net>scaler

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	6
Optimisez les performances de NetScaler VPX sur VMware ESX, Linux KVM et Citrix Hyper- visors	14
Prise en charge de l'augmentation de l'espace disque NetScaler VPX	31
Appliquez les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud	33
Améliorez les performances SSL-TPS sur les plateformes de cloud public	69
Configurer le multithreading simultané pour NetScaler VPX sur les clouds publics	70
Outil NetScaler Sanity Checker	74
Installation d'une instance NetScaler VPX sur un serveur bare metal	75
Installer une instance NetScaler VPX sur Citrix Hypervisor/XenServer	76
Configurer les instances VPX pour utiliser les interfaces réseau de virtualisation des E/S racine unique (SR-IOV)	80
Installation d'une instance NetScaler VPX sur VMware ESX	86
Configurer une instance NetScaler VPX pour utiliser l'interface réseau VMXNET3	91
Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV	103
Configurer un hyperviseur NetScaler VPX sur ESX pour utiliser Intel QAT pour l'accéléra- tion SSL en mode SR-IOV	121
Migration du NetScaler VPX de l'E1000 vers les interfaces réseau SR-IOV ou VMXNET3	125
Configurer une instance NetScaler VPX pour utiliser l'interface réseau PCI passthrough	125
Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX	129
Installation d'une instance NetScaler VPX sur le cloud VMware sur AWS	139
Installation d'une instance NetScaler VPX sur un serveur Microsoft Hyper-V	142
Installation d'une instance NetScaler VPX sur la plateforme Linux-KVM	147

Conditions préalables à l'installation d'une instance NetScaler VPX sur une plateforme Linux-KVM	148
Provisionner l'instance NetScaler VPX à l'aide d'OpenStack	153
Provisionnez l'instance NetScaler VPX à l'aide du Virtual Machine Manager	162
Configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV	178
Configurer un NetScaler VPX sur l'hyperviseur KVM pour utiliser Intel QAT pour l'accéléra- tion SSL en mode SR-IOV	188
Configurer une instance NetScaler VPX pour utiliser des interfaces réseau PCI passthrough	194
Provisionnez l'instance NetScaler VPX à l'aide du programme virsh	198
Gérer les machines virtuelles clientes NetScaler VPX	202
Provisionner l'instance NetScaler VPX avec SR-IOV, sur OpenStack	205
Configurer une instance NetScaler VPX sur KVM pour utiliser les interfaces hôtes basées sur OVS DPDK	212
Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur KVM	222
NetScaler VPX sur AWS	224
Terminologie AWS	227
Matrice de prise en charge AWS-VPX	230
Limitations et directives d'utilisation	233
Conditions préalables	235
Configurer les rôles AWS IAM sur une instance NetScaler VPX	237
Comment fonctionne une instance NetScaler VPX sur AWS	248
Déployer une instance autonome NetScaler VPX sur AWS	250
Scénario : instance autonome	255
Télécharger une licence NetScaler VPX	264

Serveurs d'équilibrage de charge dans différentes zones de disponibilité	271
Comment fonctionne la haute disponibilité sur AWS	272
Déployer une paire HA VPX dans la même zone de disponibilité AWS	274
Haute disponibilité dans différentes zones de disponibilité AWS	286
Déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans dif- férentes zones AWS	287
Déployez une paire VPX haute disponibilité avec des adresses IP privées dans différentes zones AWS	292
Déployer une instance NetScaler VPX sur AWS Outposts	305
Protégez AWS API Gateway à l'aide du pare-feu NetScaler Web App Firewall	309
Ajouter le service principal AWS Autoscaling	313
Déployez NetScaler GSLB sur AWS	318
Déployez NetScaler Web App Firewall sur AWS	334
Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV	359
Configurer une instance NetScaler VPX pour utiliser la mise en réseau améliorée avec AWS ENA	362
Mettre à niveau une instance NetScaler VPX sur AWS	362
Dépannage d'une instance VPX sur AWS	368
Questions fréquentes sur AWS	369
Déployer une instance NetScaler VPX sur Microsoft Azure	372
Terminologie Azure	378
Architecture réseau pour les instances NetScaler VPX sur Microsoft Azure	382
Configurer une instance autonome NetScaler VPX	385
Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX	398
Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes résea	u404

Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell	415
Déployez une paire de haute disponibilité NetScaler sur Azure avec ALB en mode IP flot- tant désactivé	427
Déployer une zone privée DNS NetScaler for Azure	448
Configurer une instance NetScaler VPX pour utiliser le réseau accéléré Azure	468
Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler avec Azure ILB	484
Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler pour les applications connectées à Internet	497
Configurer une configuration haute disponibilité avec des équilibreurs de charge externes et internes Azure simultanément	508
Installation d'une instance NetScaler VPX sur la solution Azure VMware	514
Configurer une instance autonome NetScaler VPX sur la solution Azure VMware	530
Configurer une configuration de haute disponibilité NetScaler VPX sur la solution Azure VMware	532
Configurer le serveur de routage Azure avec la paire NetScaler VPX HA	534
Ajouter le service principal Azure Autoscaling	538
Balises Azure pour le déploiement de NetScaler VPX	547
Configurer GSLB sur des instances NetScaler VPX	552
Configurer GSLB sur une configuration haute disponibilité active-veille	562
Déployez NetScaler GSLB sur Azure	566
Déployez NetScaler Web App Firewall sur Azure	581
Configurer les pools d'adresses IP de l'intranet pour une appliance NetScaler Gateway	607
Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX à l'aide des commandes PowerShell	610
Scripts PowerShell supplémentaires pour le déploiement Azure	617

Créez un ticket de support pour l'instance VPX sur Azure	633
FAQ Azure	635
Déployer une instance NetScaler VPX sur Google Cloud Platform	636
Déployer une paire haute disponibilité VPX sur Google Cloud Platform	651
Déployer une paire haute disponibilité VPX avec une adresse IP statique externe sur Google Cloud Platform	653
Déployez une paire de cartes réseau VPX à haute disponibilité unique avec une adresse IP privée sur Google Cloud Platform	664
Déployer une paire VPX haute disponibilité avec une adresse IP privée sur Google Cloud Platform	674
Installation d'une instance NetScaler VPX sur Google Cloud VMware Engine	683
Ajouter un service GCP Autoscaling principal	702
Support de dimensionnement VIP pour l'instance NetScaler VPX sur GCP	707
Résoudre les problèmes d'une instance VPX sur GCP	714
Trames Jumbo sur les instances NetScaler VPX	715
Automatisez le déploiement et les configurations de NetScaler	717
FAQ	720

Matrice de prise en charge de NetScaler VPX

June 12, 2025

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.

	Date de sortie d'			
	ESXi	Numéro de build	Version de	Gamme de
Version ESXi	(AAAA/MM/JJ)	ESXi	NetScaler VPX	performances
Mise à jour 3e d' ESXi 8.0	2025/04/10	24674464	Versions 14.1-43.x et supérieures	
Mise à jour d'ESXi 8.0 3d	2025/03/04	24585383	Versions 14.1-38.x et supérieures	10 Mbps à 100 Gbps
ESXi 8.0 update 3c	2025/01/23	24414501	Versions 14.1-29.x et supérieures	
Mise à jour 3b d' ESXi 8.0	2024/09/17	24280767	Versions 14.1-17.x et supérieures	
ESXi 8.0 mise à jour 3	2024/06/25	24022510	Versions 14.1-17.x et supérieures	
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	
Mise à jour ESXi 7.0 3s	2025/03/04	24585291	Versions 14.1-29.x et supérieures	

Instance VPX sur l'hyperviseur VMware ESX

	Date de sortie d'			
	ESXi	Numéro de build	Version de	Gamme de
Version ESXi	(AAAA/MM/JJ)	ESXi	NetScaler VPX	performances
Mise à jour 3r d'	2024/12/12	24411414	Versions 14.1-29.x	
ESXi 7.0			et supérieures	
ESXi 7.0 mise à	2024/03/05	23794027	Versions 14.1-17.x	
jour 3o			et supérieures	
Mise à jour 3n d'	Navigateurs pris	23307199	Versions 14.1-4.x	
ESXi 7.0	en charge		et supérieures	
Mise à jour ESXi	2023/09/28	22348816	Versions 14.1-4.x	
7.0 3m			et supérieures	
Mise à jour 3n d'	2023/07/06	21930508	Versions 14.1-8.x	
ESXi 7.0			et supérieures	
Mise à jour ESXi	2023/05/03	21686933	Versions 14.1-4.x	
7.0 3m			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	450000	10 Mbps à 40 Gbps
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		

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	450070	10 Mbps à 100 Gbps
Ubuntu 16.04, Ubuntu 18.04,		
Ubuntu 22.04		

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.
 - 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.cfgà 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
GCP	450070	10 Mbps à 10 Gbps

Fonctionnalités VPX prises en charge sur les hyperviseurs

Hyperviseurs VPX sur XenServer	VPX sur VMware ESX
<u>→</u>	

^^Carac	téristiqu	ies								
\checkmark	۸۸		~ ~				٨٨	٨٨		
Interfac →	:eBV	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
Balisago VLAN	e Oui	Oui	Oui	Oui	Oui	Oui	Oui (unique- ment sur 2012R2)	Oui	Oui	Oui
Détectio des événe- ments de lien/HA Mon	onNon²	Oui ³	Non ²	Oui ³	Non ²	Oui ³	Non ²	Non ²	Oui ³	Oui ³
Configu des paramè d' inter- face	ir àlio n tres	Non	Non	Non	Non	Oui	Non	Non	Non	Oui
LA sta- tique	Oui ²	Oui ³	Oui²	Non	Oui²	Oui ³	Oui²	Oui²	Oui ³	Oui ³
LACP	Non	Oui ³	Oui²	Non	Oui ²	Oui ³	Non	Oui²	Oui ³	Oui ³

^^Cara	^^Caractéristiques											
\checkmark	٨٨		٨٨				٨٨	~ ~				
CLAG sta- tique	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non		
CLAG de la C.A.L.F	Non •	Non	Oui²	Non	Oui²	Oui ³	Non	Oui²	Oui ³	Oui ³		
BranchenNent à chaud		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 ↓	^^	٨٨	٨٨
Prise en charge multi-PE	Oui	Oui	Oui
Prise en charge du clustering	Non	Non	Non
Balisage VLAN	Non	Non	Non
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

NetScaler VPX 14.1

^^Caractéristiques ↓	٨٨	٨٨	^^
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 de la liaison 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

Pour plus d'informations sur les navigateurs pris en charge pour accéder aux versions 14.1 et 13.1 de l'interface graphique NetScaler, consultez Navigateurs compatibles.

Processeurs pris en charge pour NetScaler VPX

Plates-formes	Processeur Intel	Processeur AMD
Citrix Hypervisor	Oui	Non
Hyperviseur ESXi	Oui	Oui
Hyper-V	Oui	Non
KVM	Oui	Non
AWS	Oui	Oui
Azure	Oui	Oui
GCP	Oui	Oui

Cartes réseau prises en charge pour NetScaler VPX

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

réseau → CX-3 CX-4 CX-5 SRIOV VF X710/X722/XL7th@nsfert SRIOV VF PCI Intel X710/XI 710/XX/7	Cartes	Mellanox	Mellanox	Mellanox	Intel 82599	Intel	Mode de
SRIOV VF PCI Intel	réseau →	CX-3	CX-4	CX-5	SRIOV VF	X710/X722/X	KL7thansfert
X710/XI 710/XX//7						SRIOV VF	PCI Intel
							X710/XL710/XXV710

^^Plateformes										
\checkmark	٨٨	۸۸	۸۸	٨٨	۸۸	۸۸				
Citrix Hypervisor	S/O	S/O	S/O	Oui	Oui	Non				
Hyperviseur ESXi	Non	Oui	Non	Oui	Non	Oui				
Hyper-V	S/O	S/O	S/O	Non	Non	Non				
KVM	Non	Oui	Oui	Oui	Oui	Non				
AWS	S/O	S/O	S/O	Oui	S/O	S/O				
Azure	Oui	Oui	Oui	S/O	S/O	S/O				
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 la prise en charge des produits Citrix Ready, consultez la page des partenaires Citrix Ready
- 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

April 1, 2025

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:

```
1 #vsish -e get /net/pNics/vmnic7/properties | grep NUMA
2 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:

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

- For ESX version 6.0 onwards:

```
1 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:

```
1 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.

```
bind vlan 3 -ifnum 1/2 - tagged
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).

```
    add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
Listenpolicy None -cltTimeout 180
    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
    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:

1 esxcli system settings advanced set - o /Net/NetTxWorldlet - i

- For ESX version 6.0 onwards:

1 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 :

```
1 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 :

```
1 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.

[root@l	calhost ~]# lstopo-no-graphics
Machine	(128GB)
NUMAN	000 L#U (P#U 040B)
300	el 1#0 7 ES E#0 (2016) > 1#0 (756KR) + 114 1#0 (32KR) + 111 1#0 (32KR) + Coro 1#0 + DILL#0 (D#0)
i i	2 #1 (256KB) + 11d #1 (32KB) + 111 #1 (32KB) + Core #1 + PU #1 (P#1)
i i	L#2 (256KB) + L1d L#2 (32KB) + L1i L#2 (32KB) + Core L#2 + PU L#2 (P#2)
L	2 L#3 (256KB) + L1d L#3 (32KB) + L1i L#3 (32KB) + Core L#3 + PU L#3 (P#3)
L	2 L#4 (256KB) + L1d L#4 (32KB) + L1i L#4 (32KB) + Core L#4 + PU L#4 (P#4)
L	2 L#5 (256KB) + L1d L#5 (32KB) + L1i L#5 (32KB) + Core L#5 + PU L#5 (P#5)
L	2 L#6 (256KB) + L1d L#6 (32KB) + L1i L#6 (32KB) + Core L#6 + PU L#6 (P#6)
L	2 L#/ (256KB) + L1d L#/ (32KB) + L11 L#/ (32KB) + Core L#/ + PU L#/ (P#/)
HOS	Bridge L#0
P	PCT_8686+1521
	Net L#0 "eno1"
	PCI 8086:1521
	Net L#1 "eno2"
P	IBridge
	PCI 8086:1584
	Net L#2 "ens3"
P	IBridge
	Not 1 #2 "ope4"
P	I 8086:8d62
· ·	Block L#4 "sda"
	Block L#5 "sdb"
P	IBridge
	PCIBridge
	PCI 1a03:2000
	GPU L#G "cardu" GPU L#7 "controlD64"
P	T 8886-8482
NUMAN	de L#1 (P#1 64GB)
Soc	et L#1 + L3 L#1 (20MB)
L	2 L#8 (256KB) + L1d L#8 (32KB) + L1i L#8 (32KB) + Core L#8 + PU L#8 (P#8)
L	2 L#9 (256KB) + L1d L#9 (32KB) + L1i L#9 (32KB) + Core L#9 + PU L#9 (P#9)
L -	2 L#10 (256KB) + L1d L#10 (32KB) + L1i L#10 (32KB) + Core L#10 + PU L#10 (P#10)
	(L#II (ZOONB) + LIG L#II (JZNB) + LII L#II (JZNB) + UOTE L#II + PU L#II (P#II)
1	2 L#12 (256KB) + L10 L#12 (32KB) + L11 L#12 (32KB) + Core L#12 + PO L#12 (P#12)
l i	2 L#14 (256KB) + L1d L#14 (32KB) + L11 L#14 (32KB) + Core L#14 + PU L#14 (P#14)
i i	L#15 (256KB) + L1d L#15 (32KB) + L1i L#15 (32KB) + Core L#15 + PU L#15 (P#15)
Hos	Bridge L#6
P	TBridge
	PCI 8086:1584
	Net L#8 "ens2"
^P	PCI 8086-10fb
1	Net L#9 "ens1f0"
	PCI 8086:10fb
1	Net L#10 "enslfl"
1	PCI ffff:fff
	Net L#11 "enp131s16"
[root@l	calnost ∼j# modprobe kvm-intel acpienv=N

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 :

- 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

```
1 virsh vcpupin <VPX name>
coot@localhost gemu]# virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
0: 8
1: 9
2: 10
3: 11
```

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

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

1 mpstat -P ALL 5

Linux 3.10.0-123.e17.x86_64 (localhost.localdomain)		0.9	5/17/201	6 _	x86_64_		(16 CPU)					
2:26:20	PM	CPU	<pre>%usr</pre>	<pre>%nice</pre>	%sys	<pre>%iowait</pre>	\$irg	%soft	<pre>%steal</pre>	%guest	%gnice	\$idle
2:26:25	PM	all	0.24	0.00	1.67	0.00	0.00	0.00	0.00	17.32	0.00	80.7
2:26:25	PM		0.20	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	98.80
2:26:25	PM		0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.60
2:26:25	PM		0.20	0.00	0.40	0.00	0.00	0.00	0.00	0.00	0.00	99.4
2:26:25	PM		0.00	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.8
2:26:25	PM	4	0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.6
2:26:25	PM		0.60	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.2
2:26:25	PM		0.40	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	99.6
2:26:25	PM		1.62	0.00	1.42	0.00	0.00	0.00	0.00	0.00	0.00	96.9
2:26:25	PM		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM		0.00	0.00	7.60	0.00	0.00	0.00	0.00	92.40	0.00	0.00
2:26:25	PM	10	0.20	0.00	7.00	0.00	0.00	0.00	0.00	92.80	0.00	0.0
2:26:25	PM	11	0.00	0.00	8.60	0.00	0.00	0.00	0.00	91.40	0.00	0.0
2:26:25	PM	12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM	13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM	14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM	15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0

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

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

2. Ajoutez la balise suivante :

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

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

 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.

```
1 [root@localhost ~]# kvm_stat -1 | grep EXTERNAL
2 kvm_exit(EXTERNAL_INTERRUPT) 1728349 27738
3 [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 :

```
1 echo 0000000f > /proc/irq/55/smp_affinity
2 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:

TTPuTTY (Multi-Tabbed PuTTY)	- a ×
Server View Tools Help	
a Start page X) rootBlocalhost-~ X rootBlocalhost-~ X rootBlocalhost-~ X rootBlocalhost-~ X rootBlocalhost-~ X	,
top - 14:48:08 up 6 days, 17 min, 4 users, load average: 1.46, 0.42, 0.65	
Tasks: 486 total, 3 running, 483 sleeping, 0 stopped, 0 zombie	
<pre>%Cpu(s): 4.1 us, 5.1 sy, 0.0 ni, 89.2 id, 0.0 wa, 0.0 hi, 1.7 si, 0.0 st</pre>	
KiB Mem: 13175540+total, 6496624 used, 12525878+free, 884 buffers	
KiB Swap: 4194300 total, 0 used, 4194300 free. 2088468 cached Mem	
PTD USER PR NI VIET RES SHES &CPU &MEM TIME+ COMMAND	P
29824 gemu 20 0 12,786g 742864 8040 S 139,2 0.6 8789:04 gemu-kym	11
29838 root 20 0 0 0 0 0 R 100.0 0.0 5659:06 whost-29824	8
29837 root 20 0 0 0 0 R 99.7 0.0 5659:25 vhost-29824	1
3063 root 20 0 1073944 23992 9396 s 1.7 0.0 111:58.18 libvirtd	0
1070 root 39 19 0 0 0 S 1.0 0.0 91:35.98 kipmi0	14
27439 test 20 0 2710032 1.159g 25868 s 0.7 0.9 45:35.56 virt-manager	7
16500 root 20 0 0 0 0 S 0.3 0.0 0:16.96 kworker/25:0	25
1 root 20 0 53704 7724 2536 S 0.0 0.0 0:13.69 systemd	15
2 root 20 0 0 0 0 S 0.0 0.0 0:00.22 kthreadd	1
3 root 20 0 0 0 0 S 0.0 0.0 384:17.42 ksoftirgd/0	0
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H	0
6 root 20 0 0 0 0 0 S 0.0 0.0 0:00.00 kworker/u64:0	18
8 root rt 0 0 0 0 0 s 0.0 0.0 0 mgration/0	U
	2
11 root 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
12 root 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
13 root 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
14 root 20 0 0 0 0 S 0.0 0.0 roub/4	0
15 root 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/6	0
17 root 20 0 0 0 0 0 0.0 0.0 0:00.00 rcuob/7	0
18 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/8	9
19 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/9	0
20 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/10	0
21 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/11	0
22 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/12	0
23 root 20 0 0 0 0 S 0.0 0.0 0:00.00 reuob/13	0
📑 🔿 l'm Cortana. Ask me anything. 👘 📑 🌍 🐎 🧕 💁 🕋 🖬 🖬 💀 🛃	t d× 💭 ENG 14:48

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

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

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

Exemple

1 taskset - pc 12 29838

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

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

```
2
     <cpu>
3
         </cpu>
4
             <cpus num='8'>
5
                 <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
                  <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
6
                 <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
7
                 <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
8
                 <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
9
                 <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
11
                 <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
12
                 <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
13
             </cpus>
14
             <cpus num='8'>
15
16
             <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
             <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
17
             <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
18
             <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
19
20
             <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
             <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
21
             <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
             <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
23
24
             </cpus>
25
26
         <cpuselection/>
27
         <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 :

1 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:

4	<pre><memory unit="KiB">8097152</memory></pre>
5	<pre><currentmemory unit="KiB">8097152</currentmemory></pre>
6	<vcpu placement="static">4</vcpu>
7	
8	<cputune></cputune>
9	<vcpupin cpuset="8" vcpu="0"></vcpupin>
10	<vcpupin cpuset="9" vcpu="1"></vcpupin>
11	<vcpupin cpuset="10" vcpu="2"></vcpupin>
12	<vcpupin cpuset="11" vcpu="3"></vcpupin>
13	
14	
15	<numatune></numatune>
16	<memory mode="strict" nodeset="1"></memory>
17	
18	
19	

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:

1 xl info -n

Pin vCPUs of VPX to physical cores.

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

Check binding of vCPUs.

1 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.

<pre>[root@xenserver-uuffyqlx ~]# xl list</pre>					
Name	ID	Mem	VCPUs	State	Time(s)
Domain-0	0	4092	8	r	633321.0
Sai_VPX	5	8192	4	r	1529471.0
[root@xenserver-uuffyqlx ~]#					
[root@xenserver-uuffyqlx ~]#					
<pre>[root@xenserver-uuffyqlx ~]# ps -ax gr</pre>	ep "vif	5"			
Warning: bad syntax, perhaps a bogus '-'	? See /1	usr/sł	nare/doc/	procps-3.	2.7/FAQ
20447 pts/6 S+ 0:00 grep vif5					
29187 ? S 1:09 [vif5.0-guest	-rx]				
29188 ? S 0:00 [vif5.0-deall	oc]				
29189 ? S 201:33 [vif5.1-guest	-rx]				
29190 ? S 80:51 [vif5.1-deall	oc]				
29191 ? S 0:20 [vif5.2-guest	-rx]				
29192 ? S 0:00 [vif5.2-deall	oc]				
[root@xenserver-uuffyqlx ~]#					

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

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

Exemple

1 taskset -pc 1 29189

Prise en charge de l'augmentation de l'espace disque NetScaler VPX

March 20, 2025

NetScaler VPX prend en charge un espace disque par défaut de 20 Go. Si vous rencontrez des contraintes de taille de disque pour diverses raisons, les options suivantes sont disponibles pour augmenter l'espace disque VPX :

- Augmentez manuellement la taille du disque principal
- Augmentez dynamiquement la taille du disque principal
- Ajouter un disque secondaire

Remarque :

La possibilité d'augmenter l'espace disque NetScaler VPX est disponible pour les déploiements VPX sur site et VPX dans le cloud. Le redimensionnement du disque principal NetScaler VPX n' est pas pris en charge à l'aide du service de gestion SDX.

Augmentez manuellement la taille du disque principal sur NetScaler VPX

Suivez ces étapes pour augmenter manuellement la taille du disque principal VPX à l'aide d'un hyperviseur ou d'une plate-forme Cloud :

- 1. Arrêtez la VM.
- Étendez la taille du disque par défaut de 20 Go à une valeur supérieure, telle que 30 Go ou 40
 Go. Pour Azure, étendez la taille du 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 utilisateur unique à l'aide de la commande boot -s.
- 5. Vérifiez l'espace disque. Vous pouvez vérifier l'espace disque nouvellement alloué en utilisant la commande gpart show.
- 6. Notez le nom de la partition. Dans l'exemple suivant, la partition VM 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/da0s1e

 Redémarrez la machine virtuelle et vérifiez l'espace disque augmenté à l'aide de la commande df -h sur l'invite du shell.

Augmentez dynamiquement la taille du disque principal sur NetScaler VPX

Les administrateurs peuvent augmenter dynamiquement la taille du disque principal sur NetScaler VPX de 20 Go à 1 To à la fois. Pour chaque augmentation ultérieure, vous pouvez à nouveau étendre jusqu'à 1 To. Assurez-vous d'arrêter la machine virtuelle chaque fois que vous augmentez la taille du disque principal. Cela permet au système de reconnaître correctement la nouvelle taille du disque, de mettre à jour la table de partition et de maintenir la stabilité du système. Pour augmenter l'espace disque, augmentez la taille du disque principal d'au moins 1 Go dans l'interface utilisateur du cloud ou de l'hyperviseur concerné.

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.

Ajouter un disque secondaire

Vous pouvez augmenter l'espace disque sur l'instance NetScaler VPX en ajoutant un disque secondaire. Lorsque vous connectez le disque secondaire, le répertoire /var/crash est automatiquement monté sur ce disque. Le disque secondaire est utilisé pour stocker les fichiers principaux et les journaux. Les répertoires existants pour les fichiers principaux et les fichiers journaux continuent de fonctionner comme avant.

Remarque :

Effectuez une sauvegarde externe avant de rétrograder 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 associer un disque secondaire à des instances VPX déployées sur Azure, assurez-vous que les machines virtuelles 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 disque dur à VPX, certains 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 physiques vers les fichiers qui ont été déplacés vers le nouveau disque dur.

Remplacez toutes ces commandes par $\ln -s$ pour utiliser un lien symbolique. Mettez également à jour les scripts défaillants en conséquence.

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 àConfigurer les détails de l'instance > Détails avancés, puisfournissez 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.

aws	Services 🗸	Resource Groups 👻 🔭
1. Choose AMI	2. Choose Instance Type	3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review
Step 3: C	onfigure Instan	ce Details
	Domain join directory	No directory Create new directory
	IAM role	(i) None C Create new IAM role
	Shutdown behavior	() Stop 4
St	op - Hibernate behavior	(i) Enable hibernation as an additional stop behavior
Enable	e termination protection	(i) Protect against accidental termination
	Monitoring	Enable CloudWatch detailed monitoring Additional charges apply.
	Tenancy	(i) Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
	Credit specification	Unlimited Additional charges may apply
	File systems	Add file system Create new file system
 Advance 	d Details	
	Metadata accessible	i Enabled
	Metadata version	(i) V1 and V2 (token optional)
Metadata to	oken res <mark>ponse hop limit</mark>	1
	User data	(i) ● As text ○ As file □ Input is already base64 encoded
		(Optional)

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 \
1
2
        --image-id ami-Oabcdef1234567890 \
3
        --instance-type t2.micro \
4
        --count 1 \setminus
5
         --subnet-id subnet-08fc749671b2d077c \
6
         --key-name MyKeyPair \
7
         --security-group-ids sg-0b0384b66d7d692f9 \
         --user-data file://my_script.txt
8
```

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 :

```
1 az vm create \
2 --resource-group myResourceGroup \
3 --name MyVm \
4 --image debian \
5 --custom-data MyCloudInitScript.txt \
```

Exemple



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 **MyClou-dInitScript.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 :

```
1 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 <LO-CAL_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& gt;
- 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>
1
2
          <NS-CONFIG>
                               </NS-CONFIG>
3
          <NS-BOOTSTRAP>
                               </NS-BOOTSTRAP>
4
          <NS-SCRIPTS>
                               </NS-SCRIPTS>
5
          <NS-LICENSE-CONFIG>
                               </NS-LICENSE-CONFIG>
    </NS-PRE-BOOT-CONFIG>
6
```

Exemple 2 :

```
1 <NS-PRE-BOOT-CONFIG>
2 <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
```

```
3<NS-SCRIPTS></NS-SCRIPTS>4<NS-BOOTSTRAP></NS-BOOTSTRAP>5<NS-CONFIG></NS-CONFIG>6</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.

<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 <u>5.0.0.201</u> 5.0.0.201

add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip D SABLED -usip

NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO add lb vserver preboot_v4_101 HTTP ________80 -persistenceType NONE -cltTimeout 180 </NS-CONFIG>

</NS-PRE-BOOT-CONFIG>

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

1	<ns-pre-boot-config></ns-pre-boot-config>
2	<ns-config></ns-config>
3	add vlan 5
4	add ns ip 5.0.0.1 255.255.255.0
5	bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
6	enable ns feature WL SP LB RESPONDER
7	add server 5.0.0.201 5.0.0.201
8	add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
	maxClient 0 -maxReq 0 -cip DISABLED -usip
9	NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO
	-TCPB NO -CMP NO
10	add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
	persistenceType NONE -cltTimeout 180
11	
12	

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

> sn ns	1p							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
_								
1)	10.160.0.72		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	5.0.0.1		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	4.0.0.101		VIP	Active	Enabled	Enabled	Enabled	Enabled
Done								
> sh vl	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::4001						
	Interfaces : 1/1	1/2 LO/1						
2)	VLAN ID: 5	VLAN Alias Name:						
	IPs :							
	5.0.0.1	Mask: 255.255.25	5.0					
3)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 0/1							
	IPs :							
	10.160.0.72	Mask: 25	5.255.240.0					
Done								



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.

S-PRE-BOOT-CONFIG>	
<pre></pre>	∑ 2

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

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

```
<NS-PRE-BOOT-CONFIG>
1
2
        <NS-SCRIPTS>
3
        <SCRIPT>
               4
5
                   #Shell script
                   echo "Running script 1" > /var/script-1.output
6
                   date >> /var/script-1.output
8
               </SCRIPT-CONTENT>
9
                    script-1.sh </SCRIPT-NAME>
10
                    /var/ </SCRIPT-TARGET-</pre>
11
                      LOCATION>
12
                   sh /var/script-1.sh</SCRIPT-NS-</pre>
                      BOOTUP>
            </SCRIPT>
13
14
        </NS-SCRIPTS>
15
    </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.

root@ns#				
root@ns # ls /var/				
.monit.id	core	gui	nsinstall	pubkey
.monit.state	crash	install	nslog	python
.snap	cron	krb	nsproflog	run
AAA	db	learnt_data	nssynclog	safenet
app_catalog	dev	log	nstemplates	script-1.output
cloudhadaemon	download	mastools	nstmp	script-1.sh
cloudhadaemon.tgz	empty	netscaler	nstrace	tmp
clusterd	file-2.txt	ns_gui	opt	vpn
configdb	gcfl	ns_sys_backup	osr_compliance	vpns
root@ns#				
root@ns# cat /var/script	:-1.sh			
#Shell script				
echo "Running script 1"	<pre>> /var/script-l.output</pre>			
date >> /var/script-l.ou	itput			
root@ns#				
root@ns# cat /var/script	t-1.output			
Running script l				
Wed Jan 6 05:25:33 UTC	2021			
root@ns#				
root@ns#				

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.

<script> #Shell script</th><th>script-1.sh</th></tr><tr><th><pre>tenting script 1 > /var/script-1.output tate >> /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>	€ file-2.txt
<pre></pre>	NS Consumer module should consume this

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

```
<NS-PRE-BOOT-CONFIG>
1
2
       <NS-SCRIPTS>
3
           <SCRIPT>
4
              5
                 #Shell script
                 echo "Running script 1" > /var/script-1.output
6
7
                 date >> /var/script-1.output
              </SCRIPT-CONTENT>
8
9
               script-1.sh </SCRIPT-NAME>
10
11
               /var/ </SCRIPT-TARGET-LOCATION>
12
              sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
13
              </SCRIPT>
14
           <SCRIPT>
15
              16
17
                  This script has no execution point.
                  It will just be saved at the target location
18
19
                  NS Consumer module should consume this script/file
20
              </SCRIPT-CONTENT>
              file-2.txt</SCRIPT-NAME>
21
22
              /var/</SCRIPT-TARGET-LOCATION>
23
           </SCRIPT>
24
        </NS-SCRIPTS>
25
    </NS-PRE-BOOT-CONFIG>
```

ot@ns# ls /var/ core nsinstall monit.id pubkey install monit.state crash nslog python nsproflog snap krb nssynclog AAA safenet app catalog dev nstemplates script-l.output loudhadaemon download mastools nstmp script-1.sh nstrace cloudhadaemon.tgz empty netscaler .txt clusterd ns gui vpn file osr compliance onfigdb ns sys backup vpns oot@ns# ot@ns# cat /var/script-l.sh Shell script cho "Running script l" > /var/script-l.output late >> /var/script-l.output oot@ns# ot@ns# cat /var/script-l.output unning s ed Jan 6 05:08:56 UTC 2021 oot@ns# ot@ns# ot@ns# cat /var/file-2.txt This script has no execution point. It will just be saved at the target location NS Consumer module should consume this script/file ot@ns#

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).

<ns-pre-boot-config></ns-pre-boot-config>	
<ns-license-config></ns-license-config>	
<license-commands></license-commands>	
add ns ligenseserver 10.102.38.214 -port 2800	
set ns capacity -unit stops -bandwidth 3 edition platinum	
<ns-license-config></ns-license-config>	
<ns-pre-boot-config></ns-pre-boot-config>	

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

```
<NS-PRE-BOOT-CONFIG>
1
2
       <NS-LICENSE-CONFIG>
3
             <LICENSE-COMMANDS>
                 add ns licenseserver 10.102.38.214 -port 2800
4
5
                 set ns capacity -unit gbps -bandwidth 3 edition platinum
6
             </LICENSE-COMMANDS>
        </NS-LICENSE-CONFIG>
7
    </NS-PRE-BOOT-CONFIG>
8
```

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.

```
> sh licenseserver
License Server: 10.102.38.214 Port: 2800 Status:
Done
>
>
```

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.

Comportement Bootstrap Le comportement d'amorçage
Le comportement d'amorçage
nouvelle séquence d'amorçage personnalisée fournie dans la <ns-bootstrap></ns-bootstrap>
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></ns-config>

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.



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.

Network Interface eth1

Interface ID	<u>eni-021961099be6815eb</u>
VPC ID	vpc-6b258c02
Attachment Owner	566658252593
Attachment Status	attached
Attachment Time	Fri Jan 01 11:11:23 GMT+530 2021
Delete on Terminate	false
Private IP Address	172.31.52.88
Private DNS Name	ip-172-31-52-88.ap-south-
	1.compute.internal

Network interface eth0

Interface ID	eni-039e5f3329cd879e9
VPC ID	vpc-6b258c02
Attachment Owner	566658252593
Attachment Status	attached
Attachment Time	Fri Jan 01 10:58:28 GMT+530 2021
Delete on Terminate	true
Private IP Address	172.31.5.155
Private DNS Name	ip-172-31-5-155.ap-south-
	1 compute internal

Network Interface eth2

Interface ID	eni-09e55a6cfb791e68d
VPC ID	vpc-6b258c02
Attachment Owner	566658252593
Attachment Status	attached
Attachment Time	Fri Jan 01 11:11:33 GMT+530 2021
Delete on Terminate	false
Private IP Address	<u>172.31.76.177</u> @
Private DNS Name	ip-172-31-76-177.ap-south-1.compute.internal
	<u>ත</u>

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	Туре	Mode	Arp	Icmp V	Vserver	State		
1) 2) 3) Done > sh vl	172.31.52.88 172.31.76.177 172.31.5.155 an	0 0 0	<u>NetScaler IP</u> <u>SNIP</u> VIP	Active Active Active Active	 Enabled Enabled Enabled	Enabled 1 Enabled 1 Enabled 1 Enabled 1	NA NA Enabled	Enabled Enabled Enabled		
1)	<pre>1) VLAN ID: 1 Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64 Interfaces : 1/1 1/3 LO/1</pre>									
2)	VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 172.31.52.88 Mask: 255.255.240.0									
Done										
> sh ro	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Dor	main Ty	pe		
1)	0.0.0.0	0.0.0.0	172.31.48.1	0	UP	0	STA	TIC		
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT		
3)	172.31.0.0	255.255.240.0	172.31.5.155		UP		DIR	ECT		
4)	172.31.48.0	255.255.240.0	172.31.52.88		UP		DIR	ECT		
5)	172.31.64.0	255.255.240.0	172.31.76.177		UP		DIR	ECT		
6)	172.31.0.2	255.255.255.255	172.31.48.1		UP		STA	TIC		
Done										

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.



Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **por**tail Azure > Instance de machine virtuelle > Mise en réseauet 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.

	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
)	172.27.2.53	0	NetScaler IP	Active	Enabled	Enabled	NA	Enable
:)	172.27.0.53		SNIP	Active	Enabled	Enabled	NA	Enable
)	172.27.1.53		VIP	Active	Enabled	Enabled	Enabled	Enable
Done								
sh vl	lan							
)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::20d:	3aff:fec9:c26c/64					
	Interfaces : 0/1	1/1 LO/1						
	VIAN ID: 10	VIAN Alias Name						
)	Trtorfocog : 1/2	VLAN AIIds Name:						
	Interfaces : 1/2							
	172 27 2 53	Maole 25	5 255 255 0					
Done	1/2.2/.2.00	, nask. 25	3.233.233.0					
20110								
sh ro	oute							
sh re	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic D	omain Ty	ире
sh ro	Network 0.0.0.0	Netmask 0.0.0.0	Gateway/OwnedIP 172.27.2.1	VLAN 0	State UP	Traffic D 	omain Ty ST#	/pe ATIC
))	Dute Network 0.0.0.0 127.0.0.0	Netmask 0.0.0.0 255.0.0.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1	VLAN 0 0	State UP UP	Traffic D 0 0	omain Ty STP PEF	ATIC ATIC
sh ro))	Network 0.0.0.0 127.0.0.0 172.27.0.0	Netmask 0.0.0.0 255.0.0.0 255.255.255.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.53	VLAN 0 0 0	State UP UP UP	Traffic D 0 0 0	omain Ty STA PEF DIF	/pe ATIC RMANENT RECT
sh ro)))	Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0	Netmask 0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53	VLAN 0 0 0 0 0	State UP UP UP UP	Traffic D 0 0 0 0 0	omain Ty STZ PEF DIF DIF	/pe ATIC RMANENT RECT RECT
sh r))))	Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0	Netmask 255.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0	Gateway/OwnedIP 	VLAN 0 0 0 0 0 0	State UP UP UP UP UP UP	Traffic D 0 0 0 0 0 0 0 0	omain Ty STA PEF DIF DIF DIF	ATIC ATIC RMANENT RECT RECT RECT
sh r()))))	Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0 169.254.0.0	Netmask 255.0.0.0 255.255.255.0 255.255.255.0 255.255.0.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1	VLAN 0 0 0 0 0 0 0	State UP UP UP UP UP UP	Traffic D 	omain Ty STA PEF DIF DIF DIF STA	ADE ATIC RMANENT RECT RECT RECT ATIC
sh r()))))	Network 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0 169.254.0.0 168.63.129.16	Netmask 255.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.255.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1 172.27.0.1	VLAN 0 0 0 0 0 0 0 0 0	State UP UP UP UP UP UP UP UP	Traffic D 	omain Ty STA PEF DIF DIF DIF STA STA	ATIC ATIC RMANENT RECT RECT RECT ATIC ATIC
)))))))	Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0 169.254.0.0 168.63.129.16 169.254.169.254	Netmask 0.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.255 255.255.255.255	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1 172.27.0.1 172.27.0.1	VLAN 0 0 0 0 0 0 0 0 0 0 0 0 0	State UP UP UP UP UP UP UP UP UP UP	Traffic D 0 0 0 0 0 0 0 0 0 0 0 0 0	omain Ty STA PEF DIF DIF DIF STA STA STA	ATIC ATIC RMANENT RECT RECT RECT ATIC ATIC

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.



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 in	nterfaces							
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 DN	S PTR Record							

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)	10.128.4.27	0	NetScaler IP	 Active	 Enabled	Enabled	 NA	Enabled
2)	10.160.0.71		SNIP	Active	Enabled	Enabled 1	NA	Enabled
3)	10.128.0.40		VIP	Active	Enabled	Enabled	Enabled	Enabled
Done								
> sh vl	an							
1)	VLAN ID: 1							
_ /	Link-local IPv6	addr: fe80::4001	:aff:fea0:47/64					
	Interfaces : 0/1	1/1 LO/1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
5	10.128.4.27	Mask: 25	5.255.255.0					
Done								
> sn ro	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main Ty	pe
1.			10, 129, 4, 1				CTN	 TIC
1) 2)	127 0 0 0	255 0 0 0	10.120.4.1		TIP		DED	MANENT
3)	10.128.0.0	255.255.255.0	10.128.0.40		TIP		DTR	ECT
4)	10.128.4.0	255.255.255.0	10.128.4.27	0	UP	0	DIR	ECT
5)	10.160.0.0	255.255.240.0	10.160.0.71		UP		DIR	ECT
Done								
- U								

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.

> sh ns	; ip							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp Vs	server	State
1)	172.31.52.88	0	NetScaler IP	Active	Enabled	Enabled NA	4 	Enabled
2)	172.31.76.177		SNIP	Passive	Enabled	Enabled NA	Ŧ	Enabled
3)	172.31.5.155		VIP	Passive	Enabled	Enabled Er	nabled	Enabled
Done								
> sh vl	.an							
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							
	1FS :	No	5 255 240 O					
Dono	172.31.32.0	o Mask: 25	5.255.240.0					
> eh ro	1114							
/ 511 10	Network	Netmask	Gateway/OwnedIP	VI.AN	State	Traffic Doma	ain Tu	ne
1)	0.0.0	0.0.0.0	172.31.48.1		UP		STA	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
3)	172.31.0.0	255.255.240.0	172.31.5.155		UP		DIR	ECT
4)	172.31.48.0	255.255.240.0	172.31.52.88		UP		DIR	ECT
5)	172.31.64.0	255.255.240.0	172.31.76.177		UP		DIR	ECT
6)	172.31.0.2	255.255.255.255	172.31.48.1		UP		STA	TIC
Done								
S .								

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)



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

🖳 Overview	^ · · · · · · · · · · · · · · · · · · ·	
 Activity log 	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3	
Access control (IAM)	IP configuration \odot	
🗳 Tags	ipconfig1 (Primary)	
Diagnose and solve problems	Construction in the security rules Topology	
Settings	Virtual network/subnet: vsk-mgmt-vnet-southindia/vsk-server-subnet NIC Public IP: 104.211.241.141 NIC Private IP: 172.272.53 Accelerated networking:	Disabled
Networking	Inbound port rules Outbound port rules Application security groups Load balancing	
Overview		
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3	
Access control (IAM)	IP configuration 💿	
🗳 Tags	ipconfig1 (Primary)	
Diagnose and solve problems	Network Interface: vsk-client-nic3 Effective security rules Topology	
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-client-subnet NIC Public IP: 52.172.10.184 NIC Private IP: 172.27.1.53 Accelerated networking	: Disabled
2 Networking	Inbound port rules Outbound port rules Application security groups Load balancing	

Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
🗳 Tags	ipconfig1 (Primary) V
Diagnose and solve problems	Network Interface Vsk-server-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/default NIC Public IP: 52.172.10.59 NIC Private IP: 172.27.0.53 Accelerated networking: Disabled
Networking	Inbound port rules Outbound port rules Application security groups Load balancing

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.

> sn ns	тb							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
1)	172.27.2.53	0	NetScaler IP	Active	Enabled	Enabled	NA	Enable
2)	172.27.0.53	0	SNIP	Active	Enabled	Enabled	NA	Enable
3)	172.27.1.53	0	VIP	Active	Enabled	Enabled	Enabled	Enable
Done								
> sh vl	an							
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: 25	5.255.255.0					
Done								
> sh ro	ute							
	Network	Netmask	Gateway/OwnedIF	VLAN	State	Traffic Do	main Ty	pe
1)			 172 27 2 1				 ST7	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1	0	UP		PEL	MANENT
3)	172.27.0.0	255.255.255.0	172.27.0.53	0	UP		DTE	ECT
4)	172.27.1.0	255.255.255.0	172.27.1.53	0	ПР		DTE	ECT
5)	172 27 2 0	255 255 255 0	172 27 2 53	0	ПР		DTI	TCT
5) 6)	169 254 0 0	255 255 0 0	172 27 0 1		TTP		STI	TTC
7)	168 63 129 16	255 255 255 255 255	172 27 0 1		TIP		ST7	TTC
R)	169 254 169 254	255.255.255.255	172.27.0.1		TIP		STP ST7	TTC
Done	105.251.105.251	200.200.200.200	1/2.2/.0.1		01		511	1110

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)



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 i	nterfaces							
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.

> sh ns	; ip							
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp V	server	State
1)	10.128.4.31		NetScaler IP	Active	Enabled	Enabled N	A	Enabled
2)	10.160.0.75		SNIP	Passive	Enabled	Enabled N	A	Enabled
3)	10.128.0.43	0	VIP	Passive	Enabled	Enabled E	nabled	Enabled
Done								
> sh vl	.an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::4001	:aff:fea0:4b/64					
	Interfaces : 0/1	1/1 LO/1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :	N 1 05						
D	10.128.4.31	Mask: 25	5.255.255.0					
Done								
> sn ro	Matural	Matrical	Contraction data	177 3 31	C+-+-	Turffin Dem	T	
	Network	Netmask	Gateway/Ownedip	VLAN	State	IFAILIC DOM	ain iy	pe
1)	0 0 0 0	0 0 0 0	10 128 4 1		 ПР	0	STA	 TTC
±/ 2)	127 0 0 0	255 0 0 0	127 0 0 1			0	DED	MANENT
3)	10 128 0 0	255 255 255 0	10 128 0 43		TIP	0	DTP	FCT
4)	10.128.4.0	255 255 255 0	10 128 4 31			0	DIN	FCT
5)	10.160.0.0	255.255.255.0	10.160.0.75		TIP	0	DIR	FCT
Done	1011001010	2001200120010	101100101/0		01		DIK	101
>								

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. NetScaler VPX 14.1



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

1	<ns-pre-boot-config></ns-pre-boot-config>
2	<ns-config></ns-config>
3	
4	set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
5	add route 0.0.0.0 0.0.0.0 172.31.48.1
6	set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
7	add route 172.31.0.2 255.255.255.255 172.31.48.1
8	
9	enable ns feature WL SP LB RESPONDER
10	add server 5.0.0.201 5.0.0.201
11	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
12	add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
	persistenceType NONE -cltTimeout 180
13	
14	
15	
16	<ns-bootstrap></ns-bootstrap>
17	<skip-default-bootstrap>YES</skip-default-bootstrap>
18	<new-bootstrap-sequence> NO </new-bootstrap-sequence>
19	
20	
21	
22	

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.

Network Interface eth1		
Interface ID	eni-021961099be6815eb	
VPC ID	vpc-6b258c02	
Attachment Owner	566658252593	
Attachment Status	attached	
Attachment Time	Fri Jan 01 11:11:23 GMT+530 2021	
Delete on Terminate	false	
Private IP Address	172.31.52.88	
Private DNS Name	ip-172-31-52-88.ap-south-	
	1.compute.internal	
Network Interface eth0		
Network Interface eth0 Interface ID	<u>eni-039e5f3329cd879e9</u>	
Network Interface eth0 Interface ID VPC ID	<u>eni-039e5f3329cd879e9</u> vpc-6b258c02	
Network Interface eth0 Interface ID VPC ID Attachment <u>Owner</u>	<u>eni-039e5f3329cd879e9</u> vpc-6b258c02 566658252593	
Network Interface eth0 Interface ID VPC ID Attachment Owner Attachment <u>Status</u>	<u>eni-039e5f3329cd879e9</u> vpc-6b258c02 566658252593 attached	
Network Interface eth0 Interface ID VPC ID Attachment Owner Attachment Status Attachment Time	<u>eni-039e5f3329cd879e9</u> vpc-6b258c02 566658252593 attached Fri Jan 01 10:58:28 GMT+530 <u>2021</u>	
Network Interface eth0 Interface ID VPC ID Attachment Owner Attachment Status Attachment Time Delete on Terminate	<u>eni-039e5f3329cd879e9</u> vpc-6b258c02 566658252593 attached Fri Jan 01 10:58:28 GMT+530 2021 true	
Network Interface eth0 Interface ID VPC ID Attachment Owner Attachment Status Attachment Time Delete on Terminate Private IP A <u>ddress</u>	eni-039e5f3329cd879e9 vpc-6b258c02 566658252593 attached Fri Jan 01 10:58:28 GMT+530 2021 true 172.31.5.155	
Network Interface eth0 Interface ID VPC ID Attachment Owner Attachment Status Attachment Time Delete on Terminate Private IP Address Private DNS Name	eni-039e5f3329cd879e9 vpc-6b258c02 566658252593 attached Fri Jan 01 10:58:28 GMT+530 2021 true 172.31.5.155 ip-172-31-5-155.ap-south-	

Network Interface eth2	
Interface ID	eni-09e55a6cfb791e68d
VPC ID	vpc-6b258c02
Attachment Owner	566658252593
Attachment Status	attached
Attachment Time	Fri Jan 01 11:11:33 GMT+530 2021
Delete on Terminate	false
Private IP Address	172.31.76.177 @
Private DNS Name	ip-172-31-76-177.ap-south-1.compute.internal 但

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	Туре	Mode	Arp	Icmp	Vserve	r State		
)	172.31.52.88	0	NetScaler IP	Active	Enabled	Enabled	NA	Enabled		
Done	4.0.0.101	0	VIP	ACLIVE	Fugbred	Епартеа	Enable	a Enablea		
sh vla	an									
	VLAN ID: 1									
	Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64									
	Interfaces : 1/	'1 1/3 LO/1								
	VLAN ID: 10 VLAN Alias Name:									
	Interfaces : 1/2									
	IPs :									
	172.31.52.	.88 Mask: 25	5.255.240.0							
one										
sh rou	ute									
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic I	omain	Туре		
	0.0.0.0	0.0.0.0	172.31.48.1	0	UP	0	S	TATIC		
	127.0.0.0	255.0.0.0	127.0.0.1	0	UP	0	P	ERMANENT		
	172.31.48.0	255.255.240.0	172.31.52.88	0	UP	0	D	IRECT		
one	172.31.0.2	255.255.255.255	172.31.48.1	0	UP	0	S	TATIC		

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.



1	<ns-pre-boot-config></ns-pre-boot-config>
2	
3	<ns-config></ns-config>
4	
5	set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
6	add route 0.0.0.0 0.0.0.0 172.27.2.1
7	set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
8	add ns ip 172.27.0.61 255.255.255.0 -type SNIP
9	add route 169.254.169.254 255.255.255.255 172.27.0.1
10	add route 168.63.129.16 255.255.255.255 172.27.0.1
11	

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	
20	
21	<ns-bootstrap></ns-bootstrap>
22	
23	<skip-default-bootstrap>YES</skip-default-bootstrap>
24	<new-bootstrap-sequence> NO </new-bootstrap-sequence>
25	
26	
27	
28	

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	Туре	Mode	Arp	Icmp V	Vserver	State
1)	172.27.2.61	0	NetScaler IP	Active	Enabled	Enabled 1	AV	Enabled
2)	172.27.0.61	0	SNIP	Active	Enabled	Enabled 1	AW	Enabled
3) Done	4.0.0.101	0	VIP	Active	Enabled	Enabled H	Enabled	Enabled
> sh vl	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::20d:3	3aff:fec9:9076/64					
	<pre>Interfaces : 0/1</pre>	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	5.255.255.0					
Done								
> sh ro	ute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Dom	nain Ty	pe
1)	0.0.0.0	0.0.0.0	172.27.2.1		UP		STA	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
3)	172.27.0.0	255.255.255.0	172.27.0.61		UP	0	DIR	ECT
4)	172.27.2.0	255.255.255.0	172.27.2.61		UP	0	DIR	ECT
5)	169.254.0.0	255.255.0.0	172.27.0.1		UP	0	STA	TIC
6)	168.63.129.16	255.255.255.255	172.27.0.1		UP	0	STA	TIC
7)	169.254.169.254	255.255.255.255	172.27.0.1		UP		STA	TIC
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 :

1	<ns-pre-boot-config></ns-pre-boot-config>
2	
3	<ns-config></ns-config>
4	
5	set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
6	add route 0.0.0.0 0.0.0.0 10.128.0.1
7	set ns config -nsvlan 10 -ifnum 1/1 -tagged NO
8	
9	enable ns feature WL SP LB RESPONDER
10	add server 5.0.0.201 5.0.0.201
11	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
12	add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 - persistenceType NONE -cltTimeout 180
13	
14	
15	
16	<ns-bootstrap></ns-bootstrap>
17	<skip-default-bootstrap>YES</skip-default-bootstrap>
18	<pre><new-bootstrap-sequence> NO </new-bootstrap-sequence></pre>
19	
20	
21	

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	Vserve	r State
1) 2)	10.128.0.2 4.0.0.101	0 0	NetScaler IP VIP	Active Active	Enabled Enabled	Enabled Enabled	NA Enable	Enabled d Enabled
Done > sh vl	an							
1)	VLAN ID: 1 Link-local IPv Interfaces : 0,	6 addr: fe80::4001 /1 1/2 LO/1	:aff:fea0:4a/64					
2)	VLAN ID: 10 Interfaces : 1, IPs : 10.128.0.;	VLAN Alias Name: /1 2 Mask: 25	5.255.255.0					
Done								
> sh ro	Network	Netmask	Gatewav/OwnedIP	VLAN	State	Traffic D	omain	Tvpe
1)	0.0.0.0	0.0.0.0	10.128.0.1		UP		S	TATIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		P	ERMANENT
3) Done	10.128.0.0	255.255.255.0	10.128.0.2	0	UP	0	D	IRECT

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 :

show cpuparam

Exemple

1

```
    show cpuparam
    Pemode: CPUBOUND
    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.

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

```
nscli> reboot
3
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.

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

```
shell rm -f /nsconfig/.smt_handling
1
2
      Done
3
4
    reboot
5
    Are you sure you want to restart NetScaler (Y/N)?
6
                                                          [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
   netscaler.smt_handling: 0
3
    netscaler.smt_handling_active: 0
4
```

Dépannage

. . .

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

```
1
    > shell sysctl -a | grep smt_handling
2
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.

1	> shell sysctl -a grep smt_handling
2	<pre>netscaler.smt_handling_platform: 1 (available)</pre>
3	<pre>netscaler.smt_handling: 0 (not enabled)</pre>
4	<pre>netscaler.smt_handling_active: 0 (not active)</pre>

Outil NetScaler Sanity Checker

October 17, 2024

L'outil de vérification de l'intégrité évalue la santé et les performances de NetScaler, et identifie également les problèmes de configuration courants.

Remarque:

Actuellement, l'outil NetScaler Sanity Checker n'est pris en charge que pour le cloud AWS.

L'outil NetScaler Sanity Checker exécute également les opérations suivantes :

- Valide la topologie haute disponibilité, la mise en réseau, la gestion des licences et les autorisations.
- Rationalise le processus de résolution des problèmes.
- Permet de résoudre rapidement les problèmes observés dans les clouds publics.
- Génère des résultats dans plusieurs formats tels que des journaux en texte brut, JSON et HTML.

Outil NetScaler Sanity Checker pour AWS

L'outil NetScaler Sanity Checker exécute les validations suivantes en fonction du type de déploiement.

Déploiements autonomes et haute disponibilité dans la même zone	Déploiement haute disponibilité multizone à l'aide d'adresses IP élastiques	Déploiement haute disponibilité multizone à l'aide d'adresses IP privées
 Validation des autorisations IAM Vérification des licences Vérification du stockage Vérification de l'itinéraire des métadonnées Vérification de la résolution DNS Vérification du point de terminaison Amazon EC2 Vérification de la passerelle par défaut Vérification de la configuration du LAN 	 Validation des autorisations IAM Vérification des interfaces Vérification des adresses IP élastiques Vérification du mode INC Vérification IPSet 	 Validation des autorisations IAM Vérification des interfaces Vérification des itinéraires Vérification de l'index des appareils Vérification Src/Dst
Vérification de l'ARP Exécutez foutil Sality Check	ker à l'aide de la CLI NetScale	r

À l'inveloueboorannees, tapez :

1 > Shell
2 > root@ns# sanitychecker -c [standalone | multizone]

Après avoir exécuté l'outil Sanity Checker, les fichiers suivants sont générés aux formats JSON et HTML.

- /var/cloudsanitychecker/results.json
- /var/cloudsanitychecker/standalone.html

Ces fichiers contiennent les résultats détaillés des vérifications effectuées, qui peuvent servir à identifier et à analyser les problèmes potentiels.

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.

Installer une instance NetScaler VPX sur Citrix Hypervisor/XenServer

January 15, 2025

Pour installer des instances VPX sur Citrix Hypervisor/XenServer, 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/XenServer

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.
Carte d'interface réseau	Note: L'installation de l'hyperviseur crée une ଅନ୍ୟେମ୍ଟିସେମ୍ଟିସିହିସ୍ଟିସେମ୍ପ ମିଟିଧ୍ୟିମ୍ବିତିଥିର୍ଦ୍ଧୋମ୍ପରେମ୍ପର୍ମତା de ମନ୍ତ୍ୟଙ୍କେଟ୍ଟିମ୍ବିବିସ୍ଟିସେମ୍ବି ନିର୍ବାଧିକରେ restant est
	disponible pour l'instance NetScaler VPX et d'

Pour plus d'informations, consultez la page Documentation de la page Documentation de la page de la

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 in-stance nCore VPX

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.
- 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)

January 30, 2025

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_l*

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>
1
```

Exemple

```
1
    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
1
2
                uuid ( R0) : e2874343-f1de-1fa7-8fef-98547c348783
3
4
                device (RO): eth18
5
    currently-attached ( R0): true
6
                  VLAN ( RO): -1
          network-uuid ( R0): f865bd85-44dd-b865-ab65-dcd6ae28c16e
7
```

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=<
1
       physical-pif-uuid>
```

Exemple

1

```
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 :

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

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 :

```
1 [root@citrix-XS82-TOPO ~]# xe vm-list
2 uuid ( R0): b507e8a6-f5ca-18eb-561d-308218a9dd68
3 name-label ( RW): sai-vpx-1
4 power-state ( R0): 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.

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

Exemple

[root@citrix-XS82-TOP0 ~]# xe vif-destroy uuid=3e1e2e58-b2ad-6 dc0-61d4-1d149c9c6466

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.

Autres références

Cartes réseau compatibles SR-IOV

Ajouter un réseau SR-IOV

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.vm ware.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.ymware.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			

NetScaler VPX 14.1

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 dialogueDéployer le modèle OVF, dansDéployer 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.

Virtual Hardware VM C	options SDRS Rules	VA	op Options	3		
CPU	2	•	0	_		
Memory	2048	F	MB	-		
🚐 Hard disk 1	20		GB	-		
G SCSI controller 0	LSI Logic Parallel				/	
属 Network adapter 1	VM Network			-	Connect	
💌 Network adapter 2	1/2			-	Connect	
📕 Video card	Specify custom setting	gs		-		
WCI device						
Other Devices						
Upgrade	Schedule VM Comp	atibil	ity Upgrad	le		
New device:	Select		-	-	Add	

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

Virtual Hardware VM Options	SDRS Rules vApp Options
🕶 🔲 *CPU	4 🔹 🕢
Cores per Socket	1 Sockets: 4
CPU Hot Plug	Enable CPU Hot Add
Reservation	0 v MHz v
Limit	Unlimited
Shares	Normal - 4000 -
CPUID Mask	Expose the NX/XD flag to guest - Advanced
Hardware virtualization	Expose hardware assisted virtualization to the guest OS
Performance counters	Enable virtualized CPU performance counters
Scheduling Affinity	Hyperthreading Status: Active Available CPUs: 24 (logical CPUs) Select logical processor affinity for this virtual machine. Use '-' for ranges and ',' to separate values. For example, "0, 2, 4- 7" would indicate processors 0, 2, 4, 5, 6 and 7. Clear the string to remove affinity settings.
CPU/MMU Virtualization	Automatic ESXi can automatically determine if a virtual machine should use
New device:	Select Add

- 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.

	ons	App Opti	lules	SDR	VM Options	ual Hardware
	0	-		4		* CPU
4	Sockets:	1 Soc		ocket	Cores per Socket	
		t Add	CPU	En	Ig	CPU Hot Plu
•	MHz	-		0		Reservation
•	MHz	Hz	value: (Curre		Limit
-	4000	Hz	n: (Minin		Shares
+ Adva	uest	6 MHz	n: 8	Maxir	c	CPUID Mask
tion to the	ed virtualiz	e assist	e hard	Exp	tualization	Hardware vir
e counters	erforman	d CPU p	e virtua	🗌 En	e counters	Performance
al CPUs)	: Active 24 (log	ig Status Js:	erthrea Iable C	ł	Affinity	Scheduling /
Add	-		Select ·		levice:	New d

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

Virtual Hardware VM Options	SDRS Rules	vApp Op	tions		
- 🗖 *CPU	4	•	0		
Cores per Socket	1 +		Sockets: 4		
CPU Hot Plug	Enable CPU H	ot Add			
Reservation (*)	8396	-	MHz	-	
Limit	Unlimited	-	MHz	-	
Shares	Current value: Ur	nlimited	4000	-	
CPUID Mask	Minimum: 83	396 MHz	guest	-	Advar
Hardware virtualization	Maximum: Unlimited ted virtualization to the				
Performance counters	📃 Enable virtualiz	zed CPU	performan	ce cou	nters
Scheduling Affinity	Hyperthread Available CF	ling Statu PUs:	ıs: Active 24 (log	gical Cl	PUs)
New device:	Select		-	Ad	d

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

Virtual Hardware VM Option:	SDRS Rules V	App Opt	ions			
🗸 🔲 *CPU	4	•	0			
Cores per Socket	1	-	Sockets	: 4		
CPU Hot Plug	Enable CPU Ho	ot Add				
Reservation (*)	8396	-	MHz	-		
Limit	Unlimited	-	MHz	-		
Shares (*)	Custom	•	4000	-		
CPUID Mask	Expose the NX/XE) fl. Mini	mum 0		Adva	
Hardware virtualization	Expose hardware Maximum 10000 n to the					
Performance counters	Enable virtualized CPU performance counters					
Scheduling Affinity	Hyperthreadin Available CPU Select logical proc	ng Statu Us: essor af	s: Active 24 (Io finity for th	gical iis viri	CPUs) tual ma	
New device:	Select		-	-	Add	

- 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.

al Hardware VM Optic	ons SDRS R	Rules	vApp Opt	ions			
*CPU	4		•	0			
*Memory							
RAM (*)	8396		-	MB	-		
Reservation	0		-	MB	-		
	Reser	ve all g	uestmem	ory (All loc	ked)		
Limit	Unlimite	d	-	MB	-		
Shares	Normal		-	83960	-		
Memory Hot Plug	Enable	1					
Hard disk 1	20	20 🖨 GB			-		
SCSI controller 0	LSI Logic	Paralle	el				
Network adapter 1	VM Netw	VM Network			-	∎c	0
Network adapter 2	1/2				•	₫c	C
New device:	5	Select -		-	P	\dd	1

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.

irtual Hardware VM Opti	ons	SDRS Rules	vApp Op	tions		
CPU *CPU	4		•	0		
Memory						
RAM (*)	8	192	-	MB	-	
Reservation (*)	8	192	¥	MB	-	
	V	Reserve all g	guestmem	nory (All Io	cked)	
Limit	L	Inlimited	-	MB	-	
Shares	N	Iormal	-	81920		
Memory Hot Plug		Enable				
🚍 Hard disk 1	20		* *	GB	-	
💁 SCSI controller 0	LS	SI Logic Paral	lel			
🗾 Network adapter 1	adapter 1 VM Network			-	⊻ co	
Network adapter 2	1	/2			•	⊻ Co
New device:		Select			A	bb

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

		1	2				1
/irtual Hardware	VM Options	SDRS Rules	vApp Opti	ons			
CPU *CPU		4	•	0			
Memory							
RAM (*)		8192	•	MB	-		
Reservation	(*)	8192		MB	-		
		🔄 Reserve all g	uestmemo	ory (All loci	ked)		
Limit		Unlimited	-	MB	-		
Shares		Normal 👻		81920			
Memory Hot Plug		Enable					-
🕨 🛄 Hard disk 1		20	* *	GB	-		
G SCSI control	er 0	LSI Logic Parall	el				
🕨 ় Network adapter 1		VM Network			+	🗹 Co	0
Network adapter 2		1/2				√ Co	D
New d	evice:	Select			A	dd	1
				-		•	

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

Virtual Hardware VM C	ptions	SDRS Rules	vApp Opt	ions			
CPU		4		0			-
- 🌆 *Memory							
RAM (*)		8192	•	MB	-		
Reservation (*)		8192	•	MB	-		
		Reserve all g	uestmem	ory (All loc	ked)		
Limit		Unlimited	-	MB	-		
Shares (*)		Custom	-	00000	-		
Memory Hot Plug		Enable	Minimum 1				
🕨 🛄 Hard disk 1		20	Maximum 10000				
G_ SCSI controller 0		LSI Logic Parall	el				
Metwork adapter 1		VM Network		-	⊡ Co	5	
🕨 🗾 Network adapter 2		1/2			-	⊡ Co	2
New device:	<u> </u>	Select			A	dd	1

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

🔂 NSVPX-DEMO - Edit Se	ettings		? ₩
Virtual Hardware VM O	ptions SDRS Rules vA	pp Options	
▶ ■ *CPU	4	• 0	
Memory	A New Hard Disk	▼ MB ▼	
Hard disk 1	Existing Hard Disk	GB V	
▶ G SCSI controller 0	😤 RDM Disk		
Metwork adapter 1	Network	Connect	
Network adapter 2		Connect	
🕨 💻 Video card	CD/DVD Drive	tings 🗸 🗸	
► 00 VMCI device	Floppy Drive		
 Other Devices 	oo Serial Port		
▶ Upgrade	Parallel Port	mpatibility Upgrade	
New Network	Host USB Device	Connect	
	• USB Controller		
	SCSI Device		
	PCI Device		
	SCSI Controller		
	SATA Controller		
New device:	Metwork	Add	
Compatibility: ESXi 5.5 and	d later (VM version 10)	ок с	ancel

- 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.

🚯 NSVPX-ESX - Edit Settings		? ₩
Virtual Hardware VM Options	SDRS Rules vApp Options	
▶ 🔲 CPU	4 • •	
▶ 🏧 Memory	8192 v MB v	
▶ 🛄 Hard disk 1	20 GB V	
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
Network adapter 1	VM Network	
▶ 🛄 Video card	Specify custom settings	
VMCI device		
▶ Other Devices		
👻 🌉 New Network	1/2 🗸	
Status	Connect At Power On	
Adapter Type	VMXNET 3	
DirectPath I/O	E1000	
MAC Address	SR-IOV passthrough Automatic V	
	VIMAINET 3	
New device:	Metwork Add	
Compatibility: ESXi 6.0 and later	(VM version 11) OK Ca	ancel

- 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 :

1	>	show interface	summary			
2						
3		Interface	MTU	MAC	Suffix	
4						
5	1	0/1	1500	00:0c:29:89:1d:0e	NetScaler Vir	
		rface, VMXNE	ГЗ			
6	2	1/1	9000	00:0c:29:89:1d:18	NetScaler Vir	
		rface, VMXNE	ГЗ			

_ _ _

7 3	1/2	9000	00:0c:29:89:1d:22	NetScaler Vir
r 8 4	face, VMXN LO/1	ET3 9000	00:0c:29:89:1d:0e	Netscaler Loopback

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.

Navigator 📕	3 10.102.38.201 Actions -			=
Home	Getting Started Summary Mo	onitor Manage Relate	d Objects	
10.102.38.250	Settings Networking Storage	Alarm Definitions Tags	Permissions	
 ▼ Im VPX ▶ Im 10.102.100.100 ▶ Im 10.102.38.201 	Virtual switches	Physical adapters	∎ • (Q Filter	
10.217.195.204	VMkernel adapters	Observed IP ranges	Wake on LAN Support	SR-IOV Status
M 10.211.133.220	Physical adapters	No networks	No	Disabled
	TCP/IP configuration	No networks	No	Disabled
	Advanced	No networks	No	Enabled
		No networks	No	Disabled
		No networks	No	Disabled
		No networks	No	Disabled
		4		•

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

vmware [®] vSphere	Web Client _ ਜ ≘	U Ad	ministrator@VSPHERE	Local 🕶 丨	Help
Navigator I	🔂 10.102.38.201 Actions 🔻				=*
Home	Getting Started Summary M	Ionitor Manage Related	Objects		
▼	Settings Networking Storage	Alarm Definitions Tags	Permissions		
	K 44 Virtual switches	Physical adapters			
 10.217.195.20 10.217.195.22 	VMkernel adapters	Observer P ranges	Wake on LAN Support	SR-IOV Status	•
	TCP/IP configuration	No networks	No No	Disabled Disabled	
	Advanced	No networks	No	Enabled	
		No networks	No	Disabled	_
		No networks	No :::	Disabled	v F
		Physical network adapter	: vmnic5		
		All Properties CD	P LLDP		
		Adapter	Intel Cor 10 Gigab Network	poration 82599 vit Dual Port Connection	
		Name	vmnic5		

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

飅 vmnic5 - Edit Settings	?
Configured speed, Duplex:	Auto negotiate 🔹 🔻
SR-IOV	
SR-IOV is a technology that all to use the same PCI device as Status:	ows multiple virtual machines a virtual pass-through device.
Number of virtual functions:	Enabled
🔄 Changes will not take effec	Disabled t until the system is restarted.
	OK Cancel

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

💌 vmnic5 - Edit Settings		?
Configured speed, Duplex:	Auto negotiate	•
SR-IOV		
SR-IOV is a technology that all to use the same PCI device as Status:	ows multiple virtual mach s a virtual pass-through de Enabled	ines evice.
Number of virtual functions:	1	*
📌 Changes will not take effec	t until the system is restai	ted.
	ОК	Cancel

- 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**.

Configure VM Compatibility	?	**
Select a compatibility for virtual machine upgrade.		
Compatible with: ESXi 5.5 and later	0	
This virtual machine uses hardware version 10, which is also compatible with ESXi 6.0.		
ОК Са	incel)

3. Cliquez avec le bouton droit sur l'instance NetScaler VPX et cliquez sur Modifier les paramètres.
| NSVPX-ESX-DEMO - E | Edit Settings | | | | ? |
|---------------------------|------------------------|---------|-------------|-----------|----------|
| Virtual Hardware VM C | options SDRS Rule | s vA | App Optior | IS | |
| CPU | 2 | - | 0 | | |
| Memory | 2048 | - | MB | | |
| 🚐 Hard disk 1 | 20 | | GB | • | |
| G SCSI controller 0 | LSI Logic Parallel | | | | |
| 属 Network adapter 1 | VM Network | | | ✓ Connect | |
| 飅 Network adapter 2 | 1/2 | | | Connect | |
| 📃 Video card | Specify custom sett | ings | | • | |
| 🔅 VMCI device | | | | | |
| Other Devices | | | | | |
| Upgrade | Schedule VM Con | npatib | ility Upgra | de | |
| | | | | | |
| New device: | Sele | ct | | Add | |
| ompatibility: ESXi 5.5 an | d later (VM version 10 |) | | 0 | K Cancel |

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

/irtual Hardware VM Option:	s SDRS Rules vApp Options
F 🔲 *CPU	4 🖉 🛛
Cores per Socket	1 Sockets: 4
CPU Hot Plug	Enable CPU Hot Add
Reservation	0 • MHz •
Limit	Unlimited
Shares	Normal 🔍 4000 👻
CPUID Mask	Expose the NX/XD flag to guest - Advanced
Hardware virtualization	Expose hardware assisted virtualization to the guest OS
Performance counters	Enable virtualized CPU performance counters
Scheduling Affinity	Hyperthreading Status: Active Available CPUs: 24 (logical CPUs) Select logical processor affinity for this virtual machine. Use '-' for ranges and ',' to separate values. For example, "0, 2, 4- 7" would indicate processors 0, 2, 4, 5, 6 and 7. Clear the string to remove affinity settings.
CPU/MMU Virtualization	Automatic SXi can automatically determine if a virtual machine should use
New device:	Select Add

- 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.

		ons	vApp Opti	SDRS Rules	VM Options	irtual Hardware
		0	•	4		🔲 *CPU
	4	Sockets:	-	1	ocket	Cores per So
			lot Add	Enable CPU	g	CPU Hot Plu
	-	MHz	-	0		Reservation
	-	MHz	MHz	Current value:		Limit
	-	4000	MHz	Minimum:		Shares
ldvar	-	guest	396 MHz	Maximum:		CPUID Mask
o the	ation	ted virtualiz	are assis	Expose hard	tualization	Hardware vir
nters	e co	performanc	zed CPU (📃 Enable virtua	counters	Performance
vUs)	cal C	s: Active 24 (log	ding Status PUs:	Hyperthre: Available (ffinity	Scheduling A
1	A	-		Select	evice:	New d

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

Virtual Hardware VM Option	IS SDRS Rules	vApp Op	tions			
- 🔲 *CPU	4	-	0			
Cores per Socket	1	-) Sockets:	4		
CPU Hot Plug	Enable CPI	J Hot Add				
Reservation (*)	8396	-	MHz	-		
Limit	Unlimited	-	MHz	-		
Shares	Current value	: Unlimited	4000	-		
CPUID Mask	Minimum:	Minimum: 8396 MHz		-	Adva	
Hardware virtualization	Maximum:	Maximum: Unlimited sted virtualization to				
Performance counters	📃 Enable virtu	alized CPU	performan	ce co	unters	
Scheduling Affinity	Hyperthro Available	eading Stati CPUs:	us: Active 24 (log	gical (CPUs)	
New device:	Selec	:t	-	A	dd	

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

Virtual Hardware VM Opti	ons SE	ORS Rules	vApp C	ptic	ons		
🕶 🔲 *CPU	4			•	0		
Cores per Socket	1			-	Sockets	: 4	
CPU Hot Plug	E	Enable CPU I	Hot Add				
Reservation (*)	839	96		•	MHz	-	
Limit	Un	limited		•	MHz	-	
Shares (*)	Cu	stom		•	4000	-	
CPUID Mask	Exp	oose the NX/	XD fl M	inim	num 0		Adva
Hardware virtualization	ם 🗌 ב	xpose hardv	vare M	axin	num 100	00	n to th
Performance counters	E	Enable virtual	ized CP	Uр	erformai	nce co	ounters
Scheduling Affinity	Sele	Hyperthrea Available C ect logical pro	ding Sta PUs: ocessor	atus affi	Active 24 (Io nity for th	gical nis vir	CPUs) tual ma
New device:	-	Select -			-	1	٨dd

- 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.

al Hardware VM Option	ons	SDRS Rules	vApp Op	tions			
*CPU	(4		0			
*Memory							
RAM (*)		8396	-	MB	-	ĺ	
Reservation		0	-	МВ	•)	
	[Reserve all g	uestmem	nory (All loc	ked)		
Limit		Unlimited		MB	-)	
Shares		Normal	-	83960	-		
Memory Hot Plug	1	Enable					
Hard disk 1	[20 GB			-	Ì	
a SCSI controller 0		LSI Logic Parall	el				
Network adapter 1		VM Network			+	l∎ c	:0
Network adapter 2	(1/2			•	⊻ c	0
New device:		Select				Add	1

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.

	ions	o Opti	vAp	SDRS Rules	VM Options	tual Hardware
0	0	-		4		🗖 *CPU
						Memory
в 💽	MB	-		8192		RAM (*)
в 💌	MB	-		8192	(*)	Reservation
All locked)	ory (All	nemo	juest	🖌 Reserve all g		
в 🖵	MB	-		Unlimited		Limit
1920 👻	819	-		Normal		Shares
				Enable	Plug	Memory Hot
B	GB	-		20		🔜 Hard disk 1
			el	LSI Logic Paralle	ler 0	🛃 SCSI control
▼ 20	VM Network				pter 1	📕 Network ada
- I				1/2	pter 2	📕 Network ada
Add				Select -	evice:	New d

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

		s	ioi	Opt	vApp	SDRS Rules	VM Options	ual Hardware
)	1	•		4		∎ *CPU
								*Memory
ĺ	-	MB		-		8192		RAM (*)
)	-	MB	(-		8192	Reservation (*)	
	(ed)	Reserve all guest memory (All locked						
)	-	MB	(-	Unlimited -		Limit	
1	-	81920		-		Normal		Shares
		Enable					Plug	Memory Hot
)	-	GB	20 (GB			20		🔒 Hard disk 1
					el	LSI Logic Paralle	ler 0	SCSI control
) 🗹 c	-	VM Network					pter 1	Network ada
) 🗹 c	•					1/2	💌 Network adapter 2	
Add	1		-			Select -	evice:	New d

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

Virtual Hardware	VM Options	SDRS Rules	vApp Opti	ions		
🕨 🔲 *CPU		4	•	0		
🕶 🌃 *Memory						
RAM (*)		8192	-	MB	-	
Reservation (*)		8192	-	MB	-	
		🔄 Reserve all g	uestmem	ory (All loc	ked)	
Limit		Unlimited .		MB	-	
Shares (*)		Custom	-	00000	-	
Memory Hot I	Plug	Enable	Minir	mum 1		
🕨 🛄 Hard disk 1		20	Maxi	mum 100	00	
🛛 🛃 SCSI controll	er 0	LSI Logic Parall	el			
🕨 🗾 Network ada	pter 1	VM Network				[Co
Network ada	pter 2	1/2			-	[Co
New d	evice:	Select			Add	

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

Virtual Hardware VM O	otions	SDRS Rules v	App Optic	ons			
CPU		4	-	0			
Hard disk 1	A Ne	ew Hard Disk disting Hard Disk DM Disk	•	MB GB			
Network adapter 1	mi Ne	etwork	Jk-DVS	1)	- -	Connect.	8
Status Port ID	CI	D/DVD Drive oppy Drive	rOn				
Adapter Type	010 Se ▲ Pa ∦ Ho ≪ US	erial Port arallel Port ost USB Device SB Controller	ual mac ough de ite with hachine	chine op evices a vMotion, s.	eration re pres or take	is are unavaila sent. You cann e or restore sn	ble when ot apshots
Physical function MAC Address Guest OS MTU Cha	SC C	CSI Device CI Device			•	Automatic	•
Video card	ାତ କୁ	CSI Controller ATA Controller	tings		•		
New device:		对 Network		•	A	dd	

- 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.

NSVPX-ESX - E	dit Settings				?
Virtual Hardware	VM Options	SDRS Rules	vApp Options		
🕨 🛄 Hard disk 1		20	GB	•	
🕨 🛃 SCSI controll	er 0	LSI Logic Para	llel	20	
🕨 飅 Network adap	oter 1	VM Network		🚽 🗹 Connect	
🕨 🎫 Network adap	oter 2	VM Network 2		Connect	
🕨 🛄 Video card		Specify custor	m settings	-	
VMCI device					
Other Devices					
🕶 飅 New Network	ĸ	CITRIX_PG1 (DVS_SRIOV_CITRIX) 🚽	
Status		Connect At I	Power On		
Port ID					
Adapter Type		SR-IOV passt	hrough		
		E1000		is are unavailable wh	nen
		SR-IOV passt	nrough	e or restore snapsho	ts
		VMXNET 3			
Physical func	tion	vmnic4 0000:	03:00.0 Intel Corp	•	
MAC Address	5			Automatic 🛛 🗸	
Guest OS MT	U Change	Disallow		•	
New de	evice:	飅 Netwo	ork 💌	Add	
compatibility: ESXI	6.0 and later (vm version 11)		ОК	Cancel

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

🚯 NSVPX-ESX - Edit Settings		? ••
Virtual Hardware VM Options	SDRS Rules vApp Options	
🕨 🛄 Hard disk 1	20 GB V	•
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
Metwork adapter 1	VM Network 🖉 Connect	
▶ 飅 Network adapter 2	VM Network 2	
Video card	Specify custom settings	
VMCI device		
▶ Other Devices		
👻 飅 New Network	CITRIX_PG1 (DVS_SRIOV_CITRIX)	
Status	Connect At Power On	
Port ID		
Adapter Type	SR-IOV passthrough	
	Note: Some virtual machine operations are unavailable when SR-IOV passthrough devices are present. You cannot suspend, migrate with vMotion, or take or restore snapshots of such virtual machines.	
Physical function	vmnic4 0000:03:00.0 Intel Corp 💌	
MAC Address	vmnic4 0000:03:00.0 Intel Corporation 82599 10 Gigabit Dual	
Guest OS MTU Change	Disallow	-
New device:	🐖 Network <	
Compatibility: ESXi 6.0 and later	(VM version 11) OK Can	cel

- 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**.

NSVPA-ESA-DEMO - Edit Setti	igs (r	
/irtual Hardware VM Options	SDRS Rules VApp Options	
VMware Tools	Expand for VMware Tools settings	1
Power management	Expand for power management settings	
Boot Options	Expand for boot options	1
Advanced		
Settings	Disable acceleration	
	✓ Enable logging	
Debugging and statistics	Run normally 🔹	1
Swap file location	 Default Use the settings of the cluster or host containing the virtual machine. Virtual machine directory Store the swap files in the same directory as the virtual 	
	 Datastore specified by host Store the swap files in the datastore specified by the host to be used for swap files. If not possible, store the swap files in the same directory as the virtual machine. Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines. 	
Configuration Parameters	Edit Configuration	Í
Latency Sensitivity	High 🔹 🚯 🔥 Check CPU reservation 🚯	
ompatibility: ESXi 5.5 and later (V	Low Normal Medium OK Cance	

- 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	МТО	MAC	Suffix	

4					
5	1	0/1 Interface	1500	00:0c:29:1b:81:0b	NetScaler Virtual
6	2	10/1	1500	00:50:56:9f:0c:6f	Intel 82599 10G VF
7	3	10/2	1500	00:50:56:9f:5c:1e	Intel 82599 10G VF
8	4	Interface 10/3	1500	00:50:56:9f:02:1b	Intel 82599 10G VF
9	5	Interface 10/4	1500	00:50:56:9f:5a:1d	Intel 82599 10G VF
10	6	Interface 10/5	1500	00:50:56:9f:4e:0b	Intel 82599 10G VF
11	7	Interface L0/1	1500	00:0c:29:1b:81:0b	Netscaler Loopback
		interface			
12	Do	one			
13	> 5	show inter 10	/1		
14	1)	Interfa	ce 10/1 (Intel 82599 10G VF Inte	rface) #1
15		flags=0	xe460 <en< td=""><td>ABLED, UP, UP, HAMON, 8</td><td>02.1q></td></en<>	ABLED, UP, UP, HAMON, 8	02.1q>
16		MTU=150 h21m	0, native n53s	vlan=55, MAC=00:50:56:	9f:0c:6f, uptime 0
17		Actual: thro	media FI oughput 10	BER, speed 10000, duple 000	x FULL, fctl NONE,
18		LLDP Mo	de: NONE,	LR Pri	ority: 1024
19					2
20		RX: Pkt Stal	s(8380207 lls(0)	42) Bytes(860888485431)	Errs(0) Drops(2527)
21		TX: Pkt Stal	s(8381499 lls(0)	54) Bytes(860895860507)	Errs(0) Drops(0)
22		NIC: In (0)	Disc(0) O	utDisc(0) Fctls(0) Stal	ls(0) Hangs(0) Muted
23		Bandwid	th thresh	olds are not set.	
24	Do	one			

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

- 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.

irtual Hardware VM Options						
Add hard disk 🛛 🛤 Add network a	dapter		Add other device			
CPU	5	0	CD/DVD drive			
Managa		-	Floppy drive			
Memory	12	010	Serial port			
Hard disk 1	20	B	Parallel port			8
SCSI Controller 0		÷¢	USB controller			
	LSI	1	USB device	~		8
Metwork Adapter 1	VM	0	Sound controller	🗸 🗸 Conr	nect	\otimes
Matwork Adapter 2	PG1		PCI device	🗸 🗹 Conr	nect	0
Video Card	Spa		Dynamic PCI device			
	Spe	¢	SCSI controller			
PCI device 1	c6x0	SATA	SATA controller		~	\otimes
PCI device 2	c6x0	17	NVMe controller		~	0

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

Network Adapter 2	PG1-v1	V 🗹 Co	nnect	\otimes
Jideo Card	Specify custom settings	~		
FCI device 1	c6xx QAT VF - 0000:1a:01.0		~	8
PCI device 2	c6xx QAT VF - 0000:1b:01.0		~	8
PCI device 3	c6xx QAT VF - 0000:1a:01.1		~	\otimes
PCI device 4			~	\otimes
PCI device 5	c6xx QAT VF - 0000:1b:01.1		~	\otimes
PCI device 6	c6xx QAT VF - 0000:1b:01.2		~	\otimes
PCI device 7	c6xx QAT VF - 0000:1b:01.3		~	\otimes
New PCI device	c6xx QAT VF - 0000:1a:01.4		~	8

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.

> stat ssl	
SSL Summary	
# SSI cardo procont	,
# SSL Cards present	1
# SSL cards UP	1
SSL engine status	1

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

April 1, 2025

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**.

All PCI Devices					
-				Q FI	Iter -
ID		Status	Vendor Name	Device Name	ESX Name
V 0000:05:00	✔ 🜆 0000:05:00.3		Intel Corporation	Ethernet Controll	*
🗹 📷 0000:05:00	0.0	Available	Intel Corporation	Ethernet Controll	
0000:0 📷 🗌	0:1A.0	Unavailable	Intel Corporation	Wellsburg USB	
▼ 0000:00:1	C.4	Not Configurable	Intel Corporation	Wellsburg PCI E	
▼ 0000:0	9:00.0	Not Configurable	ASPEED Techn	AST1150 PCI-to	
	0.00:0A:00.0	Unavailable	ASPEED Techn	ASPEED Graphi	
0000:0 📷 🗌	0:1D.0	Unavailable	Intel Corporation	Wellsburg USB	
▼ 0000:80:0	3.0	Not Configurable	Intel Corporation	Haswell-E PCI E	•
1 device will become	available when this	host is rebooted.		00500ED (0.0)	
0000:00:01.0					
This device cannot be	e made available for	VMs to use			
Name	Haswell-E PCI Ex	Haswell-E PCI Express Root Port 1		Intel Corporation	
Device ID	2F02		Vendor ID	8086	
Subdevice ID	0		Subvendor ID	0	
Class ID	604				
Bus Location					
ID	0000:00:01.0		Slot	1	
Bus	0		Function	0	
					OK Cancel

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**.

B NSVPX-ESX-DEMO -	Edit Settings		(?) ₩
Virtual Hardware VM C	Options SDRS Rules	vApp Options	
F 🔲 CPU	2	• 0	
► III Memory	4096	▼ MB ▼	
▶ → Hard disk 1	20	GB V	
▶ I SCSI controller 0	LSI Logic Parallel		
Network adapter 1	VM Network	Connect	
Video card	Specify custom setting	gs 🛛 🗸	
VMCI device			
 Other Devices 			
Now dovice:			
New device:		evice Add	
Compatibility: ESXi 6.0 an	d later (VM version 11)	ОК	Cancel

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.

NSVPX-ESX-DEMO - Edit S	ettings	6	? }
Virtual Hardware VM Options	SDRS Rules	vApp Options	
▶ 🔲 CPU	2	• 0	
▶ Image Memory	4096	▼ MB ▼	
▶ 🛄 Hard disk 1	20	GB V	
▶ G SCSI controller 0	LSI Logic Paralle	llel 4816	
▶ Image Network adapter 1	VM Network	Connect	
▶ Uideo card	Specify custom	m settings 🛛 🖵	
▶ i VMCI device			
 Other Devices 			
✓ New PCI device	0000:05:00.3 1	Intel Corporation Ethe	
Physical PCI/PCIe device	0000:05:00.3 In 10GbE SFP+	Intel Corporation Ethernet Controller X710 for	
	Note: Some PCI/PCIe pa suspend, mig such virtual r	e virtual machine operations are unavailable when passthrough devices are present. You cannot nigrate with vMotion, or take or restore snapshots of I machines.	
New device:	📴 PCI De	Device Add	
Compatibility: ESXi 6.0 and later	(VM version 11)	OK Canc	el

5. 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

April 1, 2025

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 & lt; NS-CONFIG> section:

```
<NS-PRE-BOOT-CONFIG>
1
2
3
         <NS-CONFIG>
4
             add route 0.0.0.0 0.0.0.0 10.102.38.1
5
         </NS-CONFIG>
6
         <NS-BOOTSTRAP>
7
                 <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
8
9
                  <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
11
             <MGMT-INTERFACE-CONFIG>
                      <INTERFACE-NUM> eth0 </INTERFACE-NUM>
12
13
                      <IP> 10.102.38.216 </IP>
14
                      <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
15
             </MGMT-INTERFACE-CONFIG>
         </NS-BOOTSTRAP>
16
17
18
     </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 :

 Créez un fichier dont le nom contient user data 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.

```
1
     root@ubuntu:~/sai/14jul2021# ls -l total 4
2
     drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
3
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
4
5
     -rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
6
     root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
          ./esx_preboot_userdata
     I: -input-charset not specified, using utf-8 (detected in locale
7
         settings)
     Total translation table size: 0
8
9
     Total rockridge attributes bytes: 0
10
     Total directory bytes: 112
     Path table size(bytes): 10
11
     Max brk space used 0
12
13
     176 extents written (0 MB)
14
     root@ubuntu:~/sai/14jul2021# ls -lh
15
     total 356K
     drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
16
17
     -rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.
        iso
18
     root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
19
20
     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
21
         settings)
22
     Total translation table size: 0
23
     Total rockridge attributes bytes: 0
24
     Total directory bytes: 112
     Path table size(bytes): 10
26
     Max brk space used 0
27
     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.

🎦 New virtual machine - sai-test-iso						
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options Select deployment options					
5 Ready to complete	Network mappings	VM Network VM Netwo	rk		v	
	Disk provisioning	Thin O Thick				
	Power on automatically	D				
vmware						
			Back	Next	Finish	Cancel

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

Edit settings - sai-test-iso (ESXi 5.1	virtual n	achine)		
Virtual Hardware VM Options				
🔜 Add hard disk 🛛 🛤 Add network a	dapter	Add other device		
+ 🔲 CPU	2	CD/DVD drive		
h W Managa		Floppy drive		
ma memory	2	Serial port		
Hard disk 1	20	Parallel port		0
► IM SCSI Controller 0		USB controller		-
	LSI	use device		0
INTERPORT Network Adapter 1	VM	Sound controller	V Connect	٥
🕨 🎆 Video Card	Spe	PCI device	~	
		Dynamic PCI device		
		CSI controller		
			Save	Cance

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

Virtual Hardware VM Options			
🔜 Add hard disk 🛛 🎫 Add network a	idapter 🗧 Add other device		
• 🔲 CPU	2 v		
Memory	2 GB ~		
) 🔚 Hard disk 1	20 GB ~		0
SCSI Controller 0	LSI Logic Parallel		۵
Main Network Adapter 1	VM Network	Connect	۵
New CD/DVD Drive	Host device	Connect	0
🕨 🛄 Video Card	Host device Datastore ISO file		

6. Select a Datastore in the vSphere Client.

🔯 Datastore browser			
🛉 Upload 📑 Download	🙀 Delete 🛛 🔒 Move 👔 C	opy 🏾 🎦 Create dir	rectory 🛛 🤁 Refresh
🧮 datastore1	៉ .sdd.sf	💿 esx	
늘 vmimages	🚞 centosiso	i pre	1
	늘 centosnirmal_225	i pre	esx_preboot_userdata.i
	늘 fips-t1	i pre	Wednesday, July 14, 2
	늘 fips1	💿 pre	
	៉ sai-test-iso	🍥 pre	
	🚞 sai-test-rs130	sai	
	🚞 sai-vpx-2	🛄 sai	
	늘 sai-vpx-test	sai	
	늘 sai-vpx3	👔 sai	
	៉ Shreesh-blx-centos	sai	
	🚞 Venkata	iii vm	
		i vm	
		III 📄 vm II	1
[datastore1] sai-vpx-2/es	_preboot_userdata.iso		
			Select Cancel

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.

- 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:

1	base64	<userdata-fil< th=""><th>ename> ></th><th><outuput-file></outuput-file></th><th></th></userdata-fil<>	ename> >	<outuput-file></outuput-file>	
Exemp	le				
1	base64	esx_userdata.	xml > esx_	_userdata_b64	
root@ub	untu:~/sai/	14jul2021# base64	esx_userdata.x	ml > esx_userdata_b64	
root@ub	untu:~/sai/	14jul2021# 14jul2021#_cat_esy	userdata b64		
PE5TLVB	SRS1CT09ULU	NPTkZJRz4KICAgIDxO	Uy1DT05GSUc+Cg	lhZGQgcm91dGUgMC4wLjAuMCA	W
LjAuMC4	wIDEwLjEwMi	4zOC4xCiAgICA8L05T	LUNPTkZJRz4KCi	AgICA8T1MtQk9PVFNUUkFQPgo	g
ICAGICA	gICAgICA8U0	tJUC1ERUZBVUxULUJP	T1RTVFJBUD5ZRV	M8L1NLSVAtREVGQVVMVC1CT09	U
VFJBUC1	TRVFVRU5DRT	4KCiAqICAqICAqPE1H	TVOtSU5URVJGOU	NFLUNPTkZJRz4KICAgICAgICA	a
ICAGICA	gIDxJTlRFUk	ZBQ0UtTlVNPiBldGgw	IDwvSU5URVJGQU	NFLU5VTT4KICAgICAgICAgICA	đ
ICAgIDx	JUD4gICAgMT	AuMTAyLjM4LjIxOSA8	L01QPgogICAgIC	AgICAgICAgICAgPFNVQk5FVC1	N
QVNLPiA	yNTUuMjU1Lj	I1NS4wIDwvU1VCTkVU	LU1BU0s+CiAgIC	AgICAgPC9NR01ULU1OVEVSRkF	D
RS1DT05	GSUc+CiAgIC	A8L05TLUJPT1RTVFJB	UD4KPC90Uy1QUk	UtQk9PVC1DT05GSUc+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:

1	<productsection></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
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></productsection>	
2		
3	<into>Information about the installed software</into>	
4	<pre><product>NSVPX-VSK Template</product> </pre>	
С С	<pre></pre> <pre><</pre>	
7	(Category) Preboot Userdata (/Category)	
8	<pre><property ovf:<="" ovf:key="guestinfo.userdata" ovf:type="string" td=""><td></td></property></pre>	
0	ovf voluo-"PESTLVRSPS1CT001111NPTk73Pz4KTCAgTDv011v1DT05CSUc+	
9	Cglh7GOgcm91dGUgMC4wLiAuMCAw	
10	LjAuMC4wIDEwLjEwMi4z0C4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQ	<9PVFNUUk
11	ICAgICAgICAgICA8U0tJUC1ERUZBVU×ULUJPT1RTVFJBUD5ZRVM8L1NLSVAtR	EVGQVVMVC
12	U1RSQVA+ CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTk	VXLUJPT1F
13	VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJR	z4KICAgIC
14	ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KI	CAgICAgIC
15	ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgI	CAgPFNVQk
16	QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+ CiAgTCAgTCAgPC9NR01ULU]OVEVSRkED	
17	RS1DT05GSUc+ CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uv10UkUt0k9PVC1DT05GSUc+	
	Cg==">	
18		
19	<label>Userdata</label>	
20	<pre><description> Userdata for ESX VPX </description></pre>	
21		
22	(ProductSection)	
23		

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

<pre>Please change the default NSROOT password. Enter new password: Please re-enter your password: Done > sh ns ver</pre>
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
<pre>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 </pre>
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
<pre>> 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 </pre>
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
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
<pre>> sh ns ip</pre>
In the type Mode Arp Icmp Vserver S tate
Therefore There
 1) 10.102.38.219 0 NetScaler IP Active Enabled Enabled NA E nabled
1) 10.102.38.219 0 NetScaler IP Active Enabled Enabled NA E nabled
nabled
Done
> sh route
Network Netmask Gateway/OwnedIP VLAN State Traffic Domain Type
C C C C C C C C C C C C C C C C C C C
2) 127.0.0.0 255.0.0.0 127.0.0.1 0 0P 0 PERMA
5) 10.102.38.0 255.255.0 10.102.38.219 0 0P 0 DIREC

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.

- 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:

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

Exemple

1	base64	esx_user	data.xml	>	esx_us	erdata_	b64	
root@ubunt	u:~/sai/	14jul2021# b	ase64 esx 1	userd	ata.xml	> esx use:	rdata b64	
root@ubunt	u:~/sai/	14jul2021#						
root@ubunt	u:~/sai/	14jul2021# c	at esx_use:	rdata	_b64			
PE5TLVBSRS	1CT09ULU	NPTkZJRz4KIC	AgIDxOUy1D	ro5GS	Uc+CglhZ(GQgcm91dG	UgMC4wLjA	uMCAw
LjAuMC4wII)EwLjEwMi	4zOC4xCiAgIC	A8L05TLUNP	TkZJR	z4KCiAgI(CA8T1MtQk	9PVFNUUkF	QPgog
ICAgICAgIC	AgICA8U0	tJUC1ERUZBVU	xULUJPT1RT	VFJBU	D5ZRVM8L1	INLSVATRE	VGQVVMVC1	CT09U
U1RSQVA+Ci	AgICAgIC	AgICAgIDxORV	ctQk9PVFNU	UkFQL	VNFUVVFT]	kNFPllFUz	wvTkVXLUJ	PT1RT
VFJBUC1TRV	FVRU5DRT	4KCiAgICAgIC	AgPE1HTVQt	SU5UR	VJGQUNFLU	JNPTkZJRz	4KICAgICA	gICAg
ICAgICAgII	xJTlRFUk	ZBQ0UtTlVNPi	BldGgwIDwv	SU5UR	VJGQUNFLU	J5VTT4KIC	AgICAgICA	gICAg
ICAgIDxJU	4gICAgMT	AuMTAyLjM4Lj	IXOSA8L01Q	PgogI	CAgICAgI	CAgICAgIC	AgPFNVQk5	FVC1N
QVNLPiAyNI	'UuMjU1Lj	I1NS4wIDwvU1	VCTkVULU1B	U0s+C	iAgICAgI	CAgPC9NR0	1ULU1OVEV	SRkFD
RS1DT05GSU	Ic+CiAgIC	A8L05TLUJPT1	RTVFJBUD4K	PC9OU	y1QUkUtQl	k9PVC1DT0	5GSUc+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:

1	<productsection></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	
9	<property ovf:<br="" ovf:key="guestinfo.userdata" ovf:type="string">userConfigurable="true" ovf:value=""></property>
10	
11	<label>Userdata</label>
12	<description> Userdata for ESX VPX </description>
13	
14	
15	

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

1	<productsection></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:<="" ovf:key="guestinfo.userdata" ovf:type="string" td=""></property>
	userConfigurable="true"
9	ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+
	CglhZGQgcm91dGUgMC4wLjAuMCAw
10	LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQ

11	ICAgICAgICAgICA8U0tJUC1ERUZBVU×ULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC
12	U1RSQVA+ CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1
13	VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgIC
14	ICAgICAgID×JTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgIC
15	ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQ
16	QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+ CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
17	RS1DT05GSUc+ CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+ Cg==">
18	
19	<label>Userdata</label>
20	<pre><description> Userdata for ESX VPX </description></pre>
21 22	
23	

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 (Enter ne	change the defaul	t NSROOT password	1.						
Please : Done	re-enter your pas	sword:							
> sh ns	ver								
	NetScaler NS13.0	: Build 83.9005.r	nc, Date: Jul 13 2	2021, 02:	56:05	(64-bit)			
Done									
> sh ns	ip								
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserve	er S	3
tate									
1)	10.102.38.219		NetScaler IP	Active	Enabled	Enabled	NA	I	2
nabled Done									
> sh rou	ute								
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main	Туре	e -
1) C	0.0.0.0	0.0.0.0	10.102.38.1		UP		S	TAT	Γ
2) NENT	127.0.0.0	255.0.0.0	127.0.0.1		UP		E	PERM/	A
3) T Done	10.102.38.0	255.255.255.0	10.102.38.219		UP		E	IRE	

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 dialogueDéployer le modèle OVF, dansDéployer 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://te chnet.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-netscalervpx-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 (NetScalerADC).
- 5. Sous NetScaler Release X.X > Appliances virtuelles, cliquez sur NetScalerVPX 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 sélection-nez Copier la machine virtuelle (créez unnouvel 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"?>
1
2
     <Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment
3
         /1`"
4
5
     xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"
6
     oe:id=""
7
8
     xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">
9
10
11
     <PlatformSection>
12
13
     <Kind>HYPER-V</Kind>
14
15
     <Version>2013.1</Version>
16
     <Vendor>CITRIX</Vendor>
17
18
     <Locale>en</Locale>
19
     </PlatformSection>
22
23
     <PropertySection>
24
25
     <property oe:key="com.citrix.netscaler.ovf.version" oe:value="</pre>
         1.0"/>
```

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

- 2. Copiez l'image ISO sur le serveur Hyper-V.
- 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.
- 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 :

1	[root@localhost ~]# ethtool -K eth6
2	
3	Offload parameters for eth6:
4	
5	rx-checksumming: on
6	
7	tx-checksumming: on
8	
9	scatter-gather: on
10	
11	tcp-segmentation-offload: on
12	
13	udp-fragmentation-offload: off
14	
15	generic-segmentation-offload: on
16	
17	generic-receive-offload: off
18	
19	large-receive-offload: off
20	
21	rx-vlan-offload: on
22	
23	tx-vlan-offload: on
24	
25	ntuple-filters: off
26	
27	receive-hashing: on
28	
29	[root@localnost ~]#

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
1
2
                                                     STP enabled interfaces
3
         bridge name
                          bridge id
4
5
         eth6_br
                          8000.00e0ed1861ae
                                                                   eth6
                                                       no
6
7
                                                                   vnet0
8
9
                                                                   vnet2
          [root@localhost ~]#
11
```

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.

```
1 ethtool -K vnet0 gro off
2 ethtool -K vnet2 gro off
3 ethtool -K vnet0 lro off
4 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
1
     [root@localhost ~]# ifconfig eth6
2
3
     eth6
                Link encap:Ethernet HWaddr 78:2b:cb:51:54:a3
                 inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
4
                 UP BROADCAST RUNNING PROMISC MULTICAST MTU:9000 Metric
5
                     :1
6
                 RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
                 TX packets:2895843 errors:0 dropped:0 overruns:0 carrier
7
                     :0
8
                 collisions:0 txqueuelen:1000
                 RX bytes:14330008 (14.3 MB) TX bytes:1019416071 (1.0 GB)
9
10
11
     [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 :

1 lsmod | grep "vhost_net"

Si vhost_net n'est pas encore en cours d'exécution, entrez la commande suivante pour l'exécuter :

1 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.

1	· · · ·
2	xml version="1.0" encoding="UTF-8" standalone="no"?
3	<environment <="" td="" xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"></environment>
4	<pre>xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"</pre>
5	oe:id=""
6	<pre>xmlns="http://schemas.dmtf.org/ovf/environment/1"</pre>
7	<pre>xmlns:cs="http://schemas.citrix.com/openstack"></pre>
8	<platformsection></platformsection>
9	<kind></kind>
10	<version>2016.1</version>
11	<vendor>VPX</vendor>
12	<locale>en</locale>
13	
14	<propertysection></propertysection>
15	<property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"></property>
16	<property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"></property>
17	<pre><property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-</pre></td></tr><tr><td></td><td>orch-env"></property></pre>
18	<property <="" oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22" td=""></property>
	/>
19	<property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="</td></tr><tr><td></td><td>255.255.255.0"></property>
20	<property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="</td></tr><tr><td></td><td>10.1.2.1"></property>
21	
22	<cs:scriptsection></cs:scriptsection>
23	<cs:version>1.0</cs:version>
24	<pre><scriptsettingsection xmlns="http://schemas.citrix.com/openstack</pre></td></tr><tr><td>~ -</td><td>" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></scriptsettingsection></pre>
25	<scripts></scripts>
26	<script></script>

```
37
                       <Type>python</Type>
38
                       <BootScript>after</BootScript>
39
                        <Text>
                              #!/bin/python
40
      print("Hello");
41
42
                        </Text>
43
                 </Script>
44
         <Script>
                       <Type>perl</Type>
45
46
                       <BootScript>before</BootScript>
47
                        <Text>
48
                              !/usr/bin/perl
      my $name = "VPX";
49
      print "Hello, World $name !\n";
50
51
                        </Text>
52
                 </Script>
53
                 <Script>
                      <Type>nscli</Type>
54
                      <BootScript>after</BootScript>
                      <Text>
57
                       add vlan 33
58
      bind vlan 33 -ifnum 1/2
                      </Text>
                 </Script>
61
               </Scripts>
62
           </ScriptSettingSection>
63
      </cs:ScriptSection>
64
     </Environment>
       Dans le fichier OVF qui précède, « PropertySection » est utilisé
       pour la configuration réseau de NetScaler tandis que \langle < 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

```
1 tar xvzf <TAR file>
2 tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
3 NSVPX-KVM.xml
4 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.

```
1 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>
2
3 glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --ispublic=
4 true --container-format=bare --disk-format=qcow2< NSVPX-KVM
    -12.0-26.2_nc.qcow2</pre>
```

Figure 1 : L'illustration suivante fournit un exemple de sortie pour la commande glance imagecreate.

+	
Field	Value
<pre>checksum container_format created_at disk_format file id min_disk min_ram name owner properties protected schema size status updated_at virtual_size visibility</pre>	154ade3fc7dca7d1706b1d03d7d97552 bare 2017-03-13T08:52:31Z qcow2 /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file 322c1e0f-cce8-4b7b-b53e-bd8152c388ed 0 0 VPX-KVM-12.0-26.2 58d17d81df5d4406afbb4fdab3a58d79 hw_disk_bus='ide' False /v2/schemas/image 784338944 active 2017-03-13T08:52:43Z None 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.

ect	~	Inst	tances										
compute	Ŧ	Inst	tances			Filter			Q Filer	+	unch instance	Set Res	oot instances
1 Deniew			Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Uptime	Actions
nstances /olumes	1		dhcp	NS-VPX- 10-5-49-3	10.0.0.5	m1.medium 4GB RAM 2 VCPU 40.0GB Disk		Active	nova	None	Running	1 hour, 50 minutes	Create Snapshot 8
mages			NS1000+- 10-5-4	NS-VPX- 10-5-49-3	10.0.0.4	m1.medium 4G8 RAM 2 VCPU 40.0G8 Disk		Active	nova	None	Running	1 hour, 57 minutes	Create Snapshot
letwork	>		NS1000+10-5	NS-VPX- 10-5-49-3	10.0.0.2	m1.medium 4G8 RAM 2 VCPU 40.0G8 Disk		Active	nova	None	Running	2 hours, 16 minutes	Create Snapshot

- 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

Details *	Access & Security *	Networking *	Post-Creation Adv	vanced Options
Availability Z	one:		Snecify the details for la	inching an instance
nova		•	The chart below shows the	he resources used by this project
Instance Nam	ne: *		in relation to the project's	s quotas.
NSVPX 10 1			Flavor Details	
	_		Name	m1.medium
Flavor: *			VCPUs	2
m1.medium		•	Root Disk	40 GB
Instance Cou	nt: *		Ephemeral Disk	0 GB
1			Total Disk	40 GB
Instance Boo	t Source:		RAM	4,096 MB
Boot from im	age	•	Project Limits	
Image Name:			Number of Instances	6 of 10 Used
NS-VPX-10-1	-130-11 (20.0 GB)	•	Number of VCPUs	12 of 20 Used
			Total RAM	24,576 of 51,200 MB Used

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** .

ev Pair Name *	
NewKey	Description:
ublic Key *	Key Pairs are how you login to your instance after it is launched.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCIZih	Choose a key pair name you will recognise and paste your SSH public key into the space provided.
03te1FrwL38iGXbilByc2+oBV7ZIFRiYQEtk2UfM+ EtJJlcx92m4aIn1RigFvukXECHiXGqfQXVI06pyim	SSH key pairs can be generated with the ssh-keygen command:
KRWigXhI+h+tvPGS4iltJ3uWKwfh1PDGYkmgAik osA955L+W9ngVloVyaK40OuAqYCTwIQNBKVuZ	ssh-keygen -t rsa -f cloud.key
EcvsxOvhdb3LW9YADAVnihVK4NLeBc4HIsFeHI 5UY0IYyGk7aW/2SXIzkwRqZ8cX1Oba0XoDiCYN apRVOT6FB//yknvu+BSVF4v0og3	This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.
	After launching an instance, you login using the private key (the username might be different depending on the image you launched):
	ssh -i cloud.key <username>@<instance_ip></instance_ip></username>

- 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**.

Launch	Instance				×
Details *	Access & Security	Networking *	Post-Creation	Advanced Options	
Disk Partition	0		Specify advan	nced options to use wher	n launching an
Automatic		instance.			
 Configuration 	on Drive 🕑				
				Ca	ancel 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 :

```
openstack server create --flavor FLAVOR_ID --image IMAGE_ID --
1
        key-name KEY_NAME
2
    --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id
        =net-uuid
    INSTANCE_NAME
3
    openstack server create --image VPX-ToT-Image --flavor m1.medium
4
         --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	I MANUAL
OS-EXT-AZ:availability zone	
0S-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor hostname	None
0S-EXT-SRV-ATTR: instance name	instance-000001c2
0S-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
0S-EXT-STS:vm_state	building
0S-SRV-USG: Launched at	None
0S-SRV-USG:terminated at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtg7N8Z6
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)
kev name	None
name	IVPX-ToT
os-extended-volumes:volumes attached	
progress	10
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

January 28, 2025

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 -0 qcow2 original-image.raw image-converted.qcow2

Exemple:

qemu-img convert -0 qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5
_nc.qcow2

Un déploiement standard de NetScaler VPX sur KVM comprend les étapes suivantes :

- Vérification des conditions préalables au provisionnement automatique d'une instance NetScaler VPX
- Provisionnement de l'instance NetScaler VPX à l'aide d'une image RAW
- Provisionnement de l'instance NetScaler VPX à l'aide d'une image QCOW2
- Ajout d'interfaces supplémentaires à une instance VPX à l'aide du gestionnaire de machines virtuelles

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"`</pre>
```

4 5	<pre>xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`</pre>
6	
7	oe:id=""
9	<pre>xmlns="`http://schemas.dmtf.org/ovf/environment/1"`</pre>
11	<pre>xmlns:cs="`http://schemas.citrix.com/openstack">`</pre>
12 13 14	<platformsection></platformsection>
15 16	<kind></kind>
17 18	<version>2016.1</version>
19 20	<vendor>VPX</vendor>
21 22	<locale>en</locale>
23 24	
25 26	<propertysection></propertysection>
27 28	<property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"></property>
29 30	<property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"></property>
31 32	<property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"></property>
33	<property <br="" oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22">/></property>
34	
35	<property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
255.255.255.0"></property>
36	
37	<property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
10.1.2.1"></property>
38	
39 40	
41	

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.

V? localhost.localdomain:6 (admin)	
Activities WWirtual Machine M	Thu 02:24
r	Virtual Machine Manager
File Edit View Help	
🔛 🗏 🔲 Open 🗇 💷 🗖 🗸	
Name	
Locathost (GEMU) New Connec Discon	
Delete Dgtails	
<(•

- 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**.

localhost.localdomain:6 (admin)		
Activities WWirtual Machi	ne Manager	Thu 02:26
		Virtual Machine Manager
le Edit View Help		
🞴 📃 Open 🗇 💷 🖪	×	
ame		
localhost (GEMU)	New VM	
	Create a new virtual machine	
	Step 1 of 4	
	Enter your virtual machine details	
	Name: NetScaler-VPX	
	Connection: localbost (QEMLI/KVM)	
	Choose how you would like to install the operating system	
	 Local install media (ISO image or CDROM) 	
	 Network Install (HTTP, FTP, or NFS) 	
	O Network Boot (PXE)	
	Import existing disk image	
	Cancel Back Forward	
	-	

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**.

localhost.localdomain:6 (admin)		
		Virtual Machine Manager
le Edit View Help		
🎴 🗍 🔲 Open 🔉 💷 👩	~	
ne		
ocalhost (GEMU)	New VM	
	New VM	
	Create a new virtual machine Step 2 of 4	
	Provide the existing storage path:	
	/Libvirt/images/NSVPX-KVM-10.1-118.7_nc.raw Browse	
	Choose an operating system type and version	
	OS type: UNIX	
	Version: FreeBSD 6.x	
	Cancel Back Forward	

- 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



 Sélectionnez l'icône Personnaliser la configuration avant l'installation case à cocher. 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.

ut (OBER		
ost (GEMU)	New VM	
	Create a new virtual machine Step 4 of 4	
	Ready to begin installation of NetScaler-VPX	
	OS: FreeBSD 6.x	
	Install: Import existing OS image	
	CPUs: 2	
	Storage: 20.0 GB /var/lb/lbvirt/mages/NSVPX-KVM-10.1-118.7_n	
	☑ Customize configuration before install	
	Virtual network 'default' : NAT	
	✓ Set a fixed MAC address	
	52:54:00:0d:22:cb	
	Virt Type: kvm	
	Architecture: x86_64 🗘	
	Cancel Back Finish L.	

- 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**.
- 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 :

 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'icône **QCOW2** image dans **Étape 5**.

2. Sélectionnez Disque 1 et cliquez sur Options avancées .

3. Sélectionnez **qcow2** dans la liste déroulante Format de stockage.

AN .	test Virtual Machine	· · · ·
🥜 Begin Installation 🛛 💥 C	ancel	
Overview Processor Memory Boot Options Disk 1 Input Display Spice Sound: default Console Channel Video Default	Virtual Disk Target device: Disk] Source path: /home/dummy_dut/NSVPX-KVM-11.1-12.5_nc.qcow Storage size: 788.25 MB Readonly: Shareable: Shareable: Shareable: Shareable: Storage format: Grow2 Performance options Cache mode: default Cache mode: default Cache mode: default Cache mode: Disk back Cache mode: Di	
	KBytes/Sec IOPS/Sec	
	Read: 0 1 0	
	Write: 0 🗘 0	
	Total: 0 0	
	Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS	

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.
- Cliquez surGéreret 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.

2 Virtual Machine View Send	l Key				
0 🕨 📔 🕘 🔹 🕤					
Aug 11 10:14:55 (loop)	a lant > no mostar	+[2570]· Dootom	t: mataaa	lan (naatan	t ob
exited normally. Exit	code (0)	ILZDIOI NESLAP	t. Zhetsea	let/ll22rgt	t.su
Aug 11 10:14:55 <local< td=""><td>9.alert> ns restar</td><td>t[2578]: Succ</td><td>essfully d</td><td>eregistere</td><td>d wit</td></local<>	9.alert> ns restar	t[2578]: Succ	essfully d	eregistere	d wit
n ritbuss					
Transford and the set					
login: nsroot Password:					
Aug 11 10:15:04 <auth.< td=""><td>notice> ns login:</td><td>ROOT LOGIN (nsr</td><td>oot) ON tt</td><td>yv0</td><td></td></auth.<>	notice> ns login:	ROOT LOGIN (nsr	oot) ON tt	yv0	
Copyright (c) 1992-2013	3 The FreeBSD Proj	ect.	4002 400	1004	
Copyright (c) 1992-2011 Copyright (c) 1979, 198 The Regents of	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of	ect. 188, 1989, 1991, California. Al	1992, 1993 l rights ri	3, 1994 eserved.	
Copyright (c) 1992-2011 Copyright (c) 1979, 194 The Regents of	3 The FreeBSD Proj 80, 1983, 1986, 19 the University of	ect. 88, 1989, 1991, California. Al	1992, 1993 l rights ri	3, 1994 eserved.	
Copyright (c) 1992-201 Copyright (c) 1979, 194 The Regents of Done > sh in	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of	ject. 88, 1989, 1991, California. Al	1992, 1993 l rights ro	3, 1994 eserved.	
Copyright (c) 1992-201 Copyright (c) 1979, 194 The Regents of Done > sh ip Ipaddress	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain	iect. 88, 1989, 1991, California. Al Type	1992, 1993 l rights ro Mode	3, 1994 eserved. Arp	Icmp
Copyright (c) 1992-201 Copyright (c) 1979, 19 The Regents of Done > sh ip Userver State	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain	iect. 88, 1989, 1991, California. Al Type	1992, 1993 l rights ro Mode 	3, 1994 eserved. Arp 	Icmp
Copyright (c) 1992-201 Copyright (c) 1979, 19 The Regents of Done > sh ip Ipaddress Userver State	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 	ect. 88, 1989, 1991, California. Al Type 	1992, 199 l rights ro Mode 	3, 1994 eserved. Arp 	Icmp
Copyright (c) 1992-201 Copyright (c) 1979, 191 The Regents of Done > sh ip Ipaddress Userver State 	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 	ect. 88, 1989, 1991, California. Al Type NetScaler IP	1992, 199 l rights ro Mode Active	3, 1994 eserved. Arp Enabled	Icmp Enab
Copyright (c) 1992-201 Copyright (c) 1979, 191 The Regents of Done > sh ip Ipaddress Vserver State 1) 10.1.2.22 led NA Enabled Done	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 	ject. 88, 1989, 1991, California. Al Type NetScaler IP	1992, 199 l rights ro Mode Active	3, 1994 eserved. Arp Enabled	Icmp Enab
Copyright (c) 1992-201 Copyright (c) 1979, 194 The Regents of Done > sh ip Ipaddress Userver State 	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 0 al0.alert> ns rest	ect. 88, 1989, 1991, California. Al Type NetScaler IP art[2578]: Ns	1992, 1993 l rights ro Mode Active shutdown lo	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab ed !
Copyright (c) 1992-201 Copyright (c) 1979, 194 The Regents of Done > sh ip Ipaddress Userver State 	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 0 al0.alert> ns rest	iect. 88, 1989, 1991, California. Al Type NetScaler IP .art[2578]: Ns	1992, 1993 l rights ro Mode Active shutdown lo	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab
Copyright (c) 1992-2011 Copyright (c) 1979, 194 The Regents of Done > sh ip Ipaddress Userver State 	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 0 al0.alert> ns rest	iect. 88, 1989, 1991, California. Al Type NetScaler IP Aart[2578]: Ns	1992, 199 l rights ro Mode Active shutdown lo	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab
Copyright (c) 1992-2011 Copyright (c) 1979, 196 The Regents of Done > sh ip Ipaddress Userver State 	3 The FreeBSD Proj 30, 1983, 1986, 19 the University of Traffic Domain 0 al0.alert> ns rest	ect. 88, 1989, 1991, California. Al Type NetScaler IP art[2578]: Ns	1992, 199 l rights ro Mode Active shutdown lo	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab ed !

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 du 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.

le Virtual Machine Vi	w Send Key
= 💽 Þ 🛛 🛛	× \$
 Overview Performance Processor Memory Boot Options IDE Disk 1 NIC :0d:22:cb NIC :a9:77:fc Mouse Display VNC Sound: ich6 Serial 1 Video Controller USB Controller IDE 	Add New Virtual Hardware Storage Network Input Sound Sound
A dd 11	▷ Security

- 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.

		Add New Vi	rtual Hardware
	Storage	Network	
2	Network	k	
0	Input	Please indicate how	w you'd like to connect your
	Graphics	new virtual netwo	rk device to the host network.
	Sound	Host device:	Host device macytan2 : macytan
-	Serial		
~	Parallel	MAC address:	☑ 52:54:00:fb:bb:e5
~	Channel	D : 11	
33	USB Host Device	Device model:	Virtio
33	PCI Host Device		
<u>_</u>	Video		
	Watchdog		
	Filesystem		
2	Smartcard		
	second and solar and solar and solar s		
			Cancel Finish

iii. Cliquez sur **Terminer**. Vous pouvez afficher la carte réseau nouvellement ajoutée dans le volet de navigation.

		NetS	caler-VPX Virtual	Machine			-
ile	Virtual Machine View	Send Key					
	e a	× [
2	Overview	Virtual Network	Interface				
	Performance Processor	Source device:	Host device p1p1	: macvtap	0		
	Memory	Device model:	virtio	0			
33	Boot Options	MAC address:	52:54:00:a9:77:fc				
-	IDE Disk 1	Source mode:	Default				
se R	NIC :a9:77:fc	Virtual port	VEPA				
3	Mouse		Bridge				
	Display VNC		Private				
ŋ	Sound: ich6		Passthrough				
2	Serial 1						
2	Video						
	Controller USB						
	Controller IDE						
	Add Hardware			F	Remove	Cancel	Apply

- 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

January 15, 2025

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

Pour plus d'informations, consultez Cartes réseau prises en charge pour NetScaler VPX.

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.	Ajoutez l'entrée suivante dans le fichier /etc/mod- probe.d/blacklist.conf : blacklist i40evf.
	4.3.15 (recommandé).	2.0.26 (recommandé).
Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
--	---	---
1. Activez les fonctions virtuelles SR-IOV (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> > ; /sys/class/net/< device_name>/ device/sriov_numvfs. Voir l'exemple de la figure 1.</number_of_vfs> 	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.</device_name& </number_of_vfs </number_of_vfs>
 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.
--

Terminal - root@ubuntu: /etc	+ - • ×
File Edit View Terminal Tabs Help	
root@ubuntu:/etc# echo 1 > /sys/class/net/ens3f0/device/sriov_numvfs	
root@ubuntu:/etc# echo 1 > /sys/class/net/ens3f1/device/sriov_numvfs	
root@ubuntu:/etc# lspci grep 82599	
02:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	
02:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	
02:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)	
02:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)	
root@ubuntu:/etc#	

Figure 2 : activer les VF SR-IOV sur l'hôte KVM pour les cartes réseau Intel X710 10G et XL710 40G.

ootedountu.~#
ooteubuntu:~# Lspci grep /10
3:00.0 Ethernet controller: Intel Corporation Ethernet Controller X 710 for 10GbE SFP+ (rev 01)
3:00.1 Ethernet controller: Intel Corporation Ethernet Controller X 710 for 10GbE SFP+ (rev 01)
3:00.2 Ethernet controller: Intel Corporation Ethernet Controller X 710 for 10GbE SFP+ (rev 01)
3:00.3 Ethernet controller: Intel Corporation Ethernet Controller X 710 for 10GbE SFP+ (rev 01)
3:06.0 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:06.1 Ethernet controller: Intel Corporation XL 710 /X 710 Virtual Function (rev 01)
3:0a.0 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0a.1 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0a.2 Ethernet controller: Intel Corporation XL 710 /X 710 Virtual Function (rev 01)
3:0a.3 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0e.0 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0e.1 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0e.2 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
3:0e.3 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 01)
1:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 01)
2:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 02)
2:00.1 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 02)
2:02.0 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 02)
2:02.1 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 02)
2:0a.0 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 02)
2:0a.1 Ethernet controller: Intel Corporation XL 710/X710 Virtual Function (rev 02)
oot@ubuntu:~#

Figure 3 : activer les VF SR-IOV sur l'hôte KVM pour la carte réseau Intel X722 10G.

root@ubu	intu:~# 1s	spci grep	"37cd'					
84:02.0	Ethernet	controller:	Intel	Corporation	Device	37cd	(rev	04)
84:0a.0	Ethernet	controller:	Intel	Corporation	Device	37cd	(rev	04)

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.

UEN		Demo_VPX on QEMU/KVM	↑ _ □ ×
	Virtual Machine View Send I Virtual Machine View Send I Video Starset Video Senial Video Video Senia Video Senial Video Video Senia Senial Video Video Senia Senial Char @ USB Redirection Vide With TPM Senia Senial	Xey Add New Virtual Hardware Charage Create a disk image for the virtual machine 20.0 - + GiB 748.9 GiB available in the default location Select or create custom storage Manage Device type: Disk device Device type: Disk device Bus type: IDE Advanced options	
	Cont Cont Cont Cont Cont Controller VirtlO Serial USB Redirector 1 USB Redirector 2 CSB Redirector 2	⊘ Cancel √ Finish	

- 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

0	Add New Virtual Hardware
Storage	PCI Device
Controller	
Network	Host Device:
Input	UUUU:UU:IF:6 Intig Corporation C610/X99 series chipset Thermal Subsystem
Graphics	0000:01:00:0 Intel Corporation I350 Gigabit Network Connection (Interface e
Sound	0000:01:00:1 Intel Corporation I350 Gigabit Network Connection (Interface e
Serial	0000:02:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Conne
Parallel	0000:02:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Conne
Console	0000:02:10:0 Intel Corporation 82599 Ethernet Controller Virtual Function
Channel	0000:02:10:1 Intel Corporation 82599 Ethernet Controller Virtual Function
🔏 USB Host Device	0000:03:00:0 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel
🔏 PCI Host Device	0000:03:00:1 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel
Video	0000:03:00:2 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel
📑 Watchdog	0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel
Filesystem	0000:06:00:0 ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge
Smartcard	0000:07:00:0 ASPEED Technology, Inc. ASPEED Graphics Family
USB Redirection	0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
ТРМ	0000:7F:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
🔏 RNG	0000:7F:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
🔏 Panic Notifier	0000:7F:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 &
	(≩Cancel √ Finish
USB Redirector 1	

Figure 5 : VF pour carte réseau Intel XL710 40G

202		Add New Virtual Hardware	$\uparrow \times$
	Storage Controller Network	PCI Device Host Device:	
	Input Graphics Sound Serial Parallel Console	0000:02:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Col 0000:02:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Col 0000:03:00:0 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:1 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:2 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+	nne (Into (Into (Into (Into
	Video Video Watchdog Filesystem Smartcard USB Redirection TPM RNG Papic Notifier	0000:03:06:0 Intel Corporation XL710/X710 Virtual Function 0000:03:06:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:0 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:2 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:3 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:0 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:2 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:3 Intel Corporation XL710/X710 Virtual Function	
[love)		Cancel	ish

Figure 6 :	VF pour	^r carte réseau	Intel X722 10G
------------	---------	---------------------------	----------------

NB		Add New Virtual Hardware				
	Storage Controller	PCI Device				
N	Network	Host Device:				
0	Input	0000:81:02:6 Intel Corporation XL/10/X/10 Virtual Function (Interface enp12)				
	Graphics	0000:81:02:7 Intel Corporation XL710/X710 Virtual Function (Interface enp12				
	Sound	0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12				
7	Serial	0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12				
7	Parallel	0000:82:00:0 Intel Corporation				
7	Console	0000:83:03:0 Intel Corporation				
7	Channel	0000:84:00:0 Intel Corporation (Interface enp132s0f0)				
8	USB Host Device	0000:84:00:1 Intel Corporation (Interface enp132s0f1)				
	PCI Host Device	0000:84:02:0 Intel Corporation (Interface enp132s2)				
	Video	0000:84:0A:0 Intel Corporation (Interface enp132s10)				
	Watchdog	0000:FF:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0				
	Filesystem	0000:FF:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0				
	Smartcard	0000:FF:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0				
8	USB Redirection	0000:FF:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 &				
	TPM	0000:FF:0B:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 &				
8	RNG	0000:FF:0B:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 &				
80	Panic Notifier	0000:FF:0C:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 Unicast Regist				

- 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.

M				Demo_VPX on QEMU/KVM		↑ _ □ X
File	Virtua	I Machine Vie	w Send Key			
	1	• • • •				[™] ≊
	> sho	w interface	summary			
		Interface	MTU 	MAC	Suffix	
	1	0/1	1500	52:54:00:7f:81:87	NetScaler Virtual Interfac	8
	2	10/1	1500	8e:e7:e7:06:50:3f	Intel 82599 10G VF Interfa	се
	3	10/2	1500	8e:1a:71:cc:a8:3e	Intel 82599 10G VF Interfa	ce
	4	L0/1	1500	52:54:00:7f:81:87	Netscaler Loopback interfac	ce
	Done >					

Figure 7. Résumé de la sortie pour les cartes réseau Intel X710 et XL710.

	Interface	MTU	МАС	Suffix
1	0/1	1500	52:54:00:e7:cb:bd	NetScaler Virtual Interface
2	40/1	1500	ea:a9:3d:67:e7:a6	Intel X710/XLG VF Interface
3	40/2	1500	aa:7c:50:ad:c7:fa	Intel X710/XLG VF Interface
4	40/3	1500	3a:45:a3:a9:ee:86	Intel X710/XLG VF Interface
5	LA/6	1500	52:74:94:b6:f9:cb	802.3ad Link Aggregate
6	L0/1	1500	52:54:00:e7:cb:bd	Netscaler Loopback interface
Done				

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 \\<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 :

Templeal mathiakanaka late	
Ierminai - rootigubuntu: /etc	
File Edit View Terminal Tabs Help	
root@ubuntu:/etc# ip link show ens3f0	
6: ens3f0: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7e brd ff:ff:ff:ff:ff	
vf 0 MAC 8e:e7:e7:06:50:3f, spoof checking on, link-state auto	
root@ubuntu:/etc#	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip_link show ens3f1	
7: ens3f1: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default glen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff	
vf θ MAC 8e:1a:71:cc:a8:3e, spoof checking on, link-state auto	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip link set ens3f0 vf θ spoofchk off	
root@ubuntu:/etc# ip link show ens3f0	
6: ens3f0: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7e brd ff:ff:ff:ff:ff	
vf 0 MAC 8e:e7:e7:06:50:3f, spoof checking off, link-state auto	
root@ubuntu:/etc# ip link set ens3f1 vf θ spoofchk off	
root@ubuntu:/etc# ip link show ens3f1	
7: ens3f1: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff	
vf θ MAC 8e:la:71:cc:a8:3e, spoof checking off, link-state auto	
root@ubuntu:/etc#	

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

 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.

root@venkat-Super-Server:~# adf_ctl status				
Checking status of all devices.				
There is 47 QAT acceleration device(s) in the system:				
gat_dev8 - type: c6xx, inst_id: 0, node_id	: 0, bsf: 0000:1a:00.0, #accel: 5 #engines: 10 state: up			
qat_dev1 - type: c6xx, inst_id: 1, node_id	: 0, bsf: 0000:1b:00.0, #accel: 5 #engines: 10 state: up			
qat_dev2 - type: c6xx, inst_id: 2, node_id	: 0, bsf: 6000:1c:00.0, #accel: 5 #engines: 10 state: up			
gat_dev3 - type: c6xxvf, inst_id: 0, node_'	id: 0, bsf: 0000:1a:01.0, #accel: 1 #engines: 1 state: up			
qat_dev4 - type: c6xxvf, inst_id: 1, node_'	id: 0, bsf: 0000:1a:01.7, #accel: 1 #engines: 1 state: up			
qat_dev5 - type: c6xxvf, inst_id: 2, node_	id: 0, bsf: 0000:1a:01.1, #accel: 1 #engines: 1 state: up			
qat_dev6 - type: c6xxvf, inst_id: 3, node_	id: 0, bsf: 0000:1a:02.0, #accel: 1 #engines: 1 state: up			
qat_dev7 - type: c6xxvf, inst_id: 4, node_	id: 0, bsf: 0000:1a:01.2, #accel: 1 #engines: 1 state: up			
<pre>qat_dev8 - type: c6xxvf, inst_id: 5, node_</pre>	id: 0, bsf: 0000:la:01.3, #accel: 1 #engines: 1 state: up			
<pre>qat_dev9 - type: c6xxvf, inst_id: 6, node_</pre>	id: 0, bsf: 6000:1a:02.1, #accel: 1 #engines: 1 state: up			
<pre>qat_dev10 - type: c6xxvf, inst_id: 7, node</pre>	_id: 0, bsf: 0000:1a:01.4, #accel: 1 #engines: 1 state: up			
qat_dev11 - type: c6xxvf, inst_id: 8, node	id: 0, bsf: 0000:la:01.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev12 - type: c6xxvf, inst_id: 9, node</pre>	id: 0, bsf: 0000:1a:02.2, #accel: 1 #engines: 1 state: up			
<pre>qat_dev13 - type: c6xxvf, inst_id: 10, node</pre>	e_id: 0, bsf: 0000:1a:01.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev14 - type: c6xxvf, inst_id: 11, node</pre>	e_id: 0, bsf: 0000:1a:02.3, #accel: 1 #engines: 1 state: up			
qat_dev15 - type: c6xxvf, inst_id: 12, node	e_id: 0, bsf: 0000:1a:02.4, #accel: 1 #engines: 1 state: up			
qat_dev16 - type: c6xxvf, inst_id: 13, node	e_id: 0, bsf: 0000:1a:02.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev17 - type: c6xxvf, inst_id: 14, node</pre>	e_id: 0, bsf: 0000:1a:02.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev18 - type: c6xxvf, inst_id: 15, node</pre>	e_id: 0, bsf: 0000:la:02.7, #accel: 1 #engines: 1 state: up			
<pre>qat_dev19 - type: c6xxvf, inst_id: 16, node</pre>	e_id: 0, bsf: 0000:1b:01.0, #accel: 1 #engines: 1 state: up			
<pre>qat_dev20 - type: c6xxvf, inst_id: 17, node</pre>	e_id: 0, bsf: 0000:1b:01.1, #accel: 1 #engines: 1 state: up			
<pre>qat_dev21 - type: c6xxvf, inst_id: 18, node</pre>	e_id: 0, bsf: 0000:1b:01.2, #accel: 1 #engines: 1 state: up			
<pre>qat_dev22 - type: c6xxvf, inst_id: 19, nod</pre>	e_id: 0, bsf: 0000:1b:01.3, #accel: 1 #engines: 1 state: up			
<pre>qat_dev23 - type: c6xxvf, inst_id: 20, nod</pre>	e_id: 0, bsf: 0000:1b:01.4, #accel: 1 #engines: 1 state: up			
<pre>qat_dev24 - type: c6xxvf, inst_id: 21, nod</pre>	e_id: 0, bsf: 0000:1b:01.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev25 - type: c6xxvf, inst_id: 22, nod</pre>	e_id: 0, bsf: 0000:1b:01.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev26 - type: c6xxvf, inst_id: 23, nod</pre>	e_id: 0, bsf: 0000:1b:01.7, #accel: 1 #engines: 1 state: up			
<pre>qat_dev27 - type: c6xxvf, inst_id: 24, nod</pre>	e_id: 0, bsf: 0000:1b:02.0, #accel: 1 #engines: 1 state: up			
<pre>qat_dev28 - type: c6xxvf, inst_id: 25, node</pre>	e_id: 0, bsf: 0000:lb:02.1, #accel: 1 #engines: 1 state: up			
<pre>qat_dev29 - type: c6xxvf, inst_id: 26, nod</pre>	e_id: 0, bsf: 0000:1b:02.2, #accel: 1 #engines: 1 state: up			
<pre>qat_dev30 - type: c6xxvf, inst_id: 27, nod</pre>	e_id: 0, bsf: 0000:1b:02.3, #accel: 1 #engines: 1 state: up			
<pre>qat_dev31 - type: c6xxvf, inst_id: 28, nod</pre>	e_id: 0, bsf: 0000:1b:02.4, #accel: 1 #engines: 1 state: up			
<pre>qat_dev32 - type: c6xxvf, inst_id: 29, node</pre>	e_id: 0, bsf: 0000:1b:02.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev33 - type: c6xxvf, inst_id: 30, nod</pre>	e_id: 0, bsf: 0000:1b:02.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev34 - type: c6xxvf, inst_id: 31, nod</pre>	e_id: 0, bsf: 0000:1b:02.7, #accel: 1 #engines: 1 state: up			
<pre>qat_dev39 - type: c6xxvf, inst_id: 32, nod</pre>	e_1d: 0, bsf: 0000:1c:01.4, #accel: 1 #engines: 1 state: up			
<pre>qat_dev40 - type: c6xxvf, inst_id: 33, node</pre>	e_id: 0, bsf: 0000:lc:01.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev41 - type: c6xxvf, inst_id: 34, nod</pre>	e_id: 0, bsf: 0000:1c:01.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev42 - type: c6xxvf, inst_id: 35, nod</pre>	e_id: 0, bsf: 0988:1c:01.7, #accel: 1 #engines: 1 state: up			
<pre>qat_dev43 - type: c6xxvf, inst_id: 36, nod</pre>	e_id: 0, bsf: 0000:1c:02.0, #accel: 1 #engines: 1 state: up			
<pre>qat_dev44 - type: c6xxvf, inst_id: 37, nod</pre>	e_id: 0, bsf: 0000:1c:02.1, #accel: 1 #engines: 1 state: up			
<pre>qat_dev45 - type: c6xxvf, inst_id: 38, nod</pre>	e_id: 0, bsf: 0000:1c:02.2, #accel: 1 #engines: 1 state: up			
<pre>qat_dev46 - type: c6xxvf, inst_id: 39, nod</pre>	e_1d: 0, bsf: 0000:1c:02.3, #accel: 1 #engines: 1 state: up			
<pre>qat_dev47 - type: c6xxvf, inst_id: 40, nod</pre>	e_1d: 0, bsf: 0000:1c:02.4, #accel: 1 #engines: 1 state: up			
<pre>qat_dev48 - type: c6xxvf, inst_id: 41, nod</pre>	e_id: 0, bsf: 0000:1c:02.5, #accel: 1 #engines: 1 state: up			
<pre>qat_dev49 - type: c6xxvf, inst_id: 42, nod</pre>	e_id: 0, bsf: 0000:1c:02.6, #accel: 1 #engines: 1 state: up			
<pre>qat_dev50 - type: c6xxvf, inst_id: 43, node</pre>	e_1d: 0, bsf: 0000:1c:02.7, #accel: 1 #engines: 1 state: up			
root@venkat-Super-Server:~#				

- 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).

-	Press Control 1+Alt 1 to rel	ease pointer vox-kym-14 1 op O	
		ease poincer. vpx-kviii-14.1 on Q	
File	Virtual Machine View Send Key		
	1 - 0 -		
	SSL Summary		
	# SSL cards present	4	
	# SSL cards UP	4	
	SSL engine status	1	
	SSL sessions (Rate)	Θ	
	Crupto Utilization(%)		
	Asummetric Crupto Utilization	0.00	
	Symmetric Crypto Utilization	0.00	
	System		
	Transactions	Rate (/s)	Total
	SSL transactions	Θ	Θ
	SSLv3 transactions	Θ	Θ

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.

Virtual Machine Manager	(+ _ O ×
File Edit View Help	
🔛 💻 Open ⊳ 🔢 🥝 🔹	
Name 🔻	CPU usage
▼ QEMU/KVM	
Demo_VPX Shutoff	

3. Dans la fenêtre Virtual_machine sur KVM, cliquez sur l'icône i.

BEM		,	Demo_VPX on QEMU/KVM	↑ _ □ ×
File	Virtual Machine View	Send Key		
	🕐 🕨 🖉 🔹	6		<mark>م</mark> ۲
	Overview	Basic Details	i	
-An	Performance	Name:	Demo_VPX	
	CPUs	UUID:	2f82dfa1-ae7d-46bf-b63f-833387798cf0	
	Memory	Status:	Shutoff (Destroyed)	
-	Boot Options	Title:		
	IDE Disk 1	Description:		
	NIC :7f:81:87			
	Mouse			
	Keyboard			
	Display VNC	Hypervisor D	etails	
	Sound: ich6	Hypervisor:	KVM	
	Serial 1	Architecture:	: x86_64	
	Channel spice	Emulator:	/usr/bin/kvm-spice	
	Video QXL	Chinset:	1440EX	
	Controller USB	empset.		
	Controller PCI			
	Controller IDE			
	Controller VirtlO Serial			
1	USB Redirector 1			
1	USB Redirector 2			
	Add Hardware		©Cance!	Apply

- 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**.

File Virtu	ual Mach	hine View Send K	ey Add llew Virtual Hardware	
💻 🥡			Add New Virtual Hardware	
Dvei	100			×
	in 🦷	Storage Controller	PCI Device	
Perfo	s U	Network Input Graphics	0000:00:1C:4 Intel Corporation C610/X99 series chipset PCI Express Root PC 0000:00:1D:0 Intel Corporation C610/X99 series chipset USB Enhanced Host) t
Mem Boot	t	Sound Serial	0000:00:1F:0 Intel Corporation C610/X99 series chipset UPC Controller 0000:00:1F:2 Intel Corporation C610/X99 series chipset 6-Port SATA Controll	e
Virtle		Parallel Console Channel	0000:00:1F:3 Intel Corporation C610/X99 series chipset SMBus Controller 0000:00:1F:6 Intel Corporation C610/X99 series chipset Thermal Subsystem 0000:01:00:0 Intel Corporation I350 Gigabit Network Connection (Interface	e
E Disp	bi 🐅	USB Host Device PCI Host Device	0000:01:00:1 Intel Corporation I350 Gigabit Network Connection (Interface 0000:03:00:0 Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+	e
Seria	a 🖷	Watchdog Filesystem	0000:05:00:0 Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ 0000:09:00:0 ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge 0000:0A:00:0 ASPEED Technology, Inc. ASPEED Graphics Family	C
Cont	tr 👰	Smartcard USB Redirection	0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0 0000:7F:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0	
Cont	tr 3	RNG Panic Notifier	0000:7F:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0 0000:7F:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 0000:7F:0B:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0	
			Cancel Finish	

- 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 :



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

		Pres	s Control_L+A	lt_L to release pointer. Net	Scaler-VPX on QEMU/KVM	×
File	Virtual	Machine View	/ Send Key			
		⊳ 00	•			•
	> sho	w interface	summary			_
		Interface	MTU	MAC	Suffix	
	1	0/1	1500	52:54:00:3f:57:7c	NetScaler Virtual Interface	
	2	10/1	1500	0c:c4:7a:8e:b8:2d	Intel XL710, SR, 10 Gbit	
	3	10/2	1500	0c:c4:7a:8e:b8:2e	Intel XL710, SR, 10 Gbit	
	4	40/1	1500	3c:fd:fe:9e:d8:d9	Intel XL710 40Gbit Interface	
	5	L0/1	1500	52:54:00:3f:57:7c	Netscaler Loopback interface	
	Done >					

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

```
1 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

```
1 <name>NetScaler-VPX</name>
2 <mac address='52:54:00:29:74:b3'/>
3 <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

```
1 <name>NetScaler-VPX</name>
2 <mac address='52:54:00:29:74:b3'/>
3 <driver name ='qemu' type='qcow2'/>
4 <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

1	<interface type="direct"></interface>
2	<mac address="52:54:00:29:74:b3"></mac>
3	<source dev="eth0" mode="bridge"/>
4	<target dev="macvtap0"></target>
5	<model type="virtio"></model>
6	<alias name="net0"></alias>
7	<address <="" bus="0x00" domain="0x0000" slot="0x03" th="" type="pci"></address>
	<pre>function='0x0'/></pre>
8	

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

```
1 virsh start NetScaler-VPX
```

7. Connectez la machine virtuelle invitée via la console:

```
virsh console \[\<DomainName\> | \<DomainUUID\> |\<DomainID\> \]
```

Exemple

1 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

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

1	<interface type="bridge"></interface>
2	<mac address="52:54:00:2d:43:a4"></mac>
3	<source bridge="br0"/>
4	<model type="virtio"></model>

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.

V localhost.localdomain:6 (admin) Activities	ichine Manager		Thu 03:07
			Virtual Machine Manager
File Edit View Help			
🛀 💻 Open ▷ 🛛	8 v		
Name			
7 localhost (GEMU)			
NetScaler-VPX			
Running	Run		
	Pause		
	Shut Down Ze	it Down	
	Clone Eo	ce Off	
	Delete Sa	10	
	0		
	Open		
<[

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 :

1	Id Name	State
2		
3	0 Domain-0	running
4	1 Domain-1	paused
5	2 Domain-2	inactive
6	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 :

```
echo <number_of_VFs> > /sys/class/net/<device_name>/device/
    sriov_numvfs
```

Où:

1

- 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 :

```
1 tar xvzf <TAR file>
2 tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
3 NSVPX-KVM.xml
4 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 :

```
1 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>
2
3 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</pre>
```

L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

+ Property	+Value
<pre>+ checksum container_format created_at disk_format hw_disk_bus id min_disk min_ram name owner protected size status tags updated_at virtual_size visibility</pre>	<pre>+</pre>
+	±

3. Une fois qu'une image OpenStack est créée, provisionnez l'instance NetScaler VPX.

```
1 nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
userdata
2 ./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
3 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=218ba819-9f55-4991adb6-02086a6bdee2 est le VF OpenStack.

L'illustration suivante donne un exemple de sortie de la commande nova boot.

roperty	I Value
S-DCF:diskConfig	-+
S-EXT-AZ:availability zone	
S-EXT-SRV-ATTR:host	-
S-EXT-SRV-ATTR:hypervisor_hostname	-
S-EXT-SRV-ATTR:instance_name	instance-0000003c
S-EXT-STS:power_state	0
S-EXT-STS:task_state	scheduling
S-EXT-STS:vm_state	building
S-SRV-USG:launched_at	-
S-SRV-USG:terminated_at	1 - 1
ccessIPv4	1
ccessIPv6	1
dminPass	43EjPdM5shLz
onfig_drive	True
reated	2017-02-20T11:53:37Z
lavor	m1.medium (3)
ostId	1
d	6b9f6968-aab9-463c-b619-d58c73db3187
mage	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
ey_name	-
etadata	{}
ame	NSVPX-10
s-extended-volumes:volumes_attached	[]
rogress	10
ecurity_groups	default
tatus	BUILD
enant_id	06c41a73b32f4b48af55359fd7d3502c
pdated	2017-02-20T11:53:38Z
ser_id	418524f7101b4f0389ecbb36da9916b5

L'illustration suivante montre un exemple du fichier userdata.txt. Les valeurs contenues dans les\

1	xml version="1.0" encoding="UTF-8" standalone="no"?
2	<environment 2001="" http:="" th="" www.w3.org="" xmlns:oe="http://schemas.dmtf.org/ovf/environment/1</th></tr><tr><th>3</th><th>xmlns:xsi=" xmlschema-instance"<=""></environment>
4	oe:id=""
5	<pre>xmlns="http://schemas.dmtf.org/ovf/environment/1"></pre>
6	<platformsection></platformsection>
7	<kind>NOVA</kind>
8	<version>2013.1</version>
9	<vendor>Openstack</vendor>
10	<locale>en</locale>
11	
12	<propertysection></propertysection>
13	<property oe:key="com.citrix.netscaler.ovf.version" oe:value=" 1.0"></property>
14	<property oe:key="com.citrix.netscaler.platform" oe:value="vpx"></property>
15	citrix.com 4
16	<property <="" oe:key="com.citrix.netscaler.orch env" pre=""></property>
17	oe:value="openstack-orch-env"/>
18	<property <="" oe:key="com.citrix.netscaler.mgmt.ip" th=""></property>
19	oe:value="10.1.0.100"/>
20	<property <="" oe:key="com.citrix.netscaler.mgmt.netmask" th=""></property>
21	oe:value="255.255.0.0"/>
22	<property <="" oe:key="com.citrix.netscaler.mgmt.gateway" th=""></property>

```
23 oe:value="10.1.0.1"/>
24 </PropertySection>
25 </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

4:	enp8s0f0: <broadcast,multicast,up,lower_up< th=""><th>> mtu 1500 qdisc mq state UP mode DEFAULT qlen 1000</th></broadcast,multicast,up,lower_up<>	> mtu 1500 qdisc mq state UP mode DEFAULT qlen 1000
	link/ether 00:1b:21:7b:d7:88 brd ff:ff:ff	:ff:ff:ff
	vf 0 MAC 00:00:00:00:00:00, spoof checkin	g on, link-state auto, trust off
	vf 1 MAC 00:00:00:00:00:00, spoof checkin	g on, link-state auto, trust off
	vf 2 MAC 00:00:00:00:00:00, spoof checkin	g on, link-state auto, trust off
	vf 3 MAC fa:16:3e:1e:0b:ee, spoof checkin	g on, link-state auto, trust off
	vf 4 MAC fa:16:3e:0d:05:62, spoof checkin	g on, link-state auto, trust off
	vf 5 MAC 5e:46:0d:79:de:f8, spoof checkin	g on, link-state auto, trust off
	vf 6 MAC fa:16:3e:db:ea:b3, vlan 10 spoo	f checking on, link-state auto, trust off
	vf 7 MAC 00:00:00:00:00:00, spoof checkin	g on, link-state auto, trust off

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

[root@localhost ~]# ip link show enp8	s0f0	
4: enp8s0f0: <broadcast,multicast,up,< td=""><td>LOWER_UP> mtu 1500 qdisc m</td><td>mq state UP mode DEFAULT qlen 1000</td></broadcast,multicast,up,<>	LOWER_UP> mtu 1500 qdisc m	mq state UP mode DEFAULT qlen 1000
link/ether 00:1b:21:7b:d7:88 brd	ff:ff:ff:ff:ff	
vf 0 MAC 00:00:00:00:00:00, spoof	checking on, link-state	auto, trust off
vf 1 MAC 00:00:00:00:00:00, spoof	checking on, link-state	auto, trust off
vf 2 MAC 00:00:00:00:00:00, spoof	checking on, link-state	auto, trust off
vf 3 MAC fa:16:3e:1e:0b:ee, spoof	checking on, link-state	auto, trust off
vf 4 MAC fa:16:3e:0d:05:62, spoof	checking on, link-state	auto, trust off
vf 5 MAC 5e.46.0d.70.de.f8 spoof	checking on, link-state	auto, trust off
vf 6 MAC fa:16:3e:db:ea:b3, spoof	checking on, link-state	auto, trust off
VT / MAC 00:00:00:00:00:00; spoor	checking on, link-state	auto, trust off

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 :

Commande RHOS :

1 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 :

```
1 > $0VS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set
Interface dpdk0 type=dpdk options:dpdk-devargs=0000:03:00.0
2
3 > $0VS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set
Interface dpdk1 type=dpdk options:dpdk-devargs=0000:03:00.1
```

Commande RHOS :

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 :

1	> \$OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 set Interface vhost-user1 type=dpdkvhostuser set Interface vhost- user1 mtu_request=9000
2	
3	> \$OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 set Interface vhost-user2 type=dpdkvhostuser set Interface vhost- user2 mtu_request=9000
4	
5	chmod g+w /usr/local/var/run/openvswitch/vhost*

Commande RHOS :

```
1 ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
	type=dpdkvhostuser -- set Interface vhost-user1 mtu_request=9000
2
3 ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
	type=dpdkvhostuser -- set Interface vhost-user2 mtu_request=9000
4
5 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** :

```
1
     qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \
2
     -object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages
3
        ,share=on -numa node,memdev=mem \
4
5
     -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> \
6
     -device ide-drive, bus=ide.0, unit=0, drive=drive-ide0-0-0, id=ide0-0-0,
7
        bootindex=1 \
8
9
     -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
     -device virtio-net-pci, netdev=hostnet0, id=net0, mac=52:54:00:3c:d1:ae,
11
        bus=pci.0,addr=0x3 \
12
```

```
-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
13
        user1> \
14
     -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
15
        virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
16
     -chardev socket, id=char1, path=</usr/local/var/run/openvswitch/vhost-
17
        user2> \
18
     -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
19
        virtio-net
20
21
     pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
22
23
     --nographic
```

Pour RHOS, utilisez l'exemple de fichier XML suivant pour provisionner l'instance NetScaler VPX, en utilisant. virsh

1	<domain type="kvm"></domain>
2	<pre>chame>dndk-vnv1</pre>
4	(name) apart (printine)
5	<uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
6	
7	<memory unit="KiB">16777216</memory>
8	
9	<currentmemory unit="KiB">16///216</currentmemory>
11	<pre>(memoryBacking)</pre>
12	(incluor y buck ring)
13	<hugepages></hugepages>
14	
15	<page size="1048576" unit="KiB"></page>
16	
17	
18	
19	
20	(venu placement=letatic)>6//venu>
21	Vepu pracement- static /0(/vepu/
23	<pre><cputune></cputune></pre>
24	
25	<shares>4096</shares>
26	
27	<vcpupin cpuset="0" vcpu="0"></vcpupin>
28	
29	<vcpupin cpuset="2" vcpu="1"></vcpupin>
30	
31	<pre><vcpupin cpuset="4" vcpu="2"></vcpupin></pre>
32	$\langle v_{cnunin}, v_{cnu} = \frac{13!}{cnuset} = \frac{16!}{2}$
34	
- ·	
35	<emulatorpin cpuset="0,2,4,6"></emulatorpin>
----------	---
36	
37	
38	
39	<numatune></numatune>
40	(memory mode-letrict) podecet-101/
41	<pre><memory mode="strict" nodeset="0"></memory></pre>
42	
44	
45	<resource></resource>
46	
47	<partition>/machine</partition>
48	
49	
50	
51	<0S>
52	
53	<type arch="x86_64" machine="pc-i440tx-rhel7.0.0">hvm</type>
54	(heat download ()
55	<pre><bool dev="nd"></bool></pre>
57	$\langle los \rangle$
58	()03/
59	<features></features>
60	
61	<acpi></acpi>
62	
63	<apic></apic>
64	
65	
66	
67	<cpu check="full" match="minimum" mode="custom"></cpu>
68	(model_fellback=lellew!>Heewell_neTSV(/model>
69 70	<pre><modet lattback="attow">maswett=nolsx</modet></pre>
71	<pre><vendor>Intel</vendor></pre>
72	
73	<topology cores="6" sockets="1" threads="1"></topology>
74	
75	<feature name="ss" policy="require"></feature>
76	
77	<feature name="pcid" policy="require"></feature>
78	
79	<feature name="hypervisor" policy="require"></feature>
80	
18	<reature name="arat" policy="require"></reature>
02 02	(domain type=1/ym)
84	Kuomann cype- Kvm /
85	<name>dpdk-vpx1</name>
86	
87	<uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

88 89	<pre><memory unit="KiB">16777216</memory></pre>
90	
91 92	<currentmemory unit="KiB">16777216</currentmemory>
93	<memorybacking></memorybacking>
94	
95	<pre>cnugepages/</pre>
97	<page size="1048576" unit="KiB"></page>
99	
100	
101	
103	<vcpu placement="static">6</vcpu>
104 105	
106	
107	<shares>4096</shares>
108	<vcpupin cpuset="0" vcpu="0"></vcpupin>
110	
111	<vcpupin cpuset="2" vcpu="1"></vcpupin>
113	<vcpupin cpuset="4" vcpu="2"></vcpupin>
114 115	<vcpupin cpuset="6" vcpu="3"></vcpupin>
116	
117 118	<emulatorpin cpuset="0,2,4,6"></emulatorpin>
119	
120 121	
122	
123	<memory mode="strict" nodeset="0"></memory>
124	
126	
127	<resource></resource>
129	<partition>/machine</partition>
130 131	
132	
133 134	<05>
135	<type arch="x86_64" machine="pc-i440fx-rhel7.0.0">hvm</type>
136	(heat dout hd) ()
137	Noot dev= nd //
139	
140	

141	<features></features>			
142				
143	<acpi></acpi>			
144				
145	<apic></apic>			
146				
147				
148				
149	<cpu check="full" match="minimum" mode="custom"></cpu>			
150				
151	<model fallback="allow">Haswell-noTSX</model>			
152				
153	<vendor>Intel</vendor>			
154				
155	<topology cores="6" sockets="1" threads="1"></topology>			
156				
157	<reature name="ss" policy="require"></reature>			
158	(feature malieur luceurine), nemer locid! ()			
159	<reature name="pcid" policy="require"></reature>			
161	(feature policy-troquiret pame-thypervicert/)			
162	creature potrey-require name-hypervisor //			
163	<pre>{feature policy=!require! name=!arat!/></pre>			
164	steature potrey require name arac //			
165	<feature name="tsc\ adjust" policy="require"></feature>			
166				
167	<feature name="xsaveopt" policy="require"></feature>			
168				
169	<feature name="pdpe1gb" policy="require"></feature>			
170				
171	<numa></numa>			
172				
173	<cell cpus="0-5" id="0" memaccess="</td" memory="16777216" unit="KiB"></cell>			
	'shared'/>			
174				
175				
176				
1//				
178				
1/9	<clock offset="utc"></clock>			
101				
101	<on_powerott>destroy</on_powerott>			
102	(an) repeats restart (an) repeats			
103				
185	(on) crash)destrou((on) crash)			
186				
187	<devices></devices>			
188				
189	<emulator>/usr/libexec/gemu-kvm</emulator>			
190				
191	<disk device="disk" type="file"></disk>			
192				

```
193
             <driver name='qemu' type='qcow2' cache='none'/>
194
             <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>
195
196
             <target dev='vda' bus='virtio'/>
197
198
             <address type='pci' domain='0x0000' bus='0x00' slot='0x07'</pre>
199
                function='0x0'/>
201
           </disk>
202
           <controller type='ide' index='0'>
204
             <address type='pci' domain='0x0000' bus='0x00' slot='0x01'</pre>
                function='0x1'/>
206
           </controller>
207
208
209
           <controller type='usb' index='0' model='piix3-uhci'>
210
211
             <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
                function='0x2'/>
212
           </controller>
213
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'/>
             <source dev='enp129s0f0' mode='bridge'/>
221
222
             <model type='virtio'/>
224
225
             <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
                function='0x0'/>
226
           </interface>
227
228
           <interface type='vhostuser'>
230
             <mac address='52:54:00:55:55:56'/>
231
233
             <source type='unix' path='/var/run/openvswitch/vhost-user1'</pre>
                mode='client'/>
234
             <model type='virtio'/>
235
236
             <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
237
                function='0x0'/>
238
           </interface>
```

```
240
241
           <interface type='vhostuser'>
242
243
             <mac address='52:54:00:2a:32:64'/>
244
             <source type='unix' path='/var/run/openvswitch/vhost-user2'</pre>
245
                mode='client'/>
246
247
             <model type='virtio'/>
248
             <address type='pci' domain='0x0000' bus='0x00' slot='0x05'</pre>
249
                 function='0x0'/>
251
           </interface>
252
253
           <interface type='vhostuser'>
254
             <mac address='52:54:00:2a:32:74'/>
255
256
             <source type='unix' path='/var/run/openvswitch/vhost-user3'</pre>
257
                mode='client'/>
258
259
             <model type='virtio'/>
260
             <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
261
                 function='0x0'/>
262
263
           </interface>
264
           <interface type='vhostuser'>
             <mac address='52:54:00:2a:32:84'/>
267
269
             <source type='unix' path='/var/run/openvswitch/vhost-user4'</pre>
                mode='client'/>
270
271
            <model type='virtio'/>
272
             <address type='pci' domain='0x0000' bus='0x00' slot='0x09'</pre>
273
                 function='0x0'/>
274
275
           </interface>
276
277
           <serial type='pty'>
278
             <target port='0'/>
279
           </serial>
281
           <console type='pty'>
284
285
             <target type='serial' port='0'/>
```

287 288	
289 290	<input bus="ps2" type="mouse"/>
291 292	<input bus="ps2" type="keyboard"/>
293 294	<pre><graphics autoport="yes" port="-1" type="vnc"></graphics></pre>
295 296	<listen type="address"></listen>
297 298	
299	<video></video>
301 302	<model heads="1" primary="yes" type="cirrus" vram="16384"></model>
303	<address <br="" bus="0x00" domain="0x0000" slot="0x02" type="pci">function='0x0'/></address>
304	
305 306	
307 308	<memballoon model="virtio"></memballoon>
309	<address <br="" bus="0x00" domain="0x0000" slot="0x08" type="pci">function='0x0'/></address>
310	
311	
312	
313	
314	
315	

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.

```
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 & lt; NS-CONFIG> section:

```
1
     <NS-PRE-BOOT-CONFIG>
2
         <NS-CONFIG>
3
4
             add route 0.0.0.0 0.0.0.0 10.102.38.1
         </NS-CONFIG>
5
6
         <NS-BOOTSTRAP>
7
                  <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
8
                  <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
9
10
             <MGMT-INTERFACE-CONFIG>
11
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.

```
root@ubuntu:~/sai/19oct# ls -lh
1
2
     total 4.0K
3
     -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
    root@ubuntu:~/sai/19oct#
4
    root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
5
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
     Total directory bytes: 0
9
   Path table size(bytes): 10
10
```

```
11 Max brk space used 0
12 175 extents written (0 MB)
13 root@ubuntu:~/sai/19oct#
14 root@ubuntu:~/sai/19oct# ls -lh
15 total 356K
16 -rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
17 -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

April 1, 2025

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. L'option de licence disponible pour les instances NetScaler VPX exécutées sur AWS est Bring Your Own License (BYOL).

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
- Découvrez les avantages de NetScaler et d'AWS

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.
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.

Terme	Définition
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
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.
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.

Terme	Définition
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
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

January 15, 2025

Les tableaux suivants répertorient les offres VPX prises en charge, les régions AWS, les types d'instances et les services.

Tableau 1 : Offres VPX prises en charge sur AWS

Offres VPX prises en charge

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 (Melbourne)

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)

régions AWS prises en charge UE (Francfort) UE (Irlande) UE (Londres) UE (Daris) 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) Moyen-Orient (EAU) Afrique (Le Cap) C2S

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

c6in.large, c6in.xlarge, c6in.2xlarge, c6in.4xlarge, c6in.8xlarge, c6in.12xlarge, c6in.16xlarge, c6in.24xlarge, c6in.32xlarge

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

Types d'instance AWS pris en charge

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

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 c 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.

VPX avec licence groupée ou flexible (licences de	
bande passante)	Instance AWS recommandée
Jusqu'à 200 Mbits/s	m5.xLarge

/PX avec licence groupée ou flexible (licences de			
bande passante)	Instance AWS recommandée		
1 à 5 Gbit/s	m5.2xLarge		
5 à 8 Gbit/s	c5n.4xLarge		
8 à 25 Gbit/s	c5n.9xLarge		

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.
- NetScalerset 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 Cloud-Watch. Pour plus d'informations, consultez Surveillez vos instances à l'aide d'Amazon Cloud-Watch.

- 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 :

```
    "ec2:DescribeInstances",
    "ec2:AssignPrivateIpAddresses",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "ec2:CreateTags"
```

Paire HA avec des adresses IPv6 dans la même zone AWS :

```
    "ec2:DescribeInstances",
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "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 :

"ec2:DescribeInstances",
 "ec2:DescribeAddresses",
 "ec2:AssociateAddress",
 "ec2:DisassociateAddress",
 "iam:SimulatePrincipalPolicy",
 "iam:GetRole",
 "ec2:CreateTags"

Paire HA avec des adresses IP privées dans différentes zones AWS :

```
"ec2:DescribeInstances",
1
2
     "ec2:DescribeRouteTables",
     "ec2:DeleteRoute",
3
    "ec2:CreateRoute",
4
   "ec2:ModifyNetworkInterfaceAttribute",
5
     "iam:SimulatePrincipalPolicy",
6
     "iam:GetRole",
7
     "ec2:CreateTags"
8
```

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	<pre>"ec2:DescribeRouteTables",</pre>
6	"ec2:DeleteRoute",
7	"ec2:CreateRoute",
8	"ec2:ModifyNetworkInterfaceAttribute",
9	"iam:SimulatePrincipalPolicy",
10	"iam:GetRole",
11	"ec2:CreateTags"

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",
14 "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.
- **CLIAWS** : 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

April 1, 2025

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",
    "iam:GetRole"
```

Paire HA avec des adresses IP élastiques dans différentes zones AWS :

```
    "ec2:DescribeInstances",
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "iam:SimulatePrincipalPolicy",
    "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".
     "ec2:DescribeAddresses",
2
     "ec2:AssociateAddress",
3
    "ec2:DisassociateAddress",
4
5 "ec2:DescribeRouteTables",
   "ec2:DeleteRoute",
6
    "ec2:CreateRoute",
7
     "ec2:ModifyNetworkInterfaceAttribute",
8
9
     "iam:SimulatePrincipalPolicy",
     "iam:GetRole"
10
```

Autoscaling du backend AWS :

```
1
     "ec2:DescribeInstances".
2
     "autoscaling:*",
     "sns:CreateTopic",
3
     "sns:DeleteTopic",
4
5
    "sns:ListTopics",
     "sns:Subscribe",
6
7
     "sqs:CreateQueue",
     "sqs:ListQueues",
8
     "sqs:DeleteMessage",
9
     "sqs:GetQueueAttributes",
10
     "sqs:SetQueueAttributes",
11
12
     "iam:SimulatePrincipalPolicy",
     "iam:GetRole"
13
```

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.

New EC2 Experience X	Instances (1) Info
EC2 Dashboard	Q Find instance by attribute or tag (case-sensitive)
EC2 Global View	□ Name ♥ Instance ID Instance state ♥ Instance type ♥ Status check Alarm status Availability Zone
Events	□ adc i-0cc53b7cdd39f9621 ⊘Running @Q m5.xlarge ⊘2/2 checks passed No alarms + us-east-1a
Tags	L
Limits	
▼ Instances	
Instances New	
Instance Types	
Launch Templates	
Spot Requests	=
Savings Plans	Select an instance 🐵 🗙
Reserved Instances New	
Dedicated Hosts	
Scheduled Instances	
Capacity Reservations	
▼ Images	
AMIs New	
AMI Catalog	
Elastic Block Store	
Volumes	

3. Accédez à Actions > Sécurité > Modifier le rôle IAM.

New EC2 Experience	Instances (1/1) Info	C Connect	Instance state	Actions A Launch inst	ances 🔻
rea us what you think	Q. Find instance by attribute or tag (case-sensitive)			Connect	1 > ©
EC2 Dashboard		L testeres state		View details	
EC2 Global View	Name V Instance ID	Instance state V Insta	ance type ∨ Statu	Manage instance state	allability Zone
Events	adc i-0cc53b7cdd39f962	Pl ⊘Running @Q m5.2	klarge 🛛 2/	2 che	-east-1a
Tags				Networking	
Limits				Networking	
			Change security group	ps Security	
Instances			Get Windows passwor	rd Image and templates	
Instances New			Modify IAM role	Monitor and troubleshoot 🕨	
Instance Types					_
Launch Templates					
Spot Requests		=			
Savings Plans	Instance: i-0cc53b7cdd39f9621 (adc)				⊚ ×
Reserved Instances New	Details Security Networking Storage Status checks Monitoring Tags Instance summary Info Info <t< td=""></t<>				
Dedicated Hosts					
Scheduled Instances					
Capacity Reservations	Instance ID	Public IPv4 address	Pri	ivate IPv4 addresses	
	i-0cc53b7cdd39f9621 (adc)	🗇 52.3.230.117 open address 🗹	6	10.10.1.160	
 Images 	IPv6 address	Instance state	Pu	ıblic IPv4 DNS	
AMIs New	-	⊘ Running	-		
AMI Catalog	Hesteametype	Private IP DNS name (IPv4 only)			
Elastic Block Store	IP name: ip-10-10-1-160.ec2.internal	ip-10-10-1-160.ec2.internal			
Volumes	Answer private resource DNS name	Instance type	Ela	astic IP addresses	

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.

≡	EC2 > Instances > i-Occ53b7cdd39f9621 > Modify IAM role	
	Modify IAM role Info Attach an IAM role to your instance.	
	Instance ID I-Occ53b7cdd39f9621 (adc) IAM role Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance. Choose IAM role I you choose No IAM Role, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?	
	Cancel Update IAM role	

b) Sur la page **Rôles**, cliquez sur **Créer un rôle**.

Roles (35) Info	C	Delete	Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.			
O Search			1 2 > 6

c) Sélectionnez le service AWS sous Type d'entité de confiance et EC2 sous Cas d'utilisation courants, puis cliquez sur Suivant.

AWS service Adox AWS services like EC2, Lambda, or others to perform actions in this account.	AWS account Allow entries in other AVIS accounts belonging to you or a Bid party to perform actions in this account.	 Web identity Allows users federated by the specified external web identity provider to assume this rule to perform actions in this account. 	
 SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account. 	Custom trust policy Cruste a custom trust policy to enable others to perform actions in this account.		
Use case			
Allow an AIVS service like EC2, Lambda, or	others to perform actions in this account.		
Adow an AWS service like EC2, Lambda, or Common use cases EC2 Adows EC2 instances to call AWS servi	others to perform actions in this account.		
Common use cases Common	others to perform actions in this account.		
Common use cases Common use cases Common use cases CC Advance CC2 instances to call AVIS service Advance CC2 instances to call AVIS services Use cases for other AVIS services: Use cases for other AVIS services:	others to perform actions in this account,		

d) Sur la page **Ajouter des autorisations**, cliquez sur **Créer une politique**.

Add permissions												
Permissions policies (755) Choose one or more policies to attach to your new role.							C	C	create	e poli	cy (3
Q. Filter policies by property or policy name and press enter	<	1	2	3	4	5	6	7	3	38)		٢

	s that you can assign to a user, group, or role. You can create and edit a polic	cy in the visual editor and using JSON. Learn more
Visual editor JSON		Import managed polic
1-{ 2 "Version": "20 3 "Statement": [4 }	2-10-17",	

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 :

```
1
     {
2
3
          "Version": "2012-10-17",
          "Statement": [
4
5
              {
6
7
                  "Sid": "VisualEditor0",
                  "Effect": "Allow",
8
                  "Action": [
9
10
                       "ec2:DescribeInstances",
                       "autoscaling:*",
11
                       "sns:CreateTopic",
12
                       "sns:DeleteTopic",
13
14
                       "sns:ListTopics",
                       "sns:Subscribe",
15
                       "sqs:CreateQueue",
16
                       "sqs:ListQueues",
17
                       "sqs:DeleteMessage",
18
                       "sqs:GetQueueAttributes",
19
                       "sqs:SetQueueAttributes",
20
                       "iam:SimulatePrincipalPolicy",
21
22
                       "iam:GetRole"
23
                  ],
                  "Resource": "*"
24
               }
25
26
27
          ]
      }
28
```

Assurez-vous que la paire clé-valeur « Version » que vous fournissez est identique à celle générée automatiquement par AWS.

g) Cliquez sur Suivant : Réviser.

Create policy	1 2 3
Add tags (Optional) Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.	
No tags associated with the resource. Add tag You can add up to 50 more tags.	
	Cancel Previous Next: Review

h) Dans l'onglet **Révision de la politique**, donnez un nom valide à la politique, puis cliquez sur **Créer une politique**.

Create policy						1 2 3
Review policy						
Name*	backend_autoscaling_policy			1		
	Use alphanumeric and '+=,.@' cha	racters. Maximum 128 characte	ars.			
Description						
						li.
	Maximum 1000 characters. Use alph	anumeric and '+=,.@' charac	ters.			
Summary	Q Filter					
	Service 💌	Access level		Resource	Request conditi	on
	Allow (5 of 338 services) Sh	ow remaining 333				
	EC2	Limited: List		All resources	None	
	EC2 Auto Scaling	Full access		All resources	None	
	IAM	Limited: Read		All resources	None	
	SNS	Limited: List, Write		All resources	None	
	SQS	Limited: Read, Write		All resources	None	
Tags	Кеу		•	Value		\bigtriangledown
			No tags associate	ad with the resource.		
* Required					 	

 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.

·		0
Add permissions 👞		
Permissions palities (Selected 1/784) and Occase one or more policies to attach to your marrele.		D. Unite policy (2)
Q. Plike policies by property or policy name and press and	and the second se	< 1 + 1 + 1 + 2 - 41 5 0
B Polyzane (?	/ Bendefen	
B C tockerd_actocaling Caston		
backeed_autoscaling_policy		C free Ent
4. ("Ne": "Newlifeiner".		
i "echtbesonite Instances" Centrary Line: 11.	ou*.	
38 "See Create Depts", See Oxford Depts",		
52 "seactist/spice",		
15 "Sep Set Arbeirs ; 36 "sep Set Arbeirs sepp",		
11 See Settlementeriture		
28 "wcb:Aux/grPrivotalpAd	pOhtors', pohtors',	
21 "Saciatitics", 23 "and sharing Dysidebryon		
		li li
DoubhanColuctup		
0 @ Ondrandoketry dates		
🗇 🛞 🔒 AMSSimetionet AMS m	Provides mad only areas in a AMS Simel Convert on Inte AMS Management Consult.	
🕘 🛞 Americanista . 🛛 ANS m	Provides mad unly anoma to Amazon Stanior for the Web Managament Consults.	
🗋 🛞 🛛 ANDRANASIAN 👘 🖉 🖉	Provides the datility in advancedure and evanisments in ACS Underspinent submarks, advance universe indexional from View Underspinent Yeary Bulkerey (and provides advancedure) and provides advancedure ICS	
 (a) O ANSISCONNERS. ARE m 	Advisitional to 182 Century	
 Image: State of the state of th	Provide matching woods to MME ET 1 Outs	
 B B AndoringSensel. APD n 	Positike mad-arky assess to Ado Stanley sin the AMS Management Downlo.	
B B Annord Mitheau. And m.	Provide access to rearys 50 within the regions to 1045.	
	. The Oxfort M IM ethe	
C C MONITARE. AND M.	. Rives M access to The WB Health-Age and HealthCoard Coard Coard	
0 0 Anafotharead. Aftin	Prote preve exolute access to Assert Public access annos	
0 0 Americantha Articles		
In the second contract of the second contr	Posida da assess tra Ansen 165 es tra Addi Mengarwat Cansale.	
🔅 😟 Separther 🛛 ANS m	. This purity gravity particulars to insuline have in an AHE assume. This policy also enables that are to content-MHE support to contact and manage same.	
C C Record Cityline. All e	Penida di anasa ka Asan KC vi ka Mili Sinogenet Corada.	
🗧 🛞 🔒 Serestaktorogonile	Provide available available available for Risk Reagers & Br ANS Navagers & De ANS Na	
🗇 🛞 🔒 Antie Thogstop Alti n	Pila polity alters come to ingene Pilog at took using APS M. Burtheydageballur/tak API	
 B Brancheddina ANS n 	Provides read-only access to Andato Document/20 with MorgoDB competitivity. Note that the party access to Andaton MDB and Andaton ADB and ADB	
 But survisesions boundary - applicatif up 		
for a particular boundary is some the maximum particulars the	All situations has any source after pays or an it is highly prefer or approximate response to the	
		Ford Deces

j) Dans la page **Nom, révision et création**, attribuez un nom valide au rôle.

=	Step 1 Select trusted entity	Name, review, and create	0
	Step 2 Add permissions	Role details	
	Step 3	Role name Enter a meaningful name to identify this role.	
	Name, review, and create	ADC_JAMRicle Maximum 64 characters. Use alphanumeric and '4++, 0+-,' characters.	
		Description Add a short explanation for this role. Allows EC2 instances to call AWS services on your behalf. Maximum 1000 characters. Use alphanumeric and "+=,,@" characters.	
		Step 1: Select trusted entities	
		1 {{ 2 "Version": "2012-10-17", 3 - "Statement": [4 - { 5 "Effect": "Allow", 6 - "Action": [7 "Sts:AssumeRole" 8], 9 - "Principal": { 10 - "Service": [11 ''ec2.amazonows.com"	

k) Cliquez sur **Créer un rôle**.

Permissions policy summary			
Policy name C [*]	▽ Туре	✓ Attached as	
backend_autoscaling_policy	Customer managed	Permissions policy	
Tags Add tags (Optional) Tags are key-value pairs that you can add to AWS r	esources to help identify, organize, or search for resources.		
Tags Add tags (Optional) Tags are key-value pairs that you can add to AWS r	esources to help identify, organize, or search for resources.		
Tags Add tags (Optional) Tags are key-value pairs that you can add to AWS i No tags associated with the resource.	esources to help identify, organize, or search for resources,		
Tags Add tags (Optional) Tags are key-value pairs that you can add to AWS to No tags associated with the resource. Add tag	esources to help identify, organize, or search for resources.		
Tags Add tags (Optional) Tags are key-value pairs that you can add to AWS a No tags associated with the resource. Add tag You can add in to 50 more tags	esources to help identify, organize, or search for resources.		

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.

Modify IAM role info	
Attach an IAM role to your instance.	
instance ID	
🗇 i-099f319d4e89f0ca2 (adc)	
AM role Select an IAM role to attach to your instance or create a new rol surrently attached to your instance.	te if you haven't created any. The role you select replaces any roles that
AM role Select an IAM role to attach to your instance or create a new rol surrently attached to your instance. Choose IAM role	Le if you haven't created any. The role you select replaces any roles that
AM role elect an IAM role to attach to your instance or create a new rol urrently attached to your instance. Choose IAM role	le if you haven't created any. The role you select replaces any roles that
IAM role Sect an IAM role to attach to your instance or create a new rol currently attached to your instance. Choose IAM role Q No IAM Role Choose this option to detach an IAM role	le if you haven't created any. The role you select replaces any roles that C Create new IAM role [2 pinstance will be removed. Are you

7. Cliquez sur Mettre à jour le rôle IAM.

Modify IA	M role Info ole to your instance.					
Instance ID	20506a5b6e (NetS	caler Gateway)				
IAM role Select an IAM ro currently attach	ole to attach to your in ed to your instance.	stance or create a new	role if you haven't cre	ated any. The role	you select repl	aces any roles that are
ADC_IAMRo	le			• 0	Create	new IAM role 🛂

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.

 Sur la pageIAM, 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.

Identity and Access X Management (IAM)	IAM > Roles > ADC_IAMRole
	ADC_IAMRole
Dashboard	Allows EC2 instances to call AWS services on your behalf.
 Access management User groups 	Summary Edit
Users	Creation date ARN Instance profile ARN
Roles	July 18, 2022, 19:37 (UTC+05:30)
Policies	C_IAMROIe
Identity providers	Last activity Maximum session duration
Account settings	
 Access reports Access analyzer Archive rules 	Permissions Trust relationships Tags Access Advisor Revoke sessions
Analyzers	
Settings	Permissions policies (1)
Credential report	You can attach up to 10 managed policies.
Organization activity	Q. Filter policies by property or policy name and press enter < 1 > ③
Service control policies (SCPs)	
	Policy name C ² ∇ Type ∇ Description
Related consoles	□
IAM Identity Center 🛛 New	

2. Dans la console du **simulateur de politiques IAM**, sélectionnez **Politiques existantes** comme **mode.**

1AM Policy Simulator				Mode : Existing Policies - Existing Policies	role/AWSReservedSSO_ITH	assumed- NanagedOwnerAccess_cb743 /subhojitg ~	₹ 8e0bc5be63f
Users, Groups, and Roles	Policy Simulato	or		New Policy			
Users V Filter	Select service -	Select actions 🔹	Select All	Deselect All	Reset Contexts	Clear Results Ru	In Simulation
There are no users associated with this account.	Global Settings Action Settings an	d Results [0 actions so	elected. 0 action	ns not simulated. 0 actions	allowed. 0 actions denied.]		
	Service	Action		Resource Type	Simulation Resource	Permission	

3. Dans l'onglet **Utilisateurs, groupes et rôles**, sélectionnez **Rôles** dans le menu déroulant et choisissez un rôle existant.

i IAM Policy Simulator					Node : Existing Polic	cies -			2
Users, Groups, and Roles	Policy Simulato	or				-			
Roles V Filter	Select service -	Select actions	Ŧ	Select All	Deselect All		Reset Contexts	Clear Results	Run Simulation
ADC_IAMRole	ADC_JAMRole Global Settings								
aws-controltower-AdministratorExecuti Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions denied.]									
aws-controltower-ConfigRecorderRole	Service	Action	1		Resource Typ	be Simul	ation Resource	Permission	
aws-controltower-ForwardSnsNotificati									

4. Après avoir sélectionné le rôle existant, sélectionnez la politique existante en dessous de celuici.

Folicies	Policy Simulator									
Selected role: ADC_IAMRole	Select service - Sele	ect actions - Select	All Deselect All	Reset Contexts	Clear Results Run Simulation					
WS Organizations SCPs	 Global Settings ① 									
Service control policies (SCPs) applied to your account can impact your access to AWS services.	Action Settings and Re	Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]								
Learn more.	Service	Action	Resource Type	Simulation Resource	Permission					
Custom IAM Policies There are no policies to display!	2									
Permissions Boundary Policy You can simulate a maximum of one permissions	-									

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.

Policies Back	Policy Simulator	r						
Editing policy: backend_autoscaling_policy	Amazon EC2 A 👻	Select actions 🔹	Select All	Deselect All	Reset C	ontexts	Clear Results	Run Simulation
<pre>Editing policy: backend_auroscaling_policy { "Version": "2012-10-17", "Statement": { {</pre>	Global Settings Action Settings and Service	Attachinstances BatchPutScheduledUp. CreateLainchConfigur. DeleteLifecycleHook DeleteLifecycleHook DescribeLaunchConfigur. DescribeLaunchConfigur. DescribeLaundBalancers DescribeLaundBalancers ExecutePolicy PutNotificationConfigur. RecortLifecycleAction. SatinstanceProtection	Attachi Attachi Attachi Cancel Cancel Cancel Delete Delete Delete Descrit Descrit Descrit Descrit Descrit Descrit Descrit Descrit Startist Startist	LoadBalancerTar InstancerTars DrUpdateTags NotificationConfi VarmPool eeAutoScalingIn eeLifecycleHock eeScalingProces eeScalingProces eeScalingProces eeScalingProces eeScalingProces estanceRefresh	AttachLoadBalancers CompleteLifecycleAction DeleteAutoScalingGroup DeletePolicy DescribeActoountLimits DescribeAutoScalingN DescribeAutoScalingN DescribeNotificationCo DescribeScheduleActI DescribeScheduleActI Detachinstances EnableMetricsCollection GetPredictiveScalingFo PutScheduledUpdateG SetDesiredCapacity SuspendProcesses	Batchh	DeleteScheduled AutoScalingGroup LaunchConfigura ScheduledAction bbeAdjustmentTy bbeIotagBalancer bbeIotagBalancer bbeTagas LoadBalancerTa Standby seycleHook armPool tanceHealth nateInstanceInAut	

6. Cliquez sur **Exécuter la simulation**.

Policies	Policy Simulator								
Editing policy: backend_autoscaling_policy	Amazon EC2 A 👻 61 Action	n(s) sel Select All	Deselect All	Reset Contexts	Clear Results Run Simulation				
{	 Global Settings 1 								
"Version": "2012-10-17", "Statement": [Action Settings and Results [61 actions selected. 0 actions not simulated. 61 actions allowed. 0 actions denied.]								
{ "Sid": "VieualEditor0"	Service	Action	Resource Type	Simulation Resource	Permission				
"Effect": "Allow",	Amazon EC2 Auto Scaling	AttachInstances	autoScalingGroup	•	allowed 1 matching statements.				
"Action": ["ec2:DescribeInstances", "autoscaling:", "ans:OreataTopic", "ans:DeletaTopic", "ans:Subscribe", "ans:Subscribe",	Amazon EC2 Auto Scaling	AttachLoadBalancerTargetGr	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	AttachLoadBalancers	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	BatchDeleteScheduledAction	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	BatchPutScheduledUpdateG	autoScalingGroup	•	allowed 1 matching statements.				
"sqs:ListQueues", "sqs:DeleteMessage",	Amazon EC2 Auto Scaling	CancelInstanceRefresh	autoScalingGroup	•	allowed 1 matching statements.				
"sqs:GetQueueAttributes", "sqs:SetQueueAttributes",	Amazon EC2 Auto Scaling	CompleteLifecycleAction	autoScalingGroup	•	allowed 1 matching statements.				
"iam:SimulatePrincipalPolicy", "iam:GetRole"	Amazon EC2 Auto Scaling	CreateAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.				
], "Percurse": ""	Amazon EC2 Auto Scaling	CreateLaunchConfiguration	launchConfiguration	•	allowed 1 matching statements.				
} } }	Amazon EC2 Auto Scaling	CreateOrUpdateTags	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	DeleteAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	DeleteLaunchConfiguration	launchConfiguration	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	DeleteLifecycleHook	autoScalingGroup	•	allowed 1 matching statements.				
	Amazon EC2 Auto Scaling	DeleteNotificationConfiguration	autoScalingGroup	•	allowed 1 matching statements.				

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

April 1, 2025

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**.

Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance
Note: Your instances will launch in the Asia Pacific (Mumbai) region

- 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

🧊 Servi	ces 👻 Resource Gr	oups 🗸 🛠				
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review

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

April 1, 2025

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. SélectionnezVPC avec un seul sous-réseau publicet 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 10.0.0/24. (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**.

Step 2: VPC with a Sin	gle Public Subnet	
IPv4 CIDR block:*	10.0.0/16	(65531 IP addresses available)
IPv6 CIDR block:	No IPv6 CIDR Block Amazon provided IPv6 C	JDR block
VPC name:	NSDoc	
Public subnet's IPv4 CIDR:*	10.0.0/24	(251 IP addresses available)
Availability Zone:*	ap-south-1a 🛊	
Subnet name:	NSDoc-MGMT	
	You can add more subnets	after AWS creates the VPC.
Service endpoints		
	Add Endpoint	
Enable DNS hostnames:*	O Yes ○ No	
Hardware tenancy:*	Default \$	
		Cancel and Exit Back Create 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.

Create Subnet						×
Use the CIDR format to spec netmask and /28 netmask. A	cify your subnet's IP address bloc Iso, note that a subnet can be the	k (e.g., 10.0.0 e same size a	.0/24). No s your VPC	te that block sizes mus C. An IPv6 CIDR block	st be between a / must be a /64 CII	16 DR block.
Name tag	NSDoc-client		0			
VPC	vpc-ac9ad2c5 NSDoc 🛟 🚺					
VPC CIDRs	CIDR	Status		Status Reason		
	10.0.0/16	associated				
Availability Zone IPv4 CIDR block	ap-south-1a 🛟 🕄		0			
					Cancel Yes	, Create

3. Répétez les étapes pour créer un sous-réseau supplémentaire pour les serveurs principaux.

Create Subnet			×
Use the CIDR format to spec netmask and /28 netmask. A	ify your subnet's IP address Iso, note that a subnet can	s block (e.g., 10.0.0.0/2 be the same size as yo	4). Note that block sizes must be between a /16 ur VPC. An IPv6 CIDR block must be a /64 CIDR block.
Name tag	NSDoc-server	0	
VPC	vpc-ac9ad2c5 NSDoc	• 0	
VPC CIDRs	CIDR	Status	Status Reason
	10.0.0/16	associated	
Availahility Zone	No Preference		
IPv4 CIDR block	10.0.2.0/24	0	
			Cancel Yes, Create

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.

Create Route Tabl	e	×
A route table specifies how p and your VPN connection.	packets are forwarded between the subn	ets within your VPC, the Internet,
Name tag VPC	NSDoc-internet-traffic vpc-ac9ad2c5 NSDoc 🛟 🛈	0
		Cancel 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.

b-4329082	a NSD	oc-internet-tra	ffic					
Summa	ıry	Routes	Subne	et Associatio	ns	Route	Propagation	Т
Cancel	Save							
Associate	Subne	ət		IPv4 CIDR	IP	6 CIDR	Current Route	Table
2	subnet	-c4ce9aad NSD	oc-MGMT	10.0.0/24	-		rtb-735a7b1a	
2	subnet	-31ce9a58 NSD	oc-client	10.0.1.0/24	-		Main	
	subnet	-d0cd99b9 NSE	oc-server	10.0.2.0/24	-		Main	

- 7. Cliquez sur Itinéraires > Modifier > Ajouter un autre itinéraire.
- 8. Dans le champ Destination, ajoutez 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.

rtb-4329082a NSDoc-internet-traffic							
Summary	Routes	Subnet Associations	Ro	ute Propa	gation		Tags
Cancel Save							
	View:	All rules					
Destination		Target		Status	Propag	gated	Remove
10.0.0/16		local		Active	No		
0.0.0/0		igw-9fbe2df6			No		0
Add another route							

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

🧊 Services - Resource	pups v 🔭	🕽 nirmalanaj @ nirmalanaj ~	Mumbai • Support •
1. Choose AMI 2. Choose Instance Type	3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review		
Step 3: Configure Instan Configure the instance to suit your require more.	e Details ents. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower price	ing, assign an access manageme	nt role to the instance, and
Number of instances	Launch into Auto Scaling Group ()		
Purchasing option	Request Spot Instances		
Network	Vpc-ac9ad2c5 NSDoc Create new VPC		
Subnet	subnet-c4ce9aad NSDoc-MGMT ap-south-1a Create new subnet 251 IP Addresses available		
Auto-assign Public IP	Enable		
Placement group	No placement group		
IAM role	None Create new IAM role		
Shutdown behavior) Stop 🖸		
Enable termination protection	Protect against accidental termination		
Monitoring	 Enable CloudWatch detailed monitoring Additional charges apply. 		
EBS-optimized instance	CLaunch as EBS-optimized instance		
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.		
	Cancel	Previous Review and Launa	Next: Add Storage

- 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 : Con-***figurer le groupe de sécurité*.
- 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.

Select an existing key pair or create a new key pair	×
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you securely SSH into your instance.	d to
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.	
Choose an existing key pair	
Select a key pair	
NSDOCKeypair 📀	
I acknowledge that I have access to the selected private key file (NSDOCKeypair.pem), and that without this file, I won't be able to log into my instance.	
Cancel Launch 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**.

Create Netwo	ork lı	nterface		×
Description	(j)	NSDoc-VIP-NIC		
Subnet	0	subnet-31ce9a58 ap-south-1a NSDoc-client		
Private IP	0			
Security groups		sg-use3186d - Netscaler VPX - Customer Licensed-12-U-41-23-Auto sg-d2946fba - default - default VPC security group		
			Cancel	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**.

Name	Network Interna	Subilet ID	VPCID	Zone	Security groups
NSDoc-VIP	eni-3c843657	subnet-31ce9a	vpc-ac9ad2c5	ap-south-1a	default
NSDoc-SNIP	eni-3e8b3955	subnet-d0cd99	vpc-ac9ad2c5	ap-south-1a	default
	eni-dd1cacb6	subnet-9d43f6f4	vpc-52ab033b	ap-south-1a	FreeBSD 11-11-0-R
NSDoc-NSIP	eni-878133ec	subnet-c4ce9aad	vpc-ac9ad2c5	ap-south-1a	NetScaler VPX - Cu
	eni-2da8a261	subpet-fe6882b3	vpc-52ab033b	an-south-1h	AL1
	eni-e0f9128b	Attach Net	work Inter	face	×
	eni-0e55e565				
	eni-1fa9ef53	Network Interfa	ace: eni-3e8b3	955	
	eni-23ff4a48	Instance	ID: i-0296946	19cd5b71ec - NSDoc-	VM (running)
	eni-45fb4e2e				
	eni-76f84d1d				
	eni-72ff183d			Car	

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 nou-velle 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.

Associate address					
Select the instance OR network interface to	which you want to associate	e this Elastic IP addres	ss (13.126.158.205)		
Resource type	 Instance () Network interface 				
Network interface	eni-878133ec	•	C		
Private IP	Q Filter by attributes		C 0		
Reassociation	eni-0e55e565 eni-dd1cacb6 eni-76f84d1d		tached 🚯		
Warning If you associate an Elastic IP ad	eni-72ff183d eni-878133ec eni-23ff4ø48 eni-1fa9ef53	NSDoc-NSIP	ress is released. Learn more.		
* Required	eni-2da8a261		l	Cancel	Associate

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 \\<location of your private key\\> ns root@\\< public DNS of the instance\\>

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 https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US

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.

 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.

Welcome to	
Backup and R	estore
he backup and restore fun sed to restore the Citrix Al o create a backup, click th	ctionality of the Citrix ADC appliance allows you to create a backup file of the Citrix ADC configurations. This file can later be C configurations to the previous state. e "Backup" link shown below. When required, select one of the backups and restore the appliance.

- 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.

Backup/Impor			
Create	Import		
Citrix ADC Versio NS13.1: Build 50.	n I9.nc, Date: Sep 25 20)23, 21:28:29 (64-bit)	
File Name			
fullbackup		(j)	
Level*			
Full		~ (i)	
Comment			
None			
Backup	Cancel		

System > Backup and Restore > Backup/Import

d) Cliquez sur **Sauvegarde**. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et le télécharger sur votre machine locale.

System > B	ackup and Restore											
Backup	o and Rest	ore	D								\sim	F
Backup/Im	Delete	✓ Select	ct Action	Dowr	nload							
Q Click here	e to search or you can e	Rest	ore	at								()
	FILE NAME		LEVEL		CREATED BY	CREATION TI	ME			SIZE (IN KB	3)	
	fullbackup.tgz		Full		nsroot	Wed Oct 415	:01:42 2023			2117 KB		
Total 1							25 Per Page	\sim	Page	1 of 1		

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.

System	>	Backup and Restore	>	Backup/Import
--------	---	---------------------------	---	---------------

I	3ackup/Import	
(Create Import	
F	File Name*	_
	Choose File 🗸	🚺 🌗 Please choose file
	Local	-
	Appliance Cancel	

- d) Sélectionnez le fichier.
- e) Dans le menu déroulant Sélectionner une action, sélectionnez Restaurer.

System > Ba	ackup and Restore							
Backup	and Resto	ore 🕕						
Backup/Im	port Delete	✓ Select Ad Download Restore	tion	ore				Û
	to search of you carre		Jac					0
	FILE NAME	¢ Le	VEL 🌩	CREATED BY	CREATION TIME		SIZE (IN KB)	
	fullbackup.tgz	Fu	l	nsroot	Wed Oct 4 15:01:42 2023		2117 KB	
Total 1					25 Per Page	∨ Page	1 of 1	• •

f) Sur la page **Restaurer**, vérifiez les détails du fichier, puis cliquez sur **Restaurer**.

← Restore

File Name fullbackup.tgz
Level Full
Citrix ADC Version NS13.1-50.19
IP Address 10.102.126.34
Size (in KB) 2117
Created By nsroot
Creation Time Wed Oct 4 15:01:42 2023
Comment None
Skip Backup (i)
Restore Close

- 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 réseauet 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.

New EC2 Experience Tell us what you think	Network interfaces (1)			
EC2 Dashboard New	Q. Filter network interfaces			
Events	Network Interface ID: eni-0			
Tags		Attach network interface	×	
Limits	🗹 Name 🔻			
Instances	- 2	Network interface		
Instances New		eni-0432953739657651e		
Instance Types		Instance		
Launch Templates		Choose an instance	Ψ	
Spot Requests				
Savings Plans			Cancel Attach	
Reserved Instances New				_
Dedicated Hosts				
Scheduled Instances				
Capacity Reservations				

- 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 IPet 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.

aws	Services 🔻	Q Search for services, feature	res, marketplace products, and docs	[Alt+S]
	IPv4 addresses			
	Private IP address	Public IP address		
	192.168.1.180	3.209.165.4	Unassign	
	192.168.1.121		Undo	
	192.168.1.243		Undo	
	Assign new IP add	ess		
	 Allow secondary privat Allows you to reassign a pr instance or network interful 	e IPv4 addresses to be reassig ivate IPv4 address that is assigned ace.	ined to this network interface to another	
				Cancel Save

- 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, reportezvous 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 activepassive 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 :

```
1 ssh -i <location of your private key> nsroot@<public DNS of the
instance>
```

Ensuite, configurez VIP et SNIP.

Pour les VIP, tapez :

1 add ns ip <IPAddress> <netmask> -type <type>

Pour SNIP, tapez :

1 add ns ip <IPAddress> <netmask> -type SNIP

Tapez save config pour enregistrer.

Pour voir les adresses IP configurées, tapez la commande suivante :

1 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 :

1

```
add ha node <id> <private IP address of the management NIC of the secondary node>
```

Sur le nœud secondaire, tapez la commande suivante :

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 HABasculement.

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 régiondu 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.

Step 1 Specify template	Create stack	
Step 2 Specify stack details	Prerequisite - Prepare template	
Step 3	Prepare template Every stack is based on a template. A template is a JSON or VAML file that contains configuration info	ormation about the AWS resources you want to include in the stack.
Configure stack options	Template is ready Use a sample template	 Create template in Designer
Step 4 Review		
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon 53 URL where it will be stored.	
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. • Amazon S3 URL	load a template file
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Image: Amazon S3 URL Amazon S3 URL Amazon S3 URL	load a template file
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL Amazon S3 URL https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4	load a template file b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-45b4-8b9

- 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 clientet 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 clientet 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-amazoncloudWatch).
- 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.

Step 1 Specify template	Specify stack details
Step 2 Specify stack details	Stack name
	Stack name
Step 3	Enter a stack name
Configure stack options	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Step 4	
Review	Parameters Parameters are defined in your template and allow you to input custom values when you create or update a stack.
	Network Configuration
	VPC ID to deploy the resources
	· · · · · · · · · · · · · · · · · · ·
	Address range to access Management interfaces via SSH, HTTP, HTTPS ports Must be a valid IP COR range of the form xxxxx/x
	Subnet ID associated with Primary and Secondary ADCs Management interface
	Subnet ID associated with Primary and Secondary ADCs Client interface (Traffic coming from `client` to the `ADC VIP`)
	Subnet ID associated with Primary and Secondary ADCs Client Interface (Traffic leaving from the 'ADC SNIP' to the 'backend')
	¥
	VPCTenancy
	default V
	Citrix ADC Configuration
	ms stame
	Keynair to scoriate to ADC c
	Publish custom metrics to CloudWatch?
	Yes
	Optional Configuration
	Should PublicIP(EIP) be assigned to management Interfaces? If not specified, the private ip will be auto assigned
	No
	Should PubliciP(EIP) be assigned to client interface?

- 14. Cliquez sur Suivant.
- 15. La page **Configurer les options de la pile** apparaît. Il s'agit d'une page facultative.

Step 1 Specify template	Configure stack options
Step 2 Specify stack details	Tags . You can specify tags flery-value paint to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more 🕑
Step 3 Configure stack options	Kay Value R
Step 4 Review	m o v e
	Add tag
	Permissions Onose an IMM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more
	IAM role - optional Concest the IAM role for CloudFormation to use for all operations performed on the stack. IAM role name Conceleration conceleration
	Advanced options You can set additional options for your stack, like notification options and a stack policy. Learn more [2]
	 Stack policy Defines the resources that you want to protect from unintentional updates during a stack update.
	Rollback configuration Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back, Learn more C
	► Notification options
	Stack creation options

- 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.

C Stacks (1)	© × < 1 >	Stack info Events 1	Resources	Outputs Parameters	Delete Template Change sets	Update Stack actions V
2020-10-28 13:42:49 UTC+0530	0	Q. Search events				
		Timestamp		Logical ID	Status	Status reason
		2020-10-28 13:45:59 UTC+053	0		CREATE_COMPLETE	
		2020-10-28 13:45:56 UTC+053	0	SecondaryInstance	O CREATE_COMPLETE	
		2020-10-28 13:45:39 UTC+053	0	SecondaryInstance	CREATE_IN_PROGRESS	Resource creation Initiated
		2020-10-28 13:45:37 UTC+053	0	SecondaryInstance	CREATE_IN_PROGRESS	
		2020-10-28 13:45:34 UTC+053	0	PrimaryInstance	CREATE_COMPLETE	
		2020-10-28 13:45:18 UTC+053	0	PrimaryInstance	CREATE_IN_PROGRESS	Resource creation Initiated
		2020-10-28 13:45:15 UTC+053	0	PrimaryInstance	CREATE_IN_PROGRESS	
		2020-10-28 13:45:13 UTC+053	0		CREATE_COMPLETE	
		2020-10-28 13:43:22 UTC+053	0	PrimaryManagementENI	CREATE_COMPLETE	

- 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'utilisateurnsroot 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.

Node	S 2										
Add	Edit	Delete	ics	Select Ac	tion 🗸	·					
	ID	IP ADDRESS		HOST NAME		MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE		SYNCHRONIZAT
	0					Primary	• UP	DISABLED	ENABLED		-NA-
	1					Secondary	• UP	DISABLED	SUCCESS		-NA-
Total 2										2	5 Per Page 🗸 🗸

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.

testfarhan-PrimaryInstance	i-0bb6e330c2b51d145 ORunning	⊕ Q m5.xlarge	 Initializing 	No alarms	us-east-1b	-
testfarhan-SecondaryInstance	i-02ad0511c02899312	@.Q m5.xlarge	⊘ 2/2 checks	No alarms	us-east-1b	-
stance: i-0bb6e330c2b51d145 (testfarhan-Primar	yInstance)					
Details Security Networking Storag	ge Status Checks Monitoring	Tags				
			Add to dashboard 1h	3h 12h 1	d 3d 1w custom	2 🖬
CPU utilization (%) Percent 27 15.5 07:30 07:45 08:00 08:15 08:30 01:0bb6e330c2b51d145 (testfarhan-PrimaryInstar	Status check failed (any) (count) Count 1 0 5 0 07:30 07:45 08:00 08:15 00 • i-0bb5e330c2b51d145 (testfarhan-PrimaryInsta	Status check Count 1 0.5 0 3:30 07:30 07:30 07:30 07:30	failed (instance) (cou 45 08:00 08:15 08:30 510145 (testfarhan-PrimaryInstar	Status o Count 1 0.5 0 07:30	heck failed (syste 07:45 08:00 330c2b51d145 (testfarha	em) (count) 08:15 08:30 In-PrimaryInstar
Network in (bytes) Bytes	Network out (bytes) Bytes	Network pac	kets in (count)	Network Count	k packets out (co	unt)

5. Sous Toutes les mesures, cliquez sur votre ID d'instance.

Α	All metrics	Graphed metrics	Graph options	Source
A	• •	<i-01c50c91dd353< td=""><td>7d7a> Q Search</td><td>for any metri</td></i-01c50c91dd353<>	7d7a> Q Search	for any metri
5	5 Metrics			
	CPU			
	2 Metrics			
	Throughp	out		
	2 Metrics			

- 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.

Untitle	ed graph	I					1h 3h	12h 1d 3	ld 1w <mark>custo</mark>	m (2w) 🔸	Line	✓ Ac	tions •	C • 0
Percen	t													
3.7 -														
0.933														
Mar	04/26 agement CP	04/27 U usage 🥚 Pack	04/28 ket CPU usa	04/29 ige	04/30	05/01	05/02	05/03	05/04	05/05	05/06	05/07	05/08	05/09
Mar	04/26 agement CP etrics	04/27 U usage Pack Graphed metri	04/28 ket CPU usa	04/29 Ige Graph opt	04/30	05/01 Source	05/02		05/04	05/05	05/06	05/07	05/08	05/09
MarAll meAd	04/26 agement CP etrics d a math e	04/27 U usage Pack Graphed metri	04/28 ket CPU usa	04/29 ige Graph opt	04/30	05/01 Source	05/02		05/04	05/05 Statisti	05/06	o5/o7 ✓ Period:	05/08 5 Minutes ~	05/09 Remove al
All me	04/26 agement CP etrics d a math e Lat	04/27 U usage Pack Graphed metri expression Pack	04/28 xet CPU usa	04/29 ige Graph opt	04/30 ions Details	05/01 Source	05/02		05/04	05/05 Statisti	05/06 c: Average tatistic	 O5/07 Period: 	05/08 5 Minutes V Y Axis	05/09 Remove all Actions
All me	04/26 agement CP etrics d a math e Lat Ma	04/27 U usage Pack Graphed metri expression Pack agement CPU	04/28 xet CPU usa ics (2) usage	04/29 lige Graph opt	04/30 ions Details	05/01 Source	05/02	05/03 *** > * Manager	05/04 ment CPU usag	Statisti ge * Av	05/06 c: Average tatistic verage	 Period: Period 5 Minutes 	05/08 5 Minutes ↓ Y Axis < >	Remove all Actions △ ② ③

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 sousréseau 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 <server_type&#062; vserver &#060;vserver_name&#062;
<protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -
ipset \\<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'utilisateurnsroot 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**.
- 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**.

Load Balancing Virtual Server Export as a Template						
Basic Settin	ıgs					
Name Protocol State IP Address Port Traffic Domain	vserver1 HTTP DOWN 192.168.2.129 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging	- NONE IP 1 ipset123 PASSIVE ENABLED			
		AppFlow Logging Retain Connections on Cluster				

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



Before failover

After failover

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.

Add	Edit	Statistics	Select Action $~~$				
•	ID	IP Address	Host Name	Master State	Node State	INC	Synchronization State
	0	192.168.1.108		Primary	• UP	ENABLED	ENABLED
	1	192.168.6.82		Secondary	• UP	ENABLED	SUCCESS

5. Après un basculement forcé, le secondaire devient le nouveau principal.

Nodes	2	Route Monitors 0 Failove	r Interface Set 0				
Add	Edit	Delete Statistics	Select Action				
	ID	IP Address	Host Name	Master State	Node State	INC	Synchronization State
	0	192.168.1.108		Secondary	• UP	ENABLED	SUCCESS
	1	192.168.6.82		Primary	• UP	ENABLED	ENABLED

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 :

```
{
1
2
          "Version": "2012-10-17",
3
          "Statement": [
4
5
              {
6
                  "Action": [
7
                       "ec2:DescribeInstances",
8
9
                       "ec2:DescribeAddresses",
                      "ec2:AssociateAddress",
10
                      "ec2:DisassociateAddress",
11
12
                      "ec2:DescribeRouteTables",
13
                       "ec2:DeleteRoute",
                       "ec2:CreateRoute"
14
                       "ec2:ModifyNetworkInterfaceAttribute",
15
                       "iam:SimulatePrincipalPolicy",
16
                       "iam:GetRole"
17
                  ],
                  "Resource": "*",
19
                  "Effect": "Allow"
20
21
               }
         ]
24
      }
```

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 :

1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidrblock 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.

aws Services 🔻

Route Tables > Edit routes

Edit routes

Destination	Target
192.168.0.0/16	local 🗸
0.0.0/0	igw-0b6da15e72de5729e 🔹
10.10.0/24	eni-09ad18f01f854b8ab 🗸
5500/16	oni 00od18f01f854b8ob
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'utilisateurnsroot 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.

G Load Balancing Virtual Server

Load Balar	Load Balancing Virtual Server Export as a Template							
Basic Settin	gs							
Name Protocol State IP Address Port Traffic Domain	My LB HTTP © UP 10.10.10.10 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- IP 1 - PASSIVE ENABLED NO -					
Services an	d Service Groups							
1 Load Balan	cing Virtual Server Service Binding							

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
```

5		"Sid": "VisualEditor0",
6		"Effect": "Allow",
7		"Action": [
8		"ec2:DisassociateAddress",
9		"iam:GetRole",
10		"iam:SimulatePrincipalPolicy",
11		"ec2:DescribeInstances",
12		"ec2:DescribeAddresses",
13		<pre>"ec2:ModifyNetworkInterfaceAttribute",</pre>
14		"ec2:AssociateAddress",
15		"sts:AssumeRole"
16],	
17		"Resource": "*"
18	}	
19		
20]	
21	}	

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 :

```
1
      {
2
           "Version": "2012-10-17",
3
4
           "Statement": [
               {
5
6
                   "Sid": "VisualEditor0",
7
                   "Effect": "Allow",
8
                   "Action": [
9
                        "ec2:CreateRoute",
                        "ec2:DeleteRoute",
11
12
                        "ec2:DescribeRouteTables"
13
                   ],
                   "Resource": "*"
14
                }
15
17
           ]
18
        }
```

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.

Create role			
Select type of trusted enti	ty		
AWS service EC2, Lambda and others	Another AWS a Belonging to you o	account or 3rd party Web identity Cognito or any O provider	penID
Allows entities in other accounts to perfors Specify accounts that car	orm actions in this accour	int. Learn more	
Ac	count ID*	0	

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**.

Q Search Menu		AWS	~ P
Favorites	\sim	Configuration Commonwe	Confirmum Claud Departmenters
AWS	\sim	No Cloud Profile	Change Cloud Parameters
Cloud Profile			
System	>		
AppExpert	>		

2. Sur la page Configurer les paramètres du cloud AWS, entrez la valeur du champ ROLearn.

← Configure AWS Cloud Parameters

neo.rolearn

errtfvf

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 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 :

1 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.

TRANSIT	<											2
GATEWAYS	Transit Gat	teway Route Tal	ble: taw-rtb-09f12d	a61473654a7								Ē
Transit Gateways		,	5									
Transit Gateway	Details	Associations	Propagations	Prefix list references	Routes	Tags						
Attachments	The Arbit	h - l		0 to to to to								
Transit Gateway	The table	e below will return	a maximum of 100	o routes. Narrow the filter	or use expor	t routes to vi	ew more ro	outes.				
Route Tables	Create	static route										
Transit Gateway												
Multicast	Q Filt	er by attributes or	search bv kevword							K < 1 to 3	of 3 > >	

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.

Transit Gateway Route Tables > Create	static route		
Create static route			
Add a static route to your Transit Gateway	route table.		
Transit Gateway ID	tgw-0b3e99191e03c16ed		
Transit Gateway route table ID	tgw-rtb-09f12ca61473654a7		
CIDR*		0	
Blackhole			
Choose attachment	•	C	
* Required			Cancel Create static route

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 surhttps://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 :

- 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 :
 - 1 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.

```
1 add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER
        (\"Host\")" "\"citrix.execute-api.<region>.amazonaws.com\""
2
3 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.

```
1 add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER(\"Host
    \").CONTAINS(\"restapi.citrix.com\") "rewrite_host_hdr_act
2
3 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.

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/usergui de/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",
           "Statement": \[
4
5
            {
6
                   "Action": \[
7
                        "ec2:DescribeInstances",
8
9
                        "ec2:DescribeNetworkInterfaces",
                        "ec2:DetachNetworkInterface",
10
                        "ec2:AttachNetworkInterface",
11
                        "ec2:StartInstances",
12
                        "ec2:StopInstances",
14
                        "ec2:RebootInstances".
                        "autoscaling:\*",
15
16
                        "sns:\*",
                        "sqs:\*"
17
```

```
18
19
                    "iam: SimulatePrincipalPolicy"
                    "iam: GetRole"
20
21
                    \],
                    "Resource": "\*".
22
                    "Effect": "Allow"
23
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.

← Create Cloud Profile

Name	
test-cloudprofile	
Virtual Server IP Address*	
~	
Load Balancing Server Protocol	
нттр 🗸	
Load Balancing Server Port	
80	
Auto Scale Group	
test-script	
Auto Scale Group Protocol	
HTTP ~	
Auto Scale Group Port	
80	
Select this option to drain the connections	gracefully. Else the connections will be dropped in the event of scale down.
Graceful	
Delay (Seconds)	

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.

Q Search Menu	AWS > Cloud Profile						
Favorites ~	Cloud Profile 1						
AWS ~	Add Edit Delete						
Cloud Profile	Q Click here to search or you can enter Key : Value format						
System >	NAME AUTO SCALE GROUP LOAD BALANCING VIRTUAL SERVER AUTO SCALE GROUP PROTOCOL GR	ACEFUL					
AppExpert >	test-cloudprofile _test-script_80 _CP_test-cloudprofile_192.168.2.53_LB_ HTTP NO)					
Traffic Management >	Total 1 25 Per Page Y Page 1 of 1						
Optimization							

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

April 1, 2025

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 & SE-CURITY > 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.

```
    Connectez-vous au **groupe de ressources AWS**utilisateur et accé
dez à **EC2 > NETWORK & SECURITY > Elastic IPs**.
    Cliquez sur**Attribuer une nouvelle adresse**pour créer une adresse
IP élastique.
    Configurez l'adresse IP élastique pour qu'elle pointe vers l'
utilisateur qui exécute l'instance NetScaler dans AWS.
    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 AWSutilisateur et accédez à EC2 > LOAD BAL-ANCING > 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 parentenfant.

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 parentenfant 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 Style-Book 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, consultez 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.

Déployez NetScaler Web App Firewall sur AWS

October 17, 2024

Le NetScaler Web App Firewall peut être installé en tant que périphérique réseau de couche 3 ou en tant que pont réseau de couche 2 entre les serveurs du client et les utilisateurs du client, généralement derrière le routeur ou le pare-feu de l'entreprise cliente. NetScaler Web App Firewall doit être installé à un endroit où il peut intercepter le trafic entre les serveurs Web et le hub ou le commutateur via lequel les utilisateurs accèdent à ces serveurs Web. Les utilisateurs configurent ensuite le réseau pour envoyer des requêtes au Web Application Firewall plutôt que directement à leurs serveurs Web, et des réponses au Web Application Firewall plutôt que directement à leurs utilisateurs. Le Web Application Firewall filtre ce trafic avant de le transférer vers sa destination finale, en utilisant à la fois son ensemble de règles internes et les ajouts et modifications de l'utilisateur. Il bloque ou rend inoffensif toute activité qu'il détecte comme nuisible, puis transfère le trafic restant au serveur Web. L'image précédente donne un aperçu du processus de filtrage.

Pour plus d'informations, consultez Comment fonctionne NetScaler Web App Firewall.

Architecture pour NetScaler Web App Firewall sur AWS pour le déploiement en production

Citrix WAF in AWS Cloud(Production Deployment) **NWS Cloud** Availability Zone 1 Availability Zone 2 Client Ð AWS IAM interface 0.050/24 10.0.2.0/24 Secondary Citrix WAR Cityix WAF HA pai Priman Citrix W Privati distant and ntentace vierface 100.03.0/24 10.0.4.0/24 06073 30.0.0.0/16

L'image montre un cloud privé virtuel (VPC) avec des **paramètres par défaut** qui crée un environnement NetScaler Web App Firewall dans le cloud AWS.

Dans un déploiement de production, les paramètres suivants sont configurés pour l'environnement NetScaler Web App Firewall :

- Cette architecture suppose l'utilisation d'un modèle AWS CloudFormation.
- Un VPC qui couvre deux zones de disponibilité, configuré avec deux sous-réseaux publics et quatre sous-réseaux privés, conformément aux bonnes pratiques AWS, afin de vous fournir votre propre réseau virtuel sur AWS avec un bloc de routage inter-domaine sans classe (CIDR) /16 (un réseau avec 65 536 adresses IP privées).

- Deux instances de NetScaler Web App Firewall (principale et secondaire), une dans chaque zone de disponibilité.
- **Trois groupes de sécurité**, un pour chaque interface réseau (gestion, client, serveur), qui agissent comme des pare-feu virtuels pour contrôler le trafic pour leurs instances associées.
- **Trois sous-réseaux**, pour chaque instance : un pour la gestion, un pour le client et un pour le serveur principal.
- Une passerelle Internet connectée au VPC et une table de routage de sous-réseaux publics qui est associée à des sous-réseaux publics afin de permettre l'accès à Internet. Cette passerelle est utilisée par l'hôte du Web App Firewall pour envoyer et recevoir du trafic. Pour plus d'informations sur les passerelles Internet, voir : Passerelles Internet.
- 5 tables de routage : une table de routage publique associée aux sous-réseaux clients du Web App Firewall principal et secondaire. Les 4 tables de routage restantes sont liées à chacun des 4 sous-réseaux privés (sous-réseaux de gestion et côté serveur du Web App Firewall principal et secondaire).
- AWS Lambda in Web App Firewall prend en charge les tâches suivantes :
 - Configuration de deux Web App Firewall dans chaque zone de disponibilité du mode HA
 - Création d'un exemple de profil de Web App Firewall et extension de cette configuration par rapport au Web App Firewall
- AWS Identity and Access Management (IAM) pour contrôler en toute sécurité l'accès aux services et ressources AWS pour vos utilisateurs. Par défaut, le modèle CloudFormation (CFT) crée le rôle IAM requis. Les utilisateurs peuvent toutefois fournir leur propre rôle IAM pour les instances NetScaler ADC.
- Dans les sous-réseaux publics, deux passerelles de traduction d'adresses réseau (NAT) gérées permettent l'accès Internet sortant aux ressources des sous-réseaux publics.

Remarque :

Le modèle CFT Web App Firewall qui déploie le NetScaler Web App Firewall dans un VPC existant ignore les composants marqués par des astérisques et invite les utilisateurs à indiquer leur configuration VPC existante.

Les serveurs principaux ne sont pas déployés par le CFT.

Coûts et licences

Les utilisateurs sont responsables du coût des services AWS utilisés lors de l'exécution des déploiements AWS. Les modèles AWS CloudFormation qui peuvent être utilisés pour ce déploiement incluent des paramètres de configuration que les utilisateurs peuvent personnaliser selon les besoins. Certains de ces paramètres, tels que le type d'instance, ont une incidence sur le coût du déploiement. Pour les estimations de coûts, les utilisateurs doivent consulter les pages de tarification de chaque service AWS qu'ils utilisent. Les prix sont sujets à changement.

Un NetScaler Web App Firewall sur AWS nécessite une licence. Pour obtenir une licence NetScaler Web App Firewall, les utilisateurs doivent placer la clé de licence dans un compartiment S3 et spécifier son emplacement lorsqu'ils lancent le déploiement.

Remarque :

Lorsque les utilisateurs choisissent le modèle de licence BYOL (Bring your own license), ils doivent s'assurer qu'une fonctionnalité AppFlow est activée. Pour plus d'informations sur les licences BYOL, consultez : AWS Marketplace/Citrix VPX - Licence client.

Les options de licence suivantes sont disponibles pour Citrix ADC Web App Firewall exécuté sur AWS. Les utilisateurs peuvent choisir une AMI (Amazon Machine Image) en fonction d'un seul facteur, tel que le débit.

- **Modèle de licence** : Pay as You Go (PAYG, pour les licences de production) ou Bring Your Own License (BYOL, pour l'AMI sous licence client - NetScaler ADC Pooled Capacity). Pour plus d' informations sur NetScaler ADC Pooled Capacity, voir : NetScaler ADC Pooled Capacity.
 - Pour BYOL, il existe 3 modes de licence :
 - * Configurer la capacité groupée NetScaler : Configurer la capacité groupée Citrix ADC
 - * Licences d'enregistrement et de retrait NetScaler VPX (CICO) : Licences d'enregistrement et de retrait Citrix ADC VPX

Conseil:

Si les utilisateurs choisissent la licence CICO avec le type de plate-forme d'application VPX-200, VPX-1000, VPX-3000, VPX-5000 ou VPX-8000, ils doivent s'assurer que la licence de débit est la même sur leur serveur de licences NetScaler Console.

* Licence de processeur virtuel NetScaler : Licences de processeur virtuel NetScaler

Remarque :

Si les utilisateurs souhaitent modifier dynamiquement la bande passante d'une instance VPX, ils doivent sélectionner une option BYOL, par exemple la **capacité groupée NetScaler** où ils peuvent allouer les licences depuis NetScaler Console, ou ils peuvent extraire les licences auprès de NetScaler en fonction de la capacité minimale et maximale de l'instance à la demande et sans redémarrage. Un redémarrage n'est requis que si les utilisateurs souhaitent modifier l'édition de la licence.

- Débit : 200 Mbits/s ou 1 Gbit/s
- Offre groupée : Premium

Options de déploiement

Ce guide de déploiement propose deux options de déploiement :

- La première option consiste à déployer à l'aide du format Guide de démarrage rapide et des options suivantes :
 - Déployez NetScaler Web App Firewall dans un nouveau VPC (déploiement de bout en bout). Cette option crée un nouvel environnement AWS composé du VPC, des sousréseaux, des groupes de sécurité et d'autres composants d'infrastructure, puis déploie NetScaler Web App Firewall dans ce nouveau VPC.
 - Déployez NetScaler Web App Firewall dans un VPC existant. Cette option permet de configurer NetScaler Web App Firewall dans l'infrastructure AWS existante de l'utilisateur.
- La deuxième option consiste à déployer à l'aide de Web App Firewall StyleBooks à l'aide de la console NetScaler.

Démarrage rapide AWS

Étape 1 : connectez-vous au compte AWS de l'utilisateur

- Connectez-vous au compte utilisateur sur AWS : AWS avec un rôle utilisateur IAM (Identity and Access Management) qui possède les autorisations nécessaires pour créer un compte Amazon (si nécessaire) ou se connecter à un compte Amazon.
- Utilisez le sélecteur de région dans la barre de navigation pour choisir la région AWS dans laquelle les utilisateurs souhaitent déployer la haute disponibilité dans les zones de disponibilité AWS.
- Assurez-vous que le compte AWS de l'utilisateur est correctement configuré. Reportez-vous à la section Exigences techniques de ce document pour plus d'informations.

Étape 2 : abonnez-vous à l'AMI NetScaler Web App Firewall

- Ce déploiement nécessite un abonnement à l'AMI pour NetScaler Web App Firewall sur AWS Marketplace.
- Connectez-vous au compte AWS de l'utilisateur.

- Ouvrez la page de l'offre NetScaler Web App Firewall en choisissant l'un des liens du tableau suivant.
 - Lorsque les utilisateurs lancent le Guide de démarrage rapide pour déployer NetScaler Web App Firewall à l'étape 3 ci-dessous, ils utilisent le paramètre NetScaler Web App Firewall Image pour sélectionner l'option de bundle et de débit correspondant à leur abonnement AMI. La liste suivante répertorie les options de l'AMI et les paramètres correspondants. L'instance AMI VPX nécessite au moins 2 processeurs virtuels et 2 Go de mémoire.

Remarque:

Pour récupérer l'ID AMI, consultez la page Produits NetScaler sur AWS Marketplace sur GitHub : Produits Citrix sur AWS Marketplace.

- AMI AWS Marketplace
 - NetScaler Web App Firewall (Web App Firewall) 200 Mbit/s : Citrix Web App Firewall (Web App Firewall) 200 Mbit/s
 - NetScaler Web App Firewall (Web App Firewall) 1 000 Mbit/s : Citrix Web App Firewall (Web App Firewall) - 1 000 Mbit/s
- Sur la page AMI, choisissez **Continue to Subscribe**.

🐡 aws n Gelegetes -	harketplace	olutions - Migra	ton Mapping Autistant	Your Saved List		Partners S	C.	Amazon Web Sen	Halls, B Has light
(CİTRIX	Citrix Web / By: Obix Systems, Unav/Unix	App Firewall	l (WAF) - 20 den: 15:0-47:34	0 Mbps		Continuer to 1 Save to Typical Trin \$2.15, Trinal pricing are track heated on mit along o Vegena) View Details	Listscribe List at Price /her not for services in US East (N.	
	overview Product Ove	rview	icing	Utage		Support		Reviews	
	Otrix Web App Firewall (N the art protections for mo public-facing assets, inclu P reputation based filteri protections, Layer 7 00x5 mforce authentication, vi policies. Using beth basic provides competitionale p if use, Getting up and nar automated learning mode procious time. By automat Date WAF adapts to the a speciations. Other WAF he and bodies, including PCI templates, it has rever be	6AF) is an enterprise g dom applications. Cit ding websites, web ap ng, Bot mitigation, Or i protestion and mere roug SSL/TLS ophors, as web as advanced M rotaction for year app ming is a matter of rm i, callud dynamic prof fsally learning how a splication even as de learning internation and learning internation and splication even as de learning internation and splication even as de splication even as	rade solution offering to WAF millipatos the ps, and APIs. Citola W MASP Top 10 applicat Alao included and TLS 13, rate limiting the protections, Citris Kications with unpair Ming, Citris WAF save protected application protected application references display and a to all major regulatos a. With our CountForm	g state of outs against WF includes does to does to gand rowito cWAF disting case an types	Highlights • Comprehensive App powerful ADC platfor claud, physical, vitu enables consistency applications and we security from Layer 3 protection-ensures y vulnerable. • Secure your Website applications is more Citris WW includes 1 reputation based fills	Security Citrix m - a single co al, bare-metal, across your hyt Afbws, Heldol to Layer 7 an to afort, have 1 so afort, have 1 than just basic easis (through a arring, bot mith	WAV is based on the do base across and containers that brid multi cloud c application d built-in APH is werry about being WAV functionality. dearced WAV, IP gation,		

• Passez en revue les termes et conditions d'utilisation du logiciel, puis choisissez **Accepter les termes**.

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (FULA) (2). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the <u>AWS Privacy</u> Notice (2). Your use of AWS services is subject to the <u>AWS Customer Agreement</u> or other agreement with AWS governing your use of such services.

Remarque:

Les utilisateurs reçoivent une page de confirmation et un e-mail de confirmation est envoyé au propriétaire du compte. Pour obtenir des instructions d'abonnement détaillées, consultez Getting Started dans la documentation AWS Marketplace : Getting Started.

 Lorsque le processus d'abonnement est terminé, quittez AWS Marketplace sans autre action. Ne mettez pas en service le logiciel depuis AWS Marketplace. Les utilisateurs déploieront l'AMI à l'aide du guide de démarrage rapide.

Étape 3 : Lancez AWS Quick Start

- Connectez-vous au compte AWS de l'utilisateur et choisissez l'une des options suivantes pour lancer le modèle AWS CloudFormation. Pour obtenir de l'aide sur le choix d'une option, consultez les options de déploiement plus haut dans ce guide.
 - Déployez NetScaler VPX dans un nouveau VPC sur AWS à l'aide de l'un des modèles AWS CloudFormation disponibles ici :
 - * Citrix/Citrix-ADC-AWS-CloudFormation/Modèles/Haute disponibilité/Toutes les zones de disponibilité
 - Citrix/Citrix-ADC-AWS-CloudFormation/Modèles/Haute disponibilité/Zone de disponibilité identique

Important :

Si les utilisateurs déploient NetScaler Web App Firewall sur un VPC existant, ils doivent s'assurer que leur VPC couvre deux zones de disponibilité, avec un sous-réseau public et deux sousréseaux privés dans chaque zone de disponibilité pour les instances de charge de travail, et que les sous-réseaux ne sont pas partagés. Ce guide de déploiement ne prend pas en charge les sousréseaux partagés, voir Working with Shared VPC : Working with Shared VPC. Ces sous-réseaux nécessitent des passerelles NAT dans leurs tables de routage pour permettre aux instances de télécharger des packages et des logiciels sans les exposer à Internet. Pour plus d'informations sur les passerelles NAT, voir Passerelles NAT. Configurez les sous-réseaux afin qu'il n'y ait pas de chevauchement de sous-réseaux.

Accept Terms

De plus, les utilisateurs doivent s'assurer que l'option de nom de domaine dans les options DHCP est configurée comme expliqué dans la documentation Amazon VPC disponible ici : Ensembles d'options DHCP Ensembles d'options DHCP. Les utilisateurs sont invités à entrer leurs paramètres VPC lorsqu' ils lancent le guide de démarrage rapide.

- Chaque déploiement prend environ 15 minutes.
- Vérifiez la région AWS qui s'affiche dans le coin supérieur droit de la barre de navigation et modifiez-la si nécessaire. C'est là que l'infrastructure réseau du Citrix Web App Firewall sera construite. Le modèle est lancé par défaut dans la région USA Est (Ohio).

Remarque :

Ce déploiement inclut NetScaler Web App Firewall, qui n'est actuellement pas pris en charge dans toutes les régions AWS. Pour obtenir la liste actuelle des régions prises en charge, consultez le document AWS Service Endpoints : AWS Service Endpoints.

- Sur la page **Select Template**, conservez le paramètre par défaut pour l'URL du modèle, puis choisissez Next.
- Sur la page Spécifier les détails, spécifiez le nom de la pile selon la commodité de l'utilisateur. Passez en revue les paramètres du modèle. Fournissez des valeurs pour les paramètres qui nécessitent une entrée. Pour tous les autres paramètres, passez en revue les paramètres par défaut et personnalisez-les si nécessaire.
- Dans le tableau suivant, les paramètres sont répertoriés par catégorie et décrits séparément pour l'option de déploiement :
- Paramètres permettant de déployer NetScaler Web App Firewall sur un VPC nouveau ou existant (option de déploiement 1)
- Lorsque les utilisateurs ont fini de vérifier et de personnaliser les paramètres, ils doivent choisir Suivant.

Paramètres pour déployer NetScaler Web App Firewall dans un nouveau VPC

Configuration du réseau VPC

Libellé du paramètre (nom)	Valeur par défaut	Description
Zone de disponibilité principale	Nécessite une saisie	La zone de disponibilité pour le déploiement principal de
(PrimaryAvailabilityZone)		NetScaler Web App Firewall

Libellé du paramètre (nom)	Valeur par défaut	Description
Zone de disponibilité secondaire (SecondaryAvailabilityZone)	Nécessite une saisie	La zone de disponibilité pour le déploiement secondaire de NetScaler Web App Firewall
CIDR VPC (VPCCIDR)	10.0.0/16	Bloc d'adresse CIDR pour le VPC. Il doit s'agir d'une plage d' adresses CIDR IP valide de la forme x.x.x.x/x.
IP CIDR SSH distante (gestion) (RestrictedSSHCIDR)	Nécessite une saisie	Plage d'adresses IP qui peut établir une connexion SSH avec l'instance EC2 (port : 22). Par exemple, l'utilisation de 0.0.0.0/0 permet à toutes les adresses IP d'accéder à l' instance utilisateur via SSH ou RDP. Remarque : Autorisez uniquement une adresse IP ou une plage d'adresses spécifiques pour accéder à l' instance utilisateur, car son utilisation en production n'est pas sûre.
IP CIDR HTTP distante (client) (RestrictedWebAppCidr)	0.0.0/0	La plage d'adresses IP qui peut accéder via HTTP à l'instance EC2 (port : 80)
IP CIDR HTTP distante (client) (RestrictedWebAppCidr)	0.0.0/0	La plage d'adresses IP qui peut accéder via HTTP à l'instance EC2 (port : 80)
CIDR de sous-réseau privé de gestion primaire (PrimaryMan- agementPrivateSubnetCIDR)	10.0.1.0/24	Bloc CIDR pour le sous-réseau de gestion principal situé dans la zone de disponibilité 1.
IP privée de gestion principale (PrimaryManage- mentPrivateIP)		IP privée attribuée à l'ENI de gestion principale (le dernier octet doit être compris entre 5 et 254) à partir du CIDR du sous-réseau de gestion principal.

Libellé du paramètre (nom)	Valeur par défaut	Description
CIDR de sous-réseau public du client principal (Prima- ryClientPublicSubnetCIDR) IP privée du client principal	10.0.2.0/24	Bloc d'adresse CIDR pour le sous-réseau du client principal situé dans la zone de disponibilité 1. IP privée attribuée à l'ENI du
(PrimaryClientPrivateIP)		client principal (le dernier octet doit être compris entre 5 et 254) à partir de l'adresse IP du client principal à partir de l'adresse CIDR du sous-réseau du client principal.
CIDR de sous-réseau privé du serveur principal (Primary- ServerPrivateSubnetCIDR)	10.0.3.0/24	Bloc d'adresse CIDR pour le serveur principal situé dans la zone de disponibilité 1.
IP privée du serveur principal (PrimaryServerPrivateIP)	_	IP privée attribuée à l'ENI du serveur primaire (le dernier octet doit être compris entre 5 et 254) à partir de l'adresse CIDR du sous-réseau du serveur primaire.
CIDR de sous-réseau privé de gestion secondaire (SecondaryManagementPri- vateSubnetCIDR)	10.0.4.0/24	Bloc CIDR pour le sous-réseau de gestion secondaire situé dans la zone de disponibilité 2.
IP privée de gestion secondaire (SecondaryMan- agementPrivateIP)		IP privée attribuée à l'ENI de gestion secondaire (le dernier octet doit être compris entre 5 et 254). Il allouerait une adresse IP de gestion secondaire à partir du CIDR du sous-réseau de gestion secondaire.
CIDR de sous-réseau public du client secondaire (SecondaryClientPublicSubnet- CIDR)	10.0.5.0/24	Bloc d'adresse CIDR pour le sous-réseau client secondaire situé dans la zone de disponibilité 2.

Libellé du paramètre (nom)	Valeur par défaut	Description
IP privée du client secondaire (SecondaryClientPrivateIP)		IP privée attribuée à l'ENI du client secondaire (le dernier octet doit être compris entre 5 et 254). Il allouerait l'adresse IP du client secondaire à partir du CIDR du sous-réseau du client secondaire.
CIDR de sous-réseau privé du serveur secondaire (SecondaryServerPrivateSub- netCIDR)	10.0.6.0/24	Bloc CIDR pour le sous-réseau du serveur secondaire situé dans la zone de disponibilité 2.
IP privée du serveur secondaire (SecondaryServerPrivateIP)		IP privée attribuée à l'ENI du serveur secondaire (le dernier octet doit être compris entre 5 et 254). Il allouerait l'adresse IP du serveur secondaire à partir du CIDR du sous-réseau du serveur secondaire
Attribut de location de VPC (VPCTenancy)	default	Location autorisée des instances lancées dans le VPC. Choisissez Dedicated tenancy pour lancer des instances EC2 dédiées à un seul client.

Configuration de l'hôte Bastion

Libellé du paramètre (nom)	Valeur par défaut	Description
Hôte Bastion requis	Non	Par défaut, aucun hôte bastion
(LinuxBastionHosteIP)		n'est configuré. Mais si les
		utilisateurs souhaitent opter
		pour le déploiement en
		sandbox, sélectionnez oui dans
		le menu, ce qui permettrait de
		déployer un hôte bastion
		Linux dans le sous-réseau
		public avec une EIP qui
		permettrait aux utilisateurs d'
		accéder aux composants du
		sous-réseau privé et public.

Configuration de NetScaler Web App Firewall

Libellé du paramètre (nom)	Valeur par défaut	Description
Nom de la paire de clés	Nécessite une saisie	Une paire de clés
(KeyPairName)		publique/privée, qui permet
		aux utilisateurs de se connecter
		en toute sécurité à l'instance
		utilisateur après son
		lancement. Il s'agit de la paire
		de clés créée par les
		utilisateurs dans leur région
		AWS préférée ; consultez la
		section Exigences techniques.
Type d'instance NetScaler	m4.xlarge	Type d'instance EC2 à utiliser
(CitrixADCInstanceType)		pour les instances ADC.
		Assurez-vous que le type d'
		instance choisi correspond aux
		types d'instances disponibles
		sur AWS Marketplace, sinon le
		CFT risque d'échouer.

Libellé du paramètre (nom)	Valeur par défaut	Description
ID d'AMI NetScaler ADC (CitrixADCImageID)		L'AMI AWS Marketplace à utiliser pour le déploiement de NetScaler Web App Firewall. Cela doit correspondre aux utilisateurs de l'AMI auxquels ils sont abonnés à l'étape 2.
Rôle IAM NetScaler ADC VPX (iam:GetRole)		Ce modèle : AWS-QuickStart/QuickStart- Citrix-ADC-VPX/Templates crée le rôle IAM et le profil d' instance requis pour NetScaler VPX . S'il est laissé vide, CFT crée le rôle IAM requis.
IP publique du client (EIP) (ClientPublicEIP)	Non	Sélectionnez « Oui » si les utilisateurs souhaitent attribuer une adresse IP publique à l'interface réseau client utilisateur. Sinon, même après le déploiement, les utilisateurs ont toujours la possibilité de l'attribuer ultérieurement si nécessaire.

Configuration des licences groupées

Libellé du paramètre (nom)	Valeur par défaut	Description
Licences groupées de la console NetScaler	Non	Si vous choisissez l'option BYOL pour les licences, sélectionnez Oui dans la liste. Cela permet aux utilisateurs de télécharger leurs licences déjà achetées. Avant de commencer, les utilisateurs doivent configurer la capacité groupée NetScaler ADC pour garantir la disponibilité des licences groupées NetScaler Console. Reportez-vous à la section Configurer la capacité groupée NetScaler ADC
Adresse IP de la console NetScaler ou de l'agent de la console NetScaler accessible	Nécessite une saisie	Pour l'option Licence client, que les utilisateurs déploient NetScaler Console sur site ou un agent dans le cloud, assurez-vous de disposer d'une adresse IP de la console NetScaler accessible qui sera ensuite utilisée comme paramètre d'entrée. Les utilisateurs peuvent choisir
Mode de licence	Facultatif	parmi les 3 modes de licence Configurez la capacité groupée de NetScaler. Pour plus d' informations, voir Configurer la
Bande passante de licence en Mbps	0 Mbits/s	capacité groupée Citrix ADC Ce champ apparait Licence d'enregistrement et de uniquement si le mode de départ NetScaler VPX (CICO) licence est Pooled-Licensing. II Pour plus d'informations, alloue une bande passante consultez la section Licences d' initiale de la licence en Mbps a enregistrement et de départ allouer après la creation des Citrix ADC VPX ADC BYOL. Il doit être un Licence de processeur virtuel multiple de 10 Mbps. NetScaler. Pour plus d' informations, consultez la section Licences de processeurs virtuels Citrix ADC

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Libellé du paramètre (nom)	Valeur par défaut	Description
Édition de licence	Premium	L'édition de licence pour le mode de licence à capacité groupée est Premium .
Type de plate-forme d' appliance	Facultatif	Choisissez le type de plate-forme d'appliance requis, uniquement si les utilisateurs optent pour le mode de licence CICO. Les utilisateurs obtiennent les options répertoriées : VPX-200, VPX-1000, VPX-3000, VPX-5000,
Édition de licence	Premium	L'édition de licence pour les licences basées sur un processeur virtuel est Premium .

Configuration d'AWS Quick Start

Remarque:

Nous recommandons aux utilisateurs de conserver les paramètres par défaut pour les deux paramètres suivants, sauf s'ils personnalisent les modèles du Guide de démarrage rapide pour leurs propres projets de déploiement. La modification des paramètres de ces paramètres met automatiquement à jour les références de code pour pointer vers un nouvel emplacement du guide de démarrage rapide. Pour plus de détails, consultez le guide de démarrage rapide AWS Contributor's Guide situé ici : AWS Quick Starts/Option 1 - Adopt a Quick Start.

Libellé du paramètre (nom)	Valeur par défaut	Description
Guide de démarrage	aws-quickstart	Les utilisateurs du
rapide Nom du		compartiment S3 créés pour
compartiment S3		leur copie des ressources du
(QSS3BucketName)		guide de démarrage rapide, si
		les utilisateurs décident de
		personnaliser ou d'étendre le
		guide de démarrage rapide
		pour leur propre usage. Le nom
		du compartiment peut inclure
		des chiffres, des lettres
		minuscules, des lettres
		majuscules et des traits d'
		union, mais ne doit pas
		commencer ni se terminer par
		un trait d'union.
Guide de démarrage rapide	démarrage rapide	Le préfixe de nom de clé S3,
Préfixe de clé S3	citrix-adc-vpx/	issu de la clé d'objet et
(QSS3KeyPrefix)		métadonnées : clé d'objet et
		métadonnées, est utilisé pour
		simuler un dossier pour la
		copie utilisateur des ressources
		du Guide de démarrage rapide,
		si les utilisateurs décident de
		personnaliser ou d'étendre le
		guide de démarrage rapide
		pour leur propre usage. Ce
		préfixe peut inclure des chiffres,
		des lettres minuscules, des
		lettres majuscules, des traits d'
		union et des barres obliques.

- Sur la page **Options**, les utilisateurs peuvent spécifier une balise de ressource ou une paire clévaleur pour les ressources de votre pile et définir des options avancées. Pour plus d'informations sur les balises de ressources, voir Balise de ressource. Pour plus d'informations sur la définition des options de la pile AWS CloudFormation, consultez Définition des options de la pile AWS CloudFormation. Lorsque les utilisateurs ont terminé, ils doivent choisir Next.
- Sur la page Révision, vérifiez et confirmez les paramètres du modèle. Sous Capabilities, cochez

les deux cases pour confirmer que le modèle crée des ressources IAM et qu'il peut nécessiter la capacité de développer automatiquement des macros.

- Choisissez Create pour déployer la pile.
- Surveillez l'état de la pile. Lorsque l'état est **CREATE_COMPLETE**, l'instance de NetScaler Web App Firewall est prête.
- Utilisez les URL affichées dans l'onglet **Sorties** de la pile pour afficher les ressources qui ont été créées.

Ondformation > Stads > quidotart-ant-b				
🗉 Stacks (1) 🛛 🔿	Stack info Events Resources	Outputs Parameters	Template Change sets	
Q, Filter by stack name				
Active: # CB View nested	Outputs (16)			σ
Quidatari waf-ik 2020-05-04 TSATUT UTC-0030 © CRAFE, COMPLETE	Q, Search acquits			•
	Key A	Value v	Description v	Export name 14
	CientiecurityGroupID	sg-0056eh123c9c5a264	Security group ID for client ADC DNs	
	ManagementSecurityGroupID	sg-08c5c20e6a382206d	Security group ID-for management ADC DNs	
	PrimaryA0Omtanoe0	1-068041197285x5084	Primary ADC instance ID	
	PrimaryClentPrivateVP	10.0.2.118	Primary Client private VIP	
	PrimaryClientPublicSubnetID	subret-025745e2b66d13d59	Primary Client public subret ID	
	PrimaryManagementPrivatehSiP	10.0.1.149	Primary Management private NSIP	
	PrimaryManagementPrivateGubnetD	subret-0810b54%x9925813	Primary Management private subnet ID	
	PrimaryServerHivataSubnetID	subnet-071057012154ec15c	Primary Server private subnet ID	
	SecondaryADCristanceID	10030495793845394	Secondary ADC instance ID	
	SecondaryClientPrivate/IIP	10.8.5.231	Secondary Client private VIP	
	SecondaryClientPublicSubnetD	subret-07941cd7905840aec	Secondary Client public subnet 10	
	SecondaryManagementPrivateNSIP	10.0.4.213	Secondary Management private NSIP	
	SecondaryManagementPrivateSubnetD	subret-00x82966625/548x22	Secondary Management private subnet: D	
	SecondaryServerPrivateSubnetID	subnet-030018e83538h4453	Secondary Server private subnet ID	
	ServerSecurityGroup@	sg-0s?##Msea%iSecd?	Security group 10 for server ADC ENIs	
	VPOD	vpc-06a7vb/bul0425/fbb	VPCID	

Étape 4 : tester le déploiement

Dans ce déploiement, nous appelons les instances **principales** et **secondaires**. Chaque instance possède des adresses IP différentes qui lui sont associées. Une fois le Quick Start déployé avec succès, le trafic passe par l'instance principale de NetScaler Web App Firewall configurée dans la zone de disponibilité 1. En cas de basculement, lorsque l'instance principale ne répond pas aux demandes des clients, l'instance secondaire du Web App Firewall prend le relais.

L'adresse IP Elastic de l'adresse IP virtuelle de l'instance principale migre vers l'instance secondaire, qui prend le relais en tant que nouvelle instance principale.

Lors du processus de basculement, NetScaler Web App Firewall effectue les opérations suivantes :

- NetScaler Web App Firewall vérifie les serveurs virtuels auxquels sont associés des ensembles d'adresses IP.
- NetScaler Web App Firewall trouve l'adresse IP à laquelle est associée une adresse IP publique parmi les deux adresses IP écoutées par le serveur virtuel. L'un qui est directement connecté au serveur virtuel et l'autre qui est connecté via l'ensemble d'adresses IP.
- NetScaler Web App Firewall associe l'adresse IP Elastic publique à l'adresse IP privée qui appartient à la nouvelle adresse IP virtuelle principale.

Pour valider le déploiement, effectuez les opérations suivantes :

• Connectez-vous à l'instance principale

Par exemple, avec un serveur proxy, un hôte de saut (une instance Linux/Windows/FW exécutée dans AWS, ou l'hôte Bastion), ou un autre appareil accessible à ce VPC ou Direct Connect s'il s'agit d'une connectivité sur site.

• Exécutez une action de déclenchement pour forcer le basculement et vérifier si l'instance secondaire prend le relais.

Conseil:

Pour valider davantage la configuration par rapport à NetScaler Web App Firewall, exécutez la commande suivante après vous être connecté à l'**instance principale de NetScaler Web App Firewall** :

Sh appfw profile QS-Profile

Connectez-vous à la paire NetScaler Web App Firewall HA à l'aide de l'hôte Bastion

Si les utilisateurs optent pour le déploiement Sandbox (par exemple, dans le cadre de CFT, les utilisateurs choisissent de configurer un hôte Bastion), un hôte Bastion Linux déployé dans un sous-réseau public sera configuré pour accéder aux interfaces du Web App Firewall.

Dans la console AWS CloudFormation, accessible en vous connectant ici : Connectez-vous, choisissez la pile principale et, dans l'onglet **Outputs**, recherchez la valeur de **LinuxBastionHosteIP1**.

Outputs (17)		
Q. Search autputs		
Key 🔺	Value	♥ Description
InstanceProfileName	tCaT-tag-cltrix-adc-master-10599535 WorkLoadStack-GZX61DAOP4J- IAMRoleStack-36JSFNFGO22N- CitrixNodesProfile-7R84KI62FPA3	9- Instance Profile for ADCs
LinuxBastionHostEIP1	3.124.177.42	Elastic IP 1 for Bastion
PrimaryADCInstanceID	I-09956d309fe8f4752	Primary ADC Instance ID
PrimaryClientPrivateVIP	10.0.2.203	Primary Client Private VIP
PrimaryClientPublicEIP	18.195.151.157	Primary Client Public EIP
PrimaryClientPublicSubnetID	subnet-04c7c93c8f0e12d5e	Primary Client Public Subnet ID
PrimaryManagementPrivateNSIP	10.0.1.91	Primary Management Private NSIP

- Valeur des clés**PrivateManagementPrivateNSIPet PrimaryADCINstanceID** à utiliser dans les étapes ultérieures pour SSH dans l'ADC.
- Choisissez Services.
- Dans l'onglet **Calcul**, sélectionnez **EC2**.
 - Sous Resources, choisissez Running Instances.
 - Dans l'onglet **Description** de l'instance principale du Web App Firewall, notez l'adresse
 IP publique IPv4. Les utilisateurs ont besoin de cette adresse IP pour créer la commande
 SSH.

tost-tag-cit	rix-ado-master-eu-ce	ntral-1-97a6acc9-	VorkLoad	Stack-XY-SecondaryADCh	nstance-NV30OQYJ9DBJ Sec	ondary	i-0d671adb473d1d7	m4.xlarge
stance: I-07 005VH2MRA	197878fc2cafaed (WG Primary) E	(tcat-tag-citrix-a lastic IP: 3.122.1	dc-mast 41.245	er-eu-central-1-97a6ac	c9-WorkLoadStack-XYC4-	PrimaryA	OCInstance-	880
escription	Status Checks	Monitoring	Tags	Usage Instructions				
	Instance ID	i-07197878fc2ce	feed		Public DNS (IPv4)			
	Instance state	running			IPv4 Public IP	3.122.141	245	
	Instance type	m4.xlarge			IP-6 IPs			
	Eastic IPs	3.122.141.246*			Private CNS	ip-10-0-1- 1.compute	61.eu-central- s.internal	
	Availability zone	eu-central-1a			Private IPs	10.0.3.104	, 10.0.1.81, 10.0.2.23	
	Security groups	tost-tag-citrix-ad 1-97a6acc9-Wor	ic-master kLoadSta	eu-central- ck-XYC4-	Secondary private IPs			

 Pour enregistrer la clé dans le trousseau de l'utilisateur, exécutez la commande ssh-add -K [your-key-pair].pem Sous Linux, les utilisateurs peuvent avoir besoin d'omettre l'indicateur -K.

• Connectez-vous à l'hôte bastion à l'aide de la commande suivante, en utilisant la valeur pour **LinuxBastionHostelP1** que les utilisateurs ont notée à l'étape 1.

```
ssh -A ubuntu@[LinuxBastionHostEIP1]
```

• À partir de l'hôte bastion, les utilisateurs peuvent se connecter à l'instance principale du Web App Firewall à l'aide de SSH.

```
ssh nsroot@[Primary Management Private NSIP]
```

Mot de passe : [ID de l'instance ADC principale]

```
[ubuntu@ip-10-0-5-243:~$ ssh nsroot@10.0.1.91
ž
                                                  #
#
      WARNING: Access to this system is for authorized users only
                                                  #
      Disconnect IMMEDIATELY if you are not an authorized user!
ø
                                                  #
                                                  #
#
********
Last login: Thu Oct 31 19:31:49 2019 from 10.0.5.243
Done
>
```

Les utilisateurs sont désormais connectés à l'instance principale de NetScaler Web App Firewall. Pour voir les commandes disponibles, les utilisateurs peuvent exécuter la commande help. Pour afficher la configuration HA actuelle, les utilisateurs peuvent exécuter la commande show HA node.

Console NetScaler

NetScaler Application Delivery Management Service fournit une solution simple et évolutive pour gérer les déploiements NetScaler, notamment NetScaler MPX, NetScaler VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler SDX, NetScaler ADC CPX et appliances NetScaler SD-WAN déployées sur site ou dans le cloud.

La documentation du service NetScaler Console inclut des informations sur la façon de démarrer avec le service, une liste des fonctionnalités prises en charge par le service et la configuration spécifique à cette solution de service.

Pour plus d'informations, consultez la section Présentation de la console NetScaler.

Déploiement d'instances NetScaler VPX sur AWS à l'aide de NetScaler Console

Lorsque les clients déplacent leurs applications vers le cloud, les composants qui font partie de leur application augmentent, sont plus distribués et doivent être gérés de manière dynamique.

Pour plus d'informations, consultez Provisioning d'instances NetScaler VPX sur AWS.

Top 10 de NetScaler Web App Firewall et OWASP -2017

L'Open Web Application Security Project : OWASP a publié le Top 10 OWASP pour 2017 en matière de sécurité des applications Web. Cette liste répertorie les vulnérabilités les plus courantes des applications Web et constitue un excellent point de départ pour évaluer la sécurité Web. Nous expliquons ici comment configurer le NetScaler Web App Firewall (Web App Firewall) pour atténuer ces failles. Le Web App Firewall est disponible en tant que module intégré dans NetScaler (Premium Edition) ainsi que dans une gamme complète d'appliances.

L'intégralité du document OWASP Top 10 est disponible à l'adresse suivante : OWASP Top Ten.

Les signatures fournissent les options de déploiement suivantes pour aider les utilisateurs à optimiser la protection des applications utilisateur :

- Modèle de sécurité négatif : avec le modèle de sécurité négatif, les utilisateurs utilisent un ensemble complet de règles de signature préconfigurées pour appliquer la puissance de la correspondance de modèles afin de détecter les attaques et de se protéger contre les vulnérabilités des applications. Les utilisateurs bloquent uniquement ce qu'ils ne veulent pas et autorisent le reste. Les utilisateurs peuvent ajouter leurs propres règles de signature, en fonction des besoins de sécurité spécifiques des applications utilisateur, afin de concevoir leurs propres solutions de sécurité personnalisées.
- Modèle de sécurité hybride : Outre l'utilisation de signatures, les utilisateurs peuvent utiliser des contrôles de sécurité positifs pour créer une configuration parfaitement adaptée aux applications utilisateur. Utilisez des signatures pour bloquer ce que les utilisateurs ne veulent pas, et utilisez des contrôles de sécurité positifs pour appliquer ce qui est autorisé.

Pour protéger les applications utilisateur à l'aide de signatures, les utilisateurs doivent configurer un ou plusieurs profils afin d'utiliser leur objet de signatures. Dans une configuration de sécurité hybride, les modèles d'injection SQL et de script intersite, ainsi que les règles de transformation SQL, dans l' objet signatures utilisateur sont utilisés non seulement par les règles de signature, mais également par les contrôles de sécurité positifs configurés dans le profil Web Application Firewall qui utilise le objet signatures.

Le Web Application Firewall examine le trafic vers les sites Web et les services Web protégés par l'utilisateur afin de détecter le trafic correspondant à une signature. Une correspondance n'est déclenchée que lorsque chaque motif de la règle correspond au trafic. Lorsqu'une correspondance se produit, les actions spécifiées pour la règle sont appelées. Les utilisateurs peuvent afficher une page d'erreur ou un objet d'erreur lorsqu'une demande est bloquée. Les messages de journal peuvent aider les utilisateurs à identifier les attaques lancées contre les applications des utilisateurs. Si les utilisateurs activent les statistiques, le Web Application Firewall conserve les données relatives aux demandes qui correspondent à une signature ou à un contrôle de sécurité du Web Application Firewall.

Si le trafic correspond à la fois à une signature et à un contrôle de sécurité positif, la plus restrictive

des deux actions est appliquée. Par exemple, si une demande correspond à une règle de signature pour laquelle l'action de blocage est désactivée, mais que la demande correspond également à une vérification de sécurité positive SQL Injection pour laquelle l'action est bloquée, la demande est bloquée. Dans ce cas, la violation de signature peut être enregistrée comme [non bloquée], bien que la demande soit bloquée par le contrôle d'injection SQL.

Personnalisation : si nécessaire, les utilisateurs peuvent ajouter leurs propres règles à un objet de signatures. Les utilisateurs peuvent également personnaliser les modèles SQL/XSS. La possibilité d' ajouter leurs propres règles de signature, en fonction des besoins de sécurité spécifiques des applications utilisateur, permet aux utilisateurs de concevoir leurs propres solutions de sécurité personnalisées. Les utilisateurs bloquent uniquement ce qu'ils ne veulent pas et autorisent le reste. Un modèle de correspondance rapide spécifique à un emplacement spécifique peut réduire considérablement les frais de traitement afin d'optimiser les performances. Les utilisateurs peuvent ajouter, modifier ou supprimer des modèles d'injection SQL et de script intersite. Les éditeurs d'expressions régulières et d'expressions intégrés aident les utilisateurs à configurer des modèles utilisateur et à vérifier leur exactitude.

Web App Firewall NetScaler

Web App Firewall est une solution destinée aux entreprises qui offre des protections de pointe pour les applications modernes. NetScaler Web App Firewall atténue les menaces qui pèsent sur les actifs destinés au public, notamment les sites Web, les applications Web et les API. NetScaler Web App Firewall inclut le filtrage basé sur la réputation IP, l'atténuation des bots, la protection contre les 10 principales menaces applicatives de l'OWASP, la protection DDoS de couche 7 et bien plus encore. Sont également incluses des options pour appliquer l'authentification, des chiffrements SSL/TLS forts, TLS 1.3, la limitation du débit et des stratégies de réécriture. En utilisant à la fois des protections de base et avancées du Web App Firewall, NetScaler Web App Firewall fournit une protection complète à vos applications avec une facilité d'utilisation inégalée. Se lever et courir ne prend que quelques minutes. En outre, grâce à un modèle d'apprentissage automatisé, appelé profilage dynamique, NetScaler Web App Firewall permet aux utilisateurs de gagner un temps précieux. En apprenant automatiquement le fonctionnement d'une application protégée, le Web App Firewall s'adapte à l'application même lorsque les développeurs déploient et modifient les applications. NetScaler Web App Firewall contribue à la conformité à toutes les principales normes et organismes réglementaires, notamment les normes PCI-DSS, HIPAA, etc. Avec nos modèles CloudFormation, il n'a jamais été aussi facile d'être rapidement opérationnel. Grâce à la mise à l'échelle automatique, les utilisateurs peuvent être assurés que leurs applications restent protégées même lorsque leur trafic augmente.

Stratégie de déploiement du Web App Firewall

La première étape du déploiement du pare-feu d'application Web consiste à évaluer quelles applications ou données spécifiques nécessitent une protection de sécurité maximale, celles qui sont moins vulnérables et celles pour lesquelles l'inspection de sécurité peut être contournée en toute sécurité. Cela aide les utilisateurs à établir une configuration optimale et à concevoir des stratégies et des points de liaison appropriés pour séparer le trafic. Par exemple, les utilisateurs peuvent vouloir configurer une stratégie pour contourner l'inspection de sécurité des demandes de contenu Web statique, tels que des images, des fichiers MP3 et des films, et configurer une autre stratégie pour appliquer des contrôles de sécurité avancés aux demandes de contenu dynamique. Les utilisateurs peuvent utiliser plusieurs stratégies et profils pour protéger différents contenus d'une même application.

L'étape suivante consiste à référencer le déploiement. Commencez par créer un serveur virtuel et testez le trafic via celui-ci pour avoir une idée du débit et de la quantité de trafic circulant dans le système utilisateur.

Déployez ensuite le Web App Firewall. Utilisez la console NetScaler et Web App Firewall StyleBook pour configurer Web App Firewall. Consultez la section StyleBook ci-dessous dans ce guide pour plus de détails.

Une fois le Web App Firewall déployé et configuré à l'aide de Web App Firewall StyleBook, une prochaine étape utile serait d'implémenter NetScaler ADC Web App Firewall et l'OWASP Top 10.

Enfin, trois des protections du Web App Firewall sont particulièrement efficaces contre les types courants d'attaques Web et sont donc plus couramment utilisées que toutes les autres. Ils doivent donc être mis en œuvre lors du déploiement initial.

Console NetScaler

La console NetScaler fournit une solution évolutive pour gérer les déploiements NetScaler ADC, notamment NetScaler ADC MPX, NetScaler ADC VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler ADC SDX, NetScaler ADC SDX Appliances ADC CPX et NetScaler SD-WAN déployées sur site ou dans le cloud.

Fonctionnalités d'analyse et de gestion des applications de la console NetScaler

Les fonctionnalités prises en charge sur la console NetScaler sont essentielles au rôle de la console NetScaler dans App Security.

Pour plus d'informations sur les fonctionnalités, consultez la section Fonctionnalités et solutions.

Conditions préalables

Avant de tenter de créer une instance VPX dans AWS, les utilisateurs doivent s'assurer que les prérequis sont remplis. Pour plus d'informations, voir Prérequis:

Limitations et directives d'utilisation

Les limitations et les directives d'utilisation disponibles sur Les limitations et les directives d'utilisation s'appliquent lors du déploiement d'une instance Citrix ADC VPX sur AWS.

Exigences techniques

Avant que les utilisateurs ne lancent le Guide de démarrage rapide pour commencer un déploiement, le compte utilisateur doit être configuré comme indiqué dans le tableau de ressources suivant. Dans le cas contraire, le déploiement peut échouer.

Ressources

Si nécessaire, connectez-vous au compte utilisateur Amazon et demandez une augmentation de la limite de service pour les ressources suivantes ici : AWS/Sign in. Cela peut être nécessaire si vous disposez déjà d'un déploiement utilisant ces ressources et que vous pensez que vous pourriez dépasser les limites par défaut avec ce déploiement. Pour connaître les limites par défaut, consultez les quotas de service AWS dans la documentation AWS : AWS Service Quotas.

AWS Trusted Advisor, disponible ici : AWS/Sign in, propose une vérification des limites de service qui affiche l'utilisation et les limites pour certains aspects de certains services.

Ressource	Ce déploiement utilise		
VPC	1		
Adresses IP Elastic	0/1 (pour l'hôte Bastion)		
Groupes de sécurité IAM	3		
Rôles IAM	1		
Sous-réseaux	6 (3/zone de disponibilité)		
Passerelle Internet	1		
Tables de routage	5		
Instances VPX du Web App Firewall	2		

Ressource	Ce déploiement utilise
Hôte Bastion	0/1
Passerelle NAT	2

Régions

NetScaler Web App Firewall sur AWS n'est actuellement pas pris en charge dans toutes les régions AWS. Pour obtenir la liste actuelle des régions prises en charge, consultez AWS Service Endpoints dans la documentation AWS : AWS Service Endpoints.

Pour plus d'informations sur les régions AWS et l'importance de l'infrastructure cloud, consultez : Global Infrastructure.

Paire de clés

Assurez-vous qu'au moins une paire de clés Amazon EC2 existe dans le compte AWS de l'utilisateur dans la région où les utilisateurs prévoient de déployer à l'aide du guide de démarrage rapide. Notez le nom de la paire de clés. Les utilisateurs sont invités à fournir ces informations lors du déploiement. Pour créer une paire de clés, suivez les instructions relatives aux paires de clés Amazon EC2 et aux instances Linux dans la documentation AWS : Amazon EC2 Key Pairs and Linux Instances.

Si les utilisateurs déploient le guide de démarrage rapide à des fins de test ou de validation de principe, nous leur recommandons de créer une nouvelle paire de clés au lieu de spécifier une paire de clés déjà utilisée par une instance de production.

Références

- Contrôle d'injection HTML SQL
- Vérification de l'injection XML SQL
- Utilisation de la ligne de commande pour configurer la vérification des scripts intersites HTML
- Vérification des scripts intersites XML
- Utilisation de la ligne de commande pour configurer le contrôle de sécurité en cas de dépassement de la mémoire tampon
- Ajouter ou supprimer un objet de signature
- Configuration ou modification d'un objet Signatures
- Mettre à jour un objet de signature

- Intégration de règles Snort
- Détection de bot
- Déployer une instance NetScaler VPX sur Microsoft Azure

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.
> sho	w interface	summary		
	Interface	MTU	мас	Suffix
1	1/1	1500	Øa:1e:2e:17:a2:37	Intel 82599 10G VF Interface
2 Done	L0/1	1500	Øa:1e:2e:17:a2:37	Netscaler Loopback interface

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 2 Done >	1/1 L0/1	1500 1500	12:fc:04:c5:d0:12 12:fc:04:c5:d0:12	NetScaler Virtual Interface Netscaler Loopback interface

Pour plus d'informations sur la modification du type d'interface en SR-IOV, voir http://docs.aws.ama zon.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 \\<instance
\\_id\\> --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 \\<
instance\\_id\\> --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.

	Interface	MTU	MAC	Suffix
1	10/1	1500	Øa: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
8	10/3	1500	Øa:de:5d:31:bf:c3	Intel 82599 10G VF Interface
4	L0/1	1500	Øa:1e:2e:17:a2:37	Netscaler Loopback interface

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-adcami-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 ns root 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 :

1 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>

Parexemple, 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)?
	γ

 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 302Done3> save config4Done
```

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.

Q Search in Menu		System / System Information	
AWS	>	System	
System	\sim		
Licenses		System Information System Sessions 1 System Network	
Settings		System Upgrade Reboot Migration Statistics Call Home	
Diagnostics			
High Availability	>	System Information	
NTP Servers		Citrix ADC IP Address	
Reports		Netmask	
Profiles		Node Star	ndalone
Partition Administration	>	Time Zone Coo	ordinated Universal Time
User Administration	>	System Time Web	d, 18 Dec 2019 06:16:59 UTC
Authentication	>	Last Config Changed Time Wec	d, 18 Dec 2019 06:16:40 UTC
Auditing	>	Last Config Saved Time Wee	d, 18 Dec 2019 05:41:16 UTC
SNMP	>	Hardware Information	
AppFlow	(!) >	Distorm Net	tScalor Virtual Appliance 450040
Cluster	>	Manufactured on 2/13	7/2009
Network	>	CPU 230	IS MHZ
Web Interface	>	Host Id	
WebFront	>	Serial no Encoded serial no	
Backup and Restore		Citrix ADC UUID	
Encryption Keys			

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, devonsnous 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 sousréseau dans AWS, comme dans le cas d'un déploiement de deux cartes réseau sur un sousréseau. 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

March 20, 2025

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.

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 valide. Les options de licence disponibles pour les instances NetScaler VPX exécutées sur Azure sont les suivantes :

- Apportez votre propre permis (BYOL): Pour utiliser l'option BYOL, procédez comme suit :
 - Utilisez le portail de licences sur le site Web de NetScaler pour générer une licence valide.
 - Téléchargez la licence générée dans l'instance.
- NetScaler VPX Check-in et Check-out de licence: Ce modèle de licence vous permet d'extraire une licence d'un pool de licences disponibles et de la réarchiver lorsqu'elle n'est plus nécessaire. Pour plus d'informations et des instructions détaillées, consultez Enregistrement et extraction de la licence NetScaler VPX.

Remarque :

- Les licences basées sur un abonnement ne sont plus prises en charge pour les instances NetScaler VPX sur Azure.
- Effectuez un redémarrage à chaud avant d'apporter des modifications de configuration sur l'instance NetScaler VPX afin d'activer la licence NetScaler VPX correcte.

Performances VPX et types d'instances Azure recommandés

Pour obtenir les performances VPX souhaitées, les types d'instances Azure suivants sont recommandés.

Performan	ce <u>s</u>	L	
VPX	Carte	istances Azur	re
	réseau		VPX
	VPX 1/2	Carte	jusqu'à 8
	cartes	réseau	cartes
	réseau	VPX 3	réseau
Jusqu'à 200 Mbits/s	Standard _.	_D2\$ <u>t</u> aı5dard_	_D8 bl_orb ne_D16_v5
Jusqu'à 1 Gbit/s	Standard <u>.</u>	_D4§ <u>t</u> an5dard_	_D8 blorb ne_D16_v5
Jusqu'à 5 Gbit/s	Standard <u>.</u>	_D8 Sits<u>a</u>nvd5 ard_	_D8 Silsa_nv5 fard_DS <u>Silta</u> n2dard_D8Silsa_nv55ard_D8Silsa_nv55ard_DS14o_v12ne_D16_v1
Jusqu'à	Standard	_D8 S<u>t</u>an5 dard	_D8 blov5 ne_D16_v5
10 Gbit/s			

Points à noter

- Azure prend en charge un débit VPX jusqu'à 10 Gbit/s. Pour plus d'informations, consultez la fiche technique de NetScaler VPX.
- Pour obtenir des performances optimales sur les instances NetScaler VPX avec un débit supérieur à 1 Gbit/s, vous devez activer la mise en réseau accélérée Azure. À cette fin, il est recommandé d'utiliser un type d'instance Azure qui prend en charge la mise en réseau accélérée. 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.
- 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.
- 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.

Support IPv6 pour l'instance NetScaler VPX dans Azure

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

- 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.

Terminologie Azure

October 17, 2024

Certains des termes Azure utilisés dans la documentation Azure de NetScaler VPX sont répertoriés ci-dessous.

- 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.
- 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 instances 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

January 15, 2025

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**.

See all
es in an
y
ry itions
of your irces
ex

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**.

≡ + New	New Search the marketplace	_ 🗆 ×	Networking	_ D X	Virtual Ne Microsoft	etwork
Resource groupsAll resources	MARKETPLACE		FEATURED APPS	See all	Create a logically isolated section	n in Microsoft Azure w
C Recent	Virtual Machines Web + Mobile		Virtual Network Create a logically isol Microsoft Azure and connect it outward.	lated section in securely	connect it to your on-premises Virtual Networks make it easy fo Azure while providing connectiv on Windows Server, mainframes	datacenter or a single or you to take advantag vity to data and applica s, and UNIX.
SQL databases	Data + Storage Data + Analytics		Traffic Manager pr Create a Microsoft Az Manager Profile that	rofile zure Traffic allows you to	Use Virtual Network to: • Extend your datacenter • Build distributed applica	tions
 Virtual machines (classic) Virtual machines 	Internet of Things Networking	> >	control the distributio	on of user	Remotely debug your ap f in y ^c 8 ^c	oplications
Cloud services (classic) Subscriptions	Media + CDN Hybrid Integration		Experience a faster, p connection to Micros	orivate soft Azure.	PUBLISHER	Microsoft
Browse >	Security + Identity Developer Services		Virtual network ga The VPN device in yo network and used wit and VNet-to-VNet VR	nteway our Azure virtual th site-to-site PN connections.	Select a deployment model @ Resource Manager	v
	Management		Cocal network gate Represents the VPN (local network and use	eway device in your ed to set up a	Create	
	C	<hr/>	site-to-site VPN conn	nection.		

- 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 sousréseau 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

Create virtual network _
 * Name NetScalerVNet ✓ * Address space ^① 22.22.0.0/16 ✓ 22.22.0.0 - 22.22.255.255 (65536 addresses) * Subnet name NSFrontEnd ✓
 * Subnet address range ● 22.22.1.0/24 ✓ 22.22.1.0 - 22.22.1.255 (256 addresses) * Subscription Microsoft Azure Enterprise ✓ * Resource group ● Create new ● Use existing NSDocs ✓
* Location Southeast Asia ✓
Create Automation options

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**.

NetScalerVNet - Subnets						*	—	×
virtual network		Gate	way subnet					
Search (Ctrl+/)	Search sub	onets						
	NAME	^	ADDRESS RANGE	^	AVAILABLE ADDR ^	SECURITY GROUP	^	
	NSFrontEnd		22.22.1.0/24		251	-		
Access control (IAM)								
· · · · · ·								
SETTINGS								
↔ Address space								
 Connected devices 								
<-> Subnets								

- 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**.

Add subnet	- 🗖
* Name	
NSBackEnd	 ✓
* Address range (CIDR block) 🛛	
22.22.2.0/24	~
22.22.2.0 - 22.22.2.255 (256 addresses)	
Network security group	
None	
Route table	、 、
None	/
ОК	_

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 Cré	éer.
--------------------	------

		_ 🗖 ×		_ 🗖 ×
+ New	New		Data + S	Storage
Resource groups	Search the marketplace	See all	7 PREVIEW	Data Lake Store (preview) Hyper-scale repository for big data analytic workloads
All resources	Virtual Machines			
C Recent	Web + Mobile	>		SQL Data Warehouse (preview) Fully elastic, managed, and parallelized relational database.
Services	Data + Storage	\geq	FREVIEW	Analyze and scale in seconds.
👼 SQL databases	Data + Analytics	>		Azure DocumentDB Scalable and managed NoSQL
Virtual machines (classic)	Internet of Things	>		document database service for modern cloud applications.
Virtual machines	Networking	>	_	Storage account
Cloud services (classic)	Media + CDN	>		Use Blobs, Tables, Queues, and Files for reliable, economical cloud
💡 Subscriptions	Hybrid Integration	>		storage.
Results N	Security + Identity	>		Redis Cache
browse >	Developer Services	>	7	service for modern cloud applications
	Management	>		
	Intelligence	>		Azure Search Search-as-a-service solution
	Containers	>		

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.

Marketplace	Virtual Machines	
	Filter	
Everything	Availability Set	
Virtual Machines		
Web + Mobile	Kesults	
Data + Storage	NAME	PUBLISHER
Data + Analytics	C Availability Set	Microsoft
Internet of Things	FortiGateNGFW High Availability (HA)	Fortinet
Networking	. € mongo	Docker
Media + CDN	logsign focus siem v4.0 byol	Logsign
Hybrid Integration	Azure vAPV - BYOL	Array Networks
Security + Identity	Windows 8.1 Enterprise N (x64)	Microsoft
Developer Services	SQL Server AlwaysOn Cluster	Microsoft
Management	Windows 7 Enterprise N SP1 (x64)	Microsoft
Intelligence	Windows 10 Enterprise N (x64)	Microsoft
Containers	Related to your search 🗸	
	FortiGate NGFW Single VM Fortinet Memcached Docker	

- 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**.

– Create availability set	
* Name	
AvSet	~
Fault domains 🖲	3
Update domains 🛛	
	5
* Subscription	
Microsoft Azure Enterprise	~
 ★ Resource group ● ○ Create new ● Use existing 	
ResGroup	~
* Location	
Southeast Asia	~
Create	

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.

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.

≡ + New	– New	NETWO	\star _ \square $ imes$ Marketplace
Resource groups	NetScaler	X	
All resources	MARKETPLACE 	See all	Everything
🕓 Recent	Web + Mobile	>	Virtual Machines
🔇 App Services	Data + Storage	>	Web + Mobile
👼 SQL databases	Data + Analytics	>	Data + Storage
Virtual machines (classic)	Internet of Things	>	Data + Analytics
Virtual machines	Networking	>	Internet of Things
Cloud services (classic)	Media + CDN		Networking
💡 Subscriptions	Hydrid Integration		Media + CDN
Browse >	Developer Services	>	Hybrid Integration
	Management	>	Security + Identity
	Intelligence	>	Developer Services
	Containers	>	Management
	RECENT		Intelligence
	Traffic Manager profile Microsoft		Containers
	Resource group Microsoft		
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 **Ges-tionnaire de ressources** et cliquez sur **Créer**.

C	reate	virtual machine _		×	Basics	_ [×
	1	Basics Configure basic settings	>		* Name Citrix-NetScaler-User		•
	2	Size Choose virtual machine size	>		SSD * User name		•
	3	Settings Configure optional features	>		* Authentication type SSH public key Password		<u>~</u>
	4	Summary NetScaler 11.1 VPX Bring Your	>		* Password		 ✓
	5	Buy	>		Subscription Microsoft Azure Enterprise		
					* Resource group Create new Use existing NetScalerResGroup Location		2
				_	Southeast Asia		

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.

Virtual machines 💉 🗙 brahasitaramanathancitrix (Default Directory)	NSDoc0330VM - Network interfaces	* ×
+ Add ≣≣ Columns ひ Refresh	Search (Ctrl+/)	
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Switch directories	NAME ^ PUBLIC IP ADDRE ^ PRIVATE IP	ADDR ^ SECURITY GROUP ^
nsdoc 1 items NAME V	Activity log 13.78.187.150 192.0.0.4 Access control (IAM) - - -	NSDoc0330VM-nsg
NSDoc0330VM ···	 Tags Diagnose and solve problems 	
	SETTINGS Availability set	
	Extensions Network interfaces	
	I Size	

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.

nsdoc0330vm923 - IP configurations Network interface						
Search (Ctrl+/)	+ Add R Save X Discard					
 Overview Activity log Access control (IAM) 	IP forwarding settings IP forwarding Virtual network					
Pags	IP configurations * Subnet					
SETTINGS						
IP configurations	Search IP configurations	IP VERSION				
DNS servers	inconfig1	IPv4				
Network security group	iptoring)					
Properties						

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 assurezvous que l'adresse IP appartient au même sous-réseau auquel la carte réseau est attachée.

Add IP configuration	
* Name ipconfig2	~
Type Primary Secondary	
Primary IP configuration already exists	
Private IP address settings	
Allocation Dynamic Static	
* IP address	
192.0.0.5	\checkmark
Public IP address Disabled Enabled	
* IP address Configure required settings	>

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**.

Create public IP address	
* Name PIP2	<
Assignment Dynamic Static	
ОК	

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.

Search IP configurations						
NAME	IP VERSION	ТҮРЕ	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS		
ipconfig1	IPv4	Primary	192.0.0.4 (Static)	13.78.187.150 (NSDoc0330VM-ip)		
ipconfig2	IPv4	Secondary	192.0.0.5 (Static)	13.78.183.123 (ipconfig2_PIP2)		
ipconfig3	IPv4	Secondary	192.0.0.6 (Static)			

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

April 1, 2025

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.





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 Power-Shell.

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.

1	Basics Configure basic settings	>	Subscription Enterprise Resource group	~
2	General Settings Configure the General settings		• Create new • Use existing NSDoc-RG	~
3	Network Settings Configure the Network settings		Location South India	~
4	Summary Netscaler HA (Staged)			
5	Buy			

5. La page Paramètres généraux s'affiche. Entrez les détails et sélectionnez OK.

Create	Citrix ADC 13.0 (High	×	General Settings	
1	Basics		User name * 🛈	nsroot 🗸
	Done		Password * 🛈	····· ··· ··· ··· ··· ··· ··· ··· ···
2	General Settings Configure the General settings	>	Confirm password * 🛈	····· ··· ··· ··· ··· ··· ··· ··· ···
			sku	BYOL
3	Network Settings Configure the Network settings		Virtual machine size * 🛈	2x Standard DS3 v2 4 vcpus, 14 GB memory
				Change size
4	Summary Citrix ADC 13.0 (High Availabilit		Publish Monitoring Metrics	true 🗸
			*Application Id ①	12345678-abcd-efgh-ijkl-mnopqrstuvwx 🗸
5			*API Access Key ①	······ ~

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 sousréseau, 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.

23 items 🗹 Show hidden types	
	TYPE 👈
🗌 🚸 alb	Load balancer
alb-publicip	Public IP address
avi-set	Availability set
🗌 😂 ns-vpx0	Disk
ns-vpx0	Virtual machine
ns-vpx0-mgmt-publicip	Public IP address
🗌 😂 ns-vpx1	Disk
ns-vpx1	Virtual machine
ns-vpx1-mgmt-publicip	Public IP address
🔲 📊 ns-vpx-nic0-01	Network interface
🔲 📊 ns-vpx-nic0-11	Network interface
ns-vpx-nic0-12	Network interface
ns-vpx-nic1-01	Network interface
ns-vpx-nic1-11	Network interface
ns-vpx-nic1-12	Network interface
🔲 🧻 ns-vpx-nic-nsg0-01	Network security group
🔲 🧻 ns-vpx-nic-nsg0-11	Network security group
🔲 🧻 ns-vpx-nic-nsg0-12	Network security group
🔲 🧻 ns-vpx-nic-nsg1-01	Network security group
Dis-vpx-nic-nsg1-11	Network security group
Dis-vpx-nic-nsg1-12	Network security group
vnet01	Virtual network
vpxhamd7fl3wouvrxk	Storage account

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.

Search (Ctrl+/)	╋ Add			
• • • •	Search frontend IP configurations			
	NAME		IP ADDRESS	
Activity log	ipconf-11		104.40.60.190 (alb-publicip)	
Access control (IAM)				
🏉 Tags				
🗙 Diagnose and solve problems				
SETTINGS				
Frontend IP configuration				

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 ?

Home > N Create	New > Marketplace > Everything : NetScaler 12.1 HA using	A	icaler X	12.1 HA using Av Basics	railability Zones > Create NetScaler 12.1 HA us
1	Basics Configure basic settings	>			This deployment requires Azure region supporting Availability Zones. Selecting a region that does not support Availability Zones will
2	General Settings Configure the General settings	>		U	result in deployment failure. Refer to the <u>list</u> of Azure regions supporting Availability Zones.
3	Network Settings Configure the Network settings	>		Subscriptio	on
4	Summary NetScaler 12.1 HA using Availa	>		* Resource	e group 🚯 e new 🕜 Use existing
5	Buy	>	-	* Location East US 2	2 ~

- 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 sousréseau, 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**.

Filter by name	All types	✓ All locations ✓	No grouping∨
2 items Show hidden types ()			
NAME 14		TYPE †↓	LOCATION 👈
🗌 🚸 alb		Load balancer	East US 2
alb-publicip		Public IP address	East US 2
ns-vpx0		Virtual machine	East US 2
s-vpx0_OsDisk_1_d7b757	o8aa804bf1991a083f319e553a	Disk	East US 2
ns-vpx0-mgmt-publicip		Public IP address	East US 2
ns-vpx1		Virtual machine	East US 2
svpx1_OsDisk_1_0c2364c	43e2b47fa896bf14b02090ee0	Disk	East US 2
ns-vpx1-mgmt-publicip		Public IP address	East US 2
ns-vpx-nic0-01		Network interface	East US 2
ns-vpx-nic0-11		Network interface	East US 2
ns-vpx-nic0-12		Network interface	East US 2
ns-vpx-nic1-01		Network interface	East US 2
ns-vpx-nic1-11		Network interface	East US 2
ns-vpx-nic1-12		Network interface	East US 2
ns-vpx-nic-nsg0-01		Network security group	East US 2
ns-vpx-nic-nsg0-11		Network security group	East US 2
ns-vpx-nic-nsg0-12		Network security group	East US 2
ns-vpx-nic-nsg1-01		Network security group	East US 2
ns-vpx-nic-nsg1-11		Network security group	East US 2
ns-vpx-nic-nsg1-12		Network security group	East US 2
⟨••⟩ test1		Virtual network	East US 2
vpxhavdosvod3v5jeu		Storage account	Fast US 2

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

January 15, 2025

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 ;	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 ;
Les règles LB et le port configurés sont HTTP (80), SSL (443), sonde d'intégrité (9000) -	Mgmtsubnet=12.5.2.0/24 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 serveur est configurée avec IPConfig4, qui	Mgmtsubnet=12.5.2.0/24 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 IPConfig8, qui
-	Inclut une adresse IP privee (12.5.3.24) ; nic3 ; BackEndSubnet=12.5.3.0/24 Les règles et les ports pour NSG sont SSH (22), HTTP (80), HTTPS (443)	inclut une adresse IP privee (12.5.3.28) ; nic6 ; BackEndSubnet=12.5.3.0/24 -

Paramètres des paramètres

Les paramètres suivants sont utilisés dans ce scénario:

1	\$locName= "South east Asia"
3	<pre>\$rgName = "MulitIP-MultiNIC-RG"</pre>
5	<pre>\$nicName1= "VM1-NIC1"</pre>
7	<pre>\$nicName2 = "VM1-NIC2"</pre>
9	<pre>\$nicName3= "VM1-NIC3"</pre>
11	<pre>\$nicName4 = "VM2-NIC1"</pre>
12	<pre>\$nicName5= "VM2-NIC2"</pre>
14	<pre>\$nicName6 = "VM2-NIC3"</pre>
17	<pre>\$vNetName = "Azure-MultiIP-ALB-vnet"</pre>
10 19 20	<pre>\$vNetAddressRange= "12.5.0.0/16"</pre>
20 21 22	<pre>\$frontEndSubnetName= "frontEndSubnet"</pre>
23	<pre>\$frontEndSubnetRange= "12.5.1.0/24"</pre>
24 25 26	<pre>\$mgmtSubnetName= "mgmtSubnet"</pre>
27	<pre>\$mgmtSubnetRange= "12.5.2.0/24"</pre>
29 30	<pre>\$backEndSubnetName = "backEndSubnet"</pre>
31 32	<pre>\$backEndSubnetRange = "12.5.3.0/24"</pre>
33 34	<pre>\$prmStorageAccountName = "multiipmultinicbstorage"</pre>
35	<pre>\$avSetName = "multiple-avSet"</pre>
37 38	<pre>\$vmSize= "Standard_DS4_V2"</pre>
39 40	<pre>\$publisher = "Citrix"</pre>
41	<pre>\$offer = "netscalervpx-120"</pre>
43 44	\$sku = "netscalerbyol"
45 46	<pre>\$version="latest"</pre>
47	<pre>\$pubIPName1="VPX1MGMT"</pre>
49	<pre>\$pubIPName2="VPX2MGMT"</pre>

50	
51 52	<pre>\$pubIPName3="ALBPIP"</pre>
53 54	\$domName1="vpx1dns"
55	<pre>\$domName2="vpx2dns"</pre>
57 58	\$domName3="vpxalbdns"
59 60	\$vmNamePrefix="VPXMultiIPALB"
61 62	<pre>\$osDiskSuffix1="osmultiipalbdiskdb1"</pre>
63 64	<pre>\$osDiskSuffix2="osmultiipalbdiskdb2"</pre>
65 66	<pre>\$lbName= "MultiIPALB"</pre>
67 68	<pre>\$frontEndConfigName1= "FrontEndIP"</pre>
69 70	<pre>\$backendPoolName1= "BackendPoolHttp"</pre>
71 72	<pre>\$lbRuleName1= "LBRuleHttp"</pre>
73 74	<pre>\$healthProbeName= "HealthProbe"</pre>
75	\$nsgName="NSG-MultiIP-ALB"
77	<pre>\$rule1Name="Inbound-HTTP"</pre>
79	<pre>\$rule2Name="Inbound-HTTPS"</pre>
81	<pre>\$rule3Name="Inbound-SSH"</pre>

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

```
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.

```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
1
        Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 101
2
3
4
     -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 80
5
6
     $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
7
        Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 110
8
9
     -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 443
11
     $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
13
        Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 120
14
15
     -SourceAddressPrefix Internet -SourcePortRange * -
16
        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.

```
6
7
     $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
         $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
     $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
         $rgName -Location $locName -AddressPrefix $vNetAddressRange -
         Subnet $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
     $subnetName ="frontEndSubnet"
13
14
15
16
     \$subnet1=\$vnet.Subnets|?{
17
    \$\_.Name -eq \$subnetName }
18
19
20
     $subnetName="backEndSubnet"
21
22
23
24
     \$subnet2=\$vnet.Subnets|?{
25
    \$\_.Name -eq \$subnetName }
26
27
28
29
     $subnetName="mgmtSubnet"
31
32
     \$subnet3=\$vnet.Subnets|?{
33
    \$\_.Name -eq \$subnetName }
```

Créez des adresses IP publiques.

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
     $IPConfigName3="IPConfig-3"
10
11
12
     $IPAddress="12.5.1.27"
13
14
15
16
     $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
         Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19
     $IPConfigName4 = "IPConfig-4"
20
21
     $IPAddress = "12.5.3.24"
22
23
24
     $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
25
          -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des configurations IP pour VPX2.

```
$IpConfigName5 = "IPConfig5"
1
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
     $IPConfigName7="IPConfig-7"
10
11
12
13
     $IPAddress="12.5.1.28"
14
15
     $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
16
         Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
     $IPConfigName8="IPConfig-8"
19
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.

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
1
        $rgName -Location $locName -IpConfiguration $IpConfig1 -
        NetworkSecurityGroupId $nsg.Id
2
3
    $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
4
        $rgName -Location $locName -IpConfiguration $IpConfig3 -
       NetworkSecurityGroupId $nsg.Id
5
6
    $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
7
        $rgName -Location $locName -IpConfiguration $IpConfig4 -
       NetworkSecurityGroupId $nsg.Id
```

Créez des cartes réseau pour VPX2.

1	<pre>\$nic4=New-AzureRmNetworkInterface -Name \$nicName4 -ResourceGroupName \$rgName -Location \$locName -IpConfiguration \$IpConfig5 - NetworkSecurityGroupId \$nsg.Id</pre>
2	
3	
4	<pre>\$nic5=New-AzureRmNetworkInterface -Name \$nicName5 -ResourceGroupName \$rgName -Location \$locName -IpConfiguration \$IpConfig7 - NetworkSecurityGroupId \$nsg.Id</pre>
5	
6	
7	<pre>\$nic6=New-AzureRmNetworkInterface -Name \$nicName6 -ResourceGroupName \$rgName -Location \$locName -IpConfiguration \$IpConfig8 - NetworkSecurityGroupId \$nsg.Id</pre>

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

0	
7	<pre>\$cred=Get-Credential -Message "Type the name and password for VPX login."</pre>
8	
9	\$vmConfig=Set-AzureRMVMOperatingSystem -VM \$vmConfig -Linux - ComputerName \$vmName -Credential \$cred
10	
11	\$vmConfig=Set-AzureRMVMSourceImage -VM \$vmConfig -PublisherName \$publisher -Offer \$offer -Skus \$sku -Version \$version
12	
13	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic1 .Id -Primary</pre>
14	
15	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic2 .Id</pre>
16	
17	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic3 .Id</pre>
18	
19	ŚosDiskName=ŚvmName + "-" + ŚosDiskSuffix1
20	
20	
21	<pre>\$osVhdUr1=\$prmStorageAccount.PrimaryEndpoints.Blob.loString() +</pre>
22	
23	<pre>\$vmConfig=Set-AzureRMVMOSDisk -VM \$vmConfig -Name \$osDiskName - VhdUri \$osVhdUri -CreateOption fromImage</pre>
24	
25	Set-AzurePm\/MPlan -\/M \$vmConfig -Publisher \$publisher -Product
25	\$offer -Name \$sku
26	
27	New-AzureRMVM -VM \$vmConfig -ResourceGroupName \$rgName - Location \$locName

Créez VPX2.

```
• • •
1
2
     $suffixNumber=2
3
4
     $vmName=$vmNamePrefix + $suffixNumber
5
6
7
     $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
8
        AvailabilitySetId $avSet.Id
9
10
11
     $cred=Get-Credential -Message "Type the name and password for VPX
        login."
12
13
14
     $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
        ComputerName $vmName -Credential $cred
15
```

```
NetScaler VPX 14.1
```

```
16
17
     $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
         $publisher -Offer $offer -Skus $sku -Version $version
18
19
     $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
31
     $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
32
         /" + $osDiskName + ".vhd"
34
     $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
          $osVhdUri -CreateOption fromImage
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
      $nic3.IPConfig
 8
9
10
      $nic4.IPConfig
11
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.

Resource Group HA INC NIC O NIC 1 NIC 2 VPX 1 Server Farm 1 ALS Public IP ALB NIC O Internet NIC 1 NIC 2 VPX 2 Server Farm 2 VNET

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).

\equiv Microsoft Azure	Search resources, services, and docs (G+/)				
Home > Create a resource >					
Marketplace					
Get Started	NetScaler ADC 14.1 X Pricing : All				
Service Providers					
Management	Azure benefit eligible only ① Azure services only				
management	Showing 1 to 1 of 1 results for 'NetScaler ADC 14.1'. Clear search				
Private Marketplace					
Private Offer Management	net-scaler				
My Marketplace	NetScaler ADC 14.1				
Favorites	Cloud Software Group				
My solutions	Virtual Machine				
Recently created	Kubernetes Ingress LB				
Private plans					
Categories	Starts at \$ 0.26/3 years				
	Create 🗸 🗢				
Compute (1)					

2. Sélectionnez le mode de licence ADC requis, puis cliquez sur **Créer**.

NetScal	er ADC 14.1 ☆ … Group				
net/scaler.	NetScaler ADC 14.1 \bigcirc Add to Favorites				
	Free trial				
	Plan NetScaler ADC 14.1 VPX Standard Edi Create P Filter	Start with a pre-set configuration Purchase a reservation			
Overview	NetScaler ADC 14.1 VPX Standard Edition - 5000 Mbps NetScaler ADC 14.1 VPX Bring Your Own License NetScaler ADC 14.1 VPX Express - 20 Mbps	ıtings + Reviews			
NetScaler AI and pricing f the hybrid cl	NetScaler ADC 14.1 VPX Express - 20 Mips	/ery controller that delivers your applications quickly, reliably, and securely, with ovide operational consistency and a smooth user experience, NetScaler ADC $\epsilon\epsilon$			
You can lear Why NetScal	NetScaler ADC 14.1 VPX Advanced Edition - 10 Mbps	acture with NetScaler ADC on Microsoft Azure by reading the eBook, available			
NetScaler AD for applicatio every step of	NetScaler ADC 14.1 VPX Standard Edition - 200 Mbps NetScaler ADC 14.1 VPX Advanced Edition - 200 Mbps	delivery, a comprehensive centralization management system, and orchestratic tScaler's all-in-one solution brings point solutions under one roof, ensuring sin			
Key Benefits: • Flexib	NetScaler ADC 14.1 VPX Premium Edition - 200 Mbps NetScaler ADC 14.1 VPX Standard Edition - 1000 Mbps	ature-rich ADC available across a wide variety of deployment options with the			
capac Best U route	NetScaler ADC 14.1 VPX Advanced Edition - 1000 Mbps	gent, global load-balancing service that uses real-time Internet traffic and data			

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.

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review +	create
--	--------

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more a

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * (i)		~
Resource group * (i)	(New) demo	~
	Create new	
Instance details		
Virtual machine name * 🕕	vm1-demo	\checkmark
Region * (i)	US) East US	~
Availability options (i)	Availability zone	\checkmark
Availability zone * 🕕	Zones 1	~
Review + create < Previ	ous Next : Disks >	

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.
Create a virtual machine

 Basics
 Disks
 Networking
 Management
 Monitoring
 Advanced
 Tags
 Review + create

 Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

Network interface

Learn more 🗹

When creating a virtual machine, a network interface will be created for you.

Virtual notwork *	(now) vm1-domo-vnot	~
Virtual network	Create new	×
Subnet * 🔅	(new) default (10.2.0.0/24)	\sim
	(new) um1 demo in	
	(new) vm I-demo-ip	~
NIC network security group 🔅	○ None	
	Basic	
	O Advanced	
Public inbound ports * 🕕	○ None	
	 Allow selected ports 	
Select inbound ports *	SSH (22)	\sim
	This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab t create rules to limit inbound traffic to known IP addresses.	0
Delete public IP and NIC when VM is		
deleted (i)		
Enable accelerated networking \bigcirc		
Load balancing		
You can place this virtual machine in the	backend pool of an existing Azure load balancing solution. Learn more $ec d$	
Load balancing ontions	None	
	Supports all TCP/UDP network traffic, port-forwarding, and outbound flow	s.
	Web traffic load balancer for HTTP/HTTPS with URL-based routing. SSL	

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**.

Create a virtual machine

Validation pass	ed						
Basics Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create	
1 Cost given be	low is an estimate	and not the final price	ce. Please use Prie	cing calculator d	for all you	r pricing needs.	
Price							
11100							
NetScaler ADC 14.	1	Not covered	by credits 🛈				
by Cloud Software C Terms of use Priva	Group Cy policy	2.3000 US	D/hr				
1 X Standard DS2	12	Subscription	credits apply	6			
by Microsoft	-	Subscription	refeates apply				
Terms of use Priva	cy policy	0.0880 US	D/hr				
		Pricing for	other VM sizes				
TERMS							
By clicking "Create", above; (b) authorize billing frequency as information with the provide rights for the	I (a) agree to the Microsoft to bill my Azure subscr provider(s) of th ird-party offering	e legal terms and pr my current paymer iption; and (c) agree e offering(s) for su gs. See the Azure M	rivacy statement nt method for th e that Microsoft pport, billing an larketplace Term	(s) associated w e fees associate may share my o d other transact s for additional	vith the Ma ed with the contact, us tional activ details.	arketplace offering(s) listed e offering(s), with the same sage and transactional vities. Microsoft does not	
Name							
Preferred e-mail add	iress						
Preferred phone nu	mber	-					
A You have set back to Basics	SSH port(s) oper tab.	n to the internet. Th	nis is only recomm	ended for testin	g. If you w	ant to change this setting, go	
Create		Deviews					

5. Une fois le déploiement terminé, cliquez sur **Accéder à la ressource** pour voir les détails de configuration.

CreateVm-citrix.nets	calervpx-141-netscaler5000sta-20230908103924 Overview 🖉 🗠
	📋 Delete 🛇 Cancel 🏦 Redeploy 🚽 Download 💍 Refresh
 ♣ Overview ♀ Inputs ♀ Outputs P Template 	 Vour deployment is complete Deployment name: CreateVm-citrix.netscalervpx-141-netscaler500 Subscription: Resource group: demo Start time: 8/9/2023, 11:41:20 AM Correlation ID: 902798eb-f8b1-4c0a-a6bb-efe734476f71 Deployment details Next steps Setup auto-shutdown Recommended Monitor VM health, performance and network dependencies Recommended Run a script inside the virtual machine Recommended Go to resource
	Give feedback ${\cal R}^{2}$ Tell us about your experience with deployment

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**.

Home > vm1-demo | Networking >

Create network interface

Project details
Subscription ①
NSDev Platform CA anoop.agarwal@citrix.com
Resource aroun *
demo
Create new
Location (A)
(05) Last 05
Network interface
Name *
vm1-demo-nic
Virtual network ①
vm1-demo-vnet
Subnet * (i)
client (10.2.1.0/24)
NIC network security group (i)
U Advanced
Public inbound ports * ①
None
O Allow selected ports
Select inbound ports
Select one or more ports
All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.
Private IP address assignment Dynamic Static Private IP address (IPv6) Accelerated networking ① Disabled Enabled
Create

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.

Create load balancer

Project details			
Subscription *			/
Resource group *	demo Create new	~	
Instance details			
Name *	alb1	×	/
Region *	Southeast Asia	~	~
SKU * 🕕	 Standard Gateway Basic 		
Туре * 🛈	Public Internal		
Tier *	RegionalGlobal		
Review + create < Previous	Next : Frontend IP configuration >	Download a template for automation	중 Give

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.

Creat	e load balancer							
Basics	Frontend IP configuration	Backend pools	Inbound rules	Outbound rules	Tags	Review + create		
A fronter	nd IP configuration is an IP addr	ess used for inbound	and/or outbound co	ommunication as defi	ned withiı	n load balancing, inbound	d NAT, and outbou	nd rules.
+ Ado	d a frontend IP configuration							
Name	¢↑	_		IP a	address 1	¢1		
Add a fi	rontend IP to get started							

Add frontend IP configuration	\times
Name *	
alb-frontend	\checkmark
Duarrian	
IP type	
IP address IP prefix	
Public IP address *	
(New) alb-public-ip	\sim
Create new	
Gateway Load balancer (i)	
None	\sim



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.

Create load balancer

Basics	Frontend IP configuration	on Backend pools	nbound rules Outb	ound rules Tag	gs Review + create	
A backen	nd pool is a collection of res	ources to which your load ba	lancer can send traffic. A	A backend pool can	contain virtual machine	es, virtual machine s
+ Add	d a backend pool					
						15 I I
Name	Vi	rtual network	Resource Name	Network	interface	IP address
Name \checkmark alb	-backend-pool	rtual network	Resource Name	Network	tinterface	IP address
Name	-backend-pool :kend-pool vn	n1-demo-vnet	Resource Name vm1-demo	Network vm1-den	no324_z1	10.2.0.4

5. Dans l'onglet Inbound rules (Règles entrantes), cliquez sur Add a Load balancing rule (Ajouter unerègle 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.

Add load balancing rule

alb1

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *	lb-rule1
IP Version *	IPv4
	O IPv6
Frontend IP address * 🛈	alb-frontend (To be created) \checkmark
Backend pool * 🛈	alb-backend-pool \checkmark
Protocol	• ТСР
	O UDP
Port *	80
Backend port * 🗊	10
Health probe * 🛈	(new) health-probe1 (TCP:80)
	Create new
Session persistence (i)	None 🗸
Idle timeout (minutes) * (i)	4
Enable TCP Reset	
Enable Floating IP (i)	
Outbound source network address translation (SNAT) 🛈	(Recommended) Use outbound rules to provide backend pool members access to the internet. Learn more. 2
	○ Use default outbound access. This is not recommended because it can cause SNAT port exhaustion. Learn more. ²
Save Cancel	오 Give feedback

 \times

Cliquez sur Réviser + Créer. Une fois la validation passée, cliquez sur Créer.
 Create load balancer

🕑 Val	idation passed					
	5	Parlanda and			-	
Basics	Frontend IP configuration	Backend pools	Indound rules	Outbound rules	Tags	Review + create
Basics						
Subscrip	tion					
Resource	e group	demo				
Name		alb1				
Region		Southeast Asia				
SKU		Standard				
Tier		Regional				
Туре		Public				
Fronten	d IP configuration					
Frontend	IP configuration name	alb-frontend				
Frontend	IP configuration IP address	To be created				
Backene	d pools					
Backend	pool name	alb-backend-pool				
Inbound	d rules					
Load bal	ancing rule name	lb-rule1				
Health p	robe name	health-probe1				
Outbou	nd rules					
None						
Tags						
None						
Create	< Previous	Next > D	ownload a template	e for automation 🛛 🕅 Gi	ve feedba	ack

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**.

← Create HA Node

Remote Node IP Address*	
10 . 4 . 1 . 5	0
Configure remote system to participate	High Availability setup
Turn Off HA Monitor inter face/channels	s that are down
Furn on INC(Independent Network Cont Units)	hguration) mode on solt node 🕕
Remote System Login Credential	
User Name	
Pessword	
Secure Access	

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**.

숙 Create HA Node

Remote Node IP Address*	
10 . 4 . 1 . 4	\bigcirc
Configure remote system to participate	High Availability setup
🗹 Turn Off HA Monitor interface/channels	that are down
Turn on INC(Independent Network Cont	figuration) mode on self node
RPC Node Password	
	$(\mathbf{\hat{l}})$
Remote System Login Credential	
User Name	
Password	
Secure Access	
Create Close	

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.

System > High Availability > Nodes											
Nodes 🔹											
Add Edit Delete Statistics Select Action V											
	ID :	IP ADDRESS	HOST NAME 0	MASTER STATE 0	NODE STATE	INC 0	SYNCHRONIZATION STATE	© SYNCHRONIZATION FAILURE RE	ASON 0		
	0	10.4.1.4	citrix-adc-1	Primary	●UP	ENABLED	ENABLED	-NA-			
	1	10.4.1.5		Secondary	●UP	ENABLED	SUCCESS	-NA-			
Total 2								25 Per Page ∨ Page 1 of1			

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**.

System > Not	System > Network > IPs > IPV4s												
IPs													C 😭
IPV4s 4	IPV6s 1	Port Allocation											
Add Edi	it Delete	Statistics Select Act	ian 🗸										
Q Click here to	o search or you can	enter Key : Value format											(i)
	IP ADDRESS	≎ STATE ≎	TYPE	MODE		ARP		ICMP		VIRTUAL SERVER		TRAFFIC DOMAIN	
	10.4.3.4	ENABLED	Subnet IP	Active		ENABLED		ENABLED		-N/A-			0
	10.4.2.5	ENABLED	Virtual IP	Active		ENABLED		ENABLED		ENABLED			0
	10.4.2.4	ENABLED	Virtual IP	Active		ENABLED		ENABLED		ENABLED			0
	10.4.1.4	ENABLED	NetScaler IP	Active		ENABLED		ENABLED		-N/A-			0
Total 4										25 Per	Page 🗸	Page 1 of 1	<

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.

System > No	work yirs y	IL A HO									
IPs										É	ž 😭
IPV4s 3	IPV6s 1	Port Allocation									
Add Ed	it Delete	Statistics	ect Action 🗸								
Q Click here to	o search or you can	enter Key : Value format									0
	IP ADDRESS	≑ STATE	TYPE	© MOD	E 0	ARP	ICMP	VIRTUAL SERVER		TRAFFIC DOMAIN	
	10.4.3.5	ENABLED	Subnet IP	Activ	e	ENABLED	ENABLED	-N/A-			0
	10.4.2.5	ENABLED	Virtual IP	Passi	ive	ENABLED	ENABLED	ENABLED			0
	10.4.1.5	ENABLED	NetScaler IP	Activ	e	ENABLED	ENABLED	-N/A-			0
Total 3								25 Per Page	~	Page 1 of 1	•

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.

🕤 Create IP Set	IPV4s 🖪										С×
Nerve"	Add Edit	Delete Stati	tics Select Actio	nv.							
ipoett	Q. Click here to sear	h ar you can enter Key:	lailue format								0
Traffic Domain	0	IP ADDRESS :	TRAFFIC DOMAIN :	OWNER NODE	: STATE	TYPE	: MODE :	ARP	: ICMP	: VIRTUAL SET	RVER :
	0	10.4.1.4	0	ALL NODES (255)	ENABLED	NetScalar IP	Active	ENABLED	ENABLED	-N/A-	
	0	10.4.2.4	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	
1994 1990	•	10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	
		10.4.3.4	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	
Insert Delete	Total 4								25 Per Page 🛛 🛩	Page 1 of 1	
IP ADDRESS No items	Insert	Close									
Crosts Close											

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.

← Create IP Set	IPV4s 3									С×
Name'	Add Edit	Delete	tatistics	at Action~						
	Q Click here to seerc	h or you can enter K	ey : Value format							()
	0	IP ADDRESS 0	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER
	0	10.4.1.5	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
		10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED
		10.4.3.5	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
	Total 3							25 Per Pa	ge 🗸 Paga	1 of 1 🚽 🕨
	Insert	Close								
No items										

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.

← Load Balancing Virtual Server

Basic Settings		
Create a virtual server by specifying a name, an i area network (LAN) or wide area network (WAN), You can configure multiple virtual servers to reco	IP address, a port, and a protocol type. If an application is accessible fro , the VIP is usually a private (ICANN non-noutable) IP address, avec client requests, thereby increasing the availability of resources to pr	In the linternet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local rocass client requests.
Name G		
VI	/	
Protocol*		
HTTP		
IP Address Type*		
IP Address V		
IP Address*		
10 . 4 . 2 . 4	0	
Port"		
80	0	
Traffic Domain	Add	Virtual Server State I Nit Sole AppTox Logins
IP Hange IP Set settings		Retain Connections on Cluster
(Deat		
inset v	Add Edit ()	
ganti V		
Redirection Mode*		
B.Razed		
Listen Priority		

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.

NetScaler VPX 14.1

c 1	and Pal	Inneing Virtual Server	Service Bind	ng > Service							
· · ·			Service	0							×
			-								
			Select	Add Edit							
			Q. Clickhere t	o search or you can enter Key : Value format							()
			0	NAME	STATE :	IP ADDRESS/DOMAIN NAME :	TRAFFIC DOMAIN	PORT :	PROTOCOL :	MAX CLIENTS :	MAX REQU
		DOWN		azurelbdnsservice0	• UP	168.63.129.16	0	53	DNS	0	
				sl	●UP	10.4.3.6	0	80	HTTP	0	
				2	●UP	10.4.3.7	0	80	нттр	0	
			Total 3						25 Per Page	⊻ Page 1 of1	\rightarrow

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.

Q Search Menu		System > High Availability > Nodos						
Favorites	\sim	Nodes 😰						C 😭
AZURE	>	Add Edit Delete Stativ	Select Action 🗸					
System	\sim	D ID : IPADORESS	Elect Adion Force Synchronization ASTER STATE	node state	1 INC 1	SYNCHRONIZATION STATE :	SYNCHRONI/ATION HAILURE REASON	
Licenses		0 10.4.1.4	crimendo-1 Primary	O UP	ENABLED	ENABLED	-N/r-	
Settings		1 1043.5	Force Failurer	• UP	FNAR HD	SUCCESS	NA .	
Diagnostics		lotal 2					25 Per Page ∨ Page I of I	
High Availability	\sim							
Nodes								
Route Monitors								

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).

Home > mysite.net							
mysite.net							\$ ×
	Record set \rightarrow Move	e 🛅 Delete zone 💍	Refresh				
Overview	Resource group (change) gslb_phase2			Name server 1 -			
Activity log	Subscription (change)	aganalibitikoan		Name server 2 -			
Access control (IAM)	Subscription ID			Name server 3			
🛹 Tags	764bc6a9-7927-4311-8e6	7-ed073090cea3		-			
lpha Diagnose and solve problems				Name server 4 -			
Settings	Tags (change) Click here to add tags						
Properties				*			
Locks							
🖳 Automation script	NAME	ТҮРЕ	TTL	VALUE	ALIAS RESOURCE TYPE	ALIAS TARGET	
Monitoring				Email: azuredns-ho Host: internal.clou			
📮 Alerts	@	SOA	3600	Refresh: 3600 Retry: 300			
iii Metrics				Expire: 2419200 Minimum TTL: 300 Serial number: 1			
Support + troubleshooting				conta number. I			
New support request							

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.

Virtual_Network_A_10	_0				
,♀ Search (Ctrl+/)	≪ $ひ$ Refresh → Move 🛍	Delete			
-> Overview	Resource group (<u>change</u>) GSLB_Phase2		Address space 10.8.0.0/16		
Activity log	Location		DNS servers		
Access control (IAM)	Subscription (change)		10.8.0.0		
Tags	NOw Pation-Or average	web@dtrik.com			
Diagnose and solve problems	Subscription ID 764bc6a9-7927-4311-8e67-ed	073090cea3			
ttings	Tags (change)				
> Address space	Click here to add tags		*		
 Connected devices 	Connected devices				
Subnets					
DDoS protection	DEVICE	↑↓ ТҮРЕ	1 IP ADDRESS	↑↓ SUBNET	
Firewall (Preview)	nsvneta210	Network interface	10.8.0.4	default	
DNS servers	nsvneta210	Network interface	10 8 0 5	default	
Peerings	docforwarder962	Network interface	10.9.0.6	default	
Service endpoints		Network interface	10.0.0.0	default	
Properties	clientvneta27	Network interface	10.8.0.7	default	
Tropercies					
Core > Virtual_Network_B_10_9	Azure2AwsGW	Virtual network gateway		GatewaySubnet	
Locks ome > Virtual_Network_B_10_9 Virtual_Network_B_10_ Virtual_network	Azure2AwsGW 9 ≪ Č Refresh → Move 👔	Virtual network gateway		GatewaySubnet	5
Virtual_Network_B_10_9 Virtual_Network_B_10_9 Virtual_network Search (Ctrl+/) Overview	9 ≪ O Refresh → Move Resource group (change)	Virtual network gateway	- Address space	GatewaySubnet	,
Cocks Virtual_Network_B_10_9 Virtual_Network_B_10_ Virtual_network Search (Ctrl+/) Overview Activity log	Azure2AwsGW	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers	GatewaySubnet	3
	Azure2AwsGW 9 ≪ ♥ Refresh → Move ♥ Resource group (change) GSLB_Phase2 Location West US	Virtual network gateway	- Address space 10.9.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
	Azure2AwsGW 9 ≪ ひRefresh → Move GSLB Phase2 Location West US Subscription (change)	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
Virtual_Network_B_10_9 Virtual_Network_B_10_9 Virtual_network Virtual_network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems	9 ≪ ♥ Refresh → Move ■ Resource group (change) GSLB Phase2 Location West US Subscription ID 764bc6a9-7927-4311-8e67-edf	Virtual network gateway	- Address space 10.9.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
Virtual_Network_B_10_9 Virtual_Network_B_10_ Virtual_network Search (Ctrl+/) Overview Activity log Activity log Coverview Displaces control (IAM) Tags Diagnose and solve problems ttipas	9	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
	Azure2AwsGW 9 ≪ ♥ Refresh → Move ♥ Resource group (change) GSLB_Phase2 Location West US Subscription (change) Subscription ID 764bc6a9-7927-4311-8e67-ed(Tags (change) Click here to add tags	Virtual network gateway	- Address space 10.90.0/16 DNS servers 10.90.6	GatewaySubnet	5
	Azure2AwsGW 9 « ♥ Refresh → Move ♥ Resource group (change) GSLB Phase2 Location West US Subscription (change) Subscription (change) Connected devices	Virtual network gateway	- Address space 10.90.0/16 DNS servers 10.90.6	GatewaySubnet	5
	Azure2AwsGW 9 ≪ ♥ Refresh → Move ♥ GSLB Phase2 Location West US Subscription ID 764bc6a9-7927-4311-8e67-ed0 Tags (change) Cick here to add tags Connected devices Ø Search connected devices	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
	Azure2AwsGW 9 ≪ ♥ Refresh → Move ♥ GSLB Phase2 Location West US Subscription (change) Subscription ID 764bc6a9-7927-4311-8e67-ed(Tags (change) Click here to add tags Connected devices P Search connected devices DEVICE	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	3
Locks I cocks Virtual_Network_B_10_9 Virtual_Network_B_10_ Virtual_network Search (Clrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems ttings Address space Connected devices Subnets DDoS protection Firewall (Preview)	Azure2AwsGW 9 ≪	Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
I Locks I Locks Ome > Virtual_Network_B_10_9 Virtual_network Virtual_network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems ttings Address space Connected devices Subnets DDoS protection Firewall (Preview) DNS servers	Azure2AwsGW 9	Virtual network gateway Delete TYPE Network interface Network interface	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
	Azure2AwsGW 9	Virtual network gateway Delete TYPE Network interface Network interface	- Address space 10.90.0/16 DNS servers 10.90.6	GatewaySubnet	5
Itoperies Idoks Idoks Virtual_Network_B_10_9 Virtual_Network_B_10_ Virtual_network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems ttings Address space Connected devices Subnets DDoS protection Firewall (Preview) DNS servers Peerings Service endpoints Service endpoints	Azure2AwsGW 9	Virtual network gateway Virtual network gateway Virtual network gateway Tree Tree Network interface Network interface Network interface Network interface Network interface Network interface	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5
Locks Some > Virtual_Network_B_10_9 Virtual_Network_B_10_ Notework Notework Virtual_Network_B_10_ Notework Notework Notework Virtual_Network_B_10_ Notework Notework Virtual_Network_B_10_ Notework Notework Properties	Azure2AwsGW 9	Virtual network gateway Virtual network interface Virtual netw	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	5

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.

Home > Virtual_Network_A_10_8 - Peerings > Vnet_A_to_B	
Vnet_A_to_B Virtual_Network_A_10_8	×
R Save X Discard 🗰 Delete	
Name Vnet_A_to_B Peering status Connected Provisioning state Succeeded Peer details Address space 10.9.0.0/16 Virtual network Virtual network Mirtual_Network_B_10_9 Configuration Allow virtual network access ① Disabled Enabled I allow forwarded traffic ① Allow gateway transit ①	
Use remote gateways	•

L'image suivante illustre le peering réussi du réseau virtuel A vers le réseau virtuel B.

Home > Virtual_Network_A_10_8 - Pee	erings			
Virtual_Network_A_10_	8 - Peerings			
	≪ ➡ Add			
↔→ Overview	Search peerings			
Activity log	NAME	PEERING STATUS	PEER	GATEWAY 1
Access control (IAM)	Vnet_A_to_B	Connected	Virtual_Network_B_10_9	Enabled
🛷 Tags				
Diagnose and solve problems				

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.



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.

- 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 VN++ A
        zone "mysite.net" {
1
2
3
                          type forward;
4
            forwarders {
5
      168.63.129.16;
                           }
6
     ;
             }
7
8
     ;
9
            zone "ptm.mysite.net" {
10
                 type forward;
11
12
                 forwarders {
13
      10.8.0.5;
                   }
14
     ;
15
             }
16
```

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 :

```
1 zone "ptm.mysite.net" {
2
3 type forward;
4 forwarders {
5 10.8.0.5; }
6 ;
7 }
8 ;
```



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
1 zone "mysite.net" {
2 
3 type forward;
4 forwarders {
5 10.8.0.6; }
6 ;
7 }
```

```
8
     ;
9
          zone "ptm.mysite.net" {
10
               type forward;
11
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 :

🔄 Load Balancing Service	E	Load	Ba	lancing	Service
--------------------------	---	------	----	---------	---------

Service Name*	
s_adns	?
O New Server	
Server*	
10.8.0.5 (10.8.0.5)	\sim
Protocol*	
ADNS	\sim
Port*	
53	

æ	Load	Ba	lanci	na	Service
	Louu	Du	anci	''y	Jervice

Basic Settings	
Service Name*	
ADNS_TCP	
New Server O Existing Server	
IP Address*	
10 . 8 . 0 . 5	
Protocol*	
ADNS_TCP V	
Port*	
53	
▶ More	
Traffic Management / Load Balancing / Services / Services	
Services	٩
Services 2 Auto Detected Services 0 Internal Services 7	
Add Edit Delete Statistics No action	Search ∨
Name State IP Address/Domain Name Port Protocol Max Clients Max Requests Cache Type	Traffic Do
azurelbdnsservice0 ODWN 168.63.129.16 53 DNS 0 0 SERVER	
□ s_adns ●UP 10.8.0.5 53 ADNS 0 0 SERVER	
	Basic Settings Service Name* ADNS_TCP © New Server © Existing Server IP Address* 10 . 8 . 0 . 5 Protocol* ADNS_TCP Port* 53 Port* 53 More TefMagement / Lask Bancey / Serves / Serves Services

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.

Ġ Create GSLB Site

s1 🕜	
у́уре	
LOCAL V	
ite IP Address*	
10 . 8 . 0 . 5	
Public IP Address	
10 . 8 . 0 . 5	
Parent Site Backup Parent Sites Parent Site Name	
Triager Monitors*	
ALWAYS V	
Cluster IP	
Public Cluster IP	
Public Cluster IP	
Public Cluster IP NAPTR Replacement Suffix	
Public Cluster IP	
Public Cluster IP NAPTR Replacement Suffix Metric Exchange	
Public Cluster IP VAPTR Replacement Suffix Metric Exchange Network Metric Exchange	

Q. Search in Menu		Traffic Manag	gement / GS	LB / GSLB Sites						
System	>	GSLB S	Sites							
AppExpert	>									
Traffic Management	~	Add	Edit D	elete Statistics				-		
Load Balancing	>		Name	Metric Exchange (ME)	Site Metric MEP Status	Site IP Address	Туре	Public IP Address	Parent Site Name	Backup Pa
Content Switching	(!) >		s1	ENABLED		10.8.0.5	LOCAL	10.8.0.5		
Cache Dediraction	<u>~</u> \	4								

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.

G	GSLB Service
	Basic Settings
	Service Name*
	service_vnetA
	Site Name*
	s1 ~ +
	Site Type
	LOCAL
	Type*
	IP Based V
	Service Type*
	HTTP ~
	Port*
	80

10.8.0.6	~
10.0.0.0	·
Server IP*	
10 . 8 . 0 . 6	
Public IP	
10 . 8 . 0 . 6	
Public Port	
80	
Enable after Creating	
🖌 Enable Health Monitoring	
AppFlow Logging	
Comments	

- 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' GSLB Service Load Balancing Monitor Binding

	Add Binding	Edit Binding	Unbind	Edit Monitor		
		Monitor Name	Weight	State	Current State	Last Response
ruico		http	1	true	●UP	Success - HTTP response code 200 received.
rvice						

état du service.

7. Une fois que vous vous êtes connecté au moniteur HTTP, l'état des services est marqué comme

	Q Search in Menu		Traffic Manage	ement / GSLB / G	SLB Services		
	System	>	GSLB S	ervices			
	AppExpert	>					
	Traffic Management	\sim	Add	Edit Delete	Statistics	No action V	
	Load Balancing	>	•	Name	State	Effective State	IP Add
	Content Switching	() >		service_vnetA	• UP	DOWN	10.8.0
	Cache Redirection	() >		service_vnetB	• UP	DOWN	10.9.0
UP, comme indiqué dans l'image suivante : Services	DNS	>		service_Aws	• UP	DOWN	10.12.0

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.

asic Settings	
Name*	
vserver_m	0
DNS Record Type*	
A	\sim
Service Type*	
HTTP	~
Enable after Creating	
AppFlow Logging	
When this Virtual Server is	DOWN
Do not send any service	ce's IP address in response (EDR)
When this Virtual Server is	UP
Send all "active" servic	ce IPs' in response (MIR)
EDNS Client Subnet	
Respond with ECS opt	tion in the response for a DNS query with ECS
Validate ECS address is	is a private or unroutable address
Comments	

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.

GSLB Virtual Server Domain Binding							
GSLB Virtual Server Domain Binding							
Add Binding Edit Binding Unbind Show Bindings							
	FQDN	TTL (secs)	Backup IP	Cookie Domain	Cookie Time-out (mins)	Site Domain TTL (secs)	
	FQDN rr.ptm.mysite.net	TTL (secs) 5	Backup IP	Cookie Domain	Cookie Time-out (mins)	Site Domain TTL (secs)	

- 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.

GSLB Services and GSLB Servicegroup Binding ×									
Add Bindin	Edit Bin	ding Ur	bind	Edit Service					
	Service Name	IP Address	Port	Protocol	Canonical Name	State	Effective State	Weight	Dynamic Weight
	service_vnetA	10.8.0.6	80	HTTP		●UP	DOWN	1	0
	service_vnetB	10.9.0.4	80	HTTP		OUP	DOWN	1	0
	service_Aws	10.12.0.31	80	HTTP		OUP	DOWN	1	0

Après avoir lié les services et le domaine GSLB au serveur virtuel, il apparaît comme indiqué dans l'image suivante :

🕽 GSLB Vir	'irtual Server							
Basic Setting	5			/				
Name DNS Record Type Service Type State	vserver_rr A HTTP ● UP	AppFlow Logging EDR MIR ECS ECS Address Validation	ENABLED DISABLED DISABLED DISABLED DISABLED					
GSLB Services	and GSLB Servicegroup Binding							
3 GSLB Virtual S	Server to GSLBService Bindings			>				
No GSLB Virtua	I Server ServiceGroup Binding			>				
GSLB Virtual S	Server Domain Binding							
1 GSLB Virtual S	Server Domain Binding			>				
ADNS Service								
1 Service				>				
Method				/ ×				
Choose Method Tolerance (ms) IPv4 Netmask	ROUNDROBIN 0 255.255.255.255	Backup Method NC IPv6 Mask Length 128 Dynamic Weight DIS	NE) ABLED					
Done								

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.
NetScaler VPX 14.1

Q Search in Menu		Traffic Manage	ment / GSLB / GSLB Virtual Ser	vers		
System	>	GSLB V	irtual Servers			
AppExpert	>					
Traffic Management	~	Add	dit Delete Statistics	No action 🗸		
☆ Load Balancing	>		Name	State	Protocol	% Health
Content Switching	<u> </u>		vserver_rr	• UP	HTTP	100.00% 3 UP/0 DOWN
Cache Redirection	<u> </u>		vserver_sp	• UP	HTTP	100.00% 3 UP/0 DOWN

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.

- Microsoft Azure **P** Ŗ Azure services +SOL 1 Create a Marketplace Virtual Subscriptions Resource App Services Storage SQL databases Azure Database resource machines accounts for PostgreSQ.. groups լիղ
- 1. Connectez-vous au portail Azureet accédez à Azure Marketplace.

2. Sur Azure Marketplace, recherchez NetScaler.

Microsoft Azure	Ø Search resources, services, and do	cs (G+/)	5 17	1 🔅 2 🗯
Home >				
Marketplace				
Percently greated	Citrix ADC	X Pricing : All X Ope	rating System : All X Publisher	Type: All X
Service Providers		Offer Type : All X P	Publisher name : All 🗙	
Private Offers	Showing All Results			Ν
Categories				μ <u>3</u>
	citrix.	citrix.	citrix.	citrix.
Get Started	Citrix ADC 13.0	Citrix ADC	Citrix ADC 13.0 - Azure Stack	Citrix ADC VPX FIPS
AI + Machine Learning	Citrix	Citrix	Citrix	Citrix
Analytics	Virtual Machine	Azure Application	Virtual Machine	Virtual Machine
Compute	Citrix Application Delivery Controller: Load Balancer, SSL VPN, WAF & SSO	Citrix Application Delivery Controller: Load Balancer, SSL VPN, WAF & SSO	Citrix Application Delivery Controller: Load Balancer, SSL VPN, WAF & SSO	Citrix Application Delivery Contr Load Balancer, SSL VPN, WAF &
•	Software plan starts at			
	Create V	Create V	Create V	Bring your own license

3. Sélectionnez un plan NetScaler non FIPS ainsi qu'une licence, puis cliquez sur Créer.

= Micr	osoft Azure P Search resources, services, and docs (G+/)	2	Ę
Home >			
NetSca	er ADC 14.1 ☆ … Group		
netsealer	NetScaler ADC 14.1 🗢 Add to Favorites		
not/scale).	Cloud Software Group Virtual Machine		
	Free trial		
	Plan		
	NetScaler ADC 14.1 VPX Bring Your O Create Start with a pre-set configuration		
	Want to deploy programmatically? Get started		
Overview	Plans + Pricing Usage Information + Support Ratings + Reviews		
NetScaler A and pricing the hybrid c	DC (formerly NetScaler) is an enterprise-grade application delivery controller that delivers your applications q flexibility to meet your business' unique needs. Designed to provide operational consistency and a smooth us loud.	uickly, rel ser experi	liably, ence,

You can learn more building a robust, resilient application delivery infrastructure with NetScaler ADC on Microsoft Azure by reading the

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.

Home > NetScaler ADC 14.1 >

Create a virtual machine

Virtual machine name * 🕧	vpx-aan	
Region * 🕡	(US) East US	
Availability options 🕕	Availability zone	
	Zoner 1	
	You can now select multiple zones. Selecting multiple zones will create on per zone. Learn more a	ne VM
Security type (i)	Standard	``
Image * 🕕	NetScaler ADC 14.1 VPX Standard Edition - 5000 Mbps - x64 Gen1	~
	See all images Configure VM generation	
VM architecture ①	O Arm64	
	• x64	
	Arm64 is not supported with the selected image.	
Run with Azure Spot discount 🔅		
Size * 🕡	Standard_DS2_v2 - 2 vcpus, 7 GiB memory (\$ 1,743.24/month)	
	See all sizes	
Administrator account		
Authentication type 🕕	○ SSH public key	
	Password	
Username *	nsroot	
Password * 🕡	••••••	,
Confirm password * 🗊		
Inbound port rules		
Select which virtual machine network network access on the Networking tal	ports are accessible from the public internet. You can specify more limited or grand b.	ular
Public inbound ports * 🛈	 None Allow selected ports 	
Select inbound ports *	SSH (22)	```
	All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.	

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.

Basics	Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create
Define net inbound a Learn mor	work cor nd outbo e 🖻	nnectivity for your ound connectivity	r virtual machine b with security grou	y configuring net p rules, or place l	work interface o behind an existi	card (NIC) ing load b	settings. You can control por alancing solution.
Network	interfac	e					
When crea	iting a vi	rtual machine, a r	etwork interface w	vill be created for	you.		
Virtual net	work *	0	(new) vn	(-aan-vnet			
virtuariiet	WOIK	0	Create new	/			
Subnet *	(i)		(new) det	fault (10.6.0.0/24)			
	0						
Public IP	()		(new) vp	k-aan-ip			\
				•			
NIC netwo	ork securi	ity group 🕕	None				
			Basic	and			
				iceu			
Public inbo	ound po	rts * 🛈	O None				
			 Allow 	selected ports			
Select inbo	ound por	rts *	SSH (22)				
			A This reco	s will allow all IP a ommended for test ate rules to limit int	addresses to acc ing. Use the Adv bound traffic to k	cess your v vanced cor known IP a	rirtual machine. This is only ntrols in the Networking tab to ddresses.
Delete put deleted	olic IP an	d NIC when VM is	s 🗌				
Enable acc	elerated	networking 🔅	\checkmark				
Load bala	incing						
You can pl	ace this	virtual machine in	the backend pool	of an existing Az	ure load baland	cing soluti	ion. Learn more 🖻
Load balar	ncina op	tions 🗊	 None 				
	ienig op		◯ Azure	load balancer			
			Suppo	orts all TCP/UDP r	etwork traffic,	port-forw	arding, and outbound flows.
			U Applic	raffic load balanc	er for HTTP/HT	TPS with	URL-based routing, SSL

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.

≡ Microsoft Azure 🔎 Search	resources, services, and docs (G+/)		7 🗘 🚳	? 🙂
Home > citrix.netscalervpx-1vm-3nic-20	210204125107 > test-aan- > citrix.netscalervpx-1vm-3nic-202102	04125107 >		
✓ Search (Ctrl+/) «	+ Add $\equiv\equiv$ Edit columns 📋 Delete resource group 🖒 Refresh	ע Export to CSV ע	Open query	🖉 Assign ta
😥 Overview	↑ Essentials			
Activity log	Subscription (change) NSDev Platform CA	Deployments 2 Succeeded		
^ମ ୁ Access control (IAM)	Subscription ID	Location		
🔷 Tags	764bc6a9-7927-4311-8e67-ed073090cea3	South India		
🗲 Events	Tags (change) Click here to add tags			
Settings	Filter for any field Type == all × Location == all >	≺ + Add filter		
Deployments	Showing 1 to 22 of 22 records. Show hidden types ①		No grouping	~
Security				
Policies	Name ↑↓	Type ↑↓	_	Location
🔁 Properties	Citrix-adc-vpx-0	virtual machine		South Cer
🔒 Locks	< Previous Page 1 v of 1 Next >			

 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.

■ Microsoft Azure	ources, services, and docs	; (G+/)		D 🖓	P 🕸 ?	0
Home > citrix.netscalervpx-1vm-3nic-20210 citrix-adc-vpx-0 Virtual machine Virtual machine «	0204125107 > test-aan working Ø Attach network interf	> citrix.netscaler	px-1vm-3nic-20210204125107	> test-aan	> citrix-adc-vpx-(
Overview Activity log Access control (IAM) Tags	citrix-adc-vpx-nic01-0 IP configuration ① nsip (Primary)	citrix-adc-vpx-nic11	0 citrix-adc-vpx-nic12-0	1	v	
 Diagnose and solve problems Settings Networking 	Network Interface: Virtual network/subnet: Accelerated networ Inbound port rules	citrix-adc-vpx-nic01-(citrix-adc-vpx-virtual-netw king: Enabled	D Effective security rules fork/01-management-subnet	Topology NIC Public IP: 1 Load balan	3.66.88.43 NIC Pr	ivate IP: 172.17.40.5
Connect Disks Size	 Network security g Impacts 0 subnets, 1 Priority 	roup citrix-adc-vpx-nic(I network interfaces Name	01-nsg-0 (attached to network in Port	nterface: citrix-	adc-vpx-nic01-0) Source	Add inbound p
 Security Advisor recommendations 	1022	▲ ssh-22-rule	22	TCP	Internet	Any

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.	
\equiv Microsoft Azure		
Home > citrix.netscalervpx-1	vm-3nic-20210204125107 > test-aan > citrix.netscalervpx-1vm-3nic-20210204125107 > test-aan > citrix-adc-vpx-0	
citrix-adc-vpx Virtual machine	<-0 Networking	
	\ll β Attach network interface β Detach network interface	
Overview Activity log Access control (IAM)	citrix-adc-vpx-nic01-0 citrix-adc-vpx-nic11-0 citrix-adc-vpx-nic12-0	
	Welcome to Azure Cloud Shell Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session.	

2. À l'invite de commandes, exécutez la commande suivante :

1 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 :

1 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 :

1 az network nic update --name citrix-adc-vpx-nic01-0 -accelerated-networking false --resource-group rsgp1-aan 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.

≡ Microsoft Azure 🔎 Sea	irch resources, services, and doc	s (G+/)		D 다	🖉 🅸 ? 🙂	
Home > citrix.netscalervpx-1vm-3nic	-20210204125107 > test-aan	> citrix.netscalery	/px-1vm-3nic-20210204125107	' > test-aan	> citrix-adc-vpx-0	
citrix-adc-vpx-0	Networking					
	Attach network inter	face 🖉 Detach network	k interface			
Overview	A	-				
Activity log	citrix-adc-vpx-nic01-0	citrix-adc-vpx-nic11	0 citrix-adc-vpx-nic12-0			
Access control (IAM)	IP configuration ①	-		۲.	5	
Tags	nsip (Primary)	\checkmark				
Diagnose and solve problems	Network Interface	citrix-adc-vpx-nic01-(D Effective security rules	Topology		
Settings	Virtual network/subnet: Accelerated netwo	citrix-adc-vox-virtual-netw rking: Enabled	/ork/01-management-subnet	NIC Public IP: 1	3.66.88.43 NIC Privat	e IP: 172.17.40.5
Networking	Inhound nort rules	Outhound port rules	Application security groups	Load balan	cina	
🖉 Connect	inbound port rules	Outbound port fules	Application security groups	LUdu Dalah	ung	
B Disks	Network security of Impacts 0 subnets.	group citrix-adc-vpx-nic(1 network interfaces	01-nsg-0 (attached to network	interface: citrix-a	adc-vpx-nic01-0)	Add inbound p
👤 Size	Priority	Name	Port	Protocol	Source	Destinatio
Security	1022	A ssh_22_rule	22	тср	Internet	Any
Advisor recommendations	·		22	i ci	internet	Any

Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **désactivée**.

\equiv Microsoft Azure		esources, services, and docs	(G+/)			🕸 ? 😊		
Home > citrix-adc-vpx-0								
citrix-adc-v Virtual machine	px-0 Net	tworking					×	
P Search (Ctrl+/)	«	🖉 Attach network interf	ace 🔊 Detach network	c interface				
Access control (IAM)	•							^
🧳 Tags	- II.	citrix-adc-vpx-nic01-0	citrix-adc-vpx-nic11-	0 citrix-adc-vpx-nic12-0				
Diagnose and solve prob	blems	IP configuration (i)						
Settings		nsip (Primary)	\checkmark					
Networking		Network Interface:	citrix-adc-vpx-nic01-0	Effective security rules	Topology			
🖉 Connect		Virtual network/subnet: Accelerated networ	citrix-adc-vpx-virtual-netw king: Disabled	ork/01-management-subnet	NIC Public IP: 13.66	5.88.43 NIC Private IP:	172.17.40.5	
B Disks		L						
💶 Size		Inbound port rules	Outbound port rules	Application security group	os Load balancing	3		
Security		Network security g	roup citrix-adc-vpx-nic0)1-nsg-0 (attached to network	k interface: citrix-adc-	-vpx-nic01-0)	Add inbound port rule	
💠 Advisor recommendation	ns	Impacts 0 subnets, 1	I network interfaces					
Extensions		Priority	Name	Port	Protocol	Source	Destination	
🐔 Continuous delivery		1022	▲ ssh-22-rule	22	TCP	Internet	Any	
· · · · · · · · · · · · · · · · · · ·	*	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	*

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 0xfffff00 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).

> show interface 1/1	
Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) ; tlags=0xe060 <enabled, 802.1q="" heartbeat,="" up,=""> MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s LLDP Mode: NONE, LR Priority: 1024</enabled,>	#1
RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) NIC: InDisc(0) OutDisc(0) Ectls(0) Stalls(0) Hangs(0) Muted(0) Bandwidth thresholds are not set.	
> show interface 50/1	
Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2 Tags=0xe400 <enabled, 802.1q="" up,=""> MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000 LLDP Mode: NONE, LR Priority: 1024</enabled,>	
RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) NIC: InDisc(0) OutDisc(0) Ectls(0) Stalls(0) Hangs(0) Muted(0) Bandwidth thresholds are not set.	

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).

```
show interface 1/1
           Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 100/1, Datapath 100/1) #0
1)
           flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
MTU=1500, native vlan=10 MAC=00:0d:3a:9b:f2:1d,
                                                                                      uptime 10h49m10s
           LLDP Mode: NONE,
                                                              LR Priority: 1024
           RX: Pkts(310366) Bytes(98476082) Errs(0) Drops(0) Stalls(0)
TX: Pkts(44) Bytes(6368) Errs(0) Drops(0) Stalls(0)
           NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
 Done
show interface 100/1
          Interface 100/1 (CX4 VF Interface, SmartNIC, PV 1/1) #3
flags=0xe460 <ENABLED, UP, UP, 802.1g>
MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d uptime 10h49m11s
1)
           Actual: media FIBER, speed NONE, duplex FULL, tctl NONE, throughput
n
           LLDP Mode: NONE,
                                                              LR Priority: 1024
           RX: Pkts(1135870) Bytes(1487381079) Errs(0) Drops(0) Stalls(0)
           TX: Pkts(1143020) Bytes(143165922) Errs(0) Drops(0) Stalls(0)
NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
 Done
```

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.

1 add vlan 20

2. Liez un VLAN à l'interface PV.

```
bind vlan 20 – ifnum 1/1
1
2
3
     show vlan
4
5
     1) VLAN ID: 1
6
         Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
7
         Interfaces : LO/1
8
9
     2) VLAN ID: 10
                         VLAN Alias Name:
10
         Interfaces : 0/1 100/1
11
         IPs : 10.0.1.29 Mask: 255.255.255.0
12
     3) VLAN ID: 20
                        VLAN Alias Name:
13
         Interfaces : 1/1 100/2
14
```

Remarque:

L'opération de liaison VLAN n'est pas autorisée sur une interface VF accélérée.

1 bind vlan 1 -ifnum 100/1
2 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.

Custom deployment	
12 resources	Edit template Edit parameters
Deployment scope	
Select the subscription to manage deployed manage all your resources.	d resources and costs. Use resource groups like folders to organize and
Subscription * (i)	Nilber Platform CR annopagerwei@citric.com
Resource group * (i)	(New) HA-ILB
	Create new
Parameters	
Region * 🛈	West US 2 V
Admin Username 🛈	hariharana) 🗸
Admin Password * 🛈	······ ✓
Vm Size ①	Standard_DS3_v2 ~
Vm Sku 🛈	netscalerbyol V
Vnet Name ①	vnet01
Vnet Resource Group 🛈	
Vnet New Or Existing	new
Subnet Name-01 🛈	subnet_mgmt
Subnet Name-11 🛈	subnet_client
Subnet Name-12 🛈	subnet_server
Subnet Address Prefix-01 ①	10.11.0.0/24
Subnet Address Prefix-11 ①	10.11.1.0/24
Review + create < Previous	Next : Review + create >

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.

	HA-ILB ☆ Resource group		
»	$+$ Add $\equiv\equiv$ Edit columns 🛍 Delete resource group 🖒	Refresh 🞍 Export to CSV 😚 Open query	📔 🗑 Assign ta
	∧ Essentials		
	Subscription (change):		
	Subscription ID : 764bcdar9-7827-4311-6e67-ed0734996cm	a	
	Tags (change) : Click here to add tags		
	Filter by name Type == (all) X Location	== (all) X + Add filter	
	Showing 1 to 20 of 20 records. Show hidden types ①		
	Name ↑↓	Type ↑↓	Location \uparrow_{\downarrow}
	ADC-Availability-Set	Availability set	West US 2
	ADC-Azure-Load-Balancer	Load balancer	West US 2
	ADC-VPX-0	Virtual machine	West US 2
	ADC-VPX-0-management-public-ip	Public IP address	West US 2
	ADC-VPX-1	Virtual machine	West US 2
	📄 🛅 ADC-VPX-1-management-public-ip	Public IP address	West US 2
	ADC-VPX-NIC-0-01	Network interface	West US 2
	ADC-VPX-NIC-0-11	Network interface	West US 2
	ADC-VPX-NIC-0-12	Network interface	West US 2
	ADC-VPX-NIC-1-01	Network interface	West US 2
	ADC-VPX-NIC-1-11	Network interface	West US 2
	ADC-VPX-NIC-1-12	Network interface	West US 2
	ADC-VPX-NSG-0-01	Network security group	West US 2
	ADC-VPX-NSG-0-11	Network security group	West US 2
_	ADC-VPX-NSG-0-12	Network security group	West US 2
_	ADC-VPX-NSG-1-01	Network security group	West US 2

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 ig	p							
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
1)	10.11.0.5		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.11.1.5		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.4		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								

> 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 ig								
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
1)	10.11.0.4		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.11.1.6		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.5		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								



- 5. Une fois que les nœuds principal et secondaire sont UP et que l'état de synchronisation est SUC-CESS, 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.

≡	Microsoft Azure	₽ Search	resources, services, and docs	(G+/)			\geq	Ŗ	P	<u>ت</u>
Hom	e > Test_HA_Deployment	> ADC-A	zure-Load-Balancer							
•••	ADC-Azure-Load-Balancer Frontend IP configuration									
۶	Search (Ctrl+/)	~	🕂 Add 💍 Refresh							
🔶 C	Overview	^	₽ Filter by name							
Ξ Δ	Activity log		Name		IP address			Ru	ules cou	unt
<u>የ</u> ≳ △	Access control (IAM)		ADC-Load-Balancer-Front	and-IP-Configuration-rule	101114			1		
Ф т	ags		ADC LOBU Balancer From	end in configuration-rule	1011117					
PC	Diagnose and solve problem	s								

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.

Home > HA-ILB > ADC-Azure-Load-Balancer								
See ADC-Azure-Load-Balancer Load balancing rules								
	+ Add							
Activity log								
Access control (IAM)	Name	↑↓ Load balancing rule	↑↓ Backend pool	↑↓ Health probe	¢↓			
🔷 Tags	lbRule1	IbRule1 (TCP/80)	ADC-Load-Balancer-Backend-rule	e ADC-Load-Balancer-Health-Probe-r	ule 🔹			
Diagnose and solve problems								
Settings								
Frontend IP configuration								
Backend pools								
👔 Health probes								
E Load balancing rules								

• La règle d'équilibrage de la charge de travail (LBrule1) utilise le port 80, par défaut.

IbRule1 ADC-Azure-Load-Balancer	
🖫 Save 🗙 Discard 🛍 Delete	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.	
Name *	
lbRule1	
IP Version *	
● IPv4	
Frontend IP address * ①	
10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule)	\sim
Protocol	
Port *	
80	
Backend port * ①	
80	

• 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.

lbRule1	
ADC-Azure-Load-Balancer	
🔚 Save 🔀 Discard 🛍 Delete	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health p considers healthy receive new traffic.	probe
Name *	
lbRule1	
IP Version * IPv4 IPv6 	
Frontend IP address * ①	
10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule)	\sim
Protocol TCP UDP	
Port *	
443	
Backend port * ①	
443	
Backend pool ①	
ADC-Load-Balancer-Backend-rule (2 virtual machines)	\sim
Health probe ①	
ADC-Load-Balancer-Health-Probe-rule (TCP:9000)	\checkmark
Session persistence	
	\sim
Idle timeout (minutes) ①	
0	4
Floating IP (1)	
Enabled	

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.

ADC-Azure-Load-Balancer Frontend IP configuration						
		🕂 Add 💍 Refresh				
Activity log	•	P Filter by name				
Access control (IAM)		Name	IP address			
🔶 Tags		ADC-Load-Balancer-Frontend-IP-Configuration-rule	10.11.1.4			
Diagnose and solve problem	s					
Settings	0					
Frontend IP configuration						

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**.

Home > HA-ILB > ADC-Azure-Load-Balancer >					
Add frontend IP address					
	0				
Name *	ILB-Front-End-IP-2				
Virtual network	vnet01				
Subnet	subnet_client (10.11.1.0/24)				
Assignment	Dynamic Static				
Add					

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.

Home > HA-ILB > ADC-Azure-Load-Balancer							
ADC-Azure-Load-Balancer Frontend IP configuration X							
م	Search (Ctrl+/)		🕂 Add 💍 Refresh				
	Overview		O Filter by name				
	Activity log		Name	IP address		Rules count	
	Access control (IAM)		ADC Load Balancer Fronte	10 11 1 /		1	
	Tags		ILR Front End IR 2	10.11.1.4		0	
Þ	Diagnose and solve problems		HEB-FIONT-End-IP-2	10.11.1.7		0	

4. Sur la page Azure Load Balancer, sélectionnez Règles d'équilibrage de charge, puis cliquez

sur **Ajouter**.

Home > HA-ILB > ADC-Azure-Load-Balancer							
See ADC-Azure-Load-Balancer Load balancing rules							
	+ Add						
💠 Overview 🔶	${\cal P}$ Search load balancing rules						
Activity log	Name	\uparrow_{\downarrow}	Load balancing rule				
Access control (IAM)	lbRule1		lbRule1 (TCP/80)				
🗳 Tags							
Diagnose and solve problems							
Settings							
Frontend IP configuration							
Backend pools							
👔 Health probes 👔							
送 Load balancing rules							

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**.

Home > HA-ILB > ADC-Azure-Load-Balancer >	
Add load balancing rule	
ADC-Azure-Load-Balancer	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port	
combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.	
Name *	
Ibrule2	
IP Version *	
2 Frontend IP address * (i)	
10.11.1.7 (ILB-Front-End-IP-2)	\checkmark
Port *	
Backend port 🖌 🕕	
443	
Backend pool ① 5	
ADC-Load-Balancer-Backend-rule (2 virtual machines)	\checkmark
Health probe	
ADC-Load-Balancer-Health-Probe-rule (TCP:9000)	\checkmark
Nule	`
Idle timeout (minutes) ①	
	4
Floating IP ①	
Disabled Enabled	
ОК	

6. Maintenant, la **configuration IP du frontend** affiche la règle d'équilibrage de charge appliquée.

Hon	Home > HA-ILB > ADC-Azure-Load-Balancer					
م	Search (Ctrl+/)		🕂 Add 🖒 Refresh			
	Overview	^	O liitar by name			
	Activity log		Name	IP address	Rules	count
	Access control (IAM)		ADC-Load-Balancer-Frontend-IP-Configurati	10.11.1.4	1	
*	Tags		ILB-Front-End-IP-2	10.11.1.7	1	
ß	Diagnose and solve problems					
Set	tings					
	Frontend IP configuration					

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

```
1 enable feature aaa LB SSL SSLVPN
2 enable ns mode MBF
3 add vpn vserver vpn_ssl SSL 10.11.1.4 443
4 add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
5 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.

Basics VM Configurations Net	work and Additional Settings Review + create	
Project details		
Select the subscription to manage deploy manage all your resources.	ed resources and costs. Use resource groups like folders to organize and	
Subscription * 🕕	xm-test-cs-shared	/
Resource group * (i)	(New) Test_HA_Internet	~
Instance details		
Region * (i)	South India	/
Citrix ADC Release Version * 🛈	12.113.0	
License Subscription ①	Bring Your Own License	
Virtual Machine name * 🛈	citrix-adc-vpx	
Administrator account		
Username * 🛈	praveenk ~	*
Authentication type * 🕡	Password SSH Public Key	
Password * (i)		-
Confirm password *	······	🖌 🔮 Passwor
Review + create < Previous	Next : VM Configurations >	

5. Cliquez sur Suivant : Configurations de machines virtuelles.

Basics	VM Configurations	Network and Additional Settings Review + create	
Project de	etails		
Select the manage al	subscription to manage d I your resources.	eployed resources and costs. Use resource groups like folders to organize and	
Subscriptio	on* 🛈	xm-test-cs-shared	\checkmark
Re	source group * 🕡	(New) Test_HA_Internet Create new	\sim
Instance	details		
Region *	(i)	South India	\sim
Citrix ADC	Release Version * 🛈	12.113.0	
License Sul	oscription 🛈	Bring Your Own License	
Virtual Mad	hine name * 🛈	citrix-adc-vpx	
Administr	ator account		
Username	* (i)	praveenk	\checkmark
Authentica	tion type * 🗊	 Password SSH Public Key 	
Password *	0		\checkmark
Confirm pa	ssword *		V Passwor
Review	+ create < Prev	ious Next : VM Configurations >	

- 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

Virtual machine size * 🛈	1x Standard DS3 v2 4 vcpus, 14 GB memory Change size
OS disk type ①	Premium_LRS
Assign Public IP (Management) 🛈	• Yes
Assign Public IP (Client traffic) 🗊	• Yes
Unique public IP domain name suffix * 🗊	d7a2c4d49e
Azure Monitoring Metrics 🛈	C Enabled
	Disabled
Backend Autoscale 🕠	C Enabled
	Disabled
Review + create < Previous	Next : Network and Additional Settings >

8. Sur la page **Paramètres réseau et supplémentaires**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.

	vivi configurations	Network and Additional Settings Review + create	
Boot diag	nostics		
Diagnostic	storage account * 🕡	(new) citrixadcvpxd7a2c4d49e	\sim
-	-	Create New	
Network S	Settings		
Configure	virtual networks		
Virtual net	work * 🗊	(new) citrix-adc-vpx-virtual-network	\sim
		Create new	
Manageme	ent Subnet * 🛈	(new) 01-management-subnet (10.17.4.0/24)	\sim
Client Subr	net * 🛈	(new) 11-client-subnet (10.17.5.0/24)	\sim
Server Subi	net * 🛈	(new) 12-server-subnet (10.17.6.0/24)	\sim
Public IP ((Management)		
Manageme	ent Public IP (NSIP) * ()	(new) citrix-adc-vpx-nsip	\sim
-		Create new	
Manageme	ent Domain Name 🕕	citrix-adc-vpx-nsip-d7a2c4d49e	~
Manageme	ent Domain Name 🛈	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.	cloudapp.azure.com
Manageme Public IP (ent Domain Name ① (Clientside)	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.	cloudapp.azure.com
Manageme Public IP (Clientside F	ent Domain Name ① (Clientside) Public IP (VIP) * ①	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.t	<pre>cloudapp.azure.com</pre>
Manageme Public IP (Clientside F	ent Domain Name ① (Clientside) Public IP (VIP) * ④	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new	<pre>cloudapp.azure.com</pre>
Manageme Public IP (Clientside F Clientside [ent Domain Name ① (Clientside) Public IP (VIP) * ① Domain Name ①	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.d (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e	<pre>cloudapp.azure.com</pre>
Manageme Public IP (Clientside F Clientside I	ent Domain Name ① (Clientside) Public IP (VIP) * ① Domain Name ①	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.d (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia.d	<pre>cloudapp.azure.com</pre>
Manageme Public IP (Clientside F Clientside I Public Inbo	ent Domain Name ① (Clientside) Public IP (VIP) * ① Domain Name ① ound Ports (Manageme	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only)	<pre>cloudapp.azure.con</pre>
Manageme Public IP (Clientside I Clientside I Public Inbo	ent Domain Name ① (Clientside) Public IP (VIP) * ① Domain Name ① ound Ports (Management for Management public I	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only) p ① None	cloudapp.azure.com
Manageme Public IP (Clientside F Clientside I Public Inbe Ports open	ent Domain Name ① (Clientside) Public IP (VIP) * ① Domain Name ① ound Ports (Management for Management public I	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only) p () None (e) ssh (22)	<pre>cloudapp.azure.com</pre>

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.

Resource group	
$+$ Add $\equiv\equiv$ Edit columns 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV	V $~\%$ Open query $\mid ~\oslash$ Assign tags $ ightarrow$ Move $ ightarrow$ [
✓ Essentials	
Filter by name Type == all X Location == all X + Add filter	
Showing 1 to 23 of 23 records. 🔲 Show hidden types 🛈	
Name 🗘	Type ↑↓
🖳 🖳 citrix-adc-vpx-0	Virtual machine
citrix-adc-vpx-0_OsDisk_1_6749f4a73c534051b0602ba6e3ec2cf8	Disk
citrix-adc-vpx-1	Virtual machine
citrix-adc-vpx-1_OsDisk_1_8fde7770497b4dbdba385715e81505c9	Disk
🕼 citrix-adc-vpx-nic01-0	Network interface
🕼 citrix-adc-vpx-nic01-1	Network interface
🗌 🎈 citrix-adc-vpx-nic01-nsg-0	Network security group
citrix-adc-vpx-nic01-nsg-1	Network security group
Gitrix-adc-vpx-nic11-0	Network interface
citrix-adc-vpx-nic11-1	Network interface
🗌 💎 citrix-adc-vpx-nic11-nsg-0	Network security group
🗌 🎈 citrix-adc-vpx-nic11-nsg-1	Network security group
C w citrix-adc-vpx-nic12-0	Network interface
C G citrix-adc-vpx-nic12-1	Network interface
Citrix-adc-vpx-nic12-nsg-0	Network security group
Citrix-adc-vpx-nic12-nsg-1	Network security group
citrix-adc-vpx-nsip-0	Public IP address
citrix-adc-vpx-nsip-1	Public IP address
Citrix-adc-vpx-vip	Public IP address
Citrix-adc-vpx-vip-load-balancer	Load balancer
Citrix-adc-vpx-virtual-network	Virtual network
citrix-adc-vpx-vm-availability-set	Availability set

- 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		NetScaler IP	Active	 Fnabled	Fnabled	 NД	Fnabled		
2)	10.18.1.5	ŏ	SNIP	Active	Enabled	Enabled	NA	Enabled		
3)	10.18.2.4		SNIP	Active	Enabled	Enabled	NA	Enabled		
Done										
∖ eh h	a node									
2 511 11	Node TD:	0								
-/	TP.	10 18 0 4 (ns-	vpx())							
	Node State	: IIP	(Diro)							
	Master Sta	Master State: Primary								
	Fail-Safe Mode: OFF									
	INC State FNABLED									
	Sync State: FNABLED									
	Propagatio	Propagation: ENABLED								
	Enabled In	Frebled Interfaces • 0/1 1/1 1/2								
	Disabled I	Disabled Interfaces : None								
	HA MON ON	HA MON ON Interfaces : None								
	HA HEARTBE	HA HEARTBELT OFF Interfaces : None								
	Interfaces on which heartbeats are not seen : 1/1 1/2									
	Interfaces	Interfaces causing Partial Failure: None								
	SSL Card S	SSL Card Status: NOT PRESENT								
	Sync Statu	Svnc Status Strict Mode: DISABLED								
Hello Interval: 200 msecs Dead Interval: 3 secs										
	Node in th	is Master Stat	e for: 0:3:34	:21 (day	s:hrs:m	in:sec)				
2)	Node ID:	1								
	IP: 10.18.0.5									
	Node State	Node State: UP								
	Master State: Secondary									
	Fail-Safe	Fail-Safe Mode: OFF								
	INC State: ENABLED									
	Sync State	Sync State: SUCCESS								
	Propagatio	Propagation: ENABLED								
	Enabled In	Enabled Interfaces : 0/1 1/1 1/2								
	Disabled I	Disabled Interfaces : None								
	HA MON ON	HA MON ON Interfaces : None								
	HA HEARTBE	AT OFF Interfa	ces : None							
	Interfaces	on which hear	tbeats are no	t seen :	1/1 1/2	2				
	Interfaces	causing Parti	al Failure: N	one						
	SSL Card S	tatus: NOT PRE	SENT							
Done										

Sur le nœud secondaire (citrix-adc-vpx-1)



- 12. Une fois que les nœuds principal et secondaire sont UP et que l'état Synchronisation est SUC-CESS, 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**.

Home > Test_HA_Template > alb Frontend IP co	onfiguration			×
Search (Ctrl+/) «	+ Add 🕐 Refresh			
V Overview				
Activity log	Name	IP address	Rules count	
Access control (IAM)	1			
Tags	ipcont-11	52.172.55.197 (alb-publicip)	I	
Diagnose and solve problems				
Settings				
Frontend IP configuration				
Backend pools				

14. Ajoutez la règle de sécurité entrante pour le port 443 du serveur virtuel dans le groupe de sécurité réseau des deux interfaces clientes.

Home > Test_HA_Template > ns-vpx-nic0-11 >								
ns-vpx-nic-nsg0-11	\$							×
✓ Search (Ctrl+/) «	$ ightarrow$ Move \lor 📋 D	elete 💍 Refresh						
Overview								
Activity log	Resource group (chan	ge) : Test_HA_Template			Custom security ru	iles:2 inbound, 0 ou	tbound	
Access control (IAM)	Location	: South India			Associated with	: 0 subnets, 1 net	work interfaces	
Taos	Subscription (change)	: xm-test-cs-shared						
Diagnose and solve problems	Subscription ID	: db99d808-6e89-480a	-96ae-3275fe	61eed4				
	Tags (change)	: Click here to add tag	5					
Settings	Inbound security rule	25						
📩 Inbound security rules	Priority	Name		Port	Protocol	Source	Destination	Action
📩 Outbound security rules	1000	🔺 default-allow-ssh		22	TCP	Any	Any	Allow
Network interfaces	1010	Port_443		443	TCP	Any	Any	Allow
Subnets	65000	AllowVnetinBound		Any	Any	VirtualNetwork	VirtualNetwork	Allow
Properties	65001	AllowAzureLoadBalanc	erinBound	Any	Any	AzureLoadBaland	cer Any	Allow
A Locks								
Home > Test_HA_Template > ns-vpx-nic1	-11 > \$							×
✓ Search (Ctrl+/) «	→ Move ∨ 📋 Dele	ete 💍 Refresh						
Overview								
Activity log	Resource group (change)	: Test_HA_Template			Custom security rule	es:2 inbound, 0 outb	ound	
Access control (IAM)	Location	: South India			Associated with	: 0 subnets, 1 netw	ork interfaces	
Tags	Subscription (change)	: <u>xm-test-cs-shared</u>						
Diagnose and solve problems	Subscription ID	: db99d808-6e89-480a-96	ae-3275fe61e	ed4				
Cattings	Tags (change)	: Click here to add tags						
* Inhound conurity rules	Inbound security rules							
Inbound security rules	Priority	Name	Port	Protocol	Source	Destinat	ion Action	
Outbound security rules	1000	A default-allow-ssh	22	TCP	Any	Any	Allow	
INEtwork Interfaces	1010	Port_443	443	TCP	Any	Any	Allow	
v subnets	65000	AllowVnetInBound	Any	Any	VirtualNetv	vork VirtualN	etwork 🔮 Allow	
Properties	65001	AllowAzureLoadBalancer	Any	Any	AzureLoad	Balancer Any	Allow	
Locks	65500	DenyAllInBound	Any	Any	Any	Any	Ø Deny	
🕎 Export template								

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.

■ Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)
Home > Test_HA_Template > alb >	
IbRule1	
🖫 Save 🗙 Discard 📋 Delete	
IPv4 IPv6	
Frontend IP address * ①	
52.172.55.197 (ipconf-11)	~
Protocol TCP UDP	
Port *	
443	
Backend port * ①	
443	
Backend pool 🕕	
bepool-11 (2 virtual machines)	\sim
Health probe 🕕	
probe-11 (TCP:9000)	~
Session persistence 🕕	
None	~
Idle timeout (minutes) ①	
0	4
Floating IP (direct server return) ①	
Enabled	

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

```
1 enable feature aaa LB SSL SSLVPN
2 add ip 52.172.55.197 255.255.255.0 -type VIP
3 add vpn vserver vpn_ssl SSL 52.172.55.197 443
4 add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
5 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. Home > ansible_rg_ganeshb_1611818039 > New > Load Balancer >

Create load balancer

r roject details		
Subscription *		\sim
Resource group *		\sim
	Create new	
Instance details		
Name *	internal-load-balancer	~
Region *	(US) West US 2	\sim
Туре * 🕕	Internal Public	
SKU * 🕕	● Basic ○ Standard	
Configure virtual network.		
Virtual network * ①	automation_network	\sim
Subnet *	ClientSubnet (192.168.2.0/24)	\sim
	Manage subnet configuration	
IP address assignment *	🔵 Static 💿 Dynamic	

• Pour créer un équilibreur de charge externe, choisissez le type d'équilibreur de charge comme étant **Public** et créez l'adresse IP publique ici.

Microsoft Azure	▷ Search resources, services, and docs (G+/)				
me > Load balancing - help me choose (Preview) >					
Create load ba	ancer				
Туре * 🕕	O Internal Public				
SKU * 🕕	• Standard O Basic				
	 Microsoft recommends Standard SKU load balancer for production workloads. Learn more about pricing differences between Standard and Basic SKU a³ 				
Tier *	• Regional O Global				
Public IP address Public IP address * ①	• Create new 🔿 Use existing				
Public IP address name *					
Public IP address SKU	Standard				
IP address assignment	O Dynamic () Static				
Availability zone *	×				
Add a public IPv6 address	1 No Yes				
Routing preference (i)	Microsoft network Internet				
Review + create	< Previous Next : Tags > Download a template for automation				

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.

new-alb-ilb Fronter	nd IP configuration		
	🕂 Add 💍 Refresh		
Overview	P Filter by name		
Activity log	Name	IP address	Rules count
Access control (IAM)	LoadBalancerFrontEnd	52.172.96.71 (ip-alb-ilb)	0
🗳 Tags	Loughancerrontena		
Diagnose and solve problems			
Settings			
Frontend IP configuration			
Sackend pools			
P Health probes			
३ Load balancing rules			
lnbound NAT rules			
1 A.M. 1			

- 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.

```
1 add lb vserver <name> <serviceType> [<ILB Frontend IP address>]
      [<port>]
```

Exemple

1 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.

1 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).

1 add nsip <ILB Frontend IP address> -type <type>

Exemple

1 add nsip 52.172.96.71 -type vip

2. Ajoutez un IPSet sur les nœuds principaux et secondaires.

1 add ipset <name>

Exemple

1 add ipset ipset1

3. Liez les adresses IP au jeu d'adresses IP.

1 bind ipset <name> <ILB Frontend IP address>

Exemple

1 bind ipset ipset1 52.172.96.71

4. Définissez le serveur virtuel LB existant pour qu'il utilise IPSet.

1 set lb vserver <vserver name> -ipset <ipset name>

Exemple

1 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 sousréseaux 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.

Azure settings		
Subscription * 🛈		\checkmark
Resource group * ①		\checkmark
	Create new	
Location * ①	(US) East US	\checkmark
General		
Resource name * 🛈	avs-cloud1	\checkmark
SKU * 🕕	AV36 Node	\sim
ESXi hosts * 🛈	0	3
		\$11,929.68 estimated monthly total
Address block * 🛈	192.168.0.0/20	
Virtual Network	avs-cloud-vnet1	\sim
	Create new Only Virtual Networks with a valid subnet wit are available for selection. For details about a network, refer to details here	h the name "GatewaySubnet" dding subnet in a virtual

- 4. Cliquez sur **Réviser + Créer**.
- 5. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.

Home >
Create a private cloud — ×
*Basics Tags Review + create
Legal Terms
Azure VMware Solution is an Azure Service licensed to you as part of your Azure subscription and subject to the terms and conditions of the agreement under which you obtained your Azure subscription (https://azure.microsoft.com/support/legal/). The following additional terms also apply to your use of AVS:
Data Retention. AVS does not currently support retention or extraction of data stored in AVS Clusters. Once an AVS Cluster is deleted, the data cannot be recovered as it terminates all running workloads, components, and destroys all Cluster data and configuration settings, including public IP addresses.
Professional Services Data Transfer to VMware. In the event that you contact Microsoft for technical support relating to Azure VMware Solution and Microsoft must engage VMware for assistance with the issue, Microsoft will transfer the Professional Services Data and the Personal Data contained in the support case to VMware. The transfer is made subject to the terms of the Support Transfer Agreement between VMware and Microsoft, which establishes Microsoft and VMware as independent processors of the Professional Services Data. Before any transfer of Professional Services Data to VMware will occur, Microsoft will obtain and record consent from you for the transfer.
VMware Data Processing Agreement. Once Professional Services Data is transferred to VMware (pursuant to the above section), the processing of Professional Services Data, including the Personal Data contained the support case, by VMware as an independent processor will be governed by the VMware Data Processing Agreement for Microsoft AVS Customers Transferred for L3 Support. You also give authorization to allow your representative(s) who request technical support for Azure VMware Solution to provide consent on your behalf to Microsoft for the transfer of the Professional Services Data to VMware.
AVS consumption You authorize Microsoft to share with VMware your status as a customer of AVS and associated AVS deployment and usage information.
By clicking "Create", you agree to the above additional terms for AVS. If you are an individual accepting these terms on behalf of an entity, you also represent that you have the legal authority to enter into these additional terms on that entity's behalf.
Azure settings
Create Previous Next

6. Cliquez sur **Créer**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.

Home >	
Seployment	0609092342 Overview 🖈 … ×
	📋 Delete 🚫 Cancel 🏦 Redeploy 🖒 Refresh
👶 Overview	♂ We'd love your feedback! \rightarrow
🔄 Inputs	
is Outputs €	Your deployment is complete
📄 Template	Deployment name: Microsoft.AVS-20210609092342 Start time: 6/9/2021, 9:23:48 AM Subscription: Resource group: avs-cloud-new
	✓ Deployment details (Download)
	∧ Next steps
	Go to resource

7. Cliquez sur **Aller à la ressource**pour vérifier le cloud privé créé.

AVS Private cloud 🖉 …)
	🛛 📋 Delete		
Overview	∧ Essentials		JSON Vie
Activity log	Resource group (change) avs-cloud-new	ESXi hosts 3	
 Access control (IAM) Tags 	Status Succeeded	Primary peering subnet 192.168.0.232/30	
Diagnose and solve problems	Location East US	Secondary peering subnet 192.168.0.236/30	
Settings	Subscription (change)	Private Cloud Management network 192.168.0.0/26	
Locks	Subscription ID	vMotion network 192.168.1.128/25	
Manage	7640C6a9-7927-4311-8e67-ed073090Cea3		
👷 Connectivity	Tags (change) Click here to add tags		
Identity			

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.

Home > Create a resource >	
Microsoft Windows 10 🖈 … Microsoft Corporation	×
Microsoft Windows 10 \heartsuit Add to Favorites Microsoft Corporation * * * * 4.5 (6 ratings) Select a plan Windows 10 Pro, Version 2004 \checkmark Create Start with a pre-set configuration	
Overview Plans Usage Information + Support Reviews	
This software is provided by Microsoft. Use of this software in Microsoft Azure is not permitted except under a volume licensing agreement with Create, I acknowledge that I or the company I work for is licensed to use this software under a volume licensing agreement with Microsoft and th will be subject to that agreement.	Microsoft. By clicking hat the right to use it

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.

Home > Create a resource > Mic	crosoft Windows 10 >	
Create a virtual machin	ne …	
Basics Disks Networking	Management Advanced Tags Review + create	
Create a virtual machine that r marketplace or use your own of create to provision a virtual m customization. Learn more of Project details Select the subscription to man	runs Linux or Windows. Select an image from Azure customized image. Complete the Basics tab then Review + achine with default parameters or review each tab for full nage deployed resources and costs. Use resource groups like	
Subscription -		
Subscription *		
Resource group * 💿	Create new	
Instance details		
Virtual machine name * 🕤	Windows-jumpbox	
Region * 💿	(US) East US	
Availability options 💿	No infrastructure redundancy required	
Image * 💿	Windows 10 Pro, Version 2004 - Gen1 See all images	
Azure Spot instance 🕤		
Size * 💿	Standard_D2 - 2 vcpus, 7 GiB memory (US\$67.16/m See all sizes	
Administrator account		
Username * 💿	[]	
Password *	······	
Confirm password *	······	
Inbound port rules Select which virtual machine n specify more limited or granul Public inbound ports •	network ports are accessible from the public internet. You can lar network access on the Networking tab. O None	
	 Allow selected ports 	
Select inbound ports *	RDP (3389)	
	▲ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.	
Licensing		
 I confirm I have an eligible multi-tenant hosting rights 	Windows 10 license with s. •	
Review multi-tenant hosting ri	ights for Windows 10 compliance	
Review + create < Pr	Previous Next : Disks >	

- 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.

All services > Resource groups > Oviv	vekc-avs-demo > avs-cloud		
AVS Private cloud Identity	/ \$		×
, Search (Ctrl+/) «	Login credentials		
▼ Tags	vCenter credentials		
Diagnose and solve problems	Web client URL ①	https://192.168.0.2/	Copy to clipboard
Settings	Admin username 🛈	cloudadmin@vsphere.local	b
🔒 Locks	Admin password ③		
Manage	Continue to an horizon (C)	0117045414040470074150545740074130004175	
흤 Connectivity	Certificate thumpprint ()	B237D03A11B09C2907A35850E3CDB7A12B0BA2FE	U
🖳 Identity	NSX-T Manager credentials		
Clusters	Web client URL ①	https://192.168.0.3/	Ø
Workload Networking	Admin username 🛈	admin	Ø
4 Segments	Admin password ①		
TT DHCP	Certificate thumbprint ()	2362FAA1F4CAE9952646F2B62DF1BB887AC7CF368	0
Port mirroring			

2. Lancez vSphere client en saisissant l'URL du client Web vCenter.

ting Started vSphere Flash-based Web Client is deprecated in vSphere 6.7. We recommend Iching to the all-new modern HTML5-based vSphere client as the primary client and only erting to the Flash-based Web Client when necessary.	
ting Started vSphere Flash-based Web Client is deprecated in vSphere 6.7. We recommend tching to the all-new modern HTML5-based vSphere client as the primary client and only erting to the Flash-based Web Client when necessary.	
vSphere Flash-based Web Client is deprecated in vSphere 6.7. We recommend tching to the all-new modern HTML5-based vSphere client as the primary client and only erting to the Flash-based Web Client when necessary.	
LAUNCH VSPHERE .IENT (HTML5)	
LAUNCH VSPHERE WEB CLIENT (FLEX) Deprecated	
umentation	
/Mware vSphere Documentation Center	
Functionality Updates for the vSphere Client (HTML5)	

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.

 ✓ vSphere - vc.de7510d9c7d8485 ✓ → C ▲ Not secur 	<pre>x + tos://192.168.0.2/ui/#?exten</pre>	ionId=vsphere core inventory se	rverObiectViewsExtension&obiectId=	urnymomi:Folder.aroup.d1:d77	ece11-494 🗘 👌	- 0 6	×
vm vSphere Client M	enu 🗸 🛛 📿 Search in all enviro	ments		C @~	cloudadmin@VSPHERE.L0	ICAL Y	٢
□ □ □ ○	vc.de7510d9c7d848 Summary Monitor Configure	5cb31194.eastus.avs.az Permissions Datacenters	Hosts & Clusters VMs Datast	tores Networks Linked vC	enter Server Systems	Extensions	
 ✓ SDC-Datacenter ✓ Custer-1 ● esx03-r09.p03.de7 ● esx04-r02.p03.de7 ● esx14-r15.p03.de75 	Virtual Machines: 0 Hosts: 3				CPU Used 13.67 GHz Memory Used 255.83 GB Storage Used 6.52 TB	Free: 234.79 GH Capacity: 247.86 GH Free: 1.45 T Capacity: 1.68 T Free: 31.61 T Capacity: 38.42 T	た た 18 18 18 18 18 18
	Custom Attributes Attribute	Value	Tags Assigned Teg	Category	Description	^	
Recent Tasks Alarms	1		b v d			3 *	×
Target vc.de75	 ✓ Status ✓ Status ✓ Completed 	Details V Initiator HCX Disaster Recovery Plugin VSPHEI (com.xmware.hybridity VSPHEI	Outled For RELOCALlysph 10 ms	✓ Start Time ↓ ✓ Com 05/02/2021, 3:17:18 PM 05/0	npietion Time v Serv 02/2021, 3:17:19 PM vc.de	# 17510d9c7d8485c	*

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.

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.

All services > Resource groups > Ov avs-cloud Segme AVS Private doud	ivekc-avs-demo > avs-cloud ents ダーー				Add segment	×
P Search (Ctrl+/)	🕂 🕂 Add 🔋 Delete 💍 Refre	sh				
Overview	* D Filter by name	Name : All IP Address	All		Segment name * management	~
Activity log	Segment name 1	Connected gateway 74	Gateway IP ↑↓	DHCP r	Connected gateway	
Access control (IAM) Tags	TNT22-HCX-UPUNK	TNT22-T1	192.168.3.1/26		T1 TNT22-T1	
Diagnose and solve problems Settings					Type Overlay segment	
🔒 Locks					Subnet Gateway *	
Manage					192.168.4.1/24	
ldentity					DHCP ranges (optional)	
Clusters					Enter DHCP ranges	
Workload Networking						
Segments						
TT DHCP						
Port mirroring						Example: 10.1.1.0/24 or 10.1.1.10-10.1.1.100
O DNS						
Monitoring		0			OK Cancel	

2. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification NSX-T Manager.

All services > Resource groups > Ovi	ivekc-avs-demo > avs-cloud	
AVS Private doud	у 🖈 …	
Search (Ctrl+/) Gags Diagnose and solve problems	Login credentials vCenter credentials	
Settings	Web client URL ③	https://192.168.0.2/ cloudadmin@vsphere.local
Manage	Admin password () Certificate thumbprint ()	B237D65A11B69C2907A35856E3CDB7A1280BA2FE
 Identity Clusters 	NSX-T Manager credentials Web client URL ①	b https://192.168.0.3/
Workload Networking	Admin username ① Admin password ①	admin
DHCP Port mirroring	Certificate thumbprint ③	2362FAA1F4CAE9952646F2B62DF1BB87AC7CF368

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.

🖻 🛛 💋 vSphere - vc.de7510d9c7d8485 x	< .	NSX		× +					-
\leftarrow \rightarrow C \blacktriangle Not secure	https	://192	.168.0	.3/nsx/#/app/networks/segments/	/module/home			10 L	÷ @
vm NSX-T							QĹ		ad
Home Networking Secur	rity	Invent	tory	Plan & Troubleshoot System	Advanced Networking & Security				
Network Overview Connectivity	ADD	SEGM		SEGMENT PROFILES		EXPAND ALL	Filter by Nar	ne, Path or m	tore
🔁 Tier-O Gateways	Г			Segment Name	Connected Gateway & Type		Subnets	Sta	tus
🔁 Tier-1 Gateways	÷	>	~	client	TNT22-T1 Tier1 - Flexible		1	•	Up C
🕫 Segments	÷	>	~	management	TNT22-T1 Tier1 - Flexible		1	•	Up C
Network Services	3	>	æ	server	TNT22-T1 Tier1 - Flexible		1	•	Up C
@ VPN	:	>	ଜଣ୍ଡ	TNT22-HCX-UPLINK	TN122-11 Tier1 - Flexible		1	•	Up C
∃• NAT	1	>	oef	TNT22-T0-PRIVATE01-LS	None - Flexible			•	Up C
 Ŷ Load Balancing ♦ Forwarding Policies 	:	>	4	TNT22-T0-PRIVATE02-LS	None - Flexible			•	Up C

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**.

Sphere - NSVPX-ESX-13.0-7	life 🗙 🚾 NSX	× +		
← → C ▲ Not sect	ure https://192	2.168.0.2/ui/#?extensionId=vsphere.core.inve	ntory.serverObjectViewsExtension&objectId=	um:vmomi:VirtualMachine:vm-53:d77ece
vm vSphere Client	Menu 🗸 🔤 🤇	2 Search in all environments		C. (?) v doudad
₩ ₽ ₽ ₽ ₩ ₩ vc.de7510d9c7d8485cb311.	B NSV	Edit Settings NSVPX-ESX-13.0-79 Virtual Hardware VM Options	.64_nc_64	×
V SDDC-Datacenter				ADD NEW DEVICE
esx03-r09.p03.de7		> CPU	2 ~	0
esx04-r02.p03.de7	POwn	> Memory	2 GB V	
D NSVPX-ESX-13.0-7_		> Hard disk 1	20 GB ~	
	Launch Wei Launch Ren	> SCSI controller 0	LSi Logic Parallel	
		> Network adapter 1	management ~	Connect
	VM Hard	> New Network *	client ~	Connect
	Related (> New Network *	server ~	Connect
	Clust	> Video card	Specify custom settings \vee	
	Host	VMCI device	Device on the virtual machine PCI bus that provid	es support for the
	Netw		virtual machine communication interface	
Recent Tasks Alarms		> Other	Additional Hardware	
Tesk Name - Target	-			Completion Ter
Import OVF package Cluste	K-ESX-13:0-7			CANCEL OS 02/2021.4

7. Cliquez sur **Terminer** pour commencer l'installation d'une appliance virtuelle sur VMware SDDC.

Silod9c7d8485cb311 Select an arme and Silod9c7d8485cb311	plate Ready to complete folder Click Finish to start creat	ion.
OC-Datacenter Cluster-1	Provisioning type	Deploy from template
esx04-r02 p03 de7 7 Ready to complete	Name	NSVPX-ESX-13.0-79.64_nc_64
g esx14-r15.p03.de75.	Template name	NSVPX-ESX-13.0-79.64_nc_64
	Download size	599.9 MB
	Size on disk	20.0 GB
	Folder	SDDC-Datacenter
	Resource	Cluster-1
	Storage mapping	1
	All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
	Network mapping	1
	VM Network	management
isks Alarms	IP allocation settings	
~ Target	IP protocol	IPV4
package 🔲 C	IP allocation	Static - Manual

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.

VSphere - NSV	PX-ESX-13.0-79.6 × NSX	× +	- 0
vm vSobere Cl	Actions - NSVPX-ESX-13.0-79.64_n.		
vapitere ci	Power &	Power On christelle B	TILBLEOGHE *
	Guest OS	Power Off ctri+at+E	
	Snapshots	I Suspend chi + sh + 2	
vc.de7510d9c7d8	👹 Open Remote Console	astores Networks	
V 🚺 Cluster-1	🚔 Migrate	4-bit)	CPU USAGE
esx03-r05	Clone	italied	MEMORY LISAGE
exx04-r02 exx14-r05.c Fault Tolerance NSVPX.ES VM Policies Template	DNS Name:	OB OB	
	VM Policies	IP Addresses: Host: ecx04-r02.p03.de7510d9c7d8485cb31194 eastlus.avs.azure.com	STORAGE USAG
	Template		40.83 GB
	Compatibility		
	Export System Logs	✓ Notes	~
	🚱 Edit Settings	Edit Notes	
	Move to folder	^	
	Rename	Custor Attributes	^
	Edit Notes	esx04-r02.p03.de7510d9c7d8485cb31194.east	
	Tags & Custom Attributes	& cient	¹
ent Tasks Ala	Add Permission		
Name	Alarms	v Details v Initiator v Queued For v Stant Time ↓ v Completion Time	 Server
onfigure virtual	Remove from Inventory	ed VSPHERE.LOCAL.icloud 4 ms 05/02/2021, 411:08 PM 05/02/2021, 411:08 PM	vc.de7510d9c7d8485c
oy OVF template	Delete from Disk	ed VSPHERELOCALlvpxd3 ms 05/02/2021.4.08.26 PM 05/02/2021.4.09.12 PM	vc.de7510d9c7d8485c

9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.

VSphere - N	SVPX-ESX-13.0-79.64	NSVPX-ESX-13	3.0-79.64_nc_64	× 🔤 NSX		× -	+	-	o ×
$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	Not secure	https://192.168.0	0.2/ui/webcons	sole.html?vmld	=vm-53&vmName	e=NSVP	PX-ESX-13.0-79.64_nc_64&serverGuid=d77ece11-4945-4ee5-bb8e-17b4 🏠 🛠	•	g
NSVPX-ESX-13.0-7	9.64_nc_64						Enforce US Keyboard Layout View Fullscreen Se	nd Ctrl+/	Nt+Delete
	NetScal	er has st	arted	success	fully				
	Start a	dditional	daemo:	ns: M ay	2 16:12	2:54	<pre>{local0.err> ns nsconfigd: _dispatch()</pre>		
	Mau 2	10 passau 16:12:54	/locali	a orr)	ns nsconf	fiad	: dispatch(): Specified parameters are		
	not an	plicable	for th	is tune	of SSL r	orof	ile.		
	May 2	16:12:54	<local< td=""><td>0.err></td><td>ns nsconf</td><td>figd</td><td>: _dispatch(): Invalid rule.</td><td></td><td></td></local<>	0.err>	ns nsconf	figd	: _dispatch(): Invalid rule.		
	May 2	16:12:54	<local< td=""><td>0.err></td><td>ns last 🕨</td><td>Mess</td><td>age repeated 2 times</td><td></td><td></td></local<>	0.err>	ns last 🕨	Mess	age repeated 2 times		
	May 2	16:12:55	<local< td=""><td>0.err></td><td>ns nsconf</td><td>figd</td><td>: _dispatch(): No such resource</td><td></td><td></td></local<>	0.err>	ns nsconf	figd	: _dispatch(): No such resource		
	May 2	16:12:55	<local< td=""><td>0.err></td><td>ns nsconf</td><td>figd</td><td>: _dispatch(): No such policy exists</td><td></td><td></td></local<>	0.err>	ns nsconf	figd	: _dispatch(): No such policy exists		
	Monit M	onit daer	ion at	1000 aw	akened				
	Mau 2	16.12.55	(local)	arr)	ne laet b	HOCC	and repeated 4 times		
	Mau 2	16:13:00	(user.)	crit> n	s susheal	1 t hd	susid 450010. IPMI device read failed		
	-2.	10.10.00	10011		o oyonou i	2 0 210			
	May 2	16:13:00	<local< td=""><td>0.err></td><td>ns nscoll</td><td>lect</td><td>: ns_copyfile(): Not able to get info o</td><td></td><td></td></local<>	0.err>	ns nscoll	lect	: ns_copyfile(): Not able to get info o		
	f file	/var/log/	′db∕def	ault∕ns	devmap.t>	xt :	No such file or directory		
	Mau 2	16:13:01	(local)	g err)	ne neumon	nd [1	6391: nsumond daemon started		

10. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l' interface de ligne de commande :

1 ssh nsroot@<management IP address>

Exemple

```
1 ssh nsroot@192.168.4.5
```

11. Vous pouvez vérifier la configuration ADC à l'aide de la show ns ip commande.

2 OpenSSH SSH client								
Done sh ns	ip Ipaddress	Traffic Domain		Rode				State
))) Done	192.168.4.5 192.168.5.5 192.168.6.5		NetScaler IP VIP SHIP	Active Active Active	Enabled Enabled Enabled	Enabled Enabled Enabled	NA Enabled NA	Enabled Enabled Enabled
		×						

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.

```
1 add lb vserver <name> <serviceType> [<vip>] [<port>]
```

Exemple

```
1 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.

```
1 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.

1 bind lb vserver <name> <serviceName>

Exemple

1 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.

1	az network lb address-pool address add
2	resource-group <azure th="" vmc<=""></azure>
	Resource Group>
3	lb-name <lb name=""></lb>
4	pool-name <backend pool<="" th=""></backend>
	name>
5	vnet <azure vmc="" vnet=""></azure>
6	name <ip address="" name=""></ip>
7	ip-address <vip adc="" in<="" of="" th=""></vip>
	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 :

1 NSIP: 10.0.0.4/24
2 SNIP on 1/1: 10.0.1.4/24
3 SNIP on 1/2: 10.0.2.4/24
4 VIP: 172.168.1.1/32

Exemple de configuration IP pour l'instance ADC secondaire :

```
1 NSIP: 10.0.0.5/24
2 SNIP on 1/1: 10.0.1.5/24
3 SNIP on 1/2: 10.0.2.5/24
4 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.

Microsoft Azure	D Search resources, services, and docs (G+/)		TITRIX (CITRIX.ONMICROSOFT.C
Home > Resource groups > Azur	erouteserverIntegration >		
myRouteServer	* * …		×
	« 间 Delete		
😵 Overview	Essentials		JSON View
Activity log	Resource group : <u>AzurerouteserverIntegration</u> Status	: Succeeded	
Access control (IAM)	Location : eastus Virtual Network / So	ubnet : RSvnet/RouteServerSubnet	
🧳 Tags	Subscription ASN	: 65515	
Cattings	Subscription ID Peer Ips	: 10.0.3.4, 10.0.3.5	
	Tags (<u>edit</u>) : <u>Click here to add tags</u>		
Configuration			
Peers			
Properties 1			
🔒 Locks			
Monitor			
Connection monitor			
Monitoring			
Metrics			
Automation			
🚆 Tasks (preview)			
😨 Export template			

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.

Home > Resource groups > Azurerouteserverintegration > myRouteServer								
W myRouteServer Peers * ···								
P Search (Ctrl+/) ≪ + Add ◯ Refresh								
S Overview	Name	↑↓ ASN	↑↓ IPv4 Address	↑↓ Provisioning State	↑↓			
Activity log	ADC0	400	10.0.1.4	Succeeded				
^P _R Access control (IAM)	ADC1	500	10.0.1.5	Succeeded				
🧳 Tags								
Settings								

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
1
     enable ns feature LB BGP
2
3
     add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -
        dynamicRouting ENABLED
4
     VTYSH
5
     configure terminal
     router BGP 400
6
     timers bgp 1 3
7
8
     neighbor 10.0.3.4 remote-as 65515
     neighbor 10.0.3.4 advertisement-interval 3
9
     neighbor 10.0.3.4 fall-over bfd
10
11
     neighbor 10.0.3.5 remote-as 65515
12
     neighbor 10.0.3.5 advertisement-interval 3
13
     neighbor 10.0.3.5 fall-over bfd
14
     address-family ipv4
15
     redistribute kernel
16
     redistribute static
```

5. Configurez le routage dynamique dans l'instance ADC secondaire.

Exemple de configuration :

```
enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
1
     enable ns feature LB BGP
2
3
     add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -
        dynamicRouting ENABLED
4
     VTYSH
5
     configure terminal
6
     router BGP 500
     timers bgp 1 3
7
8
     neighbor 10.0.3.4 remote-as 65515
     neighbor 10.0.3.4 advertisement-interval 3
9
     neighbor 10.0.3.4 fall-over bfd
10
11
     neighbor 10.0.3.5 remote-as 65515
12
     neighbor 10.0.3.5 advertisement-interval 3
13
     neighbor 10.0.3.5 fall-over bfd
14
     address-family ipv4
15
     redistribute kernel
16
     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.

1 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 -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 sousréseau 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.

Home > new-test-14.1	
new-test-14.1 Identified Notice Virtual machine	ntity 🛪 …
₽ Search «	System assigned User assigned
Size	· · · · · · · · · · · · · · · · · · ·
Ø Microsoft Defender for Cloud	A system assigned managed identity is restricted to one per resource and is tied to the inecycle of this resource, you can grant permiss using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have
Advisor recommendations	🗟 Save 🗙 Discard 🖒 Refresh 🛛 🖗 Got feedback?
Extensions + applications	
Availability + scaling	Status (i)
Configuration	Off On
😢 Identity	
Properties	
Locks	
Operations	
✓ Bastion	

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.

Home > new-test-14.1	
new-test-14.1 Identi Virtual machine	ty ☆ ×
Search «	System assigned User assigned
Connect Solution Disks	A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID. so you don't have to store any credentials in code.
👤 Size	
Ø Microsoft Defender for Cloud	Save X Discard V Kefresh X Got feedback?
Advisor recommendations	erte O
Extensions + applications	Off On
Availability + scaling	Object (orincipal) ID ①
Configuration	78dc5c36-814f-44f0-a238-ccd992caae86
🚷 Identity	Permissions ①
Properties	Azure role assignments
Locks	
Operations	1 This resource is registered with Microsoft Entra ID. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures.
X Bastion	

- 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.

Home > new-test-14.1 Identity >	Add role assignment (Preview)
Azure role assignments	
+ Add role assignment (Preview) 💍 Refresh	Scope 🕖
If this identity has role assignments that you don't have permission to re	Subscription
Subscription *	Resource group ①
Role Resource Name	tahaj-test-ipconfig
No role assignments found for the selected subscription.	Role 🕜 Contributor 🛈
	Learn more about RBAC
	Save Discard

La page **Azure role** assignment affiche l'identité gérée que vous avez créée.

Home > new-test-14.1 Ide	antity >			
Azure role assig	nments			
+ Add role assignment (Pre	eview) 💍 Refresh			
If this identity has role assignn	nents that you don't have permission to read, they	won't be shown in the list. Learn more		
Subscription *				
		\sim		
Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	(i) tahaj-test-ipconfig	Resource Group	new-test-14.1	None

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**.

Home > new-test-14.1	ntity 🛧 …		Add user assigned managed identity	×
	System assigned User assigned			~ *
📮 Size	· · · · · · · · · · · · · · · · · · ·		User assigned managed identities	
O Microsoft Defender for Cloud	User assigned managed identities enable managed identities are created as standal	Azure resources to authenticat lone Azure resources, and have	Filter by identity name and/or resource group name	
Advisor recommendations	managed identities. Similarly, a single use	r assigned managed identity c	aibBuiUserld1600306786 Resource Group: ibLinuxGalleryRG	
Extensions + applications	🕂 Add 📋 Remove 💍 Refresh	🔗 Got feedback?	🗾 😑 test-user-assigned-mi	
Availability + scaling			Resource Group: r-test	
Configuration	Name	↑↓ Resource g	Selected identities:	
🚷 Identity	No results		est-user-assigned-mi	
Properties			Resource Group: r-test Subscrition: NSDev Platform CA anoop.agarwal@citrix.com	Remove
🔒 Locks				
Operations				
✓ Bastion			Add	
🕚 Auto-shutdown	*			

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.

← Set Credentials

Applicatio	n ID		
Applicatio	n Secret		
		_	

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.

Q Search Menu	AZURE > Cloud Profile				
Favorites	Cloud Profile 💿				
AZURE	Add Edit Delete				
Cloud Profile	Q Click here to search or you can enter Key : Value format				
System	NAME AUTO SCALE SETTING LOAD BALANCING VIRTUAL SERVER				
AppExpert	Noitems				

La page de configuration de **Create Cloud Profile** s'affiche.

← Create Cloud Profile

'irtual Server IP Address*	
10.0.1.4	\sim
уре	
AUTOSCALE	\sim
oad Balancing Server Protocol	
нттр	\sim
oad Balancing Server Port	
80	
uto Scale Setting*	
	~
uto Scale Setting Protocol	
НТТР	~
uto Scale Setting Port	

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**, assurezvous 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 àVirtual Machine Scale Sets, puis sélectionnezVirtual 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.

Name ①		Value ①	
Creator	:	d34eed9579934591afbbdf28c92caf51	1
info_no_auto_shutdown	:	temporarily disable automated vm shutdown, if set to 'true'. default value is 'false'. A 3 day lease by default will be provided during pext run of op auto script, if po	1
info_no_auto_shutdown_lease_datetime_UTC	:	view/update lease datetime. only valid if no_auto_shutdown tag set to 'true'. max 14 days lease is allowed, all generic date/time string are valid (eg. 'Tue Jun 20	İ 🗘
no_auto_shutdown	:	false	1
no_auto_shutdown_lease_datetime_UTC	:		1
tag1] :	false	10
] :		

Apply	Discard changes

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.

Create Cloud Profile

Name

Virtual Server IP Address*

52.169.111.203

Туре

AZURETAGS

Azure Tag Name

Azure Tag Value

Azure Poll Periods

60

Load Balancing Server Protocol

HTTP

Load Balancing Server Port

80

Azure Tag Setting*

Azure Tag Setting Protocol

HTTP

Azure Tag Setting Port

80

Create

Close

- 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.

```
1 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 » :

```
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
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
          Name: MyTagCloudProfile Type: azuretags
    1)
                                                          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 :

1 #> 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

1

Utilisez la commande suivante pour tuer le processus rain_tags :

```
1 # PID=`ps -aux | grep rain_tags | awk '{
2 print $2 }
3 '`; 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

January 15, 2025

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.



Region 2 (Resource Group 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.

1	<pre>\$location="West Central US"</pre>
2	
3	<pre>\$vnetName="NSVPX-vnet"</pre>
4	
5	\$RGName="multiIP-RG"
6	
(<pre>\$prmStorageAccountName="multiipstorageaccnt"</pre>
8	
9	SavSetName="Multrip-avset"
11	symsize="Standard\ DS2\ \/2"

Remarque :

La configuration minimale requise pour une instance VPX est de 2 vCPU et 2 Go de RAM.

1	<pre>\$publisher="citrix"</pre>
3	<pre>\$offer="netscalervpx111"</pre>
5	\$sku="netscalerbyol"
7	<pre>\$version="latest"</pre>
9	<pre>\$vmNamePrefix="MultiIPVPX"</pre>
10 11 12	<pre>\$nicNamePrefix="MultiipVPX"</pre>
12 13 14	<pre>\$osDiskSuffix="osdiskdb"</pre>
15	<pre>\$numberOfVMs=1</pre>
17 18	<pre>\$ipAddressPrefix="10.0.0."</pre>
10 19 20	<pre>\$ipAddressPrefix1="10.0.1."</pre>
20 21 22	<pre>\$ipAddressPrefix2="10.0.2."</pre>
23	<pre>\$pubIPName1="MultiIP-pip1"</pre>
25	<pre>\$pubIPName2="MultiIP-pip2"</pre>
20 27 28	<pre>\$IpConfigName1="IPConfig1"</pre>
29	\$IPConfigName2="IPConfig-2"
31 32	\$IPConfigName3="IPConfig-3"
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

```
1 $prmStorageAccount=New-AzureRMStorageAccount -Name
   $prmStorageAccountName -ResourceGroupName $RGName -Type
   Standard_LRS -Location $location
```

Créer un ensemble de disponibilités

```
1 $avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$RGName -Location $location
```

Création d'un réseau virtuel

1. Ajoutez des sous-réseaux.

1	<pre>\$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name</pre>
	<pre>\$frontendSubnetName -AddressPrefix "10.0.0.0/24"</pre>
2	<pre>\$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name</pre>
	<pre>\$backendSubnetName1 -AddressPrefix "10.0.1.0/24"</pre>
3	<pre>\$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name</pre>
	<pre>\$backendSubnetName2 -AddressPrefix "10.0.2.0/24"</pre>

2. Ajoutez un objet réseau virtuel.

```
1 $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
ResourceGroupName $RGName -Location $location -AddressPrefix
10.0.0.0/16 -Subnet $subnet1, $subnet2, $subnet3
```

3. Récupérez des sous-réseaux.

```
1 $frontendSubnet=$vnet.Subnets|?{
2 $_.Name -eq $frontendSubnetName }
3
4 $backendSubnet1=$vnet.Subnets|?{
5 $_.Name -eq $backendSubnetName1 }
6
7 $backendSubnet2=$vnet.Subnets|?{
8 $_.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

```
1 $nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
2 $ipAddress1=$ipAddressPrefix + $suffixNumber
```

3	<pre>\$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name \$IPConfigName1 -</pre>
	SubnetId \$frontendSubnet.Id -PublicIpAddress \$pip1 -
	PrivateIpAddress \$ipAddress1 -Primary
4	<pre>\$nic1=New-AzureRMNetworkInterface -Name \$nic1Name -ResourceGroupName</pre>
	<pre>\$RGName -Location \$location -IpConfiguration \$IpConfig1</pre>

Créer une carte réseau 1/1

1	<pre>\$nic2Name \$nicNamePrefix + \$suffixNumber + "-frontend"</pre>
2	<pre>\$ipAddress2=\$ipAddressPrefix1 + (\$suffixNumber)</pre>
3	\$ipAddress3=\$ipAddressPrefix1 + (\$suffixNumber + 1)
4	<pre>\$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name \$IPConfigName2 -</pre>
	PublicIpAddress \$pip2 -SubnetId \$backendSubnet1.Id -
	PrivateIpAddress \$ipAddress2 -Primary
5	<pre>\$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name \$IPConfigName3 -</pre>
	SubnetId \$backendSubnet1.Id -PrivateIpAddress \$ipAddress3
6	nic2=New-AzureRMNetworkInterface -Name \$nic2Name -ResourceGroupName
	<pre>\$RGName -Location \$location -IpConfiguration \$IpConfig2,</pre>
	\$IpConfig3

Créer une carte réseau 1/2

1	<pre>\$nic3Name=\$nicNamePrefix + \$suffixNumber + "-backend"</pre>
2	<pre>\$ipAddress4=\$ipAddressPrefix2 + (\$suffixNumber)</pre>
3	<pre>\$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name \$IPConfigName4 -</pre>
	SubnetId <pre>\$backendSubnet2.Id -PrivateIpAddress <pre>\$ipAddress4 -Primary</pre></pre>
4	<pre>\$nic3=New-AzureRMNetworkInterface -Name \$nic3Name -ResourceGroupName</pre>
	<pre>\$RGName -Location \$location -IpConfiguration \$IpConfig4</pre>

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

1	\$osDiskName=\$vmName + "-" + \$osDiskSuffix
2	<pre>\$osVhdUri=\$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds</pre>
	/" +\$osDiskName + ".vhd"
3	<pre>\$vmConfig=Set-AzureRMVMOSDisk -VM \$vmConfig -Name \$osDiskName -VhdUri</pre>
	<pre>\$osVhdUri -CreateOption fromImage</pre>
4	Set-AzureRmVMPlan -VM \$vmConfig -Publisher \$publisher -Product \$offer
	-Name \$sku
5	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 utilisé	ées dans VM1
--------------------------------	--------------

Carte d'interface		Adresse IP publi	Adresse IP publique		
réseau	IP privée	(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		
-	10.0.1.11	-	Configuré en tant qu' adresse IP du serveur LB. L'adresse IP publique n'est pas obligatoire		

Carte d'interface		Adresse IP publique		
réseau	IP privée	(PIP)	Description	
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	

Carte d'interface		Adresse IP publiqu	le
réseau	IP interne	(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

Tableau 2. Adresses IP utilisées dans VM2

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.

1 add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
2 Add nsip 10.0.2.10 255.255.255.0
3 add service svc1 10.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 10.0.1.11 80
5 add service s1 10.0.2.120 http 80

```
6 Add service s2 10.0.2.121 http 80
7 Bind lb vs v1 s[1-2]
```

Voici un exemple de configuration sur VM2.

```
1 add ns ip 20.0.1.10 255.255.255.0 -mgmtAccess ENABLED
2 Add nsip 20.0.2.10 255.255.255.0
3 add service svc1 20.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 20.0.1.11 80
5 Add service s1 20.0.2.90 http 80
6 Add service s2 20.0.2.91 http 80
7 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
1
2
    add gslb site site1 10.0.1.10 -publicIP PIP2
    add gslb site site2 20.0.1.10 -publicIP PIP5
3
    add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
4
        PIP3 -publicPort 80 -siteName site1
5
    add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP
        PIP6 -publicPort 80 -siteName site2
6
    add gslb vserver gslb_http_vip1 HTTP
    bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
7
    bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
8
9
    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 actifstandby 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



Region 2 (Resource Group 2)

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.

1	<pre>\$locName="South east Asia"</pre>
2	
3	\$rgName="MulitIP-MultiNIC-RG"
4	
5	<pre>\$publPName4="PIPFORGSLB1"</pre>
6	ŚdomNomo 4 - Uwpygo] bdpo !!
8	\$dollivalle4- vpxgstburis
9	\$]bName="MultiTPALB"
10	
11	<pre>\$frontEndConfigName2="FrontEndIP2"</pre>
12	
13	<pre>\$backendPoolName1="BackendPoolHttp"</pre>
14	
15	<pre>\$lbRuleName2="LBRuleGSLB1"</pre>
16	
10	\$ LDRu LeName3="LBRu LeGSLB2"
10	
19	SIDKUTENGIIEA- FDKUTEDN2

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

Étape 2. Créez des règles LB et mettez à jour l'ALB existant.

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
1
        $rgName
2
3
     $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
4
        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
13
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
        BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
14
15
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
        BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
17
18
```

19 \\$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
1
2
3
     add service dnssvc PIPFORGSLB1 ADNS 53
4
5
     add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1
6
7
     add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8
9
     add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
        publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10
11
     add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
        publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2
12
     add gslb vserver gslb_http_vip1 HTTP
13
14
15
     bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
16
17
     bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
18
19
     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

April 9, 2025

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 Style-Book 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 vivre une expérience fluide, où que vous soyez 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)

GSLB 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 en cours de création et de suppression 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 prenant en charge DNS pour déterminer les ressources de service membres de l'espace de noms DBS identifié dans le groupe Autoscale.

L'image suivante illustre les composants NetScaler GSLB DBS Autoscale avec des équilibreurs de charge cloud :



Prérequis pour Azure GSLB

Les conditions préalables pour les groupes de services NetScaler GSLB incluent un environnement Microsoft Azure fonctionnel, ainsi que les connaissances et la capacité de configurer des serveurs Web Linux, des appareils NetScaler dans Azure, des adresses IP publiques et des équilibreurs de charge Azure (ALB).

- 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-xxxxxxx.australiaeast.cloudapp.
azure.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.

≡ Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)
Home > Create a resource > Marketpla	ce > Load Balancer >	
Create load balancer		
Azure load balancer is a layer 4 load balanc balancers uses a hash-based distribution a destination port, protocol type) hash to ma accessible via public IP addresses, or interr Network Address Translation (NAT) to rout	cer that distributes incoming traffic among Igorithm. By default, it uses a 5-tuple (sour ap traffic to available servers. Load balance hal where it is only accessible from a virtua e traffic between public and private IP add	g healthy virtual machine instances. Load ree IP, source port, destination IP, ars can either be internet-facing where it is I network. Azure load balancers also support dresses. Learn more.
Project details		
Subscription *		\checkmark
Resource group *	Conta anu	
	Create new	
Instance details		
Name *	ALB	✓
Region *	East US 2	×
SKU * 🛈	• Standard	
	Gateway	
	Basic	
Туре * 🛈	O Public	
	Internal	
Tier *	Regional	
	🔘 Global	
Review + create < Previous	Next : Frontend IP configuration >	Download a template for automation RGive feedback

3. Ajoutez les pools principaux NetScaler créés.

Home > tahaj-test > ALB							
ALB Backend pool	s ☆ …						
	+ Add 🕐 Refresh						
Overview							
Activity log	The backend pool is a critical component of the load balancer. The backend pool defines the group of resources that will						
R Access control (IAM)	serve traffic for a given load-balancin	g rule. Learn more. 🕫					
Tags	P						
X Diagnose and solve problems							
Settings	Backend pool	Resource Name	IP address	Network interface	Availability zone	Rules count	Resource Status
Frontend IP configuration							
Backend pools							
🕴 Health probes							
E Load balancing rules							
Inbound NAT rules							
Properties							
🔒 Locks							
Monitoring							
Insights							
Diagnostic settings							
🧬 Logs							
II Alerts							
Metrics							

4. Créez une analyse de santé pour le port 80.

Créez une règle d'équilibrage de charge à l'aide de l'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

<u>Home</u> > tahaj-test > ALB Load bala	ncing rules >		
Add load balancing ru	le		
A load balancing rule distributes incomin backend pool instances. Only backend ins	g traffic that is sent to a selected IP address a stances that the health probe considers health	nd port combination across a group of ny receive new traffic.	
Name *	lb_rule2		
IP Version *	IPv4		
	O IPv6		
Frontend IP address * 🕡	frontend_ip (10.1.0.7)	~	
Backend pool * 🛈	backend_pool		
High availability ports 🕕			
Protocol	• тср		
Port *	80		
Backend port * 🕡	80		
Health probe * 🛈	Select an existing probe	~	
	Create new		
Session persistence 🛈	None	<u> </u>	
ldle timeout (minutes) * 🛈	4		
Enable TCP Reset			
Enable Floating IP 🛈			
Save			

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 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.

← Create Server

elb-virginia	(j)	
🔵 IP Address 🛛 🌔 Domain Name		
FQDN*		
elb-virginia-1948532428-us-eas		
Traffic Domain		
	Add	Edit
Translation IP Address		
Translation Mask		
Resolve Retry (secs)		
🗌 IPv6 Domain		
Enable after Creating		
Query Type		
A	~	
Comments		

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. Configurez le site en tant que site parent et assurez-vous que les **Moniteurs de déclenchement** sont définis sur **TOUJOURS**. 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.

← Create GSLB Site

Name*	
asia-site	\bigcirc
Туре	
REMOTE	\sim ()
Site IP Address*	
172 . 35 . 88 . 90	$(\mathbf{\hat{l}})$
Public IP Address	
18 . 232 . 14 . 212	\bigcirc
Parent Site Backup Parent Si Parent Site Name	ites
GSLBSite1	\sim (1)
Trigger Monitors*	
ALWAYS	\sim
Cluster IP	
Public Cluster IP	
NAPTR Replacement Suffix	
Metric Exchange	
Vetwork Metric Exchange	
Persistence Session Entry Exchange	
Create Close	

- 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.

← GSLB Service Group

Basic Settings	
Name*	
srv-grp-2	
Protocol*	
HTTP V	
Site Name*	
GSLBSite1 V	Add Edit
AutoScale Mode	
DNS 🗸	
✓ State	
🗸 Health Monitoring	
Comment	
OK Cancel	

7. Cliquez sur **Membres du groupe de services** et sélectionnez **Basé sur un serveur**. Sélectionnez l'ALB correspondant qui a été configuré au démarrage du guide d'exécution. Configurez le trafic pour passer par le port 80. Cliquez sur**Créer**.

Create Service Group Member								
IP Based Server Based								
Select Server*								
elb-nvirginia	> Add Edit ()							
Port*								
80	\bigcirc							
Weight								
1								
Order								
Site Prefix								
✓ State								
Create Close								

La liaison du membre du groupe de services est complétée par 2 instances qu'elle reçoit de l' ALB.

GSLB Servicegroup Member Binding								×				
Add	Edit Unbind	Monitor Details	No action \checkmark									
Q Click here	to search or you can enter Ke	ey : Value format										()
	IP ADDRESS	SERVER NAME	PORT \$	WEIGHT 🗘	ORDER		HASH ID	STATE \$	SERVICE STATE		SITE PREFIX	
	10.100.234.12	10.100.234.12	80	1				 ENABLED	UP			
	54.252.154.72	elb-nvirginia	80	1	1			 ENABLED	UP			
Close	\supset											

- 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.

← GSLB Virtual Server

Name*	
GV2	\bigcirc
DNS Record Type*	
А	\sim
Service Type*	
НТТР	\sim
Consider Effective State	
NONE	\sim ()
Toggle Order	
ASCENDING	\sim ()
Order Threshold	
Order Threshold	
Order Threshold AppFlow Logging When this Virtual Server is DO	OWN
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's	OWN s IP address in response (EDR)
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF	OWN s IP address in response (EDR) P
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service If	OWN s IP address in response (EDR) P Ps' in response (MIR)
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service IF EDNS Client Subnet	OWN s IP address in response (EDR) P Ps' in response (MIR)
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service If EDNS Client Subnet Respond with ECS option	OWN s IP address in response (EDR) P Ps' in response (MIR) in the response for a DNS query with ECS
 ✓ AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service IF EDNS Client Subnet Respond with ECS option Validate ECS address is a 	OWN s IP address in response (EDR) P Ps' in response (MIR) in the response for a DNS query with ECS private or unroutable address
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service If EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments	OWN s IP address in response (EDR) P Ps' in response (MIR) in the response for a DNS query with ECS private or unroutable address
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service IF EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments	OWN s IP address in response (EDR) P Ps' in response (MIR) in the response for a DNS query with ECS private or unroutable address
Order Threshold AppFlow Logging When this Virtual Server is DC Do not send any service's When this Virtual Server is UF Send all "active" service IF EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments	OWN & IP address in response (EDR) P Ps' in response (MIR) in the response for a DNS query with ECS private or unroutable address

l

12. Une fois le serveur virtuel GSLB créé, cliquez sur **No GSLB Virtual Server ServiceGroup Bind**ing.

← GSLB	Virtual	Server
--------	---------	--------

Basic Settings								
Name DNS Record Type Toggle Order Order Threshold Service Type Consider Effective State State	GV2 A ASCENDING 0 HTTP NONE •DOWN	AppFlow Logging EDR MIR ECS ECS Address Validation	ENABLED DISABLED DISABLED DISABLED DISABLED					
GSLB Services and GSLB Service Group Binding								
No GSLB Virtual Serve	No GSLB Virtual Server to GSLB Service Binding							
No GSLB Virtual Server to GSLB Service Group Binding								
ок	ок							

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.

ServiceGroup Binding	
Select Service Group Name*	
gslb-srv-grp1	> Add Edit
Order	
1	
Bind Close	

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. Conserver le paramètre par défaut pour les autres paramètres.

Domain Binding	
FQDN*	
www.gslbdbs.com	0
TTL (secs)	
5	
Backup IP	
Cookie Domain	
Cookie Time-out (mins)	
0	
Site Domain TTL (secs)	
3600	
Bind Close	

- 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.

← Load Balancing Service

Basic Settings	
Service Name*	
adns	\bigcirc
New Server Existing Server	
IP Address*	
172 . 31 . 27 . 121	(
Protocol*	
ADNS	(i)
Port*	
53	
5	
More	
OK Cancel	

- 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.

C. Service Marco		Traffic Manag	ement / 4918 /	Dial Virtual Senera			
ANS	>	GSLB V	firtual Serv	rers			0 😫
Syttem							
Applopent		Add	Edit Delete	Statistics No action	v		Search 🛩
Tuffic Management	\vee		Rent I	Batte	Patient	S. Haaddh	
Load Balancing	>	000	95	• UP	1079	100.00%.4 (#10.00WN	
Content Switching	• •						
Cache Redirection							
DN5							
G5L8	~						
Caritocard							
 Virtual Servers 							
Services.							

Autres ressources

Équilibrage de charge global NetScaler pour les déploiements hybrides et multicloud

Déployez NetScaler Web App Firewall sur Azure

October 17, 2024

NetScaler Web App Firewall est une solution d'entreprise offrant des protections de pointe pour les applications modernes. NetScaler Web App Firewall atténue les menaces qui pèsent sur les actifs destinés au public, notamment les sites Web, les applications Web et les API. NetScaler Web App Firewall inclut le filtrage basé sur la réputation IP, l'atténuation des bots, la protection contre les 10 principales menaces applicatives de l'OWASP, la protection DDoS de couche 7 et bien plus encore. Sont également incluses des options pour appliquer l'authentification, des chiffrements SSL/TLS forts, TLS 1.3, la limitation du débit et des stratégies de réécriture. Utilisant à la fois des protections WAF de base et avancées, NetScaler Web App Firewall fournit une protection complète à vos applications avec une facilité d'utilisation inégalée. Se lever et courir ne prend que quelques minutes. En outre, grâce à un modèle d'apprentissage automatisé, appelé profilage dynamique, NetScaler Web App Firewall permet aux utilisateurs de gagner un temps précieux. En apprenant automatiquement le fonctionnement d'une application protégée, NetScaler Web App Firewall s'adapte à l'application même lorsque les développeurs déploient et modifient les applications. NetScaler Web App Firewall contribue à la conformité à toutes les principales normes et organismes réglementaires, notamment les normes PCI-DSS, HIPAA, etc. Avec nos modèles CloudFormation, il n'a jamais été aussi facile d'être rapidement opérationnel. Grâce à la mise à l'échelle automatique, les utilisateurs peuvent être assurés que leurs applications restent protégées même lorsque leur trafic augmente.

NetScaler Web App Firewall peut être installé en tant que périphérique réseau de couche 3 ou en tant que pont réseau de couche 2 entre les serveurs du client et les utilisateurs du client, généralement derrière le routeur ou le pare-feu de l'entreprise cliente. Pour plus d'informations, consultez Introduction au pare-feu d'applications Web NetScaler.

Stratégie de déploiement de NetScaler Web App Firewall

1. Le déploiement du pare-feu d'applications Web consiste à évaluer quelles applications ou données spécifiques nécessitent une protection de sécurité maximale, celles qui sont les moins vulnérables et celles pour lesquelles l'inspection de sécurité peut être contournée en toute sécurité. Cela aide les utilisateurs à établir une configuration optimale et à concevoir des stratégies et des points de liaison appropriés pour séparer le trafic. Par exemple, les utilisateurs peuvent vouloir configurer une stratégie pour contourner l'inspection de sécurité des demandes de contenu Web statique, tels que des images, des fichiers MP3 et des films, et configurer une autre stratégie pour appliquer des contrôles de sécurité avancés aux demandes de contenu dynamique. Les utilisateurs peuvent utiliser plusieurs stratégies et profils pour protéger différents contenus d'une même application.

- 2. Pour établir une base de référence pour le déploiement, créez un serveur virtuel et testez le trafic via celui-ci pour avoir une idée du débit et de la quantité de trafic circulant dans le système utilisateur.
- 3. Déployez le pare-feu d'application Web. Utilisez NetScaler ADM et le StyleBook du pare-feu d' application Web pour configurer le pare-feu d'application Web. Consultez la section StyleBook ci-dessous dans ce guide pour plus de détails.
- 4. Mettez en œuvre le NetScaler Web App Firewall et le Top Ten de l'OWASP.

Les trois protections du Web Application Firewall sont particulièrement efficaces contre les types courants d'attaques Web et sont donc plus couramment utilisées que les autres. Ils doivent donc être mis en œuvre lors du déploiement initial. Ils sont :

- Script intersite HTML : examine les demandes et les réponses relatives aux scripts qui tentent d'accéder au contenu ou de le modifier sur un site Web différent de celui sur lequel se trouve le script. Lorsque cette vérification détecte un tel script, elle le rend inoffensif avant de transférer la requête ou la réponse à sa destination, ou elle bloque la connexion.
- Injection HTML SQL : examine les requêtes contenant des données de champs de formulaire pour détecter les tentatives d'injection de commandes SQL dans une base de données SQL. Lorsque cette vérification détecte du code SQL injecté, elle bloque la requête ou rend le code SQL injecté inoffensif avant de transférer la demande au serveur Web.

Remarque :

Assurez-vous que votre Web App Firewall est correctement configuré pour que les conditions suivantes s'appliquent à votre configuration :

- >* Si les utilisateurs activent le contrôle des scripts intersites HTML ou le contrôle de l'injection HTML SQL (ou les deux).
- >

>* Les sites Web protégés par les utilisateurs acceptent les téléchargements de fichiers ou contiennent des formulaires Web pouvant contenir des données de corps POST volumineuses.

Pour plus d'informations sur la configuration du pare-feu d'application Web pour gérer ce cas, consultez Configuration du pare-feu d'application : Configuration du pare-feu d'application Web.

• Dépassement de la mémoire tampon : examine les demandes pour détecter les tentatives de dépassement de la mémoire tampon sur le serveur Web.

Configuration du pare-feu d'application Web

Assurez-vous que le NetScaler Web App Firewall est déjà activé et fonctionne correctement. Nous vous recommandons de configurer NetScaler Web App Firewall à l'aide du Web Application Firewall StyleBook. La plupart des utilisateurs trouvent que c'est la méthode la plus simple pour configurer le Web Application Firewall, et elle est conçue pour éviter les erreurs. L'interface graphique et l'interface de ligne de commande sont destinées aux utilisateurs expérimentés, principalement pour modifier une configuration existante ou utiliser des options avancées.

Injection SQL

Le check d'injection HTML SQL de NetScaler Web App Firewall fournit des moyens de défense spéciaux contre l'injection de code SQL non autorisé susceptible de compromettre la sécurité des applications utilisateur. NetScaler Web App Firewall examine la charge utile des requêtes pour le code SQL injecté à trois emplacements : 1) le corps du POST, 2) les en-têtes et 3) les cookies. Pour plus d'informations, voir Vérification de l'injection HTML SQL.

Scriptage intersite

La vérification Script intersite HTML (script intersite) examine à la fois les en-têtes et les corps POST des requêtes utilisateur pour détecter d'éventuelles attaques de script intersite. S'il trouve un script intersite, il modifie (transforme) la demande pour rendre l'attaque inoffensive ou bloque la demande. Pour plus d'informations, voir Vérification des scripts intersites HTML.

Contrôle du dépassement de la mémoire tampon

La vérification de débordement de la mémoire tampon détecte les tentatives de provoquer un débordement de la mémoire tampon sur le serveur Web. Si le Web Application Firewall détecte que l'URL, les cookies ou l'en-tête sont plus longs que la longueur configurée, il bloque la demande car cela peut provoquer un dépassement de tampon. Pour plus d'informations, voir Vérification de dépassement de tampon.

Correctifs et signatures virtuels

Les signatures fournissent des règles spécifiques et configurables pour simplifier la tâche de protection des sites Web des utilisateurs contre les attaques connues. Une signature représente un modèle qui est un composant d'une attaque connue contre un système d'exploitation, un serveur Web, un site Web, un service Web XML ou une autre ressource. Un ensemble complet de règles intégrées ou natives préconfigurées constitue une solution de sécurité facile à utiliser, qui utilise la puissance de la correspondance de modèles pour détecter les attaques et protéger les applications contre les vulnérabilités. Pour plus d'informations, voir Signatures.

NetScaler Web App Firewall prend en charge la mise à jour **automatique et** manuelle des signatures. Nous vous suggérons également d'activer la **mise à jour automatique** pour les signatures afin de rester à jour.



Automatic signatures updates

Ces fichiers de signature sont hébergés dans l'environnement AWS et il est important d'autoriser l'accès sortant aux adresses IP NetScaler depuis les pare-feux réseau pour récupérer les derniers fichiers de signature. La mise à jour des signatures du NetScaler pendant le traitement du trafic en temps réel n'a aucun effet.

Analyse de la sécurité des applications

Le**tableau de bord de sécurité des applications**fournit une vue globale de l'état de sécurité des applications utilisateur. Par exemple, il affiche des mesures de sécurité clés telles que les violations de sécurité, les violations de signature et les index de menaces. Le tableau de bord de sécurité des applications affiche également des informations relatives aux attaques, telles que les attaques de synchronisation, les attaques par petites fenêtres et les attaques par inondation DNS pour le NetScaler découvert.

Remarque :

Pour consulter les indicateurs du tableau de bord de sécurité des applications, AppFlow for Security Insight doit être activé sur les instances NetScaler que les utilisateurs souhaitent surveiller.

Pour consulter les mesures de sécurité d'une instance NetScaler sur le tableau de bord de sécurité des applications :

- 1. Connectez-vous à NetScaler ADM à l'aide des informations d'identification d'administrateur.
- 2. Accédez à **Applications > App Security Dashboard**, puis sélectionnez l'adresse IP de l'instance dans la liste Appareils.

Les utilisateurs peuvent explorer plus en détail les anomalies signalées par Application Security Investigator en cliquant sur les bulles tracées sur le graphique.

Apprentissage centralisé sur ADM

NetScaler Web App Firewall protège les applications Web des utilisateurs contre les attaques malveillantes telles que l'injection SQL et les scripts intersites (XSS). Pour prévenir les violations de données et fournir une protection de sécurité adaptée, les utilisateurs doivent surveiller leur trafic à la recherche de menaces et de données exploitables en temps réel sur les attaques. Parfois, les attaques signalées peuvent être des faux positifs et ceux-ci doivent être fournis à titre exceptionnel.

L'apprentissage centralisé sur NetScaler ADM est un filtre de modèle répétitif qui permet au WAF d'apprendre le comportement (les activités normales) des applications Web des utilisateurs. Sur la base de la surveillance, le moteur génère une liste de règles ou d'exceptions suggérées pour chaque vérification de sécurité appliquée au trafic HTTP.

Il est beaucoup plus facile de déployer des règles de relaxation à l'aide du moteur d'apprentissage que de les déployer manuellement sous forme de relaxations nécessaires.

Pour déployer la fonctionnalité d'apprentissage, les utilisateurs doivent d'abord configurer un profil Web Application Firewall (ensemble de paramètres de sécurité) sur l'utilisateur NetScaler. Pour plus d'informations, voir Création de profils de pare-feu d'application Web.

NetScaler ADM génère une liste d'exceptions (relaxations) pour chaque contrôle de sécurité. En tant qu'administrateur, vous pouvez consulter la liste des exceptions dans NetScaler ADM et décider de les déployer ou de les ignorer.

En utilisant la fonction d'apprentissage WAF dans NetScaler ADM, vous pouvez :

- Configurez un profil d'apprentissage avec les contrôles de sécurité suivants.
 - Dépassement de tampon
 - Scriptage inter-sites HTML

Remarque :

La limite de localisation des scripts intersites s'applique uniquement à FormField. - Injection SQL HTML

```
1 > **Remarque :**
2 >
3 > Pour le contrôle de l'injection HTML SQL, les utilisateurs
doivent configurer `set -sqlinjectionTransformSpecialChars ON`
et `set -sqlinjectiontype sqlspclcharorkeywords` dans NetScaler.
```

- Vérifiez les règles de relaxation dans NetScaler ADM et décidez de prendre l'action nécessaire (déployer ou ignorer).
- Recevez les notifications par e-mail, Slack et ServiceNow.

• Utilisez le tableau de bord pour consulter les détails de la relaxation.

Pour utiliser l'apprentissage WAF dans NetScaler ADM :

- 1. Configurer le profil de formation : Configurer le profil de formation
- 2. Voir les règles de relaxation : Afficher les règles de relaxation et les règles d'inactivité
- 3. Utilisez le tableau de bord d'apprentissage WAF : Afficher le tableau de bord d'apprentissage WAF

StyleBooks

Les StyleBooks simplifient la gestion des configurations NetScaler complexes pour les applications utilisateur. Un StyleBook est un modèle que les utilisateurs peuvent utiliser pour créer et gérer des configurations NetScaler. Ici, les utilisateurs sont principalement concernés par le StyleBook utilisé pour déployer le Web Application Firewall. Pour plus d'informations sur StyleBooks, voir Style-Books.

Analyse des informations relatives à la sécurité

Les applications Web et de services Web exposées à Internet sont devenues de plus en plus vulnérables aux attaques. Pour protéger les applications contre les attaques, les utilisateurs ont besoin d'une visibilité sur la nature et l'ampleur des menaces passées, présentes et imminentes, de données exploitables en temps réel sur les attaques et de recommandations sur les contre-mesures. Security Insight fournit une solution à panneau unique pour aider les utilisateurs à évaluer l'état de sécurité des applications utilisateur et à prendre des mesures correctives pour sécuriser les applications utilisateur. Pour plus d'informations, consultez Security Insight.

Obtenir des informations détaillées sur les violations de sécurité

Les utilisateurs peuvent consulter la liste des attaques contre une application et obtenir des informations sur le type et la gravité des attaques, les actions entreprises par l'instance ADC, les ressources demandées et la source des attaques.

Par exemple, les utilisateurs peuvent vouloir déterminer le nombre d'attaques contre Microsoft Lync qui ont été bloquées, les ressources demandées et les adresses IP des sources.

Dans le tableau de**bord Security Insight**, cliquez sur**Lync > Total Violations**. Dans le tableau, cliquez sur l'icône de filtre dans l'en-tête**de colonne Action entreprise**, puis sélectionnez**Bloqué**.

1	ppleation	Summary			Action Taken 1						
	Security Check Volation	Severity 🖓	Weistine Category 🖓	Action Taken V	Bached NorBicked	9	Location	Signature Violation	Visiation Name	Same Violation Violat	found in
ï	Sec UR	Critical	Broken Authentication and Section Management	Buched	hardsmad	without I have					Form Trail
ï	Sec URL	Critical	Boles Authentication and Seulon Management	Docked		w/TestChird					Form Field
	Sec. URL	Critical	Broten duthentication and Section Management	Docked	Mp.010.102.43.0	art heat hand					form field
	Sec 185	Cillual	Broken Authentication and Sectors Management	Bisched	Mp. 75. 15.41.6	/wi/featil.html					Form Field
	Set UK.	Critical	Broken Authentication and Section Menagement	Doded	Mp.(10.10.41.6	/wi/featUnind					Form Field
	Set URL	Critical	Briten Authentication and Section Management	Disting	Mp.(70.10.41.0	(without hind					Form Field
	Sec. We	Critical	Broten Authentication and Sectors Management	Doched	Mp.(10.10.41.6	Var/Teal? Med					Form Field
	Sec URL	Citical	Broken Authentication and Section Menagement	Disting	Mp./70.10.41.6	2/wi/featUnied					Form Field
	Set URL	Citical	Broken Authentication and Section Menagement	Disted	Mp/70.1043.0	/w/test0.tend					Form Field
	244.055	Critical	Broken Authentication and Section Management	Ducked	Mp.(10.10.41.6	/without interd					Form Field
	Sec URL	Citical	Broken Authentication and Section Management	Bisched	Mp.010.101424	/wi/heat11.html					Form Frank
	Sec. 100	Called	Bookers Authentication and Service Mercarameter	Rindard	Manufacture and state	National Distance					From Date

Pour plus d'informations sur les ressources demandées, consultez la colonne**URL**. Pour plus d'informations sur les sources des attaques, consultez la colonne**IP du client**.

Afficher les détails des expressions du journal

NetScaler utilise des expressions de journal configurées avec le profil Application Firewall pour agir en cas d'attaques contre une application dans l'entreprise utilisateur. Dans **Security Insight**, les utilisateurs peuvent consulter les valeurs renvoyées pour les expressions de journal utilisées par l'instance ADC. Ces valeurs incluent, en-tête de requête, corps de requête et ainsi de suite. Outre les valeurs de l'expression de journal, les utilisateurs peuvent également afficher le nom de l'expression de journal et le commentaire de l'expression de journal définie dans le profil Application Firewall que l'instance ADC a utilisé pour prendre des mesures pour l'attaque.

Prérequis:

Assurez-vous que les utilisateurs :

- Configurez les expressions de journal dans le profil du pare-feu d'application. Pour plus d'informations, consultez la section Pare-feu d'application .
- Activez les paramètres Security Insights basés sur les expressions de journal dans NetScaler ADM. Procédez comme suit :
 - Accédez àAnalytics > Paramètres, puis cliquez surActiver les fonctionnalités pour Analytics.
 - Dans la page Activer les fonctionnalités pour Analytics, sélectionnezActiver Security Insight dans la section Paramètres de Security Insight basés sur l'expression du journalet cliquez surOK.



Par exemple, vous souhaiterez peut-être consulter les valeurs de l'expression de journal renvoyée par l'instance ADC pour l'action entreprise lors d'une attaque contre Microsoft Lync dans l'entreprise utilisateur.

Dans le tableau de **bord Security Insight**, accédez à**Lync** > **Total Violations**. Dans le tableau Résumé de l'application, cliquez sur l'URL pour afficher les détails complets de la violation dans la page**Informations sur la violation**, y compris le nom de l'expression de journal, le commentaire et les valeurs renvoyées par l'instance ADC pour l'action.

Gatoway Insight	>	Ministian Inform	atlan				
		violation inform	ation				^
	2			Violation	Informatio	n	
		Attack Time	NA				
	2	Signature Violation					
	>	Violation Name					
		Violation Value					
		Security Check Violation	Start L	a.			
		Violation Category	Broker	n Authentication and Session Ma	nagement		
		Threat Index	5				
		Severity	Mediu	im i			
		Action Taken	Blocke	ed .			
		URL	Mipch	/10.102.40.345/csrf_ft//ft//vow?1	field I-astasd		
		Pound in	Other	Location			
		Client IP	10.507	163.79			
		Location	Banga	lane			
		Total Attacks	1				
		Log Expression Name		Log Expression Comment	Log Expressi	los Value	
		L6D/P87		http request contains keyword	false		
		LGEXPRB		to request contains header	faise		
		LGDXPR6		http method expression	GET /csrt_Mo User-Agent o OpenSiL/03 Hest: 33.302/ Accept: "Y"	/ffc//um//feldlaadadHTTP/1.1 un/7137.086_64-pc-linus-gni(/lbcurl/7.197 38.082/12133.866/7155 60345	
		LGEXPRO		http method expression	true		
		LGEXPRI		http request contains header			
		LSEXPR1		http:request:header.contains.u seragent	our/7.15/7.00 2/0/1.2.3.3 R	M., 54-ac-linux-gnu) Ibcurl/7.19.7 Open55L/0.9.8k 3d9/1.15	
		LGDXPR2		http method expression	false		
		LGDXPRS		http method expression			
		NA 10.102	63.79	Start URL	Medum	Broken Authentication and Session Manager	THEFE
				MINT URL	Medium	Roken Authentication and Section Manager	

Déterminez l'indice de sécurité avant de déployer la configuration. Les failles de sécurité se produisent après que les utilisateurs ont déployé la configuration de sécurité sur une instance ADC, mais les utilisateurs peuvent vouloir évaluer l'efficacité de la configuration de sécurité avant de la déployer.

Par exemple, les utilisateurs peuvent vouloir évaluer l'indice de sécurité de la configuration de l'application SAP sur l'instance ADC avec l'adresse IP 10.102.60.27.

Dans le tableau de**bord Security Insight**, sous**Devices**, cliquez sur l'adresse IP de l'instance ADC configurée par les utilisateurs. Les utilisateurs peuvent voir que l'indice de menace et le nombre total d'attaques sont tous deux égaux à 0. L'indice de menace reflète directement le nombre et le type d'attaques contre l'application. Aucune attaque indique que l'application n'est soumise à aucune menace.

8	10w *	1 Addressey 2016 13:33:35 - 2 Meter	uny 2014 13.22.25			0	
Ove	rvšew Iotiena have Highest Throat Inde & Application has Highest Critica	n & Gewent Safety Index Attacks		MPL of System Security of 15 102	10.71 Device in Net Compliant		
App	plications					48.54	4
			Thread Index	Tably Index	Total Alberto	Devices	
	Lyne		Level 4	Level 2	4932	10.102.00.75	
	Sap		Level 0	Level 3		Threat index	
	Outlook		Level a	Level a	•	Al High	
	SharePoint .		Level #	Level 4		Low .	1
			8			Safety Index	

Cliquez sur**Sap > Safety Index > SAP_Profile**et évaluez les informations d'indice de sécurité qui s' affichent.

Application Summary				
Tortel Violations	Violations By SeverBy Critical 5846	Variations By Action Variations By Category Blocked \$846 Cross-site Soripting B		
Thread index Level 8 🙆 Safety index	Greet 2 🙆			
Safety Index Summary				
Application Firms Signatures: 1295/1300 No Security Check: 3/14 No	il Configuration A Configurad A Configurad	System Serv 4/10 Not C	rity Settings setfigured	
Application Firewall Configuration Level 2	Name Top, Forthe	Safety balox		
NetScaler System Security Level 2				

Dans le résumé du pare-feu d'application, les utilisateurs peuvent consulter l'état de configuration des différents paramètres de protection. Si un paramètre est défini pour consigner ou si un paramètre n'est pas configuré, un indice de sécurité inférieur est attribué à l'application.

Security Check	Lanvati B	Signatures Halation	Land? T
	Backed (4) Not Reshed (4) Outline(1)		Bisched (4) Bisched (4) Bisched (13) Outlind (13)
Providence Excession		Configuration Status	
XMR, Yarlaheleen		Net Cerfigured	
INE SOAP Fault		Next Configured	
Xing, and convert		Rott Configurited	
04,100		Not Certificated	
PR 200		Not Conferent	

Violations de sécurité

Les applications Web exposées à Internet sont devenues extrêmement vulnérables aux attaques. NetScaler ADM vous permet de visualiser les détails des violations exploitables afin de protéger les applications contre les attaques.

Afficher les détails des violations de sécurité des applications

Les applications Web exposées à Internet sont devenues nettement plus vulnérables aux attaques. NetScaler ADM permet aux utilisateurs de visualiser les détails des violations exploitables pour protéger les applications contre les attaques. Accédez à **Sécurité** > **Violations de sécurité** pour obtenir une solution à volet unique permettant de :

- Accédez aux violations de sécurité des applications en fonction de leurs catégories, telles que **Réseau**, **Bot**et **WAF**
- Prendre des mesures correctives pour sécuriser les applications

Pour afficher les violations de sécurité dans NetScaler ADM, assurez-vous :

- Les utilisateurs disposent d'une licence premium pour NetScaler (pour les violations du WAF et du BOT).
- Les utilisateurs ont demandé une licence sur les serveurs virtuels d'équilibrage de charge ou de commutation de contenu (pour WAF et BOT). Pour plus d'informations, consultez Gérer les licences sur les serveurs virtuels.
- Les utilisateurs peuvent activer d'autres paramètres. Pour plus d'informations, consultez la procédure disponible dans la section Configuration de la documentation produit NetScaler : Configuration.

Catégories de violation

NetScaler ADM permet aux utilisateurs de visualiser les violations disponibles dans Toutes les violations:

Configuration

En cas de violation, assurez-vous que **Metrics Collector** est activé. Par défaut, **Metrics Collector** est activé sur NetScaler. Pour plus d'informations, voirConfigurer Intelligent App Analytics.

Activez des analyses de sécurité avancées

- Accédez à Réseaux > Instances > NetScaler, puis sélectionnez le type d'instance. Par exemple, MPX.
- Sélectionnez l'instance NetScaler et dans la liste**Sélectionner une action**, sélectionnez**Configurer Analytics**.
- Sélectionnez le serveur virtuel et cliquez sur Activer Analytics.
- Dans la fenêtre Activer Analytics :
 - Sélectionnez **Web Insight**. Une fois que les utilisateurs ont sélectionné Web Insight, l'option**Advanced Security Analytics**en lecture seule est activée automatiquement.

Remarque :

L'option **Advanced Security Analytics** s'affiche uniquement pour les instances ADC sous licence Premium.

- Sélectionnez Logstream comme mode de transport
- L'expression est true par défaut
- Cliquez sur **OK**

Enable Analytics	×
Selected Virtual Server - Load Balancing: 1	
V Web Insight	
Client Side Measurement	
Security Insight	
Bot Insight	
Advanced Security Analytics	
Advanced Options	
For ADC version less than 12.0 IPFIX is default Transport mode.	
Transport Mode	
Logstream IPFIX	
Instance level options	
Enable HTTP X-Forwarded-For	
Citrix Gateway	
	_
Expression Configuration	
OK Close	

Activer les paramètres de transaction Web

Accédez à Analytics>Paramètres.

La page **Paramètres** s'affiche.

- Cliquez sur Activer les fonctionnalités pour Analytics.
- Sous Paramètres de transaction Web, sélectionnez Tout.

Enable Features for Analytics
Bulling Letings
Enable the Wolfman Relation P for extended deployment has more than one OWA ACC appliance or OWA deployment belower a single direct and variesr connection. OWA ADM analysis the number of hops for OWA detronge appliances through which the OX connections and connections a
Suddi Muthep
13 Indjil: Letting:
Enable the 12 ¹ insight basiss of Disk ADM to provide an easy and solidate solidar for monitoring the metrics of the optimization techniques and congestion control transpise for algorithmal and in Driv ADC appliances to avoid metrics in data formation.
C double K2P insight
Web toright Settings
Enable the Web might fusion to about 20th SDWIss intrinse the performance reports of web applications (scaling and centers authoring situationered that are bound to the DNIs RDC. Web insight enables stubility the entropics and about if edimensions to monitor of web applications being severing the DNIs RDC to providing integrated and use the monitoring of applications.
E divador Bala notati
Web Yanasetism Sattings
Enable Web Transactions had we to allow Chile KOM to retrine Web transactions from Chile KOC.
Evalue that Suscentiane
Avenuations Transformer
Incurity Insights Lettings
Endoti op Domaior baard learty Inight to report to report of repairing data configured with Application Farewall profile. This will help use to see desided top advect violations.
C Statis Invested Sugging
OM Disse

• Cliquez sur **OK**.

Tableau de bord des violations de sécurité

Dans le tableau de bord des violations de sécurité, les utilisateurs peuvent consulter :

• Le nombre total de violations s'est produit dans l'ensemble de NetScaler et de ses applications. Le total des violations s'affiche en fonction de la durée sélectionnée.

Security Violations	6291.500 - 3236.968 v

• Total des violations dans chaque catégorie.

Network	Bot	WAF
No violations detected	52K violations	55 violations

• Nombre total de ADC affectés, nombre total d'applications affectées et violations les plus importantes en fonction du nombre total d'occurrences et des applications affectées.

ADCrAthenet Ageleneous Atlened 5 7	
Top Violations Text on the earders of increases and the affected applications	Collect: (012) 507 Vicializes Mexandle Large Large

Pour plus d'informations sur les détails des violations, voir Toutes les violations.

Aperçu du bot

Configurez BOT Insight dans NetScaler. Pour plus d'informations, consultez Bot.

Afficher les robots

Cliquez sur le serveur virtuel pour afficher le**résumé de l'application**

pplication Summary Average RFS 0.02	as Nerth associations (as Nerth as Boos by Severity High 41.05 K		Largest Bot Category				60
Average RPS 0.02	Boto by Severity High 41.08 K		Largest Bot-Category				
Average RPS 0.02	Bots by Severity High: 41.08 K		Largest Bot Category				
			41.08 K	Largest Geo Sou Unknown 41.3	нце 53 К	Average N Bot T 84,52%	uffic
			100	32			
	0						
Critical Severity Atlants 🛛 🌻 Medium Se	weitpAttacks 😑 Low-Severity	Attacks					
66	0			in a section of the s	Contraction of the local division of the loc		
1			(')	• 10.000			
	A BOT CATEGORY	100% :	#DROPPED : #DIPTONA	: # ALLOWED :	# NTEUMT :	# REDRECT :	#100
	in the local build	40080	40000 0				0
	day for heard	207			0		247

- 1. Fournit les détails du résumé de la demande, tels que :
 - **RPS moyen** : indique le nombre moyen de demandes de transaction de bot par seconde (RPS) reçues sur les serveurs virtuels.
 - Bots par gravité : indique que les transactions de bot les plus élevées ont eu lieu en fonction de la gravité. La gravité est classée selon les catégories suivantes : critique, élevée, moyenneet faible.

Par exemple, si les serveurs virtuels ont 11 770 robots de gravité élevée et 1 550 robots de gravité critique, alors NetScaler ADM affiche **1,55 K critiques** sous **Robots par gravité**.

• Catégorie de bot la plus importante : indique que les attaques de robots les plus nombreuses se sont produites en fonction de la catégorie de bot.

Par exemple, si les serveurs virtuels ont 8 000 robots bloqués, 5 000 robots autorisés et 10 000 robots dont la limite de débit a été dépassée, alors NetScaler ADM afficheLimite de débit dépassée de 10 000 sousCatégorie de robot la plus importante.

• Source géographique la plus importante : indique que les attaques de robots les plus nombreuses se sont produites en fonction d'une région.

Par exemple, si les serveurs virtuels ont 5 000 attaques de bots à Santa Clara, 7 000 attaques de bots à Londres et 9 000 attaques de bots à Bangalore, alors NetScaler ADM affiche**Bangalore 9 K**sous**Plus grande source géographique**.

- % moyen de trafic de robots : indique le ratio de robots humains.
- 2. Affiche la gravité des attaques de robots en fonction des emplacements dans la vue cartographique
- 3. Affiche les types d'attaques de bots (bonnes, mauvaises et toutes)
- 4. Affiche le nombre total d'attaques de bots ainsi que les actions configurées correspondantes. Par exemple, si vous avez configuré :
 - Plage d'adresses IP (192.140.14.9 à 192.140.14.254) en tant que bots de liste de blocs et sélectionné Drop comme action pour ces plages d'adresses IP
 - Plage d'adresses IP (192.140.15.4 à 192.140.15.254) en tant que bots de liste noire et sélectionnée pour créer un message de journal en tant qu'action pour ces plages d'adresses IP

Dans ce scénario, NetScaler ADM affiche :

- Total des bots listés par bloc
- Nombre total de robots sous Dropped
- Nombre total de robots sous Log

Voir les robots CAPTCHA

Dans les pages Web, les CAPTCHA sont conçus pour identifier si le trafic entrant provient d'un humain ou d'un robot automatisé. Pour afficher les activités CAPTCHA dans NetScaler ADM, les utilisateurs doivent configurer CAPTCHA comme une action de bot pour les techniques de détection de réputation IP et d'empreintes digitales de l'appareil dans une instance NetScaler ADM. Pour plus d'informations, voir :Configurer la gestion des robots.

Voici les activités CAPTCHA que NetScaler ADM affiche dans Bot Insight :

- Nombre de**tentatives de CAPTCHA dépassé** : indique le nombre maximum de tentatives de CAPTCHA effectuées après un échec de connexion
- Client Captcha muted : indique le nombre de demandes client qui sont abandonnées ou redirigées parce que ces demandes ont été détectées comme des robots malveillants précédemment avec le challenge CAPTCHA.
- Humain Indique les entrées de captcha effectuées par les utilisateurs humains
- **Réponse captcha non valide** : indique le nombre de réponses CAPTCHA incorrectes reçues du bot ou de l'humain lorsque NetScaler envoie un défi CAPTCHA

BOT CATEGORY	TOTAL ATTACKS	# DROFPED	# CAPTO (A 🔅	# ALLOWED 🔅	# RATE LIMIT	# REDIRECT 0	#LOG 0
Captche Attempts Exceeded	11	11	0	0	0	0	0
Captche Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Involid Captcha Response	40	23	0	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scuper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

Afficher les pièges à

Pour afficher les pièges à bots dans NetScaler ADM, vous devez configurer le piège à bots dans NetScaler. Pour plus d'informations, voir :Configurer la gestion des robots.

pplications	1								100	1.00	at the second second second second second second second second second second second second second second second	insta	inces
lasal Bots on In	nance 10.0	06154240	are 9.77 K									8.8.3	ND (30 304 254 340)
	Total Barris	Total Muman Browners	Bot Human Ratio	Signatured Bath	Fingerprint ed Sats	Rate Record Bots	ar Reputation Bots	white lists	Machine Bots	Bat Tape	75.845	14.20	201.08
test_Ib1	440	0	100:0	0	0	0	0	0	0	0	440		
test_vserve	9.33 K	•	300:0	•	•	a	0	•	0	5	9.32 K		

Pour identifier le piège à robots, un script est activé sur la page Web et ce script est masqué aux humains, mais pas aux robots. NetScaler ADM identifie et signale les pièges de bots, lorsque ce script est consulté par les bots.

Cliquez sur le serveur virtuel et sélectionnez Zero Pixel Request

BOT CATEGORY	TOTAL 0	# DROPPED 0	z capicha 👘	# ALLOWED 0	2 RATELIMIT 0	# REDIRECT 0	#106 C
Invalid DevicePP	33450	33450	0	0	0	0	0
Zero Pixel Request	246	0		0	0	0	246
Human	100	0	0	100	0	0	0

Afficher les détails du bot

Pour plus de détails, cliquez sur le type d'attaque de**bot sous Catégorie**de robots.

Les détails tels que le temps d'attaque et le nombre total d'attaques de robots pour la catégorie de captcha sélectionnée sont affichés.

Bot Category - "Capitcha A	itempts Exceeded*					×	1.418	1 Month		-	bearch
meline Details							17.944	r 2020, 12	10-10-14 <i>i</i>	ge 2020	. 11.74

Les utilisateurs peuvent également faire glisser le graphique à barres pour sélectionner la période spécifique à afficher avec les attaques de robots.



Pour obtenir des informations supplémentaires sur l'attaque de bot, cliquez pour développer.

	1000	1000	10.00	-	10103-0408	ALC: UNKNOWN	-	10.00	Marries.	
×	140.00		**	1004	-	Market	Ballot	Respire	AND, N. M.	
×	50p 09 0248 P.,	101021.88	Bad	ontral	Drap	BLICHUST	BlackLSI	Bangalore	-184_181_3640-	
	Instance IP: 10.10 HTTP Request URI Region: Kamataka	6154240 Er/bleck_loc_test.h	trd	Total Cour Profi	Bots: 1 stry Code: IN le Name: bot_profit	e				
*	14 01 10 HT.	-	***	-	-	Barbare	Ballot	Require	AND, N. M.	

- **IP de l'instance** : indique l'adresse IP de l'instance NetScaler.
- Nombre total de bots : indique que le nombre total d'attaques de robots s'est produit pendant cette période précise.
- URL de demande HTTP : indique l'URL configurée pour les rapports captcha.
- Code de pays—Indique le pays dans lequel l'attaque du bot s'est produite.
- **Région** Indique la région dans laquelle l'attaque du bot s'est produite.
- Nom du profil—Indique le nom du profil fourni par les utilisateurs lors de la configuration.

Recherche avancée

Les utilisateurs peuvent également utiliser la zone de texte de recherche et la liste des durées, où ils peuvent afficher les détails du bot selon les besoins de l'utilisateur. Lorsque les utilisateurs cliquent sur le champ de recherche, celui-ci leur fournit la liste suivante de suggestions de recherche.

• IP de l'instance : adresse IP de l'instance NetScaler.

- Client-IP : adresse IP du client.
- **Type de robot** : Type de bot tel que Bon ou Mauvais.
- Sévérité : gravité de l'attaque du bot.
- Action entreprise : action entreprise après l'attaque du bot, telle que Drop, Aucune action, Redirection.
- **Catégorie de bot** : catégorie de l'attaque par bot, telle que liste de blocage, liste d'autorisation, empreinte digitale. En fonction d'une catégorie, les utilisateurs peuvent y associer une action de bot.
- **Détection de robots** : types de détection de robots (liste de blocage, liste d'autorisation, etc.) que les utilisateurs ont configurés sur NetScaler.
- Lieu : région/pays où l'attaque du bot a eu lieu
- Request-URL—URL qui contient les attaques possibles par des robots

Les utilisateurs peuvent également utiliser des opérateurs dans les requêtes de recherche d'utilisateurs pour affiner le champ de la recherche d'utilisateurs. Par exemple, si les utilisateurs souhaitent afficher tous les robots malveillants :

- Cliquez sur le champ de recherche et sélectionnez Bot-Type
- Cliquez à nouveau sur le champ de recherche et sélectionnez l'opérateur =
- Cliquez à nouveau sur le champ de recherche et sélectionnez Mauvais
- Cliquez sur Rechercher pour afficher les résultats

Name of Control of Con			Bot Type			
Marriero de Carlos de Carl		-	-	equal to some adult contains some adult	ò	
				1		
	Barton-I				×.,	

Taux de demandes anormalement élevé

Les utilisateurs peuvent contrôler le trafic entrant et sortant depuis ou vers une application. Une attaque de bot peut entraîner un taux de requêtes anormalement élevé. Par exemple, si les utilisateurs configurent une application pour autoriser 100 requêtes/minute et si les utilisateurs observent 350 requêtes, il peut s'agir d'une attaque de bot. À l'aide de l'indicateur de **taux de demandes anormalement élevé**, les utilisateurs peuvent analyser le taux de demandes inhabituel reçu par l'application.

VIOLATION DETAILS					
Decesive Clean Connections at 11 Mar 1817 p.m. Behavior based Discussify High Request Rate 2	Unusually High Req Anomal deviation from us	uest Rote Innanoumo	er indicates possibility of an Bot Attack.		
2 Apr 101 16 arrs Behaviour based	What Happened				
Encountry Large Download V. an	Last Occurred time 83 Apr 830 am	Tatal Occurrences 7	Applications Affected 1		
Environity Large Libbard Volument					
T-lpr 10.01 am Behadisor based	Event Details				
	Affected Application	NE.80.30ER 36382	11 P 380 (P)		
	Regard Rate				Read 2009
					111
		\sim	~~~~		
		19100 X740	15.04 33.00	21.00	A Apr mins

Sous Détails de l'événement, les utilisateurs peuvent consulter :

- L'application affectée. Les utilisateurs peuvent également sélectionner l'application dans la liste si plusieurs applications sont concernées par des violations.
- Graphique indiquant toutes les violations
- L'heure d'occurrence de la violation
- Le message de détection de la violation, indiquant le nombre total de demandes reçues et% de demandes excessives reçues par rapport aux demandes attendues
- La fourchette acceptée des taux de demandes attendus varie à partir de l'application

Détection de bot

Le système de gestion des bots NetScaler utilise différentes techniques pour détecter le trafic de bots entrant. Les techniques sont utilisées comme règles de détection pour détecter le type de bot.

Configuration de la gestion des bots à l'aide de l'interface graphique Les utilisateurs peuvent configurer la gestion des bots NetScaler en activant d'abord la fonctionnalité sur l'appliance. Pour plus d'informations, voir Détection de robots.

Réputation IP

La réputation IP est un outil qui identifie les adresses IP qui envoient des demandes indésirables. À l'aide de la liste de réputation IP, vous pouvez rejeter les demandes provenant d'une adresse IP de mauvaise réputation.

Configuration de la réputation IP à l'aide de l'interface graphique Cette configuration est une condition préalable à la fonctionnalité de réputation IP des robots. Pour plus d'informations, voir Réputation IP.

Mise à jour automatique pour les signatures de robots La technique de signature statique des bots utilise une table de recherche de signature avec une liste de bons bots et de mauvais robots. Pour plus d'informations, voir Mise à jour automatique des signatures.

NetScaler Web App Firewall et OWASP dans le top 10, 2021

L'Open Web Application Security Project (OWAP) a publié le Top 10 de l'OWASP pour 2021 en matière de sécurité des applications Web. Cette liste répertorie les vulnérabilités les plus courantes des applications Web et constitue un excellent point de départ pour évaluer la sécurité Web. Cette section explique comment configurer le NetScaler Web App Firewall pour atténuer ces failles. WAF est disponible sous forme de module intégré dans NetScaler (Premium Edition) et dans une gamme complète d'appareils.

L'intégralité du document OWASP Top 10 est disponible à l'adresse suivante : OWASP Top Ten.

Top 10 de l'OWASP 2021	Fonctionnalités de NetScaler Web App Firewall
A1:2021 Contrôle d'accès cassé	AAA, fonctionnalités de sécurité d'autorisation
	au sein du module AAA de NetScaler, protections
	des formulaires et protections contre la
	falsification des cookies, StartURL et ClosureURL
A2:2021 - Défaillances cryptographiques	Protection des cartes de crédit, commerce
	sécurisé, utilisation de cookies par proxy et
	cryptage des cookies

Top 10 de l'OWASP 2021	Fonctionnalités de NetScaler Web App Firewall
A3:2021 - Injection	Prévention des attaques par injection (injection SQL ou toute autre injection personnalisée telle que l'injection de commande du système d' exploitation, l'injection XPath et l'injection LDAP), fonction de signature de mise à jour automatique
A5:2021 Mauvaise configuration de sécurité	Cette protection inclut les contrôles WSI, la validation des messages XML et le contrôle du filtrage des erreurs XML SOAP
A6:2021 - Vulnérabilité et composants obsolètes	Rapports d'analyse de vulnérabilité, modèles de pare-feu d'application et signatures personnalisées
A7:2021 - Défaillance d'identification et d' authentification	AAA, protection contre la falsification des cookies, utilisation de cookies par proxy, cryptage des cookies, balisage CSRF, utilisation du protocole SSL
A8:2021 —Défaillances liées à l'intégrité des logiciels et des données	Contrôles de sécurité XML, type de contenu GWT, signatures personnalisées, Xpath pour JSON et XML
A9:2021 —Défaillances de journalisation et de surveillance de la sécurité	Journalisation personnalisée configurable par l' utilisateur, système d'analyse et de gestion

A1:2021 Contrôle d'accès cassé

Les restrictions concernant ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités et à des données non autorisées, telles que l'accès aux comptes d'autres utilisateurs, la consultation de fichiers sensibles, la modification des données d'autres utilisateurs ou la modification des droits d'accès.

- La fonction AAA qui prend en charge l'authentification, l'autorisation et l'audit pour tout le trafic des applications permet à un administrateur de site de gérer les contrôles d'accès avec l' appliance ADC.
- La fonction de sécurité d'autorisation du module AAA de l'appliance ADC permet à l'appliance

de vérifier le contenu d'un serveur protégé auquel elle doit autoriser l'accès de chaque utilisateur.

- Cohérence des champs de formulaire : si les références aux objets sont stockées sous forme de champs masqués dans les formulaires, vous pouvez vérifier que ces champs ne sont pas falsifiés lors de demandes ultérieures.
- Proxy des cookies et cohérence des cookies : les références aux objets stockées dans les valeurs des cookies peuvent être validées grâce à ces protections.
- Lancer la vérification d'URL avec fermeture d'URL : permet à l'utilisateur d'accéder à une liste d'URL autorisées prédéfinie. La fermeture d'URL crée une liste de toutes les URL vues dans les réponses valides pendant la session utilisateur et autorise automatiquement l'accès à celles-ci pendant cette session.

A2:2021 - Défaillances cryptographiques

De nombreuses applications Web et API ne protègent pas correctement les données sensibles, telles que les données financières, les soins de santé et les informations personnelles. Les attaquants peuvent voler ou modifier ces données mal protégées pour commettre des fraudes par carte de crédit, des vols d'identité ou d'autres délits. Les données sensibles peuvent être compromises sans protection supplémentaire, telle que le chiffrement au repos ou en transit, et nécessitent des précautions particulières lors de leur échange avec le navigateur.

Protections de NetScaler Web App Firewall

- Le Web Application Firewall protège les applications contre les fuites de données sensibles telles que les informations de carte de crédit.
- Les données sensibles peuvent être configurées en tant qu'objets sécurisés dans le cadre de la protection Safe Commerce afin d'éviter toute exposition.
- Toutes les données sensibles contenues dans les cookies peuvent être protégées par le biais du proxy et du cryptage des cookies.

A3:2021 - Injection

Les défauts d'injection, tels que l'injection SQL, NoSQL, OS et LDAP, se produisent lorsque des données non fiables sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent inciter l'interpréteur à exécuter des commandes involontaires ou à accéder à des données sans autorisation appropriée. Les failles XSS se produisent lorsqu'une application inclut des données non fiables dans une nouvelle page Web sans validation ni échappement appropriés, ou lorsqu'elle met à jour une page Web existante avec des données fournies par l'utilisateur à l'aide d'une API de navigateur capable de créer du code HTML ou JavaScript. XSS permet aux attaquants d'exécuter des scripts dans le navigateur de la victime, ce qui peut pirater des sessions utilisateur, dégrader des sites Web ou rediriger l'utilisateur vers des sites malveillants.

- La fonction de prévention des injections SQL protège contre les attaques par injection courantes. Des modèles d'injection personnalisés peuvent être téléchargés pour se protéger contre tout type d'attaque par injection, y compris XPath et LDAP. Cela s'applique aux charges utiles HTML et XML.
- La fonction de signature de mise à jour automatique maintient les signatures d'injection à jour.
- La fonction de protection du format des champs permet à l'administrateur de restreindre n' importe quel paramètre utilisateur à une expression régulière. Par exemple, vous pouvez faire en sorte qu'un champ de code postal contienne uniquement des entiers ou même des entiers à 5 chiffres.
- La cohérence des champs de formulaire valide chaque formulaire utilisateur soumis par rapport à la signature du formulaire de session utilisateur afin de garantir la validité de tous les éléments du formulaire.
- Les contrôles de dépassement de tampon garantissent que l'URL, les en-têtes et les cookies sont dans les bonnes limites, bloquant ainsi toute tentative d'injection de scripts ou de code volumineux.
- La protection XSS protège contre les attaques XSS courantes. Des modèles XSS personnalisés peuvent être téléchargés pour modifier la liste par défaut des balises et des attributs autorisés. Le WAF ADC utilise une liste blanche d'attributs et de balises HTML autorisés pour détecter les attaques XSS. Cela s'applique aux charges utiles HTML et XML.
- ADC WAF bloque toutes les attaques répertoriées dans le aide-mémoire OWASP XSS Filter Evaluation.
- La vérification du format des champs empêche un attaquant d'envoyer des données de formulaire Web inappropriées, ce qui peut constituer une attaque XSS potentielle.
- Cohérence des champs de formulaire

A5:2021 - Mauvaise configuration de la sécurité

La mauvaise configuration de la sécurité est le problème le plus fréquent. Cela est généralement dû à des configurations par défaut non sécurisées, à des configurations incomplètes ou improvisées, à un stockage cloud ouvert, à des en-têtes HTTP mal configurés et à des messages d'erreur détaillés contenant des informations sensibles. Non seulement tous les systèmes d'exploitation, infrastructures, bibliothèques et applications doivent être configurés de manière sécurisée, mais ils doivent également être corrigés et mis à niveau en temps opportun.

De nombreux processeurs XML anciens ou mal configurés évaluent les références d'entités externes dans les documents XML. Les entités externes peuvent être utilisées pour divulguer des fichiers internes à l'aide du gestionnaire d'URI de fichier, des partages de fichiers internes, de l'analyse de port interne, de l'exécution de code à distance et des attaques par déni de service

- Le rapport PCI-DSS généré par le pare-feu d'application documente les paramètres de sécurité du périphérique pare-feu.
- Les rapports issus des outils de numérisation sont convertis en signatures ADC WAF afin de gérer les erreurs de configuration en matière de sécurité.
- NetScaler Web App Firewall Web Application Firewall prend en charge Cenzic, IBM AppScan (Enterprise et Standard), Qualys, TrendMicro, WhiteHat et les rapports d'analyse de vulnérabilité personnalisés.
- En plus de détecter et de bloquer les menaces applicatives courantes qui peuvent être adaptées pour attaquer les applications basées sur XML (c'est-à-dire les scripts intersites, l'injection de commandes, etc.).
- NetScaler Web App Firewall Web Application Firewall inclut un ensemble complet de protections de sécurité spécifiques au XML. Il s'agit notamment de la validation de schéma pour vérifier en profondeur les messages SOAP et les charges utiles XML, ainsi que d'une puissante vérification des pièces jointes XML pour bloquer les pièces jointes contenant des exécutables malveillants ou des virus.
- Les méthodes d'inspection automatique du trafic bloquent les attaques par injection XPath sur les URL et les formulaires destinés à obtenir un accès.
- NetScaler Web App Firewall Web Application Firewall déjoue également diverses attaques DoS, notamment les références à des entités externes, l'expansion récursive, l'imbrication excessive et les messages malveillants contenant des attributs et des éléments longs ou nombreux.

A6:2021 - Composants vulnérables et obsolètes

Les composants, tels que les bibliothèques, les infrastructures et les autres modules logiciels, s'exécutent avec les mêmes privilèges que l'application. Si un composant vulnérable est exploité, une telle attaque peut entraîner de graves pertes de données ou la prise de contrôle du serveur. Les applications et les API utilisant des composants présentant des vulnérabilités connues peuvent compromettre les défenses des applications et permettre diverses attaques et impacts.

Protections de NetScaler Web App Firewall

- Nous vous recommandons de mettre à jour les composants tiers.
- Les rapports d'analyse des vulnérabilités convertis en signatures ADC peuvent être utilisés pour corriger virtuellement ces composants.
- Les modèles de pare-feu d'application disponibles pour ces composants vulnérables peuvent être utilisés.
- Des signatures personnalisées peuvent être liées au pare-feu pour protéger ces composants.

A7:2021 — Authentification rompue

Les fonctions d'application liées à l'authentification et à la gestion des sessions sont souvent mal mises en œuvre, ce qui permet aux attaquants de compromettre des mots de passe, des clés ou des jetons de session, ou d'exploiter d'autres failles de mise en œuvre pour assumer temporairement ou définitivement l'identité d'autres utilisateurs.

- Le module NetScaler AAA effectue l'authentification des utilisateurs et fournit une fonctionnalité d'authentification unique aux applications principales. Il est intégré au moteur de stratégies NetScaler AppExpert pour permettre des stratégies personnalisées basées sur les informations des utilisateurs et des groupes.
- À l'aide des fonctionnalités de déchargement SSL et de transformation d'URL, le pare-feu peut également aider les sites à utiliser des protocoles de couche de transport sécurisés pour empêcher le vol de jetons de session par reniflage du réseau.
- Le proxy et le chiffrement des cookies peuvent être utilisés pour limiter complètement le vol de cookies.

A8:2021 - Défaillance du logiciel et de l'intégrité des données

Une désérialisation non sécurisée entraîne souvent l'exécution de code à distance. Même si les failles de désérialisation n'entraînent pas l'exécution de code à distance, elles peuvent être utilisées pour exécuter des attaques, y compris des attaques par rediffusion, des attaques par injection et des attaques par telévation de privilèges.

Protections de NetScaler Web App Firewall

- Inspection de la charge utile JSON avec des signatures personnalisées.
- Sécurité XML : protège contre le déni de service XML (XDoS), les injections XML SQL et Xpath et les scripts intersites, les contrôles de format, la conformité aux profils de base WS-I, le contrôle des pièces jointes XML.
- Des contrôles du format des champs, de la cohérence des cookies et de la cohérence des champs peuvent être utilisés.

A9:2021 - Défaillances de journalisation et de surveillance de la sécurité

Une journalisation et une surveillance insuffisantes, associées à une intégration manquante ou inefficace avec la réponse aux incidents, permettent aux attaquants d'attaquer davantage les systèmes, de maintenir la persistance, de basculer vers d'autres systèmes et de falsifier, extraire ou détruire des données. La plupart des études sur les violations montrent que le délai de détection d'une violation est de plus de 200 jours, généralement détecté par des parties externes plutôt que par des processus internes ou une surveillance.

- Lorsque l'action de journalisation est activée pour les contrôles de sécurité ou les signatures, les messages de journal résultants fournissent des informations sur les demandes et les réponses que le pare-feu d'applications a observées lors de la protection de vos sites Web et applications.
- Le pare-feu d'application offre la commodité d'utiliser la base de données ADC intégrée pour identifier les emplacements correspondant aux adresses IP d'où proviennent les demandes malveillantes.
- Les expressions de format par défaut (PI) offrent la possibilité de personnaliser les informations incluses dans les journaux avec la possibilité d'ajouter les données spécifiques à capturer dans les messages de journal générés par le pare-feu de l'application.
- Le pare-feu d'application prend en charge les journaux CEF.

Références

- Contrôle d'injection HTML SQL
- Vérification de l'injection XML SQL
- Utilisation de la ligne de commande pour configurer la vérification des scripts intersites HTML
- Vérification des scripts intersites XML
- Utilisation de la ligne de commande pour configurer le contrôle de sécurité en cas de dépassement de la mémoire tampon
- Ajouter ou supprimer un objet de signature
- Configuration ou modification d'un objet Signatures
- Mettre à jour un objet de signature
- Intégration de règles Snort
- Détection de bot
- Déployer une instance NetScaler VPX sur Microsoft Azure

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.

 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.

NSDoc0330VM - Network interfaces				
Search (Ctrl+/)	Search network interfaces			
e iags	NAME	^ PUBLIC IP ADDRESS		
X Diagnose and solve problems	nsdoc0330vm923	13.78.187.150		
SETTINGS				
Availability set				
😤 Disks				
Extensions				
Network interfaces				
Size				

2. Cliquez sur Configurations IP, puis sur Ajouter.



3. Fournissez les détails requis comme indiqué dans l'exemple ci-dessous et cliquez sur OK.

Add IP configuration	
* Name	
PrivateIP5	~
Туре	
Primary Secondary	
Primary IP configuration already exists	
Private IP address settings	
Allocation	
Dynamic Static	
* IP address	
192.0.0.8	~
Public ID address	
Disabled Enabled	
bibliocal Endored	
ОК	

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

January 15, 2025

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.

1	<pre>\$locName="westcentralus"</pre>
2	
3 4	<pre>\$rgName="Azure-MultilP"</pre>
5	<pre>\$nicName1="VM1-NIC1"</pre>
6	
7	\$vNetName="Azure-MultiIP-vnet"
8	
9	\$vNetAddressRange="11.6.0.0/16"
10	
11	<pre>\$trontEndSubnetName="trontEndSubnet"</pre>
12	<pre>\$frontEndSubnotDongo=#11 6 1 0/24#</pre>
15 14	\$11 OILEIUSUDIIetKalige- 11.0.1.0/24
15	<pre>\$prmStorageAccountName="multiipstorage"</pre>
16	
17	<pre>\$avSetName="multiip-avSet"</pre>
18	
19	<pre>\$vmSize="Standard_DS4_V2" (This parameter creates a VM with up to four NICs.)</pre>

Remarque :

La configuration minimale requise pour une instance VPX est de 2 vCPU et 2 Go de RAM.

```
$publisher="Citrix"
1
 2
     $offer="netscalervpx110-6531" (You can use different offers.)
3
4
     $sku="netscalerbyol" (According to your offer, the SKU can be
5
         different.)
6
7
     $version="latest"
8
     $pubIPName1="PIP1"
9
10
11
     $pubIPName2="PIP2"
```

12	
13	\$domName1="multiipvpx1"
14	
15	\$domName2="multiipvpx2"
16	
17	<pre>\$vmNamePrefix="VPXMultiIP"</pre>
18	
19	<pre>\$osDiskSuffix="osmultiipalbdiskdb1"</pre>
20	
21	<pre>**Network Security Group (NSG)-related information**:</pre>
22	
23	\$nsgName="NSG-MultiIP"
24	
25	<pre>\$rule1Name="Inbound-HTTP"</pre>
26	
27	<pre>\$rule2Name="Inbound-HTTPS"</pre>
28	
29	<pre>\$rule3Name="Inbound-SSH"</pre>
30	
31	<pre>\$IpConfigName1="IPConfig1"</pre>
32	
33	<pre>\$IPConfigName2="IPConfig-2"</pre>
34	
35	\$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-AzureRmPublicIpAc -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.

```
1
    $IPAddress1="11.6.1.27"
    $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
2
        Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress
        $pip1 – Primary
3
    $IPAddress2="11.6.1.28"
4
    $IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
        Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress
        $pip2
5
    $IPAddress3="11.6.1.29"
    $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
6
        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="<resource group name&gt;" $locName="&lt;location
name, such as West US> 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&gt;" $saType="&lt;storage
account type>",spécifiez-enune: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=New-
AzureRmVirtualNetworkSubnetConfig -Nom backendSubnet -AddressPrefix
$BackendAddressPrefix New-AzureRmVirtualNetwork -Nom TestNet
-ResourceGroupName $rgName -Emplacement $locName -Préfixe d'
adresse $vnetAddressPrefix -Sous-réseau $frontendSubnet,$backendSubnet
```

```
    $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
frontendSubnet -AddressPrefix $FrontendAddressPrefix
    $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
backendSubnet -AddressPrefix $BackendAddressPrefix
    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 :

2

- 1 \$nicName="frontendNIC"
- 3 \$domName="vpxazure"

```
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

```
$∨mName="<VM name>"
```

```
$vmSize="<VM size string>"
```

```
$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName
```

```
$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetIc
$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 :

```
1 Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
2
3 $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 :

1 2	\$diskName="dynamic"
3	<pre>\$pubName="citrix"</pre>
5	<pre>\$offerName="netscalervpx110-6531"</pre>
7	\$skuName="netscalerbyol"
9	<pre>\$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName \$rgName -Name \$saName</pre>
10	
11	<pre>\$osDiskUri=\$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/</pre>
12	
13	\$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="<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
```

```
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.

\$vnetName = "LBVnet" 1 2 3 \$FrontendAddressPrefix="10.0.1.0/24" 4 \$BackendAddressPrefix="10.0.2.0/24" 5 6 7 \$vnetAddressPrefix="10.0.0/16" 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"

```
3 $publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
ResourceGroupName $rgName -Location $locName -
AllocationMethod Static -DomainNameLabel nsvpx
```

Remarque:

Vérifiez la disponibilité de la valeur pour DomainNameLabel.

```
1 $FIPName = "ELBFIP"
2
3 $frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -
Name $FIPName -PublicIpAddress $publicIP1
4
5 $BEPool = "LB-backend-Pool"
6
7 $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.

```
1 $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.

```
1 $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.

1 \$inboundNATRule1= New-

```
AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1

-FrontendIpConfiguration $frontendIP1 -Protocol

TCP -FrontendPort 22 -BackendPort 22

3 $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.

```
1 $lbName="ELB"
2
3 $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

```
1
     $nicName="NIC1"
2
3
     $lbName="ELB"
4
5
     $bePoolIndex=0
6
7
     \times Rule indexes starts from 0.
8
9
     $natRuleIndex=0
10
11
     $subnetTndex=0
12
     \* Frontend subnet index
13
14
15
     $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
         $rgName
16
17
     $nic1=New-AzureRmNetworkInterface -Name $nicName -
         ResourceGroupName $rgName -Location $locName -Subnet $vnet.
         Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
         BackendAddressPools\[$bePoolIndex\] -
         LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
         \backslash ]
```

b) NIC2 avec VPX2

Par exemple :

```
1
     $nicName="NIC2"
2
     $lbName="ELB"
3
4
     $bePoolIndex=0
5
6
7
     $natRuleIndex=1
8
9
     \* Second Inbound NAT (SSH) rule we need to use
10
     `$subnetIndex=0
11
12
13
     \* Frontend subnet index
14
     $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
15
        $rgName
16
     $nic2=New-AzureRmNetworkInterface -Name $nicName -
17
        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

```
1
     $vmName="VPX1"
2
3
     $vmSize="Standard\_A3"
4
5
     $pubName="citrix"
6
7
     $offerName="netscalervpx110-6531"
8
9
     $skuName="netscalerbyol"
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
11
        ResourceGroupName $rgName
12
13
     $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
14
```

```
$cred=Get-Credential -Message "Type Credentials which will be
        used to login to VPX instance"
16
     $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
17
         $vmName -Credential $cred -Verbose
18
     $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
19
        Offer $offerName -Skus $skuName -Version "latest"
     $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id
22
23
     $diskName="dynamic"
24
25
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
          -Name $saName
26
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
27
        vhds1/" + $diskName + ".vhd"
28
     $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
29
        $osDiskUri1 -CreateOption fromImage
30
31
     Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
         $offerName -Name $skuName
32
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
         Ś∨m1
```

b) Instance 2 de NetScaler VPX

```
1
     $vmName="VPX2"
2
     $vmSize="Standard\_A3"
3
4
5
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
     $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
9
     $cred=Get-Credential -Message " Type Credentials which will be
        used to login to VPX instance "
     $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
11
        $vmName -Credential $cred -Verbose
12
13
     $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
     $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
15
16
     $diskName="dynamic"
17
```

```
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
21
        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
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $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="\\<resource group name\\&#062;"
$locName="\\&#060;location name, such as West US\\&#062;"
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="<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 $vnetAddressPrefix="10.0.0.0/16"
4
5 $FrontendAddressPrefix="10.0.1.0/24"
6
7 $BackendAddressPrefix="10.0.2.0/24"
8
```

9	<pre>\$vnet=New-AzureRmVirtualNetwork -Name \$vnetName - ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet\`</pre>
10	
11	
ΤŢ	frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix \$FrontendAddressPrefix
12	
13	<pre>\$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name</pre>
	backendSubnet -AddressPretix SBackendAddressPretix

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.

```
1 $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.

```
1 $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

```
1 $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 sousréseau que celui du sous-réseau ajouté.

```
1 $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

```
$vmName="VPX1"
2
3
     $vmSize="Standard\_A3"
4
5
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
     $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
     $cred=Get-Credential -Message "Type Credentials which will be
9
        used to login to VPX instance"
     $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
        $vmName -Credential $cred -Verbose
12
13
     $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15
     $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id
16
     $diskName="dynamic"
17
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
20
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds1/" + $diskName + ".vhd"
23
     $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25
     Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
        $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $vm1
```

b) Instance 2 de NetScaler VPX

```
1
    $vmName="VPX2"
2
    $vmSize="Standard\_A3"
3
4
    $avSet=Get-AzureRmAvailabilitySet -Name $avName -
5
        ResourceGroupName $rgName
6
    $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
9
    $cred=Get-Credential -Message " Type Credentials which will be
```

```
used to login to VPX instance "
10
     $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
11
        $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
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName + ".vhd"
22
     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
23
        $osDiskUri1 -CreateOption fromImage
24
     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
        $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $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.

Créez un ticket de support pour l'instance VPX sur Azure

January 15, 2025

Si vous rencontrez des problèmes avec votre instance NetScaler VPX sur Azure, à des fins de dépannage, vous pouvez créer un ticket de support dans le Portail d'assistance NetScaler. Pour déposer un ticket d'assistance, assurez-vous de ce qui suit :

- Votre réseau est connecté.
- Vous avez à portée de main votre numéro de compte Azure, le code PIN de support de l'offre basée sur un abonnement NetScaler que vous avez déployée sur Azure et le journal de série Azure.
 - Vous pouvez trouver le code PIN d'assistance sur le **Page Systèmes** dans l'interface graphique VPX.

Dashboard Configuration	Reporting Documentation Downloads	¢
Q Search Menu	System > System Information	
Favorites ~	System	
AZURE >	System Information System Sessions 2 System Network	
System ~	System Upgrade Reboot Migration Statistics Call Home NetScaler ADM Service Connect	
Licenses	System Information	
Settings		
Diagnostics	NetScaler ADC IP Address	
High Availability	Netmask 255.255.0	
- Ingri Availability	Node Standalone	
NTP Servers	Time Zene Coordinated Universal Time	
Reports	System Time Fri. 24 Nov 2023 09:58:26 UTC	
Poporting Configs	Last Config Changed Time Fri, 24 Nov 2023 09:55:45 UTC	
Reporting Comigs	Last Config Saved Time Fri, 24 Nov 2023 09:56:00 UTC	
Profiles		
Destition Administration	Hardware Information	

- Vous pouvez trouver le journal de série dans le portail Azure (**Diagnostics de démarrage** de votre machine virtuelle).

C Search «	🕐 Refresh 🚳 Settings 🧷 Troubleshoot
Policies	
Run command	Screenshot Serial log
onitoring	Updated: Friday, 8 September 2023 at 6:15:06 AM UTC Download serial log
Insights	אר ער ער ער ער אר אר אר אר
Alerts	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
AIELS	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Metrics	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
Diamatia atti	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Diagnostic settings	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Logs	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
5	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Connection monitor (classic)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Workbooks	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-
	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Itomation	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Tacks (provided)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
lasks (preview)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Export template	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
p	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
F	
Resource health	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
	-\/-\/-\/-\//-\//-\//-\//-\//-\//-\//-\
Boot diagnostics	-\\/-\\/-\\/-\\/-\\/-\\/-\\/-\\/

Une fois que vous avez toutes les informations prêtes, appelez le support NetScaler. Vous êtes invité à fournir votre nom et votre adresse e-mail.

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

January 30, 2025

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**.

		ler-vpx-platform-eng ▼	
ame vpxmgmt escription (Optional) management ypp Subnets ubnets let you create your own private cloud topology within Google Cloud. Click utomatic to create a subnet in each region, or click Custom to manually define the ubnets. Learn more ubnet creation mode Custom Automatic Yew subnet Name vpxmgmtsubnet Add a description Region aia-east1 P address range 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Pone Cancel + Add subnet ymamic routing mode P address only in the region in which they were created Cloud Routers will learn routes only in the region in which they were created Cloud Routers will learn routes only in the region in which they were created Cloud Routers will learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Cre	eate a VPC network	
<pre>vpxmgmt escription (Optional) management ygg subnets ubnets let you create your own private cloud topology within Google Cloud. Click utomatic to create a subnet in each region, or click Custom to manually define the ubnets. Learn more ubnet creation mode Custom Automatic Vew subnet Vew subnet Vew subnet Add a description Region @ asia-east1 P address range @ 192.168.30.0/24 Create secondary IP range Private Google access @ On Off Flow logs On Off Flow logs On Off Plone Cancel * Add subnet ynamic routing mode @ Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router </pre>	Name 🕜		
escription (Optional) management ygc Subnets ubnets let you create your own private cloud topology within Google Cloud. Click utomatic to create a subnet in each region, or click Custom to manually define the ubnets. Learn more ubnet creation mode Custom Automatic New subnet Name Vyxmgmtsubnet Add a description Region Paddress range Piveta Google access Pi	vpxmgmt		
management ygc Subnets ubnets let you create your own private cloud topology within Google Cloud. Click utomatic to create a subnet in each region, or click Custom to manually define the ubnets. Learn more ubnet creation mode Custom Automatic New subnet New subnet Name vyxmgmtsubnet Add a description Region asia-east1 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Flow logs On Cancel + Add subnet ynamic routing mode Pegional Cloud Routers will learn routes only in the region in which they were created Global Cloud Routers will learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Description	(Optional)	
Bubnets Ubnets let you create your own private cloud topology within Google Cloud. Click Utomatic to create a subnet in each region, or click Custom to manually define the Ubnets. Learn more Ubnet creation mode Custom Automatic New subnet New subnet New subnet Name Private Coogle access On Off Flow logs On Off Flow logs On Private Google access rivate Google access Private Goog	managem	ent ypc	
ubnets let you create your own private cloud topology within Google Cloud. Click utomatic to create a subnet in each region, or click Custom to manually define the ubnets. Learn more ubnet creation mode Custom Automatic New subnet Add a description Region @ asia-east1	Subnets		
ubnet creation mode Custom Automatic Name Image: Image	Subnets let y Automatic to subnets. Lea	ou create your own private cloud topology within Google Cloud. Click o create a subnet in each region, or click Custom to manually define the rn more	
New subnet Name Vyxmgmtsubnet Add a description Region asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access IP off Flow logs On Off Flow logs On Off Pone Cancel Privatic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Subnet crea	tion mode	
New subnet Name Name Name	Custom	Automatic	
Name	New subn	et 🝵	~
Name vpxmgmtsubnet Add a description Region asia-east1 IP address range asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access IP on On Off Flow logs On Off Pone Cancel + Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router			
Add a description Region asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Flow logs On Off Done Cancel + Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	voxmam	tsubnet	
Add a description Region Region In address range In address rad	TPATIgit		
Region asia-east1 IP address range IP address	Add a des	ription	
asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Region 🕜		
IP address range IP address range IP 2.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	asia-eas	1	-
192.168.30.0/24 Create secondary IP range Private Google access • On Off Flow logs On Off Done Cancel Pregional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	IP address	range 💿	
Create secondary IP range Private Google access On Off Flow logs On Off Done Cancel reace reace reace Cancel Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	192.168	30.0/24	
Create secondary IP range Private Google access On Off Flow logs On Off Done Cancel + Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router			
Private Google access On Off Flow logs On Off Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Create sec	ondary IP range	
 On Off Flow logs On Off Done Cancel <u>Add subnet</u> ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router 	Private Go	ogle access 📀	
 Off Flow logs On Off Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	🔘 On		
Flow logs On Off Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global G	Off		
 On Off Done Cancel + Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Flow logs		
Off Done Cancel Add subnet ynamic routing mode Pegional Cloud Routers will learn routes only in the region in which they were created Global Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	🔿 On		
Done Cancel Add subnet ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Off		
Add subnet Add subnet Add subnet Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Done	Cancel	
 ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router 		+ Add subnet	
 ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router 			
Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Region	rting mode 💿 I	
Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Cloud R	outers will learn routes only in the region in which they were created	
	Global Global re VPN or i	outing lets you dynamically learn routes to and from all regions with a sin nterconnect and Cloud Router	ngle
Create			

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.

😔 netscaler-vp	x-platform-eng 👻
← Create	a firewall rule
Firewall rules con incoming traffic f	trol incoming or outgoing traffic to an instance. By default, rom outside your network is blocked. Learn more
Name 🕜	
vpxmgmtingress	srule
Description (Option	nal)
management tra	ffic ingress rules
Logs Turning on firewall Stackdriver. Learn r On	ogs can generate a large number of logs which can increase costs in nore
Off	
Network	
vpxmgmt	•
Priority 🕜 Priority can be 0 - 6	5535 Check priority of other firewall rules
1000	
Ingress Egress Action on match Allow Deny Targets	
All instances in t	he network 👻
Source filter 🕜	
IP ranges	•
Source IP ranges	0
0.0.0/0 😢	
Out and a survey film	
None	er 🕑
None	
Protocols and port Allow all Specified prot	s 😨
🗹 tcp :	22, 80, 443
udp :	all
Other pro	tocols
protoco	ols, comma separated, e.g. ah, sctp
Y Dischla mile	
 Disable rule 	
Create	el

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.

≡ Google Cloud		
🖄 Marketplace		Q. NetScaler VPX X
Marketplace > "NetScaler VPX	<"	
Marketplace home	2 results	
 ★ Your products ★ Your orders 	netscaler	NetScaler VPX FIPS - Customer Licensed Citrix Systems, Inc. NetScaler VPX FIPS (formerly Citrix ADC) is an enterprise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to meet your business indice needs. Designed to provide operational consistency and a securely, with the deployment and pricing flexibility to meet your business the hybrid cloud. Designed to provide operational consistency and a securely with the deployment and pricing flexibility to the hybrid cloud. MatScaler URE (DE is in NIEC proceed for EIDS 140.2 and 1
Type to filter		sinoun user experience, recourse eases your variation to the ryonu cloud, recourse VFX FIF3 is in First process for FIF3 140-2 Level 1
Category Security Networking	 (1) netscaler (2) 	NetScaler VPX - Customer Licensed Citrix Systems, Inc. NetScaler (formerly Citrix ADC) is an enterprise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to meet your business' unique needs. Designed to provide operational consistency and a smooth user experience, NetScaler eases your transition to the hybrid cloud. Why NetScaler? NetScaler offers high performance with fast application
Туре	^	
Virtual machines	(2)	
Price	^	
BYOL	(2)	

4. Cliquez sur Lancer sur l'abonnement sélectionné.

net>scaler.	NetScaler	VPX - Custor	ner Licensed	
	NetScaler: Load	Balancer, SSL VPN, V	VAF & SSO	
	LAUNCH	IEW DEPLOYMENTS	CONTACT SALES	
	Click to configure			

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 NICO.
- 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**.

Create a VPC network Name Name vprrgmt Description (Optional) management ygp Subnets Subnets easy out own private cloud topology within Boogle Doud. Click Automatic to ensue a value in each region, or click Contom to menually define the subnet. Learn more subnet in each region, or click Contom to menually define the subnet. Learn more subnet in each region, or click Contom to menually define the subnet. Learn more subnet in each region, or click Contom to menually define the subnet. Learn more subnet in each region, or click Contom to menually define the subnet. Learn more subnet in each region, or click Contom to menually define the subnet. Learn more subnet in each region in the subnet in each region in the subnet. Learn more subnet in each region in the subnet in the subnet. Learn more subnet in each region in the subnet in the subnet. Learn more subnet in each region in which they were created in the subnet. Cancel Presional Concel	▶ netscaler-vpx-platform-eng 👻
Name	Create a VPC network
wperngmt Description (Cptional) management ygg Subnets Subnets let you ernete your new privete cloud tapplogy within Google Cloud. Click Automatic to create a subnet in each region, cr click Custom to manually define the subnet. Learn more subnet in each region, cr click Custom to manually define the subnet. Learn more subnet is a contract of the subnet is contract on mode Custom. Automatic New subnet Automatic New subnet Add a description Region @ Sise est1 IP address range @ 192.168.30.0/24 Creats saccondary IP range Private Google access @ On Off Five logs Off Five logs Off Pradices range @ Private Google access @ Private Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @ Privet Google access @<td>Name 🛞</td>	Name 🛞
Description (Cptional) management ygg Subnets Suborts let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnet. Learn more Subnet readom mode Custom Automatic New subnet Automatic New subnet Add a description Region Segion	vpxmgmt
management ygg:	Description (Optional)
Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnets Subnet Sub	management ypp
Subrets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subret in each region, or click Custom to mensality define the submets. Learn mode Custom Automatic Name Automatic Name Automatic Name Comparison Name Comparison Subret Add a description Region Comparison Subret Add a description Region Comparison Subret National Comparison Subret National Comparison Subret Name Comparison	Subnets
Automatic to create a submet in such region, or click Custom to mensadly define the submet is usen more submet in such region, or click Custom to mensadly define the submet is usen more submet in such region and a classifier of the submet is in	Subsets lat you create your own orients cleared togethers within Genetic Cleared. Click
subnets. Lear more Subnet reaction mode Custom Automatic New subnet Name yporngmtsubnet Add a description Regin selie exit Paddress range 192: 168: 30:0:24 Creats secondary (Prange Private Google access Creats Secondary (Prange Creats Secondary (Prange	Automatic to create a subnet in each region, or click Custom to manually define the
Subnet exerction mode Custom Automatic New subnet Name yourngmtsubnet Add a description Region sibe dest1 r r edd a description Region sibe dest1 r edd a description Region a description r edd a description Region a description r edd a description r edd a description Region	subnets. Learn more
Custom Automatic New subnet Name • vpmmgntsubnet Add a description Region • sila east1 192 168,30,0/24 Creats accendary IP range Private Google access • • Off Flow logs • Off Done Cancel	Subnet creation mode
New subnet Name Yexengmitsubnet Add a description Regin asia description Regin regin asia destil regin regi	Custom Automatic
Nerre © Vpurngmitsubnet Add a description Add a description Region © Sila edst1 P address range 192.168.30.0/24 Pratic scoole access Cont Cont Cont Cont Cont Cont Cont Cont	
Name	New subnet
	Name 😥
Add a description Region	vpxmgmtsubnet
Region sila east1 IP address range 192.168.30.0/24 IP address range 192.168.30.0/24 Cracet secondary IP range Private Google access Ch Off Flow logs Off Flow logs Off Done Cancel Pregional Cheat Routers will learn noutes only in the region in which they were created Global nouting lets you dynamically learn noutes to and from all regions with a single VPN or intercontext and Coud Router 	Add a description
	Region @
IP address range IP Address range IP Address	
IP address range	asia-easti *
	IP address range 🐵
Creats secondary IP range Private Google access Creats Secondary IP range Private Google access Creats Private Google access Creats Private Google Creats Private Creat	192.168.30.0/24
Private Google soccess	Create secondary IP range
On Of Flow logs On Of Flow logs On On Of Done Cancel Cancel Paginal Clead Routers will earn noutes only in the region in which they were created Global Global Global Clead Routers to and from al regions with a single VNN or intercontex and Cloud Router Over the Cancel Cancel	Private Google access 🐵
On Of Of Flow logs On Of Of Cancel Cancel Add subnet Donamic routing mode Occurs Regional Cloud Routers will earn routes only in the region in which they were created Global Cloud Routers will earn routes on and from all regions with a single WNo ristecomest and Cloud Router Overlage Cancel Contel Cancel Contel Cancel	
	• On Off
Flow logs Off Off Cancel	
On Of Of Of Cancel Add subnet Add subnet Add subnet Cloud Routers will earn routes only in the region is which they were created Global Routers will earn routes only in the region is which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single WN or intercomet and Cloud Router Costol Cancel Cancel	Flow logs
Off One Cancel Add subnet Add subnet Pynamic routing mode Cancel Pynamic routing mode Oth Cancel Canc	0 m
Cancel Cancel Add subnet Pramic routing mode Regional Cloud Routes will learn routes only in the region in which they were created Global Global Global Concel Cancel Cancel Cancel Cancel	• off
Done Cancel + Add subnet Cloud Routers will earn routes only in the region in which they were created Obtail Cloud Routers will earn routes only in the region in which they were created Obtail Cloud Router will earn routes to and from all regions with a single VPN or interconnect and Cloud Router Cloud Router	
Add subset Pynamic routing mode Regional Cloud Routes will learn routes only in the region in which they were created Global Global VPN or interconnect and Cloud Router Oracle Casele Casel	Done Cancel
Add subset Dynamic routing mode Regional Claud Routes will learn routes only in the region in which they were created Global Global UPN or interconnect and Cloud Router Orable Cancel Ca	
Dynamic routing mode Regional Cloud Routers will learn outes only in the region in which they were created Cloud Routers will sear notes only in the region in which they were created Cloud Router Create Case Case Concert	+ Add subnet
Opmanic routing mode Image: Second seco	
regional Cloud Routes will learn notices only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router Create Cancel	Dynamic routing mode
Global Global routing lets you dynamically learn nutes to and from all regions with a single VPN or interconnect and Cloud Router Create Cancel	 Regional Cloud Routers will learn routes only in the region in which they were created
Global routing lets you dynamically learn neutes to and from all regions with a single VPN or interconnect and Cloud Reuter	Global
VPN or interconnect and Cloud Router	Global routing lets you dynamically learn routes to and from all regions with a single
Create Cancel	VPN or interconnect and Cloud Router
Create Cancel	
	Create Cancel

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.

NetScaler VPX 14.1

🔹 netscaler-vpx-platform-eng 👻
Create a firewall rule
Firewall rules control incoming or outgoing traffic to an instance. By default,
incoming traffic from outside your network is blocked. Learn more
voxmgmtingressrule
Description (Optional)
management traffic ingress rules
Logs Turning on firewall logs can generate a large number of logs which can increase costs in Steckforker. Learn more
• off
Network 🕡
vpxmgmt -
Priority ③ Priority can be 0 - 65535 Check priority of other finewall rules
1000
Action on match
All instances in the patranck
An instances in the network
Source filter 🛞
IP ranges *
Source IP ranges 💿
0.0.0.0/0 💌
Second source filter
None *
Protocols and ports Allow all Specified protocols and ports
✓ tcp : 22, 80, 443
udp: all
Other protocols
protocols, comma separated, e.g. ah, sctp
➢ Disable rule
Create Cancel

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 Engineet sélectionnez Images.
- 3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.

۲	Compute Engine	Images	[+] CREATE IMAGE	C REFRESH	CREATE INSTANCE]	⊖ DEPRECAT
B	VM instances						
4 54	Instance groups	= Filter image	S			0	Columns 👻
	Instance templates						
8	Sole tenant nodes	<< Previous	2 Next >>				
Ð	Disks	Name		Size	Created by		
0	Snapshots	🗹 🔮 nsvpx-12-1	-50-9	20 G	В		
[2]	Images						

Oranto en instance

4. Sélectionnez un type d'instance avec deux vCPU (configuration minimale pour l'ADC).

~	Create an Instance					
To cr	eate a VM instance, select one of the options:		Name ©			
A	New VM Instance Greate a single VM instance from scratch	>	vpor-Inic Labels () (Optional) shutdrawn : no			
Ħ	New VM instance from template Create a single VM instance from an existing template		+ Add label Region (i) Zone (i) Region is permanent Us-east1 (South Carolina) * Us-east1-b *			
	New VM instance from machine image Create a single VM instance from an existing machine image Marketplace Deploy a ready-to-go solution onto a VM instance	E	Machine configuration Machine family General-purpose Compute-optimized Memory-optimized Machine types for common workloads, optimized for cost and flexibility Sories N1 Powered by Intel Skylake CPU platform or one of its predecessors			
			Machine type Int-standard-2 (2 vCPU, 7.5 GB memory) vCPU Memory GPUs 2 7.5 GB CPU platform and GPU Confidential VM service Enable the Confidential Computing service on this VM instance. Container Container			

- 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 NICO.
- 3. Dans le champ **Plage d'adresses IP d'alias**, saisissez les adresses IP d'alias.

VM instance details	/ EDIT	🖑 RESET	CREATE MACHINE IMAGE	E CREA
ietwork interfaces 🛞				
Network interface		^		
You must stop the VM instance to edit network, e Network	subrietwork or inter	nal IP address		
automationmgmtnetwork		Ψ.		
Subnetwork 💮				
mgmtsubnet (192.168.1.0/24)		*		
Internal IP 192.168.1.50 Internal IP type				
Ephemeral				
Alias IP ranges Subnet range Alias IF	range 🛞			
Primary (192.168.1.0/24) * 192.1	168.1.3/32	×		
Primary (192.168.1.0/24) * 192.1	168.1.7/32	×		
+ Add IP range	e			
☆ Hide alias IP ranges				
External IP		_		
Primary (192.168.1.0/24) Primary (192.168.1.0/24) Primary (192.168.1.0/24)	168.1.3/32 168.1.7/32	× ×		
Ephemeral		*		
Network Service Tier Premium (Current project-level tier, cl Standard (us-east1)	hange) 💿			
IP forwarding Off				

- 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**.
| <u>د</u> ۱ | /M instance details | 10 | DIT ÖRESET | CREATE MACHINE IMA | DE 🐘 CREATE SIMILAR | E STOP | II SUSPEND | B DELET |
|---|--|----------------------|---------------------|--------------------------------|----------------------------|-----------------|---------------|-----------------|
| [] Eral | ble-connecting to serial ports 🔞 |) | | | | | | |
| Loge
Doud Lo
Serial pro
2 More | ogging
an 1 (console) | | | | | | | |
| Instance
2543534 | 44482010607122 | | | | | | | |
| Mashine
ni-stand | type
fair62 (2 vOPUs, 7.5 68 memory | 6 | | | | | | |
| Reserval | ian
fically choose | | | | | | | |
| ceuplat
Intellity | fam.
Aard | | | | | | | |
| Display of
Turn on a | tevice
a display device if you want to use
an display device | action capituling or | nd recording tools. | | | | | |
| Zane
so sepi1 | | | | | | | | |
| Labels | wn no | | | | | | | |
| Deation
Feb 22, 1 | time
2021, 6:19:01 PM | | | | | | | |
| Network | Interfaces
Network | Submetwork | Primary internal IP | Alias IP ranges | External IP | Network Tier () | IP forwarding | Network details |
| nică | automationingentrietwork | ingritaubent | 192.168.1.50 | 192.148.1.3/32, 192.168.1.7/32 | 106.196.190.91 (sphemoral) | Premium | Off | View details |
| Public D | NS PTR Record | | | | | | | |

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**.

CİİTIX.) fron	m Marke	tplace									HA Status Piot configured	Partition of default	nan	not ~
Dashboard	Configural	tion	Repor	ting Do	cumentation	Do	wnloads						ł	2
Q, Search in Meru		System	> Nets	eark > IPs >	IPV46									
Google Cloud Platform	>	IDe											0	
Bystem	~	IF 9											~	
Licenses		IPV4a	3	IPV8x 1										
Settings		444	1	Delete	fituation in a	Deler	Acturbe							
Diagnostics]											
High Availability	>	Q Cir	k here is	service or Ace to	menter Key : Value Ib	ernal								O
NTP Servers				PAIDRESS	C STATE		TIPE	MODE 0	ARP .	X2MP	VIETUAL SCENE	R C TRAF	TE DOMAIN	1 1
Reports			2	192.188.17	ENABLED		Satest P	Active	ENABLED	ENABLED	-10 A-			0
Profiles				192.198.1.3	ENABLED		Virtual IP	Activa	ENABLED	ENABLED	ENABLED			D
Partition Administrat	son >			192,168,150	ENABLED		NitScill P	Active	ENABLED	ENABLED	-10 A-			Ð
User Administration	>	Total	3								25 Per Page	⊻ Page 1	att	- b-
Authentication	>													
Auditing	2													

- 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 sousréseau 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.

- 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), l'adresse IP (adresse IP), l'adresse IP), l'adresse IP (adresse IP), l'adresse - 3. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bala	ancing Virtu	al Server		
Basic Settings				
Create a virtual as IP address. If the a You can configure	erver by specifying a name application is accessible o multiple virtual tervers to	, an IP address, s pr nig from the local ar receive client requ	ert, and a protocol type. If an ap to network (LAN) or wide area ests, thereby increasing the av	pitation is accessible from the internet, the virtual server IP (VIP) address is a public activory (NAVA), the VIP is usually a private IICAAN non-mutable) IP address, simbility of resources to process client requests.
Nome*		0		
Protocol*		U I		
HTTP	`	·		
IP Address Type*				
IP Address	`	·		
IP Address*				
192.168.1.3		0		
Port*		0		
► Ware				
ок	Cancel			

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 équilibragede 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 :

Remarque :

&lt; 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 valide. L'option de licence disponible pour les instances NetScaler VPX exécutées sur GCP est la suivante :

Apportez votre propre permis (BYOL): Pour utiliser l'option BYOL, procédez comme suit :

- Utilisez le portail de licences sur le site Web de NetScaler pour générer une licence valide.
- Téléchargez la licence générée dans l'instance.
- NetScaler VPX Check-in et Check-out de licence: Ce modèle de licence vous permet d'extraire une licence d'un pool de licences disponibles et de la réarchiver lorsqu'elle n'est plus nécessaire. Pour plus d'informations et des instructions détaillées, consultez Enregistrement et extraction de la licence NetScaler VPX.

Remarque :

Les licences basées sur l'abonnement ne sont plus prises en charge pour les instances NetScaler VPX sur GCP.

Offres NetScaler VPX prises en charge sur GCP

Le tableau suivant répertorie les offres NetScaler VPX prises en charge sur GCP.

Offres VPX prises en charge

NetScaler VPX – Licence client

NetScaler VPX FIPS - Licence client

Familles de types de machines GCP prises en charge

Famille de types de machines	Type de machine minimum
Machines à usage général	e2-moyen, e2-standard-2, e2-highmem-2, n1-standard-2, n1-highmem-2, n2-standard-2,
	n2-highmem-2, n2d-standard-2, n2d-highmem-2
Machines optimisées pour le calcul	c2-standard-4, c2d-standard-2, c2d-highmem-2

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.

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.

Service account iii	
Compute Engine default service account	
Allow full access to all Cloud APIs Set access for each API	

 Assurez-vous que le rôle IAM associé à votre compte de service GCP dispose des autorisations IAM suivantes :

1	REQUIRED_INSTANCE_IAM_PERMS = [
2	
3	"compute.addresses.use",
4	"compute.forwardingRules.list",
5	"compute.forwardingRules.setTarget",
6	"compute.instances.setMetadata"
7	"compute.instances.addAccessConfig",
8	"compute.instances.deleteAccessConfig",
9	"compute.instances.get",
10	"Compute.instances.list",
11	"compute.networks.useExternalIp",
12	"compute.subnetworks.useExternalIp",
13	"compute.targetInstances.list",
14	"compute.targetInstances.use",
15	"compute.targetInstances.create",
16	"compute.zones.list",
17	"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**.

Network interface	^
Network clientypc-ss	
Subnetwork	
Internal IP	
Internal IP type	
Ephemeral	•
℅ Show alias IP ranges	
External IP 📀	
None	
Ephemeral	
vpxpublic (35.229.255.208)	
Premium tier	
Create IP address	
Silv	

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**.

System / High Availa	bility / Nodes					
Nodes 2						C ;
Add Edit	Delete Statistics	Select Action \checkmark				
ID \$	IP ADDRESS 💠 HOST NAME 🗘	MASTER STATE	NODE STATE	INC \Diamond	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REASON
0	192.168.1.3	Primary	• UP	ENABLED	ENABLED	-NA-
1	192.168.1.66	Secondary	• UP	ENABLED	SUCCESS	-NA-
Total 2					25 Per	Page 🗸 Page 1 of 1 < 🕨

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**.

IPs												
IPV4s 4	IPV6s 1											
Add Edit Delete Statistics Select Action V												
\mathbf{Q} Click here to	search or you can ente	r Key : Value format								(j)		
	IP ADDRESS	STATE	TYPE 0	MODE 0	ARP		ICMP 0	VIRTUAL SERVER	C TRAFFIC DOMAIN			
Secondary VIP	192.168.2.54	ENABLED	Virtual IP	Active	ENABLED		ENABLED	ENABLED		0		
Primary SNIP	192.168.3.7	ENABLED	Subnet IP	Active	ENABLED		ENABLED	-N/A-		0		
Primary VIP	192.168.2.37	ENABLED	Virtual IP	Active	ENABLED		ENABLED	ENABLED		0		
	192.168.1.3	ENABLED	NetScaler IP	Active	ENABLED		ENABLED	-N/A-		0		
Total 4	*							25 Per Page →	Page 1 of 1 🔍	$\left \cdot \right $		

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**.

IPs												
IPV4s 3	IPV6s 1											
Add E	dit Delete	Statistics		Select Action 🗸]							
Q Click here to	search or you can enter	Key : Value forma	t									()
	IP ADDRESS	STATE		TYPE		MODE	ARP	ICMP	VIRTUAL SERVER		TRAFFIC DOMAIN	
Secondary SNIP	192.168.3.76	ENABLED		Subnet IP		Active	ENABLED	ENABLED	-N/A-			0
Secondary VIP	192.168.2.54	ENABLED		Virtual IP		Passive	ENABLED	ENABLED	ENABLED			0
	192.168.1.66	ENABLED		NetScaler IP		Active	ENABLED	ENABLED	-N/A-			0
Total 3									25 Per Page →	Pag	ge 1 of 1 🔍	

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.

NetScaler VPX 14.1

Citrix ADC VP	X Express (Fre	emium)						HA Status Primary	Partition . default	~ nsr	oot V
Dashboard	Configuration	Reporting	Documentation	Downloads							¢
G Create IP S	Set	IPV4s	0								С×
Name*		Add	Edit Delete	Statistics	Select Action ~						
ipset1		Q Click here	to search or you can enter Ke	ey : Value format							()
Traffic Domain			IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE	MODE 0	ARP 0	ICMP	VIRTUA
		Adv	192.168.1.3	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
IPut IPut			192.168.2.37	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLI
			192.168.3.7	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
Course I Course			192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLE
Insert Deich		Total 4						25 Per Pa	ige 🗸 Page	1 of 1	< >
No items		inster	Close								
Create											
										(9

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.

Dashboard	Configuration	Reporting) Do	cumentation	Downloads							٠	
G Create IP	Set	IP\	/4s 🔳									C	×
Namel		~	id Ed	lit Delete	Statistics	Select Action V							
ipset1		Qa	ck here to sea	rch or you can enter Ke	y : Value format								()
Traffic Domain				IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE 0	MODE :	ARP :	ICMP	0	VIRTUA
		Adk		192.168.1.66	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED		N/A-
10.4				192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED		ENABL
1PV4 1PV5				192.168.3.76	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED		N/A-
Insert Dele		Total	3						25 Per Pag	e 🗸 Page	1 of 1	4	Þ
IP ADDRESS			nser	Close									
No items													
Create													

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.

G Load Balancing Virtual Server

Basic Settings	Help	>
Create a virtual server by specifying a name. an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (NP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAA), the VP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests. Name* Ib-vserver1 Protocol* IP Address Type* IP Address Void Address*		
192 . 168 . 2 . 37 (D) × Please enter value		
Pog* 80		9
Traffic Domain		

- 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.

1 add ha node 1 <sec_ip> -inc ENABLED

Sur le nœud secondaire, tapez la commande suivante.

1 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.

```
1 add ns ip <primary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_vip> <subnet> -type VIP
4
5 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.

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 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 :

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
```

Sur le nœud secondaire, tapez la commande suivante :

```
1 add ipset <ipsetname>
2 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 :

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 :

1 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 :

1 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 > Ac-tion > Forcer le basculement**.

Depuis la CLI, saisissez la commande suivante :

1 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.



Firewall 🙆

Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

1 REQUIRED_INSTANCE_IAM_PERMS = [2 "compute.forwardingRules.list", 3 "compute.forwardingRules.setTarget", 4 "compute.instances.setMetadata", 5 "compute.instances.get", 6 "compute.instances.list", 7 "compute.instances.updateNetworkInterface",

```
8 "compute.targetInstances.list",
9 "compute.targetInstances.use",
10 "compute.targetInstances.create",
11 "compute.zones.list",
12 "compute.zoneOperations.get",
13 ]
```

• Si vos machines virtuelles n'ont pas accès à Internet, vous devez activer Private Google Access

	Add a subnet	
	Name 🛞 Name is permanent	
	management-subnet	
	Add a description	
	VPC Network	
	automationmgmtnetwork	
	Region 😡	
	us-east1 -	
	Reserve for Internal HTTP(S) Load Balancing 🔞	
	On Off	
	IP address range 🕡	
	192.168.2.0/24	
	Create secondary IP range	
	Private Google access 💿	
	On Off	
	Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more	
	On Off	
sur le sous-réseau VPC.	CANCEL	ADD

 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.

You must stop the VM instance to	edit network, subnetwork or internal IP addr	ess
Network 🕜		
automationmgmtnetwork		Ŧ
Subnetwork 🕜		
mgmtsubnet (192.168.1.0/24,	us-east1)	-
Internal IP 192.168.1.71		
Internal IP type		
Ephemeral		-
Subnet ranges	Alias IP range	
Primary (192.168.1.0/24)	· 192.168.1.5/32	Primary Client Alias
Primary (192.168.1.0/24)	▼ 192.168.1.6/32	Primary Server Alia
+	Add IP range	
 Uide elies ID renges 		
 Fide allas in faliges 		
External IP 💿		
		*
Ephemeral		
Ephemeral Network Service Tier		
Ephemeral Network Service Tier Premium (Current projee Standard (us-east1)	ct-level tier, change) 📀	
Ephemeral Network Service Tier Premium (Current projec Standard (us-east1)	ct-level tier, change) 💿	
Ephemeral Network Service Tier • Premium (Current projection of the second of the se	ct-level tier, change) 💿	
Ephemeral Network Service Tier Premium (Current project Standard (us-east1) Pforwarding Dff Public DNS PTR Record Enable	ct-level tier, change) 📀	

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.

Network interface		^					
You must stop the VM instance to edit n	etwork, subnetwork or internal IP address						
automationmgmtnetwork							
Subnetwork 👔							
mgmtsubnet (192.168.1.0/24, us-e	ast1)	-					
Internal IP 192.168.1.76							
Ephemeral		-					
Alias IP ranges	Secondary Subnet IP(SNIP)						
Subnet range	Alias IP range 🛞	1					
Primary (192.168.1.0/24) *	192.168.1.7/32	×					
+ Add	IP range						
☆ Hide alias IP ranges External IP							
Ephemeral		*					
Network Service Tier Premium (Current project-lev Standard (us-east1)	el tier, change) 🐵						
Public DNS PTR Record							
PTR domain name							
Done Cancel							

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.

k

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**.

System > High Availability > Nodes											
Nodes 🔹											
Add	Add Edit Delete Statistics Select Action										
	ID 🔅	IP ADDRESS 🔅	HOST NAME 🔅	MASTER STATE	NODE STATE	INC \$	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REA			
	0	192.168.1.71		Primary	• UP	ENABLED	ENABLED	-NA-			
	1	192.168.1.76		Secondary	• UP	ENABLED	SUCCESS	-NA-			
Total 2							25 Per Page	✓ Page 1 of 1 < ▶			

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 sousréseau 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**.

System > Network > IPs > IPV4s									
IPs							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	F	
IPV4s 3	IPV6s 1								
Add Ed	it Delete S	tatistics	ect Action 🗸						
Q Click here t	o search or you can ent	ter Key : Value format						(j)	
	IP ADDRESS	STATE 🗘	TYPE ‡	MODE \Diamond	ARP 0	ICMP ‡	VIRTUAL SERVER		
Primary SNIP	192.168.1.6	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0	
Primary VIP	192.168.1.5	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0	
192.168.1.71 ENABLED NetScaler IP Active ENABLED ENABLED -N/A- 0									
Total 3							25 Per Page V Page 1 of 1		
								•	

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 sousréseau VPC de l'instance de machine virtuelle secondaire.

c) Cliquez sur **Créer**.

b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.

System > Network > IPs > IPV4s										
IPs										
IPV4s (3) IPV6s (1)										
Add Edit Delete Statistics										
\boldsymbol{Q} Click here to search or you can enter Key : Value format						(i)				
IP ADDRESS 🗘 STATE 🗘	TYPE \Diamond	MODE \$	ARP 🗘	ICMP \$	VIRTUAL SERVER	ÎN ÷				
Secondary SNIP 192.168.1.7 ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0				
□ 192.168.1.76 ●ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0				
Primary VIP 192.168.1.5 ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED	0				
Total 3					25 Per Page ∨ Page 1 of 1					

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**.
 - Load Balancing Virtual Server

Basic Settings	
Create a virtual server by specifying IP address. If the application is acces You can configure multiple virtual ser	a name, an IP address, a port, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address is a publi sible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. rvers to receive client requests, thereby increasing the availability of resources to process client requests.
Name*	
lb-vserver1	\odot
Protocol*	
HTTP	\checkmark
IP Address Type*	
IP Address	\checkmark
IP Address*	
192.168.1.5	\odot
Port*	
80	
More	
OK Cancel	

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.

1 add ha node 1 <sec_ip> -inc ENABLED

Sur le nœud secondaire, tapez la commande suivante.

1 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 :

1 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 :

1 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.

1 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 :

```
1 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 :

1 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 :

1 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.



- Firewall 🙆
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
1
      REQUIRED_INSTANCE_IAM_PERMS = [
2
      "compute.forwardingRules.list",
3
      "compute.forwardingRules.setTarget",
      "compute.instances.setMetadata",
4
      "compute.instances.get",
5
      "compute.instances.list",
6
7
      "compute.instances.updateNetworkInterface",
8
      "compute.targetInstances.list",
9
      "compute.targetInstances.use",
      "compute.targetInstances.create",
10
11
      "compute.zones.list",
      "compute.zoneOperations.get",
13
      ]
```

 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 :

1	REQUIRED_INSTANCE_IAM_PERMS = [
2	"compute.addresses.use"
3	"compute.instances.addAccessConfig",
4	"compute.instances.deleteAccessConfig",
5	"compute.networks.useExternalIp",
6	"compute.subnetworks.useExternalIp",
7]

• Si vos machines virtuelles ne disposent pas d'un accès Internet, vous devez activer Private

	Add a subnet
	Name 🚱 Name is permanent
	management-subnet
	Add a description
	VPC Network
	automationmgmtnetwork
	Region 💿
	us-east1 👻
	Reserve for Internal HTTP(S) Load Balancing
	On Off
	IP address range 🔘
	192.168.2.0/24
	Create secondary IP range
	Private Google access 📀
	On Off
	Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Off
Google Access sur le sous-réseau de gestion.	CANCEL ADD

 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.

NetScaler VPX 14.1

÷	VM instance deta	ils	/ EDIT	心 RESET	CREATE SIM			
Creatio	on time							
Jan N	d, 2020, 4.00.22 PM							
Netwo	rk interfaces 🥡							
nic): automationmgmtnetwork	mgmtsubnet		1				
Netw	ork interface			^				
Netw autor Subn client	ork mationclientnetwork etwork tsubnet	1						
Interr 192.1	nal IP 168.2.65	-						
Interr	nal IP type							
Eph	nemeral			•				
Alias	IP ranges							
Subn	et range	Alias IP ra	inge 🔞					
Prin	mary (192.168.2.0/24)	▼ Exampl	e: 10.0.1.0/24 or /3	32 🗙				
	+	Add IP range						
≙ H	ide alias IP ranges							
Exter	nal IP 🛞							
Nor	ne			•				
Dee	Cancel							
00	Jancer							
nic2	2: automationservernetwork	serversubnet		1				
				l				
letwork i	nterfaces	Subpetwork	Primary internal ID	Alias ID ranges	External IP	Natwork Tier	ID forwarding	Network details
1491116	eutomotione ante stuerk	mamtsubnet	192.168.1.62	–	adc-ha-instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic0	automationingmtnetwork							View details
nic0 nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details

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**.

System > High Availability > Nodes											
Nodes 2											
Add	Edit	Delete Statist	ics Select	Action 🗸							
ID 0 IP ADDRESS 0 HOST NAME 0				MASTER STATE	NODE STATE	INC 0	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE RE			
	0	192.168.1.62		Primary	• UP	ENABLED	ENABLED	-NA-			
	1	192.168.1.6		Secondary	• UP	ENABLED	SUCCESS	-NA-			

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**.

System > Network > IPS > IPV4s											
IPs										a S	R.
IPV4s 3	IPV6s 1										
Add Edit	Delete	Sta	tistics	Selec	t Action V						
Q Click here to	search or you car	n ente	er Key : Value for	mat							i
	IP ADDRESS		STATE		TYPE		MODE	ARP	ICMP	VIRTUAL SERVER 0 TRAFFIC DOMAIN	
Primary VIP	192.168.2.7		ENABLED		Virtual IP		Active	ENABLED	ENABLED	ENABLED	0
	192.168.1.62		ENABLED		NetScaler IP		Active	ENABLED	ENABLED	-N/A-	0
Primary SNIP	192.168.3.8		ENABLED		Subnet IP		Active	ENABLED	ENABLED	-N/A-	0
Total 3										25 Per Page V Page 1 of 1	•

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**.

System > Network > IPs > IPV4s								
IPs								"
IPV4s 3	IPV6s 1							
Add Edit	Delete	atistics Sele	ct Action 🗸					
Q Click here to	search or you can ent	er Key : Value format						(j)
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER	n ≎
	192.168.1.6	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
Seconary SNIP	192.168.3.7	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
Primary VIP	192.168.2.7	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED	0
Total 3							25 Per Page 🗸 Page 1 of 1 <	•

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**.
 - G Load Balancing Virtual Server

Basic Settings	
Create a virtual server by specifying a name, address. If the application is accessible only i You can configure multiple virtual servers to Name*	an IP address, a port, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address is a public IP from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. receive client requests, thereby increasing the availability of resources to process client requests.
lb-vserver1	0
Protocol*	
HTTP	
IP Address Type*	
IP Address	
IP Address*	
192 . 168 . 2 . 5	0
Port*	
80	
▶ More	
OK Cancel	N

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.

1 add ha node 1 <sec_ip> -inc ENABLED

Sur le nœud secondaire, tapez la commande suivante.

1 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 :

```
1 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.

1 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 :

1

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.

```
1 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 :

```
1 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 :

```
1 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 :

1 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 sousréseaux GCP locaux ou autres (réseaux virtuels).

Google	e Cloud VMware Engine
	← Create Private Cloud ⑦
Home	Private Cloud name * Name your Private Cloud
Resources	Location *
Network Activity Account	Node type * ve1-standard-72 2x2& GHz, 3& Cores (72 HT), 768 GB RAM 19.2 TB Raw, 3.2 TB Cache (All-Flash) Multi Node
	Node count *
	3 (3 to 8) Customize Cores
	vSphere/vSAN subnets CIDR range *
	HCX Deployment Network CIDR range

3. Cliquez sur Vérifier et créer.

4. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.

Google	e Cloud VMware Engine
	← Create Private Cloud ⑦
Home	Good news! Your Priva
6	Compute Node Type Edit
Resources	ve1-standard-72
Network	Model: PCSN-ULT-1ND CPU: 2x2.6 GHz, 36 Cores (72 HT) RAM: 768 GB Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
伯比 Activity	Private Cloud Size Edit
(Q)	1 Node
Account	Total CPU: 36 Cores Total RAM: 768 GB Total Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
	Location Edit
	asia-northeast1 > v-zone-a > VE Placement Group 2
	Advanced Options Edit
	Cores per node: 36
	vSphere/vSAN subnets CIDR range: 10.231.0.0/22
	10.231.8.0/26
	Create Previous Cancel

- 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.

Googl	e Cloud VMware Engine				0 4	\$	d ⁰	8
	Resources							
6 Home	Private Clouds (1)						New Priv	ate Cloud
	u Download as CSV				Column setting	41	Selected	filters (0)
Resources	Name	Clusters	\$ Total Nodes	\$ Location		÷	State	
ل Network	vps-gene-demo	1	1	asia-northeast1 > v-zone-a > VE Placement Group	2		• Prov	isioning

- 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**.

Googl	ogle Cloud VMware Engine									
	Resources									
Home	← gcp-vmwa	re-demo								
Resources	SUMMARY	CLUSTERS	SUBNETS	ACTIVITY	VSPHERE MANAGEN					
Network Activity Account	Ba	asic Info		Name gcp-vmware-demo Clusters 1 vSphere/vSAN sub 10.231.0.0/22 vCenter login info <u>View</u> Reset passwor	nets CIDR range rd					

2. Notez les informations d'identification de vCenter.

Google Cloud VMware Engine						
	vCenter login					
Home Resources	CloudOwner@gve.local	ру				
Network	Password Cop	y .				

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.

Googl	e Cloud VMware Engine					0 4	\$ 4 8
	Resources						
Home	← gcp-vmware-demo					C LAUNCH VSPHERE CLIEN	ADD NODES
6	SUMMARY CLUSTERS SUBNETS	ACTIVITY VSPHERE	MANAGEMENT NETWORK	ADVANCED VCENTER SETTINGS DNS CONFIGURATION			
Resources	🛃 Download as CSV					-	[1], Selected filters (0)
Network	Type	Version	n	FQDN	\$	IP Address	\$
æ	vCenter Server Appliance	7.0.2.1	272235	vcsa-126870./3712fc5.asia-northeast	1.gve.goog	10.231.0.6	
Activity	NSX Manager	-		mx-127044/3712[c5.asia-northeast1	The sould	10.231.0.11	
0	HCX			http://doi.org/12/05.0010-0011000011	laveapor	10.231.0.13	
Account	ESIG	7.0.2.1	836573	essi-126865./3712fc5.asia-northeast1.	gve.goog	10.231.0.15	
	DNS Server 2	-		ns2-126869.f3712fc5.asia-northeast1.	gve.goog	10.231.0.9	
	DNS Server 1	-		ns1-126868.f3712fc5.asia-northeast1.	gve.goog	10.231.0.8	

4. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter indiquées à l'étape 2 de cette procédure.

VMv	vare [®] vSphere	
example@	20 1 main local	
Password	Tunnor	
Use Wi	indows session authentication	
	LOGIN	

5. Dans le client vSphere, vous pouvez vérifier les hôtes ESXi que vous avez créés sur le portail GCVE.

vm vSphere Client Menu v Q Sear					GoudOwner@GVELOCAL V
	/csa-126870.f3712fc5.asia	-northeast1.gve.goog			
V 🛃 vcsa-126870.f3712fc5.asia-northeast1.gve.goog	mary Monitor Configure Per	rmissions Datacenters Hosts & Clusters	Ms Datastores Networks	Linked vCenter Server Systems Extensions	Updates
ID Datacenter ID Ouster ID Ouster ID Couster rsion: 7.0.2 Build: 19272235				CPU Prec: 79.08 CHz Used: 14.31 CHz Capacity, 82.38 CHz Capacity, 82.38 CHz	
> C HCX Management C Workload	Clusters: 1 Hosts: 1 Virtual Martines: 0				Used: 150.67 GB Cepenty: 766.25
*					Used: 1.89 TB Capacity: 17.47 TB

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.

 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.

Google Cloud VMware Engine								
NSX-T login								
Home	User name admin	Сору						
Network Activity	Password	<u>Copy</u>						

3. Lancez NSX Manager en accédant à **VSPHERE MANAGEMENT NETWORK** et en cliquant sur le nom de domaine complet de **NSX Manager**.

Googl	e Cloud VMware Engine					
	Resources					
Home	← gcp-vmware-demo					₿ LAUNC
6	SUMMARY CLUSTERS	SUBNETS ACTIVITY	VSPHERE MANAGEMENT NETWORK	ADVANCED VCENTER SETTINGS DNS CONFIGURATION		
Resources	🛃 Download as CSV					
Network	Туре		Version	FQDN	们 ♦	IP Address
æ	vCenter Server Appliance		7.0.2.19272235	vcsa-126870.f3712fc5.asia-northeast1.gve.goog		10.231.0.6
Activity	NSX Manager			nsx-127044.f3712fc5.asia-northeast1.ave.aooa		10.231.0.11
0	нсх			hcx+127045.f3712fc5.asia-northeast1.gve.goog		10.231.0.13
(음급) Arcount	ESXi		7.0.2.18836573	esxi-126865.f3712fc5.asia-northeast1.gve.goog		10.231.0.15
Account	DNS Server 2			ns2-126869.f3712fc5.asia-northeast1.gve.goog		10.231.0.9
	DNS Server 1			ns1-126868.f3712fc5.asia-northeast1.gve.goog		10.231.0.8

4. Connectez-vous à NSX Manager à l'aide des informations d'identification indiquées à l'étape 2 de cette procédure.

VMware® NSX-T™	
Username	
Password	
LOG IN	

- 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.

vm NSX-T							Q	Â	0,	*	admin
Home Netw	vorking									POLICY	MANAGER
		DHCP									
Network Overvie											
関 Network Topolo											iore 👘 📼
Connectivity			Profile Name		Profile Type	Server IP Address	Lease Time (seconds)		w	here Used	
Tier-0 Gateways			management-client-dhq			10.220.1254/24 X Enter IP Addresses	86400				
Tier-1 Gateways											
Segments											
			Edge Cluster *	edge-cluster		Edges					
Network Services				💿 Tag							
Ø VPN											
😨 EVPN Tenant											
- NAT											

14. Répétez les étapes 6 à 13 pour la plage DHCP du serveur.

vm NSX-T					🗘 🗇 🔆 admin
Home Networking Security Inventory					POLICY MANAGER
K DHCP					
Network Overview					
Network Topology ADD CHC# PRO					
Connectivity	Profile Name	Profile Type	Server IP Address	Lease Time (seconds)	Where Used
Tier-0 Gateways	server-dhcp	DHCP Server V	10.230.2.254/24 × Enter IP Addresses	86400	
Tier-1 Gateways			CIDP w.m. IPv4 10 22 12 2/23 or IPv6 1r7w1306 rhv32-1/48		
Segments					
	Edge-Cluster edge-cluster		Edges		
Network services	Tags 💿 Tag				
@ VPN	Max 30 allowed. (
EVPN Tenant	SAVE CANCEL				
B NAT					

- 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.

vm NSX-T					
Home Networking	Security		Inven	ntory	Plan & Troubles
	« s	egr	mer	nts	
🙆 Network Overview	s	egm	ents	Se	gment Profiles
🔞 Network Topology		ADD	SEGM		
Connectivity				r 	Segment Name
🍈 Tier-O Gateways					Segment Name
🕕 Tier-1 Gateways				(d)	Tier-0-Uplink-1-A
Segments				বি	Tier-0-Uplink-1-B

- 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 ,	Superposition.**
sélectionnez **TZ-OVERLAY	

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.

Segments	Flae Matadata Droviae			
ADD SEGMENT				
Segment Name	Connected Gateway	Transport Zone	Subnets	Ports
management-client-segme *	Tieri Tieri 🛛 👻 *	TZ-OVERLAY ~	10.230.1.1/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. 1c7e1206:db42:1/48 SET DYCC CONFIG	

22. Cliquez sur Définir la configuration DHCPet entrez des valeurs pour le champ Plages DHCP.

tagment Intragement-client-segment PV4 Gateway 10:230.1/24 PV4 Gateway 10:230.1/24 PV4 Gateway 10:230.1/24 PV4 Server IPv6 Server PV4 Server IPv6 Server Settings Options PV4 Profile management-client-dncp PV6 Gateway PV6 Server PV6 Profile management-client-dncp PV6 Server Deft Deft Server PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges PV6 Ranges <th>Set DHCP (</th> <th>Config</th> <th></th> <th></th> <th></th>	Set DHCP (Config			
PV4 Gateway 10.230.11/2 PV4 Gateway Not Set PV4 Gateway Not Set PV4 Gateway Not Set PV4 Gateway Not Set PV4 Gateway PV4 Gateway PV4 Gateway PV4 Gateway Pute Parages Pute Parages Pute Parages <td>Segment mana</td> <td>agement-client-segment</td> <td></td> <td></td> <td></td>	Segment mana	agement-client-segment			
bHCP Type* Local DHCP Server IPV4 Server IPvd Server Settings Options DHCP Config Imagement-clent-dhcp DHCP Ranges Datastatatatatatatatatatatatatatatatatat	IPV4 Gateway	10.230.1.1/24 #DHCP Ranges	IPV6 Gateway	Not Set #DHCP Ranges 0	
IPv4 Server IPv6 Server Options Impact Server Impac	DHCP Type *	Local DHCP Server	DHCP Profile *	management-client-dhcp	
Settings Options DHCP Config	IPv4 Server				
DHCP Config Image: Enabled DHCP Server D230.1254/24 CUDR e.g. 10.22.12.2/23 DHCP Ranges 19 Maximum Format 172.16.14.10.172.16.14.00/24 Please verify that IP addresses in this range are not in use prior to modifying the DHCP Enter DHCP Ranges Default value is 86400 seconds) DNS Servers Enter IP Addresses e.g. 10.10.10.10 Enter IP Addresses e.g. 10.10.10.10 Image: Im		ptions			
DHCP Server Address* 102301254/24 CDR e.g. 10.2212.2/23 DHCP Ranges 99 Maximum Format 172.16.14.10-172.16.14.00 or 172.16.14.0/24 Please verify that IP addresses in this range are not in use prior to modifying the DHCP range to avoid duplicate IP address allocation (2303.10-10230.1100 ×) Enter DHCP Ranges	DHCP Config	C Enabled ()			
Address CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.12.2/23 CIDR e.g. 10.22.112.0 CIDR e.g. 10.22.12.2/23	DHCP Server	10.230.1.254/24			
DHCP Ranges 99 Maximum Format 172 16.14.100 or 172.16.14.00/24 Please verify that IP addresses in this range are not in use prior to modifying the DHCP Image: to avoid duplicate IP address allocation Image: to avoid duplicate IP addresses Enter DHCP Ranges Default value is 86400 Seconds) Image: to avoid duplicate IP addresses DNS Servers Image: the image: to avoid duplicate IP addresses e.g. 10.10.1010 Image: to avoid duplicate IP addresses e.g. 10.10.1010 Image: to avoid duplicate IP addresses Image: to avoid duplicate IP addresses Image: to avoid duplicate IP addresses	Address *	CIDR e.g. 10.22.12.2/23			
O 2301100 X Enter DHCP Ranges Lease Time seconds) Default value is 86400 Seconds) Enter IIP Addresses e.g. 10.10.10.10	DHCP Ranges	99 Maximum Format 172.16.14.10-172.16.1 range to avoid duplicate IP address alloca	4.100 or 172.16.14.0/24 Please verify t Ition		
Lease Time Default value is 86400 ONS Servers Enter IP Addresses e.g. 10.10.10.10	10.230.1.10-10.230. Enter DHCP Rang	1.100 ×) ges			
DNS Servers Enter IP Addresses	Lease Time (seconds)	Default value is 86400			
e.g. 10.10.10.10	DNS Servers	Enter IP Addresses			
					R

- 23. Cliquez sur **Appliquer** pour enregistrer votre configuration DHCP.
- 24. Cliquez sur Enregistrer.

	NOTE - Before further configurations can be done, fill out mandatory fields above (*), click 'Save' below.
>	SEGMENT PROFILES
>	DHCP STATIC BINDINGS
	CANCEL



- 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**.

ual Hardware VM Options				
			ADI	NEW DEVICE
CPU	2 ~			i
Memory	2	~	GB 🗸	
Hard disk 1	20	GB ~		
SCSI controller 0	LSI Logic Parallel			
Network adapter 1	management-client-se	gment 🗸		
Status	Connect At Power C	Dn		
Port ID	372795cc-b049-47b4-b	9		
Adapter Type	VMXNET 3	~		
DirectPath I/O	Enable			
Shares	Normal ~ 50		~	
Reservation	° T	~	Mbit/s ∨	
Limit	Unlimited	~	Mbit/s ∨	
MAC Address	00:50:56:a2:2c:2f	Autor	matic ~	
New Network *	server-segment	~		
Status	Connect At Power C	n		
Adapter Type	VMXNET 3	~		
DirectPath I/O	Enable			
Shares	Normal V 50		~	
Reservation	0	~	Mbit/s ~	
Limit	Unlimited	\sim	Mbit/s ∨	
MAC Address		Autor	natic 🗸	
Video card	Specify custom setting	is ~		
VMCI device				

7. Cliquez sur **Terminer** pour commencer à installer une appliance virtuelle sur le cloud VMware.

Deploy OVF Template	Ready to comp Click Finish to start creat	blete ×
1 Select an OVF template	Name	NSVDY-ECY.121.24.38 pc 64
2 Select a name and folder	Template name	NSVPX-ESX-13.1-24.38 nc 64
3 Select a compute resource	Download size	661.4 MB
4. Review details	Size on disk	20.0 GB
	Folder	Workload VMs
5 Select storage	Resource	Workload
6 Select networks	Storage mapping	1
7 Ready to complete	All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
	Network mapping	1
	VM Network	management-client-segment
	IP allocation settings	
	IP protocol	IPV4
	IP allocation	Static - Manual
		CANCEL BACK FINISH

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.

VSphere - NSV	PX-ESX-13.0-79.6- × NSX	x +	- o				
< → C	Not secure https://192.168	0.2/ui/#?extensionId=vsphere.core.inventory.serverObjectViewsExtension&objectId=urn:vmomi:VirtualMachine:vm-53:d77ece1	5 G 😩				
vm vSobere Cl	B Actions - NEV PEX-ESCARD - 78 64_0.						
The vopinere ci	Power &	Power On chri + all + 8	TICKLEOCHE V				
	Guest OS Snapshots	Actions Actions Actions Actions					
 VC.de7510d9c7d8 SDDC-Datacen(📽 Open Remote Console	astores Networks					
 Cluster-1 esx03-r09 esx04-r02 	Gione	Court Grane (Careford 10) Court (Careford 10)	CPU USAGE O HZ MEMORY USAGE				
esx14-r15.g	Fault Tolerance	DNS Name:	ОВ				
B NSVPX-ES	VM Policies	P Addresses: Host: esx04-r02.p03.de7510d9c7d8485cb31194.eastus.avs.azure.com	STORAGE USAGE				
	Template Compatibility		40.03 08				
	Export System Logs	✓ Notes	^				
	🚱 Edit Settings	Edit Notes					
	Move to folder Rename Edit Notes	Custom Athrbutes Custom	^				
	Tags & Custom Attributes	det					
Recent Tasks Ala Task Name v	Add Permission Alarms	Details v Initiator Outrued For v Start Time v Completion Time	v Server				
machine	Remove from Inventory	ed VSPHERELOCALicloud 4 ms 05/02/2021, 4:t08 PM 05/02/2021, 4:t08 PM	vc.de7510d9c7d8485c.				
Deploy OVF template	Delete from Disk	ed VSPHERELOCAL/vprd 3 ms 05/02/2021, 4:08:26 PM 05/02/2021, 4:09:12 PM	vc.de7510d9c7d8485c.				

9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.

🖻 🔗 všghne - NSV%-ESK-13.6.79.6. x 🕐 NSV%-ESK-13.6.79.6.4, xc, 64 x x 🔳 NSX x +		-	٥	×
C 👌 Not secure https://192.168.0.2/ui/webconsole.html?vmld=vm-53&vmName=NSVPX-ESX-13.0-79.64_nc_64&serverGuid=d77ece11-4945-4ee5-bb8e-17b4	£°≊	¢	8	
NSVPX-E9X-13.0-79.64_nc_64 Enforce US Keyboard Leyout View Fulls	creen	Send Ctr	+Alt+De	alete
NetScaler has started successfully				
Start additional daeMons: May 2 16:12:54 (local0.err) ns nsconfigd: _dispatch	()			
: Invalla passwora Mau 2 16:12:54 (local@ orr) no necenfied: dispatch(): Specified parameters a	20			
nay 2 10.12.34 (locale.err) is inscinitiguuispatch(). specifieu parameters a	re			
May 2 16:12:54 (local B. err) as asconfied: dispatch(): Invalid rule.				
May 2 16:12:54 <local0.err> ns last message repeated 2 times</local0.err>				
May 2 16:12:55 <local0.err> ns nsconfigd: _dispatch(): No such resource</local0.err>				
May 2 16:12:55 <local0.err> ns nsconfigd: _dispatch(): No such policy exists</local0.err>				
monit monit daemon at 1000 awakened				
may 2 10.12.33 (100a19.077) NS last message repeated 4 times Mau 2 16:13:00 (usar crit) ns susbalthd, susid 450010 IDMI douice road fail	ho			
	eu			
May 2 16:13:00 <local0.err> ns nscollect: ns copyfile(): Not able to get info</local0.err>	0			
f file /var/log/db/default/nsdevmap.txt : No such file or directory				
May 2 16:13:01 (locald err) as asymptotic 16391; asymptotic deemon started				

10. Lors du premier démarrage, définissez l'adresse IP de gestion et la passerelle pour l'instance ADC.

```
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
After the network changes are saved, you may either login as nsroot and
use the Citrix ADC command line interface, or use a web browser to
http://10.230.1.10 to complete or change the Citrix ADC configuration.
          1. Citrix ADC's IPv4 address [10.230.1.10]
2. Netmask [255.255.255.0]
          3. Gateway IPv4 address [10.230.1.1]
4. Save and quit
Select item (1-4) [4]: 4
cat: /nsconfig/preboot_nsconfig: No such file or directory
NetScaler...
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Creating default netscaler certificate fo
r NetScaler internal communication
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Creating the RSA root key
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Creating the CSR for the root certificate
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Create the Self-Signed Certificate root c
ertificate
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Creating the RSA key
nsstart: Thu Jul 7 10:27:54 UTC 2022 : Create the CSR for server cert
```

11. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l' interface de ligne de commande :

1 ssh nsroot@<management IP address>

Exemple

1 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.

Googl	e Cloud VMware E	ngine									0	4	183	Ø	8
	Network														
ß	FIREWALL TABLES	SUBNETS	PUBLIC IPS	VPN GATEWAYS	DNS CONFIGURATI	ON PRIVATE	CONNECTION	REGIONAL SETTI	NGS						
	Regional Settings													Add	Region
Resources	🕁 Download as CSV									0	Column se	ttings	411, S	elected fi	lters (0)
Network	Region		≑ Reș	ion Status	\$	Internet Access		Pub	lic IP Service	\$	Edge Ser	vices CII	DR		4

- 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).

NetScaler VPX 14.1

÷	Add Region
	Region *
	asia-south1 •
	1 Internet Access 🛛
	Public IP Service
	Edge Services CIDR @
	10.231.0.0 / 26
	There are no Private Clouds in asia-south1. Regional Settings will be applied when a Private Cloud is created.

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**.

Googl	e Cloud VMware E	Engine						0	9	۰	Ø	۲
	Network											
B	FIREWALL TABLES	SUBNETS	PUBLIC IPS	VPN GATEWAYS	DNS CONFIGURATION	PRIVATE CONNECTION	REGIONAL SETTINGS					
6	Public IPs (0)											Allocate
Resources												

- 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**.

Google	e Cloud VMware Engine
Â	← Allocate Public IP ③
Home	Name * 🐵
6	vpx-management-public-ip
Resources	Location *
2	asia-northeast1 -
ිදු Network	Private cloud *
0	gcp-vmware-demo -
(III) Activity	Attached local address * 🐵
Activity	10.230.1.10
Account	You need to open Firewall ports to enable traffic on this IP address through the Firewall Table feature.
	Submit Cancel

- 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.

certice account	
Compute Engine def	ault service account
Allow full access t	o all Cloud APIs

• Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
1
2
      "compute.instances.get",
3
      "compute.instanceGroupManagers.get",
4
      "compute.instanceGroupManagers.list",
5
      "compute.zones.list",
6
      "logging.sinks.create",
      "logging.sinks.delete",
7
      "logging.sinks.get",
8
      "logging.sinks.list"
9
      "logging.sinks.update",
10
      "pubsub.subscriptions.consume",
11
      "pubsub.subscriptions.create",
12
      "pubsub.subscriptions.delete",
13
14
      "pubsub.subscriptions.get",
      "pubsub.topics.attachSubscription",
15
      "pubsub.topics.create",
16
      "pubsub.topics.delete",
17
      "pubsub.topics.get",
18
      "pubsub.topics.getIamPolicy",
19
20
      "pubsub.topics.setIamPolicy",
21
      ]
```

- 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.
- 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.

Create Cloud Profile

Name	
DemoCloudProfile	
Virtual Server IP Address*	
192.168.2.24	~
Load Balancing Server Protocol	
НТТР	~
Load Balancing Server Port	
80	
Auto Scale Group*	
ansible-mig-defaultuser-1585300924-:	~
Auto Scale Group Protocol	
НТТР	~
Auto Scale Group Port	
80	

Select this option to drain the connections gracefully. Else the connections will be dropped in the event of scale down.

- 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**.

Q Search in Menu		Google Cloud	Platform / Cloud Pro	ofile			
Google Cloud Platform	\sim	Cloud F	Profile 1				C 😭
🕸 Cloud Profile							
System	>	Add	Edit Delete				
AppExpert	>	Q Click here	to search or you can en	ter Key : Value format			(i)
Traffic Management	>	-	,				Ŭ
Ontimization		\checkmark	NAME	AUTO SCALE GROUP	0 LO	DAD BALANCING VIRTUAL SERVER	AUTO SCALE GROUP PROTOCOL
Optimization		\checkmark	DemoCloudProfile	ansible-mig-defaultuser-1585300924-1	_C	CP_DemoCloudProfile_192.168.2.24_LB_	HTTP
Security	>						
Authentication	>	Total 1				25 Per Page	Page 1 of 1 🔺 🕨

La page de configuration de **Create Cloud Profile** s'affiche.

Create Cloud Profile

Name	
DemoCloudProfile	
Virtual Server IP Address*	
192.168.2.24	\sim
Load Balancing Server Protocol	
HTTP	\sim
Load Balancing Server Port	
80	
Auto Scale Group*	
ansible-mig-defaultuser-1585300924-:	\sim
Auto Scale Group Protocol	
НТТР	\sim
Auto Scale Group Port	
80	

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.

Q Search in Menu		Google Cloud Platform / Cloud Profile
Google Cloud Platform	~	Cloud Profile 1 C 📢
🕸 Cloud Profile		
System	>	Add Edit Delete
AppExpert	>	Q Click here to search or you can enter Key : Value format
Traffic Management	>	
Ontimization		NAME AUTO SCALE GROUP CALLO GROUP AUTO SCALE GROUP CALLO AD BALANCING VIRTUAL SERVER AUTO SCALE GROUP PROTOCOL
Security	>	DemoCloudProfile ansible-mig-defaultuser-1585300924-1 _CP_DemoCloudProfile_192.168.2.24_LB_ HTTP
Authentication	>	Total 1 25 Per Page 🗸 Page 1 of 1 🔺 🕨

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 :

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.list",
3	"compute.addresses.get",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.instances.use",
10	"compute.subnetworks.use",
11	"compute.targetInstances.create"
12	"compute.targetInstances.get"
13	"compute.targetInstances.use",
14]

- 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 :

1 REQUIRED_IAM_PERMS = [
2 "compute.addresses.list",
3 "compute.addresses.get",
4 "compute.addresses.use",
5 "compute.forwardingRules.create",
6 "compute.forwardingRules.delete",
7 "compute.forwardingRules.get",

```
8 "compute.forwardingRules.list",
9 "compute.instances.use",
10 "compute.subnetworks.use",
11 "compute.targetInstances.create",
12 "compute.targetInstances.list",
13 "compute.targetInstances.use",
14 ]
```

• 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 :

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.get",
3	"compute.addresses.list",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.forwardingRules.setTarget",
10	"compute.instances.use",
11	"compute.instances.get",
12	"compute.instances.list",
13	"compute.instances.setMetadata",
14	"compute.subnetworks.use",
15	"compute.targetInstances.create",
16	"compute.targetInstances.list",
17	"compute.targetInstances.use",
18	"compute.zones.list",
19]

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

Select a shielded image to use shielded VM features. Turn on all settings for the most secure configuration. Turn on Secure Boot @ Turn on VTPM @ Turn on Integrity Monitoring @ Availability policies Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips Add item SSH Keys Block project-wide SSH keys when checked, project-wide SSH keys cannot access this instat You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account.com Cloud API access scopes	tures. iration. iration. in in in in in in in in in in in in in		0111
Turn on all settings for the most secure configuration. Turn on Secure Boot @ Turn on VTPM @ Availability policies Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	m not access this instance Learn more ce account ceess scopes		
Turn on Secure Boot ♥ Turn on VPM ♥ Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips ↓ Add item SSH Keys Block project-wide SSH keys when checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	n n tot access this instance Learn more ce account ceaccount.com		
Turn on Integrity Monitoring Availability policies Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips	m not access this instance Learn more ce account ceaccount.com		
Availability policies Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips {	m not access this instance Learn more ce account ceaccount.com ccess scopes		
Availability policies Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips Custom metadata vips Heys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta SSH Keys Show and edit Service account You must stop the VM instance to edit its service account At 16809692761-compute@developer.gserviceaccount.com Cloud API access scopes	m not access this instance Learn more ce account ceaccount.com		
Preemptibility Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips	m not access this instance Learn more ce account ceaccount.com		
Off (recommended) On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips Custom metadata vips Automatic restart Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata vips Custom metadata Vips Custom	m not access this instance Learn more ce account ceaccount.com		
On host maintenance Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips tAdd item SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	not access this instance Learn more ce account ceaccount.com		
Migrate VM instance (recommended) Automatic restart On (recommended) Custom metadata vips ightarrow for the start of the	m vot access this instance Learn more ce account ceaccount.com ccess scopes		
Automatic restart On (recommended) Custom metadata Vips Lance Commended Vips Lance Commended Lance Commended Lance Commended Lance Commended Lance Commended Lance Commended Commended Lance	m not access this instance Learn more ce account ceaccount.com	-	
Automatic restart On (recommended) Custom metadata vips 4	m not access this instance Learn more ce account ceaccount.com		
On (recommended) Custom metadata vips 4 Add item SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta vou have 0 SSH keys Show and edit Service account fou must stop the VM instance to edit its service account 116809692761-compute@developer.gserviceaccount.com Cloud API access scopes	m not access this instance Learn more ce account ceaccount.com		
Custom metadata vips Add item SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	m not access this instance Learn more ce account ceaccount.com ccess scopes	*	
vips {	m not access this instance Learn more ce account ceaccount.com ccess scopes		
vips {	m not access this instance Learn more ce account ceaccount.com	-	
Add item SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	m not access this instance Learn more ce account ceaccount.com	∠ ×	
SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	not access this instance Learn more ce account ceaccount.com	٦	
SSH Keys Block project-wide SSH keys When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	not access this instance Learn more ce account ceaccount.com		
Block project-wide SSH keys When checked, project-wide SSH keys cannot access this inste You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	not access this instance Learn more ce account ceaccount.com ccess scopes		
When checked, project-wide SSH keys cannot access this insta You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	not access this instance Learn more ce account ceaccount.com ccess scopes		
You have 0 SSH keys Show and edit Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	ce account ceaccount.com ccess scopes)	
Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	ce account ceaccount.com		
Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	ce account iceaccount.com		
Service account You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	ce account iceaccount.com		
You must stop the VM instance to edit its service account 416809692761-compute@developer.gserviceaccount.com Cloud API access scopes	ce account		
416809692761-compute@developer.gserviceaccount.com	ceaccount.com		
Cloud API access scopes	ccess scopes		
	ccess scopes		
You must stop the VM instance to edit its API access scopes			
Allow full access to all Cloud APIs			

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.

Q Search in Menu	Traffic Management / Load Balancing / Virtual Servers			
Google Cloud Platform >	Virtual Servers <			
System >				
AppExpert >	Add Edit Delete Enable Disable Rer	name	Statistics	Select
Traffic Management \sim	Q Click here to search or you can enter Key : Value format			
Load Balancing 🗸 🗸				
🕆 Virtual Servers	NAME \$ STAT	ITE 🗘 E	EFFECTIVE STATE	IP A
Services	gcplbdnsvserver • U	JP	• UP	0.0.0
Service Groups	lbv2 • U	JP	● UP	10.3
Monitors	v1 ● D	NWOC	DOWN	10.2
Metric Tables	Demo-vServer	DOWN	• DOWN	34.9
Servers	Total 4			

 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**.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an app address is a public IP address. If the application is accessible only from the local area network (L (ICANN non-routable) IP address.

You can configure multiple virtual servers to receive client requests, thereby increasing the avail

Demo-vServer	(i)
Protocol*	
HTTP	\sim - 1
IP Address Type*	
IP Address	\sim
IP Address*	
34 . 93 . 61 . 42	(i)
Port*	
80	

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**.

Coad Balancing Service

ervice Name*	
Demo-Service	(j)
New Server Existing Server Address*	
10 . 30 . 1 . 54	(i)
rotocol*	
HTTP	\sim
°ort*	
80	

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.

Load Bala	ncing Virtual Server Export as a Template			
Basic Setti	ngs			/
Name Protocol State IP Address Port Traffic Domain	Demo-vServer HTTP • DOWN 34,93,61.42 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- NONE IP 1 - PASSIVE ENABLED NO -	
Services ar	nd Service Groups			
No Load Ba	lancing Virtual Server Service Binding			>
No Load Ba	lancing Virtual Server ServiceGroup Binding			>

4. Sélectionnez le service configuré à l'étape 3, puis cliquez sur Lier.

Service Binding	
Service Binding	
Select Service*	
Demo-Service	> Add Edit (i
Binding Details	
Weight	
1	

5. Enregistrez la configuration.

Résoudre les problèmes d'une instance VPX sur GCP

January 15, 2025

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**.

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.

NetScaler VPX 14.1

O Search in Menu		System / System Information
Google Cloud Platform	>	System
System	\sim	System
🖄 Licenses		System Information System Sessions 1 System Network
Settings		System Upgrade Reboot Migration Statistics Call Home Citrix ADM Service Connect
Diagnostics		
High Availability	>	System Information
NTP Servers		
Reports		Citrix ADC IP Address 10.160.15.230
Profiles		Netmask 255.255.240.0
Partition Administration	>	Technical Support PIN 4051153
User Administration	>	Time Zone Coordinated Universal Time
Authentication	>	System Time Sat, 11 Jul 2020 01:56-22 UTC
Auditing	>	Last Config Changed Time Sat, 11 Jul 2020 01:53:09 UTC
SNMP	>	Last Config Saved Time Sat, 11 Jul 2020 01:53:12 UTC
AppFlow	<u> </u>	Hardware Information
Cluster	>	

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 :

- 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 :

- 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.
- 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.linuxkvm.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/impo and-synchronizing-stylebooks-from-github-repository.html), [ServiceNow](/fr-fr/citrixapplication-delivery-management-service/setting-up/integrate-itsm-adapter-citrix-admservicenow.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

January 15, 2025

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 ?

Oui, l'ajout de cœurs de processeur peut améliorer les performances de NetScaler VPX, à condition que l'instance NetScaler VPX soit sous licence pour les vCPU supplémentaires. NetScaler VPX peut prendre en charge jusqu'à 20 vCPU (pour des performances de 41 Gbit/s à 100 Gbit/s), selon la configuration et le niveau de performances. Un plus grand nombre de vCPU peut contribuer à augmenter le débit, en particulier dans les scénarios à hautes performances. Cependant, l'impact sur les performances dépend également de facteurs tels que les pilotes réseau (par exemple, PCI passthrough ou SR-IOV) et la charge de travail spécifique. Pour plus d'informations sur le nombre de vCPU pris en charge pour différents niveaux de performances VPX, consultez la fiche technique NetScaler VPX.

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 | Pour connaître la configuration requise pour le processeur de votre plate-forme VPX, reportez-vous à la section [Processeurs pris en charge pour NetScaler VPX](/fr-fr/vpx/currentrelease/supported-hypervisors-features-limitations.html#supported-processors-for-netscaler-vpx) table. |

| 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 | Utilisez une carte réseau compatible avec votre hyperviseur. Pour plus d'informations, consultez [Cartes réseau prises en charge pour NetScaler VPX](/fr-fr/vpx/current-release/supported-hypervisors-features-limitations.html#supported-nics-for-netscaler-vpx). |

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.
- 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.

Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

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 ?

De nombreux serveurs ont des fonctionnalités d'assistance à la virtualisation (telles que VT-x ou AMD-V) désactivées par défaut dans les paramètres du BIOS. Avant de conclure que vous ne pouvez pas exécuter NetScaler VPX, vérifiez la configuration du BIOS. Si la prise en charge de la virtualisation est désactivée, vous devrez peut-être l'activer dans le BIOS pour vous assurer que votre serveur peut exécuter correctement des applications virtualisées telles que NetScaler VPX.

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 ?

Un minimum de 2 Go de mémoire doit être alloué à chaque instance NetScaler VPX. L'image disque NetScaler VPX est dimensionnée à 20 Go pour répondre aux besoins de maintenance, y compris l'espace pour stocker jusqu'à 4 Go de vidages de cœur, ainsi que des fichiers journaux et de trace. 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.

Les valeurs suivantes représentent l'espace disque alloué à des répertoires spécifiques sur l'instance NetScaler VPX :

• /flash = 965M

• /var = 14G

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 « In -s » pour utiliser un lien symbolique. Modifiez égale-

ment 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.

net>scaler

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.