



NetScaler VPX 14.1

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Tabla de compatibilidad de NetScaler VPX	6
Optimice el rendimiento de NetScaler VPX en VMware ESX, Linux KVM y Citrix Hypervisors	13
Aplicación de configuraciones NetScaler VPX en el primer arranque del dispositivo NetScaler en la nube	30
Mejore el rendimiento de SSL-TPS en plataformas de nube pública	66
Configurar subprocesos múltiples simultáneos para NetScaler VPX en nubes públicas	67
Instalar una instancia de NetScaler VPX en un servidor desnudo	71
Instalar una instancia de NetScaler VPX en Citrix Hypervisor	72
Configurar instancias VPX para que usen interfaces de red de virtualización de E/S de raíz única (SR-IOV)	76
Instalación de una instancia de NetScaler VPX en VMware ESX	81
Configurar una instancia de NetScaler VPX para usar la interfaz de red VMXNET3	87
Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV	99
Configure un NetScaler VPX en el hipervisor ESX para usar Intel QAT para la aceleración de SSL en modo SR-IOV	117
Migración de NetScaler VPX de E1000 a interfaces de red SR-IOV o VMXNET3	121
Configurar una instancia de NetScaler VPX para utilizar la interfaz de red de acceso PCI	121
Aplicar configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en el hipervisor VMware ESX	126
Instalación de una instancia NetScaler VPX en la nube de VMware en AWS	135
Instale una instancia de NetScaler VPX en el servidor Microsoft Hyper-V	138
Instalar una instancia de NetScaler VPX en la plataforma Linux-KVM	143
Requisitos previos para instalar una instancia de NetScaler VPX en la plataforma Linux-KVM	144
Aprovisione la instancia NetScaler VPX mediante OpenStack	148

Aprovisione la instancia de NetScaler VPX mediante el Administrador de máquinas virtuales	158
Configurar una instancia de NetScaler VPX para usar las interfaces de red SR-IOV	173
Configure un NetScaler VPX en el hipervisor KVM para usar Intel QAT para la aceleración de SSL en modo SR-IOV	183
Configurar una instancia de NetScaler VPX para utilizar las interfaces de red de transferencia PCI	189
Aprovisionamiento de la instancia NetScaler VPX mediante el virsh programa	193
Administrar las VM invitadas de NetScaler VPX	197
Aprovisione la instancia de NetScaler VPX con SR-IOV, en OpenStack	200
Configure una instancia de NetScaler VPX en KVM para utilizar interfaces de host basadas en DPDK de OVS	206
Aplique las configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en el hipervisor KVM	217
NetScaler VPX en AWS	219
Terminología de AWS	222
Tabla de compatibilidad de AWS-VPX	224
Limitaciones y directrices de uso	228
Requisitos previos	230
Configurar las funciones de IAM de AWS en la instancia de NetScaler VPX	232
Cómo funciona una instancia de NetScaler VPX en AWS	243
Implementación de una instancia independiente NetScaler VPX en AWS	245
Caso: Instancia independiente	250
Descargar una licencia de NetScaler VPX	259
Servidores de equilibrio de carga en diferentes zonas de disponibilidad	266
Cómo funciona la alta disponibilidad en AWS	267

Implementar un par de alta disponibilidad de VPX en la misma zona de disponibilidad de AWS	269
Alta disponibilidad en diferentes zonas de disponibilidad de AWS	281
Implementación de un par de alta disponibilidad VPX con direcciones IP elásticas en distintas zonas de AWS	282
Implementar un par de alta disponibilidad VPX con direcciones IP privadas en distintas zonas de AWS	287
Implementación de una instancia NetScaler VPX en AWS Outposts	300
Proteja AWS API Gateway mediante el Web App Firewall NetScaler	304
Agregar el servicio AWS Autoscaling de back-end	308
Implemente NetScaler GSLB en AWS	313
Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV	329
Configurar una instancia de NetScaler VPX para utilizar redes mejoradas con AWS ENA	333
Actualización de una instancia NetScaler VPX en AWS	333
Solución de problemas de una instancia VPX en AWS	339
Preguntas frecuentes sobre AWS	339
Implementar una instancia de NetScaler VPX en Microsoft Azure	343
Terminología de Azure	349
Arquitectura de red para instancias NetScaler VPX en Microsoft Azure	353
Configurar una instancia independiente de NetScaler VPX	356
Configuración de varias direcciones IP para una instancia independiente NetScaler VPX	371
Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC	377
Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell	388
Implemente un par de alta disponibilidad de NetScaler en Azure con ALB en el modo flotante de IP inhabilitada	400

Implemente una zona privada de DNS de NetScaler para Azure	421
Configurar una instancia de NetScaler VPX para usar redes aceleradas de Azure	442
Configure los nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler con Azure ILB	458
Configure los nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler para aplicaciones con conexión a Internet	471
Configurar una configuración de alta disponibilidad con balanceadores de carga externos e internos de Azure simultáneamente	482
Instalación de una instancia de NetScaler VPX en Azure VMware Solution	488
Configurar una instancia independiente de NetScaler VPX en la solución Azure VMware	504
Configurar una instalación de alta disponibilidad de NetScaler VPX en la solución Azure VMware	506
Configurar el servidor de rutas de Azure con un par de alta disponibilidad de NetScaler VPX	508
Agregue el servicio de escalado automático de Azure de back-end	512
Etiquetas de Azure para la implementación de NetScaler VPX	521
Configurar GSLB en instancias de NetScaler VPX	526
Configurar GSLB en una configuración de alta disponibilidad activa-en espera	535
Implemente NetScaler GSLB en Azure	539
Configurar grupos de direcciones IP de intranet para un dispositivo NetScaler Gateway	555
Configurar varias direcciones IP para una instancia independiente de NetScaler VPX mediante comandos de PowerShell	557
Scripts de PowerShell adicionales para la implementación de Azure	565
Create a support ticket for the VPX instance on Azure	581
Preguntas frecuentes de Azure	583
Implementar una instancia de NetScaler VPX en Google Cloud Platform	583
Implementar un par de VPX de alta disponibilidad en Google Cloud Platform	599

Implementar un par de alta disponibilidad VPX con dirección IP estática externa en Google Cloud Platform	600
Implemente un único par de NIC VPX de alta disponibilidad con dirección IP privada en Google Cloud Platform	610
Implementar un par VPX de alta disponibilidad con una dirección IP privada en Google Cloud Platform	620
Instalar una instancia de NetScaler VPX en VMware Engine de Google Cloud	629
Agregar servicio de escalado automático de GCP back-end	649
Compatibilidad con escalado VIP para la instancia NetScaler VPX en GCP	654
Solución de problemas de una instancia VPX en GCP	662
Tramas gigantes en instancias NetScaler VPX	663
Automatizar la implementación y las configuraciones de NetScaler	665
Preguntas frecuentes	668

Tabla de compatibilidad de NetScaler VPX

October 17, 2024

En este documento se enumeran los diferentes hipervisores y funciones admitidos en una instancia de NetScaler VPX. El documento también describe sus pautas de uso y las limitaciones conocidas.

Instancia VPX en el hipervisor VMware ESX

| versión ESXi | Fecha de lanzamiento de ESXi (AAA/MM/DD) | Número de compilación ESXi | Versión de NetScaler VPX | Rango de rendimiento |

| _____ | _____ | _____ | _____ |
 -| _____ |

| Actualización 3 de ESXi 8.0 | 2024/06/25 | 24022510 | versiones 14.1-17.x y superiores | De 10 Mbps a 100 Gbps |

| Actualización 2b de ESXi 8.0 | 2024/03/05 | 23825572 | versiones 14.1-17.x y superiores | ^^ |

| Actualización 2 de ESXi 8.0 | 2024/02/29 | 23305546 | Compilaciones 14.1-4.x y superiores | ^^ |

| Actualización 2 de ESXi 8.0 | 2023/09/21 | 22380479 | Compilaciones 14.1-4.x y superiores | ^^ |

| Actualización 1 de ESXi 8.0 | 2023/04/18 | 21495797 | Compilaciones 14.1-4.x y superiores | ^^ |

| ESXi 8.0c | 2023/03/30 | 21493926 | Compilaciones 14.1-4.x y superiores | ^^ |

| ESXi 8.0 | 2022/10/11 | 20513097 | Compilaciones 14.1-4.x y superiores | ^^ |

| Actualización 3o de ESXi 7.0 | 2024/03/05 | 23794027 | versiones 14.1-17.x y superiores | ^^ |

| Actualización 3n de ESXi 7.0 | 04/2024/11 | 23307199 | Compilaciones 14.1-4.x y superiores | ^^ |

| Actualización 3m de ESXi 7.0 | 2023/09/28 | 22348816 | Compilaciones 14.1-4.x y superiores | ^^ |

| Actualización 3n de ESXi 7.0 | 2023/07/06 | 21930508 | 14.1-8.x y versiones superiores | ^^ |

| Actualización 3m de ESXi 7.0 | 2023/05/03 | 21686933 | Compilaciones 14.1-4.x y superiores | ^^ |

Nota:

La compatibilidad con cada parche de ESXi se valida en la versión de NetScaler VPX especificada en la tabla anterior y se aplica a todas las versiones superiores de la versión 14.1 de NetScaler VPX.

Para obtener más información sobre las directrices de uso, consulte [Directrices de uso del hipervisor VMware ESXi](#).

Instancia VPX en XenServer o Citrix Hypervisor

Versión de XenServer o Citrix Hypervisor	SysID	Rango de rendimiento
8.4, compatible a partir de la versión 14.1, compilación 17.x de NetScaler VPX	450000	De 10 Mbps a 40 Gbps
8.2, compatible a partir de la versión 13.0, compilación 64.x de NetScaler VPX		
8.0, 7.6, 7.1		

Instancia de VPX en Microsoft Hyper-V

Versión Hyper-V	SysID	Rango de rendimiento
2016, 2019	450020	De 10 Mbps a 3 Gbps

Instancia VPX en Nutanix AHV

NetScaler VPX es compatible con Nutanix AHV a través de la [asociación Citrix Ready](#). Citrix Ready es un programa de socios tecnológicos que ayuda a los proveedores de software y hardware a desarrollar e integrar sus productos con la tecnología NetScaler para el espacio de trabajo digital, las redes y el análisis.

Para obtener más información sobre un método paso a paso para implementar una instancia de NetScaler VPX en Nutanix AHV, consulte [Implementación de un NetScaler VPX en Nutanix AHV](#).

Soporte de terceros:

Si tiene algún problema con una integración específica de un tercero (Nutanix AHV) en un entorno de NetScaler, abra un incidente de soporte directamente con el socio externo (Nutanix).

Si el socio determina que el problema parece estar relacionado con NetScaler, puede ponerse en contacto con el soporte de NetScaler para obtener más ayuda. Un recurso técnico dedicado de los socios trabaja con el equipo de soporte de NetScaler hasta que se resuelva el problema.

Instancia VPX en KVM genérico

Versión KVM genérica	SysID	Rango de rendimiento
RHEL 7.6, RHEL 8.0, RHEL 9.3 Ubuntu 16.04, Ubuntu 18.04, Ubuntu 22.04	450070	De 10 Mbps a 100 Gbps

Puntos que tener en cuenta:

Tenga en cuenta los siguientes puntos al utilizar hipervisores KVM.

- La instancia VPX está calificada para las versiones de versión de Hypervisor mencionadas en la tabla 1—4, y no para las versiones de parche de una versión. Sin embargo, se espera que la instancia VPX funcione sin problemas con las versiones de parches de una versión compatible. Si no es así, registre un caso de asistencia para solucionar problemas y depurar.
- Antes de utilizar RHEL 7.6, siga los pasos siguientes en el host KVM:
 1. Modifique `/etc/default/grub` y agregue `"kvm_intel.preemption_timer=0"` a la variable `GRUB_CMDLINE_LINUX`.
 2. Vuelva a generar `grub.cfg` con el comando `"# grub2-mkconfig -o /boot/grub2/grub.cfg"`.
 3. Reinicie el equipo host.
- Antes de utilizar Ubuntu 18.04, siga los pasos siguientes en el host KVM:
 1. Modifique `/etc/default/grub` y agregue `"kvm_intel.preemption_timer=0"` a la variable `GRUB_CMDLINE_LINUX`.
 2. Vuelva a generar `grub.cfg` con el comando `"# grub-mkconfig -o /boot/grub/grub.cfg"`.
 3. Reinicie el equipo host.

Instancia VPX en nubes públicas

Nube pública	SysID	Rango de rendimiento
AWS	450040	De 10 Mbps a 30 Gbps
Azure	450020	De 10 Mbps a 10 Gbps
GCP	450070	De 10 Mbps a 10 Gbps

Funciones VPX compatibles con hipervisores

Hipervisores VPX en XenServer VPX en VMware ESX

→

^^Características

↓

^^

^^

^^

^^

Interface	Fotovoltaica	SRa	Fotovoltaica	SRa	Emulado	Paso	Fotovoltaica	Fotovoltaica	SRa	Paso
→	IOV		IOV			a través de PCI	IOV	IOV		a través de PCI
Soporte para múltiples PE	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Soporte de agrupamiento	Sí	Sí ¹	Sí	Sí ¹	Sí	Sí	Sí	Sí	Sí ¹	Sí
Etiquetado VLAN	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Detección de eventos de enlace/HA-Mon	N. ⁰²	Sí ³	N. ⁰²	Sí ³	N. ⁰²	Sí ³	N. ⁰²	N. ⁰²	Sí ³	Sí ³

^^Características

↓	^^	^^	^^	^^	^^	^^	^^	^^	^^	^^
Configuración de parámetros de la interfaz	No	No	No	No	Sí	No	No	No	Sí	
LA es-tática	Sí ²	Sí ³	Sí ²	No	Sí ²	Sí ³	Sí ²	Sí ²	Sí ³	Sí ³
LACP	No	Sí ³	Sí ²	No	Sí ²	Sí ³	No	Sí ²	Sí ³	Sí ³
CLAG es-tático	No	No	No	No	No	No	No	No	No	No
CLAG LACP	No	No	Sí ²	No	Sí ²	Sí ³	No	Sí ²	Sí ³	Sí ³
Conexión en caliente	No	No	No	No	No	No	No	No	No	No

Funciones de VPX compatibles con las nubes públicas

Nubes públicas →	VPX en AWS	VPX en Azure	VPX en GCP
------------------	------------	--------------	------------

^^Características ↓

	^^	^^	^^
Soporte para múltiples PE	Sí	Sí	Sí
Soporte de agrupamiento	No	No	No
Etiquetado VLAN	No	No	No
Detección de eventos de enlace/HAMon	N. ⁰²	N. ⁰²	N. ⁰²

^^Características ↓	^^	^^	^^
Configuración de parámetros de la interfaz	No	No	No
LA estática	No	No	No
LACP	No	No	No
CLAG estático	No	No	No
CLAG LACP	No	No	No
Conexión en caliente	Sí	No	No

Los números en superíndice (1, 2, 3) utilizados en las dos tablas anteriores se refieren a los siguientes puntos con la numeración correspondiente:

1. La compatibilidad con clústeres está disponible en SRIOV para las interfaces orientadas al cliente y al servidor, y no para el plano posterior.
2. Los eventos de interfaz DOWN no se registran en instancias de NetScaler VPX.
3. Para LA estática, es posible que aún se envíe tráfico en la interfaz cuyo estado físico sea DOWN.

Los siguientes puntos se aplican a las funciones respectivas capturadas en las dos tablas anteriores:

- Para LACP, el dispositivo del mismo nivel conoce el evento DOWN de la interfaz basado en el mecanismo de tiempo de espera de LACP.
 - Tiempo de espera corto: 3 segundos
 - Tiempo de espera prolongado: 90 segundos
- En el caso de LACP, no comparta interfaces entre máquinas virtuales.
- Para el enrutamiento dinámico, el tiempo de convergencia depende del protocolo de enrutamiento, ya que no se detectan eventos de enlace.
- La funcionalidad Ruta estática supervisada falla si no vincula monitores a rutas estáticas porque el estado de la ruta depende del estado de la VLAN. El estado de la VLAN depende del estado del vínculo.
- La detección de fallos parciales no se produce en alta disponibilidad si se produce un error de enlace. Una afección cerebral dividida de alta disponibilidad podría ocurrir si se produce un fallo de enlace.
 - Cuando se genera cualquier evento de enlace (desactivar/habilitar, restablecer) desde una instancia VPX, el estado físico del enlace no cambia. Para LA estática, cualquier tráfico iniciado por el par se elimina en la instancia.

- Para que la función de etiquetado de VLAN funcione, en VMware ESX, configure el ID de VLAN del grupo de puertos en 1–4095 en el vSwitch del servidor VMware ESX.
- La conexión en caliente no se admite en las instancias VPX con interfaces ENA, y el comportamiento de las instancias puede ser impredecible si se intenta conectarlas en caliente. La adición en caliente solo se admite en las interfaces PV y SRIOV con NetScaler en AWS.
- La eliminación en caliente a través de la consola web de AWS o la interfaz CLI de AWS no se admite con las interfaces PV, SRIOV y ENA para NetScaler. El comportamiento de las instancias puede ser impredecible si se intenta eliminar en caliente.

Exploradores web compatibles

Sistema operativo	Explorador y versiones
Windows 7	Internet Explorer: 8, 9, 10 y 11; Mozilla Firefox 3.6.25 y superior; Google Chrome: 15 y superior
Windows de 64 bits	Internet Explorer: 8, 9; Google Chrome: 15 y superior
MAC	Mozilla Firefox - 12 y superior; Safari - 5.1.3; Google Chrome: 15 y superior

Compatibilidad con procesadores AMD para instancias de VPX

A partir de la versión 13.1 de NetScaler, la instancia de VPX admite los procesadores Intel y AMD. Los dispositivos virtuales VPX se pueden implementar en cualquier tipo de instancia que tenga dos o más núcleos virtualizados y más de 2 GB de memoria. Para obtener más información sobre los requisitos del sistema, consulte la [hoja de datos de NetScaler VPX](#).

Plataforma VPX vs. Tabla de matriz NIC

La siguiente tabla muestra las NIC compatibles con una plataforma o nube VPX.

NIC →	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	VF SRIOV Intel 82599	VF SRIOV Intel X710/X722/XL710	Modo de paso a través PCI Intel X710/XL710/XXV710

^^Plataformas						
↓	^^	^^	^^	^^	^^	^^
VPX (ESXi)	No	Sí	No	Sí	No	Sí
VPX (Citrix Hypervisor)	NA	NA	NA	Sí	Sí	No
VPX (KVM)	No	Sí	Sí	Sí	Sí	No
VPX (Hyper-V)	NA	NA	NA	No	No	No
VPX (AWS)	NA	NA	NA	Sí	NA	NA
VPX (Azure)	Sí	Sí	Sí	NA	NA	NA
VPX (GCP)	NA	NA	NA	NA	NA	NA

Otras referencias

- Para obtener productos Citrix Ready, visite [Citrix Ready Marketplace](#).
- Para obtener asistencia sobre los productos Citrix Ready, consulte la [página de preguntas frecuentes](#).
- Para ver las versiones de hardware de VMware ESX, consulte [Actualización de VMware Tools](#).

Optimice el rendimiento de NetScaler VPX en VMware ESX, Linux KVM y Citrix Hypervisors

October 17, 2024

El rendimiento de NetScaler VPX varía considerablemente según el hipervisor, los recursos del sistema asignados y las configuraciones del host. Para lograr el rendimiento deseado, primero siga las recomendaciones de la hoja de datos de VPX y, a continuación, optimice aún más mediante las prácticas recomendadas que se proporcionan en este documento.

Instancia de NetScaler VPX en hipervisores VMware ESX

Esta sección contiene detalles sobre las opciones y ajustes configurables y otras sugerencias que le ayudarán a lograr un rendimiento óptimo de la instancia de NetScaler VPX en los hipervisores VMware ESX.

- [Configuración recomendada en hosts ESX](#)
- [NetScaler VPX con interfaces de red E1000](#)
- [NetScaler VPX con interfaces de red VMXNET3](#)
- [NetScaler VPX con interfaces de red de transferencia SR-IOV y PCI](#)

Configuración recomendada en hosts ESX

Para lograr un alto rendimiento para VPX con interfaces de red de paso E1000, VMXNET3, SR-IOV y PCI, siga estas recomendaciones:

- El número total de CPU virtuales (vCPU) aprovisionadas en el host ESX debe ser inferior o igual al número total de CPU físicas (PCPU) del host ESX.
- La afinidad de acceso a memoria no uniforme (NUMA) y la afinidad de CPU deben configurarse para que el host ESX obtenga buenos resultados.

—Para encontrar la afinidad NUMA de un Vmnic, inicie sesión en el host de forma local o remota y escriba:

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

- Para establecer la afinidad de NUMA y vCPU para una VM, consulte la [documentación de VMware](#).

NetScaler VPX con interfaces de red E1000

Realice la siguiente configuración en el host de VMware ESX:

- En el host VMware ESX, cree dos vNIC a partir de un conmutador vNIC. Varias vNIC crean varios subprocesos de recepción (Rx) en el host ESX. Esto aumenta el rendimiento de Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de transmisión de vNIC (Tx), utilice un subproceso Tx independiente en el host ESX por vNIC. Utilice los siguientes comandos de ESX:
 - Para la versión 5.5 de ESX:

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

- Para la versión 6.0 de ESX en adelante:

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

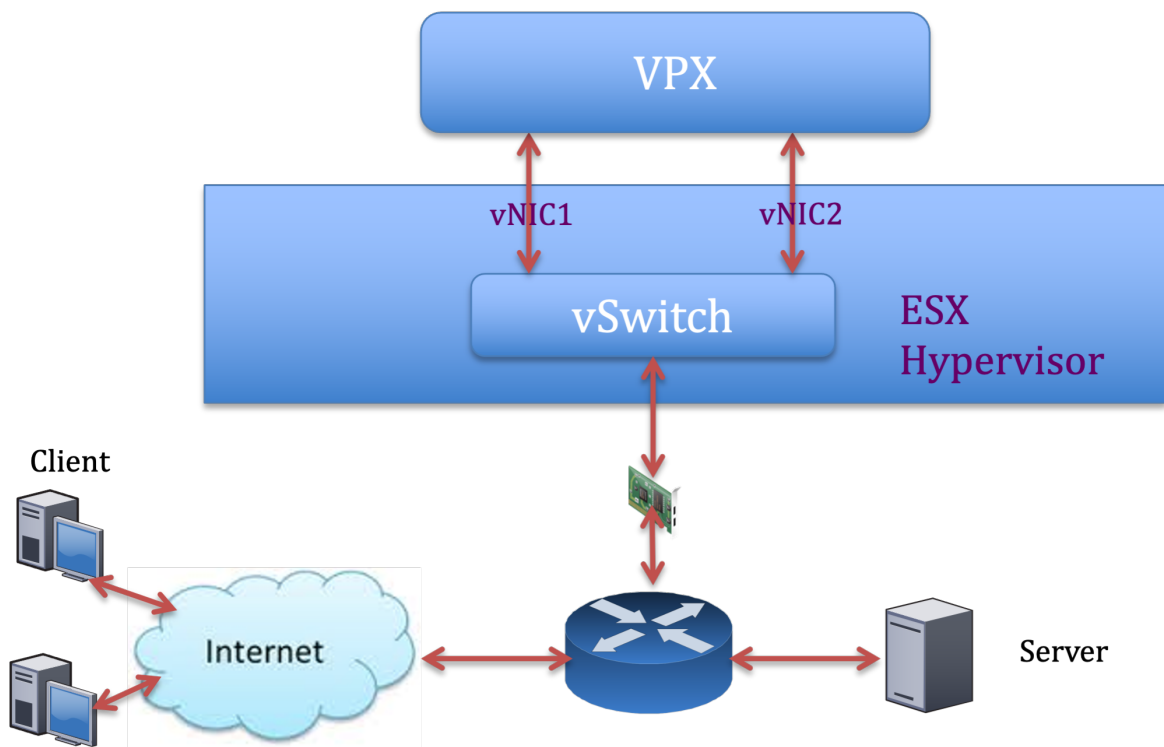
- Para aumentar aún más el rendimiento de vNIC Tx, utilice un subproceso de finalización Tx y una cola de subprocesos Rx por dispositivo (NIC) independientes. Utilice los siguientes comandos de ESX:

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

Nota:
Asegúrese de reiniciar el host de VMware ESX para aplicar la configuración actualizada.

Dos vNIC por implementación de pNIC

A continuación se muestra un ejemplo de comandos de topología y configuración para el modelo de implementación **Dos vNIC por pNIC** que ofrece un mejor rendimiento de la red.



Ejemplo de configuración de NetScaler VPX:

Para lograr la implementación que se muestra en la topología de ejemplo anterior, realice la siguiente configuración en la instancia de NetScaler VPX:

- En el lado del cliente, vincule el SNIP (1.1.1.2) a la interfaz de red 1/1 y habilite el modo de etiqueta VLAN.

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

- En el lado del servidor, vincule el SNIP (2.2.2.2) a la interfaz de red 1/1 y habilite el modo de etiqueta VLAN.

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

- Agregar un servidor virtual HTTP (1.1.1.100) y vincularlo a un servicio (2.2.2.100).

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

Nota:

Asegúrese de incluir las dos entradas siguientes en la tabla de rutas:

- subred 1.1.1.0/24 con puerta de enlace apuntando a SNIP 1.1.1.2
- Subred 2.2.2.0/24 con puerta de enlace que apunta a SNIP 2.2.2.2

NetScaler VPX con interfaces de red VMXNET3

Para lograr un alto rendimiento para VPX con interfaces de red VMXNET3, realice la siguiente configuración en el host VMware ESX:

- Cree dos vNIC a partir de un vSwitch pNIC. Varias vNIC crean varios subprocesos Rx en el host ESX. Esto aumenta el rendimiento de Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de transmisión de vNIC (Tx), utilice un subproceso Tx independiente en el host ESX por vNIC. Utilice el siguiente comando de ESX:

- Para la versión 5.5 de ESX:

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

- Para la versión 6.0 de ESX en adelante:

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

En el host de VMware ESX, realice la siguiente configuración:

- En el host VMware ESX, cree dos vNIC a partir de 1 vSwitch pNIC. Varias vNIC crean varios subprocesos Tx y Rx en el host ESX. Esto aumenta el rendimiento Tx y Rx de la interfaz pNIC.
- Habilite las VLAN en el nivel de grupo de puertos de vSwitch para cada vNIC que haya creado.
- Para aumentar el rendimiento de Tx de una vNIC, utilice un subproceso de finalización Tx y una cola de subprocesos Rx por dispositivo (NIC) independientes. Utilice el siguiente comando:

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

- Configure una máquina virtual para que use un subproceso de transmisión por vNIC, agregando la siguiente configuración a la configuración de la máquina virtual:

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

- Para configurar una máquina virtual para que utilice hasta 8 subprocesos de transmisión por vNIC, agregue la siguiente configuración a la configuración de la máquina virtual:

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

Nota:

El aumento de los subprocesos de transmisión por vNIC requiere más recursos de CPU (hasta 8) en el host ESX. Asegúrese de que haya suficientes recursos de CPU disponibles antes de realizar la configuración anterior.

Nota:

Asegúrese de reiniciar el host de VMware ESX para aplicar la configuración actualizada.

Puede configurar VMXNET3 como **dos vNIC por implementación de pNIC**. Para obtener más información, consulte [Dos vNIC por implementación de pNIC](#).

Configure la compatibilidad con múltiples colas y RSS en VMware ESX para dispositivos VMXNET3 De forma predeterminada, el dispositivo VMXNET3 solo admite 8 colas Rx y Tx. Cuando el número de vCPU en el VPX supera los 8, el número de colas Rx y Tx configuradas para una interfaz VMXNET3 cambia a 1 de forma predeterminada. Puede configurar hasta 19 colas Rx y Tx para dispositivos VMXNET3 cambiando determinadas configuraciones en ESX. Esta opción aumenta el rendimiento y la distribución uniforme de los paquetes entre las CPU virtuales de la instancia VPX.

Nota:

A partir de la versión 13.1, compilación 48.x de NetScaler, NetScaler VPX admite hasta 19 colas Rx y Tx en dispositivos ESX para VMXNET3.

Requisitos previos:

Para configurar hasta 19 colas Rx y Tx en ESX para dispositivos VMXNET3, asegúrese de que se cumplen los siguientes requisitos previos:

- La versión de NetScaler VPX es 13.1, compilación 48.X y posterior.
- NetScaler VPX se configura con una máquina virtual de hardware de versión 17 o posterior, que es compatible con VMware ESX 7.0 y versiones posteriores.

Configure las interfaces VMXNET3 para que admitan más de 8 colas Rx y Tx:

1. Abra el archivo de configuración de la máquina virtual (.vmx).
2. Especifique el número de colas Rx y TX configurando `ethernetX.maxRxQueues` los valores `ethernetX.maxTxQueues` y (donde X es el número de NIC virtuales que se van a configurar). La cantidad máxima de colas configuradas no debe ser superior a la cantidad de CPU virtuales de la máquina virtual.

Nota:

El aumento del número de colas también aumenta la sobrecarga del procesador en el host ESX. Por lo tanto, asegúrese de que haya suficientes recursos de CPU disponibles en el host ESX antes de aumentar las colas. Puede aumentar el número máximo de colas admitidas en situaciones en las que el número de colas se identifique como un obstáculo para el rendimiento. En estas situaciones, recomendamos aumentar el número de colas de forma gradual. Por ejemplo, de 8 a 12, luego a 16, luego a 20, y así sucesivamente. Evalúe el rendimiento en cada configuración, en lugar de aumentarlo directamente hasta el límite máximo.

NetScaler VPX con interfaces de red de transferencia SR-IOV y PCI

Para lograr un alto rendimiento para NetScaler VPX con interfaces de red de paso PCI y SR-IOV, consulte [Configuración recomendada en hosts ESX](#).

Pautas de uso del hipervisor VMware ESXi

- Le recomendamos que implemente una instancia de NetScaler VPX en los discos locales del servidor o en volúmenes de almacenamiento basados en SAN.

Consulte la sección **Consideraciones sobre la CPU de VMware ESXi** en el documento [Mejores prácticas de rendimiento para VMware vSphere 6.5](#). Aquí hay un extracto:

- No se recomienda implementar máquinas virtuales con una alta demanda de CPU o memoria en un host o clúster sobrecomprometidos.
- En la mayoría de los entornos, ESXi permite niveles significativos de compromiso excesivo de CPU sin afectar el rendimiento de la máquina virtual. En un host, puede ejecutar más CPU virtuales que el número total de núcleos de procesador físicos de ese host.
- Si un host ESXi se satura de la CPU, es decir, las máquinas virtuales y otras cargas del host exigen todos los recursos de CPU que tiene el host, las cargas de trabajo sensibles a la latencia podrían no funcionar bien. En este caso, reduzca la carga de la CPU, por ejemplo, apagando algunas máquinas virtuales o migrándolas a un host diferente (o permitiendo que DRS las migre automáticamente).
- NetScaler recomienda usar la versión más reciente de compatibilidad de hardware para aprovechar los conjuntos de funciones más recientes del hipervisor ESXi para la máquina virtual. Para obtener más información sobre la compatibilidad del hardware y la versión de ESXi, consulte la [documentación de VMware](#).
- El NetScaler VPX es un dispositivo virtual de alto rendimiento y sensible a la latencia. Para ofrecer el rendimiento esperado, el dispositivo requiere reserva de CPU virtuales, reserva de memoria y fijación de vCPU en el host. Además, el hipersubproceso debe estar inhabilitado en el host. Si el host no cumple con estos requisitos, pueden producirse los siguientes problemas:
 - Conmutación por error de alta disponibilidad
 - Pico de CPU en la instancia VPX
 - Lentitud en el acceso a la CLI de VPX
 - Fallo del demonio de Pit boss
 - Descarte de paquetes
 - Bajo rendimiento
- Un Hypervisor se considera sobreaprovisionado si se cumple una de las dos condiciones siguientes:
 - El número total de núcleos virtuales (CPU virtuales) aprovisionados en el host es mayor que el número total de núcleos físicos (CPU físicas).
 - El número total de máquinas virtuales aprovisionadas consume más CPU virtuales que el número total de CPU físicas.

Si una instancia está sobreaprovisionada, es posible que el hipervisor no garantice los recursos reservados (como CPU, memoria y otros) para la instancia debido a los gastos generales de programación del hipervisor, errores o limitaciones con el hipervisor. Este comportamiento puede provocar la falta de recursos de CPU para NetScaler y provocar los

problemas mencionados en el primer punto de las **Directrices de uso**. Recomendamos que los administradores reduzcan la tenencia del host para que la cantidad total de vCPU aprovisionadas en el host sea inferior o igual a la cantidad total de CPU.

Ejemplo

En el hipervisor ESX, si el parámetro %RDY% de una vCPU VPX es superior a 0 en el resultado del comando `esx top`, se dice que el host ESX tiene gastos generales de programación, lo que puede provocar problemas relacionados con la latencia en la instancia VPX.

En tal situación, reduzca la tenencia en el host para que %RDY% siempre vuelva a 0. Como alternativa, contacte con el proveedor del hipervisor para seleccionar el motivo por el que no se ha respetado la reserva de recursos realizada.

Comandos para controlar el uso de la CPU del motor de paquetes

Puede utilizar dos comandos (`set ns vpxparam` y `show ns vpxparam`) para controlar el comportamiento de uso de CPU del motor de paquetes (no administrativo) de las instancias VPX en entornos de hipervisor y nube:

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

Permita que cada máquina virtual utilice los recursos de CPU asignados a otra máquina virtual, pero que no se estén utilizando.

Set `ns vpxparam` parámetros:

-cpuyield: Libere o no libere recursos de CPU asignados pero no utilizados.

- **SÍ:** Permitir que otra máquina virtual utilice recursos de CPU asignados pero no utilizados.
- **NO:** reserve todos los recursos de CPU para la máquina virtual a la que se han asignado. Esta opción muestra un porcentaje más alto en entornos de hipervisor y nube para el uso de la CPU VPX.
- **PREDETERMINADO:** No.

Nota:

En todas las plataformas NetScaler VPX, el uso de CPU virtuales en el sistema host es del 100 por ciento. Use el comando `set ns vpxparam -cpuyield YES` para supeditar este uso.

Si quiere configurar los nodos de clúster en “yield”, debe realizar las siguientes configuraciones adicionales en CCO:

- Si se forma un clúster, todos los nodos se configuran con “yield=DEFAULT”.
- Si se forma un clúster mediante los nodos que ya están configurados en “Yield=yes”, los nodos se agregan al clúster mediante el rendimiento “DEFAULT”.

Nota:

Si quiere establecer los nodos del clúster en “Yield=Sí”, puede configurarlos solo después de formar el clúster, pero no antes de que se forme el clúster.

-masterclockcpu1: Puede mover la fuente de reloj principal de la CPU0 (CPU de administración) a la CPU1. Este parámetro tiene las siguientes opciones:

- **SÍ:** Permita que la VM mueva la fuente de reloj principal de la CPU0 a la CPU1.
- **NO:** La máquina virtual utiliza CPU0 para la fuente de reloj principal. De forma predeterminada, CPU0 es la principal fuente de reloj.

- `show ns vpxparam`

Este comando muestra los parámetros de `vpxparam` actuales.

Instancia NetScaler VPX en la plataforma Linux-KVM

Esta sección contiene detalles sobre las opciones y los ajustes configurables, así como otras sugerencias que le ayudarán a lograr un rendimiento óptimo de la instancia NetScaler VPX en la plataforma Linux-KVM.

- [Configuración de rendimiento para KVM](#)
- [NetScaler VPX con interfaces de red fotovoltaica](#)
- [NetScaler VPX con interfaces de red de transferencia SR-IOV y Fortville PCIe](#)

Configuración de rendimiento para KVM

Realice los siguientes ajustes en el host KVM:

Busque el dominio NUMA de la NIC mediante el comando `lstopo`:

Asegúrese de que la memoria del VPX y de la CPU esté fijada en la misma ubicación. En el siguiente resultado, la NIC 10G “ens2” está vinculada al dominio NUMA #1.

```
[root@localhost ~]# lstopo-no-graphics
Machine (128GB)
  NUMANode L#0 (P#0 64GB)
    Socket L#0 + L3 L#0 (20MB)
      L2 L#0 (256KB) + L1d L#0 (32KB) + L1i L#0 (32KB) + Core L#0 + PU L#0 (P#0)
      L2 L#1 (256KB) + L1d L#1 (32KB) + L1i L#1 (32KB) + Core L#1 + PU L#1 (P#1)
      L2 L#2 (256KB) + L1d L#2 (32KB) + L1i L#2 (32KB) + Core L#2 + PU L#2 (P#2)
      L2 L#3 (256KB) + L1d L#3 (32KB) + L1i L#3 (32KB) + Core L#3 + PU L#3 (P#3)
      L2 L#4 (256KB) + L1d L#4 (32KB) + L1i L#4 (32KB) + Core L#4 + PU L#4 (P#4)
      L2 L#5 (256KB) + L1d L#5 (32KB) + L1i L#5 (32KB) + Core L#5 + PU L#5 (P#5)
      L2 L#6 (256KB) + L1d L#6 (32KB) + L1i L#6 (32KB) + Core L#6 + PU L#6 (P#6)
      L2 L#7 (256KB) + L1d L#7 (32KB) + L1i L#7 (32KB) + Core L#7 + PU L#7 (P#7)
    HostBridge L#0
      PCI 8086:1521
        Net L#0 "eno1"
      PCI 8086:1521
        Net L#1 "eno2"
      PCI 8086:1584
        Net L#2 "ens3"
      PCI 8086:1584
        Net L#3 "ens4"
      PCI 8086:8d52
        Block L#4 "sda"
        Block L#5 "sdb"
      PCI 8086:2000
        GPU L#6 "card0"
        GPU L#7 "control064"
      PCI 8086:8d82
      NUMANode L#1 (P#1 64GB)
        Socket L#1 + L3 L#1 (20MB)
          L2 L#8 (256KB) + L1d L#8 (32KB) + L1i L#8 (32KB) + Core L#8 + PU L#8 (P#8)
          L2 L#9 (256KB) + L1d L#9 (32KB) + L1i L#9 (32KB) + Core L#9 + PU L#9 (P#9)
          L2 L#10 (256KB) + L1d L#10 (32KB) + L1i L#10 (32KB) + Core L#10 + PU L#10 (P#10)
          L2 L#11 (256KB) + L1d L#11 (32KB) + L1i L#11 (32KB) + Core L#11 + PU L#11 (P#11)
          L2 L#12 (256KB) + L1d L#12 (32KB) + L1i L#12 (32KB) + Core L#12 + PU L#12 (P#12)
          L2 L#13 (256KB) + L1d L#13 (32KB) + L1i L#13 (32KB) + Core L#13 + PU L#13 (P#13)
          L2 L#14 (256KB) + L1d L#14 (32KB) + L1i L#14 (32KB) + Core L#14 + PU L#14 (P#14)
          L2 L#15 (256KB) + L1d L#15 (32KB) + L1i L#15 (32KB) + Core L#15 + PU L#15 (P#15)
        HostBridge L#6
          PCI 8086:1584
            Net L#8 "ens2"
          PCI 8086:10fb
            Net L#9 "ens1f0"
          PCI 8086:10fb
            Net L#10 "ens1f1"
          PCI ffff:ffff
            Net L#11 "enp131s16"
    [root@localhost ~]# modprobe kvm-intel acpienv=N
```

Asigne la memoria VPX del dominio NUMA.

El comando `numactl` indica el dominio NUMA desde el que se asigna la memoria. En el siguiente resultado, se asignan unos 10 GB de RAM desde el nodo NUMA #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 ~]#
```

Para cambiar la asignación de nodos NUMA, sigue estos pasos.

1. Modifique el archivo.xml del VPX en el host.

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

2. Agrega la siguiente etiqueta:

```

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

```

3. Apaga el VPX.
4. Ejecute este comando:

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

Este comando actualiza la información de configuración de la máquina virtual con las asignaciones de nodos NUMA.

5. Enciende el VPX. A continuación, compruebe el resultado del comando `numactl --hardware` en el host para ver las asignaciones de memoria actualizadas para el VPX.

```

[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: 65429 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 55854 MB
node distances:
node 0 1
  0: 10 21
  1: 21 10
[root@localhost ~]#

```

Anclar vCPU de VPX a núcleos físicos.

- Para ver las asignaciones de vCPU a PCPU de un VPX, escriba el siguiente comando

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

```

root@localhost qemu]# virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
-----
0: 8
1: 9
2: 10
3: 11

```

Las vCPU 0—4 se asignan a los núcleos físicos 8—11.

- Para ver el uso actual de la PCPU, escriba el siguiente comando:

```
1 mpstat -P ALL 5
```



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

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

En este resultado, 8 es CPU de administración y 9-11 son motores de paquetes.

- Para cambiar la fijación de vCPU a pCPU, hay dos opciones.
 - Cámbielo en tiempo de ejecución después de que se inicie el VPX con el siguiente comando:

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

- Para realizar cambios estáticos en el VPX, modifique el archivo `.xml` como antes con las siguientes etiquetas:

1. Modificar el archivo.xml del VPX en el host

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

2. Agrega la siguiente etiqueta:

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

3. Apaga el VPX.
4. Actualice la información de configuración de la máquina virtual con las asignaciones de nodos NUMA mediante el siguiente comando:

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

5. Enciende el VPX. A continuación, compruebe el resultado del comando `virsh vcpupin <VPX name>` en el host para ver la fijación actualizada de la CPU.

Elimine la sobrecarga de interrupción del host.

- Detecte VM_EXITS mediante el comando `kvm_stat`.

En el nivel del hipervisor, las interrupciones del host se asignan a las mismas PCPU en las que están fijadas las vCPU de la VPX. Esto podría provocar que las vCPU de la VPX se expulsaran periódicamente.

Para encontrar las salidas de VM realizadas por las máquinas virtuales que ejecutan el host, use el comando `kvm_stat`.

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

Un valor más alto del orden 1+M indica un problema.

Si hay una sola VM presente, el valor esperado es 30–100 K. Cualquier cosa más que eso puede indicar que hay uno o más vectores de interrupción del host asignados al mismo pCPU.

- Detecte las interrupciones del host y migre las interrupciones del host.

Al ejecutar el comando `concatenate` del archivo “/proc/interrupts”, muestra todas las asignaciones de interrupción del host. Si una o más IRQ activas se asignan a la misma PCPU, su contador correspondiente aumenta.

Transfiera cualquier interrupción que se superponga con las PCPUs de NetScaler VPX a las PCPUs no utilizadas:

```
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
```

- Desactiva el saldo de IRQ.

Inhabilite el demonio de equilibrio de IRQ para que no se produzca ninguna reprogramación sobre la marcha.

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

Asegúrese de ejecutar el comando `kvm_stat` para asegurarse de que no haya muchos contadores.

NetScaler VPX con interfaces de red fotovoltaica

Puede configurar las interfaces de red de paso de para-virtualización (PV), SR-IOV y PCIe como **dos vNIC por implementación de PNIC** . Para obtener más información, consulte [Dos vNIC por implementación de PNIC](#).

Para obtener un rendimiento óptimo de las interfaces fotovoltaicas (virtio), siga estos pasos:

- Identifique el dominio NUMA al que pertenece la ranura PCIe/NIC.
- La memoria y la vCPU del VPX deben estar ancladas en el mismo dominio NUMA.
- El subproceso vhost debe estar enlazado a las CPU del mismo dominio NUMA.

Enlazar los subprocesos del host virtual a las CPU correspondientes:

1. Una vez iniciado el tráfico, ejecute el comando `top` en el host.

```

top - 14:48:08 up 6 days, 17 min, 4 users, load average: 1.46, 0.42, 0.65
taskrt 486 total, 3 running, 483 sleeping, 0 stopped, 0 zombie
%cpu(n): 4.1 us, 5.1 sy, 0.0 ni, 89.2 id, 0.0 wa, 0.0 hi, 1.7 si, 0.0 st
KiB Mem: 13175540+total, 6496624 used, 12525878+free, 884 buffers
KiB Swap: 4194300 total, 0 used, 4194300 free. 2088468 cached Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
 29824 qemu     20   0 12.786g 742864 8040 S 139.2 0.6 8789.04 qemu-kvm
 29838 root      20   0 0         0       0 R 100.0 0.0 5659.06 vhost-29824
 29837 root      20   0 0         0       0 R 99.7 0.0 5659.25 vhost-29824
 3063  root     20   0 1073944 23992 9396 S 1.7 0.0 111:58.18 libvirtd
 1070  root     39  19 0         0       0 S 1.0 0.0 91:35.98 kpmio
 27439 test     20   0 2710032 1.159g 25868 S 0.7 0.9 45:35.56 virt-manager
 16500 root     20   0 0         0       0 S 0.3 0.0 0:16.96 kworker/25:0
 1  root    20   0 53704    7724 2536 S 0.0 0.0 0:13.69 systemd
 2  root    20   0 0         0       0 S 0.0 0.0 0:00.22 kthreadd
 3  root    20   0 0         0       0 S 0.0 0.0 384:17.42 ksoftirqd/0
 5  root    0 -20 0         0       0 S 0.0 0.0 0:00.00 kworker/0:0H
 6  root    20   0 0         0       0 S 0.0 0.0 0:00.00 kworker/u64:0
 8  root    rt   0 0         0       0 S 0.0 0.0 0:03.02 migration/0
 9  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcu_bh
10  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/0
11  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/1
12  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/2
13  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/3
14  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/4
15  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/5
16  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/6
17  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/7
18  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/8
19  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/9
20  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/10
21  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/11
22  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/12
23  root    20   0 0         0       0 S 0.0 0.0 0:00.00 rcuob/13
    
```

2. Identificar el proceso de host virtual (denominado como `vhost-<pid-of-qemu>`;) afinidad.
3. Enlace los procesos vHost a los núcleos físicos del dominio NUMA identificado anteriormente mediante el siguiente comando:

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

Ejemplo

```
1 taskset -pc 12 29838
```

4. Los núcleos del procesador correspondientes al dominio NUMA se pueden identificar con el siguiente comando:

```

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

```

Enlazar el proceso QEMU al núcleo físico correspondiente:

1. Identificar los núcleos físicos en los que se ejecuta el proceso QEMU. Para obtener más información, consulte el resultado anterior.
2. Enlace el proceso QEMU a los mismos núcleos físicos a los que vincula las vCPU mediante el siguiente comando:

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

NetScaler VPX con interfaces de red de transferencia SR-IOV y Fortville PCIe

Para obtener un rendimiento óptimo de las interfaces de red de paso SR-IOV y Fortville PCIe, siga estos pasos:

- Identifique el dominio NUMA al que pertenece la ranura PCIe/NIC.
- La memoria y la vCPU de NetScaler VPX deben estar ancladas al mismo dominio NUMA.

Archivo XML VPX de ejemplo para vCPU y fijación de memoria para Linux KVM:

```
1 <domain type='kvm'>
```

```

2      <name>NetScaler-VPX</name>
3      <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
4      <memory unit='KiB'>8097152</memory>
5      <currentMemory unit='KiB'>8097152</currentMemory>
6      <vcpu placement='static'>4</vcpu>
7
8      <cputune>
9          <vcupin vcpu='0' cpuset='8' />
10         <vcupin vcpu='1' cpuset='9' />
11         <vcupin vcpu='2' cpuset='10' />
12         <vcupin vcpu='3' cpuset='11' />
13     </cputune>
14
15     <numatune>
16     <memory mode='strict' nodeset='1' />
17     </numatune>
18
19     </domain>

```

Instancia de NetScaler VPX en Citrix Hypervisors

Esta sección contiene detalles de las opciones y ajustes configurables y otras sugerencias que le ayudarán a lograr un rendimiento óptimo de la instancia de NetScaler VPX en Citrix Hypervisors.

- [Configuración de rendimiento de Citrix Hypervisors](#)
- [NetScaler VPX con interfaces de red SR-IOV](#)
- [NetScaler VPX con interfaces paravirtualizadas](#)

Configuración de rendimiento de Citrix Hypervisors

Busque el dominio NUMA de la NIC mediante el comando “xl”:

```
1 xl info -n
```

Anclar vCPU de VPX a núcleos físicos.

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

Compruebe la vinculación de las vCPU.

```
1 xl vcpu-list
```

Asigne más de 8 vCPU a las máquinas virtuales NetScaler.

Para configurar más de 8 vCPU, ejecute los siguientes comandos desde la consola de Citrix Hypervisor:

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

NetScaler VPX con interfaces de red SR-IOV

Para obtener un rendimiento óptimo de las interfaces de red SR-IOV, siga estos pasos:

- Identifique el dominio NUMA al que está vinculada la ranura PCIe o la NIC.
- Anclar la memoria y la vCPU del VPX al mismo dominio NUMA.
- Enlaza la vCPU Domain-0 a la CPU restante.

NetScaler VPX con interfaces paravirtualizadas

Para obtener un rendimiento óptimo, se recomiendan dos vNIC por cada pNIC y una vNIC por cada pNIC, como en otros entornos fotovoltaicos.

Para lograr un rendimiento óptimo de las interfaces para-virtualizadas (netfront), siga estos pasos:

- Identifique el dominio NUMA al que pertenece la ranura PCIe o la NIC.
- Anclar la memoria y la vCPU del VPX al mismo dominio NUMA.
- Enlazar la vCPU Domain-0 a la CPU restante del mismo dominio NUMA.
- Anclar subprocesos Rx/Tx del host de vNIC a vCPU de dominio 0.

Anclar subprocesos de host a vCPU Domain-0:

1. Busque el Xen-ID de NetScaler VPX utilizando el comando `xl list` en el shell del host de Citrix Hypervisor.
2. Identifique los subprocesos de host mediante el siguiente comando:

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

En el siguiente ejemplo, estos valores indican:

- **vif5.0:** los subprocesos de la primera interfaz asignada a VPX en XenCenter (interfaz de administración).
- **vif5.1:** los subprocesos de la segunda interfaz asignada a VPX, etc.

```
[root@xenserver-uuffyqlx ~]# xl list
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 ~]#
[root@xenserver-uuffyqlx ~]# ps -ax | grep "vif5"
Warning: bad syntax, perhaps a bogus '-'? See /usr/share/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-dealloc]
29189 ?           S    201:33 [vif5.1-guest-rx]
29190 ?           S    80:51  [vif5.1-dealloc]
29191 ?           S     0:20  [vif5.2-guest-rx]
29192 ?           S     0:00  [vif5.2-dealloc]
[root@xenserver-uuffyqlx ~]#
```

3. Anclar los subprocessos a las vCPU Domain-0 mediante el siguiente comando:

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

Ejemplo

```
1 taskset -pc 1 29189
```

Aplicación de configuraciones NetScaler VPX en el primer arranque del dispositivo NetScaler en la nube

October 17, 2024

Puede aplicar las configuraciones de NetScaler VPX durante el primer arranque del dispositivo NetScaler en un entorno de nube. Esta etapa se aborda como fase de **prearranque** en este documento. Por lo tanto, en algunos casos, como las licencias agrupadas por ADC, una instancia VPX específica aparece en mucho menos tiempo. Esta función está disponible en Microsoft Azure, la plataforma de Google Cloud y las nubes de AWS.

Qué son los datos de usuario

Cuando aprovisiona una instancia VPX en un entorno de nube, tiene la opción de pasar datos de usuario a la instancia. Los datos de usuario le permiten realizar tareas de configuración automatizadas comunes, personalizar los comportamientos de inicio de las instancias y ejecutar scripts después de que se inicie la instancia. En el primer arranque, la instancia NetScaler VPX realiza las siguientes tareas:

- Lee los datos del usuario.
- Interpreta la configuración proporcionada en los datos de usuario.
- Aplica la configuración recién agregada a medida que se inicia.

Cómo proporcionar datos de usuario previos al arranque en una instancia de nube

Puede proporcionar datos de usuario de prearranque a la instancia de nube en formato XML. Las distintas nubes tienen interfaces diferentes para proporcionar datos de usuario.

Proporcionar datos de usuario previos al arranque mediante la consola de AWS

Cuando aprovisiona una instancia NetScaler VPX mediante la consola de AWS, vaya a **Configurar detalles de instancias > Detalles avanzados** y proporcione la configuración de datos de usuario previo al arranque en el campo **Datos de usuario**.

Para obtener instrucciones detalladas sobre cada uno de los pasos, consulte [Implementar una instancia de NetScaler VPX en AWS mediante la consola web de AWS](#). Para obtener más información, consulte la documentación de AWS sobre el [lanzamiento de una instancia](#).

The screenshot shows the AWS console interface for configuring an instance. The 'Step 3: Configure Instance Details' section is active. Under the 'Advanced Details' section, the 'User data' field is highlighted with a yellow box. The 'User data' field has three radio buttons: 'As text' (selected), 'As file', and 'Input is already base64 encoded'. Below the radio buttons is a text input area with '(Optional)' written inside.

Nota:

La versión 13.1.48.x y las versiones posteriores de NetScaler VPX admiten únicamente el modo AWS IMDSv2 para la función de datos de usuario de prearranque.

Proporcionar datos de usuario previos al arranque mediante AWS CLI

Escriba el siguiente comando en la CLI de AWS:

```
1  aws ec2 run-instances \  
2  --image-id ami-0abcdef1234567890 \  
3  --instance-type t2.micro \  
4  --count 1 \  
5  --subnet-id subnet-08fc749671b2d077c \  
6  --key-name MyKeyPair \  
7  --security-group-ids sg-0b0384b66d7d692f9 \  
8  --user-data file://my_script.txt
```

Para obtener más información, consulte la documentación de AWS sobre [instancias en ejecución](#).

Para obtener más información, consulte la documentación de AWS sobre [Uso de datos de usuario de instancias](#)

Proporcionar datos de usuario previos al arranque mediante la consola de Azure

Cuando aprovisiona una instancia NetScaler VPX mediante la consola de Azure, vaya a **Crear una máquina virtual > ficha Avanzadas**. En el campo **Datos personalizados**, proporcione la configuración de datos de usuario de prearranque.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Basics Disks Networking Management **Advanced** Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ [Select an extension to install](#)

Custom data

Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#) ⓘ

Custom data

ⓘ Custom data on the selected image will be processed by cloud-init. [Learn more about custom data and cloud init](#) ⓘ

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group ⓘ ▼

Proporcionar datos de usuario previos al arranque mediante la CLI de Azure

Escriba el siguiente comando en la CLI de Azure:

```

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

```

Ejemplo

```

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

```

Puede pasar los datos personalizados o la configuración previa al arranque como un archivo al parámetro “—custom-data”. En este ejemplo, el nombre de archivo es **MyCloudInitScript.txt**.

Para obtener más información, consulte la [documentación de Azure CLI](#).

Proporcionar datos de usuario previos al arranque mediante la consola de GCP

Cuando aprovisione una instancia NetScaler VPX mediante la consola de GCP, complete las propiedades de la instancia. Amplíe **Administración, seguridad, discos, redes, arrendamiento único**. Acceda a la ficha **Administración**. En la sección **Automatización**, proporcione la configuración de datos de usuario de prearranque en el campo **Script de inicio**.

Para obtener información detallada sobre cómo crear la instancia VPX con GCP, consulta [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#).

The screenshot shows the 'Automation' section of the GCP console. It includes a 'Description (Optional)' text area, a 'Deletion protection' checkbox (unchecked), and a 'Reservations' dropdown menu set to 'Automatically use created reservation'. The 'Automation' section is highlighted with a yellow border and contains a 'Startup script (Optional)' text area. Below it is a 'Metadata (Optional)' section with a table for key-value pairs and an '+ Add item' button.

Key	Value

+ Add item

Proporcionar datos de usuario de prearranque mediante la CLI de gcloud

Escriba el siguiente comando en la CLI de GCP:

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

metadata-from-file: Lee el valor o los datos de usuario de un archivo almacenado en el .

Para obtener más información, consulta la [documentación de la CLI de gcloud](#)

Formato de datos de usuario de prearranque

Los datos de usuario de prearranque deben proporcionarse a la instancia de nube en formato XML. Los datos de usuario de prearranque de NetScaler que proporciona a través de la infraestructura de nube durante el arranque pueden abarcar las cuatro secciones siguientes:

- Configuración de NetScaler representada con la etiqueta `<NS-CONFIG>`;
- Arranque personalizado de NetScaler representado con la etiqueta `<NS-BOOTSTRAP>`;
- Almacenamiento de scripts de usuario en NetScaler representados con la etiqueta `<NS-SCRIPTS>`;
- Configuración de licencias agrupadas representada con la etiqueta `<NS-LICENSE-CONFIG>`;

Puede proporcionar las cuatro secciones anteriores en cualquier orden dentro de la configuración de prearranque de ADC. Asegúrese de seguir estrictamente el formato que se muestra en las secciones siguientes mientras proporciona los datos de usuario de prearranque.

Nota:

La configuración completa de datos de usuario de prearranque debe incluirse en la etiqueta `<NS-PRE-BOOT-CONFIG>`, tal y como se muestra en los ejemplos siguientes.

Ejemplo 1:

```

1 <NS-PRE-BOOT-CONFIG>
2   <NS-CONFIG>           </NS-CONFIG>
3   <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
4   <NS-SCRIPTS>         </NS-SCRIPTS>
5   <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
6 </NS-PRE-BOOT-CONFIG>
```

Ejemplo 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>
```

Utilice la etiqueta `<NS-CONFIG>` para proporcionar las configuraciones específicas de NetScaler VPX que deben aplicarse a la instancia VPX en la fase previa al arranque.

Nota:

La sección `<NS-CONFIG>` debe tener comandos CLI de ADC válidos. No se verifican los errores sintácticos ni el formato de las CLI.

Configuraciones de NetScaler

Utilice la etiqueta `<NS-CONFIG>` para proporcionar las configuraciones específicas de NetScaler VPX que deben aplicarse a la instancia VPX en la fase previa al arranque.

Nota:

La sección `<NS-CONFIG>` debe tener comandos CLI de ADC válidos. No se verifican los errores sintácticos ni el formato de las CLI.

Ejemplo

En el ejemplo siguiente, la sección `<NS-CONFIG>` contiene los detalles de las configuraciones. Una VLAN de ID '5' está configurada y enlazada al SNIP (5.0.0.1). También se configura un servidor virtual de equilibrio de carga (4.0.0.101).

```

<NS-BOOT-CONFIG>
  <NS-CONFIG>
    add vlan 5
    add ns ip 5.0.0.1 255.255.255.0

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

```

Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```

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

La instancia de NetScaler VPX muestra la configuración aplicada en la <NS-CONFIG> sección, tal como se muestra en las siguientes ilustraciones.

```
> sh ns ip
-----
1) 10.160.0.72      0      NetScaler IP      Active  Enabled  Enabled  NA      Enabled
2) 5.0.0.1          0      SNIP              Active  Enabled  Enabled  NA      Enabled
3) 4.0.0.101       0      VIP               Active  Enabled  Enabled  Enabled Enabled
Done
> sh vlan
1) VLAN ID: 1
   Link-local IPv6 addr: fe80::4001:aff:fea0:48/64
   Interfaces : 1/1 1/2 LO/1
2) VLAN ID: 5      VLAN Alias Name:
   IPs :
      5.0.0.1      Mask: 255.255.255.0
3) VLAN ID: 10     VLAN Alias Name:
   Interfaces : 0/1
   IPs :
      10.160.0.72   Mask: 255.255.240.0
Done
```

```

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

Service(s) Summary
      IP port      Type      State      Req/s
preb...s_201    5.0.0.201    80      HTTP      DOWN      0/s
gcpl...vice0 169.254.169.254    53      DNS       UP        0/s
Done
> sh service preboot_s5_201
preboot_s5_201 (5.0.0.201:80) - HTTP
State: DOWN
Last state change was at Tue Dec 29 07:18:28 2020
Time since last state change: 0 days, 00:05:02.820
Server Name: 5.0.0.201
Server ID : None      Monitor Threshold : 0
Max Conn: 0      Max Req: 0      Max Bandwidth: 0 kbits
Use Source IP: NO
Client Keepalive(CKA): NO
Monitoring Owner: 0
Access Down Service: NO
TCP Buffering(TCPB): NO
HTTP Compression(CMP): NO
Idle timeout: Client: 180 sec      Server: 360 sec
Client IP: DISABLED
Cacheable: NO
SC: OFF
SP: OFF
Down state flush: ENABLED
Monitor Connection Close : NONE
Appflow logging: ENABLED
Process Local: DISABLED

```

Guiones de usuario

Utilice la etiqueta `<NS-SCRIPTS>` para proporcionar cualquier script que deba almacenarse y ejecutarse en la instancia de NetScaler VPX.

Puede incluir muchos scripts dentro de la etiqueta `<NS-SCRIPTS>`. Cada guión debe incluirse dentro de la etiqueta `<SCRIPT>`. Cada sección `<SCRIPT>` corresponde a un guión y contiene todos los detalles del guión mediante las siguientes subetiquetas.

- **`<SCRIPT-NAME>`**: Indica el nombre del archivo de script que debe almacenarse.
- **`<SCRIPT-CONTENT>`**: Indica el contenido del archivo que debe almacenarse.
- **`<SCRIPT-TARGET-LOCATION>`**: Indica la ubicación de destino designada en la que debe almacenarse este archivo. Si no se proporciona la ubicación de destino, de forma predeterminada, el archivo o el script se guardan en el directorio `"/nsconfig"`.
- **`<SCRIPT-NS-BOOTUP>`**: Especifique los comandos que utiliza para ejecutar el script.

- Si utiliza la sección `<lt;SCRIPT-NS-BOOTUP>`, los comandos proporcionados en la sección se almacenan en `"/nsconfig/nsafter.sh "`, y los comandos se ejecutan después de que se inicie el motor de paquetes como parte de la ejecución de `"nsafter.sh"`.
- Si no utiliza la sección `<lt;SCRIPT-NS-BOOTUP>`, el archivo de script se almacena en la ubicación de destino que especifique.

Ejemplo 1:

En este ejemplo, la etiqueta `<lt;NS-SCRIPTS>` contiene detalles de un único script: `script-1.sh`. El script `"script-1.sh"` se guarda en el directorio `"/var"`. El script se rellena con el contenido especificado y se ejecuta con el comando `"sh /var/script-1.sh"` después de arrancar el motor de paquetes.

```

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

```

Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```

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

```

En la siguiente instantánea, puede comprobar que el script `"script-1.sh"` está guardado en el directorio

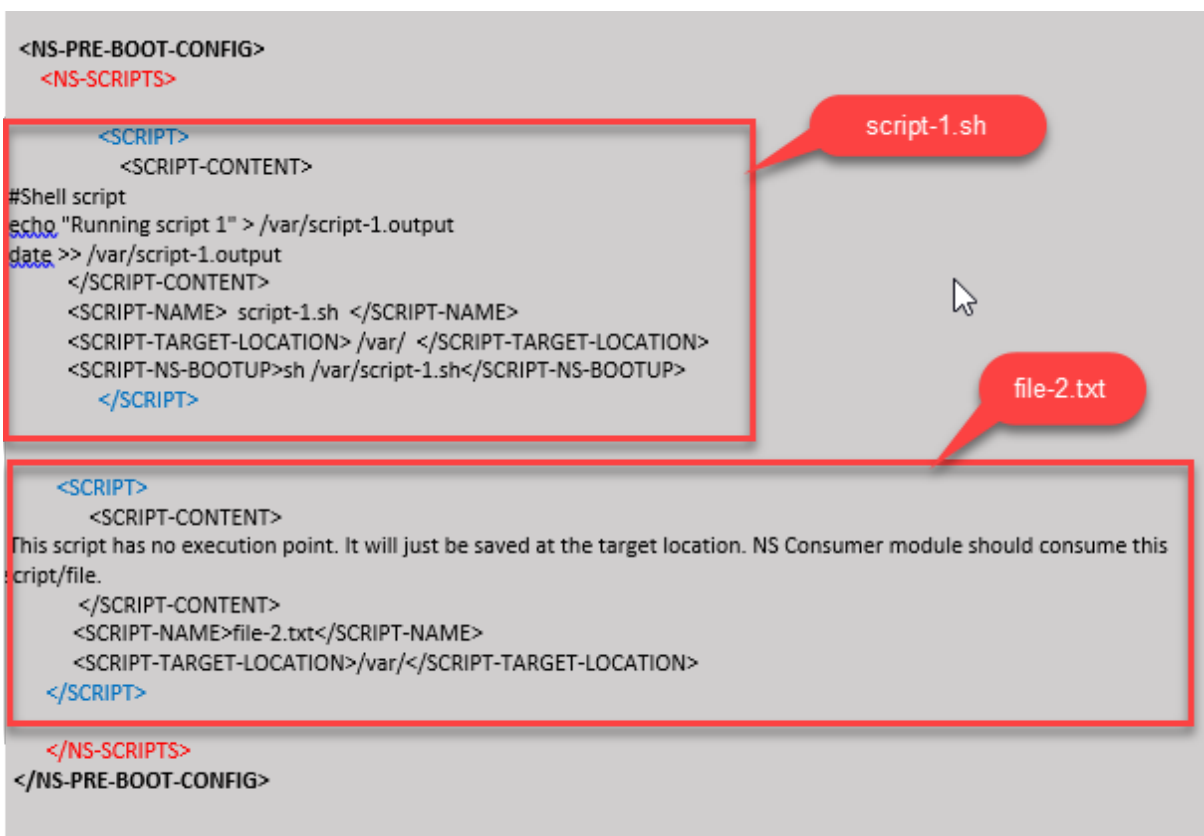
“/var/”. Se ejecuta el script “Script-1.sh”y el archivo de salida se crea correctamente.

```
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" > /var/script-1.output
date >> /var/script-1.output
root@ns#
root@ns# cat /var/script-1.output
Running script 1
Wed Jan  6 05:25:33 UTC 2021
root@ns#
root@ns#
```

Ejemplo 2:

En el ejemplo siguiente, la etiqueta `<NS-SCRIPTS>`; contiene detalles de dos scripts.

- El primer script se guarda como “script-1.sh”en el directorio “/var”. El script se rellena con el contenido especificado y se ejecuta con el comando “sh /var/script-1.sh”después de arrancar el motor de paquetes.
- El segundo script se guarda como “file-2.txt”en el directorio “/var”. Este archivo se rellena con el contenido especificado. Pero no se ejecuta porque no `<SCRIPT-NS-BOOTUP>`; se proporciona el comando de ejecución de arranque.



Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```

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

En la siguiente instantánea, puede comprobar que script-1.sh y file-2.txt se crean en el directorio “/var/”. Script-1.sh se ejecuta y el archivo de salida se crea correctamente.

```
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" > /var/script-1.output
date >> /var/script-1.output
root@ns#
root@ns# cat /var/script-1.output
Running script 1
Wed Jan  6 05:08:56 UTC 2021
root@ns#
root@ns#
root@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
root@ns#
root@ns#
```

Licensing

Utilice la etiqueta `<NS-LICENSE-CONFIG>` para aplicar las licencias agrupadas de NetScaler al iniciar la instancia VPX. Utilice la etiqueta `<LICENSE-COMMANDS>` dentro de la sección `<NS-LICENSE-CONFIG>` para proporcionar los comandos de licencia agrupados. Estos comandos deben ser válidos sintácticamente.

Puede especificar los detalles de las licencias agrupadas, como el tipo de licencia, la capacidad y el servidor de licencias en la sección `<LICENSE-COMMANDS>` mediante los comandos de licencias agrupados estándar. Para obtener más información, consulte [Configurar las licencias de capacidad agrupada de NetScaler](#).

Después de aplicar el `<NS-LICENSE-CONFIG>`, VPX aparece la edición solicitada al arrancar y VPX intenta extraer las licencias configuradas del servidor de licencias.

- Si la retirada de la licencia se realiza correctamente, el ancho de banda configurado se aplica a VPX.
- Si se produce un error en la retirada de la licencia, la licencia no se recupera del servidor de licencias en un plazo de 10 a 12 minutos aproximadamente. Como resultado, el sistema se reinicia y entra en un estado sin licencia.

Ejemplo

En el ejemplo siguiente, después de aplicar el `<NS-LICENSE-CONFIG>`, VPX aparece la edición Premium al arrancar y VPX intenta extraer las licencias configuradas del servidor de licencias (10.102.38.214).

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

    add ns licenseserver 10.102.38.214 -port 2800
    set ns capacity -unit gbps -bandwidth 3 edition platinum

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

Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

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

Como se muestra en la siguiente ilustración, puede ejecutar el comando “show license server” y comprobar que el servidor de licencias (10.102.38.214) se ha agregado al VPX.

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

Bootstrapping

Utilice la etiqueta `<NS-BOOTSTRAP>` para proporcionar la información de bootstrapping personalizada. Puede utilizar las etiquetas `<SKIP-DEFAULT-BOOTSTRAP>` y `<NEW-BOOTSTRAP-SEQUENCE>` dentro de la sección `<NS-BOOTSTRAP>`. En esta sección se informa al dispositivo NetScaler si debe evitar el arranque predeterminado o no. Si se evita el bootstrapping predeterminado, en esta sección se ofrece la opción de proporcionar una nueva secuencia de bootstrapping.

Configuración de arranque predeterminada

La configuración de arranque predeterminada en el dispositivo NetScaler sigue estas asignaciones de interfaz:

- **Eth0** - Interfaz de administración con una determinada dirección NSIP.
- **Eth1** - Interfaz orientada al cliente con una determinada dirección VIP.
- **Eth2**: Interfaz orientada al servidor con una determinada dirección SNIP.

Personalizar la configuración bootstrap

Puede omitir la secuencia de arranque predeterminada y proporcionar una nueva secuencia de arranque para la instancia NetScaler VPX. Utilice la etiqueta `<NS-BOOTSTRAP>` para proporcionar la información de bootstrapping personalizada. Por ejemplo, puede cambiar el bootstrapping predeterminado, donde la interfaz de administración (NSIP), la interfaz orientada al cliente (VIP) y la interfaz orientada al servidor (SNIP) siempre se proporcionan en un orden determinado.

En la tabla siguiente se indica el comportamiento de bootstrapping con los distintos valores permitidos en etiquetas `<SKIP-DEFAULT-BOOTSTRAP>` y `<NEW-BOOTSTRAP-SEQUENCE>`:

<code>SKIP-DEFAULT-BOOTSTRAP</code>	<code>NEW-BOOTSTRAP-SEQUENCE</code>	Comportamiento bootstrap
SÍ	SÍ	Se omite el comportamiento de bootstrapping predeterminado y se ejecuta una nueva secuencia de arranque personalizada proporcionada en la sección <code><NS-BOOTSTRAP></code> .
SÍ	NO	Se omite el comportamiento de arranque predeterminado. Se ejecutan los comandos bootstrap proporcionados en la sección <code><NS-CONFIG></code> .

Puede personalizar la configuración de arranque mediante los tres métodos siguientes:

- Proporcionar solo los detalles de la interfaz
- Proporcionar los detalles de la interfaz junto con las direcciones IP y la máscara de subred
- Proporcionar comandos relacionados con el arranque en la sección `<NS-CONFIG>`;

Método 1: arranque personalizado especificando solo los detalles de la interfaz

Se especifican las interfaces de administración, orientadas al cliente y orientadas al servidor, pero no sus direcciones IP y máscaras de subred. Las direcciones IP y las máscaras de subred se completan consultando la infraestructura en la nube.

Ejemplo de arranque personalizado para AWS

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte [Cómo proporcionar datos de usuario de prearranque en la instancia de nube](#). La interfaz Eth2 se asigna como interfaz de administración (NSIP), interfaz Eth1 como interfaz de cliente (VIP) e interfaz Eth0 como interfaz de servidor (SNIP). La sección `<NS-BOOTSTRAP>` contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.

```

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

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

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

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

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

```

Después de crear la instancia de VM, en el portal de AWS, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Vaya al **portal de AWS > instancias EC2** y seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. En la ficha **Descripción**, puede verificar las propiedades de cada interfaz de red como se muestra en las ilustraciones siguientes.



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

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	172.31.76.177 
Private DNS Name	ip-172-31-76-177.ap-south-1.compute.internal 

Puede ejecutar el comando `show nsip` en la **CLI de ADC** y comprobar las interfaces de red aplicadas a la instancia de NetScaler VPX durante el primer arranque del dispositivo ADC.

```

> sh ns ip
-----
Ipaddress      Traffic Domain  Type           Mode   Arp   Icmp   Vserver  State
-----
1) 172.31.52.88  0              NetScaler IP   Active Enabled Enabled NA      Enabled
2) 172.31.76.177 0              SNIP          Active Enabled Enabled NA      Enabled
3) 172.31.5.155  0              VIP           Active Enabled Enabled Enabled Enabled
Done
> sh vlan
-----
1) VLAN ID: 1
   Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
   Interfaces : 1/1 1/3 LO/1

2) VLAN ID: 10   VLAN Alias Name:
   Interfaces : 1/2
   IPs :
       172.31.52.88      Mask: 255.255.240.0

Done
> sh route
-----
Network      Netmask      Gateway/OwnedIP  VLAN  State  Traffic Domain  Type
-----
1) 0.0.0.0    0.0.0.0      172.31.48.1     0     UP     0               STATIC
2) 127.0.0.0  255.0.0.0    127.0.0.1       0     UP     0               PERMANENT
3) 172.31.0.0 255.255.240.0 172.31.5.155    0     UP     0               DIRECT
4) 172.31.48.0 255.255.240.0 172.31.52.88    0     UP     0               DIRECT
5) 172.31.64.0 255.255.240.0 172.31.76.177   0     UP     0               DIRECT
6) 172.31.0.2  255.255.255.255 172.31.48.1     0     UP     0               STATIC
Done

```

Ejemplo de arranque personalizado para Azure

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte [Cómo proporcionar datos de usuario de prearranque en la instancia de nube](#). La interfaz Eth1 se asigna como interfaz de administración (NSIP), interfaz Eth0 como interfaz de cliente (VIP) e interfaz Eth2 como interfaz de servidor (SNIP). La sección `<NS-BOOTSTRAP>` contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.


```

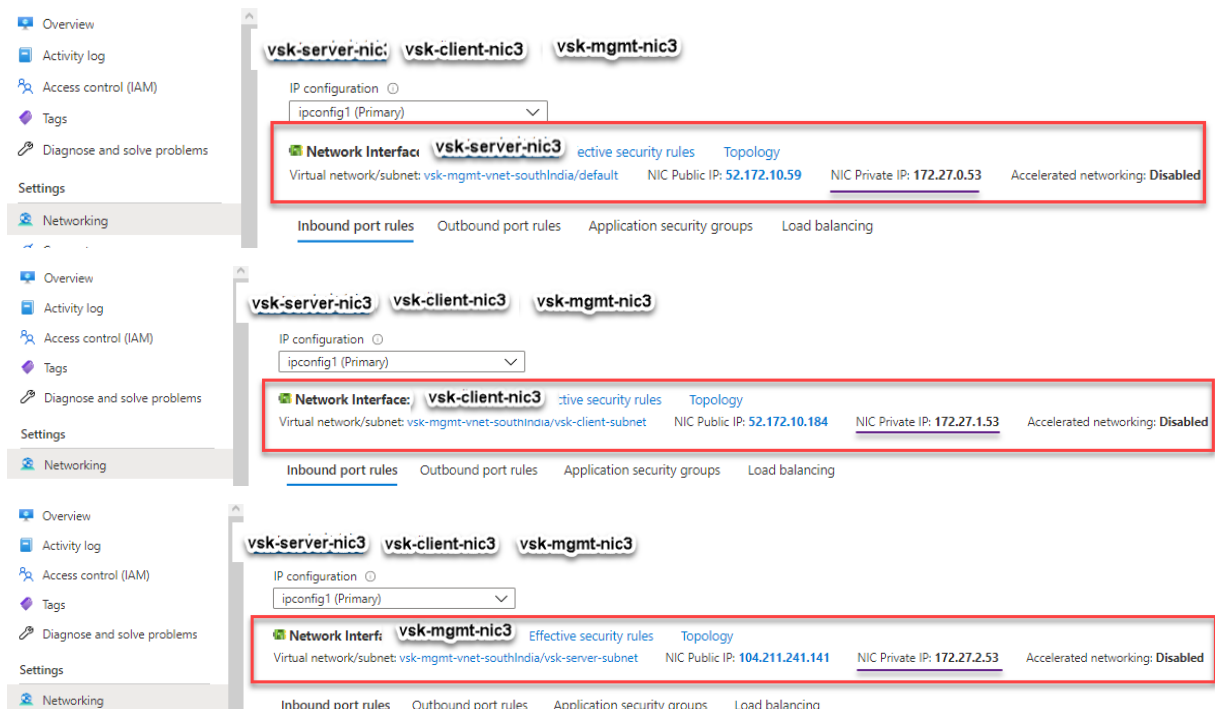
<NS-PRE-BOOT-CONFIG>
  <NS-BOOTSTRAP>
    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
    <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

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

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

    <SERVER-INTERFACE-CONFIG>
      <INTERFACE-NUM>eth0</INTERFACE-NUM>
    </SERVER-INTERFACE-CONFIG>
  </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
  
```

Puede ver que la instancia NetScaler VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes** compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.



Puede ejecutar el comando `show ns ip` en la CLI de ADC y verificar que se haya aplicado la nueva

secuencia de arranque especificada en la sección `<NS-BOOTSTRAP>`. Puede ejecutar el comando “show route” para verificar la máscara de subred.

```
> sh ns ip
      Ippaddress      Traffic Domain  Type
-----
1)    172.27.2.53      0               NetScaler IP
2)    172.27.0.53      0               SNIP
3)    172.27.1.53      0               VIP
      Mode           Arp           Icmp          Vserver      State
-----
      Active        Enabled       Enabled       NA           Enabled
      Active        Enabled       Enabled       NA           Enabled
      Active        Enabled       Enabled       Enabled      Enabled
Done
> sh vlan
1)    VLAN ID: 1
      Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
      Interfaces : 0/1 1/1 LO/1
2)    VLAN ID: 10     VLAN Alias Name:
      Interfaces : 1/2
      IPs :
          172.27.2.53      Mask: 255.255.255.0
Done
> sh route
      Network          Netmask          Gateway/OwnedIP  VLAN  State  Traffic Domain  Type
-----
1)    0.0.0.0           0.0.0.0          172.27.2.1      0     UP     0               STATIC
2)    127.0.0.0         255.0.0.0        127.0.0.1       0     UP     0               PERMANENT
3)    172.27.0.0         255.255.255.0    172.27.0.53     0     UP     0               DIRECT
4)    172.27.1.0         255.255.255.0    172.27.1.53     0     UP     0               DIRECT
5)    172.27.2.0         255.255.255.0    172.27.2.53     0     UP     0               DIRECT
6)    169.254.0.0        255.255.0.0      172.27.0.1       0     UP     0               STATIC
7)    168.63.129.16     255.255.255.255  172.27.0.1       0     UP     0               STATIC
8)    169.254.169.254   255.255.255.255  172.27.0.1       0     UP     0               STATIC
Done
>
```

Ejemplos de bootstrap personalizados para GCP

Proporciona la secuencia de arranque personalizada como se muestra en el siguiente ejemplo. Para obtener más información, consulte [Cómo proporcionar datos de usuario de prearranque en la instancia de nube](#). La interfaz Eth2 se asigna como interfaz de administración (NSIP), interfaz Eth1 como interfaz de cliente (VIP) e interfaz Eth0 como interfaz de servidor (SNIP). La sección `<NS-BOOTSTRAP>` contiene solo los detalles de la interfaz y no los detalles de las direcciones IP y las máscaras de subred.

```

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

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

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

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

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

Después de crear la instancia de VM en el portal de GCP, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Vaya a las propiedades de la interfaz de red y compruebe los detalles de la NIC de la siguiente manera

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

Public DNS PTR Record
None

Puede ejecutar el comando `show nsip` en la **CLI de ADC** y comprobar las interfaces de red aplicadas a la instancia de NetScaler VPX durante el primer arranque del dispositivo ADC.

```

> sh ns ip
      Ippaddress      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      0               SNIP                 Active Enabled Enabled NA      Enabled
3)    10.128.0.40      0               VIP                  Active Enabled Enabled Enabled Enabled
Done
> sh vlan
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 :
          10.128.4.27      Mask: 255.255.255.0
Done
> sh route
      Network          Netmask          Gateway/OwnedIP    VLAN   State   Traffic Domain  Type
      -----
1)    0.0.0.0            0.0.0.0          10.128.4.1         0      UP      0                STATIC
2)    127.0.0.0          255.0.0.0        127.0.0.1          0      UP      0                PERMANENT
3)    10.128.0.0          255.255.255.0    10.128.0.40        0      UP      0                DIRECT
4)    10.128.4.0          255.255.255.0    10.128.4.27        0      UP      0                DIRECT
5)    10.160.0.0          255.255.240.0    10.160.0.71        0      UP      0                DIRECT
Done
> █

```

Método 2: arranque personalizado especificando las interfaces, las direcciones IP y las máscaras de subred

Se especifican las interfaces de administración, orientadas al cliente y orientadas al servidor junto con sus direcciones IP y máscara de subred.

Ejemplos de arranque personalizados para AWS

En el siguiente ejemplo, omita el bootstrap predeterminado y ejecuta una nueva secuencia de arranque para el dispositivo NetScaler. Para la nueva secuencia de arranque, especifique los siguientes detalles:

- **Interfaz de administración:** Interfaz - Eth1, NSIP - 172.31.52.88 y máscara de subred - 255.255.240.0
- **Interfaz orientada al cliente:** Interfaz - Eth0, VIP - 172.31.5.155 y máscara de subred - 255.255.240.0.
- **Interfaz orientada al servidor:** Interfaz - Eth2, SNIP - 172.31.76.177 y máscara de subred - 255.255.240.0.

```
<NS-PRE-BOOT-CONFIG>
  <NS-BOOTSTRAP>
    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
    <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
    <MGMT-INTERFACE-CONFIG>
      <INTERFACE-NUM>eth1 </INTERFACE-NUM>
      <IP>172.31.52.88 </IP>
      <SUBNET-MASK>255.255.240.0 </SUBNET-MASK>
    </MGMT-INTERFACE-CONFIG>
    <CLIENT-INTERFACE-CONFIG>
      <INTERFACE-NUM>eth0 </INTERFACE-NUM>
      <IP>172.31.5.155 </IP>
      <SUBNET-MASK>255.255.240.0 </SUBNET-MASK>
    </CLIENT-INTERFACE-CONFIG>
    <SERVER-INTERFACE-CONFIG>
      <INTERFACE-NUM>eth2 </INTERFACE-NUM>
      <IP>172.31.76.177 </IP>
      <SUBNET-MASK>255.255.240.0 </SUBNET-MASK>
    </SERVER-INTERFACE-CONFIG>
  </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

Puede ejecutar el comando “show nsip” en la CLI de ADC y comprobar que se aplica la nueva secuencia de arranque especificada en la sección `<NS-BOOTSTRAP>`. Puede ejecutar el comando “show route” para verificar la máscara de subred.

```

> sh ns ip
-----
Ipaddress      Traffic Domain  Type           Mode   Arp   Icmp   Vserver  State
-----
1) 172.31.52.88   0              NetScaler IP   Active Enabled Enabled NA       Enabled
2) 172.31.76.177 0              SNIP           Passive Enabled Enabled NA       Enabled
3) 172.31.5.155  0              VIP            Passive Enabled Enabled Enabled Enabled
Done
> sh vlan
1)  VLAN ID: 1
   Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
   Interfaces : 1/1 1/3 LO/1
2)  VLAN ID: 10   VLAN Alias Name:
   Interfaces : 1/2
   IPs :
      172.31.52.88      Mask: 255.255.240.0
Done
> sh route
-----
Network      Netmask      Gateway/OwnedIP  VLAN  State  Traffic Domain  Type
-----
1) 0.0.0.0     0.0.0.0      172.31.48.1     0     UP     0              STATIC
2) 127.0.0.0   255.0.0.0    127.0.0.1      0     UP     0              PERMANENT
3) 172.31.0.0   255.255.240.0 172.31.5.155   0     UP     0              DIRECT
4) 172.31.48.0  255.255.240.0 172.31.52.88   0     UP     0              DIRECT
5) 172.31.64.0  255.255.240.0 172.31.76.177  0     UP     0              DIRECT
6) 172.31.0.2   255.255.255.255 172.31.48.1    0     UP     0              STATIC
Done

```

Ejemplo de arranque personalizado para Azure

En el ejemplo siguiente, se menciona una nueva secuencia de arranque para ADC y se omite el bootstrap predeterminado. Proporciona los detalles de la interfaz junto con las direcciones IP y las máscaras de subred de la siguiente manera:

- Interfaz de administración (eth2), NSIP (172.27.2.53) y máscara de subred (255.255.255.0)
- Interfaz orientada al cliente (eth1), VIP (172.27.1.53) y máscara de subred (255.255.255.0)
- Interfaz orientada al servidor (eth0), SNIP (172.27.0.53) y máscara de subred (255.255.255.0)

```

<NS-PRE-BOOT-CONFIG>

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

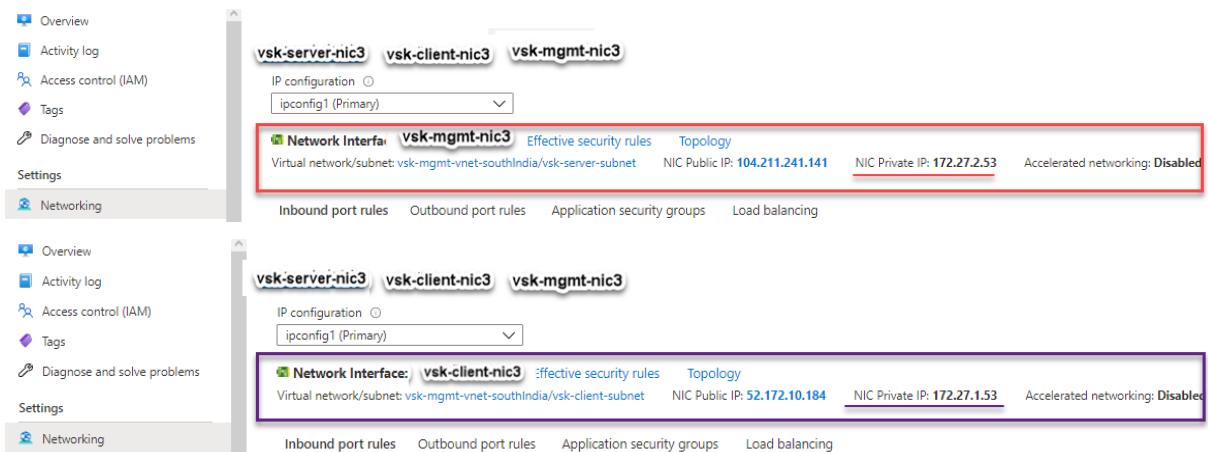
    <MGMT-INTERFACE-CONFIG>
      <INTERFACE-NUM> eth2 </INTERFACE-NUM>
      <IP> 172.27.2.53 </IP>
      <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
    </MGMT-INTERFACE-CONFIG>

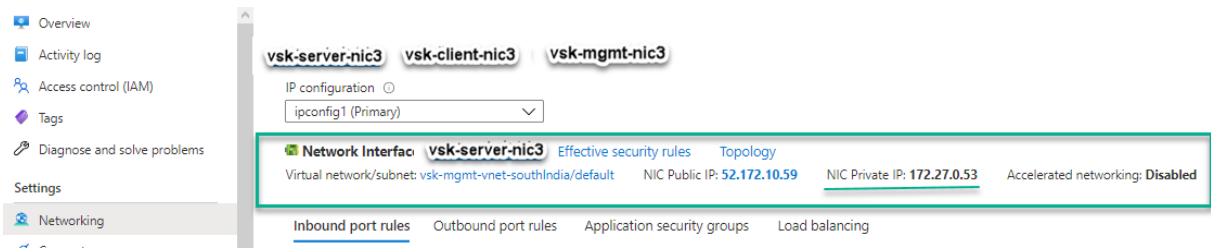
    <CLIENT-INTERFACE-CONFIG>
      <INTERFACE-NUM> eth1 </INTERFACE-NUM>
      <IP> 172.27.1.53 </IP>
      <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
    </CLIENT-INTERFACE-CONFIG>

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

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

Puede ver que la instancia NetScaler VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes** compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.





Puede ejecutar el comando “show nsip” en la CLI de ADC y comprobar que se aplica la nueva secuencia de arranque especificada en la sección <code>NS-BOOTSTRAP</code>. Puede ejecutar el comando “show route” para verificar la máscara de subred.

```
> sh ns ip
-----
1) 172.27.2.53 0 NetScaler IP Active Enabled Enabled NA Enabled
2) 172.27.0.53 0 SNIP Active Enabled Enabled NA Enabled
3) 172.27.1.53 0 VIP Active Enabled Enabled Enabled Enabled
Done
> sh vlan
1) VLAN ID: 1
Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
Interfaces : 0/1 1/1 LO/1
2) VLAN ID: 10 VLAN Alias Name:
Interfaces : 1/2
IPs :
172.27.2.53 Mask: 255.255.255.0
Done
> sh route
-----
1) 0.0.0.0 0.0.0.0 172.27.2.1 0 UP 0 STATIC
2) 127.0.0.0 255.0.0.0 127.0.0.1 0 UP 0 PERMANENT
3) 172.27.0.0 255.255.255.0 172.27.0.53 0 UP 0 DIRECT
4) 172.27.1.0 255.255.255.0 172.27.1.53 0 UP 0 DIRECT
5) 172.27.2.0 255.255.255.0 172.27.2.53 0 UP 0 DIRECT
6) 169.254.0.0 255.255.0.0 172.27.0.1 0 UP 0 STATIC
7) 168.63.129.16 255.255.255.255 172.27.0.1 0 UP 0 STATIC
8) 169.254.169.254 255.255.255.255 172.27.0.1 0 UP 0 STATIC
Done
```

Ejemplo de bootstrap personalizado para GCP

En el ejemplo siguiente, se menciona una nueva secuencia de arranque para ADC y se omite el bootstrap predeterminado. Proporciona los detalles de la interfaz junto con las direcciones IP y las máscaras de subred de la siguiente manera:

- Interfaz de administración (eth2), NSIP (10.128.4.31) y máscara de subred (255.255.255.0)
- Interfaz orientada al cliente (eth1), VIP (10.128.0.43) y máscara de subred (255.255.255.0)
- Interfaz orientada al servidor (eth0), SNIP (10.160.0.75) y máscara de subred (255.255.255.0)


```

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

    <MGMT-INTERFACE-CONFIG>
      <INTERFACE-NUM> eth2 </INTERFACE-NUM>
      <IP> 10.128.4.31 </IP>
      <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
    </MGMT-INTERFACE-CONFIG>

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

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

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

Una vez creada la instancia de VM en el portal de GCP con el bootstrap personalizado, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Vaya a las propiedades de la interfaz de red y compruebe los detalles de la NIC de la siguiente manera

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

Puede ejecutar el comando “show nsip” en la CLI de ADC y comprobar que se aplica la nueva secuencia de arranque especificada en la sección `<NS-BOOTSTRAP>`. Puede ejecutar el comando “show route” para verificar la máscara de subred.

```

> sh ns ip
-----
Ipaddress      Traffic Domain  Type           Mode   Arp   Icmp   Vserver  State
-----
1) 10.128.4.31   0              NetScaler IP   Active Enabled Enabled NA      Enabled
2) 10.160.0.75   0              SNIP          Passive Enabled Enabled NA      Enabled
3) 10.128.0.43   0              VIP           Passive Enabled Enabled Enabled Enabled
Done
> sh vlan
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 :
      10.128.4.31      Mask: 255.255.255.0
Done
> sh route
-----
Network        Netmask        Gateway/OwnedIP  VLAN   State  Traffic Domain  Type
-----
1) 0.0.0.0      0.0.0.0       10.128.4.1      0      UP     0               STATIC
2) 127.0.0.0    255.0.0.0     127.0.0.1      0      UP     0               PERMANENT
3) 10.128.0.0   255.255.255.0 10.128.0.43     0      UP     0               DIRECT
4) 10.128.4.0   255.255.255.0 10.128.4.31     0      UP     0               DIRECT
5) 10.160.0.0   255.255.255.0 10.160.0.75     0      UP     0               DIRECT
Done
>

```

Método 3: Arranque personalizado proporcionando comandos relacionados con el bootstrap en la sección <code>NS-CONFIG</code>;

Puede proporcionar los comandos relacionados con el arranque en la sección <code>NS-CONFIG</code>;. En la sección <code>NS-BOOTSTRAP</code>;, debe especificar <code>NEW-BOOTSTRAP-SEQUENCE</code>; como “No” para ejecutar los comandos de arranque de la sección <code>NS-CONFIG</code>;. También debe proporcionar los comandos para asignar NSIP, ruta predeterminada y NSVLAN. Además, proporcione los comandos relevantes para la nube que utiliza.

Antes de proporcionar un arranque personalizado, asegúrese de que su infraestructura en la nube admite una configuración de interfaz concreta.

Ejemplo de arranque personalizado para AWS

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección <code>NS-CONFIG</code>;. La sección <code>NS-BOOTSTRAP</code>; indica que se omita el bootstrapping predeterminado y se ejecuta la información de arranque personalizada proporcionada en la sección <code>NS-CONFIG</code>;. También debe proporcionar los comandos para crear NSIP, agregar una ruta predeterminada y agregar NSVLAN.

```

<NS-PRE-BOOT-CONFIG>
  <NS-CONFIG>
    set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
    add route 0.0.0.0 0.0.0.0 172.31.48.1
    set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
    add route 172.31.0.2 255.255.255.255 172.31.48.1

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

  </NS-CONFIG>

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

</NS-PRE-BOOT-CONFIG>

```

Bootstrap related commands

route to DNS server is added through default gateway

Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```

1  <NS-PRE-BOOT-CONFIG>
2    <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   </NS-CONFIG>
15
16   <NS-BOOTSTRAP>
17     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
18     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
19   </NS-BOOTSTRAP>
20
21
22 </NS-PRE-BOOT-CONFIG>

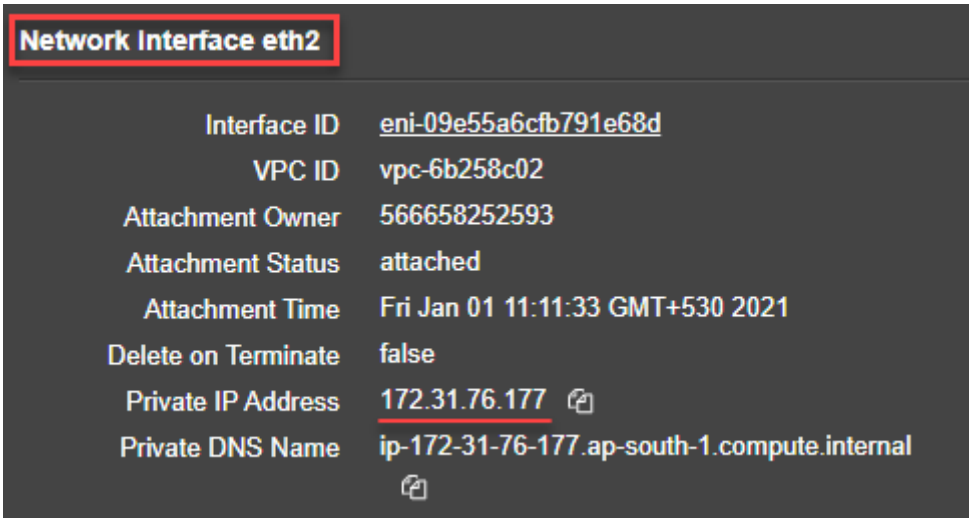
```

Después de crear la instancia de VM, en el portal de AWS, puede verificar las propiedades de la interfaz de red de la siguiente manera:

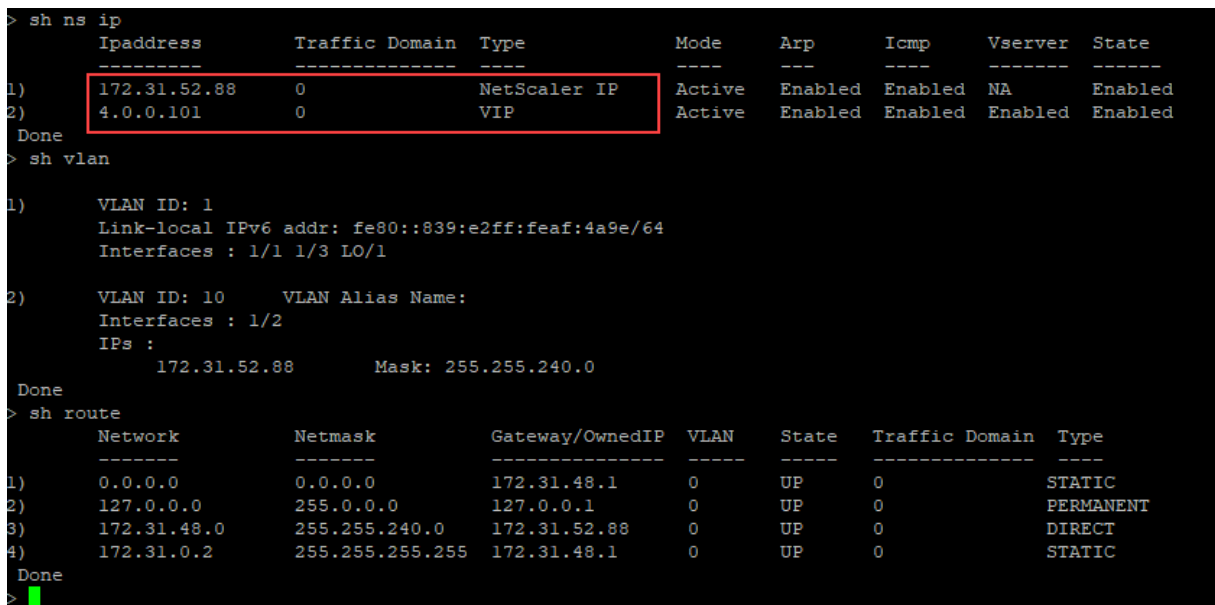
1. Vaya al **portal de AWS > instancias EC2** y seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. En la ficha **Descripción**, puede verificar las propiedades de cada interfaz de red como se muestra en las ilustraciones siguientes.

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	
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



Puede ejecutar el comando `show ns ip` en la **CLI de ADC** y comprobar las interfaces de red aplicadas a la instancia de NetScaler VPX durante el primer arranque del dispositivo ADC.



Ejemplo de arranque personalizado para Azure

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección `<NS-CONFIG>`. La sección `<NS-BOOTSTRAP>` indica que se omite el bootstrapping predefinido y se ejecuta la información de arranque personalizada proporcionada en la sección `<NS-CONFIG>`.

Nota:

Para la nube de Azure, el servidor de metadatos de instancias (IMDS) y los servidores DNS solo

se puede acceder a través de la interfaz principal (Eth0). Por lo tanto, si la interfaz Eth0 no se utiliza como interfaz de administración (NSIP), la interfaz Eth0 debe configurarse al menos como SNIP para el acceso IMDS o DNS al trabajo. También se debe agregar la ruta al extremo IMDS (169.254.169.254) y al extremo DNS (168.63.129.16) a través de la puerta de enlace de Eth0.

```

<NS-PRE-BOOT-CONFIG>

  <NS-CONFIG>

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

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

  </NS-CONFIG>

  <NS-BOOTSTRAP>

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

  </NS-BOOTSTRAP>
  
```

```

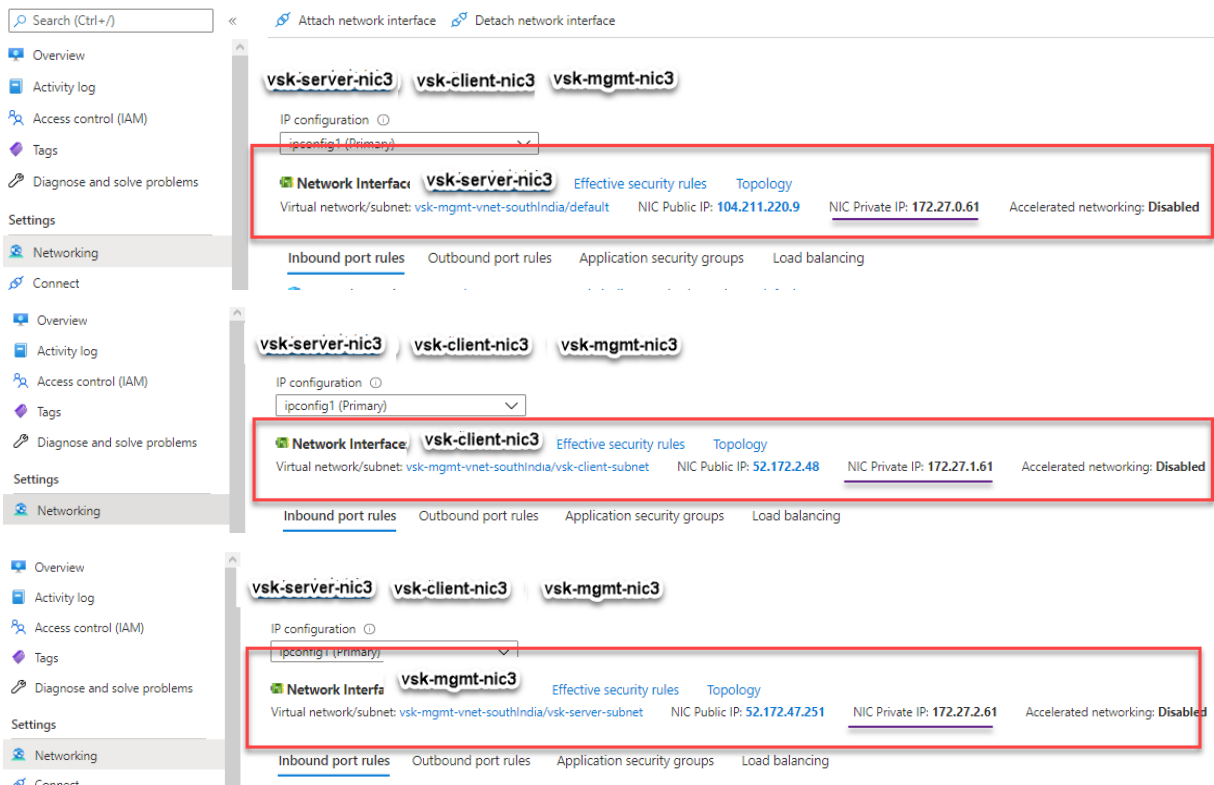
1  <NS-PRE-BOOT-CONFIG>
2
3  <NS-CONFIG>
4
5      set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
6      add route 0.0.0.0 0.0.0.0 172.27.2.1
7      set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
8      add ns ip 172.27.0.61 255.255.255.0 -type SNIP
9      add route 169.254.169.254 255.255.255.255 172.27.0.1
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     </NS-CONFIG>
20
21     <NS-BOOTSTRAP>
22
23     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26     </NS-BOOTSTRAP>
27
28     </NS-PRE-BOOT-CONFIG>

```

Puede ver que la instancia NetScaler VPX se crea con tres interfaces de red. Vaya al **portal de Azure > Instancia de VM > Redes** y compruebe las propiedades de red de las tres NIC como se muestra en las ilustraciones siguientes.



Puede ejecutar el comando “show nsip” en la CLI de ADC y comprobar que se aplica la nueva secuencia de arranque especificada en la sección <code>NS-BOOTSTRAP</code>. Puede ejecutar el comando “show route” para verificar la máscara de subred.

```

> sh ns ip
-----
Ipaddress      Traffic Domain  Type           Mode   Arp   Icmp   Vserver   State
-----
1) 172.27.2.61   0               NetScaler IP   Active Enabled Enabled NA        Enabled
2) 172.27.0.61   0               SNIP           Active Enabled Enabled NA        Enabled
3) 4.0.0.101     0               VIP            Active Enabled Enabled Enabled  Enabled
Done
> sh vlan
1) VLAN ID: 1
   Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
   Interfaces : 0/1 1/1 LO/1
2) VLAN ID: 5   VLAN Alias Name:
3) VLAN ID: 10  VLAN Alias Name:
   Interfaces : 1/2
   IPs :
     172.27.2.61      Mask: 255.255.255.0
Done
> sh route
-----
Network      Netmask      Gateway/OwnedIP  VLAN  State  Traffic Domain  Type
-----
1) 0.0.0.0    0.0.0.0      172.27.2.1      0     UP     0               STATIC
2) 127.0.0.0  255.0.0.0    127.0.0.1      0     UP     0               PERMANENT
3) 172.27.0.0 255.255.255.0 172.27.0.61    0     UP     0               DIRECT
4) 172.27.2.0 255.255.255.0 172.27.2.61    0     UP     0               DIRECT
5) 169.254.0.0 255.255.0.0  172.27.0.1     0     UP     0               STATIC
6) 168.63.129.16 255.255.255.255 172.27.0.1    0     UP     0               STATIC
7) 169.254.169.254 255.255.255.255 172.27.0.1    0     UP     0               STATIC
Done

```

Ejemplo de bootstrap personalizado para GCP

En este ejemplo, los comandos relacionados con bootstrap se proporcionan en la sección `<NS-CONFIG>`. La sección `<NS-BOOTSTRAP>` indica que se omita el bootstrapping predefinido y se aplica la información de arranque personalizada proporcionada en la sección `<NS-CONFIG>`.


```

<NS-PRE-BOOT-CONFIG>

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

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

  </NS-CONFIG>

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

</NS-PRE-BOOT-CONFIG>

```

Puede copiar la configuración que se muestra en la captura de pantalla anterior desde aquí:

```

1  <NS-PRE-BOOT-CONFIG>
2
3  <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 -
12         maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
13         YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
14         NO -CMP NO
15     add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
16         persistenceType NONE -cltTimeout 180
17
18 </NS-CONFIG>
19
20 <NS-BOOTSTRAP>
21     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
22     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
23 </NS-BOOTSTRAP>
24
25 </NS-PRE-BOOT-CONFIG>

```

Una vez creada la instancia de VM en el portal de GCP con el bootstrap personalizado, puede verificar las propiedades de la interfaz de red de la siguiente manera:

1. Seleccione la instancia que ha creado proporcionando la información de arranque personalizada.
2. Desplácese hasta las propiedades de la interfaz de red y compruebe los detalles de la NIC como se muestra en la ilustración.

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)	

Puede ejecutar el `show ns ip` comando en la **CLI de ADC** verificar que las configuraciones proporcionadas en la `<NS-CONFIG>` sección anterior se apliquen en el primer arranque del dispositivo ADC.

```
> sh ns ip
-----
Ipaddress      Traffic Domain  Type
-----
1) 10.128.0.2    0               NetScaler IP
2) 4.0.0.101    0               VIP
Done
> sh vlan
1) VLAN ID: 1
   Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
   Interfaces : 0/1 1/2 LO/1
2) VLAN ID: 10   VLAN Alias Name:
   Interfaces : 1/1
   IPs :
      10.128.0.2      Mask: 255.255.255.0
Done
> sh route
-----
Network      Netmask      Gateway/OwnedIP  VLAN  State  Traffic Domain  Type
-----
1) 0.0.0.0    0.0.0.0     10.128.0.1      0     UP     0               STATIC
2) 127.0.0.0  255.0.0.0   127.0.0.1      0     UP     0               PERMANENT
3) 10.128.0.0 255.255.255.0 10.128.0.2     0     UP     0               DIRECT
Done
```

Impacto de adjuntar y separar NIC en AWS y Azure

AWS y Azure ofrecen la opción de adjuntar una interfaz de red a una instancia y separar una interfaz de red de una instancia. La conexión o desconexión de interfaces podría alterar las posiciones de la interfaz. Por lo tanto, Citrix recomienda que se abstenga de separar las interfaces de la instancia de NetScaler VPX. Si desconecta o adjunta una interfaz cuando está configurado el arranque personalizado, la instancia de NetScaler VPX reasigna la IP principal de la interfaz recién disponible en la posición de la interfaz de administración como NSIP. Si no hay más interfaces disponibles después de la que ha desconectado, la primera interfaz se convierte en la interfaz de administración de la instancia de NetScaler VPX.

Por ejemplo, una instancia de NetScaler VPX se abre con 3 interfaces: Eth0 (SNIP), Eth1 (NSIP) y Eth2 (VIP). Si desactiva la interfaz Eth1 de la instancia, que es una interfaz de administración, ADC configura la siguiente interfaz disponible (Eth2) como interfaz de administración. De este modo, se sigue accediendo a la instancia de NetScaler VPX a través de la IP principal de la interfaz Eth2. Si Eth2 tampoco está disponible, la interfaz restante (Eth0) se hace la interfaz de administración. Por lo tanto, el acceso a la instancia de NetScaler VPX sigue existiendo.

Consideremos una asignación diferente de interfaces de la siguiente manera: Eth0 (SNIP), Eth1 (VIP) y Eth2 (NSIP). Si desactiva Eth2 (NSIP), porque no hay nueva interfaz disponible después de Eth2, la primera interfaz (Eth0) se transforma en la interfaz de administración.

Mejore el rendimiento de SSL-TPS en plataformas de nube pública

October 17, 2024

Puede obtener un mejor rendimiento de SSL-TPS en las nubes de AWS y GCP si distribuye los pesos del motor de paquetes (PE) por igual. La activación de esta función puede provocar una ligera caída en el rendimiento de HTTP de entre un 10 y un 12%.

En las nubes de AWS y GCP, las instancias de NetScaler VPX con 10 a 16 vCPU no muestran ninguna mejora en el rendimiento porque los pesos de PE se distribuyen por igual de forma predeterminada.

Nota:

En la nube de Azure, los pesos de PE se distribuyen equitativamente de forma predeterminada. Esta función no mejora el rendimiento de las instancias de Azure.

Configurar el modo PE mediante la CLI de NetScaler

Después de configurar el modo PE, debe reiniciar el sistema para que los cambios de configuración surtan efecto.

En el símbolo del sistema, escriba:

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

Cuando el modo PE se establece en CPUBOUND, las ponderaciones PE se distribuyen equitativamente. Cuando el modo PE se establece en DEFAULT, las ponderaciones PE se establecen en los valores predeterminados.

Nota:

Este comando es específico del nodo. En una configuración de clúster o de alta disponibilidad,

debe ejecutar el comando en cada nodo. Si ejecuta el comando en CLIP, se produce el siguiente error: `Operación no permitida en CLIP`

Para mostrar el estado del modo PE configurado, ejecute el siguiente comando:

```
1 show cpuparam
```

Ejemplo

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

Aplicar la configuración del modo PE en el primer arranque del dispositivo NetScaler en la nube

Para aplicar la configuración del modo PE en el primer arranque del dispositivo NetScaler en la nube, debe crear un archivo `/nsconfig/.cpubound.conf` mediante el script personalizado. Para obtener más información, consulte [Aplicar configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en la nube](#).

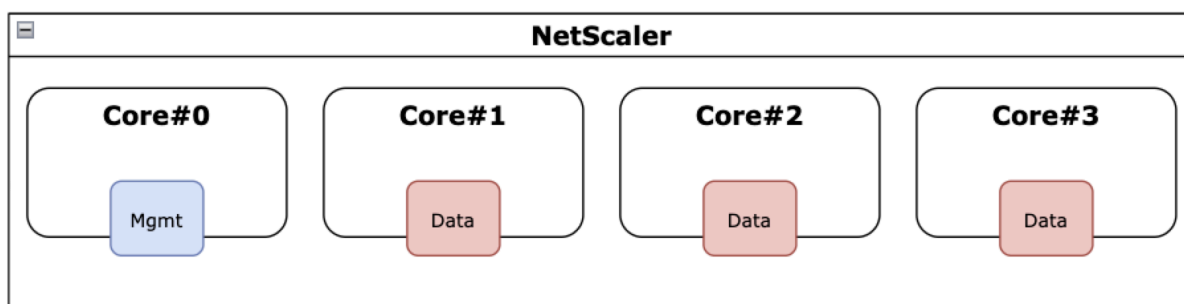
Configurar subprocesos múltiples simultáneos para NetScaler VPX en nubes públicas

October 17, 2024

NetScaler utiliza diferentes núcleos dedicados para sus funciones de administración y plano de datos. Por lo general, se asigna un núcleo a las funciones del plano de administración. El resto de los núcleos disponibles se asignan a funciones del plano de datos.

La siguiente imagen muestra una ilustración simplificada de un NetScaler VPX de 4 núcleos.

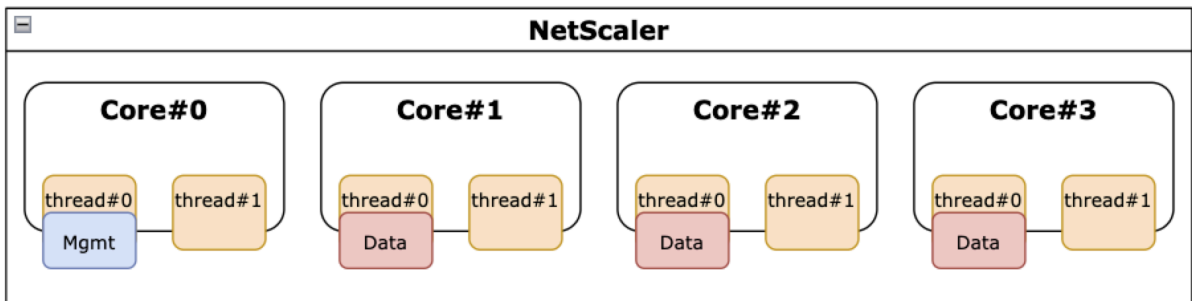
Ilustración 1. Carga de trabajo del plano de datos y administración de NetScaler en un sistema de 4 núcleos



Si bien la imagen anterior muestra la distribución de las funciones de NetScaler en los núcleos disponibles, no es necesariamente una representación precisa del hardware subyacente. La mayoría de las CPU x86 modernas proporcionan dos núcleos lógicos por núcleo físico, mediante funciones conocidas comercialmente como Intel Hyperthreading (HT) o multiproceso simultáneo (SMT) de AMD.

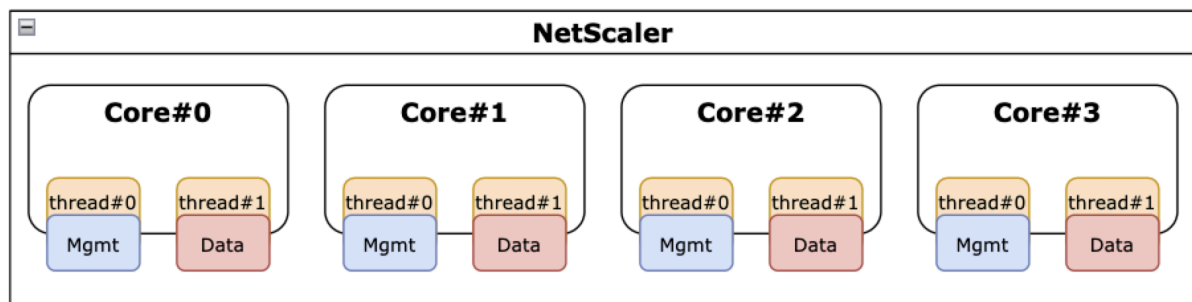
La siguiente imagen muestra NetScaler VPX ejecutándose en una CPU moderna con SMT desactivado. Cada núcleo de la CPU se divide en dos o más CPU lógicas, denominadas comúnmente subprocesos. Cada subproceso tiene su propio conjunto de recursos replicados, una parte de los recursos particionados y compite por los recursos compartidos con sus subprocesos hermanos.

Figura 2. Carga de trabajo del plano de datos y administración de NetScaler en un sistema de 4 núcleos y 8 subprocesos con SMT desactivado



La siguiente imagen muestra NetScaler VPX ejecutándose en una CPU moderna con SMT habilitado.

Figura 3 . Carga de trabajo del plano de datos y administración de NetScaler en un sistema de 4 núcleos con SMT habilitado



La activación de SMT mejora el rendimiento de NetScaler al:

- Ejecución de funciones de plano de datos en todos los núcleos físicos.
- Mover las funciones del plano de administración al subproceso hermano.
- Introducir un mecanismo flexible de límite de recursos para evitar que las funciones del plano de administración comprometan el rendimiento de las funciones del plano de datos.

Matriz de soporte SMT

En la tabla siguiente se enumeran las plataformas VPX, los tipos de instancias en la nube y las versiones de NetScaler que admiten SMT.

Plataforma VPX	Tipos de instancias	Versión de NetScaler VPX
AWS	M5, m5 n, c5, c5 n	14.1-12.x y versiones posteriores
Azure	Cualquier familia de instancias con hiperprocesamiento, por ejemplo, DS_v4	14.1-12.x y versiones posteriores
GCP	instancias e2	14.1-12.x y versiones posteriores

Nota:

Al habilitar la función SMT, el rendimiento de NetScaler VPX aumenta en los tipos compatibles.

Limitaciones

La función SMT duplica de manera efectiva las CPU virtuales disponibles para un dispositivo NetScaler. Se deben tener en cuenta los límites de licencia para permitir que el dispositivo NetScaler los utilice.

Por ejemplo, considere el NetScaler VPX ilustrado en la figura 3. Si se utiliza una licencia basada en el rendimiento, se requiere una licencia de 10 Gbps o superior con la función SMT para habilitar 8 vCPU. Anteriormente, una licencia de 1 Gbps era suficiente para habilitar 4 vCPU. Si se utiliza una licencia de vCPU, NetScaler VPX debe configurarse para que las licencias tengan el doble de vCPU para que funcione correctamente. Póngase en contacto con el soporte técnico de NetScaler para obtener más información sobre este tema.

Configurar SMT

Antes de habilitar la función SMT, asegúrese de que su plataforma admite esta función. Consulte la tabla de matrices de soporte en la sección anterior.

Para habilitar la función SMT, sigue estos pasos:

1. Cree un archivo vacío con el nombre `.smt_handling` del directorio `«/nsconfig»`.
2. Guarde la configuración actual.
3. Reinicie la instancia de NetScaler VPX.

```
1 nscli> shell touch /nsconfig/.smt_handling
2 Done
3 nscli> reboot
4 Are you sure you want to restart NetScaler (Y/N)? [N]:Y
5 Done
```

4. Tras reiniciar, NetScaler indica que la función está disponible y habilitada.

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

Para deshabilitar la función SMT, sigue estos pasos:

1. Elimine el archivo `.smt_handling`.
2. Reinicie la instancia de NetScaler VPX.

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

3. Tras reiniciar, NetScaler indica que la función está disponible pero deshabilitada.

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

Solución de problemas

Ejecute el comando shell `sysctl` para verificar el estado de la función SMT.

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

El comando puede devolver cualquiera de las siguientes salidas.

- Falta la función SMT.

El comando `sysctl` no devuelve ningún resultado.

- No se admite la función SMT.

La función SMT no es compatible por alguno de los siguientes motivos:

- Su NetScaler VPX tiene más de 13.1-48.x o 14.1-12.x.
- Su nube no admite SMT.

- El tipo de instancia de VM no admite SMT; por ejemplo, el número de vCPU es superior a 8.

```
1 > shell sysctl -a | grep smt_handling
2 netcaler.smt_handling_platform: 0(indicates not supported)
3 netcaler.smt_handling: 0 (indicates not enabled)
4 netcaler.smt_handling_active: 0 (indicates not active)
```

- La función SMT es compatible pero no está habilitada.

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

Instalar una instancia de NetScaler VPX en un servidor desnudo

October 17, 2024

Un bare metal es un servidor físico totalmente dedicado que ofrece aislamiento físico, totalmente integrado en el entorno de nube. También se conoce como servidor de un solo arrendatario. El arrendamiento único le permite evitar el efecto vecino ruidoso. Con solo metal, no sufrirá el efecto del “vecino ruidoso” porque será el único usuario.

Un servidor desnudo instalado con un hipervisor proporciona un conjunto de administración para crear máquinas virtuales en el servidor. El hipervisor no ejecuta aplicaciones de forma nativa. Su propósito es virtualizar sus cargas de trabajo en máquinas virtuales independientes para obtener la flexibilidad y fiabilidad de la virtualización.

Requisitos previos para instalar la instancia NetScaler VPX en servidores básicos

Se debe obtener un servidor desnudo de un proveedor de nube que cumpla con todos los requisitos del sistema para el hipervisor respectivo.

Instalación de la instancia de NetScaler VPX en servidores básicos

Para instalar instancias de NetScaler VPX en un servidor básico, primero debe obtener un servidor básico con los recursos de sistema adecuados de un proveedor de nube. En ese servidor básico, se debe instalar y configurar cualquiera de los hipervisores compatibles, como Linux KVM, VMware ESX, Citrix Hypervisor o Microsoft Hyper-V, antes de implementar la instancia de NetScaler VPX.

Para obtener más información sobre la lista de diferentes hipervisores y funciones compatibles con una instancia de NetScaler VPX, consulte [Matriz de soporte y pautas de uso](#).

Para obtener más información sobre la instalación de instancias de NetScaler VPX en diferentes hipervisores, consulte la documentación correspondiente.

- **Citrix Hypervisor:** Consulte [Instalar una instancia de NetScaler VPX en Citrix Hypervisor](#).
- **VMware ESX:** Consulte [Instalar una instancia de NetScaler VPX en VMware ESX](#).
- **Microsoft Hyper-V:** Consulte [Instalar una instancia de NetScaler VPX en el servidor Microsoft Hyper-V](#).
- **Plataforma Linux KVM:** Consulte [Instalar una instancia de NetScaler VPX en la plataforma Linux-KVM](#).

Instalar una instancia de NetScaler VPX en Citrix Hypervisor

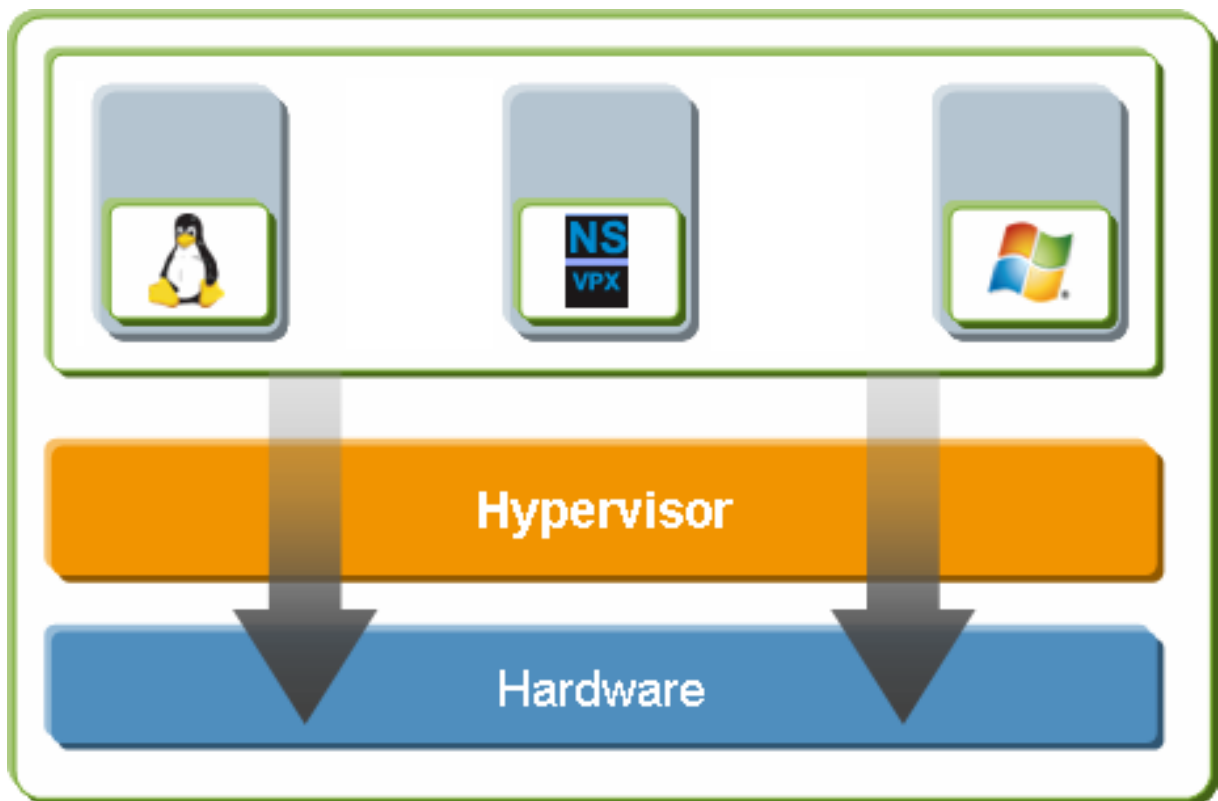
October 17, 2024

Para instalar instancias VPX en Citrix Hypervisor, primero debe instalar el Hypervisor en un equipo con los recursos del sistema adecuados. Para realizar la instalación de la instancia de NetScaler VPX, utilice Citrix XenCenter, que debe instalarse en un equipo remoto que pueda conectarse al host del hipervisor a través de la red.

Para obtener más información sobre Hypervisor, consulte la [documentación de Citrix Hypervisor](#).

En la siguiente ilustración se muestra la arquitectura de soluciones sin usar de la instancia de NetScaler VPX en Hypervisor.

Figura . Una instancia de NetScaler VPX en Citrix Hypervisor



Requisitos previos para instalar una instancia de NetScaler VPX en Hypervisor

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Instale Hypervisor versión 6.0 o posterior en hardware que cumpla los requisitos mínimos.
- Instale XenCenter en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Obtenga archivos de licencia de dispositivo virtual. Para obtener más información sobre las licencias de dispositivos virtuales, consulte la [Guía de licencias de NetScaler](#).

Requisitos de hardware de hiper

En la tabla siguiente se describen los requisitos mínimos de hardware para una plataforma Hypervisor que ejecuta una instancia NetScaler VPX.

Tabla 1. Requisitos mínimos del sistema para el hipervisor que ejecuta una instancia de nCore VPX

Componente	Requisito
CPU	2 o más CPU x86 de 64 bits con asistencia de virtualización (Intel-VT) habilitada. Para ejecutar la instancia NetScaler VPX, la compatibilidad de hardware para la virtualización debe estar habilitada en el host del hipervisor. Asegúrese de que la opción del BIOS para la compatibilidad con la virtualización no esté inhabilitada. Para obtener más información, consulte la documentación del BIOS.
RAM	3 GB
Espacio en disco	Almacenamiento conectado localmente (PATA, SATA, SCSI) con 40 GB de espacio en disco. Nota: La instalación del hipervisor crea una partición de 4 GB para el dominio de control de host del hipervisor. El espacio restante está disponible para la instancia NetScaler VPX y otras máquinas virtuales.
NIC	Una NIC de 1 Gbps; recomendada: dos NIC de 1 Gbps

Para obtener información sobre la instalación de Hypervisor, consulte la documentación del hipervisor en <http://support.citrix.com/product/xens/>.

En la tabla siguiente se enumeran los recursos informáticos virtuales que debe proporcionar Hypervisor para cada dispositivo virtual nCore VPX.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de nCore VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	2

Nota:

Para el uso en producción de la instancia NetScaler VPX, Citrix recomienda establecer la prior-

idad de la CPU (en las propiedades de la máquina virtual) en el nivel más alto para mejorar el comportamiento de la programación y la latencia de la red.

requisitos del sistema de XenCenter

XenCenter es una aplicación cliente de Windows. No se puede ejecutar en el mismo equipo que el host del hipervisor. Para obtener más información sobre los requisitos mínimos del sistema y la instalación de XenCenter, consulte los siguientes documentos del hipervisor:

- [Requisitos del sistema](#)
- [Instalación](#)

Instalar instancias NetScaler VPX en Hypervisor mediante XenCenter

Después de instalar y configurar Hypervisor y XenCenter, puede usar XenCenter para instalar dispositivos virtuales en Hypervisor. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el hardware que ejecuta Hypervisor.

Para instalar instancias de NetScaler VPX en Hypervisor mediante XenCenter, siga estos pasos:

1. Inicie **XenCenter** en su estación de trabajo.
2. En el menú **Servidor**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar nuevo servidor**, en el cuadro de texto del nombre del host, escriba la dirección IP o el nombre DNS del hipervisor al que quiere conectarse.
4. En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en **Conectar**. El nombre del hipervisor aparece en el panel de navegación con un círculo verde, lo que indica que el hipervisor está conectado.
5. En el panel de navegación, haga clic en el nombre del hipervisor en el que quiere instalar la instancia NetScaler VPX.
6. En el menú **VM**, haga clic en **Importar**.
7. En el cuadro de diálogo **Importar**, en el nombre del archivo de importación, busque la ubicación en la que guardó el archivo de imagen `.xva` de la instancia de NetScaler VPX. Asegúrese de que la opción VM exportada esté seleccionada y, a continuación, haga clic en **Siguiente**.
8. Seleccione el hipervisor en el que desee instalar el dispositivo virtual y, a continuación, haga clic en **Siguiente**.
9. Seleccione el repositorio de almacenamiento local en el que desea almacenar el dispositivo virtual y, a continuación, haga clic en **Importar** para iniciar el proceso de importación.

10. Puede agregar, modificar o eliminar las interfaces de red virtual según sea necesario. Cuando haya terminado, haga clic en **Siguiente**.

11. Haga clic en **Finalizar** para completar el proceso de importación.

Nota:

Para ver el estado del proceso de importación, haga clic en la ficha **Registro**.

12. Si quiere instalar otro dispositivo virtual, repita los pasos 5 a 11.

Nota:

Tras la configuración inicial de la instancia VPX, si quiere actualizar el dispositivo a la última versión de software, consulte [Actualización o degradación del software del sistema](#).

Configurar instancias VPX para que usen interfaces de red de virtualización de E/S de raíz única (SR-IOV)

October 17, 2024

Tras instalar y configurar una instancia de NetScaler VPX en Citrix Hypervisor, puede configurar el dispositivo virtual para que utilice las interfaces de red SR-IOV.

Se admiten las siguientes NIC:

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

Limitaciones

Citrix Hypervisor no admite algunas funciones de las interfaces SR-IOV. Las limitaciones de las NIC Intel 82599, Intel X710 e Intel XL710 se enumeran en las siguientes secciones.

Limitaciones de la NIC Intel 82599

La NIC Intel 82599 no admite las siguientes funciones:

- Conmutación del modo L2
- Agrupar en clústeres

- Particionado de administrador [modo VLAN compartida]
- Alta disponibilidad [Activo - modo activo]
- Marcos gigantes
- Protocolo IPv6 en el entorno de clúster

Limitaciones de las NIC Intel X710 10G e Intel XL710 40G

Las NIC Intel X710 10G e Intel XL710 40G tienen las siguientes limitaciones:

- No se admite la conmutación de modo L2.
- No se admite la partición de administrador (modo VLAN compartida).
- En un clúster, las tramas jumbo no se admiten cuando se utiliza la NIC XL710 como interfaz de datos.
- La lista de interfaces se reordena cuando las interfaces se desconectan y se vuelven a conectar.
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.
- Para las NIC Intel X710 10G e Intel XL710 40G, la interfaz aparece como una interfaz 40/x.
- Solo se admiten hasta 16 interfaces SR-IOV Intel X710/XL710 en una instancia VPX.

Nota:

Para que las NIC Intel X710 10G e Intel XL710 40G admitan IPv6, habilite el modo de confianza en las funciones virtuales (VF) escribiendo el siguiente comando en el host de Citrix Hypervisor:

```
# ip link set <PNIC> <VF> trust on
```

Ejemplo

```
# ip link set ens785f1 vf 0 trust on
```

Requisitos previos para la NIC Intel 82599

En el host de Citrix Hypervisor, asegúrese de:

- Agregue la NIC (NIC) Intel 82599 al host.
- Bloquear la lista del controlador `ixgbev` agregando la siguiente entrada al archivo `/etc/modprobe.d/blacklist.conf`:

lista de prohibidos `ixgbev`

- Habilite las funciones virtuales (VF) de SR-IOV agregando la siguiente entrada al archivo `/etc/modprobe.d/ixgbe`:

```
options ixgbe max_vfs=<number_of_VFs>
```

donde `<number_VFs>` es el número de VF SR-IOV que quiere crear.

- Compruebe que SR-IOV esté habilitado en el BIOS.

Nota:

Se recomienda el controlador IXGBE versión 3.22.3.

Asigne los VF Intel 82599 SR-IOV a la instancia de NetScaler VPX mediante el host Citrix Hypervisor

Para asignar una VF Intel 82599 SR-IOV a una instancia de NetScaler VPX, siga estos pasos:

1. En el host de Citrix Hypervisor, utilice el siguiente comando para asignar los VF SR-IOV a la instancia de 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>*
```

Donde:

- ****** <Xen host UUID> es el UUID del host de Citrix Hypervisor.
- <NetScaler VM UUID> es el UUID de la instancia NetScaler VPX.
- <interface name> es la interfaz para las VF de SR-IOV.
- <MAC address> es la dirección MAC del SR-IOV VF.

Nota:

Especifique la dirección MAC que quiere utilizar en el parámetro args: Mac=; si no se especifica, el script `iovirt` genera aleatoriamente y asigna una dirección MAC. Además, si quiere utilizar los VF SR-IOV en modo de agregación de enlaces, asegúrese de especificar la dirección MAC como 00:00:00:00:00:00.

2. Arranque la instancia de NetScaler VPX.

Desasigne los VF Intel 82599 SR-IOV a la instancia de NetScaler VPX mediante el host Citrix Hypervisor

Si ha asignado un VF SR-IOV incorrecto o si quiere modificar un VF SR-IOV asignado, debe anular la asignación y reasignar los VF SR-IOV a la instancia NetScaler VPX.

Para anular la asignación de la interfaz de red SR-IOV asignada a una instancia de NetScaler VPX, siga estos pasos:

1. En el host de Citrix Hypervisor, utilice el siguiente comando para asignar los VF SR-IOV a la instancia de NetScaler VPX y reiniciar la instancia de NetScaler VPX:

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

Donde:

- <Xen_host_UUID>: El UUID del host de Citrix Hypervisor.
- <Netscaler_VM_UUID>: El UUID de la instancia de NetScaler VPX

2. Arranque la instancia de NetScaler VPX.

Asigne los VF Intel X710/XL710 SR-IOV a la instancia de NetScaler VPX mediante el host Citrix Hypervisor

Para asignar un VF Intel X710/XL710 SR-IOV a la instancia de NetScaler VPX, siga estos pasos:

1. Ejecute el siguiente comando en el host de Citrix Hypervisor para crear una red.

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

Ejemplo

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

2. Determine el identificador único universal (UUID) de PIF de la NIC en la que se va a configurar la red SR-IOV.

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

3. Configure la red como una red SR-IOV. El siguiente comando también devuelve el UUID de la red SR-IOV recién creada:

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

Ejemplo

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


Para obtener más información sobre los parámetros de red SR-IOV, ejecute el siguiente comando:

```
1 [root@citrix-XS82-TOP0 ~]# xe network-sriov-param-list uuid=1629
   b44f-832a-084e-d67d-5d6d314d5e0f
2
3         uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f
4         physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783
5         logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff
6         requires-reboot ( RO): false
7         remaining-capacity ( RO): 32
```

4. Cree una interfaz virtual (VIF) y conéctela a la máquina virtual de destino.

```
1 xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-uuid=8
   ee59b73-7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-f5ca-18
   eb-561d-308218a9dd68
2 3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
```

Nota:

El número de índice NIC de la máquina virtual debe empezar por 0.

Use el siguiente comando para encontrar el UUID de VM:

```
1 [root@citrix-XS82-TOP0 ~]# xe vm-list
2 uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68
3 name-label ( RW): sai-vpx-1
4 power-state ( RO): halted
```

Elimine los VF Intel X710/XL710 SR-IOV de la instancia de NetScaler mediante el host Citrix Hypervisor

Para eliminar un VF Intel X710/XL710 SR-IOV de una instancia de NetScaler VPX, siga estos pasos:

1. Copie el UUID del VIF que quiere destruir.
2. Ejecute el siguiente comando en el host de Citrix Hypervisor para destruir el VIF.

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

Ejemplo

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

Configurar la agregación de enlaces en la interfaz SR-IOV

Para utilizar las funciones virtuales (VF) de SR-IOV en el modo de agregación de enlaces, debe inhabilitar la verificación falsa de las funciones virtuales que haya creado.

En el host de Citrix Hypervisor, utilice el siguiente comando para inhabilitar la verificación de suplantación de identidad:

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

Donde:

- <interface_name> es el nombre de la interfaz.
- <VF_id> es el identificador de función virtual.

Tras inhabilitar la verificación falsa de todas las funciones virtuales que ha creado, reinicie la instancia de NetScaler VPX y configure la agregación de enlaces. Para obtener instrucciones, consulte [Configurar la agregación de enlaces](#).

Importante:

Mientras asigna las VF de SR-IOV a la instancia de NetScaler VPX, asegúrese de especificar la dirección MAC 00:00:00:00:00:00 para las VF.

Configurar VLAN en la interfaz SR-IOV

Puede configurar la VLAN en las funciones virtuales del SR-IOV. Para obtener instrucciones, consulte [Configuración de una VLAN](#).

Importante:

Asegúrese de que el host de Citrix Hypervisor no contenga la configuración de VLAN para la interfaz VF.

Instalación de una instancia de NetScaler VPX en VMware ESX

October 17, 2024

Antes de instalar instancias de NetScaler VPX en VMware ESX, asegúrese de que VMware ESX Server esté instalado en una máquina con los recursos del sistema adecuados. Para instalar una instancia de NetScaler VPX en VMware ESXi, utilice el cliente VMware vSphere. El cliente o la herramienta deben estar instalados en un equipo remoto que pueda conectarse a VMware ESX a través de la red.

En esta sección se incluyen los temas siguientes:

- Requisitos previos
- Instalación de una instancia de NetScaler VPX en VMware ESX

Importante:

No puede instalar VMware Tools estándar ni actualizar la versión de VMware Tools disponible en una instancia de NetScaler VPX. VMware Tools para una instancia de NetScaler VPX se suministra como parte de la versión del software NetScaler.

Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Instale VMware ESX en un hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree un conmutador virtual y conecte la NIC física al conmutador virtual.
- Agregue el grupo de puertos y conéctelo al conmutador virtual.
- Adjunte el grupo de puertos a la máquina virtual.
- Obtenga archivos de licencias VPX. Para obtener más información sobre las licencias de instancia de NetScaler VPX, consulte [Descripción general de las licencias](#).

Requisitos de hardware de VMware ESX

En la tabla siguiente se describen los requisitos mínimos del sistema para los servidores de VMware ESX que ejecutan el dispositivo virtual NetScaler VPX nCore.

Tabla 2. Requisitos mínimos del sistema para un servidor VMware ESX que ejecuta una instancia NetScaler VPX

Componente	Requisito
CPU	2 o más CPU x86 de 64 bits con asistencia de virtualización (Intel-VT) habilitada. Para ejecutar una instancia de NetScaler VPX, la compatibilidad de hardware para la virtualización debe estar habilitada en el host VMware ESX. Asegúrese de que la opción BIOS para la función de virtualización no esté inhabilitada. Para obtener más información, consulte la documentación del BIOS. A partir de la versión 13.1 de NetScaler, la instancia de NetScaler VPX en el hipervisor VMware ESXi admite procesadores AMD.
RAM	2 GB VPX. Para implementaciones críticas, no recomendamos 2 GB de RAM para VPX porque el sistema funciona en un entorno con restricciones de memoria. Esto puede provocar problemas relacionados con la escala, el rendimiento o la estabilidad. Se recomiendan 4 GB de RAM u 8 GB de RAM.
Espacio en disco	20 GB más que los requisitos mínimos de servidor de VMware para configurar ESXi. Consulte la documentación de VMware para conocer los requisitos mínimos del servidor.
Red	Una NIC (NIC) de 1 Gbps; se recomiendan dos NIC de 1 Gbps

Para obtener información acerca de la instalación de VMware ESX, consulte <http://www.vmware.com/>.

Para la interfaz de red SR-IOV o la compatibilidad con la transferencia PCI, asegúrese de que estén habilitados los siguientes procesadores y configuraciones:

- Procesadores Intel compatibles con Intel-VT
- Procesadores AMD compatibles con AMD-V
- La unidad de administración de memoria de E/S (IOMMU) o SR-IOV está habilitada en la BIOS

El modo SR-IOV admite las siguientes NIC:

- NIC Mellanox ConnectX-4, a partir de la versión 13.1-42.x de NetScaler

- NIC Intel 82599

En la tabla siguiente se enumeran los recursos informáticos virtuales que el servidor de VMware ESX debe proporcionar para cada dispositivo virtual VPX nCore.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de NetScaler VPX

Componente	Requisito
Memoria	4 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En ESX, puede instalar un máximo de 10 interfaces de red virtuales si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

Nota:

Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso de producción del dispositivo virtual VPX, se debe reservar la asignación de memoria completa. Los ciclos de CPU (en MHz) iguales al menos a la velocidad de un núcleo de CPU del ESX deben reservarse.

Requisitos del sistema cliente de VMware vSphere

VMware vSphere es una aplicación cliente que se puede ejecutar en sistemas operativos Windows y Linux. No se puede ejecutar en la misma máquina que el servidor VMware ESX. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 3. Requisitos mínimos del sistema para la instalación del cliente de VMware vSphere

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Tablas de compatibilidad de vSphere” en http://kb.vmware.com/ .
CPU	750 MHz; se recomienda 1 gigahercio (GHz) o más rápido
RAM	1 GB. Se recomiendan 2 GB
NIC (NIC)	NIC de 100 Mbps o más rápido

Componente	Requisito
------------	-----------

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. No se puede ejecutar en la misma máquina que el servidor VMware ESX. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 4. Requisitos mínimos del sistema para la instalación de herramientas OVF

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Guía del usuario de herramientas OVF” en http://kb.vmware.com/ .
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC (NIC)	NIC de 100 Mbps o más rápido

Para obtener información sobre la instalación de OVF, busque el archivo PDF “Guía del usuario de la herramienta OVF” en <http://kb.vmware.com/>.

Descarga de los archivos de configuración de NetScaler VPX

El paquete de configuración de instancias NetScaler VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página principal en <http://www.citrix.com>, haga clic en el **enlace Nuevos usuarios** y siga las instrucciones para crear una cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

Citrix.com > **Descargas > NetScaler > Dispositivos virtuales.**

Copie los siguientes archivos en una estación de trabajo de la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (por ejemplo, NSVPX-ESX-13.0-71.44_nc_64.mf)

Instalación de una instancia de NetScaler VPX en VMware ESX

Una vez instalado y configurado VMware ESX, puede utilizar el cliente de VMware vSphere para instalar dispositivos virtuales en el servidor VMware ESX. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el hardware que ejecuta VMware ESX.

Para instalar instancias NetScaler VPX en VMware ESX mediante VMware vSphere Client, siga estos pasos:

1. Inicie el cliente de VMware vSphere en su estación de trabajo.
2. En el cuadro de texto **Dirección IP/Nombre**, escriba la dirección IP del servidor VMware ESX al que quiere conectarse.
3. En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en Iniciar sesión.
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla de OVF**, en **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias de NetScaler VPX, seleccione el archivo .ovf y haga clic en **Siguiente**.
6. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el host ESX. Haga clic en **Siguiente** para comenzar a instalar un dispositivo virtual en VMware ESX. Una vez finalizada la instalación, una ventana emergente le informa de que la instalación se ha realizado correctamente.
7. Ya está listo para iniciar la instancia de NetScaler VPX. En el panel de navegación, seleccione la instancia de NetScaler VPX que ha instalado y, **en el menú contextual, seleccione Encender**.
8. Después de arrancar la máquina virtual, desde la consola, configure las direcciones IP, Netmask y Gateway de NetScaler. Cuando complete la configuración, seleccione la opción **Guardar y salir** en la consola.
9. Para instalar otro dispositivo virtual, repita el proceso desde el paso 6 hasta el paso 8.

Nota:

De forma predeterminada, la instancia de NetScaler VPX utiliza interfaces de red E1000.

Tras la instalación, puede utilizar el cliente vSphere o vSphere Web Client para administrar los dispositivos virtuales en VMware ESX.

Para habilitar el etiquetado de VLAN en VMware ESX, configure el ID de VLAN del grupo de puertos

en Todos (4095) en el vSwitch. Para obtener instrucciones detalladas sobre cómo configurar una ID de VLAN en el vSwitch, consulte la documentación de VMware.

Migrar una instancia de NetScaler VPX mediante VMware vMotion

Puede migrar una instancia de NetScaler VPX mediante VMware vSphere vMotion.

Siga estas pautas de uso:

- VMware no admite la función vMotion en máquinas virtuales configuradas con interfaces PCI Passthrough y SR-IOV.
- Las interfaces compatibles son E1000 y VMXNET3. Para utilizar vMotion en la instancia VPX, asegúrese de que la instancia esté configurada con una interfaz compatible.
- Para obtener más información sobre cómo migrar una instancia mediante VMware vMotion, consulte la documentación de VMware.

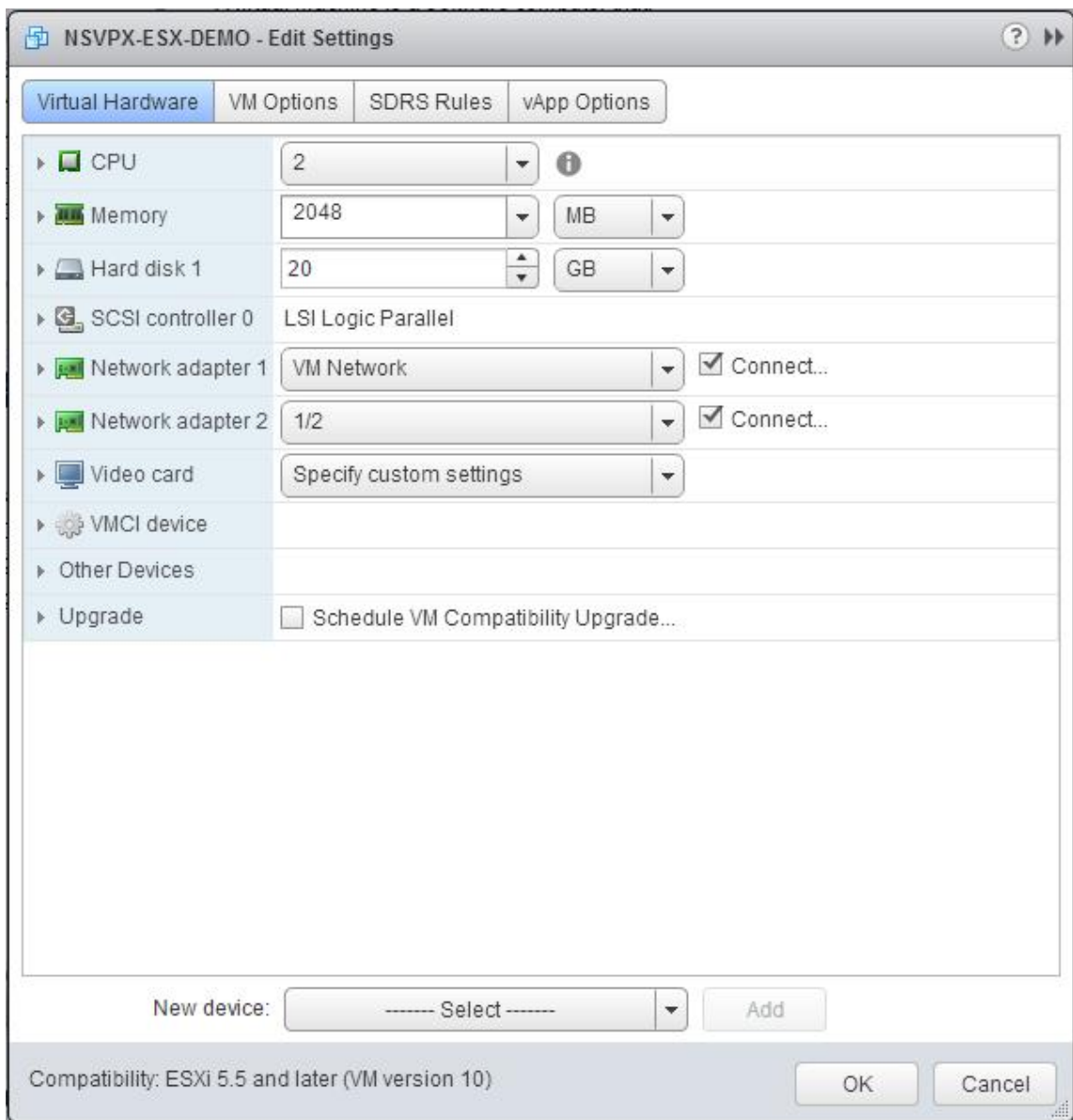
Configurar una instancia de NetScaler VPX para usar la interfaz de red VMXNET3

October 17, 2024

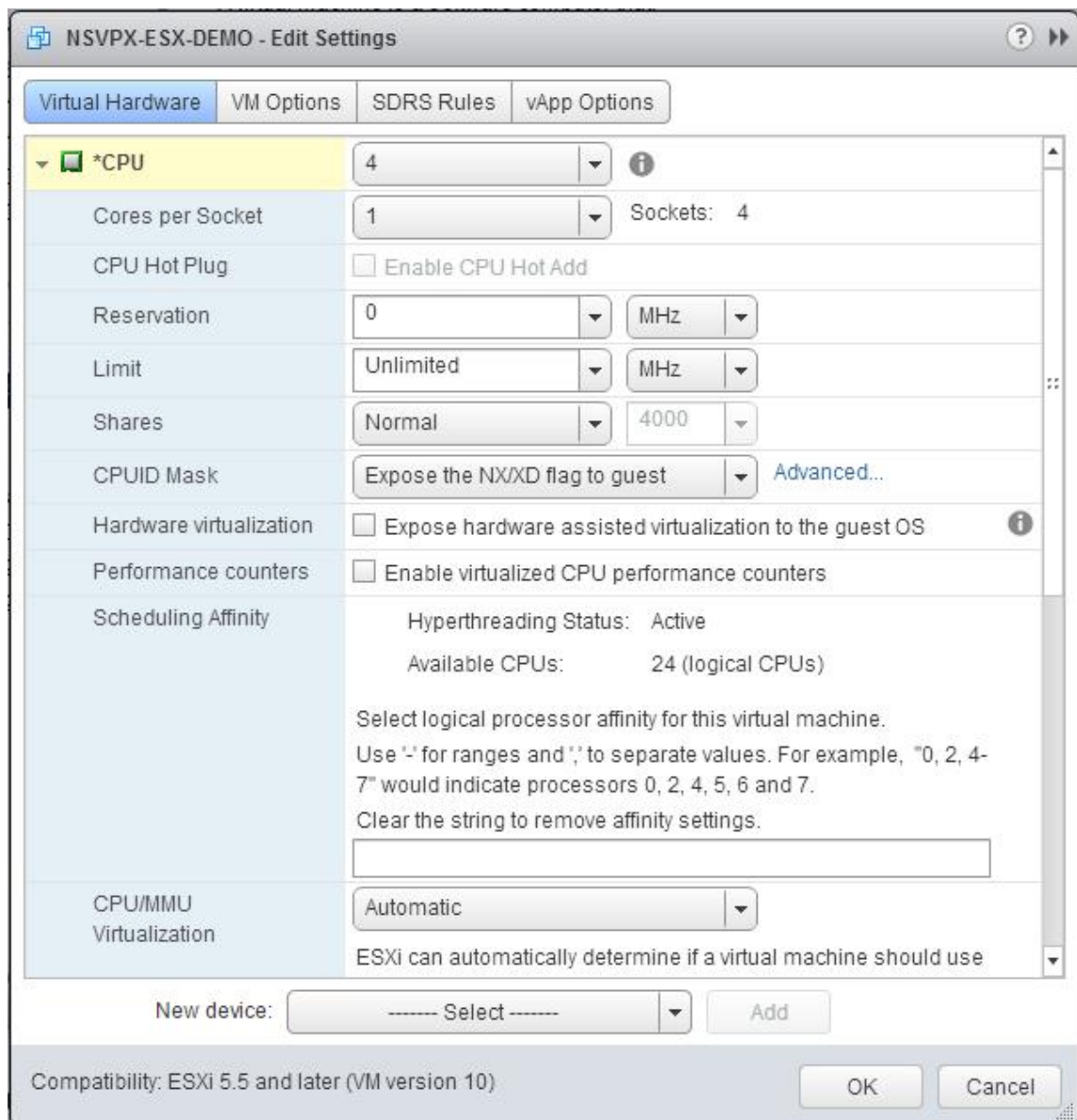
Tras instalar y configurar la instancia de NetScaler VPX en VMware ESX, puede utilizar el cliente web VMware vSphere para configurar el dispositivo virtual para que utilice las interfaces de red VMXNET3.

Para configurar las instancias de NetScaler VPX para que usen las interfaces de red VMXNET3 mediante VMware vSphere Web Client:

1. En vSphere Web Client, seleccione Hosts and Clusters.
2. Actualice la configuración de compatibilidad de la instancia de NetScaler VPX a ESX, de la siguiente manera:
 - a. Apague la instancia de NetScaler VPX.
 - b. Haga clic con el botón derecho en la instancia de NetScaler VPX y seleccione Compatibilidad > Actualizar la compatibilidad de máquinas virtuales.
 - c. En el cuadro de diálogo Configurar la compatibilidad de máquinas virtuales, seleccione ESXi 5.5 y versiones posteriores en la lista desplegable Compatible con y haga clic en Aceptar.
3. Haga clic con el botón derecho en la instancia de NetScaler VPX y haga clic en Modificar configuración.



4. En el cuadro de <virtual_appliance> diálogo: Modificar configuración, haga clic en la sección CPU.



5. En la sección CPU, actualice lo siguiente:

- Cantidad de CPU
- Número de enchufes
- Reservaciones
- Límite
- Comparte

Defina los valores de esta manera:

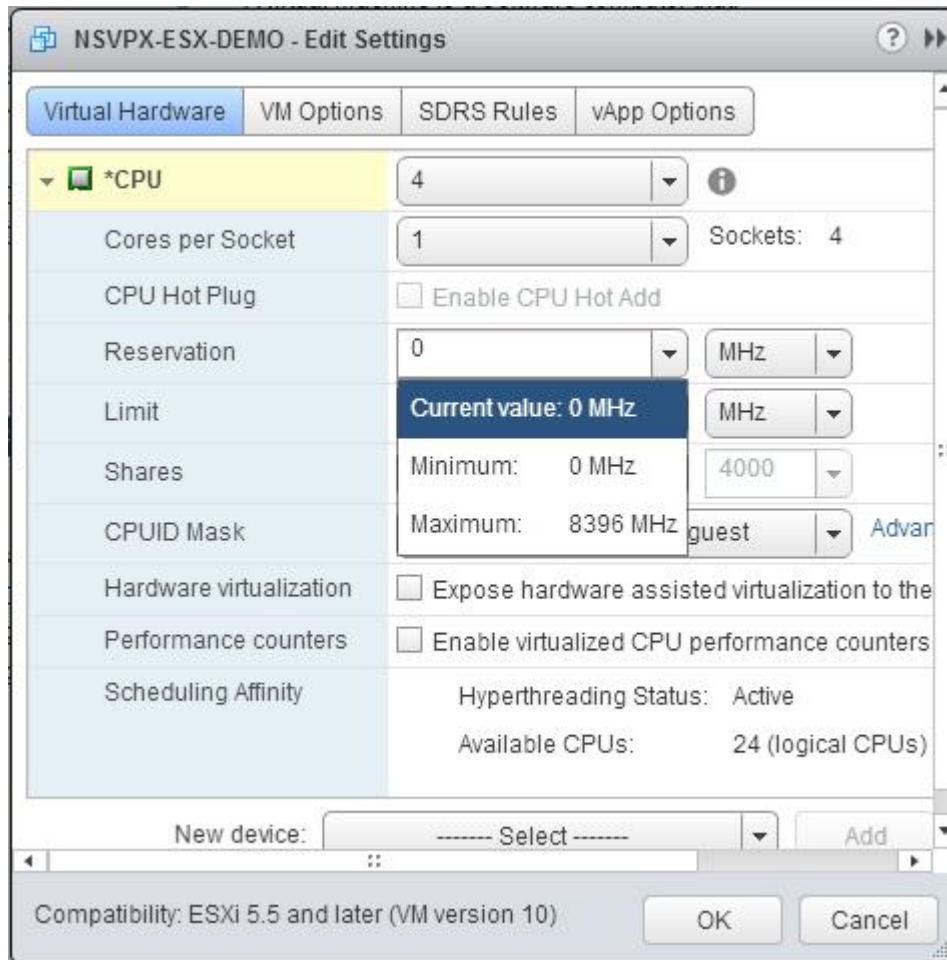
- a. En la lista desplegable CPU, seleccione el número de CPU que desea asignar al dispositivo virtual.
- b. En la lista desplegable Núcleos por socket, seleccione el número de sockets.

c. (Opcional) En el campo Hot Plug de CPU, active o anule la selección de la casilla Habilitar adición en caliente de CPU.

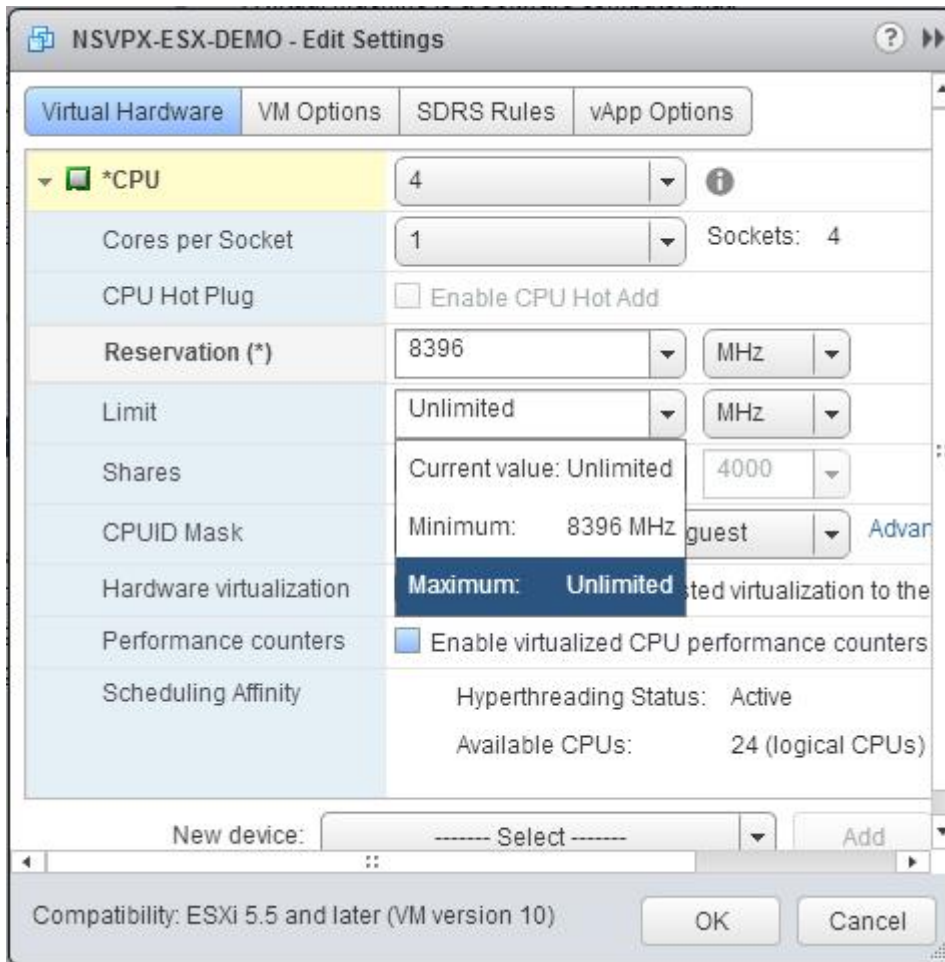
Nota:

Citrix recomienda aceptar el valor predeterminado (deshabilitado).

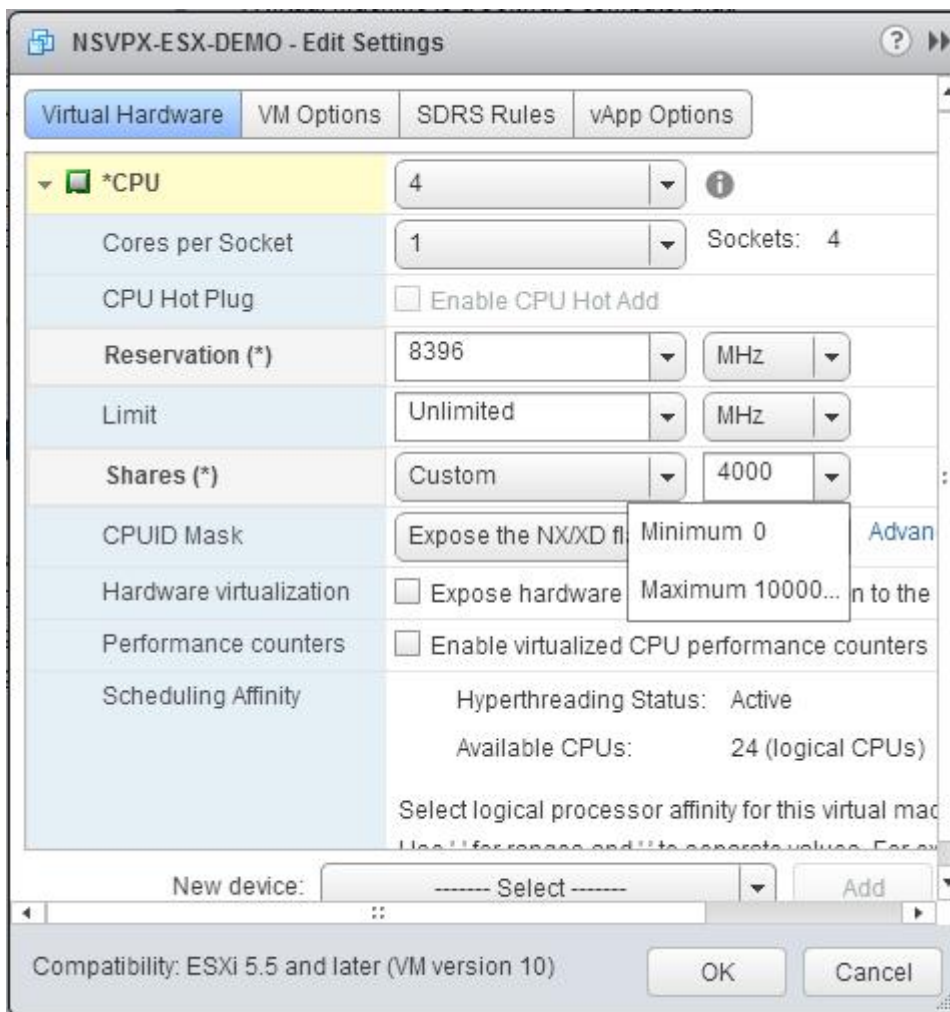
d. En la lista desplegable Reserva, seleccione el número que se muestra como valor máximo.



e. En la lista desplegable Límite, seleccione el número que se muestra como valor máximo.



f. En las listas desplegables Acciones, seleccione Personalizado y el número que se muestra como valor máximo.



6. En la sección Memoria, actualice lo siguiente:

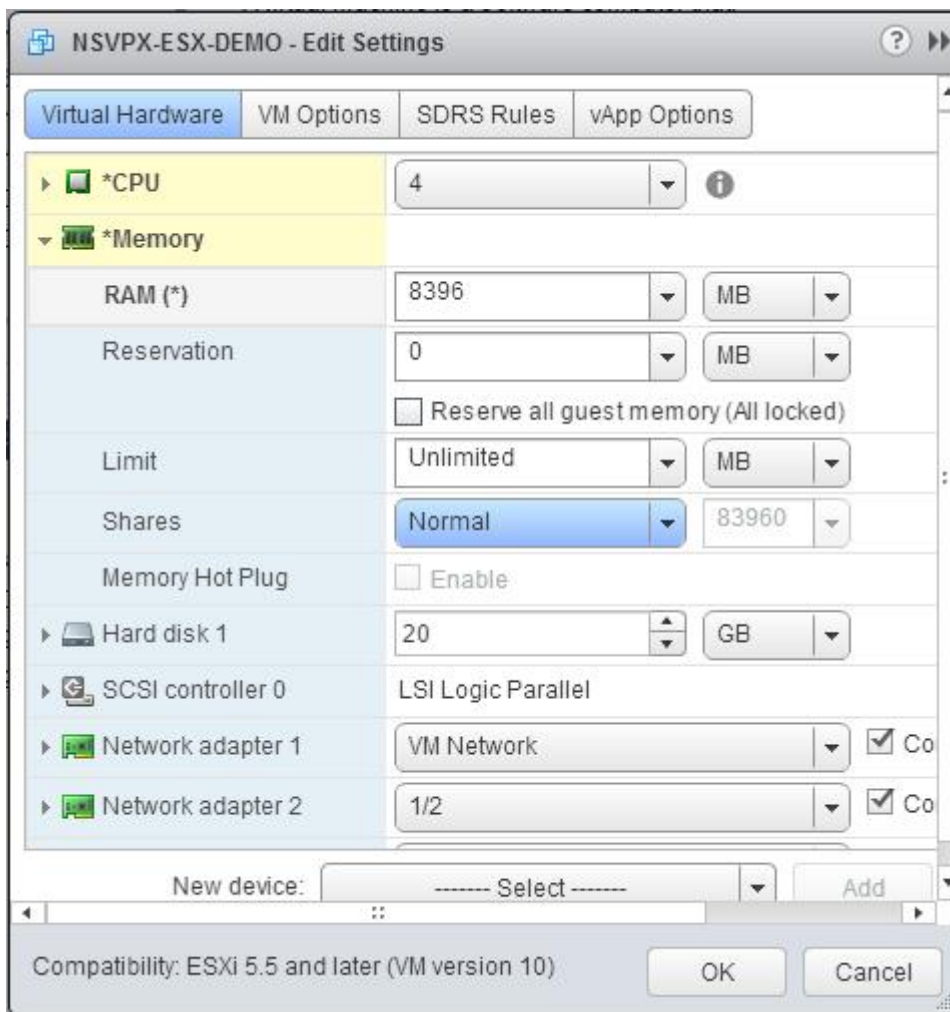
- Tamaño de RAM
- Reservaciones
- Límite
- Comparte

Defina los valores de esta manera:

a. En la lista desplegable RAM, seleccione el tamaño de la RAM. Debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la RAM debe ser de 4 x 2 GB = 8 GB.

Nota:

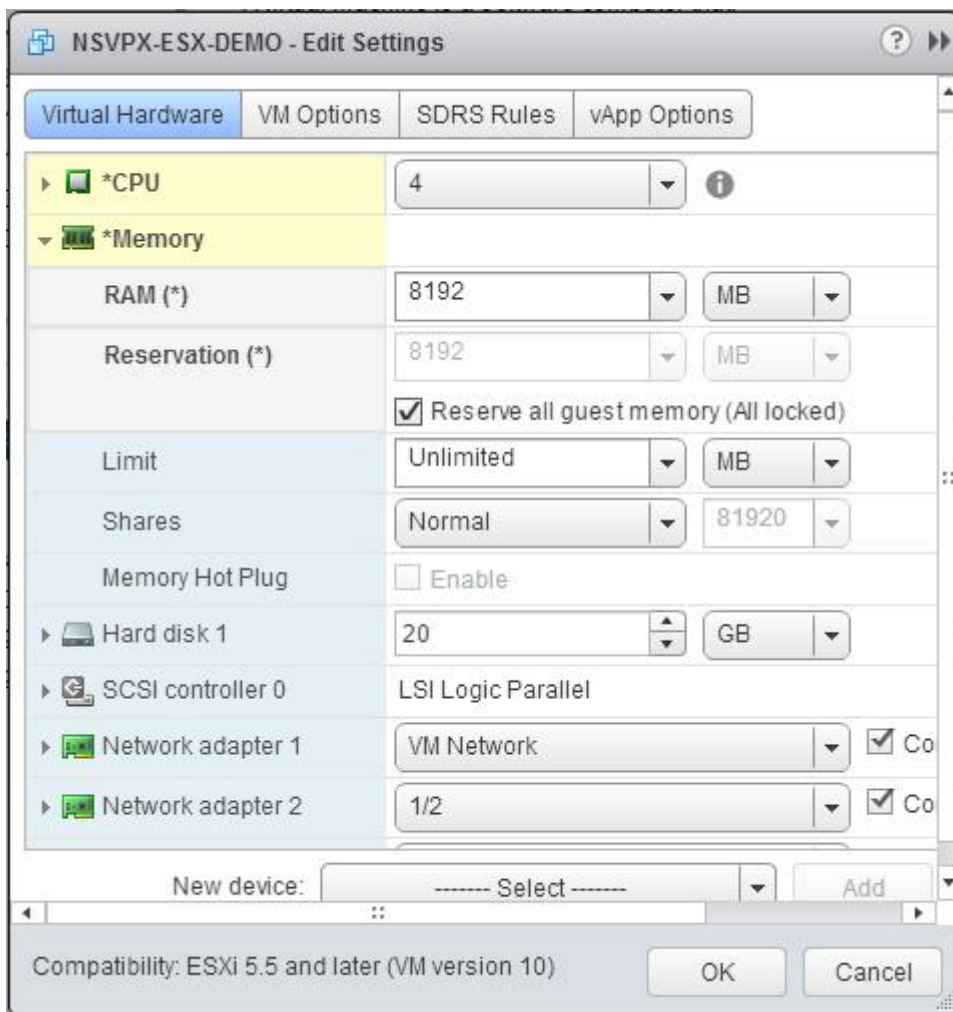
Para una edición avanzada o premium del dispositivo NetScaler VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



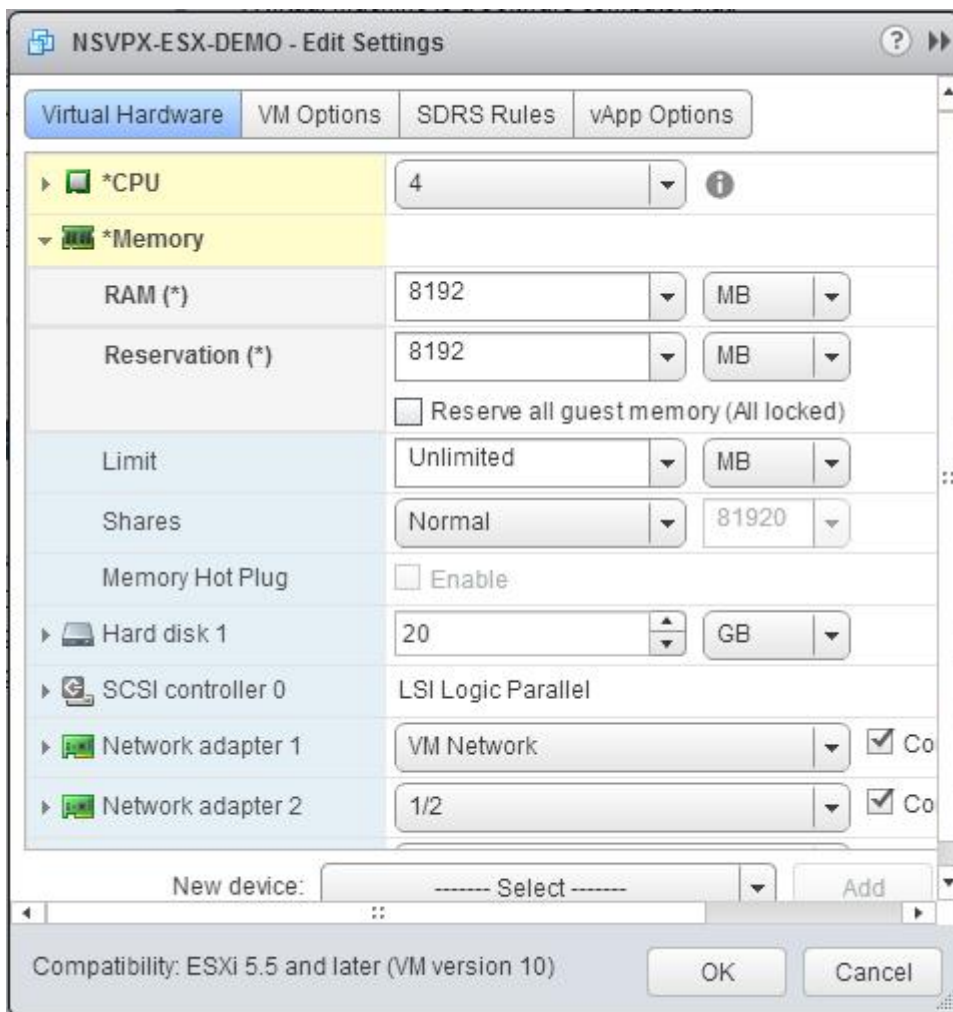
b. En la lista desplegable Reserva, introduzca el valor de la reserva de memoria y active la casilla de verificación Reservar toda la memoria de invitado (Todo bloqueado). La reserva de memoria debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la reserva de memoria debe ser de 4 x 2 GB = 8 GB.

Nota:

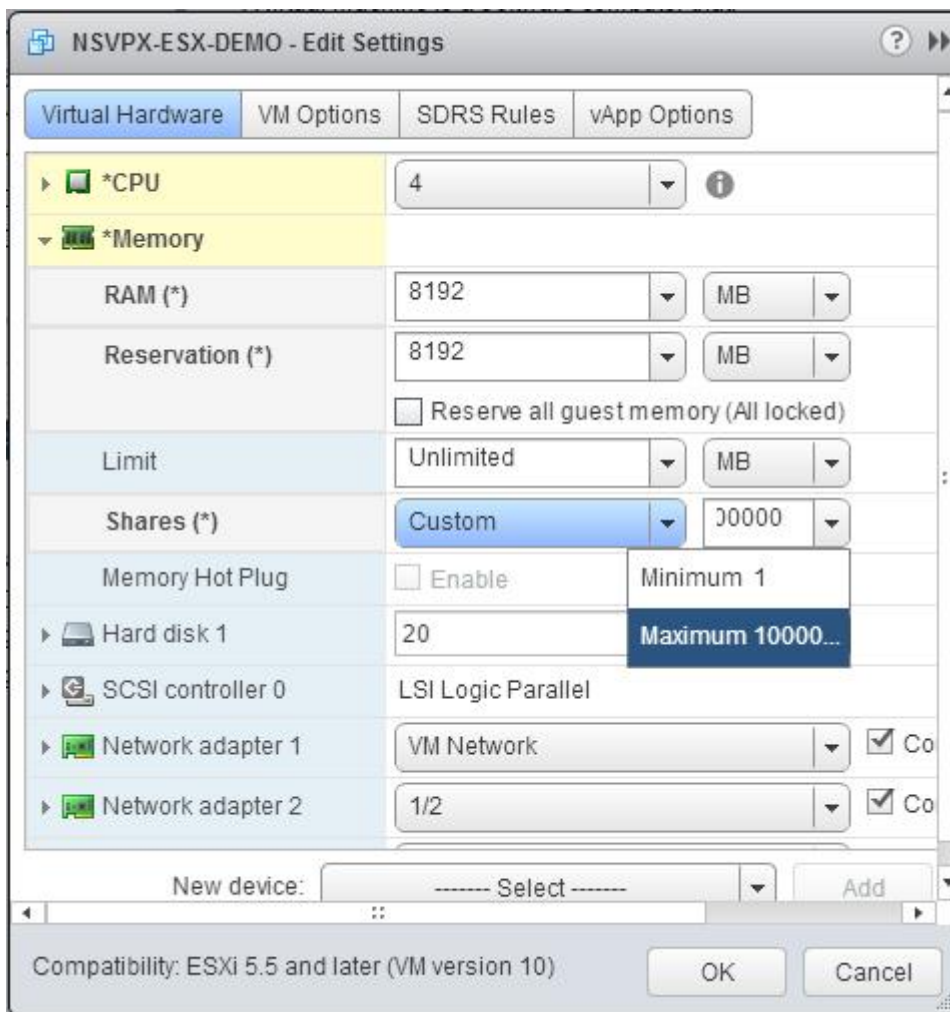
Para una edición avanzada o premium del dispositivo NetScaler VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



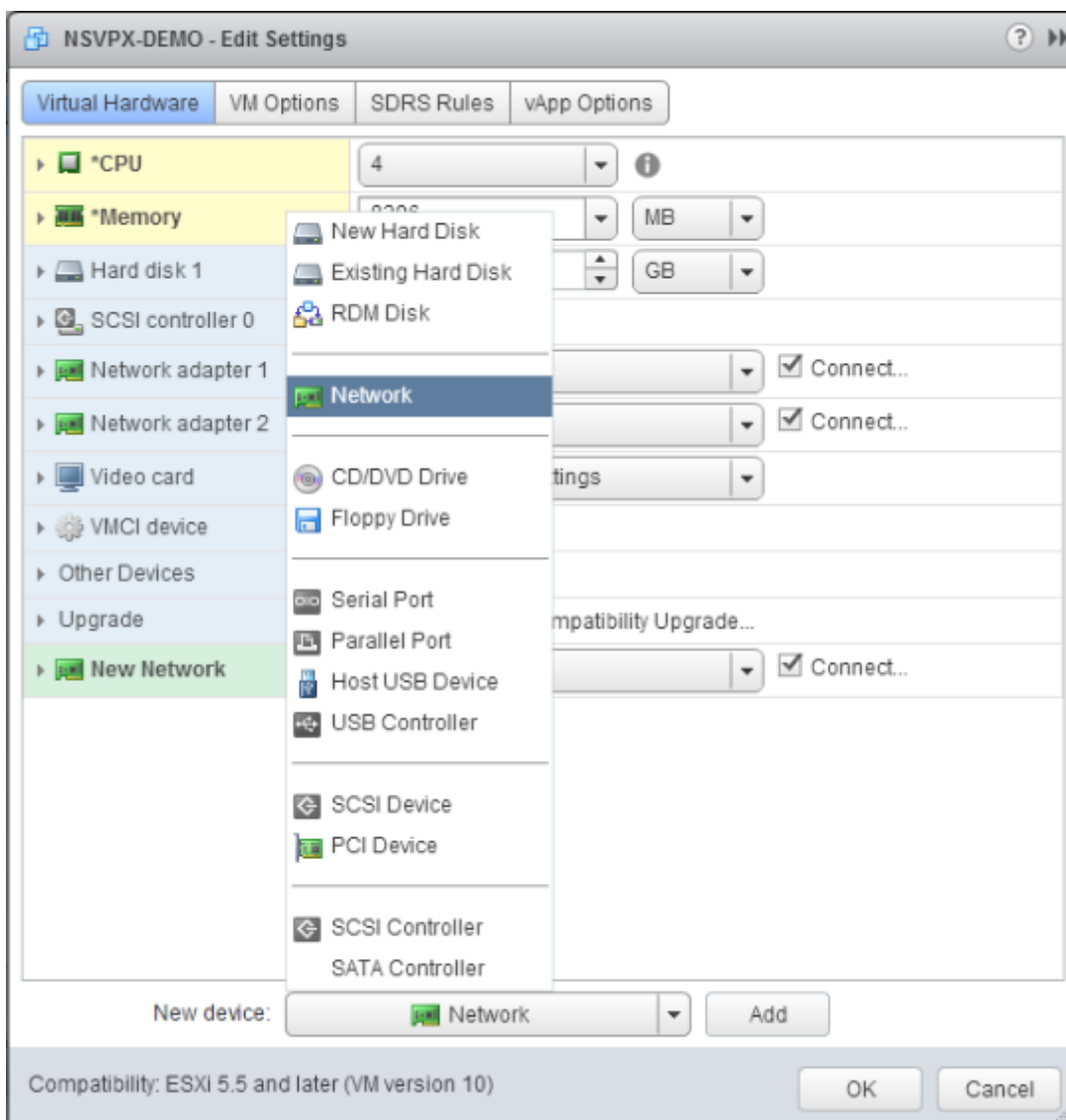
c. En la lista desplegable Límite, seleccione el número que se muestra como valor máximo.



d. En las listas desplegadas Acciones, seleccione Personalizado y el número que se muestra como valor máximo.



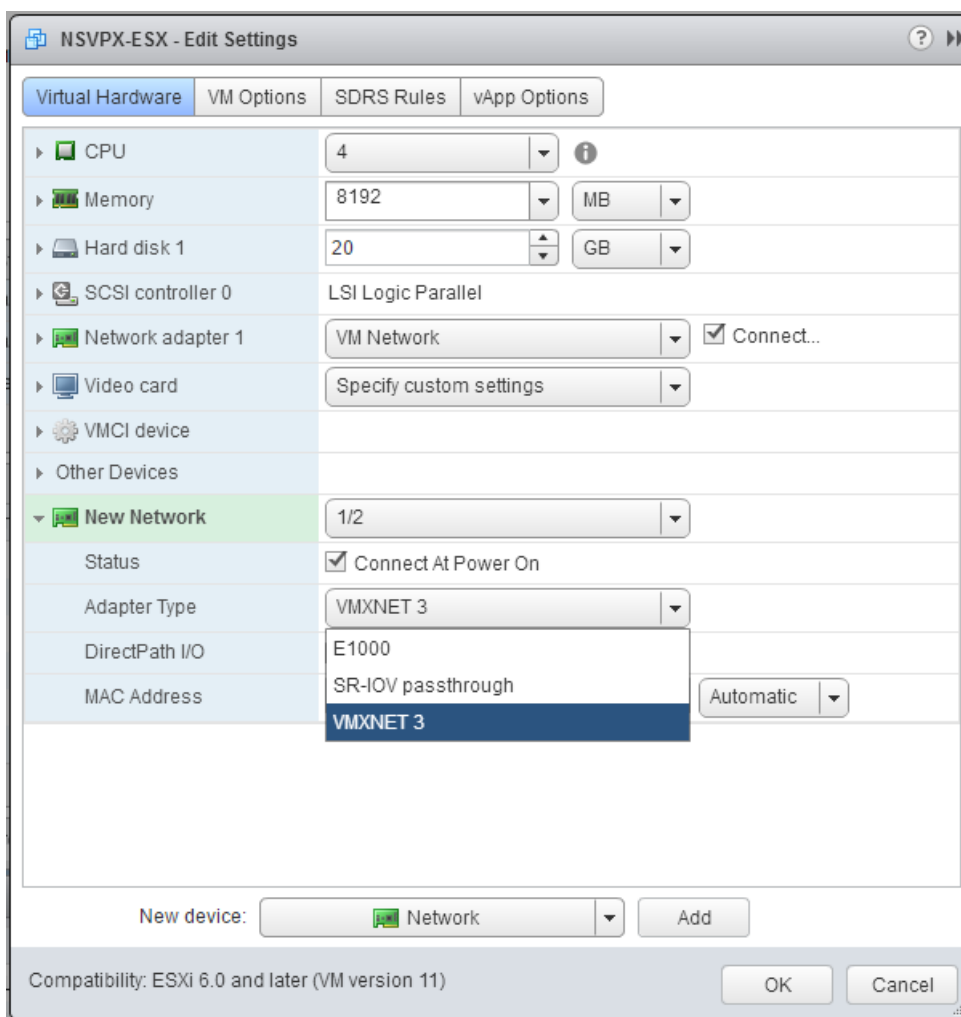
7. Agregue una interfaz de red VMXNET3. En la lista desplegable Nuevo dispositivo, seleccione Red y haga clic en Agregar.



- 8. En la sección Nueva red, en la lista desplegable, seleccione la interfaz de red y haga lo siguiente:
 - a. En la lista desplegable Tipo de adaptador, seleccione VMXNET3.

Importante:

La interfaz de red E1000 predeterminada y VMXNET3 no pueden coexistir, asegúrese de quitar la interfaz de red E1000 y utilizar VMXNET3 (0/1) como interfaz de administración.



9. Haz clic en **Aceptar**.
10. Encienda la instancia NetScaler VPX.
11. Una vez que se enciende la instancia de NetScaler VPX, puede utilizar el siguiente comando para verificar la configuración:

mostrar resumen de interfaz

El resultado debe mostrar todas las interfaces que ha configurado:

```

1 > show interface summary
2 -----
3           Interface  MTU      MAC                Suffix
4 -----
5 1      0/1          1500     00:0c:29:89:1d:0e  NetScaler Vir...
6      rface, VMXNET3
7 2      1/1          9000     00:0c:29:89:1d:18  NetScaler Vir...
8      rface, VMXNET3
    
```

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

Nota:

Después de agregar una interfaz VMXNET3 y reiniciar el dispositivo NetScaler VPX, el hipervisor VMware ESX podría cambiar el orden en que se presenta la NIC al dispositivo VPX. Por lo tanto, es posible que el adaptador de red 1 no permanezca siempre 0/1, lo que provoca la pérdida de conectividad de administración con el dispositivo VPX. Para evitar este problema, cambie la red virtual del adaptador de red en consecuencia.

Se trata de una limitación del hipervisor VMware ESX.

Establecer el tamaño del anillo de recepción para la interfaz de red VMXNET3

Puede aumentar el tamaño del anillo de recepción para las interfaces de red VMXNET3 en VMware ESX. Un tamaño de anillo más alto reduce la pérdida de paquetes cuando se produce una ráfaga repentina de tráfico.

Nota:

Esta función está disponible en la versión 14.1, compilación 14.x y posteriores.

Para establecer el tamaño del anillo en una interfaz de red VMXNET3

En el símbolo del sistema, escriba:

```
set interface id [-ringsize *entero_positivo*]
```

El tamaño máximo de anillo que puede configurar en una interfaz VMXNET3 es 2048. Solo se admite el tipo de anillo fijo. Debe guardar la configuración y reiniciar la instancia de NetScaler VPX para que la configuración surta efecto.

Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV

October 17, 2024

Después de instalar y configurar la instancia VPX de NetScaler en VMware ESX, puede utilizar el cliente web VMware vSphere para configurar el dispositivo virtual de modo que utilice interfaces de red de virtualización (SR-IOV) raíz única de E/S v virtualización (SR-IOV).

Limitaciones

Un NetScaler VPX configurado con una interfaz de red SR-IOV tiene las siguientes limitaciones:

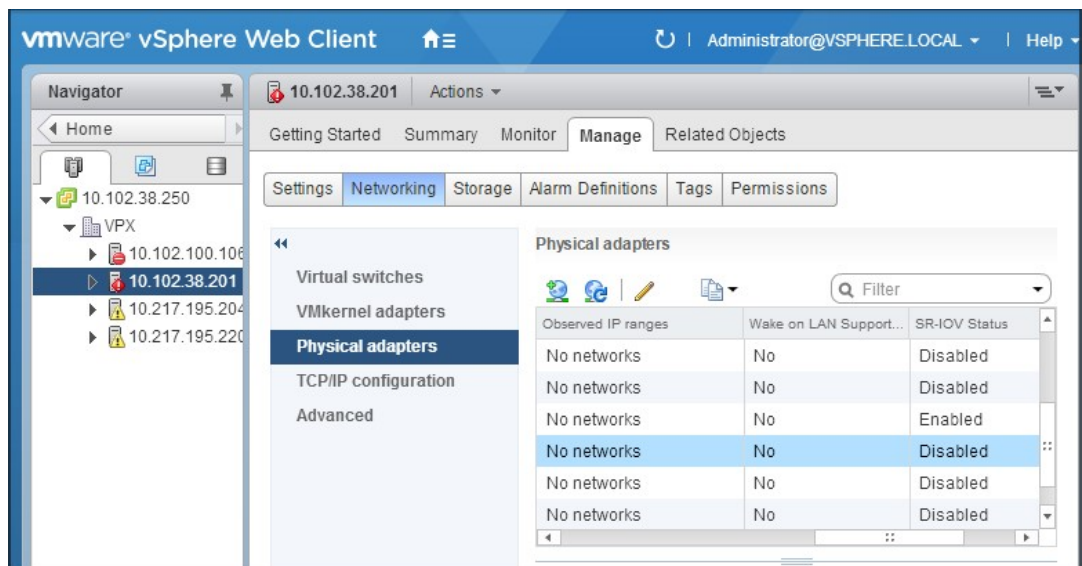
- Las siguientes funciones no se admiten en las interfaces SR-IOV que utilizan la NIC Intel 82599 10G en ESX VPX:
 - Conmutación del modo L2
 - Agregación de enlaces estáticos y LACP
 - Agrupar en clústeres
 - Particionado de administrador [modo VLAN compartida]
 - Alta disponibilidad [Activo - modo activo]
 - Marcos gigantes
 - IPv6
- Las siguientes funciones no se admiten en la interfaz SR-IOV con una NIC Intel 82599 10G en KVM VPX:
 - Agregación de enlaces estáticos y LACP
 - Conmutación del modo L2
 - Agrupar en clústeres
 - Particionado de administrador [modo VLAN compartida]
 - Alta disponibilidad [Activo —Modo activo]
 - Marcos gigantes
 - IPv6
 - No se admite la configuración de VLAN en el hipervisor para la interfaz VF SR-IOV a través del comando `ip link`

Requisito previo

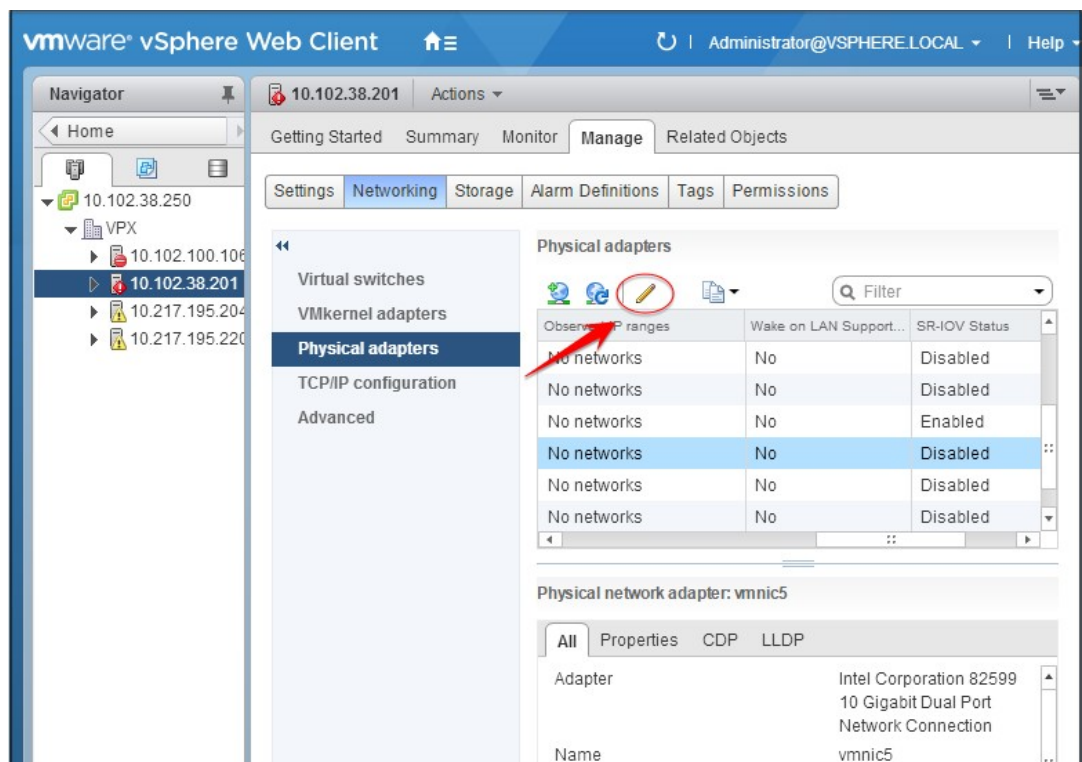
- Asegúrese de agregar cualquiera de las siguientes NIC al host ESX:
 - Se recomienda la NIC Intel 82599, controlador IXGBE versión 3.7.13.7.14iov o posterior.
 - NIC Mellanox ConnectX-4
- Habilite SR-IOV en el adaptador físico del host.

Siga este procedimiento para habilitar el SR-IOV en el adaptador físico del host:

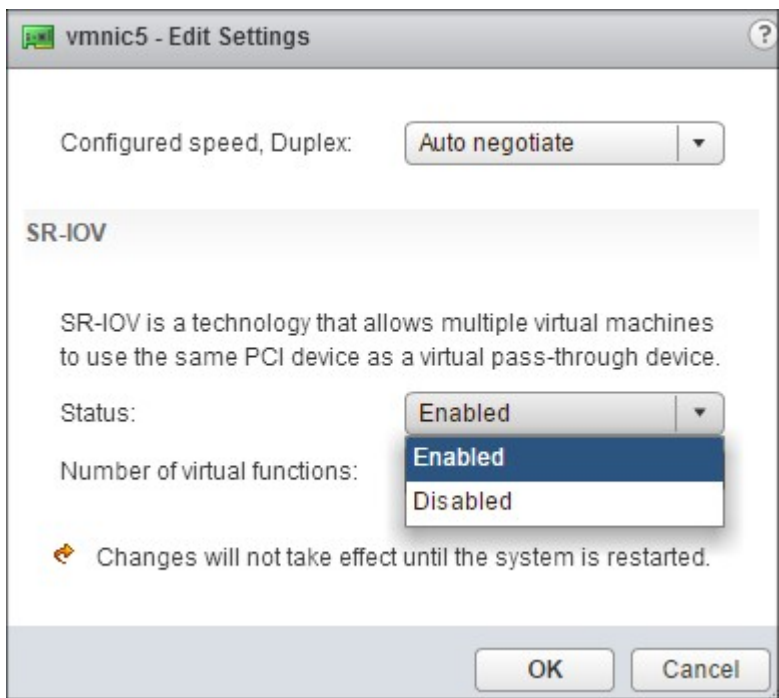
1. En vSphere Web Client, vaya al Host.
2. En la ficha **Administrar > Redes**, seleccione **Adaptadores físicos**. El campo Estado SR-IOV muestra si un adaptador físico admite SR-IOV.



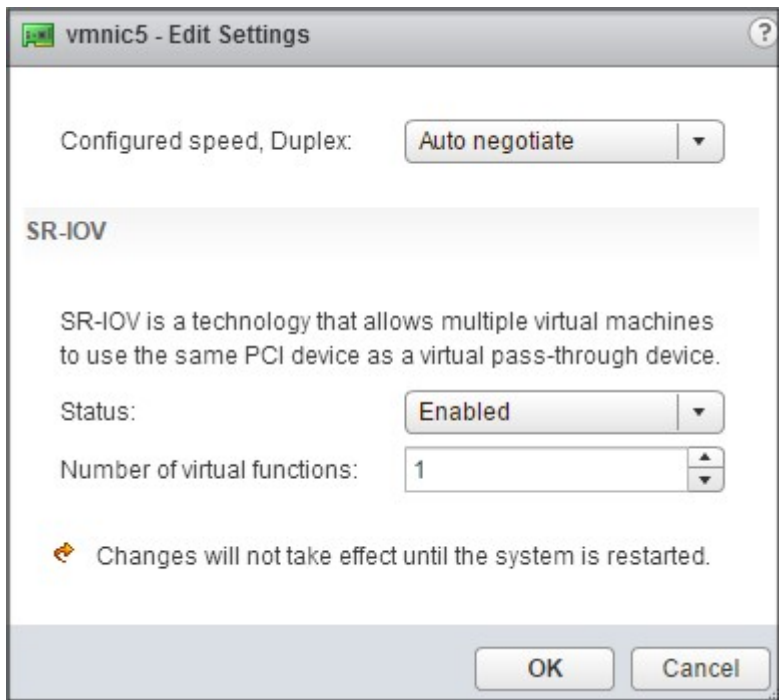
3. Seleccione el adaptador físico y, a continuación, haga clic en el icono del lápiz para abrir el cuadro de diálogo **Modificar configuración**.



4. En SR-IOV, seleccione **Habilitado** en la lista desplegable **Estado**.



5. En el campo **Número de funciones virtuales**, escriba el número de funciones virtuales que quiere configurar para el adaptador.



6. Haz clic en **Aceptar**.
 7. Reinicie el host.
- Cree un conmutador virtual distribuido (DVS) y [Portgroups](#). Para obtener instrucciones, con-

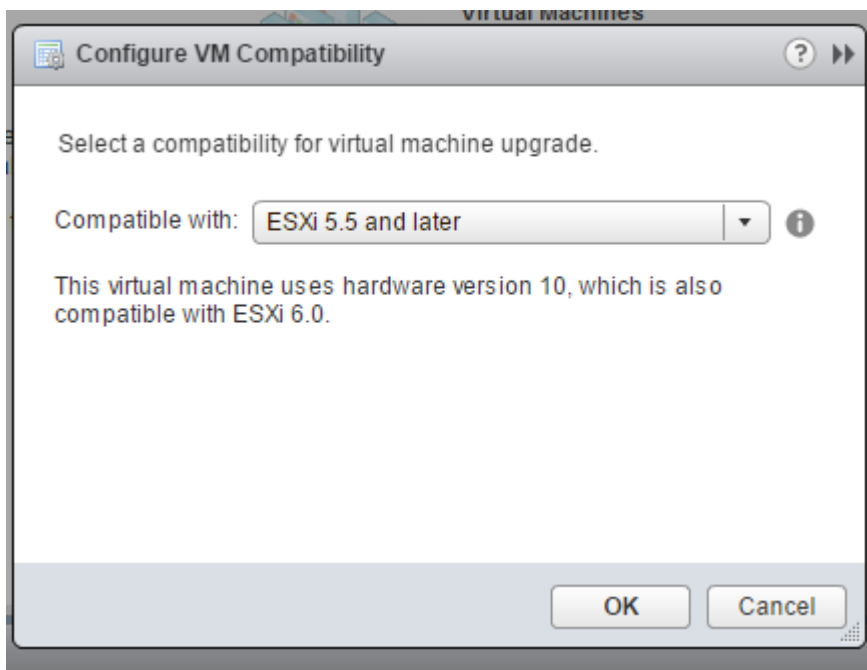
sulte la Documentación de VMware.

Nota:

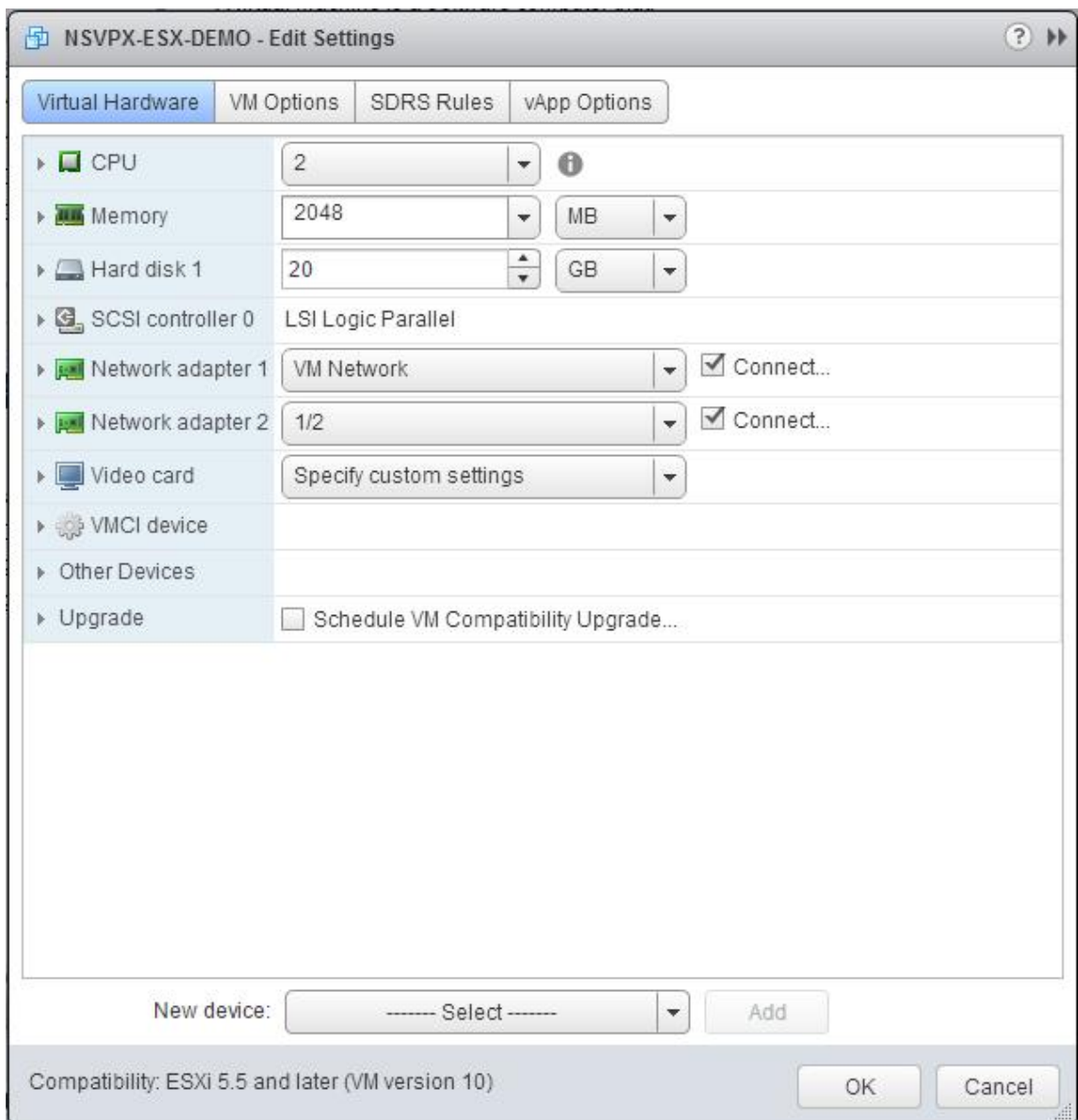
Citrix ha calificado la configuración SR-IOV en DVS y [Portgroups](#) solo.

Para configurar instancias de NetScaler VPX para que utilicen la interfaz de red SR-IOV mediante VMware vSphere Web Client:

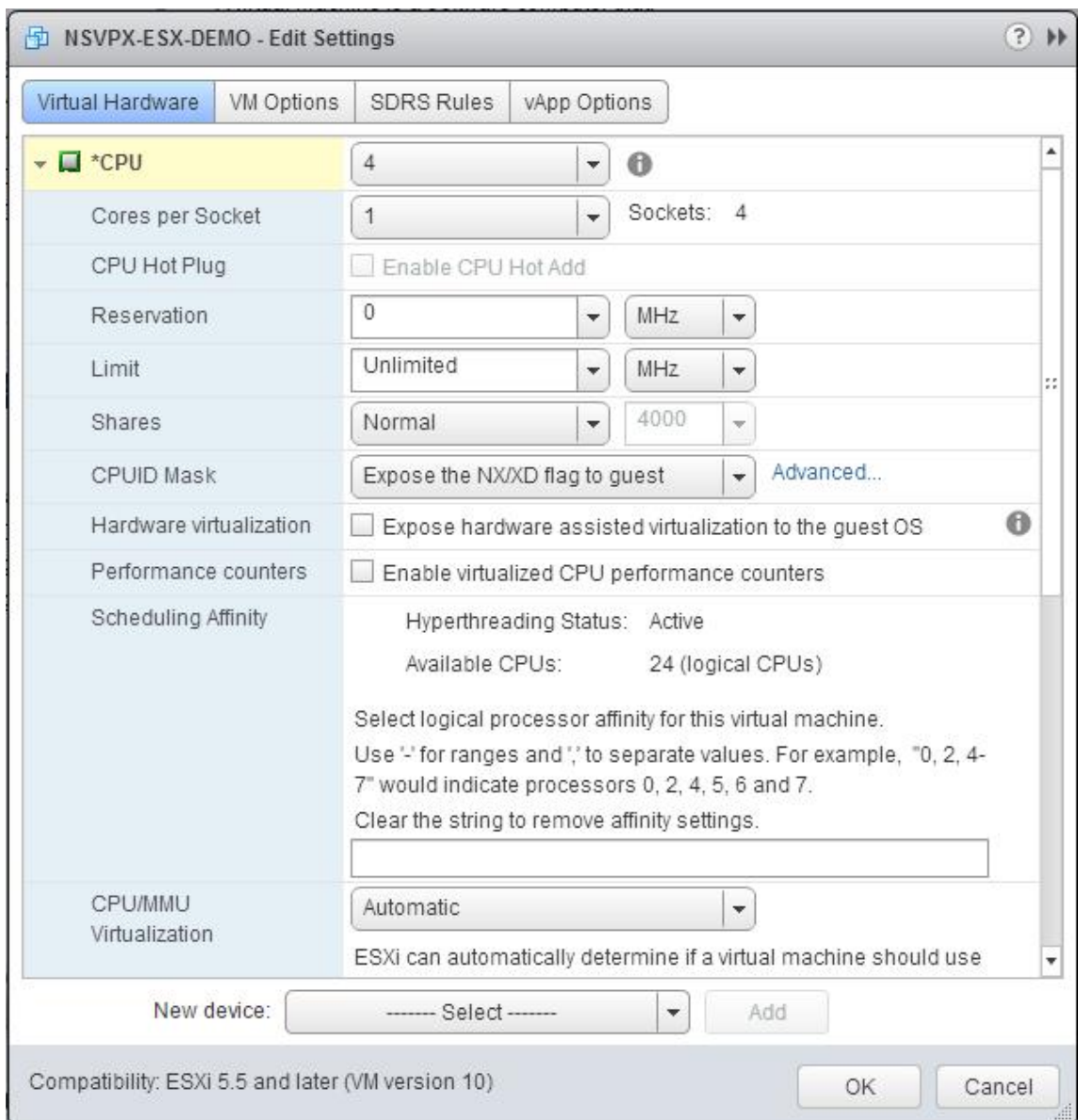
1. En vSphere Web Client, seleccione **Hosts and Clusters**.
2. Actualice la configuración de compatibilidad de la instancia NetScaler VPX a ESX 5.5 o posterior, de la siguiente manera:
 - a. Apague la instancia de NetScaler VPX.
 - b. Haga clic con el botón derecho en la instancia de NetScaler VPX y seleccione **Compatibilidad > Actualizar la compatibilidad de máquinas virtuales**.
 - c. **En el cuadro de diálogo** Configurar la compatibilidad de máquinas virtuales, **seleccione** ESXi 5.5 y versiones posteriores **en la lista desplegable** Compatible con **y haga clic en Aceptar**.



3. Haga clic con el botón derecho en la instancia de NetScaler VPX y haga clic en **Modificar configuración**.



4. En el cuadro de **<virtual_appliance>** diálogo: **Modificar configuración**, haga clic en la sección **CPU**.



5. En la sección **CPU**, actualice la siguiente configuración:

- Cantidad de CPU
- Número de enchufes
- Reservaciones
- Límite
- Comparte

Defina los valores de esta manera:

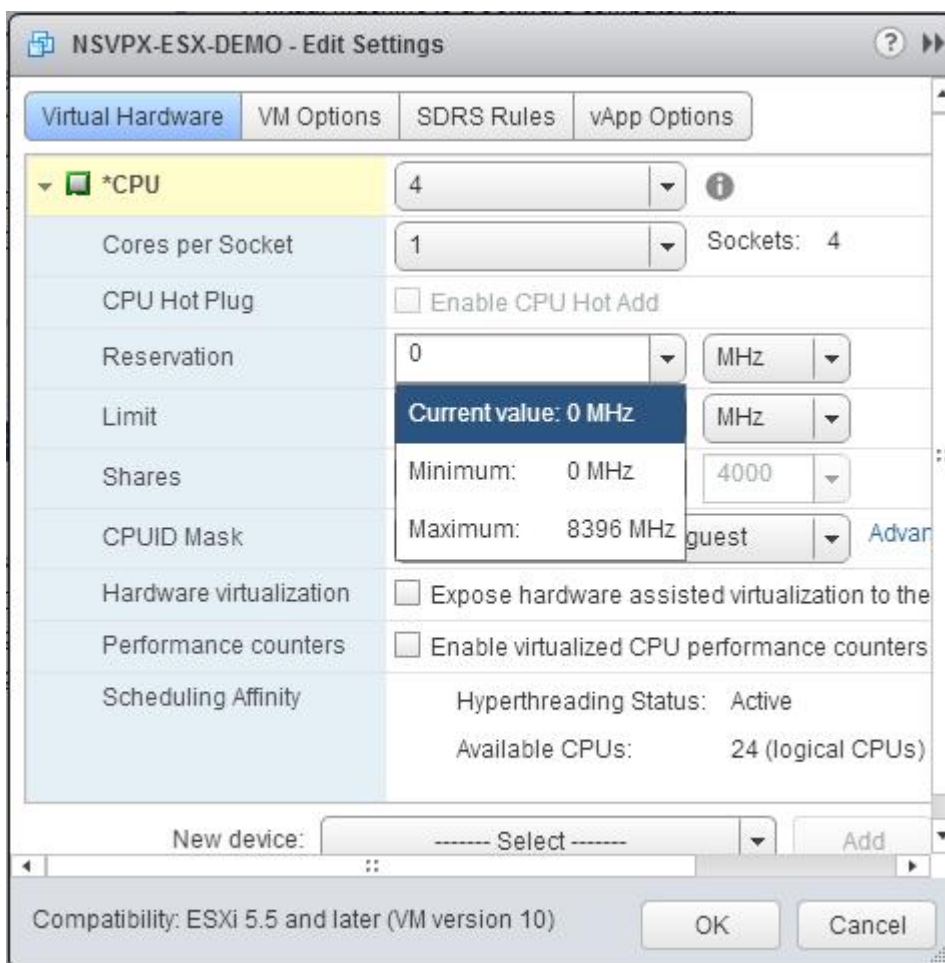
- En la lista desplegable **CPU**, seleccione el número de CPU que desea asignar al dispositivo virtual.
- En la lista desplegable **Núcleos por socket**, seleccione el número de sockets.

c. (Opcional) En el campo Conexión en **caliente de la CPU**, active o desactive la casilla **Habilitar la adición en caliente de CPU** .

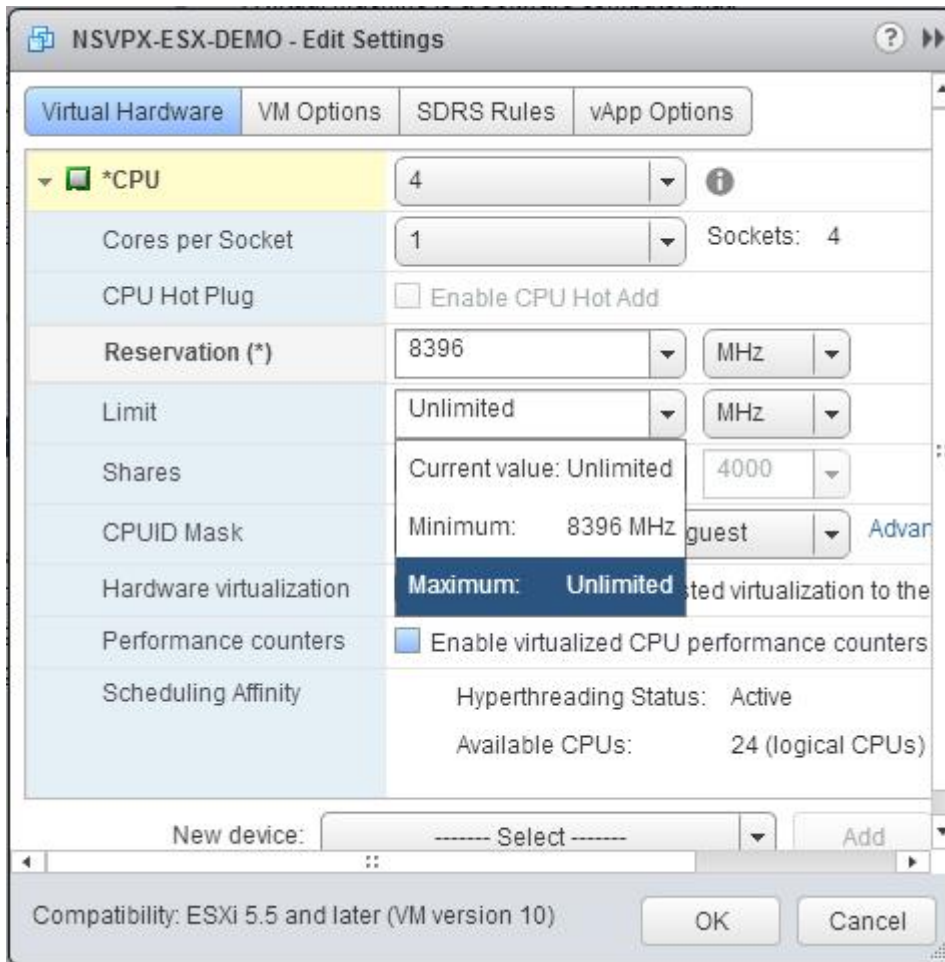
Nota:

Citrix recomienda aceptar el valor predeterminado (deshabilitado).

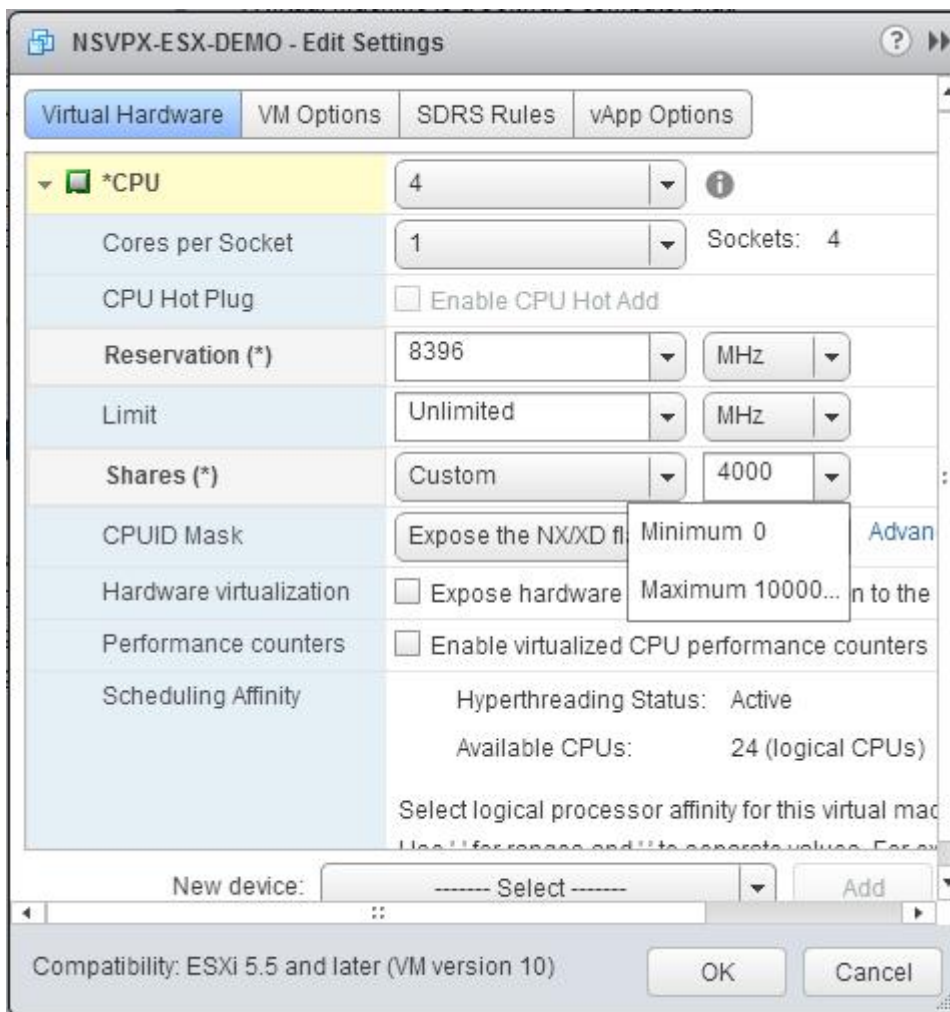
d. En la lista desplegable **Reserva**, seleccione el número que se muestra como valor máximo.



e. En la lista desplegable **Límite**, seleccione el número que se muestra como valor máximo.



f. En las listas desplegables **Acciones**, seleccione **Personalizado** y el número que se muestra como valor máximo.



6. En la sección **Memoria**, actualice la siguiente configuración:

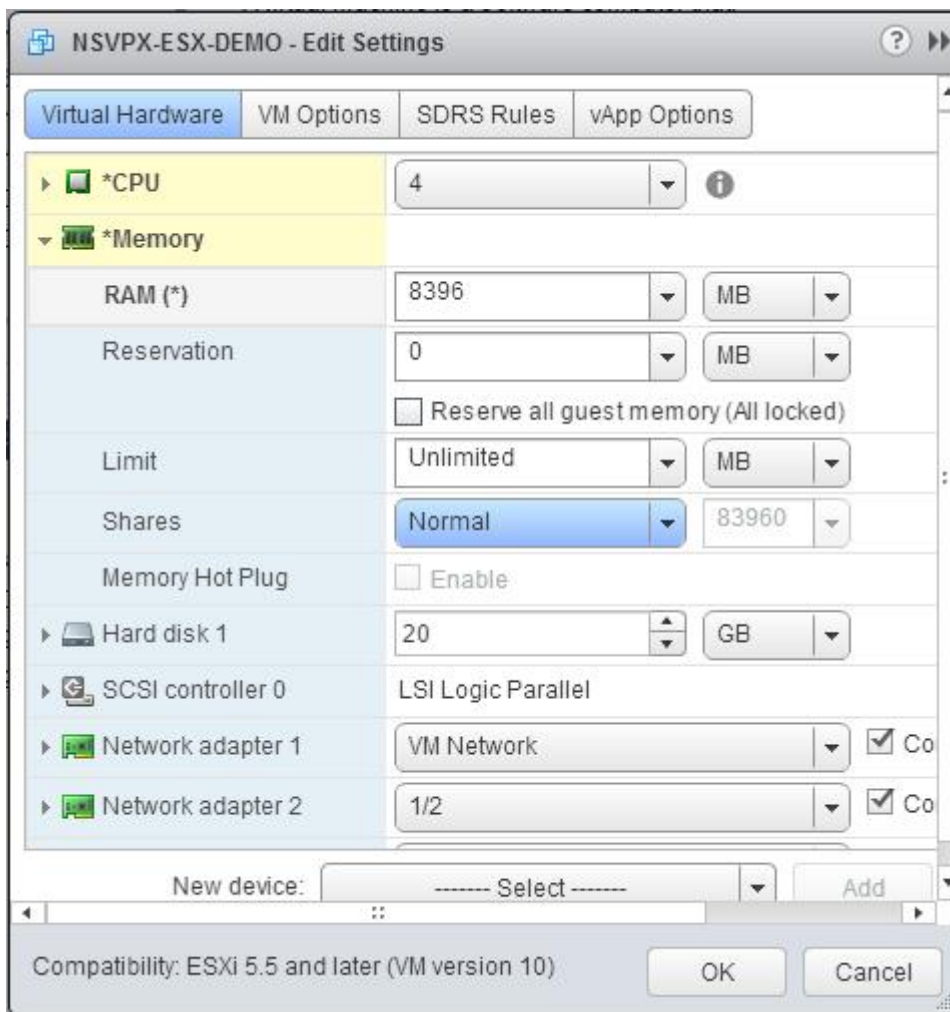
- Tamaño de RAM
- Reservaciones
- Límite
- Comparte

Defina los valores de esta manera:

a. En la lista desplegable **RAM**, seleccione el tamaño de la RAM. Debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 2 GB = 8 GB.

Nota:

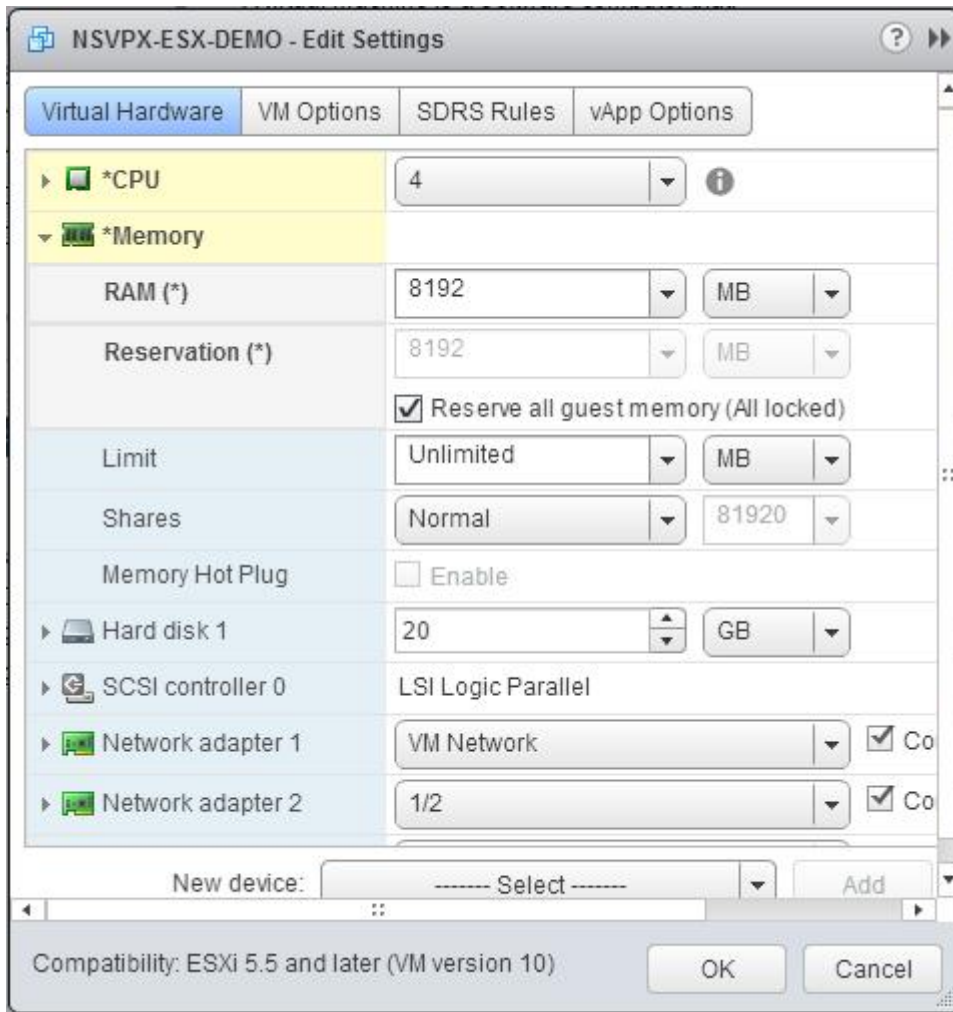
Para la edición Advanced o Premium del dispositivo NetScaler VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



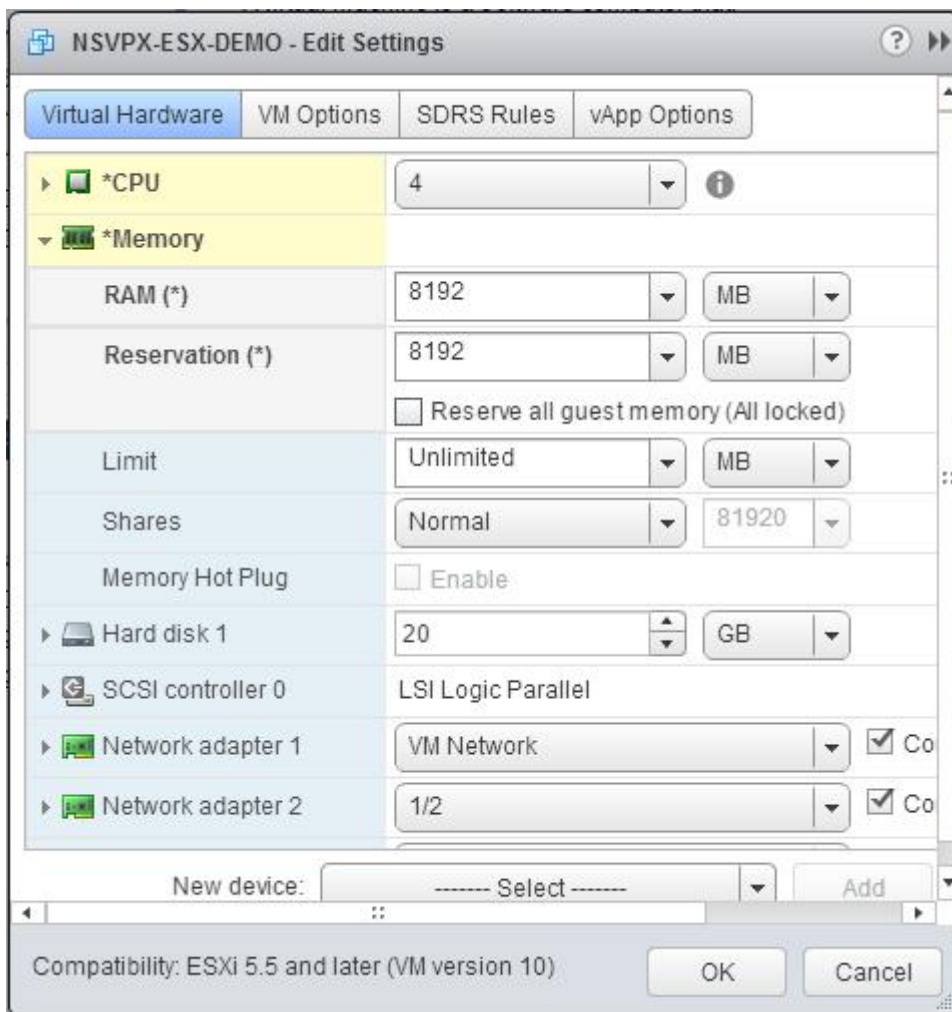
b. En la lista desplegable **Reserva**, introduzca el valor de la reserva de memoria y active la casilla de verificación Reservar **toda la memoria de invitado (Todo bloqueado)**. La reserva de memoria debe ser el número de vCPU x 2 GB. Por ejemplo, si el número de vCPU es 4, la reserva de memoria debe ser de 4 x 2 GB = 8 GB.

Nota:

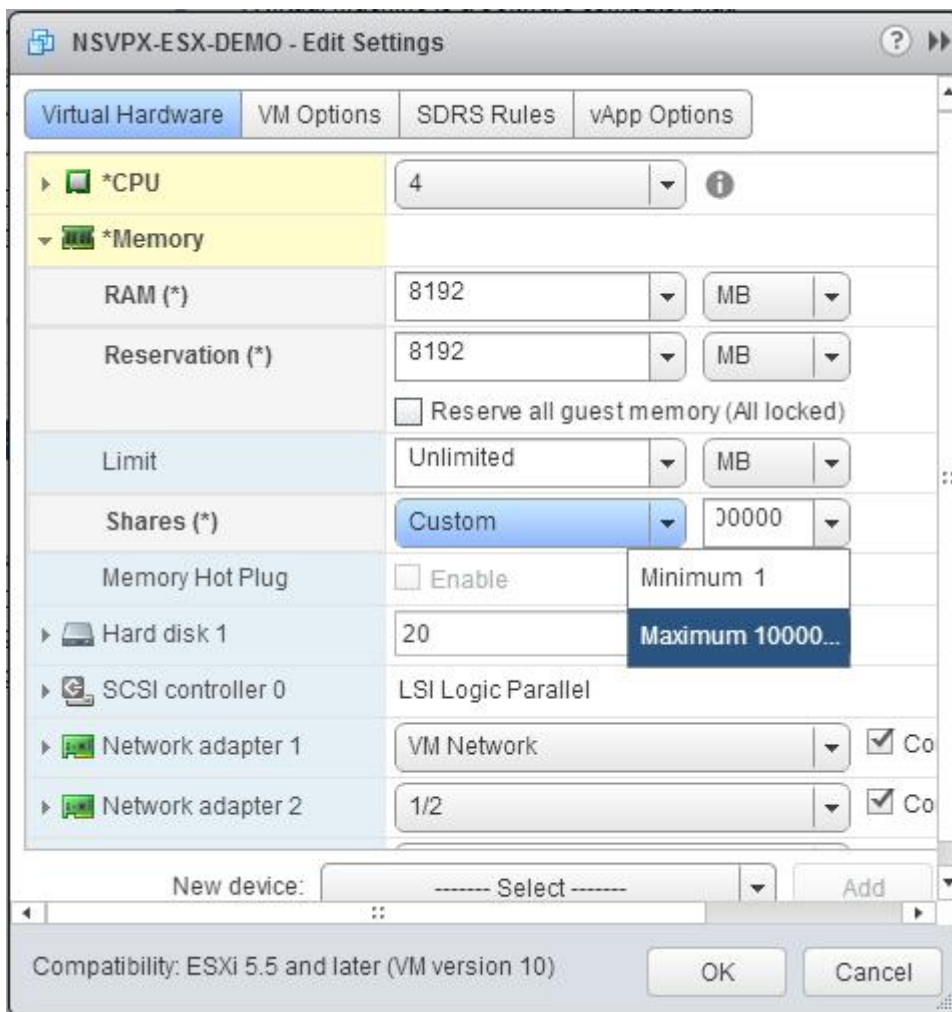
Para la edición Advanced o Premium del dispositivo NetScaler VPX, asegúrese de asignar 4 GB de RAM a cada vCPU. Por ejemplo, si el número de vCPU es 4, entonces RAM = 4 x 4 GB = 16 GB.



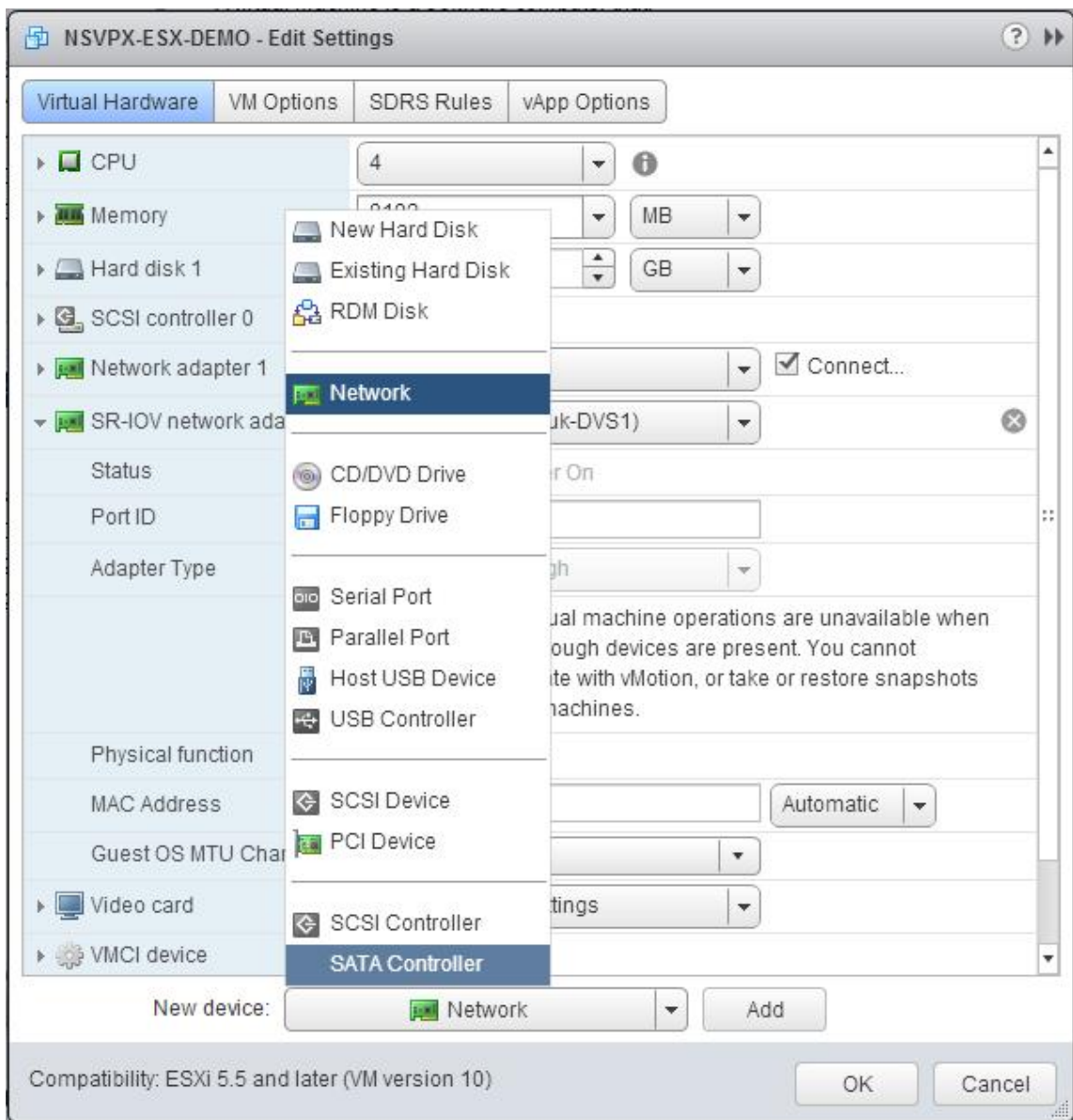
c. En la lista desplegable **Límite**, seleccione el número que se muestra como valor máximo.



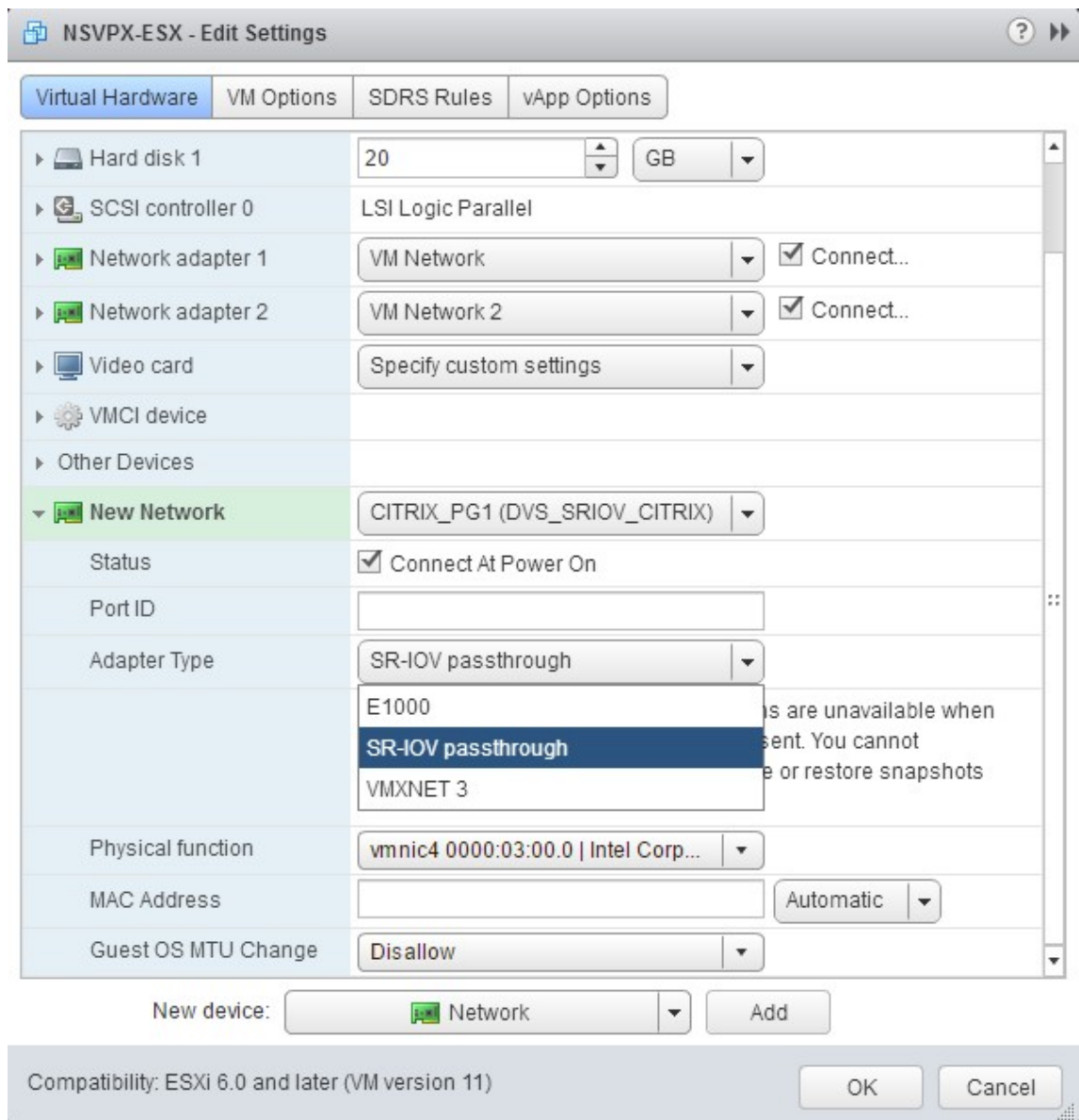
d. En las listas desplegadas **Acciones**, seleccione **Personalizado** y seleccione el número que se muestra como valor máximo.



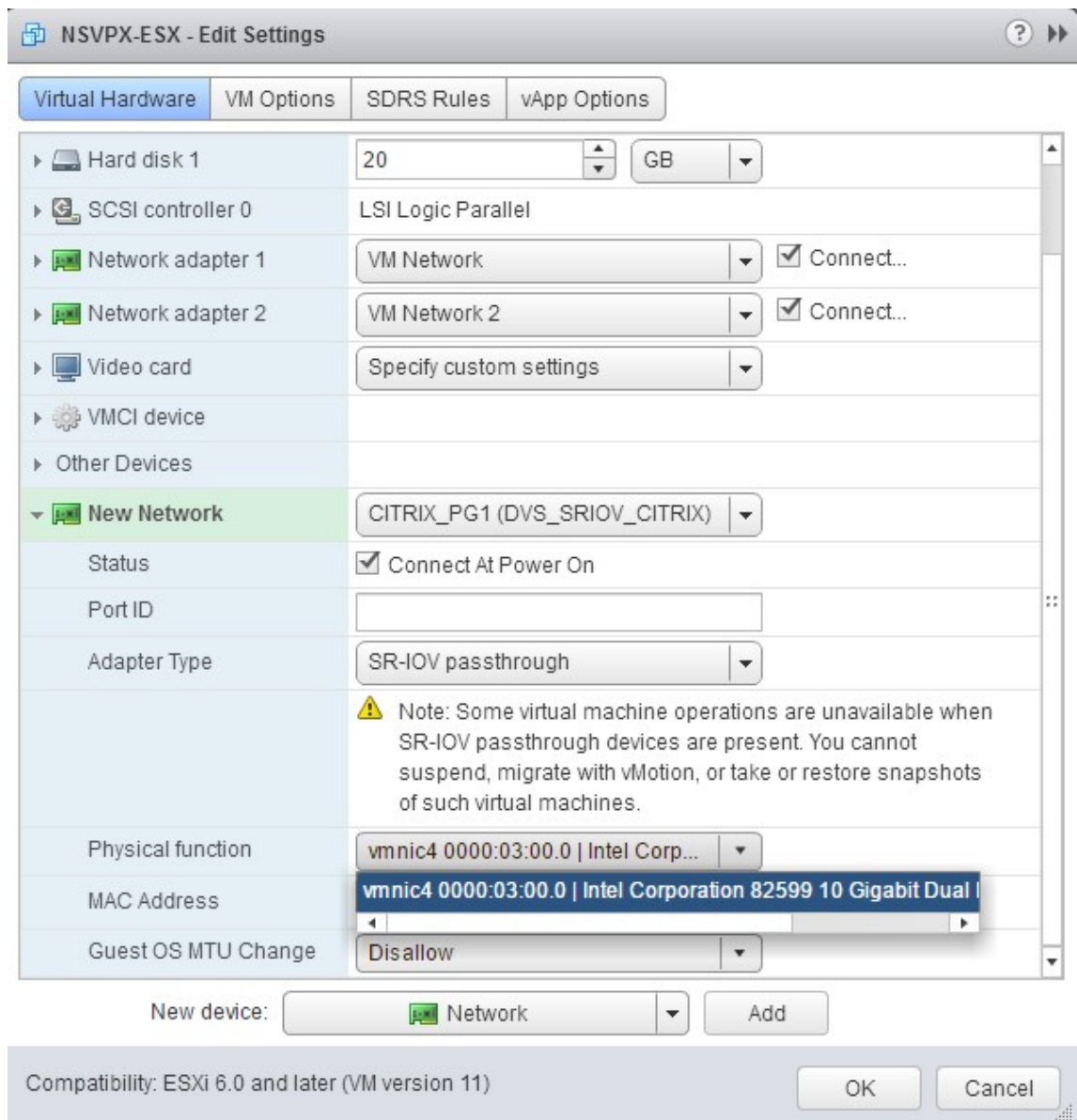
7. Agregue una interfaz de red SR-IOV. En la lista desplegable **Nuevo dispositivo**, seleccione **Red** y haga clic en **Agregar**.



- 8. En la sección **Nueva red**. En la lista desplegable, seleccione el **Portgroup** que ha creado y haga lo siguiente:
 - a. En la lista desplegable **Tipo de adaptador**, seleccione **Passthrough SR-IOV**.

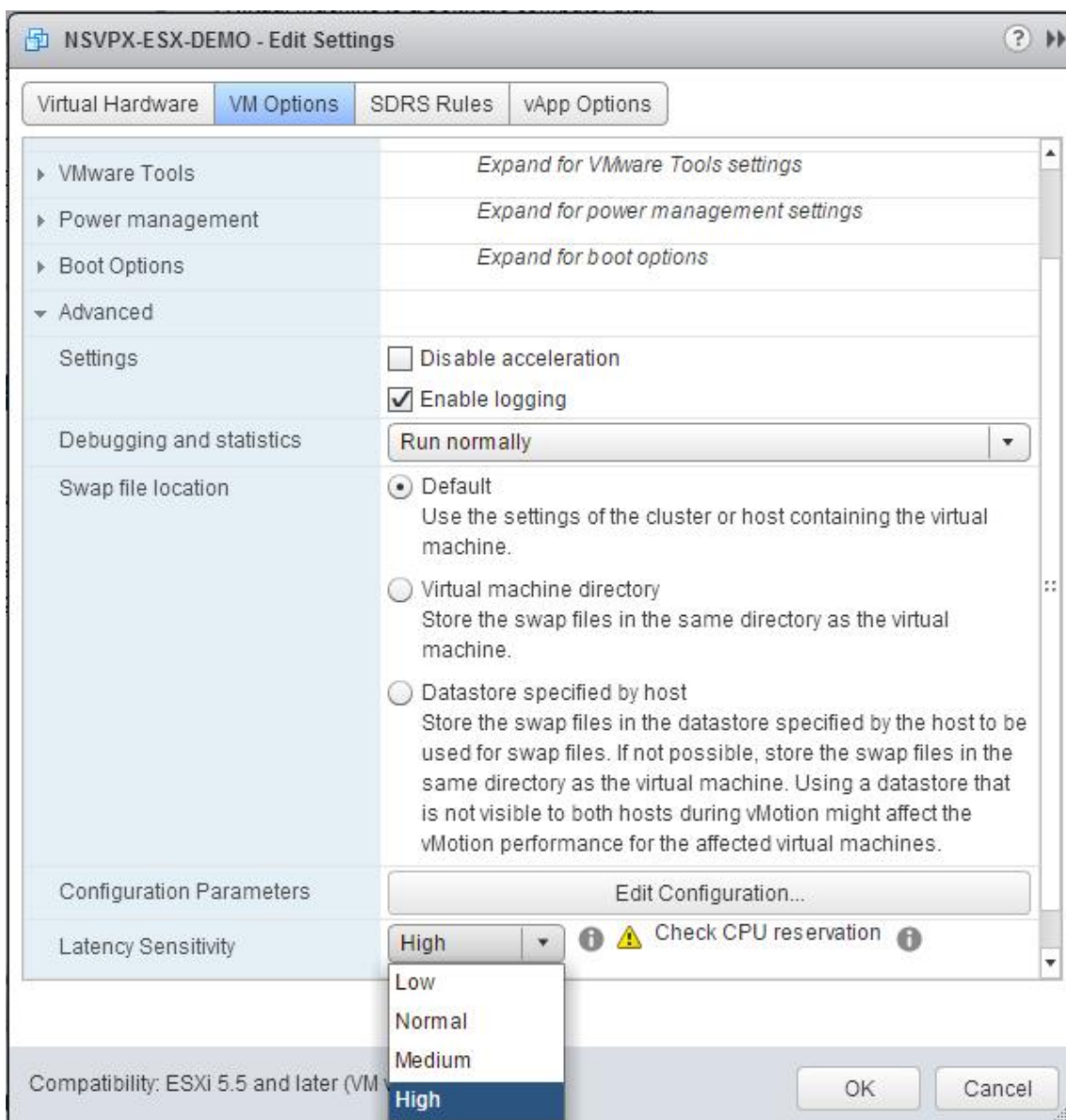


b. En la lista desplegable **Función física**, seleccione el adaptador físico asignado a **Portgroup**



c. **En la lista desplegable** Cambiar la MTU del sistema operativo huésped, **selecciona No permitir.**

9. En el <virtual_appliance>cuadro de diálogo **Editar configuración**, haga clic en la ficha **Opciones de máquina virtual** .
10. En la ficha **Opciones de máquina virtual**, seleccione la sección **Avanzadas** . En la lista desplegable **Sensibilidad de latencia**, seleccione **Alta**.



11. Haz clic en **Aceptar**.
12. Encienda la instancia NetScaler VPX.
13. Una vez que se enciende la instancia de NetScaler VPX, puede utilizar el siguiente comando para verificar la configuración:

```
mostrar resumen de interfaz
```

El resultado debe mostrar todas las interfaces que ha configurado:

```

1 > show interface summary
2 -----
3      Interface  MTU      MAC      Suffix

```

```

4 -----
5 1 0/1 1500 00:0c:29:1b:81:0b NetScaler Virtual
6   Interface
7 2 10/1 1500 00:50:56:9f:0c:6f Intel 82599 10G VF
8   Interface
9 3 10/2 1500 00:50:56:9f:5c:1e Intel 82599 10G VF
10  4 10/3 1500 00:50:56:9f:02:1b Intel 82599 10G VF
11  5 10/4 1500 00:50:56:9f:5a:1d Intel 82599 10G VF
12  6 10/5 1500 00:50:56:9f:4e:0b Intel 82599 10G VF
13  7 L0/1 1500 00:0c:29:1b:81:0b Netscaler Loopback
14  interface
15 Done
16 > show inter 10/1
17 1) Interface 10/1 (Intel 82599 10G VF Interface) #1
18   flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
19   MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
20   h21m53s
21   Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
22   throughput 10000
23   LLDP Mode: NONE, LR Priority: 1024
24
25   RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
26   Stalls(0)
27   TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0)
28   Stalls(0)
29   NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
30   (0)
31   Bandwidth thresholds are not set.
32 Done

```

Configure un NetScaler VPX en el hipervisor ESX para usar Intel QAT para la aceleración de SSL en modo SR-IOV

October 17, 2024

La instancia de NetScaler VPX del hipervisor VMware ESX puede utilizar la tecnología Intel QuickAssist (QAT) para acelerar el rendimiento de NetScaler SSL. Con Intel QAT, todo el procesamiento criptográfico de alta latencia se puede descargar al chip, lo que libera a una o más CPU host para realizar otras tareas.

Anteriormente, todo el procesamiento criptográfico de las rutas de datos de NetScaler se realizaba en el software mediante vCPU host.

Nota:

Actualmente, NetScaler VPX solo admite el modelo de chip C62x de la familia Intel QAT. Esta función se admite a partir de la versión 14.1, compilación 8.50 de NetScaler.

Requisitos previos

- El host ESX se aprovisiona con uno o más chips Intel C62x (QAT).
- NetScaler VPX cumple con los requisitos de hardware de VMware ESX. Para obtener más información, consulte [Instalar una instancia de NetScaler VPX en VMware ESX](#).

Limitaciones

No hay ninguna disposición para reservar unidades criptográficas o ancho de banda para máquinas virtuales individuales. Todas las unidades criptográficas disponibles de cualquier hardware Intel QAT se comparten entre todas las máquinas virtuales que utilizan el hardware QAT.

Configurar el entorno host para usar Intel QAT

1. Descargue e instale el controlador VMware proporcionado por Intel para el modelo de chip de la serie C62x (QAT) en el host de VMware. Para obtener más información sobre las instrucciones de instalación y descarga de los paquetes Intel, consulte el [controlador de la tecnología Intel QuickAssist para VMware](#).
2. Habilite SR-IOV en el host ESX.
3. Cree máquinas virtuales. Al crear una máquina virtual, asigne la cantidad adecuada de dispositivos PCI para cumplir con los requisitos de rendimiento.

Nota:

Cada chip C62x (QAT) puede tener hasta tres terminales PCI independientes. Cada punto final es una colección lógica de VF y comparte el ancho de banda en partes iguales con otros puntos finales PCI del chip. Cada terminal puede tener hasta 16 VF que se muestran como 16 dispositivos PCI. Puede agregar estos dispositivos a la máquina virtual para realizar la aceleración criptográfica mediante el chip QAT.

Puntos a tener en cuenta

- Si el requisito de cifrado de la máquina virtual es utilizar más de un punto final o chip PCI QAT, se recomienda elegir los dispositivos PCI o VF correspondientes de forma rotatoria para tener una distribución simétrica.

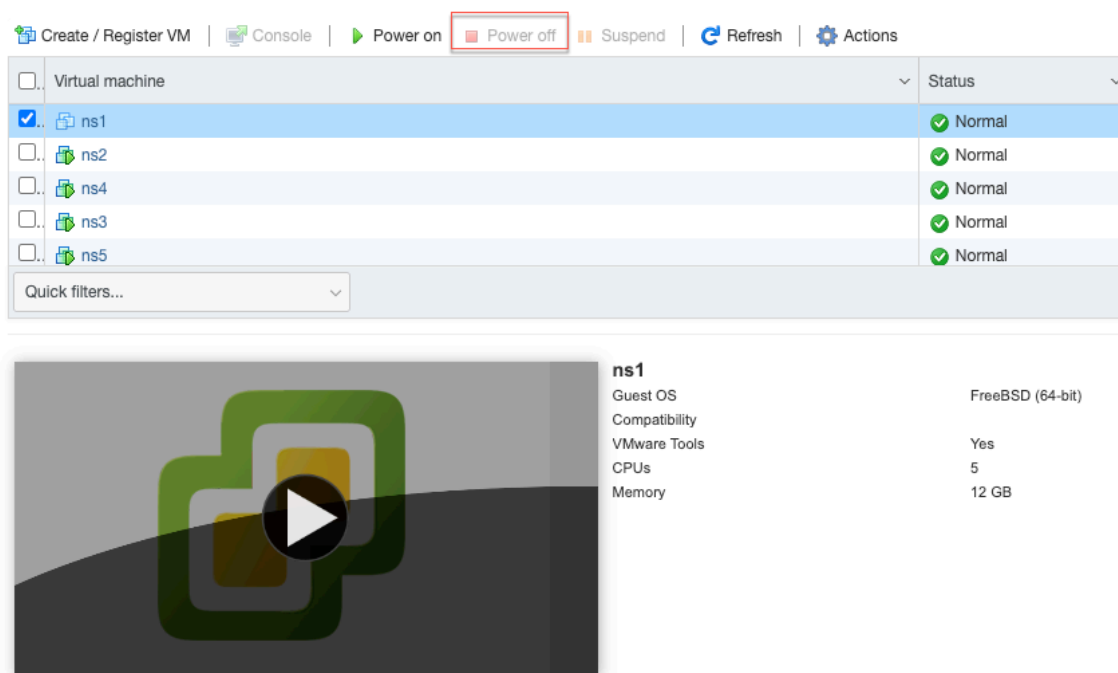
- Se recomienda que la cantidad de dispositivos PCI seleccionados sea igual a la cantidad de vCPU con licencia (sin incluir el recuento de vCPU de administración). Agregar más dispositivos PCI que la cantidad disponible de vCPU no necesariamente mejora el rendimiento.

Ejemplo

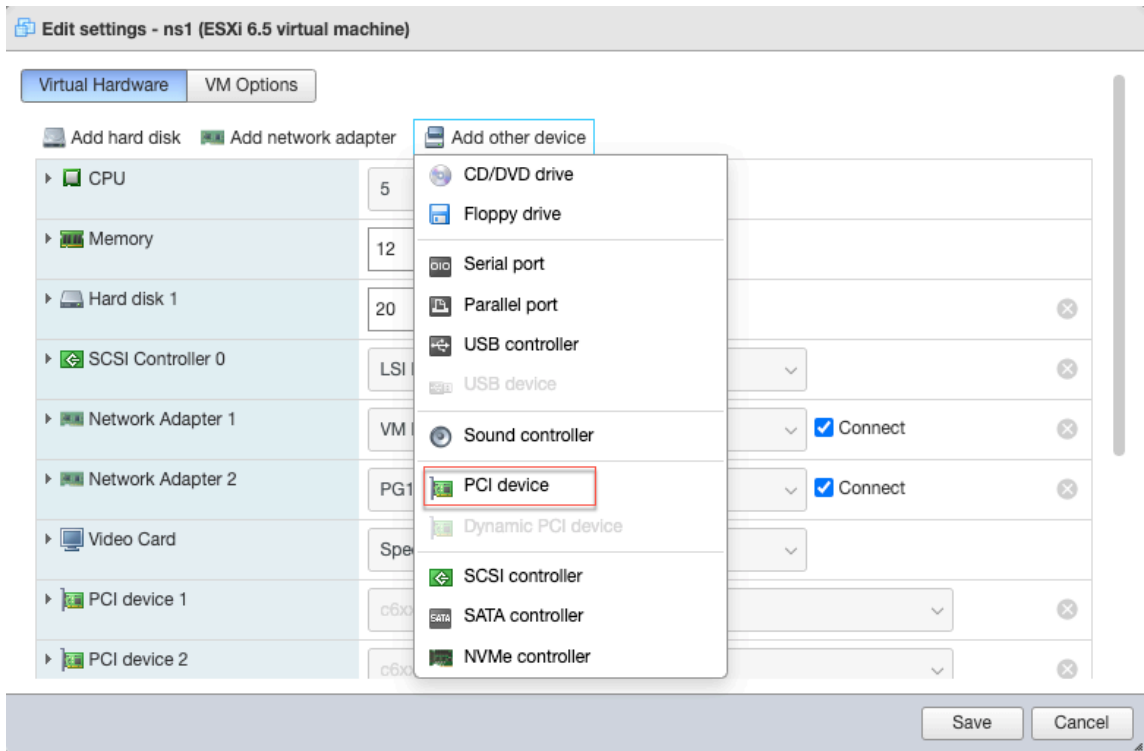
Piense en un host ESX con un chip Intel C62x que tenga 3 terminales. Al aprovisionar una máquina virtual con 6 vCPU, elija 2 máquinas virtuales de cada punto final y asígneles a la máquina virtual. Este tipo de asignación garantiza una distribución eficaz e igualitaria de las unidades criptográficas para la máquina virtual. Del total de vCPU disponibles, de forma predeterminada, una vCPU está reservada para el plano de administración y el resto de las vCPU están disponibles para los PE del plano de datos.

Asigne VF de QAT a VPX mediante el cliente web vSphere

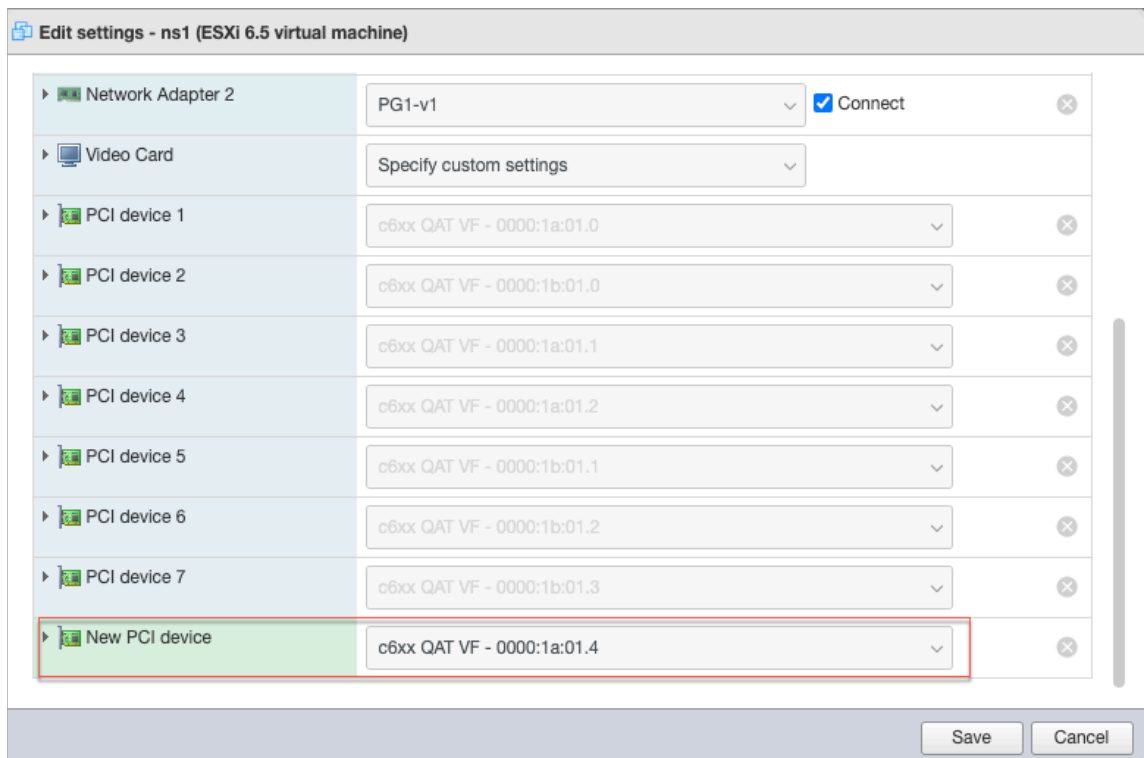
1. En vSphere web client, navegue hasta el host ESX donde se encuentra la máquina virtual y haga clic en Apagar .



2. Vaya a **Acciones > Modificar ajustes > Agregar otro dispositivo** y selecciona dispositivo PCI.



3. Para el dispositivo PCI recién agregado, asigne el C6xx QAT VF y guarde la configuración.



4. Vuelva a encender la máquina virtual.
5. Ejecute el comando `stat ssl` en la CLI de NetScaler para mostrar el resumen de SSL y veri-

fique las tarjetas SSL después de asignar las VF de QAT a VPX.

```
> stat ssl

SSL Summary

# SSL cards present           1
# SSL cards UP                1
SSL engine status            1
```

Acerca de la implementación

Esta implementación se probó con las siguientes especificaciones de componentes:

- **Versión y compilación de NetScaler VPX:** 14.1—8.50
- **Versión de VMware ESXi: 7.0.3 (compilación 20036589)**
- **Versión del controlador Intel C62x QAT para VMware :** 1.5.1.54

Migración de NetScaler VPX de E1000 a interfaces de red SR-IOV o VMXNET3

October 17, 2024

24 de mayo de 2018

Puede configurar las instancias NetScaler VPX de salida que utilizan interfaces de red E1000 para usar interfaces de red SR-IOV o VMXNET3.

Para configurar una instancia de NetScaler VPX existente para utilizar interfaces de red SR-IOV, consulte [Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV](#).

Para configurar una instancia de NetScaler VPX existente para utilizar interfaces de red VMXNET3, consulte [Configurar una instancia de NetScaler VPX para utilizar la interfaz de red VMXNET3](#).

Configurar una instancia de NetScaler VPX para utilizar la interfaz de red de acceso PCI

October 17, 2024

Información general

Tras instalar y configurar una instancia de NetScaler VPX en VMware ESX Server, puede utilizar vSphere Web Client para configurar el dispositivo virtual para que utilice las interfaces de red de transferencia PCI.

La función de transferencia PCI permite a una máquina virtual invitada acceder directamente a dispositivos PCI y PCIe físicos conectados a un host.

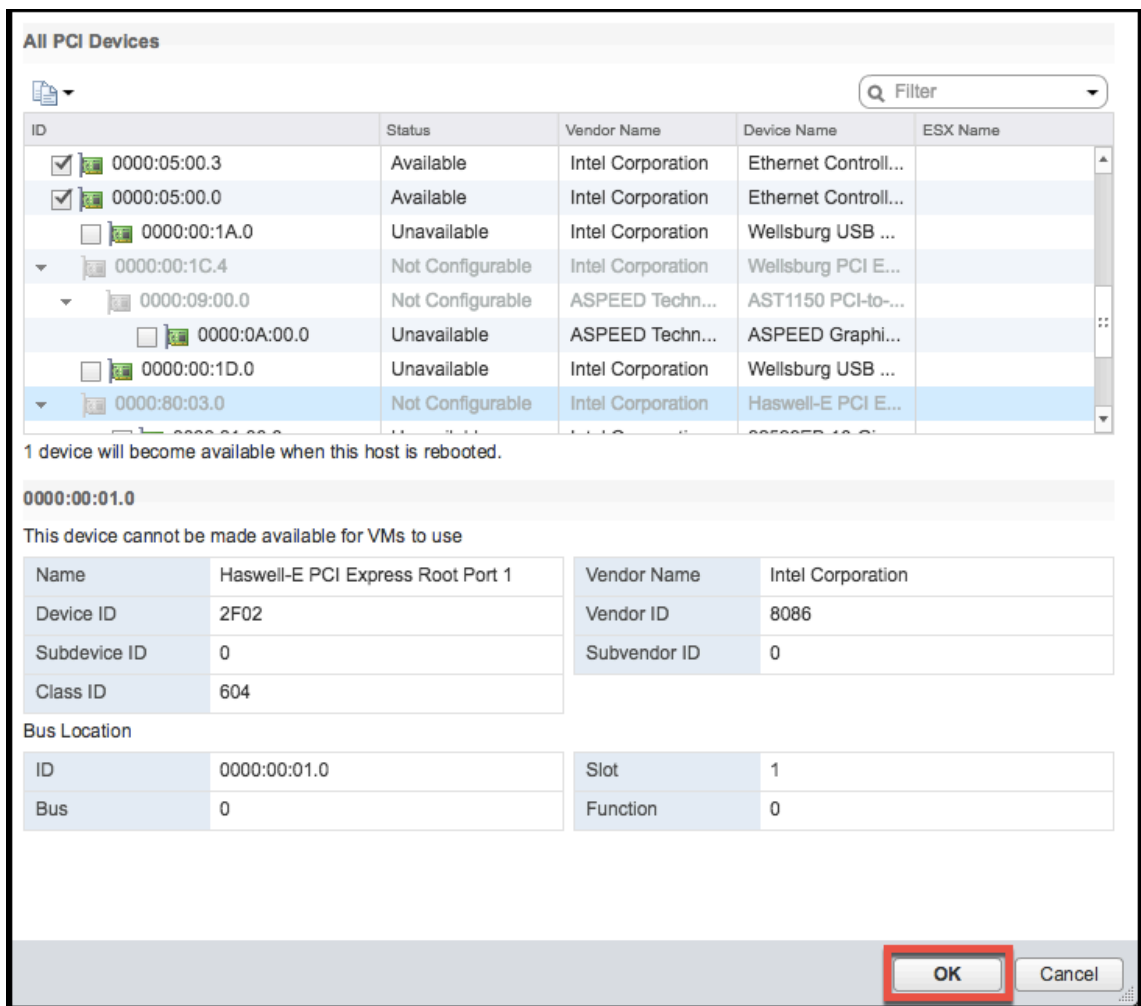
Requisitos previos

- La versión de firmware de la NIC Intel XL710 en el host es 5.04.
- Un dispositivo de transferencia PCI conectado y configurado en el host
- NIC compatibles:
 - NIC Intel X710 10G
 - Tarjeta de interfaz de red Intel XL710 de dos puertos y 40 Gb
 - Tarjeta de interfaz de red Intel XL710 de un solo puerto y 40 Gb
 - Tarjeta de interfaz de red Intel XXV710 de dos puertos y 25 Gb

Configurar dispositivos de paso en un host

Antes de configurar un dispositivo PCI de paso en una máquina virtual, debe configurarlo en la máquina host. Siga estos pasos para configurar dispositivos de paso en un host.

1. Seleccione el host en el panel Navigator de vSphere Web Client.
2. Haga clic en **Administrar > Configuración > Dispositivos PCI**. Se muestran todos los dispositivos de paso disponibles.
3. Haga clic con el botón secundario en el dispositivo que desee configurar y, a continuación, haga clic en **Modificar**.
4. Aparece la ventana **Modificar disponibilidad del dispositivo PCI**.
5. Seleccione los dispositivos que se utilizarán para el paso a través y haga clic en **Aceptar**.

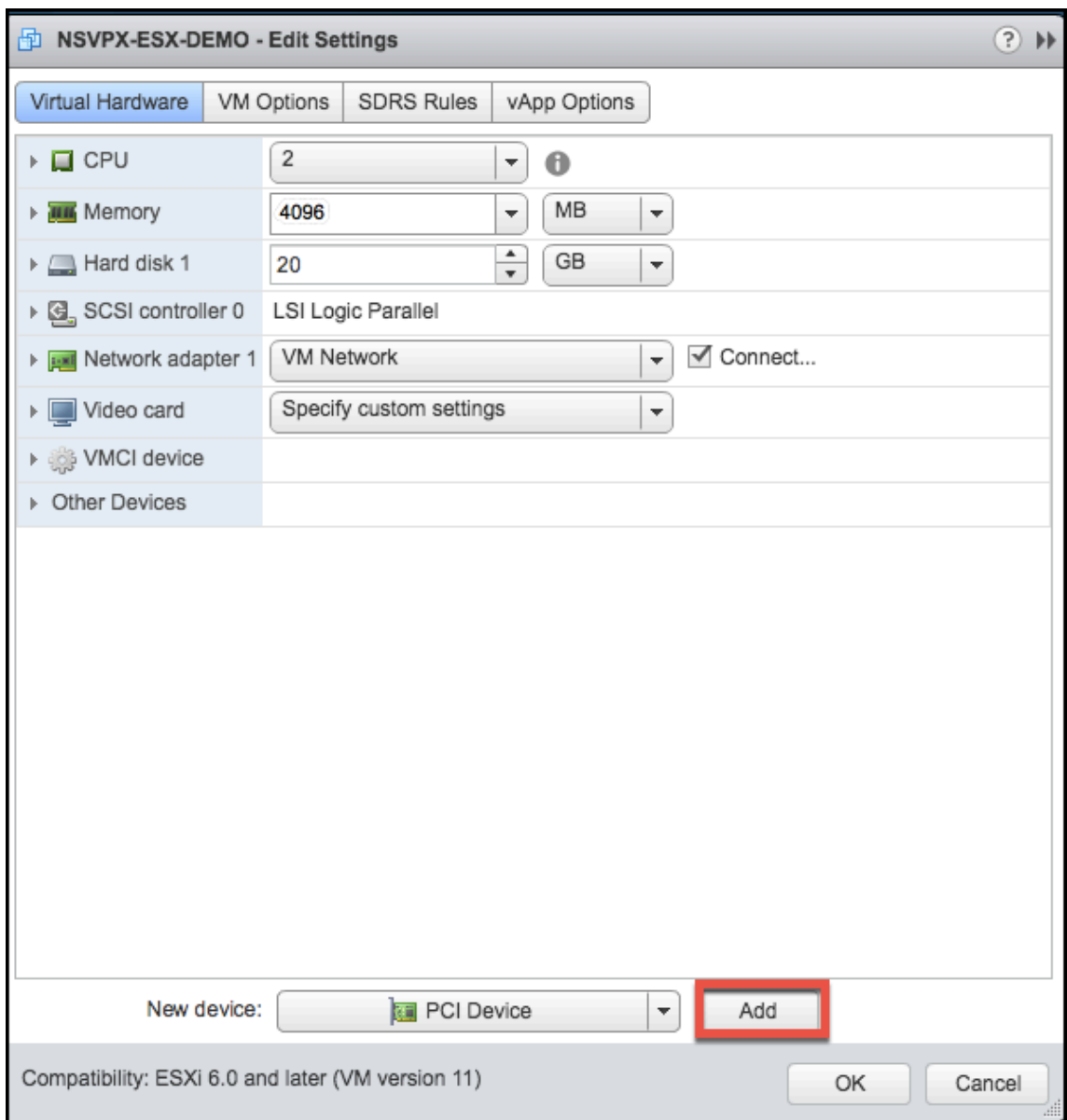


6. Reinicie el equipo host.

Configurar dispositivos de transferencia en una instancia de NetScaler VPX

Siga estos pasos para configurar un dispositivo PCI de transferencia en una instancia de NetScaler VPX.

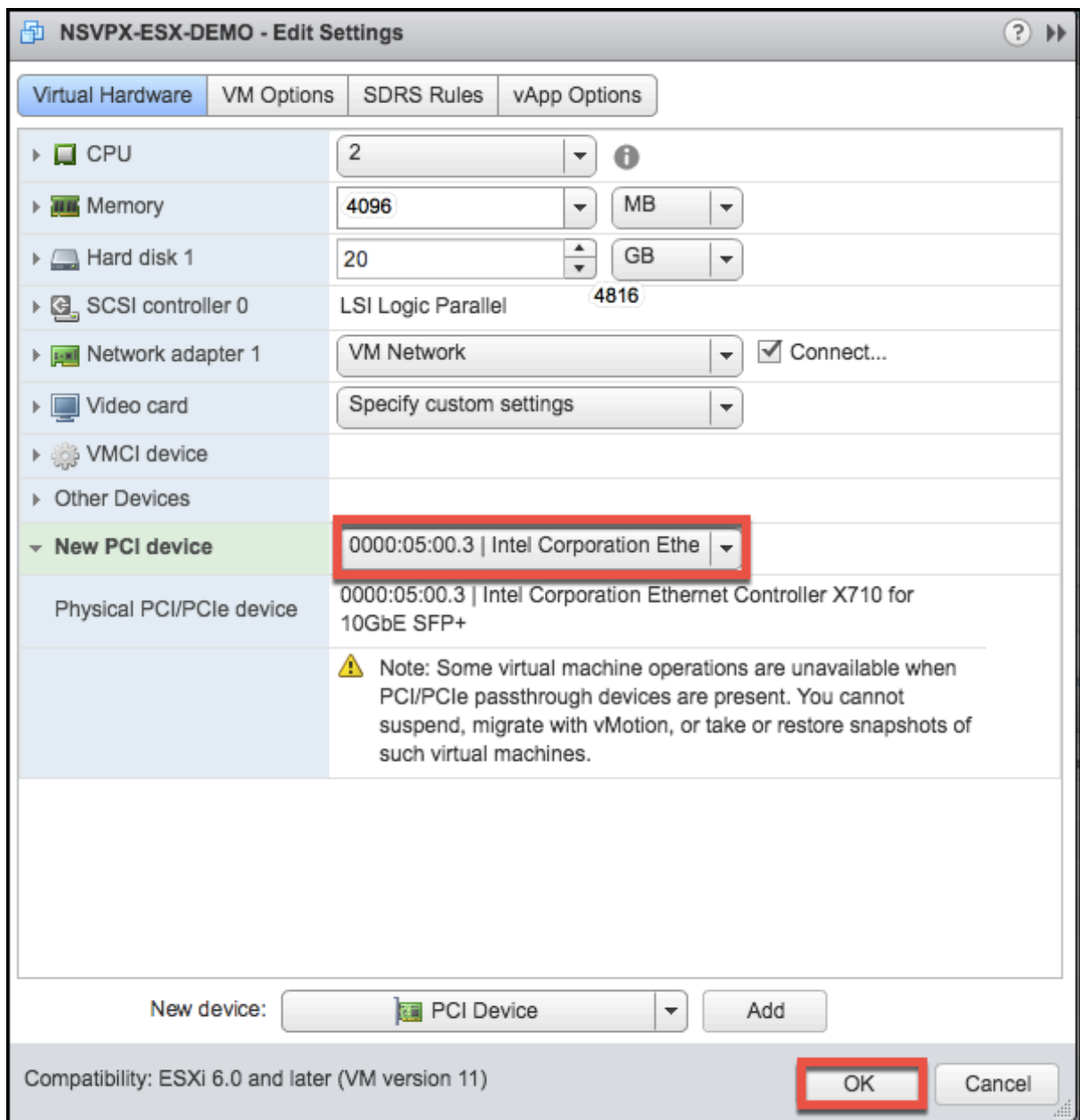
1. Apague la máquina virtual.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Modificar configuración**.
3. En la ficha **Hardware virtual**, seleccione **Dispositivo PCI** en el menú desplegable **Nuevo dispositivo** y haga clic en **Agregar**.



4. Expanda **Nuevo dispositivo PCI** y seleccione el dispositivo de paso a través para conectarse a la máquina virtual en la lista desplegable y haga clic en **Aceptar**.

Nota:

La interfaz de red VMXNET3 y la interfaz de red PCI Passthrough no pueden coexistir.



1. Encienda la máquina virtual invitada.

Ha completado los pasos para configurar NetScaler VPX para que utilice las interfaces de red de transferencia PCI.

Aplicar configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en el hipervisor VMware ESX

October 17, 2024

Puede aplicar las configuraciones de NetScaler VPX durante el primer arranque del dispositivo NetScaler en el hipervisor VMware ESX. Therefore in certain cases, a specific setup or VPX instance is brought up in much lesser time.

Para obtener más información sobre los datos de usuario de prearranque y su formato, consulte [Aplicar configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en la nube](#).

Nota:

To bootstrap using preboot user data in ESX, default gateway config must be passed in `<NS-CONFIG>` section. For more information on the content of the `<NS-CONFIG>` tag, see [Sample `<NS-CONFIG>` section](#).

Sample `<NS-CONFIG>` section:

```
1 <NS-PRE-BOOT-CONFIG>
2
3 <NS-CONFIG>
4   add route 0.0.0.0 0.0.0.0 10.102.38.1
5 </NS-CONFIG>
6
7 <NS-BOOTSTRAP>
8   <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
9   <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
10
11 <MGMT-INTERFACE-CONFIG>
12   <INTERFACE-NUM> eth0 </INTERFACE-NUM>
13   <IP> 10.102.38.216 </IP>
14   <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
15 </MGMT-INTERFACE-CONFIG>
16 </NS-BOOTSTRAP>
17
18 </NS-PRE-BOOT-CONFIG>
```

How to provide preboot user data on ESX hypervisor

Puede proporcionar datos de usuario previos al arranque en el hipervisor ESX desde el cliente web o el cliente vSphere de las dos maneras siguientes:

- Using CD/DVD ISO

- Using OVF Property

Provide user data using CD/DVD ISO

Puede utilizar el cliente VMware vSphere para inyectar datos de usuario en la máquina virtual como una imagen ISO mediante la unidad de CD/DVD.

Siga estos pasos para proporcionar datos de usuario mediante la ISO del CD/DVD:

1. Cree un archivo con un nombre de archivo `userdata` que contenga el contenido de datos de usuario previo al arranque. For more information on the content of the `<NS-CONFIG>` tag, see Sample `<NS-CONFIG>` section.

Nota:

El nombre del archivo debe usarse estrictamente como `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.

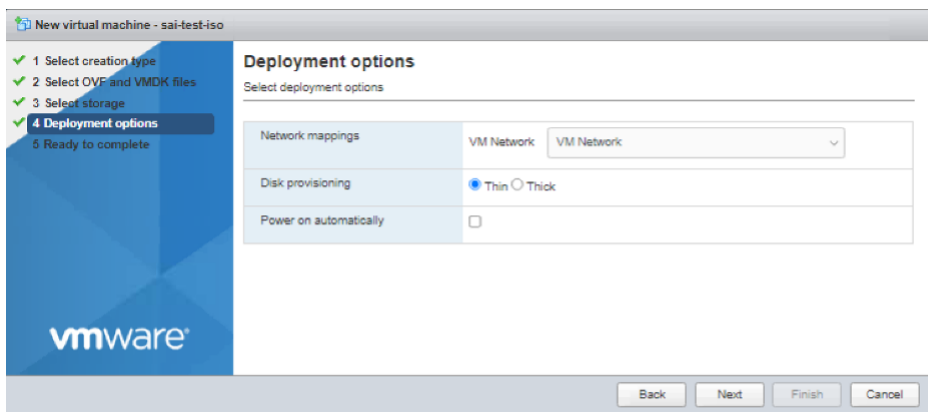
```
1 root@ubuntu:~/sai/14jul2021# ls -l total 4
2 drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
3 root@ubuntu:~/sai/14jul2021#
4 root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
5 -rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
6 root@ubuntu:~/sai/14jul2021# mkisofs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



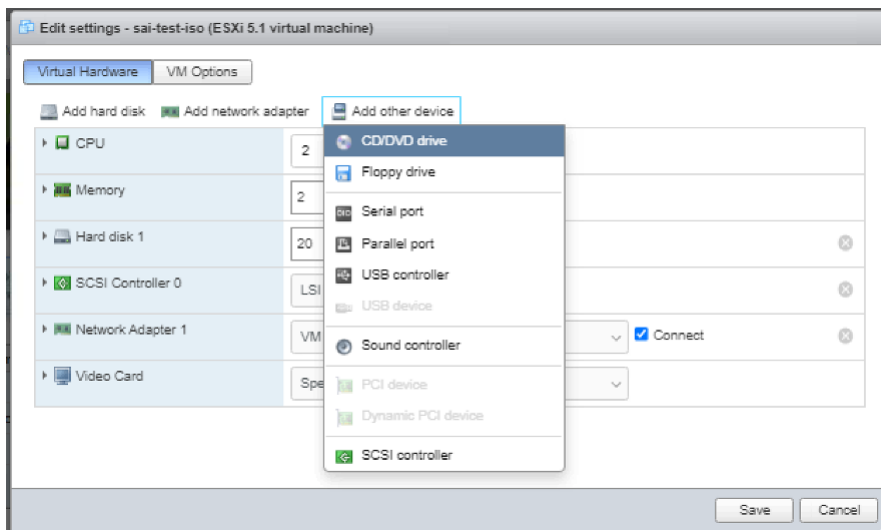
```

20 root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
21 I: -input-charset not specified, using utf-8 (detected in locale
    settings)
22 Total translation table size: 0
23 Total rockridge attributes bytes: 0
24 Total directory bytes: 112
25 Path table size(bytes): 10
26 Max brk space used 0
27 176 extents written (0 MB)
  
```

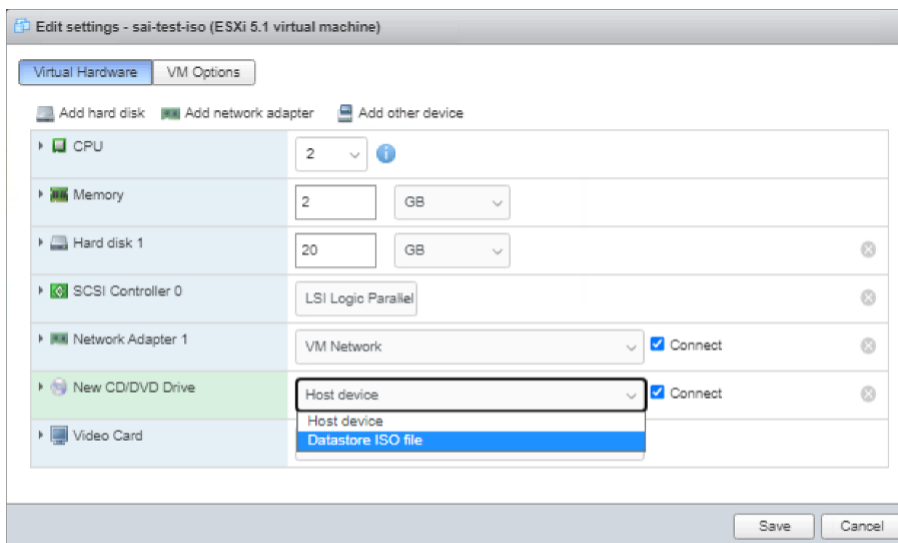
3. Aprovezione la instancia de NetScaler VPX mediante el proceso de implementación estándar para crear la VM. But do not power on the VM automatically.



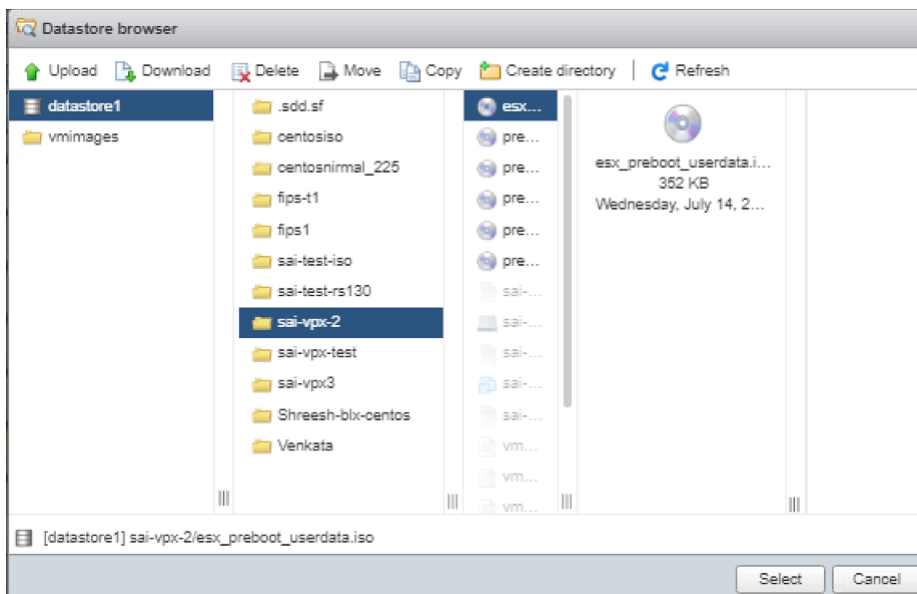
4. After the VM is successfully created, attach the ISO file as CD/DVD drive to the VM.



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



6. Select a Datastore in the vSphere Client.



7. Power on the VM.

Proporcione datos de usuario mediante la propiedad OVF del cliente web ESX

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.

```

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

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

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

```

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

- In Linux, use the following command:

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

Ejemplo

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

```

root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+CglhZGQgcml1dGUgMC4wLjAuMCAw
LjAuMCAwIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KICAgICA8TlMtQk9PVFNuUkFQpGog
ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBU05ZRVVM8L1NLSVAtREVVGQVVMVC1CT09U
U1RSQVA+CjAgICAgICAgICAgIDxORVetQk9PVFNuUkFQLVNlbnVFTkNFP11FUzwwTkVXLUJPT1RT
VFJBU0t1TRVFRVU5DRt4KICAgICAgICAgICAgPE1HTVQtsU5URVJGQUNFLUNPTkZJRz4KICAgICAg
ICAgICAgIDxJTRlRFUkZBQU0tTlVNPiBlcGwIDWwSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L01QPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CjAgICAgICAgICAgPC9NR01ULU1OVEVSRKFD
RS1DT05GSUc+CjAgICA8L05TLUJPT1RTVFJBU05ZRVVM8L1NLSVAtREVVGQVVMVC1CT09UcCg==

```

- Use online tools to encode user data content, for example, Base64 Encode and Decode.
3. Incluye una sección de **productos** en la plantilla de OVF de una instancia de NetScaler VPX en el hipervisor ESX.

Sample Product section:

```

1 <ProductSection>
2
3 <Info>Information about the installed software</Info>
4 <Product>NSVPX-VSK Template</Product>
5 <Vendor>Citrix</Vendor>
6 <VendorUrl>www.citrix.com</VendorUrl>
7 <Category> Preboot Userdata </Category>

```

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

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

```
1 <ProductSection>
2
3 <Info>Information about the installed software</Info>
4 <Product>NSVPX-VSK Template</Product>
5 <Vendor>Citrix</Vendor>
6 <VendorUrl>www.citrix.com</VendorUrl>
7 <Category> Preboot Userdata </Category>
8 <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
  userConfigurable="true"
9   ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+
   Cg lhZGQgc m91dGUgMC4wLjAuMCAw
10 LjAuMC4wIDEwLjEwMi4zOC4x CiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PFVNUUk
11 ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
12 U1RSQVA+
   CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
13 VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtsU5URVJGQUNFLUNPTkZJRz4KICAgIC
14 ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
15 ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
16 QVNLPiAyNTUuMjU1LjE1NS4wIDwvU1VCTkVULU1BU0s+
   CiAgICAgICAgPC9NR01ULU1OVEVSRkFD
17 RS1DT05GSUc+
   CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+
   Cg==">
18
19 <Label>Userdata</Label>
20 <Description> Userdata for ESX VPX </Description>
21 </Property>
22
23 </ProductSection>
```

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

```

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

```

Proporcione datos de usuario mediante la propiedad OVF del cliente ESX vSphere

Siga estos pasos para proporcionar datos de usuario mediante la propiedad OVF del cliente ESX vSphere.

1. Create a file with user data content.

```

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

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

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

```

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

- In Linux, use the following command:

```

1 base64 <userdata-filename> > <output-file>

```

Ejemplo

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

```
root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
LjAuMC4wIDewLjEwMi4zOC4xciAgICA8L05TLUNPTkZJRz4KICAgICA8TlMtQk9PFVNUUkFQPkog
ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVm8L1NLSVAtREVGVQVVMVC1CT09U
UIRSOVA+CiAgICAgICAgICAgIDxORVctQk9PFVNUUkFQLVNFUVVFTkNFP1lFUzwwTkVXLUJPT1RT
VFJBUC1TRVFRU5DRT4KICAgICAgICAgPE1HTVQtsU5URVJGQUFLUNPTkZJRz4KICAgICAgICAg
ICAgICAgIDxJTRFkZBQ0UtTlVNPiBlbGgwIDwvSU5URVJGQUFLU5VT4KICAgICAgICAgICAg
ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L01QPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
QVNLPIAyNTUumjU1Lj11NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULU1OVEVSRkFD
RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
```

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

3. Incluya una sección de **productos** en la plantilla de OVF de una instancia de NetScaler VPX en el hipervisor ESX.

Sample Product section:

```
1 <ProductSection>
2
3 <Info>Information about the installed software</Info>
4 <Product>NSVPX-VSK Template</Product>
5 <Vendor>Citrix</Vendor>
6 <VendorUrl>www.citrix.com</VendorUrl>
7 <Category> Preboot Userdata </Category>
8
9 <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
   userConfigurable="true" ovf:value="">
10
11 <Label>Userdata</Label>
12 <Description> Userdata for ESX VPX </Description>
13 </Property>
14
15 </ProductSection>
```

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

```
1 <ProductSection>
2
3 <Info>Information about the installed software</Info>
4 <Product>NSVPX-VSK Template</Product>
5 <Vendor>Citrix</Vendor>
6 <VendorUrl>www.Citrix.com</VendorUrl>
7 <Category> Preboot Userdata </Category>
8 <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
   userConfigurable="true"
9   ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
   CglhZGQgcm91dGUgMC4wLjAuMCAw
10   LjAuMC4wIDewLjEwMi4zOC4xciAgICA8L05TLUNPTkZJRz4KICAgICA8TlMtQk9PFVNUUkFQPkog
   ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVm8L1NLSVAtREVGVQVVMVC1CT09U
   UIRSOVA+CiAgICAgICAgICAgIDxORVctQk9PFVNUUkFQLVNFUVVFTkNFP1lFUzwwTkVXLUJPT1RT
   VFJBUC1TRVFRU5DRT4KICAgICAgICAgPE1HTVQtsU5URVJGQUFLUNPTkZJRz4KICAgICAgICAg
   ICAgICAgIDxJTRFkZBQ0UtTlVNPiBlbGgwIDwvSU5URVJGQUFLU5VT4KICAgICAgICAgICAg
   ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L01QPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
   QVNLPIAyNTUumjU1Lj11NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULU1OVEVSRkFD
   RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg=="
```

```

11      ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVm8L1NLSVAtrEVGQVVMVC
12      U1RSQVA+
          CiAgICAgICAgICAgIDxORVctQk9PVFNuUkFQLVNFUVVFTkNFPllFUzwwTkVXLUJPT1R
13      VFJBUC1TRVFVRU5DRt4KCiAgICAgICAgPE1HTVQtSU5URVJGQUFLUNPTkZJRz4KICAgIC
14      ICAgICAgIDxJTLRFUkZBQ0UtTVNPiBlDGgwIDwvSU5URVJGQUFLU5VTT4KICAgICAgIC
15      ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk
16      QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
          CiAgICAgICAgPC9NR01ULU1OVEVSRkFD
17      RS1DT05GSUc+
          CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+
          Cg==">
18
19      <Label>Userdata</Label>
20      <Description> Userdata for ESX VPX </Description>
21      </Property>
22
23  </ProductSection>

```

5. Agregue la propiedad `ovf:transport="com.vmware.guestInfo"` a VirtualHardwareSection de la siguiente manera:

```

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

```

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

```

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
> sh ns ver
NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05 (64-bit)
Done
> sh ns ip

```

State	IpAddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	S
1) Enabled	10.102.38.219	0	NetScaler IP	Active	Enabled	Enabled	NA	E

```

Done
> sh route

```

	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Domain	Type
1) C	0.0.0.0	0.0.0.0	10.102.38.1	0	UP	0	STATI
2) NENT	127.0.0.0	255.0.0.0	127.0.0.1	0	UP	0	PERMA
3) T	10.102.38.0	255.255.255.0	10.102.38.219	0	UP	0	DIREC

```

Done

```

Instalación de una instancia NetScaler VPX en la nube de VMware en AWS

October 17, 2024

VMware Cloud (VMC) en AWS le permite crear centros de datos definidos por software (SDDC) en la nube en AWS con el número deseado de hosts ESX. El VMC de AWS admite las implementaciones de NetScaler VPX. VMC proporciona una interfaz de usuario igual que vCenter en las instalaciones. Funciona de manera idéntica a las implementaciones de NetScaler VPX basadas en ESX.

Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Debe estar presente un SDDC de VMware con al menos un host.
- Descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree segmentos de red adecuados en VMware SDDC a los que se conectan las máquinas virtuales.
- Obtenga archivos de licencias VPX. Para obtener más información sobre las licencias de instancias de NetScaler VPX, consulte la *Guía de licencias de NetScaler VPX* en en-us/licensing/licensing-guide-for-netscaler.html.

Requisitos de hardware en la nube

En la tabla siguiente se enumeran los recursos informáticos virtuales que el SDDC de VMware debe proporcionar para cada dispositivo virtual VPX nCore.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de NetScaler VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En VMware SDDC, puede instalar un máximo de 10 interfaces de red virtuales si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

Nota:

Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso en producción del dispositivo virtual VPX, debe reservarse la asignación de memoria completa.

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. En la siguiente tabla se describen los requisitos mínimos del sistema.

Tabla 2. Requisitos mínimos del sistema para la instalación de herramientas OVF

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Guía del usuario de herramientas OVF” en http://kb.vmware.com/ .
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC	NIC de 100 Mbps o más rápido

Para obtener información sobre la instalación de OVF, busque el archivo PDF “Guía del usuario de la herramienta OVF” en <http://kb.vmware.com/>.

Descarga de los archivos de configuración de NetScaler VPX

El paquete de configuración de instancias NetScaler VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en <http://www.citrix.com>. Haga clic en el **vínculo Nuevos usuarios** y siga las instrucciones para crear una nueva cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

Citrix.com > **Descargas > NetScaler > Dispositivos virtuales.**

Copie los siguientes archivos en una estación de trabajo de la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (por ejemplo, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (por ejemplo, NSVPX-ESX-13.0-79.64.mf)

Instalar una instancia de NetScaler VPX en la nube de VMware

Después de instalar y configurar VMware SDDC, puede usar el SDDC para instalar dispositivos virtuales en la nube de VMware. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el SDDC.

Para instalar instancias de NetScaler VPX en la nube de VMware, siga estos pasos:

1. Abra VMware SDDC en su estación de trabajo.
2. En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en Iniciar sesión.
3. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
4. En el cuadro de diálogo **Implementar plantilla de OVF**, en **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias de NetScaler VPX, seleccione el archivo .ovf y haga clic en **Siguiente**.

Nota: De forma predeterminada, la instancia de NetScaler VPX utiliza interfaces de red E1000. Para implementar ADC con la interfaz VMXNET3, modifique el OVF para utilizar la interfaz VMXNET3 en lugar de E1000.

5. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el SDDC de VMware. Haga clic en **Siguiente** para iniciar la instalación de un dispositivo virtual en VMware SDDC.
6. Ya está listo para iniciar la instancia de NetScaler VPX. En el panel de navegación, seleccione la instancia de NetScaler VPX que ha instalado y, en el menú contextual, seleccione **Encendido**. Haga clic en la ficha **Console** para emular un puerto de consola.
7. Si quiere instalar otro dispositivo virtual, repita desde el paso 6.
8. Especifique la dirección IP de administración del mismo segmento seleccionado para ser la red de administración. Se utiliza la misma subred para la puerta de enlace.
9. VMware SDDC requiere que las reglas de NAT y firewall se creen explícitamente para todas las direcciones IP privadas pertenecientes a segmentos de red.

Instale una instancia de NetScaler VPX en el servidor Microsoft Hyper-V

October 17, 2024

Para instalar instancias de NetScaler VPX en Microsoft Windows Server, primero debe instalar Windows Server con la función Hyper-V habilitada, en una máquina con los recursos del sistema adecuados. Cuando instale el rol Hyper-V, debe especificar las tarjetas de interfaz de red (NIC) en el servidor que Hyper-V usa para crear las redes virtuales. Puede reservar algunas tarjetas para el host. Utilice el Administrador de Hyper-V para realizar la instalación de la instancia VPX de NetScaler.

La instancia VPX de NetScaler para Hyper-V se entrega en formato de disco duro virtual (VHD). Incluye la configuración predeterminada para elementos como CPU, interfaces de red y tamaño y formato del disco duro. Tras instalar la instancia VPX de NetScaler, puede configurar los adaptadores de red en un dispositivo virtual, agregar NIC virtuales y, a continuación, asignar la dirección IP, la máscara de subred y la puerta de enlace de NetScaler y completar la configuración básica del dispositivo virtual.

Después de la configuración inicial de la instancia VPX, si quiere actualizar el dispositivo a la última versión de software, consulte [Actualización de un dispositivo independiente NetScaler VPX](#)

Nota:

El protocolo de sistema intermedio a sistema intermedio (ISIS) no es compatible con el dispositivo virtual NetScaler VPX alojado en la plataforma HyperV-2012.

Requisitos previos para instalar la instancia NetScaler VPX en servidores de Microsoft

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Habilite la función Hyper-V en los servidores de Windows. Para obtener más información, consulte [http://technet.microsoft.com/en-us/library/ee344837\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx).
- Descargue los archivos de configuración del dispositivo virtual.
- Obtenga los archivos de licencia de la instancia VPX de NetScaler. Para obtener más información sobre las licencias de instancia de NetScaler VPX, consulte la *Guía de licencias de NetScaler VPX* en https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US.

Requisitos de hardware de servidores de Microsoft

En la siguiente tabla se describen los requisitos mínimos del sistema para los servidores de Microsoft.

Tabla 2. Requisitos mínimos del sistema para los servidores de Microsoft

Componente	Requisito
CPU	Procesador de 64 bits de 1,4 GHz
RAM	8 GB
Espacio en disco	32 GB o más

La siguiente tabla enumera los recursos informáticos virtuales para cada Instancia de NetScaler VPX.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de NetScaler VPX

Componente	Requisito
RAM	4 GB
CPU virtual	2
Espacio en disco	20 GB
Interfaces de red virtual	1

Descargue los archivos de configuración de NetScaler VPX

La instancia VPX de NetScaler para Hyper-V se entrega en formato de disco duro virtual (VHD). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en <http://www.citrix.com>, haga clic en **Iniciar sesión > Mi cuenta > Crear cuenta de Citrix** y siga las instrucciones para crear una cuenta Citrix.

Para descargar los archivos de configuración de instancias de NetScaler VPX, siga estos pasos:

1. Desde un explorador web, vaya a <http://www.citrix.com/>.
2. Inicie sesión con su nombre de usuario y contraseña.
3. Haga clic en **Descargas**.
4. En **el menú desplegable Seleccionar un producto**, seleccione **NetScaler (NetScaler ADC)**.
5. En **NetScaler Release X. X > Virtual Appliances**, haga clic en **NetScaler VPX Release X. X**
6. Descargue el archivo comprimido en su servidor.

Instalar la instancia VPX de NetScaler en los servidores de Microsoft

Una vez que haya habilitado el rol de Hyper-V en Microsoft Server y haya extraído los archivos del dispositivo virtual, puede usar el Administrador de Hyper-V para instalar la instancia VPX de NetScaler. Después de importar la máquina virtual, debe configurar las NIC virtuales asociándolas a las redes virtuales creadas por Hyper-V.

Puede configurar un máximo de ocho NIC virtuales. Incluso si la NIC física está DESACTIVADA, el dispositivo virtual asume que la NIC virtual está ACTIVADA, ya que puede seguir comunicándose con los demás dispositivos virtuales del mismo host (servidor).

Nota:

No puede cambiar ninguna configuración mientras el dispositivo virtual esté en ejecución. Apague el dispositivo virtual y, a continuación, realice los cambios.

Para instalar la instancia de NetScaler VPX en Microsoft Server mediante el Administrador de Hyper-V:

1. Para iniciar el Administrador de Hyper-V, haga clic en **Inicio**, seleccione **Herramientas administrativas** y, a continuación, haga clic en **Administrador de Hyper-V**.
2. En el panel de navegación, en **Hyper-V Manager**, seleccione el servidor en el que quiere instalar la instancia de NetScaler VPX.
3. En el menú **Acción**, haga clic en **Importar máquina virtual**.
4. En el cuadro de diálogo **Importar máquina virtual**, en **Ubicación**, especifique la ruta de la carpeta que contiene los archivos de software de la instancia NetScaler VPX y, a continuación, seleccione **Copiar la máquina virtual (crear un nuevo ID único)**. Esta carpeta es la carpeta principal que contiene las carpetas Instantáneas, Discos duros virtuales y Máquinas virtuales.

Nota:

Si ha recibido un archivo comprimido, asegúrese de extraer los archivos en una carpeta antes de especificar la ruta de acceso a la carpeta.

1. Haga clic en **Import**.
2. Compruebe que el dispositivo virtual que ha importado aparece en **Máquinas virtuales**.
3. Para instalar otro dispositivo virtual, repita los pasos **2 a 6**.

Importante:

Asegúrese de extraer los archivos a una carpeta diferente en el paso **4**.

Aprovisionamiento automático de una instancia de NetScaler VPX en Hyper-V

El aprovisionamiento automático de la instancia VPX de NetScaler es opcional. Si no se realiza el aprovisionamiento automático, el dispositivo virtual ofrece una opción para configurar la dirección IP, etc.

Para aprovisionar automáticamente una instancia de NetScaler VPX en Hyper-V, siga estos pasos.

1. Cree una imagen ISO compatible con la norma ISO9660 mediante el archivo xml tal como se muestra en el ejemplo. Asegúrese de que el nombre del archivo xml sea **userdata**.

Puede crear un archivo ISO a partir de un archivo XML mediante:

- Cualquier herramienta de procesamiento de imágenes, como PowerISO.
- Comando `mkisofs` en Linux.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
3 <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment
  /1`"
4
5 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance`"
6
7 oe:id=""
8
9 xmlns="http://schemas.dmtf.org/ovf/environment/1`">
10
11 <PlatformSection>
12
13 <Kind>HYPER-V</Kind>
14
15 <Version>2013.1</Version>
16
17 <Vendor>CITRIX</Vendor>
18
19 <Locale>en</Locale>
20
21 </PlatformSection>
22
23 <PropertySection>
24
25 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
  1.0"/>
26
27 <Property oe:key="com.citrix.netscaler.platform" oe:value="
  NS1000V"/>
28
29 <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="
  cisco-orch-env"/>
30
31 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
  10.102.100.122"/>
```

```
32
33 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
    255.255.255.128"/>
34
35 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
    10.102.100.67"/></PropertySection>
36
37 </Environment>
```

2. Copie la imagen ISO al servidor de Hyper-v.
3. Seleccione el dispositivo virtual que ha importado y, a continuación, en el menú **Acción**, seleccione **Configuración**. También puede seleccionar el dispositivo virtual y, a continuación, hacer clic con el botón derecho y seleccionar **Configuración**. Aparece la ventana **Configuración** del dispositivo virtual seleccionado.
4. En la ventana **Configuración**, en la sección de hardware, haga clic en **Controlador IDE**.
5. En el panel de la derecha de la ventana, seleccione **Unidad de DVD** y haga clic en **Agregar**. La unidad de DVD se agrega en la sección **Controlador IDE** en el panel de la ventana izquierda.
6. Seleccione la **unidad de DVD** agregada en el paso 5. En el panel de la derecha de la ventana, seleccione el **botón de opción Archivo de imagen** y haga clic en **Examinar** y seleccione la imagen ISO que copió en el servidor de Hyper-V, en el paso 2.
7. Haga clic en **Aplicar**.

Nota:

La instancia del dispositivo virtual aparece en la dirección IP predeterminada cuando:

- La unidad de DVD está conectada y no se proporciona el archivo ISO.
- El archivo ISO no incluye el archivo de datos del usuario.
- El nombre o el formato del archivo de datos de usuario no son correctos.

Para configurar las NIC virtuales en la instancia VPX de NetScaler, siga estos pasos:

1. Seleccione el dispositivo virtual que ha importado y, a continuación, en el menú **Acción**, seleccione **Configuración**.
2. En el cuadro de diálogo **Configuración de <nombre del dispositivo virtual>**, haga clic en **Agregar hardware** en el panel de la izquierda.
3. En el panel de la derecha, en la lista de dispositivos, seleccione **Adaptador de red**.
4. Haga clic en **Agregar**.
5. Compruebe que el **adaptador de red (no conectado)** aparezca en el panel de la izquierda.
6. Seleccione el adaptador de red en el panel de la izquierda.
7. En el panel de la derecha, en el menú **Red**, seleccione la red virtual a la que quiere conectar el adaptador.

8. Para seleccionar la red virtual para otros adaptadores de red que quiera usar, repita los pasos **6** y **7**.
9. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Para configurar la instancia VPX de NetScaler:

1. Haga clic con el botón secundario en el dispositivo virtual que instaló anteriormente y, a continuación, seleccione **Iniciar**.
2. Acceda a la consola haciendo doble clic en el dispositivo virtual.
3. Escriba la dirección IP, la máscara de subred y la puerta de enlace de NetScaler para su dispositivo virtual.

Ha completado la configuración básica de su dispositivo virtual. Escriba la dirección IP en un navegador web para acceder al dispositivo virtual.

Nota:

También puede utilizar la plantilla de máquina virtual (VM) para aprovisionar la instancia de NetScaler VPX mediante SCVMM.

Si utiliza la solución de agrupación de NIC Microsoft Hyper-V con instancias NetScaler VPX, consulte el artículo [CTX224494](#) para obtener más información.

Instalar una instancia de NetScaler VPX en la plataforma Linux-KVM

October 17, 2024

Para configurar un NetScaler VPX para la plataforma Linux-KVM, puede utilizar la aplicación gráfica Virtual Machine Manager (Virtual Manager). Si prefiere la línea de comandos Linux-KVM, puede utilizar el `virsh` programa.

El sistema operativo Linux host debe instalarse en el hardware adecuado mediante herramientas de virtualización como el módulo KVM y QEMU. El número de máquinas virtuales (VM) que se pueden implementar en el Hypervisor depende del requisito de la aplicación y del hardware elegido.

Después de aprovisionar una instancia NetScaler VPX, puede agregar más interfaces.

Limitaciones y directrices de uso

Recomendaciones generales

Para evitar comportamientos impredecibles, aplique las siguientes recomendaciones:

- No cambie la MTU de la interfaz de VNet asociada a la VM VPX. Apague la VM VPX antes de modificar los parámetros de configuración, como los modos de interfaz o la CPU.
- No fuerce el apagado de la VM VPX. Es decir, no use el comando **Force off**.
- Cualquier configuración realizada en el host Linux puede o no ser persistente, en función de la configuración de distribución de Linux. Puede optar por hacer que estas configuraciones sean persistentes para garantizar un comportamiento coherente en todos los reinicios del sistema operativo Linux host.
- El paquete NetScaler debe ser único para cada una de las instancias de NetScaler VPX aprovisionadas.

Limitaciones

- No se admite la migración en vivo de una instancia VPX que se ejecuta en KVM.

Requisitos previos para instalar una instancia de NetScaler VPX en la plataforma Linux-KVM

October 17, 2024

Compruebe los requisitos mínimos del sistema para un servidor Linux-KVM que se ejecuta en una instancia NetScaler VPX.

Requisito de CPU:

- Procesadores x86 de 64 bits con la función de virtualización de hardware incluida en los procesadores Intel VT-X.

Para comprobar si la CPU es compatible con el host Linux, introduzca el siguiente comando en el símbolo del shell de Linux del host:

```
1 *.egrep '^flags.*(vmx|svm)' /proc/cpuinfo*
```

Si la configuración del **BIOS** de la extensión anterior está inhabilitada, debe habilitarla en el BIOS.

- Proporcione al menos 2 núcleos de CPU al host Linux.
- No hay ninguna recomendación específica para la velocidad del procesador, pero mayor es la velocidad, mejor será el rendimiento de la aplicación de VM.

Requisito de memoria (RAM):

Mínimo 4 GB para el kernel Linux host. Agregue más memoria según lo requieran las máquinas virtuales.

Requisito de disco duro:

Calcule el espacio para los requisitos del kernel y VM de host Linux. Una sola máquina virtual NetScaler VPX requiere 20 GB de espacio en disco.

Requisitos de software

El núcleo host utilizado debe ser un núcleo Linux de 64 bits, versión 2.6.20 o posterior, con todas las herramientas de virtualización. Citrix recomienda los núcleos más nuevos, como 3.6.11-4 y versiones posteriores.

Muchas distribuciones de Linux, como Red Hat, CentOS y Fedora, han probado versiones del núcleo y herramientas de virtualización asociadas.

Requisitos de hardware de VM invitada

NetScaler VPX admite los tipos de disco duro IDE y VirtIO. El tipo de disco duro se configuró en el archivo XML, que forma parte del paquete NetScaler.

Requisitos de red

NetScaler VPX admite las interfaces de red VirtIO paravirtualizadas, SR-IOV y PCI Passthrough.

Para obtener más información acerca de las interfaces de red compatibles, consulte:

- [Aprovisione la instancia de NetScaler VPX mediante el Administrador de máquinas virtuales](#)
- [Configurar una instancia de NetScaler VPX para usar las interfaces de red SR-IOV](#)
- [Configurar una instancia de NetScaler VPX para utilizar las interfaces de red de transferencia PCI](#)

Interfaz y modos de origen

El tipo de dispositivo de origen puede ser Bridge o MacVtap. En MacVtap, son posibles cuatro modos: VEPA, Bridge, Privado y Pass-through. Compruebe los tipos de interfaces que puede utilizar y los tipos de tráfico admitidos, según lo siguiente:

Puente:

- Puente Linux.
- [Ebtables](#) y la [iptables](#) configuración del host Linux puede filtrar el tráfico en el puente si no elige la configuración correcta o inhabilita [IPtable](#) los servicios.

MacVtap (modo VEPA):

- Mejor rendimiento que un puente.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las VM.
- Comunicación entre VM mediante el mismo
- dispositivo inferior solo es posible si el conmutador ascendente o descendente admite el modo VEPA.

MacVTap (modo privado):

- Mejor rendimiento que un puente.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las VM.
- No es posible la comunicación entre VM mediante el mismo dispositivo inferior.

MacVTap (modo puente):

- Mejor en comparación con bridge.
- Las interfaces del mismo dispositivo inferior se pueden compartir entre las máquinas virtuales.
- Es posible la comunicación entre VM mediante el mismo dispositivo inferior, si el enlace inferior del dispositivo es UP.

MacVTap (modo de paso):

- Mejor en comparación con bridge.
- Las interfaces del mismo dispositivo inferior no se pueden compartir entre las máquinas virtuales.
- Solo una VM puede usar el dispositivo inferior.

Nota:

Para obtener el mejor rendimiento de la instancia VPX, asegúrese de que las capacidades `gro` y `lro` estén desactivadas en las interfaces de origen.

Propiedades de las interfaces de origen

Asegúrese de desactivar las capacidades genérico-receive-offload (`gro`) y large-receive-offload (`lro`) de las interfaces de origen. Para desactivar las `lro` capacidades `gro` y, ejecute los siguientes comandos en el símbolo del shell de Linux del host.

```
ethtool -K eth6 gro apagado ethool -K eth6 lro desactivado
```

Ejemplo:

```
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@localhost ~]#

```

Ejemplo:

Si el puente Linux host se utiliza como dispositivo de origen, como en el ejemplo siguiente, y **lro** las capacidades deben desactivarse en las interfaces de VNet, que son las interfaces virtuales que conectan el host a las máquinas virtuales invitadas.

```

1 [root@localhost ~]# brctl show eth6_br
2
3 bridge name      bridge id          STP enabled interfaces
4
5 eth6_br          8000.00e0ed1861ae  no                eth6
6
7
8
9
10
11 [root@localhost ~]#

```

En el ejemplo anterior, las dos interfaces virtuales se derivan de **eth6_br** y se representan como **vnet0** y **vnet2**. Ejecute los siguientes comandos para desactivar **gro** y activar **lro** las capacidades en estas 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

```

Modo promiscuo

El modo promiscuo debe estar habilitado para que funcionen las siguientes funciones:

- Modo L2
- Procesamiento de tráfico de multidifusión
- Emisión
- Tráfico IPv6
- MAC virtual
- Redirección dinámica

Utilice el siguiente comando para habilitar el modo promiscuo.

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

Módulo requerido

Para un mejor rendimiento de red, asegúrese de que el módulo `vhost_net` esté presente en el host Linux. Para comprobar la existencia del módulo `vhost_net`, ejecute el siguiente comando en el host Linux:

```
1 lsmod | grep "vhost\_net"
```

Si `vhost_net` aún no se está ejecutando, introduzca el siguiente comando para ejecutarlo:

```
1 modprobe vhost\_net
```

Aprovisione la instancia NetScaler VPX mediante OpenStack

October 17, 2024

Puede aprovisionar una instancia NetScaler VPX en un entorno OpenStack mediante el comando de **arranque Nova** (CLI de OpenStack) u Horizon (panel de OpenStack).

Aprovisionar una instancia VPX, opcionalmente implica el uso de datos de la unidad de configuración. La unidad de configuración es una unidad de configuración especial que se conecta a la instancia como un dispositivo de CD-ROM cuando se inicia. Esta unidad de configuración se puede utilizar para pasar la configuración de red, como la dirección IP de administración, la máscara de red, la Gateway predeterminada y para inyectar scripts de clientes.

En un dispositivo NetScaler, el mecanismo de autenticación predeterminado se basa en contraseña. Ahora, el mecanismo de autenticación de pares de claves SSH es compatible con instancias NetScaler VPX en el entorno OpenStack.

El par de claves (clave pública y clave privada) se genera antes de utilizar el mecanismo de criptografía de clave pública. Puede utilizar distintos mecanismos, como Horizon, Puttygen.exe para Windows y `ssh-keygen` para el entorno Linux, para generar el par de claves. Consulte la documentación en línea de los respectivos mecanismos para obtener más información sobre la generación de pares de claves.

Una vez disponible un par de claves, copie la clave privada en una ubicación segura a la que tienen acceso las personas autorizadas. En OpenStack, la clave pública se puede implementar en una instancia VPX mediante el comando de arranque Horizon o Nova. Cuando se aprovisiona una instancia VPX mediante OpenStack, primero detecta que la instancia se está iniciando en un entorno OpenStack leyendo una cadena de BIOS específica. Esta cadena es "OpenStack Foundation" y para las distribuciones de Red Hat Linux se almacena en `/etc/nova/release`. Se trata de un mecanismo estándar que está disponible en todas las implementaciones de OpenStack basadas en la plataforma de hipervisor KVM. La unidad debe tener una etiqueta OpenStack específica.

Si se detecta la unidad de configuración, la instancia intenta leer la configuración de red, los scripts personalizados y el par de claves SSH si se proporciona.

Archivo de datos de usuario

La instancia NetScaler VPX utiliza un archivo OVF personalizado, también conocido como archivo de datos de usuario, para inyectar la configuración de red, scripts personalizados. Este archivo se proporciona como parte de la unidad de configuración. A continuación se muestra un ejemplo de un archivo OVF personalizado.

```
1  `` `
2  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3  <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
4  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5  oe:id=""
6  xmlns="http://schemas.dmtf.org/ovf/environment/1"
7  xmlns:cs="http://schemas.citrix.com/openstack">
```

```
8 <PlatformSection>
9 <Kind></Kind>
10 <Version>2016.1</Version>
11 <Vendor>VPX</Vendor>
12 <Locale>en</Locale>
13 </PlatformSection>
14 <PropertySection>
15 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
16 <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
17 <Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
    orch-env"/>
18 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
    />
19 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
    255.255.255.0"/>
20 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
    10.1.2.1"/>
21 </PropertySection>
22 <cs:ScriptSection>
23 <cs:Version>1.0</cs:Version>
24 <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack
    " xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
25 <Scripts>
26 <Script>
27 <Type>shell</Type>
28 <Parameter>X Y</Parameter>
29 <Parameter>Z</Parameter>
30 <BootScript>before</BootScript>
31 <Text>
32 <Text>
33 <Text>
34 </Text>
35 </Script>
36 <Script>
37 <Type>python</Type>
38 <BootScript>after</BootScript>
39 <Text>
40 <Text>
41 print("Hello");
42 </Text>
43 </Script>
44 <Script>
45 <Type>perl</Type>
46 <BootScript>before</BootScript>
47 <Text>
48 <Text>
49 my $name = "VPX";
50 print "Hello, World $name !\n" ;
51 </Text>
52 </Script>
53 <Script>
54 <Type>nscli</Type>
```

```

55         <BootScript>after</BootScript>
56         <Text>
57             add vlan 33
58         bind vlan 33 -ifnum 1/2
59         </Text>
60     </Script>
61 </Scripts>
62 </ScriptSettingSection>
63 </cs:ScriptSection>
64 </Environment>
65 ``` En el archivo OVF anterior a "PropertySection" se utiliza para la
    configuración de redes de NetScaler, mientras que \<cs:ScriptSection
    > se utiliza para adjunto todos los scripts. \</Scripts> las
    etiquetas se utilizan para agrupar todos los scripts juntos. Cada
    script se define entre etiquetas \<Script> \</Script>. Cada etiqueta
    de script tiene los siguientes campos/etiquetas:

```

a) <Type>: Especifica el valor para el tipo de script. Valores posibles: Shell/Perl/Python/NSLCI (para scripts de NetScaler CLI)

b) <Parameter>: Proporciona parámetros al script. Cada script puede tener varias etiquetas <Parameter>.

c) <BootScript>: Especifica el punto de ejecución del script. Valores posibles para esta etiqueta: antes/después. “before” especifica que el script se ejecuta antes de que aparezca PE. “after” especifica que el script se ejecutará después de que aparezca PE.

d) <Text>: Pega el contenido de un script.

Nota:

Actualmente, la instancia VPX no se ocupa de la desinfección de scripts. Como administrador, debe comprobar la validez del script.

No todas las secciones necesitan estar presentes. Utilice una “PropertySection” vacía para definir únicamente los scripts que se ejecutarán en el primer arranque o en vacío

Una vez completadas las secciones requeridas del archivo OVF (archivo de datos de usuario), utilícelo para aprovisionar la instancia VPX.

Configuración de red

Como parte de la configuración de red, la instancia VPX dice lo siguiente:

- Dirección IP de administración
- Máscara de red
- Puerta de enlace predeterminada

Después de leer correctamente los parámetros, se rellenan en la configuración de NetScaler para permitir la administración remota de la instancia. Si los parámetros no se leen correctamente o la unidad de configuración no está disponible, la instancia pasa al comportamiento predeterminado, que es:

- La instancia intenta recuperar la información de la dirección IP de DHCP.
- Si DHCP falla o se agota el tiempo, la instancia presenta la configuración de red predeterminada (192.168.100.1/16).

Script del cliente

La instancia VPX permite ejecutar un script personalizado durante el aprovisionamiento inicial. El dispositivo admite comandos de tipo Shell, Perl, Python y NetScaler CLI comandos.

Autenticación de par de claves SSH

La instancia VPX copia la clave pública, disponible dentro de la unidad de configuración como parte de metadatos de instancia, en su archivo “authorized_keys”. Esto permite al usuario acceder a la instancia con clave privada.

Nota:

Cuando se proporciona una clave SSH, las credenciales predeterminadas (nsroot/nsroot) ya no funcionan, si se necesita acceso basado en contraseña, inicie sesión con la clave privada SSH correspondiente y establezca manualmente una contraseña.

Antes de comenzar

Antes de aprovisionar una instancia VPX en el entorno OpenStack, extraiga el `.qcow2` archivo del `archivo.tgz` y compile

Imagen de OpenStack de la imagen qcow2. Siga estos pasos:

1. Extraiga el `.qcow2` archivo del `.tgz` archivo escribiendo el siguiente comando

```
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. Cree una imagen de OpenStack mediante el `.qcow2` archivo extraído en el paso 1 escribiendo el siguiente comando.

```
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

```

Ilustración 1: La siguiente ilustración proporciona un ejemplo de salida para el comando `glance image-create`.

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

Aprovisionamiento de la instancia VPX

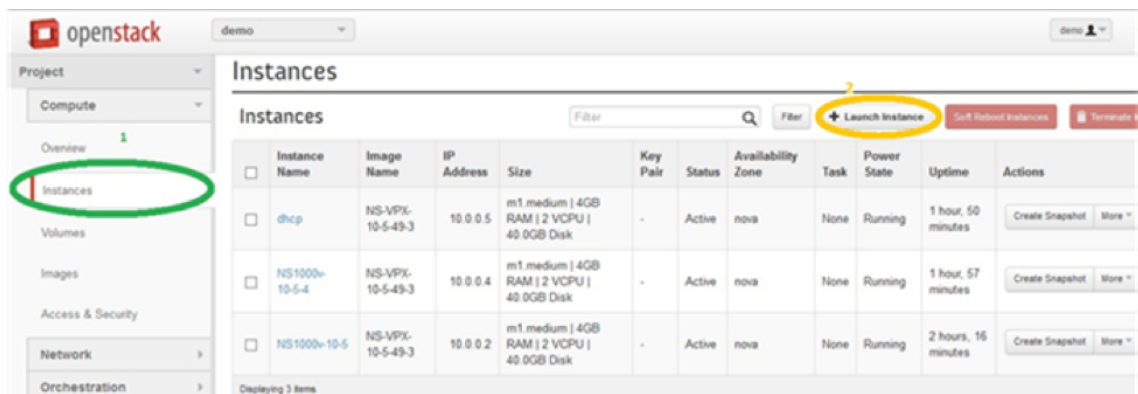
Puede aprovisionar una instancia VPX de dos maneras mediante una de las opciones:

- Horizon (panel de control de OpenStack)
- Comando de arranque Nova (CLI de OpenStack)

Aprovisione una instancia VPX mediante el panel de control de OpenStack

Siga estos pasos para aprovisionar la instancia VPX mediante Horizon:

1. Inicie sesión en el panel de control de OpenStack.
2. En el panel Proyecto, situado a la izquierda del tablero de mandos, seleccione **Instancias**.
3. En el panel Instancias, haga clic en **Iniciar instancia** para abrir el Asistente de inicio de instancias.



4. En el asistente Iniciar instancia, rellene los detalles, como:

- a) Nombre de la instancia
- b) Sabor de instancia
- c) Recuento de instancias
- d) Fuente de arranque de instancia
- e) Nombre de la imagen

Launch Instance ✕

Details *
Access & Security *
Networking *
Post-Creation
Advanced Options

Availability Zone:

nova ▼

Instance Name: *

NSVPX_10_1

Flavor: *

m1.medium ▼

Instance Count: *

1

Instance Boot Source: *

Boot from image ▼

Image Name:

NS-VPX-10-1-130-11 (20.0 GB) ▼

Specify the details for launching an instance.

The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.medium
VCPUs	2
Root Disk	40 GB
Ephemeral Disk	0 GB
Total Disk	40 GB
RAM	4,096 MB

Project Limits

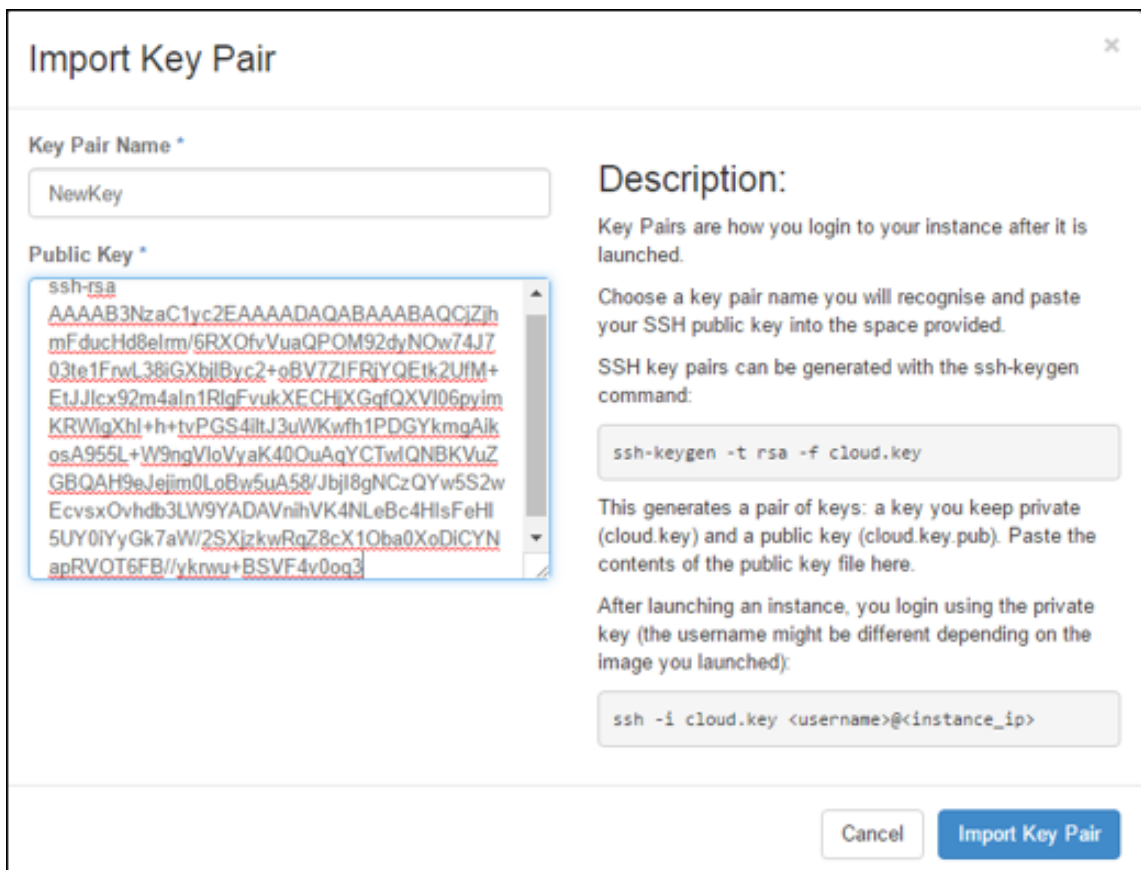
Number of Instances 6 of 10 Used

Number of VCPUs 12 of 20 Used

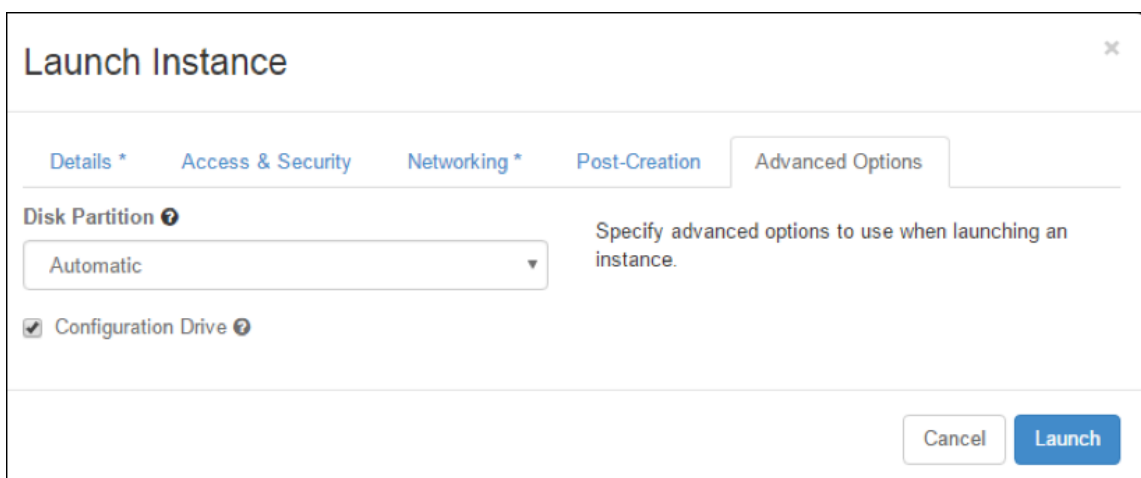
Total RAM 24,576 of 51,200 MB Used

Cancel
Launch

5. Implemente un nuevo par de claves o un par de claves existente a través de Horizon siguiendo los pasos siguientes:
 - a) Si no tiene un par de claves existente, cree la clave mediante cualquier mecanismo existente. Si ya tiene una clave, omita este paso.
 - b) Copiar el contenido de la clave pública.
 - c) Vaya a **Horizon > Instancias > Crear nuevas instancias**.
 - d) Haga clic en **Acceso y seguridad**.
 - e) Haga clic en el signo + situado junto al menú desplegable **Par de claves** y proporcione los valores de los parámetros mostrados.
 - f) Pegar contenido de clave pública en el cuadro *Clave pública*, dar un nombre a la clave y hacer clic en **Importar par de claves**.



6. Haga clic en la ficha **Creación** de publicaciones del asistente. En Script de personalización, agregue el contenido del archivo de datos de usuario. El archivo de datos de usuario contiene la dirección IP, los detalles de la máscara de red y la puerta de enlace y los scripts de cliente de la instancia VPX.
7. Después de seleccionar o importar un par de claves, marque la opción config-drive y haga clic en **Iniciar**.



Aprovisione la instancia VPX mediante OpenStack CLI

Siga estos pasos para aprovisionar una instancia VPX mediante OpenStack CLI.

1. Para crear una imagen desde qcow2, escriba el siguiente comando:

```
openstack image create --container-format bare --property hw_disk_bus=ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-Image
```

2. Para seleccionar una imagen para crear una instancia, escriba el siguiente comando:

```
openstack image list | more
```

3. Para crear una instancia de un sabor determinado, escriba el siguiente comando para elegir un ID de sabor de una lista:

```
openstack flavor list
```

4. Para conectar una NIC a una red determinada, escriba el siguiente comando para elegir un ID de red de una lista de redes:

```
openstack network list
```

5. Para crear una instancia, escriba el siguiente comando:

```
1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --
  key-name KEY_NAME
2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id
  =net-uuid
3 INSTANCE_NAME
4 openstack server create --image VPX-ToT-Image --flavor m1.medium
  --user-data
5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6
  -3efd44b761b9
6 VPX-ToT
```

Ilustración 2: La siguiente ilustración proporciona un resultado de ejemplo.

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{'u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

Aprovisione la instancia de NetScaler VPX mediante el Administrador de máquinas virtuales

October 17, 2024

Virtual Machine Manager es una herramienta de escritorio para administrar invitados de VM. Le permite crear nuevos invitados de VM y varios tipos de almacenamiento, y administrar redes virtuales. Puede acceder a la consola gráfica de invitados de VM con el visor VNC integrado y ver estadísticas de rendimiento, ya sea local o remotamente.

Después de instalar la distribución Linux preferida, con la virtualización KVM habilitada, puede continuar con el Provisioning de máquinas virtuales.

Al utilizar el Virtual Machine Manager para aprovisionar una instancia de NetScaler VPX, tiene dos opciones:

- Introduzca manualmente la dirección IP, la Gateway y la máscara de red
- Asignar automáticamente la dirección IP, la Gateway y la máscara de red (autoaprovisionamiento)

Puede utilizar dos tipos de imágenes para aprovisionar una instancia de NetScaler VPX:

- RAW

- QCOW2

Puede convertir una imagen RAW de NetScaler VPX en una imagen QCOW2 y aprovisionar la instancia de NetScaler VPX. Para convertir la imagen RAW en una imagen QCOW2, escriba el siguiente comando:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Por ejemplo:

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc.qcow
```

Una implementación típica de NetScaler VPX en KVM incluye los siguientes pasos:

- Comprobación de los requisitos previos para el Provisioning automático de una instancia de NetScaler VPX
- Provisioning de la instancia de NetScaler VPX mediante una imagen RAW
- Provisioning de la instancia NetScaler VPX mediante una imagen de QCOW2
- Adición de interfaces adicionales a una instancia VPX mediante Virtual Machine Manager

Compruebe los requisitos previos para el aprovisionamiento automático de una instancia de NetScaler VPX

El aprovisionamiento automático es una función opcional, e implica el uso de datos de la unidad CDROM. Si esta función está habilitada, no es necesario introducir la dirección IP de administración, la máscara de red ni la puerta de enlace predeterminada de la instancia de NetScaler VPX durante la configuración inicial.

Debe completar las siguientes tareas antes de poder aprovisionar automáticamente una instancia VPX:

1. Cree un archivo XML de formato abierto de virtualización (OVF) personalizado o un archivo de datos de usuario.
2. Convierta el archivo OVF en una imagen ISO mediante una aplicación en línea (por ejemplo, PowerISO).
3. Monte la imagen ISO en el host KVM mediante cualquier herramienta basada en copia segura (SCP).

Archivo XML OVF de ejemplo:

Aquí hay un ejemplo del contenido de un archivo XML OVF, que puede usar como muestra para crear el archivo.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
```



```
3 <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`
4
5 xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`
6
7 oe:id=""
8
9 xmlns="`http://schemas.dmtf.org/ovf/environment/1"`
10
11 xmlns:cs="`http://schemas.citrix.com/openstack">`
12
13 <PlatformSection>
14
15 <Kind></Kind>
16
17 <Version>2016.1</Version>
18
19 <Vendor>VPX</Vendor>
20
21 <Locale>en</Locale>
22
23 </PlatformSection>
24
25 <PropertySection>
26
27 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
28
29 <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
30
31 <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>
32
33 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
34 />
35 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
36 255.255.255.0"/>
37 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
38 10.1.2.1"/>
39 </PropertySection>
40
41 </Environment>
```

En el archivo XML de OVF anterior, se utiliza “PropertySection” para la configuración de redes de NetScaler. Al crear el archivo, especifique valores para los parámetros que se resaltan al final del ejemplo:

- Dirección IP de administración
- Máscara de red
- Gateway

Importante


Si el archivo OVF no tiene el formato XML correcto, se asigna a la instancia VPX la configuración de red predeterminada, no a los valores especificados en el archivo.

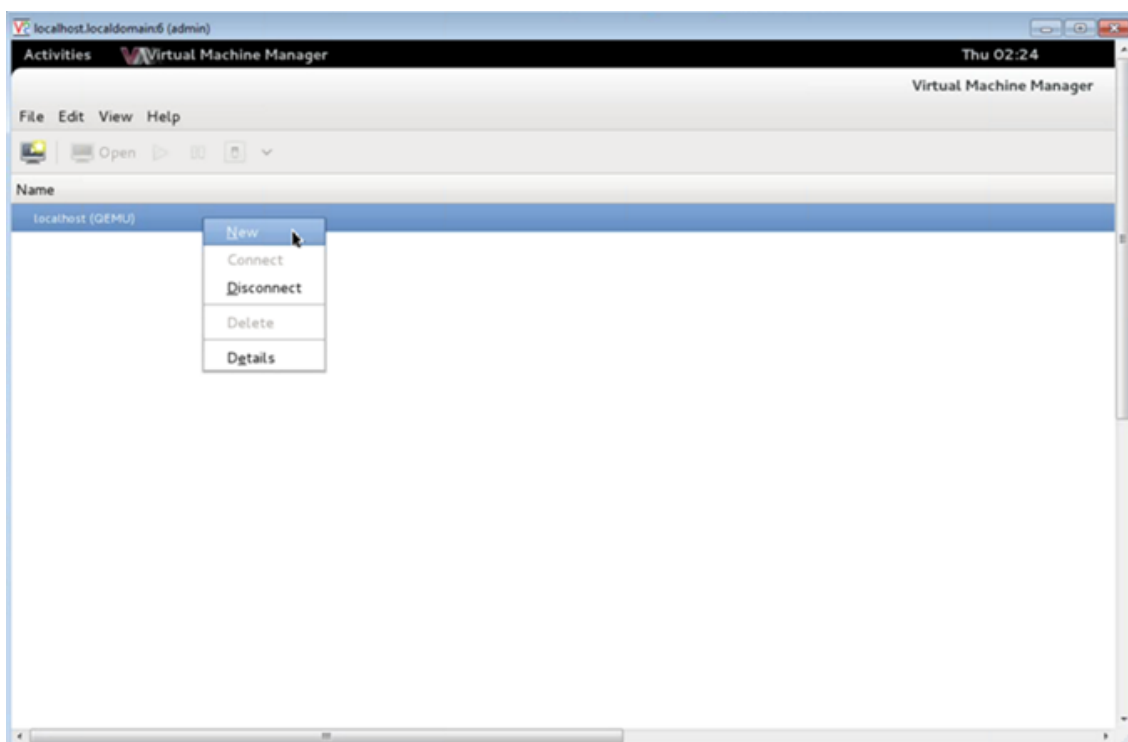
Aprovisione la instancia de NetScaler VPX mediante una imagen RAW

El administrador de máquinas virtuales le permite aprovisionar una instancia de NetScaler VPX mediante una imagen RAW.

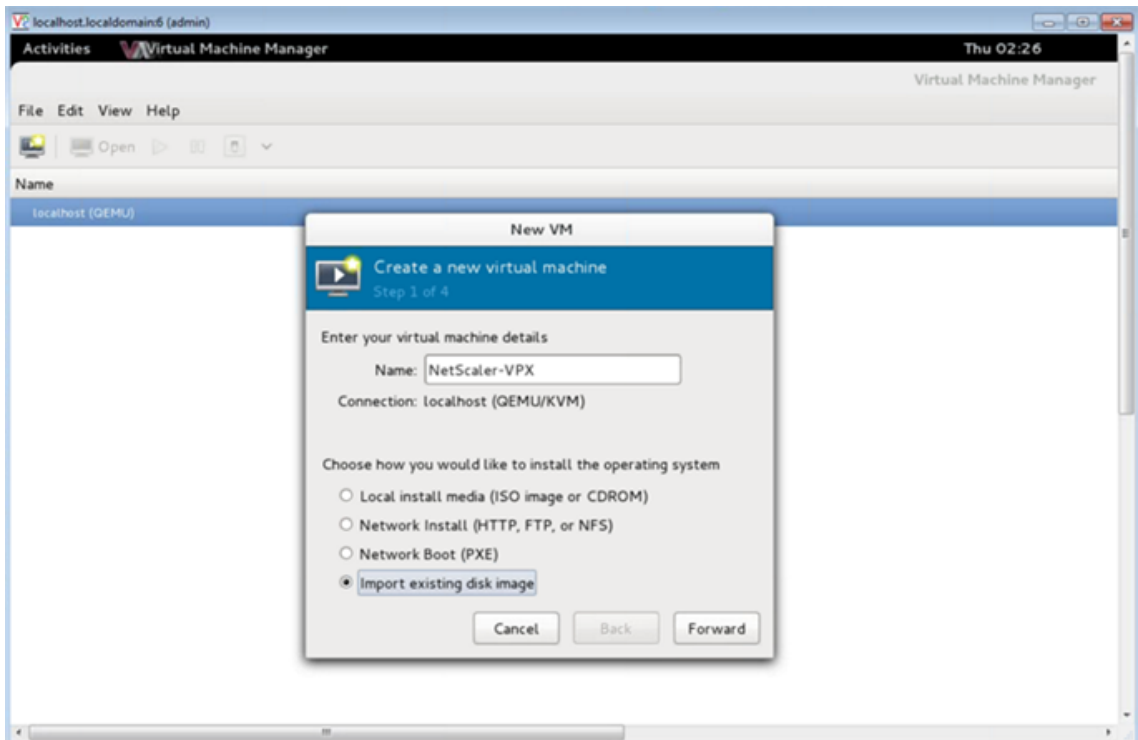
Para aprovisionar una instancia de NetScaler VPX mediante el Administrador de máquinas virtuales, siga estos pasos:

1. Abra Virtual Machine Manager (**Aplicación** > **Herramientas del sistema** > **Virtual Machine Manager**) e introduzca las credenciales de inicio de sesión en la ventana **Autenticar**.

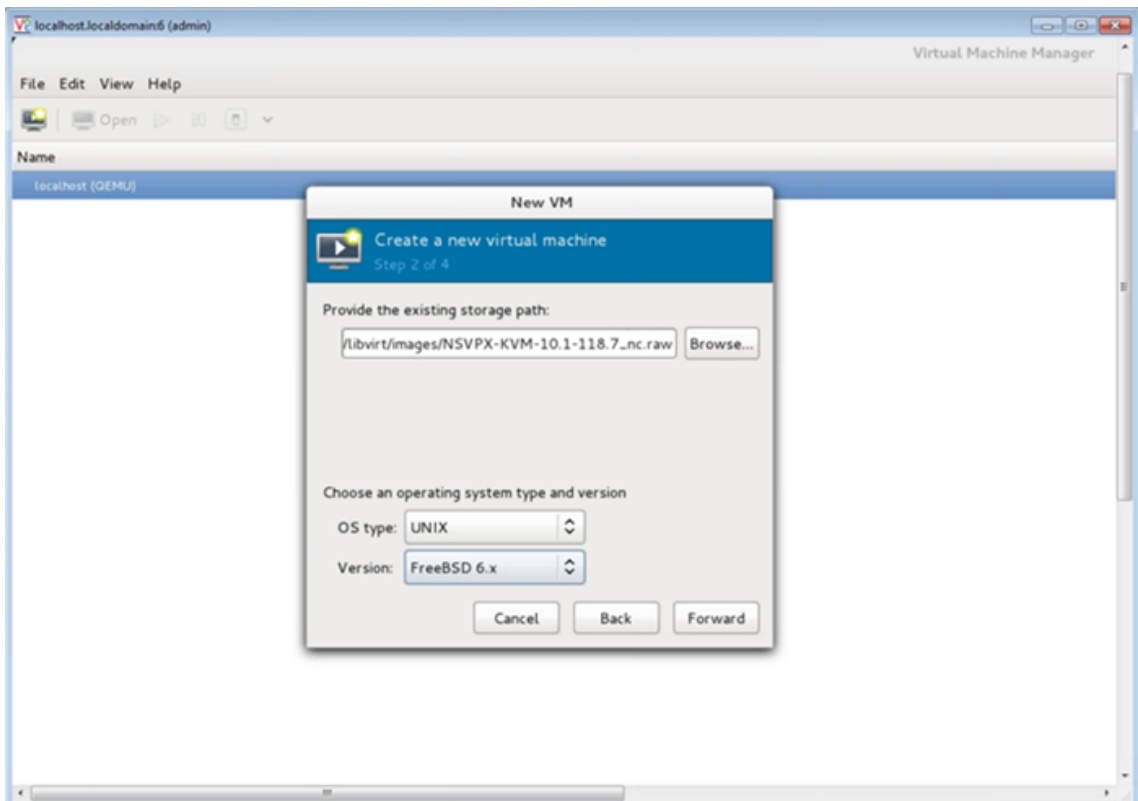
2. Haga clic en el icono de  o haga clic con el botón derecho en **localhost (QEMU)** para crear una nueva instancia NetScaler VPX.



3. En el cuadro de texto **Nombre**, escriba un nombre para la nueva VM (por ejemplo, NetScaler-VPX).
4. En la ventana **Nueva máquina virtual**, en “Elija cómo quiere instalar el sistema operativo”, seleccione **Importar imagen de disco existente** y, a continuación, haga clic en **Reenviar**.

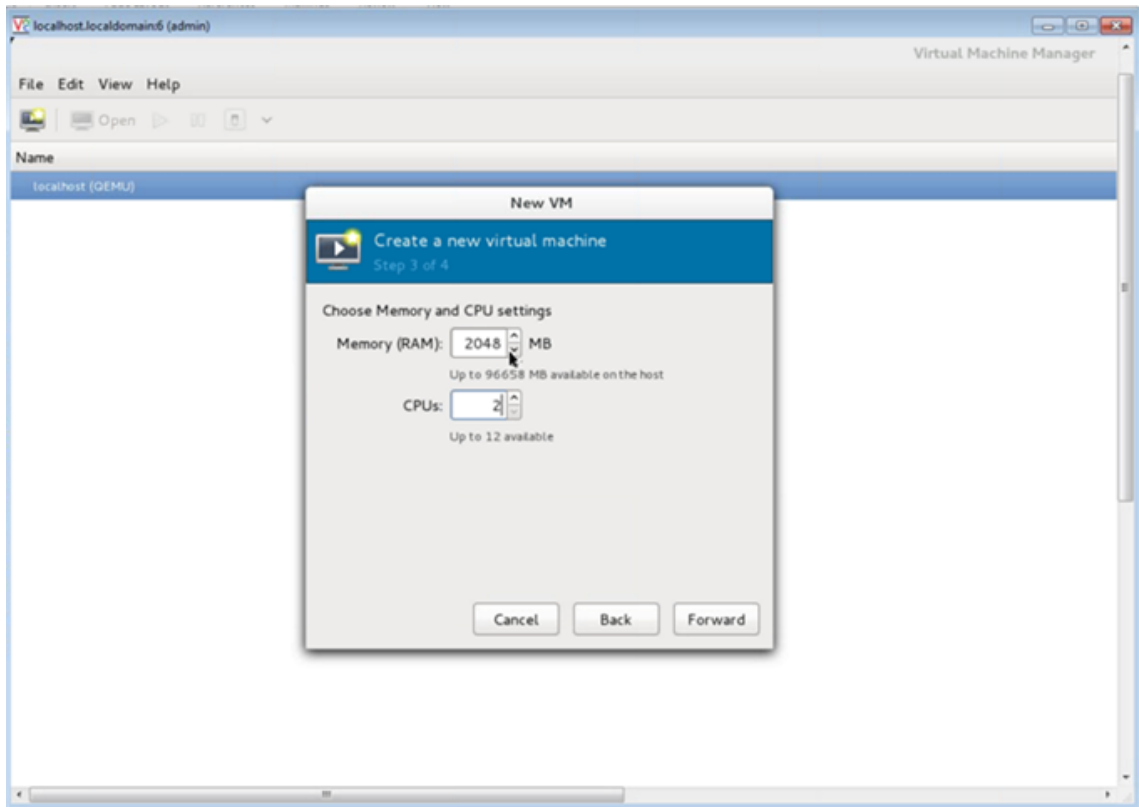


5. En el campo **Proporcionar la ruta de almacenamiento existente**, navegue por la ruta de acceso a la imagen. Elija el tipo de SO como UNIX y Versión como FreeBSD 6.x. A continuación, haga clic en **Reenviar**.

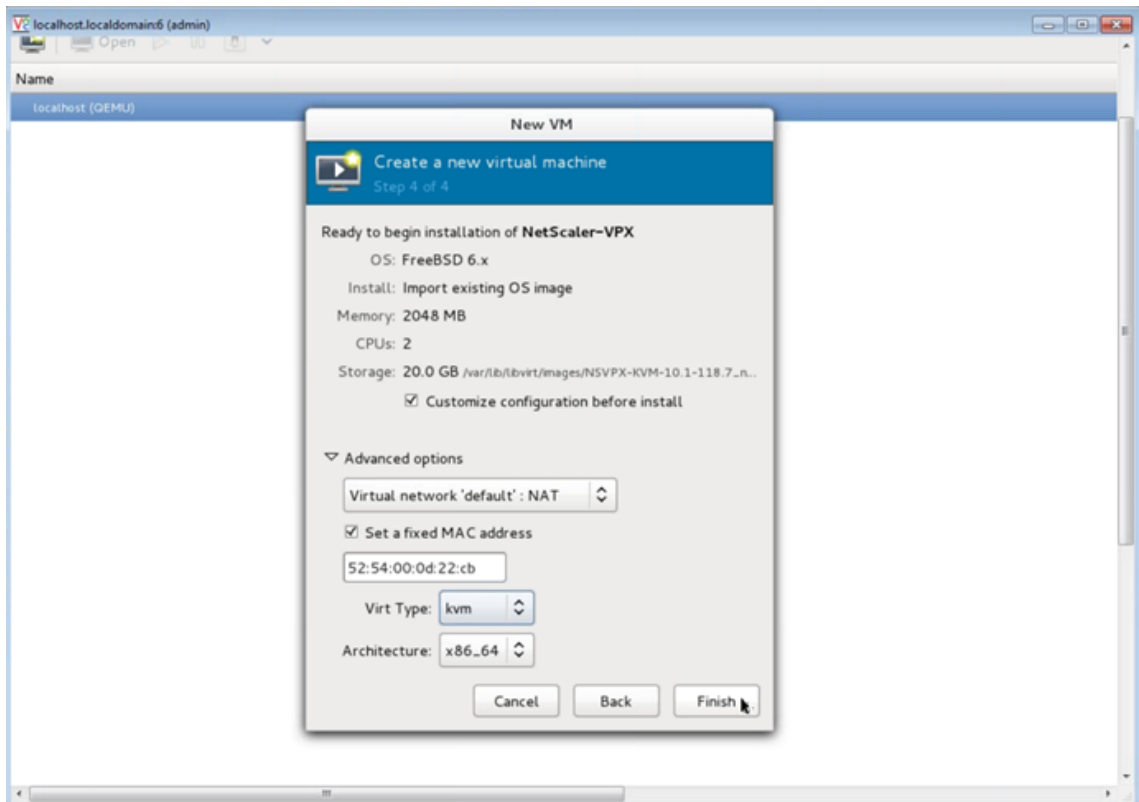


6. En **Elegir configuración de memoria y CPU**, seleccione la configuración siguiente y, a continuación, haga clic en **Reenviar** :

- Memoria (RAM): 2048 MB
- CPU—2

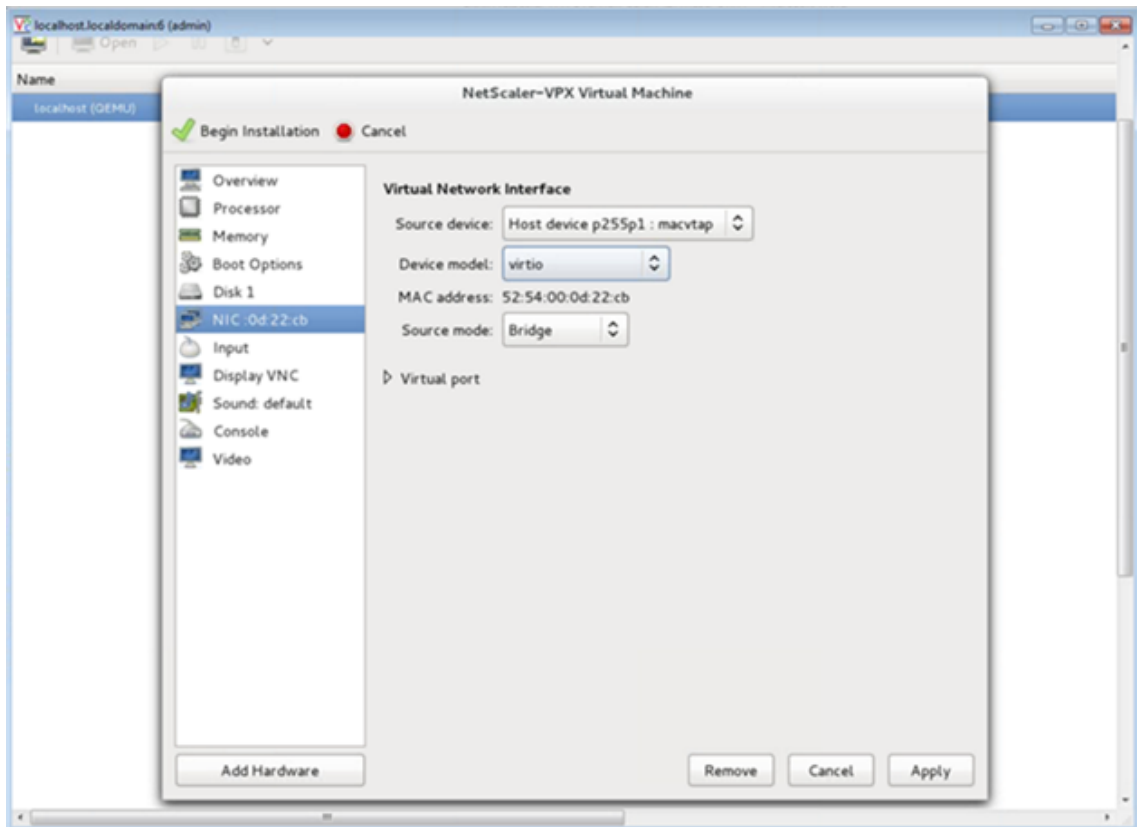


7. Active la casilla de verificación **Personalizar configuración antes de instalar**. Opcionalmente, en **Opciones avanzadas** puede personalizar la dirección MAC. Asegúrese de que el **tipo de Virt** seleccionado sea KVM y la arquitectura seleccionada es x86_64. Haga clic en **Finalizar**.



8. Seleccione una NIC y proporcione la siguiente configuración:

- Dispositivo de origen `ethX` `macvtap` o Bridge
- Modelo de dispositivo: `virtio`
- Modo de origen: Puente



9. Haga clic en **Aplicar**.
10. Si quiere aprovisionar automáticamente la instancia VPX, consulte la sección **Habilitación de Auto-Provisioning mediante Adjuntar una unidad de CDRom** en este documento. De lo contrario, haga clic en **Iniciar instalación**. Después de aprovisionar NetScaler VPX en KVM, puede agregar más interfaces.

Aprovisione la instancia de NetScaler VPX mediante una imagen QCOW2

Con el Virtual Machine Manager, puede aprovisionar la instancia de NetScaler VPX mediante una imagen de QCOW2.

Para aprovisionar una instancia de NetScaler VPX mediante una imagen QCOW2, siga estos pasos:

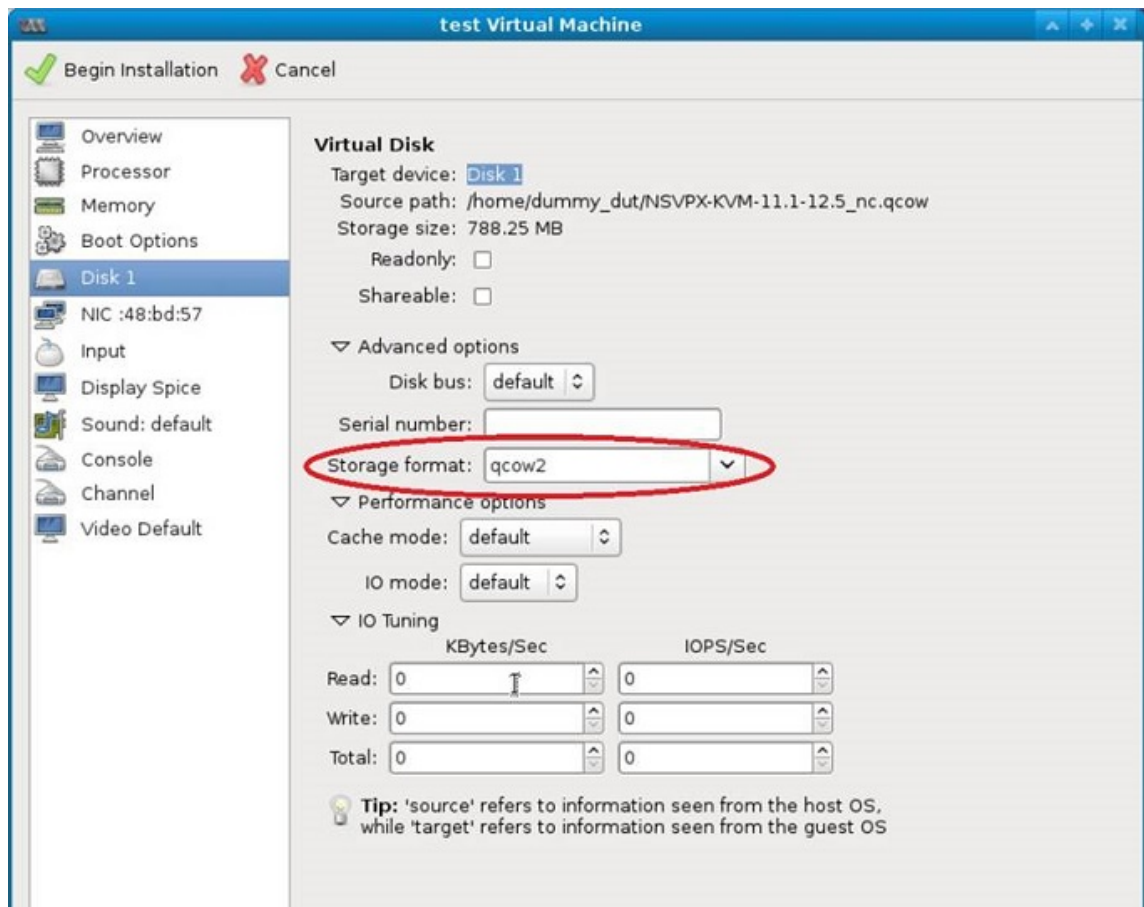
1. Siga el **paso 1** al **paso 8** de [Aprovisionamiento de la instancia NetScaler VPX mediante una imagen RAW](#).

Nota:

Asegúrese de seleccionar la imagen **qcow2** en el **paso 5**.

2. Seleccione **Disco 1** y haga clic en **Opciones avanzadas**.

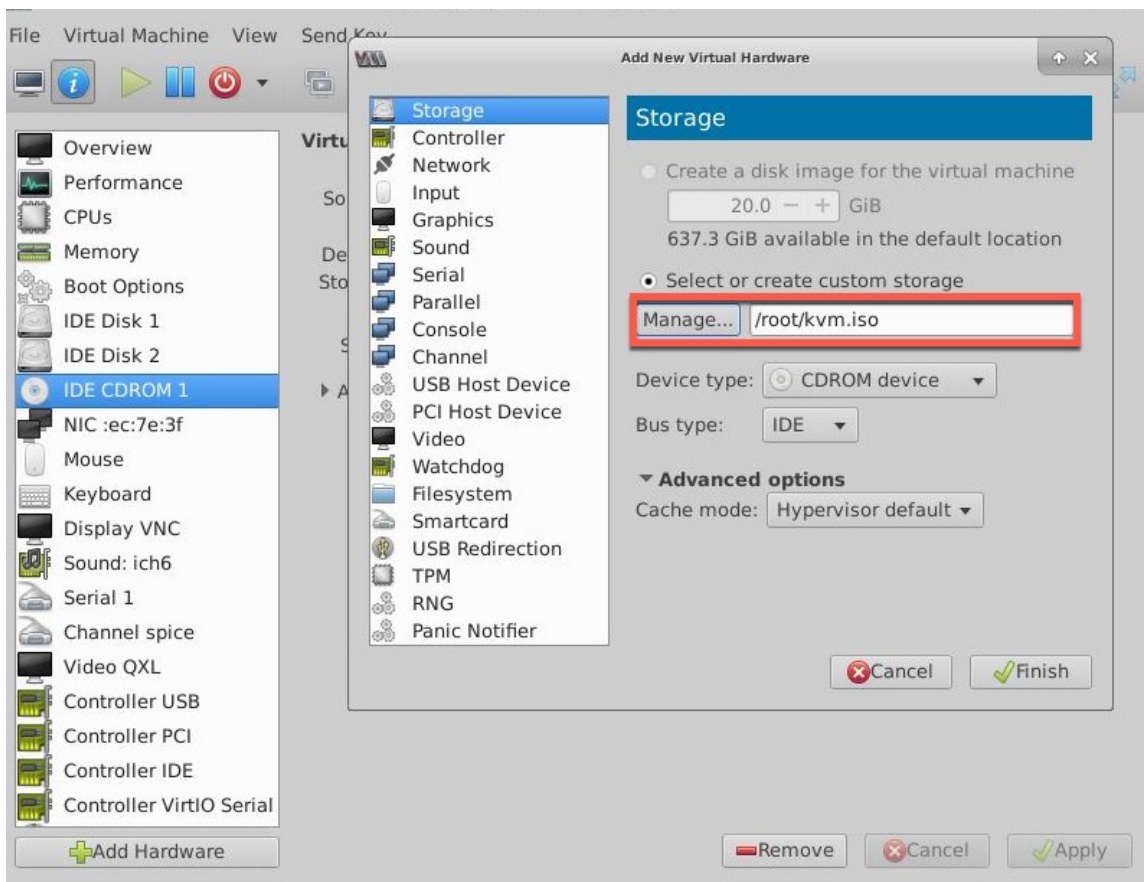
3. Seleccione **qcow2** en la lista desplegable Formato de almacenamiento.



4. Haga clic en **Aplicar** y, a continuación, haga clic en **Iniciar instalación**. Después de aprovisionar NetScaler VPX en KVM, puede agregar más interfaces.

Habilitar el aprovisionamiento automático adjuntando una unidad de CDROM

1. Haga clic en Agregar **hardware** > **Almacenamiento** > **Tipo de dispositivo** > **Dispositivo de CDROM**.
2. Haga clic en **Administrar** y seleccione el archivo ISO correcto que ha montado en la sección “Requisitos previos para el aprovisionamiento automático de una instancia NetScaler VPX” y haga clic en **Finalizar**. Se crea un nuevo CDROM en Recursos en la instancia de NetScaler VPX.



3. Encienda la instancia VPX y se aprovisiona automáticamente con la configuración de red proporcionada en el archivo OVF, como se muestra en la captura de pantalla de ejemplo.


```

File Virtual Machine View Send Key
Aug 11 10:14:55 <local0.alert> ns restart[25781]: Restart: /netscaler/nsstart.sh
exited normally. Exit code (0)
Aug 11 10:14:55 <local0.alert> ns restart[25781]: Successfully deregistered with
h Pitboss ...

login: nsroot
Password:
Aug 11 10:15:04 <auth.notice> ns login: ROOT LOGIN (nsroot) ON ttyv0
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Done
> sh ip
      Ippaddress      Traffic Domain  Type          Mode      Arp      Icmp
      Userver  State
      -----
1)    10.1.2.22      0              NetScaler IP  Active    Enabled  Enab
led NA      Enabled
Done
> Aug 11 10:15:13 <local0.alert> ns restart[25781]: Nsshutdown lock released !

```

4. Si el aprovisionamiento automático falla, la instancia aparece con la dirección IP predeterminada (192.168.100.1). En ese caso, debe completar la configuración inicial manualmente. Para obtener más información, consulte [Configurar el ADC por primera vez](#).


Agregar más interfaces a la instancia de NetScaler VPX mediante Virtual Machine Manager

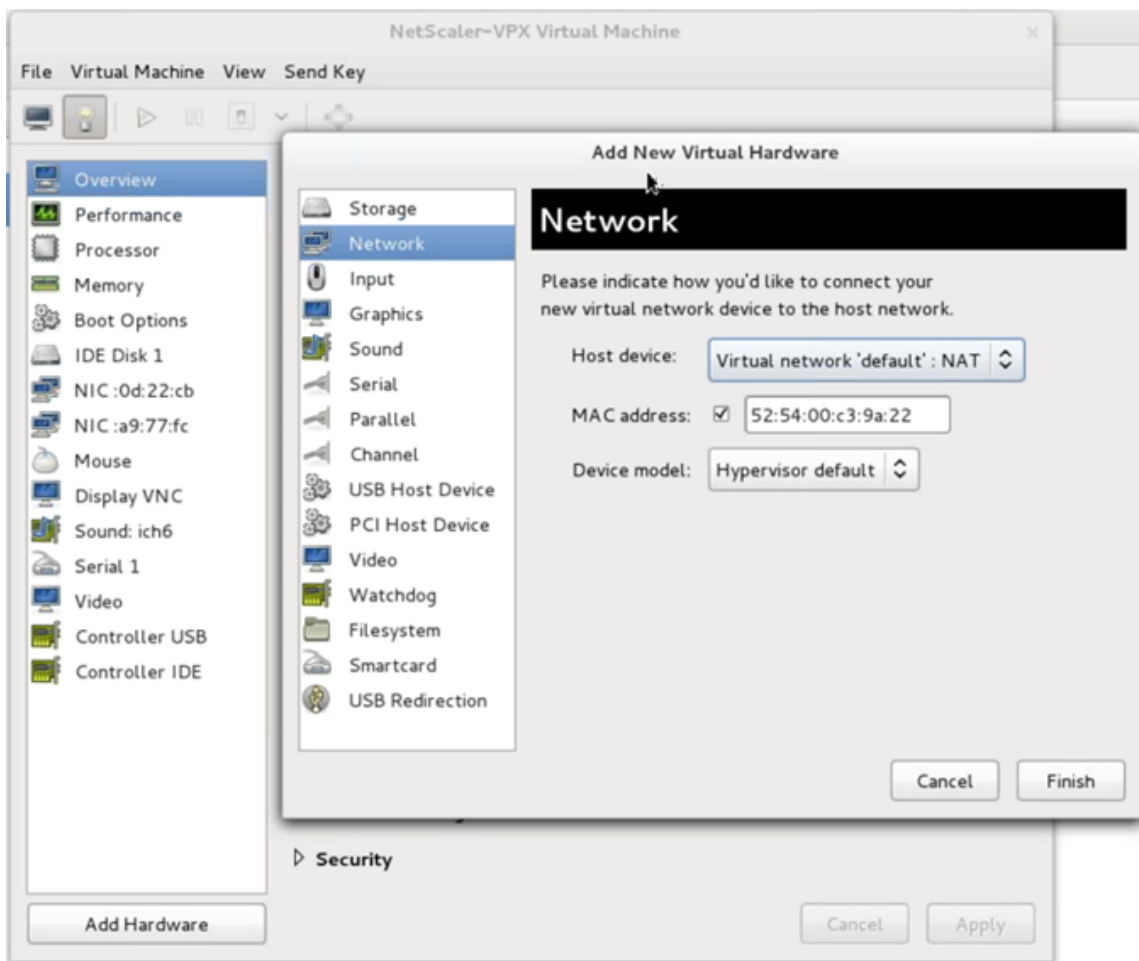
Después de haber aprovisionado la instancia de NetScaler VPX en KVM, puede agregar interfaces adicionales.

Para agregar más interfaces, sigue estos pasos.

1. Apague la instancia de NetScaler VPX que se ejecuta en el KVM.
2. Haga clic con el botón derecho en la instancia de VPX y elija **Abrir** en el menú emergente.



3. Haga clic en el icono de  del encabezado para ver los detalles del hardware virtual.
4. Haga clic en **Agregar hardware**. En la **ventana Agregar nuevo hardware virtual**, seleccione **Reden** el menú de navegación.



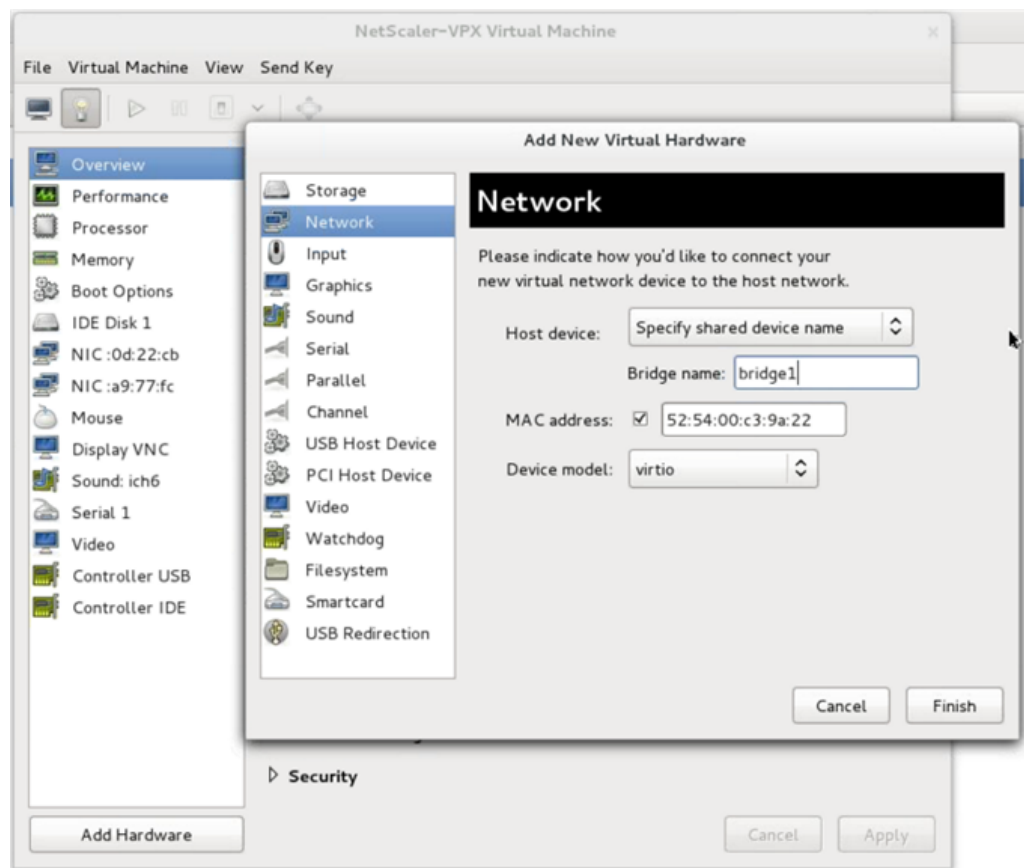
5. En el campo **Dispositivo de host**, seleccione el tipo de interfaz física. El tipo de dispositivo host puede ser Bridge o MacVtap. En el caso de MacVtap, cuatro modos posibles son VEPA, Bridge, Private y Pass-through.

a) Para Bridge

- i. Dispositivo host: Seleccione la opción “Especificar nombre de dispositivo compartido”.
- ii. Proporcione el nombre del puente configurado en el host KVM.

Nota:

Asegúrese de haber configurado un puente Linux en el host KVM, haber vinculado la interfaz física al puente y haber puesto el puente en estado activo.



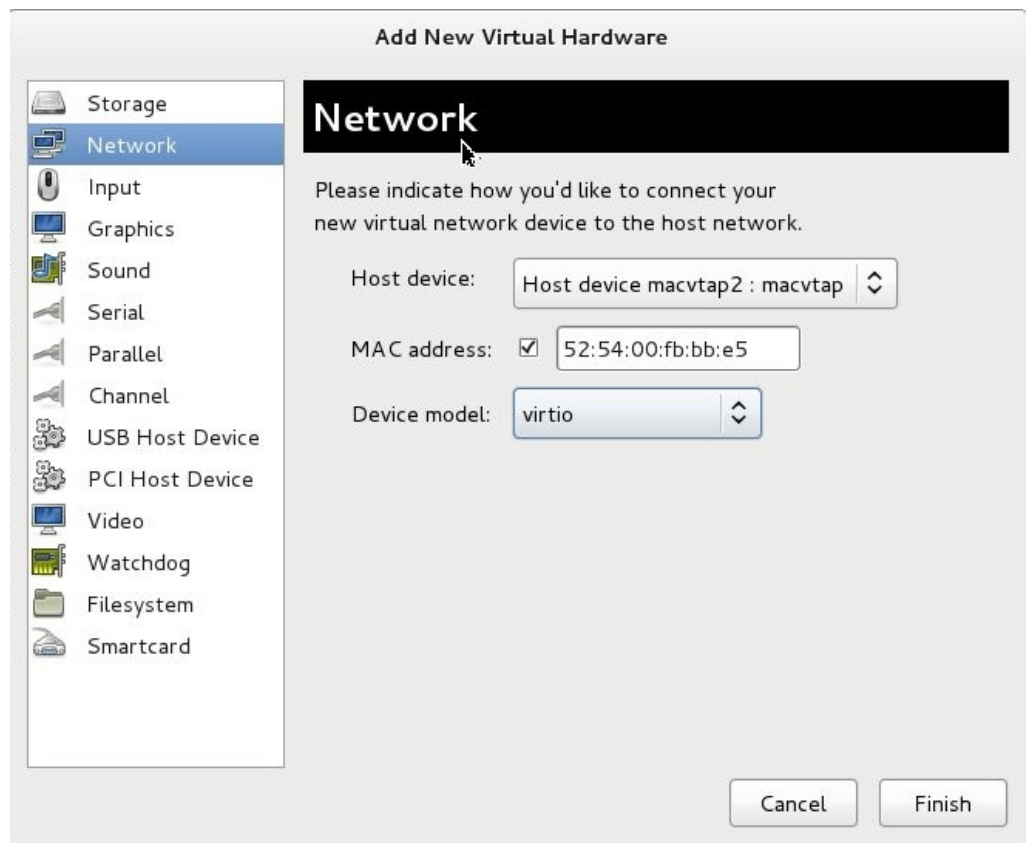
iii. Modelo de dispositivo: `virtio`.

iv. Haga clic en **Finalizar**.

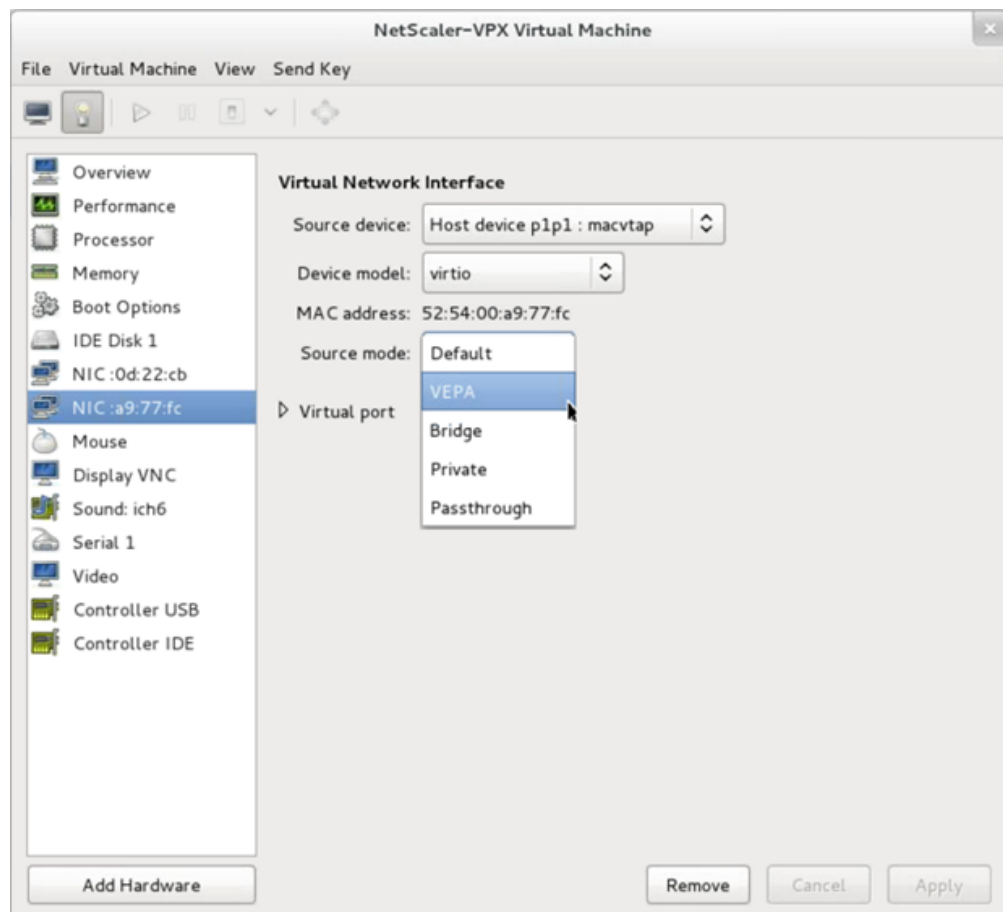
b) Para MacVtap

i. Dispositivo host: Seleccione la interfaz física en el menú.

ii. Modelo de dispositivo: `virtio`.



iii. Haga clic en **Finalizar**. Puede ver la NIC recién agregada en el panel de navegación.



iv. Seleccione la NIC recién agregada y seleccione el modo de origen para esta NIC. Los modos disponibles son VEPA, Bridge, Private y Passthrough. Para obtener más información sobre la interfaz y los modos, consulte Interfaz y modos de origen.

v. Haga clic en **Aplicar**.

6. Si quieres aprovisionar automáticamente la instancia VPX, consulta la sección “Agregar una unidad de configuración para habilitar el Provisioning automático” de este documento. De lo contrario, encienda la instancia VPX para completar la configuración inicial manualmente.

Importante:

No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociación automática.

Configurar una instancia de NetScaler VPX para usar las interfaces de red SR-IOV

October 17, 2024

Puede configurar una instancia de NetScaler VPX que se ejecute en la plataforma Linux-KVM mediante la virtualización de E/S de raíz única (SR-IOV) con las siguientes NIC:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

En esta sección se describe cómo:

- Configurar una instancia de NetScaler VPX para usar la interfaz de red SR-IOV
- Configurar LA/LACP estático en la interfaz SR-IOV
- Configurar VLAN en la interfaz SR-IOV

Limitaciones

Tenga en cuenta las limitaciones al utilizar las NIC Intel 82599, X710, XL710 y X722. No se admiten las siguientes funciones.

Limitaciones para la NIC Intel 82599:

- Conmutación de modo L2.
- Partición de administrador (modo VLAN compartido).
- Alta disponibilidad (modo activo-activo).
- Marcos gigantes.
- IPv6: Solo puede configurar hasta 30 direcciones IPv6 únicas en una instancia VPX si tiene al menos una interfaz SR-IOV.
- No se admite la configuración de VLAN en Hypervisor para la interfaz VF de SRIOV a través del `ip link` comando.
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.

Limitaciones para las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G:

- Conmutación de modo L2.
- Partición de administrador (modo VLAN compartido).

- En un clúster, las tramas jumbo no se admiten cuando se utiliza la NIC XL710 como interfaz de datos.
- La lista de interfaces se reordena cuando las interfaces se desconectan y se vuelven a conectar.
- No se admiten configuraciones de parámetros de interfaz como velocidad, dúplex y negociaciones automáticas.
- El nombre de la interfaz es 40/X para las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G
- Se pueden admitir hasta 16 interfaces Intel XL710/X710/X722 SRIOV o PCI en una instancia VPX.

Nota:

Para que las NIC Intel X710 10G, Intel XL710 40G e Intel X722 10G admitan IPv6, debe habilitar el modo de confianza en las funciones virtuales (VF) escribiendo el siguiente comando en el host KVM:

```
# ip link set <PNIC> <VF> trust on
```

Ejemplo

```
# ip link set ens785f1 vf 0 trust on
```

Requisitos previos

Antes de configurar una instancia de NetScaler VPX para usar las interfaces de red SR-IOV, complete las siguientes tareas previas. Consulte la columna NIC para obtener información detallada sobre cómo completar las tareas correspondientes.

Tarea	NIC Intel 82599	NIC Intel X710, XL710 y X722
1. Agregue la NIC al host KVM.	-	-
1. Descargue e instale el controlador Intel más reciente.	Controlador IXGBE	Controlador I40E
1. Bloquee el controlador en la lista de controladores del host KVM.	Agregue la siguiente entrada en el archivo /etc/modprobe.d/blacklist.conf: <code>blacklist ixgbev</code> . Utilice el controlador IXGBE versión 4.3.15 (recomendado).	Agregue la siguiente entrada en el archivo /etc/modprobe.d/blacklist.conf: <code>blacklist i40evf</code> . Utilice el controlador i40e versión 2.0.26 (recomendado).

Tarea	NIC Intel 82599	NIC Intel X710, XL710 y X722
<p>1. Habilite las funciones virtuales (VF) SR-IOV en el host KVM. En ambos comandos de las dos columnas siguientes: <code>number_of_VFs</code> = el número de VF virtuales que quiere crear. <code>device_name</code> = el nombre de la interfaz. <code>nombre_dispositivo</code> = el nombre de la interfaz.</p> <p>1. Haga que los VF sean persistentes agregando los comandos que utilizó para crearlos al archivo <code>rc.local</code>.</p>	<p>Si está usando una versión anterior del kernel 3.8, agregue la siguiente entrada al archivo <code>/etc/modprobe.d/ixgbe</code> y reinicie el host KVM: <code>options ixgbe max_vfs=<number_of_VFs></code>; Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando: <code>echo <number_of_VFs> &gt; /sys/class/net/<device_name>/device/sriov_numvfs</code>. Consulte el ejemplo de la imagen 1.</p> <p>Consulte el ejemplo en la imagen 3.</p>	<p>Si está usando la versión anterior del kernel 3.8, agregue la siguiente entrada al archivo <code>/etc/modprobe.d/i40e.conf</code> y reinicie el host KVM: <code>options i40e max_vfs=<number_of_VFs></code>; Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando: <code>echo <number_of_VFs> &gt; /sys/class/net/<device_name>/device/sriov_numvfs</code>. Vea el ejemplo en la ilustración 2.</p> <p>Consulte el ejemplo en la imagen 3.</p>

Importante:

Cuando cree los VF SR-IOV, asegúrese de que no asigna direcciones MAC a los VF.

Ilustración 1: Habilitar las VFs SR-IOV en el host KVM para la NIC Intel 82599 10G.

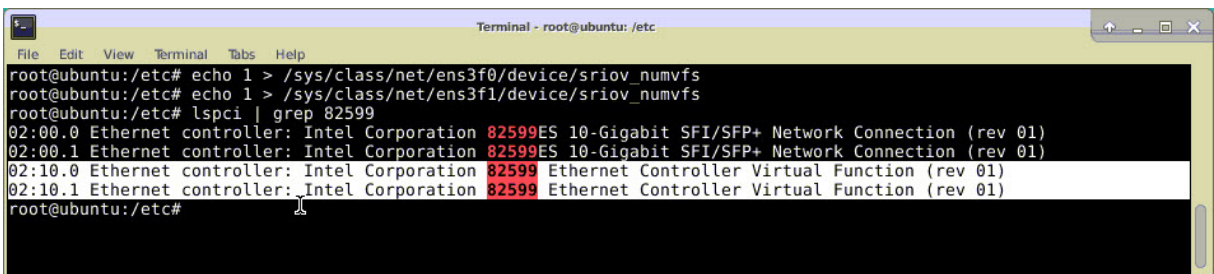


Ilustración 2: Habilitar VF SR-IOV en el host KVM para las NIC Intel X710 10G y XL710 40G.


```

root@ubuntu:~# lspci | grep 710
03:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:06.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:06.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 01)
82:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 02)
82:00.1 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 02)
82:02.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:02.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
root@ubuntu:~#

```

Ilustración 3: Habilitar las VFs SR-IOV en el host KVM para la NIC Intel X722 10G.

```

root@ubuntu:~# lspci | grep "37cd"
84:02.0 Ethernet controller: Intel Corporation Device 37cd (rev 04)
84:0a.0 Ethernet controller: Intel Corporation Device 37cd (rev 04)

```

Ilustración 4: Hacer que los VF sean persistentes.

```

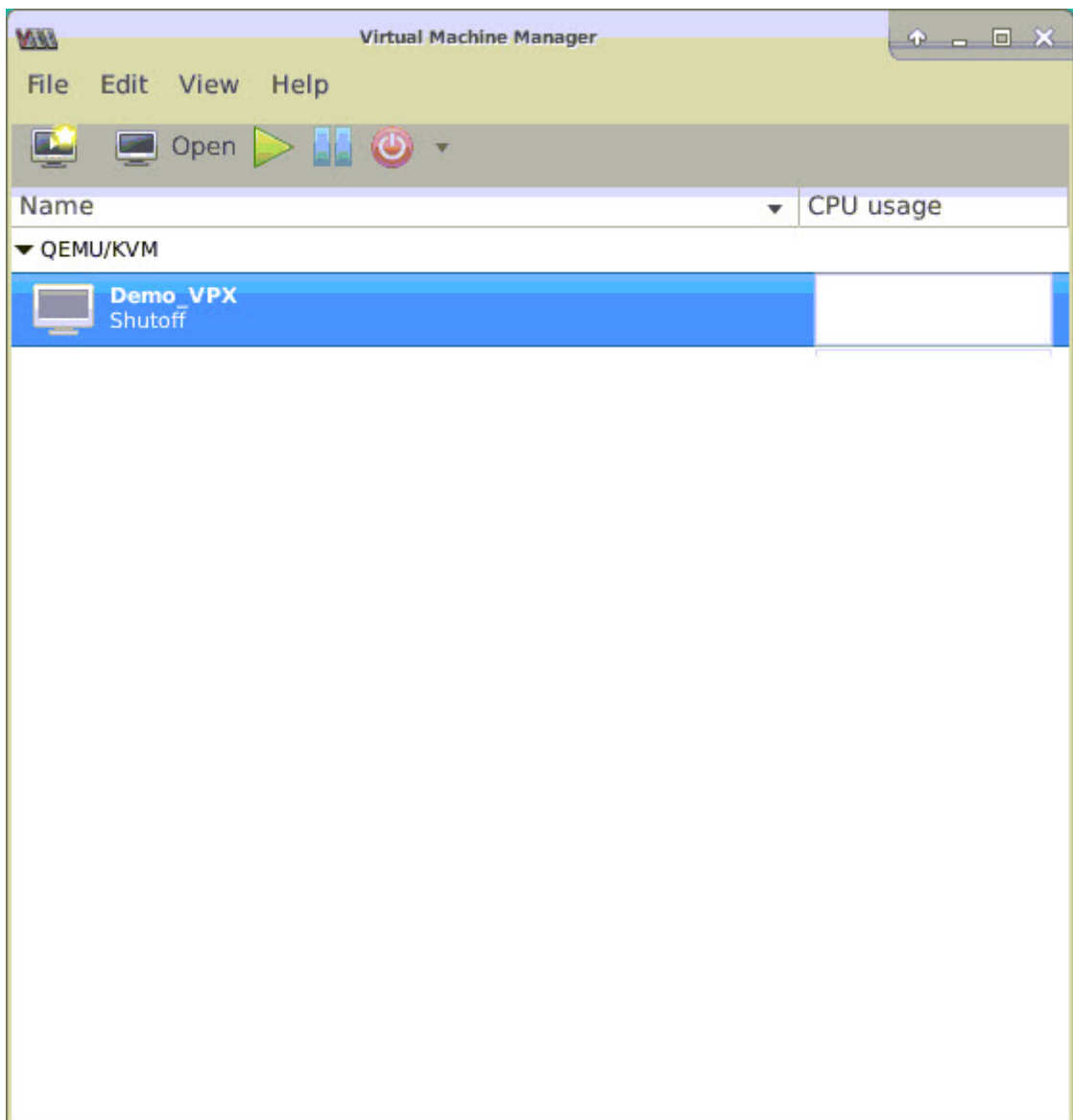
Terminal - root@ubuntu: /etc
File Edit View Terminal Tabs Help
root@ubuntu:/etc# cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
echo 1 > /sys/class/net/ens3f0/device/sriov_numvfs
echo 1 > /sys/class/net/ens3f1/device/sriov_numvfs
exit 0
root@ubuntu:/etc#

```

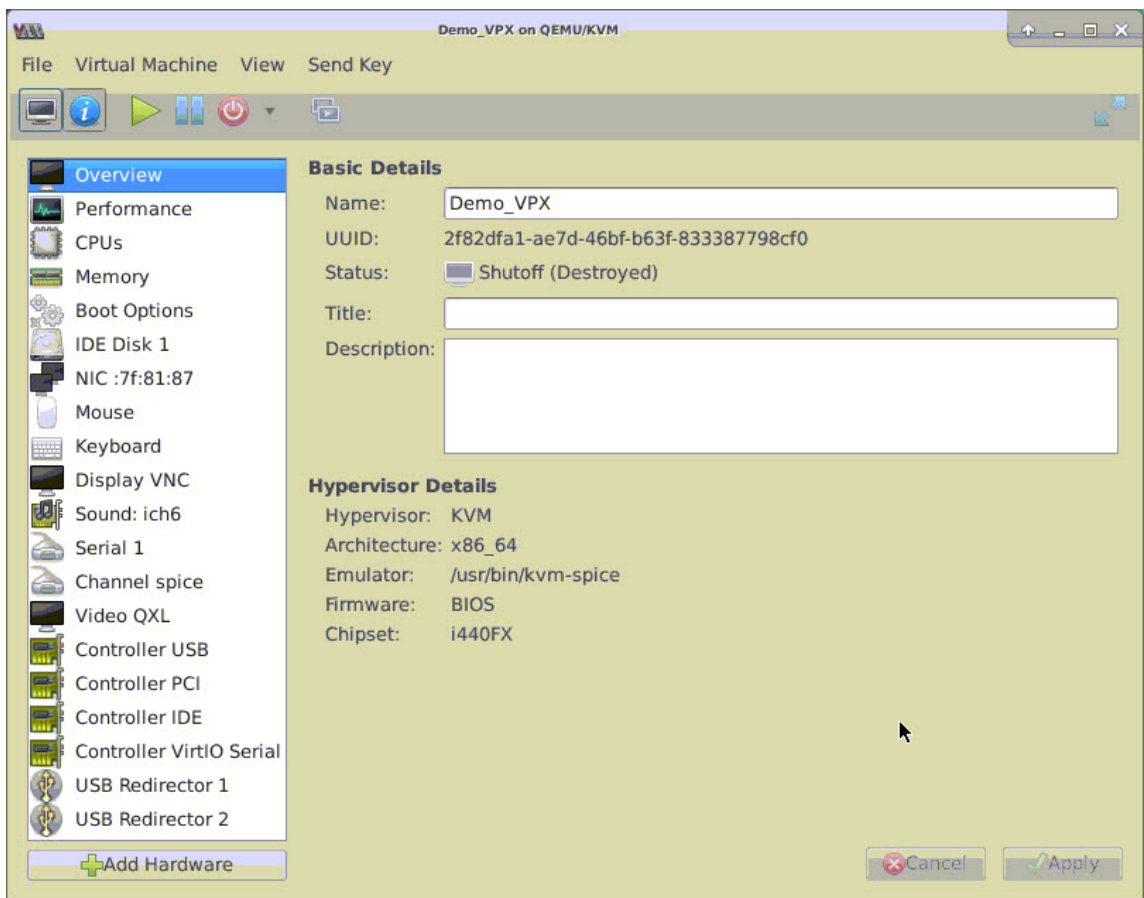
Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV

Para configurar la instancia NetScaler VPX para que use la interfaz de red SR-IOV mediante Virtual Machine Manager, siga estos pasos:

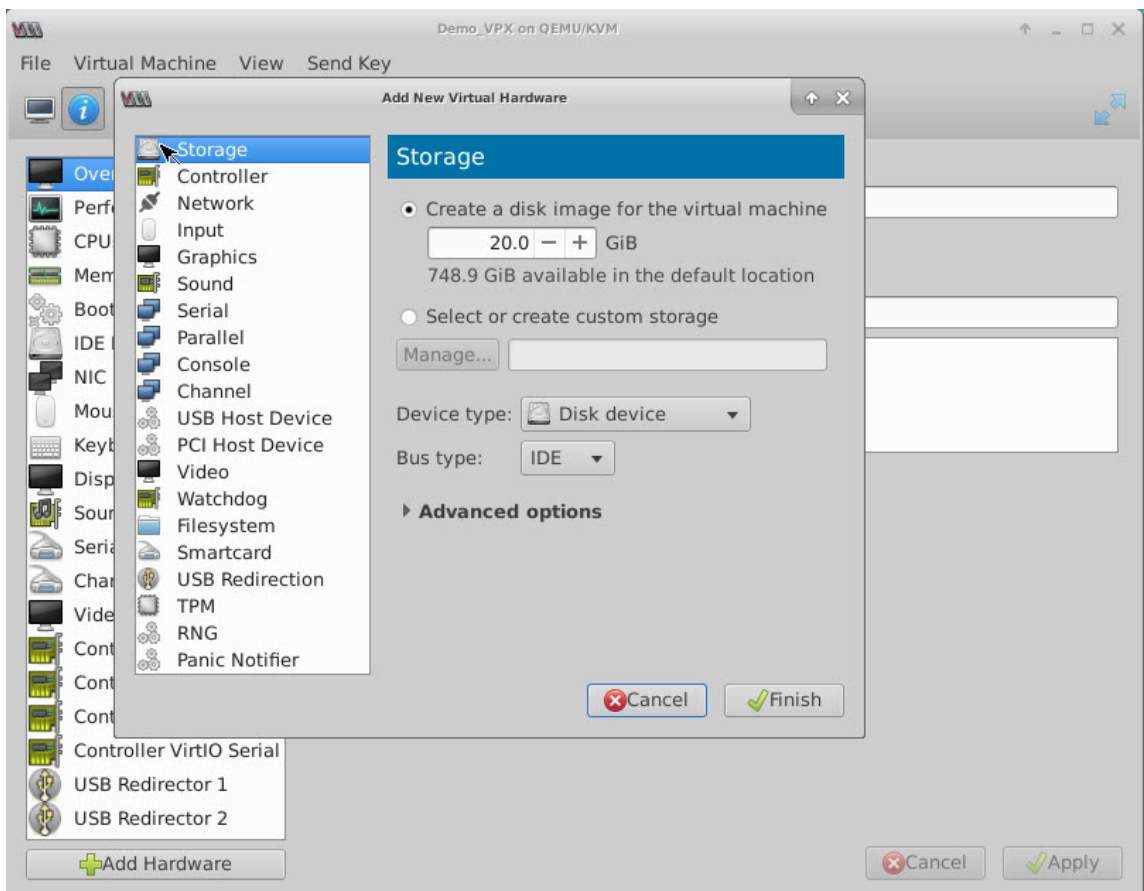
1. Apague la instancia de NetScaler VPX.
2. Seleccione la instancia de NetScaler VPX y, a continuación, seleccione Abrir.



3. En la <virtual machine on KVM>ventana, selecciona el icono **i**.



4. Seleccione **Agregar hardware**.



5. En el cuadro de diálogo **Agregar nuevo hardware virtual**, haga lo siguiente:
 - a) Seleccione Dispositivo de host PCI.
 - b) En la sección Dispositivo host, seleccione el VF que ha creado y haga clic en Finalizar.

Ilustración 4: VF para NIC Intel 82599 10G

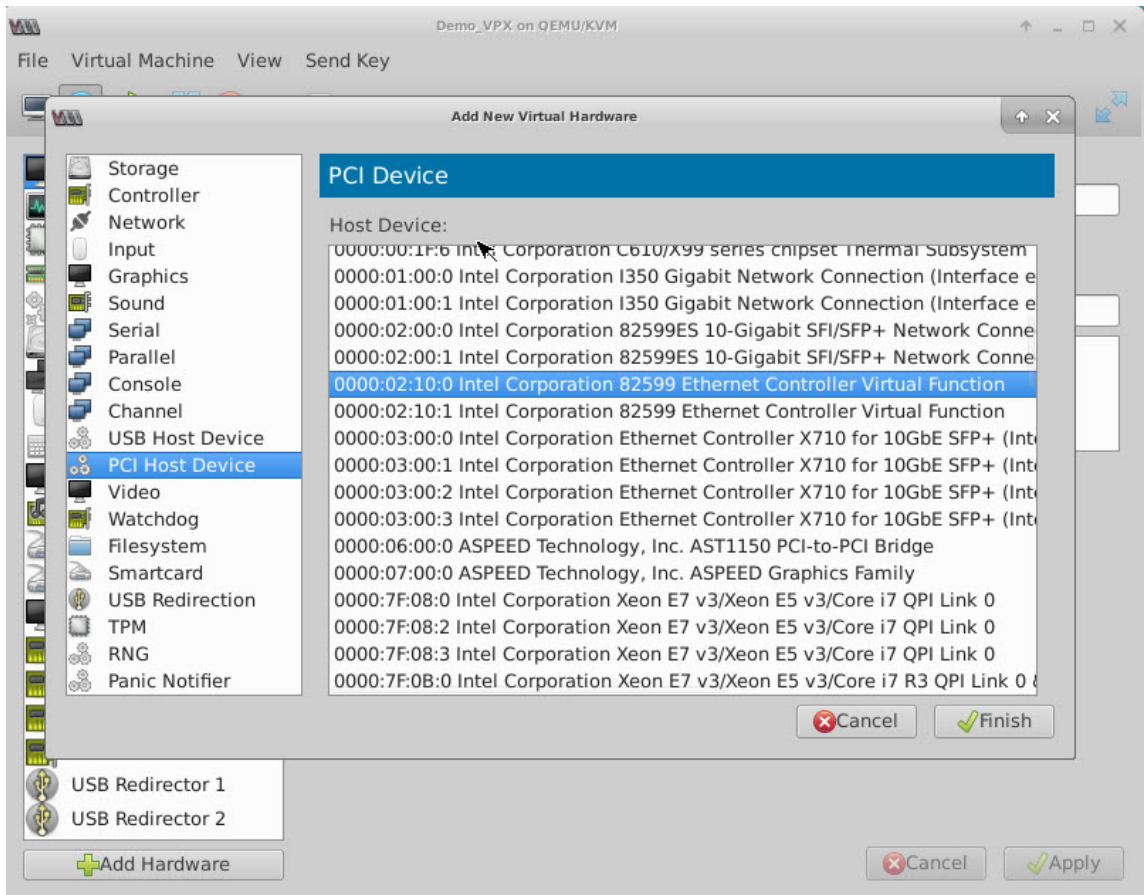


Ilustración 5: VF para la NIC Intel XL710 40G

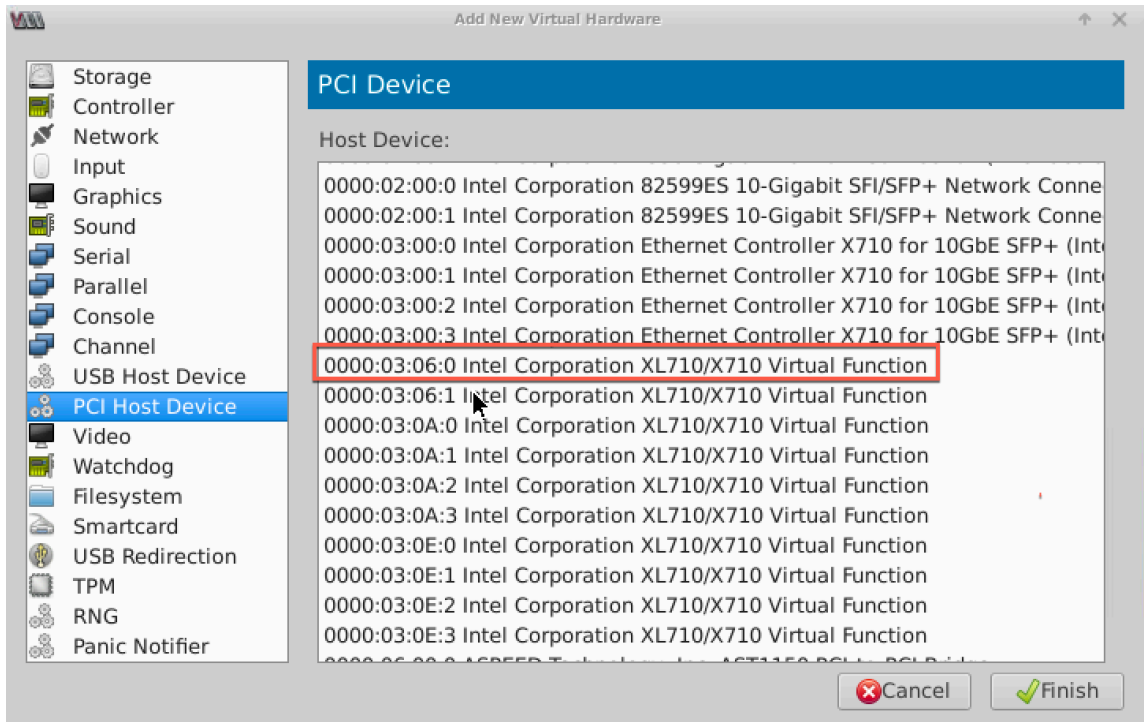
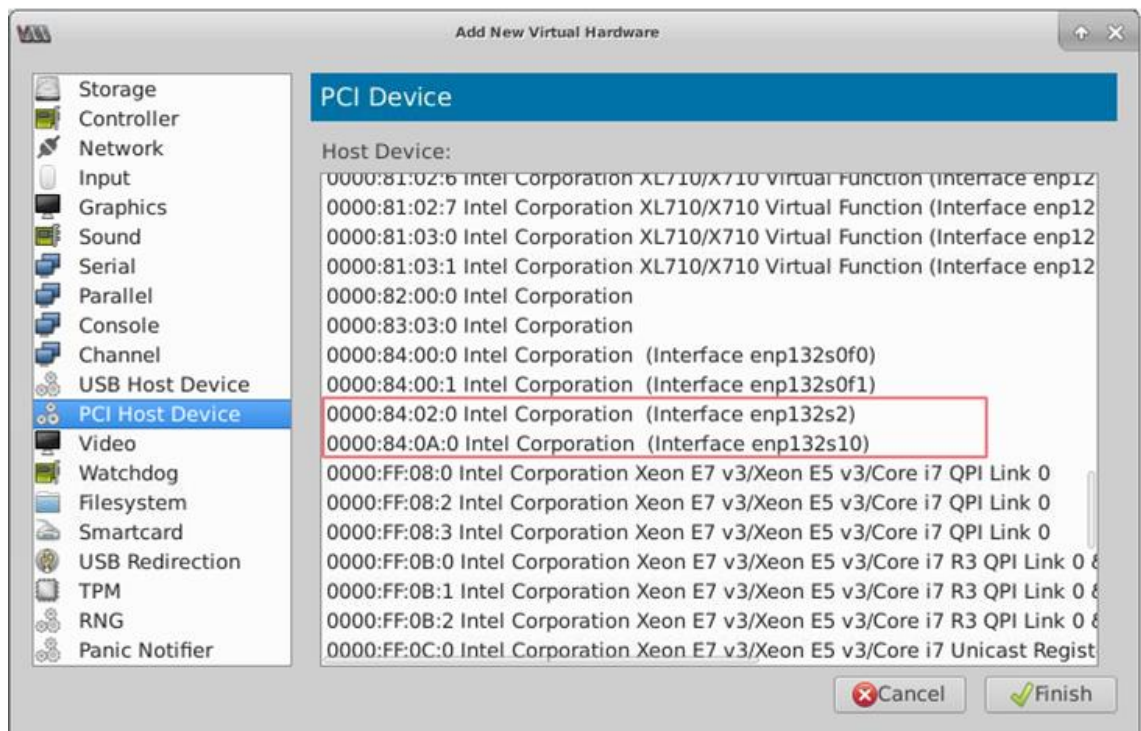


Ilustración 6: VF para la NIC Intel X722 10G



6. Repita los pasos 4 y 5 para agregar los VF que ha creado.
7. Encienda la instancia NetScaler VPX.
8. Una vez que se encienda la instancia de NetScaler VPX, utilice el siguiente comando para comprobar la configuración:

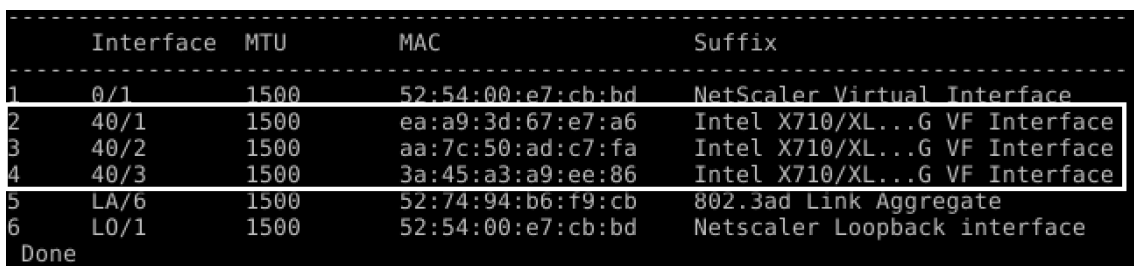
```
1 show interface summary
```

El resultado muestra todas las interfaces que configuró.

Ilustración 6: Resumen de salida para la NIC Intel 82599.



Figura 7. Resumen de salida de las NIC Intel X710 y XL710.



Configurar LA/LACP estático en la interfaz SR-IOV

Importante:

Cuando cree las VFs SR-IOV, asegúrese de no asignar direcciones MAC a las VFs.

Para utilizar las VF SR-IOV en modo de agregación de enlaces, inhabilite la comprobación de suplantación de VF que haya creado. En el host KVM, utilice el siguiente comando para inhabilitar la comprobación de suplantación:

```
*ip link set \\&#060;interface\\_name\\&#062; vf \\&#060;VF\\_id \\&#062; spoofchk off*
```

Donde:

- INTERFACE_NAME: Es el nombre de la interfaz.
- vf_id: Es el id de la función virtual.

Ejemplo:

```
Terminal - root@ubuntu: /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
    link/ether 0c:c4:7a:bd:50:7e brd ff: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 qlen 1000
    link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff:ff
    vf 0 MAC 8e:1a:71:cc:a8:3e, spoof checking on, link-state auto
root@ubuntu:/etc#
root@ubuntu:/etc# ip link set ens3f0 vf 0 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
    link/ether 0c:c4:7a:bd:50:7e brd ff: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 0 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
    link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff:ff
    vf 0 MAC 8e:1a:71:cc:a8:3e, spoof checking off, link-state auto
root@ubuntu:/etc#
```

Después de inhabilitar la comprobación de suplantación para todos los VF que ha creado. Reinicie la instancia de NetScaler VPX y configure la agregación de enlaces. Para obtener instrucciones detalladas, consulte [Configuración de la agregación de enlaces](#).

Configuración de VLAN en la interfaz SR-IOV

Puede configurar VLAN en las VFs SR-IOV. Para obtener instrucciones detalladas, consulte [Configuración de una VLAN](#).

Importante:

Asegúrese de que el host KVM no contenga la configuración de VLAN para la interfaz VF.

Configure un NetScaler VPX en el hipervisor KVM para usar Intel QAT para la aceleración de SSL en modo SR-IOV

October 17, 2024

La instancia de NetScaler VPX en el hipervisor KVM de Linux puede utilizar la tecnología Intel Quick-Assist (QAT) para acelerar el rendimiento de NetScaler SSL. Con Intel QAT, todo el procesamiento criptográfico de alta latencia se puede descargar al chip, lo que libera a una o más CPU host para realizar otras tareas.

Anteriormente, todo el procesamiento criptográfico de las rutas de datos de NetScaler se realizaba en el software mediante vCPU host.

Nota:

Actualmente, NetScaler VPX solo admite el modelo de chip C62x de la familia Intel QAT. Esta función se admite a partir de la versión 14.1, compilación 8.50 de NetScaler.

Requisitos previos

- El host Linux está equipado con un chip Intel QAT C62x, integrado directamente en la placa base o agregado en una tarjeta PCI externa.

Modelos de la serie Intel QAT C62x: C625, C626, C627, C628. Sólo estos modelos C62x incluyen capacidad de cifrado de clave pública (PKE). Otras variantes de C62x no admiten PKE.

- El NetScaler VPX cumple con los requisitos de hardware de VMware ESX. Para obtener más información, consulte [Instalar una instancia de NetScaler VPX en la plataforma Linux KVM](#).

Limitaciones

No hay ninguna disposición para reservar unidades criptográficas o ancho de banda para máquinas virtuales individuales. Todas las unidades criptográficas disponibles de cualquier hardware Intel QAT se comparten entre todas las máquinas virtuales que utilizan el hardware QAT.

Configurar el entorno host para usar Intel QAT

1. Descargue e instale el controlador suministrado por Intel para el modelo de chip de la serie C62x (QAT) en el host Linux. Para obtener más información sobre las instrucciones de instalación y descarga del paquete Intel, consulte el [controlador de tecnología Intel QuickAssist para Linux](#). Hay un archivo readme disponible como parte del paquete de descarga. Un archivo Léame está disponible como parte del paquete de descarga. Este archivo proporciona instrucciones sobre cómo compilar e instalar el paquete en el host.

Tras descargar e instalar el controlador, realice las siguientes comprobaciones de seguridad:

- Anote la cantidad de chips C62x. Cada chip C62x tiene hasta 3 terminales PCIe.
- Asegúrese de que todos los puntos finales estén activos. Ejecute el comando `adf_ctl status` para mostrar el estado de todos los puntos finales PF (hasta 3).

```
1 root@Super-Server:~# adf_ctl status
2
3 Checking status of all devices.
4 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
```

- Habilite SRIOV (soporte VF) para todos los puntos finales de 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
```

- Asegúrese de que se muestren todas las VF (16 VF por punto final, lo que hace un total de 48 VF).
- Ejecute el comando `adf_ctl status` para verificar que todos los puntos finales PF (hasta 3) y los VF de cada chip Intel QAT estén activos. En este ejemplo, el sistema solo tiene un chip C62x. Por lo tanto, tiene 51 puntos finales (3 + 48 VF) en total.

```

root@venkat-Super-Server:~# adf_ctl status
Checking status of all devices.
There is 47 QAT acceleration device(s) in the system:
qat_dev0 - 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: 0000:1c:00.0, #accel: 5 #engines: 10 state: up
qat_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
qat_dev8 - type: c6xxvf, inst_id: 5, node_id: 0, bsf: 0000:1a:01.3, #accel: 1 #engines: 1 state: up
qat_dev9 - type: c6xxvf, inst_id: 6, node_id: 0, bsf: 0000:1a:02.1, #accel: 1 #engines: 1 state: up
qat_dev10 - type: c6xxvf, inst_id: 7, node_id: 0, bsf: 0000:1a:01.4, #accel: 1 #engines: 1 state: up
qat_dev11 - type: c6xxvf, inst_id: 8, node_id: 0, bsf: 0000:1a:01.5, #accel: 1 #engines: 1 state: up
qat_dev12 - type: c6xxvf, inst_id: 9, node_id: 0, bsf: 0000:1a:02.2, #accel: 1 #engines: 1 state: up
qat_dev13 - type: c6xxvf, inst_id: 10, node_id: 0, bsf: 0000:1a:01.6, #accel: 1 #engines: 1 state: up
qat_dev14 - type: c6xxvf, inst_id: 11, node_id: 0, bsf: 0000:1a:02.3, #accel: 1 #engines: 1 state: up
qat_dev15 - type: c6xxvf, inst_id: 12, node_id: 0, bsf: 0000:1a:02.4, #accel: 1 #engines: 1 state: up
qat_dev16 - type: c6xxvf, inst_id: 13, node_id: 0, bsf: 0000:1a:02.5, #accel: 1 #engines: 1 state: up
qat_dev17 - type: c6xxvf, inst_id: 14, node_id: 0, bsf: 0000:1a:02.6, #accel: 1 #engines: 1 state: up
qat_dev18 - type: c6xxvf, inst_id: 15, node_id: 0, bsf: 0000:1a:02.7, #accel: 1 #engines: 1 state: up
qat_dev19 - type: c6xxvf, inst_id: 16, node_id: 0, bsf: 0000:1b:01.0, #accel: 1 #engines: 1 state: up
qat_dev20 - type: c6xxvf, inst_id: 17, node_id: 0, bsf: 0000:1b:01.1, #accel: 1 #engines: 1 state: up
qat_dev21 - type: c6xxvf, inst_id: 18, node_id: 0, bsf: 0000:1b:01.2, #accel: 1 #engines: 1 state: up
qat_dev22 - type: c6xxvf, inst_id: 19, node_id: 0, bsf: 0000:1b:01.3, #accel: 1 #engines: 1 state: up
qat_dev23 - type: c6xxvf, inst_id: 20, node_id: 0, bsf: 0000:1b:01.4, #accel: 1 #engines: 1 state: up
qat_dev24 - type: c6xxvf, inst_id: 21, node_id: 0, bsf: 0000:1b:01.5, #accel: 1 #engines: 1 state: up
qat_dev25 - type: c6xxvf, inst_id: 22, node_id: 0, bsf: 0000:1b:01.6, #accel: 1 #engines: 1 state: up
qat_dev26 - type: c6xxvf, inst_id: 23, node_id: 0, bsf: 0000:1b:01.7, #accel: 1 #engines: 1 state: up
qat_dev27 - type: c6xxvf, inst_id: 24, node_id: 0, bsf: 0000:1b:02.0, #accel: 1 #engines: 1 state: up
qat_dev28 - type: c6xxvf, inst_id: 25, node_id: 0, bsf: 0000:1b:02.1, #accel: 1 #engines: 1 state: up
qat_dev29 - type: c6xxvf, inst_id: 26, node_id: 0, bsf: 0000:1b:02.2, #accel: 1 #engines: 1 state: up
qat_dev30 - type: c6xxvf, inst_id: 27, node_id: 0, bsf: 0000:1b:02.3, #accel: 1 #engines: 1 state: up
qat_dev31 - type: c6xxvf, inst_id: 28, node_id: 0, bsf: 0000:1b:02.4, #accel: 1 #engines: 1 state: up
qat_dev32 - type: c6xxvf, inst_id: 29, node_id: 0, bsf: 0000:1b:02.5, #accel: 1 #engines: 1 state: up
qat_dev33 - type: c6xxvf, inst_id: 30, node_id: 0, bsf: 0000:1b:02.6, #accel: 1 #engines: 1 state: up
qat_dev34 - type: c6xxvf, inst_id: 31, node_id: 0, bsf: 0000:1b:02.7, #accel: 1 #engines: 1 state: up
qat_dev39 - type: c6xxvf, inst_id: 32, node_id: 0, bsf: 0000:1c:01.4, #accel: 1 #engines: 1 state: up
qat_dev40 - type: c6xxvf, inst_id: 33, node_id: 0, bsf: 0000:1c:01.5, #accel: 1 #engines: 1 state: up
qat_dev41 - type: c6xxvf, inst_id: 34, node_id: 0, bsf: 0000:1c:01.6, #accel: 1 #engines: 1 state: up
qat_dev42 - type: c6xxvf, inst_id: 35, node_id: 0, bsf: 0000:1c:01.7, #accel: 1 #engines: 1 state: up
qat_dev43 - type: c6xxvf, inst_id: 36, node_id: 0, bsf: 0000:1c:02.0, #accel: 1 #engines: 1 state: up
qat_dev44 - type: c6xxvf, inst_id: 37, node_id: 0, bsf: 0000:1c:02.1, #accel: 1 #engines: 1 state: up
qat_dev45 - type: c6xxvf, inst_id: 38, node_id: 0, bsf: 0000:1c:02.2, #accel: 1 #engines: 1 state: up
qat_dev46 - type: c6xxvf, inst_id: 39, node_id: 0, bsf: 0000:1c:02.3, #accel: 1 #engines: 1 state: up
qat_dev47 - type: c6xxvf, inst_id: 40, node_id: 0, bsf: 0000:1c:02.4, #accel: 1 #engines: 1 state: up
qat_dev48 - type: c6xxvf, inst_id: 41, node_id: 0, bsf: 0000:1c:02.5, #accel: 1 #engines: 1 state: up
qat_dev49 - type: c6xxvf, inst_id: 42, node_id: 0, bsf: 0000:1c:02.6, #accel: 1 #engines: 1 state: up
qat_dev50 - type: c6xxvf, inst_id: 43, node_id: 0, bsf: 0000:1c:02.7, #accel: 1 #engines: 1 state: up
root@venkat-Super-Server:~#

```

2. Habilite SR-IOV en el host Linux.
3. Cree máquinas virtuales. Al crear una máquina virtual, asigne la cantidad adecuada de dispositivos PCI para cumplir con los requisitos de rendimiento.

Nota:

Cada chip C62x (QAT) puede tener hasta tres terminales PCI independientes. Cada punto final es una colección lógica de VF y comparte el ancho de banda en partes iguales con otros puntos finales PCI del chip. Cada terminal puede tener hasta 16 VF que se muestran como 16 dispositivos PCI. Agregue estos dispositivos a la máquina virtual para realizar la aceleración criptográfica con el chip QAT.

Puntos a tener en cuenta

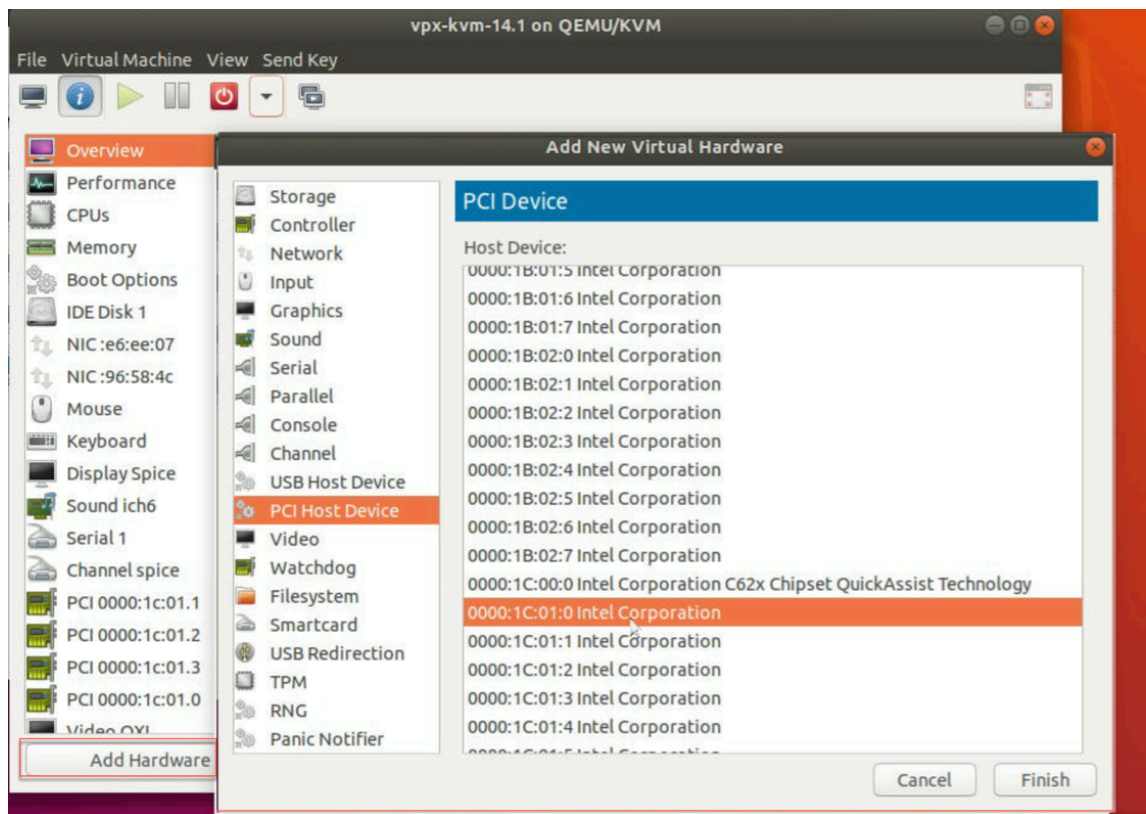
- Si el requisito de cifrado de máquinas virtuales es utilizar más de un punto final o chip PCI QAT, le recomendamos que elija los dispositivos PCI o VF correspondientes de forma rotativa para tener una distribución simétrica.
- Recomendamos que la cantidad de dispositivos PCI seleccionados sea igual a la cantidad de vCPU con licencia (sin incluir el recuento de vCPU de administración). Agregar más dispositivos PCI que la cantidad disponible de vCPU no necesariamente mejora el rendimiento.

Ejemplo

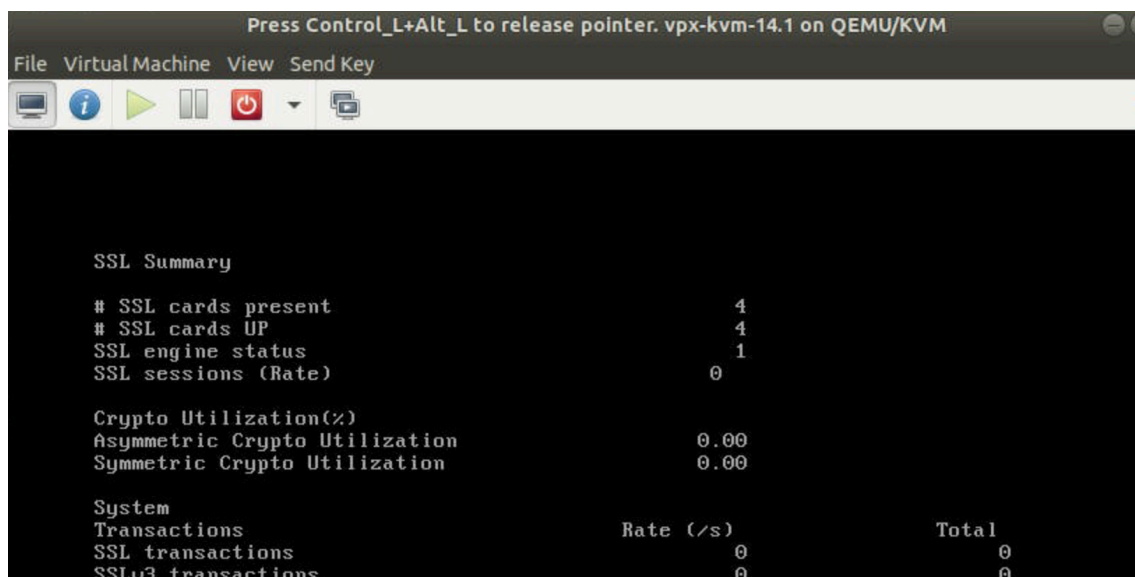
Considere un host Linux con un chip Intel C62x que tenga 3 terminales. Al provisionar una máquina virtual con 6 vCPU, elija 2 máquinas virtuales de cada punto final y asígnelas a la máquina virtual. Esta asignación garantiza una distribución efectiva y equitativa de las unidades criptográficas para la máquina virtual. Del total de vCPU disponibles, de forma predeterminada, una vCPU está reservada para el plano de administración y el resto de las vCPU están disponibles para los PE del plano de datos.

Asigne vF de QAT a NetScaler VPX implementado en el hipervisor KVM de Linux

1. En el administrador de máquinas virtuales KVM de Linux, asegúrese de que la máquina virtual (NetScaler VPX) esté apagada.
2. Navegue hasta **Agregar hardware > Dispositivo host PCI**.
3. Asigne Intel QAT VF al dispositivo PCI.



4. Haga clic en **Finalizar**.
5. Repita los pasos anteriores para asignar una o más VF Intel QAT a la instancia de NetScaler VPX hasta el límite de una unidad menos que la cantidad total de vCPU. Porque una vCPU está reservada para el proceso de administración.
 Cantidad de VF de QAT por VM = Cantidad de vCPU: 1
6. Power on the VM.
7. Ejecute el comando `stat ssl` en la CLI de NetScaler para mostrar el resumen de SSL y verifique las tarjetas SSL después de asignar las VF de QAT a NetScaler VPX.
 En este ejemplo, hemos utilizado 5 vCPU, lo que implica 4 motores de paquetes (PE).



```
Press Control_L+Alt_L to release pointer. vpx-kvm-14.1 on QEMU/KVM
File Virtual Machine View Send Key
SSL Summary
# SSL cards present          4
# SSL cards UP              4
SSL engine status           1
SSL sessions (Rate)        0

Crypto Utilization(%)
Asymmetric Crypto Utilization 0.00
Symmetric Crypto Utilization  0.00

System
Transactions                Rate (/s)      Total
SSL transactions            0              0
SSLv3 transactions         0              0
```

Acerca de la implementación

Esta implementación se probó con las siguientes especificaciones de componentes:

- Versión y compilación de **NetScaler VPX** : 14.1—8.50
- **Versión de Ubuntu**: 18.04, Kernel 5.4.0-146
- **Versión del controlador Intel C62x QAT para Linux** : L.4.21.0-00001

Configurar una instancia de NetScaler VPX para utilizar las interfaces de red de transferencia PCI

October 17, 2024

Tras instalar y configurar una instancia de NetScaler VPX en la plataforma Linux-KVM, puede utilizar el Administrador de máquinas virtuales para configurar el dispositivo virtual para que utilice las interfaces de red de transferencia PCI.

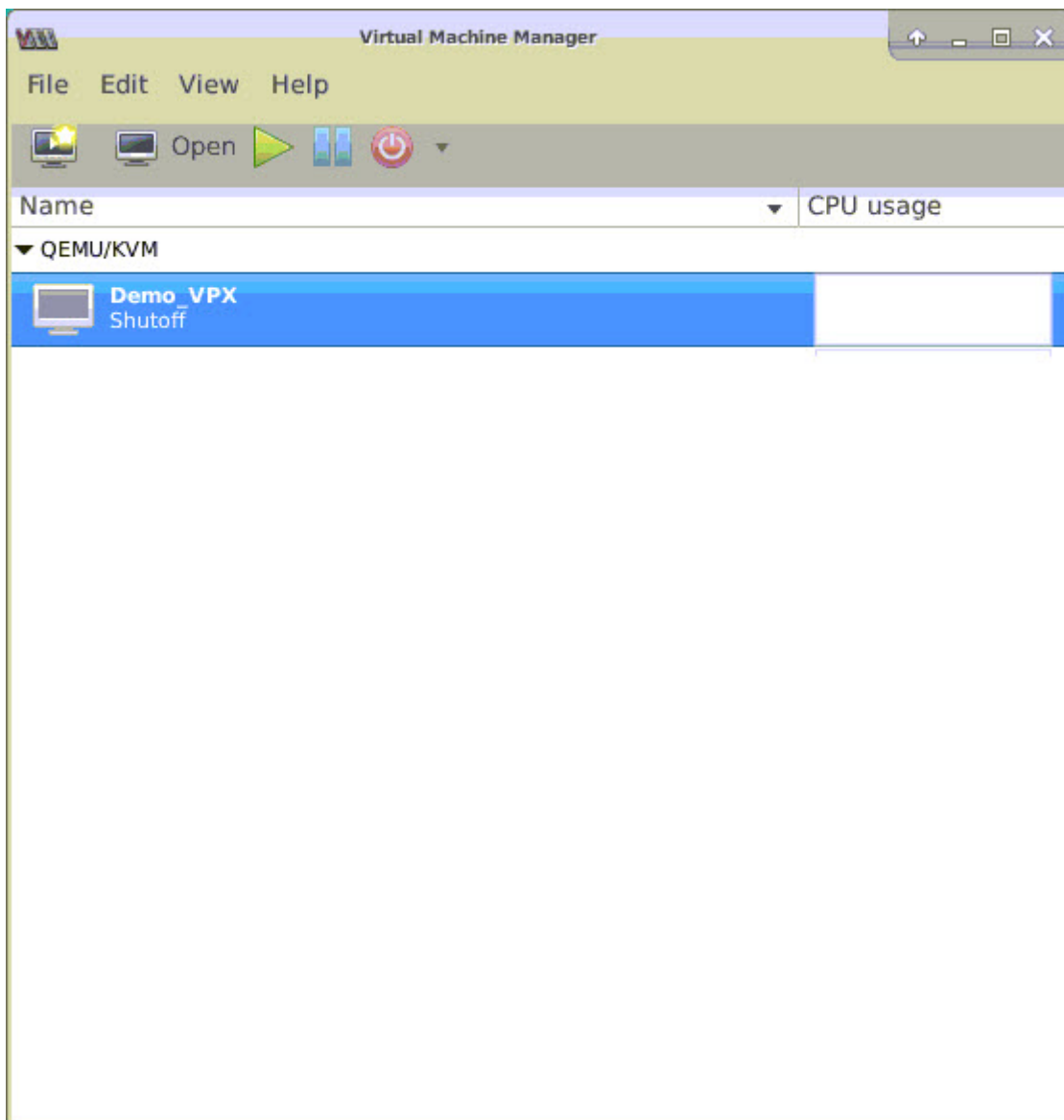
Requisitos previos

- La versión de firmware de la NIC (NIC) Intel XL710 en el host KVM es 5.04.
- El host KVM admite la unidad de administración de memoria de entrada/salida (IOMMU) e Intel VT-d, y están habilitados en el BIOS del host KVM. En el host KVM, para habilitar IOMMU, agregue la siguiente entrada al archivo **/boot/grub2/grub.cfg**: **intel_iommu=1**

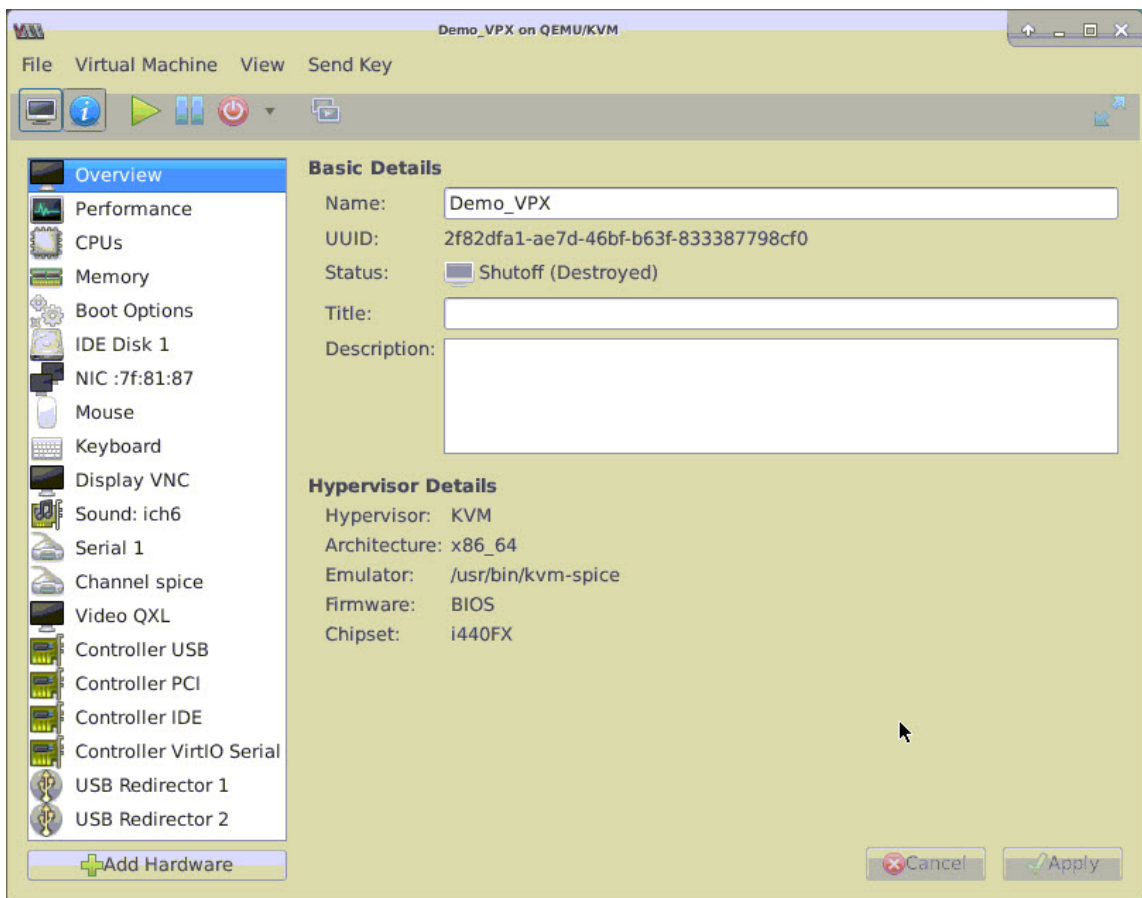
- Ejecute el siguiente comando y reinicie el host KVM: **Grub2-mkConfig --o /boot/-grub2/grub.cfg**

Para configurar instancias de NetScaler VPX para que utilicen interfaces de red de transferencia PCI mediante Virtual Machine Manager:

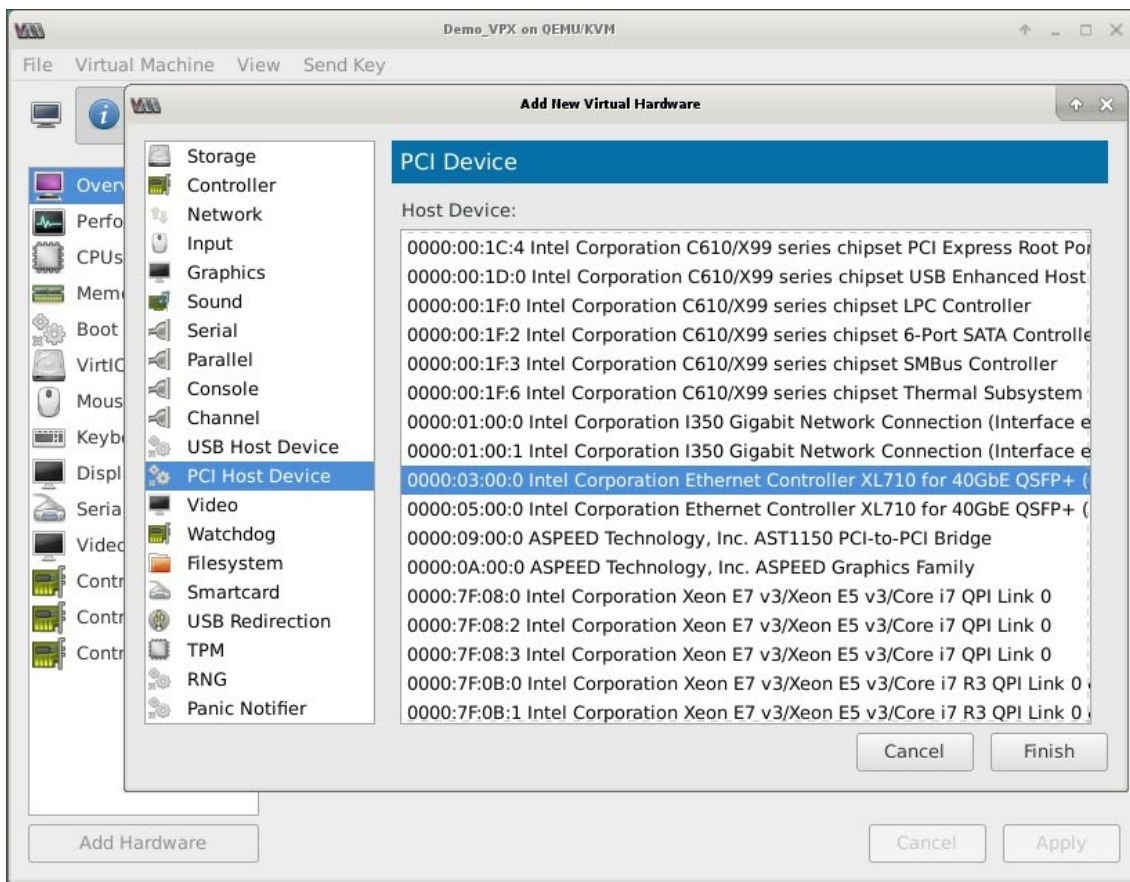
1. Apague la instancia de NetScaler VPX.
2. Seleccione la instancia de NetScaler VPX y haga clic en **Abrir**.



3. En la ventana **virtual_machine en KVM**, haga clic en el icono **i**.



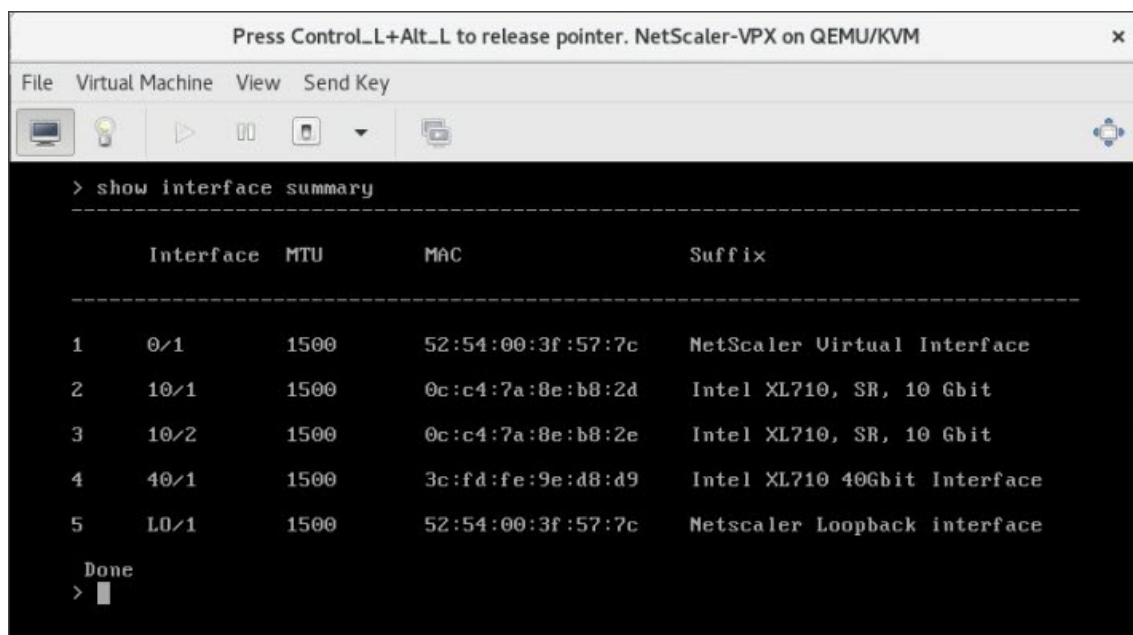
4. Haga clic en **Agregar hardware**.
5. En el cuadro de diálogo **Agregar nuevo hardware virtual**, haga lo siguiente:
 - a. Seleccione **Dispositivo host PCI**.
 - b. En la sección **Dispositivo anfitrión**, seleccione la función física Intel XL710.
 - c. Haga clic en **Finalizar**.



6. Repita los pasos 4 y 5 para agregar funciones físicas adicionales de Intel XL710.
7. Encienda la instancia NetScaler VPX.
8. Una vez que se enciende la instancia de NetScaler VPX, puede utilizar el siguiente comando para verificar la configuración:

```
COMMAND
> show interface summary
```

El resultado debe mostrar todas las interfaces que ha configurado:



```
> show 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
> █
```

Aprovisionamiento de la instancia NetScaler VPX mediante el virsh programa

October 17, 2024

El `virsh` programa es una herramienta de línea de comandos para administrar invitados de VM. Su funcionalidad es similar a la de Virtual Machine Manager. Le permite cambiar el estado de un invitado de VM (iniciar, detener, pausar, etc.), configurar nuevos invitados y dispositivos y modificar las configuraciones existentes. El `virsh` programa también es útil para crear scripts de operaciones de administración de invitados de VM.

Para aprovisionar NetScaler VPX mediante el `virsh` programa, siga estos pasos:

1. Utilice el comando `tar` para desatar el paquete NetScaler VPX. El paquete `NSVPX-KVM-*_NC.tgz` contiene los siguientes componentes:
 - Archivo XML de dominio que especifica atributos VPX [`NSVPX-KVM-*_NC.xml`]
 - Comprobar la suma de la imagen de disco NS-VM [`Checksum.txt`]
 - Imagen de disco NS-VM [`NSVPX-KVM-*_NC.raw`]

Ejemplo

```
1 tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
2 NSVPX-KVM-10.1-117_nc.xml
3 NSVPX-KVM-10.1-117_nc.raw
4 checksum.txt
```

2. Copie el archivo XML `NSVPX-KVM-*_nc.xml` en un archivo llamado `\\<DomainName\\>-NSVPX-KVM-*_nc.xml`. El `<DomainName>` es también el nombre de la máquina virtual. Ejemplo

```
1 cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.xml
```

3. Edite el archivo `\\<DomainName\\>-NSVPX-KVM-*_nc.xml` para especificar los siguientes parámetros:

- name: Especifique el nombre.
- Mac: especifique la dirección MAC.

Nota:

El nombre de dominio y la dirección MAC deben ser únicos.

- archivo fuente: especifique la ruta de origen absoluta de la imagen de disco. La ruta del archivo tiene que ser absoluta. Puede especificar la ruta del archivo de imagen RAW o de un archivo de imagen QCOW2.

Si quiere especificar un archivo de imagen RAW, especifique la ruta de origen de la imagen de disco como se muestra en el ejemplo siguiente:

Ejemplo

```
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' />
```

Especifique la ruta de origen de imagen de disco QCOW2 absoluta y defina el tipo de controlador como **qcow2**, como se muestra en el ejemplo siguiente:

Ejemplo

```
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. Edite el archivo `\\<DomainName\\>-NSVPX-KVM-*_nc.xml` para configurar los detalles de la red:

- source dev: Especifique la interfaz.
- modo: Especifique el modo. La interfaz predeterminada es **Macvtap Bridge**.

Ejemplo: Modo: puente MacVTap Establecer interfaz de destino como `ethx` y modo como puente Tipo de modelo como `virtio`

```

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

```

Aquí, eth0 es la interfaz física conectada a la VM.

- Defina los atributos de la máquina virtual en el archivo `\\<DomainName\\>-NSVPX-KVM-*_nc.xml` utilizando el siguiente comando:

```
1 virsh define \\<DomainName>-NSVPX-KVM-*\\_nc.xml
```

Ejemplo

```
1 virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

- Inicio la máquina virtual ingresando el siguiente comando:

```
1 virsh start \\<DomainName> | \\<DomainUUID>\\
```

Ejemplo

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

- Conectar la VM invitada a través de la consola:

```
1 virsh console \\<DomainName> | \\<DomainUUID> | \\<DomainID> \\
```

Ejemplo

```
1 virsh console NetScaler-VPX
```

Agregar más interfaces a la instancia NetScaler VPX mediante el `virsh` programa

Después de haber provisionado NetScaler VPX en KVM, puede agregar interfaces adicionales.

Para añadir más interfaces, sigue estos pasos:

- Apague la instancia de NetScaler VPX que se ejecuta en el KVM.
- Edite el archivo `\\<DomainName\\>-NSVPX-KVM-*_nc.xml` usando el comando:

```
1 virsh edit \\<DomainName> | \\<DomainUUID>\\
```

3. En el archivo `\\<DomainName\\>-NSVPX-KVM-*_nc.xml` , agregue los siguientes parámetros:

a) **Para MacVtap**

- Tipo de interfaz: Especifique el tipo de interfaz como 'direct'.
- Dirección MAC: especifique la dirección MAC y asegúrese de que la dirección MAC sea única en todas las interfaces.
- source dev: Especifique el nombre de la interfaz.
- mode: especifique el modo. Los modos admitidos son: Bridge, VEPA, Privado y Pass-through
- tipo de modelo: especifique el tipo de modelo como `virtio`

Ejemplo

Modo: MacVTap PassThrough

Establecer la interfaz de destino como `ethx`, Modo como puente y tipo de modelo como `virtud`

```
1 <interface type='direct'>
2     <mac address='52:54:00:29:74:b3' />
3     <source dev='eth1' mode='passthrough' />
4     <model type='virtio' />
5 </interface>
```

Aquí `eth1` es la interfaz física conectada a la VM.

b) **Para modo puente**

Nota:

Asegúrese de haber configurado un puente Linux en el host KVM, haber vinculado la interfaz física al puente y haber puesto el puente en estado activo.

- Tipo de interfaz: Especifique el tipo de interfaz como "puente".
- Dirección MAC: especifique la dirección MAC y asegúrese de que la dirección MAC sea única en todas las interfaces.
- puente de origen: Especifique el nombre del puente.
- tipo de modelo: especifique el tipo de modelo como `virtio`

Ejemplo: modo Bridge

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

Administrar las VM invitadas de NetScaler VPX

October 17, 2024

Puede utilizar Virtual Machine Manager y el `virsh` programa para realizar tareas de administración, como iniciar o detener un invitado de máquina virtual, configurar nuevos invitados y dispositivos, modificar configuraciones existentes y conectarse a la consola gráfica mediante Virtual Network Computing (VNC).

Administrar las VM invitadas VPX mediante Virtual Machine Manager

- Listar los invitados de VM

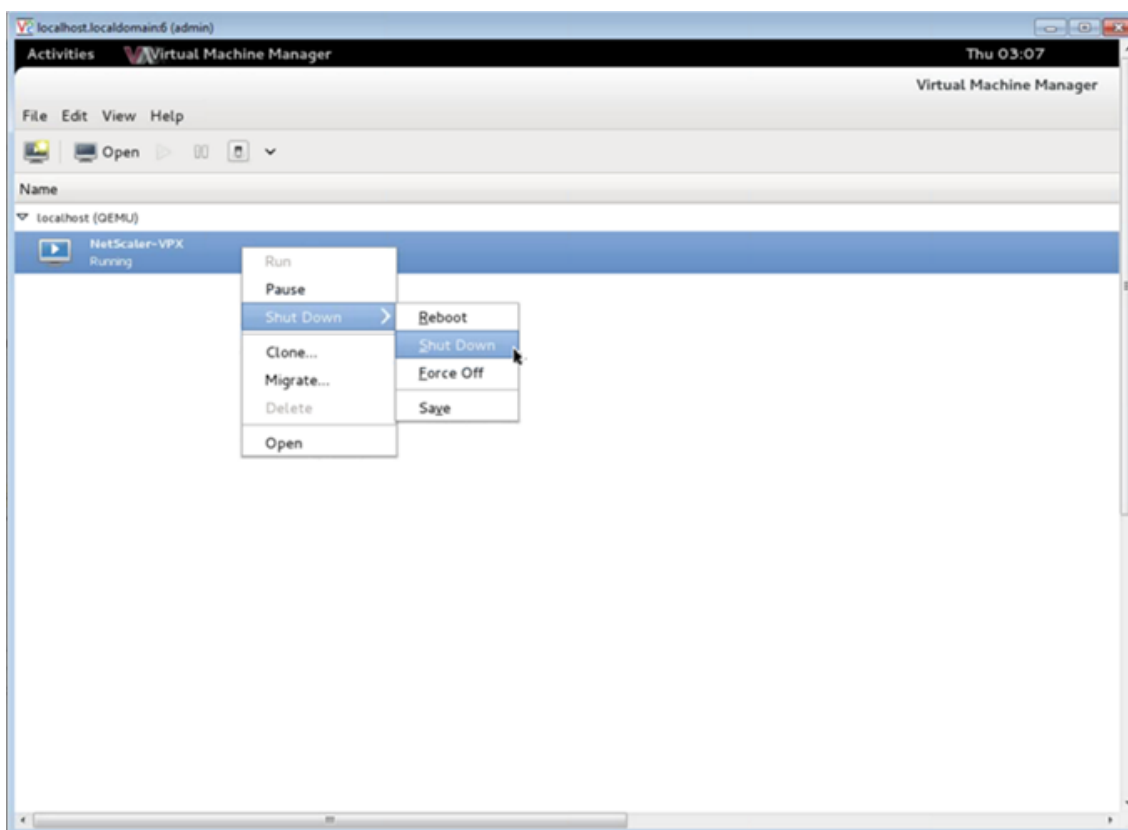
La ventana principal de Virtual Machine Manager muestra una lista de todos los invitados de VM para cada servidor host de VM al que está conectado. Cada entrada de invitado de máquina virtual contiene el nombre de la máquina virtual, junto con su estado (En ejecución, pausa o apagado) que se muestra como en el icono.

- Abrir una consola gráfica

Abrir una consola gráfica a un invitado de VM le permite interactuar con la máquina como lo haría con un host físico a través de una conexión VNC. Para abrir la consola gráfica en Virtual Machine Manager, haga clic con el botón derecho en la entrada de VM Guest y seleccione la opción Abrir en el menú emergente.

- Iniciar y cerrar un invitado

Puede iniciar o detener un invitado de VM desde Virtual Machine Manager. Para cambiar el estado de la VM, haga clic con el botón secundario en la entrada Invitado de VM y seleccione Ejecutar o una de las opciones de Apagar en el menú emergente.



- Reiniciar un invitado

Puede reiniciar un invitado de VM desde Virtual Machine Manager. Para reiniciar la VM, haga clic con el botón secundario en la entrada Invitado de VM y, a continuación, seleccione Apagar > Reiniciar en el menú emergente.

- Eliminar un invitado

Al eliminar un invitado de VM, se elimina su configuración XML de forma predeterminada. También puede eliminar los archivos de almacenamiento de un invitado. Al hacerlo, se borra completamente al invitado.

1. En Virtual Machine Manager, haga clic con el botón secundario en la entrada VM Guest.
2. Seleccione Eliminar en el menú emergente. Se abre una ventana de confirmación.

Nota:

La opción Eliminar está habilitada solo cuando el invitado de la máquina virtual está apagado.

3. Haga clic en **Eliminar**.
4. Para borrar completamente el invitado, elimine el archivo.raw asociado activando la casilla de verificación Eliminar archivos de almacenamiento asociados.

Administrar las máquinas virtuales invitadas NetScaler VPX mediante el `virsh` programa

- Enumere los invitados de VM y sus estados actuales.

Para utilizar `virsh` para mostrar información sobre los Huéspedes

```
virsh list --all
```

El resultado del comando muestra todos los dominios con sus estados. Salida de ejemplo:

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

- Abre una `virsh` consola.

Conectar la VM invitada a través de la consola

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

Ejemplo

```
virsh console NetScaler-VPX
```

- Empezar y cerrar a un invitado.

Los invitados se pueden iniciar mediante `DomainName` o `Domain-UUID`.

```
virsh start [<DomainName> | <DomainUUID>]
```

Ejemplo

```
virsh start NetScaler-VPX
```

Para cerrar un invitado:

```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
```

Ejemplo

```
virsh shutdown NetScaler-VPX
```

- Reiniciar un invitado

```
virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
```

Ejemplo

```
virsh reboot NetScaler-VPX
```

Eliminar un invitado

Para eliminar una máquina virtual invitada, debe apagar la máquina invitada y anular la definición de -NSVPX-KVM <DomainName>- * _nc.xml antes de ejecutar el comando delete.

```
1  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
2  virsh undefine [<DomainName> | <DomainUUID>]
```

Ejemplo

```
1  virsh shutdown NetScaler-VPX
2  virsh undefine NetScaler-VPX
```

Nota:

El comando eliminar no elimina el archivo de imagen de disco, que debe eliminarse manualmente.

Aprovisione la instancia de NetScaler VPX con SR-IOV, en OpenStack

October 17, 2024

Puede implementar instancias de NetScaler VPX de alto rendimiento que utilicen la tecnología de virtualización de E/S de raíz única (SR-IOV) en OpenStack.

Puede implementar una instancia de NetScaler VPX que utilice la tecnología SR-IOV, en OpenStack, en tres pasos:

- Habilite las funciones virtuales (VF) de SR-IOV en el host.
- Configure y haga que los VF estén disponibles para OpenStack.
- Aprovisione el NetScaler VPX en OpenStack.

Requisitos previos

Asegúrese de que:

- Agregue la NIC (NIC) Intel 82599 al host.
- Descargue e instale el controlador IXGBE más reciente de Intel.
- Lista de bloques del controlador IXGBEVF del host. Agregue la siguiente entrada en el archivo `/etc/modprobe.d/blacklist.conf`: Lista de bloques `ixgbev`

Nota:

La versión del `ixgbe` controlador debe ser mínima 5.0.4.

Habilitar las VF SR-IOV en el host

Realice uno de los siguientes pasos para habilitar las VF SR-IOV:

- <number_of_VFs> Si está usando una versión del núcleo anterior a 3.8, agregue la siguiente entrada al archivo /etc/modprobe.d/ixgbe y reinicie el host: Options ixgbe max_vfs=
- Si está usando la versión 3.8 del kernel o posterior, cree VF mediante el siguiente comando:

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

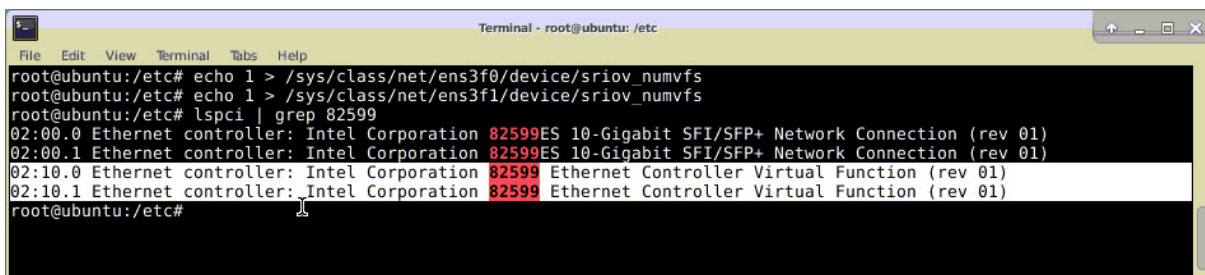
Donde:

- número_de_vfs es el número de funciones virtuales que quiere crear.
- nombre_dispositivo es el nombre de la interfaz.

Importante:

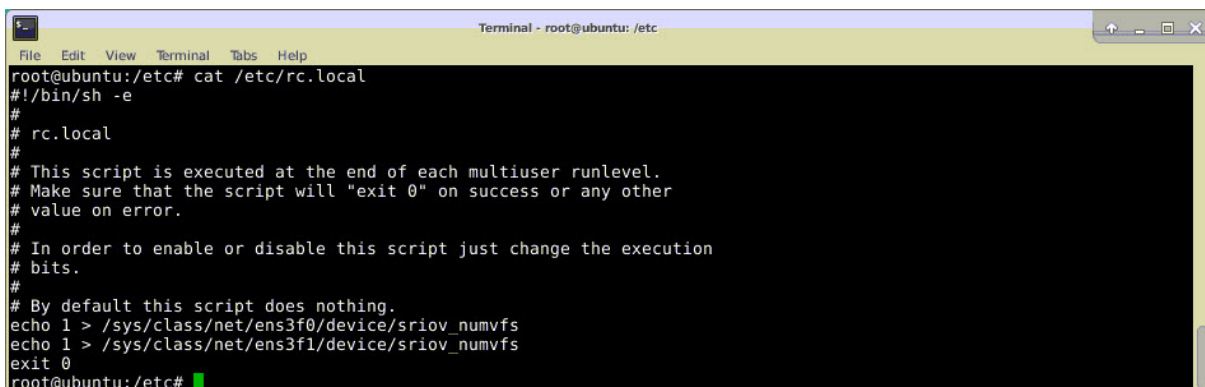
Mientras crea las VFs SR-IOV, asegúrese de no asignar direcciones MAC a las VFs.

Aquí hay un ejemplo de cuatro VF que se están creando.



```
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#
```

Haga que los VF sean persistentes, agregue los comandos que utilizó para crear VF al archivo **rc.local**. A continuación se muestra un ejemplo que muestra el contenido del archivo rc.local.



```
Terminal - root@ubuntu: /etc
File Edit View Terminal Tabs Help
root@ubuntu:/etc# cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
echo 1 > /sys/class/net/ens3f0/device/sriov_numvfs
echo 1 > /sys/class/net/ens3f1/device/sriov_numvfs
exit 0
root@ubuntu:/etc#
```

Para obtener más información, consulte esta [Guía de configuración de Intel SR-IOV](#).

Configurar y hacer que los VF estén disponibles para OpenStack

Siga los pasos que se indican en el siguiente enlace para configurar SR-IOV en OpenStack: <https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking>.

Aprovisione la instancia NetScaler VPX en OpenStack

Puede aprovisionar una instancia NetScaler VPX en un entorno OpenStack mediante la CLI de OpenStack.

Aprovisionar una instancia VPX, opcionalmente implica el uso de datos de la unidad de configuración. La unidad de configuración es una unidad de configuración especial que se conecta a la instancia cuando se inicia. Esta unidad de configuración se puede utilizar para pasar información de configuración de red, como la dirección IP de administración, la máscara de red y la puerta de enlace predeterminada, etc. a la instancia antes de configurar la configuración de red de la instancia.

Cuando OpenStack aprovisiona una instancia VPX, primero detecta que la instancia se está iniciando en un entorno OpenStack, leyendo una cadena de BIOS específica (OpenStack Foundation) que indica OpenStack. Para distribuciones de Red Hat Linux, la cadena se almacena en `/etc/nova/release`. Este es un mecanismo estándar que está disponible en todas las implementaciones de OpenStack basadas en la plataforma de hipervisor KVM. La unidad debe tener una etiqueta OpenStack específica. Si se detecta la unidad de configuración, la instancia intenta leer la siguiente información del nombre de archivo especificado en el comando de `nova` arranque. En los procedimientos siguientes, el archivo se llama “`userdata.txt`”.

- Dirección IP de administración
- Máscara de red
- Puerta de enlace predeterminada

Una vez que los parámetros se leen correctamente, se rellenan en la pila NetScaler. Esto ayuda a administrar la instancia de forma remota. Si los parámetros no se leen correctamente o la unidad de configuración no está disponible, la instancia pasa al comportamiento predeterminado, que es:

- La instancia intenta recuperar la información de la dirección IP de DHCP.
- Si DHCP falla o supera el tiempo de espera, la instancia aparece con la configuración de red predeterminada (192.168.100.1/16).

Aprovisione la instancia de NetScaler VPX en OpenStack mediante CLI

Puede aprovisionar una instancia VPX en un entorno OpenStack mediante la CLI de OpenStack. Este es el resumen de los pasos para aprovisionar una instancia de NetScaler VPX en OpenStack:

1. Extracción del `.qcow2` archivo del `archivo.tgz`

2. Crear una imagen de OpenStack a partir de la imagen qcow2
3. Aprovisionamiento de una instancia VPX

Para aprovisionar una instancia VPX en un entorno OpenStack, siga estos pasos.

1. Extraiga el `qcow2` del `.tgz` archivo escribiendo el comando:

```
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. Cree una imagen de OpenStack mediante el `qcow2` archivo extraído en el paso 1 escribiendo el siguiente comando:

```
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
```

La siguiente ilustración proporciona un ejemplo de salida para el comando `glance image-create`.

Property	Value
checksum	735dae4ea6e46e39ed3f0acfb02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Después de crear una imagen de OpenStack, aprovisione la instancia 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-
4 02086a6bdee2 NSVPX-10

```

En el comando anterior, `userdata.txt` es el archivo que contiene detalles como dirección IP, máscara de red y puerta de enlace predeterminada para la instancia VPX. El archivo de datos de usuario es un archivo personalizable por el usuario. `NSVPX-KVM-12.0-26.2` es el nombre del dispositivo virtual que desea aprovisionar. `--NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2` es OpenStack VF.

En la siguiente ilustración se muestra un resultado de ejemplo del comando de `nova` arranque.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

En la siguiente ilustración se muestra un ejemplo del archivo userdata.txt. Los valores de las\

```

1  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2  <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
   "
3  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4  oe:id=""
5  xmlns="http://schemas.dmtf.org/ovf/environment/1">
6  <PlatformSection>
7  <Kind>NOVA</Kind>
8  <Version>2013.1</Version>
9  <Vendor>Openstack</Vendor>
10 <Locale>en</Locale>
11 </PlatformSection>
12 <PropertySection>
13 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
   1.0"/>
14 <Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"
   />
15 citrix.com 4
16 <Property oe:key="com.citrix.netscaler.orch_env"
17 oe:value="openstack-orch-env"/>
18 <Property oe:key="com.citrix.netscaler.mgmt.ip"
19 oe:value="10.1.0.100"/>
20 <Property oe:key="com.citrix.netscaler.mgmt.netmask"
21 oe:value="255.255.0.0"/>
22 <Property oe:key="com.citrix.netscaler.mgmt.gateway"
23 oe:value="10.1.0.1"/>

```

```
24 </PropertySection>
25 </Environment>
```

Configuraciones adicionales admitidas: Creación y eliminación de VLAN en VF SR-IOV del host

Escriba el siguiente comando para crear una VLAN en SR-IOV VF:

```
ip link show enp8s0f0 vf 6 vlan 10
```

En el comando anterior, “enp8s0f0” aparece el nombre de la función física.

Ejemplo: VLAN 10, creada en vf 6

```
4: enp8s0f0: <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 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:79:de:f8, spoof checking on, link-state auto, trust off
    vf 6 MAC fa:16:3e:db:ea:b3, vlan 10, spoof checking on, link-state auto, trust off
    vf 7 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
```

Escriba el siguiente comando para eliminar una VLAN en la VF SR-IOV:

```
ip link show enp8s0f0 vf 6 vlan 0
```

Ejemplo: VLAN 10, eliminada de vf 6

```
[root@localhost ~]# ip link show enp8s0f0
4: enp8s0f0: <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 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:79: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
    vf 7 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
```

Estos pasos completan el procedimiento para implementar una instancia de NetScaler VPX que utiliza la tecnología SRIOV, en OpenStack.

Configure una instancia de NetScaler VPX en KVM para utilizar interfaces de host basadas en DPDK de OVS

October 17, 2024

Puede configurar una instancia de NetScaler VPX que se ejecute en KVM (Fedora y RHOS) para utilizar Open vSwitch (OVS) con el Kit de desarrollo de planos de datos (DPDK) para un mejor rendimiento de la red. En este documento se describe cómo configurar la instancia NetScaler VPX para que funcione en los `vhost-user` puertos expuestos por OVS-DPDK en el host KVM.

[OVS](#) es un conmutador virtual multicapa licenciado bajo la licencia Apache 2.0 de código abierto. [DPDK](#) es un conjunto de bibliotecas y controladores para un procesamiento rápido de paquetes.

Las siguientes versiones de Fedora, RHOS, OVS y DPDK están calificadas para configurar una instancia de NetScaler VPX:

Fedora	RHOS
Fedora 25	RHOS 7,4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Requisitos previos

Antes de instalar DPDK, asegúrese de que el host tiene páginas enormes de 1 GB.

Para obtener más información, consulte esta [documentación de requisitos del sistema de DPDK](#). A continuación se presenta un resumen de los pasos necesarios para configurar una instancia de NetScaler VPX en KVM para utilizar interfaces de host basadas en DPDK de OVS:

- Instale DPDK.
- Construir e instalar OVS.
- Cree un puente OVS.
- Conecte una interfaz física al puente OVS.
- Conecte `vhost-user` puertos a la ruta de datos OVS.
- Aprovechone un KVM-VPX con `vhost-user` puertos basados en OVS-DPDK.

Instalar DPDK

Para instalar DPDK, siga las instrucciones que se dan en este documento [Open vSwitch con DPDK](#).

Crear e instalar OVS

Descargue OVS desde la [página de descargas](#) de OVS. A continuación, cree e instale OVS mediante una ruta de datos DPDK. Siga las instrucciones que figuran en el documento [Instalación de Open vSwitch](#).

Para obtener información más detallada, [Guía de introducción de DPDK para Linux](#).

Creación de un puente OVS

Dependiendo de su necesidad, escriba el comando Fedora o RHOS para crear un puente OVS:

Comando de Fedora:

```
1 > $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
   datapath_type=netdev
```

Comando RHOS:

```
1 ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

Conecte la interfaz física al puente OVS

Enlace los puertos a DPDK y luego conéctelos al puente OVS escribiendo los siguientes comandos de Fedora o RHOS:

Comando de Fedora:

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

Comando RHOS:

```
1 ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dtpdk
   options:dtpdk-devargs=0000:03:00.0
2
3
4 ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dtpdk
   options:dtpdk-devargs=0000:03:00.1
```

El `dpdk-devargs` mostrado como parte de las opciones especifica el PCI BDF de la NIC física respectiva.

Adjuntar vhost-user puertos a la ruta de datos OVS

Escriba los siguientes comandos de Fedora o RHOS para conectar `vhost-user` puertos a la ruta de datos OVS:

Comando de 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*
```

Comando 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*
```

Aprovisionamiento de un KVM-VPX con vhost-user puertos basados en OVS-DPDK

Puede aprovisionar una instancia VPX en Fedora KVM con puertos `vhost-user` basados en OVS-DPDK solo desde la CLI usando los siguientes comandos QEMU: **Comando de Fedora:**

```
1 qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \
2
3 -object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages
  ,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
7 -device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
  bootindex=1 \
8
9 -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
11 -device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
  bus=pci.0,addr=0x3 \
12
13 -chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
  user1> \
14
15 -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
  virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
16
17 -chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
  user2> \
```

```
18
19  -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
    virtio-net
20
21  pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
22
23  --nographic
```

Para RHOS, utilice el siguiente archivo XML de ejemplo para aprovisionar la instancia NetScaler VPX, mediante `virsh`.

```
1  <domain type='kvm'>
2
3    <name>dpgk-vpx1</name>
4
5    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
6
7    <memory unit='KiB'>16777216</memory>
8
9    <currentMemory unit='KiB'>16777216</currentMemory>
10
11   <memoryBacking>
12
13     <hugepages>
14
15       <page size='1048576' unit='KiB' />
16
17     </hugepages>
18
19   </memoryBacking>
20
21   <vcpu placement='static'>6</vcpu>
22
23   <cputune>
24
25     <shares>4096</shares>
26
27     <vcpupin vcpu='0' cpuset='0' />
28
29     <vcpupin vcpu='1' cpuset='2' />
30
31     <vcpupin vcpu='2' cpuset='4' />
32
33     <vcpupin vcpu='3' cpuset='6' />
34
35     <emulatorpin cpuset='0,2,4,6' />
36
37   </cputune>
38
39   <numatune>
40
41     <memory mode='strict' nodeset='0' />
42
```

```
43     </numatune>
44
45     <resource>
46         <partition>/machine</partition>
47     </resource>
48
49     <os>
50
51         <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
52
53         <boot dev='hd' />
54
55     </os>
56
57     <features>
58
59         <acpi />
60
61         <apic />
62
63     </features>
64
65     <cpu mode='custom' match='minimum' check='full'>
66
67         <model fallback='allow'>Haswell-noTSX</model>
68
69         <vendor>Intel</vendor>
70
71         <topology sockets='1' cores='6' threads='1' />
72
73         <feature policy='require' name='ss' />
74
75         <feature policy='require' name='pcid' />
76
77         <feature policy='require' name='hypervisor' />
78
79         <feature policy='require' name='arat' />
80
81     </cpu>
82
83     <domain type='kvm'>
84
85         <name>dpdk-vpx1</name>
86
87         <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89         <memory unit='KiB'>16777216</memory>
90
91         <currentMemory unit='KiB'>16777216</currentMemory>
92
93         <memoryBacking>
94
95             <hugepages>
```

```
96     <page size='1048576' unit='KiB' />
97
98
99     </hugepages>
100
101 </memoryBacking>
102
103 <vcpu placement='static'>6</vcpu>
104
105 <cputune>
106
107     <shares>4096</shares>
108
109     <vcupin vcpu='0' cpuset='0' />
110
111     <vcupin vcpu='1' cpuset='2' />
112
113     <vcupin vcpu='2' cpuset='4' />
114
115     <vcupin vcpu='3' cpuset='6' />
116
117     <emulatorpin cpuset='0,2,4,6' />
118
119 </cputune>
120
121 <numatune>
122
123     <memory mode='strict' nodeset='0' />
124
125 </numatune>
126
127 <resource>
128
129     <partition>/machine</partition>
130
131 </resource>
132
133 <os>
134
135     <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
136
137     <boot dev='hd' />
138
139 </os>
140
141 <features>
142
143     <acpi />
144
145     <apic />
146
147 </features>
148
```

```
149     <cpu mode='custom' match='minimum' check='full'>
150
151         <model fallback='allow'>Haswell-noTSX</model>
152
153         <vendor>Intel</vendor>
154
155         <topology sockets='1' cores='6' threads='1'/>
156
157         <feature policy='require' name='ss'/>
158
159         <feature policy='require' name='pcid'/>
160
161         <feature policy='require' name='hypervisor'/>
162
163         <feature policy='require' name='arat'/>
164
165         <feature policy='require' name='tsc\_adjust'/>
166
167         <feature policy='require' name='xsaveopt'/>
168
169         <feature policy='require' name='pdpe1gb'/>
170
171         <numa>
172
173             <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess=
174                 'shared'/>
175
176         </numa>
177     </cpu>
178
179     <clock offset='utc'/>
180
181     <on\_poweroff>destroy</on\_poweroff>
182
183     <on\_reboot>restart</on\_reboot>
184
185     <on\_crash>destroy</on\_crash>
186
187     <devices>
188
189         <emulator>/usr/libexec/qemu-kvm</emulator>
190
191         <disk type='file' device='disk'>
192
193             <driver name='qemu' type='qcow2' cache='none'/>
194
195             <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>
196
197             <target dev='vda' bus='virtio'/>
198
199             <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
200                 function='0x0'/>
```

```
200
201     </disk>
202
203     <controller type='ide' index='0'>
204         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
205             function='0x1' />
206
207     </controller>
208
209     <controller type='usb' index='0' model='piix3-uhci'>
210
211         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
212             function='0x2' />
213
214     </controller>
215
216     <controller type='pci' index='0' model='pci-root' />
217
218     <interface type='direct'>
219
220         <mac address='52:54:00:bb:ac:05' />
221
222         <source dev='enp129s0f0' mode='bridge' />
223
224         <model type='virtio' />
225
226         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
227             function='0x0' />
228
229     </interface>
230
231     <interface type='vhostuser'>
232
233         <mac address='52:54:00:55:55:56' />
234
235         <source type='unix' path='/var/run/openvswitch/vhost-user1'
236             mode='client' />
237
238         <model type='virtio' />
239
240         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
241             function='0x0' />
242
243     </interface>
244
245     <interface type='vhostuser'>
246
247         <mac address='52:54:00:2a:32:64' />
248
249         <source type='unix' path='/var/run/openvswitch/vhost-user2'
250             mode='client' />
```

```
247     <model type='virtio' />
248
249     <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
        function='0x0' />
250
251 </interface>
252
253 <interface type='vhostuser'>
254
255     <mac address='52:54:00:2a:32:74' />
256
257     <source type='unix' path='/var/run/openvswitch/vhost-user3'
        mode='client' />
258
259     <model type='virtio' />
260
261     <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
        function='0x0' />
262
263 </interface>
264
265 <interface type='vhostuser'>
266
267     <mac address='52:54:00:2a:32:84' />
268
269     <source type='unix' path='/var/run/openvswitch/vhost-user4'
        mode='client' />
270
271     <model type='virtio' />
272
273     <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
        function='0x0' />
274
275 </interface>
276
277 <serial type='pty'>
278     <target port='0' />
279
280 </serial>
281
282 <console type='pty'>
283     <target type='serial' port='0' />
284
285 </console>
286
287 <input type='mouse' bus='ps2' />
288
289 <input type='keyboard' bus='ps2' />
290
291 <graphics type='vnc' port='-1' autoport='yes'>
292
293
294
```



```
295     <listen type='address' />
296
297   </graphics>
298
299   <video>
300
301     <model type='cirrus' vram='16384' heads='1' primary='yes' />
302
303     <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
304       function='0x0' />
305
306   </video>
307
308   <memballoon model='virtio'>
309     <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
310       function='0x0' />
311
312   </memballoon>
313 </devices>
314
315 </domain
```

Puntos a tener en cuenta

En el archivo XML, el [hugepage](#) tamaño debe ser de 1 GB, como se muestra en el archivo de ejemplo.

```
1   <memoryBacking>
2
3     <hugepages>
4
5       <page size='1048576' unit='KiB' />
6
7     </hugepages>
```

Además, en el archivo de ejemplo `vhost-user1` está el puerto de `vhost` usuario vinculado a `ovs-br0`.

```
1   <interface type='vhostuser'>
2
3     <mac address='52:54:00:55:55:56' />
4
5     <source type='unix' path='/var/run/openvswitch/vhost-user1'
6       mode='client' />
7
8     <model type='virtio' />
9
10    <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
11      function='0x0' />
```

```
11 </interface>
```

Para abrir la instancia NetScaler VPX, empiece a utilizar el comando `virsh`.

Aplique las configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en el hipervisor KVM

October 17, 2024

Puede aplicar las configuraciones de NetScaler VPX en el hipervisor KVM durante el primer arranque del dispositivo NetScaler. Por lo tanto, la configuración de un cliente en una instancia VPX se puede configurar en mucho menos tiempo.

Para obtener más información sobre los datos de usuario de prearranque y su formato, consulte [Aplicar configuraciones de NetScaler VPX en el primer arranque del dispositivo NetScaler en la nube](#).

Nota:

Para arrancar utilizando los datos de usuario de prearranque en el hipervisor KVM, la configuración de puerta de enlace predeterminada debe pasarse en la sección `<NS-CONFIG>`. Para obtener más información sobre el contenido de la etiqueta `<NS-CONFIG>`, consulte esta sección `<NS-CONFIG>`; de ejemplo.

Sample `<NS-CONFIG>` section:

```
1 <NS-PRE-BOOT-CONFIG>
2
3 <NS-CONFIG>
4   add route 0.0.0.0 0.0.0.0 10.102.38.1
5 </NS-CONFIG>
6
7 <NS-BOOTSTRAP>
8   <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
9   <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
10
11 <MGMT-INTERFACE-CONFIG>
12   <INTERFACE-NUM> eth0 </INTERFACE-NUM>
13   <IP> 10.102.38.216 </IP>
14   <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
15 </MGMT-INTERFACE-CONFIG>
16 </NS-BOOTSTRAP>
17
18 </NS-PRE-BOOT-CONFIG>
```

Cómo proporcionar datos de usuario previos al arranque en el hipervisor KVM

Puede proporcionar datos de usuario de prearranque en el hipervisor KVM a través de un archivo ISO, que se adjunta mediante un dispositivo CDROM.

Proporcionar datos de usuario mediante un archivo ISO de CDROM

Puede usar Virtual Machine Manager (VMM) para inyectar datos de usuario en la máquina virtual (VM) como una imagen ISO mediante el dispositivo CDROM. KVM admite CD-ROM en VM Guest, ya sea accediendo directamente a una unidad física en el servidor host de VM o accediendo a imágenes ISO.

Los siguientes pasos le permiten proporcionar datos de usuario mediante el archivo ISO de CDROM:

1. Cree un archivo con un nombre de archivo `userdata` que contenga el contenido de datos de usuario antes del arranque.

Nota:

El nombre del archivo debe usarse estrictamente como `userdata`.

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

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

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

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

```
1 root@ubuntu:~/sai/19oct# ls -lh
2 total 4.0K
3 -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
4 root@ubuntu:~/sai/19oct#
5 root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
6 I: -input-charset not specified, using utf-8 (detected in locale
  settings)
7 Total translation table size: 0
8 Total rockridge attributes bytes: 0
9 Total directory bytes: 0
10 Path table size(bytes): 10
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. Aprovechone la instancia de NetScaler VPX mediante el proceso de implementación estándar para crear la VM. But do not power on the VM automatically.
4. Agregue un dispositivo de CD-ROM con Virtual Machine Manager mediante los siguientes pasos:
 - a) Haga doble clic en una entrada de VM Guest en Virtual Machine Manager para abrir su consola y cambiar a la vista Detalles con **Ver > Detalles**.
 - b) Haga clic en **Agregar hardware > Almacenamiento > Tipo de dispositivo > Dispositivo de CDRom**.
 - c) Haga clic en **Administrar**, seleccione el archivo ISO correcto y haga clic en **Finalizar**. Se crea un nuevo CDRom en **Recursos** en la instancia de NetScaler VPX.
5. Power on the VM.

NetScaler VPX en AWS

October 17, 2024

Puede lanzar una instancia de NetScaler VPX en Amazon Web Services (AWS). El dispositivo NetScaler VPX está disponible como Amazon Machine Image (AMI) en el mercado de AWS. Una instancia NetScaler VPX en AWS le permite utilizar las capacidades de computación en la nube de AWS y utilizar las funciones de equilibrio de carga y administración de tráfico de NetScaler para sus necesidades empresariales. La instancia VPX admite todas las funciones de administración del tráfico de un dispositivo NetScaler físico, y se puede implementar como instancias independientes o en pares de alta disponibilidad. Para obtener más información sobre las funciones de VPX, consulte la [hoja de datos de VPX](#).

Introducción

Antes de empezar con la implementación de VPX, debe estar familiarizado con la siguiente información:

- [Terminología de AWS](#)
- [Tabla de compatibilidad de AWS-VPX](#)
- [Limitaciones y directrices de uso](#)
- [Requisitos previos](#)
- [Cómo funciona una instancia de NetScaler VPX en AWS](#)

Implementar una instancia de NetScaler VPX en AWS

En AWS, se admiten los siguientes tipos de implementación para las instancias VPX:

- [Independiente](#)
- [Alta disponibilidad \(activo-pasivo\)](#)
 - [Alta disponibilidad dentro de la misma zona](#)
 - [Alta disponibilidad en diferentes zonas mediante Elastic IP](#)
 - [Alta disponibilidad en diferentes zonas mediante IP privada](#)
- [GSLB activo-activo](#)
- [Escalado automático \(activo-activo\) mediante ADM](#)

Implementaciones híbridas

- [Implemente NetScaler en AWS Outpost](#)
- [Implemente NetScaler en VMC en AWS](#)

Licensing

Una instancia de NetScaler VPX en AWS requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias de NetScaler VPX que se ejecutan en AWS:

- [Gratis \(ilimitado\)](#)
- [Cada hora](#)
- [Anual](#)
- [BYOL](#)
- [Prueba gratuita \(todas las ofertas de suscripción a NetScaler VPX-AWS durante 21 días gratis en el mercado de AWS\).](#)

Automatización

- [NetScaler ADM: Implementación inteligente](#)
- [CFT de GitHub: plantillas y scripts de NetScaler para la implementación de AWS](#)
- [GitHub Ansible: plantillas y scripts de NetScaler para la implementación de AWS](#)
- [GitHub Terraform: plantillas y scripts de NetScaler para la implementación de AWS](#)
- [Biblioteca de patrones de AWS \(PL\): NetScaler VPX](#)

Entradas de blog

- [Cómo NetScaler en AWS ayuda a los clientes a entregar aplicaciones de forma segura](#)
- [Entrega de aplicaciones en la nube híbrida con NetScaler y AWS](#)
- [Citrix es socio competente en redes de AWS](#)
- [NetScaler: siempre preparado para las nubes públicas](#)
- [Escale o amplíe fácilmente en nubes públicas a través de NetScaler](#)
- [Citrix amplía las opciones de implementación de ADC con AWS Outposts](#)
- [Uso de NetScaler con redirección de entrada de Amazon VPC](#)
- [Citrix ofrece opciones, rendimiento e implementación simplificada en AWS](#)
- [La seguridad de NetScaler Web App Firewall, ahora en AWS Marketplace](#)
- [Cómo Aria Systems usa NetScaler Web App Firewall en AWS](#)

Vídeos

- [Simplificación de las implementaciones de NetScaler en la nube pública a través de ADM](#)
- [Aprovisionamiento y configuración de NetScaler VPX en AWS mediante scripts de terraform listos para usar](#)
- [Implementación de NetScaler HA en AWS mediante la plantilla de CloudFormation](#)
- [Implemente NetScaler HA en las zonas de disponibilidad mediante AWS QuickStart](#)
- [NetScaler Autoscale mediante ADM](#)

Estudios de casos de clientes

- [Solución tecnológica - Xenit AB](#)
- [Una mejor manera de hacer negocios con Citrix y la nube de AWS —Aria](#)
- [Descubra las ventajas de NetScaler y AWS](#)
- [Rain for Rent - Historia de cliente](#)

Soluciones

- [Implementar una plataforma de publicidad digital en AWS con NetScaler](#)
- [Mejorar el análisis de Clickstream en AWS con NetScaler](#)

Asistencia

- [Abrir un caso de asistencia](#)
- Para la oferta de suscripción de NetScaler, consulte [Solucionar problemas de una instancia VPX en AWS](#). Para presentar un caso de soporte, busque su número de cuenta de AWS y su código PIN de soporte y llame al soporte de NetScaler.
- Para la oferta con licencia del cliente de NetScaler o BYOL, asegúrese de tener el acuerdo de asistencia y mantenimiento válido. Si no tiene un acuerdo, póngase en contacto con su representante de NetScaler.

Referencias adicionales

- [Seminario web bajo demanda de AWS: NetScaler en AWS](#)
- [Hoja de datos de NetScaler VPX](#)
- [NetScaler en AWS Marketplace](#)
- [NetScaler forma parte de las soluciones de socios de redes de AWS \(balanceadores de carga\)](#)
- [Preguntas frecuentes sobre AWS](#)

Terminología de AWS

October 17, 2024

En esta sección se describe la lista de términos y frases de AWS de uso común. Para obtener más información, consulte [Glosario de AWS](#).

Término	Definición
Imagen de máquina de Amazon (AMI)	Imagen de máquina, que proporciona la información necesaria para iniciar una instancia, que es un servidor virtual en la nube.
Elastic Block Store	Proporciona volúmenes de almacenamiento de bloques persistentes para su uso con instancias de Amazon EC2 en la nube de AWS.
Servicio de almacenamiento simple (S3)	Almacenamiento para Internet. Está diseñado para que la informática a escala web sea más fácil para los desarrolladores.

Término	Definición
Elastic Compute Cloud (EC2)	Un servicio web que proporciona una capacidad informática segura y de tamaño variable en la nube. Está diseñado para que la informática en la nube a escala web sea más fácil para los desarrolladores.
Elastic Load Balancing (ELB)	Distribuye el tráfico de aplicaciones entrantes en varias instancias de EC2, en varias zonas de disponibilidad. Esto aumenta la tolerancia a fallos de sus aplicaciones.
Interfaz de red elástica (ENI)	Interfaz de red virtual que puede adjuntar a una instancia en una nube privada virtual (VPC).
Dirección IP elástica (EIP)	Dirección IPv4 pública y estática que ha asignado en Amazon EC2 o Amazon VPC y que, a continuación, se adjunta a una instancia. Las direcciones IP elásticas están asociadas a su cuenta, no a una instancia específica. Son elásticas porque puede asignarlos, conectarlos, separarlos y liberarlos fácilmente a medida que cambien tus necesidades.
Tipo de instancia	Amazon EC2 ofrece una amplia selección de tipos de instancia optimizados para adaptarse a diferentes casos de uso. Los tipos de instancia comprenden diversas combinaciones de CPU, memoria, almacenamiento y capacidad de red, y le ofrecen la flexibilidad de elegir la combinación adecuada de recursos para sus aplicaciones.
Identity and Access Management (IAM)	Una identidad de AWS con directivas de permisos que determinan lo que la identidad puede y no puede hacer en AWS. Puede utilizar un rol de IAM para permitir que las aplicaciones que se ejecutan en una instancia de EC2 accedan de forma segura a los recursos de AWS. El rol de IAM es necesario para implementar instancias VPX en una configuración de alta disponibilidad.
Puerta de enlace de Internet	Conecta una red a Internet. Puede enrutar el tráfico de direcciones IP fuera de la VPC a la Gateway de Internet.

Término	Definición
Par de llaves	Conjunto de credenciales de seguridad que utiliza para demostrar su identidad electrónicamente. Un par de claves consiste en una clave privada y una clave pública.
Tablas de redirecciones	Conjunto de reglas de redirección que controla el tráfico que sale de cualquier subred asociada a la tabla de redirecciones. Puede asociar varias subredes a una sola tabla de redirecciones, pero una subred solo puede asociarse a una tabla de redirecciones a la vez.
Grupos de seguridad	Conjunto con nombre asignado de conexiones de red entrantes permitidas para una instancia.
Subredes	Segmento del intervalo de direcciones IP de una VPC al que se pueden conectar instancias EC2. Puede crear subredes para agrupar instancias de acuerdo con las necesidades operativas y de seguridad.
Nube privada virtual (VPC)	Un servicio web para Provisioning una sección aislada lógicamente de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que defina.
Escalado automático	Servicio web para iniciar o finalizar instancias de Amazon EC2 automáticamente en función de directivas, programaciones y comprobaciones de estado definidas por el usuario.
CloudFormation	Un servicio para escribir o cambiar plantillas que crean y eliminan recursos relacionados de AWS juntos como una unidad.

Tabla de compatibilidad de AWS-VPX

October 17, 2024

En las siguientes tablas se enumeran el modelo VPX y las regiones, los tipos de instancias y los servicios de AWS admitidos.

Tabla 1: Modelos VPX compatibles en AWS

Modelo VPX compatible

NetScaler VPX Advanced: 200 Mbps

NetScaler VPX Premium: 1 Gbps

NetScaler VPX Premium: 5 Gbps

NetScaler VPX Express: 20 Mbps

NetScaler VPX: licencia de cliente

NetScaler VPX FIPS: licencia del cliente

NetScaler VPX FIPS ENA: licencia del cliente

Tabla 2: Regiones de AWS compatibles

| Regiones de AWS admitidas |

|—————|

| Oeste de EE. UU. (Oregón) |

| Oeste de EE. UU. (Norte de California) |

| Este de EE. UU. (Ohio) |

| Este de EE. UU. (Ohio) |

| Asia Pacífico (Bombay) |

| Asia Pacífico (Seúl) |

| Asia Pacífico (Singapur) |

| Asia Pacífico (Sídney) |

| Asia Pacífico (Tokio) |

| Asia Pacífico (Hong Kong) |

| Asia Pacífico (Osaka) |

| Asia Pacífico (Yakarta) |

| Asia Pacífico (Hyderabad) |

| Canadá (Central) |

| UE (Fráncfort) |

| UE (Irlanda) |

| UE (Londres) |

| UE (París) |

| EU (Milán) |

| Sudamérica (São Paulo) |

| AWS GovCloud (US-East) |

| AWS GovCloud (US-West) |

| AWS Top Secret (C2S) |
| Oriente Medio (Baréin) |
| África (Ciudad del Cabo) |
| C2S |

Nota:

Para la región de Hong Kong de AWS, la compatibilidad con NetScaler VPX solo está disponible con licencias BYOL.

Tabla 3: tipos de instancias de AWS compatibles

| Tipos de instancia de AWS admitidos |

| c4.large, c4.xlarge, c4.2 x large, c4.4 x large, c4.8 x large |
| c5.large, c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.18xlarge, c5.24xlarge |
| C5n.large, C5n.xlarge, C5n.2xlarge, C5n.4xlarge, C5n.9xlarge, C5n.18xlarge |
| d2.x grande, d2.2 x grande, d2.4 x grande, d2.8 x grande |
| m3.large, m3.xlarge, m3.2xlarge |
| m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16x large |
| m5.grande, m5.x grande, m5.2 x grande, m5.4 x grande, m5.8 x grande, m5.12 x grande, m5.16 x grande, m5.24 x grande |
| m5a.large, m5a.xlarge, m5a.2xlarge, m5a.4xlarge, m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge |
| m5n.large, m5n.xlarge, m5n.2xlarge, m5n.4xlarge, m5n.8xlarge, m5n.12xlarge, m5n.16xlarge, m5n.24xlarge |
| m6i.large, m6i.xlarge, m6i.2xlarge, m6i.4xlarge, m6i.8x grande, m6i.12x grande, m6i.16x grande, m6i.24x grande, m6i.32x grande |
| r7iz.large, r7iz.xlarge, r7iz.2xlarge, r7iz.4xlarge, r7iz.8xlarge, r7iz.12xlarge, r7iz.16xlarge, r7iz.32xlarge |
| t2.mediano, t2.grande, t2.xgrande, t2.2xgrande |
| t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge |

Nota:

El NetScaler VPX provisionado en los tipos de instancia m6i y r7iz de AWS no admite la función de cola de baja latencia (LLQ) de ENA.

Tabla 4: Servicios de AWS admitidos

Servicios de AWS compatibles

EC2: lanza instancias de ADC.

Servicios de AWS compatibles

Lambda: invoca las API NITRO de NetScaler VPX durante el aprovisionamiento de instancias de NetScaler VPX de

Redirección de entrada de VPC y VPC: VPC crea redes aisladas en las que se puede iniciar ADC. La redirección de

Route53: distribuye el tráfico entre todos los nodos de NetScaler VPX de la solución NetScaler Autoscale.

ELB: distribuye el tráfico entre todos los nodos de NetScaler VPX de la solución NetScaler Autoscale.

Cloudwatch: supervisa el rendimiento y los parámetros del sistema para la instancia de NetScaler VPX.

AWS Autoscaling: se utiliza para el escalado automático de servidores back-end.

Formación en la nube: las plantillas de CloudFormation se utilizan para implementar instancias de NetScaler VPX

Servicio de cola simple (SQS): supervisa los eventos de escalado hacia arriba y hacia abajo en el escalado autor

Servicio de notificación simple (SNS): supervisa los eventos de escalado hacia arriba y hacia abajo en el escalado

Administración de identidades y accesos (IAM): proporciona acceso a los servicios y recursos de AWS.

AWS Outposts: aprovisiones de instancias de NetScaler VPX en AWS Outposts.

NetScaler recomienda los siguientes tipos de instancias de AWS:

- Series M5 y C5n para ediciones de mercado o licencias de grupos basadas en ancho de banda.
- Serie C5n para licencias de grupos basados en vCPU.

Oferta de VPX en el mercado de AWS	Recomendación de instancia de AWS
VPX Express 20, VPX 200	M5.xLarge
VPX 1G, VPX 5G	M5.2xLarge

NetScaler recomienda los siguientes tipos de instancias de AWS en función del rendimiento.

VPX con licencias agrupadas (licencias de ancho de banda)	Recomendación de instancia de AWS
VPX 8 G	C5n.4xLarge
VPX 10 G, VPX 15 G, VPX 25 G	C5n.9xLarge

Nota:

La oferta VPX 25G no ofrece el rendimiento deseado de 25G en AWS, pero puede ofrecer una tasa de transacciones SSL más alta.

Para lograr un rendimiento superior a 5G, haga lo siguiente:

- Elija **NetScaler VPX: oferta con licencia del cliente (BYOL)** en el mercado de AWS.
- Seleccione Licencias **agrupadas (licencias de ancho de banda)** en la GUI o la CLI de NetScaler.

Para determinar su instancia en función de diferentes métricas, como los paquetes por segundo y la tasa de transacciones SSL, póngase en contacto con su contacto de NetScaler para obtener orientación. Para obtener instrucciones sobre licencias y dimensionamiento de grupos basados en vCPU, póngase en contacto con el soporte de NetScaler.

Limitaciones y directrices de uso

October 17, 2024

Las siguientes limitaciones y directrices de uso se aplican al implementar una instancia de NetScaler VPX en AWS:

- Antes de comenzar, lea la sección de terminología de AWS en [Implementar una instancia de NetScaler VPX en AWS](#).
- La función de agrupación de clústeres no es compatible con VPX.
- Para que la configuración de alta disponibilidad funcione eficazmente, asocie un dispositivo NAT dedicado a la interfaz de administración o asocie EIP a NSIP. Para obtener más información sobre NAT, en la documentación de AWS, consulte [Instancias NAT](#).
- El tráfico de datos y el tráfico de administración deben estar segregados con ENIs pertenecientes a diferentes subredes.
- Solo la dirección del NSIP debe estar presente en la ENI de administración.
- Si se utiliza una instancia de NAT para la seguridad en lugar de asignar un EIP al NSIP, se requieren cambios de redirección de nivel de VPC adecuados. Para obtener instrucciones sobre cómo realizar cambios de redirección a nivel de VPC, en la documentación de AWS, consulte [Caso 2: VPC con subredes públicas y privadas](#).
- Una instancia VPX se puede mover de un tipo de instancia EC2 a otro (por ejemplo, de m3.large a m3.xlarge).
- Para las opciones de almacenamiento para VPX en AWS, Citrix recomienda EBS, porque es duradero y los datos están disponibles incluso después de separarlos de la instancia.

- No se admite la adición dinámica de ENIs a VPX. Reinicie la instancia VPX para aplicar la actualización. Citrix recomienda detener la instancia independiente o de alta disponibilidad, conectar la nueva ENI y reiniciar la instancia.
- Puede asignar varias direcciones IP a una ENI. El número máximo de direcciones IP por ENI viene determinado por el tipo de instancia EC2; consulte la sección “Direcciones IP por interfaz de red por tipo de instancia” en [Interfaces de red elásticas](#). Debe asignar las direcciones IP en AWS antes de asignarlas a ENI. Para obtener más información, consulte [Interfaces de red elásticas](#).
- Citrix recomienda evitar el uso de los comandos `enable` and `disable interface` en las interfaces NetScaler VPX.
- Los comandos `set ha node \\<NODE_ID\\> -haStatus STAYPRIMARY` y `set ha node \\<NODE_ID\\> -haStatus STAYSECONDARY` de NetScaler están inhabilitados de forma predeterminada.
- IPv6 no es compatible con VPX.
- Debido a las limitaciones de AWS, estas funciones no son compatibles:
 - ARP gratuito (GARP)
 - Modo L2
 - VLAN etiquetada
 - Redirección dinámica
 - MAC virtual
- Para que RNAT funcione, asegúrese de que la **comprobación de origen/destino** esté inhabilitada. Para obtener más información, consulte “Cambio de la comprobación de origen/destino” en [Elastic Network Interfaces](#).
- En una implementación de NetScaler VPX en AWS, en algunas regiones de AWS, es posible que la infraestructura de AWS no pueda resolver llamadas a la API de AWS. Esto ocurre si las llamadas a la API se emiten a través de una interfaz que no es de administración en la instancia de NetScaler VPX. Como solución alternativa, restrinja las llamadas a la API únicamente a la interfaz de administración. Para ello, cree una NSVLAN en la instancia VPX y vincule la interfaz de administración a la NSVLAN mediante el comando apropiado. Por ejemplo: `establecer configuración ns -nsvlan <vlan id> -ifnum 1/1 - etiquetado NO guardar configuración` Reinicie la instancia VPX cuando se le solicite. Para obtener más información sobre la configuración `nsvlan`, consulte [Configuración de NSVLAN](#).
- En la consola de AWS, el uso de vCPU que se muestra para una instancia VPX en la ficha **Supervisión** puede ser alto (hasta un 100 por ciento), incluso cuando el uso real es mucho menor. Para ver el uso real de la vCPU, vaya a **Ver todas las métricas de CloudWatch**. Para obtener más información, consulte [Monitorear sus instancias usando Amazon CloudWatch](#).

- La adición en caliente solo se admite en las interfaces PV y SRIOV con NetScaler en AWS. Las instancias VPX con interfaces ENA no admiten conexión en marcha y el comportamiento de las instancias puede ser impredecible si se intenta conectar en caliente.
- La eliminación en caliente a través de la consola web de AWS o la interfaz CLI de AWS no se admite con las interfaces PV, SRIOV y ENA para NetScaler. El comportamiento de las instancias puede ser impredecible si se intenta eliminar en caliente.

Requisitos previos

October 17, 2024

Antes de intentar crear una instancia VPX en AWS, asegúrese de tener lo siguiente:

- **Una cuenta de AWS:** para lanzar una AMI de NetScaler VPX en una nube privada virtual (VPC) de AWS. Puede crear una cuenta de AWS de forma gratuita en www.aws.amazon.com.
- **Una cuenta de usuario de AWS Identity and Access Management (IAM):** Para controlar de forma segura el acceso a los servicios y recursos de AWS para sus usuarios. Para obtener más información sobre cómo crear una cuenta de usuario de IAM, consulte [Creación de usuarios de IAM \(consola\)](#). Una función de IAM es obligatoria tanto para implementaciones independientes como para implementaciones de alta disponibilidad.

La función de IAM asociada a su cuenta de AWS debe tener los siguientes permisos de IAM para varios casos.

HA se empareja con direcciones IPv4 en la misma zona de AWS:

```
1  "ec2:DescribeInstances",
2  "ec2:AssignPrivateIpAddresses",
3  "iam:SimulatePrincipalPolicy",
4  "iam:GetRole",
5  "ec2:CreateTags"
```

Ha emparejado con direcciones IPv6 en la misma zona de AWS:

```
1  "ec2:DescribeInstances",
2  "ec2:AssignIpv6Addresses",
3  "ec2:UnassignIpv6Addresses",
4  "iam:SimulatePrincipalPolicy",
5  "iam:GetRole",
6  "ec2:CreateTags"
```

HA se empareja con direcciones IPv4 e IPv6 en la misma zona de AWS:

```
1  "ec2:DescribeInstances",
```

```
2 "ec2:AssignPrivateIpAddresses",
3 "ec2:AssignIpv6Addresses",
4 "ec2:UnassignIpv6Addresses",
5 "iam:SimulatePrincipalPolicy",
6 "iam:GetRole",
7 "ec2:CreateTags"
```

La alta disponibilidad se empareja con direcciones IP elásticas en diferentes zonas de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:DescribeAddresses",
3 "ec2:AssociateAddress",
4 "ec2:DisassociateAddress",
5 "iam:SimulatePrincipalPolicy",
6 "iam:GetRole",
7 "ec2:CreateTags"
```

La alta disponibilidad se empareja con direcciones IP privadas en diferentes zonas de AWS:

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

HA se empareja con direcciones IP privadas e IP elásticas en diferentes zonas de AWS:

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

Escalado automático de backend de 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"
```

Nota:

- Si usa cualquier combinación de las funciones anteriores, use la combinación de permisos de IAM para cada una de las funciones.
 - Si usa la plantilla de Citrix CloudFormation, la función de IAM se crea automáticamente. La plantilla no permite seleccionar una función de IAM ya creada.
 - Cuando inicia sesión en la instancia VPX a través de la GUI, aparece un mensaje para configurar los privilegios necesarios para la función de IAM. Ignore la solicitud si ya configuró los privilegios.
- **CLI de AWS:** Para utilizar toda la funcionalidad proporcionada por AWS Management Console desde el programa de terminal. Para obtener más información, consulte la [guía del usuario de la CLI de AWS](#). También necesita la CLI de AWS para cambiar el tipo de interfaz de red a SR-IOV.
 - **Adaptador de red elástico (ENA):** para el tipo de instancia habilitada para controladores ENA, por ejemplo, instancias M5, C5, la versión del firmware debe ser 13.0 y superior.
 - Debe configurar el Servicio de metadatos de instancias (IMDS) en la instancia EC2 para NetScaler VPX. IMDSv1 e IMDSv2 son dos modos disponibles para acceder a los metadatos de la instancia desde una instancia de AWS EC2 en ejecución. IMDSv2 es más seguro que IMDSv1. Puede configurar la instancia para que utilice ambos métodos (la opción predeterminada) o solo el modo IMDSv2 (inhabilitando IMDSv1). Citrix ADC VPX solo admite el modo IMDSv2 a partir de la versión 13.1.48.x de NetScaler VPX.

Configurar las funciones de IAM de AWS en la instancia de NetScaler VPX

October 17, 2024

Las aplicaciones que se ejecutan en una instancia de Amazon EC2 deben incluir credenciales de AWS en las solicitudes de API de AWS. Puede almacenar las credenciales de AWS directamente en la instancia de Amazon EC2 y permitir que las aplicaciones de esa instancia las usen. Sin embargo, debe administrar las credenciales y asegurarse de que las transfieran de forma segura a cada instancia y actualizar cada instancia de Amazon EC2 cuando llegue el momento de rotar las credenciales. Eso es mucho trabajo adicional.

En su lugar, puede y debe usar una función de administración de identidades y accesos (IAM) para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia de Amazon EC2. Cuando usa un rol, no tiene que distribuir credenciales a largo plazo (como un nombre de usuario y una contraseña o claves de acceso) a una instancia de Amazon EC2. En cambio, la función proporciona permisos temporales que las aplicaciones pueden usar cuando realizan llamadas a otros recursos de AWS. Cuando lanza una instancia de Amazon EC2, especifica un rol de IAM para asociarlo a la instancia. Las aplicaciones que se ejecutan en la instancia pueden entonces usar las credenciales temporales proporcionadas por la función para firmar las solicitudes de API.

La función de IAM asociada a su cuenta de AWS debe tener los siguientes permisos de IAM para varios casos.

HA se empareja con direcciones IPv4 en la misma zona de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:AssignPrivateIpAddresses",
3 "iam:SimulatePrincipalPolicy",
4 "iam:GetRole"
```

Ha emparejado con direcciones IPv6 en la misma zona de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:AssignIpv6Addresses",
3 "ec2:UnassignIpv6Addresses",
4 "iam:SimulatePrincipalPolicy",
5 "iam:GetRole"
```

HA se empareja con direcciones IPv4 e IPv6 en la misma zona de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:AssignPrivateIpAddresses",
3 "ec2:AssignIpv6Addresses",
4 "ec2:UnassignIpv6Addresses",
5 "iam:SimulatePrincipalPolicy",
6 "iam:GetRole"
```

La alta disponibilidad se empareja con direcciones IP elásticas en diferentes zonas de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:DescribeAddresses",
3 "ec2:AssociateAddress",
4 "ec2:DisassociateAddress",
5 "iam:SimulatePrincipalPolicy",
6 "iam:GetRole"
```

La alta disponibilidad se empareja con direcciones IP privadas en diferentes zonas de AWS:

```
1 "ec2:DescribeInstances",
2 "ec2:DescribeRouteTables",
3 "ec2>DeleteRoute",
4 "ec2:CreateRoute",
```

```
5 "ec2:ModifyNetworkInterfaceAttribute",
6 "iam:SimulatePrincipalPolicy",
7 "iam:GetRole"
```

HA se empareja con direcciones IP privadas e IP elásticas en diferentes zonas de AWS:

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

Escalado automático de backend de 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"
```

Puntos que tener en cuenta:

- Si usa cualquier combinación de las funciones anteriores, use la combinación de permisos de IAM para cada una de las funciones.
- Si usa la plantilla de Citrix CloudFormation, la función de IAM se crea automáticamente. La plantilla no permite seleccionar una función de IAM ya creada.
- Cuando inicia sesión en la instancia VPX a través de la GUI, aparece un mensaje para configurar los privilegios necesarios para la función de IAM. Ignore la solicitud si ya configuró los privilegios.
- Una función de IAM es obligatoria tanto para implementaciones independientes como para implementaciones de alta disponibilidad.

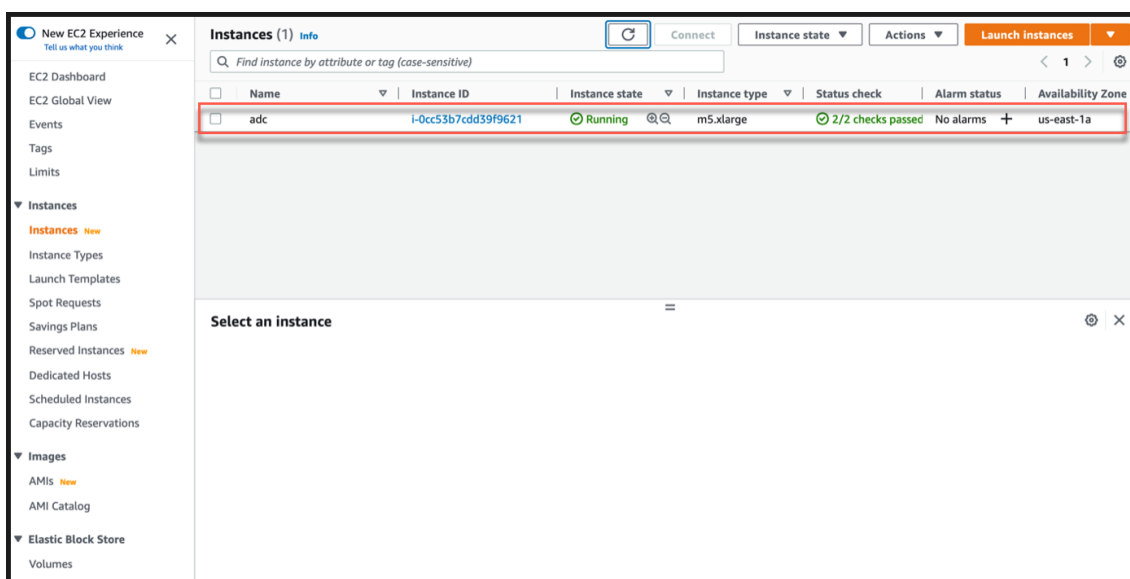
Crear un rol de IAM

Este procedimiento describe cómo crear una función de IAM para la función de escalado automático de back-end de AWS.

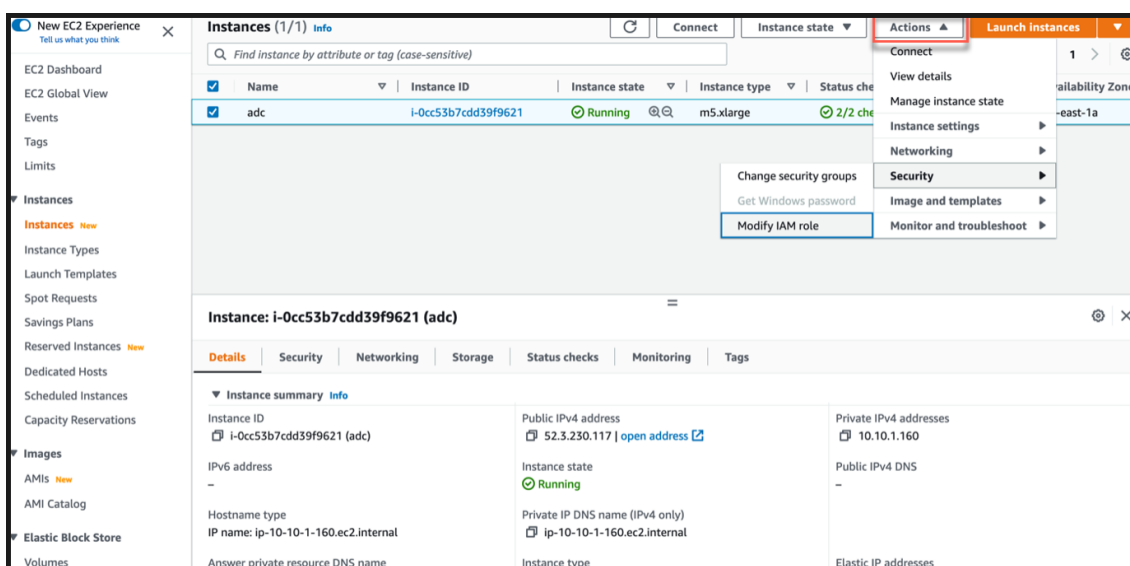
Nota:

Puede seguir el mismo procedimiento para crear cualquier función de IAM correspondiente a otras funciones.

1. Inicie sesión en la consola de administración de AWS para EC2.
2. Vaya a la página de instancias de EC2 y seleccione su instancia de ADC.



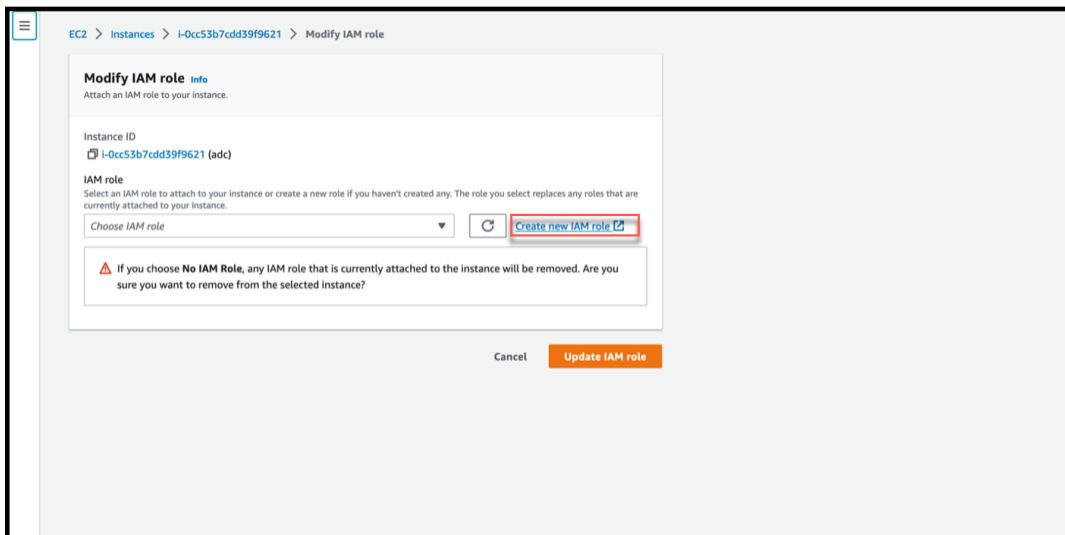
3. Vaya a **Acciones > Seguridad > Modificar el rol de IAM**.



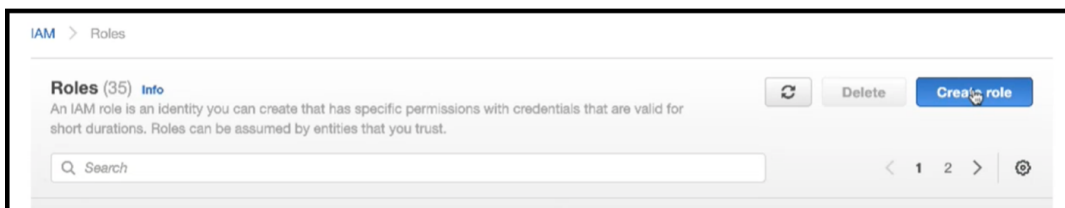
4. En la página **Modificar función de IAM**, puede elegir una función de IAM existente o crear una función de IAM.

5. Para crear un rol de IAM, siga estos pasos:

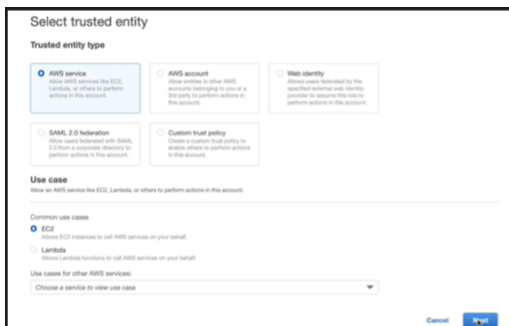
a) En la página **Modificar rol de IAM**, haga clic en **Crear un nuevo rol de IAM**.



b) En la página **Funciones**, haga clic en **Crear rol**.



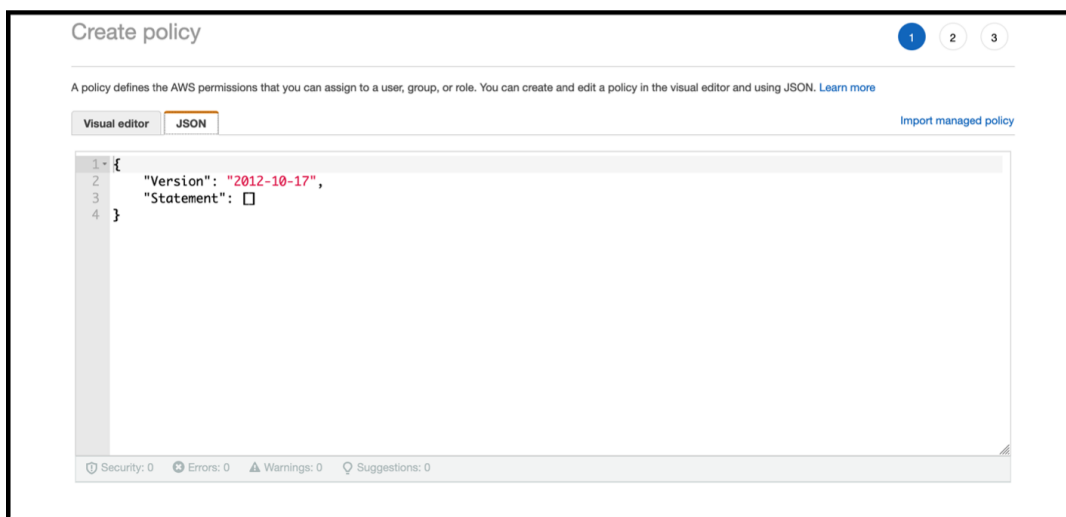
c) Seleccione el **servicio AWS** en el **tipo de entidad de confianza** y **EC2** en **Casos de uso comunes** y, a continuación, haga clic en **Siguiente**.



d) En la página **Agregar permisos**, haga clic en **Crear directiva**.



e) Haga clic en la ficha **JSON** para abrir el editor de JSON.



f) En el editor de JSON, borre todo y pegue los permisos de IAM para la función que quiera usar.

Por ejemplo, pegue los siguientes permisos de IAM para la función de escalado automático de back-end de AWS:

```

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

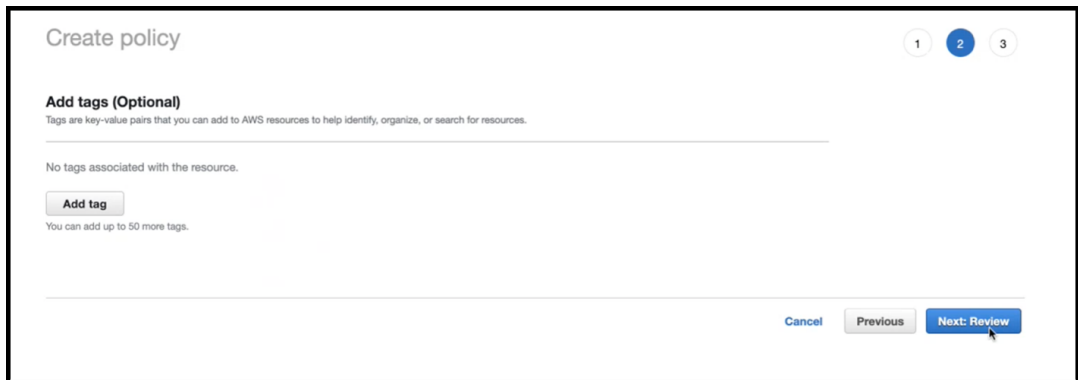
```

```

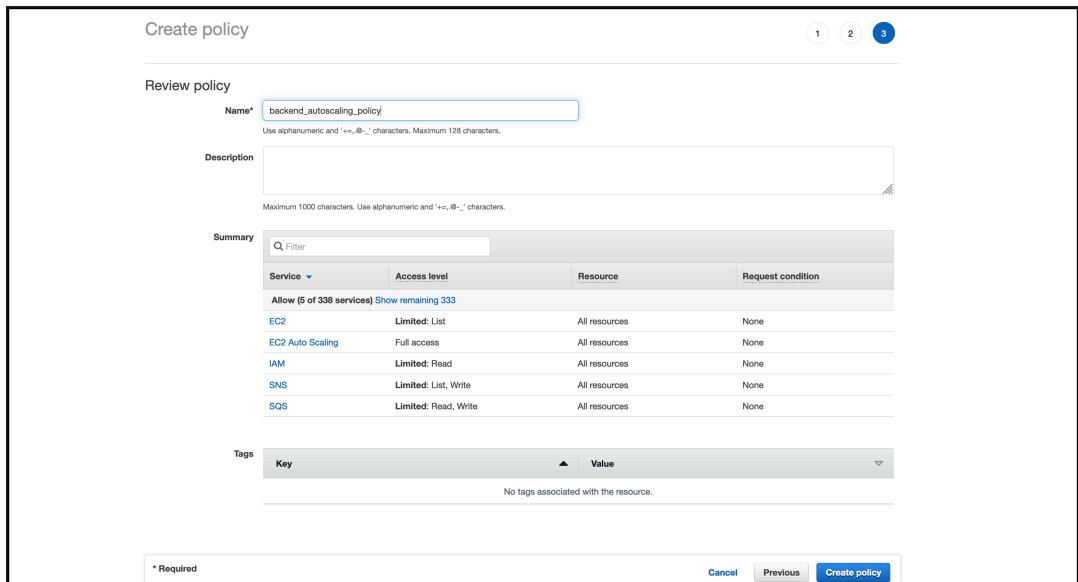
22         "iam:GetRole"
23     ],
24     "Resource": "*"
25 }
26
27 ]
28 }
    
```

Asegúrese de que el par clave-valor “Versión” que proporcione sea el mismo que AWS generó automáticamente.

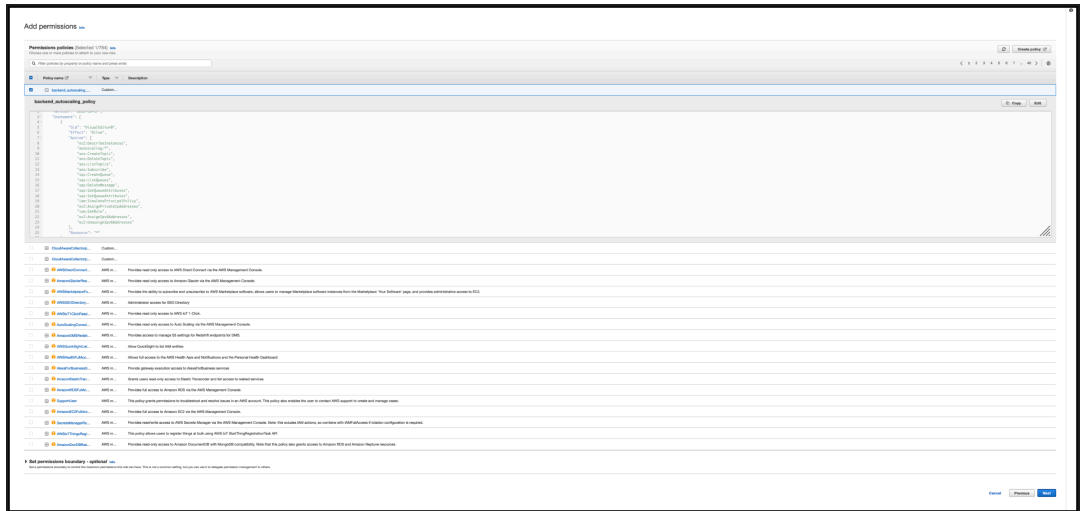
g) Haz clic en **Siguiente: Revisar**.



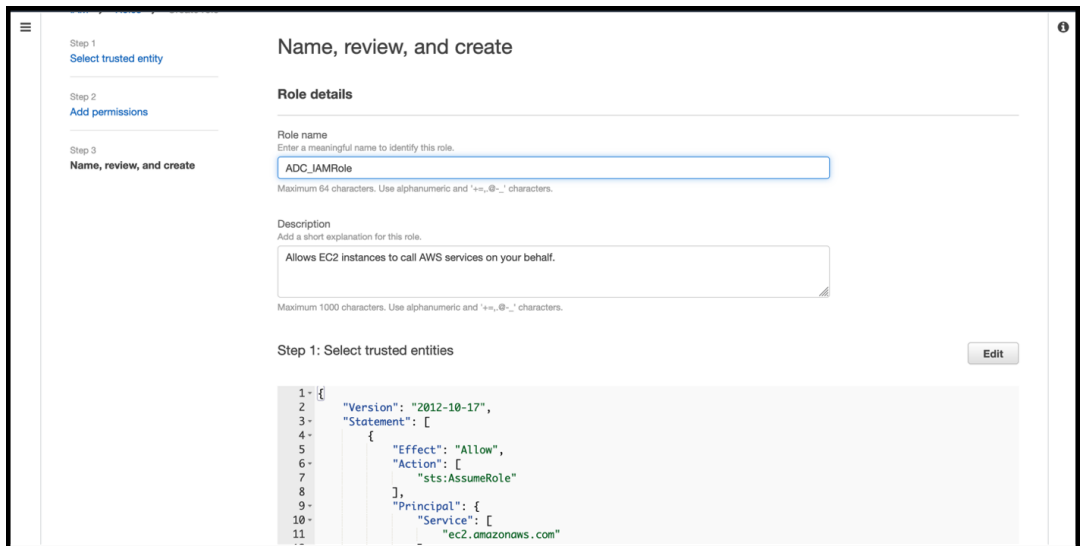
h) En la ficha **Revisar directiva**, asigne un nombre válido a la directiva y haga clic en **Crear directiva**.



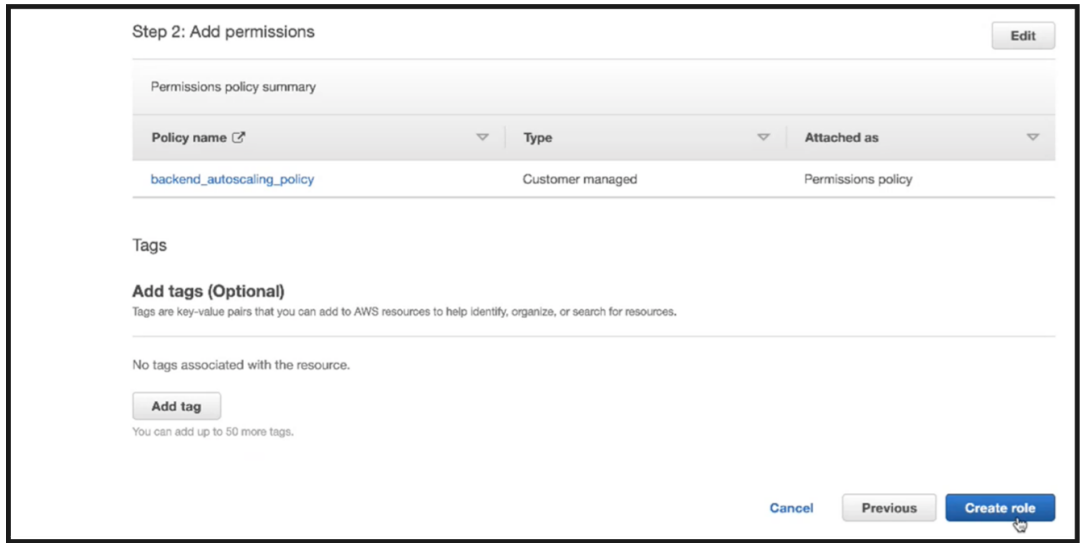
i) En la página **de administración de acceso a identidades**, haga clic en el nombre de la directiva que creó. Amplíe la directiva para comprobar todo el JSON y haga clic en **Siguiente**.



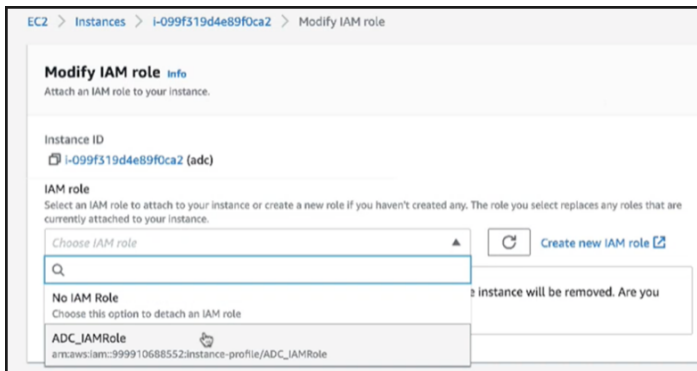
j) En la página **Nombre, revisión y creación**, asigne un nombre válido al rol.



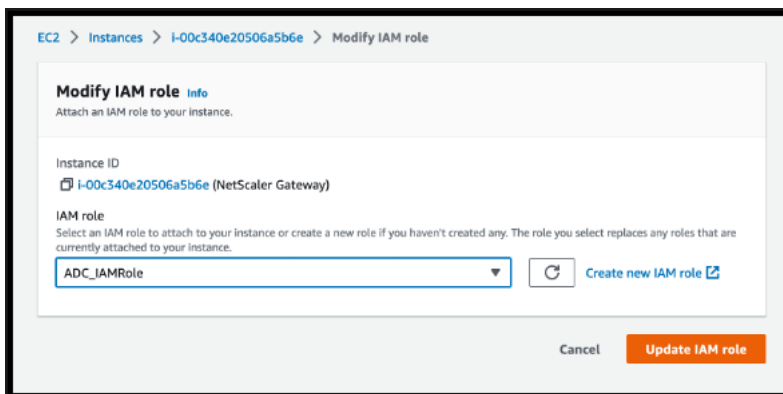
k) Haz clic en **Crear rol**.



6. Repita los pasos: 1, 2 y 3. Seleccione el botón **Actualizar** y seleccione el menú desplegable para ver el rol que creó.



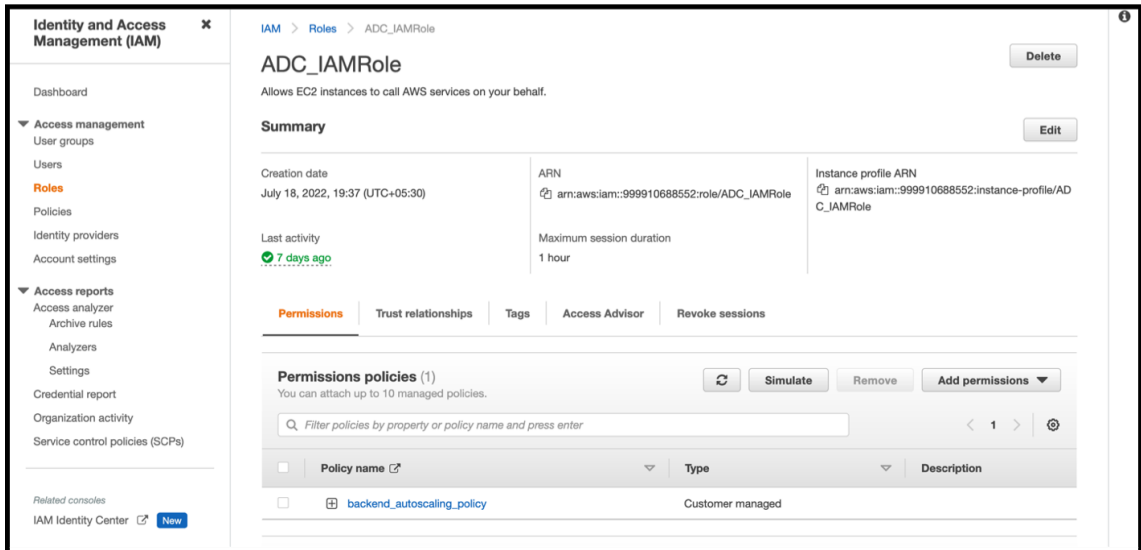
7. Haga clic en **Actualizar rol de IAM**.



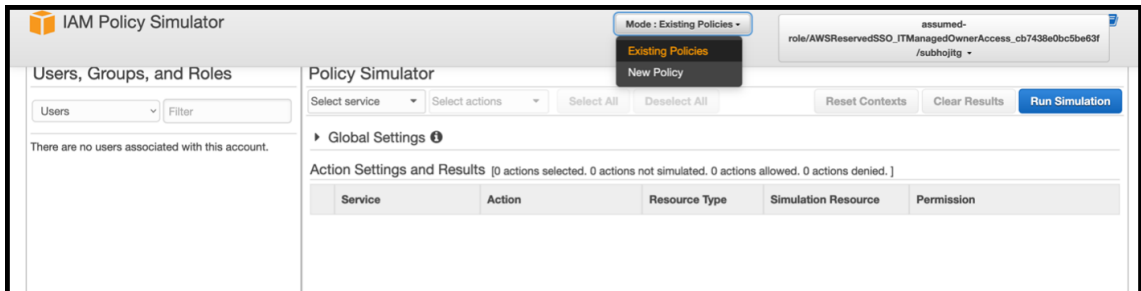
Pruebe las directivas de IAM con el simulador de directivas de IAM

El simulador de directivas de IAM es una herramienta que permite probar los efectos de las directivas de control de acceso de IAM antes de ponerlas en producción. Es más fácil verificar y solucionar problemas de permisos.

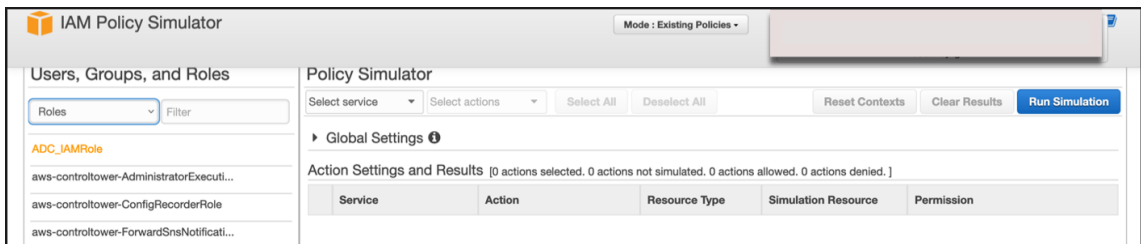
1. En la página de **IAM**, seleccione el rol de IAM que quiera probar y haga clic en **Simular**. En el siguiente ejemplo, “ADC_IAMRole” es el rol de IAM.



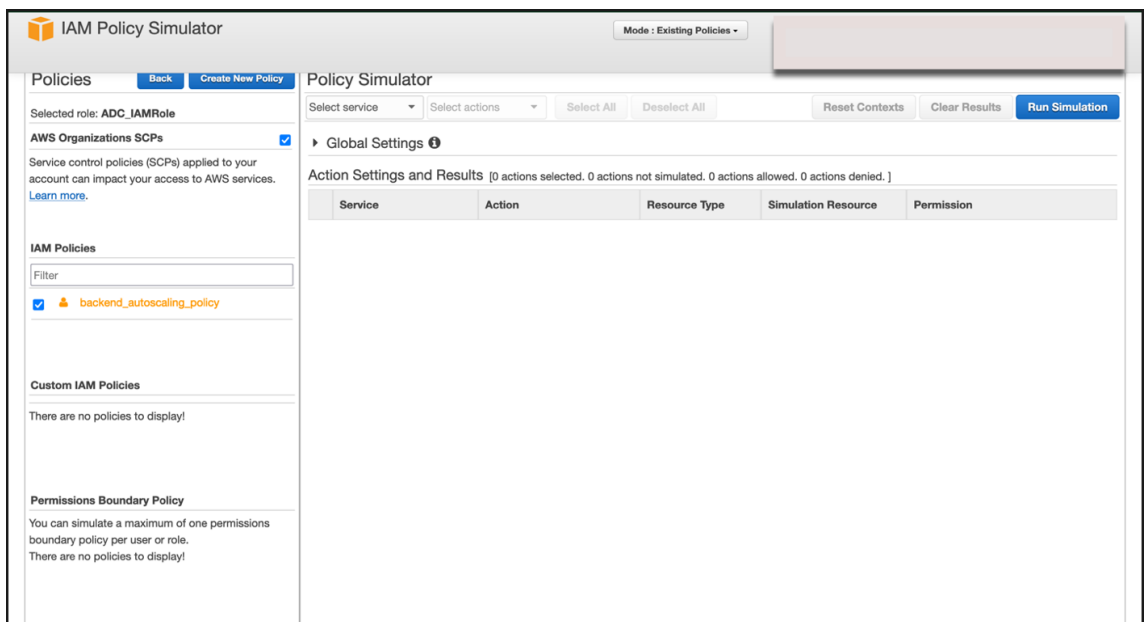
2. En la consola del **simulador de directivas de IAM**, seleccione **Directivas existentes** como **modo**.



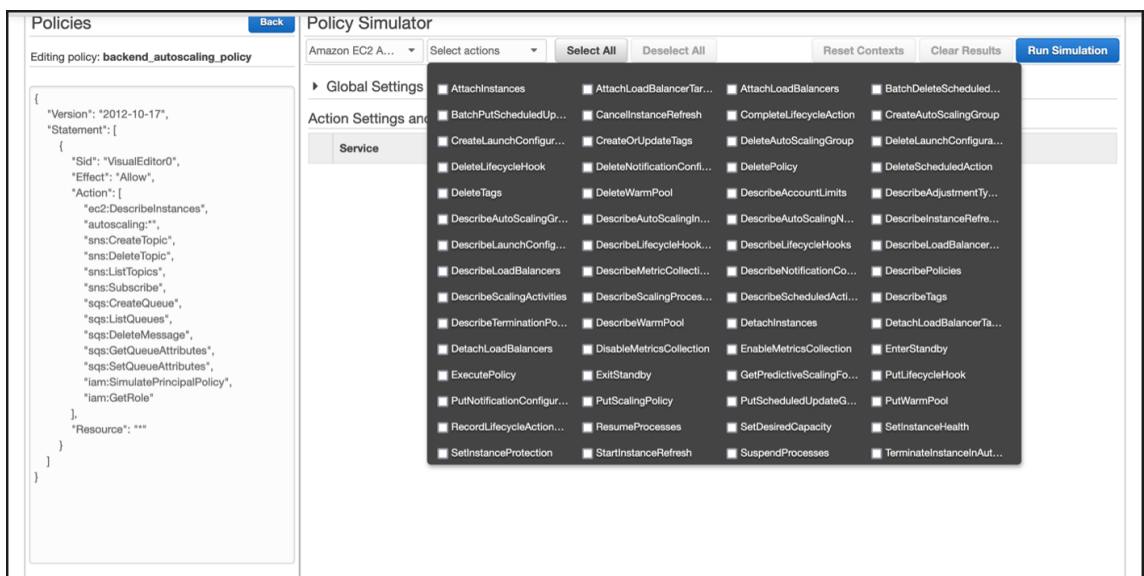
3. En la ficha **Usuarios, grupos y funciones**, seleccione **Funciones** en el menú desplegable y elija una función existente.



4. Después de seleccionar el rol existente, seleccione la política existente debajo de él.



- Después de seleccionar la directiva, puede ver el JSON exacto en la parte izquierda de la pantalla. Seleccione las acciones que quiera en el menú desplegable **Seleccionar acciones**.



- Haga clic en **Ejecutar simulación**.

Policies [Back] **Policy Simulator**

Editing policy: backend_autoscaling_policy

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "autoscaling:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateQueue",
        "sqs:ListQueues",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "iam:SimulatePrincipalPolicy",
        "iam:GetRole"
      ],
      "Resource": "*"
    }
  ]
}
    
```

Amazon EC2 A... | 61 Action(s) sel... | Select All | Deselect All | Reset Contexts | Clear Results | Run Simulation

▶ Global Settings ⓘ

Action Settings and Results [61 actions selected. 0 actions not simulated. 61 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2 Auto Scaling	AttachInstances	autoScalingGroup	*	allowed 1 matching statements.
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.
Amazon EC2 Auto Scaling	CancelInstanceRefresh	autoScalingGroup	*	allowed 1 matching statements.
Amazon EC2 Auto Scaling	CompleteLifecycleAction	autoScalingGroup	*	allowed 1 matching statements.
Amazon EC2 Auto Scaling	CreateAutoScalingGroup	autoScalingGroup	*	allowed 1 matching statements.
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.

Para obtener información detallada, consulte la [documentación de AWS IAM](#).

Otras referencias

[Uso de una función de IAM para conceder permisos a las aplicaciones que se ejecutan en instancias de Amazon EC2](#)

Cómo funciona una instancia de NetScaler VPX en AWS

October 17, 2024

La instancia de NetScaler VPX está disponible como AMI en AWS Marketplace y se puede lanzar como instancia EC2 dentro de una VPC de AWS. La instancia de AMI de NetScaler VPX requiere un mínimo de 2 CPU virtuales y 2 GB de memoria. Una instancia EC2 lanzada dentro de una VPC de AWS también puede proporcionar las múltiples interfaces, varias direcciones IP por interfaz y direcciones IP públicas y privadas necesarias para la configuración VPX. Cada instancia VPX requiere al menos tres subredes IP:

- Una subred de administración
- Una subred (VIP) orientada al cliente
- Una subred orientada al back-end (SNIP, MIP, etc.)

Citrix recomienda tres interfaces de red para una instancia VPX estándar en la instalación de AWS.

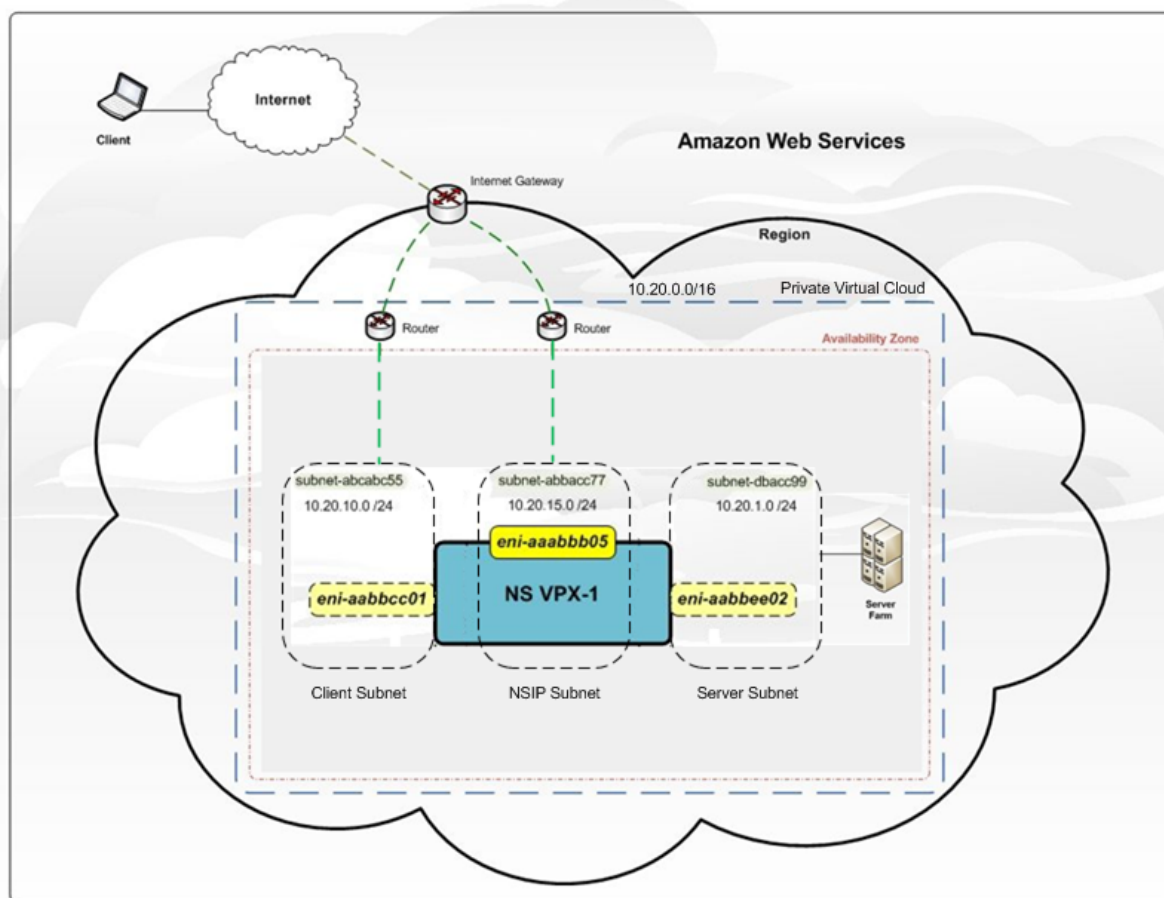
Actualmente, AWS hace que la funcionalidad de IP múltiple esté disponible solo para las instancias que se ejecutan en una VPC de AWS. Una instancia VPX en una VPC se puede utilizar para equilibrar la

carga de servidores que se ejecutan en instancias EC2. Una VPC de Amazon le permite crear y controlar un entorno de red virtual, incluido su propio intervalo de direcciones IP, subredes, tablas de rutas y puertas de enlace de red.

Nota:

De forma predeterminada, puede crear hasta 5 instancias de VPC por región de AWS para cada cuenta de AWS. Puede solicitar mayores límites de VPC enviando el formulario de solicitud de Amazon <http://aws.amazon.com/contact-us/vpc-request>.

Figura 1. Ejemplo de implementación de una instancia NetScaler VPX en la arquitectura de AWS



La figura 1 muestra una topología simple de una VPC de AWS con una Implementación de NetScaler VPX. La VPC de AWS tiene:

1. Una única Gateway de Internet para enrutar el tráfico de entrada y salida de la VPC.
2. Conectividad de red entre la Gateway de Internet e Internet.
3. Tres subredes, una para administración, cliente y servidor cada una.
4. Conectividad de red entre la Gateway de Internet y las dos subredes (administración y cliente).

5. Una instancia de NetScaler VPX independiente implementada en la VPC. La instancia VPX tiene tres ENIs, uno asociado a cada subred.

Implementación de una instancia independiente NetScaler VPX en AWS

October 17, 2024

Puede implementar una instancia independiente de NetScaler VPX en AWS mediante las siguientes opciones:

- Consola web de AWS
- Plantilla CloudFormation creada por Citrix
- AWS CLI

En este tema se describe el procedimiento para implementar una instancia de NetScaler VPX en AWS.

Antes de iniciar la implementación, lea los siguientes temas:

- [Requisitos previos](#)
- [Pautas de limitación y uso](#)

Implemente una instancia de NetScaler VPX en AWS mediante la consola web de AWS

Puede implementar una instancia de NetScaler VPX en AWS a través de la consola web de AWS. El proceso de implementación incluye los siguientes pasos:

1. Crear un par de claves
2. Crear una nube privada virtual (VPC)
3. Agregar más subredes
4. Crear grupos de seguridad y reglas de seguridad
5. Agregar tablas de redirecciones
6. Crea una puerta de enlace a internet
7. Crear una instancia de NetScaler VPX
8. Crear y conectar más interfaces de red
9. Adjuntar IP elásticas a la NIC de administración
10. Conectarse a la instancia VPX

Paso 1: Crear un par de claves.

Amazon EC2 utiliza un par de claves para cifrar y descifrar la información de inicio de sesión. Para iniciar sesión en la instancia, debe crear un par de claves, especificar el nombre del par de claves al iniciar la instancia y proporcionar la clave privada cuando se conecte a la instancia.

Cuando revise e inicie una instancia mediante el asistente AWS Launch Instance, se le pedirá que utilice un par de claves existente o cree un nuevo par de claves. Para obtener más información sobre cómo crear un par de claves, consulte [Pares de claves de Amazon EC2](#).

Paso 2: Cree una VPC.

Una instancia de VPC de NetScaler se implementa dentro de una VPC de AWS. Una VPC le permite definir la red virtual dedicada a su cuenta de AWS. Para obtener más información sobre AWS VPC, consulte [Introducción a Amazon VPC](#).

Al crear una VPC para su instancia de NetScaler VPX, tenga en cuenta los siguientes puntos.

- Utilice la opción VPC con una única subred pública únicamente para crear una VPC de AWS en una zona de disponibilidad de AWS.
- Citrix recomienda crear al menos **tres subredes**, de los siguientes tipos:
 - Una subred para el tráfico de administración. Coloque la IP de administración (NSIP) en esta subred. Por defecto, la interfaz de red elástica (ENI) eth0 se utiliza para la administración de IP.
 - Una o más subredes para el tráfico de acceso de cliente (de usuario a NetScaler VPX), a través de las cuales los clientes se conectan a una o más direcciones IP virtuales (VIP) asignadas a servidores virtuales de equilibrio de carga ADC de Citrix.
 - Una o más subredes para el tráfico de acceso al servidor (VPX a Servidor), a través del cual los servidores se conectan a direcciones IP de subred (SNIP) propiedad de VPX. Para obtener más información sobre el equilibrio de carga y los servidores virtuales de NetScaler, las direcciones IP virtuales (VIP) y las direcciones IP de subred (SNIP), consulte:
 - Todas las subredes deben estar en la misma zona de disponibilidad.

Paso 3: Agregar subredes.

Cuando utilizó el Asistente para VPC, solo se creó una subred. Dependiendo de sus necesidades, es posible que quiera crear más subredes. Para obtener más información sobre cómo crear más subredes, consulte [Adición de una subred a la VPC](#).

Paso 4: Crear grupos de seguridad y reglas de seguridad.

Para controlar el tráfico entrante y saliente, cree grupos de seguridad y agregue reglas a los grupos. Para obtener más información sobre cómo crear grupos y agregar reglas, consulte [Grupos de seguridad para la VPC](#).

Para las instancias de NetScaler VPX, el asistente EC2 proporciona grupos de seguridad predeterminados, generados por AWS Marketplace y basados en la configuración recomendada por Citrix. Sin embargo, puede crear más grupos de seguridad según sus requisitos.

Nota:

Puertos 22, 80, 443 que se abrirá en el grupo Seguridad para acceso SSH, HTTP y HTTPS respectivamente.

Paso 5: Agregar tablas de redirecciones.

La tabla de redirecciones contiene un conjunto de reglas, denominadas redirecciones, que se utilizan para determinar adónde se dirige el tráfico de red. Cada subred de la VPC debe estar asociada a una tabla de redirecciones. Para obtener más información sobre cómo crear una tabla de redirección, consulte [Tablas de redirección](#).

Paso 6: Crear una puerta de enlace a Internet.

Una puerta de enlace de Internet tiene dos propósitos: proporcionar un destino en las tablas de redirecciones de VPC para el tráfico redirigible a Internet y realizar la traducción de direcciones de red (NAT) para las instancias a las que se han asignado direcciones IPv4 públicas.

Crear una Gateway de Internet para el tráfico de Internet. Para obtener más información sobre cómo crear una puerta de enlace de Internet, consulte la sección [Adjuntar una puerta de enlace de Internet](#).

Paso 7: Cree una instancia de NetScaler VPX mediante el servicio AWS EC2.

Para crear una instancia de NetScaler VPX mediante el servicio AWS EC2, siga estos pasos.

1. En el panel de AWS, vaya a **Compute > EC2 > Launch Instance > AWS Marketplace**.

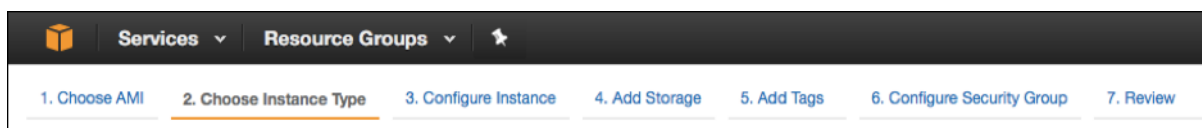
Antes de hacer clic en **Launch Instance**, asegúrese de que su región es correcta comprobando la nota que aparece en **Launch Instance**.



2. En la barra Search AWS Marketplace, busque con la palabra clave NetScaler VPX.
3. Seleccione la versión que quiere implementar y, a continuación, haga clic en **Seleccionar**. Para la versión NetScaler VPX, tiene las siguientes opciones:
 - Una versión con licencia
 - Dispositivo NetScaler VPX Express (se trata de un dispositivo virtual gratuito, disponible en NetScaler 12.0 56.20).
 - Trae su propio dispositivo

Se inicia el asistente de inicio de instancias. Siga el asistente para crear una instancia. El asistente le pide que:

- Elegir tipo de instancia
- Configurar instancia
- Añadir almacenamiento
- Agregar etiquetas
- Configurar grupo de seguridad
- Revisar



Paso 8: Cree y conecte más interfaces de red.

Cree dos interfaces de red más para VIP y SNIP. Para obtener más información sobre cómo crear más interfaces de red, consulte la sección [Creación de una interfaz de red](#).

Después de crear las interfaces de red, debe adjuntarlas a la instancia VPX. Antes de conectar la interfaz, apague la instancia VPX, conecte la interfaz y encienda la instancia. Para obtener más información sobre cómo conectar interfaces de red, consulte la sección [Adjuntar una interfaz de red al iniciar una instancia](#).

Paso 9: Asignar y asociar IP elásticas.

Si asigna una dirección IP pública a una instancia EC2, permanecerá asignada solo hasta que se detenga la instancia. Después de eso, la dirección se libera de nuevo al grupo. Al reiniciar la instancia, se asigna una nueva dirección IP pública.

Por el contrario, una dirección IP elástica (EIP) permanece asignada hasta que la dirección se desasocia de una instancia.

Asigne y asocie una IP elástica para la NIC de administración. Para obtener más información acerca de cómo asignar y asociar direcciones IP elásticas, consulte estos temas:

- [Asignación de una dirección IP elástica](#)
- [Asociación de una dirección IP elástica con una instancia en ejecución](#)

Estos pasos completan el procedimiento para crear una instancia de NetScaler VPX en AWS. La instancia puede tardar unos minutos en estar lista. Compruebe que su instancia ha superado las comprobaciones de estado. Puede ver esta información en la columna **Comprobaciones de estado** de la página Instancias.

Paso 10: Conéctese a la instancia VPX.

Después de crear la instancia VPX, se conecta la instancia mediante la interfaz gráfica de usuario y un cliente SSH.

- Interfaz gráfica (GUI)

Las siguientes son las credenciales de administrador predeterminadas para acceder a una instancia de NetScaler VPX

Nombre de usuario: `nsroot`

Contraseña: la contraseña predeterminada para la cuenta raíz ns se establece en el ID de instancia de AWS de la instancia de NetScaler VPX. La primera vez que inicie sesión, se le pedirá que cambie la contraseña por motivos de seguridad. Después de cambiar la contraseña, debe guardar la configuración. Si la configuración no se guarda y la instancia se reinicia, debe iniciar sesión con la contraseña predeterminada. Vuelva a cambiar la contraseña en el indicador.

- Cliente SSH

En la consola de administración de AWS, seleccione la instancia de NetScaler VPX y haga clic en Conectar. Siga las instrucciones que aparecen en la página **Conéctese a su instancia** . Siga las instrucciones que se indican en la página **Conectar a su instancia**.

Para obtener más información sobre cómo implementar una instancia independiente de NetScaler VPX en AWS mediante la consola web de AWS, consulte [Escenario: instancia independiente](#)

Configure una instancia de NetScaler VPX mediante la plantilla Citrix CloudFormation

Puede utilizar la plantilla CloudFormation proporcionada por Citrix para automatizar el lanzamiento de instancias VPX. La plantilla proporciona funciones para lanzar una sola instancia de NetScaler VPX o para crear un entorno de alta disponibilidad con un par de instancias de NetScaler VPX.

Puede iniciar la plantilla desde AWS Marketplace o GitHub.

La plantilla CloudFormation requiere un entorno de VPC existente y lanza una instancia VPX con tres interfaces de red elásticas (ENI). Antes de iniciar la plantilla de CloudFormation, asegúrese de completar los siguientes requisitos:

- Una nube privada virtual (VPC) de AWS
- Tres subredes dentro de la VPC: Una para administración, otra para tráfico de clientes y otra para servidores back-end
- Un par de claves EC2 para habilitar el acceso SSH a la instancia
- Un grupo de seguridad con puertos UDP 3003, TCP 3009—3010, HTTP y SSH abiertos

Consulte la sección “Implementar una instancia de NetScaler VPX en AWS mediante el uso de la consola web de AWS” o la documentación de AWS para obtener más información sobre cómo completar los requisitos previos.

Vea este [vídeo](#) para obtener información sobre cómo configurar e iniciar una instancia independiente NetScaler VPX mediante la plantilla Citrix CloudFormation disponible en AWS Marketplace.

<https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/>

Una función de IAM no es obligatoria para una implementación independiente. Sin embargo, Citrix recomienda crear y adjuntar un rol de IAM con los privilegios necesarios a la instancia, para futuras necesidades. El rol de IAM garantiza que la instancia independiente se convierta fácilmente a un nodo de alta disponibilidad con SR-IOV, cuando sea necesario.

Para obtener más información sobre los privilegios necesarios, consulte [Configuración de instancias de NetScaler VPX para usar la interfaz de red SR-IOV](#).

Nota:

Si implementa una instancia de NetScaler VPX en AWS mediante la consola web de AWS, el servicio CloudWatch está habilitado de forma predeterminada. Si implementa una instancia de NetScaler VPX mediante la plantilla de Citrix CloudFormation, la opción predeterminada es “Sí”. Si desea deshabilitar el servicio CloudWatch, seleccione “No”. Para obtener más información, consulte [Supervisar sus instancias mediante Amazon CloudWatch](#)

Configure una instancia de NetScaler VPX mediante la CLI de AWS

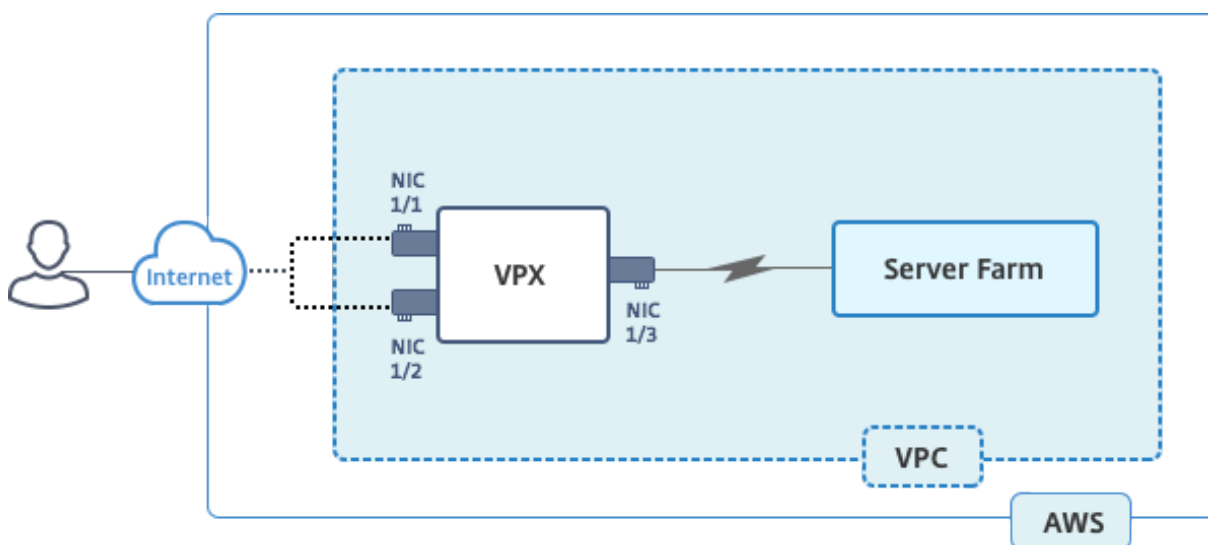
Puede utilizar la CLI de AWS para iniciar instancias. Para obtener más información, consulte la [documentación de AWS Command Line Interface](#).

Caso: Instancia independiente

October 17, 2024

Este caso ilustra cómo implementar una instancia EC2 independiente de NetScaler VPX en AWS mediante la interfaz gráfica de usuario de AWS. Cree una instancia VPX independiente con tres NIC. La instancia, que está configurada como un servidor virtual de equilibrio de carga, se comunica con los servidores de fondo (el conjunto de servidores). Para esta configuración, configure las rutas de comunicación necesarias entre la instancia y los servidores back-end, y entre la instancia y los hosts externos en Internet público.

Para obtener más detalles sobre el procedimiento para implementar una instancia VPX, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#).



Cree tres NIC. Cada NIC se puede configurar con un par de direcciones IP (públicas y privadas). Las NIC sirven para los siguientes propósitos.

NIC	Propósito	Asociada con
eth0	Sirve tráfico de administración (NSIP)	Una dirección IP pública y una dirección IP privada
eth1	Sirve tráfico del lado del cliente (VIP)	Una dirección IP pública y una dirección IP privada
eth2	Se comunica con servidores back-end (SNIP)	Una dirección IP pública (la dirección IP privada no es obligatoria)

Paso 1: Cree una VPC.

1. Inicie sesión en la consola web de AWS y vaya a **Redes y entrega de contenido > VPC**. Haz clic en **Iniciar asistente de VPC**.
2. **Seleccione**VPC con una única subred pública y **haga clic en Seleccionar**.
3. Defina el bloque IP CIDR en 10.0.0.0/16 para este caso.
4. Asigne un nombre a la VPC.
5. Configure la subred pública en 10.0.0.0/24. (Esta es la red de administración).
6. Seleccione una zona de disponibilidad.
7. Dar un nombre para la subred.
8. Haga clic en Crear **VPC**.

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block:* (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block
 Amazon provided IPv6 CIDR block

VPC name:

Public subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:*

Subnet name:

You can add more subnets after AWS creates the VPC.

Service endpoints

Enable DNS hostnames:* Yes No

Hardware tenancy:*

Paso 2: Crea subredes adicionales.

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, seleccione Subredes y Crear subred después de introducir los siguientes detalles.
 - Etiqueta de nombre: proporcione un nombre para la subred.
 - VPC: elige la VPC para la que vas a crear la subred.
 - Zona de disponibilidad: elija la zona de disponibilidad en la que creó la VPC en el paso 1.
 - Bloque CIDR IPv4: especifique un bloque CIDR IPv4 para la subred. Para este caso, elija 10.0.1.0/24.

Create Subnet ✕

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: ⓘ

VPC: ⓘ

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability Zone: ⓘ

IPv4 CIDR block: ⓘ

3. Repita los pasos para crear una subred más para los servidores de fondo.

Create Subnet ✕

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC ⓘ

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability Zone ⓘ

IPv4 CIDR block ⓘ

Paso 3: Crea una tabla de rutas.

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija **Tablas de rutas > Crear tabla de rutas**.
3. En la ventana Crear tabla de rutas, añada un nombre y seleccione la VPC que creó en el paso 1.
4. Haga clic en **Yes, Create**.

Create Route Table ✕

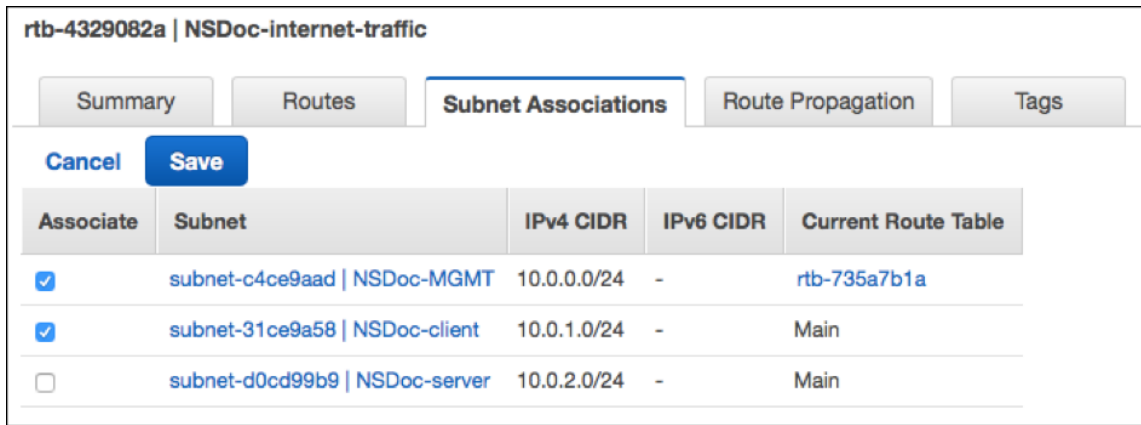
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag ⓘ

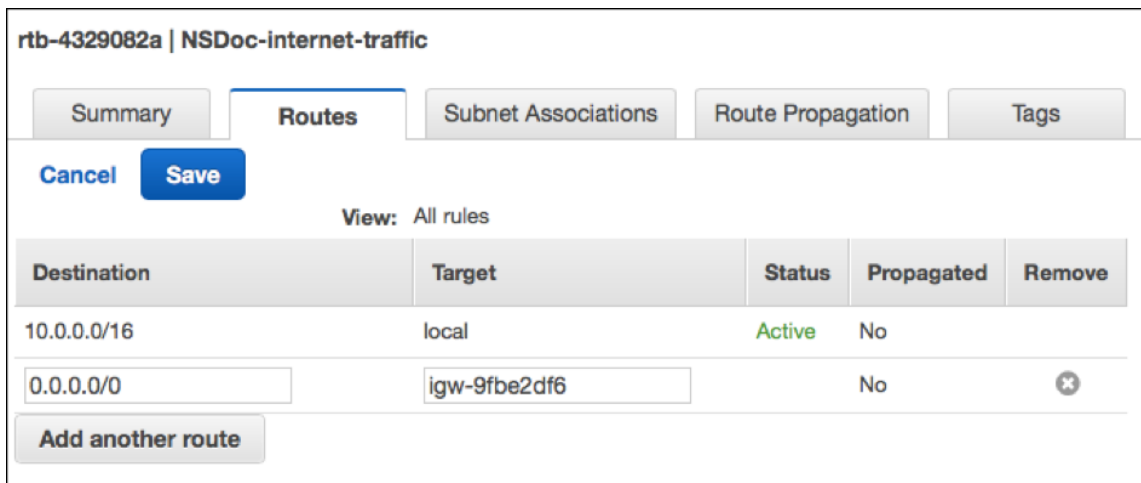
VPC ⓘ

La tabla de redirección se asigna a todas las subredes que ha creado para esta VPC, de modo que la redirección del tráfico de una instancia de una subred pueda llegar a una instancia de otra subred.

5. Haga clic en **Asociaciones de subredy**, a continuación, haga clic en **Editar**.
6. Haga clic en la subred de administración y cliente y, a continuación, en Guardar. Esto crea una tabla de rutas únicamente para el tráfico de Internet.



7. Haga clic en **Rutas > Editar > Añadir otra ruta**.
8. En el campo Destino, añada 0.0.0.0/0 y haga clic en el campo Destino para seleccionar igw-the <xxxx> Internet Gateway que el asistente de VPC creó automáticamente.
9. Haga clic en **Guardar**.

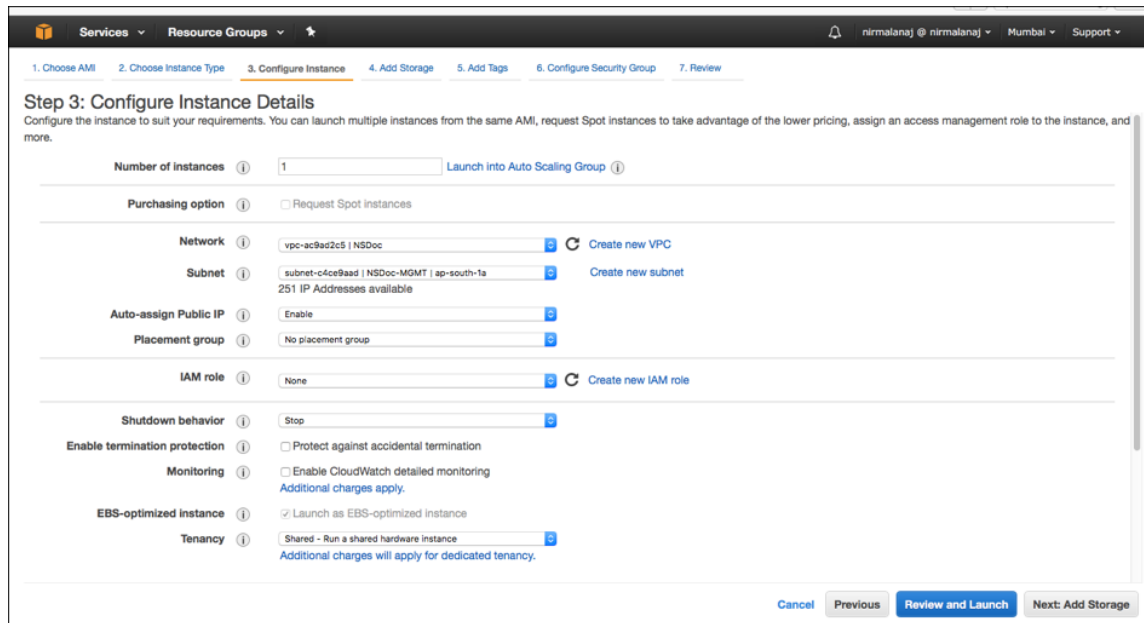


10. Siga los pasos para crear una tabla de rutas para el tráfico del lado del servidor.

Paso 4: Cree una instancia de NetScaler VPX.

1. Inicie sesión en la consola de administración de AWS y haga clic en **EC2 en Compute**.
2. Haga clic en AWS Marketplace. En la barra Buscar en AWS Marketplace, escriba NetScaler VPX y presione Entrar. Se muestran las ediciones de NetScaler VPX disponibles.
3. Haga clic en **Seleccionar** para elegir la edición de NetScaler VPX que desee. Se inicia el asistente de instancias de EC2.
4. En la página **Elija el tipo de instancia**, seleccione **m4. Xlarge** (recomendado) y haga clic en **Siguiente: Configurar detalles de la instancia**.
5. En la página Configurar detalles de instancia, seleccione lo siguiente y luego haga clic en **Siguiente: Agregar almacenamiento**.

- Número de instancias: 1
- Red: la VPC que se creó en el paso 1
- Subred: la subred de administración
- Asignación automática de IP pública: Habilitar



6. En la página Agregar almacenamiento, seleccione la opción predeterminada y haga clic en **Siguiente: Agregar etiquetas**.
7. En la página Agregar etiquetas, agregue un nombre para la instancia y haga clic en **Siguiente: Configurar el grupo de seguridad**.
8. En la página Configurar grupo de seguridad, seleccione la opción predeterminada (que la genera AWS Marketplace y se basa en la configuración recomendada por Citrix Systems) y, a continuación, haga clic en **Revisar e iniciar > Iniciar**.
9. Se le solicitará que seleccione un par de claves existente o que cree un nuevo par de claves. En la lista desplegable Seleccione un par de claves, seleccione el par de claves que creó como requisito previo (consulte la sección Requisitos previos).
10. Marque la casilla para reconocer el par de claves y haga clic en **Iniciar instancias**.

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 to securely SSH into your instance.

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

El asistente de lanzamiento de instancias muestra el estado de lanzamiento y la instancia aparece en la lista de instancias cuando se ha lanzado por completo.

Para verificar la instancia, vaya a la consola de AWS y haga clic en **EC2 > Instancias en ejecución**. Seleccione la instancia y añada un nombre. Asegúrese de que el estado de la instancia esté en ejecución y que las comprobaciones de estado estén completas.

Paso 5: Crear y conectar más interfaces de red.

Cuando creaste la VPC, solo había una interfaz de red asociada a ella. Ahora, agregue dos interfaces de red más a la VPC, para VIP y SNIP.

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Interfaces de red.
3. Seleccione Crear interfaz de red.
4. Para **Descripción**, ingrese un nombre descriptivo.
5. Para **Subred**, seleccione la subred que creó anteriormente para el VIP.
6. Para **IP privada**, deje la opción predeterminada.
7. Para los grupos de seguridad **, seleccione el grupo.
8. Haga clic en **Yes, Create**.

9. Una vez creada la interfaz de red, añada un nombre a la interfaz.
10. Repita los pasos para crear una interfaz de red para el tráfico del lado del servidor.

Conecta las interfaces de red:

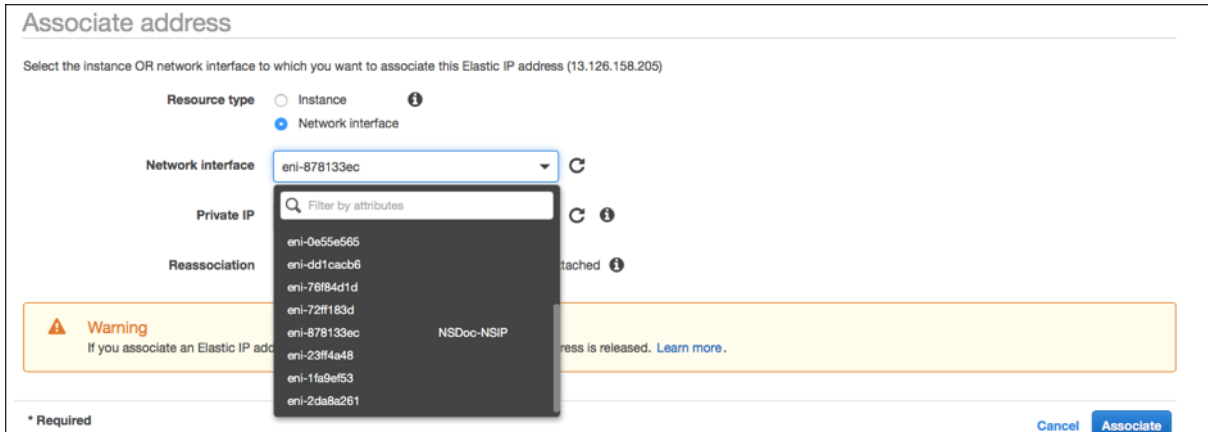
1. En el panel de navegación, elija Interfaces de red.
2. Seleccione la interfaz de red y haga clic en **Adjuntar**.
3. En el cuadro de diálogo Conectar interfaz de red, seleccione la instancia y haga clic en **Adjuntar**.

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups	
<input type="checkbox"/>	NSDoc-VIP-...	eni-3c843657	subnet-31ce9a...	vpc-ac9ad2c5	ap-south-1a	default
<input checked="" type="checkbox"/>	NSDoc-SNIP	eni-3e8b3955	subnet-d0cd99...	vpc-ac9ad2c5	ap-south-1a	default
<input type="checkbox"/>		eni-dd1cacb6	subnet-9d43f6f4	vpc-52ab033b	ap-south-1a	FreeBSD 11-11-0-R
<input type="checkbox"/>	NSDoc-NSIP	eni-878133ec	subnet-c4ce9aad	vpc-ac9ad2c5	ap-south-1a	NetScaler VPX - Cu
<input type="checkbox"/>		eni-2da8a261	subnet-f6882b3	vpc-52ab033b	ap-south-1b	All
<input type="checkbox"/>		eni-e0f9128b				
<input type="checkbox"/>		eni-0e55e565				
<input type="checkbox"/>		eni-1fa9ef53				
<input type="checkbox"/>		eni-23ff4a48				
<input type="checkbox"/>		eni-45fb4e2e				
<input type="checkbox"/>		eni-76f84d1d				
<input type="checkbox"/>		eni-72ff183d				

Paso 6: Adjunte una IP elástica al NSIP.

1. Desde la consola de administración de AWS, vaya a **RED Y SEGURIDAD > Elastic IPs**.
2. Compruebe si hay un EIP gratuito disponible para adjuntarlo. Si no hay ninguna, haz clic en **Asignar nueva dirección**.
3. Seleccione la dirección IP recién asignada y elija **Acciones > Dirección asociada**.
4. Haga clic en el botón de radio **de la interfaz de red**.

5. En la lista desplegable de la interfaz de red, seleccione la NIC de administración.
6. En el menú desplegable **IP privada**, seleccione la dirección IP generada por AWS.
7. Seleccione la casilla **Reasociación**.
8. Haz clic en **Asociar**.



Acceda a la instancia VPX:

Después de configurar una instancia de NetScaler VPX independiente con tres NIC, inicie sesión en la instancia VPX para completar la configuración del lado de NetScaler. Uso de las siguientes opciones:

- GUI: escriba la IP pública de la NIC de administración en el navegador. Inicie sesión con el nombre de usuario y el ID de instancia (i-0c1ffe1d987817522) `nsroot` como contraseña.

Nota:

La primera vez que inicie sesión, se le pedirá que cambie la contraseña por motivos de seguridad. Después de cambiar la contraseña, debe guardar la configuración. Si la configuración no se guarda y la instancia se reinicia, debe iniciar sesión con la contraseña predeterminada. Vuelva a cambiar la contraseña cuando se le solicite y guarde la configuración.

- SSH: Abre un cliente SSH y escribe:

```
ssh -i \\&#060;location of your private key\\&#062; ns root@\\&#060;  
public DNS of the instance\\&#062;
```

Para buscar el DNS público, haz clic en la instancia y, a continuación, en **Conectar**.

Información relacionada:

- Para configurar las direcciones IP propiedad de NetScaler (NSIP, VIP y SNIP), consulte [Configuración de direcciones IP propiedad de NetScaler](#).
- Ha configurado una versión BYOL del dispositivo NetScaler VPX, para obtener más información, consulte la Guía de licencias de VPX en <http://support.citrix.com/article/CTX122426>

Descargar una licencia de NetScaler VPX

October 17, 2024

Después del lanzamiento de la instancia con licencia del cliente de NetScaler VPX desde el mercado de AWS, se requiere una licencia. Para obtener más información sobre las licencias VPX, consulte [Descripción general de licencias](#).

<http://support.citrix.com/article/CTX122426> Es necesario que:

1. Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
2. Cargue la licencia en la instancia.

Si se trata de una instancia de mercado de **pago**, no es necesario instalar licencia. El conjunto de funciones y el rendimiento correctos se activan automáticamente.

Si utiliza una instancia de NetScaler VPX con un número de modelo superior a VPX 5000, es posible que el rendimiento de red no sea el mismo especificado en la licencia de la instancia. Sin embargo, otras funciones, como el rendimiento SSL y las transacciones SSL por segundo, podrían mejorar.

El ancho de banda de red de 5 Gbps se observa en el tipo de `c4.8xlarge` instancia.

Cómo migrar la suscripción de AWS a BYOL

En esta sección se describe el procedimiento para migrar de la suscripción de AWS a Bring your own license (BYOL) y, por el contrario.

Siga los siguientes pasos para migrar una suscripción de AWS a BYOL:

Nota:

Los **pasos 2 y 3** se realizan en la instancia NetScaler VPX y todos los demás pasos se realizan en el portal de AWS.

1. Cree una instancia BYOL EC2 mediante [NetScaler VPX: licencia del cliente](#) en la misma zona de disponibilidad que la antigua instancia de EC2 que tiene el mismo grupo de seguridad, rol de IAM y subred. La nueva instancia EC2 debe tener solo una interfaz ENI.
2. Para hacer copias de seguridad de los datos de la antigua instancia de EC2 mediante la GUI de NetScaler, siga estos pasos.
 - a) Diríjase a **Sistema > Copia de seguridad y restauración**.
 - b) En la página de **bienvenida**, haga clic en **Copia/Importar** para iniciar el proceso.

System > Backup and Restore

Welcome to
Backup and Restore

The backup and restore functionality of the Citrix ADC appliance allows you to create a backup file of the Citrix ADC configurations. This file can later be used to restore the Citrix ADC configurations to the previous state.
To create a backup, click the "Backup..." link shown below. When required, select one of the backups and restore the appliance.

[Backup/Import](#)

c) En la página **Copia/Importación**, rellene los siguientes detalles:

- **Nombre:** Nombre del archivo de copia de seguridad.
- **Nivel:** Seleccione el nivel de copia de seguridad como **Completo**.
- **Comentario:** Proporcione una breve descripción de la copia de seguridad.

System > Backup and Restore > Backup/Import

Backup/Import

Create Import

Citrix ADC Version
NS13.1: Build 50.19.nc, Date: Sep 25 2023, 21:28:29 (64-bit)

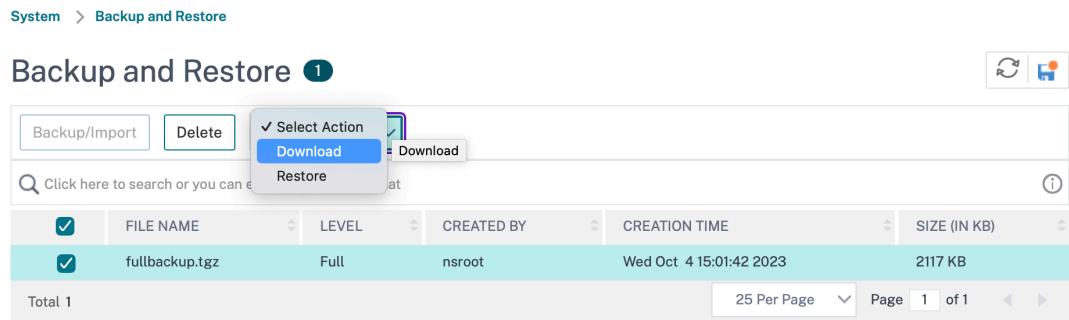
File Name
 ⓘ

Level*
 ⓘ

Comment

[Backup](#) [Cancel](#)

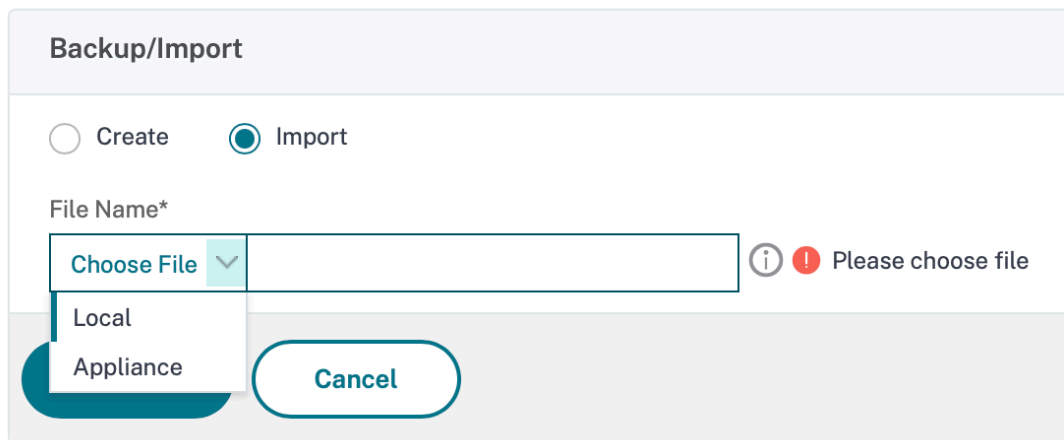
- d) Haga clic en **Copia de seguridad**. Una vez finalizada la copia de seguridad, puede seleccionar el archivo y descargarlo en el equipo local.



3. Para restaurar los datos de la nueva instancia de EC2 mediante la GUI de NetScaler, siga estos pasos:

- Diríjase a **Sistema > Copia de seguridad y restauración**.
- Haga clic en **Copia de seguridad/importación** para iniciar el proceso.
- Seleccione la opción **Importar** y cargue el archivo de copia de seguridad.

System > Backup and Restore > Backup/Import



- Selecciona el archivo.
- En el menú desplegable **Seleccionar acción**, seleccione **Restaurar**.

System > Backup and Restore

Backup and Restore 1

Backup/Import Delete Select Action Download Restore


Click here to search or you can e Restore

<input checked="" type="checkbox"/>	FILE NAME	LEVEL	CREATED BY	CREATION TIME	SIZE (IN KB)
<input checked="" type="checkbox"/>	fullbackup.tgz	Full	nsroot	Wed Oct 4 15:01:42 2023	2117 KB

Total 1 25 Per Page Page 1 of 1

f) En la página **Restaurar**, verifique los detalles del archivo y haga clic en **Restaurar**.

← Restore

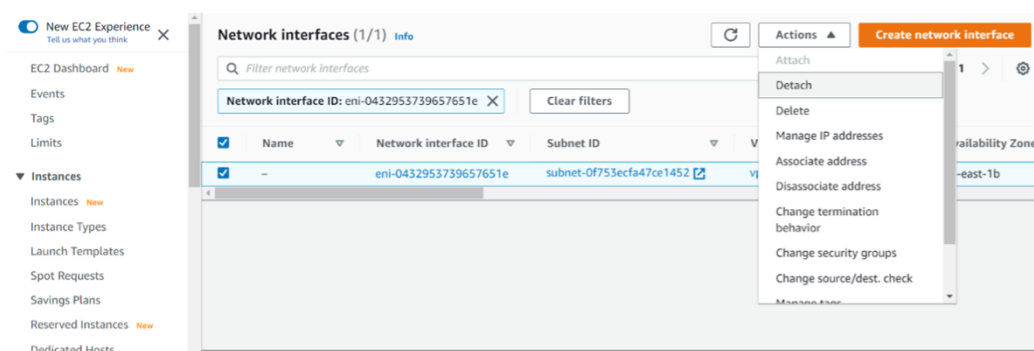
File Name	fullbackup.tgz
Level	Full
Citrix ADC Version	NS13.1-50.19
IP Address	10.102.126.34
Size (in KB)	2117
Created By	nsroot
Creation Time	Wed Oct 4 15:01:42 2023
Comment	None
<input type="checkbox"/> Skip Backup	

Restore **Close**

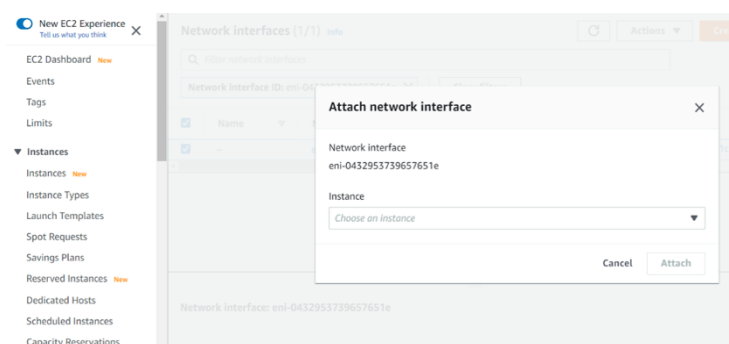
- g) Después de la restauración, reinicie la instancia EC2.
4. Mueva todas las interfaces (excepto la interfaz de administración a la que está enlazada la direc-

ción NSIP) de la antigua instancia EC2 a la nueva instancia EC2. Para mover una interfaz de red de una instancia EC2 a otra, sigue estos pasos:

- a) En el **portal de AWS**, detenga las instancias EC2 antiguas y nuevas.
- b) Vaya a **Interfaces de red** y seleccione la interfaz de red conectada a la antigua instancia EC2.
- c) Desconecte la instancia de EC2 haciendo clic en **Acciones > Desconectar**.



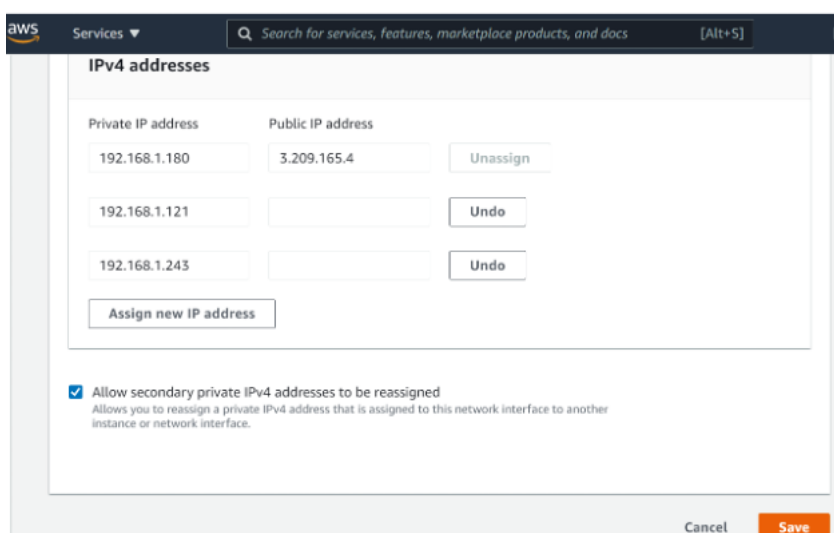
- d) Adjunte la interfaz de red a la nueva instancia de EC2 haciendo clic en **Acciones > Adjuntar**. Introduzca el nombre de instancia EC2 al que debe asociarse la interfaz de red.



- e) Realice el **paso 1 al paso 4** para todas las demás interfaces conectadas. Asegúrese de seguir la secuencia y mantener el orden de la interfaz. Es decir, primero desconecte la interfaz 2 y conéctela, y luego desmonte la interfaz 3 y conéctela, etc.
5. No se puede separar la interfaz de administración de una instancia EC2 anterior. Por lo tanto, mueva todas las direcciones IP secundarias (si las hay) de la interfaz de administración (interfaz de red principal) de la antigua instancia EC2 a la nueva instancia EC2. Para mover una dirección IP de una interfaz a otra, sigue estos pasos:

- a) En el **portal de AWS**, asegúrese de que las instancias EC2 antiguas y nuevas estén en estado **Stop**.
- b) Vaya a **Interfaces de red** y seleccione la interfaz de red de administración asociada a la antigua instancia EC2.

- c) Haga clic en **Acciones > Administrar dirección IP** y anote todas las direcciones IP secundarias asignadas (si las hay).
- d) Desplácese hasta la interfaz de red de administración o la interfaz principal de la nueva instancia EC2.
- e) Haga clic en **Acciones > Administrar direcciones IP**.
- f) En **Direcciones IPv4**, haga clic en **Asignar nueva dirección IP**.
- g) Introduzca las direcciones IP, que se indican en el **paso 3**.
- h) Active la casilla de verificación **Permitir que se reasignen direcciones IP privadas secundarias**.
- i) Haga clic en **Guardar**.



6. Inicie la nueva instancia de EC2 y verifique la configuración. Después de mover toda la configuración, puede eliminar o conservar la antigua instancia de EC2 según sus necesidades.
7. Si se adjunta alguna dirección EIP a la dirección NSIP de la instancia EC2 anterior, mueva la dirección NSIP de la instancia anterior a la nueva dirección NSIP de instancia.
8. Si quieres volver a la instancia anterior, sigue los mismos pasos en sentido contrario entre la instancia anterior y la nueva.
9. Después de pasar de la instancia de suscripción a la instancia BYOL, se requiere una licencia. Para instalar una licencia, siga estos pasos:
 - Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
 - Cargue la licencia en la instancia.

Nota:

Cuando mueve la instancia BYOL a la instancia de suscripción (instancia de mercado de pago), no es necesario instalar la licencia. El conjunto de funciones y el rendimiento correctos se activan automáticamente.

Limitaciones

La interfaz de administración no se puede mover a la nueva instancia EC2. Por lo tanto, Citrix recomienda configurar manualmente la interfaz de administración. Para obtener más información, consulte el **paso 5** del procedimiento anterior. Se crea una nueva instancia EC2 con la réplica exacta de la antigua instancia EC2, pero solo la dirección NSIP tiene una nueva dirección IP.

Servidores de equilibrio de carga en diferentes zonas de disponibilidad

October 17, 2024

Una instancia VPX se puede utilizar para equilibrar la carga de servidores que se ejecutan en la misma zona de disponibilidad, o en:

- Una zona de disponibilidad diferente (AZ) en la misma VPC de AWS
- Una región de AWS diferente
- AWS EC2 en una VPC

Para permitir que una instancia VPX equilibre la carga de servidores que se ejecutan fuera de la VPC de AWS, la instancia VPX está activa; configure la instancia para usar EIP para enrutar el tráfico a través de la puerta de enlace de Internet, de la siguiente manera:

1. Configure un SNIP en la instancia de NetScaler VPX mediante la CLI de NetScaler o la GUI.
2. Habilite que el tráfico se enrute fuera de la AZ, creando una subred pública para el tráfico del lado del servidor.
3. Agregue una ruta de Gateway de Internet a la tabla de redirecciones mediante la consola GUI de AWS.
4. Asocie la tabla de redirección que ha actualizado a la subred del lado del servidor.
5. Asocie un EIP con la dirección IP privada del servidor asignada a una dirección SNIP de NetScaler.

Cómo funciona la alta disponibilidad en AWS

October 17, 2024

Puede configurar dos instancias de NetScaler VPX en AWS como un par activo-pasivo de alta disponibilidad (HA). Al configurar una instancia como nodo principal y la otra como nodo secundario, el nodo principal acepta las conexiones y administra los servidores. El nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

En AWS, se admiten los siguientes tipos de implementación para las instancias VPX:

- Alta disponibilidad dentro de la misma zona
- Alta disponibilidad en diferentes zonas

Nota:

Para que funcione la alta disponibilidad, asegúrese de que ambas instancias de NetScaler VPX estén asociadas a funciones de IAM y asignadas la dirección IP elástica (EIP) al NSIP. No es necesario asignar un EIP al NSIP si el NSIP puede acceder a Internet a través de la instancia de NAT.

Alta disponibilidad dentro de las mismas zonas

En una implementación de alta disponibilidad dentro de las mismas zonas, ambas instancias VPX deben tener configuraciones de red similares.

Siga estas dos reglas:

Regla 1. Cualquier NIC de una instancia de VPX debe estar en la misma subred que la NIC correspondiente de la otra VPX. Ambas instancias deben tener:

- Interfaz de administración en la misma subred (denominada subred de administración)
- Interfaz de cliente en la misma subred (denominada subred de cliente)
- Interfaz de servidor en la misma subred (denominada subred del servidor)

Artículo 2. La secuencia de NIC de administración, NIC cliente y NIC de servidor en ambas instancias debe ser la misma. Por ejemplo, no se admite el siguiente caso.

Instancia VPX 1

NIC 0: administración NIC 1: cliente NIC 2: Servidor

Instancia VPX 2

NIC 0: administración

NIC 1: servidor

NIC 2: cliente

En este caso, la NIC 1 de la instancia 1 está en la subred del cliente mientras que la NIC 1 de la instancia 2 está en la subred del servidor. Para que ha funcionado, la NIC 1 de ambas instancias debe estar en la subred cliente o en la subred del servidor.

A partir de 13.0 41.xx, se puede lograr una alta disponibilidad migrando direcciones IP privadas secundarias conectadas a las NIC (NIC del cliente y del servidor) del nodo HA primario al nodo HA secundario después de la conmutación por error. En esta implementación:

- Ambas instancias VPX tienen el mismo número de NIC y asignación de subred según la enumeración de NIC.
- Cada NIC VPX tiene una dirección IP privada adicional, excepto la primera NIC, que corresponde a la dirección IP de administración. La dirección IP privada adicional aparece como la dirección IP privada principal en la consola web de AWS. En nuestro documento, nos referimos a esta dirección IP adicional como dirección IP ficticia).
- Las direcciones IP ficticias no deben configurarse en la instancia de NetScaler como VIP y SNIP.
- Otras direcciones IP privadas secundarias deben crearse, según sea necesario, y configurarse como VIP y SNIP.
- En la conmutación por error, el nuevo nodo principal busca SNIP y VIP configurados y los mueve de las NIC asociadas al principal anterior a las NIC correspondientes en el nuevo primario.
- Las instancias NetScaler requieren permisos de IAM para que funcione HA. Agregue los siguientes privilegios de IAM a la directiva de IAM agregada a cada instancia.

```
"iam:GetRole" "ec2:DescribeInstances" "ec2:DescribeInterfacesDeRed"  
"ec2:AsignarDireccionesIPPrivadas"
```

Nota:

`unassignPrivateIpAddress` no es obligatorio.

Este método es más rápido que el método tradicional. En el método anterior, HA depende de la migración de las interfaces de red elásticas de AWS del nodo principal al nodo secundario.

Para un método heredado, se requieren las siguientes directivas:

```
"iam:GetRole" "ec2:DescribeInstances" "ec2:DescribeDirecciones" "ec2:  
Dirección asociada" "ec2:DesasociarDirección"
```

Para obtener más información, consulte [Implementar un par de alta disponibilidad en AWS](#).

Alta disponibilidad en diferentes zonas

Puede configurar dos instancias de NetScaler VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes, como un par activo-pasivo de alta disponibilidad en modo de configuración de red independiente (INC). Tras la conmutación por error, el EIP (Elastic IP) del VIP de la instancia principal migra al secundario, que toma el relevo como el nuevo primario. En el proceso de conmutación por error, la API de AWS:

- Comprueba los servidores virtuales que tienen `IPSets` adjuntado a ellos.
- Busca la dirección IP que tiene una IP pública asociada, de las dos direcciones IP en las que está escuchando el servidor virtual. Uno que se conecta directamente al servidor virtual y otro que se conecta a través del conjunto de IP.
- Reasocia la IP pública (EIP) a la IP privada que pertenece al nuevo VIP principal.

Para HA en diferentes zonas, se requieren las siguientes directivas:

```
"iam:GetRole" "ec2:DescribeInstances" "ec2:DescribeDirecciones" "ec2:
Dirección asociada" "ec2:DesasociarDirección"
```

Para obtener más información, consulte [Alta disponibilidad en las zonas de disponibilidad de AWS](#).

Antes de iniciar la implementación

Antes de iniciar cualquier implementación de HA en AWS, lea el siguiente documento:

- [Requisitos previos](#)
- [Limitaciones y directrices de uso](#)
- [Implementar una instancia de NetScaler VPX en AWS](#)
- [Alta disponibilidad](#)

Solución de problemas

Para solucionar cualquier error durante una conmutación por error de HA de una instancia de NetScaler VPX en la nube de AWS, compruebe el archivo `cloud-ha-daemon.log` almacenado en la ubicación `/var/log/`.

Implementar un par de alta disponibilidad de VPX en la misma zona de disponibilidad de AWS

October 17, 2024

Nota:

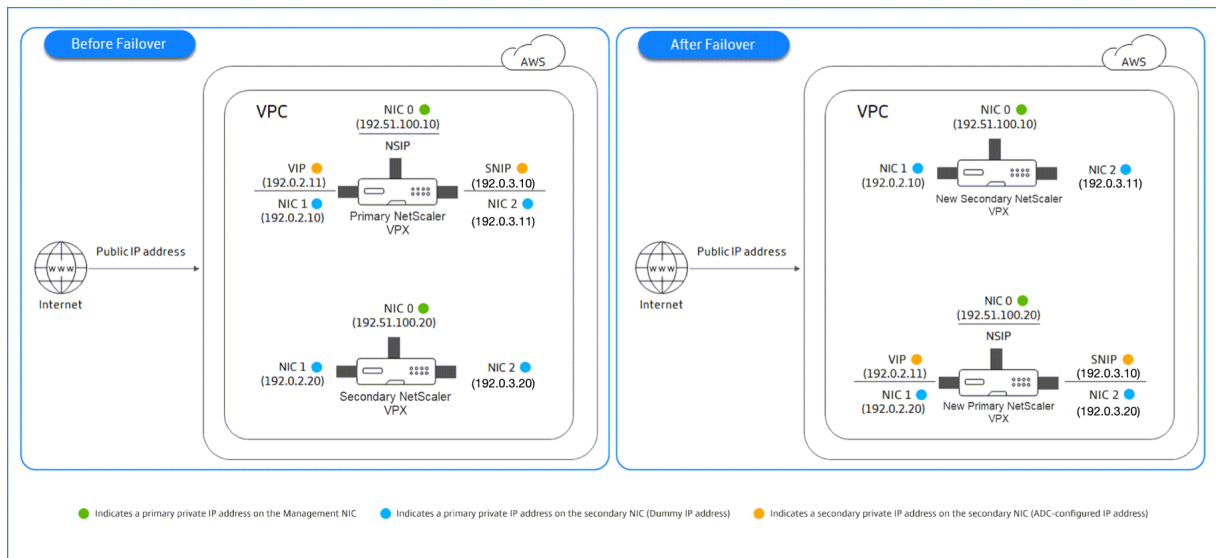
A partir de la versión 13.1 compilación 27.x de NetScaler, el par VPX HA en la misma zona de disponibilidad de AWS admite direcciones IPv6.

Puede configurar dos instancias NetScaler VPX en AWS como un par de alta disponibilidad, en la misma zona de AWS, donde ambas instancias VPX están en la misma subred. La alta disponibilidad se logra migrando las direcciones IP privadas secundarias conectadas a las NIC (NIC del lado del cliente y del servidor) del nodo de alta disponibilidad principal al nodo de alta disponibilidad secundario después de la conmutación por error. También se migran todas las direcciones IP elásticas asociadas a las direcciones IP privadas secundarias.

El par de alta disponibilidad de NetScaler VPX admite direcciones IPv4 e IPv6 en la misma zona de disponibilidad de AWS.

En la siguiente ilustración se muestra un caso de conmutación por error de alta disponibilidad mediante la migración de direcciones IP privadas secundarias.

Ilustración 1. Un par de alta disponibilidad de NetScaler VPX en AWS, mediante la migración de IP privada



Antes de empezar el documento, lee los siguientes documentos:

- [Requisitos previos](#)
- [Limitaciones y directrices de uso](#)
- [Implementar una instancia de NetScaler VPX en AWS](#)
- [Alta disponibilidad](#)

Cómo implementar un par VPX HA en la misma zona

Este es el resumen de los pasos para implementar un par VPX HA en la misma zona:

1. Cree dos instancias VPX en AWS, cada una con tres NIC.
2. Asigne la dirección IP privada secundaria de AWS al VIP y al SNIP del nodo principal.
3. Configure VIP y SNIP en el nodo principal con las direcciones IP privadas secundarias de AWS.
4. Configure HA en ambos nodos.

Paso 1. Cree dos instancias VPX (nodos primario y secundario) mediante la misma VPC, cada una con tres NIC (Ethernet 0, Ethernet 1, Ethernet 2)

Siga los pasos que se indican en [Implementación de una instancia NetScaler VPX en AWS mediante la consola web de AWS](#).

Paso 2. Paso 2: En el nodo principal, asigne direcciones IP privadas para Ethernet 1 (IP de cliente o VIP) y Ethernet 2 (IP de servidor back-end o SNIP)

La consola de AWS asigna automáticamente direcciones IP privadas principales a las NIC configuradas. Asigne más direcciones IP privadas a VIP y SNIP, conocidas como direcciones IP privadas secundarias.

Para asignar una dirección IP privada a una interfaz de red, siga estos pasos:

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija **Interfases de red** y, a continuación, seleccione la interfaz de red conectada a la instancia.
3. Elija **Acciones > Administrar direcciones IP**.
4. Seleccione **Direcciones IPv4** o **Direcciones IPv6** según sus necesidades.
5. Para direcciones IPv4:
 - a) Seleccione **Asignar nueva IP**.
 - b) Introduce una dirección IPv4 específica que esté dentro del intervalo de subredes de la instancia o deja el campo en blanco para que Amazon seleccione una dirección IP para ti.
 - c) (Opcional) Elija **Permitir reasignación** para permitir que se reasigne la dirección IP privada secundaria si ya está asignada a otra interfaz de red.
6. Para direcciones IPv6:
 - a) Seleccione **Asignar nueva IP**.
 - b) Introduce una dirección IPv6 específica que esté dentro del rango de subredes de la instancia o deja el campo en blanco para que Amazon pueda seleccionar una dirección IP por ti.

- c) (Opcional) Elija **Permitir reasignación** para permitir que se reasigne la dirección IP privada principal o secundaria si ya está asignada a otra interfaz de red.

7. Selecciona **Sí > Actualizar**.

En la **descripción de la instancia**, aparecen las direcciones IP privadas asignadas.

Nota:

En una implementación de par de alta disponibilidad IPv4, puede asignar solo las direcciones IPv4 secundarias en la interfaz y usarlas como direcciones VIP y SNIP. Sin embargo, en una implementación de par IPv6 HA, puede asignar la dirección IPv6 principal o la dirección IPv6 secundaria en la interfaz y utilizarlas como direcciones VIP y SNIP.

Paso 3. Configurar VIP y SNIP en el nodo principal, mediante direcciones IP privadas secundarias

Acceda al nodo principal mediante SSH. Abra un cliente ssh y escriba:

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

A continuación, configure VIP y SNIP.

Para VIP, escriba:

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

Para SNIP, escriba:

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

Escriba `save config` para guardar.

Para ver las direcciones IP configuradas, escriba el siguiente comando:

```
1 show ns ip
```

Para obtener más información, consulte estos temas:

- [Configurar y administrar direcciones IP virtuales \(VIP\)](#)
- [Configurar la dirección IP de NetScaler](#)

Paso 4: configurar HA en ambas instancias

En el nodo principal, abra un cliente de Shell y escriba el siguiente comando:

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

En el nodo secundario, escriba el siguiente comando:

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

Escriba `save config` para guardar la configuración.

Para ver los nodos de alta disponibilidad configurados, escriba `show ha node`.

Tras la conmutación por error, las direcciones IP privadas secundarias configuradas como VIP y SNIP en el nodo principal anterior se migran al nuevo nodo principal.

Para forzar una conmutación por error en un nodo, escriba `force HA` conmutación por error.

Migre un par de HA heredado a un nuevo par de HA en función de la migración de IP privada secundaria

Nota:

El método heredado para implementar el par VPX HA que funciona en función de la migración de ENI está en desuso. Por lo tanto, le recomendamos que utilice la implementación de pares de alta disponibilidad basada en la migración de IP privada secundaria.

Para permitir una migración sin problemas de un par de alta disponibilidad heredado a un nuevo par de alta disponibilidad basada en la migración de IP privada secundaria, asegúrese de lo siguiente:

1. Tanto el nodo principal como el secundario deben tener el mismo número de interfaces y estas interfaces deben estar en las mismas subredes.
2. El VIP y el SNIP configurados como dirección IP privada principal en el método heredado se deben migrar a una dirección IP privada secundaria en el nuevo método.
3. Los permisos de IAM necesarios para la nueva implementación de alta disponibilidad se deben agregar a las instancias de NetScaler principales y secundarias.
4. Reinicie las instancias principales y secundarias de NetScaler.

Para obtener más información, consulta [Alta disponibilidad en las mismas zonas](#).

Implemente un par de alta disponibilidad mediante la plantilla Citrix CloudFormation

Antes de iniciar la plantilla de CloudFormation, asegúrese de cumplir los siguientes requisitos:

- UN VPC
- Tres subredes dentro de la VPC

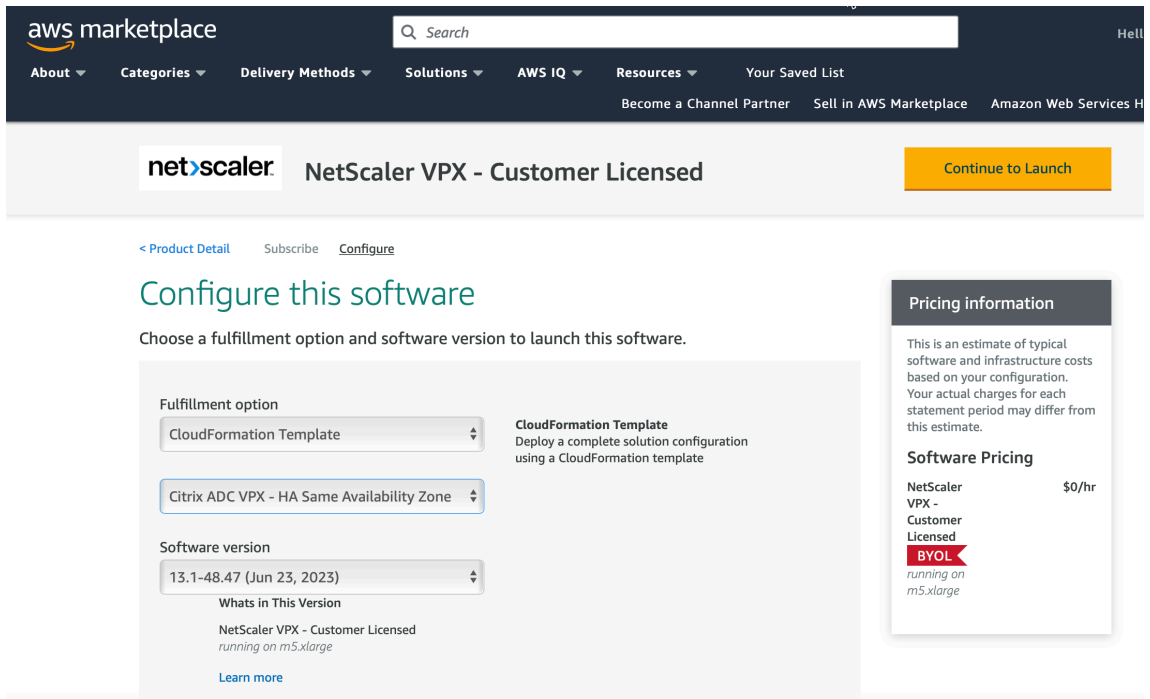
- Un grupo de seguridad con puertos UDP 3003, TCP 3009—3010, HTTP y SSH abiertos
- Un par de llaves
- Crea una puerta de enlace a internet
- Modificar tablas de rutas para que las redes de clientes y de administración apunten a la puerta de enlace de Internet

Nota:

La plantilla de Citrix CloudFormation crea automáticamente un rol de IAM. Las funciones de IAM existentes no aparecen en la plantilla.

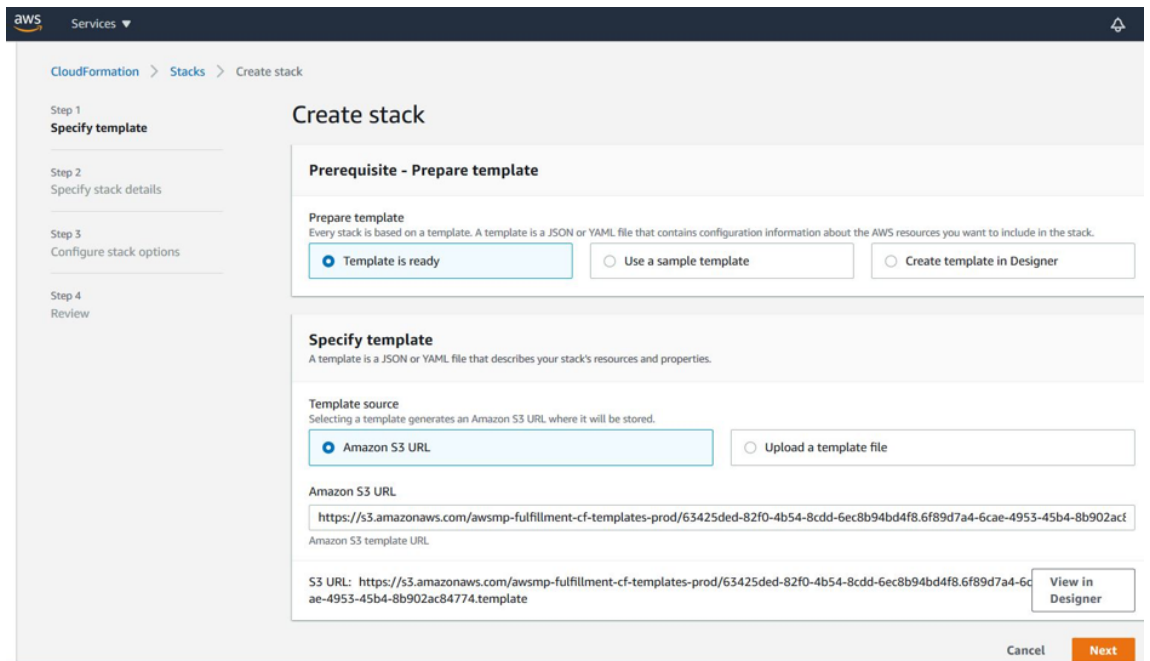
Para iniciar la plantilla de Citrix CloudFormation:

1. Inicie sesión en el [mercado de AWS](#) mediante sus credenciales de AWS.
2. En el campo de búsqueda, escriba **NetScaler VPX** para buscar la AMI de NetScaler y haga clic en **Ir**.
3. En la página de resultados de búsqueda, haga clic en la oferta de NetScaler VPX deseada.
4. Haga clic en la ficha **Precios** para ir a **Información de precios**.
5. Seleccione la región y la **opción de gestión logística** como **NetScaler VPX: licencia del cliente**.
6. Haga clic en **Continuar para suscribirse**.
7. Consulte los detalles en la página **Suscribirse** y haga clic en **Continuar con la configuración**.
8. Seleccione **Método de entrega** como **plantilla de CloudFormation**.
9. Seleccione la plantilla de CloudFormation requerida.
10. Seleccione **Versión de software** y **región** y haga clic en **Continuar para iniciar**.



11. En **Elegir acción**, seleccione **Launch CloudFormation** y haga clic en **Launch**. Aparece la página **Crear pila**.

12. Haga clic en **Siguiente**.



13. Aparece la página **Especificar detalles de pila**. Introduzca los siguientes detalles.

- Escriba un **nombre de pila**. El nombre debe tener 25 caracteres.
- En **Configuración de red**, lleve a cabo lo siguiente:

- Seleccione **Subred de administración, Subred de cliente y Subred de servidor**. Asegúrese de seleccionar las subredes correctas que creó en la VPC que seleccionó bajo ID de VPC.
- Agregue **IP de administración primaria, IP de administración secundaria, IP de cliente IP de servidor**. Las direcciones IP deben pertenecer a las mismas subredes de las respectivas subredes. Alternativamente, puede dejar que la plantilla asigne las direcciones IP automáticamente.
- Seleccione el **valor predeterminado** para **VPCTenancy**.
- En **Configuración de NetScaler**, lleve a cabo lo siguiente:
 - Seleccione **m5.xlarge** para **Tipo de instancia**.
 - Seleccione el par de claves que ya ha creado en el menú de **Par de claves**.
 - De forma predeterminada, **¿Publicar métricas personalizadas en CloudWatch?** La opción está establecida en **Sí**. Si quiere inhabilitar esta opción, seleccione **No**. Para obtener más información sobre las métricas de CloudWatch, consulte [Monitorear sus instancias usando Amazon CloudWatch] (#monitor-your-instances-using-amazon-cloudWatch).
- En **Configuración opcional**, haga lo siguiente:
 - De forma predeterminada, el método **¿Se debe asignar publicIP(EIP) a las interfaces de administración?** La opción está establecida en **No**.
 - De forma predeterminada, el método **¿Se debe asignar publicIP(EIP) a la interfaz de cliente?** La opción está establecida en **No**.

aws Services

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

Enter a stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

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 CIDR range of the form x.x.x.x/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

Citrix ADC Configuration

Citrix ADC instance type

m5.xlarge

Keypair to associate to ADCs

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

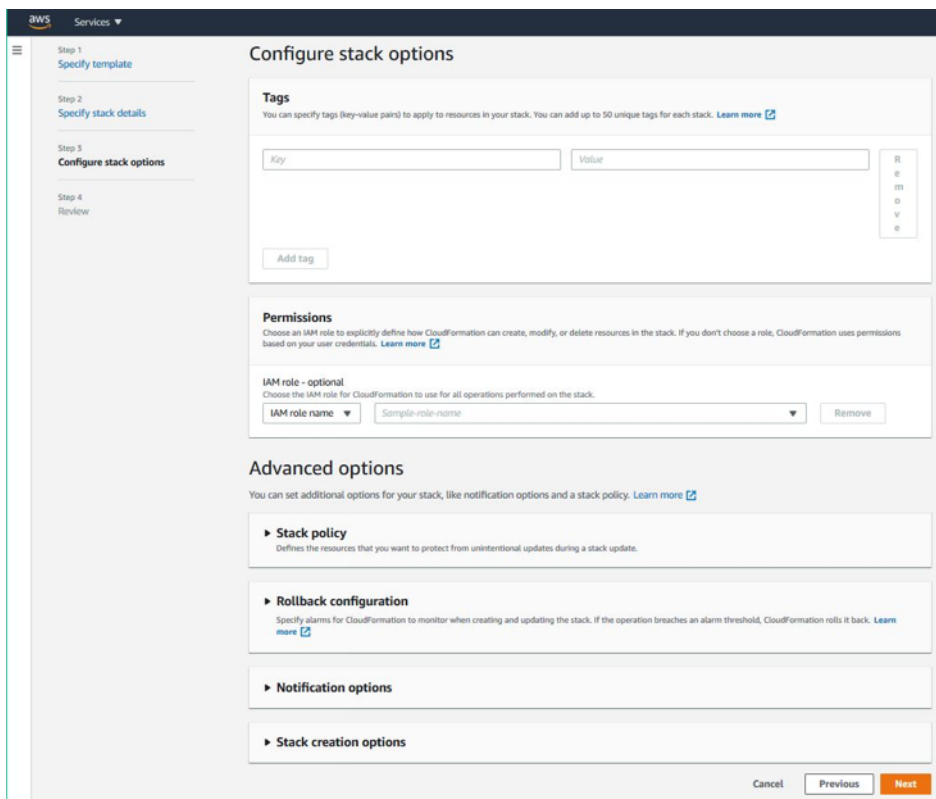
Should PublicIP(EIP) be assigned to client interface?

No

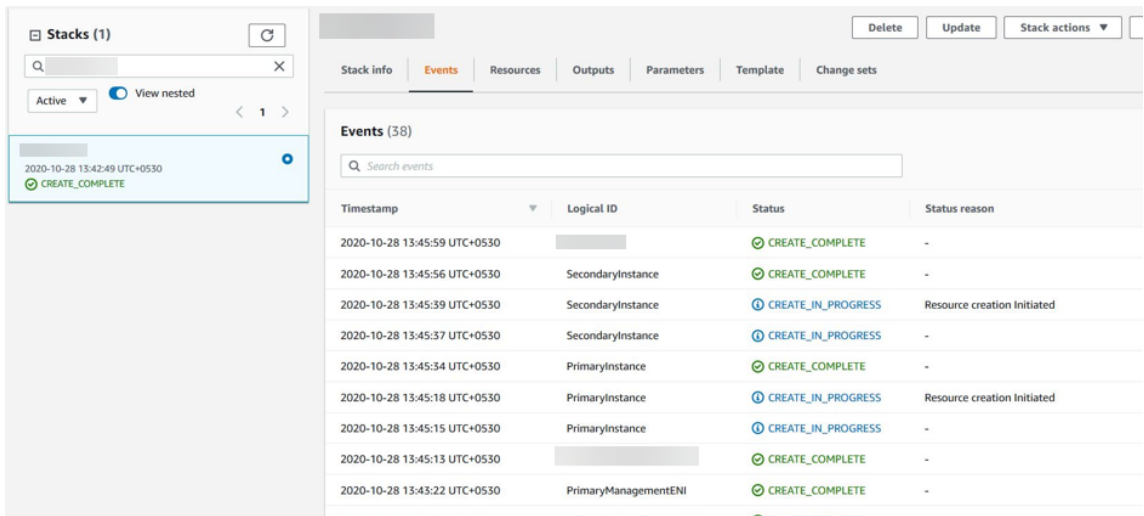
Cancel Previous Next

14. Haga clic en **Siguiente**.

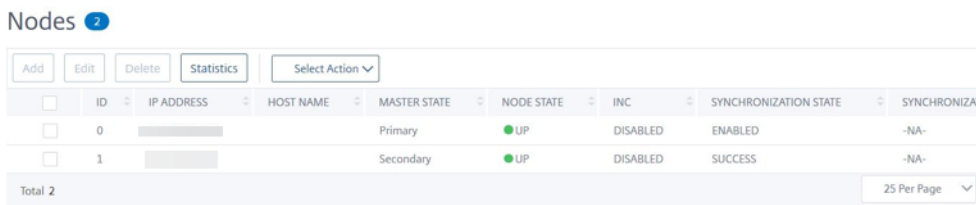
15. Aparece la página **Configurar opciones de pila**. Esta página es opcional.



16. Haga clic en **Siguiente**.
17. Aparecerá la página **Opciones**. (Esta es una página opcional). Haga clic en **Siguiente**.
18. Aparecerá la página **Revisar**. Dedique un momento a revisar la configuración y realizar cambios, si es necesario.
19. Seleccione **Reconozco que AWS CloudFormation podría crear recursos IAM**. casilla de verificación y luego haga clic en **Crear pila**.
20. Aparece el estado **CREATE-IN-PROGRESS**. Espere hasta que el estado sea **CREATE-COMPLETE**. Si el estado no cambia a **COMPLETADO**, compruebe la ficha **Eventos** por el motivo de un error y vuelva a crear la instancia con las configuraciones adecuadas.



- Después de crear un recurso de IAM, vaya a **EC2 Management Console > Instancias**. Encontrará dos instancias VPX creadas con el rol de IAM. Los nodos principal y secundario se crean cada uno con tres direcciones IP privadas y tres interfaces de red.
- Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña. Desde la GUI, vaya a **Sistema > Alta disponibilidad > Nodos**. NetScaler VPX ya está configurado en par HA mediante la plantilla CloudFormation.
- Aparece el par NetScaler VPX HA.



Supervisar las instancias con Amazon CloudWatch

Puede utilizar el servicio Amazon CloudWatch para supervisar un conjunto de métricas de NetScaler VPX, como la utilización de la CPU y la memoria, y el rendimiento. CloudWatch supervisa los recursos y las aplicaciones que se ejecutan en AWS, en tiempo real. Puede acceder al panel de Amazon CloudWatch mediante la consola de administración de AWS. Para obtener más información, consulte [Amazon CloudWatch](#).

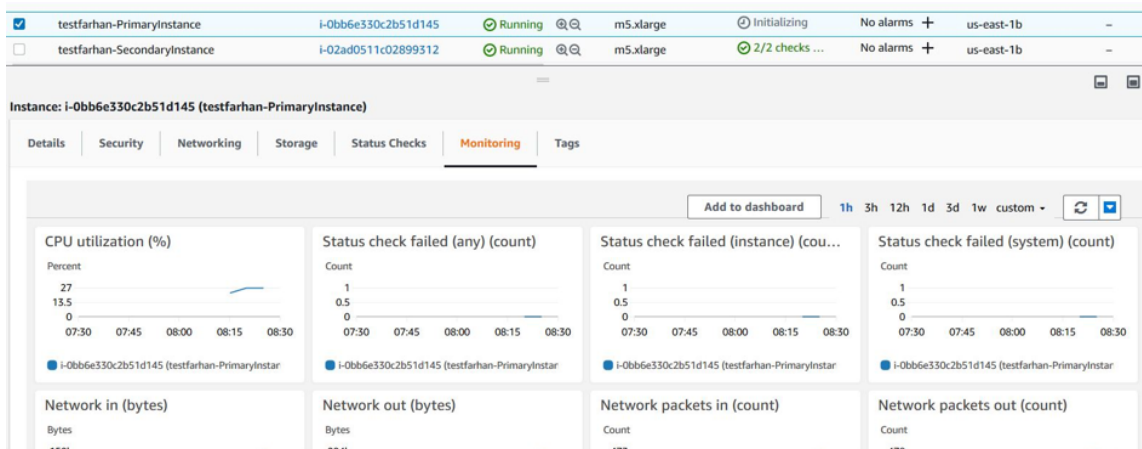
Puntos a tener en cuenta

- Si implementa una instancia de NetScaler VPX en AWS mediante la consola web de AWS, el servicio CloudWatch está habilitado de forma predeterminada.
- Si implementa una instancia de NetScaler VPX mediante la plantilla de Citrix CloudFormation, la opción predeterminada es “Sí”. Si desea deshabilitar el servicio CloudWatch, seleccione “No”.
- Las métricas están disponibles para la CPU (administración y uso de la CPU de paquetes), la memoria y el rendimiento (entrante y saliente).

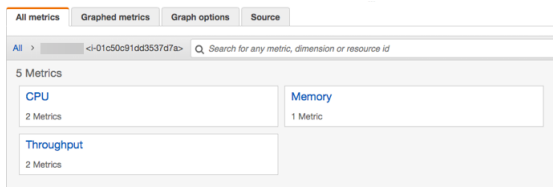
Cómo ver las métricas de CloudWatch

Para ver las métricas de CloudWatch de su instancia, siga estos pasos:

1. Inicie sesión en la **consola de administración de AWS > EC2 > Instancias**.
2. Seleccione la instancia.
3. Haga clic en **Supervisión**.
4. Haga clic en **Ver todas las métricas de CloudWatch**.



5. En Todas las métricas, haga clic en su ID de instancia.



6. Haga clic en las métricas que quiera ver y establezca la duración (en minutos, horas, días, semanas, meses).

Puntos a tener en cuenta

- Lea los siguientes documentos antes de comenzar la implementación:
 - [Terminología de AWS](#)
 - [Requisitos previos](#)
 - [Limitaciones y directrices de uso](#)
- El par de alta disponibilidad VPX puede residir en la misma zona de disponibilidad en una subred diferente o en dos zonas de disponibilidad de AWS diferentes.
- Citrix recomienda usar diferentes subredes para la administración (NSIP), el tráfico de clientes (VIP) y el servidor back-end (SNIP).
- La alta disponibilidad debe establecerse en el modo Configuración de red independiente (INC) para que funcione una conmutación por error.
- Las dos instancias deben tener el puerto 3003 abierto para el tráfico UDP, ya que se usa para los latidos.
- Las subredes de administración de ambos nodos deben tener acceso a Internet o al servidor API de AWS a través de NAT interna para que las demás API funcionen.
- El rol de IAM debe tener permiso E2 para la migración de IP pública o IP elástica (EIP) y permisos de tabla de ruta EC2 para la migración de IP privada.

Puede implementar alta disponibilidad en las zonas de disponibilidad de AWS de las siguientes formas:

- [Uso de direcciones IP elásticas](#)
- [Uso de direcciones IP privadas](#)

Referencias adicionales

Para obtener más información sobre NetScaler Application Delivery Management (ADM) para AWS, consulte [Instalar el agente NetScaler ADM en AWS](#).

Implementación de un par de alta disponibilidad VPX con direcciones IP elásticas en distintas zonas de AWS

October 17, 2024

Puede configurar dos instancias de NetScaler VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes mediante direcciones IP elásticas (EIP) en el modo INC.

Para obtener más información sobre la alta disponibilidad, consulte [Alta disponibilidad](#). Para obtener más información sobre INC, consulte [Configuración de nodos de alta disponibilidad en distintas sub-redes](#).

Cómo funciona la HA con direcciones EIP en diferentes zonas de AWS

Tras la conmutación por error, el EIP del VIP de la instancia principal migra a la secundaria, que se convierte en la nueva instancia principal. En el proceso de conmutación por error, la API de AWS:

1. Comprueba los servidores virtuales que tienen [IPSets](#) adjuntado a ellos.
2. Busca la dirección IP que tiene una IP pública asociada, de las dos direcciones IP en las que está escuchando el servidor virtual. Uno que se conecta directamente al servidor virtual y el que se conecta a través del conjunto de IP.
3. Reasocia la IP pública (EIP) a la IP privada que pertenece al nuevo VIP principal.

Nota:

Para proteger su red de ataques como la denegación de servicio (DoS), al utilizar una EIP, puede crear grupos de seguridad en AWS para restringir el acceso a la IP. Para obtener una alta disponibilidad, puede cambiar de EIP a una solución de movimiento IP privada según sus implementaciones.

Cómo implementar un par de alta disponibilidad VPX con direcciones IP elásticas en diferentes zonas de AWS

A continuación se presenta un resumen de los pasos para implementar un par VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes.

1. Cree una nube privada virtual de Amazon.
2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes o en la misma zona pero en subredes diferentes.
3. Paso 3: Configurar alta disponibilidad
 - a) Configure la alta disponibilidad en modo INC en ambas instancias.
 - b) Agregue un conjunto de IP en ambas instancias.
 - c) Enlazar el conjunto de IP en ambas instancias al VIP.
 - d) Agregue un servidor virtual en la instancia principal.

Para los pasos 1 y 2, utilice la consola de AWS. Para los pasos 3, use la GUI de NetScaler VPX o la CLI.

Paso 1. Cree una nube privada virtual de Amazon (VPC).

Paso 2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes o en la misma zona pero en subredes diferentes. Adjunte un EIP al VIP de la VPX principal.

Para obtener más información sobre cómo crear una VPC e implementar una instancia VPX en AWS, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#) y [Escenario: instancia independiente](#)

Paso 3. Configurar alta disponibilidad. Puede utilizar la CLI o la GUI de NetScaler VPX para configurar la alta disponibilidad.

Configurar la alta disponibilidad mediante la CLI

1. Configure la alta disponibilidad en modo INC en ambas instancias.

En el nodo principal:

```
add ha node 1 <sec_ip> -inc ENABLED
```

En el nodo secundario:

```
add ha node 1 <prim_ip> -inc ENABLED
```

<sec_ip> hace referencia a la dirección IP privada de la NIC de administración del nodo secundario

<prim_ip> hace referencia a la dirección IP privada de la NIC de administración del nodo principal

2. Agregue el conjunto de IP en ambas instancias.

Escriba el siguiente comando en ambas instancias.

```
add ipset <ipsetname>
```

3. Enlaza el conjunto de IP al conjunto VIP en ambas instancias.

Escriba el siguiente comando en ambas instancias:

```
add ns ip <secondary vip> <subnet> -type VIP
```

```
bind ipset <ipsetname> <secondary VIP>
```

Nota:

Puede vincular el conjunto de IP a la VIP principal o a la VIP secundaria. Sin embargo, si vincula el conjunto de IP al VIP principal, utilice el VIP secundario para agregar al servidor virtual, y viceversa.

4. Agregue un servidor virtual en la instancia principal.

Escriba este comando:

```
add &#060;server_type&#062; vserver &#060;vserver_name&#062;  
&#060;protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -  
ipset \\&#060;ipset_name&#062;
```

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

1. Configurar la alta disponibilidad en modo INC en ambas instancias
2. Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña.
3. Desde la interfaz gráfica de usuario, vaya a **Configuración > Sistema > Alta disponibilidad**. Haga clic en **Agregar**.
4. En el campo **Dirección IP del nodo remoto**, agregue la dirección IP privada de la NIC de administración del nodo secundario.
5. Seleccione **Activar el modo NIC (Configuración de red independiente)** en el nodo propio.
6. En **Credencial de inicio de sesión en el sistema remoto**, agregue el nombre de usuario y la contraseña del nodo secundario y haga clic en **Crear**.
7. Repita los pasos en el nodo secundario.
8. Agregue conjunto de IP y enlace conjunto de IP al conjunto VIP en ambas instancias.
9. Desde la GUI, vaya a **Sistema > Red > IP > Agregar**.
10. Agregue los valores requeridos para Dirección IP, máscara de red, Tipo de IP (IP virtual) y haga clic en **Crear**.
11. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
12. En la página IPv4s, seleccione la IP virtual y haga clic en **Insertar**. Haga clic en **Crear** para crear el conjunto de IP.
13. Agregar un servidor virtual en la instancia principal

En la GUI, vaya a **Configuración > Administración del tráfico > Servidores virtuales > Agregar**.

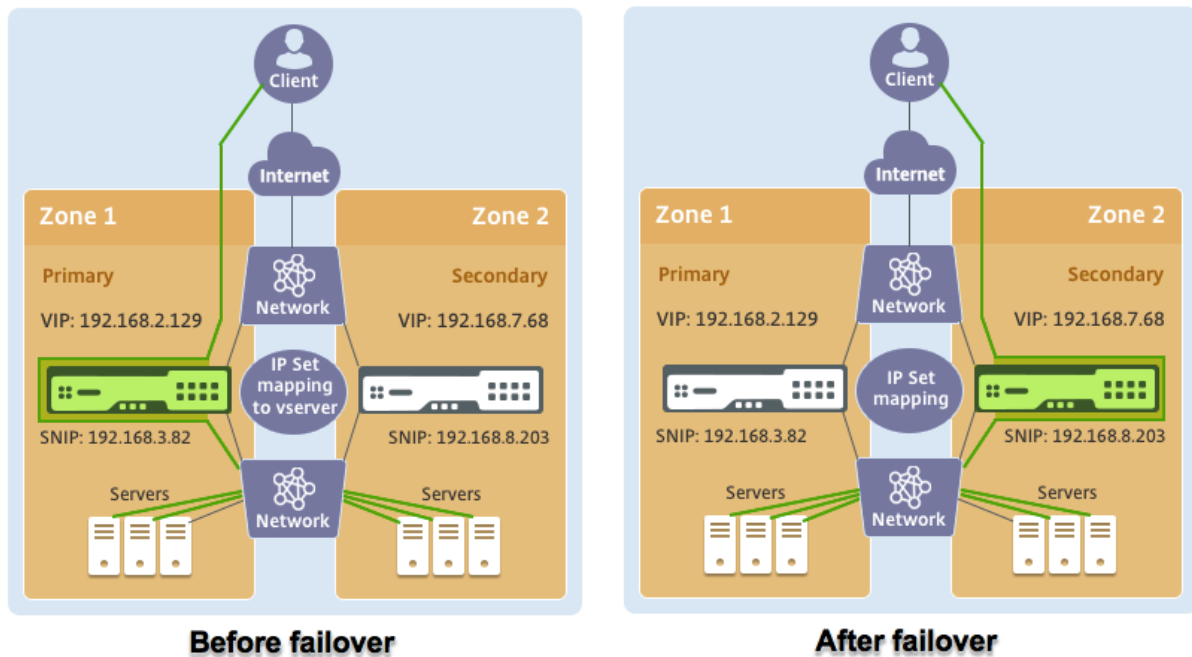
Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings	
Name	vserver1
Protocol	HTTP
State	● DOWN
IP Address	192.168.2.129
Port	80
Traffic Domain	0
Listen Priority	-
Listen Policy Expression	NONE
Redirection Mode	IP
Range	1
IPset	ipset123
RHI State	PASSIVE
AppFlow Logging	ENABLED
Retain Connections on Cluster	NO

Caso

En este caso, se crea una única VPC. En esa VPC, se crean dos instancias VPX en dos zonas de disponibilidad. Cada instancia tiene tres subredes: una para administración, otra para el cliente y otra para el servidor back-end. Se adjunta una EIP al VIP del nodo principal.

Diagrama: Este diagrama ilustra la configuración de alta disponibilidad de NetScaler VPX en modo INC, en AWS



En este caso, utilice la CLI para configurar la alta disponibilidad.

1. Configure la alta disponibilidad en modo INC en ambas instancias.

Escriba los siguientes comandos en los nodos primario y secundario.

En primaria:

```
add ha node 1 192.168.6.82 -inc enabled
```

En este caso, 192.168.6.82 se refiere a la dirección IP privada de la NIC de administración del nodo secundario.

En secundaria:

```
add ha node 1 192.168.1.108 -inc enabled
```

En este caso, 192.168.1.108 se refiere a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un conjunto de IP y enlace el conjunto de IP a la VIP en ambas instancias

En primaria:

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bindipset ipset123 192.168.7.68
```

En secundaria:

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bind ipset ipset123 192.168.7.68
```

3. Agregue un servidor virtual en la instancia principal.

El siguiente comando:

```
add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
```

4. Verifique la configuración.

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Statistics"/> <input type="button" value="Select Action"/>							
<input type="checkbox"/>	ID	IP Address	Host Name	Master State	Node State	INC	Synchronization State
<input type="checkbox"/>	0	192.168.1.108		Primary	● UP	ENABLED	ENABLED
<input type="checkbox"/>	1	192.168.6.82		Secondary	● UP	ENABLED	SUCCESS

5. Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario.

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Statistics"/> <input type="button" value="Select Action"/>							
<input type="checkbox"/>	ID	IP Address	Host Name	Master State	Node State	INC	Synchronization State
<input type="checkbox"/>	0	192.168.1.108		Secondary	● UP	ENABLED	SUCCESS
<input type="checkbox"/>	1	192.168.6.82		Primary	● UP	ENABLED	ENABLED

Implementar un par de alta disponibilidad VPX con direcciones IP privadas en distintas zonas de AWS

October 17, 2024

Puede configurar dos instancias de NetScaler VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS diferentes mediante direcciones IP privadas en el modo INC. Esta solución se puede integrar fácilmente con el par VPX de alta disponibilidad multizona [existente con direcciones IP elásticas](#). Por lo tanto, puede utilizar ambas soluciones juntas.

Para obtener más información sobre la alta disponibilidad, consulte [Alta disponibilidad](#). Para obtener más información sobre INC, consulte [Configuración de nodos de alta disponibilidad en distintas subredes](#).

Nota:

Esta implementación se admite desde NetScaler versión 13.0 compilación 67.39 en adelante.
Esta implementación es compatible con AWS Transit Gateway.

Emparejamiento de alta disponibilidad con direcciones IP privadas mediante una VPC no compartida de AWS

Requisitos previos

Asegúrese de que el rol de IAM asociado a su cuenta de AWS tenga los siguientes permisos de IAM:

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:DescribeInstances",
9                  "ec2:DescribeAddresses",
10                 "ec2:AssociateAddress",
11                 "ec2:DisassociateAddress",
12                 "ec2:DescribeRouteTables",
13                 "ec2>DeleteRoute",
14                 "ec2:CreateRoute",
15                 "ec2:ModifyNetworkInterfaceAttribute",
16                 "iam:SimulatePrincipalPolicy",
17                 "iam:GetRole"
18             ],
19             "Resource": "*",
20             "Effect": "Allow"
21         }
22     ]
23 }
24 }
```

Implemente un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC no compartida de AWS

A continuación se presenta un resumen de los pasos para implementar un par VPX en dos subredes diferentes o en dos zonas de disponibilidad de AWS distintas mediante direcciones IP privadas.

1. Cree una nube privada virtual de Amazon.

2. Implementa dos instancias VPX en dos zonas de disponibilidad diferentes.
3. Paso 3: Configurar alta disponibilidad
 - a) Configure la alta disponibilidad en modo INC en ambas instancias.
 - b) Agregue las tablas de redirección respectivas en la VPC que apunta a la interfaz del cliente.
 - c) Agregue un servidor virtual en la instancia principal.

Para los pasos 1, 2 y 3b, use la consola de AWS. Para los pasos 3a y 3c, utilice la GUI o la CLI de NetScaler VPX.

Paso 1. Cree una nube privada virtual de Amazon (VPC).

Paso 2. Implemente dos instancias VPX en dos zonas de disponibilidad diferentes con la misma cantidad de ENI (interfaz de red).

Para obtener más información sobre cómo crear una VPC e implementar una instancia VPX en AWS, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#) y [Escenario: instancia independiente](#)

Paso 3. Configure las direcciones VIP de ADC eligiendo una subred que no se superponga con las subredes de Amazon VPC. Si su VPC es 192.168.0.0/16, para configurar las direcciones VIP de ADC, puede elegir cualquier subred de estos intervalos de direcciones IP:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

En este ejemplo, la subred 10.10.10.0/24 elegida y se crearon VIP en esta subred. Puede elegir cualquier subred que no sea la subred VPC (192.168.0.0/16).

Paso 4. Agregue una ruta que apunte a la interfaz de cliente (VIP) del nodo principal desde la tabla de rutas de VPC.

En la CLI de AWS, escriba el siguiente comando:

```
1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-block 10.10.10.0/24 --gateway-id <eni-client-primary>
```

Desde la GUI de AWS, lleve a cabo los siguientes pasos para agregar una ruta:

1. Abra la [consola de Amazon EC2](#).
2. En el panel de navegación, elija **Tablas de redirección** y seleccione la tabla de redirección.
3. Seleccione **Acciones** y haga clic en **Modificar rutas**.
4. Para agregar una ruta, elige **Agregar ruta**. En **Destino**, introduzca el bloque CIDR de destino, una única dirección IP o el ID de una lista de prefijos. Para ID de puerta de enlace, seleccione el ENI de una interfaz de cliente del nodo principal.

Destination	Target
192.168.0.0/16	local
0.0.0.0/0	igw-0b6da15e72de5729e
10.10.10.0/24	eni-09ad18f01f854b8ab
5.5.0.0/16	eni-09ad18f01f854b8ab

Nota:
Debe inhabilitar la **comprobación de origen/destino** en el ENI del cliente de la instancia principal.

Para inhabilitar la comprobación de origen/destino de una interfaz de red mediante la consola, realice los siguientes pasos:

1. Abra la [consola de Amazon EC2](#).
2. En el panel de navegación, elija **Interfaces de red**.
3. Seleccione la interfaz de red de una interfaz de cliente principal, elija **Acciones** y haga clic en **Cambiar fuente/destino. Comprobar**.
4. En el cuadro de diálogo, seleccione **Inhabilitado** y haga clic en **Guardar**.

Change Source/Dest. Check ✕

Network Interface eni-0047841c06c3e9012

Source/dest. check Enabled
 Disabled

Cancel Save

Paso 5. Configurar alta disponibilidad. Puede utilizar la CLI o la GUI de NetScaler VPX para configurar la alta disponibilidad.

Configurar la alta disponibilidad mediante la CLI

1. Configure la alta disponibilidad en modo INC en ambas instancias.

En el nodo principal:

```
1 add ha node 1 \<<sec\_ip\> -inc ENABLED
```

En el nodo secundario:

```
1 add ha node 1 \<<prim\_ip\> -inc ENABLED
```

<sec_ip>hace referencia a la dirección IP privada de la NIC de administración del nodo secundario.

<prim_ip>hace referencia a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un servidor virtual en la instancia principal. Debe agregarlo desde la subred elegida, por ejemplo, 10.10.10.0/24.

Escriba este comando:

```
1 add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
    primary\_vip\> \<port\>
```

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

1. Configurar la alta disponibilidad en modo INC en ambas instancias
2. Inicie sesión en el nodo principal con el nombre de usuario `nsroot` y el ID de instancia como contraseña.
3. Vaya a **Configuración > Sistema > Alta disponibilidad** y haga clic en **Agregar**.
4. En el campo **Dirección IP del nodo remoto**, agregue la dirección IP privada de la NIC de administración del nodo secundario.
5. Seleccione **Activar el modo NIC (Configuración de red independiente)** en el nodo propio.
6. En **Credencial de inicio de sesión en el sistema remoto**, agregue el nombre de usuario y la contraseña del nodo secundario y haga clic en **Crear**.
7. Repita los pasos en el nodo secundario.
8. Agregar un servidor virtual en la instancia principal

Vaya a **Configuración > Administración del tráfico > Servidores virtuales > Agregar**.

← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings			
Name	My LB	Listen Priority	-
Protocol	HTTP	Listen Policy Expression	NONE
State	UP	Redirection Mode	IP
IP Address	10.10.10.10	Range	1
Port	80	IPset	-
Traffic Domain	0	RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Retain Connections on Cluster	NO
		TCP Probe Port	-

Services and Service Groups	
1	Load Balancing Virtual Server Service Binding

Implemente un par de alta disponibilidad de VPX con direcciones IP privadas mediante la VPC compartida de AWS

En un modelo de VPC compartida de AWS, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes). Por lo tanto, tiene una cuenta de propietario de VPC y una cuenta de participante. Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar sus recursos de aplicación en las subredes compartidas con ellos. Los

participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC.

Para obtener información sobre la VPC compartida de AWS, consulte la [documentación de AWS](#).

Nota:

Los pasos de configuración para implementar un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC compartida de AWS son los mismos que para implementar un par de alta disponibilidad de VPX con direcciones IP privadas mediante una VPC no compartida de AWS, con la siguiente excepción:

- Las tablas de rutas de la VPC que apuntan a la interfaz del cliente deben agregarse desde la *cuenta del propietario de la VPC*.

Requisitos previos

- Asegúrese de que el rol de IAM asociado a la instancia de NetScaler VPX en la cuenta del participante de AWS tenga los siguientes permisos de IAM:

```

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             "ec2:ModifyNetworkInterfaceAttribute",
14             "ec2:AssociateAddress",
15             "sts:AssumeRole"
16         ],
17         "Resource": "*"
18     }
19 ]
20 ]
21 }
```

Nota:

AssumeRole permite a la instancia de NetScaler VPX asumir la función de IAM multicuenta, que crea la cuenta del propietario de la VPC.

- Asegúrese de que la cuenta del propietario de la VPC proporcione los siguientes permisos de IAM a la cuenta del participante mediante la función de IAM multicuenta:

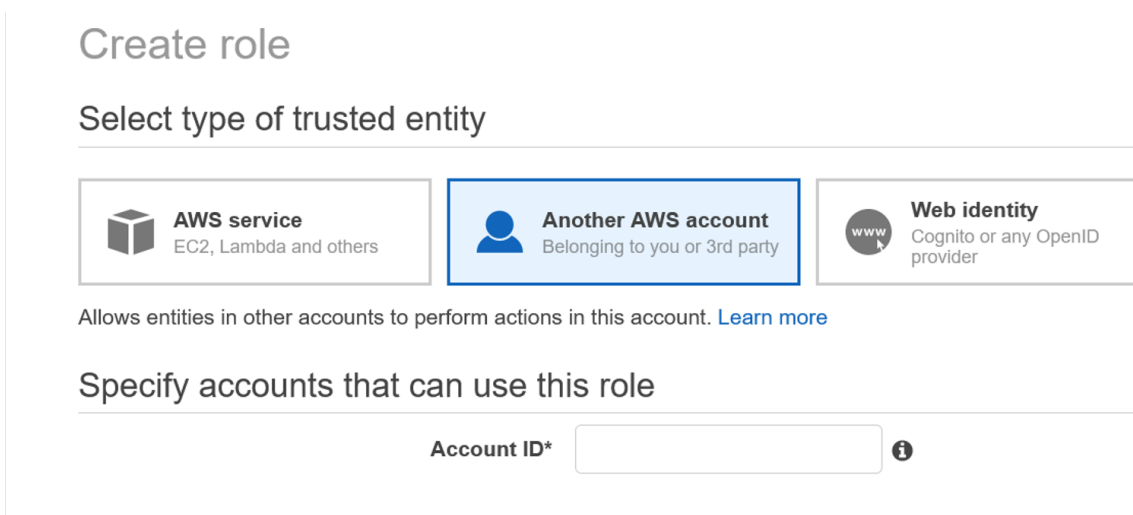
```

1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Sid": "VisualEditor0",
8              "Effect": "Allow",
9              "Action": [
10                 "ec2:CreateRoute",
11                 "ec2:DeleteRoute",
12                 "ec2:DescribeRouteTables"
13             ],
14             "Resource": "*"
15         }
16     ]
17 }
18

```

Crear función de IAM multicuenta

1. Inicie sesión en la consola web de AWS.
2. En la ficha **IAM**, vaya a **Roles** y, a continuación, elija **Create Role**.
3. Elija **otra cuenta de AWS**.



4. Introduzca el número de identificación de cuenta de 12 dígitos de la cuenta de participante a la que quiere conceder acceso de administrador.

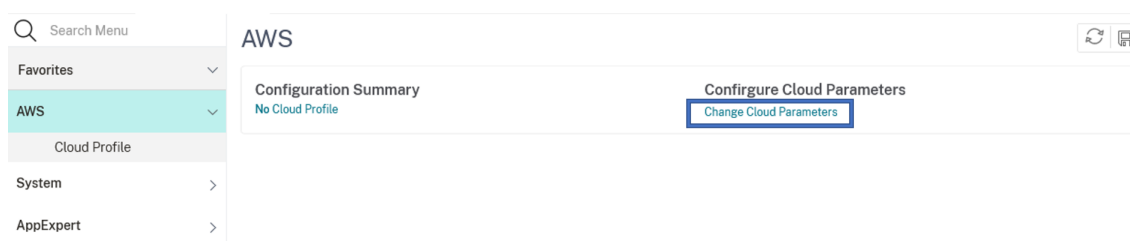
Establecer la función de IAM multicuenta mediante la CLI de NetScaler

El siguiente comando permite que la instancia NetScaler VPX asuma la función de IAM multicuenta que existe en la cuenta del propietario de la VPC.

```
1 set cloud awsParam -roleARN <string>
```

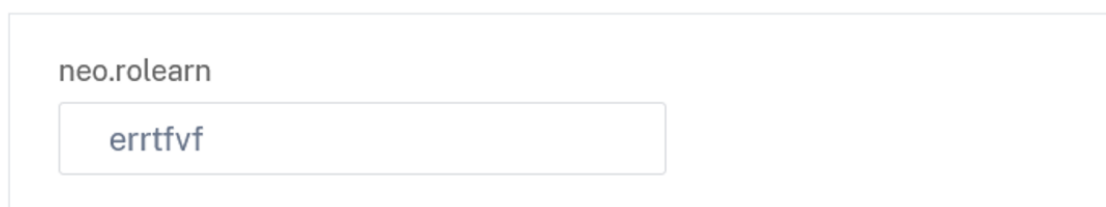
Establecer la función de IAM multicuenta mediante la GUI de NetScaler

1. Inicie sesión en el dispositivo NetScaler y vaya a **Configuración > AWS > Cambiar parámetros de la nube**.



2. En la página **Configurar parámetros de la nube de AWS**, introduzca el valor del campo **RoLearn**.

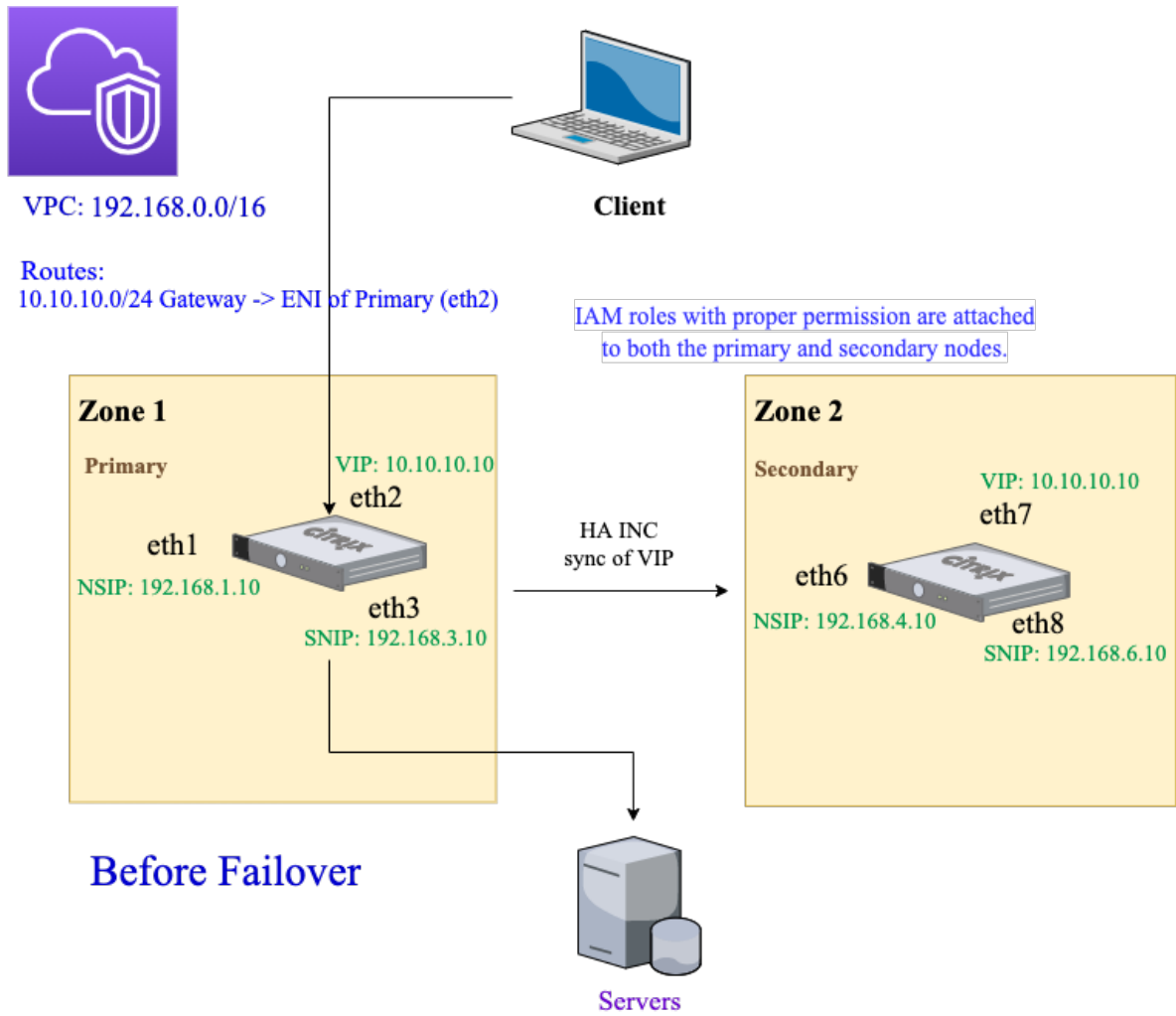
← Configure AWS Cloud Parameters

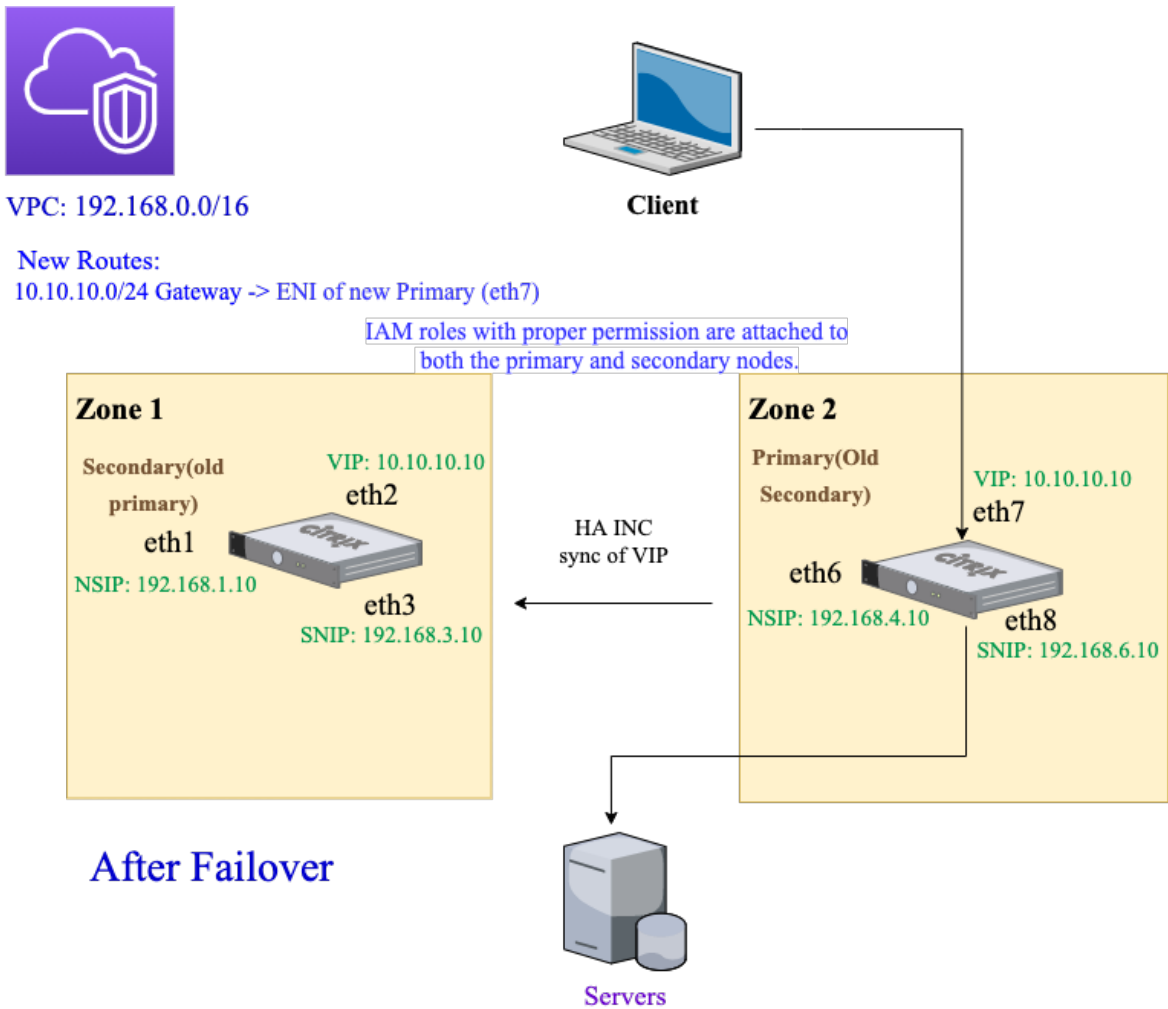


Caso

En este caso, se crea una única VPC. En esa VPC, se crean dos instancias VPX en dos zonas de disponibilidad. Cada instancia tiene tres subredes: una para administración, otra para el cliente y otra para el servidor back-end.

Los diagramas siguientes ilustran la configuración de alta disponibilidad de NetScaler VPX en modo INC, en AWS. La subred personalizada 10.10.10.10, que no forma parte de la VPC, se utiliza como VIP. Por lo tanto, la subred 10.10.10.10 se puede utilizar en todas las zonas de disponibilidad.





En este caso, utilice la CLI para configurar la alta disponibilidad.

1. Configure la alta disponibilidad en modo INC en ambas instancias.

Escriba los siguientes comandos en los nodos primario y secundario.

En el nodo principal:

```
1 add ha node 1 192.168.4.10 -inc enabled
```

En este caso, 192.168.4.10 se refiere a la dirección IP privada de la NIC de administración del nodo secundario.

En el nodo secundario:

```
1 add ha node 1 192.168.1.10 -inc enabled
```

En este caso, 192.168.1.10 se refiere a la dirección IP privada de la NIC de administración del nodo principal.

2. Agregue un servidor virtual en la instancia principal.

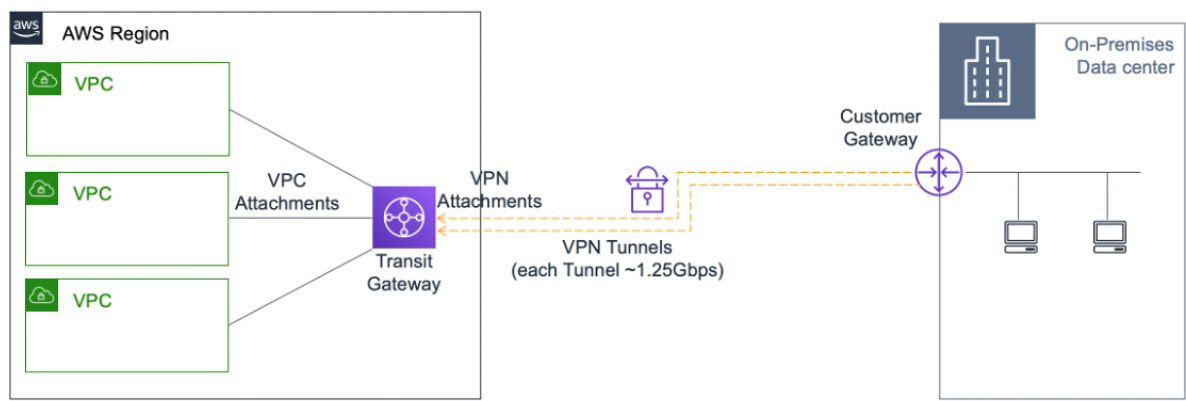
Escriba este comando:

```
1 add lbvserver vserver1 http 10.10.10.10 80
```

3. Verifique la configuración.
4. Tras una conmutación por error forzada:
 - La instancia secundaria se convierte en la nueva instancia principal.
 - La ruta de la VPC que apunta al ENI principal migra al ENI del cliente secundario.
 - El tráfico del cliente se reanuda en la nueva instancia principal.

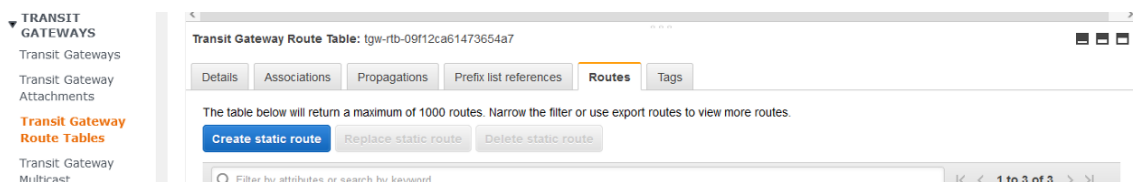
Configuración de AWS Transit Gateway para solución IP privada de alta disponibilidad

Necesita AWS Transit Gateway para que la subred VIP privada se pueda redirigir dentro de la red interna, en las VPC de AWS, regiones y redes locales. La VPC debe conectarse a AWS Transit Gateway. Se crea una ruta estática para la subred VIP o el grupo de IP dentro de la tabla de rutas de AWS Transit Gateway y se dirige hacia la VPC.



Para configurar AWS Transit Gateway, siga estos pasos:

1. Abra la [consola de Amazon VPC](#).
2. En el panel de navegación, elija **Tablas de rutas de Transit Gateway**.
3. Seleccione la ficha **Rutas** y haga clic en **Crear ruta estática**.



4. Cree una ruta estática en la que CIDR apunte a su subred VIPS privada y apunte a la VPC que tiene 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*

Blackhole

Choose attachment

* Required

Cancel [Create static route](#)

5. Haga clic en **Crear ruta estática** y selecciona **Cerrar**.

Solución de problemas

Si tiene algún problema al configurar la solución IP privada de alta disponibilidad en una HA multi-zona, compruebe los siguientes puntos clave para solucionar problemas:

- Tanto el nodo principal como el secundario tienen el mismo conjunto de permisos de IAM.
- El modo INC está activado tanto en el nodo principal como en el secundario.
- Tanto los nodos primarios como los secundarios tienen el mismo número de interfaces.
- Al crear una instancia, sigue la misma secuencia de conexión de interfaces en los nodos principal y secundario según el número de índice del dispositivo. Supongamos que en un nodo principal, la interfaz de cliente se conecta primero y la interfaz de servidor se conecta en segundo lugar. Siga también la misma secuencia en el nodo secundario. Si hay alguna discrepancia, separe y vuelva a conectar las interfaces en el orden correcto.
- Puede verificar la secuencia de interfaces siguiendo esta ruta de navegación: **consola de AWS > Red y seguridad > ENI > Número de índice de dispositivos**. De forma predeterminada, se asignan los siguientes números de índice de dispositivo a estas interfaces: - Interfaz de administración —0 - Interfaz de cliente —1 - Interfaz de servidor —2
 - Interfaz de gestión —0
 - Interfaz de cliente —1
 - Interfaz del servidor —2
- Si la secuencia de números de índice del dispositivo en el ENI principal es: 0, 1, 2. El ENI secundario también debe seguir la misma secuencia de números de índice del dispositivo: 0, 1, 2.

Si hay una discrepancia en la secuencia de números de índice del dispositivo, todas las rutas no coincidentes se transfieren al índice 0, la interfaz de administración, para evitar la pérdida

de rutas. Sin embargo, aún debe separar las interfaces y volver a conectarlas en la secuencia correcta para evitar el movimiento de las rutas hacia la interfaz de administración, ya que puede provocar congestión de tráfico.

- Si el tráfico no fluye, asegúrese de seleccionar “Fuente/destino”. La opción “Comprobar” está inhabilitada en la interfaz de cliente del nodo principal por primera vez.
- Asegúrese de que el `cloudhadaemon` comando (`ps -aux | grep cloudha`) se esté ejecutando en Shell.
- Asegúrese de que la versión del firmware de NetScaler sea la 13.0 build 70.x o posterior.
- Para problemas con el proceso de conmutación por error, consulte el archivo de registro disponible en: `/var/log/cloud-ha-daemon.log`

Implementación de una instancia NetScaler VPX en AWS Outposts

October 17, 2024

AWS Outposts es un conjunto de prestaciones informáticas y de almacenamiento de AWS implementadas en su sitio. Outposts proporciona la infraestructura y los servicios de AWS en su ubicación local. AWS opera, supervisa y administra esta prestación como parte de una región de AWS. Puede utilizar las mismas instancias, API de AWS, herramientas e infraestructura de NetScaler VPX en las instalaciones y en la nube de AWS para disfrutar de una experiencia híbrida uniforme.

Puede crear subredes en Outposts y especificarlas al crear recursos de AWS, como instancias EC2, volúmenes de EBS, clústeres de ECS e instancias de RDS. Las instancias de las subredes Outposts se comunican con otras instancias de la región de AWS mediante direcciones IP privadas, todas dentro de la misma Amazon Virtual Private Cloud (VPC).

Para obtener más información, consulte la [guía del usuario de AWS Outposts](#).

Cómo funciona AWS Outposts

AWS Outposts está diseñado para funcionar con una conexión constante y coherente entre Outposts y una región de AWS. Para lograr esta conexión con la región y con las cargas de trabajo locales de su entorno local, debe conectar Outpost a su red local. Su red local debe proporcionar acceso WAN a la región e Internet. Internet también debe proporcionar acceso mediante LAN o WAN a la red local en la que residen las cargas de trabajo o aplicaciones locales.

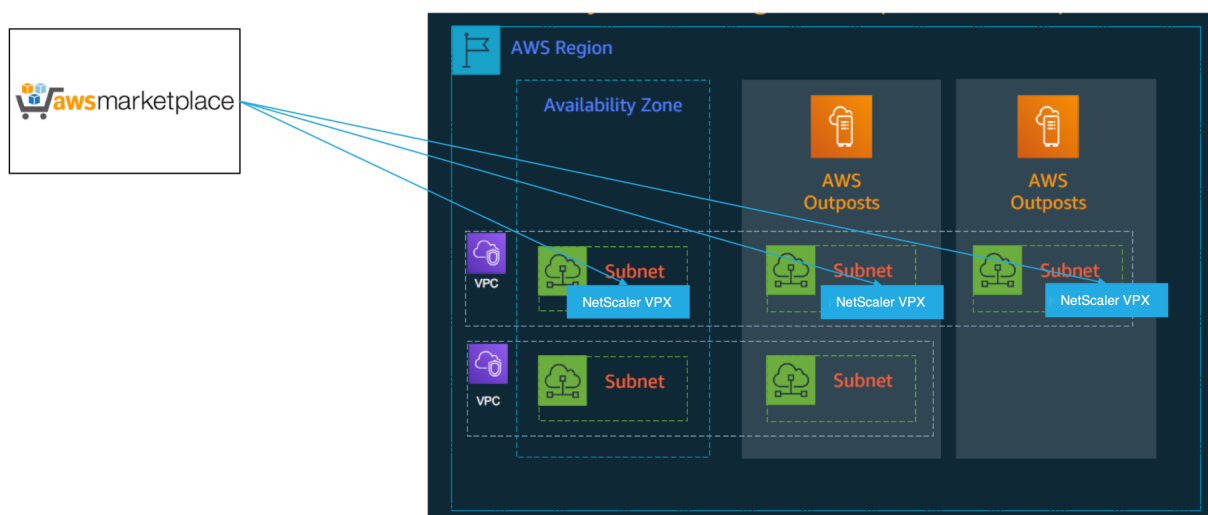
Requisito previo

- Debe instalar AWS Outposts en su sitio.
- La capacidad de procesamiento y almacenamiento de AWS Outposts debe estar disponible para su uso.

Para obtener más información sobre cómo realizar un pedido de AWS Outposts, consulte la siguiente documentación de AWS: <https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/>

Implementar una instancia de NetScaler VPX en AWS Outposts mediante la consola web de AWS

En la siguiente ilustración se muestra una implementación sencilla de instancias de NetScaler VPX en Outposts. La AMI de NetScaler presente en AWS Marketplace también se implementa en Outposts.



Inicie sesión en la consola web de AWS y complete los siguientes pasos para implementar instancias EC2 de NetScaler VPX en sus AWS Outposts.

1. Crea un par de claves.
2. Cree una nube privada virtual (VPC).
3. Agregue más subredes.
4. Cree grupos de seguridad y reglas de seguridad.
5. Agregue tablas de rutas.
6. Cree una puerta de enlace a Internet.
7. Cree una instancia de NetScaler VPX mediante el servicio AWS EC2. Desde el panel de AWS, vaya a **Compute > EC2 > Launch Instance > AWS Marketplace**.
8. Cree y conecte más interfaces de red.
9. Conecte IP elásticas a la NIC de administración.

10. Conéctese a la instancia de VPX.

Para obtener instrucciones detalladas sobre cada uno de los pasos, consulte [Implementar una instancia de NetScaler VPX en AWS mediante la consola web de AWS](#).

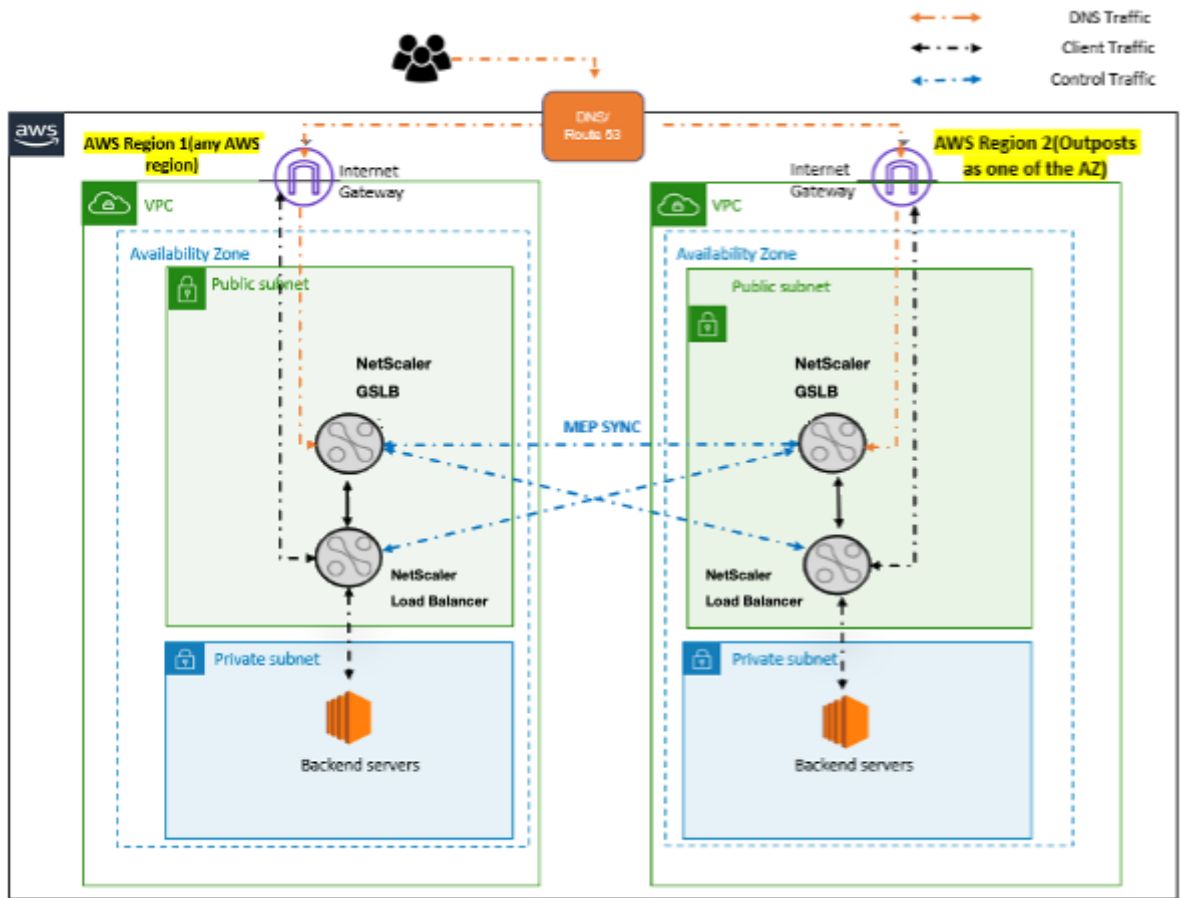
Para una alta disponibilidad dentro de la misma implementación de zona de disponibilidad, consulte [Implementar un par de alta disponibilidad en AWS](#).

Implementar una instancia de NetScaler VPX en la nube híbrida con AWS Outposts

Puede implementar una instancia de NetScaler VPX en una nube híbrida en un entorno de AWS que contenga puestos de avanzada de AWS. Puede simplificar el mecanismo de entrega de aplicaciones mediante la solución de equilibrio de carga de servidores global (GSLB) de NetScaler. La solución GSLB distribuye el tráfico de aplicaciones entre varios centros de datos en nubes híbridas que se crean utilizando las regiones de AWS y la infraestructura de AWS Outposts.

NetScaler GSLB admite los tipos de implementación activa-activa y activa-pasiva para abordar diferentes casos de uso. Junto con estas opciones de implementación flexibles y mecanismos de entrega de aplicaciones, NetScaler protege toda la cartera de redes y aplicaciones, independientemente de si las aplicaciones se implementan de forma nativa en AWS Cloud o en AWS Outposts.

El siguiente diagrama ilustra la entrega de una aplicación con un dispositivo NetScaler en una nube híbrida con AWS.



En una implementación activa-activa, NetScaler dirige el tráfico a nivel mundial a través de un entorno distribuido. Todos los sitios del entorno intercambian métricas sobre la disponibilidad y el estado de los recursos a través del Protocolo de intercambio de métricas (MEP). El dispositivo NetScaler utiliza esta información para equilibrar la carga del tráfico entre los sitios y envía las solicitudes de los clientes al sitio GSLB más adecuado según lo determine el método definido (ronda por turnos, conexión mínima y proximidad estática) especificado en la configuración de GSLB.

Puede utilizar la implementación activa y activa de GSLB para:

- Optimizar la utilización de los recursos con todos los nodos activos.
- Mejorar la experiencia del usuario dirigiendo las solicitudes al sitio más cercano a cada usuario individual.
- Migrar las aplicaciones a la nube a un ritmo definido por el usuario.

Puede utilizar la implementación de GSLB activa-pasiva para:

- Recuperación ante desastres
- Ampliación en la nube

Referencias

- [Implementar una instancia de NetScaler VPX en AWS](#)
- [Implementar una instancia de NetScaler VPX en AWS Outposts mediante la consola web de AWS](#)
- [Configurar GSLB en instancias de NetScaler VPX](#)

Proteja AWS API Gateway mediante el Web App Firewall NetScaler

October 17, 2024

Puede implementar un dispositivo NetScaler en frente de su AWS API Gateway y proteger la puerta de enlace de API de amenazas externas. NetScaler Web App Firewall (WAF) puede defender su API contra las 10 principales amenazas y los ataques de día cero de OWASP. NetScaler Web App Firewall utiliza una única base de código en todos los formatos de ADC. Por lo tanto, puede aplicar y aplicar directivas de seguridad de manera consistente en cualquier entorno. El NetScaler Web App Firewall es fácil de implementar y está disponible como una licencia única. El Web App Firewall de NetScaler le ofrece las siguientes funciones:

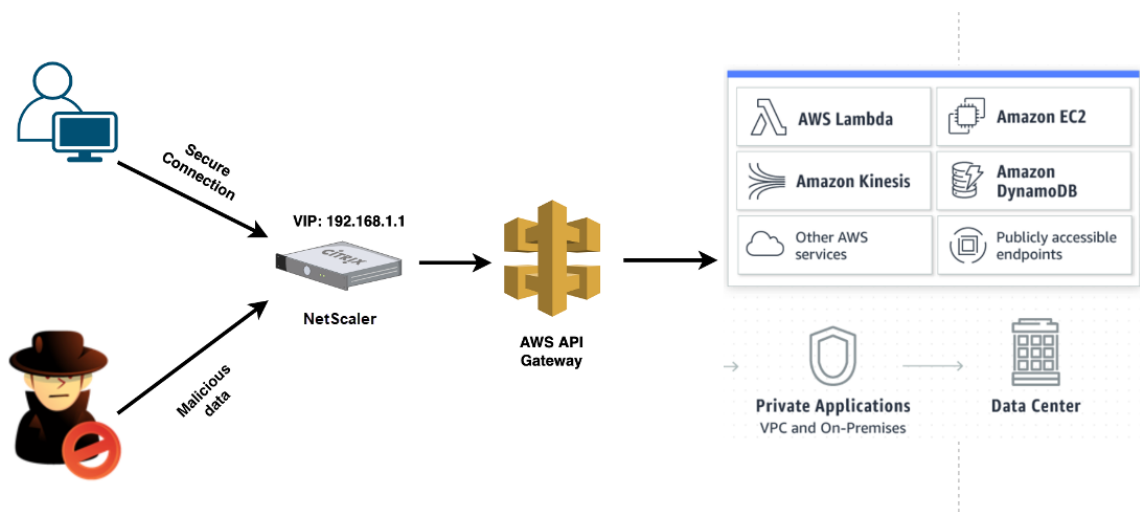
- Configuración simplificada
- Administración de bots
- Visibilidad integral
- Recopilar datos de varias fuentes y mostrar los datos en una pantalla unificada

Además de la protección de puerta de enlace de API, también puede usar las demás funciones de NetScaler. Para obtener más información, consulte la [documentación de NetScaler](#). Además de evitar las conmutaciones por error del centro de datos y minimizar el tiempo de apagado, puede colocar ADC en alta disponibilidad dentro o entre las zonas de disponibilidad. También puede usar o configurar la agrupación en clústeres con la función Autoscale.

Anteriormente, AWS API Gateway no admitía las protecciones necesarias para proteger las aplicaciones detrás de él. Sin las protecciones de firewall de aplicaciones web (WAF), las API eran propensas a las amenazas de seguridad.

Implementar el dispositivo NetScaler frente a la puerta de enlace de API de AWS

En el siguiente ejemplo, se implementa un dispositivo NetScaler frente a la puerta de enlace de la API de AWS.



Supongamos que hay una solicitud de API genuina para el servicio de AWS Lambda. Esta solicitud puede ser para cualquiera de los servicios de API, como se menciona en la [documentación de Amazon API Gateway](#). Como se muestra en el diagrama anterior, el flujo de tráfico es el siguiente:

1. El cliente envía una solicitud a la función AWS Lambda (XYZ). Esta solicitud de cliente se envía al servidor virtual NetScaler (192.168.1.1).
2. El servidor virtual inspecciona el paquete y comprueba si hay contenido malicioso.
3. El dispositivo NetScaler desencadena una directiva de reescritura para cambiar el nombre de host y la URL en una solicitud de cliente. Por ejemplo, quiere cambiar `https://restapi.citrix.com/default/LambdaFunctionXYZ` a `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ`.
4. El dispositivo NetScaler reenvía esta solicitud a la puerta de enlace de la API de AWS.
5. AWS API Gateway envía la solicitud al servicio de Lambda y llama a la función de Lambda “XYZ”.
6. Al mismo tiempo, si un atacante envía una solicitud de API con contenido malicioso, la solicitud maliciosa llega al dispositivo NetScaler.
7. El dispositivo NetScaler inspecciona los paquetes y los descarta en función de la acción configurada.

Configurar el dispositivo NetScaler con WAF habilitado

Para habilitar WAF en un dispositivo NetScaler, lleve a cabo los siguientes pasos:

1. Agregue un servidor virtual de conmutación de contenido o equilibrio de carga. Supongamos que la dirección IP del servidor virtual es 192.168.1.1, que se resuelve en un nombre de dominio (restapi.citrix.com).
2. Habilite la directiva WAF en el servidor virtual NetScaler. Para obtener más información, consulte [Configuración de Web App Firewall](#).

- Habilite la directiva de reescritura para cambiar el nombre de dominio. Supongamos que quiere cambiar la solicitud entrante a un equilibrador de carga en el nombre de dominio “restapi.citrix.com” para que se vuelva a escribir en la puerta de enlace de la API de AWS de back-end en “citrix.execute-api.<region>.amazonaws”.
- Habilite el modo L3 en el dispositivo NetScaler para que actúe como proxy. Utilice el siguiente comando:

```
1 enable ns mode L3
```

En el paso 3 del ejemplo anterior, supongamos que el administrador del sitio web quiere que el dispositivo NetScaler reemplace el nombre de dominio “restapi.citrix.com” por “citrix.execute-api.<region>.amazonaws.com” y la URL con “Default/Lambda/xyz”.

El siguiente procedimiento describe cómo cambiar el nombre de host y la URL en una solicitud de cliente mediante la función de reescritura:

- Inicie sesión en el dispositivo NetScaler mediante SSH.
- Agregue acciones de reescritura.

```
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\""
```

- Agregue directivas de reescritura para las acciones de reescritura.

```
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
```

- Enlazar las directivas de reescritura a un servidor virtual.

```
1 bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol
  -priority 10 -gotoPriorityExpression 20 -type REQUEST
2
3 bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
  priority 20 -gotoPriorityExpression END -type REQUEST
```

Para obtener más información, consulte [Configurar la reescritura para cambiar el nombre de host y la URL en la solicitud del cliente en el dispositivo NetScaler](#).

Características y capacidades de NetScaler

El dispositivo NetScaler, además de proteger la implementación, también puede mejorar la solicitud en función de los requisitos del usuario. El dispositivo NetScaler proporciona las siguientes funciones clave.

- **Equilibrar la puerta de enlace de API:** Si tiene más de una puerta de enlace de API, puede equilibrar la carga de varias puertas de enlace de API mediante el dispositivo NetScaler y definir el comportamiento de la solicitud de API.
 - Hay diferentes métodos de equilibrio de carga disponibles. Por ejemplo, el método de conexión mínima evita la sobrecarga del límite de API Gateway, el método de carga personalizada mantiene una carga específica en una puerta de enlace de API en particular, etc. Para obtener más información, consulte [Algoritmos de equilibrio de carga](#).
 - La descarga SSL se configura sin interrumpir el tráfico.
 - El modo Usar IP de origen (USIP) está habilitado para conservar la dirección IP del cliente.
 - Configuración SSL definida por el usuario: puede tener su propio servidor virtual SSL con sus propios certificados y algoritmos firmados.
 - Servidor virtual de respaldo: si no se puede acceder a la puerta de enlace de la API, puede enviar la solicitud a un servidor virtual de respaldo para realizar acciones adicionales.
 - Hay disponibles muchas otras funciones de equilibrio de carga. Para obtener más información, consulte [Equilibrio de carga del tráfico en un dispositivo NetScaler](#).
- **Autenticación, autorización y auditoría:** puede definir sus propios métodos de autenticación, como LDAP, SAML, RADIUS, y autorizar y auditar las solicitudes de API.
- **Respondedor:** puede redirigir las solicitudes de API a otra puerta de enlace de API durante el tiempo de cierre.
- **Limitación de velocidad:** puede configurar la función de limitación de velocidad para evitar la sobrecarga de una puerta de enlace de API.
- **Mejor disponibilidad:** puede configurar un dispositivo NetScaler en una configuración de alta disponibilidad o en una configuración de clúster para brindar una mejor disponibilidad a sus tráficos de API de AWS.
- **API REST:** admite la API REST, que se puede utilizar para automatizar el trabajo en entornos de producción en la nube.
- **Supervisar datos:** supervisa y registra los datos como referencia.

El dispositivo NetScaler proporciona muchas más funciones, que se pueden integrar con la puerta de enlace de la API de AWS. Para obtener más información, consulte la [documentación de NetScaler](#).

Agregar el servicio AWS Autoscaling de back-end

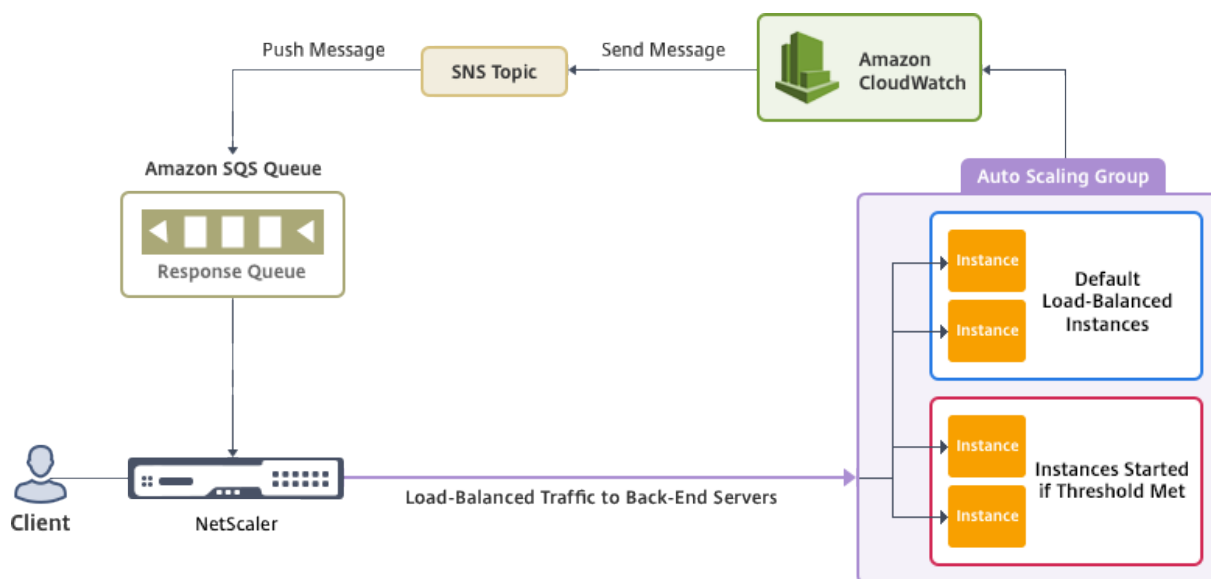
October 17, 2024

El alojamiento eficiente de aplicaciones en una nube implica una gestión fácil y rentable de los recursos en función de la demanda de la aplicación. Para satisfacer la creciente demanda, debe ampliar los recursos de la red. Cuando la demanda disminuye, es necesario reducir la escala para evitar el costo innecesario de los recursos inactivos. Puede minimizar el costo de ejecución de las aplicaciones implementando solo tantas instancias como sean necesarias durante un tiempo determinado. Para lograrlo, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, etc. Sin embargo, la supervisión manual del tráfico es engorrosa. Para que el entorno de aplicaciones se escale hacia arriba o hacia abajo de forma dinámica, debe automatizar los procesos de supervisión del tráfico y escalar los recursos hacia arriba y hacia abajo siempre que sea necesario.

Integrada con el servicio AWS Auto Scaling, la instancia NetScaler VPX ofrece las siguientes ventajas:

- **Equilibrio y administración** de la carga : configura automáticamente los servidores para ampliarlos o reducirlos, según la demanda. La instancia VPX detecta automáticamente los grupos de Autoscale en la subred de fondo y permite al usuario seleccionar los grupos de Autoscale para equilibrar la carga. Todo esto se hace configurando automáticamente las direcciones IP virtuales y de subred en la instancia VPX.
- **Alta disponibilidad**: detecta grupos de escalabilidad automática que abarcan varias zonas de disponibilidad y servidores de equilibrio de carga.
- **Mejor disponibilidad de red**: la instancia VPX admite:
 - Servidores de fondo en diferentes VPC, mediante el emparejamiento de VPC
 - Servidores back-end en los mismos grupos de ubicación
 - Servidores de fondo en diferentes zonas de disponibilidad
- **Terminación correcta de la conexión: elimina los servidores de escalado automático sin problemas y evita la pérdida de conexiones de los clientes cuando se produce una actividad de reducción de escala, mediante la función GracefulTimeout.**
- **Drenaje de conexión para los servidores en espera**: evita el envío de nuevas conexiones de cliente al servidor en estado de espera. Sin embargo, los servidores en espera siguen formando parte del grupo de escalado automático y seguirán gestionando las conexiones de cliente existentes hasta que se cierran. Cuando el servidor vuelve al estado InService, el servidor vuelve a gestionar las nuevas conexiones. Puede usar el estado de espera para actualizar, modificar o solucionar problemas de los servidores, o para reducirlo en función de las necesidades. Para obtener más información, consulte la [documentación de AWS](#).

Diagrama: Servicio de escalado automático de AWS con una instancia de NetScaler VPX



Este diagrama ilustra cómo el servicio AWS Autoscaling es compatible con una instancia de NetScaler VPX (servidor virtual de equilibrio de carga). Para obtener más información, consulte los siguientes temas de AWS.

- [Grupos de ajuste de escala automático](#)
- [CloudWatch](#)
- [Servicio de notificación simple \(SNS\)](#)
- [Servicio de cola simple \(Amazon SQS\)](#)

Antes de comenzar

Antes de empezar a utilizar AutoScaling con su instancia de NetScaler VPX, debe completar las siguientes tareas.

- Lea los siguientes temas:
 - [Requisitos previos](#)
 - [Pautas de limitación y uso](#)
- Cree una instancia de NetScaler VPX en AWS según sus requisitos.
 - Para obtener más información sobre cómo crear una instancia independiente de NetScaler VPX, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#) y [Escenario: instancia independiente](#)
 - Para obtener más información sobre cómo implementar instancias VPX en modo HA, consulte [Implementar un par de alta disponibilidad en AWS](#).

Nota:

Recomendamos lo siguiente:

- Utilice la plantilla de CloudFormation para crear instancias de NetScaler VPX en AWS.
- Cree tres interfaces independientes: una para la administración (NSIP), otra para el servidor virtual LB (VIP) orientado al cliente y otra para la IP de subred (NSIP).

- Cree un grupo de AWS Autoscale. Si no tiene una configuración de ajuste de escala automático existente, debe:

1. Crear una configuración de lanzamiento
2. Crear un grupo de escalado automático
3. Verificar el grupo de escalado automático

Para obtener más información, consulte <http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html>.

- A partir de la versión 14.1-12.x de NetScaler, en un grupo de AWS Autoscale, debe especificar una directiva de escalado descendente solo si ha habilitado la opción Graceful. En las versiones de NetScaler anteriores a 14.1-12.x, era necesario especificar al menos una política de reducción de escala independientemente de si la opción Graceful estaba habilitada o no.

La instancia de NetScaler VPX solo admite la directiva de escalado por pasos. La directiva de escalado simple y la directiva de escalado de seguimiento de objetivos no son compatibles con el grupo Autoscale.

- Asegúrese de que su cuenta de AWS tenga los siguientes permisos de IAM:

```
1   {
2
3     "Version": "2012-10-17",
4     "Statement": \[
5       {
6
7         "Action": \[
8           "ec2:DescribeInstances",
9           "ec2:DescribeNetworkInterfaces",
10          "ec2:DetachNetworkInterface",
11          "ec2:AttachNetworkInterface",
12          "ec2:StartInstances",
13          "ec2:StopInstances",
14          "ec2:RebootInstances",
15          "autoscaling:*",
16          "sns:*",
17          "sqs:*"
18
19          "iam: SimulatePrincipalPolicy "
20          "iam: GetRole "
```

```

21         \],
22         "Resource": "\*",
23         "Effect": "Allow"
24     }
25
26     \]
27 }

```

Agregue el servicio AWS Autoscaling a una instancia de NetScaler VPX

Complete los siguientes pasos para agregar el servicio de escalado automático a una instancia VPX:

1. Inicie sesión en la instancia VPX con sus credenciales de `nsroot`.
2. Vaya a **Sistema > AWS > Perfil de nube** y haga clic en **Agregar**.

Aparece la página **de configuración de Crear perfil en la nube**.

← Create Cloud Profile

The screenshot shows the 'Create Cloud Profile' configuration page. The form contains the following fields and values:

- Name: test-cloudprofile
- Virtual Server IP Address*: [Redacted]
- Load Balancing Server Protocol: HTTP
- Load Balancing Server Port: 80
- Auto Scale Group: test-script
- Auto Scale Group Protocol: HTTP
- Auto Scale Group Port: 80
- Graceful:
- Delay (Seconds): 60

At the bottom of the form, there are two buttons: 'Create' and 'Close'.

Puntos a tener en cuenta al crear un perfil de nube:

- La dirección IP del servidor virtual se rellena automáticamente a partir de la dirección IP gratuita disponible para la instancia VPX. Para obtener más información, consulte [Administrar varias direcciones IP](#).
- Escriba el nombre exacto del grupo de Autoscale que configuró en su cuenta de AWS. Para obtener más información, consulte los [grupos de AWS Auto Scaling](#).

- Al seleccionar el puerto y el protocolo del grupo de escalado automático, asegúrese de que los servidores escuchen esos protocolos y puertos y de vincular el monitor correcto al grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- En el caso del escalado automático del tipo de protocolo SSL, después de crear el perfil de nube, el servidor virtual o grupo de servicios de equilibrio de carga parece estar inactivo debido a la falta de un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.
- Seleccione **Graceful** y especifique un valor de tiempo de espera en el campo **Retraso** para eliminar los servidores de Autoscale sin problemas. Esta opción inicia un evento de reducción de escala. La instancia VPX no elimina el servidor inmediatamente, sino que marca uno de los servidores para eliminarlo correctamente. Durante este período, la instancia VPX no permite nuevas conexiones a este servidor. Las conexiones existentes se atienden hasta que se agote el tiempo de espera. Una vez transcurrido el tiempo de espera, la instancia VPX elimina el servidor.

Si no selecciona la opción **Graceful**, el servidor del grupo Autoscale se elimina inmediatamente después de que se detenga la carga. Esto podría provocar la interrupción del servicio para los clientes conectados existentes.

Después de crear el perfil de nube, se crean un servidor virtual de equilibrio de carga de NetScaler y un grupo de servicios con miembros como servidores del grupo de escalado automático. Los servidores back-end deben ser accesibles a través del SNIP configurado en la instancia VPX.

Nota:

- **Para ver la información relacionada con AutoScaling en la consola de AWS, vaya a EC2>Panel> Auto Scaling >Auto Scaling Group.****
- Puede crear diferentes perfiles de nube para diferentes servicios (utilizando diferentes puertos) con el mismo grupo de escalado automático (ASG) en AWS. Por lo tanto, la instancia de NetScaler VPX admite varios servicios con el mismo grupo de escalado automático en la nube pública.

Implemente NetScaler GSLB en AWS

October 17, 2024

La configuración de GSLB para NetScaler en AWS consiste básicamente en configurar NetScaler para equilibrar la carga del tráfico a los servidores ubicados fuera de la VPC a la que pertenece NetScaler, por ejemplo, dentro de otra VPC en una región de disponibilidad diferente o en un centro de datos local.



Descripción general de DBS

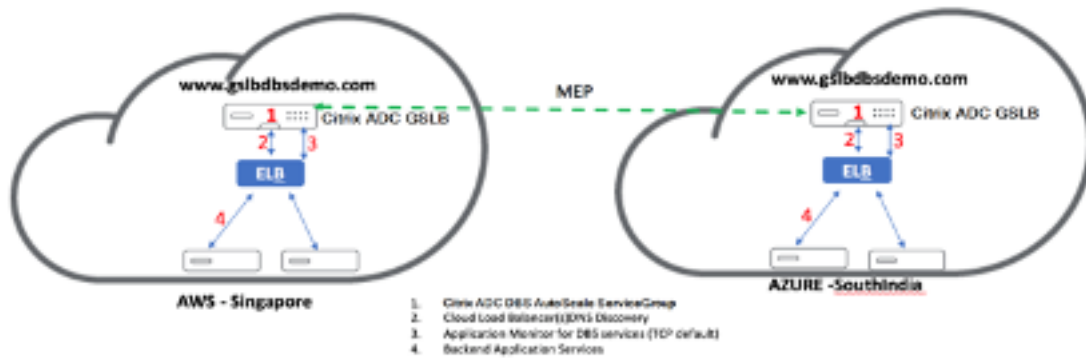
La compatibilidad de NetScaler GSLB con servicios basados en nombres de dominio (DBS) para balanceadores de carga en la nube permite el descubrimiento automático de servicios en la nube dinámicos mediante una solución de balanceador de carga en la nube. Esta configuración permite que NetScaler implemente servicios basados en nombres de dominio de equilibrio de carga de servidor global (GSLB DBS) en un entorno activo-activo. DBS permite escalar los recursos de back-end en entornos de AWS a partir del descubrimiento de DNS.

En esta sección se describen las integraciones entre NetScaler en entornos de AWS AutoScaling. La sección final del documento detalla la capacidad de configurar un par de ADC de NetScaler de alta disponibilidad que abarquen dos zonas de disponibilidad (AZ) diferentes específicas de una región de AWS.

DBS con ELB

GSLB DBS utiliza el FQDN del usuario Elastic Load Balancer (ELB) para actualizar dinámicamente los grupos de servicios de GSLB a fin de incluir los servidores back-end que se crean y eliminan en AWS. Los servidores o instancias back-end de AWS se pueden configurar para que escalen en función de la demanda de la red o la utilización de la CPU. Para configurar esta función, dirija NetScaler al ELB para enrutarlo dinámicamente a diferentes servidores de AWS sin tener que actualizar NetScaler manualmente cada vez que se cree y elimine una instancia en AWS. La función NetScaler DBS para grupos de servicios GSLB utiliza el descubrimiento de servicios con reconocimiento de DNS para determinar los recursos de servicio miembro del espacio de nombres DBS identificado en el grupo de escala automática.

Componentes de escalado automático de NetScaler GSLB DBS con balanceadores de carga en la nube:



Configurar los componentes de AWS

Grupos de seguridad

Nota:

Le recomendamos que cree diferentes grupos de seguridad para ELB, la instancia GSLB de NetScaler y la instancia de Linux, ya que el conjunto de reglas requerido para cada una de estas entidades es diferente. Este ejemplo tiene una configuración de grupo de seguridad consolidada para mayor brevedad.

Para garantizar la configuración adecuada del firewall virtual, consulte [Grupos de seguridad para su VPC](#).

1. Inicie sesión en el **grupo de recursos de AWS** del usuario y vaya a **EC2 > NETWORK & SECURITY > Security Groups**.

2. Haga clic en **Crear grupo de seguridad** y proporcione un nombre y una descripción. Este grupo de seguridad abarca los servidores web back-end de NetScaler y Linux.
3. Agregue las reglas de puertos de entrada de la siguiente captura de pantalla.

Nota:

Se recomienda limitar el acceso IP de origen para el endurecimiento granular. Para obtener más información, consulte [Reglas del servidor web](#).

1. Servicios web back-end de Amazon Linux

- a) Inicie sesión en el **grupo de recursos de AWS** del usuario y vaya a **EC2 > Instancias**.
- b) Haga clic en **Lanzar instancia** con los detalles que aparecen a continuación para configurar la instancia de **Amazon Linux**.

Ingrese los detalles sobre la configuración de un servidor web o un servicio back-end en esta instancia.

2. Configuración de NetScaler

- a) Inicie sesión en el **grupo de recursos de AWS** del usuario y vaya a **EC2 > Instancias**.
- b) Haga clic en **Launch Instance** y utilice los siguientes detalles para configurar la instancia de **Amazon AMI**.

3. Configuración de IP elástica

Nota:

También se puede hacer que NetScaler se ejecute con una sola IP elástica si es necesario para reducir los costes, al no tener una IP pública para el NSIP. En su lugar, adjunte una IP elástica al SNIP que pueda cubrir el acceso de administración a la caja, además de la IP del sitio GSLB y la IP de ADNS.

- 1 1. Inicie sesión en el **grupo de recursos de AWS** del usuario y vaya a **EC2 > RED Y SEGURIDAD > IP elásticas**.
- 2
- 3 1. Haga clic en **Asignar nueva dirección** para crear una dirección IP elástica.
- 4
- 5 1. Configure la IP elástica para que apunte al usuario que ejecuta la instancia de NetScaler en AWS.
- 6
- 7 1. Configure una segunda IP elástica y vuelva a dirigirla al usuario que ejecuta la instancia de NetScaler.

1. Equilibrador de carga elástico

a) Inicie sesión en el **grupo de recursos de AWS** del usuario y vaya a **EC2 > LOAD BALANCING > Load Balancers**.

b) Haga clic en **Crear equilibrador de carga** para configurar un equilibrador de carga clásico.

Los Elastic Load Balancers de usuario permiten a los usuarios equilibrar la carga de sus instancias de Amazon Linux de back-end y, al mismo tiempo, pueden equilibrar la carga de otras instancias que se ponen en marcha según la demanda.

Configuración de servicios basados en nombres de dominio de equilibrio de carga de servidores globales

Para configuraciones de administración de tráfico, consulte [Configurar el servicio basado en dominio GSLB de NetScaler](#).

Tipos de implementación

Implementación de tres NIC

- Despliegues típicos
 - Libro de estilo GSLB
 - Con ADM
 - Con GSLB (Route53 con registro de dominio)
 - Licencias - Pooled/Marketplace
- Casos de uso
 - Se utilizan implementaciones de tres NIC para lograr un aislamiento real del tráfico de datos y administración.
 - Las implementaciones de tres NIC también mejoran la escala y el rendimiento del ADC.
 - Las implementaciones de tres NIC se utilizan en aplicaciones de red donde el rendimiento suele ser de 1 Gbps o superior y se recomienda una implementación de tres NIC.

Despliegue de CFT

Los clientes implementarían el uso de plantillas de CloudFormation si están personalizando sus implementaciones o si están automatizando sus implementaciones.

Pasos de implementación

Los siguientes son los pasos de implementación:

1. Implementación de tres NIC para GSLB
2. Licensing
3. opciones de implementación

Implementación de tres NIC para GSLB La instancia de NetScaler VPX está disponible como Amazon Machine Image (AMI) en el mercado de AWS y se puede lanzar como una instancia de Elastic Compute Cloud (EC2) dentro de una VPC de AWS. El tipo mínimo de instancia EC2 permitido como AMI compatible en NetScaler VPX es m4.large. La instancia AMI de NetScaler VPX requiere un mínimo de 2 CPU virtuales y 2 GB de memoria. Una instancia EC2 lanzada dentro de una VPC de AWS también puede proporcionar las múltiples interfaces, varias direcciones IP por interfaz y direcciones IP públicas y privadas necesarias para la configuración VPX. Cada instancia VPX requiere al menos tres subredes IP:

- Una subred de administración
- Una subred (VIP) orientada al cliente
- Una subred orientada al back-end (SNIP)

NetScaler recomienda tres interfaces de red para una instalación de VPX estándar en AWS.

Actualmente, AWS hace que la funcionalidad de IP múltiple esté disponible solo para las instancias que se ejecutan en una VPC de AWS. Una instancia VPX en una VPC se puede utilizar para equilibrar la carga de servidores que se ejecutan en instancias EC2. Una red VPC de Amazon permite a los usuarios crear y controlar un entorno de red virtual, que incluye su propio intervalo de direcciones IP, subredes, tablas de redirección y puertas de enlace de red.

Nota:

De forma predeterminada, los usuarios pueden crear hasta 5 instancias de VPC por región de AWS para cada cuenta de AWS. Los usuarios pueden solicitar límites de VPC más altos enviando el formulario de solicitud de Amazon [aquí](#):

Licensing Una instancia de NetScaler VPX en AWS requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias de NetScaler VPX que se ejecutan en AWS:

- Gratis (ilimitado)
- Cada hora
- Anual
- Trae su propia licencia

- Prueba gratuita (todas las ofertas de suscripción a NetScaler VPX-AWS durante 21 días gratis en AWS Marketplace).

Opciones de implementación Los usuarios pueden implementar una instancia independiente de NetScaler VPX en AWS. Para obtener más información, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#)

Equilibrio de carga de servidores globales de NetScaler para implementaciones híbridas y multicloud

La solución de balanceo de cargas de servidores globales (GSLB) de NetScaler, híbrida y multinube, permite a los usuarios distribuir el tráfico de aplicaciones en varios centros de datos en nubes híbridas, nubes múltiples e implementaciones locales. La solución GSLB híbrida y multinube de NetScaler ayuda a los usuarios a gestionar su configuración de equilibrio de carga en entornos híbridos o multinube sin alterar la configuración existente. Además, si los usuarios tienen una configuración local, pueden probar algunos de sus servicios en la nube con la solución GSLB híbrida y multinube de NetScaler antes de migrar por completo a la nube. Por ejemplo, los usuarios solo pueden redirigir un pequeño porcentaje de su tráfico a la nube y gestionar la mayor parte del tráfico en las instalaciones. La solución GSLB híbrida y multinube de NetScaler también permite a los usuarios gestionar y supervisar las instancias de NetScaler en distintas ubicaciones geográficas desde una única consola unificada.

Una arquitectura híbrida y multinube también puede mejorar el rendimiento empresarial general al evitar la “dependencia del proveedor” y utilizar una infraestructura diferente para satisfacer las necesidades de los socios usuarios y los clientes. Con una arquitectura multicloud, los usuarios pueden administrar mejor sus costos de infraestructura ya que ahora tienen que pagar solo por lo que usan. Los usuarios también pueden escalar mejor sus aplicaciones, ya que ahora utilizan la infraestructura a pedido. También ofrece la posibilidad de cambiar rápidamente de una nube a otra para aprovechar las mejores ofertas de cada proveedor.

Los nodos GSLB de NetScaler manejan la resolución de nombres DNS. Cualquiera de estos nodos GSLB puede recibir solicitudes de DNS desde cualquier ubicación de cliente. El nodo GSLB que recibe la solicitud de DNS devuelve la dirección IP del servidor virtual del equilibrador de carga seleccionada por el método de equilibrio de carga configurado. Las métricas (métricas de sitio, red y persistencia) se intercambian entre los nodos GSLB mediante el protocolo de intercambio de métricas (MEP), que es un protocolo patentado de NetScaler. Para obtener más información sobre el protocolo MEP, consulte [Configurar el protocolo de intercambio de métricas](#).

El monitor configurado en el nodo GSLB monitorea el estado del servidor virtual de equilibrio de carga en el mismo centro de datos. En una topología padre-hijo, las métricas entre los nodos GSLB

y NetScaler se intercambian mediante MEP. Sin embargo, la configuración de las sondas de monitorización entre un nodo GSLB y un nodo NetScaler LB es opcional en una topología padre-hijo.

El agente NetScaler permite la comunicación entre NetScaler ADM y las instancias administradas en el centro de datos del usuario. Para obtener más información sobre los agentes de NetScaler y cómo instalarlos, consulte [Primeros pasos](#).

Nota:

En este documento se hacen las siguientes suposiciones:

- Si los usuarios tienen una configuración de equilibrio de carga existente, está en funcionamiento.
- Se configura una dirección SNIP o una dirección IP de sitio GSLB en cada nodo GSLB de NetScaler. Esta dirección IP se utiliza como dirección IP de origen del centro de datos al intercambiar métricas con otros centros de datos.
- Se configura un servicio ADNS o ADNS-TCP en cada una de las instancias GSLB de NetScaler para recibir el tráfico de DNS.
- El firewall y los grupos de seguridad necesarios se configuran en los proveedores de servicios en la nube.

Configuración de grupos de seguridad

Los usuarios deben configurar la configuración de grupos de firewall/seguridad requerida en los proveedores de servicios en la nube. Para obtener más información sobre las características de seguridad de AWS, consulte [AWS/Documentación/Amazon VPC/Guía del usuario/Seguridad](#).

Además, en el nodo GSLB, los usuarios deben abrir el puerto 53 para la dirección IP del servidor DNS y el servicio ADNS y el puerto 3009 para la dirección IP del sitio GSLB para el intercambio de tráfico MEP. En el nodo de equilibrio de carga, los usuarios deben abrir los puertos adecuados para recibir el tráfico de la aplicación. Por ejemplo, los usuarios deben abrir el puerto 80 para recibir tráfico HTTP y abrir el puerto 443 para recibir tráfico HTTPS. Abra el puerto 443 para la comunicación NITRO entre el agente NetScaler y NetScaler ADM.

Para el método GSLB dinámico de ida y vuelta, los usuarios deben abrir el puerto 53 para permitir las sondas UDP y TCP, según el tipo de sonda LDNS configurado. Las sondas UDP o TCP se inician con uno de los SNIP y, por lo tanto, esta configuración debe realizarse para los grupos de seguridad enlazados a la subred del lado del servidor.

Capacidades de la solución GSLB híbrida y multinube de NetScaler

En esta sección se describen algunas de las capacidades de la solución GSLB híbrida y multinube de NetScaler.

Compatibilidad con otras soluciones de equilibrio de carga

La solución GSLB híbrida y multinube de NetScaler es compatible con varias soluciones de equilibrio de carga, como NetScaler Load Balancer, NGINX, HAProxy y otros balanceadores de carga de terceros.

Nota:

Las soluciones de equilibrio de carga distintas de NetScaler solo se admiten si se utilizan métodos GSLB basados en la proximidad y no en métricas y si la topología padre-hijo no está configurada.

Métodos GSLB

La solución GSLB híbrida y multinube de NetScaler admite los siguientes métodos de GSLB.

- Métodos GSLB basados en métricas. Los métodos GSLB basados en métricas recopilan métricas de los demás nodos de NetScaler mediante el protocolo de intercambio de métricas.
 - Conexión mínima: la solicitud del cliente se redirige al equilibrador de carga que tiene el menor número de conexiones activas.
 - Ancho de banda mínimo: La solicitud del cliente se redirige al equilibrador de carga que actualmente está sirviendo la menor cantidad de tráfico.
 - Cantidad mínima de paquetes: la solicitud del cliente se envía al balanceador de cargas que ha recibido la menor cantidad de paquetes en los últimos 14 segundos.
- Métodos GSLB no métricos
 - Round Robin: la solicitud del cliente se envía a la dirección IP del balanceador de carga que se encuentra en la parte superior de la lista de balanceadores de carga. A continuación, ese balanceador de carga pasa al final de la lista.
 - Hash de IP de origen: este método utiliza el valor de hash de la dirección IP del cliente para seleccionar un balanceador de cargas.
- Métodos GSLB basados en la proximidad
 - Proximidad estática: La solicitud del cliente se redirige al equilibrador de carga más cercano a la dirección IP del cliente.

- Tiempo de ida y vuelta (RTT): este método utiliza el valor RTT (el tiempo de demora en la conexión entre el servidor DNS local del cliente y el centro de datos) para seleccionar la dirección IP del equilibrador de carga con mejor rendimiento.

Para obtener más información sobre los métodos de equilibrio de carga, consulte [Algoritmos de equilibrio de carga](#).

Topologías GSLB

La solución GSLB híbrida y multinube de NetScaler admite la topología activa-pasiva y la topología padre-hijo.

- Topología activa-pasiva: proporciona recuperación ante desastres y garantiza la disponibilidad continua de las aplicaciones al protegerlas contra los puntos de falla. Si el centro de datos principal falla, el centro de datos pasivo entra en funcionamiento. Para obtener más información sobre la topología activa-pasiva de GSLB, consulte [Configurar GSLB para recuperación ante desastres](#).
- Topología padre-hijo: se puede utilizar si los clientes utilizan los métodos GSLB basados en métricas para configurar GSLB y nodos de equilibrio de carga y si los nodos de equilibrio de carga están implementados en una instancia de NetScaler diferente. En una topología principal-secundaria, el nodo LB (sitio secundario) debe ser un dispositivo NetScaler porque el intercambio de métricas entre el sitio primario y el secundario se realiza a través del protocolo de intercambio de métricas (MEP).

Para obtener más información sobre la topología padre-hijo, consulte [Implementación de topología padre-hijo usando el protocolo MEP](#).

Compatibilidad con IPv6

La solución GSLB híbrida y multinube de NetScaler también admite IPv6.

Supervisión

La solución GSLB híbrida y multinube de NetScaler admite monitores integrados con la opción de habilitar la conexión segura. Sin embargo, si las configuraciones de LB y GSLB están en la misma instancia de NetScaler o si se usa la topología padre-hijo, la configuración de los monitores es opcional.

Persistencia

La solución GSLB híbrida y multinube de NetScaler admite lo siguiente:

- Sesiones de persistencia basadas en IP de origen, de modo que varias solicitudes del mismo cliente se dirijan al mismo servicio si llegan dentro de la ventana de tiempo de espera configurada. Si el valor de tiempo de espera expira antes de que el cliente envíe otra solicitud, la sesión se descarta y el algoritmo de equilibrio de carga configurado se utiliza para seleccionar un nuevo servidor para la siguiente solicitud del cliente.
- Persistencia de rebose para que el servidor virtual de copia de seguridad continúe procesando las solicitudes que recibe, incluso después de que la carga en el primario caiga por debajo del umbral. Para obtener más información, consulte [Configurar Spillover](#).
- Persistencia del sitio para que el nodo GSLB seleccione un centro de datos para procesar la solicitud de un cliente y reenvíe la dirección IP del centro de datos seleccionado para todas las solicitudes de DNS posteriores. Si la persistencia configurada se aplica a un sitio que está INACTIVO, el nodo GSLB utiliza un método GSLB para seleccionar un sitio nuevo y el nuevo sitio pasa a ser persistente para las solicitudes posteriores del cliente.

Configuración mediante NetScaler ADM StyleBooks

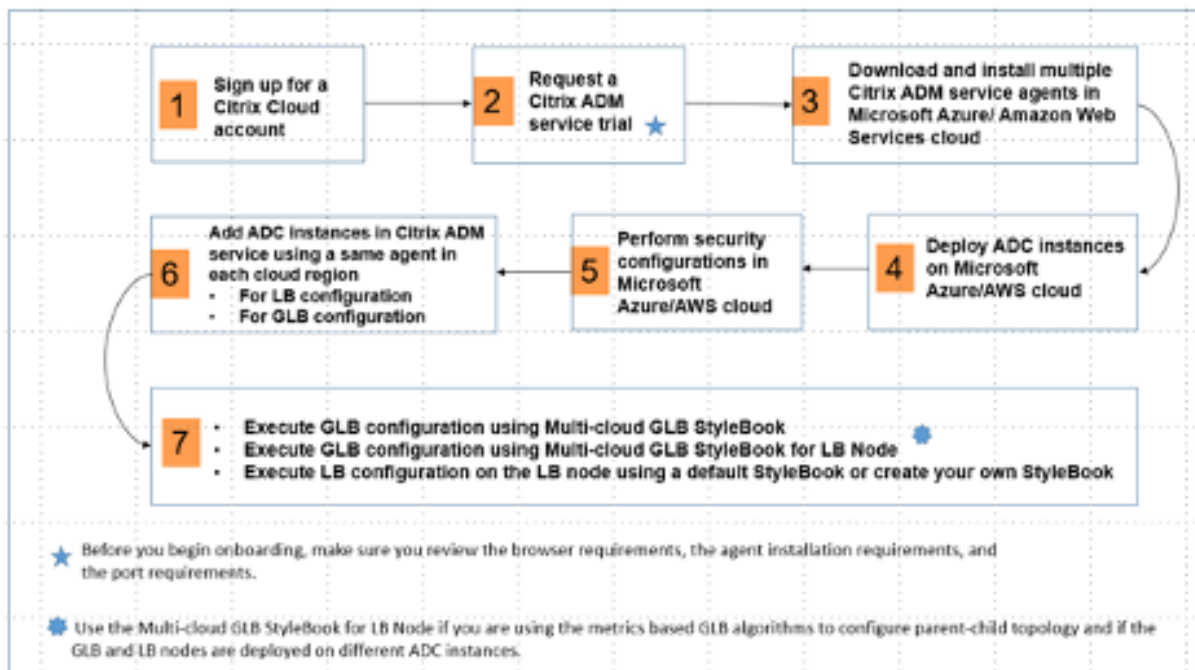
Los clientes pueden usar el StyleBook GSLB multicloud predeterminado en NetScaler ADM para configurar instancias de NetScaler con configuraciones GSLB híbridas y multicloud.

Los clientes pueden usar el StyleBook GSLB multicloud predeterminado para el StyleBook de nodo de equilibrio de carga para configurar los nodos de equilibrio de carga de NetScaler, que son los sitios secundarios en una topología padre-hijo que manejan el tráfico de la aplicación. Utilice este StyleBook solo si los usuarios desean configurar nodos de equilibrio de carga en una topología padre-hijo. Sin embargo, cada nodo LB debe configurarse por separado mediante este StyleBook.

Flujo de trabajo de la configuración de la solución GSLB híbrida y multinube de NetScaler

Los clientes pueden usar el StyleBook GSLB multicloud enviado en NetScaler ADM para configurar instancias de NetScaler con configuraciones GSLB híbridas y multicloud.

El siguiente diagrama muestra el flujo de trabajo para configurar una solución GSLB híbrida y multinube de NetScaler. Los pasos del diagrama de flujo de trabajo se explican con más detalle después del diagrama.



Realice las siguientes tareas como administrador de la nube:

1. Regístrese para obtener una cuenta de NetScaler Cloud.

Para comenzar a utilizar NetScaler ADM, cree una cuenta de empresa de NetScaler Cloud o únase a una existente que haya sido creada por alguien de su empresa.

2. Cuando los usuarios inicien sesión en NetScaler Cloud, **haga clic** en Administrar en el mosaico **NetScaler Application Delivery Management** para configurar el servicio ADM por primera vez.

3. Descargue e instale varios agentes de servicio NetScaler ADM.

Los usuarios deben instalar y configurar el agente de servicio NetScaler ADM en su entorno de red para habilitar la comunicación entre NetScaler ADM y las instancias administradas en su centro de datos o nube. Instale un agente en cada región para que puedan configurar las configuraciones de LB y GSLB en las instancias administradas. Las configuraciones LB y GSLB pueden compartir un único agente. Para obtener más información sobre las tres tareas anteriores, consulte [Primeros pasos](#).

4. Implemente balanceadores de carga en los centros de datos locales o en la nube de Microsoft AWS.

Según el tipo de equilibradores de carga que los usuarios implementen en la nube y en las instalaciones, aprovisionelos en consecuencia. Por ejemplo, los usuarios pueden aprovisionar instancias de NetScaler VPX en una nube privada virtual de Amazon Web Services (AWS) y en centros de datos locales. Configure las instancias de NetScaler para que funcionen como nodos

LB o GSLB en modo independiente mediante la creación de las máquinas virtuales y la configuración de otros recursos. Para obtener más información sobre cómo implementar instancias de NetScaler VPX, consulte los siguientes documentos:

- [NetScaler VPX en AWS](#).
- [Configure una instancia independiente de NetScaler VPX](#).

5. Realice configuraciones de seguridad.

Configure los grupos de seguridad de red y las ACL de red en ARM y en AWS para controlar el tráfico entrante y saliente de las instancias de usuario y las subredes.

6. Agregue instancias de NetScaler en NetScaler ADM.

Las instancias de NetScaler son dispositivos de red o dispositivos virtuales que los usuarios desean descubrir, administrar y monitorear desde NetScaler ADM. Para administrar y supervisar estas instancias, los usuarios deben agregarlas al servicio y registrar tanto las instancias LB (si los usuarios usan NetScaler para LB) como las instancias GSLB. Para obtener más información sobre cómo agregar instancias de NetScaler en NetScaler ADM, consulte [Primeros pasos](#)

7. Implemente las configuraciones GSLB y LB utilizando los StyleBooks de NetScaler ADM predefinidos.

- Utilice GSLB StyleBook de múltiples nubes para ejecutar la configuración de GSLB en las instancias de GSLB NetScaler seleccionadas.
- Implemente la configuración de equilibrio de carga. (Los usuarios pueden omitir este paso si ya tienen configuraciones de LB en las instancias administradas). Los usuarios pueden configurar balanceadores de carga en instancias de NetScaler de una de dos maneras:
- Configure manualmente las instancias para equilibrar la carga de las aplicaciones. Para obtener más información sobre cómo configurar manualmente las instancias, consulte [Configurar el equilibrio de carga básico](#).
- Use StyleBooks. Los usuarios pueden utilizar uno de los StyleBooks de NetScaler ADM (StyleBook de equilibrio de carga HTTP/SSL o StyleBook de equilibrio de carga HTTP/SSL (con monitores)) para crear la configuración del equilibrador de carga en la instancia de NetScaler seleccionada. Los usuarios también pueden crear sus propios StyleBooks. Para obtener más información sobre StyleBooks, consulte [StyleBooks](#).

8. Utilice el StyleBook GSLB multicloud para el nodo LB para configurar la topología padre-hijo de GSLB en cualquiera de los siguientes casos:

- Si los usuarios utilizan los algoritmos GSLB basados en métricas (menor cantidad de paquetes, menor cantidad de conexiones, menor ancho de banda) para configurar GSLB y los nodos de equilibrio de carga y si los nodos de equilibrio de carga están implementados en una instancia de NetScaler diferente.

- Si se requiere persistencia del sitio.

Uso de StyleBooks para configurar GSLB en nodos de equilibrio de carga de NetScaler

Los clientes pueden usar el StyleBook GSLB multicloud **para el nodo LB** si usan los algoritmos GSLB basados en métricas (menos paquetes, menos conexiones, menos ancho de banda) para configurar GSLB y nodos de equilibrio de carga y si los nodos de equilibrio de carga se implementan en una instancia de NetScaler diferente.

Los usuarios también pueden usar este StyleBook para configurar más sitios secundarios para un sitio principal existente. Este StyleBook configura un sitio secundario a la vez. Por lo tanto, cree tantas configuraciones (paquetes de configuración) a partir de este StyleBook como sitios secundarios. El StyleBook aplica la configuración GSLB en los sitios secundarios. Los usuarios pueden configurar un máximo de 1024 sitios secundarios.

Nota:

Utilice GSLB StyleBook de múltiples nubes para configurar los sitios principales.

Este StyleBook hace las siguientes suposiciones:

- Se configura una dirección SNIP o una dirección IP de sitio GSLB.
- El firewall y los grupos de seguridad necesarios se configuran en los proveedores de servicios en la nube.

Configuración de un sitio secundario en una topología principal-secundaria mediante el uso de GSLB StyleBook multicloud para el nodo LB

1. Vaya a **Aplicaciones > Configuración > Crear nueva**.
2. Vaya a **Aplicaciones > Configuración** y haga clic en **Crear nuevo**.

El StyleBook aparece como una página de interfaz de usuario en la que los usuarios pueden introducir los valores de todos los parámetros definidos en este StyleBook.

Nota:

Los términos centro de datos y sitios se utilizan indistintamente en este documento.

1. Defina los siguientes parámetros:
 - **Nombre de la aplicación.** Introduzca el nombre de la aplicación GSLB implementada en los sitios GSLB para los que desea crear sitios secundarios.
 - **Protocolo.** Seleccione el protocolo de aplicación de la aplicación implementada en el cuadro de lista desplegable.

- **LB Health Check** (opcional)
- **Tipo de chequeo de salud.** En el cuadro de lista desplegable, seleccione el tipo de sonda que se utiliza para comprobar el estado de la dirección VIP del balanceador de cargas que representa la aplicación en un sitio.
- **Modo seguro.** (Opcional) Seleccione **Sí** para habilitar este parámetro si se requieren comprobaciones de estado basadas en SSL.
- **Solicitud HTTP.** (Opcional) Si los usuarios seleccionaron HTTP como tipo de verificación de estado, introduzca la solicitud HTTP completa utilizada para sondear la dirección VIP.
- **Lista de códigos de respuesta de estado HTTP.** (Opcional) Si los usuarios seleccionaron HTTP como tipo de verificación de estado, introduzca la lista de códigos de estado HTTP que se esperan en las respuestas a las solicitudes HTTP cuando el VIP esté en buen estado.

2. Configurando el sitio principal.

- Proporcione los detalles del sitio principal (nodo GSLB) en el que desea crear el sitio secundario (nodo LB).
 - **Nombre del sitio.** Introduzca el nombre del sitio.
 - **Dirección IP del sitio.** Introduzca la dirección IP que el sitio principal utiliza como dirección IP de origen al intercambiar métricas con otros sitios. Se supone que esta dirección IP ya está configurada en el nodo GSLB de cada sitio.
 - **Dirección IP pública del sitio.** (Opcional) Introduzca la dirección IP pública del sitio secundario que se utiliza para intercambiar métricas, si la dirección IP de ese sitio tiene NAT.

3. Configurando el sitio hijo.

- Proporcione los detalles del sitio infantil.
 - **Nombre del sitio.** Introduzca el nombre del sitio principal.
 - **Dirección IP del sitio.** Introduzca la dirección IP del sitio secundario. Aquí, utilice la dirección IP privada o el SNIP del nodo de NetScaler que se está configurando como sitio secundario.
 - **Dirección IP pública del sitio.** (Opcional) Introduzca la dirección IP pública del sitio principal que se utiliza para intercambiar métricas, si la dirección IP de ese sitio tiene NAT.

4. Configuración de los servicios GSLB activos (opcional)

- Configure los servicios GSLB activos solo si la dirección IP del servidor virtual LB no es una dirección IP pública. Esta sección permite a los usuarios configurar la lista de servicios GSLB locales en los sitios donde se implementa la aplicación.

- **IP de servicio.** Introduzca la dirección IP del servidor virtual de equilibrio de carga de este sitio.
 - **Dirección IP pública de servicio.** Si la dirección IP virtual es privada y tiene una dirección IP pública con NAT, especifique la dirección IP pública.
 - **Puerto de servicio.** Introduzca el puerto del servicio GSLB en este sitio.
 - **Nombre del sitio.** Introduzca el nombre del sitio en el que se encuentra el servicio GSLB.
5. Haga clic en **Instancias de destino y seleccione las instancias** de NetScaler configuradas como instancias GSLB en cada sitio en el que desee implementar la configuración GSLB.
 6. Haga clic en **Crear** para crear la configuración de LB en la instancia de NetScaler seleccionada (nodo LB). Los usuarios también pueden hacer clic en **Ejecución en seco** para comprobar los objetos que se crearían en las instancias de destino. La configuración de StyleBook que han creado los usuarios aparece en la lista de configuraciones de la página Configuraciones. Los usuarios pueden examinar, actualizar o eliminar esta configuración mediante la GUI de NetScaler ADM.

Despliegue de plantillas de CloudFormation

NetScaler VPX está disponible como imágenes de máquina de Amazon (AMI) en AWS Marketplace. Antes de usar una plantilla de CloudFormation para aprovisionar un NetScaler VPX en AWS, el usuario de AWS debe aceptar los términos y suscribirse al producto de AWS Marketplace. Cada edición de NetScaler VPX del Marketplace requiere este paso.

Cada plantilla del repositorio de CloudFormation incluye documentación que describe el uso y la arquitectura de la plantilla. Las plantillas intentan codificar la arquitectura de implementación recomendada de NetScaler VPX, o presentar NetScaler al usuario o demostrar una característica, edición u opción en particular. Los usuarios pueden reutilizar, modificar o mejorar las plantillas para adaptarlas a sus necesidades particulares de producción y pruebas. La mayoría de las plantillas requieren permisos EC2 completos, además de permisos para crear funciones de IAM.

Las plantillas de CloudFormation contienen ID de AMI que son específicos de una versión concreta de NetScaler VPX (por ejemplo, la versión 12.0-56.20) y una edición (por ejemplo, NetScaler VPX Platinum Edition - 10 Mbps) O NetScaler BYOL. Para usar una versión/edición diferente de NetScaler VPX con una plantilla de CloudFormation, es necesario que el usuario edite la plantilla y sustituya los ID de AMI.

Los últimos AWS-AMI-ID de NetScaler se encuentran aquí: [NetScaler AWS CloudFormation Master](#).

Implementación de CFT Three-NIC

Esta plantilla implementa una VPC, con 3 subredes (administración, cliente, servidor) para 2 zonas de disponibilidad. Implementa una puerta de enlace de Internet, con una ruta predeterminada en las

subredes públicas. Esta plantilla también crea un par de alta disponibilidad en las zonas de disponibilidad con dos instancias de NetScaler: 3 ENI asociadas a 3 subredes de VPC (administración, cliente, servidor) en la principal y 3 ENI asociadas a 3 subredes de VPC (administración, cliente, servidor) en la secundaria. Todos los nombres de recursos creados por esta CFT llevan el prefijo `tagName` del nombre de la pila.

El resultado de la plantilla de CloudFormation incluye:

- `PrimaryCitrixADCManagementURL`: URL HTTPS a la GUI de administración del VPX principal (utiliza un certificado autofirmado)
- `PrimaryCitrixADCManagementUrl2`: URL HTTP a la GUI de administración del VPX principal
- `PrimaryCitrixAdcInstanceId`: Id. de instancia de la instancia VPX primaria recién creada
- `PrimaryCitrixAdcPublicVIP`: dirección IP elástica de la instancia VPX principal asociada al VIP
- `PrimaryCitrixADCPrivateNSIP`: IP privada (NS IP) utilizada para la administración del VPX principal
- `PrimaryCitrixAdcPublicNSIP`: IP pública (NS IP) utilizada para la administración del VPX principal
- `PrimaryCitrixADCPrivateVIP`: dirección IP privada de la instancia VPX principal asociada al VIP
- `PrimaryCitrixAdcsnip`: dirección IP privada de la instancia VPX principal asociada con el SNIP
- `SecondaryCitrixADCManagementURL`: URL HTTPS a la GUI de administración del VPX secundario (utiliza un certificado autofirmado)
- `SecondaryCitrixADCManagementUrl2`: URL HTTP a la GUI de administración del VPX secundario
- `SecondaryCitrixAdcInstanceId`: Id. de instancia de la instancia VPX secundaria recién creada
- `SecondaryCitrixADCPrivateNSIP`: IP privada (NS IP) utilizada para la administración del VPX secundario
- `SecondaryCitrixADCPublicNSIP`: IP pública (NS IP) utilizada para la administración del VPX secundario
- `SecondaryCitrixADCPrivateVIP`: dirección IP privada de la instancia VPX secundaria asociada al VIP
- `SecondaryCitrixAdcsnip`: dirección IP privada de la instancia VPX secundaria asociada al SNIP
- `SecurityGroup`: ID de grupo de seguridad al que pertenece VPX

Al proporcionar información a la CFT, la comparación `*` con cualquier parámetro en la CFT implica que es un campo obligatorio. Por ejemplo, `VPC ID*` es un campo obligatorio.

Se deben cumplir los siguientes requisitos previos. La plantilla de CloudFormation requiere permisos suficientes para crear funciones de IAM, más allá de los privilegios totales normales de EC2. El usuario

de esta plantilla también debe aceptar los términos y suscribirse al producto de AWS Marketplace antes de usar esta plantilla de CloudFormation.

También debe estar presente lo siguiente:

- Par de claves
- 3 EIP no asignadas
- Administración primaria
- Cliente VIP
- Administración secundaria

Para obtener más información sobre el aprovisionamiento de instancias de NetScaler VPX en AWS, los usuarios pueden visitar: [Aprovisionamiento de instancias de NetScaler VPX en AWS](#).

Para obtener información sobre cómo configurar GSLB usando StyleBooks, visita [Uso de StyleBooks para configurar GSLB](#)

Recuperación ante desastres (DR)

El desastre es una interrupción repentina de las funciones empresariales causada por desastres naturales o eventos causados por seres humanos. Los desastres afectan a las operaciones del centro de datos, después de lo cual los recursos y los datos perdidos en el sitio del desastre deben reconstruirse y restaurarse por completo. La pérdida de datos o el tiempo de inactividad en el centro de datos es fundamental y colapsa la continuidad del negocio.

Uno de los desafíos a los que se enfrentan los clientes hoy en día es decidir dónde colocar su sitio de recuperación ante desastres. Las empresas buscan uniformidad y rendimiento independientemente de cualquier falla de red o infraestructura subyacente.

Para implementar GSLB para recuperación ante desastres, consulte [Implementar una instancia independiente de NetScaler VPX en AWS](#)

Otros recursos

[NetScaler ADM GSLB para implementaciones híbridas y de múltiples nubes.](#)

Configurar una instancia de NetScaler VPX para utilizar la interfaz de red SR-IOV

October 17, 2024

Nota:

La compatibilidad con interfaces SR-IOV en una configuración de alta disponibilidad está disponible desde NetScaler versión 12.0 57.19 en adelante.

Después de crear una instancia NetScaler VPX en AWS, puede configurar el dispositivo virtual para que use interfaces de red SR-IOV mediante la CLI de AWS.

En todos los modelos de NetScaler VPX, excepto NetScaler VPX AWS Marketplace Editions de 3G y 5G, SR-IOV no está habilitado en la configuración predeterminada de una interfaz de red.

Antes de iniciar la configuración, lea los siguientes temas:

- [Requisitos previos](#)
- [Instrucciones de uso y limitaciones](#)

En esta sección se incluyen los temas siguientes:

- Cambie el tipo de interfaz a SR-IOV
- Configurar SR-IOV en una configuración de alta disponibilidad

Cambie el tipo de interfaz a SR-IOV

Puede ejecutar el comando `show interface summary` para comprobar la configuración predeterminada de una interfaz de red.

Ejemplo 1: La siguiente captura de pantalla de CLI muestra la configuración de una interfaz de red en la que SR-IOV está habilitado de forma predeterminada en NetScaler VPX AWS Marketplace Editions of 3G y 5G.

```
> show interface summary
-----
      Interface  MTU      MAC              Suffix
-----
1      1/1        1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2      L0/1        1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
Done
```

Ejemplo 2: La siguiente captura de pantalla CLI muestra la configuración predeterminada de una interfaz de red donde SR-IOV no está habilitado.

```

Done
[> sh int s
-----
Interface  MTU      MAC          Suffix
-----
1   1/1      1500      12:fc:04:c5:d0:12  NetScaler Virtual Interface
2   L0/1     1500      12:fc:04:c5:d0:12  Netscaler Loopback interface
Done
>

```

Para obtener más información sobre cómo cambiar el tipo de interfaz a SR-IOV, consulte <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html>

Para cambiar el tipo de interfaz a SR-IOV

1. Cierre la instancia de NetScaler VPX que se ejecuta en AWS.
2. Para habilitar SR-IOV en la interfaz de red, escriba el siguiente comando en la CLI de AWS.


```
$ aws ec2 modify-instance-attribute --instance-id \&#060;instance \
\_id\&#062; --sriov-net-support simple
```
3. Para comprobar si SR-IOV se ha habilitado, escriba el siguiente comando en la CLI de AWS.


```
$ aws ec2 describe-instance-attribute --instance-id \&#060;instance \
\_id\&#062; --attribute sriovNetSupport
```

Ejemplo 3: El tipo de interfaz de red cambió a SR-IOV mediante la CLI de AWS.

```

aws ec2 modify-instance-attribute --instance-id i-008c1230aaf303bee --sriov-net-support simple
aws ec2 describe-instance-attribute --instance-id i-008c1230aaf303bee --attribute sriovNetSupport
{
  "InstanceId": "i-008c1230aaf303bee",
  "SriovNetSupport": {
    "Value": "simple"
  }
}

```

Si SR-IOV no está habilitado, el valor para SriovnetSupport está ausente.

Ejemplo 4: En el ejemplo siguiente, el soporte para SR-IOV no está habilitado.

```

{
  "InstanceId": "i-0c3e84cfa65b04cc8",
  "SriovNetSupport": {}
}

```

4. Encienda la instancia VPX. Para ver el estado modificado de la interfaz de red, escriba “show interface summary” en la CLI.

Ejemplo 5: La siguiente captura de pantalla muestra las interfaces de red con SR-IOV habilitado. Las interfaces 10/1, 10/2, 10/3 están habilitadas para SR-IOV.

```
> show interface summary
-----
Interface  MTU      MAC              Suffix
-----
1   10/1      1500            0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2   10/2      1500            0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3   10/3      1500            0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4   LO/1      1500            0a:1e:2e:17:a2:37  Netscaler Loopback interface
Done
```

Estos pasos completan el procedimiento para configurar las instancias VPX para utilizar interfaces de red SR-IOV.

Configure SR-IOV en una configuración de alta disponibilidad

Las interfaces SR-IOV admiten la alta disponibilidad a partir de la versión 12.0 de NetScaler, versión 57.19.

Si la configuración de alta disponibilidad se implementó manualmente o mediante la plantilla de Citrix CloudFormation para NetScaler versión 12.0 56.20 o versiones anteriores, la función de IAM asociada a la configuración de alta disponibilidad debe tener los siguientes privilegios:

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns:*
- sqs: *
- IAM: Simular directiva principal
- Soy: obtener rol

De forma predeterminada, la plantilla de Citrix CloudFormation para NetScaler versión 12.0 57.19 agrega automáticamente los privilegios necesarios a la función de IAM.

Nota:

Una configuración de alta disponibilidad con interfaces SR-IOV tarda alrededor de 100 segundos de tiempo de inactividad.

Recursos relacionados:

Para obtener más información sobre los roles de IAM, consulte la [documentación de AWS](#).

Configurar una instancia de NetScaler VPX para utilizar redes mejoradas con AWS ENA

October 17, 2024

Después de crear una instancia NetScaler VPX en AWS, puede configurar el dispositivo virtual para utilizar [redes mejoradas](#) con [AWS Elastic Network Adapter \(ENA\)](#) mediante AWS CLI.

Junto con AWS ENA, las redes mejoradas proporcionan mayor ancho de banda, mayor rendimiento de paquete por segundo (PPS) y latencia entre instancias cada vez menor.

Antes de iniciar la configuración, lea los siguientes temas:

- [Requisitos previos](#)
- [Instrucciones de uso y limitaciones](#)

Se admiten las siguientes configuraciones de alta disponibilidad para instancias habilitadas para ENA:

- Las direcciones IP privadas se pueden mover dentro de la misma zona de disponibilidad.
- Las direcciones IP elásticas se pueden mover a través de las zonas de disponibilidad.

Actualización de una instancia NetScaler VPX en AWS

October 17, 2024

Puede actualizar el tipo de instancia de EC2, el rendimiento, la edición de software y el software del sistema de un NetScaler VPX que se ejecuta en AWS. Para ciertos tipos de actualizaciones, Citrix recomienda utilizar el método Configuración de alta disponibilidad para minimizar el tiempo de inactividad.

Nota:

- La versión 10.1.e-124.1308.e o posterior del software NetScaler para una AMI de NetScaler VPX (incluidas la licencia de utilidad y la licencia de cliente) no admite las familias de instancias M1 y M2.
- Debido a los cambios en la compatibilidad con instancias VPX, no se admite la reducción

de 10.1.e-124 o una versión posterior a 10.1.123.x o una versión anterior.

- La mayoría de las actualizaciones no requieren el lanzamiento de una nueva AMI y la actualización se puede realizar en la instancia de AMI de NetScaler actual. Si desea actualizar a una nueva instancia de AMI de NetScaler, utilice el método de configuración de alta disponibilidad.

Cambiar el tipo de instancia EC2 de una instancia de NetScaler VPX en AWS

Si sus instancias de NetScaler VPX ejecutan la versión 10.1.e-124.1308.e o posterior, puede cambiar el tipo de instancia EC2 desde la consola de AWS de la siguiente manera:

1. Detenga la instancia VPX.
2. Cambie el tipo de instancia de EC2 desde la consola de AWS.
3. Inicie la instancia.

También puede utilizar el procedimiento anterior para cambiar el tipo de instancia EC2 para una versión anterior a 10.1.e-124.1308.e, a menos que quiera cambiar el tipo de instancia a M3. En ese caso, debe seguir primero el procedimiento de actualización estándar de NetScaler, en, para actualizar el software NetScaler a 10.1.e-124 o a una versión posterior y, a continuación, seguir los pasos anteriores.

Actualice el rendimiento o la edición de software de una instancia de NetScaler VPX en AWS

Para actualizar la edición de software (por ejemplo, para actualizar de la edición estándar a la Premium) o el rendimiento (por ejemplo, para actualizar de 200 Mbps a 1000 mbps), el método depende de la licencia de la instancia.

Uso de una licencia de cliente (Bring-Your-Own-License)

Si utiliza una licencia de cliente, puede comprar y descargar la nueva licencia desde el sitio web de Citrix y, a continuación, instalar la licencia en la instancia de VPX. Para obtener más información acerca de cómo descargar e instalar una licencia desde el sitio web de Citrix, consulte la Guía de licencias de VPX.

Uso de una licencia de utilidad (licencia de utilidad con tarifa horaria)

AWS no admite actualizaciones directas para instancias basadas en tarifas. Para actualizar la edición de software o el rendimiento de una instancia de NetScaler VPX basada en tarifas, inicie una nueva AMI

con la licencia y la capacidad deseadas y migre la configuración de instancia anterior a la nueva instancia. Esto se puede lograr mediante el uso de una configuración de alta disponibilidad de NetScaler como se describe en la subsección [Actualizar a una nueva instancia de NetScaler AMI mediante el uso de una configuración de alta disponibilidad de NetScaler] (#actualizar-a-una-nueva-instancia-de-citrix-adc-ami-mediante-el-uso-de-una-configuración-de-alta-disponibilidad-de-citrix-adc) en esta página.

Actualizar el software del sistema de una instancia de NetScaler VPX en AWS

Si necesita actualizar una instancia VPX que ejecuta 10.1.e-124.1308.e o una versión posterior, siga el procedimiento de actualización estándar de NetScaler en [Actualizar y bajar de categoría un dispositivo NetScaler](#).

Si necesita actualizar una instancia VPX que ejecute una versión anterior a 10.1.e-124.1308.e a 10.1.e-124.1308.e o una versión posterior, actualice primero el software del sistema y, a continuación, cambie el tipo de instancia a M3 de la siguiente manera:

1. Detenga la instancia VPX.
2. Cambie el tipo de instancia de EC2 desde la consola de AWS.
3. Inicie la instancia.

Actualice a una nueva instancia de AMI de NetScaler mediante una configuración de alta disponibilidad de NetScaler

Para utilizar el método de alta disponibilidad para actualizar a una nueva instancia de AMI de NetScaler, realice las siguientes tareas:

- Cree una nueva instancia con el tipo de instancia EC2, la edición de software, el rendimiento o la versión de software deseados desde el mercado de AWS.
- Configure la alta disponibilidad entre la instancia antigua (que se va a actualizar) y la nueva. Una vez configurada la alta disponibilidad entre la instancia anterior y la nueva, la configuración de la instancia anterior se sincroniza con la nueva instancia.
- Forzar una conmutación por error de alta disponibilidad de la instancia anterior a la nueva instancia. Como resultado, la nueva instancia se convierte en primaria y comienza a recibir tráfico.
- Detenga y vuelva a configurar o eliminar la instancia anterior de AWS.

Requisitos previos y puntos a considerar

- Asegúrese de comprender cómo funciona la alta disponibilidad entre dos instancias de NetScaler VPX en AWS. Para obtener más información sobre la configuración de alta disponi-

bilidad entre dos instancias de NetScaler VPX en AWS, consulte [Implementar un par de alta disponibilidad en AWS](#).

- Debe crear la nueva instancia en la misma zona de disponibilidad que la instancia anterior, teniendo exactamente el mismo grupo de seguridad y subred.
- La configuración de alta disponibilidad requiere claves de acceso y secretas asociadas a la cuenta de AWS Identity and Access Management (IAM) del usuario para ambas instancias. Si no se utiliza la información de clave correcta al crear instancias VPX, se produce un error en la configuración de HA. Para obtener más información sobre cómo crear una cuenta IAM para una instancia VPX, consulte [Requisitos previos](#).
 - Debe utilizar la consola EC2 para crear la nueva instancia. No puede utilizar el inicio de AWS 1-Clic, ya que no acepta las claves de acceso y secretas como entrada.
 - La nueva instancia debe tener solo una interfaz ENI.

Para actualizar una instancia de NetScaler VPX mediante una configuración de alta disponibilidad, siga estos pasos:

1. Configure la alta disponibilidad entre la instancia anterior y la nueva. Para configurar la alta disponibilidad entre dos instancias NetScaler VPX, en el símbolo del sistema de cada instancia, escriba:

- `add ha node <nodeID> <IPaddress of the node to be added>`
- `save config`

Ejemplo:

En la línea de comandos de la instancia anterior, escriba:

```
1 add ha node 30 192.0.2.30
2 Done
```

En la línea de comandos de la nueva instancia, escriba:

```
1 add ha node 10 192.0.2.10
2 Done
```

Tenga en cuenta lo siguiente:

- En la configuración de HA, la instancia anterior es el nodo principal y la nueva instancia es el nodo secundario.
- La dirección IP de NSIP no se copia de la instancia anterior a la nueva instancia. Por lo tanto, después de la actualización, la nueva instancia tiene una dirección IP de administración diferente de la anterior.
- La contraseña de `nsroot` cuenta de la nueva instancia se establece en la de la instancia anterior tras la sincronización de alta disponibilidad.

Para obtener más información sobre la configuración de alta disponibilidad entre dos instancias de NetScaler VPX en AWS, consulte [Implementar un par de alta disponibilidad en AWS](#).

2. Forzar una conmutación por error de alta disponibilidad. Para forzar una conmutación por error en una configuración de alta disponibilidad, en la línea de comandos de cualquiera de las instancias, escriba:

```
1 force HA failover
```

Como resultado de forzar una conmutación por error, los ENI de la instancia anterior se migran a la nueva instancia y el tráfico fluye a través de la nueva instancia (el nuevo nodo principal). La instancia anterior (el nuevo nodo secundario) se reinicia.

Si aparece el siguiente mensaje de advertencia, escriba N para anular la operación:

```
1 [WARNING]:Force Failover may cause configuration loss, peer
   health not optimum. Reason(s):
2 HA version mismatch
3 HA heartbeats not seen on some interfaces
4 Please confirm whether you want force-failover (Y/N)?
```

El mensaje de advertencia aparece porque el software del sistema de las dos instancias VPX no es compatible con HA. Como resultado, la configuración de la instancia anterior no se puede sincronizar automáticamente con la nueva instancia durante una conmutación por error forzada.

A continuación se presenta la solución alternativa para este problema:

- a) En el indicador de shell de NetScaler de la instancia anterior, escriba el siguiente comando para crear una copia de seguridad del archivo de configuración (`ns.conf`):

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

- b) Elimine la siguiente línea del archivo de configuración de respaldo (`ns.conf.bkp`):

- `set ns config -IPAddress <IP> -netmask <MASK>`

Por ejemplo, `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

- c) Copie el archivo de configuración de respaldo de la instancia anterior (`ns.conf.bkp`) al directorio `/nsconfig` de la nueva instancia.

- d) En el indicador de shell de NetScaler de la nueva instancia, escriba el siguiente comando para cargar el archivo de configuración de la instancia anterior (`ns.conf.bkp`) en la nueva instancia:

- `batch -f /nsconfig/ns.conf.bkp`

- e) Guarde la configuración en la nueva instancia.

- `save config`

- f) En el símbolo del sistema de cualquiera de los nodos, escriba el comando siguiente para forzar una conmutación por error y, a continuación, escriba Y para el mensaje de advertencia para confirmar la operación de conmutación por error de fuerza:

- `force ha failover`

Ejemplo:

```
1          > force ha failover
2
3  [WARNING]:Force Failover may cause configuration loss, peer
           health not optimum.
4           Reason(s):
5           HA version mismatch
6           HA heartbeats not seen on some interfaces
7           Please confirm whether you want force-failover (Y/N)?
           Y
```

3. Elimine la configuración de HA, de modo que las dos instancias ya no estén en una configuración de HA. Primero elimine la configuración de HA del nodo secundario y, a continuación, elimine la configuración de HA del nodo primario.

Para quitar una configuración de alta disponibilidad entre dos instancias de NetScaler VPX, en el símbolo del sistema de cada instancia, escriba:

```
1          > remove ha node \<nodeID\>
2          > save config
```

Para obtener más información sobre la configuración de alta disponibilidad entre dos instancias VPX en AWS, consulte [Implementar un par de alta disponibilidad en AWS](#).

Ejemplo:

En la línea de comandos de la instancia anterior (nuevo nodo secundario), escriba:

```
1          > remove ha node 30
2          Done
3          > save config
4          Done
```

En el símbolo del sistema de la nueva instancia (nuevo nodo principal), escriba:

```
1          > remove ha node 10
2          Done
3          > save config
4          Done
```

Solución de problemas de una instancia VPX en AWS

October 17, 2024

Amazon no proporciona acceso de consola a una instancia de NetScaler VPX. Para solucionar problemas, debe utilizar la interfaz gráfica de usuario de AWS para ver el registro de actividad. Solo puede depurar si la red está conectada. Para ver el registro del sistema de una instancia, haga clic con el botón derecho en la instancia y seleccione Registro del sistema.

NetScaler ofrece soporte para instancias de NetScaler VPX con licencia de AWS Marketplace (licencia de utilidad con tarifa por hora) en AWS. Para presentar un caso de soporte, busque su número de cuenta de AWS y su código PIN de soporte y llame al soporte de NetScaler. También se le pedirá su nombre y su dirección de correo electrónico. Para encontrar el PIN de soporte, inicie sesión en la GUI de VPX y vaya a la página del sistema.

Aquí hay un ejemplo de una página del sistema que muestra el PIN de soporte.

The screenshot shows the NetScaler System Information page. On the left is a navigation menu with 'System' selected. The main content area is titled 'System' and has tabs for 'System Information', 'System Sessions (1)', and 'System Network'. Below the tabs are buttons for 'System Upgrade', 'Reboot', 'Migration', 'Statistics', and 'Call Home'. The 'System Information' section displays various system details:

Citrix ADC IP Address	
Netmask	
Node	Standalone
Technical Support PIN	
Time Zone	Coordinated Universal Time
System Time	Wed, 18 Dec 2019 06:16:59 UTC
Last Config Changed Time	Wed, 18 Dec 2019 06:16:40 UTC
Last Config Saved Time	Wed, 18 Dec 2019 05:41:16 UTC

The 'Hardware Information' section displays:

Platform	NetScaler Virtual Appliance 450040
Manufactured on	2/17/2009
CPU	2305 MHZ
Host Id	
Serial no	
Encoded serial no	
Citrix ADC UUID	

Preguntas frecuentes sobre AWS

October 17, 2024

- **¿Una instancia de NetScaler VPX admite los volúmenes cifrados en AWS?**

El cifrado y el descifrado ocurren a nivel del Hypervisor y, por lo tanto, funcionan perfectamente con cualquier instancia. Para obtener más información acerca de los volúmenes cifrados, consulte el siguiente documento de AWS:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

- **¿Cuál es la mejor manera de aprovisionar una instancia de NetScaler VPX en AWS?**

Puede aprovisionar una instancia de NetScaler VPX en AWS de cualquiera de las siguientes maneras:

- Plantilla de AWS CloudFormation (CFT) en el mercado de AWS
- Administrador de dispositivos NetScaler
- Inicio rápido de AWS
- Citrix AWS CFT en GitHub
- Scripts de Citrix Terraform en GitHub
- Libros de jugadas de Citrix Ansible en GitHub
- flujo de trabajo de lanzamiento de AWS EC2

Puede elegir cualquiera de las opciones enumeradas en función de la herramienta de automatización que utilice.

Para obtener más detalles sobre las opciones, consulte [NetScaler VPX en AWS](#).

- **¿ Cómo actualizar la instancia de NetScaler VPX en AWS?**

Para actualizar la instancia de NetScaler VPX en AWS, puede actualizar el software del sistema o actualizar a una nueva imagen de máquina de Amazon (AMI) de NetScaler VPX siguiendo el procedimiento en [Actualizar una instancia de NetScaler VPX en AWS](#).

La forma recomendada de actualizar una instancia NetScaler VPX es utilizar el servicio ADM siguiendo el procedimiento de [Utilizar trabajos para actualizar instancias de NetScaler](#).

- **¿ Cuál es el tiempo de conmutación por error de alta disponibilidad para NetScaler VPX en AWS?**

- La conmutación por error de alta disponibilidad de NetScaler VPX dentro de la zona de disponibilidad de AWS tarda aproximadamente 3 segundos.
- La conmutación por error de alta disponibilidad de NetScaler VPX en las zonas de disponibilidad de AWS tarda unos 5 segundos.

- **¿ Qué nivel de soporte se proporciona a los clientes de suscripción de NetScaler VPX Marketplace que proporcionan el PIN de soporte técnico?**

De forma predeterminada, el servicio “Seleccionar software” se proporciona a los clientes que proporcionan el PIN de soporte técnico.

- **En la implementación de [Alta disponibilidad en diferentes zonas usando IP elástica](#) , ¿necesitamos crear múltiples IPsets para cada aplicación?**

Sí. Si hay varias aplicaciones con varios VIP asignados a varios EIP, se requieren varios IPsets. Por lo tanto, durante la conmutación por error de alta disponibilidad, todas las asignaciones VIP principales de los EIP se cambian a VIP secundarias (nuevas primarias).

- **¿Por qué está habilitado el modo INC en alta disponibilidad en diferentes implementaciones de zonas?**

Los pares de alta disponibilidad en todas las zonas de disponibilidad se encuentran en redes diferentes. Para la sincronización de alta disponibilidad, la configuración de red no debe sincronizarse. Esto se logra habilitando el modo INC en el par HA.

- **¿Puede el nodo de alta disponibilidad de una zona de disponibilidad comunicarse con los servidores back-end de otra zona de disponibilidad, siempre que esas zonas de disponibilidad estén en la misma VPC?**

Sí, se puede acceder a subredes de diferentes zonas de disponibilidad de la misma VPC agregando una ruta adicional que apunta a la subred del servidor backend mediante SNIP. Por ejemplo, si la subred SNIP de ADC en AZ1 es 192.168.3.0/24 y la subred del servidor backend de AZ2 es 192.168.6.0/24, se debe agregar una ruta en el dispositivo NetScaler presente en AZ1 como 192.168.6.0 255.255.255.0 192.168.3.1.

- **¿Pueden funcionar juntas las implementaciones de [alta disponibilidad en diferentes zonas usando IP elástica](#) y de [alta disponibilidad en diferentes zonas usando IP privada](#) ?**

Sí, ambas configuraciones se pueden aplicar en el mismo par HA.

- **En la implementación de [Alta disponibilidad en diferentes zonas usando IP privada](#) , si hay múltiples subredes con múltiples tablas de rutas en una VPC, ¿cómo sabe un nodo secundario en un par de HA sobre la tabla de rutas que se debe verificar durante la conmutación por error de HA?**

El nodo secundario conoce las NIC principales y busca en todas las tablas de redirección de una VPC.

- **¿Cuál es el tamaño de la `/var` partición cuando se utiliza la imagen predeterminada para VPX en AWS? ¿Cómo aumentar el espacio en disco?**

El tamaño del disco raíz está limitado a 20 GB para mantener la imagen del disco pequeña.

Si desea aumentar el espacio del directorio `/var/core/` o el `/var/crash/` directorio, conecte un disco adicional. Para aumentar el `/var` tamaño, actualmente, debe adjuntar un disco adicional y crear un enlace simbólico al `/var`, después de copiar el contenido crítico en el nuevo disco.

- **¿Cuántos motores de paquetes están activados y asignados a vCPU?**

Los motores de paquetes (PE) están limitados por el número de vCPU con licencia. Los daemons de NetScaler no están anclados a ninguna vCPU concreta y pueden ejecutarse en cualquiera de las vCPU que no sean PE. Según AWS, la C5.9xLarge es una instancia de 36 VCPU con 72 GB de memoria. Con las licencias agrupadas, la instancia NetScaler VPX se implementa con el número máximo de PE. En este caso, 19 PE se ejecutan en los núcleos del 1 al 19. Sin embargo, los procesos de administración de ADC se ejecutan desde las CPU 20-31.

• **¿Cómo decidir la instancia de AWS correcta para ADC?**

1. Comprenda su caso de uso y requisitos, como el rendimiento, el PPS, los requisitos SSL y el tamaño medio de los paquetes.
2. Elija la oferta y las licencias de ADC correctas que cumplan sus requisitos, como las ofertas de ancho de banda VPX o las licencias basadas en vCPU.
3. En función de la oferta elegida, decida la instancia de AWS.

Ejemplo

Una licencia de 5 Gbps permite 5 motores de paquetes de datos. Por lo tanto, el requisito de vCPU es 6 (5+1 para administración). Sin embargo, la instancia de 6 vCPU no está disponible. Por lo tanto, una CPU virtual de 8 es lo suficientemente buena para alcanzar ese rendimiento siempre que elija una red que admita un ancho de banda de 5 Gbps. Por ejemplo, debe elegir m5.2xlarge para una licencia de ancho de banda de 5 Gbps para permitir la asignación máxima de PE para una licencia de 5 Gbps. Pero si utiliza una licencia de vCPU que no está limitada por el rendimiento, es posible que obtenga un rendimiento de 5 Gbps mediante la propia instancia m5.xlarge.

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

• **¿Es obligatoria la implementación de tres NIC y tres subredes para ADC en AWS?**

Three NICs-three subnets es la implementación recomendada, donde cada una para la administración, el cliente y la red de servidores. Esta implementación proporciona un mejor aislamiento del tráfico y un rendimiento VPX. Dos NIC, dos subredes y una subred NIC uno son las otras opciones disponibles. No se recomienda tener varias NIC compartiendo una subred en AWS, como una implementación de dos NIC y una subred. Este escenario puede causar problemas de red como enrutamiento asimétrico. Para obtener más información, consulte [Prácticas recomendadas para configurar interfaces de red en AWS](#).

- **¿Por qué un controlador ENA en AWS siempre indica una velocidad de enlace de 1 Gbps (1/1), independientemente de las capacidades de red de la instancia?**

La velocidad informada de un adaptador de red elástica (ENA) de AWS a menudo se muestra como 1 Gbps (1/1), independientemente del tipo de instancia seleccionado. Esto se debe a que la velocidad indicada no refleja directamente el rendimiento real de la red. A diferencia de las interfaces de red tradicionales, las velocidades de ENA pueden escalar dinámicamente según los requisitos y la carga de trabajo de la instancia. El verdadero rendimiento de la red está determinado principalmente por el tipo y el tamaño de la instancia. Por lo tanto, el rendimiento real de la red puede variar significativamente según el tipo de instancia específica y la carga de red actual.

Implementar una instancia de NetScaler VPX en Microsoft Azure

October 17, 2024

Al implementar una instancia de NetScaler VPX en Microsoft Azure Resource Manager (ARM), puede usar los dos conjuntos de funciones siguientes para satisfacer las necesidades de su empresa:

- Capacidades de cloud computing de Azure
- Funciones de equilibrio de carga y administración del tráfico de NetScaler

Puede implementar instancias NetScaler VPX en ARM como instancias independientes o como pares de alta disponibilidad en modos activo-en espera.

Puede implementar una instancia NetScaler VPX en Microsoft Azure de dos formas:

- A través de Azure Marketplace. El dispositivo virtual NetScaler VPX está disponible como imagen en Microsoft Azure Marketplace.
- Usar la plantilla json de Azure Resource Manager (ARM) de NetScaler disponible en GitHub. Para obtener más información, consulte el [repositorio de GitHub para las plantillas de soluciones NetScaler](#).

La pila de Microsoft Azure es una plataforma integrada de hardware y software que ofrece los servicios de nube pública de Microsoft Azure en un centro de datos local para que las organizaciones puedan construir nubes híbridas. Ahora puede implementar las instancias de NetScaler VPX en la pila de Microsoft Azure.

Nota:

Azure restringe el acceso al tráfico que se origina fuera de Azure y lo bloquea. Para proporcionar acceso, habilite el servicio o el puerto agregando una regla de entrada en el grupo de seguridad

de red conectado a la NIC de la máquina virtual a la que está conectada una dirección IP pública. Para obtener más información, consulte la documentación de Azure sobre [las reglas de NAT de entrada](#).

Requisito previo

Necesita algunos conocimientos previos antes de implementar una instancia de NetScaler VPX en Azure.

- Familiaridad con la terminología de Azure y los detalles de red. Para obtener información, consulte [Terminología de Azure](#).
- Conocimiento de un dispositivo NetScaler. Para obtener información detallada sobre el dispositivo NetScaler, consulte [NetScaler](#).
- Conocimiento de las redes NetScaler. Consulte el tema [Redes](#).

Cómo funciona una instancia de NetScaler VPX en Azure

En una implementación local, una instancia de NetScaler VPX requiere al menos tres direcciones IP:

- Dirección IP de administración, denominada dirección NSIP
- Dirección IP de subred (SNIP) para comunicarse con el conjunto de servidores
- Dirección IP del servidor virtual (VIP) para aceptar solicitudes de clientes

Para obtener más información, consulte [Arquitectura de red para instancias NetScaler VPX en Microsoft Azure](#).

Nota:

La instancia de NetScaler VPX admite los procesadores Intel y AMD. Los dispositivos virtuales VPX se pueden implementar en cualquier tipo de instancia que tenga dos o más núcleos virtualizados y más de 2 GB de memoria. Para obtener más información sobre los requisitos del sistema, consulte la [hoja de datos de NetScaler VPX](#).

En una implementación de Azure, puede aprovisionar una instancia de NetScaler VPX en Azure de tres maneras:

- Arquitectura multi-IP multi-NIC
- Arquitectura multi-IP de NIC única
- IP única NIC única

En función de sus necesidades, puede utilizar cualquiera de estos tipos de arquitectura compatibles.

Arquitectura multi-IP multi-NIC

En este tipo de implementación, puede tener más de una interfaz de red (NIC) conectada a una instancia VPX. Cualquier NIC puede tener una o más configuraciones IP: direcciones IP públicas y privadas estáticas o dinámicas asignadas.

Para obtener más información, consulte los siguientes casos de uso:

- [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC](#)
- [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell](#)

Nota:

Para evitar que MAC se mueva y se silencie la interfaz en los entornos de Azure, Citrix recomienda crear una VLAN por interfaz de datos (sin etiqueta) de la instancia de NetScaler VPX y vincular la IP principal de la NIC en Azure. Para obtener más información, consulte el artículo [CTX224626](#).

Arquitectura multi-IP de NIC única

En este tipo de implementación, una interfaz de red (NIC) asociada a varias configuraciones IP: direcciones IP públicas y privadas estáticas o dinámicas asignadas. Para obtener más información, consulte los siguientes casos de uso:

- [Configuración de varias direcciones IP para una instancia independiente NetScaler VPX](#)
- [Configurar varias direcciones IP para una instancia independiente de NetScaler VPX mediante comandos de PowerShell](#)

IP única NIC única

En este tipo de implementación, una interfaz de red (NIC) asociada a una única dirección IP, que se utiliza para realizar las funciones de NSIP, SNIP y VIP.

Para obtener más información, consulte [Configurar una instancia independiente de NetScaler VPX](#).

Nota:

El modo IP única solo está disponible en implementaciones de Azure. Este modo no está disponible para una instancia de NetScaler VPX en sus instalaciones, en AWS ni en otros tipos de implementación.

Licencias de NetScaler VPX

Una instancia de NetScaler VPX en Azure requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias NetScaler VPX que se ejecutan en Azure.

- **Licencias basadas en suscripción:** los dispositivos NetScaler VPX están disponibles como instancias de pago en Azure Marketplace. Las licencias basadas en suscripciones son una opción de pago por uso. A los usuarios se les cobra cada hora.

Nota:

En el caso de las licencias basadas en suscripciones, la facturación de la suscripción se aplica durante todo el período de licencia de un modelo de licencia determinado. Debido a las restricciones de la nube, Azure no admite cambiar ni eliminar el modelo de licencia aplicable a la suscripción. Para cambiar o eliminar una licencia de suscripción, elimine la máquina virtual de ADC existente y vuelva a crear una nueva máquina virtual de ADC con la licencia requerida.

NetScaler proporciona soporte técnico para instancias de licencias basadas en suscripciones. Para presentar un caso de asistencia, consulte [Asistencia para NetScaler en Azure: licencia de suscripción con precio por hora](#).

- **Traiga su propia licencia (BYOL):** Si trae su propia licencia (BYOL), consulte la Guía de licencias de VPX en <http://support.citrix.com/article/CTX122426> Es necesario que:
 - Utilice el portal de licencias del sitio web de NetScaler para generar una licencia válida.
 - Cargue la licencia en la instancia.

Nota:

En un entorno de pila de Azure, **BYOL** es la única opción de licencia disponible.

- Licencias de **Check-in/Check-out de NetScaler VPX:** Para obtener más información, consulte **Licencias de Check-in/Check-out de NetScaler VPX**.

A partir de la versión 12.0 56.20 de NetScaler, NetScaler VPX Express para implementaciones locales y en la nube no requiere un archivo de licencia. Para obtener más información sobre NetScaler VPX Express, consulte la sección “Licencia de NetScaler VPX Express” de la [descripción general de licencias de NetScaler](#).

Rendimiento de VPX y tipos de instancias de Azure recomendados

Para obtener el rendimiento de VPX deseado, se recomiendan los siguientes tipos de instancias de Azure.

Rendimiento de VPX	Tipos de instancias de Azure			
	1 NIC/2			
	NIC de VPX	Tarjeta de red VPX 3	VPX hasta 8 NIC	
Hasta 200 Mbps	Standard_D2_v4	Standard_DS2_v2	Standard_DS4_v2	Standard_DS8_v2
Hasta 1 Gbps	Standard_D4_v4	Standard_DS4_v2	Standard_DS8_v2	Standard_DS16_v2
Hasta 5 Gbps	Estándar_D8_v5	Estándar_D8_v5	Estándar_D16_v5	Estándar_D32_v5
Hasta 10 Gbps	Estándar_D2_v5	Estándar_D8_v5	Estándar_D16_v5	

Puntos a tener en cuenta

- Para lograr un rendimiento óptimo en las instancias de NetScaler VPX con un rendimiento de 1 Gbps y 5 Gbps, debe habilitar la red acelerada de Azure.
Para obtener más información sobre cómo configurar redes aceleradas, consulte [Configurar una instancia de NetScaler VPX para usar redes aceleradas de Azure](#).
- Independientemente de la licencia por hora basada en suscripción adquirida en Azure Marketplace, en casos excepcionales, la instancia de NetScaler VPX implementada en Azure podría tener una licencia predeterminada de NetScaler. Esto ocurre debido a problemas con Azure Instance Metadata Service (IMDS).
- Realice un reinicio rápido antes de realizar cualquier cambio de configuración en la instancia de NetScaler VPX para habilitar la licencia NetScaler VPX correcta.

Compatibilidad con IPv6 para la instancia de NetScaler VPX en Azure

A partir de la versión 13.1-21.x, la instancia independiente de NetScaler VPX admite direcciones IPv6 en Azure. Puede configurar las direcciones IPv6 como direcciones VIP y SNIP en la instancia independiente de NetScaler VPX en la nube de Azure.

Para obtener información sobre cómo habilitar IPv6 en Azure, consulte la siguiente documentación de Azure:

- [¿Qué es IPv6 para la red virtual de Azure?](#)
- [Agregar IPv6 a una aplicación IPv4 en la red virtual de Azure: CLI de Azure](#)

- [Tipos de direcciones](#)

Para obtener información sobre cómo el dispositivo NetScaler admite IPv6, consulte [Protocolo de Internet versión 6](#).

Limitaciones de IPv6:

- Las implementaciones de IPv6 en NetScaler actualmente no admiten el escalado automático de backend de Azure.
- La implementación de alta disponibilidad de NetScaler VPX no admite IPv6.

Limitaciones

La ejecución de la solución de equilibrio de carga de NetScaler VPX en ARM impone las siguientes limitaciones:

- La arquitectura Azure no admite las siguientes funciones de NetScaler:
 - ARP gratuito (GARP)
 - Modo L2
 - VLAN etiquetada
 - Redirección dinámica
 - MAC virtual
 - USIP
 - Agrupar en clústeres

Nota:

Con la función de escalado automático de NetScaler Application Delivery Management (ADM) (implementación en la nube), las instancias de ADC admiten la agrupación en clústeres en todas las licencias. Para obtener información, consulte [Escalado automático de NetScaler VPX en Microsoft Azure mediante NetScaler ADM](#).

- Si espera que tenga que apagar y desasignar temporalmente la máquina virtual NetScaler VPX en cualquier momento, asigne una dirección IP interna estática al crear la máquina virtual. Si no asigna una dirección IP interna estática, Azure podría asignar a la máquina virtual una dirección IP diferente cada vez que se reinicie, y es posible que no se pueda acceder a la máquina virtual.
- Azure admite un rendimiento de VPX de hasta 10 Gbps. Para obtener más información, consulte la [hoja de datos de NetScaler VPX](#).
- Al utilizar una instancia de NetScaler VPX con un rendimiento superior a 3 Gbps, es posible que el rendimiento real de la red no coincida con el rendimiento especificado en la licencia de la instancia. Sin embargo, otras funciones, como el rendimiento de SSL y las transacciones SSL por segundo, podrían mejorar.

- El ID de implementación que genera Azure durante el aprovisionamiento de máquinas virtuales no está visible para el usuario en ARM. No puede usar el ID de implementación para implementar el dispositivo NetScaler VPX en ARM.
- Cuando se inicializa, la instancia NetScaler VPX admite funciones de edición estándar y de rendimiento de 20 Mbps.
- Las instancias NetScaler VPX en Azure con redes aceleradas habilitadas proporcionan un mejor rendimiento. Las instancias de NetScaler VPX admiten redes aceleradas de Azure a partir de la versión 13.0 compilación 76.x. Para habilitar las redes aceleradas en NetScaler VPX, Citrix recomienda utilizar un tipo de instancia de Azure que admita redes aceleradas.
- Para la implementación de Citrix Virtual Apps and Desktops, se puede configurar un servidor virtual VPN en una instancia VPX de los siguientes modos:
 - Modo básico, donde el parámetro del servidor virtual de VPN `ICAOnly` está activado. El modo Básico funciona completamente en una instancia de NetScaler VPX sin licencia.
 - Modo SmartAccess, donde el parámetro del servidor virtual de VPN `ICAOnly` está desactivado. El modo SmartAccess solo funciona para cinco usuarios de sesión de NetScaler AAA en una instancia de NetScaler VPX sin licencia.

Nota:

Para configurar la función SmartControl, debe aplicar una licencia Premium a la instancia de NetScaler VPX.

Terminología de Azure

October 17, 2024

A continuación se enumeran algunos de los términos de Azure que se utilizan en la documentación de NetScaler VPX Azure.

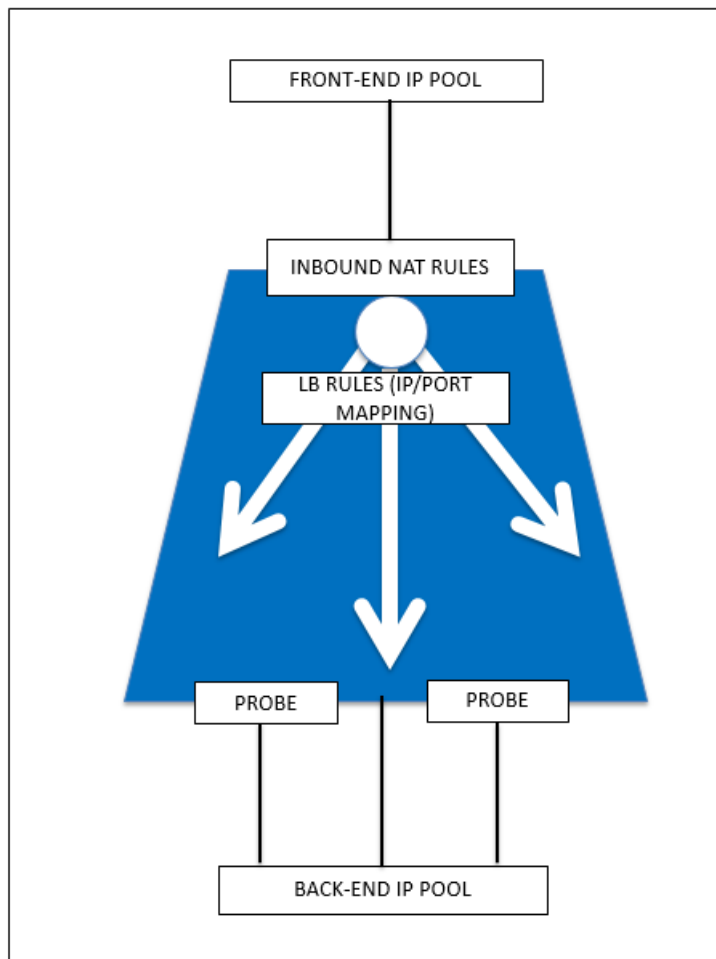
1. El equilibrador de carga de Azure es un recurso que distribuye el tráfico entrante entre los equipos de una red. El tráfico se distribuye entre máquinas virtuales definidas en un conjunto de equilibradores de carga. Un equilibrador de carga puede ser externo o orientado a Internet, o puede ser interno.
2. Azure Resource Manager (ARM): ARM es el nuevo marco de administración para los servicios de Azure. Azure Load Balancer se administra mediante API y herramientas basadas en ARM.
3. Grupo de direcciones de back-end: son direcciones IP asociadas a la NIC de máquina virtual (NIC) a la que se distribuirá la carga.

4. BLOB: Objeto binario grande: Cualquier objeto binario como un archivo o una imagen que se puede almacenar en el almacenamiento de Azure.
5. Configuración de IP de front-end: Un equilibrador de carga de Azure puede incluir una o más direcciones IP de front-end, también conocidas como IP virtuales (VIP). Estas direcciones IP sirven como entrada para el tráfico.
6. IP pública de nivel de instancia (ILPIP): Un ILPIP es una dirección IP pública que puede asignar directamente a su máquina virtual o instancia de rol, en lugar de al servicio en la nube en el que reside la máquina virtual o la instancia de rol. Esto no ocupa el lugar del VIP (IP virtual) que se asigna a su servicio en la nube. Más bien, es una dirección IP adicional que puede usar para conectarse directamente a su máquina virtual o instancia de rol.

Nota:

En el pasado, a un ILPIP se lo denominaba PIP, que significa IP pública.

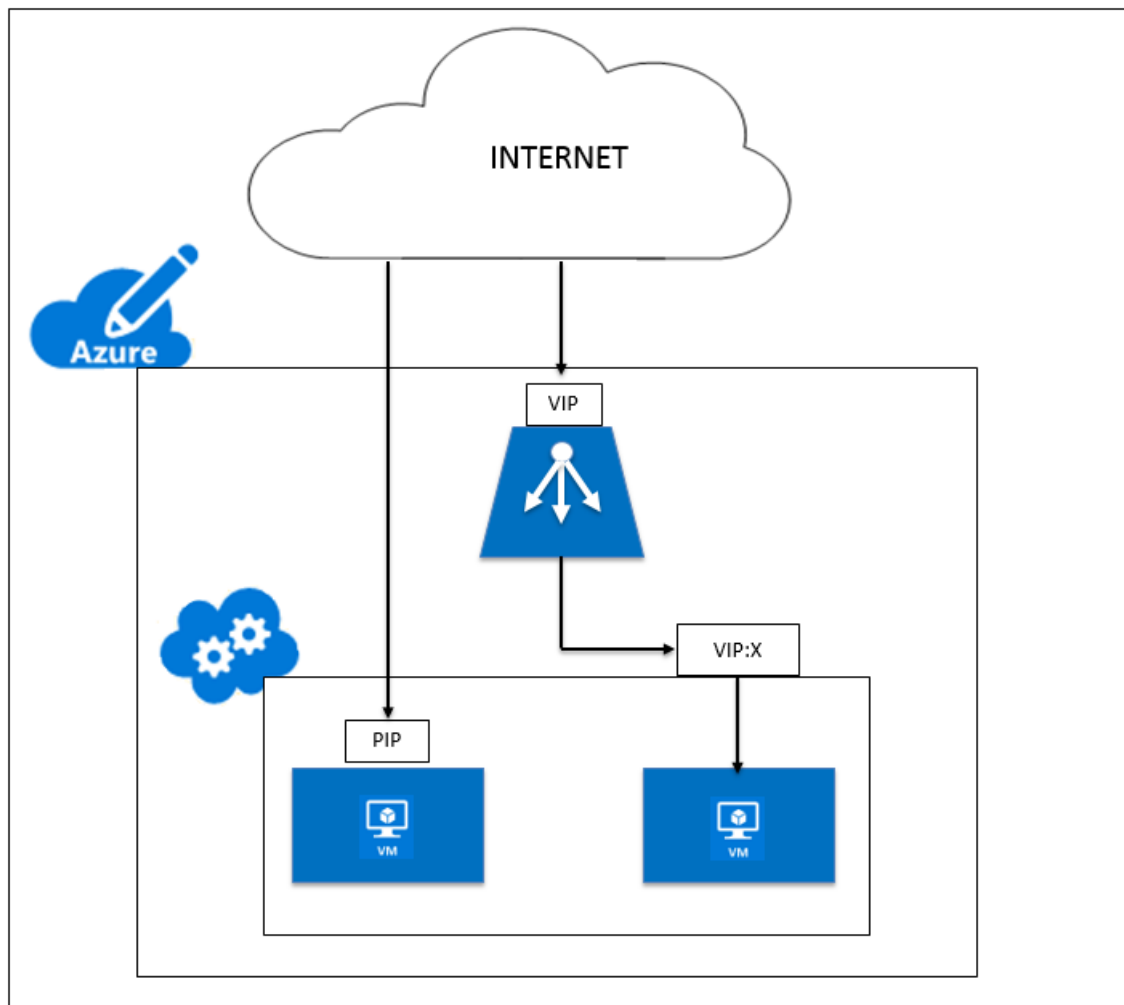
7. Reglas NAT entrantes: Contiene reglas que asignan un puerto público en el equilibrador de carga a un puerto para una máquina virtual específica en el grupo de direcciones back-end.
8. IP-config: Se puede definir como un par de direcciones IP (IP pública e IP privada) asociado a una NIC individual. En una configuración IP, la dirección IP pública puede ser NULL. Cada NIC puede tener varias IP-config asociadas, que pueden ser de hasta 255.
9. Reglas de equilibrio de carga: Propiedad de regla que asigna una combinación de puertos y IP de front-end dada a un conjunto de direcciones IP de back-end y combinación de puertos. Con una sola definición de un recurso de equilibrador de carga, puede definir varias reglas de equilibrio de carga, cada regla refleja una combinación de una IP de front-end y una IP de puerto y de back-end y un puerto asociado con máquinas virtuales.



10. Grupo de seguridad de red: contiene una lista de reglas de lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a las instancias de máquina virtual en una red virtual. Los NSG se pueden asociar con subredes o instancias individuales de máquinas virtuales dentro de esa subred. Cuando un grupo de seguridad de red está asociado a una subred, las reglas de ACL se aplican a todas las instancias de máquina virtual de esa subred. Además, el tráfico a una máquina virtual individual se puede restringir aún más asociando un grupo de seguridad de red directamente a esa máquina virtual.
11. Direcciones IP privadas: Se utilizan para la comunicación dentro de una red virtual de Azure y la red local cuando utiliza una Gateway VPN para extender la red a Azure. Las direcciones IP privadas permiten que los recursos de Azure se comuniquen con otros recursos de una red virtual o local a través de una Gateway VPN o un circuito ExpressRoute, sin utilizar una dirección IP accesible a Internet. En el modelo de implementación de Azure Resource Manager, se asocia una dirección IP privada con los siguientes tipos de recursos de Azure: Máquinas virtuales, equilibradores de carga internos (ILB) y puertas de enlace de aplicaciones.
12. Sondeos: Contiene sondeos de estado utilizados para comprobar la disponibilidad de instancias de máquinas virtuales en el grupo de direcciones back-end. Si una máquina virtual en par-

ticular no responde a los sondeos de estado durante algún tiempo, entonces se saca del servicio de tráfico. Los sondeos permiten realizar un seguimiento del estado de las instancias virtuales. Si falla un sondeo de estado, la instancia virtual se quitará automáticamente de rotación.

13. Direcciones IP públicas (PIP): PIP se utiliza para la comunicación con Internet, incluidos los servicios públicos de Azure y se asocia con máquinas virtuales, equilibradores de carga orientados a Internet, puertas de enlace VPN y puertas de enlace de aplicaciones.
14. Región: área dentro de una geografía que no cruza las fronteras nacionales y que contiene uno o varios centros de datos. Los precios, los servicios regionales y los tipos de oferta están expuestos a nivel regional. Una región suele estar emparejada con otra región, que puede estar hasta varios cientos de millas de distancia, para formar un par regional. Los pares regionales se pueden utilizar como mecanismo para la recuperación ante desastres y casos de alta disponibilidad. También se conoce generalmente como ubicación.
15. Grupo de recursos: Un contenedor en el Administrador de recursos contiene recursos relacionados para una aplicación. El grupo de recursos puede incluir todos los recursos de una aplicación, o solo aquellos recursos que se agrupan lógicamente.
16. Cuenta de almacenamiento: Una cuenta de almacenamiento de Azure le da acceso a los servicios de blob, colas, tablas y archivos de Azure en Almacenamiento de Azure. La cuenta de almacenamiento proporciona el espacio de nombres único para los objetos de datos de almacenamiento de Azure.
17. Máquina virtual: Implementación de software de un equipo físico que ejecuta un sistema operativo. Varias máquinas virtuales pueden ejecutarse simultáneamente en el mismo hardware. En Azure, las máquinas virtuales están disponibles en una variedad de tamaños.
18. Una red virtual de Azure es una representación de su propia red en la nube. Es un aislamiento lógico de la nube de Azure dedicada a su suscripción. Puede controlar completamente los bloques de direcciones IP, la configuración de DNS, las directivas de seguridad y las tablas de redirecciones dentro de esta red. También puede segmentar aún más su vNet en subredes e iniciar máquinas virtuales de Azure IaaS y servicios en la nube (instancias de rol PaaS). Además, puede conectar la red virtual a la red local mediante una de las opciones de conectividad disponibles en Azure. En esencia, puede expandir su red a Azure, con un control completo de los bloques de direcciones IP con el beneficio de Azure a escala empresarial.



Arquitectura de red para instancias NetScaler VPX en Microsoft Azure

October 17, 2024

En Azure Resource Manager (ARM), una máquina virtual (VM) NetScaler VPX reside en una red virtual. Se puede crear una única interfaz de red en una subred dada de la Red Virtual y se puede conectar a la instancia VPX. Puede filtrar el tráfico de red hacia y desde una instancia VPX en una red virtual de Azure con un grupo de seguridad de red. Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o saliente desde una instancia VPX. Para obtener más información, consulte [Grupos de seguridad](#).

El grupo de seguridad de red filtra las solicitudes a la instancia de NetScaler VPX y la instancia VPX las envía a los servidores. La respuesta de un servidor sigue la misma ruta en sentido inverso. El grupo de seguridad de red se puede configurar para filtrar una sola VM VPX o, con subredes y redes virtuales,

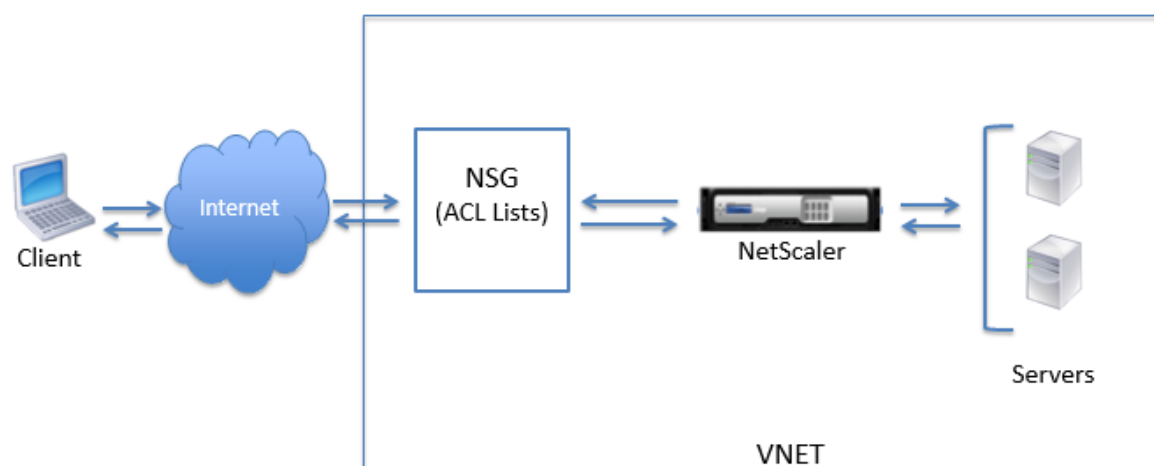
puede filtrar el tráfico en la implementación de varias instancias VPX.

La NIC contiene detalles de configuración de red como la red virtual, las subredes, la dirección IP interna y la dirección IP pública.

Mientras esté en ARM, es bueno conocer las siguientes direcciones IP que se utilizan para acceder a las VM implementadas con una sola NIC y una sola dirección IP:

- La dirección IP pública (PIP) es la dirección IP orientada a Internet configurada directamente en la NIC virtual de la máquina virtual de NetScaler. Esto le permite acceder directamente a una máquina virtual desde la red externa.
- La dirección IP de NetScaler (también conocida como NSIP) es la dirección IP interna configurada en la máquina virtual. No es enrutable.
- La dirección IP virtual (VIP) se configura mediante el NSIP y un número de puerto. Los clientes acceden a los servicios de NetScaler a través de la dirección PIP, y cuando la solicitud llega a la NIC de la máquina virtual NetScaler VPX o el equilibrador de carga de Azure, el VIP se traduce a IP interna (NSIP) y número de puerto interno.
- La dirección IP interna es la dirección IP interna privada de la máquina virtual del grupo de espacio de direcciones de la red virtual. No se puede acceder a esta dirección IP desde la red externa. Esta dirección IP es dinámica de forma predeterminada, a menos que la establezca en estática. El tráfico de Internet se enruta a esta dirección de acuerdo con las reglas creadas en el grupo de seguridad de red. El grupo de seguridad de red se integra con la NIC para enviar selectivamente el tipo de tráfico correcto al puerto correcto de la NIC, lo que depende de los servicios configurados en la máquina virtual.

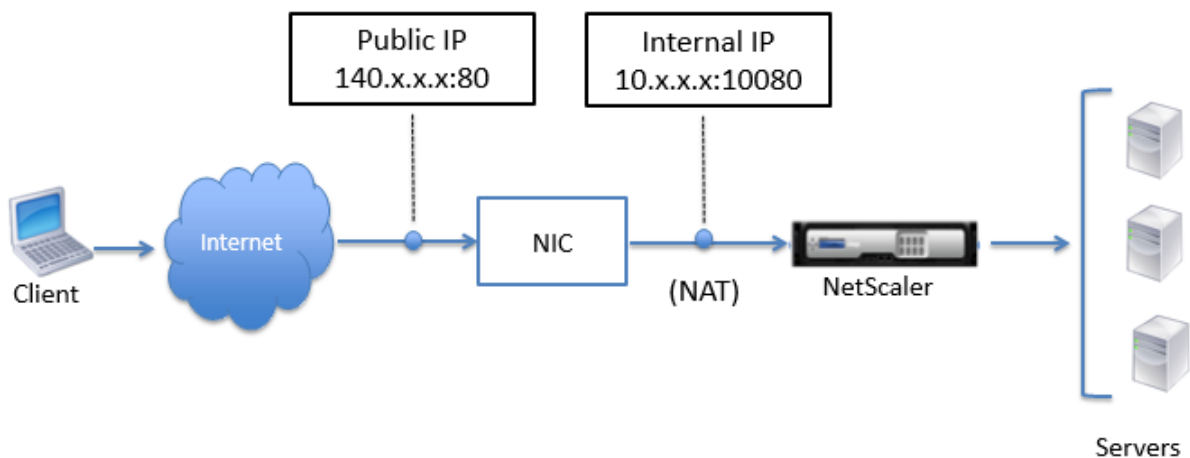
La siguiente ilustración muestra cómo fluye el tráfico de un cliente a un servidor a través de una instancia de NetScaler VPX aprovisionada en ARM.



Flujo de tráfico a través de la traducción de direcciones de red

También puede solicitar una dirección IP pública (PIP) para su instancia de NetScaler VPX (nivel de instancia). Si utiliza este PIP directo en el nivel de VM, no necesita definir reglas de entrada y salida para interceptar el tráfico de red. La solicitud entrante de Internet se recibe directamente en la máquina virtual. Azure realiza la traducción de direcciones de red (NAT) y reenvía el tráfico a la dirección IP interna de la instancia VPX.

La siguiente ilustración muestra cómo Azure realiza la traducción de direcciones de red para asignar la dirección IP interna de NetScaler.



En este ejemplo, la IP pública asignada al grupo de seguridad de red es 140.x.x.x y la dirección IP interna es 10.x.x.x. Cuando se definen las reglas de entrada y salida, el puerto HTTP público 80 se define como el puerto en el que se reciben las solicitudes del cliente, y el puerto privado correspondiente, 10080, se define como el puerto en el que escucha la instancia de NetScaler VPX. La solicitud del cliente se recibe en la dirección IP pública (140.x.x.x). Azure realiza la traducción de direcciones de red para asignar el PIP a la dirección IP interna 10.x.x.x en el puerto 10080 y reenvía la solicitud del cliente.

Nota:

Las máquinas virtuales NetScaler VPX de alta disponibilidad están controladas por balanceadores de carga externos o internos que tienen definidas reglas de entrada para controlar el tráfico de equilibrio de carga. El tráfico externo es interceptado primero por estos equilibradores de carga y el tráfico se desvía de acuerdo con las reglas de equilibrio de carga configuradas, que tienen grupos back-end, reglas NAT y sondeos de estado definidos en los equilibradores de carga.

Directrices de uso de puertos

Puede configurar más reglas entrantes y salientes en un grupo de seguridad de red mientras crea la instancia NetScaler VPX o después de aprovisionar la máquina virtual. Cada regla de entrada y salida está asociada con un puerto público y un puerto privado.

Antes de configurar las reglas de grupo de seguridad de red, tenga en cuenta las siguientes pautas relativas a los números de puerto que puede utilizar:

1. La instancia de NetScaler VPX reserva los siguientes puertos. No se pueden definir como puertos privados cuando se utiliza la dirección IP pública para las solicitudes de Internet.

Puertos 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

Sin embargo, si desea que los servicios orientados a Internet, como el VIP, utilicen un puerto estándar (por ejemplo, el puerto 443), debe crear una asignación de puertos mediante el grupo de seguridad de red. A continuación, el puerto estándar se asigna a un puerto diferente configurado en NetScaler para este servicio VIP.

Por ejemplo, un servicio VIP podría estar ejecutándose en el puerto 8443 en la instancia VPX, pero asignarse al puerto público 443. Por lo tanto, cuando el usuario accede al puerto 443 a través de la IP pública, la solicitud se dirige al puerto privado 8443.

2. La dirección IP pública no admite protocolos en los que la asignación de puertos se abre dinámicamente, como FTP pasivo o ALG.
3. La alta disponibilidad no funciona para el tráfico que utiliza una dirección IP pública (PIP) asociada a una instancia VPX, en lugar de un PIP configurado en el equilibrador de carga de Azure.

Nota:

En Azure Resource Manager, una instancia de NetScaler VPX está asociada a dos direcciones IP: Una dirección IP pública (PIP) y una dirección IP interna. Mientras el tráfico externo se conecta al PIP, la dirección IP interna o el NSIP no se puede enrutar. Para configurar VIP en VPX, utilice la dirección IP interna y cualquiera de los puertos libres disponibles. No utilice el PIP para configurar VIP.

Configurar una instancia independiente de NetScaler VPX

October 17, 2024

Puede aprovisionar una sola instancia de NetScaler VPX en el portal Azure Resource Manager (ARM) de forma independiente creando la máquina virtual y configurando otros recursos.

Antes de comenzar

Compruebe que tiene lo siguiente:

- Una cuenta de usuario de Microsoft Azure
- Acceso al Administrador de recursos de Microsoft Azure
- SDK de Microsoft Azure
- Microsoft Azure PowerShell

En la página [Microsoft Azure Portal](#), inicie sesión en el portal de Azure Resource Manager proporcionando su nombre de usuario y contraseña.

Nota:

En el portal ARM, al hacer clic en una opción de un panel se abre un nuevo panel a la derecha. Navegue de un panel a otro para configurar el dispositivo.

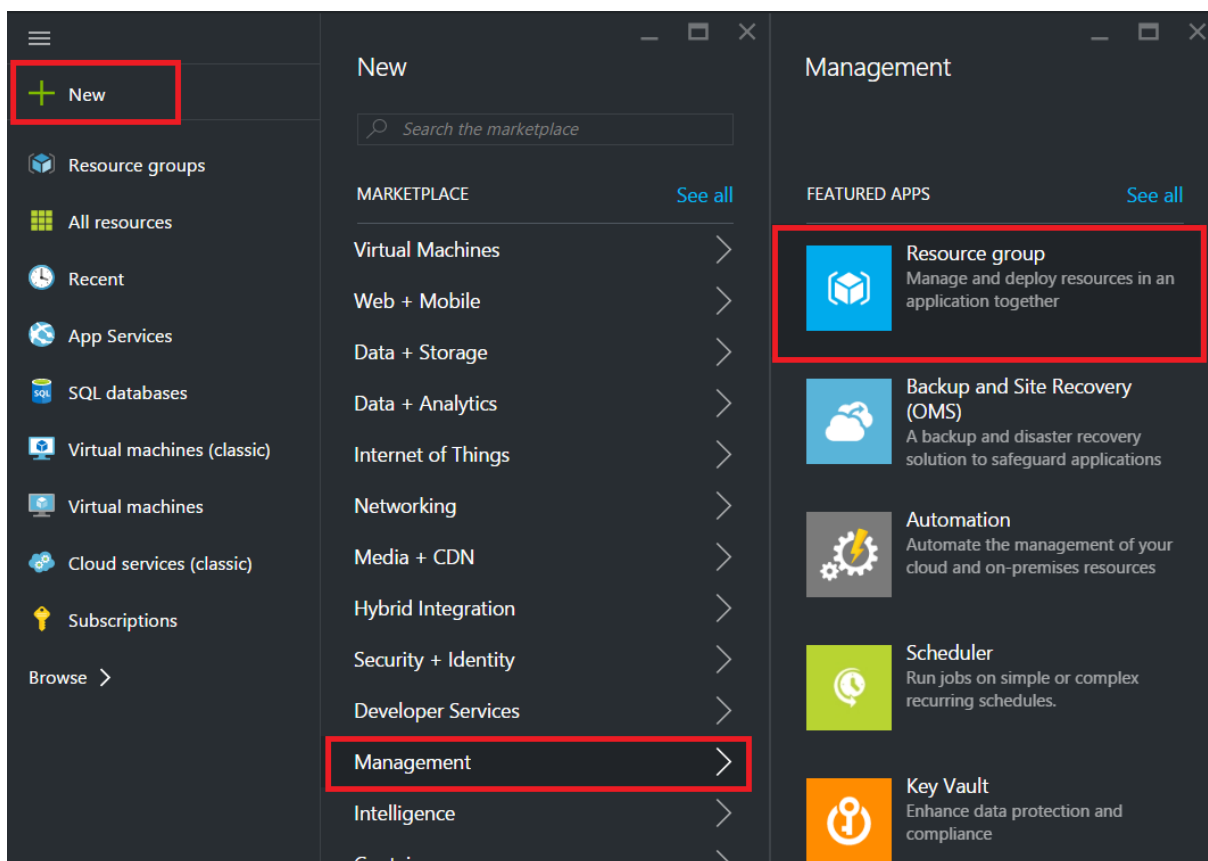
Resumen de los pasos de configuración

1. Configurar un grupo de recursos
2. Configurar un grupo de seguridad de red
3. Configurar la red virtual y sus subredes
4. Configurar una cuenta de almacenamiento
5. Configurar un conjunto de disponibilidad
6. Configure una instancia de NetScaler VPX.

Configurar un grupo de recursos

Cree un nuevo grupo de recursos que sea un contenedor para todos sus recursos. Utilice el grupo de recursos para implementar, administrar y supervisar los recursos como grupo.

1. Haga clic en **Nuevo > Administración > Grupo de recursos**.
2. En el panel **Grupo de recursos**, introduzca los siguientes detalles:
 - Nombre del grupo de recursos
 - Ubicación del grupo de recursos
3. Haga clic en **Create**.



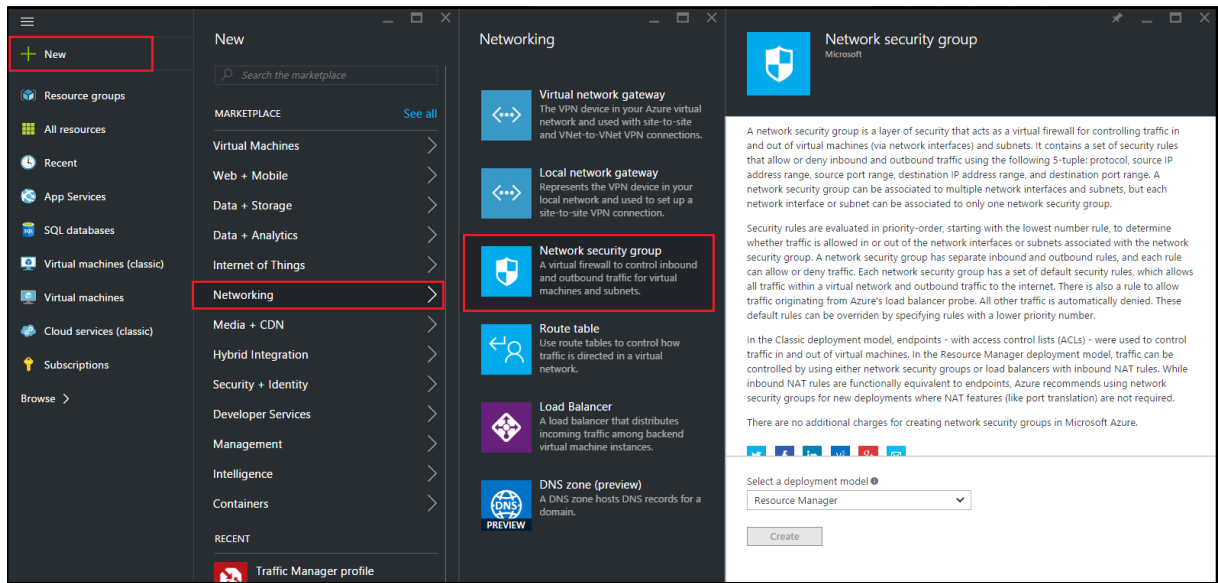
Configurar un grupo de seguridad de red

Cree un grupo de seguridad de red para asignar reglas entrantes y salientes para controlar el tráfico entrante y saliente dentro de la red virtual. El grupo de seguridad de red le permite definir reglas de seguridad para una única máquina virtual y también definir reglas de seguridad para una subred de red virtual.

1. Haga clic en **Nuevo > Redes > Grupo de seguridad de red**.
2. En el panel **Crear grupo de seguridad de red**, introduzca los siguientes detalles y, a continuación, haga clic en **Crear**.
 - Nombre: escriba un nombre para el grupo de seguridad
 - Grupo de recursos: seleccione el grupo de recursos de la lista desplegable

Nota:

Asegúrese de haber seleccionado la ubicación correcta. La lista de recursos que aparecen en la lista desplegable es diferente para diferentes ubicaciones.

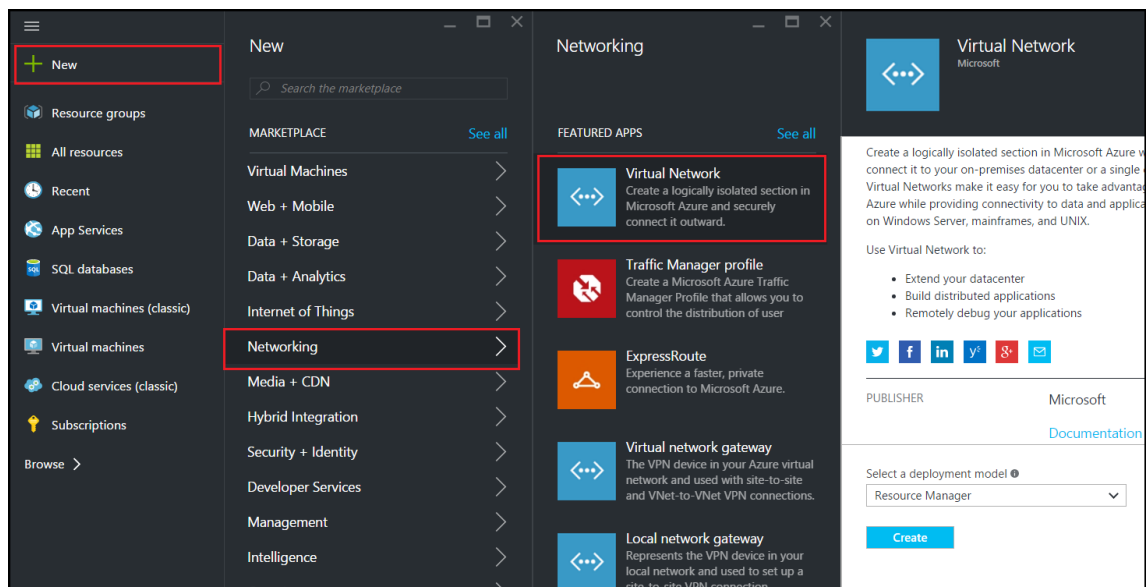


Configurar una red virtual y subredes

Las redes virtuales en ARM proporcionan una capa de seguridad y aislamiento a sus servicios. Las máquinas virtuales y los servicios que forman parte de la misma red virtual pueden tener acceso entre sí.

Siga estos pasos para crear una red virtual y subredes.

1. Haga clic en **Nuevo > Redes > Red virtual**.
2. En el panel **Red virtual**, asegúrese de que el modo de implementación es **Administrador de recursos** y haga clic en **Crear**.



3. En el panel **Crear red virtual**, escriba los siguientes valores y, a continuación, haga clic en **Crear**.
 - Nombre de la red virtual
 - Espacio de direcciones: escriba el bloque de direcciones IP reservado para la red virtual
 - Subred: escriba el nombre de la primera subred (creará la segunda subred más adelante en este paso)
 - Intervalo de direcciones de subred: escriba el bloque de direcciones IP reservadas de la subred
 - Seleccione el grupo de recursos creado anteriormente en la lista desplegable

Create virtual network

* Name
NetScalerVNet ✓

* Address space ⓘ
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 ▼

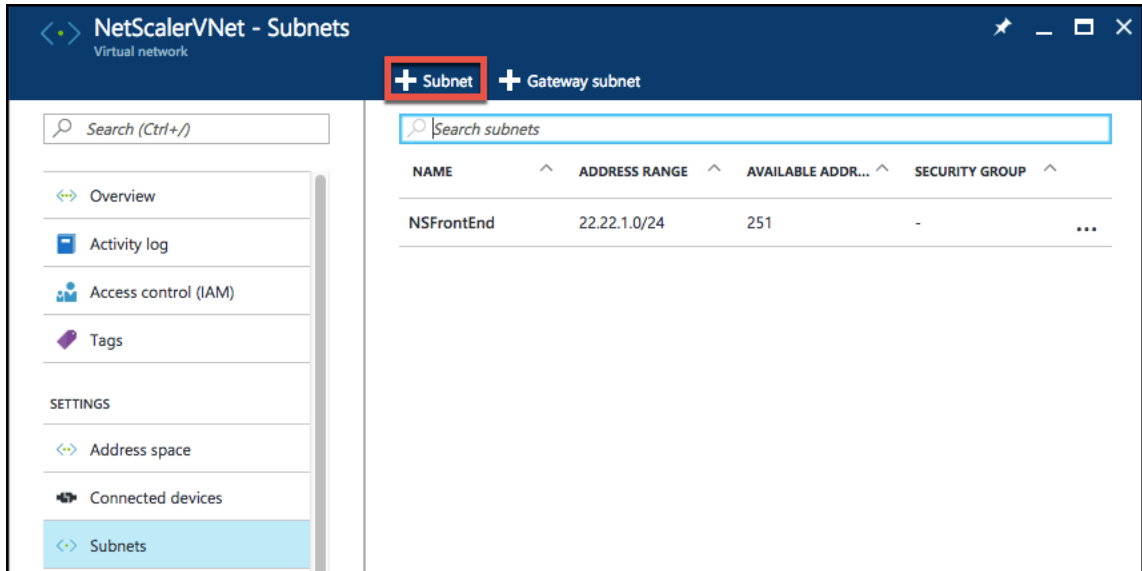
* Location
Southeast Asia ▼

Pin to dashboard

Create [Automation options](#)

Configurar la segunda subred

1. Seleccione la red virtual recién creada en el panel **Todos los recursos** y, en el panel **Configuración**, haga clic en **Subredes**.



2. Haga clic en **+Subred** y cree la segunda subred introduciendo los siguientes detalles.
 - Nombre de la segunda subred
 - Escriba el bloque de direcciones IP reservado de la segunda subred
 - Grupo de seguridad de red: seleccione el grupo de seguridad de red de la lista desplegable
3. Haga clic en **Create**.

Add subnet
NetScalerVNet

* 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 >

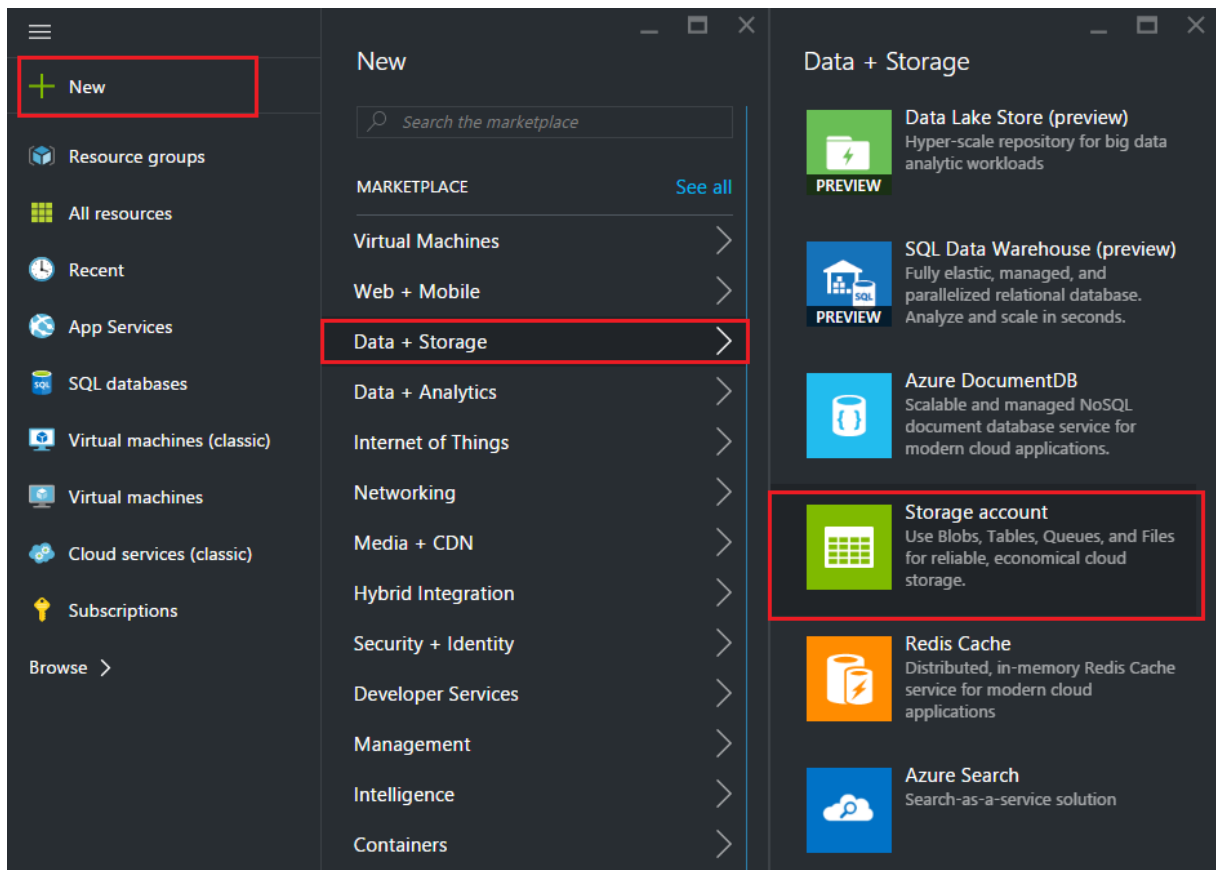
OK

Configurar una cuenta de almacenamiento

El almacenamiento de infraestructura ARM IaaS incluye todos los servicios en los que podemos almacenar datos en forma de blobs, tablas, colas y archivos. También puede crear aplicaciones utilizando estas formas de datos de almacenamiento en ARM.

Crea una cuenta de almacenamiento para almacenar todos tus datos.

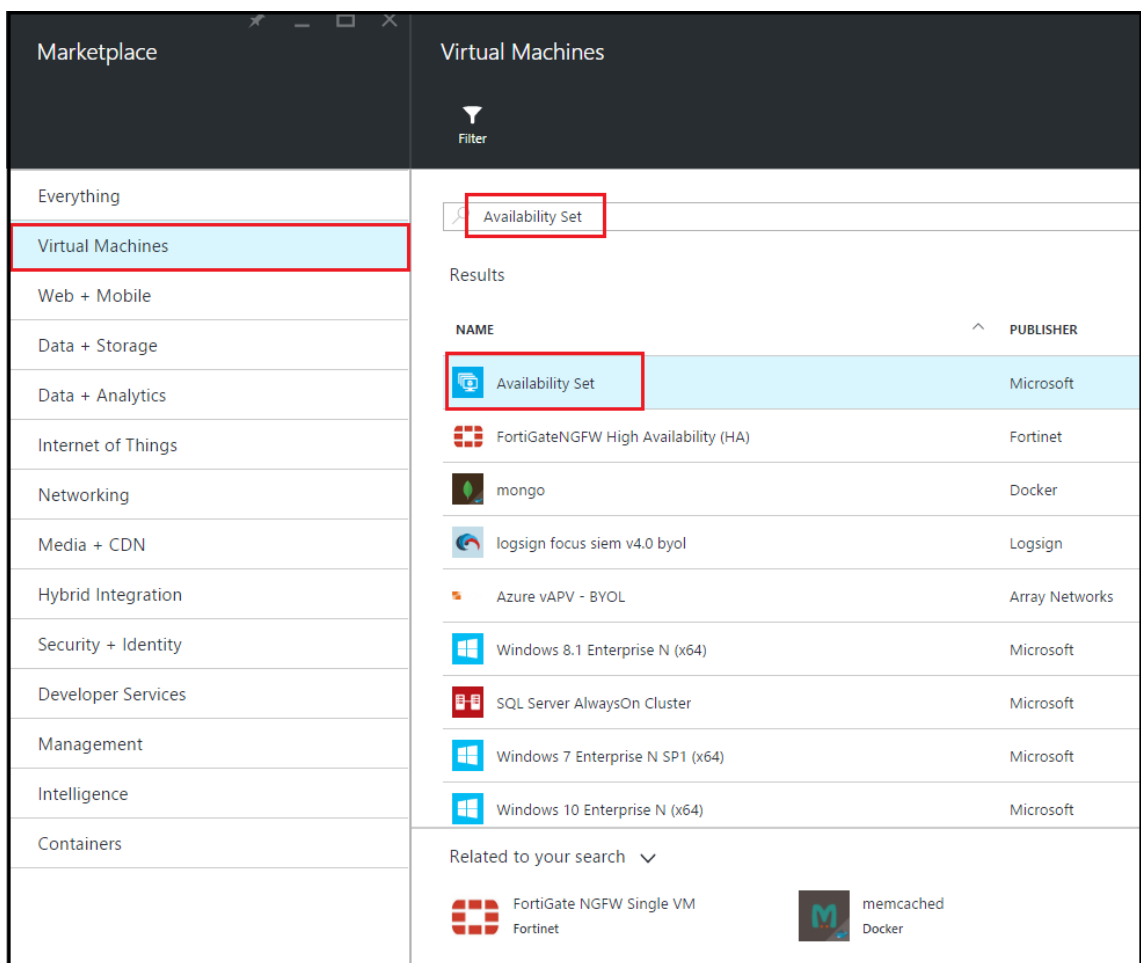
1. Haga clic en **+Nuevo > Datos + Almacenamiento > Cuenta de almacenamiento**.
2. En el panel **Crear cuenta de almacenamiento**, introduzca los siguientes detalles:
 - Nombre de la cuenta
 - Modo de implementación: asegúrese de seleccionar **Resource Manager**
 - Tipo de cuenta: seleccione **Propósito general** en la lista desplegable
 - Replicación: seleccione **Almacenamiento con redundancia local** en la lista desplegable
 - Grupo de recursos: seleccione el grupo de recursos recién creado en la lista desplegable
3. Haga clic en **Create**.



Configurar un conjunto de disponibilidad

Un conjunto de disponibilidad garantiza que al menos una máquina virtual se mantenga en funcionamiento en caso de mantenimiento planificado o no planificado. Dos o más máquinas virtuales bajo el mismo “conjunto de disponibilidad” se colocan en diferentes dominios de fallas para lograr servicios redundantes.

1. Haz clic en **+Nuevo**.
2. Haga clic en **Ver todo** en el panel MARKETPLACE y, a continuación, en **Máquinas virtuales**.
3. Busque el conjunto de disponibilidad y, a continuación, seleccione Entidad de **conjunto de disponibilidad** en la lista que se muestra.



4. Haga clic en **Crear y**, en el panel **Crear conjunto de disponibilidad**, introduzca los siguientes detalles:
 - Nombre del conjunto
 - Grupo de recursos: seleccione el grupo de recursos recién creado en la lista desplegable
5. Haga clic en **Create**.

The screenshot shows a 'Create availability set' dialog box. It contains the following fields and options:

- Name:** A text input field containing 'AvSet' with a green checkmark on the right.
- Fault domains:** A slider control with a blue bar and a numeric input field set to '3'.
- Update domains:** A slider control with a blue bar and a numeric input field set to '5'.
- Subscription:** A dropdown menu showing 'Microsoft Azure Enterprise'.
- Resource group:** Radio buttons for 'Create new' and 'Use existing' (selected), followed by a dropdown menu showing 'ResGroup'.
- Location:** A dropdown menu showing 'Southeast Asia'.
- Create:** A blue button at the bottom of the form.

Configurar una instancia de NetScaler VPX

Cree una instancia de NetScaler VPX en la red virtual. Obtenga la imagen de NetScaler VPX de Azure Marketplace y, a continuación, utilice el portal Azure Resource Manager para crear una instancia de NetScaler VPX.

Antes de empezar a crear la instancia de NetScaler VPX, asegúrese de haber creado una red virtual con las subredes necesarias en las que reside la instancia. Puede crear redes virtuales durante el

Provisioning de VM, pero sin la flexibilidad necesaria para crear subredes diferentes. Para obtener información sobre la creación de redes virtuales, consulte <http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/>.

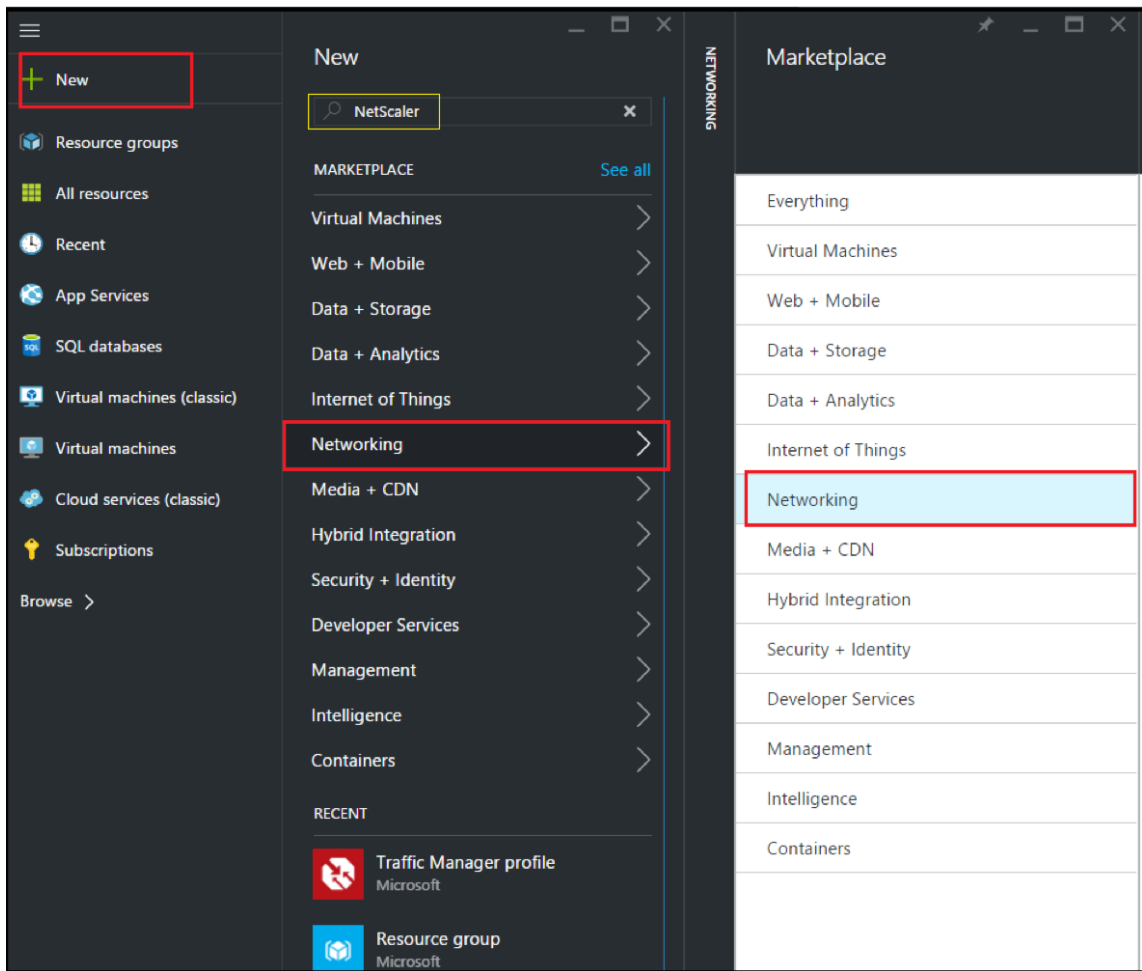
Si lo desea, configure la conectividad del servidor DNS y la VPN que permita a una máquina virtual acceder a los recursos de Internet.

Nota:

Citrix recomienda crear un grupo de recursos, un grupo de seguridad de red, una red virtual y otras entidades antes de aprovisionar la máquina virtual NetScaler VPX, de modo que la información de la red esté disponible durante el aprovisionamiento.

1. Haz clic en **+Nuevo > Redes**.
2. Haga clic en **Ver todo** y, en el panel Redes, en **NetScaler 13.0**.
3. Seleccione **Bring Your Own License de NetScaler 13.0 VPX** en la lista de planes de software.

Como forma rápida de encontrar cualquier entidad en el portal ARM, también puede escribir el nombre de la entidad en el cuadro de búsqueda de Azure Marketplace y pulsar <Enter>. Escriba NetScaler en el cuadro de búsqueda para buscar las imágenes de NetScaler.



Nota:

Asegúrese de seleccionar la imagen más reciente. Es posible que la imagen de NetScaler tenga el número de versión en el nombre.

4. En la página **NetScaler VPX Bring Your Own License**, en la lista desplegable, seleccione **Resource Manager** y haga clic en **Crear**.

5. En el panel **Crear máquina virtual**, especifique los valores necesarios en cada sección para crear una máquina virtual. Haga clic en **Aceptar** en cada sección para guardar la configuración.

Básico:

- Nombre: especifique un nombre para la instancia de NetScaler VPX
- Tipo de disco de máquina virtual: seleccione SSD (valor predeterminado) o HDD en el menú desplegable
- Nombre de usuario y contraseña: especifique un nombre de usuario y una contraseña para acceder a los recursos del grupo de recursos que ha creado
- Tipo de autenticación: seleccione clave pública o contraseña SSH

- Grupo de recursos: seleccione el grupo de recursos que ha creado en la lista desplegable

Puede crear un grupo de recursos aquí, pero Citrix recomienda crear un grupo de recursos a partir de los grupos de recursos de Azure Resource Manager y, a continuación, seleccionar el grupo en la lista desplegable.

Nota:

En un entorno de pila de Azure, además de los parámetros básicos, especifique los siguientes parámetros:

- Dominio de Azure Stack
- Arrendatario de Azure Stack (opcional)
- Cliente Azure (opcional)
- Secreto de cliente de Azure (opcional)

Tamaño:

Según el tipo de disco de la máquina virtual, SDD o HDD, que haya seleccionado en la configuración básica, se muestran los tamaños de los discos.

- Seleccione un tamaño de disco según sus necesidades y haga clic en **Seleccionar**.

Configuración:

- Seleccione el tipo de disco predeterminado (estándar)
- Cuenta de almacenamiento: selecciona la cuenta de almacenamiento
- Red virtual: seleccione la red virtual
- Subred: establece la dirección de la subred
- Dirección IP pública: seleccione el tipo de asignación de direcciones IP
- Grupo de seguridad de red: seleccione el grupo de seguridad que ha creado. Asegúrese de que las reglas de entrada y salida estén configuradas en el grupo de seguridad.
- Conjunto de disponibilidad: seleccione el conjunto de disponibilidad en el cuadro del menú desplegable

Resumen:

Los ajustes de configuración se validan y la página de resumen muestra el resultado de la validación. Si se produce un error en la validación, la página de resumen muestra el motivo del error. Vuelva a la sección en particular y realice los cambios necesarios. Si se pasa la validación, haga clic en **Aceptar**.

Comprar:

Revisa los detalles de la oferta y las condiciones legales en la página de compra y haz clic en **Comprar**.

Para una implementación de alta disponibilidad, cree dos instancias independientes de NetScaler VPX en el mismo conjunto de disponibilidad y en el mismo grupo de recursos para implementarlas en una configuración activa y en espera.

Configuración de varias direcciones IP para una instancia independiente NetScaler VPX

October 17, 2024

En esta sección se explica cómo configurar una instancia independiente de NetScaler VPX con varias direcciones IP, en Azure Resource Manager (ARM). La instancia VPX puede tener una o más NIC conectadas y cada NIC puede tener asignadas una o más direcciones IP públicas y privadas estáticas o dinámicas. Puede asignar varias direcciones IP como NSIP, VIP, SNIP, etc.

Para obtener más información, consulte la documentación de Azure [Asignar varias direcciones IP a máquinas virtuales mediante el portal de Azure](#).

Si desea utilizar comandos de PowerShell, consulte [Configuración de varias direcciones IP para una instancia de NetScaler VPX en modo independiente mediante comandos de PowerShell](#).

Caso de uso

En este caso, un dispositivo NetScaler VPX independiente se configura con una única NIC conectada a una red virtual (VNET). La NIC está asociada a tres configuraciones IP (ipconfig), cada servidor tiene un propósito diferente, como se muestra en la tabla.

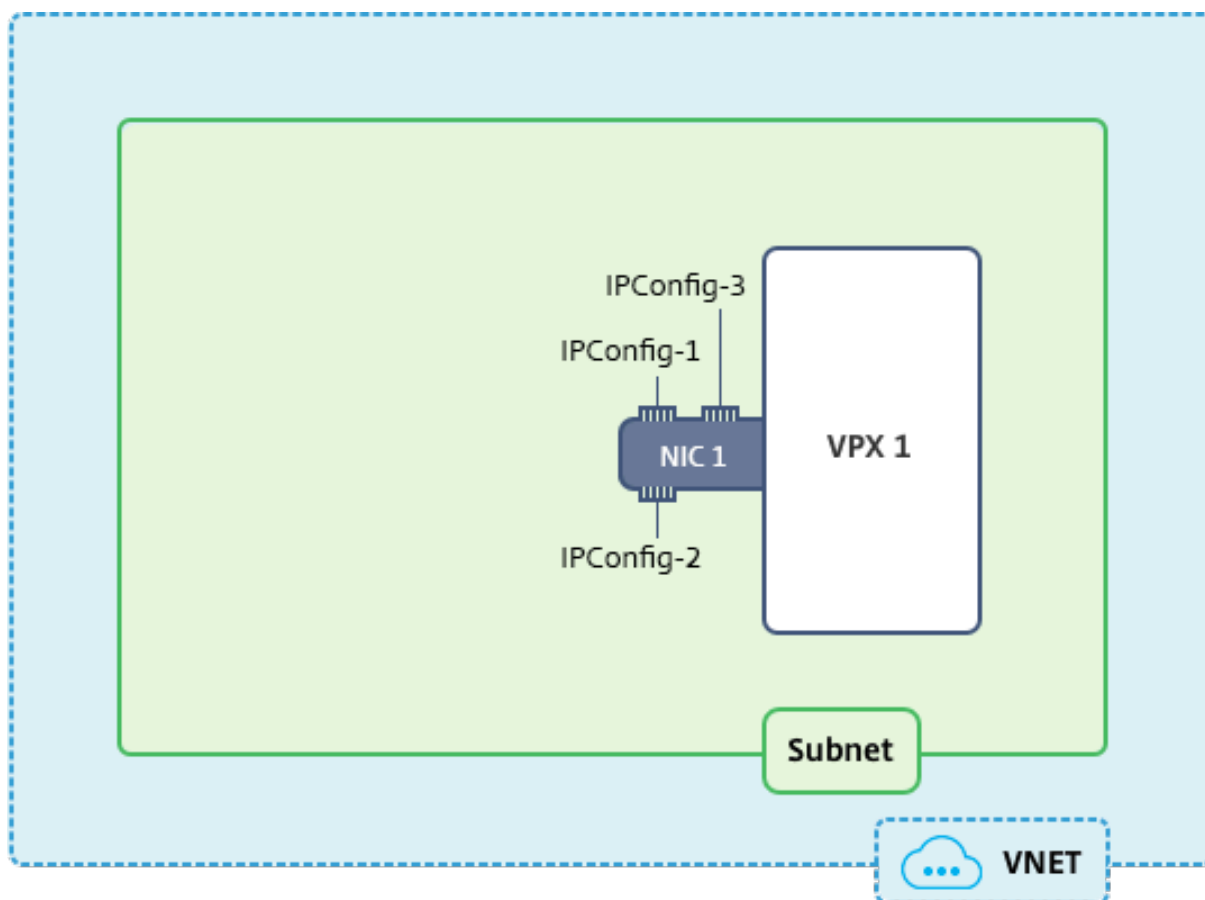
Configuración IP	Asociada con	Propósito
ipconfig1	Dirección IP pública estática; dirección IP privada estática	Sirve tráfico de administración
ipconfig2	Dirección IP pública estática; dirección privada estática	Sirve tráfico del lado del cliente
ipconfig3	Dirección IP privada estática	Se comunica con servidores back-end

Nota:

IPConfig-3 no está asociada a ninguna dirección IP pública.

Diagrama: Topología

Aquí está la representación visual del caso de uso.

**Nota:**

En una implementación Multi-NIC, Multi-IP Azure NetScaler VPX, la IP privada asociada a la principal (primera) `IPConfig` de la NIC principal (primera) se agrega automáticamente como NSIP de administración del dispositivo. Las restantes direcciones IP privadas asociadas `IPConfigs` deben agregarse a la instancia VPX como VIP o SNIP mediante el comando `add ns ip`, de acuerdo con sus requisitos.

Antes de comenzar

Antes de empezar, cree una instancia VPX siguiendo los pasos que se indican en este enlace:

[Configurar una instancia independiente de NetScaler VPX](#)

Para este caso de uso, se crea la instancia VPX NSDoc0330VM.

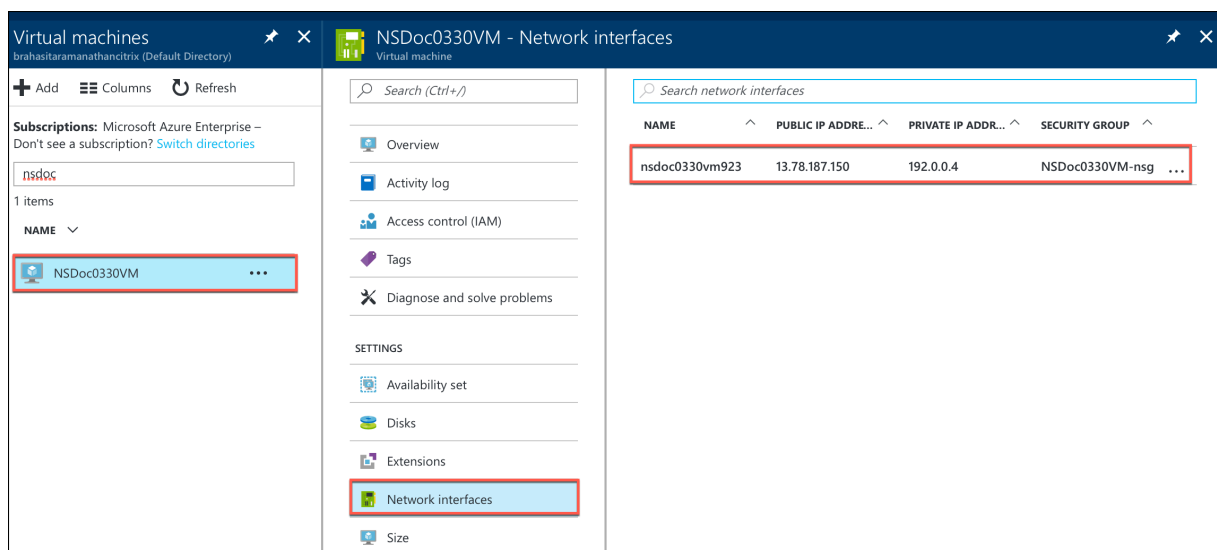
Procedimiento para configurar varias direcciones IP para una instancia de NetScaler VPX en modo independiente.

Para configurar varias direcciones IP para un dispositivo NetScaler VPX en modo independiente:

1. Agregar direcciones IP a la VM
2. Configurar direcciones IP propiedad de NetScaler

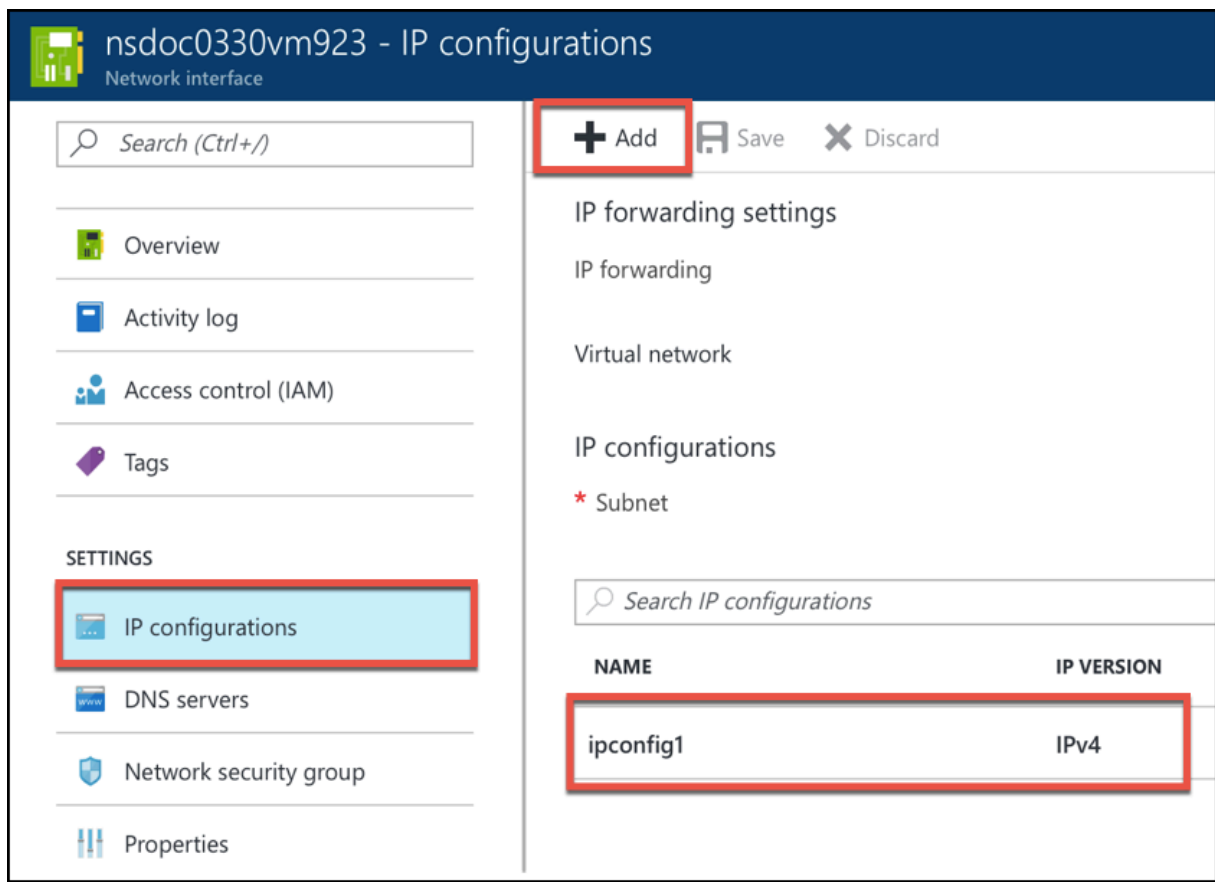
Paso 1: Agregar direcciones IP a la máquina virtual

1. En el portal, haga clic en **Más servicios > escriba máquinas virtuales** en el cuadro de filtro y, a continuación, haga clic en **Máquinas virtuales**.
2. En el blade de **máquinas virtuales**, haga clic en la máquina virtual a la que desea agregar direcciones IP. Haga clic en **Interfaces de red** en el blade de máquina virtual que aparece y, a continuación, seleccione la interfaz de red.



En el blade que aparece para la NIC seleccionada, haga clic en **Configuraciones IP**. Se muestra la configuración IP existente que se asignó al crear la máquina virtual, **ipconfig1**. Para este caso de uso, asegúrese de que las direcciones IP asociadas con ipconfig1 sean estáticas. A continuación, cree dos configuraciones IP más: Ipconfig2 (VIP) e ipconfig3 (SNIP).

Para crear más **ipconfigs**, crea **Agregar**.



En la ventana **Agregar configuración de IP**, introduzca un **nombre**, especifique el método de asignación como **estático**, introduzca una dirección IP (192.0.0.5 para este caso de uso) y habilite la **dirección IP pública**.

Nota:

Antes de agregar una dirección IP privada estática, compruebe la disponibilidad de la dirección IP y asegúrese de que la dirección IP pertenece a la misma subred a la que está conectada la NIC.

Add IP configuration
nsdoc0330vm923

* Name
ipconfig2 ✓

Type
Primary Secondary

i Primary IP configuration already exists

Private IP address settings

Allocation
Dynamic Static

* IP address
192.0.0.5 ✓

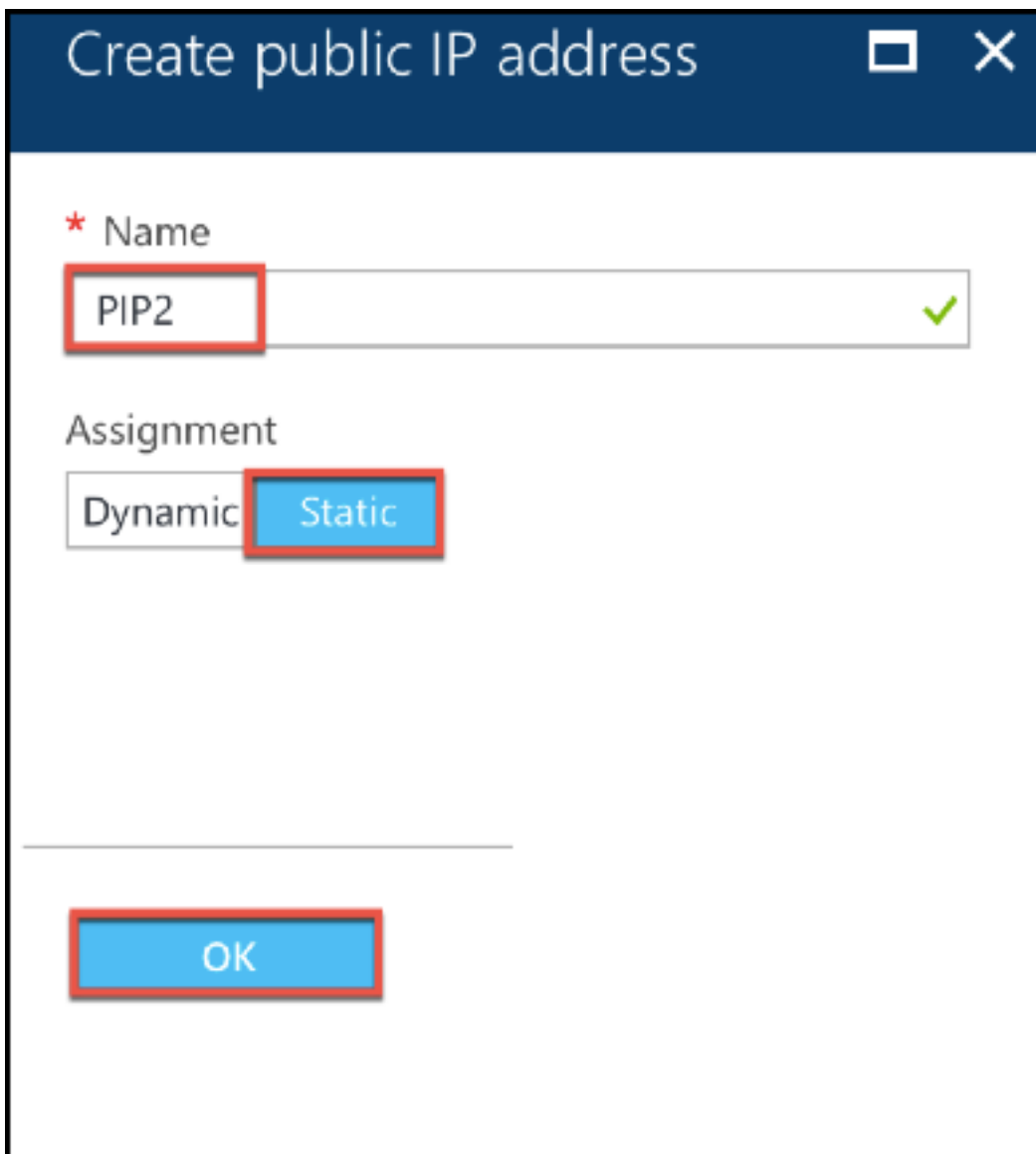
Public IP address
Disabled Enabled

* IP address
Configure required settings >

A continuación, haga clic en **Configurar los ajustes necesarios** para crear una dirección IP pública estática para ipconfig2.

De forma predeterminada, las direcciones IP públicas son dinámicas. Para asegurarse de que la máquina virtual utilice siempre la misma dirección IP pública, cree una IP pública estática.

En el módulo Crear dirección IP pública, añada un nombre y, en Asignación, haga clic en **Estático**. Y, a continuación, haga clic en **Aceptar**.



Nota:

Incluso si establece el método de asignación como estático, no puede especificar la dirección IP real asignada al recurso IP público. En su lugar, se asigna desde un conjunto de direcciones IP disponibles en la ubicación de Azure en la que se creó el recurso.

Siga los pasos para agregar una configuración IP más para ipconfig3. La IP pública no es obligatoria.

Search IP configurations					
NAME	IP VERSION	TYPE	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)	-	

Paso 2: Configurar direcciones IP propiedad de NetScaler

Configure las direcciones IP propiedad de NetScaler mediante la GUI o el comando `add ns ip`. Para obtener más información, consulte [Configuración de direcciones IP propiedad de NetScaler](#).

Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC

October 17, 2024

En una implementación de Microsoft Azure, se logra una configuración de alta disponibilidad de dos instancias de NetScaler VPX mediante Azure Load Balancer (ALB). Esto se consigue configurando un sondeo de estado en ALB, que supervisa cada instancia VPX enviando un sondeo de estado cada 5 segundos a instancias primarias y secundarias.

En esta configuración, solo el nodo principal responde a los sondeos de estado y el secundario no. Una vez que el primario envía la respuesta al sondeo de estado, el ALB comienza a enviar el tráfico de datos a la instancia. Si la instancia principal pierde dos sondeos de mantenimiento consecutivos, ALB no redirige el tráfico a esa instancia. En caso de conmutación por error, el nuevo primario comienza a responder a los sondeos de mantenimiento y el ALB redirige el tráfico hacia él. El tiempo de conmutación por error de alta disponibilidad VPX estándar es de tres segundos. El tiempo total de conmutación por error que puede tardar en cambiar el tráfico puede ser de un máximo de 13 segundos.

Puede implementar un par de instancias de NetScaler VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener varias direcciones IP.

Están disponibles las siguientes opciones para una implementación de alta disponibilidad con varias NIC:

- Alta disponibilidad mediante el conjunto de disponibilidad de Azure
- Alta disponibilidad mediante zonas de disponibilidad de Azure

Para obtener más información sobre Azure Availability Set y zonas de disponibilidad, consulte la documentación de Azure [Administrar la disponibilidad de máquinas virtuales Linux](#).

Alta disponibilidad mediante el conjunto de disponibilidad

Una configuración de alta disponibilidad que utilice un conjunto de disponibilidad debe cumplir los siguientes requisitos:

- Configuración de red independiente de HA (INC)

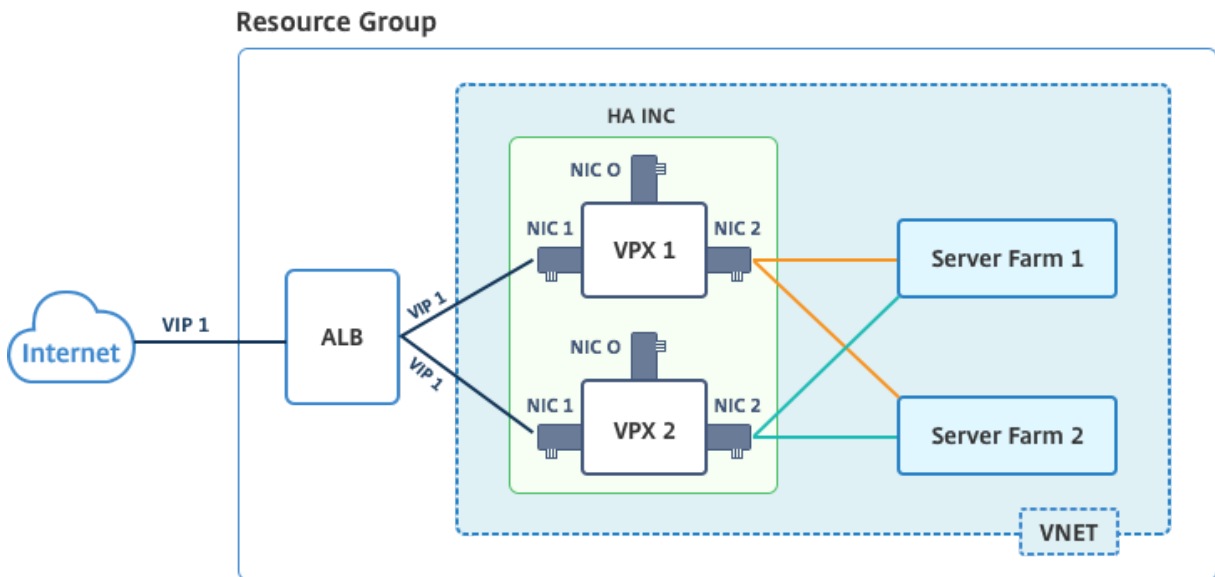
- El Azure Load Balancer (ALB) en modo Direct Server Return (DSR)

Todo el tráfico pasa por el nodo principal. El nodo secundario permanece en modo de espera hasta que falla el nodo principal.

Nota:

Para que funcione una implementación de alta disponibilidad de NetScaler VPX en la nube de Azure, necesita una IP pública flotante (PIP) que pueda moverse entre los dos nodos VPX. Azure Load Balancer (ALB) proporciona ese PIP flotante, que se mueve automáticamente al segundo nodo en caso de una conmutación por error.

Diagrama: ejemplo de una arquitectura de implementación de alta disponibilidad con Azure Availability Set



En una implementación activo-pasiva, las direcciones IP públicas (PIP) front-end de ALB se agregan como direcciones VIP en cada nodo VPX. En la configuración HA-INC, las direcciones VIP son flotantes y las direcciones SNIP son específicas de la instancia.

Puede implementar un par VPX en el modo de alta disponibilidad activo-pasivo de dos maneras mediante:

- **Plantilla de alta disponibilidad estándar de NetScaler VPX:** utilice esta opción para configurar un par de HA con la opción predeterminada de tres subredes y seis NIC.
- **Comandos de Windows PowerShell:** utilice esta opción para configurar un par de HA de acuerdo con los requisitos de la subred y la NIC.

En este tema se describe cómo implementar un par VPX en la configuración de HA activo-pasiva mediante la plantilla de Citrix. Si desea utilizar comandos de PowerShell, consulte [Configuración de una instalación de alta disponibilidad con múltiples direcciones IP y NIC mediante comandos de PowerShell](#).

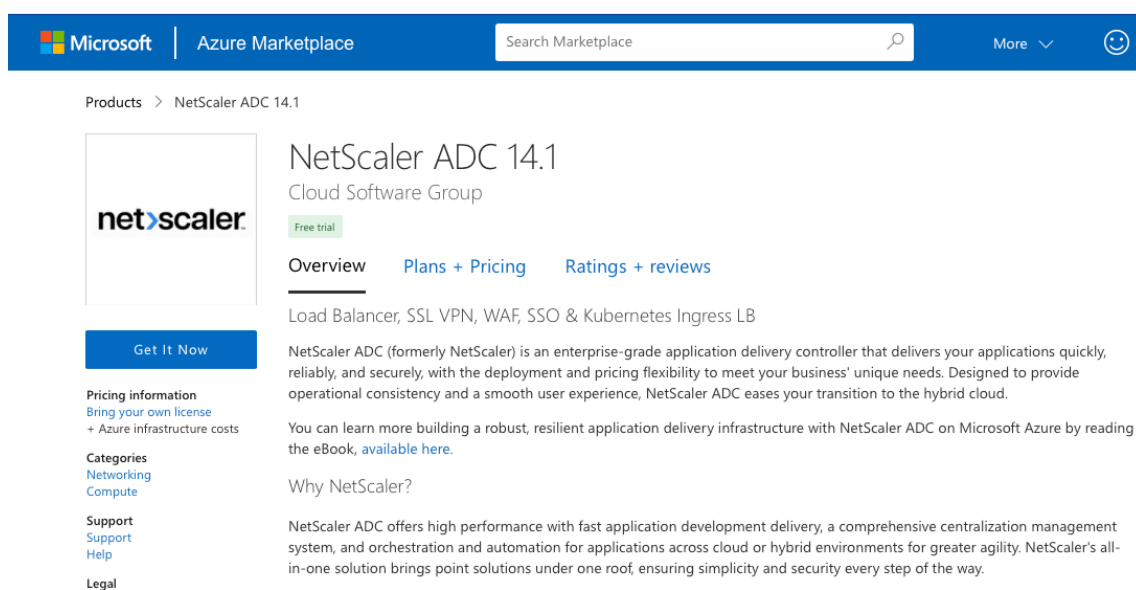
Configure los nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler

Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para la administración, el cliente y el tráfico del lado del servidor, y cada subred tiene dos NIC para ambas instancias VPX.

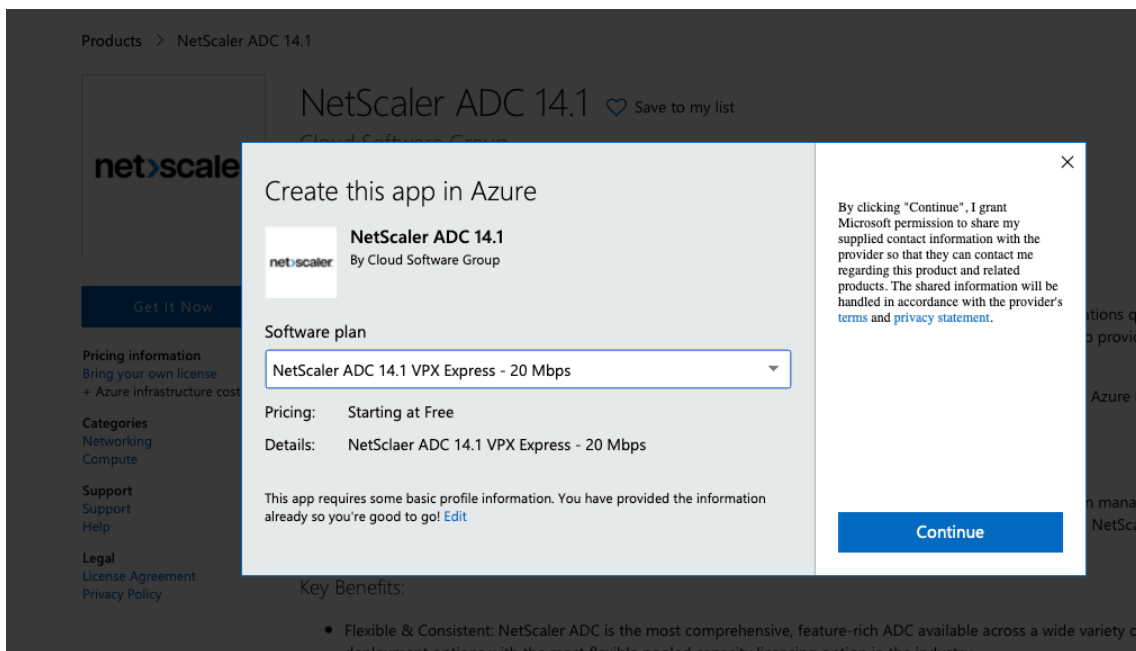
Puede obtener la plantilla NetScaler HA Pair en [Azure Marketplace](#).

Complete los siguientes pasos para lanzar la plantilla e implementar un par VPX de alta disponibilidad mediante conjuntos de disponibilidad de Azure.

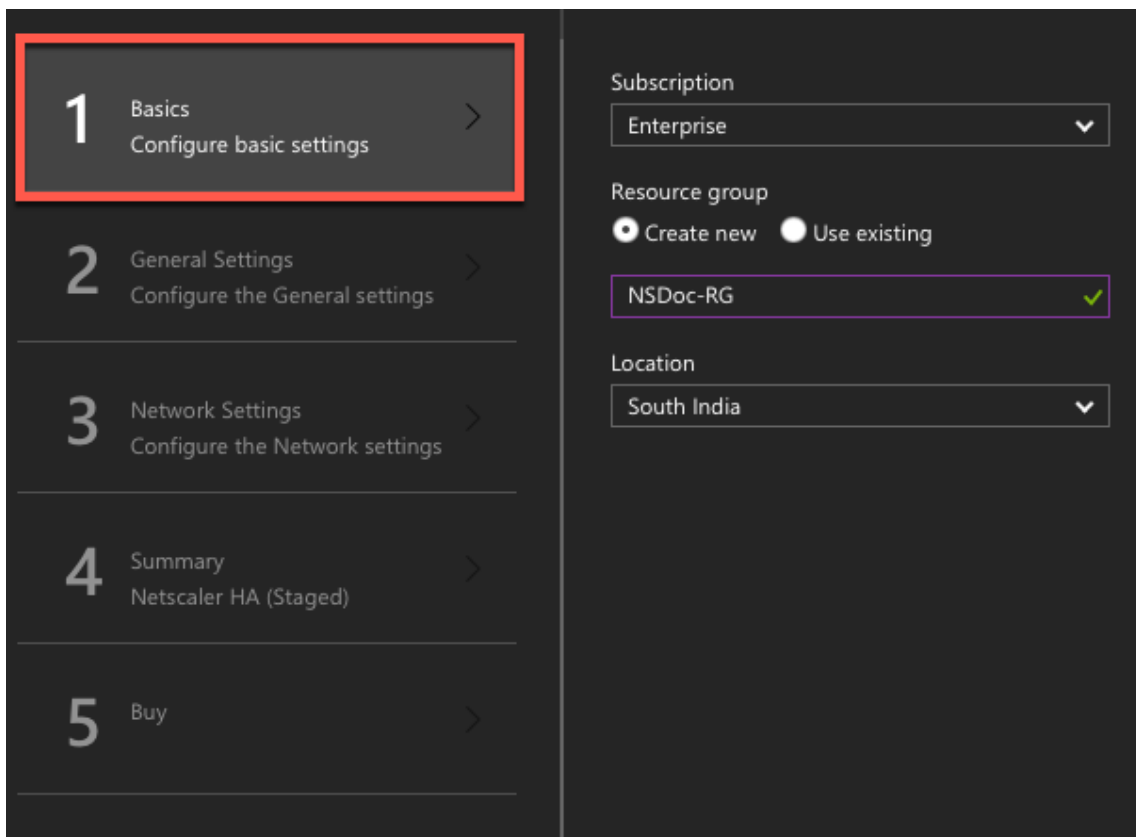
1. En Azure Marketplace, busque **NetScaler**.



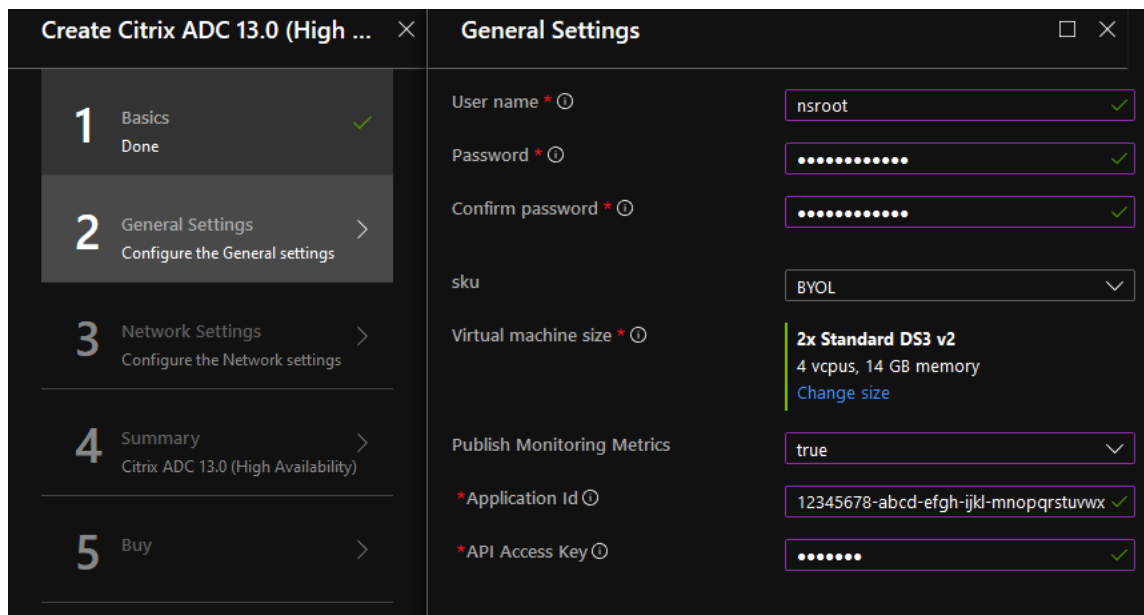
2. Haga clic en **OBTENER AHORA**.
3. Seleccione la implementación de alta disponibilidad requerida junto con la licencia y haga clic en **Continuar**.



4. Aparecerá la página **Básicos**. Cree un grupo de recursos y seleccione **Aceptar**.



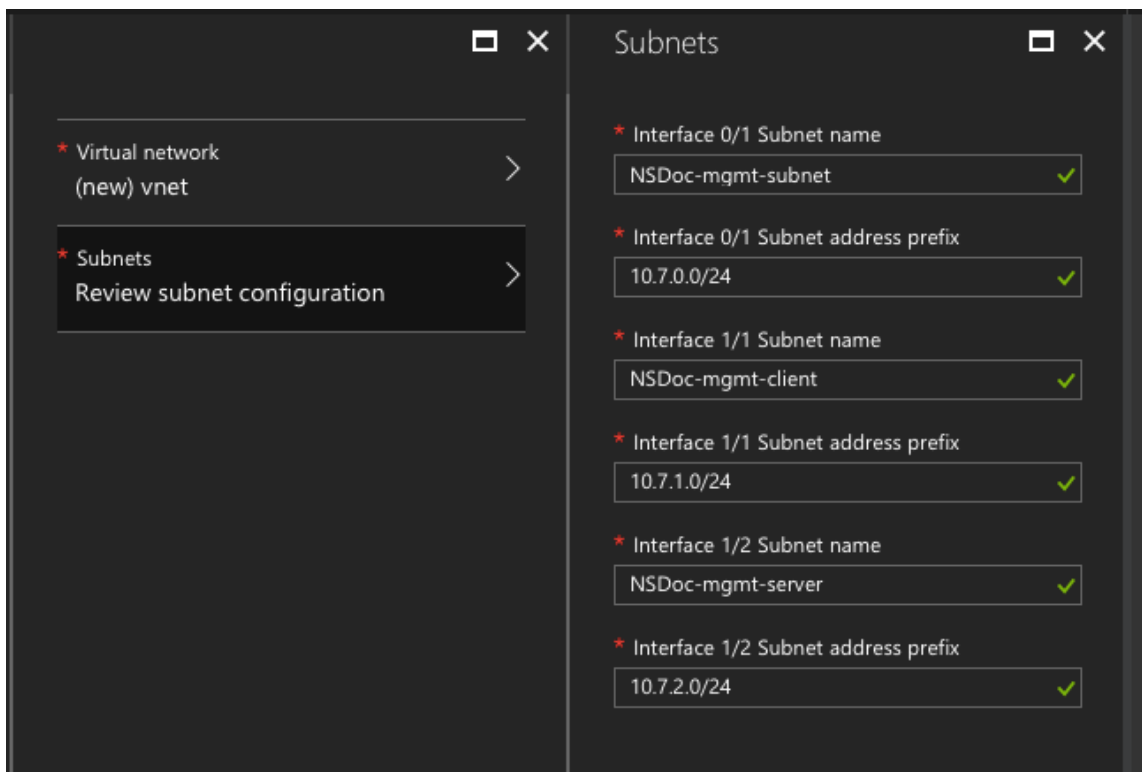
5. Aparecerá la página **Configuración general**. Escriba los detalles y seleccione **Aceptar**.



Nota:

De forma predeterminada, la opción **Publishing Monitoring Metrics** está configurada en **false**. Si desea habilitar esta opción, seleccione **true**. Cree una aplicación de Azure Active Directory (ADD) y una entidad de servicio que pueda tener acceso a los recursos. Asigne el rol colaborador a la aplicación AAD recién creada. Para obtener más información, consulte [Uso del portal para crear una aplicación y un principal de servicio de Azure Active Directory que pueda acceder a los recursos](#).

6. Aparecerá la página **Configuración de red**. Compruebe las configuraciones de VNet y subred, modifique la configuración requerida y seleccione **Aceptar**.


























7. Aparecerá la página **Resumen**. Revise la configuración y modifique en consecuencia. Seleccione **Aceptar** para confirmar.

8. Aparecerá la página **Comprar**. Seleccione **Comprar** para completar la implementación.

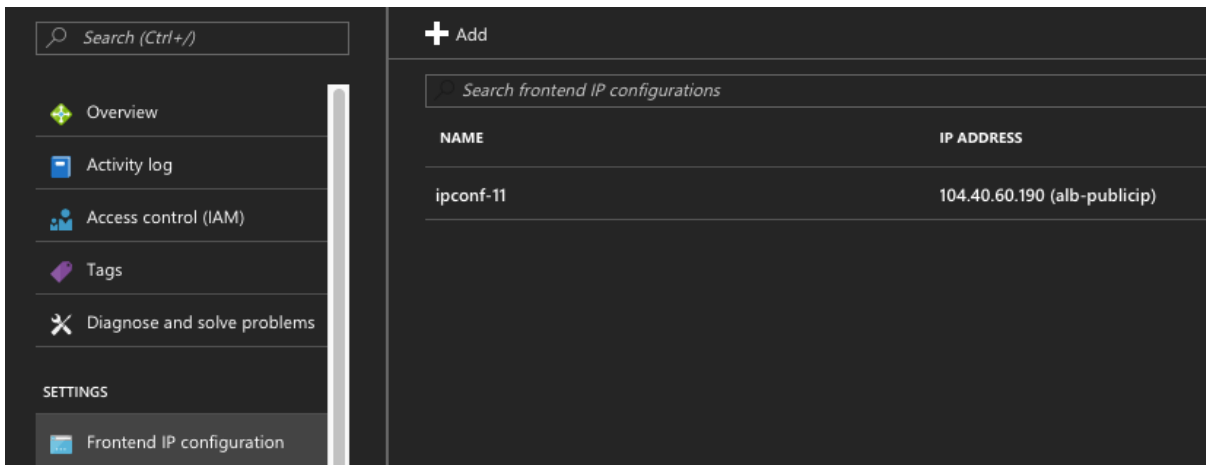
Es posible que el Azure Resource Group demore un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el **grupo de recursos** en el portal de Azure para ver los detalles de configuración, como reglas de LB, grupos de back-end, sondeos de estado. El par de alta disponibilidad aparece como ns-vpx0 y ns-vpx1.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

23 items Show hidden types ⓘ

<input type="checkbox"/>	NAME <small>↑↓</small>	TYPE <small>↑↓</small>
<input type="checkbox"/>	 alb	Load balancer
<input type="checkbox"/>	 alb-publicip	Public IP address
<input type="checkbox"/>	 avl-set	Availability set
<input type="checkbox"/>	 ns-vpx0	Disk
<input type="checkbox"/>	 ns-vpx0	Virtual machine
<input type="checkbox"/>	 ns-vpx0-mgmt-publicip	Public IP address
<input type="checkbox"/>	 ns-vpx1	Disk
<input type="checkbox"/>	 ns-vpx1	Virtual machine
<input type="checkbox"/>	 ns-vpx1-mgmt-publicip	Public IP address
<input type="checkbox"/>	 ns-vpx-nic0-01	Network interface
<input type="checkbox"/>	 ns-vpx-nic0-11	Network interface
<input type="checkbox"/>	 ns-vpx-nic0-12	Network interface
<input type="checkbox"/>	 ns-vpx-nic1-01	Network interface
<input type="checkbox"/>	 ns-vpx-nic1-11	Network interface
<input type="checkbox"/>	 ns-vpx-nic1-12	Network interface
<input type="checkbox"/>	 ns-vpx-nic-nsg0-01	Network security group
<input type="checkbox"/>	 ns-vpx-nic-nsg0-11	Network security group
<input type="checkbox"/>	 ns-vpx-nic-nsg0-12	Network security group
<input type="checkbox"/>	 ns-vpx-nic-nsg1-01	Network security group
<input type="checkbox"/>	 ns-vpx-nic-nsg1-11	Network security group
<input type="checkbox"/>	 ns-vpx-nic-nsg1-12	Network security group
<input type="checkbox"/>	 vnet01	Virtual network
<input type="checkbox"/>	 vpxhamd7fi3wouvrk	Storage account

A continuación, debe configurar el servidor virtual de equilibrio de carga con la **dirección IP pública (PIP) del Frontend de ALB**, en el nodo principal. Para encontrar el PIP de ALB, seleccione ALB > Configuración de IP de **interfaz**.



Consulte la sección **Recursos** para obtener más información sobre cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes enlaces proporcionan información adicional relacionada con la implementación de alta disponibilidad y la configuración del servidor virtual:

- [Configuración de nodos de alta disponibilidad en diferentes subredes](#)
- [Configurar el equilibrio de carga básico](#)

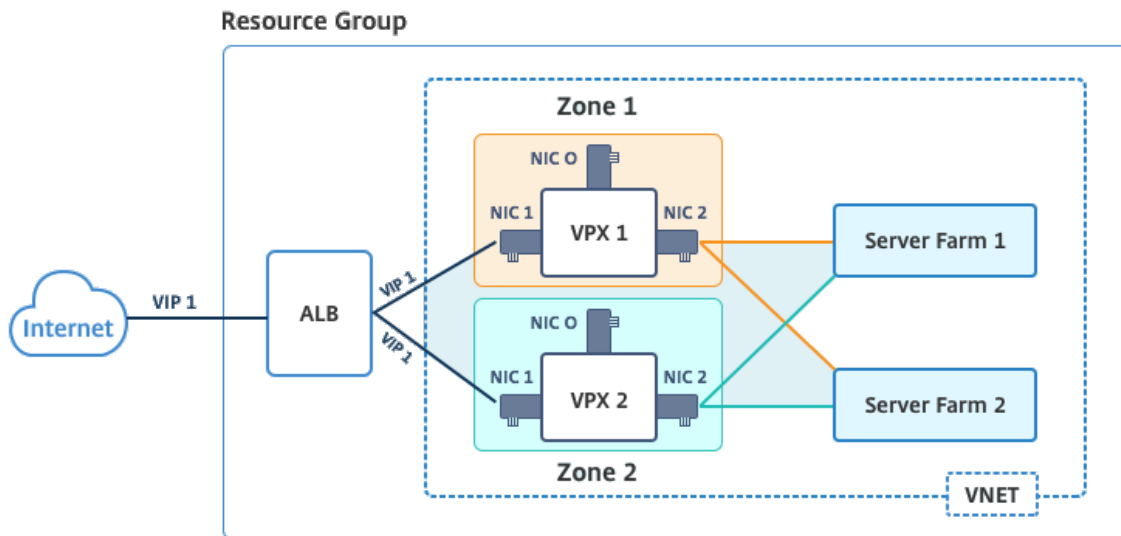
Recursos relacionados:

- [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell](#)
- [Configuración de GSLB en la implementación de HA activa en espera en Azure](#)

Alta disponibilidad mediante zonas de disponibilidad

Las zonas de disponibilidad de Azure son ubicaciones aisladas por errores dentro de una región de Azure, que proporcionan alimentación redundante, refrigeración y redes y aumentan la resiliencia. Solo las regiones específicas de Azure admiten zonas de disponibilidad. Para obtener más información sobre las regiones que admiten zonas de disponibilidad, consulte la documentación de Azure [¿Qué son las zonas de disponibilidad de Azure?](#).

Diagrama: Ejemplo de una arquitectura de implementación de alta disponibilidad, con zonas de disponibilidad de Azure



Puede implementar un par VPX en modo de alta disponibilidad mediante la plantilla denominada “NetScaler 13.0 HA con zonas de disponibilidad”, disponible en Azure Marketplace.

Complete los siguientes pasos para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante las zonas de disponibilidad de Azure.

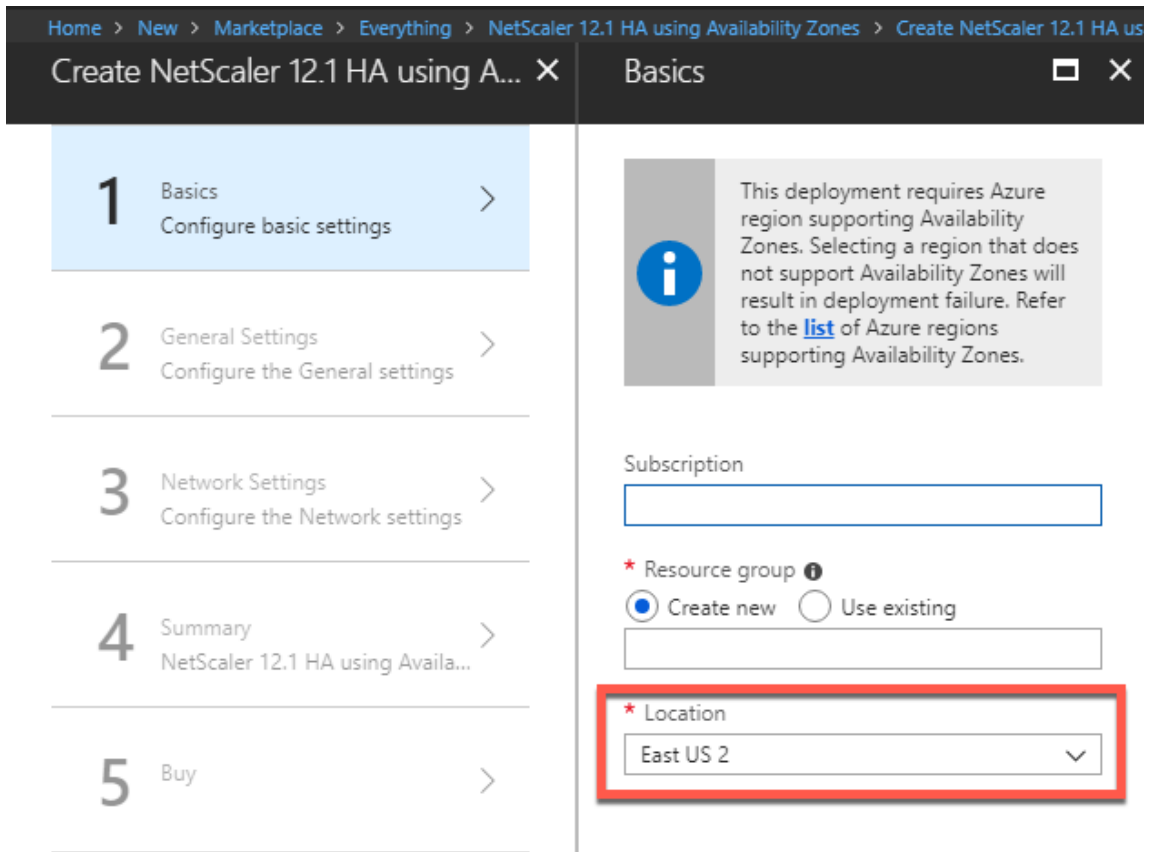
1. En Azure Marketplace, seleccione e inicie la plantilla de solución Citrix.



2. Asegúrese de que el tipo de implementación sea Administrador de recursos y seleccione **Crear**.
3. Aparecerá la página **Básicos**. Introduzca los detalles y haga clic en **Aceptar**.

Nota:

Asegúrese de seleccionar una región de Azure que admita zonas de disponibilidad. Para obtener más información sobre las regiones que admiten zonas de disponibilidad, consulte la documentación de Azure [¿Qué son las zonas de disponibilidad de Azure?](#)



4. Aparecerá la página **Configuración general**. Escriba los detalles y seleccione **Aceptar**.
5. Aparecerá la página **Configuración de red**. Compruebe las configuraciones de VNet y subred, modifique la configuración requerida y seleccione **Aceptar**.
6. Aparecerá la página **Resumen**. Revise la configuración y modifique en consecuencia. Seleccione **Aceptar** para confirmar.
7. Aparecerá la página **Comprar**. Seleccione **Comprar** para completar la implementación.

Es posible que el Azure Resource Group demore un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el **grupo de recursos** para ver los detalles de la configuración, como las reglas de LB, los grupos de back-end, las sondas de estado, etc., en el portal de Azure. El par de alta disponibilidad aparece como ns-vpx0 y ns-vpx1. Además, puede ver la ubicación en la columna **Ubicación**.

Filter by name... All types All locations No grouping

22 items Show hidden types

NAME	TYPE	LOCATION
alb	Load balancer	East US 2
alb-publicip	Public IP address	East US 2
ns-vpx0	Virtual machine	East US 2
ns-vpx0_OsDisk_1_d7b757b8aa804bf1991a083f319e553a	Disk	East US 2
ns-vpx0-mgmt-publicip	Public IP address	East US 2
ns-vpx1	Virtual machine	East US 2
ns-vpx1_OsDisk_1_0c2364d43e2b47fa896bf14b02090ee0	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
vpxhavadosvod3v5jeu	Storage account	East US 2

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Supervisar las instancias mediante métricas en el monitor de Azure

Puede utilizar métricas en la plataforma de datos de monitor de Azure para supervisar un conjunto de recursos NetScaler VPX, como CPU, utilización de memoria y rendimiento. El servicio Metrics supervisa los recursos de NetScaler VPX que se ejecutan en Azure, en tiempo real. Puede utilizar el **Explorador de métricas** para acceder a los datos recopilados. Para obtener más información, consulte [Descripción general de las métricas de Azure Monitor](#).

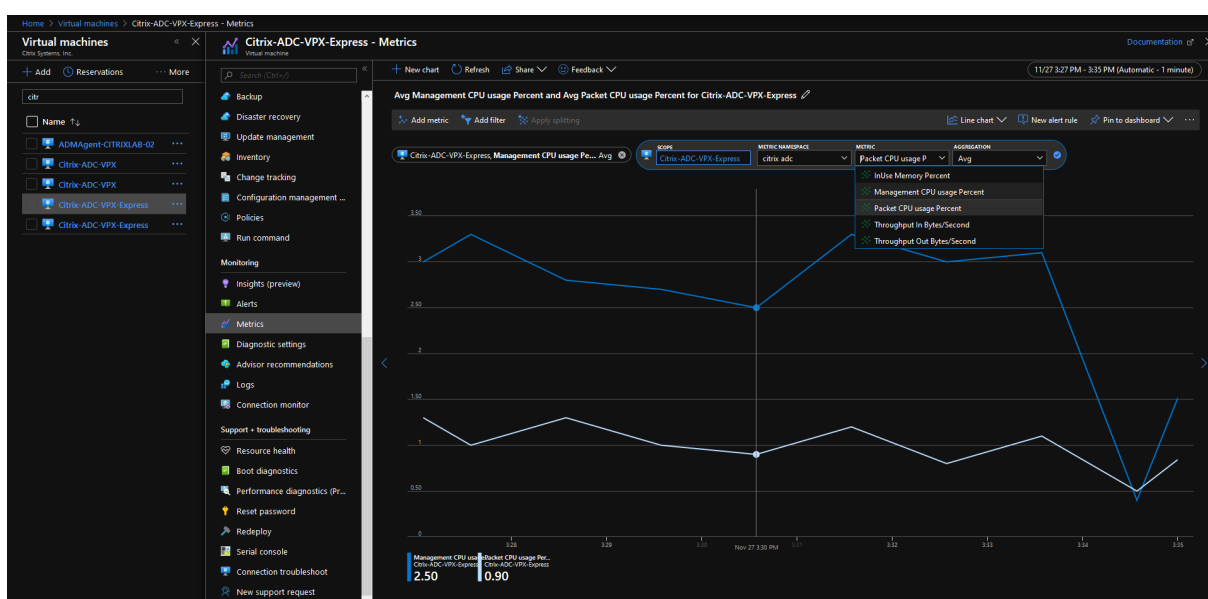
Puntos a tener en cuenta

- Si implementa una instancia de NetScaler VPX en Azure mediante la oferta Azure Marketplace, el servicio Metrics está inhabilitado de forma predeterminada.
- La CLI de Azure no admite el servicio Metrics.
- Las métricas están disponibles para la CPU (administración y uso de la CPU de paquetes), la memoria y el rendimiento (entrante y saliente).

Cómo ver métricas en el monitor de Azure

Para ver las métricas en el monitor de Azure de la instancia, lleve a cabo estos pasos:

1. Inicie sesión en **Azure Portal > Máquinas virtuales**.
2. Seleccione la máquina virtual que es el nodo principal.
3. En la sección **Supervisión**, haga clic en **Métricas**.
4. En el menú desplegable **Metric Namespace**, haga clic en **NetScaler**.
5. En **Todas las métricas**, en **Métricas**, haga clic en las métricas que quieras ver.
6. Haga clic en **Agregar métrica** para ver otra métrica en el mismo gráfico. Use las opciones del gráfico para personalizar el gráfico.



Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell

October 17, 2024

Puede implementar un par de instancias de NetScaler VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener varias direcciones IP.

Una implementación activo-pasiva requiere:

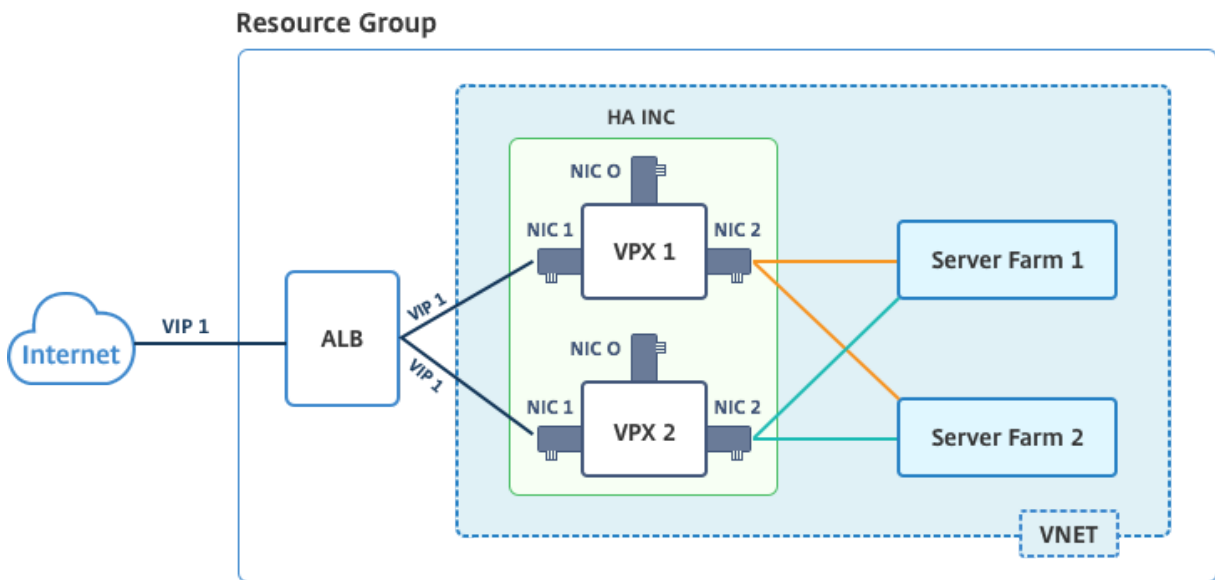
- Configuración de red independiente de HA (INC)
- El Azure Load Balancer (ALB) en modo Direct Server Return (DSR)

Todo el tráfico pasa por el nodo principal. El nodo secundario permanece en modo de espera hasta que falla el nodo principal.

Nota:

Para que funcione una implementación de alta disponibilidad de NetScaler VPX en una nube de Azure, necesita una IP pública flotante (PIP) que se pueda mover entre los dos nodos de alta disponibilidad. Azure Load Balancer (ALB) proporciona ese PIP flotante, que se mueve automáticamente al segundo nodo en caso de una conmutación por error.

Diagrama: Ejemplo de una arquitectura de implementación activo-pasiva



En una implementación activo-pasiva, las direcciones IP públicas flotantes (PIP) ALB se agregan como direcciones VIP en cada nodo VPX. En la configuración HA-INC, las direcciones VIP son flotantes y las direcciones SNIP son específicas de la instancia.

ALB supervisa cada instancia VPX enviando una sonda de estado cada 5 segundos y redirige el tráfico a esa instancia solo que envía la respuesta de los sondeos de estado en intervalos regulares. Por lo tanto, en una configuración de HA, el nodo primario responde a sondeos de estado y secundario no. Si las instancias principales pierden dos sondeos de estado consecutivos, ALB no redirige el tráfico a esa instancia. En caso de conmutación por error, el nuevo primario comienza a responder a los sondeos de mantenimiento y el ALB redirige el tráfico hacia él. El tiempo de conmutación por error de alta disponibilidad VPX estándar es de tres segundos. El tiempo total de conmutación por error que puede tardar en el cambio de tráfico puede ser de 13 segundos como máximo.

Puede implementar un par VPX en la configuración de HA activa-pasiva de dos maneras mediante:

- **Plantilla de alta disponibilidad estándar de NetScaler VPX:** utilice esta opción para configurar un par de HA con la opción predeterminada de tres subredes y seis NIC.

- **Comandos de Windows PowerShell:** utilice esta opción para configurar un par de HA de acuerdo con los requisitos de la subred y la NIC.

En este tema se describe cómo implementar un par VPX en la instalación de HA activo-pasiva mediante comandos de PowerShell. Si desea utilizar la plantilla HA estándar de NetScaler VPX, consulte [Configuración de una instalación de HA con varias direcciones IP y NIC](#).

Configuración de nodos HA-INC mediante comandos de PowerShell

Caso: Implementación de PowerShell de HA-INC

En este caso, se implementa un par NetScaler VPX mediante la topología que se indica en la tabla. Cada instancia VPX contiene tres NIC, cada NIC se implementa en una subred diferente. A cada NIC se le asigna una configuración IP.

ALB	VPX1	VPX2
ALB está asociado con IP pública 3 (pip3)	La IP de administración se configura con IPConfig1, que incluye una IP pública (pip1) y una IP privada (12.5.2.24); nic1; Mgmtsubnet=12.5.2.0/24	La IP de administración se configura con IPConfig5, que incluye una IP pública (pip3) y una IP privada (12.5.2.26); nic4; Mgmtsubnet=12.5.2.0/24
Las reglas LB y el puerto configurados son HTTP (80), SSL (443), sonda de estado (9000)	La IP del lado del cliente está configurada con IPConfig3, que incluye una IP privada (12.5.1.27); nic2; FrontenDSubet=12.5.1.0/24	La IP del lado del cliente está configurada con IPConfig7, que incluye una IP privada (12.5.1.28); nic5; FrontenDSubet=12.5.1.0/24
-	La IP del lado del servidor está configurada con IPConfig4, que incluye una IP privada (12.5.3.24); nic3; backendSubnet=12.5.3.0/24	La IP del lado del servidor está configurada con IPConfig8, que incluye una IP privada (12.5.3.28); nic6; backendSubnet=12.5.3.0/24
-	Las reglas y puertos para NSG son SSH (22), HTTP (80), HTTPS (443)	-

Configuración de parámetros

En este caso se utilizan los parámetros siguientes.

\$locName= "South east Asia"
\$rgName = "MultiIP-MultiNIC-RG"
\$nicName1= "VM1-NIC1"
\$nicName2 = "VM1-NIC2"
\$nicName3= "VM1-NIC3"
\$nicName4 = "VM2-NIC1"
\$nicName5= "VM2-NIC2"
\$nicName6 = "VM2-NIC3"
\$vNetName = "Azure-MultiIP-ALB-vnet"
\$vNetAddressRange= "12.5.0.0/16"
\$frontEndSubnetName= "frontEndSubnet"
\$frontEndSubnetRange= "12.5.1.0/24"
\$mgmtSubnetName= "mgmtSubnet"
\$mgmtSubnetRange= "12.5.2.0/24"
\$backEndSubnetName = "backEndSubnet"
\$backEndSubnetRange = "12.5.3.0/24"
\$prmStorageAccountName = "multiipmultinicbstorage"
\$avSetName = "multiple-avSet"
\$vmSize= "Standard_DS4_V2"
\$editor = "Citrix"
\$offer = "netscalervpx-120"
\$sku = "netscalerbyol"
\$version="latest"
\$pubIPName1="VPX1MGMT"
\$pubIPName2="VPX2MGMT"
\$pubIPName3="ALBPIP"
\$domName1="vpx1dns"
\$domName2="vpx2dns"
\$domName3="vpxalbdns"


```
$vmNamePrefix="VPXMultiIPALB"  
$osDiskSuffix1="osmultiipalbdiskdb1"  
$osDiskSuffix2="osmultiipalbdiskdb2"  
$lbName= "MultiIPALB"  
$frontEndConfigName1= "FrontEndIP"  
$backendPoolName1= "BackendPoolHttp"  
$lbRuleName1= "LBRuleHttp"  
$healthProbeName= "HealthProbe"  
$nsgName="NSG-MultiIP-ALB"  
$rule1name="HTTP entrante"  
$rule2Name="HTTPS entrante"  
$rule3name="SSH entrante"
```

Para completar la implementación, complete los pasos siguientes mediante comandos de PowerShell:

1. Crear un grupo de recursos, una cuenta de almacenamiento y un conjunto de disponibilidad
2. Crear un grupo de seguridad de red y agregar reglas
3. Crear una red virtual y tres subredes
4. Crear direcciones IP públicas
5. Crear configuraciones IP para VPX1
6. Crear configuraciones IP para VPX2
7. Crear NIC para VPX1
8. Crear NIC para VPX2
9. Crear VPX1
10. Crear VPX2
11. Crear ALB

Cree un grupo de recursos, una cuenta de almacenamiento y un conjunto de disponibilidad.

```
1 New-AzureRmResourceGroup -Name $rgName -Location $locName  
2  
3  
4 $prmStorageAccount=New-AzureRMStorageAccount -Name  
   $prmStorageAccountName -ResourceGroupName $rgName -Type  
   Standard_LRS -Location $locName  
5  
6  
7 $avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName  
   $rgName -Location $locName
```

Cree un grupo de seguridad de red y agregue reglas.

```

1  $rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
    Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 101
2
3
4  -SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 80
5
6
7  $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
    Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 110
8
9
10 -SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 443
11
12
13 $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
    Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 120
14
15
16 -SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 22
17
18
19 $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
    Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
    $rule3

```

Cree una red virtual y tres subredes.

```

1  $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
    parameter value should be as per your requirement)
2
3
4  $mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $mgmtSubnetName -AddressPrefix $mgmtSubnetRange
5
6
7  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10 $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vNetAddressRange -
    Subnet $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13 $subnetName ="frontEndSubnet"

```

```
14
15
16   \${subnet1}=\${vnet.Subnets}|?{
17   \${_}.Name -eq \${subnetName} }
18
19
20
21   $subnetName="backEndSubnet"
22
23
24   \${subnet2}=\${vnet.Subnets}|?{
25   \${_}.Name -eq \${subnetName} }
26
27
28
29   $subnetName="mgmtSubnet"
30
31
32   \${subnet3}=\${vnet.Subnets}|?{
33   \${_}.Name -eq \${subnetName} }
```

Crear direcciones IP públicas.

```
1   $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
      $rgName -DomainNameLabel $domName1 -Location $locName -
      AllocationMethod Dynamic
2
3   $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
      $rgName -DomainNameLabel $domName2 -Location $locName -
      AllocationMethod Dynamic
4
5   $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
      $rgName -DomainNameLabel $domName3 -Location $locName -
      AllocationMethod Dynamic
```

Cree configuraciones IP para VPX1.

```
1   $IPConfigName1 = "IPConfig1"
2
3
4   $IPAddress = "12.5.2.24"
5
6
7   $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
      Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
      $pip1 -Primary
8
9
10  $IPConfigName3="IPConfig-3"
11
12
13  $IPAddress="12.5.1.27"
14
```

```

15
16  $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
      Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19  $IPConfigName4 = "IPConfig-4"
20
21
22  $IPAddress = "12.5.3.24"
23
24
25  $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
      -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary

```

Cree configuraciones IP para VPX2.

```

1  $IpConfigName5 = "IPConfig5"
2
3
4  $IPAddress="12.5.2.26"
5
6
7  $IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
      Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
      $pip2 -Primary
8
9
10  $IPConfigName7="IPConfig-7"
11
12
13  $IPAddress="12.5.1.28"
14
15
16  $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
      Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19  $IPConfigName8="IPConfig-8"
20
21
22  $IPAddress="12.5.3.28"
23
24
25  $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
      Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary

```

Crear NIC para VPX1.

```

1  $nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig1 -
      NetworkSecurityGroupId $nsg.Id
2
3

```

```

4   $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig3 -
    NetworkSecurityGroupId $nsg.Id
5
6
7   $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig4 -
    NetworkSecurityGroupId $nsg.Id

```

Crear NIC para VPX2.

```

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

```

Crear VPX1.

Este paso incluye los siguientes pasos secundarios:

- Crear objeto de configuración de máquina virtual
- Establecer credenciales, SO e imagen
- Agregar NIC
- Especificar el disco del sistema operativo y crear VM

```

1   $suffixNumber = 1
2
3   $vmName=$vmNamePrefix + $suffixNumber
4
5   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
6
7   $cred=Get-Credential -Message "Type the name and password for
    VPX login."
8
9   $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
10
11  $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
12

```

```
13 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1
    .Id -Primary
14
15 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2
    .Id
16
17 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3
    .Id
18
19 $osDiskName=$vmName + "-" + $osDiskSuffix1
20
21 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +
    "vhds/" + $osDiskName + ".vhd"
22
23 $vmConfig=Set-AzureRMVMOsDisk -VM $vmConfig -Name $osDiskName -
    VhdUri $osVhdUri -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product
    $offer -Name $sku
26
27 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -
    Location $locName
```

Crear VPX2.

```
1 ````
2 $suffixNumber=2
3
4
5 $vmName=$vmNamePrefix + $suffixNumber
6
7
8 $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    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
16
17 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
18
19
20 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
    Primary
21
22
23 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
```

```
24
25
26 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
29 $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
    /" + $osDiskName + ".vhd"
33
34
35 $vmConfig=Set-AzureRMVMOsdisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
36
37
38 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
    -Name $sku
39
40
41 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
    $locName
42 ```
```

Para ver las direcciones IP privadas y públicas asignadas a las NIC, escriba los siguientes comandos:

```
1 ```
2 $nic1.IPConfig
3
4
5 $nic2.IPConfig
6
7
8 $nic3.IPConfig
9
10
11 $nic4.IPConfig
12
13
14 $nic5.IPConfig
15
16
17 $nic6.IPConfig
18 ```
```

Crear equilibrio de carga de Azure (ALB).

Este paso incluye los siguientes pasos secundarios:

- Crear configuración IP front-end
- Crear sonda de salud
- Crear grupo de direcciones de backend

- Crear reglas de equilibrio de carga (HTTP y SSL)
- Crear ALB con configuración IP front-end, grupo de direcciones backend y regla LB
- Asociar configuración de IP con grupos de back-end

```

$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

```

Después de implementar correctamente el par NetScaler VPX, inicie sesión en cada instancia VPX para configurar HA-INC y las direcciones SNIP y VIP.

1. Escriba el siguiente comando para agregar nodos HA.
2. Agregar direcciones IP privadas de NIC del lado del cliente como SNIP para VPX1 (NIC2) y VPX2 (NIC5)

```

add ha node 1 PeerNodeNSIP -inc Enabled

agregar nsip privateIPofNIC2 255.255.255.0 -tipo SNIP      agregar
nsip privateIPofNIC5 255.255.255.0 -tipo SNIP

```


3. Agregue un servidor virtual de equilibrio de carga en el nodo principal con la dirección IP front-end (IP pública) de ALB.

```
add lb virtual server v1 HTTP FrontEndIPofALB 80
```

Recursos relacionados:

[Configuración de GSLB en la implementación de HA activa en espera en Azure](#)

Implemente un par de alta disponibilidad de NetScaler en Azure con ALB en el modo flotante de IP inhabilitada

October 17, 2024

Puede implementar un par de instancias de NetScaler VPX con varias NIC en una configuración de alta disponibilidad (HA) activo-pasiva en Azure. Cada NIC puede contener muchas direcciones IP.

Una implementación activo-pasiva requiere:

- Configuración de red independiente de HA (INC)
- Azure Load Balancer (ALB) con:
 - Modo habilitado para IP flotante o modo Direct Server Return (DSR)
 - Modo de IP flotante inhabilitado

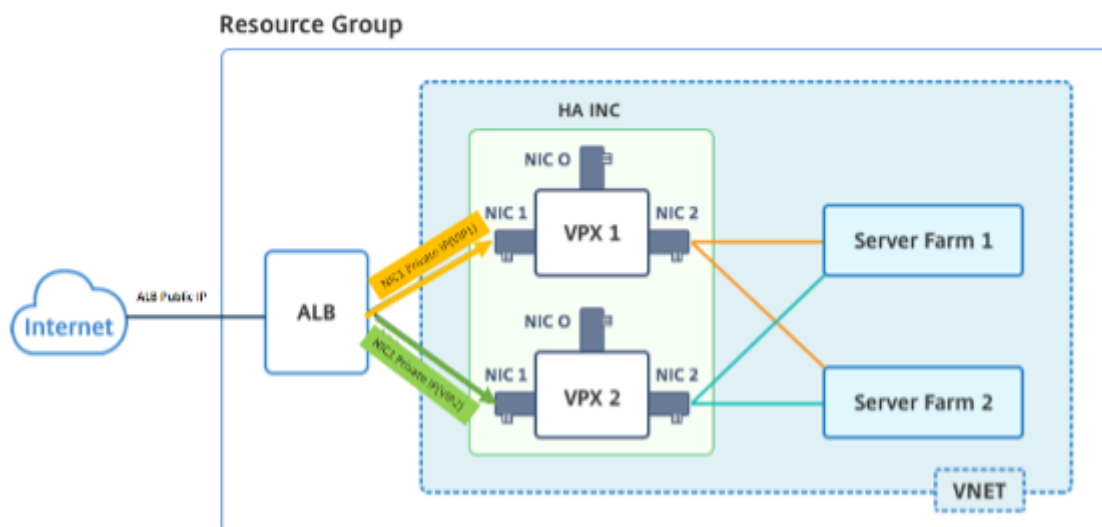
Para obtener más información sobre las opciones de IP flotante de ALB, consulte la [documentación de Azure](#).

Si desea implementar un par VPX en una configuración de alta disponibilidad activa-pasiva en Azure con IP flotante ALB habilitada, consulte [Configurar una configuración de alta disponibilidad con múltiples direcciones IP y NIC mediante comandos de PowerShell](#).

Arquitectura de implementación de alta disponibilidad con ALB en modo flotante con IP inhabilitada

En una implementación activa-pasiva, las direcciones IP privadas de la interfaz de cliente de cada instancia se agregan como direcciones VIP en cada instancia VPX. Configure en el modo HA-INC con las direcciones VIP que se comparten mediante IPset y las direcciones SNIP son específicas de la instancia. Todo el tráfico pasa por la instancia principal. La instancia secundaria está en modo de espera hasta que se produce un error en la instancia principal.

Diagrama: Ejemplo de una arquitectura de implementación activo-pasiva



Requisitos previos

Debe estar familiarizado con la siguiente información antes de implementar una instancia de NetScaler VPX en Azure.

- Terminología y detalles de red de Azure. Para obtener más información, consulte [Terminología de Azure](#).
- Funcionamiento de un dispositivo NetScaler. Para obtener más información, consulte la [documentación de NetScaler](#).
- Redes NetScaler. Para obtener más información, consulte [ADC Networking](#).
- Configuración de reglas de equilibrio de carga y equilibrador de carga de Azure. Para obtener más información, consulte la [documentación de Azure ALB](#).

Cómo implementar un par de alta disponibilidad de VPX en Azure con la IP flotante de ALB inhabilitada

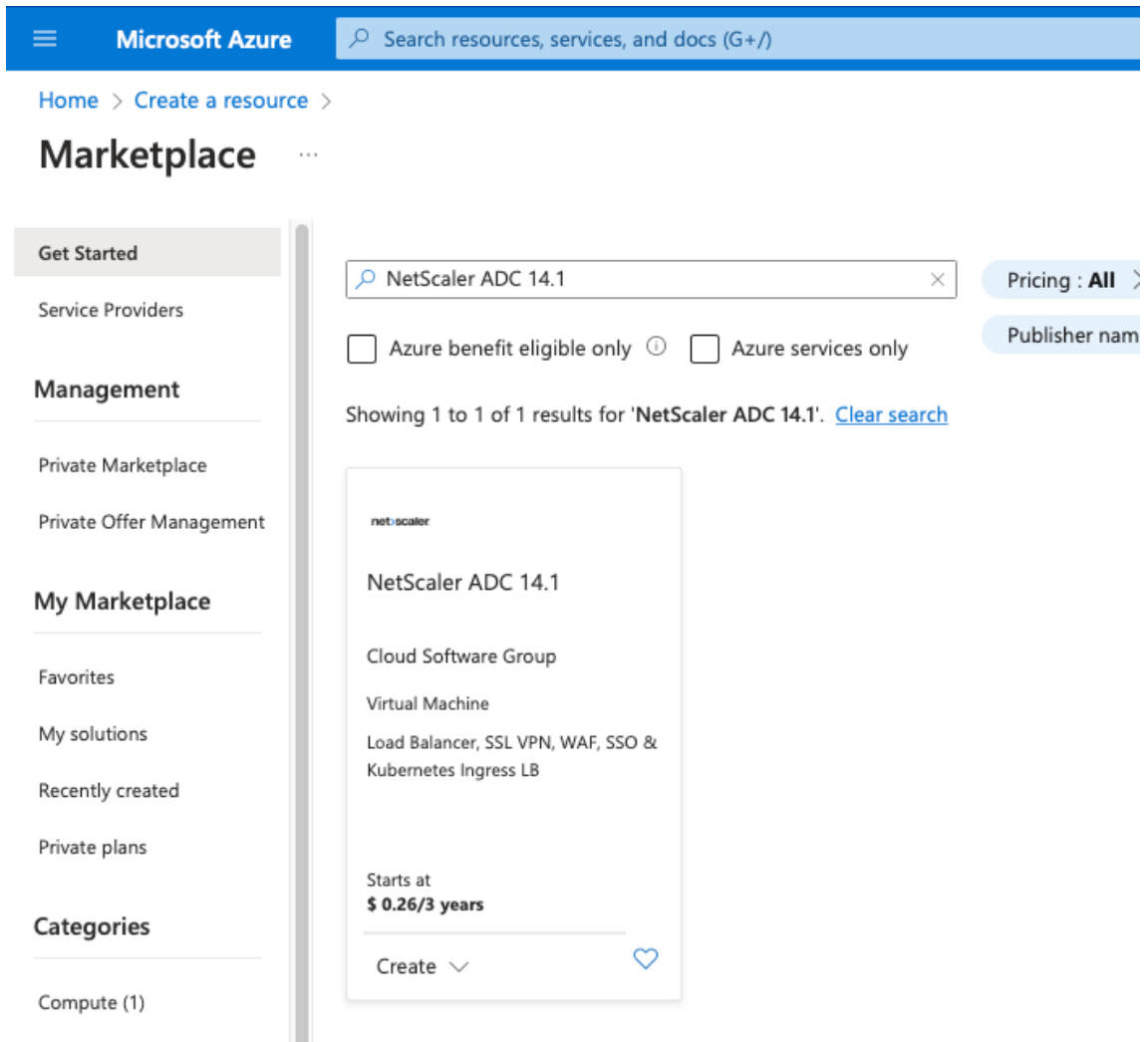
Este es un resumen de los pasos de implementación de HA y ALB:

1. Implemente dos instancias VPX (instancias principal y secundaria) en Azure.
2. Agregue NIC de cliente y servidor en ambas instancias.
3. Implemente una ALB con regla de equilibrio de carga cuyo modo de IP flotante esté inhabilitado.
4. Configure la configuración de HA en ambas instancias mediante la GUI de NetScaler.

Paso 1. Implemente dos instancias VPX en Azure.

Cree dos instancias VPX siguiendo estos pasos:

1. Seleccione la versión de NetScaler en Azure Marketplace (en este ejemplo, se utiliza la versión 13.1 de NetScaler).



2. Seleccione el modo de licencia de ADC requerido y haga clic en **Crear**.

NetScaler ADC 14.1 🔖 ⋮
Cloud Software Group

NetScaler ADC 14.1 ♥️ [Add to Favorites](#)
Cloud Software Group | Virtual Machine

Free trial

Plan

NetScaler ADC 14.1 VPX Standard Edi... ▼ Create Start with a pre-set configuration Purchase a reservation

Filter

NetScaler ADC 14.1 VPX Standard Edition - 5000 Mbps

Overview

NetScaler ADC 14.1 VPX Bring Your Own License

NetScaler ADC 14.1 VPX Express - 20 Mbps

NetScaler ADC 14.1 VPX Standard Edition - 10 Mbps

NetScaler ADC 14.1 VPX Premium Edition - 10 Mbps

NetScaler ADC 14.1 VPX Advanced Edition - 10 Mbps

NetScaler ADC 14.1 VPX Standard Edition - 200 Mbps

NetScaler ADC 14.1 VPX Advanced Edition - 200 Mbps

NetScaler ADC 14.1 VPX Premium Edition - 200 Mbps

NetScaler ADC 14.1 VPX Standard Edition - 1000 Mbps

NetScaler ADC 14.1 VPX Advanced Edition - 1000 Mbps

NetScaler ADC 14.1 VPX Premium Edition - 1000 Mbps

Key Benefits:

- Flexibl
- capaci
- Best U

atings + Reviews

very controller that delivers your applications quickly, reliably, and securely, with provide operational consistency and a smooth user experience, NetScaler ADC e

icture with NetScaler ADC on Microsoft Azure by reading the eBook, [available](#)

delivery, a comprehensive centralization management system, and orchestratic tScaler's all-in-one solution brings point solutions under one roof, ensuring sin

ature-rich ADC available across a wide variety of deployment options with the i

gent, global load-balancing service that uses real-time Internet traffic and data

Se abre la página **Crear una máquina virtual**.

3. Complete los detalles requeridos en cada ficha: Conceptos básicos, Discos, Redes, Administración, Supervisión, Avanzada y Etiquetas, para una implementación exitosa.

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](#)

Project details

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ ▼

Availability options ⓘ ▼

Availability zone * ⓘ ▼

[Review + create](#)

< Previous

Next : Disks >

En la ficha **Redes**, cree una nueva red virtual con 3 subredes, una para cada una: NIC de administración, cliente y servidor. De lo contrario, también puede utilizar una red virtual existente. La NIC de administración se crea durante la implementación de la VM. Las NIC de cliente y servidor se crean y se conectan después de crear la máquina virtual. Para el grupo de seguridad de red de NIC, puede realizar una de las siguientes acciones:

- Seleccione **Avanzado** y utilice un grupo de seguridad de red existente que se adapte a sus requisitos.
- Seleccione **Basic** y seleccione los puertos necesarios.

Nota:

También puede cambiar la configuración del grupo de seguridad de red después de que se complete la implementación de la VM.

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. [Learn more](#)

Network interface

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

Virtual network * ⓘ [Create new](#)

Subnet * ⓘ

Public IP ⓘ [Create new](#)

NIC network security group ⓘ None
 Basic
 Advanced

Public inbound ports * ⓘ None
 Allow selected ports

Select inbound ports *

⚠ 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.

Delete public IP and NIC when VM is deleted ⓘ

Enable accelerated networking ⓘ

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options ⓘ None
 Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
 Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

[Review + create](#) [< Previous](#) [Next : Management >](#)

4. Haga clic en Siguiente: **Revisar + crear**.

Una vez que la validación se haya realizado correctamente, revise la configuración básica, las configuraciones de VM, la red y la configuración adicional y haga clic en **Crear**.

Create a virtual machine ...

✔ Validation passed

Basics Disks Networking Management Monitoring Advanced Tags Review + create

📘 Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

NetScaler ADC 14.1
by Cloud Software Group
[Terms of use](#) | [Privacy policy](#)

Not covered by credits ⓘ

2.3000 USD/hr

1 X Standard DS2 v2
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

0.0880 USD/hr

[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name	<input type="text"/>
Preferred e-mail address	<input type="text"/>
Preferred phone number	<input type="text" value="-"/>

⚠ **You have set SSH port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

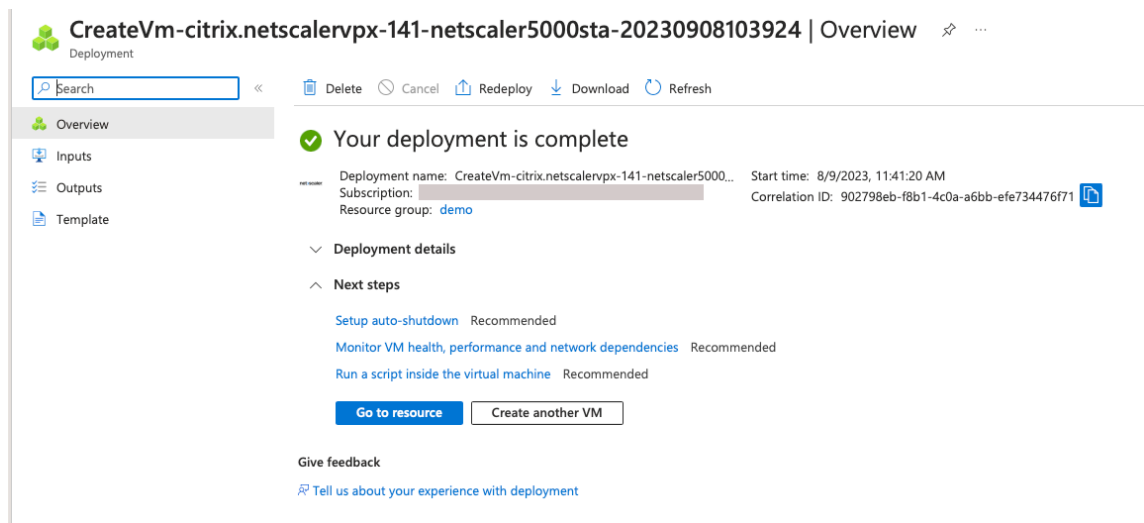
Create

< Previous

Next >

[Download a template for automation](#)

5. Una vez completada la implementación, haga clic en **Ir al recurso** para ver los detalles de la configuración.



Del mismo modo, implemente una segunda instancia de NetScaler VPX.

Paso 2. Agregue NIC de cliente y servidor en ambas instancias.

Nota:

Para conectar más NIC, primero debe detener la VM. En el portal de Azure, seleccione la VM que quiere detener. En la ficha **Descripción general**, haga clic en **Detener**. Espere a que el estado aparezca como **Detenido**.

Para agregar una NIC de cliente en la instancia principal, sigue estos pasos:

1. Vaya a **Redes > Adjuntar interfaz de red**.

Puede seleccionar una NIC existente o crear y conectar una nueva interfaz.

2. Para el grupo de seguridad de red de NIC, puede usar un grupo de seguridad de red existente seleccionando **Avanzado** o crear uno seleccionando **Básico**.

[Home](#) > [vm1-demo | Networking](#) >

Create network interface ...

Project details

Subscription ⓘ

NSDev Platform CA anoop.agarwal@citrix.com

Resource group * ⓘ

demo

[Create new](#)

Location ⓘ

(US) East US

Network interface

Name *

vm1-demo-nic

Virtual network ⓘ

vm1-demo-vnet

Subnet * ⓘ

client (10.2.1.0/24)

NIC network security group ⓘ

None

Basic

Advanced

Public inbound ports * ⓘ

None

Allow selected ports

Select inbound ports

Select one or more ports

i 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 ⓘ

Disabled Enabled

Create

Para agregar una NIC de servidor, siga los mismos pasos que para agregar una NIC de cliente.

La instancia de NetScaler VPX tiene las tres NIC (NIC de administración, NIC de cliente y NIC de servidor) conectadas.

Repita los pasos anteriores para agregar NIC en la instancia secundaria.

Después de crear y conectar las NIC en ambas instancias, reinicie ambas instancias en **Descripción general > Iniciar**.

Nota:

Debe permitir el tráfico a través del puerto en la regla de entrada de la NIC del cliente, que se utilizará más adelante para crear un servidor virtual de equilibrio de carga al configurar la instancia de NetScaler VPX.

Paso 3. Implemente una ALB con regla de equilibrio de carga cuyo modo de IP flotante esté inhabilitado.

Para iniciar la configuración de ALB, siga estos pasos:

1. Vaya a la página **Equilibradores de carga** y haga clic en **Crear**.
2. En la página **Crear equilibrador de cargas**, proporcione los detalles necesarios.

En el siguiente ejemplo, implementamos un equilibrador de carga público regional de SKU estándar.

Create load balancer ...

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region *

SKU * ⓘ Standard
 Gateway
 Basic

Type * ⓘ Public
 Internal

Tier * Regional
 Global

[Review + create](#)

[< Previous](#)

Next : Frontend IP configuration >

[Download a template for automation](#)

Nota:

Todas las IP públicas conectadas a las máquinas virtuales de NetScaler deben tener la misma SKU que la de ALB. Para obtener más información sobre las SKU de ALB, consulte la [documentación de las SKU de Azure Load Balancer](#).

3. En la ficha **Configuración de IP de frontend**, cree una dirección IP o utilice una dirección IP existente.

Create load balancer ...

Basics **Frontend IP configuration** Backend pools Inbound rules Outbound rules Tags Review + create

A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.

[+ Add a frontend IP configuration](#)

Name ↑↓

IP address ↑↓

Add a frontend IP to get started

Add frontend IP configuration ✕

Name *

alb-frontend ✓

IP version

IPv4 IPv6

IP type

IP address IP prefix

Public IP address *

(New) alb-public-ip ∨

[Create new](#)

Gateway Load balancer ⓘ

None ∨

Add

4. En la ficha **Grupos de backend**, seleccione Configuración de grupos de backend basada en NIC y agregue las NIC de cliente de ambas máquinas virtuales de NetScaler.

Create load balancer ...

Basics Frontend IP configuration **Backend pools** Inbound rules Outbound rules Tags Review + create

A backend pool is a collection of resources to which your load balancer can send traffic. A backend pool can contain virtual machines, virtual machine s

[+](#) Add a backend pool

Name	Virtual network	Resource Name	Network interface	IP address
∨ alb-backend-pool				
alb-backend-pool	vm1-demo-vnet	vm1-demo	vm1-demo324_z1	10.2.0.4
alb-backend-pool	vm1-demo-vnet	vm1-demo	client-nic	10.2.1.4

5. En la ficha **Reglas de entrada**, haga clic en **Agregar una regla de equilibrio de carga** y proporcione la dirección IP de frontend y el grupo de backend creados en los pasos anteriores. Seleccione el protocolo y el puerto según sus necesidades. Cree o utilice una sonda de estado existente. Desactive la casilla de verificación **Habilitar IP flotante**.

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 *	<input type="text" value="lb-rule1"/>
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Frontend IP address * ⓘ	<input type="text" value="alb-frontend (To be created)"/>
Backend pool * ⓘ	<input type="text" value="alb-backend-pool"/>
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Port *	<input type="text" value="80"/>
Backend port * ⓘ	<input type="text" value="10"/>
Health probe * ⓘ	<input type="text" value="(new) health-probe1 (TCP:80)"/> Create new
Session persistence ⓘ	<input type="text" value="None"/>
Idle timeout (minutes) * ⓘ	<input type="text" value="4"/>
Enable TCP Reset	<input type="checkbox"/>
Enable Floating IP ⓘ	<input type="checkbox"/>
Outbound source network address translation (SNAT) ⓘ	<input checked="" type="radio"/> (Recommended) Use outbound rules to provide backend pool members access to the internet. Learn more. <input type="radio"/> Use default outbound access. This is not recommended because it can cause SNAT port exhaustion. Learn more.

Save

Cancel

Give feedback

6. Haga clic en **Revisar + Crear**. Una vez superada la validación, haga clic en **Crear**.

Create load balancer ...

✔ Validation passed

Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create

Basics

Subscription	
Resource group	demo
Name	alb1
Region	Southeast Asia
SKU	Standard
Tier	Regional
Type	Public

Frontend IP configuration

Frontend IP configuration name	alb-frontend
Frontend IP configuration IP address	To be created

Backend pools

Backend pool name	alb-backend-pool
-------------------	------------------

Inbound rules

Load balancing rule name	lb-rule1
Health probe name	health-probe1

Outbound rules

None

Tags

None

Create

< Previous

Next >

[Download a template for automation](#) [Give feedback](#)

Paso 4. Configure los parámetros de alta disponibilidad en ambas instancias de NetScaler VPX mediante la GUI de NetScaler.

Después de crear las instancias de NetScaler VPX en Azure, puede configurar HA mediante la GUI de NetScaler.

Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

En la instancia principal, realice los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y la contraseña proporcionados al implementar la instancia.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración de la instancia secundaria, por ejemplo: 10.4.1.5.
4. Seleccione la casilla **Activar el modo INC (configuración de red independiente) en el nodo propio**.
5. Haga clic en **Create**.



← Create HA Node

Remote Node IP Address*

10 . 4 . 1 . 5 ⓘ

Configure remote system to participate High Availability setup

Turn Off HA Monitor interface/channels that are down

Turn on INC (Independent Network Configuration) mode on self node ⓘ

Remote System Login Credential

User Name

Password

Secure Access

En la instancia secundaria, realice los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y la contraseña proporcionados al implementar la instancia.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración de la instancia principal, por ejemplo: 10.4.1.4.
4. Seleccione la casilla **Activar el modo INC (configuración de red independiente) en el nodo propio**.
5. Haga clic en **Create**.

← Create HA Node

Remote Node IP Address*

 ⓘ

Configure remote system to participate High Availability setup

Turn Off HA Monitor interface/channels that are down

Turn on INC(Independent Network Configuration) mode on self node

RPC Node Password

 ⓘ

Remote System Login Credential

User Name

Password

Secure Access

Create **Close**

Antes de continuar, asegúrese de que el **estado de sincronización** de la instancia secundaria aparezca como **SUCCESS** en la página **Nodos**.

Nota:

Ahora, la instancia secundaria tiene las mismas credenciales de inicio de sesión que la instancia

principal.

System > High Availability > Nodes

Nodes 2

Add Edit Delete Statistics Select Action

ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REASON
0	10.4.1.4	citrix-adc-1	Primary	UP	FNARI FD	FNARI FD	-NA-
1	10.4.1.5		Secondary	UP	ENABLED	SUCCESS	-NA-

Total 2 25 Per Page Page 1 of 1

Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambas instancias.

En la instancia principal, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP principal siguiendo estos pasos:
 - a) Introduzca la dirección IP privada de la NIC del cliente de la instancia principal y la máscara de red configurada para la subred del cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Agregue una dirección SNIP principal siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la NIC del servidor de la instancia principal y la máscara de red configurada para la subred del servidor en la instancia principal.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.
4. Agregue una dirección VIP secundaria siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la NIC del cliente de la instancia secundaria y la máscara de red configurada para la subred del cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.

System > Network > IPs > IPv4s

IPs

IPv4s 4 IPv6s 1 Port Allocation

Add Edit Delete Statistics Select Action

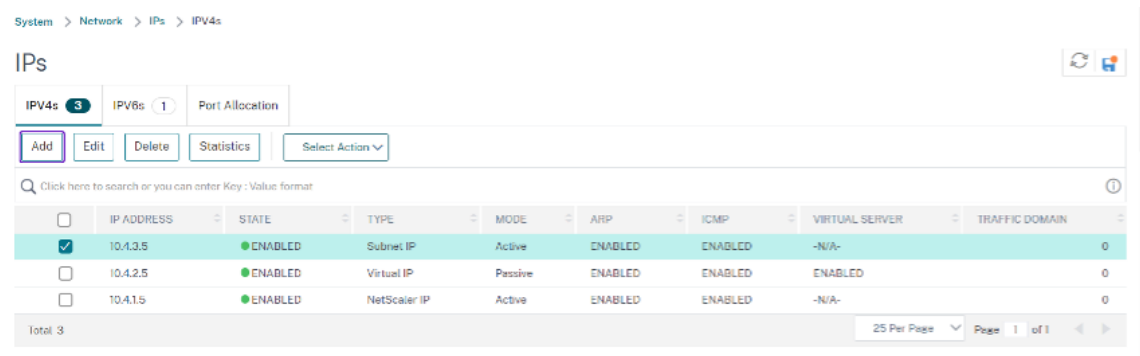
Click here to search or you can enter Key : Value format

IP ADDRESS	STATE	TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	TRAFFIC DOMAIN
10.4.3.4	FNARI FD	Subnet IP	Active	FNARI FD	FNARI FD	-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	FNARI FD	NetScaler IP	Active	FNARI FD	FNARI FD	-N/A-	0

Total 4 25 Per Page Page 1 of 1

En la instancia secundaria, lleve a cabo los siguientes pasos:

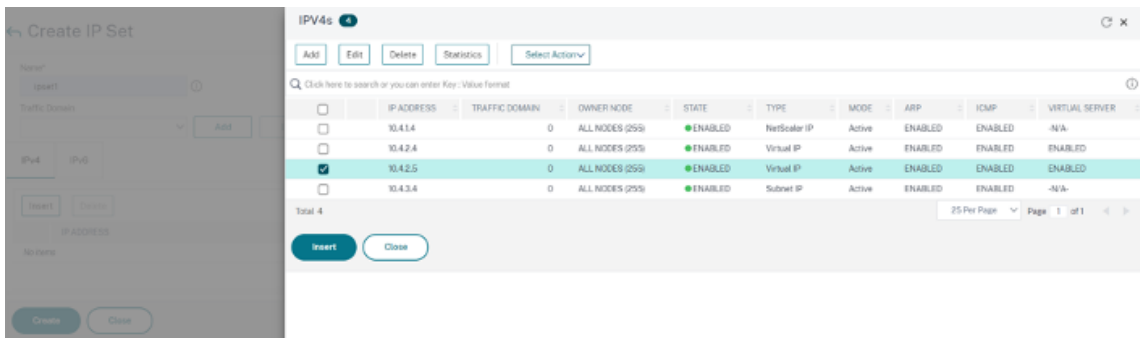
1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP secundaria siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la NIC del cliente de la instancia secundaria y la máscara de red configurada para la subred del cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
3. Agregue una dirección SNIP secundaria siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la NIC del servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor en la instancia secundaria.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.



Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP al VIP secundario en ambas instancias.

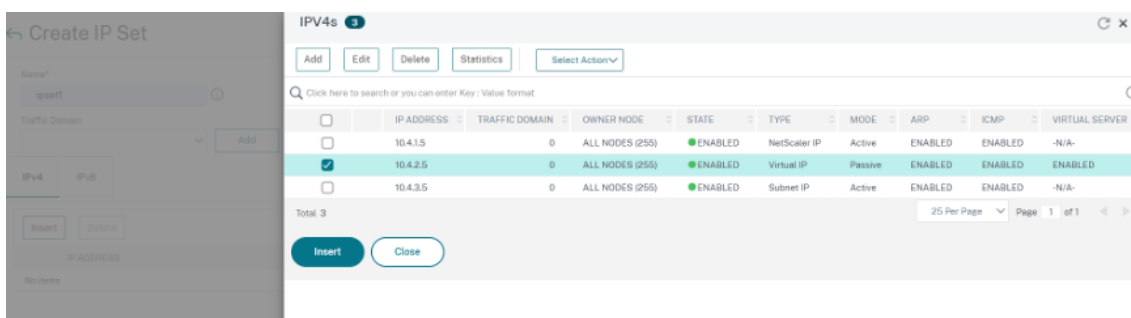
En la instancia principal, realice los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



En la instancia secundaria, realice los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



Nota:

El nombre del conjunto de IP debe ser el mismo en las instancias principal y secundaria.

Paso 4. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga de la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), dirección IP (VIP principal) y Puerto.
3. Haga clic en **Más**. Vaya a **Configuración del conjunto de IP de rango IP**, seleccione **IPset** en el menú desplegable y proporcione el IPset creado en el **paso 3**.
4. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.

[← 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 application is accessible from the internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (RFC1918 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*
v1 ⓘ

Protocol*
HTTP

IP Address type*
IP Address

IP Address*
10 . 4 . 2 . 4 ⓘ

Port*
80 ⓘ

Traffic Domain
Add Edit

IP Range IP Set settings
IPSet
IPSet
Add Edit ⓘ

Redirection Mode*
IP Based

Listen Priority

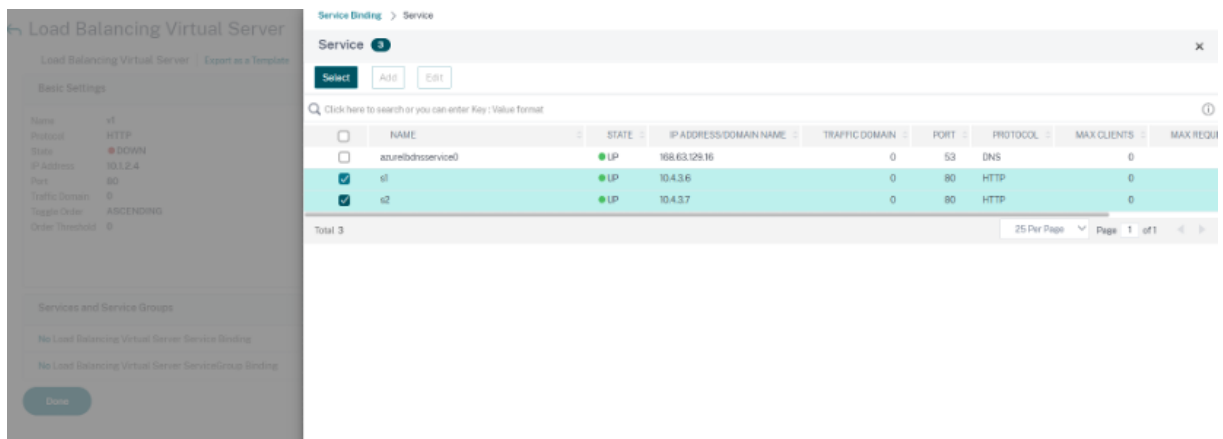
Virtual Server State
 Full State
 AppFlow Logging
 Retain Connections on Cluster

Paso 5. Agregue un servicio o grupo de servicios en la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 6. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga de la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 4** y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 5** y haga clic en **Enlazar**.



Paso 7. Verifique la configuración.

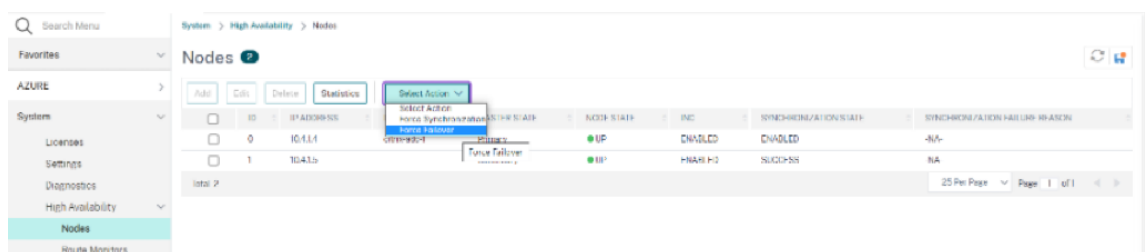
De lo contrario, toda la configuración se pierde tras un reinicio o si se produce un reinicio instantáneo.

Paso 8. Verifique la configuración.

Asegúrese de que se pueda acceder a la dirección IP del frontend de ALB después de una conmutación por error.

1. Copie la dirección IP del frontend de ALB.
2. Pegue la dirección IP en el navegador y asegúrese de que se pueda acceder a los servidores de fondo.
3. En la instancia principal, realice la conmutación por error:

En la GUI de NetScaler, vaya a **Configuración > Sistema > Alta disponibilidad > Acción > Forzar conmutación por error.**



4. Asegúrese de que los servidores back-end estén accesibles después de la conmutación por error a través de la IP de frontend de ALB utilizada anteriormente.

Implemente una zona privada de DNS de NetScaler para Azure

October 17, 2024

Azure DNS es un servicio de la infraestructura de Microsoft Azure para alojar dominios DNS y proporcionar resolución de nombres.

Las zonas privadas DNS de Azure son un servicio centrado en la resolución de nombres de dominio en una red privada. Con las zonas privadas, los clientes pueden usar sus propios nombres de dominio personalizados en lugar de los nombres proporcionados por Azure que están disponibles en la actualidad.

NetScaler, la solución líder de entrega de aplicaciones, es la más adecuada para proporcionar capacidades de equilibrio de carga y GSLB para una zona privada de DNS de Azure. Al suscribirse a la zona privada de DNS de Azure, la empresa puede confiar en la potencia y la inteligencia de NetScaler Global Server Load Balancing (GSLB) para distribuir el tráfico de la intranet entre las cargas de trabajo en varias geografías y centros de datos, conectados a través de túneles VPN seguros. Esta colaboración garantiza a las empresas un acceso sin problemas a parte de la carga de trabajo que desean trasladar a la nube pública de Azure.

Descripción general del DNS de Azure

El Sistema de nombres de dominio (DNS) es responsable de traducir o resolver el nombre de un servicio a su dirección IP. Azure DNS, un servicio de alojamiento para dominios DNS, proporciona resolución de nombres mediante la infraestructura de Microsoft Azure. Además de admitir dominios DNS con conexión a Internet, Azure DNS ahora también admite dominios DNS privados.

Azure DNS proporciona un servicio de DNS fiable y seguro para administrar y resolver nombres de dominio en una red virtual sin necesidad de una solución de DNS personalizada. Al usar zonas DNS privadas, puede usar sus propios nombres de dominio personalizados en lugar de los nombres proporcionados por Azure. El uso de nombres de dominio personalizados le ayuda a adaptar la arquitectura de red virtual para que se adapte mejor a las necesidades de su organización. Proporciona resolución de nombres para máquinas virtuales (VM) dentro de una red virtual y entre redes virtuales. Además, los clientes pueden configurar los nombres de las zonas con una vista de horizonte dividido, lo que permite que una zona DNS privada y una pública compartan un nombre.

¿Por qué elegir NetScaler GSLB para la zona privada DNS de Azure?

En el mundo actual, las empresas desean realizar la transición de sus cargas de trabajo de las instalaciones a la nube de Azure. La transición a la nube les permite aplicar el tiempo de comercialización, los gastos/precio de capital, la facilidad de implementación y la seguridad. El servicio de zona privada DNS de Azure ofrece una propuesta única para las empresas que están realizando la transición de parte de sus cargas de trabajo a la nube de Azure. Estas empresas pueden crear su nombre DNS privado, que tenían durante años en las implementaciones locales, cuando utilizan el servicio de zona privada. Dado que este modelo híbrido de servidores de aplicaciones de intranet se encuentran en

las instalaciones y en la nube de Azure conectados a través de túneles VPN seguros, el único desafío es tener un acceso perfecto a estas aplicaciones de intranet. NetScaler resuelve este caso de uso único con su función de equilibrio de carga global, que enruta el tráfico de la aplicación a las cargas de trabajo o servidores distribuidos más óptimos, ya sea en las instalaciones o en la nube de Azure, y proporciona el estado del servidor de aplicaciones.

Caso de uso

Los usuarios de una red local y de diferentes redes virtuales de Azure pueden conectarse a los servidores más óptimos de una red interna para acceder al contenido requerido. Esto garantiza que la aplicación esté siempre disponible, que los costes estén optimizados y que la experiencia del usuario sea buena. La gestión del tráfico privado (PTM) de Azure es el requisito principal en este caso. Azure PTM garantiza que las consultas DNS de los usuarios se resuelvan en una dirección IP privada adecuada del servidor de aplicaciones.

Solución de casos de uso

NetScaler incluye la función de equilibrio de carga global de servidores (GSLB) para cumplir con el requisito de PTM de Azure. GSLB actúa como un servidor DNS, que recibe las solicitudes DNS y resuelve la solicitud DNS en una dirección IP adecuada para proporcionar:

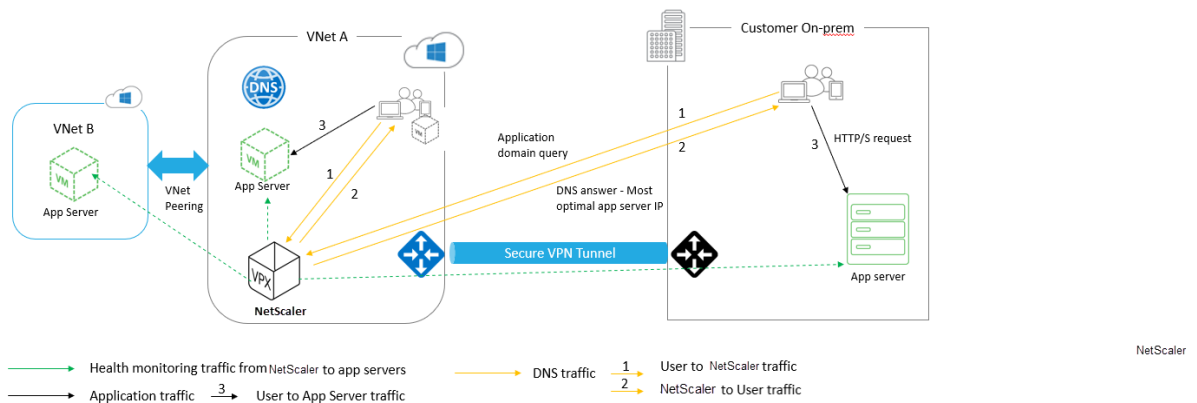
- Conmutación por error perfecta basada en DNS.
- Migración gradual de las instalaciones a la nube.
- Prueba A/B de una nueva función.

Entre los muchos métodos de equilibrio de carga compatibles, los siguientes métodos pueden resultar útiles en esta solución:

1. Round Robin
2. Proximidad estática (selección de servidor basada en la ubicación). Se puede implementar de dos maneras:
 - a) GSLB basado en la subred de cliente EDNS (ECS) en NetScaler.
 - b) Implemente un reenviador de DNS para cada red virtual.

Topología

La siguiente figura muestra la implementación GSLB de NetScaler para una zona DNS privada de Azure.



Un usuario puede acceder a cualquier servidor de aplicaciones en Azure o local según el método GSLB de NetScaler en una zona DNS privada de Azure. Todo el tráfico entre la red virtual local y la de Azure se realiza únicamente a través de un túnel VPN seguro. El tráfico de aplicaciones, el tráfico DNS y el tráfico de supervisión se muestran en la topología anterior. Según la redundancia requerida, NetScaler y el reenviador de DNS se pueden implementar en las redes virtuales y los centros de datos. Para simplificar, aquí solo se muestra un NetScaler, pero recomendamos al menos un conjunto de NetScaler y reenviador de DNS para la región de Azure. Todas las consultas de DNS de los usuarios van primero al reenviador de DNS que tiene reglas definidas para reenviar las consultas a un servidor DNS adecuado.

Configuración de NetScaler para la zona privada DNS de Azure

Productos y versiones probados:

Producto	Versión
Azure	Suscripción Cloud
NetScaler VPX	BYOL (traiga su propia licencia)

Nota:

La implementación se ha probado y sigue siendo la misma con NetScaler versión 12.0 y versiones posteriores.

Requisitos previos

Los siguientes son requisitos previos generales.

- Cuenta de portal de Microsoft Azure con una suscripción válida.

- Garantice la conectividad (túnel VPN seguro) entre las instalaciones y la nube de Azure. Para configurar un túnel VPN seguro en Azure, consulte [Paso a paso: configuración de una puerta de enlace VPN de sitio a sitio entre Azure y el entorno local](#).

Descripción de la solución

Si desea alojar una aplicación, la zona privada de DNS de Azure (rr.ptm.mysite.net) que se ejecuta en HTTPS y se implementa en Azure y en las instalaciones con acceso a la intranet basado en el método de equilibrio de carga GSLB por turnos. Para lograr esta implementación, habilite GSLB para la zona DNS privada de Azure con NetScaler, que consta de las siguientes configuraciones:

1. Configure Azure y la configuración local.
2. Dispositivo NetScaler en la red virtual Azure.

Configurar Azure y la configuración local

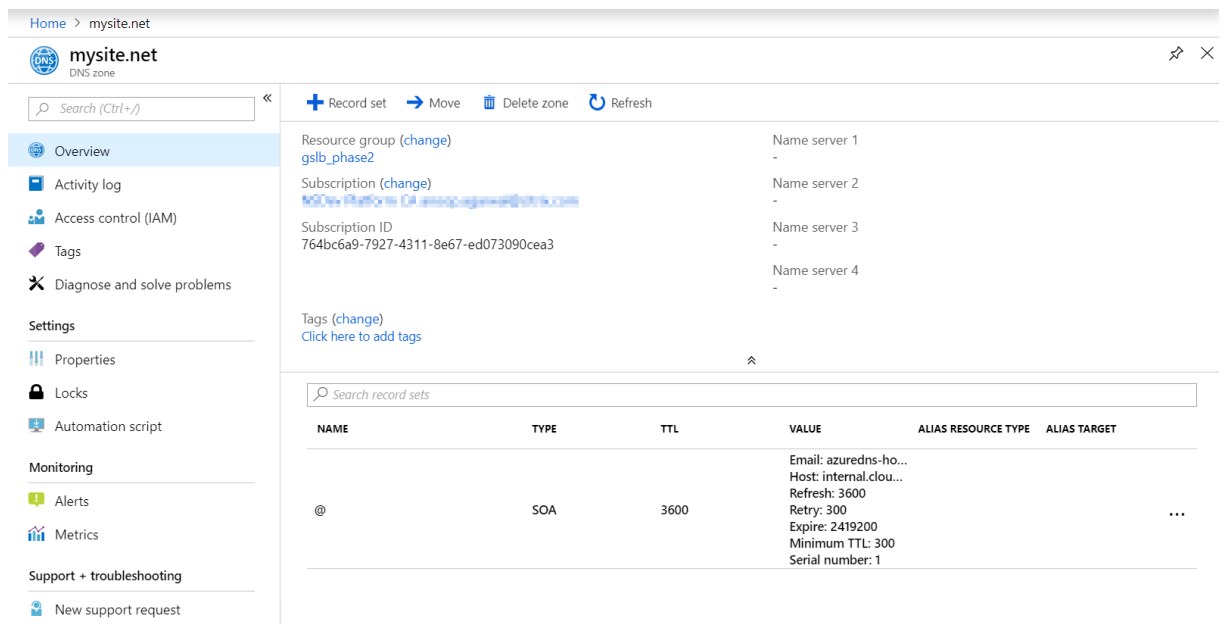
Como se muestra en la topología, configure la red virtual de Azure (vNet A, vNet B en este caso) y la configuración local.

1. Cree una zona DNS privada de Azure con un nombre de dominio (mysite.net).
2. Cree dos redes virtuales (vNet A, vNet B) en un modelo Hub and Spoke en una región de Azure.
3. Implemente App Server, reenviador de DNS, cliente Windows 10 Pro y NetScaler en VNet A.
4. Implemente un servidor de aplicaciones e implemente un reenviador de DNS si hay algún cliente en la VNet B.
5. Implemente un servidor de aplicaciones, un reenviador de DNS y un cliente Windows 10 pro en las instalaciones.

Zona DNS privada de Azure

Cree una zona DNS privada de Azure con un nombre de dominio.

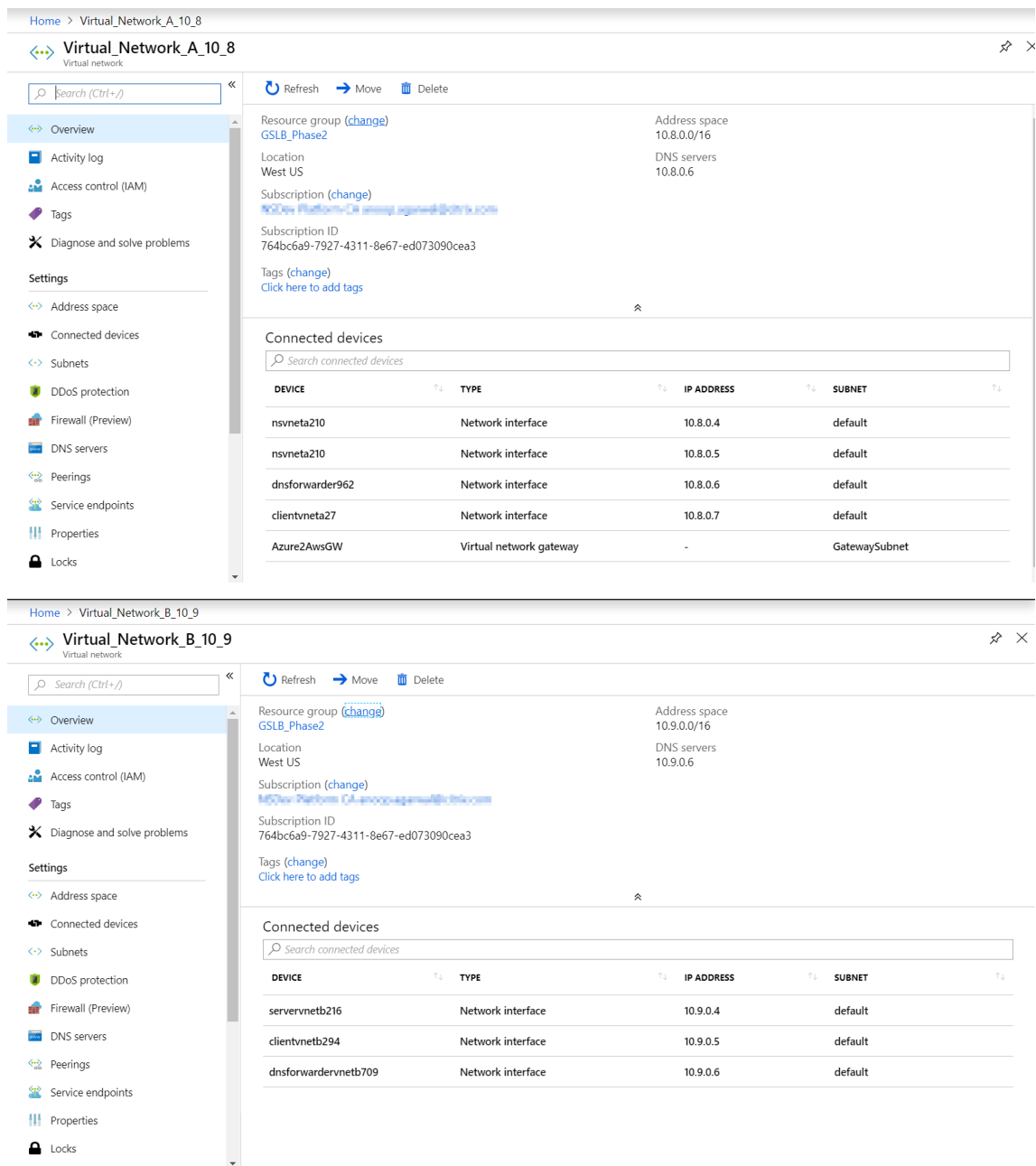
1. Inicie sesión en el portal de Azure y seleccione o cree un panel.
2. Haga clic en **crear un recurso** y busque la zona DNS para crear (mysite.net en este caso) una zona DNS privada de Azure con un nombre de dominio (mysite.net).



Redes virtuales de Azure (vNet A, vNet B) en el modelo Hub and spoke

Cree dos redes virtuales (vNet A, vNet B) en un modelo Hub and Spoke en una región de Azure.

1. Cree dos redes virtuales.
2. Seleccione el mismo panel y haga clic en **crear un recurso** y busque redes virtuales para crear dos redes virtuales, a saber, VNet A y VNet B en la misma región y compáralas para formar un modelo Hub and Spoke, como se muestra en la siguiente imagen. Para obtener más información sobre cómo configurar una topología de concentrador y radio, consulte [Implementación de una topología de red concentrador radial](#) en Azure.



Peering de vNet A a vNet B

Para emparejar la VNet A y la VNet B:

1. Haga clic en **Interconexiones en el menú Configuración**** de la VNet A y en la VNet B del mismo nivel.
2. Habilite **Permitir el tráfico reenviado** y **Permitir el tránsito de la puerta** de enlace, como se muestra en la siguiente imagen.

Home > Virtual_Network_A_10_8 - Peerings > Vnet_A_to_B

Vnet_A_to_B

Virtual_Network_A_10_8

Save 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_B_10_9

Configuration

Allow virtual network access **Enabled**

Allow forwarded traffic

Allow gateway transit

Use remote gateways

La siguiente imagen muestra el emparejamiento correcto de la vNet A a la vNet B.

Home > Virtual_Network_A_10_8 - Peerings

Virtual_Network_A_10_8 - Peerings

Virtual network

Search (Ctrl+)

+ Add

Search peerings

NAME	PEERING STATUS	PEER	GATEWAY 1
Vnet_A_to_B	Connected	Virtual_Network_B_10_9	Enabled

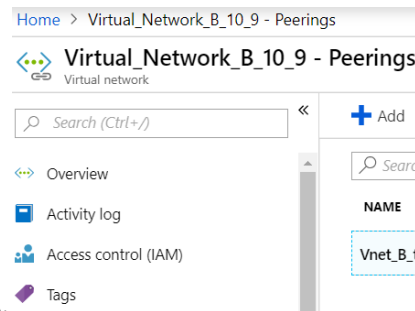
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Peering de vNet B a vNet A

Para emparejar la VNet B y la VNet A:

1. Haga clic en **Emparejamiento** en el menú **Configuración** de la VNet B y en la VNet A.
2. Habilite **Permitir tráfico reenviado** y use puertas de enlace remotas como se muestra en la siguiente imagen.

1 ! [VNet B to A] (/en-us/vpx/media/image-07.png)



La siguiente imagen muestra el emparejamiento correcto de la VNet B a la VNet A.

Implemente el servidor de aplicaciones, el reenviador de DNS, el cliente Windows 10 Pro y NetScaler en la VNet A

Discutiremos brevemente sobre el servidor de aplicaciones, el reenviador de DNS, el cliente Windows 10 pro y NetScaler en la VNet A.

1. Seleccione el mismo panel y haga clic en **Crear un recurso**.
2. Busque las instancias respectivas y asigne una IP desde la subred A de la vNet.

Servidor de aplicaciones El servidor de aplicaciones no es más que el servidor web (servidor HTTP) en el que se implementa un servidor Ubuntu 16.04 como instancia en la máquina virtual Azure o local. Para convertirlo en un servidor web, en la línea de comandos, escriba:

```
sudo apt install apache2
```

Cliente de Windows 10 Pro Inicie la instancia de Windows 10 pro como máquina cliente en la vNet A y en las instalaciones.

NetScaler NetScaler complementa la zona privada de Azure DNA con un chequeo de estado y análisis de NetScaler MAS. Inicie un dispositivo NetScaler desde Azure Marketplace según sus requisitos, aquí hemos utilizado NetScaler (BYOL) para esta implementación.

Para ver los pasos detallados sobre cómo implementar NetScaler en Microsoft Azure. Consulte [Implementar una instancia de NetScaler VPX en Microsoft Azure](#).

Después de la implementación, use NetScaler IP para configurar NetScaler GSLB.

reenviador de DNS Se utiliza para reenviar las solicitudes de los clientes de los dominios alojados enlazados a NetScaler GSLB (ADNS IP). Inicie un servidor Ubuntu 16.04 como instancia de Linux (servidor Ubuntu 16.04) y consulte la siguiente URL para saber cómo configurarlo como reenviador de DNS.

Nota:

Para el método de equilibrio de carga GSLB por turnos, basta con un reenviador de DNS para la región de Azure, pero para la proximidad estática, necesitamos un reenviador de DNS por red virtual.

1. Después de implementar el reenviador, cambie la configuración del servidor DNS de la red virtual A de predeterminada a personalizada con la IP del reenviador DNS de vNet A, como se muestra en la siguiente imagen.
2. Modifique el `named.conf.options` archivo en el reenviador DNS de vNet A para añadir reglas de reenvío para el dominio (`mysite.net`) y el subdominio (`ptm.mysite.net`) a la IP ADNS de NetScaler GSLB.
3. Reinicie el reenviador de DNS para que refleje los cambios realizados en el archivo `named.conf.options`.

Configuración del reenviador DNS VNet A

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

Nota:

Para la dirección IP de la zona de dominio («mysite.net»), utilice la dirección IP DNS de su región de Azure. Para la dirección IP de zona del subdominio («ptm.mysite.net»), use todas las direc-

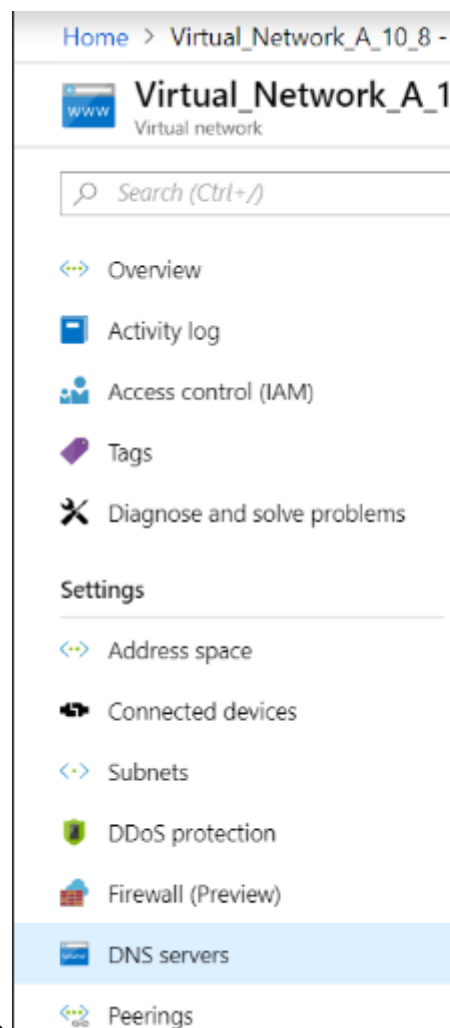
ciones IP ADNS de sus instancias GSLB.

Implemente un servidor de aplicaciones y un reenviador de DNS si hay algún cliente en la VNet B

1. Para la red virtual B, seleccione el mismo panel y haga clic en **crear un recurso**.
2. Busque las instancias respectivas y asigne una IP desde la subred VNet B.
3. Inicie el servidor de aplicaciones y el reenviador de DNS si hay un equilibrio de carga GSLB de proximidad estática similar al de la VNet A.
4. Edite la configuración del reenviador DNS de VNet B `named.conf.options` como se muestra en la siguiente configuración:

Configuración del reenviador DNS de vNet B:

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

La siguiente imagen muestra la configuración del reenviador DNS de la VNet B:

Implemente el servidor de aplicaciones, el reenviador de DNS y el cliente Windows 10 pro en las instalaciones

1. En el caso de las instalaciones, inicie las máquinas virtuales de forma remota e incorpore el servidor de aplicaciones, el reenviador de DNS y el cliente Windows 10 pro de forma similar a la vNet A.
2. Edite la configuración del reenviador de DNS local `named.conf.options` como se muestra en el siguiente ejemplo.

Configuración del reenviador de DNS local

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

```
7     }
8 ;
9     zone "ptm.mysite.net" {
10
11         type forward;
12         forwarders {
13     10.8.0.5; }
14 ;
15     }
16 ;
```

Para ello `mysite.net`, hemos asignado la IP del reenviador de DNS de la vNet A en lugar de la IP del servidor de zona DNS privada de Azure porque es una dirección IP especial a la que no se puede acceder desde las instalaciones locales. Por lo tanto, este cambio es necesario en la configuración del reenviador de DNS de On-premise.

Configurar NetScaler en la red virtual de Azure

Como se muestra en la topología, implemente NetScaler en la red virtual de Azure (VNet A en este caso) y acceda a él a través de la GUI de NetScaler.

Configuración de NetScaler GSLB

1. Cree el servicio ADNS.
2. Cree sitios locales y remotos.
3. Cree servicios para los servidores virtuales locales.
4. Cree servidores virtuales para los servicios GSLB.

Añadir servicio ADNS

1. Inicie sesión en la GUI de NetScaler.
2. En la pestaña **Configuración**, vaya a **Administración del tráfico > Equilibrio de carga > Servicios**.
3. Añada un servicio. Le recomendamos que configure el servicio ADNS tanto en TCP como en UDP, como se muestra en la siguiente imagen:

Load Balancing Service

Basic Settings

Service Name*



New Server Existing Server

Server*



Protocol*



Port*

 More

← Load Balancing Service

Basic Settings

Service Name*

 ?

New Server Existing Server

IP Address*

 ?

Protocol*

 ?

Port*

▶ More

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
- Load Balancing >
- Virtual Servers
- Services
- Service Groups
- Monitors
- Metric Tables

Traffic Management / Load Balancing / Services / Services

Services ↻ 📄

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 Dom
<input type="checkbox"/>	azurelbndnservice0	DOWN	168.63.129.16	53	DNS	0	0	SERVER	
<input type="checkbox"/>	s_adns	UP	10.8.0.5	53	ADNS	0	0	SERVER	

Añadir sitios GSLB

1. Agregue sitios locales y remotos entre los que se configurará GSLB.
2. En la ficha **Configuración**, vaya a **Administración del tráfico > GSLB > Sitios GSLB**. Agregue un sitio como se muestra en el siguiente ejemplo y repita el mismo procedimiento para otros sitios.

← Create GSLB Site

Name*
 ?

Type
 ▾

Site IP Address*

Public IP Address

Parent Site Backup Parent Sites

Parent Site Name

Trigger Monitors*
 ▾

Cluster IP

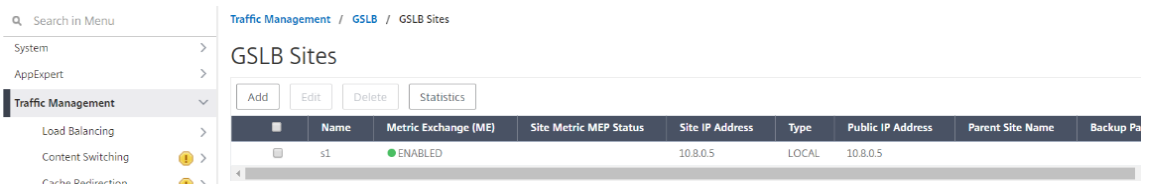
Public Cluster IP

NAPTR Replacement Suffix
 ?

Metric Exchange

Network Metric Exchange

Persistence Session Entry Exchange



Añadir servicios GSLB

1. Agregue servicios GSLB para los servidores virtuales locales y remotos que equilibran la carga de los servidores de aplicaciones.
2. En la pestaña **Configuración**, vaya a **Administración del tráfico > GSLB > Servicios GSLB**.
3. Agregue los servicios como se muestra en los siguientes ejemplos.
4. Enlace el monitor HTTP para comprobar el estado del servidor.

← GSLB Service

Basic Settings

Service Name*
 ?

Site Name*
 ▼ +

Site Type

Type*
 ▼

Service Type*
 ▼

Port*

Existing Servers
 New Server
 Virtual Servers

Server Name*

10.8.0.6

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. Después de crear el servicio, vaya a la pestaña **Configuración avanzada** dentro del servicio GSLB.

6. Haga clic en **Agregar monitor** para vincular el servicio GSLB con un monitor HTTP y mostrar el

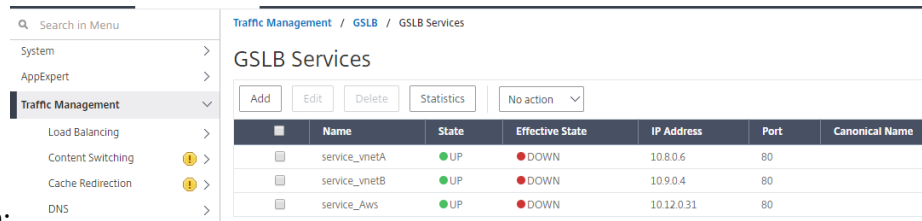
GSLB Service Load Balancing Monitor Binding

	Monitor Name	Weight	State	Current State	Last Response
<input type="checkbox"/>	http	1	true	● UP	Success - HTTP response code 200 received.

estado del servicio.

7. Una vez enlazado con el monitor HTTP, el estado de los servicios se marca como UP, como se

muestra en la siguiente imagen:



Agregar servidor virtual GSLB

Agregue un servidor virtual GSLB a través del cual se pueda acceder a los servicios GSLB de alias de los servidores de aplicaciones.

1. En la pestaña **Configuración**, vaya a **Administración del tráfico > GSLB > Servidores virtuales GSLB**.
2. Agregue los servidores virtuales como se muestra en el siguiente ejemplo.
3. Enlazar los servicios GSLB y el nombre de dominio a él.

← GSLB Virtual Server

Basic Settings

Name* ?

DNS Record Type* A ▼

Service Type* HTTP ▼

Enable after Creating

AppFlow Logging

When this Virtual Server is DOWN

Do not send any service's IP address in response (EDR)

When this Virtual Server is UP

Send all "active" service IPs' in response (MIR)

EDNS Client Subnet

Respond with ECS option in the response for a DNS query with ECS

Validate ECS address is a private or unroutable address

Comments

- Tras crear el servidor virtual GSLB y seleccionar el método de equilibrio de carga adecuado (Round Robin en este caso), vincule los servicios y dominios de GSLB para completar el paso.

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)
☐	rr.ptm.mysite.net	5			0	3600

Close

5. Vaya a la pestaña **Configuración avanzada** del servidor virtual y haga clic en la pestaña **Agregar dominios** para vincular un dominio.
6. Vaya a **Avanzado > Servicios** y haga clic en la flecha para vincular un servicio GSLB y vincular los tres servicios (vNet A, vNet B, local) al servidor virtual.

GSLB Services and GSLB Servicegroup Binding									
	Service Name	IP Address	Port	Protocol	Canonical Name	State	Effective State	Weight	Dynamic Weight
<input type="checkbox"/>	service_vnetA	10.8.0.6	80	HTTP		UP	DOWN	1	0
<input type="checkbox"/>	service_vnetB	10.9.0.4	80	HTTP		UP	DOWN	1	0
<input type="checkbox"/>	service_Aws	10.12.0.31	80	HTTP		UP	DOWN	1	0

Después de vincular los servicios y el dominio de GSLB al servidor virtual, aparece como se muestra en la siguiente imagen:

← GSLB Virtual Server

Basic Settings

Name	vserver_rr	AppFlow Logging	ENABLED
DNS Record Type	A	EDR	DISABLED
Service Type	HTTP	MIR	DISABLED
State	UP	ECS	DISABLED
		ECS Address Validation	DISABLED

GSLB Services and GSLB Servicegroup Binding

- 3 GSLB Virtual Server to GSLBService Bindings
- No GSLB Virtual Server ServiceGroup Binding

GSLB Virtual Server Domain Binding

- 1 GSLB Virtual Server Domain Binding

ADNS Service

- 1 Service

Method

Choose Method	ROUNDROBIN	Backup Method	NONE
Tolerance (ms)	0	IPv6 Mask Length	128
IPv4 Netmask	255.255.255.255	Dynamic Weight	DISABLED

Done

Compruebe si el servidor virtual GSLB está funcionando y en buen estado al 100%. Cuando el monitor muestra que el servidor está activo y en buen estado, significa que los sitios están sincronizados y que los servicios de back-end están disponibles.

Traffic Management / GSLB / GSLB Virtual Servers

GSLB Virtual Servers

Add Edit Delete Statistics No action

	Name	State	Protocol	% Health
<input type="checkbox"/>	vserver_rr	UP	HTTP	100.00% 3 UP/0 DOWN
<input type="checkbox"/>	vserver_sp	UP	HTTP	100.00% 3 UP/0 DOWN

Para probar la implementación, acceda a la URL del dominio rr.ptm.mysite.net desde una máquina cliente en la nube o una máquina cliente local. Si accede a él desde una máquina cliente Windows en la nube, asegúrese de acceder al servidor de aplicaciones local en una zona DNS privada

sin necesidad de soluciones de DNS personalizadas o de terceros.

Configurar una instancia de NetScaler VPX para usar redes aceleradas de Azure

October 17, 2024

Las redes aceleradas permiten la tarjeta NIC de función virtual (VF) de virtualización de E/S de raíz única (SR-IOV) en una máquina virtual, lo que mejora el rendimiento de la red. Puede utilizar esta función con cargas de trabajo pesadas que necesitan enviar o recibir datos a un mayor rendimiento con streaming fiable y una menor utilización de la CPU. Cuando una NIC está habilitada con redes aceleradas, Azure agrupa la interfaz paravirtualizada (PV) existente de la NIC con una interfaz VF SR-IOV. El soporte de la interfaz VF SR-IOV permite y mejora el rendimiento de la instancia NetScaler VPX.

Las redes aceleradas ofrecen las siguientes ventajas:

- Latencia inferior
- Mayor rendimiento de paquetes por segundo (pps)
- Rendimiento mejorado
- Fitter reducido
- Disminución del uso de CPU

Nota:

Las instancias de NetScaler VPX admiten las redes aceleradas de Azure a partir de la versión 13.0, compilación 76.29.

Requisitos previos

- Asegúrese de que el tamaño de su máquina virtual cumple los requisitos de la red acelerada de Azure.
- Detenga las máquinas virtuales (individuales o en un conjunto de disponibilidad) antes de habilitar la red acelerada en cualquier NIC.

Limitaciones

Las redes aceleradas solo se pueden habilitar en algunos tipos de instancias. Para obtener más información, consulte [Tipos de instancias compatibles](#).

NIC compatibles para redes aceleradas

Azure proporciona las NIC Mellanox ConnectX3, ConnectX4 y ConnectX5 en modo SR-IOV para acelerar las redes.

Cuando la red acelerada está habilitada en una interfaz NetScaler VPX, Azure incluye la interfaz ConnectX3, ConnectX4 o ConnectX5 con la interfaz PV existente de un dispositivo NetScaler VPX.

Para obtener más información sobre cómo habilitar redes aceleradas antes de conectar una interfaz a una máquina virtual, consulte [Creación de una interfaz de red con redes aceleradas](#).

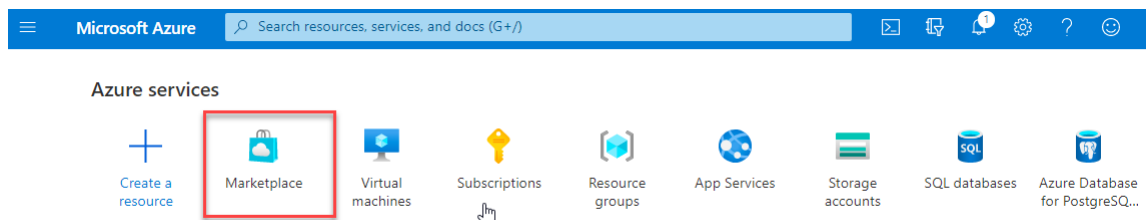
Para obtener más información sobre cómo habilitar redes aceleradas en una interfaz existente de una máquina virtual, consulte [Habilitar interfaces existentes en una máquina virtual](#).

Cómo habilitar las redes aceleradas en una instancia de NetScaler VPX mediante la consola de Azure

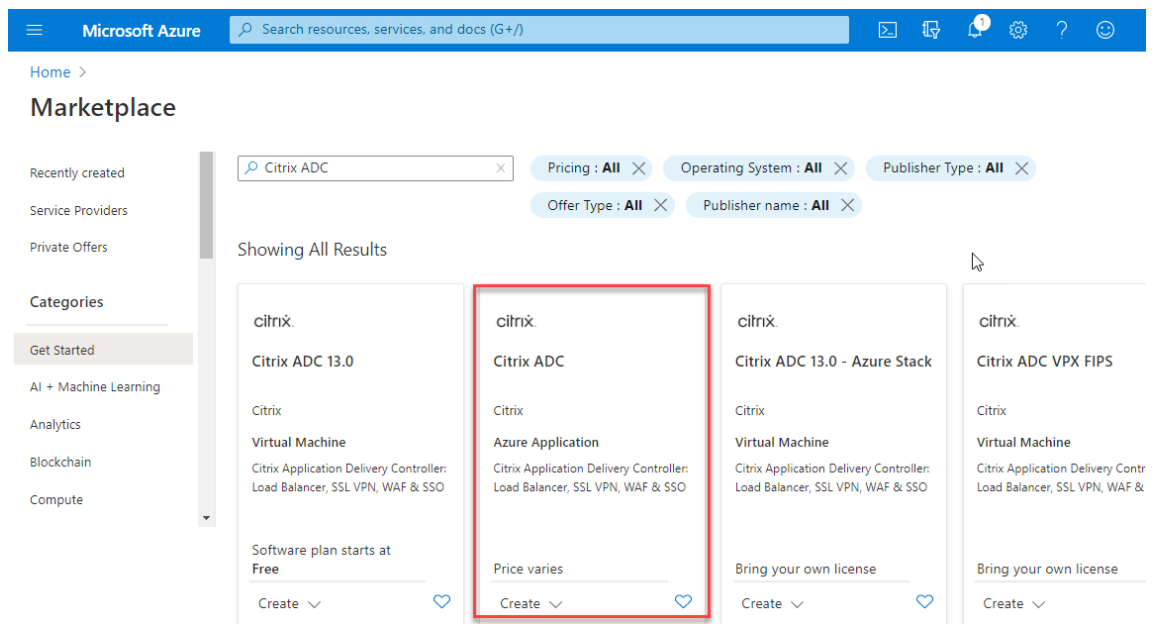
Puede habilitar la red acelerada en una interfaz específica mediante la consola de Azure o Azure PowerShell.

Siga los siguientes pasos para habilitar redes aceleradas mediante conjuntos de disponibilidad o zonas de disponibilidad de Azure.

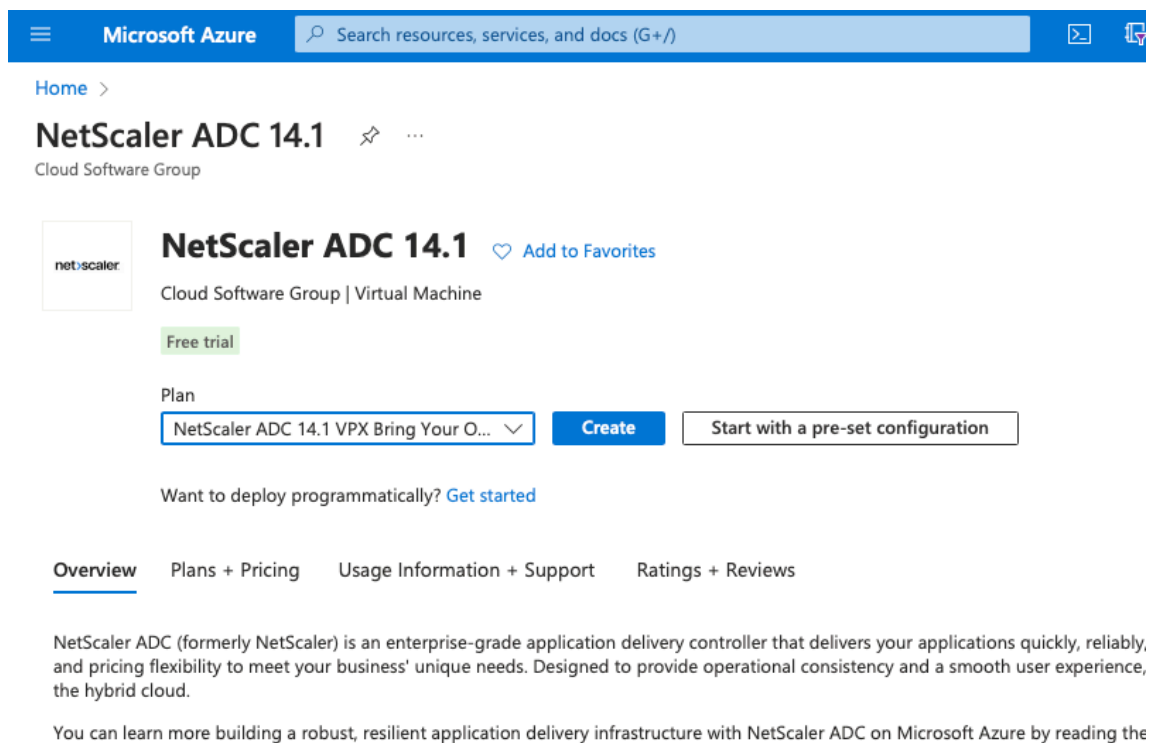
1. Inicie sesión en el [portal de Azure](#) y vaya a **Azure Marketplace**.



2. En **Azure Marketplace**, busque **NetScaler**.



3. Seleccione un plan de NetScaler que no sea FIPS junto con la licencia y haga clic en **Crear**.



Aparece la página **Crear NetScaler**.

4. En la ficha **Conceptos básicos**, cree un grupo de recursos. En la ficha **Parámetros**, introduce los detalles de la región, el nombre de usuario del administrador, la contraseña de administrador, el tipo de licencia (SKU de máquina virtual) y otros campos.

Create a virtual machine ...

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ ▼

Availability options ⓘ ▼

Availability zone * ⓘ ▼

🔗 You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) ↗

Security type ⓘ ▼

Image * ⓘ ▼

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64
 x64

📘 Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Size * ⓘ ▼

[See all sizes](#)

Administrator account

Authentication type ⓘ SSH public key
 Password

Username * ⓘ ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ None
 Allow selected ports

Select inbound 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.

[Review + create](#)

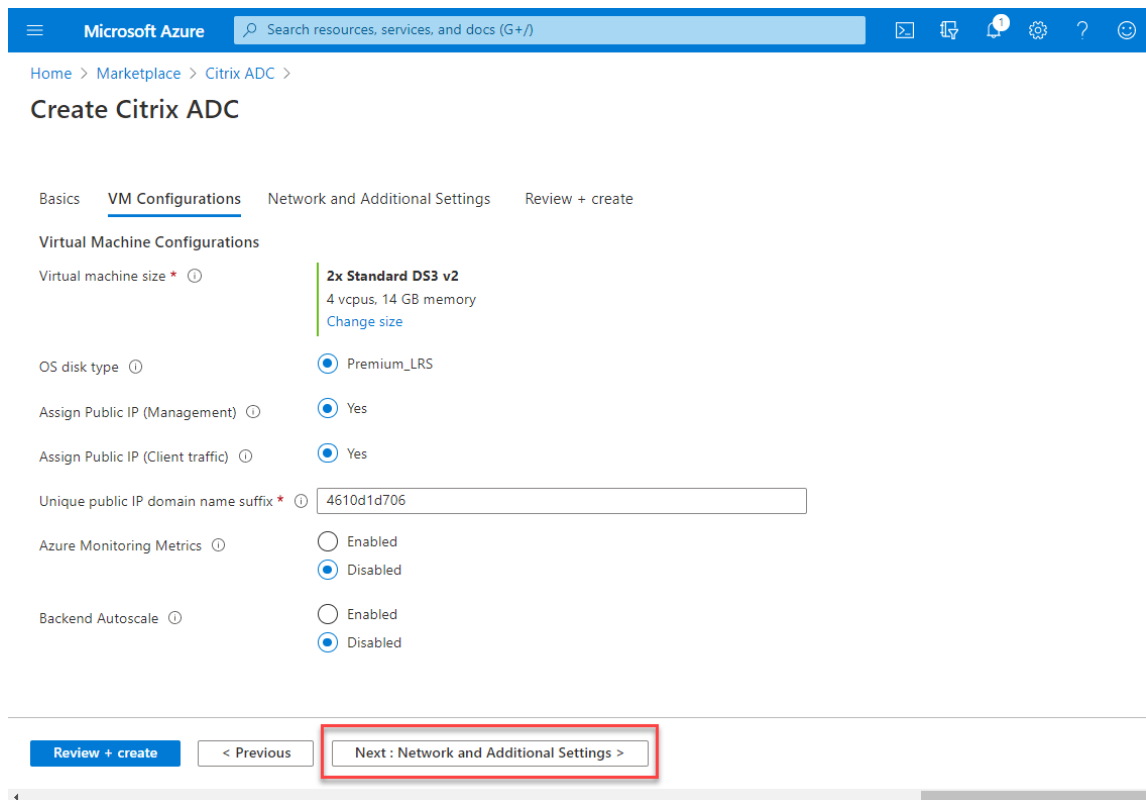
[< Previous](#)

[Next : Disks >](#)

5. Haga clic en **Siguiente: Configuraciones de VM.**

En la página **Configuraciones de VM**, realice lo siguiente:

- a) Configure un sufijo de nombre de dominio IP público.
- b) Habilitar o inhabilitar las **métricas de Azure Monitoring**.
- c) Habilitar o inhabilitar la **escalabilidad automática de backend**.



6. Haga clic en **Siguiente: Red y configuración adicional.**

En la página **Red y Configuración adicional**, cree una cuenta de diagnóstico de arranque y configure los ajustes de red.

En la sección **Redes aceleradas**, tiene la opción de habilitar o inhabilitar la red acelerada por separado para la interfaz de administración, la interfaz del cliente y la interfaz del servidor.

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. [Learn more](#)

Network interface

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

Virtual network *	<input type="text" value="(new) vpx-aan-vnet"/>
	Create new
Subnet *	<input type="text" value="(new) default (10.6.0.0/24)"/>
Public IP	<input type="text" value="(new) vpx-aan-ip"/>
	Create new
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="SSH (22)"/>

⚠ 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.

Delete public IP and NIC when VM is deleted	<input type="checkbox"/>
Enable accelerated networking	<input checked="" type="checkbox"/>

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options	<input checked="" type="radio"/> None <input type="radio"/> Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows. <input type="radio"/> Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
------------------------	---

7. Haga clic en **Siguiente: Revisar + crear**.

Una vez que la validación se haya realizado correctamente, revise la configuración básica, las configuraciones de VM, la red y la configuración adicional y haga clic en **Crear**. El grupo de recursos de Azure puede tardar algún tiempo en crearse con las configuraciones necesarias.

Microsoft Azure Search resources, services, and docs (G+)

Home > Marketplace > Citrix ADC >

Create Citrix ADC

Validation Passed

Basics VM Configurations Network and Additional Settings **Review + create**

PRODUCT DETAILS

Citrix ADC
by Citrix
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	NSDev Platform CA
Resource group	test-aan
Region	South Central US
Citrix ADC Release Version	13.0
License Subscription	Bring Your Own License
Virtual Machine name prefix	citrix-adc-vpx
Username	
Password	*****
Azure Monitoring Metrics	Disabled
Backend Autoscale	Disabled

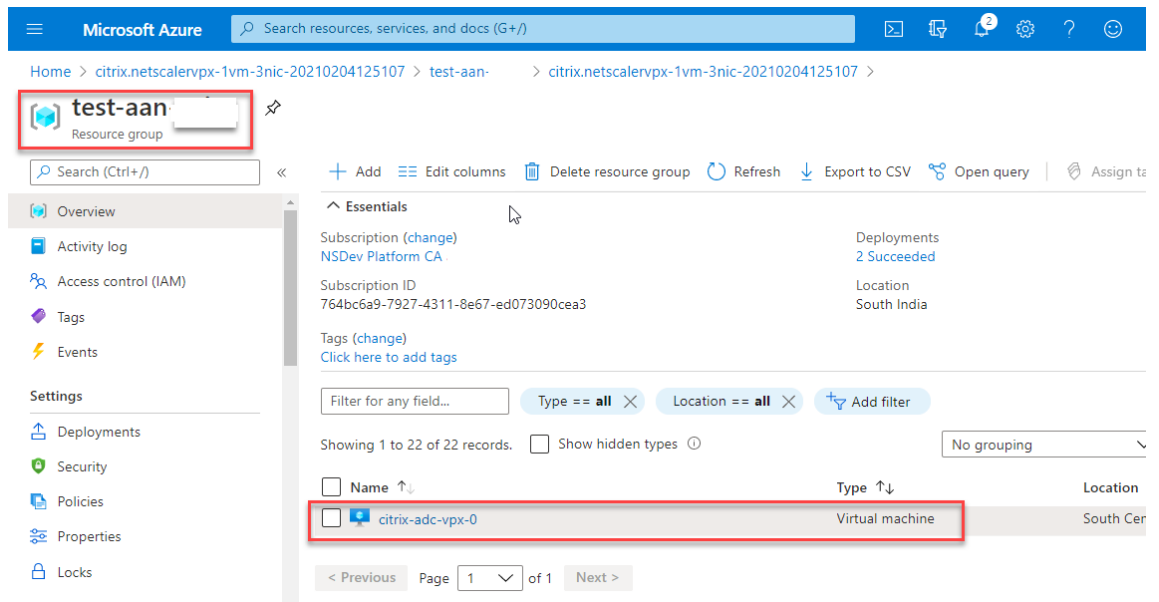
Network and Additional Settings

Diagnostic storage account	citrixadcpx4610d1d706
Virtual network	citrix-adc-vpx-virtual-network
Management Subnet	01-management-subnet
Address prefix (Management Subnet)	172.17.40.0/24
Client Subnet	11-client-subnet
Address prefix (Client Subnet)	172.17.41.0/24
Server Subnet	12-server-subnet
Address prefix (Server Subnet)	172.17.42.0/24
Accelerated Networking (Management I...	On
Accelerated Networking (Client Interface)	On
Accelerated Networking (Server Interface)	On
Public IP address	citrix-adc-vpx-nsip-0
Domain name label	citrix-adc-vpx-nsip-0-4610d1d706
Public IP address	citrix-adc-vpx-nsip-1
Domain name label	citrix-adc-vpx-nsip-1-4610d1d706
Public IP address	citrix-adc-vpx-vip
Domain name label	citrix-adc-vpx-vip-4610d1d706
Ports open for Management public IP	ssh (22)

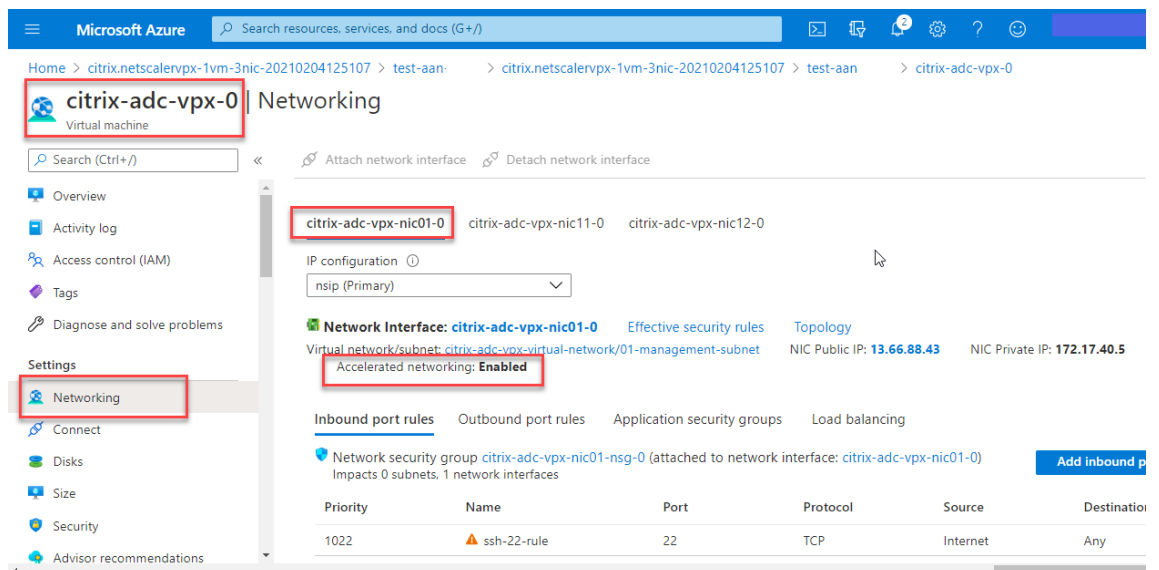
Create < Previous Next Download a template for automation

8. Una vez completada la implementación, seleccione el **grupo de recursos** para ver los detalles

de la configuración.



- Para verificar las configuraciones de redes aceleradas, seleccione **Máquina virtual > Redes**. El estado Redes aceleradas se muestra como **Habilitado o Inhabilitado**** para cada NIC.



Habilitar redes aceleradas mediante Azure PowerShell

Si necesita habilitar la red acelerada después de la creación de la máquina virtual, puede hacerlo mediante Azure PowerShell.

Nota:

Asegúrese de detener la máquina virtual antes de habilitar la red acelerada mediante Azure Pow-

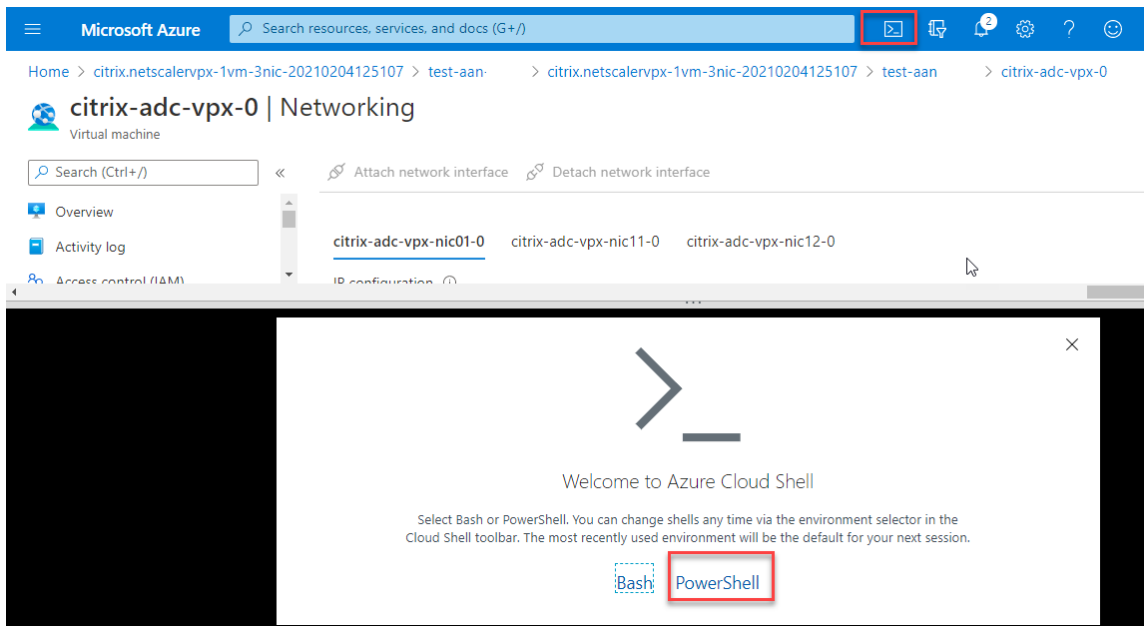
erShell.

Lleve a cabo los siguientes pasos para habilitar la red acelerada mediante Azure PowerShell.

1. Vaya al **portal de Azure** y haga clic en el icono de **PowerShell** en la esquina superior derecha.

Nota:

Si se encuentra en modo Bash, cambie al modo PowerShell.



2. En el símbolo del sistema, ejecute el siguiente comando:

```
1 az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
```

El parámetro de red acelerada acepta uno de los siguientes valores:

- **True:** habilita la red acelerada en la NIC especificada.
- **False:** inhabilita la red acelerada en la NIC especificada.

Para habilitar redes aceleradas en una NIC específica:

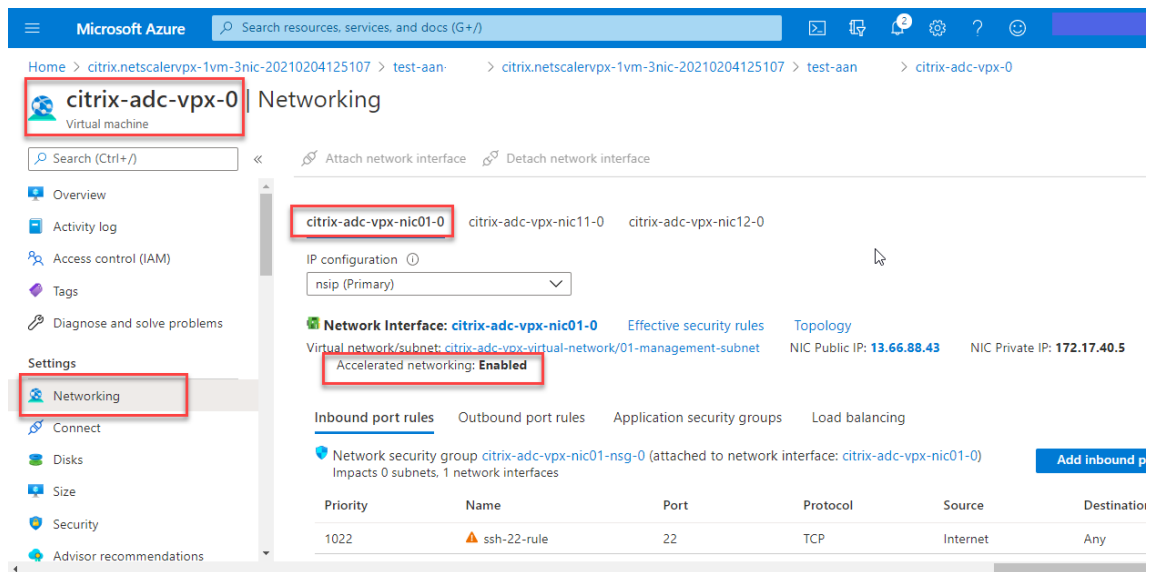
```
1 az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
```

Para inhabilitar la red acelerada en una NIC específica:

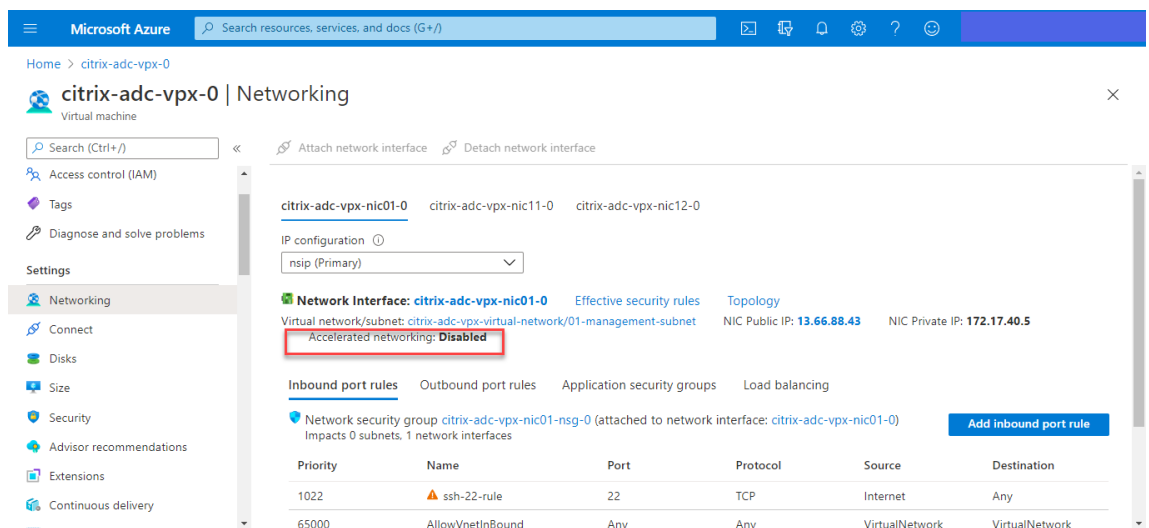
```
1 az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
```

3. Para comprobar el estado de las redes aceleradas una vez finalizada la implementación, vaya a **VM > Redes**.

En el siguiente ejemplo, puede ver que la red acelerada está **habilitada**.



En el siguiente ejemplo, puede ver que la red acelerada está **inhabilitada**.



Para verificar las redes aceleradas en una interfaz mediante FreeBSD Shell de NetScaler

Puede iniciar sesión en el shell de FreeBSD de NetScaler y ejecutar los siguientes comandos para comprobar el estado de la red acelerada.

Ejemplo de NIC ConnectX3:

En el ejemplo siguiente se muestra el resultado del comando “ifconfig” de la NIC Mellanox ConnectX3. El “50/n” indica las interfaces VF de las NIC Mellanox ConnectX3. 0/1 y 1/1 indican las interfaces fotovoltaicas de la instancia VPX de NetScaler VPX. Puede observar que tanto la interfaz fotovoltaica (1/1)

como la interfaz VF CX3 (50/1) tienen las mismas direcciones MAC (00:22:48:1c:99:3e). Esto indica que las dos interfaces están agrupadas juntas.

```
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
```

Ejemplo de NIC ConnectX4:

En el ejemplo siguiente se muestra el resultado del comando “ifconfig” de la NIC Mellanox ConnectX4. El “100/n” indica las interfaces VF de las NIC Mellanox ConnectX4. 0/1, 1/1 y 1/2 indican las interfaces PV de la instancia NetScaler VPX. Puede observar que tanto la interfaz fotovoltaica (1/1) como la interfaz CX4 VF (100/1) tienen las mismas direcciones MAC (00:0 d:3a:9b:f 2:1 d). Esto indica que las dos

interfaces están agrupadas juntas. Del mismo modo, la interfaz fotovoltaica (1/2) y la interfaz CX4 VF (100/2) tienen las mismas direcciones MAC (00:0d:3a:1e:d2:23).

```

root@SmartNIC-CX4-NS-DUT-NEW1# 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>
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
ether 00:0d:3a:9b:f2:1d
inet 10.0.1.29 netmask 0xfffff00 broadcast 10.0.1.255
inet6 fe80::20d:3aff:fe9b:f21d%0/1 prefixlen 64 autoconf scopeid 0x2
nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
media: Ethernet autoselect (10Gbase-T <full-duplex>)
status: active

1/2: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
ether 00:0d:3a:1e:d2:23
media: Ethernet autoselect (10Gbase-T <full-duplex>)
status: active

100/1: flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0d:3a:9b:f2:1d
media: Ethernet autoselect <full-duplex rxpause txpause> (autoselect
<full-duplex rxpause>)
status: active

100/2: flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0d:3a:1e:d2:23
media: Ethernet autoselect <full-duplex rxpause txpause> (autoselect
<full-duplex rxpause>)
status: active

```

Para verificar redes aceleradas en una interfaz mediante la CLI de ADC

Ejemplo de NIC ConnectX3:

El siguiente resultado del comando show interface indica que la interfaz PV 1/1 está incluida con la función virtual 50/1, que es una NIC VF SR-IOV. Las direcciones MAC de las NIC 1/1 y 50/1 son las mismas. Una vez habilitada la red acelerada, los datos de la interfaz 1/1 se envían a través de la ruta de datos de la interfaz 50/1, que es una interfaz ConnectX3. Puede ver que la salida “mostrar interfaz” de la interfaz fotovoltaica (1/1) apunta al VF (50/1). Del mismo modo, la salida “show interface” de la interfaz VF (50/1) apunta a la interfaz fotovoltaica (1/1).

```
> show interface 1/1

Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) #1
Flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
LLDP Mode: NONE, LR Priority: 1024

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) FcTls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.

Done

> show interface 50/1

Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
Flags=0xe400 <ENABLED, UP, UP, 802.1q>
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

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) FcTls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
```

Ejemplo de NIC ConnectX4:

El siguiente resultado del comando show interface indica que la interfaz PV 1/1 está incluida con la función virtual 100/1, que es una NIC VF SR-IOV. Las direcciones MAC de las NIC 1/1 y 100/1 son las mismas. Una vez habilitada la red acelerada, los datos de la interfaz 1/1 se envían a través de la ruta de datos de la interfaz 100/1, que es una interfaz ConnectX4. Puede ver que la salida “show interface” de la interfaz fotovoltaica (1/1) apunta al VF (100/1). Del mismo modo, la salida “show interface” de la interfaz VF (100/1) apunta a la interfaz fotovoltaica (1/1).


```

> show interface 1/1
1) Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 100/1, Datapath 100/1) #0
   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
1) Interface 100/1 (CX4 VF Interface, SmartNIC, PV 1/1) #3
   flags=0xe460 <ENABLED, UP, UP, 802.1q>
   MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d, uptime 10h49m11s
   Actual: media FIBER, speed NONE, duplex FULL, fct1 NONE, throughput
0
   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
>

```

Puntos a tener en cuenta en NetScaler

- La interfaz fotovoltáica se considera la interfaz principal o principal para todas las operaciones necesarias. Las configuraciones deben realizarse únicamente en interfaces fotovoltáicas.
- Todas las operaciones de “set” en una interfaz VF están bloqueadas excepto las siguientes:
 - habilitar interfaz
 - inhabilitar interfaz
 - interfaz de reinicio
 - estadísticas claras

Nota:

Citrix recomienda que no realice ninguna operación en la interfaz VF.

- Puede verificar la vinculación de la interfaz fotovoltáica con la interfaz VF mediante el comando `show interface`.
- A partir de la versión 13.1-33.x de NetScaler, una instancia de NetScaler VPX puede gestionar sin problemas las eliminaciones dinámicas de NIC y la reconexión de las NIC eliminadas en las redes aceleradas de Azure. Azure puede eliminar la NIC VF SR-IOV de las redes aceleradas para sus actividades de mantenimiento del host. Cada vez que se elimina una NIC de Azure VM, la

instancia de NetScaler VPX muestra el estado de la interfaz como “Enlace inactivo” y el tráfico pasa únicamente por la interfaz virtual. Una vez que se vuelve a conectar la NIC eliminada, las instancias VPX utilizan la NIC VF SR-IOV que se ha vuelto a conectar. Este proceso se lleva a cabo sin problemas y no requiere ninguna configuración.

Configurar una VLAN en una interfaz fotovoltaica

Cuando una interfaz fotovoltaica está enlazada a una VLAN, la interfaz VF acelerada asociada también se enlaza a la misma VLAN que la interfaz fotovoltaica. En este ejemplo, la interfaz fotovoltaica (1/1) está enlazada a VLAN (20). La interfaz VF (100/1) que se incluye con la interfaz fotovoltaica (1/1) también está enlazada a la VLAN 20.

Ejemplo

1. Cree una VLAN.

```
1 add vlan 20
```

2. Enlace una VLAN a la interfaz fotovoltaica.

```
1 bind vlan 20 -ifnum 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 : L0/1
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
13 3) VLAN ID: 20    VLAN Alias Name:
14   Interfaces : 1/1 100/2
```

Nota:

La operación de enlace de VLAN no está permitida en una interfaz VF acelerada.

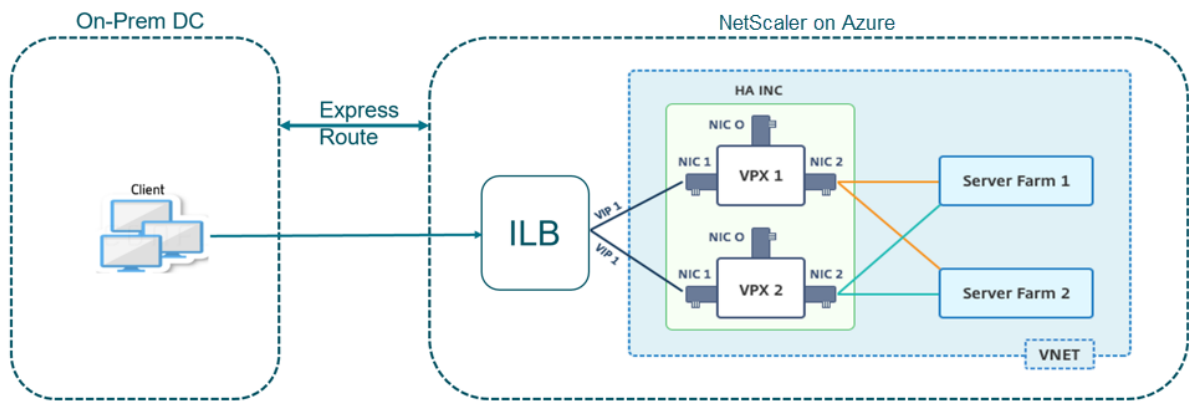
```
1 bind vlan 1 -ifnum 100/1
2 ERROR: Operation not permitted
```

Configure los nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler con Azure ILB

October 17, 2024

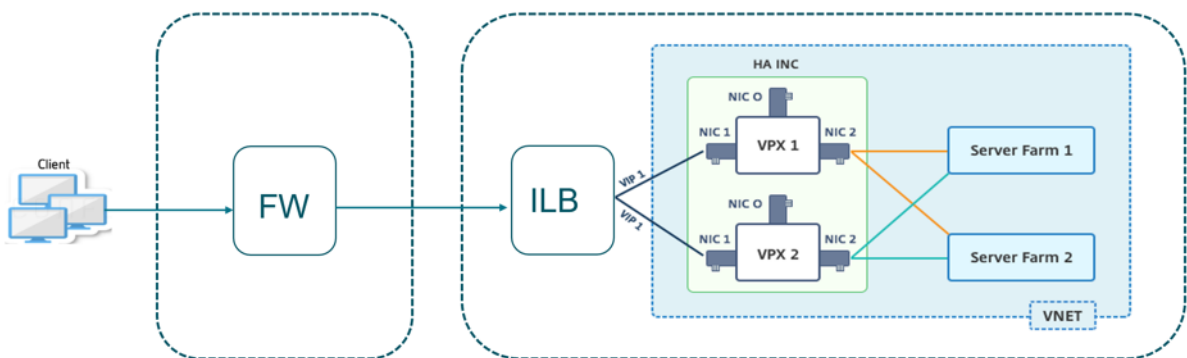
Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar para aplicaciones de intranet. El equilibrador de carga interna (ILB) de Azure utiliza una dirección IP interna o privada para el front-end, como se muestra en la Ilustración 1. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para el tráfico de administración, del cliente y del lado del servidor, y cada subred pertenece a una NIC diferente en cada dispositivo.

Ilustración 1: Par de NetScaler HA para clientes de una red interna



También puede utilizar esta implementación cuando el par de NetScaler HA está detrás de un firewall, como se muestra en la Ilustración 2. La dirección IP pública pertenece al firewall y es NAT a la dirección IP del front-end del ILB.

Ilustración 2: NetScaler HA emparejar con firewall con dirección IP pública



Puede obtener la plantilla de par de alta disponibilidad de NetScaler para aplicaciones de intranet en el [portal de Azure](#)

Complete los pasos siguientes para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante los conjuntos de disponibilidad de Azure.

1. En el portal de Azure, vaya a la página **Implementación personalizada**.
2. Aparecerá la página **Básicos**. Cree un grupo de recursos. En la ficha **Parámetros**, introduzca los detalles de la región, el nombre de usuario de administrador, la contraseña de administrador, el tipo de licencia (VM sku) y otros campos.

Custom deployment
Deploy from a custom template
12 resources

[Edit template](#) [Edit parameters](#)

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Parameters

Region * ⓘ

Admin Username ⓘ

Admin Password * ⓘ

Vm Size ⓘ

Vm Sku ⓘ

Vnet Name ⓘ

Vnet Resource Group ⓘ

Vnet New Or Existing

Subnet Name-01 ⓘ

Subnet Name-11 ⓘ

Subnet Name-12 ⓘ

Subnet Address Prefix-01 ⓘ

Subnet Address Prefix-11 ⓘ

[Review + create](#) [< Previous](#) [Next : Review + create >](#)

3. Haga clic en **Siguiente: Revisar y crear >**.

Es posible que el Azure Resource Group demore un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el grupo de recursos en el portal de Azure para ver los detalles de configuración, como reglas de LB, grupos de back-end, sondeos de estado. El par de alta disponibilidad aparece como ADC-VPX-0 y ADC-VPX-1.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Una vez completada la configuración requerida, se crean los siguientes recursos.

The screenshot shows the Azure portal interface for the 'HA-ILB' Resource group. At the top, there are navigation options like 'Add', 'Edit columns', 'Delete resource group', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. Below this, the 'Essentials' section displays subscription information: 'Subscription (change) : NSDev Platform (8.amaoquaj@msn.com)', 'Subscription ID : 704bc0a9-7827-4311-8a67-ed873990caa3', and 'Tags (change) : Click here to add tags'. A filter bar shows 'Type == (all)' and 'Location == (all)'. The main area displays a table of 20 resources, all located in 'West US 2'. The resources include an Availability set, a Load balancer, two Virtual machines (ADC-VPX-0 and ADC-VPX-1), two Public IP addresses, twelve Network interfaces, and six Network security groups.

Name	Type	Location
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. Inicie sesión en los nodos **ADC-VPX-0** y **ADC-VPX-1** para validar la siguiente configuración:

- Las direcciones NSIP de ambos nodos deben estar en la subred de administración.
- En los nodos principal (ADC-VPX-0) y secundario (ADC-VPX-1), debe ver dos direcciones SNIP. Un SNIP (subred cliente) se usa para responder a las sondas de ILB y el otro SNIP (subred del servidor) se usa para la comunicación del servidor back-end.

Nota:

En el modo HA-INC, la dirección de SNIP de las máquinas virtuales ADC-VPX-0 y ADC-VPX-1 son diferentes mientras se encuentran en la misma subred, a diferencia de la implementación clásica de ADC de alta disponibilidad local donde ambas son iguales. Para admitir implementaciones cuando el SNIP del par VPX se encuentra en subredes diferentes o cuando el VIP no esté en la misma subred que un SNIP, debe habilitar el reenvío basado en Mac (MBF) o agregar una ruta de host estática para cada VIP a cada nodo VPX.

En el nodo principal (ADC-VPX-0)

```
> sh ip
-----
1) 10.11.0.5      0      NetScaler IP  Active  Enabled  Enabled  NA      Enabled
2) 10.11.1.5      0      SNIP         Active  Enabled  Enabled  NA      Enabled
3) 10.11.3.4      0      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 msec
   Dead Interval: 3 sec
   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
> █

```

En el nodo secundario (ADC-VPX-1)

```

> sh ip

```

	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
	-----	-----	----	----	---	----	-----	-----
1)	10.11.0.4	0	NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.11.1.6	0	SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.5	0	SNIP	Active	Enabled	Enabled	NA	Enabled

```

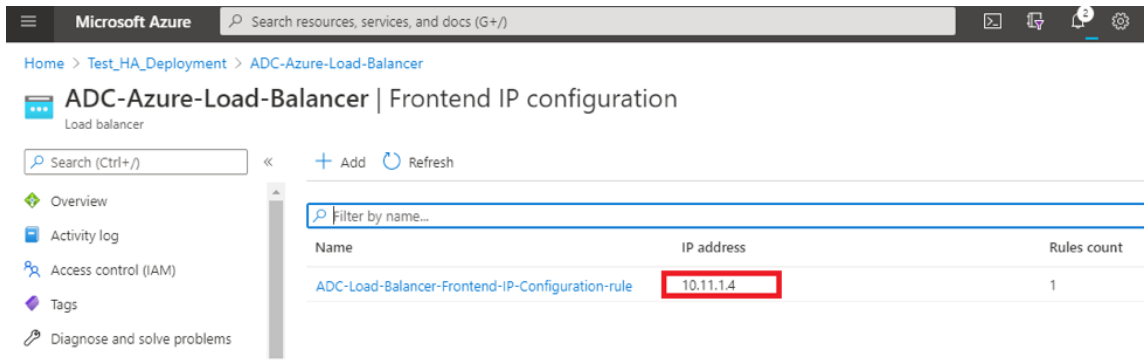
Done
> █

```

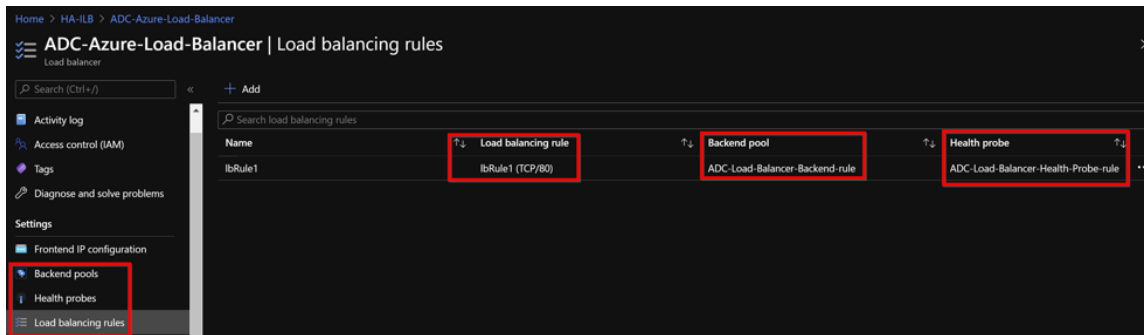
```
> sh ha node
1) Node ID: 0
   IP: 10.11.0.4 (ADC-VPX-1)
   Node State: UP
   Master State: Secondary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: SUCCESS
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
   Sync Status Strict Mode: DISABLED
   Hello Interval: 200 msec
   Dead Interval: 3 secs
   Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2) Node ID: 1
   IP: 10.11.0.5
   Node State: UP
   Master State: Primary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: ENABLED
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT

Done
> █
```

5. Después de que los nodos principal y secundario estén **ACTIVADOS** y el estado de sincronización sea **SUCCESS**, debe configurar el servidor virtual de equilibrio de carga o el servidor virtual de puerta de enlace en el nodo principal (ADC-VPX-0) con la dirección IP flotante privada (FIP) del equilibrador de carga ADC Azure. Para obtener más información, consulte la sección [Configuración de ejemplo](#).
6. Para buscar la dirección IP privada del equilibrador de carga de ADC Azure, vaya a **Azure Portal > Equilibrador de carga de Azure ADC > Configuración de IP de frontend**.



7. En la página de configuración de **Azure Load Balancer**, la implementación de la plantilla ARM ayuda a crear la regla de LB, grupos de back-end y sondeos de estado.



- La regla LB (LbRule1) usa el puerto 80, de forma predeterminada.

lbRule1
ADC-Azure-Load-Balancer

Save Discard Delete

i 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 IPv6

Frontend IP address * ⓘ
10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule) ✓

Protocol
 TCP UDP

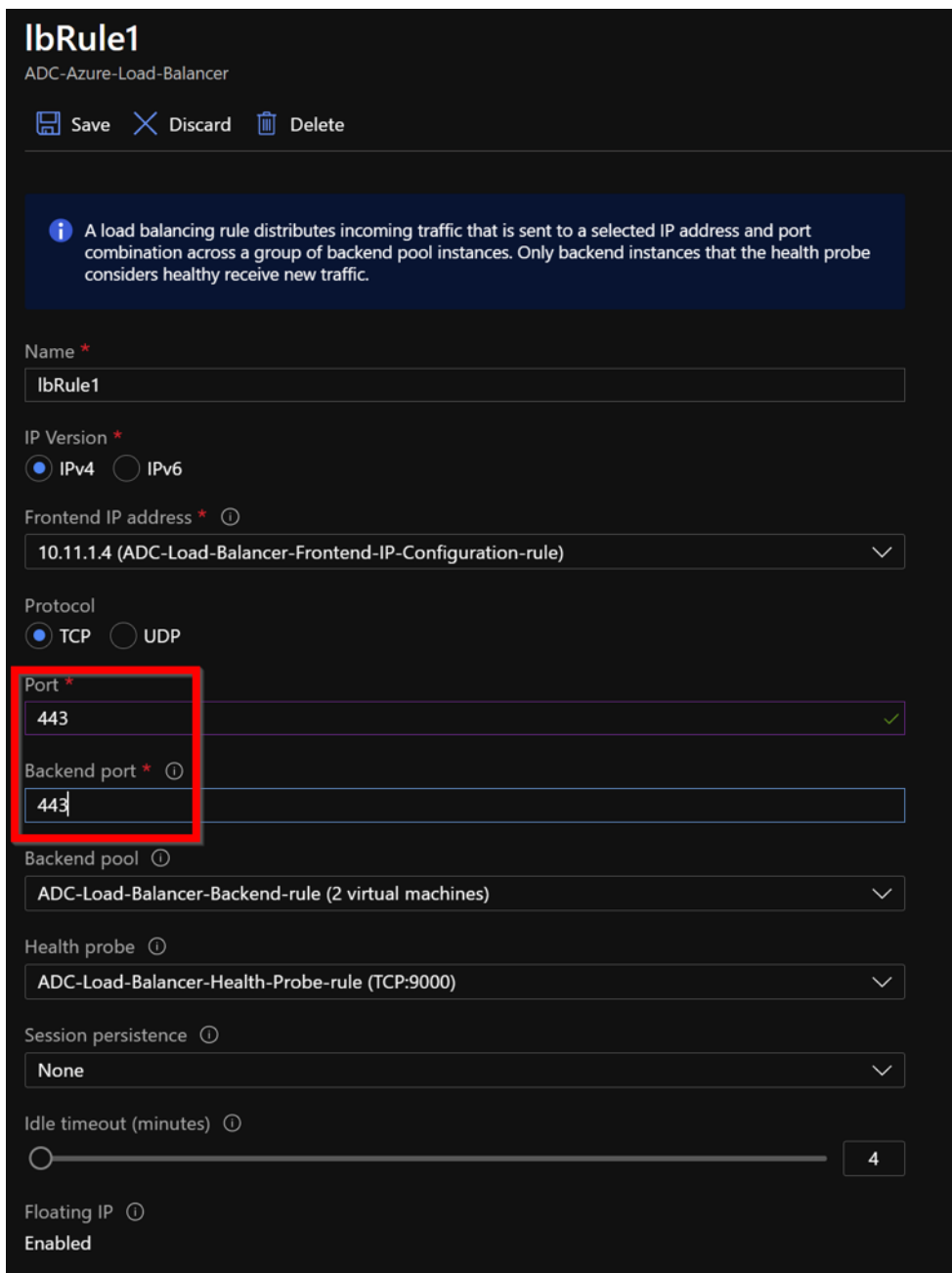
Port *
80

Backend port * ⓘ
80

- Modifique la regla para usar el puerto 443 y guarde los cambios.

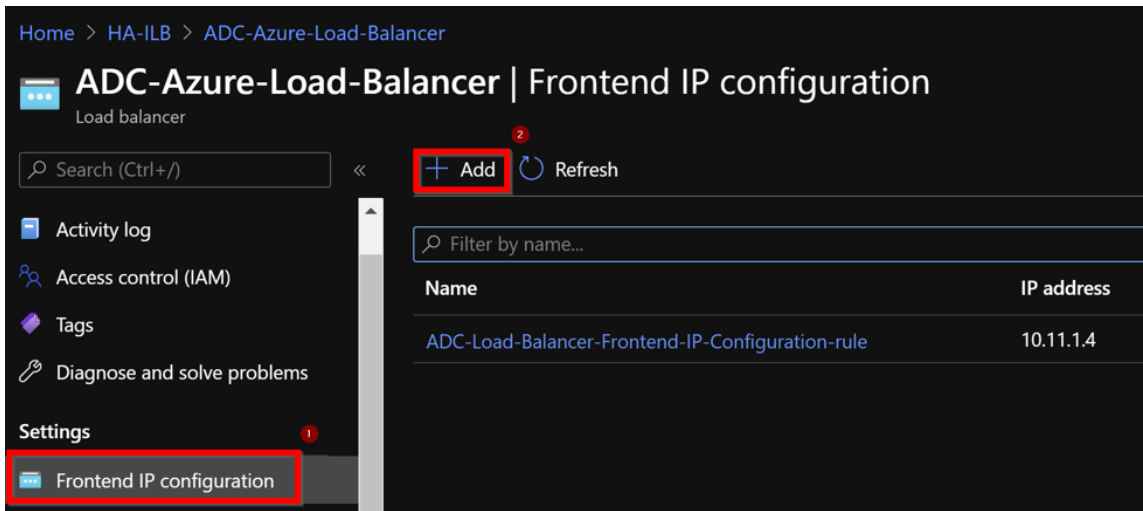
Nota:

Para mejorar la seguridad, Citrix recomienda utilizar el puerto SSL 443 para el servidor virtual LB o el servidor virtual Gateway.

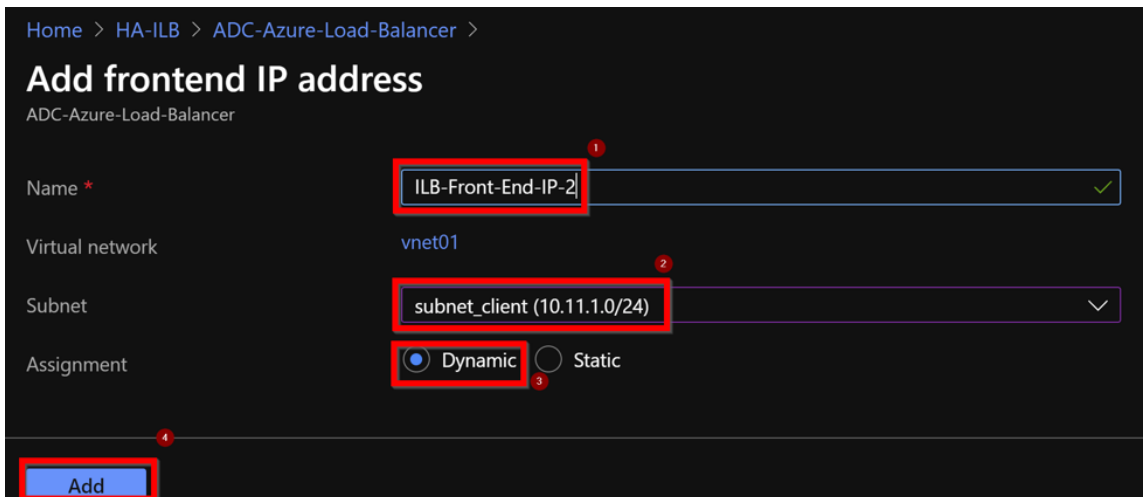


Para agregar más direcciones VIP en el ADC, lleve a cabo los siguientes pasos:

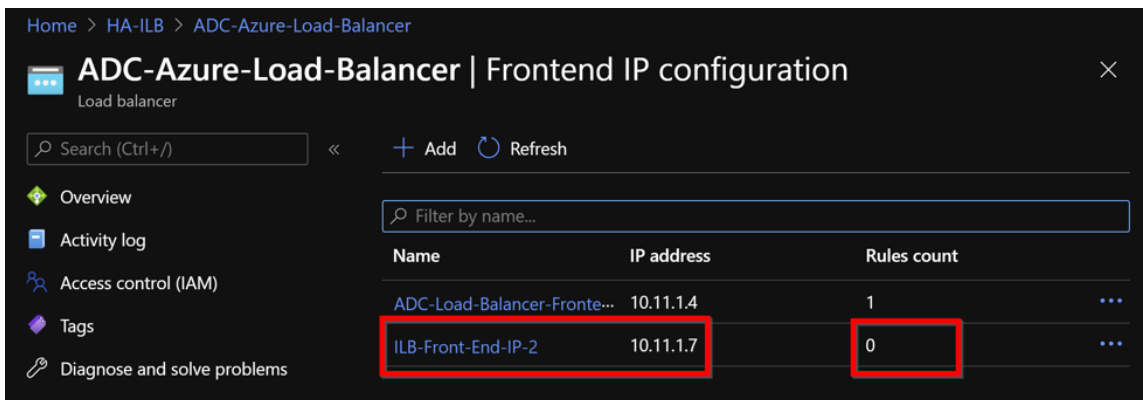
1. Vaya a **Azure Load Balancer > Configuración de IP de frontend** y haga clic en **Agregar** para crear una nueva dirección IP del equilibrador de carga interno.



2. En la página **Agregar dirección IP frontend**, introduce un nombre, elige la subred del cliente, asigna una dirección IP dinámica o estática y haga clic en **Agregar**.

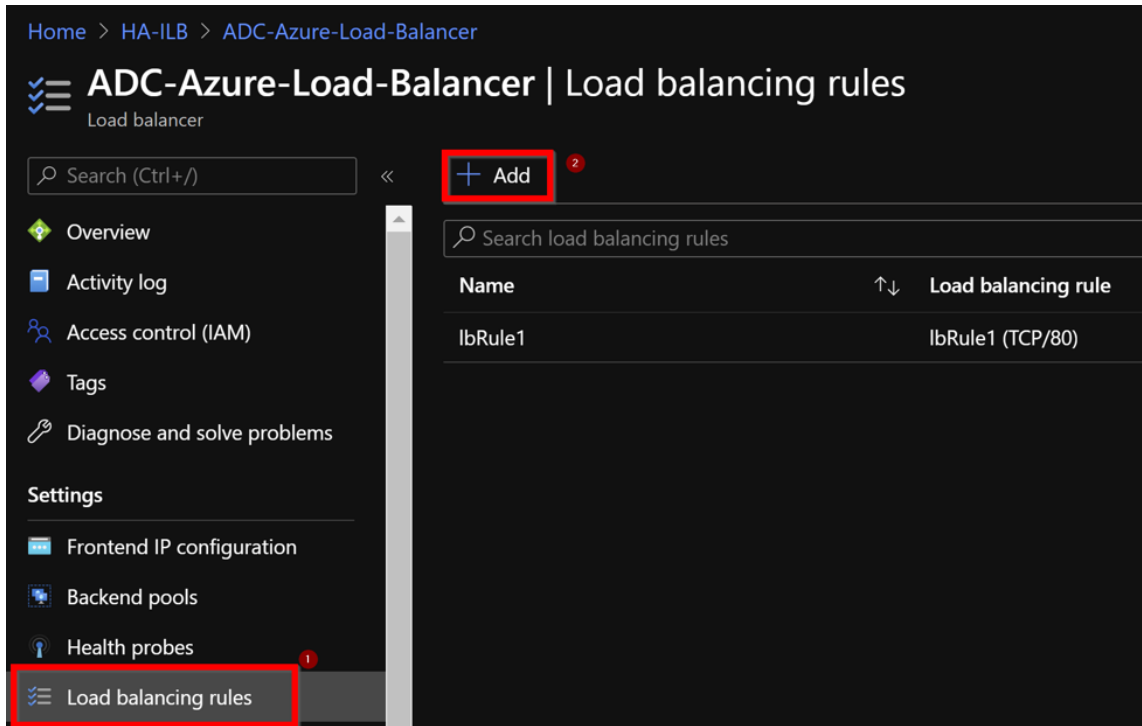


3. La dirección IP de front-end se crea pero no se asocia una regla de LB. Crea una nueva regla de equilibrio de carga y asocia a la dirección IP del front-end.

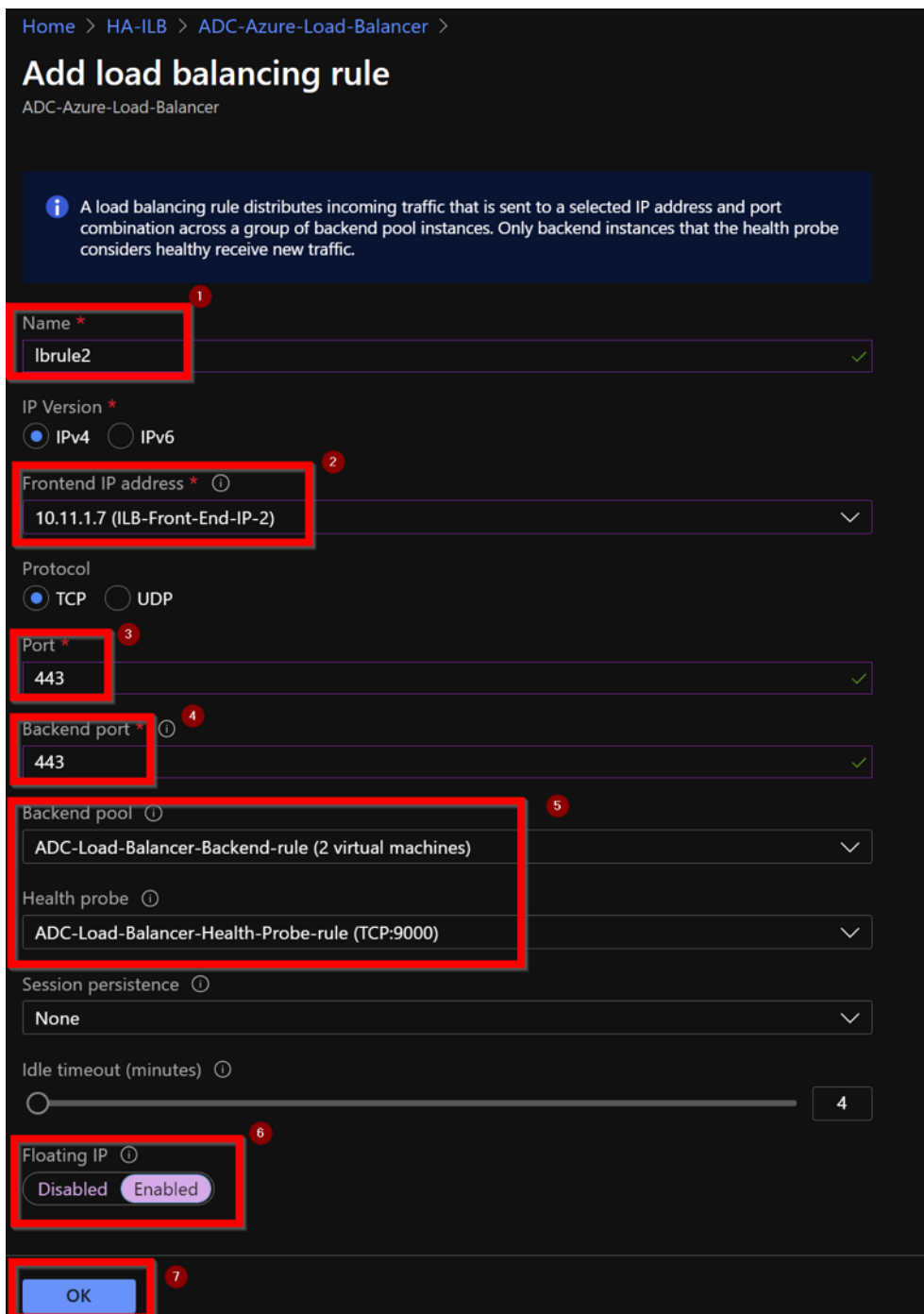


4. En la página **Azure Load Balancer**, seleccione **Reglas de equilibrio de carga** y, a continuación,

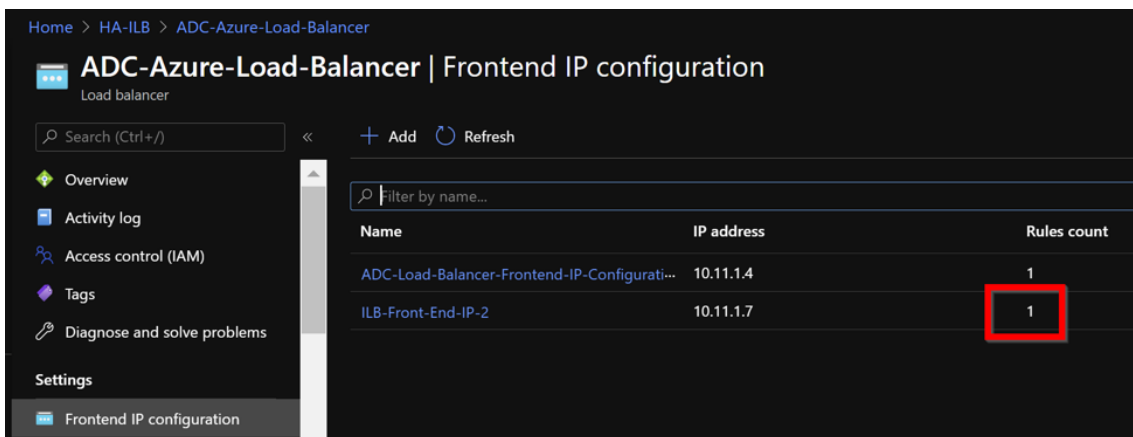
haga clic en **Agregar**.



5. Cree una nueva regla de LB eligiendo la nueva dirección IP de front-end y el puerto. El campo **IP flotante** debe establecerse en **Habilitado**.



6. Ahora la **configuración de IP frontend** muestra la regla LB que se aplica.



Configuración de ejemplo

Para configurar un servidor virtual VPN de puerta de enlace y un servidor virtual de equilibrio de carga, ejecute los siguientes comandos en el nodo principal (ADC-VPX-0). La configuración se sincroniza automáticamente con el nodo secundario (ADC-VPX-1).

Configuración de ejemplo de puerta de enlace

```

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
    
```

Configuración de muestra de equilibrio de carga

```

1 enable feature LB SSL
2 enable ns mode MBF
3 add lb vserver lb_vs1 SSL 10.11.1.7 443
4 bind ssl vserver lb_vs1 -certkeyName ckp
    
```

Ahora puede acceder al servidor virtual de equilibrio de carga o VPN mediante el nombre de dominio completo (FQDN) asociado a la dirección IP interna del ILB.

Consulte la sección **Recursos** para obtener más información sobre cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes enlaces proporcionan información adicional relacionada con la implementación de alta disponibilidad y la configuración del servidor virtual:

- [Configuración de nodos de alta disponibilidad en diferentes subredes](#)
- [Configurar el equilibrio de carga básico](#)

Recursos relacionados:

- [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell](#)
- [Configuración de GSLB en la implementación de HA activa en espera en Azure](#)

Configure los nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler para aplicaciones con conexión a Internet

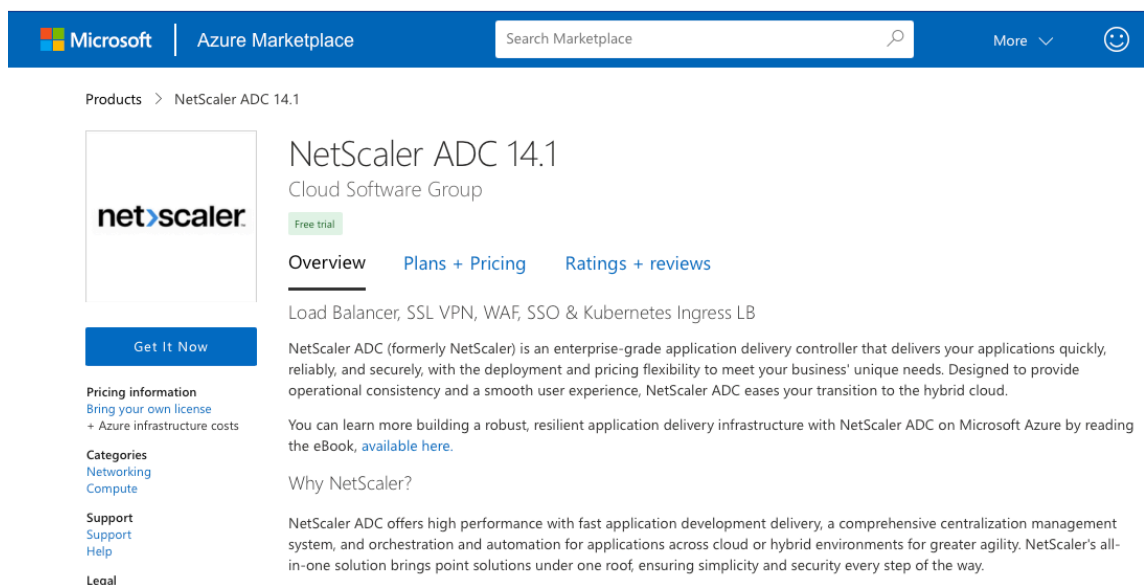
October 17, 2024

Puede implementar de forma rápida y eficiente un par de instancias VPX en modo HA-INC mediante la plantilla estándar para aplicaciones conectadas a Internet. El balanceador de carga de Azure (ALB) usa una dirección IP pública para la interfaz. La plantilla crea dos nodos, con tres subredes y seis NIC. Las subredes son para el tráfico del lado de la administración, del cliente y del servidor. Cada subred tiene dos NIC para ambas instancias VPX.

Puede obtener la plantilla de par NetScaler HA para aplicaciones orientadas a Internet en [Azure Marketplace](#).

Complete los pasos siguientes para iniciar la plantilla e implementar un par VPX de alta disponibilidad mediante conjuntos de disponibilidad de Azure o zona de disponibilidad.

1. En Azure Marketplace, busque **NetScaler**.
2. Haga clic en **OBTENER AHORA**.



Products > NetScaler ADC 14.1

Microsoft | Azure Marketplace Search Marketplace More

NetScaler ADC 14.1

Cloud Software Group

Free trial

Overview Plans + Pricing Ratings + reviews

Load Balancer, SSL VPN, WAF, SSO & Kubernetes Ingress LB

NetScaler ADC (formerly NetScaler) 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 ADC eases your transition to the hybrid cloud.

You can learn more building a robust, resilient application delivery infrastructure with NetScaler ADC on Microsoft Azure by reading the eBook, [available here](#).

Why NetScaler?

NetScaler ADC offers high performance with fast application development delivery, a comprehensive centralization management system, and orchestration and automation for applications across cloud or hybrid environments for greater agility. NetScaler's all-in-one solution brings point solutions under one roof, ensuring simplicity and security every step of the way.

Get It Now

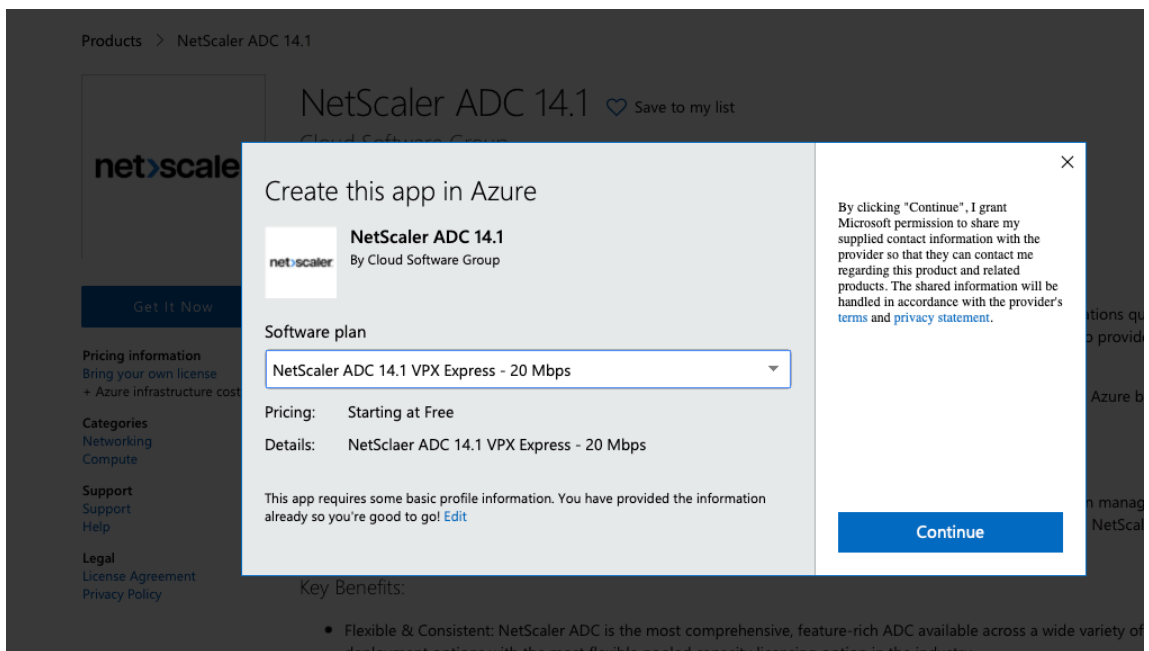
Pricing information
Bring your own license
+ Azure infrastructure costs

Categories
Networking
Compute

Support
Support
Help

Legal

3. Seleccione la implementación de alta disponibilidad requerida junto con la licencia y haga clic en **Continuar**.



4. Aparecerá la página **Básicos**. Cree un grupo de recursos. En la ficha **Parámetros**, introduce los detalles de la región, el nombre de usuario del administrador, la contraseña de administrador, el tipo de licencia (SKU de máquina virtual) y otros campos.

[Basics](#) [VM Configurations](#) [Network and Additional Settings](#) [Review + create](#)

Project details

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Region * ⓘ

Citrix ADC Release Version * ⓘ 12.1 13.0

License Subscription ⓘ Bring Your Own License

Virtual Machine name * ⓘ

Administrator account

Username * ⓘ ✓

Authentication type * ⓘ Password SSH Public Key

Password * ⓘ ✓

Confirm password * ✓ ✓ Password

[Review + create](#) [< Previous](#) [Next : VM Configurations >](#)

5. Haga clic en **Siguiente: Configuraciones de VM.**

Basics VM Configurations Network and Additional Settings Review + create

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

Subscription * ⓘ xm-test-cs-shared ✓
Resource group * ⓘ (New) Test_HA_Internet ✓
[Create new](#)

Instance details

Region * ⓘ South India ✓

Citrix ADC Release Version * ⓘ
 12.1
 13.0

License Subscription ⓘ
 Bring Your Own License

Virtual Machine name * ⓘ citrix-adc-vmx

Administrator account

Username * ⓘ praveenk ✓

Authentication type * ⓘ
 Password
 SSH Public Key

Password * ⓘ ✓

Confirm password * ✓ ✓ Password

[Review + create](#) [< Previous](#) [Next : VM Configurations >](#)

6. En la página **Configuraciones de VM**, realice lo siguiente:

- Configurar el sufijo de nombre de dominio IP público
- Habilitar o inhabilitar las **métricas de monitoreo de Azure**
- Habilitar o inhabilitar **Backend Autoscale**

7. Haga clic en **Siguiente: Configuración de red y adicionales**

Virtual machine size * ⓘ	1x Standard DS3 v2 4 vcpus, 14 GB memory Change size
OS disk type ⓘ	<input checked="" type="radio"/> Premium_LRS
Assign Public IP (Management) ⓘ	<input checked="" type="radio"/> Yes
Assign Public IP (Client traffic) ⓘ	<input checked="" type="radio"/> Yes
Unique public IP domain name suffix * ⓘ	<input type="text" value="d7a2c4d49e"/>
Azure Monitoring Metrics ⓘ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Backend Autoscale ⓘ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

[Review + create](#) [< Previous](#) [Next : Network and Additional Settings >](#)

8. En la página **Configuración de red y adicionales**, cree una cuenta de diagnóstico de arranque y configure los ajustes de red.

Basics VM Configurations **Network and Additional Settings** Review + create

Boot diagnostics

Diagnostics storage account * ⓘ (new) citrixadcvpdx7a2c4d49e [Create New](#)

Network Settings

Configure virtual networks

Virtual network * ⓘ (new) citrix-adc-vpx-virtual-network [Create new](#)

Management Subnet * ⓘ (new) 01-management-subnet (10.17.4.0/24)

Client Subnet * ⓘ (new) 11-client-subnet (10.17.5.0/24)

Server Subnet * ⓘ (new) 12-server-subnet (10.17.6.0/24)

Public IP (Management)

Management Public IP (NSIP) * ⓘ (new) citrix-adc-vpx-nsip [Create new](#)

Management Domain Name ⓘ citrix-adc-vpx-nsip-d7a2c4d49e [.southindia.cloudapp.azure.com](#)

Public IP (Clientside)

Clientside Public IP (VIP) * ⓘ (new) citrix-adc-vpx-vip [Create new](#)

Clientside Domain Name ⓘ citrix-adc-vpx-vip-d7a2c4d49e [.southindia.cloudapp.azure.com](#)

Public Inbound Ports (Management only)

Ports open for Management public IP ⓘ None ssh (22) ssh (22), http (80), https (443)

[Review + create](#) [< Previous](#) [Next : Review + create >](#)

9. Haga clic en **Siguiente: Revisar + crear**.

10. Revise la configuración básica, la configuración de la máquina virtual, la red y la configuración adicional, y haga clic en **Crear**.


Es posible que el Azure Resource Group demore un momento en crearse con las configuraciones requeridas. Una vez finalizado, seleccione el grupo de recursos en el portal de Azure para ver los detalles de la configuración, como las reglas de LB, los grupos de back-end y los sondeos de

estado. El par de alta disponibilidad aparece como **citrix-adc-vpx-0** y **citrix-adc-vpx-1**.

Si se requieren más modificaciones para la configuración de HA, como la creación de más reglas de seguridad y puertos, puede hacerlo desde el portal de Azure.

Una vez completada la configuración requerida, se crean los siguientes recursos.

Home > citrix.netscalervpx-1vm-3nic-20201006140352 >
























Test_HA_Internet_App 
Resource group

» [+ Add](#) [Edit columns](#) [Delete resource group](#) [Refresh](#) [Export to CSV](#) [Open query](#) | [Assign tags](#) → [Move](#) [D](#)

Essentials

Filter by name... [Type == all](#) [Location == all](#) [+ Add filter](#)

Showing 1 to 23 of 23 records. Show hidden types

<input type="checkbox"/> Name ↑↓	Type ↑↓
<input type="checkbox"/>  citrix-adc-vpx-0	Virtual machine
<input type="checkbox"/>  citrix-adc-vpx-0_OsDisk_1_6749f4a73c534051b0602ba6e3ec2cf8	Disk
<input type="checkbox"/>  citrix-adc-vpx-1	Virtual machine
<input type="checkbox"/>  citrix-adc-vpx-1_OsDisk_1_8fde7770497b4dbdba385715e81505c9	Disk
<input type="checkbox"/>  citrix-adc-vpx-nic01-0	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic01-1	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic01-nsg-0	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nic01-nsg-1	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nic11-0	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic11-1	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic11-nsg-0	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nic11-nsg-1	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nic12-0	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic12-1	Network interface
<input type="checkbox"/>  citrix-adc-vpx-nic12-nsg-0	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nic12-nsg-1	Network security group
<input type="checkbox"/>  citrix-adc-vpx-nsip-0	Public IP address
<input type="checkbox"/>  citrix-adc-vpx-nsip-1	Public IP address
<input type="checkbox"/>  citrix-adc-vpx-vip	Public IP address
<input type="checkbox"/>  citrix-adc-vpx-vip-load-balancer	Load balancer
<input type="checkbox"/>  citrix-adc-vpx-virtual-network	Virtual network
<input type="checkbox"/>  citrix-adc-vpx-vm-availability-set	Availability set
<input type="checkbox"/>  citrixadcpx9db3901a6a	Storage account

11. Debe iniciar sesión en los nodos **citrix-adc-vpx-0** y **citrix-adc-vpx-1** para validar la siguiente configuración:

- Las direcciones NSIP de ambos nodos deben estar en la subred de administración.
- En los nodos primario (citrix-adc-vpx-0) y secundario (citrix-adc-vpx-1), debe ver dos direcciones SNIP. Un SNIP (subred del cliente) se usa para responder a las sondas ALB y el otro SNIP (subred del servidor) se usa para la comunicación con el servidor de fondo.

Nota:

En el modo HA-INC, las direcciones SNIP de las máquinas virtuales citrix-adc-vpx-0 y citrix-adc-vpx-1 son diferentes, a diferencia de la implementación clásica de alta disponibilidad de ADC local, donde ambas son iguales.

En el nodo principal (citrix-adc-vpx-0)

```
> sh ip
-----
1) 10.18.0.4 0 NetScaler IP Active Enabled Enabled NA Enabled
2) 10.18.1.5 0 SNIP Active Enabled Enabled NA Enabled
3) 10.18.2.4 0 SNIP Active Enabled Enabled NA Enabled
Done
```

```
> sh ha node
1) Node ID: 0
   IP: 10.18.0.4 (ns-vpx0)
   Node State: UP
   Master State: Primary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: ENABLED
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
   Sync Status Strict Mode: DISABLED
   Hello Interval: 200 msec
   Dead Interval: 3 secs
   Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2) Node ID: 1
   IP: 10.18.0.5
   Node State: UP
   Master State: Secondary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: SUCCESS
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
Done
```

En el nodo secundario (citrix-adc-vpx-1)

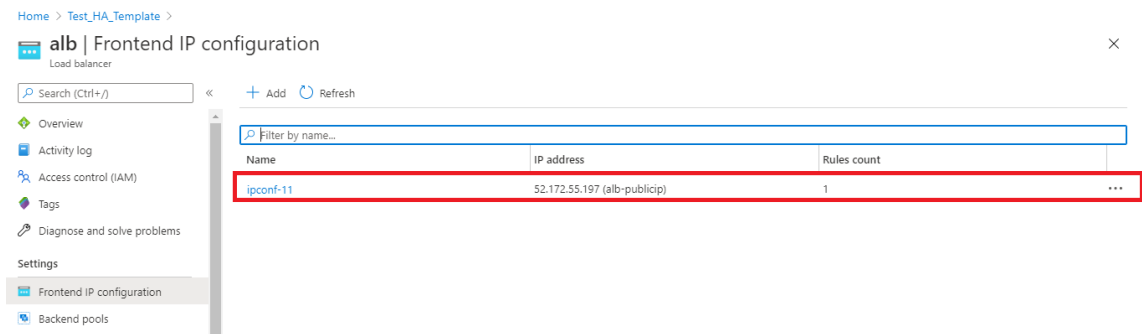
```
> show ip
-----
1) 10.18.0.5 0 NetScaler IP Active Enabled Enabled NA Enabled
2) 10.18.1.4 0 SNIP Active Enabled Enabled NA Enabled
3) 10.18.2.5 0 SNIP Active Enabled Enabled NA Enabled
Done
>
```

```

> sh ha node
1) Node ID: 0
   IP: 10.18.0.5 (ns-vpx1)
   Node State: UP
   Master State: Secondary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: SUCCESS
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
   Sync Status Strict Mode: DISABLED
   Hello Interval: 200 msec
   Dead Interval: 3 secs
   Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2) Node ID: 1
   IP: 10.18.0.4
   Node State: UP
   Master State: Primary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: ENABLED
   Propagation: ENABLED
   Enabled Interfaces : 0/1 1/1 1/2
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : 1/1 1/2
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
Done
>

```

12. Después de que los nodos primario y secundario estén UP y el estado de sincronización es **SUCCESS**, debe configurar el servidor virtual de equilibrio de carga o el servidor virtual de puerta de enlace en el nodo principal (citrix-adc-vpx-0) con la dirección IP pública del servidor virtual ALB. Para obtener más información, consulte la sección [Configuración de ejemplo](#).
13. Para buscar la dirección IP pública del servidor virtual ALB, vaya a **Azure Portal > Azure Load Balancer > Configuración de IP de frontend**.



14. Agregue la regla de seguridad de entrada para el puerto 443 del servidor virtual en el grupo de seguridad de red de ambas interfaces de cliente.

NetScaler VPX 14.1

The image displays two screenshots of the Azure portal interface for configuring Network Security Groups (NSGs).

Top Screenshot: ns-vpx-nic-nsg0-11

- Resource group: Test_HA_Template
- Location: South India
- Subscription: xm-test-cs-shared
- Subscription ID: db99d808-6e89-480a-96ae-3275fe61eed4
- Tags: Click here to add tags
- Custom security rules: 2 inbound, 0 outbound
- Associated with: 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
1000	default-allow-ssh	22	TCP	Any	Any	Allow
1010	Port_443	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow

Bottom Screenshot: ns-vpx-nic-nsg1-11

- Resource group: Test_HA_Template
- Location: South India
- Subscription: xm-test-cs-shared
- Subscription ID: db99d808-6e89-480a-96ae-3275fe61eed4
- Tags: Click here to add tags
- Custom security rules: 2 inbound, 0 outbound
- Associated with: 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
1000	default-allow-ssh	22	TCP	Any	Any	Allow
1010	Port_443	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

15. Configure el puerto ALB al que desea acceder y cree una regla de seguridad de entrada para el puerto especificado. El puerto de fondo es el puerto del servidor virtual de equilibrio de carga o el puerto del servidor virtual VPN.

Microsoft Azure

Home > Test_HA_Template > alb >

lbRule1

alb

Save Discard Delete

Version

IPv4 IPv6

Frontend IP address * ⓘ

52.172.55.197 (ipconf-11)

Protocol

TCP UDP

Port *

443

Backend port * ⓘ

443

Backend pool ⓘ

bepool-11 (2 virtual machines)

Health probe ⓘ

probe-11 (TCP:9000)

Session persistence ⓘ

None

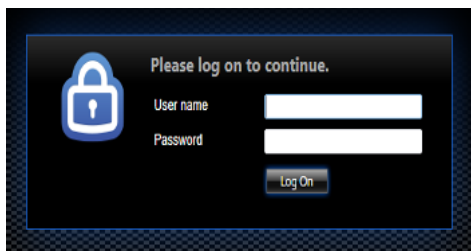
Idle timeout (minutes) ⓘ

4

Floating IP (direct server return) ⓘ

Enabled

16. Ahora, puede acceder al servidor virtual de equilibrio de carga o al servidor virtual VPN mediante el nombre de dominio completo (FQDN) asociado a la dirección IP pública de ALB.



Configuración de ejemplo

Para configurar un servidor virtual VPN de puerta de enlace y un servidor virtual de equilibrio de carga, ejecute los siguientes comandos en el nodo principal (ADC-VPX-0). La configuración se sincroniza automáticamente con el nodo secundario (ADC-VPX-1).

Configuración de ejemplo de puerta de enlace

```
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
```

Configuración de muestra de equilibrio de carga

```
1 enable feature LB SSL
2 enable ns mode MBF
3 add lb vserver lb_vs1 SSL 52.172.55.197 443
4 bind ssl vserver lb_vs1 -certkeyName ckp
```

Ahora puede acceder al servidor virtual VPN o de equilibrio de carga mediante el FQDN asociado a la dirección IP pública de ALB.

Consulte la sección **Recursos** para obtener más información sobre cómo configurar el servidor virtual de equilibrio de carga.

Recursos:

Los siguientes enlaces proporcionan información adicional relacionada con la implementación de alta disponibilidad y la configuración del servidor virtual:

- [Creación de servidores virtuales](#)
- [Configurar el equilibrio de carga básico](#)

Configurar una configuración de alta disponibilidad con balanceadores de carga externos e internos de Azure simultáneamente

October 17, 2024

El par de alta disponibilidad de Azure admite equilibradores de carga externos e internos simultáneamente.

Dispone de las dos opciones siguientes para configurar un par de alta disponibilidad mediante equilibradores de carga externos e internos de Azure:

- Uso de dos servidores virtuales LB en el dispositivo NetScaler.
- Uso de un servidor virtual LB y un conjunto de IP. El único servidor virtual LB envía tráfico a varias IP, definidas por IPset.

Lleve a cabo los siguientes pasos para configurar un par de alta disponibilidad en Azure mediante los equilibradores de carga externos e internos simultáneamente:

Para los pasos 1 y 2, utilice el portal de Azure. Para los pasos 3 y 4, utilice la GUI de NetScaler VPX o la CLI.

Paso 1. Configure un equilibrador de carga de Azure, ya sea un equilibrador de carga externo o un equilibrador de carga interno.

Para obtener más información sobre cómo configurar una configuración de alta disponibilidad con equilibradores de carga externos de Azure, consulte [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC](#).

Para obtener más información sobre cómo configurar la configuración de alta disponibilidad con equilibradores de carga internos de Azure, consulte [Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler con Azure ILB](#).

Paso 2. Cree un balanceador de carga adicional (ILB) en su grupo de recursos. En el paso 1, si ha creado un equilibrador de carga externo, ahora creará un equilibrador de carga interno y, por el contrario.

- Para crear un equilibrador de carga interno, elija el tipo de equilibrador de carga como **Interno**. Para el campo **Subred**, debe elegir la subred cliente NetScaler. Puede elegir proporcionar una dirección IP estática en esa subred, siempre que no haya conflictos. De lo contrario, elija la dirección IP dinámica.

[Home](#) > [ansible_rg_ganeshb_1611818039](#) > [New](#) > [Load Balancer](#) >

Create load balancer

Project details

Subscription *

Resource group *

[Create new](#)

Instance details

Name * ✓

Region * ▼

Type * ⓘ Internal Public

SKU * ⓘ Basic Standard

Configure virtual network.

Virtual network * ⓘ ▼

Subnet * ▼

[Manage subnet configuration](#)

IP address assignment * Static Dynamic

[Review + create](#) [< Previous](#) [Next : Tags >](#) [Download a template for automation](#)

- Para crear un balanceador de cargas externo, elija el tipo de equilibrador de carga como **Público** y cree aquí la dirección IP pública.

The screenshot shows the 'Create load balancer' page in the Microsoft Azure portal. The page is titled 'Create load balancer' and includes a search bar at the top. The configuration options are as follows:

- Type: Internal Public
- SKU: Standard Basic
- Tier: Regional Global
- Public IP address: Create new Use existing
- Public IP address name: [Empty text box]
- Public IP address SKU: Standard
- IP address assignment: Dynamic Static
- Availability zone: [Dropdown menu]
- Add a public IPv6 address: No Yes
- Routing preference: Microsoft network Internet

At the bottom of the page, there is a 'Review + create' button, a '< Previous' button, a 'Next : Tags >' button, and a 'Download a template for automation' link.

1. Después de crear Azure Load Balancer, vaya a **Configuración IP frontend** y anote la dirección IP que se muestra aquí. Debe utilizar esta dirección IP al crear el servidor virtual de equilibrio de carga de ADC como en el paso 3.



2. En la página de **configuración de Azure Load Balancer**, la implementación de la plantilla ARM ayuda a crear la regla LB, los grupos de back-end y las sondas de estado.
3. Agregue las NIC cliente de par de alta disponibilidad al grupo de back-end de la ILB.
4. Creación de un sondeo de estado (TCP, puerto 9000)
5. Cree dos reglas de equilibrio de carga:
 - Una regla LB para el tráfico HTTP (caso de uso de aplicaciones web) en el puerto 80. La regla también debe utilizar el puerto de back-end 80. Seleccione el grupo de back-end creado y el sondeo de estado. La IP flotante debe estar habilitada.
 - Otra regla LB para el tráfico HTTPS o CVAD en el puerto 443. El proceso es el mismo que el tráfico HTTP.

Paso 3. En el nodo principal del dispositivo NetScaler, cree un servidor virtual de equilibrio de carga para ILB.

1. Agregue un servidor virtual de equilibrio de carga.

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

Ejemplo

```
1 add lb vserver vserver_name HTTP 52.172.96.71 80
```

Nota:

Utilice la dirección IP frontend del equilibrador de carga, que está asociada con el equilibrador de carga adicional que crea en el paso 2.

2. Enlazar un servicio a un servidor virtual de equilibrio de carga.

```
1 bind lb vserver <name> <serviceName>
```

Ejemplo

```
1 bind lb vserver Vserver-LB-1 Service-HTTP-1
```

Para obtener más información, consulte [Configuración del equilibrio de carga básico](#).

Paso 4: Como alternativa al paso 3, puede crear un servidor virtual de equilibrio de carga para ILB mediante IPsets.

1. Agregue una dirección IP del tipo IP del servidor virtual (VIP).

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

Ejemplo

```
1 add nsip 52.172.96.71 -type vip
```

2. Agregue un IPset en los nodos primario y secundario.

```
1 add ipset <name>
```

Ejemplo

```
1 add ipset ipset1
```

3. Enlazar direcciones IP al conjunto de IP.

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

Ejemplo

```
1 bind ipset ipset1 52.172.96.71
```

4. Configure el servidor virtual LB existente para que use el IPSet.

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

Ejemplo

```
1 set lb vserver vserver_name -ipset ipset1
```

Para obtener más información, consulte [Configuración de un servidor virtual multi-IP](#).

Instalación de una instancia de NetScaler VPX en Azure VMware Solution

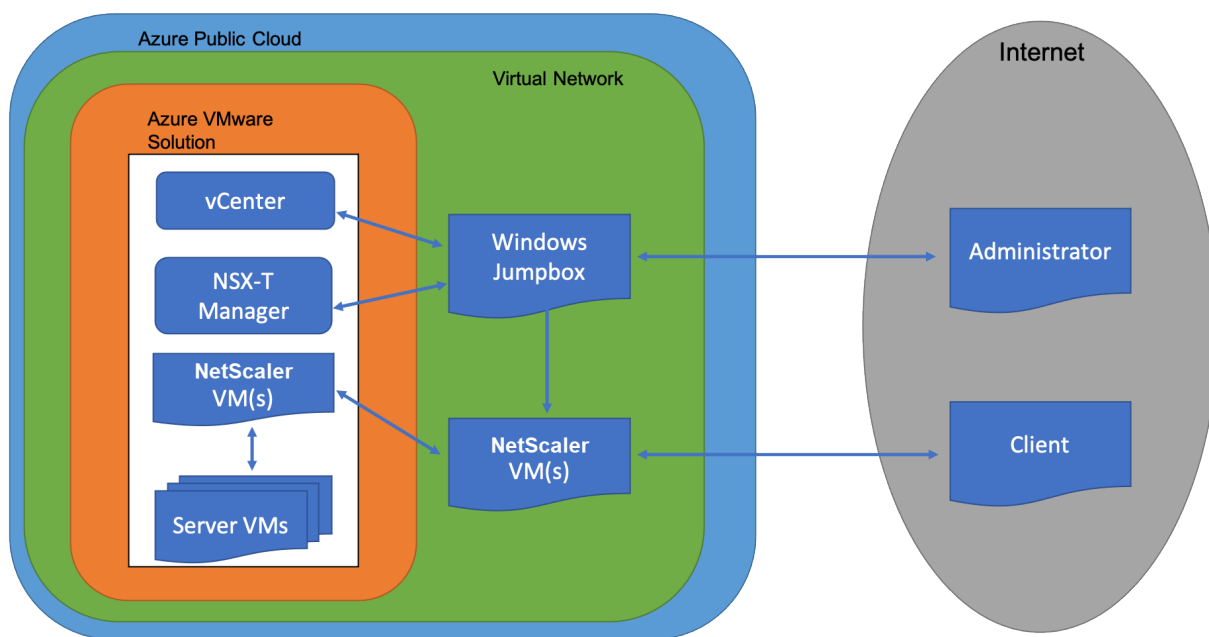
October 17, 2024

Azure VMware Solution (AVS) le proporciona nubes privadas que contienen clústeres de vSphere, creados a partir de una infraestructura exclusiva de Azure exclusiva. La implementación inicial mínima es de tres hosts, pero se pueden agregar hosts adicionales uno a uno, hasta un máximo de 16 hosts por clúster. Todas las nubes privadas aprovisionadas tienen vCenter Server, vSAN, vSphere y NSX-T.

VMware Cloud (VMC) en Azure le permite crear centros de datos definidos por software en la nube (SDDC) en Azure con el número de hosts ESX que desea. La VMC en Azure admite implementaciones NetScaler VPX. VMC proporciona una interfaz de usuario igual que vCenter en las instalaciones. Funciona de forma similar a las implementaciones NetScaler VPX basadas en ESX.

En el siguiente diagrama se muestra la solución Azure VMware en la nube pública de Azure a la que un administrador o un cliente pueden acceder a través de Internet. Un administrador puede crear, administrar y configurar máquinas virtuales de servidor o de carga de trabajo mediante la solución Azure VMware. El administrador puede acceder a vCenter basado en web y NSX-T Manager de AVS desde un Windows Jumpbox. Puede crear instancias NetScaler VPX (par independientes o de alta disponibilidad) y las máquinas virtuales de servidor dentro de Azure VMware Solution mediante vCenter y administrar la red correspondiente mediante NSX-T manager. La instancia NetScaler VPX en AVS funciona de forma similar al clúster de hosts de VMware local. AVS se administra desde un Windows Jumpbox creado en la misma red virtual.

Un cliente solo puede acceder al servicio AVS si se conecta al VIP de ADC. Otra instancia NetScaler VPX fuera de Azure VMware Solution pero en la misma red virtual de Azure ayuda a agregar la VIP de la instancia NetScaler VPX dentro de Azure VMware Solution como servicio. Según el requisito, puede configurar la instancia NetScaler VPX para proporcionar servicio a través de Internet.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la [documentación de Azure VMware Solution](#).
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte [Implementación de una nube privada de Azure VMware Solution](#).
- Para obtener más información sobre la creación de una máquina virtual Windows Jump box para acceder y administrar Azure VMware Solution, consulte [Acceso a una nube privada de Azure VMware Solution](#).
- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte [Agregar un segmento de red en Azure VMware Solution](#).
- Obtenga archivos de licencias VPX.
- Las máquinas virtuales (VM) creadas o migradas a la nube privada de Azure VMware Solution deben estar conectadas a un segmento de red.

RequiVMware de hardware en la nube

En la tabla siguiente se enumeran los recursos informáticos virtuales que el SDDC de VMware debe proporcionar para cada dispositivo virtual VPX nCore.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de NetScaler VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En VMware SDDC, puede instalar un máximo de 10 interfaces de red virtuales si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

Nota:

Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso en producción del dispositivo virtual VPX, debe reservarse la asignación de memoria completa.

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. En la tabla siguiente se describen los requisitos del sistema para instalar la herramienta OVF.

Tabla 2. Requisitos del sistema para instalar herramientas OVF

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Guía del usuario de herramientas OVF” en http://kb.vmware.com/ .
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC	NIC de 100 Mbps o más rápido

Para obtener información sobre la instalación de OVF, busque el archivo PDF “Guía del usuario de la herramienta OVF” en <http://kb.vmware.com/>.

Descarga de los archivos de configuración de NetScaler VPX

El paquete de configuración de instancias NetScaler VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en <http://www.citrix.com>. Haga clic en el **vínculo Nuevos usuarios** y siga las instrucciones para crear una nueva cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

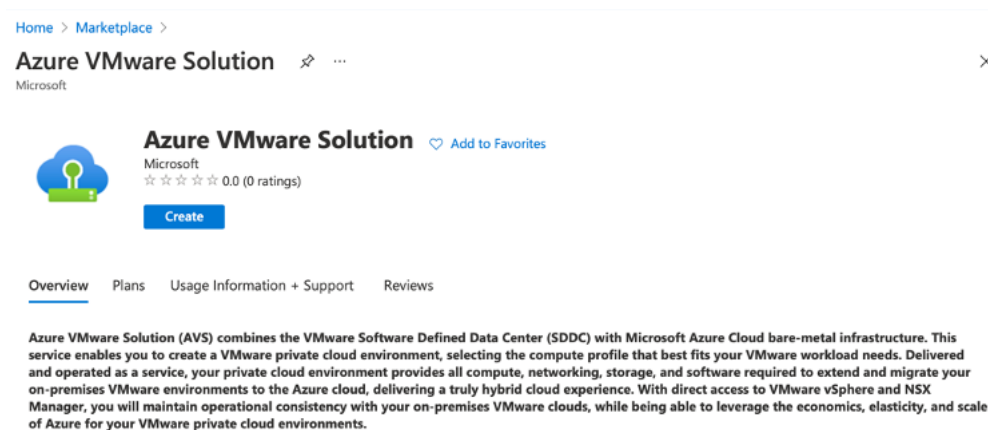
Citrix.com > **Descargas** > **NetScaler** > **Dispositivos virtuales**.

Copie los siguientes archivos en una estación de trabajo de la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (por ejemplo, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (por ejemplo, NSVPX-ESX-13.0-79.64.mf)

Implementación de la solución Azure VMware

1. Inicie sesión en su [portal de Microsoft Azure](#) y vaya a **Azure Marketplace**.
2. En **Azure Marketplace**, busque **Azure VMware Solution** y haga clic en **Crear**.



3. En la página **Crear una nube privada**, introduzca los siguientes detalles:
 - Seleccione un mínimo de 3 hosts ESXi para crear el clúster predeterminado de su nube privada.
 - Para el campo **Bloque de direcciones**, utilice el espacio de direcciones **/22**.
 - Para la **red virtual**, asegúrese de que el rango CIDR no se superponga con ninguna de sus subredes locales u otras subredes de Azure (redes virtuales) o con la subred de puerta de enlace.

- La subred de puerta de enlace se utiliza para enrutar expresamente la conexión con la nube privada.

[Home](#) >

Create a private cloud ...

Azure settings

Subscription * ⓘ

Resource group * ⓘ
[Create new](#)

Location * ⓘ

General

Resource name * ⓘ

SKU * ⓘ

ESXi hosts * ⓘ

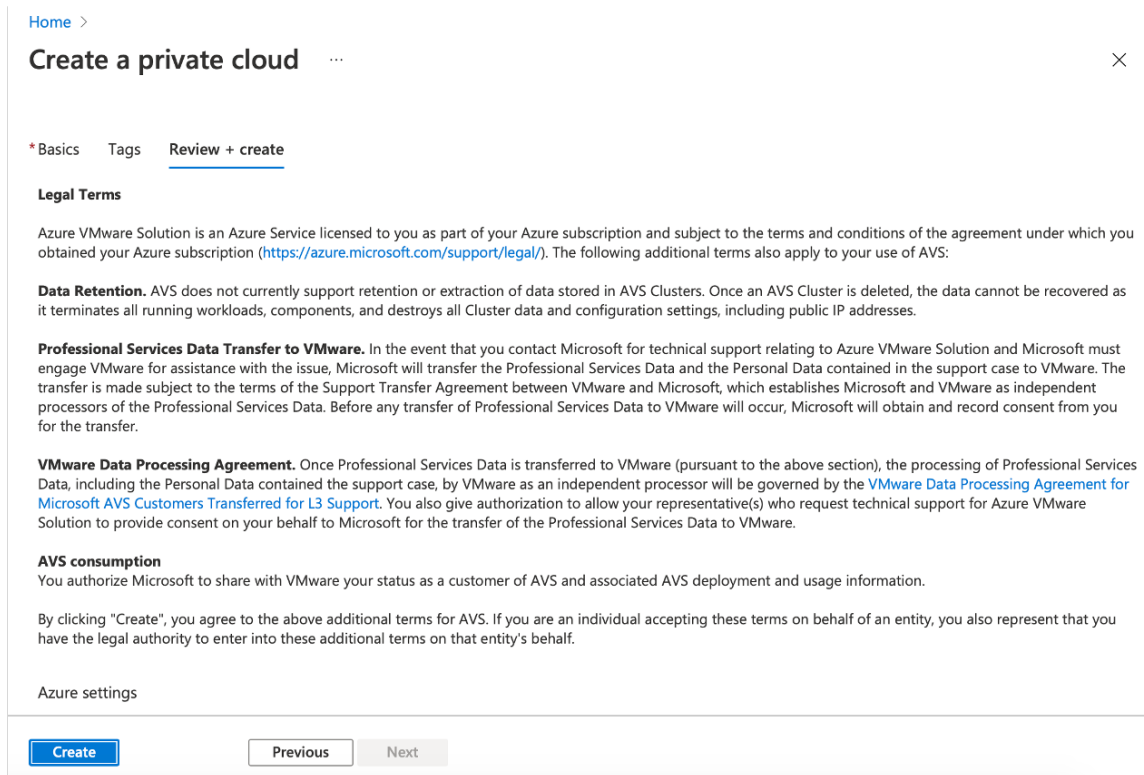
\$11,929.68
estimated monthly total

Address block * ⓘ

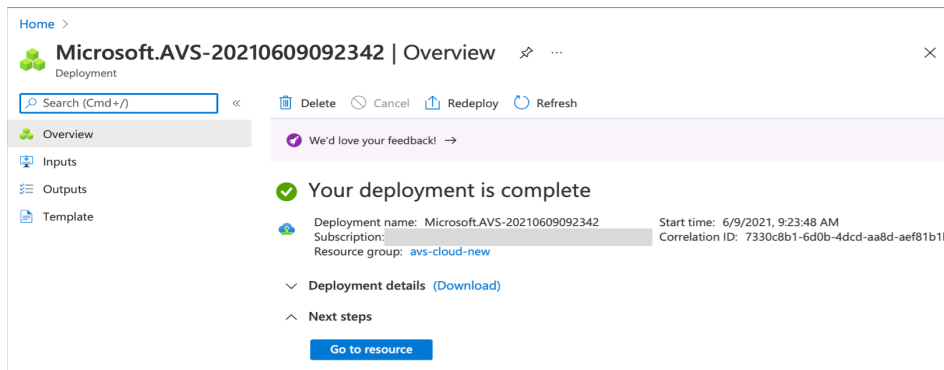
Virtual Network
[Create new](#)
Only Virtual Networks with a valid subnet with the name "GatewaySubnet" are available for selection. For details about adding subnet in a virtual network, refer to details [here](#)

[Review + create](#) [Previous](#) [Next : Tags >](#)

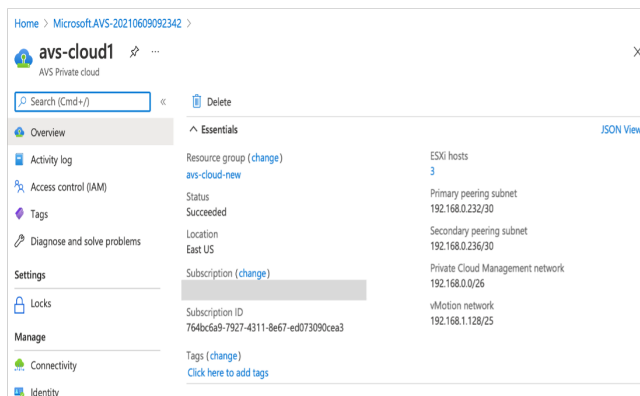
4. Haga clic en **Revisar + Crear**.
5. Revise la configuración. Si debe cambiar la configuración, haga clic en **Anterior**.



6. Haga clic en **Create**. Comienza el proceso de aprovisionamiento de nube privada. La nube privada puede tardar hasta dos horas en aprovisionarse.



7. Haga clic en **Ir al recurso** para verificar la nube privada creada.



Nota:

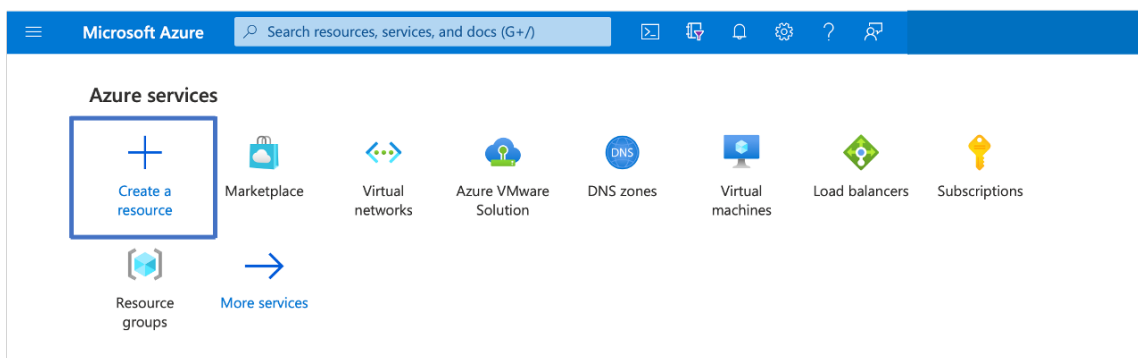
Para acceder a este recurso, necesita una máquina virtual en Windows que actúe como Jump box.

Conectarse a una máquina virtual de Azure que ejecuta Windows

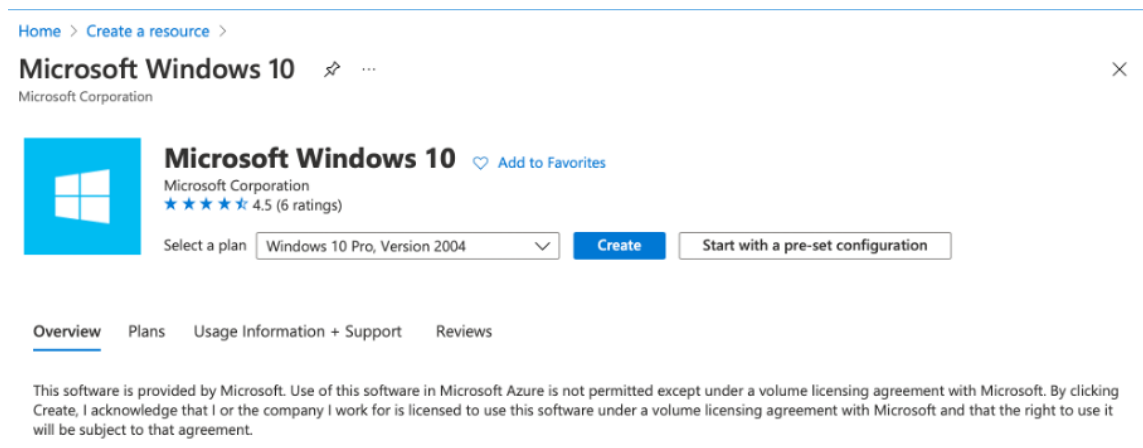
En este procedimiento se muestra cómo utilizar el portal de Azure para implementar una máquina virtual (VM) en Azure que ejecuta Windows Server 2019. Para ver la máquina virtual en acción, a continuación, RDP en la máquina virtual e instala el servidor web de IIS.

Para acceder a la nube privada que ha creado, debe crear un cuadro de Windows Jump dentro de la misma red virtual.

1. Vaya al **portal de Azure** y haga clic en **Crear un recurso**.



2. Busque **Microsoft Windows 10** y haga clic en **Crear**.



3. Cree una máquina virtual (VM) que ejecute Windows Server 2019. Aparece la página **Crear una máquina virtual**. Introduzca todos los detalles en la ficha **Conceptos básicos** y active la casilla de verificación **Licencias**. Deje los valores predeterminados restantes y, a continuación, seleccione el botón **Revisar + crear** en la parte inferior de la página.

Home > Create a resource > Microsoft Windows 10 >

Create a virtual machine

Basics | Disks | Networking | Management | 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](#)

Project details

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

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Image * [See all images](#)

Azure Spot instance

Size * [See all sizes](#)

Administrator account

Username *

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports *

⚠ 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 Windows 10 license with multi-tenant hosting rights. [Review multi-tenant hosting rights for Windows 10 compliance](#)

[Review + create](#) < Previous Next: Disks >

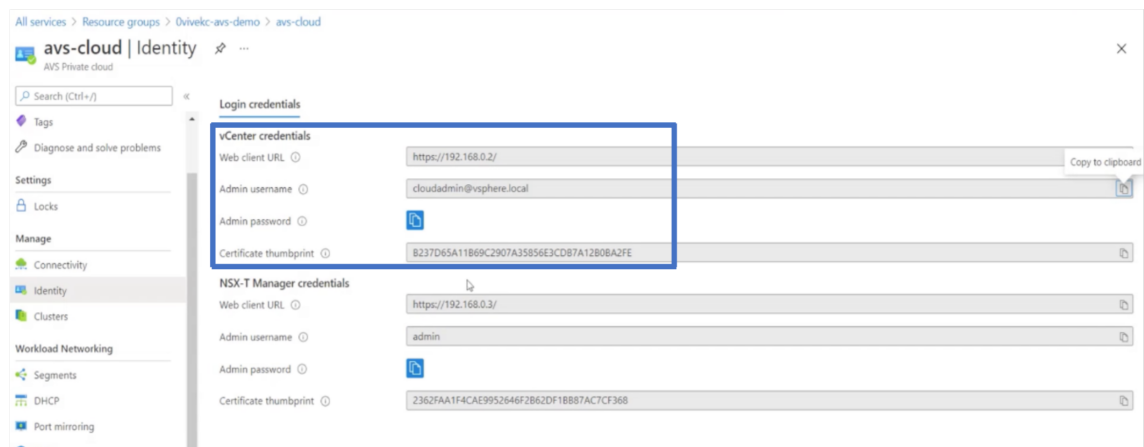
4. Una vez ejecutada la validación, seleccione el botón **Crear** en la parte inferior de la página.
5. Una vez finalizada la implementación, seleccione **Ir al recurso**.
6. Vaya a la máquina virtual de Windows que ha creado. Utilice la dirección IP pública de la máquina virtual de Windows y conéctese mediante RDP.

Utilice el botón **Conectar** del portal de Azure para iniciar una sesión de Escritorio remoto (RDP) desde un escritorio Windows. Primero se conecta a la máquina virtual y, a continuación, inicia sesión.

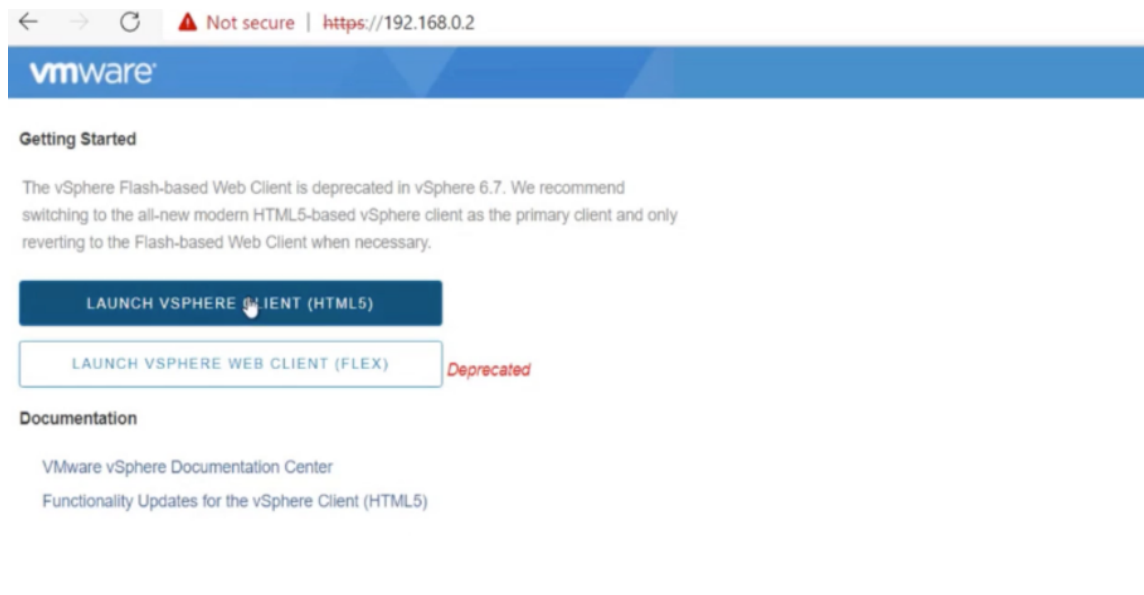
Para conectarse a una máquina virtual Windows desde una Mac, debe instalar un cliente RDP para Mac, como Microsoft Remote Desktop. Para obtener más información, consulte [Cómo conectarse e iniciar sesión en una máquina virtual de Azure que ejecuta Windows](#).

Acceda a su portal vCenter de nube privada

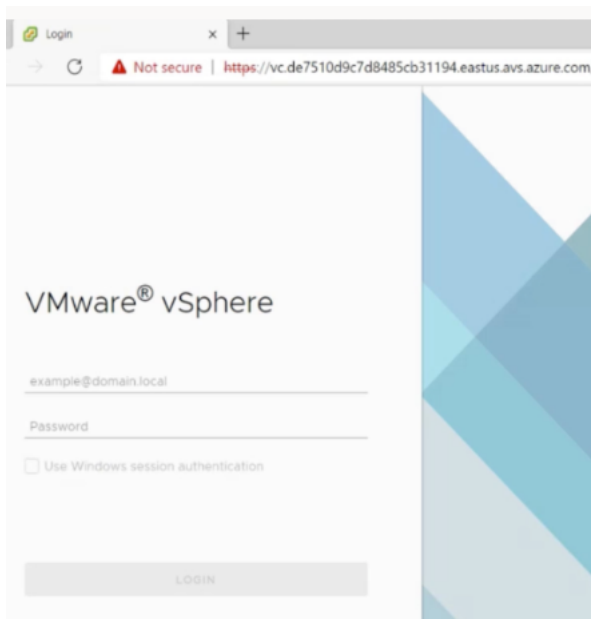
1. En la nube privada de Azure VMware Solution, en **Administrar**, seleccione **Identidad**. Anote las credenciales de vCenter.



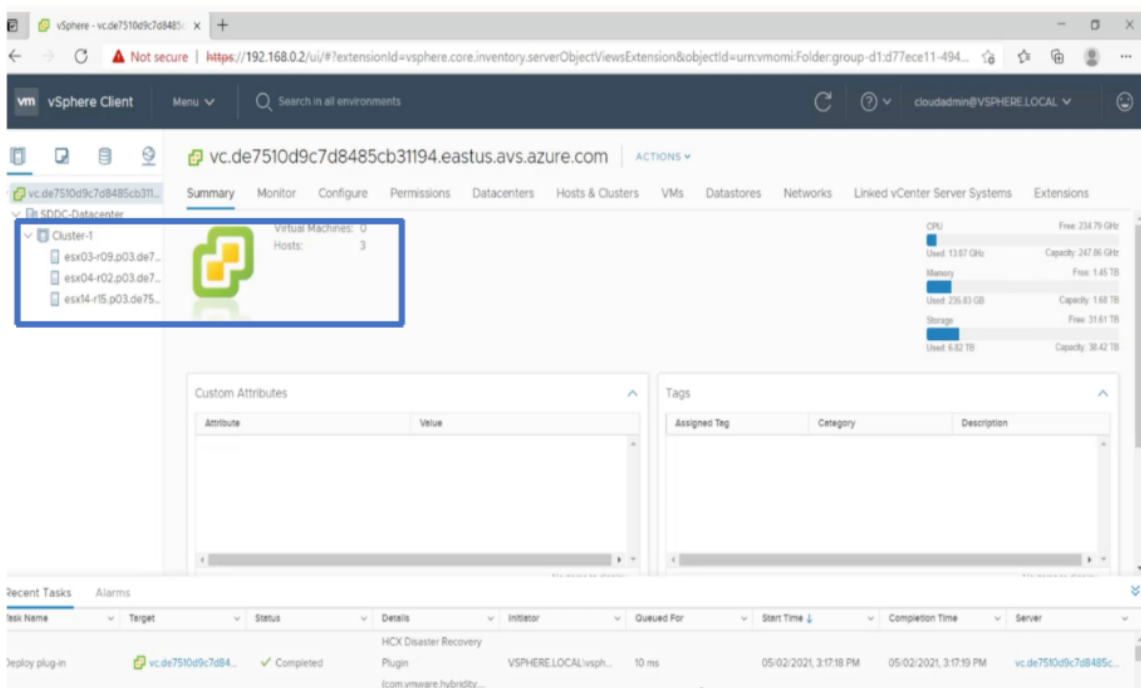
2. Inicie el cliente de vSphere escribiendo la URL del cliente web de vCenter.



3. Inicie sesión en VMware vSphere mediante las credenciales de vCenter de la nube privada de Azure VMware Solution.



4. En el cliente de vSphere, puede verificar los hosts ESXi que ha creado en el portal de Azure.



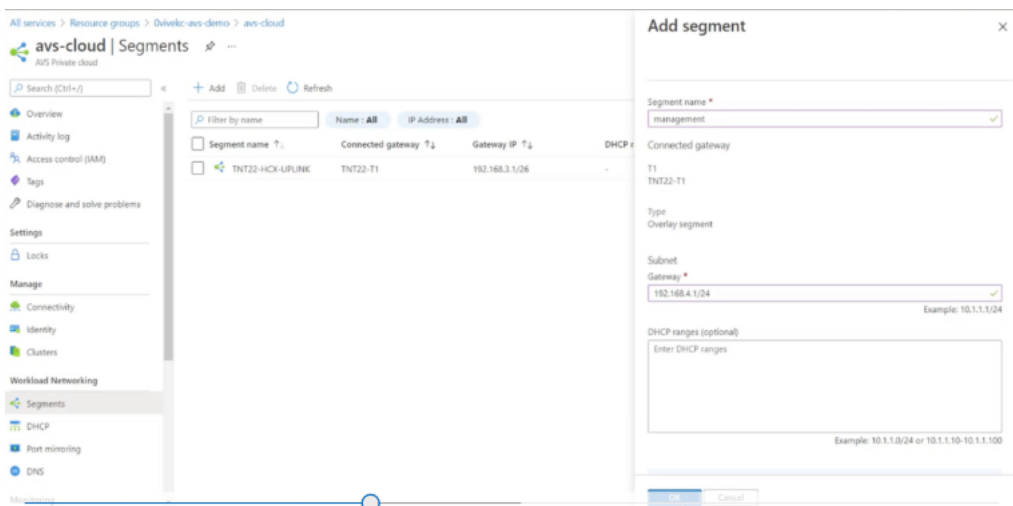
Para obtener más información, consulte [Acceso al portal de vCenter de Private Cloud](#).

Creación de un segmento NSX-T en el portal de Azure

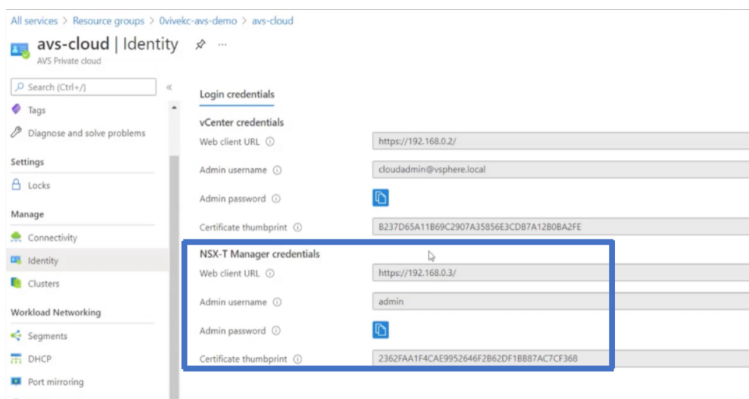
Puede crear y configurar un segmento de NSX-T desde la consola de Azure VMware Solution en el portal de Azure. Estos segmentos están conectados a la puerta de enlace predeterminada de nivel

1 y las cargas de trabajo de estos segmentos obtienen conectividad Este-Oeste y Norte-Sur. Una vez creado el segmento, se muestra en NSX-T Manager y vCenter.

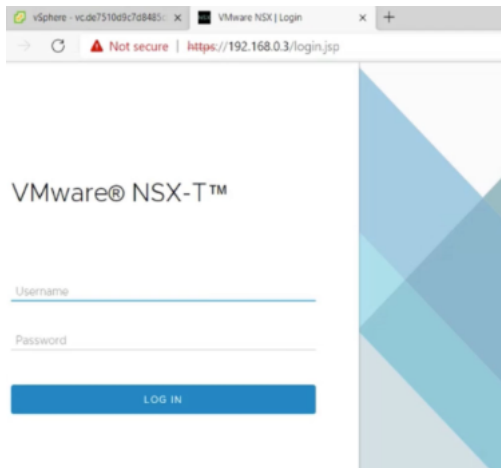
1. En la nube privada de Azure VMware Solution, en **Redes de carga de trabajo**, seleccione **Segmentos > Agregar**. Proporcione los detalles del nuevo segmento lógico y seleccione **Aceptar**. Puede crear tres segmentos independientes para las interfaces de cliente, administración y servidor.



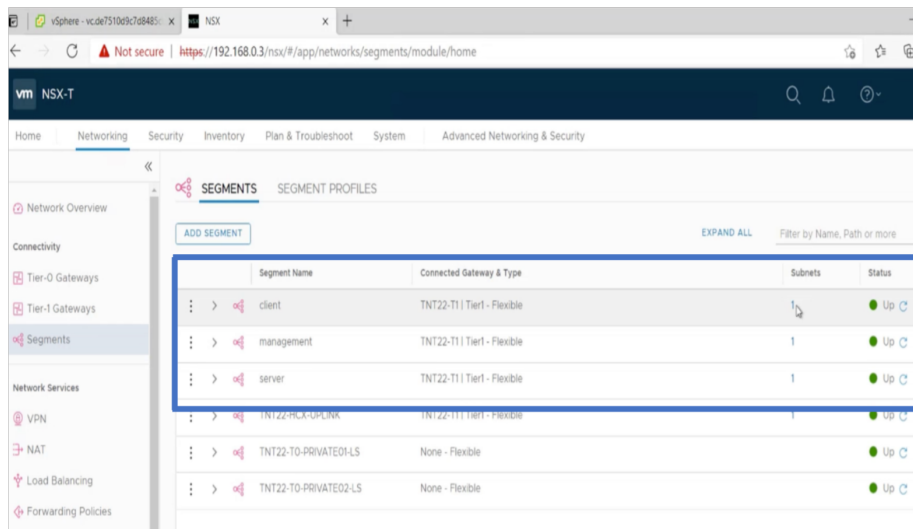
2. En la nube privada de Azure VMware Solution, en **Administrar**, seleccione **Identidad**. Anote las credenciales de NSX-T Manager.



3. Inicie VMware NSX-T Manager escribiendo la URL del cliente web de NSX-T.



4. En el gestor de NSX-T, en **Redes > Segmentos**, puede ver todos los segmentos que ha creado. También puede verificar las subredes.



Para obtener más información, consulte [Creación de un segmento de NSX-T en el portal de Azure](#).

Instalar una instancia de NetScaler VPX en la nube de VMware

Después de instalar y configurar el centro de datos definido por software (SDDC) de VMware, puede utilizar el SDDC para instalar dispositivos virtuales en la nube de VMware. El número de dispositivos virtuales que puede instalar depende de la cantidad de memoria disponible en el SDDC.

Para instalar instancias NetScaler VPX en la nube de VMware, lleve a cabo estos pasos en Windows Jumpbox VM:

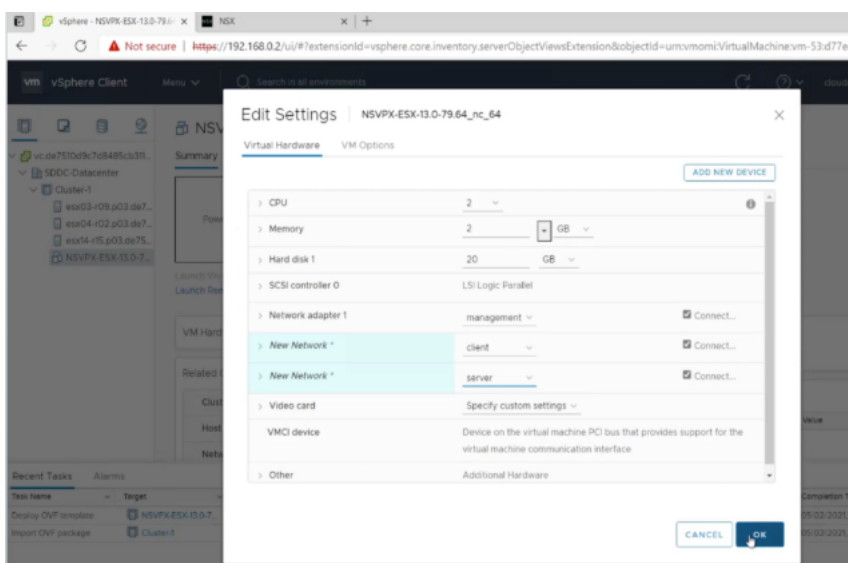
1. Descargue los archivos de configuración de instancias de NetScaler VPX para el host ESXi desde el sitio de descargas de NetScaler.

2. Abra VMware SDDC en Windows Jumpbox.
3. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en **Iniciar sesión**.
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla OVF**, en el campo **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias NetScaler VPX, seleccione el archivo.ovf y haga clic en **Siguiente**.

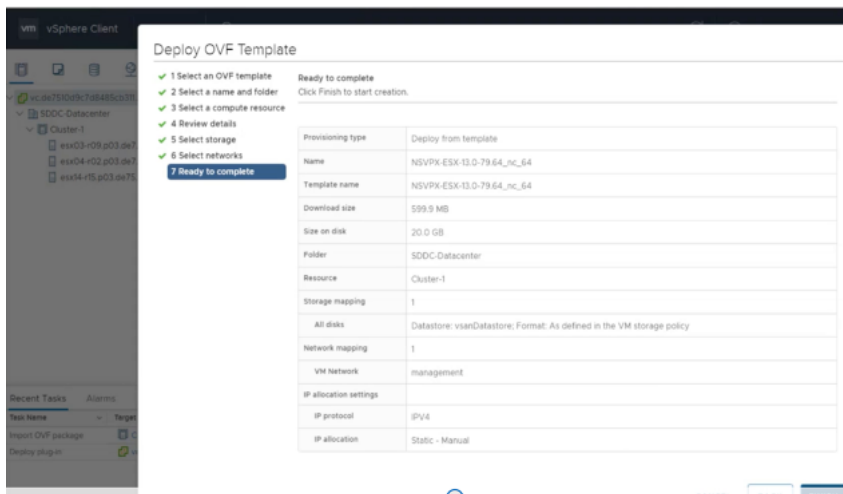
Nota:

De forma predeterminada, la instancia de NetScaler VPX utiliza interfaces de red E1000. Para implementar ADC con la interfaz VMXNET3, modifique el OVF para utilizar la interfaz VMXNET3 en lugar de E1000. La disponibilidad de la interfaz VMXNET3 está limitada por la infraestructura de Azure y es posible que no esté disponible en Azure VMware Solution.

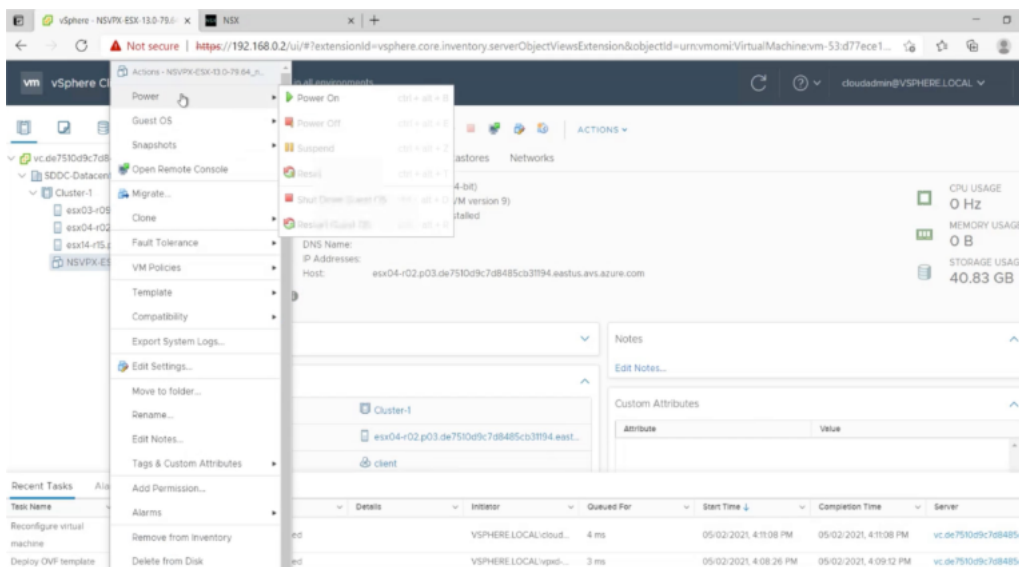
6. Asigne las redes que se muestran en la plantilla OVF del dispositivo virtual a las redes configuradas en el SDDC de VMware. Haz clic en **Aceptar**.



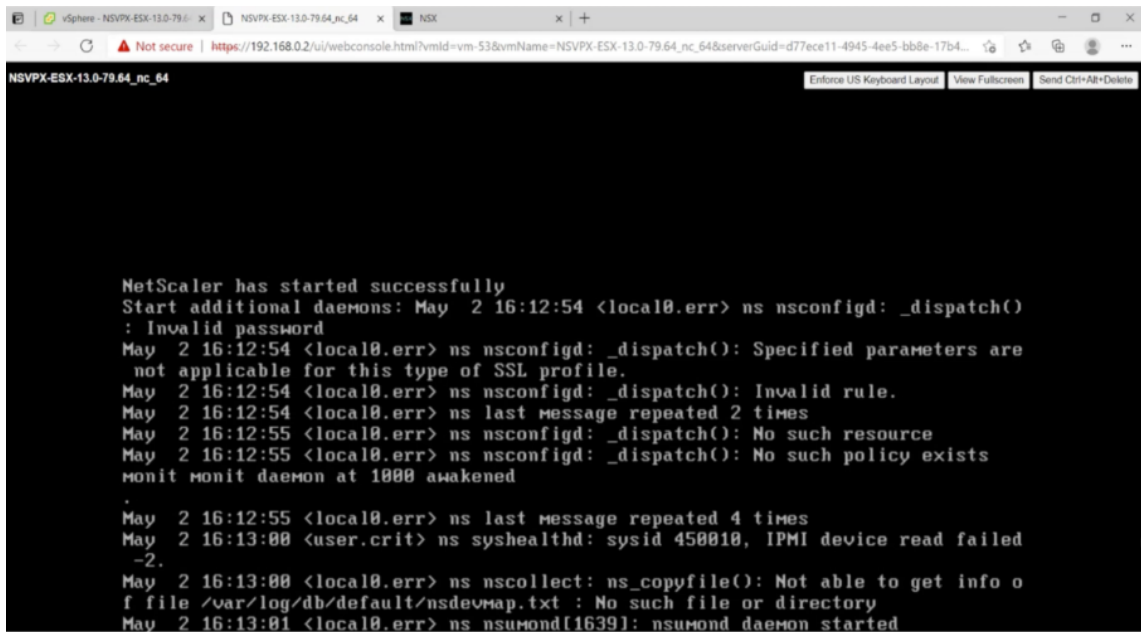
7. Haga clic en **Finalizar** para iniciar la instalación de un dispositivo virtual en VMware SDDC.



8. Ya está listo para iniciar la instancia de NetScaler VPX. En el panel de navegación, seleccione la instancia de NetScaler VPX que ha instalado y, en el menú contextual, seleccione **Encendido**. Haga clic en la ficha **Console** para emular un puerto de consola.



9. Ahora está conectado a la máquina virtual NetScaler desde el cliente de vSphere.



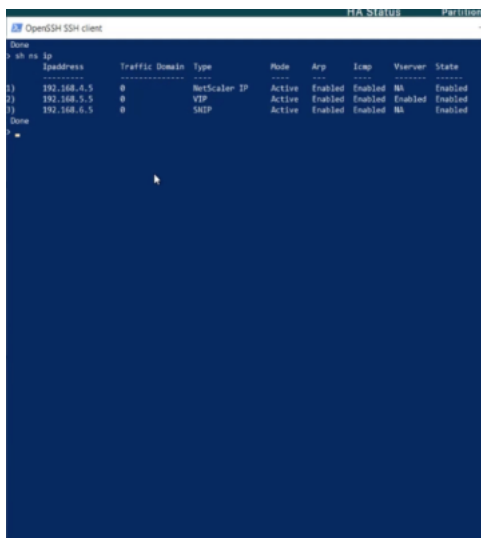
10. Para acceder al dispositivo NetScaler mediante las claves SSH, escriba el siguiente comando en la CLI:

```
1 ssh nsroot@<management IP address>
```

Ejemplo

```
1 ssh nsroot@192.168.4.5
```

11. Puede verificar la configuración de ADC mediante el comando `show ns ip`.

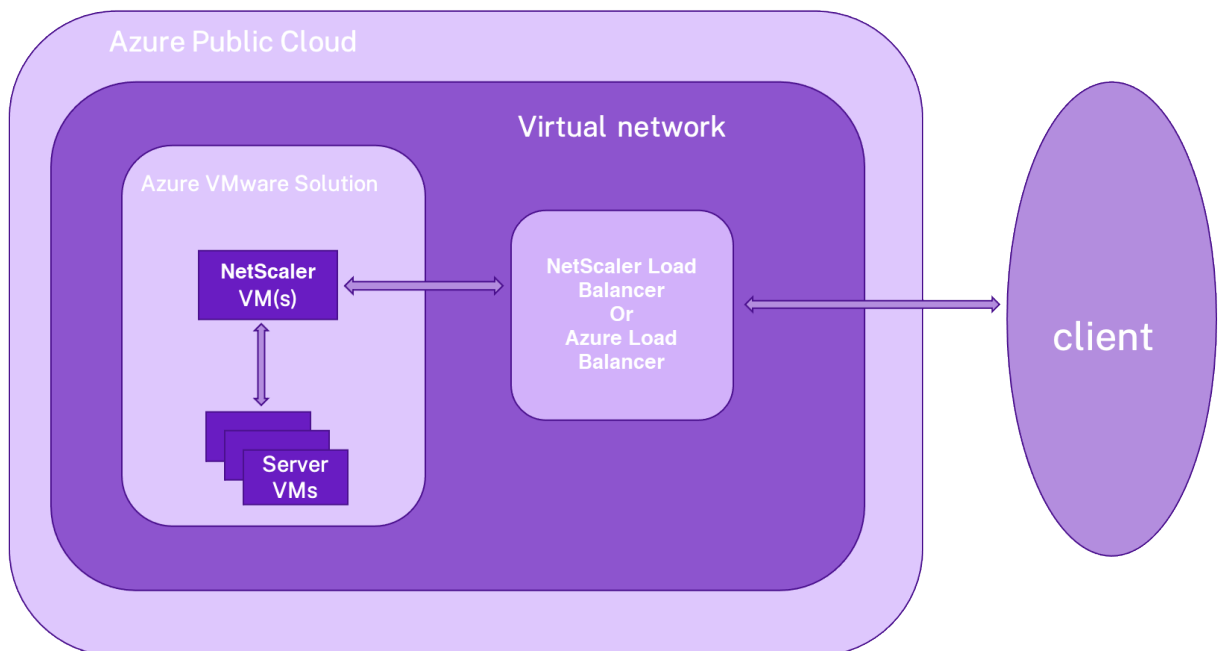


Configurar una instancia independiente de NetScaler VPX en la solución Azure VMware

October 17, 2024

Puede configurar una instancia independiente de NetScaler VPX en la solución Azure VMware (AVS) para aplicaciones orientadas a Internet.

El siguiente diagrama muestra la instancia independiente de NetScaler VPX en Azure VMware Solution. Un cliente puede acceder al servicio AVS conectándose a la dirección IP virtual (VIP) de NetScaler dentro del AVS. Puede lograrlo aprovisionando un equilibrador de carga NetScaler o la instancia del equilibrador de carga de Azure fuera de AVS pero en la misma red virtual de Azure. Configure el equilibrador de carga para acceder a la VIP de la instancia de NetScaler VPX dentro del servicio AVS.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, lea los siguientes requisitos previos de Azure:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la [documentación de Azure VMware Solution](#).
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte [Implementación de una nube privada de Azure VMware Solution](#).
- Para obtener más información sobre la creación de una máquina virtual de Windows Jump Box para acceder y administrar la solución Azure VMware, consulte [Acceder a una nube privada de](#)

[Azure VMware Solution.](#)

- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte [Agregar un segmento de red en Azure VMware Solution](#)
- Para obtener más información sobre cómo instalar una instancia de NetScaler VPX en la nube de VMware, consulte [Instalar una instancia de NetScaler VPX en la nube de VMware.](#)

Configurar una instancia independiente de NetScaler VPX en AVS mediante el equilibrador de carga NetScaler

Siga estos pasos para configurar la instancia independiente de NetScaler VPX en AVS para aplicaciones orientadas a Internet mediante el equilibrador de carga NetScaler.

1. Implemente una instancia de NetScaler VPX en la nube de Azure. Para obtener más información, consulte [Configurar una instancia independiente de NetScaler VPX.](#)

Nota:

Asegúrese de que se implemente en la misma red virtual que Azure VMware Cloud.

2. Configure la instancia de NetScaler VPX para acceder a la dirección VIP de NetScaler VPX implementada en AVS.
 - a) Agregue un servidor virtual de equilibrio de carga.

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

Ejemplo

```
1 add lb vserver lb1 HTTPS 172.31.0.6 443
```

- b) Agregue un servicio que se conecte al VIP de NetScaler VPX implementado en AVS.

```
1 add service <name> <ip> <serviceType> <port>
```

Ejemplo

```
1 add service webserver1 192.168.4.10 HTTP 80
```

- c) Enlazar un servicio al servidor virtual de equilibrio de carga.

```
1 bind lb vserver <name> <serviceName>
```

Ejemplo

```
1 bind lb vserver lb1 webserver1
```

Configurar la instancia independiente de NetScaler VPX en AVS mediante el equilibrador de carga de Azure

Siga estos pasos para configurar la instancia independiente de NetScaler VPX en AVS para aplicaciones orientadas a Internet mediante el equilibrador de carga de Azure.

1. Configure una instancia de Azure Load Balancer en la nube de Azure. Para obtener más información, consulte la [documentación de Azure sobre la creación de equilibradores de carga](#).
2. Agregue la dirección VIP de la instancia de NetScaler VPX que se implementa en AVS al grupo back-end.

El siguiente comando de Azure agrega una dirección IP de back-end al grupo de direcciones de back-end de equilibrio de carga.

```
1 az network lb address-pool address add
2                               --resource-group <Azure VMC
3                               Resource Group>
4                               --lb-name <LB Name>
5                               --pool-name <Backend pool
6                               name>
7                               --vnet <Azure VMC Vnet>
8                               --name <IP Address name>
9                               --ip-address <VIP of ADC in
10                              VMC>
```

Nota:

Asegúrese de que el equilibrador de carga de Azure se implemente en la misma red virtual que la nube de Azure VMware.

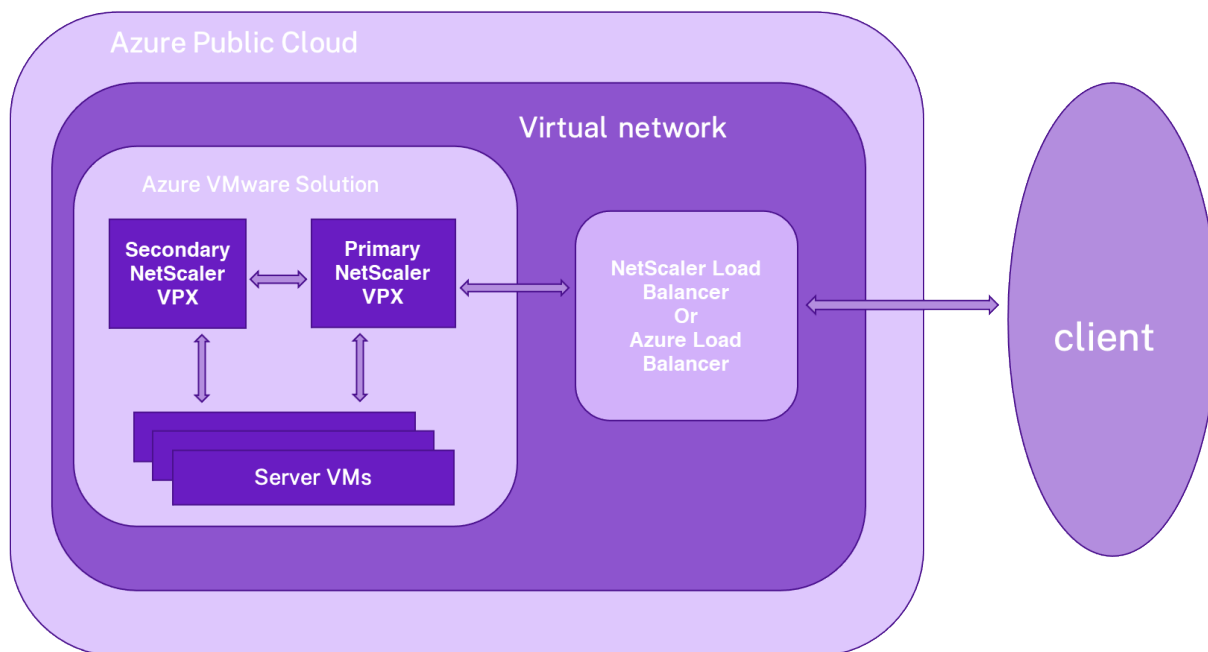
Configurar una instalación de alta disponibilidad de NetScaler VPX en la solución Azure VMware

October 17, 2024

Puede configurar una configuración de alta disponibilidad de NetScaler VPX en la solución Azure VMware (AVS) para aplicaciones orientadas a Internet.

El siguiente diagrama muestra el par de alta disponibilidad de NetScaler VPX en AVS. Un cliente puede acceder al servicio AVS conectándose al VIP del nodo ADC principal dentro del AVS. Puede lograrlo

aprovisionando un equilibrador de carga NetScaler o la instancia del equilibrador de carga de Azure fuera de AVS pero en la misma red virtual de Azure. Configure el equilibrador de carga para acceder al VIP del nodo ADC principal dentro del servicio AVS.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, lea los siguientes requisitos previos de Azure:

- Para obtener más información sobre la solución Azure VMware y sus requisitos previos, consulte la [documentación de Azure VMware Solution](#).
- Para obtener más información sobre la implementación de la solución Azure VMware, consulte [Implementación de una nube privada de Azure VMware Solution](#).
- Para obtener más información sobre la creación de una máquina virtual de Windows Jump Box para acceder y administrar la solución Azure VMware, consulte [Acceder a una nube privada de Azure VMware Solution](#).
- En la máquina virtual de Windows Jump box, descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulte [Agregar un segmento de red en Azure VMware Solution](#).

Pasos de configuración

Siga estos pasos para configurar la configuración de alta disponibilidad de NetScaler VPX en AVS para aplicaciones orientadas a Internet.

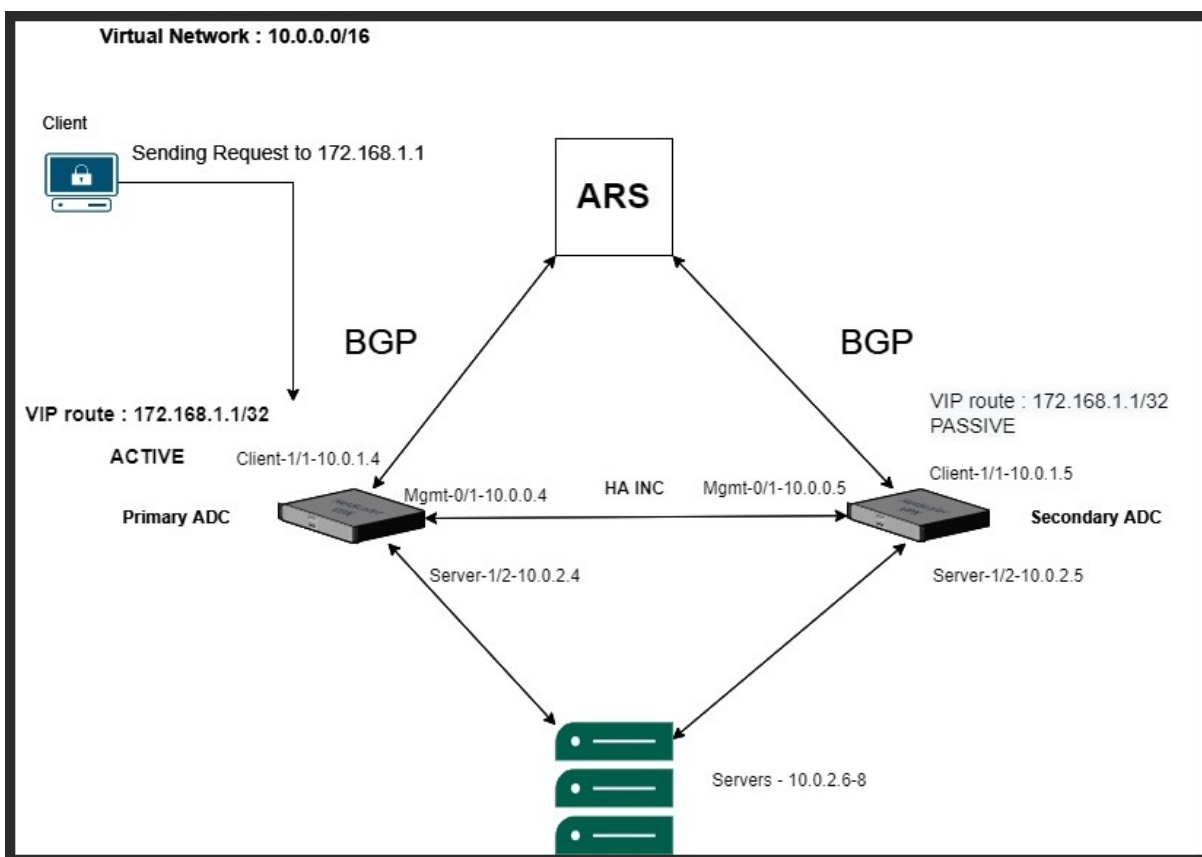
1. Cree dos instancias de NetScaler VPX en la nube de VMware. Para obtener más información, consulte [Instalar una instancia de NetScaler VPX en la nube VMware](#).
2. Configure la configuración de NetScaler HA. Para obtener más información, consulte [Configuración de alta disponibilidad](#).
3. Configure la configuración de NetScaler HA para que sea accesible para las aplicaciones orientadas a Internet.
 - Para configurar la instancia de NetScaler VPX utilizando el balanceador de carga de NetScaler, consulte [Configurar una instancia independiente de NetScaler VPX en AVS utilizando el balanceador de carga de NetScaler](#).
 - Para configurar la instancia de NetScaler VPX con el equilibrador de carga de Azure, consulte [Configurar la instancia independiente de NetScaler VPX en AVS con el equilibrador de carga de Azure](#).

Configurar el servidor de rutas de Azure con un par de alta disponibilidad de NetScaler VPX

October 17, 2024

Puede configurar el servidor de rutas de Azure con la instancia NetScaler VPX para intercambiar las rutas VIP configuradas con la red virtual mediante el protocolo BGP. El NetScaler se puede implementar de forma independiente o en modo HA-INC y, a continuación, se puede configurar con BGP. Esta implementación no requiere un equilibrador de carga (ALB) de Azure delante del par de alta disponibilidad de ADC.

El siguiente diagrama muestra cómo se integra una topología de alta disponibilidad de VPX con el servidor de rutas de Azure. Cada una de las instancias de ADC tiene 3 interfaces: una para la administración, otra para el tráfico del cliente y otra para el tráfico del servidor.



El diagrama de topología utiliza las siguientes direcciones IP.

Ejemplo de configuración de IP para la instancia de ADC principal:

```

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
    
```

Ejemplo de configuración de IP para la instancia de ADC secundaria:

```

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
    
```

Requisitos previos

Debe estar familiarizado con la siguiente información antes de implementar una instancia de NetScaler VPX en Azure.

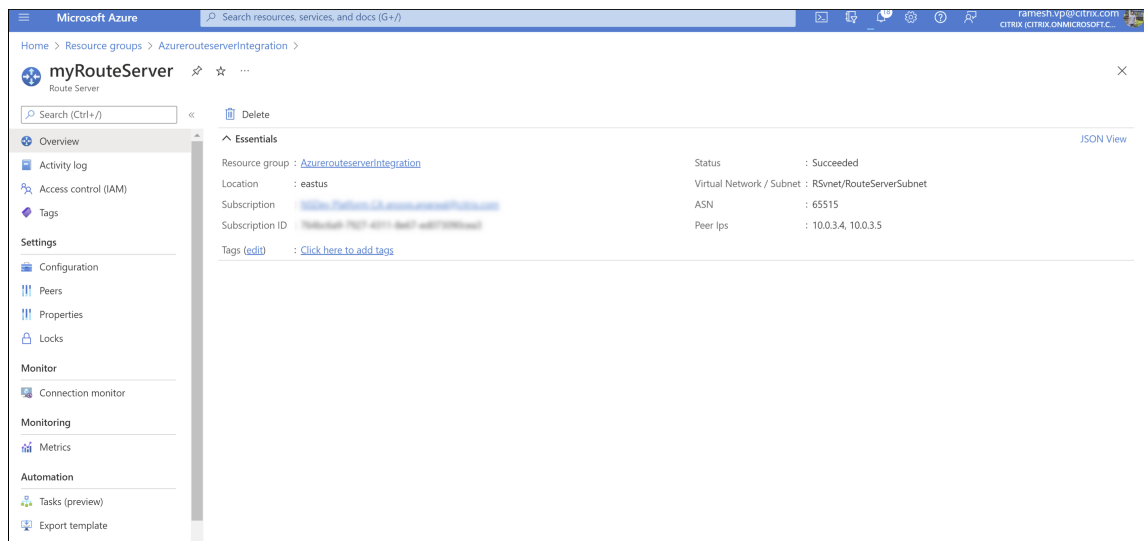
- Terminología y detalles de red de Azure. Para obtener más información, consulte [Terminología de Azure](#).

- Descripción general del servidor de rutas de Azure. Para obtener más información, consulte [What is Azure Route Server?](#).
- Funcionamiento de un dispositivo NetScaler. Para obtener más información, consulte la [documentación de NetScaler](#).
- Redes NetScaler. Para obtener más información, consulte [ADC Networking](#).

Cómo configurar un servidor de rutas de Azure con un par de alta disponibilidad de NetScaler VPX

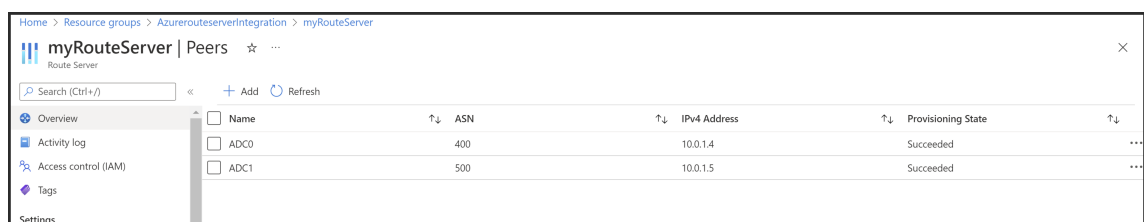
1. Cree un servidor de rutas en el portal de Azure. Para obtener más información, consulte [Crear y configurar un servidor de rutas mediante el portal de Azure](#).

En el siguiente ejemplo, la subred 10.0.3.0/24 se usa para implementar el servidor Azure. Una vez creado el servidor de rutas, obtenga las direcciones IP del servidor de rutas, por ejemplo: 10.0.3.4, 10.0.3.5.



2. Configure el emparejamiento con el dispositivo virtual de red (NVA) en el portal de Azure. Agregue su instancia NetScaler VPX como NVA. Para obtener más información, consulte [Configurar el emparejamiento con NVA](#).

En el siguiente ejemplo, se utilizan el SNIP de ADC en las interfaces 1/1: 10.0.1.4 y 10.0.1.5, y el ASN: 400 y 500, mientras se agrega el par.



3. Agregue dos instancias NetScaler VPX para la configuración de alta disponibilidad.

Siga estos pasos:

- a) Implemente dos instancias VPX (instancias principal y secundaria) en Azure.
 - b) Agregue NIC de cliente y servidor en ambas instancias.
 - c) Configure la configuración de HA en ambas instancias mediante la GUI de NetScaler.
4. Configure la redirección dinámica en la instancia de ADC principal.

Configuración de ejemplo:

```
1  enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
2  enable ns feature LB BGP
3  add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -
   dynamicRouting ENABLED
4  VTYSH
5  configure terminal
6  router BGP 400
7  timers bgp 1 3
8  neighbor 10.0.3.4 remote-as 65515
9  neighbor 10.0.3.4 advertisement-interval 3
10 neighbor 10.0.3.4 fall-over bfd
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. Configure la redirección dinámica en la instancia de ADC secundaria.

Configuración de ejemplo:

```
1  enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
2  enable ns feature LB BGP
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
7  timers bgp 1 3
8  neighbor 10.0.3.4 remote-as 65515
9  neighbor 10.0.3.4 advertisement-interval 3
10 neighbor 10.0.3.4 fall-over bfd
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. Verifique los pares de BGP establecidos mediante los comandos BGP en la interfaz de shell de

VTY. Para obtener más información, consulte [Verificación de la configuración de BGP](#).

```
1 show ip bgp neighbors
```

7. Configure el servidor virtual LB en la instancia de ADC principal.

Configuración de ejemplo:

```
1 add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute
  ENABLED
2 add lbserver v1 HTTP 172.16.1.1 80
3 add service s1 10.0.2.6 HTTP 80
4 bind lbserver v1 s1
5 enable ns feature lb
```

Un cliente en la misma red virtual que la instancia NetScaler VPX ahora puede acceder al servidor virtual LB. En este caso, la instancia de NetScaler VPX anuncia la ruta VIP al servidor de rutas de Azure.

Agregue el servicio de escalado automático de Azure de back-end

October 17, 2024

El alojamiento eficiente de aplicaciones en una nube implica una gestión fácil y rentable de los recursos en función de la demanda de la aplicación. Para satisfacer la creciente demanda, debe ampliar los recursos de red. Ya sea que la demanda disminuya, debe reducir la escala para evitar el coste innecesario de los recursos inactivos. Para minimizar el coste de ejecutar la aplicación, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, y así sucesivamente. Sin embargo, la supervisión manual del tráfico es engorrosa. Para que el entorno de aplicaciones se escale hacia arriba o hacia abajo de forma dinámica, debe automatizar los procesos de supervisión del tráfico y escalar los recursos hacia arriba y hacia abajo siempre que sea necesario.

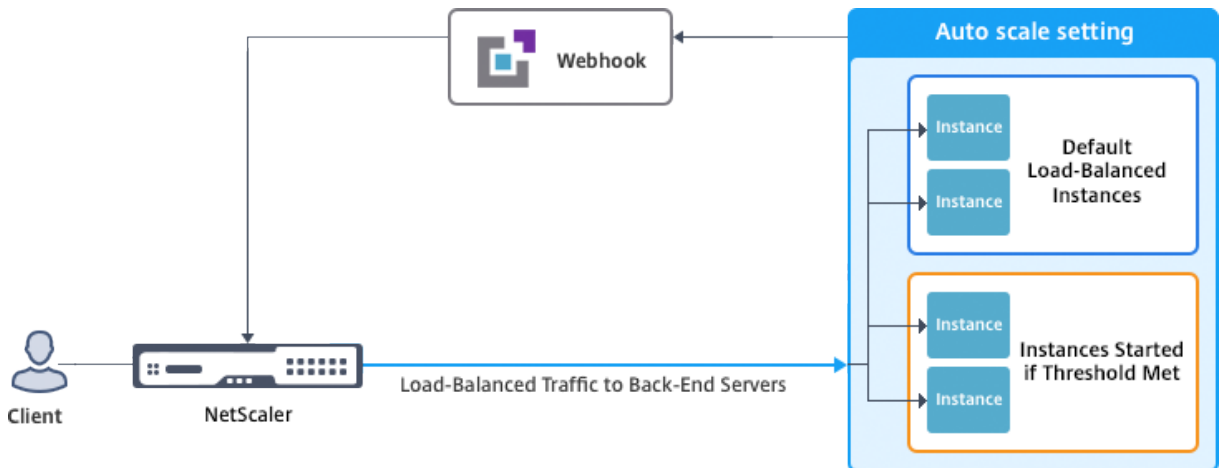
Puede utilizar Autoscale con conjuntos de básculas de máquinas virtuales (VMSS) de Azure para la implementación de alta disponibilidad y autónoma de VPX Multi-IP en Azure.

Integrada con la función Azure VMSS y Autoscale, la instancia de NetScaler VPX ofrece las siguientes ventajas:

- **Equilibrio y administración de la carga** : configura automáticamente los servidores para ampliarlos o reducirlos, según la demanda. La instancia de NetScaler VPX detecta automáticamente la configuración de escalabilidad automática de VMSS en la misma red virtual en la que se implementa la instancia VPX o las redes virtuales interconectadas que están en la misma suscripción de Azure. Puede seleccionar la configuración de escalabilidad automática de VMSS para equili-

brar la carga. Esto se hace mediante la configuración automática de la dirección IP virtual y la dirección IP de subred de NetScaler en la instancia VPX.

- Alta disponibilidad: Detecta grupos de escalabilidad automática y servidores de equilibrio de carga.
- Mejor disponibilidad de red: La instancia VPX admite servidores back-end en diferentes redes virtuales (VNEs).



Para obtener más información, consulte el siguiente tema de Azure

- [Documentación de conjuntos de escalas de máquinas virtuales](#)
- [Descripción general de la escalabilidad automática en máquinas virtuales Microsoft Azure, servicios en la nube y aplicaciones web](#)

Antes de comenzar

- Lea las pautas de uso relacionadas con Azure. Para obtener más información, consulte [Implementar una instancia de NetScaler VPX en Microsoft Azure](#).
- Cree una o más instancias de NetScaler VPX con tres interfaces de red en Azure según sus requisitos (implementación independiente o de alta disponibilidad).
- Abra el puerto TCP 9001 en el grupo de seguridad de red de la interfaz 0/1 de la instancia VPX. La instancia VPX usa este puerto para recibir la notificación de escalamiento horizontal y vertical.
- Cree un VMSS de Azure en la misma red virtual en la que se implementa la instancia de NetScaler VPX. Si la instancia de VMSS y NetScaler VPX se implementa en diferentes redes virtuales de Azure, se deben cumplir las siguientes condiciones:
 - Ambas redes virtuales deben estar en la misma suscripción a Azure.
 - Las dos redes virtuales deben estar conectadas mediante la función de emparejamiento de redes virtuales de Azure.

Si no tiene una configuración de VMSS existente, realice las siguientes tareas:

- a) Crear un VMSS
- b) Habilitar escalado automático en VMSS
- c) Cree directivas de escalado hacia adentro y hacia afuera en la configuración de VMSS Autoscale

Para obtener más información, consulte [Descripción general de la escalabilidad automática con conjuntos de básculas de máquinas virtuales de Azure](#).

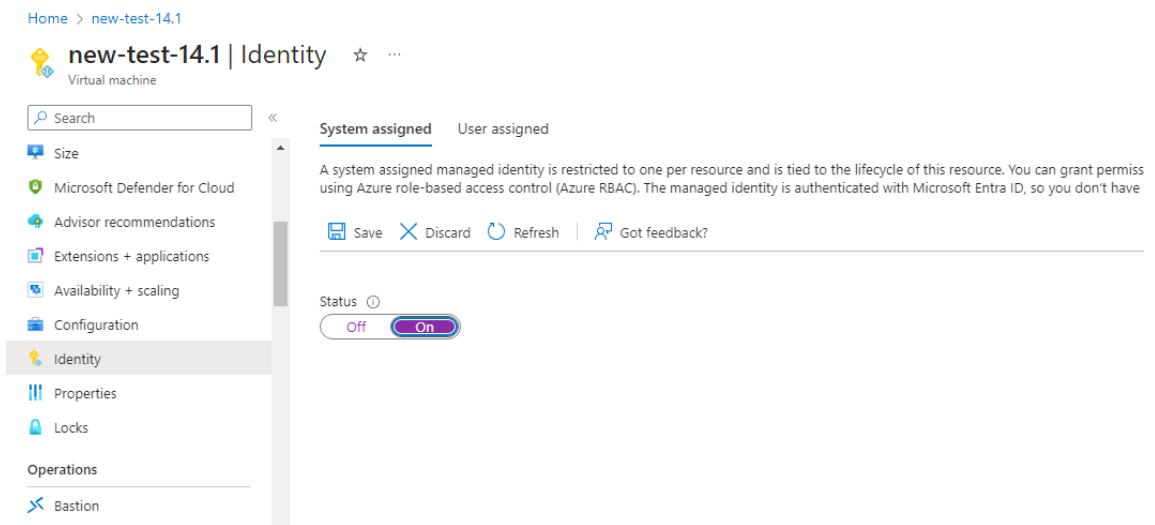
- NetScaler VPX solo admite VMSS con orquestación uniforme. No se admite VMSS con orquestación flexible. Para obtener más información, consulte [Modos de orquestación para conjuntos de escalado de máquinas virtuales en Azure](#).
- A partir de la versión 14.1-12.x de NetScaler, NetScaler VPX admite la identidad administrada en la nube de Azure. Las identidades administradas vinculan un Service Principal a un recurso de Azure, como una máquina virtual. Con la identidad gestionada, no es necesario gestionar las credenciales de la nube (ID de aplicación, secreto de aplicación e ID de arrendatario), evitando así los riesgos de seguridad. Actualmente, NetScaler VPX solo admite la identidad administrada asignada por el sistema y la asignada por un solo usuario. No se admite la identidad administrada asignada por varios usuarios.

Para las versiones de NetScaler anteriores a la 14.1-12.x, debe administrar manualmente las credenciales de nube en NetScaler VPX a través de Azure Active Directory (AAD). Asigne una función de colaborador a la aplicación de AAD recién creada. Las credenciales de la nube se deben volver a crear periódicamente una vez que caduquen. Para obtener más información, consulte [Crear una aplicación y un servicio principal de Azure Active Directory](#).

Al configurar la identidad administrada en la consola de Azure y las credenciales de nube en NetScaler, la identidad administrada tiene prioridad sobre las credenciales de nube.

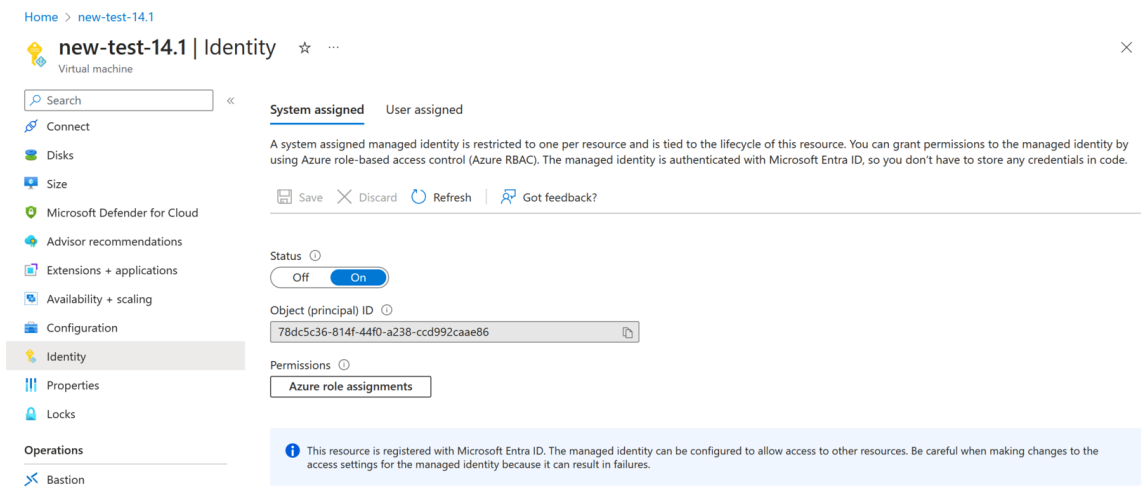
Configurar una identidad administrada en una máquina virtual

1. Inicie sesión en Azure Portal.
2. Navegue hasta la máquina virtual y seleccione **Identidad**.
3. Elija Asignado por **el sistema o Asignado por el usuario** en función de sus requisitos.
4. En **Estado**, seleccione **Activado** y, a continuación, haga clic en **Guardar**.



Una vez guardado el estado, verá que se crea un objeto principal de servicio y se asigna a la máquina virtual.

5. Haga clic en **Asignaciones de funciones de Azure**.



6. En la ventana **Agregar asignación de funciones**, seleccione un ámbito. Puede seleccionar una de las siguientes opciones:

- Subscription
 - Si el VMSS y la VM están en grupos de recursos diferentes, utilice la **suscripción** como ámbito.
- Resource group
 - Si el VMSS está en el mismo grupo de recursos que la máquina virtual, utilice el **grupo de recursos** como ámbito.
- Caja fuerte de llaves

- Almacenamiento
- SQL

En función de su selección de osciloscopios, complete los detalles de los demás campos. Asigne una función de **colaborador** y **guarde** la configuración.

Home > new-test-14.1 | Identity >

Azure role assignments

+ Add role assignment (Preview) Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *

Role Resource Name

No role assignments found for the selected subscription.

Add role assignment (Preview)

Scope

Subscription

Resource group

Role

[Learn more about RBAC](#)

Save Discard

La página de **asignaciones de funciones de Azure** muestra la identidad administrada que creó.

Home > new-test-14.1 | Identity >

Azure role assignments

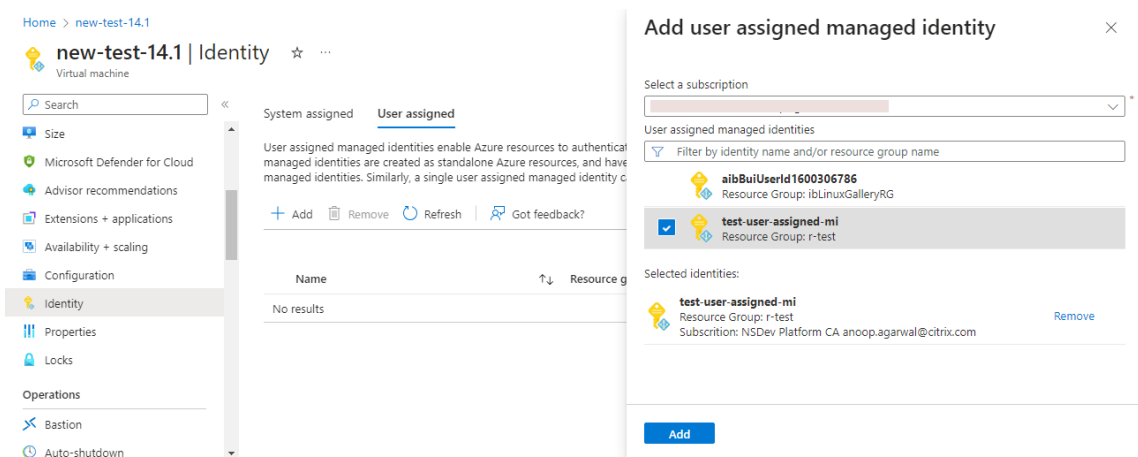
+ Add role assignment (Preview) Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	tahaj-test-ipconfig	Resource Group	new-test-14.1	None

7. Para crear una identidad administrada asignada al usuario, seleccione una suscripción, elija una identidad administrada asignada al usuario y haga clic en **Agregar**.



Agregar VMSS a una instancia de NetScaler VPX

Complete los siguientes pasos para agregar la configuración de escalabilidad automática a la instancia VPX:

1. Inicie sesión en la instancia de VPX.
2. Vaya a **Configuración > Azure > Establecer credenciales**. Agregue las credenciales de Azure necesarias para que funcione la función de escalado automático.

← Set Credentials

Tenant ID

Application ID

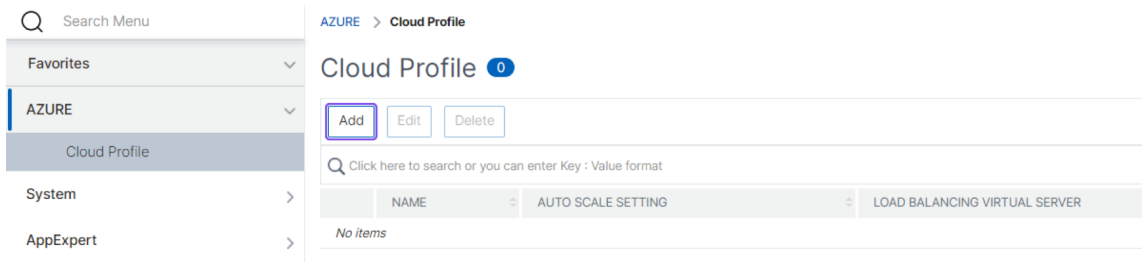
Application Secret

OK **Cancel**

Nota:

Si usa la identidad administrada de Azure, no es necesario establecer credenciales.

3. Vaya a **Sistema > Azure > Perfil de nube** y haga clic en **Agregar** para crear un perfil de nube.



Aparece la página **de configuración de Crear perfil en la nube** .

← Create Cloud Profile

Name	<input type="text" value="_CloudProfile_"/>
Virtual Server IP Address*	<input type="text" value="10.0.1.4"/>
Type	<input type="text" value="AUTOSCALE"/>
Load Balancing Server Protocol	<input type="text" value="HTTP"/>
Load Balancing Server Port	<input type="text" value="80"/>
Auto Scale Setting*	<input type="text"/>
Auto Scale Setting Protocol	<input type="text" value="HTTP"/>
Auto Scale Setting Port	<input type="text" value="80"/>

El perfil de nube crea un servidor virtual de equilibrio de carga de NetScaler y un grupo de servicios con miembros (servidores) como servidores del grupo de Auto Scaling. Los servidores back-end deben ser accesibles a través del SNIP configurado en la instancia VPX.

Puntos a tener en cuenta al crear un perfil de nube

- La dirección IP del servidor virtual se rellena automáticamente desde la dirección IP libre disponible para la instancia VPX. Para obtener más información, consulte [Asignación de varias direcciones IP a máquinas virtuales mediante el portal de Azure](#).
- La configuración de escalado automático se rellena previamente desde la instancia de VMSS que está conectada a la instancia de NetScaler VPX en la misma red virtual o en redes virtuales interconectadas. Para obtener más información, consulte [Descripción general de la escalabilidad automática con conjuntos de básculas de máquinas virtuales de Azure](#).
- Al seleccionar el **protocolo de configuración de escalado automático y el puerto de configuración de escalado automático**, asegúrese de que los servidores escuchen los protocolos y puertos y de vincular el monitor correcto al grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- Para el escalado automático del tipo de protocolo SSL, después de crear el perfil de nube, el servidor virtual o grupo de servicios de equilibrio de carga está inactivo debido a la falta de un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.

Nota:

A partir de la versión 13.1-42.x de NetScaler, puede crear diferentes perfiles de nube para diferentes servicios (con diferentes puertos) con el mismo VMSS en Azure. Por lo tanto, la instancia de NetScaler VPX admite varios servicios con el mismo grupo de escalado automático en la nube pública.

Para ver la información relacionada con el escalado automático en el portal de Azure, vaya a **Conjuntos de escalado de máquinas virtuales** y seleccione **Conjunto de escalado de máquinas virtuales > Escalado**.

Referencias

Para obtener información sobre el escalado automático de NetScaler VPX en Microsoft Azure mediante NetScaler Application Delivery and Management, consulte [Escalado automático de Azure mediante NetScaler ADM](#).

Etiquetas de Azure para la implementación de NetScaler VPX

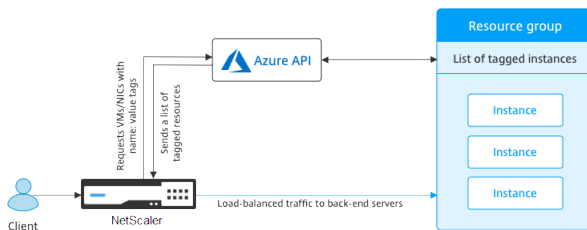
October 17, 2024

En el portal en la nube de Azure, puede etiquetar recursos con un nombre: par de valores (como Dept: Finance) para categorizar y ver los recursos de todos los grupos de recursos y, dentro del portal, entre suscripciones. El etiquetado es útil cuando necesita organizar los recursos para la facturación, la administración o la automatización.

Cómo funciona la etiqueta de Azure para la implementación de VPX















Para las instancias independientes y de alta disponibilidad de NetScaler VPX implementadas en Azure Cloud, ahora puede crear grupos de servicios de equilibrio de carga asociados a una etiqueta de Azure. La instancia VPX supervisa constantemente las máquinas virtuales de Azure (servidores back-end) y las interfaces de red (NIC), o ambas, con la etiqueta respectiva y actualiza el grupo de servicios en consecuencia.

La instancia VPX crea el grupo de servicios que equilibra la carga de los servidores back-end mediante etiquetas. La instancia consulta en la API de Azure todos los recursos que están etiquetados con un nombre de etiqueta y un valor de etiqueta determinados. Según el período de sondeo asignado (60 segundos por defecto), la instancia VPX sondea periódicamente la API de Azure y recupera los recursos disponibles con el nombre de la etiqueta y los valores de etiqueta asignados en la GUI de VPX. Siempre que se agrega o elimina una máquina virtual o NIC con la etiqueta correspondiente, el ADC detecta el cambio respectivo y agrega o elimina automáticamente la dirección IP de la máquina virtual o NIC del grupo de servicios.



Antes de comenzar

Antes de crear grupos de servicios de equilibrio de carga de NetScaler, agregue una etiqueta a los servidores de Azure. Puede asignar la etiqueta a la máquina virtual o a la NIC.

Name 	Value 	
Creator	: d34eed9579934591afbbdf28c92caf51	 
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 next run of no_auto_script if no view/update lease datetime. only valid if no_auto_shutdown tag set to 'true'. max	 
info_no_auto_shutdown_lease_datetime_UTC	: 14 days lease is allowed. all generic date/time strings are valid (ex: 'Tue Jun 20	 
no_auto_shutdown	: false	 
no_auto_shutdown_lease_datetime_UTC	:	 
tag1	: false	 
	:	

Para obtener más información sobre cómo agregar etiquetas de Azure, consulte el documento de Microsoft [Utilizar etiquetas para organizar los recursos de Azure](#).

Nota:

Los comandos CLI de ADC para agregar configuraciones de etiquetas de Azure admiten nombres de etiquetas y valores de etiquetas que comienzan solo con números o letras y no con otros caracteres del teclado.

Cómo agregar la configuración de etiquetas de Azure mediante la GUI de VPX

Puede agregar el perfil de nube de etiquetas de Azure a una instancia VPX mediante la GUI de VPX para que la instancia pueda equilibrar la carga de los servidores de fondo mediante la etiqueta especificada. Siga estos pasos:

1. Desde la GUI de VPX, vaya a **Configuración > Azure > Perfil de nube**.
2. Haga clic en Agregar para crear un perfil en la nube. Se abre la ventana del perfil en la nube.

Create Cloud Profile

Name

Virtual Server IP Address*

Type

Azure Tag Name

Azure Tag Value

Azure Poll Periods

Load Balancing Server Protocol

Load Balancing Server Port

Azure Tag Setting*

Azure Tag Setting Protocol

Azure Tag Setting Port

1. Introduzca valores para los siguientes campos:

- Nombre: Añade un nombre para su perfil
- Dirección IP del servidor virtual: La dirección IP del servidor virtual se rellena automáticamente desde la dirección IP libre disponible para la instancia VPX. Para obtener más información, consulte [Asignación de varias direcciones IP a máquinas virtuales mediante el portal de Azure](#).
- Tipo: En el menú, seleccione AZURETAGS.
- Nombre de etiqueta de Azure: Introduzca el nombre que ha asignado a las máquinas virtuales o NIC en el portal de Azure.
- Valor de etiqueta de Azure: Especifique el valor que ha asignado a las máquinas virtuales o NIC en Azure Portal.
- Periodos de sondeo de Azure: de forma predeterminada, el período de sondeo es de 60 segundos, que es el valor mínimo. Puede cambiarlo según sus necesidades.
- Protocolo del servidor de equilibrio de carga: seleccione el protocolo que escucha el balanceador de carga.
- Puerto del servidor de equilibrio de carga: seleccione el puerto en el que escucha el balanceador de carga.
- Configuración de etiquetas de Azure: el nombre del grupo de servicios que se creará para este perfil de nube.
- Protocolo de configuración de etiquetas de Azure: seleccione el protocolo que escuchan sus servidores de fondo.
- Puerto de configuración de etiquetas de Azure: seleccione el puerto que escuchan sus servidores de fondo.

2. Haga clic en **Create**.

Se crean un servidor virtual con balanceador de carga y un grupo de servicios para las máquinas virtuales o NIC etiquetadas. Para ver el servidor virtual del balanceador de carga, desde la GUI de VPX, vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

Cómo agregar la configuración de etiquetas de Azure mediante la CLI VPX

Escriba el siguiente comando en la CLI de NetScaler para crear un perfil en la nube para las etiquetas de 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 -vsrvbindsvcport 80 -azureTagName `<Azure tag specified on Azure portal>` -azureTagValue `<Azure value specified on the Azure portal>` -azurePollPeriod 60
```

Importante:

Debe guardar todas las configuraciones; de lo contrario, las configuraciones se perderán después de reiniciar la instancia. Escriba `save config`.

Ejemplo 1: Este es un comando de ejemplo para un perfil en la nube para el tráfico HTTP de todas las máquinas virtuales y NIC de Azure etiquetadas con el par “myTagName/myTagValue”:

```
1 add cloud profile MyTagCloudProfile -type azuretags -vServerName
  MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
  serviceName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
  -vsrvbindsvcport 80 -azureTagName myTagName -azureTagValue
  myTagValue -azurePollPeriod 60
2 Done
```

Para mostrar el perfil de nube, escriba `show cloudprofile`.

Ejemplo 2: El siguiente comando CLI imprime información sobre el perfil de nube recién agregado en el ejemplo 1.

```
1 show cloudprofile
2 1) Name: MyTagCloudProfile Type: azuretags VServerName:
  MyTagVServer ServiceType: HTTP IPAddress: 52.178.209.133
  Port: 80 ServiceGroupName: MyTagsServiceGroup
  BoundServiceGroupSvcType: HTTP
3 Vsvrbindsvcport: 80 AzureTagName: myTagName AzureTagValue
  : myTagValue AzurePollPeriod: 60 GraceFul: NO
  Delay: 60
```

Para eliminar un perfil de nube, escriba `rm cloud profile <cloud profile name>`;

Ejemplo 3: el siguiente comando quita el perfil de nube creado en el ejemplo 1.

```
1 > rm cloudprofile MyTagCloudProfile
2 Done
```

Solución de problemas

Problema: En casos muy raros, es posible que el comando de la CLI “rm cloud profile” no elimine el grupo de servicios y los servidores asociados con el perfil de nube eliminado. Esto sucede cuando el comando se emite segundos antes de que transcurra el período de sondeo del perfil de nube que se está eliminando.

Solución: elimine manualmente los grupos de servicios restantes introduciendo el siguiente comando de CLI para cada uno de los grupos de servicios restantes:

```
1 #> rm servicegroup <serviceName>
```

Elimine también cada uno de los servidores restantes introduciendo el siguiente comando CLI para cada uno de los servidores restantes:

```
1 #> rm server <name>
```

Problema: Si agrega una configuración de etiqueta de Azure a una instancia VPX mediante la CLI, el proceso `rain_tags` continúa ejecutándose en un nodo de par HA tras un reinicio en caliente.

Solución: Termine manualmente el proceso en el nodo secundario después de un reinicio en caliente. Desde la CLI del nodo de alta disponibilidad secundario, salga al símbolo del shell:

```
1 #> shell
```

Utilice el siguiente comando para eliminar el proceso `rain_tags`:

```
1 # PID=`ps -aux | grep rain_tags | awk '{
2 print $2 }
3 `; kill -9 $PID
```

Problema: Es posible que la instancia VPX no pueda acceder a los servidores back-end y que la instancia VPX los informe como DOWN, a pesar de estar en buen estado. **Solución:** Asegúrese de que la instancia VPX puede alcanzar la dirección IP etiquetada correspondiente al servidor back-end. Para una NIC etiquetada, ésta es la dirección IP de la NIC; mientras que para una VM etiquetada, ésta es la dirección IP principal de la VM. Si la VM/NIC reside en otra Azure VNet diferente, asegúrese de que el peering de VNet esté habilitado.

Configurar GSLB en instancias de NetScaler VPX

October 17, 2024

Los dispositivos NetScaler configurados para el equilibrio de carga global del servidor (GSLB) proporcionan recuperación ante desastres y disponibilidad continua de las aplicaciones al protegerse contra los puntos de falla en una WAN. GSLB puede equilibrar la carga entre los centros de datos dirigiendo las solicitudes de los clientes al centro de datos más cercano o de mejor rendimiento, o a centros de datos sobrevivientes si se produce una interrupción.

En esta sección se describe cómo habilitar GSLB en instancias VPX en dos sitios en un entorno de Microsoft Azure, mediante comandos de Windows PowerShell.

Nota:

Para obtener más información sobre GSLB, consulte [Equilibrio de carga global del servidor](#).

Puede configurar GSLB en una instancia NetScaler VPX en Azure, en dos pasos:

1. Cree una instancia VPX con varias NIC y varias direcciones IP en cada sitio.
2. Habilite GSLB en las instancias VPX.

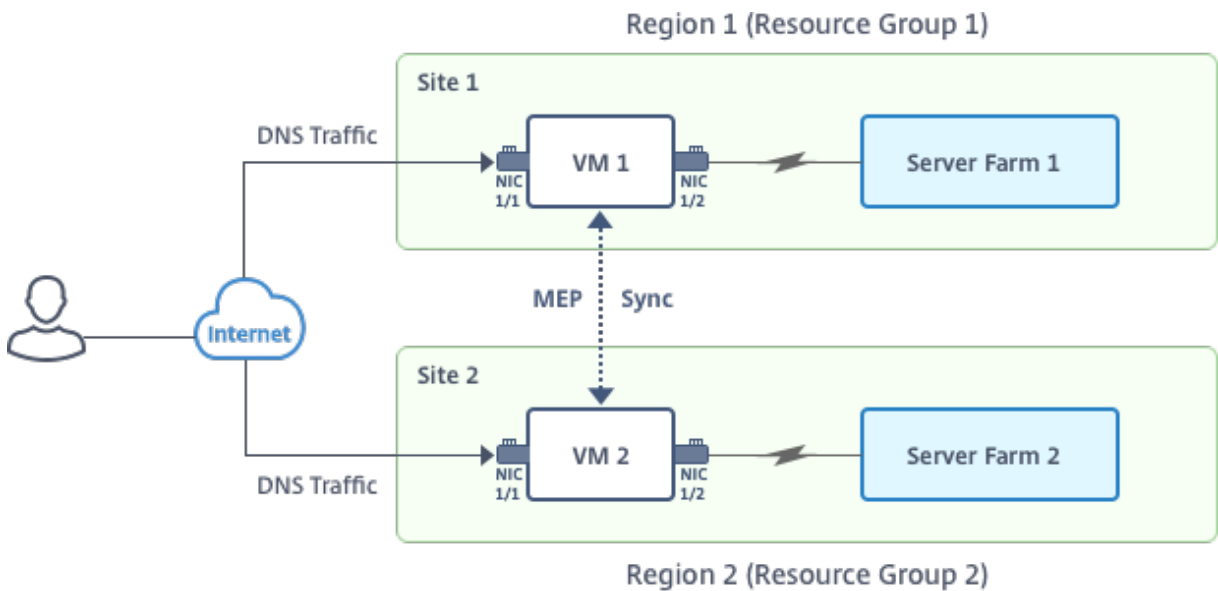
Nota:

Para obtener más información sobre la configuración de varias NIC y direcciones IP, consulte: [Configurar varias direcciones IP para una instancia NetScaler VPX en modo independiente mediante comandos de PowerShell.](#)

Caso

Este caso incluye dos sitios: el sitio 1 y el sitio 2. Cada sitio tiene una máquina virtual (VM1 y VM2) configurada con varias NIC, varias direcciones IP y GSLB.

Figura . Configuración de GSLB implementada en dos sitios: Sitio 1 y Sitio 2.



En este caso, cada VM tiene tres NIC: NIC 0/1, 1/1 y 1/2. Cada NIC puede tener varias direcciones IP públicas y privadas. Las NIC se configuran para los siguientes fines.

- NIC 0/1: para dar servicio al tráfico de administración
- NIC 1/1: para atender el tráfico del lado del cliente
- NIC 1/2: Para comunicarse con servidores back-end

Para obtener información sobre las direcciones IP configuradas en cada NIC en este caso, consulte la sección Detalles de configuración IP.

Parámetros

A continuación se presentan parámetros de ejemplo de configuración para este caso en este documento. Puede usar diferentes configuraciones si lo quiere.

```
1  $location="West Central US"
2
3  $vnetName="NSVPX-vnet"
4
5  $RGName="multiIP-RG"
6
7  $prmStorageAccountName="multiipstorageacctnt"
8
9  $avSetName="MultiIP-avset"
10
11 $vmSize="Standard\_DS3\_V2"
```

Nota:

El requisito mínimo para una instancia VPX es 2 vCPU y 2 GB de RAM.

```
1  $publisher="citrix"
2
3  $offer="netscalervpx111"
4
5  $sku="netscalerbyol"
6
7  $version="latest"
8
9  $vmNamePrefix="MultiIPVPX"
10
11 $nicNamePrefix="MultiipVPX"
12
13 $osDiskSuffix="osdiskdb"
14
15 $numberOfVMs=1
16
17 $ipAddressPrefix="10.0.0."
18
19 $ipAddressPrefix1="10.0.1."
20
21 $ipAddressPrefix2="10.0.2."
22
23 $pubIPName1="MultiIP-pip1"
24
25 $pubIPName2="MultiIP-pip2"
26
27 $IPConfigName1="IPConfig1"
28
29 $IPConfigName2="IPConfig-2"
30
31 $IPConfigName3="IPConfig-3"
```

```
32
33     $IPConfigName4="IPConfig-4"
34
35     $frontendSubnetName="default"
36
37     $backendSubnetName1="subnet\_1"
38
39     $backendSubnetName2="subnet\_2"
40
41     $suffixNumber=10
```

Crear una VM

Siga los pasos del 1 al 10 para crear VM1 con varias NIC y varias direcciones IP, mediante comandos de PowerShell:

1. [Crear grupo de recursos](#)
2. [Crear cuenta de almacenamiento](#)
3. [Crear conjunto de disponibilidad](#)
4. [Crear red virtual](#)
5. [Crear dirección IP pública](#)
6. [Crear NIC](#)
7. [Crear objeto de configuración de máquina virtual](#)
8. [Obtenga las credenciales y defina las propiedades del sistema operativo para la máquina virtual](#)
9. [Agregar NIC](#)
10. [Especificar el disco del sistema operativo y crear VM](#)

Después de completar todos los pasos y comandos para crear la VM1, repita estos pasos para crear la VM2 con parámetros específicos.

Crear grupo de recursos

```
1 New-AzureRMResourceGroup -Name $RGName -Location $location
```

Crear cuenta de almacenamiento

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

Crear conjunto de disponibilidad

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

Crear red virtual

1. Agregue subredes.

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

2. Agregue un objeto de red virtual.

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

3. Recupera subredes.

```
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 }
```

Crear dirección IP pública

```
1 $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName  
   $RGName -Location $location -AllocationMethod Dynamic  
2 $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName  
   $RGName -Location $location -AllocationMethod Dynamic
```

Crear NIC

Crear NIC 0/1

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

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

Crear NIC 1/1

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

Crear NIC 1/2

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

Crear objeto de configuración de máquina virtual

```
1 $vmName=$vmNamePrefix
2 $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
  AvailabilitySetId $avSet.Id
```

Obtenga credenciales y configure las propiedades del sistema operativo

```
1 $cred=Get-Credential -Message "Type the name and password for VPX
  login."
2 $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
  ComputerName $vmName -Credential $cred
3 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
  $publisher -Offer $offer -Skus $sku -Version $version
```

Agregar NIC

```

1 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
  Primary
2 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
3 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id

```

Especificar el disco del sistema operativo y crear VM

```

1 $osDiskName=$vmName + "-" + $osDiskSuffix
2 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
  /" + $osDiskName + ".vhd"
3 $vmConfig=Set-AzureRMVMOsdisk -VM $vmConfig -Name $osDiskName -VhdUri
  $osVhdUri -CreateOption fromImage
4 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
  -Name $sku
5 New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
  $location

```

Nota:
 Repita los pasos 1 a 10 enumerados en “Crear máquinas virtuales multiNIC mediante comandos de PowerShell” para crear VM2 con parámetros específicos de VM2.

Detalles de configuración IP

Se utilizan las siguientes direcciones IP.

Tabla 1. Direcciones IP utilizadas en VM1

NIC	IP privada	IP pública (PIP)	Descripción
0/1	10.0.0.10	PIP1	Configurado como NSIP (IP de administración)
1/1	10.0.1.10	PIP2	Configurado como IP del sitio SNIP/GSLB
-	10.0.1.11	-	Configurado como IP del servidor LB. La IP pública no es obligatoria

NIC	IP privada	IP pública (PIP)	Descripción
1/2	10.0.2.10	-	Configurado como SNIP para enviar sondeos de monitor a servicios; IP pública no es obligatoria

Tabla 2. Direcciones IP utilizadas en VM2

NIC	IP interna	IP pública (PIP)	Descripción
0/1	20.0.0.10	PIP4	Configurado como NSIP (IP de administración)
1/1	20.0.1.10	PIP5	Configurado como IP del sitio SNIP/GSLB
-	20.0.1.11	-	Configurado como IP del servidor LB. La IP pública no es obligatoria
1/2	20.0.2.10	-	Configurado como SNIP para enviar sondeos de monitor a servicios; IP pública no es obligatoria

A continuación se muestran configuraciones de ejemplo para este caso, que muestran las direcciones IP y las configuraciones LB iniciales creadas a través de la CLI de NetScaler VPX para VM1 y VM2.

He aquí un ejemplo de configuración en 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]
```

He aquí un ejemplo de configuración en 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]
```

Configurar sitios GSLB y otros parámetros

Realice las tareas que se describen en el tema siguiente para configurar los dos sitios GSLB y otros parámetros necesarios:

Global Server Load Balancing

He aquí un ejemplo de configuración GSLB en VM1 y VM2.

```
1 enable ns feature LB GSLB
2 add gslb site site1 10.0.1.10 -publicIP PIP2
3 add gslb site site2 20.0.1.10 -publicIP PIP5
4 add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
  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
7 bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
8 bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
9 bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Ha configurado GSLB en instancias NetScaler VPX que se ejecutan en Azure.

Recuperación ante desastres

El desastre es una interrupción repentina de las funciones empresariales causada por desastres naturales o eventos causados por seres humanos. Los desastres afectan a las operaciones del centro de datos, después de lo cual los recursos y los datos perdidos en el sitio del desastre deben reconstruirse y restaurarse por completo. La pérdida de datos o el tiempo de inactividad en el centro de datos es fundamental y colapsa la continuidad del negocio.

Uno de los desafíos a los que se enfrentan los clientes hoy en día es decidir dónde colocar su sitio de recuperación ante desastres. Las empresas buscan uniformidad y rendimiento independientemente de cualquier falla de red o infraestructura subyacente.

Las posibles razones por las que muchas organizaciones deciden migrar a la nube son:

- Tener un centro de datos local es muy caro. Al utilizar la nube, las empresas pueden liberar tiempo y recursos para expandir sus propios sistemas.

- Muchas de las orquestaciones automatizadas permiten una recuperación más rápida
- Replica los datos proporcionando protección de datos continua o instantáneas continuas para protegerte contra cualquier interrupción o ataque.
- Soporta casos de uso en los que los clientes necesitan muchos tipos diferentes de control de cumplimiento y seguridad que ya están presentes en las nubes públicas. Esto hace que sea más fácil lograr el cumplimiento que necesitan en lugar de crear el suyo propio.

Un NetScaler configurado para GSLB reenvía el tráfico al centro de datos menos cargado o de mejor rendimiento. Esta configuración, denominada configuración activa-activa, no solo mejora el rendimiento, sino que también proporciona recuperación ante desastres inmediata al enrutar el tráfico a otros centros de datos si un centro de datos que forma parte de la instalación falla. Por lo tanto, NetScaler ahorra a los clientes tiempo y dinero valiosos.

Implementación de múltiples NIC y múltiples IP (tres NIC) para la recuperación ante desastres

Los clientes podrían implementar mediante la implementación de tres NIC si se implementan en un entorno de producción donde la seguridad, la redundancia, la disponibilidad, la capacidad y la escalabilidad son fundamentales. Con este método de implementación, la complejidad y la facilidad de administración no son preocupaciones críticas para los usuarios.

Implementación de una sola NIC y varias IP (una NIC) para la recuperación ante desastres

Es posible que los clientes implementen mediante una sola NIC si lo están implementando en un entorno que no sea de producción por los siguientes motivos:

- Están configurando el entorno para las pruebas o están preparando un nuevo entorno antes de la implementación en producción.
- Implementación directa en la nube de forma rápida y eficiente.
- Al mismo tiempo, busca la simplicidad de una configuración de subred única.

Configurar GSLB en una configuración de alta disponibilidad activa-en espera

October 17, 2024

Puede configurar el equilibrio de carga del servidor global (GSLB) en la implementación de HA activa-en espera en Azure en tres pasos:

1. Cree un par VPX HA en cada sitio GSLB. Consulte [Configurar una configuración de alta disponibilidad con múltiples direcciones IP y NIC](#) para obtener información sobre cómo crear un par de alta disponibilidad.
2. Configure Azure Load Balancer (ALB) con la dirección IP de front-end y las reglas para permitir el tráfico GSLB y DNS.

Este paso incluye los siguientes pasos secundarios. Consulte el caso de esta sección para ver los comandos de PowerShell que se utilizan para completar estos pasos secundarios.

- a. Cree un front-end `IPconfig` para el sitio GSLB.
- b. Cree un grupo de direcciones back-end con la dirección IP de la NIC 1/1 de los nodos en HA.
- c. Cree reglas de equilibrio de carga para lo siguiente:

```

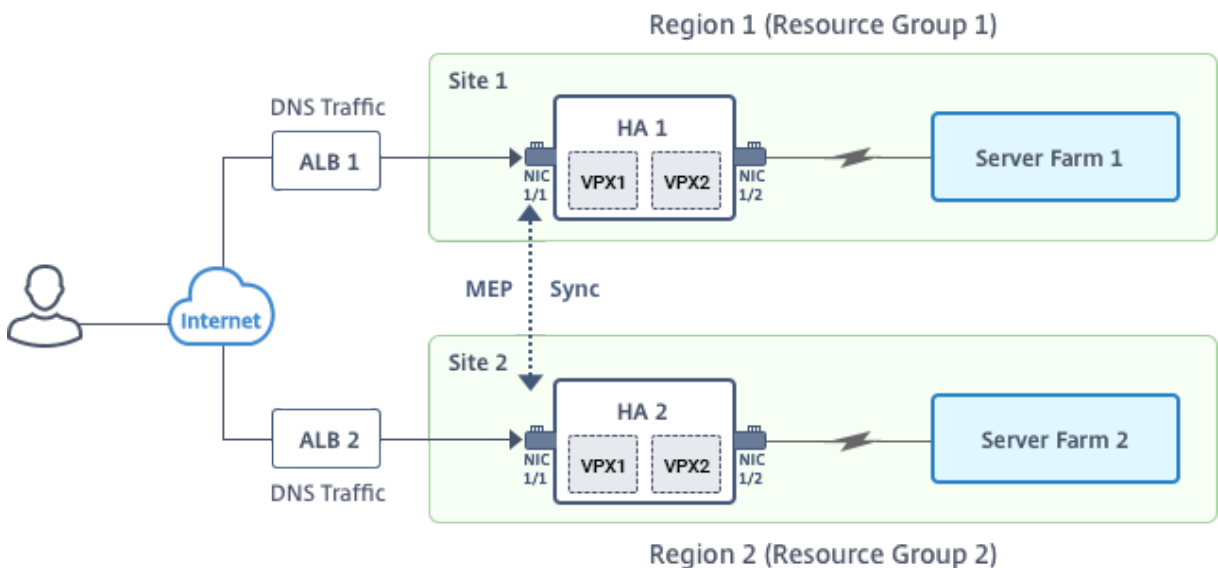
1  TCP/3009 - gslb communication
2  TCP/3008 - gslb communication
3  UDP/53 - DNS communication
    
```

- d. Asocie el grupo de direcciones back-end con las reglas LB creadas en el paso c.
 - e. Actualice el grupo de seguridad de red de la NIC 1/1 de los nodos en ambos pares HA para permitir el tráfico de los puertos TCP 3008, TCP 3009 y UDP 53.
3. Habilite GSLB en cada par HA.

Caso

Este caso incluye dos sitios: el sitio 1 y el sitio 2. Cada sitio tiene un par de HA (HA1 y HA2) configurado con varias NIC, varias direcciones IP y GSLB.

Ilustración: GSLB en la implementación de alta disponibilidad de activos en Azure



En este caso, cada VM tiene tres NIC: NIC 0/1, 1/1 y 1/2. Las NIC se configuran para los siguientes fines.

NIC 0/1: para dar servicio al tráfico de administración

NIC 1/1: para atender el tráfico del lado del cliente

NIC 1/2: Para comunicarse con servidores back-end

Configuración de parámetros

A continuación se presentan ejemplos de configuración de parámetros para ALB. Puede usar diferentes configuraciones si lo quiere.

```
1 $locName="South east Asia"
2
3 $rgName="MultiIP-MultiNIC-RG"
4
5 $pubIPName4="PIPFORGSLB1"
6
7 $domName4="vpxgslbdns"
8
9 $lbName="MultiIPALB"
10
11 $frontEndConfigName2="FrontEndIP2"
12
13 $backendPoolName1="BackendPoolHttp"
14
15 $lbRuleName2="LBRuleGSLB1"
16
17 $lbRuleName3="LBRuleGSLB2"
18
19 $lbRuleName4="LBRuleDNS"
20
21 $healthProbeName="HealthProbe"
```

Configurar ALB con la dirección IP del front-end y las reglas para permitir el tráfico GSLB y DNS

Paso 1. Crear una IP pública para la IP del sitio GSLB

```
1 $pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
   $rgName -DomainNameLabel $domName4 -Location $locName -
   AllocationMethod Dynamic
2
3
4 Get-AzureRmLoadBalancer -Name \$lbName -ResourceGroupName \$rgName |
   Add-AzureRmLoadBalancerFrontendIpConfig -Name \
   $frontEndConfigName2 -PublicIpAddress \$pip4 | Set-
   AzureRmLoadBalancer
```

Paso 2. Paso 2: Cree reglas LB y actualice el ALB existente.

```
1  $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName
2
3
4  $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2
5
6
7  $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1
8
9
10 $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName
11
12
13 \ $alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
    BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP | Set-
    AzureRmLoadBalancer
14
15
16 \ $alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
    BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP | Set-
    AzureRmLoadBalancer
17
18
19 \ $alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName4 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration \
    $frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort
    53 -Probe \$healthprobe -EnableFloatingIP | Set-
    AzureRmLoadBalancer
```

Habilitar GSLB en cada par de alta disponibilidad

Ahora tiene dos direcciones IP de front-end para cada ALB: ALB 1 y ALB 2. Una dirección IP es para el servidor virtual de LB y la otra para la IP del sitio GSLB.

HA 1 tiene las siguientes direcciones IP de front-end:

- FrontEndIPofALB1 (para el servidor virtual de equilibrio de carga)
- PIPFORGSLB1 (IP de GSLB)

HA 2 tiene las siguientes direcciones IP de front-end:

- FrontEndIPofALB2 (para el servidor virtual de equilibrio de carga)
- PIPFORGSLB2 (IP de GSLB)

Los siguientes comandos se utilizan para este caso.

```
1  enable ns feature LB GSLB
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
13 add gslb vserver gslb_http_vip1 HTTP
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
```

Recursos relacionados:

[Configurar GSLB en instancias de NetScaler VPX](#)

[Global Server Load Balancing](#)

Implemente NetScaler GSLB en Azure

October 17, 2024

Con la creciente demanda, las empresas que administran un centro de datos local que atiende a clientes regionales desean escalar e implementar en todo el mundo mediante la nube de Azure. Con NetScaler como administrador de red, puede usar el GSLB StyleBook para configurar aplicaciones tanto locales como en la nube. Puede transferir la misma configuración a la nube con NetScaler ADM. Puede acceder a recursos locales o en la nube según la proximidad con GSLB. Esto le permite tener una experiencia perfecta sin importar en qué parte del mundo se encuentre.

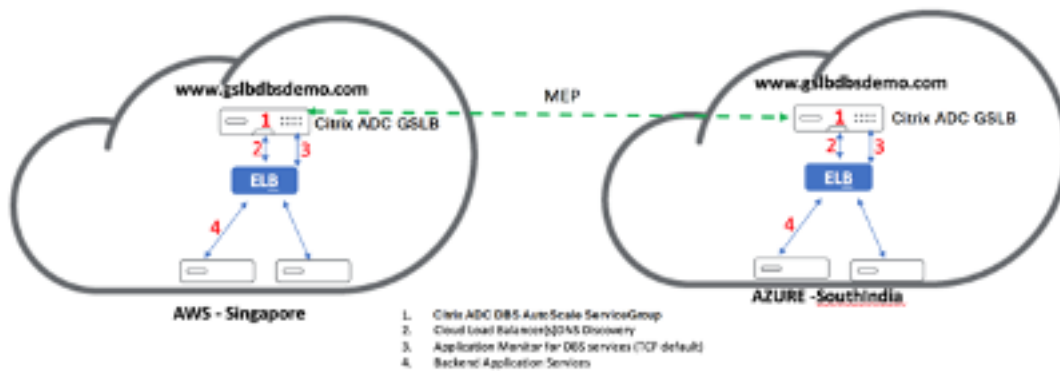
Descripción general de DBS

NetScaler GSLB admite el uso de servicios basados en dominios (DBS) para balanceadores de carga en la nube. Esto permite el descubrimiento automático de servicios en la nube dinámicos mediante una solución de equilibrador de carga en la nube. Esta configuración permite al NetScaler implementar GSLB DBS en un entorno activo-activo. DBS permite escalar los recursos de back-end en entornos de Microsoft Azure a partir del descubrimiento de DNS. En esta sección se describe la integración entre NetScalers en el entorno de Azure Autoscale.

Servicios basados en nombres de dominio que utilizan el balanceador de carga de Azure (ALB)

GSLB DBS utiliza el FQDN del usuario ALB para actualizar dinámicamente los grupos de servicios GSLB a fin de incluir los servidores de fondo que se crean y eliminan en Azure. Para configurar esta función, el usuario dirige el Citrix ADC a su ALB para enrutar dinámicamente a diferentes servidores de Azure. Pueden hacerlo sin tener que actualizar manualmente el Citrix ADC cada vez que se crea y elimina una instancia en Azure. La función Citrix ADC DBS para grupos de servicios GSLB utiliza la detección de servicios compatibles con DNS para determinar los recursos de servicio miembros del espacio de nombres de DBS identificados en el grupo de escalado automático.

La siguiente imagen muestra los componentes de escalabilidad automática de NetScaler GSLB DBS con balanceadores de carga en la nube:



Requisitos previos de Azure GSLB

Los requisitos previos para los grupos de servicios GSLB de NetScaler incluyen un entorno Microsoft Azure funcional con los conocimientos y la capacidad de configurar grupos de seguridad, servidores web Linux, dispositivos NetScaler en AWS, direcciones IP elásticas y balanceadores de carga elásticos (ELB).

- La integración del servicio GSLB DBS requiere la versión 12.0.57 de NetScaler para las instancias del balanceador de carga de Microsoft Azure.

- Entidad del grupo de servicios GSLB: NetScaler versión 12.0.57.
- Se presenta el grupo de servicios GSLB que admite el escalado automático mediante la detección dinámica de DBS.
- Los componentes de funciones de DBS (servicio basado en el dominio) deben estar enlazados al grupo de servicios GSLB.

Ejemplo

```
1  `` `
2
3  > add server sydney_server LB-Sydney-xxxxxxxxx.ap-southeast-2.elb.
    amazonaws.com
4  > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName
    sydney
5  > bind gslb serviceGroup sydney_sg sydney_server 80
6
7  `` `
```

Configurar componentes de Azure

1. Inicie sesión en el usuario Azure Portal y cree una nueva máquina virtual a partir de una plantilla de NetScaler.
2. Cree un equilibrador de carga de Azure.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Create a resource > Marketplace > Load Balancer >

Create load balancer

Overview Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers use a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region *

SKU * Standard
 Gateway
 Basic

Type * Public
 Internal

Tier * Regional
 Global

[Review + create](#) [< Previous](#) [Next : Frontend IP configuration >](#) [Download a template for automation](#) [Give feedback](#)

3. Agregue los grupos de back-end de NetScaler creados.

Home > tahaj-test > ALB

ALB | Backend pools Load balancer

Search + Add Refresh

The backend pool is a critical component of the load balancer. The backend pool defines the group of resources that will serve traffic for a given load-balancing rule. [Learn more.](#)

Backend pool	Resource Name	IP address	Network interface	Availability zone	Rules count	Resource Status
--------------	---------------	------------	-------------------	-------------------	-------------	-----------------

Overview
 Activity log
 Access control (IAM)
 Tags
 Diagnose and solve problems

Settings

Frontend IP configuration
Backend pools
 Health probes
 Load balancing rules
 Inbound NAT rules
 Properties
 Locks

Monitoring

Insights
 Diagnostic settings
 Logs
 Alerts
 Metrics

4. Cree una sonda de estado para el puerto 80.

Cree una regla de equilibrio de carga utilizando la IP de interfaz creada desde el balanceador de

carga.

- Protocolo: TCP
- Puerto de fondo: 80
- Grupo de back-end: NetScaler creado en el paso 1
- Health Probe: creada en el paso 4
- Persistencia de la sesión: ninguna

Microsoft Azure Search resources, services, and docs (G+)

Home > tahaj-test > ALB | Load balancing rules >

Add load balancing rule

ALB

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 *	<input type="text" value="lb_rule2"/>
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Frontend IP address * ⓘ	<input type="text" value="frontend_ip (10.1.0.7)"/>
Backend pool * ⓘ	<input type="text" value="backend_pool"/>
High availability ports ⓘ	<input type="checkbox"/>
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Port *	<input type="text" value="80"/>
Backend port * ⓘ	<input type="text" value="80"/>
Health probe * ⓘ	<input type="text" value="Select an existing probe"/> Create new
Session persistence ⓘ	<input type="text" value="None"/>
Idle timeout (minutes) * ⓘ	<input type="text" value="4"/>
Enable TCP Reset	<input type="checkbox"/>
Enable Floating IP ⓘ	<input type="checkbox"/>

Configurar el servicio basado en el dominio NetScaler GSLB

Las siguientes configuraciones resumen lo que se necesita para habilitar los servicios basados en dominio para el escalado automático de los ADC en un entorno habilitado para GSLB.

- [Configuraciones de administración del tráfico](#)
- [Configuraciones GSLB](#)

Configuraciones de administración del tráfico

Nota:

Es necesario configurar NetScaler con un servidor de nombres o un servidor virtual DNS a través del cual se resuelven los dominios ELB/ALB para los grupos de servicios de DBS. Para obtener más información sobre los servidores de nombres o los servidores virtuales DNS, consulte: [DNS nameServer](#)

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores**.
2. Haga clic en **Agregar** para crear un servidor y proporcione un nombre y un FQDN correspondientes al registro A (nombre de dominio) de Azure para el ALB.

← Create Server

Name*

 ⓘ

IP Address Domain Name

FQDN*

Traffic Domain

 ▼

Translation IP Address

Translation Mask

Resolve Retry (secs)

IPv6 Domain

Enable after Creating

Query Type

 ▼

Comments

3. Repita el paso 2 para agregar la segunda ALB del segundo recurso en Azure.

Configuraciones GSLB

1. Haga clic en **Agregar** para configurar un sitio GSLB.
2. Especifique los detalles para configurar el sitio GSLB

Asigne un nombre al sitio. El tipo se configura como remoto o local en función del NetScaler en el que esté configurando el sitio. La dirección IP del sitio es la dirección IP del sitio GSLB. El sitio GSLB utiliza esta dirección IP para comunicarse con los demás sitios GSLB. La dirección IP pública es necesaria cuando se utiliza un servicio en la nube en el que una dirección IP concreta está alojada en un firewall externo o en un dispositivo NAT. El sitio debe configurarse como sitio principal. Asegúrese de que los **monitores de activación** estén configurados en **SIEMPRE**. Además, asegúrese de marcar las tres casillas de la parte inferior para **Metric Exchange**, **Network Metric Exchange** y **Persistence Session Entry Exchange**.

Le recomendamos que configure el **monitor de activación** en **MEPDOWN**. Para obtener más información, consulte [Configurar un grupo de servicios GSLB](#).

← Create GSLB Site

Name*
 ⓘ

Type
 ⓘ

Site IP Address*
 ⓘ

Public IP Address
 ⓘ

Parent Site Backup Parent Sites

Parent Site Name
 ⓘ

Trigger Monitors*
 ⓘ

Cluster IP

Public Cluster IP

NAPTR Replacement Suffix

Metric Exchange
 Network Metric Exchange
 Persistence Session Entry Exchange

3. Haga clic en **Create**.
4. Vaya a **Administración del tráfico > GSLB > Grupos de servicios**.
5. Haga clic en **Agregar** para agregar un grupo de servicios.
6. Especifique los detalles para configurar el grupo de servicios

Asigne un nombre al grupo de servicios y utilice el protocolo HTTP. En **Nombre del sitio**, elija el sitio respectivo que creó. Debe configurar el modo Autoscale como DNS y marcar las casillas para Supervisión de estado y Estado. Haga clic en **Aceptar** para crear el grupo de servicios.

← GSLB Service Group

Basic Settings

Name*

Protocol*

Site Name*

AutoScale Mode

State
 Health Monitoring

Comment

7. Haga clic en **Miembros del grupo de servicios** y seleccione **Basado en servidores**. Seleccione el ELB correspondiente que se configuró al inicio de la guía de ejecución. Configure el tráfico para que pase por el puerto 80. Haga clic en **Create**.

Create Service Group Member

IP Based Server Based

Select Server*

elb-nvirginia
>

Add

Edit

i

Port*

80

i

Weight

1

Order

Site Prefix

State

Create

Close

El enlace de miembros del grupo de servicios debe incluir 2 instancias que reciba del ELB.

GSLB Servicegroup Member Binding										
IP ADDRESS	SERVER NAME	PORT	WEIGHT	ORDER	HASH ID	STATE	SERVICE STATE	SITE PREFIX		
<input type="checkbox"/>	10.100.234.12	10.100.234.12	80	1	--	ENABLED	UP			
<input type="checkbox"/>	54.252.154.72	elb-nvirginia	80	1	1	--	ENABLED	UP		

8. Repita los pasos 5 y 6 para configurar el grupo de servicios para la segunda ubicación de recursos en Azure. (Esto se puede hacer desde la misma GUI de NetScaler).
9. Para configurar un servidor virtual GSLB. Vaya a **Administración del tráfico > GSLB > Servidores virtuales**.
10. Haga clic en **Agregar** para crear el servidor virtual.
11. Especifique los detalles para configurar el servidor virtual GSLB.

Asigne un nombre al servidor, el Tipo de registro DNS se establece como A, el Tipo de servicio se establece como HTTP y marque las casillas Habilitar después de crear y Registro de AppFlow. Haga clic en **Aceptar** para crear el servidor virtual GSLB.

← GSLB Virtual Server

Basic Settings

Name*
 ⓘ

DNS Record Type*
 ▼

Service Type*
 ▼

Consider Effective State
 ▼ ⓘ

Toggle Order
 ▼ ⓘ

Enable after Creating

Order Threshold

AppFlow Logging

When this Virtual Server is DOWN

Do not send any service's IP address in response (EDR)

When this Virtual Server is UP

Send all "active" service IPs' in response (MIR)

EDNS Client Subnet

Respond with ECS option in the response for a DNS query with ECS

Validate ECS address is a private or unroutable address

Comments

- Una vez creado el servidor virtual GSLB, haga clic en **No GSLB Virtual Server ServiceGroup Binding**.

← GSLB Virtual Server

Basic Settings			
Name	GV2	AppFlow Logging	ENABLED
DNS Record Type	A	EDR	DISABLED
Toggle Order	ASCENDING	MIR	DISABLED
Order Threshold	0	ECS	DISABLED
Service Type	HTTP	ECS Address Validation	DISABLED
Consider Effective State	NONE		
State	● DOWN		

GSLB Services and GSLB Service Group Binding	
No	GSLB Virtual Server to GSLB Service Binding
No	GSLB Virtual Server to GSLB Service Group Binding

OK

- En **ServiceGroup Binding**, utilice **Seleccionar nombre de grupo de servicios** para seleccionar y agregar los grupos de servicios que se crearon en los pasos anteriores.

ServiceGroup Binding

Select Service Group Name*

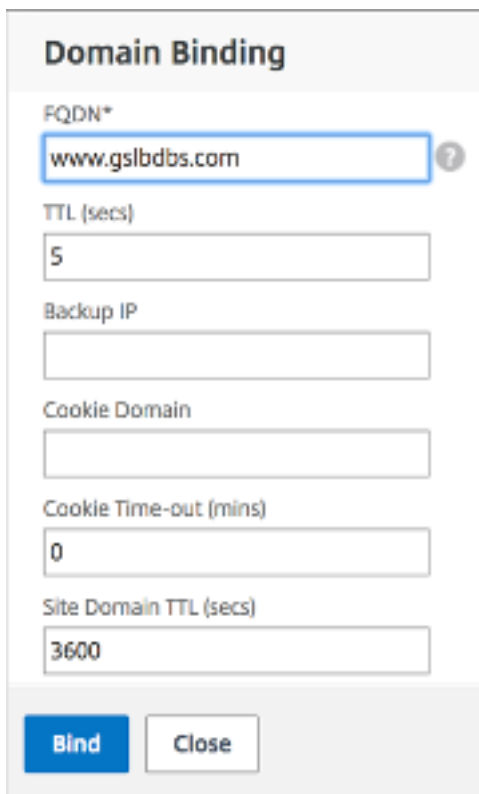
gslb-srv-grp1 > Add Edit ⓘ

Order

1

Bind Close

- Configure el enlace de dominio del servidor virtual GSLB haciendo clic en **Sin enlace de dominio de servidor virtual GSLB**. Configure el FQDN y el enlace. Conserva la configuración por defecto para los demás parámetros.



The screenshot shows a 'Domain Binding' configuration window. It contains several input fields: 'FQDN*' with the value 'www.gslbdfs.com' and a help icon; 'TTL (secs)' with the value '5'; 'Backup IP' (empty); 'Cookie Domain' (empty); 'Cookie Time-out (mins)' with the value '0'; and 'Site Domain TTL (secs)' with the value '3600'. At the bottom, there are two buttons: 'Bind' (highlighted in blue) and 'Close'.

15. Configure el servicio ADNS haciendo clic en **Sin servicio**.
16. Especifique los detalles para configurar el servicio de equilibrio de carga.

Agregue un **nombre de servicio**, haga clic en **Nuevo servidor** introduzca la **dirección IP** del servidor ADNS. Si el ADNS de usuario ya está configurado, los usuarios pueden seleccionar **Servidor existente**, a continuación, elegir el ADNS de usuario en el menú desplegable. Asegúrese de que el protocolo sea ADNS y que el tráfico esté configurado para fluir por el puerto 53.

← Load Balancing Service

Basic Settings

Service Name*

 ⓘ

New Server Existing Server

IP Address*

 ⓘ

Protocol*

 ⌵ ⓘ

Port*

▶ More

17. Configure el **método** como **conexión mínima** y el método de respaldo como **Round Robin**.
18. Haga clic en **Listo** compruebe que el servidor virtual GSLB del usuario aparezca como Activado.



Otros recursos

[Equilibrio de carga global de NetScaler para implementaciones híbridas y multinube](#)

Configurar grupos de direcciones IP de intranet para un dispositivo NetScaler Gateway

October 17, 2024

En algunas situaciones, los usuarios que se conectan con NetScaler Gateway Plug-in necesitan una dirección IP única para un dispositivo NetScaler Gateway. Al habilitar los grupos de direcciones (también conocidos como agrupaciones de IP) para un grupo, el dispositivo NetScaler Gateway puede asignar un alias de dirección IP único a cada usuario. Configurar grupos de direcciones mediante direcciones IP de intranet (IIP).

Puede configurar grupos de direcciones en un dispositivo NetScaler Gateway implementado en Azure siguiendo este procedimiento de dos pasos:

- Registro de las direcciones IP privadas que se utilizan en el grupo de direcciones, en Azure
- Configuración de grupos de direcciones en el dispositivo NetScaler Gateway

Registrar una dirección IP privada en el portal de Azure

En Azure, puede implementar una instancia de NetScaler VPX con varias direcciones IP. Puede agregar direcciones IP a una instancia VPX de dos maneras:

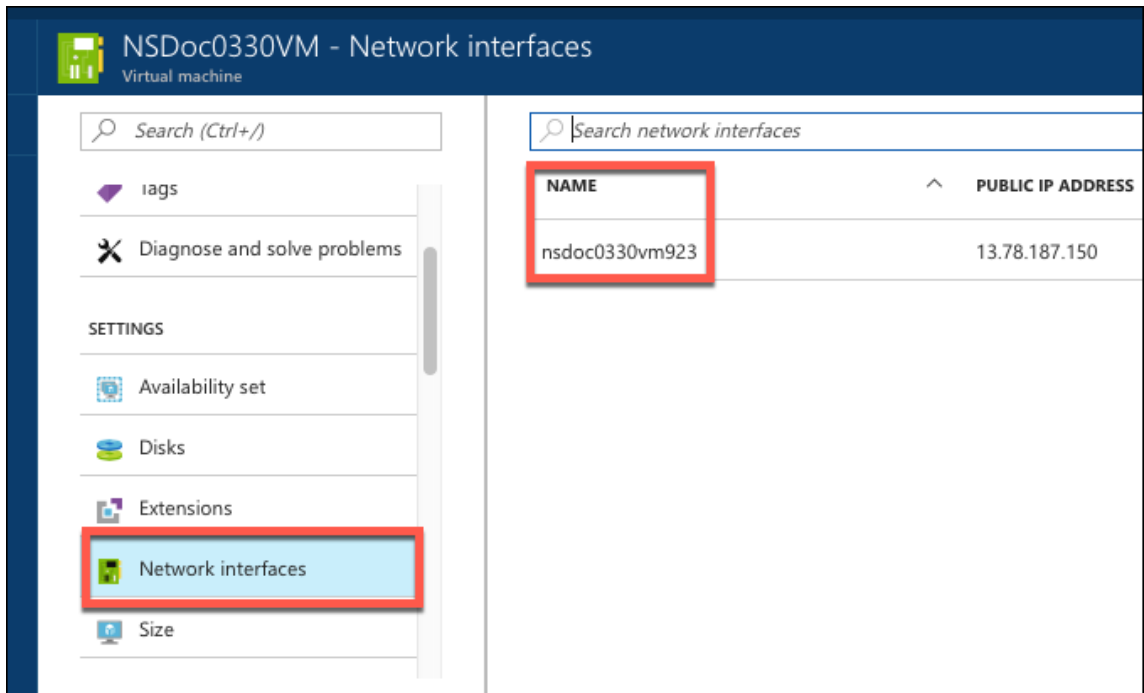
a. Durante el Provisioning de una instancia VPX

Para obtener más información sobre cómo agregar varias direcciones IP al aprovisionar una instancia VPX, consulte [Configurar varias direcciones IP para una instancia independiente de NetScaler](#). Para agregar direcciones IP mediante comandos de PowerShell mientras se aprovisiona una instancia VPX, consulte [Configurar varias direcciones IP para una instancia de NetScaler VPX en modo independiente mediante comandos de PowerShell](#).

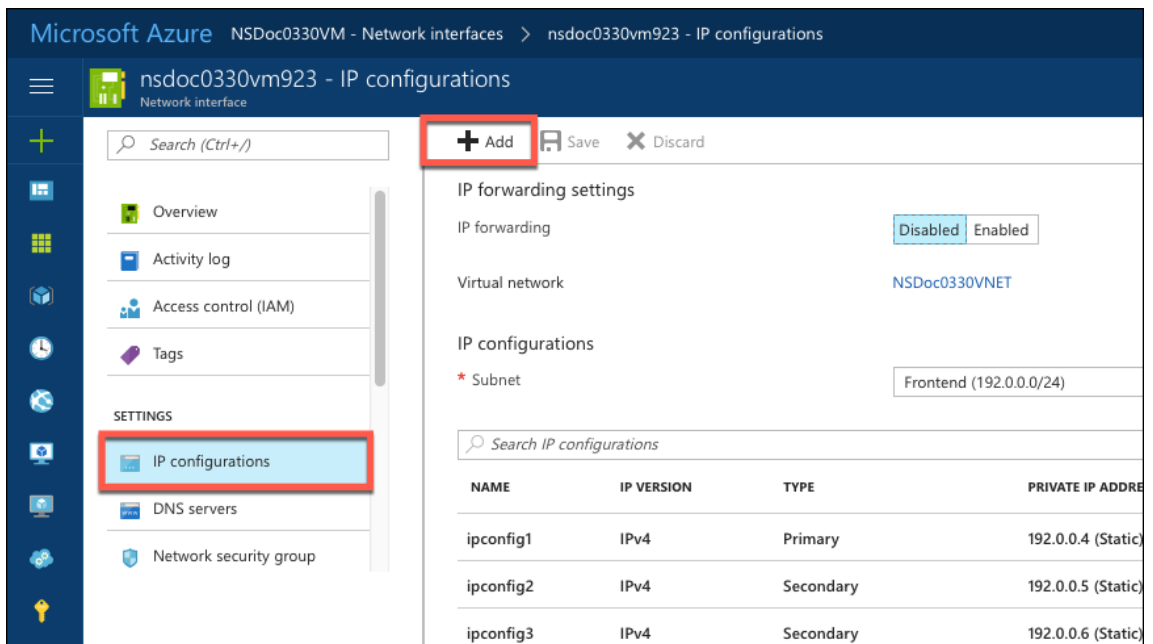
b. Después de Provisioning una instancia VPX

Tras aprovisionar una instancia VPX, siga estos pasos para registrar una dirección IP privada en el portal de Azure, que configurará como un grupo de direcciones en el dispositivo NetScaler Gateway.

1. **Desde Azure Resource Manager (ARM), vaya a la instancia de NetScaler VPX ya creada > Interfaces de red.** Elija la interfaz de red que está enlazada a una subred a la que pertenece el IIP que quiere registrar. Elija la interfaz de red que está enlazada a una subred a la que pertenece el IIP que quiere registrar.



2. Haga clic en **Configuraciones IP** y, a continuación, haga clic en **Agregar**.



3. Proporcione los detalles necesarios como se muestra en el ejemplo siguiente y haga clic en **Aceptar**.

The screenshot shows a window titled "Add IP configuration" for a device named "nsdoc0330vm923". The configuration fields are as follows:

- Name:** PrivateIP5 (with a green checkmark)
- Type:** Primary (disabled), Secondary (selected)
- Message:** Primary IP configuration already exists (with an information icon)
- Private IP address settings:**
 - Allocation:** Dynamic (disabled), Static (selected)
 - IP address:** 192.0.0.8 (with a green checkmark)
 - Public IP address:** Disabled (selected), Enabled (disabled)

An "OK" button is located at the bottom of the dialog, highlighted with a red border.

Configurar grupos de direcciones en el dispositivo NetScaler Gateway

Para obtener más información sobre cómo configurar grupos de direcciones en NetScaler Gateway, consulte [Configuración de grupos de direcciones](#).

Limitación:

No es posible vincular un rango de direcciones IIP a los usuarios. Todas las direcciones IP que se utilizan en un grupo de direcciones deben estar registradas.

Configurar varias direcciones IP para una instancia independiente de NetScaler VPX mediante comandos de PowerShell

October 17, 2024

En un entorno de Azure, se puede implementar un dispositivo virtual NetScaler VPX con varias NIC. Cada NIC puede tener varias direcciones IP. En esta sección se describe cómo implementar una instancia de NetScaler VPX con una única NIC y varias direcciones IP mediante los comandos de PowerShell. Puede utilizar el mismo script para la implementación de varias NIC y varias IP.

Nota:

En este documento, IP-Config hace referencia a un par de direcciones IP, IP pública e IP privada, asociadas a una NIC individual. Para obtener más información, consulte la sección [Terminología de Azure](#).

Caso de uso

En este caso de uso, se conecta una única NIC a una red virtual (VNET). La NIC está asociada con tres configuraciones IP, como se muestra en la siguiente tabla.

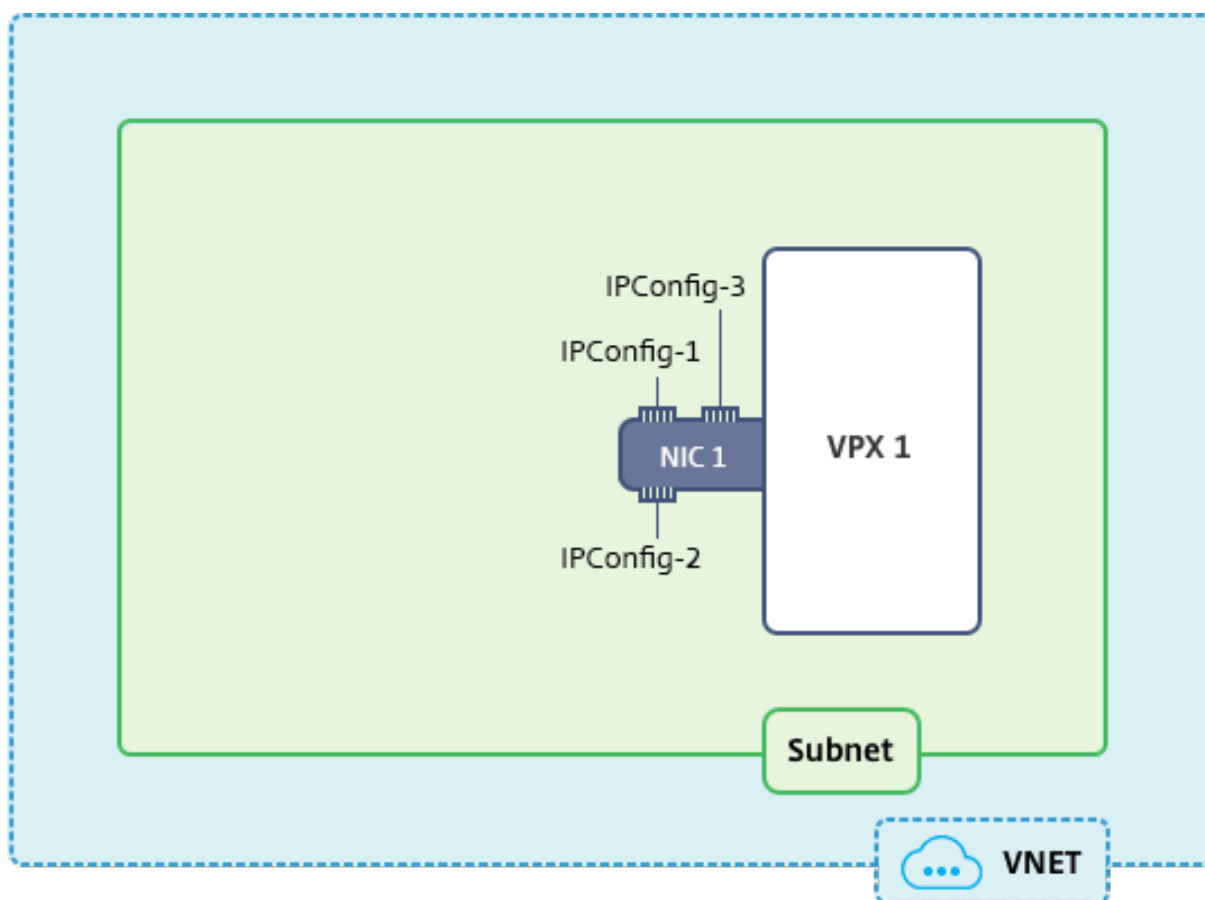
Configuración IP	Asociada con
IPConfig-1	Dirección IP pública estática; dirección IP privada estática
IPConfig-2	Dirección IP pública estática; dirección privada estática
IPConfig-3	Dirección IP privada estática

Nota:

IPConfig-3 no está asociado a ninguna dirección IP pública.

Diagrama: Topología

Aquí está la representación visual del caso de uso.

**Nota:**

En una implementación Multi-NIC, Multi-IP Azure NetScaler VPX, la dirección IP privada asociada a la principal (primera) `IPConfig` de la NIC principal (primera) se agrega automáticamente como dirección NSIP de administración del dispositivo. El resto de direcciones IP privadas asociadas a la instancia VPX `IPConfigs` deben agregarse como VIP o SNIP mediante el `add ns ip` comando, según lo determinado por sus requisitos.

A continuación se muestra el resumen de los pasos necesarios para configurar varias direcciones IP para un dispositivo virtual NetScaler VPX en modo autónomo:

1. Crear grupo de recursos
2. Crear cuenta de almacenamiento
3. Crear conjunto de disponibilidad
4. Crear grupo de servicios de red
5. Crear red virtual
6. Crear dirección IP pública
7. Asignar configuración IP
8. Crear NIC
9. Crear instancia de NetScaler VPX

10. Comprobar configuraciones de NIC
11. Comprobar las configuraciones del lado VPX

Script

Parámetros

A continuación se presentan parámetros de ejemplo de configuración para el caso de uso en este documento. Puede usar diferentes configuraciones si lo quiere.

\$locName="westcentralus"

\$rgName="Azure-MultiIP»

\$nicName1="VM1-NIC1"

\$vnetName="Azure-MultiIP-VNET»

\$vNetAddressRange="11.6.0.0/16"

\$frontendSubnetName="FrontendSubnet»

\$frontendSubnetRange="11.6.1.0/24"

\$prmStorageAccountName="Almacenamiento MultiIP»

\$avSetName="multiip-avSet"

\$VMsize="standard_DS4_V2"(Este parámetro crea una máquina virtual con hasta cuatro NIC).

Nota: El requisito mínimo para una instancia VPX es 2 vCPU y 2 GB de RAM.

\$editor="Citrix"

\$offer="netscalervpx110-6531"(puede usar ofertas diferentes)

\$sku="netscalerbyol» (Según tu oferta, el SKU puede ser diferente).

\$version="latest"

\$pubIPName1="pip1"

\$pubIPName2="pip2"

\$domName1="MultiIPVPX1"

\$DOMName2="MultiIPVPX2"

\$VMnamePrefix="VPXMultiIP»

\$osDiskSuffix="OSMultiIpAlbDiskDB1"

Información relacionada con Network Security Group (NSG):

```
$NSGname="NSG-MultiIP»  
$rule1name="HTTP entrante"  
$rule2Name="HTTPS entrante"  
$rule3name="SSH entrante"  
$ipconfigName1="ipconfig1"  
$ipconfigName2="ipconfig-2"  
$ipconfigName3="ipconfig-3"
```

1. Crear un grupo de recursos

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Crear una cuenta de almacenamiento

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName  
-ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Crear un conjunto de disponibilidad

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName  
$rgName -Location $locName
```

4. Crear un grupo de seguridad de red

1. Agregar reglas. Debe agregar una regla al grupo de seguridad de red para cualquier puerto que sirva el tráfico.

```
$rule1=New-AzureRmNetworkSecurityRuleConfig -Nombre $rule1Name  
-Descripción "Permitir HTTP"-Acceso Permitido -Protocolo Tcp -  
Dirección Entrante -Prioridad 101 -SourceAddressPrefix Internet -  
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange  
80 $rule2=New-AzureRmNetworkSecurityRuleConfig -Nombre $rule2Name  
-Descripción "Permitir HTTPS"-Acceso Permitido -Protocolo Tcp -  
Dirección Entrante -Prioridad 110 -SourceAddressPrefix Internet -  
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange  
443 $rule3=New-AzureRmNetworkSecurityRuleConfig -Nombre $rule3Name  
-Descripción "Permitir SSH"-Acceso Permitido -Protocolo Tcp -
```

```
Dirección Entrante -Prioridad 120 -SourceAddressPrefix Internet -
SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange
22
```

2. Cree un objeto de grupo de seguridad de red.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName
-Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
$rule3
```

5. Crear una red virtual

1. Agregue subredes.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$frontEndSubnetName -AddressPrefix $frontEndSubnetRange
```

2. Agregue un objeto de red virtual.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -
Subnet $frontendSubnet
```

3. Recupera subredes.

```
$subnetName="subred frontal" $subnet1=$vnet.Subredes|?{ $_.Name -
eq $subnetName }
```

6. Crear una dirección IP pública

```
$pip1=New-AzureRmPublicIpAddress -Nombre $pubIPName1 -NombreGrupoRecursos
$rgName -EtiquetaNombreDominio $domName1 -Ubicación $locName -M
étodoAsignación Estático $pip2=New-AzureRmPublicIpAddress -Nombre
$pubIPName2 -NombreGrupoRecursos $rgName -EtiquetaNombreDominio
$domName2 -Ubicación $locName -MétodoAsignación Estático
```

Nota:

Compruebe la disponibilidad de los nombres de dominio antes de utilizarlos.

El método de asignación de direcciones IP puede ser dinámico o estático.

7. Asignar configuración IP

En este caso de uso, tenga en cuenta los siguientes puntos antes de asignar direcciones IP:

- IPConfig-1 pertenece a la subred1 de VPX1.
- IPConfig-2 pertenece a la subred 1 de VPX1.
- IPConfig-3 pertenece a la subred 1 de VPX1.

Nota:

Cuando asigna varias configuraciones IP a una NIC, se debe asignar una configuración como principal.

```

1  $IPAddress1="11.6.1.27"
2  $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    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"
6  $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary

```

Utilice una dirección IP válida que cumpla los requisitos de la subred y compruebe su disponibilidad.

8. Crear NIC

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
  $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,
  $IPConfig3 -NetworkSecurityGroupId $nsg.Id
```

9. Crear una instancia de NetScaler VPX

1. Inicializar variables.

```
$suffixNumber = 1 $vmName = $vmNamePrefix + $suffixNumber
```

2. Cree un objeto de configuración de máquina virtual.

```
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
  AvailabilitySetId $avSet.Id
```

3. Establezca credenciales, SO e imagen.

```
$cred=Get-Credential -Message "Escriba el nombre y la contraseña
  para iniciar sesión en VPX". $vmConfig=Establecer-Sistema-
  operativo-AzureRMVMO -VM $vmConfig -Linux -Nombre-computadora
```

```
$vmName -Credenciales $cred $vmConfig=Set-AzureRMVMSourceImage -  
VM $vmConfig -PublisherName $publisher -Oferta $offer -SKU $sku -  
Versión $version
```

4. Agregue NIC.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.  
Id -Primary
```

Nota:

En una implementación de NetScaler VPX con varias NIC, una NIC debe ser principal. Por lo tanto, se debe agregar "-Primary" al agregar esa NIC a la instancia de NetScaler VPX.

5. Especifique el disco del sistema operativo y cree VM.

```
$osDiskName=$vmName + "-" + $osDiskSuffix1 $osVhdUri=$prmStorageAccount  
.Puntos finales primarios.Blob.ToString() + "vhds/" + $osDiskName  
+ ".vhd" $vmConfig=Establecer-AzureRMVMOSDisk -VM $vmConfig -  
Nombre $osDiskName -VhdUri $osVhdUri -OpciónDeCreación desde Imagen  
Set-AzureRmVMPlan -VM $vmConfig -Editor $publisher -Producto  
$offer -Nombre $skuNew-AzureRMVM -VM $vmConfig -NombreGrupoRecursos  
$rgName -Ubicación $locName
```

10. Verificar las configuraciones de NIC

Una vez que se inicia la instancia de NetScaler VPX, puede verificar las direcciones IP asignadas a `IPConfigs` de la NIC de NetScaler VPX mediante el siguiente comando.

```
$nic.IPConfig
```

11. Verificar las configuraciones del lado VPX

Cuando se inicia la instancia NetScaler VPX, se agrega una dirección IP privada asociada al principal `IPconfig` de la NIC principal como dirección NSIP. Las direcciones IP privadas restantes deben agregarse como direcciones VIP o SNIP, según lo determinado por sus requisitos. Utilice el siguiente comando.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Ahora ha configurado varias direcciones IP para una instancia de NetScaler VPX en modo independiente.

Scripts de PowerShell adicionales para la implementación de Azure

October 17, 2024

Esta sección proporciona los cmdlets de PowerShell con los que puede realizar las siguientes configuraciones en Azure PowerShell:

- Aprovisionar una instancia independiente de NetScaler VPX
- Aprovisionar un par NetScaler VPX en una configuración de alta disponibilidad con un balanceador de carga externo de Azure
- Aprovisionar un par NetScaler VPX en una configuración de alta disponibilidad con el balanceador de carga interno de Azure

Consulte también los temas siguientes para las configuraciones que puede realizar mediante comandos de PowerShell:

- [Configurar una configuración de alta disponibilidad con varias direcciones IP y NIC mediante comandos de PowerShell](#)
- [Configurar GSLB en instancias de NetScaler VPX](#)
- [Configurar GSLB en una configuración de alta disponibilidad activa en espera de NetScaler](#)
- [Configurar varias direcciones IP para una instancia de NetScaler VPX en modo independiente mediante comandos de PowerShell](#)

Aprovisionar una instancia independiente de NetScaler VPX

1. Crear un grupo de recursos

El grupo de recursos puede incluir todos los recursos de la solución o solo los recursos que desee administrar como grupo. La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos para crear un equilibrador de carga utilizan el mismo grupo de recursos.

```
$rgName="<resource group name>" $locName="<location name, such as West US>"  
New-AzureRmResourceGroup -Nombre $rgName -Ubicación $locName
```

Por ejemplo:

```
1 $rgName = "ARM-VPX"  
2 $locName = "West US"  
3 New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Crear una cuenta de almacenamiento

Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

```
$saName="<storage account name>" $saType="<storage
account type>", especifique uno: Standard_LRS, Standard_GRS, Standard_RAGRS
o Premium_LRS
New-AzureRmStorageAccount -Nombre $saName -NombreGrupoRecurso
$rgName -Tipo $saType -Ubicación $locName
```

Por ejemplo:

```
1 $saName="vpxstorage"
2 $saType="Standard_LRS"
3 New-AzureRmStorageAccount -Name $saName -ResourceGroupName
  $rgName -Type $saType -Location $locName
```

3. Crear un conjunto de disponibilidad

El conjunto de disponibilidad ayuda a mantener las máquinas virtuales disponibles durante el tiempo de inactividad, como durante el mantenimiento. Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

```
$avName="<availability set name>"
```

```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. Crear una red virtual

Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

```
$FrontendAddressPrefix="10.0.1.0/24" $BackendAddressPrefix="
10.0.2.0/24" $vnetAddressPrefix="10.0.0.0/16" $frontendSubnet
=New-AzureRmVirtualNetworkSubnetConfig -Nombre frontendSubnet
-PrefijoDirección $FrontendAddressPrefix $backendSubnet=New-
AzureRmVirtualNetworkSubnetConfig -Nombre backendSubnet -PrefijoDirecci
ón $BackendAddressPrefix
New-AzureRmVirtualNetwork -Nombre TestNet -ResourceGroupName $rgName -Ubicación $locName -PrefijoDirección
$vnetAddressPrefix -Subred $frontendSubnet,$backendSubnet
```

Por ejemplo:

```
1 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
  frontendSubnet -AddressPrefix $FrontendAddressPrefix
2
3 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
  backendSubnet -AddressPrefix $BackendAddressPrefix
4
5 New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName
  $rgName -Location $locName -AddressPrefix $vnetAddressPrefix
  -Subnet $frontendSubnet,$backendSubnet
```

5. Crear una NIC

Cree una NIC y asocie la NIC a la instancia de NetScaler VPX. La subred front-end creada en el procedimiento anterior se indexa en 0 y la subred back-end se indexa en 1. Ahora cree NIC de una de las tres maneras siguientes:

a) NIC con dirección IP pública

```
$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) NIC con IP pública y etiqueta 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
```

Antes de asignar \$DOMName, compruebe que está disponible o no mediante el comando:

```
Test-AzureRmDnsAvailability -DomainQualifiedName $domName -
Location $locName
$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
    $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
].Id -PublicIpAddressId $pip.Id
```

Por ejemplo:

```
1  $nicName="frontendNIC"
2
3  $domName="vpxazure"
4
5  $pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic
6
7  $nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets\[0\].Id -PublicIpAddressId $pip.Id
```

c) NIC con dirección pública dinámica y dirección IP privada estática

Asegúrese de que la dirección IP privada (estática) que agregue a la máquina virtual debe ser el mismo rango que la de la subred especificada.

```
$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. Crear un objeto virtual

```
$vmName="<VM name>"
$vmSize="<VM size string>"
$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName
$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
    $avset.Id
```

7. Obtenga la imagen de 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."
```

Proporcione sus credenciales que se utilizan para iniciar sesión en 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
```

Por ejemplo:

```
$pubName="citrix"
```

El siguiente comando se utiliza para mostrar todas las ofertas de Citrix:

```

1  Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
   Select Offer
2
3  $offerName="netscalervpx110-6531"

```

El siguiente comando se utiliza para conocer el SKU ofrecido por el editor para un nombre de oferta específico:

```

Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -
Offer $offerName | Select Skus

```

8. Crear una máquina virtual

```

$diskName="<name identifier for the disk in Azure storage, such
as OSDisk>"

```

Por ejemplo:

```

1  $diskName="dynamic"
2
3  $pubName="citrix"
4
5  $offerName="netscalervpx110-6531"
6
7  $skuName="netscalerbyol"
8
9  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
   -Name $saName
10
11 $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/
   " + $diskName + ".vhd"
12
13 $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri
   $osDiskUri -CreateOption fromImage

```

Al crear VM a partir de imágenes presentes en el mercado, utilice el siguiente comando para especificar el plan de VM:

```

Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName
-Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
$vm

```

Aprovisione un par NetScaler VPX en una configuración de alta disponibilidad con un balanceador de carga externo de Azure

Inicie sesión en AzureRMAccount con sus credenciales de usuario de Azure.

1. Crear un grupo de recursos

La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos utilizados para crear un equilibrador de carga utilizan el mismo grupo de recursos.

```
$rgName="<resource group name>"
```

```
$locName="<location name, such as West US>"
```

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

Por ejemplo:

```
1  $rgName = "ARM-LB-NS"
2
3  $locName = "West US"
4
5  New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Crear una cuenta de almacenamiento

Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

```
$saName="<storage account name>"
```

```
$saType="&lt;storage account type&gt;", especifique uno: Standard_LRS,  
Standard_GRS, Standard_RAGRS o Premium_LRS
```

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName  
$rgName -Type $saType -Location $locName
```

Por ejemplo:

```
1  $saName="vpxstorage"
2
3  $saType="Standard_LRS"
4
5  New-AzureRmStorageAccount -Name $saName -ResourceGroupName  
    $rgName -Type $saType -Location $locName
```

3. Crear un conjunto de disponibilidad

Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

```
$avName="<availability set name>"
```

```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName  
$rgName -Location $locName
```

4. Crear una red virtual

Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

```

1  $vnetName = "LBVnet"
2
3  $FrontendAddressPrefix="10.0.1.0/24"
4
5  $BackendAddressPrefix="10.0.2.0/24"
6
7  $vnetAddressPrefix="10.0.0.0/16"
8
9  $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix
10
11 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
12
13 $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
    ResourceGroupName $rgName -Location $locName -AddressPrefix
    $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet

```

Nota:

Elija el valor del parámetro AddressPrefix según sus necesidades.

Asigne subred front-end y back-end a la red virtual que creó anteriormente en este paso.

Si la subred front-end es el primer elemento de la matriz VNet, SubnetID debe ser \$vnet.subnets [0] .Id.

Si la subred front-end es el segundo elemento de la matriz, el ID de subred debe ser \$vnet.subnets [1] .Id, etc.

5. Configurar la dirección IP de front-end y crear un grupo de direcciones back-end

Configure una dirección IP front-end para el tráfico de red del equilibrador de carga entrante y cree un grupo de direcciones back-end para recibir el tráfico balanceado de carga.

```

1  $pubName="PublicIp1"
2
3  $publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -
    AllocationMethod Static -DomainNameLabel nsvpx

```

Nota:

Verifique la disponibilidad del valor para 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. Crear una sonda de salud

Cree un sondeo de estado TCP con el puerto 9000 y el intervalo de 5 segundos.

```

1     $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
        HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
        ProbeCount 2

```

7. Crear una regla de equilibrio de carga

Cree una regla LB para cada servicio que esté equilibrando la carga.

Por ejemplo:

Puede utilizar el siguiente ejemplo para equilibrar la carga del servicio HTTP.

```

1     $lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
        FrontendIpConfiguration $frontendIP1 -BackendAddressPool
        $beAddressPool1 -Probe $healthProbe -Protocol Tcp -
        FrontendPort 80 -BackendPort 80

```

8. Crear reglas NAT entrantes

Cree reglas NAT para los servicios que no esté equilibrando la carga.

Por ejemplo, al crear un acceso SSH a una instancia de NetScaler VPX.

Nota:

El triplete Protocolo-FrontEndPort-BackendPort no debe ser el mismo para dos reglas NAT.

```

1     $inboundNATRule1= New-
        AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1
        -FrontendIpConfiguration $frontendIP1 -Protocol
        TCP -FrontendPort 22 -BackendPort 22
2
3     $inboundNATRule2= New-
        AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 -
        FrontendIpConfiguration $frontendIP1 -Protocol TCP -
        FrontendPort 10022 -BackendPort 22

```

9. Crear una entidad de equilibrador de carga

Cree el equilibrador de carga agregando todos los objetos (reglas NAT, reglas de equilibrador de carga, configuraciones de sondeo) juntos.

```

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. Crear una NIC

Cree dos NIC y asocie cada NIC con cada instancia VPX

a) NIC1 con VPX1

Por ejemplo:

```

1  $nicName="NIC1"
2
3  $lbName="ELB"
4
5  $bePoolIndex=0
6
7  \* Rule indexes starts from 0.
8
9  $natRuleIndex=0
10
11 $subnetIndex=0
12
13 \* Frontend subnet index
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\[ $natRuleIndex
      \]

```

b) NIC2 con VPX2

Por ejemplo:

```

1  $nicName="NIC2"
2
3  $lbName="ELB"
4
5  $bePoolIndex=0
6
7  $natRuleIndex=1
8
9  \* Second Inbound NAT (SSH) rule we need to use

```

```

10
11 ` $subnetIndex=0
12
13 \* Frontend subnet index
14
15 $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName
16
17 $nic2=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets\[ $subnetIndex\] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools\[ $bePoolIndex\] -
    LoadBalancerInboundNatRule $lb.InboundNatRules\[
    $natRuleIndex\]

```

11. Crear instancias NetScaler VPX

Cree dos instancias de NetScaler VPX como parte del mismo grupo de recursos y conjunto de disponibilidad y conéctelas al balanceador de carga externo.

a) Instancia 1 de NetScaler VPX

Por ejemplo:

```

1  $vmName="VPX1"
2
3  $vmSize="Standard\_A3"
4
5  $pubName="citrix"
6
7  $offerName="netscalervpx110-6531"
8
9  $skuName="netscalerbyol"
10
11 $avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName
12
13 $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id
14
15 $cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"
16
17 $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose
18
19 $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"
20
21 $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id
22
23 $diskName="dynamic"
24

```

```
25 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName
26
27 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhd1/" + $diskName + ".vhd"
28
29 $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage
30
31 Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
    $offerName -Name $skuName
32
33 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
```

b) Instancia 2 de NetScaler VPX

Por ejemplo:

```
1 $vmName="VPX2"
2
3 $vmSize="Standard_A3"
4
5 $avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName
6
7 $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id
8
9 $cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhd2/" + $diskName + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
    $offerName -Name $skuName
26
```



```
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
```

12. Configurar las máquinas virtuales

Cuando se inicien ambas instancias de NetScaler VPX, conéctese a ambas instancias de NetScaler VPX mediante el protocolo SSH para configurar las máquinas virtuales.

a) Activo-Activo: ejecute el mismo conjunto de comandos de configuración en la línea de comandos de ambas instancias de NetScaler VPX.

b) Activo-Pasivo: ejecute este comando en la línea de comandos de ambas instancias de NetScaler VPX.

```
add ha node #nodeID <nsip of other NetScaler VPX>
```

En el modo Activo-Pasivo, ejecute comandos de configuración solo en el nodo principal.

Aprovisione un par NetScaler VPX en una configuración de alta disponibilidad con el balanceador de carga interno de Azure

Inicie sesión en AzureRMAccount con sus credenciales de usuario de Azure.

1. Crear un grupo de recursos

La ubicación especificada aquí es la ubicación predeterminada de los recursos de ese grupo de recursos. Asegúrese de que todos los comandos para crear un equilibrador de carga utilizan el mismo grupo de recursos.

```
$rgName="\&#060;resource group name\&#062;"
$locName="\&#060;location name, such as West US\&#062;"
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

Por ejemplo:

```
1 $rgName = "ARM-LB-NS"
2
3 $locName = "West US"
4
5 New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Crear una cuenta de almacenamiento

Elija un nombre único para su cuenta de almacenamiento que contenga solo letras y números minúsculas.

```
$saName="<storage account name>"
```

`$saType="<storage account type>"`, especifique uno: Standard_LRS, Standard_GRS, Standard_RAGRS o Premium_LRS

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName
$rgName -Type $saType -Location $locName
```

Por ejemplo:

```
1  $saName="vpxstorage"
2
3  $saType="Standard_LRS"
4
5  New-AzureRmStorageAccount -Name $saName -ResourceGroupName
   $rgName -Type $saType -Location $locName
```

3. Crear un conjunto de disponibilidad

Un equilibrador de carga configurado con un conjunto de disponibilidad garantiza que la aplicación esté siempre disponible.

```
$avName="<availability set name>"
```

```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. Crear una red virtual

Agregue una nueva red virtual con al menos una subred, si la subred no se creó previamente.

```
1  $vnetName = "LBVnet"
2
3  $vnetAddressPrefix="10.0.0.0/16"
4
5  $FrontendAddressPrefix="10.0.1.0/24"
6
7  $BackendAddressPrefix="10.0.2.0/24"
8
9  $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
   ResourceGroupName $rgName -Location $locName -AddressPrefix
   $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet`
10
11 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   frontendSubnet -AddressPrefix $FrontendAddressPrefix
12
13 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   backendSubnet -AddressPrefix $BackendAddressPrefix
```

Nota:

Elija el valor del parámetro AddressPrefix según sus necesidades.

Asigne subred front-end y back-end a la red virtual que creó anteriormente en este paso.

Si la subred front-end es el primer elemento de la matriz VNet, SubnetID debe ser \$vnet.subnets [0] .Id.

Si la subred front-end es el segundo elemento de la matriz, el ID de subred debe ser \$vnet.subnets [1] .Id, etc.

5. Crear un grupo de direcciones back-end

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -  
Name "LB-backend"
```

6. Crear reglas NAT

Cree reglas NAT para los servicios que no esté equilibrando la carga.

```
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
```

Utilice puertos front-end y back-end según sus necesidades.

7. Crear una sonda de salud

Cree un sondeo de estado TCP con el puerto 9000 y el intervalo de 5 segundos.

```
1 $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "  
    HealthProbe" " -Protocol tcp -Port 9000 -IntervalInSeconds 5  
    -ProbeCount 2
```

8. Crear una regla de equilibrio de carga

Cree una regla LB para cada servicio que esté equilibrando la carga.

Por ejemplo:

Puede utilizar el siguiente ejemplo para equilibrar la carga del servicio HTTP.

```
1 $lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -  
    FrontendIpConfiguration $frontendIP -BackendAddressPool  
    $beAddressPool -Probe $healthProbe -Protocol Tcp -  
    FrontendPort 80 -BackendPort 80
```

Utilice puertos front-end y back-end según sus necesidades.

9. Crear una entidad de equilibrador de carga

Cree el equilibrador de carga agregando todos los objetos (reglas NAT, reglas de equilibrador de carga, configuraciones de sondeo) juntos.

```

1  $NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -
    Name "InternalLB" -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,
    $inboundNatRule2 -LoadBalancingRule $lbrule -
    BackendAddressPool $beAddressPool -Probe $healthProbe

```

10. Crear una NIC

Cree dos NIC y asocie cada NIC a cada instancia de 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\[0\]

```

Esta NIC es para NetScaler VPX 1. La IP privada debe estar en la misma subred que la de la subred agregada.

```

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
    \[1\].

```

Esta NIC es para NetScaler VPX 2. El parámetro `Private IP Address` puede tener cualquier IP privada según sus requisitos.

11. Crear instancias NetScaler VPX

Cree dos instancias VPX que forman parte del mismo grupo de recursos y conjunto de disponibilidad, y conéctela al equilibrador de carga interno.

a) Instancia 1 de NetScaler VPX

Por ejemplo:

```

1  $vmName="VPX1"
2
3  $vmSize="Standard\_A3"
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName
6
7  $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"
10
11 $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
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds1/" + $diskName + ".vhd"
22
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
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
```

b) Instancia 2 de NetScaler VPX

Por ejemplo:

```
1 $vmName="VPX2"
2
3 $vmSize="Standard\_A3"
4
5 $avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName
6
7 $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id
8
9 $cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
```

```
22     vhds2/" + $diskName + ".vhd"
23     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
        $offerName -Name $skuName
26
27     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm2
```

12. Configurar las máquinas virtuales

Cuando se inicien ambas instancias de NetScaler VPX, conéctese a ambas instancias de NetScaler VPX mediante el protocolo SSH para configurar las máquinas virtuales.

a) Activo-Activo: ejecute el mismo conjunto de comandos de configuración en la línea de comandos de ambas instancias de NetScaler VPX.

b) Activo-Pasivo: ejecute este comando en la línea de comandos de ambas instancias de NetScaler VPX.

```
add ha node #nodeID <nsip of other NetScaler VPX>
```

En el modo Activo-Pasivo, ejecute comandos de configuración solo en el nodo principal.

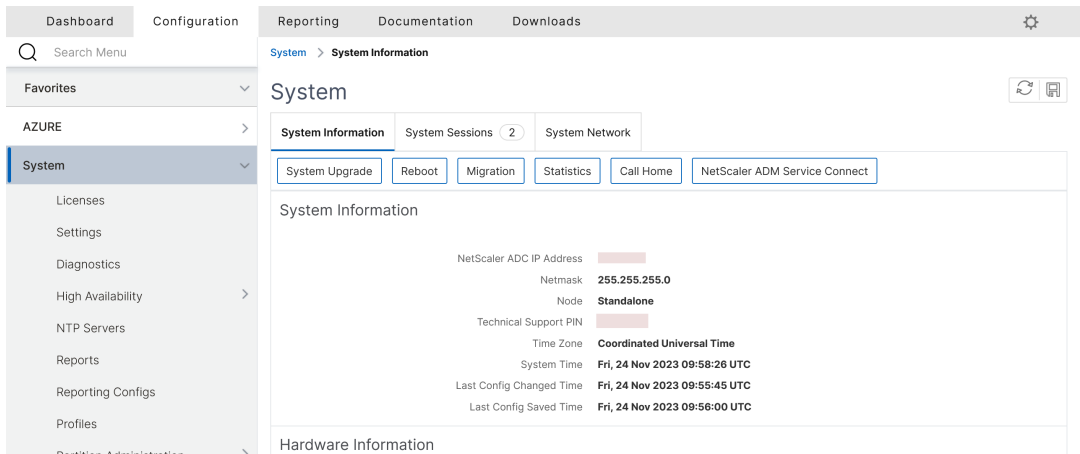
Create a support ticket for the VPX instance on Azure

April 23, 2024

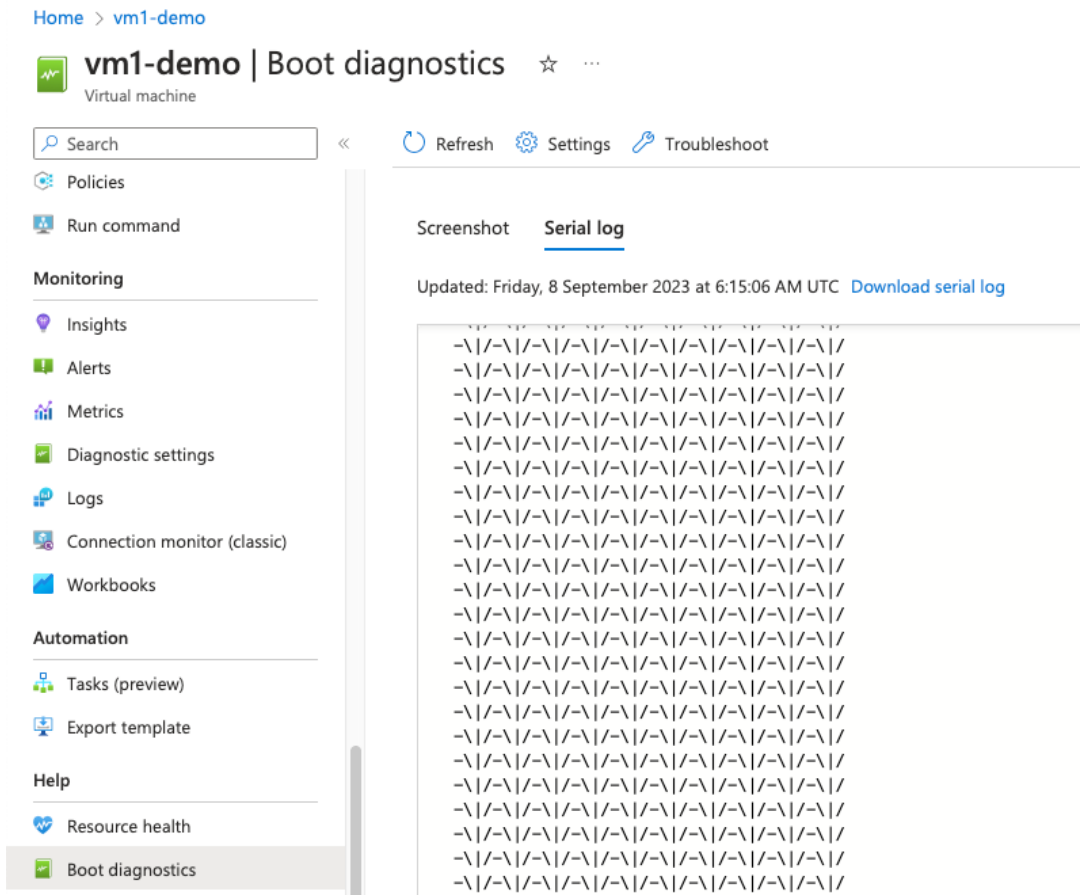
If you're experiencing issues with your NetScaler VPX instance on Azure, for troubleshooting, you can create a support ticket in the [NetScaler support portal](#).

To file a support ticket, make sure the following:

- Your network is connected.
- You have your Azure account number, the support PIN code of the NetScaler subscription-based offering that you have deployed on Azure, and the Azure serial log handy.
 - You can find the support PIN code on the **Systems page** in the VPX GUI.



- You can find the serial log in the Azure portal (**Boot diagnostics** section of your VM).



Note:

NetScaler supports subscription-based offerings on Azure (subscription license with hourly price).

Once you have all the information ready, call NetScaler support. You're asked to provide your name and email address.

Preguntas frecuentes de Azure

October 17, 2024

- **¿El procedimiento de actualización de la instancia de NetScaler VPX instalada desde Azure Marketplace es diferente del procedimiento de actualización local?**

No. Puede actualizar su instancia de NetScaler VPX en la nube de Microsoft Azure a la versión 11.1 o posterior de NetScaler VPX mediante los procedimientos de actualización estándar de NetScaler VPX. Puede actualizar mediante procedimientos GUI o CLI. Para cualquier instalación nueva, use la imagen NetScaler VPX para la nube de Microsoft Azure.

Para descargar las versiones de actualización de NetScaler VPX, vaya a Descargas de NetScaler > Firmware de NetScaler.**

- **¿Cómo corregir los movimientos MAC y los silenciamientos de la interfaz observados en instancias NetScaler VPX alojadas en Azure?**

En el entorno Multi-NIC de Azure, de forma predeterminada, todas las interfaces de datos pueden mostrar movimientos MAC y silenciamientos de la interfaz. Para evitar que MAC se mueva y se silencie la interfaz en los entornos de Azure, Citrix recomienda crear una VLAN por interfaz de datos (sin etiqueta) de la instancia NetScaler VPX y vincular la IP principal de la NIC en Azure.

Para obtener más información, consulte el artículo [CTX224626](#).

Implementar una instancia de NetScaler VPX en Google Cloud Platform

October 17, 2024

Puede implementar una instancia NetScaler VPX en Google Cloud Platform (GCP). Una instancia VPX en GCP le permite aprovechar las capacidades de computación en nube de GCP y utilizar las funciones de equilibrio de carga y administración de tráfico de Citrix para sus necesidades empresariales. Puede implementar instancias VPX en GCP como instancias independientes. Se admiten configuraciones de NIC única y NIC múltiple.

Funcionalidades admitidas

Todas las funciones Premium, Advanced y Standard son compatibles con el GCP en función del tipo de licencia/versión utilizado.

Limitación

- No se admite IPv6.

Requisitos de hardware

La instancia VPX en GCP debe tener un mínimo de 2 vCPU y 4 GB de RAM.

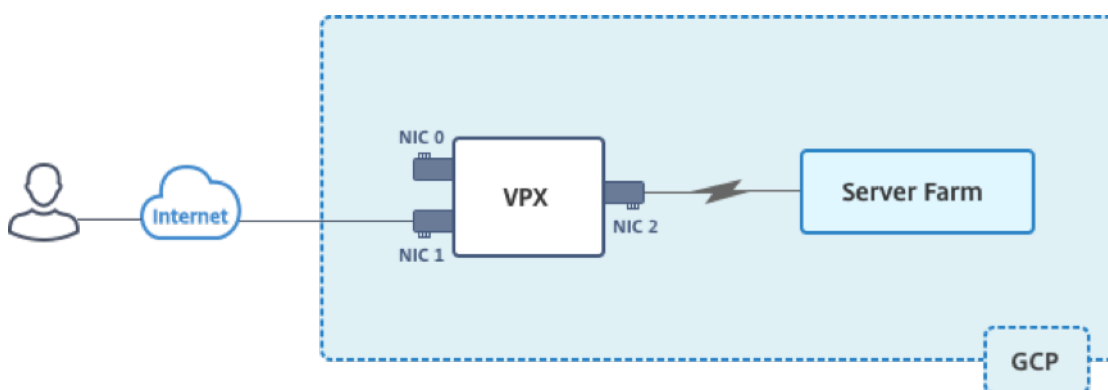
Puntos a tener en cuenta

Tenga en cuenta los siguientes puntos específicos de GCP antes de comenzar la implementación.

- Después de crear la instancia, no podrás agregar ni eliminar ninguna interfaz de red.
- Para una implementación de varias NIC, cree redes de VPC separadas para cada NIC. Una NIC solo se puede asociar a una red.
- Para una instancia de NIC única, la consola de GCP crea una red de forma predeterminada.
- Se requieren un mínimo de 4 vCPU para una instancia con más de dos interfaces de red.
- Si se requiere el reenvío de IP, debe habilitar el reenvío de IP al crear la instancia y configurar la NIC.

Escenario: Implementar una instancia independiente de NetScaler VPX con múltiples NIC y múltiples IP

Este caso ilustra cómo implementar una instancia independiente de NetScaler VPX en GCP. En este caso, se crea una instancia VPX independiente con muchas NIC. La instancia se comunica con los servidores back-end (la comunidad de servidores).



Cree tres NIC para cumplir los siguientes propósitos.

NIC	Propósito	Asociado a la red de VPC
NIC 0	Sirve el tráfico de administración (IP de NetScaler)	Red de gestión
NIC 1	Sirve tráfico del lado del cliente (VIP)	Red de clientes
NIC 2	Se comunica con servidores back-end (SNIP)	Red de servidores back-end

Configure las rutas de comunicación requeridas entre las siguientes:

- Instancia NetScaler VPX y los servidores back-end.
- Instancia de NetScaler VPX y los hosts externos en Internet público.

Resumen de los pasos de implementación

1. Cree tres redes de VPC para tres NIC diferentes.
2. Cree reglas de firewall para los puertos 22, 80 y 443.
3. Cree una instancia con tres NIC.

Seleccione la instancia de NetScaler VPX en GCP Marketplace.

Nota:

Crea una instancia en la misma región en la que creaste las redes de VPC.

Paso 1. Cree redes de VPC.

Cree tres redes de VPC asociadas con la NIC de administración, la NIC de cliente y la NIC de servidor. Para crear una red de VPC, inicie sesión en la **consola de Google > Redes > Red de VPC > Crear red de VPC**. Complete los campos obligatorios, como se muestra en la captura de pantalla, y haga clic en **Crear**.

netscaler-vpx-platform-eng

← Create a VPC network

Name ?
vpxmgmt

Description (Optional)
management vpc

Subnets

Subnets 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 subnets. [Learn more](#)

Subnet creation mode
 Custom Automatic

New subnet 🗑️ ⬆️

Name ?
vpxmgmtsubnet

[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

Dynamic 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

Del mismo modo, cree redes de VPC para NIC del lado del cliente y del servidor.

Nota:

Las tres redes de VPC deben estar en la misma región, que en este caso es asia-east1.

Paso 2. Cree reglas de firewall para los puertos 22, 80 y 443.

Cree reglas para SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443) para cada red VPC. Para obtener más información acerca de las reglas del [firewall](#), consulte [Descripción general de las reglas](#)

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](#)

Name ?

Description (Optional)

Logs
 Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

On
 Off

Network ?

Priority ?
 Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ?

Ingress
 Egress

Action on match ?

Allow
 Deny

Targets ?

Source filter ?

Source IP ranges ?

Second source filter ?

Protocols and ports ?

Allow all
 Specified protocols and ports

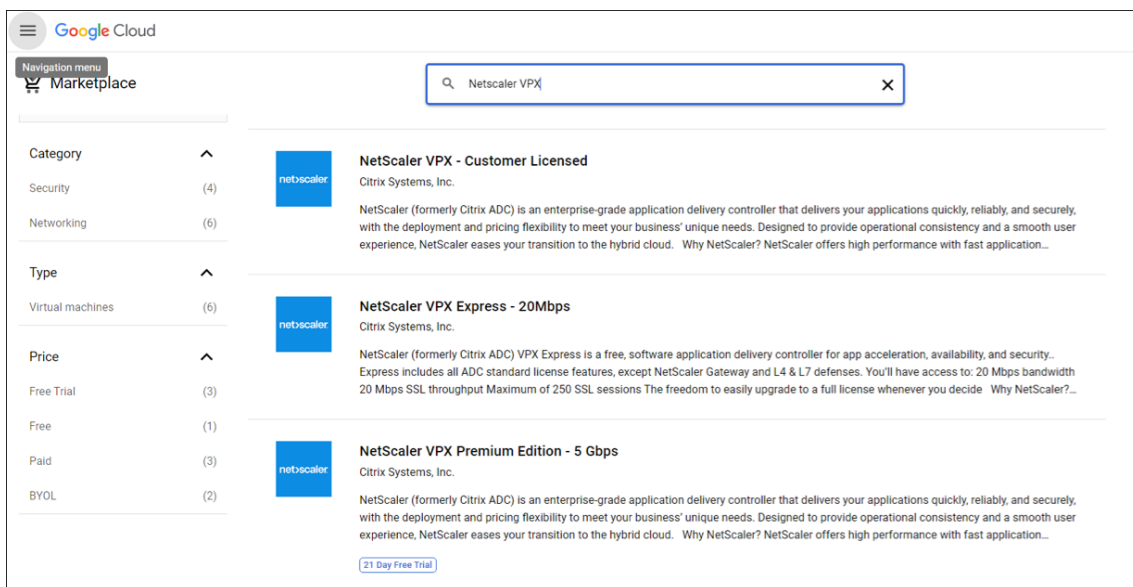
tcp :
 udp :
 Other protocols

⌵ [Disable rule](#)

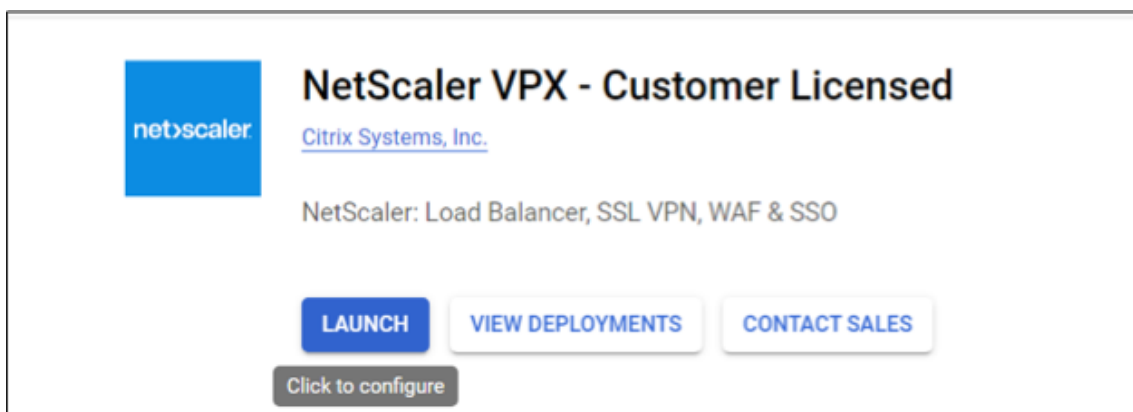
Create
Cancel

Paso 3. Crea la instancia VPX.

1. Inicie sesión en la consola de GCP.
2. Vaya a [GCP Marketplace](#).
3. Seleccione una suscripción según sus requisitos.



4. Haga clic en **Iniciar** en la suscripción seleccionada.



5. Complete el formulario de implementación y haga clic en **Implementar**.

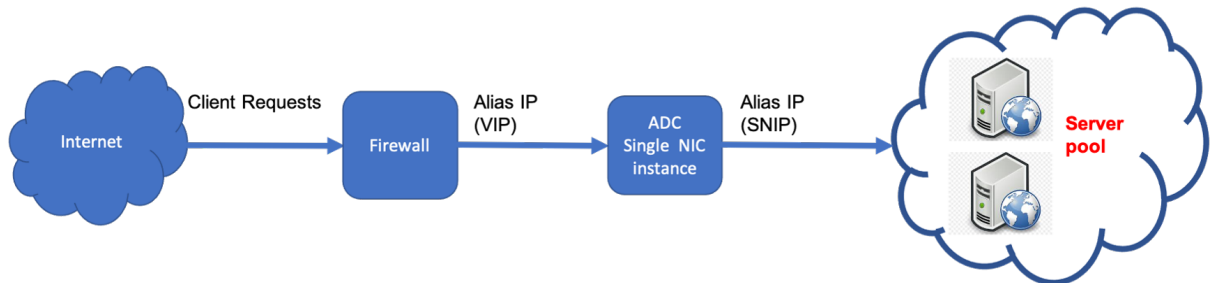
Nota:

Utilice las redes VPC creadas en el **Paso 1**.

6. La instancia implementada aparece en **Compute Engine > Instancias de VM**.
Usa el SSH de GCP o la consola serie para configurar y administrar la instancia VPX.

Caso: Implementar una instancia VPX independiente de NIC única

Este caso ilustra cómo implementar una instancia independiente de NetScaler VPX con una única NIC en GCP. Las direcciones IP de alias se utilizan para lograr esta implementación.



Cree una única NIC (NIC0) para cumplir con los siguientes propósitos:

- Gestione el tráfico de administración (NetScaler IP) en la red de administración.
- Manejar el tráfico del lado del cliente (VIP) en la red del cliente.
- Comuníquese con los servidores back-end (SNIP) en la red de servidores back-end.

Configure las rutas de comunicación requeridas entre las siguientes:

- Servidores de instancias y back-end.
- Instancia y los hosts externos en la Internet pública.

Resumen de los pasos de implementación

1. Cree una red de VPC para NIC0.
2. Cree reglas de firewall para los puertos 22, 80 y 443.
3. Crea una instancia con una única NIC.
4. Agregue direcciones IP de alias a VPX.
5. Agregue VIP y SNIP en VPX.
6. Agregue un servidor virtual de equilibrio de carga.
7. Agregue un servicio o un grupo de servicios en la instancia.
8. Enlace el servicio o el grupo de servicios al servidor virtual de equilibrio de carga en la instancia.

Nota:

Crea una instancia en la misma región en la que creaste las redes de VPC.

Paso 1. Cree una red de VPC.

Cree una red de VPC para asociarla a NIC0.

Para crear una red de VPC, siga estos pasos:

1. Inicie sesión en la **consola de GCP > Redes > Red de VPC > Crear red de VPC**
2. Complete los campos obligatorios y haga clic en **Crear**.

The image shows two screenshots from the Google Cloud Platform console. The top screenshot is titled 'Create a VPC network' and shows the following fields: 'Name' with the value 'vpxmgmt', 'Description (Optional)' with the value 'management vpc', and 'Subnet creation mode' set to 'Custom'. The bottom screenshot is titled 'New subnet' and shows: 'Name' as 'vpxmgmtsubnet', 'Region' as 'asia-east1', 'IP address range' as '192.168.30.0/24', 'Private Google access' set to 'On', and 'Flow logs' set to 'Off'. At the bottom of the second screenshot, 'Dynamic routing mode' is set to 'Regional'.

Paso 2. Cree reglas de firewall para los puertos 22, 80 y 443.

Cree reglas para SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443) para la red de VPC. Para obtener más información acerca de las reglas del [firewall](#), consulte [Descripción general de las reglas](#)

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](#)

Name

Description (Optional)

Logs
Turning on Firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

Network

Priority
Priority can be 0 - 65535 Check priority of other firewall rules

Direction of traffic
 Ingress
 Egress

Action on match
 Allow
 Deny

Targets

Source filter

Source IP ranges

Second source filter

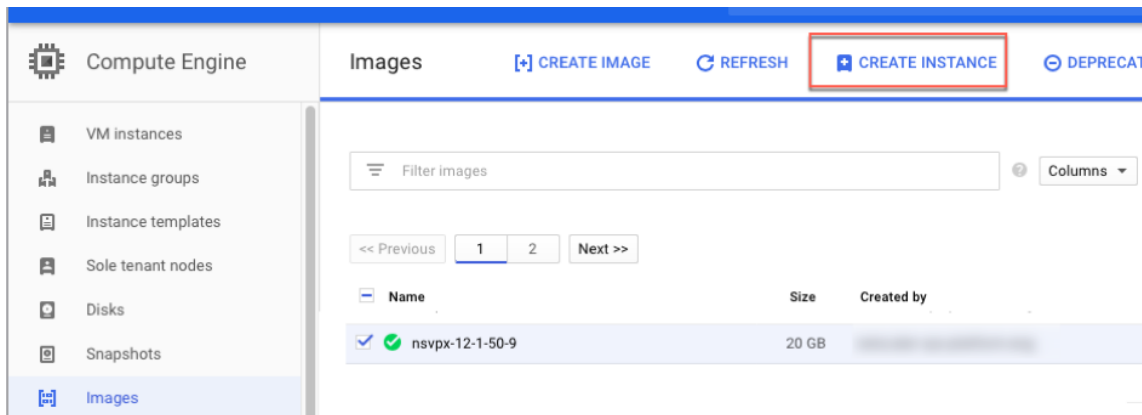
Protocols and ports
 Allow all
 Specified protocols and ports
 tcp:
 udp:
 Other protocols

Disable rule

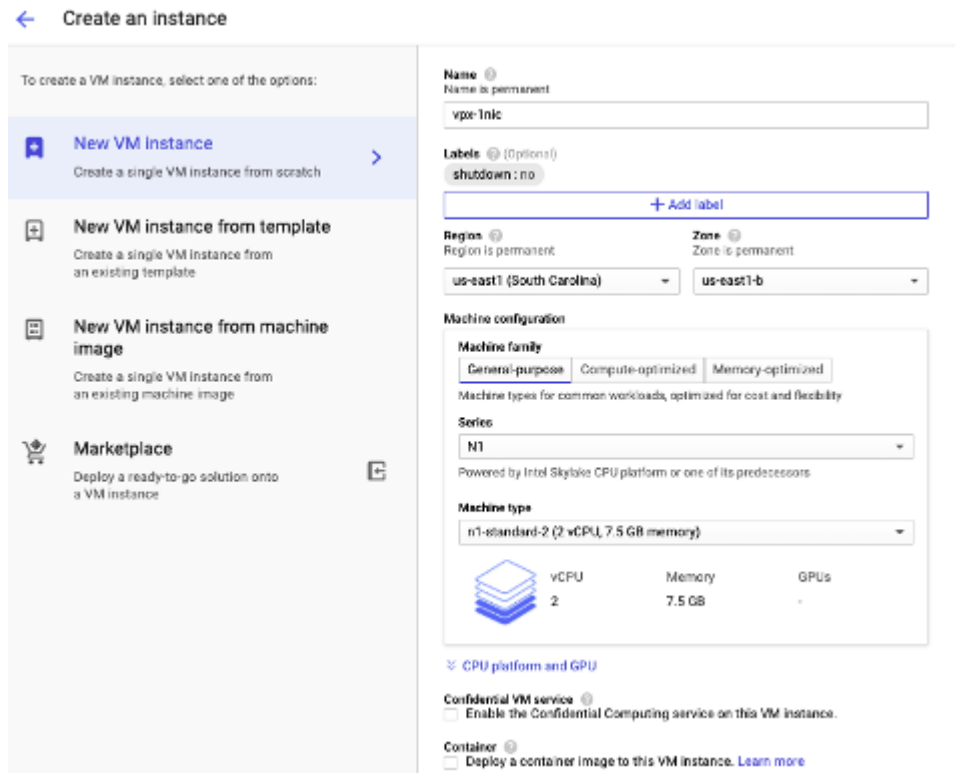
Paso 3. Cree una instancia con una NIC única.

Para crear una instancia con una sola NIC, siga estos pasos:

1. Inicie sesión en la **consola de GCP**.
2. En **Compute**, coloque el cursor sobre **Compute Engine** y seleccione **Imágenes**.
3. Seleccione la imagen y haga clic en **Crear instancia**.



4. Seleccione un tipo de instancia con dos vCPU (requisito mínimo para ADC).



5. Haga clic en la ficha **Redes** en la ventana **Administración, seguridad, discos, redes**.
6. En **Interfaces de red**, haga clic en el icono **Modificar** para modificar la NIC predeterminada.
7. En la ventana **Interfaces de red, en Red**, seleccione la red de VPC que creó.
8. Puede crear una dirección IP externa estática. En **Direcciones IP externas**, haga clic en **Crear dirección IP**.
9. En la ventana **Reservar una dirección estática**, agrega un nombre y una descripción y haga clic en **Reservar**.
10. Haga clic en **Crear** para crear la instancia VPX. La nueva instancia aparece en instancias de VM.

Paso 4. Agrega direcciones IP alias a la instancia VPX.

Asigne dos direcciones IP alias a la instancia VPX para usarlas como direcciones VIP y SNIP.

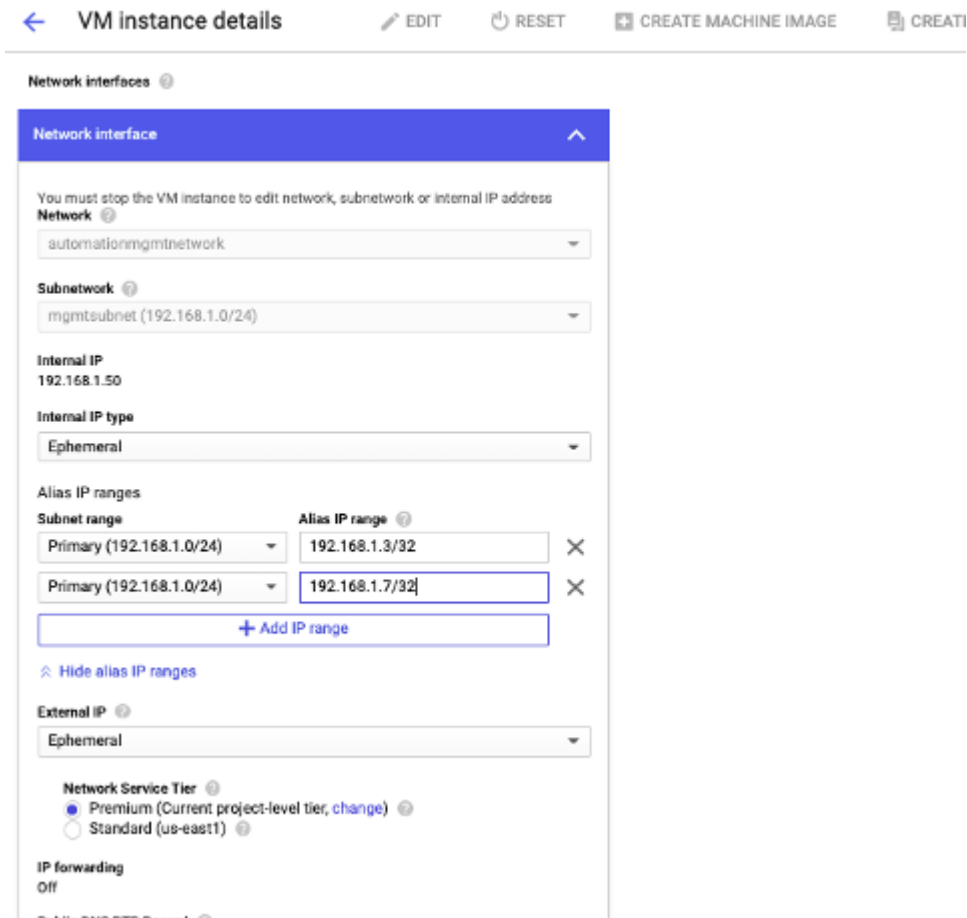
Nota:

No utilices la dirección IP interna principal de la instancia VPX para configurar el VIP o el SNIP.

Para crear una dirección IP de alias, lleve a cabo estos pasos:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz NIC0.

3. En el campo **Intervalo de IP de alias**, introduzca las direcciones IP de alias.



4. Haga clic en **Listoy**, a continuación, en **Guardar**.

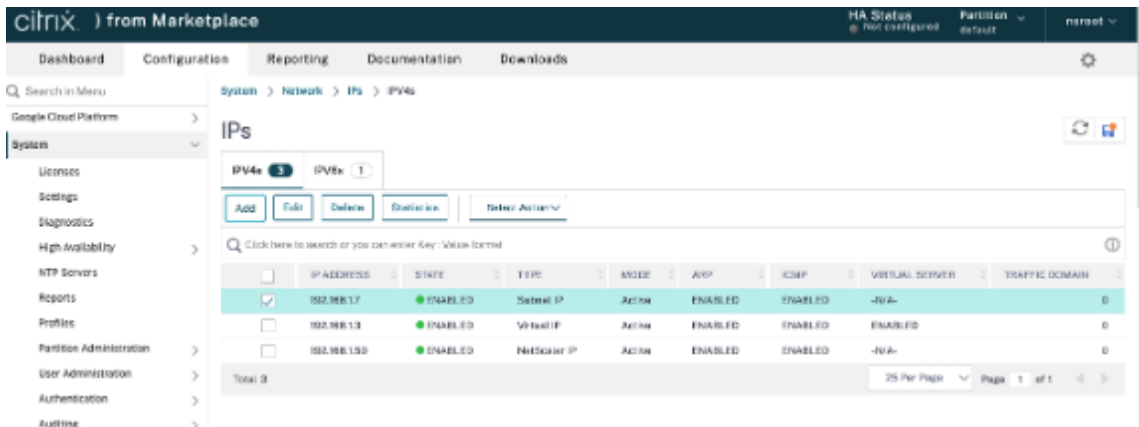
5. Compruebe las direcciones IP de alias en la página de **detalles de la instancia de VM**.



Paso 5. Agregue VIP y SNIP en la instancia VPX.

En la instancia VPX, agregue la dirección IP del alias del cliente y la dirección IP del alias del servidor.

1. En la GUI de NetScaler, vaya a **Sistema > Red > IP > IPv4** y haga clic en **Agregar**.



2. Para crear una dirección IP (VIP) de alias de cliente:

- Introduzca la dirección IP de alias de cliente y la máscara de red configuradas para la subred de VPC en la instancia de VM.
- En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
- Haga clic en **Create**.

3. Para crear una dirección IP de alias de servidor (SNIP):

- Introduzca la dirección IP de alias del servidor y la máscara de red configuradas para la subred de VPC en la instancia de VM.
- En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
- Haga clic en **Create**.

Paso 6. Agregue un servidor virtual de equilibrio de carga.

1. En la GUI de NetScaler, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales** y haga clic en **Agregar**.
2. Agregue los valores requeridos para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (IP de alias de cliente) y Puerto.
3. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.

Dashboard Configuration Reporting Documentation Downloads

← 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 application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (RFC1918) 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*

Protocol*

IP Address Type*

IP Address*

Port*

> More

Paso 7. Enlace el grupo de servicios/servicios al servidor virtual de equilibrio de carga en la instancia.

1. En la GUI de NetScaler, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios** y haga clic en **Agregar**.
2. Agregue los valores requeridos para Nombre de servicio, Dirección IP, Protocolo y Puerto y haga clic en **Aceptar**.

Paso 8. Vincula el servicio/grupo de servicios al servidor virtual de equilibrio de carga en la instancia.

1. En la GUI, vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 6** y haga clic en **Modificar**.
3. En la ventana **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 7** y haga clic en **Vincular**.

Puntos a tener en cuenta después de implementar la instancia VPX en GCP

- Inicie sesión en el VPX con el nombre de usuario `nsroot` y el ID de instancia como contraseña. Cuando se le solicite, cambie la contraseña y guarde la configuración.
- Para recopilar un paquete de asistencia técnica, ejecute el comando `shell /netscaler/showtech_cloud.pl` en lugar del habitual `show techsupport`.

- Después de eliminar una VM de NetScaler de la consola de GCP, elimine también la instancia de destino interna de NetScaler asociada. Para hacerlo, vaya a la CLI de gcloud y escriba el siguiente comando:

```
1 gcloud compute -q target-instances delete <instance-name>-  
  adcinternal --zone <zone>
```

Nota:

<instance-name>-adcinternal es el nombre de la instancia de destino que se debe eliminar.

Licencias de NetScaler VPX

Una instancia de NetScaler VPX en GCP requiere una licencia. Las siguientes opciones de licencia están disponibles para las instancias de NetScaler VPX que se ejecutan en GCP.

- **Licencias basadas en suscripción:** los dispositivos NetScaler VPX están disponibles como instancias de pago en el mercado de GCP. Las licencias basadas en suscripciones son una opción de pago por uso. A los usuarios se les cobra cada hora. Los siguientes modelos VPX y ediciones de licencias están disponibles en el mercado de GCP.

Rendimiento VPX compatible

NetScaler VPX Advanced: 200 Mbps

NetScaler VPX Premium: 1 Gbps

NetScaler VPX Premium: 5 Gbps

NetScaler VPX Express: 20 Mbps

NetScaler VPX: licencia de cliente

NetScaler VPX FIPS: licencia del cliente

- **Traiga su propia licencia (BYOL):** Si trae su propia licencia (BYOL), consulte la Guía de licencias de VPX en <http://support.citrix.com/article/CTX122426> Es necesario que:
 - Utilice el portal de licencias del sitio web de Citrix para generar una licencia válida.
 - Cargue la licencia en la instancia.
- Licencias de **Check-in/Check-out de NetScaler VPX:** Para obtener más información, consulte **Licencias de Check-in/Check-out de NetScaler VPX.**

VPX Express para implementaciones locales y en la nube no requiere un archivo de licencia. Para obtener más información sobre NetScaler VPX Express, consulte la sección “Licencia de NetScaler VPX Express” de la [descripción general de licencias de NetScaler](#).

Plantillas GDM para implementar una instancia de NetScaler VPX

Puedes usar una plantilla de Google Deployment Manager (GDM) de NetScaler VPX para implementar una instancia VPX en GCP. Para obtener más información, consulte [Plantillas GDM de NetScaler](#).

Imágenes de NetScaler Marketplace

Puede utilizar las imágenes de las plantillas de GDM para abrir el dispositivo NetScaler.

En la siguiente tabla se enumeran las imágenes que están disponibles en el sitio web de GCP.

Versión	Nombre de imagen	Ubicación de la imagen
14.1	citrix-adc-vpx-express-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-express-14-1-21-57
14.1	citrix-adc-vpx-200-enterprise-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-14-1-21-57
14.1	citrix-adc-vpx-1000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-platinum-14-1-21-57
14.1	citrix-adc-vpx-5000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-14-1-21-57
14.1	citrix-adc-vpx-byol-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-14-1-21-57

Recursos

- [Creación de instancias con múltiples interfaces de red](#)
- [Creación e inicio de una instancia de VM](#)

Información relacionada

- [Implementar un par de VPX de alta disponibilidad en Google Cloud Platform](#)

Implementar un par de VPX de alta disponibilidad en Google Cloud Platform

October 17, 2024

Puede configurar dos instancias de NetScaler VPX en Google Cloud Platform (GCP) como un par activo-pasivo de alta disponibilidad (HA). Al configurar una instancia como nodo principal y la otra como nodo secundario, el nodo principal acepta las conexiones y administra los servidores. El nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario se hace cargo.

Para obtener más información sobre HA, consulte [Alta disponibilidad](#).

Los nodos deben estar en la misma región; sin embargo, pueden estar en la misma zona o en zonas diferentes. Para obtener más información, consulte [Regiones y zonas](#).

Cada instancia VPX requiere al menos tres subredes IP (redes de Google VPC):

- Una subred de administración
- Una subred (VIP) orientada al cliente
- Una subred orientada al back-end (SNIP, MIP, etc.)

Citrix recomienda tres interfaces de red para una instancia de VPX estándar.

Puede implementar un par de alta disponibilidad VPX mediante los siguientes métodos:

- [Uso de una dirección IP estática externa](#)
- [Uso de una dirección IP privada](#)
- [Uso de máquinas virtuales de una sola NIC con dirección IP privada](#)

Plantillas de GDM para implementar un par de alta disponibilidad VPX en GCP

Puede utilizar una plantilla de NetScaler Google Deployment Manager (GDM) para implementar un par de alta disponibilidad VPX en GCP. Para obtener más información, consulte [Plantillas GDM de NetScaler](#).

Compatibilidad con reglas de reenvío para el par de alta disponibilidad VPX en GCP

Puede implementar un par de alta disponibilidad VPX en el GCP mediante reglas de reenvío.

Para obtener más información sobre las reglas de reenvío, consulte [Descripción general de las reglas de reenvío](#).

Requisitos previos

- Las reglas de reenvío deben estar en la misma región que las instancias VPX.
- Las instancias de destino deben estar en la misma zona que la instancia VPX.
- El número de instancias de destino para los nodos principal y secundario debe coincidir.

Ejemplo

Tiene un par de alta disponibilidad en la región `us-east1` con VPX principal en la zona `us-east1-b` y VPX secundario en la zona `us-east1-c`. Se configura una regla de reenvío para la VPX principal con la instancia de destino en la zona `us-east1-b`. Configure una instancia de destino para la VPX secundaria en la zona `us-east1-c` a fin de actualizar la regla de reenvío en caso de conmutación por error.

Limitaciones

La implementación de alta disponibilidad de VPX solo admite las reglas de reenvío configuradas con instancias de destino en el back-end.

Implementar un par de alta disponibilidad VPX con dirección IP estática externa en Google Cloud Platform

October 17, 2024

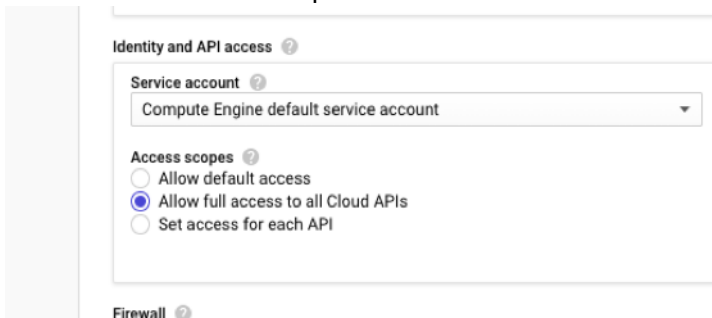
Puede implementar un par de alta disponibilidad VPX en GCP mediante una dirección IP estática externa. La dirección IP del cliente del nodo principal debe estar enlazada a una dirección IP estática externa. Tras la conmutación por error, la dirección IP estática externa se mueve al nodo secundario para que se reanude el tráfico.

Una dirección IP externa estática es una dirección IP externa que está reservada para su proyecto hasta que decida liberarla. Si utiliza una dirección IP para acceder a un servicio, puede reservar esa dirección IP para que solo su proyecto pueda utilizarla. Para obtener más información, consulte [Reserva de una dirección IP externa estática](#).

Para obtener más información sobre HA, consulte [Alta disponibilidad](#).

Antes de comenzar

- Lea la Limitación, los requisitos de hardware y los Puntos a tener en cuenta mencionados en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#). Esta información se aplica también a implementaciones de alta disponibilidad.
- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que el rol de IAM asociado a su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```

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 has configurado direcciones IP de alias en una interfaz distinta de la interfaz de administración, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM adicionales:

```

1  "compute.instances.updateNetworkInterface"

```

- Si ha configurado reglas de reenvío de GCP en el nodo principal, lea las limitaciones y los requisitos mencionados en [Compatibilidad de reglas de reenvío para el par de alta disponibilidad VPX en GCP](#) para actualizarlas al nuevo nodo principal en caso de conmutación por error.

Cómo implementar un par VPX HA en Google Cloud Platform

Este es un resumen de los pasos de implementación de alta disponibilidad:

1. Cree redes de VPC en la misma región. Por ejemplo, Asia-este.
2. Cree dos instancias VPX (nodos primario y secundario) en la misma región. Pueden estar en la misma zona o diferentes zonas. Por ejemplo, Asia east-1a y Asia East-1B.
3. Configure la configuración de HA en ambas instancias mediante los comandos de NetScaler GUI o ADC CLI.

Paso 1. Creación de redes de VPC

Cree redes de VPC en función de sus requisitos. Citrix recomienda crear tres redes de VPC para asociarse con NIC de administración, NIC cliente y NIC de servidor.

Para crear una red VPC, lleve a cabo estos pasos:

1. Inicie sesión en la **consola de Google > Redes > Red VPC > Crear red VPC**.
2. Complete los campos obligatorios y haga clic en **Crear**.

Para obtener más información, consulte la sección **Crear redes VPC** en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#).

Paso 2. Paso 2: Crear dos instancias VPX

Cree dos instancias VPX siguiendo los pasos que se indican en [Escenario: implementar una instancia VPX independiente con múltiples NIC y múltiples IP](#).

Importante:

Asigne una dirección IP externa estática a la dirección IP del cliente (VIP) del nodo principal. Puede utilizar una dirección IP reservada existente o crear una nueva. Para crear una dirección IP externa estática, vaya a **Interfaz de red > IP externa** y haga clic en **Crear dirección IP**.

Network interface

Network
clientvpc-ss

Subnetwork
clientvpc-ss-subnet

Internal IP
[Redacted]

Internal IP type
Ephemeral

∨ Show alias IP ranges

External IP ?

- None
- Ephemeral
- vpxpublic (35.229.255.208)
Premium tier

Create IP address

Después de la conmutación por error, cuando el principal antiguo se convierte en el nuevo secundario, la dirección IP externa estática se mueve desde el primario antiguo y se adjunta al nuevo primario. Para obtener más información, consulta el documento de Google Cloud [Reservar una dirección IP externa estática](#).

Después de configurar las instancias VPX, puede configurar las direcciones VIP y SNIP. Para obtener más información, consulte [Configuración de direcciones IP propiedad de NetScaler](#).

Paso 3. Paso 3: Configurar alta disponibilidad

Después de crear las instancias en Google Cloud Platform, puede configurar HA mediante la GUI de NetScaler para CLI.

Configurar HA mediante la interfaz gráfica de usuario Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo secundario.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.



En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP de nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo principal.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

Antes de continuar, asegúrese de que el estado Sincronización del nodo secundario se muestre como **CORRECTO** en la página **Nodos**.

System / High Availability / Nodes

Nodes 2

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REASON
<input type="checkbox"/>	0	192.168.1.3		Primary	● UP	ENABLED	ENABLED	-NA-
<input type="checkbox"/>	1	192.168.1.66		Secondary	● UP	ENABLED	SUCCESS	-NA-

Total 2

25 Per Page Page 1 of 1

Nota:

Ahora, el nodo secundario tiene las mismas credenciales de inicio de sesión que el nodo principal.

Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambos nodos.

En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP principal siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia principal y la máscara de red configurada para la subred cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Agregue una dirección SNIP principal siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia principal y la máscara de red configurada para la subred del servidor en la instancia principal.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.
4. Agregue una dirección VIP secundaria siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria y la máscara de red configurada para la subred cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.

IPs

IPv4s 4 IPv6s 1

Add Edit Delete Statistics Select Action

Click here to search or you can enter Key : Value format

	IP ADDRESS	STATE	TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	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

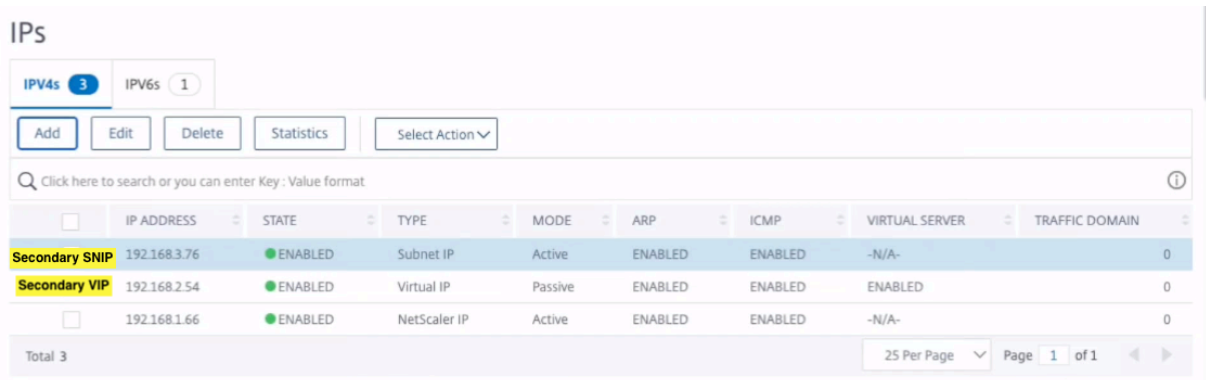
Total 4

25 Per Page Page 1 of 1

En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Agregue una dirección VIP secundaria siguiendo estos pasos:
 - a) Introduzca la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria y la máscara de red configurada para la subred cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
3. Agregue una dirección SNIP secundaria siguiendo estos pasos:

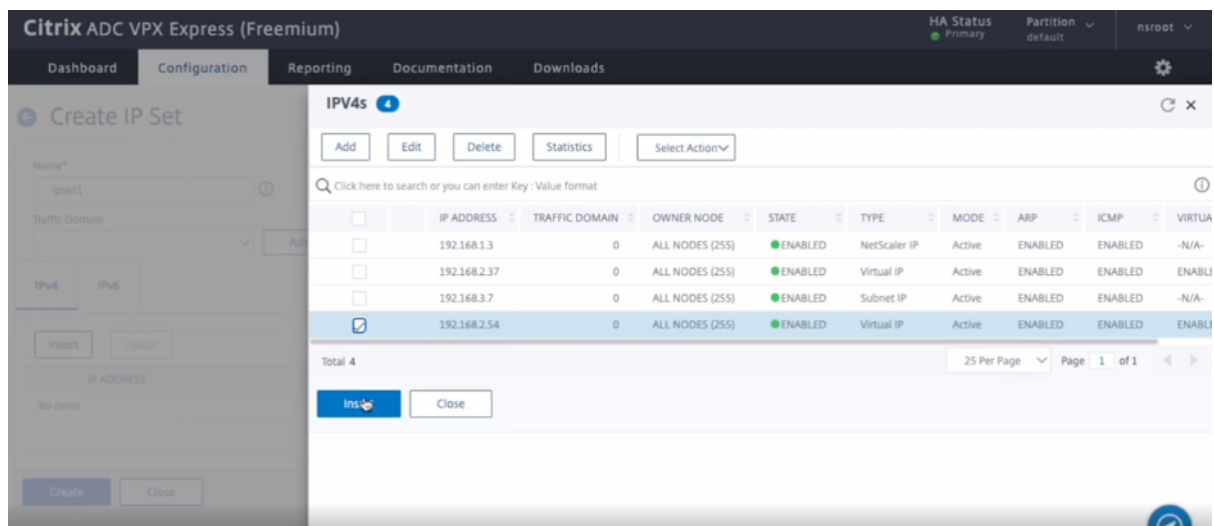
- a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor en la instancia secundaria.
- b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
- c) Haga clic en **Create**.



Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP al VIP secundario en ambas instancias.

En el **nodo principal**, lleve a cabo los siguientes pasos:

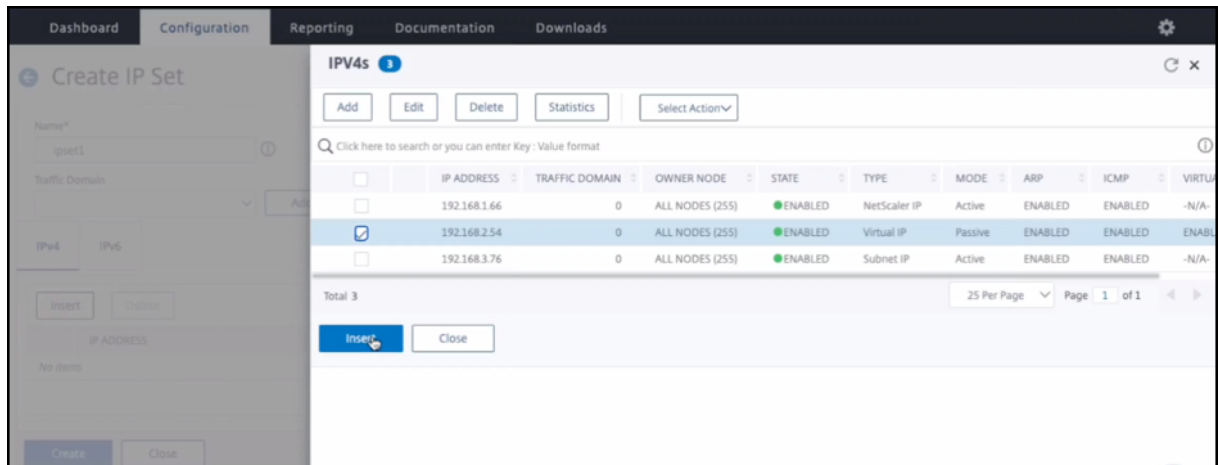
1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.
4. Haga clic en **Crear** para crear el conjunto de IP.



En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > Conjuntos de IP > Agregar**.
2. Agregue un nombre de conjunto de IP y haga clic en **Insertar**.
3. En la página **IPv4**, seleccione la IP virtual (VIP secundaria) y haga clic en **Insertar**.

4. Haga clic en **Crear** para crear el conjunto de IP.

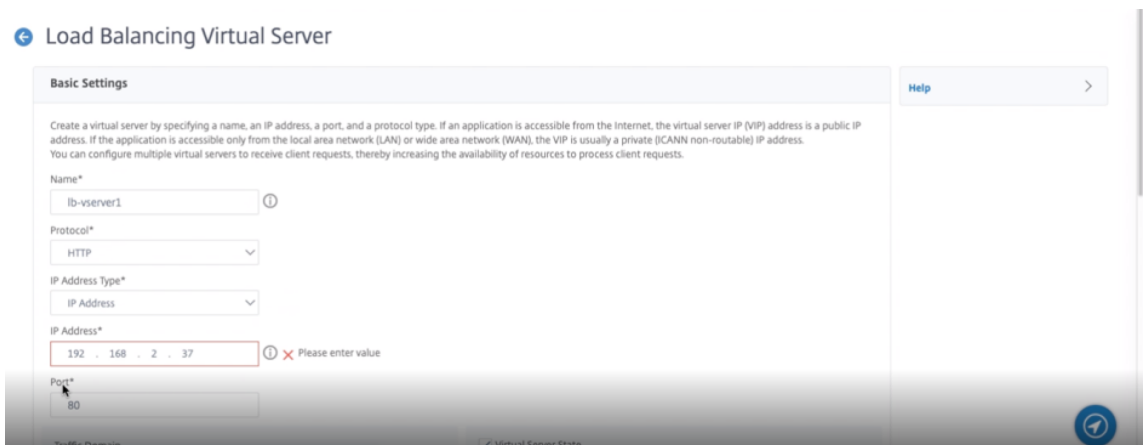


Nota:

El nombre del conjunto de IP debe ser el mismo en ambas instancias.

Paso 4. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga de la instancia principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar.**
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), dirección IP (VIP principal) y Puerto.



3. Haga clic en **Más**. Vaya a **Configuración del conjunto de IP de rango IP**, seleccione **IPset** en el menú desplegable y proporcione el IPset creado en el **paso 3**.
4. Haga clic en **Aceptar** para crear el servidor virtual de equilibrio de carga.

Paso 5. Agregue un servicio o grupo de servicios en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 6. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 4** y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 5** y haga clic en **Enlazar**.

Verifique la configuración. Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario. La IP estática externa de la antigua VIP principal se mueve a la nueva VIP secundaria.

Configurar la alta disponibilidad mediante CLI Paso 1. Configure la alta disponibilidad en modo INC en ambas instancias.

En el nodo principal, escriba el siguiente comando.

```
1 add ha node 1 <sec_ip> -inc ENABLED
```

En el nodo secundario, escriba el siguiente comando.

```
1 add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo secundario.

`prim_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo principal.

Paso 2. Agregue IP virtuales y de subred en ambos nodos.

En el nodo principal, escriba el siguiente comando.

```
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` hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia principal.

`secondary_vip` hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria.

`primary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia principal.

En el nodo secundario, escriba el siguiente comando.

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_vip` hace referencia a la dirección IP interna de la interfaz orientada al cliente de la instancia secundaria.

`secondary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria.

Paso 3. Agregue un conjunto de IP y vincule el conjunto de IP al VIP secundario en ambas instancias.

En el nodo principal, escriba el siguiente comando:

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
```

En el nodo secundario, escriba el siguiente comando:

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
```

Nota:

El nombre del conjunto de IP debe ser el mismo en ambas instancias.

Paso 4. Agregue un servidor virtual en la instancia principal.

Escriba este comando:

```
1 add <server_type> vserver <vserver_name> <protocol> <primary_vip> <
   port> -ipset <ipset_name>
```

Paso 5. Agregue un servicio o grupo de servicios en la instancia principal.

Escriba este comando:

```
1 add service <service_name> <service_ip_address> <protocol> <port>
```

Paso 6. Vincule el grupo de servicio/servicio al servidor virtual de equilibrio de carga de la instancia principal.

Escriba este comando:

```
1 bind <server_type> vserver <vserver_name> <service_name>
```

Nota:

Para guardar la configuración, escriba el comando `save config`. De lo contrario, las configuraciones se pierden después de reiniciar las instancias.

Paso 7. Verifique la configuración.

Asegúrese de que la dirección IP externa asociada a la NIC cliente principal se traslada a la secundaria en caso de failover.

1. Realice una solicitud cURL a la dirección IP externa y asegúrese de que se pueda acceder a ella.
2. En la instancia principal, realice la conmutación por error:

Desde GUI, vaya a **Configuración > Sistema > Alta disponibilidad > Acción > Forzar conmutación por error**.

En CLI, escriba el siguiente comando:

```
1 force ha failover -f
```

En la consola de GCP, vaya a la instancia secundaria. La dirección IP externa debe haberse trasladado a la NIC cliente o secundaria tras la conmutación por error.

3. Emita una solicitud cURL a la IP externa y asegúrese de que se pueda volver a acceder a ella.

Implemente un único par de NIC VPX de alta disponibilidad con dirección IP privada en Google Cloud Platform

October 17, 2024

Puedes implementar un único par de NIC VPX de alta disponibilidad en GCP mediante una dirección IP privada. La dirección IP (VIP) del cliente debe configurarse como dirección IP de alias en el nodo principal. Tras la conmutación por error, la dirección IP del cliente se mueve al nodo secundario para que el tráfico se reanude. Las direcciones IP de subred (SNIP) de cada nodo también deben configurarse como un intervalo de direcciones IP de alias.

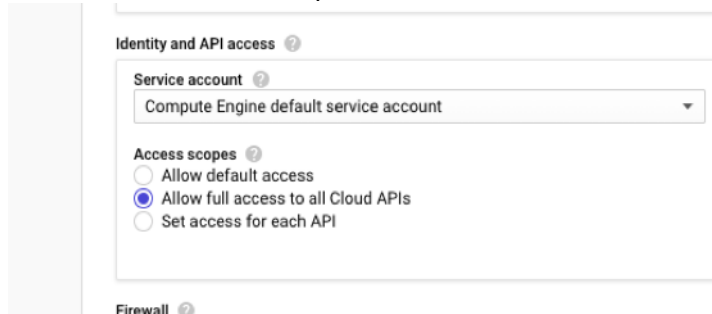
Para obtener más información sobre la alta disponibilidad, consulte [Alta disponibilidad](#).

Antes de comenzar

- Lea la Limitación, los requisitos de hardware y los Puntos a tener en cuenta mencionados en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#). Esta información se

aplica también a las implementaciones de alta disponibilidad.

- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

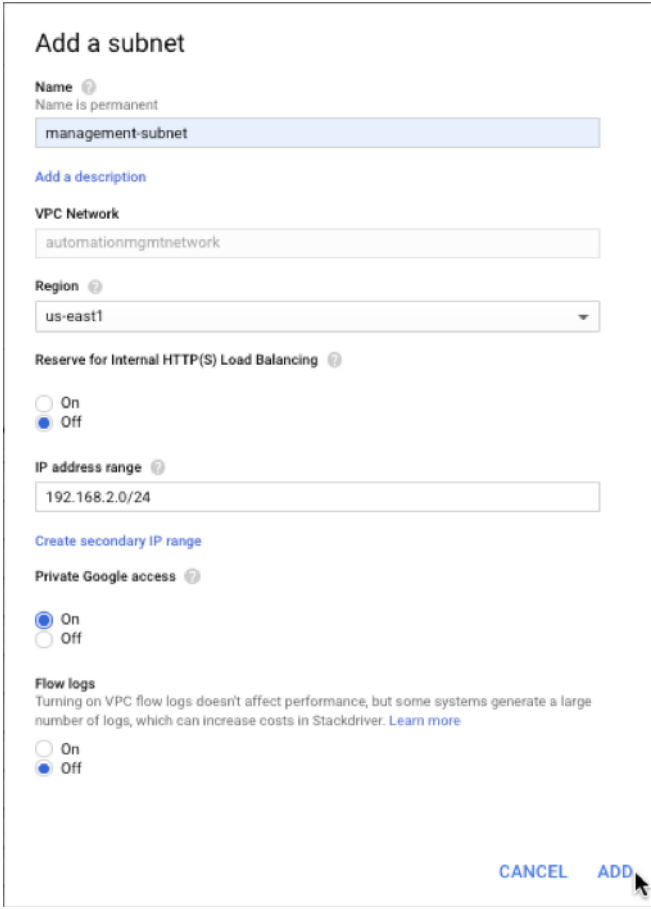
```

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 sus máquinas virtuales no tienen acceso a Internet, debe habilitar **Private Google Access** en

la subred de la VPC.



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

CANCEL **ADD**

- Si ha configurado reglas de reenvío de GCP en el nodo principal, lea las limitaciones y los requisitos mencionados en [Compatibilidad de reglas de reenvío para el par de alta disponibilidad VPX en GCP](#) para actualizarlas al nuevo nodo principal en caso de conmutación por error.

Cómo implementar un par de alta disponibilidad VPX en Google Cloud Platform

Este es un resumen de los pasos para implementar un par de HA con una sola NIC:

1. Cree una red de VPC.
2. Crea dos instancias VPX (nodos principal y secundario) en la misma región. Pueden estar en la misma zona o diferentes zonas. Por ejemplo, Asia east-1a y Asia East-1B.
3. Configure la configuración de HA en ambas instancias mediante los comandos de NetScaler GUI o ADC CLI.

Paso 1. Crear una red de VPC

Para crear una red VPC, lleve a cabo estos pasos:

1. Inicia sesión en la **consola de Google > Redes > Red de VPC > Crear red de VPC**.

2. Complete los campos obligatorios y haga clic en **Crear**.

Para obtener más información, consulte la sección **Crear redes VPC** en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#).

Paso 2. Paso 2: Crear dos instancias VPX

Cree dos instancias VPX siguiendo los pasos 1 al 3 que se detallan en [Escenario: Implementar una instancia VPX independiente con una sola NIC](#).

Importante:

Asigne una dirección IP de alias de cliente únicamente al nodo principal y direcciones IP de alias de servidor a los nodos principal y secundario. No utilice la dirección IP interna de la instancia VPX para configurar el VIP o el SNIP.

Para crear direcciones IP de alias de cliente y servidor, realice estos pasos en el nodo principal:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz del cliente (NIC0).
3. En el campo **Intervalo de IP de alias**, introduzca la dirección IP del alias del cliente.
4. Haga clic en **Agregar intervalo de IP** e introduzca la dirección IP del alias del servidor.

Para crear una dirección IP de alias de servidor, realice estos pasos en el nodo secundario:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz del cliente (NIC0).
3. En el campo **Intervalo de IP de alias**, introduzca la dirección IP del alias del servidor.

Network interface

You must stop the VM instance to edit network, subnetwork or internal IP address

Network ?
automationmgmtnetwork

Subnetwork ?
mgmtsubnet (192.168.1.0/24, us-east1)

Internal IP
192.168.1.76

Internal IP type
Ephemeral

Alias IP ranges

Subnet range
Primary (192.168.1.0/24)

Alias IP range ?
192.168.1.7/32

Secondary Subnet IP(SNIP)

+ Add IP range

⤴ Hide alias IP ranges

External IP ?
Ephemeral

Network Service Tier ?
 Premium (Current project-level tier, change) ?
 Standard (us-east1) ?

IP forwarding
Off

Public DNS PTR Record ?
 Enable
 PTR domain name

Done Cancel

Tras la conmutación por error, cuando el antiguo principal se convierte en el nuevo secundario, la dirección IP del alias del cliente se mueve del principal anterior y se adjunta al nuevo principal.

Después de configurar las instancias VPX, puede configurar las direcciones IP virtual (VIP) y de sub-red (SNIP). Para obtener más información, consulte [Configuración de direcciones IP propiedad de NetScaler](#).

Paso 3. Paso 3: Configurar alta disponibilidad

Después de crear las instancias en Google Cloud Platform, puede configurar la alta disponibilidad mediante la GUI o CLI de NetScaler.

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

Paso 1. Configure la alta disponibilidad en el modo Enabled INC en ambos nodos.

En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo secundario.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario `nsroot` y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP de nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo principal.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

Antes de continuar, asegúrese de que el estado Sincronización del nodo secundario se muestre como **CORRECTO** en la página **Nodos**.

System > High Availability > Nodes

Nodos 2

	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REA
<input type="checkbox"/>	0	192.168.1.71		Primary	● UP	ENABLED	ENABLED	-NA-
<input type="checkbox"/>	1	192.168.1.76		Secondary	● UP	ENABLED	SUCCESS	-NA-

Total 2

25 Per Page Page 1 of 1

Nota:

Una vez sincronizado el nodo secundario con el nodo principal, el nodo secundario tiene las mismas credenciales de inicio de sesión que el nodo principal.

Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambos nodos.

En el nodo principal, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:
 - a) Introduzca la dirección IP y la máscara de red del alias del cliente configuradas para la subred de VPC en la instancia de máquina virtual principal.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Para crear una dirección IP de alias de servidor (SNIP):
 - a) Introduzca la dirección IP y la máscara de red del alias del servidor configuradas para la subred de VPC en la instancia de máquina virtual principal.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.

System > Network > IPs > IPv4s

IPs 🔄 📄

IPv4s **3** IPv6s **1**

Add Edit Delete Statistics Select Action

🔍 Click here to search or you can enter Key: Value format ⓘ

<input type="checkbox"/>	IP ADDRESS	STATE	TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	TRAFFIC DOMAIN
<input checked="" type="checkbox"/>	192.168.1.6	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
<input checked="" type="checkbox"/>	192.168.1.5	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0
<input type="checkbox"/>	192.168.1.71	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0

Total 3 25 Per Page Page 1 of 1

En el nodo secundario, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:
 - a) Introduzca la dirección IP y la máscara de red del alias del cliente configuradas para la subred de VPC de la instancia de máquina virtual principal.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Para crear una dirección IP de alias de servidor (SNIP):
 - a) Introduzca la dirección IP y la máscara de red del alias del servidor configuradas para la subred de VPC de la instancia de máquina virtual secundaria.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.

System > Network > IPs > IPv4s

IPs

IPv4s 3 IPv6s 1

Add Edit Delete Statistics Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	IP ADDRESS	STATE	TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	TRAFFIC DOMAIN
<input type="checkbox"/>	192.168.1.7	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
<input type="checkbox"/>	192.168.1.76	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
<input checked="" type="checkbox"/>	192.168.1.5	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED	0

Total 3

25 Per Page Page 1 of 1

Paso 3. Agregue un servidor virtual de equilibrio de carga en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (dirección IP del alias del cliente principal) y Puerto, y haga clic en **Aceptar**.

↳ 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 application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP 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*
lb-vserver1 ⓘ

Protocol*
HTTP

IP Address Type*
IP Address

IP Address*
192.168.1.5 ⓘ

Port*
80

▶ More

OK Cancel

Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 3** y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 4** y haga clic en **Enlazar**.

Paso 6. Verifique la configuración.

Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario. El alias de cliente IP (VIP) del antiguo principal se mueve al nuevo principal.

Configurar la alta disponibilidad mediante la CLI

Paso 1. Configure la alta disponibilidad en modo **habilitado para INC** en ambas instancias mediante la CLI de NetScaler.

En el nodo principal, escriba el siguiente comando.

```
1 add ha node 1 <sec_ip> -inc ENABLED
```

En el nodo secundario, escriba el siguiente comando.

```
1 add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo secundario.

`prim_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo principal.

Paso 2. Agregue VIP y SNIP en los nodos principal y secundario.

Escriba los siguientes comandos en el nodo principal:

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

Nota:

Introduzca el alias, la dirección IP y la máscara de red configuradas para la subred del cliente en la instancia de máquina virtual.

```
1 add ns ip <primary_server_alias_ip> <subnet> -type SNIP
```

Escriba los siguientes comandos en el nodo secundario:

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

Nota:

Introduzca el alias, la dirección IP y la máscara de red configuradas para la subred del cliente en la instancia de máquina virtual.

```
1 add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```

Nota:

Introduzca el alias, la dirección IP y la máscara de red configuradas para la subred del servidor en la instancia de máquina virtual.

Paso 3. Agregue un servidor virtual en el nodo principal.

Escriba este comando:

```
1 add <server_type> vserver <vserver_name> <protocol> <
  primary_client_alias_ip> <port>
```

Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

Escriba este comando:

```
1 add service <service_name> <service_ip_address> <protocol> <port>
```

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

Escriba este comando:

```
1 bind <server_type> vserver <vserver_name> <service_name>
```

Nota:

Para guardar la configuración, escriba el comando `save config`. De lo contrario, las configuraciones se pierden después de reiniciar las instancias.

Implementar un par VPX de alta disponibilidad con una dirección IP privada en Google Cloud Platform

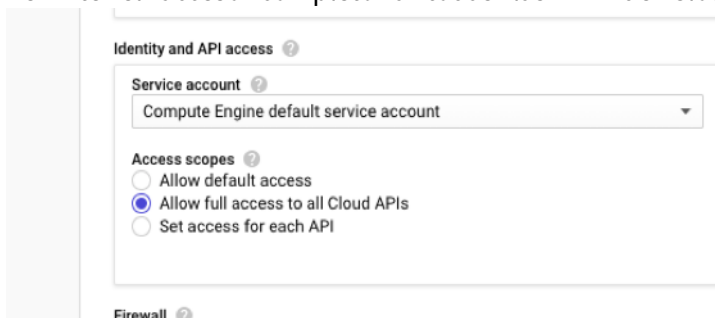
October 17, 2024

Puede implementar un par de alta disponibilidad VPX en GCP mediante una dirección IP privada. La IP del cliente (VIP) debe configurarse como dirección IP de alias en el nodo principal. Tras la conmutación por error, la dirección IP del cliente se mueve al nodo secundario para que el tráfico se reanude.

Para obtener más información sobre la alta disponibilidad, consulte [Alta disponibilidad](#).

Antes de comenzar

- Lea la Limitación, los requisitos de hardware y los Puntos a tener en cuenta mencionados en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#). Esta información se aplica también a las implementaciones de alta disponibilidad.
- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
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 ha configurado direcciones IP externas en una interfaz distinta de la interfaz de administración, asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM adicionales:

```
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 sus máquinas virtuales no tienen acceso a Internet, debe habilitar **Private Google Access** en

The screenshot shows the 'Add a subnet' configuration interface. The 'Name' field is set to 'management-subnet'. The 'VPC Network' is 'automationmgmtnetwork' and the 'Region' is 'us-east1'. The 'IP address range' is '192.168.2.0/24'. The 'Private Google access' checkbox is checked (On), and the 'Flow logs' checkbox is unchecked (Off). At the bottom right, there are 'CANCEL' and 'ADD' buttons.

la subred de administración.

- Si ha configurado reglas de reenvío de GCP en el nodo principal, lea las limitaciones y los requisitos mencionados en [Compatibilidad de reglas de reenvío para el par de alta disponibilidad VPX en GCP](#) para actualizarlas al nuevo nodo principal en caso de conmutación por error.

Cómo implementar un par de alta disponibilidad VPX en Google Cloud Platform

A continuación se presenta un resumen de los pasos de implementación de alta disponibilidad:

1. Cree redes de VPC en la misma región. Por ejemplo, Asia-este.
2. Cree dos instancias VPX (nodos primario y secundario) en la misma región. Pueden estar en la misma zona o diferentes zonas. Por ejemplo, Asia east-1a y Asia East-1B.
3. Configure los ajustes de alta disponibilidad en ambas instancias mediante los comandos de la GUI de NetScaler o de la CLI de ADC.

Paso 1. Creación de redes de VPC

Cree redes de VPC en función de sus requisitos. Citrix recomienda crear tres redes de VPC para asociarse con NIC de administración, NIC cliente y NIC de servidor.

Para crear una red VPC, lleve a cabo estos pasos:

1. Inicie sesión en la **consola de Google > Redes > Red VPC > Crear red VPC**.
2. Complete los campos obligatorios y haga clic en **Crear**.

Para obtener más información, consulte la sección **Crear redes VPC** en [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#).

Paso 2. Paso 2: Crear dos instancias VPX

Cree dos instancias VPX siguiendo los pasos que se indican en [Escenario: implementar una instancia VPX independiente con múltiples NIC y múltiples IP](#).

Importante:

Asigne una dirección IP de alias de cliente al nodo principal. No utilice la dirección IP interna de la instancia VPX para configurar el VIP.

Para crear una dirección IP de alias de cliente, realice estos pasos:

1. Vaya a la instancia de VM y haga clic en **Modificar**.
2. En la ventana **Interfaz de red**, modifique la interfaz del cliente.
3. En el campo **Intervalo de IP de alias**, introduzca la dirección IP del alias del cliente.

VM instance details

Creation time
Jan 16, 2020, 4:00:22 PM

Network interfaces

nic0: automationmgmtnetwork mgmtsubnet

Network interface

Network
automationclientnetwork

Subnetwork
clientsubnet

Internal IP
192.168.2.65

Internal IP type
Ephemeral

Alias IP ranges

Subnet range
Primary (192.168.2.0/24)

Alias IP range
Example: 10.0.1.0/24 or /32

+ Add IP range

Hide alias IP ranges

External IP
None

Done Cancel

nic2: automationservernetwork serversubnet

Network interfaces		Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	—	adc-ha-instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	—	None			View details

Después de la conmutación por error, cuando el primario anterior se convierte en el nuevo secundario, las direcciones IP de alias se mueven del principal anterior y se adjuntan al nuevo primario.

Después de configurar las instancias VPX, puede configurar las direcciones IP virtual (VIP) y de subred (SNIP). Para obtener más información, consulte [Configuración de direcciones IP propiedad de NetScaler](#).

Paso 3. Paso 3: Configurar alta disponibilidad

Después de crear las instancias en Google Cloud Platform, puede configurar la alta disponibilidad mediante la GUI o CLI de NetScaler.

Configure la alta disponibilidad mediante la interfaz gráfica de usuario

Paso 1. Configure la alta disponibilidad en el modo Enabled INC en ambos nodos.

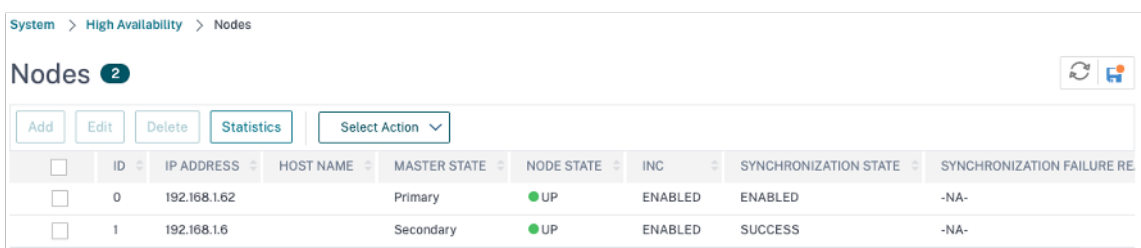
En el **nodo principal**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP del nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo secundario.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

En el **nodo secundario**, lleve a cabo los siguientes pasos:

1. Inicie sesión en la instancia con el nombre de usuario **nsroot** y el identificador de instancia del nodo desde la consola de GCP como contraseña.
2. Vaya a **Configuración > Sistema > Alta disponibilidad > Nodos** y haga clic en **Agregar**.
3. En el campo **Dirección IP de nodo remoto**, introduzca la dirección IP privada de la NIC de administración del nodo principal.
4. Active la casilla **Activar el modo INC (Configuración de red independiente) en el autonodo**.
5. Haga clic en **Create**.

Antes de continuar, asegúrese de que el estado Sincronización del nodo secundario se muestre como **CORRECTO** en la página **Nodos**.



<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE RE
<input type="checkbox"/>	0	192.168.1.62		Primary	UP	ENABLED	ENABLED	-NA-
<input type="checkbox"/>	1	192.168.1.6		Secondary	UP	ENABLED	SUCCESS	-NA-

Nota:

Una vez sincronizado el nodo secundario con el nodo principal, el nodo secundario tiene las mismas credenciales de inicio de sesión que el nodo principal.

Paso 2. Agregue la dirección IP virtual y la dirección IP de subred en ambos nodos.

En el nodo principal, lleve a cabo los siguientes pasos:

1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:

- a) Introduzca la dirección IP del alias y la máscara de red configuradas para la subred del cliente en la instancia de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP virtual** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Para crear una dirección IP del servidor (SNIP):
- a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia principal y la máscara de red configurada para la subred del servidor.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.

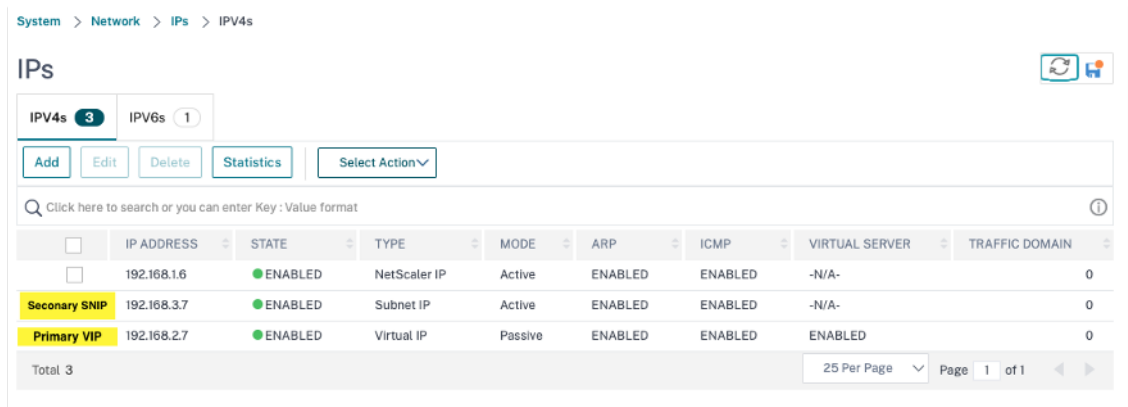
The screenshot shows the 'IPs' configuration page in NetScaler. It has tabs for 'IPv4s' (3) and 'IPv6s' (1). Below the tabs are buttons for 'Add', 'Edit', 'Delete', 'Statistics', and 'Select Action'. A search bar is present with the text 'Click here to search or you can enter Key: Value format'. Below the search bar is a table with the following data:

	IP ADDRESS	STATE	TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	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

At the bottom of the table, it shows 'Total 3' and pagination controls: '25 Per Page', 'Page 1 of 1'.

En el nodo secundario, lleve a cabo los siguientes pasos:

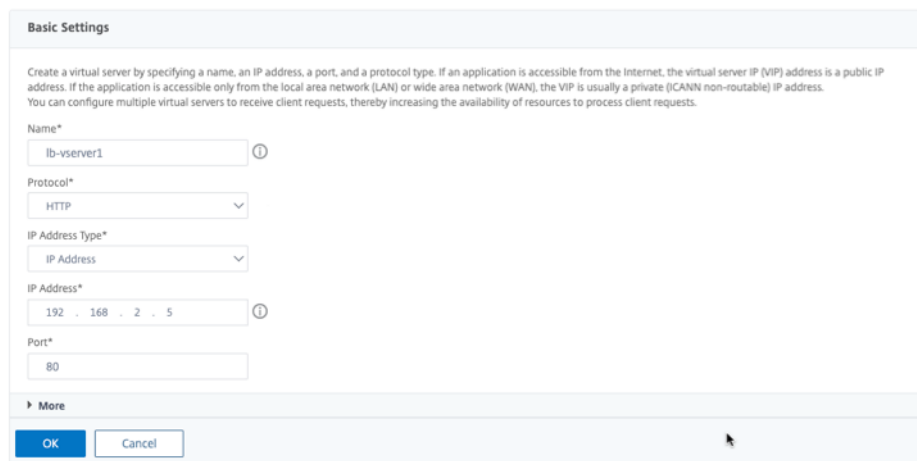
1. Vaya a **Sistema > Red > IPs > IPv4s** y haga clic en **Agregar**.
2. Para crear una dirección IP (VIP) de alias de cliente:
 - a) Introduzca la dirección IP de alias y la máscara de red configuradas para la subred cliente en la instancia principal de VM.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.
3. Para crear una dirección IP del servidor (SNIP):
 - a) Introduzca la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria y la máscara de red configurada para la subred del servidor.
 - b) En el campo **Tipo de IP**, seleccione **IP de subred** en el menú desplegable.
 - c) Haga clic en **Create**.



Paso 3. Agregue un servidor virtual de equilibrio de carga en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.
2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (dirección IP del alias del cliente principal) y Puerto, y haga clic en **Aceptar**.

Load Balancing Virtual Server



Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 3** y haga clic en **Modificar**.
3. En la ficha **Grupos de servicios y servicios**, haga clic en **Enlace de servicio de servidor virtual sin equilibrio de carga**.
4. Seleccione el servicio configurado en el **paso 4** y haga clic en **Enlazar**.

Paso 5. Verifique la configuración.

Después de una conmutación por error forzada, el secundario se convierte en el nuevo primario. La IP del alias de cliente (VIP) y la IP del alias del servidor (SNIP) de la antigua primaria se trasladan al nuevo principal.

Configurar la alta disponibilidad mediante la CLI

Paso 1. Configure la alta disponibilidad en modo **habilitado para INC** en ambas instancias mediante la CLI de NetScaler.

En el nodo principal, escriba el siguiente comando.

```
1 add ha node 1 <sec_ip> -inc ENABLED
```

En el nodo secundario, escriba el siguiente comando.

```
1 add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo secundario.

`prim_ip` hace referencia a la dirección IP interna de la NIC de administración del nodo principal.

Paso 2. Agrega VIP y SNIP en ambos nodos.

Escriba los siguientes comandos en el nodo principal:

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

Nota:

Introduzca la dirección IP del alias y la máscara de red configuradas para la subred del cliente en la instancia de VM.

```
1 add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia principal.

Escriba los siguientes comandos en el nodo secundario:

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

Nota:

Introduzca la dirección IP de alias y la máscara de red configuradas para la subred cliente en la instancia principal de VM.

```
1 add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_snip` hace referencia a la dirección IP interna de la interfaz orientada al servidor de la instancia secundaria.

Nota:

Introduzca la dirección IP y la máscara de red configuradas para la subred del servidor en la instancia de VM.

Paso 3. Agregue un servidor virtual en el nodo principal.

Escriba este comando:

```
1 add <server_type> vserver <vserver_name> <protocol> <
  primary_client_alias_ip> <port>
```

Paso 4. Agregue un servicio o grupo de servicios en el nodo principal.

Escriba este comando:

```
1 add service <service_name> <service_ip_address> <protocol> <port>
```

Paso 5. Vincule el servicio o grupo de servicios al servidor virtual de equilibrio de carga del nodo principal.

Escriba este comando:

```
1 bind <server_type> vserver <vserver_name> <service_name>
```

Nota:

Para guardar la configuración, escriba el comando `save config`. De lo contrario, las configuraciones se pierden después de reiniciar las instancias.

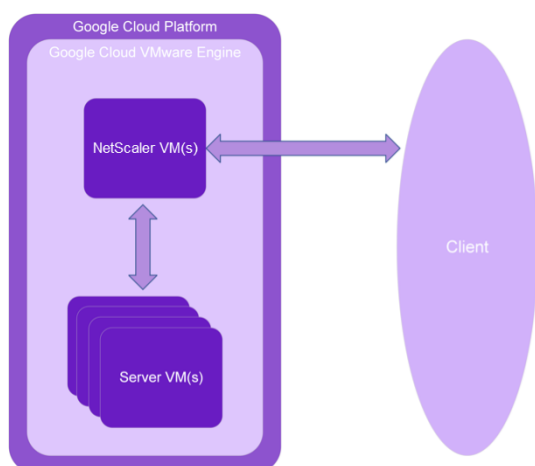
Instalar una instancia de NetScaler VPX en VMware Engine de Google Cloud

October 17, 2024

VMware Engine de Google Cloud (GCVE) le proporciona nubes privadas que contienen clústeres de vSphere, creados a partir de una infraestructura básica dedicada de Google Cloud Platform. La implementación inicial mínima es de tres hosts, pero se pueden agregar hosts adicionales de uno en uno. Todas las nubes privadas aprovisionadas tienen vCenter Server, vSAN, vSphere y NSX-T.

GCVE le permite crear centros de datos definidos por software (SDDC) en la nube en Google Cloud Platform con la cantidad deseada de hosts ESX. GCVE admite las implementaciones de NetScaler VPX. GCVE proporciona una interfaz de usuario igual a la de vCenter local. Funciona de manera idéntica a las implementaciones de NetScaler VPX basadas en ESX.

El siguiente diagrama muestra el GCVE en Google Cloud Platform al que un administrador o un cliente pueden acceder a través de Internet. Un administrador puede crear, administrar y configurar máquinas virtuales de servidores o cargas de trabajo mediante GCVE. El administrador puede acceder al vCenter y al NSX-T Manager basados en la web del GCVE mediante una conexión OpenVPN. Puede crear las instancias NetScaler VPX (independientes o pares de HA) y las máquinas virtuales de servidor dentro de GCVE mediante vCenter y administrar las redes correspondientes mediante NSX-T Manager. La instancia de NetScaler VPX en GCVE funciona de manera similar al clúster de hosts de VMware local. GCVE se puede administrar mediante una conexión OpenVPN a la infraestructura de administración.



Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, haga lo siguiente:

- Para obtener más información sobre VMware Engine de Google Cloud y sus requisitos previos, consulta la [documentación de VMware Engine de Google Cloud](#).
- Para obtener más información sobre la implementación de VMware Engine de Google Cloud, consulta [Implementar una nube privada de VMware Engine de Google Cloud](#).
- Para obtener más información sobre cómo conectarse a su nube privada mediante una puerta de enlace VPN de punto a sitio para acceder a VMware Engine de Google Cloud y administrarlo,

consulta [Acceder a una nube privada de VMware Engine de Google Cloud](#).

- En la máquina cliente VPN, descargue los archivos de configuración del dispositivo NetScaler VPX.
- Cree segmentos de red NSX-T apropiados en el SDDC de VMware al que se conectan las máquinas virtuales. Para obtener más información, consulta [Agregar un segmento de red en VMware Engine de Google Cloud](#).
- Obtenga archivos de licencias VPX. Para obtener más información sobre las licencias de instancia de NetScaler VPX, consulte [Descripción general de las licencias](#).
- Las máquinas virtuales (VM) creadas o migradas a la nube privada de GCVE deben estar conectadas a un segmento de red.

RequiVMware de hardware en la nube

En la tabla siguiente se enumeran los recursos informáticos virtuales que el SDDC de VMware debe proporcionar para cada dispositivo virtual VPX nCore.

Tabla 2. Recursos informáticos virtuales mínimos necesarios para ejecutar una instancia de NetScaler VPX

Componente	Requisito
Memoria	2 GB
CPU virtual (vCPU)	2
Interfaces de red virtual	En VMware SDDC, puede instalar un máximo de 10 interfaces de red virtuales si el hardware VPX se actualiza a la versión 7 o superior.
Espacio en disco	20 GB

Nota:

Esto se suma a cualquier requisito de disco para el Hypervisor.

Para el uso en producción del dispositivo virtual VPX, debe reservarse la asignación de memoria completa.

Requisitos del sistema OVF Tool 1.0

OVF Tool es una aplicación cliente que puede ejecutarse en sistemas Windows y Linux. En la siguiente tabla se describen los requisitos mínimos del sistema para instalar la herramienta OVF.

Tabla 2. Requisitos mínimos del sistema para la instalación de herramientas OVF

Componente	Requisito
Sistema operativo	Para conocer los requisitos detallados de VMware, busque el archivo PDF “Guía del usuario de herramientas OVF” en http://kb.vmware.com/ .
CPU	750 MHz como mínimo, se recomienda 1 GHz o más rápido
RAM	1 GB mínimo, 2 GB recomendado
NIC	NIC de 100 Mbps o más rápido

Para obtener información sobre la instalación de OVF, busque el archivo PDF “Guía del usuario de la herramienta OVF” en <http://kb.vmware.com/>.

Descarga de los archivos de configuración de NetScaler VPX

El paquete de configuración de instancias NetScaler VPX para VMware ESX sigue el estándar de formato Open Virtual Machine (OVF). Puede descargar los archivos desde el sitio web de Citrix. Necesita una cuenta de Citrix para iniciar sesión. Si no tiene una cuenta de Citrix, acceda a la página de inicio en <http://www.citrix.com>. Haga clic en el **vínculo Nuevos usuarios** y siga las instrucciones para crear una nueva cuenta de Citrix.

Una vez iniciada la sesión, navegue por la siguiente ruta desde la página principal de Citrix:

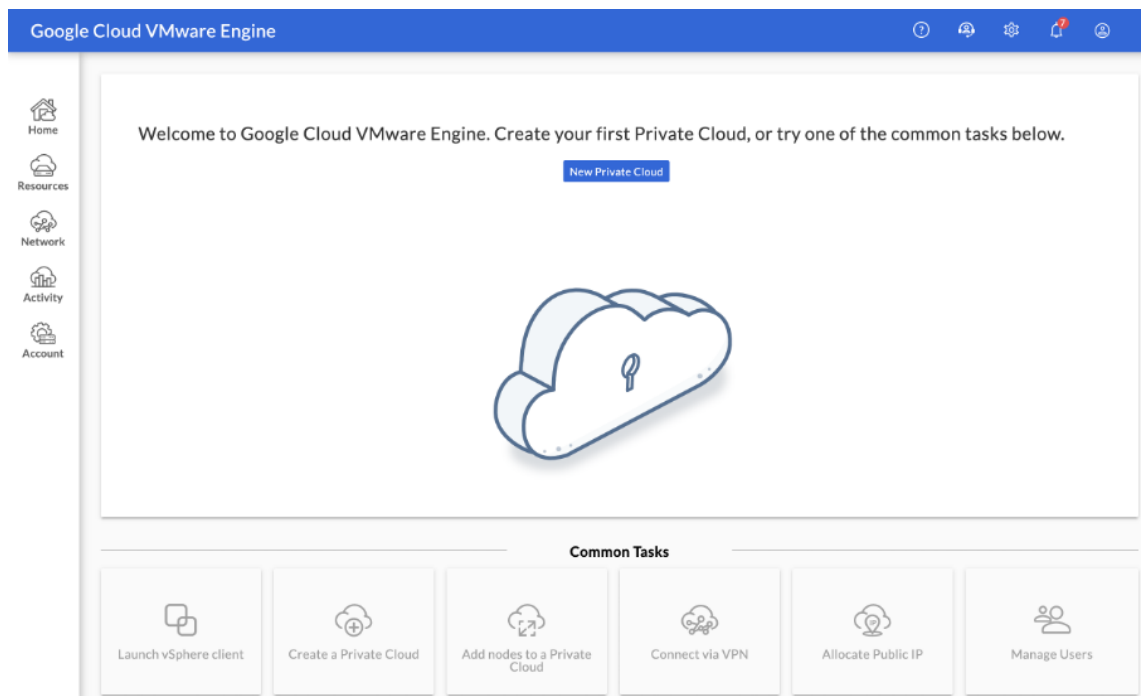
Citrix.com > **Descargas** > **NetScaler** > **Dispositivos virtuales**.

Copie los siguientes archivos en una estación de trabajo de la misma red que el servidor ESX. Copie los tres archivos en la misma carpeta.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (por ejemplo, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (por ejemplo, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (por ejemplo, NSVPX-ESX-13.0-79.64.mf)

Implementar VMware Engine de Google Cloud

1. Inicie sesión en su [portal de GCVE](#) y vaya a **Inicio**.



2. En la página **Nueva nube privada**, introduzca los siguientes detalles:

- Seleccione un mínimo de 3 hosts ESXi para crear el clúster predeterminado de su nube privada.
- Para el campo **Intervalo de CIDR de la subred de vSphere/vSAN**, utilice el espacio de direcciones /22.
- Para el campo **Intervalo de CIDR de la red de implementación de HCX**, utilice el espacio de direcciones /26.
- Para la red virtual, asegúrese de que el intervalo de CIDR no se superponga con ninguna de sus subredes locales u otras subredes de GCP (redes virtuales).

Google Cloud VMware Engine

← Create Private Cloud ⓘ

Private Cloud name *

Location *
asia-northeast1 > v-zone-a > VE Placement Group 2

Node type *
ve1-standard-72
2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM
19.2 TB Raw, 3.2 TB Cache (All-Flash)

Multi Node Single Node

Node count *

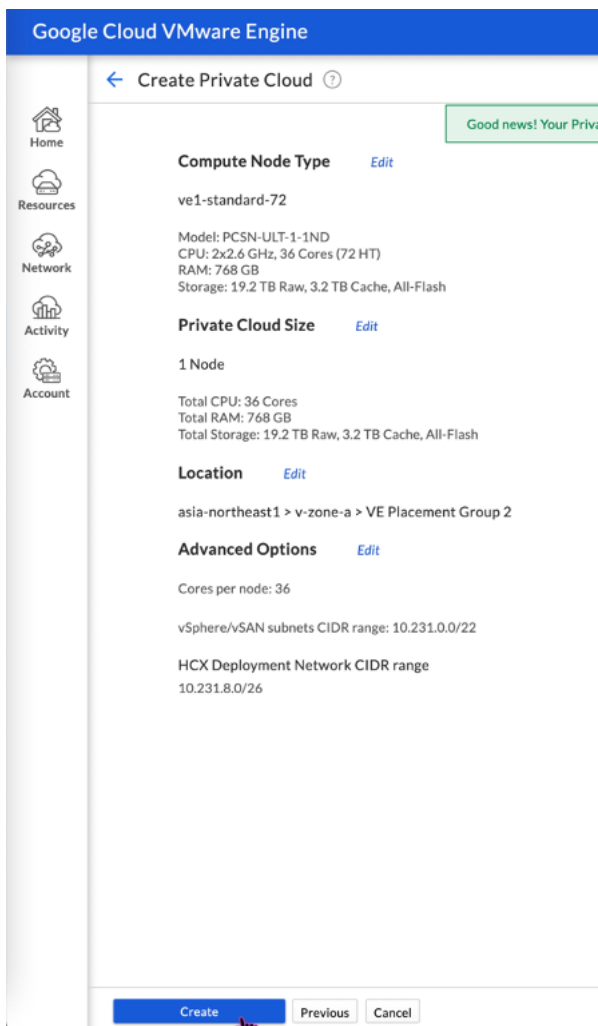
(3 to 8)

Customize Cores

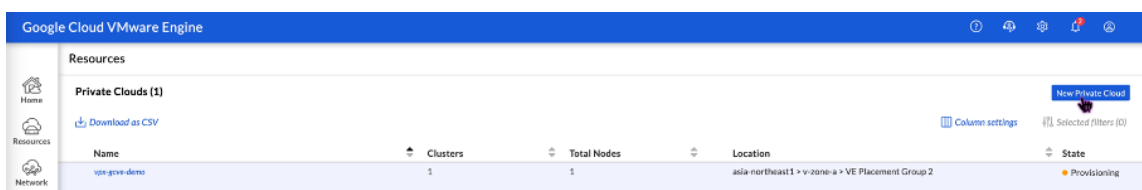
vSphere/vSAN subnets CIDR range *
 /

HCX Deployment Network CIDR range
 /

3. Haga clic en **Revisar y crear**.
4. Revise la configuración. Si necesita cambiar alguna configuración, haga clic en **Anterior**.



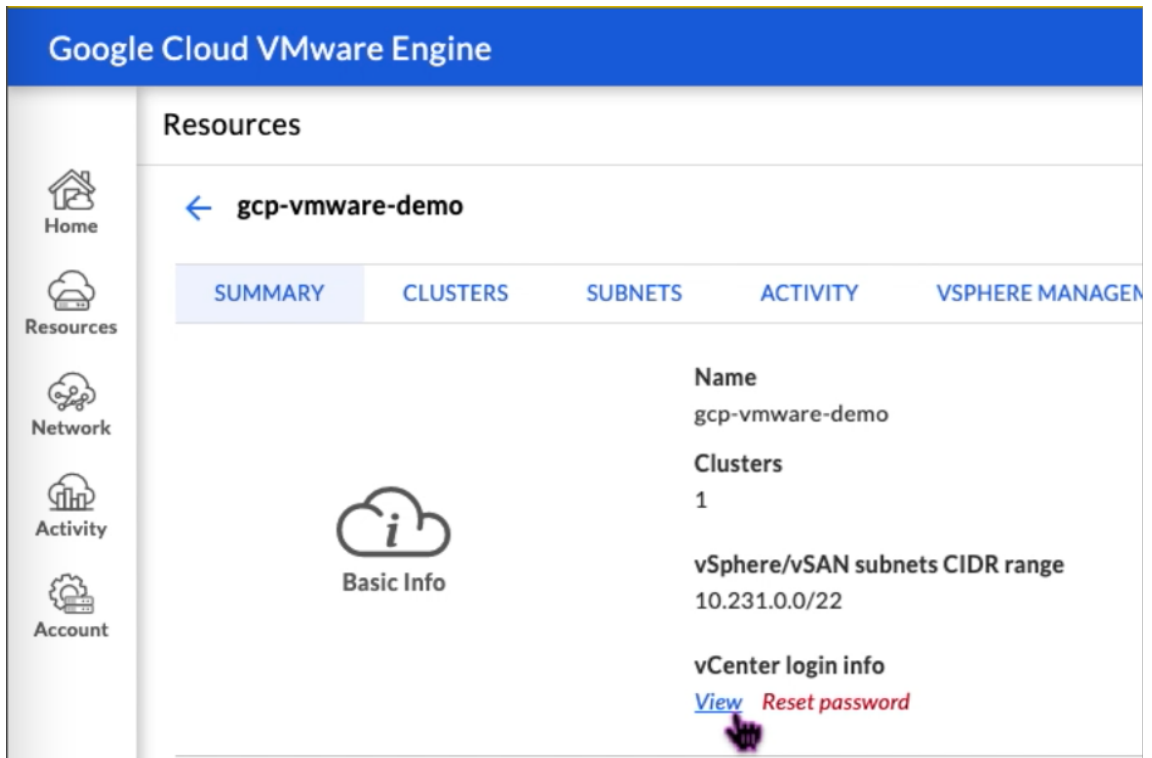
5. Haga clic en **Create**. Comienza el proceso de aprovisionamiento de nube privada. El aprovisionamiento de la nube privada puede tardar hasta dos horas.
6. Vaya a **Recursos** para verificar la nube privada que se ha creado.



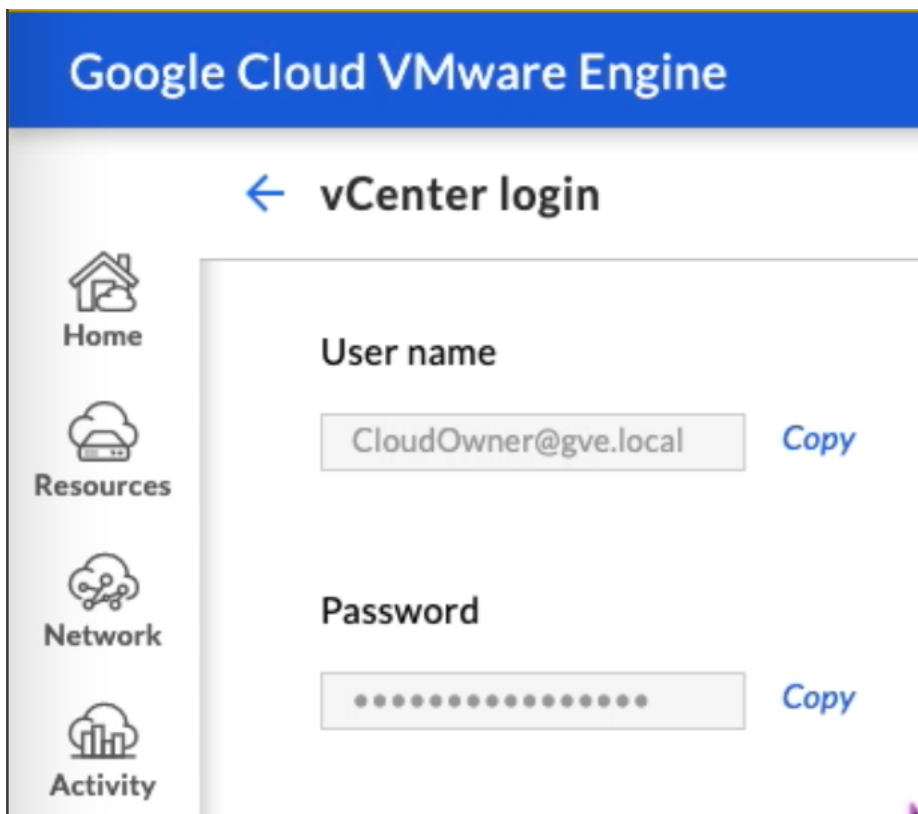
7. Para acceder a este recurso, debe conectarse a GCVE mediante una VPN punto a sitio. Para obtener más información, consulte la siguiente documentación:
 - [Puertas de enlace VPN](#)
 - [Conexión mediante VPN](#)

Acceda a su portal vCenter de nube privada

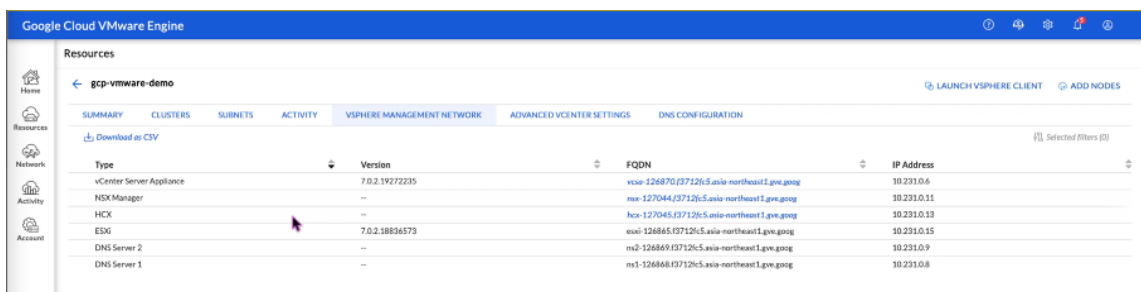
1. Vaya a su nube privada de VMware Engine de Google Cloud. En la ficha **RESUMEN**, en **Información de inicio de sesión de vCenter**, haga clic en **Ver**.



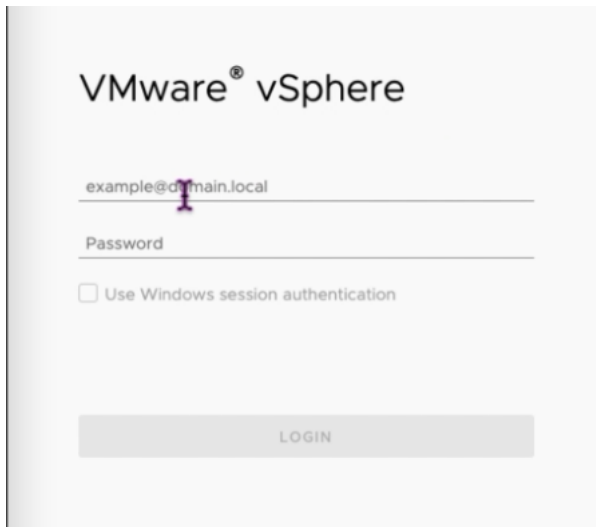
2. Anote las credenciales de vCenter.



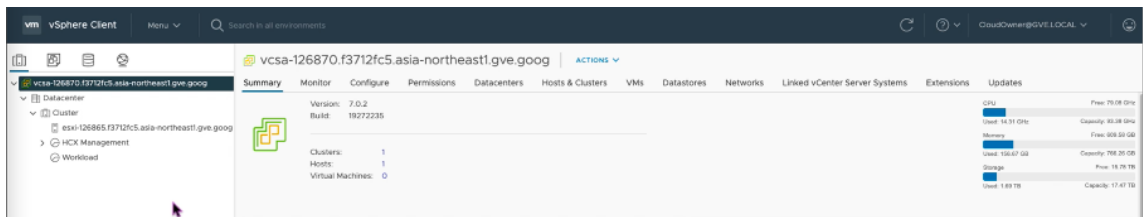
3. Inicie el cliente vSphere haciendo clic en **INICIAR CLIENTE DE VSPHERE** o vaya a **RED DE ADMINISTRACIÓN DE VSPHERE** y haga clic en el FQDN de **Servidor de vCenter**.



4. Inicie sesión en VMware vSphere con las credenciales de vCenter indicadas en el paso 2 de este procedimiento.



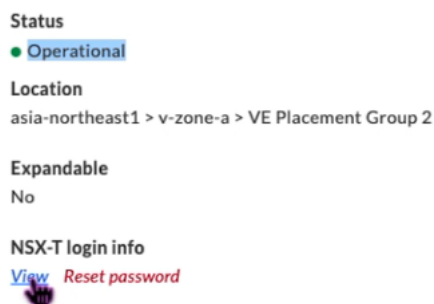
5. En el cliente vSphere, puede comprobar los hosts ESXi que creó en el portal de GCVE.



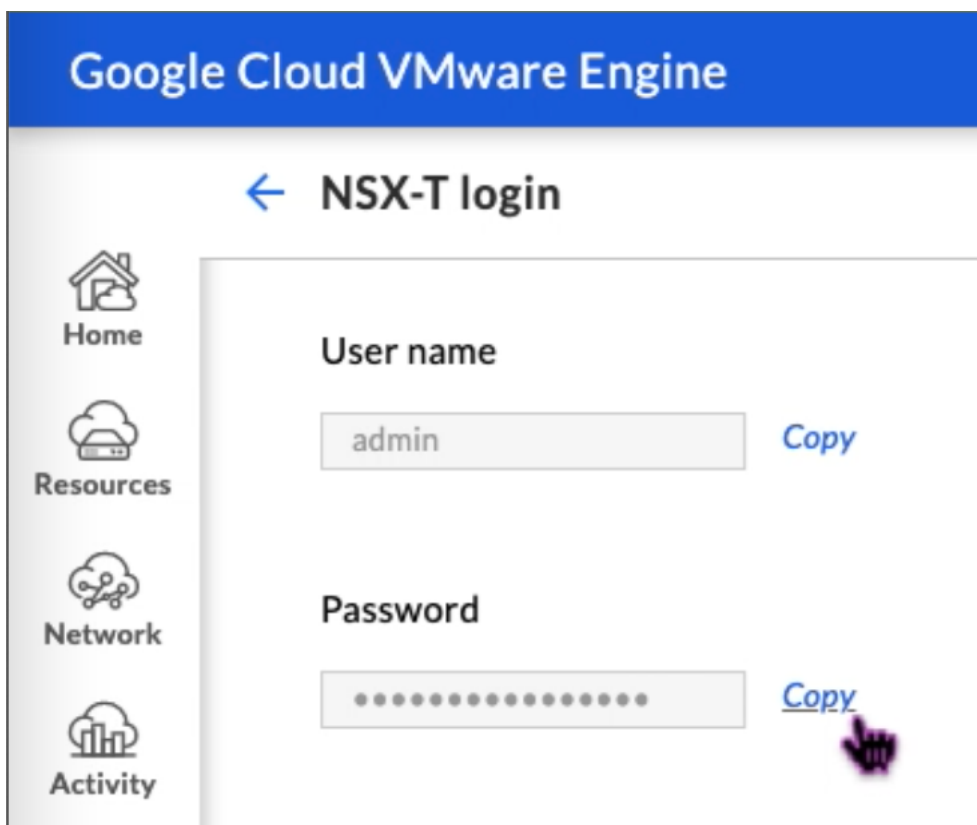
Crear un segmento de NSX-T en el portal NSX-T de GCVE

Puede crear y configurar un segmento de NSX-T desde NSX Manager en la consola de VMware Engine de Google Cloud. Estos segmentos están conectados a la puerta de enlace predeterminada de nivel 1 y las cargas de trabajo de estos segmentos obtienen conectividad Este-Oeste y Norte-Sur. Una vez creado el segmento, se muestra en vCenter.

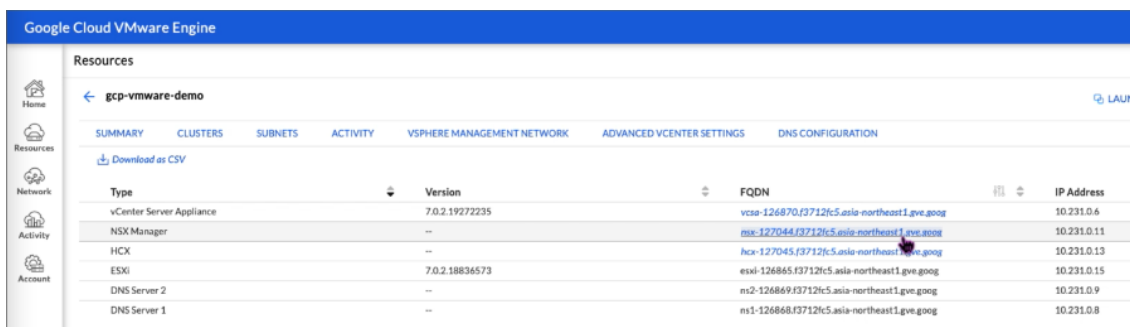
1. En su nube privada de GCVE, en **Resumen -> Información de inicio de sesión de NSX-T**, seleccione **Ver**.



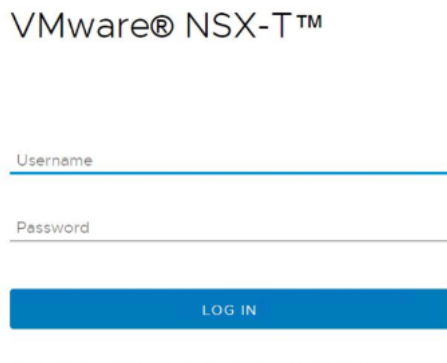
2. Tome nota de las credenciales del NSX-T.



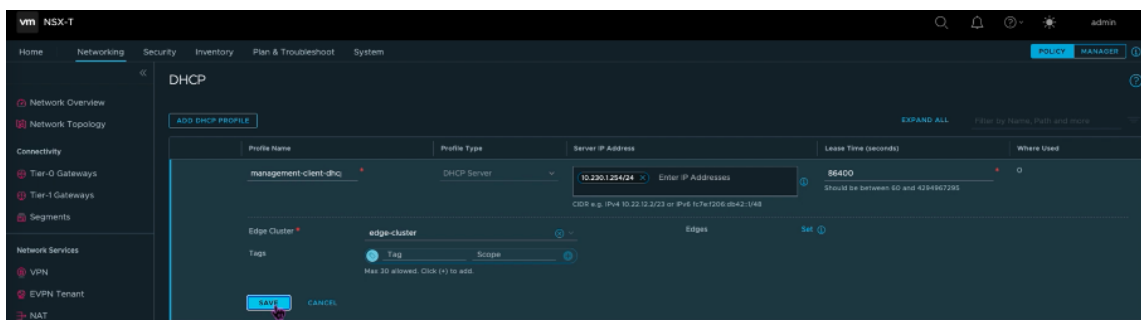
3. Para iniciar NSX Manager, vaya a **RED DE ADMINISTRACIÓN DE VSPHERE** y haga clic en el FQDN de **NSX Manager**.



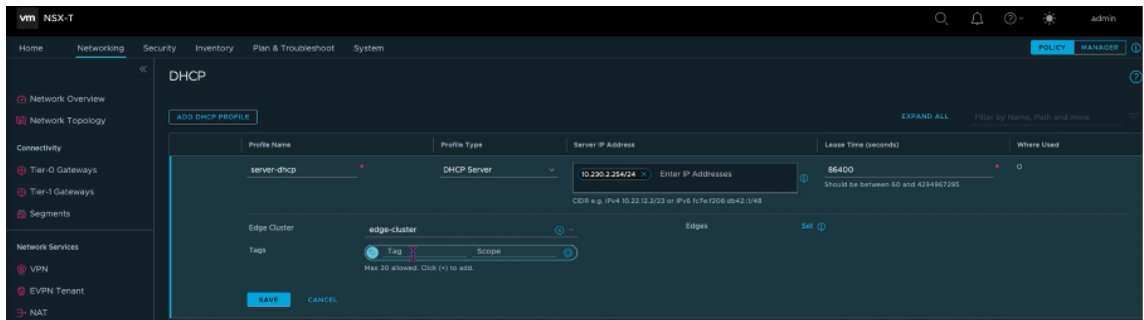
4. Inicie sesión en NSX Manager con las credenciales indicadas en el paso 2 de este procedimiento.



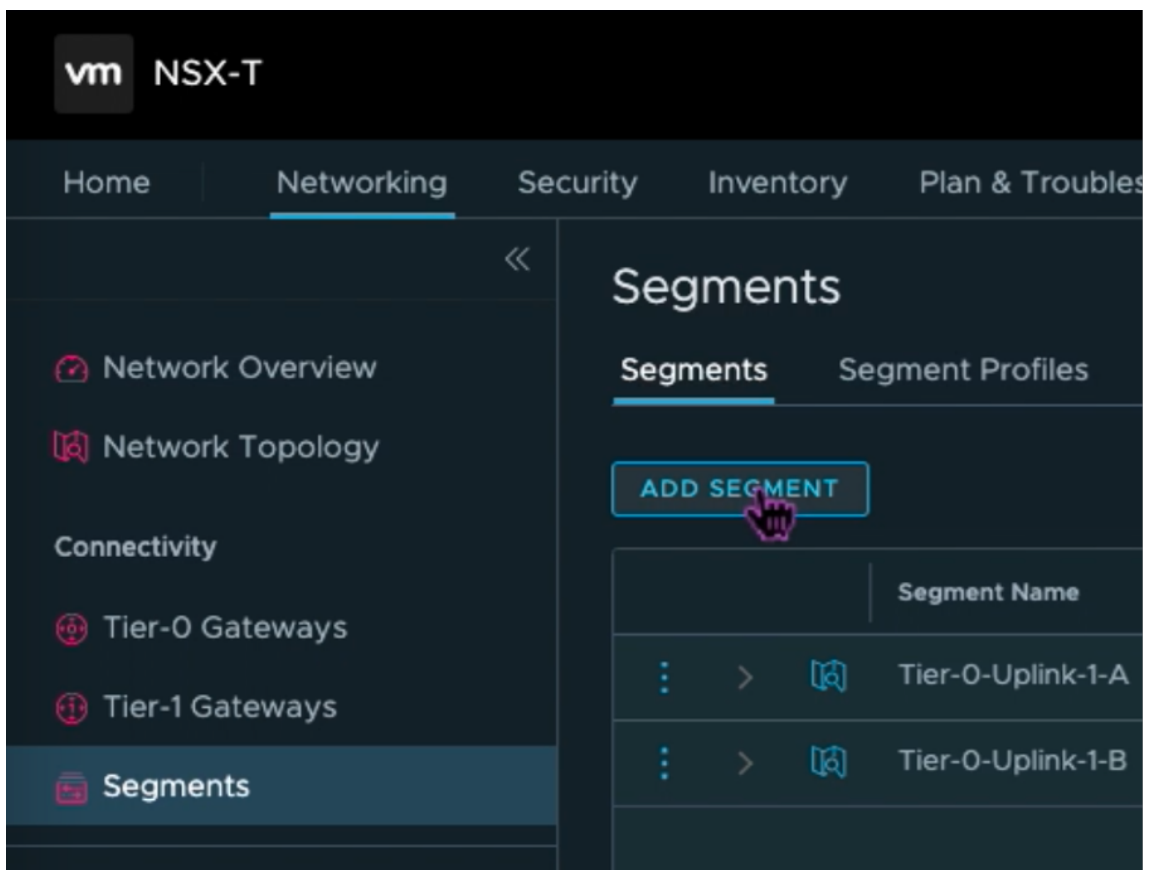
5. Configure el servicio DHCP para los nuevos segmentos o subredes.
6. Antes de poder crear una subred, configure un servicio DHCP.
7. En NSX-T, vaya a **Redes > DHCP**. El panel de control de redes muestra que el servicio crea una puerta de enlace de nivel 0 y una de nivel 1.
8. Para empezar a aprovisionar un servidor DHCP, haga clic en **Agregar perfil de DHCP**.
9. En el campo de nombre de DHCP, introduzca un nombre para el perfil **Client-Management**.
10. Seleccione **Servidor DHCP** como tipo de perfil.
11. En la columna **Dirección IP del servidor**, especifique un intervalo de direcciones IP del servicio DHCP.
12. Seleccione su **clúster de Edge**.
13. Haga clic en **Save** para crear el servicio DHCP.



14. Repita los pasos 6 a 13 para el intervalo del servidor DHCP.



15. Cree dos segmentos independientes: uno para las interfaces de cliente y de administración y otro para las interfaces de servidor.
16. En NSX-T, vaya a **Redes > Segmentos**.
17. Haga clic en **Add Segment**.



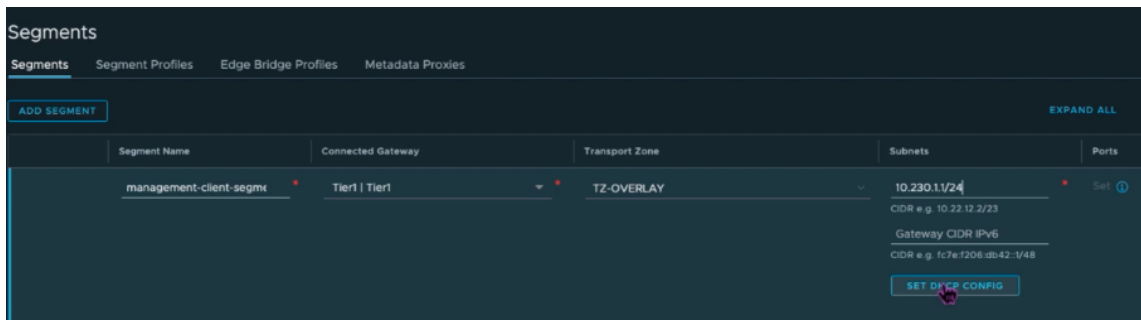
18. En el campo **Nombre del segmento**, introduzca un nombre para su segmento **Client Management**.
19. En la lista **Puerta de enlace conectada**, seleccione **Tier1** para conectarse a la puerta de enlace de nivel 1.

En la lista de **zonas de transporte**, seleccione Superposición**.

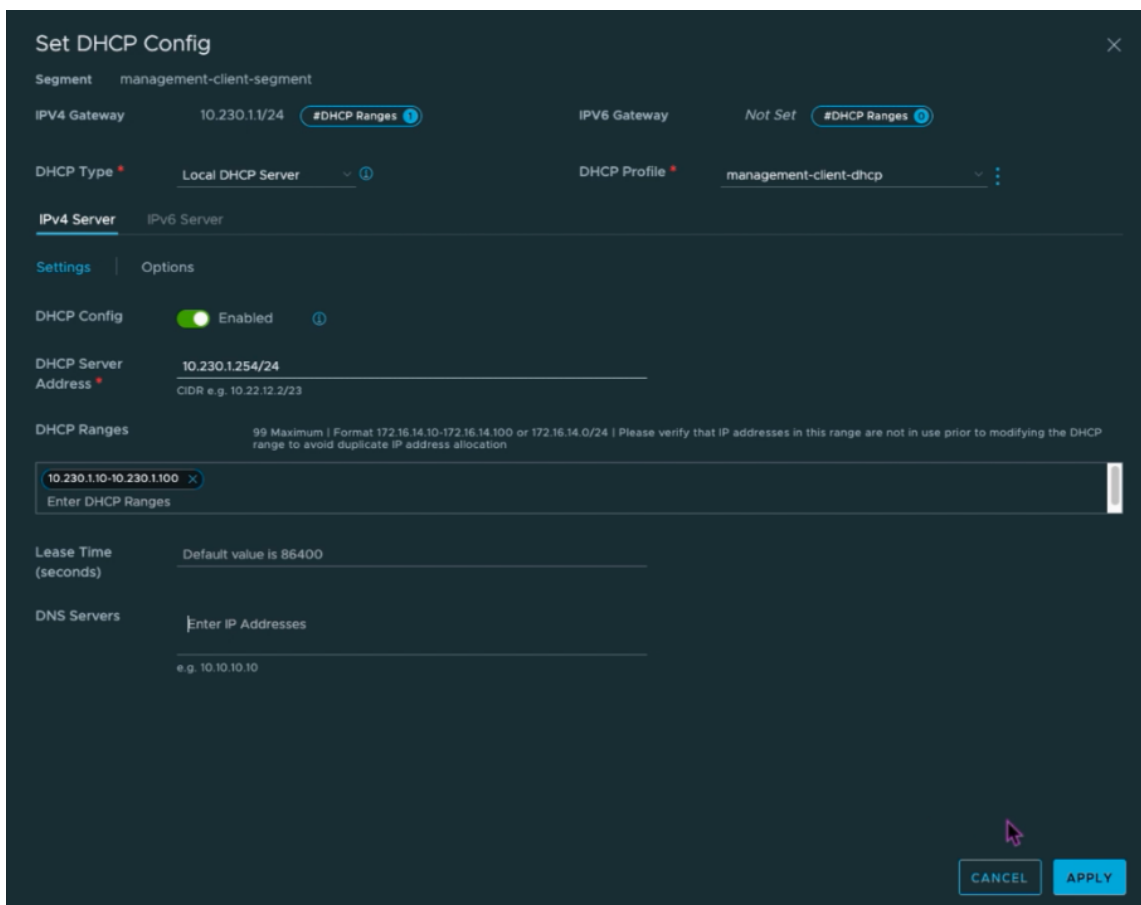
**TZ-OVERLAY

20.

21. En la columna **Subredes**, introduzca el intervalo de subredes. Especifique el rango de subredes con .1 como el último octeto. Por ejemplo, 10.12.2.1/24.

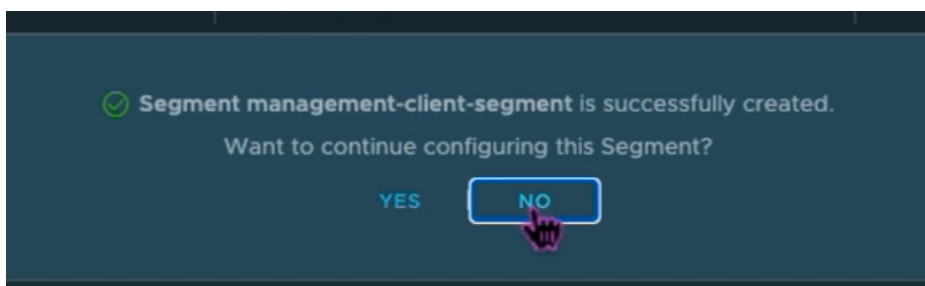
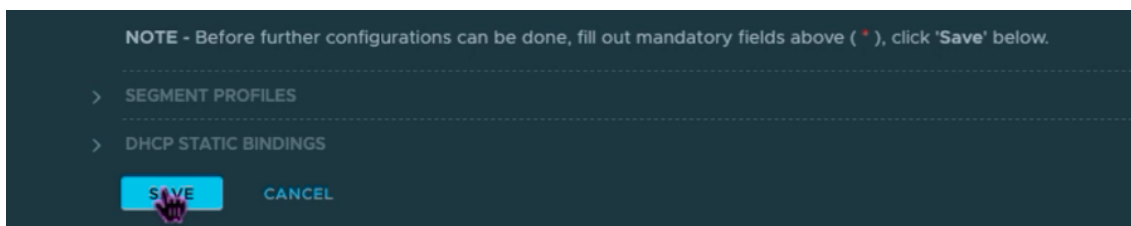


22. Haga clic en **Establecer configuración de DHCP** y proporcione valores para el campo **Intervalos de DHCP**.



23. Haga clic en **Aplicar** para guardar la configuración de DHCP.

24. Haga clic en **Guardar**.



25. Repita también los pasos 17 a 24 para el segmento Server.

26. Ahora puede seleccionar estos segmentos de red en vCenter al crear una máquina virtual.

Para obtener más información, consulte [Crear la primera subred](#).

Instalar una instancia de NetScaler VPX en la nube de VMware

Una vez que haya instalado y configurado la nube privada en GCVE, puede usar el vCenter para instalar dispositivos virtuales en VMware Engine. La cantidad de dispositivos virtuales que puede instalar depende de la cantidad de recursos disponibles en la nube privada.

Para instalar instancias de NetScaler VPX en una nube privada, lleve a cabo estos pasos en un escritorio conectado a una VPN punto a sitio de nube privada:

1. Descargue los archivos de configuración de instancias de NetScaler VPX para el host ESXi desde el sitio de descargas de NetScaler.
2. Abra VMware vCenter en un explorador web conectado a la VPN de punto a sitio de su nube privada.
3. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador y, a continuación, haga clic en **Iniciar sesión**.
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla OVF**, en el campo **Implementar desde archivo**, vaya a la ubicación en la que guardó los archivos de configuración de instancias NetScaler VPX, seleccione el archivo.ovf y haga clic en **Siguiente**.

Nota:

De forma predeterminada, la instancia de NetScaler VPX utiliza interfaces de red E1000. Para implementar ADC con la interfaz VMXNET3, modifique el OVF para utilizar la interfaz VMXNET3 en lugar de E1000. La disponibilidad de la interfaz VMXNET3 está limitada por la infraestructura de GCP y es posible que no esté disponible en VMware Engine de Google Cloud.

6. Asigne las redes que se muestran en la plantilla de OVF del dispositivo virtual a las redes que configuró en el NSX-T Manager. Haz clic en **Aceptar**.

Edit Settings | NSVPX-ESX-13.1-24.38_nc_64

Virtual Hardware | VM Options

ADD NEW DEVICE

> CPU	2		
> Memory	2	GB	
> Hard disk 1	20	GB	
> SCSI controller 0	LSI Logic Parallel		
▼ Network adapter 1	management-client-segment		
Status	<input checked="" type="checkbox"/> Connect At Power On		
Port ID	372795cc-b049-47b4-b9		
Adapter Type	VMXNET 3		
DirectPath I/O	<input checked="" type="checkbox"/> Enable		
Shares	Normal	50	
Reservation	0		Mbit/s
Limit	Unlimited		Mbit/s
MAC Address	00:50:56:a2:2c:2f	Automatic	

New Network *		server-segment	
Status	<input checked="" type="checkbox"/> Connect At Power On		
Adapter Type	VMXNET 3		
DirectPath I/O	<input checked="" type="checkbox"/> Enable		
Shares	Normal	50	
Reservation	0		Mbit/s
Limit	Unlimited		Mbit/s
MAC Address	Automatic		
> Video card	Specify custom settings		
VMCI device			

7. Haga clic en **Finalizar** para comenzar a instalar un dispositivo virtual en la nube de VMware.

Deploy OVF Template

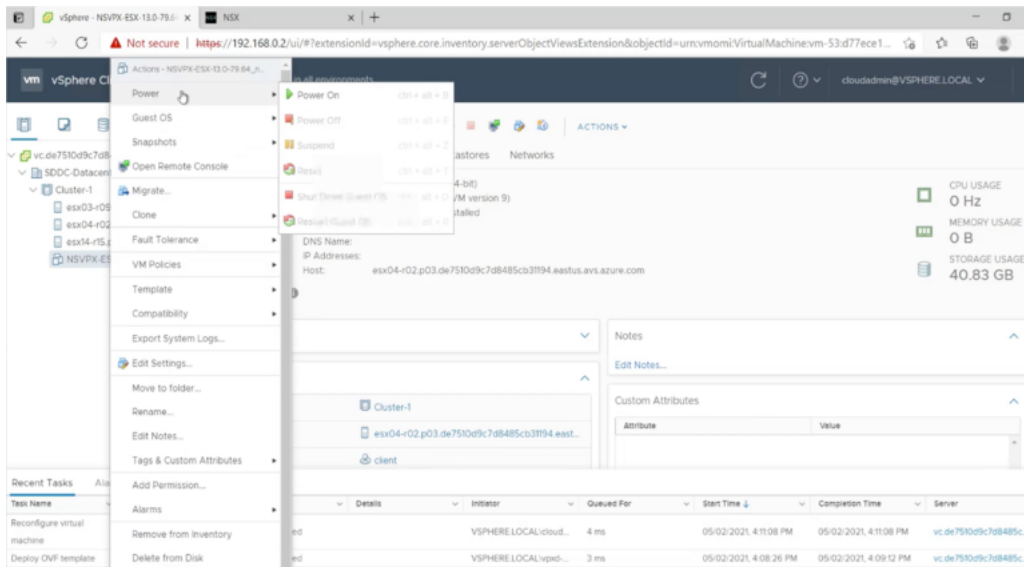
- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Ready to complete ×

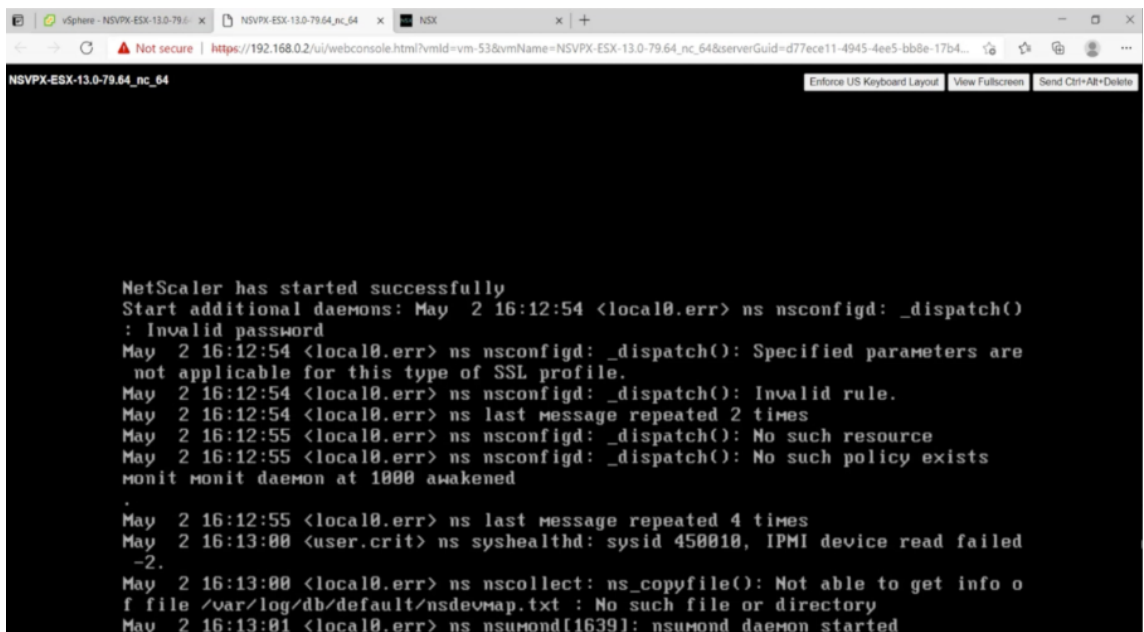
Click Finish to start creation.

Name	NSVPX-ESX-13.1-24.38_nc_64
Template name	NSVPX-ESX-13.1-24.38_nc_64
Download size	661.4 MB
Size on disk	20.0 GB
Folder	Workload VMs
Resource	Workload
Storage mapping	1
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

8. Ya está listo para iniciar la instancia de NetScaler VPX. En el panel de navegación, seleccione la instancia de NetScaler VPX que ha instalado y, en el menú contextual, seleccione **Encendido**. Haga clic en la ficha **Iniciar consola web** para emular un puerto de consola.



9. Ahora está conectado a la máquina virtual NetScaler desde el cliente de vSphere.



10. En el primer arranque, configure la IP de administración y la puerta de enlace para la instancia de 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
    
```

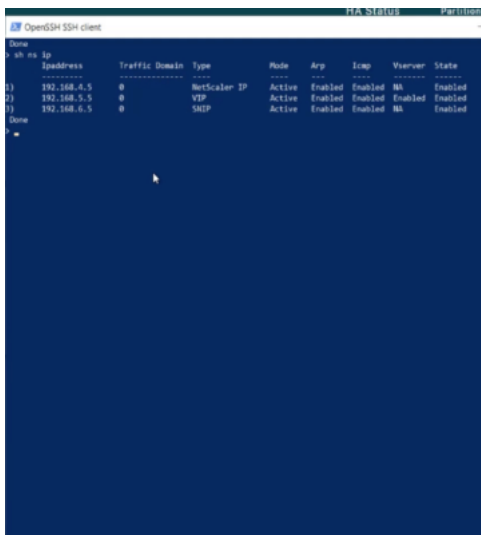
11. Para acceder al dispositivo NetScaler mediante las claves SSH, escriba el siguiente comando en la CLI:

```
1 ssh nsroot@<management IP address>
```

Ejemplo

```
1 ssh nsroot@10.230.1.10
```

12. Puede verificar la configuración de ADC mediante el comando `show ns ip`.

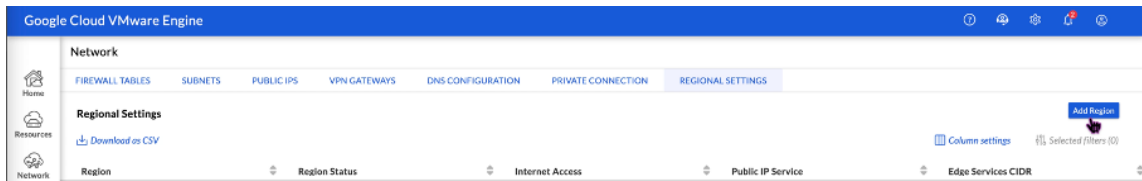


Asignar una dirección IP pública a una instancia NetScaler VPX en la nube de VMware

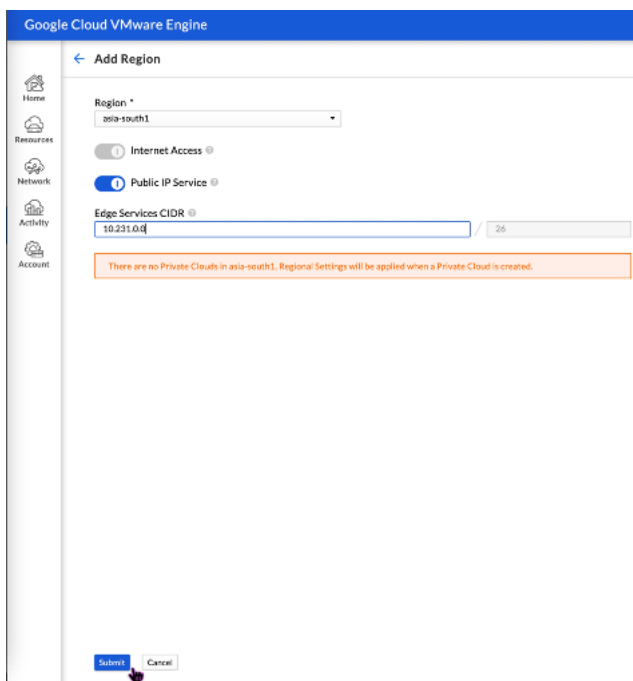
Una vez que haya instalado y configurado la instancia NetScaler VPX en GCVE, debe asignar una dirección IP pública a la interfaz del cliente. Antes de asignar direcciones IP públicas a sus máquinas virtuales, asegúrese de que el servicio IP pública esté activado en su región de Google Cloud.

Para habilitar el servicio de IP pública en una nueva región, siga estos pasos:

1. En la consola GCVE, vaya a **Red > CONFIGURACIÓN REGIONAL > Agregar región**.



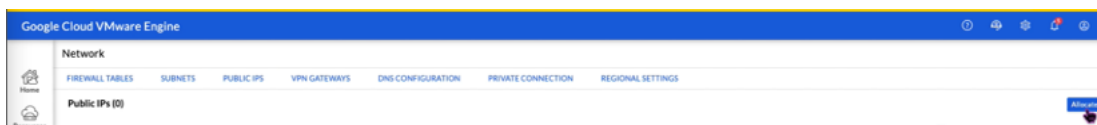
2. Seleccione su región y habilite el **acceso a Internet** y el **servicio IP público**.
3. Asigne un CIDR de Edge Services asegurándose de que el rango de CIDR no se superponga con ninguna de sus subredes locales u otras subredes GCP/GCVE (redes virtuales).



4. El servicio IP público se habilitará para la región seleccionada en unos minutos.

Para asignar una IP pública a la interfaz de cliente en la instancia NetScaler VPX en GCVE, siga estos pasos en el portal de GCVE:

1. En la consola GCVE, vaya a **Red > PUBLIC IPS > Asignar**.



2. Introduzca un nombre para la IP pública. Seleccione su región y seleccione la nube privada en la que se utilizará la IP.
3. Proporcione la IP privada de la interfaz a la que quiere que se asigne la IP pública. Esta será la **IP privada** de su interfaz de **cliente**.
4. Haga clic en **Submit**.



5. La IP pública estará lista para usarse en unos minutos.
6. Debe agregar reglas de firewall para permitir el acceso a la IP pública antes de poder usarla. Para obtener más información, consulte [Reglas de firewall](#).

Agregar servicio de escalado automático de GCP back-end

October 17, 2024

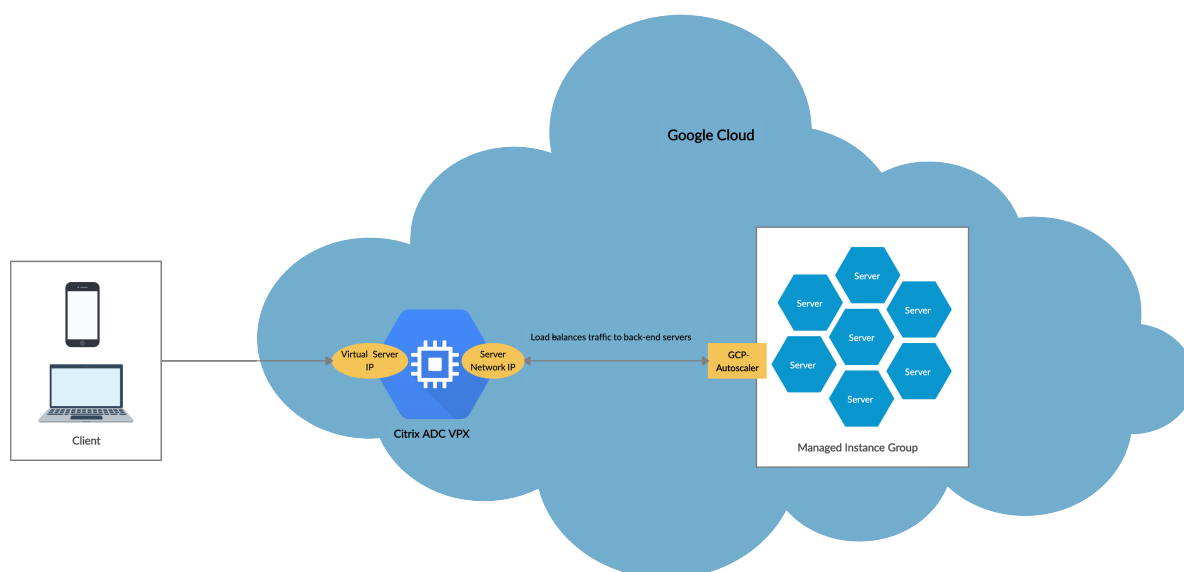
El alojamiento eficiente de aplicaciones en la nube requiere una gestión sencilla y rentable de los recursos, en función de la demanda de la aplicación. Para satisfacer la creciente demanda, debe ampliar los recursos de la red. Cuando la demanda disminuye, es necesario reducir la escala para evitar el coste innecesario de los recursos infrautilizados. Para minimizar el coste de ejecutar la aplicación, debe supervisar constantemente el tráfico, la memoria y el uso de la CPU, y así sucesivamente. Sin embargo, la supervisión manual del tráfico es engorrosa. Para que el entorno de aplicaciones se amplíe o

disminuya dinámicamente, debe automatizar los procesos de supervisión del tráfico y de ampliación de los recursos siempre que sea necesario.

Integrada con el servicio GCP Autoscaling, la instancia NetScaler VPX ofrece las siguientes ventajas:

- **Equilibrio y administración** de la carga: configura automáticamente los servidores para ampliarlos o reducirlos, según la demanda. La instancia VPX detecta automáticamente los grupos de instancias administrados en la subred de fondo y te permite seleccionar los grupos de instancias administrados para equilibrar la carga. Las direcciones IP virtuales y de subred se configuran automáticamente en la instancia VPX.
- **Alta disponibilidad:** detecta grupos de instancias administrados que abarcan varias zonas y servidores de equilibrio de carga.
- **Mejor disponibilidad de red:** la instancia VPX admite:
 - Servidores de fondo en los mismos grupos de ubicación
 - Servidores de fondo en diferentes zonas

Este diagrama ilustra cómo funciona el servicio de escalado automático de GCP en una instancia de NetScaler VPX que actúa como servidor virtual de equilibrio de carga.



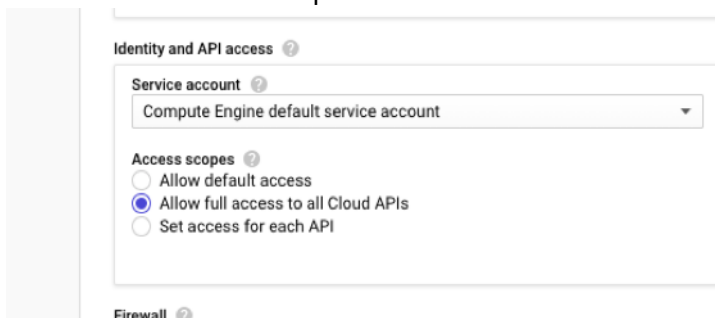
Antes de comenzar

Antes de empezar a utilizar AutoScaling con su instancia de NetScaler VPX, debe completar las siguientes tareas.

- Cree una instancia de NetScaler VPX en GCP según sus necesidades.
 - Para obtener más información sobre cómo crear una instancia de NetScaler VPX, consulte [Implementar una instancia de NetScaler VPX en Google Cloud Platform](#).

- Para obtener más información sobre cómo implementar instancias VPX en modo HA, consulta [Implementar un par de alta disponibilidad VPX en Google Cloud Platform](#).

- Habilite **Cloud Resource Manager API** para su proyecto GCP.
- Permite el acceso completo a todas las API de Cloud mientras creas las instancias.



- Asegúrate de que tu cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```

1  REQUIRED_INSTANCE_IAM_PERMS = [
2  "compute.instances.get",
3  "compute.instanceGroupManagers.get",
4  "compute.instanceGroupManagers.list",
5  "compute.zones.list",
6  "logging.sinks.create",
7  "logging.sinks.delete",
8  "logging.sinks.get",
9  "logging.sinks.list",
10 "logging.sinks.update",
11 "pubsub.subscriptions.consume",
12 "pubsub.subscriptions.create",
13 "pubsub.subscriptions.delete",
14 "pubsub.subscriptions.get",
15 "pubsub.topics.attachSubscription",
16 "pubsub.topics.create",
17 "pubsub.topics.delete",
18 "pubsub.topics.get",
19 "pubsub.topics.getIamPolicy",
20 "pubsub.topics.setIamPolicy",
21 ]

```

- Para configurar el ajuste de escala automático, asegúrese de que esté configurado lo siguiente:
 - Plantilla de instancia
 - Grupo de instancias administrado
 - Política de escalado automático

Agregar el servicio GCP Autoscaling a una instancia de NetScaler VPX

Puede agregar el servicio Autoscaling a una instancia VPX con un solo clic mediante la interfaz gráfica de usuario. Complete estos pasos para agregar el servicio Autoscaling a la instancia VPX:

1. Inicie sesión en la instancia VPX con sus credenciales de `nsroot`.
2. Cuando inicie sesión en la instancia NetScaler VPX por primera vez, verá la página de perfil de nube predeterminada. Seleccione el grupo de instancias administrado por GCP en el menú desplegable y haga clic en **Crear para crear** un perfil en la nube.

← Create Cloud Profile

Name

Virtual Server IP Address*

Load Balancing Server Protocol

Load Balancing Server Port

Auto Scale Group*

Auto Scale Group Protocol

Auto Scale Group Port

Select this option to drain the connections gracefully. Else the connections will be dropped in the event of scale down.

Graceful

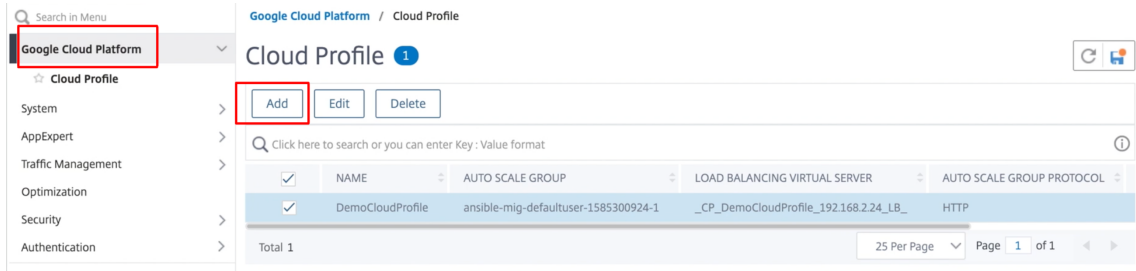
- El campo **Dirección IP del servidor virtual** se rellena automáticamente a partir de todas las direcciones IP asociadas a las instancias.
- El **grupo de escalabilidad automática** se rellena previamente desde el grupo de instancias administrado configurado en su cuenta de GCP.
- Al seleccionar el **Protocolo de grupo de escala automática** y el **puerto de grupo de escala automática**, asegúrese de que los servidores escuchan en el protocolo y los puertos configurados. Enlaza el monitor correcto al grupo de servicios. De forma predeterminada, se utiliza el monitor TCP.
- Desactive la casilla **Graceful** porque no es compatible.

Nota:

En el caso del protocolo SSL tipo AutoScaling, después de crear el perfil de nube, el servi-

dor virtual o el grupo de servicios de equilibrio de carga dejan de funcionar debido a la falta de un certificado. Puede enlazar el certificado al servidor virtual o grupo de servicios manualmente.

- Tras iniciar sesión por primera vez, si quieres crear un perfil de nube, en la GUI, ve a **Sistema > Google Cloud Platform > Perfil en la nube** y haga clic en **Agregar**.



Aparece la página **de configuración de Crear perfil en la nube**.

← Create Cloud Profile

Name: DemoCloudProfile

Virtual Server IP Address*: 192.168.2.24

Load Balancing Server Protocol: HTTP

Load Balancing Server Port: 80

Auto Scale Group*: ansible-mig-defaultuser-1585300924-

Auto Scale Group Protocol: HTTP

Auto Scale Group Port: 80

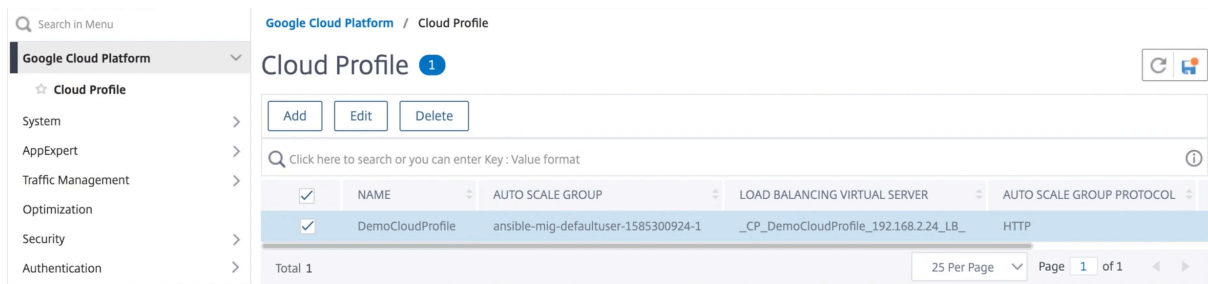
Select this option to drain the connections gracefully. Else the connections will be dropped in the event of scale down.

Graceful

Cloud Profile crea un servidor virtual de equilibrio de carga NetScaler y un grupo de servicios con miembros como servidores del grupo de instancias administrado. Los servidores back-end deben ser accesibles a través del SNIP configurado en la instancia VPX.

Nota:

A partir de la versión 13.1-42.x de NetScaler, puedes crear diferentes perfiles de nube para diferentes servicios (con diferentes puertos) con el mismo grupo de instancias administrado en GCP. Por lo tanto, la instancia NetScaler VPX admite varios servicios con el mismo grupo de escalado automático en la nube pública.



Compatibilidad con escalado VIP para la instancia NetScaler VPX en GCP

October 17, 2024

Un dispositivo NetScaler se encuentra entre los clientes y los servidores, de modo que las solicitudes de los clientes y las respuestas del servidor lo atraviesan. En una instalación típica, los servidores virtuales configurados en el dispositivo proporcionan puntos de conexión que los clientes utilizan para acceder a las aplicaciones detrás del dispositivo. El número de direcciones IP virtuales públicas (VIP) necesarias para una implementación varía según el caso.

La arquitectura de GCP restringe que cada interfaz de la instancia se conecte a una VPC diferente. Una VPC en GCP es un conjunto de subredes y cada subred puede extenderse por zonas de una región. Además, GCP impone la siguiente limitación:

- Hay una asignación 1:1 del número de direcciones IP públicas al número de NIC. Solo se puede asignar una dirección IP pública a una NIC.
- Se pueden conectar un máximo de 8 NIC en un tipo de instancia de mayor capacidad.

Por ejemplo, una instancia n1-standard 2 solo puede tener 2 NIC, y las VIP públicas que se pueden agregar están limitadas a 2. Para obtener más información, consulte [Cuotas de recursos de VPC](#).

Para lograr escalas más altas de direcciones IP virtuales públicas en una instancia de NetScaler VPX, puede configurar las direcciones VIP como parte de los metadatos de la instancia. La instancia de NetScaler VPX utiliza internamente las reglas de reenvío proporcionadas por el GCP para lograr el escalado VIP. La instancia NetScaler VPX también proporciona una alta disponibilidad a los VIP configurados. Después de configurar las direcciones VIP como parte de los metadatos, puede configurar

un servidor virtual LB mediante la misma IP que se utiliza para crear las reglas de reenvío. Por lo tanto, podemos usar reglas de reenvío para mitigar las limitaciones que tenemos a la hora de usar direcciones VIP públicas en una instancia de NetScaler VPX en GCP.

Para obtener más información sobre las reglas de reenvío, consulte [Descripción general de las reglas de reenvío](#).

Para obtener más información sobre HA, consulte [Alta disponibilidad](#).

Puntos a tener en cuenta

- Google cobra un coste adicional por cada regla de reenvío de IP virtual. El coste real depende del número de entradas creadas. El coste asociado se encuentra en los documentos de precios de Google.
- Las reglas de reenvío solo se aplican a los VIP públicos. Puede utilizar direcciones IP de alias cuando la implementación necesite direcciones IP privadas como VIP.
- Puede crear reglas de reenvío solo para los protocolos, que necesitan el servidor virtual LB. Los VIP se pueden crear, actualizar o eliminar sobre la marcha. También puede agregar un nuevo servidor virtual de equilibrio de carga con la misma dirección VIP pero con un protocolo diferente.

Antes de comenzar

- La instancia de NetScaler VPX debe implementarse en GCP.
- La dirección IP externa debe estar reservada. Para obtener más información, consulte [Reserva de una dirección IP externa estática](#).
- Asegúrese de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
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 ]
```

- Habilite **Cloud Resource Manager API** para su proyecto GCP.

- Si utilizas el escalado VIP en una instancia VPX independiente, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
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 utilizas el escalado VIP en un modo de alta disponibilidad, asegúrate de que su cuenta de servicio de GCP tenga los siguientes permisos de IAM:

```
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 ]
```

Nota:

En un modo de alta disponibilidad, si su cuenta de servicio no tiene funciones de propietario o editor, debe agregar la **función Usuario de cuenta de servicio** a su cuenta de servicio.

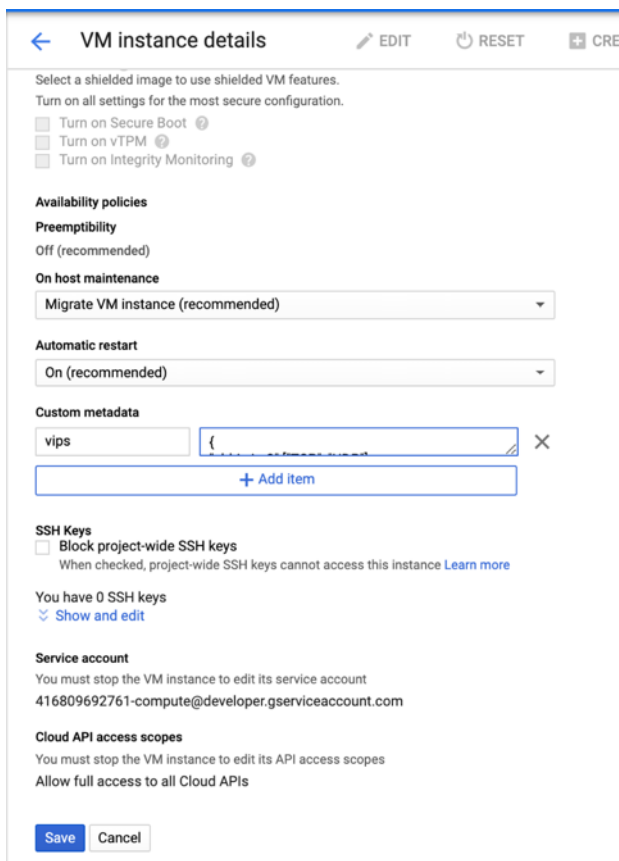
Configurar direcciones IP externas para el escalado VIP en la instancia de NetScaler VPX

1. En Google Cloud Console, vaya a la página **Instancias de VM**.
2. Crea una nueva instancia de VM o usa una instancia existente.
3. Haga clic en el nombre de la instancia. En la página de **detalles de la instancia de VM**, haga clic en **Modificar**.
4. Actualice los **metadatos personalizados** introduciendo lo siguiente:
 - Clave = vips
 - Valor = Proporcionar un valor en el siguiente formato JSON:

```
{ "Nombre de la IP reservada externa": [lista de protocolos], }
```

GCP admite los siguientes protocolos:

- AH
- ESP
- ICMP
- SCT
- TCP
- UDP



Para obtener más información, consulte [Metadatos personalizados](#).

Ejemplo de metadatos personalizados:

```
{ "nombre-ip1-externo": ["TCP", "UDP"], "nombre-ip2-externo": ["ICMP", "AH"] }
```

En este ejemplo, la instancia de NetScaler VPX crea internamente una regla de reenvío para cada par de protocolos IP. Las entradas de metadatos se asignan a las reglas de reenvío. Este ejemplo le ayuda a comprender cuántas reglas de reenvío se crean para una entrada de metadatos.

Se crean cuatro reglas de reenvío de la siguiente manera:

- a) external-ip1-name y TCP
- b) external-ip1-name y UDP
- c) external-ip2-name e ICMP
- d) external-ip2-name y AH

Nota:

En el modo HA, debes agregar metadatos personalizados solo en la instancia principal. En caso de conmutación por error, los metadatos personalizados se sincronizan con el nuevo principal.

5. Haga clic en **Guardar**.

Configuración de un servidor virtual de equilibrio de carga con dirección IP externa en una instancia de NetScaler VPX

Paso 1. Agregue un servidor virtual de equilibrio de carga.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales > Agregar**.

The screenshot displays the 'Virtual Servers' configuration page in the NetScaler VPX interface. The breadcrumb trail is 'Traffic Management / Load Balancing / Virtual Servers'. The page title is 'Virtual Servers' with a notification badge '4'. Below the title are buttons for 'Add', 'Edit', 'Delete', 'Enable', 'Disable', 'Rename', 'Statistics', and 'Select'. A search bar is present with the text 'Click here to search or you can enter Key: Value format'. The main content is a table with the following data:

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE	IP A
<input type="checkbox"/>	gcplbdnsvserver	● UP	● UP	0.0.0
<input type="checkbox"/>	lbv2	● UP	● UP	10.3
<input type="checkbox"/>	v1	● DOWN	● DOWN	10.2
<input checked="" type="checkbox"/>	Demo-vServer	● DOWN	● DOWN	34.9

Total 4

2. Agregue los valores necesarios para Nombre, Protocolo, Tipo de dirección IP (dirección IP), Dirección IP (dirección IP externa de la regla de reenvío que se agrega como VIP en ADC) y Puerto y haga clic en **Aceptar**.

← 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 (LAN) (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the avail

Name*

 ⓘ

Protocol*

 ▾

IP Address Type*

 ▾

IP Address*

 ⓘ

Port*

▶ More

Paso 2. Agregue un servicio o grupo de servicios.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servicios > Agregar**.
2. Agregue los valores necesarios para Nombre de servicio, Dirección IP, Protocolo y Puerto, y haga clic en **Aceptar**.

← Load Balancing Service

Basic Settings

Service Name*

 ⓘ

New Server Existing Server

IP Address*

 ⓘ

Protocol*

 ▾

Port*

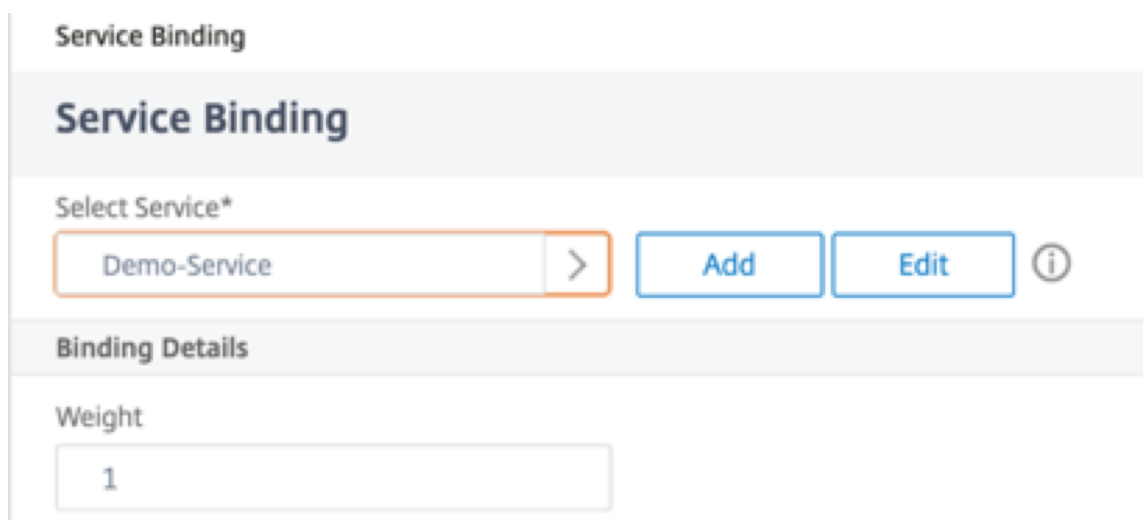
▶ More

Paso 3. Enlazar el servicio o el grupo de servicios al servidor virtual de equilibrio de carga.

1. Vaya a **Configuración > Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de equilibrio de carga configurado en el **paso 1** y haga clic en **Modificar**.
3. En la página **Grupos de servicios y servicios**, haga clic en **Sin enlace de servicio de servidor virtual de equilibrio de carga**.



4. Seleccione el servicio configurado en el **paso 3** y haga clic en **Enlazar**.



5. Verifique la configuración.

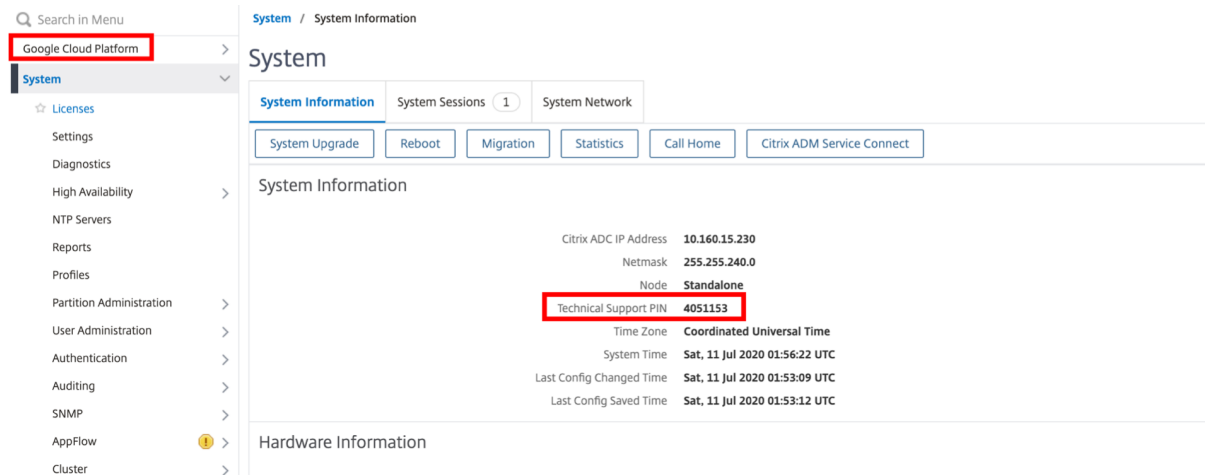
Solución de problemas de una instancia VPX en GCP

October 17, 2024

Google Cloud Platform (GCP) proporciona acceso de consola a una instancia de NetScaler VPX. Solo puede depurar si la red está conectada. Para ver el registro del sistema de una instancia, acceda a la consola y compruebe los **archivos de registro del sistema**.

NetScaler admite instancias de NetScaler VPX de pago (licencia de utilidad con tarifa por hora) en GCP. Para presentar un caso de soporte, busque su número de cuenta de GCP y su código PIN de soporte y llame al servicio de asistencia de NetScaler. Se le pedirá que proporcione su nombre y dirección de correo electrónico. Para encontrar el PIN de soporte, inicie sesión en la GUI de VPX y vaya a la página del **sistema**.

Aquí hay un ejemplo de una página del sistema que muestra el PIN de soporte.



Tramas gigantes en instancias NetScaler VPX

October 17, 2024

Los dispositivos NetScaler VPX admiten la recepción y la transmisión de tramas gigantes que contienen hasta 9216 bytes de datos IP. Las tramas gigantes pueden transferir archivos grandes de forma más eficiente de lo que es posible con el tamaño MTU IP estándar de 1500 bytes.

Un dispositivo NetScaler puede utilizar marcos gigantes en los siguientes casos de implementación:

- Jumbo a Jumbo. El dispositivo recibe datos como tramas jumbo y los envía como tramas jumbo.
- No Jumbo a Jumbo. El dispositivo recibe datos como tramas normales y los envía como tramas jumbo.
- Jumbo a No Jumbo. El dispositivo recibe datos como tramas gigantes y los envía como tramas normales.

Para obtener más información, consulte [Configuración del soporte de tramas jumbo en un dispositivo NetScaler](#).

La compatibilidad con tramas gigantes está disponible en los dispositivos NetScaler VPX que se ejecutan en las siguientes plataformas de virtualización:

- VMware ESX
- Plataforma Linux-KVM
- Citrix XenServer
- Amazon Web Services (AWS)

Las tramas jumbo en los dispositivos VPX funcionan de forma similar a las tramas jumbo en los dispositivos MPX. Para obtener más información sobre las tramas Jumbo y sus casos de uso, consulte Configuración de tramas Jumbo en dispositivos MPX. Los casos de uso de tramas jumbo en dispositivos MPX también se aplican a los dispositivos VPX.

Configurar tramas jumbo para una instancia VPX que se ejecuta en VMware ESX

Realice las siguientes tareas para configurar tramas gigantes en un dispositivo NetScaler VPX que se ejecuta en el servidor VMware ESX:

1. Establezca la MTU de la interfaz o canal del dispositivo VPX en un valor del rango 1501-9000. Utilice la CLI o GUI para establecer el tamaño de MTU. Los dispositivos NetScaler VPX que se ejecutan en VMware ESX admiten la recepción y la transmisión de tramas gigantes que contienen solo 9000 bytes de datos IP.
2. Establezca el mismo tamaño de MTU en las interfaces físicas correspondientes del servidor VMware ESX mediante sus aplicaciones de administración. Para obtener más información sobre cómo configurar el tamaño de la MTU en las interfaces físicas de VMware ESX, consulte <http://vmware.com/>.

Configurar tramas jumbo para una instancia VPX que se ejecuta en el servidor Linux-KVM

Realice las siguientes tareas para configurar marcos gigantes en un dispositivo NetScaler VPX que se ejecute en un servidor Linux-KVM:

1. Establezca la MTU de la interfaz o canal del dispositivo VPX en un valor del rango 1501-9216. Utilice la CLI o la GUI de NetScaler VPX para configurar el tamaño de la MTU.
2. Establezca el mismo tamaño de MTU en las interfaces físicas correspondientes de un servidor Linux-KVM mediante sus aplicaciones de administración. Para obtener más información sobre cómo configurar el tamaño de MTU en las interfaces físicas de Linux-KVM, consulte <http://www.linux-kvm.org/>.

Configurar tramas jumbo para una instancia VPX que se ejecuta en Citrix XenServer

Realice las siguientes tareas para configurar marcos gigantes en un dispositivo NetScaler VPX que se ejecute en Citrix XenServer:

1. Conéctese a XenServer mediante XenCenter.
2. Apague todas las instancias VPX que utilizan las redes para las que se debe cambiar la MTU.
3. En la ficha **Redes**, seleccione la red: Red 0/1/2.

4. Seleccione **Propiedades** y modifique MTU.

Después de configurar las tramas gigantes en XenServer, puede configurar las tramas gigantes en el dispositivo ADC. Para obtener más información, consulte [Configuración del soporte de tramas jumbo en un dispositivo NetScaler](#).

Configurar tramas jumbo para una instancia VPX que se ejecuta en AWS

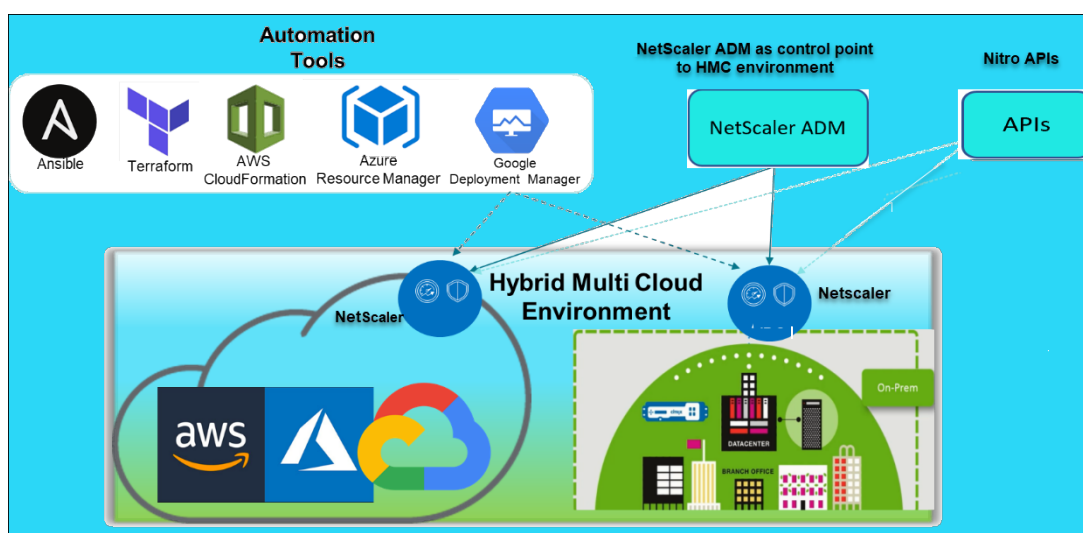
La configuración de nivel de host no es necesaria para VPX en Azure. Para configurar Jumbo Frames en VPX, siga los pasos que se indican en [Configuración del soporte de tramas jumbo en un dispositivo NetScaler](#).

Automatizar la implementación y las configuraciones de NetScaler

October 17, 2024

NetScaler proporciona varias herramientas para automatizar las implementaciones y configuraciones de ADC. Este documento proporciona un breve resumen de varias herramientas de automatización y referencias a varios recursos de automatización que puede utilizar para administrar las configuraciones de ADC.

La siguiente ilustración proporciona una descripción general de la automatización de NetScaler en un entorno híbrido de múltiples nubes (HMC).



Automatice NetScaler con NetScaler ADM

NetScaler ADM actúa como un punto de control de automatización para su infraestructura ADC distribuida. NetScaler ADM proporciona un conjunto integral de capacidades de automatización, desde el aprovisionamiento de dispositivos ADC hasta su actualización. Las siguientes son las principales funciones de automatización de ADM:

- [Aprovisionamiento de instancias de NetScaler VPX en AWS](#)
- [Aprovisionamiento de instancias de NetScaler VPX en Azure](#)
- [StyleBooks](#)
- [Trabajos de configuración](#)
- [Auditoría de configuración](#)
- [Actualizaciones de ADC](#)
- [Administración de certificados SSL](#)
- [Integraciones - GitHub, ServiceNow, Integraciones de notificaciones de eventos](#)

Blogs y vídeos de NetScaler ADM sobre automatización

- [Migraciones de aplicaciones mediante StyleBooks](#)
- [Integre configuraciones de ADC con CI/CD mediante ADM StyleBooks](#)
- [Simplificación de las implementaciones de NetScaler en la nube pública a través de ADM](#)
- [10 formas en las que el servicio NetScaler ADM facilita las actualizaciones de NetScaler](#)

NetScaler ADM también proporciona API para sus diversas capacidades que integran NetScaler ADM y NetScaler como parte de la automatización general de TI. Para obtener más información, consulte [API del servicio NetScaler ADM](#).

Automatice NetScaler con Terraform

Terraform es una herramienta que toma la infraestructura como un enfoque de código para aprovisionar y administrar la nube, la infraestructura o el servicio. Los recursos de terraform de NetScaler están disponibles en GitHub para su uso. Consulta GitHub para obtener documentación y uso detallados.

- [Módulos NetScaler Terraform para configurar ADC para varios casos de uso, como el equilibrio de carga y GSLB](#)
- [Scripts en la nube de Terraform para implementar ADC en AWS](#)
- [Scripts en la nube de Terraform para implementar ADC en Azure](#)
- [Scripts en la nube de Terraform para implementar ADC en GCP](#)
- [Implementación azul-verde mediante procesos de NetScaler VPX y Azure](#)

Blogs y vídeos sobre Terraform para la automatización de ADC

- [Automatice sus implementaciones de NetScaler con Terraform](#)
- [Aprovisionar y configurar ADC en la configuración de alta disponibilidad en AWS mediante Terraform](#)

Automatizar NetScaler mediante Consul-Terraform-Sync

El módulo NetScaler Consul-Terraform-Sync (CTS) permite a los equipos de aplicaciones agregar o eliminar automáticamente nuevas instancias de servicios en NetScaler. No es necesario generar tickets manuales a los administradores de TI o a los equipos de redes para realizar los cambios necesarios en las configuraciones de ADC.

- [Módulo NetScaler Consul-Terraform-Sync para la automatización de la infraestructura de red](#)
- Seminario web conjunto Citrix-HashiCorp: [Redes dinámicas con Consul-Terraform-Sync para Terraform Enterprise y NetScaler](#)

Automatice NetScaler con Ansible

Ansible es una herramienta de aprovisionamiento de software de código abierto, administración de configuración e implementación de aplicaciones que permite la infraestructura como código. Los módulos y playbooks de muestra de NetScaler Ansible se pueden encontrar en GitHub para su uso. Consulta GitHub para obtener documentación y uso detallados.

- [Módulos de Ansible para configurar ADC](#)
- [Documentación y guía de referencia de los módulos de ADC Ansible](#)
- [Módulos de Ansible para ADM](#)

Citrix es un socio de automatización certificado de Ansible. Los usuarios que tienen suscripción a Red Hat Ansible Automation Platform pueden acceder a las colecciones de NetScaler desde [Red Hat Automation Hub](#).

Blogs de automatización de Terraform y Ansible

- [Citrix nombrado socio de integración del año de HashiCorp](#)
- [Citrix ahora es un socio certificado de Red Hat Ansible Automation Platform](#)
- [Terraform y Ansible Automation para la entrega de aplicaciones y la seguridad](#)

Plantillas de nube pública para implementaciones de ADC

Las plantillas de nube pública simplifican el aprovisionamiento de sus implementaciones en nubes públicas. Hay diferentes plantillas de NetScaler disponibles para varios entornos. Para obtener detalles de uso, consulta los repositorios GitHub respectivos.

CFT de AWS:

- [CFT para aprovisionar NetScaler VPX en AWS](#)

Plantillas de Azure Resource Manager (ARM):

- [Plantillas ARM para aprovisionar NetScaler VPX en Azure](#)

Plantillas de Google Cloud Deployment Manager (GDM):

- [Plantillas de GDM para aprovisionar NetScaler VPX en Google](#)

Vídeos en plantillas

- [Implementación de NetScaler HA en AWS mediante la plantilla de CloudFormation](#)
- [Implemente NetScaler HA en las zonas de disponibilidad mediante AWS QuickStart](#)
- [Implementación de alta disponibilidad de NetScaler en GCP mediante plantillas de GDM](#)

API de NITRO

El protocolo NetScaler NITRO le permite configurar y supervisar mediante programación el dispositivo NetScaler mediante interfaces de transferencia de estado representacional (REST). Por lo tanto, las aplicaciones NITRO se pueden desarrollar en cualquier lenguaje de programación. Para las aplicaciones que deben desarrollarse en Java, .NET o Python, las API de NITRO se exponen a través de bibliotecas relevantes que se empaquetan como kits de desarrollo de software (SDK) separados.

- [Documentación de NITRO API](#)
- [Ejemplo de configuración de casos de uso de ADC mediante NITRO API de](#)

Preguntas frecuentes

October 17, 2024

La siguiente sección le ayuda a clasificar las preguntas frecuentes según Citrix Application Delivery Controller (ADC) VPX.

- Función y funcionalidad
- Cifrado
- Precios y empaquetado
- NetScaler VPX Express y prueba gratuita de 90 días
- Hypervisor
- Planificación o dimensionamiento de la capacidad
- Requisitos del sistema
- Otras preguntas frecuentes técnicas

Función y funcionalidad

¿Qué es NetScaler VPX?

NetScaler VPX es un dispositivo ADC virtual que se puede alojar en un hipervisor instalado en servidores estándar del sector.

¿NetScaler VPX incluye toda la funcionalidad de optimización de aplicaciones web como dispositivos ADC?

Sí. NetScaler VPX incluye todo el equilibrio de carga, la administración del tráfico, la aceleración de las aplicaciones, la seguridad de las aplicaciones (incluidos NetScaler Gateway y Citrix Application Firewall) y la funcionalidad de descarga. Para obtener una descripción completa de la función y funcionalidad de NetScaler, consulte [Entrega de aplicaciones a su manera](#).

¿Existen limitaciones con Citrix Application Firewall al usarlo en NetScaler VPX?

Citrix Application Firewall en NetScaler VPX proporciona las mismas protecciones de seguridad que en los dispositivos NetScaler. El rendimiento o el rendimiento de Citrix Application Firewall varía según la plataforma.

¿Hay alguna diferencia entre NetScaler Gateway en NetScaler VPX y NetScaler Gateway en dispositivos NetScaler?

Funcionalmente, son lo mismo. NetScaler Gateway en NetScaler VPX admite todas las funciones de NetScaler Gateway disponibles en la versión 14.1 del software NetScaler. Sin embargo, dado que los dispositivos NetScaler proporcionan hardware de aceleración SSL dedicado, ofrecen mayor escalabilidad SSL VPN que una instancia NetScaler VPX.

Además de la diferencia obvia de que NetScaler VPX puede ejecutarse en un hipervisor, ¿en qué se diferencia de los dispositivos físicos de NetScaler?

Hay dos áreas principales en las que los clientes ven diferencias de comportamiento. La primera es que NetScaler VPX no puede ofrecer el mismo rendimiento que muchos dispositivos NetScaler. La segunda es que, si bien los dispositivos NetScaler incorporan su propia funcionalidad de red L2, NetScaler VPX confía en el hipervisor para sus servicios de red L2. En general, no limita cómo se puede implementar NetScaler VPX. Puede haber cierta funcionalidad L2 configurada en un dispositivo NetScaler físico que debe configurarse en el hipervisor subyacente.

¿Qué papel desempeña NetScaler VPX en el mercado de la entrega de aplicaciones?

NetScaler VPX cambia las reglas del juego en el mercado de entrega de aplicaciones de las siguientes maneras:

- Al hacer que un dispositivo NetScaler sea aún más asequible, NetScaler VPX permite a cualquier organización de TI implementar un dispositivo NetScaler. No es solo para sus aplicaciones web más críticas, sino para todas sus aplicaciones web.
- NetScaler VPX permite a los clientes converger aún más las redes y la virtualización dentro de sus centros de datos. NetScaler VPX no solo se puede utilizar para optimizar las aplicaciones web alojadas en servidores virtualizados. También permite que la entrega de aplicaciones web se convierta en un servicio virtualizado que se puede implementar fácil y rápidamente en cualquier lugar. Las organizaciones de TI utilizan los procesos estándar del centro de datos para tareas tales como aprovisionamiento, automatización y devolución de cargo para la infraestructura de entrega de aplicaciones web.
- NetScaler VPX abre nuevas arquitecturas de implementación que no son prácticas si solo se utilizan dispositivos físicos. Los dispositivos NetScaler VPX y NetScaler MPX se pueden utilizar de base, adaptados a las necesidades individuales de cada aplicación respectiva para manejar acciones intensivas del procesador, como la compresión y la inspección del firewall de aplicaciones. En el perímetro del centro de datos, los dispositivos NetScaler MPX manejan tareas de gran volumen en toda la red, como la distribución inicial del tráfico, el cifrado o descifrado SSL, la prevención de ataques de denegación de servicio (DoS) y el equilibrio de carga global. La combinación de los dispositivos NetScaler MPX de alto rendimiento con el dispositivo virtual NetScaler VPX fácil de implementar brinda una flexibilidad y capacidades de personalización sin igual a los entornos de centros de datos modernos a gran escala y a la vez que reduce los costes generales del centro de datos.

¿Cómo encaja NetScaler VPX en nuestra estrategia de centro de entrega de Citrix?

Con la disponibilidad de NetScaler VPX, toda la oferta de centros de entrega de Citrix está disponible como una oferta virtualizada. Todo el centro de entrega de Citrix se beneficia de las potentes capacidades de administración, aprovisionamiento, supervisión y generación de informes disponibles en Citrix XenCenter. Esto se puede implementar rápidamente en casi cualquier entorno y administrarse de forma centralizada desde cualquier lugar. Con una infraestructura de entrega de aplicaciones virtualizada e integrada, las organizaciones pueden ofrecer escritorios, aplicaciones cliente-servidor y aplicaciones web.

Cifrado

¿NetScaler VPX admite la descarga SSL?

Sí. Sin embargo, NetScaler VPX realiza todo el procesamiento SSL en el software, por lo que NetScaler VPX no ofrece el mismo rendimiento SSL que los dispositivos NetScaler. NetScaler VPX puede admitir hasta 750 nuevas transacciones SSL por segundo.

¿Las tarjetas SSL de terceros instaladas en el servidor que aloja NetScaler VPX aceleran el cifrado o el descifrado SSL?

No. La compatibilidad con tarjetas SSL de terceros no puede asociar NetScaler VPX a implementaciones de hardware específicas. Disminuye en gran medida la capacidad de una organización de alojar de forma flexible NetScaler VPX en cualquier lugar del centro de datos. Los dispositivos NetScaler MPX deben utilizarse cuando se requiere un rendimiento SSL superior al que proporciona NetScaler VPX.

¿Admite NetScaler VPX los mismos cifrados de cifrado que los dispositivos NetScaler físicos?

VPX admite todos los cifrados de cifrado como dispositivos NetScaler físicos, excepto ECDSA.

¿Cuál es el rendimiento de las transacciones SSL de NetScaler VPX?

Consulte la [hoja de datos de NetScaler VPX](#) para obtener información sobre el rendimiento de las transacciones SSL.

Precios y empaquetado

¿Cómo se empaqueta NetScaler VPX?

La selección de NetScaler VPX es similar a la selección de dispositivos NetScaler. En primer lugar, el cliente selecciona la edición NetScaler en función de sus requisitos de funcionalidad. A continuación, el cliente selecciona el nivel de ancho de banda específico de NetScaler VPX en función de sus requisitos de rendimiento. NetScaler VPX está disponible en las ediciones Standard, Advanced y Premium. NetScaler VPX ofrece desde 10 Mbps (VPX 10) a 100 Gbps (VPX 100G). Puede encontrar más detalles en la hoja de datos de NetScaler VPX.

¿El precio de NetScaler VPX es el mismo para todos los hipervisores?

Sí.

¿Se utilizan los mismos SKU de NetScaler para VPX en todos los hipervisores?

Sí.

¿Se puede mover una licencia de NetScaler VPX de un hipervisor a otro (por ejemplo, de VMware a Hyper-V)?

Sí. Las licencias de NetScaler VPX son independientes del hipervisor subyacente. Si decide mover la máquina virtual NetScaler VPX de un hipervisor a otro, no necesita obtener una nueva licencia. Sin embargo, es posible que deba volver a alojar la licencia existente de NetScaler VPX.

¿Se pueden actualizar las instancias NetScaler VPX?

Sí. Tanto los límites de rendimiento como la edición de la familia NetScaler se pueden actualizar. Hay disponibles SKU de actualización para ambos tipos de ascenso de clase.

Si quiero implementar NetScaler VPX en un par de alta disponibilidad, ¿cuántas licencias necesito?

Al igual que con los dispositivos físicos NetScaler, una configuración de alta disponibilidad de NetScaler requiere dos instancias activas. Por lo tanto, el cliente debe comprar dos licencias.

NetScaler VPX Express y prueba gratuita de 90 días

¿NetScaler VPX Express incluye toda la funcionalidad estándar de NetScaler? ¿Incluye NetScaler Gateway y equilibrio de carga para la interfaz web de Citrix Virtual Apps y el broker XML?

Sí. NetScaler VPX Express incluye toda la funcionalidad de NetScaler Premium. A partir de la versión 14.1–29.65 de NetScaler, NetScaler modificó el comportamiento de VPX Express.

¿Necesita una licencia NetScaler VPX Express?

Con la última versión de NetScaler VPX Express (14.1–29.65 y posteriores), VPX Express es de uso gratuito y no requiere un archivo de licencia para su instalación o uso. No es necesario ningún compromiso. Si ya tiene una licencia de VPX Express, el comportamiento de licencia anterior continúa vigente. Sin embargo, si elimina el archivo de licencia de VPX Express existente y usa la versión 14.1–29.65 o posterior, se aplicará el comportamiento actualizado de VPX Express.

¿Caduca la licencia de NetScaler VPX Express?

Con el nuevo VPX express, no hay licencia ni fecha de vencimiento. Si ya tiene una licencia VPX express, la licencia caduca un año después de la descarga.

¿Admite NetScaler VPX Express los mismos cifrados de cifrado que los dispositivos NetScaler MPX?

Para disponibilidad general, los mismos cifrados de cifrado seguros compatibles con los dispositivos NetScaler están disponibles en NetScaler VPX y NetScaler VPX Express. Está sujeto a las mismas regulaciones de importación o exportación.

¿Puedo presentar casos de soporte técnico para NetScaler VPX Express?

No. Los usuarios de NetScaler VPX Express pueden utilizar el Centro de conocimiento de NetScaler VPX y solicitar ayuda a la comunidad mediante los foros de discusión.

¿Se puede actualizar NetScaler VPX Express a una versión comercial?

Sí. Solo tiene que comprar la licencia comercial de NetScaler VPX que necesita y, a continuación, aplicar la licencia correspondiente a la instancia de NetScaler VPX Express.

Hypervisor

¿Qué versiones de VMware admite NetScaler VPX?

NetScaler VPX admite VMware ESX y ESXi para las versiones 3.5 o posterior. Para obtener más información, consulte [Matriz de soporte y pautas de uso](#)

Para VMware, ¿cuántas interfaces de red virtual puede asignar a un VPX?

Puede asignar hasta 10 interfaces de red virtuales a un dispositivo NetScaler VPX.

Desde vSphere, ¿cómo podemos acceder a la línea de comandos de NetScaler VPX?

El cliente de VMware vSphere proporciona acceso integrado a la línea de comandos de NetScaler VPX a través de una ficha de consola. Además, puede utilizar cualquier cliente SSH o Telnet para acceder a la línea de comandos. Puede utilizar la dirección NSIP de NetScaler VPX en el cliente SSH o Telnet.

¿Cómo puede acceder a la GUI de NetScaler VPX?

Para acceder a la GUI de NetScaler VPX, escriba el NSIP de NetScaler VPX, por ejemplo, <http://NSIPaddress> en el campo de dirección de cualquier explorador.

¿Se pueden configurar dos instancias NetScaler VPX instaladas en el mismo VMware ESX en una configuración de alta disponibilidad?

Sí, pero no es recomendable. Un fallo de hardware afectaría a ambas instancias de NetScaler VPX.

¿Se pueden configurar dos instancias NetScaler VPX que se ejecutan en dos sistemas VMware ESX diferentes en una configuración de alta disponibilidad?

Sí. Se recomienda en una configuración de alta disponibilidad.

Para VMware, ¿los eventos relacionados con la interfaz son compatibles con NetScaler VPX?

No. No se admiten los eventos relacionados con la interfaz.

Para VMware, ¿las VLAN etiquetadas son compatibles con NetScaler VPX?

Sí. Las VLAN etiquetadas de NetScaler se admiten en NetScaler VPX desde la versión 11.0 y versiones posteriores. Para obtener más información, consulte la documentación de [NetScaler](#).

Para VMware, ¿se admite la agregación de enlaces y LACP en NetScaler VPX?

No. La agregación de vínculos y LACP no son compatibles con NetScaler VPX. La agregación de enlaces debe configurarse a nivel de VMware.

¿Cómo accedemos a la documentación de NetScaler VPX?

La documentación está disponible en la GUI de NetScaler VPX. Después de iniciar sesión, seleccione la ficha **Documentación**.

Planificación o dimensionamiento de la capacidad

¿Qué rendimiento puedo esperar con NetScaler VPX?

NetScaler VPX ofrece un buen rendimiento. Consulte la [hoja de datos de NetScaler VPX](#) para obtener un nivel de rendimiento específico alcanzable mediante NetScaler VPX.

Dado que la potencia de la CPU del servidor varía, ¿cómo podemos estimar el rendimiento máximo de una instancia de NetScaler?

El uso de una CPU más rápida puede dar lugar a un mayor rendimiento (hasta el máximo permitido por la licencia), mientras que usar una CPU más lenta puede limitar el rendimiento.

¿Existen límites de ancho de banda o rendimiento de NetScaler VPX para el tráfico entrante o para el tráfico entrante y saliente?

Los límites de ancho de banda de NetScaler VPX se aplican únicamente al tráfico entrante a NetScaler, independientemente de si se trata del tráfico de solicitud o de respuesta. Indica que un NetScaler VPX-1000 (por ejemplo) puede procesar simultáneamente 1 Gbps de tráfico entrante y 1 Gbps de tráfico saliente. El tráfico entrante y saliente no es lo mismo que el tráfico de solicitud y respuesta. Para NetScaler, tanto el tráfico procedente de los dispositivos de punto final (tráfico de solicitudes) como el tráfico procedente de los servidores de origen (tráfico de respuesta) es “entrante”(es decir, entra en NetScaler).

¿Se pueden ejecutar varias instancias de NetScaler VPX en el mismo servidor?

Sí. Sin embargo, asegúrese de que el servidor físico tenga suficiente capacidad de CPU y E/S para soportar la carga de trabajo total que se ejecuta en el host; de lo contrario, el rendimiento de NetScaler VPX podría verse afectado.

Si se ejecuta más de una instancia de NetScaler VPX en un servidor físico, ¿cuál es el requisito mínimo de hardware por instancia de NetScaler VPX?

A cada instancia de NetScaler VPX se le deben asignar 2 GB de RAM física, 20 GB de espacio en el disco duro y 2 vCPU. Para implementaciones críticas, no recomendamos 2 GB de RAM para VPX porque el sistema funciona en un entorno con restricciones de memoria. Esto puede provocar problemas relacionados con la escala, el rendimiento o la estabilidad. Se recomienda 4 GB de RAM u 8 GB de RAM.

Nota:

El NetScaler VPX es un dispositivo virtual de alto rendimiento y sensible a la latencia. Para ofrecer el rendimiento esperado, el dispositivo requiere reserva de CPU virtuales, reserva de memoria y fijación de vCPU en el host. Además, el hipersubproceso debe estar inhabilitado en el host. Si el host no cumple estos requisitos, se producen problemas como conmutación por error de alta disponibilidad, picos de CPU dentro de la instancia VPX, lentitud en el acceso a la CLI VPX, fallo del demonio de pit boss, caídas de paquetes y bajo rendimiento.

Asegúrese de que todas las instancias VPX cumplan las condiciones predefinidas.

¿Puedo alojar NetScaler VPX y otras aplicaciones en el mismo servidor?

Sí. Por ejemplo, NetScaler VPX, Citrix Virtual Apps Web Interface y Citrix Virtual Apps XML Broker se pueden virtualizar y ejecutar en el mismo servidor. Para obtener el mejor rendimiento, asegúrese de que el host físico tenga suficiente capacidad de CPU y E/S para admitir todas las cargas de trabajo en ejecución.

¿Agregar núcleos de CPU a una única instancia de NetScaler VPX aumentará el rendimiento de esa instancia?

Dependiendo de la licencia, una instancia de NetScaler VPX puede usar hasta 4 vCPU en la actualidad. Agregar una CPU adicional a una instancia NetScaler VPX que puede utilizar más CPU aumenta el rendimiento.

¿Por qué NetScaler VPX parece consumir más del 90% de la CPU aunque esté inactiva?

Se trata de un comportamiento normal y los dispositivos NetScaler presentan el mismo comportamiento. Para ver la verdadera extensión de la utilización de CPU de NetScaler VPX, utilice el comando `stat CPU` en la CLI de NetScaler o vea el uso de CPU de NetScaler VPX desde la GUI de NetScaler. El motor de procesamiento de paquetes NetScaler siempre está “buscando trabajo”, incluso cuando no hay trabajo por hacer. Por lo tanto, hace todo lo posible para tomar el control de la CPU y no liberarla. En un servidor instalado con NetScaler VPX y nada más, da como resultado (desde la perspectiva del hipervisor) que NetScaler VPX consume toda la CPU. Al examinar la utilización de la CPU desde “dentro de NetScaler”(mediante la CLI o la GUI) se proporciona una imagen de la capacidad de CPU NetScaler VPX que se está usando.

Requisitos del sistema

¿Cuáles son los requisitos mínimos de hardware para NetScaler VPX?

En la siguiente tabla se explican los requisitos mínimos de hardware para NetScaler VPX.

Tipo	Requisitos
Procesador	Servidor de doble núcleo con Intel Xeon o AMD EPYC.
Memoria	Mínimo 2 GB. Sin embargo, se recomiendan 4 GB.
Disco	Disco duro mínimo de 20 GB.
Hypervisor	Citrix Hypervisor 5.6 o posterior, VMware ESX/ESXi 3.5 o posterior, o Windows Server 2008 R2 con Hyper-V
Conectividad de red	100 Mbps como mínimo, pero se recomienda 1 Gbps.
NIC	Una NIC compatible con el hipervisor que está utilizando.

Nota:

Para las implementaciones críticas, se prefiere una memoria de 4 GB para NetScaler VPX. Con 2 GB de memoria, NetScaler VPX funciona en un entorno con memoria limitada. Esto puede provocar problemas relacionados con la escala, el rendimiento o la estabilidad.

Para obtener más información sobre los requisitos del sistema, consulte la [hoja de datos de NetScaler VPX](#).

Nota:

A partir de la versión 13.1 de NetScaler, la instancia de NetScaler VPX en el hipervisor VMware ESXi es compatible con los procesadores AMD EPYC.

¿Qué es el Intel VT-x?

Estas funciones, a veces denominadas «asistencia de hardware» o «asistencia de virtualización», capturan las instrucciones de la CPU confidenciales o privilegiadas ejecutadas por el sistema operativo huésped y las envían al hipervisor. Esto simplifica el alojamiento de SO invitado (BSD para NetScaler VPX) en el hipervisor.

¿Qué tan comunes son las VT-x?

Prácticamente, todos los servidores enviados en los últimos dos años podrían admitir VT-x. Muchos servidores se envían con la asistencia de virtualización inhabilitada en el BIOS. Antes de asumir que no puede ejecutar NetScaler VPX, compruebe si necesita cambiar esta configuración en el servidor.

¿Existe una lista de compatibilidad de hardware (HCL) para NetScaler VPX?

Mientras el servidor sea compatible con Intel VT-x, NetScaler VPX debe ejecutarse en cualquier servidor compatible con el hipervisor subyacente. Consulte el HCL del hipervisor para obtener una lista completa de plataformas compatibles.

¿En qué versión del sistema operativo NetScaler se basa NetScaler VPX?

NetScaler VPX se basa en NetScaler 9.1 o versiones posteriores.

Dado que NetScaler VPX se ejecuta en BSD, ¿se puede ejecutar de forma nativa en un servidor con BSD Unix instalado?

No. NetScaler VPX requiere que se ejecute el hipervisor. Los soportes detallados de hipervisor se encuentran en la [hoja de datos de NetScaler VPX](#).

Otras preguntas frecuentes técnicas

¿Funciona la agregación de enlaces en un servidor físico con varias NIC?

LACP no es compatible. Para Citrix Hypervisor, se admite la agregación de vínculos estáticos y tiene límites de cuatro canales y siete interfaces virtuales. En el caso de VMware, NetScaler VPX no admite la agregación de vínculos estáticos, pero se puede configurar a nivel de VMware.

¿VPX admite el reenvío basado en MAC (MBF)? ¿Hay algún cambio en la implementación del dispositivo NetScaler? ¿Hay algún cambio en la implementación del dispositivo NetScaler?

MBF es compatible y se comporta del mismo modo que con el dispositivo NetScaler. Básicamente, el hipervisor cambia todos los paquetes recibidos de NetScaler VPX al exterior y viceversa.

¿Cómo se lleva a cabo el proceso de actualización de NetScaler VPX?

Las actualizaciones se realizan de la misma manera que para los dispositivos NetScaler: Descargue un archivo de kernel y use `install ns` o la utilidad de actualización en la GUI.

¿Cómo se asigna el espacio flash y en disco? ¿Podemos cambiarlo?

`/flash=965M /var = 14G` Se debe asignar un mínimo de 2 GB de memoria a cada instancia de NetScaler VPX. La imagen de disco NetScaler VPX tenía un tamaño de 20 GB para facilitar el mantenimiento, por ejemplo, espacio para tomar y almacenar volcados de memoria de hasta 4 GB y archivos de registro y seguimiento. Si bien sería posible generar una imagen de disco más pequeña, no hay planes de hacerlo en este momento. `/flash` y `/var` están en la misma imagen de disco. Se mantienen como sistemas de archivos separados para fines de compatibilidad. Para obtener recomendaciones detalladas sobre la asignación de memoria, consulte la [hoja de datos de NetScaler VPX](#).

¿Podemos agregar un nuevo disco duro para aumentar el espacio en la instancia de NetScaler VPX?

Sí. A partir de NetScaler versión 13.1 compilación 21.x, tiene la opción de aumentar el espacio en disco en la instancia de NetScaler VPX agregando un segundo disco. Al conectar el segundo disco, el directorio `/var/crash` se monta automáticamente en este disco. El segundo disco se utiliza para almacenar los archivos principales y el registro. Los directorios existentes que se utilizan para almacenar archivos principales y archivos de registro siguen funcionando como antes.

Nota:

Realice copias de seguridad externas al cambiar a una versión anterior del dispositivo NetScaler para evitar la pérdida de datos.

Para obtener información sobre cómo conectar una nueva unidad de disco duro (HDD) a una instancia de NetScaler VPX en una nube, consulte lo siguiente:

- [Documentación de Azure](#)

Nota:

Para conectar un disco secundario en las instancias de NetScaler VPX implementadas en Azure, asegúrese de que los tamaños de las máquinas virtuales de Azure tengan un disco temporal local. Para obtener más información, consulte [Tamaños de máquinas virtuales de Azure sin disco temporal local](#).

- [Documentación de AWS](#)
- [Documentación de GCP](#)

Advertencia:

Después de agregar un nuevo HDD a NetScaler VPX, algunos de los scripts que funcionan en archivos que se mueven al nuevo HDD pueden fallar en las siguientes condiciones:

Si utiliza el comando shell “link” para crear enlaces físicos a los archivos, que se movieron a un disco duro nuevo.

Sustituya todos estos comandos por “ln -s” para usar un enlace simbólico. Además, modifique los scripts que fallan en consecuencia.

¿Puedo aumentar el tamaño del disco principal en NetScaler VPX?

A partir de la versión 14.1 compilación 21.x de NetScaler, los administradores pueden aumentar de forma dinámica el tamaño del disco principal en NetScaler VPX de 20 GB a 1 TB a la vez. Y la vez siguiente, puede volver a aumentar hasta 1 TB. Para aumentar el espacio en disco, amplíe el tamaño del disco principal a un mínimo de 1 GB en la interfaz de usuario de nube o hipervisor correspondiente.

Nota:

Solo puede aumentar el tamaño de los discos. Una vez que se haya asignado el nuevo tamaño, no podrá reducirlo más adelante. Por lo tanto, aumente el tamaño del disco solo si es esencial.

¿Cómo puedo aumentar manualmente el tamaño del disco principal en NetScaler VPX?

Siga estos pasos para aumentar manualmente el tamaño del disco principal VPX desde un hipervisor o una nube:

1. Apague la VM.
2. Amplíe el tamaño de disco predeterminado de 20 GB a un valor superior. Por ejemplo, de 20 GB a 30 GB o 40 GB. Para Azure, amplíe el tamaño de disco predeterminado de 32 GB a 64 GB.
3. Encienda la máquina virtual e introduzca la línea de comandos de arranque.

4. Inicie sesión en el modo de usuario único con el comando “boot -s”.
5. Verifique el espacio en disco. Puede comprobar el espacio en disco recién asignado mediante el comando “gpart show”.
6. Anote el nombre de la partición. Por ejemplo, la partición de máquina virtual es da0.
7. Cambie el tamaño de la partición del disco con el comando “gpart resize”.

Ejemplo: Redimensionemos la partición MBR da0 para incluir 10 GB de espacio libre ejecutando el siguiente comando.

```
gpart resize -i 1 da0
```

8. Combine el espacio libre con la última partición.

Ejemplo

```
gpart resize -i 5 da0s1
```

9. Amplíe el sistema de archivos para incluir el espacio libre recién asignado mediante el comando “growfs”.

Ejemplo

```
growfs /dev/ada0s1e
```

10. Reinicie la máquina virtual y verifique el aumento del espacio en disco mediante el comando “df -h” en la línea de comandos del shell.

¿Qué podemos esperar de la numeración de compilaciones de NetScaler VPX y la interoperabilidad con otras compilaciones?

NetScaler VPX tiene una numeración de compilación similar a la 9.1. Cl (clásico) y 9.1. Versiones de Nc (NCore), por ejemplo, 9.1_97.3.vpx, 9.1_97.3.nc y 9.1_97.3.cl.

¿Puede NetScaler VPX formar parte de una configuración de alta disponibilidad con un dispositivo NetScaler?

No es una configuración compatible.

¿Todas las interfaces visibles en NetScaler VPX están directamente relacionadas con el número de interfaces del hipervisor?

No. Puede agregar hasta siete interfaces (10 para VMware) a través de la utilidad de configuración de NetScaler VPX con solo una NIC física en el hipervisor.

¿Se puede usar la migración en vivo de Citrix Hypervisor XenMotion, VMware vMotion o Hyper-V para mover instancias activas de NetScaler VPX?

NetScaler VPX no admite la migración en vivo de Hyper-V. vMotion se admite a partir de la versión 13.0 de NetScaler. vMotion es compatible a partir de la versión 13.0 de NetScaler. La migración en vivo (anteriormente XenMotion) se admite a partir de la versión 14.1 build 17.38 de NetScaler.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).