          $pip2 -Primary
8
9
10    $IPConfigName7="IPConfig-7"
11
12
13    $IPAddress="12.5.1.28"
14
15
16    $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
          Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19    $IPConfigName8="IPConfig-8"
20
21
22    $IPAddress="12.5.3.28"
23
24
25    $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
          Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des cartes réseau pour VPX1.

```
1     $nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
```



```
        $rgName -Location $locName -IpConfiguration $IpConfig1 -
        NetworkSecurityGroupId $nsg.Id
2
3
4   $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig3 -
        NetworkSecurityGroupId $nsg.Id
5
6
7   $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig4 -
        NetworkSecurityGroupId $nsg.Id
```

Créez des cartes réseau pour VPX2.

```
1   $nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig5 -
        NetworkSecurityGroupId $nsg.Id
2
3
4   $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig7 -
        NetworkSecurityGroupId $nsg.Id
5
6
7   $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig8 -
        NetworkSecurityGroupId $nsg.Id
```

Créez VPX1.

Cette étape comprend les sous-étapes suivantes :

- Créer un objet de configuration de machine virtuelle
- Définir les informations d'identification, le système d'exploitation et l'image
- Ajouter des cartes réseau
- Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
1    $suffixNumber = 1
2
3    $vmName=$vmNamePrefix + $suffixNumber
4
5    $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
         AvailabilitySetId $avSet.Id
6
7    $cred=Get-Credential -Message "Type the name and password for
         VPX login."
8
9    $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
         ComputerName $vmName -Credential $cred
10
```



```
    $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
        $publisher -Offer $offer -Skus $sku -Version $version

    $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1
       .Id -Primary

    $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2
       .Id

    $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3
       .Id

    $osDiskName=$vmName + "-" + $osDiskSuffix1

    $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +
        "vhds/" + $osDiskName + ".vhd"

    $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -
       VhdUri $osVhdUri -CreateOption fromImage

    Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product
       $offer -Name $sku

    New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -
       Location $locName
```

Créez VPX2.

```
```
  $suffixNumber=2

  $vmName=$vmNamePrefix + $suffixNumber

  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
     AvailabilitySetId $avSet.Id

  $cred=Get-Credential -Message "Type the name and password for VPX
     login."

  $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
     ComputerName $vmName -Credential $cred

  $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
     $publisher -Offer $offer -Skus $sku -Version $version

  $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
     Primary
```

 
```

```
21
22
23    $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
26    $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
29    $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32    $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
          /" + $osDiskName + ".vhd"
33
34
35    $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
          $osVhdUri -CreateOption fromImage
36
37
38    Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
          -Name $sku
39
40
41    New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
          $locName
42 ```
```

Pour afficher les adresses IP privées et publiques affectées aux cartes réseau, tapez les commandes suivantes :

```
1  ```
2    $nic1.IPConfig
3
4
5    $nic2.IPConfig
6
7
8    $nic3.IPConfig
9
10
11   $nic4.IPConfig
12
13
14   $nic5.IPConfig
15
16
17   $nic6.IPConfig
18 ```
```

Créer un équilibrage de charge Azure (ALB).

Cette étape comprend les sous-étapes suivantes :

- Création d'une configuration IP frontale
- Créer une sonde de santé
- Créer un pool d'adresses back-end
- Créer des règles d'équilibrage de charge (HTTP et SSL)
- Créer un ALB avec la configuration IP frontale, le pool d'adresses backend et la règle LB
- Associer la configuration IP à des pools dorsaux

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name
$frontEndConfigName1 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
 -Protocol Tcp -Port 9000 –IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -
Name $backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1
 -FrontendIpConfiguration $frontEndIP1 -BackendAddressPool
$beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
80 -BackendPort 80 -EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
$lbName -Location $locName -FrontendIpConfiguration $frontEndIP1
-LoadBalancingRule $lbRule1 -BackendAddressPool $beAddressPool1 -
Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb
.BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb
.BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

Une fois que vous avez déployé avec succès la paire NetScaler VPX, connectez-vous à chaque instance VPX pour configurer les adresses HA-INC, SNIP et VIP.

1. Tapez la commande suivante pour ajouter des nœuds HA.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Ajouter des adresses IP privées de cartes réseau côté client en tant que SNIP pour VPX1 (NIC2) et VPX2 (NIC5)


```
ajouter nsip privateIPofNIC2 255.255.255.0 -type SNIP    ajouter
nsip privateIPofNIC5 255.255.255.0 -type SNIP
```

3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal avec l'adresse IP frontale (IP publique) d'ALB.

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

Ressources connexes :

Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Déployez une paire de haute disponibilité NetScaler sur Azure avec ALB en mode IP flottant désactivé

October 17, 2024

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir de nombreuses adresses IP.

Un déploiement actif-passif nécessite :

- Configuration de réseau indépendant HA (Independent Network Configuration)
- L'Azure Load Balancer (ALB) avec :
  - Mode adresse IP flottante ou mode Direct Server Return (DSR)
  - Mode adresse IP flottante désactivé

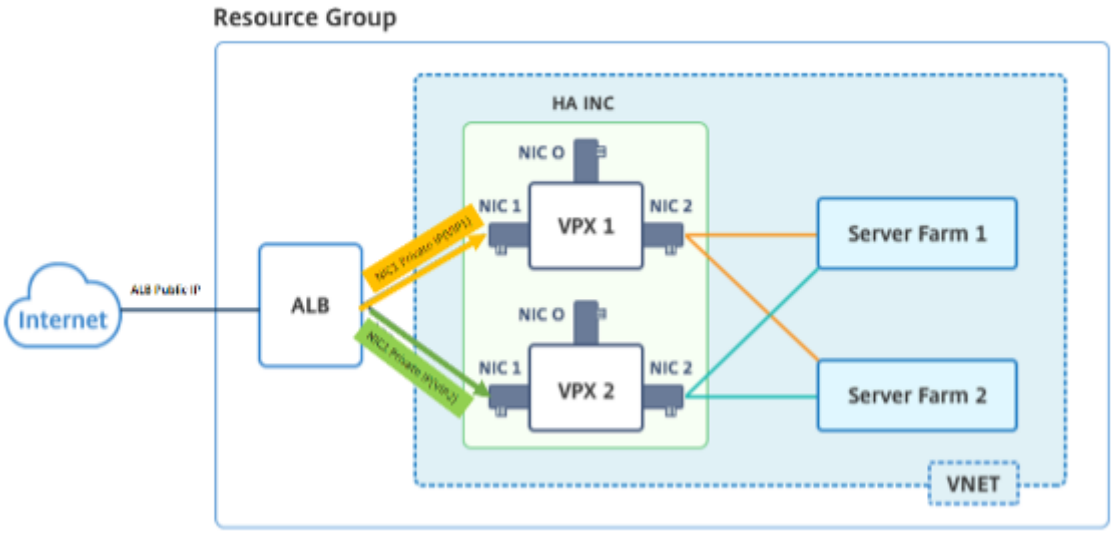
Pour plus d'informations sur les options IP flottantes ALB, consultez la documentation Azure.

Si vous souhaitez déployer une paire VPX dans une configuration HA active-passive sur Azure avec l'IP flottante ALB activée, consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell.

Architecture de déploiement HA avec ALB en mode adresse IP flottante désactivé

Dans un déploiement actif-passif, les adresses IP privées de l'interface client de chaque instance sont ajoutées en tant qu'adresses VIP dans chaque instance VPX. Configurez en mode HA-INC avec des adresses VIP partagées à l'aide d'IPSet et des adresses SNIP spécifiques à une instance. L'ensemble du trafic passe par l'instance principale. L'instance secondaire est en mode veille jusqu'à ce que l'instance principale tombe en panne.

Schéma : Exemple d'architecture de déploiement actif-passif



Conditions préalables

Vous devez connaître les informations suivantes avant de déployer une instance NetScaler VPX sur Azure.

- Terminologie Azure et détails réseau. Pour plus d'informations, consultez Terminologie Azure.
- Fonctionnement d'une appliance NetScaler. Pour plus d'informations, consultez la documentation de NetScaler.
- Réseau NetScaler. Pour plus d'informations, consultez la section Réseau ADC.
- Configuration de l'équilibreur de charge Azure et des règles d'équilibrage de charge. Pour plus d'informations, consultez la documentation Azure ALB.

Comment déployer une paire VPX HA sur Azure avec l'IP flottante ALB désactivée

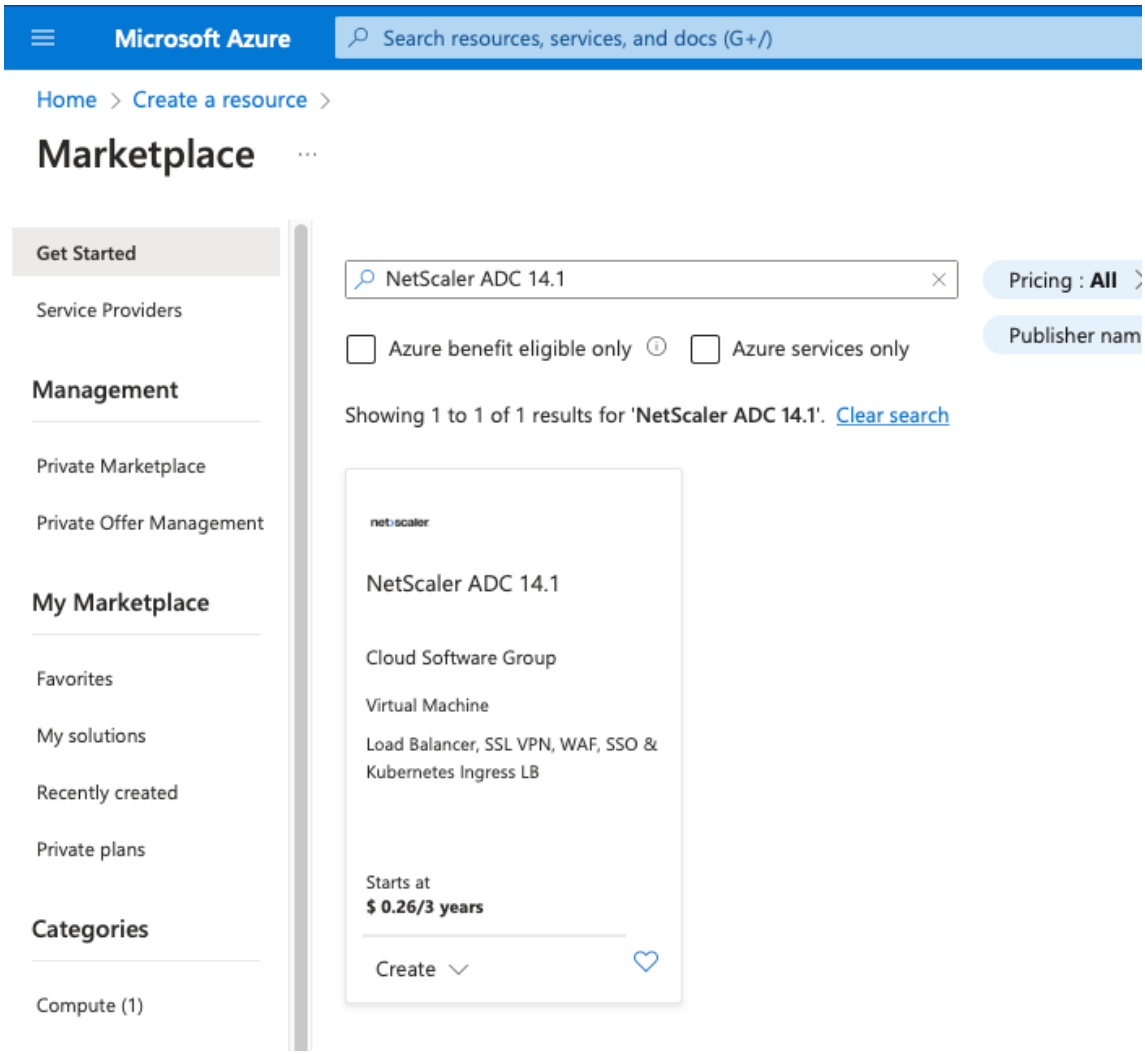
Voici un résumé des étapes de déploiement HA et ALB :

1. Déployez deux instances VPX (instances principales et secondaires) sur Azure.
2. Ajoutez une carte réseau client et serveur sur les deux instances.
3. Déployez un ALB avec une règle d'équilibrage de charge dont le mode adresse IP flottante est désactivé.
4. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler.

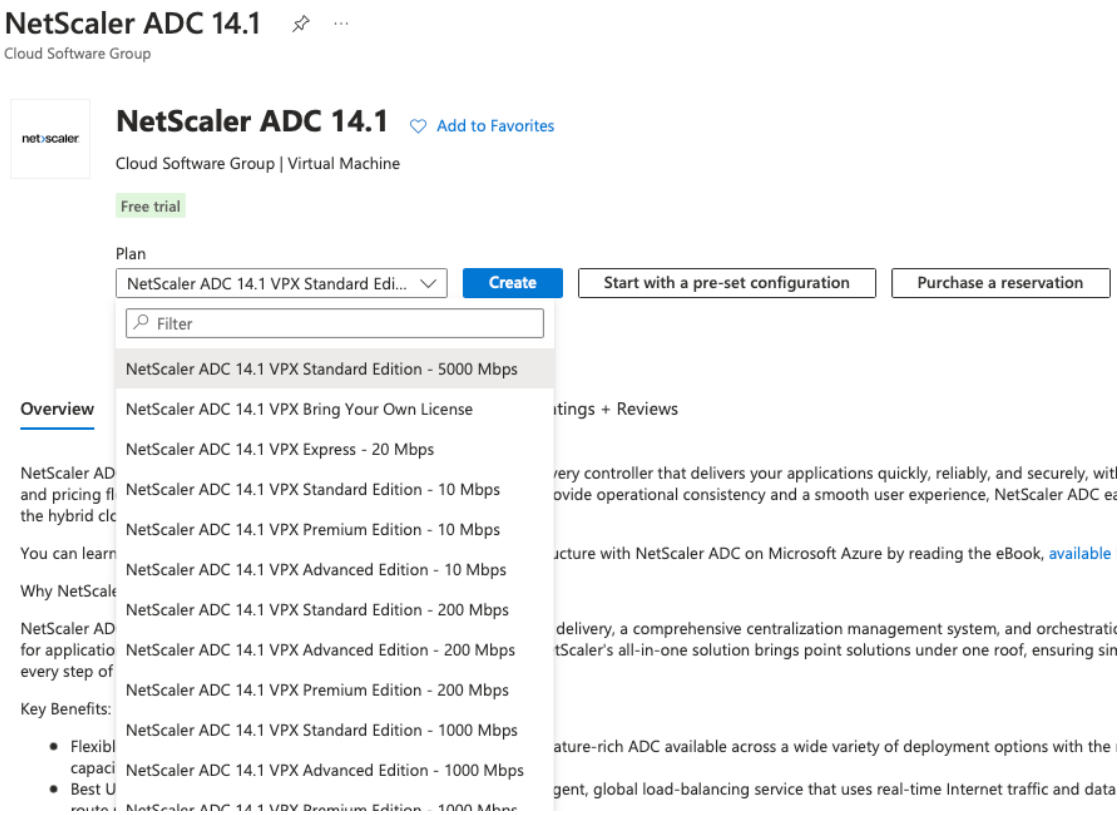
Étape 1. Déployez deux instances VPX sur Azure.

Créez deux instances VPX en suivant ces étapes :

1. Sélectionnez la version de NetScaler sur Azure Marketplace (dans cet exemple, la version 13.1 de NetScaler est utilisée).

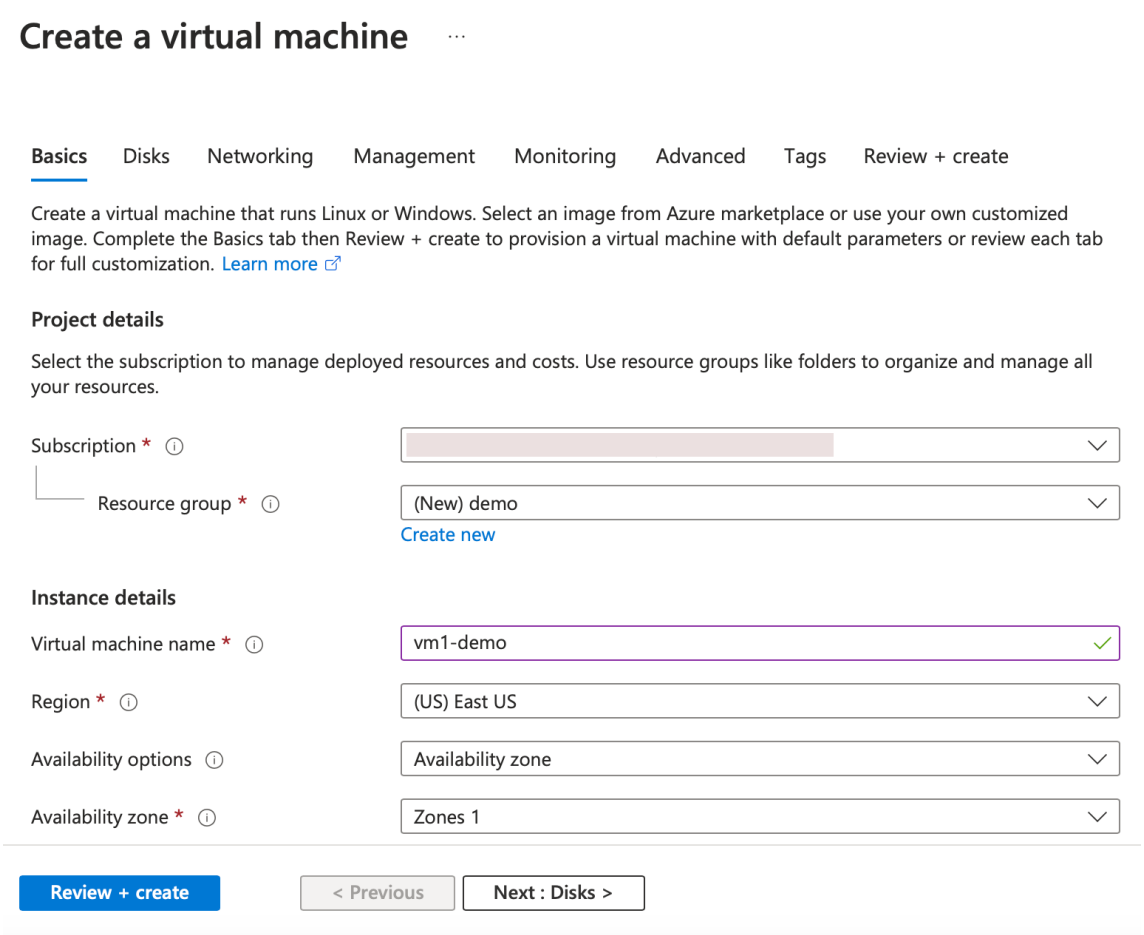


2. Sélectionnez le mode de licence ADC requis, puis cliquez sur **Créer**.



La page **Créer une machine virtuelle** s'ouvre.

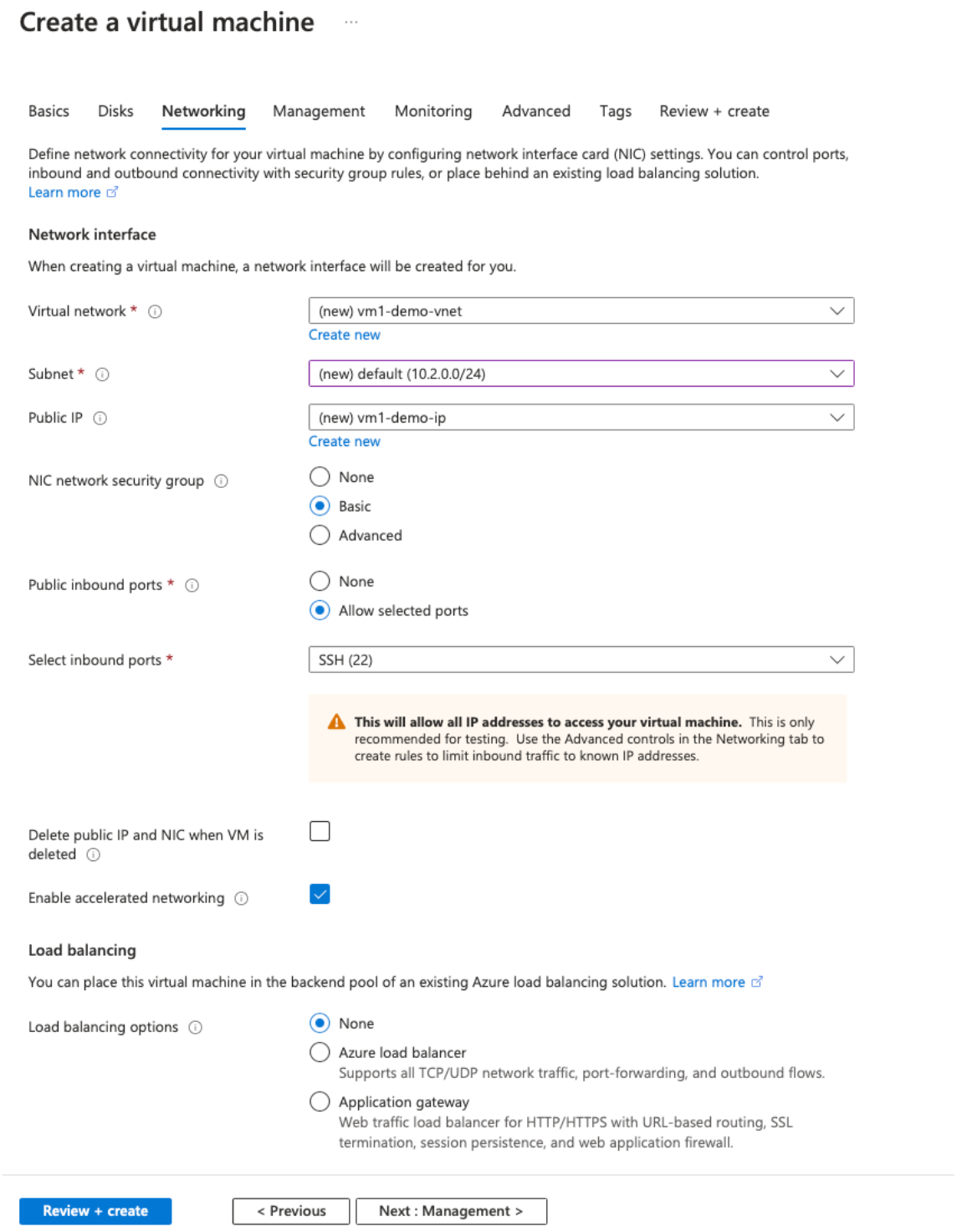
3. Renseignez les informations requises dans chaque onglet : Notions de base, disques, mise en réseau, gestion, surveillance, avancées et balises, pour un déploiement réussi.



Dans l'onglet **Mise en réseau**, créez un nouveau réseau virtuel avec 3 sous-réseaux, un pour chacun : les cartes réseau de gestion, de client et de serveur. Sinon, vous pouvez également utiliser un réseau virtuel existant. La carte réseau de gestion est créée lors du déploiement de la VM. Les cartes réseau client et serveur sont créées et attachées après la création de la machine virtuelle. Pour le groupe de sécurité réseau de la carte réseau, vous pouvez effectuer l'une des opérations suivantes :

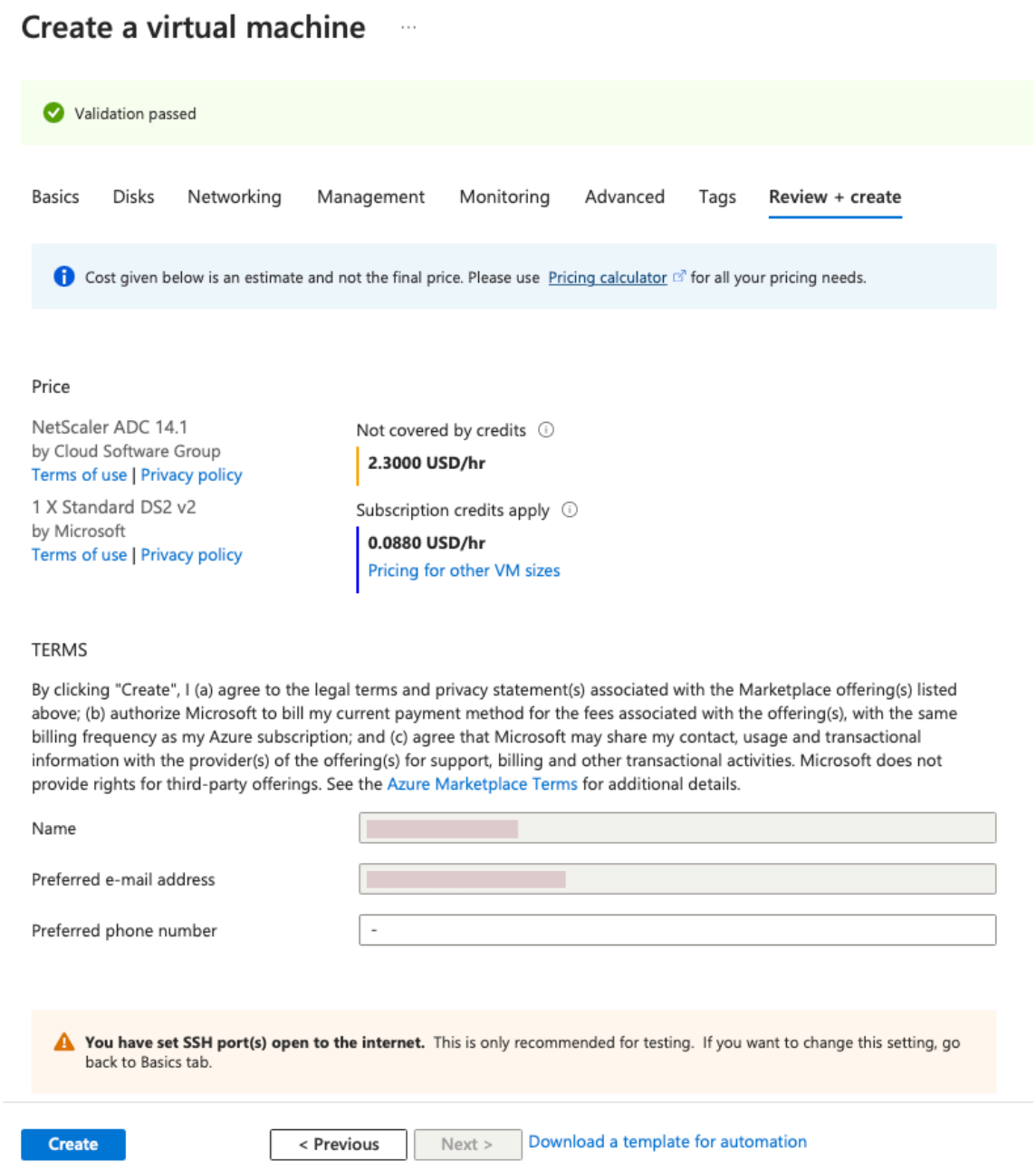
- Sélectionnez **Avancé** et utilisez un groupe de sécurité réseau existant qui répond à vos besoins.
- Sélectionnez **Basic** et sélectionnez les ports requis.

> **Remarque :**
>
> Vous pouvez également modifier les paramètres du groupe de sécurité réseau une fois le déploiement de la machine virtuelle terminé.

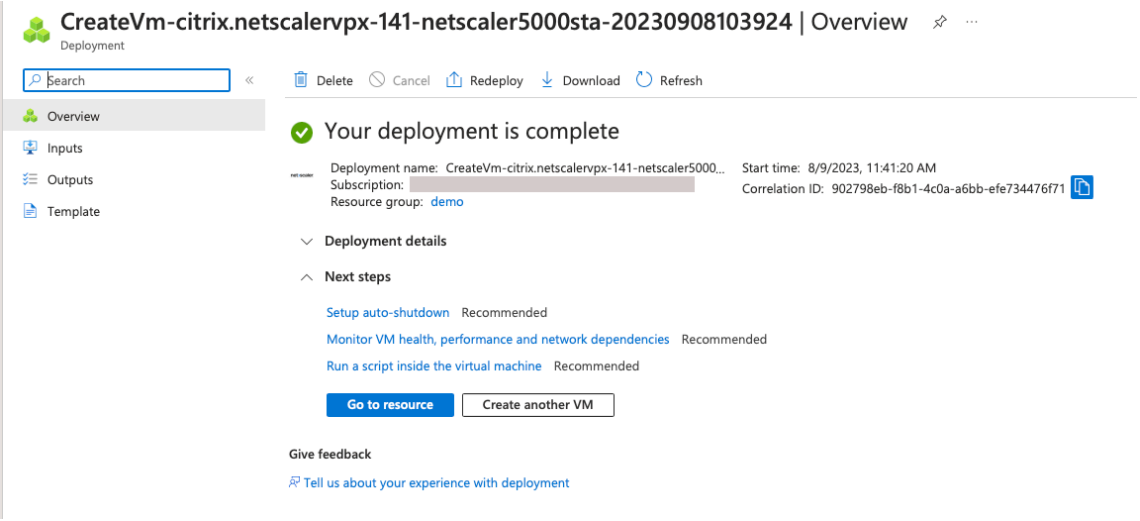


4. Cliquez sur Suivant : **Réviser + créer**.

   Une fois la validation réussie, passez en revue les paramètres de base, les configurations de machines virtuelles, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**.



5. Une fois le déploiement terminé, cliquez sur **Accéder à la ressource** pour voir les détails de configuration.



De même, déployez une seconde instance NetScaler VPX.

Étape 2. Ajoutez des cartes réseau client et serveur sur les deux instances.

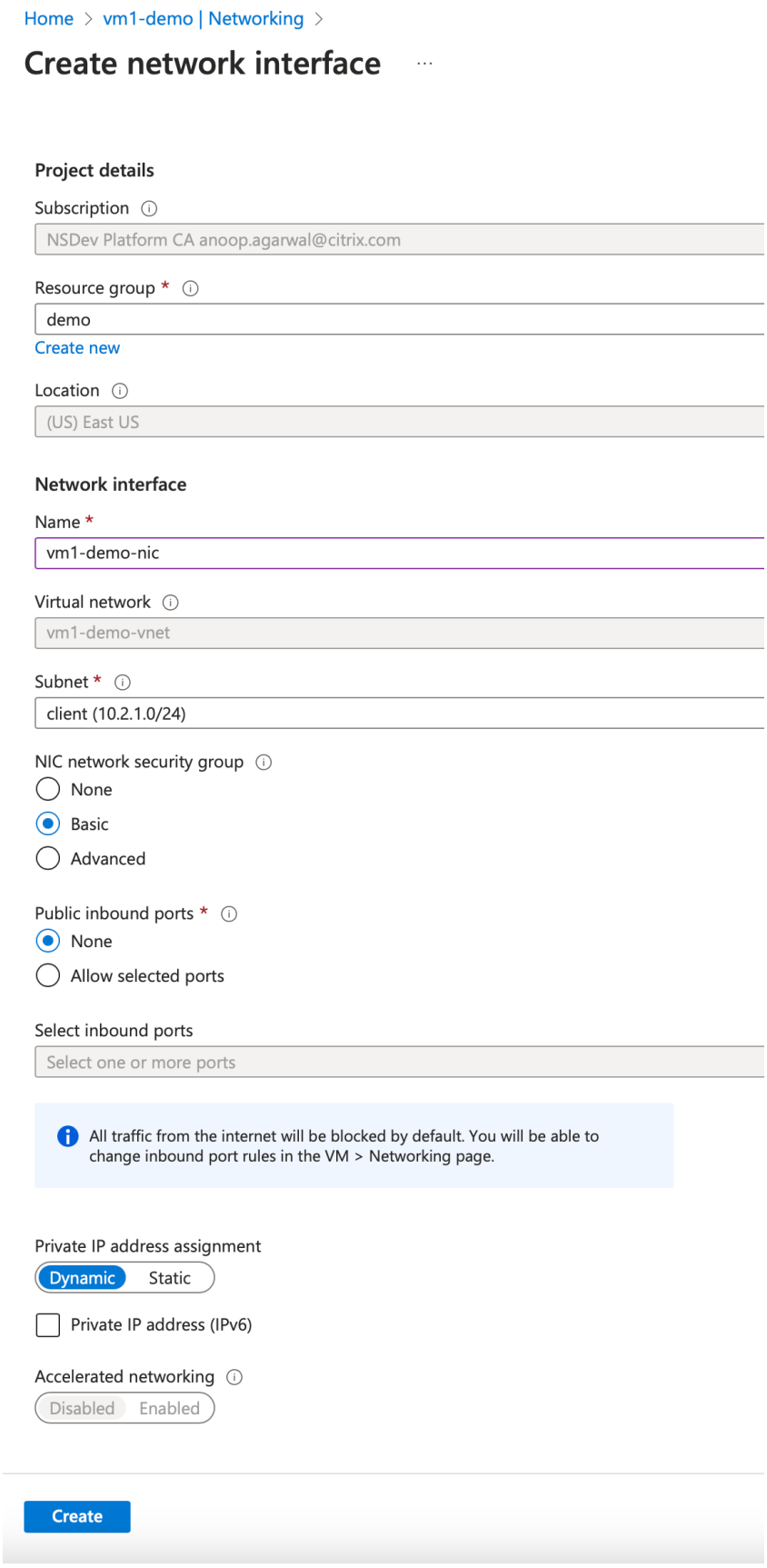
> **Remarque :**
>
> Pour associer davantage de cartes réseau, vous devez d'abord arrêter la machine virtuelle. Dans le portail Azure, sélectionnez la machine virtuelle que vous souhaitez arrêter. Dans l'onglet **Aperçu**, cliquez sur **Arrêter**. Attendez que Status indique **Stopped**.

Pour ajouter une carte réseau cliente sur l'instance principale, procédez comme suit :

1. Accédez à **Mise en réseau > Connecter une interface réseau**.

   Vous pouvez sélectionner une carte réseau existante ou créer et associer une nouvelle interface.

2. Pour le groupe de sécurité réseau de la carte réseau, vous pouvez utiliser un groupe de sécurité réseau existant en sélectionnant **Avancé** ou en créer un en sélectionnant **Basic**.



Pour ajouter une carte réseau de serveur, suivez les mêmes étapes que pour ajouter une carte réseau client.

Les trois cartes réseau (carte réseau de gestion, carte réseau client et carte réseau serveur) sont connectées à l'instance NetScaler VPX.

Répétez les étapes précédentes pour ajouter des cartes réseau sur l'instance secondaire.

Après avoir créé et attaché des cartes réseau sur les deux instances, redémarrez-les en accédant à **Overview > Start**.

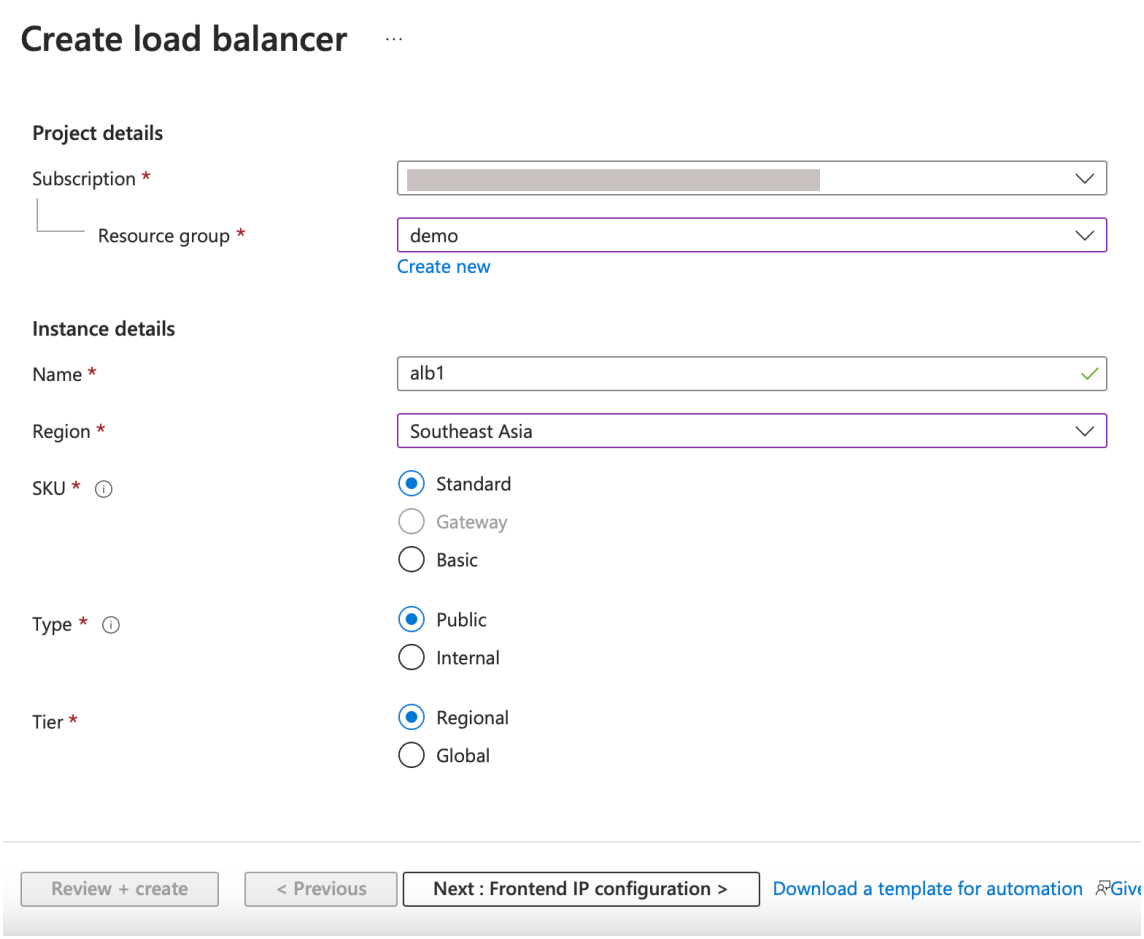
> **Remarque :**
>
> Vous devez autoriser le trafic via le port dans la règle entrante de la carte réseau cliente, qui sera utilisée ultérieurement pour créer un serveur virtuel d'équilibrage de charge lors de la configuration de l'instance NetScaler VPX.

Étape 3. Déployez un ALB avec une règle d'équilibrage de charge dont le mode adresse IP flottante est désactivé.

Pour démarrer la configuration d'ALB, procédez comme suit :

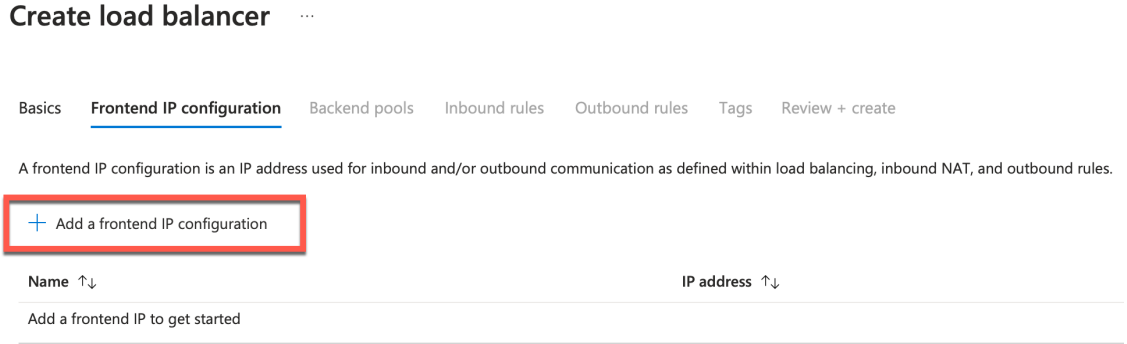
1. Accédez à la page **Load Balancers** et cliquez sur **Create**.
2. Sur la page **Créer un équilibreur** de charge, fournissez les détails nécessaires.

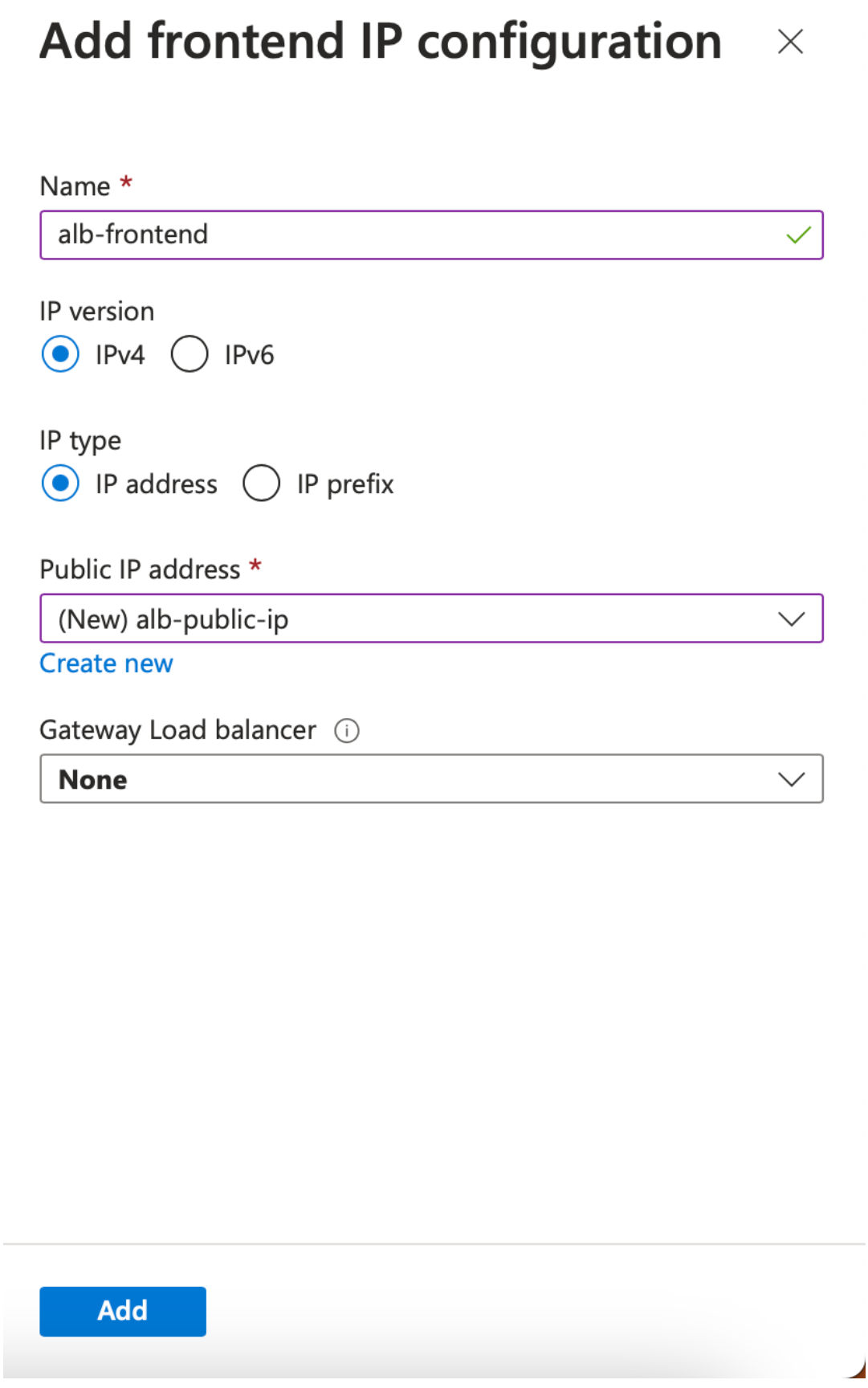
   Dans l'exemple suivant, nous déployons un équilibreur de charge public régional de SKU standard.



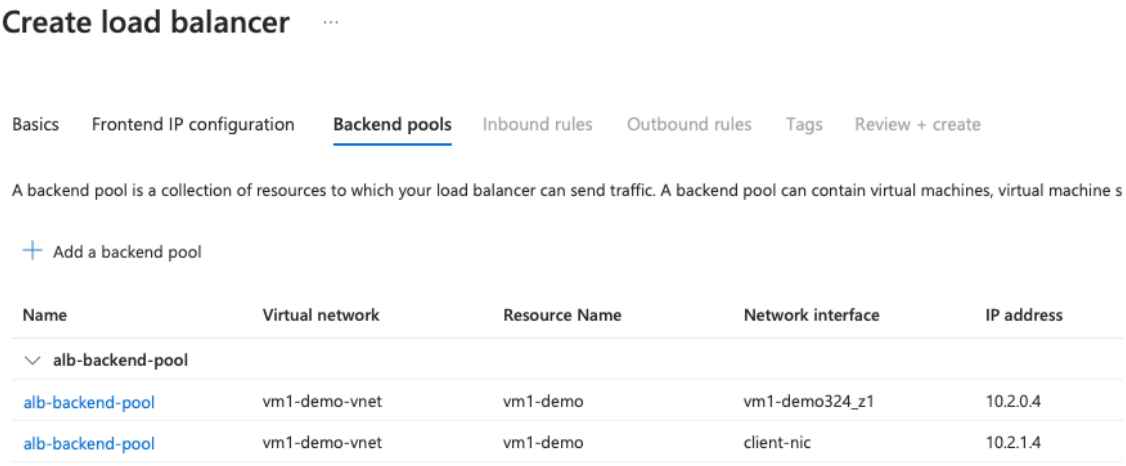
> **Remarque :**
>
> Toutes les adresses IP publiques associées aux machines virtuelles NetScaler doivent avoir le même SKU que celui d'ALB. Pour plus d'informations sur les SKU ALB, consultez la documentation des SKU de l'équilibreur de charge Azure.

3. Dans l'onglet **Configuration IP Frontend**, créez une adresse IP ou utilisez une adresse IP existante.

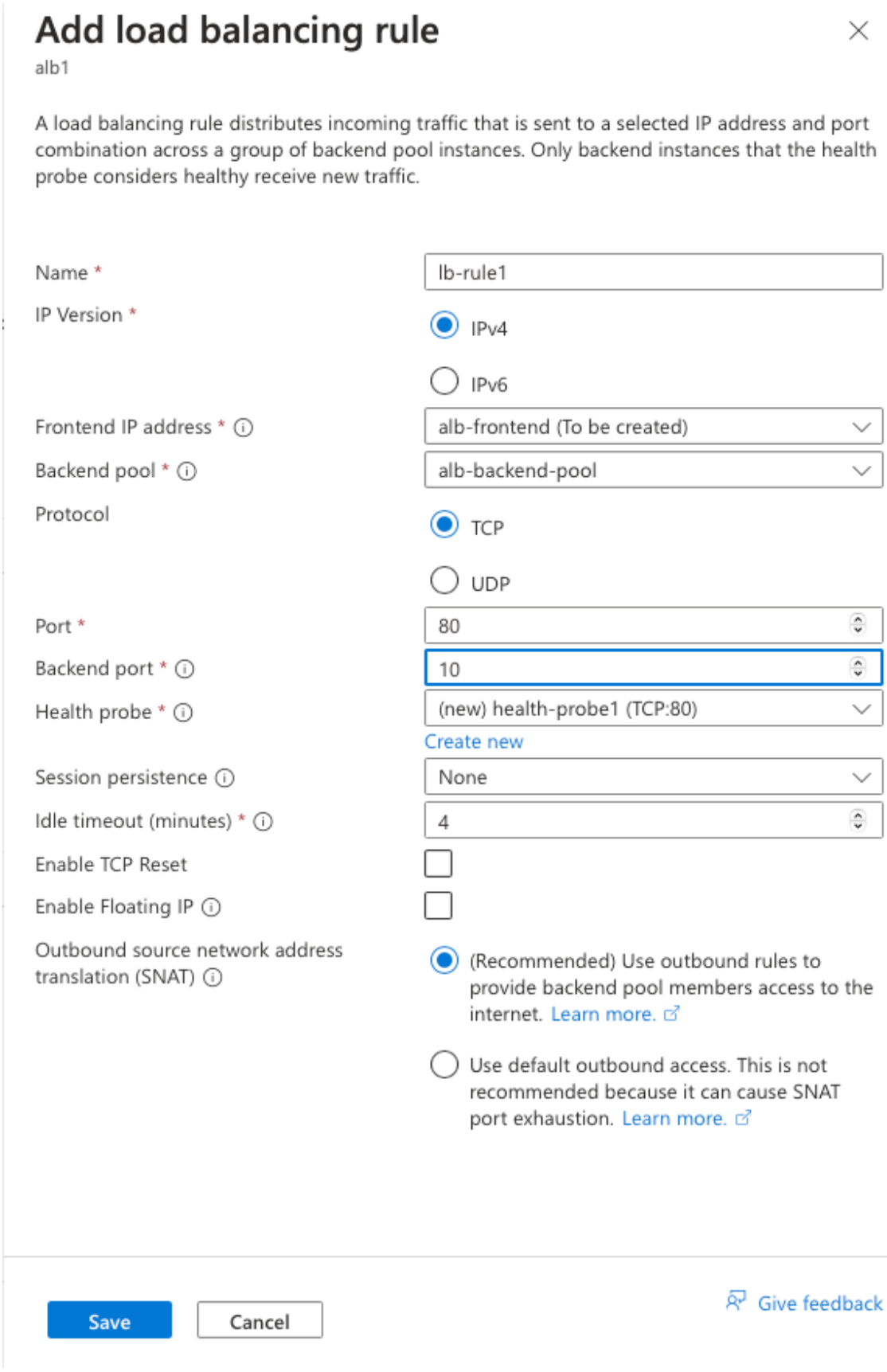




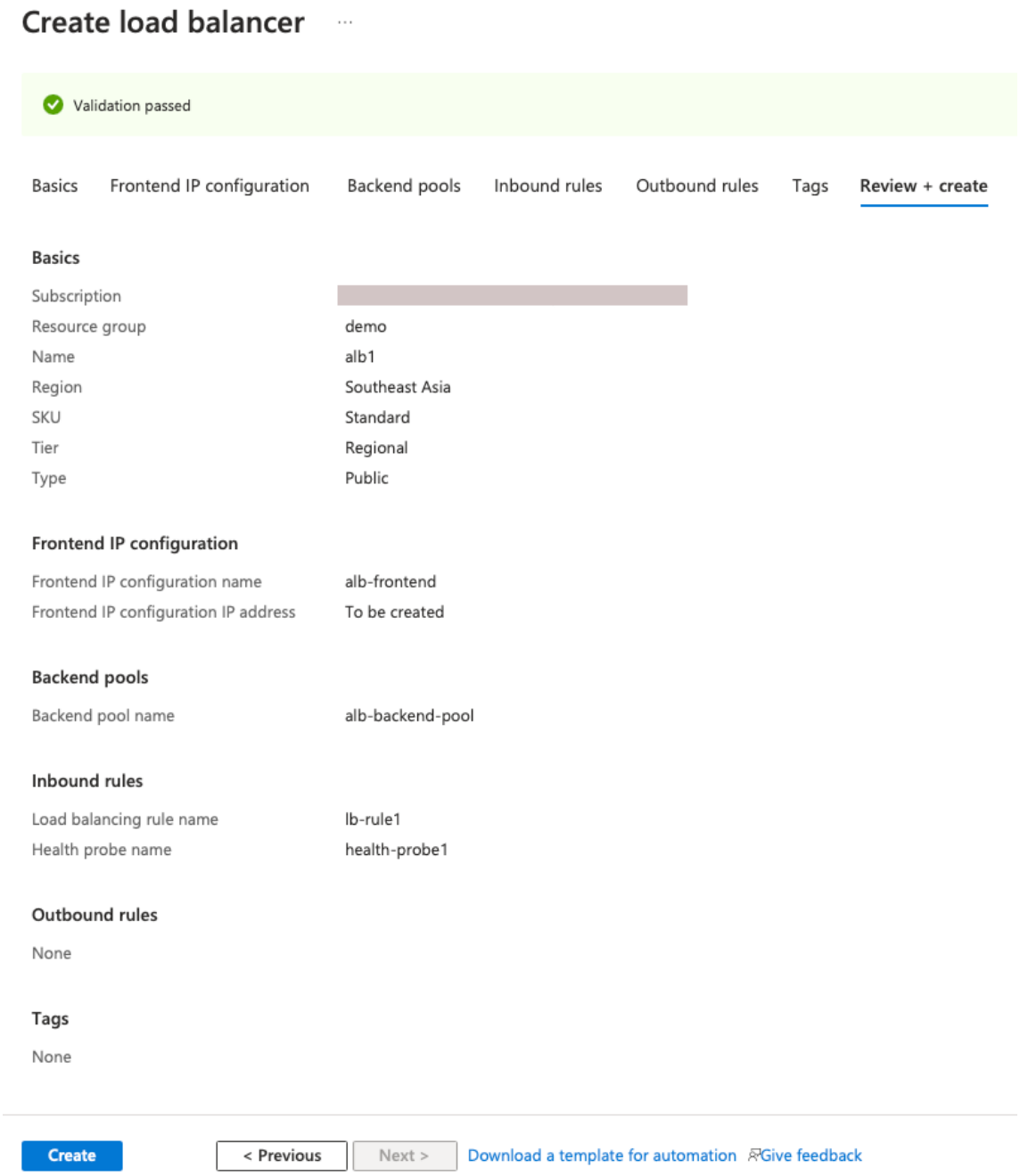
4. Dans l'onglet **Pools de backend**, sélectionnez la configuration du pool de backend basée sur les cartes réseau et ajoutez les cartes réseau clientes des deux machines virtuelles NetScaler.



5. Dans l'onglet **Inbound rules (Règles entrantes)**, cliquez sur **Add a Load balancing rule (Ajouter une**règle d'équilibrage de charge) et indiquez l'adresse IP du frontend et le pool backend créés au Sélectionnez le protocole et le port en fonction de vos besoins. Sélectionnez le protocole et le port en fonction de vos besoins. Créez ou utilisez une sonde de santé existante. Décochez la case **Activer l'adresse IP flottante** .



6. Cliquez sur **Réviser + Créer**. Une fois la validation passée, cliquez sur **Créer**.



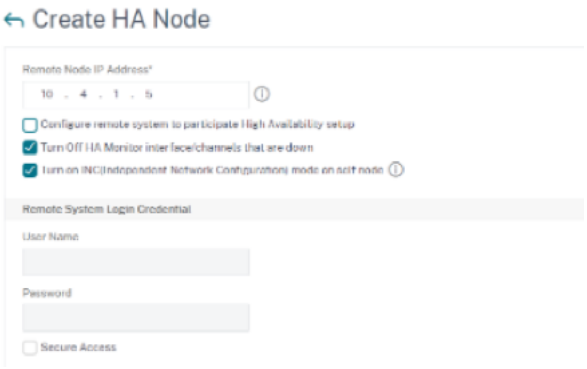
Étape 4. Configurez les paramètres HA sur les deux instances de NetScaler VPX à l'aide de l'interface graphique de NetScaler.

Après avoir créé les instances NetScaler VPX sur Azure, vous pouvez configurer HA à l'aide de l'interface graphique NetScaler.

Étape 1. Configurez la haute disponibilité en mode INC sur les deux instances.

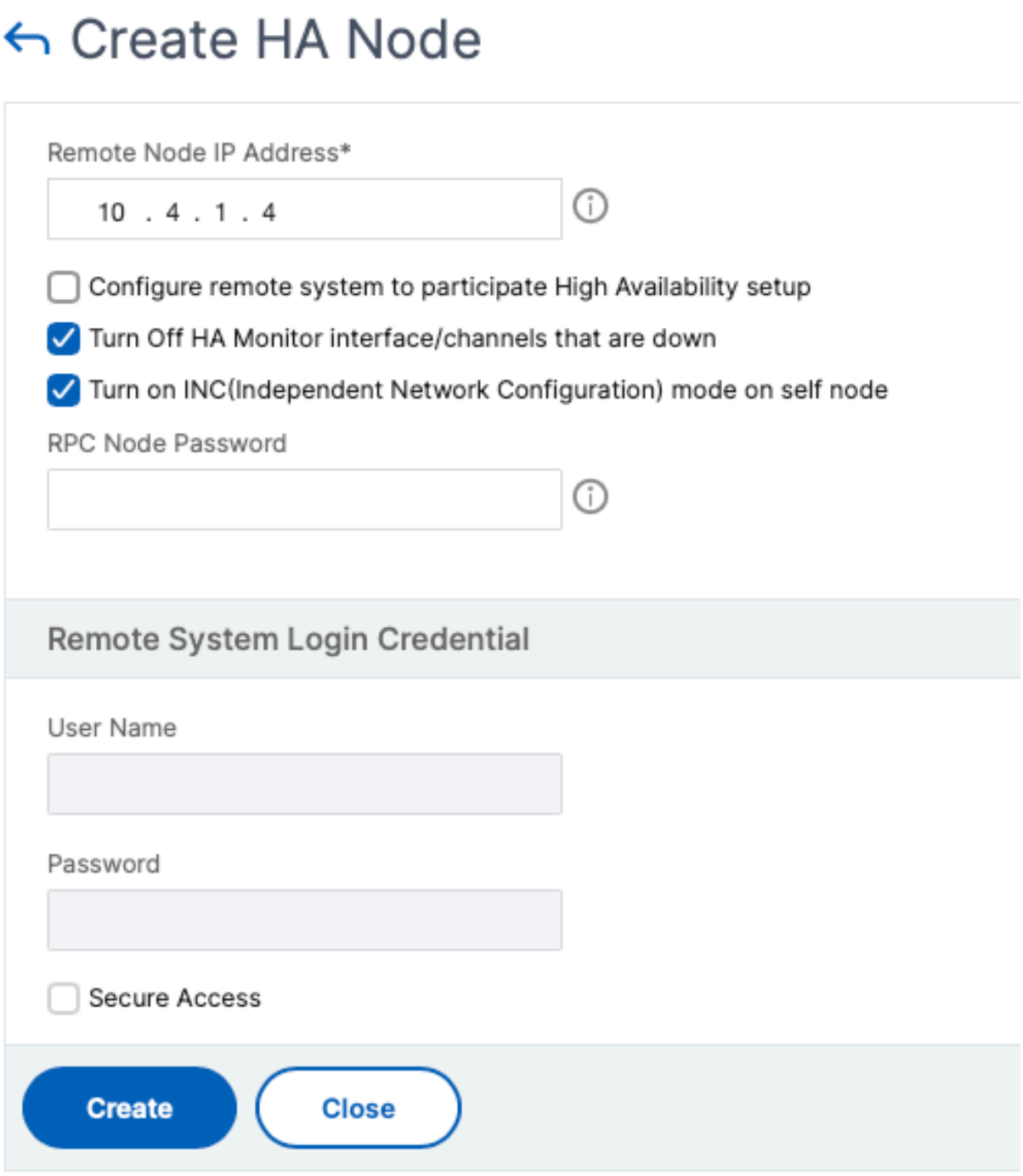
Sur l'instance principale, effectuez les étapes suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et le mot de passe fournis lors du déploiement de l'instance.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion de l'instance secondaire, par exemple : 10.4.1.5.
4. Cochez la case **Activer le mode INC (Independent Network Configuration) sur le nœud autonome** .
5. Cliquez sur **Créer**.



Sur l'instance secondaire, effectuez les étapes suivantes :

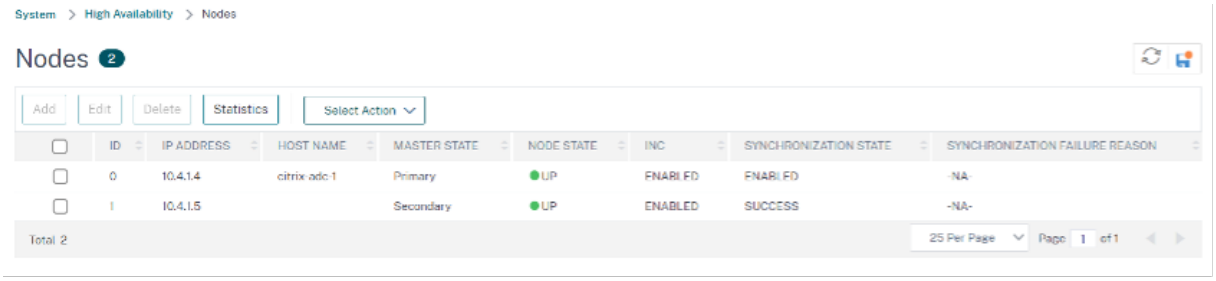
1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et le mot de passe fournis lors du déploiement de l'instance.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion de l'instance principale, par exemple : 10.4.1.4.
4. Cochez la case **Activer le mode INC (Independent Network Configuration) sur le nœud autonome** .
5. Cliquez sur **Créer**.



Avant de poursuivre, assurez-vous que l'**état de synchronisation de l'** instance secondaire est indiqué comme **SUCCESS** sur la page **Nodes** .

> **Remarque :**
>
> L'instance secondaire possède désormais les mêmes informations d'identification de connexion

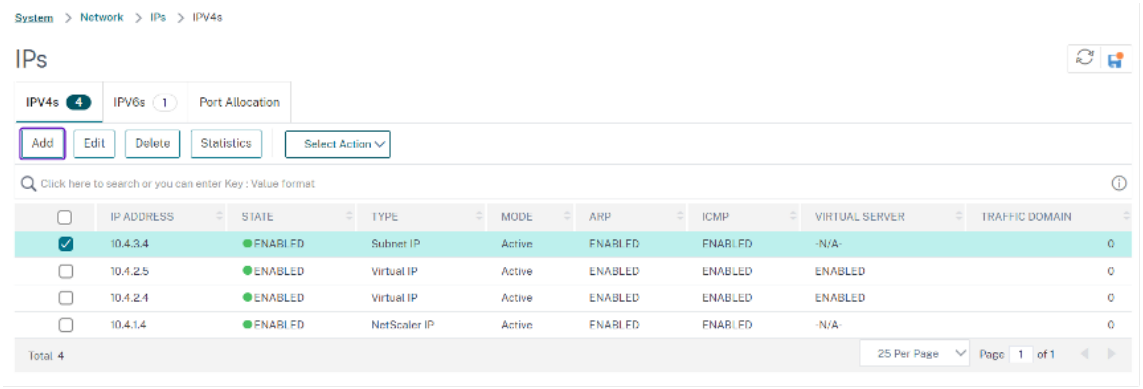
> que l'instance principale.



Étape 2. Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux instances.

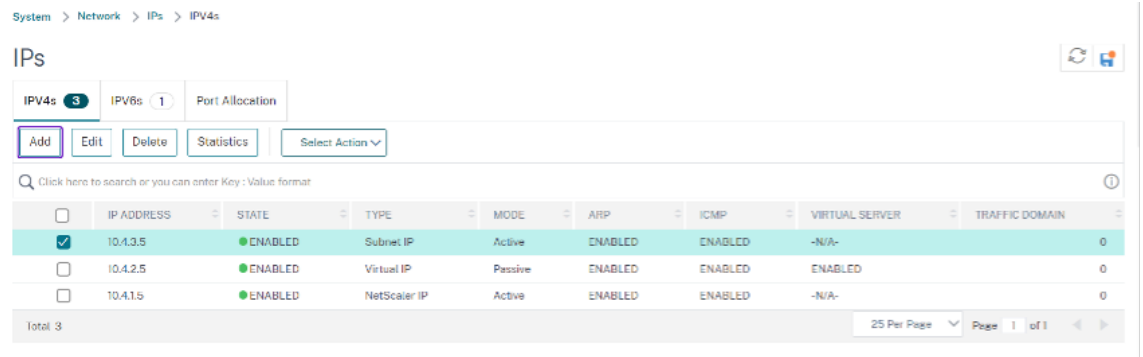
Sur l'instance principale, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP principale en procédant comme suit :
    a) Entrez l'adresse IP privée de la carte réseau client de l'instance principale et le masque réseau configuré pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.
3. Ajoutez une adresse SNIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de la carte réseau du serveur de l'instance principale et le masque réseau configuré pour le sous-réseau du serveur dans l'instance principale.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Créer**.
4. Ajoutez une adresse VIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de la carte réseau client de l'instance secondaire et le masque réseau configuré pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.



Sur l'instance secondaire, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP secondaire en procédant comme suit :
   a) Entrez l'adresse IP interne de la carte réseau client de l'instance secondaire et le masque réseau configuré pour le sous-réseau client dans l'instance de machine virtuelle.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
3. Ajoutez une adresse SNIP secondaire en procédant comme suit :
   a) Entrez l'adresse IP interne de la carte réseau du serveur de l'instance secondaire et le masque réseau configuré pour le sous-réseau du serveur dans l'instance secondaire.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Créer**.

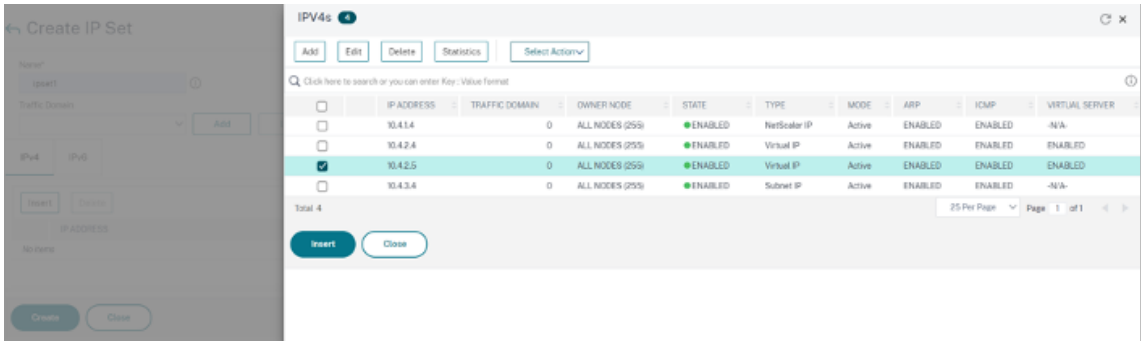


Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

Sur l'instance principale, effectuez les étapes suivantes :

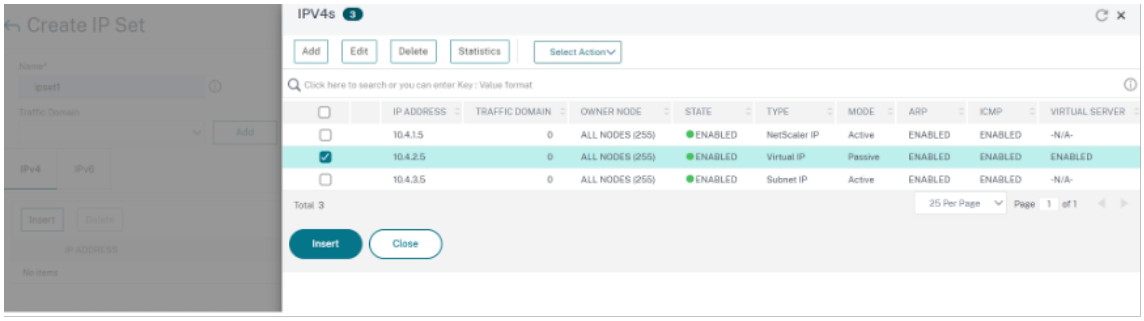
1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.

4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



Sur l'instance secondaire, effectuez les étapes suivantes :

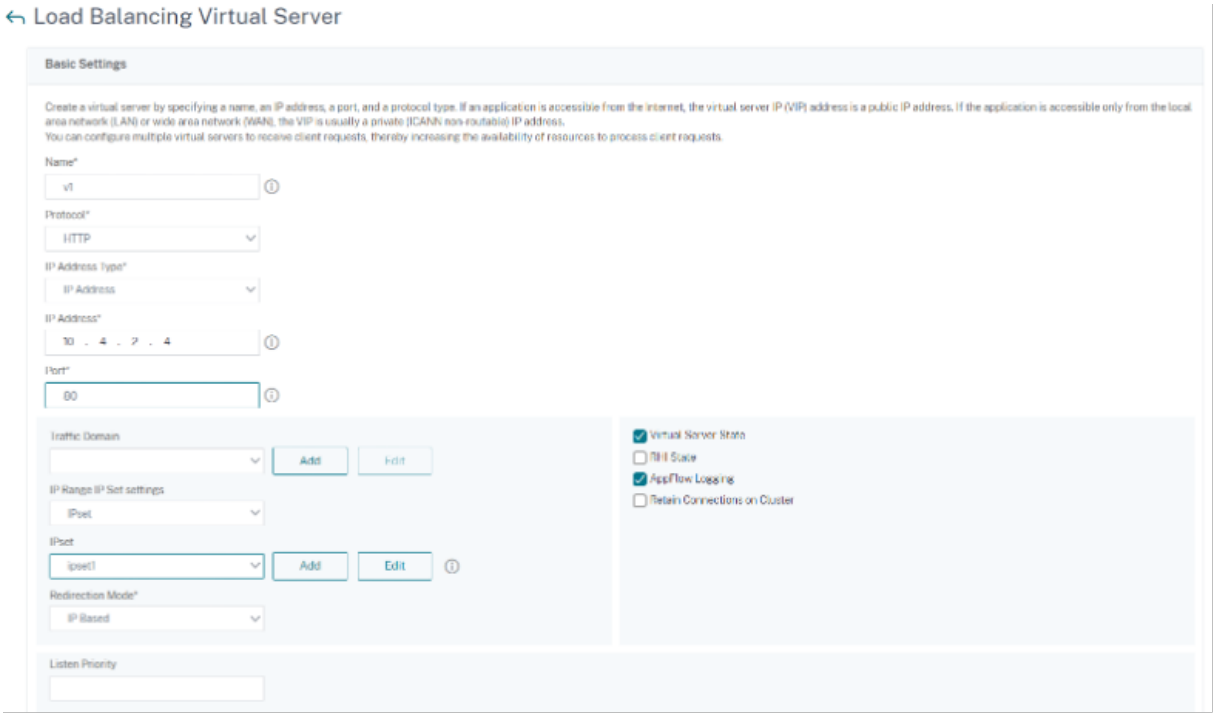
1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'adresse IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



> **Remarque :**
>
> Le nom de l'ensemble d'adresses IP doit être identique sur les instances principale et secondaire.

Étape 4. Ajoutez un serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (VIP principale) et le port.
3. Cliquez sur **Plus**. Accédez à **Paramètres du jeu d'adresses IP de plage IP**, sélectionnez **IPset** dans le menu déroulant et indiquez l'IPSet créé à l'**étape 3**.
4. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

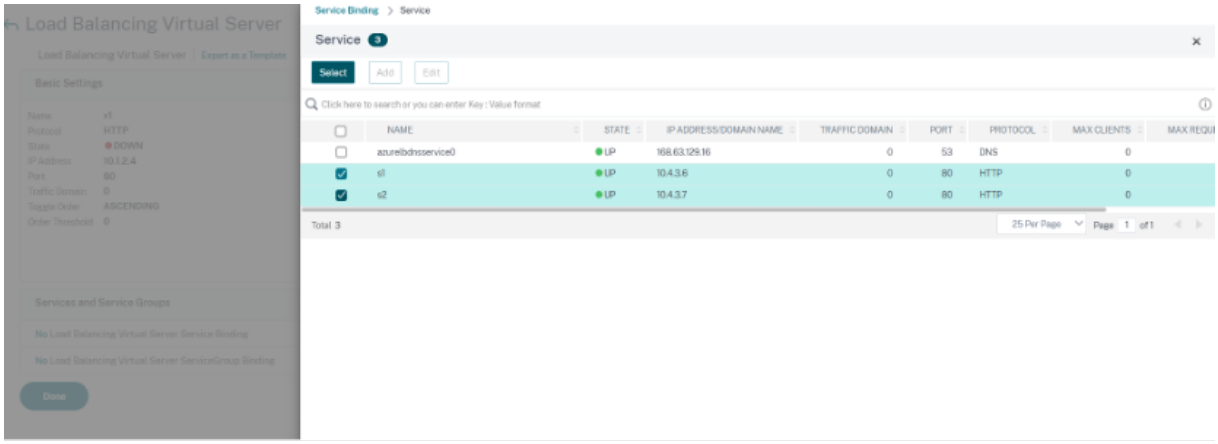


Étape 5. Ajoutez un service ou un groupe de services sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 6. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 4**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 5**, puis cliquez sur **Lier**.



Étape 8. Enregistrez la configuration.

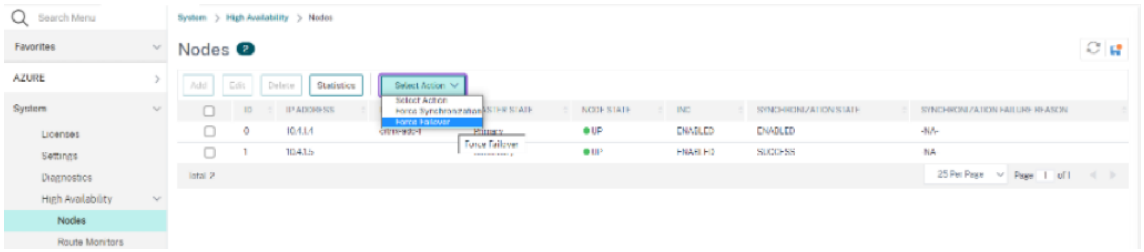
Sinon, toute la configuration est perdue après un redémarrage ou s'il y a un redémarrage instantané.

Étape 8. Vérifiez la configuration.

Assurez-vous que l'adresse IP du frontend ALB est accessible après un basculement.

1. Copiez l'adresse IP de l'interface ALB.
2. Collez l'adresse IP dans le navigateur et assurez-vous que les serveurs principaux sont accessibles.
3. Sur l'instance principale, effectuez un basculement :

   Depuis l'interface graphique de NetScaler, accédez à **Configuration > Système > Haute disponibilité > Action > Forcer**le basculement.



4. Assurez-vous que les serveurs back-end sont accessibles après le basculement via l'IP frontend ALB utilisée précédemment.

Déployer une zone privée DNS NetScaler for Azure

October 17, 2024

Azure DNS est un service de l'infrastructure Microsoft Azure destiné à héberger des domaines DNS et à fournir une résolution de noms.

Les zones privées Azure DNS sont un service axé sur la résolution des noms de domaine dans un réseau privé. Avec les zones privées, les clients peuvent utiliser leurs propres noms de domaine personnalisés plutôt que les noms fournis par Azure disponibles aujourd'hui.

NetScaler, la principale solution de mise à disposition d'applications, est la mieux adaptée pour fournir des fonctionnalités d'équilibrage de charge et de GSLB pour une zone privée Azure DNS. En s'abonnant à la zone privée Azure DNS, l'entreprise peut compter sur la puissance et l'intelligence de NetScaler Global Server Load Balancing (GSLB) pour répartir le trafic intranet entre les charges de travail dans plusieurs zones géographiques et entre les centres de données, connectés via des tunnels VPN sécurisés. Cette collaboration garantit aux entreprises un accès fluide à une partie de leur charge de travail qu'elles souhaitent transférer vers le cloud public Azure.

Présentation d'Azure DNS

Le système de noms de domaine (DNS) est chargé de traduire ou de résoudre un nom de service en adresse IP. Service d'hébergement pour les domaines DNS, Azure DNS permet de résoudre les noms en utilisant l'infrastructure Microsoft Azure. En plus de prendre en charge les domaines DNS accessibles sur Internet, Azure DNS prend désormais également en charge les domaines DNS privés.

Azure DNS fournit un service DNS fiable et sécurisé pour gérer et résoudre les noms de domaine dans un réseau virtuel sans avoir besoin d'une solution DNS personnalisée. En utilisant des zones DNS privées, vous pouvez utiliser vos propres noms de domaine personnalisés plutôt que les noms fournis par Azure. L'utilisation de noms de domaine personnalisés vous permet d'adapter l'architecture de votre réseau virtuel aux besoins de votre entreprise. Il fournit une résolution de noms pour les machines virtuelles (VM) au sein d'un réseau virtuel et entre les réseaux virtuels. Les clients peuvent également configurer les noms de zone avec une vue à horizon partagé, ce qui permet à une zone DNS privée et à une zone DNS publique de partager un nom.

Pourquoi choisir la zone privée NetScaler GSLB pour Azure DNS ?

Dans le monde d'aujourd'hui, les entreprises souhaitent transférer leurs charges de travail des applications locales vers le cloud Azure. La transition vers le cloud leur permet d'appliquer le délai de mise sur le marché, les dépenses en capital et le prix, la facilité de déploiement et la sécurité. Le service de zone privée Azure DNS constitue une proposition unique pour les entreprises qui transfèrent une partie de leurs charges de travail vers le cloud Azure. Ces entreprises peuvent créer leur nom DNS privé, qu'elles utilisaient depuis des années lors de déploiements sur site, lorsqu'elles utilisent le service de zone privée. Avec ce modèle hybride de serveurs d'applications intranet sur site et connectés au cloud Azure via des tunnels VPN sécurisés, le seul défi consiste à disposer d'un accès fluide à ces

applications intranet. NetScaler résout ce cas d'utilisation unique grâce à sa fonctionnalité d'équilibrage de charge global, qui achemine le trafic des applications vers les charges de travail/serveurs distribués les plus optimaux, sur site ou sur le cloud Azure, et fournit l'état de santé du serveur d'applications.

Cas d'utilisation

Les utilisateurs d'un réseau sur site et de différents réseaux virtuels Azure peuvent se connecter aux serveurs les plus optimaux d'un réseau interne pour accéder au contenu requis. Cela garantit que l'application est toujours disponible, que les coûts sont optimisés et que l'expérience utilisateur est bonne. La gestion du trafic privé Azure (PTM) est ici la principale exigence. Azure PTM garantit que les requêtes DNS des utilisateurs sont résolues vers une adresse IP privée appropriée du serveur d'applications.

Solution de cas d'utilisation

NetScaler inclut la fonctionnalité d'équilibrage de charge global du serveur (GSLB) pour répondre aux exigences d'Azure PTM. GSLB agit comme un serveur DNS, qui reçoit les requêtes DNS et les résout en une adresse IP appropriée pour fournir :

- Basculement sans faille basé sur le DNS.
- Migration progressive de l'environnement sur site vers le cloud.
- Test A/B d'une nouvelle fonctionnalité.

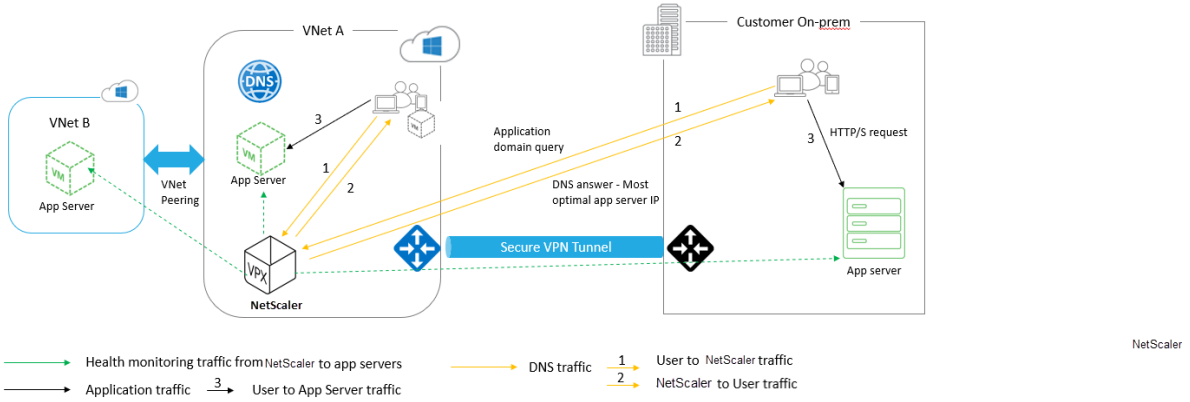
Parmi les nombreuses méthodes d'équilibrage de charge prises en charge, les méthodes suivantes peuvent être utiles dans cette solution :

1. Round Robin
2. Proximité statique (sélection du serveur basée sur l'emplacement). Il peut être déployé de deux manières :

    a) GSLB basé sur le sous-réseau du client EDNS (ECS) sur NetScaler.
    b) Déployez un redirecteur DNS pour chaque réseau virtuel.

Topologie

La figure suivante illustre le déploiement de NetScaler GSLB pour une zone DNS privée Azure.



Un utilisateur peut accéder à n'importe quel serveur d'applications sur Azure ou sur site selon la méthode NetScaler GSLB dans une zone DNS privée Azure. Tout le trafic entre On-Prem et le réseau virtuel Azure passe uniquement par un tunnel VPN sécurisé. Le trafic des applications, le trafic DNS et le trafic de surveillance sont présentés dans la topologie précédente. En fonction de la redondance requise, NetScaler et le redirecteur DNS peuvent être déployés dans les réseaux virtuels et les centres de données. Pour des raisons de simplicité, un seul NetScaler est présenté ici, mais nous recommandons au moins un ensemble de NetScaler et de redirecteur DNS pour la région Azure. Toutes les requêtes DNS des utilisateurs sont d'abord envoyées au redirecteur DNS dont les règles sont définies pour le transfert des requêtes vers un serveur DNS approprié.

Configuration de la zone privée DNS NetScaler pour Azure

Produits et versions testés :

Produit	Version
Azure	Abonnement au cloud
NetScaler VPX	BYOL (apportez votre propre licence)

> **Remarque :**
>
> Le déploiement est testé et reste le même avec NetScaler version 12.0 et supérieure.

Conditions préalables

Les prérequis généraux sont les suivants.

- Compte du portail Microsoft Azure avec un abonnement valide.

- Garantissez la connectivité (tunnel VPN sécurisé) entre On-Prem et le cloud Azure. Pour configurer un tunnel VPN sécurisé dans Azure, voir Étape par étape : Configuration d'une passerelle VPN de site à site entre Azure etles sites locaux.

Description de la solution

Si vous souhaitez héberger une application Azure DNS private zone (rr.ptm.mysite.net) qui s'exécute sur HTTPS et est déployée sur Azure et sur site avec un accès à l'intranet basé sur la méthode d'équilibrage de charge GSLB en boucle. Pour réaliser ce déploiement, activez GSLB pour la zone DNS privée Azure avec NetScaler, qui comprend les configurations suivantes :

1. Configurez Azure et la configuration locale.
2. Appliance NetScaler sur le réseau virtuel Azure.

Configuration d'Azure et de la configuration locale

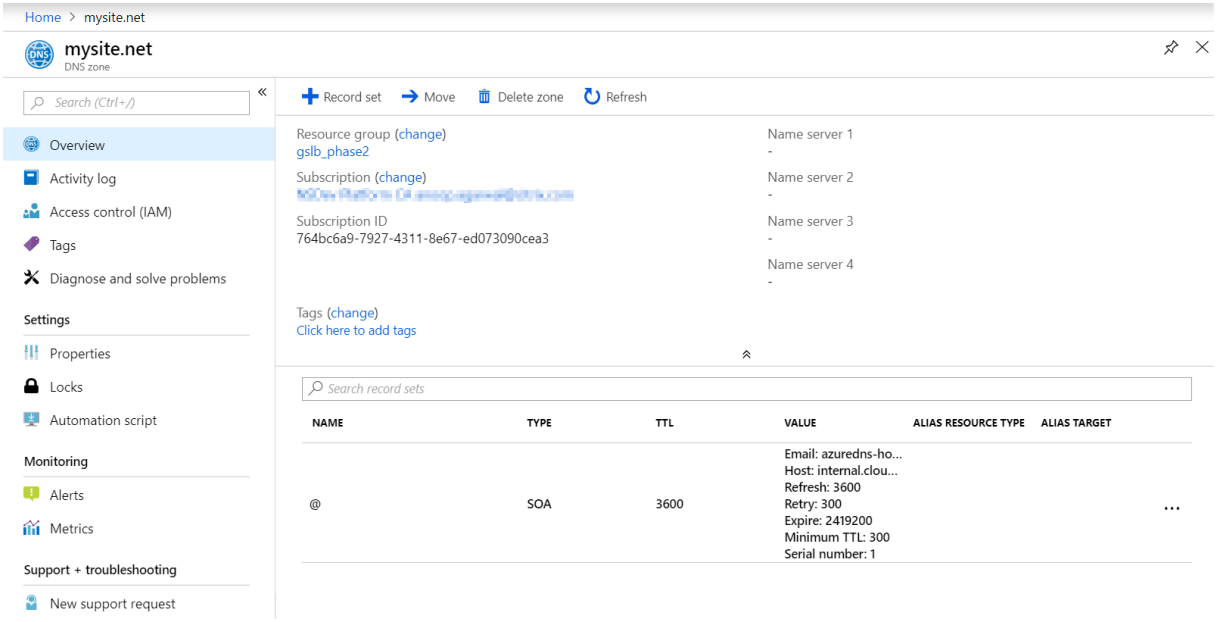
Comme indiqué dans la topologie, configurez le réseau virtuel Azure (VNet A, VNet B dans ce cas) et la configuration sur site.

1. Créez une zone DNS privée Azure avec un nom de domaine (mysite.net).
2. Créez deux réseaux virtuels (VNet A, VNet B) dans un modèle Hub et Spoke dans une région Azure.
3. Déployez un serveur d'applications, un redirecteur DNS, un client Windows 10 Pro, NetScaler dans le réseau virtuel A.
4. Déployez un serveur d'applications et déployez un redirecteur DNS si des clients se trouvent dans le réseau virtuel B.
5. Déployez un serveur d'applications, un redirecteur DNS et un client Windows 10 pro sur site.

Zone DNS privée Azure

Créez une zone DNS privée Azure avec un nom de domaine.

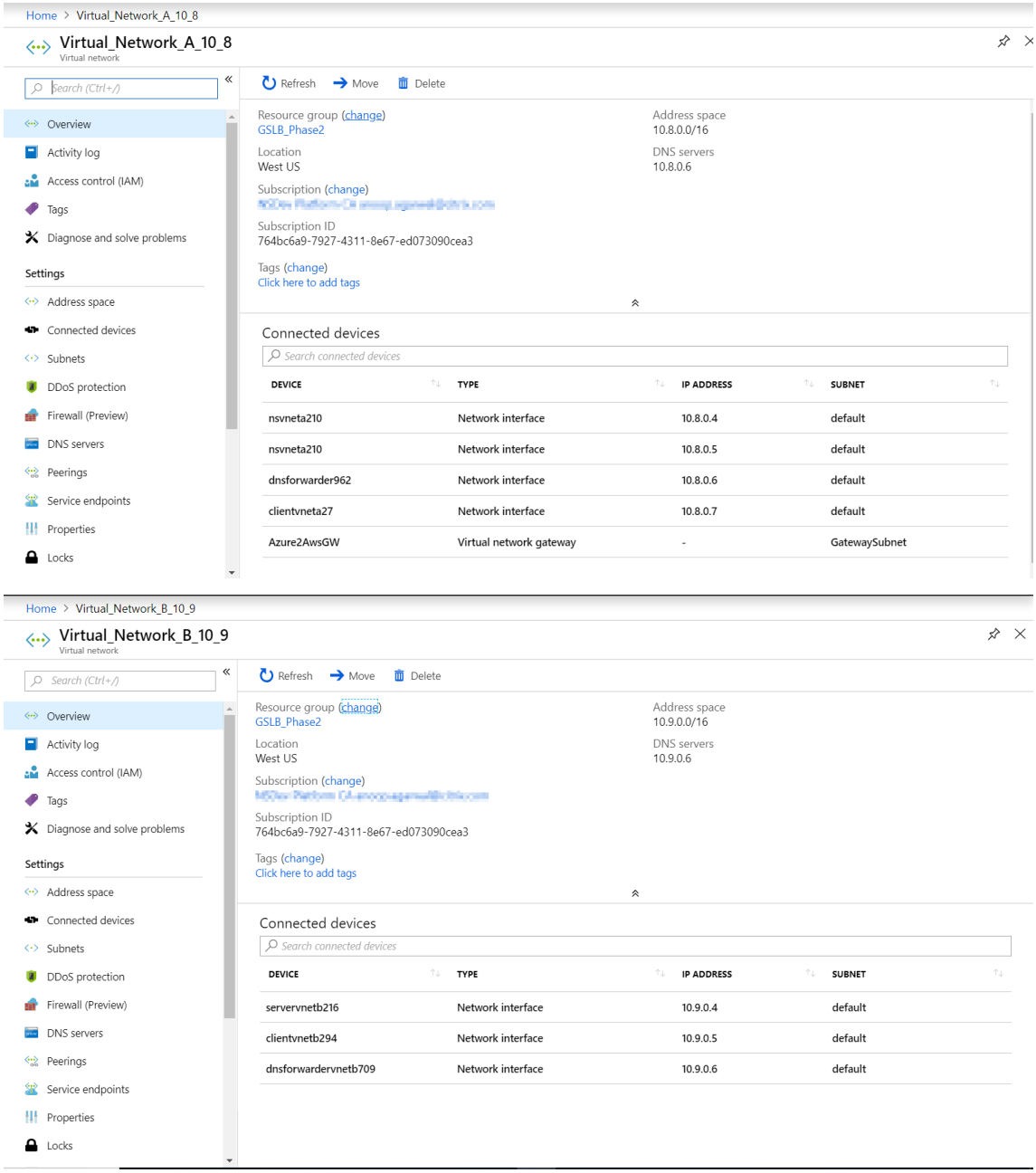
1. Connectez-vous au portail Azure et sélectionnez ou créez un tableau de bord.
2. Cliquez sur **Créer une ressource** et recherchez la zone DNS pour créer (mysite.net dans ce cas) la zone DNS privée Azure avec le nom de domaine (mysite.net).



Réseaux virtuels Azure (VNet A, VNet B) dans le modèle Hub and Spoke

Créez deux réseaux virtuels (VNet A, VNet B) dans un modèle Hub et Spoke dans une région Azure.

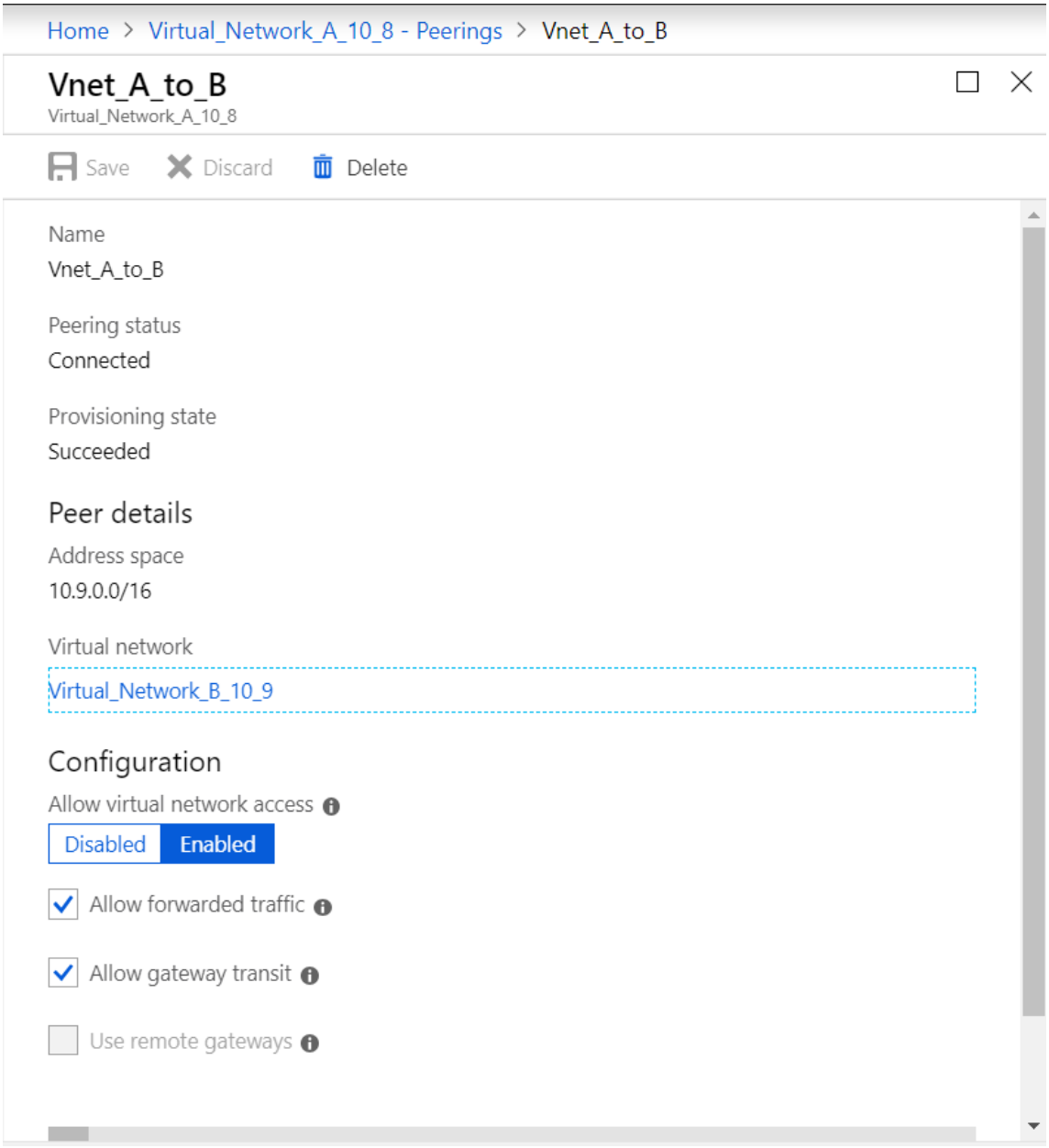
1. Créez deux réseaux virtuels.
2. Sélectionnez le même tableau de bord, cliquez sur **Créer une ressource** et recherchez des réseaux virtuels pour créer deux réseaux virtuels, à savoir le réseau virtuel A et le réseau virtuel B dans la même région, puis associez-les pour former un modèle Hub and Spoke, comme illustré dans l'image suivante. Pour plus d'informations sur la configuration d'une topologie en forme de hub and spoke, voir Implémenter une topologie de réseau en étoiledans Azure.



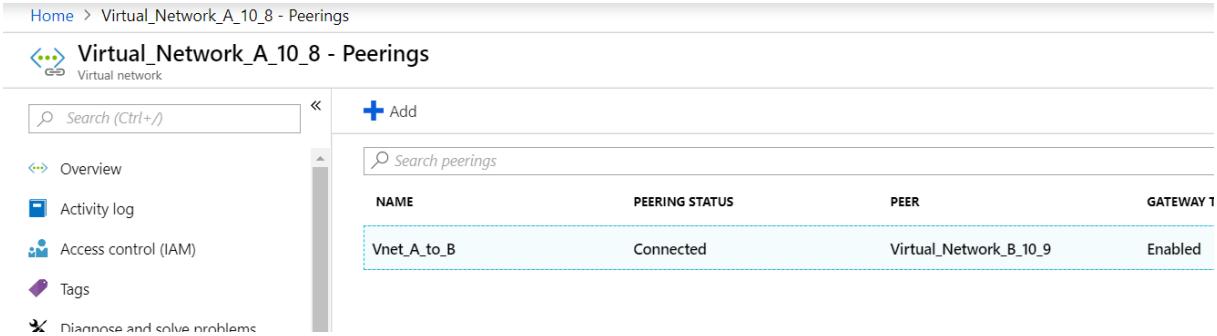
Peering entre réseaux virtuels A et réseau virtuel B

Pour associer VNet A et VNet B :

1. Cliquez sur **Peerings dans** le menu **Paramètres** du réseau virtuel A et du réseau virtuel homologue B.
2. Activez **Autoriser le trafic transféré** et **Autoriser le transit par la passerelle**, comme indiqué dans l'image suivante.



L'image suivante illustre le peering réussi du réseau virtuel A vers le réseau virtuel B.



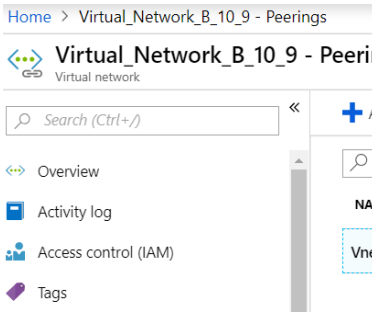
Peering d'un réseau VNet B vers un réseau VNet A

Pour associer le réseau virtuel B et le réseau virtuel A :

1. Cliquez sur **Peerings dans** le menu **Paramètres** du réseau virtuel B et du réseau virtuel homologue A.
2. Activez **Autoriser le trafic transféré** et utilisez des passerelles distantes comme indiqué dans l'image suivante.

```
1 ![VNet B to A](/en-us/vpx/media/image-07.png)
```

L'image suivante illustre le peering réussi du réseau virtuel B vers le réseau virtuel A.



Déployer un serveur d'applications, un redirecteur DNS, un client Windows 10 Pro, NetScaler dans le réseau virtuel A

Nous discutons brièvement du serveur d'applications, du redirecteur DNS, du client Windows 10 pro et de NetScaler sur le réseau virtuel A.

1. Sélectionnez le même tableau de bord, puis cliquez sur **Créer une ressource**.
2. Recherchez les instances respectives et attribuez une adresse IP à partir du sous-réseau VNet A.

Serveur d'applications Le serveur d'applications n'est rien d'autre que le serveur Web (serveur HTTP) sur lequel un serveur Ubuntu 16.04 est déployé en tant qu'instance sur la machine virtuelle Azure ou sur site. Pour en faire un serveur Web, à l'invite de commande, tapez :

```
sudo apt install apache2
```

Client Windows 10 Professionnel Lancez l'instance Windows 10 pro en tant que machine cliente sur VNet A et sur site.

NetScaler NetScaler complète la zone privée Azure DNA grâce au bilan de santé et aux analyses de NetScaler MAS. Lancez un NetScaler depuis Azure Marketplace en fonction de vos besoins. Ici, nous avons utilisé NetScaler (BYOL) pour ce déploiement.

Pour connaître les étapes détaillées du déploiement de NetScaler sur Microsoft Azure. Voir Déployer une instance NetScaler VPX sur Microsoft Azure.

Après le déploiement, utilisez NetScaler IP pour configurer NetScaler GSLB.

redirecteur DNS Il est utilisé pour transférer les demandes des clients des domaines hébergés liés à NetScaler GSLB (ADNS IP). Lancez un serveur Ubuntu 16.04 en tant qu'instance Linux (serveur Ubuntu 16.04) et consultez l'URL ci-dessous pour savoir comment le configurer en tant que redirecteur DNS.

> **Remarque :**
>
> pour la méthode d'équilibrage de charge Round Robin GSLB, un redirecteur DNS pour la région Azure est suffisant, mais pour la proximité statique, nous avons besoin d'un redirecteur DNS par réseau virtuel.

1. Après avoir déployé le redirecteur, remplacez les paramètres du serveur DNS du réseau virtuel A par défaut par des paramètres personnalisés avec l'adresse IP du redirecteur DNS VNet A, comme indiqué dans l'image suivante.
2. Modifiez le `named.conf.options` fichier dans le redirecteur DNS de VNet A pour ajouter des règles de transfert pour le domaine (mysite.net) et le sous-domaine (ptm.mysite.net) à l'adresse IP ADNS de NetScaler GSLB.
3. Redémarrez le redirecteur DNS pour refléter les modifications apportées au fichier `named.conf.options`.

Paramètres du redirecteur DNS VNet A

```
      zone "mysite.net" {

                  type forward;
      forwarders {
   168.63.129.16;  }
  ;
        }
  ;
      zone "ptm.mysite.net" {

          type forward;
          forwarders {
   10.8.0.5;  }
  ;
        }
  ;
```

> **Remarque :**
>
> Pour l'adresse IP de la zone de domaine (« mysite.net »), utilisez l'adresse IP DNS de votre ré-

> gion Azure. Pour l'adresse IP de zone du sous-domaine (« ptm.mysite.net »), utilisez toutes les adresses IP ADNS de vos instances GSLB.

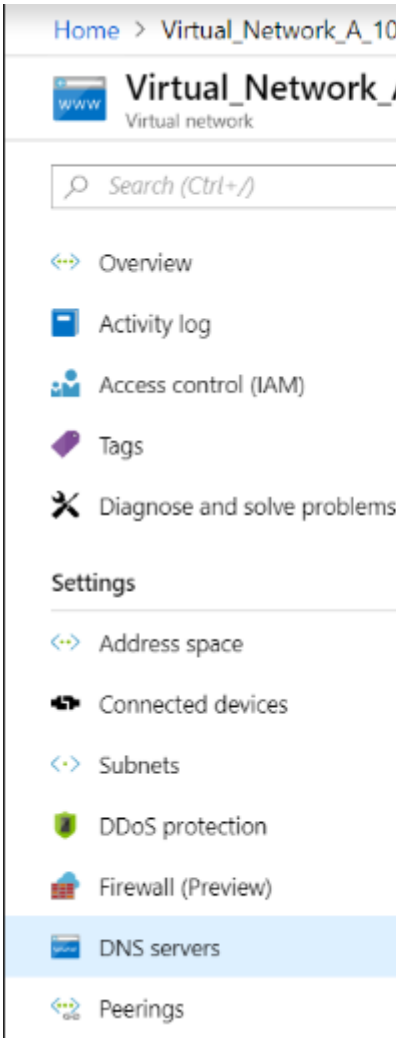
Déployez un serveur d'applications et un redirecteur DNS si des clients se trouvent dans le réseau virtuel B

1. Pour le réseau virtuel B, sélectionnez le même tableau de bord, cliquez sur **Créer une ressource**.
2. Recherchez les instances respectives et attribuez une adresse IP à partir du sous-réseau VNet B.
3. Lancez le serveur d'applications et le redirecteur DNS s'il existe un équilibrage de charge GSLB de proximité statique similaire à celui du réseau virtuel A.
4. Modifiez les paramètres du redirecteur DNS VNet B `named.conf.options` comme indiqué dans le paramètre suivant :

   Paramètres du redirecteur DNS VNet B :

```
      zone "ptm.mysite.net" {

          type forward;
          forwarders {
 10.8.0.5;  }
;
       }
;
```

L'image suivante illustre les paramètres du redirecteur DNS VNet B : Serveurs DNS

Déployer un serveur d'applications, un redirecteur DNS et un client Windows 10 pro sur site

1. Pour les applications sur site, lancez les machines virtuelles sur du matériel vierge et installez le serveur d'applications, le redirecteur DNS et le client Windows 10 pro similaires au réseau virtuel A.
2. Modifiez les paramètres du redirecteur DNS local `named.conf.options` comme indiqué dans l'exemple suivant.

Paramètres du redirecteur DNS sur site

```
      zone "mysite.net" {

                  type forward;
                  forwarders {
 10.8.0.6;  }
;
       }
```



```
8   ;
9         zone "ptm.mysite.net" {
10
11              type forward;
12              forwarders {
13    10.8.0.5;  }
14  ;
15          }
16  ;
```

En effet `mysite.net`, nous avons attribué l'adresse IP du redirecteur DNS VNet A au lieu de l'adresse IP du serveur de zone DNS privé Azure, car il s'agit d'une adresse IP spéciale qui n'est pas accessible depuis les locaux. Cette modification est donc requise dans le paramètre du redirecteur DNS sur site.

Configurer le réseau virtuel NetScaler sur Azure

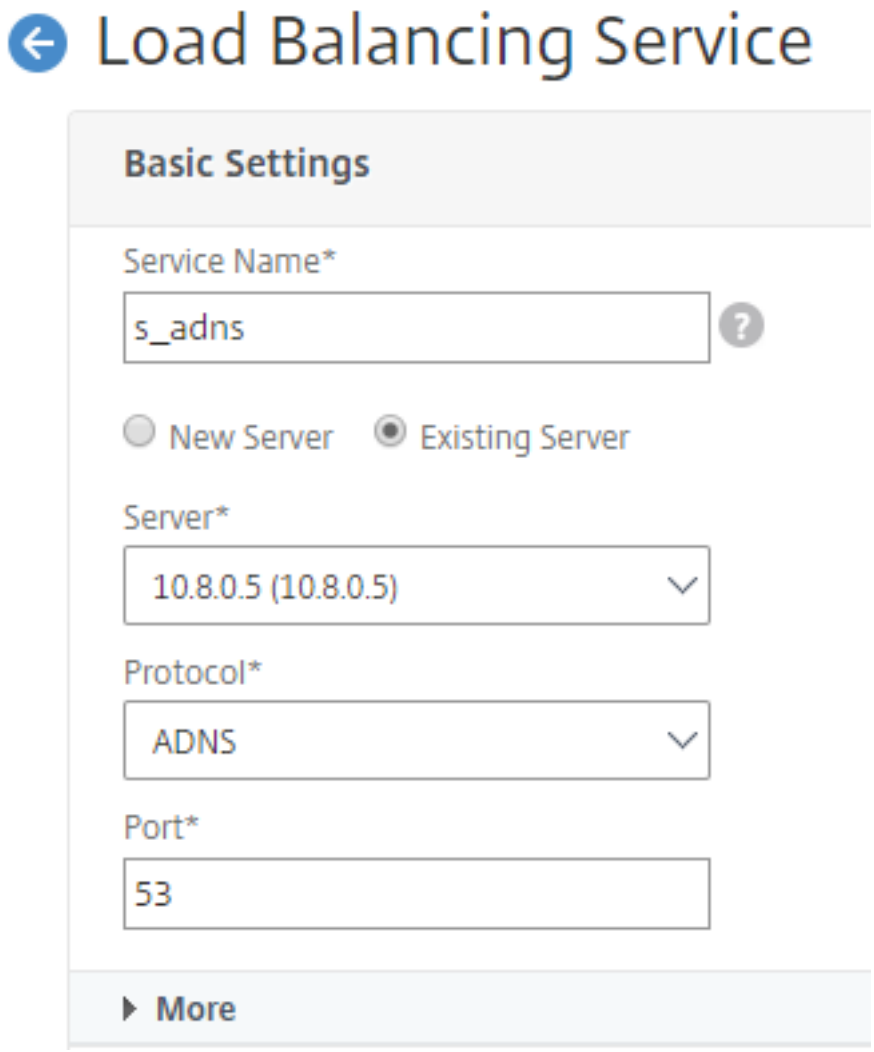
Comme indiqué dans la topologie, déployez NetScaler sur le réseau virtuel Azure (VNet A dans ce cas) et accédez-y via l'interface graphique de NetScaler.

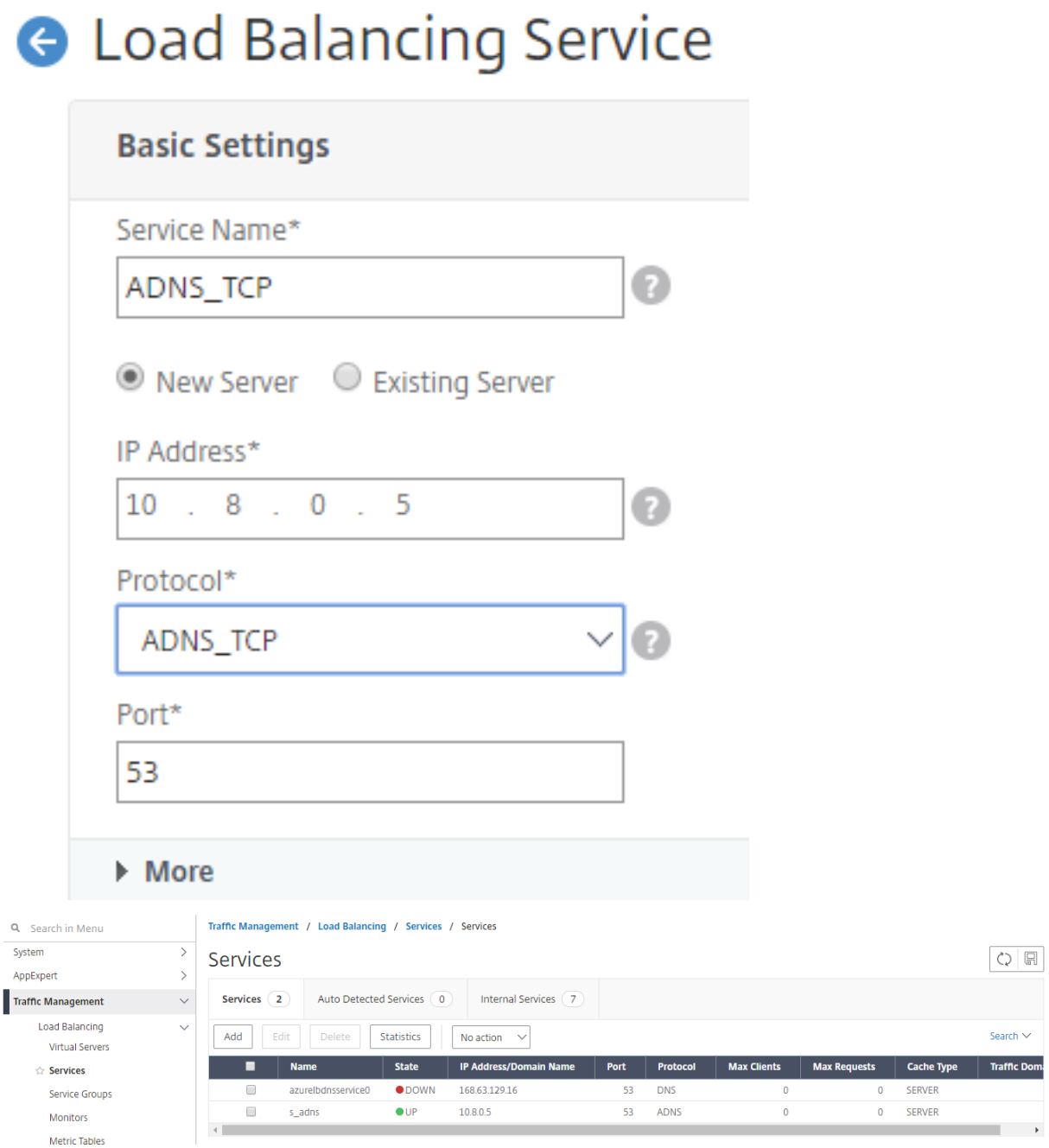
Configuration de NetScaler GSLB

1. Créez un service ADNS.
2. Créez des sites locaux et distants.
3. Créez des services pour les serveurs virtuels locaux.
4. Créez des serveurs virtuels pour les services GSLB.

Ajouter un service ADNS

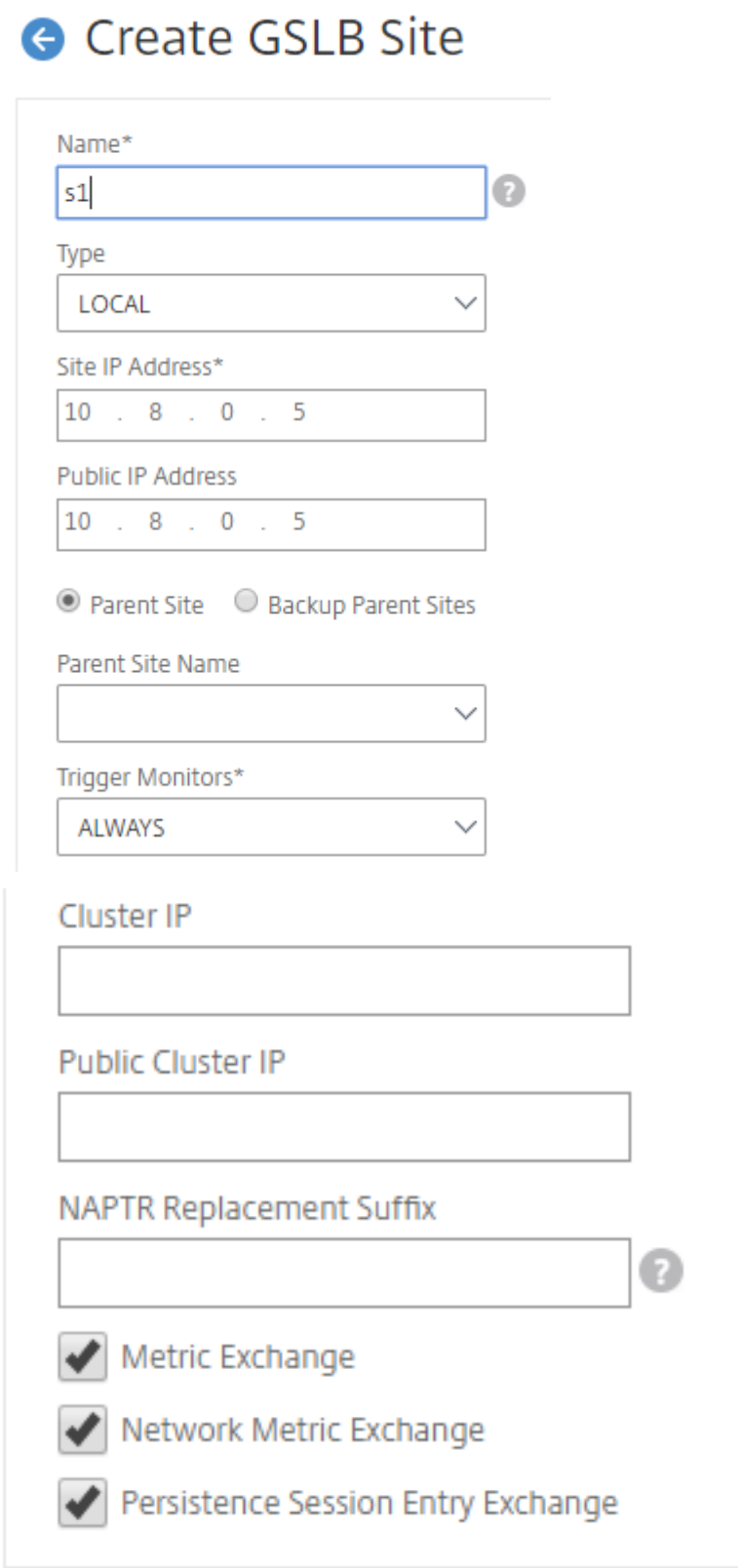
1. Connectez-vous à l'interface graphique de NetScaler.
2. Dans l'onglet **Configuration**, accédez à **Gestion du trafic > Équilibrage de charge > Services**.
3. Ajoutez un service. Nous vous recommandons de configurer le service ADNS à la fois en TCP et en UDP, comme indiqué dans l'image suivante :

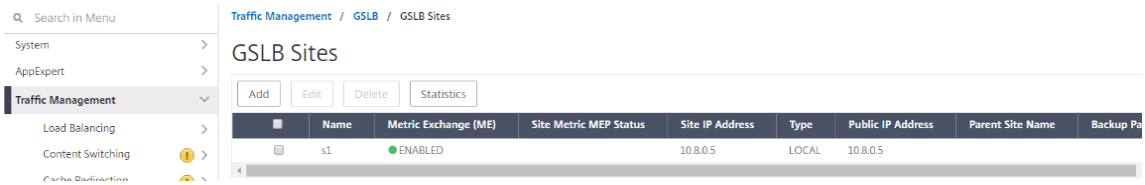




Ajouter des sites GSLB

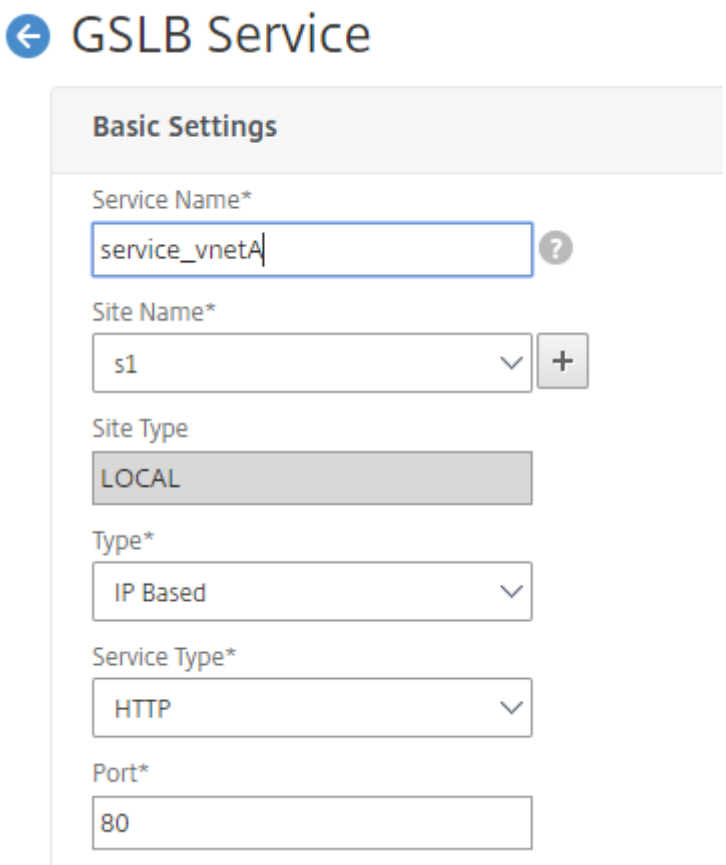
1. Ajoutez des sites locaux et distants entre lesquels le GSLB sera configuré.
2. Dans l'onglet **Configuration**, accédez à **Gestion du trafic > GSLB > Sites GSLB**. Ajoutez un site comme indiqué dans l'exemple suivant et répétez la même procédure pour les autres sites.



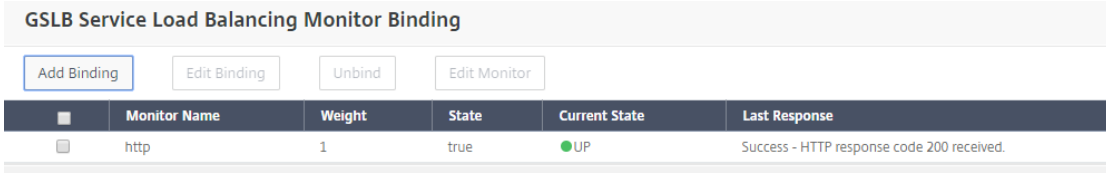


Ajouter des services GSLB

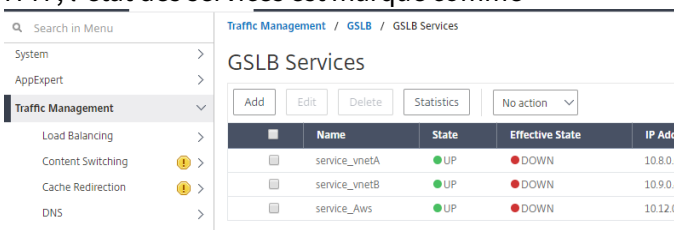
1. Ajoutez des services GSLB pour les serveurs virtuels locaux et distants afin d'équilibrer la charge des serveurs d'applications.
2. Dans l'onglet **Configuration**, accédez à **Gestion du trafic > GSLB > Services GSLB**.
3. Ajoutez les services comme indiqué dans les exemples suivants.
4. Liez le moniteur HTTP pour vérifier l'état du serveur.



5. Après avoir créé le service, accédez à l'onglet **Paramètres avancés** du service GSLB.
6. Cliquez sur **Ajouter un moniteur** pour lier le service GSLB à un moniteur HTTP afin d'afficher l'état du service.



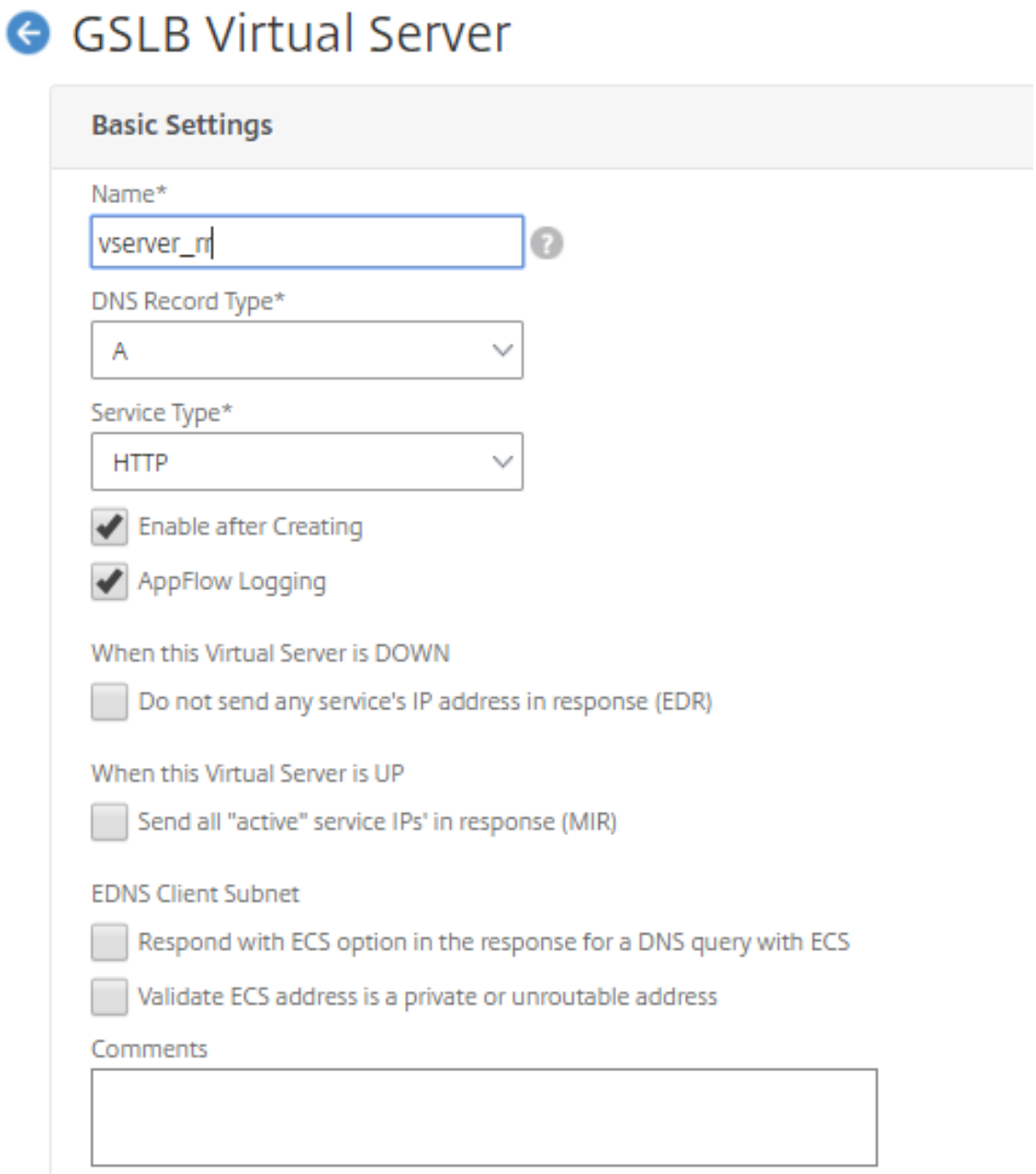
7. Une fois que vous vous êtes connecté au moniteur HTTP, l'état des services est marqué comme UP, comme indiqué dans l'image suivante : Services



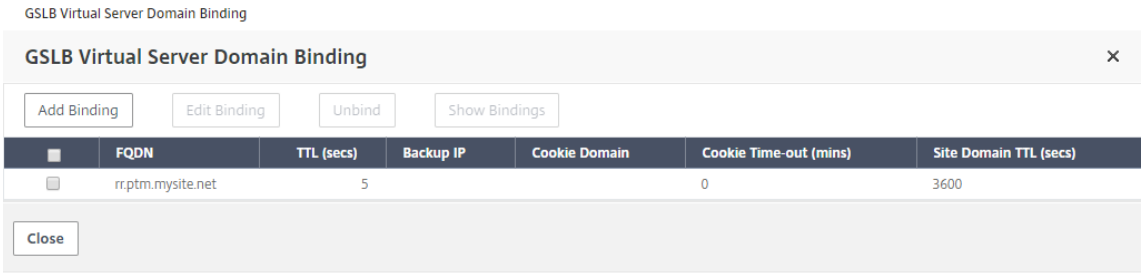
Ajouter un serveur virtuel GSLB

Ajoutez un serveur virtuel GSLB via lequel les services GSLB alias des serveurs d'applications sont accessibles.

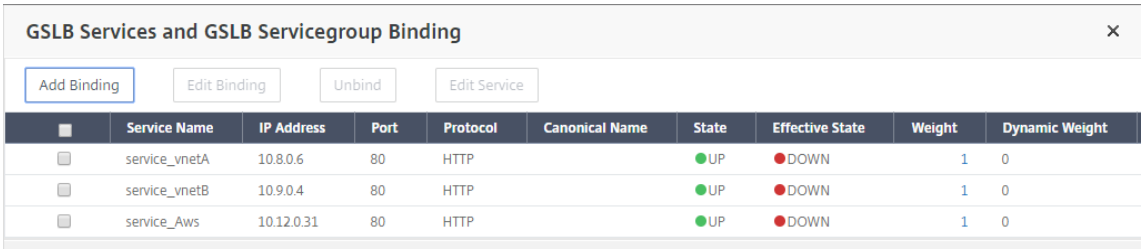
1. Dans l'onglet **Configuration**, accédez à **Gestion du trafic > GSLB > Serveurs virtuels GSLB**.
2. Ajoutez les serveurs virtuels comme indiqué dans l'exemple suivant.
3. Liez les services GSLB et le nom de domaine à celui-ci.



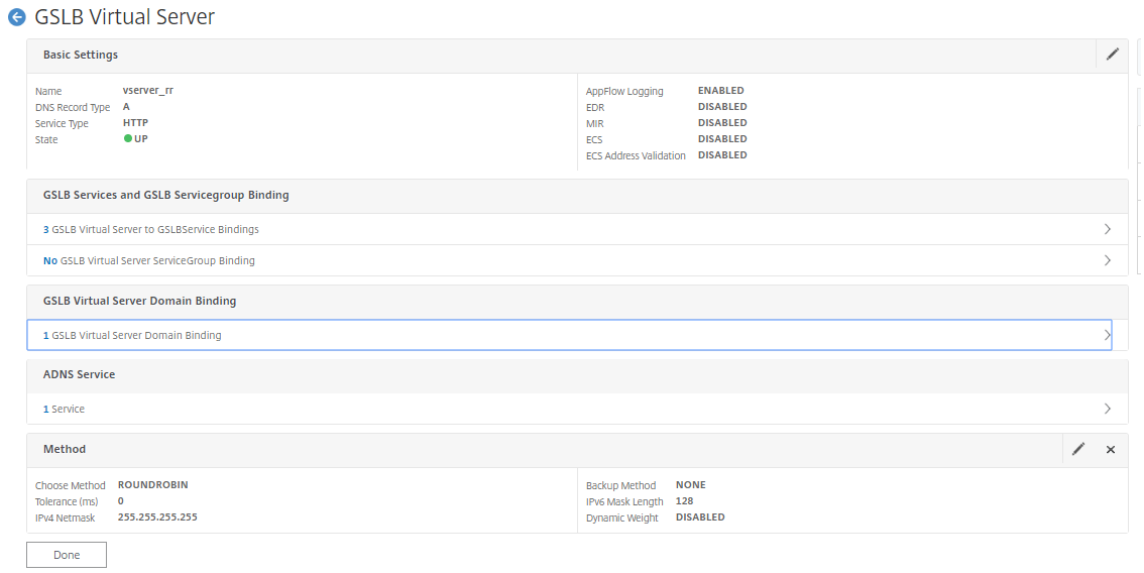
4. Après avoir créé le serveur virtuel GSLB et sélectionné la méthode d'équilibrage de charge appropriée (Round Robin dans ce cas), liez les services et les domaines GSLB pour terminer l'étape.



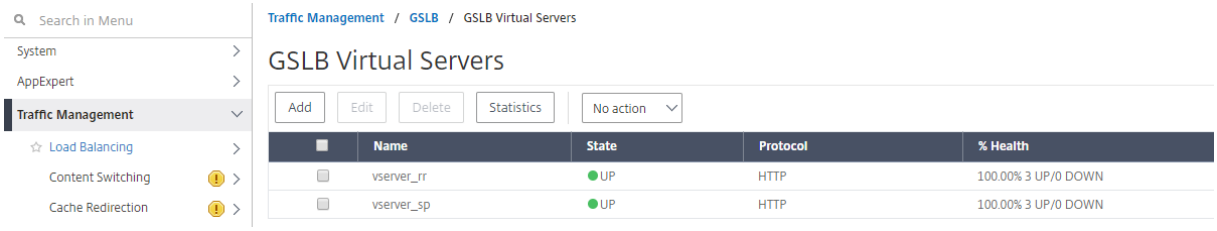
5. Accédez à l'onglet **Paramètres avancés** du serveur virtuel et cliquez sur l'onglet **Ajouter des domaines** pour lier un domaine.
6. Accédez à **Avancé > Services** et cliquez sur la flèche pour lier un service GSLB et lier les trois services (réseau virtuel A, réseau virtuel B, local) au serveur virtuel.



Après avoir lié les services et le domaine GSLB au serveur virtuel, il apparaît comme indiqué dans l'image suivante :



Vérifiez si le serveur virtuel GSLB est actif et sain à 100 %. Lorsque le moniteur indique que le serveur est opérationnel et en bon état, cela signifie que les sites sont synchronisés et que les services principaux sont disponibles.



Pour tester le déploiement, accédez à l'URL du domaine `rr.ptm.mysite.net` depuis la machine cliente cloud ou depuis la machine cliente locale. Si vous y accédez depuis une machine cliente Windows dans le cloud, assurez-vous que le serveur d'applications local est accessible dans une zone DNS privée sans avoir besoin de solutions DNS tierces ou personnalisées.

Configurer une instance NetScaler VPX pour utiliser le réseau accéléré Azure

October 17, 2024

La mise en réseau accélérée permet la carte réseau (VF) à fonction virtuelle (SR-IOV) de virtualisation d'E/S à racine unique sur une machine virtuelle, ce qui améliore les performances réseau. Vous pouvez utiliser cette fonctionnalité avec des charges de travail lourdes qui doivent envoyer ou recevoir des données à un débit supérieur avec un streaming fiable et une utilisation réduite du processeur. Lorsqu'une carte réseau est activée avec une mise en réseau accélérée, Azure associe l'interface para virtualisée (PV) existante de la carte réseau à une interface VF SR-IOV. La prise en charge de l'interface SR-IOV VF active et améliore le débit de l'instance NetScaler VPX.

La mise en réseau accélérée offre les avantages suivants :

- Latence inférieure
- Performances supérieures des paquets par seconde (pps)
- Débit amélioré
- gigue réduite
- Utilisation réduite du processeur

> **Remarque :**
>
> La mise en réseau accélérée Azure est prise en charge sur les instances NetScaler VPX à partir de la version 13.0 build 76.29.

Conditions préalables

- Assurez-vous que la taille de votre machine virtuelle correspond aux exigences relatives à la mise en réseau accélérée Azure.

- Arrêtez les machines virtuelles (individuelles ou dans un jeu de disponibilité) avant d'activer la mise en réseau accélérée sur n'importe quelle carte réseau.

Limitations

La mise en réseau accélérée peut être activée uniquement sur certains types d'instances. Pour plus d'informations, voir Types d'instances pris en charge.

cartes réseau prises en charge pour une mise en réseau accélérée

Azure fournit des cartes d'interface réseau Mellanox ConnectX3, ConnectX4 et ConnectX5 en mode SR-IOV pour une mise en réseau accélérée.

Lorsque la mise en réseau accélérée est activée sur une interface NetScaler VPX, Azure associe l'interface ConnectX3, ConnectX4 ou ConnectX5 à l'interface PV existante d'une appliance NetScaler VPX.

Pour plus d'informations sur l'activation d'une mise en réseau accélérée avant d'attacher une interface à une machine virtuelle, voir Créer une interface réseau avec une mise en réseau accélérée.

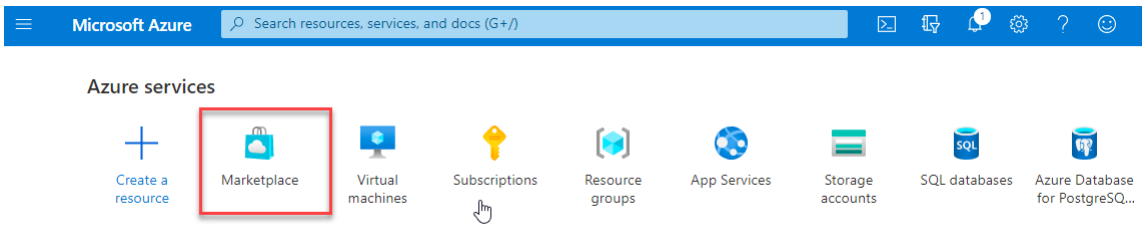
Pour plus d'informations sur l'activation d'une mise en réseau accélérée sur une interface existante sur une machine virtuelle, voir Activer les interfaces existantes sur une machine virtuelle.

Comment activer la mise en réseau accélérée sur une instance NetScaler VPX à l'aide de la console Azure

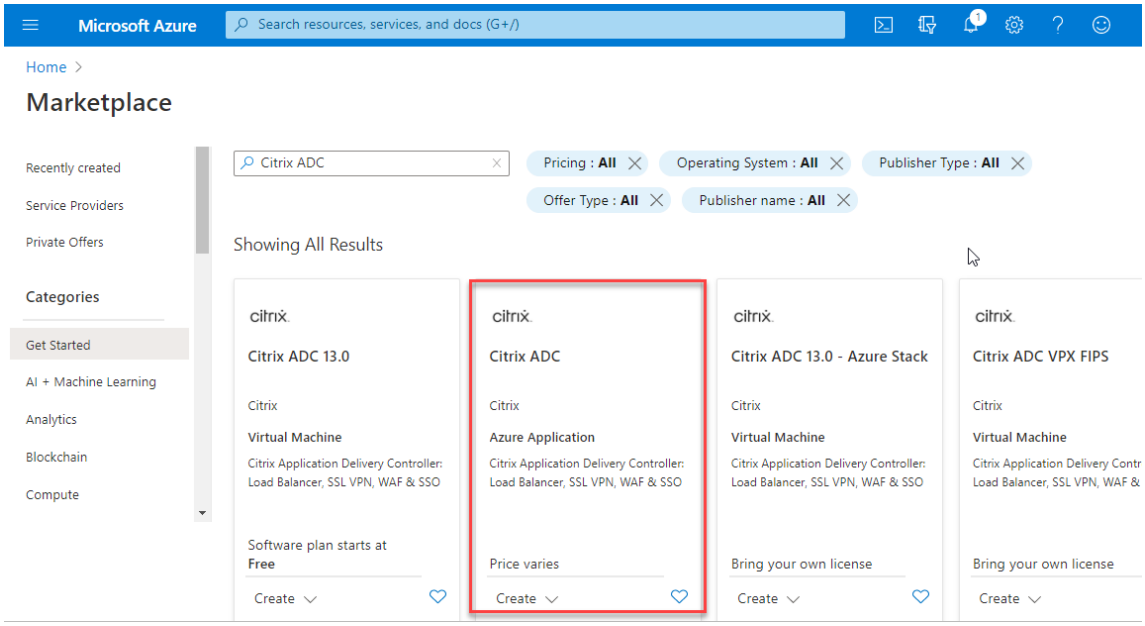
Vous pouvez activer la mise en réseau accélérée sur une interface spécifique à l'aide de la console Azure ou d'Azure PowerShell.

Procédez comme suit pour activer la mise en réseau accélérée à l'aide de jeux de disponibilité ou de zones de disponibilité Azure.

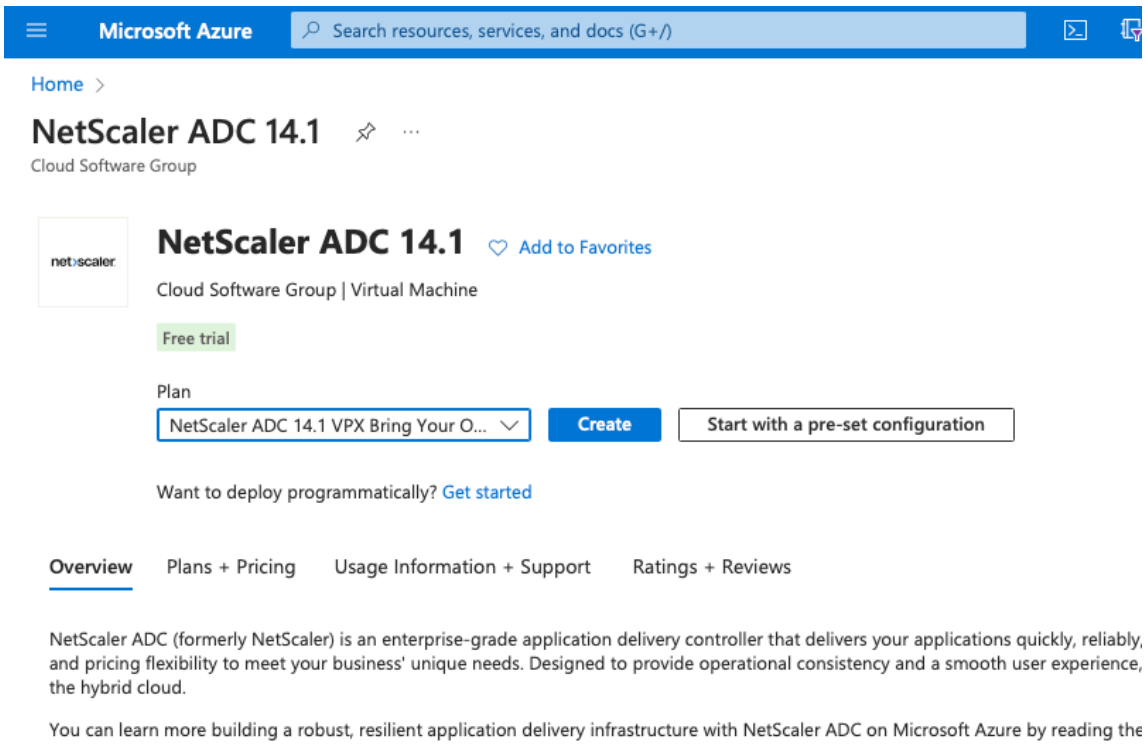
1. Connectez-vous au portail Azureet accédez à **Azure Marketplace**.



2. Sur **Azure Marketplace**, recherchez **NetScaler**.

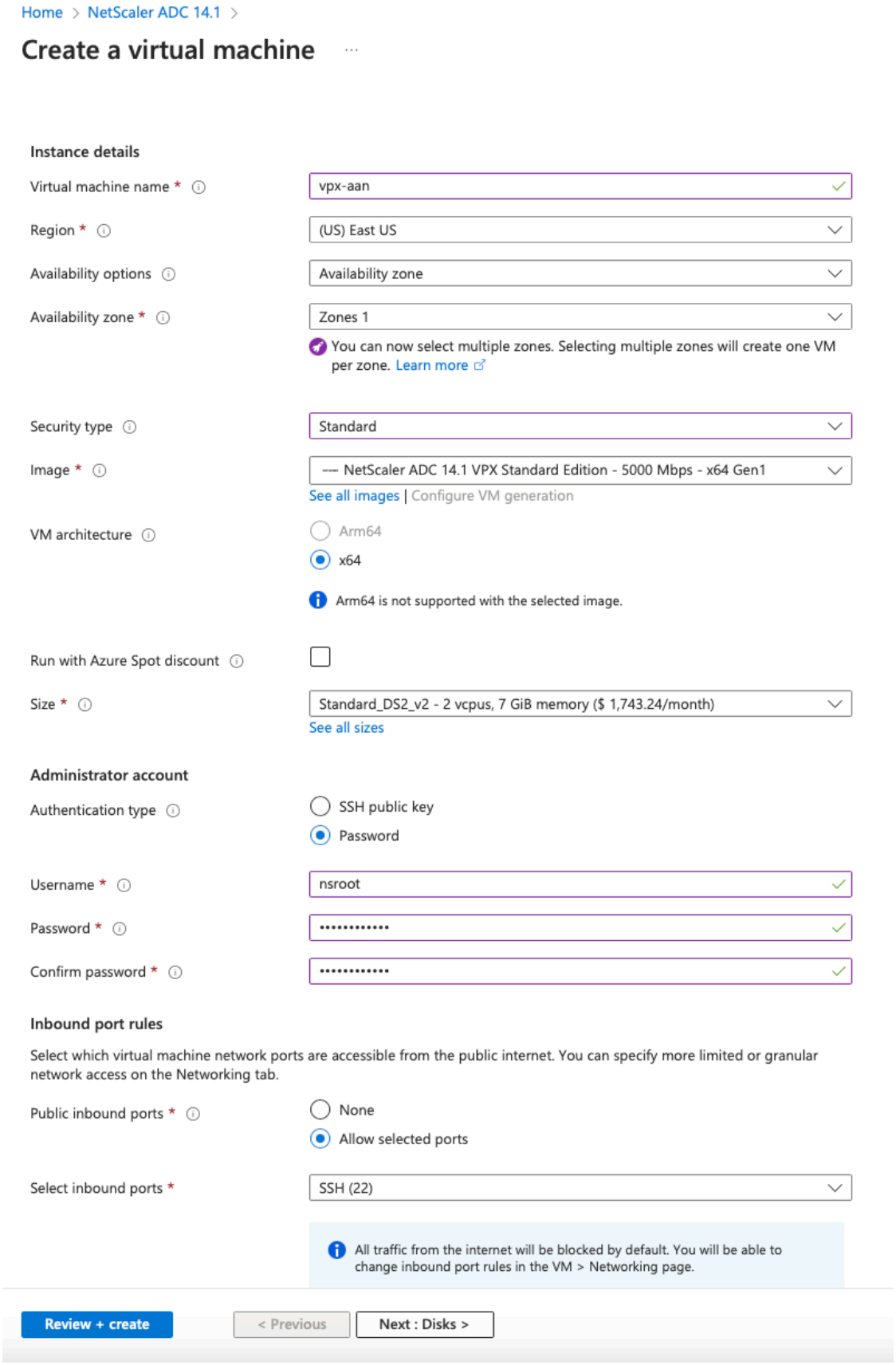


3. Sélectionnez un plan NetScaler non FIPS ainsi qu'une licence, puis cliquez sur Créer.



La page **Créer un NetScaler** s'affiche.

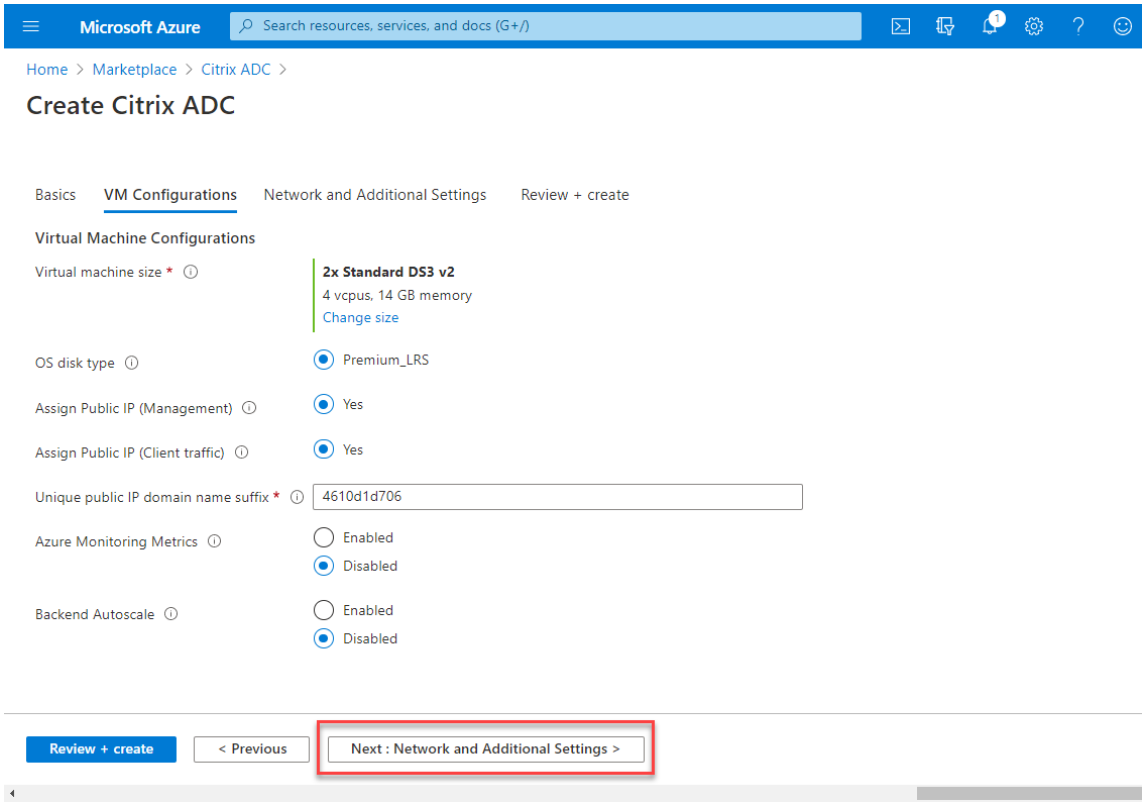
4. Dans l'onglet Notions de **base**, créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



5. Cliquez sur **Suivant : Configurations de machines virtuelles**.

   Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :

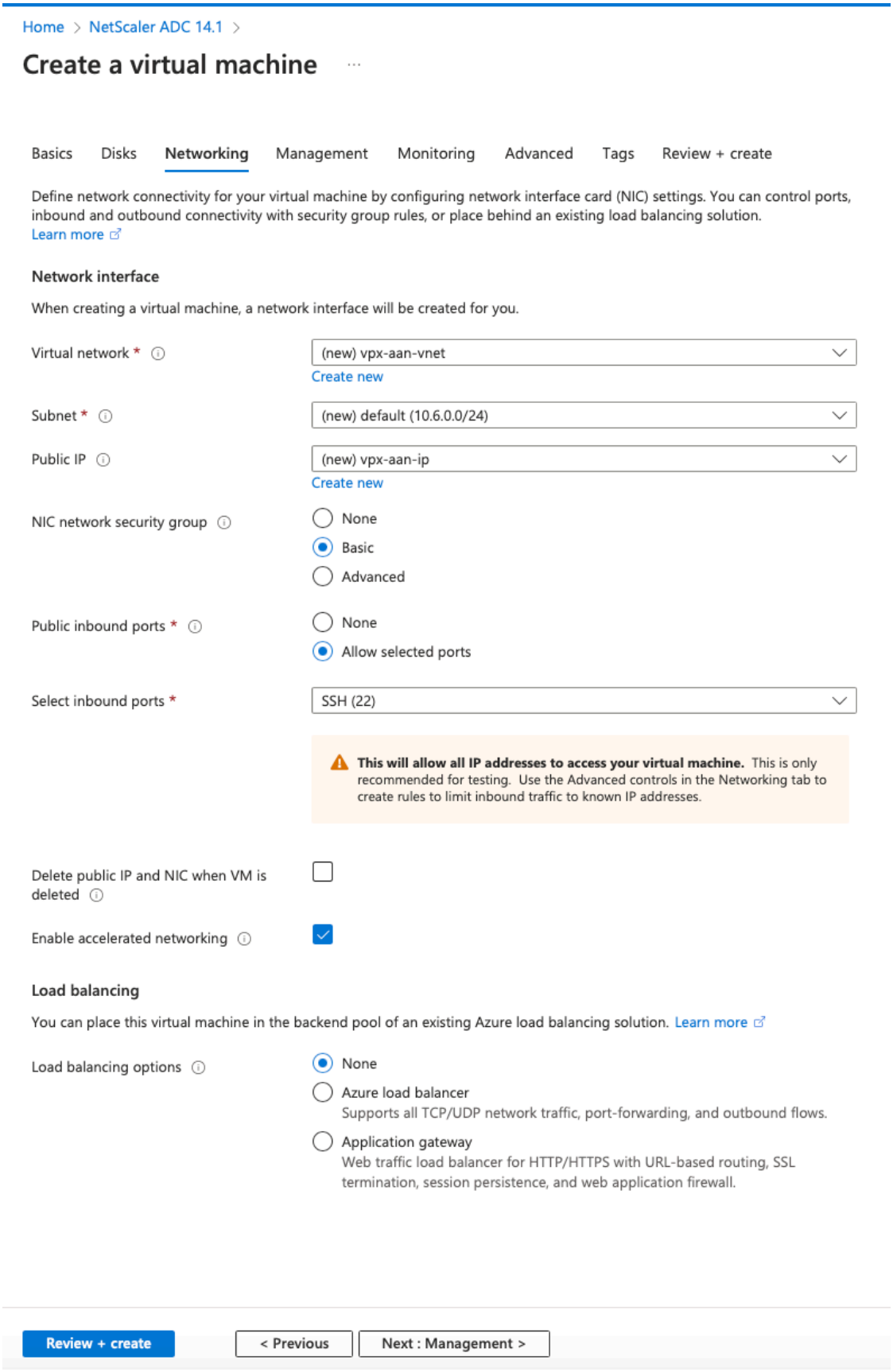
   a) Configurez un suffixe de nom de domaine IP public.
   b) Activez ou désactivez **Azure Monitoring Metrics**.
   c) Activez ou désactivez **Backend Autoscale**.



6. Cliquez sur **Suivant : Paramètres réseau et supplémentaires**.

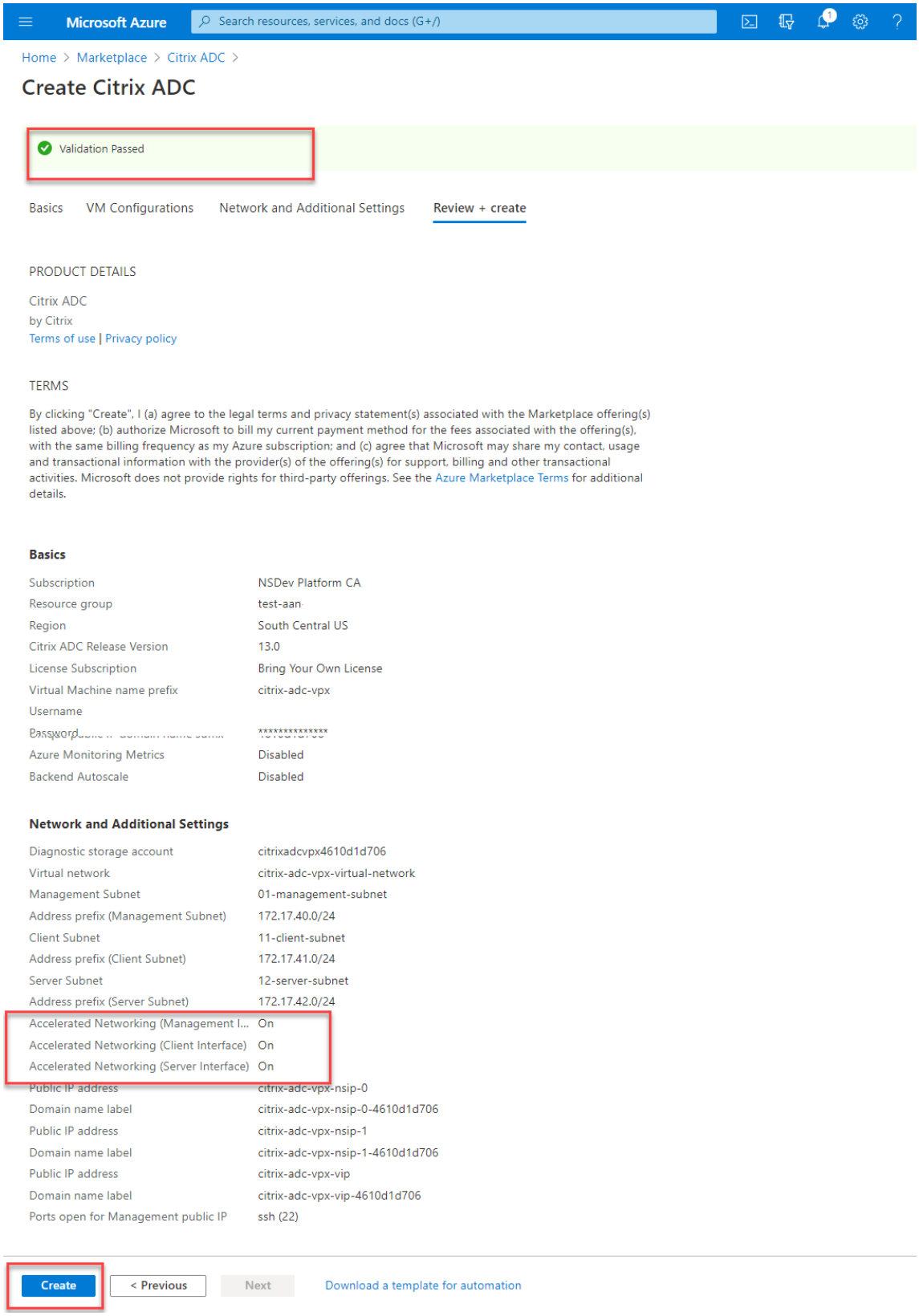
   Sur la page **Network and Additional Settings**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.

   Dans la section **Accelerated Networking**, vous avez la possibilité d'activer ou de désactiver la mise en réseau accélérée séparément pour l'interface de gestion, l'interface client et l'interface serveur.



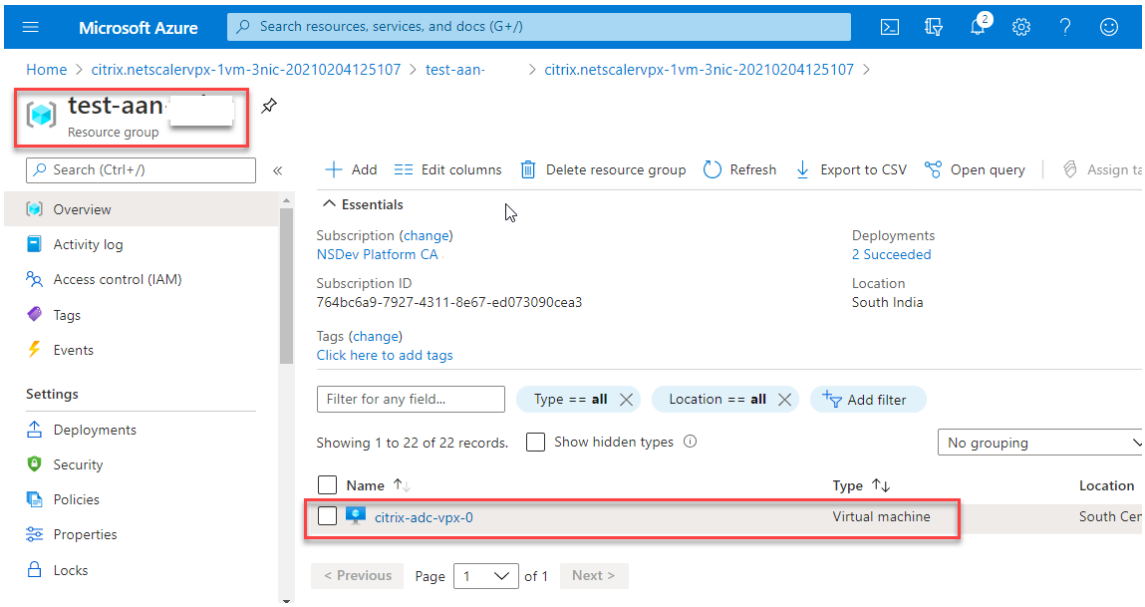
7. Cliquez sur **Suivant : Réviser + créer**.

   Une fois la validation réussie, passez en revue les paramètres de base, les configurations de machines virtuelles, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**. La création du groupe de ressources Azure avec les configurations requises peut prendre un certain temps.

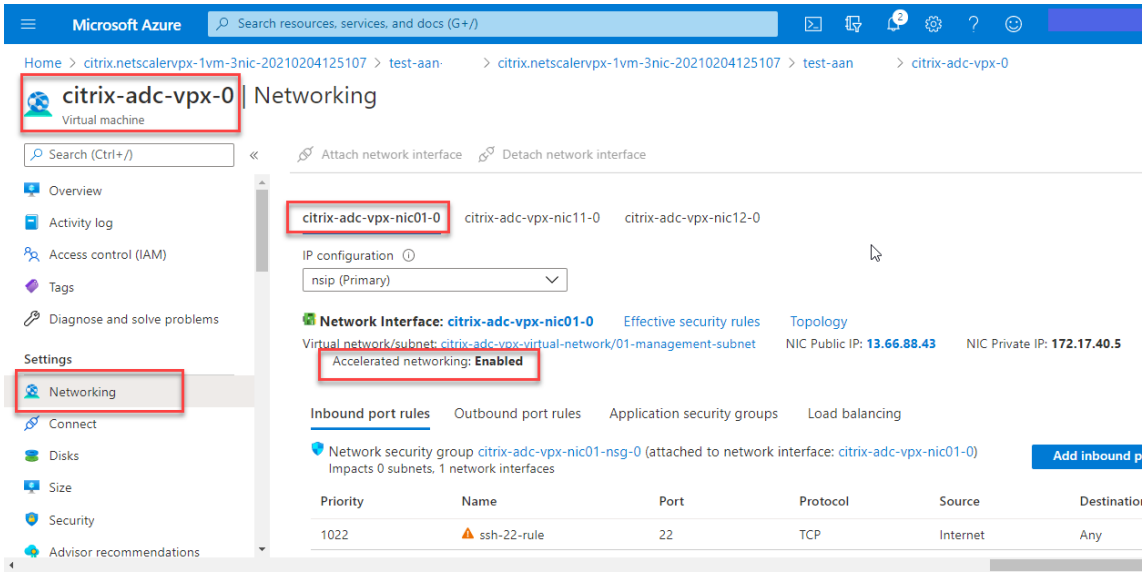


8. Une fois le déploiement terminé, sélectionnez le **groupe de ressources** pour voir les détails de

configuration.



9. Pour vérifier les configurations Accelerated Networking, sélectionnez **Machine virtuelle > Mise en réseau**. L'état Accelerated Networking s'affiche sous la forme **Activé** ou **Désactivé** pour chaque carte réseau.



Activer la mise en réseau accélérée avec Azure PowerShell

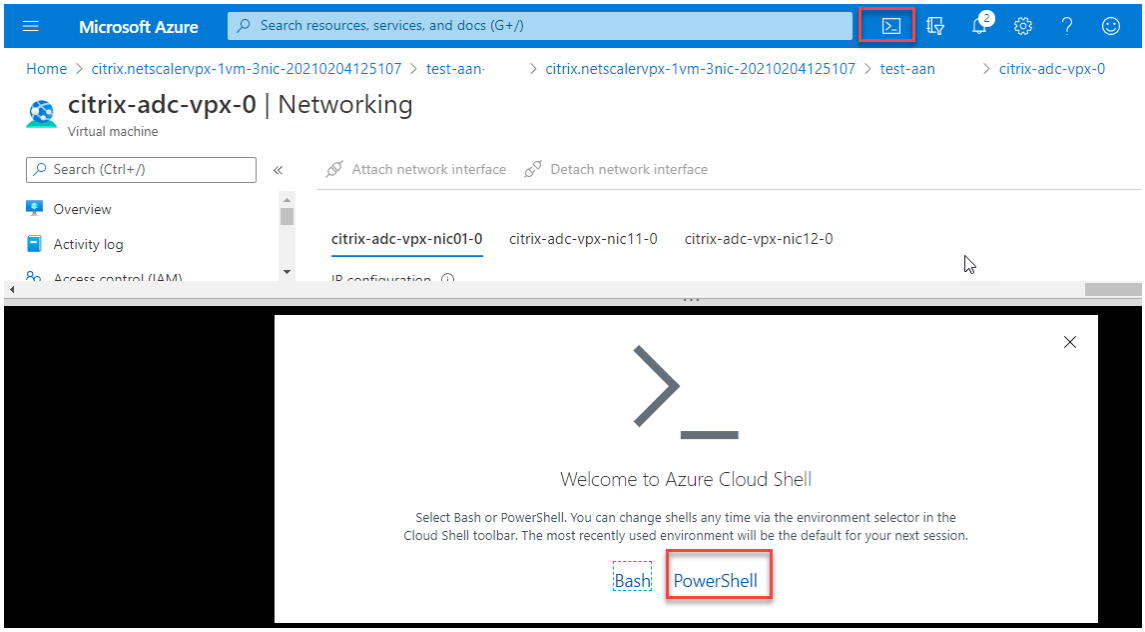
Si vous devez activer la mise en réseau accélérée après la création de la machine virtuelle, vous pouvez le faire à l'aide d'Azure PowerShell.

> **Remarque :**
>
> Assurez-vous d'arrêter la machine virtuelle avant d'activer Accelerated Networking à l'aide d'Azure PowerShell.

Effectuez les étapes suivantes pour activer la mise en réseau accélérée à l'aide d'Azure PowerShell.

1. Accédez au **portail Azure**, cliquez sur l'icône **PowerShell** dans le coin supérieur droit.

   > **Remarque :**
   >
   > Si vous êtes en mode Bash, passez au mode PowerShell.



2. À l'invite de commandes, exécutez la commande suivante :

```
az network nic update --name <nic-name> --accelerated-networking
    [true | false] --resource-group <resourcegroup-name>
```

   Le paramètre de mise en réseau accéléré accepte l'une des valeurs suivantes :

   - **Vrai :** active la mise en réseau accélérée sur la carte réseau spécifiée.
   - **Faux :** désactive la mise en réseau accélérée sur la carte réseau spécifiée.

   Pour activer la mise en réseau accélérée sur une carte réseau spécifique :

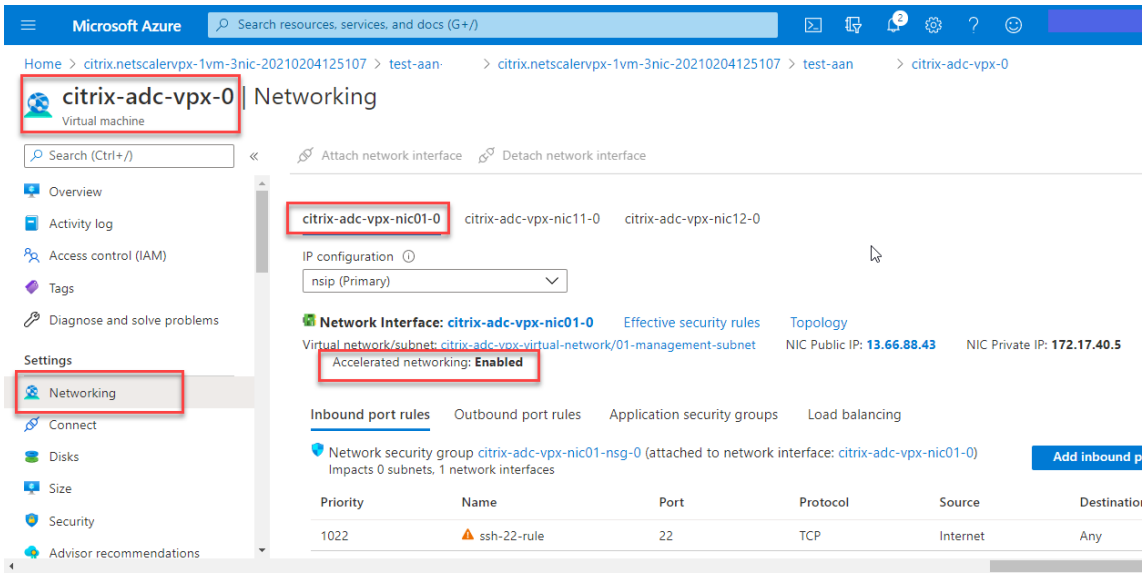
```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking true --resource-group rsgp1-aan
```

   Pour désactiver la mise en réseau accélérée sur une carte réseau spécifique :

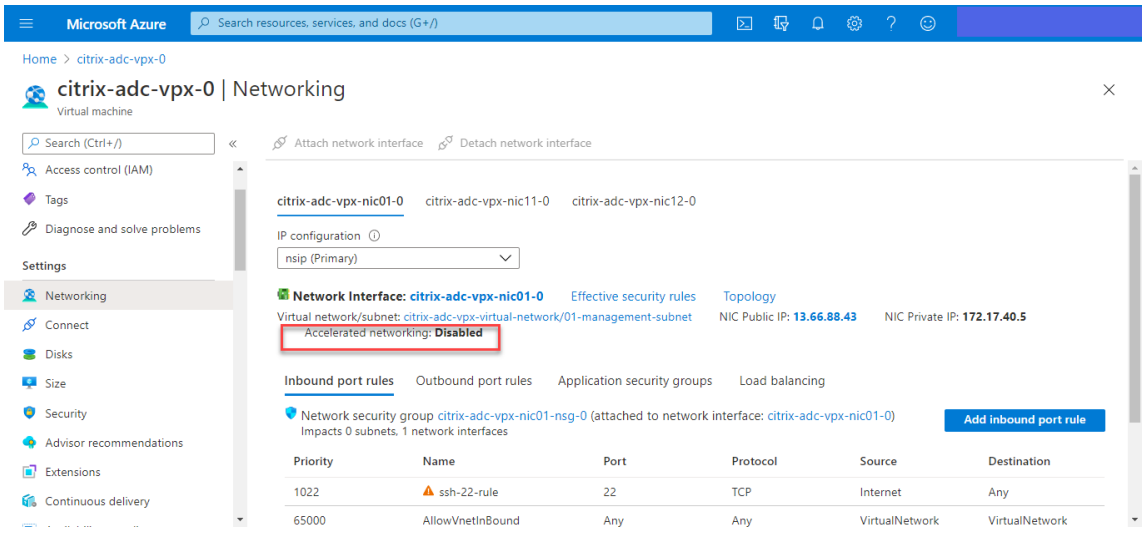
```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking false --resource-group rsgp1-aan
```


3. Pour vérifier que l'état de la mise en réseau accélérée une fois le déploiement terminé, accédez à **VM > Mise en réseau**.

   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **activée**.



   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **désactivée**.



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide de FreeBSD Shell de NetScaler

Vous pouvez vous connecter au shell FreeBSD de NetScaler et exécuter les commandes suivantes pour vérifier l'état du réseau accéléré.

Exemple de carte réseau ConnectX3 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox ConnectX3. Le « 50/n » indique les interfaces VF des cartes réseau Mellanox ConnectX3. 0/1 et 1/1 indiquent les interfaces PV de l'instance NetScaler VPX. Vous pouvez observer que l'interface PV (1/1) et l'interface VF CX3 (50/1) ont les mêmes adresses MAC (00:22:48:1c:99:3e). Cela indique que les deux interfaces sont regroupées ensemble.

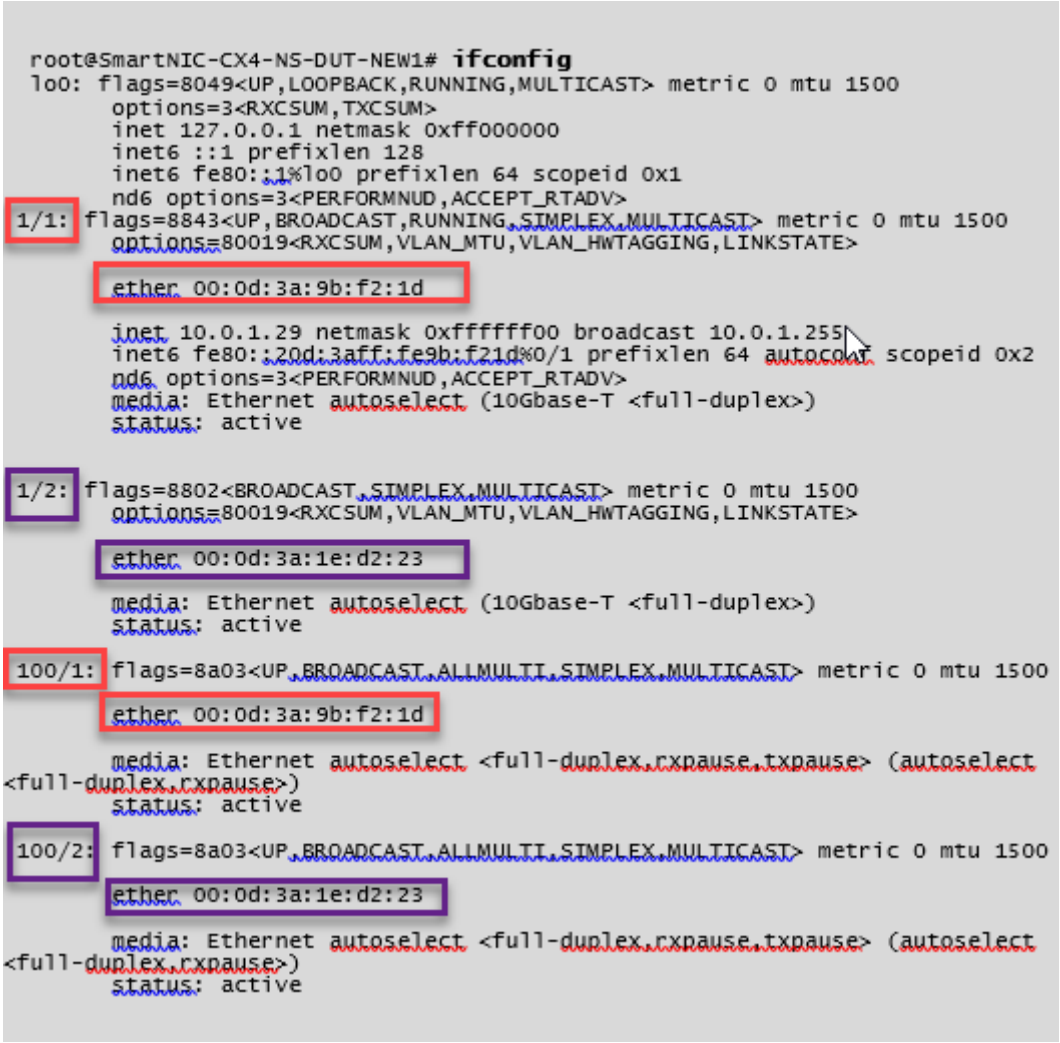
```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Exemple de carte réseau ConnectX4 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox Con-

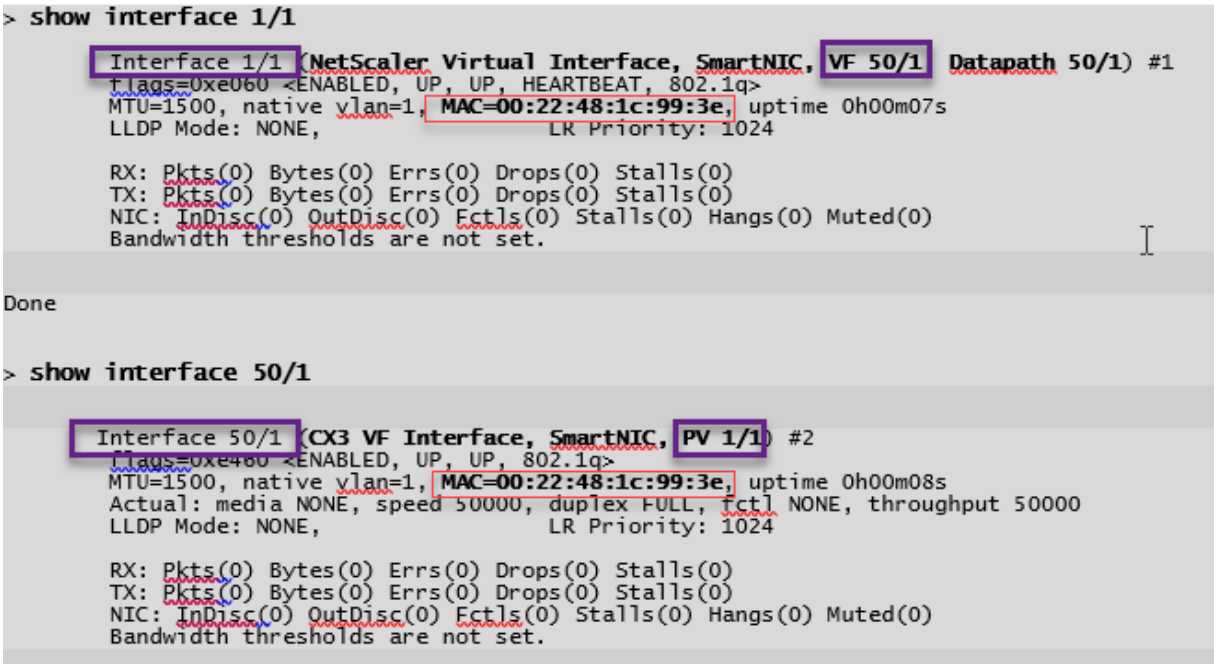
nectX4. Le « 100/n » indique les interfaces VF des cartes réseau Mellanox ConnectX4. 0/1, 1/1 et 1/2 indiquent les interfaces PV de l'instance NetScaler VPX. Vous pouvez observer que les interfaces PV (1/1) et CX4 VF (100/1) ont les mêmes adresses MAC (00:0d:3a:9b:f2:1d). Cela indique que les deux interfaces sont regroupées ensemble. De même, l'interface PV (1/2) et l'interface VF CX4 (100/2) ont les mêmes adresses MAC (00:0 d:3a:1e:d 2:23).



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide d'ADC CLI

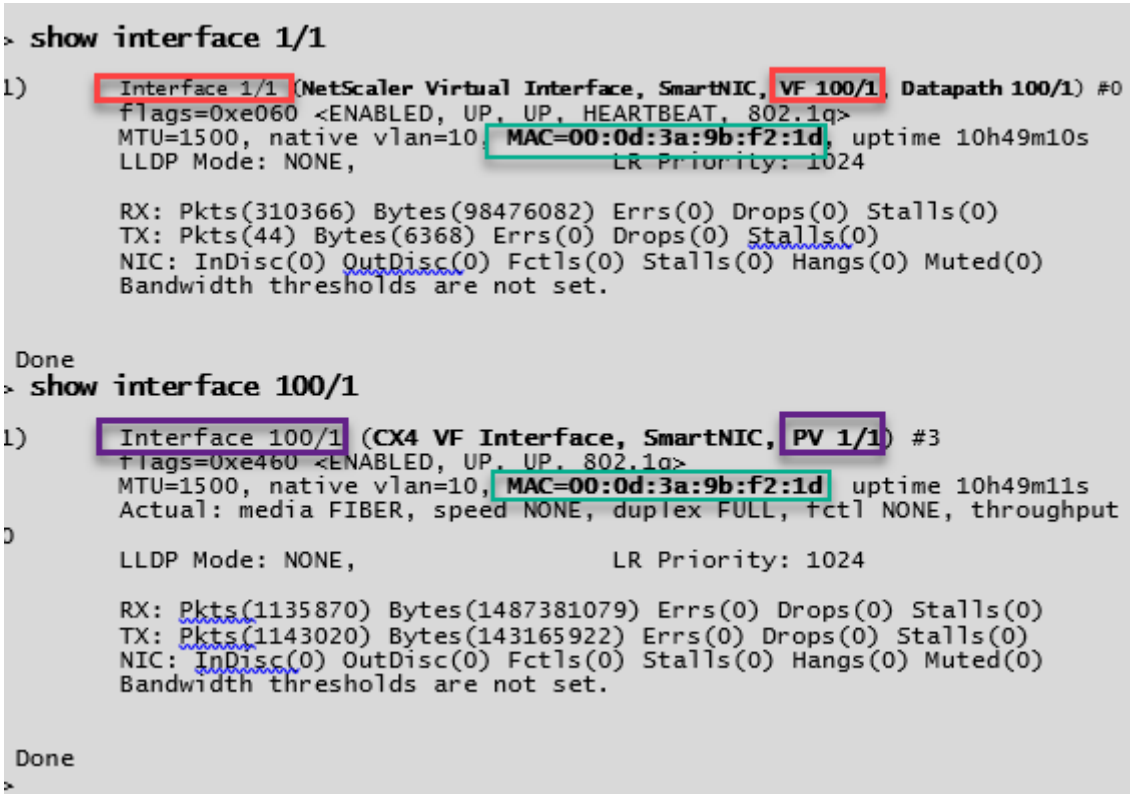
Exemple de carte réseau ConnectX3 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 50/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 50/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 50/1, qui est une interface ConnectX3. Vous pouvez voir que la sortie « show interface » de l'interface PV (1/1) pointe vers le VF (50/1). De même, la sortie « show interface » de l'interface VF (50/1) pointe vers l'interface photovoltaïque (1/1).



Exemple de carte réseau ConnectX4 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 100/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 100/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 100/1, qui est une interface ConnectX4. Vous pouvez voir que la sortie « show interface » de l'interface photovoltaïque (1/1) pointe vers le VF (100/1). De même, la sortie « show interface » de l'interface VF (100/1) pointe vers l'interface photovoltaïque (1/1).



Points à noter dans NetScaler

- L'interface photovoltaïque est considérée comme l'interface principale ou principale pour toutes les opérations nécessaires. Les configurations doivent être effectuées uniquement sur des interfaces photovoltaïques.
- Toutes les opérations « set » sur une interface VF sont bloquées à l'exception des opérations suivantes :
  - interface d'activation
  - interface de désactivation
  - interface de réinitialisation
  - statistiques claires

> **Remarque :**
>
> Citrix recommande de ne pas effectuer d'opérations sur l'interface VF.

- Vous pouvez vérifier la liaison de l'interface PV avec l'interface VF à l'aide de la `show interface` commande.
- À partir de la version 13.1-33.x de NetScaler, une instance NetScaler VPX peut gérer de manière fluide les suppressions dynamiques et le rattachement des cartes réseau supprimées dans le

réseau accéléré Azure. Azure peut supprimer la carte réseau VF SR-IOV de la mise en réseau accélérée pour ses activités de maintenance d'hôtes. Chaque fois qu'une carte réseau est supprimée d'une machine virtuelle Azure, l'instance NetScaler VPX affiche l'état de l'interface comme « Link Down » et le trafic passe uniquement par l'interface virtuelle. Une fois la carte réseau supprimée reconnectée, les instances VPX utilisent la carte réseau VF SR-IOV reconnectée. Ce processus se déroule sans problème et ne nécessite aucune configuration.

Configurer un VLAN sur une interface PV

Lorsqu'une interface PV est liée à un VLAN, l'interface VF accélérée associée est également liée au même VLAN que l'interface PV. Dans cet exemple, l'interface PV (1/1) est liée au VLAN (20). L'interface VF (100/1) fournie avec l'interface PV (1/1) est également liée au VLAN 20.

Exemple

1. Créez un VLAN.

```
add vlan 20
```

2. Liez un VLAN à l'interface PV.

```
bind vlan 20  – ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2
```

> **Remarque :**
>
> L'opération de liaison VLAN n'est pas autorisée sur une interface VF accélérée.

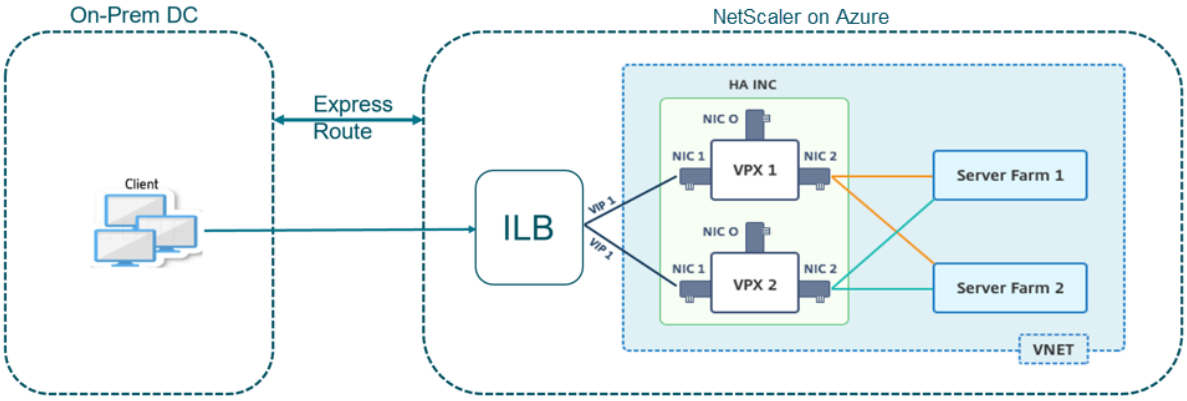
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
```


Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler avec Azure ILB

October 17, 2024

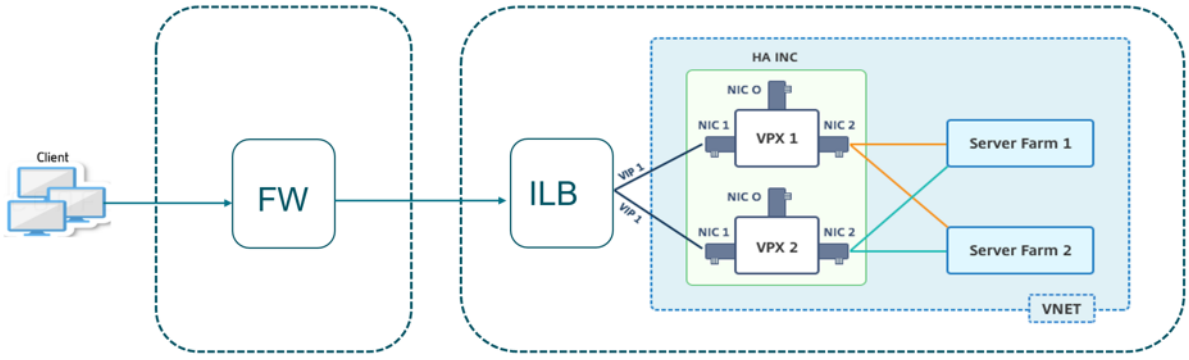
Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard pour les applications intranet. L'équilibreur de charge interne (ILB) Azure utilise une adresse IP interne ou privée pour le frontal, comme illustré à la Figure 1. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au trafic côté client et côté serveur, chaque sous-réseau appartenant à une carte réseau différente sur chaque périphérique.

Figure 1 : paire NetScaler HA pour les clients d'un réseau interne



Vous pouvez également utiliser ce déploiement lorsque la paire NetScaler HA se trouve derrière un pare-feu, comme le montre la Figure 2. L'adresse IP publique appartient au pare-feu et est NAT à l'adresse IP frontale de l'ILB.

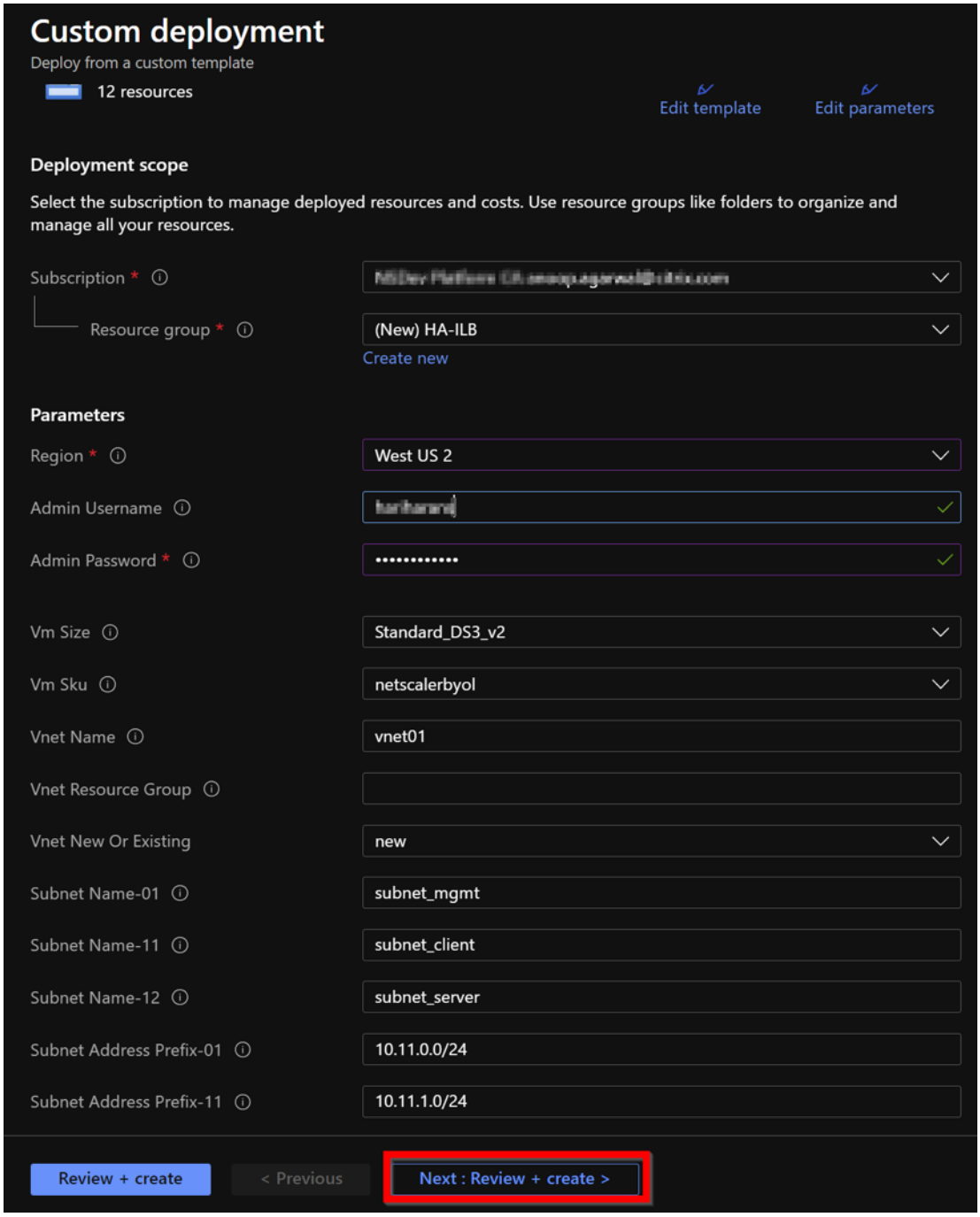
Figure 2 : paire NetScaler HA avec un pare-feu doté d'une adresse IP publique



Vous pouvez obtenir le modèle de paire NetScaler HA pour les applications intranet sur le portail Azure

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide des jeux de disponibilité Azure.

1. Sur le portail Azure, accédez à la page **Déploiement personnalisé** .
2. La page **Principes** de base s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, entrez les détails de la région, du nom d'utilisateur administrateur, du mot de passe administrateur, du type de licence (`VM sku`) et d'autres champs.

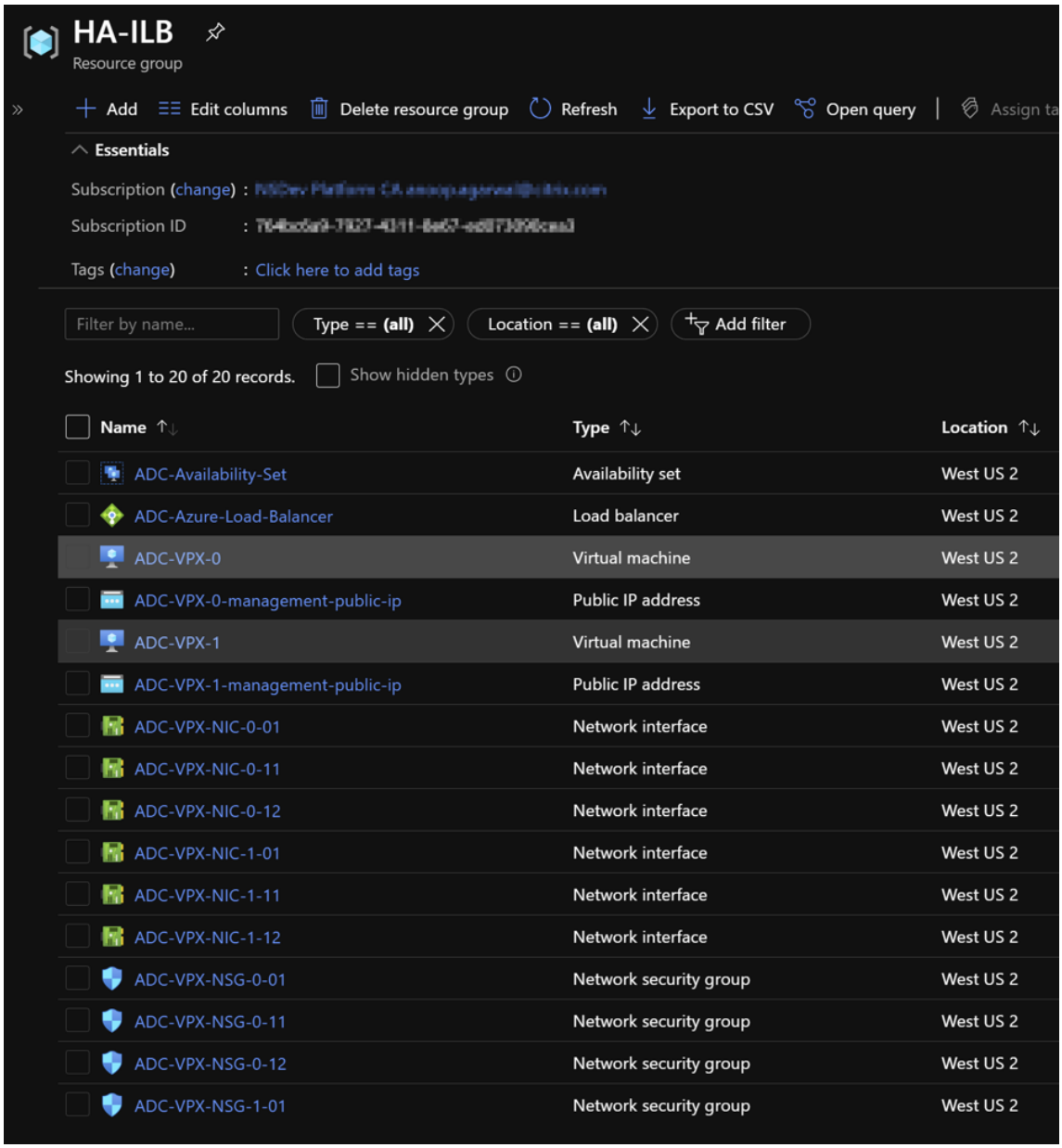


3. Cliquez sur **Next : Review + create >**.

   Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le groupe de ressources sur le portail Azure pour afficher les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité s'affiche sous la forme ADC-VPX-0 et ADC-VPX-1.

   Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

   Une fois la configuration requise terminée, les ressources suivantes sont créées.



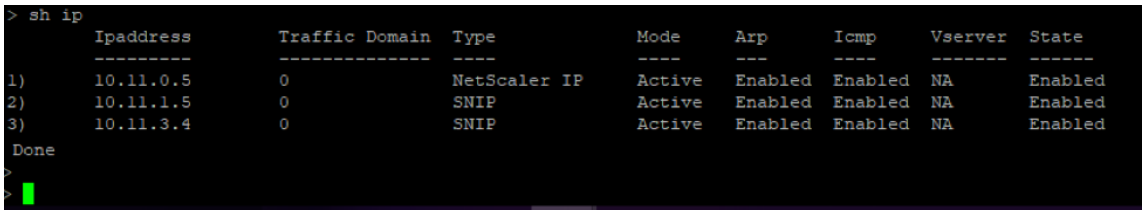
4. Ouvrez une session sur les nœuds **ADC-VPX-0** et **ADC-VPX-1** pour valider la configuration suiv-

ante :

- Les adresses NSIP des deux nœuds doivent se trouver dans le sous-réseau de gestion.
- Sur les nœuds principal (ADC-VPX-0) et secondaire (ADC-VPX-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ILB et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication avec le serveur principal.

> **Remarque :**
>
> En mode HA-INC, l'adresse SNIP des machines virtuelles ADC-VPX-0 et ADC-VPX-1 est différente dans le même sous-réseau, contrairement au déploiement ADC HA local classique où les deux sont identiques. Pour prendre en charge les déploiements lorsque le SNIP de la paire VPX se trouve dans des sous-réseaux différents ou chaque fois que le VIP ne se trouve pas dans le même sous-réseau qu'un SNIP, vous devez soit activer le transfert basé sur Mac (MBF), soit ajouter une route hôte statique pour chaque VIP à chaque nœud VPX.

Sur le nœud principal (ADC-VPX-0)




```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

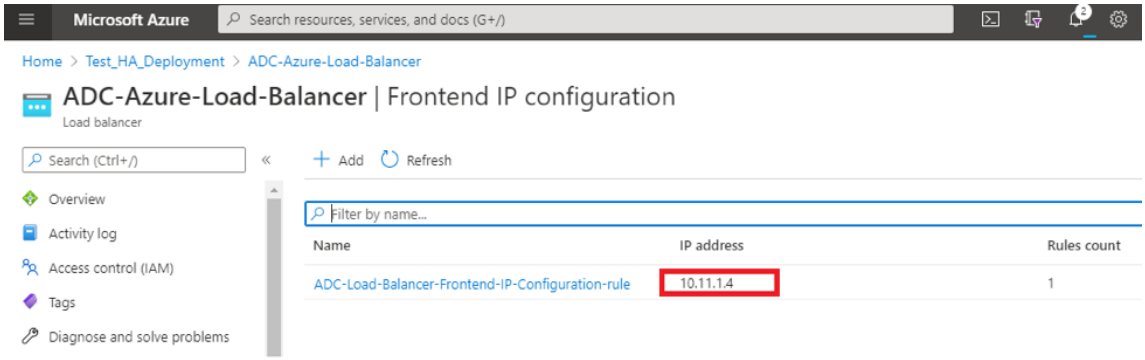
Sur le nœud secondaire (ADC-VPX-1)

```
> sh ip
        Ipaddress       Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------       --------------  ----            ----     ---      ----     -------  ------
1)      10.11.0.4       0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.6       0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.5       0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

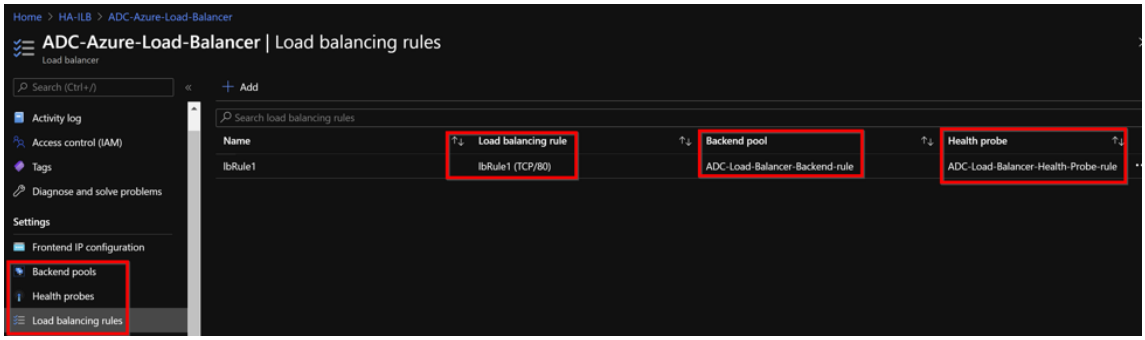


```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

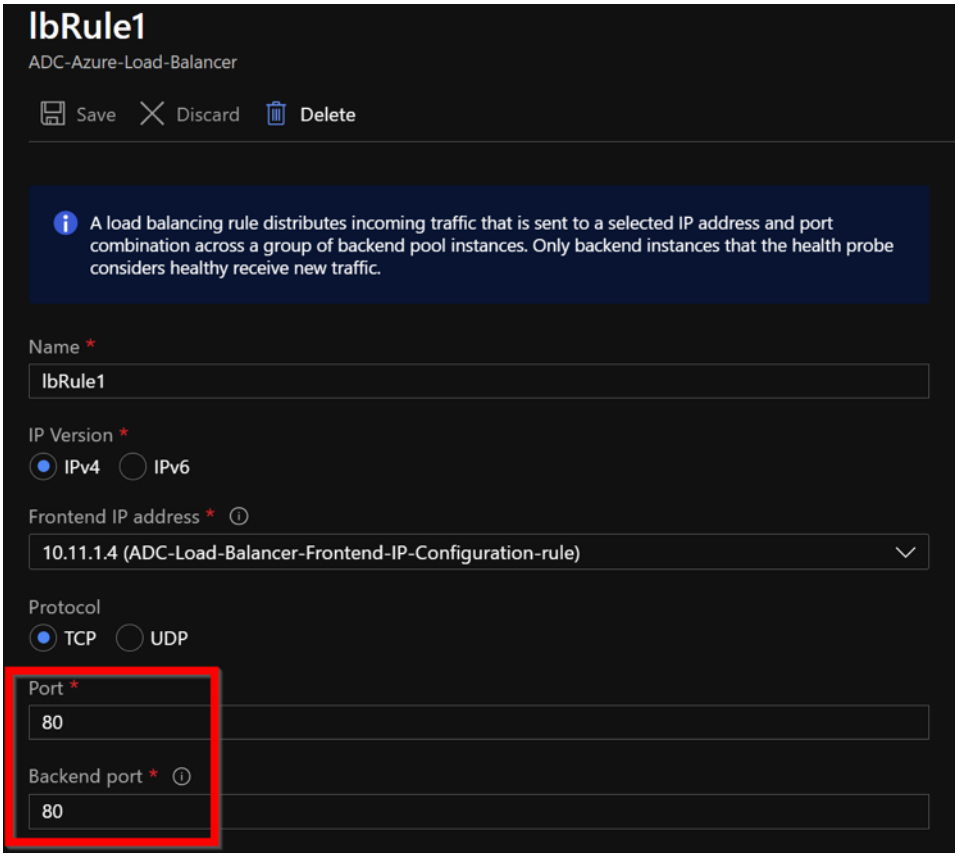
5. Une fois que les nœuds principal et secondaire sont UP et que l'état de synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (ADC-VPX-0) avec l'adresse IP flottante privée (FIP) de l'équilibreur de charge ADC Azure. Pour plus d'informations, consultez la section Exemple de configuration .
6. Pour rechercher l'adresse IP privée de l'équilibreur de charge ADC Azure, accédez au **portail Azure > AdC Azure Load Balancer > Configuration IP frontend**.



7. Dans la page de configuration de l'**Azure Load Balancer**, le déploiement du modèle ARM permet de créer la règle d'équilibrage de charge, les pools principaux et les sondes d'état.

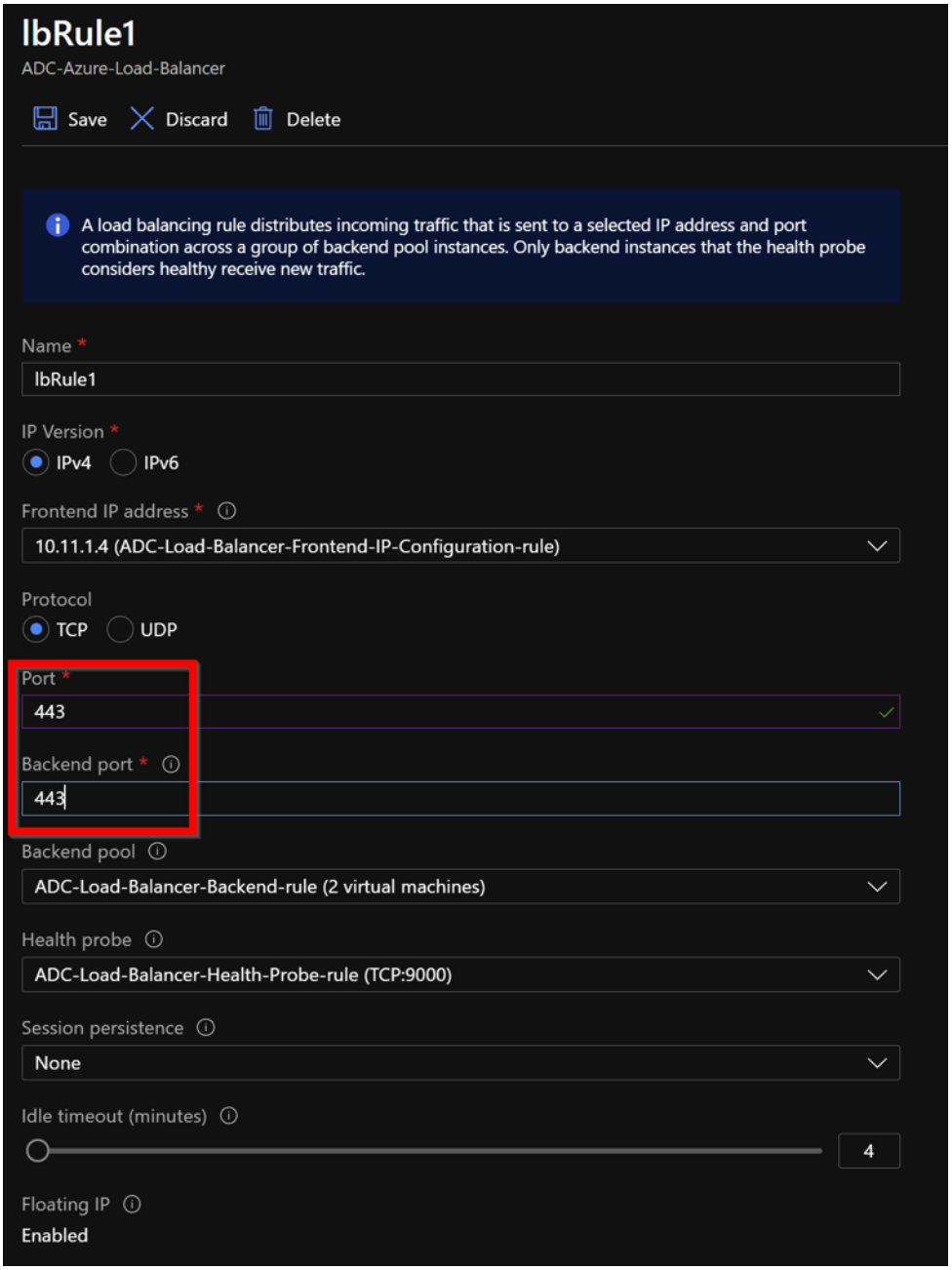


   - La règle d'équilibrage de la charge de travail (LBrule1) utilise le port 80, par défaut.



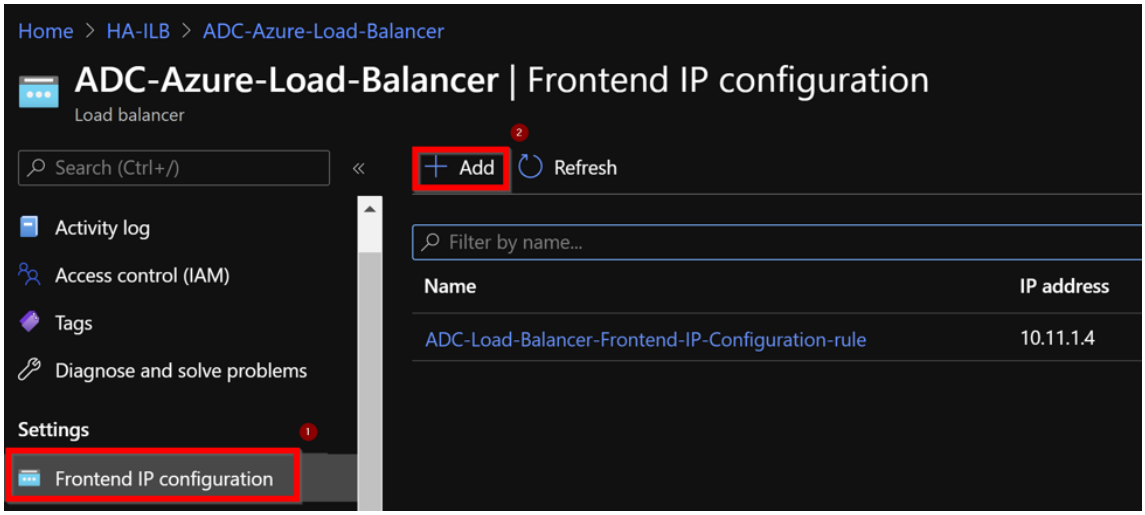
- Modifiez la règle pour utiliser le port 443 et enregistrez les modifications.

  > **Remarque :**
  >
  > Pour une sécurité renforcée, Citrix vous recommande d'utiliser le port SSL 443 pour le serveur virtuel LB ou le serveur virtuel Gateway.

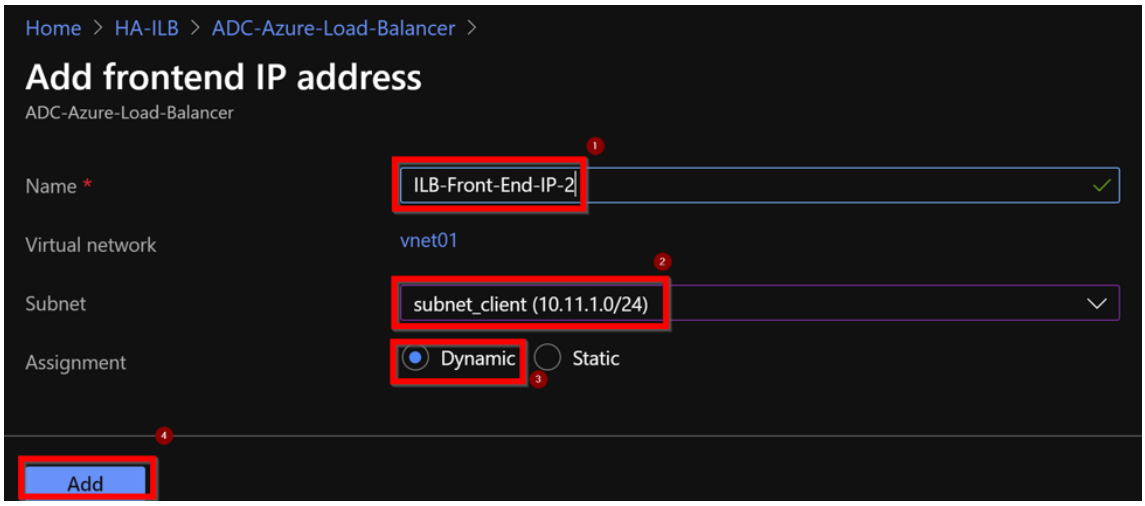


Pour ajouter d'autres adresses VIP sur l'ADC, effectuez les opérations suivantes :

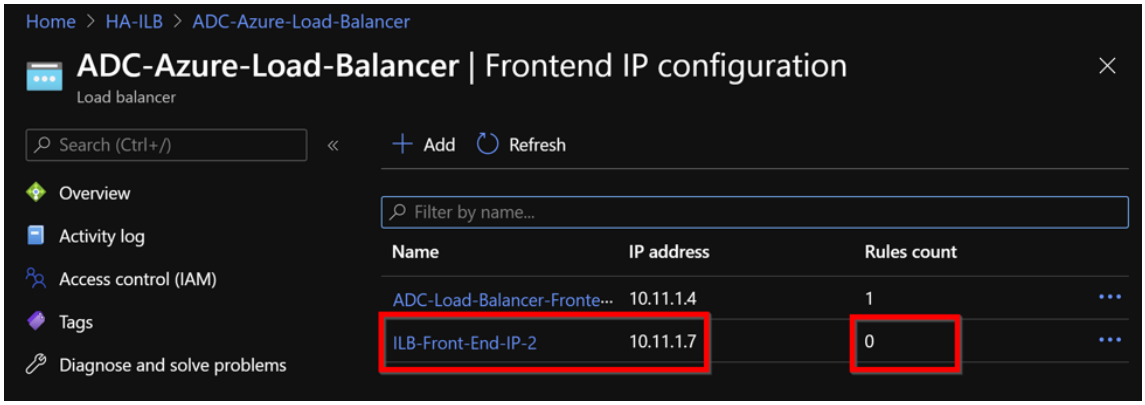
1. Accédez à **Azure Load Balancer > Configuration IP frontend**, puis cliquez sur **Ajouter** pour créer une nouvelle adresse IP d'équilibrage de charge interne.



2. Dans la page **Ajouter une adresse IP frontale**, saisissez un nom, choisissez le sous-réseau client, attribuez une adresse IP dynamique ou statique, puis cliquez sur **Ajouter**.

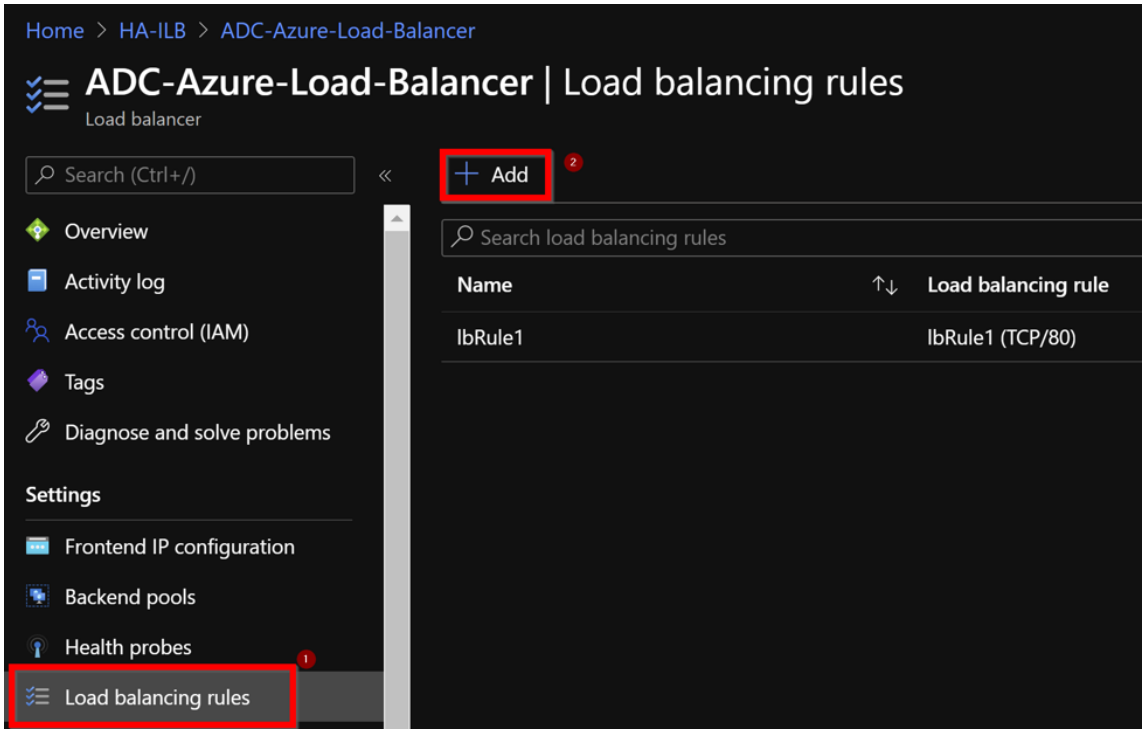


3. L'adresse IP frontale est créée mais aucune règle d'équilibrage de charge n'est associée. Créez une nouvelle règle d'équilibrage de charge et associez-la à l'adresse IP frontale.

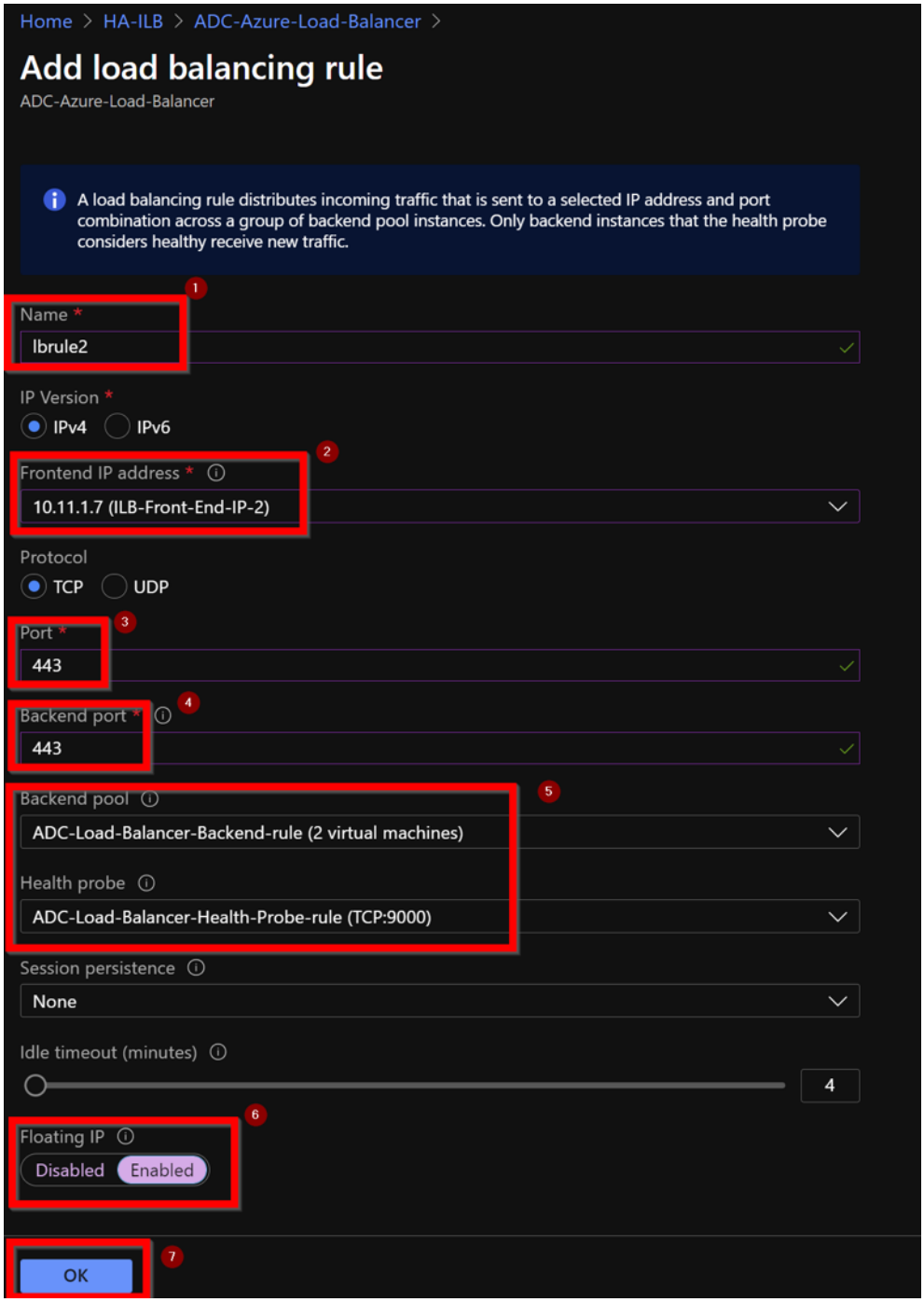


4. Sur la page **Azure Load Balancer**, sélectionnez **Règles d'équilibrage**de charge, puis cliquez

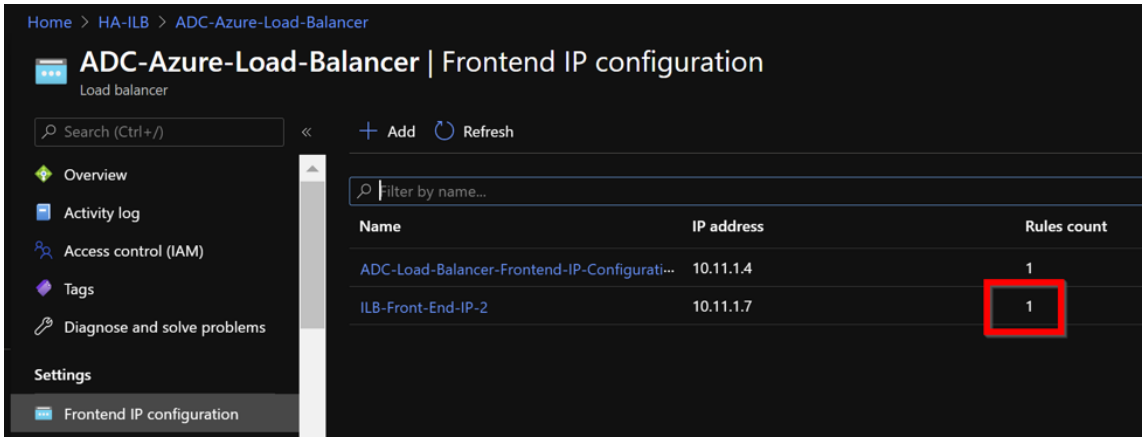
sur **Ajouter**.



5. Créez une nouvelle règle d'équilibrage de la charge de travail en choisissant la nouvelle adresse IP frontale et le port. Le champ**IP flottant** doit être défini sur **Activé**.



6. Maintenant, la **configuration IP du frontend** affiche la règle d'équilibrage de charge appliquée.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
```

Vous pouvez désormais accéder à l'équilibrage de charge ou au serveur virtuel VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP interne de l'ILB.

Consultez la section **Ressources** pour plus d'informations sur la façon de configurer le serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Configuration de nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler pour les applications connectées à Internet

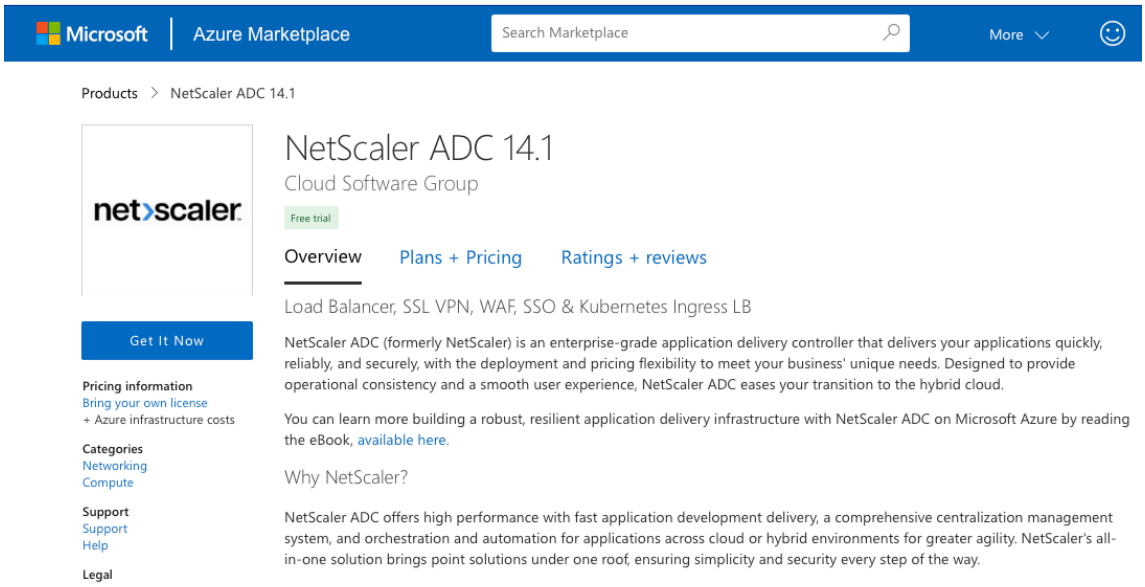
October 17, 2024

Vous pouvez déployer rapidement et efficacement deux instances VPX en mode HA-INC en utilisant le modèle standard pour les applications connectées à Internet. L'équilibreur de charge Azure (ALB) utilise une adresse IP publique pour le front-end. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au trafic côté client et côté serveur. Chaque sous-réseau possède deux cartes réseau pour les deux instances VPX.

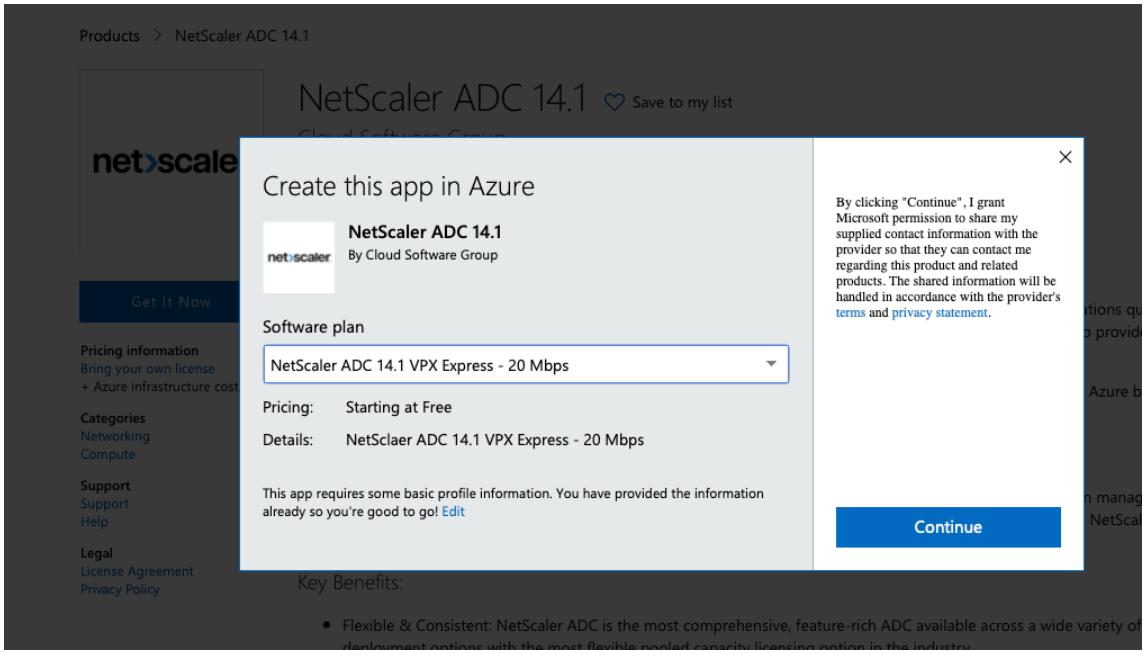
Vous pouvez obtenir le modèle de paire NetScaler HA pour les applications connectées à Internet sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide de jeux de disponibilité Azure ou d'une zone de disponibilité.

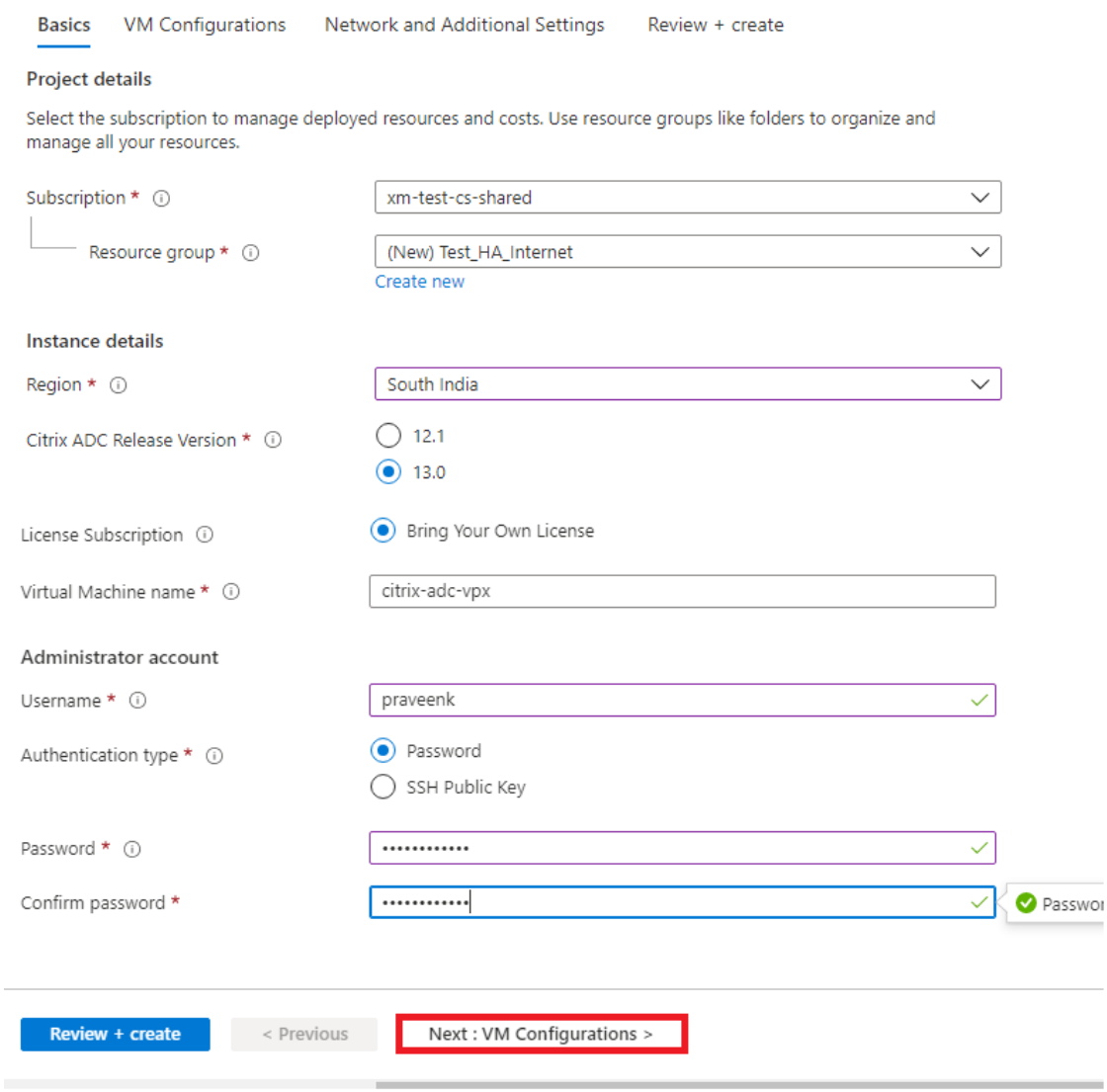
1. Sur Azure Marketplace, recherchez **NetScaler.**
2. Cliquez sur **GET IT NOW**.



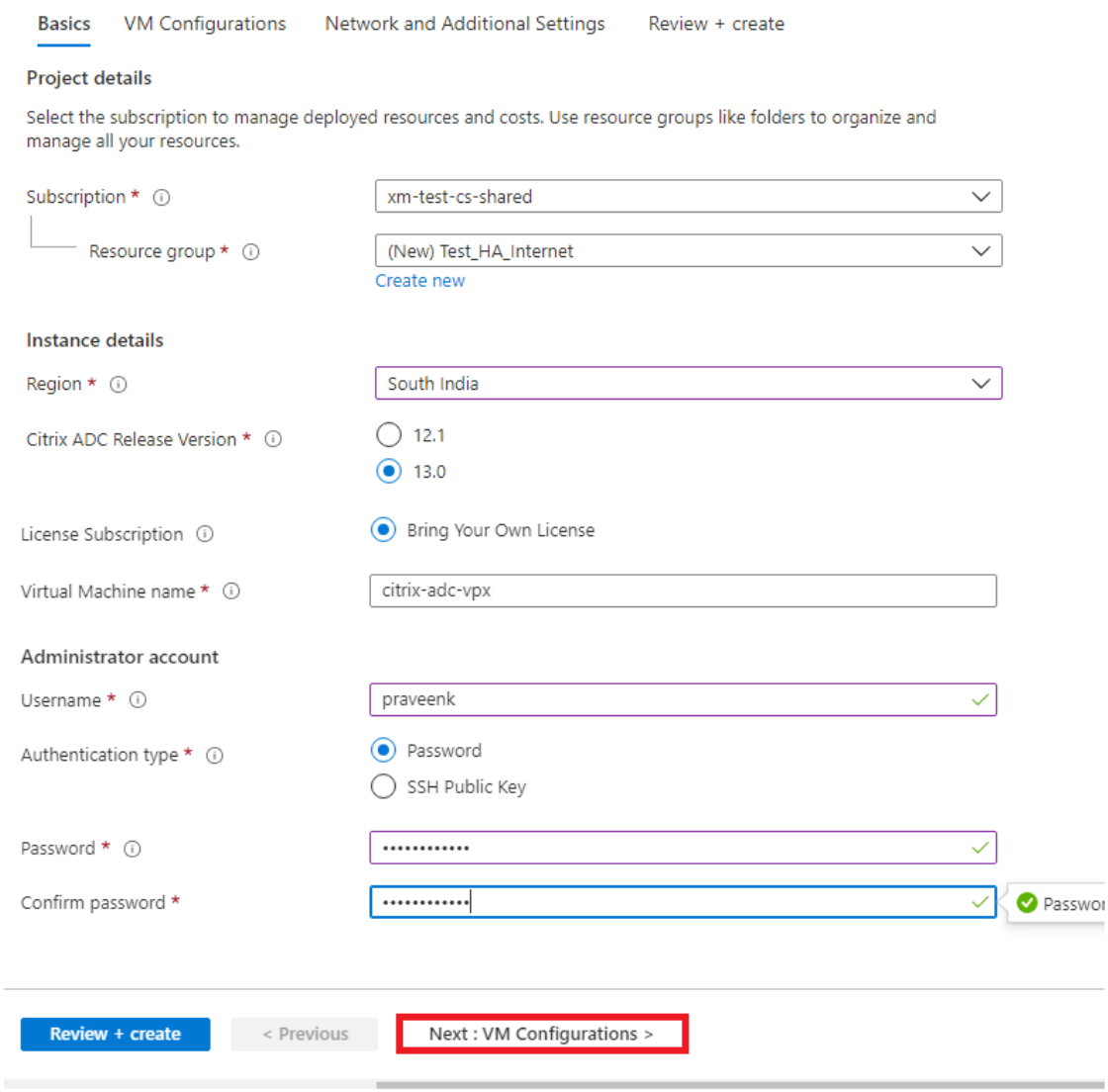
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



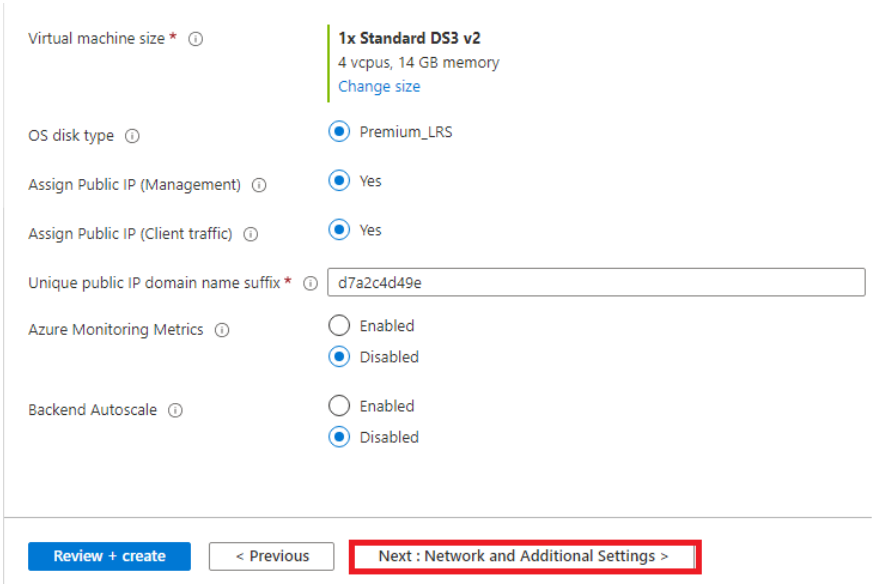
4. La page **Principes** de base s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



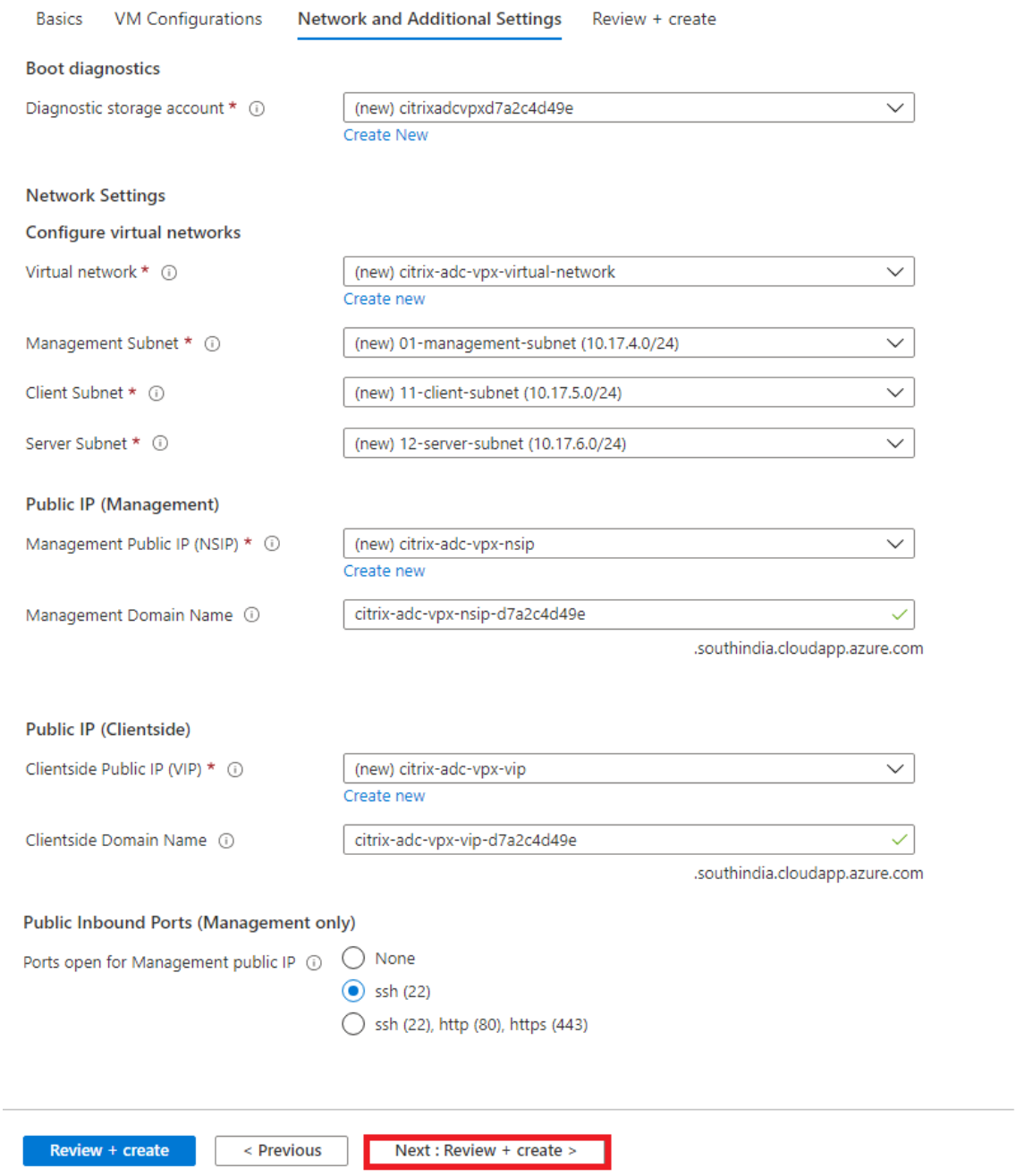
5. Cliquez sur **Suivant : Configurations de machines virtuelles**.



6. Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :
   - Configurer le suffixe du nom de domaine IP public
   - Activer ou désactiver **Azure Monitoring Metrics**
   - Activer ou désactiver **Backend Autoscale**
7. Cliquez sur **Suivant : Réseau et paramètres supplémentaires**



8. Sur la page **Paramètres réseau et supplémentaires**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.



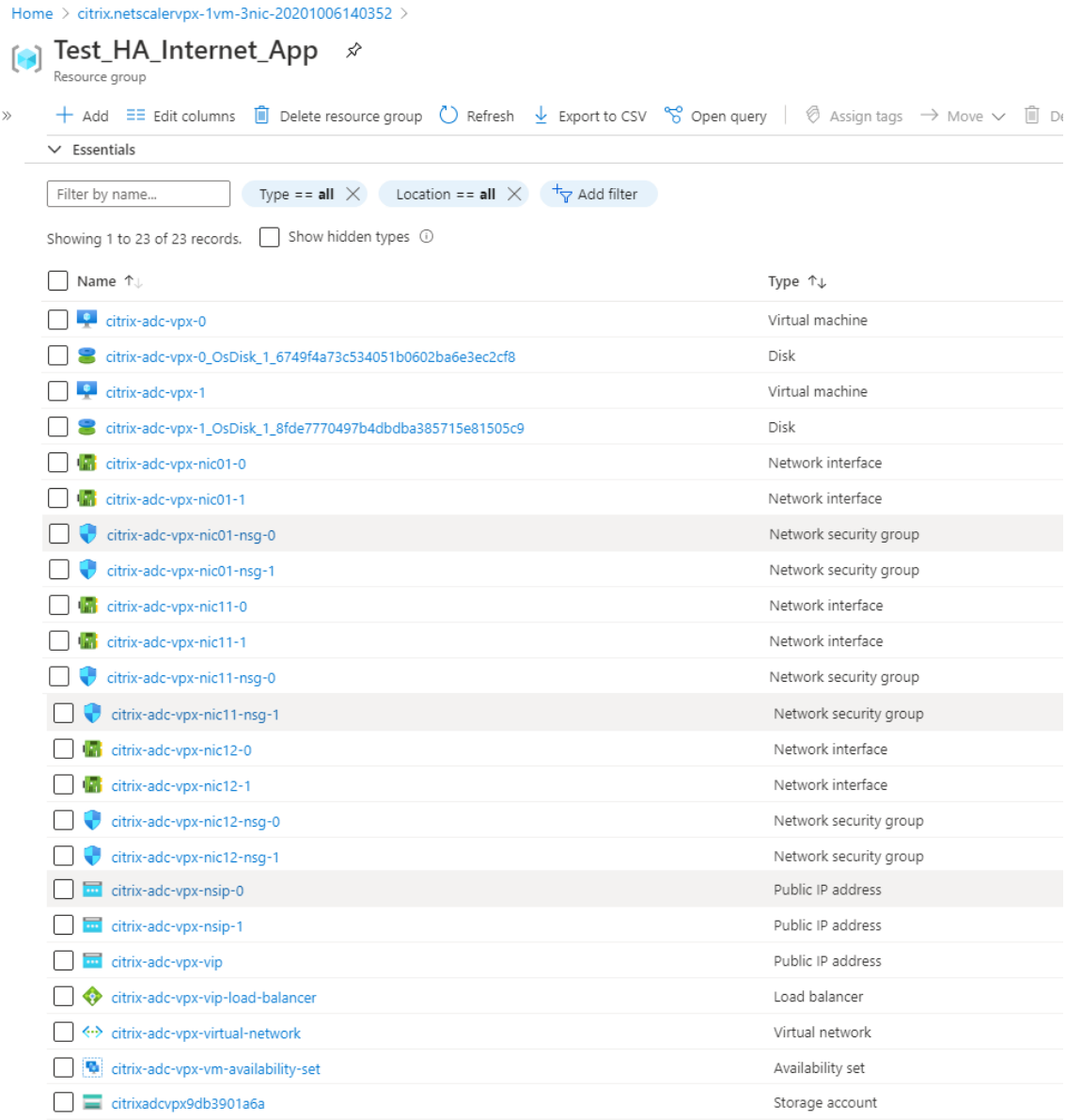
9. Cliquez sur **Suivant : Réviser + créer**.
10. Passez en revue les paramètres de base, la configuration de la machine virtuelle, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**.

    Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois l'opération terminée, sélectionnez le groupe de ressources sur le portail Azure pour voir les détails de configuration, tels que les règles LB, les pools dorsaux et

les sondes de santé. La paire haute disponibilité apparaît sous les **formes citrix-adc-vpx-0** et **citrix-adc-vpx-1**.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Une fois la configuration requise terminée, les ressources suivantes sont créées.



11. Vous devez vous connecter aux nœuds **citrix-adc-vpx-0** et **citrix-adc-vpx-1** pour valider la configuration suivante :

    - Les adresses NSIP des deux nœuds doivent se trouver dans le sous-réseau de gestion.
    - Sur les nœuds principal (citrix-adc-vpx-0) et secondaire (citrix-adc-vpx-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ALB

et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication avec le serveur principal.

> **Remarque :**
>
> En mode HA-INC, les adresses SNIP des machines virtuelles citrix-adc-vpx-0 et citrix-adc-vpx-1 sont différentes, contrairement au déploiement classique de haute disponibilité ADC sur site où les deux sont identiques.

Sur le nœud principal (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

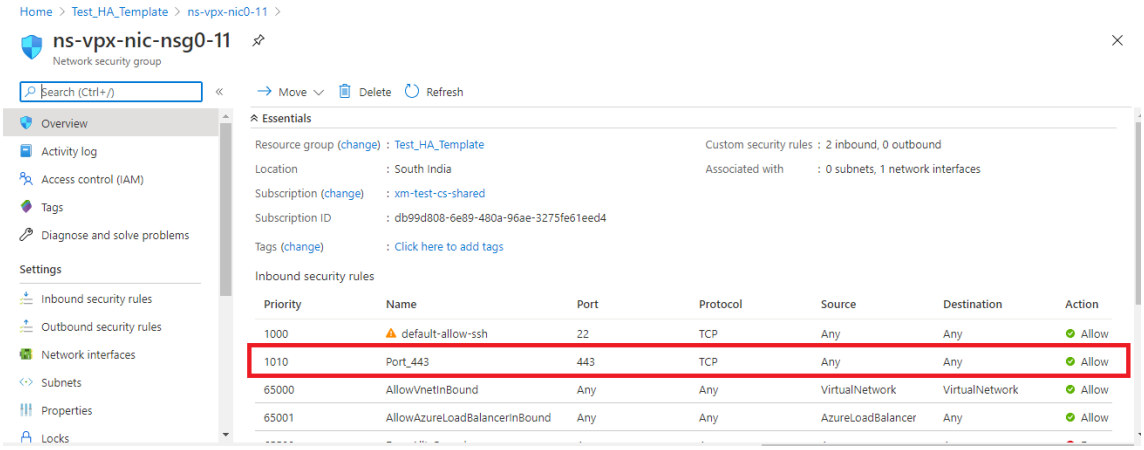
Sur le nœud secondaire (citrix-adc-vpx-1)

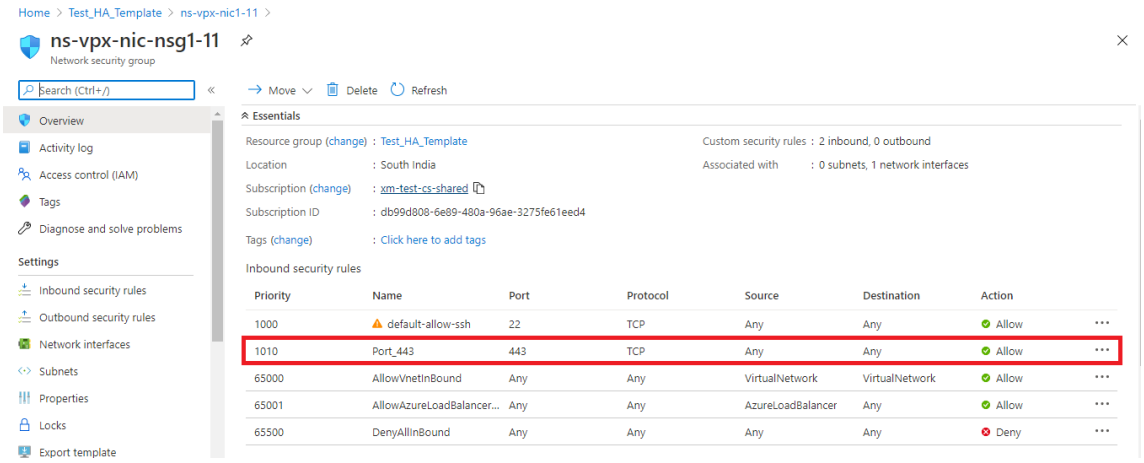

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

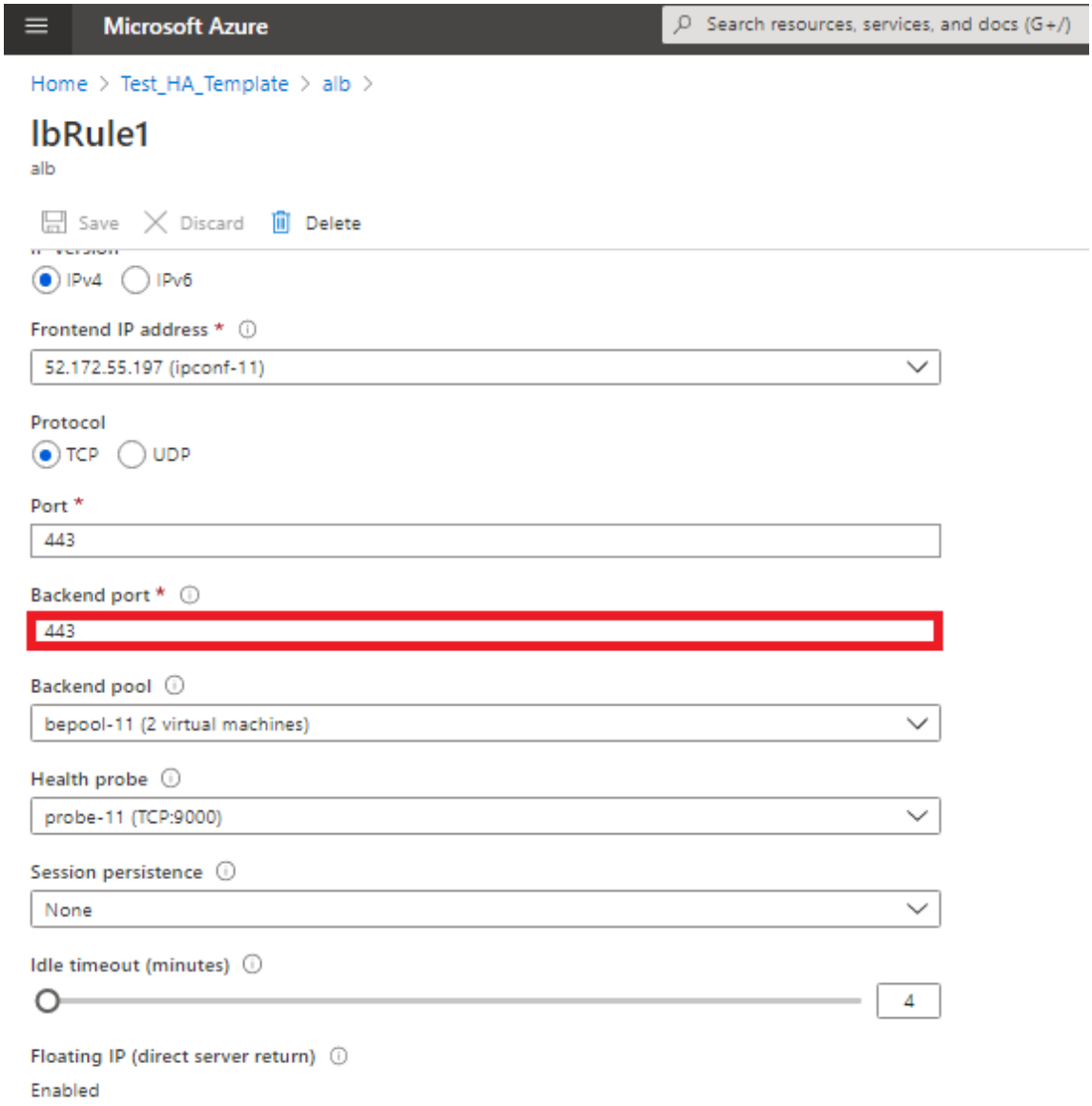
12. Une fois que les nœuds principal et secondaire sont UP et que l'état Synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (citrix-adc-vpx-0) avec l'adresse IP publique du serveur virtuel ALB. Pour plus d'informations, consultez la section Exemple de configuration .
13. Pour rechercher l'adresse IP publique du serveur virtuel ALB, accédez au **portail Azure > Équilibreur de charge Azure > Configuration IP frontend**.

14. Ajoutez la règle de sécurité entrante pour le port 443 du serveur virtuel dans le groupe de sécurité réseau des deux interfaces clientes.

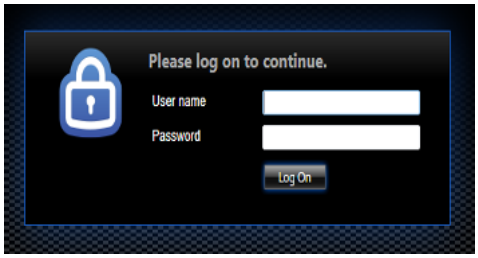




15. Configurez le port ALB auquel vous souhaitez accéder et créez une règle de sécurité entrante pour le port spécifié. Le port principal est le port de votre serveur virtuel d'équilibrage de charge ou le port du serveur virtuel VPN.



16. Vous pouvez désormais accéder au serveur virtuel d'équilibrage de charge ou au serveur virtuel VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP publique ALB.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
```

Vous pouvez désormais accéder à l'équilibrage de charge ou au serveur virtuel VPN à l'aide du FQDN associé à l'adresse IP publique d'ALB.

Consultez la section **Ressources** pour plus d'informations sur la configuration du serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Créer des serveurs virtuels
- Configurer l'équilibrage de charge de base

Configurer une configuration haute disponibilité avec des équilibreurs de charge externes et internes Azure simultanément

October 17, 2024

La paire haute disponibilité sur Azure prend en charge simultanément les équilibreurs de charge externes et internes.

Vous disposez des deux options suivantes pour configurer une paire haute disponibilité à l'aide d'équilibreurs de charge externes et internes Azure :

- Utilisation de deux serveurs virtuels LB sur l'appliance NetScaler.
- Utilisation d'un serveur virtuel LB et d'un ensemble d'adresses IP. Le serveur virtuel LB unique sert le trafic vers plusieurs adresses IP définies par l'IPSet.

Effectuez les étapes suivantes pour configurer une paire haute disponibilité sur Azure en utilisant simultanément les équilibreurs de charge externes et internes :

Pour les étapes 1 et 2, utilisez le portail Azure. Pour les étapes 3 et 4, utilisez l'interface graphique NetScaler VPX ou la CLI.

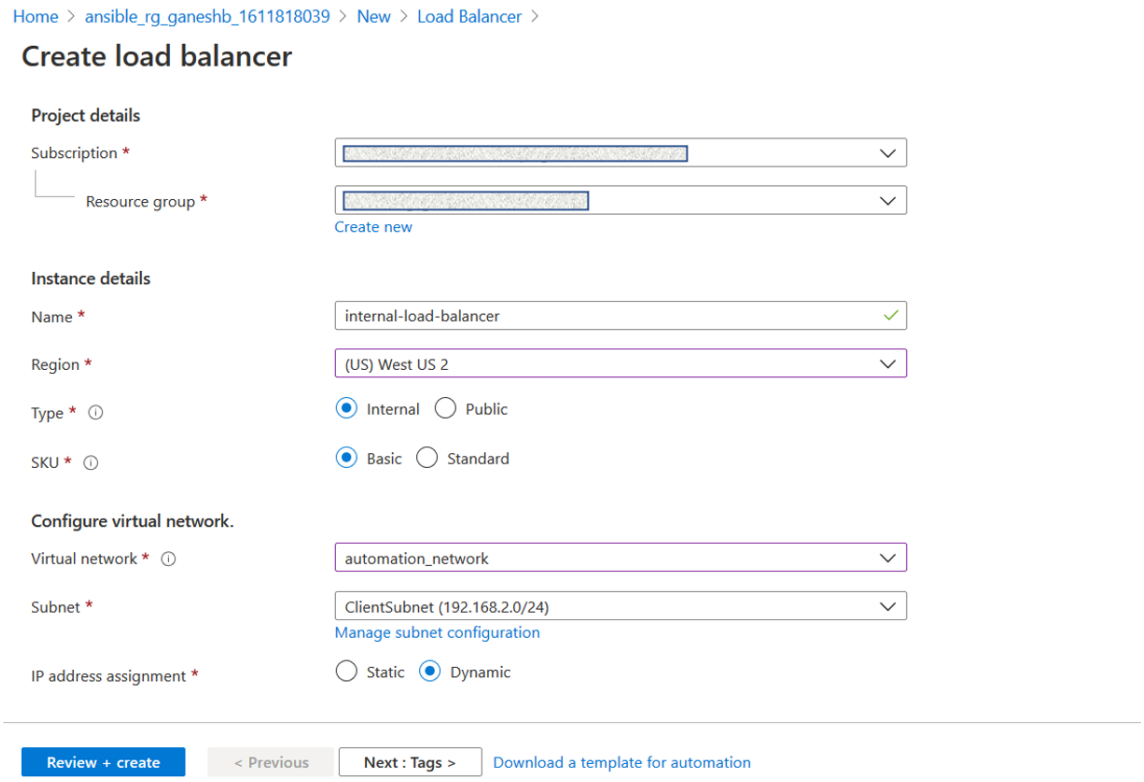
Étape 1. Configurez un équilibreur de charge Azure, soit un équilibreur de charge externe, soit un équilibreur de charge interne.

Pour plus d'informations sur la configuration d'une configuration haute disponibilité avec des équilibreurs de charge externes Azure, consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et carte réseau.

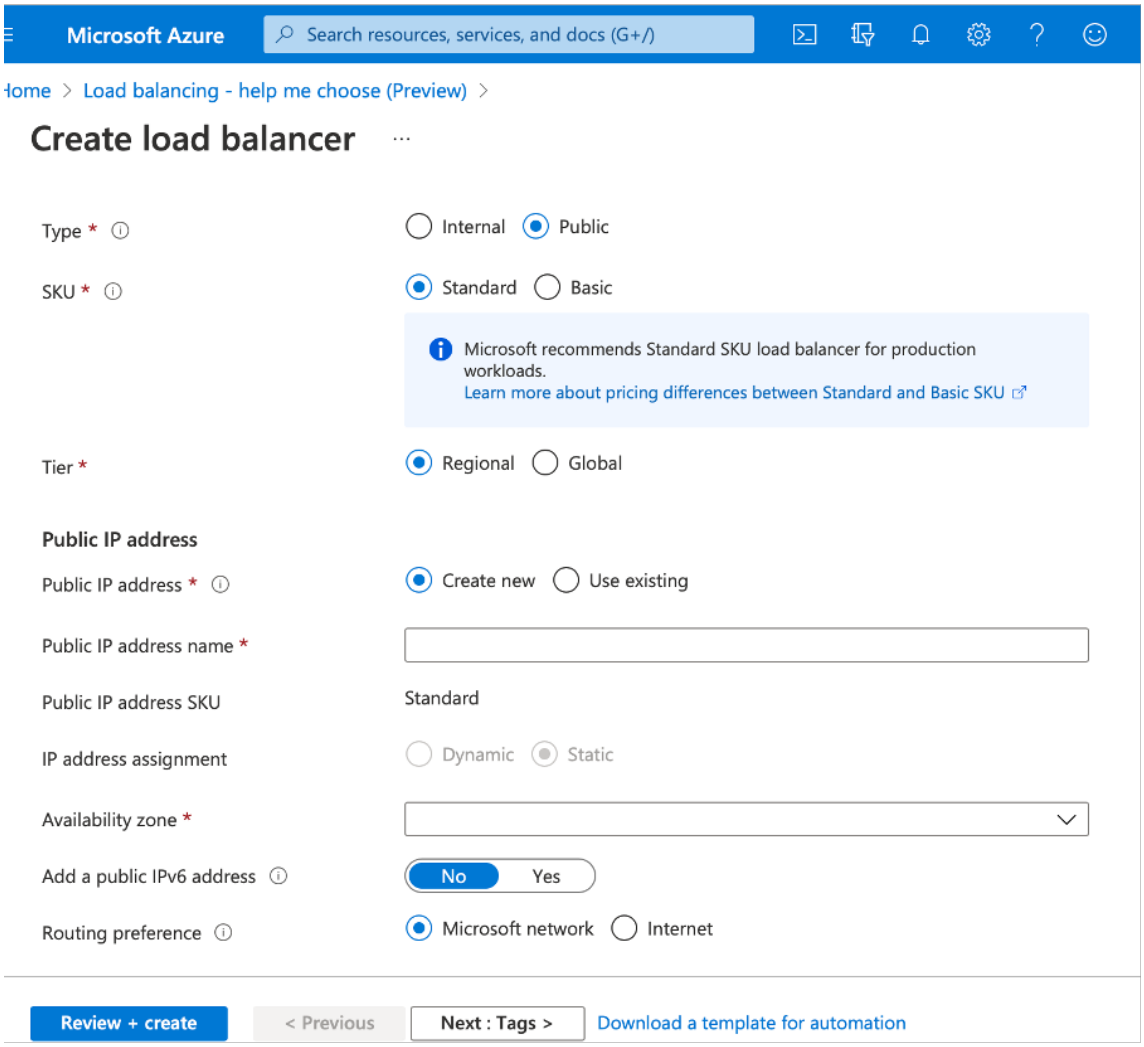
Pour plus d'informations sur la configuration de la haute disponibilité avec les équilibreurs de charge internes Azure, consultez Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler avec Azure ILB.

Étape 2. Créez un équilibreur de charge supplémentaire (ILB) dans votre groupe de ressources. À l'étape 1, si vous avez créé un équilibreur de charge externe, vous créez maintenant un équilibreur de charge interne et inversement.

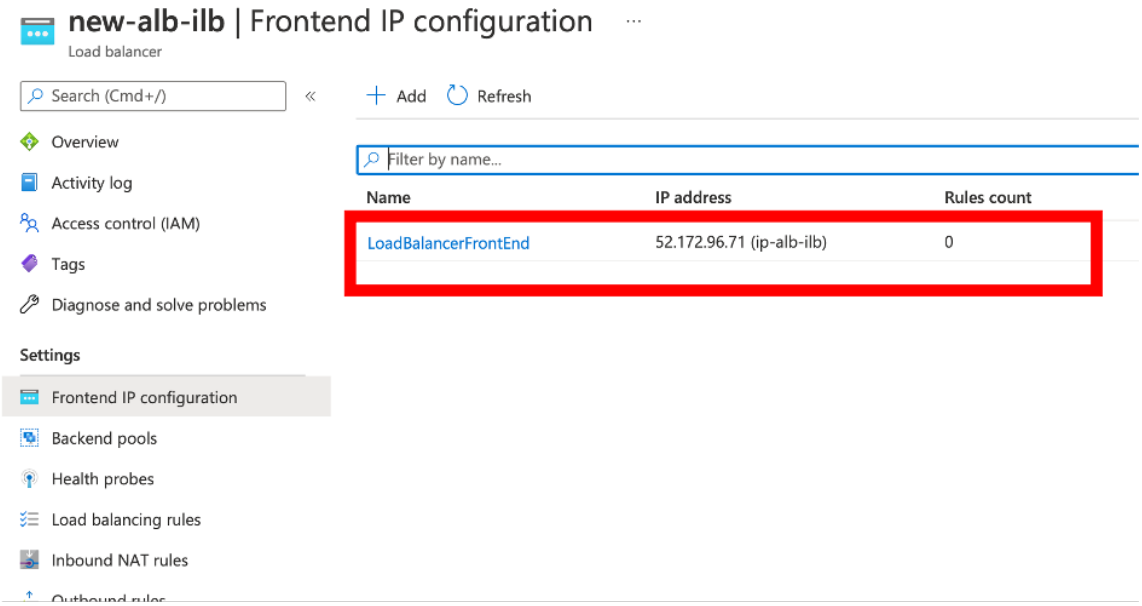
- Pour créer un équilibreur de charge interne, choisissez le type d'équilibreur de charge comme **Interne**. Pour le champ **Sous-réseau**, vous devez choisir le sous-réseau de votre client NetScaler. Vous pouvez choisir de fournir une adresse IP statique dans ce sous-réseau, à condition qu'il n'y ait pas de conflit. Sinon, choisissez l'adresse IP dynamique.



- Pour créer un équilibreur de charge externe, choisissez le type d'équilibreur de charge comme étant **Public** et créez l'adresse IP publique ici.



1. Après avoir créé Azure Load Balancer, accédez à la **configuration IP frontend** et notez l'adresse IP affichée ici. Vous devez utiliser cette adresse IP lors de la création du serveur virtuel d'équilibrage de charge ADC, comme à l'étape 3.



2. Sur la page de **configuration d'Azure Load Balancer**, le déploiement du modèle ARM permet de créer la règle LB, les pools principaux et les sondes de santé.
3. Ajoutez les cartes réseau client de la paire haute disponibilité au pool principal de l'ILB.
4. Créer une sonde de santé (TCP, port 9000)
5. Créez deux règles d'équilibrage de charge :
    - Une règle LB pour le trafic HTTP (cas d'utilisation de l'application Web) sur le port 80. La règle doit également utiliser le port principal 80. Sélectionnez le pool de backend créé et la sonde de santé. L'adresse IP flottante doit être activée.
    - Une autre règle LB pour le trafic HTTPS ou CVAD sur le port 443. Le processus est le même que le trafic HTTP.

Étape 3. Sur le nœud principal de l'appliance NetScaler, créez un serveur virtuel d'équilibrage de charge pour ILB.

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>]
   [<port>]
```

Exemple

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```

> **Remarque :**

> Utilisez l'adresse IP frontale de l'équilibreur de charge, associée à l'équilibreur de charge supplémentaire que vous créez à l'étape 2.

2. Liez un service à un serveur virtuel d'équilibrage de charge.

```
bind lb vserver <name> <serviceName>
```

Exemple

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

Pour plus d'informations, voir Configurer l'équilibrage de charge de base.

Étape 4 : Au lieu de l'étape 3, vous pouvez créer un serveur virtuel d'équilibrage de charge pour ILB à l'aide d'IPsets.

1. Ajoutez une adresse IP de type IP de serveur virtuel (VIP).

```
add nsip <ILB Frontend IP address> -type <type>
```

Exemple

```
add nsip 52.172.96.71 -type vip
```

2. Ajoutez un IPSet sur les nœuds principaux et secondaires.

```
add ipset <name>
```

Exemple

```
add ipset ipset1
```

3. Liez les adresses IP au jeu d'adresses IP.

```
bind ipset <name> <ILB Frontend IP address>
```

Exemple

```
bind ipset ipset1 52.172.96.71
```

4. Définissez le serveur virtuel LB existant pour qu'il utilise IPSet.

```
set lb vserver <vserver name> -ipset <ipset name>
```

Exemple

```
set lb vserver vserver_name -ipset ipset1
```

Pour plus d'informations, voir Configurer un serveur virtuel multi-IP.

Installation d'une instance NetScaler VPX sur la solution Azure VMware

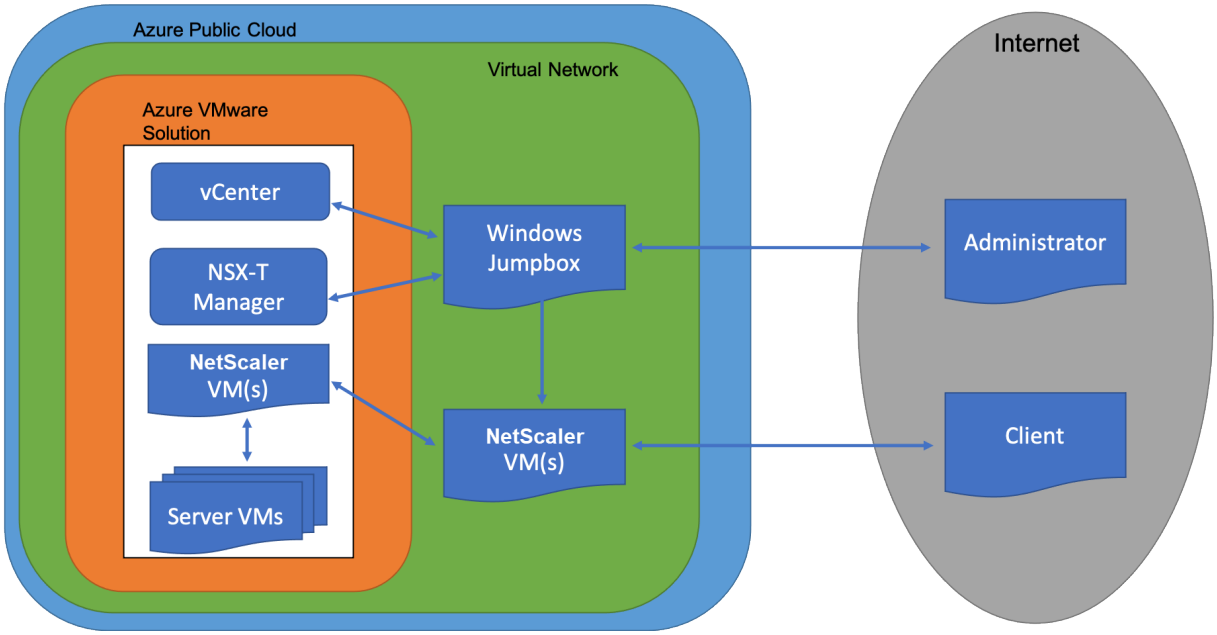
October 17, 2024

La solution Azure VMware (AVS) vous fournit des clouds privés contenant des clusters vSphere, construits à partir d'une infrastructure Azure dédiée. Le déploiement initial minimum est de trois hôtes, mais des hôtes supplémentaires peuvent être ajoutés un à la fois, jusqu'à 16 hôtes maximum par cluster. Tous les clouds privés provisionnés sont dotés de vCenter Server, vSAN, vSphere et NSX-T.

VMware Cloud (VMC) on Azure vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur Azure avec le nombre d'hôtes ESX que vous souhaitez. La VMC sur Azure prend en charge les déploiements NetScaler VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Le diagramme suivant montre la solution Azure VMware sur le cloud public Azure à laquelle un administrateur ou un client peut accéder via Internet. Un administrateur peut créer, gérer et configurer des machines virtuelles de charge de travail ou de serveur à l'aide de la solution Azure VMware. L'administrateur peut accéder au vCenter Web et au gestionnaire NSX-T de l'AVS à partir d'une boîte de dialogue Windows. Vous pouvez créer les instances NetScaler VPX (paire autonome ou haute disponibilité) et les machines virtuelles de serveur au sein de la solution Azure VMware à l'aide de vCenter, et gérer le réseau correspondant à l'aide de NSX-T manager. L'instance NetScaler VPX sur AVS fonctionne de la même manière que le cluster d'hôtes VMware sur site. AVS est géré à partir d'une Jumpbox Windows créée sur le même réseau virtuel.

Un client ne peut accéder au service AVS qu'en se connectant au VIP d'ADC. Une autre instance NetScaler VPX en dehors de la solution Azure VMware mais située dans le même réseau virtuel Azure permet d'ajouter le VIP de l'instance NetScaler VPX dans la solution Azure VMware en tant que service. Selon vos besoins, vous pouvez configurer l'instance NetScaler VPX pour fournir un service via Internet.



Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, consultez Access an Azure VMware Solution Private Cloud.
- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Azure VMware Solution.
- Obtenir des fichiers de licence VPX.
- Les machines virtuelles (VM) créées ou migrées vers le cloud privé Azure VMware Solution doivent être attachées à un segment réseau.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> **Remarque :**
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration système requise pour l'installation de l'outil OVF.

Tableau 2. Configuration système requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

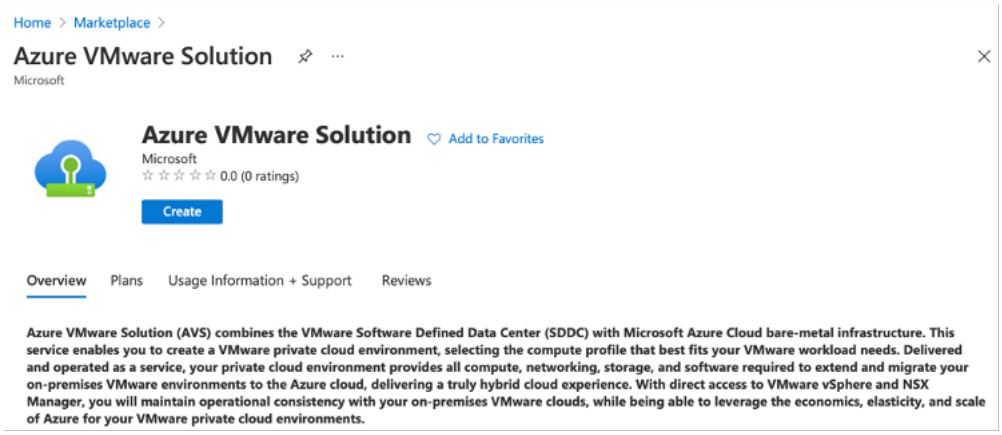
Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-79.64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-79.64.mf)

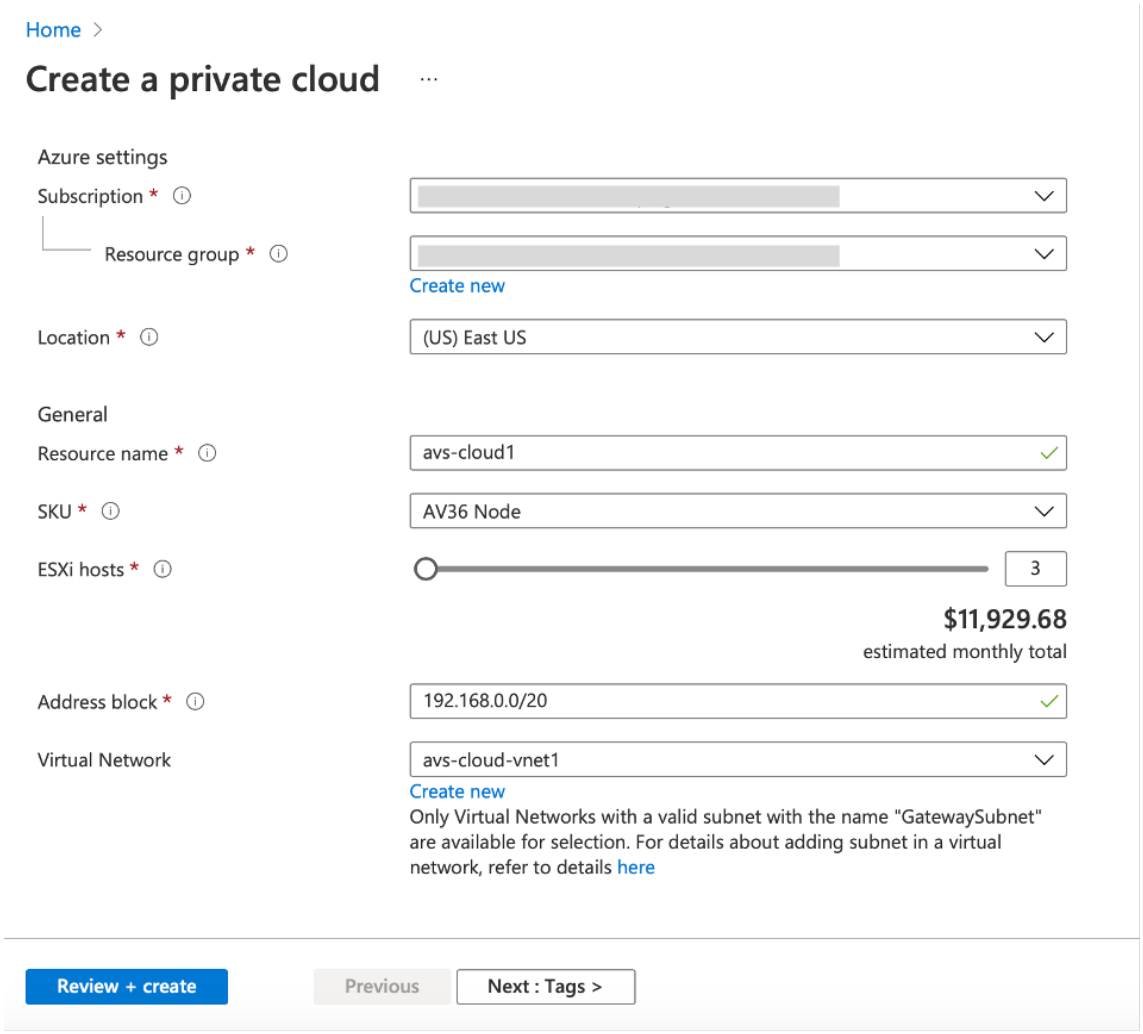
Déploiement de la solution Azure VMware

1. Connectez-vous à votre portail Microsoft Azureet accédez à **Azure Marketplace**.
2. Depuis **Azure Marketplace**, recherchez la **solution Azure VMware** et cliquez sur **Créer**.

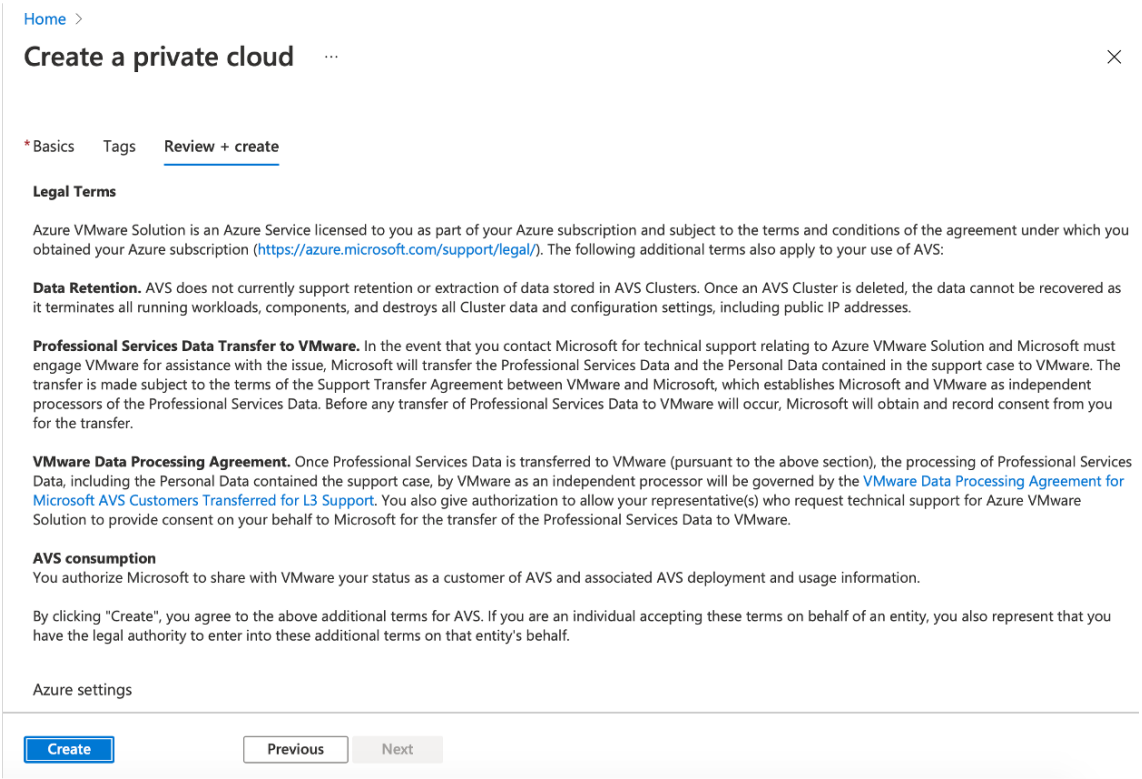


3. Sur la page **Créer un cloud privé**, entrez les informations suivantes :
    - Sélectionnez au moins 3 hôtes ESXi pour créer le cluster par défaut de votre cloud privé.
    - Pour le champ **Bloc d'adresse**, utilisez l'espace d'adressage **/22** .
    - Pour le **réseau virtuel**, assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux locaux ou autres sous-réseaux Azure (réseaux virtuels) ou avec le sous-réseau de passerelle.

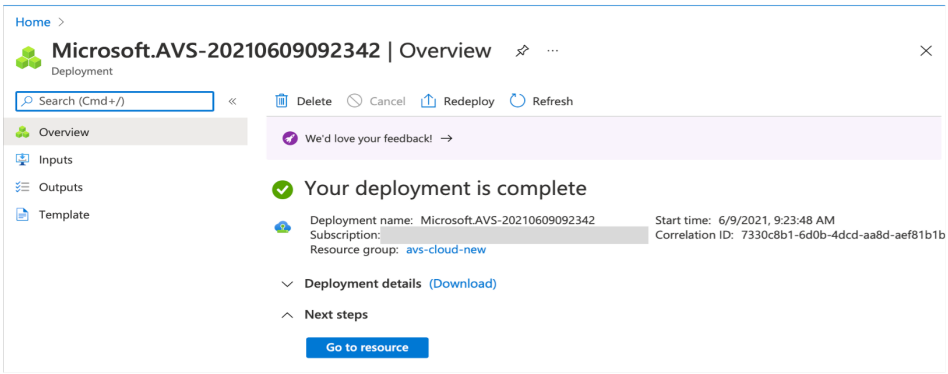
- Le sous-réseau Gateway est utilisé pour exprimer le routage de la connexion avec le cloud privé.



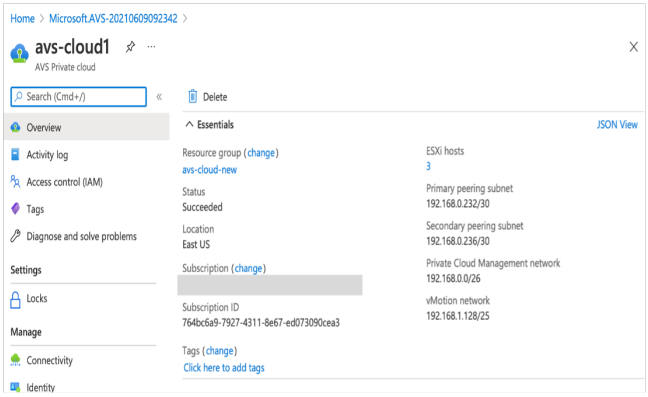
4. Cliquez sur **Réviser + Créer**.
5. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.



6. Cliquez sur **Créer**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.



7. Cliquez sur **Aller à la ressource**pour vérifier le cloud privé créé.



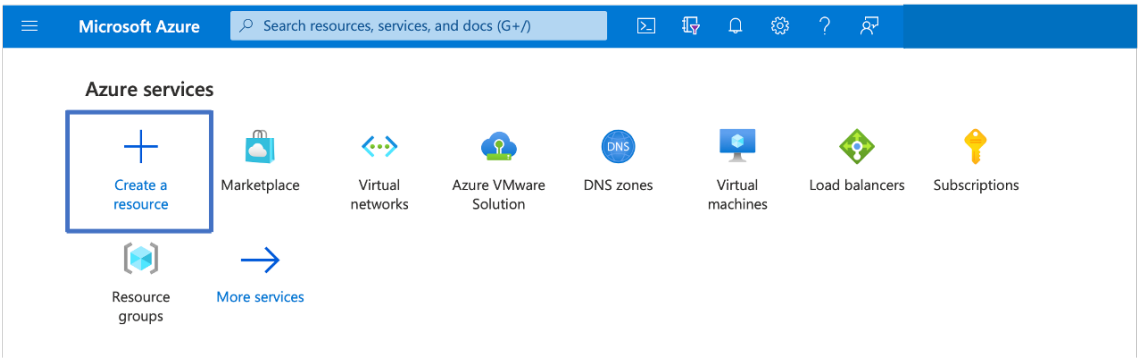
> **Remarque :**
>
> Pour accéder à cette ressource, vous devez disposer d'une machine virtuelle sous Windows qui agit comme une boîte de dialogue Jump.

Connexion à une machine virtuelle Azure exécutant Windows

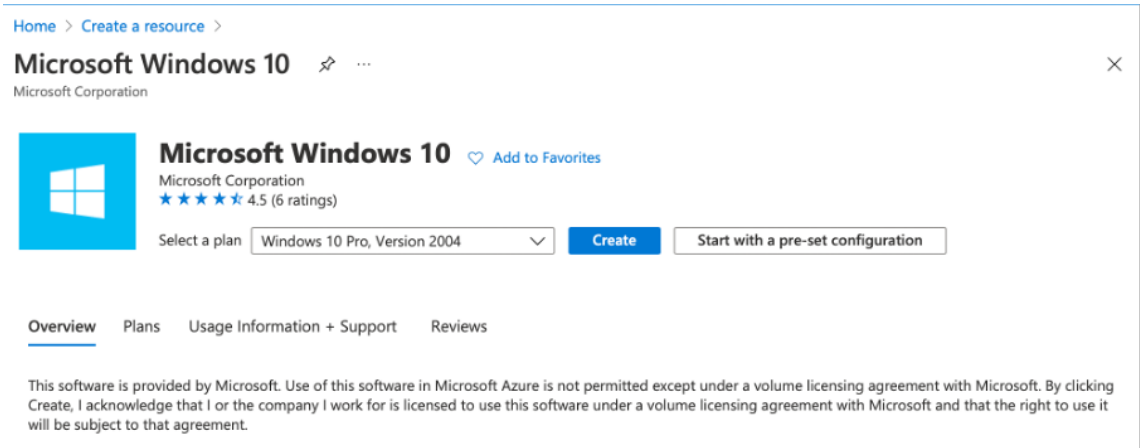
Cette procédure explique comment utiliser le portail Azure pour déployer une machine virtuelle (VM) dans Azure qui exécute Windows Server 2019. Pour voir votre machine virtuelle en action, vous devez ensuite effectuer un RDP sur la machine virtuelle et installer le serveur Web IIS.

Pour accéder au cloud privé que vous avez créé, vous devez créer un Jump Box Windows au sein du même réseau virtuel.

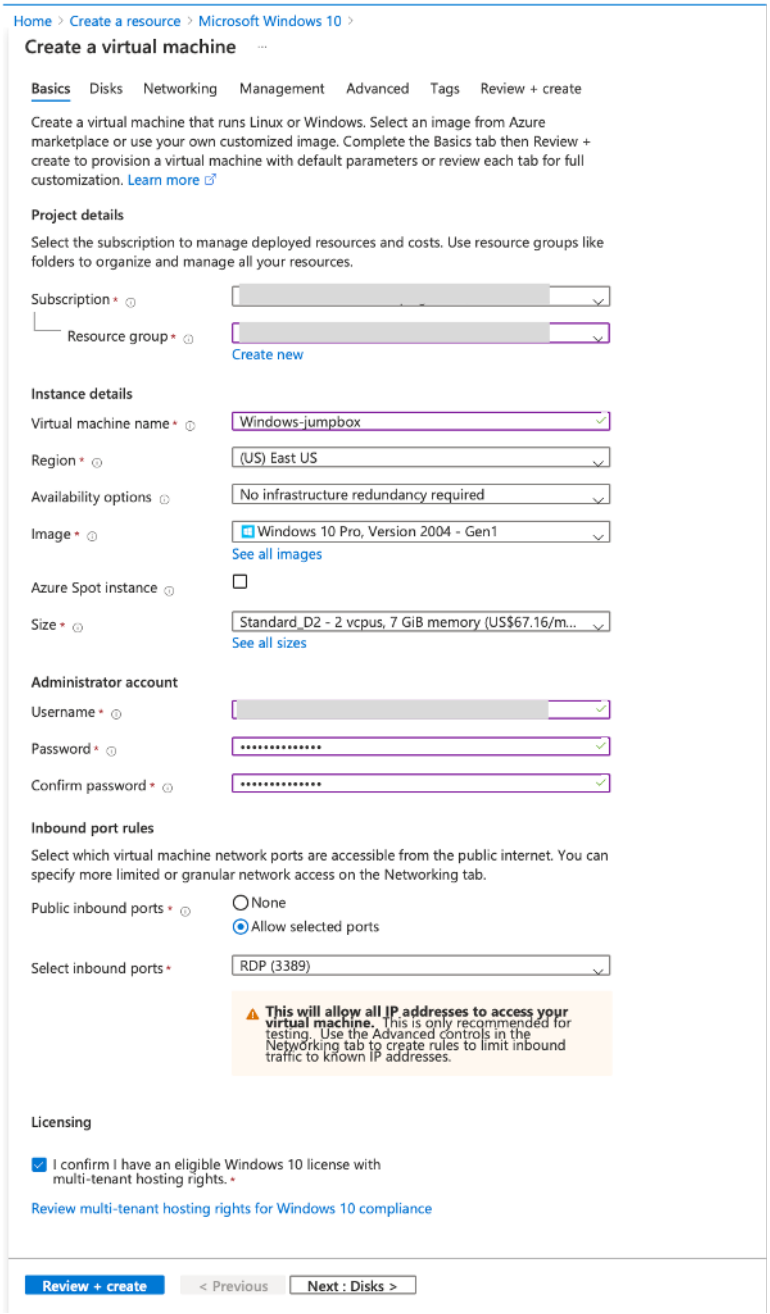
1. Accédez au **portail Azure**, puis cliquez sur **Créer une ressource**.



2. Recherchez **Microsoft Windows 10**, puis cliquez sur **Créer**.



3. Créez une machine virtuelle (VM) qui exécute Windows Server 2019. La page **Créer une machine virtuelle** apparaît. Saisissez tous les détails dans l'onglet **Principes** de base, puis cochez la case **Licences** . Laissez les valeurs par défaut restantes, puis cliquez **sur le bouton Réviser + créer** au bas de la page.



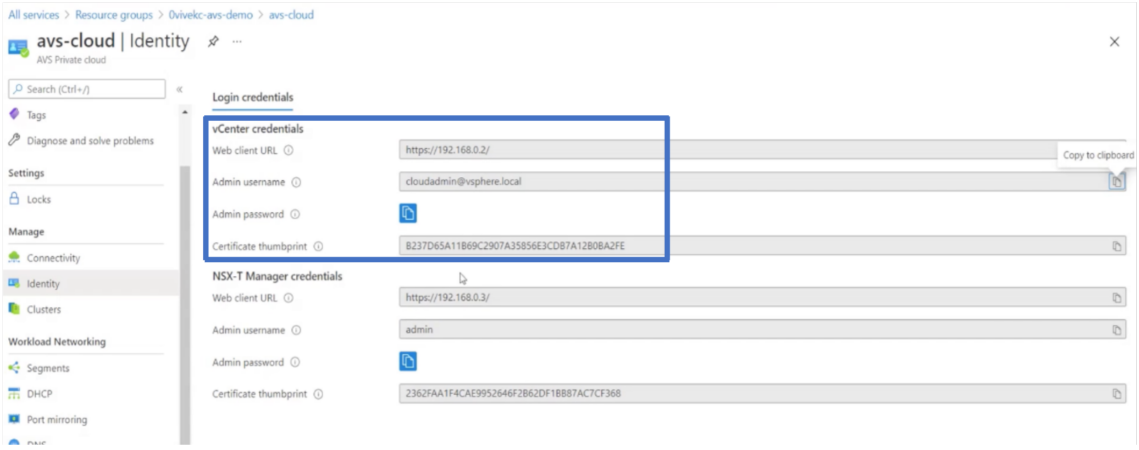
4. Une fois la validation exécutée, cliquez sur le bouton **Créer** en bas de la page.
5. Une fois le déploiement terminé, sélectionnez **Aller à la ressource**.
6. Accédez à la machine virtuelle Windows que vous avez créée. Utilisez l'adresse IP publique de la machine virtuelle Windows et connectez-vous à l'aide de RDP.

   Utilisez le bouton **Connexion** du portail Azure pour démarrer une session Bureau à distance (RDP) à partir d'un poste de travail Windows. Vous vous connectez d'abord à la machine virtuelle, puis vous vous connectez.

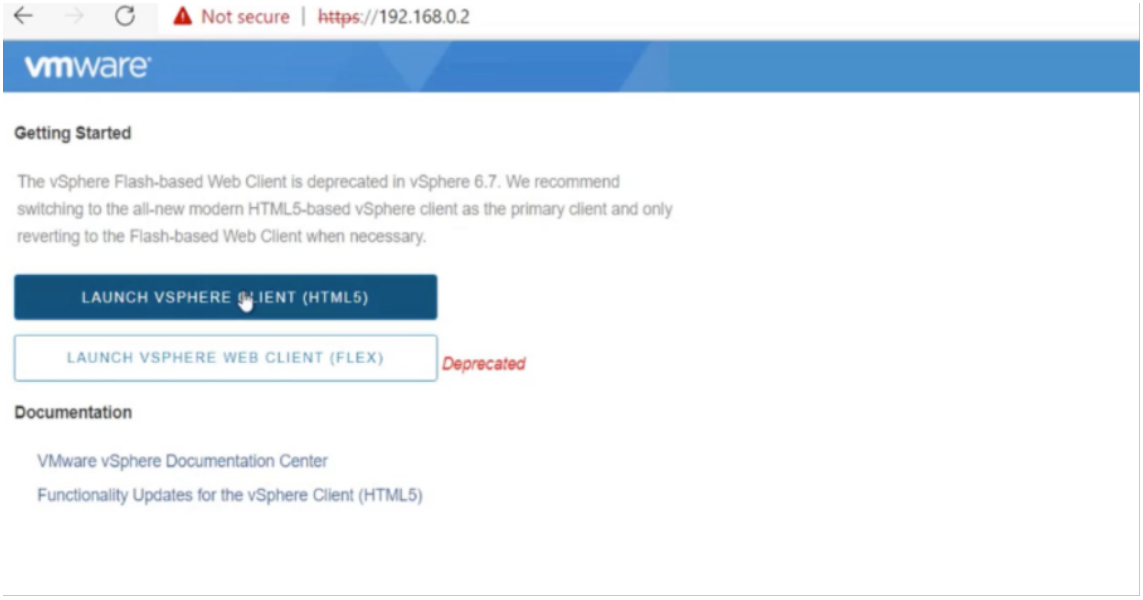
Pour vous connecter à une machine virtuelle Windows à partir d'un Mac, vous devez installer un client RDP pour Mac tel que Microsoft Remote Desktop. Pour plus d'informations, voir Comment se connecter et se connecter à une machine virtuelle Azure exécutant Windows.

Accédez à votre portail Private Cloud vCenter

1. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification de vCenter.

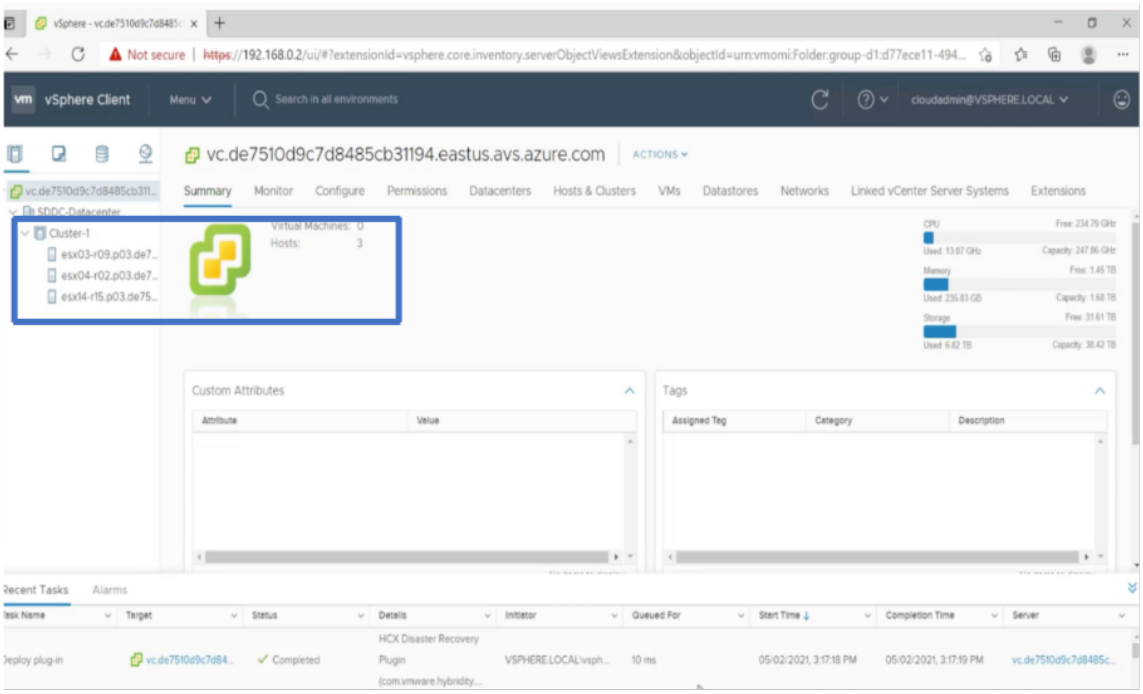


2. Lancez vSphere client en saisissant l'URL du client Web vCenter.



3. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter de votre cloud privé Azure VMware Solution.

4. Dans vSphere Client, vous pouvez vérifier les hôtes ESXi que vous avez créés dans le portail Azure.



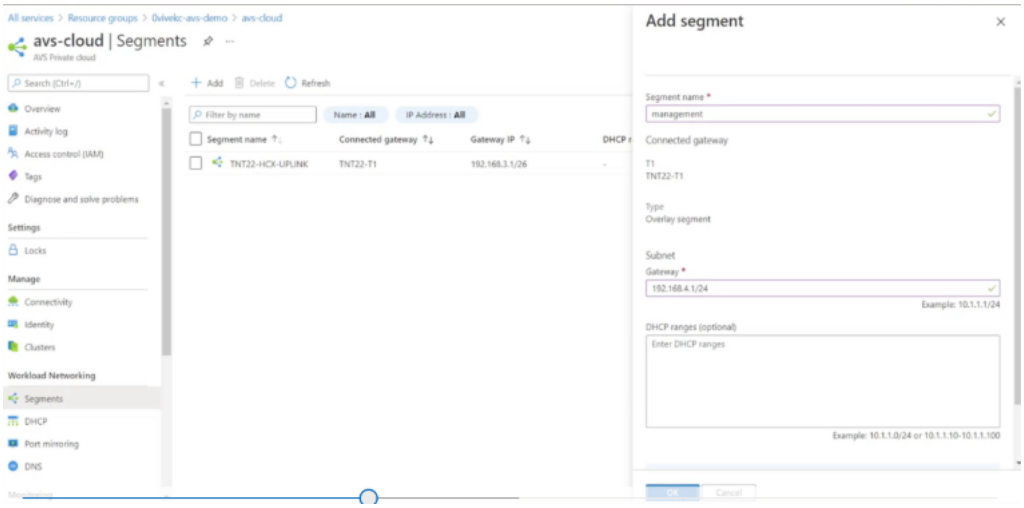
Pour plus d'informations, voir Accès à votre portail Private Cloud vCenter.

Création d'un segment NSX-T dans le portail Azure

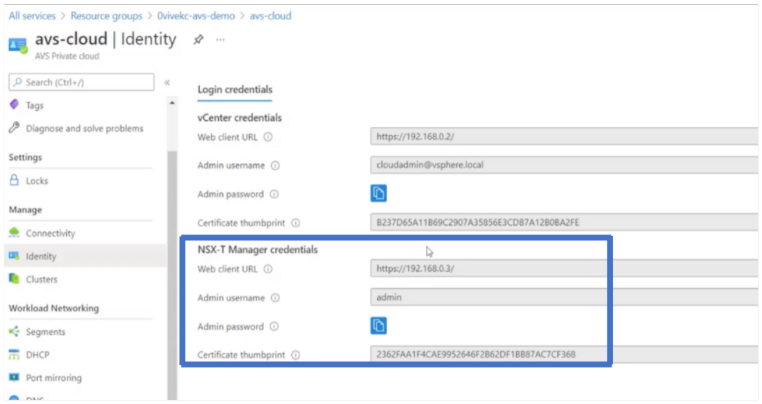
Vous pouvez créer et configurer un segment NSX-T à partir de la console Azure VMware Solution dans le portail Azure. Ces segments sont connectés à la passerelle de niveau 1 par défaut, et les charges

de travail de ces segments sont connectées Est-Ouest et Nord-Sud. Une fois que vous avez créé le segment, il s'affiche dans NSX-T Manager et vCenter.

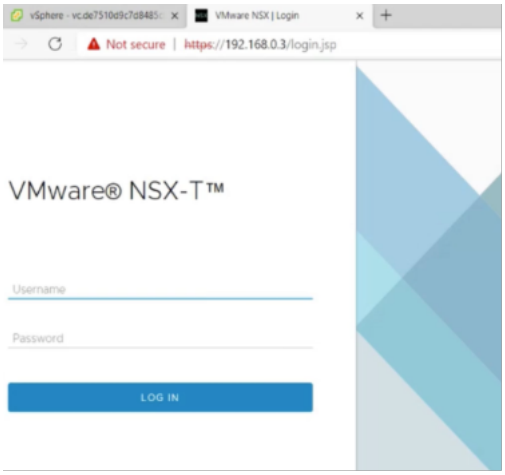
1. Dans votre cloud privé Azure VMware Solution, sous **Workload Networking**, sélectionnez **Segments > Ajouter**. Fournissez les détails du nouveau segment logique et sélectionnez **OK**. Vous pouvez créer trois segments distincts pour les interfaces Client, Management et Server.



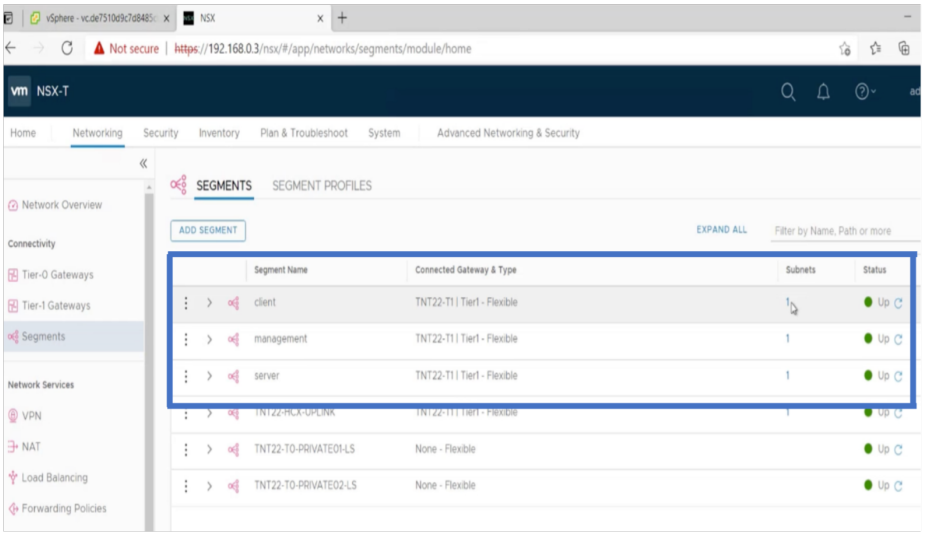
2. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification NSX-T Manager.



3. Lancez VMware NSX-T Manager en saisissant l'URL du client Web NSX-T.



4. Dans le gestionnaire NSX-T, sous **Mise en réseau > Segments**, vous pouvez voir tous les segments que vous avez créés. Vous pouvez également vérifier les sous-réseaux.



Pour plus d'informations, voir Créer un segment NSX-T dans le portail Azure.

Installation d'une instance NetScaler VPX sur le cloud VMware

Après avoir installé et configuré VMware Software-Defined Data Center (SDDC), vous pouvez utiliser le SDDC pour installer des appliances virtuelles sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

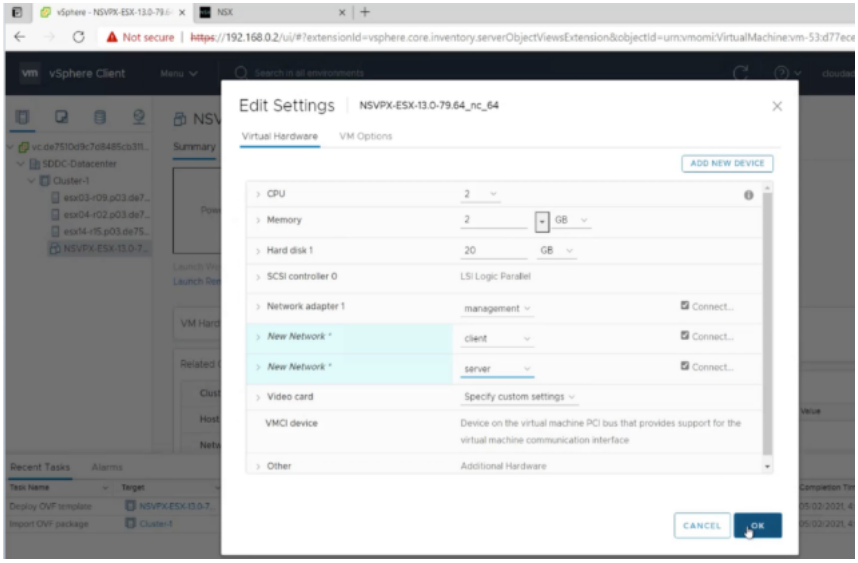
Pour installer des instances NetScaler VPX sur le cloud VMware, effectuez ces étapes dans la machine virtuelle Windows Jumpbox :

1. Téléchargez les fichiers de configuration de l'instance NetScaler VPX pour l'hôte ESXi depuis le site de téléchargement de NetScaler.

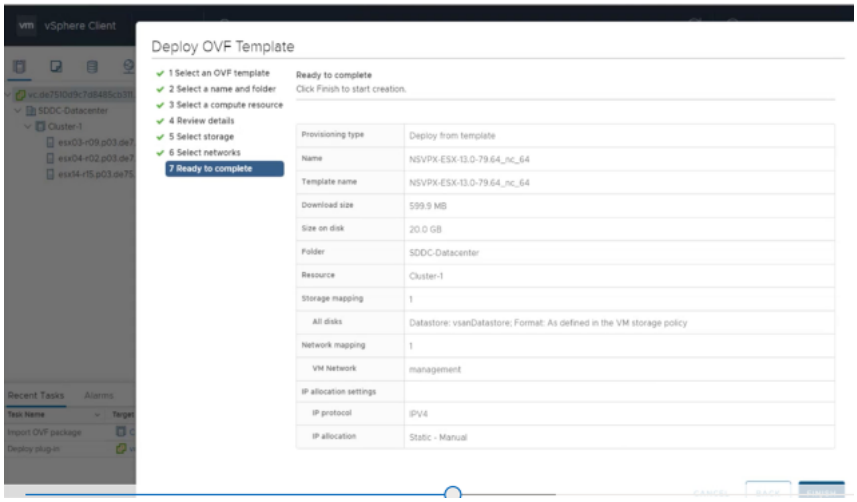
2. Ouvrez le SDDC VMware dans la Jumpbox Windows.
3. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. Dans la boîte de dialogue **Déployer un modèle OVF**, dans le champ **Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers d'installation de l'instance NetScaler VPX, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.

   > **Remarque :**
   >
   > Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000. La disponibilité de l'interface VMXNET3 est limitée par l'infrastructure Azure et peut ne pas être disponible dans Azure VMware Solution.

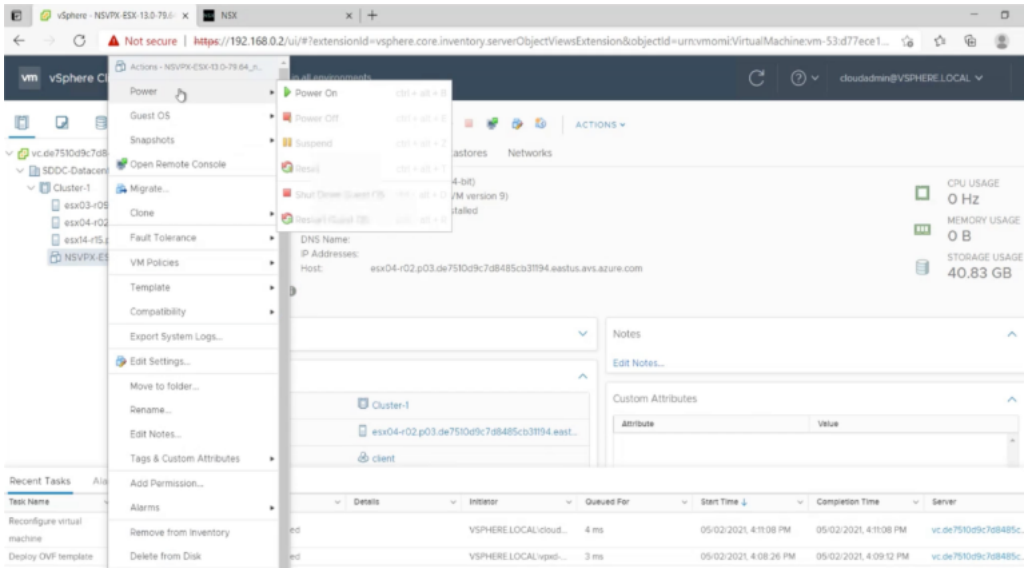
6. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **OK**.



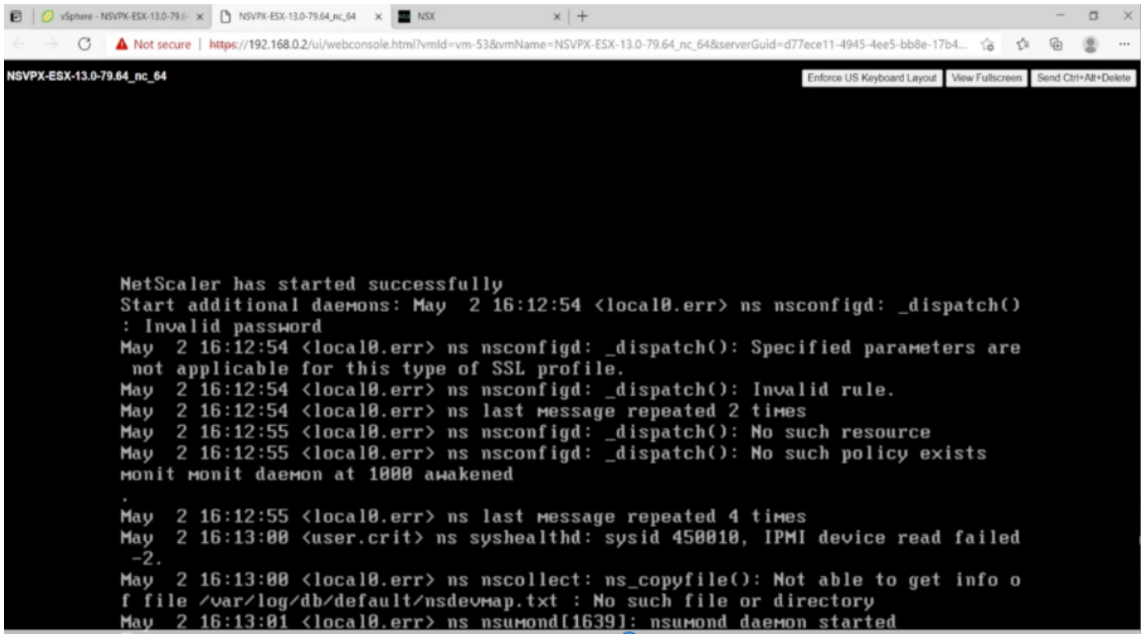
7. Cliquez sur **Terminer** pour commencer l'installation d'une appliance virtuelle sur VMware SDDC.



8. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Console** pour émuler un port de console. Cliquez sur l'onglet **Console** pour émuler un port de console.



9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.



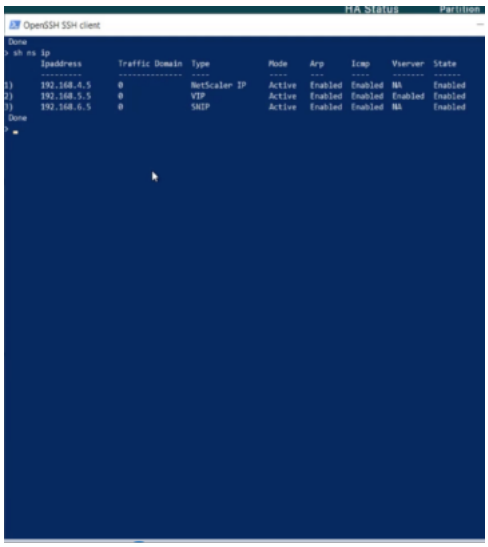
10. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l'interface de ligne de commande :

```
ssh nsroot@<management IP address>
```

Exemple

```
ssh nsroot@192.168.4.5
```

11. Vous pouvez vérifier la configuration ADC à l'aide de la `show ns ip` commande.

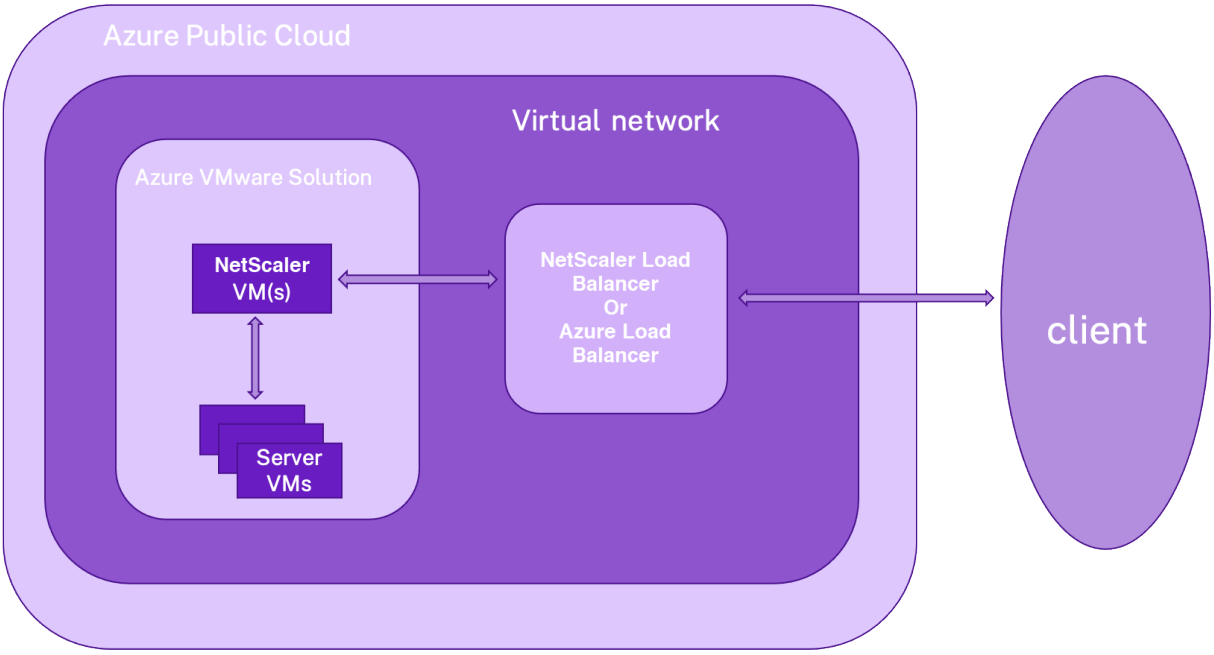


Configurer une instance autonome NetScaler VPX sur la solution Azure VMware

October 17, 2024

Vous pouvez configurer une instance autonome NetScaler VPX sur la solution Azure VMware (AVS) pour les applications connectées à Internet.

Le schéma suivant montre l'instance autonome NetScaler VPX sur la solution Azure VMware. Un client peut accéder au service AVS en se connectant à l'adresse IP virtuelle (VIP) de NetScaler au sein de l'AVS. Vous pouvez y parvenir en provisionnant un équilibreur de charge NetScaler ou l'instance d'équilibreur de charge Azure en dehors d'AVS mais dans le même réseau virtuel Azure. Configurez l'équilibreur de charge pour accéder au VIP de l'instance NetScaler VPX au sein du service AVS.



Conditions préalables

Avant de commencer à installer un dispositif virtuel, lisez les conditions préalables Azure suivantes :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, voir Accéder à un cloud privé Azure VMware Solu-

tion.

- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Azure VMware Solution.
- Pour plus d'informations sur l'installation d'une instance NetScaler VPX sur le cloud VMware, consultez Installer une instance NetScaler VPX sur le cloud VMware.

Configurer une instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge NetScaler

Suivez ces étapes pour configurer l'instance autonome NetScaler VPX sur AVS pour les applications connectées à Internet à l'aide de l'équilibreur de charge NetScaler.

1. Déployez une instance NetScaler VPX sur le cloud Azure. Pour plus d'informations, voir Configurer une instance autonome NetScaler VPX.

   > **Remarque :**
   >
   > Assurez-vous qu'il est déployé sur le même réseau virtuel que le cloud Azure VMware.

2. Configurez l'instance NetScaler VPX pour accéder à l'adresse VIP de NetScaler VPX déployé sur AVS.

   a) Ajoutez un serveur virtuel d'équilibrage de charge.

   ```
   add lb vserver <name> <serviceType> [<vip>] [<port>]
   ```

   Exemple

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   ```

   b) Ajoutez un service qui se connecte au VIP de NetScaler VPX déployé sur AVS.

   ```
   add service <name> <ip> <serviceType> <port>
   ```

   Exemple

   ```
   add service webserver1 192.168.4.10 HTTP 80
   ```

   c) Liez un service au serveur virtuel d'équilibrage de charge.

   ```
   bind lb vserver <name> <serviceName>
   ```

   Exemple

   ```
   bind lb vserver lb1 webserver1
   ```


Configurer l'instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge Azure

Suivez ces étapes pour configurer l'instance autonome NetScaler VPX sur AVS pour les applications connectées à Internet à l'aide de l'équilibreur de charge Azure.

1. Configurez une instance d'Azure Load Balancer de charge Azure sur le cloud Azure. Pour plus d'informations, consultez la documentation Azure sur la création d'un équilibreurde charge.
2. Ajoutez l'adresse VIP de l'instance NetScaler VPX déployée sur AVS au pool principal.

   La commande Azure suivante ajoute une adresse IP principale dans le pool d'adresses principal d'équilibrage de charge.

```
az network lb address-pool address add
                                    --resource-group <Azure VMC
                                       Resource Group>
                                    --lb-name <LB Name>
                                    --pool-name <Backend pool
                                       name>
                                    --vnet <Azure VMC Vnet>
                                    --name <IP Address name>
                                    --ip-address <VIP of ADC in
                                       VMC>
```

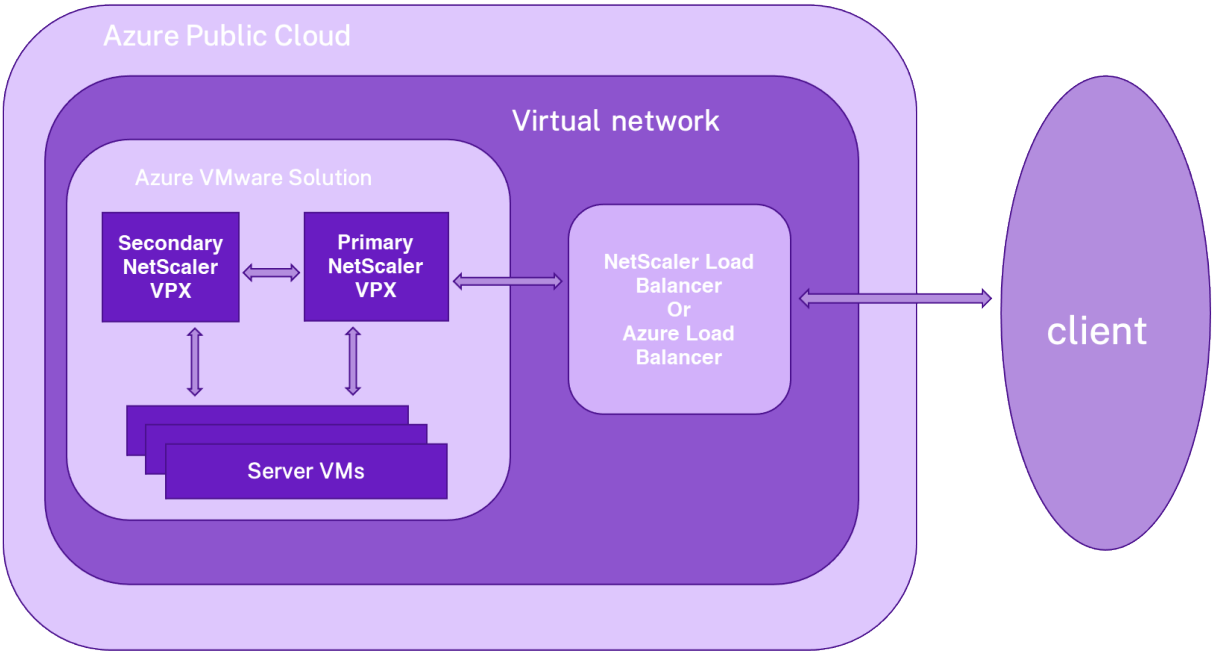
> **Remarque :**
>
> Assurez-vous que l'équilibreur de charge Azure est déployé sur le même réseau virtuel que le cloud Azure VMware.

Configurer une configuration de haute disponibilité NetScaler VPX sur la solution Azure VMware

October 17, 2024

Vous pouvez configurer une configuration NetScaler VPX HA sur la solution Azure VMware (AVS) pour les applications connectées à Internet.

Le schéma suivant montre la paire NetScaler VPX HA sur AVS. Un client peut accéder au service AVS en se connectant au VIP du nœud ADC principal à l'intérieur de l'AVS. Vous pouvez y parvenir en provisionnant un équilibreur de charge NetScaler ou l'instance d'équilibreur de charge Azure en dehors d'AVS mais dans le même réseau virtuel Azure. Configurez l'équilibreur de charge pour accéder à l'adresse IP virtuelle du nœud ADC principal dans le service AVS.



Conditions préalables

Avant de commencer à installer un dispositif virtuel, lisez les conditions préalables Azure suivantes :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, voir Accéder à un cloud privé Azure VMware Solution.
- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, consultez Ajouter un segment réseau dans la solution Azure VMware.

Étapes de configuration

Suivez ces étapes pour configurer la configuration de haute disponibilité de NetScaler VPX dans AVS pour les applications connectées à Internet.

1. Créez deux instances NetScaler VPX sur le cloud VMware. Pour plus d'informations, consultez Installer une instance NetScaler VPX sur le cloud VMware.

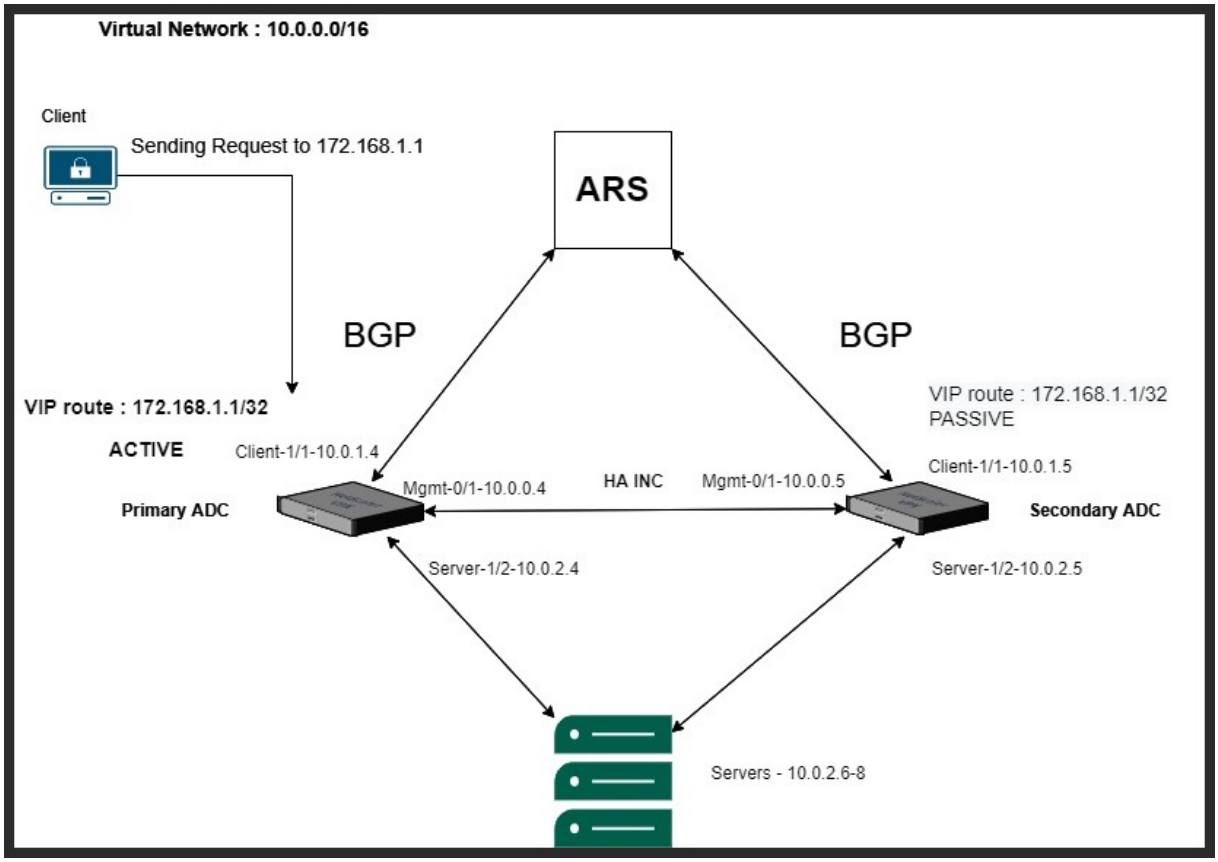
2. Configurez la configuration de NetScaler HA. Pour plus d'informations, voir Configuration de la haute disponibilité.
3. Configurez la configuration NetScaler HA pour qu'elle soit accessible aux applications connectées à Internet.
    - Pour configurer l'instance NetScaler VPX à l'aide de l'équilibreur de charge NetScaler, consultez Configurer une instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge NetScaler.
    - Pour configurer l'instance NetScaler VPX à l'aide de l'équilibreur de charge Azure, consultez Configurer l'instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge Azure.

Configurer le serveur de routage Azure avec la paire NetScaler VPX HA

October 17, 2024

Vous pouvez configurer le serveur de route Azure avec l'instance NetScaler VPX pour échanger les itinéraires VIP configurés avec le réseau virtuel à l'aide du protocole BGP. Le NetScaler peut être déployé en mode autonome ou en mode HA-INC, puis configuré avec BGP. Ce déploiement ne nécessite pas d'équilibreur de charge Azure (ALB) devant la paire ADC HA.

Le diagramme suivant montre comment une topologie VPX HA est intégrée au serveur de routage Azure. Chacune des instances ADC possède 3 interfaces : une pour la gestion, une pour le trafic client et une pour le trafic serveur.



Le diagramme topologique utilise les adresses IP suivantes.

Exemple de configuration IP pour l'instance ADC principale :

```
NSIP: 10.0.0.4/24
SNIP on 1/1: 10.0.1.4/24
SNIP on 1/2: 10.0.2.4/24
VIP: 172.168.1.1/32
```

Exemple de configuration IP pour l'instance ADC secondaire :

```
NSIP: 10.0.0.5/24
SNIP on 1/1: 10.0.1.5/24
SNIP on 1/2: 10.0.2.5/24
VIP: 172.168.1.1/32
```

Conditions préalables

Vous devez connaître les informations suivantes avant de déployer une instance NetScaler VPX sur Azure.

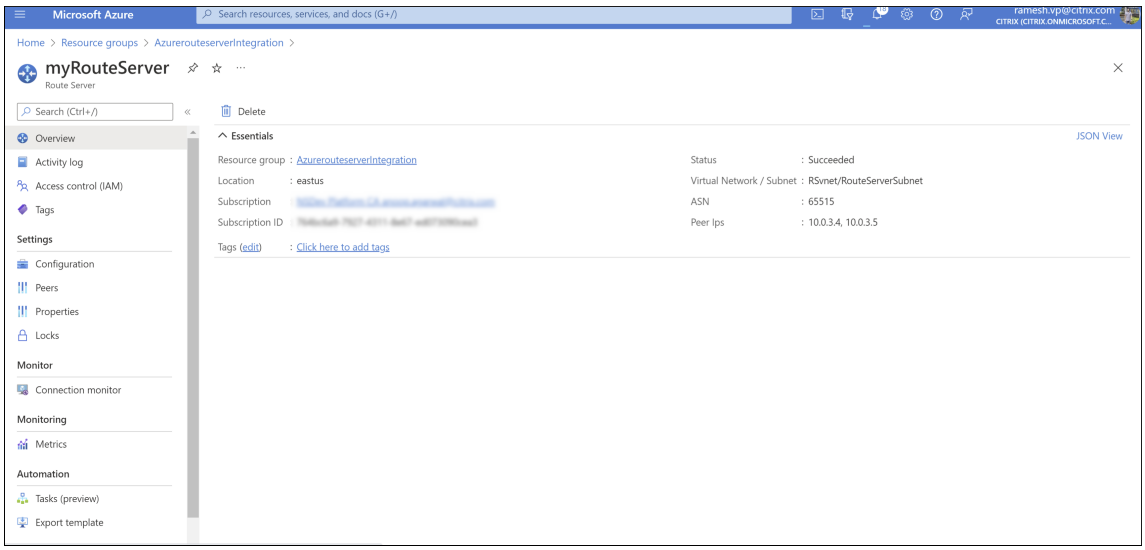
- Terminologie Azure et détails réseau. Pour plus d'informations, consultez Terminologie Azure.

- Présentation d'Azure Route Server. Pour plus d'informations, consultez Qu'est-ce qu'Azure Route Server ?.
- Fonctionnement d'une appliance NetScaler. Pour plus d'informations, consultez la documentation de NetScaler.
- Réseau NetScaler. Pour plus d'informations, consultez la section Réseau ADC.

Comment configurer un serveur de routage Azure avec la paire NetScaler VPX HA

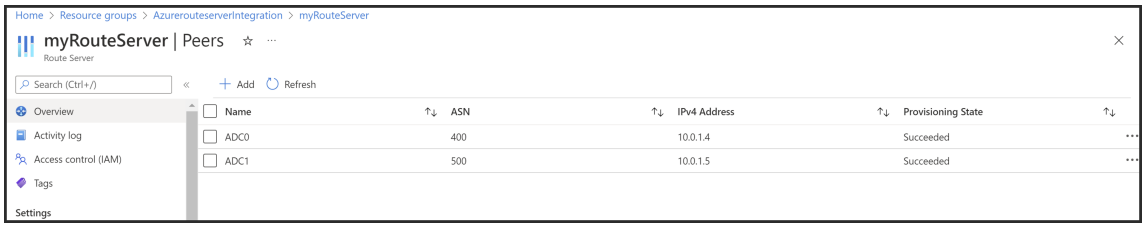
1. Créez un serveur de routage sur le portail Azure. Pour plus d'informations, consultez Créer et configurer un serveur de routage à l'aide du portail Azure.

   Dans l'exemple suivant, le sous-réseau 10.0.3.0/24 est utilisé pour déployer le serveur Azure. Une fois le serveur de routage créé, récupérez les adresses IP du serveur de routage, par exemple : 10.0.3.4, 10.0.3.5.



2. Configurez l'appairage avec l'appliance virtuelle réseau (NVA) dans le portail Azure. Ajoutez votre instance NetScaler VPX en tant que NVA. Pour plus d'informations, consultez la section Configuration de l'appairage avec NVA.

   Dans l'exemple suivant, le SNIP ADC sur les interfaces 1/1 : 10.0.1.4 et 10.0.1.5, et l'ASN : 400 et 500, sont utilisés lors de l'ajout de l'homologue.



3. Ajoutez deux instances NetScaler VPX pour la configuration HA.

Effectuez les étapes suivantes :

a) Déployez deux instances VPX (instances principales et secondaires) sur Azure.
b) Ajoutez une carte réseau client et serveur sur les deux instances.
c) Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler.

4. Configurez le routage dynamique dans l'instance ADC principale.

   Exemple de configuration :

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -
   dynamicRouting ENABLED
VTYSH
configure terminal
router BGP 400
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
```

5. Configurez le routage dynamique dans l'instance ADC secondaire.

   Exemple de configuration :

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -
   dynamicRouting ENABLED
VTYSH
configure terminal
router BGP 500
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
```

6. Vérifiez les homologues BGP établis à l'aide des commandes BGP dans l'interface shell VTY. Pour

plus d'informations, consultez la section Vérification de la configuration BGP.

```
show ip bgp neighbors
```

7. Configurez le serveur virtuel LB dans l'instance ADC principale.

   Exemple de configuration :

```
add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute
   ENABLED
add lbvserver v1 HTTP 172.16.1.1 80
add service s1 10.0.2.6 HTTP 80
bind lbvserver v1 s1
enable ns feature lb
```

   Un client du même réseau virtuel que celui de l'instance NetScaler VPX peut désormais accéder au serveur virtuel LB. Dans ce cas, l'instance NetScaler VPX annonce l'itinéraire VIP vers le serveur de routage Azure.

Ajouter le service principal Azure Autoscaling

October 17, 2024

L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources du réseau. Que la demande diminue, vous devez réduire la demande afin d'éviter le coût inutile des ressources inutilisées. Pour minimiser le coût d'exécution de l'application, vous devez surveiller en permanence le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement applicatif puisse évoluer à la hausse ou à la baisse de manière dynamique, vous devez automatiser les processus de surveillance du trafic et d'augmentation et de diminution des ressources chaque fois que cela est nécessaire.

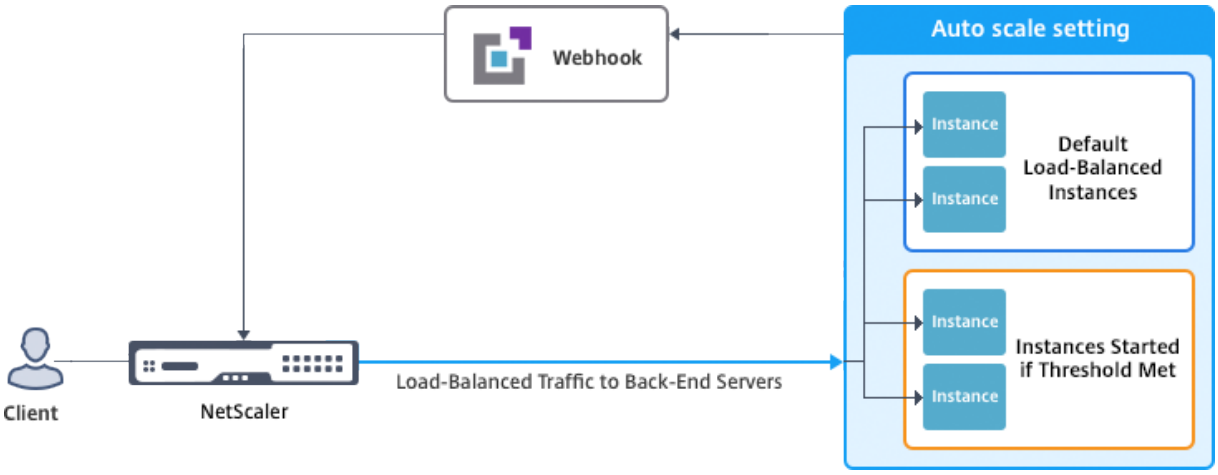
Vous pouvez utiliser Autoscale avec des jeux d'échelle de machines virtuelles Azure (VMSS) pour le déploiement autonome et haute disponibilité VPX Multi-IP sur Azure.

Intégrée aux fonctionnalités Azure VMSS et Autoscale, l'instance NetScaler VPX offre les avantages suivants :

- Équilibre de charge et gestion : configure automatiquement les serveurs pour les faire évoluer à la hausse ou à la baisse, en fonction de la demande. L'instance NetScaler VPX détecte automatiquement le paramètre VMSS Autoscale dans le même réseau virtuel que celui où l'instance VPX est déployée, ou dans les réseaux virtuels homologues qui font partie du même abonnement Azure. Vous pouvez sélectionner le paramètre VMSS Autoscale pour équilibrer la charge. Cela

se fait en configurant automatiquement l'adresse IP virtuelle NetScaler et l'adresse IP du sous-réseau sur l'instance VPX.

- Haute disponibilité : détecte les groupes Autoscale et équilibre la charge des serveurs.
- Meilleure disponibilité du réseau : l'instance VPX prend en charge les serveurs back-end sur différents réseaux virtuels (VNET).



Pour plus d'informations, consultez la rubrique Azure suivante

- Documentation sur les jeux d'échelle de machine virtuelle
- Présentation d'Autoscale dans les machines virtuelles Microsoft Azure, les services cloud et les applications Web

Avant de commencer

- Lisez les instructions d'utilisation relatives à Azure. Pour plus d'informations, consultez Déployer une instance NetScaler VPX sur Microsoft Azure.
- Créez une ou plusieurs instances NetScaler VPX avec trois interfaces réseau sur Azure en fonction de vos besoins (déploiement autonome ou haute disponibilité).
- Ouvrez le port TCP 9001 sur le groupe de sécurité réseau de l'interface 0/1 de l'instance VPX. L'instance VPX utilise ce port pour recevoir la notification de scale-out et de scale-in.
- Créez un Azure VMSS dans le même réseau virtuel que celui où l'instance NetScaler VPX est déployée. Si les instances VMSS et NetScaler VPX sont déployées dans différents réseaux virtuels Azure, les conditions suivantes doivent être remplies :
  - Les deux réseaux virtuels doivent appartenir au même abonnement Azure.
  - Les deux réseaux virtuels doivent être connectés à l'aide de la fonctionnalité d'appairage de réseaux virtuels d'Azure.

  Si vous n'avez pas de configuration VMSS existante, effectuez les tâches suivantes :

a) Créer un VMSS

b) Activer Autoscale sur VMSS

c) Créez des stratégies de scale-in et de scale-out dans le paramètre VMSS Autoscale

Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.

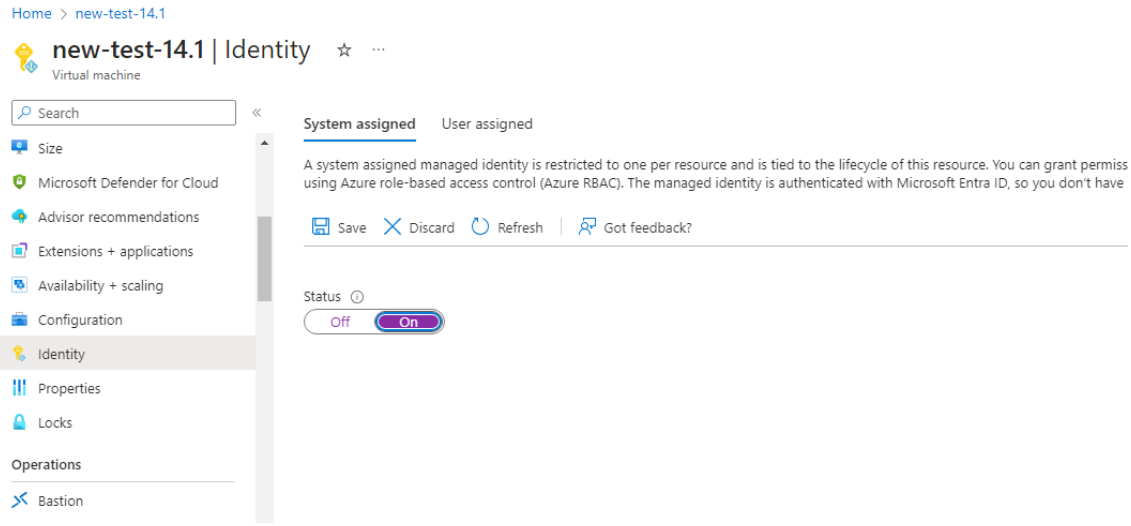
- NetScaler VPX prend en charge les VMSS avec orchestration uniforme uniquement. Les systèmes VMSS avec orchestration flexible ne sont pas pris en charge. Pour plus d'informations, consultez Modes d'orchestration pour les Virtual Machine Scale Sets dans Azure.
- À partir de la version 14.1-12.x de NetScaler, NetScaler VPX prend en charge les identités gérées dans le cloud Azure. Les identités gérées relient un principal de service à une ressource Azure telle qu'une machine virtuelle. Avec l'identité gérée, vous n'avez pas besoin de gérer les informations d'identification du cloud (ID de l'application, secret de l'application et ID du locataire), évitant ainsi les risques de sécurité. Actuellement, NetScaler VPX ne prend en charge que l'identité gérée attribuée au système et une identité gérée attribuée à un seul utilisateur. L'identité gérée attribuée à plusieurs utilisateurs n'est pas prise en charge.

  Pour les versions de NetScaler antérieures aux versions 14.1-12.x, vous devez gérer manuellement les informations d'identification cloud dans NetScaler VPX via Azure Active Directory (AAD). Attribuez un rôle de contributeur à la nouvelle application AAD. Les informations d'identification du cloud doivent être recréées périodiquement après leur expiration. Pour plus d'informations, voir Création d'une application Azure Active Directory et d'un principal de service.

  Lorsque vous configurez une identité gérée sur la console Azure et des informations d'identification cloud dans NetScaler, l'identité gérée a priorité sur les informations d'identification cloud.

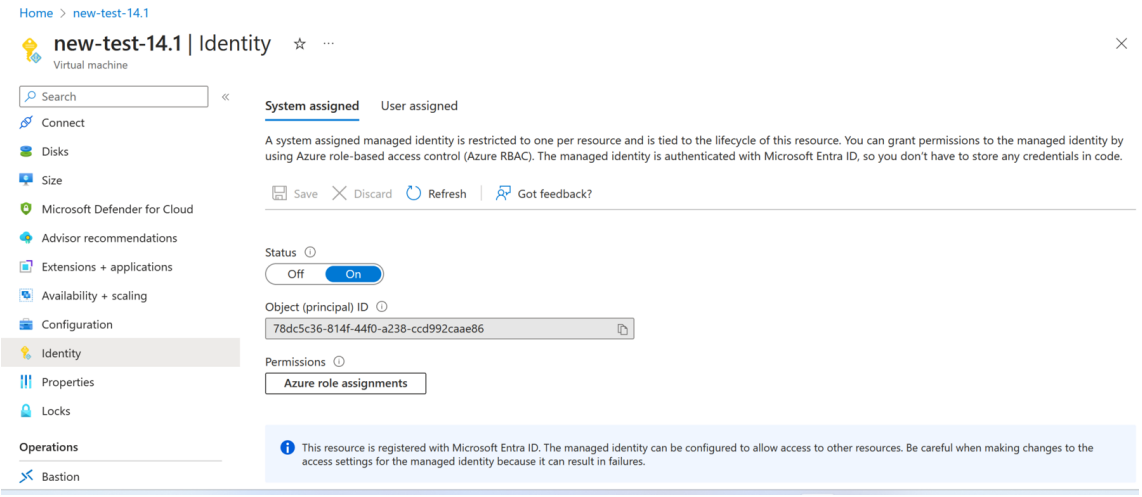
Configuration d'une identité gérée sur une machine virtuelle

1. Connectez-vous au portail Azure.
2. Accédez à votre machine virtuelle et sélectionnez **Identity**.
3. Choisissez soit **le système attribué**, soit **l'utilisateur affecté** en fonction de vos besoins.
4. Sous **État**, sélectionnez **Activé**, puis cliquez sur **Enregistrer**.



Une fois le statut enregistré, vous voyez qu'un objet principal de service est créé et attribué à la machine virtuelle.

5. Cliquez sur **Azure role assignment**.



6. Dans la fenêtre **Ajouter une attribution de rôle**, sélectionnez une étendue. Vous pouvez choisir parmi les options suivantes :

   - Abonnement

     Si le VMSS et la machine virtuelle appartiennent à des groupes de ressources différents, utilisez **Subscription** comme étendue.

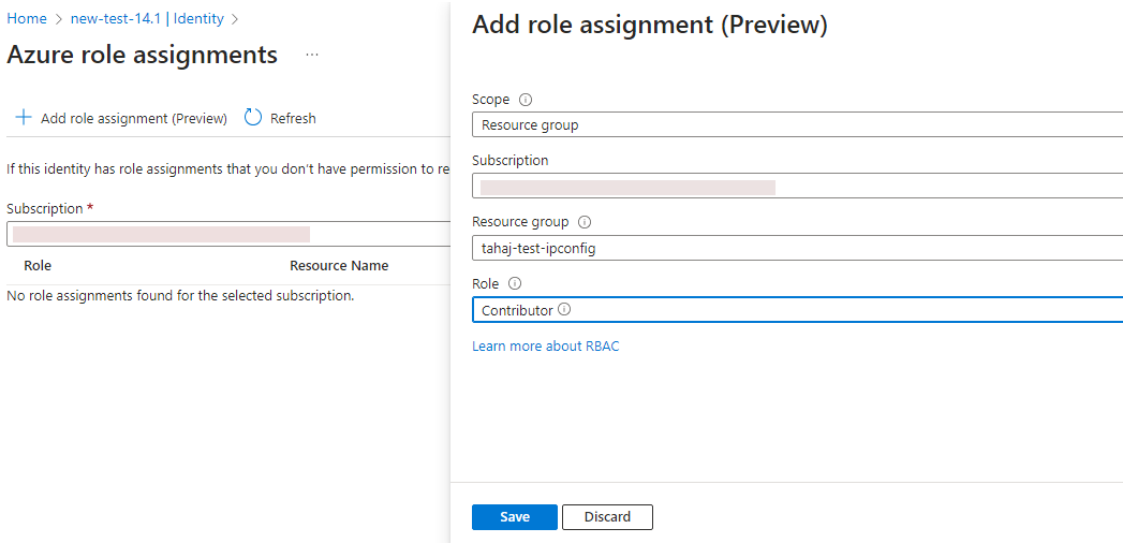
   - Groupe de ressources

     Si le VMSS se trouve dans le même groupe de ressources que votre machine virtuelle, utilisez le **groupe de ressources** comme étendue.

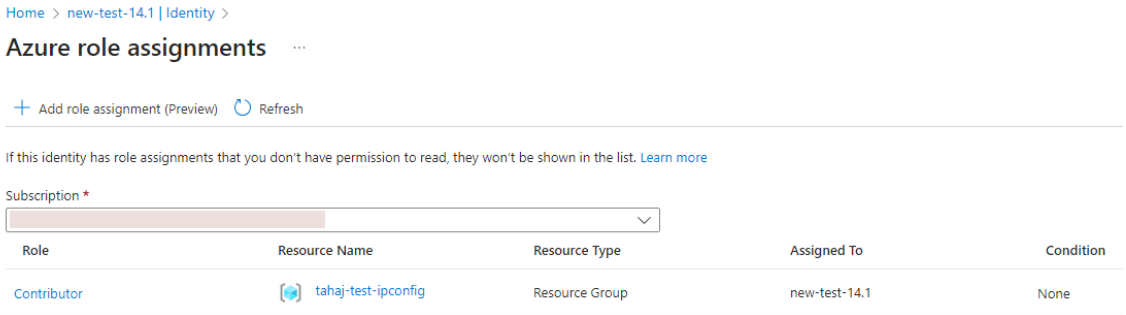
   - Clés Vault

- Stockage
- SQL

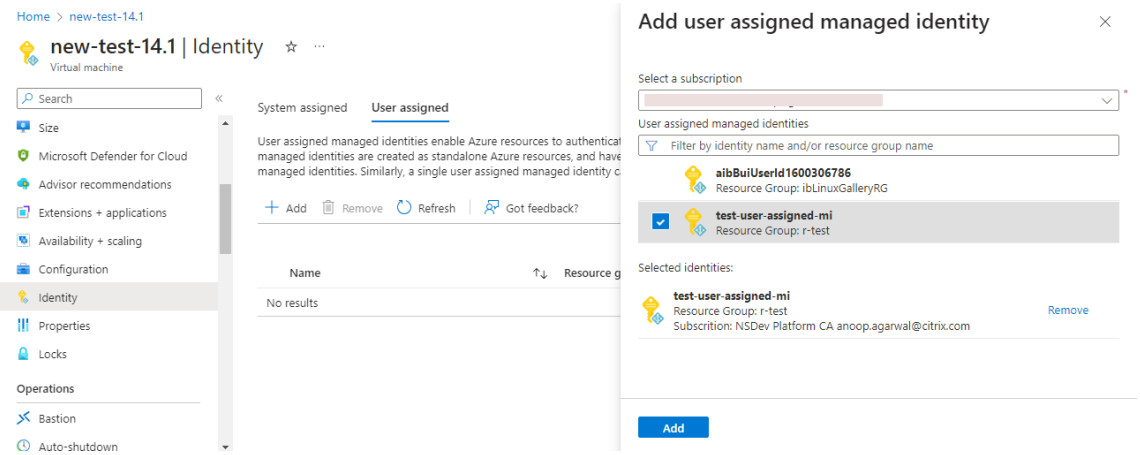
En fonction de l'étendue que vous avez sélectionnée, renseignez les informations des autres champs. Attribuez un rôle de **contributeur** et **enregistrez** la configuration.



La page **Azure role** assignment affiche l'identité gérée que vous avez créée.



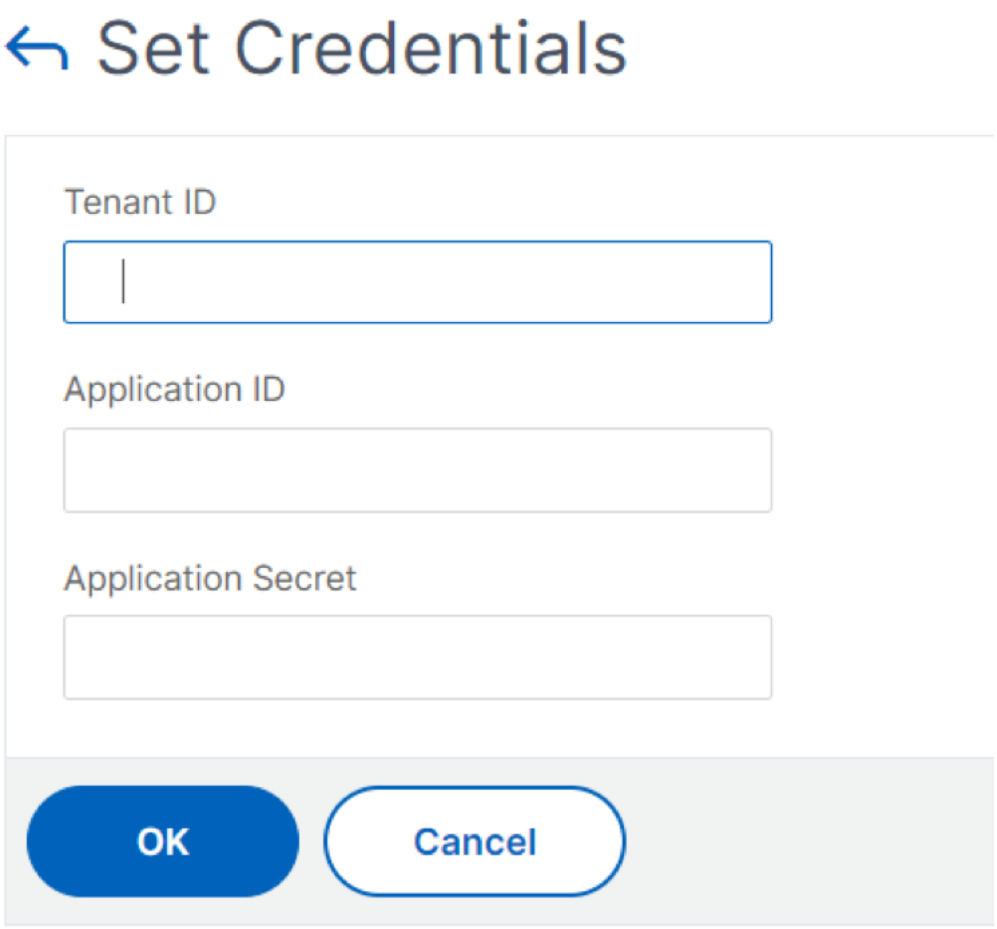
7. Pour créer une identité gérée attribuée à l'utilisateur, sélectionnez un abonnement, choisissez une identité gérée attribuée à l'utilisateur, puis cliquez sur **Ajouter**.



Ajouter VMSS à une instance NetScaler VPX

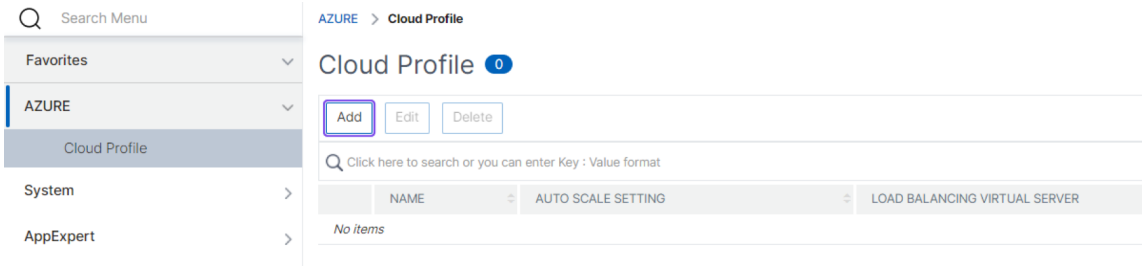
Procédez comme suit pour ajouter le paramètre Autoscale à l'instance VPX :

1. Ouvrez une session sur l'instance VPX.
2. Accédez à **Configuration > Azure > Définir les informations d'identification**. Ajoutez les informations d'identification Azure requises pour que la fonctionnalité Autoscale fonctionne.

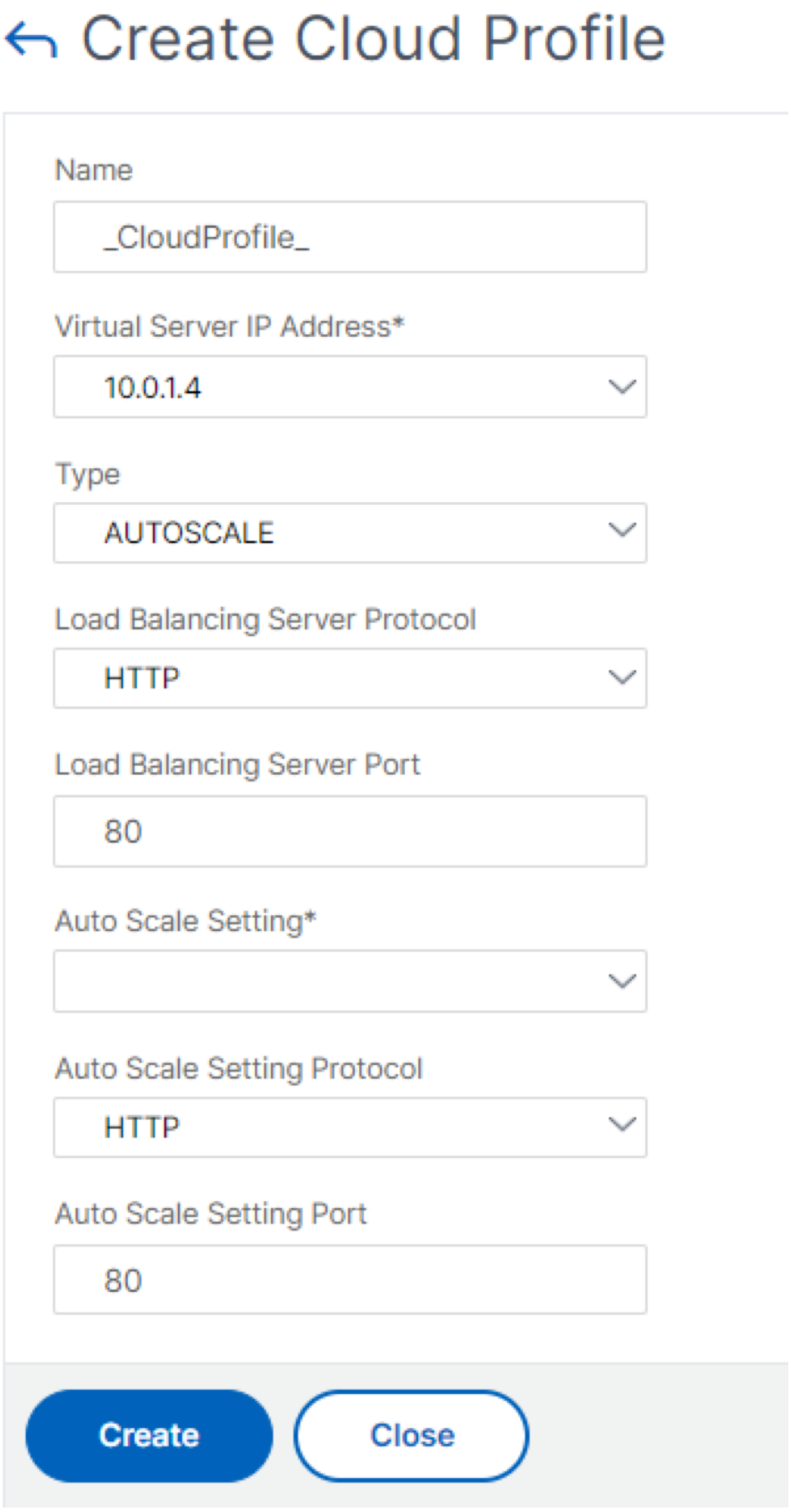


> **Remarque :**
>
> Si vous utilisez Azure Managed Identity, il n'est pas nécessaire de définir des informations d'identification.

3. Accédez à **System > Azure > Cloud Profile** et cliquez sur **Ajouter** pour créer un profil cloud.



La page de configuration de **Create Cloud Profile** s'affiche.



Le profil cloud crée un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services dont les membres (serveurs) font office de serveurs du groupe Auto Scaler. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

Points à garder à l'esprit lors de la création d'un profil cloud

- L'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
- Le paramètre autoscale est prérempli à partir de l'instance VMSS connectée à l'instance NetScaler VPX soit sur le même réseau virtuel, soit sur des réseaux virtuels homologues. Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.
- Lors de la sélection du **protocole Auto Scale Setting et duport Auto Scale Setting**, assurez-vous que vos serveurs écoutent les protocoles et les ports, et que vous associez le bon moniteur au groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour l'autoscaling de type protocole SSL, une fois que vous avez créé le profil cloud, le serveur virtuel ou le groupe de services d'équilibrage de charge est en panne en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.

> **Remarque :**
>
> À partir de la version 13.1-42.x de NetScaler, vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même VMSS dans Azure. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.

Pour consulter les informations relatives à la mise à l'échelle automatique sur le portail Azure, accédez à Virtual Machine Scale Sets**, puis sélectionnez**Virtual Machine Scale Set**> Scaling.**

Références

Pour plus d'informations sur la mise à l'échelle automatique de NetScaler VPX dans Microsoft Azure à l'aide de NetScaler Application Delivery and Management, consultez Azure Autoscale à l'aide de NetScaler ADM.

Balises Azure pour le déploiement de NetScaler VPX

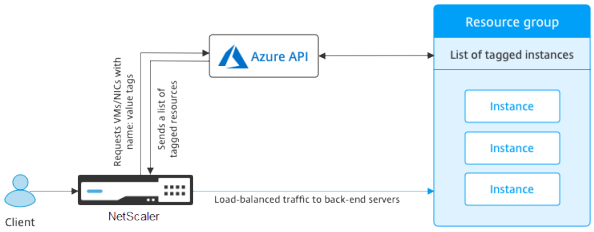
October 17, 2024

Dans le portail cloud Azure, vous pouvez baliser les ressources avec un nom : paire de valeurs (comme Dept : Finance) pour catégoriser et afficher les ressources entre les groupes de ressources et, au sein du portail, sur tous les abonnements. Le balisage est utile lorsque vous avez besoin d'organiser des ressources pour la facturation, la gestion ou l'automatisation.

Comment fonctionne la balise Azure pour le déploiement VPX

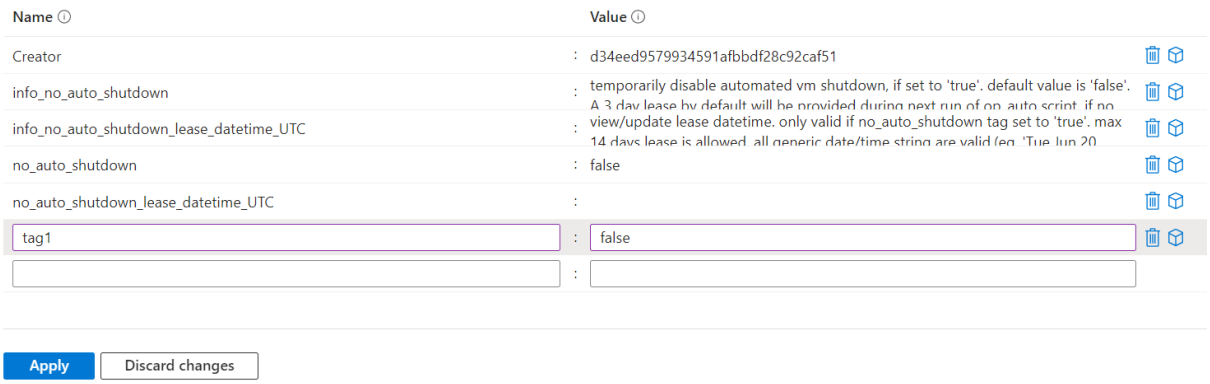
Pour les instances autonomes et à haute disponibilité NetScaler VPX déployées sur Azure Cloud, vous pouvez désormais créer des groupes de services d'équilibrage de charge associés à une balise Azure. L'instance VPX surveille constamment les machines virtuelles Azure (serveurs back-end) et les interfaces réseau (NIC), ou les deux, avec la balise respective et met à jour le groupe de services en conséquence.

L'instance VPX crée le groupe de services qui équilibre la charge des serveurs back-end à l'aide de balises. L'instance interroge l'API Azure pour toutes les ressources qui sont balisées avec un nom de balise et une valeur de balise particuliers. En fonction de la période d'interrogation attribuée (60 secondes par défaut), l'instance VPX interroge régulièrement l'API Azure et récupère les ressources disponibles avec le nom et les valeurs de balise attribués dans l'interface graphique VPX. Chaque fois qu'une machine virtuelle ou une carte réseau avec le tag approprié est ajoutée ou supprimée, l'ADC détecte la modification correspondante et ajoute ou supprime automatiquement l'adresse IP de la machine virtuelle ou de la carte réseau du groupe de services.



Avant de commencer

Avant de créer des groupes de services d'équilibrage de charge NetScaler, ajoutez une balise aux serveurs dans Azure. Vous pouvez affecter la balise à la machine virtuelle ou à la carte réseau.



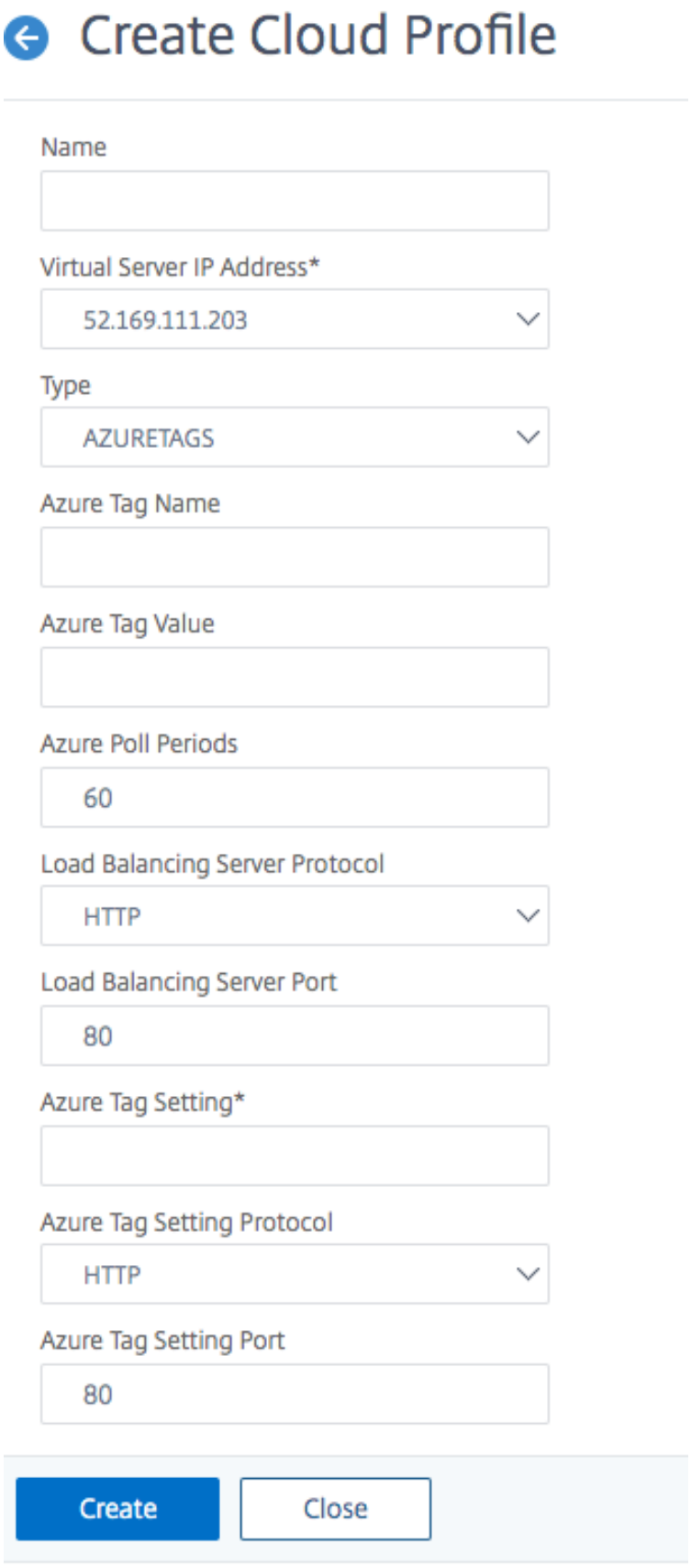
Pour plus d'informations sur l'ajout de balises Azure, consultez le document Microsoft Utiliser des balises pour organiser vos ressources Azure.

> **Remarque :**
>
> Les commandes ADC CLI permettant d'ajouter des paramètres de balise Azure prennent en charge les noms de balise et les valeurs de balise qui commencent uniquement par des chiffres ou des lettres et non par d'autres caractères du clavier.

Comment ajouter des paramètres de balise Azure à l'aide de l'interface graphique VPX

Vous pouvez ajouter le profil de cloud de balises Azure à une instance VPX à l'aide de l'interface graphique VPX afin que l'instance puisse équilibrer la charge des serveurs principaux à l'aide de la balise spécifiée. Procédez comme suit :

1. À partir de l'interface graphique VPX, accédez à **Configuration > Azure > Cloud Profile**.
2. Cliquez sur Ajouter pour créer un profil cloud. La fenêtre du profil cloud s'ouvre.



1. Entrez des valeurs pour les champs suivants :
    - Nom : Ajoutez un nom à votre profil
    - Adresse IP du serveur virtuel : l'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
    - Type : Dans le menu, sélectionnez AZURETAGS.
    - Nom de balise Azure : entrez le nom que vous avez attribué aux machines virtuelles ou aux cartes réseau dans le portail Azure.
    - Valeur de balise Azure : entrez la valeur que vous avez attribuée aux machines virtuelles ou aux cartes réseau dans le portail Azure.
    - Périodes de sondage Azure : par défaut, la période de sondage est de 60 secondes, ce qui est la valeur minimale. Vous pouvez le modifier selon vos besoins.
    - Protocole du serveur d'équilibrage de charge : sélectionnez le protocole que votre équilibreur de charge écoute.
    - Port du serveur d'équilibrage de charge : sélectionnez le port sur lequel votre équilibreur de charge écoute.
    - Paramètre de balise Azure : nom du groupe de services qui sera créé pour ce profil cloud.
    - Protocole de réglage des balises Azure : sélectionnez le protocole que vos serveurs principaux écoutent.
    - Port de réglage des balises Azure : sélectionnez le port sur lequel vos serveurs principaux écoutent.
2. Cliquez sur **Créer**.

Un serveur virtuel d'équilibrage de charge et un groupe de services sont créés pour les machines virtuelles ou les cartes réseau balisées. Pour voir le serveur virtuel d'équilibrage de charge, à partir de l'interface graphique VPX, accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

Comment ajouter des paramètres de balise Azure à l'aide de l'interface de ligne de commande VPX

Tapez la commande suivante sur l'interface de ligne de commande NetScaler pour créer un profil cloud pour les balises Azure.

```
add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>`
     -port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
     specified on the Azure portal>` -azurePollPeriod 60
```


> **Important :**
>
> Vous devez enregistrer toutes les configurations ; sinon, les configurations sont perdues après le redémarrage de l'instance. Tapez `save config`.

Exemple 1 : Voici un exemple de commande pour un profil cloud pour le trafic HTTP de toutes les machines virtuelles/cartes réseau Azure étiquetées avec la paire « MyTagName/MyTagValue » :

```
1   add cloud profile MyTagCloudProfile -type azuretags -vServerName
       MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
       serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
        -vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue
       myTagValue -azurePollPeriod 60
2   Done
```

Pour afficher le profil de cloud, tapez `show cloudprofile`.

Exemple 2 : la commande CLI suivante imprime des informations sur le profil de cloud nouvellement ajouté dans l'exemple 1.

```
1   show cloudprofile
2   1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
        MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
       Port:  80               ServiceGroupName:  MyTagsServiceGroup
       BoundServiceGroupSvcType:  HTTP
3          Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue
              :  myTagValue AzurePollPeriod:  60     GraceFul:  NO
                        Delay:  60
```

Pour supprimer un profil cloud, tapez rm cloud profile <cloud profile name>

Exemple 3 : La commande suivante supprime le profil de cloud créé dans l'exemple 1.

```
1   > rm cloudprofile MyTagCloudProfile
2     Done
```

Dépannage

Problème : Dans de très rares cas, la commande CLI « profil cloud rm » peut ne pas supprimer le groupe de services et les serveurs associés au profil cloud supprimé. Cela se produit lorsque la commande est émise secondes avant l'expiration de la période d'interrogation du profil de cloud en cours de suppression.

Solution : supprimez manuellement les groupes de services restants en saisissant la commande CLI suivante pour chacun des groupes de services restants :

```
1   #> rm servicegroup <serviceGroupName>
```


Supprimez également chacun des serveurs restants en entrant la commande CLI suivante pour chacun des serveurs restants :

```
#> rm server <name>
```

Problème : Si vous ajoutez un paramètre de balise Azure à une instance VPX à l'aide de l'interface de ligne de commande, le processus rain_tags continue de s'exécuter sur un nœud de paire HA après un redémarrage chaud.

Solution : Terminer manuellement le processus sur le nœud secondaire après un redémarrage à chaud. À partir de l'interface de ligne de commande du nœud HA secondaire, sortez de l'invite de commandes :

```
#> shell
```

Utilisez la commande suivante pour tuer le processus rain_tags :

```
# PID=`ps -aux | grep rain_tags | awk '{
print $2 }
'`; kill -9 $PID
```

Problème : les serveurs back-end peuvent ne pas être accessibles et signalés comme DOWN par l'instance VPX, bien qu'ils soient en bonne santé. **Solution** : Assurez-vous que l'instance VPX peut atteindre l'adresse IP balisée correspondant au serveur principal. Pour une carte réseau balisée, il s'agit de l'adresse IP de la carte réseau ; alors que pour une machine virtuelle balisée, il s'agit de l'adresse IP principale de la machine virtuelle. Si la VM/NIC réside sur un autre réseau virtuel Azure, assurez-vous que l'appairage de VNet est activé.

Configurer GSLB sur des instances NetScaler VPX

October 17, 2024

Les appliances NetScaler configurées pour l'équilibrage global de la charge des serveurs (GSLB) assurent la reprise après sinistre et la disponibilité continue des applications en les protégeant contre les points de défaillance d'un réseau étendu. GSLB peut équilibrer la charge entre les centres de données en dirigeant les demandes des clients vers le centre de données le plus proche ou le plus performant, ou vers les centres de données survivants en cas de panne.

Cette section décrit comment activer GSLB sur des instances VPX sur deux sites dans un environnement Microsoft Azure, à l'aide des commandes Windows PowerShell.

> **Remarque :**
>
> Pour plus d'informations sur GSLB, consultez Global Server Load Balancing.

Vous pouvez configurer GSLB sur une instance NetScaler VPX sur Azure, en deux étapes :

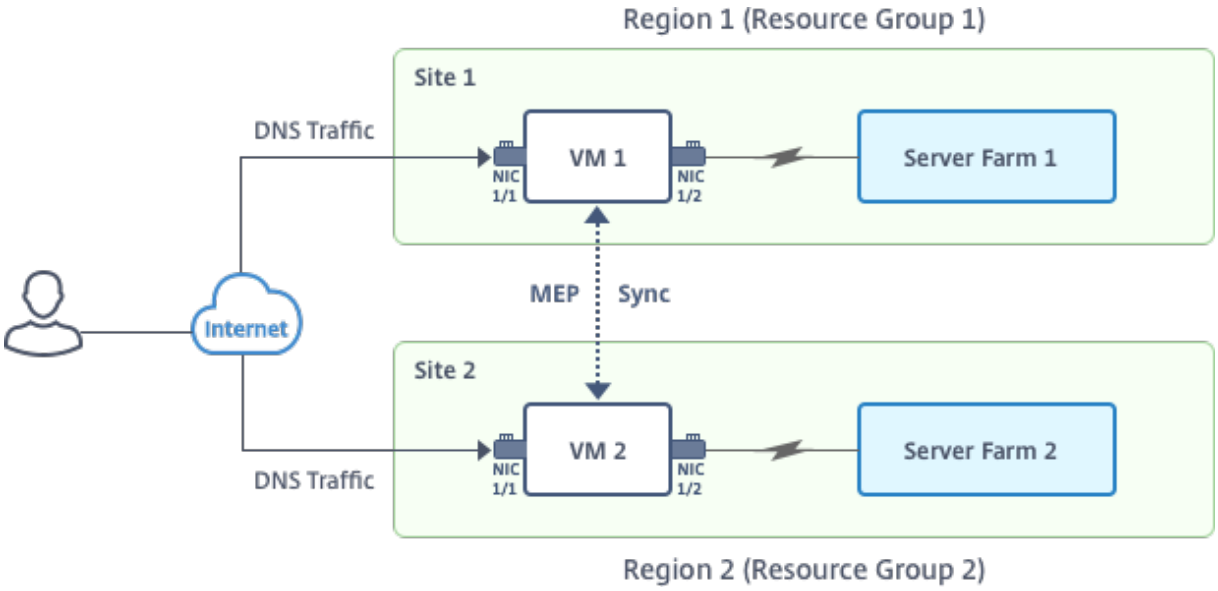
1. Créez une instance VPX avec plusieurs cartes réseau et plusieurs adresses IP, sur chaque site.
2. Activez GSLB sur les instances VPX.

> **Remarque :**
>
> Pour plus d'informations sur la configuration de plusieurs cartes réseau et adresses IP, voir : Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome àl'aide des commandes PowerShell

Scénario

Ce scénario inclut deux sites : le site 1 et le site 2. Chaque site possède une machine virtuelle (VM1 et VM2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

Chiffre. Configuration GSLB mise en œuvre sur deux sites : Site 1 et Site 2.



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Chaque carte réseau peut avoir plusieurs adresses IP privées et publiques. Les cartes réseau sont configurées aux fins suivantes.

- Carte réseau 0/1 : pour le trafic de gestion
- Carte réseau 1/1 : pour servir le trafic côté client
- NIC 1/2 : pour communiquer avec les serveurs back-end

Pour plus d'informations sur les adresses IP configurées sur chaque carte réseau dans ce scénario, reportez-vous à la section Détails de la configuration IP .

Paramètres

Voici des exemples de paramètres de paramètres pour ce scénario dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard\_DS3\_V2"
```

> **Remarque :**
>
> La configuration minimale requise pour une instance VPX est de 2 vCPU et 2 Go de RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"
```



```
32
33    $IPConfigName4="IPConfig-4"
34
35    $frontendSubnetName="default"
36
37    $backendSubnetName1="subnet\_1"
38
39    $backendSubnetName2="subnet\_2"
40
41    $suffixNumber=10
```

Créer une machine virtuelle

Suivez les étapes 1 à 10 pour créer VM1 avec plusieurs cartes réseau et plusieurs adresses IP, à l'aide des commandes PowerShell :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un ensemble de disponibilités
4. Création d'un réseau virtuel
5. Créer une adresse IP publique
6. Créer des cartes réseau
7. Créer un objet de configuration de machine virtuelle
8. Obtenir des informations d'identification et définir les propriétés du système d'exploitation pour la machine virtuelle
9. Ajouter des cartes réseau
10. Spécifier le disque du système d'exploitation et créer une machine virtuelle

Après avoir effectué toutes les étapes et commandes nécessaires à la création de VM1, répétez ces étapes pour créer une VM2 avec les paramètres qui lui sont spécifiques.

Créer un groupe de ressources

```
1    New-AzureRMResourceGroup -Name $RGName -Location $location
```

Créer un compte de stockage


```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $RGName -Type
    Standard_LRS -Location $location
```

Créer un ensemble de disponibilités

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
```

Création d'un réseau virtuel

1. Ajoutez des sous-réseaux.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix "10.0.0.0/24"
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix "10.0.1.0/24"
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
```

2. Ajoutez un objet réseau virtuel.

```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -
    ResourceGroupName $RGName -Location $location -AddressPrefix
    10.0.0.0/16 -Subnet $subnet1, $subnet2, $subnet3
```

3. Récupérez des sous-réseaux.

```
 $frontendSubnet=$vnet.Subnets|?{
$_.Name -eq $frontendSubnetName }

 $backendSubnet1=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName1 }

 $backendSubnet2=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName2 }
```

Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
```


Créer des cartes réseau

Créer une carte réseau 0/1

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -
    PrivateIpAddress $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
```

Créer une carte réseau 1/1

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2,
    $IpConfig3
```

Créer une carte réseau 1/2

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
```

Créer un objet de configuration de machine virtuelle

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
```

Obtenir des informations d'identification et définir les propriétés du système d'exploitation

```
$cred=Get-Credential -Message "Type the name and password for VPX
    login."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
```


Ajouter des cartes réseau

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
```

Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
    /" +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
     $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
     -Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
```

> **Remarque :**
>
> Répétez les étapes 1 à 10 répertoriées dans « Créer des machines virtuelles multi-cartes réseau à l'aide des commandes PowerShell » pour créer VM2 avec des paramètres spécifiques à VM2.

Détails de la configuration IP

Les adresses IP suivantes sont utilisées.

Tableau 2. Adresses IP utilisées dans VM1

Carte d'interface réseau	IP privée	Adresse IP publique (PIP)	Description
0/1	10.0.0.10	PIP1	Configuré en tant que NSIP (IP de gestion)
1/1	10.0.1.10	PIP2	Configuré en tant qu'adresse IP du site SNIP/GSLB

Carte d'interface réseau	IP privée	Adresse IP publique (PIP)	Description
-	10.0.1.11	-	Configuré en tant qu'adresse IP du serveur LB. L'adresse IP publique n'est pas obligatoire
1/2	10.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Tableau 2. Adresses IP utilisées dans VM2

Carte d'interface réseau	IP interne	Adresse IP publique (PIP)	Description
0/1	20.0.0.10	PIP4	Configuré en tant que NSIP (IP de gestion)
1/1	20.0.1.10	PIP5	Configuré en tant qu'adresse IP du site SNIP/GSLB
-	20.0.1.11	-	Configuré en tant qu'adresse IP du serveur LB. L'adresse IP publique n'est pas obligatoire
1/2	20.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Voici des exemples de configurations pour ce scénario, montrant les adresses IP et les configurations LB initiales créées via l'interface de ligne de commande NetScaler VPX pour VM1 et VM2.

Voici un exemple de configuration sur VM1.


```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
Add nsip 10.0.2.10 255.255.255.0
add service svc1 10.0.1.10 ADNS 53
add lb vserver v1 HTTP 10.0.1.11 80
add service s1 10.0.2.120 http 80
Add service s2 10.0.2.121 http 80
Bind lb vs v1 s[1-2]
```

Voici un exemple de configuration sur VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
```

Configurer les sites GSLB et d'autres paramètres

Effectuez les tâches décrites dans la rubrique suivante pour configurer les deux sites GSLB et les autres paramètres nécessaires :

Équilibrage de charge de serveur global

Voici un exemple de configuration GSLB sur VM1 et VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
   PIP3 -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP
   PIP6 -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Vous avez configuré GSLB sur des instances NetScaler VPX exécutées sur Azure.

Récupération d'urgence

La catastrophe est une perturbation soudaine des fonctions commerciales causée par des catastrophes naturelles ou des événements d'origine humaine. Les catastrophes affectent les opérations des centres de données, après quoi les ressources et les données perdues sur le site du sinistre doivent être entièrement reconstruites et restaurées. La perte de données ou les temps d'arrêt dans le datacenter sont critiques et réduit la continuité de l'activité.

L'un des défis auxquels les clients sont confrontés aujourd'hui est de décider où placer leur site de reprise après sinistre. Les entreprises recherchent la cohérence et les performances indépendamment des défaillances de l'infrastructure sous-jacente ou du réseau.

Les raisons possibles pour lesquelles de nombreuses entreprises décident de migrer vers le cloud sont les suivantes :

- Disposer d'un centre de données sur site coûte très cher. En utilisant le cloud, les entreprises peuvent libérer du temps et des ressources pour étendre leurs propres systèmes.
- La plupart des orchestrations automatisées permettent une restauration plus rapide
- Répliquez les données en fournissant une protection continue des données ou des instantanés continus pour vous prémunir contre toute panne ou attaque.
- Prenez en charge les cas d'utilisation dans lesquels les clients ont besoin de différents types de contrôles de conformité et de sécurité déjà présents sur les clouds publics. Ils leur permettent d'atteindre plus facilement la conformité dont ils ont besoin plutôt que de créer leur propre solution.

Un NetScaler configuré pour GSLB transfère le trafic vers le centre de données le moins chargé ou le plus performant. Cette configuration, appelée configuration active-active, améliore non seulement les performances, mais assure également une reprise après sinistre immédiate en acheminant le trafic vers d'autres centres de données si un centre de données faisant partie de la configuration est en panne. NetScaler permet ainsi aux clients d'économiser du temps et de l'argent.

Déploiement de plusieurs cartes réseau et de plusieurs adresses IP (trois cartes réseau) pour la reprise après sinistre

Les clients peuvent déployer à l'aide d'un déploiement à trois cartes réseau s'ils effectuent un déploiement dans un environnement de production où la sécurité, la redondance, la disponibilité, la capacité et l'évolutivité sont essentielles. Avec cette méthode de déploiement, la complexité et la facilité de gestion ne sont pas des préoccupations critiques pour les utilisateurs.

Déploiement d'une seule carte réseau et de plusieurs adresses IP (une carte réseau) pour la reprise après sinistre

Les clients sont susceptibles de procéder à un déploiement à l'aide d'une seule carte réseau s'ils le déploient dans un environnement hors production pour les raisons suivantes :

- Ils configurent l'environnement à des fins de test, ou ils mettent en place un nouvel environnement avant le déploiement en production.
- Déploiement rapide et efficace directement dans le cloud.

- Tout en recherchant la simplicité d'une configuration de sous-réseau unique.

Configurer GSLB sur une configuration haute disponibilité active-veille

October 17, 2024

Vous pouvez configurer l'équilibrage de charge globale du serveur (GSLB) sur un déploiement HA actif-standby sur Azure en trois étapes :

1. Créez une paire HA VPX sur chaque site GSLB. Consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau pour plus d'informations sur la création d'une paire HA.
2. Configurez l'équilibreur de charge Azure (ALB) avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS.

   Cette étape implique les sous-étapes suivantes. Reportez-vous au scénario de cette section pour connaître les commandes PowerShell utilisées pour effectuer ces sous-étapes.

   a. Créez un site frontal `IPconfig` pour GSLB.

   b. Créez un pool d'adresses back-end avec l'adresse IP de la carte réseau 1/1 des nœuds en HA.

   c. Créez des règles d'équilibrage de charge pour les éléments suivants :

   ```
   TCP/3009 – gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

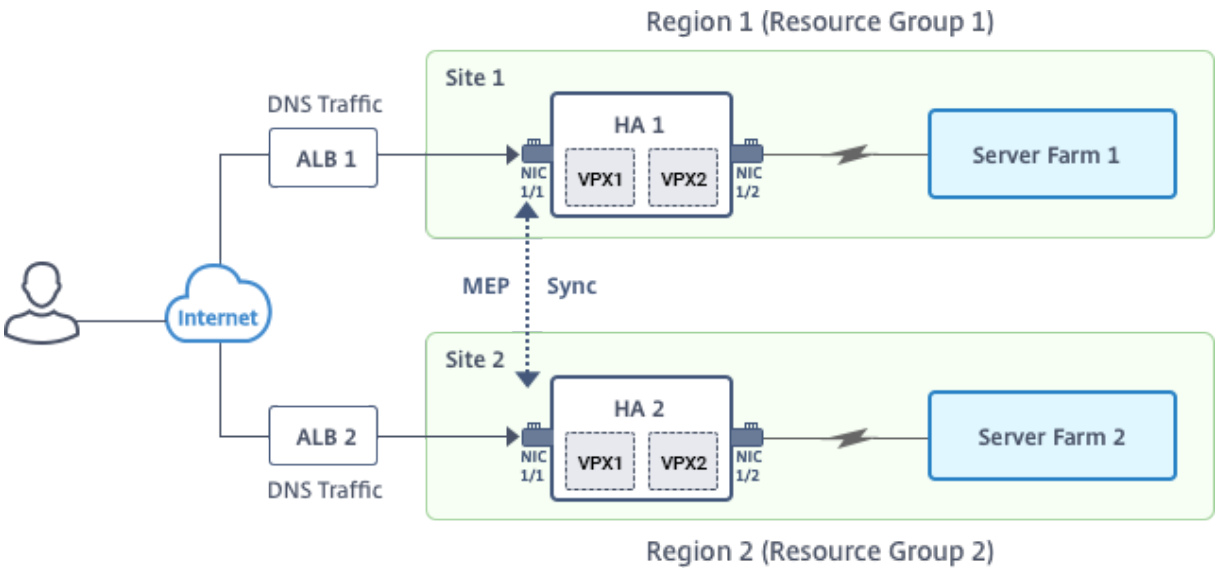
   d. Associer le pool d'adresses back-end aux règles LB créées à l'étape c.

   e. Mettez à jour le groupe de sécurité réseau de la carte réseau 1/1 des nœuds dans la paire HA pour autoriser le trafic pour les ports TCP 3008, TCP 3009 et UDP 53.
3. Activez GSLB sur chaque paire HA.

Scénario

Ce scénario inclut deux sites : le site 1 et le site 2. Chaque site possède une paire HA (HA1 et HA2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

Figure : GLSB sur un déploiement HA active-Standy sur Azure



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Les cartes réseau sont configurées aux fins suivantes.

Carte réseau 0/1 : pour le trafic de gestion

Carte réseau 1/1 : pour servir le trafic côté client

NIC 1/2 : pour communiquer avec les serveurs back-end

Réglages des paramètres

Vous trouverez ci-dessous des exemples de paramètres pour l'ALB. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"

$lbRuleName3="LBRuleGSLB2"

$lbRuleName4="LBRuleDNS"
```



```
20
21   $healthProbeName="HealthProbe"
```

Configurer ALB avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS

Étape 1. **Créer une adresse IP publique pour l'adresse IP du site GSLB**

```
1   $pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
        $rgName -DomainNameLabel $domName4 -Location $locName -
    AllocationMethod Dynamic
2
3
4   Get-AzureRmLoadBalancer -Name \$lbName -ResourceGroupName \$rgName |
    Add-AzureRmLoadBalancerFrontendIpConfig -Name \
    $frontEndConfigName2 -PublicIpAddress \$pip4 | Set-
    AzureRmLoadBalancer
```

Étape 2. **Créez des règles LB et mettez à jour l'ALB existant**.

```
1   $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName
2
3
4   $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2
5
6
7   $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1
8
9
10  $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName
11
12
13  \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
    BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
14
15
16  \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
    BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
17
18
```



```
\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName4 -
   BackendAddressPool \$backendPool -FrontendIPConfiguration  \
   $frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort
    53 -Probe \$healthprobe -EnableFloatingIP  | Set-
   AzureRmLoadBalancer
```

Activer GSLB sur chaque paire haute disponibilité

Vous avez maintenant deux adresses IP frontales pour chaque ALB : ALB 1 et ALB 2. Une adresse IP est destinée au serveur virtuel LB et l'autre à l'adresse IP du site GSLB.

HA 1 possède les adresses IP frontales suivantes :

- FrontEndIPofALB1 (pour serveur virtuel LB)
- PIPFORGSLB1 (IP GSLB)

HA 2 possède les adresses IP frontales suivantes :

- FrontEndIPofALB2 (pour serveur virtuel LB)
- PIPFORGSLB2 (IP GSLB)

Les commandes suivantes sont utilisées pour ce scénario.

```
enable ns feature LB GSLB

add service dnssvc PIPFORGSLB1 ADNS 53

add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1

add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2

add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
   publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
   publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Ressources connexes :

Configurer GSLB sur des instances NetScaler VPX

Équilibrage de charge de serveur global

Déployez NetScaler GSLB sur Azure

October 17, 2024

Face à la demande croissante, les entreprises qui exploitent un centre de données sur site au service de clients régionaux souhaitent évoluer et déployer leurs activités dans le monde entier à l'aide du cloud Azure. Avec NetScaler du côté de l'administrateur réseau, vous pouvez utiliser le GSLB StyleBook pour configurer des applications sur site et dans le cloud. Vous pouvez transférer la même configuration vers le cloud avec NetScaler ADM. Vous pouvez accéder aux ressources sur site ou dans le cloud en fonction de la proximité avec GSLB. Cela vous permet de bénéficier d'une expérience fluide, où que vous vous trouviez dans le monde.

Présentation de DBS

NetScaler GSLB prend en charge l'utilisation de services basés sur le domaine (DBS) pour les équilibreurs de charge dans le cloud. Cela permet la découverte automatique des services cloud dynamiques à l'aide d'une solution d'équilibreur de charge cloud. Cette configuration permet à NetScaler d'implémenter GSLB DBS dans un environnement Active-Active. DBS permet de dimensionner les ressources dorsales dans les environnements Microsoft Azure à partir de la découverte DNS. Cette section couvre l'intégration entre NetScalers dans l'environnement Azure Autoscale.

Services basés sur des noms de domaine utilisant Azure Load Balancer (ALB)

GLSB DBS utilise le nom de domaine complet de l'utilisateur ALB pour mettre à jour dynamiquement les groupes de services GSLB afin d'inclure les serveurs principaux créés et supprimés dans Azure. Pour configurer cette fonctionnalité, l'utilisateur pointe le Citrix ADC vers son ALB afin d'acheminer dynamiquement vers différents serveurs dans Azure. Ils peuvent le faire sans avoir à mettre à jour manuellement Citrix ADC chaque fois qu'une instance est créée et supprimée dans Azure. La fonctionnalité Citrix ADC DBS pour les groupes de services GSLB utilise la découverte de services compatible DNS pour déterminer les ressources de service membres de l'espace de noms DBS identifié dans le groupe Autoscale.

L'image suivante décrit les composants de mise à l'échelle automatique NetScaler GSLB DBS avec des équilibreurs de charge cloud :

Prérequis pour Azure GSLB

Les prérequis pour les groupes de services NetScaler GSLB incluent un environnement Microsoft Azure fonctionnel doté des connaissances et des capacités nécessaires pour configurer des groupes de sécurité, des serveurs Web Linux, des appliances NetScaler au sein d'AWS, des adresses IP élastiques et des équilibreurs de charge élastiques (ELB).

- L'intégration du service GSLB DBS nécessite NetScaler version 12.0.57 pour les instances d'équilibreur de charge Microsoft Azure.
- Entité du groupe de services GSLB : NetScaler version 12.0.57.
- Le groupe de services GSLB est introduit. Il prend en charge la mise à l'échelle automatique à l'aide de la découverte dynamique DBS.
- Les composants fonctionnels DBS (service basé sur le domaine) doivent être liés au groupe de services GSLB.

Exemple

```
```

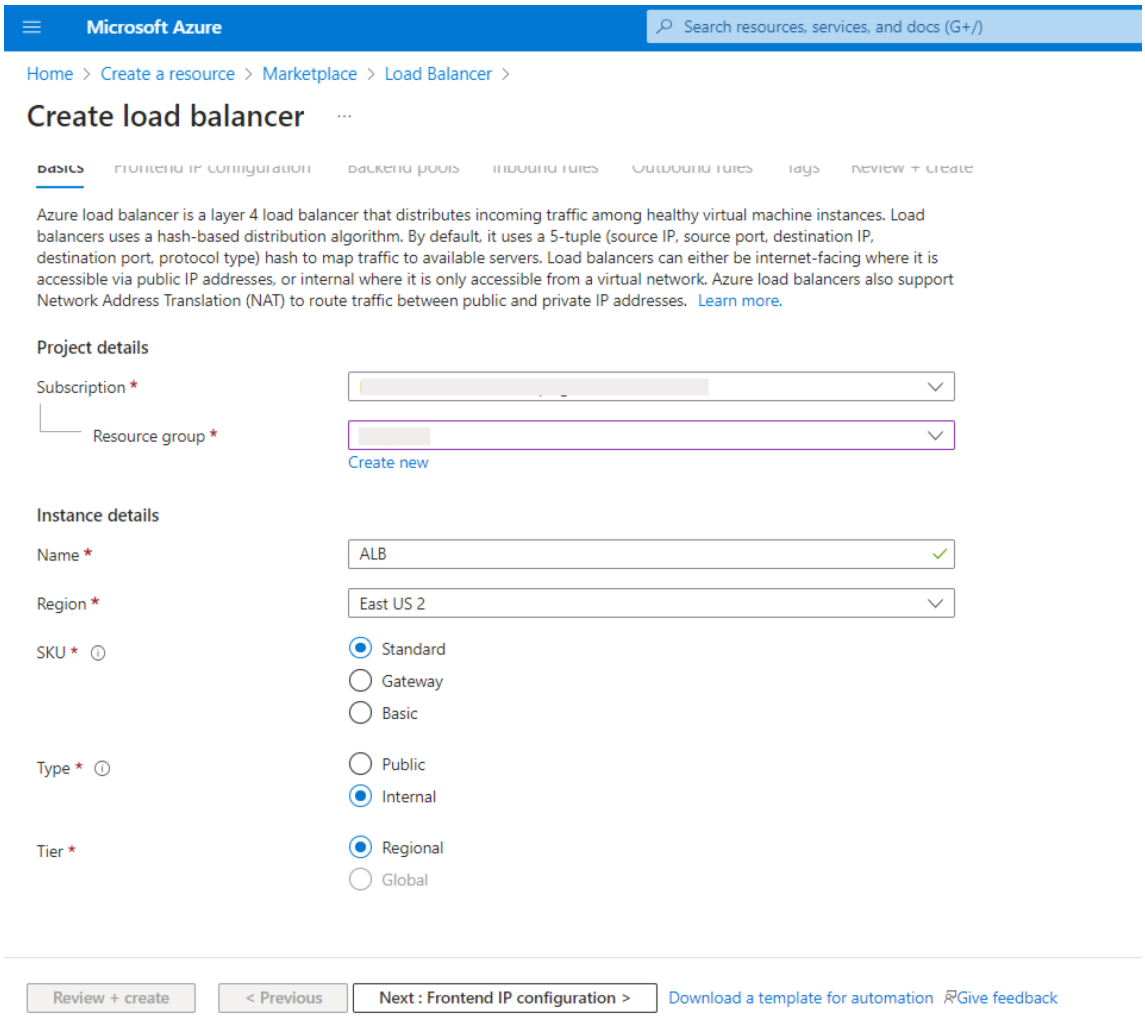
```
    > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
       amazonaws.com
    > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName
       sydney
    > bind gslb serviceGroup sydney_sg sydney_server 80
```

```
```

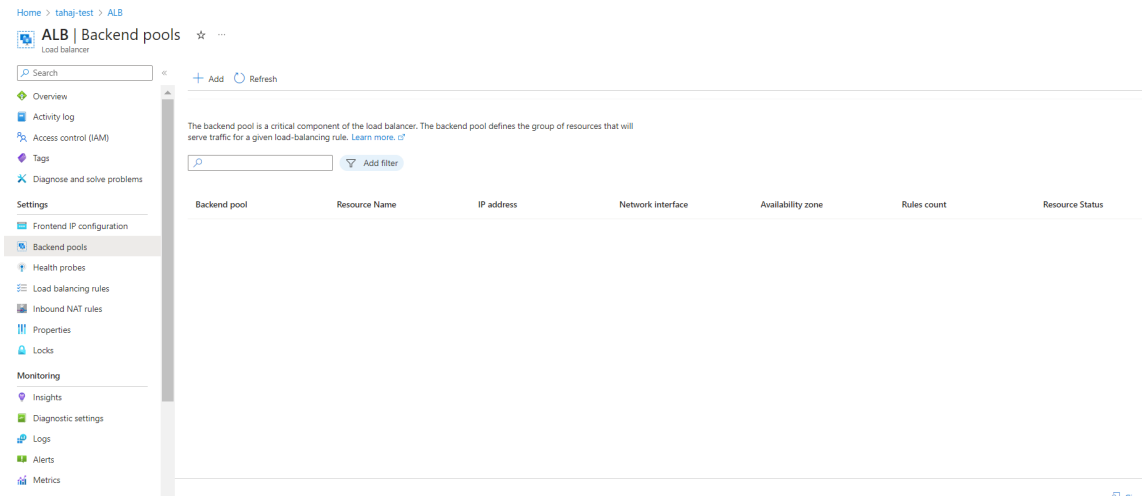
Configuration des composants Azure

1. Connectez-vous à l'utilisateur Azure Portal et créez une nouvelle machine virtuelle à partir d'un modèle NetScaler.

2. Créez un équilibreur de charge Azure.



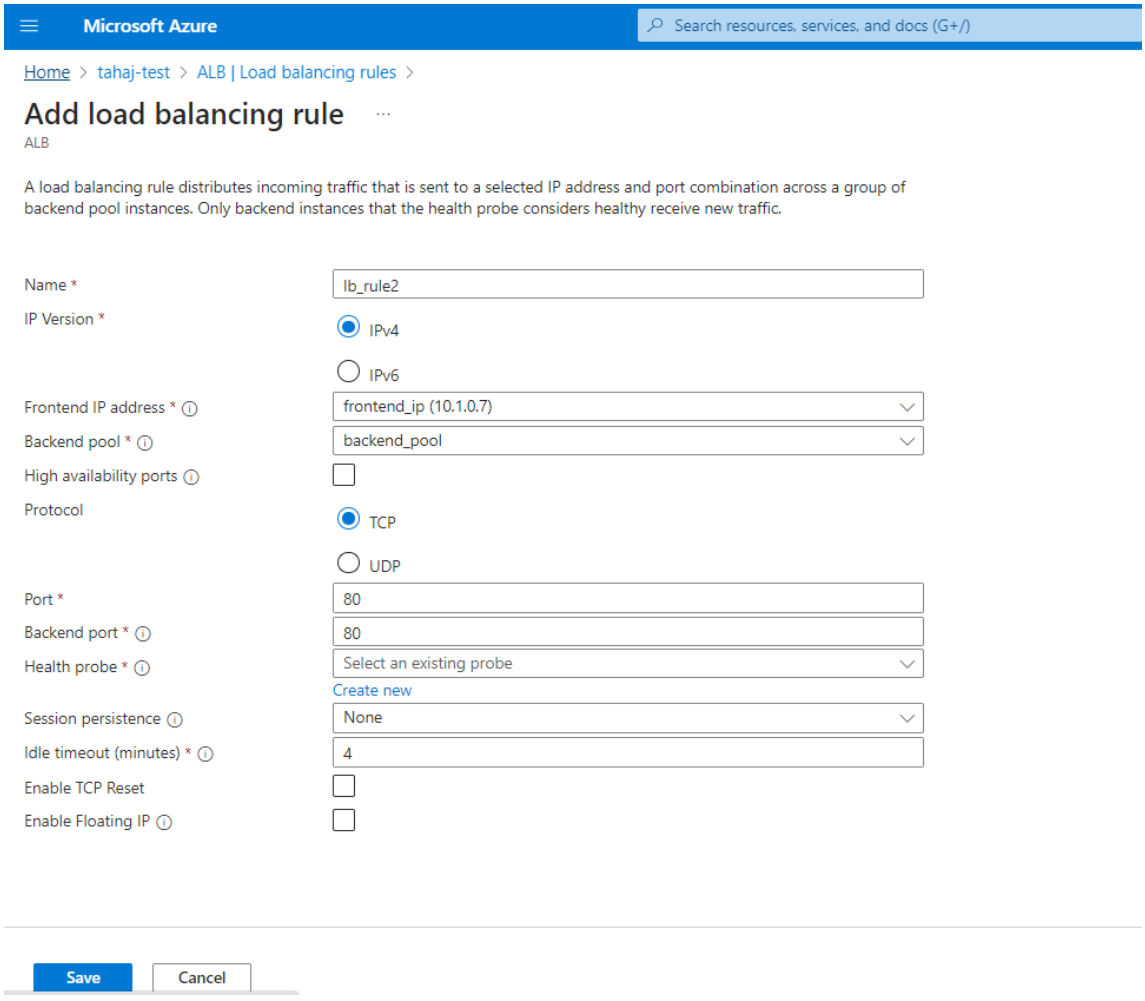
3. Ajoutez les pools principaux NetScaler créés.



4. Créez une analyse de santé pour le port 80.

Créez une règle d'équilibrage de charge à l'aide de l'adresse IP frontale créée à partir de l'équilibreur de charge.

- Protocole : TCP
- Port principal : 80
- Pool principal : NetScaler créé à l'étape 1
- Analyse de santé : créée à l'étape 4
- Persistance de la session : Aucun



Configurer le service basé sur le domaine NetScaler GSLB

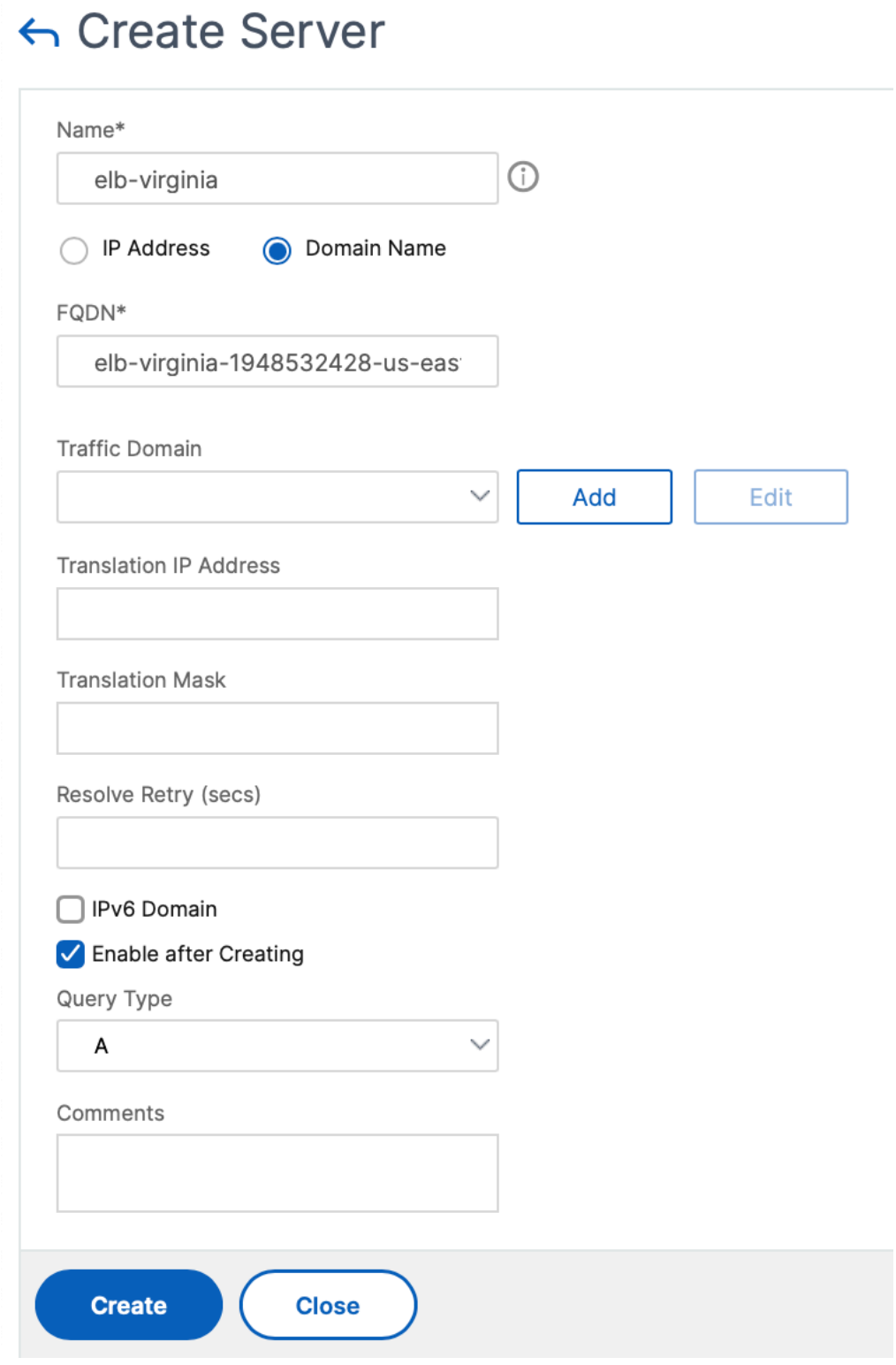
Les configurations suivantes résument ce qui est nécessaire pour activer les services basés sur le domaine pour la mise à l'échelle automatique des ADC dans un environnement compatible GSLB.

- Configurations de gestion du trafic
- Configurations GSLB

Configurations de gestion du trafic

> **Remarque :**
>
> Il est nécessaire de configurer NetScaler avec un serveur de noms ou un serveur virtuel DNS via lequel les domaines ELB /ALB sont résolus pour les groupes de services DBS. Pour plus d'informations sur les serveurs de noms ou les serveurs virtuels DNS, voir : DNS NameServer

1. Accédez à**Gestion du trafic > Équilibrage de charge > Serveurs**.
2. Cliquez sur **Ajouter** pour créer un serveur, fournir un nom et un FQDN correspondant à l'enregistrement A (nom de domaine) dans Azure pour l'ALB.



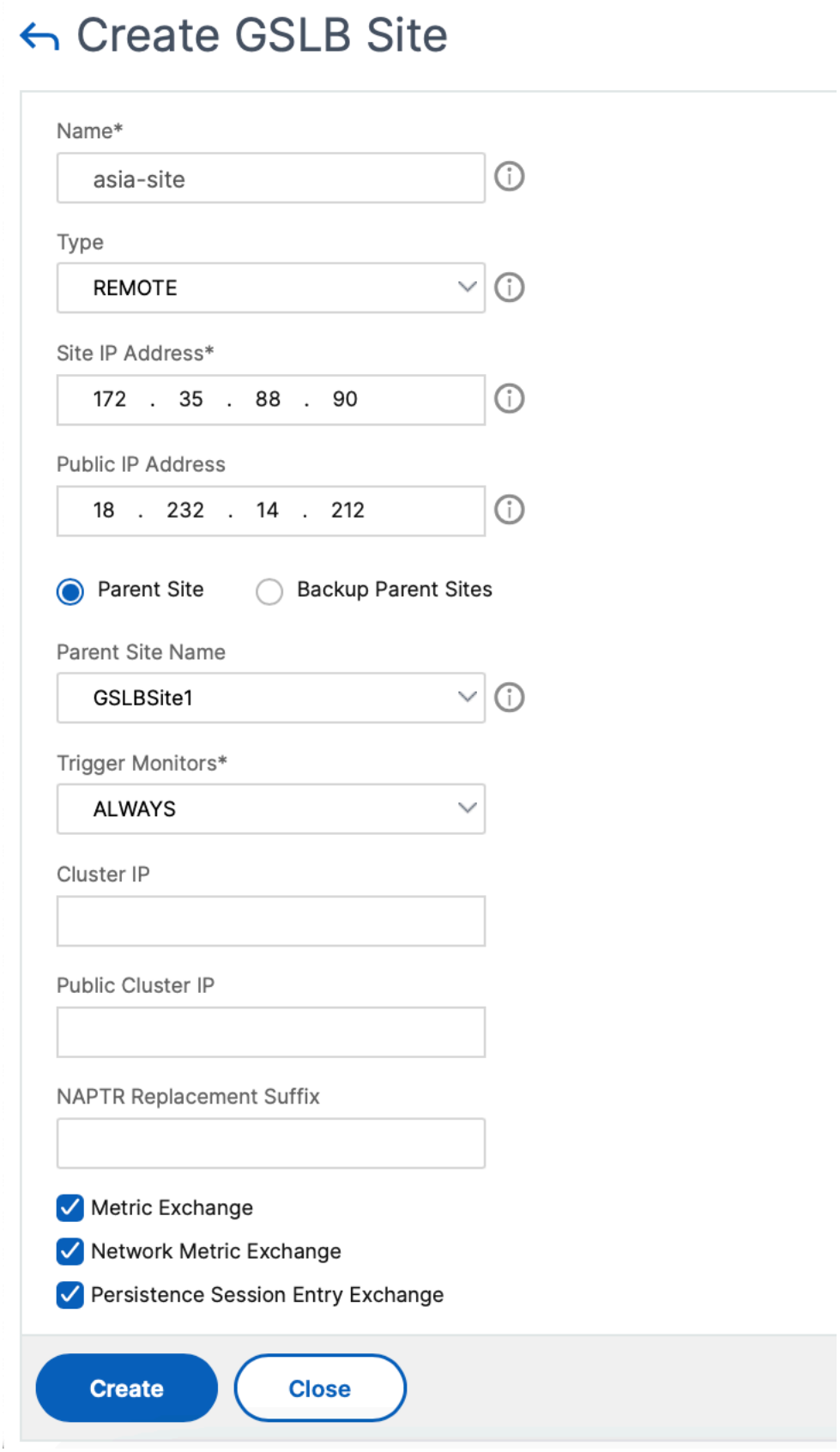
3. Répétez l'étape 2 pour ajouter le deuxième ALB à partir de la deuxième ressource dans Azure.

Configurations GSLB

1. Cliquez sur **Ajouter**pour configurer un site GSLB.
2. Spécifiez les détails de configuration du site GSLB

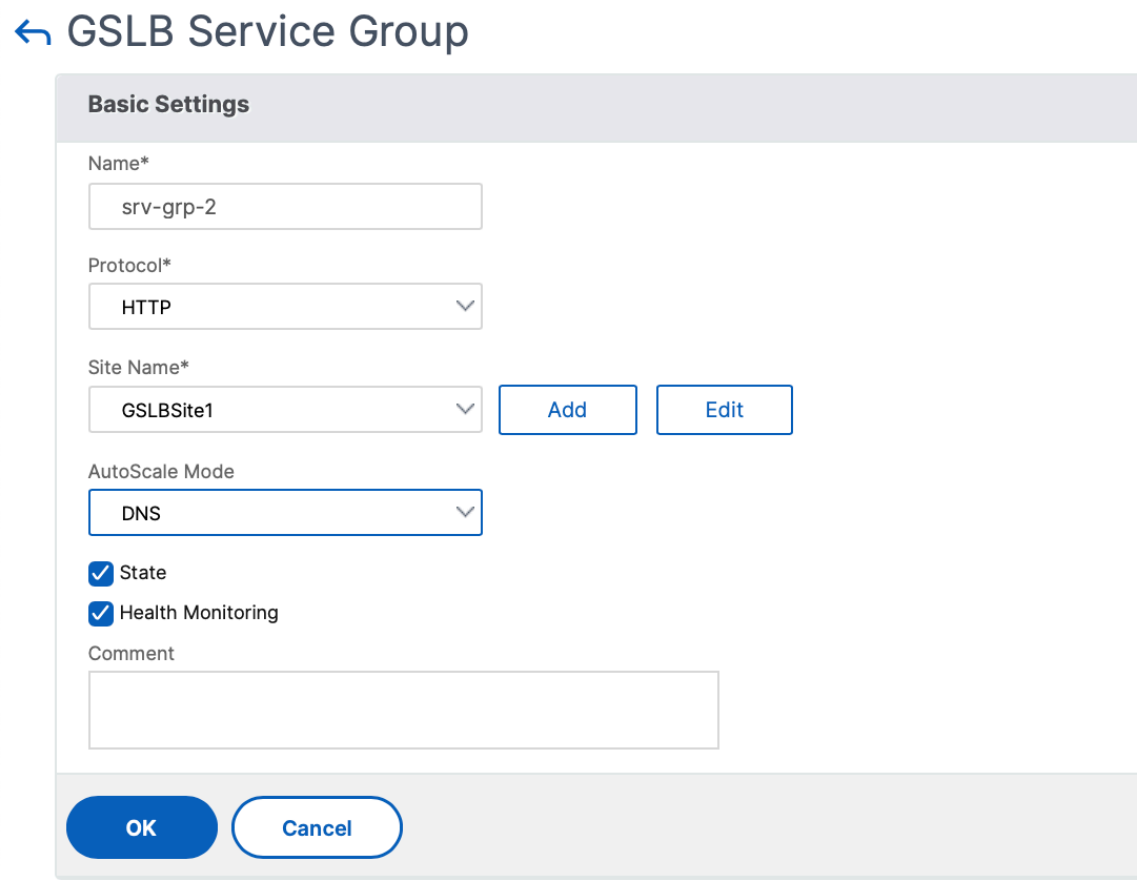
   Donnez un nom au site. Le type est configuré comme distant ou local en fonction du NetScaler sur lequel vous configurez le site. L'adresse IP du site est l'adresse IP du site GSLB. Le site GSLB utilise cette adresse IP pour communiquer avec les autres sites GSLB. L'adresse IP publique est requise lors de l'utilisation d'un service cloud où une adresse IP particulière est hébergée sur un pare-feu externe ou un périphérique NAT. Le site doit être configuré en tant que site parent. Assurez-vous que les **moniteurs de déclenchement** sont réglés sur **ALWAYS**. Assurez-vous également de cocher les trois cases en bas pour **Metric Exchange**, **Network Metric Exchange**et **Persistence Session Entry Exchange**.

   Nous vous recommandons de régler le **moniteur Trigger** sur **MEPDOWN**. Pour plus d'informations, voirConfigurer un groupe de services GSLB.

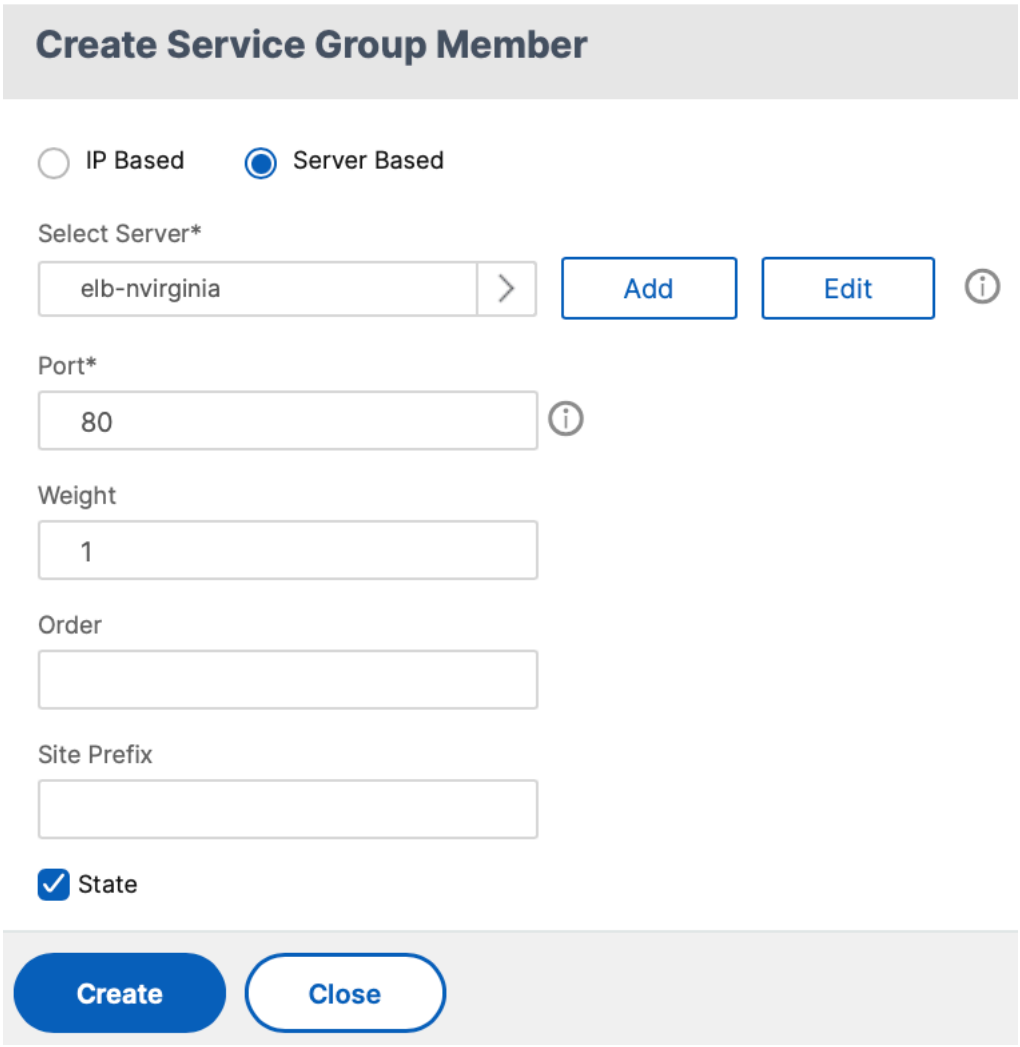


3. Cliquez sur**Créer**.
4. Accédez à**Gestion du trafic > GSLB > Groupes de services.**
5. Cliquez sur **Ajouter** pour ajouter un groupe de services.
6. Spécifiez les détails pour configurer le groupe de services

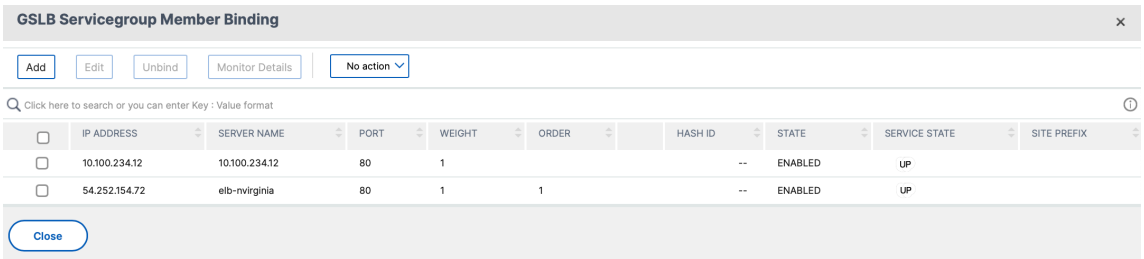
   Nommez le groupe de services, utilisez le protocole HTTP. Sous **Nom du site**, choisissez le site que vous avez créé. Assurez-vous de configurer le mode AutoScale en tant que DNS et cochez les cases État et Contrôle de l'intégrité. Cliquez sur **OK** pour créer le groupe de services.



7. Cliquez sur **Membres du groupe de services** et sélectionnez **Basé sur un serveur**. Sélectionnez l'ELB correspondant qui a été configuré au début du guide d'exécution. Configurez le trafic pour passer par le port 80. Cliquez sur**Créer**.



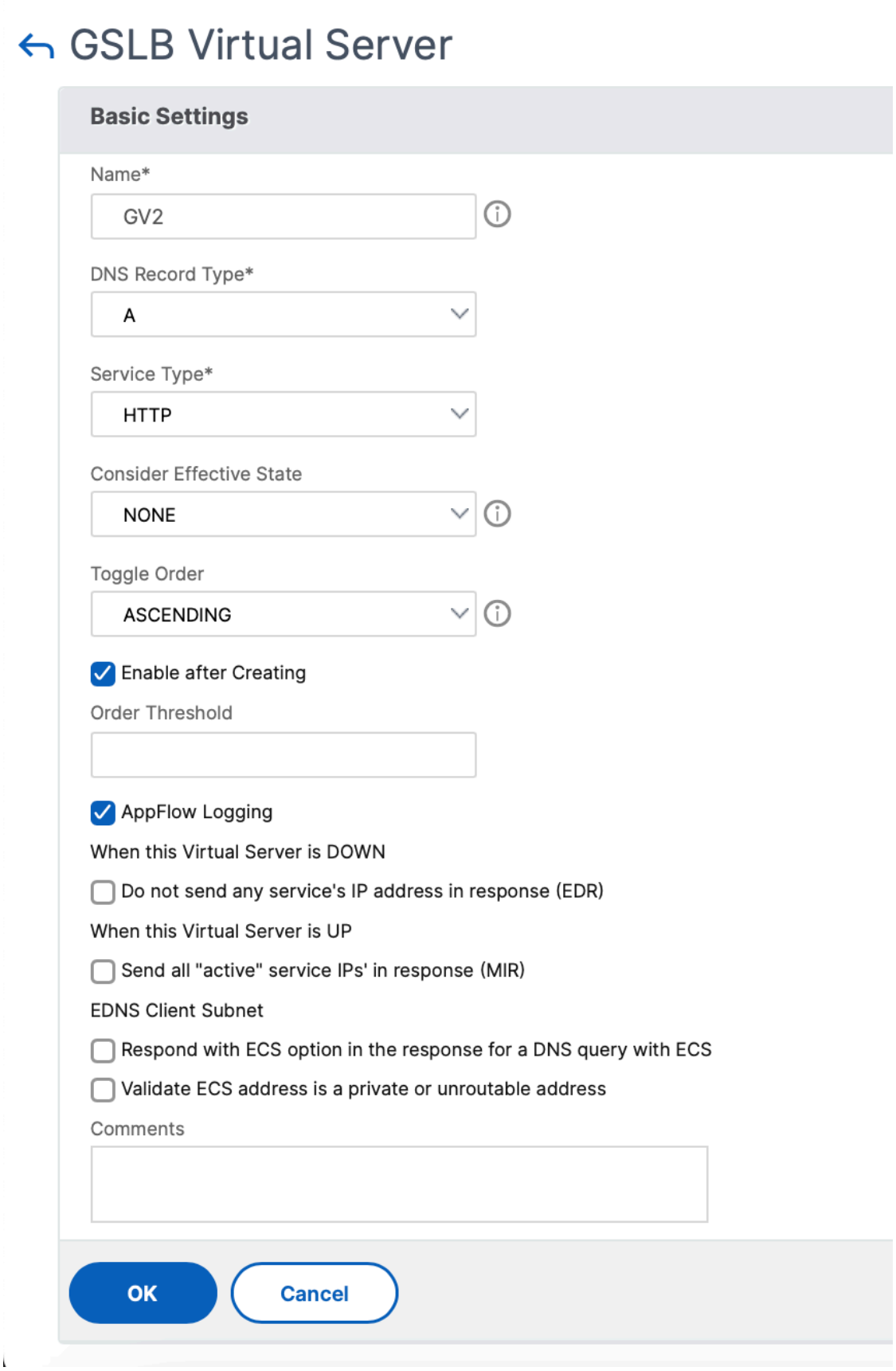
La liaison des membres du groupe de services doit être renseignée avec 2 instances qu'elle reçoit de l'ELB.



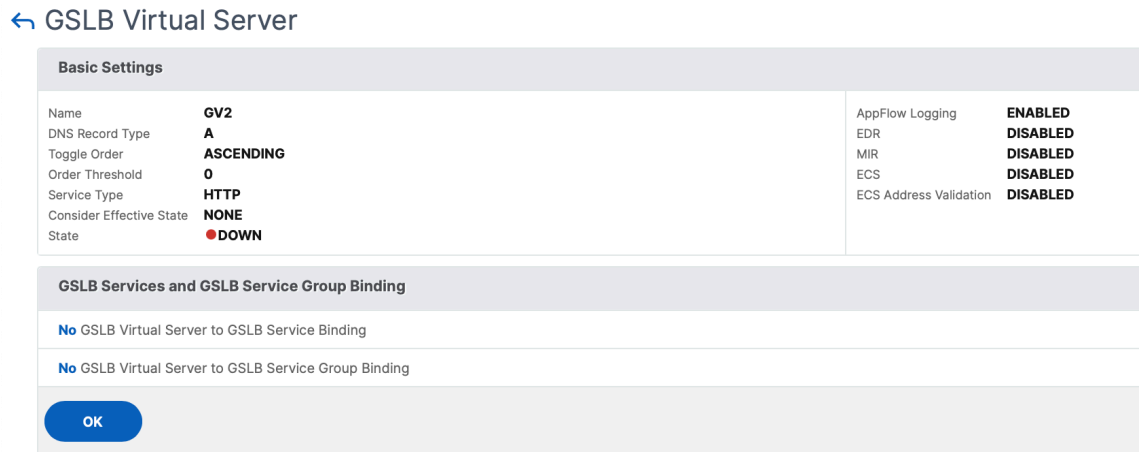
8. Répétez les étapes 5 et 6 pour configurer le groupe de services pour le deuxième emplacement de ressources dans Azure. (Cela peut être fait à partir de la même interface graphique NetScaler).
9. Pour configurer un serveur virtuel GSLB. Accédez à **Gestion du trafic > GSLB > Serveurs virtuels**.

10. Cliquez sur **Ajouter** pour créer le serveur virtuel.
11. Spécifiez les détails pour configurer le serveur virtuel GSLB.

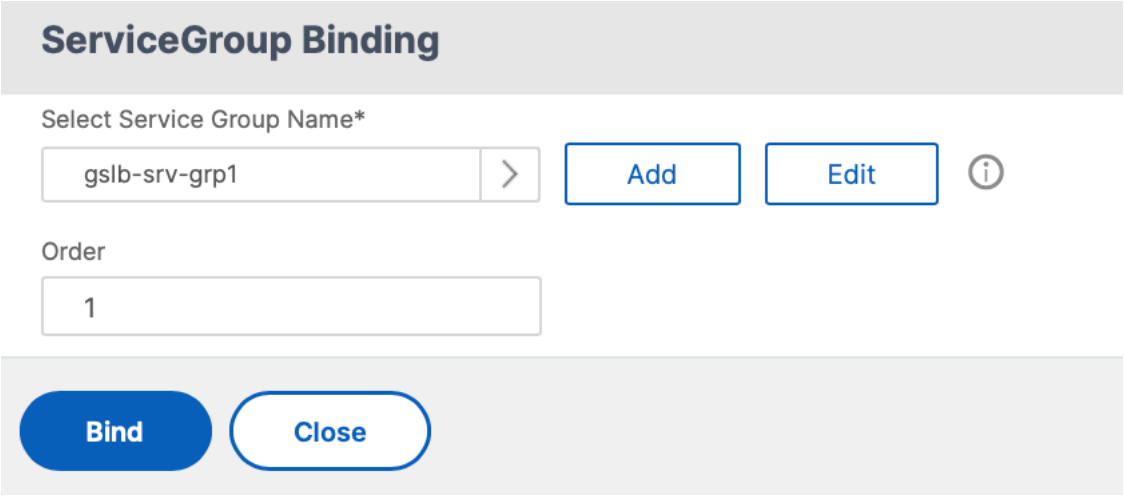
    Nommez le serveur, le type d'enregistrement DNS est défini comme A, le type de service est défini comme HTTP et cochez les cases Activer après la création et la journalisation AppFlow. Cliquez sur **OK** pour créer le serveur virtuel GSLB.



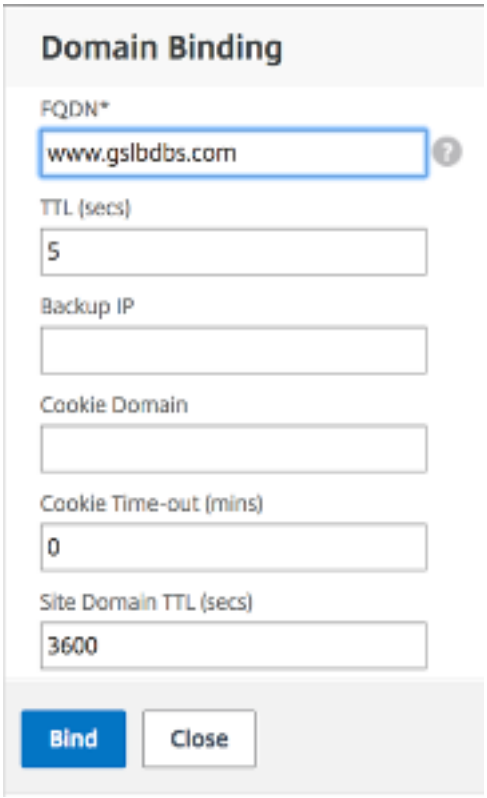
12. Une fois le serveur virtuel GSLB créé, cliquez sur **No GSLB Virtual Server ServiceGroup Binding**.



13. Sous **ServiceGroup Binding**, utilisez**Select Service Group Name** pour sélectionner et ajouter les groupes de services qui ont été créés lors des étapes précédentes.

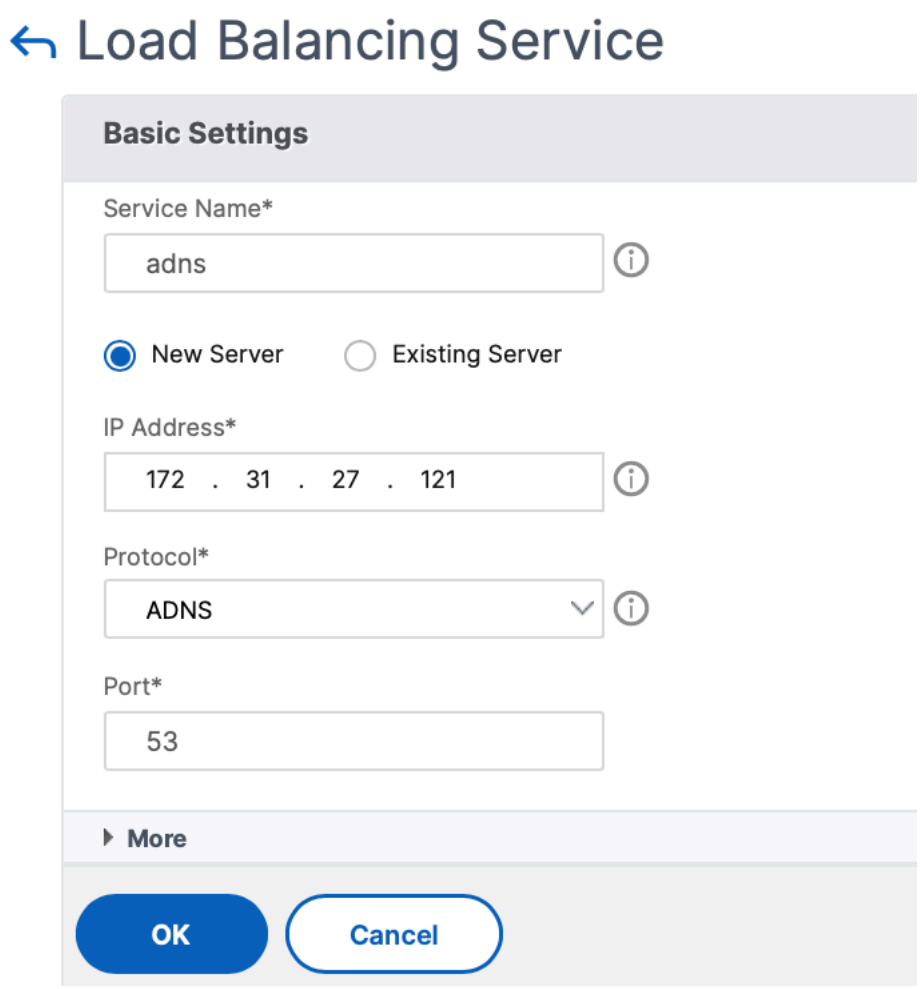


14. Configurez la liaison de domaine du serveur virtuel GSLB en cliquant sur **Aucune liaison de domaine du serveur virtuel GSLB**. Configurez le FQDN et liez. Conservez le réglage par défaut pour les autres paramètres.



15. Configurez le service ADNS en cliquant sur **Aucun service**.
16. Spécifiez les détails pour configurer le service d'équilibrage de charge.

    Ajoutez un **nom de service**, cliquez sur **Nouveau serveur** et entrez l'**adresse IP** du serveur ADNS. Si l'ADNS utilisateur est déjà configuré, les utilisateurs peuvent sélectionner le **serveur existant**, puis choisir l'ADNS utilisateur dans le menu déroulant. Assurez-vous que le protocole est ADNS et que le trafic est configuré pour passer par le port 53.



17. Configurez la **méthode** en tant que **connexion minimale** et la méthode de sauvegarde en tant que **Round Robin**.
18. Cliquez sur **Terminé** et vérifiez que le serveur virtuel GSLB de l'utilisateur est affiché comme étant actif.

Autres ressources

Équilibrage de charge global NetScaler pour les déploiements hybrides et multicloud

Configurer les pools d'adresses IP de l'intranet pour une appliance NetScaler Gateway

October 17, 2024

Dans certains cas, les utilisateurs qui se connectent à l'aide du plug-in NetScaler Gateway ont besoin d'une adresse IP unique pour un dispositif NetScaler Gateway. Lorsque vous activez des pools d'adresses (également appelés pool d'adresses IP) pour un groupe, l'appliance NetScaler Gateway peut attribuer un alias d'adresse IP unique à chaque utilisateur. Vous configurez des pools d'adresses à l'aide d'adresses IP intranet (IIP).

Vous pouvez configurer des pools d'adresses sur une appliance NetScaler Gateway déployée sur Azure en suivant cette procédure en deux étapes :

- Enregistrement des adresses IP privées utilisées dans le pool d'adresses, dans Azure
- Configuration des pools d'adresses dans l'appliance NetScaler Gateway

Enregistrer une adresse IP privée dans le portail Azure

Dans Azure, vous pouvez déployer une instance NetScaler VPX avec plusieurs adresses IP. Vous pouvez ajouter des adresses IP à une instance VPX de deux manières :

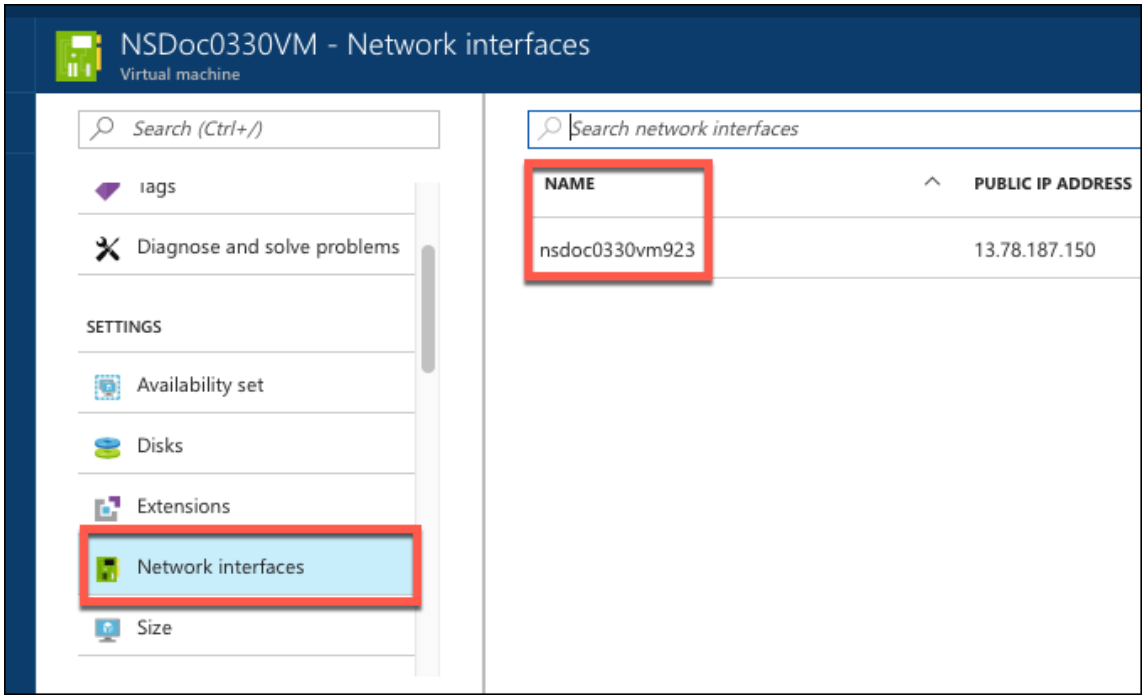
a. Lors du Provisioning d'une instance VPX

Pour plus d'informations sur la façon d'ajouter plusieurs adresses IP lors de la mise en service d'une instance VPX, consultez Configurer plusieurs adresses IP pour une instance autonome NetScaler. Pour ajouter des adresses IP à l'aide de commandes PowerShell lors de la mise en service d'une instance VPX, consultez Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome à l'aide des commandes PowerShell.

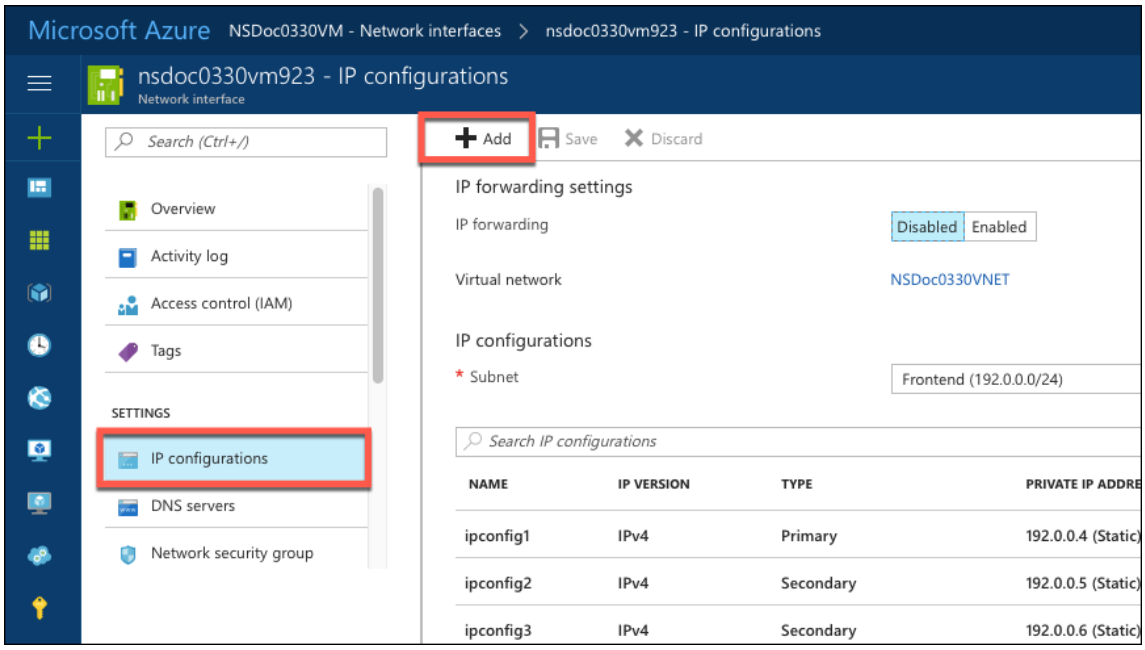
b. Après avoir Provisioning une instance VPX

Après avoir provisionné une instance VPX, procédez comme suit pour enregistrer une adresse IP privée sur le portail Azure, que vous configurez en tant que pool d'adresses dans l'appliance NetScaler Gateway.

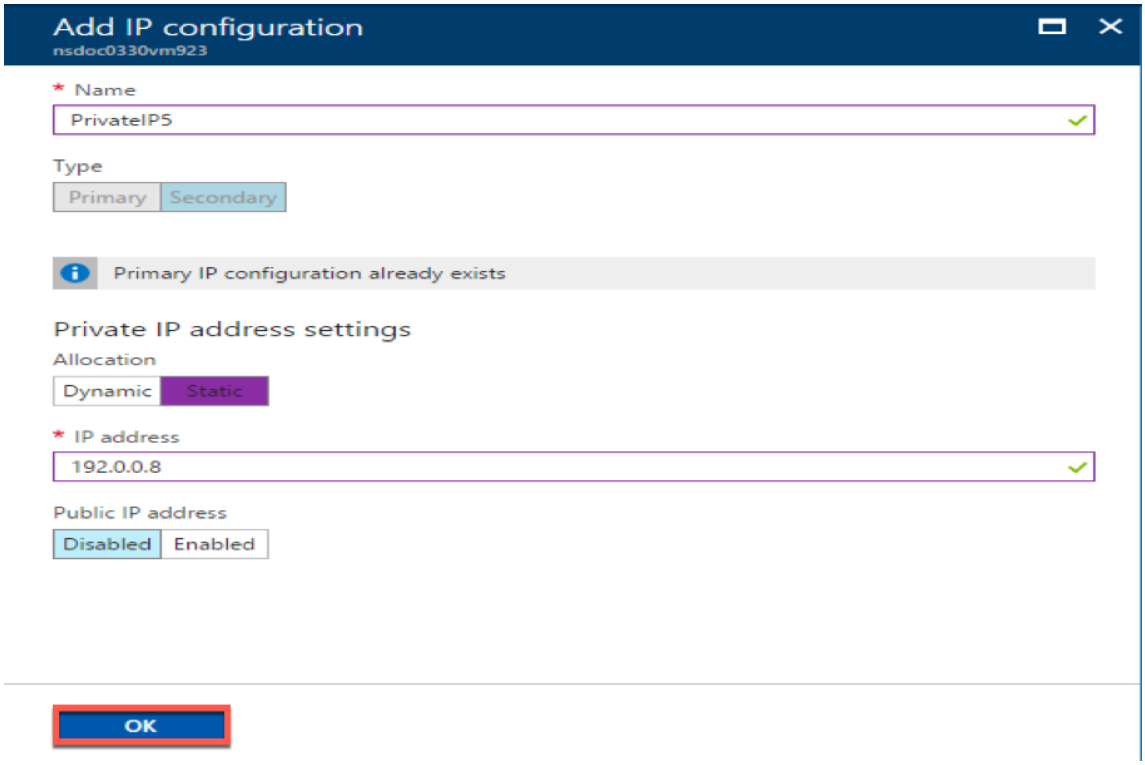
1. **Dans Azure Resource Manager (ARM), accédez à l'instance NetScaler VPX déjà créée > Interfaces réseau.** Choisissez l'interface réseau qui est liée à un sous-réseau auquel appartient l'IIP que vous souhaitez enregistrer. Choisissez l'interface réseau qui est liée à un sous-réseau auquel appartient l'IIP que vous souhaitez enregistrer.



2. Cliquez sur **Configurations IP**, puis sur **Ajouter**.



3. Fournissez les détails requis comme indiqué dans l'exemple ci-dessous et cliquez sur **OK**.



Configurer les pools d'adresses dans l'appliance NetScaler Gateway

Pour plus d'informations sur la configuration des pools d'adresses sur NetScaler Gateway, consultez Configuration des pools d'adresses.

> **Limitation :**
>
> Vous ne pouvez pas lier une plage d'adresses IIP aux utilisateurs. Chaque adresse IIP utilisée dans un pool d'adresses doit être enregistrée.

Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX à l'aide des commandes PowerShell

October 17, 2024

Dans un environnement Azure, une appliance virtuelle NetScaler VPX peut être déployée avec plusieurs cartes réseau. Chaque carte réseau peut comporter plusieurs adresses IP. Cette section explique comment déployer une instance NetScaler VPX avec une seule carte réseau et plusieurs adresses IP, à l'aide des commandes PowerShell. Vous pouvez utiliser le même script pour le déploiement multi-cartes réseau et multi-IP.

> **Remarque :**
>
> Dans ce document, IP-Config fait référence à une paire d'adresses IP, IP publique et IP privée, associées à une carte réseau individuelle. Pour plus d'informations, consultez la section Terminologie Azure .

Cas d'utilisation

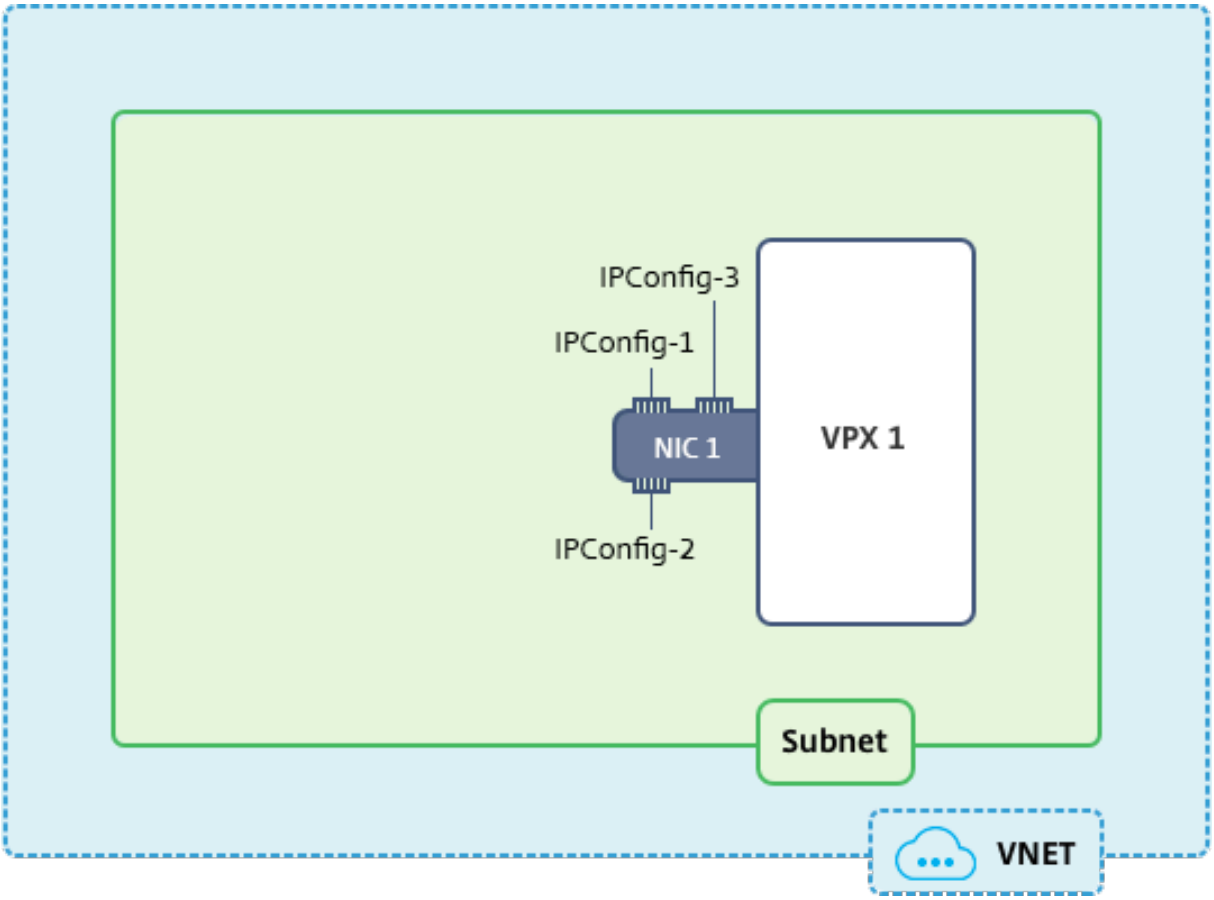
Dans ce cas d'utilisation, une seule carte réseau est connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP, comme indiqué dans le tableau suivant.

Configuration IP	Associé à
IPConfig-1	Adresse IP publique statique ; adresse IP privée statique
IPConfig-2	Adresse IP publique statique ; adresse privée statique
IPConfig-3	Adresse IP privée statique

> **Remarque :**
>
> IPConfig-3 n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque :**
>
> Dans un déploiement Azure NetScaler VPX multi-NIC et multi-IP, l'adresse IP privée associée à la principale (première) `IPConfig` de la (première) carte réseau principale est automatiquement ajoutée en tant qu'adresse NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, comme déterminé par vos besoins.

Voici le résumé des étapes requises pour configurer plusieurs adresses IP pour une appliance virtuelle NetScaler VPX en mode autonome :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un jeu de disponibilité
4. Créer un groupe de services réseau
5. Créer un réseau virtuel
6. Créer une adresse IP publique
7. Attribuer une configuration IP
8. Créer une carte réseau
9. Création d'une instance NetScaler VPX

10. Vérifier les configurations de carte réseau
11. Vérifier les configurations côté VPX

Script

Paramètres

Voici des exemples de paramètres pour le cas d'utilisation dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

$locName="westcentralus"

$rgname="Azure-MultiIP »

$nicName1="VM1-NIC1"

$VNetName="Azure-MultiIP-VNet »

$vNetAddressRange="11.6.0.0/16"

$FrontendSubnetName= « FrontendSubnet »

$frontEndSubnetRange="11.6.1.0/24"

$prmStorageAccountName="MultiIPStorage »

$avSetName="multiip-avSet"

$VMSize="Standard_DS4_v2"(Ce paramètre crée une machine virtuelle comportant jusqu'à quatre cartes réseau.)

Remarque : La configuration minimale requise pour une instance VPX est de 2 processeurs virtuels et de 2 Go de RAM.

$publisher = « Citrix »

$offer="netscalervpx110-6531"(Vous pouvez utiliser différentes offres.)

$sku="netscalerbyol » (Selon votre offre, le SKU peut être différent.)

$version="dernière »

$pubIPName1="PIP1"

$pubIPName2="PIP2"

$domName1="multiipvpx1"

$domName2="multiipvpx2"

$vmNamePrefix="VPXMultiIP »

$osDiskSuffix="osmultiipalbdiskdb1"

Informations relatives au groupe de sécurité réseau (NSG) :

$NSGName=”NSG-MultiIP »

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Créer un groupe de ressources

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Créer un compte de stockage

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Créer un ensemble de disponibilité

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
 $rgName -Location $locName
```

4. Créer un groupe de sécurité réseau

1. Ajoutez des règles. Vous devez ajouter une règle au groupe de sécurité réseau pour n’importe quel port desservant le trafic.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name
   -Description "Autoriser HTTP"-Accès Autorisé-Protocole Tcp -
   Direction Entrant -Priorité101 -SourceAddressPrefix Internet -
   SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange
    80  $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name
    -Description "Autoriser HTTPS"-Accès Autorisé-Protocole Tcp
   -Direction Entrant -Priorité110 -SourceAddressPrefix Internet -
   SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange
    443 $rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name
   ```



```
 -Description "Autoriser SSH"-Accès Autorisé-Protocole Tcp -
Direction Entrant -Priorité120 -SourceAddressPrefix Internet -
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange
 22
```

2. Créez un objet de groupe de sécurité réseau.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName
-Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
$rule3
```

5. Créer un réseau virtuel

1. Ajoutez des sous-réseaux.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$frontEndSubnetName -AddressPrefix $frontEndSubnetRange
```

2. Ajoutez un objet réseau virtuel.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
 $rgName -Location $locName -AddressPrefix $vNetAddressRange -
Subnet $frontendSubnet
```

3. Récupérez des sous-réseaux.

```
$subnetName="frontEndSubnet"   $subnet1=$vnet.Sous-réseaux|?{ $_.
Name -eq $subnetName }
```

6. Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Nom $pubIPName1 -Nom du groupe
 de ressources $rgName -Étiquette du nom de domaine $domName1 -
Emplacement $locName -Méthode d'allocation statique$pip2=New-AzureRmPublicIpAd
 -Nom $pubIPName2 -Nom du groupe de ressources $rgName -Étiquette du
nom de domaine $domName2 -Emplacement $locName -Méthode d'allocation
statique
```

> **Remarque :**
>
> Vérifiez la disponibilité des noms de domaine avant de les utiliser.
>
> La méthode d'allocation des adresses IP peut être dynamique ou statique.

7. Attribuer la configuration IP

Dans ce cas d'utilisation, tenez compte des points suivants avant d'attribuer des adresses IP :

- IPConfig-1 appartient au sous-net1 de VPX1.
- IPConfig-2 appartient au sous-réseau 1 du VPX1.
- IPConfig-3 appartient au sous-réseau 1 de VPX1.

> **Remarque :**
>
> Lorsque vous affectez plusieurs configurations IP à une carte réseau, une configuration doit être affectée comme principale.

```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress
    $pip1  – Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress
    $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Utilisez une adresse IP valide qui répond aux exigences de votre sous-réseau et vérifiez sa disponibilité.

8. Créer une carte réseau

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
 $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,
$IPConfig3 -NetworkSecurityGroupId $nsg.Id
```

9. Créer une instance NetScaler VPX

1. Initialisez les variables.

   ```
   $suffixNumber = 1 $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Créez un objet de configuration VM.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
   AvailabilitySetId $avSet.Id
   ```


3. Définissez les informations d'identification, le système d'exploitation et l'image.

```
$cred=Get-Credential -Message "Saisissez le nom et le mot de
passe pour la connexion àVPX."$vmConfig=Set-AzureRMVMOperatingSystem
 -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
$publisher -Offre $offer -SKU $sku -Version $version
```

4. Ajoutez une carte réseau.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
Id -Primary
```

> **Remarque :**
>
> Dans un déploiement NetScaler VPX multi-NIC, une carte réseau doit être principale. Ainsi, « -Primary » doit être ajouté lors de l'ajout de cette carte réseau à l'instance NetScaler VPX.

5. Spécifiez le disque du système d'exploitation et créez une machine virtuelle.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1$osVhdUri=$prmStorageAccount
.PrimaryEndpoints.Blob.ToString()+ "vhds/"+ $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Nom $osDiskName -
VhdUri $osVhdUri -CreateOption fromImage   Set-AzureRmVMPlan -VM
$vmConfig -Éditeur $publisher -Produit $offer -Nom $sku   Nouveau
-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. Vérifiez les configurations de la carte réseau

Une fois l'instance NetScaler VPX démarrée, vous pouvez vérifier les adresses IP allouées à `IPConfigs` de la carte réseau NetScaler VPX à l'aide de la commande suivante.

```
$nic.IPConfig
```

11. Vérifiez les configurations côté VPX

Lorsque l'instance NetScaler VPX démarre, une adresse IP privée associée à la carte réseau principale `IPconfig` est ajoutée en tant qu'adresse NSIP. Les adresses IP privées restantes doivent être ajoutées en tant qu'adresses VIP ou SNIP, selon vos besoins. Utilisez la commande suivante.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Vous avez maintenant configuré plusieurs adresses IP pour une instance NetScaler VPX en mode autonome.

Scripts PowerShell supplémentaires pour le déploiement Azure

October 17, 2024

Cette section fournit les applets de commande PowerShell avec lesquels vous pouvez effectuer les configurations suivantes dans Azure PowerShell :

- Provisionner une instance autonome NetScaler VPX
- Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure
- Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Consultez également les rubriques suivantes pour les configurations que vous pouvez effectuer à l'aide des commandes PowerShell :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configurer GSLB sur des instances NetScaler VPX
- Configurer GSLB sur une configuration haute disponibilité active de secours NetScaler
- Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome à l'aide des commandes PowerShell

Provisionner une instance autonome NetScaler VPX

1. **Créer un groupe de ressources**

   Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="&lt;resource group name&gt;"     $locName="&lt;location name, such as West US&gt; New-AzureRmResourceGroup -Nom $rgName -Emplacement $locName
   ```

   Par exemple :

   ```
   1   $rgName = "ARM-VPX"
   2   $locName = "West US"
   3   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```


2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   `$saName="<storage account name>"  $saType="<storage account type>"`, spécifiez-en une : `Standard_LRSStandard_GRS`, `Standard_RAGRS`, ou `Premium_LRS` `Nouveau-AzureRmStorageAccount -Nom $saName -ResourceGroupName $rgName -Type $saType -Emplacement $locName`

   Par exemple :

   ```
   $saName="vpxstorage"
   $saType="Standard\_LRS"
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
       $rgName -Type $saType -Location $locName
   ```

3. **Créer un jeu de disponibilité**

   Le jeu de disponibilité permet de garder vos machines virtuelles disponibles pendant les temps d'arrêt, par exemple pendant la maintenance. Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
   $rgName -Location $locName
   ```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"  $BackendAddressPrefix="
   10.0.2.0/24"  $vnetAddressPrefix="10.0.0.0/16"  $frontendSubnet
   =New-AzureRmVirtualNetworkSubnetConfig -Nom frontendSubnet
   -Préfixe d'adresse $FrontendAddressPrefix  $backendSubnet=New-
   AzureRmVirtualNetworkSubnetConfig -Nom backendSubnet -AddressPrefix
    $BackendAddressPrefix  New-AzureRmVirtualNetwork -Nom TestNet
    -ResourceGroupName $rgName -Emplacement $locName -Préfixe d'
   adresse $vnetAddressPrefix -Sous-réseau $frontendSubnet,$backendSubnet
   ```

   Par exemple :

   ```
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix

   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       backendSubnet -AddressPrefix $BackendAddressPrefix
   ```



```
4
5    New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName
        $rgName -Location $locName -AddressPrefix $vnetAddressPrefix
        -Subnet $frontendSubnet,$backendSubnet
```

5. **Créer une carte réseau**

   Créez une carte réseau et associez-la à l'instance NetScaler VPX. Le sous-réseau frontal créé dans la procédure ci-dessus est indexé à 0 et le sous-réseau arrière est indexé à 1. Créez maintenant une carte réseau de l'une des trois façons suivantes :

   a) *Carte réseau avec adresse IP publique*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
    $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
    $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
   ].Id -PublicIpAddressId $pip.Id
   ```

   b) *Carte réseau avec étiquette IP publique et DNS*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
    $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
    Dynamic
   ```

   Avant d'assigner $domName, vérifiez qu'il est disponible ou non en utilisant la commande :

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -
   Location $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
    $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
   ].Id -PublicIpAddressId $pip.Id
   ```

   Par exemple :

   ```
   1    $nicName="frontendNIC"
   2
   3    $domName="vpxazure"
   4
   5    $pip = New-AzureRmPublicIpAddress -Name $nicName -
           ResourceGroupName $rgName -DomainNameLabel $domName -Location
            $locName -AllocationMethod Dynamic
   6
   ```



```
7    $nic = New-AzureRmNetworkInterface -Name $nicName -
        ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
        Subnets\[0\].Id -PublicIpAddressId $pip.Id
```

c) *Carte réseau avec adresse publique dynamique et adresse IP privée statique*

Assurez-vous que l'adresse IP privée (statique) que vous ajoutez à la machine virtuelle doit correspondre à celle du sous-réseau spécifié.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
 $rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
 $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
].Id -PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Créer un objet virtuel**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
 $rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. **Obtenir l'image NetScaler VPX**

```
$pubName="<Image publisher name>"

$offerName="<Image offer name>"

$skuName="<Image SKU name>"

$cred=Get-Credential -Message "Type the name and password of the
local administrator account."
```

Fournissez vos informations d'identification utilisées pour vous connecter à VPX

```
$vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName
$vmName -Credential $cred -Verbose

$vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -
Offer $offerName -Skus $skuName -Version "latest"

$vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
```


Par exemple :

```
$pubName="citrix"
```

La commande suivante est utilisée pour afficher toutes les offres de Citrix :

```
Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
    Select Offer

$offerName="netscalervpx110-6531"
```

La commande suivante permet de connaître le SKU proposé par l'éditeur pour un nom d'offre spécifique :

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -
Offer $offerName | Select Skus
```

8. **Créer une machine virtuelle**

```
$diskName="<name identifier for the disk in Azure storage, such
as OSDisk>"
```

Par exemple :

```
$diskName="dynamic"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName

$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/
   " + $diskName  + ".vhd"

$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri
   $osDiskUri -CreateOption fromImage
```

Lorsque vous créez une machine virtuelle à partir d'images présentes sur le site de vente, utilisez la commande suivante pour spécifier le plan de machine virtuelle :

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName
 -Name $skuName
```

```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
$vm
```


Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure

Connectez-vous à AzureRMAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Créer un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes utilisées pour créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="<resource group name>"

   $locName="<location name, such as West US>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   1   $rgName = "ARM-LB-NS"
   2
   3   $locName = "West US"
   4
   5   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   ```
   $saName="<storage account name>"

   $saType="&lt;storage account type&gt;"
   ```

   , spécifiez-en une : `Standard_LRS` `Standard_GRS`, `Standard_RAGRS`, ou `Premium_LRS`

   ```
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
   $rgName -Type $saType -Location $locName
   ```

   Par exemple :

   ```
   1   $saName="vpxstorage"
   2
   3   $saType="Standard_LRS"
   4
   5   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
           $rgName -Type $saType -Location $locName
   ```

3. **Créer un jeu de disponibilité**

   Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.


```
$avName="<availability set name>"

New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

```
1   $vnetName = "LBVnet"
2
3   $FrontendAddressPrefix="10.0.1.0/24"
4
5   $BackendAddressPrefix="10.0.2.0/24"
6
7   $vnetAddressPrefix="10.0.0.0/16"
8
9   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        frontendSubnet -AddressPrefix $FrontendAddressPrefix
10
11  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        backendSubnet -AddressPrefix $BackendAddressPrefix
12
13  $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
        ResourceGroupName $rgName -Location $locName -AddressPrefix
        $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet
```

   > **Remarque :**
   >
   > Choisissez la valeur du paramètre AddressPrefix selon vos besoins.

   Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

   Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

   Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Configurer l'adresse IP frontale et créer un pool d'adresses back-end**

   Configurez une adresse IP frontale pour le trafic réseau d'équilibrage de charge entrant et créez un pool d'adresses back-end pour recevoir le trafic équilibré de charge.

```
1   $pubName="PublicIp1"
2
3   $publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
        ResourceGroupName $rgName -Location $locName -
        AllocationMethod Static -DomainNameLabel nsvpx
```


Remarque :

Vérifiez la disponibilité de la valeur pour DomainNameLabel.

```
$FIPName = "ELBFIP"

$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -
    Name $FIPName -PublicIpAddress $publicIP1

$BEPool = "LB-backend-Pool"

$beaddresspool1= New-
    AzureRmLoadBalancerBackendAddressPoolConfig -Name
    $BEPool
```

6. **Créer une sonde de santé**

   Créez une sonde de santé TCP avec le port 9000 et l'intervalle 5 secondes.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
```

7. **Créer une règle d'équilibrage de charge**

   Créez une règle de LB pour chaque service que vous répartirez la charge.

   Par exemple :

   Vous pouvez utiliser l'exemple suivant pour équilibrer la charge service HTTP.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -
    FrontendPort 80 -BackendPort 80
```

8. **Créer des règles NAT entrantes**

   Créez des règles NAT pour les services dont vous n'êtes pas l'équilibrage de charge.

   Par exemple, lors de la création d'un accès SSH à une instance NetScaler VPX.

   Remarque :

   Le triplet Protocol-FrontEndPort-BackendPort ne doit pas être le même pour deux règles NAT.

```
$inboundNATRule1= New-
    AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1
        -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-
```



```
AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 -
FrontendIpConfiguration $frontendIP1 -Protocol TCP -
FrontendPort 10022 -BackendPort 22
```

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles d'équilibrage de charge, configurations de sonde) ensemble.

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -
    Name $lbName -Location $locName -InboundNatRule
    $inboundNATRule1, $inboundNATRule2 -FrontendIpConfiguration
    $frontendIP1 -LoadBalancingRule $lbrule1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe
```

10. **Créer une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance VPX

    a) NIC1 avec VPX1

    Par exemple :

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

\* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

\* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic1=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools\[$bePoolIndex\] -
    LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
    \]
```

    b) NIC2 avec VPX2

    Par exemple :


```
$nicName="NIC2"

$lbName="ELB"

$bePoolIndex=0

$natRuleIndex=1

\* Second Inbound NAT (SSH) rule we need to use

`$subnetIndex=0

\* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic2=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools\[$bePoolIndex\] -
    LoadBalancerInboundNatRule  $lb.InboundNatRules\[
    $natRuleIndex\]
```

11. **Création d'instances NetScaler VPX**

    Créez deux instances NetScaler VPX faisant partie du même groupe de ressources et du même ensemble de disponibilité, puis associez-les à l'équilibreur de charge externe.

    a) Instance 1 de NetScaler VPX

    Par exemple :

```
$vmName="VPX1"

$vmSize="Standard\_A3"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
```



```
        $vmName -Credential $cred -Verbose
18
19  $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
20
21  $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id
22
23  $diskName="dynamic"
24
25  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
26
27  $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds1/" + $diskName  + ".vhd"
28
29  $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
30
31  Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
        $offerName -Name $skuName
32
33  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm1
```

b) Instance 2 de NetScaler VPX

Par exemple :

```
1   $vmName="VPX2"
2
3   $vmSize="Standard\_A3"
4
5   $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
7   $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
8
9   $cred=Get-Credential -Message " Type Credentials which will be
        used to login to VPX instance "
10
11  $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
        $vmName -Credential $cred -Verbose
12
13  $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15  $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17  $diskName="dynamic"
18
19  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
20
```



```
$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds2/" + $diskName  + ".vhd"

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
    $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
```

12. **Configurer les machines virtuelles**

    Lorsque les deux instances NetScaler VPX démarrent, connectez-vous aux deux instances NetScaler VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des deux instances de NetScaler VPX.

    b) Actif-Passif : exécutez cette commande sur la ligne de commande des deux instances NetScaler VPX.

    ```
    add ha node #nodeID <nsip of other NetScaler VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Connectez-vous à AzureRMAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Créer un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="\\&#060;resource group name\\&#062;"

   $locName="\\&#060;location name, such as West US\\&#062;"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   ```



```
5    New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres et des chiffres minuscules.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, spécifiez-en une : `Standard_LRS` `Standard_GRS`, `Standard_RAGRS`, ou `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Par exemple :

```
1    $saName="vpxstorage"
2
3    $saType="Standard_LRS"
4
5    New-AzureRmStorageAccount -Name $saName -ResourceGroupName
        $rgName -Type $saType -Location $locName
```

3. **Créer un jeu de disponibilité**

   Un équilibreur de charge configuré avec un jeu de disponibilité garantit que votre application est toujours disponible.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

```
1    $vnetName = "LBVnet"
2
3    $vnetAddressPrefix="10.0.0.0/16"
4
5    $FrontendAddressPrefix="10.0.1.0/24"
6
7    $BackendAddressPrefix="10.0.2.0/24"
8
9    $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
        ResourceGroupName $rgName -Location $locName -AddressPrefix
        $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet\`
10
11   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
        frontendSubnet -AddressPrefix $FrontendAddressPrefix
```



```
12
13    $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
          backendSubnet -AddressPrefix $BackendAddressPrefix
```

> **Remarque :**
>
> Choisissez la valeur du paramètre AddressPrefix selon vos besoins.

Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Créer un pool d'adresses backend**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -
Name "LB-backend"
```

6. **Créer des règles NAT**

Créez des règles NAT pour les services dont vous n'êtes pas l'équilibrage de charge.

```
1    $inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
         Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
         Protocol TCP -FrontendPort 3441 -BackendPort 3389
2
3    $inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
         Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol
         TCP -FrontendPort 3442 -BackendPort 3389
```

Utilisez les ports frontaux et back-end selon vos besoins.

7. **Créer une sonde de santé**

Créez une sonde de santé TCP avec le port 9000 et l'intervalle 5 secondes.

```
1    $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
         HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5
          -ProbeCount 2
```

8. **Créer une règle d'équilibrage de charge**

Créez une règle de LB pour chaque service que vous répartirez la charge.

Par exemple :

Vous pouvez utiliser l'exemple suivant pour équilibrer la charge service HTTP.


```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -
    FrontendPort 80 -BackendPort 80
```

Utilisez les ports frontaux et back-end selon vos besoins.

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles d'équilibrage de charge, configurations de sonde) ensemble.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -
    Name "InternalLB" -Location $locName -FrontendIpConfiguration
     $frontendIP -InboundNatRule $inboundNATRule1,
    $inboundNatRule2 -LoadBalancingRule $lbrule -
    BackendAddressPool $beAddressPool -Probe $healthProbe
```

10. **Créer une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance NetScaler VPX

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
     10.0.2.6 -Subnet $backendSubnet -
    LoadBalancerBackendAddressPool $nrplb.BackendAddressPools
    \[0\] -LoadBalancerInboundNatRule $nrplb.InboundNatRules\[0\]
```

Cette carte réseau est destinée à NetScaler VPX 1. L'IP privée doit se trouver dans le même sous-réseau que celui du sous-réseau ajouté.

```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
     10.0.2.7 -Subnet $backendSubnet -
    LoadBalancerBackendAddressPool $nrplb.BackendAddressPools
    \[0\] -LoadBalancerInboundNatRule $nrplb.InboundNatRules
    \[1\].
```

Cette carte réseau est destinée à NetScaler VPX 2. Le paramètre `Private IPAddress` peut avoir n'importe quelle adresse IP privée selon vos besoins.

11. **Création d'instances NetScaler VPX**

    Créez deux instances VPX faisant partie du même groupe de ressources et du même jeu de disponibilité, puis attachez-les à l'équilibreur de charge interne.

    a) Instance 1 de NetScaler VPX

    Par exemple :

```
$vmName="VPX1"

```



```
$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
     -Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds1/" + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
    $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
```

b) Instance 2 de NetScaler VPX

Par exemple :

```
$vmName="VPX2"

$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
```



```
        $vmName -Credential $cred -Verbose
12
13  $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15  $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
17  $diskName="dynamic"
18
19  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
20
21  $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName  + ".vhd"
22
23  $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25  Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
        $offerName -Name $skuName
26
27  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm2
```

12. **Configurer les machines virtuelles**

    Lorsque les deux instances NetScaler VPX démarrent, connectez-vous aux deux instances NetScaler VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des deux instances de NetScaler VPX.

    b) Actif-Passif : exécutez cette commande sur la ligne de commande des deux instances NetScaler VPX.

    ```
    add ha node #nodeID <nsip of other NetScaler VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

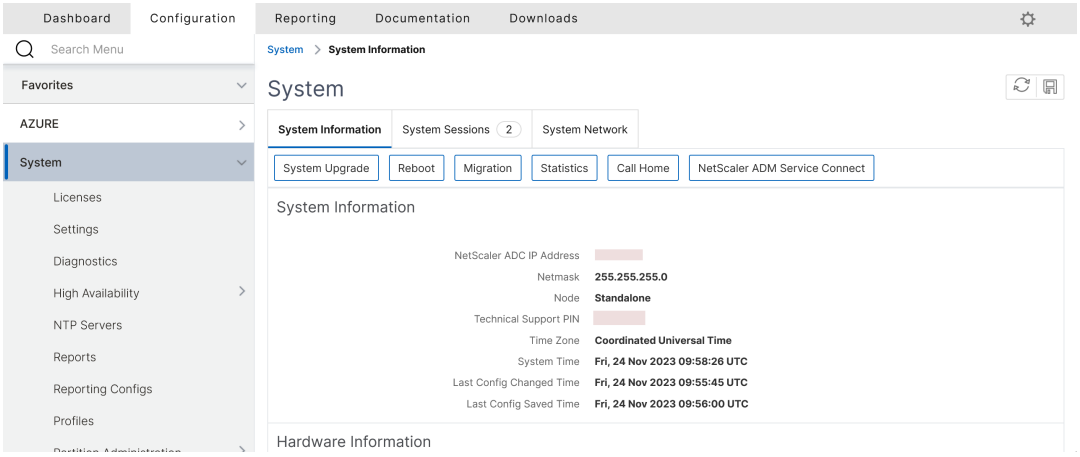
Create a support ticket for the VPX instance on Azure

April 23, 2024

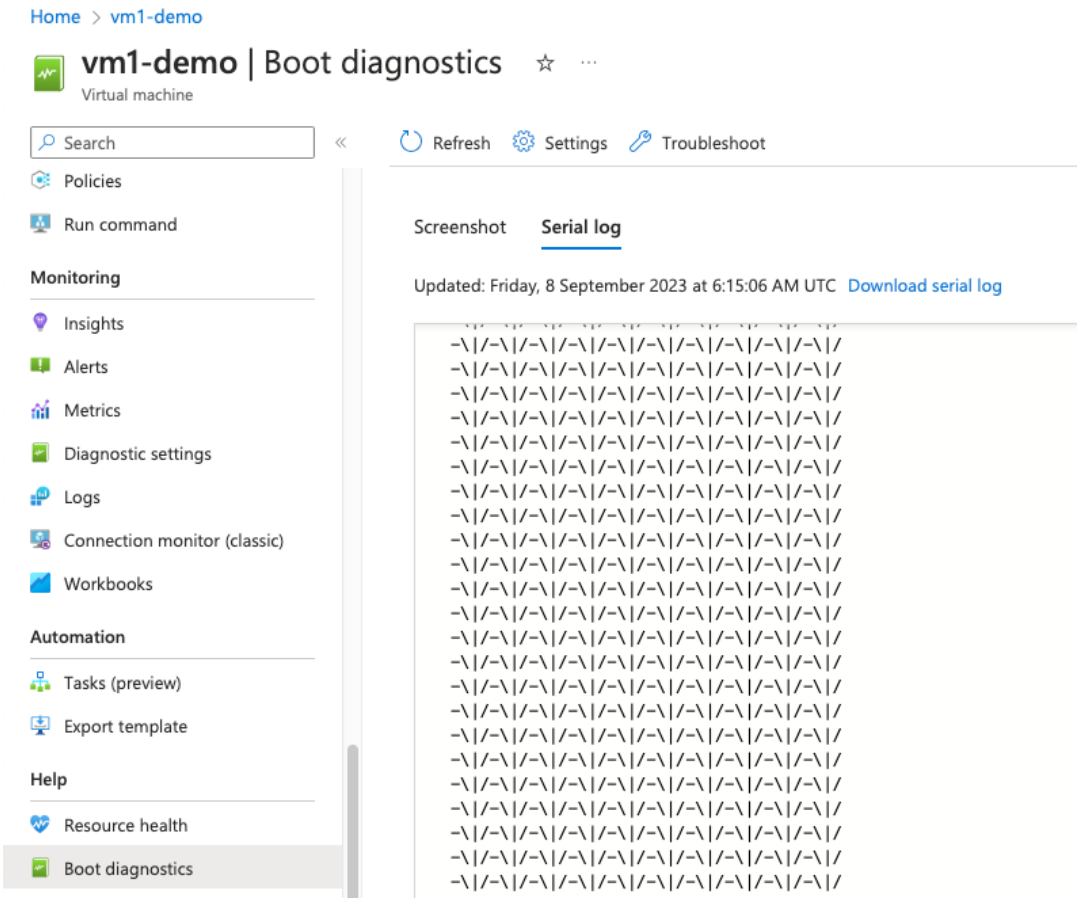
If you're experiencing issues with your NetScaler VPX instance on Azure, for troubleshooting, you can create a support ticket in the NetScaler support portal.

To file a support ticket, make sure the following:

- Your network is connected.
- You have your Azure account number, the support PIN code of the NetScaler subscription-based offering that you have deployed on Azure, and the Azure serial log handy.
  - You can find the support PIN code on the **Systems page** in the VPX GUI.



  - You can find the serial log in the Azure portal (**Boot diagnostics** section of your VM).



> **Note:**
>
> NetScaler supports subscription-based offerings on Azure (subscription license with hourly price).

Once you have all the information ready, call NetScaler support. You're asked to provide your name and email address.

FAQ Azure

October 17, 2024

- **La procédure de mise à niveau de l'instance NetScaler VPX installée depuis Azure Marketplace est-elle différente de la procédure de mise à niveau locale ?**

  Oui. Vous pouvez mettre à niveau votre instance NetScaler VPX dans le cloud Microsoft Azure vers NetScaler VPX version 11.1 ou ultérieure, à l'aide des procédures de mise à niveau standard de NetScaler VPX. Vous pouvez effectuer la mise à niveau à l'aide de procédures GUI ou CLI. Pour toute nouvelle installation, utilisez l'image NetScaler VPX pour le cloud Microsoft Azure.

  Pour télécharger les versions de mise à niveau de NetScaler VPX, accédez à **Téléchargements de NetScaler** > **Microprogramme NetScaler**.

- **Comment corriger les mouvements MAC et les désactivations d'interface observées sur les instances NetScaler VPX hébergées sur Azure ?**

  Dans un environnement Azure Multi-NIC, par défaut, toutes les interfaces de données peuvent afficher des mouvements MAC et des muettes d'interface. Pour éviter les déplacements du MAC et les désactivations d'interface dans les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de l'instance NetScaler VPX et de lier l'adresse IP principale de la carte réseau dans Azure.

  Pour plus d'informations, consultez l'article CTX224626 .

Déployer une instance NetScaler VPX sur Google Cloud Platform

October 17, 2024

Vous pouvez déployer une instance NetScaler VPX sur Google Cloud Platform (GCP). Une instance VPX dans GCP vous permet de tirer parti des fonctionnalités de cloud computing GCP et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix pour vos besoins professionnels. Vous

pouvez déployer des instances VPX dans GCP en tant qu'instances autonomes. Les configurations à carte réseau unique et à plusieurs cartes réseau sont prises en charge.

Fonctionnalités prises en charge

Toutes les fonctionnalités Premium, Advanced et Standard sont prises en charge sur le GCP en fonction de la licence/du type de version utilisé.

Limitation

- IPv6 n'est pas pris en charge.

Configuration matérielle requise

L'instance VPX dans GCP doit avoir au moins 2 vCPU et 4 Go de RAM.

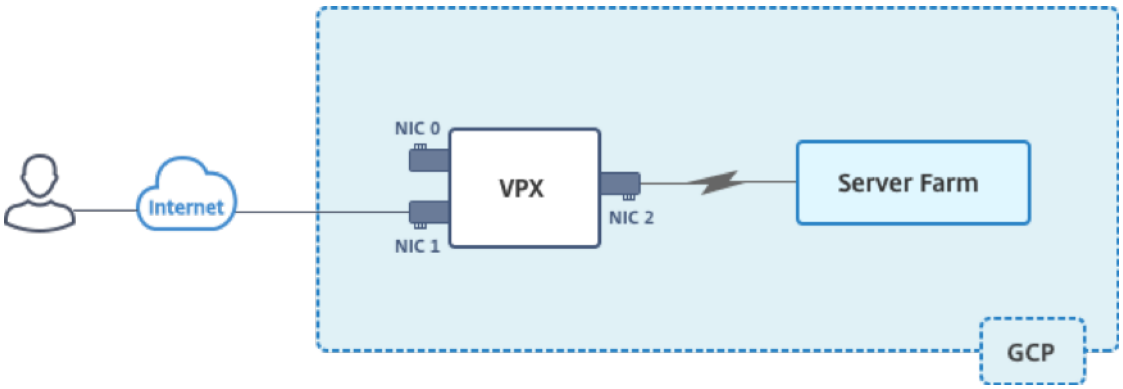
Points à noter

Prenez en compte les points spécifiques au GCP suivants avant de commencer votre déploiement.

- Après avoir créé l'instance, vous ne pouvez ni ajouter ni supprimer d'interfaces réseau.
- Pour un déploiement multi-cartes réseau, créez des réseaux VPC distincts pour chaque carte réseau. Une carte réseau ne peut être associée qu'à un seul réseau.
- Pour une instance à carte réseau unique, la console GCP crée un réseau par défaut.
- Au moins 4 vCPU sont requis pour une instance avec plus de deux interfaces réseau.
- Si le transfert IP est requis, vous devez activer le transfert IP lors de la création de l'instance et de la configuration de la carte réseau.

Scénario : déployer une instance NetScaler VPX autonome multi-NIC et multi-IP

Ce scénario montre comment déployer une instance autonome NetScaler VPX dans GCP. Dans ce scénario, vous créez une instance VPX autonome avec de nombreuses cartes réseau. L'instance communique avec les serveurs principaux (la batterie de serveurs).



Créez trois cartes réseau pour atteindre les objectifs suivants.

Carte d'interface réseau	Motif	Associé au réseau VPC
NIC 0	Trafic de gestion des serveurs (NetScaler IP)	Réseau de gestion
NIC 1	Sert le trafic côté client (VIP)	Réseau client
NIC 2	Communication avec les serveurs back-end (SNIP)	Réseau de serveurs dorsaux

Configurez les routes de communication requises entre les éléments suivants :

- Instance NetScaler VPX et les serveurs back-end.
- Instance NetScaler VPX et les hôtes externes sur l'Internet public.

Résumé des étapes de déploiement

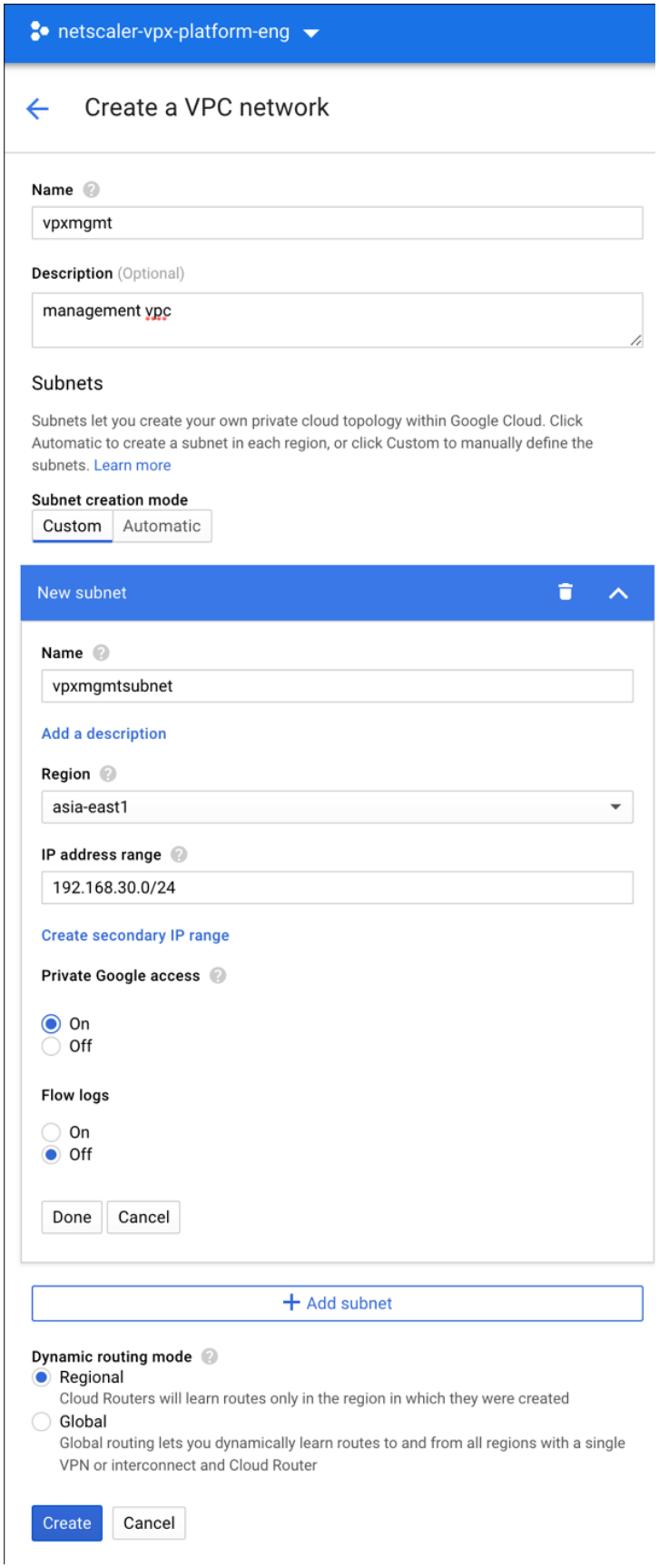
1. Créez trois réseaux VPC pour trois cartes réseau différentes.
2. Créez des règles de pare-feu pour les ports 22, 80 et 443.
3. Créez une instance avec trois cartes réseau.

Sélectionnez l'instance NetScaler VPX sur GCP Marketplace.

> **Remarque :**
>
> Créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez des réseaux VPC.

Créez trois réseaux VPC associés à la carte réseau de gestion, à la carte réseau cliente et à la carte réseau de serveur. Pour créer un réseau VPC, connectez-vous à **la console Google > Réseau > Réseau VPC > Créer un réseau VPC**. Renseignez les champs obligatoires, comme indiqué dans la capture d'écran, puis cliquez sur **Créer**.

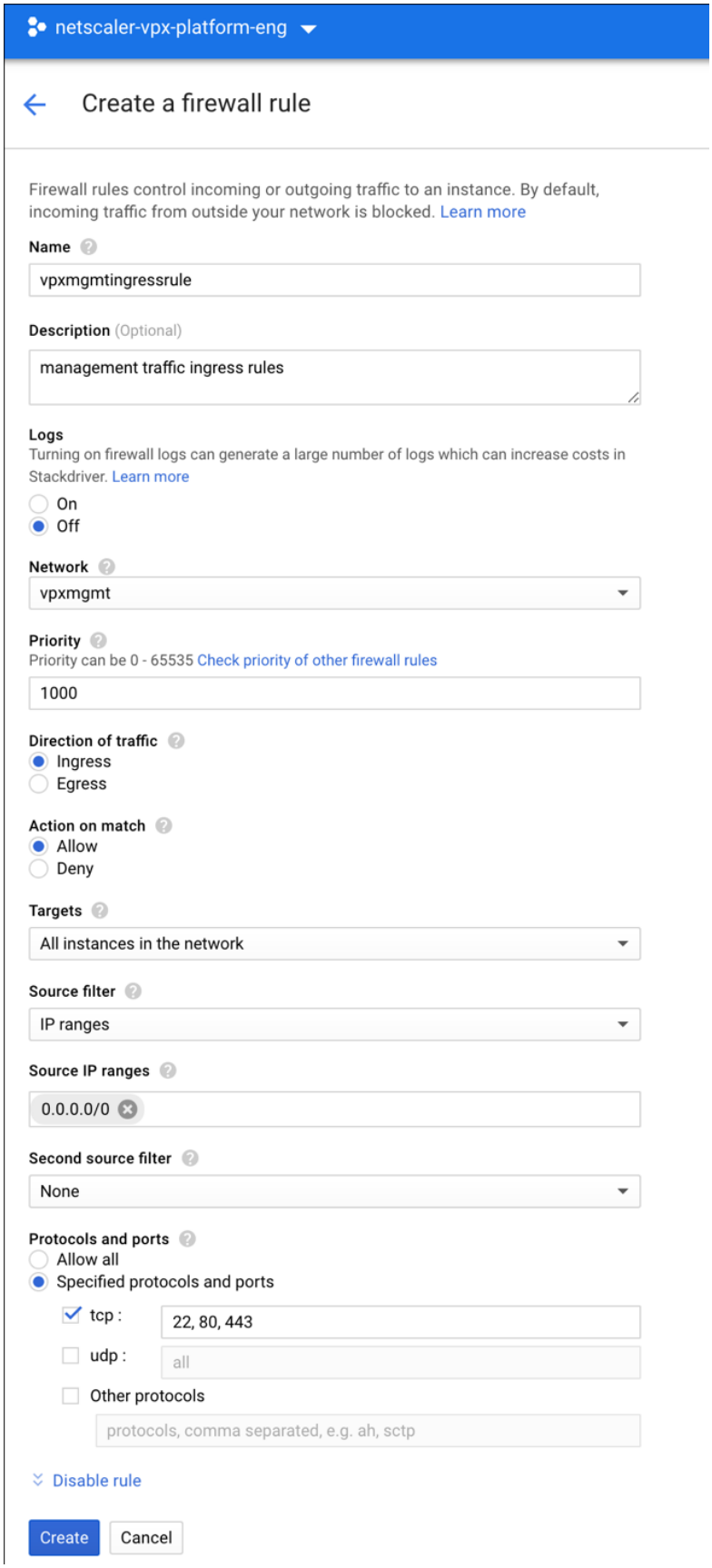


De même, créez des réseaux VPC pour les cartes réseau côté client et côté serveur.

> **Remarque :**
>
> Les trois réseaux VPC doivent se trouver dans la même région, à savoir asia-east1 dans ce scénario.

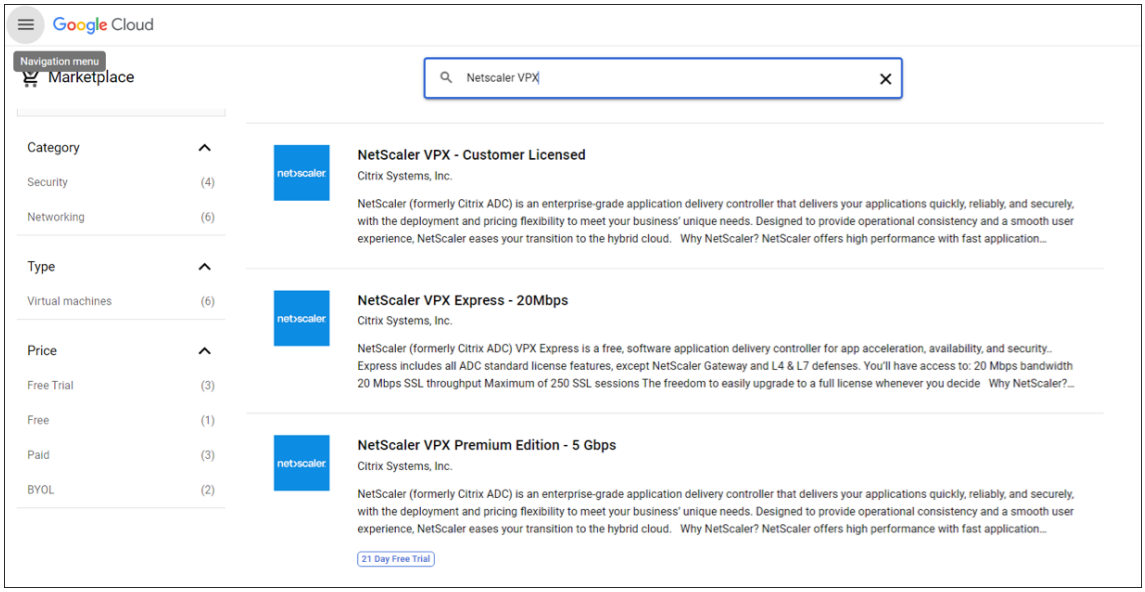
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour chaque réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d'ensemble des règles de pare-feu.

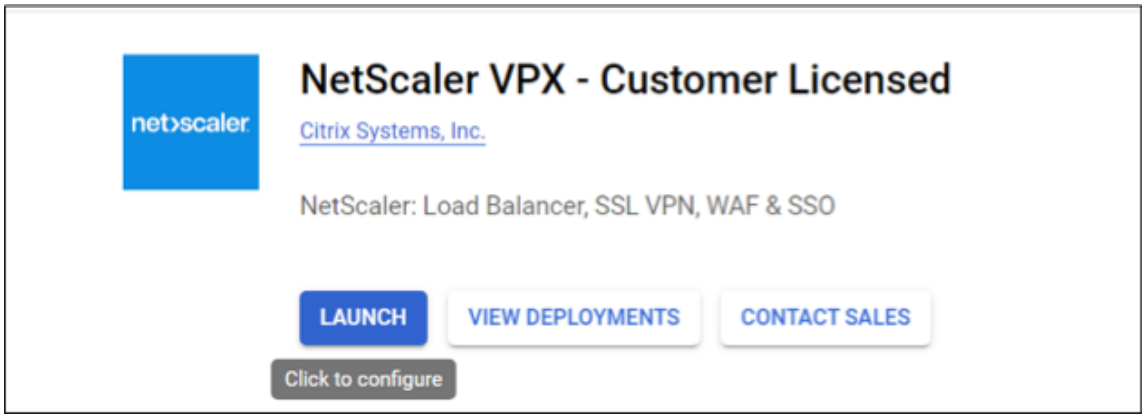


Étape 3. Créez l'instance VPX.

1. Ouvrez une session sur la console GCP.
2. Accédez à GCP Marketplace.
3. Sélectionnez un abonnement en fonction de vos besoins.



4. Cliquez sur **Lancer** sur l'abonnement sélectionné.



5. Remplissez le formulaire de déploiement et cliquez sur **Déployer**.

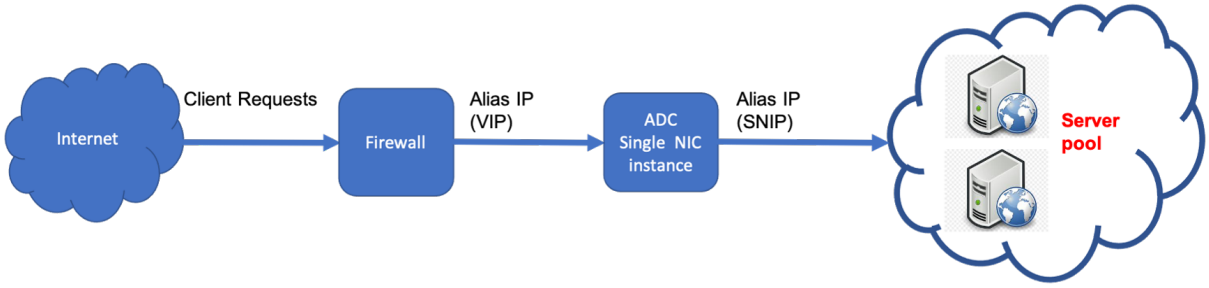
> **Remarque :**
>
> Utilisez les réseaux VPC créés à l'étape 1 **.

6. L'instance déployée apparaît sous **Compute Engine > Instances de machines virtuelles**.

   Utilisez le SSH GCP ou la console série pour configurer et gérer l'instance VPX.

Scénario : Déployer une instance VPX autonome à une seule carte réseau

Ce scénario montre comment déployer une instance autonome NetScaler VPX avec une seule carte réseau dans GCP. Les adresses IP d'alias sont utilisées pour réaliser ce déploiement.



Créez une carte réseau unique (NIC0) pour répondre aux objectifs suivants :

- Gérez le trafic de gestion (NetScaler IP) dans le réseau de gestion.
- Gérez le trafic côté client (VIP) dans le réseau client.
- Communiquez avec les serveurs principaux (SNIP) du réseau de serveurs principaux.

Configurez les routes de communication requises entre les éléments suivants :

- L'instance et les serveurs principaux.
- Instance et les hôtes externes sur l'Internet public.

Résumé des étapes de déploiement

1. Créez un réseau VPC pour NIC0.
2. Créez des règles de pare-feu pour les ports 22, 80 et 443.
3. Créez une instance avec une seule carte réseau.
4. Ajoutez des adresses IP d'alias à VPX.
5. Ajoutez VIP et SNIP sur VPX.
6. Ajoutez un serveur virtuel d'équilibrage de charge.
7. Ajoutez un service ou un groupe de services sur l'instance.
8. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur l'instance.

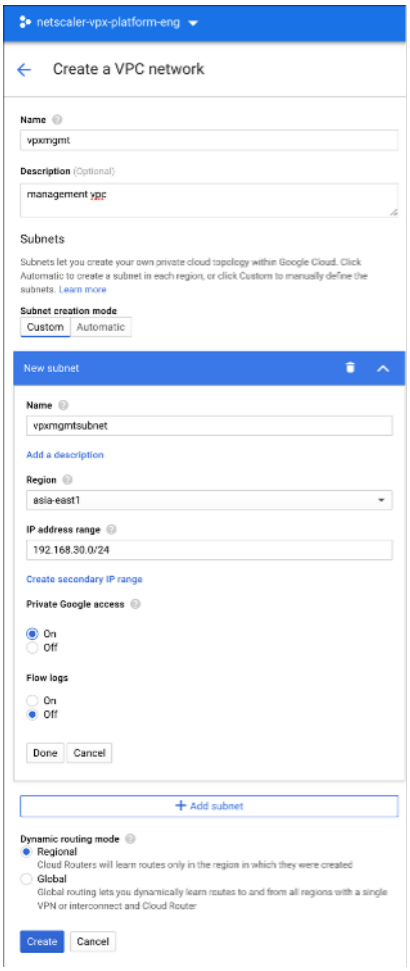
> **Remarque :**
>
> Créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez un réseau VPC.

Créez un réseau VPC à associer à NIC0.

Pour créer un réseau VPC, procédez comme suit :

1. Ouvrez une session sur **la console GCP > Mise en réseau > Réseau VPC > Créer un réseau VPC**
2. Remplissez les champs requis, puis cliquez sur **Créer**.



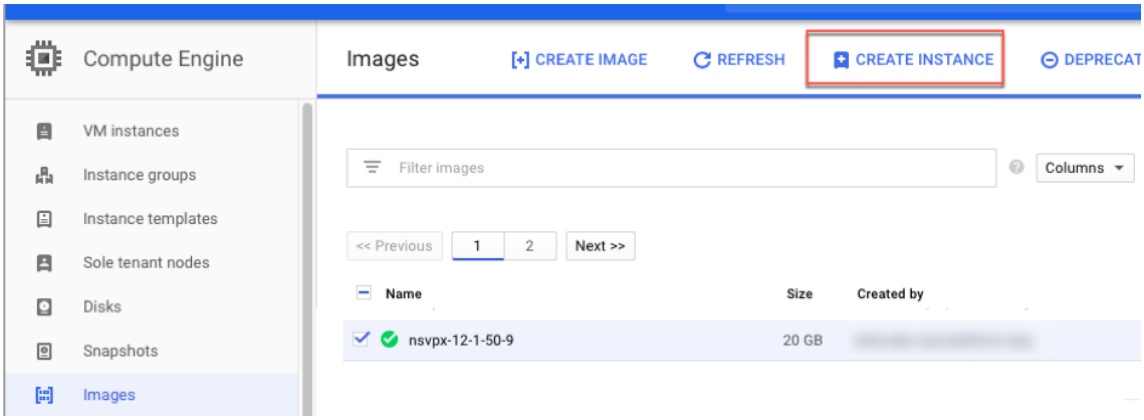
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour le réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d'ensemble des règles de pare-feu.

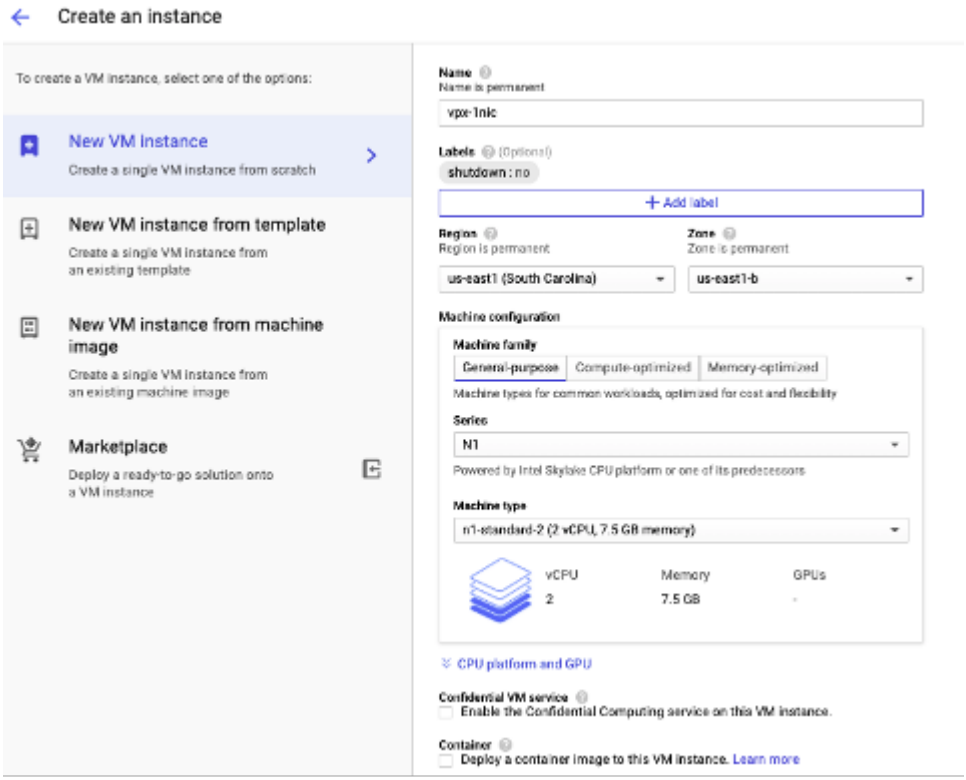
Étape 3. Créez une instance avec une seule carte réseau.

Pour créer une instance avec une seule carte réseau, procédez comme suit :

1. Ouvrez une session sur la **console GCP**.
2. Sous **Compute**, passez la souris sur **Compute Engine**et sélectionnez **Images**.
3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.



4. Sélectionnez un type d'instance avec deux vCPU (configuration minimale pour l'ADC).



5. Cliquez sur l'onglet **Mise en réseau** dans la fenêtre **Gestion, sécurité, disques, mise en réseau** .
6. Sous **Interfaces réseau**, cliquez sur l'icône **Modifier** pour modifier la carte réseau par défaut.
7. Dans la fenêtre **Interfaces réseau**, sous **Réseau**, sélectionnez le réseau VPC que vous avez créé.
8. Vous pouvez créer une adresse IP externe statique. Sous **Adresses IP externes**, cliquez sur **Créer une adresse IP**.
9. Dans la fenêtre **Réserver une adresse statique**, ajoutez un nom et une description, puis cliquez sur **Réserver**.
10. Cliquez sur **Créer** pour créer l'instance VPX. La nouvelle instance s'affiche sous Instances de machines virtuelles.

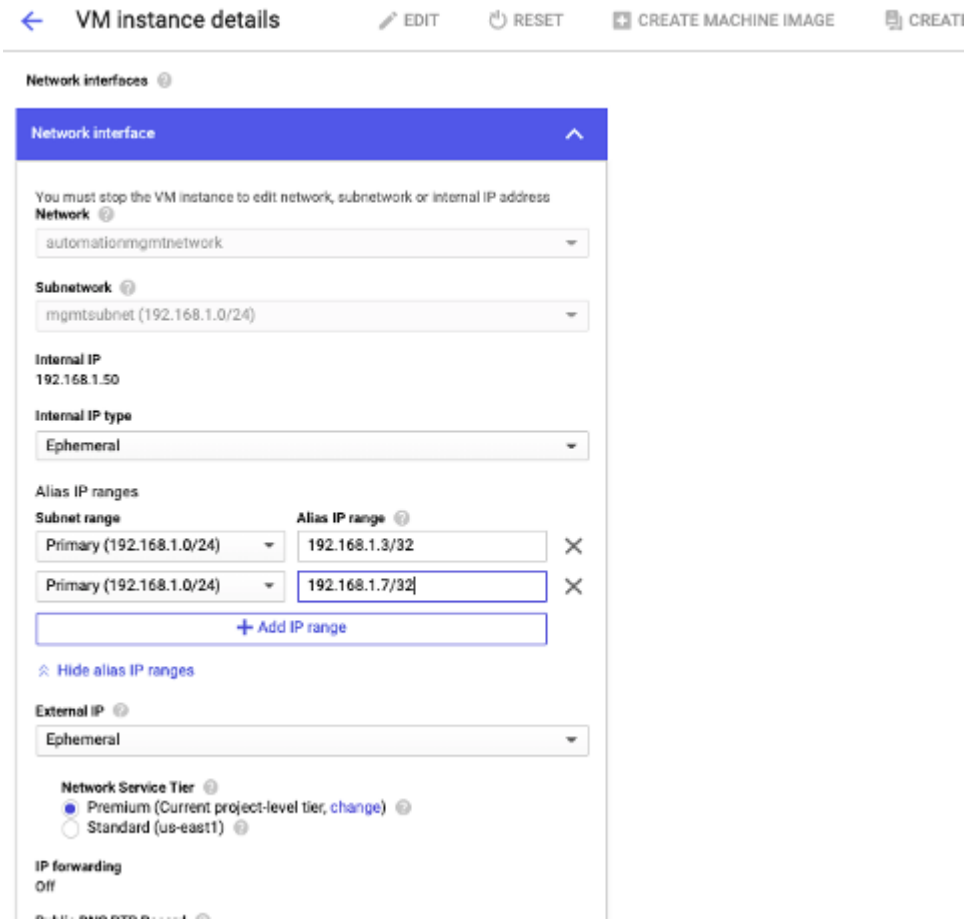
Étape 4. Ajoutez des adresses IP d'alias à l'instance VPX.

Affectez deux adresses IP d'alias à l'instance VPX à utiliser comme adresses VIP et SNIP.

> **Remarque :**
>
> N'utilisez pas l'adresse IP interne principale de l'instance VPX pour configurer l'adresse IP virtuelle ou le SNIP.

Pour créer une adresse IP d'alias, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface NIC0.
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez les adresses IP d'alias.

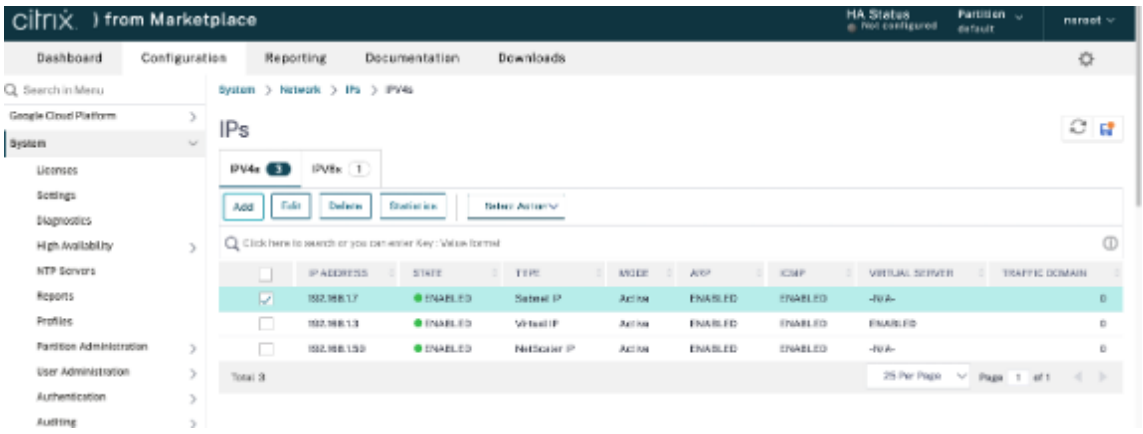


4. Cliquez sur **Terminé**, puis sur **Enregistrer**.
5. Vérifiez les adresses IP d'alias sur la page de **détails de l'instance de machine virtuelle** .

Étape 5. Ajoutez VIP et SNIP sur l'instance VPX.

Sur l'instance VPX, ajoutez l'adresse IP d'alias client et l'adresse IP d'alias de serveur.

1. Sur l'interface graphique de NetScaler, accédez à **Système > Réseau > IP IPv4s**, puis cliquez sur **Ajouter**.

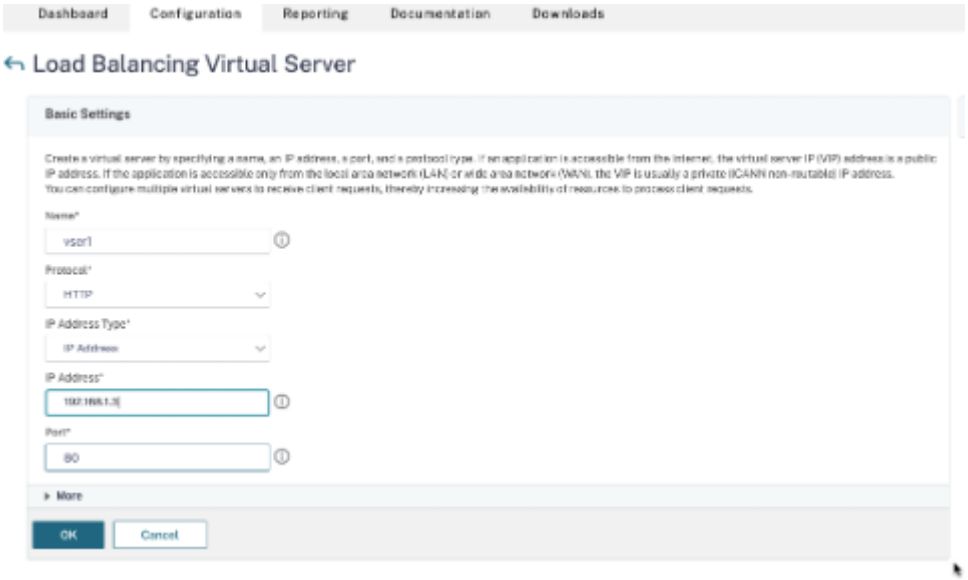


2. Pour créer une adresse IP (VIP) alias client :
   - Entrez l'adresse IP d'alias client et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.
   - Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   - Cliquez sur **Créer**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
   - Entrez l'adresse IP et le masque de réseau d'alias de serveur configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.

- Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
- Cliquez sur **Créer**.

Étape 6. Ajoutez un serveur virtuel d'équilibrage de charge.

1. Sur l'interface graphique NetScaler, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis cliquez sur **Ajouter**.
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (adresse IP d'alias client) et le port.
3. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.



Étape 8. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance.

1. À partir de l'interface graphique de NetScaler, accédez à **Configuration > Gestion du trafic > Équilibrage de charge Services**, puis cliquez sur **Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 8. Liez le service/groupe de services au serveur virtuel d'équilibrage de charge sur l'instance.

1. À partir de l'interface graphique, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 6**, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Services et groupes de services**, cliquez sur **Liaison de service de serveur virtuel sans équilibrage**de charge.
4. Sélectionnez le service configuré à l'**étape 7**, puis cliquez sur **Lier**.

Points à noter après le déploiement de l'instance VPX sur GCP

- Connectez-vous au VPX avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe. À l'invite, modifiez le mot de passe et enregistrez la configuration.
- Pour collecter un bundle de support technique, exécutez la commande `shell /netscaler/showtech_cloud.pl` au lieu de la commande habituelle `show techsupport`.
- Après avoir supprimé une machine virtuelle NetScaler de la console GCP, supprimez également l'instance cible interne NetScaler associée. Pour ce faire, accédez à l'interface de ligne de commande gcloud et tapez la commande suivante :

```
1    gcloud compute -q  target-instances delete <instance-name>-
        adcinternal --zone <zone>
```

> **Remarque :**
>
> <instance-name>-adcinternal est le nom de l'instance cible qui doit être supprimée.

Licence NetScaler VPX

Une instance NetScaler VPX sur GCP nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur GCP.

- **Licences basées sur un abonnement** : les appliances NetScaler VPX sont disponibles sous forme d'instances payantes sur la place de marché GCP. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure. Les modèles VPX et les éditions de licences suivants sont disponibles sur le marché GCP.

Performances VPX prises en charge
NetScaler VPX Advanced - 200 Mbits/s
NetScaler VPX Premium - 1 Gbit/s
NetScaler VPX Premium - 5 Gbit/s
NetScaler VPX Express - 20 Mbps
NetScaler VPX –Licence client
NetScaler VPX FIPS - Licence client

- **Apportez votre propre licence (BYOL)** : Si vous apportez votre propre licence (BYOL), consultez le guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :

  - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
  - Télécharger la licence sur l'instance.

- **Licences NetScaler VPX Check-In/Check-Out : pour plus d'informations, voir Licences NetScaler VPX Check-In/Check-Out**.

VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur NetScaler VPX Express, consultez la section « Licence NetScaler VPX Express » dans la vue d'ensemble des licences NetScaler.

Modèles GDM pour déployer une instance NetScaler VPX

Vous pouvez utiliser un modèle NetScaler VPX Google Deployment Manager (GDM) pour déployer une instance VPX sur GCP. Pour plus de détails, consultez la section Modèles NetScaler GDM.

Images de NetScaler Marketplace

Vous pouvez utiliser les images des modèles GDM pour faire apparaître l'appliance NetScaler.

Le tableau suivant répertorie les images disponibles sur le marché GCP.

Libérer	Nom de l'image	Emplacement de l'image
14.1	citrix-adc-vpx-express-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-express-14-1-21-57
14.1	citrix-adc-vpx-200-enterprise-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-14-1-21-57
14.1	citrix-adc-vpx-1000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-platinum-14-1-21-57
14.1	citrix-adc-vpx-5000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-14-1-21-57
14.1	citrix-adc-vpx-byol-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-14-1-21-57

Ressources

- Création d'instances avec plusieurs interfaces réseau
- Création et démarrage d'une instance de machine virtuelle

Informations connexes

- Déployer une paire haute disponibilité VPX sur Google Cloud Platform

Déployer une paire haute disponibilité VPX sur Google Cloud Platform

October 17, 2024

Vous pouvez configurer deux instances NetScaler VPX sur Google Cloud Platform (GCP) en tant que paire active et passive à haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si pour une raison quelconque, si le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur HA, voir Haute disponibilité.

Les nœuds doivent se trouver dans la même région ; cependant, ils peuvent se trouver soit dans la même zone, soit dans des zones différentes. Pour plus d'informations, voir Régions et zones.

Chaque instance VPX nécessite au moins trois sous-réseaux IP (réseaux Google VPC) :

- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le serveur principal (SNIP, MIP, etc.)

Citrix recommande trois interfaces réseau pour une instance VPX standard.

Vous pouvez déployer une paire VPX à haute disponibilité selon les méthodes suivantes :

- Utilisation d'une adresse IP statique externe
- Utilisation d'une adresse IP privée
- Utilisation de machines virtuelles à carte réseau unique avec adresse IP privée

Modèles GDM pour déployer une paire haute disponibilité VPX sur GCP

Vous pouvez utiliser un modèle NetScaler Google Deployment Manager (GDM) pour déployer une paire de haute disponibilité VPX sur GCP. Pour plus de détails, consultez la section Modèles NetScaler GDM.

Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP

Vous pouvez déployer une paire VPX haute disponibilité sur le GCP à l'aide de règles de transfert.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Conditions préalables

- Les règles de transfert doivent se situer dans la même région que les instances VPX.
- Les instances cibles doivent se trouver dans la même zone que l'instance VPX.
- Le nombre d'instances cibles pour les nœuds principal et secondaire doit correspondre.

Exemple

Vous disposez d'une paire à haute disponibilité dans la `us-east1` région avec un VPX principal dans la `us-east1-b` zone et un VPX secondaire dans la `us-east1-c` zone. Une règle de transfert est configurée pour le VPX principal avec l'instance cible dans la `us-east1-b` zone. Configurez une instance cible pour le VPX secondaire dans la `us-east1-c` zone afin de mettre à jour la règle de transfert en cas de basculement.

Limitations

Seules les règles de transfert configurées avec des instances cibles en arrière-plan sont prises en charge dans le déploiement à haute disponibilité de VPX.

Déployer une paire haute disponibilité VPX avec une adresse IP statique externe sur Google Cloud Platform

October 17, 2024

Vous pouvez déployer une paire haute disponibilité VPX sur GCP à l'aide d'une adresse IP statique externe. L'adresse IP du client du nœud principal doit être liée à une adresse IP statique externe. Lors

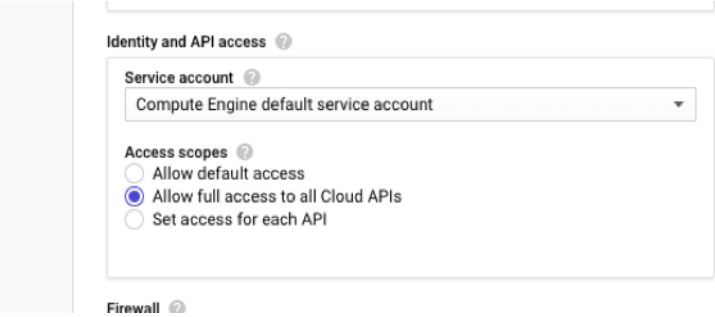
du basculement, l'adresse IP statique externe est déplacée vers le nœud secondaire pour que le trafic reprenne.

Une adresse IP externe statique est une adresse IP externe réservée à votre projet jusqu'à ce que vous décidiez de le libérer. Si vous utilisez une adresse IP pour accéder à un service, vous pouvez réserver cette adresse IP afin que seul votre projet puisse l'utiliser. Pour plus d'informations, voir Réserver une adresse IP externe statique.

Pour plus d'informations sur HA, voir Haute disponibilité.

Avant de commencer

- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur Google Cloud Platform. Ces informations s'appliquent également aux déploiements HA.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que le rôle IAM associé à votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.instances.get",
"Compute.instances.list",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
```



```
18     ]
```

- Si vous avez configuré des adresses IP d'alias sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :

```
1     "compute.instances.updateNetworkInterface"
```

- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et les exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau nœud principal lors du basculement.

Comment déployer une paire VPX HA sur Google Cloud Platform

Voici un résumé des étapes de déploiement HA :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent être dans la même zone ou des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

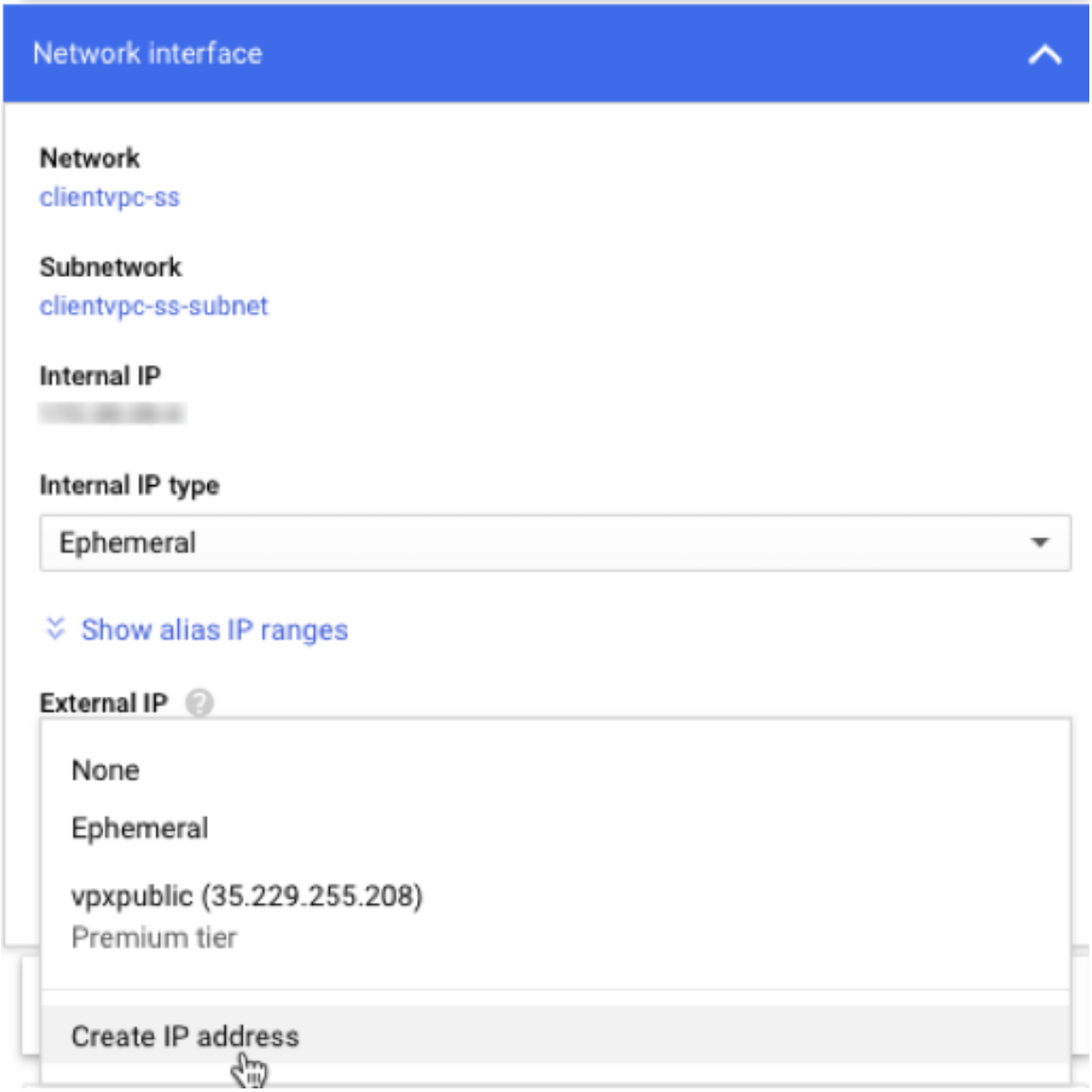
1. Connectez-vous à la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX sur Google Cloud Platform.

Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-NIC et multi-IP.

> **Important :**
>
> Attribuez une adresse IP externe statique à l'adresse IP du client (VIP) du nœud principal. Vous pouvez utiliser une adresse IP réservée existante ou en créer une nouvelle. Pour créer une adresse IP externe statique, accédez à **Interface réseau > IP externe**, cliquez sur **Créer une adresse IP**.



Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, l'adresse IP externe statique se déplace de l'ancien principal et est attachée au nouveau principal. Pour plus d'informations, consultez le document Google Cloud Reserving a Static External IP Address.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses VIP et

SNIP. Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique NetScaler pour CLI.

Configurer HA à l'aide de l'interface graphique **Étape 1**. Configurez la haute disponibilité en mode INC sur les deux instances.

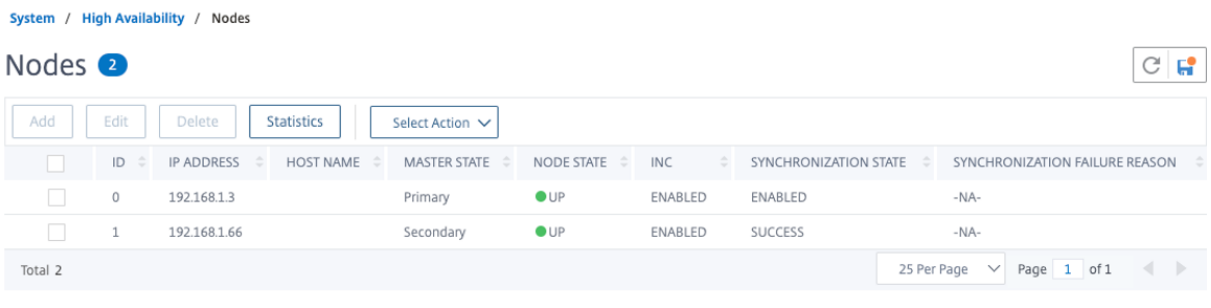
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .

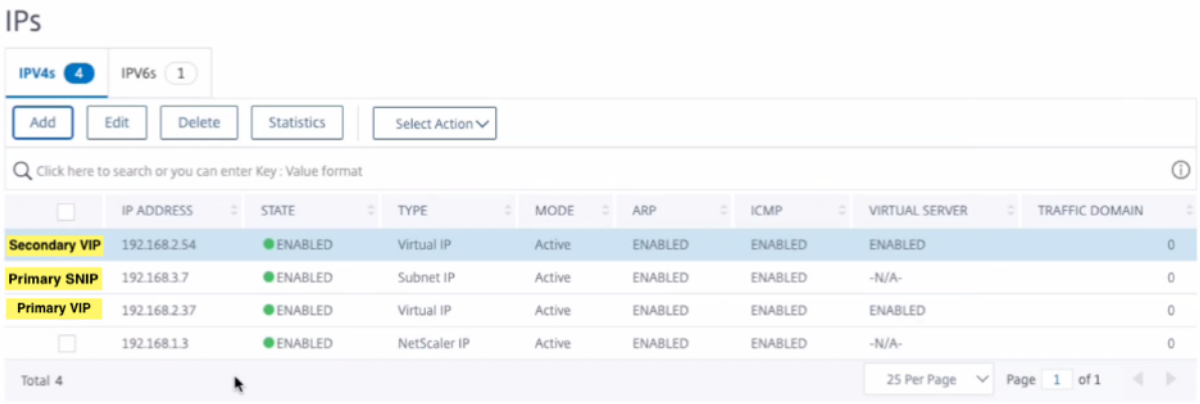


> **Remarque :**
>
> Maintenant, le nœud secondaire a les mêmes informations d'identification d'ouverture de session que le nœud principal.

Étape 2. Ajoutez des IP virtuelles et des adresses IP de sous-réseau sur les deux nœuds.

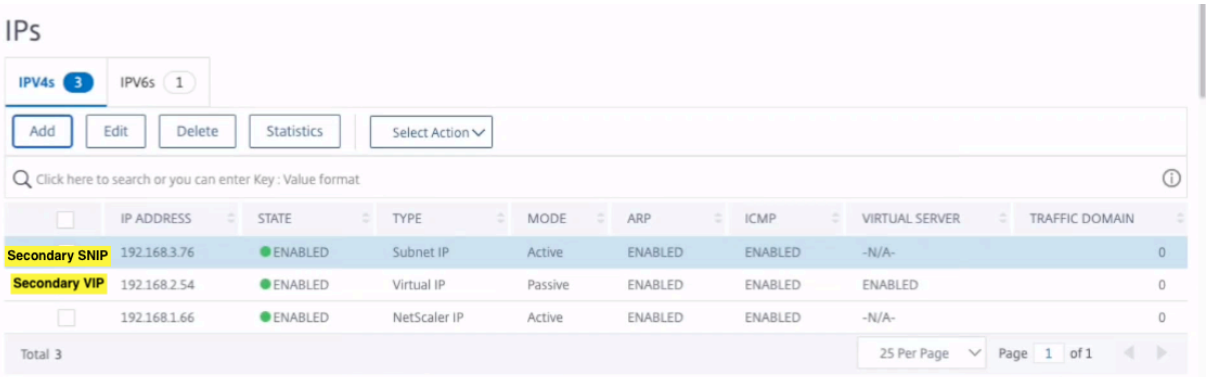
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance principale et du masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.
3. Ajoutez une adresse SNIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance principale.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Créer**.
4. Ajoutez une adresse VIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
3. Ajoutez une adresse SNIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance secondaire.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Créer**.

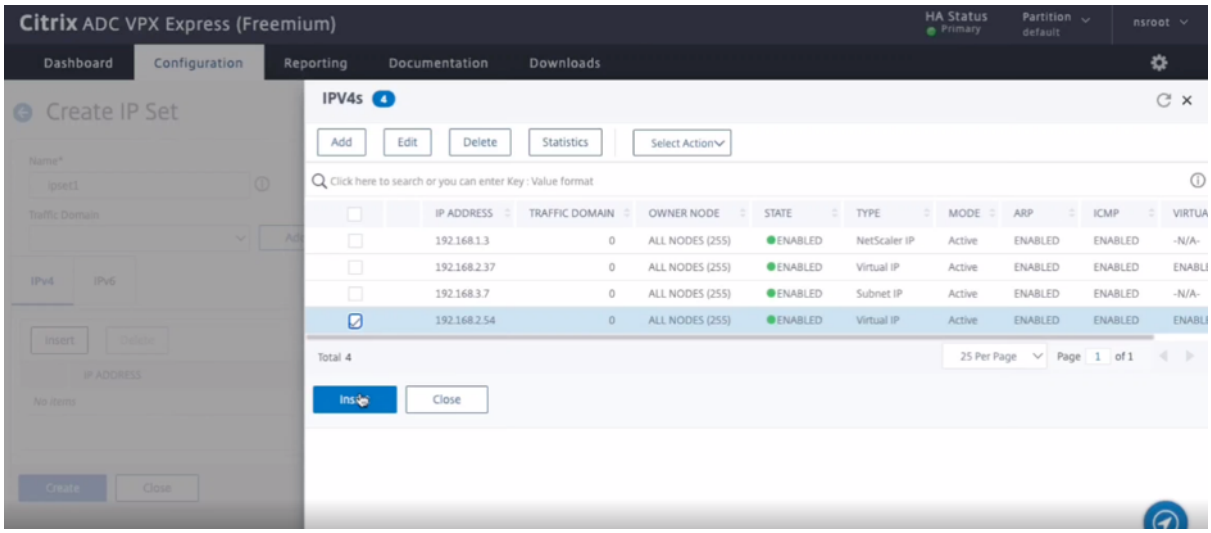


Étape 2 Ajoutez un service ou un groupe de services. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

Sur le **nœud principal**, effectuez les opérations suivantes :

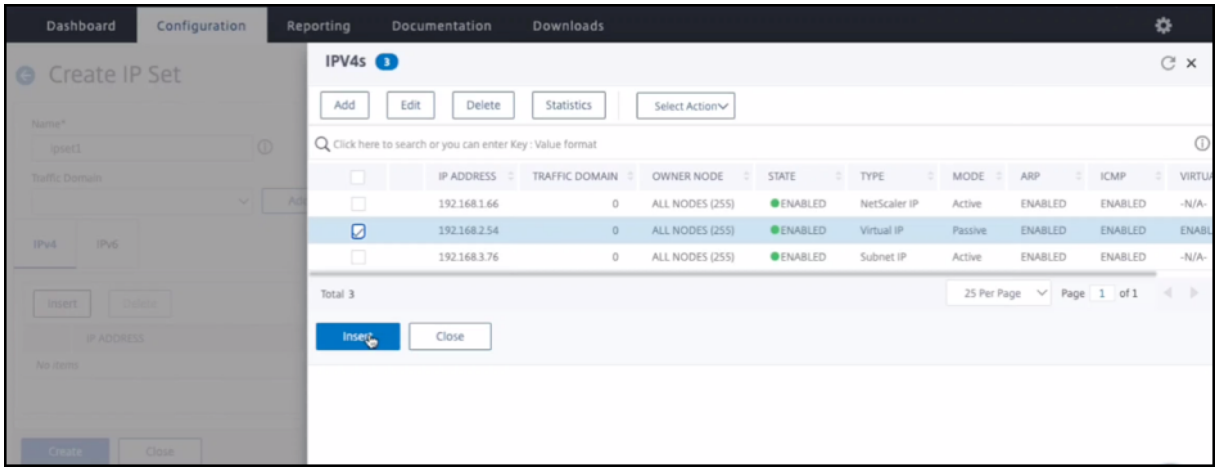
1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.

4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > Jeux d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.

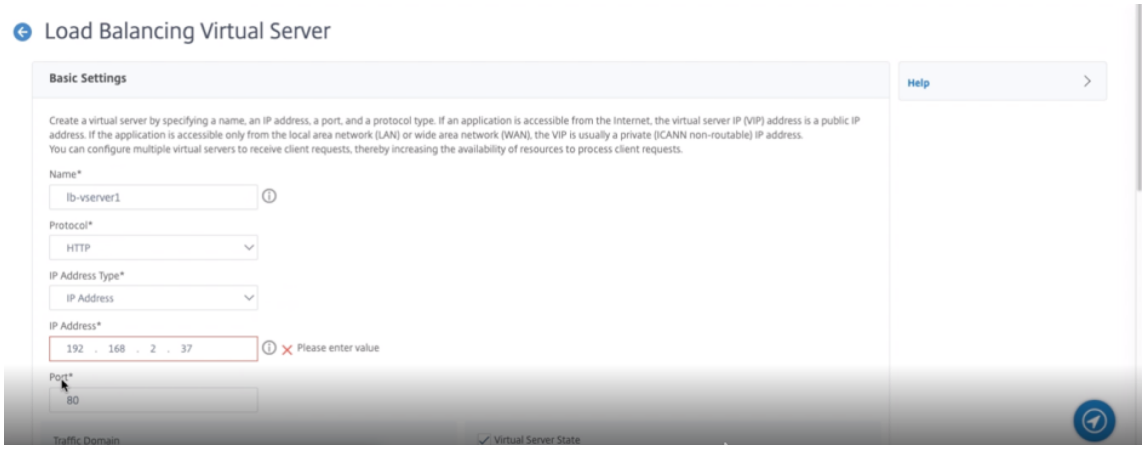


> **Remarque :**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Ajoutez un serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.

2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (VIP principale) et le port.



3. Cliquez sur **Plus**. Accédez à **Paramètres du jeu d'adresses IP de plage IP**, sélectionnez **IPset** dans le menu déroulant et indiquez l'IPSet créé à l'**étape 3**.
4. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 6. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 4**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 5**, puis cliquez sur **Lier**.

Enregistrez la configuration. Après un basculement forcé, le secondaire devient le nouveau principal. L'IP statique externe de l'ancien VIP principal se déplace vers le nouveau VIP secondaire.

Configuration de la haute disponibilité à l'aide de l'interface **Étape 1**. Configurez la haute disponibilité en mode INC dans les deux instances.

Sur le nœud principal, tapez la commande suivante.


```
add ha node 1 <sec_ip> -inc ENABLED
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

`prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2. Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

Sur le nœud principal, tapez la commande suivante.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance principale.

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Sur le nœud secondaire, tapez la commande suivante.

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

Étape 2 Ajoutez un service ou un groupe de services. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

Sur le nœud principal, tapez la commande suivante :

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
```

Sur le nœud secondaire, tapez la commande suivante :


```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
```

> **Remarque :**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Ajoutez un serveur virtuel sur l'instance principale.

Entrez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <
   port> -ipset <ipset_name>
```

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Ajoutez un service ou un groupe de services sur l'instance principale.

Entrez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
```

Étape 6. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

Entrez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
```

> **Remarque :**
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Étape 7. Vérifiez la configuration.

Assurez-vous que l'adresse IP externe attachée à la carte réseau client principale se déplace vers la secondaire lors d'un basculement.

1. Effectuez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est accessible.
2. Sur l'instance principale, effectuez un basculement :

   Depuis l'interface graphique, accédez à **Configuration > Système > Haute disponibilité > Action > Forcer le basculement**.

   Depuis la CLI, saisissez la commande suivante :

   ```
   force ha failover -f
   ```


Sur la console GCP, accédez à l'instance secondaire. L'adresse IP externe doit avoir été déplacée vers la carte réseau client de secondaire après basculement.

3. Émettez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est à nouveau accessible.

Déployez une paire de cartes réseau VPX à haute disponibilité unique avec une adresse IP privée sur Google Cloud Platform

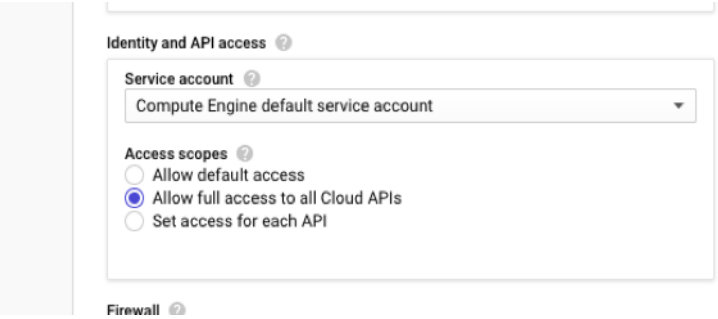
October 17, 2024

Vous pouvez déployer une seule paire de cartes réseau VPX à haute disponibilité sur GCP à l'aide d'une adresse IP privée. L'adresse IP du client (VIP) doit être configurée comme adresse IP d'alias sur le nœud principal. Lors du basculement, l'adresse IP du client est déplacée vers le nœud secondaire, pour que le trafic reprenne. Les adresses IP de sous-réseau (SNiP) de chaque nœud doivent également être configurées en tant que plage d'adresses IP d'alias.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Avant de commencer

- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur Google Cloud Platform. Ces informations s'appliquent également aux déploiements haute disponibilité.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



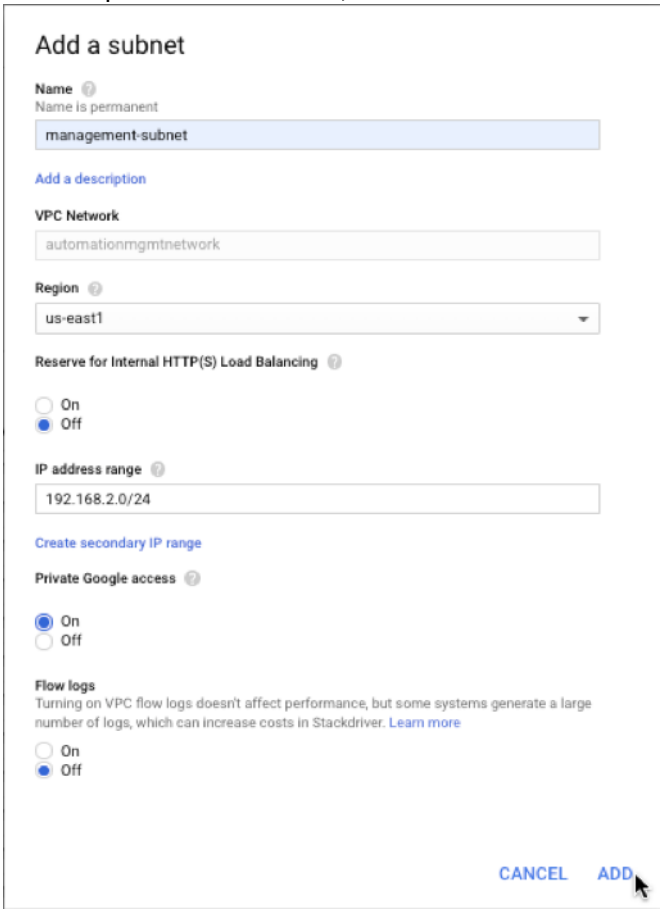
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
```



```
    "compute.instances.get",
    "compute.instances.list",
    "compute.instances.updateNetworkInterface",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.targetInstances.create",
    "compute.zones.list",
    "compute.zoneOperations.get",
    ]
```

- Si vos machines virtuelles n'ont pas accès à Internet, vous devez activer **Private Google Access** sur le sous-réseau VPC.



- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et les exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau nœud principal lors du basculement.

Comment déployer une paire haute disponibilité VPX sur Google Cloud Platform

Voici un résumé des étapes à suivre pour déployer une paire HA avec une seule carte réseau :

1. Créez un réseau VPC.

2. Créez deux instances VPX (nœuds principal et secondaire) dans la même région. Ils peuvent être dans la même zone ou des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Création d'un réseau VPC

Pour créer un réseau VPC, procédez comme suit :

1. Connectez-vous à la **console Google > Réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX sur Google Cloud Platform.

Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes 1 à 3 indiquées dans Scénario : Déployer une instance VPX autonome à carte réseau unique.

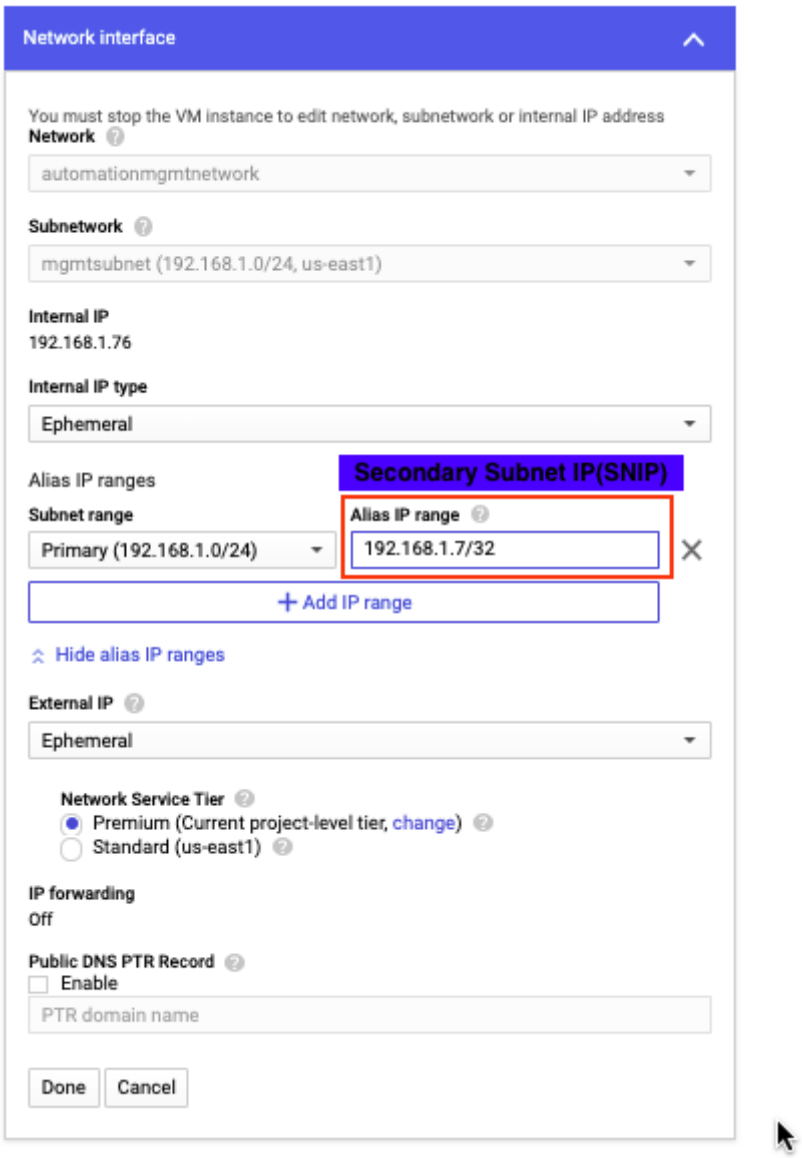
> **Important :**
>
> Attribuez une adresse IP d'alias client uniquement au nœud principal et des adresses IP d'alias de serveur aux nœuds principal et secondaire. N'utilisez pas l'adresse IP interne de l'instance VPX pour configurer le VIP ou le SNIP.

Pour créer des adresses IP d'alias de client et de serveur, effectuez ces étapes sur le nœud principal :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client (NIC0).
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez l'adresse IP de l'alias du client.
4. Cliquez sur **Ajouter une plage d'adresses IP** et entrez l'adresse IP de l'alias du serveur.

Pour créer une adresse IP d'alias de serveur, effectuez ces étapes sur le nœud secondaire :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client (NIC0).
3. Dans le champ **Plage IP d'alias**, entrez l'adresse IP de l'alias du serveur.



Après le basculement, lorsque l'ancien serveur principal devient le nouveau serveur secondaire, l'adresse IP de l'alias du client est déplacée de l'ancien serveur principal et est associée au nouveau serveur principal.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses IP virtuelles (VIP) et SNIP (Subnet IP). Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique ou de la CLI de NetScaler.

Configurer la haute disponibilité à l'aide de l'interface graphique

Étape 1. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

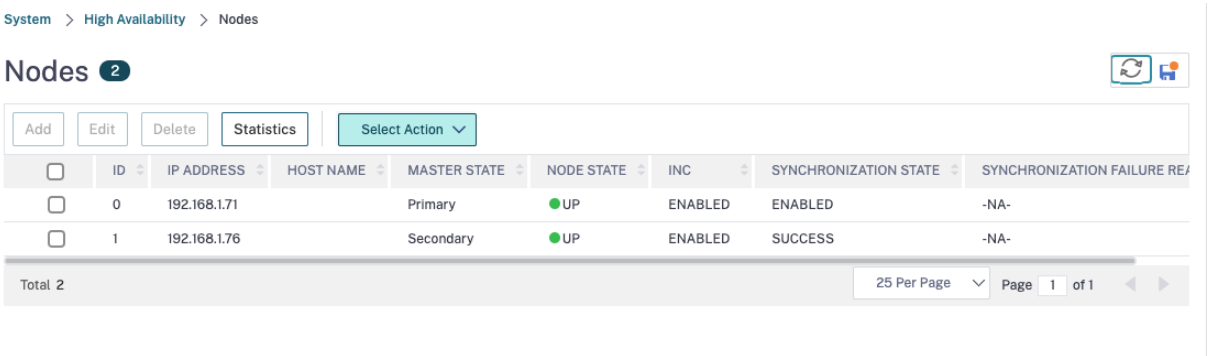
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .

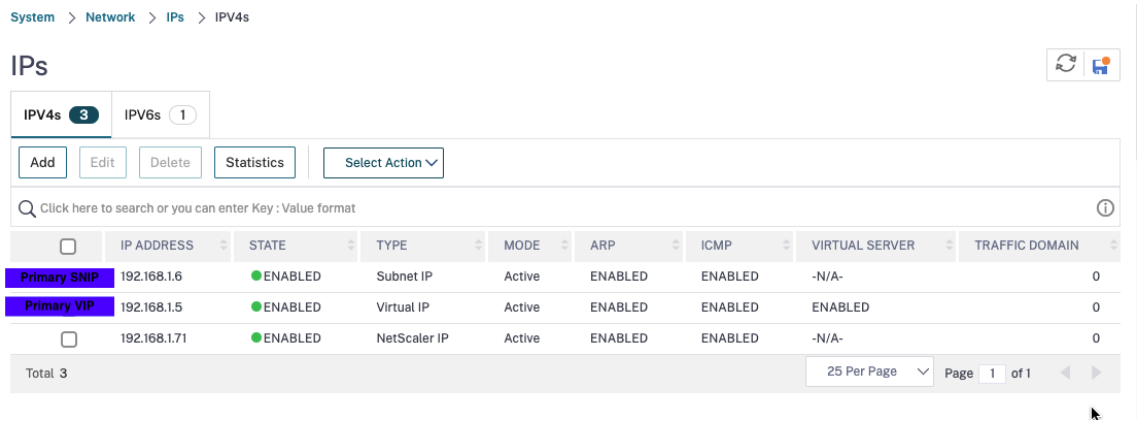


> **Remarque :**
>
> Une fois le nœud secondaire synchronisé avec le nœud principal, le nœud secondaire possède les mêmes informations de connexion que le nœud principal.

Étape 2. Ajoutez des IP virtuelles et des adresses IP de sous-réseau sur les deux nœuds.

Sur le nœud principal, effectuez les opérations suivantes :

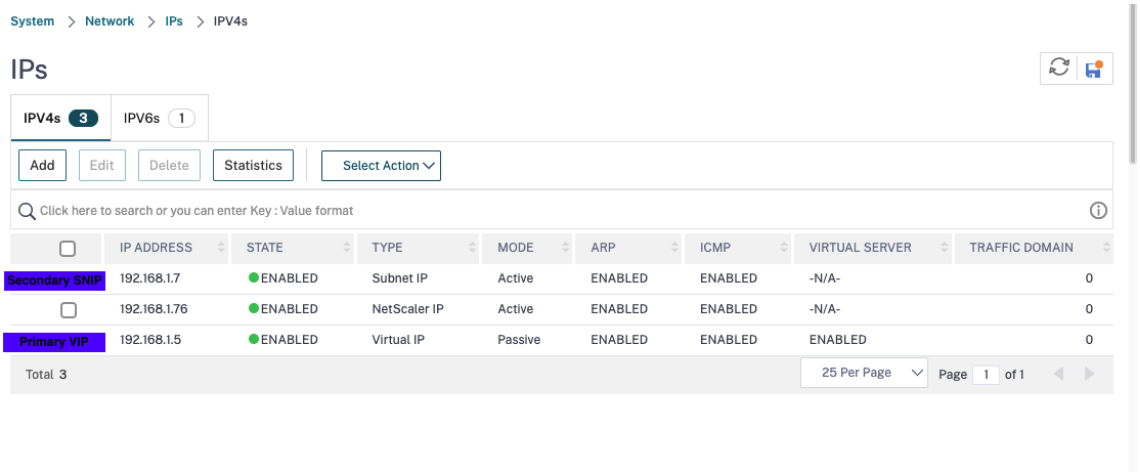
1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
    a) Entrez l'alias du client, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle principale.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
    a) Entrez l'alias du serveur, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle principale.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Créer**.



Sur le nœud secondaire, effectuez les opérations suivantes :

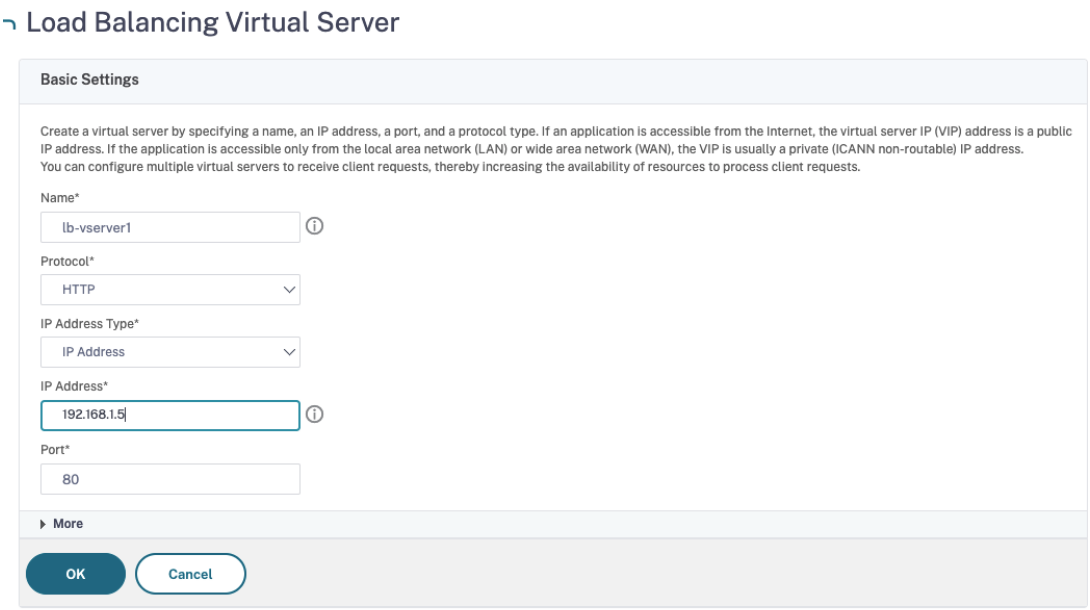
1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
    a) Entrez l'alias du client, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC de l'instance de machine virtuelle principale.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Créer**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
    a) Entrez l'alias du serveur, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC de l'instance de machine virtuelle secondaire.

b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Créer**.



Étape 2 Ajoutez un service ou un groupe de services. **Étape 3** Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias principal du client) et Port, puis cliquez sur **OK**.



Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.

2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 3**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 4**, puis cliquez sur **Lier**.

Étape 6. Enregistrez la configuration.

Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP d'alias client (VIP) de l'ancien serveur principal est transférée vers le nouveau serveur principal.

Configuration de la haute disponibilité à l'aide de la CLI

Étape 1. Configurez la haute disponibilité en mode **INC Enabled** dans les deux instances à l'aide de l'interface de ligne de commande NetScaler.

Sur le nœud principal, tapez la commande suivante.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
```

Le `sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

Le `prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2. Ajoutez VIP et SNIP sur les nœuds principaux et secondaires.

Tapez les commandes suivantes sur le nœud principal :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.


```
add ns ip <primary_server_alias_ip> <subnet> -type SNIP
```

Tapez les commandes suivantes sur le nœud secondaire :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau du serveur dans l'instance de machine virtuelle.

Étape 2 Ajoutez un service ou un groupe de services. Ajoutez un serveur virtuel sur le nœud principal.

Entrez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

Entrez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
```

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

Entrez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
```

> **Remarque :**
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Déployer une paire VPX haute disponibilité avec une adresse IP privée sur Google Cloud Platform

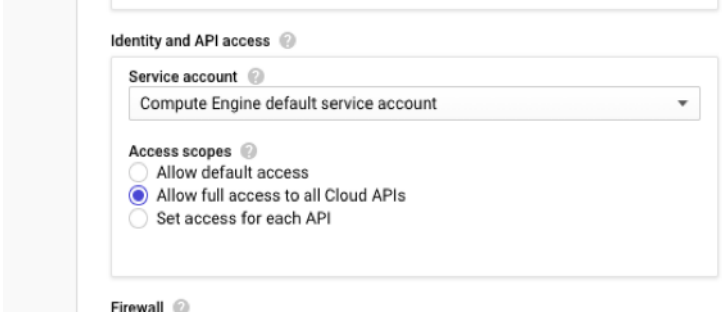
October 17, 2024

Vous pouvez déployer une paire VPX haute disponibilité sur GCP à l'aide d'une adresse IP privée. L'adresse IP du client (VIP) doit être configurée en tant qu'adresse IP alias sur le nœud principal. Lors du basculement, l'adresse IP du client est déplacée vers le nœud secondaire, pour que le trafic reprenne.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Avant de commencer

- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur Google Cloud Platform. Ces informations s'appliquent également aux déploiements haute disponibilité.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



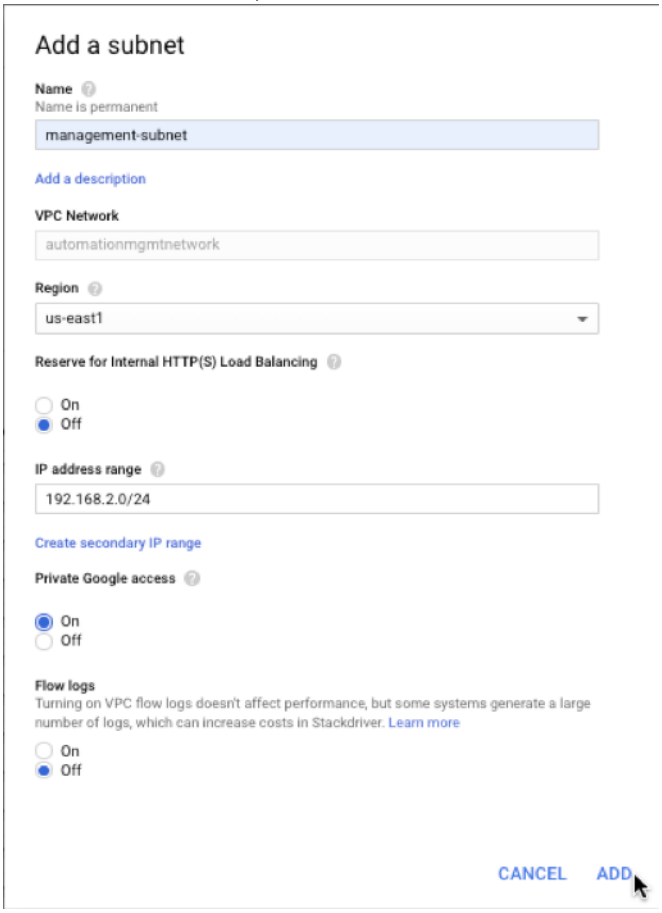
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
```


- Si vous avez configuré des adresses IP externes sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.addresses.use"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
]
```

- Si vos machines virtuelles ne disposent pas d'un accès Internet, vous devez activer **Private Google Access** sur le sous-réseau de gestion.



- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et les exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau nœud principal lors du basculement.

Comment déployer une paire haute disponibilité VPX sur Google Cloud Platform

Voici un résumé des étapes de déploiement haute disponibilité :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent être dans la même zone ou des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres de haute disponibilité sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

1. Connectez-vous à la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX sur Google Cloud Platform.

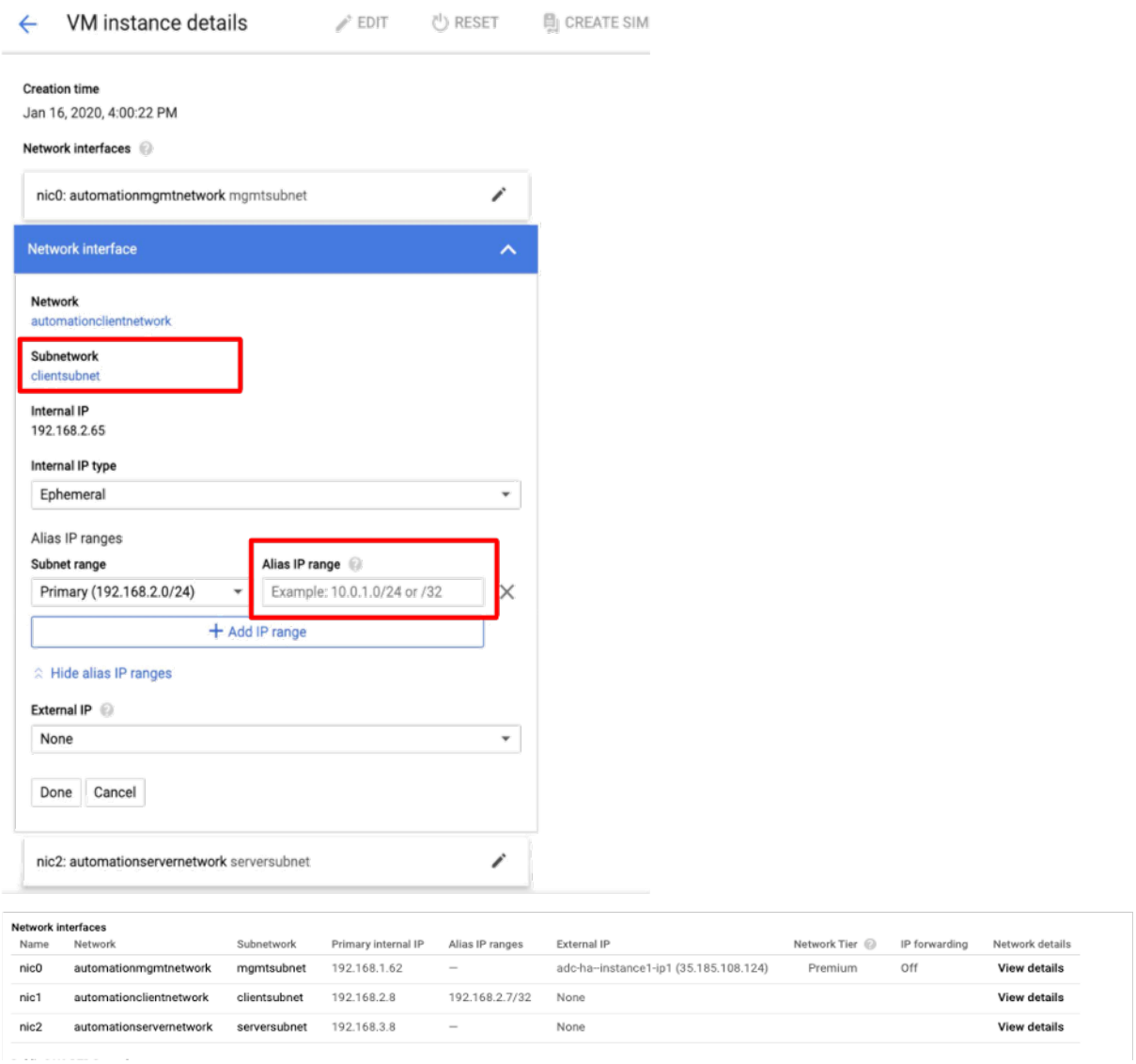
Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-NIC et multi-IP.

> **Important :**
>
> Attribuez une adresse IP d'alias client au nœud principal. N'utilisez pas l'adresse IP interne de l'instance VPX pour configurer le VIP.

Pour créer une adresse IP d'alias client, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client.
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez l'adresse IP de l'alias du client.



Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, les adresses IP de l'alias se déplacent de l'ancien principal et sont attachées au nouveau principal.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses IP virtuelles (VIP) et SNIP (Subnet IP). Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique ou de la CLI de NetScaler.

Configurer la haute disponibilité à l'aide de l'interface graphique

Étape 1. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

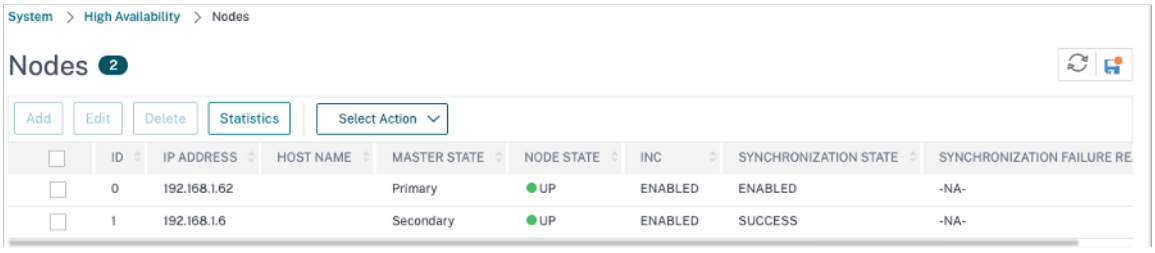
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. **Activez la case à cocher Activer le mode INC (Independent Network Configuration) sur auto-nœud** .
5. Cliquez sur **Créer**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .

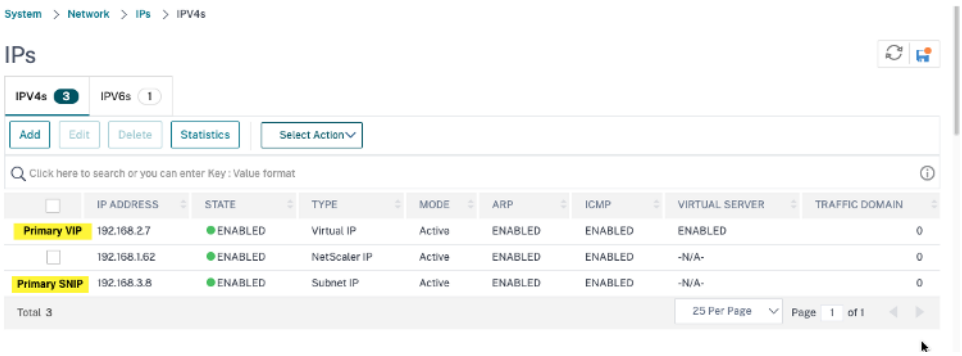


> **Remarque :**
>
> Une fois le nœud secondaire synchronisé avec le nœud principal, le nœud secondaire possède les mêmes informations de connexion que le nœud principal.

Étape 2. Ajoutez des IP virtuelles et des adresses IP de sous-réseau sur les deux nœuds.

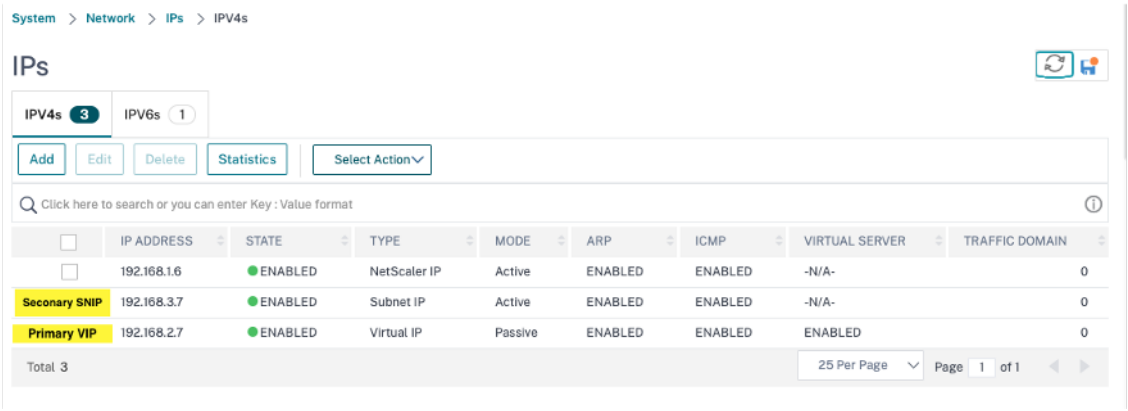
Sur le nœud principal, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
   a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   c) Cliquez sur **Créer**.
3. Pour créer une adresse IP du serveur (SNIP) :
   a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Créer**.



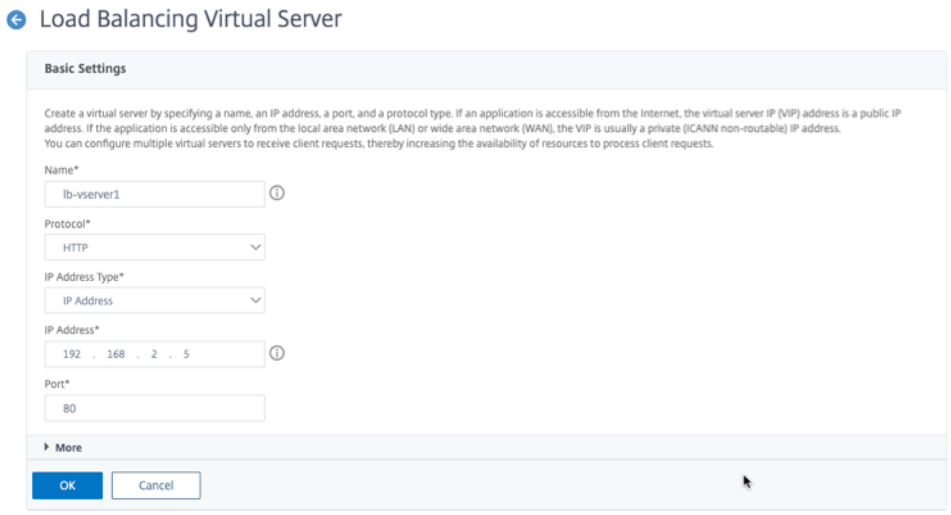
Sur le nœud secondaire, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
   a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Créer**.
3. Pour créer une adresse IP du serveur (SNIP) :
   a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Créer**.



Étape 2 Ajoutez un service ou un groupe de services. **Étape 3** Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias principal du client) et Port, puis cliquez sur **OK**.



Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 3**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 4**, puis cliquez sur **Lier**.

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Enregistrez la configuration.

Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP de l'alias client (VIP) et l'adresse IP de l'alias de serveur (SNIP) de l'ancien serveur principal sont déplacées vers la nouvelle adresse principale.

Configuration de la haute disponibilité à l'aide de la CLI

Étape 1. Configurez la haute disponibilité en mode **INC Enabled** dans les deux instances à l'aide de l'interface de ligne de commande NetScaler.

Sur le nœud principal, tapez la commande suivante.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
```

Le `sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

Le `prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2. Ajoutez VIP et SNIP sur les deux nœuds.

Tapez les commandes suivantes sur le nœud principal :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Remarque :**
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
add ns ip <primary_snip> <subnet> -type SNIP
```

Le `primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Tapez les commandes suivantes sur le nœud secondaire :


```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Remarque :**
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

Le `secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

> **Remarque :**
>
> Entrez l'adresse IP et le masque de réseau configurés pour le sous-réseau du serveur dans l'instance de machine virtuelle.

Étape 2 Ajoutez un service ou un groupe de services. Ajoutez un serveur virtuel sur le nœud principal.

Entrez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

Entrez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
```

Étape 5 Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

Entrez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
```

> **Remarque :**
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

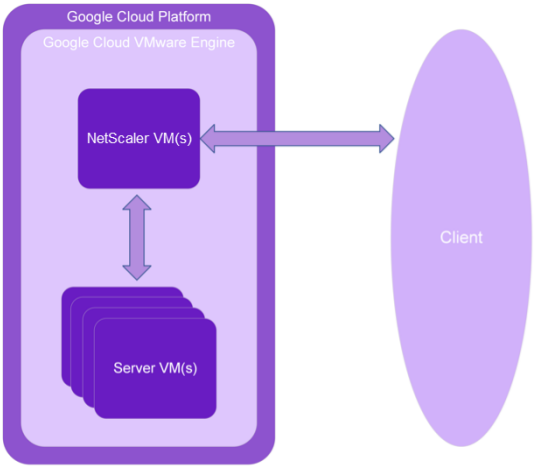
Installation d'une instance NetScaler VPX sur Google Cloud VMware Engine

October 17, 2024

Google Cloud VMware Engine (GCVE) met à votre disposition des clouds privés contenant des clusters vSphere, conçus à partir d'une infrastructure Google Cloud Platform dédiée. Le déploiement initial minimum est de trois hôtes, mais des hôtes supplémentaires peuvent être ajoutés un par un. Tous les clouds privés provisionnés sont dotés de vCenter Server, vSAN, vSphere et NSX-T.

GCVE vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur Google Cloud Platform avec le nombre souhaité d'hôtes ESX. GCVE prend en charge les déploiements NetScaler VPX. GCVE fournit une interface utilisateur identique à celle de vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Le schéma suivant montre le GCVE sur la Google Cloud Platform auquel un administrateur ou un client peut accéder via Internet. Un administrateur peut créer, gérer et configurer des machines virtuelles de charge de travail ou de serveur à l'aide de GCVE. L'administrateur peut accéder au vCenter et au NSX-T Manager basés sur le Web du GCVE via une connexion OpenVPN. Vous pouvez créer les instances NetScaler VPX (autonomes ou par paire HA) et les machines virtuelles de serveur au sein de GCVE à l'aide de vCenter, et gérer le réseau correspondant à l'aide de NSX-T manager. L'instance NetScaler VPX sur GCVE fonctionne de la même manière que le cluster d'hôtes VMware sur site. Le GCVE peut être géré à l'aide d'une connexion OpenVPN à l'infrastructure de gestion.



Conditions préalables

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Pour plus d'informations sur Google Cloud VMware Engine et ses prérequis, consultez la documentation Google Cloud VMware Engine.
- Pour plus d'informations sur le déploiement de Google Cloud VMware Engine, voir Déployer un cloud privé Google Cloud VMware Engine.
- Pour plus d'informations sur la connexion à votre cloud privé à l'aide d'une passerelle VPN point à site pour accéder à Google Cloud VMware Engine et le gérer, consultez Accéder à un cloud privé Google Cloud VMware Engine.
- Sur la machine cliente VPN, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Google Cloud VMware Engine.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez la section Vue d'ensemble des licences.
- Les machines virtuelles (VM) créées ou migrées vers le cloud privé GCVE doivent être connectées à un segment réseau.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> **Remarque :**
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration système minimale requise pour l'installation de l'outil OVF.

Tableau 2. Tableau 2 Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
Système d'exploitation	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

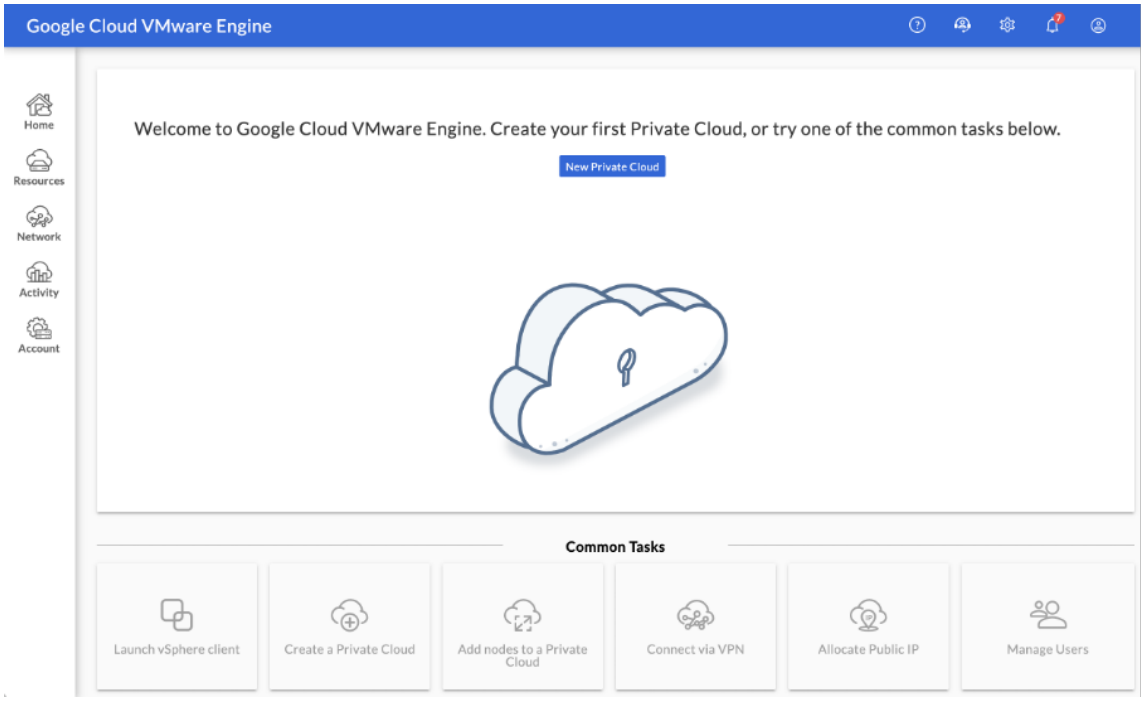
Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-79.64-Disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (par exemple, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (par exemple, NSVPX-ESX-13.0-79.64.mf)

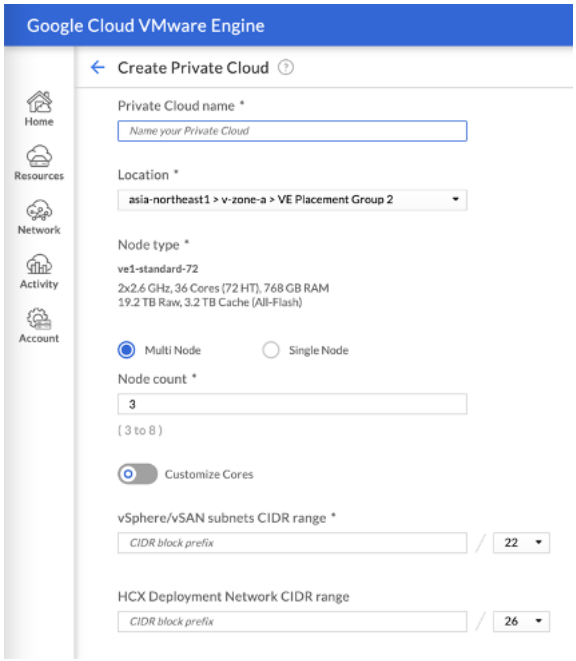
Déployer Google Cloud VMware Engine

1. Connectez-vous à votre portail GCVEet accédez à la page d'**accueil**.

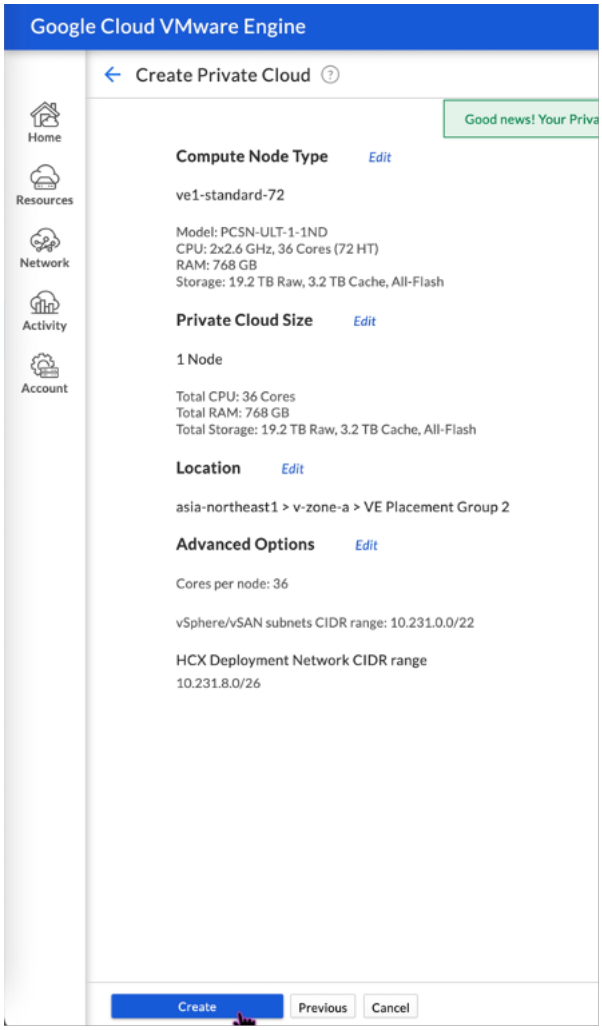


2. Sur la page **Nouveau cloud privé**, entrez les informations suivantes :

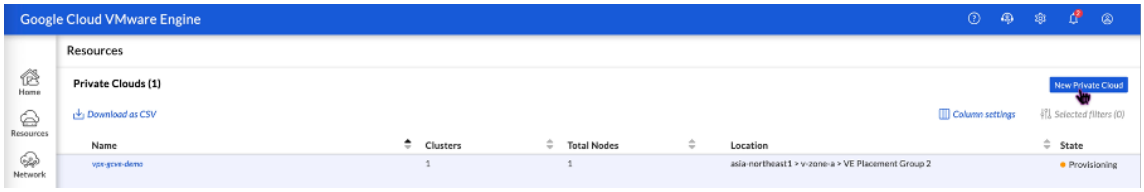
   - Sélectionnez au moins 3 hôtes ESXi pour créer le cluster par défaut de votre cloud privé.
   - Pour le champ de **plage d'adresses CIDR du sous-réseau vSphère/vSAN**, utilisez l'espace d'adressage /22.
   - Pour le champ de **plage d'adresses CIDR du réseau de déploiement HCX**, utilisez l'espace d'adressage /26.
   - Pour le réseau virtuel, assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux GCP locaux ou autres (réseaux virtuels).



3. Cliquez sur **Vérifier et créer**.
4. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.



5. Cliquez sur **Créer**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.
6. Accédez à **Ressources** pour vérifier le cloud privé créé.

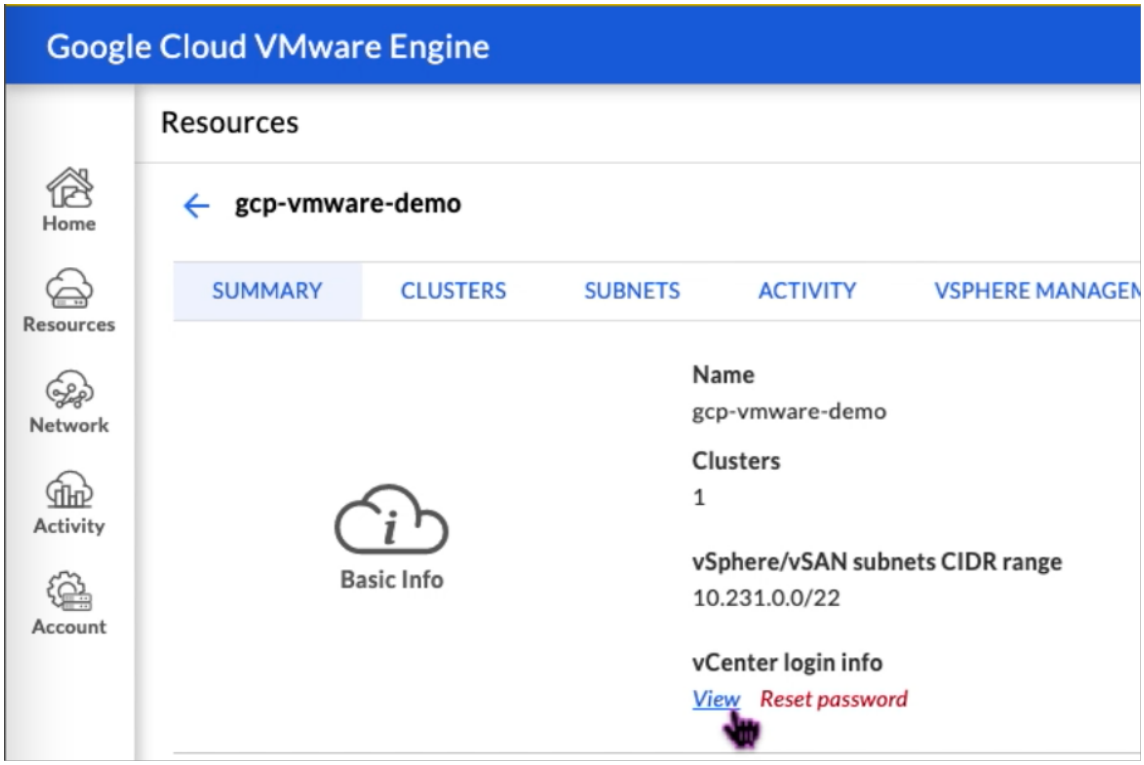


7. Pour accéder à cette ressource, vous devez vous connecter à GCVE à l'aide d'un VPN point à site. Pour plus d'informations, consultez la documentation suivante :

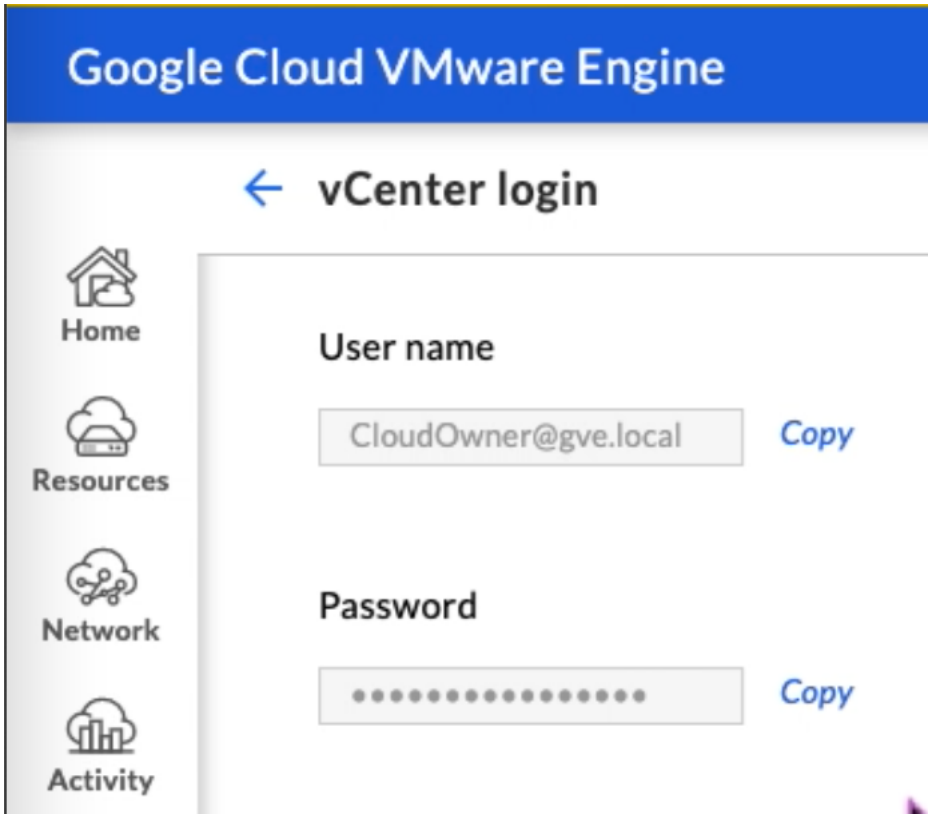
   - Passerelles VPN
   - Connexion via un VPN

Accédez à votre portail Private Cloud vCenter

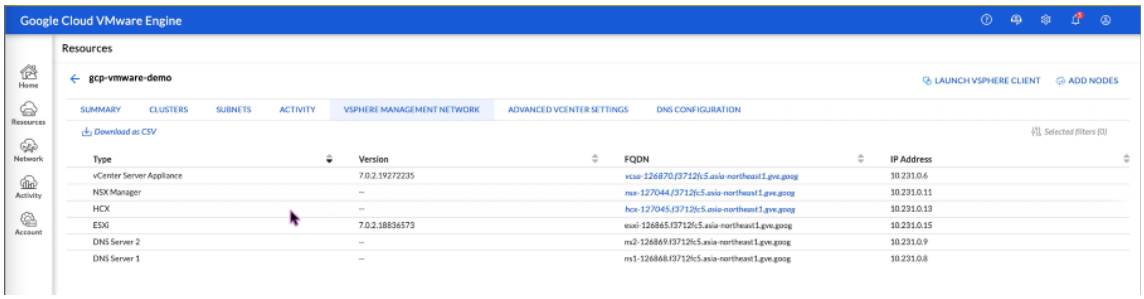
1. Accédez à votre cloud privé Google Cloud VMware Engine. Dans l'onglet **RÉSUMÉ**, sous **Informations de connexion à vCenter**, cliquez sur **Afficher**.



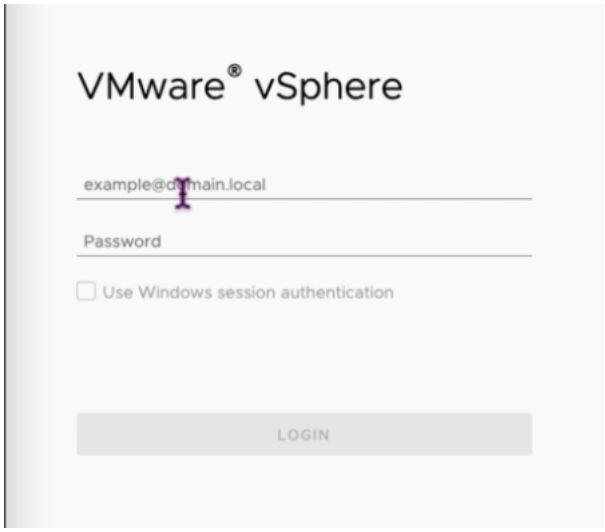
2. Notez les informations d'identification de vCenter.



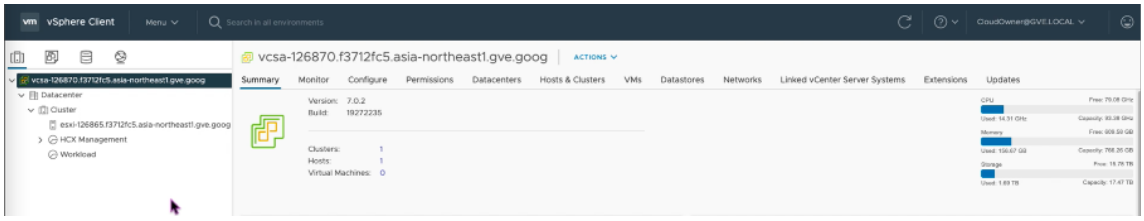
3. Lancez le client vSphere en cliquant sur **LANCER VSPHERE CLIENT** ou accédez à **VSPHERE MANAGEMENT NETWORK** et cliquez sur le nom de domaine complet de **vCenter Server Appliance** .



4. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter indiquées à l'étape 2 de cette procédure.



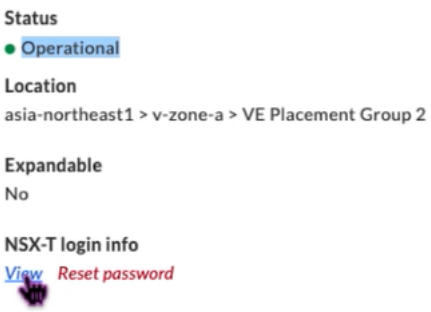
5. Dans le client vSphere, vous pouvez vérifier les hôtes ESXi que vous avez créés sur le portail GCVE.



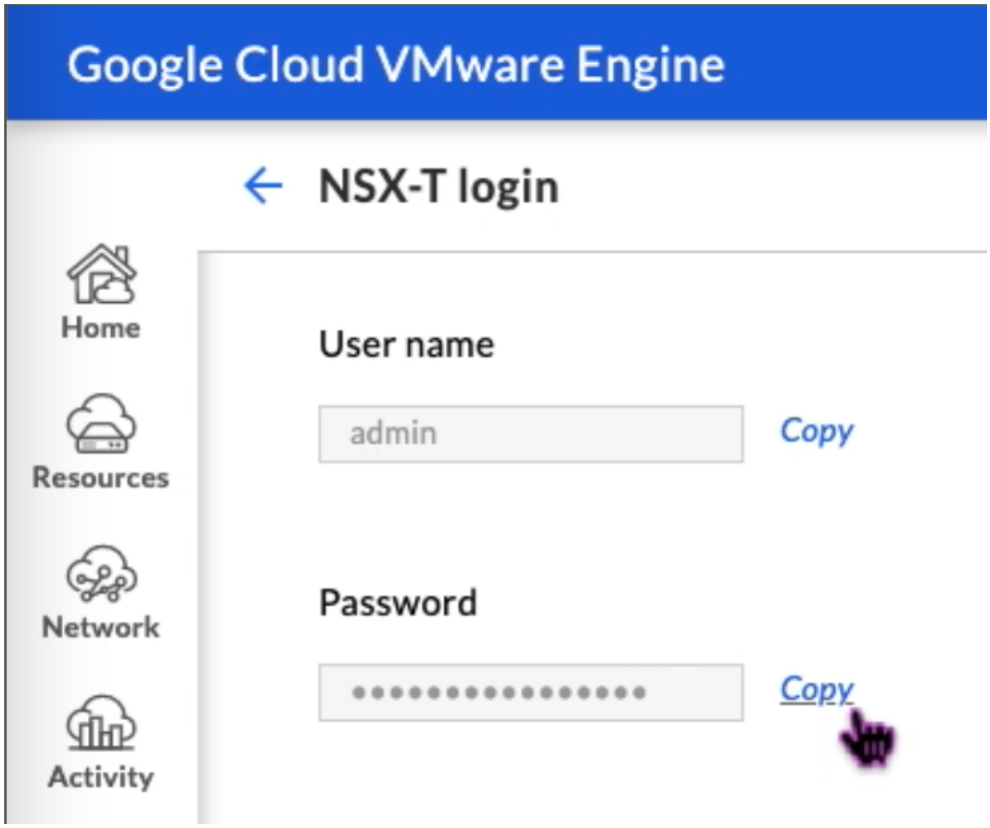
Création d'un segment NSX-T dans le portail GCVE NSX-T

Vous pouvez créer et configurer un segment NSX-T à partir de NSX Manager dans la console Google Cloud VMware Engine. Ces segments sont connectés à la passerelle de niveau 1 par défaut, et les charges de travail de ces segments sont connectées Est-Ouest et Nord-Sud. Une fois que vous avez créé le segment, il s'affiche dans vCenter.

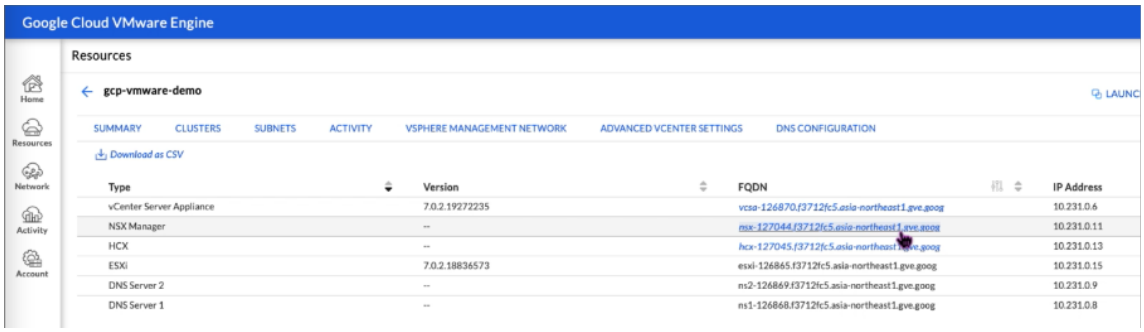
1. Dans votre cloud privé GCVE, sous **Résumé -> Informations de connexion NSX-T**, sélectionnez **Afficher**.



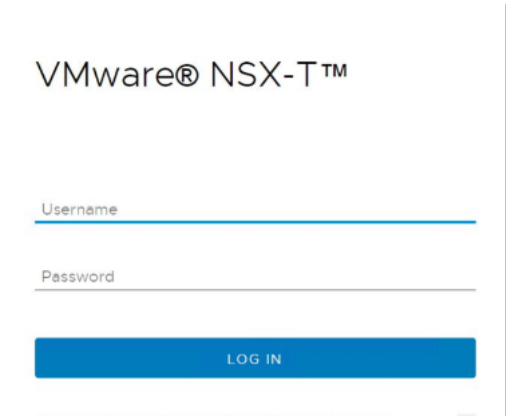
2. Prenez note des informations d'identification de la NSX-T.



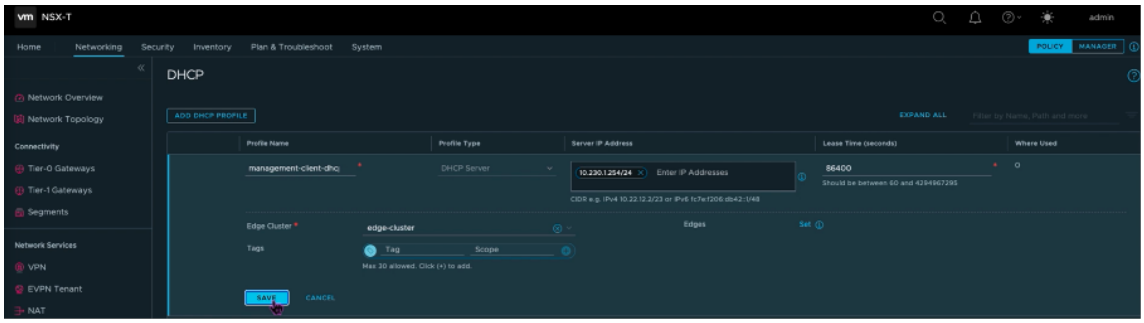
3. Lancez NSX Manager en accédant à **VSPHERE MANAGEMENT NETWORK** et en cliquant sur le nom de domaine complet de **NSX Manager** .



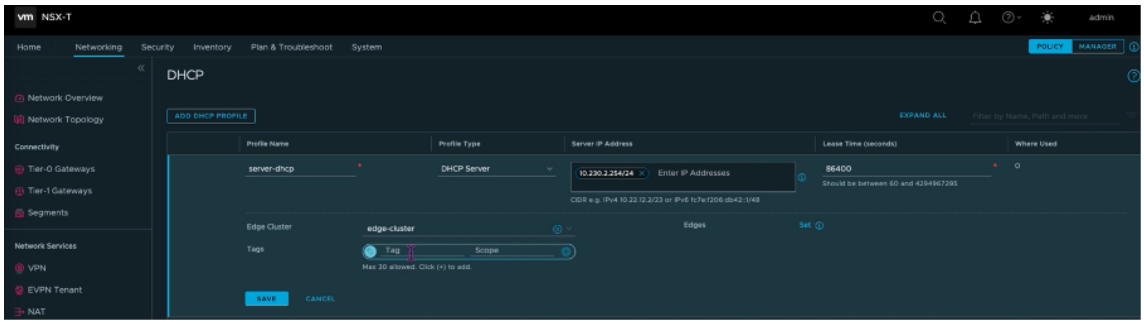
4. Connectez-vous à NSX Manager à l'aide des informations d'identification indiquées à l'étape 2 de cette procédure.



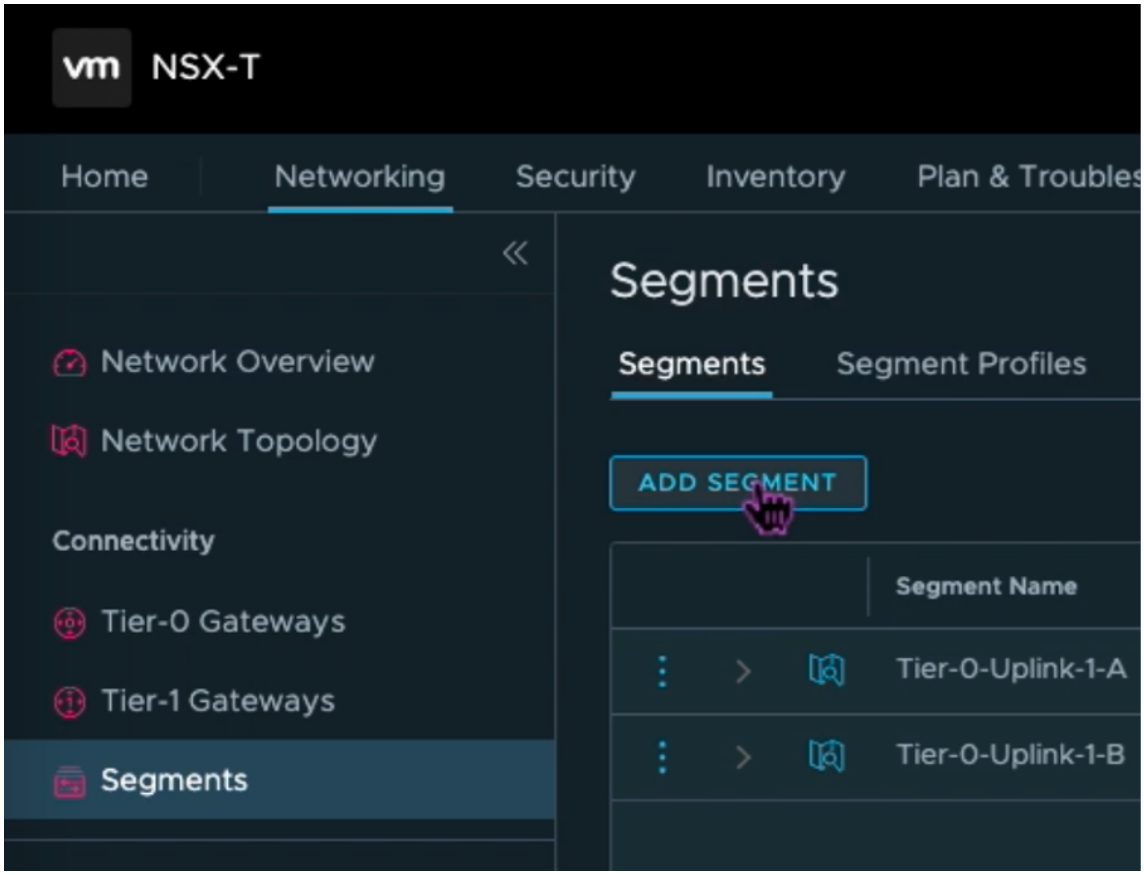
5. Configurez le service DHCP pour les nouveaux segments ou sous-réseaux.
6. Avant de créer un sous-réseau, configurez un service DHCP.
7. Dans NSX-T, accédez à **Réseau > DHCP**. Le tableau de bord réseau indique que le service crée une passerelle de niveau 0 et une passerelle de niveau 1.
8. Pour commencer à approvisionner un serveur DHCP, cliquez sur **Ajouter un profil DHCP**.
9. Dans le champ Nom DHCP, entrez le nom du profil **Client-Management** .
10. Sélectionnez le **serveur DHCP** comme type de profil.
11. Dans la colonne **Adresse IP du serveur**, indiquez une plage d'adresses IP du service DHCP.
12. Sélectionnez votre **Edge Cluster**.
13. Cliquez sur **Enregistrer** pour créer le service DHCP.



14. Répétez les étapes 6 à 13 pour la plage DHCP du serveur.



15. Créez deux segments distincts : l'un pour les interfaces client et de gestion, et l'autre pour les interfaces serveur.
16. Dans NSX-T, accédez à **Mise en réseau > Segments**.
17. Cliquez sur **Add Segment**.

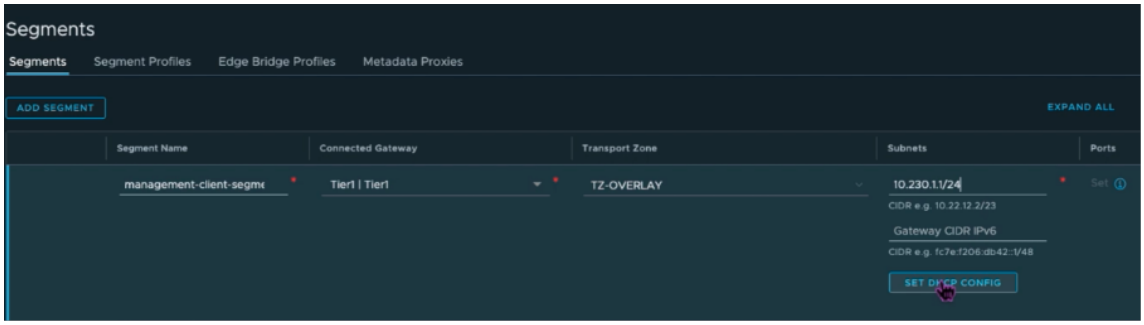


18. Dans le champ **Nom du segment**, entrez le nom de votre segment **Gestion des clients** .
19. Dans la liste des **passerelles connectées**, sélectionnez **Tier1** pour vous connecter à la passerelle de niveau 1.

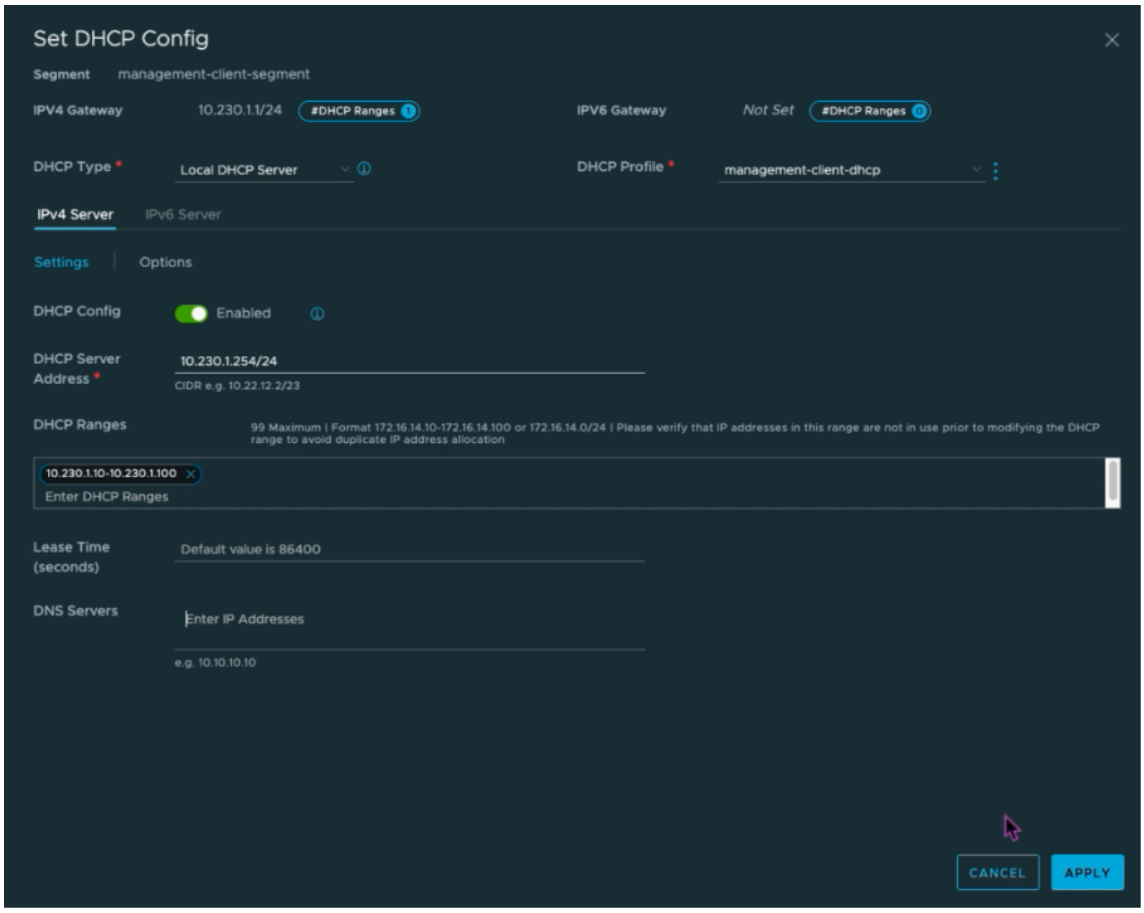
Dans la liste des **zones de transport**, sélectionnez **TZ-OVERLAY

Superposition.**

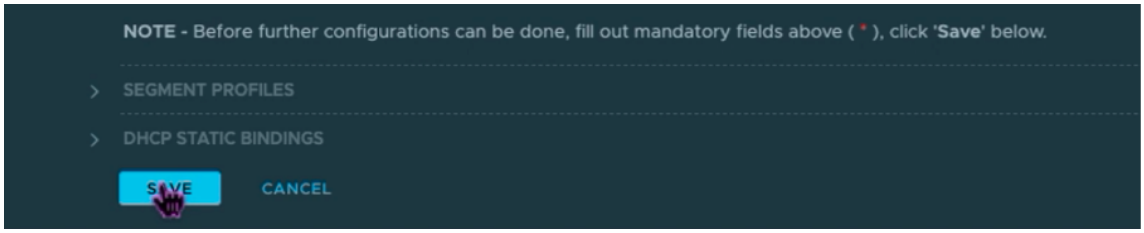
20.
21. Dans la colonne **Sous-réseaux**, entrez la plage de sous-réseaux. Spécifiez la plage de sous-réseaux avec **.** 1 comme dernier octet. Par exemple, 10.12.2.1/24.

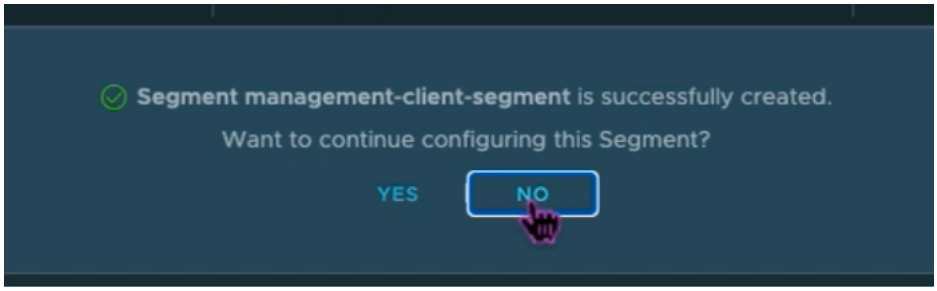


22. Cliquez sur **Définir la configuration DHCP**et entrez des valeurs pour le champ **Plages DHCP** .



23. Cliquez sur **Appliquer** pour enregistrer votre configuration DHCP.
24. Cliquez sur **Enregistrer**.





25. Répétez également les étapes 17 à 24 pour le segment de serveur.
26. Vous pouvez désormais sélectionner ces segments de réseau dans vCenter lors de la création d'une machine virtuelle.

Pour plus d'informations, voir Création de votre premier sous-réseau.

Installation d'une instance NetScaler VPX sur le cloud VMware

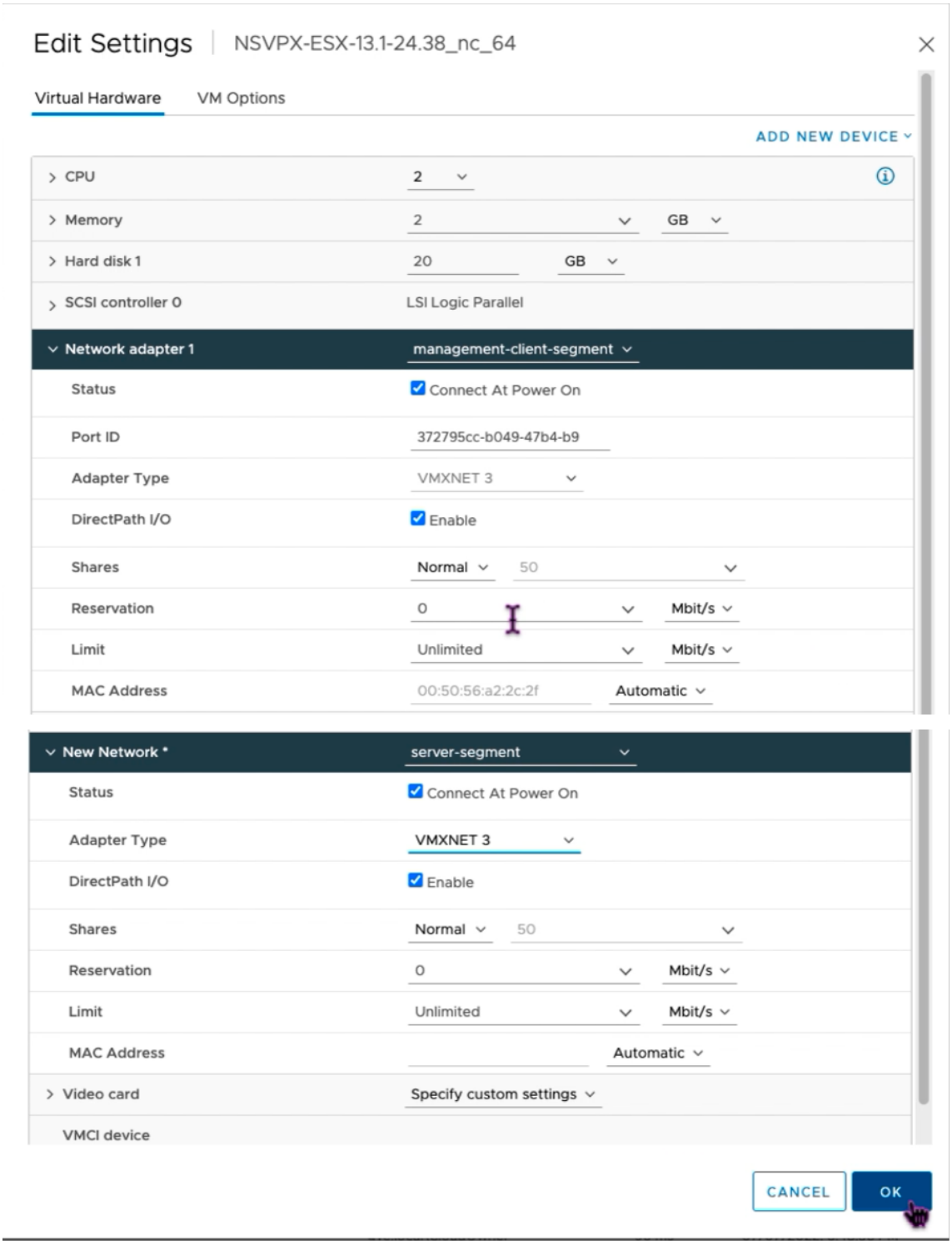
Après avoir installé et configuré Private Cloud sur GCVE, vous pouvez utiliser le vCenter pour installer des appliances virtuelles sur VMware Engine. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de ressources disponibles sur le cloud privé.

Pour installer des instances NetScaler VPX sur un cloud privé, effectuez ces étapes sur un poste de travail connecté à un VPN point à site de cloud privé :

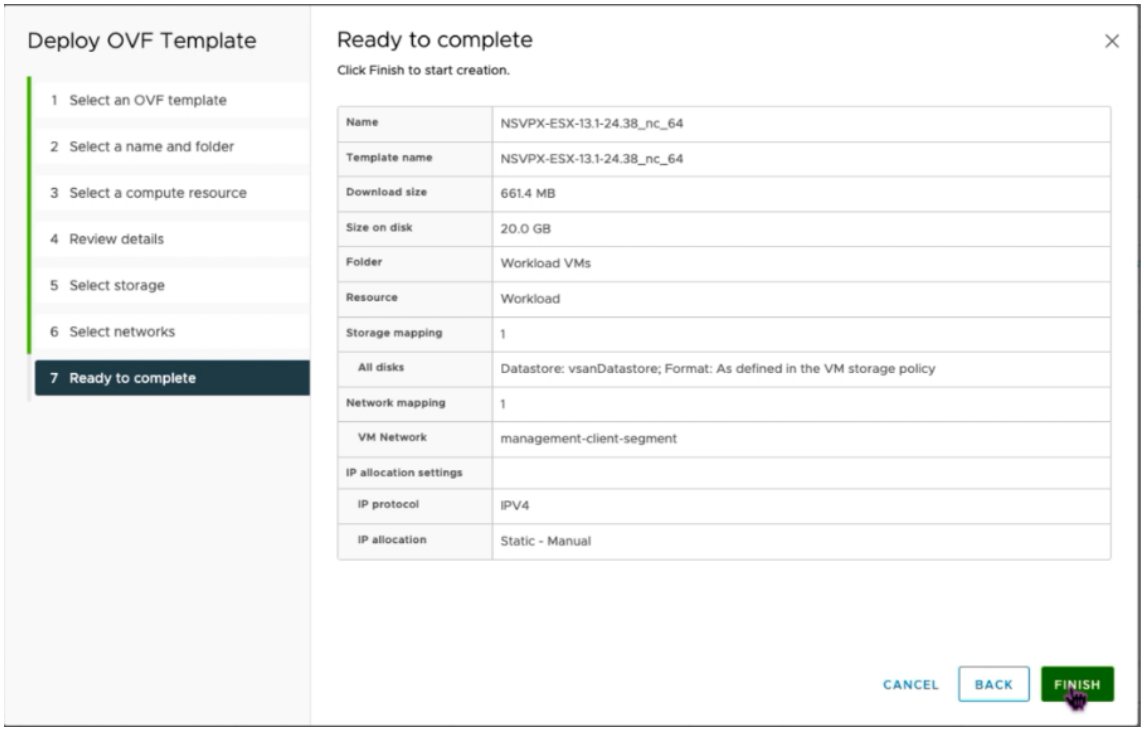
1. Téléchargez les fichiers de configuration de l'instance NetScaler VPX pour l'hôte ESXi depuis le site de téléchargement de NetScaler.
2. Ouvrez VMware vCenter dans un navigateur connecté à votre VPN point à site de cloud privé.
3. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. Dans la boîte de dialogue **Déployer un modèle OVF**, dans le champ **Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers d'installation de l'instance NetScaler VPX, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.

   > **Remarque :**
   >
   > Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000. La disponibilité de l'interface VMXNET3 est limitée par l'infrastructure GCP et peut ne pas être disponible dans Google Cloud VMware Engine.

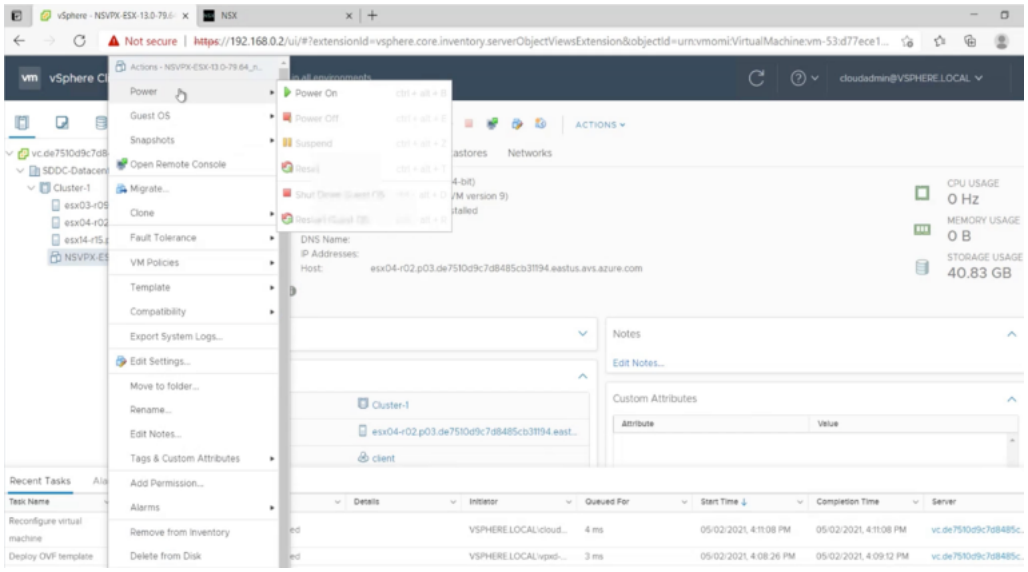
6. Mappez les réseaux affichés dans le modèle OVF du dispositif virtuel aux réseaux que vous avez configurés sur NSX-T Manager. Cliquez sur **OK**.



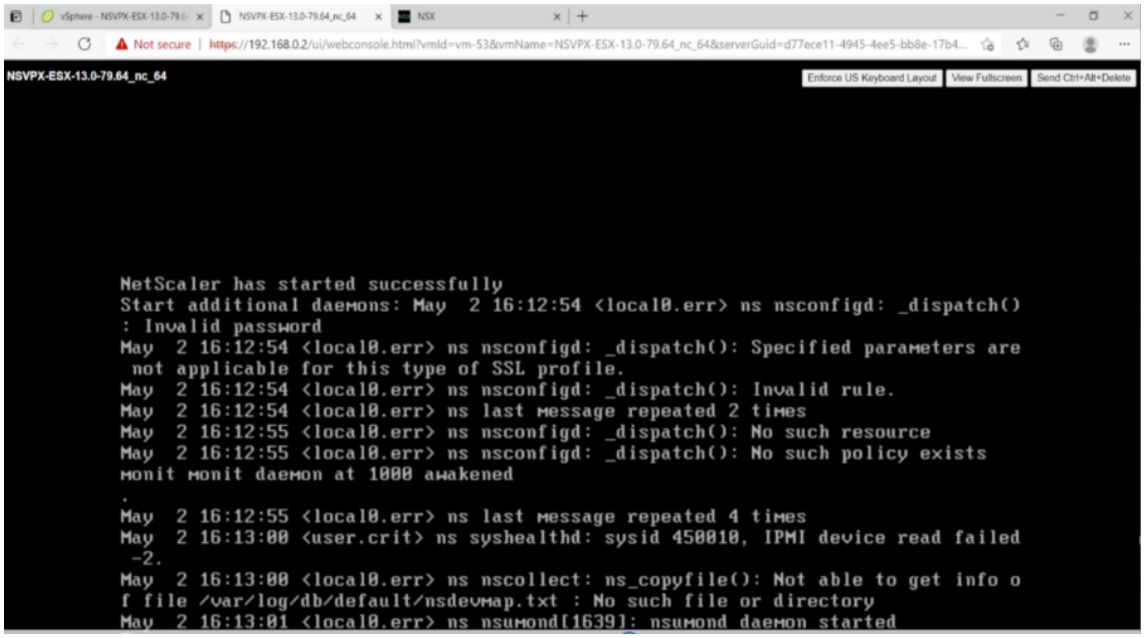
7. Cliquez sur **Terminer** pour commencer à installer une appliance virtuelle sur le cloud VMware.



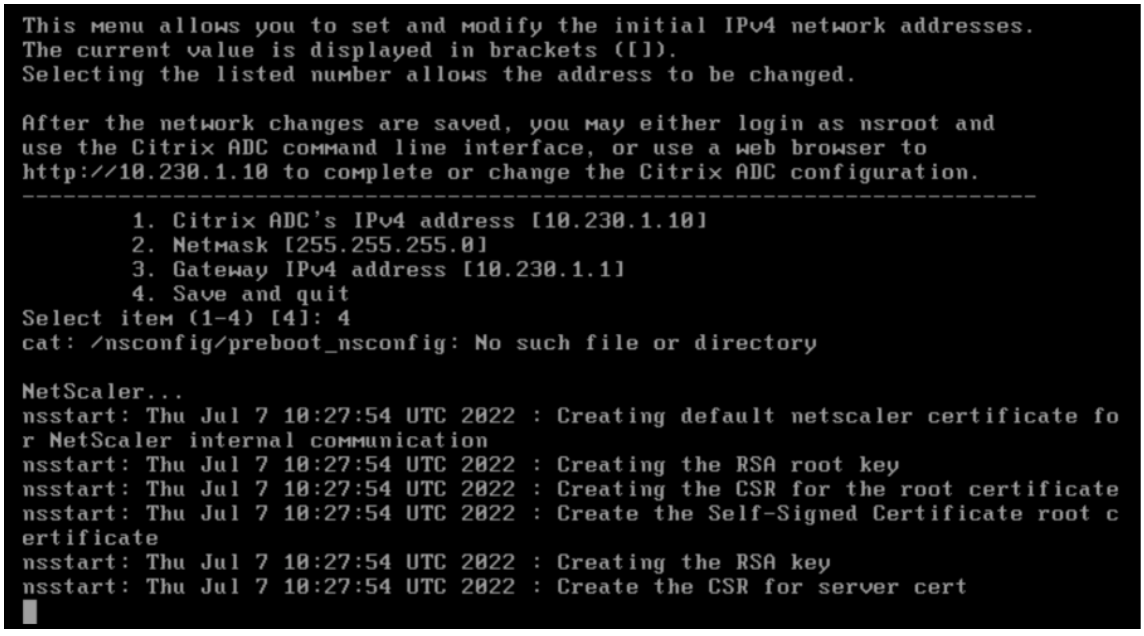
8. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Console** pour émuler un port de console. Cliquez sur l'onglet **Lancer la console Web** pour émuler un port de console.



9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.



10. Lors du premier démarrage, définissez l'adresse IP de gestion et la passerelle pour l'instance ADC.



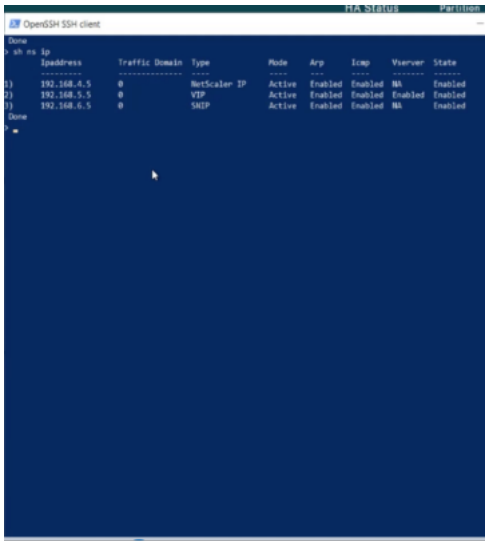
11. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l'interface de ligne de commande :

```
ssh nsroot@<management IP address>
```

Exemple

```
ssh nsroot@10.230.1.10
```


12. Vous pouvez vérifier la configuration ADC à l'aide de la `show ns ip` commande.

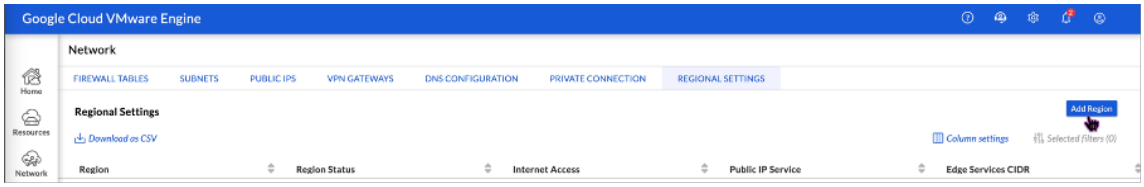


Attribuer une adresse IP publique à une instance NetScaler VPX sur le cloud VMware

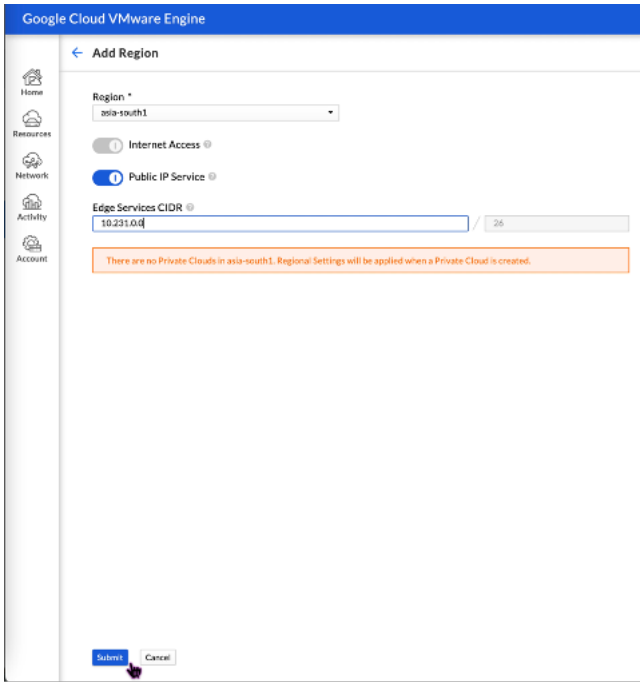
Après avoir installé et configuré l'instance NetScaler VPX sur GCVE, vous devez attribuer une adresse IP publique à l'interface client. Avant d'attribuer des adresses IP publiques à vos machines virtuelles, assurez-vous que le service IP public est activé pour votre région Google Cloud.

Pour activer le service IP public pour une nouvelle région, procédez comme suit :

1. Sur la console GCVE, accédez à **Réseau > PARAMÈTRES RÉGIONAUX > Ajouter une région**.



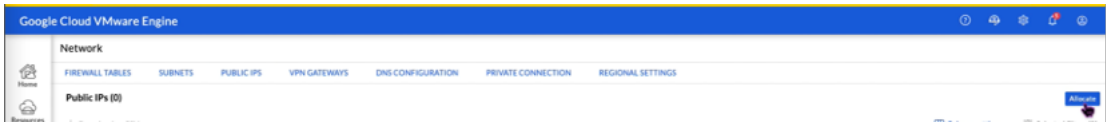
2. Sélectionnez votre région et activez l'**accès à Internet** et le **service IP public**.
3. Attribuez un CIDR Edge Services en vous assurant que la plage d'adresses CIDR ne chevauche aucun de vos sous-réseaux GCP/GCVE locaux ou autres (réseaux virtuels).



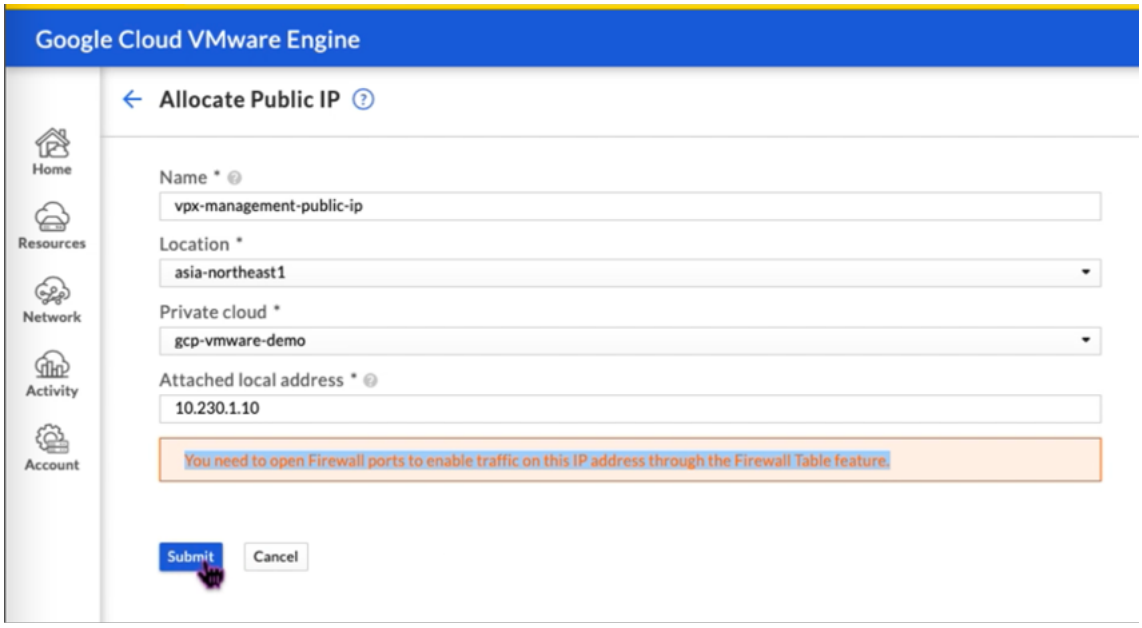
4. Le service IP public sera activé pour la région sélectionnée dans quelques minutes.

Pour attribuer une adresse IP publique à l'interface client sur l'instance NetScaler VPX sur GCVE, effectuez ces étapes sur le portail GCVE :

1. Sur la console GCVE, accédez à **Réseau > IP PUBLIC > Allouer**.



2. Entrez un nom pour l'adresse IP publique. Sélectionnez votre région et sélectionnez le cloud privé dans lequel l'adresse IP sera utilisée.
3. Fournissez l'adresse IP privée de l'interface sur laquelle vous souhaitez que l'adresse IP publique soit mappée. Il s'agira de l'**adresse IP privée** de votre interface **client** .
4. Cliquez sur **Envoyer**.



5. L'adresse IP publique est prête à être utilisée en quelques minutes.
6. Vous devez ajouter des règles de pare-feu pour autoriser l'accès à l'IP publique avant de pouvoir l'utiliser. Pour plus d'informations, consultez la section Règles de pare-feu.

Ajouter un service GCP Autoscaling principal

October 17, 2024

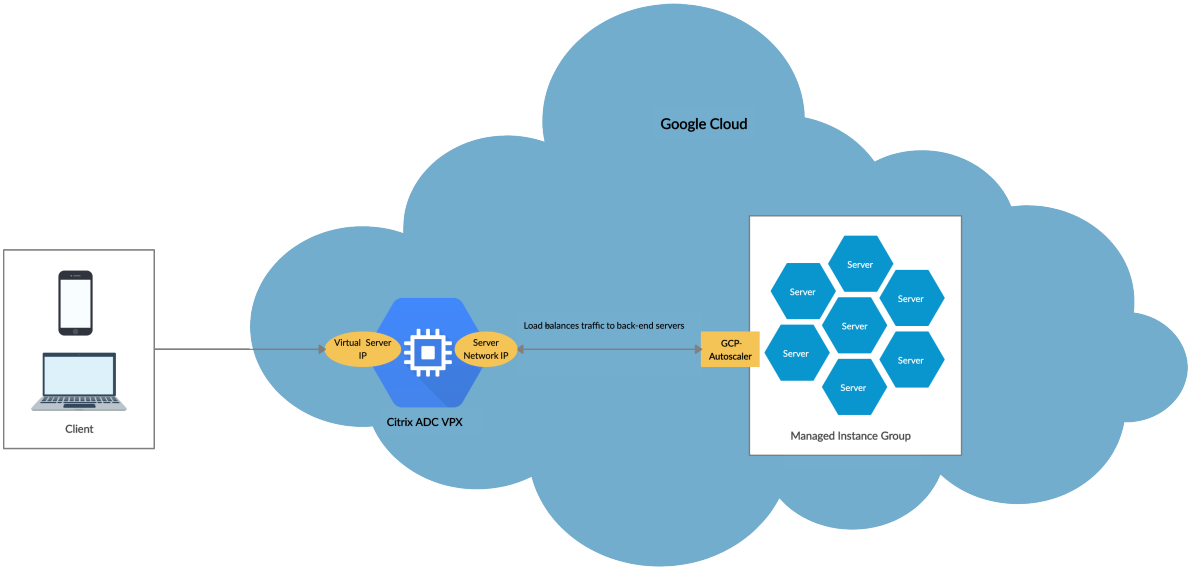
L'hébergement efficace des applications dans le cloud nécessite une gestion simple et rentable des ressources, en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources du réseau. Lorsque la demande diminue, vous devez réduire vos dépenses pour éviter les coûts inutiles liés à la sous-utilisation des ressources. Pour minimiser le coût d'exécution de l'application, vous devez surveiller en permanence le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Intégrée au service GCP Autoscaling, l'instance NetScaler VPX offre les avantages suivants :

- **Équilibrage et gestion de la charge** : configure automatiquement les serveurs pour qu'ils puissent évoluer vers le haut et vers le bas, en fonction de la demande. L'instance VPX détecte automatiquement les groupes d'instances gérés dans le sous-réseau principal et vous permet de sélectionner les groupes d'instances gérés pour équilibrer la charge. Les adresses IP virtuelles et de sous-réseau sont configurées automatiquement sur l'instance VPX.

- **Haute disponibilité** : détecte les groupes d'instances gérés qui couvrent plusieurs zones et les serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs principaux situés dans les mêmes groupes de placement
  - Serveurs dorsaux sur différentes zones

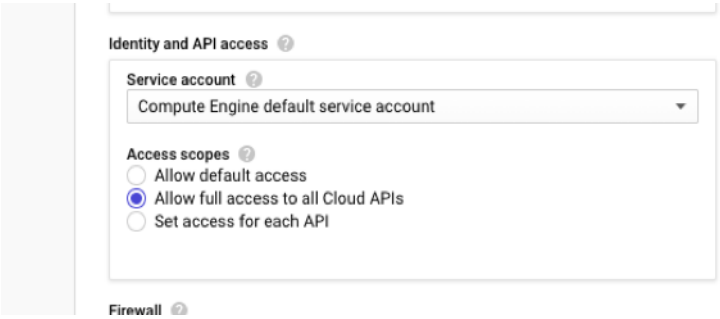
Ce diagramme illustre le fonctionnement du service GCP Autoscaling dans une instance NetScaler VPX agissant en tant que serveur virtuel d'équilibrage de charge.



Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance NetScaler VPX, vous devez effectuer les tâches suivantes.

- Créez une instance NetScaler VPX sur GCP en fonction de vos besoins.
  - Pour plus d'informations sur la création d'une instance NetScaler VPX, consultez Déployer une instance NetScaler VPX sur Google Cloud Platform.
  - Pour plus d'informations sur le déploiement d'instances VPX en mode HA, consultez Déployer une paire haute disponibilité VPX sur Google Cloud Platform.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

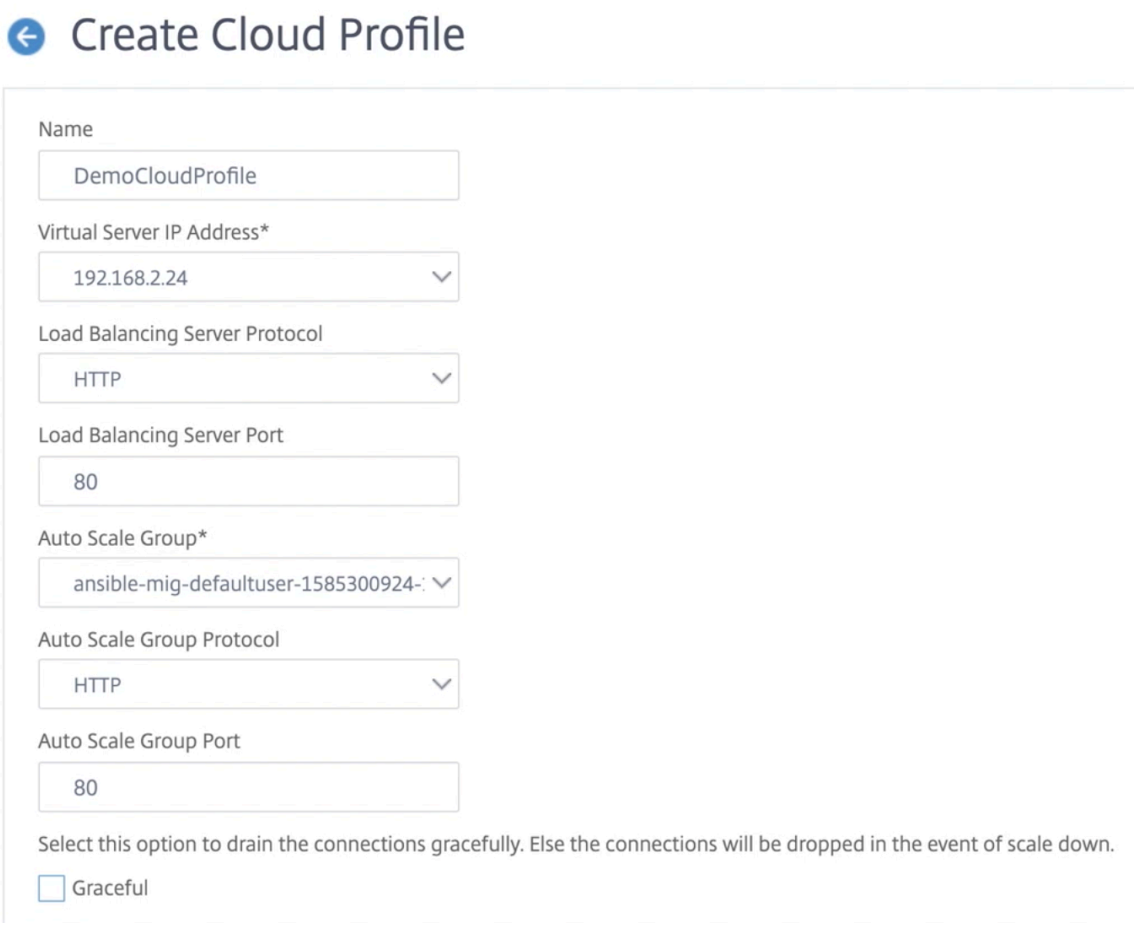
```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.instances.get",
"compute.instanceGroupManagers.get",
"compute.instanceGroupManagers.list",
"compute.zones.list",
"logging.sinks.create",
"logging.sinks.delete",
"logging.sinks.get",
"logging.sinks.list",
"logging.sinks.update",
"pubsub.subscriptions.consume",
"pubsub.subscriptions.create",
"pubsub.subscriptions.delete",
"pubsub.subscriptions.get",
"pubsub.topics.attachSubscription",
"pubsub.topics.create",
"pubsub.topics.delete",
"pubsub.topics.get",
"pubsub.topics.getIamPolicy",
"pubsub.topics.setIamPolicy",
]
```

- Pour configurer Autoscaling, assurez-vous que les éléments suivants sont configurés :
  - Modèle d'instance
  - Groupe d'instances géré
  - Politique de mise à l'échelle automatique

Ajouter le service GCP Autoscaling à une instance NetScaler VPX

Vous pouvez ajouter le service Autoscaling à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le service Autoscaling à l'instance VPX :

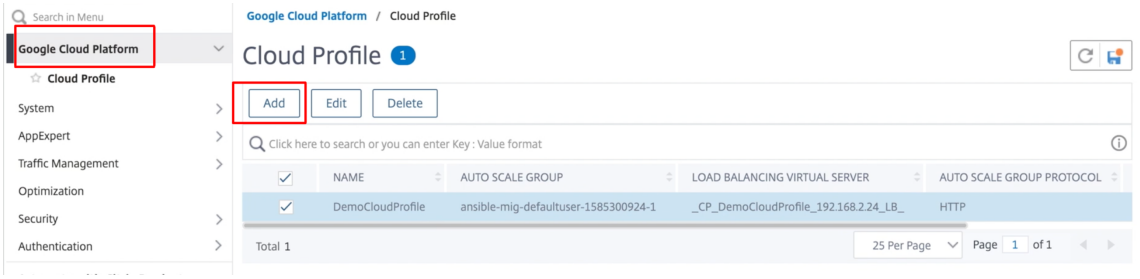
1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour `nsroot`.
2. Lorsque vous vous connectez à l'instance NetScaler VPX pour la première fois, la page Cloud Profile par défaut s'affiche. Sélectionnez le groupe d'instances géré par GCP dans le menu déroulant et cliquez sur **Créer** pour créer un profil cloud.



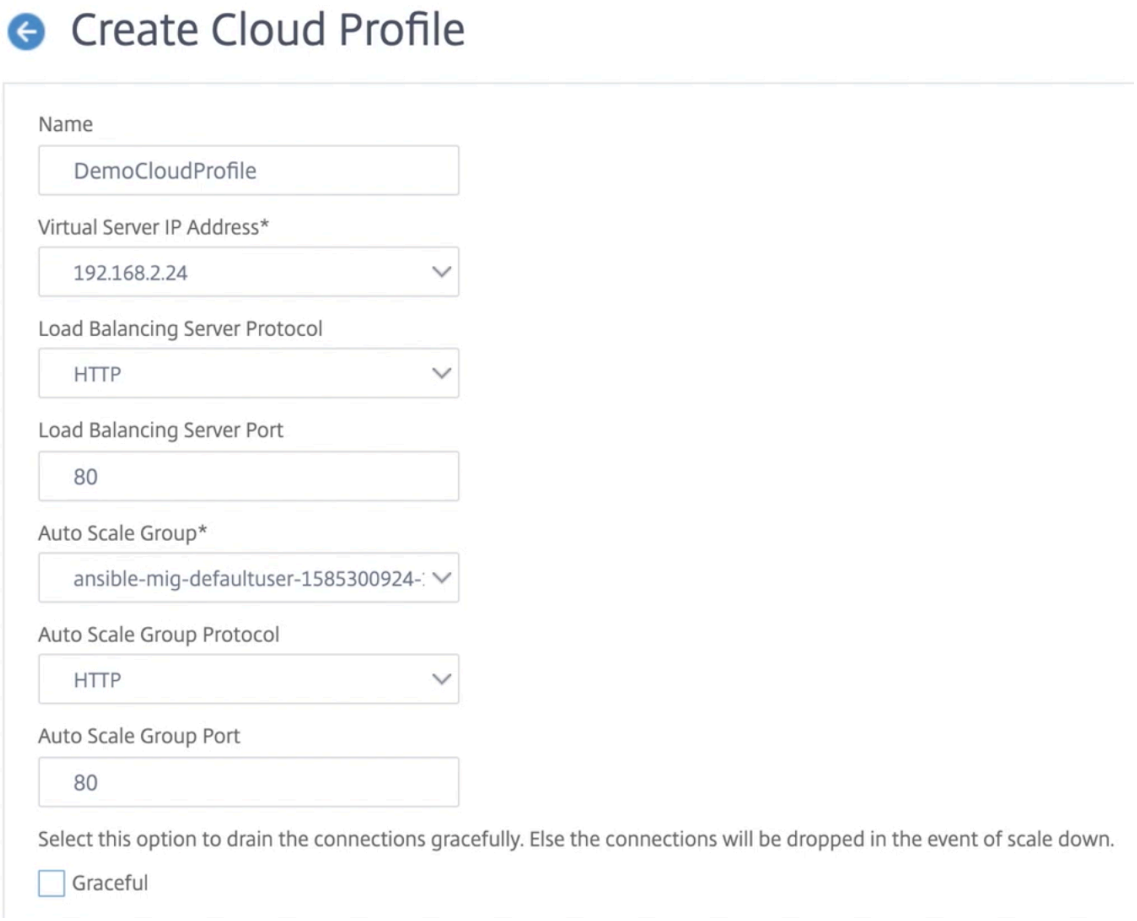
- Le champ **Adresse IP du serveur virtuel** est automatiquement renseigné à partir de toutes les adresses IP associées aux instances.
- Le **groupe Autoscale** est prérempli à partir du groupe d'instances géré configuré sur votre compte GCP.
- Lorsque vous sélectionnez le **protocole de groupe de mise** à l'**échelle automatique et le port de groupe**de mise à l'échelle automatique, assurez-vous que vos serveurs écoutent le protocole et les ports configurés. Liez le moniteur approprié au groupe de services. Par défaut, le moniteur TCP est utilisé.
- Décochez la case **Graceful** car elle n'est pas prise en charge.

> **Remarque :**
>
> Pour le protocole SSL Autoscaling, une fois le profil cloud créé, le serveur virtuel ou le groupe de services d'équilibrage de charge est hors service en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.

3. Après la première connexion, si vous souhaitez créer un profil cloud, dans l'interface graphique, accédez à **Système > Google Cloud Platform > Profil cloud** et cliquez sur **Ajouter**.

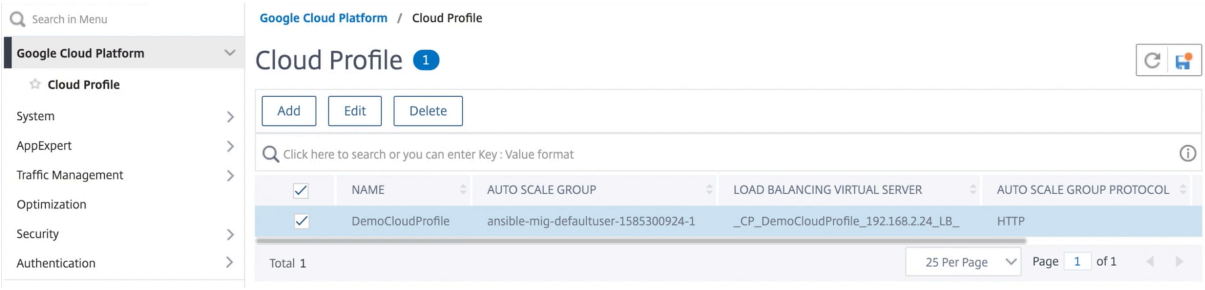


La page de configuration de **Create Cloud Profile** s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services dont les membres sont les serveurs du groupe d'instances géré. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

> **Remarque :**
>
> À partir de la version 13.1-42.x de NetScaler, vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même groupe d'instances géré dans GCP. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.



Support de dimensionnement VIP pour l'instance NetScaler VPX sur GCP

October 17, 2024

Une appliance NetScaler se trouve entre les clients et les serveurs, de sorte que les demandes des clients et les réponses du serveur passent par elle. Dans une installation standard, les serveurs virtuels configurés sur l'appliance fournissent des points de connexion que les clients utilisent pour accéder aux applications derrière l'appliance. Le nombre d'adresses IP virtuelles (VIP) publiques nécessaires pour un déploiement varie au cas par cas.

L'architecture GCP limite chaque interface de l'instance à connecter à un VPC différent. Un VPC sur GCP est un ensemble de sous-réseaux, et chaque sous-réseau peut s'étendent sur plusieurs zones d'une région. De plus, GCP impose la limitation suivante :

- Il existe un mappage 1:1 du nombre d'adresses IP publiques au nombre de cartes réseau. Une seule adresse IP publique peut être attribuée à une carte réseau.
- Un maximum de 8 cartes réseau peuvent être attachées à un type d'instance de capacité supérieure.

Par exemple, une instance n1-standard-2 ne peut avoir que 2 cartes réseau, et les VIP publics pouvant être ajoutés sont limités à 2. Pour plus d'informations, consultez Quotas de ressources VPC.

Pour obtenir des échelles plus élevées d'adresses IP virtuelles publiques sur une instance NetScaler VPX, vous pouvez configurer les adresses VIP dans le cadre des métadonnées de l'instance. L'instance NetScaler VPX utilise en interne les règles de transfert fournies par le GCP pour réaliser le dimensionnement VIP. L'instance NetScaler VPX fournit également une haute disponibilité aux VIP configurés. Une fois que vous avez configuré les adresses VIP dans le cadre des métadonnées, vous pouvez configurer un serveur virtuel LB à l'aide de la même adresse IP que celle utilisée pour créer les règles de transfert. Ainsi, nous pouvons utiliser des règles de transfert pour atténuer les limites d'échelle liées à l'utilisation d'adresses VIP publiques sur une instance NetScaler VPX sur GCP.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Pour plus d'informations sur HA, voir Haute disponibilité.

Points à noter

- Google facture des frais supplémentaires pour chaque règle de transfert d'adresse IP virtuelle. Le coût réel dépend du nombre d'entrées créées. Le coût associé est disponible dans les documents de tarification de Google.
- Les règles de transfert ne s'appliquent qu'aux VIP publics. Vous pouvez utiliser des adresses IP d'alias lorsque le déploiement a besoin d'adresses IP privées en tant que VIP.
- Vous pouvez créer des règles de transfert uniquement pour les protocoles qui nécessitent le serveur virtuel LB. Les VIP peuvent être créés, mis à jour ou supprimés à la volée. Vous pouvez également ajouter un nouveau serveur virtuel d'équilibrage de charge avec la même adresse VIP, mais avec un protocole différent.

Avant de commencer

- L'instance NetScaler VPX doit être déployée sur GCP.
- L'adresse IP externe doit être réservée. Pour plus d'informations, voir Réservation d'une adresse IP externe statique.
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]
```

- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Si vous utilisez la mise à l'échelle VIP sur une instance VPX autonome, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
```



```
    "compute.forwardingRules.list",
    "compute.instances.use",
    "compute.subnetworks.use",
    "compute.targetInstances.create",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    ]
```

- Si vous utilisez la mise à l'échelle VIP en mode haute disponibilité, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
    REQUIRED_IAM_PERMS = [
    "compute.addresses.get",
    "compute.addresses.list",
    "compute.addresses.use",
    "compute.forwardingRules.create",
    "compute.forwardingRules.delete",
    "compute.forwardingRules.get",
    "compute.forwardingRules.list",
    "compute.forwardingRules.setTarget",
    "compute.instances.use",
    "compute.instances.get",
    "compute.instances.list",
    "compute.instances.setMetadata",
    "compute.subnetworks.use",
    "compute.targetInstances.create",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.zones.list",
    ]
```

> **Remarque :**
>
> En mode haute disponibilité, si votre compte de service n'a pas de rôle de propriétaire ou d'éditeur, vous devez ajouter le **rôle d'utilisateur du compte de service** à votre compte de service.

Configurer des adresses IP externes pour le dimensionnement VIP sur une instance NetScaler VPX

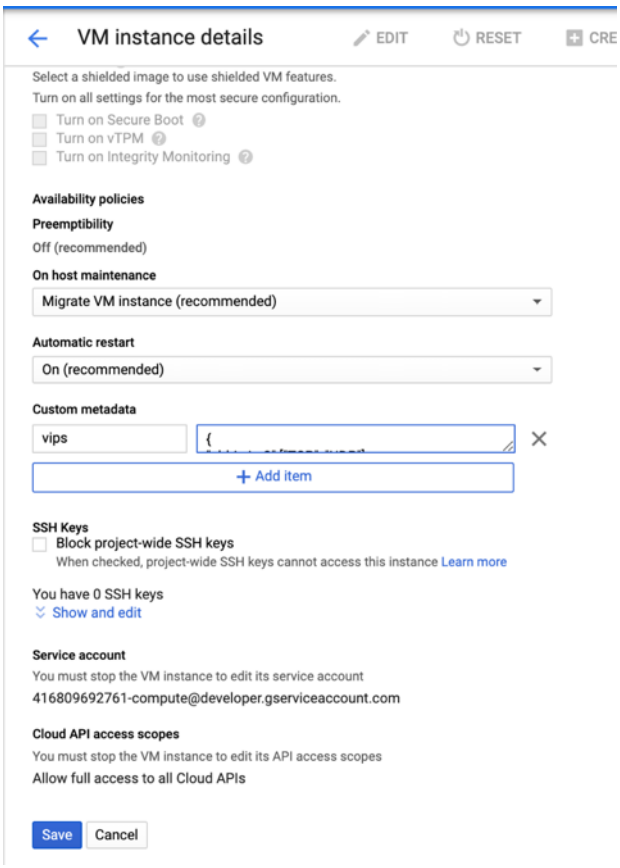
1. Dans la console Google Cloud, accédez à la page **Instances de machine virtuelle** .
2. Créez une nouvelle instance de machine virtuelle ou utilisez une instance existante.
3. Cliquez sur le nom de l'instance. Sur la page des **détails de l'instance de machine virtuelle**, cliquez sur **Modifier**.
4. Mettez à jour les **métadonnées personnalisées** en saisissant ce qui suit :
    - Clé = VIP

- Valeur = Fournir une valeur au format JSON suivant :

  { “Name of external reserved IP”: [list of protocols], }

GCP prend en charge les protocoles suivants :

- AH
- ESP
- ICMP
- SCT
- TCP
- UDP



Pour plus d’informations, voir Métadonnées personnalisées.

Exemple de métadonnées personnalisées :

{ “external-ip1-name”:[“TCP”, “UDP”], “external-ip2-name”:[“ICMP”, “AH”] }

Dans cet exemple, l’instance NetScaler VPX crée en interne une règle de transfert pour chaque paire de protocoles IP. Les entrées de métadonnées sont mappées aux règles de transfert. Cet exemple vous aide à comprendre le nombre de règles de transfert créées pour une entrée de métadonnées.

Quatre règles de transfert sont créées comme suit :

a) nom-ip1-externe et TCP
b) nom-ip1-externe et UDP
c) nom-ip2 externe et ICMP
d) nom-ip2 externe et AH

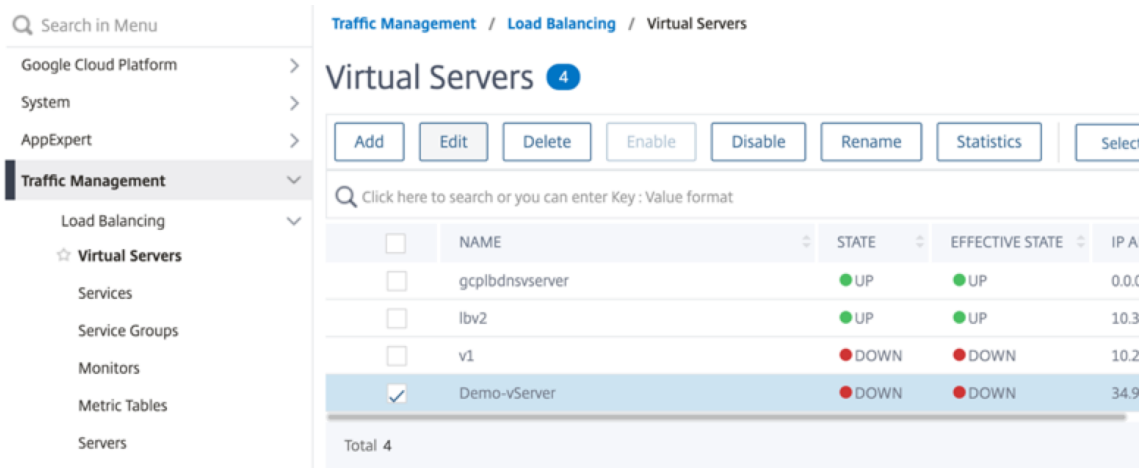
> **Remarque :**
>
> En mode HA, vous devez ajouter des métadonnées personnalisées uniquement sur l'instance principale. En cas de basculement, les métadonnées personnalisées sont synchronisées avec le nouveau serveur principal.

5. Cliquez sur **Enregistrer**.

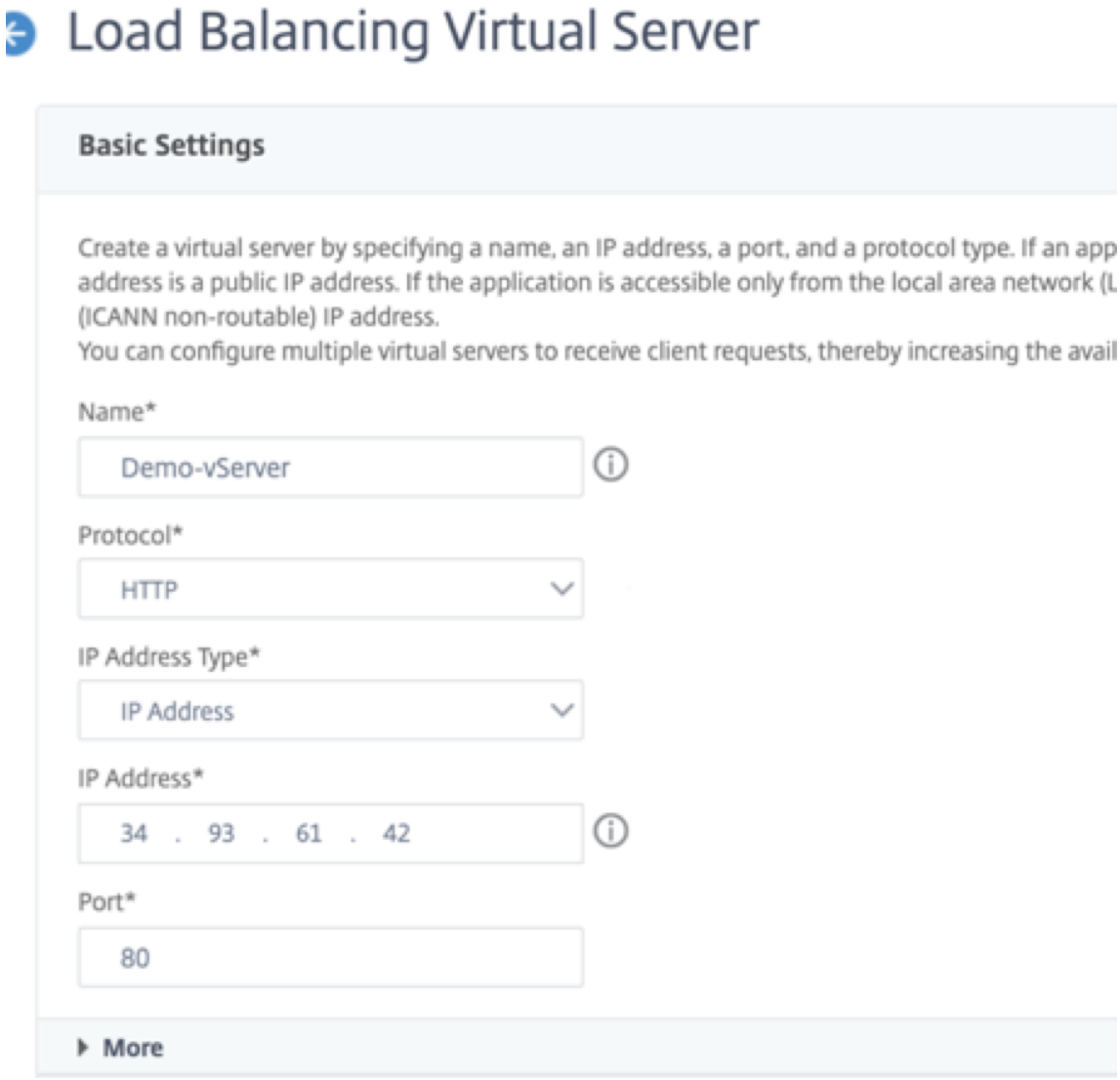
Configuration d'un serveur virtuel d'équilibrage de charge avec adresse IP externe sur une instance NetScaler VPX

Étape 1. Ajoutez un serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.

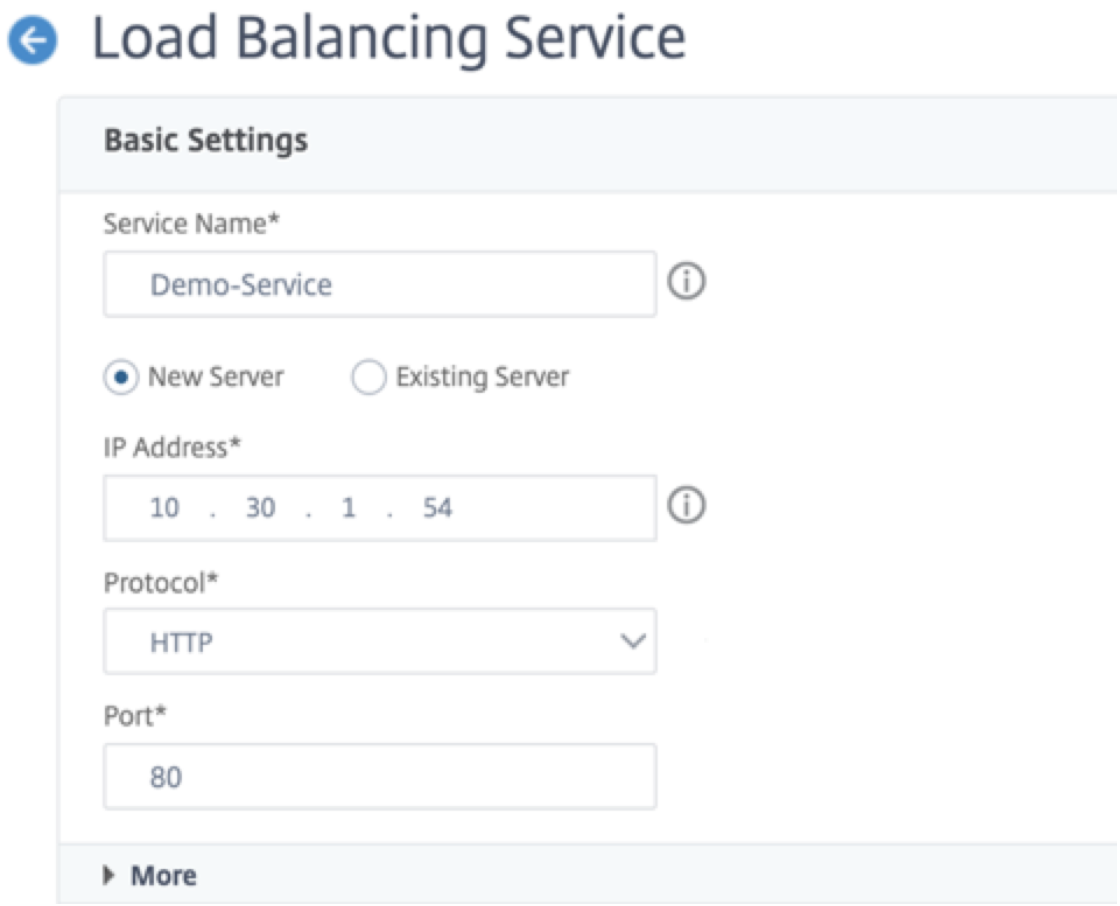


2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (adresse IP externe de la règle de transfert ajoutée en tant que VIP sur ADC) et le port, puis cliquez sur **OK**.



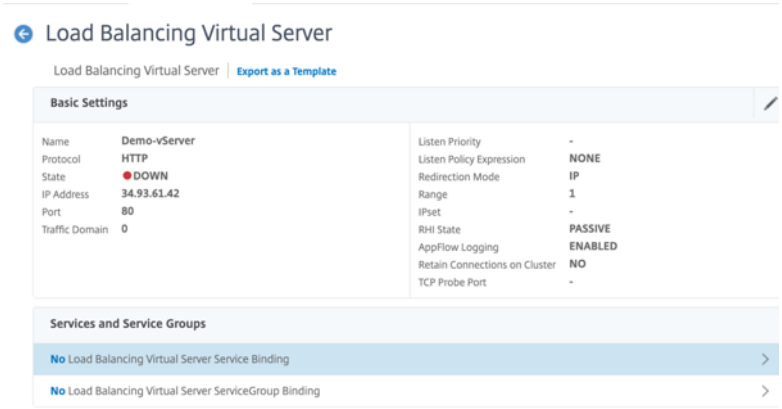
Étape 2. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

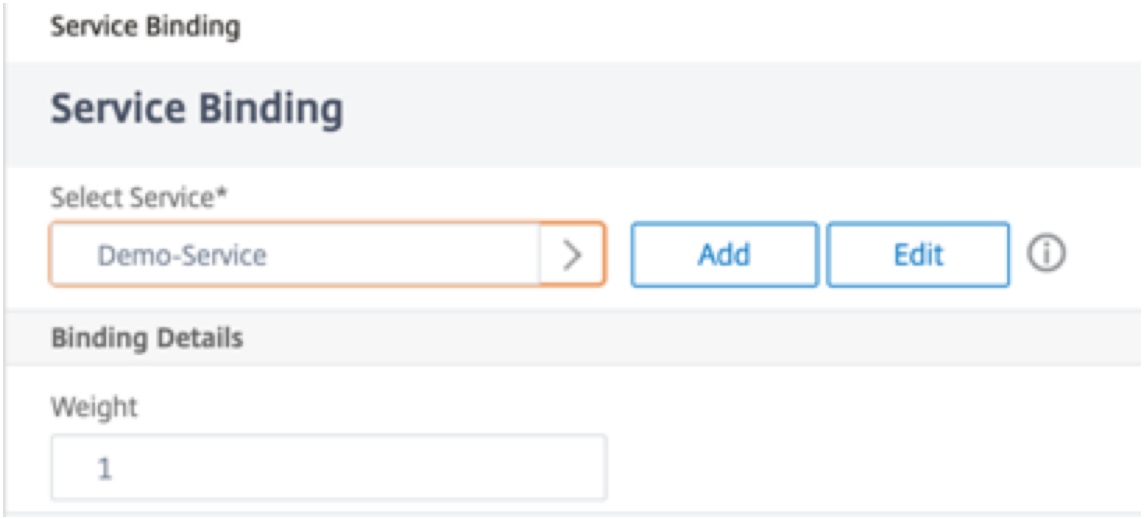


Étape 2 Ajoutez un service ou un groupe de services. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 1**, puis cliquez sur **Modifier**.
3. Dans la page **Groupes de services et de services**, cliquez sur **Liaison de service de serveur virtuel sans équilibrage de charge**.



4. Sélectionnez le service configuré à l'**étape 3**, puis cliquez sur **Lier**.



5. Enregistrez la configuration.

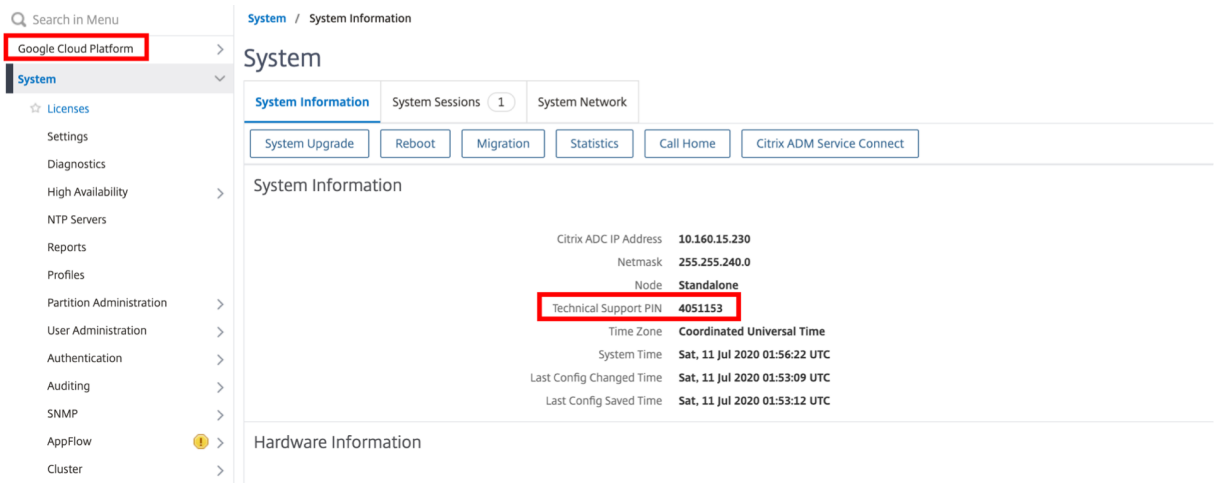
Résoudre les problèmes d'une instance VPX sur GCP

October 17, 2024

Google Cloud Platform (GCP) fournit un accès console à une instance NetScaler VPX. Vous ne pouvez déboguer que si le réseau est connecté. Pour afficher le journal système d'une instance, accédez à la console et vérifiez **les fichiers journaux système**.

NetScaler prend en charge les instances NetScaler VPX payantes (licence utilitaire avec tarif horaire) sur GCP. Pour déposer une demande d'assistance, recherchez votre numéro de compte GCP et votre code PIN d'assistance, puis appelez le support NetScaler. Il vous est demandé de fournir votre nom et votre adresse e-mail. Pour trouver le code PIN de support, connectez-vous à l'interface graphique VPX et accédez à la page **Système**.

Voici un exemple de page système montrant le code PIN de support.



Trames Jumbo sur les instances NetScaler VPX

October 17, 2024

Les appliances NetScaler VPX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9 216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille MTU IP standard de 1 500 octets.

Une appliance NetScaler peut utiliser des trames jumbo dans les scénarios de déploiement suivants :

- Jumbo à Non-Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie en tant que trames régulières.
- Non-Jumbo vers Jumbo. L'appliance reçoit les données sous forme de trames normales et les envoie sous forme de trames jumbo.
- De Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames Jumbo et les envoie sous forme de trames Jumbo.

Pour plus d'informations, consultez la sectionConfiguration de la prise en charge des Jumbo Frames sur une appliance NetScaler.

La prise en charge des trames Jumbo est disponible sur les appliances NetScaler VPX exécutées sur les plateformes de virtualisation suivantes :

- VMware ESX
- Plateforme Linux-KVM
- Citrix XenServer

- Amazon Web Services (AWS)

Les trames Jumbo sur les appliances VPX fonctionnent de la même manière que les trames Jumbo sur les appliances MPX. Pour plus d'informations sur les cadres Jumbo et leurs cas d'utilisation, consultez la section Configuration des cadres Jumbo sur des appliances MPX. Les cas d'utilisation des trames jumbo sur les appliances MPX s'appliquent également aux appliances VPX.

Configurer des trames jumbo pour une instance VPX exécutée sur VMware ESX

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur le serveur VMware ESX :

1. Définissez la MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501—9000. Utilisez l'interface de ligne de commande ou l'interface graphique pour définir la taille de la MTU. Les appliances NetScaler VPX exécutées sur VMware ESX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9 000 octets de données IP.
2. Définissez la même taille MTU sur les interfaces physiques correspondantes du serveur VMware ESX à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille du MTU sur les interfaces physiques de VMware ESX, voir http://vmware.com/.

Configurer des trames jumbo pour une instance VPX exécutée sur un serveur Linux-KVM

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur un serveur Linux-KVM :

1. Définissez le MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501 et 9216. Utilisez la CLI ou l'interface graphique NetScaler VPX pour définir la taille de la MTU.
2. Définissez la même taille de MTU sur les interfaces physiques correspondantes d'un serveur Linux-KVM à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille de la MTU sur les interfaces physiques de Linux-KVM, consultez. http://www.linux-kvm.org/

Configurer des trames jumbo pour une instance VPX exécutée sur Citrix XenServer

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur Citrix XenServer :

1. Connectez-vous au XenServer à l'aide de XenCenter.
2. Arrêtez toutes les instances VPX qui utilisent les réseaux pour lesquels le MTU doit être modifié.

3. Dans l'onglet **Réseau**, sélectionnez le réseau - réseau 0/1/2.
4. Sélectionnez **Propriétés** et modifiez MTU.

Après avoir configuré les trames jumbo sur XenServer, vous pouvez configurer les trames jumbo sur l'appliance ADC. Pour plus d'informations, consultez la sectionConfiguration de la prise en charge des Jumbo Frames sur une appliance NetScaler.

Configurer des trames jumbo pour une instance VPX exécutée sur AWS

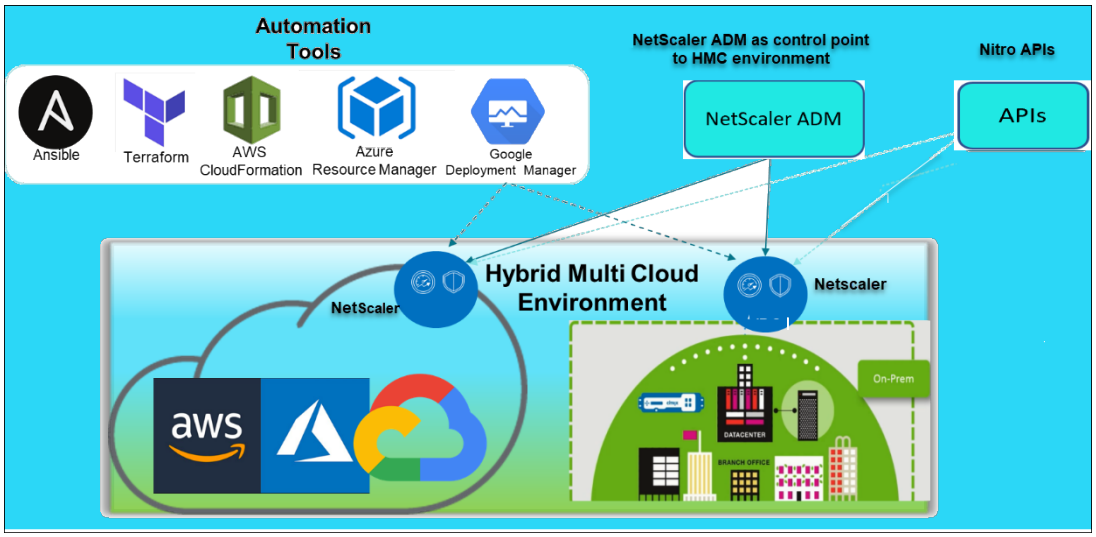
La configuration au niveau de l'hôte n'est pas requise pour VPX sur Azure. Pour configurer les Jumbo Frames sur VPX, suivez les étapes décrites dans Configuration de la prise en charge des Jumbo Frames sur uneappliance NetScaler.

Automatisez le déploiement et les configurations de NetScaler

October 17, 2024

NetScaler fournit plusieurs outils pour automatiser vos déploiements et configurations ADC. Ce document fournit un bref résumé des différents outils d'automatisation et des références aux différentes ressources d'automatisation que vous pouvez utiliser pour gérer les configurations de ADC.

L'illustration suivante fournit une vue d'ensemble de l'automatisation NetScaler dans un environnement hybride multicloud (HMC).



Automatisez NetScaler à l'aide de NetScaler ADM

NetScaler ADM agit comme un point de contrôle d'automatisation pour votre infrastructure ADC distribuée. NetScaler ADM fournit un ensemble complet de fonctionnalités d'automatisation, depuis la mise en service des appareils ADC jusqu'à leur mise à niveau. Voici les principales fonctionnalités d'automatisation d'ADM :

- Provisioning d'instances NetScaler VPX sur AWS
- Provisioning d'instances NetScaler VPX sur Azure
- StyleBooks
- Tâches de configuration
- Audit de configuration
- Mises à niveau ADC
- Gestion des certificats SSL
- Intégrations - Intégrations [GitHub](/fr-fr/citrix-application-delivery-management-service/stylebooks/impor and-synchronizing-stylebooks-from-github-repository.html), [ServiceNow](/fr-fr/citrix-application-delivery-management-service/setting-up/integrate-itsm-adapter-citrix-adm-servicenow.html), notifications d'événements

Blogs et vidéos NetScaler ADM sur l'automatisation

- Migrations d'applications à l'aide de StyleBooks
- Intégrez les configurations ADC avec CI/CD à l'aide des StyleBooks ADM
- Simplification des déploiements NetScaler dans le cloud public grâce à ADM
- 10 façons dont le service NetScaler ADM facilite les mises à niveau de NetScaler

NetScaler ADM fournit également des API pour ses différentes fonctionnalités qui intègrent NetScaler ADM et NetScaler dans le cadre de l'automatisation informatique globale. Pour plus d'informations, consultez API du service NetScaler ADM.

Automatisez NetScaler à l'aide de Terraform

Terraform est un outil qui prend l'infrastructure en tant qu'approche de code pour fournir et gérer le cloud, l'infrastructure ou le service. Les ressources NetScaler Terraform sont disponibles sur GitHub pour être utilisées. Consultez GitHub pour obtenir une documentation et une utilisation détaillées.

- Modules NetScaler Terraform pour configurer l'ADC pour divers cas d'utilisation tels que l'équilibrage de charge et le GSLB
- Scripts cloud Terraform pour déployer ADC dans AWS
- Scripts cloud Terraform pour déployer ADC dans Azure
- Scripts cloud Terraform pour déployer ADC dans GCP

- Déploiement bleu-vert à l'aide de pipelines NetScaler VPX et Azure

Blogs et vidéos sur Terraform pour l'automatisation ADC

- Automatisez vos déploiements NetScaler avec Terraform
- Provisionner et configurer ADC dans la configuration HA dans AWS à l'aide de Terraform

Automatisez NetScaler à l'aide de Consul-Terraform-Sync

Le module NetScaler Consul-Terraform-Sync (CTS) permet aux équipes d'applications d'ajouter ou de supprimer automatiquement de nouvelles instances de services dans NetScaler. Il n'est pas nécessaire d'envoyer des tickets manuels aux administrateurs informatiques ou aux équipes réseau pour apporter les modifications nécessaires aux configurations ADC.

- Module NetScaler Consul-Terraform-Sync pour l'automatisation de l'infrastructure réseau
- Webinaire conjoint entre Citrix-HashiCorp : mise en réseau dynamique avec Consul-Terraform-Sync pour Terraform Enterprise et NetScaler

Automatisez NetScaler à l'aide d'Ansible

Ansible est un outil open source de provisionnement de logiciels, de gestion de la configuration et de déploiement d'applications permettant l'infrastructure en tant que code. Les modules NetScaler Ansible et des exemples de playbooks peuvent être consultés sur GitHub. Consultez GitHub pour obtenir une documentation et une utilisation détaillées.

- Modules Ansible pour configurer l'ADC
- Documentation et guide de référence des modules ADC Ansible
- Modules Ansible pour ADM

Citrix est un partenaire certifié Ansible Automation. Les utilisateurs abonnés à Red Hat Ansible Automation Platform peuvent accéder aux collections NetScaler depuis Red HatAutomation Hub.

Blogs d'automatisation Terraform et Ansible

- Citrix nommé partenaire d'intégration HashiCorp de l'année
- Citrix est désormais un partenaire certifié Red Hat Ansible Automation Platform
- Terraform et Ansible Automation pour la mise à disposition et la sécurité des applications

Modèles de cloud public pour les déploiements ADC

Les modèles de cloud public simplifient le provisionnement de vos déploiements dans les clouds publics. Différents modèles NetScaler sont disponibles pour différents environnements. Pour plus de détails sur l'utilisation, reportez-vous aux référentiels GitHub respectifs.

CFT AWS :

- Les CFT vont provisionner NetScaler VPX sur AWS

Modèles Azure Resource Manager (ARM) :

- Modèles ARM pour provisionner NetScaler VPX sur Azure

Modèles Google Cloud Deployment Manager (GDM) :

- Modèles GDM pour provisionner NetScaler VPX sur Google

Vidéos sur les modèles

- Déployer NetScaler HA dans AWS à l'aide du modèle CloudFormation
- Déployez NetScaler HA dans les zones de disponibilité à l'aide d'AWS QuickStart
- Déploiement de NetScaler HA dans GCP à l'aide de modèles GDM

API NITRO

Le protocole NetScaler NITRO vous permet de configurer et de surveiller par programmation l'appliance NetScaler à l'aide des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. Pour les applications qui doivent être développées en Java, .NET ou Python, les API NITRO sont exposées par le biais de bibliothèques pertinentes qui sont empaquetées sous forme de kits de développement logiciel (SDK) distincts.

- Documentation de l'API NITRO
- Exemple de configuration de cas d'utilisation d'ADC à NITRO aide de

FAQ

October 17, 2024

La section suivante vous aide à classer les questions fréquentes en fonction de Citrix Application Delivery Controller (ADC) VPX.

- Fonctionnalité et fonctionnalité
- Encryption
- Prix et emballage
- NetScaler VPX Express et essai gratuit de 90 jours
- Hyperviseur
- Planification ou dimensionnement des capacités
- Configuration système requise
- Autres FAQ techniques

Fonctionnalité et fonctionnalité

Qu'est-ce que NetScaler VPX ?

NetScaler VPX est une appliance ADC virtuelle qui peut être hébergée sur un hyperviseur installé sur des serveurs conformes aux normes du secteur.

NetScaler VPX inclut-il toutes les fonctionnalités d'optimisation des applications Web sous forme d'appliances ADC ?

Oui. NetScaler VPX inclut toutes les fonctionnalités d'équilibrage de charge, de gestion du trafic, d'accélération des applications, de sécurité des applications (y compris NetScaler Gateway et Citrix Application Firewall) et de déchargement. Pour une présentation complète des fonctionnalités de NetScaler, voir Application Delivery your way.

Le pare-feu d'applications Citrix est-il soumis à des limites lors de son utilisation sur NetScaler VPX ?

Le pare-feu d'applications Citrix sur NetScaler VPX fournit les mêmes protections de sécurité que sur les appliances NetScaler. Les performances ou le débit de Citrix Application Firewall varient selon la plateforme.

Existe-t-il des différences entre NetScaler Gateway sur NetScaler VPX et NetScaler Gateway sur des appliances NetScaler ?

Sur le plan fonctionnel, ils sont identiques. NetScaler Gateway sur NetScaler VPX prend en charge toutes les fonctionnalités de NetScaler Gateway disponibles dans la version 14.1 du logiciel NetScaler.

Toutefois, étant donné que les appliances NetScaler fournissent du matériel d'accélération SSL dédié, elles offrent une évolutivité VPN SSL supérieure à celle d'une instance NetScaler VPX.

Outre la différence évidente que NetScaler VPX peut fonctionner sur un hyperviseur, en quoi diffère-t-il des appliances physiques NetScaler ?

Il existe deux principaux domaines dans lesquels les clients constatent des différences de comportement. La première est que NetScaler VPX ne peut pas offrir les mêmes performances que de nombreuses appliances NetScaler. La seconde est que si les appliances NetScaler intègrent leurs propres fonctionnalités réseau L2, NetScaler VPX s'appuie sur l'hyperviseur pour ses services réseau L2. En général, cela ne limite pas la manière dont NetScaler VPX peut être déployé. Certaines fonctionnalités L2 configurées sur une appliance NetScaler physique peuvent devoir être configurées sur l'hyperviseur sous-jacent.

Quel est le rôle de NetScaler VPX sur le marché de la diffusion d'applications ?

NetScaler VPX change la donne sur le marché de la fourniture d'applications de la manière suivante :

- En rendant une appliance NetScaler encore plus abordable, NetScaler VPX permet à toute organisation informatique de déployer une appliance NetScaler. Il ne s'agit pas uniquement de leurs applications Web les plus critiques, mais également de toutes leurs applications Web.
- NetScaler VPX permet aux clients de faire davantage converger la mise en réseau et la virtualisation au sein de leurs centres de données. NetScaler VPX ne peut pas uniquement être utilisé pour optimiser les applications Web hébergées sur des serveurs virtualisés. Il permet également à la livraison d'applications Web elle-même de devenir un service virtualisé qui peut être facilement et rapidement déployé n'importe où. Les organisations informatiques utilisent les processus standard du centre de données pour des tâches telles que le provisionnement, l'automatisation et la rétrofacturation pour l'infrastructure de distribution d'applications Web.
- NetScaler VPX ouvre la voie à de nouvelles architectures de déploiement qui ne sont pas pratiques si seules des appliances physiques sont utilisées. Les appliances NetScaler VPX et NetScaler MPX peuvent être utilisées de manière standard, adaptées aux besoins individuels de chaque application respective pour gérer des actions gourmandes en processeur telles que la compression et l'inspection du pare-feu des applications. À la périphérie du datacenter, les appliances NetScaler MPX gèrent des tâches à volume élevé à l'échelle du réseau, telles que la distribution initiale du trafic, le chiffrement ou le déchiffrement SSL, la prévention des attaques par déni de service (DoS) et l'équilibrage de charge global. L'association d'appliances NetScaler MPX hautes performances à une appliance virtuelle NetScaler VPX facile à déployer apporte une flexibilité et des capacités de personnalisation inégalées aux environnements

de centres de données modernes à grande échelle, tout en réduisant les coûts globaux des centres de données.

Comment NetScaler VPX s'intègre-t-il à notre stratégie de centre de livraison Citrix ?

Avec la disponibilité de NetScaler VPX, l'ensemble de l'offre du centre de distribution Citrix est disponible sous forme d'offre virtualisée. L'ensemble du centre de mise à disposition Citrix bénéficie des puissantes fonctionnalités de gestion, de provisionnement, de surveillance et de création de rapports disponibles dans Citrix XenCenter. Cela peut être déployé rapidement dans presque n'importe quel environnement et géré de manière centralisée depuis n'importe où. Grâce à une infrastructure intégrée et virtualisée de distribution d'applications, les entreprises peuvent fournir des postes de travail, des applications client-serveur et des applications Web.

Encryption

NetScaler VPX prend-il en charge le déchargement SSL ?

Oui. NetScaler VPX Express inclut toutes les fonctionnalités de NetScaler Standard. À partir des versions 12.0-56.20 de NetScaler, Citrix a modifié le comportement de VPX Express.

Les cartes SSL tierces installées sur le serveur hébergeant NetScaler VPX accélèrent-elles le chiffrement ou le déchiffrement SSL ?

Oui. La prise en charge des cartes SSL tierces ne permet pas d'associer le NetScaler VPX à des implémentations matérielles spécifiques. Cela réduit considérablement la capacité d'une entreprise à héberger NetScaler VPX de manière flexible n'importe où dans le centre de données. Les appliances NetScaler MPX doivent être utilisées lorsqu'un débit SSL supérieur à celui fourni par NetScaler VPX est requis.

NetScaler VPX prend-il en charge les mêmes chiffrements de chiffrement que les appliances NetScaler physiques ?

VPX prend en charge tous les chiffrements de chiffrement en tant qu'appliances NetScaler physiques, à l'exception de l'ECDSA.

Quel est le débit des transactions SSL de NetScaler VPX ?

Consultez la fiche technique de NetScaler VPX pour plus d'informations sur le débit des transactions SSL.

Prix et emballage

Comment est packagé NetScaler VPX ?

La sélection de NetScaler VPX est similaire à la sélection d'appliances NetScaler. Tout d'abord, le client sélectionne l'édition NetScaler en fonction de ses exigences fonctionnelles. Le client sélectionne ensuite le niveau de bande passante NetScaler VPX spécifique en fonction de ses besoins en matière de débit. NetScaler VPX est disponible dans les éditions Standard, Advanced et Premium. NetScaler VPX propose des débits allant de 10 Mbit/s (VPX 10) à 100 Gbit/s (VPX 100G). Vous trouverez plus de détails dans la fiche technique de NetScaler VPX.

Le prix de NetScaler VPX est-il le même pour tous les hyperviseurs ?

Oui.

Les mêmes SKU NetScaler sont-ils utilisés pour VPX sur tous les hyperviseurs ?

Oui.

Une licence NetScaler VPX peut-elle être déplacée d'un hyperviseur à un autre (par exemple de VMware vers Hyper-V) ?

Oui. Les licences NetScaler VPX sont indépendantes de l'hyperviseur sous-jacent. Si vous décidez de déplacer la machine virtuelle NetScaler VPX d'un hyperviseur à un autre, il n'est pas nécessaire d'obtenir une nouvelle licence. Toutefois, il se peut que vous deviez réhéberger la licence NetScaler VPX existante.

Les instances NetScaler VPX peuvent-elles être mises à niveau ?

Oui. Les limites de débit et l'édition de la famille NetScaler peuvent être mises à niveau. Les SKU de mise à niveau pour les deux types de mise à niveau sont disponibles.

Si je souhaite déployer NetScaler VPX dans une paire haute disponibilité, de combien de licences ai-je besoin ?

Comme pour les appliances physiques NetScaler, une configuration haute disponibilité de NetScaler nécessite deux instances actives. Par conséquent, le client doit acheter deux licences.

NetScaler VPX Express et essai gratuit de 90 jours

NetScaler VPX Express inclut-il toutes les fonctionnalités standard de NetScaler ? Inclut-il NetScaler Gateway et l'équilibrage de charge pour l'interface Web Citrix Virtual Apps (anciennement XenApp) et le broker XML ?

Oui. NetScaler VPX Express inclut toutes les fonctionnalités de NetScaler Premium. À partir de la version 14.1–29.65 de NetScaler, NetScaler a modifié le comportement de VPX Express.

NetScaler VPX Express nécessite-t-il une licence ?

Avec la dernière version de NetScaler VPX Express (14.1–29.65 et versions ultérieures), VPX Express est gratuit et ne nécessite pas de fichier de licence pour l'installation ou l'utilisation. Aucun engagement n'est nécessaire. Si vous disposez déjà d'une licence VPX Express, le comportement de licence précédent reste en vigueur. Toutefois, si vous supprimez le fichier de licence VPX Express existant et utilisez la version 14.1–29.65 ou ultérieure, le comportement VPX Express mis à jour s'appliquera.

La licence NetScaler VPX Express expire-t-elle ?

Avec le nouveau VPX express, il n'y a pas de licence ni de date d'expiration. Si vous possédez déjà une licence VPX express, la licence expire un an après le téléchargement.

NetScaler VPX Express prend-il en charge les mêmes chiffrements de chiffrement que les appliances NetScaler MPX ?

Pour une disponibilité générale, les mêmes chiffrements de chiffrement puissants pris en charge par les appliances NetScaler sont disponibles sur NetScaler VPX et NetScaler VPX Express. Il est soumis aux mêmes réglementations en matière d'importation ou d'exportation.

Puis-je déposer des dossiers de support technique pour NetScaler VPX Express ?

Oui. Les utilisateurs de NetScaler VPX Express sont libres d'utiliser le centre de connaissances NetScaler VPX et de demander de l'aide à la communauté via les forums de discussion.

NetScaler VPX Express peut-il être mis à niveau vers une version commerciale ?

Oui. Il vous suffit d'acheter la licence NetScaler VPX de détail dont vous avez besoin, puis d'appliquer la licence correspondante à l'instance NetScaler VPX Express.

Hyperviseur

Quelles sont les versions de VMware prises en charge par NetScaler VPX ?

NetScaler VPX prend en charge VMware ESX et ESXi pour les versions 3.5 ou ultérieures. Pour plus d'informations, voir Matrice de support et directives d'utilisation

Pour VMware, combien d'interfaces réseau virtuelles pouvez-vous allouer à un VPX ?

Vous pouvez allouer jusqu'à 10 interfaces réseau virtuelles à un NetScaler VPX.

Depuis vSphere, comment accéder à la ligne de commande NetScaler VPX ?

Le client VMware vSphere fournit un accès intégré à la ligne de commande NetScaler VPX via un onglet de console. En outre, vous pouvez utiliser n'importe quel client SSH ou Telnet pour accéder à la ligne de commande. Vous pouvez utiliser l'adresse NSIP du NetScaler VPX dans le client SSH ou Telnet.

Comment accéder à l'interface graphique de NetScaler VPX ?

Pour accéder à l'interface graphique de NetScaler VPX, saisissez le NSIP du NetScaler VPX, par exemple `http://NSIP address` dans le champ d'adresse de n'importe quel navigateur.

Deux instances NetScaler VPX installées sur le même VMware ESX peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui, mais ce n'est pas recommandé. Une panne matérielle affecterait les deux instances de NetScaler VPX.

Deux instances NetScaler VPX exécutées sur deux systèmes VMware ESX différents peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui. Il est recommandé dans une configuration haute disponibilité.

Pour VMware, les événements liés à l'interface sont-ils pris en charge sur NetScaler VPX ?

Oui. Vous pouvez ajouter jusqu'à sept interfaces (10 pour VMware) via l'utilitaire de configuration NetScaler VPX avec une seule carte réseau physique sur l'hyperviseur.

Pour VMware, les VLAN balisés sont-ils pris en charge sur NetScaler VPX ?

Oui. NetScaler VPX nécessite l'hyperviseur pour fonctionner. Les supports détaillés des hyperviseurs sont disponibles dans la fiche technique de NetScaler VPX.

Pour VMware, l'agrégation de liens et le LACP sont-ils pris en charge sur NetScaler VPX ?

Oui. L'agrégation de liens et le LACP ne sont pas pris en charge pour NetScaler VPX. L'agrégation de liens doit être configurée au niveau VMware.

Comment accéder à la documentation de NetScaler VPX ?

La documentation est disponible à partir de l'interface graphique de NetScaler VPX. Une fois connecté, sélectionnez l'onglet **Documentation** .

Planification ou dimensionnement des capacités

À quelles performances puis-je m'attendre avec NetScaler VPX ?

NetScaler VPX offre de bonnes performances. Consultez la fiche technique de NetScaler VPX pour connaître le niveau de performance spécifique pouvant être atteint à l'aide de NetScaler VPX.

Étant donné que la puissance du processeur du serveur varie, comment pouvons-nous estimer les performances maximales d'une instance NetScaler ?

L'utilisation d'un processeur plus rapide peut entraîner des performances supérieures (jusqu'au maximum autorisé par la licence), tandis que l'utilisation d'un processeur plus lent peut certainement limiter les performances.

La bande passante ou le débit de NetScaler VPX sont-ils limités au trafic entrant uniquement, ou à la fois au trafic entrant et sortant ?

Les limites de bande passante de NetScaler VPX sont appliquées uniquement au trafic entrant vers NetScaler, qu'il s'agisse du trafic de requête ou du trafic de réponse. Cela indique qu'un NetScaler VPX-1000 (par exemple) peut traiter simultanément 1 Gbit/s de trafic entrant et 1 Gbit/s de trafic sortant. Le trafic entrant et sortant n'est pas le même que le trafic de demande et de réponse. Pour NetScaler, le trafic provenant des points de terminaison (trafic de requêtes) et le trafic provenant des serveurs d'origine (trafic de réponse) sont « entrants » (c'est-à-dire entrant dans NetScaler).

Est-il possible d'exécuter plusieurs instances de NetScaler VPX sur le même serveur ?

Oui. Assurez-vous toutefois que le serveur physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge la charge de travail totale exécutée sur l'hôte, sinon les performances de NetScaler VPX pourraient être affectées.

Si plusieurs instances de NetScaler VPX s'exécutent sur un serveur physique, quelle est la configuration matérielle minimale requise par instance de NetScaler VPX ?

Chaque instance NetScaler VPX doit se voir allouer 2 Go de RAM physique, 20 Go d'espace disque et 2 processeurs virtuels. Pour les déploiements critiques, nous ne recommandons pas 2 Go de RAM pour VPX car le système fonctionne dans un environnement où la mémoire est limitée. Cela peut entraîner des problèmes liés à l'échelle, aux performances ou à la stabilité. La quantité recommandée est de 4 Go de RAM ou 8 Go de RAM.

> **Remarque :**
>
> Le NetScaler VPX est une appliance virtuelle haute performance sensible à la latence. Pour fournir les performances attendues, le dispositif nécessite la réservation du processeur virtuel, la réservation de la mémoire et l'épinglage du processeur virtuel sur l'hôte. En outre, l'hyper thread doit être désactivé sur l'hôte. Si l'hôte ne répond pas à ces exigences, des problèmes tels que basculement haute disponibilité, pic de processeur dans l'instance VPX, lenteur dans l'accès à l'interface de ligne de commande VPX, plantage du démon pit boss, pertes de paquets et faible débit se produisent.
>
> Assurez-vous que chaque instance VPX répond aux conditions prédéfinies.

Puis-je héberger NetScaler VPX et d'autres applications sur le même serveur ?

Oui. Par exemple, NetScaler VPX, Citrix Virtual Apps Web Interface et Citrix Virtual Apps XML Broker peuvent tous être virtualisés et exécutés sur le même serveur. Pour des performances optimales, assurez-vous que l'hôte physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge toutes les charges de travail en cours d'exécution.

L'ajout de cœurs de processeur à une seule instance NetScaler VPX augmentera-t-il les performances de cette instance ?

Selon la licence, une instance NetScaler VPX peut utiliser jusqu'à 4 processeurs virtuels aujourd'hui. L'ajout d'un processeur supplémentaire à une instance NetScaler VPX qui peut utiliser davantage de processeurs augmente les performances.

Pourquoi NetScaler VPX semble consommer plus de 90 % du processeur alors qu'il est inactif ?

Il s'agit d'un comportement normal et les appliances NetScaler présentent le même comportement. Pour connaître l'étendue réelle de l'utilisation du processeur NetScaler VPX, utilisez la commande stat CPU dans l'interface de ligne de commande NetScaler ou consultez l'utilisation du processeur NetScaler VPX à partir de l'interface graphique de NetScaler. Le moteur de traitement de paquets NetScaler est toujours « à la recherche de travail », même lorsqu'il n'y a rien à faire. Par conséquent, il fait tout pour prendre le contrôle de la CPU et ne pas le libérer. Sur un serveur installé avec NetScaler VPX et rien d'autre, cela donne l'impression (du point de vue de l'hyperviseur) que NetScaler VPX consomme la totalité du processeur. L'examen de l'utilisation du processeur « au sein de NetScaler » (à l'aide de l'interface de ligne de commande ou de l'interface graphique) fournit une image de la capacité du processeur NetScaler VPX utilisée.

Configuration système requise

Quelle est la configuration matérielle minimale requise pour NetScaler VPX ?

Le tableau suivant explique la configuration matérielle minimale requise pour NetScaler VPX.

Type	Exigences
Processeur	Serveur double cœur avec Intel Xeon ou AMD EPYC.
Mémoire	Minimum 2 Go. Cependant, 4 Go sont recommandés.
Disque	Disque dur de 20 Go minimum.
Hyperviseur	Citrix Hypervisor 5.6 ou version ultérieure, VMware ESX/ESXi 3.5 ou version ultérieure, ou Windows Server 2008 R2 avec Hyper-V
Connectivité réseau	100 Mbits/s minimum, mais 1 Gbit/s est recommandé.
Carte d'interface réseau	Une carte réseau compatible avec l'hyperviseur que vous utilisez.

> **Remarque :**
>
> Pour les déploiements critiques, une mémoire de 4 Go est préférable pour NetScaler VPX. Avec 2 Go de mémoire, NetScaler VPX fonctionne dans un environnement à mémoire limitée. Cela peut entraîner des problèmes liés à l'échelle, aux performances ou à la stabilité.

Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

> **Remarque :**

> À partir de la version 13.1 de NetScaler, l'instance NetScaler VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD EPYC.

Qu'est-ce que l'Intel VT-x ?

Ces fonctionnalités, parfois appelées « assistance matérielle » ou « assistance à la virtualisation », interceptent les instructions sensibles ou privilégiées du processeur exécutées par le système d'exploitation invité vers l'hyperviseur. Cela simplifie l'hébergement des systèmes d'exploitation invités (BSD pour un NetScaler VPX) sur l'hyperviseur.

Quelle est la commune de VT-x ?

Pratiquement, tous les serveurs livrés au cours des deux dernières années peuvent prendre en charge VT-x. De nombreux serveurs sont livrés avec l'aide à la virtualisation désactivée dans le BIOS. Avant de supposer que vous ne pouvez pas exécuter NetScaler VPX, vérifiez si vous devez modifier ce paramètre sur le serveur.

Existe-t-il une liste de compatibilité matérielle (HCL) pour NetScaler VPX ?

Tant que le serveur prend en charge la technologie Intel VT-x, NetScaler VPX doit s'exécuter sur n'importe quel serveur compatible avec l'hyperviseur sous-jacent. Consultez la HCL de l'hyperviseur pour obtenir une liste complète des plates-formes prises en charge.

Sur quelle version de NetScaler OS est basé NetScaler VPX ?

NetScaler VPX est basé sur NetScaler 9.1 ou versions ultérieures.

Étant donné que NetScaler VPX fonctionne sous BSD, peut-il être exécuté nativement sur un serveur sur lequel BSD Unix est installé ?

Oui. NetScaler VPX nécessite l'hyperviseur pour fonctionner. Les supports d'hyperviseur détaillés peuvent être trouvés dans la fiche technique NetScaler VPX.

Autres FAQ techniques

L'agrégation de liens sur un serveur physique avec plusieurs cartes réseau fonctionne-t-elle ?

LACP n'est pas pris en charge. Pour Citrix Hypervisor, l'agrégation de liens statiques est prise en charge et est limitée à quatre canaux et sept interfaces virtuelles. Pour VMware, l'agrégation de liens

statiques n'est pas prise en charge dans NetScaler VPX, mais elle peut être configurée au niveau de VMware.

Le transfert basé sur MAC (MBF) est-il pris en charge sur VPX ? Y a-t-il eu un changement par rapport à l'implémentation de l'appliance NetScaler ?

Le MBF est pris en charge et se comporte de la même manière qu'avec l'appliance NetScaler. L'hyperviseur fait essentiellement basculer tous les paquets reçus de NetScaler VPX vers l'extérieur et inversement.

Comment s'effectue le processus de mise à niveau de NetScaler VPX ?

Les mises à niveau s'effectuent de la même manière que pour les appliances NetScaler : téléchargez un fichier de noyau et utilisez install ns ou l'utilitaire de mise à niveau dans l'interface graphique.

Comment sont alloués la mémoire flash et l'espace disque ? Pouvons-nous le changer ?

/flash = 965M /var = 14G Un minimum de 2 Go de mémoire doit être alloué à chaque instance NetScaler VPX. L'image disque de NetScaler VPX a été dimensionnée à 20 Go pour des raisons de facilité de maintenance, par exemple pour accueillir et stocker jusqu'à 4 Go de dumps principaux et de fichiers journaux et de traçage. Bien qu'il soit possible de générer une image disque plus petite, il n'est pas prévu de le faire actuellement. `/flash` et `/var` se trouvent tous les deux dans la même image disque. Ils sont conservés en tant que systèmes de fichiers distincts à des fins de compatibilité. Pour des recommandations détaillées en matière d'allocation de mémoire, consultez la fiche technique de NetScaler VPX.

Pouvons-nous ajouter un nouveau disque dur pour augmenter l'espace sur l'instance NetScaler VPX ?

Oui. À partir de la version 13.1 build 21.x de NetScaler, vous avez la possibilité d'augmenter l'espace disque sur l'instance NetScaler VPX en ajoutant un deuxième disque. Lorsque vous connectez le second disque, le répertoire « /var/crash » est automatiquement monté sur ce disque. Le second disque est utilisé pour le stockage des fichiers principaux et la journalisation. Les répertoires existants qui sont utilisés pour stocker les fichiers principaux et les fichiers journaux continuent de fonctionner comme précédemment.

> **Remarque :**
>
> Effectuez une sauvegarde externe lors de la rétrogradation de l'appliance NetScaler pour éviter

> toute perte de données.

Pour plus d'informations sur la façon de connecter un nouveau disque dur (HDD) à une instance NetScaler VPX sur un cloud, consultez les rubriques suivantes :

- Documentation Azure

  > **Remarque :**
  >
  > Pour attacher un disque secondaire sur les instances NetScaler VPX déployées sur Azure, assurez-vous que les tailles de machine virtuelle Azure disposent d'un disque temporaire local. Pour plus d'informations, consultez la section Tailles des machines virtuelles Azure sans disque temporaire local.

- Documentation AWS
- Documentation GCP

> **Avertissement :**
>
> Après avoir ajouté un nouveau disque dur à NetScaler VPX, certains des scripts qui fonctionnent sur les fichiers déplacés vers le nouveau disque dur peuvent échouer dans les conditions suivantes :
>
> Si vous utilisez la commande shell « link » pour créer des liens matériels vers les fichiers qui ont été déplacés vers un nouveau disque dur.
>
> Remplacez toutes ces commandes par « ln -s » pour utiliser un lien symbolique. Modifiez également les scripts défaillants en conséquence.

Puis-je augmenter la taille du disque principal sur NetScaler VPX ?

À partir de NetScaler version 14.1 build 21.x, les administrateurs peuvent augmenter dynamiquement la taille du disque principal sur NetScaler VPX de 20 Go à 1 To à la fois. Et la fois suivante, vous pouvez à nouveau augmenter jusqu'à 1 To. Pour augmenter l'espace disque, augmentez la taille du disque principal à un minimum de 1 Go dans l'interface utilisateur du cloud ou de l'hyperviseur correspondante.

> **Remarque :**
>
> Vous pouvez uniquement augmenter la taille des disques. Une fois que la nouvelle taille est attribuée, vous ne pouvez pas la diminuer ultérieurement. Par conséquent, n'augmentez la taille du disque que si cela est essentiel.

Comment augmenter manuellement la taille du disque principal sur NetScaler VPX ?

Pour augmenter manuellement la taille du disque principal VPX depuis un hyperviseur ou un cloud, procédez comme suit :

1. Arrêtez la machine virtuelle.
2. Étendez la taille de disque par défaut de 20 Go à une valeur supérieure. Par exemple, 20 Go à 30 Go ou 40 Go. Pour Azure, étendez la taille de disque par défaut de 32 Go à 64 Go.
3. Allumez la machine virtuelle et entrez l'invite de démarrage.
4. Connectez-vous en mode mono-utilisateur à l'aide de la commande « boot -s ».
5. Vérifiez l'espace disque. Vous pouvez vérifier l'espace disque nouvellement alloué à l'aide de la commande « gpart show ».
6. Notez le nom de la partition. Par exemple, la partition de la machine virtuelle est da0.
7. Redimensionnez la partition du disque à l'aide de la commande « gpart resize ».

   Exemple : Redimensionnons la partition MBR da0 pour inclure 10 Go d'espace libre en exécutant la commande suivante.

   ```
   gpart resize -i 1 da0
   ```

8. Fusionnez l'espace libre avec la dernière partition.

   Exemple

   ```
   gpart resize -i 5 da0s1
   ```

9. Étendez le système de fichiers pour inclure l'espace libre nouvellement alloué à l'aide de la commande « growfs ».

   Exemple

   ```
   growfs /dev/ada0s1e
   ```

10. Redémarrez la machine virtuelle et vérifiez l'augmentation de l'espace disque à l'aide de la commande « df -h » à l'invite du shell.

Que pouvons-nous espérer considérer la numérotation de build NetScaler VPX et l'interopérabilité avec d'autres versions ?

La numérotation des versions de NetScaler VPX est similaire à celle de la version 9.1. Cl (classique) et 9.1. Les versions Nc (NCore), par exemple 9.1_97.3.vpx, 9.1_97.3.nc et 9.1_97.3.cl.

Le NetScaler VPX peut-il faire partie d'une configuration de haute disponibilité avec une appliance NetScaler ?

Configuration non prise en charge.

Toutes les interfaces visibles dans NetScaler VPX sont-elles directement liées au nombre d'interfaces sur l'hyperviseur ?

Oui. Vous pouvez ajouter jusqu'à sept interfaces (10 pour VMware) via l'utilitaire de configuration NetScaler VPX avec une seule carte réseau physique sur l'hyperviseur.

La migration dynamique Citrix Hypervisor XenMotion, VMware vMotion ou Hyper-V peut-elle être utilisée pour déplacer des instances actives de NetScaler VPX ?

NetScaler VPX ne prend pas en charge la migration dynamique vers Hyper-V. vMotion est pris en charge à partir de la version 13.0 de NetScaler. Live Migration (anciennement XenMotion) est pris en charge à partir de la version 14.1 build 17.38 de NetScaler.