NetScaler VPX 14.1

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

NetScaler VPX-Unterstützungsmatrix

October 17, 2024

In diesem Dokument werden die verschiedenen Hypervisoren und Funktionen aufgeführt, die auf einer NetScaler VPX-Instanz unterstützt werden. Das Dokument beschreibt auch ihre Nutzungsrichtlinien und bekannten Einschränkungen.

VPX-Instanz auf dem VMware ESX-Hypervisor

| ESXi-Version | ESXi-Veröffentlichungsdatum (YYYY/MM/DD) | ESXi-Build-Nummer | NetScaler VPX Version | Leistungsbereich |
|———————————————————————————————|———————
- |————————|————————————|——————————|
ESXi 8.0 Update 3	2024/06/25	24022510	14.1-17.x und höhere Builds	10 Mbit/s bis 100 Gbit/s
VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G	–	23825572	14.1-17.x und höhere Builds	^^
ESXi 8.0 update 2b	2024/02/29	23305546	14.1-4.x und höhere Builds	^^
ESXi 8.0 Update 2	2023/09/21	22380479	14.1-4.x und höhere Builds	^^
ESXi 8.0-Aktualisierung 1	2023/04/18	21495797	14.1-4.x und höhere Builds	^^
ESXi 8.0c	2023/03/30	21493926	14.1-4.x und höhere Builds	^^
ESXi 8.0	2022/10/11	20513097	14.1-4.x und höhere Builds	^^
ESXi 7.0 Update 3o	–	23794027	14.1-17.x und höhere Builds	^^
ESXi 7.0 update 3p	–	23307199	14.1-4.x und höhere Builds	^^
ESXi 7.0 Update 3m	2023/09/28	22348816	14.1-4.x und höhere Builds	^^
ESXi 7.0 Aktualisierung 3n	2023/07/06	21930508	14.1-8.x und höhere Builds	^^
ESXi 7.0 Update 3m	2023/05/03	21686933	14.1-4.x und höhere Builds	^^

> **Hinweis:**
>
> Jede ESXi-Patchunterstützung wird für die in der obigen Tabelle angegebene NetScaler VPX-Version validiert und gilt für alle höheren Builds der NetScaler VPX 14.1-Version.

Weitere Informationen zu Nutzungsrichtlinien finden Sie unter Nutzungsrichtlinien für den VMware ESXi Hypervisor.

VPX-Instanz auf XenServer oder Citrix Hypervisor

XenServer- oder Citrix Hypervisor-Version	SysID	Leistungsbereich
8.4, unterstützt ab NetScaler VPX Version 14.1 Build 17.x 8.2, unterstützt ab NetScaler VPX Version 13.0 Build 64.x 8.0, 7.6, 7.1	450000	10 Mbit/s bis 40 Gbit/s

VPX-Instanz auf Microsoft Hyper-V

Hyper-V-Version	SysID	Leistungsbereich
2016, 2019	450020	10 Mbit/s bis 3 Gbit/s

VPX-Instanz auf Nutanix AHV

NetScaler VPX wird auf Nutanix AHV durch die Citrix Ready-Partnerschaft unterstützt. Citrix Ready ist ein Technologiepartnerprogramm, das Software- und Hardwareanbieter bei der Entwicklung und Integration ihrer Produkte mit der NetScaler-Technologie für digitale Workspace, Netzwerke und Analysen unterstützt.

Weitere Informationen zu einer schrittweisen Methode zur Bereitstellung einer NetScaler VPX-Instanz auf Nutanix AHV finden Sie unter Deploying aNetScaler VPX auf Nutanix AHV.

Unterstützung durch Dritte:

Wenn Sie Probleme mit der Integration eines bestimmten Drittanbieters (Nutanix AHV) in einer NetScaler-Umgebung haben, wenden Sie sich direkt an den Drittanbieter-Partner (Nutanix).

Wenn der Partner feststellt, dass das Problem offenbar bei NetScaler liegt, kann er sich an den NetScaler-Support wenden, um weitere Unterstützung zu erhalten. Eine spezielle technische Ressource von Partnern arbeitet mit dem NetScaler-Supportteam zusammen, bis das Problem behoben ist.

VPX-Instanz auf generischem KVM

Generische KVM-Version	SysID	Leistungsbereich
RHEL 7.6, RHEL 8.0, RHEL 9.3 Ubuntu 16.04, Ubuntu 18.04, Ubuntu 22.04	450070	10 Mbit/s bis 100 Gbit/s

Wichtige Hinweise:

Berücksichtigen Sie bei der Verwendung von KVM-Hypervisoren die folgenden Punkte.

- Die VPX-Instanz ist für Hypervisor Releaseversionen in Tabelle 1–4 und nicht für Patch-Releases innerhalb einer Version qualifiziert. Es wird jedoch erwartet, dass die VPX-Instanz nahtlos mit Patch-Versionen einer unterstützten Version funktioniert. Wenn dies nicht der Fall ist, öffnen Sie einen Supportfall für die Fehlerbehebung und das Debuggen.
- Bevor Sie RHEL 7.6 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:
  1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
  2. Generieren Sie grub.cfg mit dem Befehl `"# grub2-mkconfig -o /boot/grub2/grub.cfg"` neu.
  3. Starten Sie den Hostcomputer neu.
- Bevor Sie Ubuntu 18.04 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:
  1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
  2. Generieren Sie grub.cfg mit dem Befehl `"# grub-mkconfig -o /boot/grub/grub.cfg “` neu.
  3. Starten Sie den Hostcomputer neu.

VPX-Instanz in öffentlichen Clouds

Öffentliche Cloud	SysID	Leistungsbereich
AWS	450040	10 Mbit/s bis 30 Gbit/s
Azure	450020	10 Mbit/s bis 10 Gbit/s
GCP	450070	10 Mbit/s bis 10 Gbit/s

VPX-Funktionen, die auf Hypervisors unterstützt werden

Hypervisoren →	VPX auf XenServer				VPX auf VMware ESX					
^^Funktionen ↓	^^		^^				^^	^^		
Interfaces →	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Emuliert**	**PCI-Passthrough**	**PV**	**PV**	**SR-IOV**	**PCI-Passthrough**
Multi-PE-Unterstützung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Clustering-Unterstützung	Ja	Ja[1]	Ja	Ja[1]	Ja	Ja	Ja	Ja	Ja[1]	Ja
VLAN-Tagging	Ja	Ja	Ja	Ja	Ja	Ja	Ja (nur bei 2012R2)	Ja	Ja	Ja
Erkennen von Link-Ereignissen/HAMon	Nein[2]	Ja[3]	Nein[2]	Ja[3]	Nein[2]	Ja[3]	Nein[2]	Nein[2]	Ja[3]	Ja[3]
Konfiguration der Schnittstellen-parameter	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
Statische LA	Ja[2]	Ja[3]	Ja[2]	Nein	Ja[2]	Ja[3]	Ja[2]	Ja[2]	Ja[3]	Ja[3]
LACP	Nein	Ja[3]	Ja[2]	Nein	Ja[2]	Ja[3]	Nein	Ja[2]	Ja[3]	Ja[3]
Statische CLAG	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
LACP CLAG	Nein	Nein	Ja[2]	Nein	Ja[2]	Ja[3]	Nein	Ja[2]	Ja[3]	Ja[3]

^^Funktionen ↓	^^		^^				^^	^^		
Hot-Plug-fähig	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

VPX-Features, die in öffentlichen Clouds unterstützt werden

Öffentliche Clouds →	VPX auf AWS	VPX auf Azure	VPX auf GCP
^^Funktionen ↓	^^	^^	^^
Multi-PE-Unterstützung	Ja	Ja	Ja
Clustering-Unterstützung	Nein	Nein	Nein
VLAN-Tagging	Nein	Nein	Nein
Erkennen von Link-Ereignissen/HAMon	Nein[2]	Nein[2]	Nein[2]
Konfiguration der Schnittstellenparameter	Nein	Nein	Nein
Statische LA	Nein	Nein	Nein
LACP	Nein	Nein	Nein
Statische CLAG	Nein	Nein	Nein
LACP CLAG	Nein	Nein	Nein
Hot-Plug-fähig	Ja	Nein	Nein

Die in den beiden vorangegangenen Tabellen verwendeten hochgestellten Zahlen (1, 2, 3) beziehen sich auf die folgenden Punkte mit entsprechender Nummerierung:

1. Clustering-Unterstützung ist auf SRIOV für clientseitige und serverseitige Schnittstellen und nicht für die Rückwandplatine verfügbar.
2. Interface DOWN Ereignisse werden in NetScaler VPX-Instanzen nicht aufgezeichnet.

3. Für statische LA wird möglicherweise weiterhin Datenverkehr auf der Schnittstelle gesendet, deren physischer Status DOWN ist.

Die folgenden Punkte gelten für die jeweiligen Features, die in den beiden vorangegangenen Tabellen erfasst wurden:

- Für LACP kennt das Peer-Gerät das Interface DOWN-Ereignis basierend auf dem LACP-Timeout-Mechanismus.
  - Kurzes Timeout: 3 Sekunden
  - Langes Timeout: 90 Sekunden
- Teilen Sie für LACP keine Schnittstellen zwischen VMs.
- Beim dynamischen Routing hängt die Konvergenzzeit vom Routing-Protokoll ab, da Linkereignisse nicht erkannt werden.
- Die überwachte statische Route-Funktionalität schlägt fehl, wenn Sie keine Monitore an statische Routen binden, da der Routenstatus vom VLAN-Status abhängt. Der VLAN-Status hängt vom Verbindungsstatus ab.
- Eine teilweise Fehlererkennung erfolgt bei hoher Verfügbarkeit nicht, wenn ein Verbindungsfehler vorliegt. Eine Hohe-Verfügbarkeit-Split-Brain-Bedingung kann auftreten, wenn ein Verbindungsfehler vorliegt.
  - Wenn ein Linkereignis (Deaktivieren/Aktivieren, Zurücksetzen) von einer VPX-Instanz generiert wird, ändert sich der physische Status des Links nicht. Bei statischer LA wird jeder vom Peer initiierte Datenverkehr auf der Instanz gelöscht.
  - Damit die VLAN-Tagging-Funktion auf dem VMware ESX funktioniert, legen Sie die VLAN-ID der Portgruppe auf dem vSwitch des VMware ESX-Servers auf 1–4095 fest.
- Hot-Plug wird auf VPX-Instanzen mit ENA-Schnittstellen nicht unterstützt, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn ein Hot-Plugging versucht wird. Hot Adding wird nur für PV- und SRIOV-Schnittstellen mit NetScaler auf AWS unterstützt.
- Hot-Removal über die AWS-Webkonsole oder die AWS CLI-Schnittstelle wird mit den PV-, SRIOV- und ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn versucht wird, Hot-Removal durchzuführen.

Unterstützte Browser

Betriebssystem	Browser und Versionen
Windows 7	Internet Explorer-8, 9, 10 und 11; Mozilla Firefox 3.6.25 und höher; Google Chrome-15 und höher
Windows 64-Bit	Internet Explorer − 8, 9; Google Chrome − 15 und höher
MAC	Mozilla Firefox - 12 und höher; Safari - 5.1.3; Google Chrome - 15 und höher

AMD-Prozessorunterstützung für VPX-Instanzen

Ab NetScaler Version 13.1 unterstützt die VPX-Instanz sowohl die Intel- als auch die AMD-Prozessoren. Virtuelle VPX-Appliances können auf jedem Instanztyp bereitgestellt werden, der über zwei oder mehr virtualisierte Kerne und mehr als 2 GB Arbeitsspeicher verfügt. Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

VPX-Plattform vs. NIC-Matrixtabelle

In der folgenden Tabelle sind die Netzwerkkarten aufgeführt, die auf einer VPX-Plattform oder Cloud unterstützt werden.

NICs →	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/XL710 SRIOV VF	Intel X710/XL710/XXV710 PCI-Passthrough-Modus
^^Plattformen ↓	^^	^^	^^	^^	^^	^^
VPX (ESXi)	Nein	Ja	Nein	Ja	Nein	Ja
VPX (Citrix Hypervisor)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Ja	Nein
VPX (KVM)	Nein	Ja	Ja	Ja	Ja	Nein
VPX (Hyper-V)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nein	Nein	Nein

^^Plattformen ↓	^^	^^	^^	^^	^^	^^
VPX (AWS)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Nicht verfügbar	Nicht verfügbar
VPX (Azure)	Ja	Ja	Ja	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
VPX (GCP)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Andere Referenzen

- Für Citrix Ready-Produkte besuchen Sie Citrix Ready Marketplace.
- Informationen zum Citrix Ready-Produktsupport finden Sie auf der FAQ-Seite.
- Informationen zu VMware ESX-Hardwareversionen finden Sie unter Upgrade von VMware Tools.

Optimieren der Leistung von NetScaler VPX auf VMware ESX, Linux KVM und Citrix Hypervisors

October 17, 2024

Die Leistung von NetScaler VPX hängt stark vom Hypervisor, den zugewiesenen Systemressourcen und den Hostkonfigurationen ab. Um die gewünschte Leistung zu erzielen, befolgen Sie zunächst die Empfehlungen im VPX-Datenblatt und optimieren Sie es dann mithilfe der in diesem Dokument enthaltenen Best Practices weiter.

NetScaler VPX-Instanz auf VMware ESX-Hypervisoren

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf VMware ESX-Hypervisoren erzielen können.

- Empfohlene Konfiguration auf ESX-Hosts
- NetScaler VPX mit E1000-Netzwerkschnittstellen
- NetScaler VPX mit VMXNET3-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV- und PCI Passthrough-Netzwerkschnittstellen

Empfohlene Konfiguration auf ESX-Hosts

Befolgen Sie diese Empfehlungen, um eine hohe Leistung für VPX mit E1000-, VMXNET3-, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen:

- Die Gesamtzahl der auf dem ESX-Host bereitgestellten virtuellen CPUs (vCPUs) muss kleiner oder gleich der Gesamtzahl der physischen CPUs (PCPUs) auf dem ESX-Host sein.
- Affinität und CPU-Affinität für ungleichmäßigen Speicherzugriff (NUMA) müssen festgelegt werden, damit der ESX-Host gute Ergebnisse erzielt.

  —Um die NUMA-Affinität eines Vmnic zu ermitteln, melden Sie sich lokal oder remote beim Host an und geben Sie Folgendes ein:

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

  - Informationen zum Festlegen der NUMA- und vCPU-Affinität für eine VM finden Sie in der VMware-Dokumentation

NetScaler VPX mit E1000-Netzwerkschnittstellen

Nehmen Sie die folgenden Einstellungen auf dem VMware ESX-Host vor:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Empfangsthreads (Rx) auf dem ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den vNIC-Übertragungsdurchsatz (Tx) zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie die folgenden ESX-Befehle:

  - Für ESX Version 5.5:

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

  - Für ESX ab Version 6.0:

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

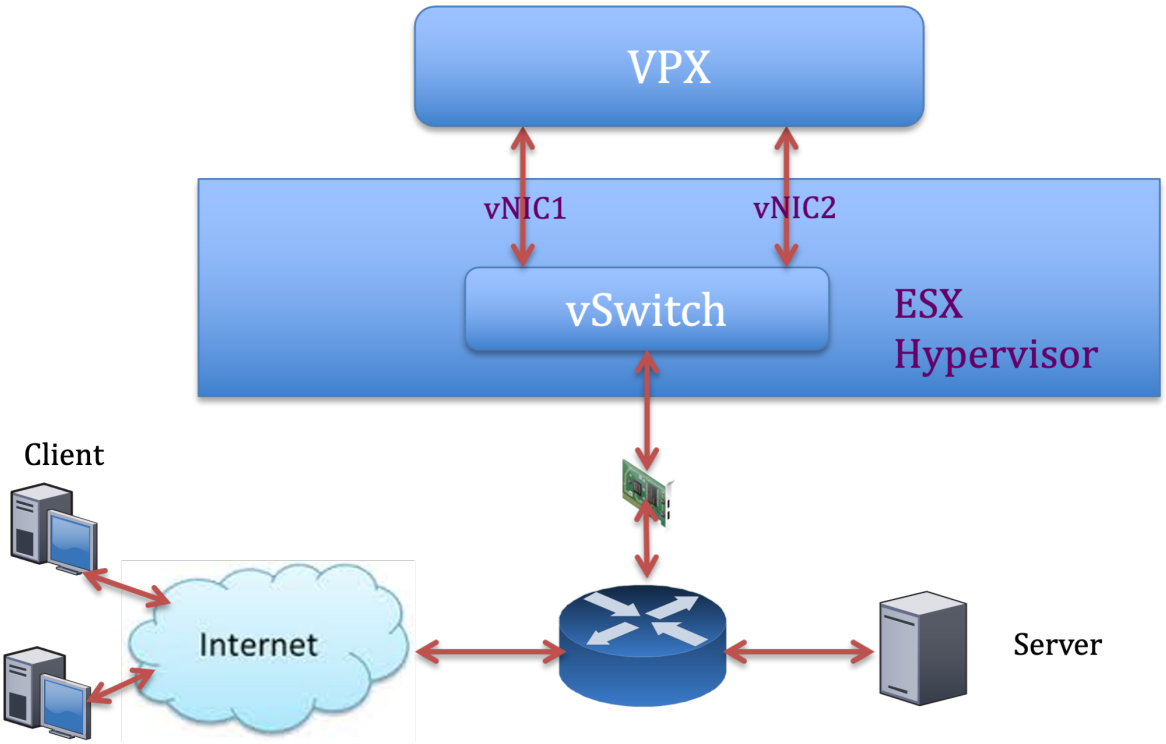
- Um den vNIC Tx-Durchsatz weiter zu erhöhen, verwenden Sie einen separaten Tx-Vervollständigungs-Thread und Rx-Threads pro Gerät (NIC) -Warteschlange. Verwenden Sie die folgenden ESX-Befehle:


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

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

Zwei vNICs pro pNIC-Bereitstellung

Im Folgenden finden Sie ein Beispiel für Topologie und Konfigurationsbefehle für das Bereitstellungsmodell mit **zwei vNICs pro pNIC**, das eine bessere Netzwerkleistung bietet.



NetScaler VPX Beispielkonfiguration:

Um die in der vorherigen Beispieltopologie gezeigte Bereitstellung zu erreichen, führen Sie die folgende Konfiguration auf der NetScaler VPX-Instanz durch:

- Binden Sie auf Clientseite das SNIP (1.1.1.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.

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

- Binden Sie auf der Serverseite das SNIP (2.2.2.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.


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

- Fügen Sie einen virtuellen HTTP-Server (1.1.1.100) hinzu und binden Sie ihn an einen Dienst (2.2.2.100).

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

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die folgenden beiden Einträge in die Routentabelle aufnehmen:
>
> - 1.1.1.0/24 Subnetz mit Gateway, das auf SNIP zeigt 1.1.1.2
> - 2.2.2.0/24 Subnetz mit Gateway, das auf SNIP zeigt 2.2.2.2

NetScaler VPX mit VMXNET3-Netzwerkschnittstellen

Um eine hohe Leistung für VPX mit VMXNET3-Netzwerkschnittstellen zu erzielen, nehmen Sie die folgenden Einstellungen auf dem VMware ESX-Host vor:

- Erstellen Sie zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Rx-Threads im ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den vNIC-Übertragungsdurchsatz (Tx) zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie den folgenden ESX-Befehl:
  - Für ESX Version 5.5:

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

  - Für ESX ab Version 6.0:

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

Führen Sie auf dem VMware ESX-Host die folgende Konfiguration durch:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Tx- und Rx-Threads im ESX-Host. Dies erhöht den Tx- und Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.

- Um den Tx-Durchsatz einer vNIC zu erhöhen, verwenden Sie einen separaten Tx-Vervollständigungs-Thread und Rx-Threads pro Gerät (NIC) -Warteschlange. Verwenden Sie den folgenden Befehl:

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

- Konfigurieren Sie eine VM für die Verwendung eines Übertragungs-Threads pro vNIC, indem Sie der Konfiguration der VM die folgende Einstellung hinzufügen:

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

- Konfigurieren Sie eine VM so, dass sie bis zu 8 Übertragungs-Threads pro vNIC verwendet, indem Sie der Konfiguration der VM die folgende Einstellung hinzufügen:

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

> **Hinweis:**
>
> Eine Erhöhung der Übertragungs-Threads pro vNIC erfordert mehr CPU-Ressourcen (bis zu 8) auf dem ESX-Host. Stellen Sie sicher, dass genügend CPU-Ressourcen verfügbar sind, bevor Sie die obigen Einstellungen vornehmen.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

Sie können VMXNET3 als Bereitstellung mit **zwei vNICs pro pNIC** konfigurieren. Weitere Informationen finden Sie unter Zwei vNICs pro pNIC-Bereitstellung.

Konfiguration der Multi-Queue- und RSS-Unterstützung auf VMware ESX für VMXNET3-Geräte
Standardmäßig unterstützt das VMXNET3-Gerät nur 8 Rx- und Tx-Warteschlangen. Wenn die Anzahl der vCPUs auf dem VPX 8 überschreitet, wird die Anzahl der für eine VMXNET3-Schnittstelle konfigurierten Rx- und Tx-Warteschlangen standardmäßig auf 1 gesetzt. Sie können bis zu 19 Rx- und Tx-Warteschlangen für VMXNET3-Geräte konfigurieren, indem Sie bestimmte Konfigurationen auf ESX ändern. Diese Option erhöht die Leistung und die gleichmäßige Verteilung der Pakete über die vCPUs der VPX-Instanz.

> **Hinweis:**
>
> Ab NetScaler Version 13.1 Build 48.x unterstützt NetScaler VPX bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräte.

Voraussetzungen:

Um bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräten zu konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die NetScaler VPX-Version ist 13.1 Build 48.X und höher.
- NetScaler VPX ist mit einer virtuellen Maschine der Hardwareversion 17 und höher konfiguriert, die von VMware ESX 7.0 und höher unterstützt wird.

Konfigurieren Sie VMXNET3-Schnittstellen für die Unterstützung von mehr als 8 Rx- und Tx-Warteschlangen:

1. Öffnen Sie die Konfigurationsdatei der virtuellen Maschine (.vmx).
2. Geben Sie die Anzahl der Rx- und TX-Warteschlangen an, indem Sie die `ethernetX.maxRxQueues` Werte `ethernetX.maxTxQueues` und konfigurieren (wobei X die Anzahl der zu konfigurierenden virtuellen NICs ist). Die maximale Anzahl der konfigurierten Warteschlangen darf nicht größer als die Anzahl der vCPUs in der virtuellen Maschine sein.

   > **Hinweis:**
   >
   > Eine Erhöhung der Anzahl der Warteschlangen erhöht auch den Prozessor-Overhead auf dem ESX-Host. Stellen Sie daher sicher, dass ausreichend CPU-Ressourcen auf dem ESX-Host verfügbar sind, bevor Sie die Warteschlangen erhöhen. Sie können die maximale Anzahl der unterstützten Warteschlangen in Szenarien erhöhen, in denen die Anzahl der Warteschlangen als Leistungsengpass identifiziert wird. In diesen Situationen empfehlen wir, die Anzahl der Warteschlangen schrittweise zu erhöhen. Zum Beispiel von 8 bis 12, dann bis 16, dann bis 20 und so weiter. Bewerten Sie die Leistung bei jeder Einstellung, anstatt sie direkt bis zur Höchstgrenze zu erhöhen.

NetScaler VPX mit SR-IOV- und PCI Passthrough-Netzwerkschnittstellen

Um eine hohe Leistung für NetScaler VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen, siehe Empfohlene Konfiguration auf ESX-Hosts.

Nutzungsrichtlinien für den VMware ESXi Hypervisor

- Wir empfehlen Ihnen, eine NetScaler VPX-Instanz auf lokalen Festplatten des Servers oder SAN-basierten Speichervolumes bereitzustellen.

  Weitere Informationen finden Sie im Abschnitt **VMware ESXi CPU Considerations** im Dokument Performance Best Practices for VMware vSphere 6.5. Hier ist ein Auszug:

- Es wird nicht empfohlen, virtuelle Maschinen mit hohem CPU- oder Speicherbedarf auf einem überlasteten Host oder Cluster bereitzustellen.

- In den meisten Umgebungen ermöglicht ESXi eine erhebliche CPU-Überbelegung, ohne die Leistung der virtuellen Maschine zu beeinträchtigen. Auf einem Host können Sie mehr vCPUs ausführen als die Gesamtzahl der physischen Prozessorkerne in diesem Host.
- Wenn ein ESXi-Host CPU-gesättigt wird, d.h. die virtuellen Maschinen und andere Lasten auf dem Host alle CPU-Ressourcen verlangen, die der Host hat, funktionieren latenzsensitive Workloads möglicherweise nicht gut. Reduzieren Sie in diesem Fall beispielsweise die CPU-Last, indem Sie einige virtuelle Maschinen ausschalten oder sie auf einen anderen Host migrieren (oder DRS erlauben, sie automatisch zu migrieren).
- NetScaler empfiehlt, die neueste Hardwarekompatibilitätsversion zu verwenden, um die neuesten Funktionen des ESXi Hypervisors für die virtuelle Maschine nutzen zu können. Weitere Informationen zur Hardware- und ESXi-Versionskompatibilität finden Sie in der VMware-Dokumentation.
- Der NetScaler VPX ist eine latenzempfindliche, leistungsstarke virtuelle Appliance. Um die erwartete Leistung zu erbringen, benötigt die Appliance vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert werden. Wenn der Host diese Anforderungen nicht erfüllt, können die folgenden Probleme auftreten:
  - Hochverfügbares Failover
  - CPU-Spitze innerhalb der VPX-Instanz
  - Trägheit beim Zugriff auf die VPX-CLI
  - Absturz des Pitboss-Daemons
  - Paketverluste
  - Niedriger Durchsatz
- Ein Hypervisor gilt als übermäßig bereitgestellt, wenn eine der folgenden beiden Bedingungen erfüllt ist:
  - Die Gesamtzahl der auf dem Host bereitgestellten virtuellen Kerne (vCPU) ist größer als die Gesamtzahl der physischen Kerne (pCPUs).
  - Die Gesamtzahl der bereitgestellten VMs verbrauchen mehr vCPUs als die Gesamtzahl der pCPUs.

    Wenn eine Instanz übermäßig bereitgestellt wird, garantiert der Hypervisor möglicherweise nicht die für die Instanz reservierten Ressourcen (wie CPU, Speicher und andere) aufgrund von Hypervisor-Planungs-Overheads, Fehlern oder Einschränkungen mit dem Hypervisor. **Dieses Verhalten kann zu einem Mangel an CPU-Ressourcen für NetScaler führen und zu den im ersten Punkt unter Nutzungsrichtlinien genannten Problemen führen. Wir empfehlen den Administratoren, die Tenancy des Hosts so zu reduzieren, dass die Gesamtzahl der auf dem Host bereitgestellten vCPUs kleiner oder gleich der Gesamtzahl der pCPUs ist.

Beispiel

Wenn für den ESX-Hypervisor der Parameter %RDY% einer VPX-vCPU in der Befehlsausgabe `esxtop` größer als 0 ist, wird für den ESX-Host ein Planungsaufwand gemeldet, der zu latenzbedingten Problemen für die VPX-Instanz führen kann.

Reduzieren Sie in einer solchen Situation die Mandanten auf dem Host, sodass %RDY% immer auf 0 zurückkehrt. Wenden Sie sich alternativ an den Hypervisor-Anbieter, um den Grund für die Nichteinhaltung der Ressourcenreservierung zu ermitteln.

Befehle zur Steuerung der CPU-Auslastung der Paket-Engine

Sie können zwei Befehle (`set ns vpxparam` und `show ns vpxparam`) verwenden, um das CPU-Auslastungsverhalten von VPX-Instanzen in Hypervisor- und Cloud-Umgebungen zu steuern:

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

  Erlauben Sie jeder VM, die CPU-Ressourcen zu verwenden, die einer anderen VM zugewiesen sind, aber nicht verwendet werden.

  Parameter für `Set ns vpxparam`:

  -cpuyield: Freigabe von zugewiesenen, aber nicht genutzten CPU-Ressourcen.

  - **YES**: Erlauben Sie, dass zugewiesene, aber ungenutzte CPU-Ressourcen von einer anderen VM verwendet werden.
  - **NEIN**: Reservieren Sie alle CPU-Ressourcen für die VM, der sie zugewiesen wurden. Diese Option zeigt in Hypervisor- und Cloud-Umgebungen einen höheren Prozentsatz für die VPX-CPU-Auslastung.
  - **DEFAULT**: Nein.

  > **Hinweis:**
  >
  > Auf allen NetScaler VPX-Plattformen beträgt die vCPU-Auslastung auf dem Hostsystem 100 Prozent. Verwenden Sie den Befehl `set ns vpxparam –cpuyield YES`, um diese Verwendung zu überschreiben.

  Wenn Sie die Clusterknoten auf “yield”setzen möchten, müssen Sie die folgenden zusätzlichen Konfigurationen für CCO durchführen:

  - Wenn ein Cluster gebildet wird, werden alle Knoten auf “yield=default”gesetzt.
  - Wenn ein Cluster unter Verwendung der Knoten gebildet wird, die bereits auf “yield=YES” eingestellt sind, werden die Knoten mit “yield=DEFAULT”zum Cluster hinzugefügt.

> **Hinweis:**
>
> Wenn Sie die Clusterknoten auf “yield=YES”setzen möchten, können Sie erst nach der Bildung des Clusters konfigurieren, aber nicht bevor der Cluster gebildet wurde.

-masterclockcpu1: Sie können die Haupttaktquelle von CPU0 (Management-CPU) auf CPU1 verschieben. Dieser Parameter hat die folgenden Optionen:

- **YES**: Erlauben Sie der VM, die Haupttaktquelle von CPU0 auf CPU1 zu verschieben.
- **NO**: VM verwendet CPU0 für die Haupttaktquelle. Standardmäßig ist CPU0 die Haupttaktquelle.

- `show ns vpxparam`

  Dieser Befehl zeigt die aktuellen `vpxparam` Einstellungen an.

NetScaler VPX-Instanz auf Linux-KVM-Plattform

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf der Linux-KVM-Plattform erzielen können.

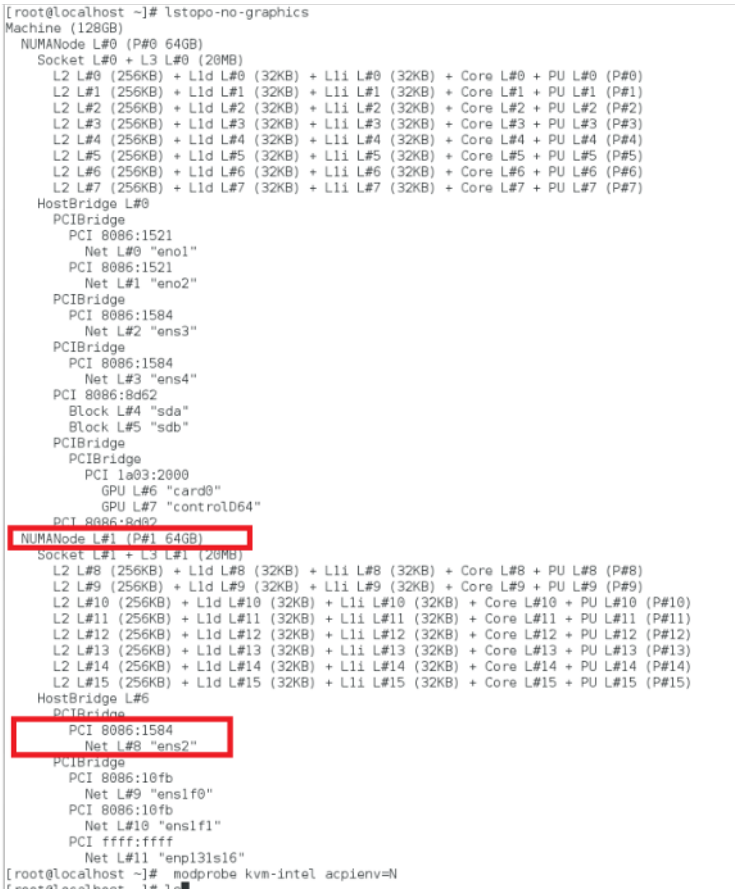
- Leistungseinstellungen für KVM
- NetScaler VPX mit PV-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV und Fortville PCIe Passthrough-Netzwerkschnittstellen

Leistungseinstellungen für KVM

Nehmen Sie die folgenden Einstellungen auf dem KVM-Host vor:

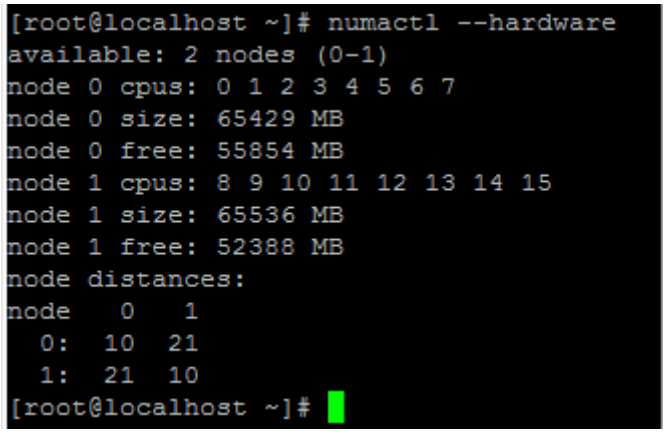
Finden Sie die NUMA-Domäne der NIC mit dem `lstopo` Befehl:

Stellen Sie sicher, dass der Speicher für den VPX und die CPU an derselben Stelle angeheftet ist. In der folgenden Ausgabe ist die 10G-NIC “ens2”an die NUMA-Domäne #1 gebunden.



Weisen Sie den VPX-Speicher aus der NUMA-Domäne zu.

Der `numactl` Befehl gibt die NUMA-Domäne an, von der der Speicher zugewiesen wird. In der folgenden Ausgabe werden etwa 10 GB RAM vom NUMA-Knoten #0 zugewiesen.



Gehen Sie folgendermaßen vor, um die NUMA-Knotenzuordnung zu ändern.

1. Bearbeiten Sie die XML des VPX auf dem Host.

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


2. Fügen Sie das folgende Tag hinzu:

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

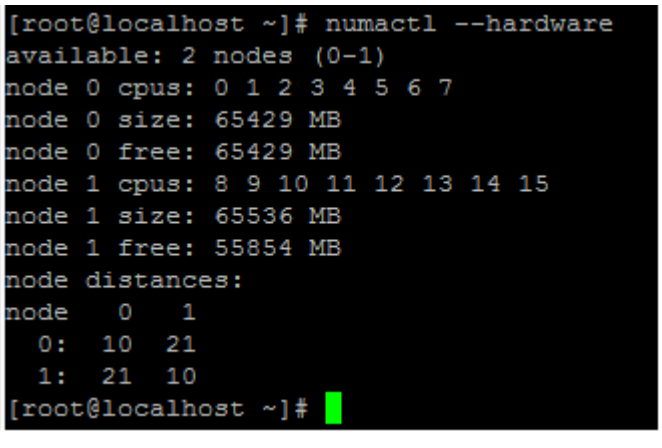
3. Fahren Sie den VPX herunter.

4. Führen Sie den folgenden Befehl aus:

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

   Dieser Befehl aktualisiert die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen.

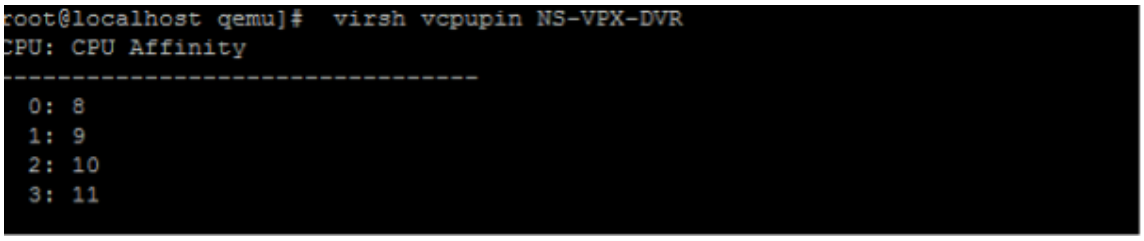
5. Schalten Sie den VPX ein. Überprüfen Sie dann die `numactl –hardware` Befehlsausgabe auf dem Host, um die aktualisierten Speicherzuweisungen für den VPX zu sehen.



Pin vCPUs von VPX an physische Kerne.

- Um die vCPU zu pCPU-Zuordnungen einer VPX anzuzeigen, geben Sie den folgenden Befehl ein

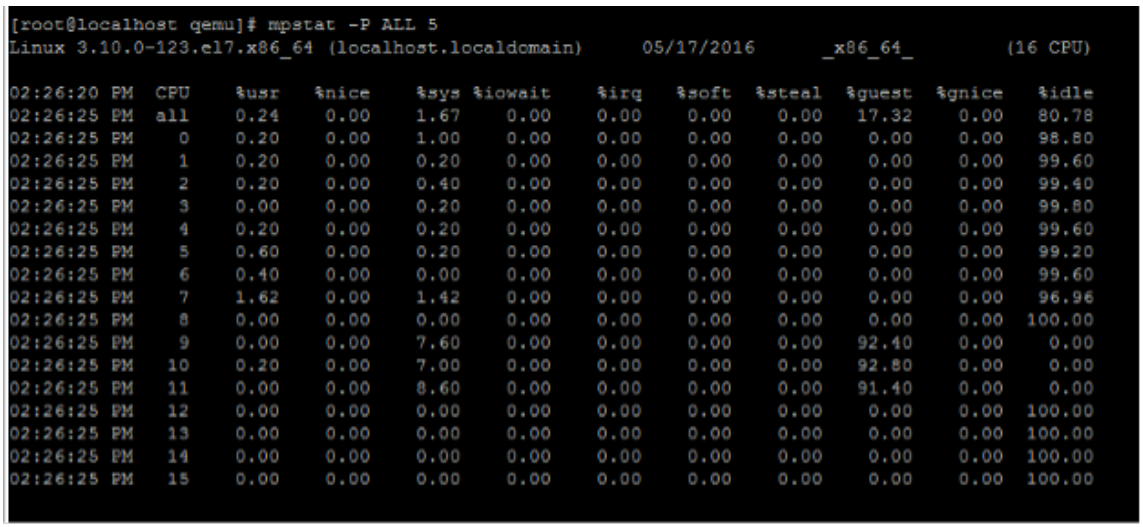
```
virsh vcpupin <VPX name>
```



  Die vCPUs 0—4 werden physikalischen Kernen 8—11 zugeordnet.

- Um die aktuelle pCPU-Nutzung anzuzeigen, geben Sie den folgenden Befehl ein:

```
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
```

In dieser Ausgabe ist 8 Management-CPU und 9—11 Paket-Engines.

- Um die vCPU auf pCPU-Pinning zu ändern, gibt es zwei Möglichkeiten.
  - Ändern Sie es zur Laufzeit, nachdem der VPX mit dem folgenden Befehl hochgefahren wurde:

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

  - Um statische Änderungen an der VPX vorzunehmen, bearbeiten Sie die `.xml` Datei wie zuvor mit den folgenden Tags:

    1. Bearbeiten Sie die XML-Datei des VPX auf dem Host

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

    2. Fügen Sie das folgende Tag hinzu:

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

    3. Fahren Sie den VPX herunter.
    4. Aktualisieren Sie die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen mithilfe des folgenden Befehls:

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


5. Schalten Sie den VPX ein. Überprüfen Sie dann die `virsh vcpupin <VPX name>` Befehlsausgabe auf dem Host, um das aktualisierte CPU-Pinning zu sehen.

Eliminieren Sie Host-Interrupt-Overhead.

- Erkennt VM_EXITS mithilfe des `kvm_stat` Befehls.

  Auf Hypervisor-Ebene werden Host-Interrupts denselben PCPUs zugeordnet, auf denen die vCPUs des VPX angeheftet sind. Dies kann dazu führen, dass vCPUs auf dem VPX regelmäßig rausgeschmissen werden.

  Verwenden Sie den `kvm_stat` Befehl, um die VM-Exits zu finden, die von VMs durchgeführt wurden, auf denen der Host ausgeführt wird

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

  Ein höherer Wert in der Größenordnung von 1+M weist auf ein Problem hin.

  Wenn eine einzelne VM vorhanden ist, liegt der erwartete Wert bei 30–100 K. Alles darüber hinaus kann darauf hinweisen, dass ein oder mehrere Host-Interrupt-Vektoren derselben pCPU zugeordnet sind.

- Erkennen Sie Host-Interrupts und migrieren Sie Host-Interrupts.

  Wenn Sie den `concatenate` Befehl für die Datei "/proc/interrupts"ausführen, werden alle Host-Interrupt-Zuordnungen angezeigt. Wenn ein oder mehrere aktive IRQs derselben pCPU zugeordnet werden, erhöht sich der entsprechende Zähler.

  Verschieben Sie alle Interrupts, die sich mit den PCPUs Ihres NetScaler VPX überschneiden, auf ungenutzte PCPUs:

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

- Deaktivieren Sie das IRQ Guthaben

  Deaktivieren Sie den IRQ-Balance-Daemon, damit im laufenden Betrieb keine Umschuldung erfolgt.

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

  Stellen Sie sicher, dass Sie den `kvm_stat` Befehl ausführen, um sicherzustellen, dass es nicht viele Zähler gibt.

NetScaler VPX mit PV-Netzwerkschnittstellen

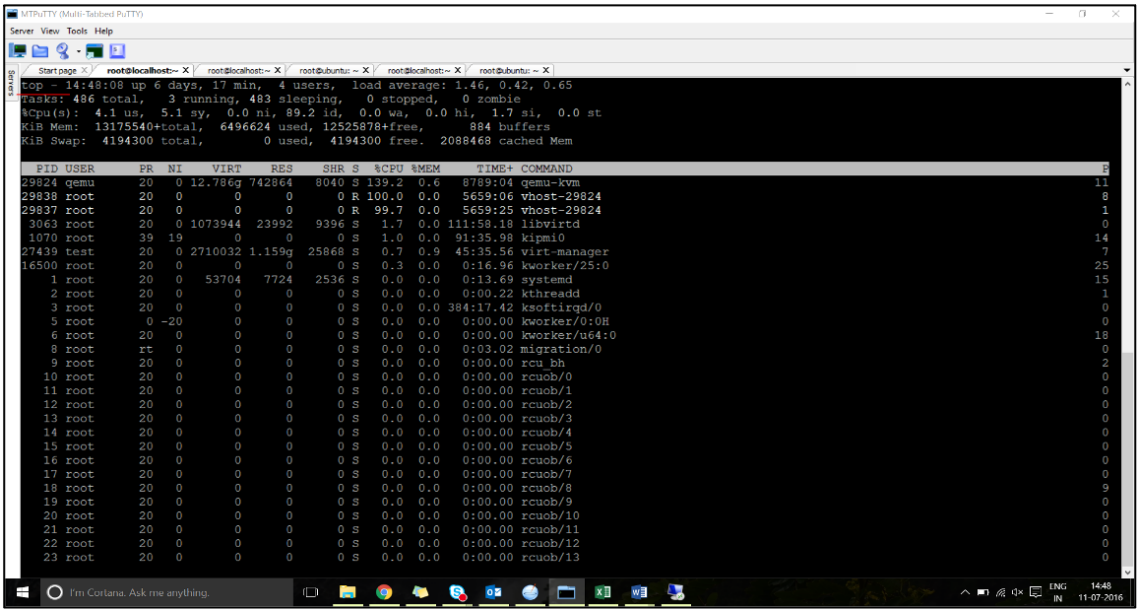
Sie können Para-Virtualization (PV), SR-IOV und PCIe-Passthrough-Netzwerkschnittstellen als **Zwei vNICs pro pNIC-Bereitstellung** konfigurieren. Weitere Informationen finden Sie unter Zwei vNICs pro pNIC-Bereitstellung.

Gehen Sie folgendermaßen vor, um eine optimale Leistung von PV (virtio) -Schnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/die NIC gehört.
- Der Speicher und die vCPU für den VPX müssen an dieselbe NUMA-Domäne angeheftet sein.
- Der Vhost-Thread muss an die CPUs in derselben NUMA-Domäne gebunden sein.

Binden Sie die virtuellen Host-Threads an die entsprechenden CPUs:

1. Sobald der Verkehr gestartet wurde, führen Sie den `top` Befehl auf dem Host aus.



2. Identifizieren Sie die Affinität des virtuellen Host-Prozesses (benannt als `vhost-<pid-of-qemu>`).
3. Binden Sie die vHost-Prozesse mit dem folgenden Befehl an die zuvor identifizierten physischen Kerne in der NUMA-Domäne:

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

Beispiel

```
taskset -pc 12 29838
```

4. Die Prozessorkerne, die der NUMA-Domäne entsprechen, können mit dem folgenden Befehl identifiziert werden:


```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>

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

    <cpuselection/>
    <cpuselection/>
```

Binden Sie den QEMU-Prozess an den entsprechenden physikalischen Kern:

1. Identifizieren Sie die physikalischen Kerne, auf denen der QEMU-Prozess läuft. Weitere Informationen finden Sie in der vorhergehenden Ausgabe.
2. Binden Sie den QEMU-Prozess mit dem folgenden Befehl an dieselben physikalischen Kerne, an die Sie die vCPUs binden:

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

NetScaler VPX mit SR-IOV und Fortville PCIe Passthrough-Netzwerkschnittstellen

Gehen Sie folgendermaßen vor, um eine optimale Leistung der SR-IOV- und Fortville PCIe-Passthrough-Netzwerkschnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/die NIC gehört.
- Der Speicher und die vCPU für NetScaler VPX müssen an dieselbe NUMA-Domäne gebunden sein.

Beispiel für eine VPX-XML-Datei für vCPU und Speicher-Pinning für Linux KVM:


```
<domain type='kvm'>
    <name>NetScaler-VPX</name>
    <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
    <memory unit='KiB'>8097152</memory>
    <currentMemory unit='KiB'>8097152</currentMemory>
    <vcpu placement='static'>4</vcpu>

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

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

</domain>
```

NetScaler VPX-Instanz auf Citrix Hypervisors

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf Citrix Hypervisors erzielen können.

- Leistungseinstellungen für Citrix Hypervisors
- NetScaler VPX mit SR-IOV-Netzwerkschnittstellen
- NetScaler VPX mit paravirtualisierten Schnittstellen

Leistungseinstellungen für Citrix Hypervisors

Finden Sie die NUMA-Domäne der NIC mit dem Befehl “xl”:

```
xl info -n
```

Pin vCPUs von VPX an physische Kerne.

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

Überprüfen Sie die Bindung von vCPUs.

```
xl vcpu-list
```

Weisen Sie NetScaler VMs mehr als 8 vCPUs zu.

Führen Sie zum Konfigurieren von mehr als 8 vCPUs die folgenden Befehle von der Citrix Hypervisor-Konsole aus:


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

NetScaler VPX mit SR-IOV-Netzwerkschnittstellen

Gehen Sie folgendermaßen vor, um eine optimale Leistung der SR-IOV-Netzwerkschnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, an die der PCIe-Steckplatz oder die NIC gebunden ist.
- Stecken Sie den Speicher und die vCPU für den VPX an dieselbe NUMA-Domäne an.
- Binden Sie die Domain-0 vCPU an die verbleibende CPU.

NetScaler VPX mit paravirtualisierten Schnittstellen

Für eine optimale Leistung werden zwei vNICs pro pNIC und eine vNIC pro pNIC-Konfiguration empfohlen, wie in anderen PV-Umgebungen.

Gehen Sie folgendermaßen vor, um eine optimale Leistung paravirtualisierter (Netfront) Schnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz oder die NIC gehört.
- Stecken Sie den Speicher und die vCPU für den VPX an dieselbe NUMA-Domäne an.
- Binden Sie die Domain-0 vCPU an die verbleibende CPU derselben NUMA-Domäne.
- Pin Host Rx/Tx-Threads von vNIC an Domain-0 vCPUs.

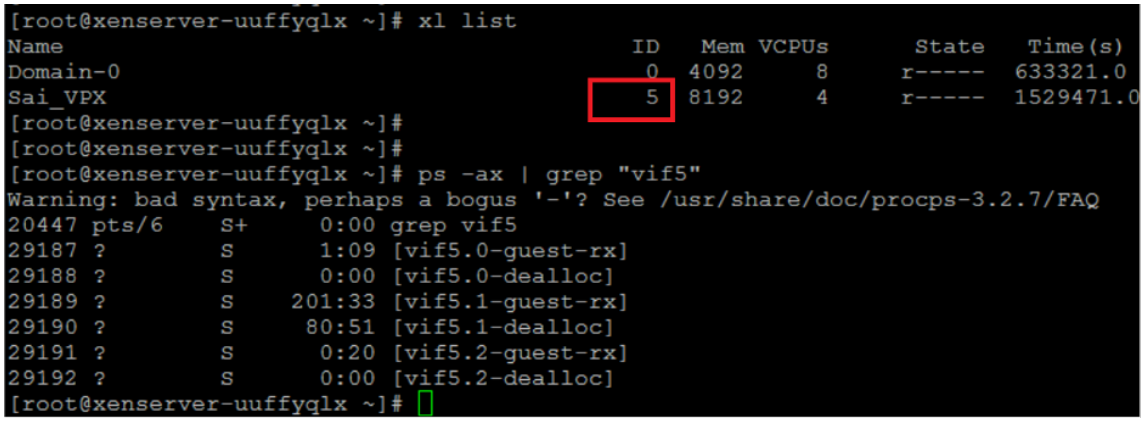
Host-Threads an Domain-0 vCPUs anheften:

1. Suchen Sie die Xen-ID von NetScaler VPX mithilfe des Befehls `xl list` in der Citrix Hypervisor-Host-Shell.
2. Identifizieren Sie Host-Threads mithilfe des folgenden Befehls:

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

   Im folgenden Beispiel zeigen diese Werte an:

   - **vif5.0** – Die Threads für die erste Schnittstelle, die VPX in XenCenter (Verwaltungsschnittstelle) zugewiesen ist.
   - **vif5.1** – Die Threads für die zweite Schnittstelle, die VPX usw. zugewiesen ist.



3. Stecken Sie die Threads mit dem folgenden Befehl an Domain-0 vCPUs an:

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

Beispiel

```
taskset -pc 1 29189
```

NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in der Cloud anwenden

October 17, 2024

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in einer Cloud-Umgebung anwenden. Diese Phase wird in diesem Dokument als **Preboot-Phase** behandelt. Daher wird in bestimmten Fällen wie der ADC-gepoolten Lizenzierung eine bestimmte VPX-Instanz in viel geringerer Zeit aufgebracht. Diese Funktion ist in Microsoft Azure, Google Cloud-Plattform und AWS-Clouds verfügbar.

Was sind Benutzerdaten

Wenn Sie eine VPX-Instanz in einer Cloud-Umgebung bereitstellen, haben Sie die Möglichkeit, Benutzerdaten an die Instanz zu übergeben. Mit den Benutzerdaten können Sie allgemeine automatisierte Konfigurationsaufgaben ausführen, das Startverhalten von Instanzen anpassen und Skripts ausführen, nachdem die Instanz gestartet wurde. Beim ersten Start führt die NetScaler VPX-Instanz die folgenden Aufgaben aus:

- Liest die Benutzerdaten.
- Interpretiert die in Benutzerdaten bereitgestellte Konfiguration.
- Wendet die neu hinzugefügte Konfiguration beim Booten an.

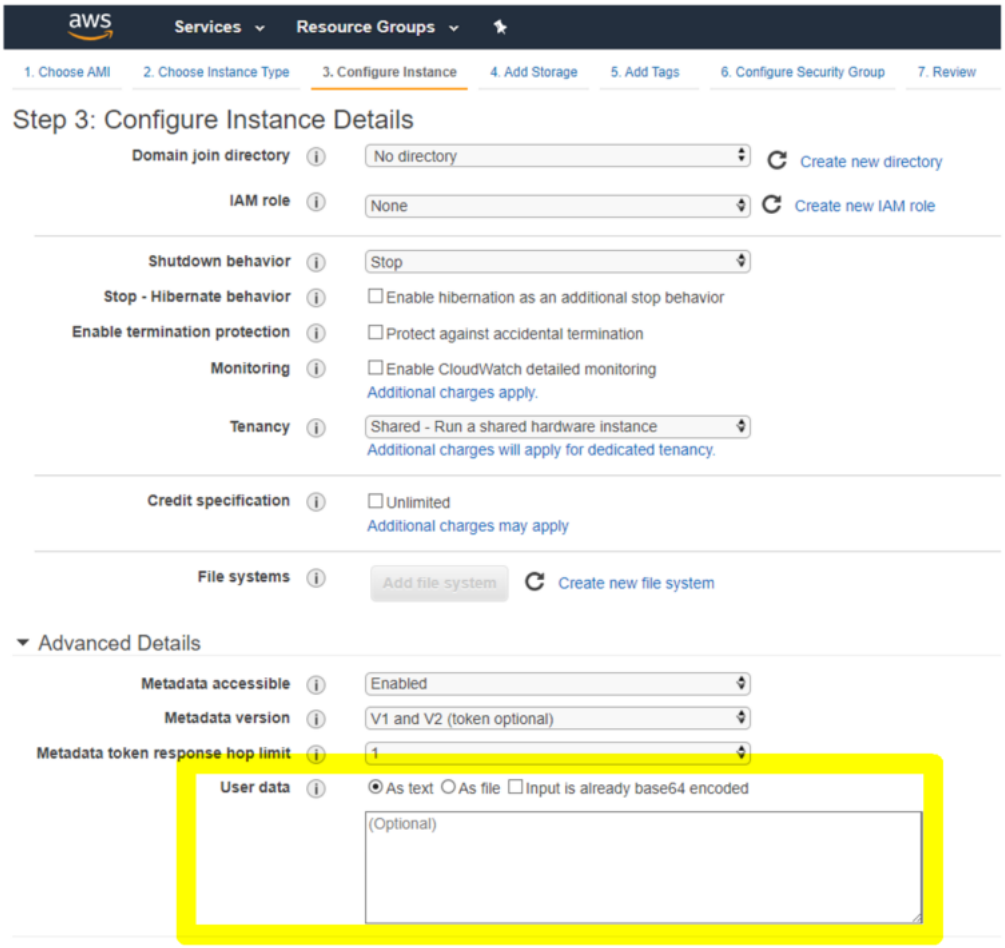
So stellen Sie Preboot-Benutzerdaten in Cloud-Instanz zur Verfügung

Sie können der Cloud-Instanz Preboot-Benutzerdaten im XML-Format zur Verfügung stellen. Verschiedene Clouds haben unterschiedliche Schnittstellen zur Bereitstellung von Benutzerdaten.

Bereitstellung von Preboot-Benutzerdaten über die AWS-Konsole

Wenn Sie eine NetScaler VPX-Instanz über die AWS-Konsole bereitstellen, navigieren **Sie zu Instanzdetails konfigurieren > Erweiterte Details**und geben Sie die Preboot-Benutzerdatenkonfiguration im Feld **Benutzerdaten** an.

Ausführliche Anweisungen zu den einzelnen Schritten finden Sie unter Stellen Sie mithilfe der AWS-Webkonsole eine NetScaler VPX-Instanz auf AWS bereit. Weitere Informationen finden Sie in der AWS-Dokumentation zum Starten einer Instanz.



> **Hinweis:**
>
> Der reine AWS-IMDSv2-Modus für die Preboot-Benutzerdatenfunktion wird ab NetScaler VPX Ver-

> sion 13.1.48.x und späteren Versionen unterstützt.

Bereitstellung von Preboot-Benutzerdaten mit AWS CLI

Geben Sie den folgenden Befehl in die AWS CLI ein:

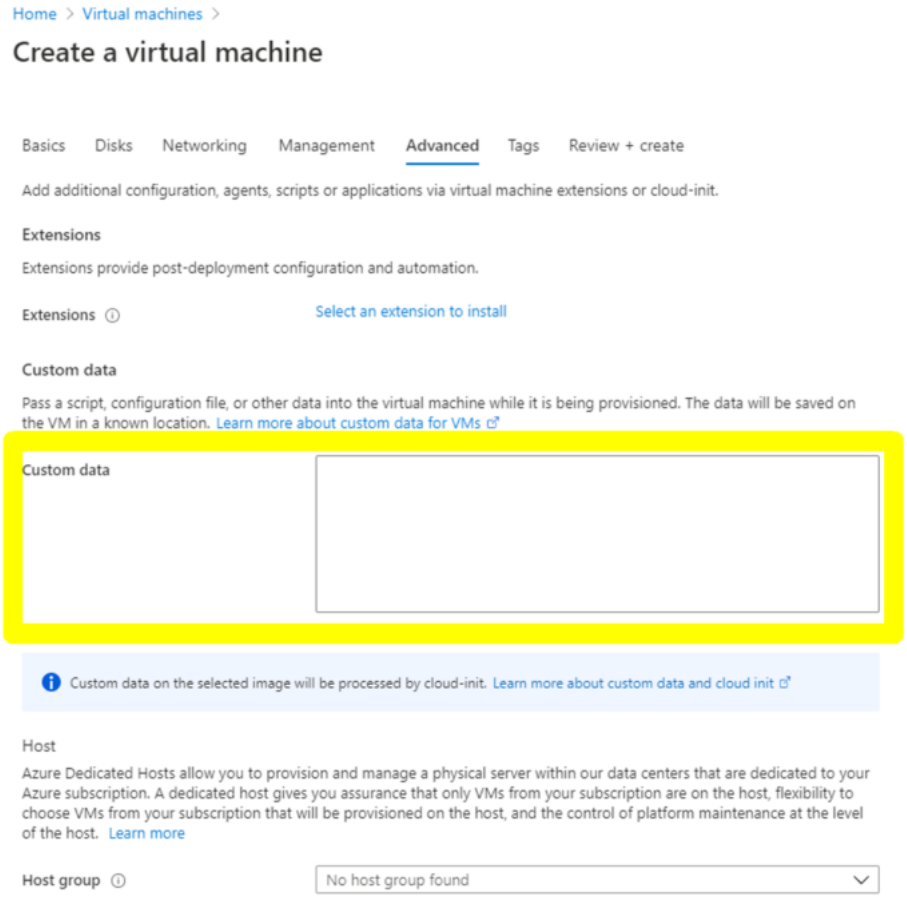
```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
```

Weitere Informationen finden Sie in der AWS-Dokumentation zu Running Instances.

Weitere Informationen finden Sie in der AWS-Dokumentation zur Verwendung von Instanz-Benutzerdaten

Stellen Sie Preboot-Benutzerdaten mit der Azure-Konsole bereit

Wenn Sie eine NetScaler VPX-Instanz mit der Azure-Konsole bereitstellen, navigieren **Sie zu Virtuelle Maschine erstellen > Erweitert** . Geben Sie im Feld **Benutzerdefinierte Daten** eine Preboot-Benutzerdatenkonfiguration an.



Bereitstellen von Preboot-Benutzerdaten mit der Azure CLI

Geben Sie den folgenden Befehl in die Azure CLI ein:

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

Beispiel

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

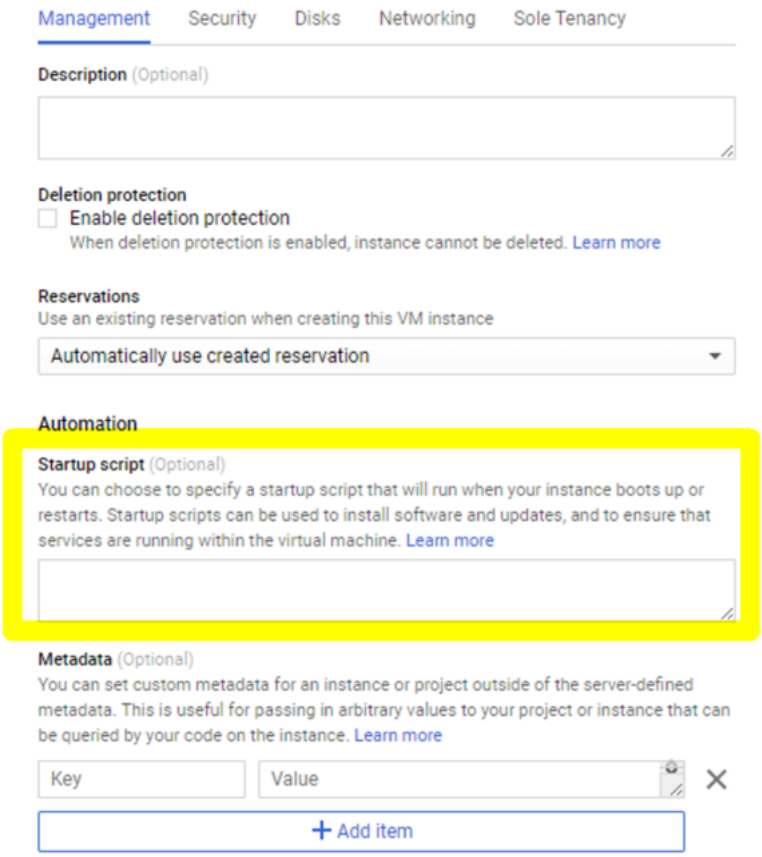
Sie können Ihre benutzerdefinierten Daten oder Preboot-Konfiguration als Datei an den Parameter “—custom-data”übergeben. In diesem Beispiel lautet der Dateiname **MyCloudInitScript.txt**.

Weitere Informationen finden Sie in der Azure CLI-Dokumentation.

Stellen Sie Preboot-Benutzerdaten mit der GCP-Konsole bereit

Wenn Sie eine NetScaler VPX-Instanz mit der GCP-Konsole bereitstellen, füllen Sie die Eigenschaften der Instanz aus. Erweitern Sie **Management, Sicherheit, Datenträger, Netzwerke, Einzelmandanten**. Navigieren Sie zur Registerkarte **Verwaltung**. Geben Sie im Abschnitt **Automatisierung** die Konfiguration der Preboot-Benutzerdaten im Feld **Startskript** ein.

Ausführliche Informationen zum Erstellen der VPX-Instanz mit GCP finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.



Stellen Sie Preboot-Benutzerdaten mit der gcloud CLI bereit

Geben Sie den folgenden Befehl in die GCP CLI ein:

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

metadata-from-file - Liest den Wert oder die Benutzerdaten aus einer Datei, die im .

Weitere Informationen finden Sie in der gcloud CLI-Dokumentation

Preboot-Benutzerdatenformat

Die Preboot-Benutzerdaten müssen der Cloud-Instanz im XML-Format zur Verfügung gestellt werden. Die NetScaler Preboot-Benutzerdaten, die Sie während des Bootens über die Cloud-Infrastruktur bereitstellen, können die folgenden vier Abschnitte umfassen:

- NetScaler-Konfiguration wird mit dem <NS-CONFIG> Tag dargestellt.
- Benutzerdefiniertes Bootstrapping des NetScaler, der mit dem <NS-BOOTSTRAP> Tag dargestellt wird.
- Speichern von Benutzerskripten in NetScaler, dargestellt mit dem <NS-SCRIPTS> Tag.
- Gepoolte Lizenzierungskonfiguration, die mit dem <NS-LICENSE-CONFIG> Tag dargestellt wird.

Sie können die vorangegangenen vier Abschnitte in beliebiger Reihenfolge innerhalb der ADC-Preboot-Konfiguration angeben. Stellen Sie sicher, dass Sie die in den folgenden Abschnitten gezeigten Formatierung genau befolgen, während Sie die Preboot-Benutzerdaten bereitstellen.

> **Hinweis:**
>
> Die gesamte Preboot-Benutzerdatenkonfiguration muss in das <NS-PRE-BOOT-CONFIG > Tag eingeschlossen sein, wie in den folgenden Beispielen gezeigt.

Beispiel 1:

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

Beispiel 2:

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

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen.

> **Hinweis:**
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs

> werden nicht auf die syntaktischen Fehler oder das Format überprüft.

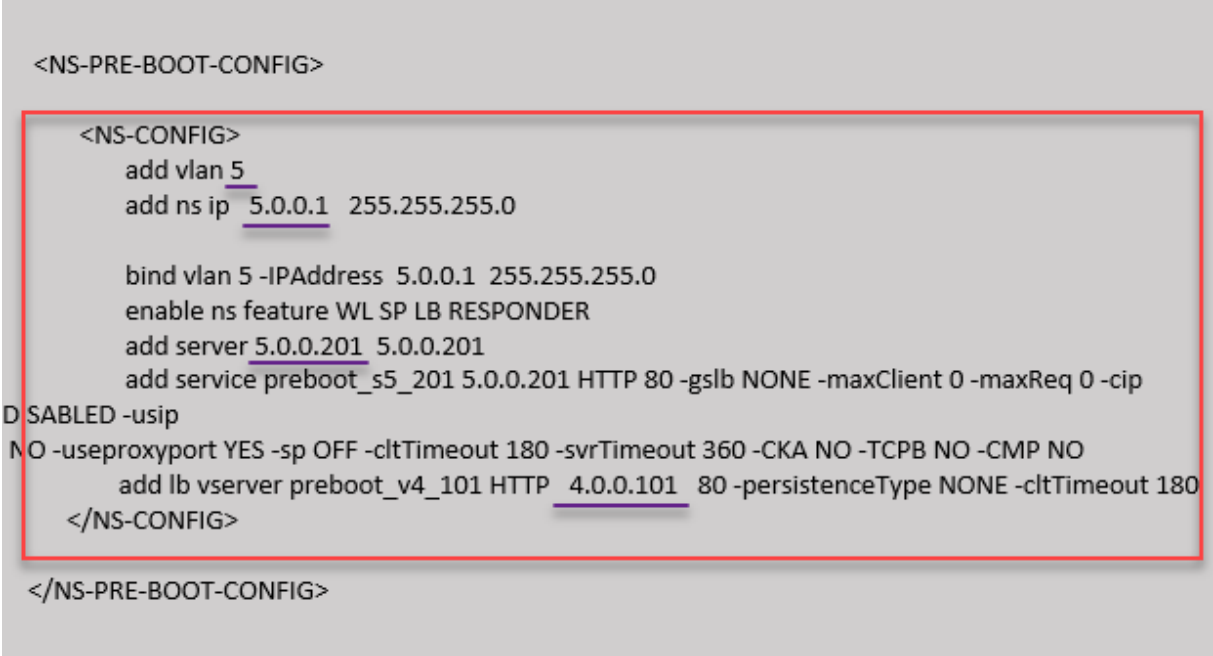
NetScaler-Konfigurationen

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen.

> **Hinweis:**
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs werden nicht auf die syntaktischen Fehler oder das Format überprüft.

Beispiel

Im folgenden Beispiel enthält der <NS-CONFIG> Abschnitt die Details der Konfigurationen. Ein VLAN der ID '5'ist konfiguriert und an das SNIP gebunden (5.0.0.1). Ein virtueller Lastenausgleichsserver (4.0.0.101) ist ebenfalls konfiguriert.



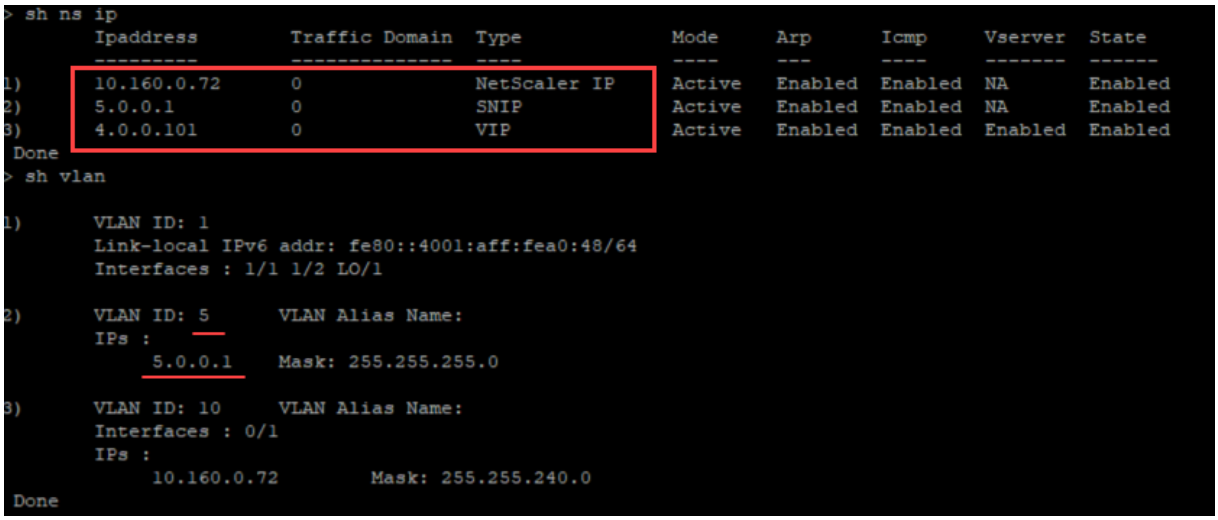
Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

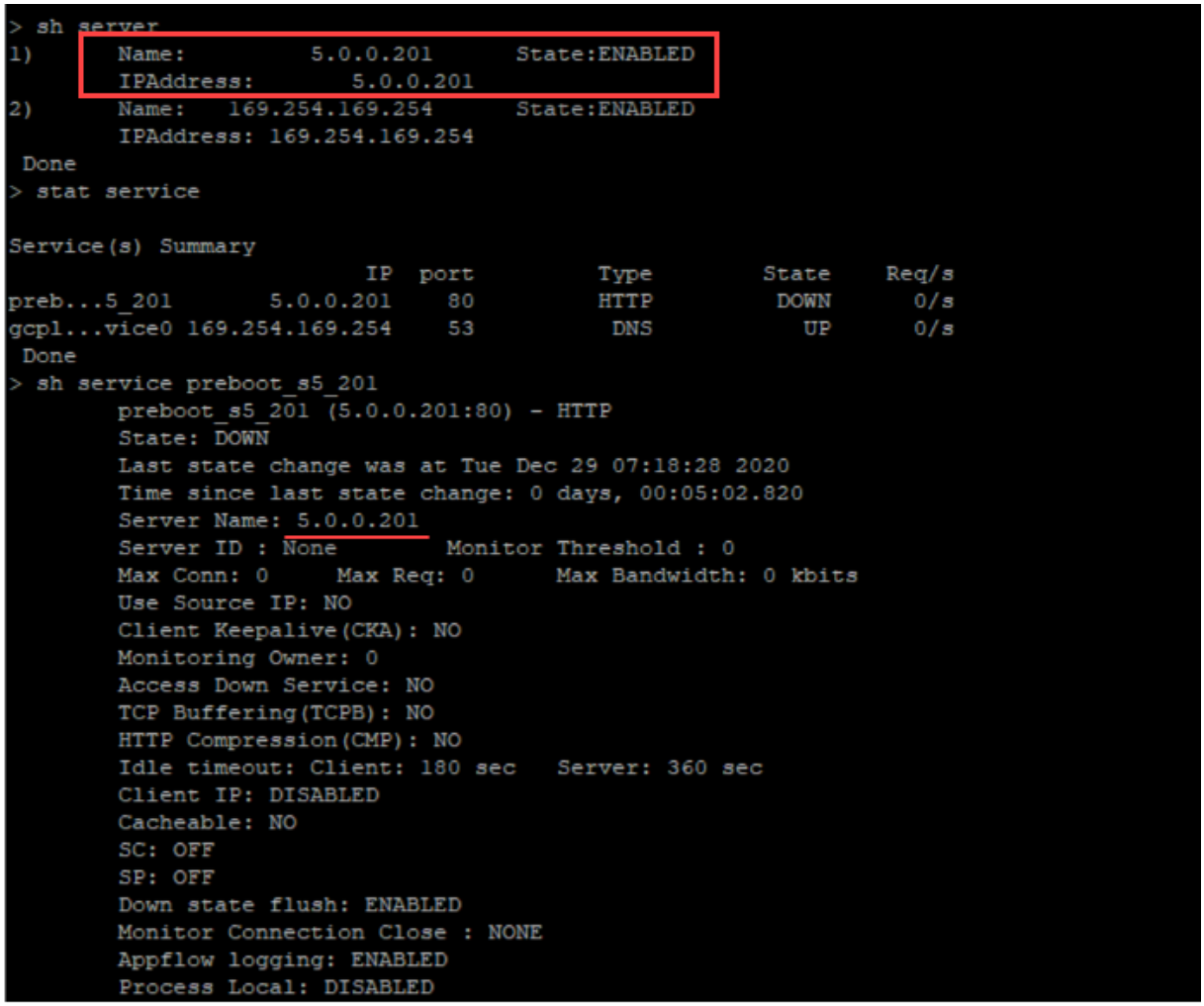
```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add vlan 5
        add ns ip 5.0.0.1 255.255.255.0
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
           maxClient 0 -maxReq 0 -cip DISABLED -usip
```



```
 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>
```

Die NetScaler VPX-Instanz enthält die im <NS-CONFIG> Abschnitt angewendete Konfiguration, wie in den folgenden Abbildungen gezeigt.





Benutzer-Skripts

Verwenden Sie das <NS-SCRIPTS> Tag, um jedes Skript bereitzustellen, das in der NetScaler VPX-Instanz gespeichert und ausgeführt werden muss.

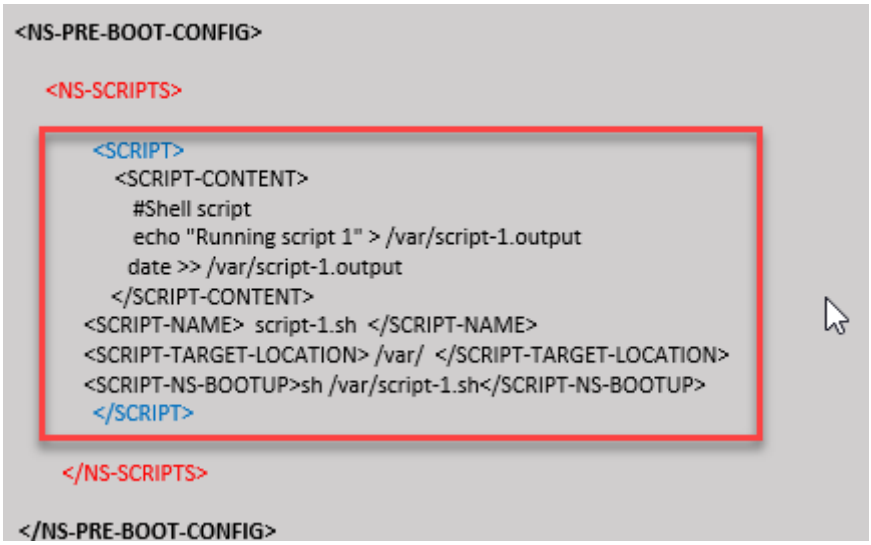
Sie können viele Skripts in das <NS-SCRIPTS> Tag aufnehmen. Jedes Skript muss in das <SCRIPT> Tag aufgenommen sein. Jeder <SCRIPT> Abschnitt entspricht einem Skript und enthält alle Details des Skripts unter Verwendung der folgenden Sub-Tags.

- **<SCRIPT-NAME>:** Gibt den Namen der Skriptdatei an, die gespeichert werden muss.
- **<SCRIPT-CONTENT>:** Gibt den Inhalt der Datei an, die gespeichert werden muss.
- **<SCRIPT-TARGET-LOCATION>:** Gibt den angegebenen Zielspeicherort an, an dem diese Datei gespeichert werden muss. Wenn der Zielspeicherort nicht angegeben wird, wird die Datei oder das Skript standardmäßig im Verzeichnis "/nsconfig"gespeichert.
- **<SCRIPT-NS-BOOTUP>:** Geben Sie die Befehle an, die Sie zum Ausführen des Skripts verwenden.

- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt verwenden, werden die in diesem Abschnitt bereitgestellten Befehle in "/nsconfig/nsafter.sh"gespeichert, und die Befehle werden ausgeführt, nachdem die Paket-Engine im Rahmen der Ausführung "nsafter.sh"hochgefahren ist.
- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt nicht verwenden, wird die Skriptdatei an dem von Ihnen angegebenen Zielspeicherort gespeichert.

Beispiel 1:

In diesem Beispiel enthält das <NS-SCRIPTS> Tag Details zu nur einem Skript: script-1.sh. Das "script-1.sh"-Skript wird im Verzeichnis "/var"gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl "sh /var/script-1.sh" ausgeführt.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

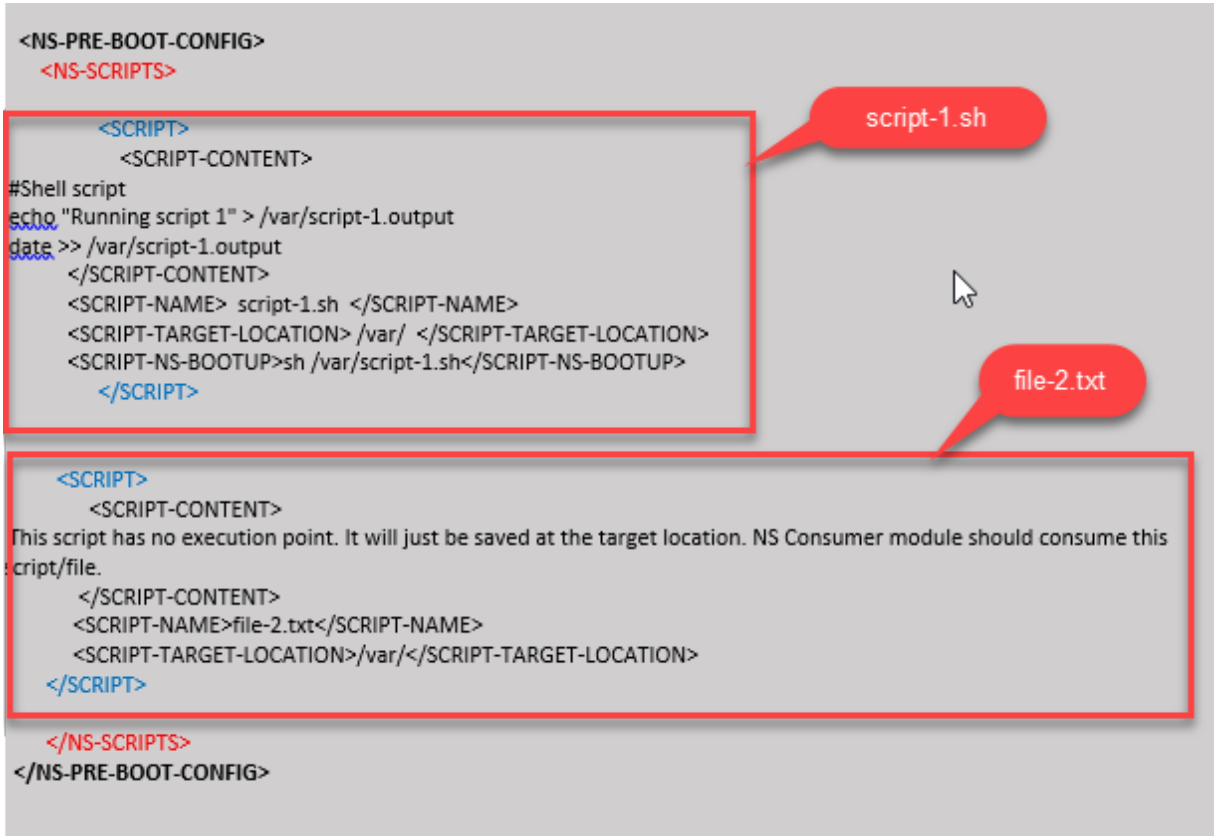
```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <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>
```


Im folgenden Snapshot können Sie überprüfen, ob das “script-1.sh”-Skript im Verzeichnis “/var/” gespeichert ist. Das “Script-1.sh”-Skript wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.

Beispiel 2:

Im folgenden Beispiel enthält das <NS-SCRIPTS> Tag Details zu zwei Skripten.

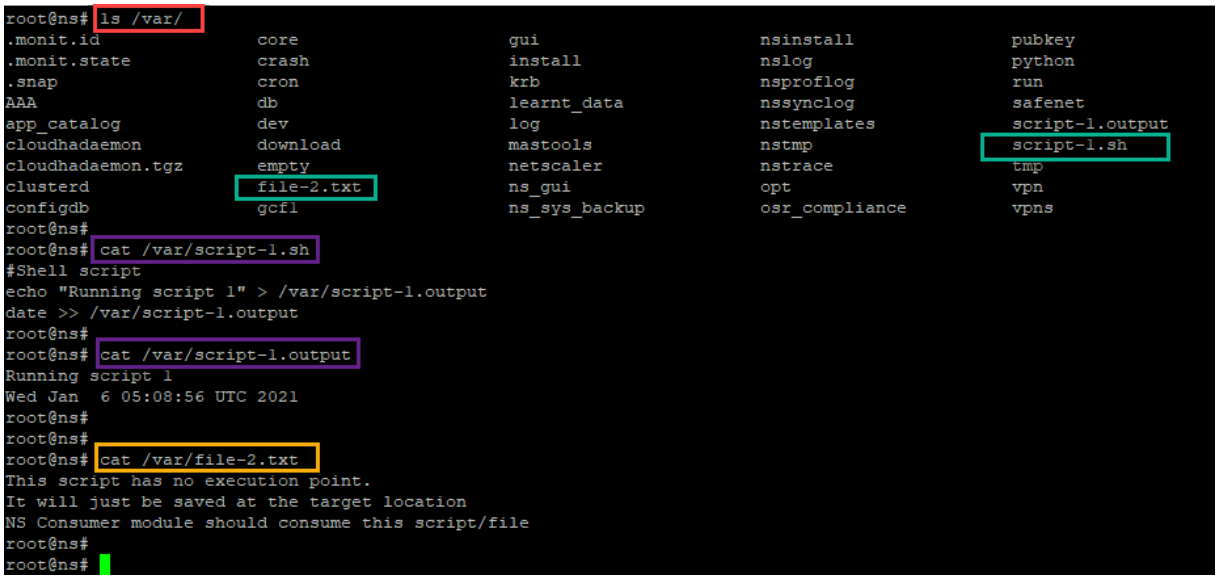
- Das erste Script wird als “script-1.sh”im Verzeichnis “/var”gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl “sh /var/script-1.sh”ausgeführt.
- Das zweite Script wird als “file-2.txt”im Verzeichnis “/var”gespeichert. Diese Datei wird mit dem angegebenen Inhalt gefüllt. Es wird jedoch nicht ausgeführt, da der Bootup-Ausführungsbefehl nicht bereitgestellt <SCRIPT-NS-BOOTUP> wird.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

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

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

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


Im folgenden Snapshot können Sie überprüfen, ob script-1.sh und file-2.txt im Verzeichnis "/var/" erstellt wurden. Die Script-1.sh wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.



Lizenzierung

Verwenden Sie das <NS-LICENSE-CONFIG> Tag, um die gepoolte NetScaler-Lizenzierung anzuwenden, während Sie die VPX-Instanz hochfahren. Verwenden Sie das <LICENSE-COMMANDS> Tag im <NS-LICENSE-CONFIG> Abschnitt, um die gepoolten Lizenzbefehle bereitzustellen. Diese Befehle müssen syntaktisch gültig sein.

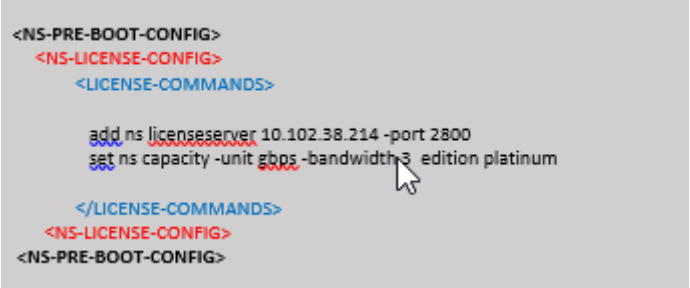
Sie können die gepoolten Lizenzierungsdetails wie Lizenztyp, Kapazität und Lizenzserver im <LICENSE-COMMANDS> Abschnitt mit den standardmäßigen gepoolten Lizenzbefehlen angeben. Weitere Informationen finden Sie unter Konfigurieren der Lizenzierung der gepoolten Kapazität von NetScaler.

Nach dem <NS-LICENSE-CONFIG>Anwenden des wird der VPX beim Booten mit der angeforderten Edition geliefert, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken.

- Wenn das Auschecken der Lizenz erfolgreich ist, wird die konfigurierte Bandbreite auf VPX angewendet.
- Wenn das Auschecken der Lizenz fehlschlägt, wird die Lizenz nicht innerhalb von 10 bis 12 Minuten vom Lizenzserver abgerufen. Infolgedessen wird das System neu gestartet und wechselt in einen nicht lizenzierten Zustand.

Beispiel

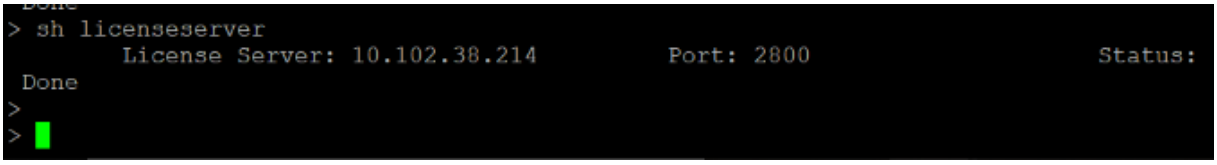
Im folgenden Beispiel wird der VPX nach dem <NS-LICENSE-CONFIG>Anwenden des beim Booten die Premium Edition bereitgestellt, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken (10.102.38.214).



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<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>
```

Wie in der folgenden Abbildung gezeigt, können Sie den Befehl “show license server”ausführen und überprüfen, ob der Lizenzserver (10.102.38.214) zum VPX hinzugefügt wurde.



Bootstrapping

Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können die <NEW-BOOTSTRAP-SEQUENCE> Tags <SKIP-DEFAULT-BOOTSTRAP> und innerhalb des <NS-BOOTSTRAP> Abschnitts verwenden. In diesem Abschnitt wird NetScaler-Appliance darüber informiert, ob der Standard-Bootstrap vermieden werden soll oder nicht. Wenn das Standard-Bootstrapping vermieden wird, bietet Ihnen dieser Abschnitt die Möglichkeit, eine neue Bootstrapping-Sequenz bereitzustellen.

Standardmäßige Bootstrap-Konfiguration

Die Standard-Bootstrap-Konfiguration in der NetScaler-Appliance folgt diesen Schnittstellenzuweisungen:

- **Eth0** - Verwaltungsschnittstelle mit einer bestimmten NSIP-Adresse.
- **Eth1** - Clientorientierte Schnittstelle mit einer bestimmten VIP-Adresse.
- **Eth2** - Server-Schnittstelle mit einer bestimmten SNIP-Adresse.

Anpassen der Bootstrap-Konfiguration

Sie können die standardmäßige Bootstrap-Sequenz überspringen und eine neue Bootstrap-Sequenz für die NetScaler VPX-Instanz bereitstellen. Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können beispielsweise das Standard-Bootstrapping ändern, bei dem die Verwaltungsschnittstelle (NSIP), die clientseitige Schnittstelle (VIP) und die Serverschnittstelle (SNIP) immer in einer bestimmten Reihenfolge bereitgestellt werden.

Die folgende Tabelle zeigt das Bootstrapping-Verhalten mit den verschiedenen zulässigen Werten <SKIP-DEFAULT-BOOTSTRAP> und <NEW-BOOTSTRAP-SEQUENCE> Tags an.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Bootstrap-Verhalten
JA	JA	Das standardmäßige Bootstrapping-Verhalten wird übersprungen, und eine neue benutzerdefinierte Bootstrap-Sequenz im <NS-BOOTSTRAP> Abschnitt wird ausgeführt.
JA	NEIN	Das standardmäßige Bootstrapping-Verhalten wird übersprungen. Die im <NS-CONFIG> Abschnitt bereitgestellten Bootstrap-Befehle werden ausgeführt.

Sie können die Bootstrap-Konfiguration mit den folgenden drei Methoden anpassen:

- Geben Sie nur die Schnittstellendetails
- Geben Sie die Schnittstellendetails zusammen mit IP-Adressen und Subnetzmaske an
- Geben Sie Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt

Methode 1: Benutzerdefinierter Bootstrap durch Angabe nur der Schnittstellendetails

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen an, nicht jedoch deren IP-Adressen und Subnetzmasken. Die IP-Adressen und Subnetzmasken werden durch Abfragen der Cloud-Infrastruktur ausgefüllt.

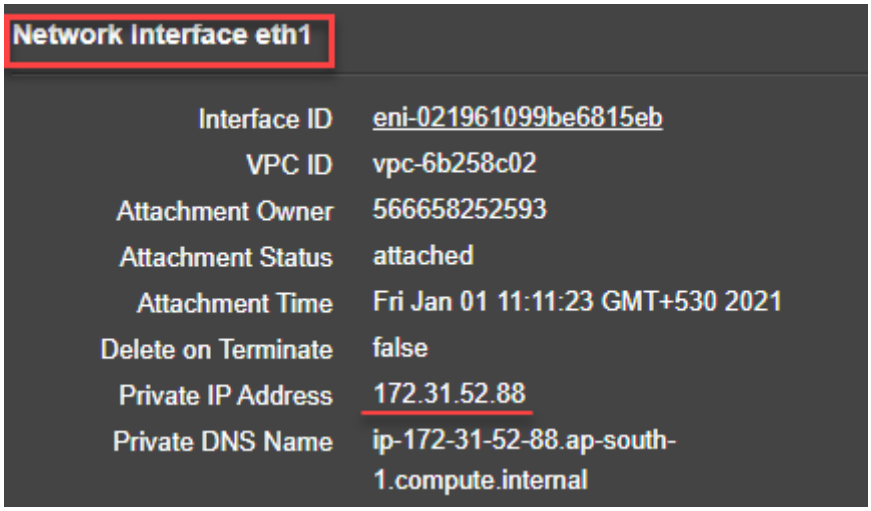
Benutzerdefiniertes Bootstrap-Beispiel für AWS

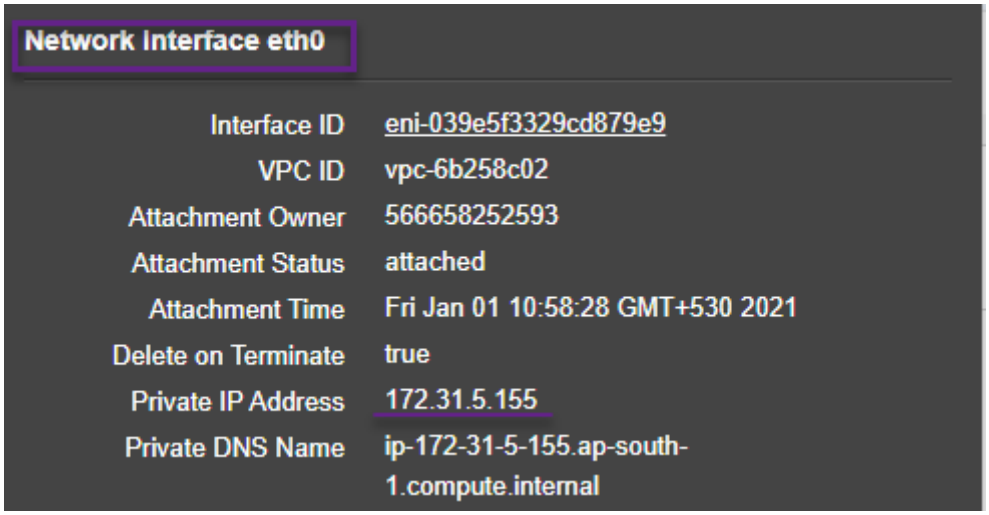
Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.

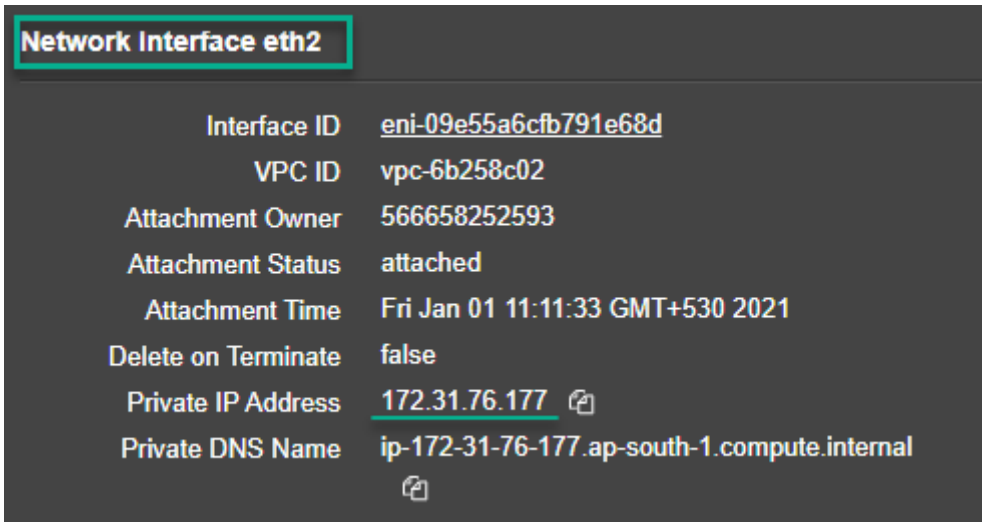
```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <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>
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

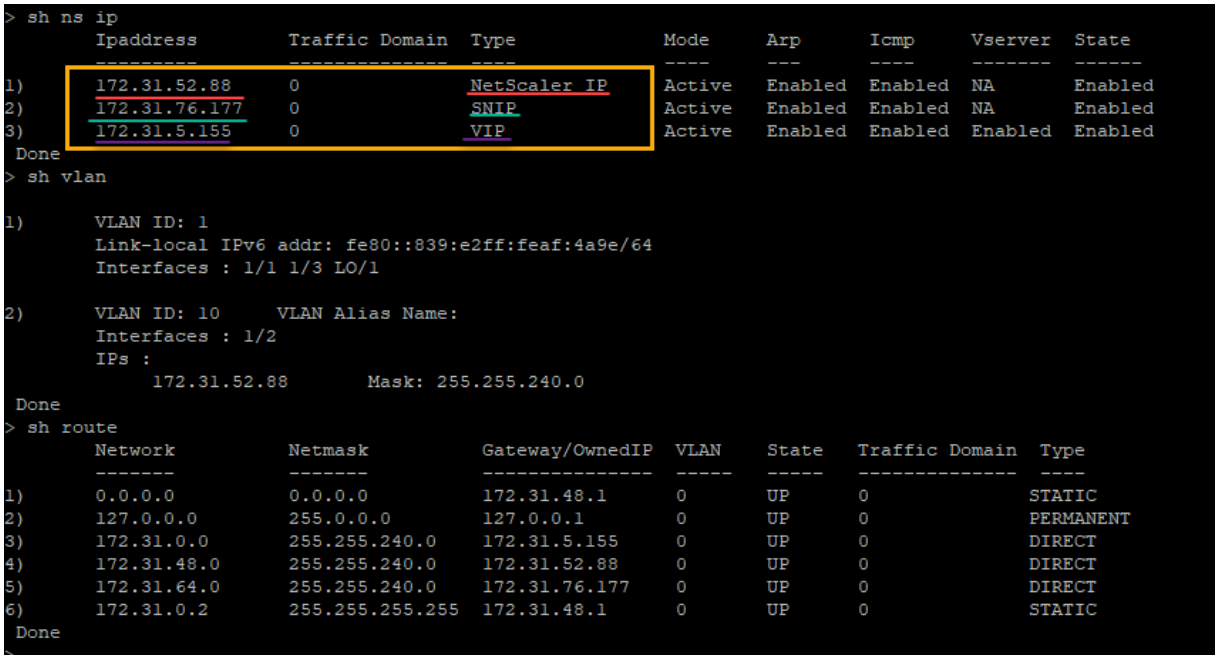
1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.



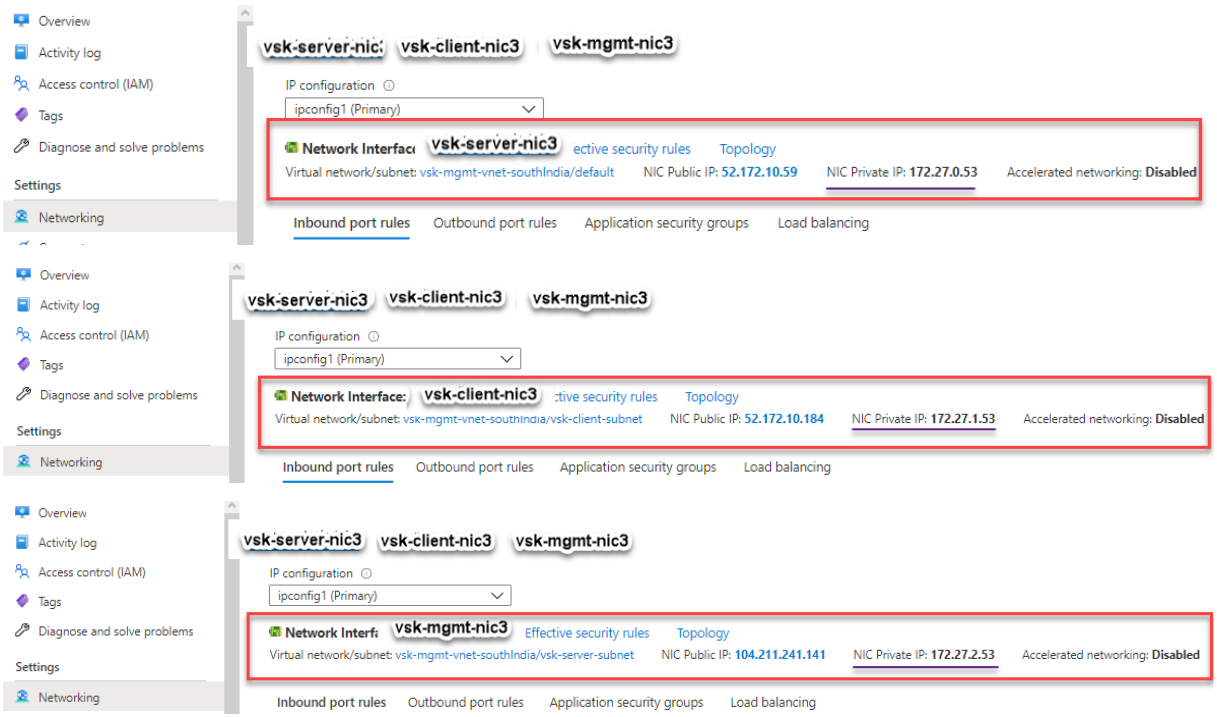
```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  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
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.

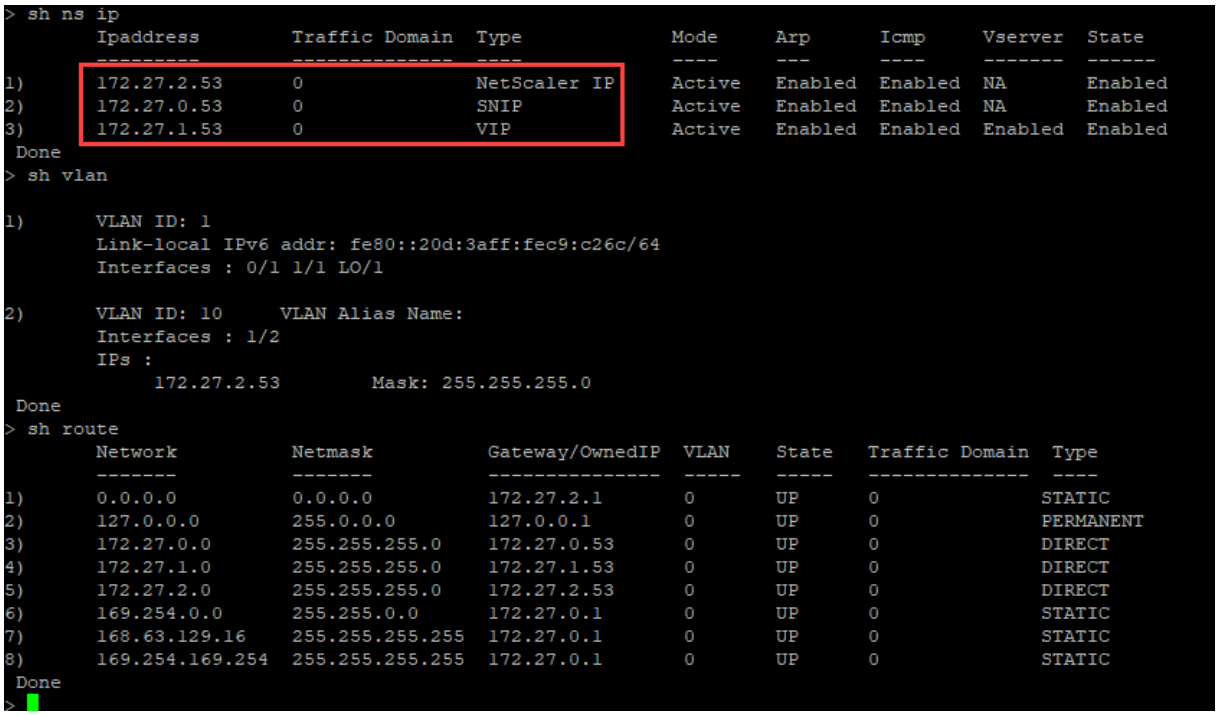

```
<NS-PRE-BOOT-CONFIG>

    <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>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.



Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS

−BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen”ausführen, um die Subnetzmaske zu überprüfen.



Benutzerdefinierte Bootstrap-Beispiele für GCP

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS−BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.


```
<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>
```

Nachdem die VM-Instanz im GCP-Portal erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

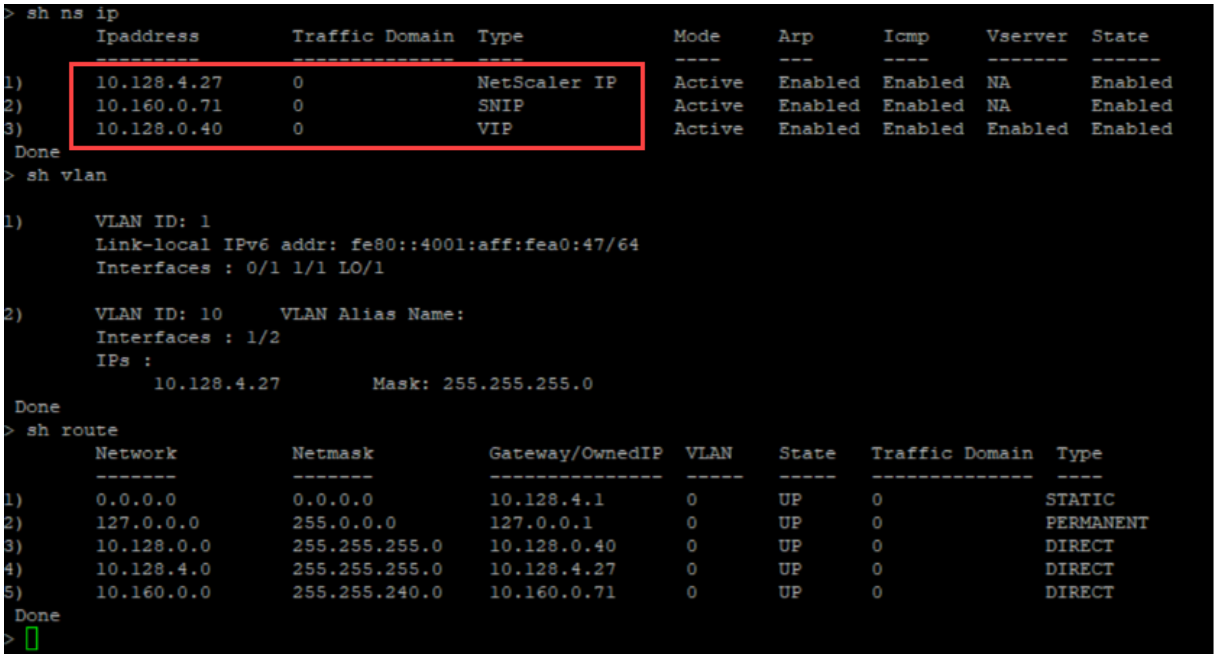
1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details wie folgt:

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

Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.



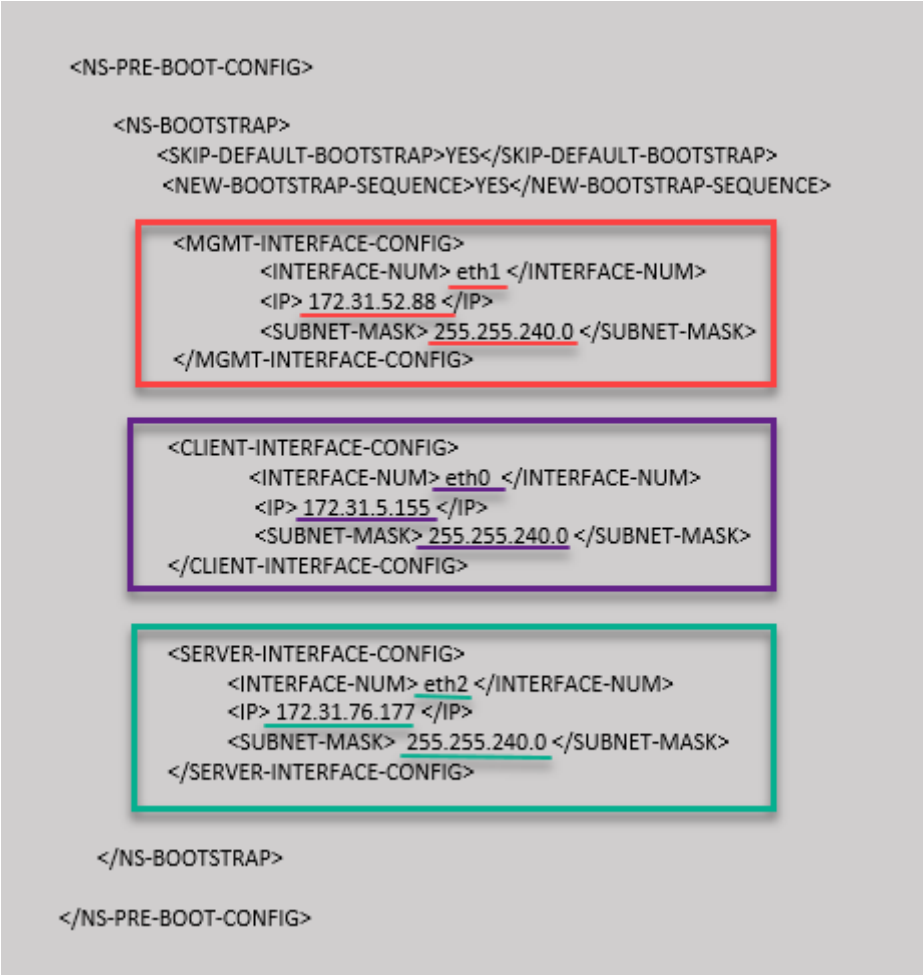
Methode 2: Benutzerdefiniertes Bootstrap durch Angabe der Schnittstellen, IP-Adressen und Subnetzmasken

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen zusammen mit ihren IP-Adressen und der Subnetzmaske an.

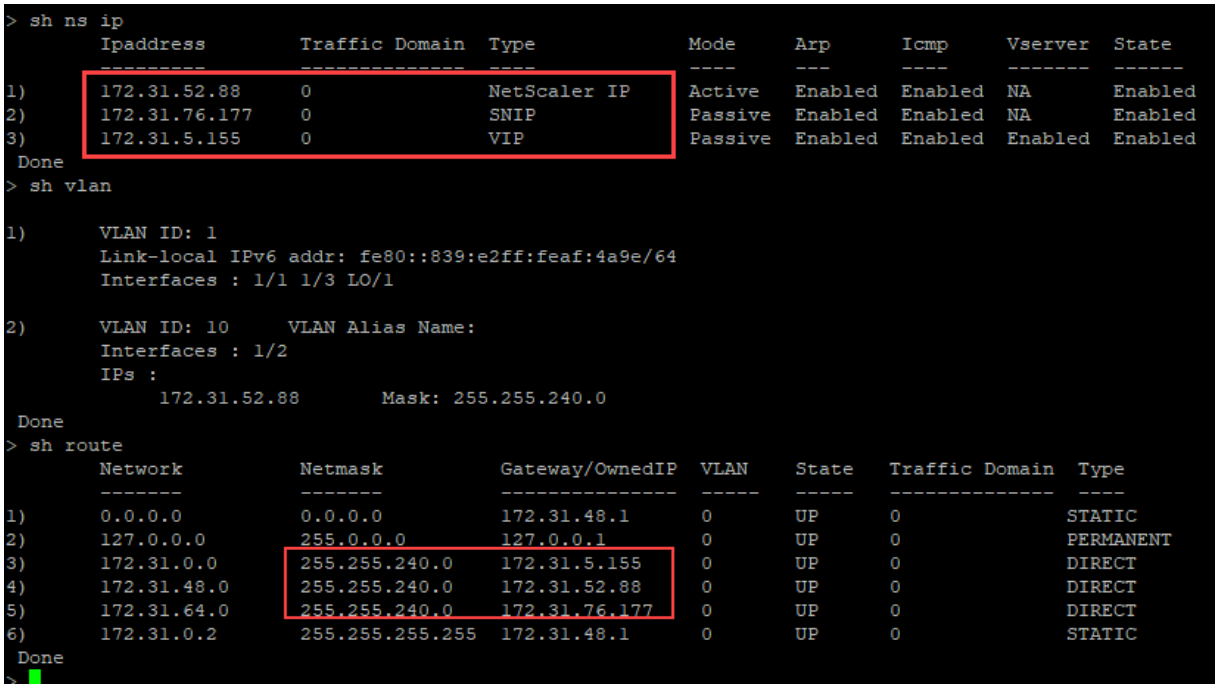
Benutzerdefinierte Bootstrap-Beispiele für AWS

Im folgenden Beispiel überspringen Sie den Standard-Bootstrap und führen eine neue Bootstrap-Sequenz für die NetScaler-Appliance aus. Für die neue Bootstrap-Sequenz geben Sie folgende Details an:

- **Verwaltungsschnittstelle:** Interface - Eth1, NSIP - 172.31.52.88 und Subnetzmaske - 255.255.240.0
- **Clientorientierte Schnittstelle:** Schnittstelle - Eth0, VIP - 172.31.5.155 und Subnetzmaske - 255.255.240.0.
- **Server-zugewandte Schnittstelle:** Schnittstelle - Eth2, SNIP - 172.31.76.177 und Subnetzmaske - 255.255.240.0.



Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im `<NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen"ausführen, um die Subnetzmaske zu überprüfen.



```
> 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
>
```

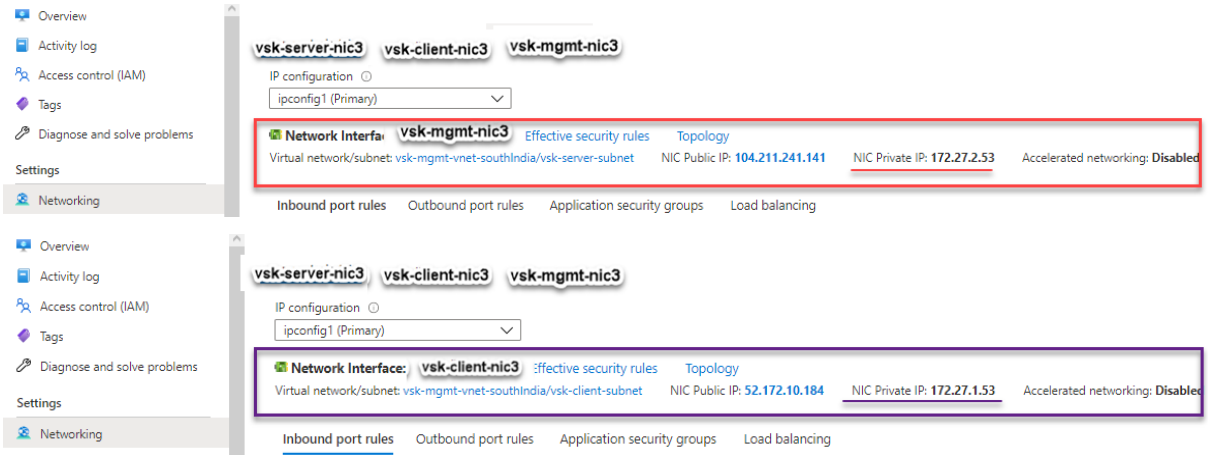
Benutzerdefiniertes Bootstrap-Beispiel für Azure

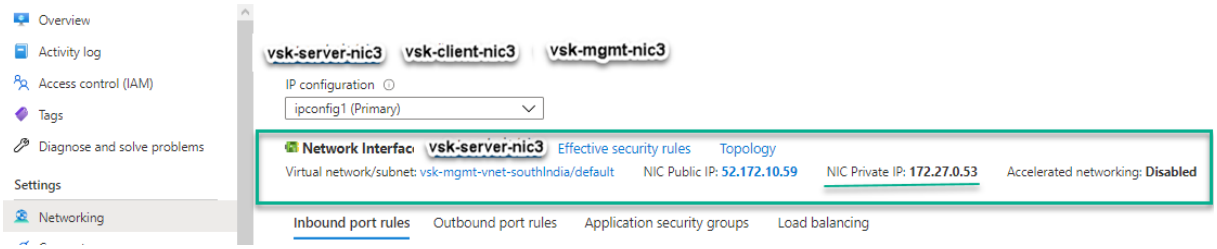
Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (172.27.2.53) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (172.27.1.53) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (172.27.0.53) und Subnetzmaske (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>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.





Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im &`lt;NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen"ausführen, um die Subnetzmaske zu überprüfen.

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

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

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

Benutzerdefiniertes Bootstrap-Beispiel für GCP

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (10.128.4.31) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (10.128.0.43) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (10.160.0.75) und Subnetzmaske (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>
```

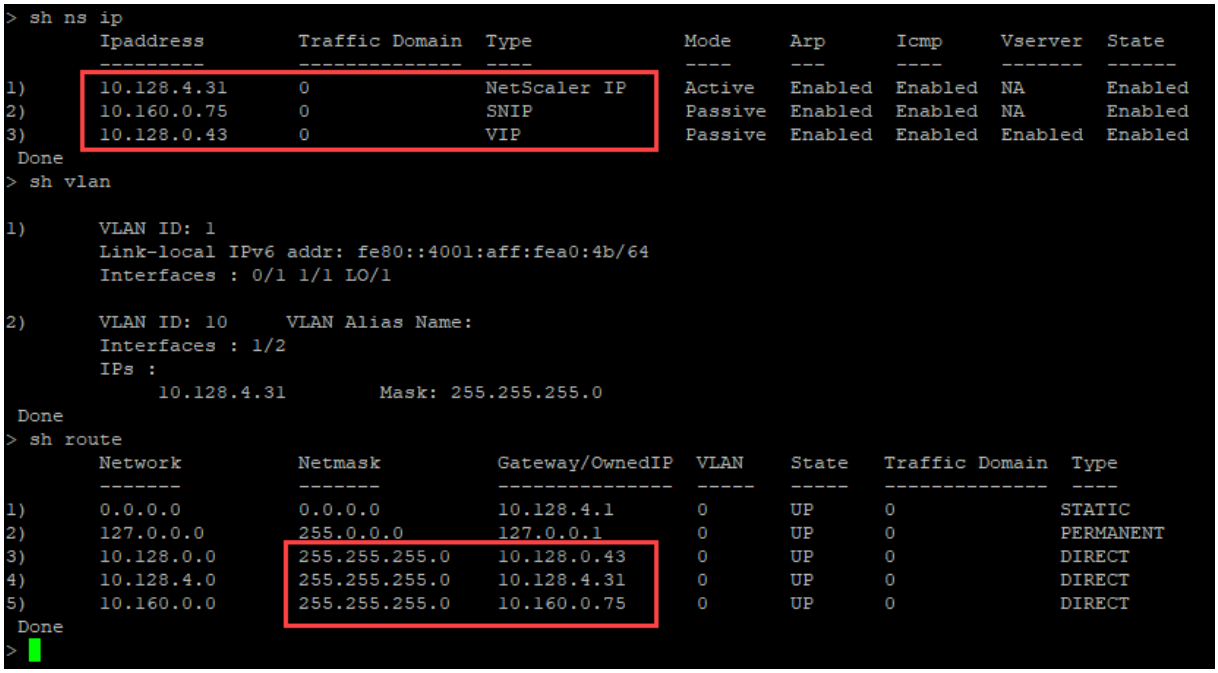
Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie folgt.

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

Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im &`lt;NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen”ausführen, um die Subnetzmaske zu überprüfen.



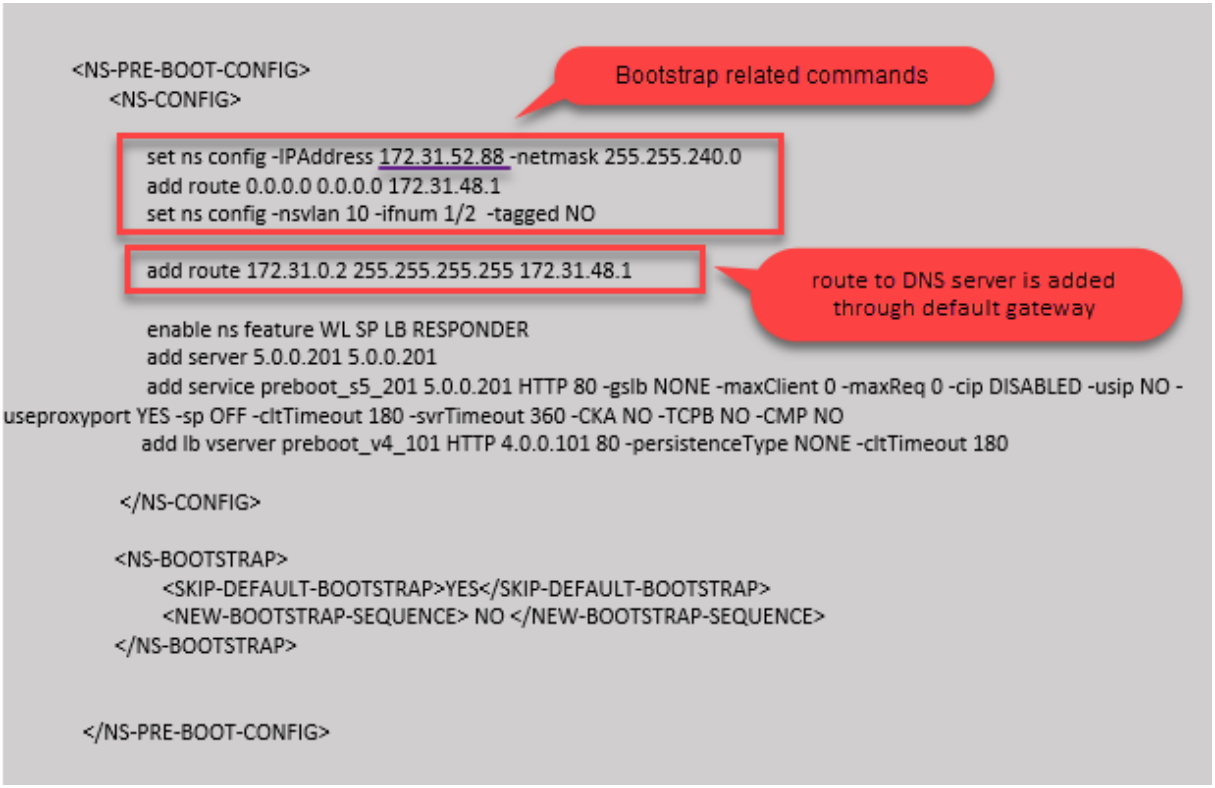
Methode 3: Benutzerdefiniertes Bootstrap durch Bereitstellung von Bootstrap-bezogenen Befehlen im <NS-CONFIG> Abschnitt

Sie können die Bootstrap-bezogenen Befehle im <NS-CONFIG> Abschnitt angeben. In <NS-BOOTSTRAP> diesem Abschnitt müssen Sie das <NEW-BOOTSTRAP-SEQUENCE> als "Nein"angeben, um die Bootstrapping-Befehle im <NS-CONFIG> Abschnitt auszuführen. Sie müssen auch die Befehle angeben, um NSIP, Standardroute und NSVLAN zuzuweisen. Geben Sie außerdem die Befehle ein, die für die von Ihnen verwendete Cloud relevant sind.

Stellen Sie vor der Bereitstellung eines benutzerdefinierten Bootstrap sicher, dass Ihre Cloud-Infrastruktur eine bestimmte Schnittstellenkonfiguration unterstützt.

Benutzerdefiniertes Bootstrap-Beispiel für AWS

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden. Sie müssen auch die Befehle zum Erstellen von NSIP, zum Hinzufügen einer Standardroute und zum Hinzufügen von NSVLAN angeben.

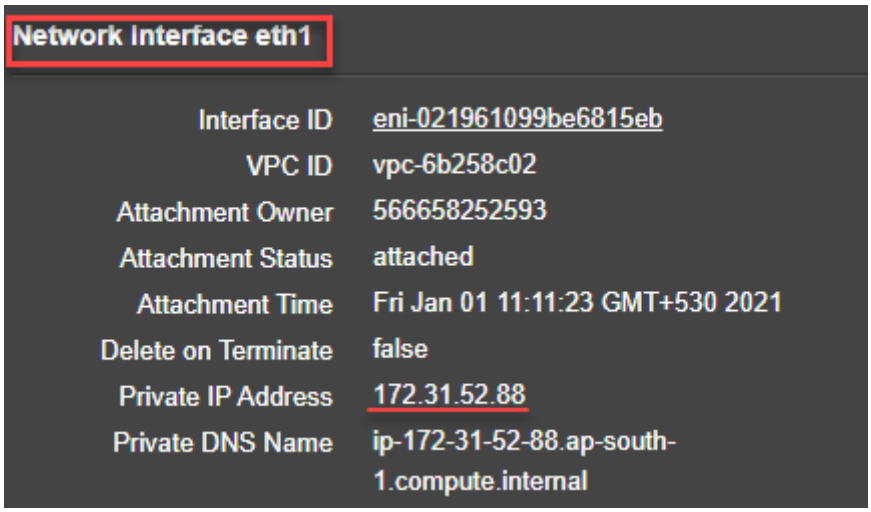


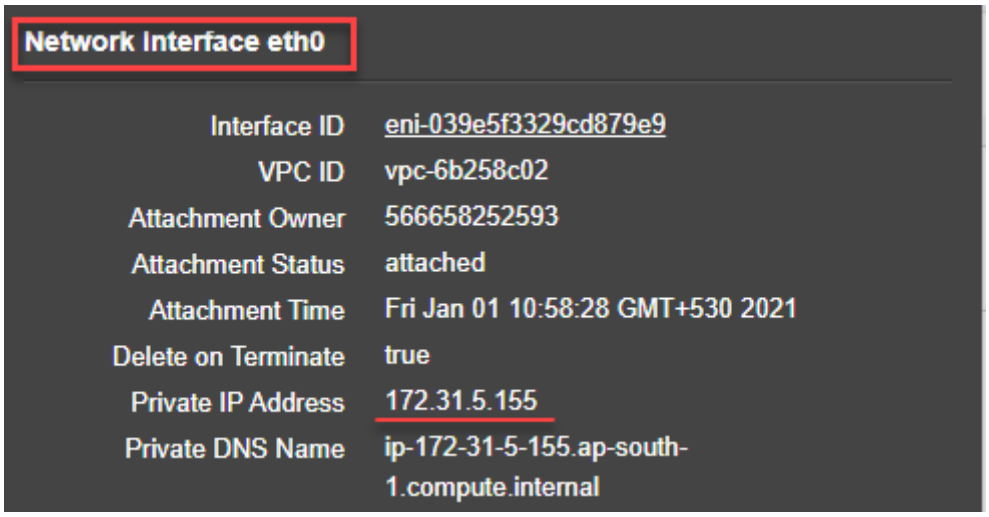
Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

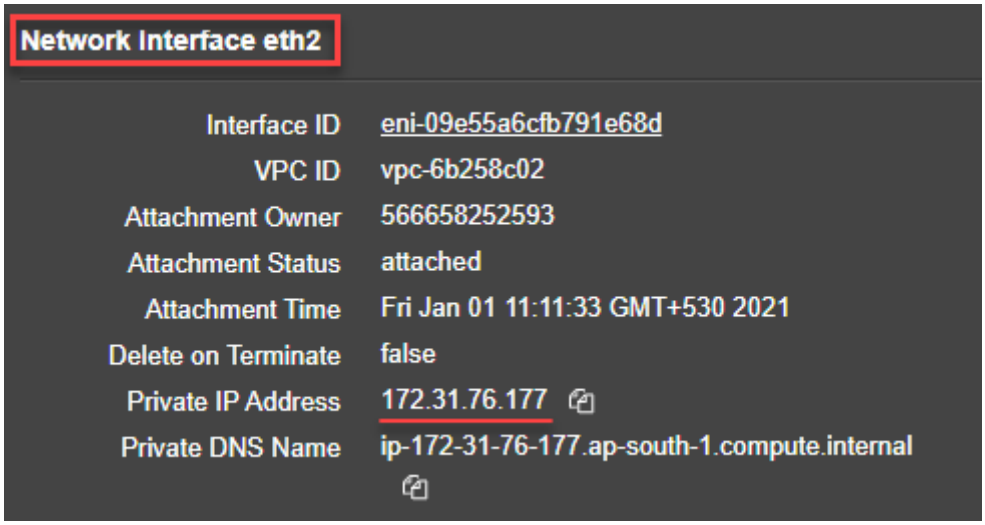
```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        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>
```


Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

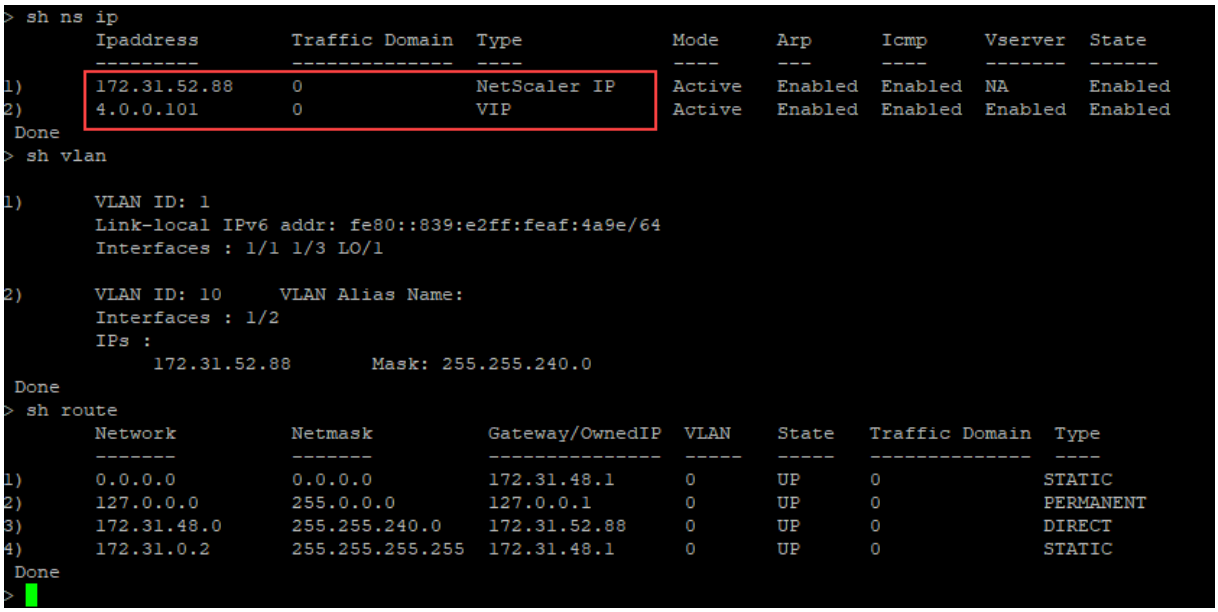
1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.

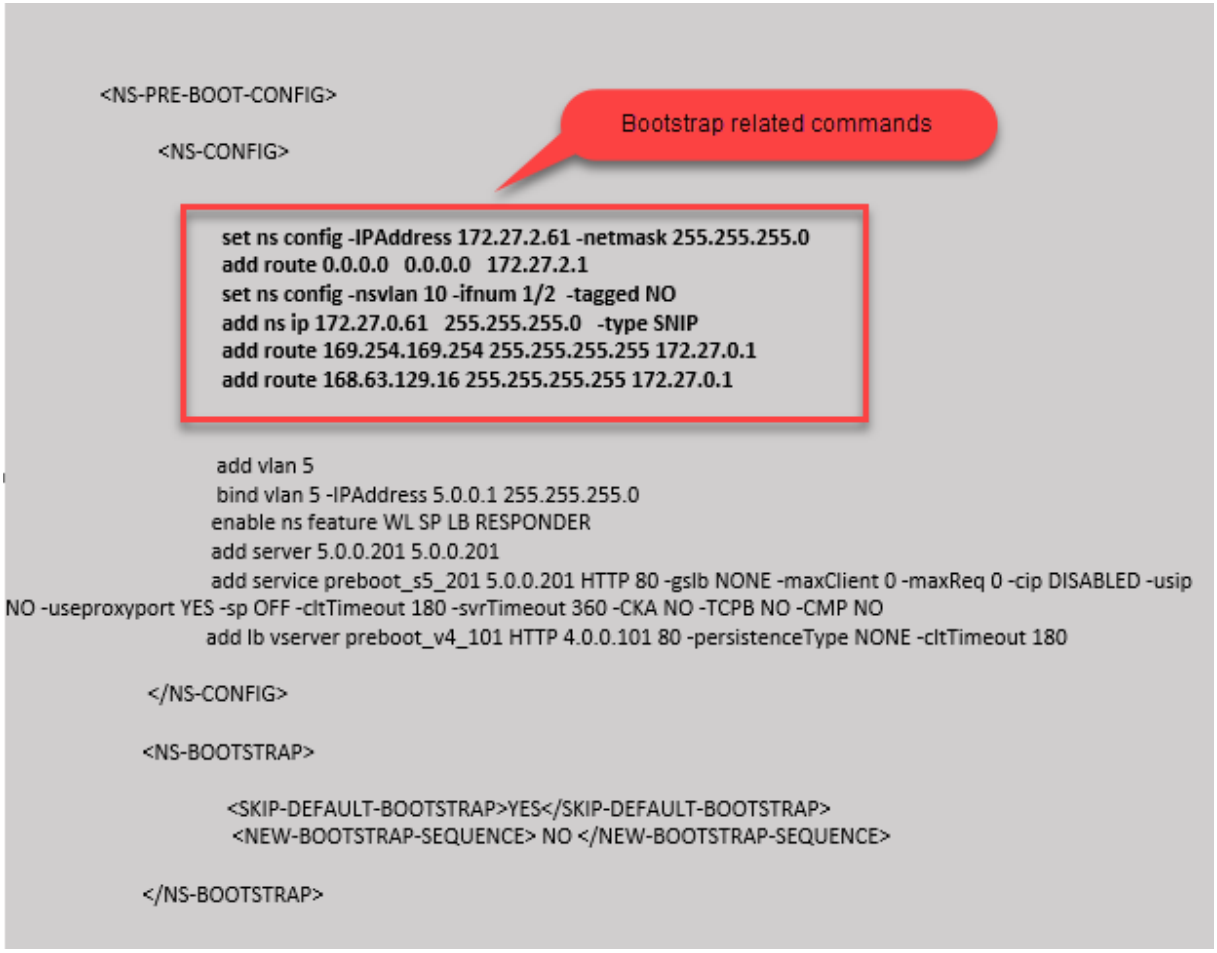


Benutzerdefiniertes Bootstrap-Beispiel für Azure

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden.

> **Hinweis:**
>
> Für Azure Cloud sind Instance Metadata Server (IMDS) und DNS-Server nur über die primäre

> Schnittstelle (Eth0) zugänglich. Wenn die Eth0-Schnittstelle nicht als Verwaltungsschnittstelle (NSIP) verwendet wird, muss die Eth0-Schnittstelle daher zumindest als SNIP für IMDS- oder DNS-Zugriff auf die Arbeit konfiguriert werden. Die Route zum IMDS-Endpunkt (169.254.169.254) und zum DNS-Endpunkt (168.63.129.16) über das Gateway von Eth0 muss ebenfalls hinzugefügt werden.

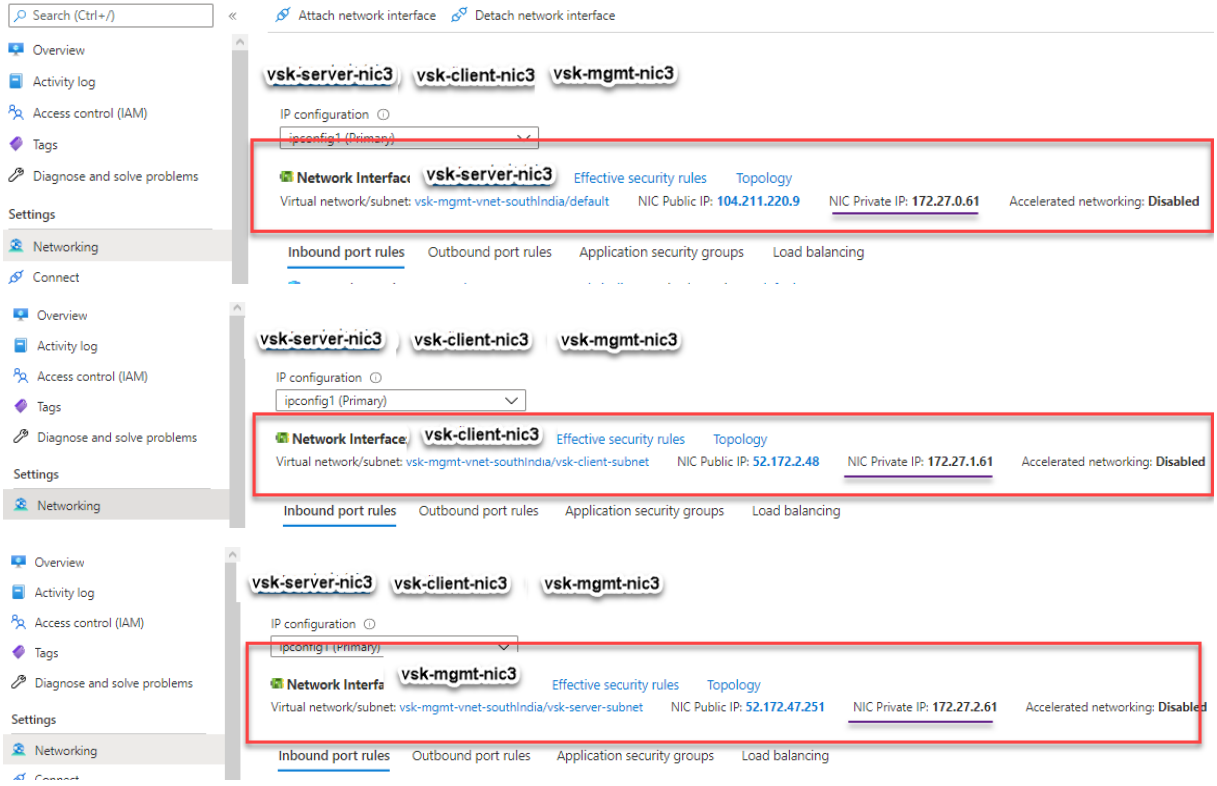



```
<NS-PRE-BOOT-CONFIG>

   <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
```

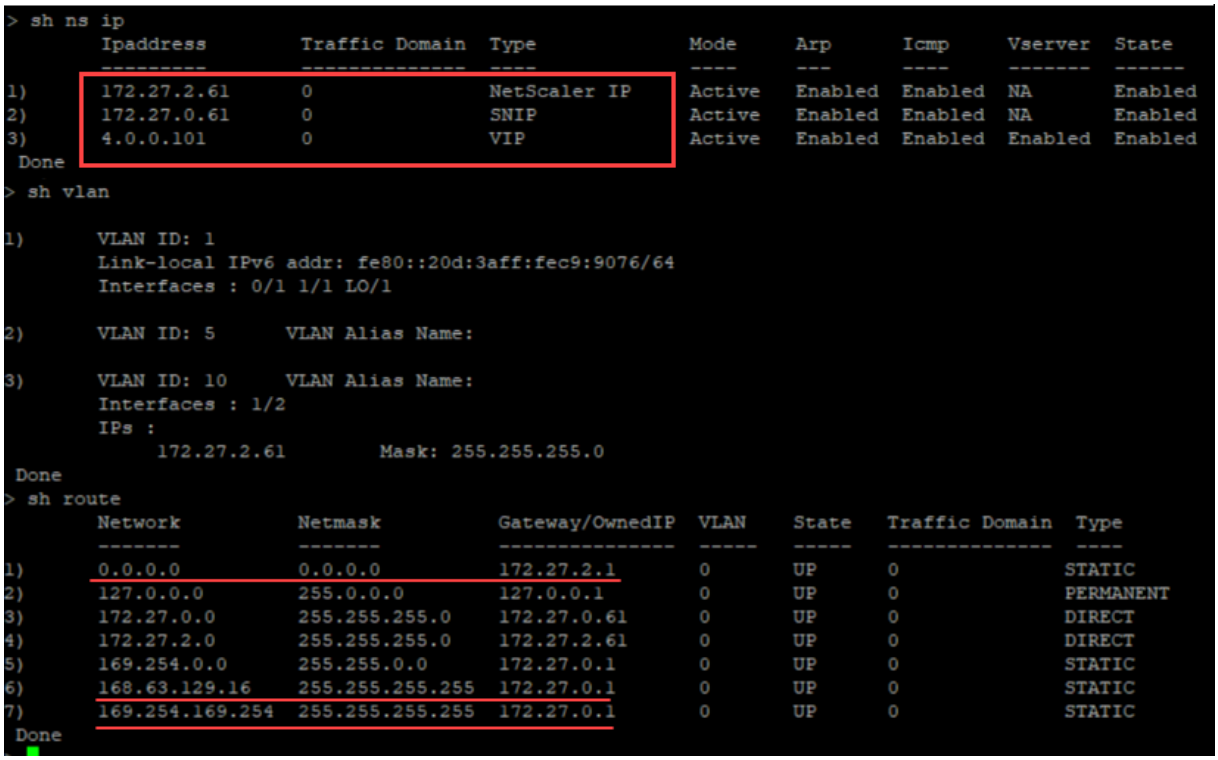


```
16          add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
               maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
                YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
                NO -CMP NO
17          add lb vserver preboot_v4_101 HTTP 4.0.0.101 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>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.



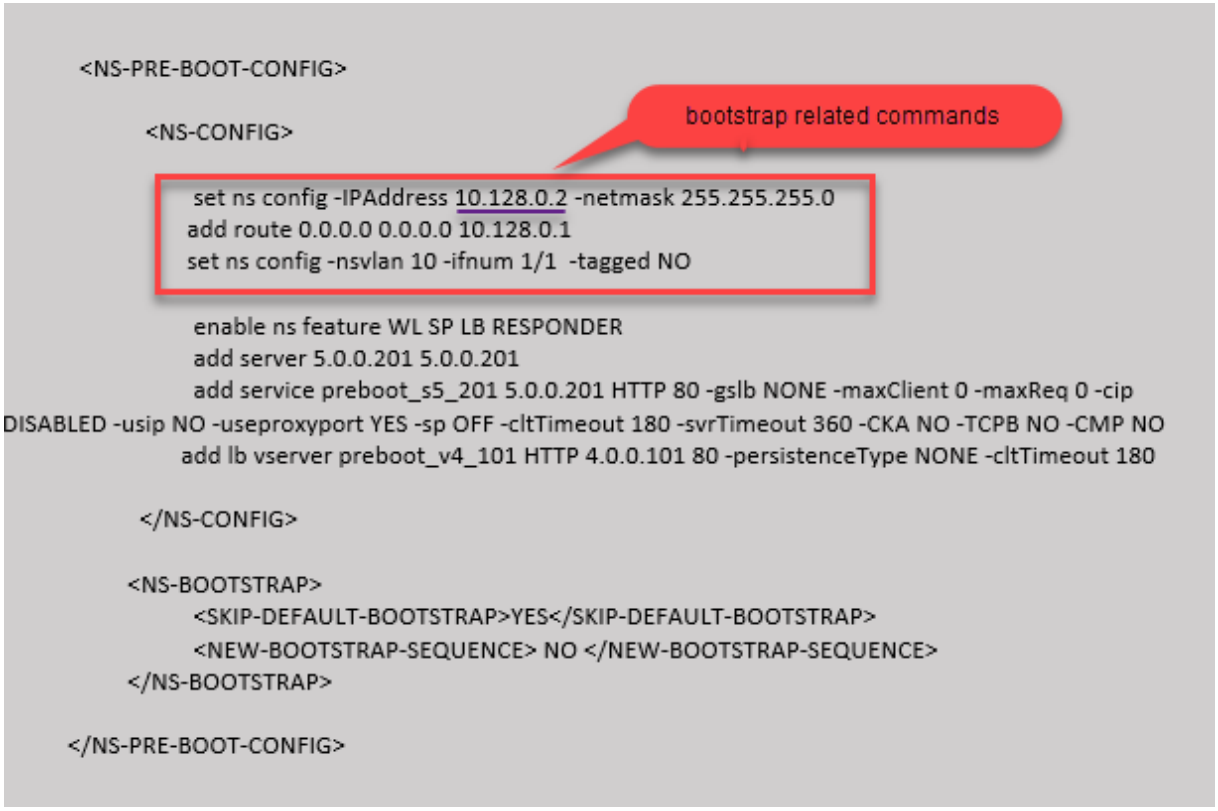
Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im &`lt;NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen"ausführen, um die Subnetzmaske zu überprüfen.



```
> 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
```

Benutzerdefiniertes Bootstrap-Beispiel für GCP

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen angewendet werden.

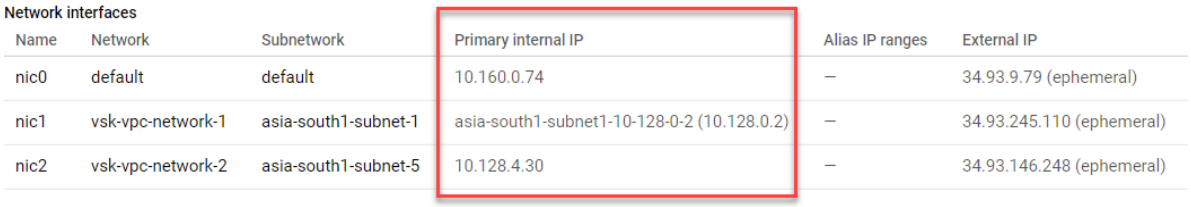


Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<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>
```


Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

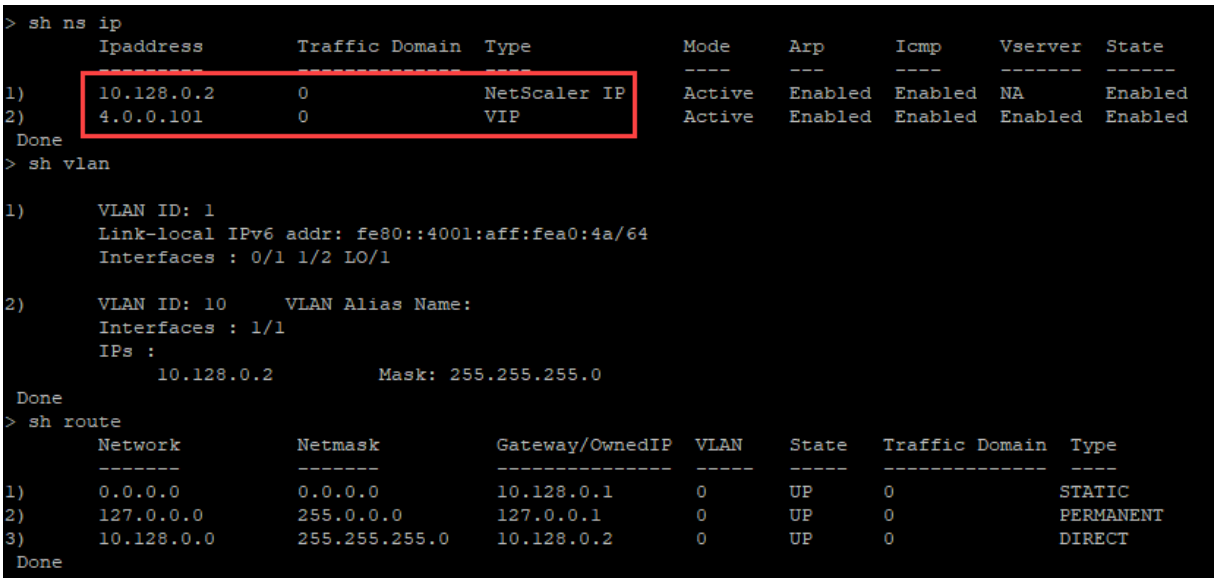
1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie in der Abbildung gezeigt.



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)

Sie können den `show nsip` Befehl in **ADC CLI**ausführen und sicherstellen, dass die im vorherigen <NS-CONFIG> Abschnitt bereitgestellten Konfigurationen beim ersten Start der ADC-Appliance angewendet werden.



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

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

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

Auswirkungen des Anhängen und Trennen von NICs in AWS und Azure

AWS und Azure bieten die Möglichkeit, eine Netzwerkschnittstelle an eine Instanz anzuschließen und eine Netzwerkschnittstelle von einer Instanz zu trennen. Das Anhängen oder Trennen von Schnittstellen kann die Positionen der Schnittstelle verändern. Daher empfiehlt Citrix, Schnittstellen nicht von der NetScaler VPX-Instanz zu trennen. Wenn Sie eine Schnittstelle trennen oder anhängen, wenn benutzerdefiniertes Bootstrapping konfiguriert ist, weist die NetScaler VPX-Instanz die primäre IP der neu verfügbaren Schnittstelle in der Position der Verwaltungsschnittstelle als NSIP zu. Wenn

nach der von Ihnen getrennten Schnittstelle keine weiteren Schnittstellen verfügbar sind, wird die erste Schnittstelle zur Verwaltungsschnittstelle für die NetScaler VPX-Instanz gemacht.

Zum Beispiel wird eine NetScaler VPX-Instanz mit 3 Schnittstellen aufgebracht: Eth0 (SNIP), Eth1 (NSIP) und Eth2 (VIP). Wenn Sie die Eth1-Schnittstelle von der Instanz trennen, bei der es sich um eine Verwaltungsschnittstelle handelt, konfiguriert ADC die nächste verfügbare Schnittstelle (Eth2) als Verwaltungsschnittstelle. Dadurch wird auf die NetScaler VPX-Instanz weiterhin über die primäre IP der Eth2-Schnittstelle zugegriffen. Wenn Eth2 ebenfalls nicht verfügbar ist, wird die verbleibende Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht. Daher besteht der Zugriff auf die NetScaler VPX-Instanz weiterhin.

Betrachten wir eine andere Zuweisung von Schnittstellen wie folgt: Eth0 (SNIP), Eth1 (VIP) und Eth2 (NSIP). Wenn Sie Eth2 (NSIP) trennen, da nach Eth2 keine neue Schnittstelle verfügbar ist, wird die erste Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht.

Verbessern der SSL-TPS-Leistung auf Public-Cloud-Plattformen

October 17, 2024

Sie können eine bessere SSL-TPS-Leistung in AWS- und GCP-Clouds erzielen, indem Sie die Gewichte der Paket-Engine (PE) gleichmäßig verteilen. Die Aktivierung dieser Funktion kann zu einem leichten Rückgang des HTTP-Durchsatzes um etwa 10—12% führen.

In AWS- und GCP-Clouds zeigen die NetScaler VPX-Instanzen mit 10—16 vCPUs keine Leistungsverbesserung, da die PE-Gewichte standardmäßig gleichmäßig verteilt sind.

> **Hinweis:**
>
> In der Azure-Cloud sind die PE-Gewichte standardmäßig gleichmäßig verteilt. Diese Funktion verbessert nicht die Leistung der Azure-Instanzen.

Konfigurieren des PE-Modus mithilfe der NetScaler CLI

Nachdem Sie den PE-Modus eingestellt haben, müssen Sie das System neu starten, damit die Konfigurationsänderungen wirksam werden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Wenn der PE-Modus auf CPUBOUND eingestellt ist, sind die PE-Gewichte gleichmäßig verteilt. Wenn der PE-Modus auf DEFAULT eingestellt ist, werden die PE-Gewichte auf Standardwerte eingestellt.

> **Hinweis:**
>
> Dieser Befehl ist knotenspezifisch. In einem Hochverfügbarkeits- oder Cluster-Setup müssen Sie den Befehl auf jedem Knoten ausführen. Wenn Sie den Befehl auf CLIP ausführen, tritt der folgende Fehler auf: `Vorgang auf CLIP nicht zulässig`

Führen Sie den folgenden Befehl aus, um den Status des konfigurierten PE-Modus anzuzeigen:

```
show cpuparam
```

Beispiel

```
> show cpuparam
    Pemode:  CPUBOUND
 Done
```

Wenden Sie die PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud an

Um die PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud anzuwenden, müssen Sie eine Datei `/nsconfig/.cpubound.conf` mit dem benutzerdefinierten Skript erstellen. Weitere Informationen finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start des NetScaler-Geräts in der Cloud.

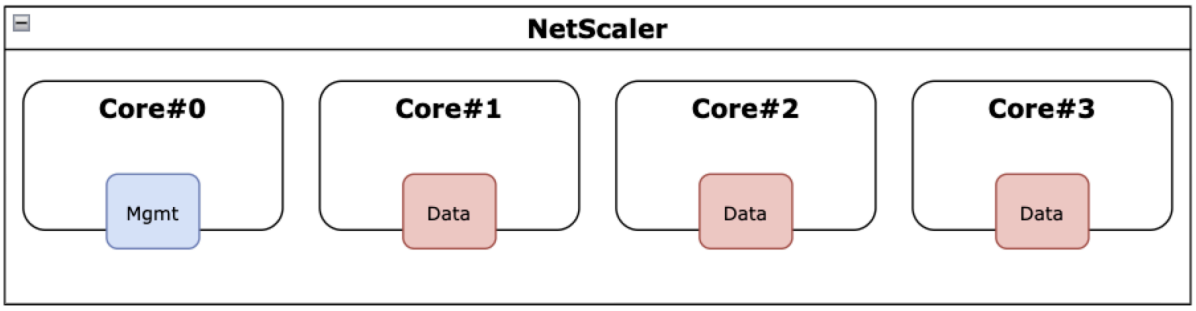
Gleichzeitiges Multithreading für NetScaler VPX in öffentlichen Clouds konfigurieren

October 17, 2024

NetScaler verwendet verschiedene dedizierte Kerne für seine Management- und Datenebenenfunktionen. Ein Kern wird in der Regel Funktionen der Managementebene zugewiesen. Die restlichen verfügbaren Kerne sind Datenebenenfunktionen zugewiesen.

Die folgende Abbildung zeigt eine vereinfachte Darstellung eines NetScaler VPX mit 4 Kernen.

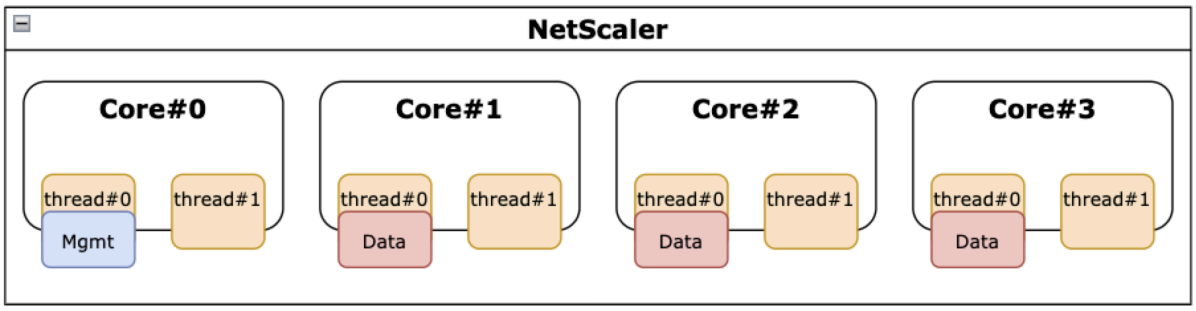
Abbildung 2. NetScaler-Management und Datenebenenworkload auf einem Vierkernsystem



Das vorherige Bild zeigt zwar die Verteilung der NetScaler-Funktionen auf die verfügbaren Kerne, es ist jedoch nicht unbedingt eine genaue Darstellung der zugrunde liegenden Hardware. Die meisten modernen x86-CPUs bieten zwei logische Kerne pro physischem Kern über Funktionen, die kommerziell als Intel Hyperthreading (HT) oder AMD Simultaneous Multithreading (SMT) bekannt sind.

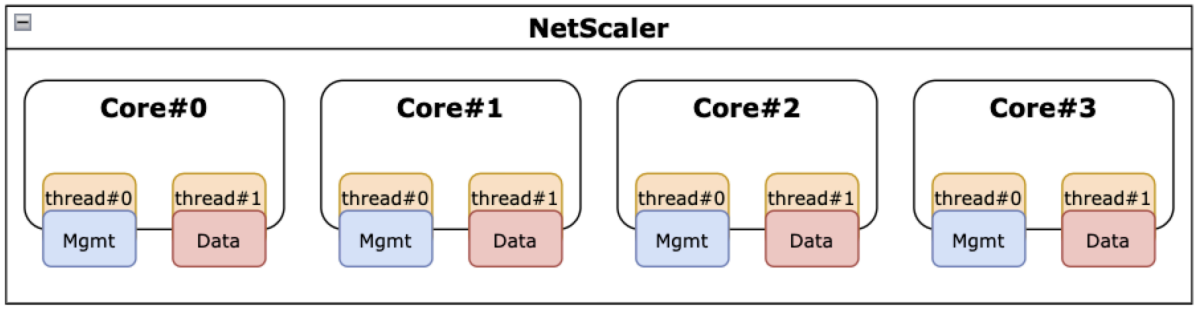
Das folgende Bild zeigt NetScaler VPX, das auf einer modernen CPU mit deaktiviertem SMT läuft. Jeder CPU-Kern ist in zwei oder mehr logische CPUs aufgeteilt, die allgemein als Threads bezeichnet werden. Jeder Thread hat seinen eigenen Satz replizierter Ressourcen, einen Teil der partitionierten Ressourcen, und konkurriert mit seinen Geschwister-Threads um gemeinsam genutzte Ressourcen.

Abbildung 2. NetScaler-Management und Datenebenenworkload auf einem 4-Core-/8-Thread-System mit deaktiviertem SMT



Das folgende Bild zeigt NetScaler VPX, das auf einer modernen CPU mit aktiviertem SMT ausgeführt wird.

Abbildung 3. NetScaler-Management und Workload auf Datenebene auf einem 4-Core-System mit aktiviertem SMT



Die Aktivierung von SMT verbessert die NetScaler-Leistung durch:

- Ausführen von Datenebenenfunktionen auf allen physischen Kernen.
- Verschieben der Funktionen der Verwaltungsebene in den Geschwisterthread.
- Einführung eines flexiblen Mechanismus zur Ressourcenbegrenzung, um zu verhindern, dass Funktionen der Verwaltungsebene die Leistung von Funktionen der Datenebene beeinträchtigen.

SMT-Unterstützungsmatrix

Die VPX-Plattformen, Cloud-Instanztypen und NetScaler-Versionen, die SMT unterstützen, sind in der folgenden Tabelle aufgeführt.

VPX-Plattform	Instanztypen	NetScaler VPX Version
————	————	————
AWS	M5, 5n, c5, c5n	14.1-12.x und höher
Azure	Jede Instanzfamilie mit Hyperthreading, zum Beispiel DS_v4	14.1-12.x und höher
GCP	e2-Instanzen	14.1-12.x und höher

> **Hinweis:**
>
> Durch die Aktivierung der SMT-Funktion wird die NetScaler VPX-Leistung bei den unterstützten Typen gesteigert.

Einschränkungen

Die SMT-Funktion verdoppelt effektiv die vCPUs, die einer NetScaler-Appliance zur Verfügung stehen. Die Lizenzbeschränkungen müssen berücksichtigt werden, damit die NetScaler Appliance sie verwenden kann.

Betrachten Sie beispielsweise NetScaler VPX, das in Abbildung 3 dargestellt ist. Wenn eine durchsatzbasierte Lizenzierung verwendet wird, ist eine Lizenz von 10 Gbit/s oder höher mit der SMT-Funktion erforderlich, um 8 vCPUs zu aktivieren. Bisher war eine 1-Gbit/s-Lizenz ausreichend, um 4 vCPUs zu aktivieren. Wenn eine vCPU-Lizenzierung verwendet wird, muss NetScaler VPX so konfiguriert werden, dass Lizenzen für die doppelte Anzahl an vCPUs ausgecheckt werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist. Wenden Sie sich an den technischen Support von NetScaler, um weitere Informationen zu diesem Thema zu erhalten.

SMT konfigurieren

Bevor Sie die SMT-Funktion aktivieren, stellen Sie sicher, dass Ihre Plattform diese Funktion unterstützt. Weitere Informationen finden Sie in der Tabelle mit der Unterstützungsmatrix im vorherigen

Abschnitt.

Gehen Sie wie folgt vor, um die SMT-Funktion zu aktivieren:

1. Erstellen Sie eine leere Datei mit dem Namen `.smt_handling` im Verzeichnis "/nsconfig".
2. Speichert die aktuelle Konfiguration.
3. Starten Sie die NetScaler VPX-Instanz neu.

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

4. Nach dem Neustart zeigt NetScaler an, dass die Funktion sowohl verfügbar als auch aktiviert ist.

```
smt_handling and smt_handling_active are set to " 1 "

> shell sysctl -a | grep smt_handling
netscaler.smt_handling_platform: 1
netscaler.smt_handling: 1
netscaler.smt_handling_active: 1
```

Gehen Sie wie folgt vor, um die SMT-Funktion zu deaktivieren:

1. Entfernen Sie die Datei `.smt_handling`.
2. Starten Sie die NetScaler VPX-Instanz neu.

```
shell rm -f /nsconfig/.smt_handling
  Done

reboot

Are you sure you want to restart NetScaler (Y/N)?   [N]:Y
Done
```

3. Nach dem Neustart zeigt NetScaler an, dass die Funktion verfügbar, aber deaktiviert ist.

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

Problembehandlung

Führen Sie den Shell-Befehl `sysctl` aus, um den Status der SMT-Funktion zu überprüfen.


```
```
  > shell sysctl -a | grep smt_handling
  >
```
```

Der Befehl kann jede der folgenden Ausgaben zurückgeben.

- Die SMT-Funktion fehlt.

  Der Befehl `sysctl` gibt keine Ausgabe zurück.

- Die SMT-Funktion wird nicht unterstützt.

  Die SMT-Funktion wird aus einem der folgenden Gründe nicht unterstützt:

  - Ihr NetScaler VPX ist älter als 13.1-48.x oder 14.1-12.x.
  - Ihre Cloud unterstützt SMT nicht.
  - Ihr VM-Instanztyp unterstützt SMT nicht. Beispielsweise ist die Anzahl der vCPUs höher als 8.

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

- Die SMT-Funktion wird unterstützt, aber nicht aktiviert.

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

Installieren einer NetScaler VPX Instanz auf einem Bare-Metal-Server

October 17, 2024

Ein Bare-Metal ist ein vollständig dedizierter physischer Server, der physische Isolation bietet und vollständig in die Cloud-Umgebung integriert ist. Es wird auch als Single-Tenant-Server bezeichnet. Mit einem Mandantenverhältnis können Sie den lauten Nachbareffekt vermeiden. Mit Bare-Metal werden Sie nicht Zeuge des lauten Nachbareffekts, da Sie der einzige Benutzer sind.

Ein Bare-Metal-Server, der mit einem Hypervisor installiert wird, bietet Ihnen eine Management-Suite zum Erstellen virtueller Maschinen auf dem Server. Der Hypervisor führt keine Anwendungen nativ aus. Ziel ist es, Ihre Workloads in separate virtuelle Maschinen zu virtualisieren, um die Flexibilität und Zuverlässigkeit der Virtualisierung zu erreichen.

Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Bare-Metal-Servern

Ein Bare-Metal-Server muss von einem Cloud-Anbieter bezogen werden, der alle Systemanforderungen für den jeweiligen Hypervisor erfüllt.

Installieren Sie die NetScaler VPX-Instanz auf Bare-Metal-Servern

Um NetScaler VPX-Instances auf einem Bare-Metal-Server zu installieren, müssen Sie zunächst einen Bare-Metal-Server mit ausreichenden Systemressourcen von einem Cloud-Anbieter erwerben. Auf diesem Bare-Metal-Server muss jeder der unterstützten Hypervisoren wie Linux KVM, VMware ESX, Citrix Hypervisor oder Microsoft Hyper-V installiert und konfiguriert werden, bevor die NetScaler VPX-Instanz bereitgestellt wird.

Weitere Informationen zur Liste der verschiedenen Hypervisoren und Funktionen, die auf einer NetScaler VPX-Instanz unterstützt werden, finden Sie unter Supportmatrix und Nutzungsrichtlinien.

Weitere Informationen zur Installation von NetScaler VPX Instanzen auf verschiedenen Hypervisoren finden Sie in der entsprechenden Dokumentation.

- **Citrix Hypervisor:** Siehe Installieren Sie eine NetScaler VPX-Instanz auf Citrix Hypervisor.
- **VMware ESX:** Siehe Installieren Sie eine NetScaler VPX-Instanz auf VMware ESX.
- **Microsoft Hyper-V:** Siehe Installieren Sie eine NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server.
- **Linux KVM-Plattform:** Siehe Installieren Sie eine NetScaler VPX-Instanz auf der Linux-KVM-Plattform.

Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor

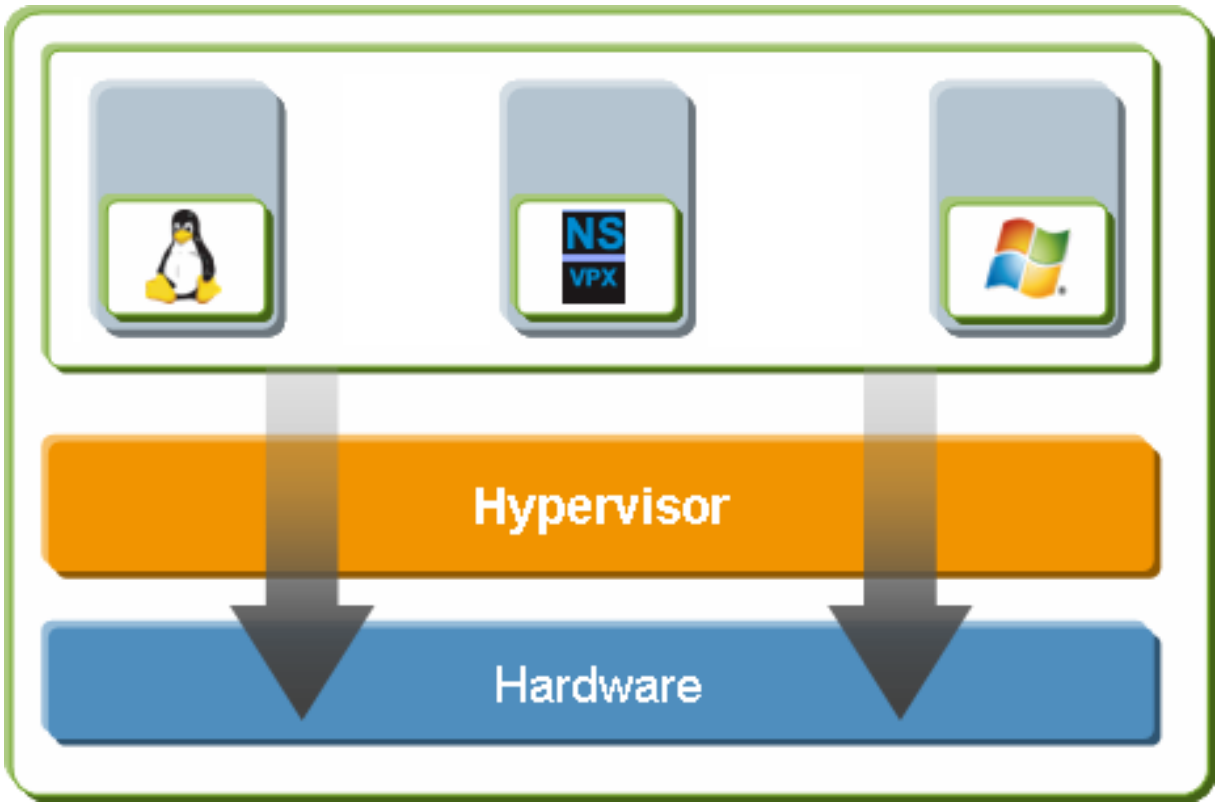
October 17, 2024

Um VPX-Instanzen auf dem Citrix Hypervisor zu installieren, müssen Sie zuerst den Hypervisor auf einem Computer mit ausreichenden Systemressourcen installieren. Um die NetScaler VPX-Instanzinstallation durchzuführen, verwenden Sie Citrix XenCenter, das auf einem Remotecomputer installiert sein muss, der über das Netzwerk eine Verbindung zum Hypervisor-Host herstellen kann.

Weitere Informationen zu Hypervisor finden Sie in der Citrix Hypervisor-Dokumentation.

Die folgende Abbildung zeigt die Bare-Metal-Lösungsarchitektur der NetScaler VPX-Instanz auf Hypervisor.

Abbildung. Eine NetScaler VPX-Instanz auf Citrix Hypervisor



Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf Hypervisor

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie Hypervisor Version 6.0 oder höher auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie XenCenter auf einer Verwaltungsarbeitsstation, die die Mindestsystemanforderungen erfüllt.
- Besorgen Sie sich Lizenzdateien für virtuelle Appliances. Weitere Informationen zu Lizenzen für virtuelle Appliances finden Sie im NetScaler-Lizenzierungshandbuch.

Hypervisor-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestanforderungen an die Hardware für eine Hypervisor-Plattform beschrieben, auf der eine NetScaler VPX-Instanz ausgeführt wird.

Tabelle 1. In VM1 verwendete IP-Adressen **Tabelle 1.** Mindestsystemanforderungen für Hypervisor, der eine NCore VPX-Instanz ausführt

Komponente	Voraussetzung
CPU	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um die NetScaler VPX-Instanz auszuführen, muss die Hardwareunterstützung für die Virtualisierung auf dem Hypervisor-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Einzelheiten finden Sie in der BIOS-Dokumentation.
RAM	3 GB
Speicherplatz	Lokal angeschlossener Speicher (PATA, SATA, SCSI) mit 40 GB Speicherplatz. Hinweis: Die Hypervisor-Installation erstellt eine 4-GB-Partition für die Hypervisor-Host-Steuerdomäne. Der verbleibende Speicherplatz ist für die NetScaler VPX-Instanz und andere virtuelle Maschinen verfügbar.
Netzwerkkarte	Eine 1-Gbit/s-NIC; empfohlen: zwei 1-Gbit/s-NICs

Informationen zur Installation von Hypervisor finden Sie in der Hypervisor-Dokumentation unter http://support.citrix.com/product/xens/.

In der folgenden Tabelle sind die virtuellen Rechenressourcen aufgeführt, die Hypervisor für jede virtuelle NCore VPX-Appliance bereitstellen muss.

Tabelle 2. **Tabelle 2.** Minimale virtuelle Computing-Ressourcen, die zum Ausführen einer NCore VPX-Instanz erforderlich sind

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	2

> **Hinweis:**
>
> Für den Produktionseinsatz der NetScaler VPX-Instanz empfiehlt Citrix, die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf die höchste Stufe einzustellen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

XenCenter Systemanforderungen

XenCenter ist eine Windows-Clientanwendung. Es kann nicht auf demselben Computer wie der Hypervisor-Host ausgeführt werden. Weitere Informationen zu Mindestsystemanforderungen und zur Installation von XenCenter finden Sie in den folgenden Hypervisor-Dokumenten:

- Systemanforderungen
- Installieren

Installieren Sie NetScaler VPX-Instanzen auf Hypervisor mithilfe von XenCenter

Nachdem Sie Hypervisor und XenCenter installiert und konfiguriert haben, können Sie XenCenter verwenden, um virtuelle Appliances auf Hypervisor zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge an Speicher ab, die auf der Hardware verfügbar ist, auf der Hypervisor ausgeführt wird.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen auf Hypervisor mithilfe von XenCenter zu installieren:

1. Starten Sie **XenCenter** auf Ihrer Workstation.
2. Klicken Sie im Menü **Server** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Neuen Server hinzufügen** in das Textfeld Hostname die IP-Adresse oder den DNS-Namen des Hypervisors ein, zu dem Sie eine Verbindung herstellen möchten.
4. Geben Sie in den Textfeldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Verbinden**. Der Hypervisor-Name wird im Navigationsbereich mit einem grünen Kreis angezeigt, der angibt, dass der Hypervisor verbunden ist.
5. Klicken Sie im Navigationsbereich auf den Namen des Hypervisor, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
6. Klicken Sie im Menü **VM** auf **Importieren**.
7. Navigieren Sie im Dialogfeld **Import** im Namen der Importdatei zu dem Speicherort, an dem Sie die NetScaler VPX `.xva` VPX-Instanzbilddatei gespeichert haben. Stellen Sie sicher, dass die Option Exportierte VM ausgewählt ist, und klicken Sie dann auf **Weiter**.

8. Wählen Sie den Hypervisor aus, auf dem Sie die virtuelle Appliance installieren möchten, und klicken Sie dann auf **Weiter**.
9. Wählen Sie das lokale Speicher-Repository aus, in dem die virtuelle Appliance gespeichert werden soll, und klicken Sie dann auf **Importieren**, um den Importprozess zu starten
10. Sie können die virtuellen Netzwerkschnittstellen nach Bedarf hinzufügen, ändern oder löschen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
11. Klicken Sie auf **Fertig stellen**, um den Importvorgang abzuschließen.

    > **Hinweis:**
    >
    > Klicken Sie auf **Fertig stellen**, um den Importvorgang ab Um den Status des Importvorgangs anzuzeigen, klicken Sie auf die Registerkarte **Protokoll**.

12. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie die Schritte 5 bis 11.

> **Hinweis:**
>
> Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, lesen Sie Upgraden oder Downgrade der Systemsoftware.

Konfigurieren von VPX-Instanzen für die Verwendung von Single-Root-I/O-Virtualisierungs-Netzwerkschnittstellen (SR-IOV)

October 17, 2024

Nachdem Sie eine NetScaler VPX-Instanz auf Citrix Hypervisor installiert und konfiguriert haben, können Sie die virtuelle Appliance für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren.

Die folgenden NICs werden unterstützt:

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

Einschränkungen

Citrix Hypervisor unterstützt einige Funktionen auf SR-IOV-Schnittstellen nicht. Die Einschränkungen bei Intel 82599, Intel X710 und Intel XL710 NICs sind in den folgenden Abschnitten aufgeführt.

Einschränkungen für Intel 82599 NIC

Intel 82599 NIC unterstützt die folgenden Funktionen nicht:

- L2-Modus Umschaltung
- Clustering
- Adminpartitionierung [Freigegebener VLAN-Modus]
- Hochverfügbarkeit [Aktiv - Aktiver Modus]
- Jumbo-Rahmen
- IPv6-Protokoll in Cluster-Umgebung

Einschränkungen für Intel X710 10G und Intel XL710 40G NICs

Intel X710 10G und Intel XL710 40G NICs weisen die folgenden Einschränkungen auf:

- Die Umschaltung im L2-Modus wird nicht unterstützt.
- Admin-Partitionierung (Shared VLAN-Modus) wird nicht unterstützt.
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710-NIC als Datenschnittstelle verwendet wird.
- Die Schnittstellenliste ordnet neu an, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und automatische Absprache werden nicht unterstützt.
- Sowohl für Intel X710 10G- als auch für Intel XL710 40G-NICs ist die Schnittstelle als 40/x-Schnittstelle verfügbar.
- Bis zu nur 16 Intel X710/XL710 SR-IOV-Schnittstellen können auf einer VPX-Instanz unterstützt werden.

> **Hinweis:**
>
> Damit Intel X710 10G- und Intel XL710 40G-NICs IPv6 unterstützen, aktivieren Sie den Vertrauensmodus für die virtuellen Funktionen (VFs), indem Sie den folgenden Befehl auf dem Citrix Hypervisor-Host eingeben:
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> **Beispiel**
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```

Voraussetzungen für Intel 82599 NIC

Stellen Sie auf dem Citrix Hypervisor-Host sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Blockieren Sie den Treiber `ixgbevf`, indem Sie der Datei **/etc/modprobe.d/blacklist.conf** den folgenden Eintrag hinzufügen:

  blacklist ixgbevf
- Aktivieren Sie SR-IOV Virtual Functions (VFs), indem Sie der Datei **/etc/modprobe.d/ixgbe** den folgenden Eintrag hinzufügen:

  optionen ixgbe max_vfs=* <number_of_VFs>*

  Dabei ist <*number_VFs*> die Anzahl der SR-IOV-VFs, die Sie erstellen möchten.
- Stellen Sie sicher, dass SR-IOV im BIOS aktiviert ist.

> **Hinweis:**
>
> IXGBE-Treiberversion 3.22.3 wird empfohlen.

Weisen Sie der NetScaler VPX-Instanz Intel 82599 SR-IOV VFs zu, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um der NetScaler VPX-Instanz einen Intel 82599 SR-IOV-VFs zuzuweisen:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV-VFs der NetScaler VPX-Instanz zuzuweisen:

   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>*

   Ort:

   - ** <Xen host UUID>ist die UUID des Citrix Hypervisor-Hosts.
   - <*NetScaler VM UUID*> ist die UUID der NetScaler VPX-Instanz.
   - <*interface name*> ist die Schnittstelle für die SR-IOV-VFs.
   - <*MAC address* > ist die MAC-Adresse des SR-IOV VF.

   > **Hinweis:**
   >
   > Geben Sie die MAC-Adresse an, die Sie im Parameter args:mac= verwenden möchten. Wenn nicht angegeben, generiert das Skript `iovirt` zufällig eine MAC-Adresse und weist sie zu. Wenn Sie die SR-IOV-VFs im Link-Aggregationsmodus verwenden möchten, stellen Sie sicher, dass Sie die MAC-Adresse als 00:00:00:00:00:00 angeben.

2. Starten Sie die NetScaler VPX-Instanz.

Aufheben der Zuweisung von Intel 82599 SR-IOV-VFs zur NetScaler VPX-Instanz mithilfe des Citrix Hypervisor-Hosts

Wenn Sie ein falsches SR-IOV-VFs zugewiesen haben oder wenn Sie ein zugewiesenes SR-IOV-VFs ändern möchten, müssen Sie die Zuweisung der SR-IOV-VFs aufheben und der NetScaler VPX-Instanz neu zuweisen.

Gehen Sie folgendermaßen vor, um die Zuweisung der SR-IOV-Netzwerkschnittstelle aufzuheben, die einer NetScaler VPX-Instanz zugewiesen ist:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV-VFs der NetScaler VPX-Instanz zuzuweisen und die NetScaler VPX-Instanz neu zu starten:

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

   Ort:

   - <*Xen_host_UUID*> - Die UUID des Citrix Hypervisor-Hosts.
   - <*Netscaler_VM_UUID*> - Die UUID der NetScaler VPX-Instanz ist.

2. Starten Sie die NetScaler VPX-Instanz.

Weisen Sie der NetScaler VPX-Instanz Intel X710/XL710 SR-IOV VFs zu, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um der NetScaler VPX-Instanz einen Intel X710/XL710 SR-IOV VF zuzuweisen:

1. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um ein Netzwerk zu erstellen.

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

   Beispiel

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

2. Ermitteln Sie den PIF Universal Unique Identifier (UUID) der NIC, auf der das SR-IOV-Netzwerk konfiguriert werden soll.

   ```
   xe pif-list

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


3. Konfigurieren Sie das Netzwerk als SR-IOV-Netzwerk. Der folgende Befehl gibt auch die UUID des neu erstellten SR-IOV-Netzwerks zurück:

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

Beispiel

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

Um weitere Informationen zu den SR-IOV-Netzwerkparametern zu erhalten, führen Sie den folgenden Befehl aus:

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

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

4. Erstellen Sie eine virtuelle Schnittstelle (VIF) und hängen Sie sie an die Ziel-VM an.

```
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
3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
```

> **Hinweis:**
>
> Die NIC-Indexnummer der VM muss mit 0 beginnen.

Verwenden Sie den folgenden Befehl, um die VM-UUID zu finden:

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

Entfernen Sie Intel X710/XL710 SR-IOV VFs aus der NetScaler-Instanz, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um einen Intel X710/XL710 SR-IOV VF aus einer NetScaler VPX-Instanz zu entfernen:

1. Kopieren Sie die UUID für das VIF, das Sie löschen möchten.

2. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um die VIF zu zerstören.

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

Beispiel

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

Konfigurieren Sie die Link-Aggregation auf der SR-IOV-Schnittstelle

Um die virtuellen SR-IOV-Funktionen (VFs) im Link-Aggregationsmodus verwenden zu können, müssen Sie die Spoof-Prüfung für virtuelle Funktionen, die Sie erstellt haben, deaktivieren.

Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

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

Ort:

- <interface_name>ist der Schnittstellenname.
- <VF_id>ist die virtuelle Funktions-ID.

Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten virtuellen Funktionen deaktiviert haben, starten Sie die NetScaler VPX-Instanz neu und konfigurieren Sie die Linkaggregation. Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

> **Wichtig:**
>
> Stellen Sie beim Zuweisen der SR-IOV-VFs zur NetScaler VPX-Instanz sicher, dass Sie die MAC-Adresse 00:00:00:00:00:00 für die VFs angeben.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN für die virtuellen SR-IOV-Funktionen konfigurieren. Anweisungen finden Sie unter Konfiguration eines VLAN.

> **Wichtig:**
>
> Stellen Sie sicher, dass der Citrix Hypervisor-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Installieren einer NetScaler VPX-Instanz auf VMware ESX

October 17, 2024

Stellen Sie vor der Installation von NetScaler VPX-Instanzen auf VMware ESX sicher, dass der VMware ESX Server auf einem Computer mit ausreichenden Systemressourcen installiert ist. Um eine NetScaler VPX-Instanz auf VMware ESXi zu installieren, verwenden Sie den VMware vSphere-Client. Der Client oder das Tool muss auf einem Remote-Computer installiert sein, der über das Netzwerk eine Verbindung zu VMware ESX herstellen kann.

Dieser Abschnitt enthält die folgenden Themen:

- Voraussetzungen
- Installieren einer NetScaler VPX-Instanz auf VMware ESX

> **Wichtig:**
>
> Sie können keine standardmäßigen VMware Tools installieren oder die auf einer NetScaler VPX-Instanz verfügbare Version von VMware Tools aktualisieren. VMware Tools für eine NetScaler VPX-Instanz werden im Rahmen der NetScaler-Softwareversion bereitgestellt.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie VMware ESX auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie einen virtuellen Switch und verbinden Sie die physische Netzwerkkarte mit dem virtuellen Switch.
- Fügen Sie eine Portgruppe hinzu und verbinden Sie sie mit dem virtuellen Switch.
- Hängen Sie die Portgruppe an die VM an.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzierungsübersicht.

VMware ESX-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestsystemanforderungen für VMware ESX-Server beschrieben, auf denen die virtuelle NetScaler VPX nCore Appliance ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für einen VMware ESX-Server, auf dem eine NetScaler VPX-Instanz ausgeführt wird

Komponente	Voraussetzung
CPU	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um eine NetScaler VPX-Instanz ausführen zu können, muss Hardwareunterstützung für die Virtualisierung auf dem VMware ESX-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in Ihrer BIOS-Dokumentation. Ab der NetScaler 13.1 Version unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi Hypervisor AMD-Prozessoren.
RAM	2 GB VPX. Für kritische Bereitstellungen empfehlen wir 2 GB RAM für VPX nicht, da das System in einer Umgebung mit begrenztem Arbeitsspeicher betrieben wird. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen. Empfohlen werden 4 GB RAM oder 8 GB RAM.
Speicherplatz	20 GB mehr als die minimalen Serveranforderungen von VMware für die Einrichtung von ESXi. Die Mindestanforderungen an den Server finden Sie in der VMware-Dokumentation.
Netzwerk	Eine 1-Gbit/s-NIC (NIC); Zwei 1-Gbit/s-NICs empfohlen

Hinweise zur Installation von VMware ESX finden Sie unterhttp://www.vmware.com/.

Stellen Sie für die SR-IOV-Netzwerkschnittstelle oder die PCI-Passthrough-Unterstützung sicher, dass die folgenden Prozessoren und Einstellungen aktiviert sind:

- Intel-Prozessoren, die Intel-VT unterstützen
- AMD-Prozessoren, die AMD-V unterstützen
- Die I/O Memory Management Unit (IOMMU) oder SR-IOV ist im BIOS aktiviert

Die folgenden Netzwerkkarten werden im SR-IOV-Modus unterstützt:

- Mellanox ConnectX-4 NIC, ab NetScaler Release 13.1-42.x
- Intel 82599 NIC

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die der VMware ESX-Server für jede virtuelle VPX nCore Appliance bereitstellen muss.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	4 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In ESX können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> **Hinweis:**
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktionsnutzung der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden. CPU-Zyklen (in MHz), die mindestens der Geschwindigkeit eines CPU-Kerns des ESX entsprechen, müssen reserviert werden.

Systemanforderungen für VMware vSphere-Clients

VMware vSphere ist eine Clientanwendung, die auf Windows- und Linux-Betriebssystemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 3. Mindestsystemanforderungen für die Installation des VMware vSphere-Clients

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware, suchen Sie nach der PDF-Datei “vSphere Compatibility Matrixes”unter http://kb.vmware.com/.
CPU	750 MHz; 1 Gigahertz (GHz) oder schneller empfohlen
RAM	1 GB. 2 GB empfohlen

Komponente	Voraussetzung
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 4. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei "OVF Tool User Guide"http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei "OVF Tool User Guide" http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix Konto haben, rufen Sie die Homepage unter http://www.citrix.comauf, klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen zum Erstellen eines Citrix Kontos.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

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

Installieren einer NetScaler VPX-Instanz auf VMware ESX

Nachdem Sie VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Client verwenden, um virtuelle Appliances auf dem VMware ESX-Server zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge an Speicher ab, die auf der Hardware verfügbar ist, auf der VMware ESX ausgeführt wird.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen auf VMware ESX mithilfe von VMware vSphere Client zu installieren:

1. Starten Sie den VMware vSphere Client auf Ihrer Workstation.
2. Geben Sie im Textfeld **IP-Adresse/Name** die IP-Adresse des VMware ESX-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldedaten ein, und klicken Sie dann auf Anmelden.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Deploy from file** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setupdateien gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.
6. Ordnen Sie die in der OVF-Vorlage für virtuelle Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem ESX-Host konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware ESX zu beginnen. Wenn die Installation abgeschlossen ist, informiert Sie ein Popup-Fenster über die erfolgreiche Installation.
7. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Rechtsklickmenü die Option **Power On**aus.
8. Nachdem die VM gestartet wurde, konfigurieren Sie von der Konsole aus die NetScaler IP-, Netmask- und Gateway-Adressen. Wenn Sie die Konfiguration abgeschlossen haben, wählen Sie in der Konsole die Option **Speichern und beenden** .
9. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte 6 bis Schritt 8.

> **Hinweis:**
>
> Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen.
>
> Nach der Installation können Sie den vSphere Client oder vSphere Web Client verwenden, um virtuelle Appliances auf VMware ESX zu verwalten.

> Um VLAN-Tagging auf VMware ESX zu aktivieren, konfigurieren Sie die VLAN-ID der Portgruppe auf dem vSwitch auf „Alle“(4095). Detaillierte Anweisungen zum Festlegen einer VLAN-ID auf dem vSwitch finden Sie in der VMware-Dokumentation.

Migrieren Sie eine NetScaler VPX-Instanz mithilfe von VMware VMotion

Sie können eine NetScaler VPX-Instanz mithilfe von VMware vSphere vMotion migrieren.

Folgen Sie diesen Nutzungsrichtlinien:

- VMware unterstützt die VMotion-Funktion auf virtuellen Maschinen, die mit PCI-Passthrough- und SR-IOV-Schnittstellen konfiguriert sind, nicht.
- Unterstützte Schnittstellen sind E1000 und VMXNET3. Um vMotion auf Ihrer VPX-Instanz zu verwenden, stellen Sie sicher, dass die Instanz mit einer unterstützten Schnittstelle konfiguriert ist.
- Weitere Informationen zur Migration einer Instanz mithilfe von VMware VMotion finden Sie in der VMware-Dokumentation.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der VMXNET3-Netzwerkschnittstelle

October 17, 2024

Nachdem Sie die NetScaler VPX-Instanz auf dem VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Webclient verwenden, um die virtuelle Appliance für die Verwendung von VMXNET3-Netzwerkschnittstellen zu konfigurieren.

Gehen Sie wie folgt vor, um NetScaler VPX-Instanzen für die Verwendung von VMXNET3-Netzwerkschnittstellen mithilfe des VMware vSphere Web Client zu konfigurieren:

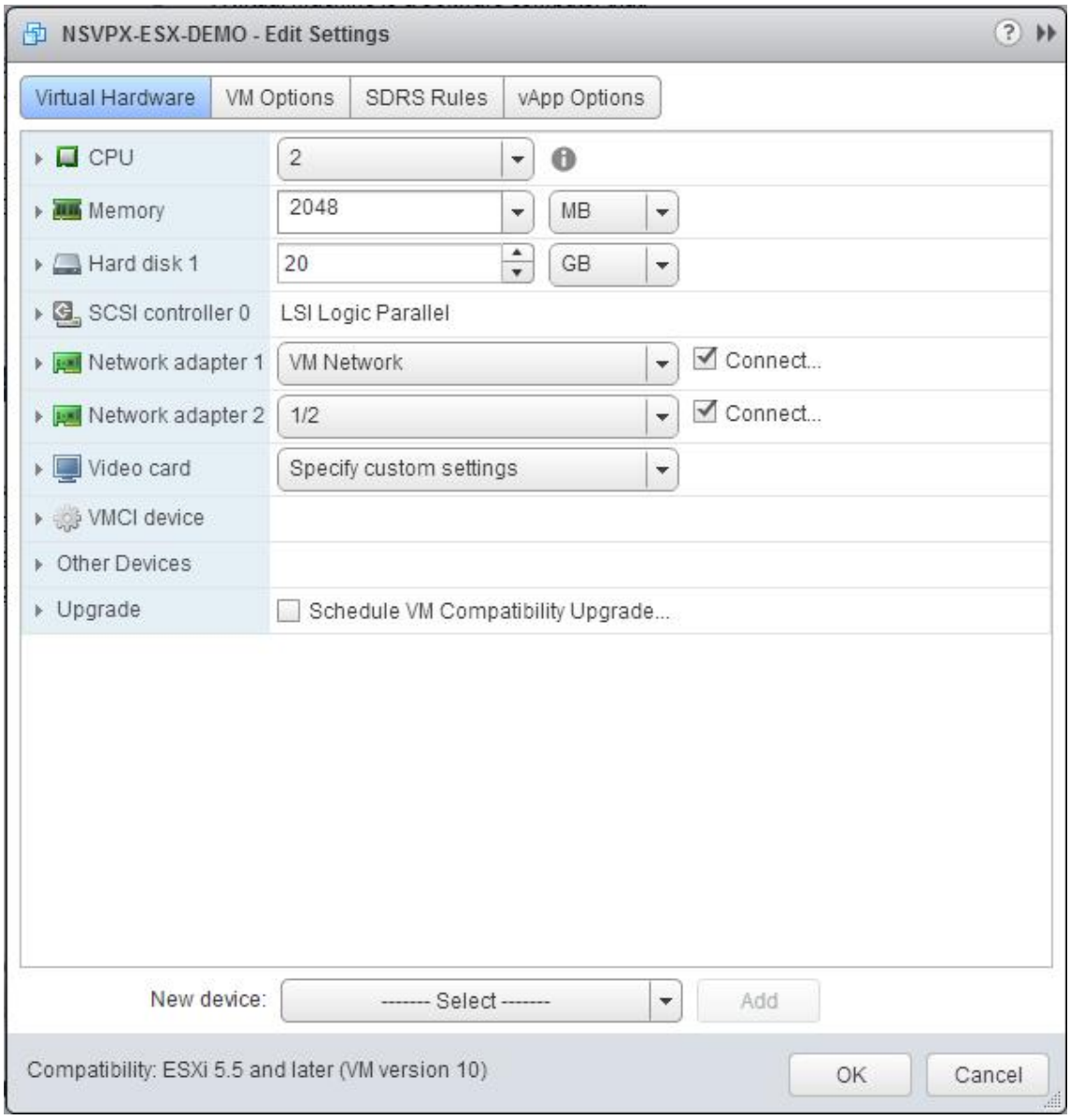
1. Wählen Sie im vSphere Web Client Hosts und Clusteraus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz wie folgt auf ESX:

   a. Schalten Sie die NetScaler VPX-Instanz aus.

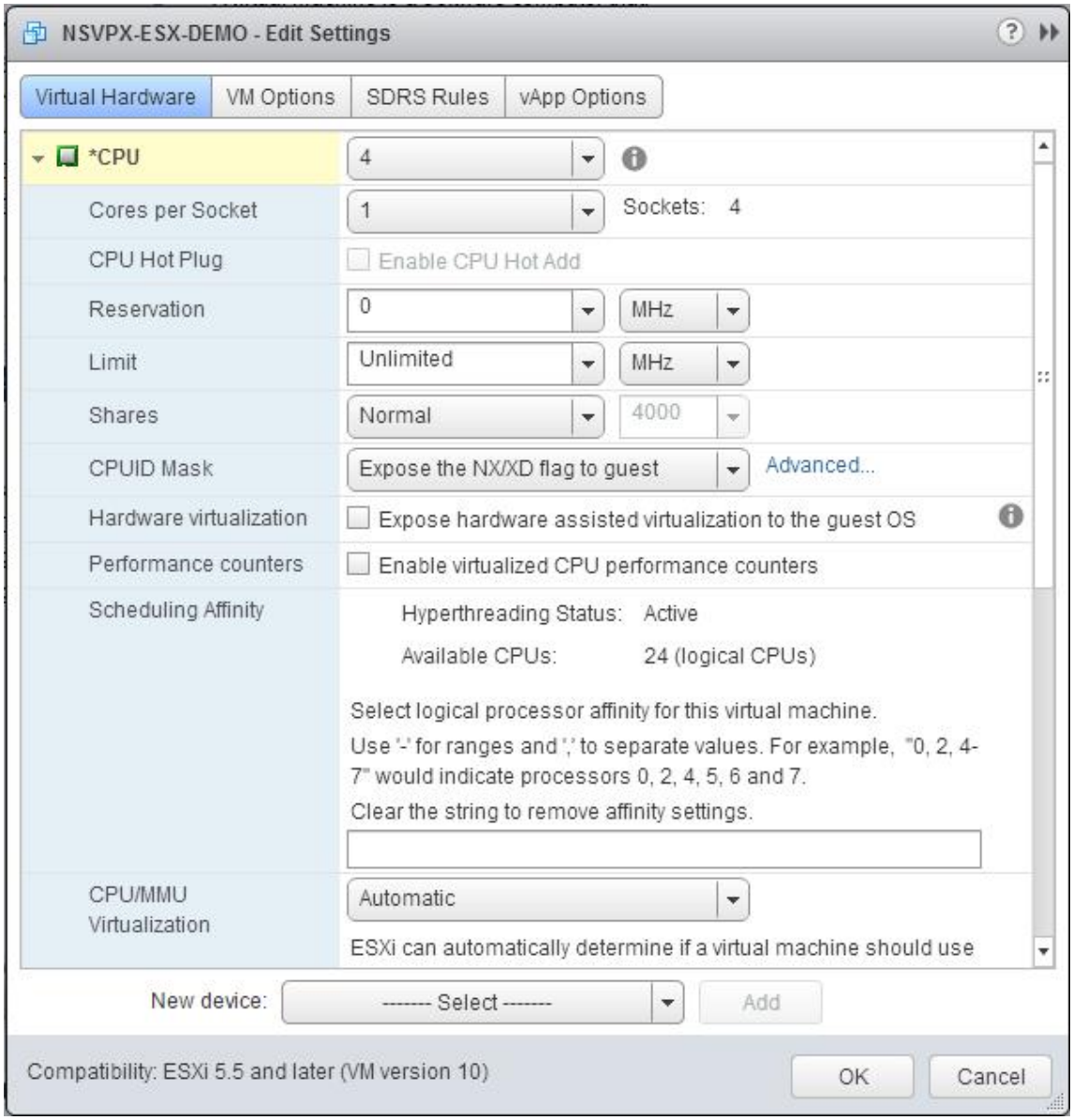
   b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie Kompatibilität > VM-Kompatibilität aktualisieren.

   c. Wählen Sie im Dialogfeld „VM-Kompatibilität konfigurieren “in der Dropdownliste „ Kompatibel mit “die Option ESXi 5.5 und höher aus und klicken Sie auf „ OK“.

3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX Instanz, und klicken Sie auf Einstellungen bearbeiten.



4. Klicken Sie im Dialogfeld <virtual_appliance> - Einstellungen bearbeiten auf den Abschnitt CPU.



5. Aktualisieren Sie im Abschnitt CPU Folgendes:

   - CPU-Anzahl
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

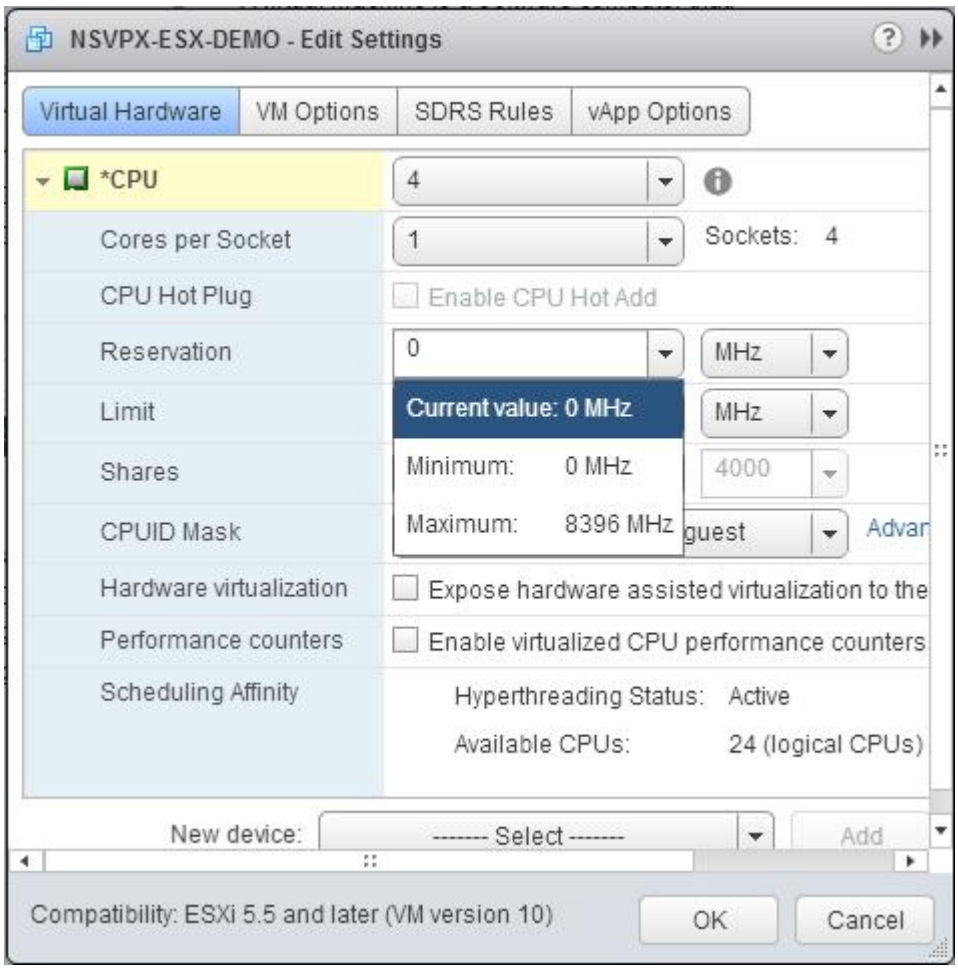
   a. Wählen Sie in der Dropdownliste CPU die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste Kerne pro Socket die Anzahl der Sockets aus.

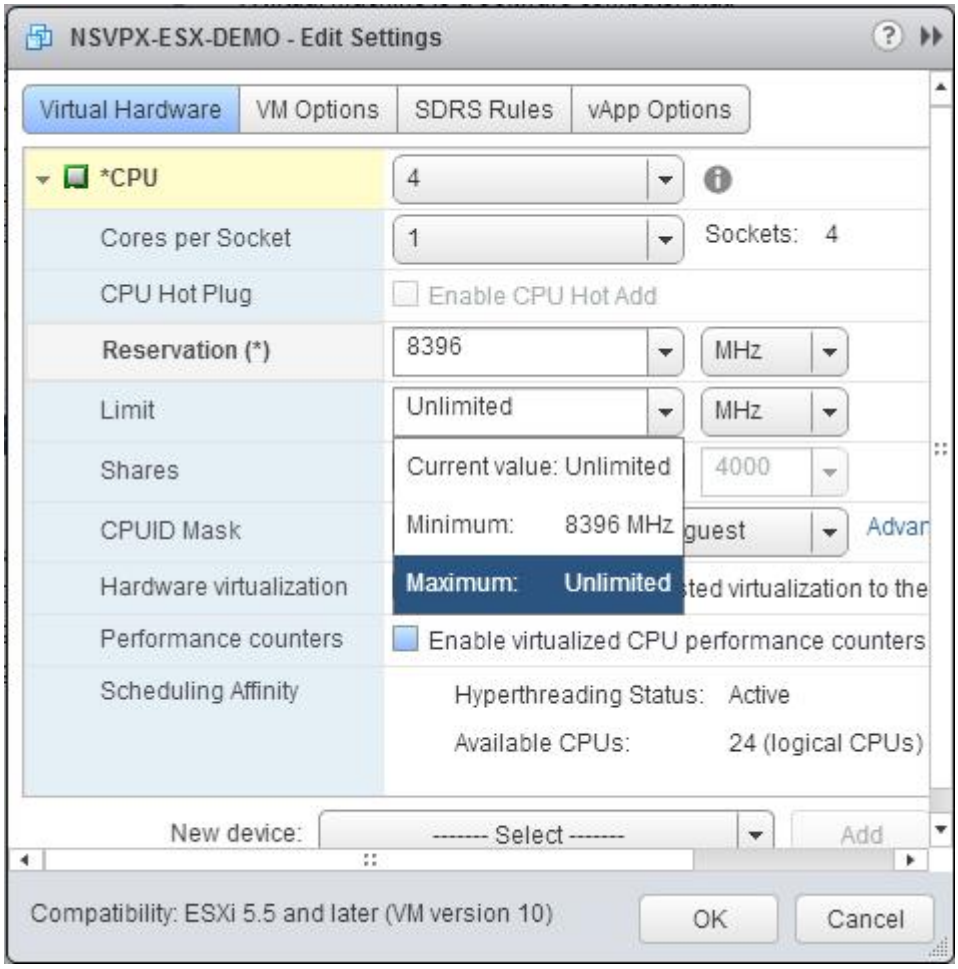
c. (Optional) Aktivieren oder deaktivieren Sie im Feld CPU-Hotplug das Kontrollkästchen CPU-Hotadd aktivieren.

> **Hinweis:**
>
> Citrix empfiehlt, die Standardeinstellung (deaktiviert) zu akzeptieren.

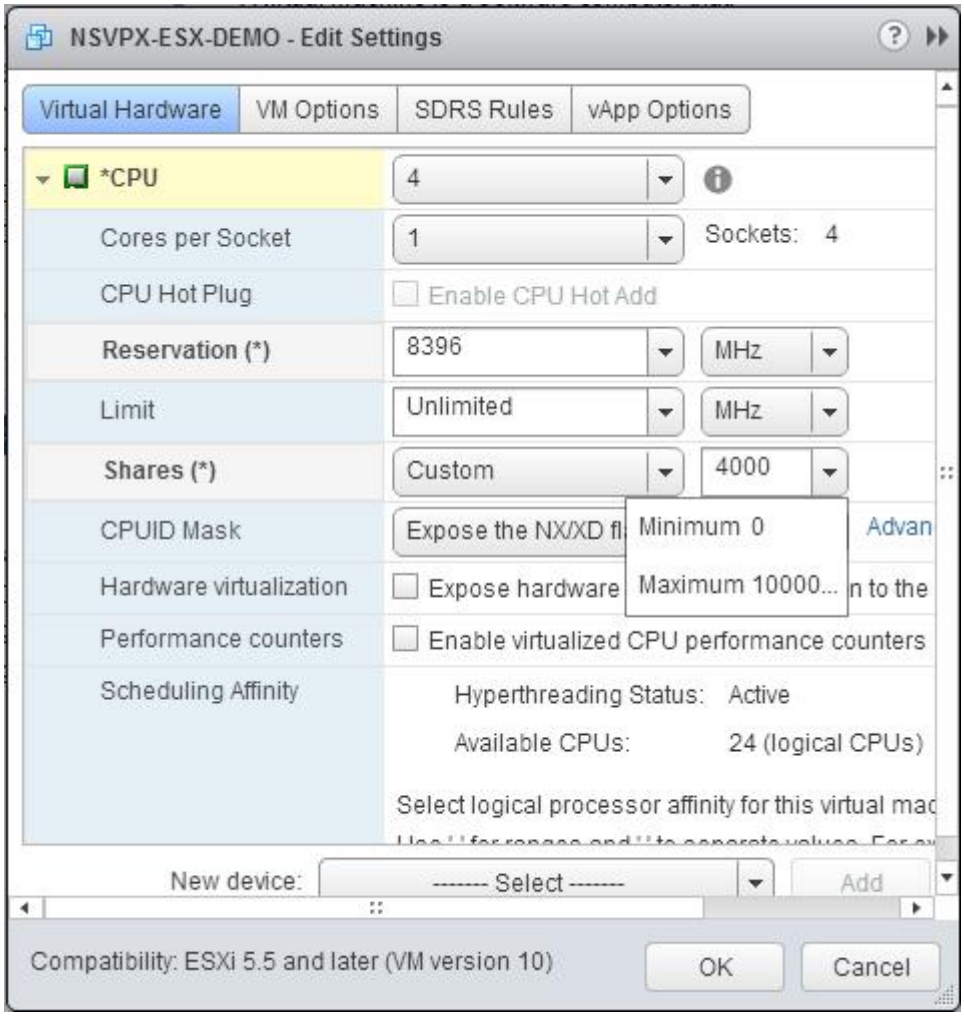
d. Wählen Sie in der Dropdownliste Reservierung die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten Anteile die Option Benutzerdefiniert und die Zahl aus, die als Maximalwert angezeigt wird.



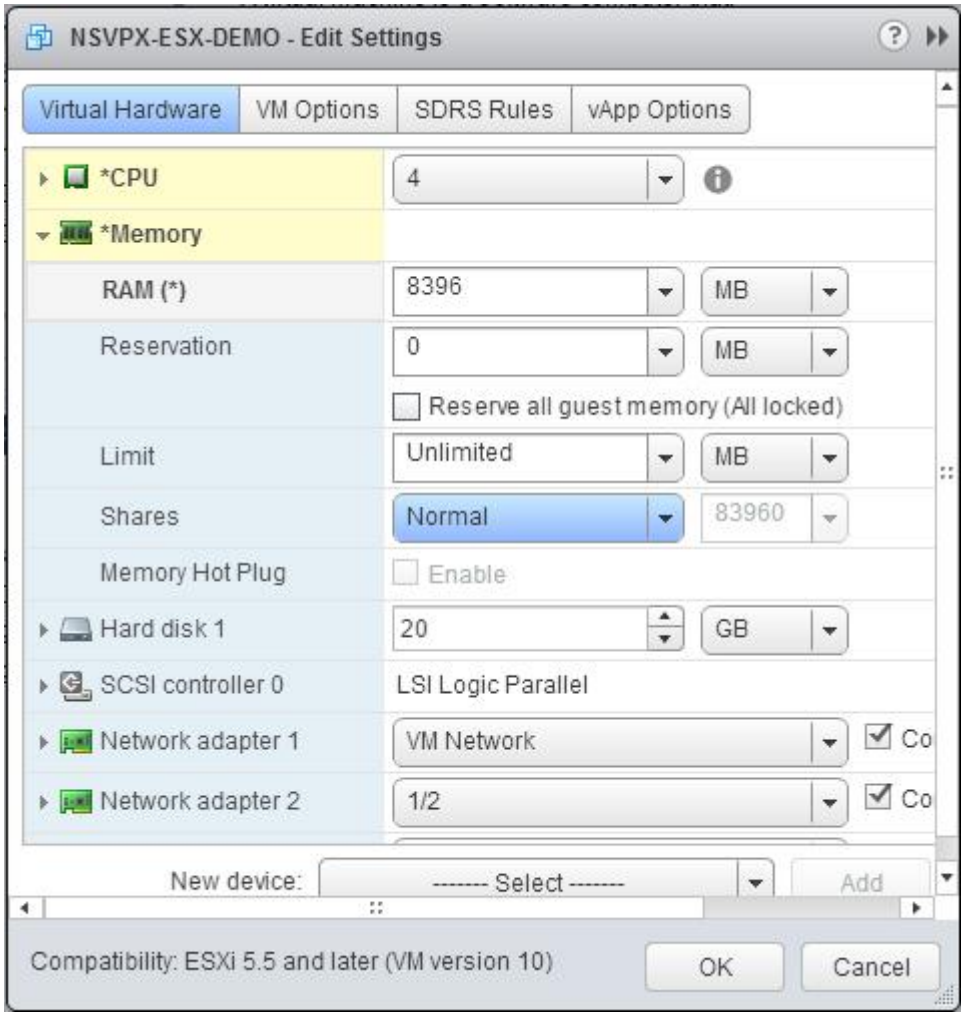
6. Aktualisieren Sie im Abschnitt Speicher Folgendes:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

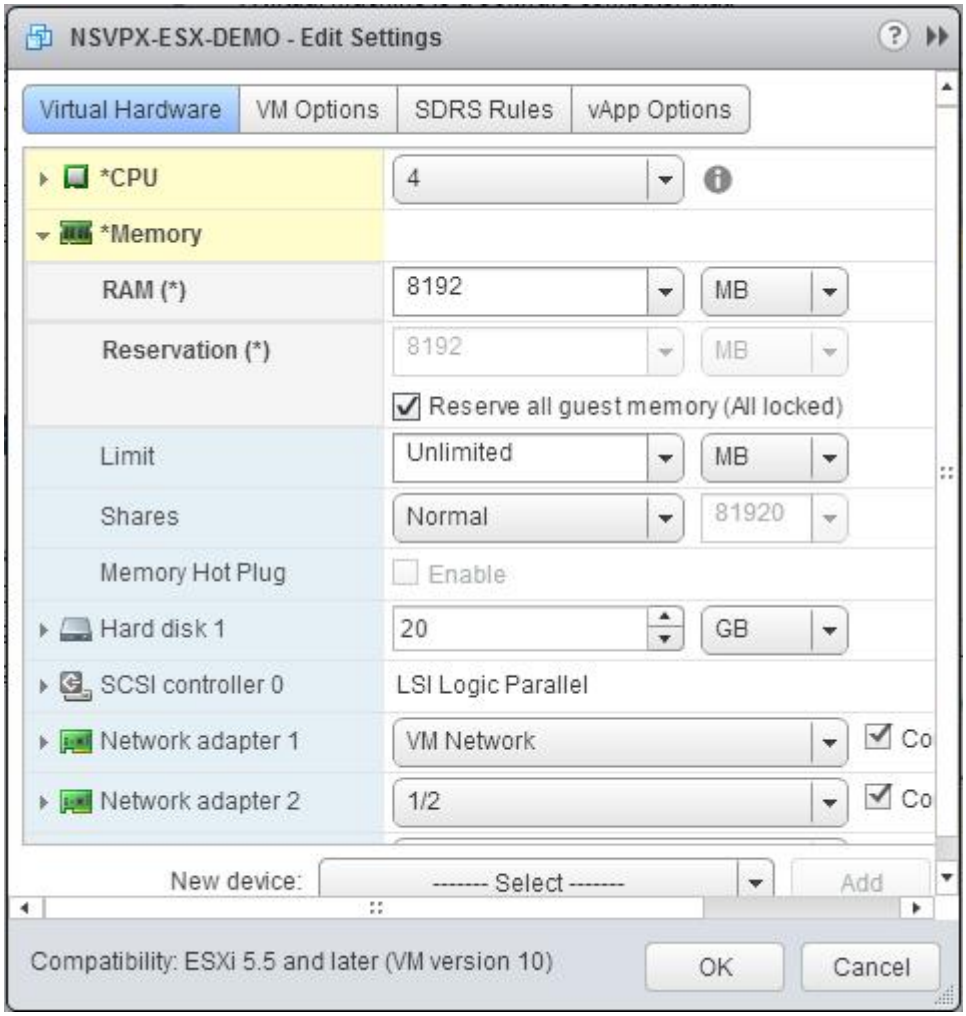
   a. Wählen Sie in der RAM-Dropdownliste die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss der Arbeitsspeicher 4 x 2 GB = 8 GB betragen.

   > **Hinweis:**
   >
   > Stellen Sie bei einer Advanced- oder Premium-Edition des NetScaler VPX-Geräts sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

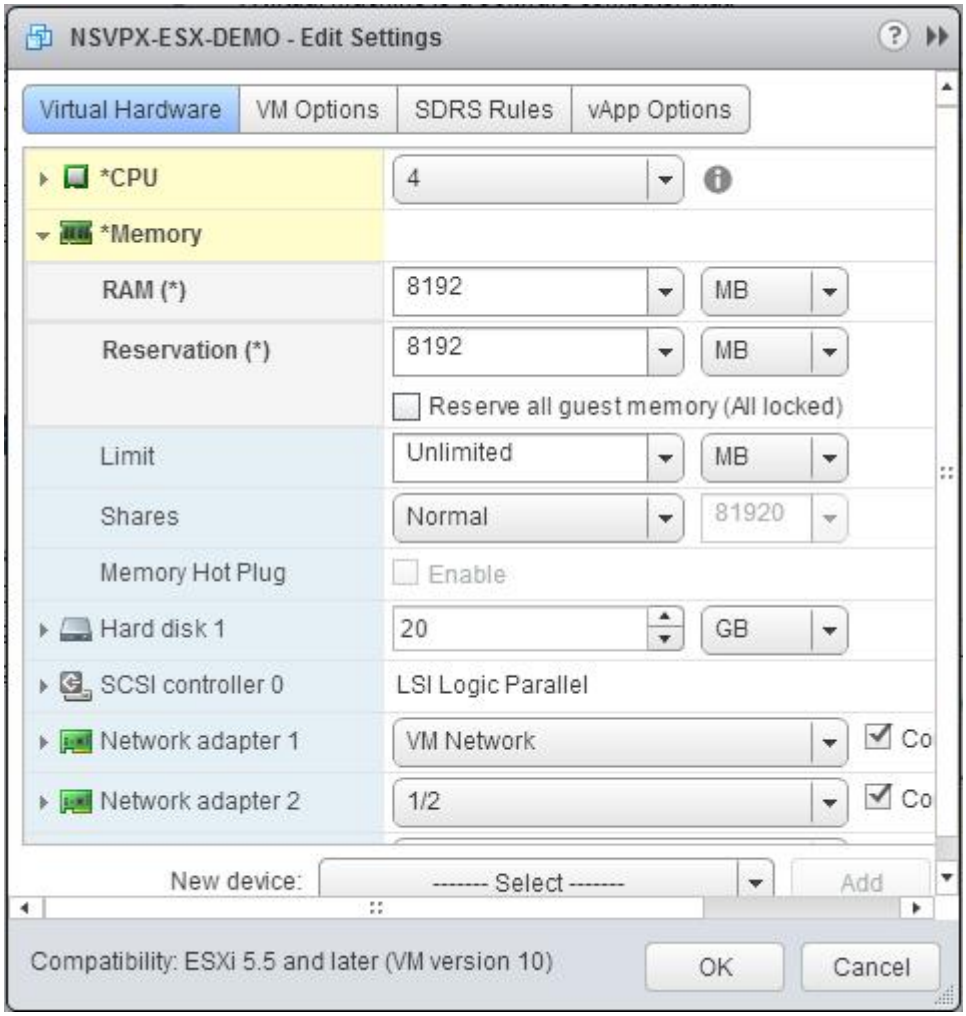


b. Geben Sie in der Dropdownliste Reservierung den Wert für die Speicherreservierung ein und aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alles gesperrt) . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Die Speicherreservierung muss der Anzahl der vCPUs x 2 GB entsprechen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

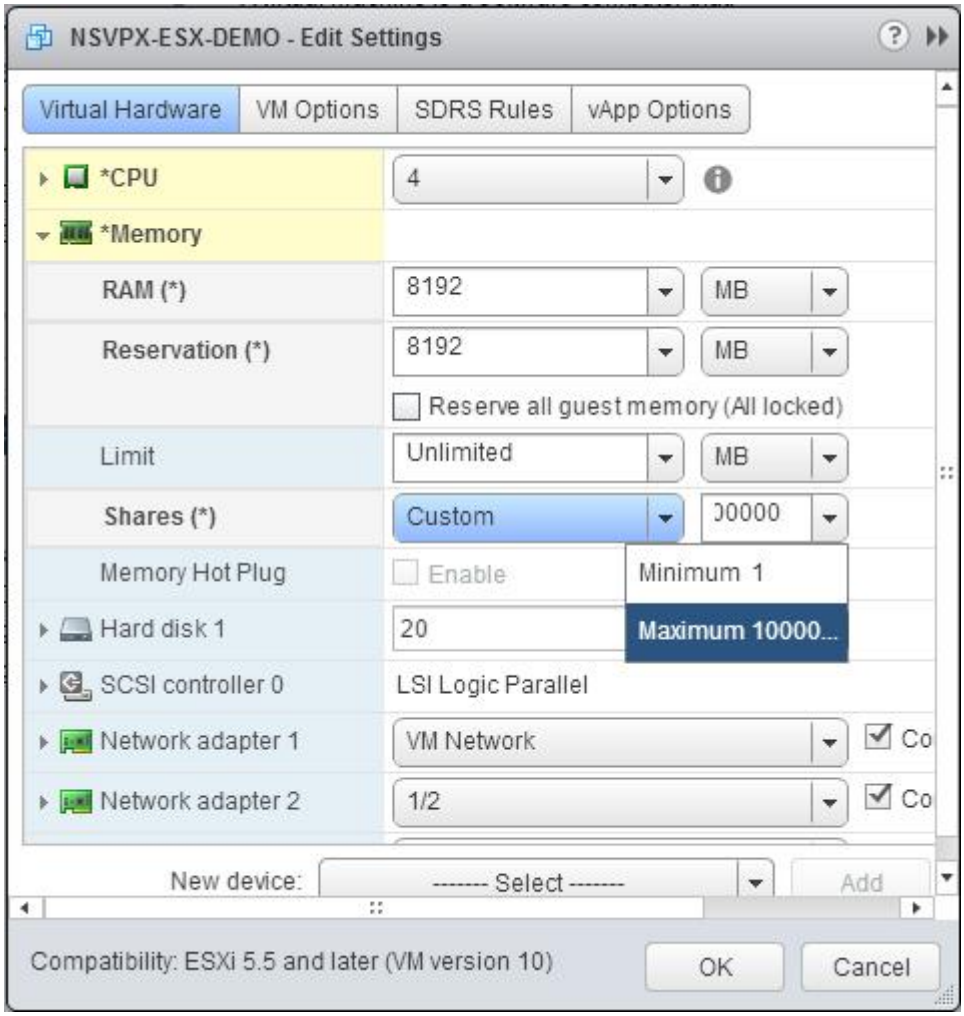
> **Hinweis:**
>
> Stellen Sie bei einer Advanced- oder Premium-Edition des NetScaler VPX-Geräts sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



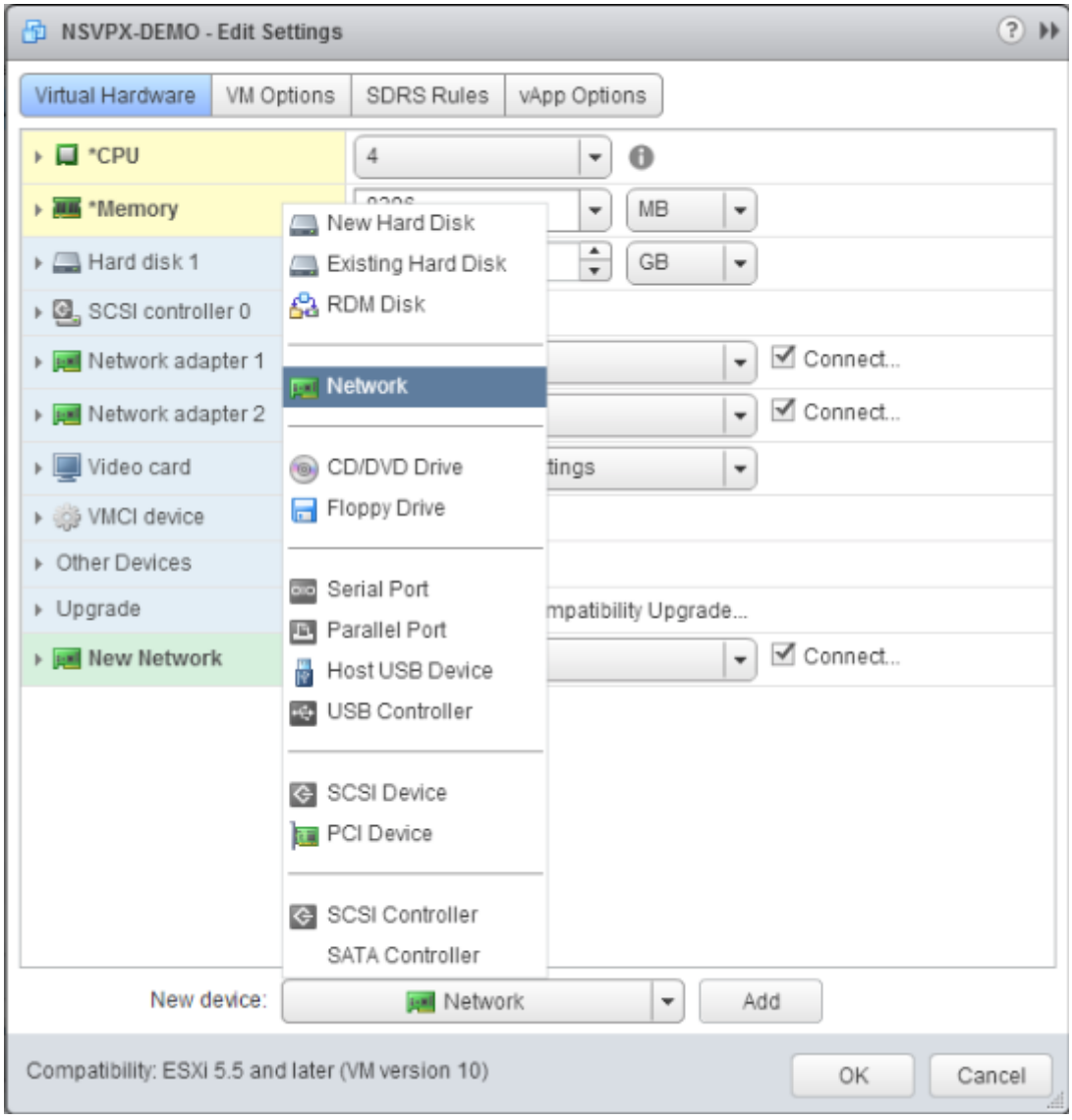
c. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten Anteile die Option Benutzerdefiniert und die Zahl aus, die als Maximalwert angezeigt wird.



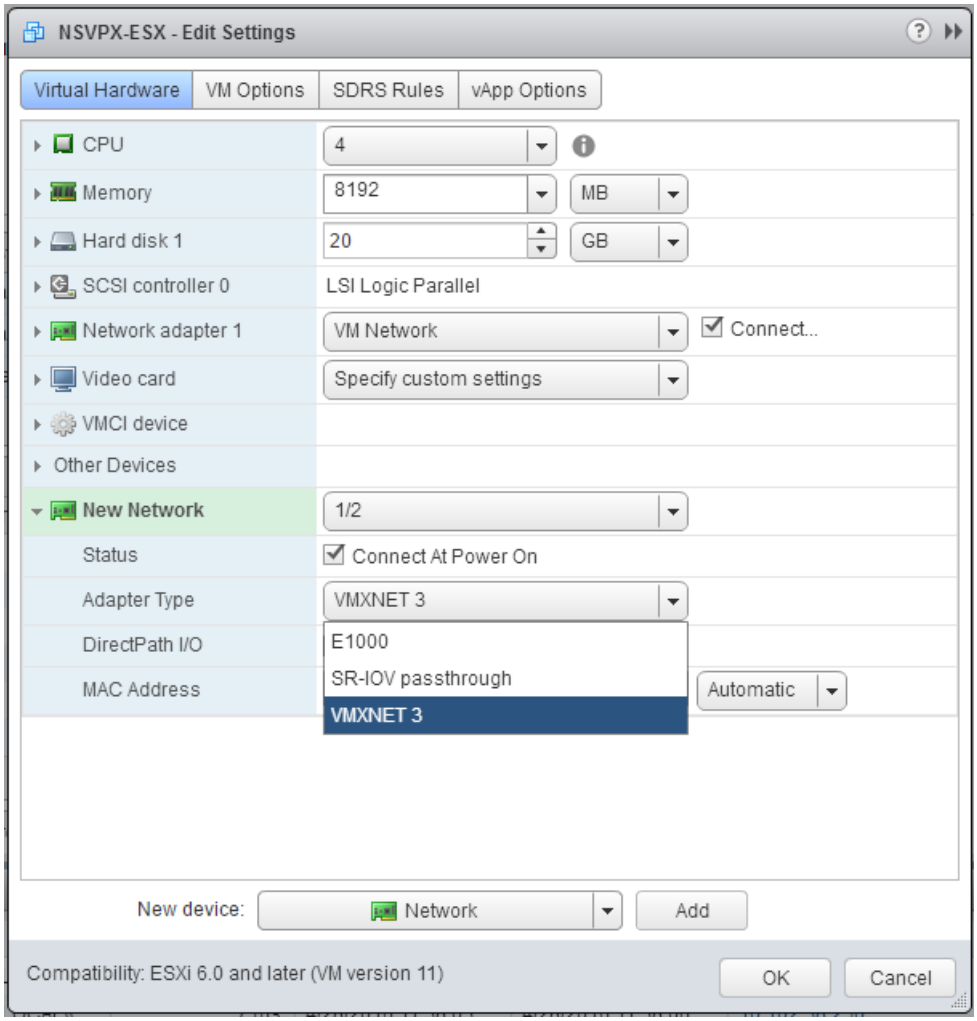
7. Fügen Sie eine VMXNET3-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste Neues Gerät die Option Netzwerk aus und klicken Sie auf Hinzufügen.



8. Wählen Sie im Abschnitt Neues Netzwerk aus der Dropdownliste die Netzwerkschnittstelle aus, und führen Sie die folgenden Schritte aus:

   a. Wählen Sie in der Dropdownliste Adaptertyp die Option VMXNET3 aus.

   > **Wichtig:**
   >
   > Die standardmäßige E1000-Netzwerkschnittstelle und VMXNET3 können nicht koexistieren. Stellen Sie sicher, dass Sie die E1000-Netzwerkschnittstelle entfernen und VMXNET3 (0/1) als Verwaltungsschnittstelle verwenden.



9. Klicken Sie auf **OK**.
10. Schalten Sie die NetScaler VPX-Instanz ein.
11. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    ```
    show interface summary
    ```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

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

3         Interface  MTU        MAC                Suffix
4   ---------------------------------------------------------------------------

5   1     0/1        1500       00:0c:29:89:1d:0e  NetScaler Vir...
       rface, VMXNET3
6   2     1/1        9000       00:0c:29:89:1d:18  NetScaler Vir...
       rface, VMXNET3
```



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

> **Hinweis:**
>
> Nachdem Sie eine VMXNET3-Schnittstelle hinzugefügt und die NetScaler VPX Appliance neu gestartet haben, ändert der VMware ESX-Hypervisor möglicherweise die Reihenfolge, in der die NIC der VPX-Appliance angezeigt wird. Daher bleibt der Netzwerkadapter 1 möglicherweise nicht immer 0/1, was zu einem Verlust der Verwaltungskonnektivität mit der VPX-Appliance führt. Um dieses Problem zu vermeiden, ändern Sie das virtuelle Netzwerk des Netzwerkadapters entsprechend.
>
> Dies ist eine Einschränkung des VMware ESX Hypervisors.

Stellen Sie die Empfangsringgröße für die VMXNET3-Netzwerkschnittstelle ein

Sie können die Empfangsringgröße für VMXNET3-Netzwerkschnittstellen auf VMware ESX erhöhen. Eine höhere Ringgröße reduziert die Paketverluste, wenn es zu einem plötzlichen Anstieg des Datenverkehrs kommt.

> **Hinweis:**
>
> Diese Funktion ist in Version 14.1 Build 14.x und höher verfügbar.

So legen Sie die Ringgröße auf einer VMXNET3-Netzwerkschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

set interface *id* [-ringsize *positive_integer*]

Die maximale Ringgröße, die Sie auf einer VMXNET3-Schnittstelle festlegen können, ist 2048. Nur der feste Ringtyp wird unterstützt. Sie müssen die Konfiguration speichern und die NetScaler VPX-Instanz neu starten, damit die Einstellungen wirksam werden.

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

October 17, 2024

Nachdem Sie die NetScaler VPX-Instanz auf VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Webclient verwenden, um die virtuelle Appliance für die Verwendung von Single-Root-I/O-V-Virtualisierungs-Netzwerkschnittstellen (SR-IOV) zu konfigurieren.

Einschränkungen

Für NetScaler VPX, die mit SR-IOV-Netzwerkschnittstelle konfiguriert ist, gelten folgende Einschränkungen:

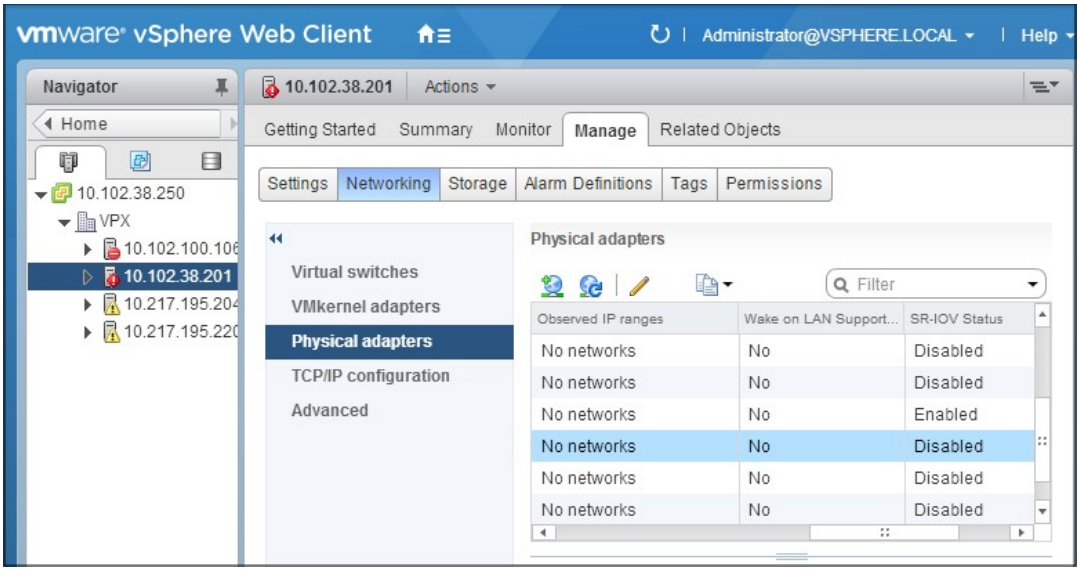
- Die folgenden Funktionen werden auf SR-IOV-Schnittstellen, die die Intel 82599 10G-NIC auf ESX VPX verwenden, nicht unterstützt:
  - L2-Modus Umschaltung
  - Statische Link-Aggregation und LACP
  - Clustering
  - Adminpartitionierung [Freigegebener VLAN-Modus]
  - Hochverfügbarkeit [Aktiv - Aktiver Modus]
  - Jumbo-Rahmen
  - IPv6
- Die folgenden Funktionen werden auf der SR-IOV-Schnittstelle mit einer Intel 82599 10G-NIC auf KVM VPX nicht unterstützt:
  - Statische Link-Aggregation und LACP
  - L2-Modus Umschaltung
  - Clustering
  - Adminpartitionierung [Freigegebener VLAN-Modus]
  - Hochverfügbarkeit [Aktiv —Aktiver Modus]
  - Jumbo-Rahmen
  - IPv6
  - Die VLAN-Konfiguration auf Hypervisor für SR-IOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt

Voraussetzung

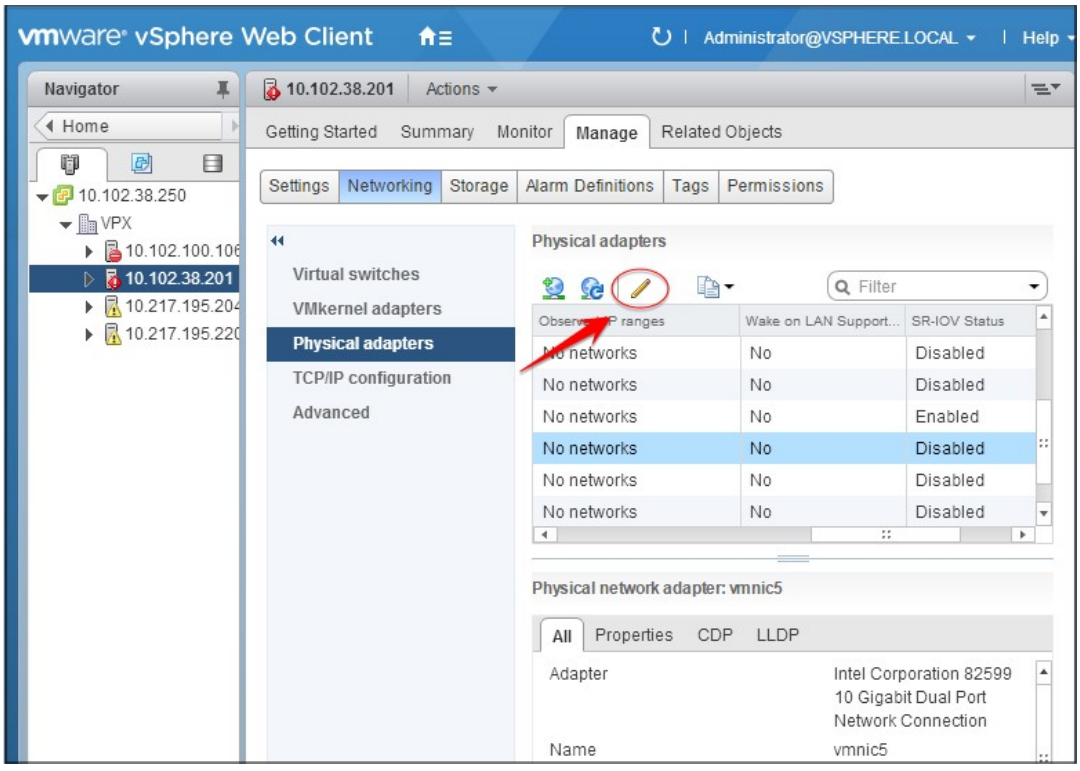
- Stellen Sie sicher, dass Sie dem ESX-Host eine der folgenden Netzwerkkarten hinzufügen:
  - Intel 82599 NIC, IXGBE-Treiberversion 3.7.13.7.14iov oder höher wird empfohlen.
  - Mellanox ConnectX-4 NIC
- Aktivieren Sie SR-IOV auf dem physischen Hostadapter.

  Gehen Sie wie folgt vor, um SR-IOV auf dem physischen Hostadapter zu aktivieren:

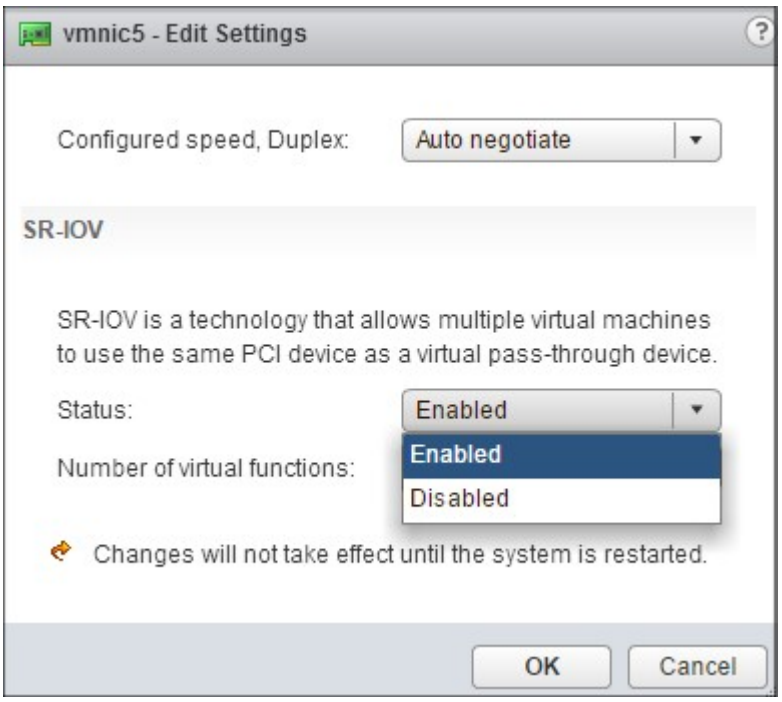
1. Navigieren Sie im vSphere Web Client zum Host.
2. Wählen Sie auf der Registerkarte **Verwalten > Netzwerk** die Option **Physische Adapter** aus. Das Feld SR-IOV Status zeigt an, ob ein physischer Adapter SR-IOV unterstützt.



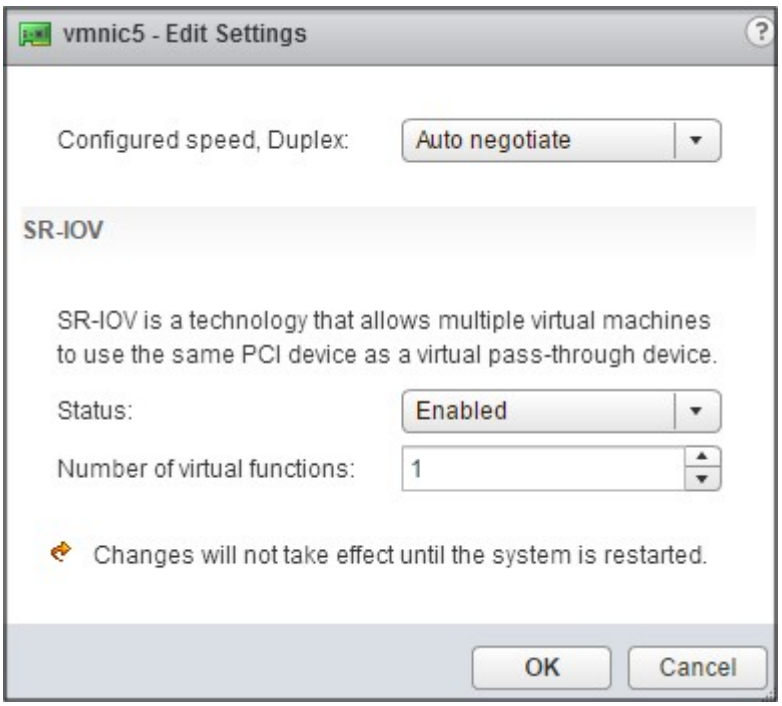
3. Wählen Sie den physischen Adapter aus, und klicken Sie dann auf das Stiftsymbol, um das Dialogfeld **Einstellungen bearbeiten** zu öffnen.



4. Wählen Sie unter SR-IOV in der Dropdownliste **Status** die Option **Aktiviert** aus.



5. Geben Sie im Feld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen ein, die Sie für den Adapter konfigurieren möchten.



6. Klicken Sie auf **OK**.
7. Starten Sie den Host neu.

- Erstellen Sie einen Distributed Virtual Switch (DVS) und `Portgroups`. Anweisungen finden Sie

in der VMware Dokumentation.

> **Hinweis:**
>
> Citrix hat die SR-IOV-Konfiguration `Portgroups` nur auf DVS qualifiziert.

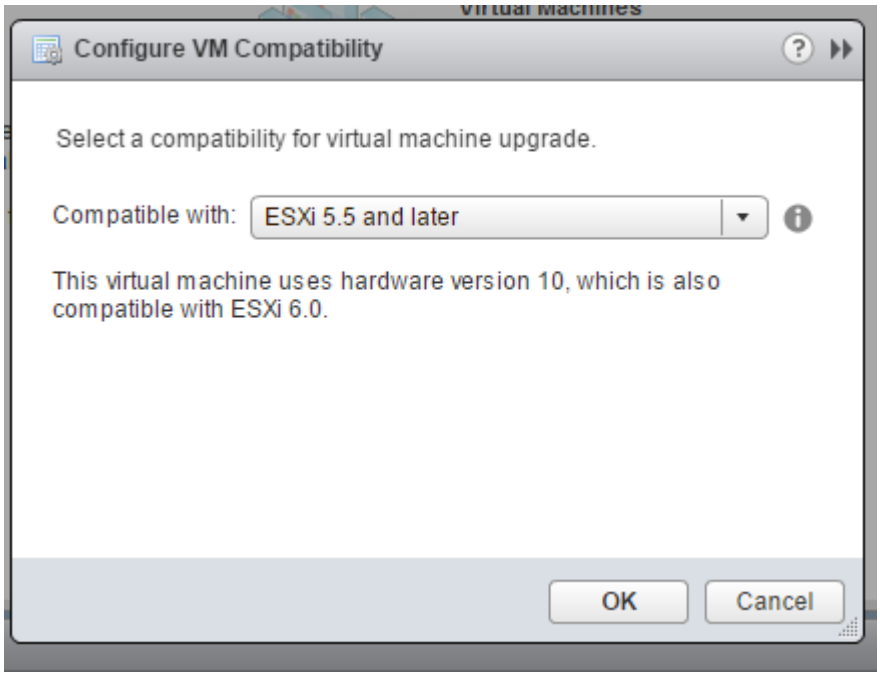
So konfigurieren Sie NetScaler VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle mithilfe von VMware vSphere Web Client:

1. Wählen Sie im vSphere Web Client **Hosts und Cluster**aus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz wie folgt auf ESX 5.5 oder höher:

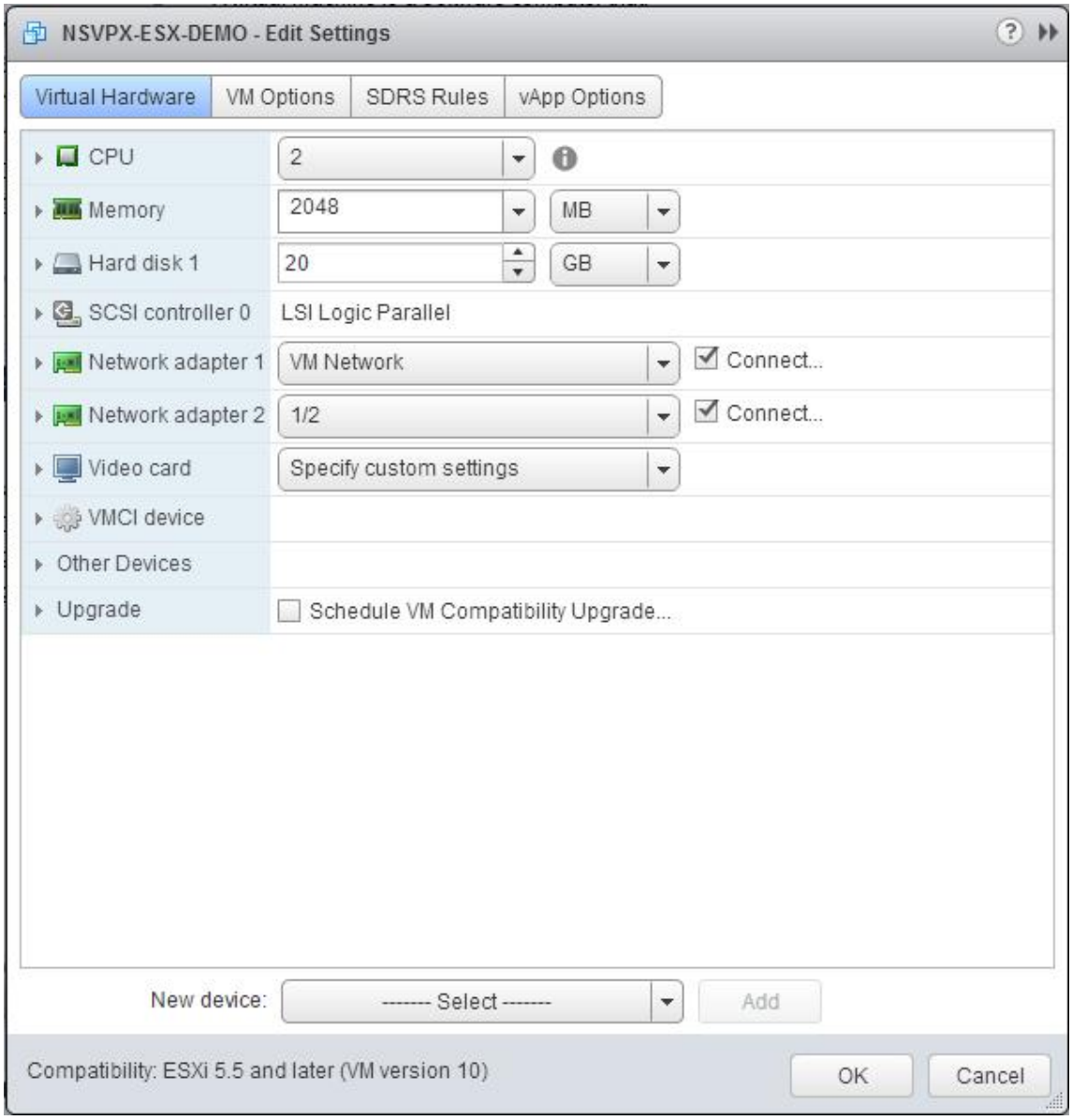
   a. Schalten Sie die NetScaler VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie **Kompatibilität > VM-Kompatibilität aktualisieren**.

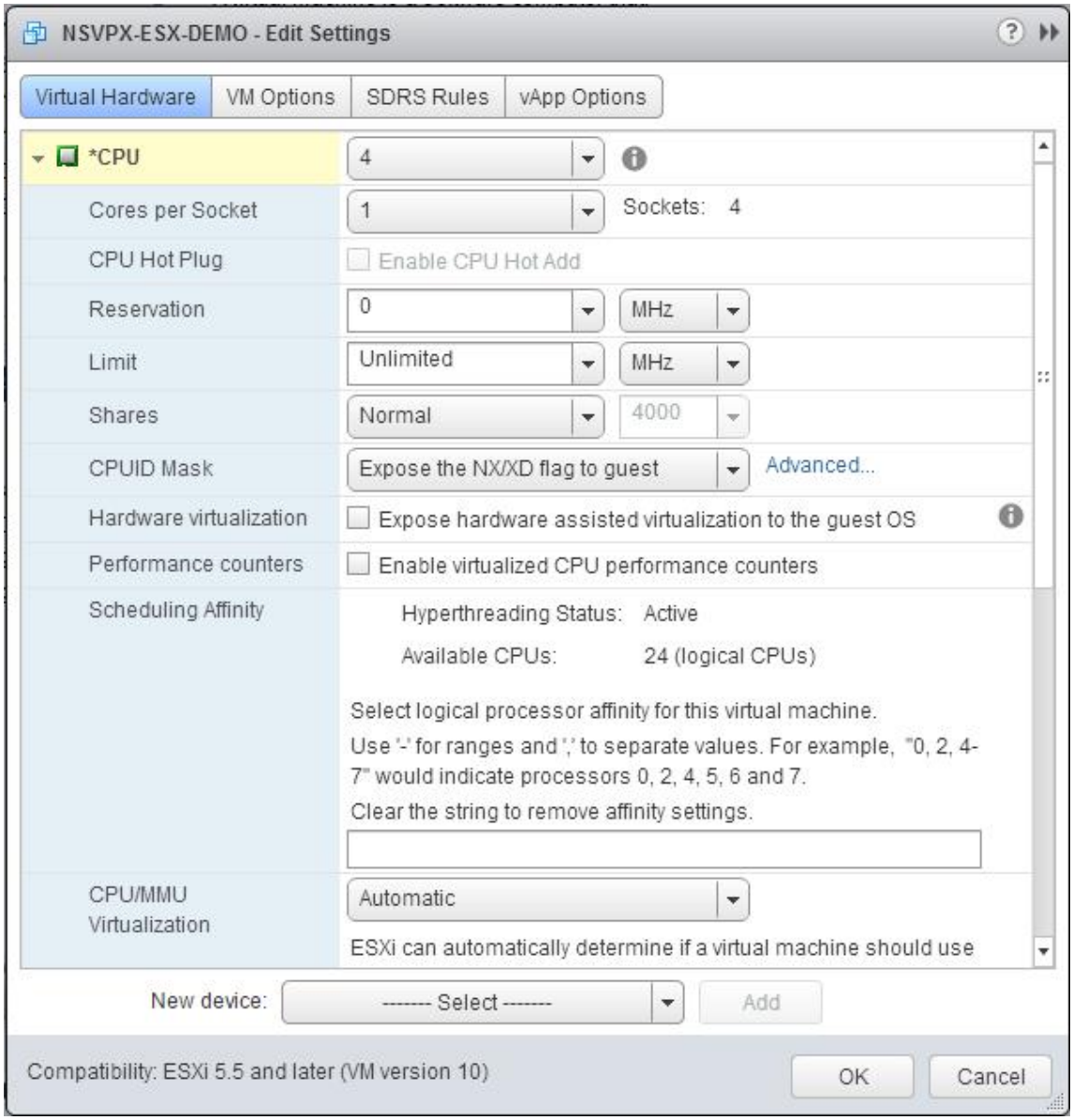
   c. Wählen Sie im Dialogfeld **VM-Kompatibilität konfigurieren** die Option **ESXi 5.5 und höher** aus der Dropdownliste **Kompatibel mit** aus, und klicken Sie auf **OK**.



3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX Instanz, und klicken Sie auf **Einstellungen bearbeiten**.



4. Klicken Sie im Dialogfeld **<virtual_appliance> - Einstellungen bearbeiten** auf den Abschnitt **CPU**.



5. Aktualisieren Sie im Abschnitt **CPU** die folgenden Einstellungen:

   - CPU-Anzahl
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

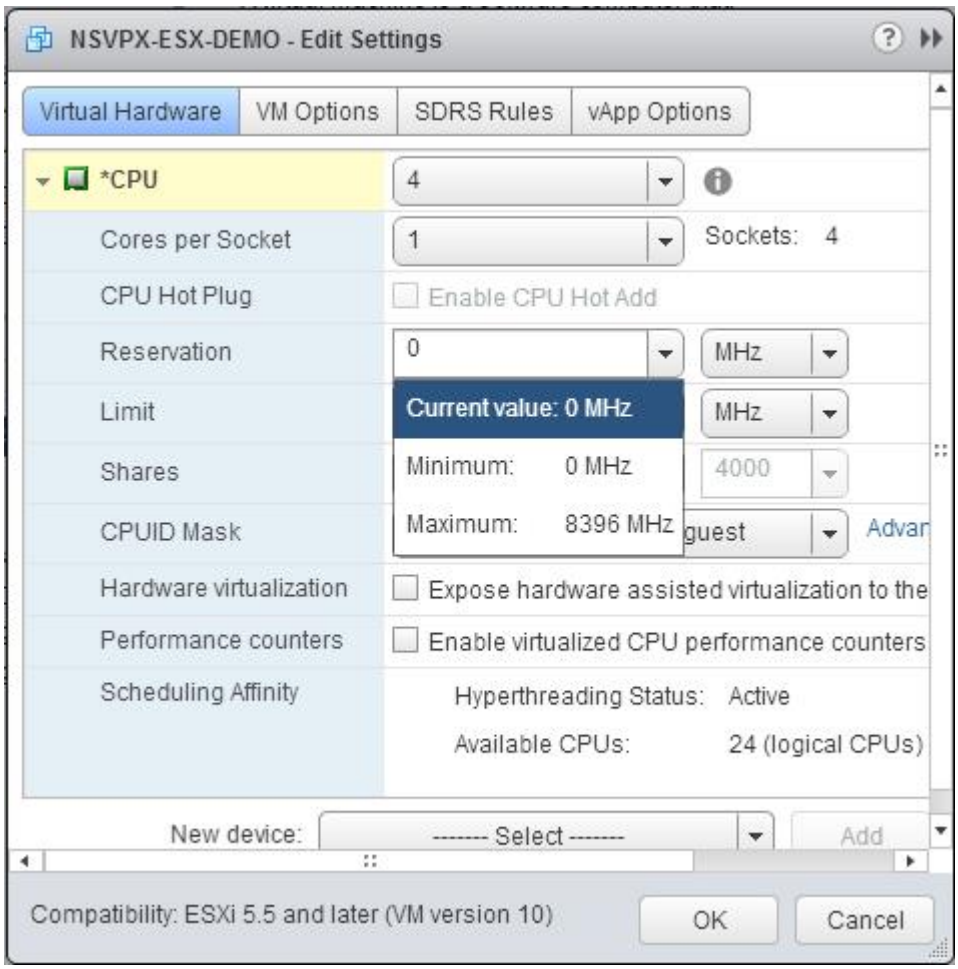
   a. Wählen Sie in der Dropdownliste **CPU** die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste **Kerne pro Sockel** die Anzahl der Sockets aus.

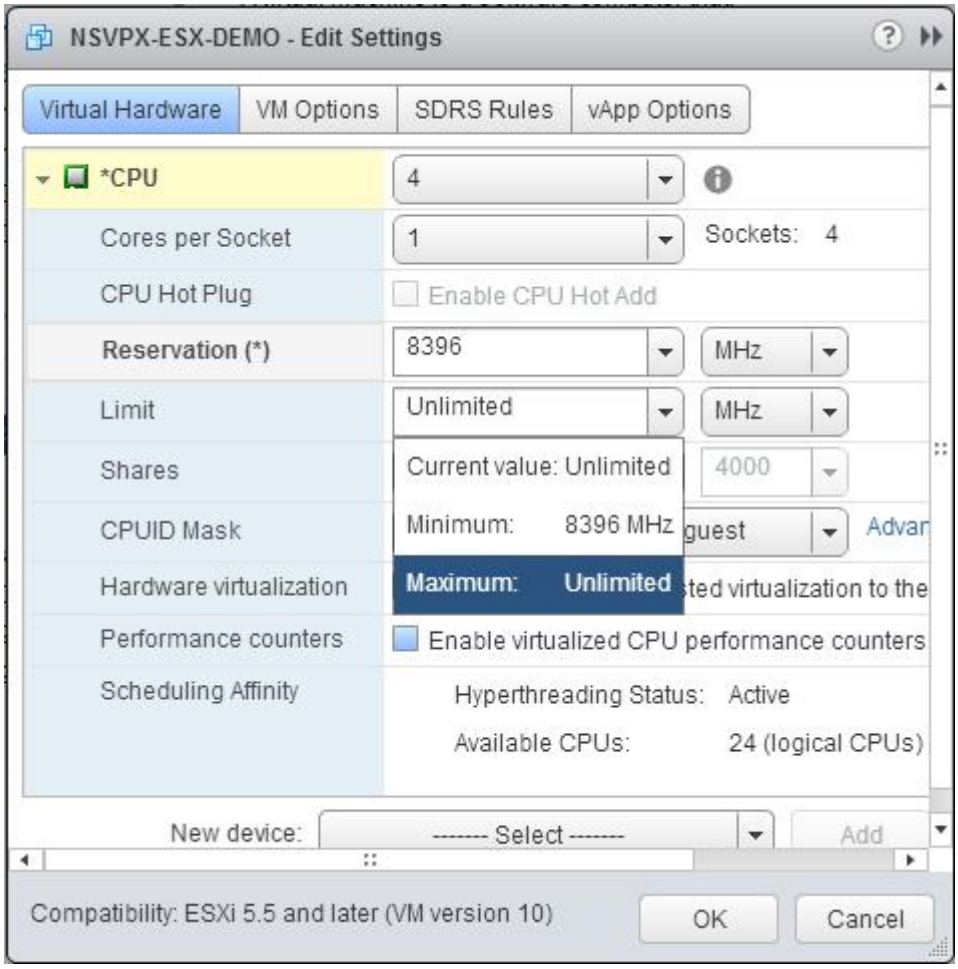
c. (Optional) Aktivieren oder deaktivieren Sie im Feld **CPU Hot Plug** das Kontrollkästchen **CPU Hot Add aktivieren** .

> **Hinweis:**
>
> Citrix empfiehlt, die Standardeinstellung (deaktiviert) zu akzeptieren.

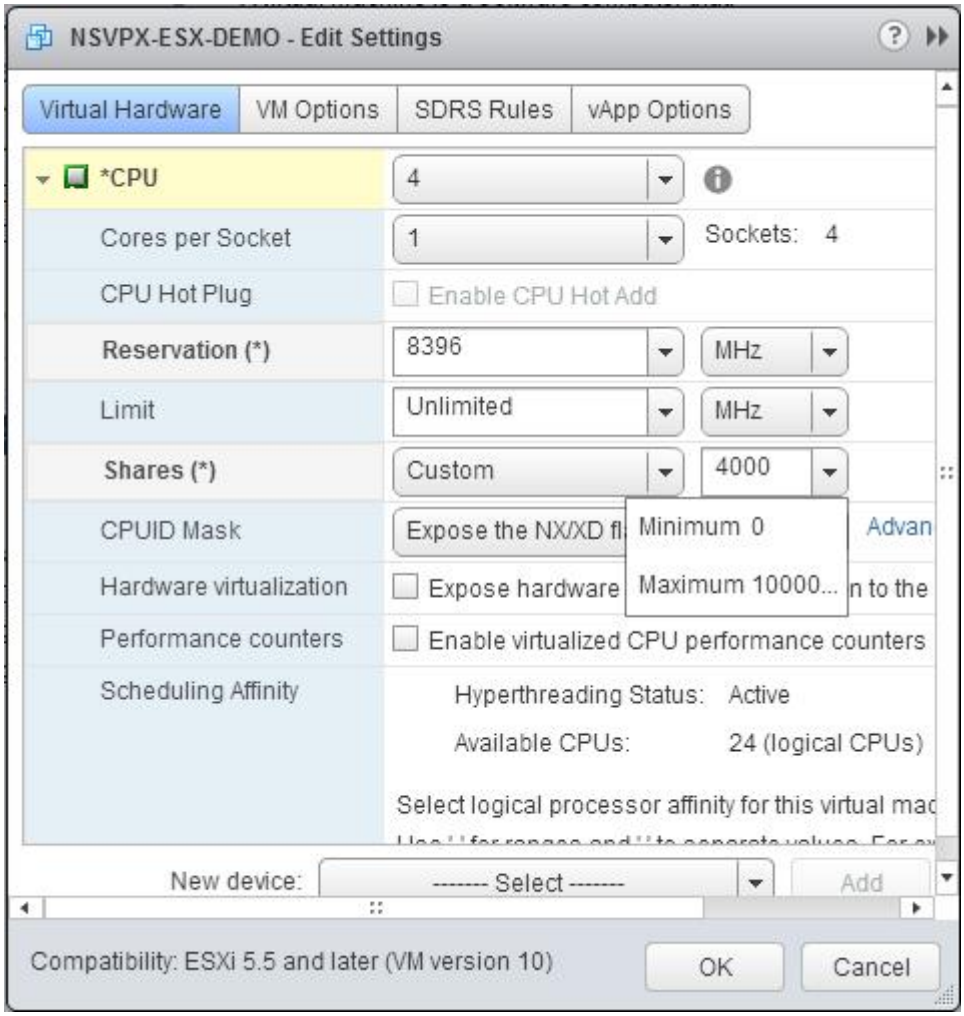
d. Wählen Sie in der Dropdownliste **Reservierung** die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten **Freigaben** die Option **Benutzerdefiniert** und die Zahl, die als Maximalwert angezeigt wird.



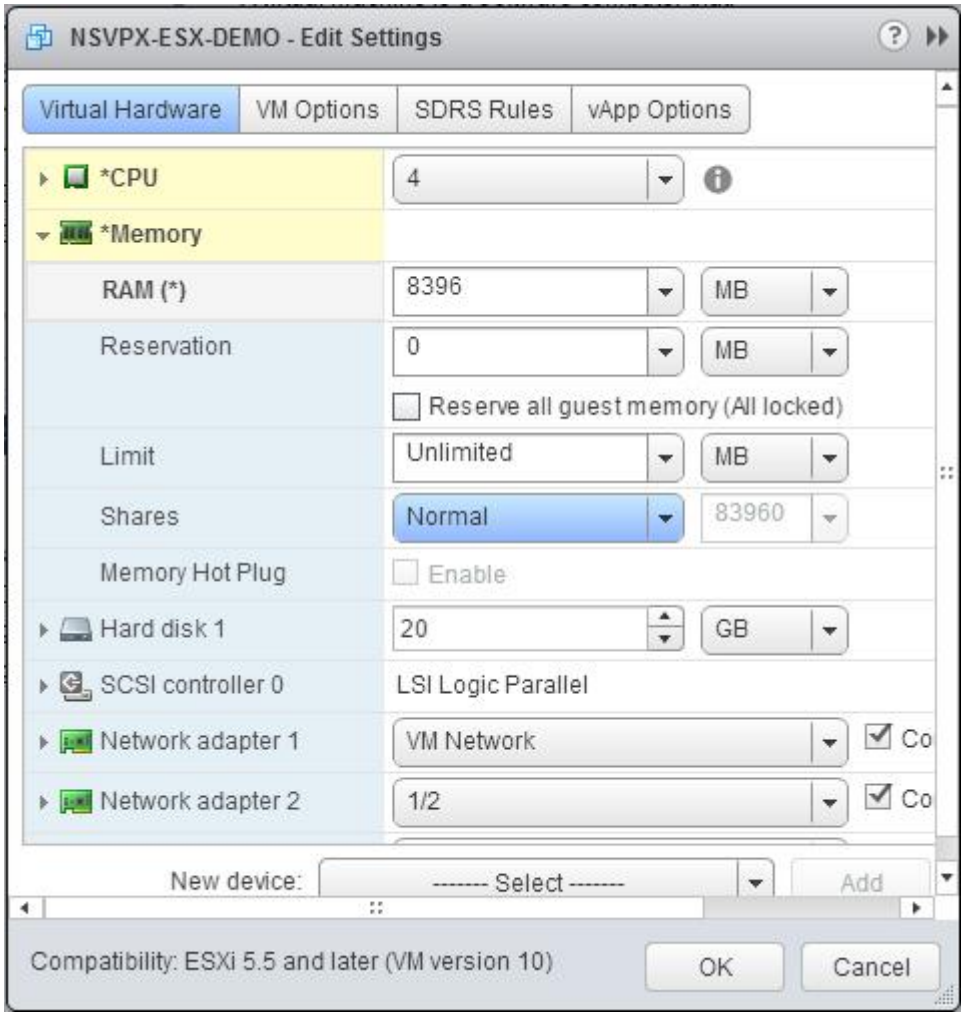
6. Aktualisieren Sie im Abschnitt **Speicher** die folgenden Einstellungen:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

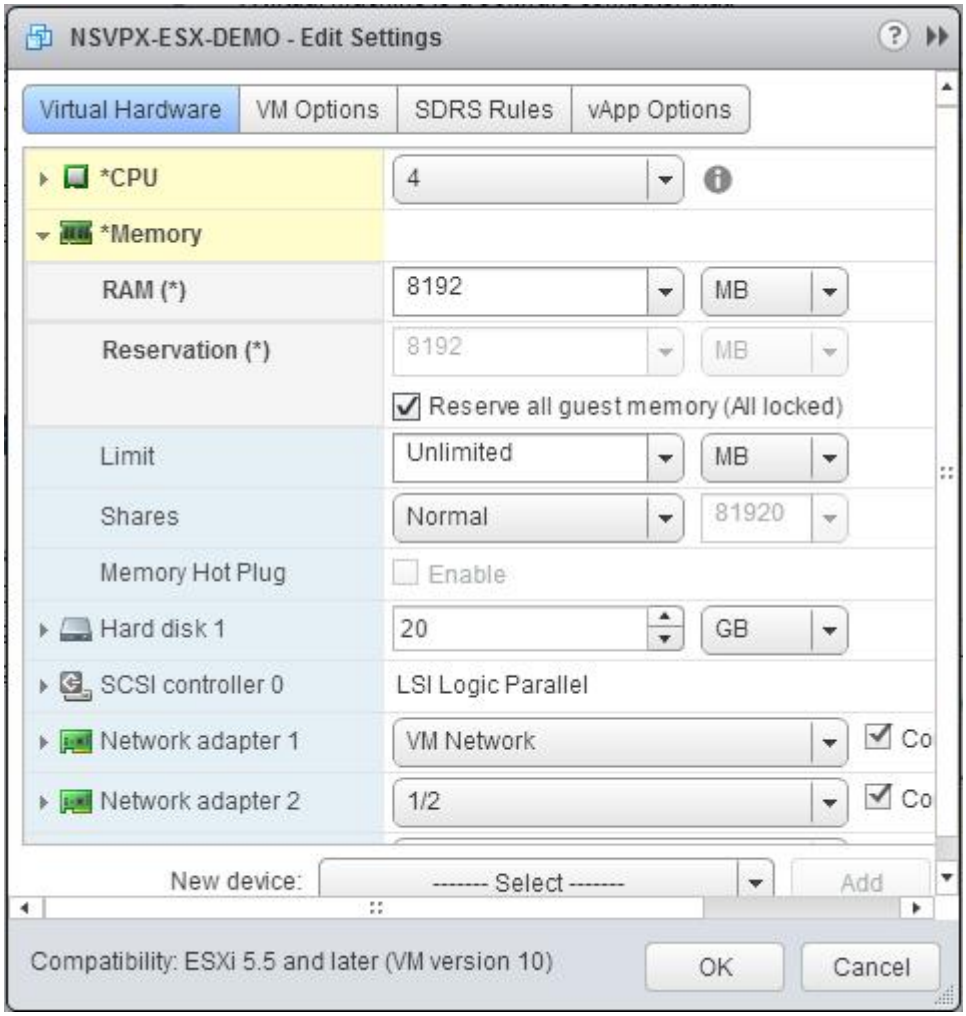
   a. Wählen Sie in der Dropdownliste **RAM** die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 2 GB = 8 GB.

   > **Hinweis:**
   >
   > Stellen Sie bei der Advanced- oder Premium-Edition des NetScaler VPX-Geräts sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

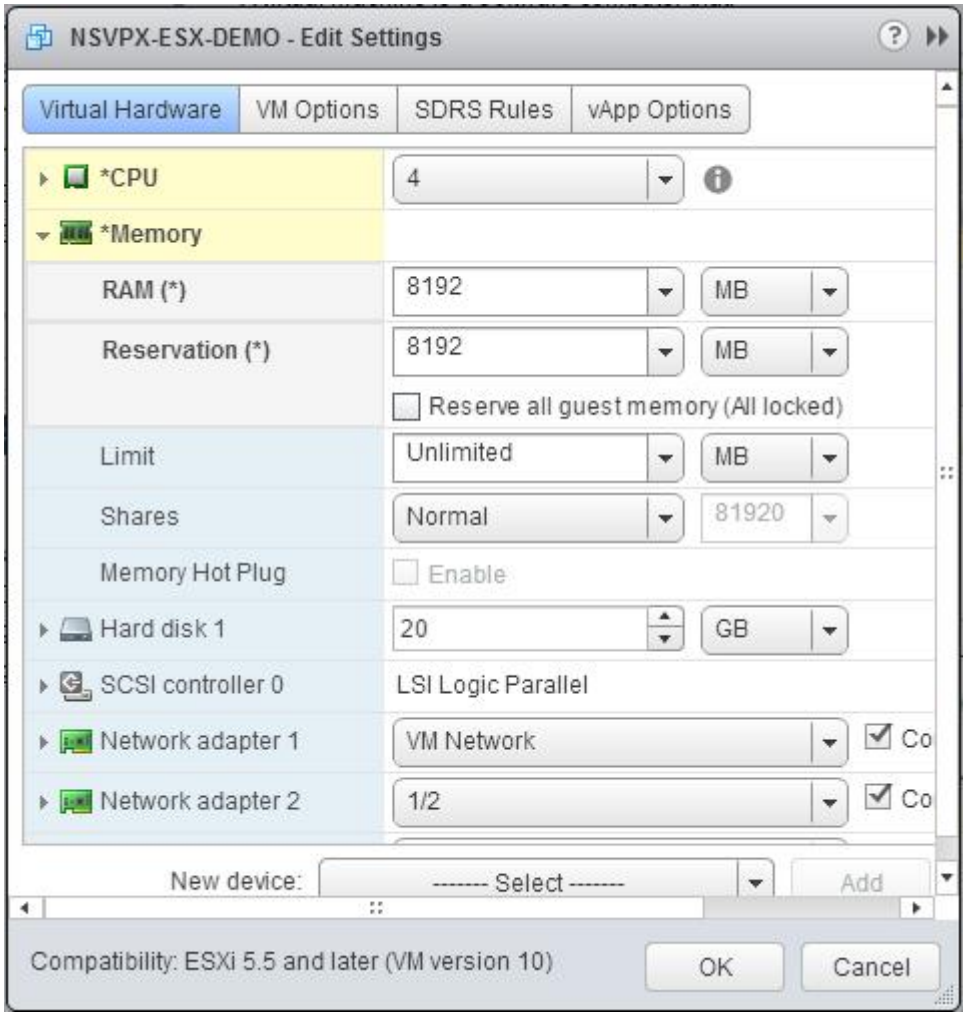


b. Geben Sie in der Dropdownliste **Reservierung** den Wert für die Speicherreservierung ein, und aktivieren Sie das Kontrollkästchen **Alle Gastspeicher reservieren (Alle gesperrt)** . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

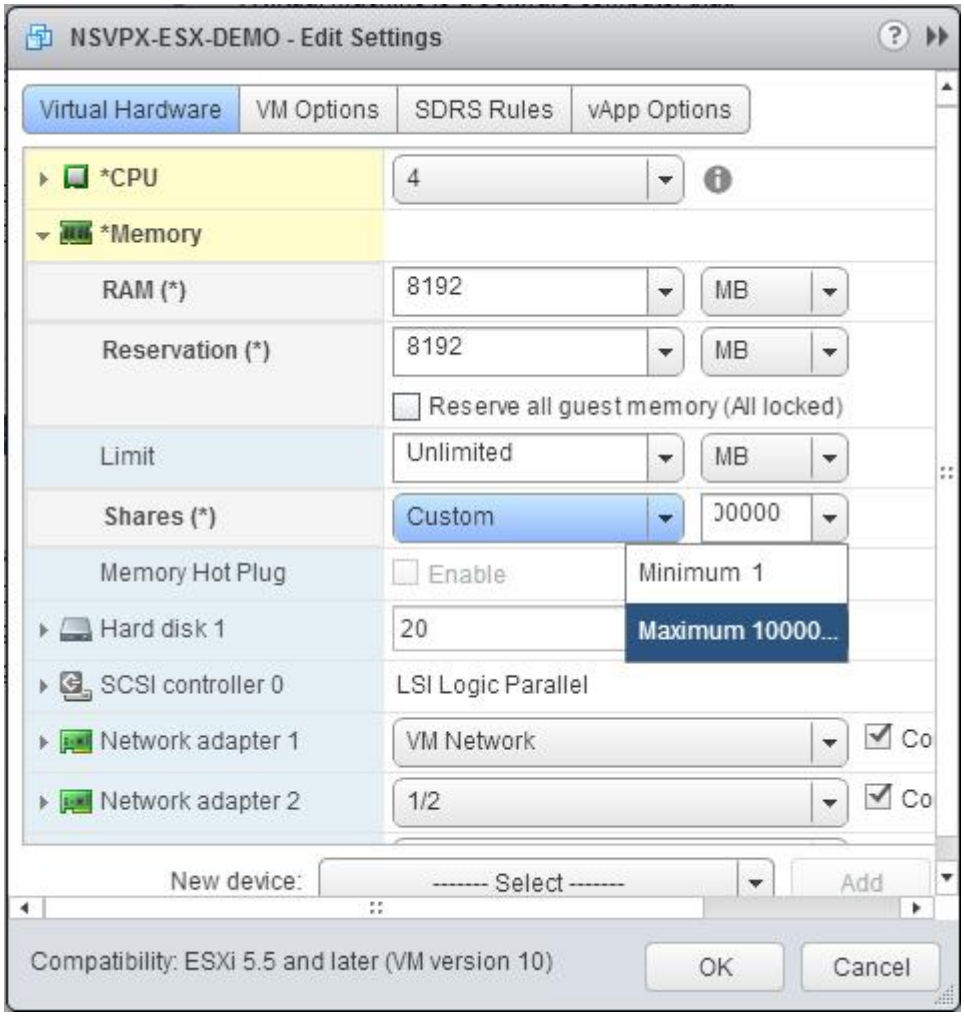
> **Hinweis:**
>
> Stellen Sie bei der Advanced- oder Premium-Edition des NetScaler VPX-Geräts sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



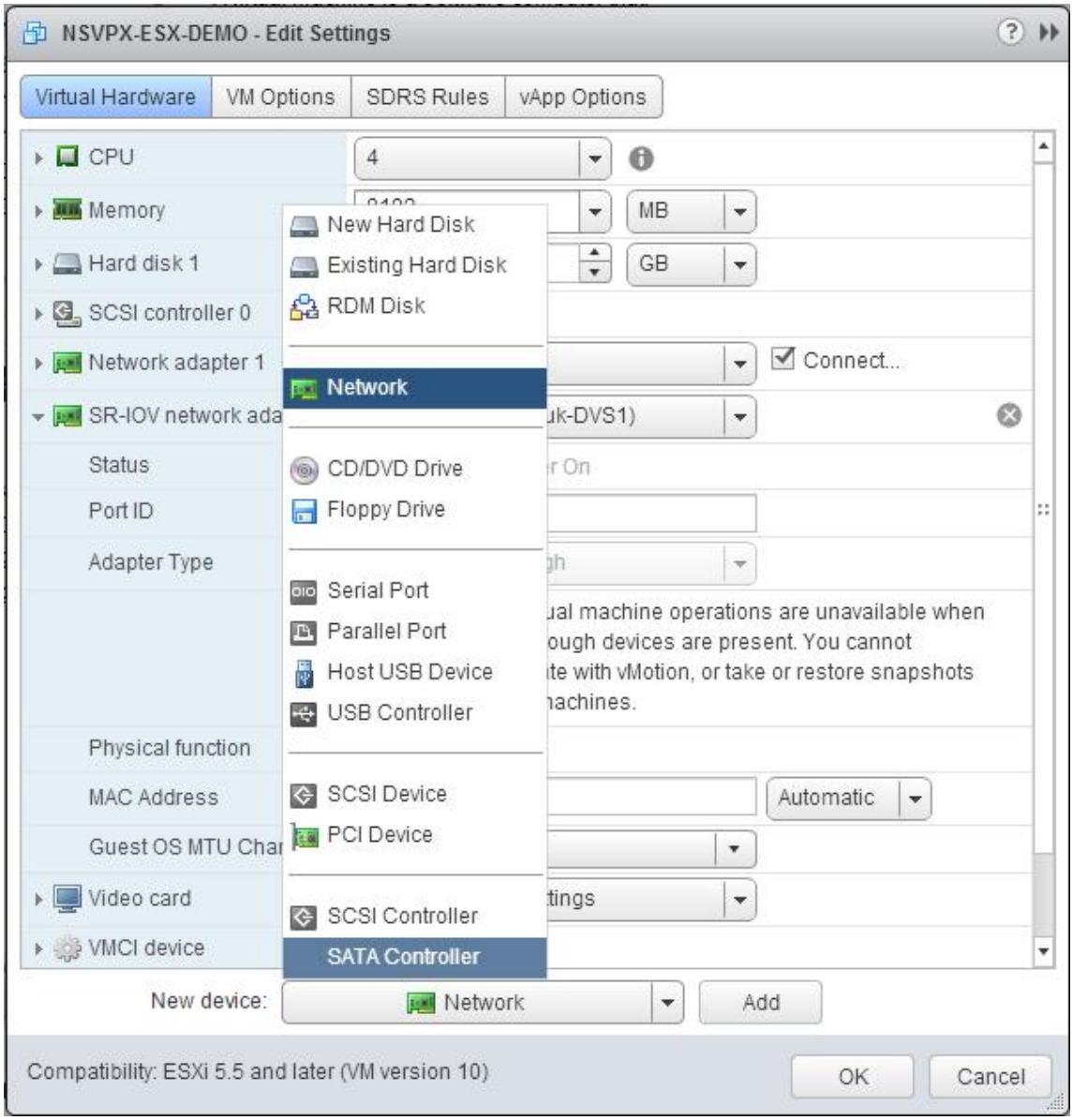
c. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten **Freigaben** die Option **Benutzerdefiniert** aus, und wählen Sie die Zahl aus, die als Maximalwert angezeigt wird.

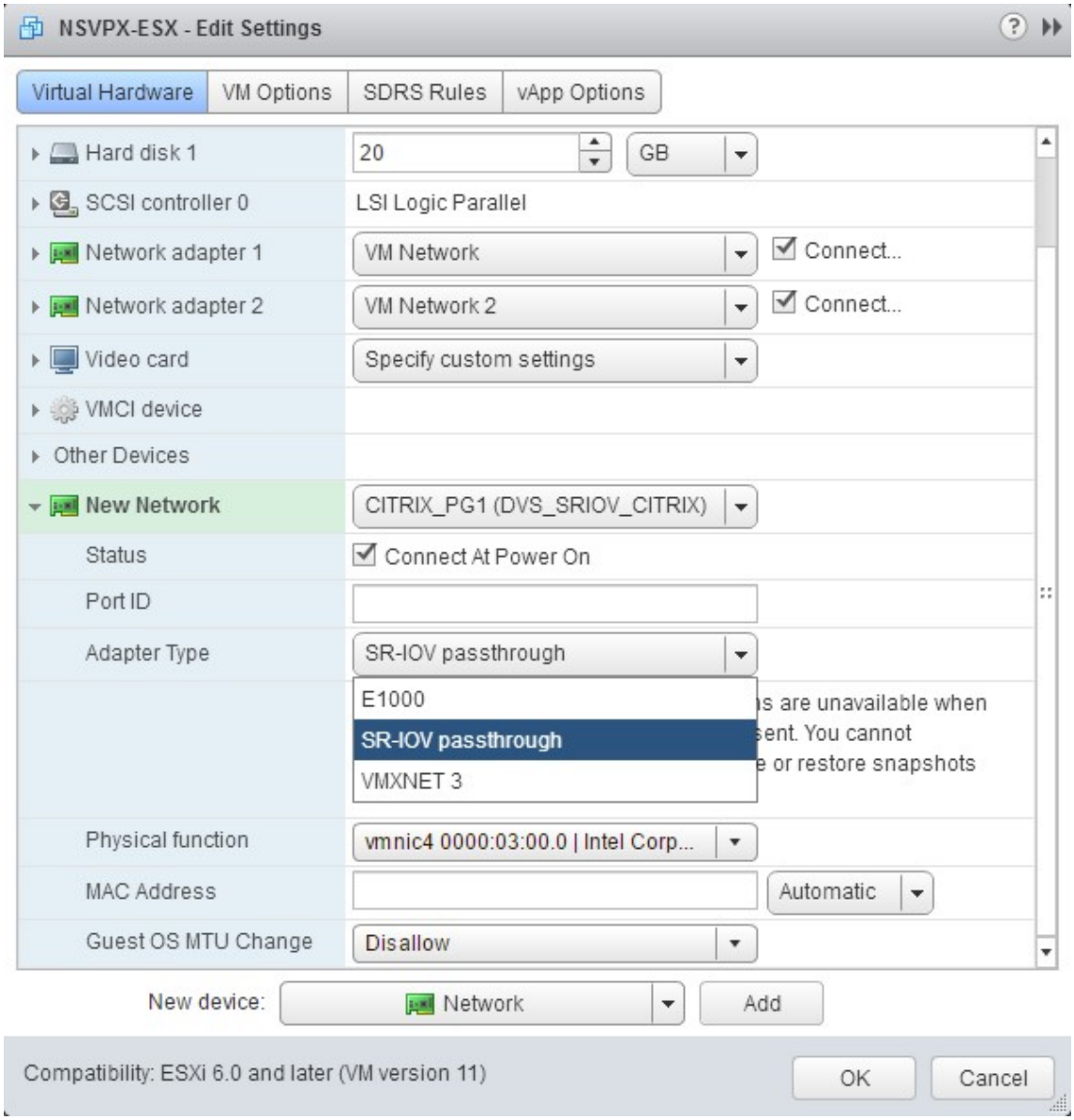


7. Fügen Sie eine SR-IOV-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste **Neues Gerät** die Option **Netzwerk** aus und klicken Sie auf **Hinzufügen**.

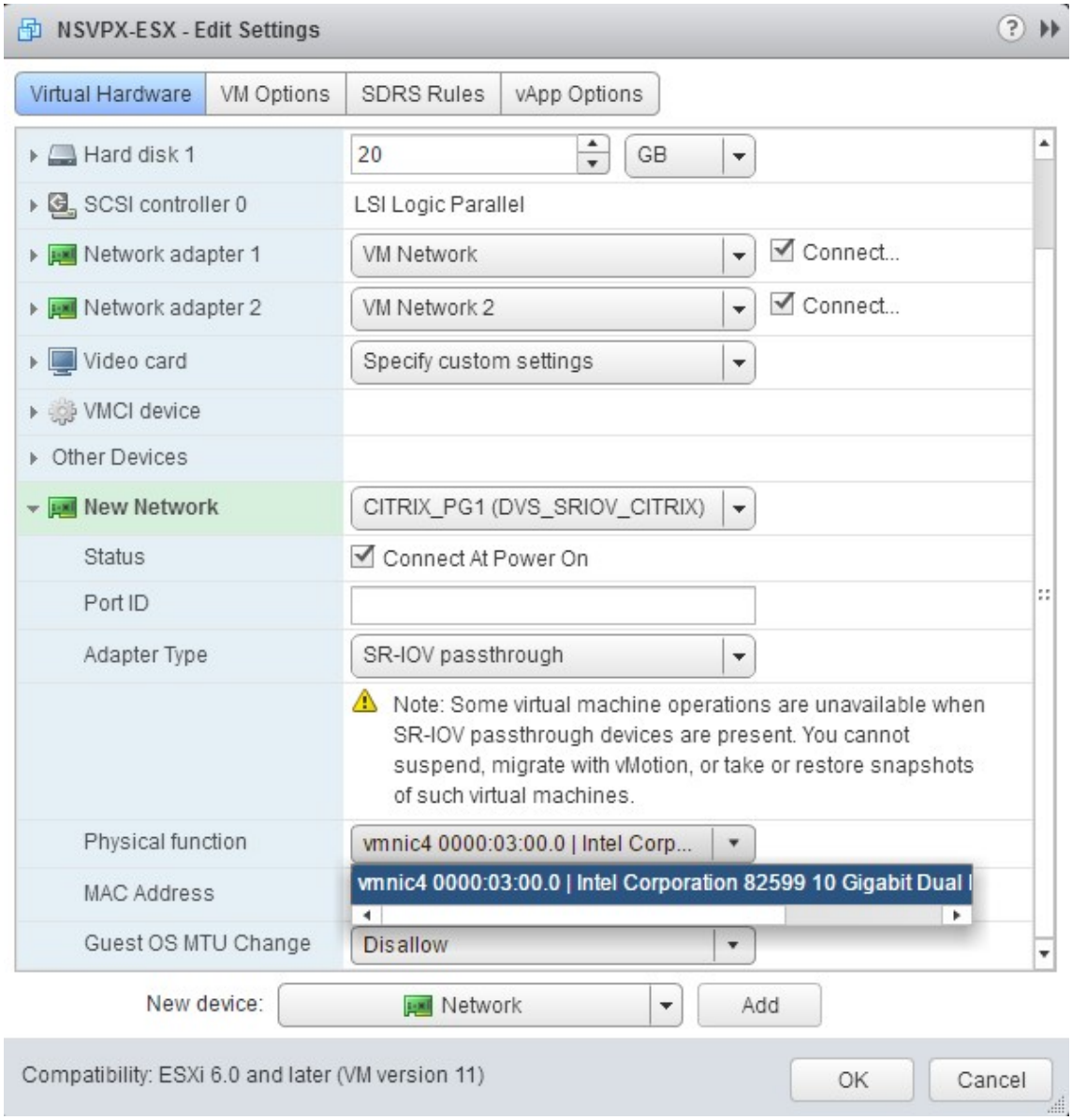


8. Im Abschnitt **Neues Netzwerk**. Wählen Sie in der Dropdownliste `Portgroup` das von Ihnen erstellte aus, und gehen Sie wie folgt vor:

   a. Wählen Sie in der Dropdownliste **Adaptertyp** die Option **SR-IOV-Passthrough** aus.

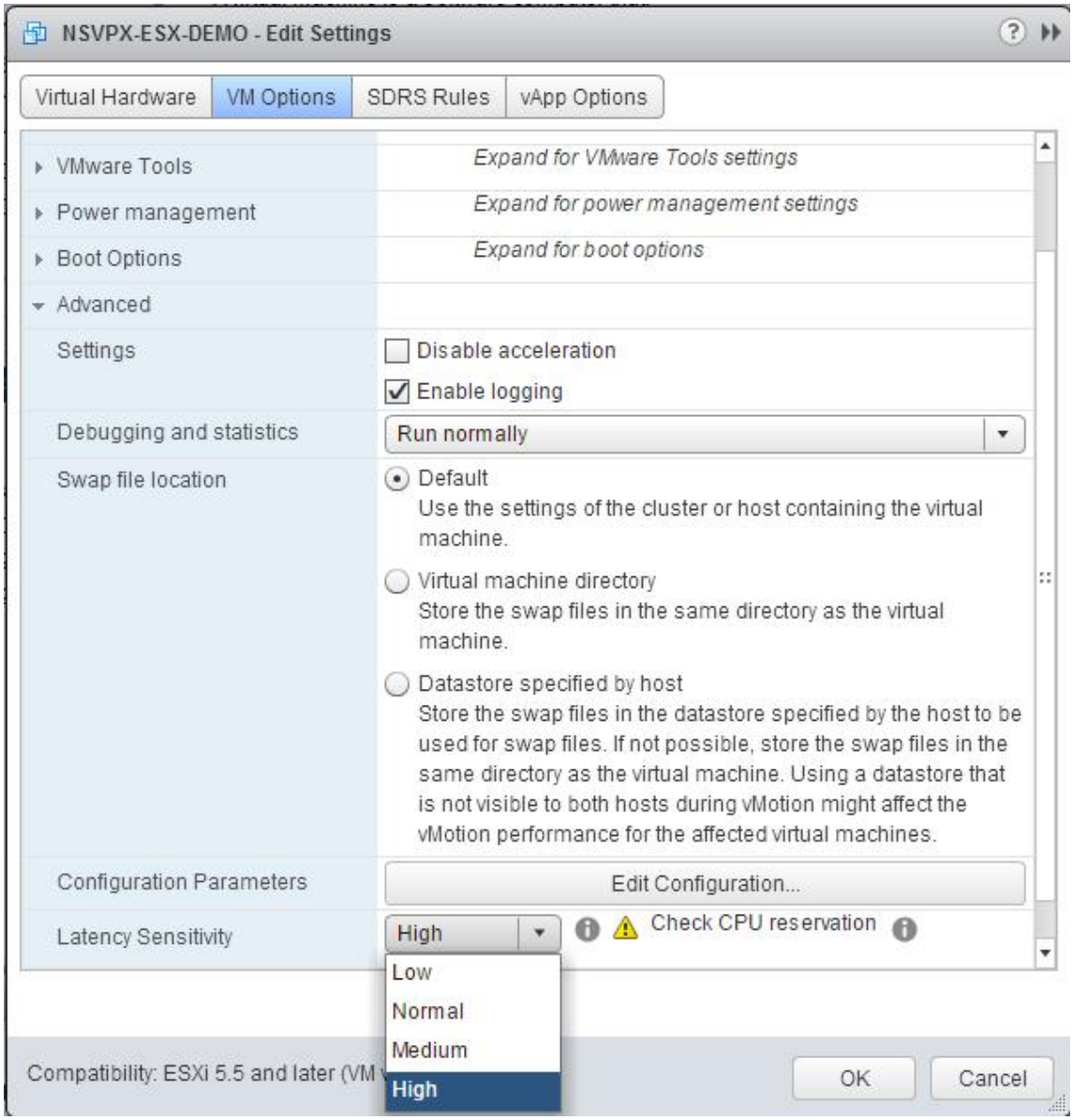


b. Wählen Sie in der Dropdownliste **Physische Funktion** den physischen Adapter aus, der dem zugeordnet ist `Portgroup`.



c. Wählen Sie in der Dropdownliste **Gastbetriebssystem-MTU-Änderung** die Option **Verbieten** aus.

9. Klicken Sie im <virtual_appliance> Dialogfeld **- Einstellungen bearbeiten** auf die Registerkarte **VM-Optionen**.
10. Wählen Sie auf der Registerkarte **VM-Optionen** den Abschnitt **Erweitert** aus. Wählen Sie in der Dropdownliste **Latenzempfindlichkeit** die Option **Hoch** aus.



11. Klicken Sie auf **OK**.
12. Schalten Sie die NetScaler VPX-Instanz ein.
13. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    ```
    show interface summary
    ```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

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



```
---------------------------------------------------------------------------

1     0/1         1500       00:0c:29:1b:81:0b    NetScaler Virtual
   Interface
2     10/1        1500       00:50:56:9f:0c:6f    Intel 82599 10G VF
   Interface
3     10/2        1500       00:50:56:9f:5c:1e    Intel 82599 10G VF
   Interface
4     10/3        1500       00:50:56:9f:02:1b    Intel 82599 10G VF
   Interface
5     10/4        1500       00:50:56:9f:5a:1d    Intel 82599 10G VF
   Interface
6     10/5        1500       00:50:56:9f:4e:0b    Intel 82599 10G VF
   Interface
7     LO/1        1500       00:0c:29:1b:81:0b    Netscaler Loopback
   interface
 Done
> show inter 10/1
1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
        flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
        MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
           h21m53s
        Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
           throughput 10000
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
           Stalls(0)
        TX: Pkts(838149954) Bytes(860895860507) 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
```

Konfigurieren Sie einen NetScaler VPX auf dem ESX-Hypervisor, um Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus zu verwenden

October 17, 2024

Die NetScaler VPX-Instanz auf dem VMware ESX-Hypervisor kann die Intel QuickAssist-Technologie (QAT) verwenden, um die NetScaler SSL-Leistung zu beschleunigen. Mithilfe von Intel QAT kann die gesamte Kryptoverarbeitung mit hoher Latenz auf den Chip verlagert werden, sodass eine oder mehrere Host-CPUs für andere Aufgaben frei werden.

Zuvor wurde die gesamte Kryptoverarbeitung von NetScaler-Datenpfaden in der Software mithilfe von Host-vCPUs durchgeführt.

> **Hinweis:**
>
> Derzeit unterstützt NetScaler VPX nur das C62x-Chipmodell der Intel QAT-Familie. Diese Funktion wird ab NetScaler Version 14.1 Build 8.50 unterstützt.

Voraussetzungen

- Der ESX-Host ist mit einem oder mehreren Intel C62x (QAT)-Chips ausgestattet.
- NetScaler VPX erfüllt die VMware ESX-Hardwareanforderungen. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz auf VMware ESX.

Einschränkungen

Es ist nicht vorgesehen, Kryptoeinheiten oder Bandbreite für einzelne VMs zu reservieren. Alle verfügbaren Kryptoeinheiten jeder Intel QAT-Hardware werden von allen VMs gemeinsam genutzt, die die QAT-Hardware verwenden.

Richten Sie die Host-Umgebung für die Verwendung von Intel QAT ein

1. Laden Sie den von Intel bereitgestellten VMware-Treiber für das Chipmodell der C62x-Serie (QAT) herunter und installieren Sie ihn auf dem VMware-Host. Weitere Informationen zu den Intel Paket-Downloads und Installationsanweisungen finden Sie unter Intel QuickAssist-Technologie-Treiber für VMware.
2. Aktivieren Sie SR-IOV auf dem ESX-Host.
3. Erstellen Sie virtuelle Maschinen. Weisen Sie beim Erstellen einer VM die entsprechende Anzahl von PCI-Geräten zu, um die Leistungsanforderungen zu erfüllen.

> **Hinweis:**
>
> Jeder C62x (QAT) -Chip kann bis zu drei separate PCI-Endpunkte haben. Jeder Endpunkt ist eine logische Sammlung von VFs und teilt sich die Bandbreite zu gleichen Teilen mit anderen PCI-Endpunkten des Chips. Jeder Endpunkt kann bis zu 16 VFs haben, die als 16 PCI-Geräte angezeigt werden. Sie können diese Geräte zur VM hinzufügen, um die Kryptobeschleunigung mithilfe des QAT-Chips durchzuführen.

Punkte zu beachten

- Wenn die VM-Kryptoanforderung darin besteht, mehr als einen QAT-PCI-Endpunkt/-Chip zu verwenden, wird empfohlen, die entsprechenden PCI-Geräte/VFs nach dem Round-Robin-Verfahren auszuwählen, um eine symmetrische Verteilung zu erhalten.

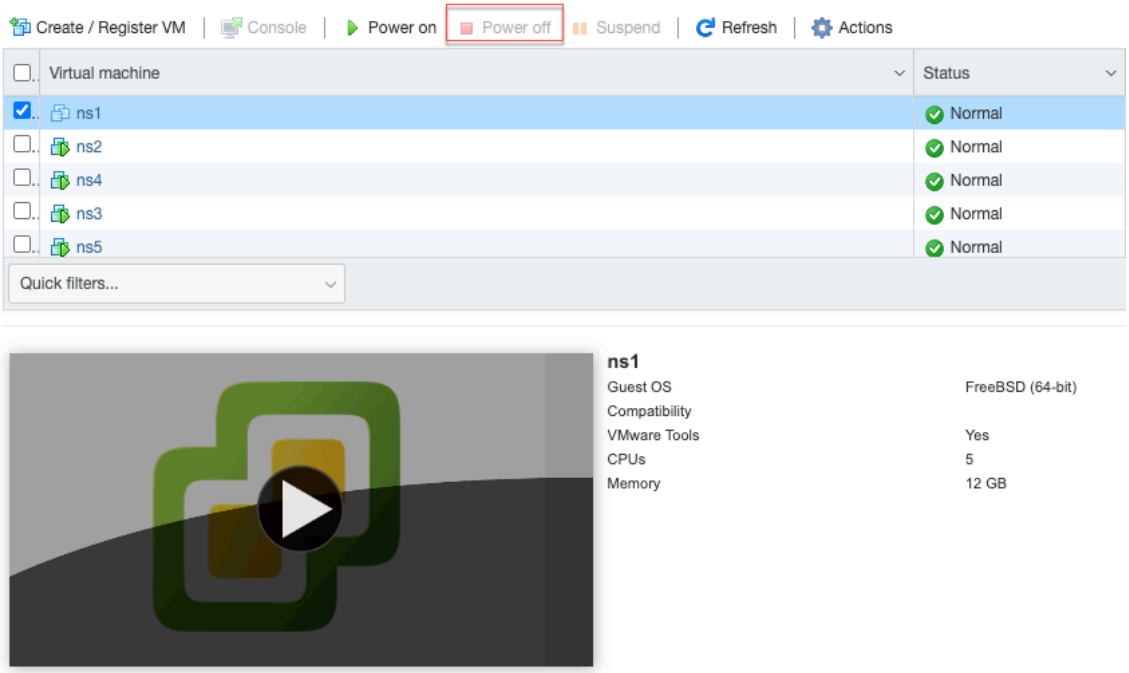
- Es wird empfohlen, dass die Anzahl der ausgewählten PCI-Geräte der Anzahl der lizenzierten vCPUs entspricht (ohne die Anzahl der Management-vCPUs). Das Hinzufügen von mehr PCI-Geräten als die verfügbare Anzahl an vCPUs verbessert nicht unbedingt die Leistung.

  Beispiel

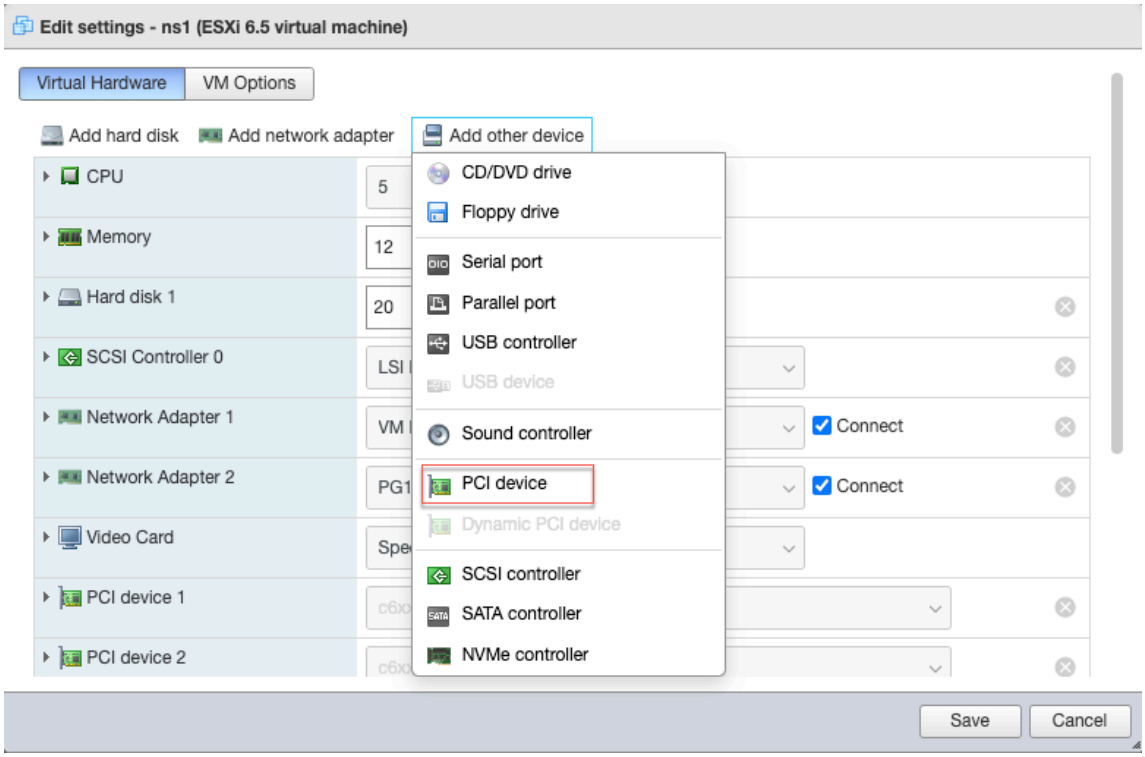
  Stellen Sie sich einen ESX-Host mit einem Intel C62x-Chip vor, der über 3 Endpunkte verfügt. Wählen Sie bei der Bereitstellung einer VM mit 6 vCPUs 2 VFs von jedem Endpunkt aus und weisen Sie sie der VM zu. Diese Art der Zuweisung gewährleistet eine effektive und gleichmäßige Verteilung der Kryptoeinheiten für die VM. Von den insgesamt verfügbaren vCPUs ist standardmäßig eine vCPU für die Managementebene reserviert, und die übrigen vCPUs sind für die PEs der Datenebene verfügbar.

Weisen Sie VPX mithilfe des vSphere Web Client QAT-VFs zu

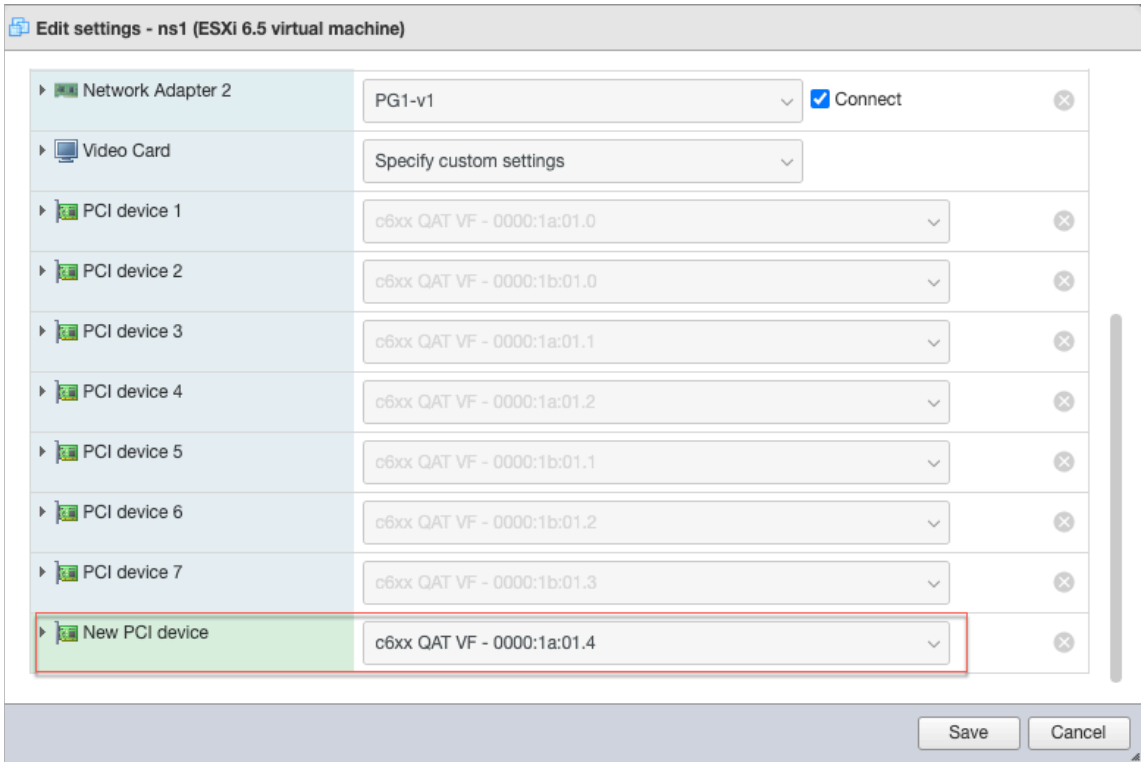
1. Navigieren Sie im vSphere Web Client zum ESX-Host, auf dem sich die virtuelle Maschine befindet, und klicken Sie auf **Ausschalten**.



2. Navigieren Sie zu **Aktionen > Einstellungen bearbeiten > Anderes Gerät hinzufügen**und wählen Sie PCI-Gerät aus.



3. Weisen Sie dem neu hinzugefügten PCI-Gerät den c6xx QAT VF zu und speichern Sie die Konfiguration.



4. Schalten Sie die VM erneut ein.

5. Führen Sie den Befehl `stat ssl` in der NetScaler-CLI aus, um die SSL-Zusammenfassung anzuzeigen, und überprüfen Sie die SSL-Karten, nachdem Sie VPX QAT-VFs zugewiesen haben.

Über den Einsatz

Diese Bereitstellung wurde mit den folgenden Komponentenspezifikationen getestet:

- **NetScaler VPX Version und Build:** 14.1-8.50
- **VMware ESXi Version:** 7.0.3 (Build 20036589)
- **Intel C62x QAT-Treiberversion für VMware** : 1.5.1.54

Migration des NetScaler VPX von E1000 auf SR-IOV- oder VMXNET3-Netzwerkschnittstellen

October 17, 2024

24. Mai 2018

Sie können Ihre beendenden NetScaler VPX-Instanzen, die E1000 Netzwerkschnittstellen verwenden, so konfigurieren, dass SR-IOV- oder VMXNET3-Netzwerkschnittstellen verwendet werden.

Informationen zum Konfigurieren einer vorhandenen NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle.

Informationen zum Konfigurieren einer vorhandenen NetScaler VPX-Instanz zur Verwendung von VMXNET3-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der VMXNET3-Netzwerkschnittstelle.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der PCI-Passthrough-Netzwerkschnittstelle

October 17, 2024

Übersicht

Nachdem Sie eine NetScaler VPX-Instanz auf VMware ESX Server installiert und konfiguriert haben, können Sie den vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

Die PCI-Passthrough-Funktion ermöglicht einem virtuellen Gastcomputer den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind.

Voraussetzungen

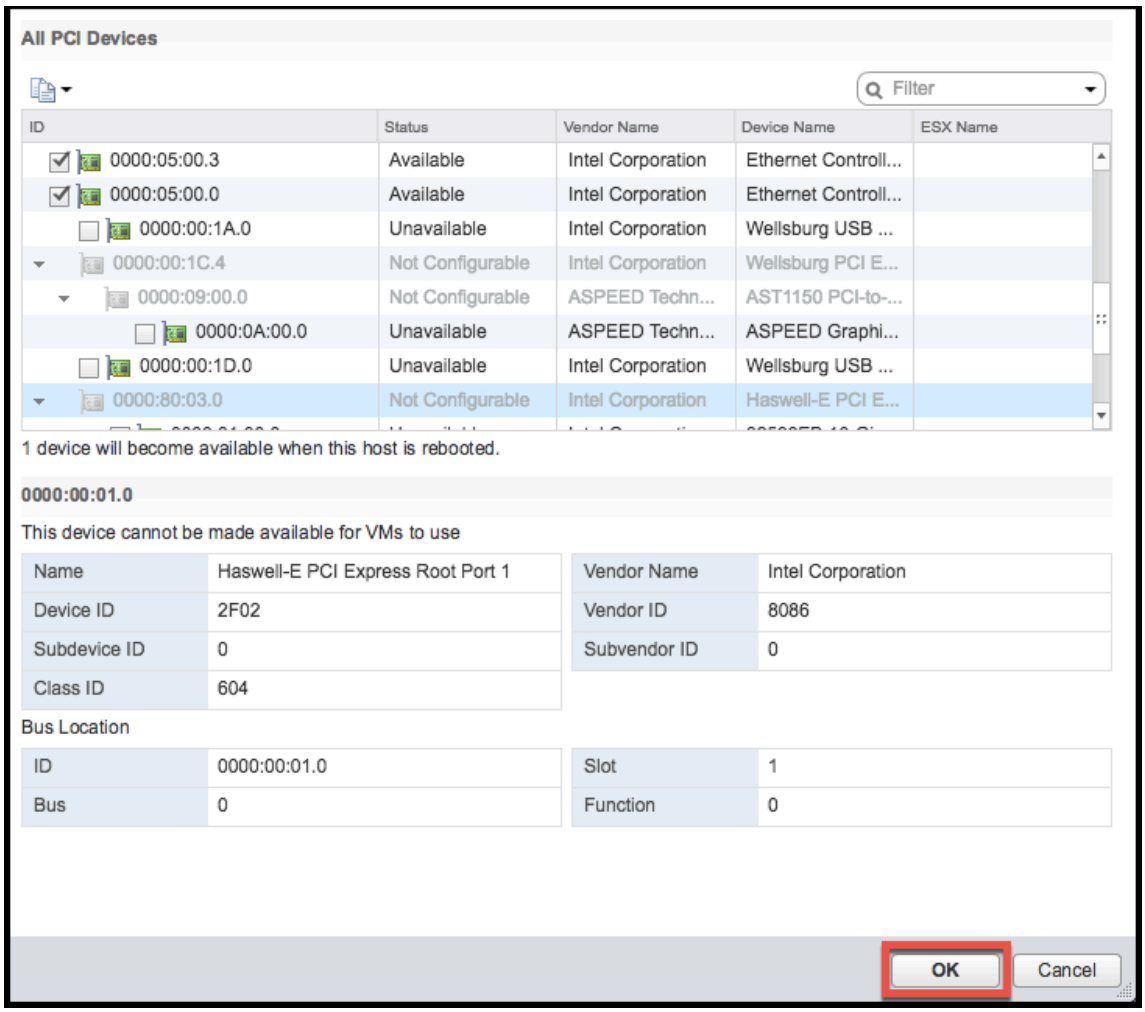
- Die Firmware-Version der Intel XL710 NIC auf dem Host ist 5.04.
- Ein PCI-Passthrough-Gerät, das mit dem Host verbunden und konfiguriert ist
- Unterstützte Netzwerkkarten:
  - Intel X710 10G NIC
  - Intel XL710 Dual-Port 40G NIC
  - Intel XL710 Single-Port 40G NIC
  - Intel XXV710 Dual-Port 25G NIC

Konfigurieren von Passthrough-Geräten auf einem Host

Bevor Sie ein Passthrough-PCI-Gerät auf einer virtuellen Maschine konfigurieren, müssen Sie es auf dem Host-Computer konfigurieren. Gehen Sie folgendermaßen vor, um Passthrough-Geräte auf einem Host zu konfigurieren.

1. Wählen Sie den Host im Navigator-Bedienfeld des vSphere Web Client aus.
2. Klicken Sie auf **Verwalten** > **Einstellungen** > **PCI-Geräte** . Alle verfügbaren Passthrough-Geräte werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
4. Das Fenster **PCI-Geräteverfügbarkeit bearbeiten** wird angezeigt.

5. Wählen Sie die Geräte aus, die für den Passthrough verwendet werden sollen, und klicken Sie auf **OK**.

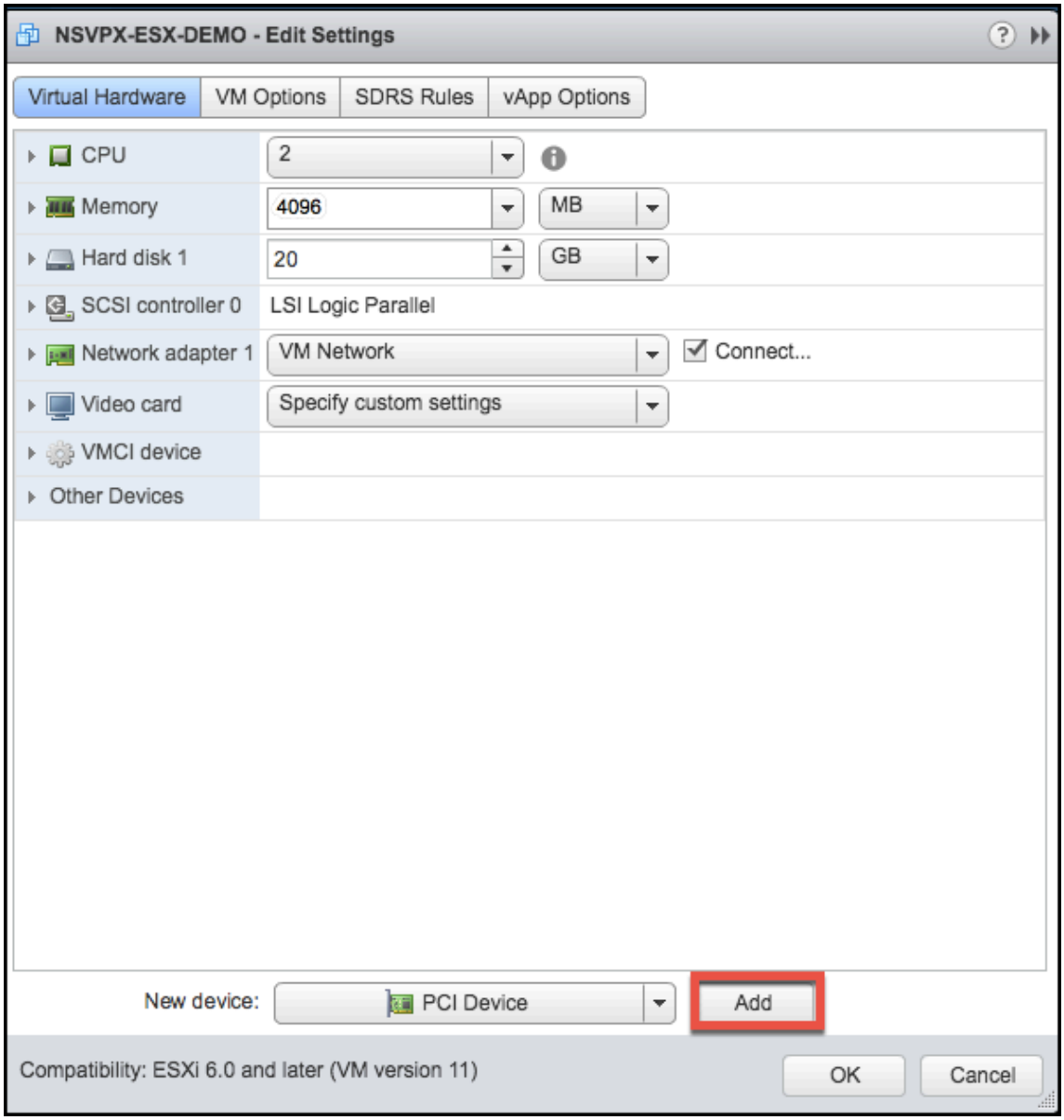


6. Starten Sie den Hostcomputer neu.

Passthrough-Geräte auf einer NetScaler VPX-Instanz konfigurieren

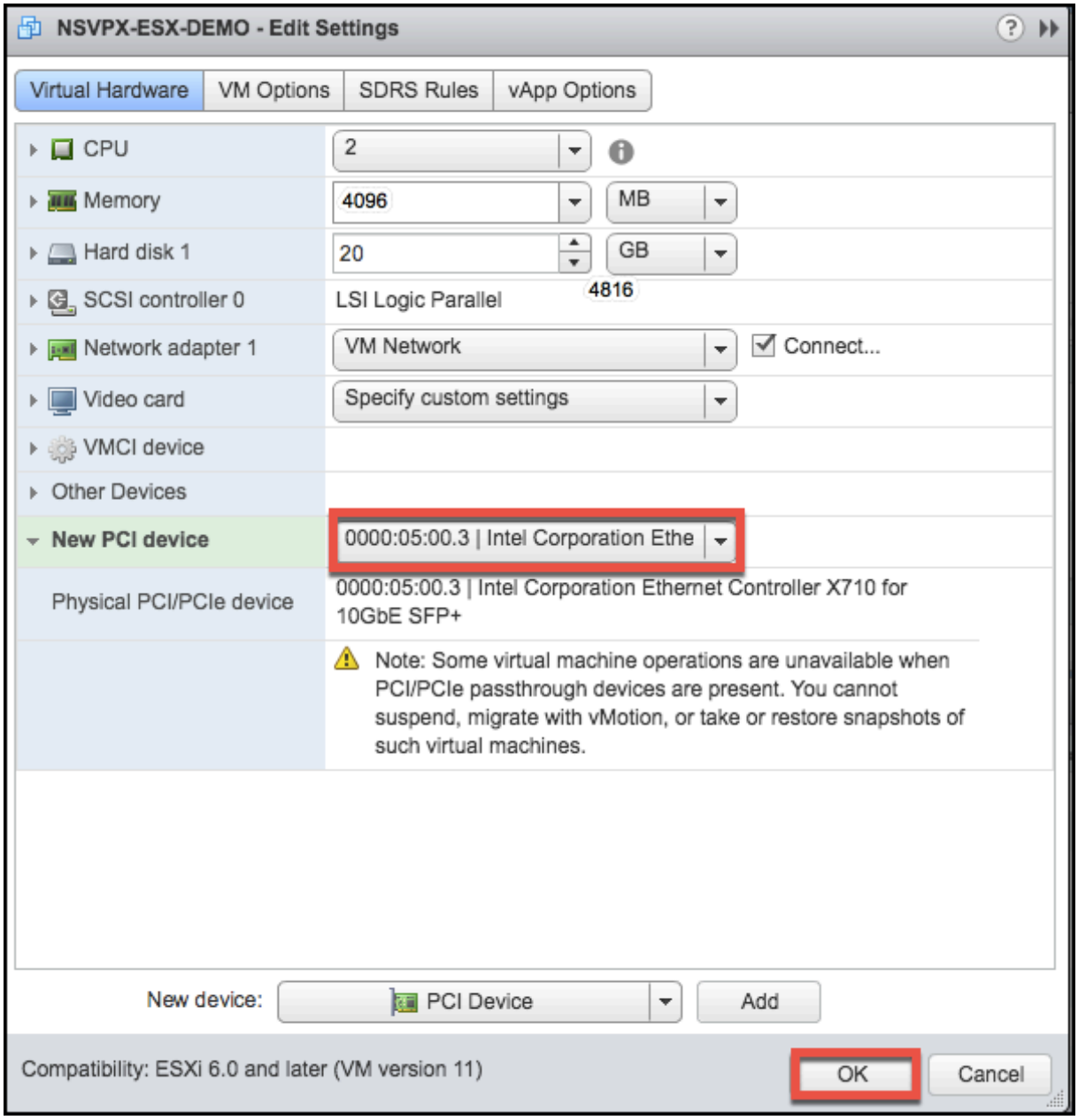
Gehen Sie wie folgt vor, um ein Passthrough-PCI-Gerät auf einer NetScaler VPX-Instanz zu konfigurieren.

1. Schalten Sie die virtuelle Maschine aus.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** im Dropdownmenü **Neues Gerät** die Option **PCI-Gerät** aus, und klicken Sie auf **Hinzufügen**.



4. Erweitern Sie **Neues PCI-Gerät**, und wählen Sie das Passthrough-Gerät aus, das mit der virtuellen Maschine verbunden werden soll, aus der Dropdownliste aus, und klicken Sie auf **OK**.

> **Hinweis:**
>
> VMXNET3-Netzwerkschnittstelle und PCI-Passthrough-Netzwerkschnittstelle können nicht koexistieren.



1. Schalten Sie den virtuellen Gastcomputer ein.

Sie haben die Schritte zur Konfiguration von NetScaler VPX für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen abgeschlossen.

Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem VMware ESX Hypervisor

October 17, 2024

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem VMware ESX-Hypervisor anwenden. Therefore in certain cases, a specific setup or VPX instance is brought up in much lesser time.

Weitere Informationen zu Preboot-Benutzerdaten und ihrem Format finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud.

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

Sample <NS-CONFIG> section:

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

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

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

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

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

How to provide preboot user data on ESX hypervisor

Sie können Preboot-Benutzerdaten auf dem ESX Hypervisor vom Webclient oder vSphere-Client aus auf die folgenden zwei Arten bereitstellen:

- Using CD/DVD ISO
- Using OVF Property

Provide user data using CD/DVD ISO

Sie können den VMware vSphere-Client verwenden, um Benutzerdaten mithilfe des CD/DVD-Laufwerks als ISO-Image in die VM einzufügen.

Gehen Sie wie folgt vor, um Benutzerdaten mithilfe der CD/DVD-ISO bereitzustellen:

1. Erstellen Sie eine Datei mit einem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält. For more information on the content of the <NS-CONFIG> tag, see Sample <NS-CONFIG> section.

   > **Hinweis:**
   >
   > Der Dateiname muss strikt als `userdata`verwendet werden.

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

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

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

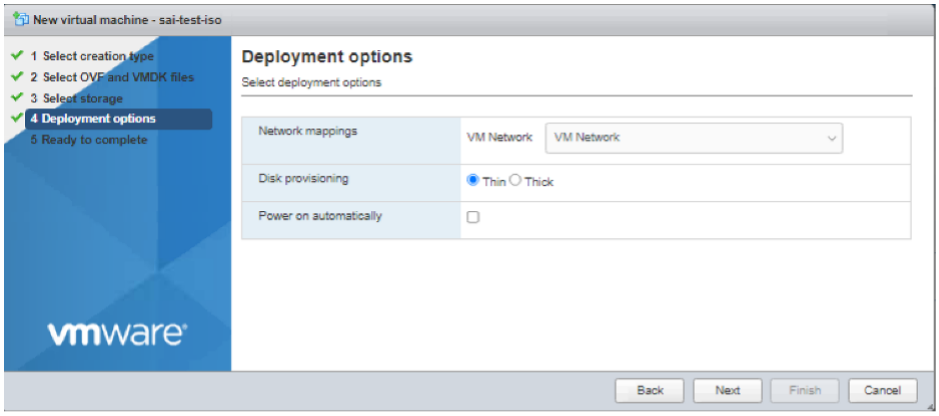
   The following sample configuration shows how to generate an ISO image using the `mkisofs` command in Linux.

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

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

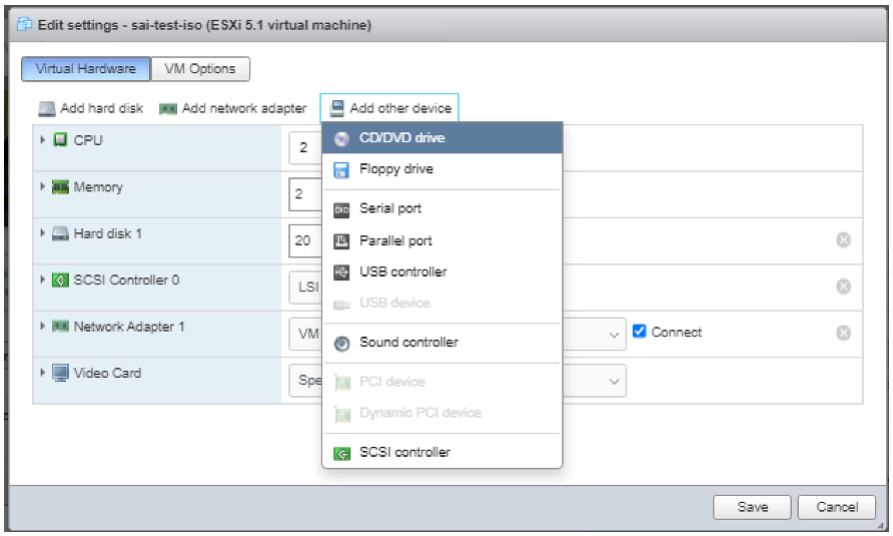


```
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
```

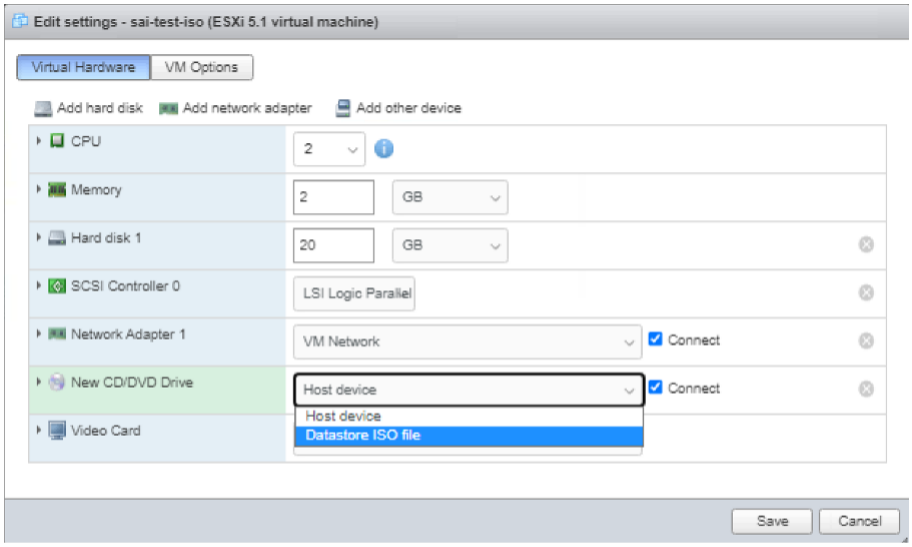
3. Stellen Sie die NetScaler VPX-Instanz über den Standardbereitstellungsprozess zum Erstellen der VM bereit. But do not power on the VM automatically.



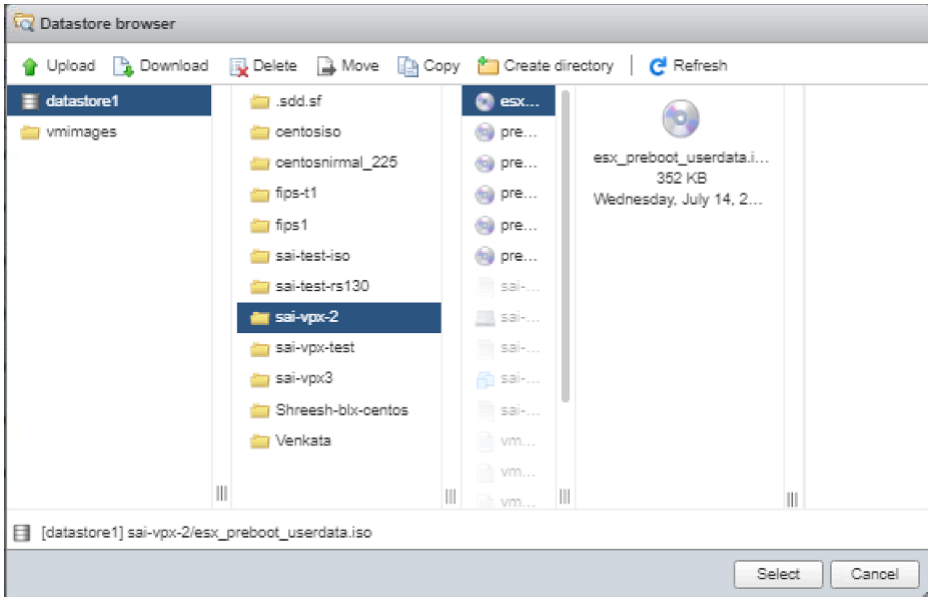
4. After the VM is successfully created, attach the ISO file as CD/DVD drive to the VM.



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.

Stellen Sie Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX-Webclient bereit

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.


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

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

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

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

   - In Linux, use the following command:

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

     Beispiel

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

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

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

3. Nehmen Sie einen **Produktabschnitt** in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor auf.

   Sample Product section:

   ```
   <ProductSection>

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



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

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

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

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


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

Stellen Sie Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX vSphere-Client bereit

Gehen Sie wie folgt vor, um Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX vSphere Client bereitzustellen.

1. Create a file with user data content.

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

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

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

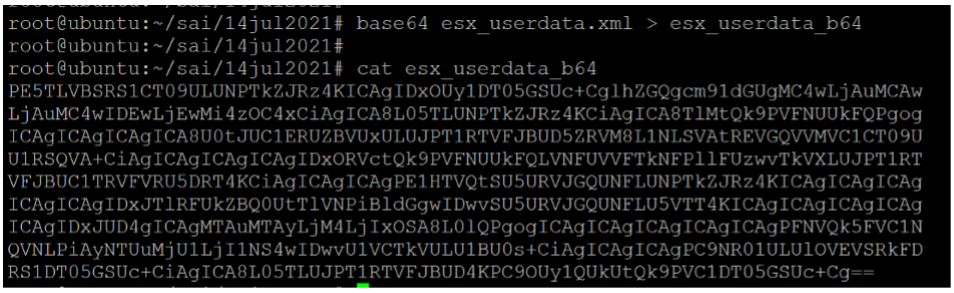
2. Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

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

     Beispiel


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



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

3. Nehmen Sie einen **Produktabschnitt** in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor auf.

   Sample Product section:

```
<ProductSection>

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

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

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

</ProductSection>
```

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

```
<ProductSection>

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



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

5. Fügen Sie die Eigenschaft wie folgt `ovf:transport="com.vmware.guestInfo"` zu VirtualHardwareSection hinzu:

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

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

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


Installieren einer NetScaler VPX-Instanz in der VMware Cloud auf AWS

October 17, 2024

Mit VMware Cloud (VMC) auf AWS können Sie Cloud-Softwaredefinierte Rechenzentren (SDDC) in AWS mit der gewünschten Anzahl von ESX-Hosts erstellen. Das VMC auf AWS unterstützt NetScaler VPX-Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Ein VMware SDDC muss mindestens mit einem Host vorhanden sein.
- Laden Sie die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie entsprechende Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie im *NetScaler VPX-Lizenzierungshandbuch* unter </en-us/licensing/licensing-guide-for-netscaler.html>.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX NCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> **Hinweis:**
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei "OVF Tool User Guide"http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei "OVF Tool User Guide" http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie VMware SDDC installiert und konfiguriert haben, können Sie mit dem SDDC virtuelle Appliances in der VMware Cloud installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen in der VMware-Cloud zu installieren:

1. Öffnen Sie VMware SDDC auf Ihrer Workstation.
2. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldedaten ein, und klicken Sie dann auf Anmelden.
3. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
4. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Deploy from file** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setupdateien gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.

   > **Hinweis:** Standardmäßig verwendet die NetScaler VPX Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird.

5. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.
6. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.
7. Wenn Sie eine andere virtuelle Appliance installieren möchten, wiederholen Sie dies in Schritt 6.
8. Geben Sie die Verwaltungs-IP-Adresse aus demselben Segment an, das als Verwaltungsnetzwerk ausgewählt wurde. Das gleiche Subnetz wird für das Gateway verwendet.
9. VMware SDDC erfordert, dass NAT- und Firewall-Regeln explizit für alle privaten IP-Adressen erstellt werden, die zu Netzwerksegmenten gehören.

Installieren Sie eine NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server

October 17, 2024

Um NetScaler VPX-Instanzen auf Microsoft Windows Server zu installieren, müssen Sie zuerst Windows Server mit aktivierter Hyper-V-Rolle auf einem Computer mit ausreichenden Systemressourcen installieren. Beim Installieren der Hyper-V-Rolle müssen Sie die Netzwerkkarten auf dem Server angeben, den Hyper-V zum Erstellen von virtuellen Netzwerken verwenden soll. Sie können einige NICs für den Host reservieren. Verwenden Sie Hyper-V Manager, um die Installation der NetScaler VPX-Instanz durchzuführen.

Die NetScaler VPX-Instanz für Hyper-V wird im Format der virtuellen Festplatte (VHD) bereitgestellt. Es enthält die Standardkonfiguration für Elemente wie CPU, Netzwerkschnittstellen sowie Festplattengröße und -format. Nach der Installation der NetScaler VPX-Instanz können Sie die Netzwerkadapter auf einer virtuellen Appliance konfigurieren, virtuelle Netzwerkkarten hinzufügen und dann die NetScaler IP-Adresse, Subnetzmaske und Gateway zuweisen und die Grundkonfiguration der virtuellen Appliance abschließen.

Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, finden Sie weitere Informationen unter Aufrüsten einer eigenständigen NetScalerVPX-Appliance

> **Hinweis:**
>
> Das ISIS-Protokoll (Intermediate System-to-Intermediate System) wird auf der virtuellen NetScaler VPX-Appliance, die auf der HyperV-2012-Plattform gehostet wird, nicht unterstützt.

Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Microsoft-Servern

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Aktivieren Sie die Hyper-V-Rolle auf Windows-Servern. Weitere Informationen finden Sie unter http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Laden Sie die Setupdateien der virtuellen Appliance
- Holen Sie sich NetScaler VPX-Instanzlizenzdateien. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie im *NetScaler VPX Licensing Guide* unter https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US.

Hardwareanforderungen für Microsoft-Server

In der folgenden Tabelle werden die Mindestsystemanforderungen für Microsoft-Server beschrieben.

Tabelle 1. Mindestsystemanforderungen für Microsoft-Server

Komponente	Voraussetzung
CPU	1,4 GHz 64-Bit-Prozessor
RAM	8 GB
Speicherplatz	32 GB oder mehr

In der folgenden Tabelle sind die virtuellen Computerressourcen für jeden NetScaler VPX-Instanz.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
RAM	4 GB
Virtuelle CPU	2
Speicherplatz	20 GB
Virtuelle Netzwerkschnittstellen	1

Laden Sie die NetScaler VPX-Setup-Dateien herunter

Die NetScaler VPX-Instanz für Hyper-V wird im Format der virtuellen Festplatte (VHD) bereitgestellt. Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf, klicken Sie auf **Anmelden > Mein Konto > Citrix Account erstellen** und folgen Sie den Anweisungen zum Erstellen eines Citrix-Kontos.

Gehen Sie folgendermaßen vor, um die Setup-Dateien der NetScaler VPX Instanz herunterzuladen:

1. Navigieren Sie in einem Webbrowser zu http://www.citrix.com/.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
3. Klicken Sie auf **Downloads**.
4. Wählen Sie im Dropdownmenü **Produkt auswählen** die Option **NetScaler (NetScaler ADC)** aus.
5. Klicken Sie unter **NetScaler Release X.X > Virtual Appliances**auf **NetScaler**VPX Release X.X.
6. Laden Sie die komprimierte Datei auf Ihren Server herunter.

Installieren Sie die NetScaler VPX-Instanz auf Microsoft-Servern

Nachdem Sie die Hyper-V-Rolle auf Microsoft Server aktiviert und die Dateien der virtuellen Appliance extrahiert haben, können Sie Hyper-V Manager verwenden, um die NetScaler VPX-Instanz zu installieren. Nachdem Sie die virtuelle Maschine importiert haben, müssen Sie die virtuellen Netzwerkkarten konfigurieren, indem Sie sie den von Hyper-V erstellten virtuellen Netzwerken zuordnen.

Sie können maximal acht virtuelle Netzwerkkarten konfigurieren. Selbst wenn die physische Netzwerkkarte DOWN ist, geht die virtuelle Appliance davon aus, dass die virtuelle Netzwerkkarte AKTIV ist, da sie weiterhin mit den anderen virtuellen Appliances auf demselben Host (Server) kommunizieren kann.

> **Hinweis:**
>
> Sie können keine Einstellungen ändern, während die virtuelle Appliance ausgeführt wird. Fahren Sie die virtuelle Appliance herunter und nehmen Sie dann Änderungen vor.

So installieren Sie die NetScaler VPX-Instanz mit Hyper-V Manager auf Microsoft Server:

1. Klicken Sie zum Starten von Hyper-V Manager auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Navigationsbereich unter **Hyper-V Manage**r den Server aus, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
3. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren**e.
4. Geben Sie im Dialogfeld **Virtuelle Maschine importieren** unter **Speicherort**den Pfad des Ordners an, der die NetScaler VPX-Instanzsoftwaredateien enthält, und wählen Sie dann **Die virtuelle Maschine kopieren (neue eindeutige ID erstellen)**aus. Dieser Ordner ist der übergeordnete Ordner, der die Ordner Snapshots, Virtuelle Festplatten und Virtuelle Maschinen enthält.

> **Hinweis:**
>
> Wenn Sie eine komprimierte Datei erhalten haben, stellen Sie sicher, dass Sie die Dateien in einen Ordner extrahieren, bevor Sie den Pfad zum Ordner angeben.

1. Klicken Sie auf **Importieren**.
2. Stellen Sie sicher, dass die importierte virtuelle Appliance unter **Virtuelle Maschinen**aufgeführt ist.
3. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte **2** bis **6.**

> **Wichtig:**
>
> Stellen Sie sicher, dass Sie die Dateien in Schritt **4**in einen anderen Ordner extrahieren.

Automatische Bereitstellung einer NetScaler VPX-Instanz auf Hyper-V

Die automatische Bereitstellung der NetScaler VPX-Instanz ist optional. Wenn die automatische Bereitstellung nicht erfolgt, bietet die virtuelle Appliance eine Option zum Konfigurieren der IP-Adresse usw.

Führen Sie die folgenden Schritte aus, um die NetScaler VPX-Instanz auf Hyper-V automatisch bereitzustellen.

1. Erstellen Sie ein ISO9660-konformes ISO-Image mit der xml-Datei, wie im Beispiel dargestellt. Stellen Sie sicher, dass der Name der xml-Datei **userdata**lautet.

   Sie können eine ISO-Datei aus einer XML-Datei erstellen, indem Sie Folgendes verwenden:

   • Jedes Imageverarbeitungstool wie PowerISO.

   • `mkisofs` Befehl unter Linux.

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

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

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

oe:id=""

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

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

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

<Property oe:key="com.citrix.netscaler.platform" oe:value="
    NS1000V"/>

<Property oe:key="com.citrix.netscaler.orch\_env" oe:value="
    cisco-orch-env"/>

```



```
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. Kopieren Sie das ISO-Image auf den Hyper-V-Server.
3. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**aus. Sie können auch die virtuelle Appliance auswählen und dann mit der rechten Maustaste klicken und **Einstellungen**auswählen. Das Fenster **Einstellungen** für die ausgewählte virtuelle Appliance wird angezeigt.
4. Klicken **Sie im Fenster Einstellungen** unter dem Abschnitt Hardware auf **IDE Controller**.
5. Wählen Sie im rechten Fensterbereich **DVD-Laufwerk** und klicken Sie auf **Hinzufügen**. Das DVD-Laufwerk wird im Abschnitt **IDE Controller** im linken Fensterbereich hinzugefügt.
6. Wählen Sie das in Schritt 5 hinzugefügte **DVD-Laufwerk** aus. Aktivieren Sie im rechten Fensterbereich das **Optionsfeld Image-Datei**, klicken Sie auf **Durchsuchen** und wählen Sie das ISO-Image aus, das Sie in Schritt 2 auf den Hyper-V-Server kopiert haben.
7. Klicken Sie auf **Übernehmen**.

> **Hinweis:**
>
> Die Instanz der virtuellen Appliance wird in folgenden Fällen mit der Standard-IP-Adresse angezeigt:

- Das DVD-Laufwerk ist angeschlossen und die ISO-Datei wird nicht bereitgestellt.
- Die ISO-Datei enthält nicht die Benutzerdatendatei.
- Der Name oder das Format der Benutzerdatendatei ist nicht korrekt.

Gehen Sie folgendermaßen vor, um virtuelle Netzwerkkarten auf der NetScaler VPX-Instanz zu konfigurieren:

1. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**aus.
2. <virtual appliance name>Klicken **Sie im Dialogfeld Einstellungen für** im linken Bereich auf **Hardware hinzufügen** .
3. Wählen Sie im rechten Bereich aus der Geräteliste die Option **Netzwerkadapter**aus.
4. Klicken Sie auf **Hinzufügen**.
5. Stellen Sie sicher, dass **Netzwerkadapter (nicht verbunden)** im linken Bereich angezeigt wird.

6. Wählen Sie im linken Bereich den Netzwerkadapter aus.
7. Wählen Sie im rechten Bereich im Menü **Netzwerk** das virtuelle Netzwerk aus, mit dem der Adapter verbunden werden soll.
8. Wiederholen Sie die Schritte **6** und **7**, um das virtuelle Netzwerk für andere Netzwerkadapter auszuwählen, die Sie verwenden möchten.
9. Klicken Sie auf **Übernehmen** und dann auf **OK**.

So konfigurieren Sie die NetScaler VPX-Instanz:

1. Klicken Sie mit der rechten Maustaste auf die zuvor installierte virtuelle Appliance, und wählen Sie dann **Starten**.
2. Rufen Sie die Konsole auf, indem Sie auf die virtuelle Appliance doppelklicken.
3. Geben Sie die NetScaler-IP-Adresse, die Subnetzmaske und das Gateway für Ihre virtuelle Appliance ein.

Sie haben die Grundkonfiguration Ihrer virtuellen Appliance abgeschlossen. Geben Sie die IP-Adresse in einen Webbrowser ein, um auf die virtuelle Appliance zuzugreifen.

> **Hinweis:**
>
> Sie können auch die Vorlage für virtuelle Maschinen (VM) verwenden, um die NetScaler VPX-Instanz mithilfe von SCVMM bereitzustellen.
>
> Wenn Sie die Microsoft Hyper-V NIC-Teaming-Lösung mit NetScaler VPX-Instanzen verwenden, finden Sie im Artikel CTX224494 weitere Informationen.

Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

October 17, 2024

Um einen NetScaler VPX für die Linux-KVM-Plattform einzurichten, können Sie die grafische Virtual Machine Manager (Virtual Manager) -Anwendung verwenden. Wenn Sie die Linux-KVM-Befehlszeile bevorzugen, können Sie das `virsh` Programm verwenden.

Das Host-Linux-Betriebssystem muss mit Virtualisierungstools wie KVM Module und QEMU auf geeigneter Hardware installiert werden. Die Anzahl der virtuellen Maschinen (VMs), die auf dem Hypervisor bereitgestellt werden können, hängt von der Anwendungsanforderung und der ausgewählten Hardware ab.

Nachdem Sie eine NetScaler VPX-Instanz bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Einschränkungen und Nutzungsrichtlinien

Allgemeine Empfehlungen

Um unvorhersehbares Verhalten zu vermeiden, wenden Sie die folgenden Empfehlungen an:

- Ändern Sie nicht die MTU der VNet-Schnittstelle, die mit der VPX-VM verknüpft ist. Fahren Sie die VPX-VM herunter, bevor Sie Konfigurationsparameter wie Schnittstellenmodi oder CPU ändern.
- Erzwingen Sie das Herunterfahren der VPX-VM nicht. Das heißt, verwenden Sie nicht den Befehl **Erzwingen aus** .
- Alle Konfigurationen, die auf dem Host Linux durchgeführt werden, sind möglicherweise dauerhaft, abhängig von Ihren Linux-Distributionseinstellungen. Sie können diese Konfigurationen dauerhaft festlegen, um ein konsistentes Verhalten bei Neustarts des Host-Linux-Betriebssystems sicherzustellen.
- Das NetScaler-Paket muss für jede bereitgestellte NetScaler VPX-Instanz einzigartig sein.

Einschränkungen

- Live-Migration einer VPX-Instanz, die auf KVM ausgeführt wird, wird nicht unterstützt.

Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

October 17, 2024

Überprüfen Sie die Mindestsystemanforderungen für einen Linux-KVM-Server, der auf einer NetScaler VPX-Instanz ausgeführt wird.

CPU-Anforderung:

- 64-Bit-x86-Prozessoren mit der Hardwarevirtualisierungsfunktion, die in Intel VT-X-Prozessoren enthalten ist.

Um zu testen, ob Ihre CPU den Linux-Host unterstützt, geben Sie den folgenden Befehl an der Linux-Shell-Eingabeaufforderung

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

Wenn die **BIOS-Einstellungen** für die vorhergehende Erweiterung deaktiviert sind, müssen Sie sie im BIOS aktivieren.

- Stellen Sie mindestens 2 CPU-Kerne für Host Linux bereit.
- Es gibt keine spezifische Empfehlung für die Prozessorgeschwindigkeit, aber je höher die Geschwindigkeit, desto besser ist die Leistung der VM-Anwendung.

Speicherbedarf (RAM):

Mindestens 4 GB für den Host-Linux-Kernel. Fügen Sie mehr Arbeitsspeicher hinzu, wie es von den VMs benötigt wird.

Festplattenanforderung:

Berechnen Sie den Speicherplatz für den Host-Linux-Kernel und die VM-Anforderungen. Eine einzelne NetScaler VPX-VM benötigt 20 GB Festplattenspeicher.

Softwareanforderungen

Der verwendete Host-Kernel muss ein 64-Bit-Linux-Kernel, Version 2.6.20 oder höher, mit allen Virtualisierungstools sein. Citrix empfiehlt neuere Kernel wie 3.6.11-4 und höher.

Viele Linux-Distributionen wie Red Hat, CentOS und Fedora haben Kernelversionen und zugehörige Virtualisierungstools getestet.

Hardwareanforderungen für Gast-VM

NetScaler VPX unterstützt IDE- und VirtIO-Festplattentypen. Der Festplattentyp wurde in der XML-Datei konfiguriert, die Teil des NetScaler-Pakets ist.

Netzwerkanforderungen

NetScaler VPX unterstützt paravirtualisierte VirtIO-, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen.

Weitere Informationen zu den unterstützten Netzwerkschnittstellen finden Sie unter:

- NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitstellen
- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen
- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

Quellschnittstelle und Modi

Der Quellgerätetyp kann entweder Bridge oder MacVTap sein. In MacVTap sind vier Modi möglich - VEPA, Bridge, Private und Pass-Through. Überprüfen Sie die Arten von Schnittstellen, die Sie verwenden können, und die unterstützten Datenverkehrstypen wie folgt:

Brücke:

- Linux-Brücke.
- `Ebtables` und `iptables` Einstellungen auf Host Linux filtern möglicherweise den Datenverkehr auf der Bridge, wenn Sie nicht die richtige Einstellung auswählen oder `IPtable` Dienste deaktivieren.

MacVTap (VEPA-Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen desselben niedrigeren Geräts können von allen VMs gemeinsam genutzt werden.
- Inter-VM-Kommunikation mit derselben
- niedrigeres Gerät ist nur möglich, wenn der Upstream- oder Downstream-Switch den VEPA-Modus unterstützt.

MacVTap (privater Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen desselben niedrigeren Geräts können von allen VMs gemeinsam genutzt werden.
- Eine VM-Kommunikation mit demselben niedrigeren Gerät ist nicht möglich.

MacVTAP (Bridge-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können für die VMs gemeinsam genutzt werden.
- Die Kommunikation zwischen VM mit demselben niedrigeren Gerät ist möglich, wenn die untere Geräteverbindung UP ist.

MacVTap (Pass-Through-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können nicht für die VMs freigegeben werden.
- Nur eine VM kann das untere Gerät verwenden.

> **Hinweis:**
>
> Um eine optimale Leistung der VPX-Instanz zu erzielen, stellen Sie sicher, dass die Funktionen `gro` und `lro` auf den Quellschnittstellen deaktiviert sind.

Eigenschaften von Quellschnittstellen

Stellen Sie sicher, dass Sie die Funktionen generic-Receive-offload (`gro`) und Large-Receive-Offload (`lro`) der Quellschnittstellen ausschalten. Um die `lro` Funktionen `gro` und auszuschalten, führen Sie die folgenden Befehle an der Linux-Shell des Hosts aus.

`ethtool -K eth6 gro aus ethool -K eth6 lro aus`

Beispiel:

```
[root@localhost ~]# ethtool -K eth6

                    Offload parameters for eth6:

                                        rx-checksumming: on

                                        tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

[root@localhost ~]#
```

Beispiel:

Wenn die Linux-Brücke des Hosts wie im folgenden Beispiel als Quellgerät verwendet wird, müssen die `lro` Funktionen an den VNet-Schnittstellen ausgeschaltet werden, bei denen es sich um die virtuellen Schnittstellen handelt, die den Host mit den Gast-VMs verbinden.

```
[root@localhost ~]# brctl show eth6_br

bridge name     bridge  id               STP enabled interfaces

eth6_br         8000.00e0ed1861ae          no         eth6

                                                      vnet0

                                                      vnet2

[root@localhost ~]#
```

Im vorhergehenden Beispiel werden die beiden virtuellen Schnittstellen von eth6_br abgeleitet und

werden als vnet0 und vnet2 dargestellt. Führen Sie die folgenden Befehle aus, um auszuschalten `gro` und `lro` Funktionen für diese Schnittstellen.

```
1       ethtool -K vnet0 gro off
2               ethtool -K vnet2 gro off
3               ethtool -K vnet0 lro off
4                       ethtool -K vnet2 lro off
```

Promiscuous-Modus

Der Promiscuous-Modus muss aktiviert sein, damit die folgenden Funktionen funktionieren:

- L2-Modus
- Verarbeitung des Multicast-Datenverkehrs
- Übertragung
- IPv6-Verkehr
- virtueller MAC
- Dynamisches Routing

Verwenden Sie den folgenden Befehl, um den Promiscuous-Modus zu aktivieren.

```
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
                   :1
6              RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
7              TX packets:2895843 errors:0 dropped:0 overruns:0 carrier
                   :0
8              collisions:0 txqueuelen:1000
9              RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)
10
11  [root@localhost ~]#
```

Modul erforderlich

Stellen Sie für eine bessere Netzwerkleistung sicher, dass das Modul vhost_net auf dem Linux-Host vorhanden ist. Um zu überprüfen, ob das Modul vhost_net vorhanden ist, führen Sie den folgenden Befehl auf dem Linux-Host aus:

```
1   lsmod | grep "vhost\_net"
```

Wenn vhost_net noch nicht läuft, geben Sie den folgenden Befehl ein, um es auszuführen:

```
1   modprobe vhost\_net
```


Bereitstellen der NetScaler VPX Instanz mithilfe von OpenStack

October 17, 2024

Sie können eine NetScaler VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie entweder den **Nova-Boot-Befehl** (OpenStack CLI) oder Horizon (OpenStack-Dashboard) verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten als CD-ROM-Gerät an die Instanz anhängt. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfiguration wie Verwaltungs-IP-Adresse, Netzwerkmaske, Standard-Gateway zu übergeben und Kundenskripte zu injizieren.

In einer NetScaler Appliance ist der Standardauthentifizierungsmechanismus kennwortbasiert. Jetzt wird der SSH-Schlüsselpaar-Authentifizierungsmechanismus für NetScaler VPX-Instanzen in der OpenStack-Umgebung unterstützt.

Das Schlüsselpaar (öffentlicher Schlüssel und privater Schlüssel) wird generiert, bevor der Public Key Cryptographie-Mechanismus verwendet wird. Sie können verschiedene Mechanismen wie Horizon, Puttygen.exe für Windows und `ssh-keygen` für die Linux-Umgebung verwenden, um das Schlüsselpaar zu generieren. Weitere Informationen zum Generieren von Schlüsselpaaren finden Sie in der Online-Dokumentation der jeweiligen Mechanismen.

Sobald ein Schlüsselpaar verfügbar ist, kopieren Sie den privaten Schlüssel an einen sicheren Ort, auf den autorisierte Personen Zugriff haben. In OpenStack kann Public Key mit dem Boot-Befehl Horizon oder Nova auf einer VPX-Instanz bereitgestellt werden. Wenn eine VPX-Instanz mithilfe von OpenStack bereitgestellt wird, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge liest. Diese Zeichenfolge ist OpenStack Foundation und für Red Hat Linux-Distributionen wird sie in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben.

Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die Netzwerkkonfiguration, die benutzerdefinierten Skripts und das SSH-Schlüsselpaar zu lesen, falls vorhanden.

Benutzer-Datendatei

Die NetScaler VPX-Instanz verwendet eine benutzerdefinierte OVF-Datei, auch Benutzerdatendatei genannt, um Netzwerkkonfiguration, benutzerdefinierte Skripts zu injizieren. Diese Datei wird als Teil des Konfigurationslaufwerks bereitgestellt. Hier ist ein Beispiel für eine benutzerdefinierte OVF-Datei.

```
1 ```
```



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1"
xmlns:cs="http://schemas.citrix.com/openstack">
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
<Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
   orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
   />
<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
   10.1.2.1"/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack
        " xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
                  <Text>
                        #!/bin/bash
                        echo "Hi, how are you" $1 $2 >> /var/sample.
                           txt
                  </Text>
           </Script>
           <Script>
                 <Type>python</Type>
                 <BootScript>after</BootScript>
                  <Text>
                       #!/bin/python
 print("Hello");
                  </Text>
           </Script>
   <Script>
                 <Type>perl</Type>
                 <BootScript>before</BootScript>
                  <Text>
                       !/usr/bin/perl
```



```
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  ``` In der OVF-Datei vor "PropertySection" wird für die NetScaler-
      Netzwerkkonfiguration verwendet, während sie zum Einschließen aller
      Skripts verwendet \<cs:ScriptSection> wird. \</Scripts> Tags werden
      verwendet, um alle Skripts zusammen zu bündeln. Jedes Skript ist
      zwischen \<Script> \</Script> Tags definiert. Jedes Skript-Tag hat
      folgende Felder/Tags:
```

a) <Type>: Gibt den Wert für den Skripttyp an. Mögliche Werte: Shell/Perl/Python/NSLCI (für NetScaler CLI-Skripts)

b) <Parameter>: Stellt Parameter für das Skript bereit. Jedes Skript kann mehrere <Parameter> Tags haben.

c) <BootScript>: Gibt den Skriptausführungspunkt an. Mögliche Werte für dieses Tag: vorher/nachher. “before”gibt an, dass das Skript ausgeführt wird, bevor PE auftaucht. “after”gibt an, dass das Skript ausgeführt wird, nachdem PE angezeigt wird.

d) <Text>: Fügt den Inhalt eines Skripts ein.

> **Hinweis:**
>
> Derzeit kümmert sich die VPX-Instanz nicht um die Bereinigung von Skripten. Als Administrator müssen Sie die Gültigkeit des Skripts überprüfen.
>
> Nicht alle Abschnitte müssen vorhanden sein. Verwenden Sie eine leere “PropertySection”, um nur Skripts zu definieren, die beim ersten Start oder einer leeren Ausführung ausgeführt werden
>
> Nachdem die erforderlichen Abschnitte der OVF-Datei (Benutzerdatendatei) ausgefüllt wurden, verwenden Sie diese Datei, um die VPX-Instanz bereitzustellen.

Netzwerkkonfiguration

Im Rahmen der Netzwerkkonfiguration lautet die VPX-Instanz:

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Nachdem die Parameter erfolgreich gelesen wurden, werden sie in der NetScaler Konfiguration aufgefüllt, damit die Instanz remote verwaltet werden kann. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP ausfällt oder Times-Out ausfällt, wird die Instanz mit der Standardnetzwerkkonfiguration (192.168.100.1/16) erstellt.

Kundenskript

Die VPX-Instanz erlaubt es, während der ersten Bereitstellung ein benutzerdefiniertes Skript auszuführen. Die Appliance unterstützt Skripts vom Typ Shell, Perl, Python und NetScaler CLI-Befehle.

SSH-Schlüsselpaar-Authentifizierung

Die VPX-Instanz kopiert den öffentlichen Schlüssel, der im Konfigurationslaufwerk als Teil der Instanzmeta-Daten verfügbar ist, in die Datei authorized_keys. Dadurch kann der Benutzer mit dem privaten Schlüssel auf die Instanz zugreifen.

> **Hinweis:**
>
> Wenn ein SSH-Schlüssel angegeben wird, funktionieren die Standardanmeldeinformationen (nsroot/nsroot) nicht mehr. Wenn ein kennwortbasierter Zugriff erforderlich ist, melden Sie sich mit dem entsprechenden privaten SSH-Schlüssel an und legen Sie manuell ein Kennwort fest.

Voraussetzungen

Bevor Sie eine VPX-Instanz in der OpenStack-Umgebung bereitstellen, extrahieren Sie die Datei `.qcow2` aus der TGZ-Datei und bauen Sie

Ein OpenStack-Bild aus dem qcow2-Image. Führen Sie folgende Schritte aus:

1. Extrahieren Sie die `.qcow2` Datei aus der `.tqz` Datei, indem Sie den folgenden Befehl eingeben

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```


2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben.

```
openstack image create --container-format bare --property
   hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2
   file> --public <name of the OpenStack image>

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

Abbildung 1: Die folgende Abbildung enthält eine Beispielausgabe für den Befehl 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                                                 |
+------------------+--------------------------------------------------------+
```

Provisioning einer VPX-Instanz

Sie können eine VPX-Instanz auf zwei Arten bereitstellen, indem Sie eine der folgenden Optionen verwenden:

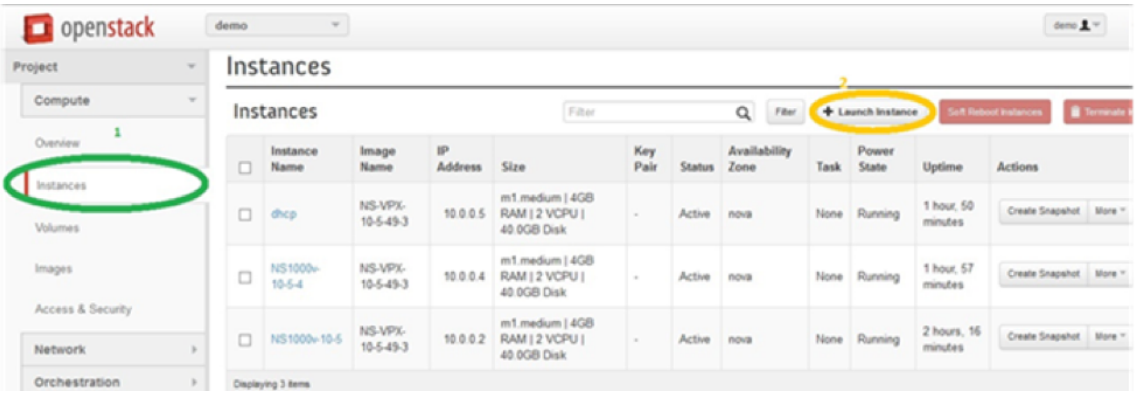
- Horizon (OpenStack-Dashboard)
- Nova-Startbefehl (OpenStack CLI)

Bereitstellen einer VPX-Instanz mit dem OpenStack-Dashboard

Gehen Sie folgendermaßen vor, um die VPX-Instanz mithilfe von Horizon bereitzustellen:

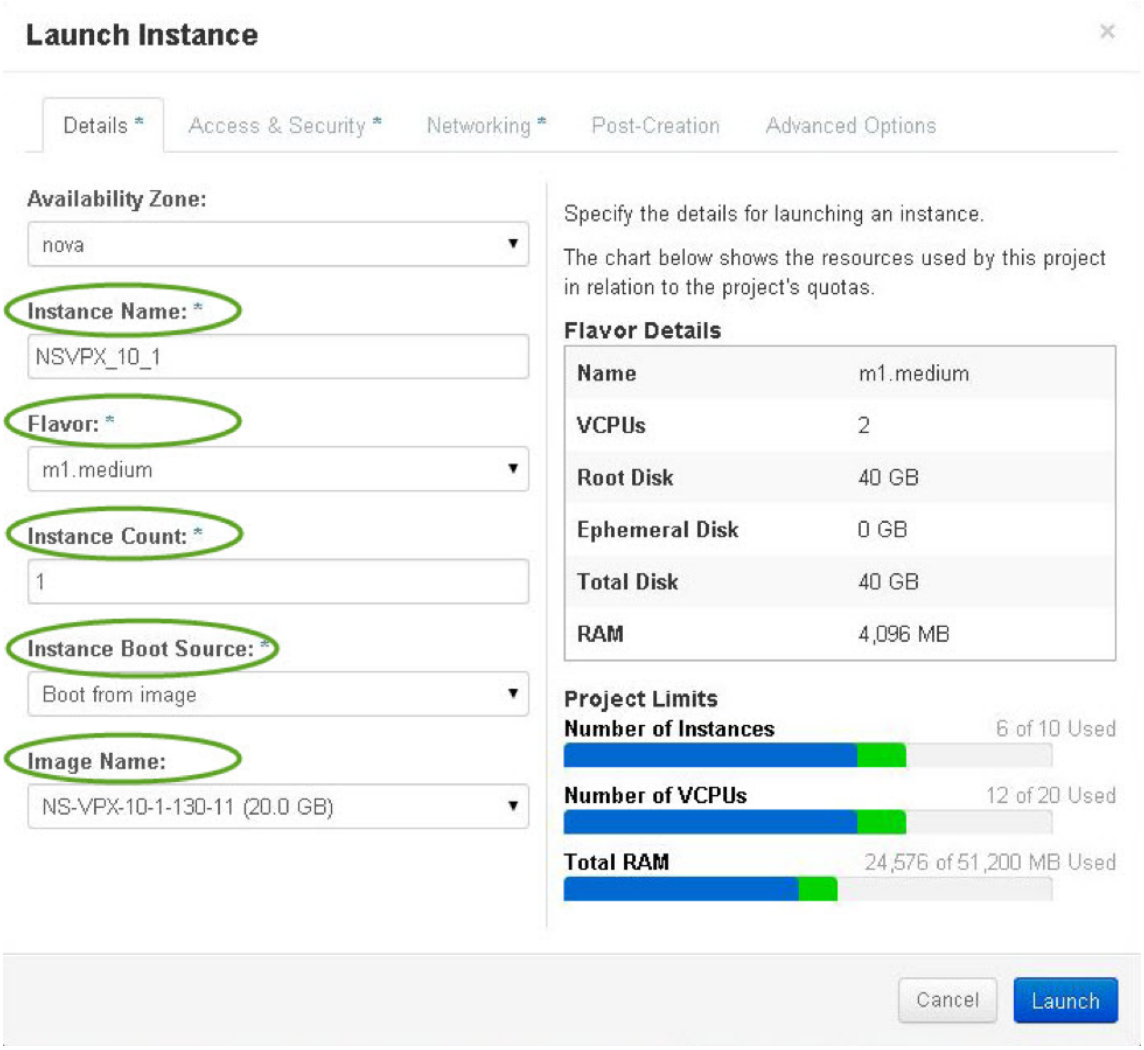
1. Melden Sie sich beim OpenStack-Dashboard an.

2. Wählen Sie im Projektfenster auf der linken Seite des Dashboards die Option **Instanzen**aus.
3. Klicken Sie im Instanzen Bedienfeld auf **Instanz starten**, um den Instanzentart-Assistenten zu öffnen.



4. Geben Sie im Assistenten zum Starten von Instanz die folgenden Details ein:

   a) Instanzname
   b) Instanzgeschmack
   c) Instanzanzahl
   d) Instanz-Boot-Quelle
   e) Imagename



5. Stellen Sie ein neues Schlüsselpaar oder ein vorhandenes Schlüsselpaar über Horizon bereit, indem Sie die folgenden Schritte ausführen:

   a) Wenn Sie kein vorhandenes Schlüsselpaar haben, erstellen Sie den Schlüssel mithilfe vorhandener Mechanismen. Wenn Sie einen vorhandenen Schlüssel haben, überspringen Sie diesen Schritt.

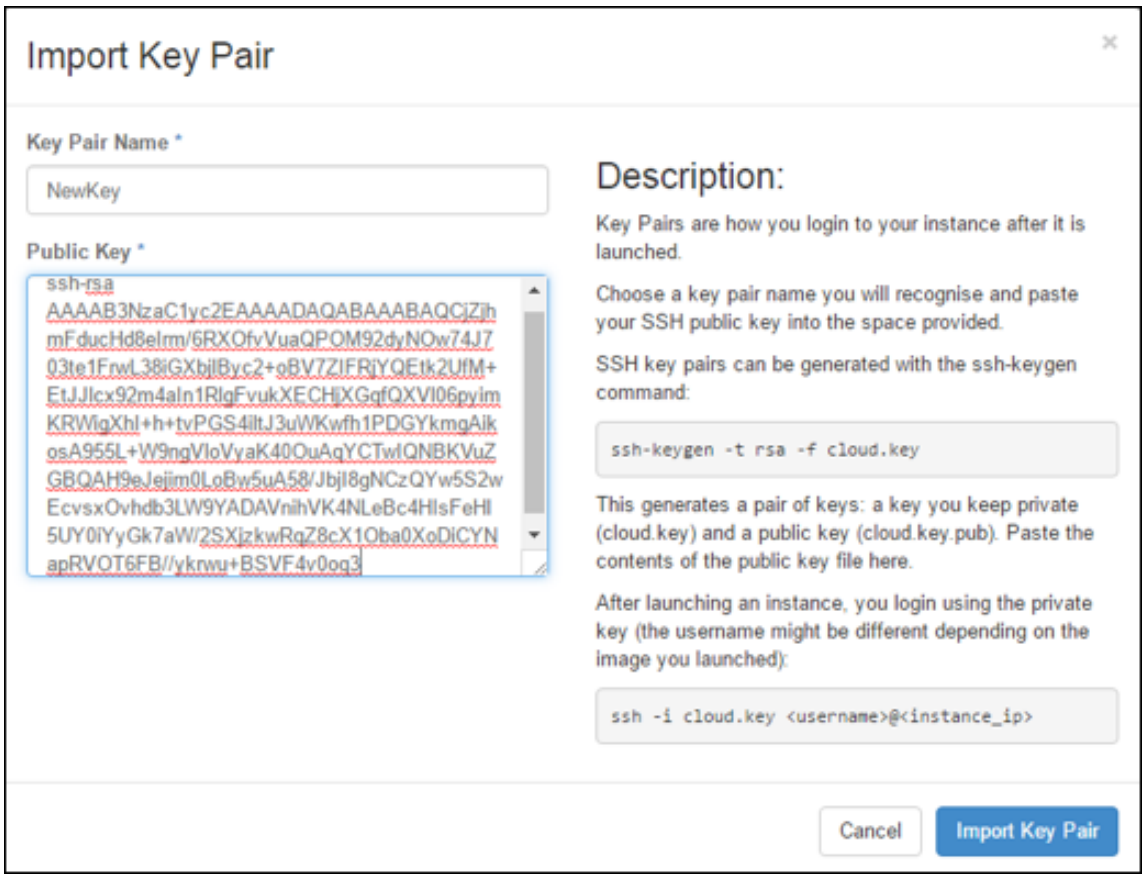
   b) Kopieren Sie den Inhalt des öffentlichen Schlüssels.

   c) Gehen Sie zu **Horizon > Instanzen > Neue Instanzen erstellen**.

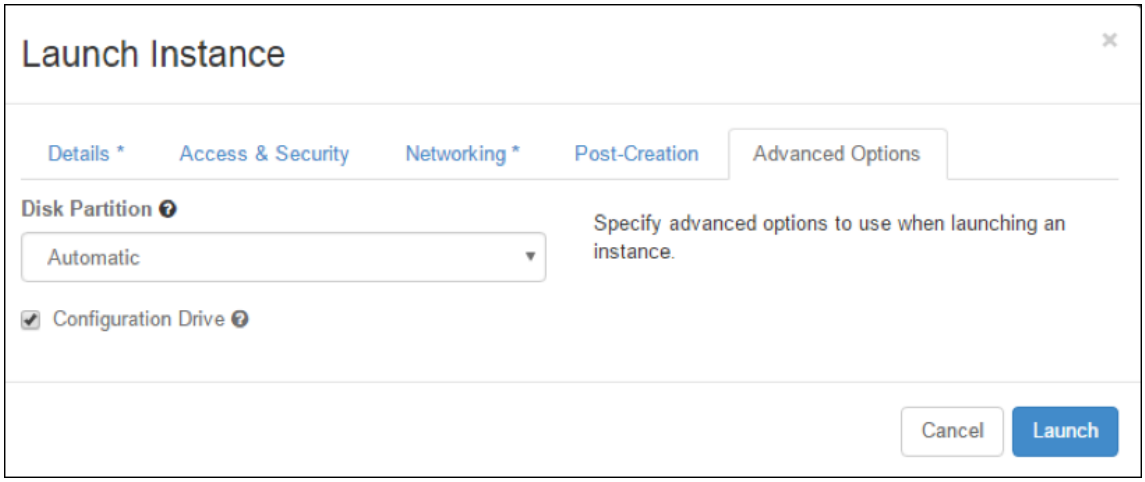
   d) Klicken Sie auf **Zugriff und Sicherheit**.

   e) Klicken Sie auf das + Zeichen neben dem Dropdownmenü **Schlüsselpaar** und geben Sie Werte für die angezeigten Parameter an.

   f) Fügen Sie den Inhalt des öffentlichen Schlüssels in das Feld *Öffentlicher Schlüssel* ein, geben Sie dem Schlüssel einen Namen und klicken Sie auf **Schlüsselpaar importieren**.



6. Klicken Sie im Assistenten auf die Registerkarte **Post-Creation**. Fügen Sie im Anpassungsskript den Inhalt der Benutzerdatendatei hinzu. Die Benutzerdatendatei enthält die IP-Adresse, Netmask- und Gateway-Details sowie Kundenskripte der VPX-Instanz.
7. Nachdem ein Schlüsselpaar ausgewählt oder importiert wurde, aktivieren Sie die Option config-drive und klicken Sie auf **Starten**.



Provisioning der VPX-Instanz mi OpenStack CLI

Folgen Sie diesen Schritten zum Provisioning einer VPX-Instanz mit OpenStack CLI.

1. Um ein Image aus qcow2 zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   openstack image create --container-format bare --property hw_disk_bus
   =ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX
   -ToT-Image
   ```

2. Um ein Image zum Erstellen einer Instanz auszuwählen, geben Sie den folgenden Befehl ein:

   ```
   openstack image list | more
   ```

3. Um eine Instanz eines bestimmten Flavor zu erstellen, geben Sie den folgenden Befehl ein, um eine Flavor-ID/Name von aus einer Liste auszuwählen:

   ```
   openstack flavor list
   ```

4. Um eine Netzwerkkarte an ein bestimmtes Netzwerk anzuhängen, geben Sie den folgenden Befehl ein, um eine Netzwerk-ID aus einer Netzwerkliste auszuwählen:

   ```
   openstack network list
   ```

5. Um eine Instanz zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   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
   ```

Abbildung 2: Die folgende Abbildung zeigt eine Beispielausgabe.

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

NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitstellen

October 17, 2024

Der Virtual Machine Manager ist ein Desktop-Tool zur Verwaltung von VM-Gästen. Es ermöglicht Ihnen, neue VM-Gäste und verschiedene Speichertypen zu erstellen und virtuelle Netzwerke zu verwalten. Sie können mit dem integrierten VNC-Viewer auf die grafische Konsole der VM-Gäste zugreifen und Leistungsstatistiken entweder lokal oder remote einsehen.

Nachdem Sie Ihre bevorzugte Linux-Distribution mit aktivierter KVM-Virtualisierung installiert haben, können Sie mit der Bereitstellung virtueller Maschinen fortfahren.

Wenn Sie den Virtual Machine Manager zur Bereitstellung einer NetScaler VPX-Instanz verwenden, haben Sie zwei Möglichkeiten:

- Geben Sie die IP-Adresse, das Gateway und die Netzmaske manuell ein
- Automatische Zuweisung der IP-Adresse, des Gateway und der Netzmaske (automatische Bereitstellung)

Sie können zwei Arten von Images verwenden, um eine NetScaler VPX-Instanz bereitzustellen:

- ROH

- QCOW2

Sie können ein NetScaler VPX-RAW-Image in ein QCOW2-Image konvertieren und die NetScaler VPX-Instanz bereitstellen. Um das RAW-Bild in ein QCOW2-Bild zu konvertieren, geben Sie den folgenden Befehl ein:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Beispiel:

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5
_nc.qcow
```

Eine typische NetScaler VPX-Bereitstellung auf KVM umfasst die folgenden Schritte:

- Überprüfung der Voraussetzungen für die automatische Provisioning einer NetScaler VPX-Instance
- Provisioning der NetScaler VPX-Instanz mithilfe eines RAW-Images
- Provisioning der NetScaler VPX-Instanz mithilfe eines QCOW2-Images
- Hinzufügen zusätzlicher Schnittstellen zu einer VPX-Instanz mithilfe von Virtual Machine Manager

Überprüfen Sie die Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz

Die automatische Bereitstellung ist eine optionale Funktion, bei der Daten vom CD-ROM-Laufwerk verwendet werden. Wenn diese Funktion aktiviert ist, müssen Sie die Management-IP-Adresse, die Netzwerkmaske und das Standard-Gateway der NetScaler VPX-Instanz bei der Ersteinrichtung nicht eingeben.

Sie müssen die folgenden Aufgaben ausführen, bevor Sie eine VPX-Instanz automatisch bereitstellen können:

1. Erstellen Sie eine benutzerdefinierte XML-Datei oder Benutzerdatendatei (Open Virtualization Format) (OVF).
2. Konvertieren Sie die OVF-Datei in ein ISO-Image mit einer Online-Anwendung (z. B.
3. Hängen Sie das ISO-Image auf dem KVM-Host mit beliebigen Secure Copy (SCP) -basierten Tools ein.

Beispiel für OVF-XML-Datei:

Hier ist ein Beispiel für den Inhalt einer OVF-XML-Datei, die Sie als Beispiel verwenden können, um Ihre Datei zu erstellen.

```
1    <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
```



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

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

oe:id=""

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

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

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

<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>

<Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
   />

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
   10.1.2.1"/>

</PropertySection>

</Environment>
```

In der vorangehenden OVF-XML-Datei wird “PropertySection”für die NetScaler-Netzwerkkonfiguration verwendet. Wenn Sie die Datei erstellen, geben Sie Werte für die Parameter an, die am Ende des Beispiels hervorgehoben werden:

- Verwaltungs-IP-Adresse
- Netzmaske
- Gateway

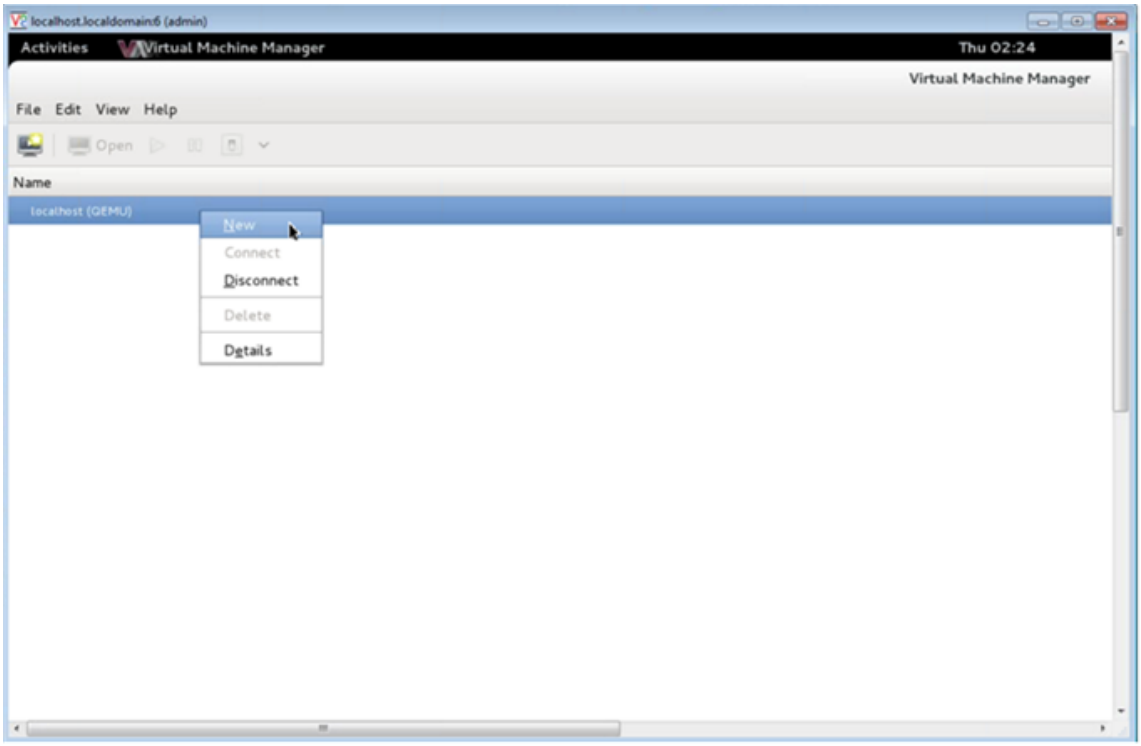
> **Wichtig!**
>
> Wenn die OVF-Datei nicht richtig XML-formatiert ist, wird der VPX-Instanz die Standard-Netzwerkkonfiguration zugewiesen, nicht die in der Datei angegebenen Werte.

Stellen Sie die NetScaler VPX-Instanz mithilfe eines RAW-Images bereit

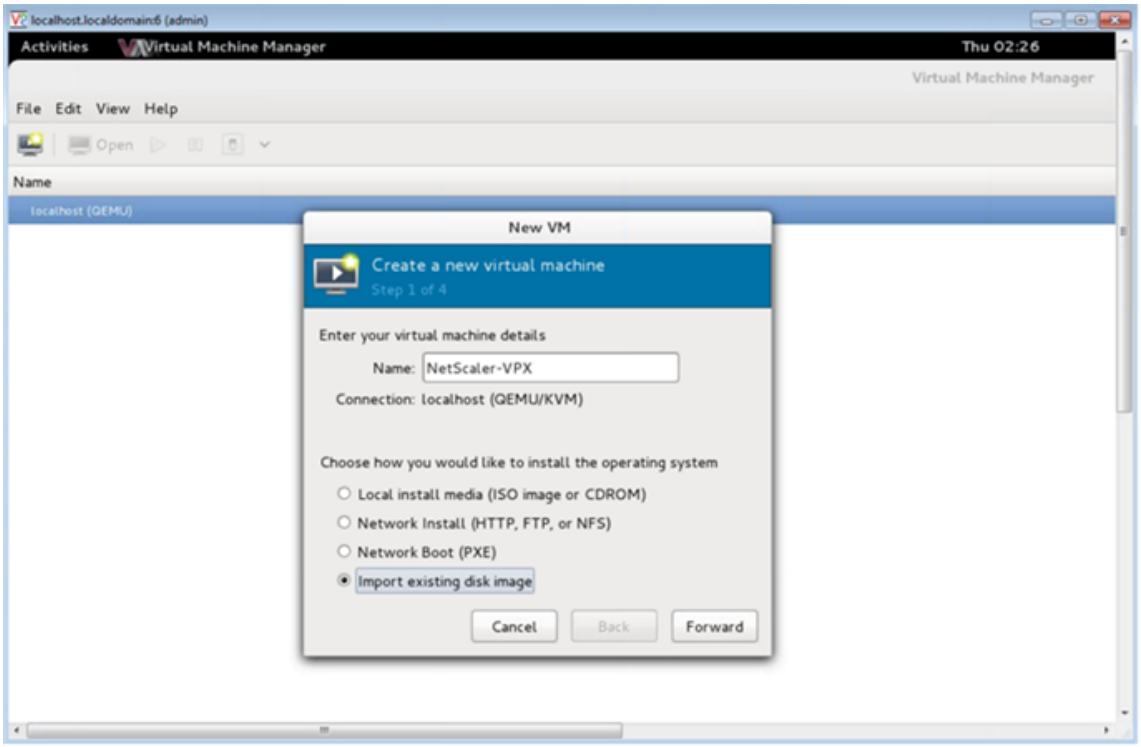
Mit dem Virtual Machine Manager können Sie eine NetScaler VPX-Instanz mithilfe eines RAW-Images bereitstellen.

Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitzustellen:

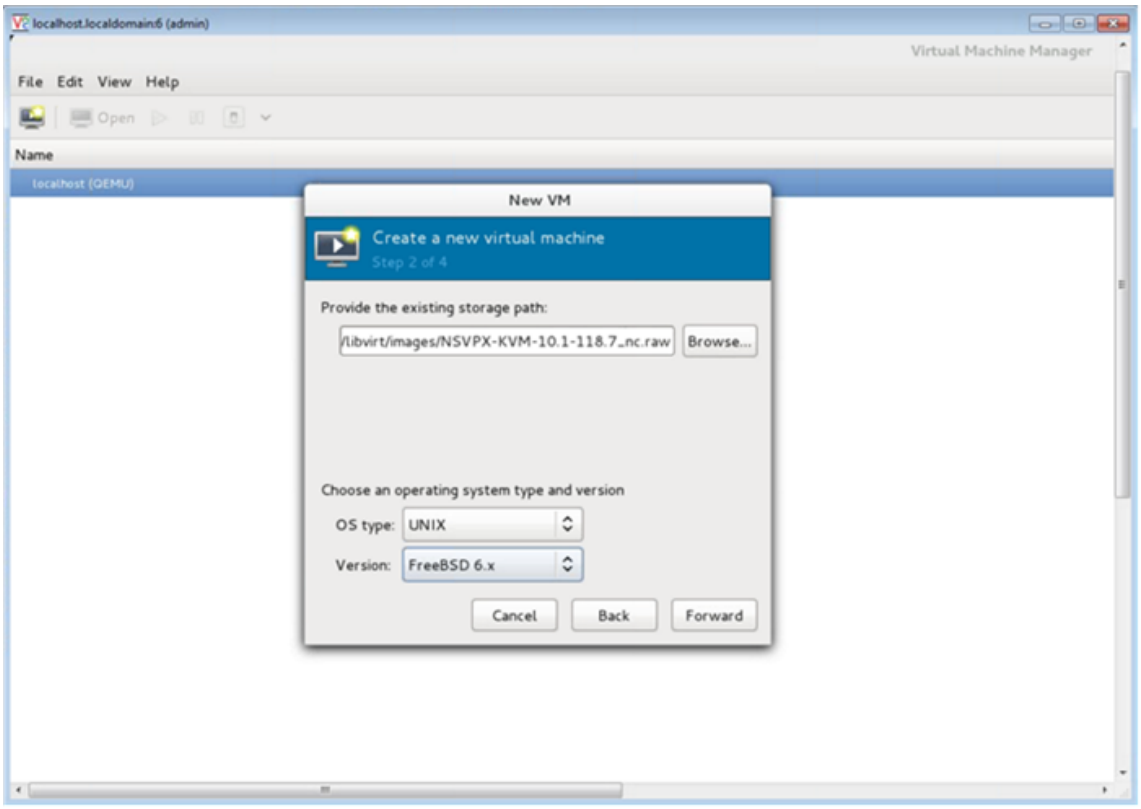
1. Öffnen Sie den Virtual Machine Manager (**Anwendung** > **Systemprogramme** > **Virtual Machine Manager**), und geben Sie die Anmeldeinformationen im Fenster **Authentifizieren** ein.
2. Klicken Sie auf das  oder klicken Sie mit der rechten Maustaste auf **localhost (QEMU)**, um eine neue NetScaler VPX-Instanz zu erstellen.



3. Geben Sie im Textfeld **Name** einen Namen für die neue VM ein (z. B. NetScaler-VPX).
4. Wählen Sie im Fenster **Neue virtuelle Maschine** unter „Wählen Sie aus, wie Sie das Betriebssystem installieren möchten“die Option **Vorhandenes Festplatten-Image importieren**und klicken Sie dann auf **Weiterleiten**.

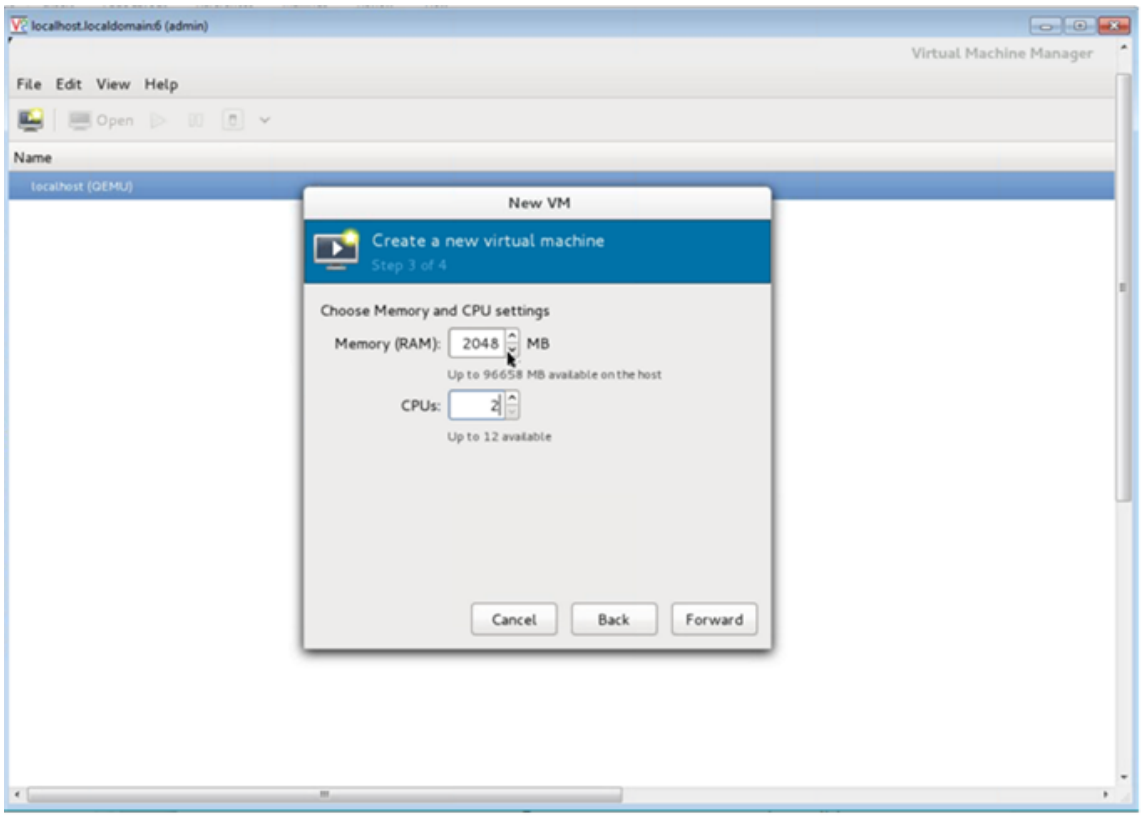


5. Navigieren **Sie im Feld Vorhandenen Speicherpfad angeben** zum Pfad zum Image. Wählen Sie den Betriebssystemtyp UNIX und die Version FreeBSD 6.x. Klicken Sie dann auf **Weiterleiten**. Klicken Sie dann auf **Weiter**.

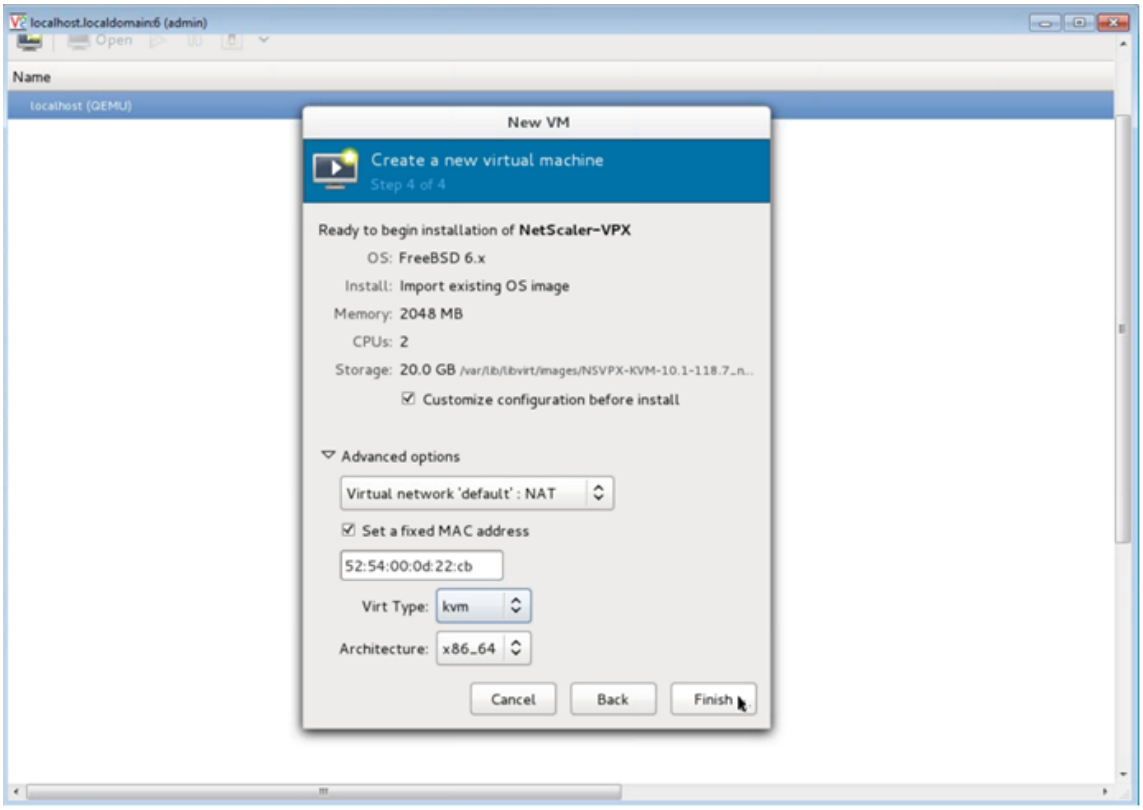


6. **Wählen Sie unter Speicher- und CPU-Einstellungen** auswählen die folgenden Einstellungen aus, und klicken Sie dann auf **Weiterleiten**:

   - Speicher (RAM) —2048 MB
   - CPUs —2

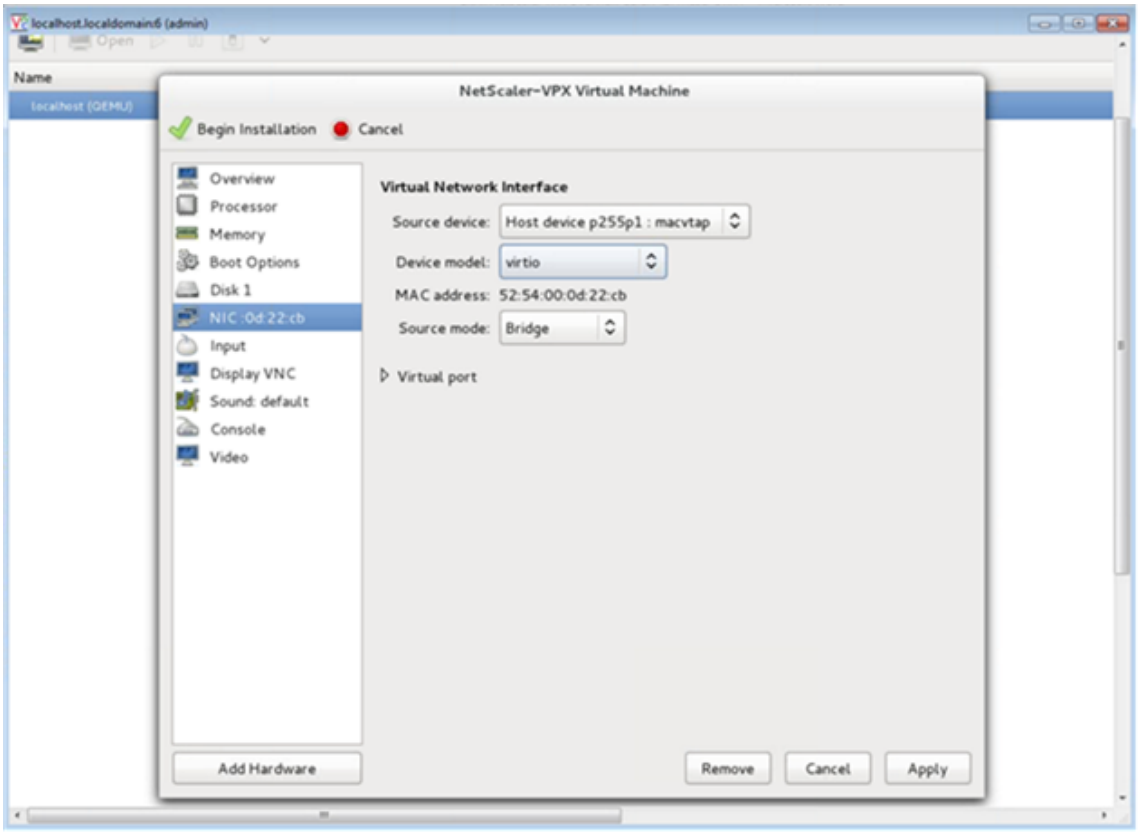


7. Aktivieren Sie das Kontrollkästchen **Konfiguration vor der Installation anpassen** . Optional können Sie unter **Erweiterte Optionen** die MAC-Adresse anpassen. Stellen Sie sicher, dass der ausgewählte **Virt-Typ** KVM ist und die ausgewählte Architektur x86_64 ist. Klicken Sie auf **Fertig stellen**.



8. Wählen Sie eine Netzwerkkarte aus, und stellen Sie die folgende Konfiguration bereit:

   - Quellgerät- `ethX macvtap` oder Bridge
   - Geräte-Modell—`virtio`
   - Quellmodus—Brücke



9. Klicken Sie auf **Übernehmen**.
10. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt **Aktivieren der automatischen Provisioning durch Anhängen eines CD-ROM-Laufwerks** in diesem Dokument. Klicken Sie andernfalls auf **Installation beginnen**. Nachdem Sie den NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Bereitstellen der NetScaler VPX Instanz mithilfe eines QCOW2-Images

Mit dem Virtual Machine Manager können Sie die NetScaler VPX-Instanz mithilfe eines QCOW2-Images bereitstellen.

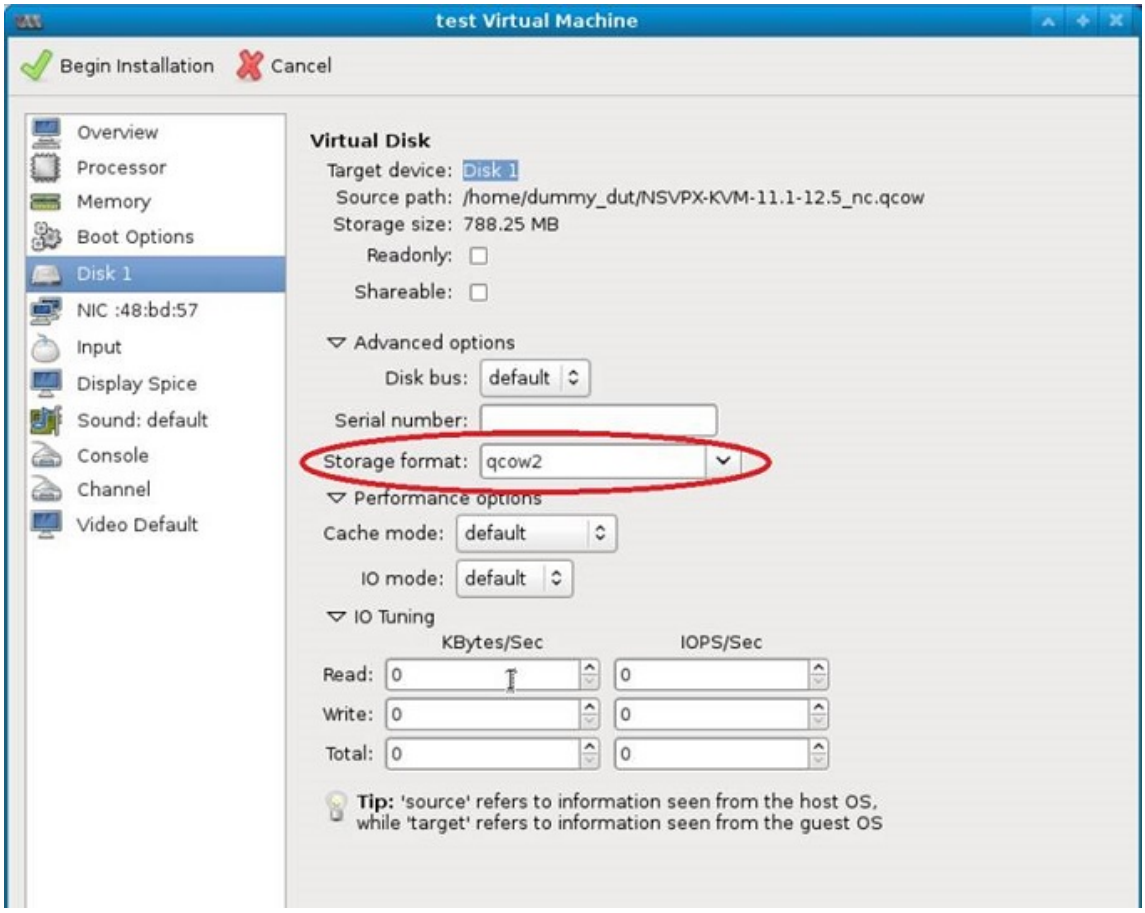
Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mit einem QCOW2-Image bereitzustellen:

1. Folgen Sie **Schritt 1** bis **Schritt 8** unter Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass Sie in **Schritt 5**das Bild **qcow2** auswählen.

2. Wählen Sie **Disk 1** und klicken Sie auf **Erweiterte Optionen**.

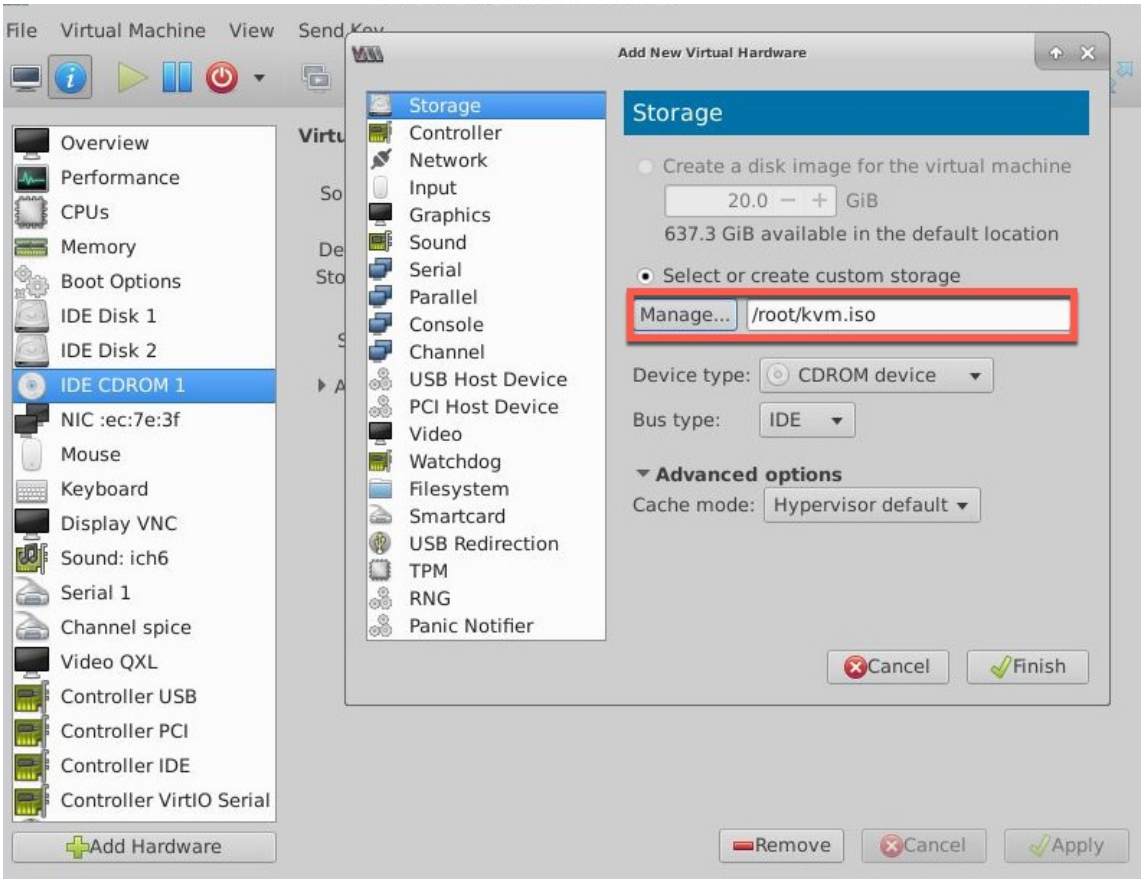
3. Wählen Sie **qcow2** aus der Dropdownliste Speicherformat aus.



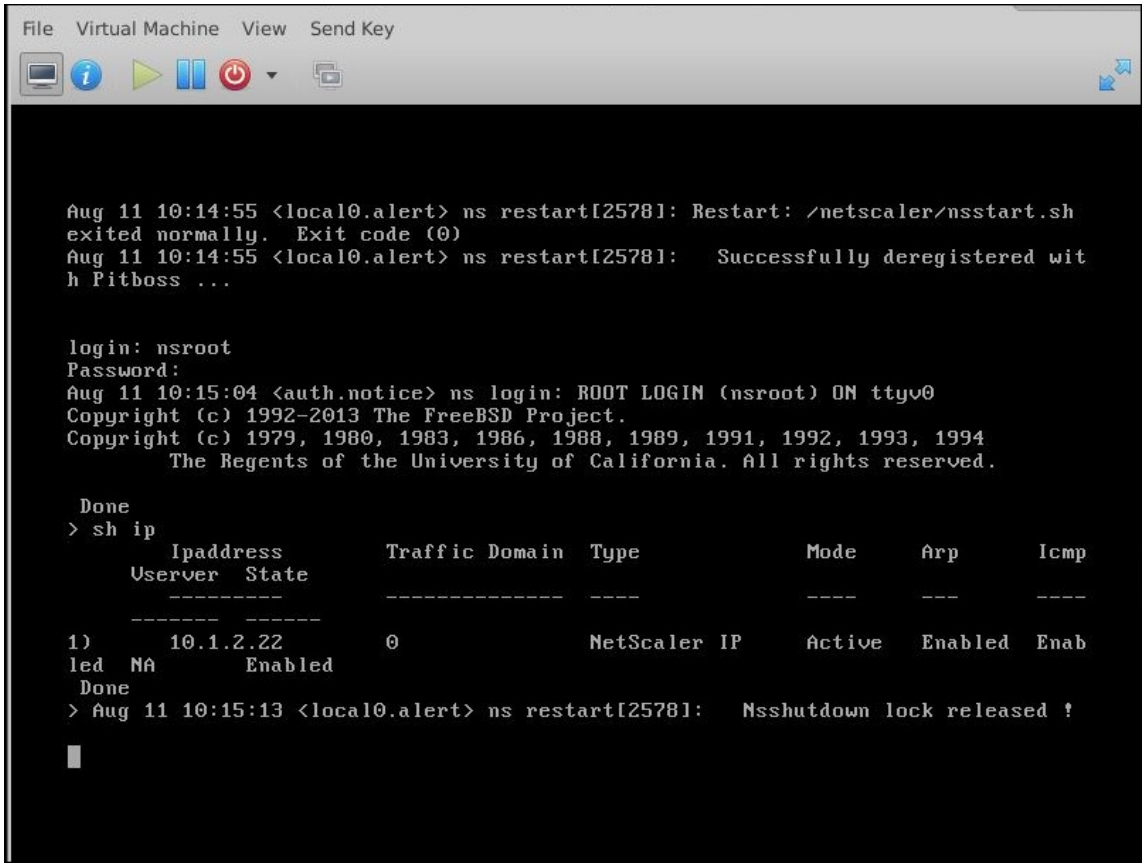
4. Klicken Sie auf **Übernehmen**, und klicken Sie dann auf **Installation beginnen**. Nachdem Sie den NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Aktivieren der automatischen Bereitstellung durch Anfügen eines CD-ROM-Laufwerks

1. Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
2. Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus, die Sie im Abschnitt "Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz"bereitgestellt haben, und klicken Sie auf **Fertig stellen**. Eine neue CD-ROM unter Resources auf Ihrer NetScaler VPX-Instanz wird erstellt.



3. Schalten Sie die VPX-Instanz ein und stellt automatisch die in der OVF-Datei bereitgestellte Netzwerkkonfiguration bereit, wie in der Beispielbildaufnahme gezeigt.



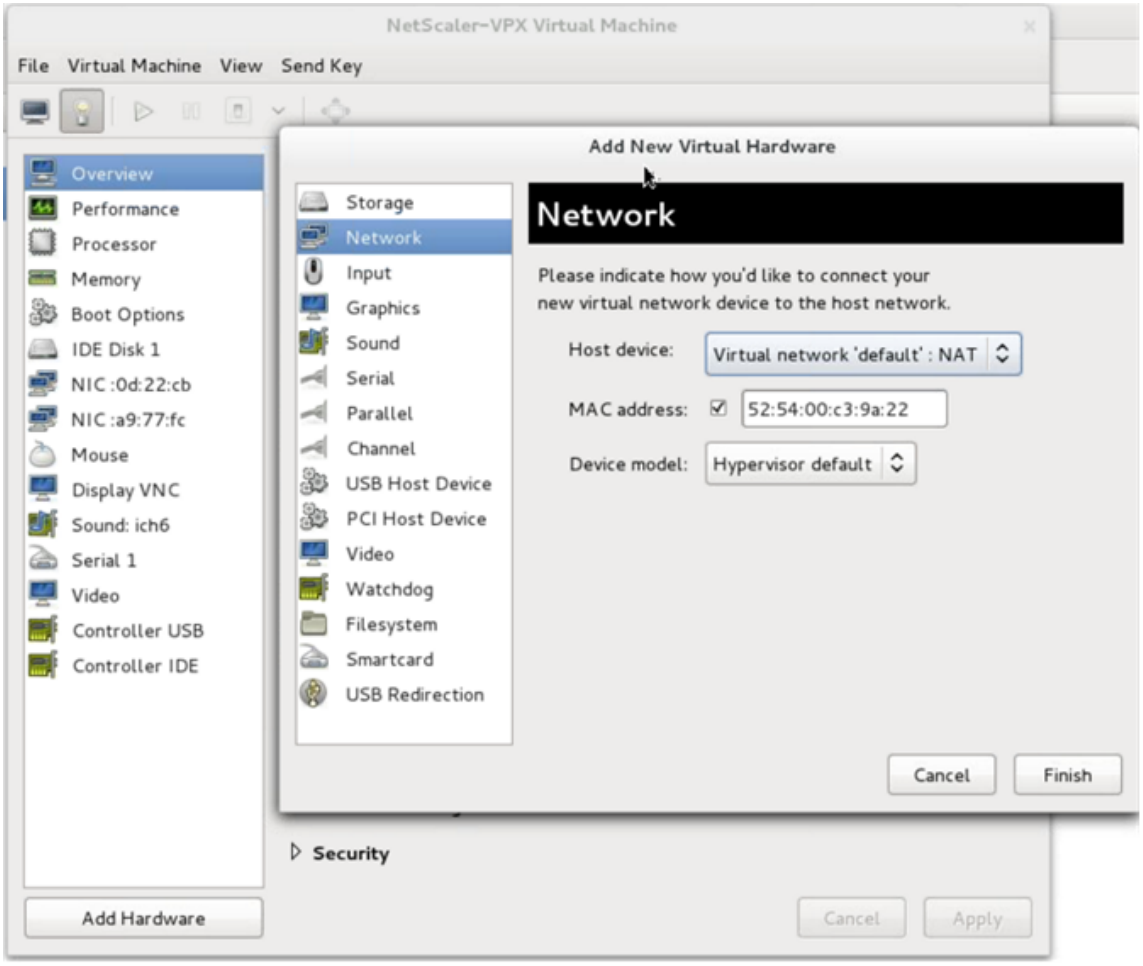
4. Wenn die automatische Bereitstellung fehlschlägt, wird die Instanz die Standard-IP-Adresse (192.168.100.1) angezeigt. In diesem Fall müssen Sie die Erstkonfiguration manuell abschließen. Weitere Informationen finden Sie unter Konfigurieren des ADC zum ersten Mal.

Fügen Sie der NetScaler VPX-Instanz weitere Schnittstellen hinzu, indem Sie den Virtual Machine Manager verwenden

Nachdem Sie die NetScaler VPX-Instanz auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen.

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf der KVM ausgeführt wird.
2. Klicken Sie mit der rechten Maustaste auf die VPX-Instanz und wählen Sie **Öffnen** aus dem Popup-Menü.
3. Klicken Sie auf das  in der Kopfzeile, um die Details der virtuellen Hardware anzuzeigen.
4. Klicken Sie auf **Hardware hinzufügen**. Wählen **Sie im Fenster Neue virtuelle Hardware hinzufügen**im Navigationsmenü die Option **Netzwerk** aus.



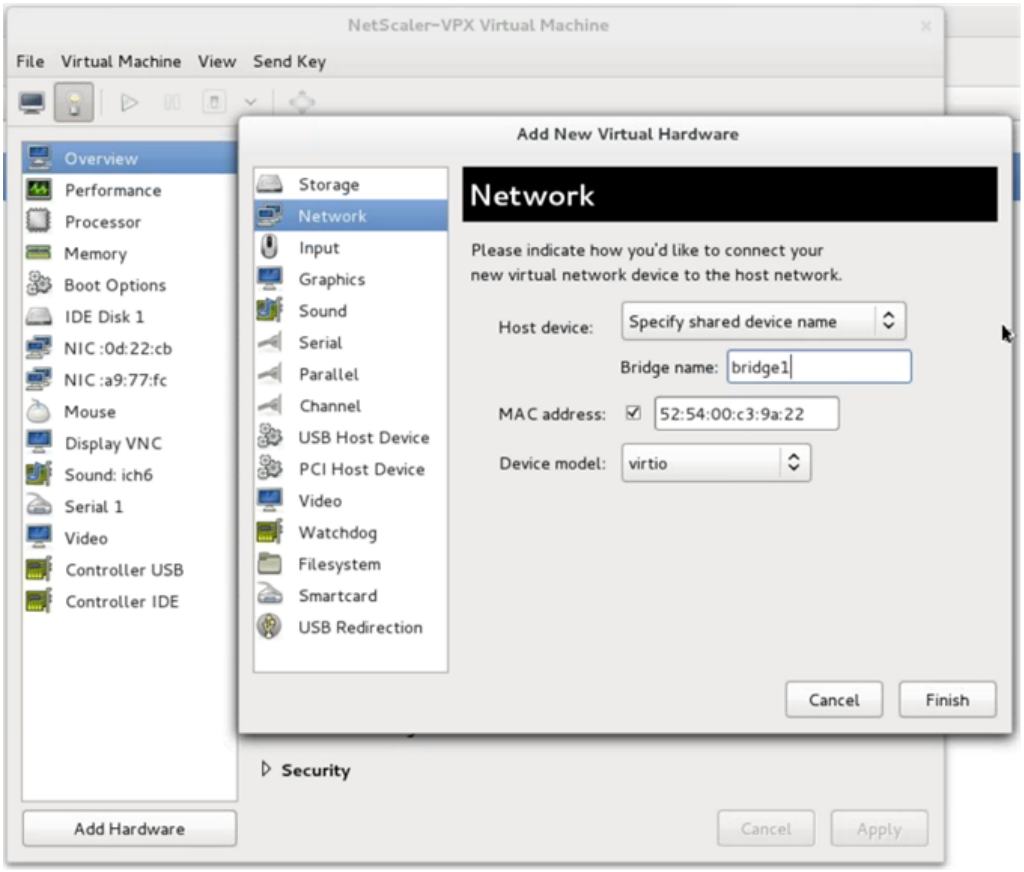
5. Wählen Sie im Feld **Host-Gerät** den physischen Schnittstellentyp aus. Der Hostgerätetyp kann entweder Bridge oder MacVTap sein. Im Falle von MacVTap sind VEPA, Bridge, Private und Pass-Through vier Modi möglich.

    a) Für Brücke

        i. Host-Gerät —Wählen Sie die Option „Namen des gemeinsam genutzten Geräts angeben“.

        ii. Geben Sie den Bridge-Namen ein, der auf dem KVM-Host konfiguriert ist.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie im KVM-Host eine Linux-Bridge konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den Status „UP “versetzt haben.



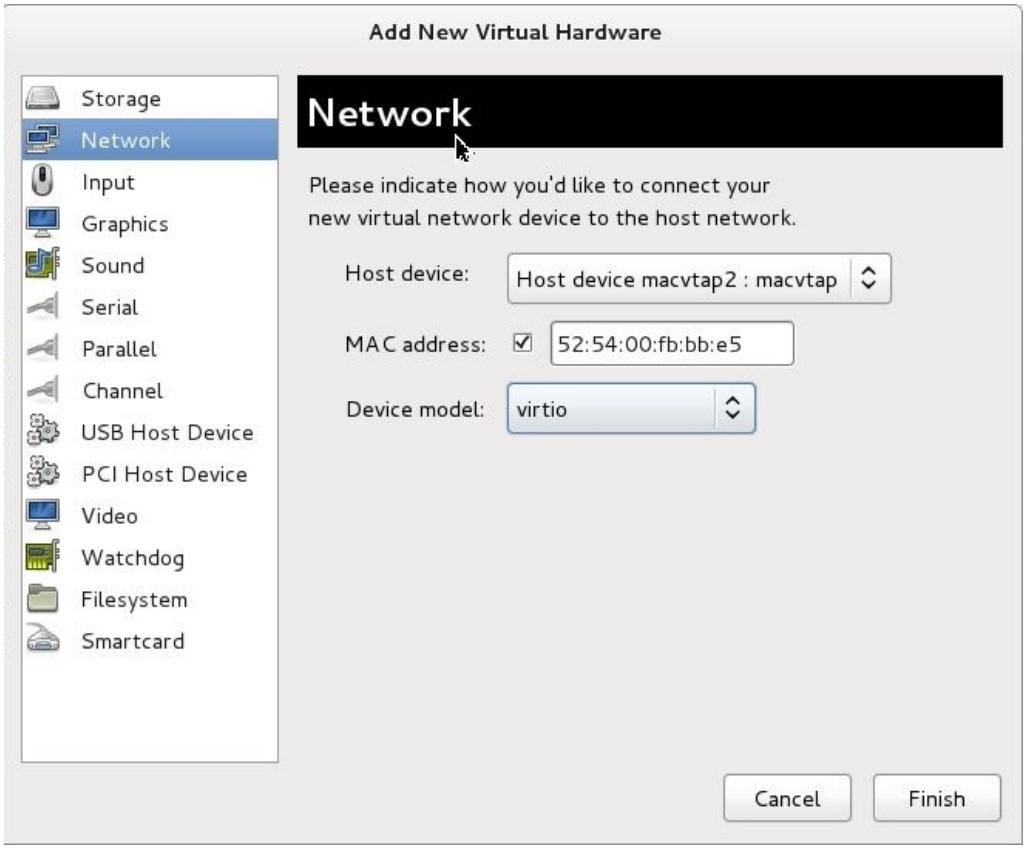
iii. Gerätemodell—`virtio`.

iv. Klicken Sie auf **Fertig stellen**.

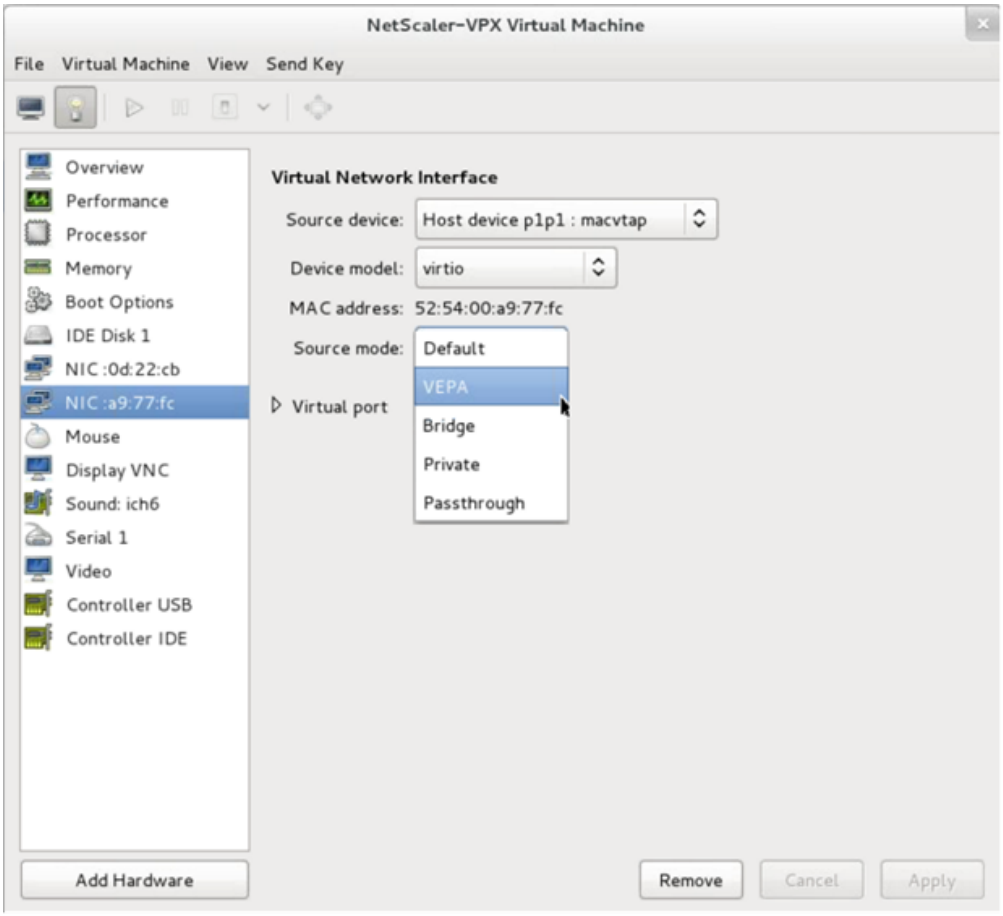
b) Für MacVtap

i. Hostgerät —Wählen Sie die physische Schnittstelle aus dem Menü aus.

ii. Gerätemodell—`virtio`.



iii. Klicken Sie auf **Fertig stellen**. Sie können die neu hinzugefügte NIC im Navigationsbereich anzeigen.



iv. Wählen Sie die neu hinzugefügte NIC und wählen Sie den Quellmodus für diese NIC. Die verfügbaren Modi sind VEPA, Bridge, Private und Passthrough. Weitere Informationen zur Benutzeroberfläche und den Modi finden Sie unter Quellschnittstelle und Modi.

v. Klicken Sie auf **Übernehmen**.

6. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt „Hinzufügen eines Konfigurationslaufwerks zur Aktivierung der automatischen Provisioning“in diesem Dokument. Andernfalls schalten Sie die VPX-Instanz ein, um die Erstkonfiguration manuell abzuschließen.

> **Wichtig:**
>
> Konfigurationen von Schnittstellenparametern wie Geschwindigkeit, Duplex und Autonegotiation werden nicht unterstützt.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen

October 17, 2024

Sie können eine NetScaler VPX-Instanz konfigurieren, die auf einer Linux-KVM-Plattform ausgeführt wird, mithilfe der Single-Root-I/O-Virtualisierung (SR-IOV) mit den folgenden Netzwerkkarten:

- Intel 82599 10 G
- Intel X710 10 G
- Intel XL710 40 G
- Intel X722 10G

In diesem Abschnitt wird beschrieben, wie Sie:

- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle
- Statisches LA/LACP auf der SR-IOV-Schnittstelle konfigurieren
- VLAN auf der SR-IOV-Schnittstelle konfigurieren

Einschränkungen

Beachten Sie die Einschränkungen bei der Verwendung von Intel 82599-, X710-, XL710- und X722-NICs. Die folgenden Funktionen werden nicht unterstützt.

Einschränkungen für Intel 82599 NIC:

- L2-Moduswechsel.
- Admin-Partitionierung (gemeinsam genutzter VLAN-Modus).
- Hohe Verfügbarkeit (aktiv-aktiver Modus).
- Jumbo-Rahmen.
- IPv6: Sie können nur bis zu 30 eindeutige IPv6-Adressen in einer VPX-Instanz konfigurieren, wenn Sie mindestens eine SR-IOV-Schnittstelle haben.
- Die VLAN-Konfiguration auf Hypervisor für SRIOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiationen werden nicht unterstützt.

Einschränkungen für Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs:

- L2-Moduswechsel.
- Admin-Partitionierung (gemeinsam genutzter VLAN-Modus).

- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710-NIC als Datenschnittstelle verwendet wird.
- Die Schnittstellenliste ordnet neu an, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und automatische Absprache werden nicht unterstützt.
- Der Schnittstellenname ist 40/X für Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs
- Bis zu 16 Intel XL710/X710/X722 SRIOV- oder PCI-Passthrough-Schnittstellen können auf einer VPX-Instance unterstützt werden.

> **Hinweis:**
>
> Damit die Netzwerkkarten Intel X710 10G, Intel XL710 40G und Intel X722 10G IPv6 unterstützen, müssen Sie den Vertrauensmodus für die virtuellen Funktionen (VFs) aktivieren, indem Sie den folgenden Befehl auf dem KVM-Host eingeben:
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> Beispiel
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```

Voraussetzungen

Bevor Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren, müssen Sie die folgenden erforderlichen Aufgaben ausführen. Einzelheiten zur Ausführung der entsprechenden Aufgaben finden Sie in der Spalte NIC.

Aufgabe	Intel 82599 NIC	Intel X710-, XL710- und X722-Netzwerkkarten
1. Fügen Sie die Netzwerkkarte zum KVM-Host hinzu.	-	-
1. Laden Sie den neuesten Intel-Treiber herunter und installieren Sie ihn.	IXGBE-Treiber	I40E-Treiber

Aufgabe	Intel 82599 NIC	Intel X710-, XL710- und X722-Netzwerkkarten
1. Setzen Sie den Treiber auf dem KVM-Host auf die Blockliste.	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist ixgbevf`. Verwenden Sie die IXGBE-Treiberversion 4.3.15 (empfohlen).	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist i40evf`. Verwenden Sie die i40e-Treiberversion 2.0.26 (empfohlen).
4.Aktivieren Sie virtuelle SR-IOV-Funktionen (VFs) auf dem KVM-Host. In beiden Befehlen in den nächsten beiden Spalten: `number_of_VFs` = die Anzahl der virtuellen VFs, die Sie erstellen möchten. `device_name` = der Name der Schnittstelle.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/i40e.conf den folgenden Eintrag hinzu und starten Sie den KVM-Host neu:. `options i40e max_vfs =<number_of_VFs>` Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo< number_of_VFs> > /sys/class/net/< device_name>/ device/sriov_numvfs`. Siehe Beispiel in Abbildung 2.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/ixgbe den folgenden Eintrag hinzu und starten Sie den KVM-Host neu: `options ixgbe max_vfs =<number_of_VFs>` Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo < number_of_VFs> > /sys/class/net/< device_name>/ device/sriov_numvfs`. Wenn Sie Kernel-Version 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo< number_of_VFs> > /sys/class/net/< device_name>/ device/sriov_numvfs`. Siehe Beispiel in Abbildung 1.

Aufgabe	Intel 82599 NIC	Intel X710-, XL710- und X722-Netzwerkkarten
1. Machen Sie die VFs persistent, indem Sie die Befehle, die Sie zum Erstellen der VFs verwendet haben, zur Datei rc.local hinzufügen.	Siehe Beispiel in Abbildung 3.	Siehe Beispiel in Abbildung 3.

> **Wichtig:**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

Abbildung 1: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für die Intel 82599 10G-NIC.

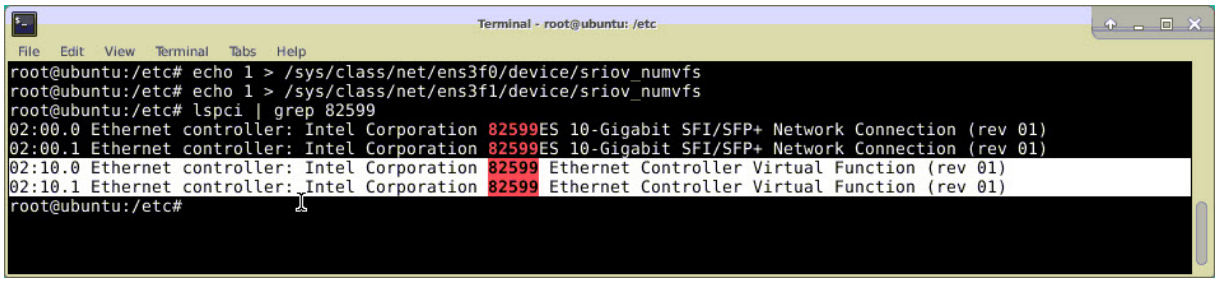


Abbildung 2: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel X710 10G- und XL710 40G-NICs.

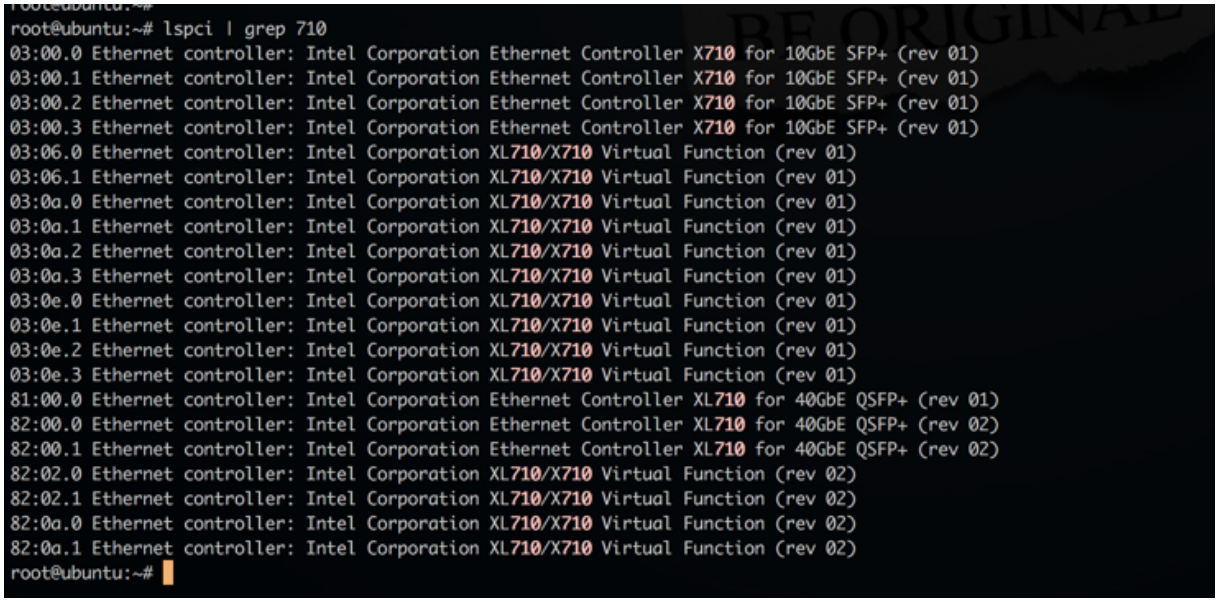
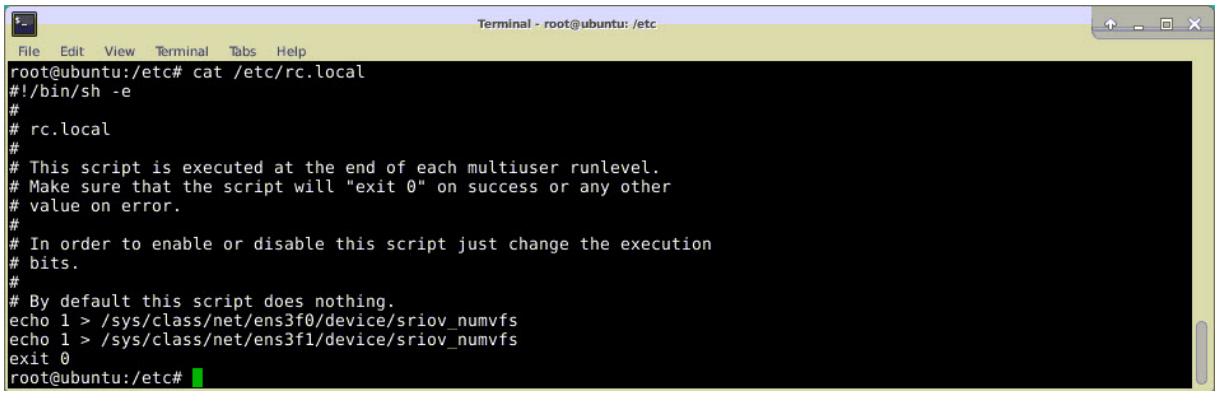


Abbildung 3: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für die Intel X722 10G-NIC.


```
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)
```

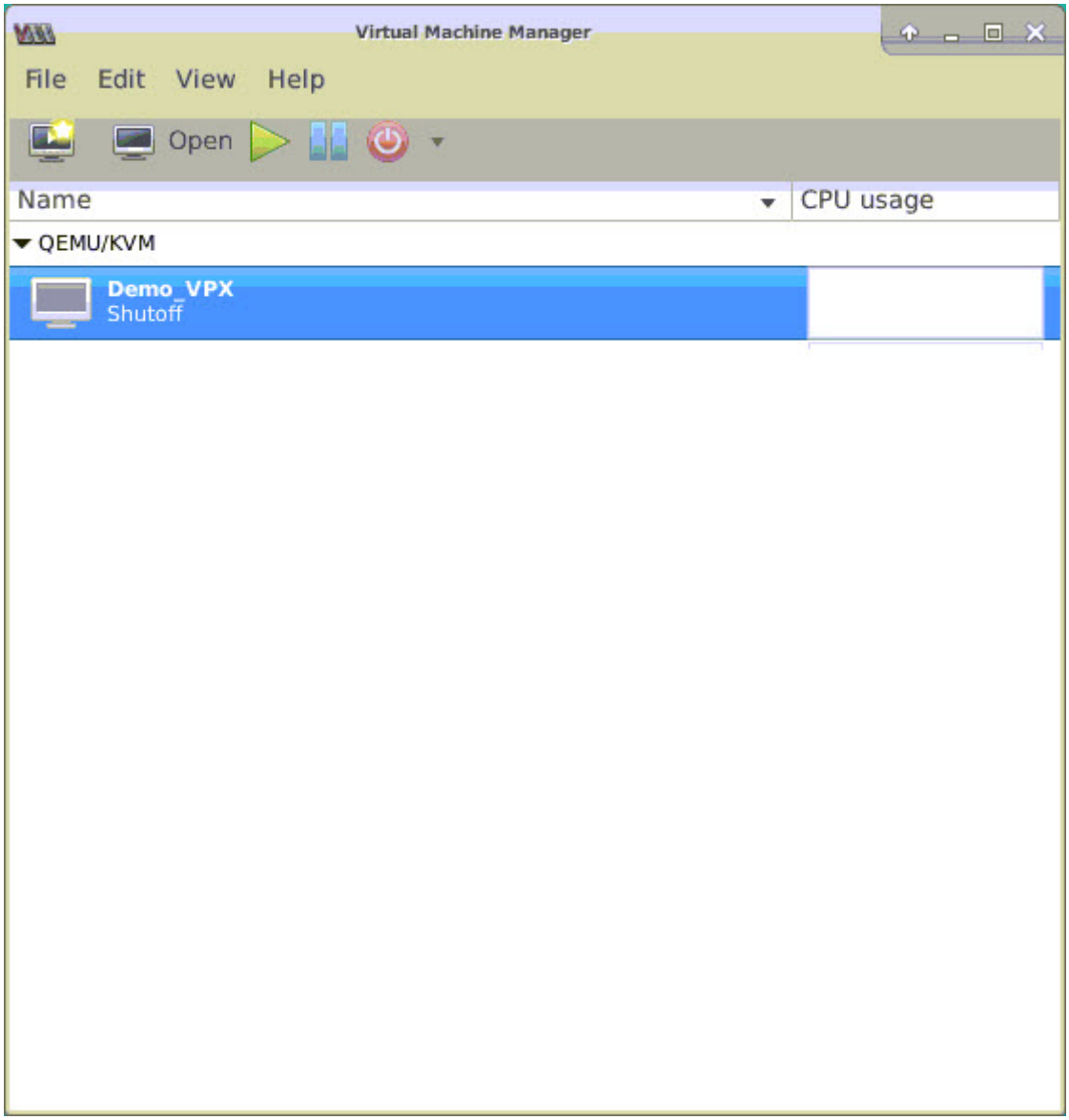
Abbildung 4: Machen Sie die VFs persistent.



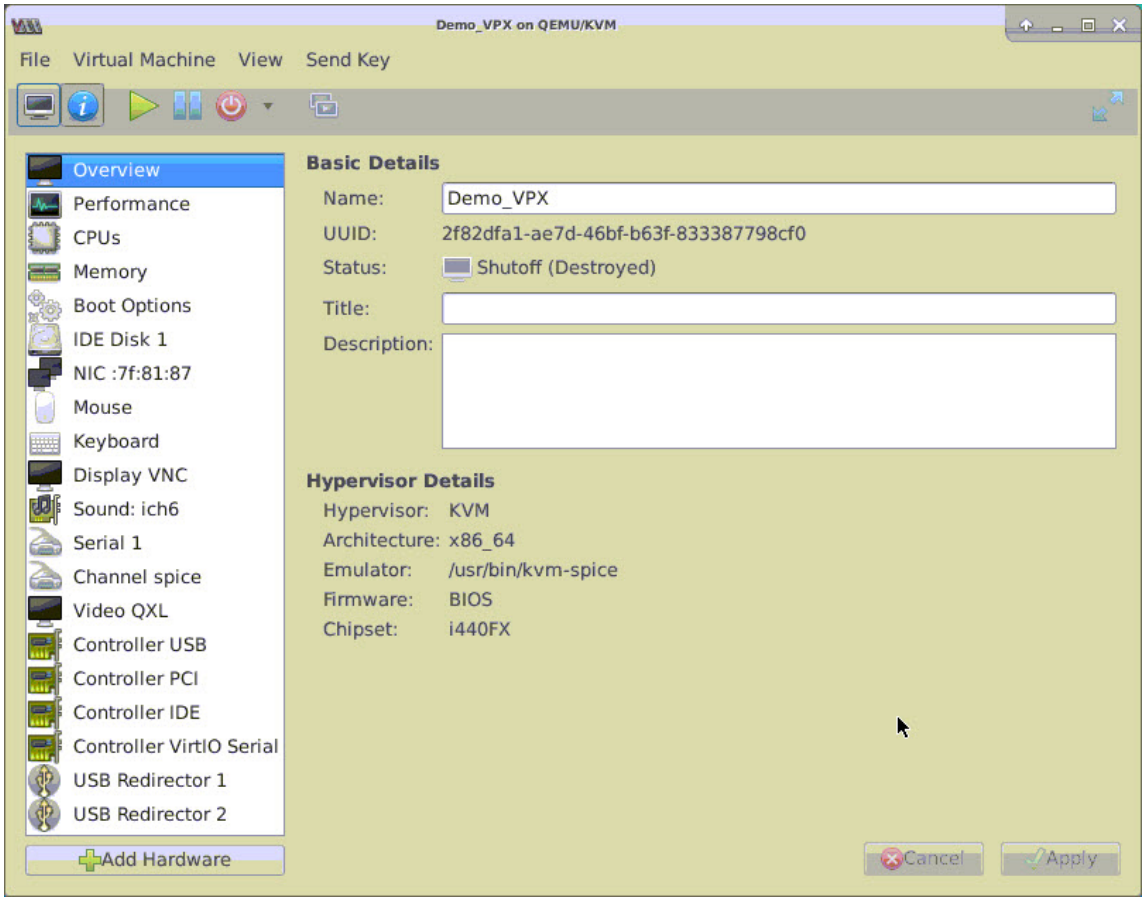
Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

Führen Sie die folgenden Schritte aus, um die NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle mit Virtual Machine Manager zu konfigurieren:

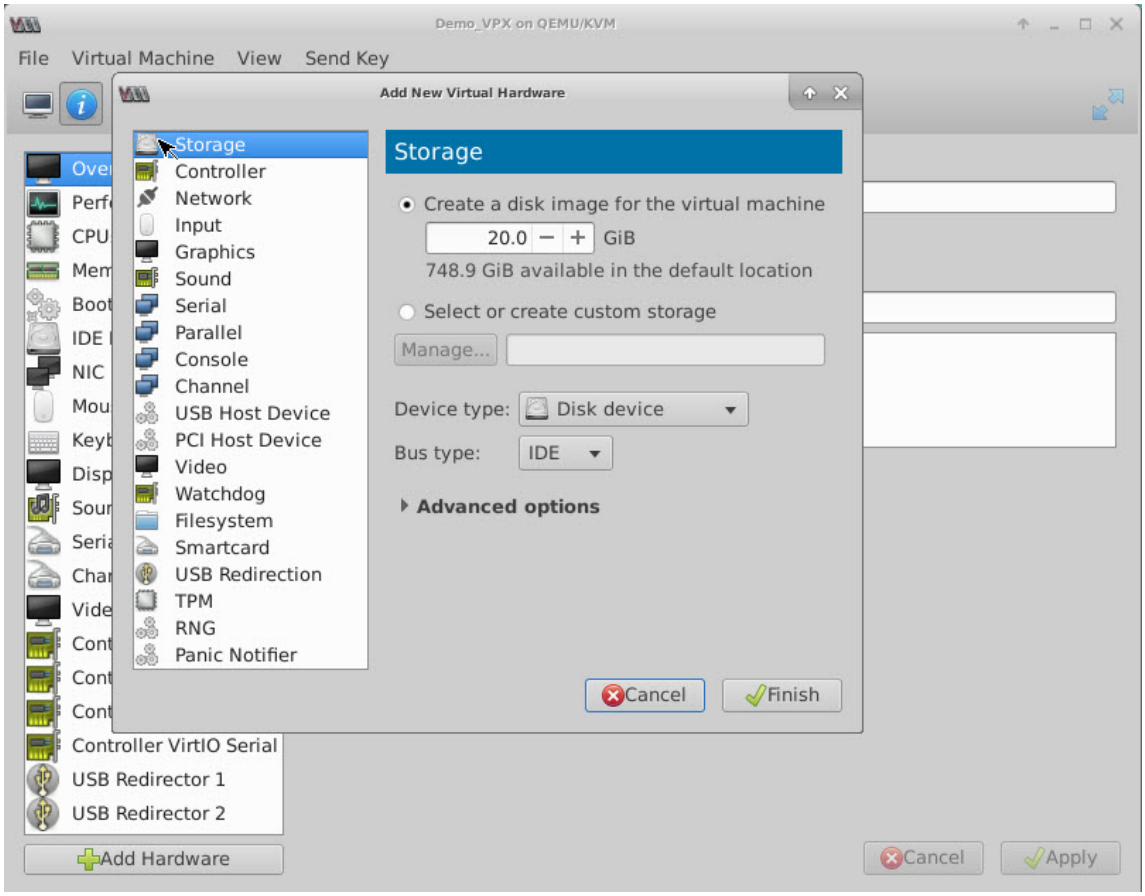
1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz und dann Öffnen aus.



3. <virtual machine on KVM>Wählen Sie im Fenster das **I-Symbol** aus.



4. Wählen Sie **Hardware hinzufügen**aus.



5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a) Wählen Sie PCI-Host-Gerätaus.
   b) Wählen Sie im Abschnitt Host-Gerät das VF aus, das Sie erstellt haben, und klicken Sie auf Fertig stellen.

Abbildung 4: VF für Intel 82599 10G-NIC

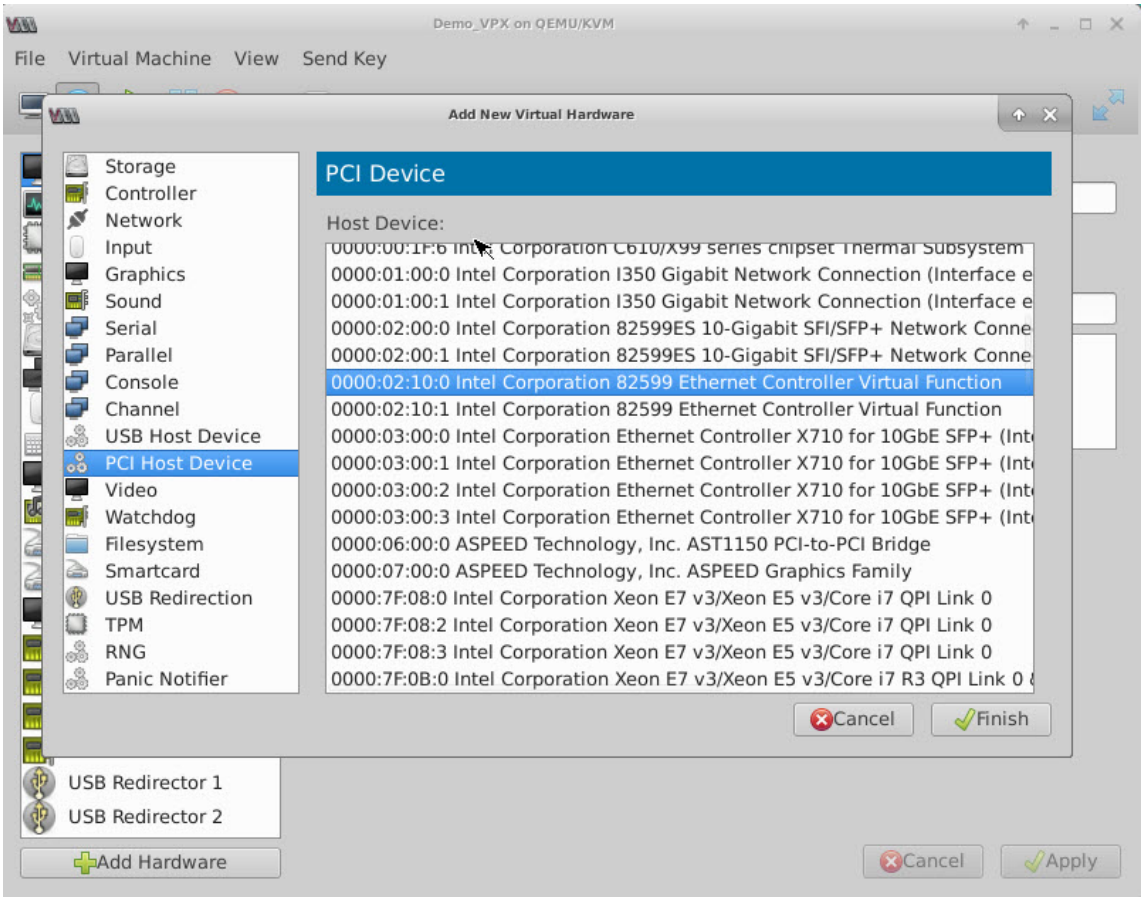


Abbildung 5: VF für Intel XL710 40G NIC

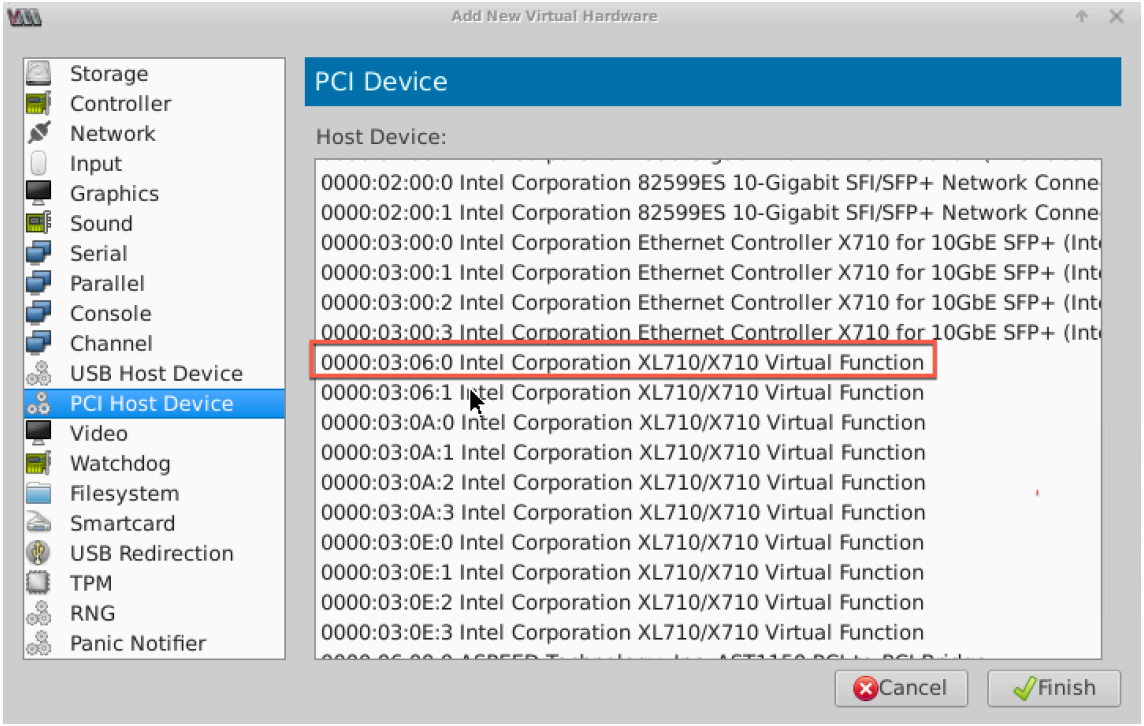
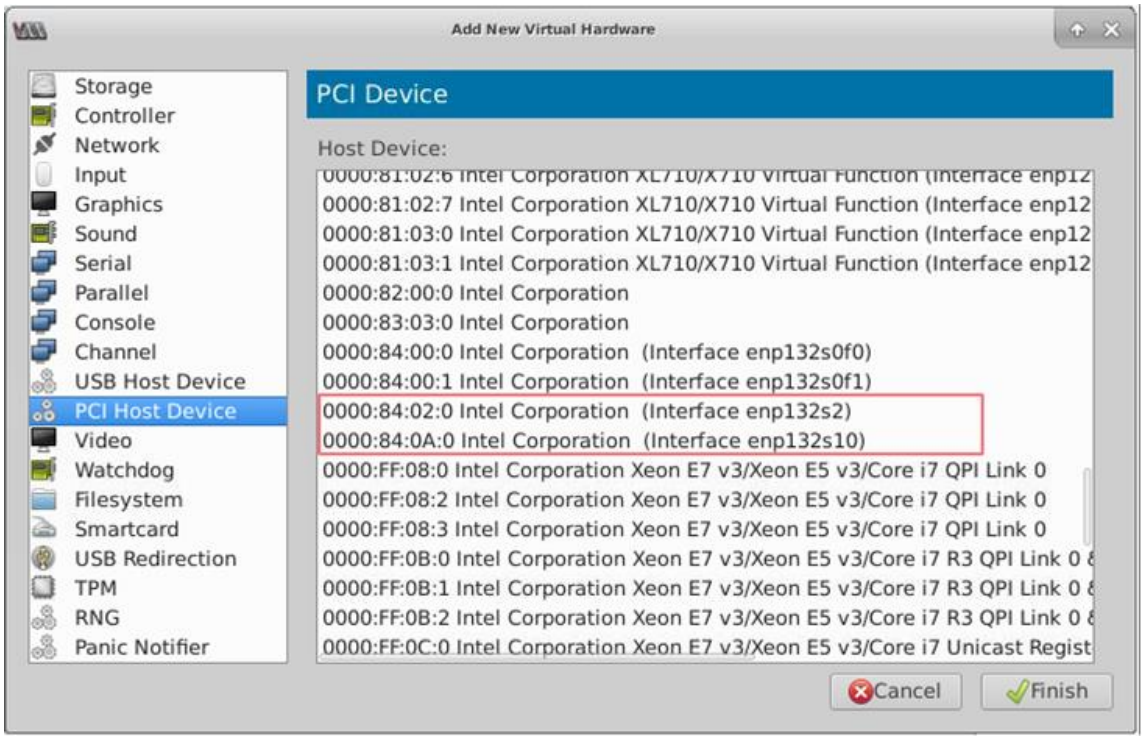


Abbildung 6: VF für Intel X722 10G-NIC



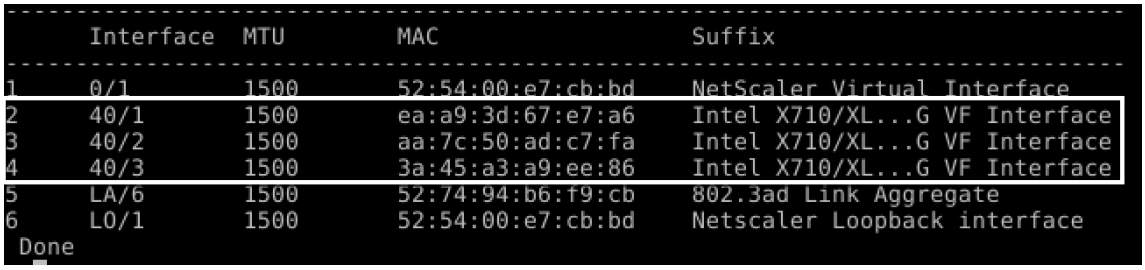
6. Wiederholen Sie die Schritte 4 und 5, um die von Ihnen erstellten VFs hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Verwenden Sie nach dem Einschalten der NetScaler VPX-Instanz den folgenden Befehl, um die Konfiguration zu überprüfen:

```
1    show interface summary
```

Die Ausgabe zeigt alle Schnittstellen, die Sie konfiguriert haben.

Abbildung 6: Zusammenfassung der Ausgabe für Intel 82599 NIC.

Abbildung 7. Entfernen einer bestehenden SSD ohne RAID **Abbildung 7.** Zusammenfassung der Ausgangsdaten für Intel X710- und XL710-NICs.



Konfigurieren Sie statisches LA/LACP auf der SR-IOV-Schnittstelle

> **Wichtig:**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

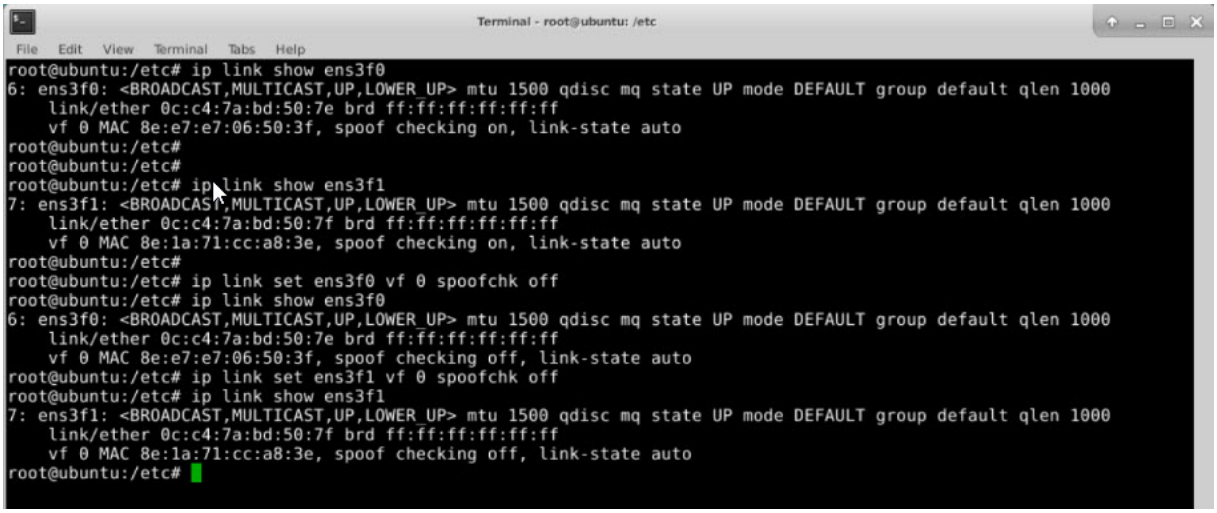
Um die SR-IOV-VFs im Link-Aggregationsmodus zu verwenden, deaktivieren Sie die Spoof-Prüfung für von Ihnen erstellte VFs. Verwenden Sie auf dem KVM-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

```
*ip link set \\&#060;interface\\_name\\&#062; vf \\&#060;VF\\_id
\\&#062; spoofchk off*
```

Ort:

- interface_name —ist der Schnittstellenname.
- vf_ID —ist die virtuelle Funktions-ID.

Beispiel:



Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten VFs deaktiviert haben. Starten Sie die NetScaler VPX-Instanz neu, und konfigurieren Sie die Linkaggregation. Ausführliche Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN auf SR-IOV-VFs konfigurieren. Ausführliche Anweisungen finden Sie unter Konfigurieren eines VLANs.

> **Wichtig:**
>
> Stellen Sie sicher, dass der KVM-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Konfigurieren Sie einen NetScaler VPX auf dem KVM-Hypervisor, um Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus zu verwenden

October 17, 2024

Die NetScaler VPX-Instanz auf dem Linux-KVM-Hypervisor kann die Intel QuickAssist Technology (QAT) verwenden, um die NetScaler SSL-Leistung zu beschleunigen. Mithilfe von Intel QAT kann die gesamte Kryptoverarbeitung mit hoher Latenz auf den Chip verlagert werden, sodass eine oder mehrere Host-CPUs für andere Aufgaben frei werden.

Zuvor wurde die gesamte Kryptoverarbeitung von NetScaler-Datenpfaden in der Software mithilfe von Host-vCPUs durchgeführt.

> **Hinweis:**
>
> Derzeit unterstützt NetScaler VPX nur das C62x-Chipmodell der Intel QAT-Familie. Diese Funktion wird ab NetScaler Version 14.1 Build 8.50 unterstützt.

Voraussetzungen

- Der Linux-Host ist mit einem Intel QAT C62x-Chip ausgestattet, der entweder direkt in das Motherboard integriert oder auf einer externen PCI-Karte hinzugefügt ist.

  Modelle der Intel QAT C62x-Serie: C625, C626, C627, C628. Nur diese C62x-Modelle verfügen über die Funktion Public Key Encryption (PKE). Andere C62x-Varianten unterstützen PKE nicht.

- Der NetScaler VPX erfüllt die VMware ESX-Hardwareanforderungen. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz auf einer Linux KVM-Plattform.

Einschränkungen

Es ist nicht vorgesehen, Kryptoeinheiten oder Bandbreite für einzelne VMs zu reservieren. Alle verfügbaren Kryptoeinheiten jeder Intel QAT-Hardware werden von allen VMs gemeinsam genutzt, die die QAT-Hardware verwenden.

Richten Sie die Host-Umgebung für die Verwendung von Intel QAT ein

1. Laden Sie den von Intel bereitgestellten Treiber für das Chipmodell der C62x-Serie (QAT) herunter und installieren Sie ihn auf dem Linux-Host. Weitere Informationen zu den Paket-Downloads und Installationsanweisungen von Intel finden Sie unter Treiber für die Intel QuickAssist-Technologie für Linux. Eine Readme-Datei ist als Teil des Download-Pakets verfügbar. Diese Datei enthält Anweisungen zum Kompilieren und Installieren des Pakets auf dem Host.

   Nachdem Sie den Treiber heruntergeladen und installiert haben, führen Sie die folgenden Plausibilitätsprüfungen durch:

   - Notieren Sie sich die Anzahl der C62x-Chips. Jeder C62x-Chip hat bis zu 3 PCIe-Endpunkte.
   - Stellen Sie sicher, dass alle Endpunkte aktiv sind. Führen Sie den Befehl `adf_ctl status` aus, um den Status aller PF-Endpunkte (bis zu 3) anzuzeigen.

     ```
     root@Super-Server:~# adf_ctl status

     Checking status of all devices.
     There is 51 QAT acceleration device(s) in the system
     ```

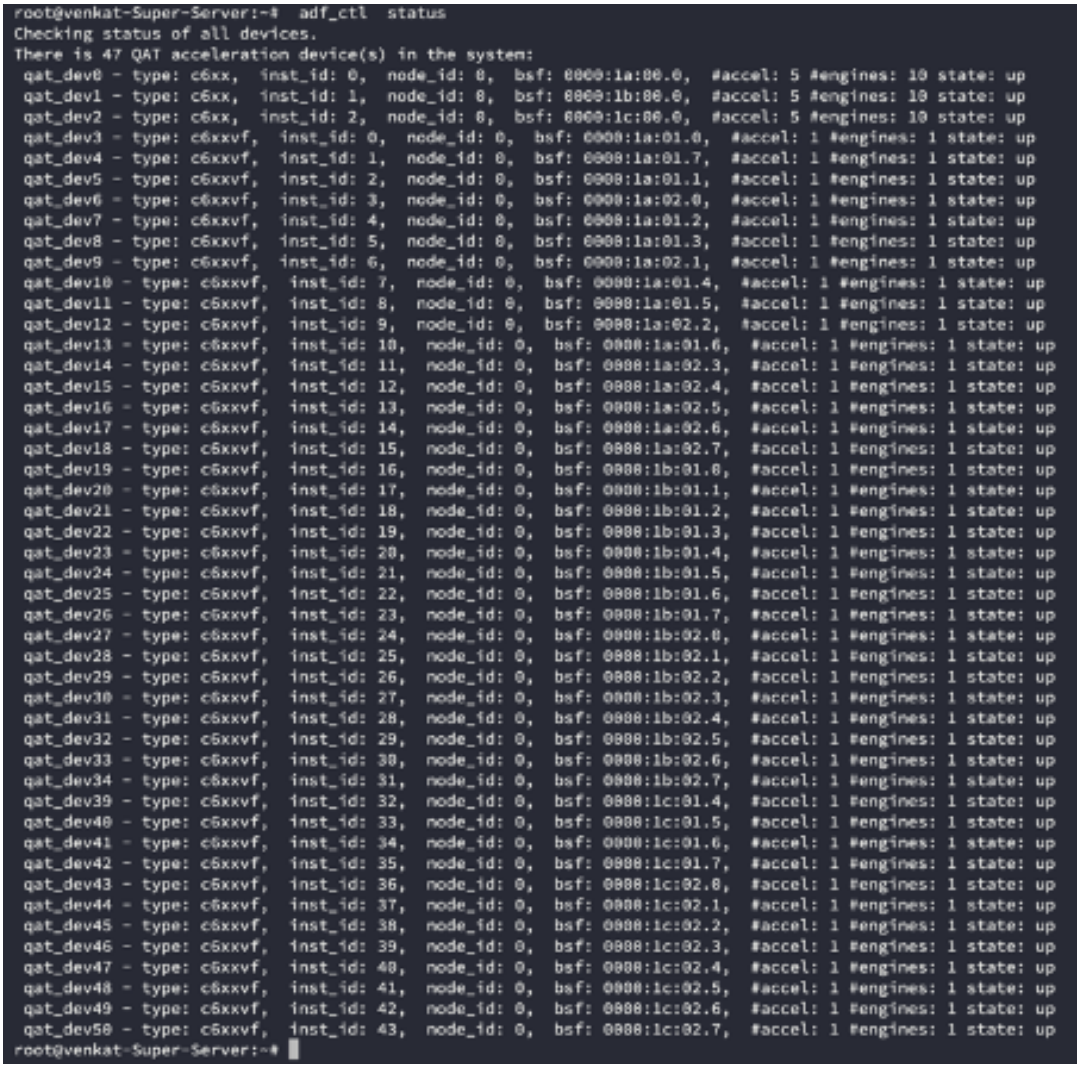


```
5    qat_dev0 - type: c6xx,  inst_id: 0,  node_id: 0,  bsf:
        0000:1a:00.0,  #accel: 5 #engines: 10 state: up
6    qat_dev1 - type: c6xx,  inst_id: 1,  node_id: 0,  bsf:
        0000:1b:00.0,  #accel: 5 #engines: 10 state: up
7    qat_dev2 - type: c6xx,  inst_id: 2,  node_id: 0,  bsf:
        0000:1c:00.0,  #accel: 5 #engines: 10 state: up
```

- Aktivieren Sie SRIOV (VF-Unterstützung) für alle QAT-Endpunkte.

```
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
```

- Stellen Sie sicher, dass alle VFs angezeigt werden (16 VFs pro Endpunkt, insgesamt 48 VFs).
- Führen Sie den Befehl adf_ctl status aus, um zu überprüfen, ob alle PF-Endpunkte (bis zu 3) und die VFs jedes Intel QAT-Chips AKTIV sind. In diesem Beispiel hat das System nur einen C62x-Chip. Es hat also insgesamt 51 Endpunkte (3 + 48 VFs).



2. Aktivieren Sie SR-IOV auf dem Linux-Host.
3. Erstellen Sie virtuelle Maschinen. Weisen Sie beim Erstellen einer VM die entsprechende Anzahl von PCI-Geräten zu, um die Leistungsanforderungen zu erfüllen.

> **Hinweis:**
>
> Jeder C62x (QAT) -Chip kann bis zu drei separate PCI-Endpunkte haben. Jeder Endpunkt ist eine logische Sammlung von VFs und teilt sich die Bandbreite zu gleichen Teilen mit anderen PCI-Endpunkten des Chips. Jeder Endpunkt kann bis zu 16 VFs haben, die als 16 PCI-Geräte angezeigt werden. Fügen Sie diese Geräte zur VM hinzu, um die Kryptobeschleunigung mithilfe des QAT-Chips durchzuführen.

Punkte zu beachten

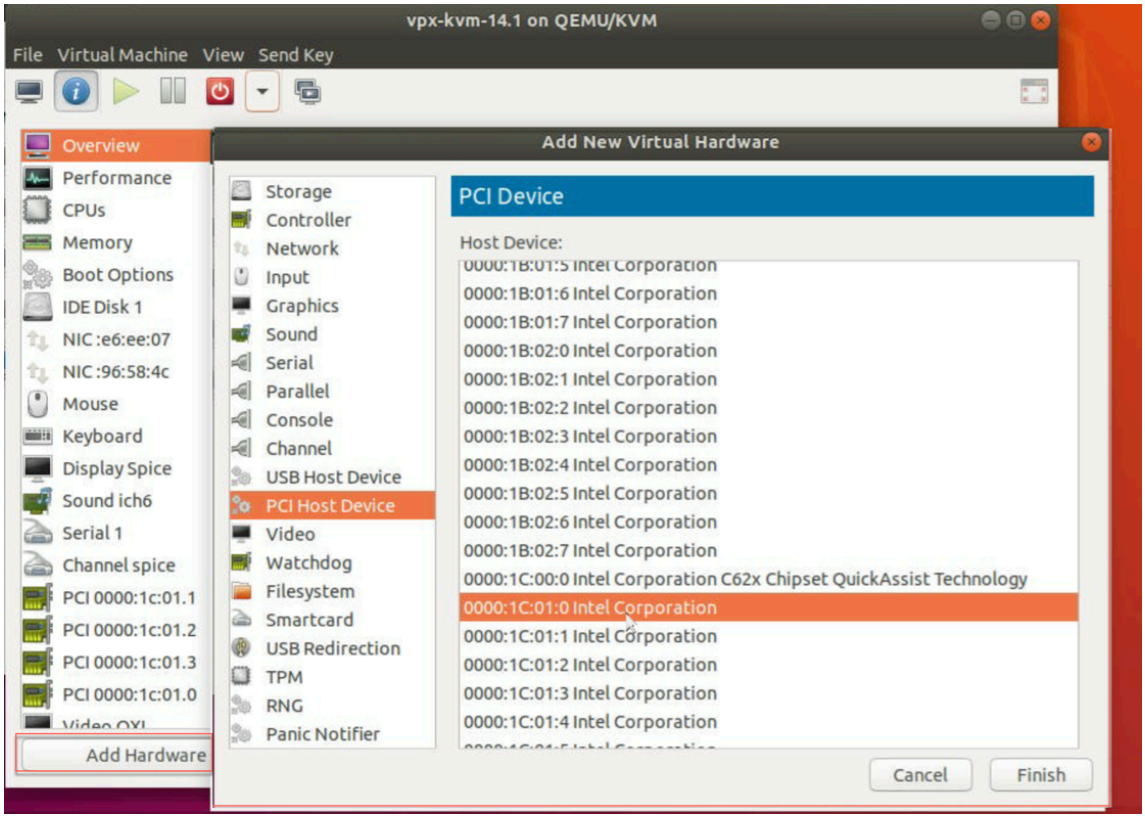
- Wenn die VM-Kryptoanforderung darin besteht, mehr als einen QAT-PCI-Endpunkt/-Chip zu verwenden, empfehlen wir, dass Sie die entsprechenden PCI-Geräte/VFs nach dem Round-Robin-Verfahren auswählen, um eine symmetrische Verteilung zu erzielen.
- Wir empfehlen, dass die Anzahl der ausgewählten PCI-Geräte der Anzahl der lizenzierten vCPUs entspricht (ohne die Anzahl der Verwaltungs-vCPUs einzubeziehen). Das Hinzufügen von mehr PCI-Geräten als die verfügbare Anzahl an vCPUs verbessert nicht unbedingt die Leistung.

  Beispiel

  Stellen Sie sich einen Linux-Host mit einem Intel C62x-Chip vor, der über 3 Endpunkte verfügt. Wählen Sie bei der Bereitstellung einer VM mit 6 vCPUs 2 VFs von jedem Endpunkt aus und weisen Sie sie der VM zu. Diese Zuordnung gewährleistet eine effektive und gleichmäßige Verteilung der Kryptoeinheiten für die VM. Von den insgesamt verfügbaren vCPUs ist standardmäßig eine vCPU für die Managementebene reserviert, und die übrigen vCPUs sind für die PEs der Datenebene verfügbar.

Weisen Sie QAT-VFs NetScaler VPX zu, das auf dem Linux-KVM-Hypervisor bereitgestellt wird

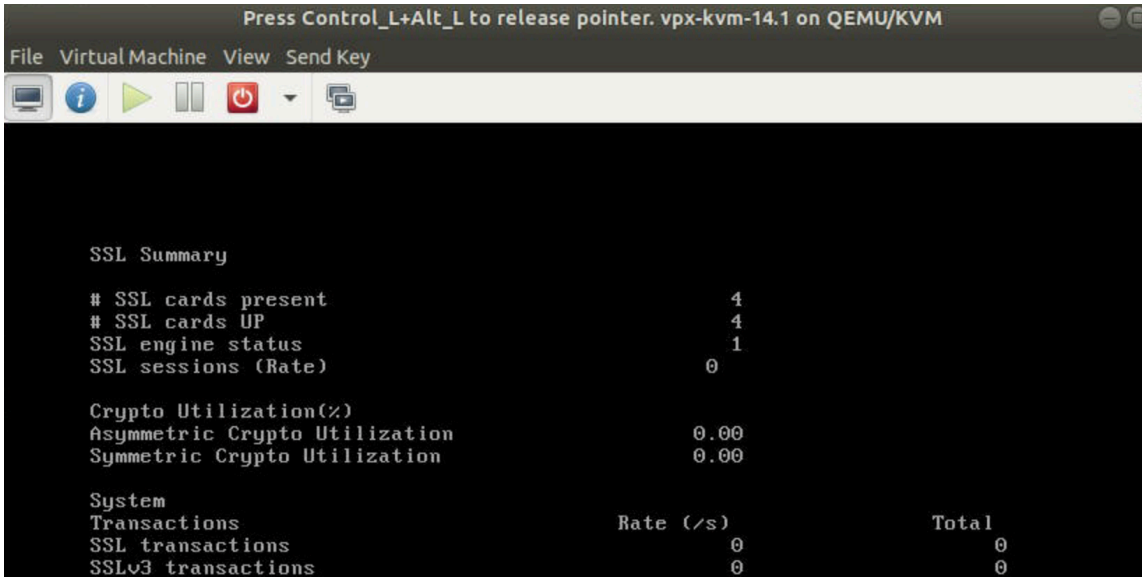
1. Stellen Sie im Linux KVM Virtual Machine Manager sicher, dass die VM (NetScaler VPX) ausgeschaltet ist.
2. Navigieren Sie zu **Hardware hinzufügen > PCI-Hostgerät**.
3. Weisen Sie dem PCI-Gerät Intel QAT VF zu.



4. Klicken Sie auf **Fertig stellen**.
5. Wiederholen Sie die vorherigen Schritte, um der NetScaler VPX-Instanz ein oder mehrere Intel QAT-VFs zuzuweisen, bis zu einer Grenze, die unter der Gesamtzahl der vCPUs liegt. Weil eine vCPU für den Verwaltungsprozess reserviert ist.

   Anzahl der QAT-VFs pro VM = Anzahl der vCPUs —1
6. Power on the VM.
7. Führen Sie den `stat ssl` Befehl in der NetScaler CLI aus, um die SSL-Zusammenfassung anzuzeigen, und überprüfen Sie die SSL-Karten, nachdem Sie NetScaler VPX QAT-VFs zugewiesen haben.

   In diesem Beispiel haben wir 5 vCPUs verwendet, was 4 Packet Engines (PES) impliziert.



Über den Einsatz

Diese Bereitstellung wurde mit den folgenden Komponentenspezifikationen getestet:

- **NetScaler VPX Version und Build:** 14.1—8.50
- **Ubuntu-Version:** 18.04, Kernel 5.4.0-146
- **Intel C62x QAT-Treiberversion für Linux** : L.4.21.0-00001

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

October 17, 2024

Nachdem Sie eine NetScaler VPX-Instanz auf der Linux-KVM-Plattform installiert und konfiguriert haben, können Sie den Virtual Machine Manager verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

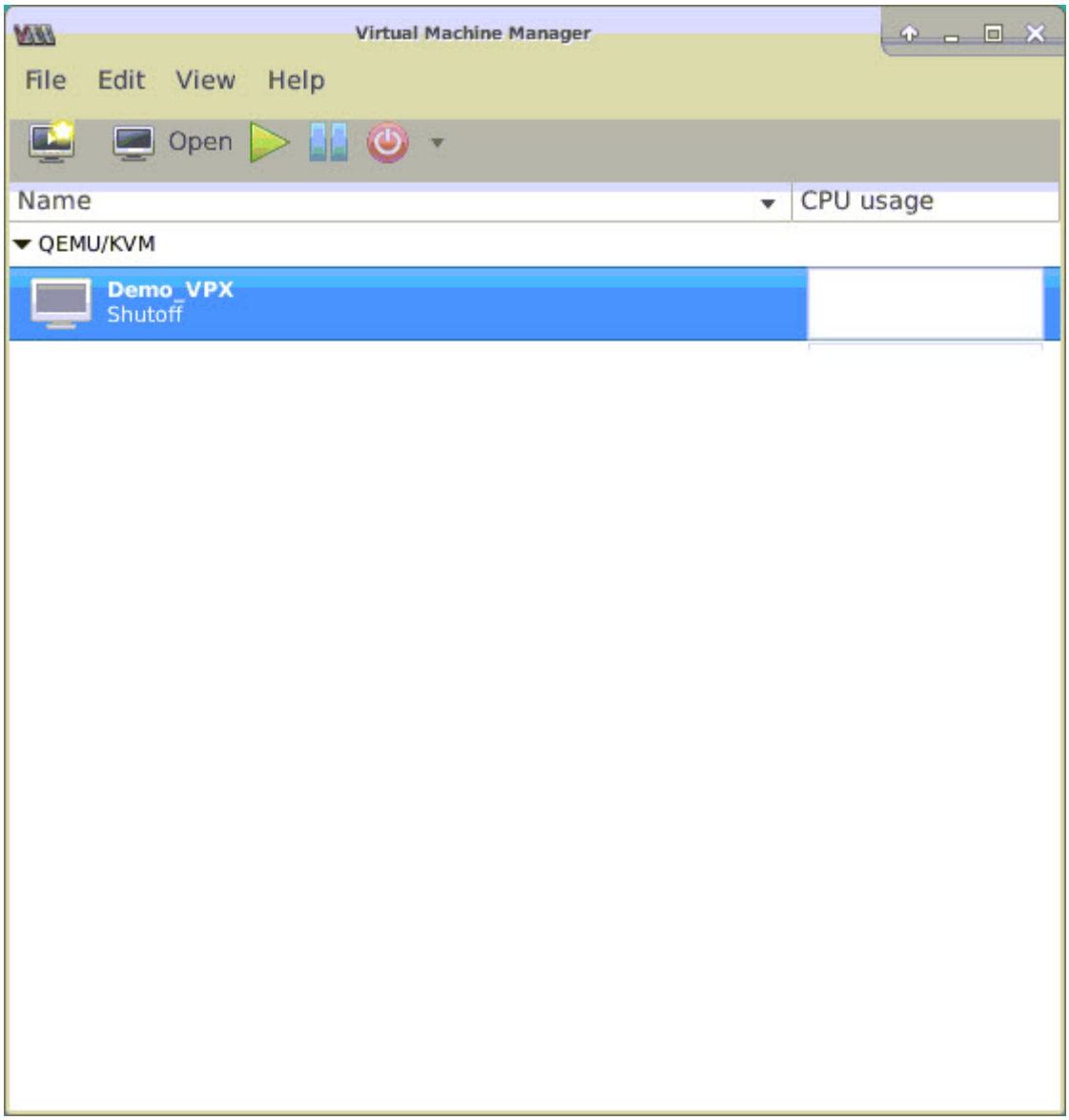
Voraussetzungen

- Die Firmware-Version der Intel XL710-NIC (NIC) auf dem KVM-Host ist 5.04.
- Der KVM-Host unterstützt Eingabe-Output-Speicherverwaltungseinheit (IOMMU) und Intel VT-d und ist im BIOS des KVM-Hosts aktiviert. Fügen Sie auf dem KVM-Host den folgenden Eintrag zur Datei **/boot/grub2/grub.cfg** hinzu, um IOMMU zu aktivieren:**intel_iommu=1**

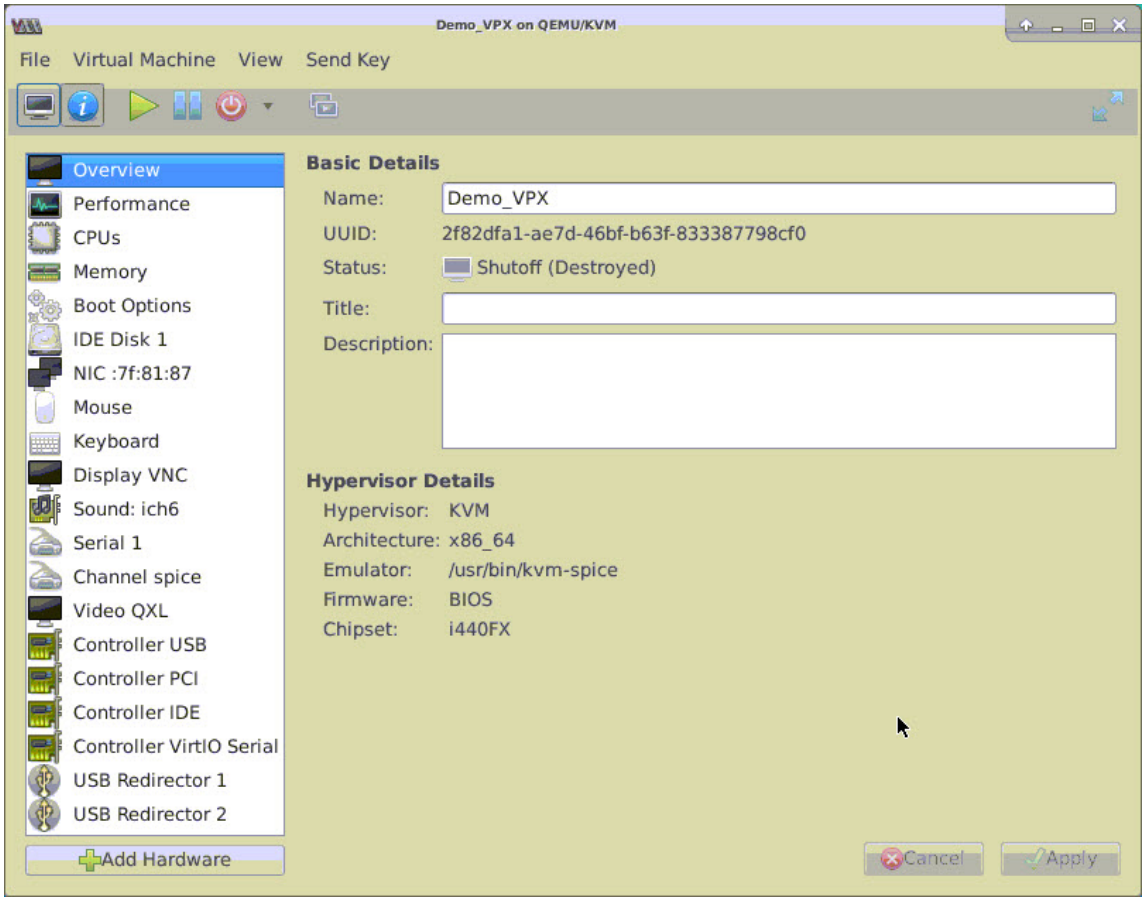
- Führen Sie den folgenden Befehl aus und starten Sie den KVM-Host neu: **Grub2-mkConfig —o /boot/grub2/grub.cfg**

So konfigurieren Sie NetScaler VPX-Instanzen für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen mithilfe des Virtual Machine Manager:

1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz aus, und klicken Sie auf **Öffnen**.



3. Klicken Sie im Fenster **virtual_machine im KVM** -Fenster auf das **I-Symbol** .

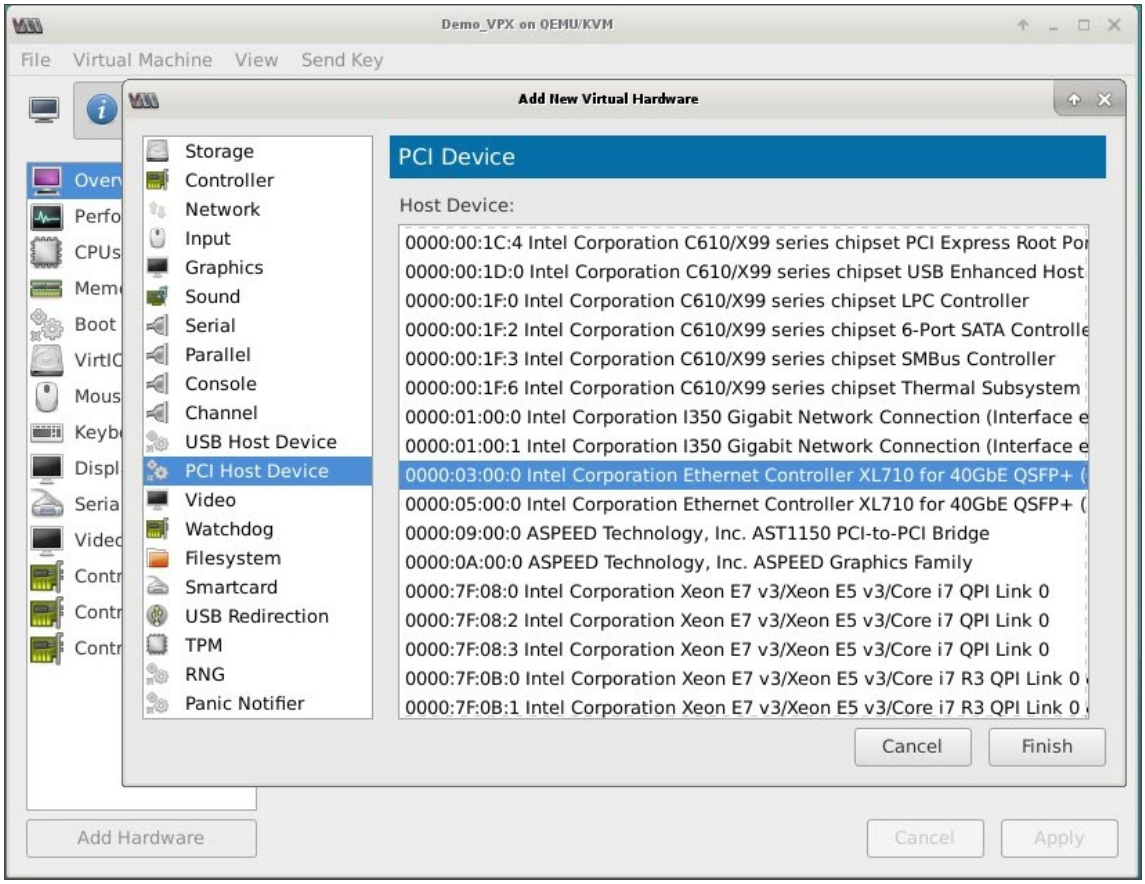


4. Klicken Sie auf **Hardware hinzufügen**.
5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a. Wählen Sie **PCI-Hostgerät**aus.

   b. Wählen Sie im Abschnitt **Hostgerät** die physische Intel XL710 Funktion aus.

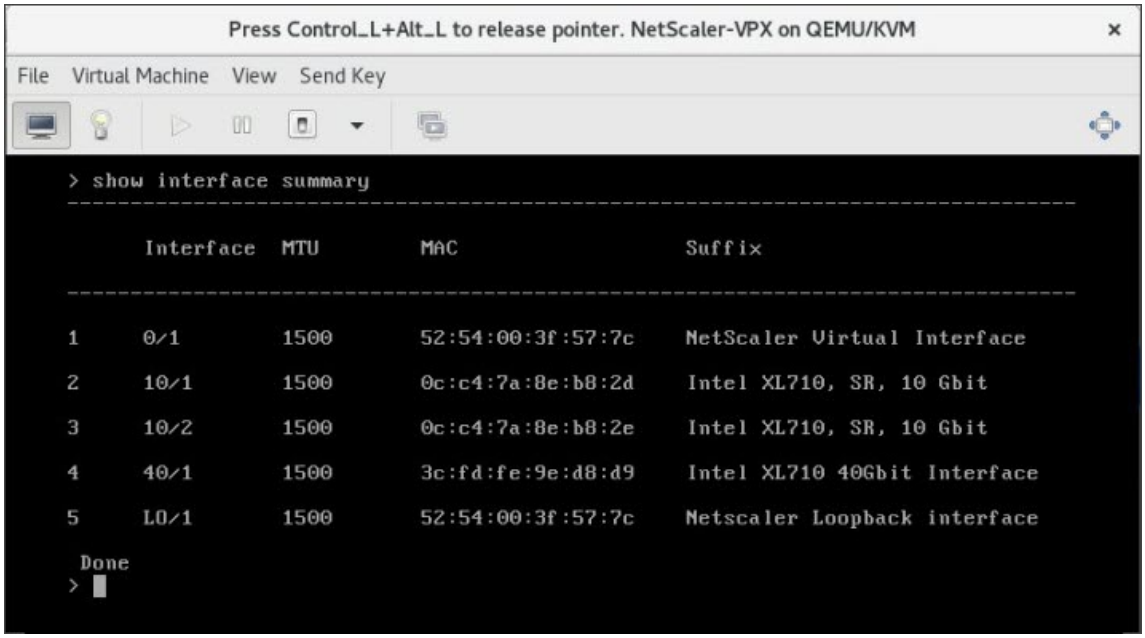
   c. Klicken Sie auf **Fertig stellen**.



6. Wiederholen Sie die Schritte **4** und **5**, um zusätzliche physische Funktionen des Intel XL710 hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

```
COMMAND

> show interface summary
```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:



Stellen Sie die NetScaler VPX-Instanz mithilfe des virsh Programms bereit

October 17, 2024

Das `virsh` Programm ist ein Befehlszeilentool zur Verwaltung von VM-Gästen. Seine Funktionalität ähnelt der von Virtual Machine Manager. Es ermöglicht Ihnen, den Status eines VM-Gastes (Start, Stopp, Pause usw.) zu ändern, neue Gäste und Geräte einzurichten und vorhandene Konfigurationen zu bearbeiten. Das `virsh` Programm ist auch nützlich für das Skripten von VM-Gastverwaltungsvorgängen.

Gehen Sie folgendermaßen vor, um NetScaler VPX mithilfe des `virsh` Programms bereitzustellen:

1. Verwenden Sie den Befehl tar, um das NetScaler VPX-Paket aufzuheben. Das Paket NSVPX-KVM-*_nc.tgz enthält die folgenden Komponenten:

   - Die Domänen-XML-Datei mit VPX-Attributen [NSVPX-KVM-*_nc.xml]
   - Prüfen Sie die Summe des NS-VM-Datenträgerimages [CheckSum.txt]
   - NS-VM-Datenträgerabbildimage [NSVPX-KVM-*_nc.raw]

   Beispiel

   ```
   tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
   NSVPX-KVM-10.1-117_nc.xml
   NSVPX-KVM-10.1-117_nc.raw
   checksum.txt
   ```


2. Kopieren Sie die XML-Datei NSVPX-KVM-*_nc.xml in eine Datei mit dem Namen \\<DomainName\\>-NSVPX-KVM-*_nc.xml. Der <DomainName> ist auch der Name der virtuellen Maschine. Beispiel

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc
    .xml
```

3. Bearbeiten Sie die Datei \\<DomainName\\>-NSVPX-KVM-*_nc.xml , um die folgenden Parameter anzugeben:

   - name—Geben Sie den Namen an.
   - Mac - Geben Sie die MAC-Adresse an.

     > **Hinweis:**
     >
     > Der Domänenname und die MAC-Adresse müssen eindeutig sein.

   - Quelldatei - Geben Sie den absoluten Quellpfad für das Datenträgerimage an. Der Dateipfad muss absolut sein. Sie können den Pfad der RAW-Imagedatei oder einer QCOW2-Imagedatei angeben.

     Wenn Sie eine RAW-Image-Datei angeben möchten, geben Sie den Pfad der Datenträgerimagequelle an, wie im folgenden Beispiel gezeigt:

     Beispiel

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
```

     Geben Sie den absoluten QCOW2-Datenträgerimagequellpfad an, und definieren Sie den Treibertyp als **qcow2**, wie im folgenden Beispiel gezeigt:

     Beispiel

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<driver name ='qemu' type='qcow2'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
```

4. Bearbeiten Sie die Datei \\<DomainName\\>-NSVPX-KVM-*_nc.xml , um die Netzwerkdetails zu konfigurieren:

   - source dev—Geben Sie die Schnittstelle an.
   - mode —Geben Sie den Modus an. Die Standardschnittstelle ist **Macvtap Bridge**.

   Beispiel: Modus: MacVTap Bridge Setzen Sie Zielschnittstelle als ethx und Modus als Bridge-Modelltyp als virtio


```
    <interface type='direct'>
        <mac address='52:54:00:29:74:b3'/>
        <source dev='eth0' mode='bridge'/>
        <target dev='macvtap0'/>
        <model type='virtio'/>
        <alias name='net0'/>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
            function='0x0'/>
      </interface>
```

Hier ist eth0 die physische Schnittstelle, die an die VM angeschlossen ist.

5. Definieren Sie die VM-Attribute in der Datei \\<DomainName\\>-NSVPX-KVM-*_nc.xml mit dem folgenden Befehl:

```
virsh define \<DomainName\>-NSVPX-KVM-\*\_nc.xml
```

Beispiel

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

6. Starten Sie die VM, indem Sie den folgenden Befehl eingeben:

```
virsh start \[\<DomainName\> | \<DomainUUID\>\]
```

Beispiel

```
virsh start NetScaler-VPX
```

7. Verbinden der Gast-VM über die Konsole:

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

Beispiel

```
virsh console NetScaler-VPX
```

Fügen Sie NetScaler VPX-Instanz mithilfe `virsh` des Programms weitere Schnittstellen hinzu

Nachdem Sie NetScaler VPX auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen:

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf der KVM ausgeführt wird.
2. Bearbeiten Sie die Datei \\<DomainName\\>-NSVPX-KVM-*_nc.xml mit dem folgenden Befehl:


```
virsh edit \[\<DomainName\> | \<DomainUUID\>\]
```

3. Fügen Sie in der Datei \\<DomainName\\>-NSVPX-KVM-*_nc.xml die folgenden Parameter hinzu:

   a) **Für MacVtap**

   - Schnittstellentyp —Geben Sie den Schnittstellentyp als ‘direct’an.
   - MAC-Adresse—Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
   - source dev—Geben Sie den Schnittstellennamen an.
   - mode - Geben Sie den Modus an. Die unterstützten Modi sind Bridge, VEPA, Private und Pass-Through
   - Modelltyp—Geben Sie den Modelltyp an als `virtio`

   Beispiel

   Modus: MacVTap Pass-Through

   Zielschnittstelle festlegen als `ethx`, Modus als Brücke und Modelltyp als `Virtio`

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
```

   Hier eth1 ist die physische Schnittstelle, die an die VM angeschlossen ist.

   b) **Für Bridge-Modus**

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie im KVM-Host eine Linux-Bridge konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den Status „UP“versetzt haben.

   - Schnittstellentyp —Geben Sie den Schnittstellentyp als ‘Bridge’an.
   - MAC-Adresse—Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
   - Quellbrücke —Geben Sie den Bridge-Namen an.
   - Modelltyp—Geben Sie den Modelltyp an als `virtio`

   Beispiel: Bridge-Modus

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
```



```
5     </interface>
```

Verwalten der NetScaler VPX Gast-VMs

October 17, 2024

Sie können den Virtual Machine Manager und das `virsh` Programm verwenden, um Verwaltungsaufgaben wie das Starten oder Stoppen eines VM-Gastes, das Einrichten neuer Gäste und Geräte, das Bearbeiten vorhandener Konfigurationen und die Verbindung mit der grafischen Konsole über Virtual Network Computing (VNC) auszuführen.

Verwalten der VPX-Gast-VMs mithilfe von Virtual Machine Manager

- Liste der VM-Gäste

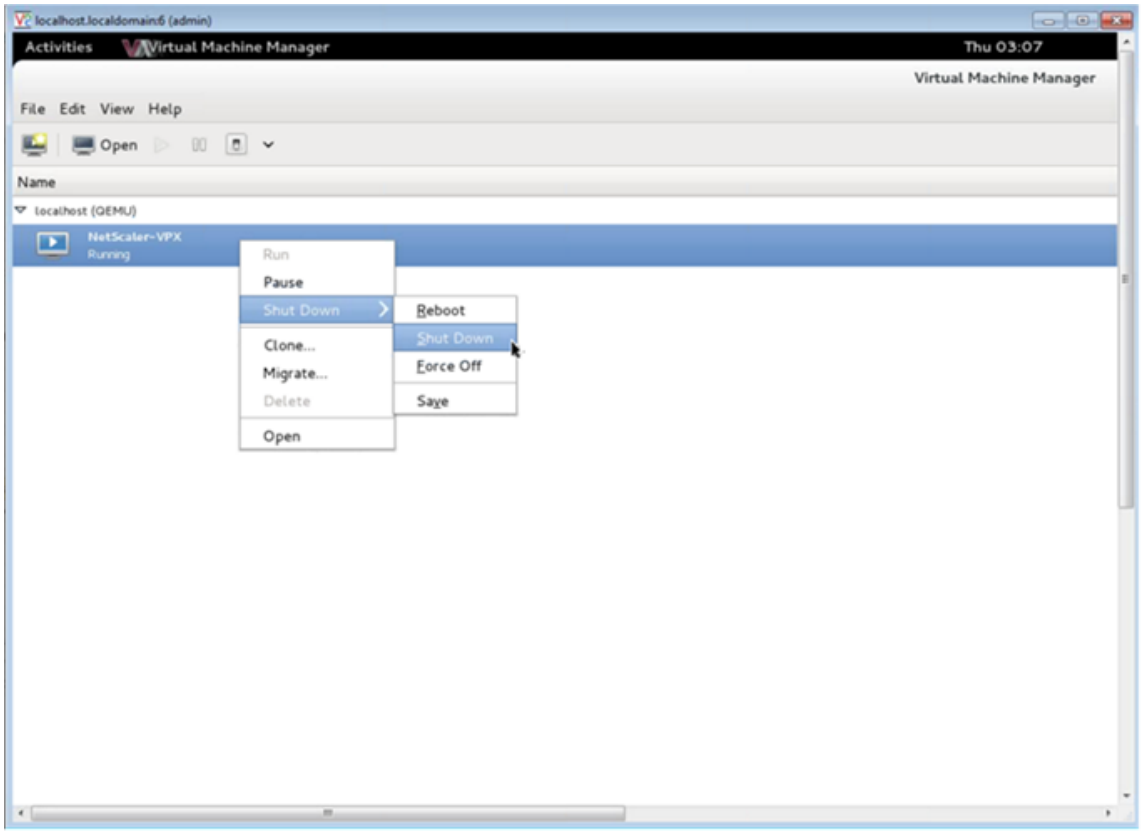
  Im Hauptfenster des Virtual Machine Manager wird eine Liste aller VM-Gäste für jeden VM-Hostserver angezeigt, mit dem er verbunden ist. Jeder VM-Gasteintrag enthält den Namen der virtuellen Maschine zusammen mit seinem Status (Ausführen, Pausiert oder Shutoff), der wie im Symbol angezeigt wird.

- Öffnen einer grafischen Konsole

  Wenn Sie einem VM-Gast eine grafische Konsole öffnen, können Sie mit dem Computer wie mit einem physischen Host über eine VNC-Verbindung interagieren. Um die grafische Konsole im Virtual Machine Manager zu öffnen, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie im Popup-Menü die Option Öffnen.

- Einen Gast starten und herunterfahren

  Sie können einen VM-Gast vom Virtual Machine Manager aus starten oder beenden. Um den Status der VM zu ändern, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie Ausführen oder eine der Optionen zum Herunterfahren aus dem Popupmenü.



- Einen Gast neu starten

  Sie können einen VM-Gast über den Virtual Machine Manager neu starten. Um die VM neu zu starten, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie dann im Popupmenü die Option Herunterfahren > Neustarten aus.

- Löschen eines Gastes

  Beim Löschen eines VM-Gastes wird standardmäßig dessen XML-Konfiguration entfernt. Sie können auch die Speicherdateien eines Gastes löschen. Dadurch wird der Gast vollständig gelöscht.

  1. Klicken Sie im Virtual Machine Manager mit der rechten Maustaste auf den VM-Gasteintrag.
  2. Wählen Sie im Popup-Menü die Option Löschen aus. Ein Bestätigungsfenster öffnet sich.

     > **Hinweis:**
     >
     > Die Option „Löschen“ist nur aktiviert, wenn der VM-Gast heruntergefahren ist.

  3. Klicken Sie auf **Löschen**.
  4. Um den Gast vollständig zu löschen, löschen Sie die zugehörige RAW-Datei, indem Sie das Kontrollkästchen Zugehörige Speicherdateien löschen aktivieren.

Verwalten Sie die NetScaler VPX-Gast-VMs mit dem `virsh` Programm

- Listen Sie die VM-Gäste und ihre aktuellen Status auf.

  So zeigen `virsh` Sie Informationen über die Gäste an

  ```
  virsh list --all
  ```

  Die Befehlsausgabe zeigt alle Domänen mit ihrem Status an. Beispiel für eine Ausgabe:

  ```
  Id Name                 State
  ----------------------------------
    0 Domain-0            running
    1 Domain-1            paused
    2 Domain-2            inactive
    3 Domain-3            crashed
  ```

- Öffne eine `virsh` Konsole.

  Verbinden der Gast-VM über die Konsole

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

  Beispiel

  ```
  virsh console NetScaler-VPX
  ```

- Startet und schaltet einen Gast aus.

  Gäste können mit dem DomainNamen oder der Domain-UUID gestartet werden.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Beispiel

  ```
  virsh start NetScaler-VPX
  ```

  Um einen Gast herunterzufahren:

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel

  ```
  virsh shutdown NetScaler-VPX
  ```

- Einen Gast neu starten

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel

  ```
  virsh reboot NetScaler-VPX
  ```

  Löschen eines Gastes

  Um eine Gast-VM zu löschen, müssen Sie die Gast-VM herunterfahren und die Definition von <DomainName>-NSVPX-KVM-*_nc.xml aufheben, bevor Sie den Löschbefehl ausführen.


```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
```

Beispiel

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
```

> **Hinweis:**
>
> Der Löschbefehl entfernt keine Disk-Image-Datei, die manuell entfernt werden muss.

Stellen Sie die NetScaler VPX-Instanz mit SR-IOV auf OpenStack bereit

October 17, 2024

Sie können leistungsstarke NetScaler VPX-Instances auf OpenStack bereitstellen, die die Single-Root-I/O-Virtualisierungstechnologie (SR-IOV) verwenden.

Sie können eine NetScaler VPX-Instanz, die die SR-IOV-Technologie verwendet, auf OpenStack in drei Schritten bereitstellen:

- Aktivieren Sie virtuelle SR-IOV-Funktionen (VFs) auf dem Host.
- Konfigurieren Sie die vFS und stellen Sie sie OpenStack zur Verfügung.
- Stellen Sie den NetScaler VPX auf OpenStack bereit.

Voraussetzungen

Stellen Sie sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Laden Sie den neuesten IXGBE Treiber von Intel herunter und installieren Sie ihn.
- Blockieren Sie den IXGBEVF-Treiber auf dem Host auf. Fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/blacklist.conf hinzu: Sperrliste `ixgbevf`

> **Hinweis:**
>
> Die `ixgbe` Treiberversion muss mindestens 5.0.4 sein.

Aktivieren von SR-IOV-VFs auf dem Host

Führen Sie einen der folgenden Schritte aus, um SR-IOV-VFs zu aktivieren:

- Wenn Sie eine ältere Kernelversion als 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/ixgbe den folgenden Eintrag hinzu und starten Sie den Host neu: options ixgbe max_vfs= <number_of_VFs>
- Wenn Sie die Kernel-Version 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl:

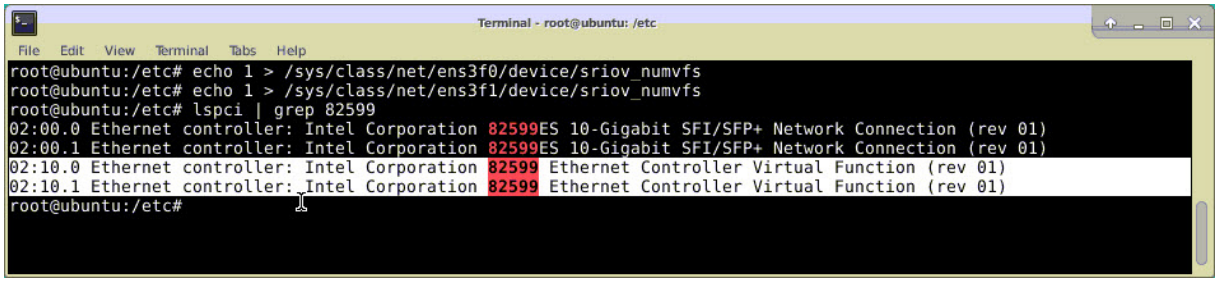
```
1        echo <number_of_VFs> > /sys/class/net/<device_name>/device/
            sriov_numvfs
```

Ort:

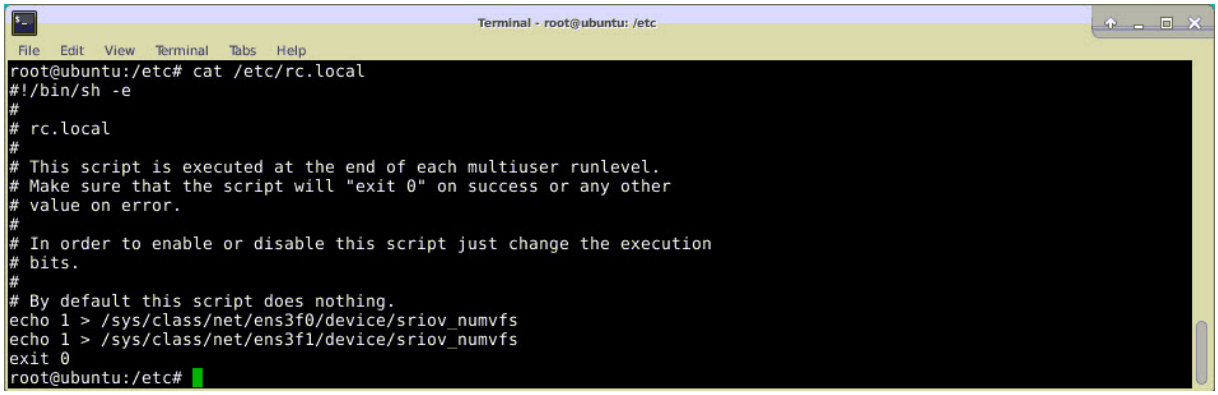
- Number_of_VFS ist die Anzahl der virtuellen Funktionen, die Sie erstellen möchten.
- device_name ist der Schnittstellenname.

> **Wichtig:**
>
> Achten Sie beim Erstellen der SR-IOV-VFs darauf, dass Sie den VFs keine MAC-Adressen zuweisen.

Hier ist ein Beispiel für vier VFs, die erstellt werden.



Machen Sie die VFs persistent, fügen Sie die Befehle, die Sie zum Erstellen von VFs verwendet haben, zur Datei **rc.local** hinzu. Hier ist ein Beispiel, das den Inhalt der rc.local-Datei zeigt.



Weitere Informationen finden Sie in diesem Intel SR-IOV-Konfigurationshandbuch.

Konfigurieren und stellen Sie die VFs für OpenStack zur Verfügung

Folgen Sie den Schritten unter dem folgenden Link, um SR-IOV auf OpenStack zu konfigurieren:. https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking

Bereitstellen der NetScaler VPX Instanz auf OpenStack

Sie können eine NetScaler VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie die OpenStack-CLI verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten an die Instanz anhängt. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfigurationsinformationen wie Management-IP-Adresse, Netzwerkmaske und Standardgateway usw. an die Instanz zu übergeben, bevor Sie die Netzwerkeinstellungen für die Instanz konfigurieren.

Wenn OpenStack eine VPX-Instanz zur Verfügung stellt, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge (OpenStack Foundation) liest, die OpenStack angibt. Für Red Hat Linux-Distributionen wird die Zeichenfolge in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben. Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die folgenden Informationen aus dem im `nova` Boot-Befehl angegebenen Dateinamen zu lesen. In den folgenden Verfahren heißt die Datei userdata.txt.

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Sobald die Parameter erfolgreich gelesen wurden, werden sie in den NetScaler-Stack gefüllt. Dies hilft bei der Remote-Verwaltung der Instanz. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP ausfällt oder ein Timeout auftritt, erstellt die Instance die Standard-Netzwerkkonfiguration (192.168.100.1/16).

Stellen Sie die NetScaler VPX-Instanz auf OpenStack über CLI bereit

Sie können eine VPX-Instanz in einer OpenStack-Umgebung mithilfe der OpenStack-CLI bereitstellen. Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen einer NetScaler VPX-Instanz auf OpenStack:

1. Extrahieren der `.qcow2` Datei aus der TGZ-Datei
2. Erstellen eines OpenStack-Images aus dem qcow2-Image
3. Provisioning einer VPX-Instanz

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz in einer OpenStack-Umgebung bereitzustellen.

1. Extrahiere das. `qcow2` Datei aus der `.tqz` Datei, indem Sie den Befehl eingeben:

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben:

```
glance image-create --name="<name of the OpenStack image>" --
   property hw_disk_bus=ide --is-public=true --container-format=
   bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
   hw_disk_bus=ide --is-public= true --container-format=bare --
   disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
```

   Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.


```
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| checksum         | 735dae4ea6e46e39ed3f0acfba02e755     |
| container_format | bare                                 |
| created_at       | 2017-02-16T10:03:29Z                 |
| disk_format      | qcow2                                |
| hw_disk_bus      | ide                                  |
| id               | aeaa13e9-b49b-411c-ab54-c61820a8e2f3 |
| min_disk         | 0                                    |
| min_ram          | 0                                    |
| name             | NSVPX-KVM-12.0-26.2                  |
| owner            | 06c41a73b32f4b48af55359fd7d3502c     |
| protected        | False                                |
| size             | 717946880                            |
| status           | active                               |
| tags             | []                                   |
| updated_at       | 2017-02-16T10:03:38Z                 |
| virtual_size     | None                                 |
| visibility       | private                              |
+------------------+--------------------------------------+
```

3. Nachdem ein OpenStack-Image erstellt wurde, stellen Sie die NetScaler VPX-Instanz bereit.

```
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
```

Im vorherigen Befehl ist userdata.txt die Datei, die Details wie IP-Adresse, Netzmaske und Standardgateway für die VPX-Instanz enthält. Die Benutzerdatendatei ist eine vom Benutzer anpassbare Datei. NSVPX-KVM-12.0-26.2 ist der Name der virtuellen Appliance, die Sie bereitstellen möchten. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 ist der OpenStack ss.

Die folgende Abbildung zeigt eine Beispielausgabe des nova Boot-Befehls.

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

Die folgende Abbildung zeigt ein Beispiel der Datei userdata.txt. Die Werte innerhalb der Tags <PropertySection></PropertySection> sind die vom Benutzer konfigurierbaren Werte und enthalten Informationen wie IP-Adresse, Netzmaske und Standardgateway.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
    "
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
    1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"
    />
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
```



```
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>
```

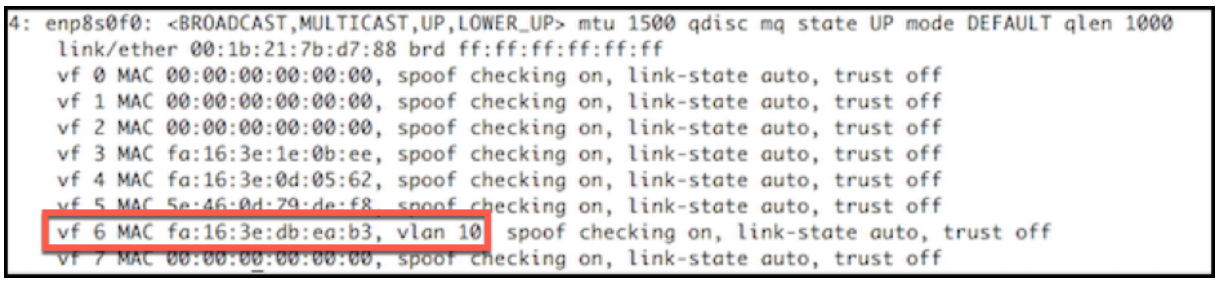
Zusätzliche unterstützte Konfigurationen: Erstellen und Löschen von VLANs auf SR-IOV-VFs vom Host

Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu erstellen:

```
ip link show enp8s0f0 vf 6 vlan 10
```

Im vorherigen Befehl “enp8s0f0”ist der Name der physikalischen Funktion.

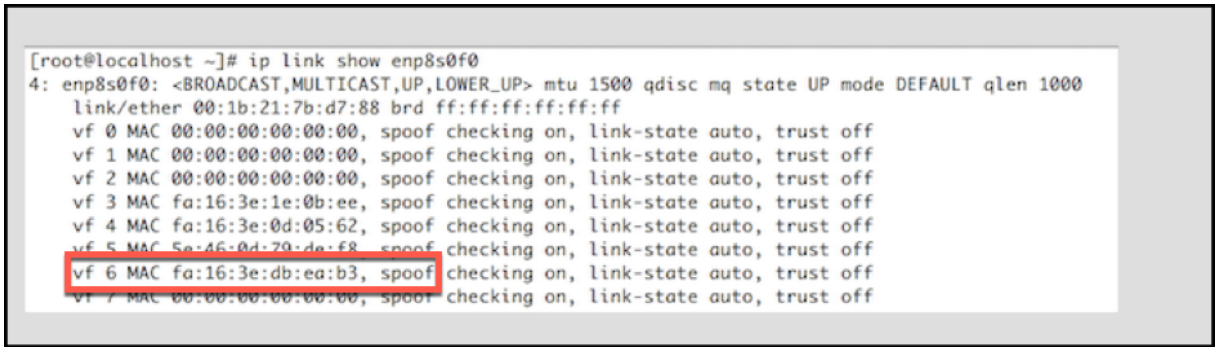
Beispiel: VLAN 10, erstellt auf vf 6



Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu löschen:

```
ip link show enp8s0f0 vf 6 vlan 0
```

Beispiel: VLAN 10, aus vf 6 entfernt



Mit diesen Schritten wird das Verfahren zum Bereitstellen einer NetScaler VPX-Instanz, die die SRIOV-Technologie verwendet, auf OpenStack abgeschlossen.

Konfigurieren Sie eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS-DPDK-basierten Hostschnittstellen

October 17, 2024

Sie können eine NetScaler VPX-Instanz konfigurieren, die auf KVM (Fedora und RHOS) ausgeführt wird, um Open vSwitch (OVS) mit Data Plane Development Kit (DPDK) für eine bessere Netzwerkleistung zu verwenden. In diesem Dokument wird beschrieben, wie die NetScaler VPX-Instanz so konfiguriert wird, dass sie an den `vhost-user` Ports arbeitet, die von OVS-DPDK auf dem KVM-Host bereitgestellt werden.

OVS ist ein Multilayer-Virtual Switch, der unter der Open-Source-Apache 2.0-Lizenz lizenziert DPDK ist eine Reihe von Bibliotheken und Treibern für die schnelle Paketverarbeitung. DPDK ist ein Satz von Bibliotheken und Treibern für die schnelle Paketverarbeitung.

Die folgenden Versionen von Fedora, RHOS, OVS und DPDK sind für die Konfiguration einer NetScaler VPX-Instanz qualifiziert:

Fedora	RHOS
Fedora 25	RHOS 7,4
OVS 2.7.0	VERSION 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Voraussetzungen

Stellen Sie vor der Installation von DPDK sicher, dass der Host über 1 GB große Seiten verfügt.

Weitere Informationen finden Sie in dieser Dokumentation zu den DPDK-Systemanforderungen. Es folgt eine Zusammenfassung der Schritte, die erforderlich sind, um eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS DPDK-basierten Host-Interfaces zu konfigurieren:

- Installieren Sie DPDK.
- Erstellen und installieren Sie OVS.
- Erstellen Sie eine OVS-Brücke.
- Schließen Sie eine physikalische Schnittstelle an die OVS-Brücke an.
- Hängen Sie `vhost-user` Ports an den OVS-Datenpfad an.
- Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit.

DPDK installieren

Um DPDK zu installieren, folgen Sie den Anweisungen in diesem Open vSwitch mit DPDK-Dokument
.

Erstellen und Installieren von OVS

Laden Sie OVS von der OVS-Downloadseite herunter. Erstellen und installieren Sie als Nächstes OVS mit einem DPDK-Datapath. Folgen Sie den Anweisungen im Dokument Installieren von Open vSwitch
.

Ausführlichere Informationen finden Sie im DPDK Getting Started Guide für Linux.

Erstellen einer OVS-Brücke

Geben Sie je nach Bedarf den Befehl Fedora oder RHOS ein, um eine OVS-Bridge zu erstellen:

Fedora-Befehl:

```
1    > $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
       datapath_type=netdev
```

RHOS-Befehl:

```
1    ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

Verbinden Sie die physische Schnittstelle mit der OVS-Brücke

Binden Sie die Ports an DPDK und verbinden Sie sie dann mit der OVS-Bridge, indem Sie die folgenden Fedora- oder RHOS-Befehle eingeben:

Fedora-Befehl:

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

RHOS-Befehl:

```
1    ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
       options:dpdk-devargs=0000:03:00.0
2
3
4    ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
       options:dpdk-devargs=0000:03:00.1
```


Die als Teil der Optionen `dpdk-devargs` gezeigte gibt den PCI-BDF der jeweiligen physikalischen NIC an.

Anhängen von `vhost-user` Ports an den OVS-Datenpfad

Geben Sie die folgenden Fedora- oder RHOS-Befehle ein, um `vhost-user` Ports an den OVS-Datenpfad anzuhängen:

Fedora-Befehl:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
```

RHOS-Befehl:

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
```

Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit

Sie können eine VPX-Instanz auf Fedora KVM mit OVS-DPDK-basierten `vhost-user` -Ports nur über die CLI bereitstellen, indem Sie die folgenden QEMU-Befehle verwenden: **Fedora-Befehl**:

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \

-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

```



```
-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
   bus=pci.0,addr=0x3 \

-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
   user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
   virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
   user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
   virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

--nographic
```

Verwenden Sie für RHOS die folgende XML-Beispieldatei, um die NetScaler VPX-Instanz mithilfe von bereitzustellen `virsh`.

```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>

  <cputune>

    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>
```



```
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
47        <partition>/machine</partition>
48
49      </resource>
50
51      <os>
52
53        <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55        <boot dev='hd'/>
56
57      </os>
58
59      <features>
60
61        <acpi/>
62
63        <apic/>
64
65      </features>
66
67      <cpu mode='custom' match='minimum' check='full'>
68
69        <model fallback='allow'>Haswell-noTSX</model>
70
71        <vendor>Intel</vendor>
72
73        <topology sockets='1' cores='6' threads='1'/>
74
75        <feature policy='require' name='ss'/>
76
77        <feature policy='require' name='pcid'/>
78
79        <feature policy='require' name='hypervisor'/>
80
81        <feature policy='require' name='arat'/>
82
83    <domain type='kvm'>
84
```



```
<name>dpdk-vpx1</name>

<uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

<memory unit='KiB'>16777216</memory>

<currentMemory unit='KiB'>16777216</currentMemory>

<memoryBacking>

  <hugepages>

    <page size='1048576' unit='KiB'/>

  </hugepages>

</memoryBacking>

<vcpu placement='static'>6</vcpu>

<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>

  <vcpupin vcpu='1' cpuset='2'/>

  <vcpupin vcpu='2' cpuset='4'/>

  <vcpupin vcpu='3' cpuset='6'/>

  <emulatorpin cpuset='0,2,4,6'/>

</cputune>

<numatune>

  <memory mode='strict' nodeset='0'/>

</numatune>

<resource>

  <partition>/machine</partition>

</resource>

<os>

  <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>

  <boot dev='hd'/>
```



```
138
139       </os>
140
141       <features>
142
143         <acpi/>
144
145         <apic/>
146
147       </features>
148
149       <cpu mode='custom' match='minimum' check='full'>
150
151         <model fallback='allow'>Haswell-noTSX</model>
152
153         <vendor>Intel</vendor>
154
155         <topology sockets='1' cores='6' threads='1'/>
156
157         <feature policy='require' name='ss'/>
158
159         <feature policy='require' name='pcid'/>
160
161         <feature policy='require' name='hypervisor'/>
162
163         <feature policy='require' name='arat'/>
164
165         <feature policy='require' name='tsc\_adjust'/>
166
167         <feature policy='require' name='xsaveopt'/>
168
169         <feature policy='require' name='pdpe1gb'/>
170
171         <numa>
172
173           <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess=
                'shared'/>
174
175         </numa>
176
177       </cpu>
178
179       <clock offset='utc'/>
180
181       <on\_poweroff>destroy</on\_poweroff>
182
183       <on\_reboot>restart</on\_reboot>
184
185       <on\_crash>destroy</on\_crash>
186
187       <devices>
188
189         <emulator>/usr/libexec/qemu-kvm</emulator>
```



```
190
191         <disk type='file' device='disk'>
192
193           <driver name='qemu' type='qcow2' cache='none'/>
194
195           <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>
196
197           <target dev='vda' bus='virtio'/>
198
199           <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
                 function='0x0'/>
200
201         </disk>
202
203         <controller type='ide' index='0'>
204
205           <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
                 function='0x1'/>
206
207         </controller>
208
209         <controller type='usb' index='0' model='piix3-uhci'>
210
211           <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
                 function='0x2'/>
212
213         </controller>
214
215         <controller type='pci' index='0' model='pci-root'/>
216
217         <interface type='direct'>
218
219           <mac address='52:54:00:bb:ac:05'/>
220
221           <source dev='enp129s0f0' mode='bridge'/>
222
223           <model type='virtio'/>
224
225           <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
                 function='0x0'/>
226
227         </interface>
228
229         <interface type='vhostuser'>
230
231           <mac address='52:54:00:55:55:56'/>
232
233           <source type='unix' path='/var/run/openvswitch/vhost-user1'
                 mode='client'/>
234
235           <model type='virtio'/>
236
237           <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
```



```
            function='0x0'/>
238
239         </interface>
240
241         <interface type='vhostuser'>
242
243           <mac address='52:54:00:2a:32:64'/>
244
245           <source type='unix' path='/var/run/openvswitch/vhost-user2'
                mode='client'/>
246
247           <model type='virtio'/>
248
249           <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
                function='0x0'/>
250
251         </interface>
252
253         <interface type='vhostuser'>
254
255           <mac address='52:54:00:2a:32:74'/>
256
257           <source type='unix' path='/var/run/openvswitch/vhost-user3'
                mode='client'/>
258
259           <model type='virtio'/>
260
261           <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
                function='0x0'/>
262
263         </interface>
264
265         <interface type='vhostuser'>
266
267           <mac address='52:54:00:2a:32:84'/>
268
269           <source type='unix' path='/var/run/openvswitch/vhost-user4'
                mode='client'/>
270
271          <model type='virtio'/>
272
273           <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
                function='0x0'/>
274
275         </interface>
276
277         <serial type='pty'>
278
279           <target port='0'/>
280
281         </serial>
282
283         <console type='pty'>
```



```
284
285         <target type='serial' port='0'/>
286
287       </console>
288
289       <input type='mouse' bus='ps2'/>
290
291       <input type='keyboard' bus='ps2'/>
292
293       <graphics type='vnc' port='-1' autoport='yes'>
294
295         <listen type='address'/>
296
297       </graphics>
298
299       <video>
300
301         <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303         <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
              function='0x0'/>
304
305       </video>
306
307       <memballoon model='virtio'>
308
309         <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
              function='0x0'/>
310
311       </memballoon>
312
313     </devices>
314
315   </domain
```

Punkte zu beachten

In der XML-Datei muss die hugepage Größe 1 GB betragen, wie in der Beispieldatei gezeigt.

```
1   <memoryBacking>
2
3       <hugepages>
4
5         <page size='1048576' unit='KiB'/>
6
7       </hugepages>
```

In der Beispieldatei ist vhost-user1 auch der vhost Benutzerport, der an ovs-br0 gebunden ist.

```
1   <interface type='vhostuser'>
2
```



```
        <mac address='52:54:00:55:55:56'/>

        <source type='unix' path='/var/run/openvswitch/vhost-user1'
           mode='client'/>

        <model type='virtio'/>

        <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
           function='0x0'/>

      </interface>
```

Um die NetScaler VPX-Instanz aufzurufen, verwenden Sie den `virsh` Befehl.

Anwenden der NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem KVM-Hypervisor

October 17, 2024

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem KVM-Hypervisor anwenden. Daher kann ein Kunden-Setup auf einer VPX-Instanz in viel kürzerer Zeit konfiguriert werden.

Weitere Informationen zu Preboot-Benutzerdaten und deren Format finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start des NetScaler-Geräts in der Cloud.

> **Hinweis:**
>
> Um mithilfe von Preboot-Benutzerdaten im KVM-Hypervisor bootstrappen zu können, muss die Standard-Gateway-Konfiguration im <NS-CONFIG> Abschnitt übergeben werden. Weitere Informationen zum Inhalt des <NS-CONFIG> Transponders finden Sie im folgenden <NS-CONFIG> Abschnitt "Beispiel".

Sample <NS-CONFIG> section:

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

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

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

        <MGMT-INTERFACE-CONFIG>
```



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

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

So stellen Sie Preboot-Benutzerdaten auf dem KVM-Hypervisor bereit

Sie können Preboot-Benutzerdaten auf dem KVM-Hypervisor über eine ISO-Datei bereitstellen, die mit einem CD-ROM-Gerät angehängt wird.

Benutzerdaten mit CD-ROM-ISO-Datei bereitstellen

Sie können Virtual Machine Manager (VMM) verwenden, um Benutzerdaten mit dem CD-ROM-Gerät als ISO-Image in die virtuelle Maschine (VM) zu injizieren. KVM unterstützt CD-ROMs in VM Guest entweder durch direkten Zugriff auf ein physisches Laufwerk auf dem VM-Hostserver oder durch Zugriff auf ISO-Images.

Mit den folgenden Schritten können Sie Benutzerdaten mithilfe der CD-ROM-ISO-Datei bereitstellen:

1. Erstellen Sie eine Datei mit dem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält.

   > **Hinweis:**
   >
   > Der Dateiname muss strikt als `userdata`verwendet werden.

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

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

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

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

   ```
   root@ubuntu:~/sai/19oct# ls -lh
   total 4.0K
   -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
   root@ubuntu:~/sai/19oct#
   root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
   I: -input-charset not specified, using utf-8 (detected in locale
       settings)
   ```



```
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
```

3. Stellen Sie die NetScaler VPX-Instanz mithilfe des Standardbereitstellungsprozesses bereit, um die VM zu erstellen. But do not power on the VM automatically.
4. Fügen Sie mit Virtual Machine Manager ein CD-ROM-Gerät hinzu, indem Sie die folgenden Schritte ausführen:

   a) Doppelklicken Sie im Virtual Machine Manager auf einen VM-Gasteintrag, um dessen Konsole zu öffnen, und wechseln Sie mit Ansicht **> Details zur Ansicht Details**.
   b) Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
   c) Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus und klicken Sie auf **Fertig stellen**. Eine neue CD-ROM unter **Resources** auf Ihrer NetScaler VPX-Instanz wird erstellt.

5. Power on the VM.

NetScaler VPX auf AWS

October 17, 2024

Sie können eine NetScaler VPX-Instanz auf Amazon Web Services (AWS) starten. Die NetScaler VPX-Appliance ist als Amazon Machine Image (AMI) im AWS Marketplace verfügbar. Mit einer NetScaler VPX-Instanz auf AWS können Sie AWS-Cloud-Computing-Funktionen nutzen und NetScaler Load Balancing- und Traffic-Management-Funktionen für ihre Geschäftsanforderungen verwenden. Die VPX-Instanz unterstützt alle Funktionen der Datenverkehrsverwaltung einer physischen NetScaler Appliance und kann als eigenständige Instanzen oder in HA-Paaren bereitgestellt werden. Weitere Informationen zu VPX-Funktionen finden Sie im VPX-Datenblatt.

Erste Schritte

Bevor Sie mit Ihrer VPX-Bereitstellung beginnen, müssen Sie mit den folgenden Informationen vertraut sein:

- AWS-Terminologie
- AWS-VPX-Unterstützungsmatrix
- Einschränkungen und Nutzungsrichtlinien
- Voraussetzungen
- So funktioniert eine NetScaler VPX-Instanz auf AWS

Bereitstellen einer NetScaler VPX-Instanz auf AWS

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Eigenständig
- Hochverfügbarkeit (aktiv-Passiv)
  - Hochverfügbarkeit innerhalb derselben Zone
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Elastic IP
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Private IP
- Aktiv-Aktiv GSLB
- Autoscaling (Active-Active) mit ADM

Hybrid-Bereitstellungen

- Bereitstellen von NetScaler in AWS Outpost
- Bereitstellen von NetScaler in VMC in AWS

Lizenzierung

Für eine NetScaler VPX-Instanz auf AWS ist eine Lizenz erforderlich. Die folgenden Lizenzoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf AWS ausgeführt werden:

- Kostenlos (unbegrenzt)
- Stündlich
- jährlich
- BYOL
- Kostenlose Testversion (alle NetScaler VPX-AWS-Abonnementangebote für 21 Tage kostenlos im AWS Marketplace.)

Automatisierung

- NetScaler ADM: Intelligente Bereitstellung

- GitHub CFTs: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Ansible: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Terraform: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- AWS-Pattern-Bibliothek (PL): NetScaler VPX

Blogs

- Wie NetScaler auf AWS Kunden hilft, Anwendungen sicher bereitzustellen
- Anwendungsbereitstellung in Hybrid Cloud mit NetScaler und AWS
- Citrix ist ein AWS-Netzwerkkompetenzpartner
- NetScaler: Immer bereit für Public Clouds
- Einfache Skalierung oder Skalierung in öffentlichen Clouds mit NetScaler
- Citrix erweitert die Auswahl an ADC-Bereitstellungen mit AWS Outposts
- Verwenden von NetScaler mit Amazon VPC-Ingress-Routing
- Citrix bietet Auswahl, Leistung und vereinfachte Bereitstellung in AWS
- Die Sicherheit der NetScaler Web App Firewall —jetzt auf dem AWS Marketplace
- Wie Aria Systems die NetScaler Web App Firewall auf AWS verwendet

Videos

- Vereinfachung der Public Cloud NetScaler-Bereitstellungen durch ADM
- Provisioning und Konfiguration von NetScaler VPX in AWS mit sofort einsatzbereiten Terraform-Skripten
- Bereitstellen von NetScaler HA in AWS mithilfe der CloudFormation-Vorlage
- Bereitstellen von NetScaler HA über Availability Zones hinweg mit AWS QuickStart
- NetScaler Autoscale mit ADM

Fallstudien von Kunden

- Technologielösung —Xenit AB
- Ein besserer Weg, um mit Citrix und AWS Cloud Geschäfte zu machen —Aria
- Entdecken Sie den Vorteil von NetScaler und AWS
- Regen zu vermieten - Kundenbericht

Lösungen

- Bereitstellung einer digitalen Werbeplattform auf AWS mit NetScaler
- Verbesserung der Clickstream-Analyse in AWS mit NetScaler

Support

- Öffnen eines Support-Falls
- Informationen zum NetScaler-Abonnementangebot finden Sie unter Fehlerbehebung bei einer VPX-Instanz auf AWS. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer AWS-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support.
- Stellen Sie für NetScaler Customer Licensed Offering oder BYOL sicher, dass Sie über den gültigen Support- und Wartungsvertrag verfügen. Wenn Sie keine Vereinbarung haben, wenden Sie sich an Ihren NetScaler-Ansprechpartner.

Zusätzliche Referenzen

- AWS-Webinar auf Abruf —NetScaler auf AWS
- NetScaler VPX —Datenblatt
- NetScaler im AWS Marketplace
- NetScaler ist Teil der AWS-Netzwerkpartnerlösungen (Load Balancer)
- AWS FAQs

AWS-Terminologie

October 17, 2024

In diesem Abschnitt wird die Liste der häufig verwendeten AWS-Begriffe und -Ausdrücke beschrieben. Weitere Informationen finden Sie unter AWS Glossar.

Begriff	Definition
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.

Begriff	Definition
Elastic Block Store	Bietet persistente Blockspeicher-Volumes für die Verwendung mit Amazon EC2-Instanzen in der AWS-Cloud.
Einfacher Speicherservice (S3)	Speicher für das Internet. Es wurde entwickelt, um Web-Scale-Computing für Entwickler einfacher zu machen.
Elastic Compute Cloud (EC2)	Ein Webservice, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastic Load Balancing (ELB)	Verteilt eingehenden Anwendungsdatenverkehr auf mehrere EC2-Instances in mehreren Availability Zones. Dies erhöht die Fehlertoleranz Ihrer Anwendungen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer Virtual Private Cloud (VPC) anhängen können.
Elastische IP-Adresse (EIP)	Eine statische, öffentliche IPv4-Adresse, die Sie in Amazon EC2 oder Amazon VPC zugewiesen und dann an eine Instance angehängt haben. Elastic IP-Adressen sind mit Ihrem Konto verknüpft, nicht mit einer bestimmten Instanz. Sie sind elastisch, da Sie sie leicht zuordnen, anbringen, abnehmen und freigeben können, wenn sich Ihre Bedürfnisse ändern.
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.

Begriff	Definition
Identity and Access Management (IAM)	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen. Die IAM-Rolle ist erforderlich, um VPX-Instanzen in einem Hochverfügbarkeits-Setup bereitzustellen.
Internet-Gateway	Verbindet ein Netzwerk mit dem Internet. Sie können den Datenverkehr für IP-Adressen außerhalb Ihrer VPC an das Internet-Gateway weiterleiten.
Schlüsselpaar	Eine Reihe von Sicherheitsanmeldeinformationen, mit denen Sie Ihre Identität elektronisch nachweisen. Ein Schlüsselpaar besteht aus einem privaten Schlüssel und einem öffentlichen Schlüssel.
Routentabellen	Eine Reihe von Routing-Regeln, die den Datenverkehr steuern, der jedes Subnetz verlässt, das der Routing-Tabelle zugeordnet ist. Sie können einer einzigen Routing-Tabelle mehrere Subnetze zuordnen, aber ein Subnetz kann jeweils nur einer Routing-Tabelle zugeordnet werden.
Sicherheitsgruppen	Ein benannter Satz zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an den EC2-Instanzen angehängt werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und Betriebsanforderungen zu gruppieren.
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Begriff	Definition
Automatische Skalierung	Ein Webservice zum automatischen Starten oder Beenden von Amazon EC2-Instanzen basierend auf benutzerdefinierten Richtlinien, Zeitplänen und Zustandsprüfungen.
CloudFormation	Ein Service zum Schreiben oder Ändern von Vorlagen, die zugehörige AWS-Ressourcen zusammen als Einheit erstellen und löschen.

AWS-VPX-Unterstützungsmatrix

October 17, 2024

In den folgenden Tabellen sind das unterstützte VPX-Modell und die AWS-Regionen, Instanztypen und Dienste aufgeführt.

Tabelle 1: Unterstützte VPX-Modelle auf AWS

Unterstütztes VPX-Modell
NetScaler VPX Advanced − 200 Mbit/s
NetScaler VPX Premium –1 Gbit/s
NetScaler VPX Premium –5 Gbit/s
NetScaler VPX Express –20 Mbit/s
NetScaler VPX –Kundenlizenz
NetScaler VPX FIPS –Kundenlizenz
NetScaler VPX FIPS ENA –Kundenlizenz

Tabelle 2: Unterstützte AWS-Regionen

Unterstützte AWS Regionen
USA West (Oregon)
USA West (Nordkalifornien) Kalifornien)
USA Ost (Ohio)

USA Ost (Nord-Virginia) Virginia)
Asien-Pazifik (Mumbai)
Asien-Pazifik (Seoul)
Asien-Pazifik (Singapur)
Asien-Pazifik (Sydney)
Asien-Pazifik (Tokio)
Asien-Pazifik (Hongkong)
Asien-Pazifik (Osaka)
Asien-Pazifik (Jakarta)
Asien-Pazifik (Hyderabad)
Kanada (Central)
EU (Frankfurt)
EU (Irland)
EU (London)
EU (Paris)
EU (Mailand)
Südamerika (São Paulo)
AWS GovCloud (USA-Ost)
AWS GovCloud (USA, West)
AWS Streng geheim (C2S)
Naher Osten (Bahrain)
Afrika (Kapstadt)
C2S

> **Hinweis:**
>
> Für die AWS-Region Hongkong ist NetScaler VPX-Unterstützung nur mit BYOL-Lizenzen verfügbar.

Tabelle 3: Unterstützte AWS-Instanztypen

Unterstützte AWS-Instanztypen
c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge
c5.large, c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.18xlarge, c5.24xlarge
c5n.large, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge
d2.xlarge, d2.2xlarge, d2.4xlarge, d2.8xlarge
m3.large, m3.xlarge, m3.2xlarge
m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge
m5.large, m5.xlarge, m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.12xlarge, m5.16xlarge, m5.24xlarge
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.8xlarge, m6i.12xlarge, m6i.16xlarge, m6i.24xlarge, m6i.32xlarge |
| r7iz.large, r7iz.xlarge, r7iz.2xlarge, r7iz.4xlarge, r7iz.8xlarge, r7iz.12xlarge, r7iz.16xlarge, r7iz.32xlarge |
| t2.medium, t2.large, t2.xlarge, t2.2xlarge |
| t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge |

> **Hinweis:**
>
> NetScaler VPX, das auf den AWS-Instance-Typen m6i und r7iz bereitgestellt wird, unterstützt die ENA-Funktion für Warteschlangen mit niedriger Latenz (LLQ) nicht.

Tabelle 4: Unterstützte AWS-Services

Unterstützte AWS Services
EC2: Startet ADC-Instanzen.
Lambda: Ruft NetScaler VPX NITRO-APIs während der Bereitstellung von NetScaler VPX-Instanzen über CFT auf.
VPC- und VPC-Ingress-Routing: VPC erstellt isolierte Netzwerke, in denen ADC gestartet werden kann. Das VPC I
Route53: Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung.
ELB: Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung.
Cloudwatch: Überwacht Leistung und Systemparameter für die NetScaler VPX Instanz.
AWS Autoscaling: Wird für die automatische Skalierung von Backend-Servern verwendet.
Cloud-Bildung: CloudFormation-Vorlagen werden verwendet, um NetScaler VPX-Instanzen bereitzustellen.
Simple Queue Service (SQS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-Autos
Simple Notification Service (SNS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-
Identitäts- und Zugriffsmanagement (IAM): Bietet Zugriff auf AWS-Services und -Ressourcen.
AWS-Außenposten: Bereitstellung von NetScaler VPX-Instanzen in AWS Outposts.

NetScaler empfiehlt die folgenden AWS-Instanztypen:

- M5- und C5n-Serien für Marketplace-Editionen oder bandbreitenbasierte Poollizenzierung.
- C5n-Serie für vCPU-basierte Pool-Lizenzierung.

VPX-Angebot auf dem AWS-Marktplatz	AWS-Instanzempfehlung
VPX Express 20, VPX 200	M5.xLarge
VPX 1G, VPX 5G	M5.2xLarge

NetScaler empfiehlt die folgenden AWS-Instanztypen basierend auf dem Durchsatz.

VPX mit gepoolter Lizenzierung (Bandbreitenlizenzen)	AWS-Instanzempfehlung
VPX 8G	C5n.4xLarge
VPX 10G, VPX 15G, VPX 25G	C5n.9xLarge

> **Hinweis:**
>
> Das VPX 25G-Angebot bietet nicht den gewünschten 25-G-Durchsatz in AWS, kann jedoch eine höhere SSL-Transaktionsrate bieten.

Gehen Sie wie folgt vor, um einen Durchsatz von mehr als 5G zu erreichen:

- Wählen Sie **NetScaler VPX – Customer Licensed (BYOL) im AWS-Marktplatz**.
- Wählen Sie **Pooled Licensing (Bandbreitenlizenzen)** in der NetScaler GUI oder CLI aus.

Um Ihre Instanz anhand verschiedener Metriken wie Pakete pro Sekunde und SSL-Transaktionsrate zu ermitteln, wenden Sie sich an Ihren NetScaler-Ansprechpartner, um Hilfe zu erhalten. Hinweise zur Lizenzierung und Dimensionierung von vCPU-basierten Pools erhalten Sie beim NetScaler-Support.

Einschränkungen und Nutzungsrichtlinien

October 17, 2024

Bei der Bereitstellung einer NetScaler VPX-Instanz in AWS gelten die folgenden Einschränkungen und Verwendungsrichtlinien:

- Lesen Sie vor dem Start den Abschnitt zur AWS-Terminologie in Bereitstellen einer NetScaler VPX-Instanz auf AWS.
- Das Clustering-Feature wird für VPX nicht unterstützt.

- Damit das Hochverfügbarkeitssetup effektiv funktioniert, verknüpfen Sie ein dediziertes NAT-Gerät der Verwaltungsschnittstelle oder verknüpfen Sie EIP mit NSIP. Weitere Informationen zu NAT finden Sie in der AWS-Dokumentation unter NAT-Instances.
- Datenverkehr und Verwaltungsverkehr müssen durch ENIs getrennt werden, die zu verschiedenen Subnetzen gehören.
- Nur die NSIP-Adresse darf auf der Management-ENI vorhanden sein.
- Wenn eine NAT-Instanz zur Sicherheit verwendet wird, anstatt dem NSIP einen EIP zuzuweisen, sind entsprechende Änderungen beim Routing auf VPC-Ebene erforderlich. Anweisungen zum Vornehmen von Routingänderungen auf VPC-Ebene finden Sie in der AWS-Dokumentation unter Szenario 2: VPC mit öffentlichen und privaten Subnetzen.
- Eine VPX-Instanz kann von einem EC2-Instanztyp in einen anderen verschoben werden (z. B. von m3.large zu m3.xlarge).
- Für Speicheroptionen für VPX in AWS empfiehlt Citrix EBS, da es dauerhaft ist und die Daten auch verfügbar sind, nachdem sie von der Instanz getrennt wurden.
- Das dynamische Hinzufügen von ENIs zu VPX wird nicht unterstützt. Starten Sie die VPX-Instanz neu, um das Update anzuwenden. Citrix empfiehlt, die eigenständige Instanz oder die HA-Instanz zu beenden, das neue ENI anzuhängen und die Instanz dann neu zu starten.
- Sie können einem ENI mehrere IP-Adressen zuweisen. Die maximale Anzahl von IP-Adressen pro ENI wird durch den EC2-Instanztyp bestimmt, siehe Abschnitt "IP-Adressen pro Netzwerkschnittstelle pro Instanztyp"in Elastic Network Interfaces. Sie müssen die IP-Adressen in AWS zuweisen, bevor Sie sie ENIs zuweisen. Weitere Informationen finden Sie unter Elastic Network Interfaces.
- Citrix empfiehlt, die Interface-Befehle zum Aktivieren und Deaktivieren von NetScaler VPX Schnittstellen zu vermeiden.
- Die NetScaler Befehle `set ha node \\<NODE\\_ID\\> -haStatus STAYPRIMARY` und `set ha node \\<NODE\\_ID\\> -haStatus STAYSECONDARY` sind standardmäßig deaktiviert.
- IPv6 wird für VPX nicht unterstützt.
- Aufgrund von AWS-Einschränkungen werden diese Funktionen nicht unterstützt:
  - Gratuitous ARP(GARP)
  - L2-Modus
  - Getaggtes VLAN
  - Dynamisches Routing
  - virtueller MAC

- Stellen Sie sicher, dass die **Quell-/Zielprüfung** deaktiviert ist, damit RNAT funktioniert. Weitere Informationen finden Sie unter "Ändern der Quelle/Zielüberprüfung"in Elastic Network Interfaces.
- In einer NetScaler VPX Bereitstellung auf AWS in einigen AWS-Regionen kann die AWS-Infrastruktur möglicherweise keine AWS-API-Aufrufe auflösen. Dies passiert, wenn die API-Aufrufe über eine Nicht-Verwaltungsschnittstelle auf der NetScaler VPX-Instanz ausgegeben werden. Beschränken Sie zur Problemumgehung die API-Aufrufe nur auf die Verwaltungsschnittstelle. Erstellen Sie dazu ein NSVLAN auf der VPX-Instanz und binden Sie die Verwaltungsschnittstelle mit dem entsprechenden Befehl an das NSVLAN. Beispiel: `setze ns-Konfiguration -nsvlan <vlan id> -ifnum 1/1 -tagged NO Konfiguration speichern` Starten Sie die VPX-Instanz an der Eingabeaufforderung neu. Weitere Informationen zum Konfigurieren `nsvlan`finden Sie unter Konfigurieren von NSVLAN.
- In der AWS-Konsole kann die vCPU-Auslastung, die für eine VPX-Instanz auf der Registerkarte **Überwachung** angezeigt wird, hoch sein (bis zu 100 Prozent), selbst wenn die tatsächliche Auslastung wesentlich geringer ist. Um die tatsächliche vCPU-Auslastung **anzuzeigen, navigieren Sie zu Alle CloudWatch-Metriken**anzeigen. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instanzen mit Amazon CloudWatch.
- Hot Adding wird nur für PV- und SRIOV-Schnittstellen mit NetScaler auf AWS unterstützt. VPX-Instanzen mit ENA-Schnittstellen unterstützen kein Hot-Plug, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn Hot-Plugging versucht wird.
- Hot-Removal über die AWS-Webkonsole oder die AWS CLI-Schnittstelle wird mit den PV-, SRIOV- und ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn versucht wird, Hot-Removal durchzuführen.

Voraussetzungen

October 17, 2024

Bevor Sie versuchen, eine VPX-Instanz in AWS zu erstellen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- **Ein AWS-Konto**: zum Starten eines NetScaler VPX AMI in einer AWS Virtual Private Cloud (VPC). Sie können auf www.aws.amazon.com kostenlos ein AWS-Konto erstellen.
- **Ein AWS Identity and Access Management (IAM) -Benutzerkonto**: zum sicheren Steuern des Zugriffs auf AWS-Services und -Ressourcen für Ihre Benutzer. Weitere Informationen zum Erstellen eines IAM-Benutzerkontos finden Sie unter Erstellen von IAM-Benutzern (Konsole). Eine

IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss für verschiedene Szenarien über die folgenden IAM-Berechtigungen verfügen.

HA-Paar mit IPv4-Adressen in derselben AWS-Zone:

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

HA-Paar mit IPv6-Adressen in derselben AWS-Zone:

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

HA-Paar mit IPv4- und IPv6-Adressen in derselben AWS-Zone:

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

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

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

HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
```


HA-Paar mit privaten IP- und Elastic IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
```

Autoscaling des AWS-Backends:

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListTopics",
"sns:Subscribe",
"sqs:CreateQueue",
"sqs:ListQueues",
"sqs:DeleteMessage",
"sqs:GetQueueAttributes",
"sqs:SetQueueAttributes",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
```

> **Hinweis:**
>
> - Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen für jede der Funktionen.
> - Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt es nicht, eine bereits erstellte IAM-Rolle auszuwählen.
> - Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.

- **AWS CLI**: So verwenden Sie alle Funktionen, die von der AWS Management Console aus Ihrem Terminalprogramm bereitgestellt werden. Weitere Informationen finden Sie im AWS CLI-Benutzerhandbuch. Sie benötigen auch die AWS CLI, um den Netzwerkschnittstellentyp in SR-IOV zu ändern.
- **Elastic Network Adapter (ENA)**: Für den treiberfähigen ENA-Instanz-Typ, z. B. M5-, C5-Instanzen, muss die Firmware-Version 13.0 und höher sein.

- Sie müssen den Instance Metadata Service (IMDS) auf der EC2-Instance für NetScaler VPX konfigurieren. IMDSv1 und IMDSv2 sind zwei Modi, die für den Zugriff auf Instance-Metadaten von einer laufenden AWS EC2-Instance verfügbar sind. IMDSv2 ist sicherer als IMDSv1. Sie können die Instanz so konfigurieren, dass sie entweder beide Methoden (die Standardoption) oder nur den IMDSv2-Modus verwendet (indem Sie IMDSv1 deaktivieren). Citrix ADC VPX unterstützt ab NetScaler VPX Version 13.1.48.x nur den IMDSv2-Modus.

AWS IAM-Rollen auf der NetScaler VPX-Instanz konfigurieren

October 17, 2024

Anwendungen, die auf einer Amazon EC2-Instanz ausgeführt werden, müssen AWS-Anmeldeinformationen in den AWS-API-Anfragen enthalten. Sie können AWS-Anmeldeinformationen direkt in der Amazon EC2-Instanz speichern und Anwendungen in dieser Instanz erlauben, diese Anmeldeinformationen zu verwenden. Dann müssen Sie jedoch die Anmeldeinformationen verwalten und sicherstellen, dass sie die Anmeldeinformationen sicher an jede Instanz weitergeben, und jede Amazon EC2-Instanz aktualisieren, wenn es Zeit ist, die Anmeldeinformationen zu wechseln. Das ist eine Menge zusätzlicher Arbeit.

Stattdessen können und müssen Sie eine Identity and Access Management (IAM) -Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2-Instanz ausgeführt werden. Wenn Sie eine Rolle verwenden, müssen Sie keine langfristigen Anmeldeinformationen (wie Benutzername und Kennwort oder Zugriffsschlüssel) an eine Amazon EC2-Instanz verteilen. Stattdessen bietet die Rolle temporäre Berechtigungen, die Anwendungen verwenden können, wenn sie andere AWS-Ressourcen aufrufen. Wenn Sie eine Amazon EC2-Instanz starten, geben Sie eine IAM-Rolle an, die der Instanz zugeordnet werden soll. Anwendungen, die auf der Instanz ausgeführt werden, können dann die von der Rolle bereitgestellten temporären Anmeldeinformationen verwenden, um API-Anfragen zu signieren.

Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss für verschiedene Szenarien über die folgenden IAM-Berechtigungen verfügen.

HA-Paar mit IPv4-Adressen in derselben AWS-Zone:

```
1    "ec2:DescribeInstances",
2    "ec2:AssignPrivateIpAddresses",
3    "iam:SimulatePrincipalPolicy",
4    "iam:GetRole"
```

HA-Paar mit IPv6-Adressen in derselben AWS-Zone:

```
1    "ec2:DescribeInstances",
2    "ec2:AssignIpv6Addresses",
```



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

HA-Paar mit IPv4- und IPv6-Adressen in derselben AWS-Zone:

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

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

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

HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

```
    "ec2:DescribeInstances",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
    "ec2:CreateRoute",
    "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

HA-Paar mit privaten IP- und Elastic IP-Adressen über verschiedene AWS-Zonen hinweg:

```
    "ec2:DescribeInstances",
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
    "ec2:CreateRoute",
    "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

Autoscaling des AWS-Backends:

```
    "ec2:DescribeInstances",
    "autoscaling:*",
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:ListTopics",
    "sns:Subscribe",
```



```
7     "sqs:CreateQueue",
8     "sqs:ListQueues",
9     "sqs:DeleteMessage",
10    "sqs:GetQueueAttributes",
11    "sqs:SetQueueAttributes",
12    "iam:SimulatePrincipalPolicy",
13    "iam:GetRole"
```

Wichtige Hinweise:

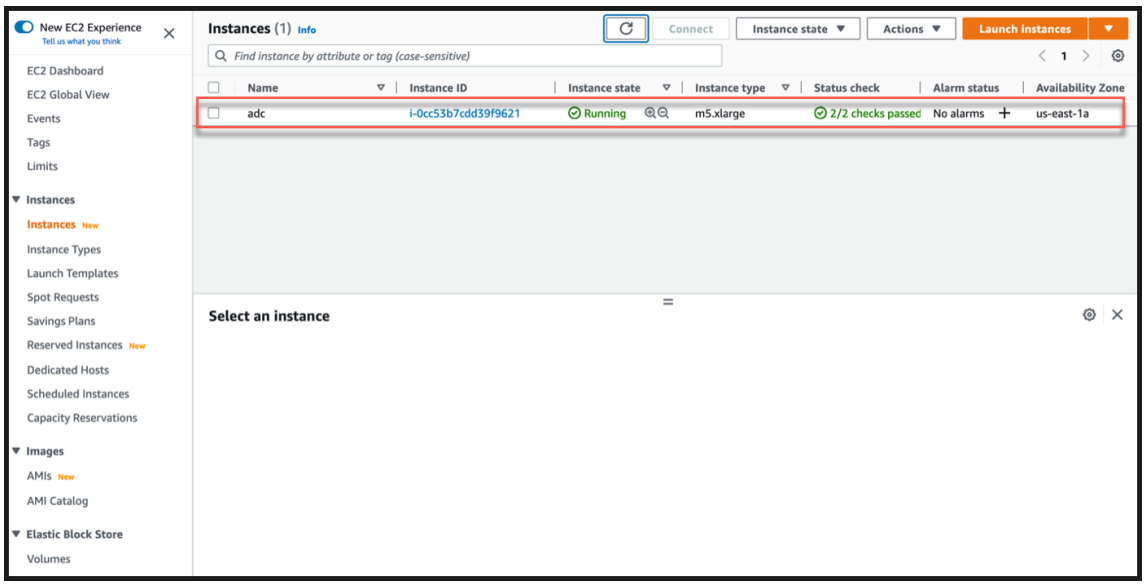
- Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen für jede der Funktionen.
- Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt es nicht, eine bereits erstellte IAM-Rolle auszuwählen.
- Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.
- Eine IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

Erstellen einer IAM-Rolle

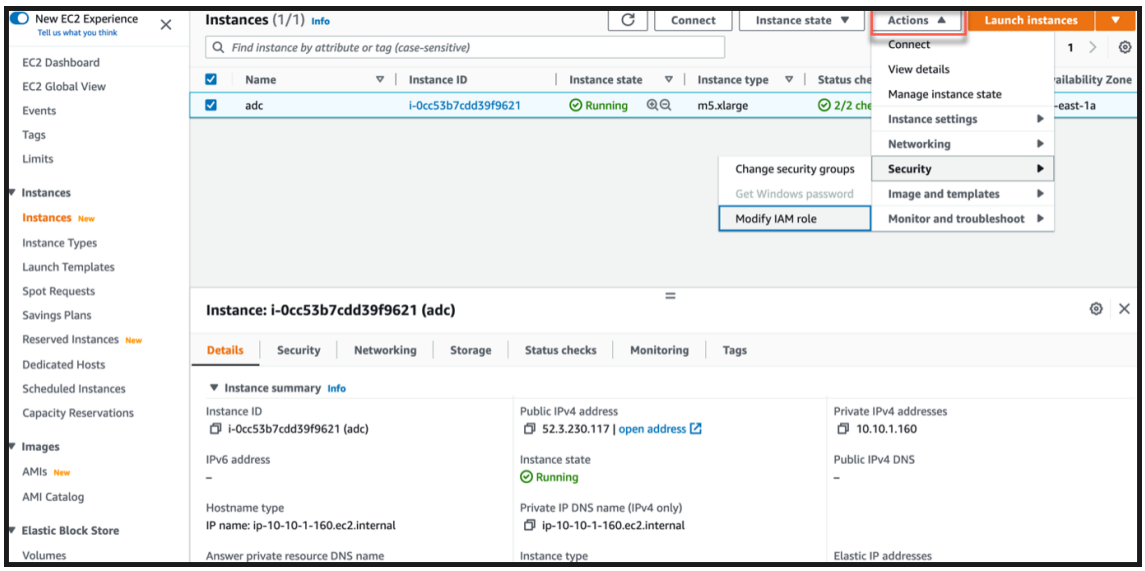
Dieses Verfahren beschreibt, wie Sie eine IAM-Rolle für die AWS-Back-End-Autoscaling-Funktion erstellen.

> **Hinweis:**
>
> Sie können dasselbe Verfahren anwenden, um alle IAM-Rollen zu erstellen, die anderen Funktionen entsprechen.

1. Melden Sie sich an der AWS-Managementkonsole für EC2an.
2. Gehen Sie zur EC2-Instanz-Seite und wählen Sie Ihre ADC-Instanz aus.

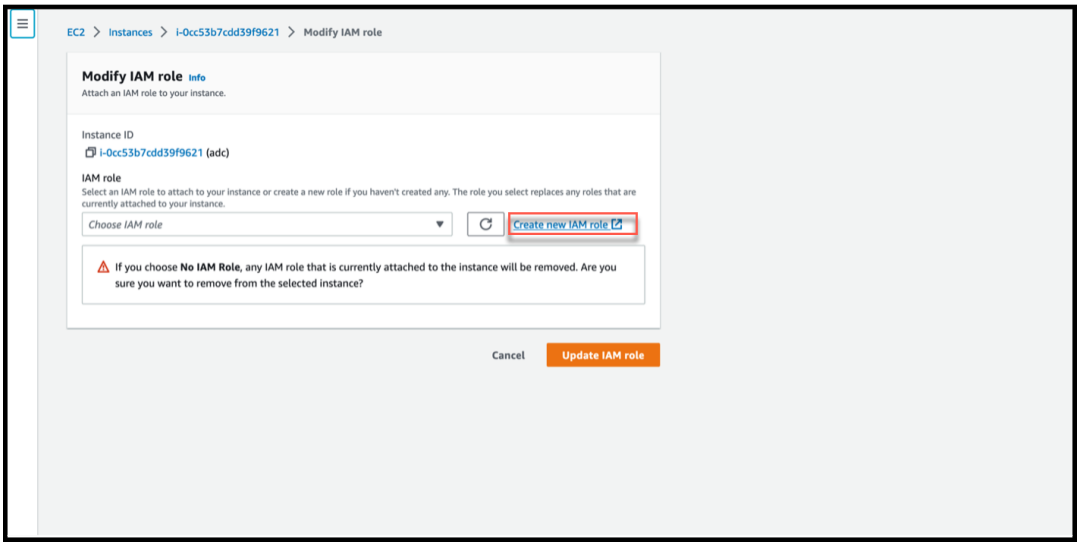


3. Navigieren Sie zu **Aktionen > Sicherheit > IAM-Rolle ändern**.

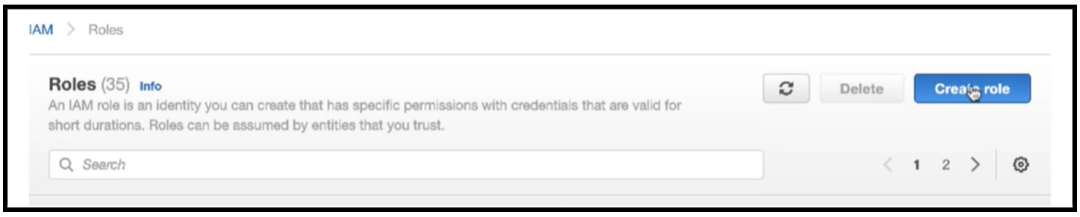


4. Auf der Seite "**IAM-Rolle ändern** "können Sie entweder eine bestehende IAM-Rolle auswählen oder eine IAM-Rolle erstellen.
5. Gehen Sie wie folgt vor, um eine IAM-Rolle zu erstellen:

    a) Klicken Sie auf der Seite "**IAM-Rolle ändern** "auf **Neue IAM-Rolle erstellen**.

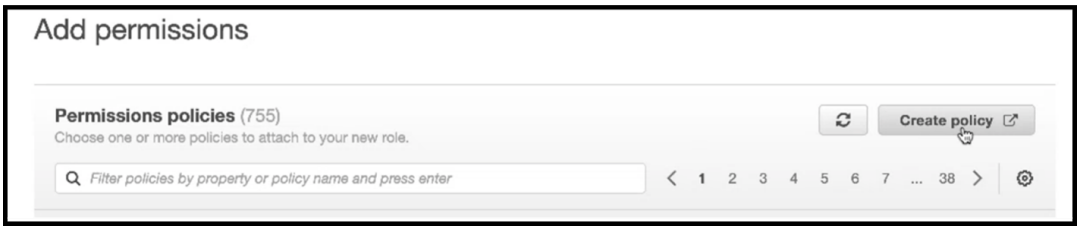


b) Klicken Sie auf der Seite **Rollen** auf **Rolle erstellen**.



c) Wählen Sie **AWS-Service** unter **Trusted Entity Type** und **EC2** unter **Common Use Cases** aus und klicken Sie dann auf **Weiter**.

d) Klicken Sie auf der Seite "**Berechtigungen hinzufügen** "auf **Richtlinie erstellen**.



e) Klicken Sie auf den **JSON-Tab**, um den JSON-Editor zu öffnen.

f) Löschen Sie im JSON-Editor alles und fügen Sie die IAM-Berechtigungen für die Funktion ein, die Sie verwenden möchten.

Fügen Sie beispielsweise die folgenden IAM-Berechtigungen für die AWS-Back-End-Autoscaling-Funktion ein:

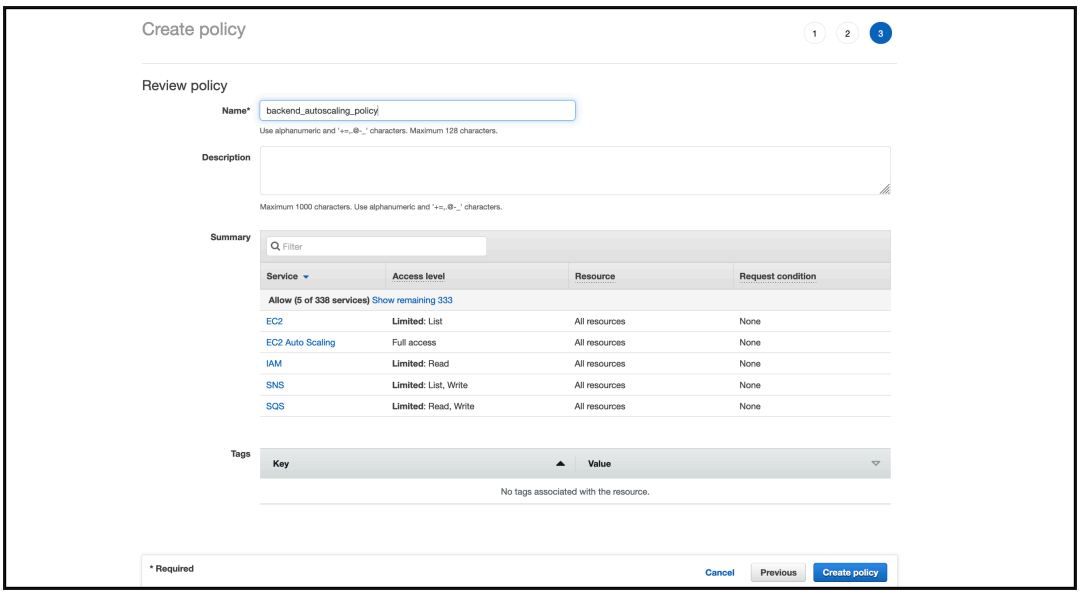
```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "autoscaling:*",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListTopics",
                "sns:Subscribe",
                "sqs:CreateQueue",
                "sqs:ListQueues",
                "sqs:DeleteMessage",
                "sqs:GetQueueAttributes",
                "sqs:SetQueueAttributes",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*"
        }

    ]
}
```

Stellen Sie sicher, dass das Schlüsselwertpaar “Version”, das Sie angeben, mit dem iden-

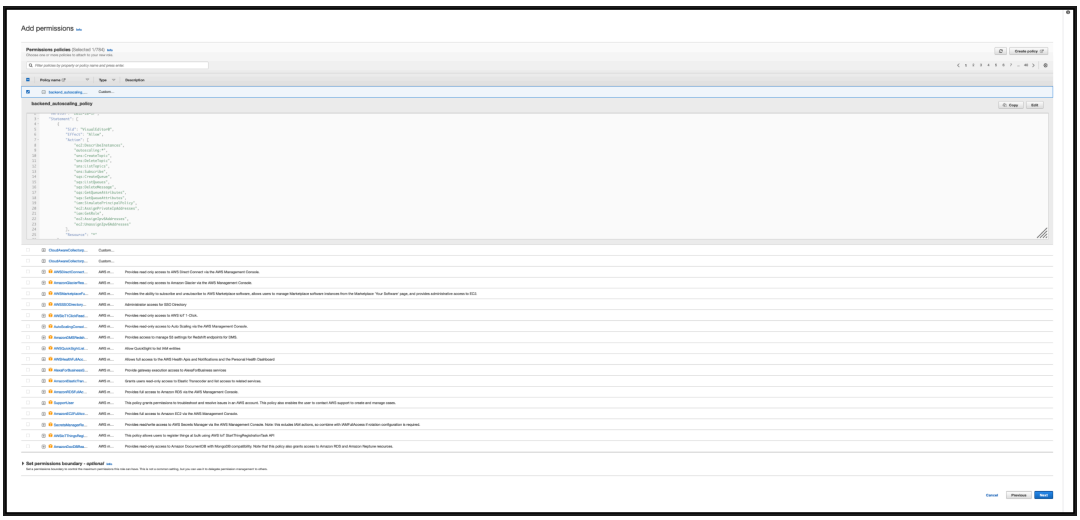
tisch ist, das automatisch von AWS generiert wird.

g) Klicken Sie auf **Weiter: Überprüfen**.

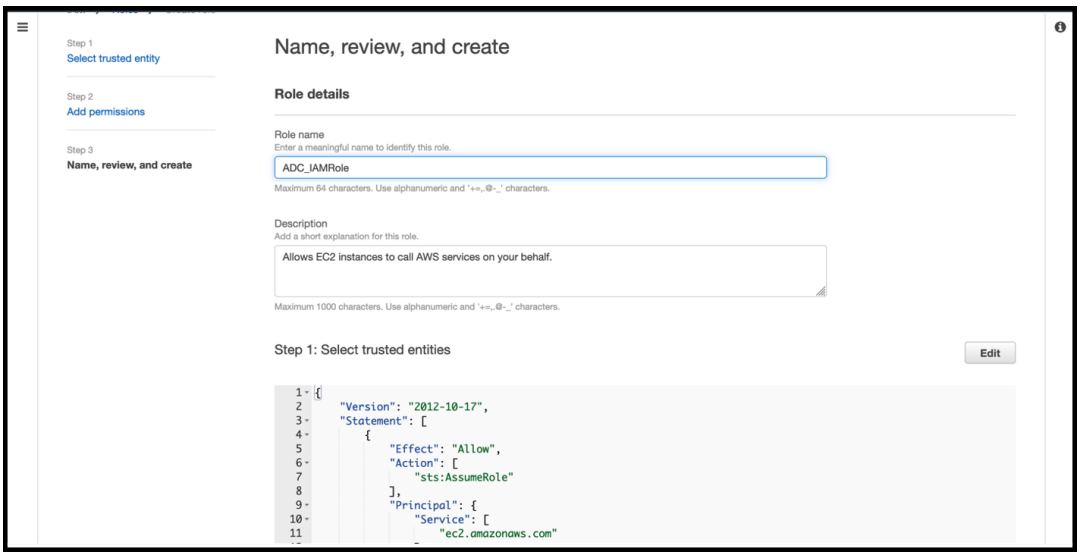
h) Geben Sie auf der Registerkarte **Richtlinie überprüfen** der Richtlinie einen gültigen Namen und klicken Sie auf **Richtlinie erstellen**.



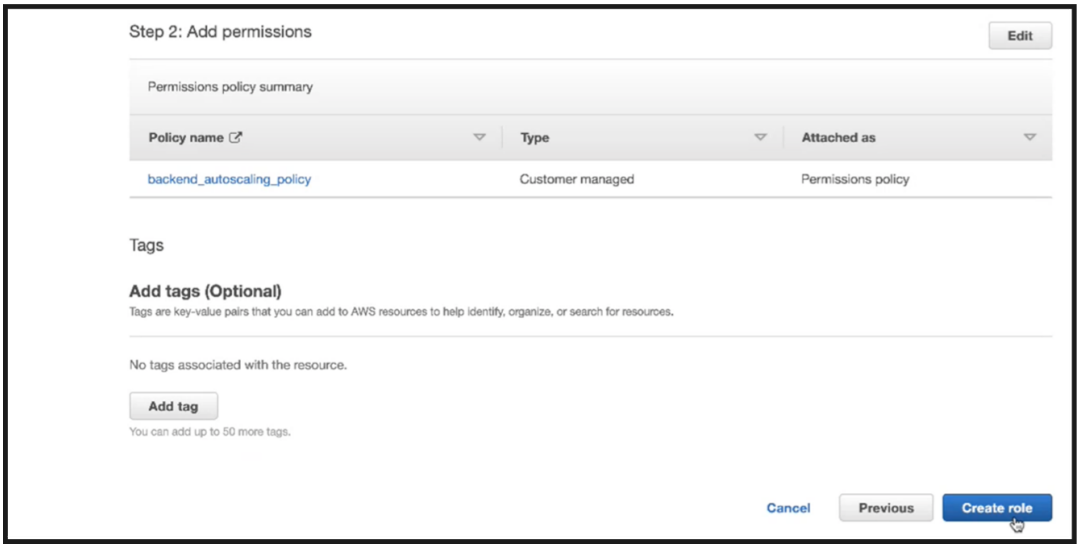
i) Klicken Sie auf der Seite **Identity Access Management** auf den Richtliniennamen, den Sie erstellt haben. Erweitern Sie die Richtlinie, um den gesamten JSON-Code zu überprüfen, und klicken Sie auf **Weiter**.



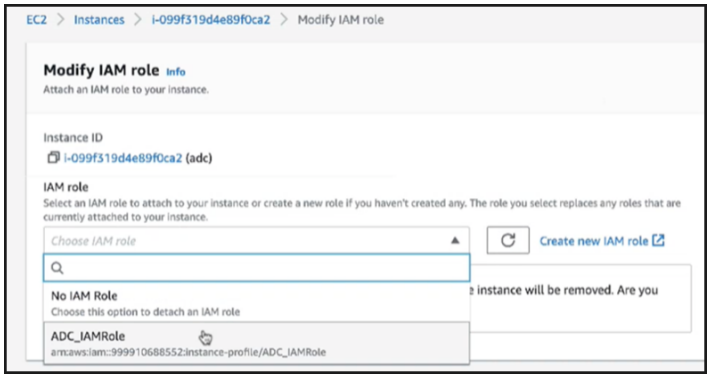
j) Geben Sie der Rolle auf der Seite **Name, Überprüfung und Erstellen** einen gültigen Namen.



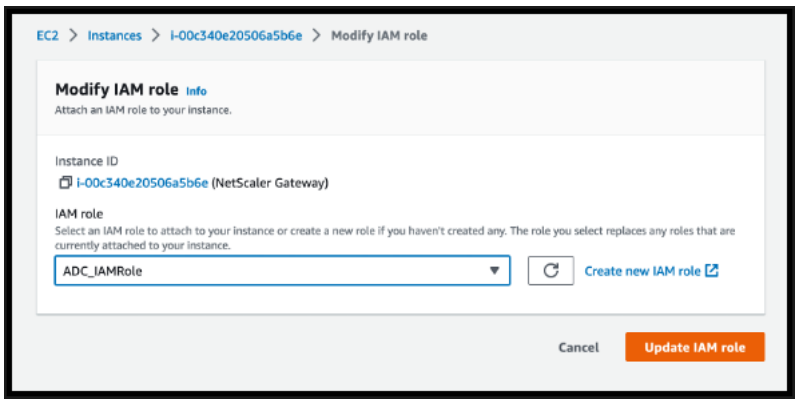
k) Klicken Sie auf **Rolle erstellen**.



6. Wiederholen Sie die Schritte 1, 2 und 3. Wählen Sie die Schaltfläche **Aktualisieren** und dann das Dropdownmenü aus, um die von Ihnen erstellte Rolle zu sehen.



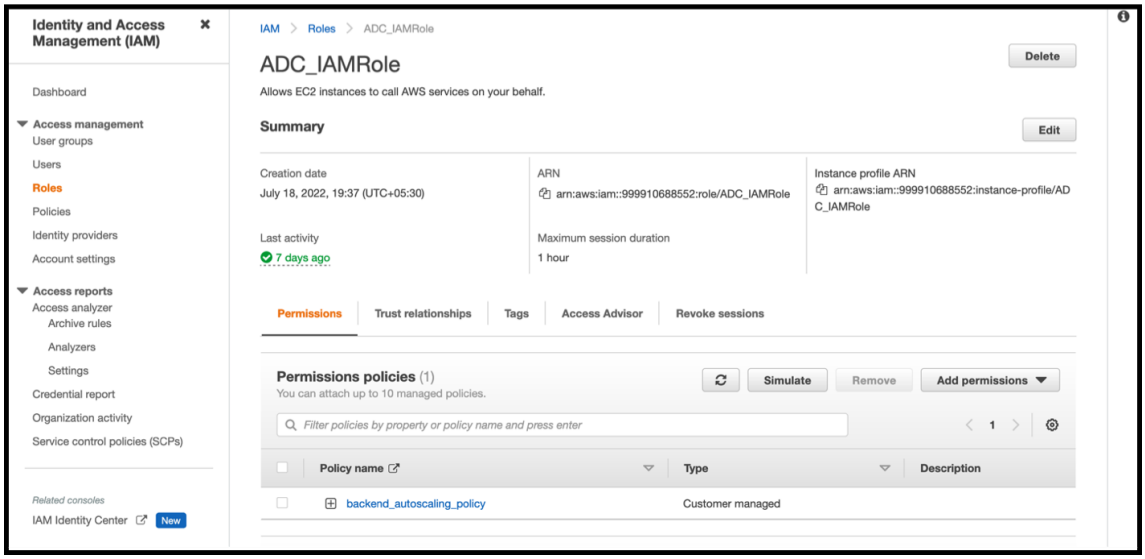
7. Klicken Sie auf **IAM-Rolle aktualisieren**.



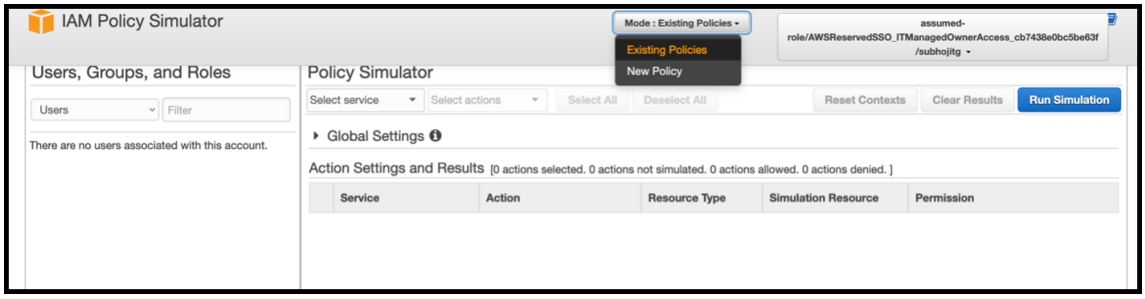
Testen Sie IAM-Richtlinien mit dem IAM-Richtliniensimulator

Der IAM-Richtliniensimulator ist ein Tool, mit dem Sie die Auswirkungen von IAM-Zugriffskontrollrichtlinien testen können, bevor Sie sie in die Produktion übernehmen. Es ist einfacher, Berechtigungen zu überprüfen und Fehler zu beheben.

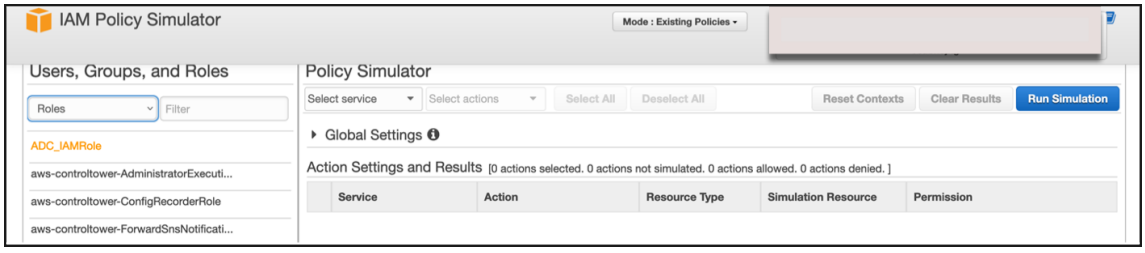
1. Wählen Sie auf der **IAM-Seite** die IAM-Rolle aus, die Sie testen möchten, und klicken Sie auf **Simulieren**. Im folgenden Beispiel ist “ADC_IAMRole”die IAM-Rolle.



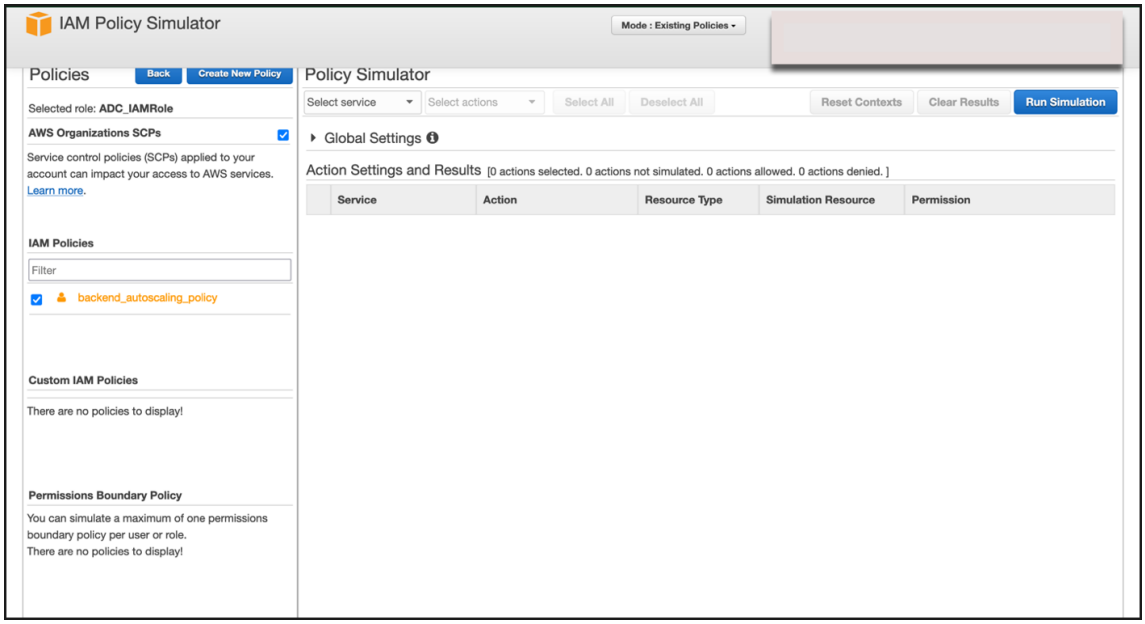
2. Wählen Sie in der **IAM-Policy Simulator-KonsoleExisting Policies**als**Modus** aus.



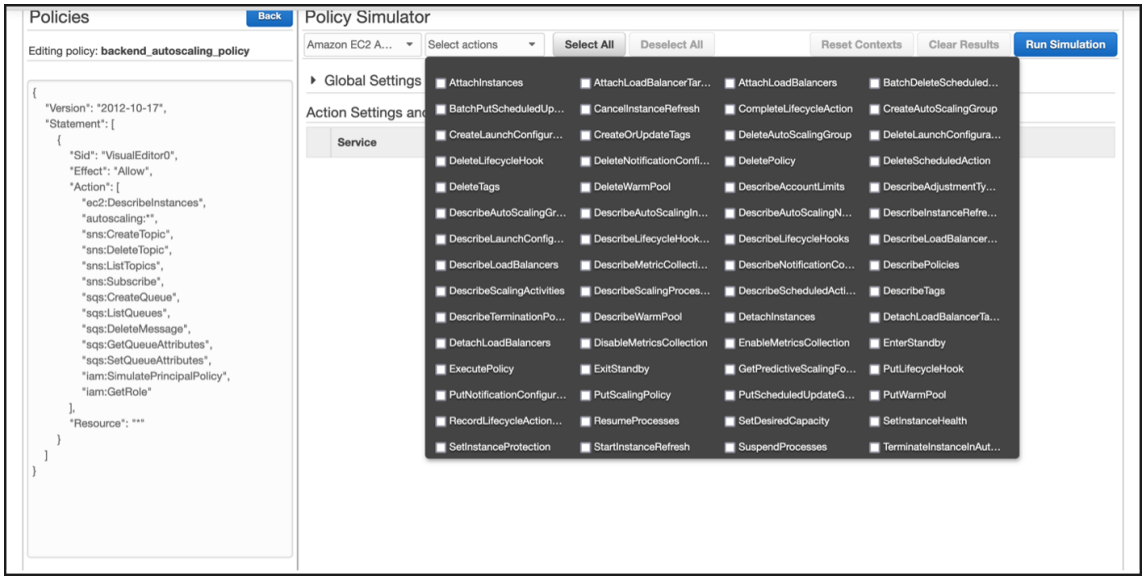
3. Wählen Sie auf der Registerkarte **Benutzer, Gruppen und Rollen** die Option **Rollen** aus dem Dropdownmenü aus und wählen Sie eine vorhandene Rolle aus.



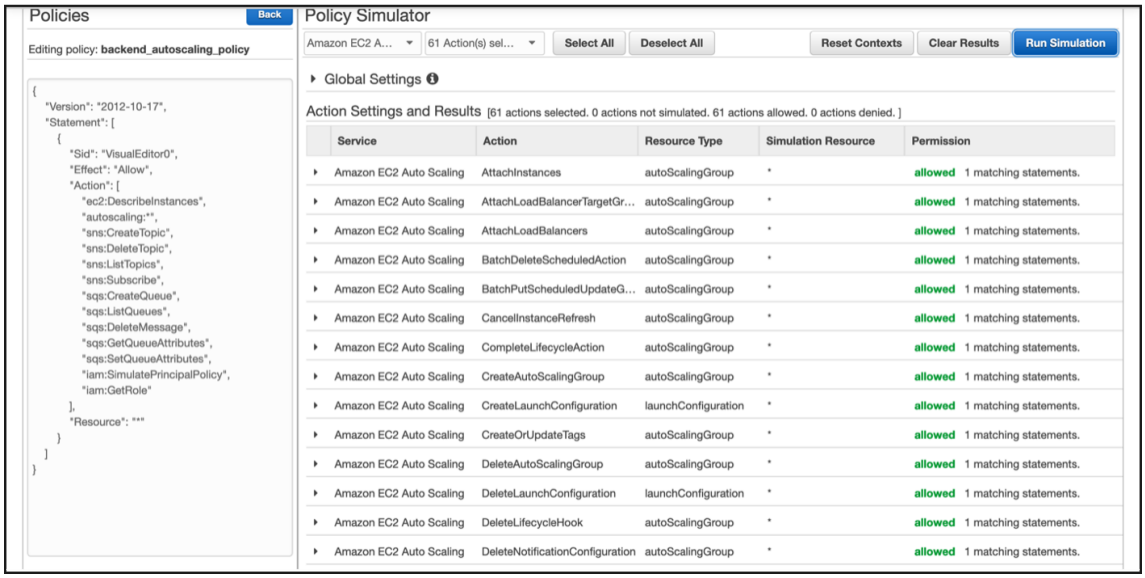
4. Nachdem Sie die vorhandene Rolle ausgewählt haben, wählen Sie die darunter befindliche Richtlinie aus.



5. Nachdem Sie die Richtlinie ausgewählt haben, können Sie den genauen JSON-Code auf der linken Seite des Bildschirms sehen. Wählen Sie die gewünschten Aktionen im Dropdownmenü **Aktionen auswählen** aus.



6. Klicken Sie auf **Simulation ausführen**.



Detaillierte Informationen finden Sie in der AWS IAM-Dokumentation.

Andere Referenzen

Verwenden einer IAM-Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden

So funktioniert eine NetScaler VPX-Instanz auf AWS

October 17, 2024

Die NetScaler VPX-Instance ist als AMI im AWS-Marketplace verfügbar und kann als EC2-Instance innerhalb einer AWS-VPC gestartet werden. Die NetScaler VPX AMI-Instanz benötigt mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine EC2-Instanz, die in einer AWS VPC gestartet wird, kann auch die für die VPX-Konfiguration erforderlichen Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen. Jede VPX-Instanz benötigt mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Backend-Subnetz (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz in der AWS-Installation.

AWS stellt derzeit Multi-IP-Funktionen nur für Instanzen zur Verfügung, die in einer AWS VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastausgleich von Servern verwendet

werden, die in EC2-Instanzen ausgeführt werden. Mit einer Amazon VPC können Sie eine virtuelle Netzwerkumgebung erstellen und steuern, einschließlich Ihres eigenen IP-Adressbereichs, Subnetze, Routentabellen und Netzwerk-Gateways.

> **Hinweis:**
>
> Standardmäßig können Sie für jedes AWS-Konto bis zu 5 VPC-Instanzen pro AWS-Region erstellen. Sie können höhere VPC-Grenzwerte anfordern, indem Sie das Antragsformular von Amazon absendenhttp://aws.amazon.com/contact-us/vpc-request.

Abbildung 1. Ein Beispiel für die Bereitstellung einer NetScaler VPX-Instanz auf der AWS-Architektur

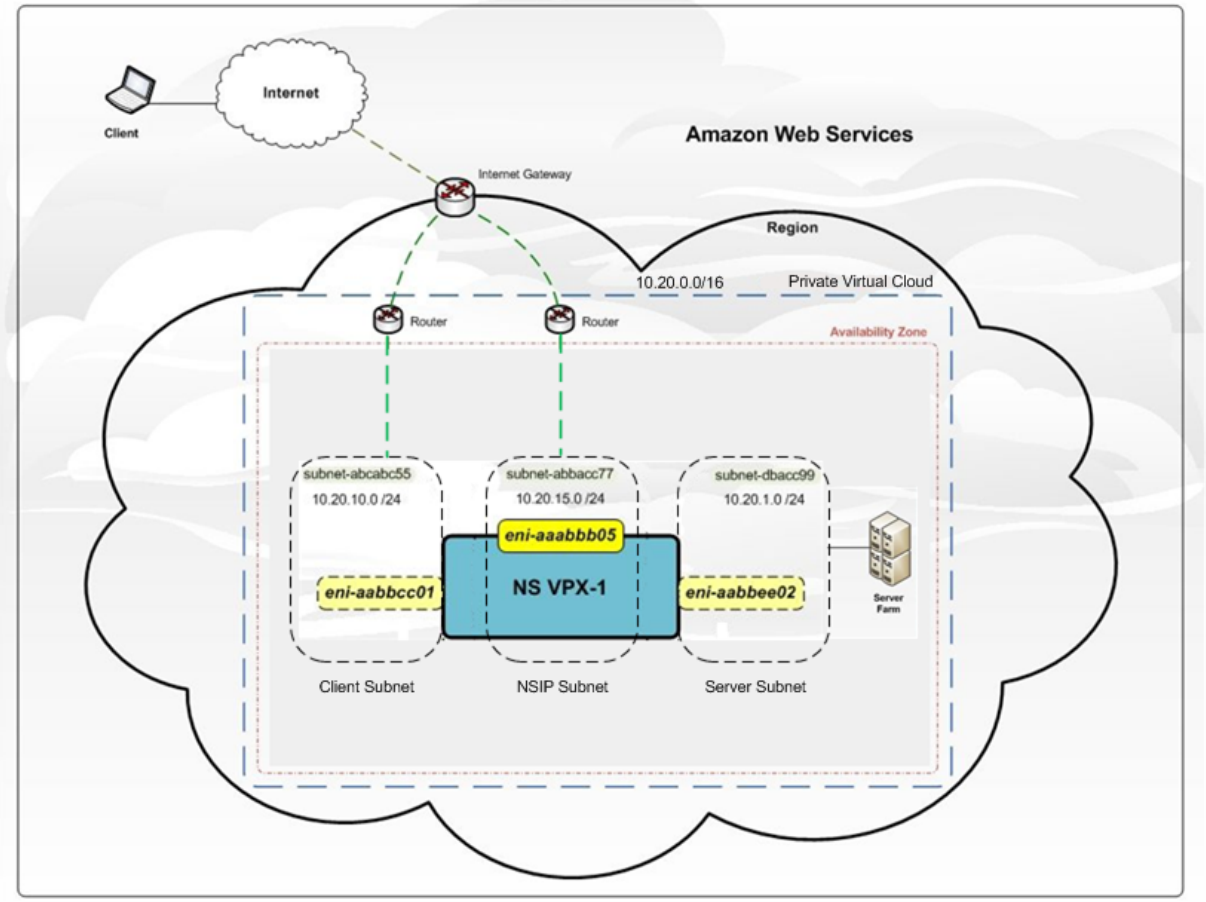


Abbildung 1 zeigt eine einfache Topologie einer AWS VPC mit einem NetScaler VPX-Bereitstellung. Die AWS VPC verfügt über:

1. Ein einzelnes Internet-Gateway zum Weiterleiten des Datenverkehrs in und aus der VPC.
2. Netzwerkverbindung zwischen dem Internet-Gateway und dem Internet.
3. Drei Subnetze, jeweils eines für Management, Client und Server.

4. Netzwerkverbindung zwischen dem Internet-Gateway und den beiden Subnetzen (Verwaltung und Client).
5. Eine eigenständige NetScaler VPX-Instanz, die innerhalb der VPC bereitgestellt wird. Die VPX-Instanz verfügt über drei ENIs, eine mit jedem Subnetz verbunden.

Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

October 17, 2024

Sie können eine eigenständige NetScaler VPX-Instance auf AWS bereitstellen, indem Sie die folgenden Optionen verwenden:

- AWS-Webkonsole
- Von Citrix verfasste CloudFormation-Vorlage
- AWS CLI

In diesem Thema wird das Verfahren zur Bereitstellung einer NetScaler VPX-Instance auf AWS beschrieben.

Lesen Sie die folgenden Themen, bevor Sie mit der Bereitstellung beginnen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Stellen Sie mithilfe der AWS-Webkonsole eine NetScaler VPX-Instance auf AWS bereit

Sie können eine NetScaler VPX-Instance auf AWS über die AWS-Webkonsole bereitstellen. Der Bereitstellungsprozess umfasst die folgenden Schritte:

1. Erstellen eines Schlüsselpaars
2. Erstellen einer Virtual Private Cloud (VPC)
3. Weitere Subnetze hinzufügen
4. Erstellen von Sicherheitsgruppen und Sicherheitsregeln
5. Routentabellen hinzufügen
6. Erstellen Sie ein Internet-Gateway
7. Erstellen Sie eine NetScaler VPX-Instanz
8. Weitere Netzwerkschnittstellen erstellen und anhängen
9. Elastische IPs an die Management-NIC anhängen
10. Herstellen einer Verbindung mit der VPX-Instanz

Schritt 1: Erstellen Sie ein Schlüsselpaar.

Amazon EC2 verwendet ein Schlüsselpaar, um Anmeldeinformationen zu verschlüsseln und zu entschlüsseln. Um sich bei Ihrer Instance anzumelden, müssen Sie ein Schlüsselpaar erstellen, den Namen des Schlüsselpaars angeben, wenn Sie die Instance starten, und den privaten Schlüssel angeben, wenn Sie eine Verbindung zur Instance herstellen.

Wenn Sie eine Instanz mit dem AWS Launch Instance Wizard überprüfen und starten, werden Sie aufgefordert, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar zu erstellen. Weitere Informationen zum Erstellen eines Schlüsselpaars finden Sie unter Amazon EC2-Schlüsselpaare.

Schritt 2: Erstellen einer VPC.

Eine NetScaler VPC-Instanz wird in einer AWS VPC bereitgestellt. Mit einer VPC können Sie das virtuelle Netzwerk definieren, das Ihrem AWS-Konto gewidmet ist. Weitere Informationen zu AWS VPC finden Sie unter Erste Schritte mit Amazon VPC.

Beachten Sie beim Erstellen einer VPC für Ihre NetScaler VPX-Instanz die folgenden Punkte:

- Verwenden Sie die Option VPC with a Single Public Subnet, um eine AWS-VPC in einer AWS-Availability Zone zu erstellen.
- Citrix empfiehlt, mindestens **drei Subnetze**der folgenden Typen zu erstellen:
  - Ein Subnetz für den Verwaltungsdatenverkehr. Sie platzieren die Management-IP (NSIP) in diesem Subnetz. Standardmäßig wird das Elastic Network Interface (ENI) eth0 für die Management-IP verwendet.
  - Ein oder mehrere Subnetze für den Clientzugriffsverkehr (User-to-NetScaler VPX), über die Clients eine Verbindung zu einer oder mehreren virtuellen IP (VIP) -Adressen herstellen, die den virtuellen Servern des NetScaler Load Balancing zugewiesen sind.
  - Ein oder mehrere Subnetze für den Serverzugriffsverkehr (VPX-to-Server), über den Ihre Server eine Verbindung zu VPX-eigenen Subnetz-IP-Adressen (SNIP) herstellen. Weitere Informationen zum NetScaler-Lastenausgleich und zu virtuellen Servern, virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) finden Sie unter:
  - Alle Subnetze müssen sich in derselben Availability Zone befinden.

Schritt 3: Fügen Sie Subnetzehinzu.

Als Sie den VPC-Assistenten verwendet haben, wurde nur ein Subnetz erstellt. Je nach Anforderung möchten Sie möglicherweise weitere Subnetze erstellen. Weitere Informationen zum Erstellen weiterer Subnetze finden Sie unter Hinzufügen eines Subnetzes zu Ihrer VPC.

Schritt 4: Erstellen von Sicherheitsgruppen und Sicherheitsregeln.

Um eingehenden und ausgehenden Datenverkehr zu steuern, erstellen Sie Sicherheitsgruppen und fügen Sie den Gruppen Regeln hinzu. Weitere Informationen zum Erstellen von Gruppen und zum Hinzufügen von Regeln finden Sie unter Sicherheitsgruppen für Ihre VPC.

Für NetScaler VPX -Instanzen stellt der EC2-Assistent Standardsicherheitsgruppen bereit, die von AWS Marketplace generiert werden und auf empfohlenen Einstellungen von Citrix basieren. Sie können jedoch je nach Ihren Anforderungen weitere Sicherheitsgruppen erstellen.

> **Hinweis:**
>
> Port 22, 80, 443, der in der Sicherheitsgruppe jeweils für den SSH-, HTTP- und HTTPS-Zugriff geöffnet wird.

Schritt 5: Fügen Sie Routentabellenhinzu.

Die Routentabelle enthält eine Reihe von Regeln, die als Routen bezeichnet werden und anhand derer bestimmt wird, wohin der Netzwerkverkehr geleitet wird. Jedes Subnetz in Ihrer VPC muss einer Routentabelle zugeordnet sein. Weitere Informationen zum Erstellen einer Routentabelle finden Sie unter Routentabellen.

Schritt 6: Erstellen Sie ein Internet-Gateway.

Ein Internet-Gateway dient zwei Zwecken: der Bereitstellung eines Ziels in Ihren VPC-Routing-Tabellen für internetfähigen Datenverkehr und der Durchführung von Netzwerkadressübersetzungen (NAT) für Instanzen, denen öffentliche IPv4-Adressen zugewiesen wurden.

Erstellen Sie ein Internet-Gateway für den Internetverkehr. Weitere Informationen zum Erstellen eines Internet-Gateways finden Sie im Abschnitt Anhängen eines Internet-Gateways.

Schritt 7: Erstellen Sie eine NetScaler VPX-Instanz mithilfe des AWS EC2-Dienstes.

Gehen Sie wie folgt vor, um mithilfe des AWS EC2-Service eine NetScaler VPX-Instance zu erstellen.

1. Gehen Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instance > AWS Marketplace**.

   Bevor Sie auf **Launch Instance**klicken, stellen Sie sicher, dass Ihre Region korrekt ist, indem Sie den Hinweis überprüfen, der unter **Launch Instance**erscheint.

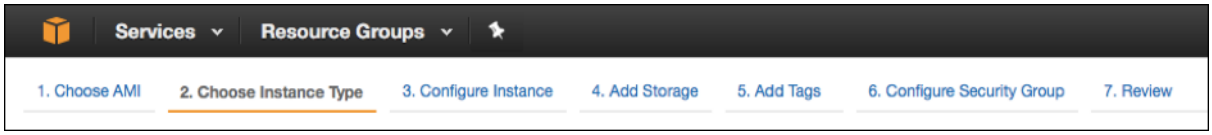
2. Suchen Sie in der Leiste Search AWS Marketplace nach dem Schlüsselwort NetScaler VPX.
3. Wählen Sie die Version aus, die Sie bereitstellen möchten, und klicken Sie dann auf **Auswählen**. Für die NetScaler VPX-Version haben Sie folgende Optionen:

   - Eine lizenzierte Version

- NetScaler VPX Express Appliance (Dies ist eine kostenlose virtuelle Appliance, die ab NetScaler 12.0 56.20 verfügbar ist.)
- Bringen Sie Ihr eigenes Gerät

Der Assistent Instance starten wird gestartet. Folgen Sie dem Assistenten, um eine Instanz zu erstellen. Der Assistent fordert Sie auf:

- Instanztyp auswählen
- Instanz konfigurieren
- Speicher hinzufügen
- Tags hinzufügen
- Sicherheitsgruppe konfigurieren
- Bewertung



Schritt 8: Weitere Netzwerkschnittstellen erstellen und anhängen.

Erstellen Sie zwei weitere Netzwerkschnittstellen für VIP und SNIP. Weitere Informationen zum Erstellen weiterer Netzwerkschnittstellen finden Sie im Abschnitt Erstellen einer Netzwerkschnittstelle .

Nachdem Sie die Netzwerkschnittstellen erstellt haben, müssen Sie sie an die VPX-Instanz anhängen. Fahren Sie vor dem Anfügen der Schnittstelle die VPX-Instanz herunter, schließen Sie die Schnittstelle an und schalten Sie die Instanz ein. Weitere Informationen zum Anhängen von Netzwerkschnittstellen finden Sie im Abschnitt Anhängen einer Netzwerkschnittstelle beim Starten einer Instanz .

Schritt 9: Zuweisen und Zuordnen von elastischen IPs.

Wenn Sie einer EC2-Instance eine öffentliche IP-Adresse zuweisen, bleibt diese nur so lange zugewiesen, bis die Instance gestoppt wird. Danach wird die Adresse wieder in den Pool freigegeben. Wenn Sie die Instance neu starten, wird eine neue öffentliche IP-Adresse zugewiesen.

Im Gegensatz dazu bleibt eine elastische IP-Adresse (EIP) zugewiesen, bis die Adresse von einer Instanz getrennt wird.

Weisen Sie eine elastische IP für die Management-NIC zu und ordnen Sie sie zu. Weitere Informationen zur Zuweisung und Zuordnung von elastischen IP-Adressen finden Sie in den folgenden Themen:

- Zuweisen einer elastischen IP-Adresse
- Eine Elastic IP-Adresse mit einer laufenden Instance verknüpfen

Diese Schritte vervollständigen das Verfahren zur Erstellung einer NetScaler VPX-Instance auf AWS. Es kann einige Minuten dauern, bis die Instanz fertig ist. Vergewissern Sie sich, dass Ihre Instance ihre

Statusprüfungen bestanden hat. Sie können diese Informationen in der Spalte **Status Checks** auf der Seite Instances einsehen.

Schritt 10: Stellen Sie eine Verbindung zur VPX-Instanzher.

Nachdem Sie die VPX-Instanz erstellt haben, verbinden Sie die Instanz mithilfe der GUI und eines SSH-Clients.

- Grafische Benutzeroberfläche (GUI)

Im Folgenden finden Sie die standardmäßigen Administratoranmeldeinformationen für den Zugriff auf eine NetScaler VPX-Instanz.

Benutzername: `nsroot`

Passwort: Das Standardkennwort für das ns-Root-Konto ist auf die AWS-Instance-ID der NetScaler VPX-Instance festgelegt. Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Kennwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Passwort erneut, wenn Sie dazu aufgefordert werden.

- SSH-Client

Wählen Sie in der AWS-Managementkonsole die NetScaler VPX-Instance aus und klicken Sie auf Verbinden. Folgen Sie den Anweisungen auf der Seite **Mit Ihrer Instance verbinden** . Folgen Sie den Anweisungen auf der Seite Mit **Ihrer Instanz verbinden**.

Weitere Informationen zum Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole finden Sie unter Szenario: eigenständige Instanz

Konfigurieren Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage

Sie können die von Citrix bereitgestellte CloudFormation-Vorlage verwenden, um den Start der VPX-Instance zu automatisieren. Die Vorlage bietet Funktionen zum Starten einer einzelnen NetScaler VPX-Instance oder zum Erstellen einer Hochverfügbarkeitsumgebung mit zwei NetScaler VPX-Instances.

Sie können die Vorlage über AWS Marketplace oder GitHub starten.

Die CloudFormation-Vorlage erfordert eine bestehende VPC-Umgebung und startet eine VPX-Instance mit drei elastischen Netzwerkschnittstellen (ENIs). Bevor Sie mit der CloudFormation-Vorlage beginnen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine virtuelle Private Cloud (VPC) von AWS

- Drei Subnetze innerhalb der VPC: eines für die Verwaltung, eines für den Client-Verkehr und eines für Back-End-Server
- Ein EC2-Schlüsselpaar, um den SSH-Zugriff auf die Instance zu ermöglichen
- Eine Sicherheitsgruppe mit UDP 3003, TCP 3009—3010, HTTP, SSH-Ports geöffnet

Weitere Informationen zum Vervollständigen der Voraussetzungen finden Sie im Abschnitt Bereitstellen einer NetScaler VPX-Instanz auf AWS mit der AWS Web Console oder in der AWS-Dokumentation.

In diesem Video erfahren Sie, wie Sie eine eigenständige NetScaler VPX-Instanz mithilfe der im AWS Marketplace verfügbaren Citrix CloudFormation-Vorlage konfigurieren und starten können.

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Eine IAM-Rolle ist für eine eigenständige Bereitstellung nicht zwingend erforderlich. Citrix empfiehlt jedoch, dass Sie eine IAM-Rolle mit den erforderlichen Rechten erstellen und der Instanz zuordnen, um sie in Zukunft benötigen zu können. Die IAM-Rolle stellt sicher, dass die eigenständige Instanz bei Bedarf problemlos mit SR-IOV in einen Hochverfügbarkeitsknoten konvertiert wird.

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Konfigurieren von NetScaler VPX-Instanzen zur Verwendung der SR-IOV-Netzwerkschnittstelle.

> **Hinweis:**
>
> Wenn Sie eine NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert. Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, lautet die Standardoption „Ja“. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie „Nein“. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instanzen mit Amazon CloudWatch

Konfigurieren einer NetScaler VPX-Instanz mithilfe der AWS CLI

Sie können die AWS CLI zum Starten von Instanzen verwenden. Weitere Informationen finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle.

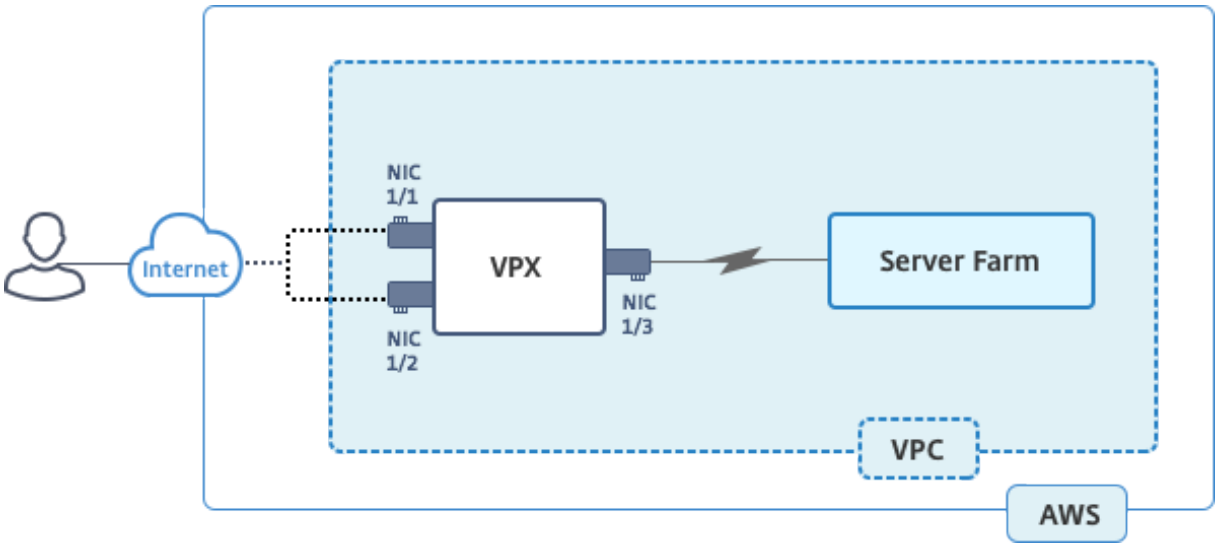
Szenario: Standalone-Instanz

October 17, 2024

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-EC2-Instance in AWS mithilfe der AWS-GUI bereitgestellt wird. Erstellen Sie eine eigenständige VPX-Instanz mit drei Netzwerkkarten. Die Instanz, die als virtueller Lastausgleichsserver konfiguriert ist, kommuniziert mit Backend-Servern

(der Serverfarm). Richten Sie für diese Konfiguration die erforderlichen Kommunikationswege zwischen der Instanz und den Back-End-Servern sowie zwischen der Instanz und den externen Hosts im öffentlichen Internet ein.

Weitere Einzelheiten zum Verfahren zum Bereitstellen einer VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS.



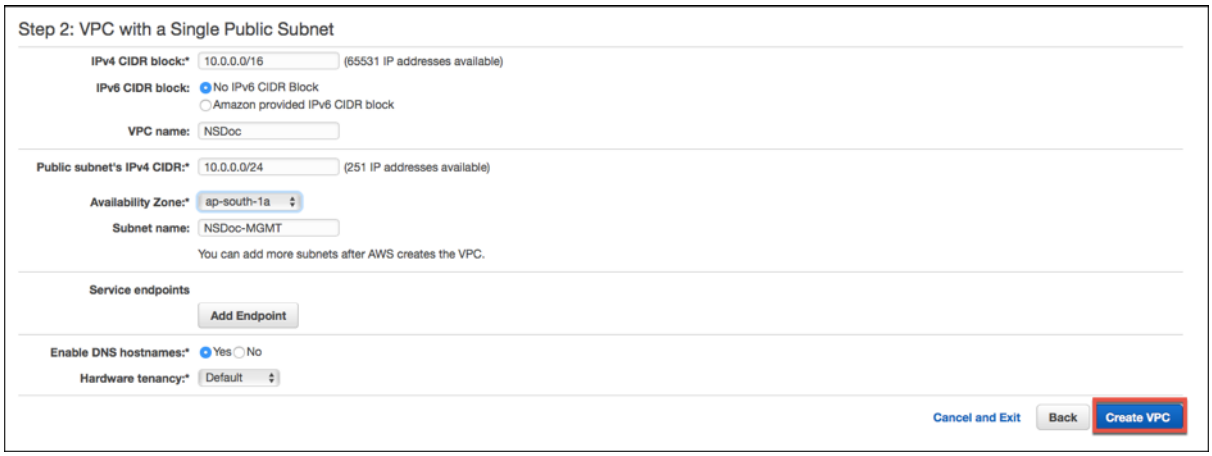
Erstellen Sie drei Netzwerkkarten. Jede Netzwerkkarte kann mit einem Paar von IP-Adressen (öffentlich und privat) konfiguriert werden. Die NICs dienen den folgenden Zwecken.

Netzwerkkarte	Zweck	Verbunden mit
eth0	Bedienen des Management-Datenverkehrs (NSIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth1	Dient clientseitigem Datenverkehr (VIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth2	Kommuniziert mit Back-End-Servern (SNIP)	Eine öffentliche IP-Adresse (Private IP-Adresse ist nicht zwingend erforderlich)

Schritt 1: Erstellen einer VPC.

1. Melden Sie sich bei der AWS-Webkonsole an, und navigieren Sie zu **Netzwerk- und Inhaltsbereitstellung** > **VPC**. Klicken Sie auf **VPC-Assistenten starten**.
2. Wählen Sie **VPC mit einem einzelnen öffentlichen Subnetz** aus, und klicken Sie auf **Auswählen**.
3. Legen Sie für dieses Szenario den IP-CIDR-Block auf 10.0.0.0/16 fest.

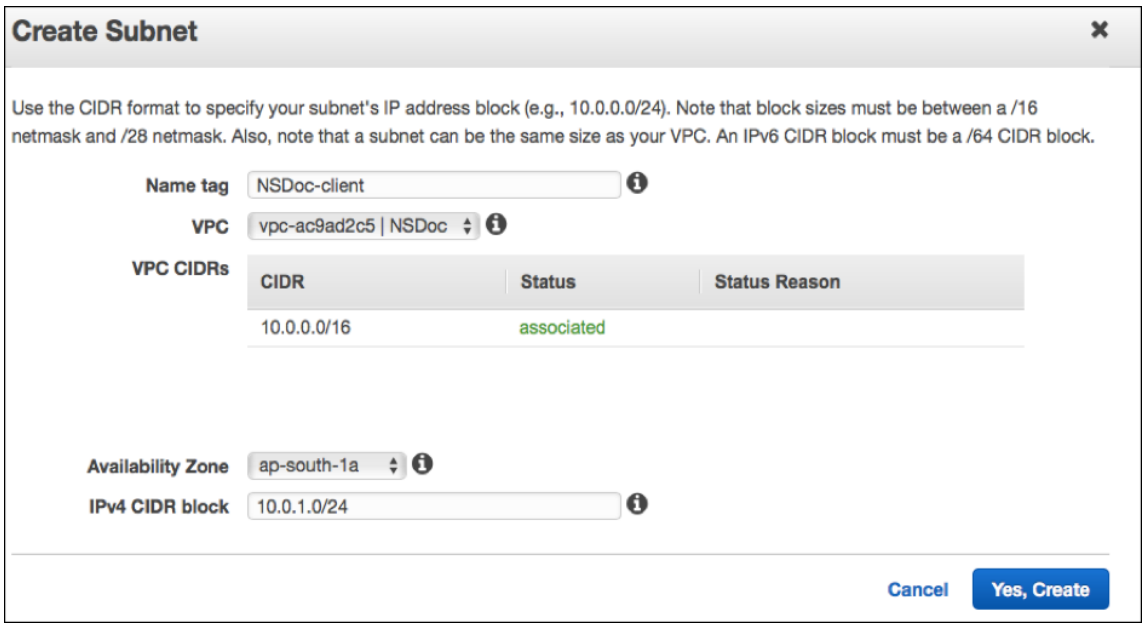
4. Geben Sie einen Namen für die VPC an.
5. Stellen Sie das öffentliche Subnetz auf 10.0.0.0/24. (Dies ist das Verwaltungsnetzwerk).
6. Wählen Sie eine Verfügbarkeitszone aus.
7. Geben Sie einen Namen für das Subnetz an.
8. Klicken Sie auf **VPC**erstellen.



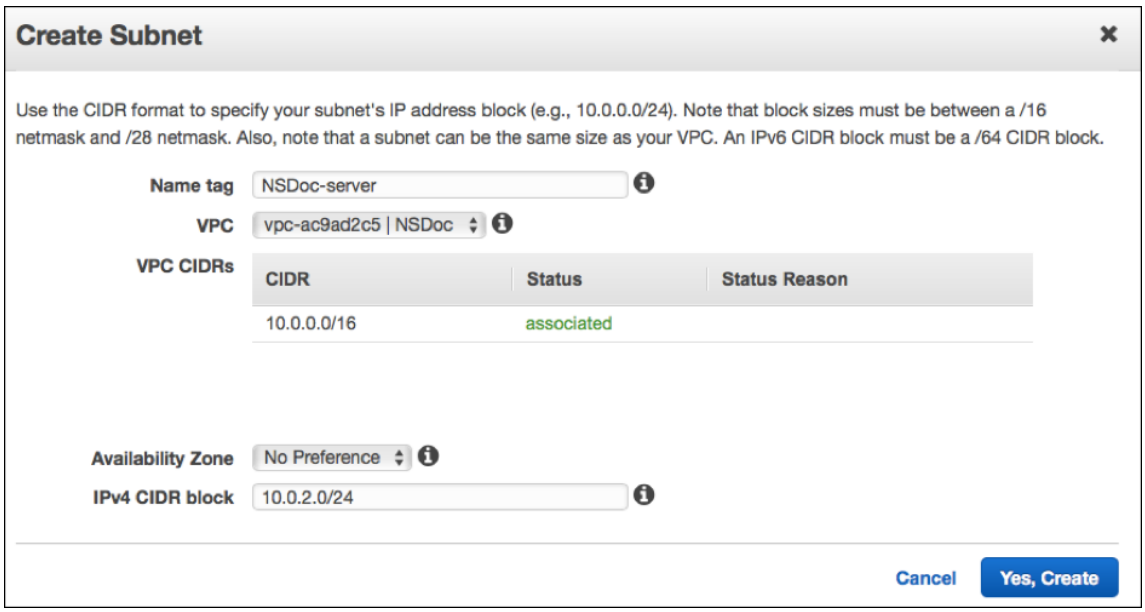
Schritt 2: Erstellen Sie zusätzliche Subnetze.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets, Subnet erstellen, nachdem Sie die folgenden Details eingegeben haben.

   - Namensschild: Geben Sie einen Namen für Ihr Subnetz an.
   - VPC: Wählen Sie die VPC aus, für die Sie das Subnetz erstellen.
   - Availability Zone: Wählen Sie die Availability Zone, in der Sie die VPC in Schritt 1 erstellt haben.
   - IPv4-CIDR-Block: Geben Sie einen IPv4-CIDR-Block für Ihr Subnetz an. Wählen Sie für dieses Szenario 10.0.1.0/24.

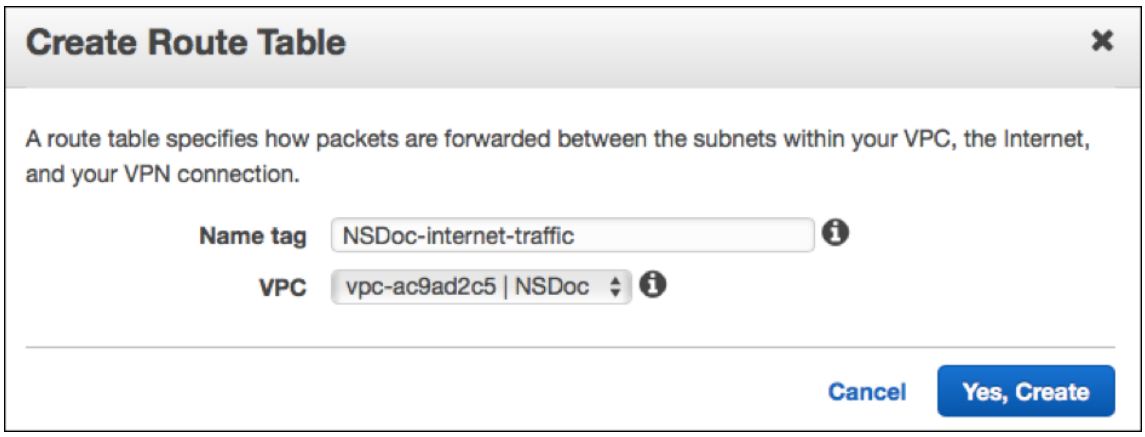


3. Wiederholen Sie die Schritte, um ein weiteres Subnetz für Back-End-Server zu erstellen.



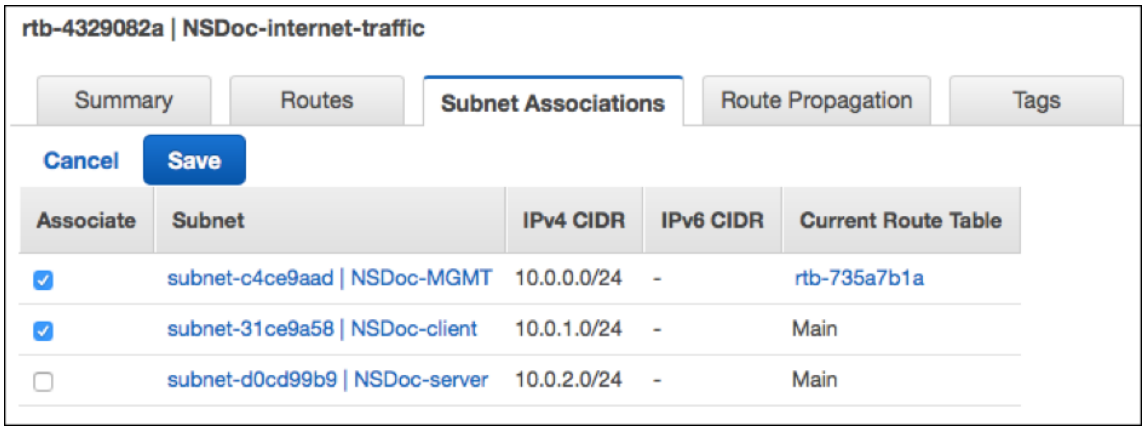
Schritt 3: Erstellen Sie eine Routentabelle.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich **Routentabellen** > **Routentabelle erstellen**.
3. Fügen Sie im Fenster Routentabelle erstellen einen Namen hinzu, und wählen Sie die VPC aus, die Sie in Schritt 1 erstellt haben.
4. Klicken Sie auf **Yes, Create**.

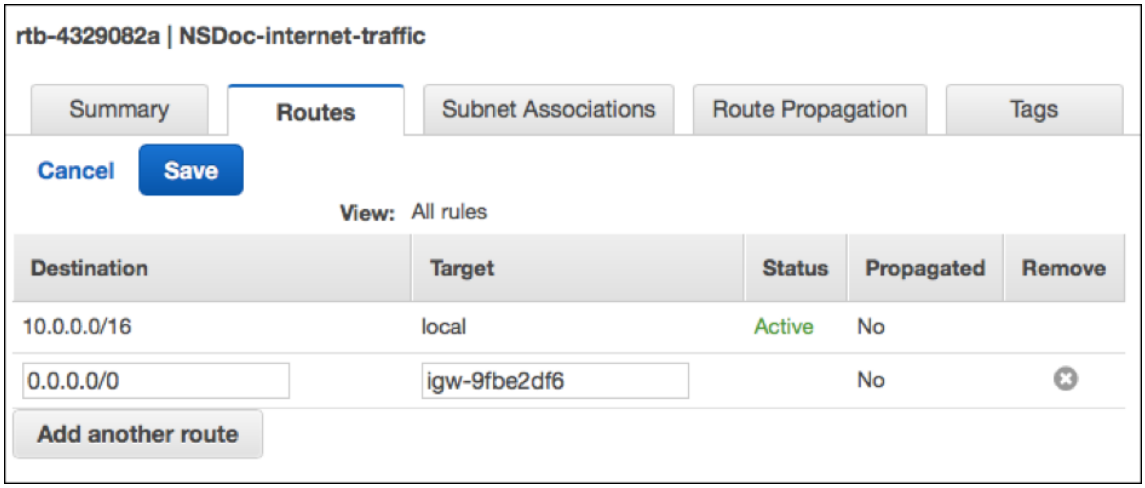


Die Routing-Tabelle wird allen Subnetzen zugewiesen, die Sie für diese VPC erstellt haben, so dass das Routing von Datenverkehr von einer Instanz in einem Subnetz eine Instanz in einem anderen Subnetz erreichen kann.

5. Klicken Sie auf **Subnetzzuordnungen**und dann auf **Bearbeiten**.
6. Klicken Sie auf das Verwaltungs- und Client-Subnetz, und klicken Sie auf Speichern. Dadurch wird eine Routentabelle nur für den Internetverkehr erstellt.



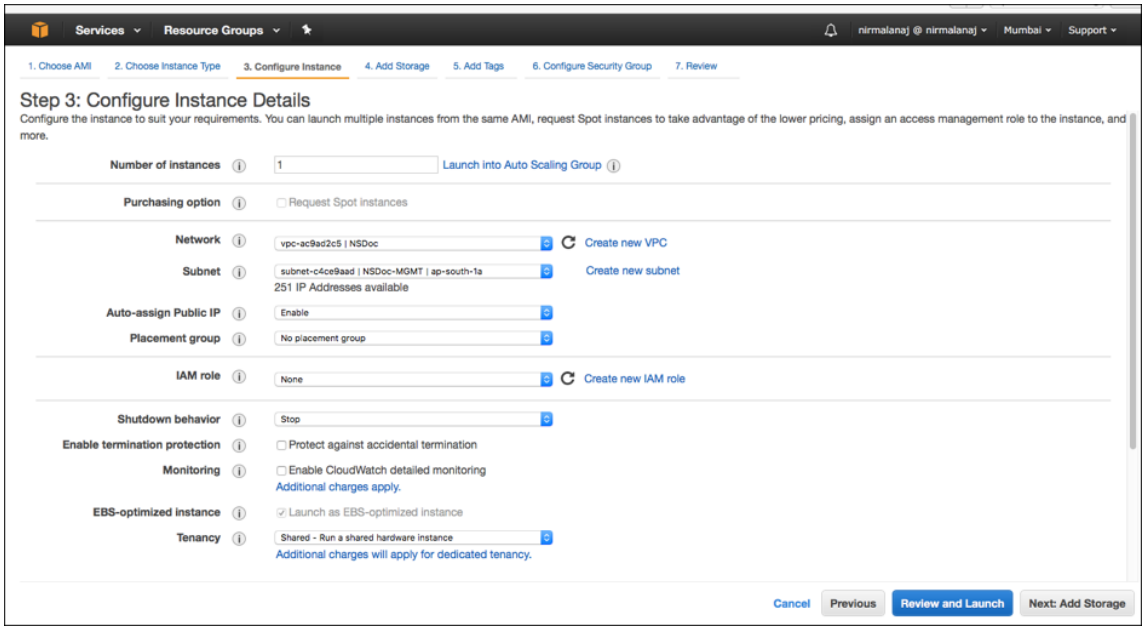
7. Klicken Sie auf **Routen > Bearbeiten > Weitere Route hinzufügen**.
8. Fügen Sie im Feld Ziel 0.0.0.0/0 hinzu, und klicken Sie auf das Feld Ziel, um igw- <xxxx> das Internet Gateway auszuwählen, das der VPC-Assistent automatisch erstellt hat.
9. Klicken Sie auf **Speichern**.



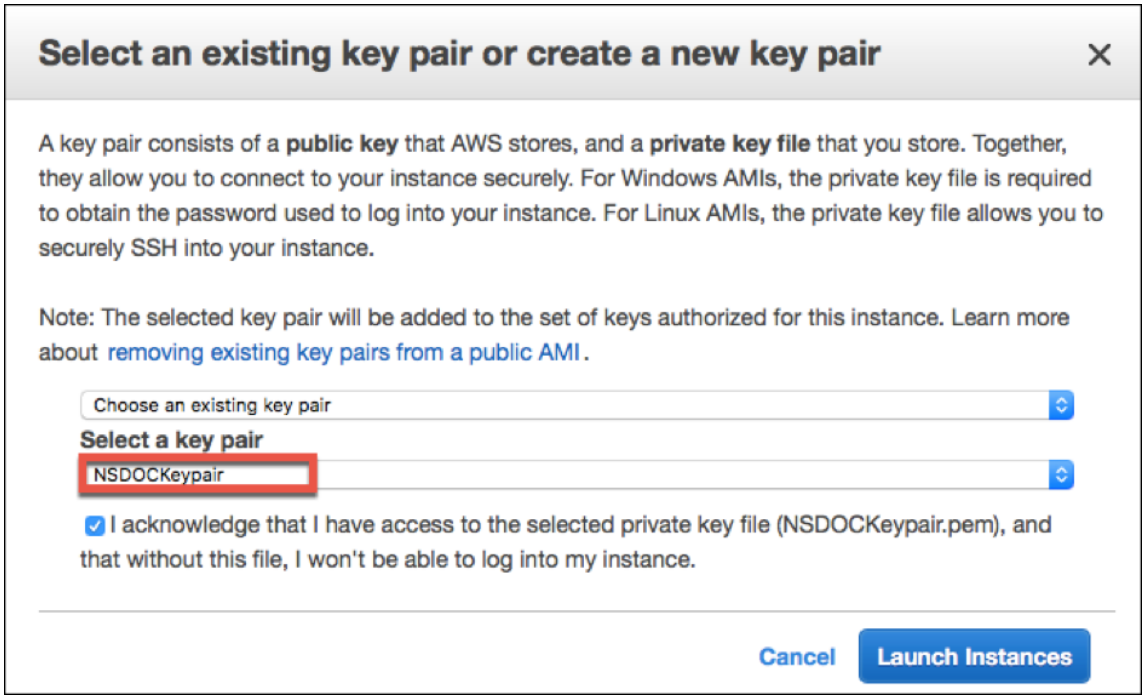
10. Führen Sie die Schritte aus, um eine Routentabelle für serverseitigen Datenverkehr zu erstellen.

Schritt 4: Erstellen Sie eine NetScaler VPX-Instanz.

1. Melden Sie sich an der AWS Management Console an, und klicken Sie unter **Compute** auf **EC2** .
2. Klicken Sie auf AWS Marketplace. Geben Sie in der Suchleiste von AWS Marketplace NetScaler VPX ein und drücken Sie die Eingabetaste. Die verfügbaren NetScaler VPX-Editionen werden angezeigt.
3. Klicken Sie auf **Auswählen**, um die gewünschte NetScaler VPX-Edition auszuwählen. Der EC2-Instanz-Assistent wird gestartet.
4. Wählen Sie auf der Seite **Instanztyp auswählen** die Option **m4. Xlarge** (empfohlen) und klicken Sie auf **Weiter: Instanzdetails konfigurieren**.
5. Wählen Sie auf der Seite „Instanzdetails konfigurieren“Folgendes aus und klicken Sie dann auf **Weiter: Speicher hinzufügen**.
    - Anzahl der Instanzen: 1
    - Netzwerk: die VPC, die in Schritt 1 erstellt wurde
    - Subnetz: das Management-Subnetz
    - Öffentliche IP automatisch zuweisen: Aktivieren



6. Wählen Sie auf der Seite „Speicher hinzufügen“die Standardoption und klicken Sie auf **Weiter: Tags hinzufügen**.
7. Geben Sie auf der Seite „Tags hinzufügen“einen Namen für die Instanz ein und klicken Sie auf **Weiter: Sicherheitsgruppe konfigurieren**.
8. Wählen Sie auf der Seite Configure Security Group die Standardoption (die von AWS Marketplace generiert wird und auf den empfohlenen Einstellungen von Citrix Systems basiert) und klicken Sie dann auf **Review and Launch > Launch**.
9. Sie werden aufgefordert, ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen. Wählen Sie in der Dropdownliste Schlüsselpaar auswählen das Schlüsselpaar aus, das Sie als Voraussetzung erstellt haben (siehe Abschnitt Voraussetzung).
10. Aktivieren Sie das Kontrollkästchen, um das Schlüsselpaar zu bestätigen, und klicken Sie auf **Instanzen starten**.



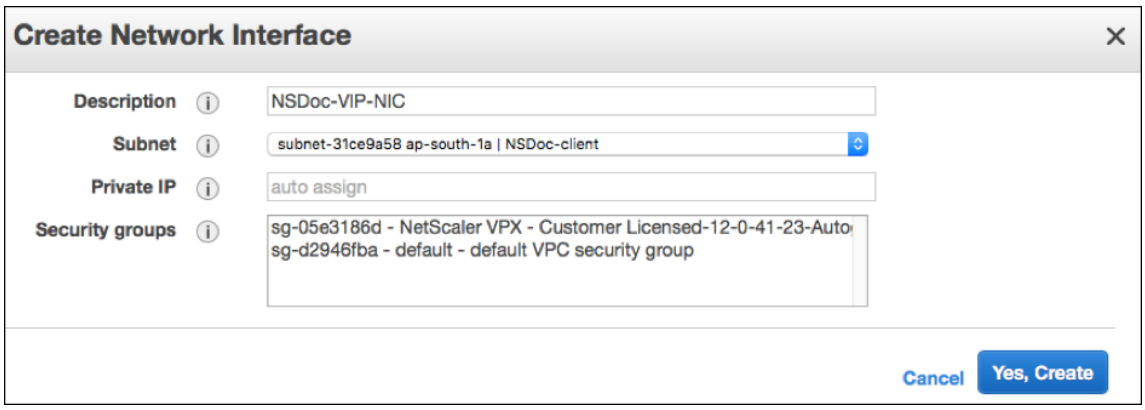
Der Assistent zum Starten von Instanz zeigt den Startstatus an, und die Instanz wird in der Liste der Instanzen angezeigt, wenn sie vollständig gestartet wurde.

Um die Instanz zu überprüfen, gehen Sie zur AWS-Konsole und klicken Sie auf **EC2 > Running Instances**. Wählen Sie die Instanz aus, und fügen Sie einen Namen hinzu. Stellen Sie sicher, dass der Instanzentatus ausgeführt wird und die Statusüberprüfungen abgeschlossen sind.

Schritt 5: Erstellen und Anfügen weiterer Netzwerkschnittstellen.

Wenn Sie die VPC erstellt haben, ist nur eine Netzwerkschnittstelle zugeordnet. Fügen Sie nun der VPC zwei weitere Netzwerkschnittstellen für VIP und SNIP hinzu.

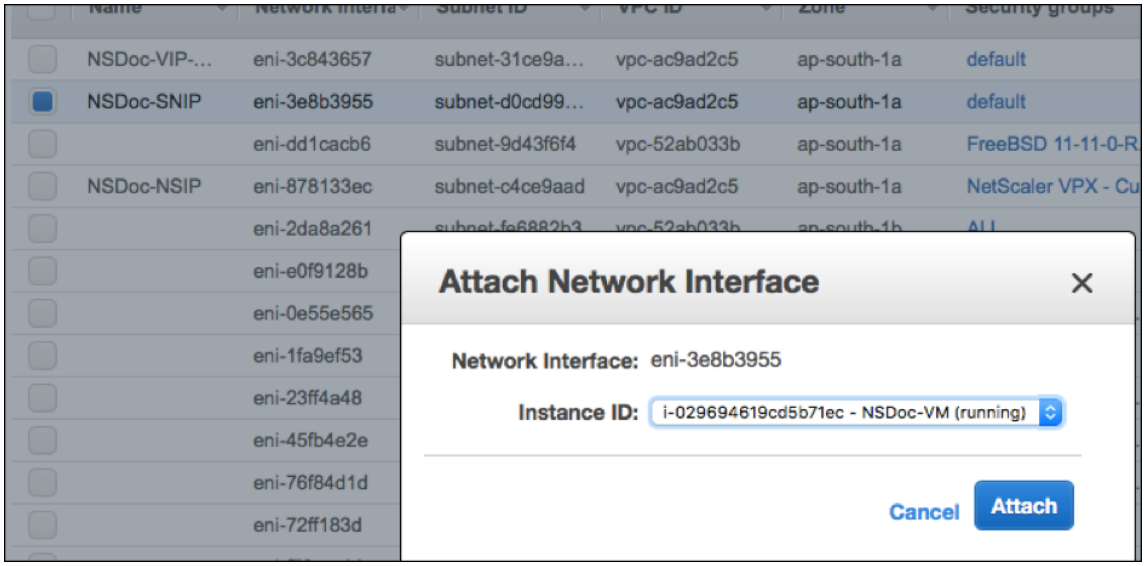
1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfacesaus.
3. Wählen Sie Netzwerkschnittstelle erstellen.
4. Geben Sie für **Beschreibung**einen beschreibenden Namen ein.
5. Wählen Sie für **Subnetz**das Subnetz aus, das Sie zuvor für die VIP erstellt haben.
6. Belassen Sie für **Private IP**die Standardoption.
7. Wählen Sie für **Sicherheitsgruppen**die Gruppe aus.
8. Klicken Sie auf **Yes, Create**.



9. Nachdem die Netzwerkschnittstelle erstellt wurde, fügen Sie der Schnittstelle einen Namen hinzu.
10. Wiederholen Sie die Schritte, um eine Netzwerkschnittstelle für serverseitigen Datenverkehr zu erstellen.

Schließen Sie die Netzwerkschnittstellenan:

1. Wählen Sie im Navigationsbereich Network Interfacesaus.
2. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Anhängen**.
3. Wählen Sie im Dialogfeld „Netzwerkschnittstelle anhängen“die Instanz aus und klicken Sie auf **Anhängen**.



Schritt 6: Bringen Sie eine elastische IP an das NSIP an.

1. Wechseln Sie in der AWS-Verwaltungskonsole zu **NETWORK & SECURITY > Elastic IPs**.
2. Überprüfen Sie, ob verfügbare kostenlose EIP beigefügt werden kann. Wenn keine, klicken Sie auf **Neue Adresse zuweisen**.

3. Wählen Sie die neu zugewiesene IP-Adresse aus und wählen Sie **Aktionen > Adresse zuordnen**.
4. Klicken Sie auf das Optionsfeld **Netzwerkschnittstelle**.
5. Wählen Sie in der Dropdownliste Netzwerkschnittstelle die Verwaltungs-NIC aus.
6. Wählen Sie im Dropdownmenü **Private IP** die von AWS generierte IP-Adresse aus.
7. Aktivieren Sie das Kontrollkästchen **Neuzuordnen**.
8. Klicken Sie auf **Zuordnen**.

Zugriff auf die VPX-Instanz:

Nachdem Sie eine eigenständige NetScaler VPX-Instanz mit drei NICs konfiguriert haben, melden Sie sich bei der VPX-Instanz an, um die NetScaler-seitige Konfiguration abzuschließen. Verwendung der folgenden Optionen:

- GUI: Geben Sie die öffentliche IP der Management-NIC im Browser ein. Melden Sie sich an, indem Sie `nsroot` als Benutzernamen und die Instanz-ID (i-0c1ffe1d987817522) als Kennwort verwenden.

> **Hinweis:**
>
> Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Kennwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Kennwort erneut an der Eingabeaufforderung und speichern Sie die Konfiguration.

- SSH: Öffnen Sie einen SSH-Client und geben Sie ein:

```
ssh -i \\&#060;location of your private key\\&#062; ns root@\\&#060;
public DNS of the instance\\&#062;
```

Um den öffentlichen DNS zu finden, klicken Sie auf die Instanz und dann auf **Verbinden**.

Weitere Informationen:

- Informationen zum Konfigurieren der IP-Adressen im Besitz von NetScaler (NSIP, VIP und SNIP) finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.
- Sie haben eine BYOL-Version der NetScaler VPX Appliance konfiguriert. Weitere Informationen finden Sie im VPX-Lizenzierungshandbuch unterhttp://support.citrix.com/article/CTX122426

Download einer NetScaler VPX-Lizenz

October 17, 2024

Nach dem Start der NetScaler VPX-kundenlizenzierten Instanz vom AWS-Marktplatz ist eine Lizenz erforderlich. Weitere Informationen zur VPX-Lizenzierung finden Sie unter Übersicht über die Lizenzierung.

Sie müssen:

1. Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Wenn Sie eine NetScaler VPX-Instanz mit einer Modellnummer über VPX 5000 verwenden, ist der Netzwerkdurchsatz möglicherweise nicht der gleiche wie in der Lizenz der Instanz angegeben. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde können jedoch verbessert werden.

Im `c4.8xlarge` Instanztyp wird eine 5-Gbit/s-Netzwerkbandbreite beobachtet.

So migrieren Sie das AWS-Abonnement auf BYOL

In diesem Abschnitt wird das Verfahren zur Migration vom AWS-Abonnement auf Bring your own License (BYOL) beschrieben, und umgekehrt.

Führen Sie die folgenden Schritte aus, um ein AWS-Abonnement auf BYOL zu migrieren:

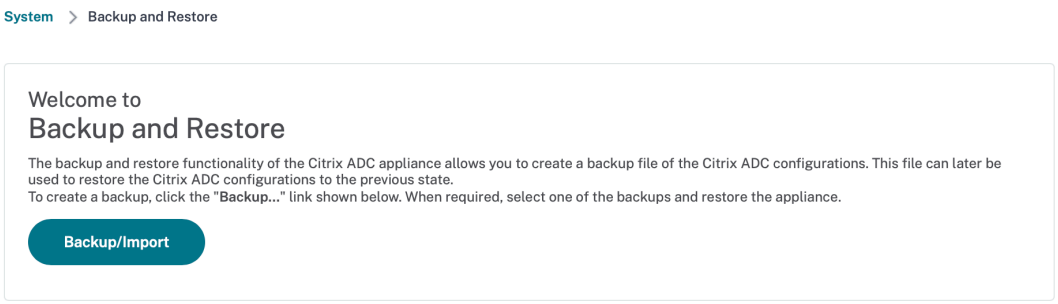
> **Hinweis:**
>
> Der **Schritt 2** und der **Schritt 3** werden auf der NetScaler VPX-Instanz ausgeführt, und alle anderen Schritte werden im AWS-Portal ausgeführt.

1. Erstellen Sie eine BYOL EC2-Instanz mit NetScaler VPX - Kundenlizenziert in derselben Availability Zone wie die alte EC2-Instanz, die dieselbe Sicherheitsgruppe, IAM-Rolle und das gleiche Subnetz hat. Die neue EC2-Instanz muss nur eine ENI-Schnittstelle haben.

2. Gehen Sie folgendermaßen vor, um die Daten auf der alten EC2-Instanz mit der NetScaler GUI zu sichern.

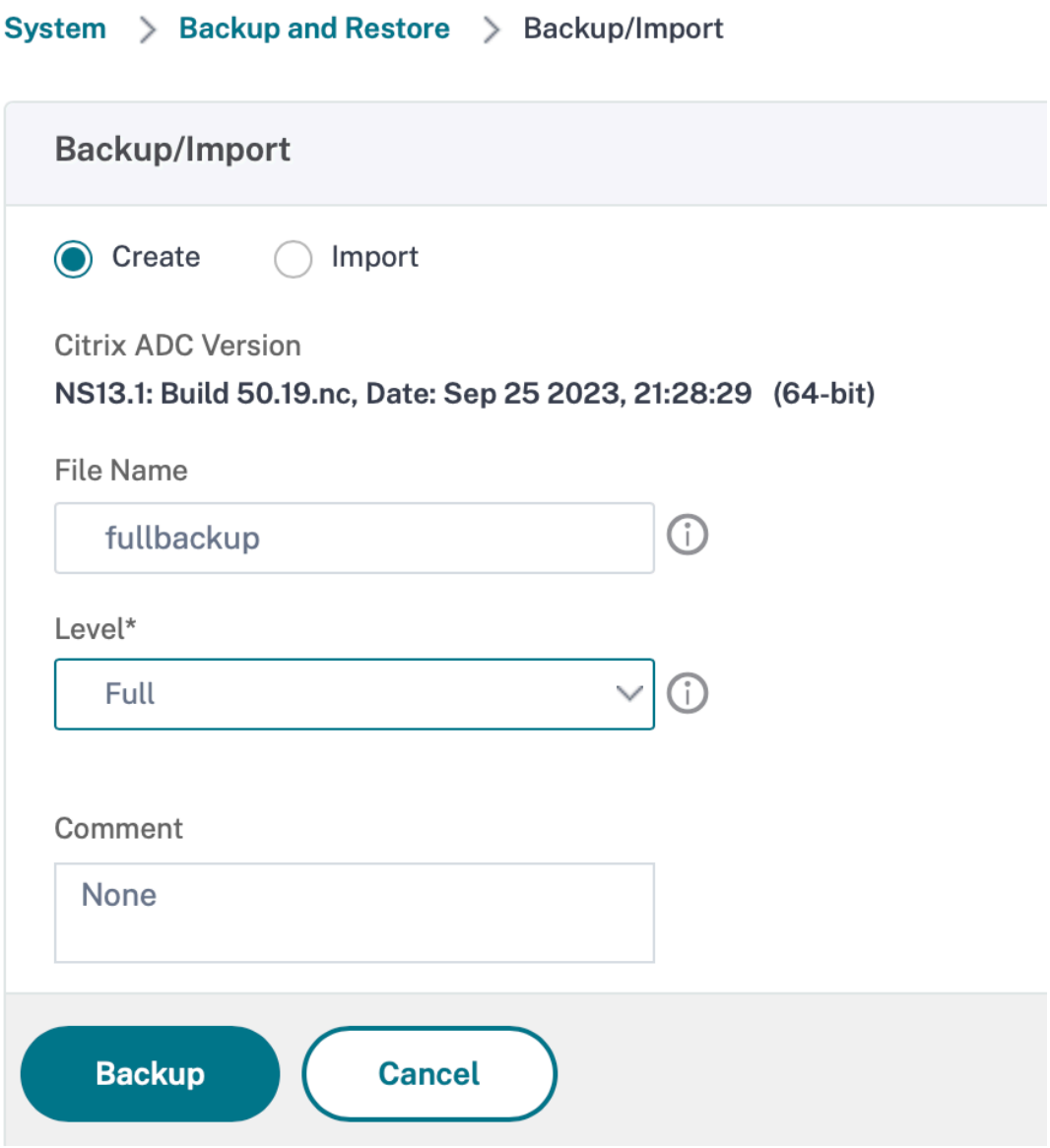
   a) Navigieren Sie zu **System > Backup und Wiederherstellen**.

   b) Klicken Sie auf der **Begrüßungsseite** auf **Backup/Importieren**, um den Vorgang zu starten.

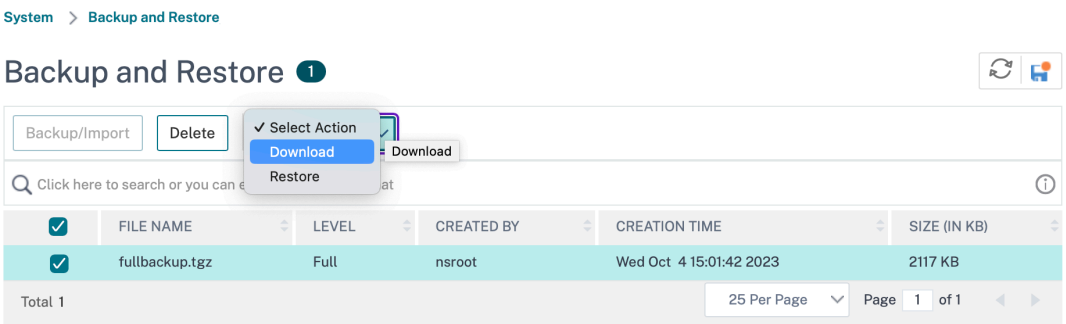


   c) Geben Sie auf der Seite **“Backup/Import** “die folgenden Details ein:

   - **Name** —Name der Sicherungsdatei.
   - **Level** —Wählen Sie die Backup-Level als **Full**aus.
   - **Kommentar** —Geben Sie eine kurze Beschreibung des Backup an.



d) Klicken Sie auf **Backup**. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf Ihren lokalen Computer herunterladen.



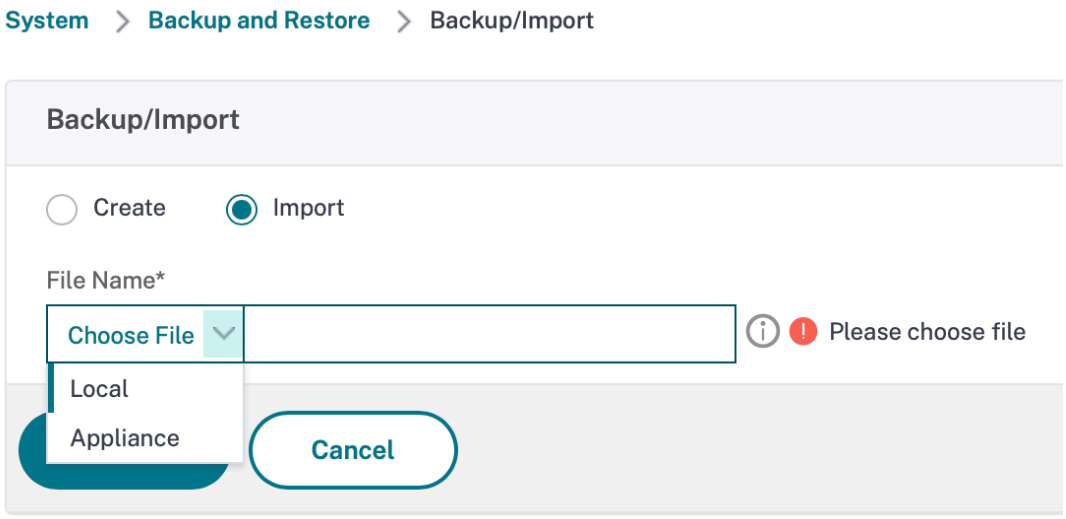
3. Gehen Sie folgendermaßen vor, um die Daten auf der neuen EC2-Instanz mit der NetScaler GUI

wiederherzustellen:

a) Navigieren Sie zu **System > Backup und Wiederherstellen**.

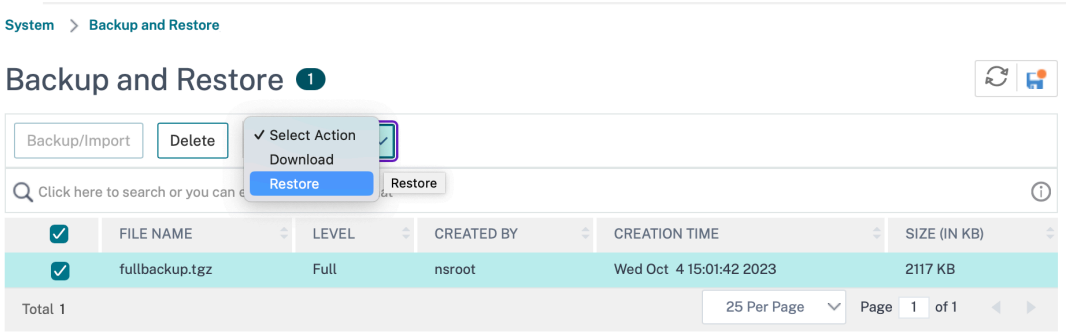
b) Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.

c) Wählen Sie die Option **Importieren** aus und laden Sie die Sicherungsdatei hoch.

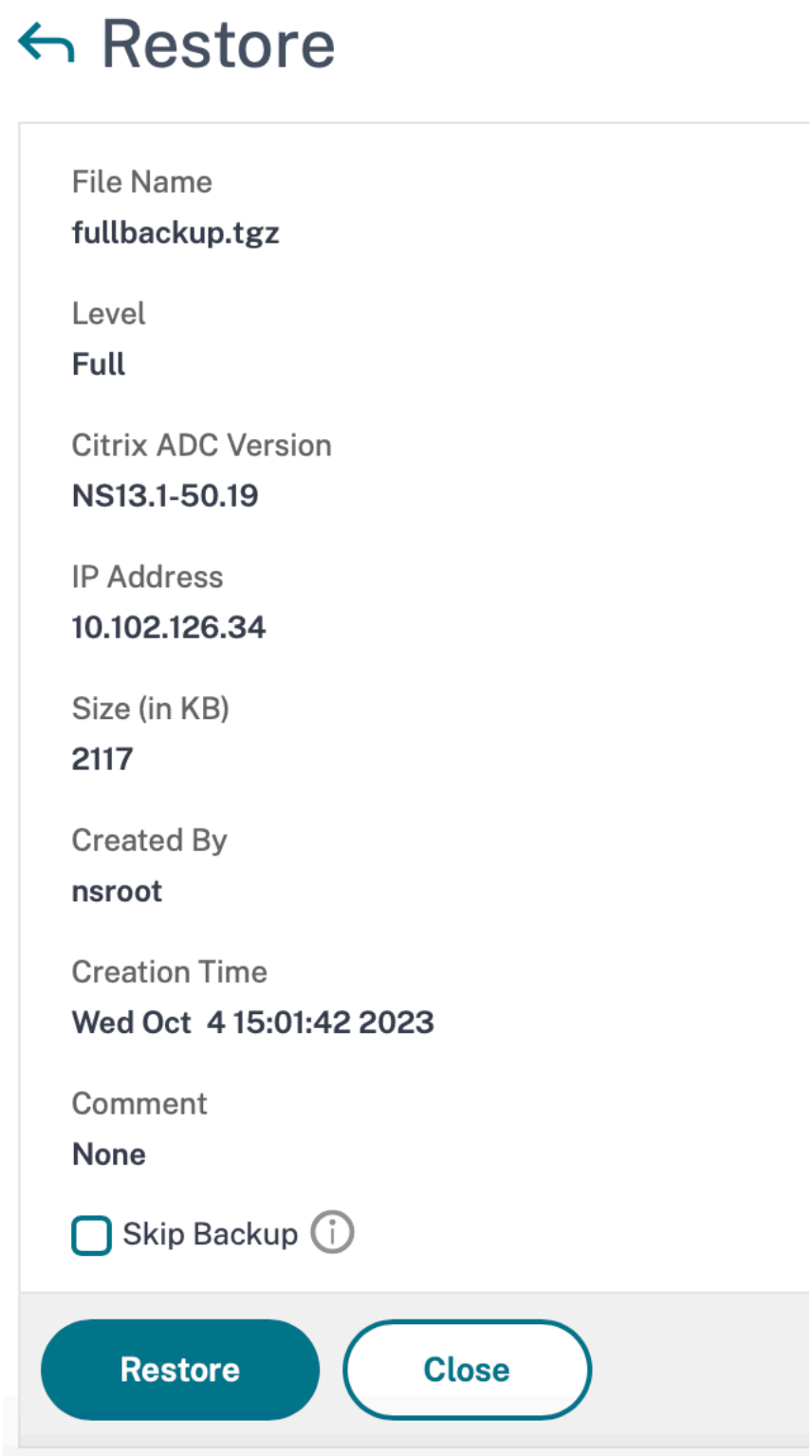


d) Wählen Sie die Datei aus.

e) **Wählen Sie im Dropdownmenü Aktion** auswählen die Option **Wiederherstellen**aus.



f) Überprüfen Sie auf der Seite **Wiederherstellen** die Dateidetails und klicken Sie auf **Wiederherstellen**.



g) Starten Sie nach der Wiederherstellung die EC2-Instanz neu.

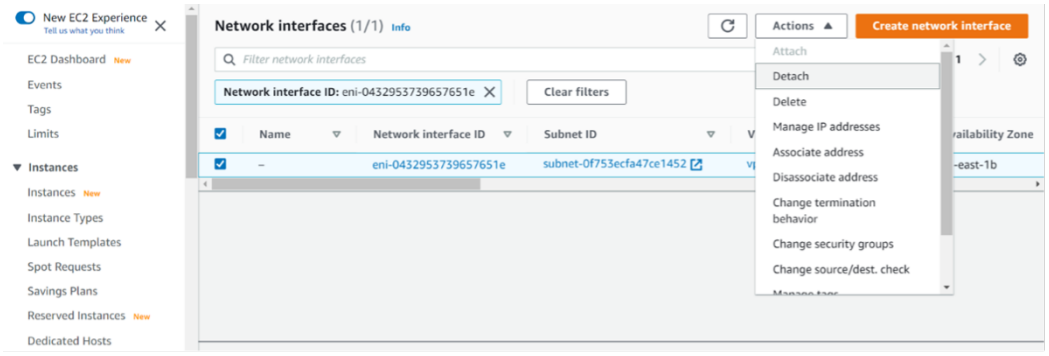
4. Verschieben Sie alle Schnittstellen (mit Ausnahme der Verwaltungsschnittstelle, an die die NSIP-

Adresse gebunden ist) von der alten EC2-Instanz zur neuen EC2-Instanz. Gehen Sie folgendermaßen vor, um eine Netzwerkschnittstelle von einer EC2-Instanz in eine andere zu verschieben:

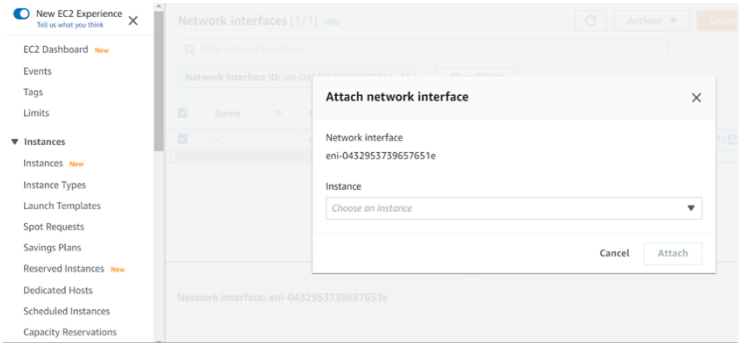
a) Stoppen Sie im **AWS-Portal**sowohl die alte als auch die neue EC2-Instanz.

b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Netzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

c) Trennen Sie die EC2-Instanz, indem Sie auf **Aktionen > Trennen**klicken.



d) Schließen Sie die Netzwerkschnittstelle an die neue EC2-Instanz an, indem Sie auf **Aktionen > Anhängen**klicken. Geben Sie den Namen der EC2-Instanz ein, an den die Netzwerkschnittstelle angeschlossen werden muss.



e) Führen Sie den **Schritt 1** bis **Schritt 4** für alle anderen angehängten Schnittstellen aus. Vergewissern Sie sich, dass Sie die Reihenfolge befolgen und die Reihenfolge der Schnittstelle beibehalten. Das heißt, trennen Sie zuerst Schnittstelle 2 und schließen Sie es an, trennen Sie dann Schnittstelle 3 und schließen Sie es an und so weiter.

5. Sie können die Verwaltungsschnittstelle nicht von einer alten EC2-Instanz trennen. Verschieben Sie also alle sekundären IP-Adressen (falls vorhanden) auf der Verwaltungsschnittstelle (primäre Netzwerkschnittstelle) der alten EC2-Instanz auf die neue EC2-Instanz. Gehen Sie folgendermaßen vor, um eine IP-Adresse von einer Schnittstelle in eine andere zu verschieben:

a) Stellen Sie im **AWS-Portal**sicher, dass sich sowohl die alten als auch die neue EC2-Instanzen im Status "**Stop** "befinden.

b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Verwaltungsnetzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

c) Klicken Sie auf **Aktionen > IP-Adresse verwalten**und notieren Sie sich alle sekundären IP-Adressen (falls vorhanden).

d) Navigieren Sie zur Verwaltungsnetzwerkschnittstelle oder zur primären Schnittstelle der neuen EC2-Instanz.

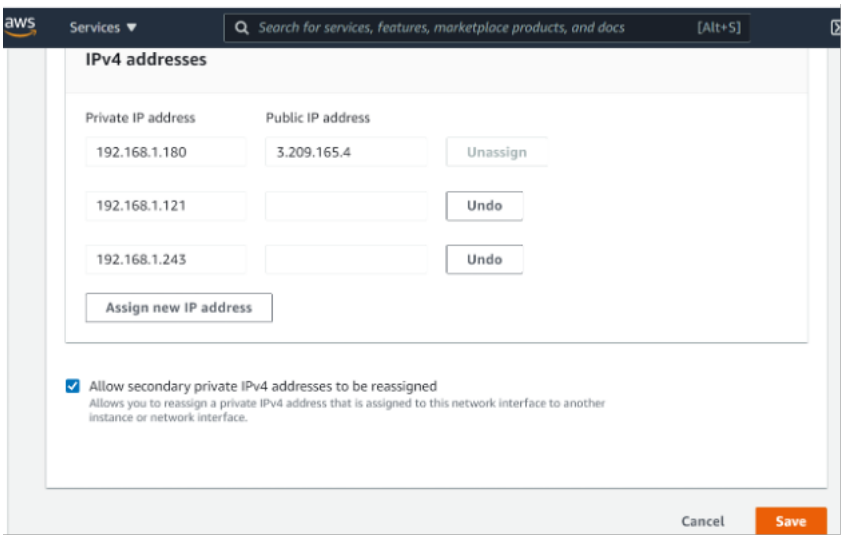
e) Klicken Sie auf **Aktionen > IP-Adressen verwalten**.

f) Klicken Sie unter **IPv4-Adressen**auf **Neue IP-Adresse zuweisen**.

g) Geben Sie die IP-Adressen ein, die im **Schritt 3**vermerkt sind.

h) Aktivieren **Sie das Kontrollkästchen Neuzuweisung sekundärer privater IP-Adressen** zulassen.

i) Klicken Sie auf **Speichern**.



6. Starten Sie die neue EC2-Instanz und überprüfen Sie die Konfiguration. Nachdem die gesamte Konfiguration verschoben wurde, können Sie die alte EC2-Instanz gemäß Ihren Anforderungen löschen oder behalten.
7. Wenn eine EIP-Adresse an die NSIP-Adresse der alten EC2-Instanz angehängt ist, verschieben Sie die alte Instanz-NSIP-Adresse an die NSIP-Adresse der neuen Instanz.
8. Wenn Sie zur alten Instanz zurückkehren möchten, führen Sie die gleichen Schritte in entgegengesetzter Weise zwischen der alten und der neuen Instanz aus.
9. Nachdem Sie von der Abonnementinstanz zur BYOL-Instanz umgezogen sind, ist eine Lizenz erforderlich. Gehen Sie folgendermaßen vor, um eine Lizenz zu installieren:

   - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.

- Laden Sie die Lizenz auf die Instanz hoch.

> **Hinweis:**
>
> Wenn Sie die BYOL-Instanz auf eine Abonnementinstanz (kostenpflichtige Marketplace-Instanz) verschieben, müssen Sie die Lizenz nicht installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Einschränkungen

Die Verwaltungsschnittstelle kann nicht auf die neue EC2-Instanz verschoben werden. Citrix empfiehlt daher, die Verwaltungsschnittstelle manuell zu konfigurieren. Weitere Informationen finden Sie unter **Schritt 5** des vorherigen Verfahrens. Eine neue EC2-Instanz wird mit dem genauen Replikat der alten EC2-Instanz erstellt, aber nur die NSIP-Adresse hat eine neue IP-Adresse.

Lastausgleichsserver in verschiedenen Availability Zones

October 17, 2024

Eine VPX-Instanz kann zum Lastenausgleich von Servern verwendet werden, die in derselben Availability Zone ausgeführt werden, oder in:

- Eine andere Availability Zone (AZ) in derselben AWS VPC
- Eine andere AWS-Region
- AWS EC2 in einer VPC

Um einer VPX-Instanz den Lastenausgleich für Server zu ermöglichen, die außerhalb des AWS VPC laufen, Wenn sich die VPX-Instanz in der Instanz befindet, konfigurieren Sie sie so, dass der Datenverkehr mithilfe von EIPs über das Internet-Gateway geleitet wird:

1. Konfigurieren Sie ein SNIP auf der NetScaler VPX-Instanz mithilfe der NetScaler-CLI oder der GUI.
2. Aktivieren Sie das Routing von Datenverkehr aus der AZ, indem Sie ein öffentliches Subnetz für den serverseitigen Datenverkehr erstellen.
3. Fügen Sie der Routingtabelle mithilfe der AWS GUI-Konsole eine Internet-Gateway -Route hinzu.
4. Ordnen Sie die Routingtabelle, die Sie aktualisiert haben, dem serverseitigen Subnetz zu.
5. Ordnen Sie eine EIP der serverseitigen privaten IP-Adresse zu, die einer NetScaler SNIP-Adresse zugeordnet ist.

So funktioniert Hochverfügbarkeit auf AWS

October 17, 2024

Sie können zwei NetScaler VPX-Instanzen auf AWS als aktives und passives Paar mit hoher Verfügbarkeit (HA) konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Hochverfügbarkeit innerhalb derselben Zone
- Hohe Verfügbarkeit über verschiedene Zonen hinweg

> **Hinweis:**
>
> Damit die Hochverfügbarkeit funktioniert, stellen Sie sicher, dass beide NetScaler VPX-Instanzen mit IAM-Rollen verknüpft und dem NSIP die Elastic IP (EIP)-Adresse zugewiesen sind. Sie müssen NSIP keine EIP zuweisen, wenn das NSIP über die NAT-Instanz das Internet erreichen kann.

Hohe Verfügbarkeit innerhalb derselben Zonen

In einer Hochverfügbarkeitsbereitstellung innerhalb derselben Zonen müssen beide VPX-Instanzen ähnliche Netzwerkkonfigurationen haben.

Folgen Sie diesen beiden Regeln:

Regel 1. Jede Netzwerkkarte auf einer VPX-Instanz muss sich im selben Subnetz befinden wie die entsprechende Netzwerkkarte in der anderen VPX. Beide Instanzen müssen Folgendes haben:

- Verwaltungsschnittstelle im selben Subnetz (als Management-Subnetz bezeichnet)
- Client-Schnittstelle im selben Subnetz (als Client-Subnetz bezeichnet)
- Serverschnittstelle im selben Subnetz (als Serversubnetz bezeichnet)

Regel 2. Die Reihenfolge der Mgmt-NIC, der Client-NIC und der Server-NIC auf beiden Instanzen muss identisch sein. Beispielsweise wird das folgende Szenario nicht unterstützt.

VPX-Instanz 1

NIC 0: Verwaltung NIC 1: Client NIC 2: Server

VPX-Instanz 2

NIC 0: Verwaltung

NIC 1: Server

NIC 2: Client

In diesem Szenario befindet sich NIC 1 von Instanz 1 im Clientsubnetz, während NIC 1 von Instanz 2 im Serversubnetz ist. Damit HA funktioniert, muss sich NIC 1 der beiden Instanzen entweder im Client-Subnetz oder im Serversubnetz befinden.

Ab 13.0 41.xx kann eine hohe Verfügbarkeit erreicht werden, indem sekundäre private IP-Adressen migriert werden, die an die Netzwerkkarten (Client- und serverseitige Netzwerkkarten) des primären HA-Knotens nach dem Failover angeschlossen sind. In dieser Bereitstellung gilt:

- Beide VPX-Instanzen haben die gleiche Anzahl von Netzwerkkarten und Subnetzzuordnung gemäß der NIC-Aufzählung.
- Jede VPX-NIC hat eine zusätzliche private IP-Adresse, mit Ausnahme der ersten NIC - die der Verwaltungs-IP-Adresse entspricht. Die zusätzliche private IP-Adresse wird als primäre private IP-Adresse in der AWS-Webkonsole angezeigt. In unserem Dokument bezeichnen wir diese zusätzliche IP-Adresse als Dummy-IP-Adresse).
- Die Dummy-IP-Adressen dürfen auf der NetScaler-Instanz nicht als VIP und SNIP konfiguriert werden.
- Andere sekundäre private IP-Adressen müssen bei Bedarf erstellt und als VIP und SNIP konfiguriert werden.
- Bei Failover sucht der neue Primärknoten nach konfigurierten SNIPs und VIPs und verschiebt sie von NICs, die an den vorherigen primären Knoten angeschlossen sind, auf die entsprechenden Netzwerkkarten auf dem neuen Primärbereich.
- NetScaler Instanzen erfordern IAM-Berechtigungen, damit HA funktioniert. Fügen Sie der IAM-Richtlinie, die jeder Instanz hinzugefügt wurde, die folgenden IAM-Berechtigungen hinzu.

„iam:GetRole“ "ec2:Instanzen beschreiben" "ec2:Netzwerkschnittstellen beschreiben" "ec2:PrivateIp-Adressen zuweisen"

> **Hinweis:**
>
> unassignPrivateIpAddress ist nicht erforderlich.

Diese Methode ist schneller als die Legacy-Methode. Bei der älteren Methode hängt HA von der Migration elastischer AWS-Netzwerkschnittstellen des primären Knotens zum sekundären Knoten ab.

Für eine Legacy-Methode sind die folgenden Richtlinien erforderlich:

„iam:GetRole“ "ec2:Instanzen beschreiben" "ec2:Adressen beschreiben" "ec2:Partneradresse" "ec2:Adresse trennen"

Weitere Informationen finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.

Hohe Verfügbarkeit über verschiedene Zonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als aktiv-passives Paar mit hoher Verfügbarkeit im Modus Independent Network Configuration (INC) konfigurieren. Beim Failover migriert die EIP (Elastic IP) des VIP der primären Instanz auf die sekundäre, die als neue primäre Instanz übernommen wird. Im Failover-Prozess wird die AWS-API:

- Überprüft die virtuellen Server, an die `IPSets` angeschlossen sind.
- Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und eine, die über den IP-Satz angeschlossen ist.
- Ordnet die öffentliche IP (EIP) der privaten IP zu, die zum neuen primären VIP gehört.

Für HA über verschiedene Zonen hinweg sind folgende Richtlinien erforderlich:

„`iam:GetRole“ "ec2:Instanzen beschreiben" "ec2:Adressen beschreiben" "ec2:Partneradresse" "ec2:Adresse trennen"`

Weitere Informationen finden Sie unter Hohe Verfügbarkeit in AWS-Verfügbarkeitszonen.

Bevor Sie mit der Bereitstellung beginnen

Bevor Sie mit einer HA-Bereitstellung auf AWS beginnen, lesen Sie das folgende Dokument:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Hohe Verfügbarkeit

Problembehandlung

Um Fehler während eines HA-Failovers der NetScaler VPX-Instanz in der AWS-Cloud zu beheben, überprüfen Sie die am Speicherort `/var/log/` gespeicherte Datei `cloud-ha-daemon.log`.

Bereitstellen eines VPX-HA-Paar in derselben AWS-Verfügbarkeitszone

October 17, 2024

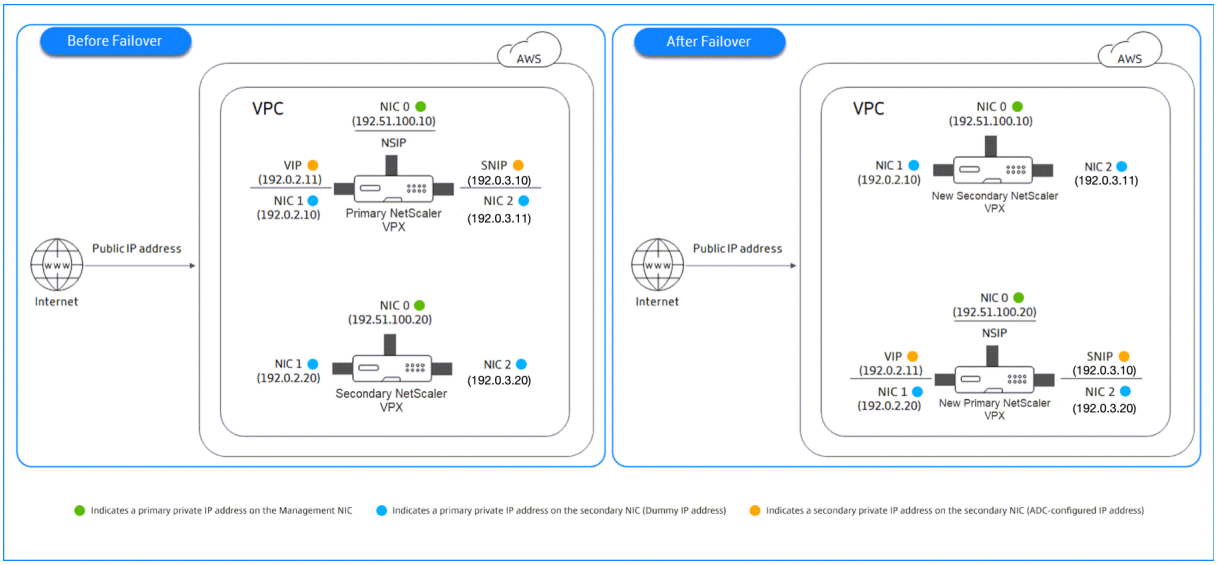
> **Hinweis:**
>
> Ab NetScaler Version 13.1 Build 27.x unterstützt das VPX HA-Paar in derselben AWS-Verfügbarkeitszone IPv6-Adressen.

Sie können zwei NetScaler VPX-Instanzen in AWS als HA-Paar in derselben AWS-Zone konfigurieren, in der sich beide VPX-Instanzen im selben Subnetz befinden. HA wird erreicht, indem sekundäre private IP-Adressen, die an die NICs (client- und serverseitige NICs) des primären HA-Knotens angeschlossen sind, nach einem Failover zum sekundären HA-Knoten migriert. Alle Elastic IP-Adressen, die mit den sekundären privaten IP-Adressen verknüpft sind, werden ebenfalls migriert.

Das NetScaler VPX HA-Paar unterstützt sowohl IPv4- als auch IPv6-Adressen in derselben AWS-Verfügbarkeitszone.

Die folgende Abbildung zeigt ein HA-Failoverszenario durch Migration sekundärer privater IP-Adressen.

Abbildung 2. Ein NetScaler VPX HA-Paar auf AWS mit privater IP-Migration



Bevor Sie mit Ihrem Dokument beginnen, lesen Sie die folgenden Dokumente:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Hohe Verfügbarkeit

So stellen Sie ein VPX-HA-Paar in derselben Zone bereit

Hier ist eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-HA-Paars in derselben Zone:

1. Erstellen Sie zwei VPX-Instanzen auf AWS mit jeweils drei NICs.
2. Weisen Sie VIP und SNIP des primären Knotens eine sekundäre private AWS-IP-Adresse zu.
3. Konfigurieren Sie VIP und SNIP auf dem primären Knoten mithilfe sekundärer privater AWS-IP-Adressen.
4. Konfigurieren Sie HA auf beiden Knoten.

Schritt 1. Schritt 1: Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) mit derselben VPC mit jeweils drei NICs (Ethernet 0, Ethernet 1, Ethernet 2)

Befolgen Sie die Schritte unter Bereitstellen einer NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole.

Schritt 2. Schritt 2: Weisen Sie auf dem primären Knoten private IP-Adressen für Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Backend-Server-IP oder SNIP) zu

Die AWS-Konsole weist den konfigurierten NICs automatisch primäre private IP-Adressen zu. Weisen Sie VIP und SNIP mehr private IP-Adressen zu, die als sekundäre private IP-Adressen bekannt sind.

Gehen Sie folgendermaßen vor, um einer Netzwerkschnittstelle eine private IP-Adresse zuzuweisen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich **Netzwerkschnittstellen** und dann die Netzwerkschnittstelle aus, die mit der Instanz verbunden ist.
3. Wählen Sie **Aktionen > IP-Adressen verwalten**.
4. Wählen Sie je nach Anforderung **IPv4-Adressenoder IPv6-Adressen** aus.
5. Für IPv4-Adressen:

    a) Wählen Sie **Neue IP zuweisen**.
    b) Geben Sie eine bestimmte IPv4-Adresse ein, die innerhalb des Subnetzbereichs der Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählen kann.
    c) (Optional) Wählen Sie **Neuzuweisung** zulassen, damit die sekundäre private IP-Adresse neu zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.

6. Für IPv6-Adressen:

    a) Wählen Sie **Neue IP zuweisen**.
    b) Geben Sie eine bestimmte IPv6-Adresse ein, die innerhalb des Subnetzbereichs für die Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählen kann.

c) (Optional) Wählen Sie **Neuzuweisung** zulassen, damit die primäre oder sekundäre private IP-Adresse neu zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.

7. Wählen Sie **Ja > Aktualisieren**.

Unter der **Instanzbeschreibung**werden die zugewiesenen privaten IP-Adressen angezeigt.

> **Hinweis:**
>
> In einer IPv4-HA-Paarbereitstellung können Sie nur die sekundären IPv4-Adressen auf der Schnittstelle zuweisen und sie als VIP- und SNIP-Adressen verwenden. In einer IPv6-HA-Pair-Bereitstellung können Sie jedoch entweder die primären IPv6- oder sekundären IPv6-Adressen auf der Schnittstelle zuweisen und sie als VIP- und SNIP-Adressen verwenden.

Schritt 3. Schritt 3: Konfigurieren von VIP und SNIP auf dem primären Knoten mit sekundären privaten IP-Adressen

Greifen Sie mit SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und geben Sie ein:

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

Konfigurieren Sie als Nächstes VIP und SNIP.

Geben Sie für VIP Folgendes ein:

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

Geben Sie für SNIP Folgendes ein:

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

Tippen Sie `save config` zum Speichern ein.

Um die konfigurierten IP-Adressen anzuzeigen, geben Sie den folgenden Befehl ein:

```
show ns ip
```

Weitere Informationen finden Sie in den folgenden Artikeln:

- Virtuelle IP-Adressen (VIP) konfigurieren und verwalten
- Konfigurieren der NSIP-Adresse

Schritt 4: Konfigurieren von HA auf beiden Instanzen

Öffnen Sie auf dem primären Knoten einen Shell-Client und geben Sie den folgenden Befehl ein:


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

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

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

Geben Sie `save config` ein, um die Konfiguration zu speichern.

Um die konfigurierten HA-Knoten anzuzeigen, geben Sie ein `show ha node`.

Nach dem Failover werden die sekundären privaten IP-Adressen, die auf dem vorherigen primären Knoten als VIP und SNIP konfiguriert sind, auf den neuen primären Knoten migriert.

Um ein Failover auf einem Knoten zu erzwingen, geben Sie `force HA`Failover ein.

Migrieren Sie ein Legacy-HA-Paar auf ein neues HA-Paar basierend auf der sekundären privaten IP-Migration

> **Hinweis:**
>
> Die veraltete Methode zur Bereitstellung eines VPX-HA-Paars, die auf der ENI-Migration basiert, ist veraltet. Daher empfehlen wir Ihnen, die HA-Paar-Bereitstellung auf der Grundlage der sekundären privaten IP-Migration zu verwenden.

Um eine nahtlose Migration vom alten HA-Paar zu einem neuen HA-Paar auf der Grundlage einer sekundären privaten IP-Migration zu ermöglichen, stellen Sie Folgendes sicher:

1. Sowohl der primäre als auch der sekundäre Knoten müssen dieselbe Anzahl von Schnittstellen haben, und diese Schnittstellen müssen sich in denselben Subnetzen befinden.
2. VIP und SNIP, die in der alten Methode als primäre private IP-Adresse konfiguriert wurden, müssen in der neuen Methode auf eine sekundäre private IP-Adresse migriert werden.
3. Die für die neue HA-Bereitstellung erforderlichen IAM-Berechtigungen müssen den primären und sekundären NetScaler-Instanzen hinzugefügt werden.
4. Starten Sie sowohl die primäre als auch die sekundäre NetScaler-Instanz neu.

Weitere Informationen finden Sie unter Hochverfügbarkeit innerhalb derselben Zonen.

Stellen Sie mithilfe der Citrix CloudFormation-Vorlage ein Hochverfügbarkeitspaar bereit

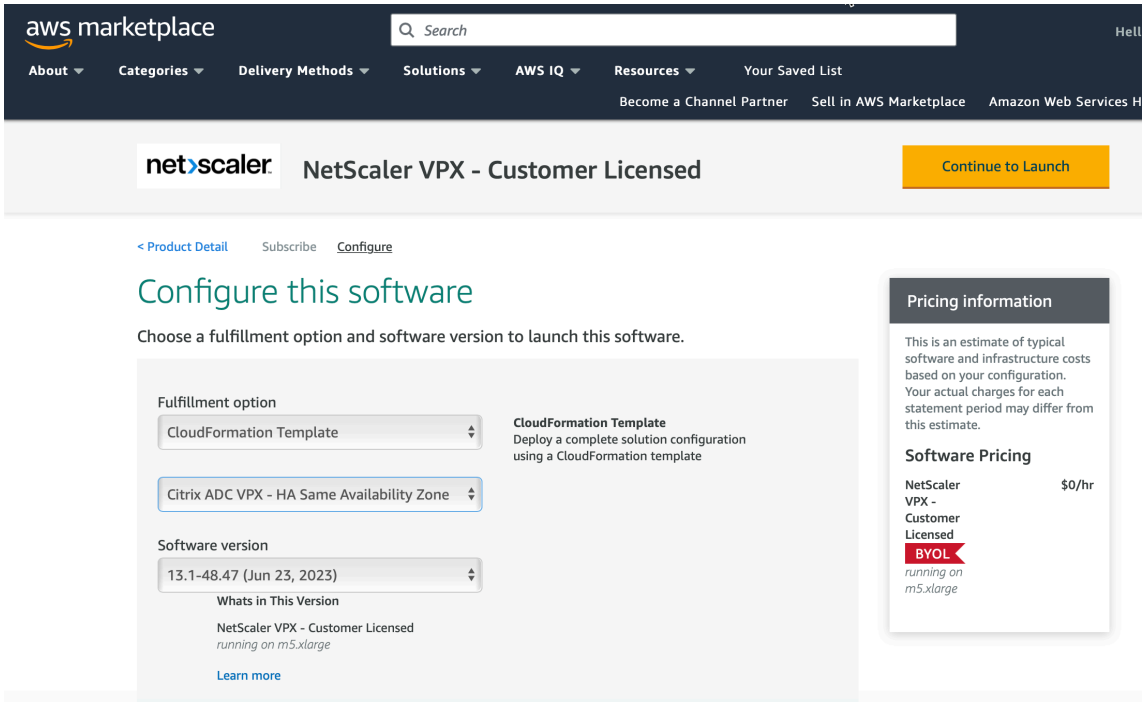
Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine VPC
- Drei Subnetze innerhalb der VPC
- Eine Sicherheitsgruppe mit UDP 3003, TCP 3009—3010, HTTP, SSH-Ports geöffnet
- Ein Schlüsselpaar
- Erstellen Sie ein Internet-Gateway
- Bearbeiten von Routinetabellen für Client- und Verwaltungsnetzwerke, um auf das Gateway

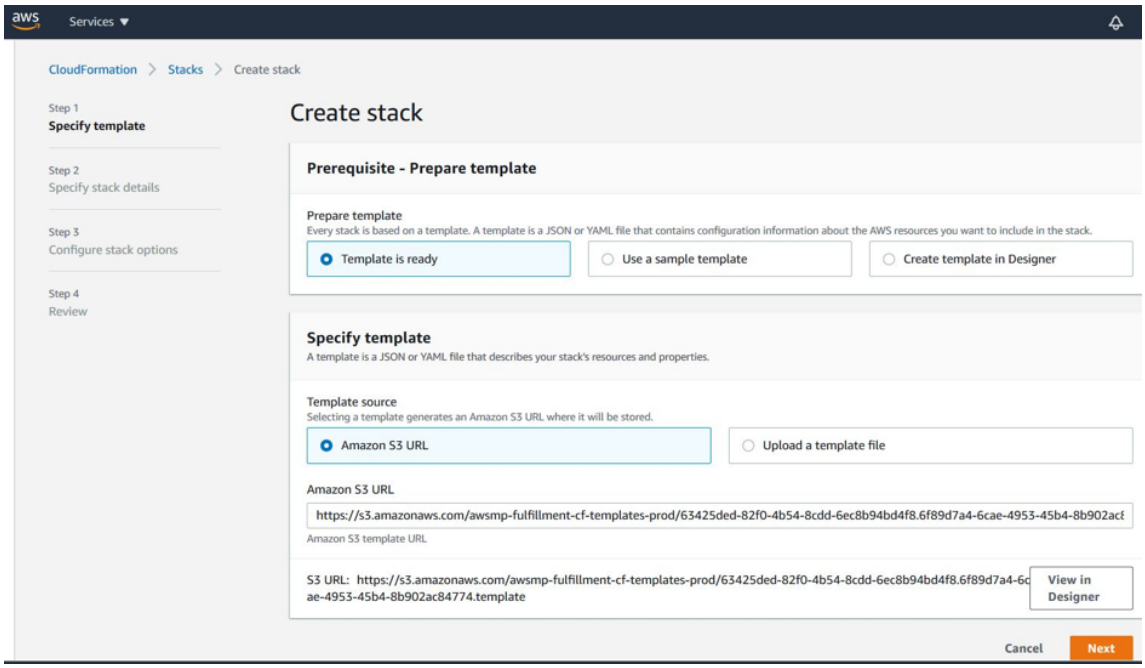
> **Hinweis:**
>
> Die Citrix CloudFormation-Vorlage erstellt automatisch eine IAM-Rolle. Bestehende IAM-Rollen werden nicht in der Vorlage angezeigt.

So starten Sie die Citrix CloudFormation-Vorlage:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen am AWS-Marketplace an.
2. Geben Sie im Suchfeld **NetScaler VPX** ein, um nach dem NetScaler AMI zu suchen, und klicken Sie auf **Los**.
3. Klicken Sie auf der Suchergebnisseite auf das gewünschte NetScaler VPX Angebot.
4. Klicken Sie auf die Registerkarte **Preise**, um zu **Preisinformationen** zu gelangen.
5. Wählen Sie die Region und die **Fulfillment-Option** als **NetScaler VPX** —**Kundenlizenziert**aus.
6. Klicken Sie auf **Weiter, um zu abonnieren**.
7. Überprüfen Sie die Details auf der Seite **Abonnieren** und klicken Sie **auf Configuration fortsetzen**.
8. Wählen Sie **Bereitstellungsmethode** als **CloudFormation-Vorlage** aus.
9. Wählen Sie die erforderliche CloudFormation-Vorlage aus.
10. Wählen Sie **Softwareversion** und **Region** aus und klicken Sie auf **Weiter zu Launch**.



11. Wählen Sie unter **Aktion auswählen** die Option **CloudFormation starten** aus, und klicken Sie auf **Starten**. Die Seite **Stapel erstellen** wird angezeigt.
12. Klicken Sie auf **Weiter**.

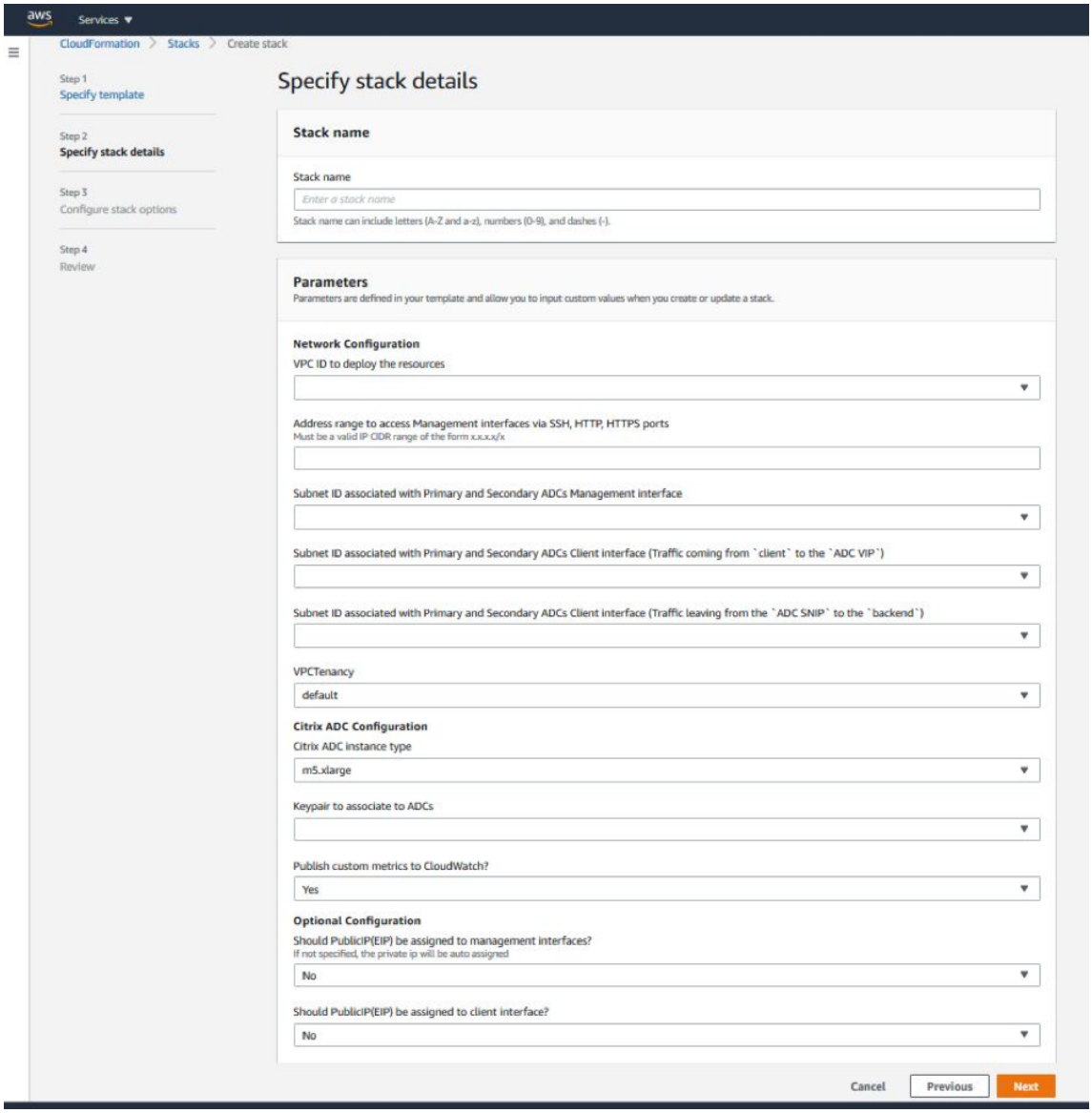


13. Die Seite **Stapeldetails angeben** wird angezeigt. Geben Sie die folgenden Details ein.

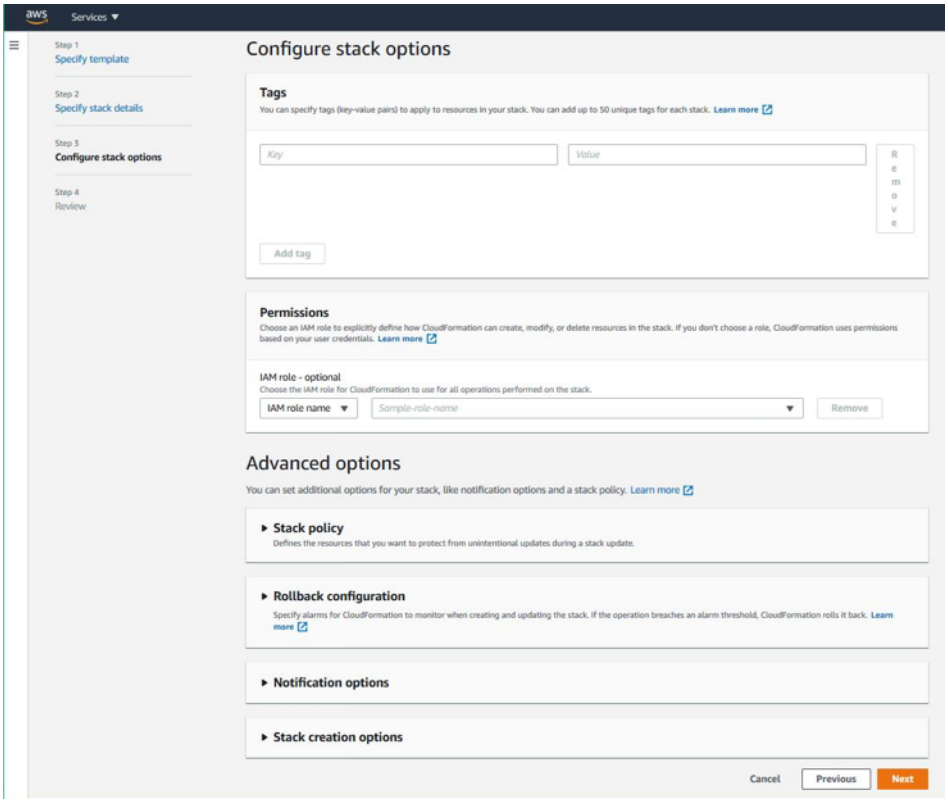
    - Geben Sie einen **Stack-Namen**ein. Der Name muss innerhalb von 25 Zeichen sein.
    - Führen Sie unter **Netzwerkkonfiguration**die folgenden Schritte aus:

- Wählen Sie **Verwaltungsteilnetz**, **Client-Subnetz** und **Server-Subnetz** aus. Stellen Sie sicher, dass Sie die richtigen Teilnetze auswählen, die Sie in der VPC erstellt haben, die Sie unter VPC-ID ausgewählt haben.
- Fügen Sie **primäre Verwaltungs-IP**, **sekundäre Verwaltungs-IP, Client-IPund Server-** Die IP-Adressen müssen zu denselben Subnetzen der jeweiligen Teilnetze gehören. Die IP-Adressen müssen zu den gleichen Subnetzen der jeweiligen Subnetze gehören. Alternativ können Sie die Vorlage die IP-Adressen automatisch zuweisen lassen.
- Wählen Sie **Standard** für **vpcTenancy**aus.

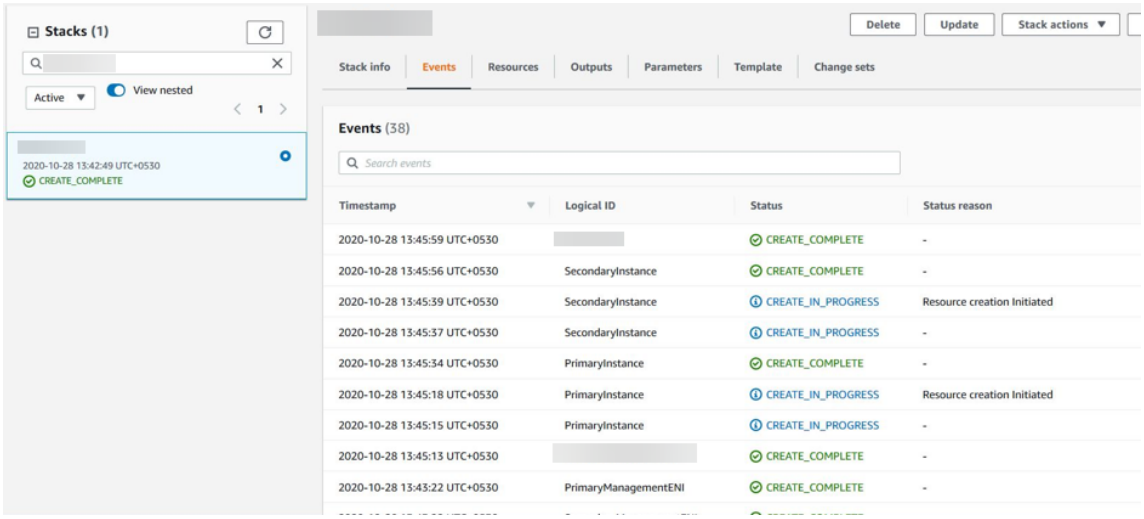
- Führen Sie unter **NetScaler Configuration**die folgenden Schritte aus:
  - Wählen Sie **m5.xlarge** als **Instanztyp**aus.
  - Wählen Sie im Menü für Schlüsselpaar das **Schlüsselpaar**aus, das Sie bereits erstellt haben.
  - Standardmäßig wird die **Benutzerdefinierte Metriken in CloudWatch veröffentlichen?** Option ist auf **Ja**eingestellt. Wenn Sie diese Option deaktivieren möchten, wählen Sie **Nein**aus.
    Weitere Informationen zu CloudWatch-Metriken finden Sie unter [Überwachen Sie Ihre Instanzen mit Amazon CloudWatch] (#monitor-your-instances-using-amazon-cloudWatch).
- Führen Sie unter **Optionale Konfiguration**Folgendes aus:
  - Standardmäßig lautet die **: Soll den Verwaltungsschnittstellen eine öffentliche IP (EIP) zugewiesen werden?** Option ist auf **Nein**eingestellt.
  - Standardmäßig lautet die Adresse **. Soll der Clientschnittstelle eine öffentliche IP (EIP) zugewiesen werden?** Option ist auf **Nein**eingestellt.



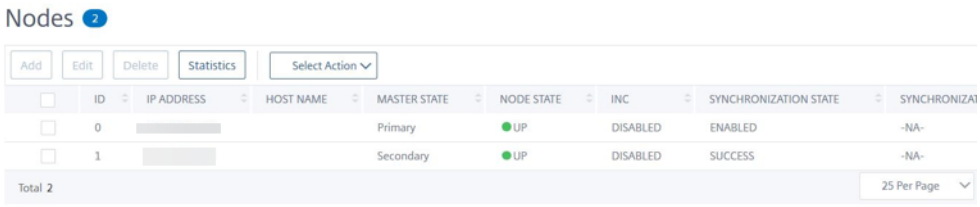
14. Klicken Sie auf **Weiter**.
15. Die Seite **Stack-Optionen konfigurieren** wird angezeigt. Dies ist eine optionale Seite.



16. Klicken Sie auf **Weiter**.
17. Die Seite **Optionen** wird angezeigt. (Dies ist eine optionale Seite.). Klicken Sie auf **Weiter**.
18. Die Seite **Überprüfen** wird angezeigt. Nehmen Sie sich einen Moment Zeit, um die Einstellungen zu überprüfen und gegebenenfalls Änderungen vorzunehmen.
19. Wählen Sie **Ich erkenne an, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt.** und klicken Sie dann auf **Stapel erstellen**.
20. Der Status **CREATE-IN-PROGRESS** wird angezeigt. Warten Sie bis der Status **CREATE-COMPLETE**ist. Wenn sich der Status nicht in **COMPLETE**ändert, überprüfen Sie die Registerkarte **Ereignisse** auf den Grund des Fehlers und erstellen Sie die Instanz mit den richtigen Konfigurationen neu.



21. Navigieren Sie nach dem Erstellen einer IAM-Ressource zu **EC2 Management Console > Instanzen**. Sie finden zwei VPX-Instanzen, die mit IAM-Rolle erstellt wurden. Die primären und sekundären Knoten werden jeweils mit drei privaten IP-Adressen und drei Netzwerkschnittstellen erstellt.
22. Melden Sie sich am primären Knoten mit dem Benutzernamen`nsroot` und der Instanz-ID als Kennwort an. Navigieren Sie in der GUI zu **System > Hochverfügbarkeit > Knoten**. Der NetScaler VPX ist bereits von der CloudFormation-Vorlage als HA-Paar konfiguriert.
23. Das NetScaler VPX HA-Paar wird angezeigt.



Überwachen Sie Ihre Instanzen mit Amazon CloudWatch

Sie können den Amazon CloudWatch-Dienst verwenden, um eine Reihe von NetScaler VPX-Metriken wie CPU- und Speicherauslastung und Durchsatz zu überwachen. CloudWatch überwacht Ressourcen und Anwendungen, die auf AWS ausgeführt werden, in Echtzeit. Sie können über die AWS Management Console auf das Amazon CloudWatch-Dashboard zugreifen. Weitere Informationen finden Sie unter Amazon CloudWatch.

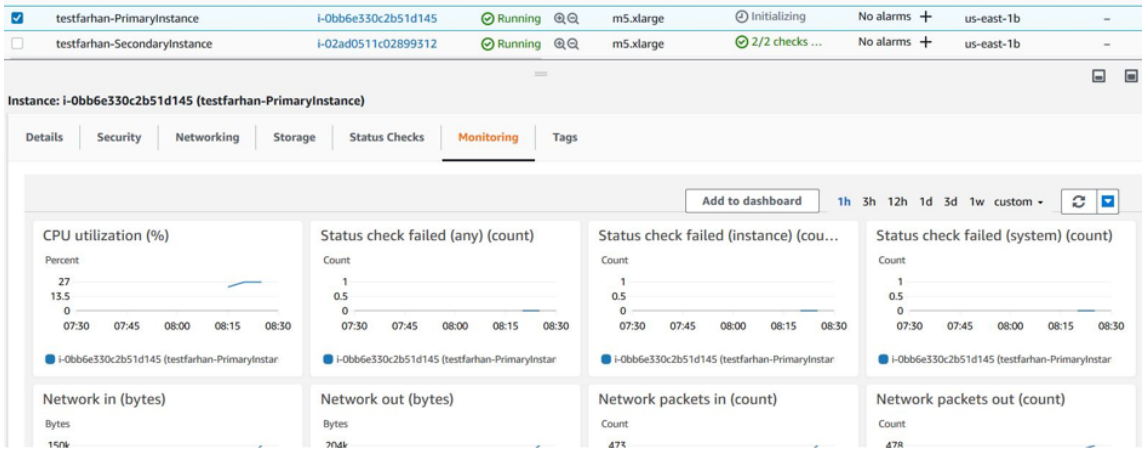
Punkte zu beachten

- Wenn Sie eine NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert.
- Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, lautet die Standardoption „Ja“. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie „Nein“.
- Metriken sind für CPU (Verwaltung und Paket-CPU-Auslastung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

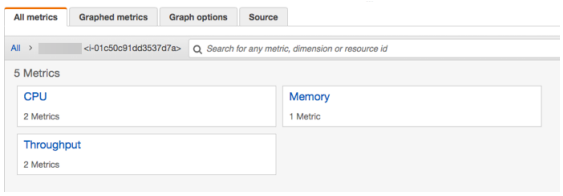
So zeigen Sie CloudWatch-Metriken an

Gehen Sie folgendermaßen vor, um CloudWatch-Metriken für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **AWS Management Console > EC2 > Instanzen** an.
2. Wählen Sie die Instanz aus.
3. Klicken Sie auf **Überwachung**.
4. Klicken Sie auf **Alle CloudWatch-Metriken anzeigen**.

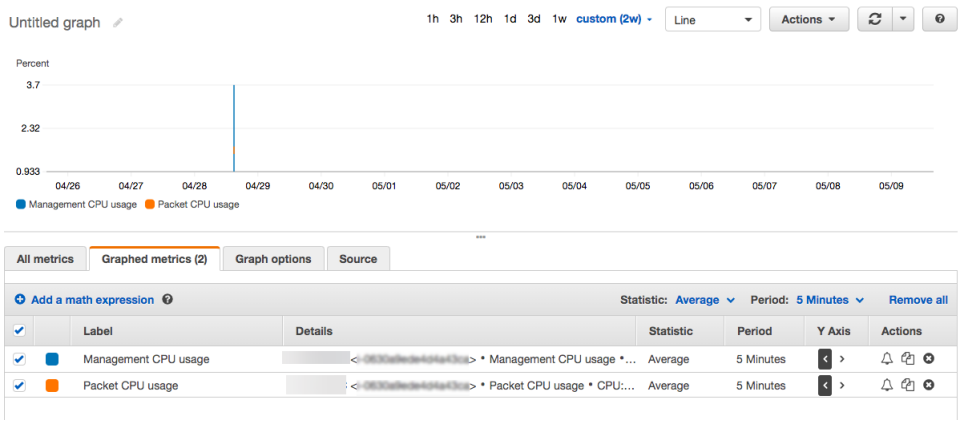


5. Klicken Sie unter Alle Metriken auf Ihre Instanz-ID.



6. Klicken Sie auf die Metriken, die Sie anzeigen möchten, und legen Sie die Dauer fest (nach Minuten, Stunden, Tagen, Wochen, Monaten).
7. Klicken Sie auf **Befehlseinschleusung**, um die Nutzungsstatistiken anzuzeigen. Verwenden Sie die **Graph options**, um Ihr Diagramm anzupassen.

Abbildung. Graphische Metriken für die CPU-



Konfigurieren von SR-IOV auf einem Hochverfügbarkeitssetup

Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab NetScaler Version 12.0 57.19 verfügbar. Weitere Informationen zum Konfigurieren von SR-IOV finden Sie unter Konfigurieren von NetScaler VPX-Instanzen zur Verwendung der SR-IOV-Netzwerkschnittstelle.

Zugehörige Ressourcen

So funktioniert Hochverfügbarkeit auf AWS

Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen

October 17, 2024

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als aktiv-passives Paar mit hoher Verfügbarkeit im Modus Independent Network Configuration (INC) konfigurieren. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

Punkte zu beachten

- Lesen Sie die folgenden Dokumente, bevor Sie mit der Bereitstellung beginnen:

  - AWS-Terminologie
  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien

- Das VPX-Hochverfügbarkeitspaar kann sich entweder in derselben Availability Zone in einem anderen Subnetz oder in zwei verschiedenen AWS-Verfügbarkeitszonen befinden.
- Citrix empfiehlt, dass Sie verschiedene Subnetze für die Verwaltung (NSIP), den Clientverkehr (VIP) und den Back-End-Server (SNIP) verwenden.
- Hochverfügbarkeit muss im Modus Independent Network Configuration (INC) festgelegt werden, damit ein Failover funktioniert.
- Für die beiden Instanzen muss Port 3003 für UDP-Verkehr geöffnet sein, da dieser für Heartbeats verwendet wird.
- Die Management-Subnetze beider Knoten müssen über interne NAT Zugriff auf das Internet oder auf den AWS-API-Server haben, damit die restlichen APIs funktionsfähig sind.
- Die IAM-Rolle muss über eine E2-Berechtigung für die öffentliche IP- oder Elastic IP (EIP) -Migration und EC2-Routentabellen-Berechtigungen für die private IP-Migration verfügen.

Sie können Hochverfügbarkeit in AWS Availability Zones auf folgende Weise bereitstellen:

- Verwenden von elastischen IP-Adressen
- Verwenden privater IP-Adressen

Zusätzliche Referenzen

Weitere Informationen zu NetScaler Application Delivery Management (ADM) für AWS finden Sie unter Installieren des NetScaler ADM-Agenten auf AWS.

Bereitstellen eines VPX Hochverfügbarkeitspaars mit elastischen IP-Adressen in verschiedenen AWS-Zonen

October 17, 2024

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mithilfe von elastischen IP-Adressen (EIP) im INC-Modus konfigurieren.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

So funktioniert HA mit EIP-Adressen in verschiedenen AWS-Zonen

Bei einem Failover migriert das EIP des VIP der primären Instanz zur sekundären Instanz, die als neue primäre Instanz übernimmt. Im Failover-Prozess führt die AWS-API:

1. Überprüft die virtuellen Server, an die `IPSets` angeschlossen sind.
2. Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und derjenige, der über den IP-Satz angeschlossen ist.
3. Ordnet die öffentliche IP (EIP) der privaten IP zu, die zum neuen primären VIP gehört.

> **Hinweis:**
>
> Um Ihr Netzwerk vor Angriffen wie Denial-of-Service (DoS) zu schützen, können Sie bei der Verwendung eines EIP Sicherheitsgruppen in AWS erstellen, um den IP-Zugriff einzuschränken. Zur Hochverfügbarkeit können Sie gemäß Ihren Bereitstellungen von EIP zu einer privaten IP-Verlagungslösung wechseln.

So stellen Sie ein VPX-Paar mit hoher Verfügbarkeit und elastischen IP-Adressen in verschiedenen AWS-Zonen bereit

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones oder in derselben Zone, aber in verschiedenen Subnetzen bereit.
3. Konfigurieren der Hochverfügbarkeit
    a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
    b) Fügen Sie in beiden Instanzen einen IP-Satz hinzu.
    c) Binden Sie die in beiden Instanzen festgelegte IP an den VIP.
    d) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1 und 2 die AWS-Konsole. Verwenden Sie für Schritte 3 die NetScaler VPX GUI oder die CLI.

Schritt 1. Erstellen Sie eine virtuelle private Cloud (VPC) von Amazon.

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Verfügbarkeitszonen oder in derselben Zone, aber in unterschiedlichen Subnetzen bereit. Schließen Sie eine EIP an die VIP des primären VPX an.

Weitere Informationen zum Erstellen einer VPC und Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Szenario: eigenständige Instanz

Schritt 3. Konfigurieren der Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   Auf dem sekundären Knoten:

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens

   <prim_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des primären Knotens

2. Fügen Sie das IP-Set in beiden Instanzen hinzu.

   Geben Sie in beiden Instanzen den folgenden Befehl ein.

   ```
   add ipset <ipsetname>
   ```

3. Binden Sie den IP-Satz an den VIP-Satz auf beiden Instanzen.

   Geben Sie den folgenden Befehl für beide Instanzen ein:

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Hinweis:**
   >
   > Sie können den IP-Satz an den primären VIP oder an den sekundären VIP binden. Wenn Sie jedoch den IP-Satz an den primären VIP binden, verwenden Sie den sekundären VIP, um dem virtuellen Server hinzuzufügen, und umgekehrt.

4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

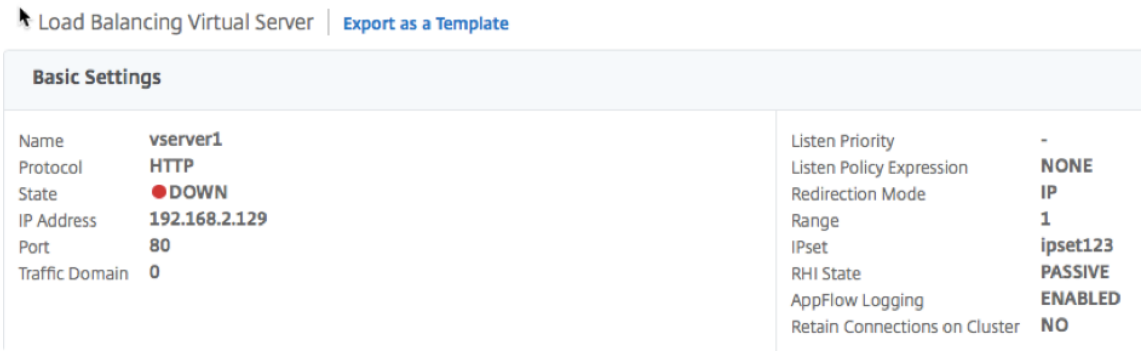
   Geben Sie den folgenden Befehl ein:

   ```
   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;
   ```


Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich am primären Knoten mit Benutzername`nsroot` und Instanz-ID als Kennwort an.
3. Wechseln Sie in der GUI zu **Konfiguration** > **System** > **Hochverfügbarkeit**. Klicken Sie auf **Hinzufügen**.
4. Fügen Sie im Feld **Remote-Knoten-IP-Adresse** die private IP-Adresse der Management-NIC des sekundären Knotens hinzu.
5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .
6. Fügen Sie unter **Anmeldeinformationen des Remote-Systems** den Benutzernamen und das Kennwort für den sekundären Knoten hinzu, und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie den IP-Satz hinzu und binden Sie den IP-Satz an den VIP-Satz beider Instanzen
9. Navigieren Sie in der GUI zu **System** > **Netzwerk** > **IPs** > **Hinzufügen**.
10. Fügen Sie die erforderlichen Werte für IP-Adresse, Netzwerkmaske, IP-Typ (virtuelle IP) hinzu und klicken Sie auf **Erstellen**.
11. Navigieren Sie zu **System** > **Netzwerk** > **IP-Sets** > **Hinzufügen**. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
12. Wählen Sie auf der Seite IPv4s die virtuelle IP aus und klicken Sie auf **Einfügen**. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.
13. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

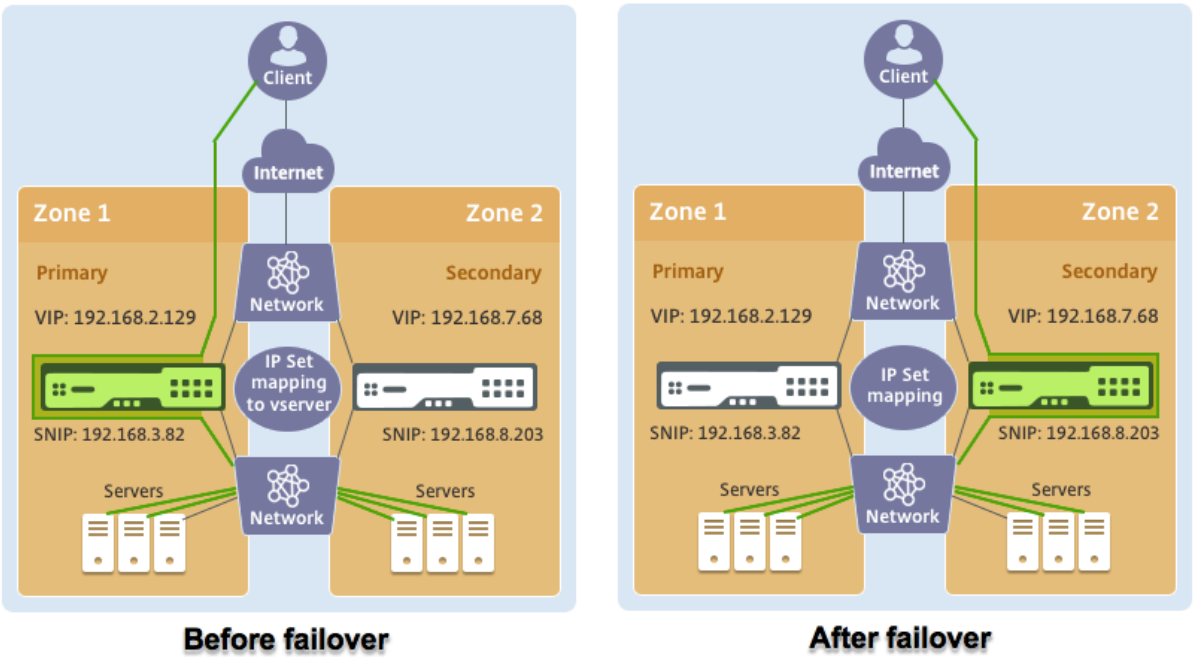
    Gehen Sie in der GUI zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.



Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server. Ein EIP ist an den VIP des primären Knotens angeschlossen.

Diagramm: Dieses Diagramm veranschaulicht das NetScaler VPX Hochverfügbarkeits-Setup im INC-Modus in AWS



Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf Primär:

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Hier bezieht sich 192.168.6.82 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf Sekundarstufe:

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Hier bezieht sich 192.168.1.108 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz auf beiden Instanzen an den VIP

Auf Primär:

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bindipset ipset123 192.168.7.68
```

Auf Sekundarstufe:

```
add ipset ipset123
add ns ip 192.168.7.68 255.255.255.0 -type VIP
bind ipset ipset123 192.168.7.68
```

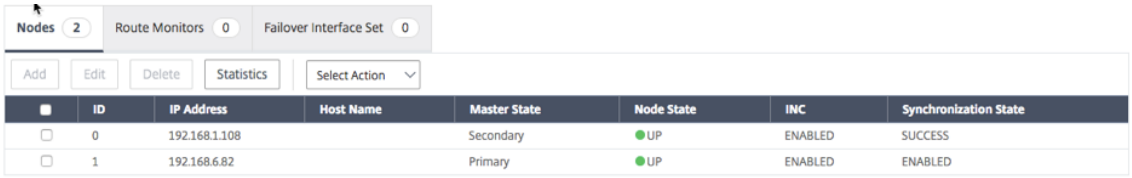
3. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Der folgende Befehl:

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Speichern Sie die Konfiguration.

5. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären.



Bereitstellen eines VPX Hochverfügbarkeitspaars mit privaten IP-Adressen in verschiedenen AWS-Zonen

October 17, 2024

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mit privaten IP-Adressen im INC-Modus konfigurieren. Diese Lösung kann problemlos in das vorhandene Multizonen-VPX-Hochverfügbarkeitspaar mit elastischen IP-Adressenintegriert werden. Daher können Sie beide Lösungen zusammen verwenden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

> **Hinweis:**
>
> Diese Bereitstellung wird ab NetScaler Release 13.0 Build 67.39 unterstützt. Diese Bereitstellung ist mit AWS Transit Gateway kompatibel.

Hochverfügbarkeits-Paar mit privaten IP-Adressen unter Verwendung von AWS nicht gemeinsam genutzter VPC

Voraussetzungen

Stellen Sie sicher, dass die mit Ihrem AWS-Konto verknüpfte IAM-Rolle über die folgenden IAM-Berechtigungen verfügt:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }
```

Bereitstellen eines VPX-HA-Paars mit privaten IP-Adressen mithilfe der nicht gemeinsam genutzten AWS VPC

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen unter Verwen-

dung privater IP-Adressen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones bereit.
3. Konfigurieren der Hochverfügbarkeit

    a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
    b) Fügen Sie die entsprechenden Routentabellen in der VPC hinzu, die auf die Clientschnittstelle verweist.
    c) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1, 2 und 3b die AWS-Konsole. Verwenden Sie für die Schritte 3a und 3c die NetScaler VPX-GUI oder die CLI.

Schritt 1. Erstellen Sie eine virtuelle private Cloud (VPC) von Amazon.

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Verfügbarkeitszonen mit der gleichen Anzahl von ENI (Netzwerkschnittstellen) bereit.

Weitere Informationen zum Erstellen einer VPC und Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Szenario: eigenständige Instanz

Schritt 3. Konfigurieren Sie die ADC-VIP-Adressen, indem Sie ein Subnetz auswählen, das sich nicht mit den Amazon VPC-Subnetzen überschneidet. Wenn Ihre VPC 192.168.0.0/16 ist, können Sie zur Konfiguration von ADC-VIP-Adressen ein beliebiges Subnetz aus diesen IP-Adressbereichen auswählen:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

In diesem Beispiel wurde das ausgewählte 10.10.10.0/24-Subnetz und VIPs in diesem Subnetz erstellt. Sie können ein beliebiges Subnetz außer dem VPC-Subnetz (192.168.0.0/16) wählen.

Schritt 4. Fügen Sie eine Route hinzu, die aus der VPC-Routentabelle auf die Client-Schnittstelle (VIP) des primären Knotens verweist.

Geben Sie in der AWS CLI den folgenden Befehl ein:

```
aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-block 10.10.10.0/24 --gateway-id <eni-client-primary>
```

Führen Sie in der AWS-GUI die folgenden Schritte aus, um eine Route hinzuzufügen:

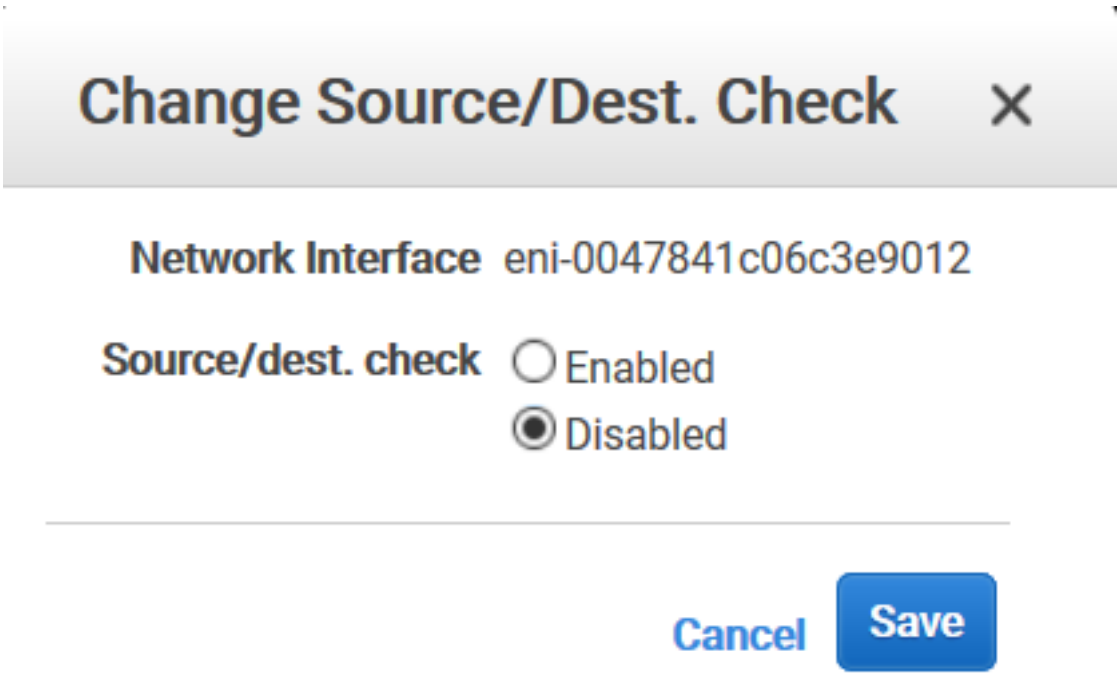
1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Route Tables**und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie **Aktionen**und klicken Sie auf **Routen bearbeiten**.

4. Um eine Route hinzuzufügen, wählen Sie **Route hinzufügen**. Geben Sie für **Destination**den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein. Wählen Sie für Gateway-ID das ENI einer Client-Schnittstelle des primären Knotens aus.

> **Hinweis:**
>
> Sie müssen **Source/Dest-Check** auf dem Client-ENI der primären Instanz deaktivieren.

Um die Quell-/Zielüberprüfung für eine Netzwerkschnittstelle mithilfe der Konsole zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Network Interfaces**aus.
3. Wählen Sie die Netzwerkschnittstelle einer primären Clientschnittstelle aus, wählen Sie **Aktionen**aus und klicken Sie auf Quelle/Dest **ändern. Überprüfe**.
4. Wählen Sie im Dialogfeld **Deaktiviert**und klicken Sie auf **Speichern**.



Schritt 5. Konfigurieren der Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   1    add ha node 1 \<sec\_ip\> -inc ENABLED
   ```

   Auf dem sekundären Knoten:

   ```
   1    add ha node 1 \<prim\_ip\> -inc ENABLED
   ```

   <sec_ip>bezieht sich auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   <prim_ip>bezieht sich auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu. Sie müssen es aus dem ausgewählten Subnetz hinzufügen, z. B. 10.10.10.0/24.

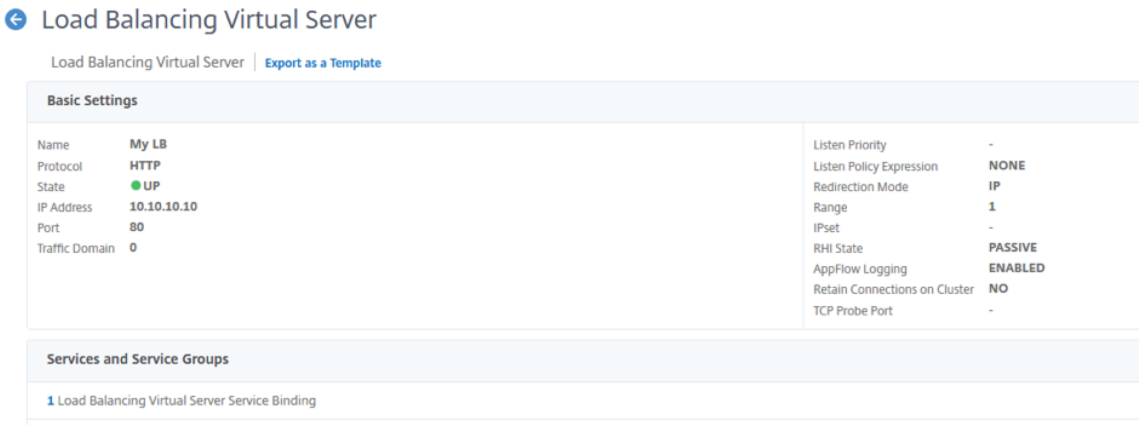
   Geben Sie den folgenden Befehl ein:

   ```
   1    add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
           primary\_vip\> \<port\>
   ```


Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich am primären Knoten mit Benutzername`nsroot` und Instanz-ID als Kennwort an.
3. Navigieren Sie zu **Konfiguration** > **System** > **Hochverfügbarkeit**und klicken Sie auf **Hinzufügen**.
4. Fügen Sie im Feld **Remote-Knoten-IP-Adresse** die private IP-Adresse der Management-NIC des sekundären Knotens hinzu.
5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .
6. Fügen Sie unter **Anmeldeinformationen des Remote-Systems** den Benutzernamen und das Kennwort für den sekundären Knoten hinzu, und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

   Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.



Bereitstellen eines VPX-HA-Paars mit privaten IP-Adressen mithilfe von AWS Shared VPC

In einem gemeinsam genutzten AWS-VPC-Modell teilt sich das Konto, dem die VPC (Eigentümer) gehört, ein oder mehrere Subnetze mit anderen Konten (Teilnehmern). Daher haben Sie ein VPC-Besitzerkonto und ein Teilnehmerkonto. Nachdem ein Subnetz freigegeben wurde, können die Teilnehmer ihre Anwendungsressourcen in den für sie freigegebenen Subnetzen anzeigen, erstellen, ändern und löschen. Teilnehmer können keine Ressourcen anzeigen, ändern oder löschen, die anderen Teilnehmern oder dem VPC-Besitzer gehören.

Informationen zu AWS Shared VPC finden Sie in der AWS-Dokumentation.

> **Hinweis:**
>
> Die Konfigurationsschritte für die Bereitstellung eines VPX-HA-Paars mit privaten IP-Adressen mithilfe der gemeinsam genutzten AWS-VPC sind dieselben wie bei Bereitstellen eines VPX-HA-Paars mit privaten IP-Adressen mithilfe der nicht gemeinsam genutzten AWS-VPC mit der folgenden Ausnahme:
>
> - Die Routing-Tabellen in der VPC, die auf die Clientschnittstelle verweisen, müssen aus dem *VPC-Besitzerkonto*hinzugefügt werden.

Voraussetzungen

- Stellen Sie sicher, dass die IAM-Rolle, die der NetScaler VPX-Instance im AWS-Teilnehmerkonto zugeordnet ist, über die folgenden IAM-Berechtigungen verfügt:

```
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    }
```

> **Hinweis:**
>
> Mit der **AssumeRole** kann die NetScaler VPX-Instanz die kontenübergreifende IAM-Rolle übernehmen, die vom VPC-Besitzerkonto erstellt wird.

- Stellen Sie sicher, dass das VPC-Besitzerkonto dem Teilnehmerkonto mithilfe der kontenübergreifenden IAM-Rolle die folgenden IAM-Berechtigungen bereitstellt:

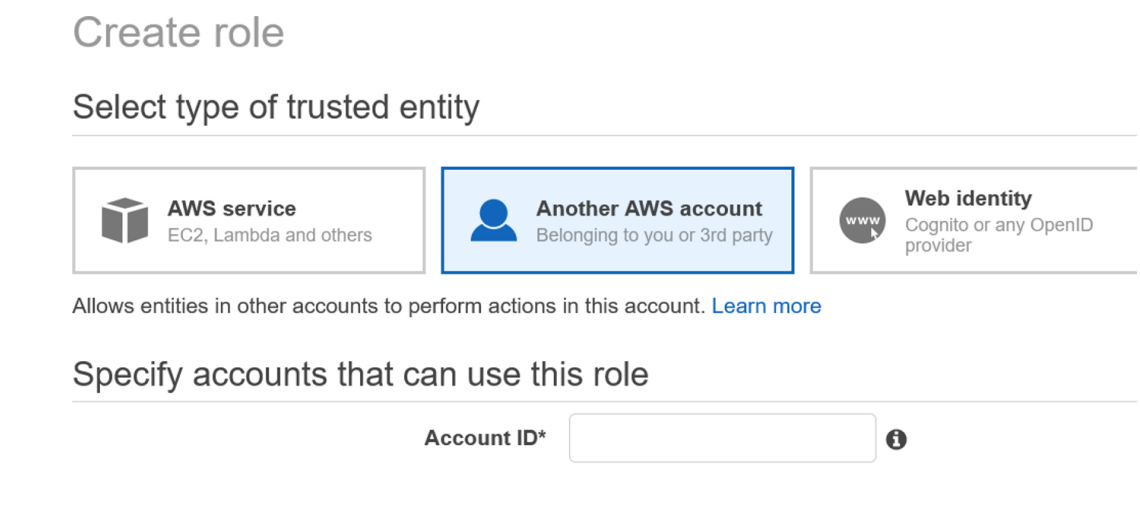
```
1    {
2
```



```
        "Version": "2012-10-17",
        "Statement": [
            {

                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "ec2:CreateRoute",
                    "ec2:DeleteRoute",
                    "ec2:DescribeRouteTables"
                ],
                "Resource": "*"
             }

        ]
    }
```

Erstellen einer kontenübergreifenden IAM-Rolle

1. Melden Sie sich bei der AWS-Webkonsole an.
2. Navigieren Sie auf der Registerkarte **IAM** zu **Roles**, und wählen Sie dann **Create Role**aus.
3. Wählen Sie **ein anderes AWS-Konto**.



4. Geben Sie die 12-stellige Konto-ID des Teilnehmerkontos ein, auf das Sie Administratorzugriff gewähren möchten.

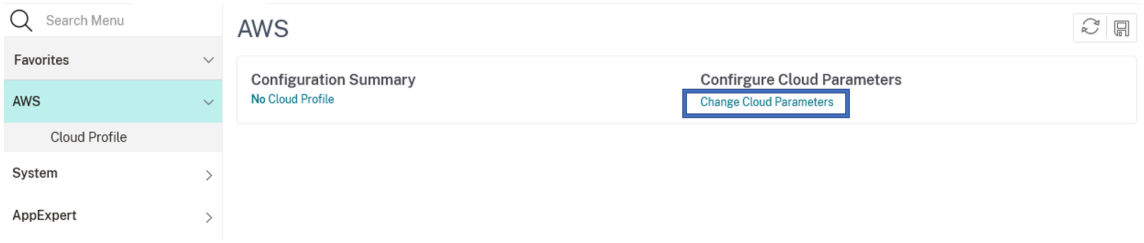
Festlegen der kontenübergreifenden IAM-Rolle mithilfe der NetScaler CLI

Mit dem folgenden Befehl kann die NetScaler VPX-Instanz die kontoübergreifende IAM-Rolle übernehmen, die im VPC-Besitzerkonto vorhanden ist.

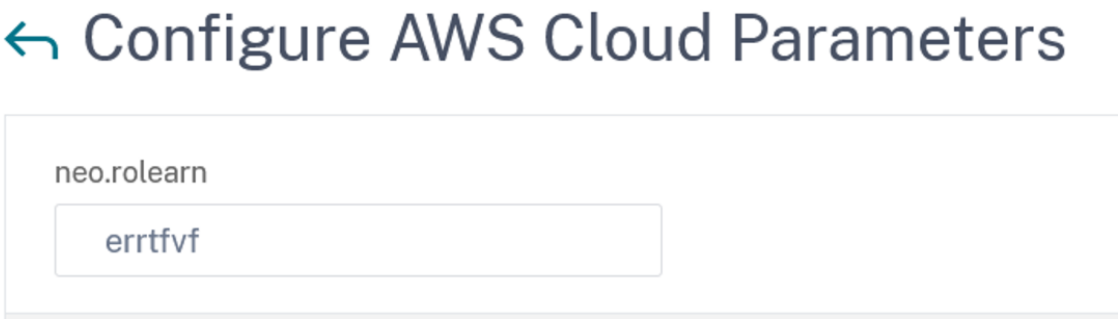

```
set cloud awsParam -roleARN <string>
```

Festlegen der kontenübergreifenden IAM-Rolle mithilfe der NetScaler GUI

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration > AWS > Cloud-Parameter ändern**.



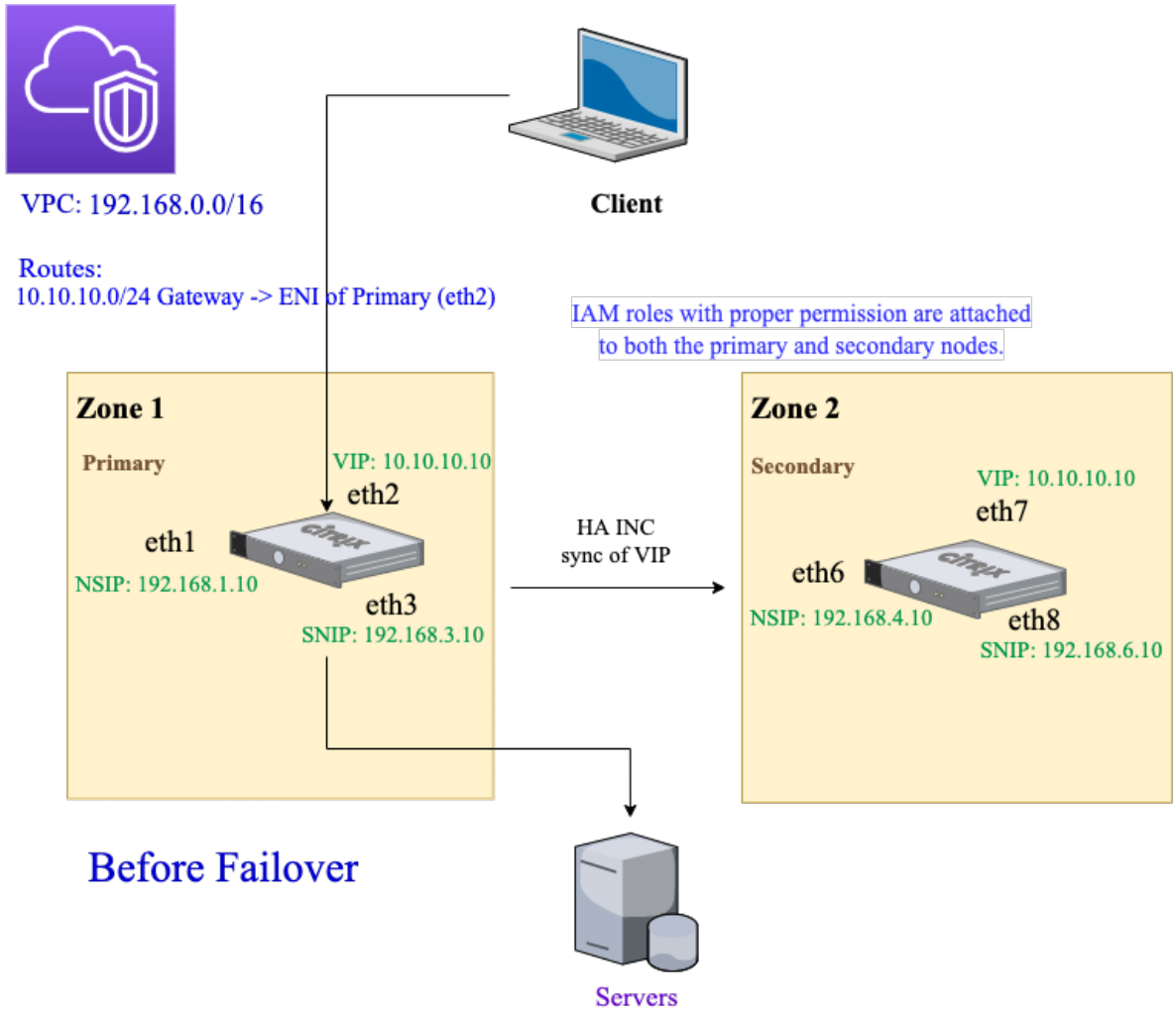
2. Geben Sie auf der Seite **AWS-Cloud-Parameter konfigurieren** den Wert für das Feld **RoleARN** ein.

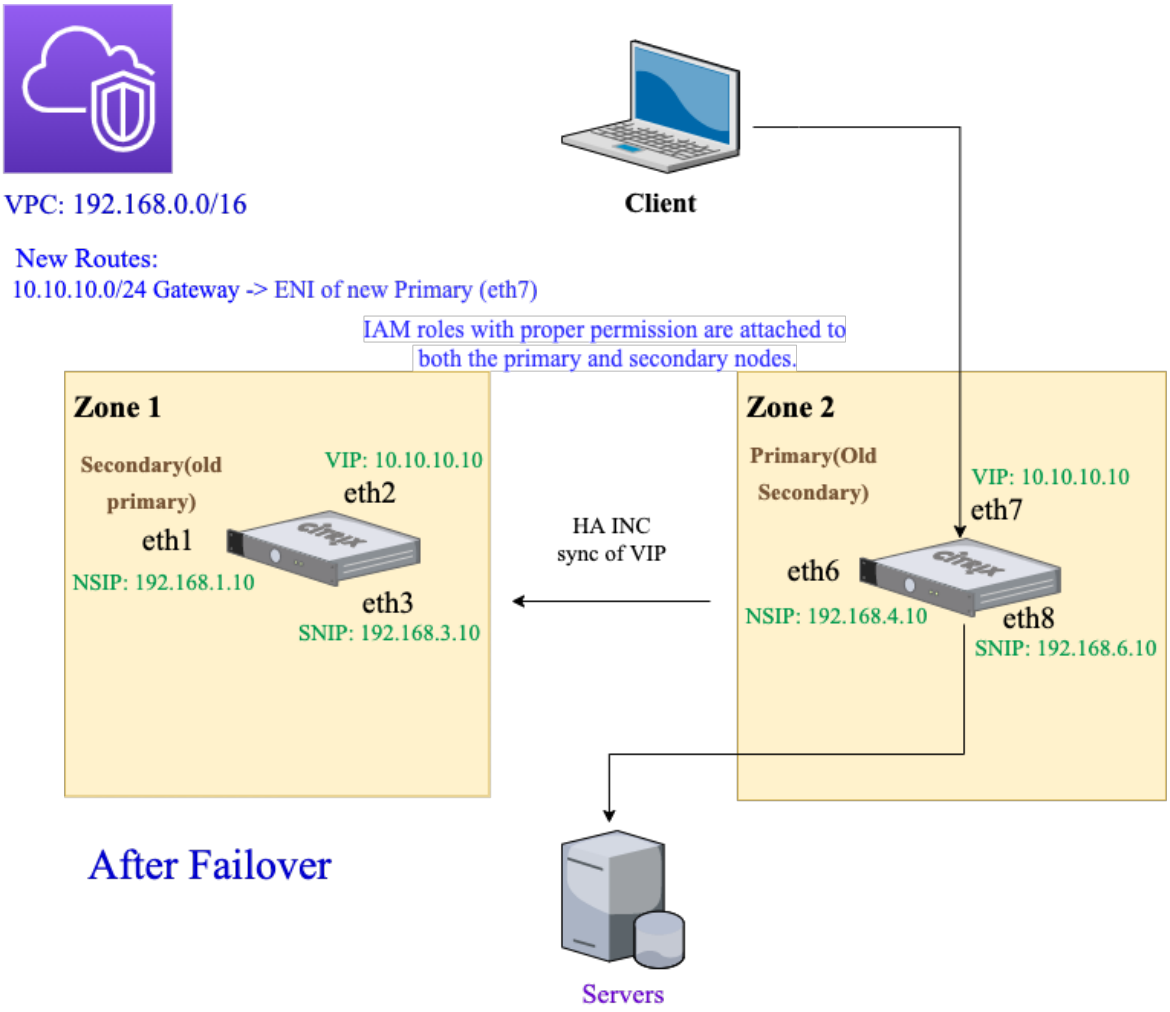


Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server.

Die folgenden Diagramme veranschaulichen das NetScaler VPX Hochverfügbarkeitssetup im INC-Modus auf AWS. Das benutzerdefinierte Subnetz 10.10.10.10, das nicht Teil der VPC ist, wird als VIP verwendet. Daher kann das Subnetz 10.10.10.10 über Availability Zones hinweg verwendet werden.





Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf dem primären Knoten:

   ```
   1    add ha node 1 192.168.4.10 -inc enabled
   ```

   Hier bezieht sich 192.168.4.10 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf dem sekundären Knoten:

   ```
   1    add ha node 1 192.168.1.10 -inc enabled
   ```

   Hier bezieht sich 192.168.1.10 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

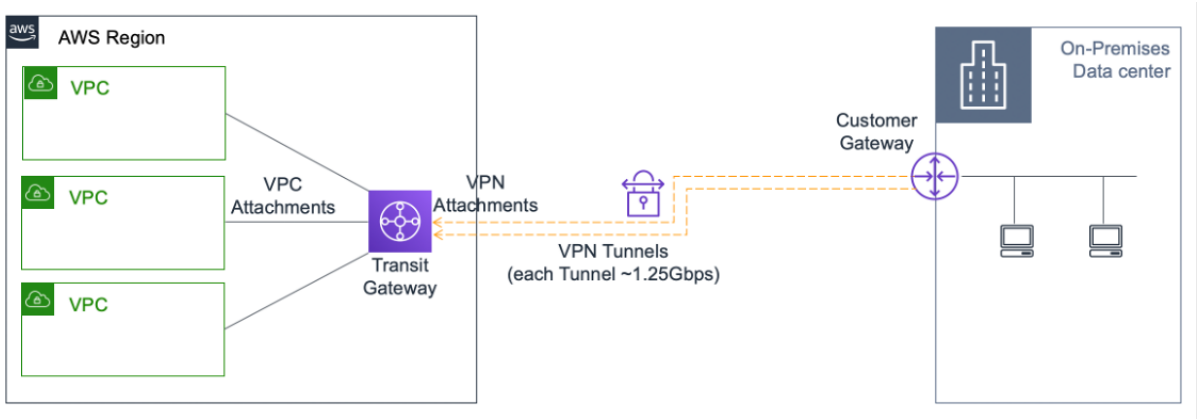
Geben Sie den folgenden Befehl ein:

```
1    add lbvserver vserver1 http 10.10.10.10 80
```

3. Speichern Sie die Konfiguration.
4. Nach einem erzwungenen Failover:
   - Die sekundäre Instanz wird zur neuen primären Instanz.
   - Die VPC-Route, die auf die primäre ENI zeigt, migriert zum sekundären Client-ENI.
   - Der Clientverkehr wird auf die neue primäre Instanz fortgesetzt.

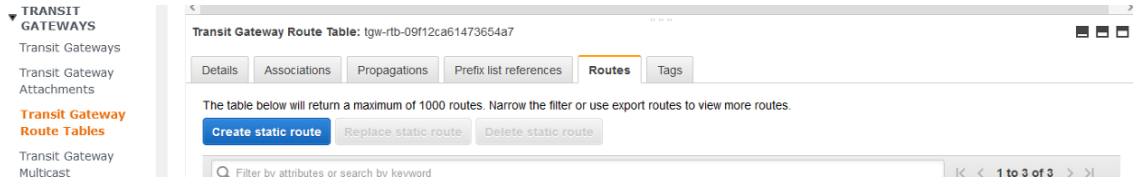
AWS Transit Gateway-Konfiguration für eine private HA-IP-Lösung

Sie benötigen AWS Transit Gateway, um das private VIP-Subnetz innerhalb des internen Netzwerks über AWS-VPCs, Regionen und lokale Netzwerke hinweg routbar zu machen. Die VPC muss eine Verbindung zu AWS Transit Gateway herstellen. Eine statische Route für das VIP-Subnetz oder den IP-Pool in der AWS Transit Gateway-Routingtabelle wird erstellt und auf die VPC gerichtet.

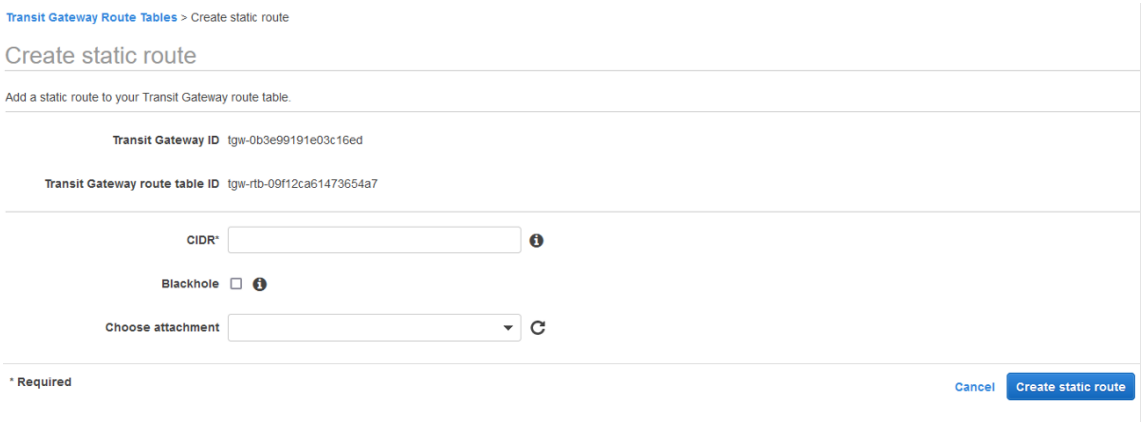


Gehen Sie folgendermaßen vor, um AWS Transit Gateway zu konfigurieren:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich **Transit Gateway Route Table** aus.
3. Wählen Sie die Registerkarte **Routen** und klicken Sie auf **Statische Route erstellen**.



4. Erstellen Sie eine statische Route, bei der CIDR auf Ihr privates VIPS-Subnetz und die Anschlusspunkte auf die VPC mit NetScaler VPX verweist.



5. Klicken Sie auf **Statische Route erstellen**und wählen Sie dann **Schließen**.

Problembehandlung

Wenn Sie bei der Konfiguration der privaten HA-IP-Lösung für Multizonen-HA auf Probleme stoßen, überprüfen Sie die folgenden wichtigen Punkte zur Fehlerbehebung:

- Sowohl der primäre als auch der sekundäre Knoten haben dieselben IAM-Berechtigungen.
- Der INC-Modus ist sowohl auf dem primären als auch auf dem sekundären Knoten aktiviert.
- Sowohl der primäre als auch der sekundäre Knoten haben die gleiche Anzahl von Schnittstellen.
- Folgen Sie beim Erstellen einer Instanz der gleichen Reihenfolge beim Anhängen von Schnittstellen auf primären und sekundären Knoten, basierend auf der Geräteindexnummer. Nehmen wir an, auf einem Primärknoten wird zuerst die Client-Schnittstelle und dann die Serverschnittstelle angehängt. Folgen Sie der gleichen Reihenfolge auch auf dem sekundären Knoten. Wenn es eine Diskrepanz gibt, trennen Sie die Schnittstellen und fügen Sie sie in der richtigen Reihenfolge wieder an.
- Sie können die Reihenfolge der Schnittstellen überprüfen, indem Sie diesem Navigationspfad folgen: **AWS-Konsole > Netzwerk und Sicherheit > ENI > Geräteindexnummer**. Standardmäßig sind diesen Schnittstellen die folgenden Geräteindexnummern zugewiesen: - Verwaltungsschnittstelle —0 - Client-Schnittstelle —1 - Serverschnittstelle —2
  - Verwaltungsschnittstelle –0
  - Client-Schnittstelle –1
  - Serverschnittstelle –2
- Wenn die Reihenfolge der Geräteindexnummern auf dem primären ENI wie folgt lautet: 0, 1, 2. Das sekundäre ENI muss ebenfalls derselben Reihenfolge der Geräteindexnummern folgen: 0, 1, 2.

Wenn die Reihenfolge der Geräteindexnummern nicht übereinstimmt, werden alle nicht übereinstimmenden Routen an den Index 0, die Verwaltungsschnittstelle, übertragen, um einen Verlust von Routen zu vermeiden. Sie müssen jedoch die Schnittstellen trennen und sie in der richtigen Reihenfolge wieder anhängen, um zu vermeiden, dass Routen zur Verwaltungsschnittstelle verschoben werden, da dies zu Verkehrsstaus führen kann.

- Wenn kein Verkehr fließt, vergewissern Sie sich, dass die "Source/dest. Check"ist auf der Client-Oberfläche des primären Knotens beim ersten Mal deaktiviert.
- Stellen Sie sicher, dass der Befehl `cloudhadaemon` (`ps -aux | grep cloudha`) in der Shell ausgeführt wird.
- Stellen Sie sicher, dass die NetScaler-Firmware-Version 13.0 Build 70.x oder höher ist.
- Bei Problemen mit dem Failover-Prozess überprüfen Sie die Protokolldatei unter: `/var/log/cloud-ha-daemon.log`

Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts

October 17, 2024

AWS Outposts ist ein Pool von AWS-Rechen- und Speicherkapazität, der an Ihrem Standort bereitgestellt wird. Outposts stellt AWS-Infrastruktur und -Services an Ihrem On-Premises-Standort bereit. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region. Sie können dieselben NetScaler VPX-Instanzen, AWS-APIs, Tools und Infrastrukturen on-premises und in der AWS-Cloud verwenden, um ein konsistentes Hybriderlebnis zu erzielen.

Sie können Subnetze auf Ihren Outposts erstellen und diese angeben, wenn Sie AWS-Ressourcen wie EC2-Instanzen, EBS-Volumes, ECS-Cluster und RDS-Instanzen erstellen. Instanzen in den Außenposten-Subnetzen kommunizieren mit anderen Instanzen in der AWS-Region über private IP-Adressen, alle innerhalb derselben Amazon Virtual Private Cloud (VPC).

Weitere Informationen finden Sie im Benutzerhandbuch für AWS Outposts.

Funktionsweise von AWS Outposts

AWS Outposts ist für den Betrieb mit einer ständigen und konsistenten Verbindung zwischen Ihren Outposts und einer AWS-Region konzipiert. Um diese Verbindung zur Region und zu den lokalen Workloads in Ihrer on-premises Umgebung herzustellen, müssen Sie Ihren Outpost mit Ihrem on-premises Netzwerk verbinden. Ihr on-premises Netzwerk muss einen WAN-Zugriff zurück zur Region und zum Internet bieten. Das Internet muss auch einen LAN- oder WAN-Zugriff auf das lokale Netzwerk bieten, in dem sich Ihre on-premises Workloads oder Anwendungen befinden.

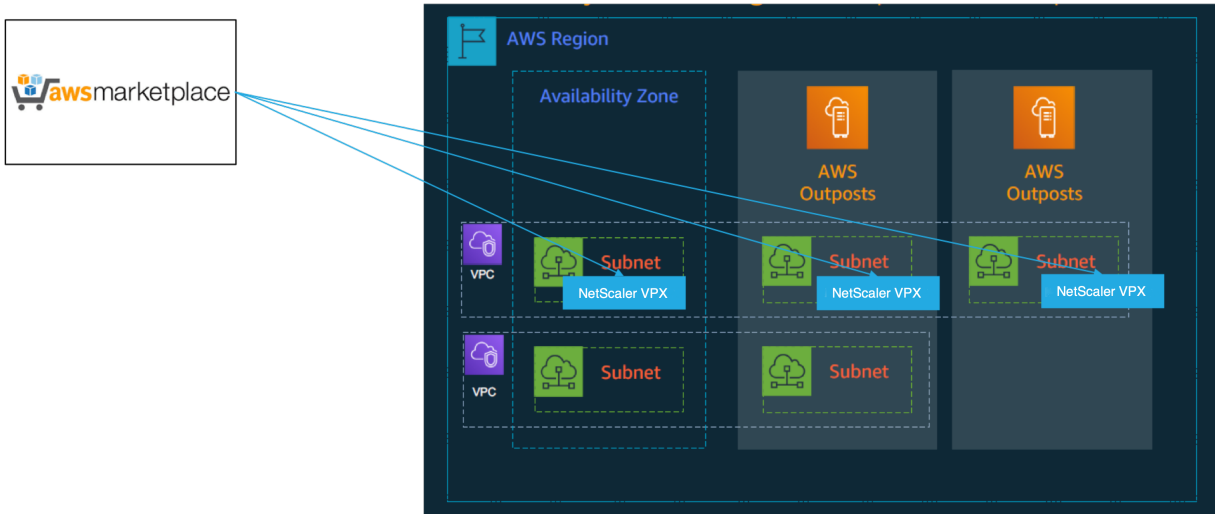
Voraussetzung

- Sie müssen einen AWS Outposts in Ihrer Site installieren.
- Die Rechen- und Speicherkapazität der AWS Outposts muss zur Nutzung verfügbar sein.

Weitere Informationen zum Aufgeben einer Bestellung für AWS Outposts finden Sie in der folgenden AWS-Dokumentation: https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

NetScaler VPX-Instanz auf AWS Outposts mit der AWS-Webkonsole bereitstellen

Die folgende Abbildung zeigt eine einfache Bereitstellung von NetScaler VPX-Instanzen auf den Outposts. Das im AWS Marketplace vorhandene NetScaler AMI wird auch in den Outposts bereitgestellt.



Melden Sie sich bei der AWS-Webkonsole an und führen Sie die folgenden Schritte aus, um NetScaler VPX EC2-Instances auf Ihren AWS-Outposts bereitzustellen.

1. Erstellen Sie ein Schlüsselpaar.
2. Erstellen Sie eine Virtual Private Cloud (VPC).
3. Fügen Sie weitere Subnetze hinzu.
4. Erstellen Sie Sicherheitsgruppen und Sicherheitsregeln.
5. Fügen Sie Routingtabellen hinzu.
6. Erstellen Sie ein Internet-Gateway.
7. Erstellen Sie eine NetScaler VPX-Instance mithilfe des AWS EC2-Service. Navigieren Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instanz > AWS Marketplace**.
8. Erstellen Sie mehr Netzwerkschnittstellen und fügen Sie sie hinzu.
9. Hängen Sie elastische IPs an die Management-NIC an.
10. Stellen Sie eine Verbindung mit der VPX-Instanz her.

Ausführliche Anweisungen zu den einzelnen Schritten finden Sie unter Stellen Sie mithilfe der AWS-Webkonsole eine NetScaler VPX-Instanz auf AWS bereit.

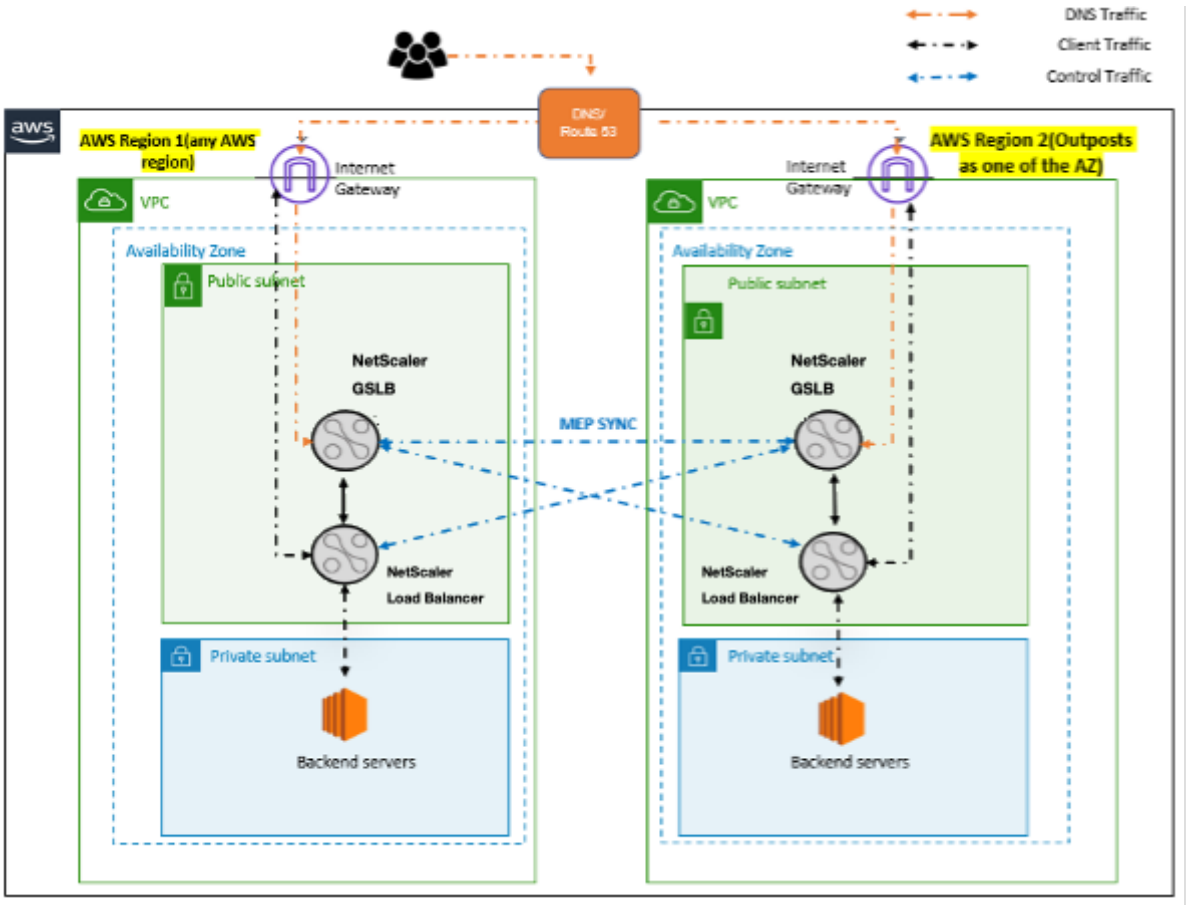
Informationen zur Hochverfügbarkeit innerhalb der Bereitstellung in derselben Verfügbarkeitszone finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.

Eine NetScaler VPX-Instanz in der Hybrid Cloud mit AWS Outposts bereitstellen

Sie können eine NetScaler VPX-Instanz in einer Hybrid Cloud in einer AWS-Umgebung bereitstellen, die AWS-Outposts enthält. Sie können den Mechanismus zur Bereitstellung von Apps mithilfe der NetScaler Global Server Load Balancing (GSLB) -Lösung vereinfachen. Die GSLB-Lösung verteilt den Anwendungsdatenverkehr auf mehrere Rechenzentren in Hybrid-Clouds, die auf der Grundlage der AWS-Regionen und der Infrastruktur von AWS Outpost erstellt wurden.

NetScaler GSLB unterstützt sowohl die aktiv-aktiven als auch die aktiv-passiven Bereitstellungstypen, um verschiedene Anwendungsfälle zu adressieren. Zusammen mit diesen flexiblen Bereitstellungsoptionen und Mechanismen zur Anwendungsbereitstellung sichert NetScaler das gesamte Netzwerk- und Anwendungsportfolio, unabhängig davon, ob Anwendungen nativ in der AWS Cloud oder in AWS Outposts bereitgestellt werden.

Das folgende Diagramm zeigt eine Anwendungsbereitstellung mit der NetScaler Appliance in der Hybrid Cloud mit AWS.



In einer aktiven und aktiven Bereitstellung steuert der NetScaler den Datenverkehr global über eine verteilte Umgebung. Alle Standorte in der Umgebung tauschen über das Metrics Exchange Protocol (MEP) Kennzahlen über ihre Verfügbarkeit und den Zustand der Ressourcen aus. Die NetScaler-Appliance verwendet diese Informationen, um den Datenverkehr zwischen den Standorten zu verteilen, und sendet Clientanforderungen an die am besten geeigneten GSLB-Site, die durch die in der GSLB-Konfiguration angegebene definierte Methode (Round Robin, kleinste Verbindung und statische Nähe) bestimmt wird.

Sie können das aktiv-aktive GSLB-Deployment verwenden, um:

- Optimieren Sie die Ressourcenauslastung, wenn alle Knoten aktiv sind.
- Verbessern Sie die Benutzererfahrung, indem Sie Anfragen an die Website weiterleiten, die jedem einzelnen Benutzer am nächsten ist.
- Migrieren Sie Anwendungen in einem benutzerdefinierten Tempo in die Cloud.

Sie können das aktiv-passive GSLB-Deployment verwenden für:

- Notfallwiederherstellung
- Cloudburst

Referenzen

- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- NetScaler VPX-Instanz auf AWS Outposts mit der AWS-Webkonsole bereitstellen
- Konfigurieren von GSLB auf NetScaler VPX-Instanzen

Schützen Sie das AWS API Gateway mithilfe der NetScaler Web App Firewall

October 17, 2024

Sie können eine NetScaler Appliance vor Ihrem AWS API Gateway bereitstellen und das API-Gateway vor externen Bedrohungen schützen. NetScaler Web App Firewall (WAF) kann Ihre API vor den 10 wichtigsten OWASP-Bedrohungen und Zero-Day-Angriffen schützen. NetScaler Web App Firewall verwendet eine einzige Codebasis für alle ADC-Formfaktoren. Daher können Sie Sicherheitsrichtlinien in jeder Umgebung konsequent anwenden und durchsetzen. NetScaler Web App Firewall ist einfach zu implementieren und als Einzellizenz erhältlich. Die NetScaler Web App Firewall bietet Ihnen die folgenden Funktionen:

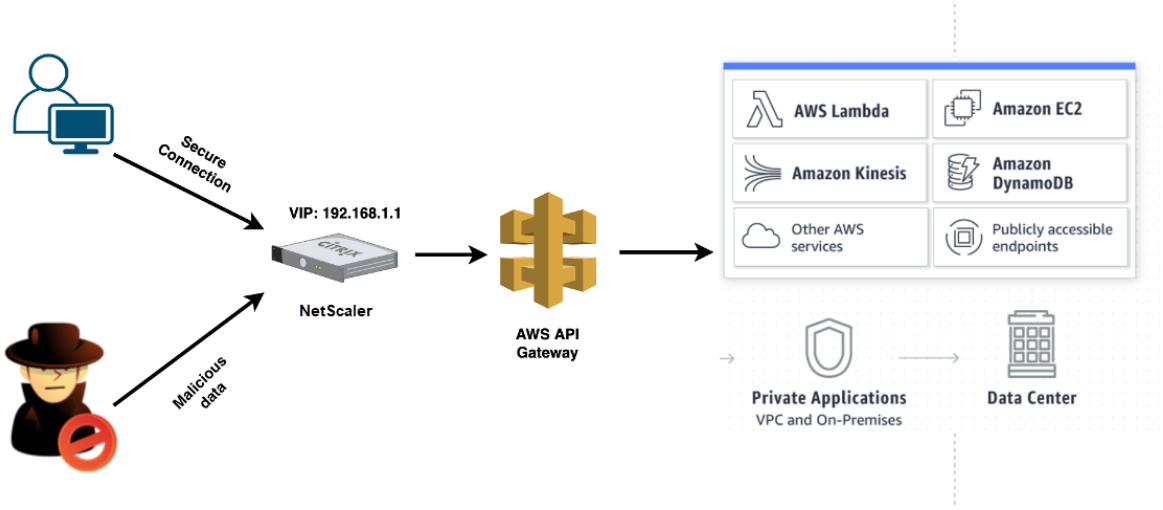
- Vereinfachte Konfiguration
- Bot-Verwaltung
- Ganzheitliche Sichtbarkeit
- Sammeln Sie Daten aus mehreren Quellen und zeigen Sie die Daten in einem einheitlichen Bildschirm an

Zusätzlich zum API-Gateway-Schutz können Sie auch die anderen NetScaler-Funktionen verwenden. Weitere Informationen finden Sie in der NetScaler-Dokumentation. Um Ausfallzeiten von Rechenzentren zu vermeiden und die Herunterfahrzeit zu minimieren, können Sie ADC in oder über Availability Zones hinweg in Hochverfügbarkeit versetzen. Sie können auch Clustering mit der Autoscale-Funktion verwenden oder konfigurieren.

Zuvor unterstützte AWS API Gateway den erforderlichen Schutz nicht, um die dahinter stehenden Anwendungen zu sichern. Ohne den Schutz der Web Application Firewall (WAF) waren APIs anfällig für Sicherheitsbedrohungen.

Stellen Sie die NetScaler Appliance vor dem AWS API-Gateway bereit

Im folgenden Beispiel wird eine NetScaler Appliance vor dem AWS-API-Gateway bereitgestellt.



Nehmen wir an, es gibt eine echte API-Anforderung für den AWS Lambda-Service. Diese Anforderung kann für jeden der API-Dienste gelten, wie in der Amazon API Gateway-Dokumentationerwähnt. Wie im vorhergehenden Diagramm gezeigt, ist der Verkehrsfluss wie folgt:

1. Der Client sendet eine Anfrage an die AWS Lambda-Funktion (XYZ). Diese Clientanforderung wird an den virtuellen NetScaler-Server (192.168.1.1) gesendet.
2. Der virtuelle Server prüft das Paket und prüft auf schädliche Inhalte.
3. Die NetScaler Appliance löst eine Rewrite-Richtlinie aus, um den Hostnamen und die URL in einer Clientanforderung zu ändern. Zum Beispiel möchten Sie `https://restapi.citrix.com/default/LamdaFunctionXYZ` zu `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ` ändern.
4. Die NetScaler Appliance leitet diese Anforderung an das AWS-API-Gateway weiter.
5. Das AWS API Gateway sendet die Anforderung weiter an den Lambda-Dienst und ruft die Lambda-Funktion "XYZ"auf.
6. Wenn ein Angreifer gleichzeitig eine API-Anfrage mit schädlichem Inhalt sendet, landet die böswillige Anfrage auf der NetScaler Appliance.
7. Die NetScaler Appliance untersucht die Pakete und verwirft die Pakete basierend auf der konfigurierten Aktion.

Konfigurieren der NetScaler Appliance mit aktivierter WAF

Führen Sie die folgenden Schritte aus, um WAF auf einer NetScaler Appliance zu aktivieren:

1. Fügen Sie einen Content Switching oder einen virtuellen Lastausgleichsserver hinzu. Nehmen wir an, die IP-Adresse des virtuellen Servers ist 192.168.1.1, was zu einem Domainnamen (restapi.citrix.com) aufgelöst wird.
2. Aktivieren Sie die WAF-Richtlinie auf dem virtuellen NetScaler-Server. Weitere Informationen finden Sie unter Konfigurieren der Web App Firewall.

3. Aktivieren Sie Rewrite-Richtlinie, um den Domainnamen zu ändern. Nehmen wir an, Sie möchten die eingehende Anforderung für den Load Balancer unter “restapi.citrix.com” -Domänennamen ändern, um in das Back-End-AWS-API-Gateway unter “citrix.execute-api”neu geschrieben zu werden.<region>.amazonaws”Domänenname.
4. Aktivieren Sie den L3-Modus auf der NetScaler Appliance, damit sie als Proxy fungiert. Verwenden Sie den folgenden Befehl:

```
enable ns mode L3
```

Nehmen wir in Schritt 3 des vorherigen Beispiels an, der Website-Administrator möchte, dass die NetScaler Appliance den Domänennamen “restapi.citrix.com”durch “citrix.execute-api”ersetzt.<region>.amazonaws.com”und die URL mit “Default/Lambda/XYZ”.

Das folgende Verfahren beschreibt, wie Sie den Hostnamen und die URL in einer Clientanforderung mithilfe der Rewrite-Funktion ändern:

1. Melden Sie sich mit SSH bei der NetScaler Appliance an.
2. Aktionen zum Umschreiben hinzufügen.

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

add rewrite action rewrite_url_act replace HTTP.REQ.URL.
    PATH_AND_QUERY "\"/default/lambda/XYZ\""
```

3. Fügen Sie Richtlinien zum Umschreiben für die Umschreibaktionen hinzu.

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

add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER(\"Host\").
    CONTAINS(\"restapi.citrix.com\") "rewrite_url_act
```

4. Binden Sie die Umschreibungsrichtlinien an einen virtuellen Server.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol
    -priority 10 -gotoPriorityExpression 20 -type REQUEST

bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
    priority 20 -gotoPriorityExpression END -type REQUEST
```

Weitere Informationen finden Sie unter Konfigurieren des Umschreibens, um den Hostnamen und die URL in der Clientanforderung auf der NetScaler Appliance zu ändern.

NetScaler Funktionen und Funktionen

Die NetScaler Appliance kann neben der Sicherung der Bereitstellung auch die Anforderung basierend auf den Benutzeranforderungen verbessern. Die NetScaler Appliance bietet die folgenden Hauptfunktionen.

- **Lastausgleich für das API-Gateway:** Wenn Sie über mehr als ein API-Gateway verfügen, können Sie mithilfe der NetScaler Appliance mehrere API-Gateways ausgleichen und das Verhalten der API-Anforderung definieren.
  - Es sind verschiedene Lastausgleichsmethoden verfügbar. Beispielsweise verhindert die Methode Least Connection eine Überlastung des API-Gateway-Limits, die benutzerdefinierte Lademethode behält eine bestimmte Last auf einem bestimmten API-Gateway bei und so weiter. Weitere Informationen finden Sie unter Lastausgleichsalgorithmen.
  - SSL-Offloading ist konfiguriert, ohne den Verkehr zu unterbrechen.
  - Der Modus Quell-IP (USIP) verwenden ist aktiviert, um die Client-IP-Adresse beizubehalten.
  - Benutzerdefinierte SSL-Einstellungen: Sie können Ihren eigenen virtuellen SSL-Server mit Ihren eigenen signierten Zertifikaten und Algorithmen haben.
  - Virtueller Backup-Server: Wenn das API-Gateway nicht erreichbar ist, können Sie die Anforderung für weitere Aktionen an einen virtuellen Sicherungsserver senden.
  - Viele andere Lastausgleichsfunktionen sind verfügbar. Weitere Informationen finden Sie unter Lastausgleich des Datenverkehrs auf einer NetScaler Appliance.
- **Authentifizierung, Autorisierung und Überwachung:** Sie können Ihre eigenen Authentifizierungsmethoden wie LDAP, SAML, RADIUS definieren und die API-Anforderungen autorisieren und überwachen.
- **Responder:** Sie können API-Anforderungen während des Herunterfahrens an ein anderes API-Gateway umleiten.
- **Ratenbegrenzung:** Sie können die Ratenbegrenzungsfunktion konfigurieren, um eine Überlastung eines API-Gateways zu vermeiden.
- **Bessere Verfügbarkeit:** Sie können eine NetScaler Appliance in einem Hochverfügbarkeits-Setup oder einem Cluster-Setup konfigurieren, um Ihren AWS-API-Datenverkehr besser verfügbar zu machen.
- **REST-API:** Unterstützt die REST-API, die zur Automatisierung der Arbeit in Cloud-Produktionsumgebungen verwendet werden kann.
- **Daten überwachen:** Überwacht und protokolliert die Daten als Referenz.

Die NetScaler Appliance bietet viel mehr Funktionen, die in das AWS-API-Gateway integriert werden können. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

Fügen Sie den Back-End-Dienst AWS Autoscaling hinzu

October 17, 2024

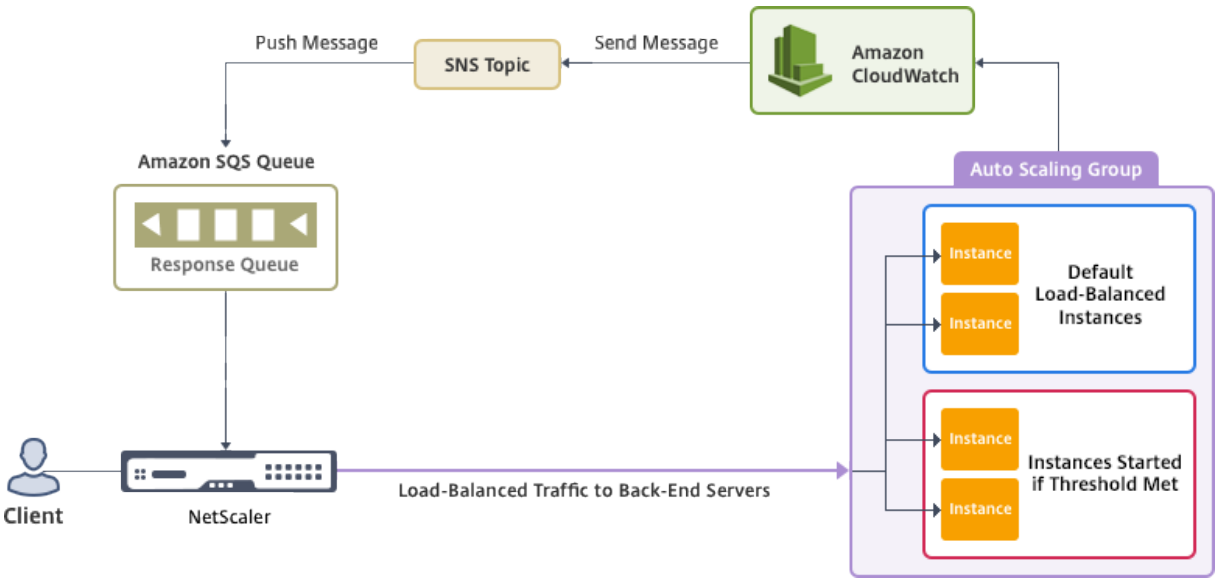
Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Wenn die Nachfrage nachlässt, müssen Sie die Ressourcen herunterskalieren, um unnötige Kosten ungenutzter Ressourcen zu vermeiden. Sie können die Kosten für die Ausführung der Anwendungen minimieren, indem Sie zu einem bestimmten Zeitpunkt nur so viele Instanzen bereitstellen, wie erforderlich sind. Um dies zu erreichen, müssen Sie den Verkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die NetScaler VPX-Instanz ist in den AWS Auto Scaling-Service integriert und bietet folgende Vorteile:

- **Lastverteilung und Verwaltung**: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch Autoscale-Gruppen im Back-End-Subnetz und ermöglicht es einem Benutzer, die Autoscale-Gruppen auszuwählen, um die Last auszugleichen. All dies erfolgt durch die automatische Konfiguration der virtuellen IP-Adressen und der Subnetz-IP-Adressen auf der VPX-Instanz.
- **Hochverfügbarkeit**: Erkennt Autoscale-Gruppen, die sich über mehrere Availability Zones erstrecken, und verteilt die Serverlast.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Backend-Server auf verschiedenen VPCs mithilfe von VPC-Peering
  - Backend-Server auf denselben Platzierungsgruppen
  - Backend-Server in verschiedenen Verfügbarkeitszonen
- **Sorgfältiger Verbindungsabbruch: Mithilfe der Funktion Graceful**Timeout werden Autoscale-Server ordnungsgemäß entfernt und so der Verlust von Client-Verbindungen vermieden, wenn eine Scale-Down-Aktivität auftritt.
- **Verbindungsverlust für Standby-Server**: Verhindert das Senden neuer Client-Verbindungen an den Server im Standby-Status. Die Standby-Server sind jedoch immer noch Teil der Autoscaling-Gruppe und verarbeiten weiterhin die vorhandenen Client-Verbindungen, bis sie geschlossen werden. Wenn der Server wieder in den Status InService wechselt, verarbeitet

der Server wieder neue Verbindungen. Sie können den Standby-Status verwenden, um Server zu aktualisieren, zu ändern oder Fehler zu beheben oder um sie je nach Anforderung herunterzuskalieren. Weitere Informationen finden Sie in der AWS-Dokumentation.

Diagramm: AWS Autoscaling-Service mit einer NetScaler VPX-Instanz



Dieses Diagramm zeigt, wie der AWS Autoscaling-Service mit einer NetScaler VPX-Instanz (virtueller Lastausgleichsserver) kompatibel ist. Weitere Informationen finden Sie in den folgenden AWS-Themen.

- Gruppen automatisch skalieren
- Cloud-Uhr
- Einfacher Benachrichtigungsdienst (SNS)
- Einfacher Warteschlangendienst (Amazon SQS)

Voraussetzungen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

- Lesen Sie die folgenden Themen:
  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien
- Erstellen Sie eine NetScaler VPX-Instanz auf AWS entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer eigenständigen NetScaler VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Szenario: eigenständige Instanz

- Weitere Informationen zum Bereitstellen von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.

> **Hinweis:**
>
> Wir empfehlen Folgendes:
>
> - Verwenden Sie die CloudFormation-Vorlage, um NetScaler VPX-Instanzen auf AWS zu erstellen.
> - Erstellen Sie drei separate Schnittstellen: eine für die Verwaltung (NSIP), eine für den clientseitigen virtuellen LB-Server (VIP) und eine für Subnetz-IP (NSIP).

- Erstellen Sie eine AWS Autoscale-Gruppe. Wenn Sie keine bestehende Autoscaling-Konfiguration haben, müssen Sie:

  1. Eine Startkonfiguration erstellen
  2. Eine Autoscaling-Gruppe erstellen
  3. Überprüfen Sie die Autoscaling-Gruppe

  Weitere Informationen finden Sie unter http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

- Ab NetScaler-Version 14.1-12.x müssen Sie in einer AWS Autoscale-Gruppe nur dann eine Scale-Down-Richtlinie angeben, wenn Sie die Option Graceful aktiviert haben. In NetScaler-Versionen vor 14.1-12.x mussten Sie mindestens eine Scale-Down-Richtlinie angeben, unabhängig davon, ob die Option „Graceful“aktiviert ist oder nicht.

  Die NetScaler VPX-Instanz unterstützt nur die Step Scaling-Richtlinie. Die einfache Skalierungsrichtlinie und die Skalierungsrichtlinie für die Zielverfolgung werden für die Autoscale-Gruppe nicht unterstützt.

- Stellen Sie sicher, dass Ihr AWS-Konto über die folgenden IAM-Berechtigungen verfügt:

```
{

    "Version": "2012-10-17",
    "Statement": \[
     {

            "Action": \[
                "ec2:DescribeInstances",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DetachNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "autoscaling:\*",
                "sns:\*",
```



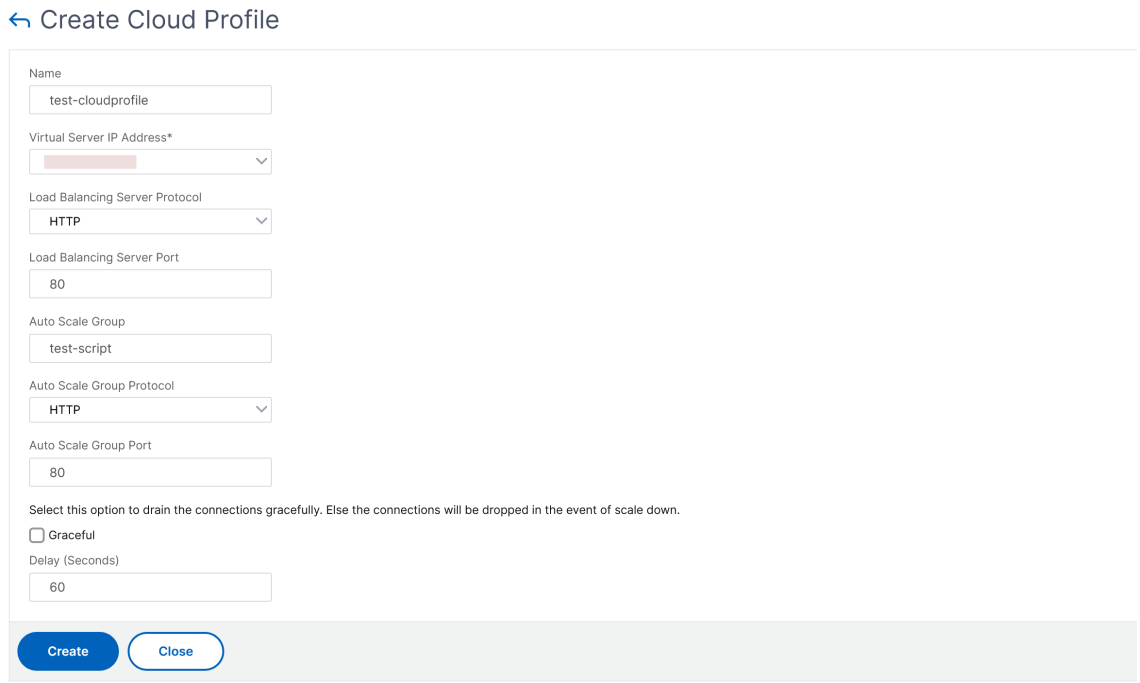
```
17                    "sqs:\*"
18
19                 “ iam: SimulatePrincipalPolicy ”
20                 “ iam: GetRole ”
21                \],
22                "Resource": "\*",
23                "Effect": "Allow"
24             }
25
26         \]
27     }
```

Fügen Sie den AWS Autoscaling-Service zu einer NetScaler VPX-Instance hinzu

Gehen Sie wie folgt vor, um den Autoscaling-Dienst zu einer VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für `nsroot`bei der VPX-Instanz an.
2. Navigieren Sie zu **System > AWS > Cloud-Profil** und klicken Sie auf **Hinzufügen**.

   Die Konfigurationsseite „ **Cloud-Profil erstellen** “wird angezeigt.



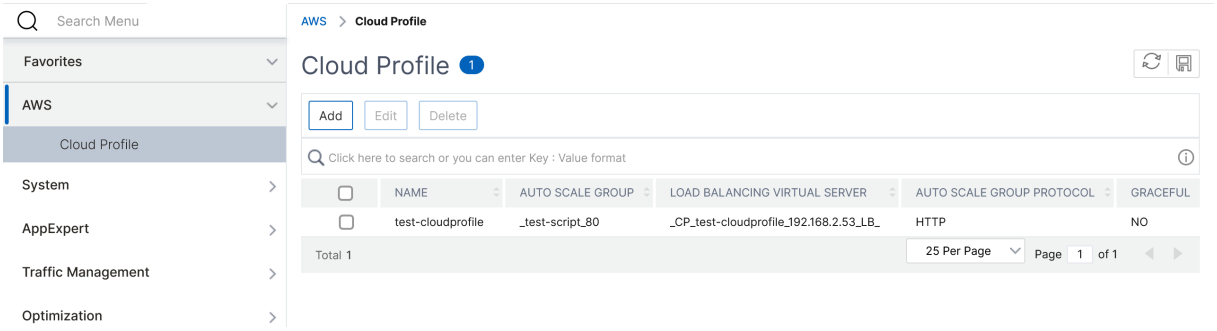
Punkte, die Sie bei der Erstellung eines Cloud-Profils beachten sollten:

- Die IP-Adresse des virtuellen Servers wird automatisch anhand der freien IP-Adresse aufgefüllt, die der VPX-Instanz zur Verfügung steht. Weitere Informationen finden Sie unter Mehrere IP-Adressen verwalten.

- Geben Sie den genauen Namen der Autoscale-Gruppe ein, die Sie in Ihrem AWS-Konto konfiguriert haben. Weitere Informationen finden Sie unter AWS Auto Scaling-Gruppen.
- Stellen Sie bei der Auswahl des Autoscaling-Gruppenprotokolls und -ports sicher, dass Ihre Server diese Protokolle und Ports überwachen, und dass Sie den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Für Autoscaling vom SSL-Protokolltyp scheint der virtuelle Lastausgleichsserver oder die Dienstgruppe nach dem Erstellen des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen zu sein. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.
- Wählen Sie **Graceful** aus und geben Sie im Feld **Delay** einen Timeout-Wert an, um die Autoscale-Server ordnungsgemäß zu entfernen. Diese Option leitet ein Scale-Down-Ereignis ein. Die VPX-Instanz entfernt den Server nicht sofort, sondern markiert einen der Server für das geordnete Löschen. Während dieses Zeitraums erlaubt die VPX-Instanz keine neuen Verbindungen zu diesem Server. Bestehende Verbindungen werden bedient, bis das Timeout eintritt. Nach dem Timeout entfernt die VPX-Instanz den Server.

  Wenn Sie die Option **Graceful** nicht auswählen, wird der Server in der Autoscale-Gruppe sofort entfernt, nachdem die Last gesunken ist. Dies kann zu Dienstunterbrechungen für die vorhandenen verbundenen Clients führen.

Nachdem Sie das Cloud-Profil erstellt haben, werden ein virtueller NetScaler-Load-Balancing-Server und eine Dienstgruppe mit Mitgliedern als Server der Autoscaling-Gruppe erstellt. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.



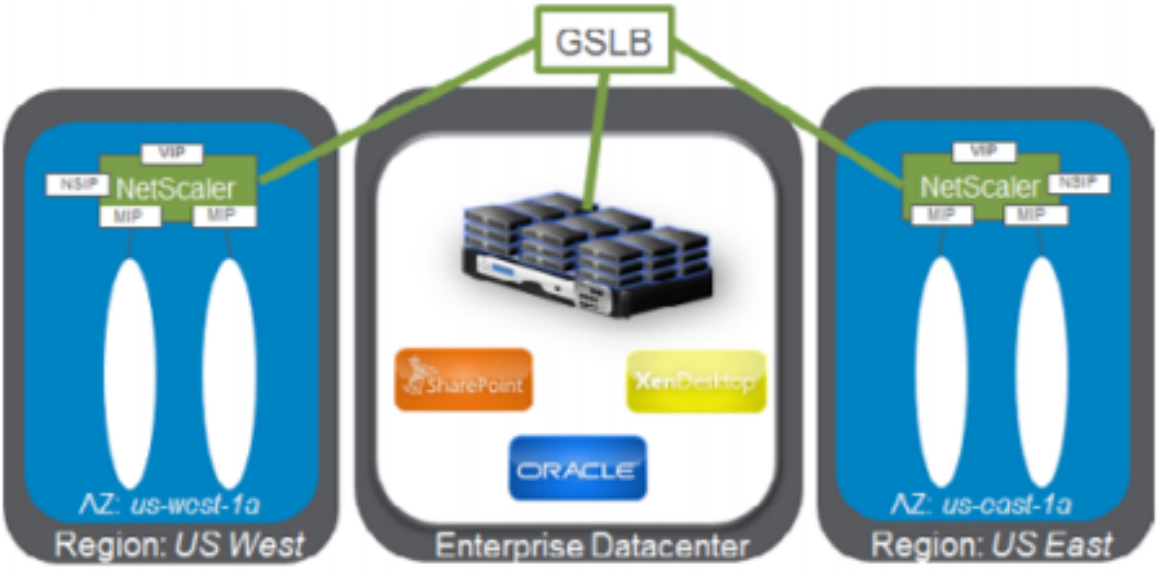
Hinweis:

- Informationen zu AutoScale finden Sie in der AWS-Konsole unter **EC2** > **Dashboard** > **Auto Scaling** > **Auto Scaling Group**.
- Sie können verschiedene Cloud-Profile für verschiedene Dienste (mit unterschiedlichen Ports) mit derselben Autoscaling-Gruppe (ASG) in AWS erstellen. Daher unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

NetScaler GSLB auf AWS bereitstellen

October 17, 2024

Das Einrichten von GSLB für NetScaler auf AWS besteht im Wesentlichen aus der Konfiguration von NetScaler für den Lastausgleich des Datenverkehrs zu Servern außerhalb der VPC, zu der NetScaler gehört, z. B. innerhalb einer anderen VPC in einer anderen Verfügbarkeitsregion oder einem on-premises Rechenzentrum.



DBS-Übersicht

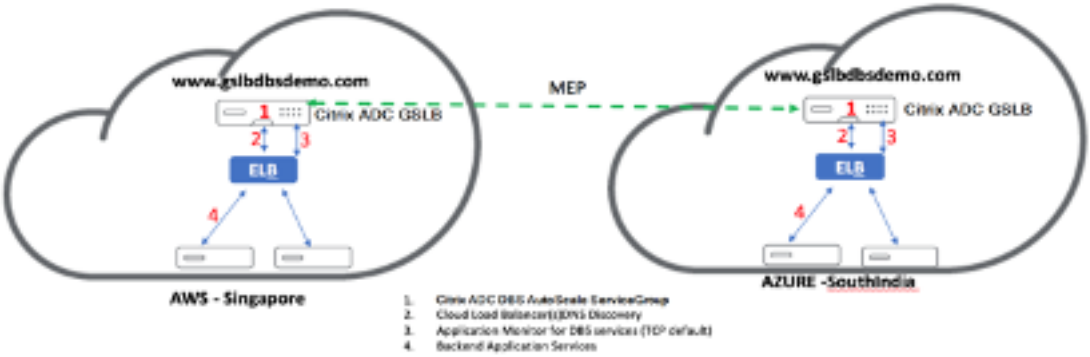
NetScaler GSLB-Unterstützung mithilfe von Domain-Name Based Services (DBS) für Cloud Load Balancer ermöglicht die automatische Erkennung dynamischer Cloud-Dienste mithilfe einer Cloud Load Balancer-Lösung. Diese Konfiguration ermöglicht es NetScaler, Global Server Load Balancing Domain-Name Based Services (GSLB DBS) in einer Active-Active-Umgebung zu implementieren. DBS ermöglicht die Skalierung von Back-End-Ressourcen in AWS-Umgebungen ab der DNS-Erkennung.

Dieser Abschnitt behandelt Integrationen zwischen NetScaler in AWS AutoScaling-Umgebungen. Im letzten Abschnitt des Dokuments wird die Möglichkeit beschrieben, ein HA-Paar von NetScaler ADCs einzurichten, die sich über zwei verschiedene Availability Zones (AZs) erstrecken, die für eine AWS-Region spezifisch sind.

DBS mit ELB

GSLB DBS verwendet den FQDN des Benutzers Elastic Load Balancer (ELB), um die GSLB-Servicegruppen dynamisch zu aktualisieren, sodass sie die Backend-Server enthalten, die in AWS erstellt und gelöscht werden. Die Back-End-Server oder -Instanzen in AWS können so konfiguriert werden, dass sie je nach Netzwerkbedarf oder CPU-Auslastung skaliert werden. Um diese Funktion zu konfigurieren, verweisen Sie NetScaler auf den ELB, um dynamisch an verschiedene Server in AWS weiterzuleiten, ohne NetScaler jedes Mal manuell aktualisieren zu müssen, wenn eine Instanz in AWS erstellt und gelöscht wird. Die NetScaler DBS-Funktion für GSLB-Dienstgruppen verwendet die DNS-basierte Diensterkennung, um die Mitgliedsdienstressourcen des in der Autoscale-Gruppe identifizierten DBS-Namespace zu bestimmen.

NetScaler GSLB DBS Autoscale-Komponenten mit Cloud Load Balancern:



AWS-Komponenten konfigurieren

Sicherheitsgruppen

> **Hinweis:**
>
> Wir empfehlen Ihnen, verschiedene Sicherheitsgruppen für ELB, NetScaler GSLB-Instanz und Linux-Instanz zu erstellen, da die für jede dieser Entitäten erforderlichen Regeln unterschiedlich sind. Dieses Beispiel verfügt über eine konsolidierte Sicherheitsgruppenkonfiguration zur Kürze.

Um die ordnungsgemäße Konfiguration der virtuellen Firewall sicherzustellen, siehe Sicherheitsgruppen für Ihr VPC.

1. Melden Sie sich bei der**AWS-Benutzergruppe**an und navigieren Sie zu**EC2 > NETWORK & SECURITY > Security Groups**.
2. Klicken Sie auf**Sicherheitsgruppe erstellen** und geben Sie einen Namen und eine Beschreibung ein. Diese Sicherheitsgruppe umfasst NetScaler- und Linux-Back-End-Webserver.
3. Fügen Sie die Regeln für eingehende Port aus dem folgenden Screenshot hinzu.

> **Hinweis:**
>
> Die Beschränkung des Quell-IP-Zugriffs wird für die granulare Härtung empfohlen. Weitere Informationen finden Sie unter Webserverregeln.

1. Amazon Linux-Backend-Webservices

    a) Melden Sie sich bei der**AWS-Benutzergruppe**an und navigieren Sie zu**EC2 > Instanzen**.

    b) Klicken Sie auf **Launch Instance** und konfigurieren Sie die**Amazon Linux-Instanz** mit den folgenden Details.

    Geben Sie die Details zum Einrichten eines Webservers oder Back-End-Dienstes für diese Instanz ein.

2. NetScaler-Konfiguration

    a) Melden Sie sich bei der**AWS-Benutzergruppe**an und navigieren Sie zu**EC2 > Instanzen**.

    b) Klicken Sie auf **Launch Instance** und konfigurieren Sie die **Amazon AMI-Instanz** anhand der folgenden Details.

3. Elastic IP-Konfiguration

> **Hinweis:**
>
> NetScaler kann bei Bedarf auch mit einer einzigen elastischen IP ausgeführt werden, um die Kosten zu senken, indem keine öffentliche IP für das NSIP vorhanden ist. Fügen Sie stattdessen dem SNIP eine elastische IP hinzu, die den Verwaltungszugriff auf die Box zusätzlich zur GSLB-Site-IP und ADNS-IP abdecken kann.

```
1. Melden Sie sich bei der**AWS-Benutzergruppe**an und navigieren Sie zu**EC2 > NETWORK & SECURITY > Elastic IPs**.

1. Klicken Sie auf**Neue Adresse**zuweisen, um eine elastische IP-Adresse zu erstellen.

1. Konfigurieren Sie die Elastic IP so, dass sie auf den Benutzer verweist, der die NetScaler-Instanz in AWS ausführt.

1. Konfigurieren Sie eine zweite Elastic IP und verweisen Sie sie erneut auf den Benutzer, der die NetScaler-Instanz ausführt.
```

1. Elastic Load Balancer

    a) Melden Sie sich bei der **AWS-Benutzergruppe**an und navigieren Sie zu**EC2 > LOAD BALANCING > Load Balancer**.

    b) Klicken Sie auf**Load Balancer erstellen**, um einen klassischen Load Balancer zu konfigurieren.

Die Benutzer Elastic Load Balancers ermöglichen Benutzern den Lastenausgleich ihrer Amazon Linux-Back-End-Instanzen und können gleichzeitig andere Instanzen ausgleichen, die je nach Bedarf hochgefahren werden.

Konfiguration von domänennamenbasierten Diensten für globalen Serverlastenausgleich

Informationen zu Verkehrsmanagementkonfigurationen finden Sie unter Konfigurieren des domänenbasierten NetScaler GSLB-Dienstes.

Bereitstellungstypen

Bereitstellung mit drei NICs

- Typische Bereitstellungen
  - GSLB StyleBook
  - Mit ADM
  - Mit GSLB (Route53 mit Domainregistrierung)
  - Lizenzierung - gepoolt/Marketplace
- Anwendungsfälle
  - Um eine echte Isolierung des Daten- und Verwaltungsverkehrs zu erreichen, werden Bereitstellungen mit drei NICs verwendet.
  - Bereitstellungen mit drei NICs verbessern außerdem die Skalierbarkeit und Leistung des ADC.
  - Bereitstellungen mit drei Netzwerkkarten werden in Netzwerkanwendungen verwendet, bei denen der Durchsatz typischerweise 1 Gbit/s oder mehr beträgt und eine Bereitstellung mit drei Netzwerkkarten empfohlen wird.

CFT-Einsatz

Kunden würden mithilfe von CloudFormation-Vorlagen bereitstellen, wenn sie ihre Bereitstellungen anpassen oder ihre Bereitstellungen automatisieren.

Bereitstellungsschritte

Im Folgenden sind die Bereitstellungsschritte aufgeführt:

1. Bereitstellung mit drei NICs für GSLB
2. Lizenzierung
3. bereitstellungsoption

Bereitstellung mit drei NICs für GSLB Die NetScaler VPX-Instanz ist als Amazon Machine Image (AMI) auf dem AWS-Marktplatz verfügbar und kann als Elastic Compute Cloud (EC2)-Instanz innerhalb einer AWS-VPC gestartet werden. Der EC2-Instanz-Typ, der als unterstütztes AMI auf NetScaler VPX mindestens zulässig ist, ist m4.large. Die NetScaler VPX AMI-Instanz benötigt mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine EC2-Instanz, die in einer AWS VPC gestartet wird, kann auch die für die VPX-Konfiguration erforderlichen Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen. Jede VPX-Instanz benötigt mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Back-End-Subnetz (SNIP)

NetScaler empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz auf einer AWS-Installation.

AWS stellt derzeit Multi-IP-Funktionen nur für Instanzen zur Verfügung, die in einer AWS VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastausgleich von Servern verwendet werden, die in EC2-Instanzen ausgeführt werden. Mit einer Amazon VPC können Benutzer eine virtuelle Netzwerkumgebung erstellen und steuern, einschließlich ihres eigenen IP-Adressbereichs, Subnetzen, Routing-Tabellen und Netzwerk-Gateways.

> **Hinweis:**
>
> Standardmäßig können Benutzer bis zu 5 VPC-Instanzen pro AWS-Region für jedes AWS-Konto erstellen. Benutzer können höhere VPC-Limits beantragen, indem sie das Antragsformular von Amazon hier einreichen: Amazon VPC-Anfrage.

Lizenzierung Für eine NetScaler VPX-Instanz auf AWS ist eine Lizenz erforderlich. Die folgenden Lizenzoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf AWS ausgeführt werden:

- Kostenlos (unbegrenzt)
- Stündlich
- jährlich
- Eigene Lizenz

- Kostenlose Testversion (alle NetScaler VPX-AWS-Abonnementangebote für 21 Tage kostenlos auf dem AWS-Marktplatz).

Bereitstellungsoption Benutzer können eine eigenständige NetScaler VPX-Instanz auf AWS bereitstellen. Weitere Informationen finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

Globaler Server-Load-Balancing von NetScaler für Hybrid- und Multi-Cloud-Bereitstellungen

Die NetScaler Hybrid- und Multi-Cloud-Lösung Global Server Load Balancing (GSLB) ermöglicht es Benutzern, den Anwendungsdatenverkehr auf mehrere Rechenzentren in Hybrid-Clouds, mehreren Clouds und on-premises Bereitstellungen zu verteilen. Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung hilft Benutzern, ihr Load Balancing-Setup in Hybrid- oder Multi-Cloud-Umgebungen zu verwalten, ohne das bestehende Setup zu ändern. Wenn Benutzer über ein lokales Setup verfügen, können sie außerdem einige ihrer Dienste in der Cloud testen, indem sie die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung verwenden, bevor sie vollständig in die Cloud migrieren. Beispielsweise können Benutzer nur einen kleinen Prozentsatz ihres Traffics in die Cloud weiterleiten und den größten Teil des Datenverkehrs on-premises abwickeln. Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung ermöglicht es Benutzern auch, NetScaler-Instanzen über geografische Standorte hinweg von einer einzigen, einheitlichen Konsole aus zu verwalten und zu überwachen.

Eine Hybrid- und Multi-Cloud-Architektur kann auch die Gesamtleistung eines Unternehmens verbessern, indem sie die Abhängigkeit von einem bestimmten Anbieter vermeidet und unterschiedliche Infrastrukturen nutzt, um die Anforderungen von Benutzerpartnern und Kunden zu erfüllen. Mit der Multi-Cloud-Architektur können Benutzer ihre Infrastrukturkosten besser verwalten, da sie jetzt nur für das zahlen, was sie nutzen. Benutzer können ihre Anwendungen auch besser skalieren, da sie die Infrastruktur jetzt bei Bedarf nutzen. Es bietet auch die Möglichkeit, schnell von einer Cloud in eine andere zu wechseln, um die Vorteile der besten Angebote jedes Anbieters zu nutzen.

NetScaler GSLB-Knoten handhaben die DNS-Namensauflösung. Jeder dieser GSLB-Knoten kann DNS-Anfragen von jedem Client-Standort empfangen. Der GSLB-Knoten, der die DNS-Anfrage empfängt, gibt die IP-Adresse des virtuellen Load Balancer-Servers zurück, wie sie von der konfigurierten Lastausgleichsmethode ausgewählt wurde. Metriken (Standort-, Netzwerk- und Persistenzmetriken) werden zwischen den GSLB-Knoten mithilfe des Metrics Exchange Protocol (MEP) ausgetauscht, einem proprietären NetScaler-Protokoll. Weitere Informationen zum MEP-Protokoll finden Sie unterKonfigurieren des Metrics Exchange Protocol.

Der im GSLB-Knoten konfigurierte Monitor überwacht den Zustand des virtuellen Lastausgleichsservers im selben Rechenzentrum. In einer übergeordneten und untergeordneten Topologie

werden Metriken zwischen den GSLB- und NetScaler-Knoten mithilfe von MEP ausgetauscht. Die Konfiguration von Monitorsonden zwischen einem GSLB- und einem NetScaler LB-Knoten ist in einer übergeordneten und untergeordneten Topologie jedoch optional.

Der NetScaler-Agent ermöglicht die Kommunikation zwischen dem NetScaler ADM und den verwalteten Instanzen im Benutzer-Rechenzentrum. Weitere Informationen zu NetScaler-Agenten und deren Installation finden Sie unterErste Schritte.

> **Hinweis:**
>
> In diesem Dokument werden die folgenden Annahmen getroffen:
>
> - Wenn Benutzer über ein vorhandenes Load Balancing-Setup verfügen, ist es betriebsbereit.
> - Eine SNIP-Adresse oder eine GSLB-Site-IP-Adresse ist auf jedem NetScaler GSLB-Knoten konfiguriert. Diese IP-Adresse wird als IP-Adresse der Rechenzentrumsquelle beim Austausch von Metriken mit anderen Rechenzentren verwendet.
> - Ein ADNS- oder ADNS-TCP-Dienst ist auf jeder NetScaler GSLB-Instanz konfiguriert, um den DNS-Verkehr zu empfangen.
> - Die erforderlichen Firewall- und Sicherheitsgruppen werden in den Cloud-Dienstanbietern konfiguriert.

Konfiguration der Sicherheitsgruppen

Benutzer müssen die erforderliche Firewall-/Sicherheitsgruppenkonfiguration in den Cloud-Dienstanbietern einrichten. Weitere Informationen zu den AWS-Sicherheitsfunktionen finden Sie unter AWS/Dokumentation/Amazon VPC/Benutzerhandbuch/Sicherheit.

Außerdem müssen Benutzer auf dem GSLB-Knoten Port 53 für die ADNS-Dienst-/DNS-Server-IP-Adresse und Port 3009 für die GSLB-Standort-IP-Adresse für den MEP-Datenaustausch öffnen. Auf dem Load Balancing-Knoten müssen Benutzer die entsprechenden Ports öffnen, um den Anwendungsdatenverkehr zu empfangen. Benutzer müssen beispielsweise Port 80 für den Empfang von HTTP-Verkehr und Port 443 für den Empfang von HTTPS-Verkehr öffnen. Öffnen Sie Port 443 für die NITRO-Kommunikation zwischen dem NetScaler-Agent und NetScaler ADM.

Für die dynamische Roundtrip-Time-GSLB-Methode müssen Benutzer Port 53 öffnen, um UDP- und TCP-Prüfungen je nach konfiguriertem LDNS-Testtyp zuzulassen. Die UDP- oder TCP-Prüfungen werden mit einem der SNiPs initiiert. Daher muss diese Einstellung für Sicherheitsgruppen vorgenommen werden, die an das serverseitige Subnetz gebunden sind.

Funktionen der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung

Einige der Funktionen der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung werden in diesem Abschnitt beschrieben.

Kompatibilität mit anderen Load Balancing-Lösungen

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt verschiedene Load Balancing-Lösungen wie NetScaler Load Balancer, NGINX, HAProxy und andere Load Balancer von Drittanbietern.

> **Hinweis:**
>
> Andere Load Balancing-Lösungen als NetScaler werden nur unterstützt, wenn proximitätsbasierte und nicht metrische GSLB-Methoden verwendet werden und wenn die übergeordnete und untergeordnete Topologie nicht konfiguriert ist.

GSLB-Methoden

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt die folgenden GSLB-Methoden.

- Metrikbasierte GSLB-Methoden. Metrikbasierte GSLB-Methoden sammeln Metriken von den anderen NetScaler-Knoten über das Metrikaustauschprotokoll.
  - Mindest Connection: Die Client-Anfrage wird an den Load Balancer weitergeleitet, der die wenigsten aktiven Verbindungen hat.
  - Geringste Bandbreite: Die Clientanforderung wird an den Load Balancer weitergeleitet, der derzeit den geringsten Datenverkehr bedient.
  - Wenigste Pakete: Die Client-Anfrage wird an den Load Balancer weitergeleitet, der in den letzten 14 Sekunden die wenigsten Pakete empfangen hat.
- Nichtmetrische GSLB-Methoden
  - Round Robin: Die Client-Anfrage wird an die IP-Adresse des Load Balancers weitergeleitet, die in der Liste der Load Balancer ganz oben steht. Dieser Load Balancer wird dann an das Ende der Liste verschoben.
  - Quell-IP-Hash: Diese Methode verwendet den Hash-Wert der Client-IP-Adresse, um einen Load Balancer auszuwählen.
- Proximity-basierte GSLB-Methoden
  - Statische Nähe: Die Clientanforderung wird an den Load Balancer weitergeleitet, der der Client-IP-Adresse am nächsten ist.

- Round-Trip-Zeit (RTT): Diese Methode verwendet den RTT-Wert (die Zeitverzögerung in der Verbindung zwischen dem lokalen DNS-Server des Clients und dem Rechenzentrum), um die IP-Adresse des Load Balancers mit der besten Leistung auszuwählen.

Weitere Informationen zu den Lastausgleichsmethoden finden Sie unter load balancingAlgorithms.

GSLB-Topologien

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt die Aktiv-Passiv-Topologie und die Parent-Child-Topologie.

- Aktiv-Passiv-Topologie —Bietet Disaster Recovery und gewährleistet die kontinuierliche Verfügbarkeit von Anwendungen durch Schutz vor Ausfallstellen. Wenn das primäre Rechenzentrum ausfällt, wird das passive Rechenzentrum betriebsbereit. Weitere Informationen zur GSLB-Aktiv-Passiv-Topologie finden Sie unter Konfigurieren von GSLB für die Notfallwiederherstellung.
- Übergeordnete/untergeordnete Topologie –Kann verwendet werden, wenn Kunden die metrikbasierten GSLB-Methoden zum Konfigurieren von GSLB- und Lastausgleichsknoten verwenden und wenn die Lastausgleichsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden. In einer über-/untergeordneten Topologie muss der LB-Knoten (untergeordneter Standort) eine NetScaler Appliance sein, da der Austausch von Metriken zwischen dem übergeordneten und dem untergeordneten Standort über das Metrikaustauschprotokoll (MEP) erfolgt.

Weitere Informationen zur Parent-Child-Topologie finden Sie unter Bereitstellung einer Parent-Child-Topologie mit dem MEP-Protokoll.

Unterstützung für IPv6

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt auch IPv6.

Überwachen

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt integrierte Monitore mit einer Option zur Aktivierung der sicheren Verbindung. Wenn sich LB- und GSLB-Konfigurationen jedoch auf derselben NetScaler-Instanz befinden oder wenn eine übergeordnete und untergeordnete Topologie verwendet wird, ist die Konfiguration von Monitoren optional.

Beharrlichkeit

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt Folgendes:

- Quell-IP-basierte Persistenzsitzungen, sodass mehrere Anforderungen desselben Clients an denselben Dienst weitergeleitet werden, wenn sie innerhalb des konfigurierten Zeitüberschreitungsfensters eintreffen. Wenn der Timeoutwert abläuft, bevor der Client eine weitere Anfrage sendet, wird die Sitzung verworfen und der konfigurierte Load Balancing-Algorithmus wird verwendet, um einen neuen Server für die nächste Anforderung des Clients auszuwählen.
- Spillover-Persistenz, so dass der virtuelle Backup-Server die empfangenen Anforderungen weiterhin verarbeitet, auch wenn die Last auf dem primären Schwellenwert unterschritten wird. Weitere Informationen finden Sie unter Spillover konfigurieren.
- Standortpersistenz, sodass der GSLB-Knoten ein Rechenzentrum für die Verarbeitung einer Client-Anfrage auswählt und die IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anfragen weiterleitet. Wenn die konfigurierte Persistenz für eine Site gilt, die DOWN ist, verwendet der GSLB-Knoten eine GSLB-Methode, um eine neue Site auszuwählen, und die neue Site wird für nachfolgende Anfragen vom Client persistent.

Konfiguration mit NetScaler ADM StyleBooks

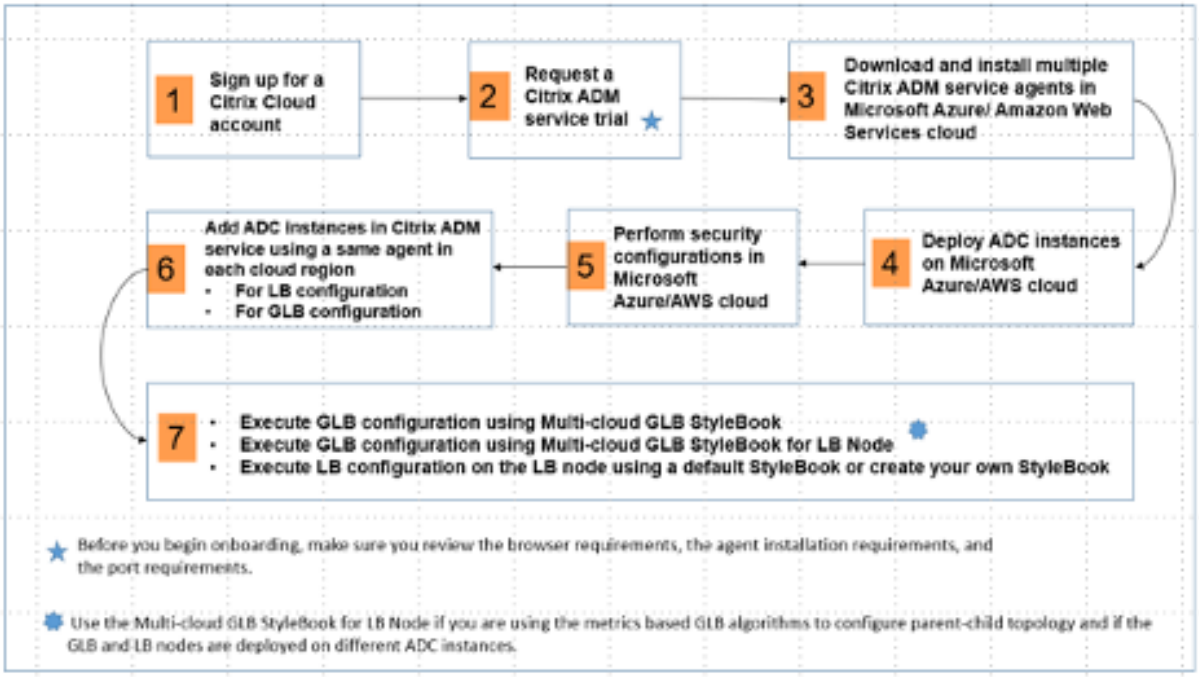
Kunden können das standardmäßige Multi-Cloud-GSLB-StyleBook auf NetScaler ADM verwenden, um NetScaler-Instanzen mit hybriden und Multi-Cloud-GSLB-Konfigurationen zu konfigurieren.

Kunden können das standardmäßige Multi-Cloud-GSLB-StyleBook für das Lastausgleichs-Node-StyleBook verwenden, um NetScaler-Lastausgleichsknoten zu konfigurieren, die die untergeordneten Sites in einer übergeordneten/untergeordneten Topologie sind, die den Anwendungsverkehr verarbeiten. Verwenden Sie dieses StyleBook nur, wenn Benutzer Lastausgleichsknoten in einer übergeordneten/untergeordneten Topologie konfigurieren möchten. Jeder LB-Knoten muss jedoch separat mit diesem StyleBook konfiguriert werden.

Arbeitsablauf der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösungskonfiguration

Kunden können das mitgelieferte Multi-Cloud-GSLB-StyleBook auf NetScaler ADM verwenden, um NetScaler-Instanzen mit hybriden und Multi-Cloud-GSLB-Konfigurationen zu konfigurieren.

Das folgende Diagramm zeigt den Arbeitsablauf für die Konfiguration einer NetScaler-Hybrid- und Multi-Cloud-GSLB-Lösung. Die Schritte im Workflow-Diagramm werden nach dem Diagramm ausführlicher erläutert.



Führen Sie die folgenden Aufgaben als Cloud-Administrator aus:

1. Eröffnen Sie ein NetScaler Cloud-Konto.

   Um mit der Verwendung von NetScaler ADM zu beginnen, erstellen Sie ein NetScaler Cloud-Firmenkonto oder treten Sie einem bestehenden Konto bei, das von jemandem in Ihrem Unternehmen erstellt wurde.

2. Nachdem sich Benutzer bei NetScaler Cloud angemeldet haben, klicken Sie auf der Kachel **NetScaler Application Delivery Management** auf **Verwalten**, um den ADM Service zum ersten Mal einzurichten.

3. Laden Sie mehrere NetScaler ADM-Dienstagenten herunter und installieren Sie sie.

   Benutzer müssen den NetScaler ADM-Dienstagenten in ihrer Netzwerkumgebung installieren und konfigurieren, um die Kommunikation zwischen NetScaler ADM und den verwalteten Instanzen in ihrem Rechenzentrum oder ihrer Cloud zu ermöglichen. Installieren Sie in jeder Region einen Agenten, damit sie LB- und GSLB-Konfigurationen auf den verwalteten Instanzen konfigurieren können. Die LB- und GSLB-Konfigurationen können sich einen einzigen Agenten teilen. Weitere Informationen zu den oben genannten drei Aufgaben finden Sie unter Erste Schritte.

4. Stellen Sie Load Balancer in Cloud-/lokalen Rechenzentren von Microsoft AWS bereit.

   Stellen Sie sie je nach Art der Load Balancer, die Benutzer in der Cloud und vor Ort bereitstellen, entsprechend bereit. Beispielsweise können Benutzer NetScaler VPX-Instanzen in einer virtuellen privaten Cloud von Amazon Web Services (AWS) und in on-premises Rechenzentren bereitstellen. Konfigurieren Sie NetScaler-Instanzen so, dass sie im Standalone-Modus als

LB- oder GSLB-Knoten funktionieren, indem Sie die virtuellen Maschinen erstellen und andere Ressourcen konfigurieren. Weitere Informationen zum Bereitstellen von NetScaler VPX Instanzen finden Sie in den folgenden Dokumenten:

- NetScaler VPX auf AWS.
- Konfigurieren Sie eine NetScaler VPX Standalone-Instanz.

5. Führen Sie Sicherheitskonfigurationen durch.

   Konfigurieren Sie Netzwerksicherheitsgruppen und Netzwerk-ACLs in ARM und in AWS, um den eingehenden und ausgehenden Datenverkehr für Benutzerinstanzen und Subnetze zu steuern.

6. Fügen Sie NetScaler-Instanzen in NetScaler ADM hinzu.

   NetScaler-Instanzen sind Netzwerkgeräte oder virtuelle Geräte, die Benutzer von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Benutzer die Instanzen zum Service hinzufügen und sowohl LB- (wenn Benutzer NetScaler for LB verwenden) als auch GSLB-Instanzen registrieren. Weitere Informationen zum Hinzufügen von NetScaler-Instanzen im NetScaler ADM finden Sie unterErste Schritte

7. Implementieren Sie die GSLB- und LB-Konfigurationen mithilfe der standardmäßigen NetScaler ADM StyleBooks.

   - Verwenden Sie das Multi-Cloud-GSLB-StyleBook, um die GSLB-Konfiguration auf den ausgewählten GSLB-NetScaler-Instanzen auszuführen.
   - Implementieren Sie die Load Balancing-Konfiguration. (Benutzer können diesen Schritt überspringen, wenn sie bereits LB-Konfigurationen auf den verwalteten Instanzen haben.) Benutzer können Load Balancer auf NetScaler-Instanzen auf eine von zwei Arten konfigurieren:
   - Konfigurieren Sie die Instanzen für den Lastenausgleich der Anwendungen manuell. Weitere Informationen zum manuellen Konfigurieren der Instanzen finden Sie unter Grundlegendes Lastenausgleich einrichten.
   - Verwenden Sie StyleBooks. Benutzer können eines der NetScaler ADM StyleBooks (HTTP/SSL-Lastausgleichs-StyleBook oder HTTP/SSL-Lastausgleichs-StyleBook (mit Monitoren)) verwenden, um die Lastausgleichskonfiguration auf der ausgewählten NetScaler-Instanz zu erstellen. Benutzer können auch ihre eigenen StyleBooks erstellen. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

8. Verwenden Sie das Multi-Cloud-GSLB-StyleBook für LB Node, um die GSLB-Parent-Child-Topologie in den folgenden Fällen zu konfigurieren:

   - Wenn Benutzer die metrikbasierten GSLB-Algorithmen (Least Packets, Least Connections, Least Bandwidth) zum Konfigurieren von GSLB und Lastausgleichsknoten verwenden

und wenn die Lastausgleichsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden.

- Wenn Site-Persistenz erforderlich ist.

Verwenden von StyleBooks zum Konfigurieren von GSLB auf NetScaler-Lastausgleichsknoten

Kunden können das**Multi-Cloud GSLB StyleBook für LB-Knoten**verwenden, wenn sie die metrikbasierten GSLB-Algorithmen (Least Packets, Least Connections, Least Bandwidth) zum Konfigurieren von GSLB- und Lastausgleichsknoten verwenden und wenn die Lastausgleichsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden.

Benutzer können dieses StyleBook auch verwenden, um mehr untergeordnete Websites für eine vorhandene übergeordnete Website zu konfigurieren. Dieses StyleBook konfiguriert jeweils eine untergeordnete Website. Erstellen Sie also so viele Konfigurationen (Config Packs) aus diesem StyleBook, wie es untergeordnete Websites gibt. Das StyleBook wendet die GSLB-Konfiguration auf die untergeordneten Sites an. Benutzer können maximal 1024 untergeordnete Websites konfigurieren.

> **Hinweis:**
>
> Verwenden Sie Multi-Cloud GSLB StyleBook, um die übergeordneten Sites zu konfigurieren.

Dieses StyleBook macht die folgenden Annahmen:

- Eine SNIP-Adresse oder eine GSLB-Site-IP-Adresse ist konfiguriert.
- Die erforderlichen Firewall- und Sicherheitsgruppen werden in den Cloud-Dienstanbietern konfiguriert.

Konfigurieren einer untergeordneten Site in einer übergeordneten/untergeordneten Topologie mithilfe des Multi-Cloud-GSLB-StyleBook für LB-Knoten

1. Navigieren Sie zu**Anwendungen > Konfiguration > Neue erstellen**.
2. Navigieren Sie zu**Anwendungen** > **Konfiguration** und klicken Sie auf **Neu erstellen**.

   Das StyleBook wird als Benutzeroberflächenseite angezeigt, auf der Benutzer die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

> **Hinweis:**
>
> Die Begriffe Rechenzentrum und Standorte werden in diesem Dokument synonym verwendet.

1. Legen Sie die folgenden Parameter fest:

- **Name der Anwendung**. Geben Sie den Namen der GSLB-Anwendung ein, die auf den GSLB-Sites bereitgestellt wird, für die Sie untergeordnete Sites erstellen möchten.
- **Protokoll**. Wählen Sie im Dropdown-Listenfeld das Anwendungsprotokoll der bereitgestellten Anwendung aus.
- **LB-Integritätsprüfung** (optional)
- **Typ der Gesundheitsüberprüfung**. Wählen Sie im Dropdown-Listenfeld den Prüftyp aus, der zum Überprüfen des Zustands der Load Balancer-VIP-Adresse verwendet wird, die die Anwendung auf einer Site darstellt.
- **Sicherer Modus**. (Optional) Wählen Sie **Ja** aus, um diesen Parameter zu aktivieren, wenn SSL-basierte Zustandsprüfungen erforderlich sind.
- **HTTP-Anforderung**. (Optional) Wenn Benutzer HTTP als Health-Check-Typ ausgewählt haben, geben Sie die vollständige HTTP-Anfrage ein, die zum Prüfen der VIP-Adresse verwendet wurde.
- **Liste der HTTP-Statusantwortcodes**. (Optional) Wenn Benutzer HTTP als Zustandsprüfungstyp ausgewählt haben, geben Sie die Liste der HTTP-Statuscodes ein, die bei Antworten auf HTTP-Anfragen erwartet werden, wenn die VIP fehlerfrei ist.

2. Konfigurieren der übergeordneten Site.

   - Geben Sie die Details der übergeordneten Site (GSLB-Knoten) an, unter der Sie die untergeordnete Site (LB-Knoten) erstellen möchten.
     - **Site-Name**. Geben Sie den Namen der Site ein.
     - **IP-Adresse des Standorts**. Geben Sie die IP-Adresse ein, die die übergeordnete Site beim Austausch von Metriken mit anderen Sites als Quell-IP-Adresse verwendet. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf dem GSLB-Knoten an jedem Standort konfiguriert ist.
     - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse der übergeordneten Site ein, die zum Austausch von Metriken verwendet wird, wenn die IP-Adresse dieser Site NAT'ed ist.

3. Konfigurieren der untergeordneten Site.

   - Geben Sie die Details der untergeordneten Site an.
     - **Standortname**. Geben Sie den Namen der übergeordneten Site ein.
     - **IP-Adresse des Standorts**. Geben Sie die IP-Adresse der untergeordneten Site ein. Verwenden Sie hier die private IP-Adresse oder SNIP des NetScaler-Knotens, der als untergeordnete Site konfiguriert wird.

- **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse der untergeordneten Site ein, die zum Austausch von Metriken verwendet wird, wenn die IP-Adresse dieser Site NAT'ed ist.

4. Konfiguration aktiver GSLB-Dienste (optional)

   - Konfigurieren Sie aktive GSLB-Dienste nur, wenn die IP-Adresse des virtuellen LB-Servers keine öffentliche IP-Adresse ist. In diesem Abschnitt können Benutzer die Liste der lokalen GSLB-Dienste auf den Websites konfigurieren, auf denen die Anwendung bereitgestellt wird.

     - **Dienst-IP**. Geben Sie die IP-Adresse des virtuellen Lastausgleichsservers auf dieser Site ein.
     - **Öffentliche IP-Adresse des Dienstes**. Wenn die virtuelle IP-Adresse privat ist und eine öffentliche IP-Adresse hat, geben Sie die öffentliche IP-Adresse an.
     - **Service-Anschluss**. Geben Sie den Port des GSLB-Dienstes auf dieser Site ein.
     - **Site-Name**. Geben Sie den Namen der Site ein, auf der sich der GSLB-Dienst befindet.

5. Klicken Sie auf **Zielinstanzen** und wählen Sie NetScaler-Instanzen aus, die als GSLB-Instanzen auf jeder Site konfiguriert sind, auf der die GSLB-Konfiguration bereitgestellt werden soll.
6. Klicken Sie auf **Erstellen**, um die LB-Konfiguration auf der ausgewählten NetScaler-Instanz (LB-Knoten) zu erstellen. Benutzer können auch auf**Trockenlauf**klicken, um die Objekte zu überprüfen, die in den Zielinstanzen erstellt würden. Die von Benutzern erstellte StyleBook-Konfiguration wird in der Liste der Konfigurationen auf der Seite Konfigurationen angezeigt. Benutzer können diese Konfiguration mithilfe der NetScaler ADM-GUI prüfen, aktualisieren oder entfernen.

Bereitstellung von CloudFormation-Vorlagen

NetScaler VPX ist als Amazon Machine Images (AMI) im AWS Marketplace verfügbar. Bevor Sie eine CloudFormation-Vorlage zur Bereitstellung eines NetScaler VPX in AWS verwenden, muss der AWS-Benutzer die Bedingungen akzeptieren und das AWS Marketplace-Produkt abonnieren. Für jede Edition von NetScaler VPX im Marketplace ist dieser Schritt erforderlich.

Jede Vorlage im CloudFormation-Repository enthält eine zusammengestellte Dokumentation, die die Verwendung und Architektur der Vorlage beschreibt. Die Vorlagen versuchen, die empfohlene Bereitstellungsarchitektur von NetScaler VPX zu kodifizieren, den Benutzer in NetScaler einzuführen oder eine bestimmte Funktion, Edition oder Option zu demonstrieren. Benutzer können die Vorlagen wiederverwenden, modifizieren oder erweitern, um sie an ihre speziellen Produktions- und Testanforderungen anzupassen. Die meisten Vorlagen erfordern neben den Berechtigungen zum Erstellen von IAM-Rollen auch vollständige EC2-Berechtigungen.

Die CloudFormation-Vorlagen enthalten AMI-IDs, die für eine bestimmte Version von NetScaler VPX (z. B. Version 12.0-56.20) und eine bestimmte Edition (z. B. NetScaler VPX Platinum Edition —10 Mbit/s) ODER NetScaler BYOL spezifisch sind. Um eine andere Version/Edition von NetScaler VPX mit einer CloudFormation-Vorlage zu verwenden, muss der Benutzer die Vorlage bearbeiten und die AMI-IDs ersetzen.

Die neuesten NetScaler AWS-AMI-IDs befinden sich hier: NetScaler AWS CloudFormation Master.

CFT-Bereitstellung mit drei NICs

Diese Vorlage stellt eine VPC mit 3 Subnetzen (Management, Client, Server) für 2 Availability Zones bereit. Es stellt ein Internet-Gateway mit einer Standardroute in den öffentlichen Subnetzen bereit. Diese Vorlage erstellt auch ein HA-Paar über Availability Zones hinweg mit zwei Instanzen von NetScaler: 3 ENIs, die 3 VPC-Subnetzen (Management, Client, Server) auf primären und 3 ENIs, die 3 VPC-Subnetzen (Management, Client, Server) zugeordnet sind, auf sekundären. Allen von dieser CFT erstellten Ressourcennamen wird ein tagName des Stacknamens vorangestellt.

Die Ausgabe der CloudFormation-Vorlage umfasst:

- primaryCitrixADCManagementUrl —HTTPS-URL zur Management-GUI des primären VPX (verwendet ein selbstsigniertes Zertifikat)
- primaryCitrixADCManagementUrl2 —HTTP-URL zur Management-GUI des primären VPX
- primaryCitrixADCInstanceId —Instanz-ID der neu erstellten primären VPX-Instanz
- primaryCitrixADCPublicVip - Elastische IP-Adresse der primären VPX-Instanz, die mit der VIP verknüpft ist
- primaryCitrixADCPrivatenSIP - Private IP (NS IP), die für die Verwaltung des primären VPX verwendet wird
- primaryCitrixADCPublicNSIP - Öffentliche IP (NS IP), die für die Verwaltung des primären VPX verwendet wird
- primaryCitrixADCPrivateVIP - Private IP-Adresse der primären VPX-Instanz, die mit der VIP verknüpft ist
- primaryCitrixADCSnip - Private IP-Adresse der primären VPX-Instanz, die mit dem SNIP verknüpft ist
- secondaryCitrixADCManagementUrl —HTTPS-URL zur Management-GUI des sekundären VPX (verwendet selbstsigniertes Zertifikat)
- SecondaryCitrixADCManagementUrl2 —HTTP-URL zur Management-GUI des sekundären VPX
- secondaryCitrixADCInstanceId —Instanz-ID der neu erstellten sekundären VPX-Instanz

- SecondaryCitrixADCPrivatenSIP - Private IP (NS IP) zur Verwaltung des sekundären VPX
- SecondaryCitrixADCPublicNSIP - Öffentliche IP (NS IP) zur Verwaltung des sekundären VPX
- SecondaryCitrixADCPrivateVIP - Private IP-Adresse der sekundären VPX-Instanz, die mit der VIP verknüpft ist
- SecondaryCitrixADCSnip - Private IP-Adresse der sekundären VPX-Instanz, die mit dem SNIP verknüpft ist
- SecurityGroup - Sicherheitsgruppen-ID, zu der der VPX gehört

Bei der Bereitstellung von Eingaben für die CFT bedeutet * das für einen beliebigen Parameter in der CFT, dass es sich um ein Pflichtfeld handelt. Zum Beispiel `VPC ID*` ist ein Pflichtfeld.

Die folgenden Voraussetzungen müssen erfüllt sein. Die CloudFormation-Vorlage erfordert ausreichende Berechtigungen, um IAM-Rollen zu erstellen, die über die normalen vollen EC2-Berechtigungen hinausgehen. Der Benutzer dieser Vorlage muss außerdem die Bedingungen akzeptieren und das AWS Marketplace-Produkt abonnieren, bevor er diese CloudFormation-Vorlage verwenden kann.

Folgendes sollte ebenfalls vorhanden sein:

- Schlüssel-Paar
- 3 nicht zugewiesene EIPs
- Primäre Verwaltung
- Kunde VIP
- Sekundäres Management

Weitere Informationen zur Bereitstellung von NetScaler VPX-Instanzen auf AWS finden Benutzer unter: Bereitstellung von NetScaler VPX-Instanzen auf AWS.

Informationen zum Konfigurieren von GSLB mit StyleBooks finden Sie unter Verwenden von StyleBooks zum Konfigurieren von GSLB

Notfallwiederherstellung (DR)

Katastrophe ist eine plötzliche Störung der Geschäftsfunktionen, die durch Naturkatastrophen oder durch Menschen verursachte Ereignisse verursacht werden. Katastrophen wirken sich auf den Betrieb des Rechenzentrums aus. Danach müssen die am Katastrophenort verlorenen Ressourcen und Daten vollständig neu aufgebaut und wiederhergestellt werden. Der Verlust von Daten oder Ausfallzeiten im Rechenzentrum ist entscheidend und reduziert die Business Continuity.

Eine der Herausforderungen, vor denen Kunden heute stehen, besteht darin, zu entscheiden, wo sie ihren DR-Standort platzieren möchten. Unternehmen suchen nach Konsistenz und Leistung, unabhängig von zugrunde liegenden Infrastruktur- oder Netzwerkfehlern.

Informationen zum Bereitstellen von GSLB für die Notfallwiederherstellung finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

Andere Ressourcen

NetScaler ADM GSLB für Hybrid- und Multi-Cloud-Bereitstellungen.

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

October 17, 2024

> **Hinweis:**
>
> Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab NetScaler Version 12.0 57.19 verfügbar.

Nachdem Sie eine NetScaler VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe der AWS CLI für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren.

In allen NetScaler VPX-Modellen, außer NetScaler VPX AWS Marketplace Editions von 3G und 5G, ist SR-IOV in der Standardkonfiguration einer Netzwerkschnittstelle nicht aktiviert.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Dieser Abschnitt enthält die folgenden Themen:

- Ändern Sie den Schnittstellentyp auf SR-IOV
- Konfiguration von SR-IOV in einem Hochverfügbarkeits-Setup

Ändern Sie den Schnittstellentyp auf SR-IOV

Sie können den Befehl show interface summary ausführen, um die Standardkonfiguration einer Netzwerkschnittstelle zu überprüfen.

Beispiel 1: Die folgende CLI-Bildschirmaufnahme zeigt die Konfiguration einer Netzwerkschnittstelle, bei der SR-IOV standardmäßig in NetScaler VPX AWS Marketplace Editions von 3G und 5G aktiviert ist.

```
> show interface summary
-------------------------------------------------------------------------
     Interface  MTU       MAC               Suffix
-------------------------------------------------------------------------
1      1/1      1500      0a:1e:2e:17:a2:37   Intel 82599 10G VF Interface
2      LO/1     1500      0a:1e:2e:17:a2:37   Netscaler Loopback interface
 Done
```

Beispiel 2: Die folgende CLI-Bildschirmaufnahme zeigt die Standardkonfiguration einer Netzwerkschnittstelle, bei der SR-IOV nicht aktiviert ist.

```
 Done
> sh int s
-------------------------------------------------------------------------
     Interface  MTU       MAC               Suffix
-------------------------------------------------------------------------
1      1/1      1500      12:fc:04:c5:d0:12   NetScaler Virtual Interface
2      LO/1     1500      12:fc:04:c5:d0:12   Netscaler Loopback interface
 Done
>
```

Weitere Informationen zum Ändern des Schnittstellentyps in SR-IOV finden Sie unterhttp://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Um den Schnittstellentyp auf SR-IOV zu ändern

1. Fahren Sie die NetScaler VPX-Instance herunter, die auf AWS ausgeführt wird.
2. Um SR-IOV auf der Netzwerkschnittstelle zu aktivieren, geben Sie den folgenden Befehl in die AWS-CLI ein.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \\&#060;instance\\_id\\&#062; --sriov-net-support simple
   ```

3. Um zu überprüfen, ob SR-IOV aktiviert wurde, geben Sie den folgenden Befehl in der AWS CLI ein.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \\&#060;instance\\_id\\&#062; --attribute sriovNetSupport
   ```

   Beispiel 3: Der Netzwerkschnittstellentyp wurde unter Verwendung der AWS CLI in SR-IOV geändert.


```
                                    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"
    }
}
```

Wenn SR-IOV nicht aktiviert ist, ist der Wert für SRIOVNetSupport nicht vorhanden.

Beispiel 4: Im folgenden Beispiel ist die SR-IOV-Unterstützung nicht aktiviert.

```
{
    "InstanceId": "i-0c3e84cfa65b04cc8",
    "SriovNetSupport": {}
}
```

4. Schalten Sie die VPX-Instanz ein. Um den geänderten Status der Netzwerkschnittstelle anzuzeigen, geben Sie “Interface-Zusammenfassung anzeigen”in die CLI ein.

   Beispiel 5: Die folgende Bildschirmaufnahme zeigt die Netzwerkschnittstellen mit aktiviertem SR-IOV. Die Schnittstellen 10/1, 10/2, 10/3 sind SR-IOV aktiviert.

```
> 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
```

Mit diesen Schritten wird das Verfahren zum Konfigurieren von VPX-Instanzen für die Verwendung von SR-IOV-Netzwerkschnittstellen abgeschlossen.

Konfiguration von SR-IOV in einem Hochverfügbarkeits-Setup

Hochverfügbarkeit wird mit SR-IOV-Schnittstellen ab NetScaler Version 12.0 Build 57.19 unterstützt.

Wenn das Hochverfügbarkeits-Setup manuell oder mithilfe der Citrix CloudFormation-Vorlage für NetScaler Version 12.0 56.20 und niedriger bereitgestellt wurde, muss die dem Hochverfügbarkeits-Setup zugeordnete IAM-Rolle über die folgenden Rechte verfügen:

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances

- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns:*
- sqs:*
- iam:SimulatePrincipalPolicy
- iam:GetRole

Standardmäßig fügt die Citrix CloudFormation-Vorlage für NetScaler Version 12.0 57.19 automatisch die erforderlichen Berechtigungen zur IAM-Rolle hinzu.

> **Hinweis:**
>
> Ein Hochverfügbarkeits-Setup mit SR-IOV-Schnittstellen benötigt etwa 100 Sekunden Ausfallzeiten.

Verwandte Ressourcen:

Weitere Informationen zu IAM-Rollen finden Sie in der AWS-Dokumentation.

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung von Enhanced Networking mit AWS ENA

October 17, 2024

Nachdem Sie eine NetScaler VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe von [AWS CLI für die Verwendung von [Enhanced Networking](https://docs.aws.amazon.com/AWSEC2/late networking.html) with AWS Elastic Network Adapter (ENA)](https://aws.amazon.com/about-aws/whats-new/2016/06/introducing-elastic-network-adapter-ena-the-next-generation-network-interface-for-ec2-instances/)konfigurieren.

In Verbindung mit AWS ENA bietet das erweiterte Netzwerk eine höhere Bandbreite, eine höhere Paketper-Sekunden-Leistung (PPS) und konstant niedrigere Instanz-Latenzen.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Die folgenden HA-Konfigurationen werden für ENA-fähige Instanzen unterstützt:

- Private IP-Adressen können innerhalb derselben Availability Zone verschoben werden.
- Elastische IP-Adressen können über Availability Zones verschoben werden.

Aktualisieren einer NetScaler VPX-Instanz auf AWS

October 17, 2024

Sie können den EC2-Instance-Typ, den Durchsatz, die Software-Edition und die Systemsoftware eines NetScaler VPX, das auf AWS ausgeführt wird, aktualisieren. Für bestimmte Arten von Upgrades empfiehlt Citrix die Verwendung der High Availability Configuration Methode, um Ausfallzeiten zu minimieren.

> **Hinweis:**
>
> - Die NetScaler-Softwareversion 10.1.e-124.1308.e oder höher für ein NetScaler VPX-AMI (einschließlich Utility-Lizenz und Kundenlizenz) unterstützt die Instance-Familien M1 und M2 nicht.
> - Aufgrund von Änderungen in der VPX-Instanzunterstützung wird ein Downgrade von 10.1.e-124 oder einer höheren Version auf 10.1.123.x oder eine frühere Version nicht unterstützt.
> - Für die meisten Upgrades ist kein neues AMI erforderlich, und das Upgrade kann auf der aktuellen NetScaler-AMI-Instance durchgeführt werden. Wenn Sie ein Upgrade auf eine neue NetScaler-AMI-Instance durchführen möchten, verwenden Sie die Hochverfügbarkeitskonfigurationsmethode.

Ändern Sie den EC2-Instance-Typ einer NetScaler VPX-Instance auf AWS

Wenn auf Ihren NetScaler VPX-Instances Version 10.1.e-124.1308.e oder höher ausgeführt wird, können Sie den EC2-Instance-Typ von der AWS-Konsole aus wie folgt ändern:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Starten Sie die Instanz.

Sie können das obige Verfahren auch verwenden, um den EC2-Instanztyp für eine Version vor 10.1.e-124.1308.e zu ändern, es sei denn, Sie möchten den Instanztyp in M3 ändern. In diesem Fall müssen Sie zuerst das standardmäßige NetScaler-Upgradeverfahren befolgen, um die NetScaler-Software auf 10.1.e-124 oder eine spätere Version zu aktualisieren, und dann die obigen Schritte ausführen.

Aktualisieren des Durchsatzes oder der Software-Edition einer NetScaler VPX-Instanz auf AWS

Um die Software-Edition (z. B. um von Standard auf Premium Edition zu aktualisieren) oder den Durchsatz (z. B. um von 200 Mbit/s auf 1000 Mbit/s zu aktualisieren), hängt die Methode von der Lizenz der Instanz ab.

Verwendung einer Kundenlizenz (Bring-Your-Own-Lizenz)

Wenn Sie eine Kundenlizenz verwenden, können Sie die neue Lizenz von der Citrix Website erwerben und herunterladen und dann die Lizenz auf der VPX-Instanz installieren. Weitere Informationen zum Herunterladen und Installieren einer Lizenz von der Citrix Website finden Sie im VPX-Lizenzhandbuch.

Verwendung einer Versorgungslizenz (Dienstprogrammlizenz mit Stundengebühr)

AWS unterstützt keine direkten Upgrades für kostenpflichtige Instanzen. Um die Software-Edition oder den Durchsatz einer gebührenbasierten NetScaler VPX-Instanz zu aktualisieren, starten Sie ein neues AMI mit der gewünschten Lizenz und Kapazität und migrieren Sie die ältere Instanzkonfiguration auf die neue Instanz. Dies kann durch die Verwendung einer NetScaler-Hochverfügbarkeitskonfiguration erreicht werden, wie im Unterabschnitt [Upgrade auf eine neue NetScaler-AMI-Instanz durch Verwendung einer NetScaler-Hochverfügbarkeitskonfiguration](#upgrade-to-a-new-citrix-adc-ami-instance-by-using-a-citrix-adc-high-availability-configuration) auf dieser Seite beschrieben.

Aktualisieren der Systemsoftware einer NetScaler VPX-Instanz auf AWS

Wenn Sie eine VPX-Instanz mit 10.1.e-124.1308.e oder einer späteren Version aktualisieren müssen, befolgen Sie das standardmäßige NetScaler-Upgradeverfahren beim Upgrade und Downgrade einer NetScaler Appliance.

Wenn Sie eine VPX-Instanz mit einer älteren Version als 10.1.e-124.1308.e auf 10.1.e-124.1308.e oder höher aktualisieren müssen, aktualisieren Sie zuerst die Systemsoftware, und ändern Sie dann den Instanztyp wie folgt auf M3:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Starten Sie die Instanz.

Führen Sie ein Upgrade auf eine neue NetScaler AMI-Instance mithilfe einer NetScaler-Hochverfügbarkeitskonfiguration durch

Gehen Sie wie folgt vor, um die Hochverfügbarkeitsmethode für ein Upgrade auf eine neue NetScaler AMI-Instance zu verwenden:

- Erstellen Sie eine neue Instanz mit dem gewünschten EC2-Instanztyp, der Software-Edition, dem Durchsatz oder der Software-Version vom AWS-Marktplatz.

- Konfigurieren Sie die hohe Verfügbarkeit zwischen der alten Instanz (die aktualisiert werden soll) und der neuen Instanz. Nachdem die hohe Verfügbarkeit zwischen der alten und der neuen Instanz konfiguriert wurde, wird die Konfiguration der alten Instanz mit der neuen Instanz synchronisiert.
- Erzwingen Sie ein HA-Failover von der alten Instanz auf die neue Instanz. Infolgedessen wird die neue Instanz primär und beginnt mit dem Empfang von Datenverkehr.
- Beenden Sie, und konfigurieren Sie die alte Instanz neu oder entfernen Sie sie aus AWS.

Zu berücksichtigende Voraussetzungen und Punkte

- Stellen Sie sicher, dass Sie verstehen, wie hohe Verfügbarkeit zwischen zwei NetScaler VPX -Instanzen in AWS funktioniert. Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.
- Sie müssen die neue Instanz in derselben Availability Zone wie die alte Instanz erstellen, wobei genau dieselbe Sicherheitsgruppe und dasselbe Subnetz vorhanden sind.
- Die Einrichtung für hohe Verfügbarkeit erfordert Zugriffs- und geheime Schlüssel, die mit dem AWS Identity and Access Management (IAM) -Konto des Benutzers für beide Instanzen verknüpft sind. Wenn beim Erstellen von VPX-Instanzen die richtigen Schlüsselinformationen nicht verwendet werden, schlägt das HA-Setup fehl. Weitere Informationen zum Erstellen eines IAM-Kontos für eine VPX-Instanz finden Sie unter Voraussetzungen.
  - Sie müssen die EC2-Konsole verwenden, um die neue Instanz zu erstellen. Sie können den AWS-1-Click-Start nicht verwenden, da er die Zugriffs- und geheimen Schlüssel nicht als Eingabe akzeptiert.
  - Die neue Instanz muss nur eine ENI-Schnittstelle haben.

Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mithilfe einer Hochverfügbarkeitskonfiguration zu aktualisieren:

1. Konfigurieren Sie die hohe Verfügbarkeit zwischen der alten und der neuen Instanz. Um die Hochverfügbarkeit zwischen zwei NetScaler VPX-Instanzen zu konfigurieren, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Beispiel:

   Geben Sie in der Befehlszeile der alten Instanz Folgendes ein:

   ```
   1  add ha node 30 192.0.2.30
   2  Done
   ```


Geben Sie in der Befehlszeile der neuen Instanz Folgendes ein:

```
1   add ha node 10 192.0.2.10
2   Done
```

Beachten Sie Folgendes:

- Im HA-Setup ist die alte Instanz der primäre Knoten und die neue Instanz der sekundäre Knoten.
- Die NSIP-IP-Adresse wird nicht von der alten Instanz in die neue Instanz kopiert. Daher hat Ihre neue Instanz nach dem Upgrade eine andere Verwaltungs-IP-Adresse als die vorherige.
- Das `nsroot` Kontokennwort der neuen Instanz wird nach der HA-Synchronisierung auf das der alten Instanz festgelegt.

Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.

2. Erzwingen Sie ein HA-Failover. Um ein Failover in einer Hochverfügbarkeitskonfiguration zu erzwingen, geben Sie an der Eingabeaufforderung einer der Instanzen Folgendes ein:

```
1   force HA failover
```

Als Ergebnis des Erzwingen eines Failovers werden die ENIs der alten Instanz auf die neue Instanz migriert und der Datenverkehr fließt durch die neue Instanz (den neuen primären Knoten). Die alte Instanz (der neue sekundäre Knoten) wird neu gestartet.

Wenn die folgende Warnmeldung angezeigt wird, geben Sie N ein, um den Vorgang abzubrechen:

```
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)?
```

Die Warnmeldung wird angezeigt, da die Systemsoftware der beiden VPX-Instanzen nicht HA-kompatibel ist. Daher kann die Konfiguration der alten Instanz während eines erzwungenen Failovers nicht automatisch mit der neuen Instanz synchronisiert werden.

Es folgt die Problemumgehung für dieses Problem:

a) Geben Sie an der NetScaler-Shell-Eingabeaufforderung der alten Instanz den folgenden Befehl ein, um eine Sicherungskopie der Konfigurationsdatei (`ns.conf`) zu erstellen:

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Entfernen Sie die folgende Zeile aus der Backup-Konfigurationsdatei (`ns.conf.bkp`):

- `set ns config -IPAddress <IP> -netmask <MASK>`

Beispiel: `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Kopieren Sie die Sicherungskonfigurationsdatei der alten Instanz (`ns.conf.bkp`) in das Verzeichnis `/nsconfig` der neuen Instanz.

d) Geben Sie an der NetScaler-Shell-Eingabeaufforderung der neuen Instanz den folgenden Befehl ein, um die Konfigurationsdatei der alten Instanz (`ns.conf.bkp`) auf die neue Instanz zu laden:

- `batch -f /nsconfig/ns.conf.bkp`

e) Speichern Sie die Konfiguration auf der neuen Instanz.

- `save conifg`

f) Geben Sie an der Eingabeaufforderung eines der Knoten den folgenden Befehl ein, um ein Failover zu erzwingen, und geben Sie dann Y für die Warnmeldung ein, um den Failover-Vorgang zu bestätigen:

- `force ha failover`

Beispiel:

```
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. Entfernen Sie die HA-Konfiguration, sodass sich die beiden Instanzen nicht mehr in einer HA-Konfiguration befinden. Entfernen Sie zuerst die HA-Konfiguration vom sekundären Knoten, und entfernen Sie dann die HA-Konfiguration vom primären Knoten.

   Um eine HA-Konfiguration zwischen zwei NetScaler VPX-Instanzen zu entfernen, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

```
1       > remove ha node \<nodeID\>
2       >  save config
```

   Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaars auf AWS.

   Beispiel:

Geben Sie an der Eingabeaufforderung der alten Instanz (neuer sekundärer Knoten) Folgendes ein:

```
> remove ha node 30
  Done
> save config
  Done
```

Geben Sie an der Eingabeaufforderung der neuen Instanz (neuer Primärknoten) Folgendes ein:

```
> remove ha node 10
  Done
> save config
  Done
```

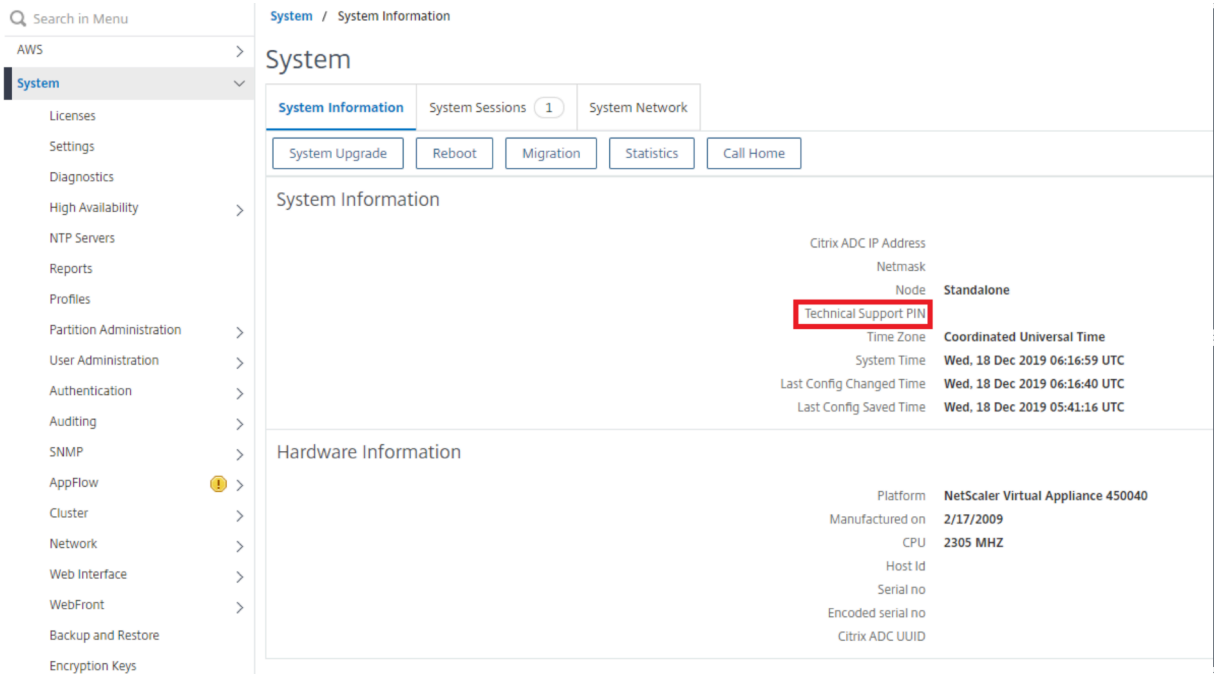
Problembehandlung bei einer VPX-Instanz in AWS

October 17, 2024

Amazon bietet keinen Konsolenzugriff auf eine NetScaler VPX-Instance. Zur Fehlerbehebung müssen Sie die AWS GUI verwenden, um das Aktivitätsprotokoll anzuzeigen. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, klicken Sie mit der rechten Maustaste auf die Instanz und wählen Sie Systemprotokoll

NetScaler bietet Support für von AWS Marketplace lizenzierte NetScaler VPX-Instances (Utility-Lizenz mit Stundengebühr) auf AWS. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer AWS-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support. Sie werden auch nach Ihrem Namen und Ihrer E-Mail-Adresse gefragt. Um die Support-PIN zu finden, melden Sie sich an der VPX-GUI an und navigieren Sie zur Systemseite.

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



AWS FAQs

October 17, 2024

- **Unterstützt eine NetScaler VPX-Instance die verschlüsselten Volumes in AWS?**

  Verschlüsselung und Entschlüsselung erfolgen auf Hypervisor Ebene und funktioniert daher nahtlos mit jeder Instanz. Weitere Informationen zu den verschlüsselten Volumes finden Sie im folgenden AWS-Dokument:

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Was ist der beste Weg, um eine NetScaler VPX-Instanz auf AWS bereitzustellen?**

  Sie können eine NetScaler VPX-Instance auf AWS auf eine der folgenden Arten bereitstellen:

  - AWS CloudFormation-Vorlage (CFT) in der AWS-Marketplace-Site
  - NetScaler ADM
  - AWS Schnellstarts
  - Citrix AWS CFTs in GitHub
  - Citrix Terraform-Skripts in GitHub
  - Citrix Ansible Playbooks in GitHub
  - AWS EC2-Start-Workflow

Sie können eine der aufgelisteten Optionen basierend auf dem von Ihnen verwendeten Automatisierungswerkzeug auswählen.

Weitere Einzelheiten zu den Optionen finden Sie unter NetScaler VPX auf AWS.

- **Wie aktualisiere ich die NetScaler VPX Instanz in AWS?**

  Um die NetScaler VPX-Instanz in AWS zu aktualisieren, können Sie die Systemsoftware aktualisieren oder auf ein neues NetScaler VPX Amazon Machine Image (AMI) aktualisieren, indem Sie das Verfahren unter Aktualisieren einer NetScaler VPX-Instanz auf AWSbefolgen.

  Die empfohlene Möglichkeit, eine NetScaler VPX-Instanz zu aktualisieren, besteht darin, den ADM-Dienst zu verwenden, indem Sie das Verfahren unter Verwenden von Jobs zum Upgrade von NetScaler-Instanzenbefolgen.

- **Wie hoch ist die HA-Failover-Zeit für NetScaler VPX in AWS?**

  - Das HA-Failover von NetScaler VPX innerhalb der AWS Availability Zone dauert etwa 3 Sekunden.
  - Das HA-Failover von NetScaler VPX in AWS-Verfügbarkeitszonen dauert etwa 5 Sekunden.

- **Welchen Support erhalten Kunden des NetScaler VPX Marketplace-Abonnements, die die PIN für den technischen Support bereitstellen?**

  Standardmäßig wird der Dienst “Für Software auswählen”Kunden zur Verfügung gestellt, die die PIN für den technischen Support bereitstellen.

- **Müssen wir bei Hochverfügbarkeit über verschiedene Zonen hinweg mithilfe der Elastic IP -Bereitstellung mehrere IPSets für jede Anwendung erstellen?**

  Ja. Wenn es mehrere Anwendungen mit mehreren VIPs gibt, die mehreren EIPs zugeordnet sind, sind mehrere IPSets erforderlich. Daher werden während des HA-Failovers alle primären VIP-Zuordnungen von EIPs in sekundäre (neue primäre) VIPs geändert.

- **Warum ist der INC-Modus bei hoher Verfügbarkeit für verschiedene Zonenbereitstellungen aktiviert?**

  HA-Paare in allen Availability Zones befinden sich in verschiedenen Netzwerken. Für die HA-Synchronisation darf die Netzwerkkonfiguration nicht synchronisiert werden. Dies wird erreicht, indem der INC-Modus für ein HA-Paar aktiviert wird.

- **Kann der HA-Knoten in einer Availability Zone mit Back-End-Servern in einer anderen Availability Zone kommunizieren, vorausgesetzt, diese Verfügbarkeitszonen befinden sich in derselben VPC?**

  Ja, Subnetze in verschiedenen Availability Zones derselben VPC sind erreichbar, indem eine zusätzliche Route hinzugefügt wird, die über SNIP auf das Backend-Server-Subnetz verweist.

Wenn das SNIP-Subnetz von ADC in AZ1 beispielsweise 192.168.3.0/24 ist und das Backend-Server-Subnetz in AZ2 192.168.6.0/24 ist, muss eine Route in der NetScaler Appliance hinzugefügt werden, die in AZ1 als 192.168.6.0 255.255.255.0 192.168.3.1 vorhanden ist.

- **Können Hohe Verfügbarkeit über verschiedene Zonen hinweg mithilfe von Elastic IP und Hohe Verfügbarkeit über verschiedene Zonen hinweg mithilfe von Private IP Bereitstellungen zusammenarbeiten?**

  Ja, beide Konfigurationen können auf dasselbe HA-Paar angewendet werden.

- **Wenn bei einer Bereitstellung mit hoher Verfügbarkeit über verschiedene Zonen hinweg mithilfe einer privaten IP-Adresse mehrere Subnetze mit mehreren Routentabellen in einer VPC vorhanden sind, woher weiß dann ein sekundärer Knoten im HA-Paar von der Routentabelle, die während eines HA-Failovers überprüft werden muss?**

  Der sekundäre Knoten kennt die primären NICs und sucht in allen Routing-Tabellen in einer VPC.

- **Wie groß ist die Partition /var, wenn das Standardimage für VPX in AWS verwendet wird? Wie erhöht man den Speicherplatz?**

  Die Größe des Rootdatenträgers ist auf 20 GB begrenzt, um das Datenträgerimage klein zu halten.

  Wenn Sie den Verzeichnisspeicher für /var/core/ oder /var/crash/ vergrößern möchten, hängen Sie einen zusätzlichen Datenträger an. Um die Größe von /var zu erhöhen, müssen Sie derzeit einen zusätzlichen Datenträger anhängen und einen symbolischen Link zu /var erstellen, nachdem Sie den kritischen Inhalt auf den neuen Datenträger kopiert haben.

- **Wie viele Paket-Engines werden aktiviert und vCPUs zugewiesen?**

  Die Paket-Engines (PEs) sind durch die Anzahl der lizenzierten vCPUs begrenzt. Die NetScaler Daemons sind nicht an eine bestimmte vCPU angeheftet und werden möglicherweise auf einem der vCPUs ohne PE ausgeführt. Laut AWS ist der C5.9XLarge eine 36VCPU-Instanz mit 72 GB Speicher. Bei der gepoolten Lizenzierung wird die NetScaler VPX-Instanz mit der maximalen Anzahl von PEs bereitgestellt. In diesem Fall laufen 19 PEs auf den Kernen 1–19. In diesem Fall laufen 19 PEs auf Kernen 1 bis 19. ADC-Managementprozesse laufen jedoch von CPUs 20 bis 31 aus.

- **Wie entscheide ich die richtige AWS-Instanz für ADC?**

  1. Verstehen Sie Ihren Anwendungsfall und Ihre Anforderungen wie Durchsatz, PPS, SSL-Anforderungen und durchschnittliche Paketgröße.
  2. Wählen Sie das richtige ADC-Angebot und die richtige Lizenzierung für ADC, die Ihren Anforderungen entspricht, wie VPX-Bandbreitenangebote oder vCPU-basierte Lizenzierung.
  3. Entscheiden Sie sich basierend auf dem gewählten Angebot für die AWS-Instanz.

  Beispiel

Eine 5-Gbit/s-Lizenz ermöglicht 5 Datenpaket-Engines. Daher ist die vCPU-Anforderung 6 (5+1 für die Verwaltung). 6 vCPU-Instanz ist jedoch nicht verfügbar. Eine 8 vCPU ist also gut genug, um diesen Durchsatz zu erreichen, vorausgesetzt, Sie wählen ein Netzwerk, das 5 Gbit/s Bandbreite unterstützt. Zum Beispiel müssen Sie m5.2xlarge für eine 5-Gbit/s-Bandbreitenlizenz wählen, um die maximale PE-Zuweisung für eine 5-Gbit/s-Lizenz zu ermöglichen. Wenn Sie jedoch eine vCPU-Lizenz verwenden, die nicht durch den Durchsatz begrenzt ist, erhalten Sie möglicherweise einen Durchsatz von 5 Gbit/s mithilfe der m5.xlarge-Instanz selbst.

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

- **Ist die Bereitstellung von drei NICs-drei Subnetzen für ADC in AWS obligatorisch?**

  Three NICs-three subnets ist die empfohlene Bereitstellung, bei der jede für Management-, Client- und Server-Netzwerk verwendet wird. Diese Bereitstellung bietet eine bessere Verkehrsisolation und VPX-Leistung. Zwei NICS-zwei Subnetze und ein NIC-One-Subnetz sind die anderen verfügbaren Optionen. Es wird nicht empfohlen, in AWS mehrere Netzwerkkarten gleichzeitig ein Subnetz zu verwenden, wie etwa eine Bereitstellung mit zwei Netzwerkkarten und einem Subnetz. Dieses Szenario kann Netzwerkprobleme wie asymmetrisches Routing verursachen. Weitere Informationen finden Sie unter Best Practices zum Konfigurieren von Netzwerkschnittstellen in AWS.

- **Warum zeigt ein ENA-Treiber auf AWS immer eine Verbindungsgeschwindigkeit von 1 Gbit/s (1/1) an, unabhängig von den Netzwerkfunktionen der Instanz?**

  Die gemeldete Geschwindigkeit eines AWS Elastic Network Adapter (ENA) wird häufig als 1 Gbit/s (1/1) angezeigt, unabhängig vom ausgewählten Instanztyp. Dies liegt daran, dass die angegebene Geschwindigkeit nicht direkt die tatsächliche Netzwerkleistung widerspiegelt. Im Gegensatz zu herkömmlichen Netzwerkschnittstellen können ENA-Geschwindigkeiten dynamisch basierend auf den Anforderungen und der Arbeitslast der Instanz skaliert werden. Die tatsächliche Netzwerkleistung wird in erster Linie durch den Instanztyp und die Instanzgröße bestimmt. Daher kann der tatsächliche Netzwerkdurchsatz je nach spezifischem Instanztyp und aktueller Netzwerkauslastung erheblich variieren.

Bereitstellen einer NetScaler VPX Instanz unter Microsoft Azure

October 17, 2024

Wenn Sie eine NetScaler VPX-Instanz in Microsoft Azure Resource Manager (ARM) bereitstellen, können Sie beide der folgenden Feature-Sets verwenden, um Ihre Geschäftsanforderungen zu erfüllen:

- Azure Cloud Computing-Funktionen
- Funktionen für NetScaler Load Balancing und Traffic Management

Sie können NetScaler VPX-Instanzen auf ARM entweder als eigenständige Instanzen oder als Hochverfügbarkeitspaare im aktiven Standby-Modus bereitstellen.

Sie können eine NetScaler VPX-Instanz auf Microsoft Azure auf zwei Arten bereitstellen:

- Über Azure Marketplace. NetScaler VPX ist eine virtuelle Appliance, die als Image in Microsoft Azure Marketplace zur Verfügung steht.
- Verwenden der auf GitHub verfügbaren JSON-Vorlage NetScaler Azure Resource Manager (ARM). Weitere Informationen finden Sie im GitHub-Repository für NetScaler-Lösungsvorlagen.

Der Microsoft Azure-Stack ist eine integrierte Plattform für Hardware und Software, die die Public Cloud-Dienste von Microsoft Azure in einem lokalen Rechenzentrum bereitstellt, damit Unternehmen Hybrid-Clouds erstellen können. Sie können jetzt die NetScaler VPX-Instanzen auf dem Microsoft Azure-Stack bereitstellen.

> **Hinweis:**
>
> Azure schränkt den Zugriff auf Datenverkehr ein, der von außerhalb von Azure stammt, und blockiert ihn. Um Zugriff zu gewähren, aktivieren Sie den Dienst oder Port, indem Sie eine Regel für eingehenden Datenverkehr in der Netzwerksicherheitsgruppe hinzufügen, die der Netzwerkkarte der VM zugeordnet ist, an die eine öffentliche IP-Adresse angehängt ist. Weitere Informationen finden Sie in der Azure-Dokumentation zu eingehenden NAT-Regeln.

Voraussetzung

Sie benötigen einige Vorkenntnisse, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen können.

- Vertrautheit mit Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Kenntnisse einer NetScaler-Appliance. Ausführliche Informationen zur NetScaler-Appliance finden Sie unter NetScaler
- Kenntnisse über NetScaler Netzwerke. Weitere Informationen finden Sie im Thema Netzwerk.

Funktionsweise einer NetScaler VPX-Instanz in Azure

In einer on-premises Bereitstellung benötigt eine NetScaler VPX-Instanz mindestens drei IP-Adressen:

- Verwaltungs-IP-Adresse, NSIP-Adresse genannt
- Subnetz-IP (SNIP) -Adresse für die Kommunikation mit der Serverfarm
- Virtual Server IP (VIP) Adresse für die Annahme von Clientanforderungen

Weitere Informationen finden Sie unter Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure.

> **Hinweis:**
>
> NetScaler VPX-Instanz unterstützt sowohl Intel- als auch AMD-Prozessoren. Virtuelle VPX-Appliances können auf jedem Instanztyp bereitgestellt werden, der über zwei oder mehr virtualisierte Kerne und mehr als 2 GB Arbeitsspeicher verfügt. Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

In einer Azure-Bereitstellung können Sie eine NetScaler VPX-Instanz in Azure auf drei Arten bereitstellen:

- Multi-NIC-Multi-IP-Architektur
- Multi-IP-Architektur mit einer NIC
- Einzelne NIC-Einzel-IP

Je nach Bedarf können Sie jeden dieser unterstützten Architekturtypen verwenden.

Multi-NIC-Multi-IP-Architektur

Bei diesem Bereitstellungstyp können Sie mehrere Netzwerkschnittstellen (NICs) an eine VPX-Instanz anschließen. Jede NIC kann eine oder mehrere IP-Konfigurationen haben - statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind.

Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren
- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle

> **Hinweis:**
>
> Um MAC-Verschiebungen und Schnittstellenstummschaltung in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden. Weitere Informationen finden Sie im

> Artikel CTX224626 .

Multi-IP-Architektur mit einer NIC

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit mehreren IP-Konfigurationen verknüpft - statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind. Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren
- Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz über PowerShell-Befehle konfigurieren

Einzelne NIC-Einzel-IP

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit einer einzigen IP-Adresse verknüpft, die zur Ausführung der Funktionen von NSIP, SNIP und VIP verwendet wird.

Weitere Informationen finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz.

> **Hinweis:**
>
> Der einzelne IP-Modus ist nur in Azure-Bereitstellungen verfügbar. Dieser Modus ist für eine NetScaler VPX-Instance in Ihren Räumlichkeiten, in AWS oder in anderen Bereitstellungsarten nicht verfügbar.

NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz auf Azure benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf Azure ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: NetScaler VPX Appliances sind als kostenpflichtige Instanzen auf Azure Marketplace verfügbar. Abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet.

  > **Hinweis:**
  >
  > Bei Abonnementlizenzinstanzen gilt Ihre Abonnementabrechnung für den gesamten Lizenzzeitraum für ein bestimmtes Lizenzmodell. Aufgrund von Cloud-Einschränkungen unterstützt Azure das Ändern oder Entfernen des für Ihr Abonnement geltenden Lizenzmodells nicht. Um eine Abonnementlizenz zu ändern oder zu entfernen, löschen Sie die vorhandene ADC-VM und erstellen Sie eine neue ADC-VM mit der erforderlichen Lizenz neu.

NetScaler bietet technischen Support für Abonnementlizenzinstanzen. Informationen zum Einreichen eines Supportfalls finden Sie unter Unterstützung für NetScaler auf Azure — Abonnementlizenz mit Stundenpreis.

- **Bringen Sie Ihre eigene Lizenz (BYOL) mit**: Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, finden Sie weitere Informationen im VPX-Lizenzierungsleitfaden unter http://support.citrix.com/article/CTX122426. Sie müssen:
  - Verwenden Sie das Lizenzierungsportal auf der NetScaler-Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.

  > **Hinweis**
  >
  > In einer Azure-Stack-Umgebung ist **BYOL** die einzig verfügbare Lizenzierungsoption.

- **NetScaler VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter NetScaler VPX Check-In/Auschecken Lizenzierung.

  Ab NetScaler Version 12.0 56.20 benötigt NetScaler VPX Express für on-premises und Cloud-Bereitstellungen keine Lizenzdatei. Weitere Informationen zu NetScaler VPX Express finden Sie im Abschnitt “NetScaler VPX Express-Lizenz”in der Übersicht über die NetScaler Lizenzierung.

VPX-Leistung und empfohlene Azure-Instanztypen

Für die gewünschte VPX-Leistung werden die folgenden Azure-Instanztypen empfohlen.

VPX-Leistung	Azure-Instanztypen		
	VPX 1 NIC/2 NIC	VPX 3 Netzwerkkarte	VPX bis zu 8 NIC
Bis zu 200 Mbit/s	Standard_D2s_v4, Standard_DS3_v2, Standard_DS4_v2, Standard_DS3_v2, Standard_DS4_v2		
Bis zu 1 Gbit/s	Standard_D4s_v4, Standard_DS3_v2, Standard_DS4_v2, Standard_DS3_v2, Standard_DS4_v2		
Bis zu 5 Gbit/s	Standard_D8s_v5, Standard_D8s_v5, Standard_DS4_v2, Standard_D8s_v5, Standard_D8s_v5, Standard_DS4_v2		
Bis zu 10 Gbit/s	Standard_D2s_v5, Standard_D8s_v5, Standard_D16_v5		

Punkte zu beachten

- Um auf NetScaler VPX-Instanzen mit 1 Gbit/s und 5 Gbit/s Durchsatz eine optimale Leistung zu erzielen, müssen Sie den beschleunigten Azure-Netzwerkbetrieb aktivieren.

  Weitere Informationen zum Konfigurieren des beschleunigten Netzwerkbetriebs finden Sie unter Konfigurieren einer NetScaler VPX-Instanz für die Verwendung des beschleunigten Azure-Netzwerkbetriebs.

- Unabhängig von der abonnementbasierten Stundenlizenz, die von Azure Marketplace gekauft wurde, wird in seltenen Fällen die NetScaler VPX Instanz, die in Azure bereitgestellt wird, möglicherweise mit einer standardmäßigen NetScaler-Lizenz geliefert. Dies geschieht aufgrund von Problemen mit dem Azure Instance Metadata Service (IMDS).
- Führen Sie einen Warmstart durch, bevor Sie eine Konfigurationsänderung an der NetScaler VPX-Instanz vornehmen, um die richtige NetScaler VPX-Lizenz zu aktivieren.

IPv6-Unterstützung für die NetScaler VPX-Instanz in Azure

Ab Version 13.1-21.x unterstützt die eigenständige NetScaler VPX-Instanz IPv6-Adressen in Azure. Sie können die IPv6-Adressen als VIP- und SNIP-Adressen auf der eigenständigen NetScaler VPX-Instanz in der Azure Cloud konfigurieren.

Informationen zum Aktivieren von IPv6 in Azure finden Sie in der folgenden Azure-Dokumentation:

- Was ist IPv6 für Azure Virtual Network?
- IPv6 zu einer IPv4-Anwendung im virtuellen Azure-Netzwerk hinzufügen —Azure CLI
- Typen von Adressen

Informationen zur Unterstützung von IPv6 durch das NetScaler-Gerät finden Sie unter Internetprotokoll, Version 6,.

IPv6-Einschränkungen:

- IPv6-Bereitstellungen in NetScaler unterstützen derzeit kein Azure-Backend-Autoscaling.
- IPv6 wird für die NetScaler VPX HA-Bereitstellung nicht unterstützt.

Einschränkungen

Die Ausführung der NetScaler VPX Load Balancing-Lösung auf ARM erlegt die folgenden Einschränkungen auf:

- Die Azure-Architektur unterstützt die folgenden NetScaler-Funktionen nicht:

  - Unentgeltliches ARP (GARP)
  - L2-Modus
  - Getaggtes VLAN
  - Dynamisches Routing
  - virtueller MAC
  - USIP
  - Clustering

> **Hinweis:**
>
> Mit der Autoscale-Funktion (Cloud-Bereitstellung) von NetScaler Application Delivery Management (ADM) unterstützen die ADC-Instanzen das Clustering auf allen Lizenzen. Weitere Informationen finden Sie unter Autoscaling von NetScaler VPX in Microsoft Azure mit NetScaler ADM.

- Wenn Sie erwarten, dass Sie die virtuelle NetScaler VPX-Maschine jederzeit herunterfahren und vorübergehend freigeben müssen, weisen Sie beim Erstellen der virtuellen Maschine eine statische interne IP-Adresse zu. Wenn Sie keine statische interne IP-Adresse zuweisen, weist Azure der virtuellen Maschine bei jedem Neustart möglicherweise eine andere IP-Adresse zu, und auf die virtuelle Maschine kann nicht zugegriffen werden.
- Azure unterstützt VPX-Durchsatz von bis zu 10 Gbit/s. Weitere Informationen finden Sie im NetScaler VPX-Datenblatt.
- Wenn Sie eine NetScaler VPX-Instanz mit einem Durchsatz von über 3 Gbit/s verwenden, stimmt der tatsächliche Netzwerkdurchsatz möglicherweise nicht mit dem in der Lizenz der Instanz angegebenen Durchsatz überein. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde könnten sich jedoch verbessern.
- Die Bereitstellungs-ID, die von Azure während der Bereitstellung virtueller Maschinen generiert wird, ist für den Benutzer in ARM nicht sichtbar. Sie können die Bereitstellungs-ID nicht verwenden, um die NetScaler VPX-Appliance auf ARM bereitzustellen.
- Die NetScaler VPX-Instanz unterstützt einen Durchsatz von 20 Mbit/s und Funktionen der Standard Edition, wenn sie initialisiert wird.
- Die NetScaler VPX-Instanzen auf Azure mit aktiviertem beschleunigtem Netzwerk bieten eine bessere Leistung. Azure-beschleunigtes Netzwerk wird ab Version 13.0 Build 76.x auf NetScaler VPX-Instanzen unterstützt. Um beschleunigtes Netzwerken auf NetScaler VPX zu aktivieren, empfiehlt Citrix, einen Azure-Instanztyp zu verwenden, der beschleunigte Netzwerke unterstützt.
- Für die Bereitstellung von Citrix Virtual Apps and Desktops kann ein virtueller VPN-Server auf einer VPX-Instanz in den folgenden Modi konfiguriert werden:

- Basismodus, in dem der Parameter `ICAOnly` des virtuellen VPN-Servers auf ON eingestellt ist. Der Basismodus funktioniert vollständig auf einer nicht lizenzierten NetScaler VPX-Instanz.
- SmartAccess-Modus, in dem der Parameter `ICAOnly` des virtuellen VPN-Servers auf OFF eingestellt ist. Der SmartAccess Modus funktioniert nur für fünf NetScaler AAA-Sitzungsbenutzer auf einer nicht lizenzierten NetScaler VPX Instanz.

> **Hinweis:**
>
> Um das SmartControl-Feature zu konfigurieren, müssen Sie eine Premium-Lizenz auf die NetScaler VPX Instanz anwenden.

Azure-Terminologie

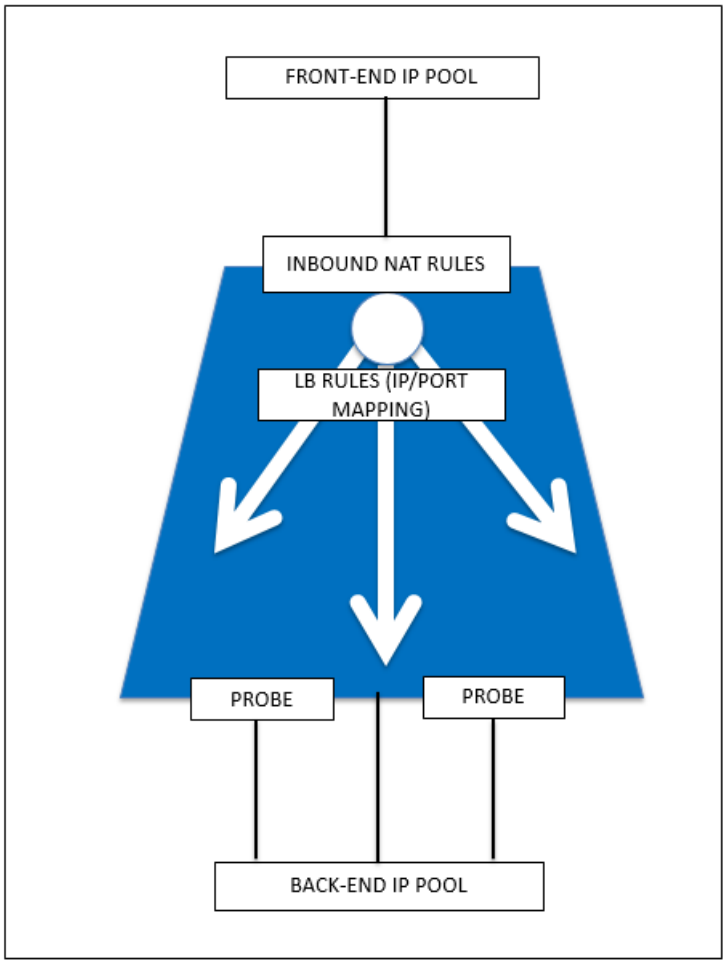
October 17, 2024

Einige der Azure-Begriffe, die in der NetScaler VPX Azure-Dokumentation verwendet werden, sind unten aufgeführt.

1. Azure Load Balancer —Azure Load Balancer ist eine Ressource, die eingehenden Datenverkehr auf Computer in einem Netzwerk verteilt. Der Datenverkehr wird auf virtuelle Maschinen verteilt, die in einem Lastausgleichssatz definiert sind. Ein Load Balancer kann extern oder mit dem Internet verbunden sein oder intern sein.
2. Azure Resource Manager (ARM) —ARM ist das neue Verwaltungsframework für Dienste in Azure. Azure Load Balancer wird mit ARM-basierten APIs und Tools verwaltet.
3. Back-End-Adresspool —Dies sind IP-Adressen, die mit der NIC (NIC) der virtuellen Maschine verknüpft sind, auf die die Last verteilt wird.
4. BLOB - Binary Large Object —Jedes binäre Objekt wie eine Datei oder ein Image, das im Azure-Speicher gespeichert werden kann.
5. Front-End-IP-Konfiguration —Ein Azure Load Balancer kann eine oder mehrere Front-End-IP-Adressen enthalten, die auch als virtuelle IPs (VIPs) bezeichnet werden. Diese IP-Adressen dienen als Eindringen für den Datenverkehr.
6. Öffentliche IP (ILPIP) auf Instanz-Ebene —Eine ILPIP ist eine öffentliche IP-Adresse, die Sie Ihrer virtuellen Maschine oder Rolleninstanz direkt zuweisen können und nicht dem Clouddienst, in dem sich die virtuelle Maschine oder Rolleninstanz befindet. Dies tritt nicht an die Stelle der VIP (virtuelle IP), die Ihrem Cloud-Dienst zugewiesen ist. Vielmehr handelt es sich um eine zusätzliche IP-Adresse, die Sie verwenden können, um eine direkte Verbindung mit Ihrer virtuellen Maschine oder Rolleninstanz herzustellen.

> **Hinweis:**
>
> Früher wurde ein ILPIP als PIP bezeichnet, was für Public IP steht.

7. Eingehende NAT-Regeln —Dies enthält Regeln, die einen öffentlichen Port auf dem Load Balancer einem Port für eine bestimmte virtuelle Maschine im Back-End-Adresspool zuordnen.
8. IP-config - Es kann als ein IP-Adresspaar (öffentliche IP und private IP) definiert werden, das mit einer einzelnen NIC verknüpft ist. In einer IP-Konfiguration kann die öffentliche IP-Adresse NULL sein. Jeder NIC kann mehrere IP-Konfig zugeordnet sein, was bis zu 255 betragen kann.
9. Lastenausgleichsregeln —Eine Regeleigenschaft, die eine gegebene Front-End-IP- und Port-Kombination einer Reihe von Back-End-IP-Adressen und einer Portkombination zuordnet. Mit einer einzelnen Definition einer Load Balancer-Ressource können Sie mehrere Load Balancing-Regeln definieren, wobei jede Regel eine Kombination aus Front-End-IP und Port sowie Back-End-IP und Port widerspiegelt, die virtuellen Maschinen zugeordnet sind.



10. Netzwerksicherheitsgruppe —Enthält eine Liste von Zugriffssteuerungslisten (ACL) -Regeln, die den Netzwerkverkehr für Ihre Instanzen der virtuellen Maschine in einem virtuellen Netzw-

erk zulassen oder verweigern. NSGs können entweder Subnetzen oder einzelnen Instanzen virtueller Maschinen innerhalb dieses Subnetzes zugeordnet werden. Wenn eine Netzwerksicherheitsgruppe mit einem Subnetz verknüpft ist, gelten die ACL-Regeln für alle Instanzen der virtuellen Maschine in diesem Subnetz. Darüber hinaus kann der Datenverkehr zu einer einzelnen virtuellen Maschine weiter eingeschränkt werden, indem eine Netzwerksicherheitsgruppe direkt mit dieser virtuellen Maschine verknüpft wird.

11. Private IP-Adressen —Wird für die Kommunikation innerhalb eines virtuellen Azure-Netzwerks und Ihres lokalen Netzwerks verwendet, wenn Sie ein VPN-Gateway verwenden, um Ihr Netzwerk auf Azure zu erweitern. Private IP-Adressen ermöglichen es Azure-Ressourcen, mit anderen Ressourcen in einem virtuellen Netzwerk oder einem lokalen Netzwerk über ein VPN-Gateway oder eine ExpressRoute-Schaltung zu kommunizieren, ohne eine vom Internet erreichbare IP-Adresse zu verwenden. Im Azure Resource Manager Bereitstellungsmodell ist eine private IP-Adresse den folgenden Arten von Azure-Ressourcen zugeordnet: virtuelle Maschinen, interne Lastausgleichsdienste (ILBs) und Anwendungsgateways.

12. Prüfpunkte —Dies enthält Integritätstprobes, die zur Überprüfung der Verfügbarkeit von Instanzen virtueller Maschinen im Back-End-Adresspool verwendet werden. Wenn eine bestimmte virtuelle Maschine für einige Zeit nicht auf Health Probes reagiert, wird sie aus dem Datenverkehr genommen. Mithilfe von Prüfpunkten können Sie den Zustand virtueller Instanzen verfolgen. Wenn ein Integritätstest fehlschlägt, wird die virtuelle Instanz automatisch aus der Rotation genommen.

13. Öffentliche IP-Adressen (PIP) —PIP wird für die Kommunikation mit dem Internet verwendet, einschließlich öffentlicher Azure-Dienste und ist mit virtuellen Maschinen, mit Internetzugang verbundenen Lastausgleichsdiensten, VPN-Gateways und Anwendungsgateways verknüpft.

14. Region - Ein Gebiet innerhalb einer Geographie, das keine nationalen Grenzen überschreitet und ein oder mehrere Rechenzentren enthält. Preise, regionale Dienstleistungen und Angebotsarten werden auf regionaler Ebene angezeigt. Eine Region wird in der Regel mit einer anderen Region gepaart, die bis zu mehreren hundert Meilen entfernt sein kann, um ein regionales Paar zu bilden. Regionale Paare können als Mechanismus für Disaster Recovery und Hochverfügbarkeitsszenarien verwendet werden. Auch allgemein als Standort bezeichnet.

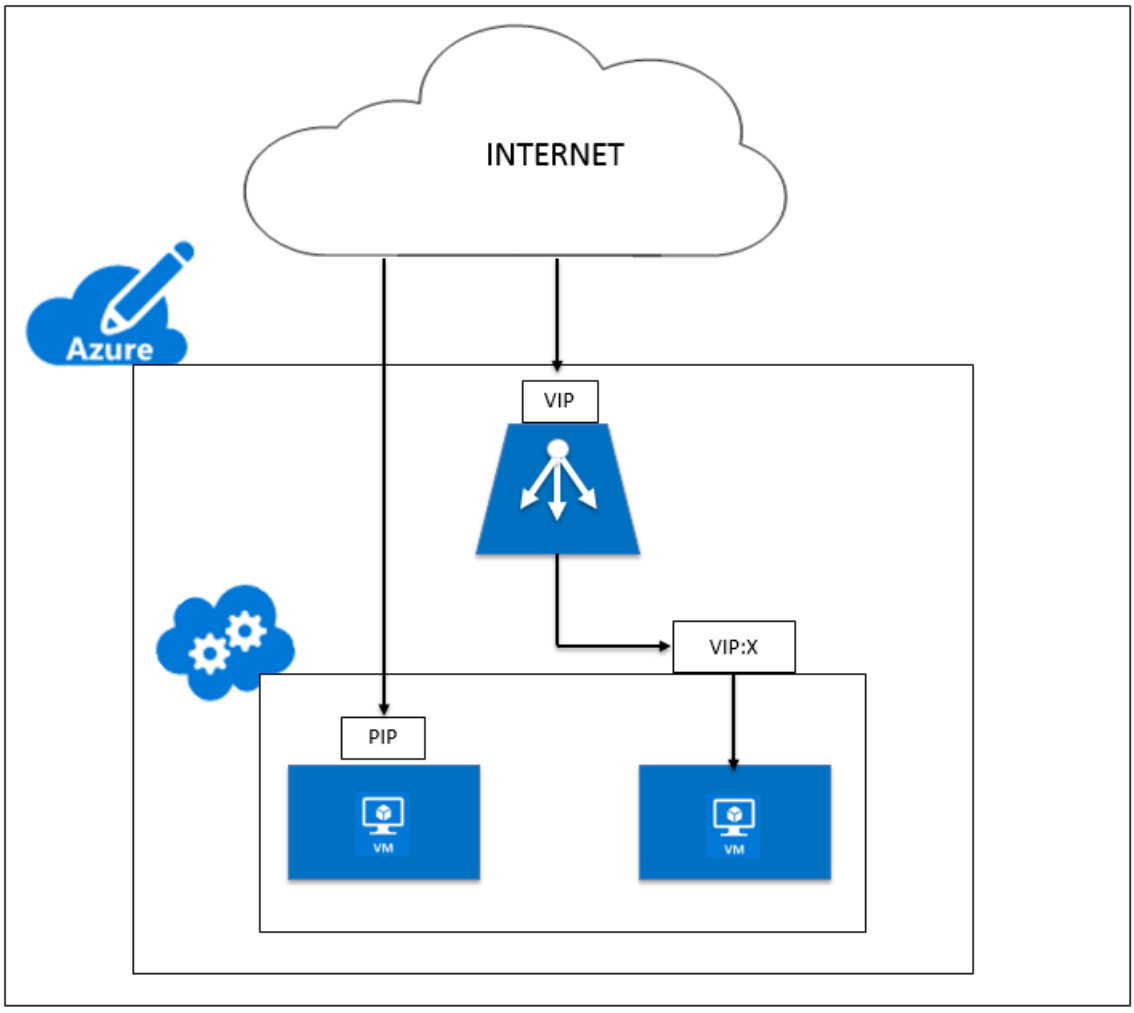
15. Ressourcengruppe - Ein Container im Ressourcen-Manager enthält zugehörige Ressourcen für eine Anwendung. Die Ressourcengruppe kann alle Ressourcen für eine Anwendung oder nur die Ressourcen enthalten, die logisch zusammengefasst sind.

16. Speicherkonto —Mit einem Azure-Speicherkonto können Sie auf den Azure-BLOB, die Warteschlange, die Tabelle und die Dateidienste in Azure Storage zugreifen. Ihr Speicherkonto stellt den eindeutigen Namespace für Ihre Azure-Speicherdatenobjekte bereit.

17. Virtuelle Maschine —Die Software-Implementierung eines physischen Computers, auf dem ein Betriebssystem ausgeführt wird. Mehrere virtuelle Maschinen können gleichzeitig auf

derselben Hardware ausgeführt werden. In Azure sind virtuelle Maschinen in einer Vielzahl von Größen verfügbar.

18. Virtuelles Netzwerk - Ein virtuelles Azure-Netzwerk ist eine Darstellung Ihres eigenen Netzwerks in der Cloud. Es handelt sich um eine logische Isolierung der Azure-Cloud, die Ihrem Abonnement gewidmet ist. Sie können die IP-Adressblöcke, DNS-Einstellungen, Sicherheitsrichtlinien und Routingtabellen in diesem Netzwerk vollständig steuern. Sie können Ihr VNet auch weiter in Subnetze segmentieren und virtuelle Azure IaaS-Maschinen und Clouddienste (PaaS-Rolleninstanzen) starten. Darüber hinaus können Sie das virtuelle Netzwerk mit Ihrem lokalen Netzwerk verbinden, indem Sie eine der in Azure verfügbaren Konnektivitätsoptionen verwenden. Im Wesentlichen können Sie Ihr Netzwerk auf Azure erweitern, mit vollständiger Kontrolle über IP-Adressblöcke mit dem Vorteil, dass Azure Enterprise Scale bietet.



Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure

October 17, 2024

In Azure Resource Manager (ARM) befindet sich eine virtuelle NetScaler VPX-Maschine (VM) in einem virtuellen Netzwerk. Eine einzelne Netzwerkschnittstelle kann in einem bestimmten Subnetz des virtuellen Netzwerks erstellt werden und kann an die VPX-Instanz angehängt werden. Sie können den Netzwerkverkehr von und zu einer VPX-Instanz in einem virtuellen Azure-Netzwerk mit einer Netzwerksicherheitsgruppe filtern. Eine Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zu oder ausgehenden Netzwerkverkehr von einer VPX-Instanz zulassen oder ablehnen. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Die Netzwerksicherheitsgruppe filtert die Anforderungen an die NetScaler VPX-Instanz, und die VPX-Instanz sendet sie an die Server. Die Antwort von einem Server folgt dem gleichen Pfad in umgekehrter Richtung. Die Netzwerksicherheitsgruppe kann so konfiguriert werden, dass eine einzelne VPX-VM gefiltert wird oder mit Subnetzen und virtuellen Netzwerken Datenverkehr bei der Bereitstellung mehrerer VPX-Instanzen filtert werden kann.

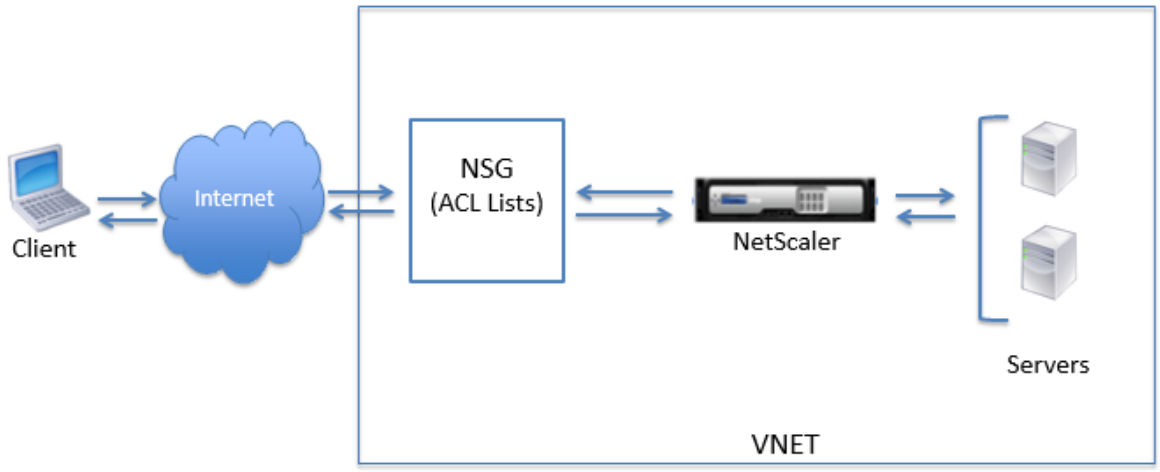
Die NIC enthält Netzwerkkonfigurationsdetails wie das virtuelle Netzwerk, Subnetze, interne IP-Adresse und öffentliche IP-Adresse.

Bei ARM sollten Sie die folgenden IP-Adressen kennen, die für den Zugriff auf die VMs verwendet werden, die mit einer einzelnen Netzwerkkarte und einer einzelnen IP-Adresse bereitgestellt werden:

- Öffentliche IP-Adresse (PIP) ist die IP-Adresse, die direkt auf der virtuellen Netzwerkkarte der NetScaler VM konfiguriert wurde. Auf diese Weise können Sie direkt über das externe Netzwerk auf eine VM zugreifen.
- Die NetScaler IP (auch NSIP genannt) Adresse ist die interne IP-Adresse, die auf der VM konfiguriert ist. Es ist nicht routingfähig.
- Die virtuelle IP-Adresse (VIP) wird mithilfe des NSIP und einer Portnummer konfiguriert. Clients greifen über die PIP-Adresse auf NetScaler-Dienste zu, und wenn die Anforderung die Netzwerkkarte der NetScaler VPX-VM oder des Azure-Load Balancers erreicht, wird der VIP in interne IP (NSIP) und interne Portnummer übersetzt.
- Interne IP-Adresse ist die private interne IP-Adresse der VM aus dem Adress-Space-Pool des virtuellen Netzwerks. Diese IP-Adresse kann nicht vom externen Netzwerk aus erreicht werden. Diese IP-Adresse ist standardmäßig dynamisch, es sei denn, Sie setzen sie auf statisch. Der Datenverkehr aus dem Internet wird gemäß den Regeln, die in der Netzwerksicherheitsgruppe erstellt wurden, an diese Adresse weitergeleitet. Die Netzwerksicherheitsgruppe lässt sich in die Netzwerkkarte integrieren, um selektiv den richtigen Datenverkehr an den richtigen Port der NIC zu senden, was von den auf der VM konfigurierten Diensten abhängt.

Die folgende Abbildung zeigt, wie der Datenverkehr von einem Client zu einem Server über eine in

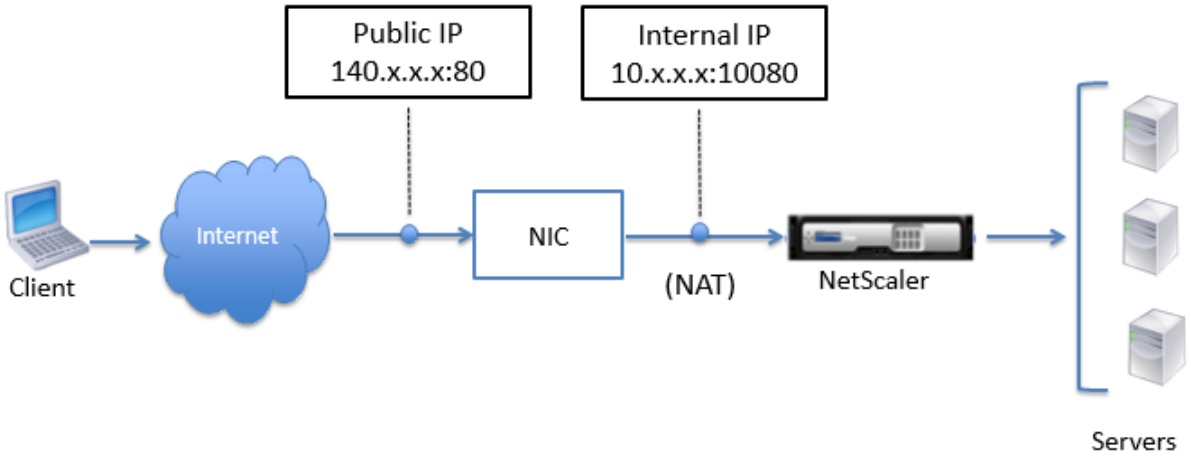
ARM bereitgestellte NetScaler VPX-Instanz fließt.



Verkehrsfluss durch Netzwerkadressübersetzung

Sie können auch eine öffentliche IP-Adresse (PIP) für Ihre NetScaler VPX-Instanz (Instanzebene) anfordern. Wenn Sie diese direkte PIP auf VM-Ebene verwenden, müssen Sie keine eingehenden und ausgehenden Regeln definieren, um den Netzwerkverkehr abzufangen. Die eingehende Anforderung aus dem Internet wird direkt auf der VM empfangen. Azure führt Network Address Translation (NAT) durch und leitet den Datenverkehr an die interne IP-Adresse der VPX-Instanz weiter.

Die folgende Abbildung zeigt, wie Azure Netzwerkadressübersetzung zur Zuordnung der internen NetScaler IP-Adresse durchführt.



In diesem Beispiel ist die der Netzwerksicherheitsgruppe zugewiesene öffentliche IP 140.xxx und die interne IP-Adresse 10.xxx. In diesem Beispiel lautet die der Netzwerksicherheitsgruppe zugewiesene öffentliche IP 140.x.x.x und die interne IP-Adresse 10.x.x.x. Wenn die eingehenden und ausgehenden

Regeln definiert sind, wird der öffentliche HTTP-Port 80 als Port definiert, auf dem die Clientanforderungen empfangen werden, und ein entsprechender privater Port, 10080, wird als Port definiert, auf dem die NetScaler VPX-Instanz wartet. Die Clientanforderung wird unter der öffentlichen IP-Adresse (140.x.x.x) empfangen. Azure führt die Netzwerkadressübersetzung durch, um das PIP der internen IP-Adresse 10.x.x.x an Port 10080 zuordnen, und leitet die Clientanforderung weiter.

> **Hinweis:**
>
> NetScaler VPX-VMs mit hoher Verfügbarkeit werden von externen oder internen Load Balancern gesteuert, auf denen eingehende Regeln zur Steuerung des Load-Balancing-Datenverkehrs definiert sind. Der externe Datenverkehr wird zuerst von diesen Lastausgleichsdiensten abgefangen, und der Datenverkehr wird entsprechend den konfigurierten Lastausgleichsregeln umgeleitet, bei denen Back-End-Pools, NAT-Regeln und Integritätstprobes auf den Lastausgleichsdiensten definiert sind.

Richtlinien zur Port-Nutzung

Sie können weitere eingehende und ausgehende Regeln n Netzwerksicherheitsgruppen konfigurieren, während Sie die NetScaler VPX-Instanz erstellen oder nachdem die virtuelle Maschine bereitgestellt wurde. Jede eingehende und ausgehende Regel ist einem öffentlichen und einem privaten Port zugeordnet.

Beachten Sie vor der Konfiguration der Regeln für Netzwerksicherheitsgruppen die folgenden Richtlinien bezüglich der Portnummern, die Sie verwenden können:

1. Die NetScaler VPX-Instanz reserviert die folgenden Ports. Sie können diese nicht als private Ports definieren, wenn Sie die öffentliche IP-Adresse für Anfragen aus dem Internet verwenden.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Wenn Sie jedoch möchten, dass Internetdienste wie der VIP einen Standardport verwenden (z. B. Port 443), müssen Sie mithilfe der Netzwerksicherheitsgruppe eine Portzuordnung erstellen. Der Standardport wird dann einem anderen Port zugeordnet, der auf dem NetScaler für diesen VIP-Dienst konfiguriert ist.

   Beispielsweise kann ein VIP-Dienst auf Port 8443 der VPX-Instanz ausgeführt werden, wird aber dem öffentlichen Port 443 zugeordnet. Wenn der Benutzer also über die Public IP auf Port 443 zugreift, wird die Anforderung an den privaten Port 8443 weitergeleitet.
2. Öffentliche IP-Adresse unterstützt keine Protokolle, in denen die Portzuordnung dynamisch geöffnet wird, z. B. passives FTP oder ALG.
3. Hochverfügbarkeit funktioniert nicht für Datenverkehr, der eine öffentliche IP-Adresse (PIP) verwendet, die einer VPX-Instanz zugeordnet ist, anstelle eines auf dem Azure-Load Balancer kon-

figurierten PIP.

> **Hinweis:**
>
> In Azure Resource Manager ist eine NetScaler VPX-Instanz zwei IP-Adressen zugeordnet - eine öffentliche IP-Adresse (PIP) und eine interne IP-Adresse. Während der externe Datenverkehr mit dem PIP verbunden ist, ist die interne IP-Adresse oder der NSIP nicht routingfähig. Um VIP in VPX zu konfigurieren, verwenden Sie die interne IP-Adresse und einen der freien Ports. Verwenden Sie nicht die PIP, um VIP zu konfigurieren.

Eigenständige NetScaler VPX-Instanz konfigurieren

October 17, 2024

Sie können eine einzelne NetScaler VPX-Instanz im Azure Resource Manager (ARM) -Portal in einem eigenständigen Modus bereitstellen, indem Sie die virtuelle Maschine erstellen und andere Ressourcen konfigurieren.

Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager
- Microsoft Azure-SDK
- Microsoft Azure PowerShell

Melden Sie sich auf der Seite Microsoft Azure-Portal beim Azure Resource Manager-Portal an, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben.

> **Hinweis:**
>
> Wenn Sie im ARM-Portal auf eine Option in einem Bereich klicken, wird rechts ein neuer Bereich geöffnet. Navigieren Sie von einem Bereich zum anderen, um Ihr Gerät zu konfigurieren.

Zusammenfassung der Konfigurationsschritte

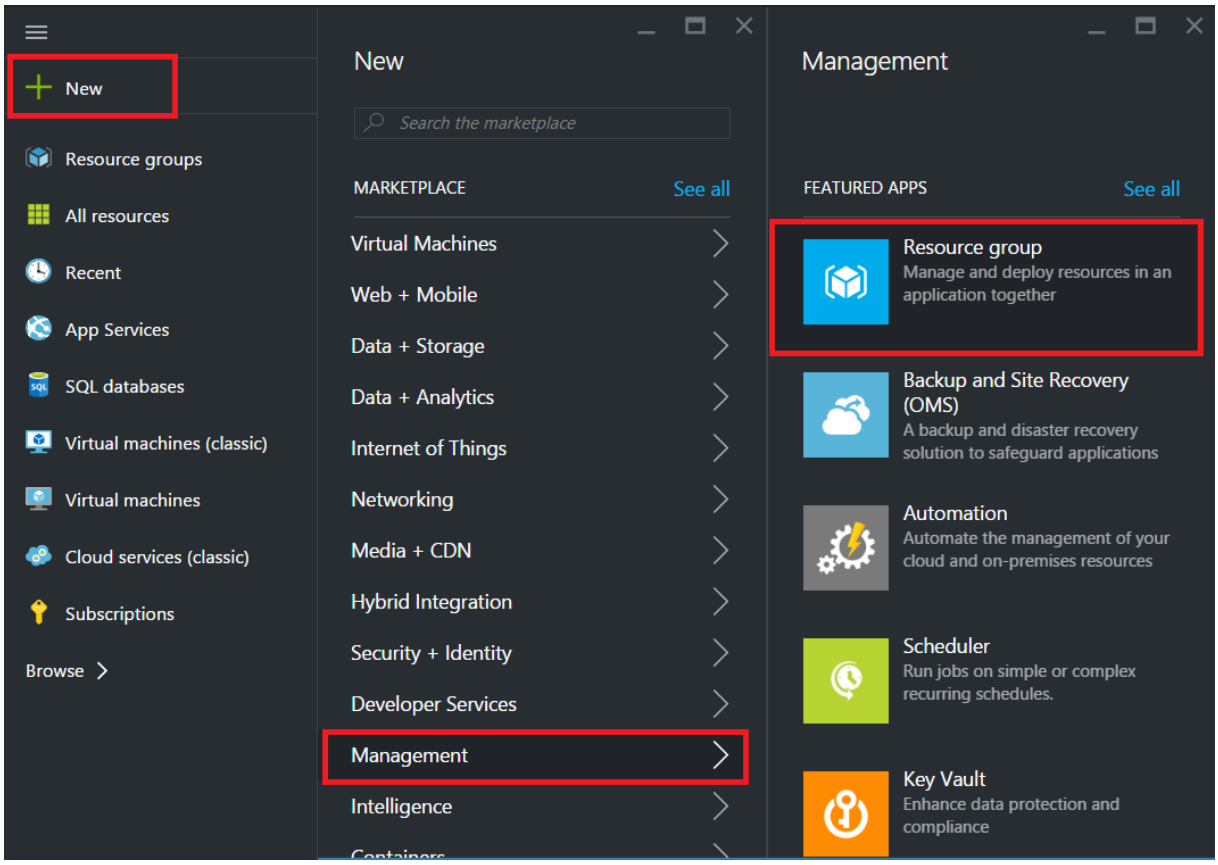
1. Eine Ressourcengruppe konfigurieren
2. Konfigurieren einer Netzwerksicherheitsgruppe
3. Virtuelles Netzwerk und seine Subnetze konfigurieren

4. Konfigurieren eines Speicherkontos
5. Konfigurieren eines Verfügbarkeitssatzes
6. Konfigurieren Sie eine NetScaler VPX-Instanz.

Eine Ressourcengruppe konfigurieren

Erstellen Sie eine neue Ressourcengruppe, die ein Container für all Ihre Ressourcen ist. Verwenden Sie die Ressourcengruppe, um Ihre Ressourcen als Gruppe bereitzustellen, zu verwalten und zu überwachen.

1. Klicken Sie auf **Neu** > **Verwaltung** > **Ressourcengruppe**.
2. Geben Sie im Bereich **Ressourcengruppe** die folgenden Details ein:
    - Ressourcengruppenname
    - Standort der Ressourcengruppe
3. Klicken Sie auf **Erstellen**.

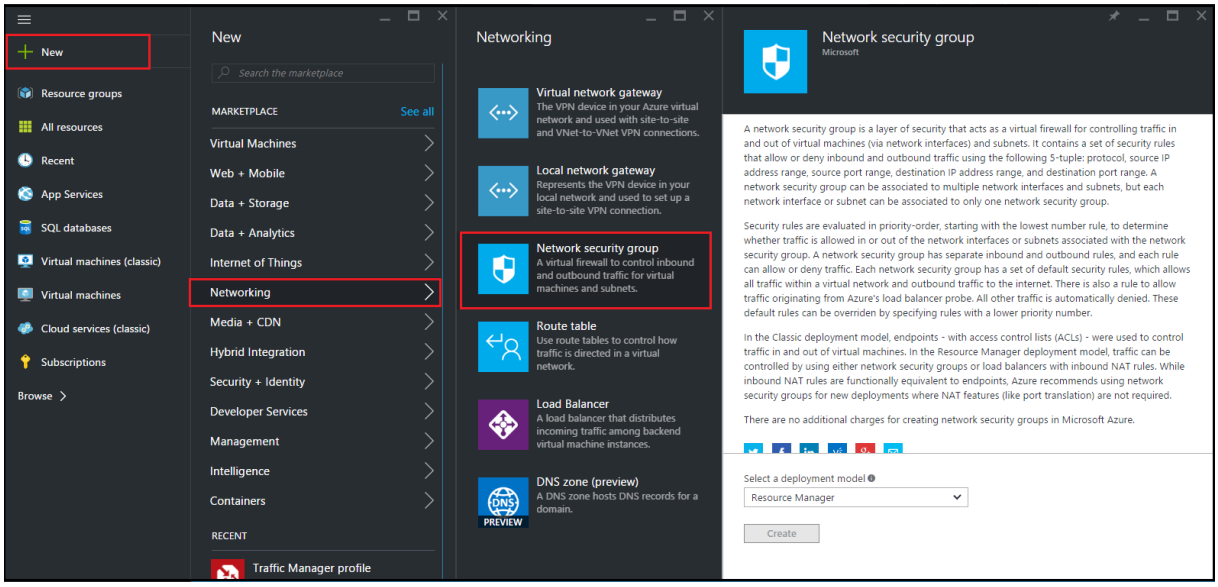


Konfigurieren einer Netzwerksicherheitsgruppe

Erstellen Sie eine Netzwerksicherheitsgruppe, um eingehende und ausgehende Regeln zuzuweisen, um den eingehenden und ausgehenden Datenverkehr innerhalb des virtuellen Netzwerks zu steuern. Mit der Netzwerksicherheitsgruppe können Sie Sicherheitsregeln für eine einzelne virtuelle Maschine definieren und Sicherheitsregeln für ein virtuelles Netzwerksubnetz definieren.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Netzwerksicherheitsgruppe**.
2. Geben **Sie im Bereich Netzwerksicherheitsgruppe erstellen** die folgenden Details ein, und klicken Sie dann auf **Erstellen**.
    - Name —geben Sie einen Namen für die Sicherheitsgruppe ein
    - Ressourcengruppe —wählen Sie die Ressourcengruppe aus der Dropdownliste aus

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den richtigen Standort ausgewählt haben. Die Liste der Ressourcen, die in der Dropdownliste angezeigt werden, unterscheidet sich für verschiedene Speicherorte.



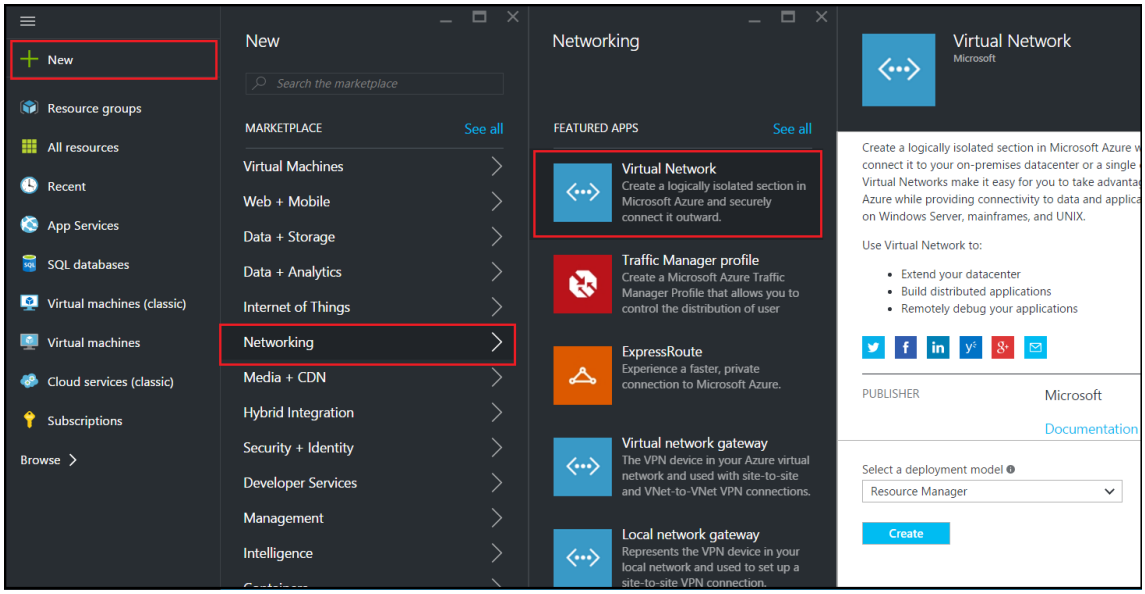
Konfigurieren eines virtuellen Netzwerks und der Subnetze

Virtuelle Netzwerke in ARM bieten eine Sicherheits- und Isolationsebene für Ihre Dienste. VMs und Dienste, die Teil desselben virtuellen Netzwerks sind, können aufeinander zugreifen.

Für diese Schritte, um ein virtuelles Netzwerk und Subnetze zu erstellen.

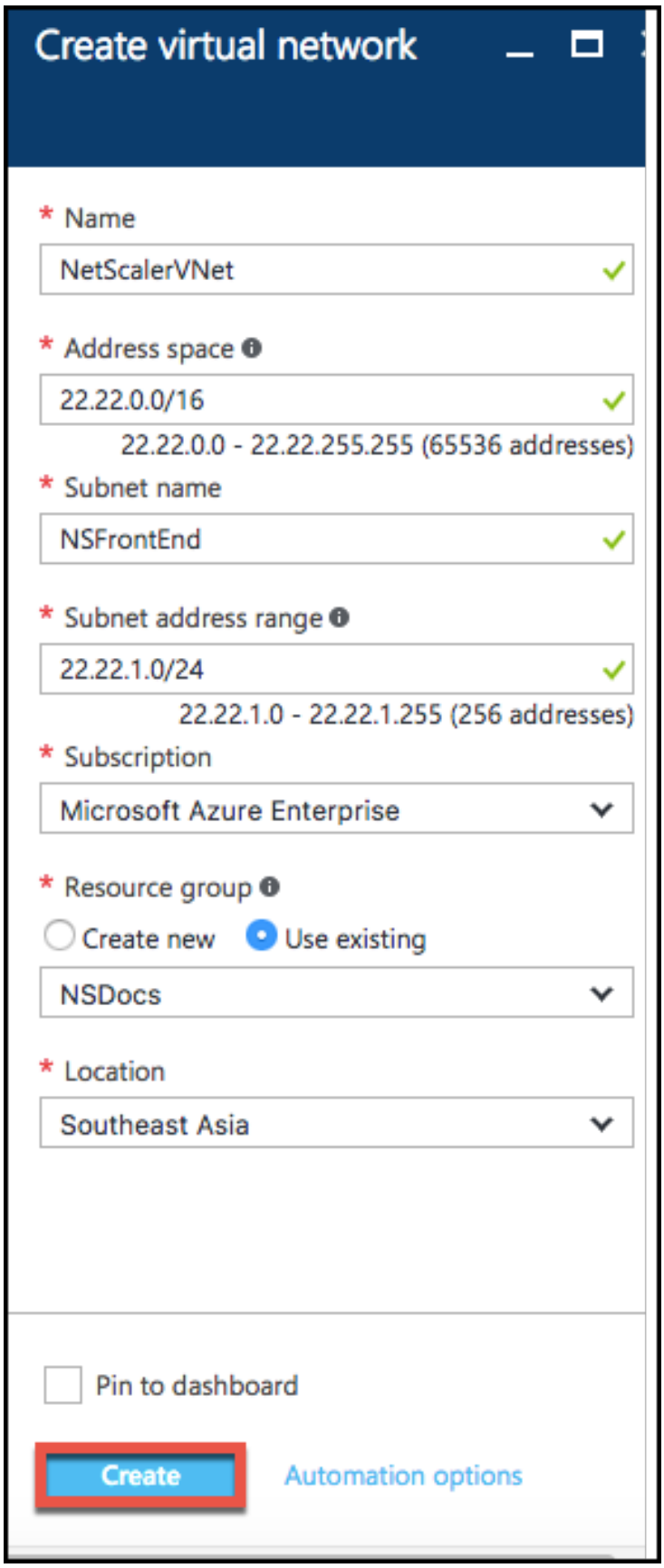
1. Klicken Sie auf **Neu** > **Netzwerk** > **Virtuelles Netzwerk**.

2. Stellen Sie im Bereich **Virtuelles Netzwerk** sicher, dass der Bereitstellungsmodus **Ressourcenmanager** ist, und klicken Sie auf **Erstellen**.



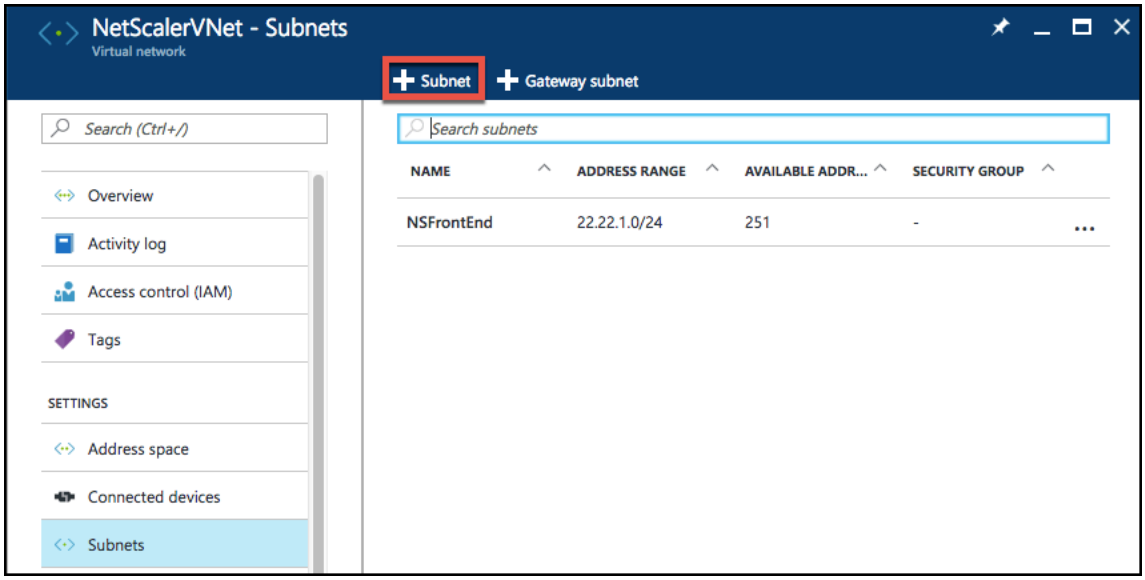
3. Geben Sie im Bereich **Virtuelles Netzwerk erstellen** die folgenden Werte ein, und klicken Sie dann auf **Erstellen**.

   - Name des virtuellen Netzwerks
   - Adressraum —geben Sie den reservierten IP-Adressblock für das virtuelle Netzwerk ein
   - Subnetz —geben Sie den Namen des ersten Subnetzes ein (das zweite Subnetz erstellen Sie später in diesem Schritt)
   - Subnetz-Adressbereich —Geben Sie den reservierten IP-Adressblock des Subnetzes ein
   - Ressourcengruppe: Wählen Sie die zuvor erstellte Ressourcengruppe aus der Dropdownliste aus



Konfigurieren des zweiten Subnetzes

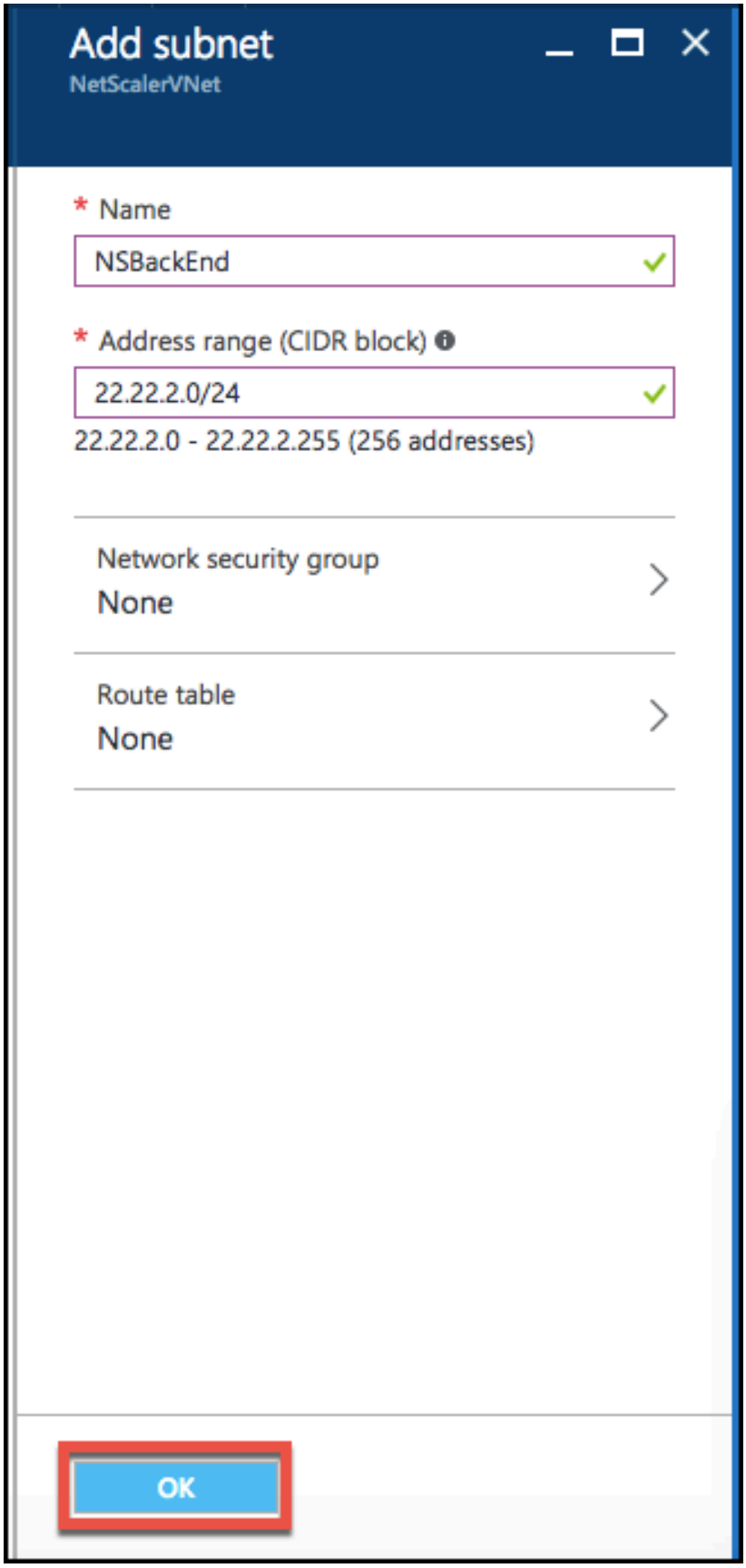
1. Wählen Sie im Bereich **Alle Ressourcen** das neu erstellte virtuelle Netzwerk aus, und klicken Sie im Bereich **Einstellungen** auf **Subnetze**.



2. Klicken Sie auf **+ Subnetz**, und erstellen Sie das zweite Subnetz, indem Sie die folgenden Details eingeben.

   - Name des zweiten Subnetzes
   - Adressbereich - Geben Sie den reservierten IP-Adressblock des zweiten Subnetzes ein
   - Netzwerksicherheitsgruppe - wählen Sie die Netzwerksicherheitsgruppe aus der Drop-downliste

3. Klicken Sie auf **Erstellen**.

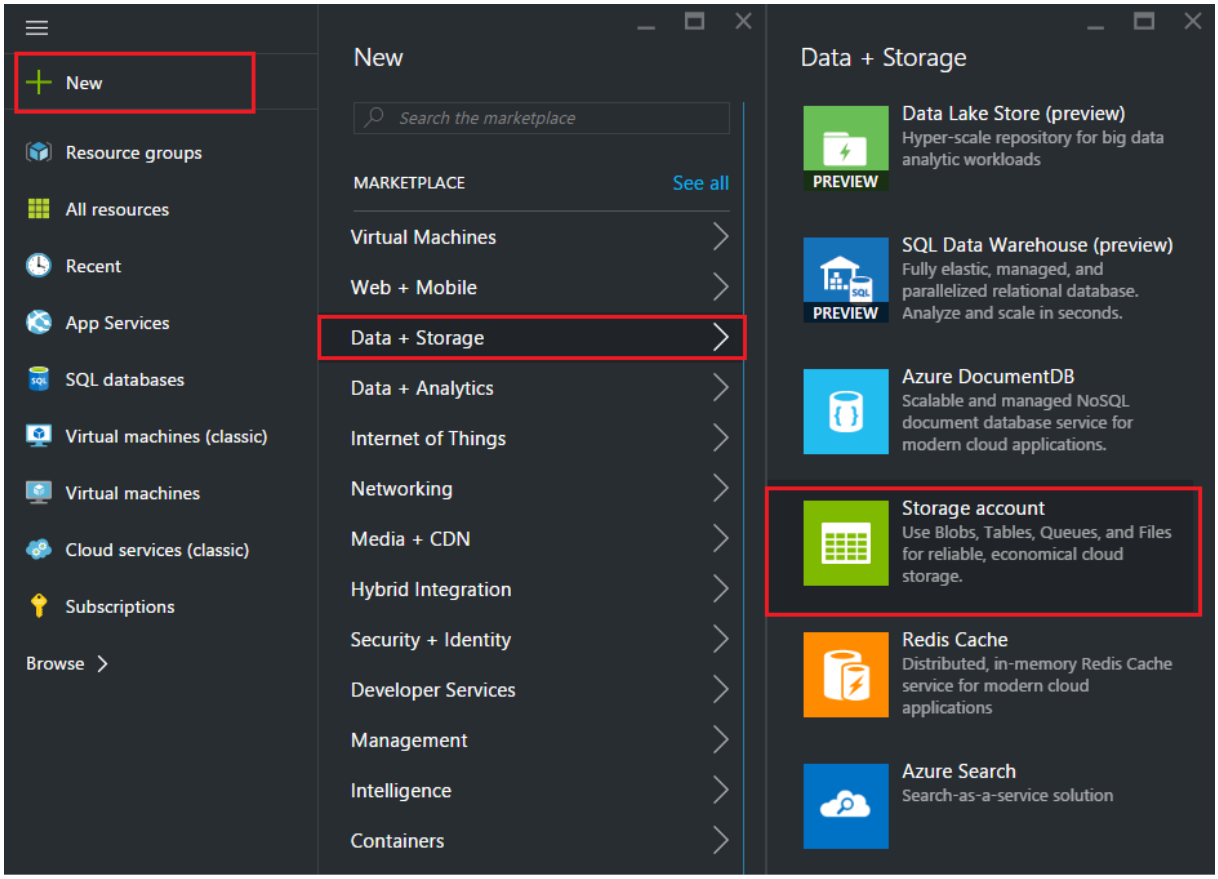


Konfigurieren eines Speicherkontos

Der ARM-IaaS-Infrastrukturspeicher umfasst alle Dienste, in denen wir Daten in Form von Blobs, Tabellen, Warteschlangen und Dateien speichern können. Sie können auch Anwendungen erstellen, die diese Formen von Speicherdaten in ARM verwenden.

Erstellen Sie ein Speicherkonto, um all Ihre Daten zu speichern.

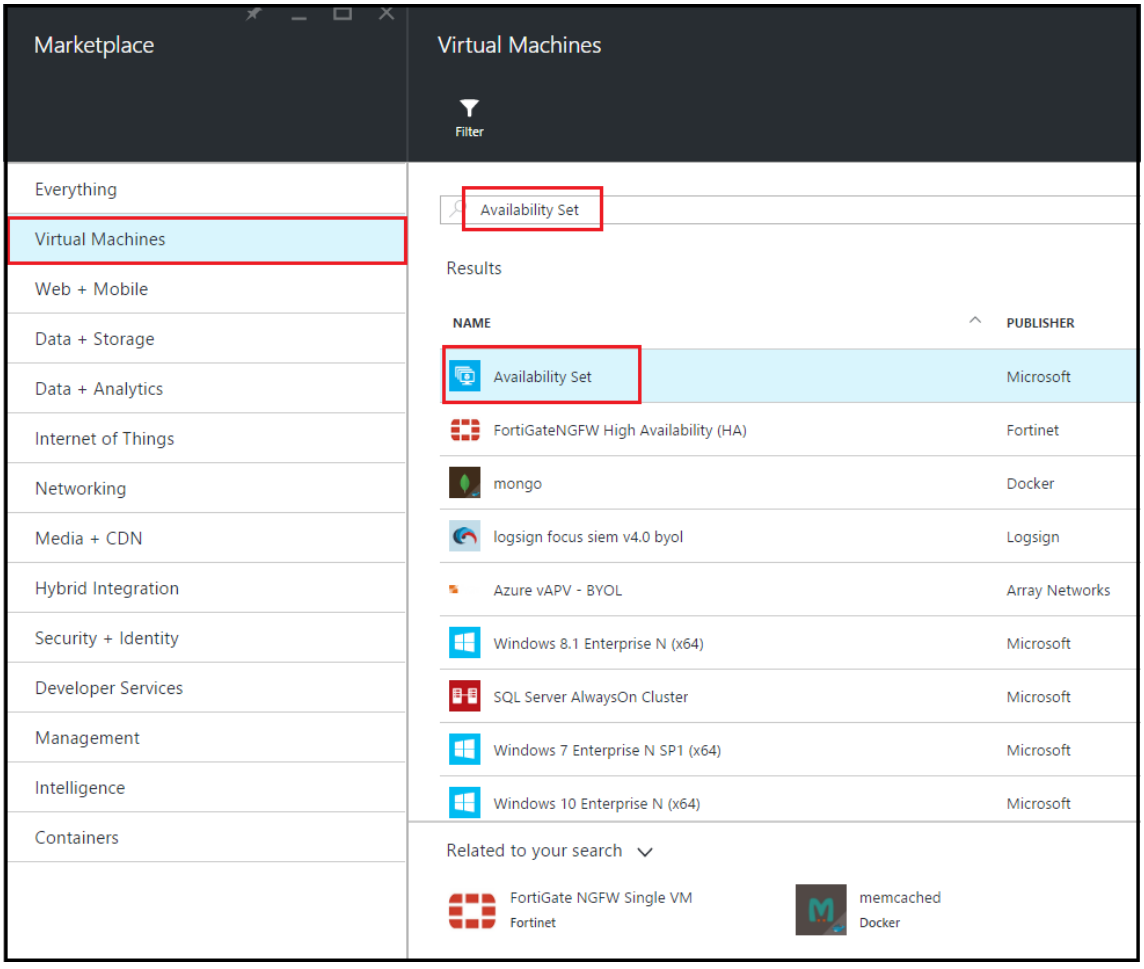
1. Klicken Sie auf **+Neu** > **Daten + Speicher** > **Speicherkonto**.
2. Geben **Sie im Bereich Speicherkonto erstellen** die folgenden Details ein:
    - Name des Accounts
    - Bereitstellungsmodus —stellen Sie sicher, dass Sie **Resource Manager**auswählen
    - Kontoart - wählen Sie **Allzweck** aus der Dropdownliste
    - Replikation —Wählen Sie **Lokal redundanter Speicher** aus der Dropdownliste aus
    - Ressourcengruppe —wählen Sie die neu erstellte Ressourcengruppe aus der Dropdownliste aus
3. Klicken Sie auf **Erstellen**.



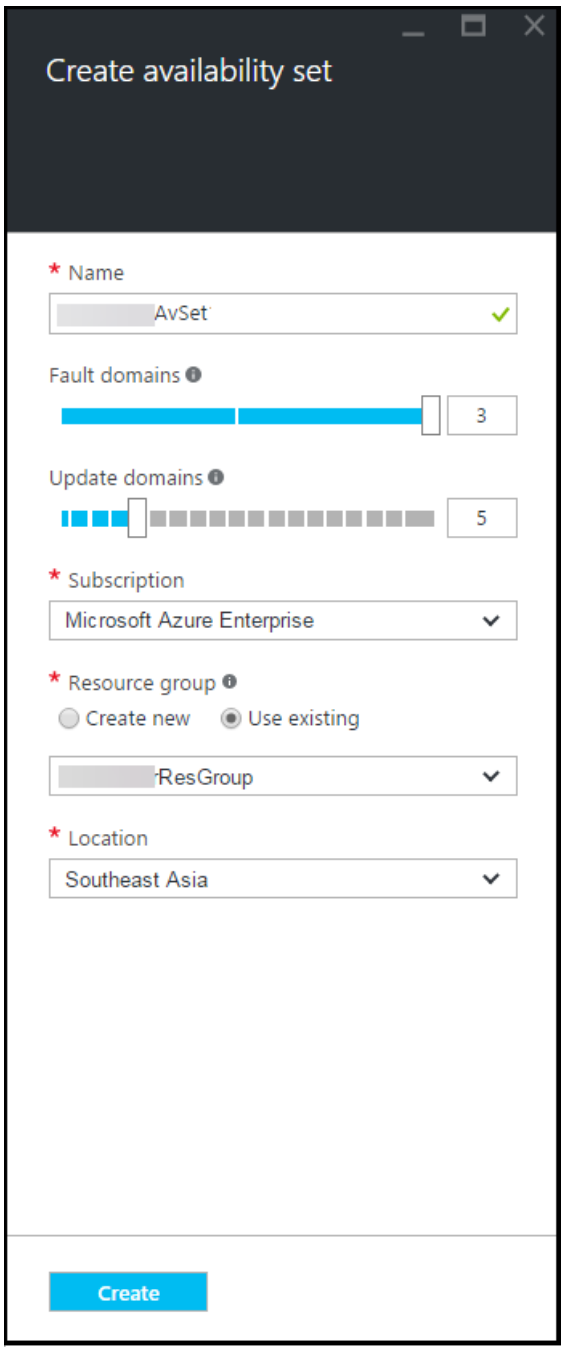
Konfigurieren eines Verfügbarkeitssatzes

Ein Verfügbarkeitsset garantiert, dass mindestens eine VM im Falle einer geplanten oder ungeplanten Wartung betriebsbereit bleibt. Zwei oder mehr VMs unter derselben „Verfügbarkeitsgruppe“werden in verschiedenen Fehlerdomänen platziert, um redundante Dienste bereitzustellen.

1. Klicken Sie auf **+Neu**.
2. Klicken **Sie im Bereich MARKETPLACE auf Alle anzeigen** und dann auf **Virtuelle Maschinen**.
3. Suchen Sie nach Verfügbarkeitssatz, und wählen Sie dann **Verfügbarkeitssatzentität** aus der angezeigten Liste aus.



4. Klicken Sie auf **Erstellen,** und geben **Sie im Bereich Verfügbarkeitssatz** erstellen die folgenden Details ein:
   - Name des Sets
   - Ressourcengruppe —wählen Sie die neu erstellte Ressourcengruppe aus der Dropdownliste aus
5. Klicken Sie auf **Erstellen**.



Konfigurieren einer NetScaler VPX-Instanz

Erstellen Sie eine Instanz von NetScaler VPX im virtuellen Netzwerk. Besorgen Sie sich das NetScaler VPX-Image vom Azure Marketplace und verwenden Sie dann das Azure Resource Manager-Portal, um eine NetScaler VPX-Instanz zu erstellen.

Bevor Sie mit der Erstellung der NetScaler VPX-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz

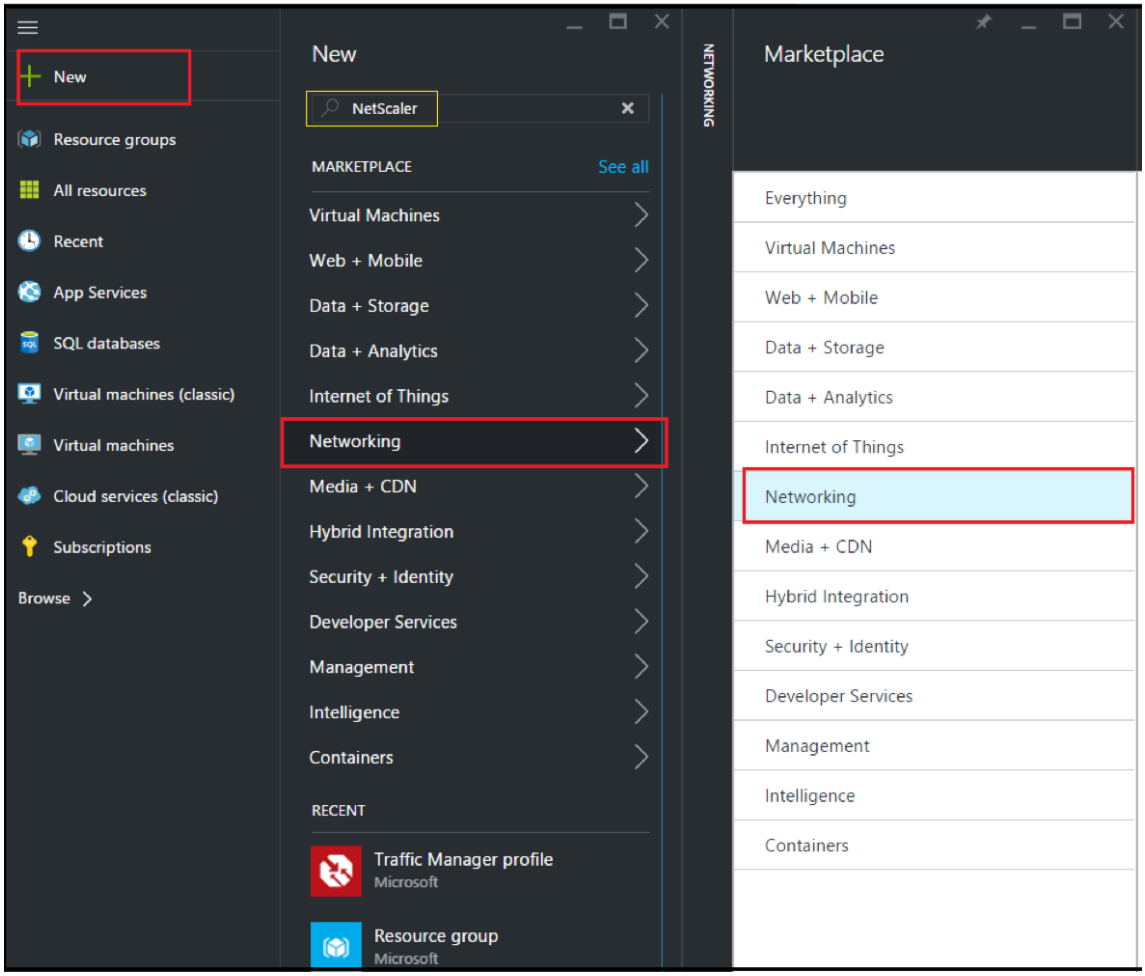
befindet. Sie können während des VM-Provisionings virtuelle Netzwerke erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze einzurichten. Hinweise zum Erstellen virtueller Netzwerke finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Konfigurieren Sie optional den DNS-Server und die VPN-Konnektivität, die es einer virtuellen Maschine ermöglichen, auf Internetressourcen zuzugreifen.

> **Hinweis:**
>
> Citrix empfiehlt, dass Sie vor der Bereitstellung der NetScaler VPX-VM eine Ressourcengruppe, eine Netzwerksicherheitsgruppe, ein virtuelles Netzwerk und andere Entitäten erstellen, damit die Netzwerkinformationen während der Bereitstellung verfügbar sind.

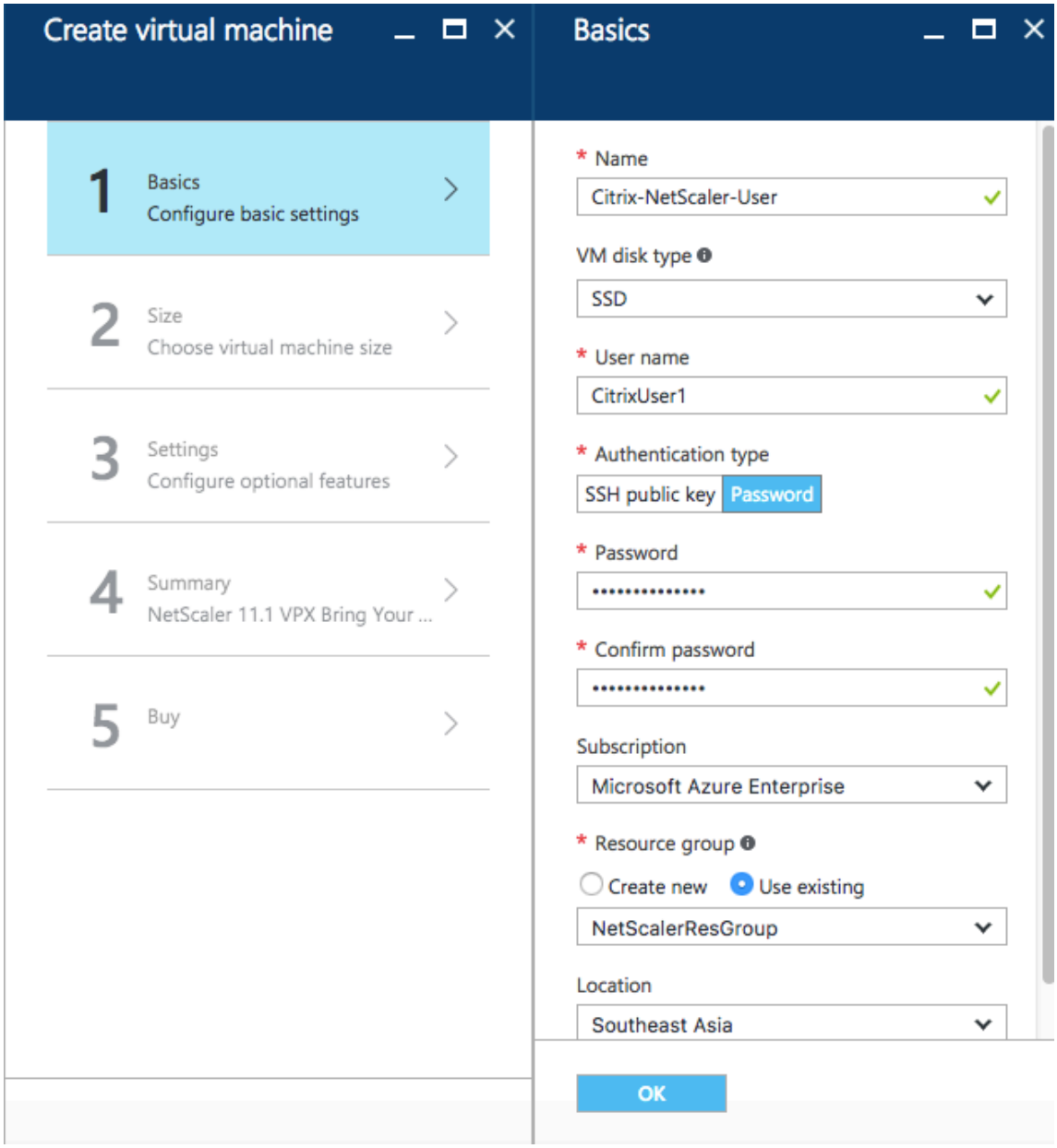
1. Klicken Sie auf **+Neu** > **Netzwerk**.
2. Klicken Sie auf **Alle anzeigen** und klicken Sie im Bereich Netzwerk auf **NetScaler 13.0**.
3. Wählen Sie **NetScaler 13.0 VPX Bring Your Own License** aus der Liste der Softwarepläne aus.

   Um schnell eine Entität im ARM-Portal zu finden, können Sie auch den Namen der Entität in das Azure Marketplace-Suchfeld eingeben und auf <Enter> drücken. Geben Sie NetScaler in das Suchfeld ein, um die NetScaler ADC-Images zu finden.



> **Hinweis:**
>
> Stellen Sie sicher, dass Sie das neueste Image auswählen. Ihr NetScaler-Image hat möglicherweise die Versionsnummer im Namen.

4. Wählen Sie auf der Seite **NetScaler VPX Bring Your Own License** aus der Dropdownliste die Option **Resource Manager** aus, und klicken Sie auf **Create**.



5. Geben Sie im Bereich **Virtuelle Maschine erstellen** in jedem Abschnitt die erforderlichen Werte an, um eine virtuelle Maschine zu erstellen. Klicken Sie in jedem Abschnitt auf **OK**, um Ihre Konfiguration zu speichern.

Grundlegend:

- Name —geben Sie einen Namen für die NetScaler VPX-Instanz an
- VM-Festplattentyp —wählen Sie SSD (Standardwert) oder HDD aus dem Drop-down-Menü
- Benutzername und Passwort —Geben Sie einen Benutzernamen und ein Passwort für den Zugriff auf die Ressourcen in der Ressourcengruppe an, die Sie erstellt haben
- Authentifizierungstyp —wählen Sie den öffentlichen SSH-Schlüssel oder das Passwort

- Ressourcengruppe —wählen Sie die von Ihnen erstellte Ressourcengruppe aus der Dropdownliste aus

Sie können hier eine Ressourcengruppe erstellen, Citrix empfiehlt jedoch, eine Ressourcengruppe aus Ressourcengruppen in Azure Resource Manager zu erstellen und die Gruppe dann aus der Dropdownliste auszuwählen.

> **Hinweis:**
>
> Geben Sie in einer Azure-Stack-Umgebung zusätzlich zu den grundlegenden Parametern die folgenden Parameter an:
>
> - Azure-Stack-Domäne
> - Azure-Stack-Mandant (optional)
> - Azure-Client (optional)
> - Azure-Clientgeheimnis (optional)

Größe:

Abhängig vom VM-Festplattentyp, SDD oder HDD, den Sie in den Grundeinstellungen ausgewählt haben, werden die Festplattengrößen angezeigt.

- Wählen Sie eine Festplattengröße entsprechend Ihren Anforderungen aus und klicken Sie auf **Auswählen**.

Einstellungen:

- Wählen Sie den Standardfestplattentyp (Standard)
- Speicherkonto —wählen Sie das Speicherkonto aus
- Virtuelles Netzwerk —wählen Sie das virtuelle Netzwerk
- Subnetz —legt die Subnetzadresse fest
- Öffentliche IP-Adresse —wählen Sie die Art der IP-Adresszuweisung aus
- Netzwerksicherheitsgruppe —Wählen Sie die Sicherheitsgruppe aus, die Sie erstellt haben. Stellen Sie sicher, dass Regeln für eingehenden und ausgehenden Datenverkehr in der Sicherheitsgruppe konfiguriert sind.
- Verfügbarkeitsset —wählen Sie das Verfügbarkeitsset aus dem Drop-down-Menüfeld aus

Zusammenfassung:

Die Konfigurationseinstellungen werden überprüft und auf der Übersichtsseite wird das Ergebnis der Überprüfung angezeigt. Schlägt die Überprüfung fehl, wird auf der Übersichtsseite die Ursache des Fehlers angezeigt. Gehen Sie zurück zum jeweiligen Abschnitt und nehmen Sie ggf. Änderungen vor. Wenn die Überprüfung erfolgreich ist, klicken Sie auf **OK**.

Kaufen:

Lesen Sie die Angebotsdetails und rechtlichen Bedingungen auf der Kaufseite und klicken Sie auf **Kaufen**.

Erstellen Sie für Hochverfügbarkeitsbereitstellungen zwei unabhängige Instanzen von NetScaler VPX in demselben Verfügbarkeitssatz und in derselben Ressourcengruppe, um sie in der aktiven Standby-Konfiguration bereitzustellen.

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren

October 17, 2024

In diesem Abschnitt wird erläutert, wie Sie eine eigenständige NetScaler VPX-Instanz mit mehreren IP-Adressen im Azure Resource Manager (ARM) konfigurieren. Der VPX-Instanz kann eine oder mehrere Netzwerkkarten angeschlossen sein, und jeder Netzwerkkarte kann eine oder mehrere statische oder dynamische öffentliche und private IP-Adressen zugewiesen sein. Sie können mehrere IP-Adressen als NSIP, VIP, SNIP usw. zuweisen.

Weitere Informationen finden Sie in der Azure-Dokumentation Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.

Wenn Sie PowerShell-Befehle verwenden möchten, finden Sie weitere Informationen unter Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

Anwendungsfall

In diesem Anwendungsfall wird eine eigenständige NetScaler VPX Appliance mit einer einzelnen Netzwerkkarte konfiguriert, die mit einem virtuellen Netzwerk (VNET) verbunden ist. Die Netzwerkkarte ist mit drei IP-Konfigurationen (ipconfig) verknüpft, wobei jeder Server einen anderen Zweck hat - wie in der Tabelle dargestellt.

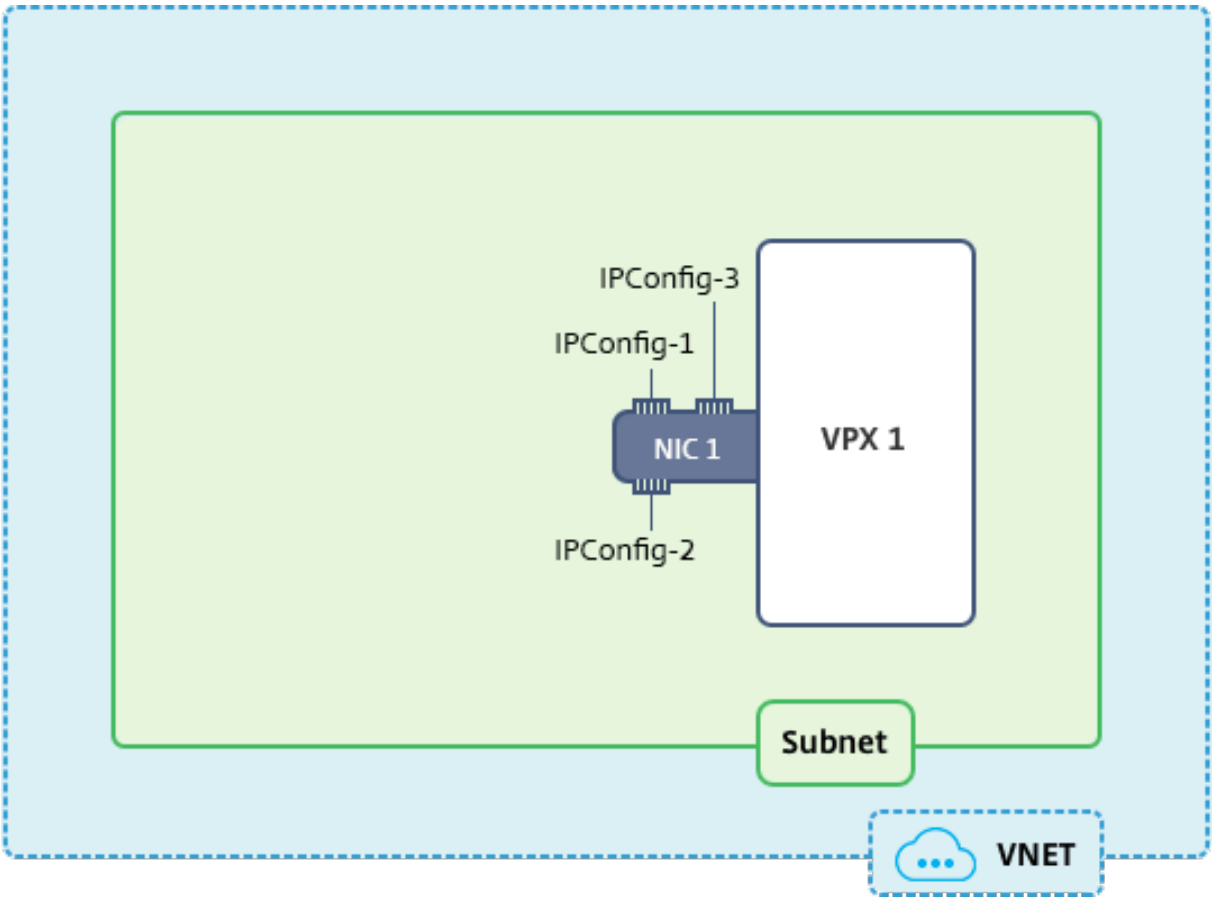
IP-Konfiguration	Verbunden mit	Zweck
ipconfig1	Statische öffentliche IP-Adresse; statische private IP-Adresse	Bedient den Verwaltungsverkehr
ipconfig2	Statische öffentliche IP-Adresse; statische private Adresse	Dient dem clientseitigen Datenverkehr

IP-Konfiguration	Verbunden mit	Zweck
ipconfig3	Statische private IP-Adresse	Kommuniziert mit Back-End-Servern

> **Hinweis:**
>
> `IPConfig-3` ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis:**
>
> In einer Multi-Nic, Multi-IP Azure NetScaler VPX-Bereitstellung wird die private IP, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als Verwaltungs-NSIP der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIP oder SNIP mithilfe des `add ns ip` Befehls entsprechend Ihrer Anforderung hinzugefügt werden.

Voraussetzungen

Bevor Sie beginnen, erstellen Sie eine VPX-Instanz, indem Sie die unter diesem Link angegebenen Schritte ausführen:

Eigenständige NetScaler VPX-Instanz konfigurieren

Für diesen Anwendungsfall wird die NSDoc0330VM VPX-Instanz erstellt.

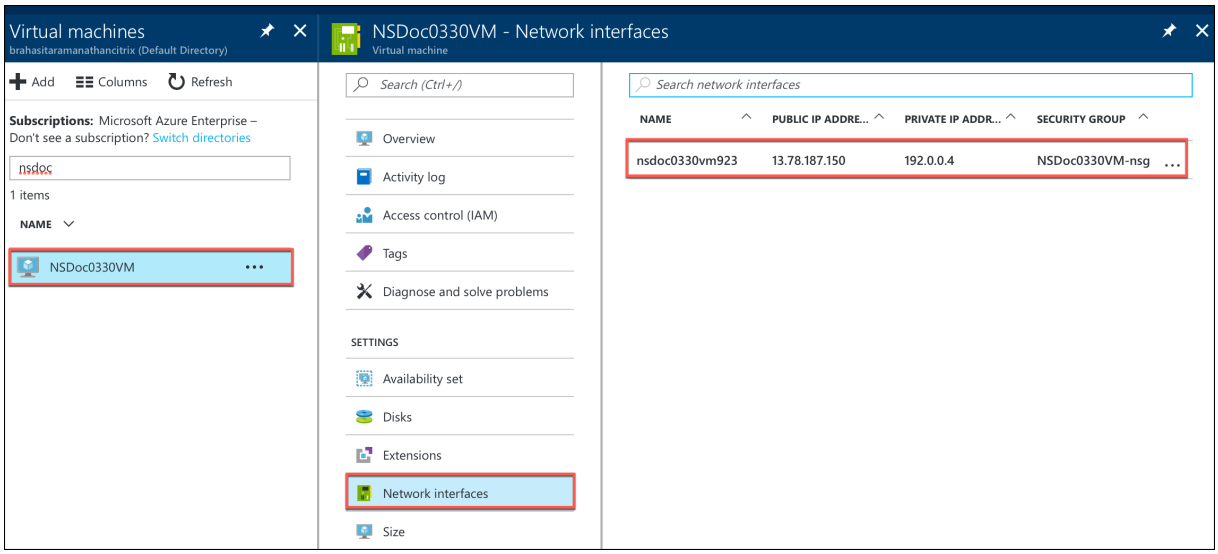
Verfahren zur Konfiguration mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus.

Um mehrere IP-Adressen für eine NetScaler VPX-Appliance im Standalone-Modus zu konfigurieren:

1. Hinzufügen von IP-Adressen zur VM
2. Konfigurieren von NetScaler eigenen IP-Adressen

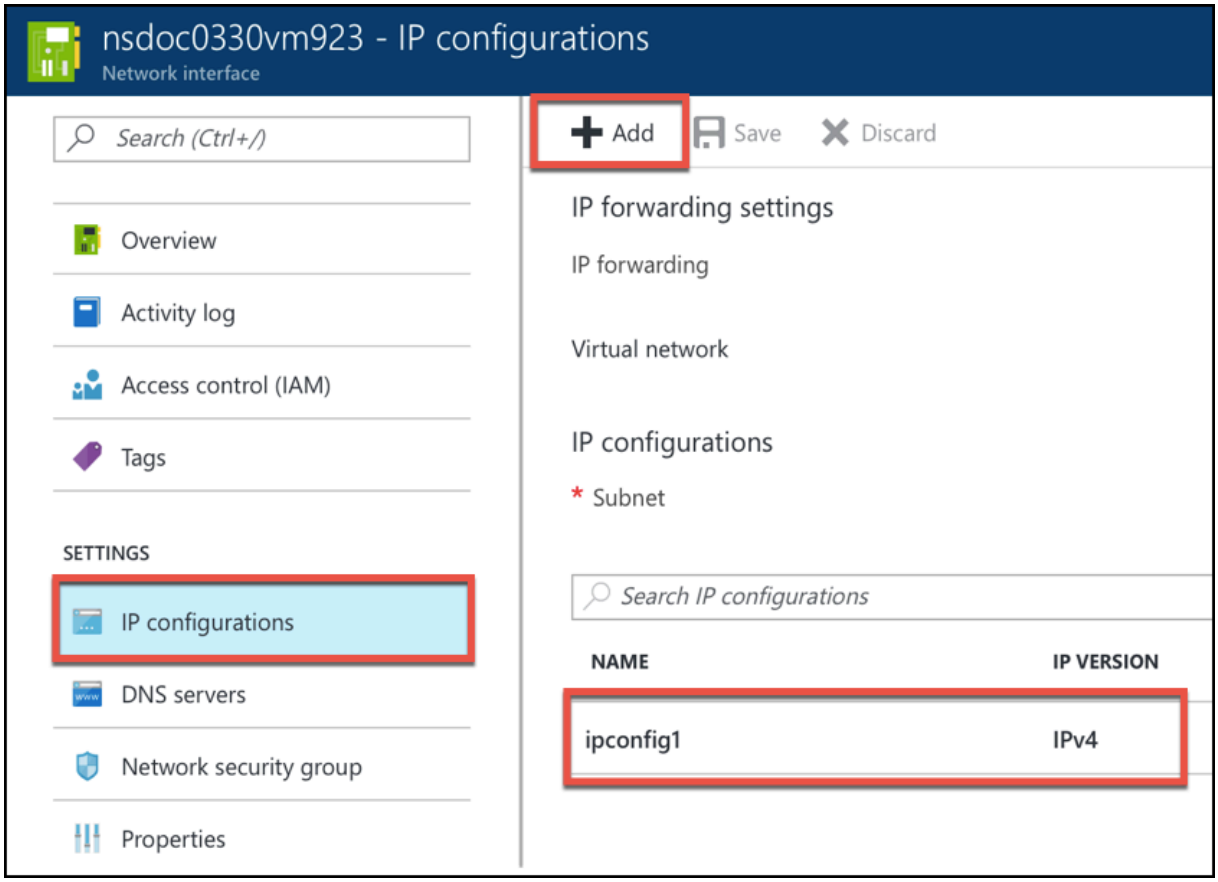
Schritt 1: Hinzufügen von IP-Adressen zur VM

1. Klicken Sie im Portal auf **Weitere Dienste > geben Sie virtuelle Maschinen** in das Filterfeld ein, und klicken Sie dann auf **Virtuelle Maschinen** .
2. Klicken Sie im Blade **Virtuelle Maschinen** auf die VM, der IP-Adressen hinzugefügt werden sollen. Klicken Sie auf **Netzwerkschnittstellen** im Blade der virtuellen Maschine, das angezeigt wird, und wählen Sie dann die Netzwerkschnittstelle aus.



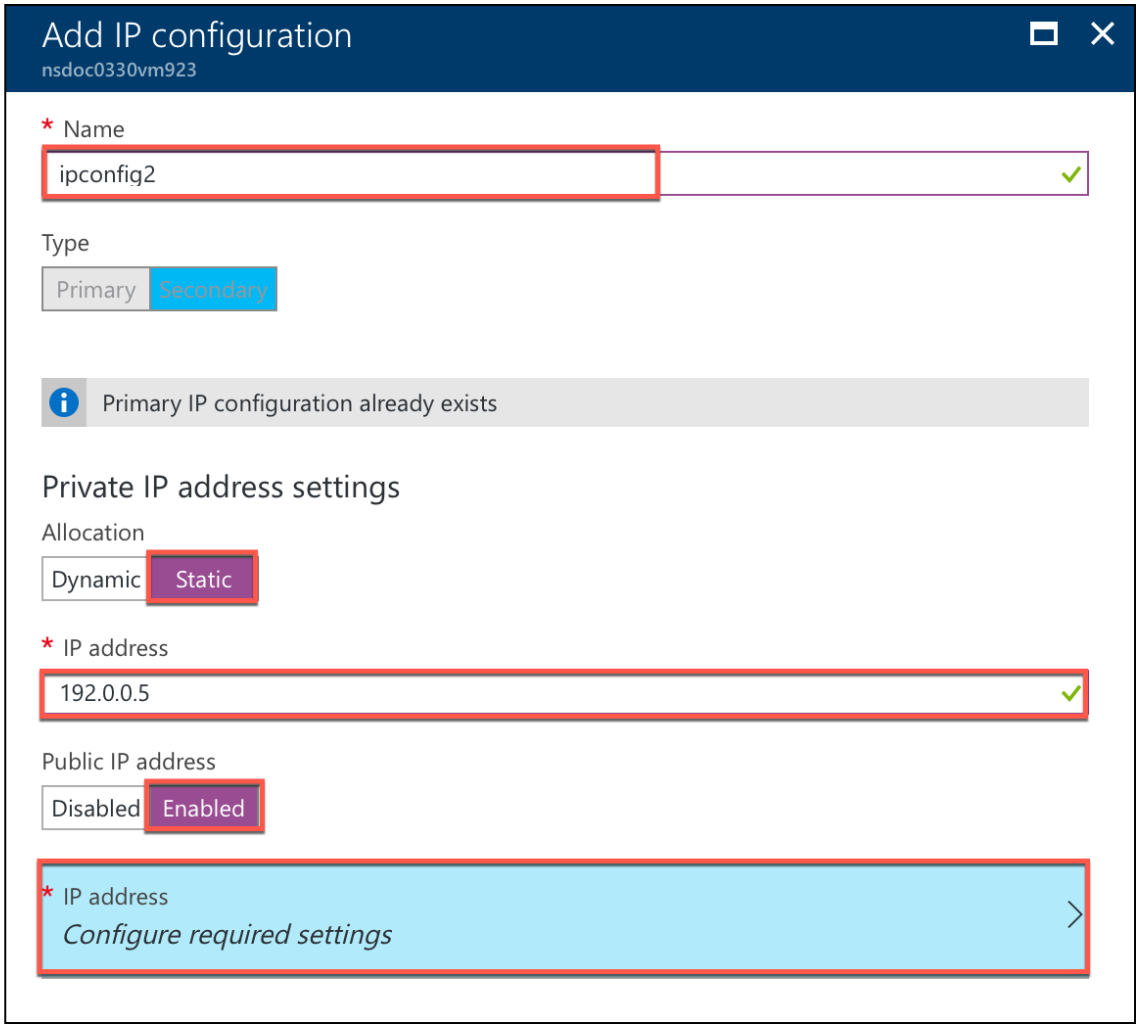
Klicken Sie im Blade, das für die ausgewählte NIC angezeigt wird, auf **IP-Konfigurationen**. Die vorhandene IP-Konfiguration, die beim Erstellen der VM, **ipconfig1**, zugewiesen wurde, wird angezeigt. Stellen Sie für diesen Anwendungsfall sicher, dass die IP-Adressen, die mit ipconfig1 verknüpft sind, statisch sind. Als nächstes erstellen Sie zwei weitere IP-Konfigurationen: ipconfig2 (VIP) und ipconfig3 (SNIP).

Um mehr zu erstellen `ipconfigs`, erstellen **Sie Hinzufügen**.



Geben **Sie im Fenster IP-Konfiguration hinzufügen** einen **Namen** ein, geben Sie die Zuweisungsmethode als **Statisch** an, geben Sie eine IP-Adresse ein (192.0.0.5 für diesen Anwendungsfall) und aktivieren Sie die **öffentliche IP-Adresse** .

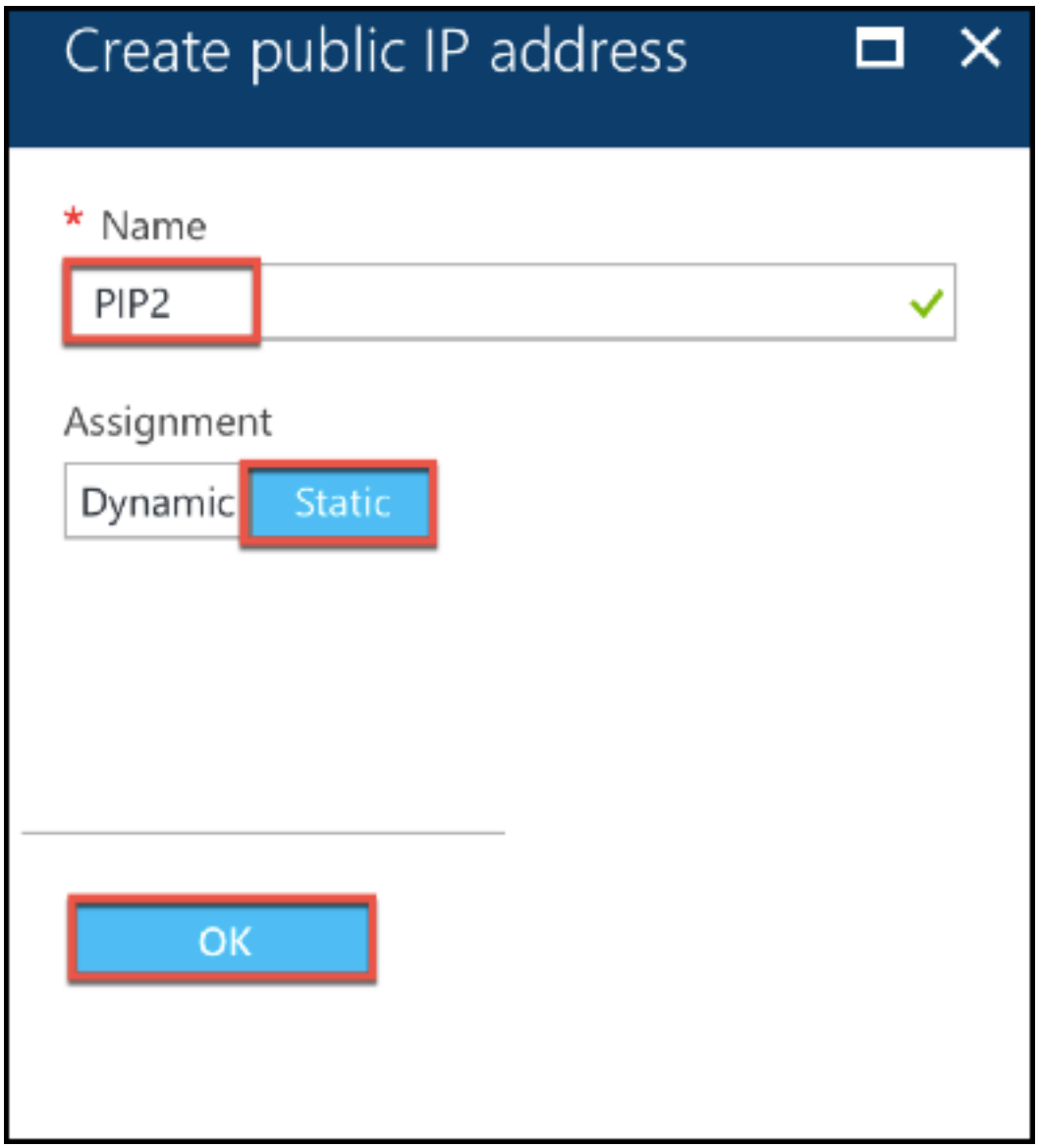
> **Hinweis:**
>
> Bevor Sie eine statische private IP-Adresse hinzufügen, überprüfen Sie die Verfügbarkeit der IP-Adresse und stellen Sie sicher, dass die IP-Adresse zu demselben Subnetz gehört, an das die Netzwerkkarte angeschlossen ist.



Klicken Sie als Nächstes auf **Erforderliche Einstellungen konfigurieren**, um eine statische öffentliche IP-Adresse für ipconfig2 zu erstellen.

Standardmäßig sind öffentliche IPs dynamisch. Um sicherzustellen, dass die VM immer dieselbe öffentliche IP-Adresse verwendet, erstellen Sie eine statische öffentliche IP.

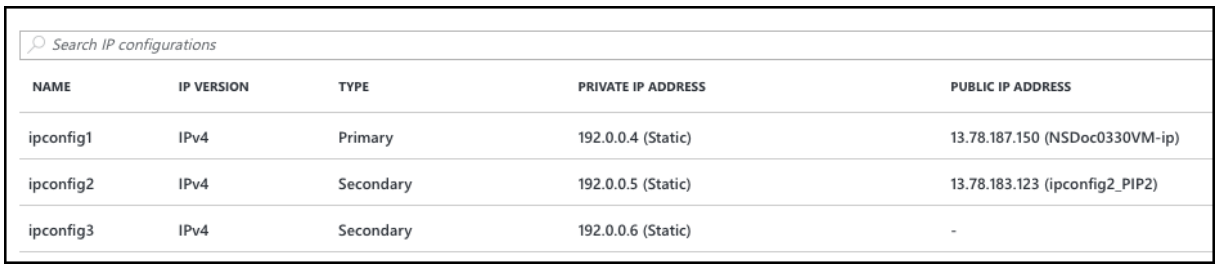
Fügen Sie im Blade Öffentliche IP-Adresse erstellen einen Namen hinzu, klicken Sie unter Zuweisung auf **Statisch**. Klicken Sie dann auf **OK**.



Hinweis:

Selbst wenn Sie die Zuweisungsmethode auf statisch festlegen, können Sie nicht die tatsächliche IP-Adresse angeben, die der öffentlichen IP-Ressource zugewiesen ist. Stattdessen wird sie aus einem Pool verfügbarer IP-Adressen am Azure-Standort zugewiesen, in dem die Ressource erstellt wird.

Führen Sie die Schritte aus, um eine weitere IP-Konfiguration für ipconfig3 hinzuzufügen. Öffentliche IP ist nicht obligatorisch.



Schritt 2: Konfigurieren von NetScaler-eigenen IP-Adressen

Konfigurieren Sie die NetScaler-eigenen IP-Adressen mit der GUI oder des Befehls`add ns ip`. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren

October 17, 2024

In einer Microsoft Azure-Bereitstellung wird eine Hochverfügbarkeitskonfiguration von zwei NetScaler VPX-Instanzen mit Azure Load Balancer (ALB) erreicht. Dies wird durch die Konfiguration einer Integritätsprobe auf ALB erreicht, die jede VPX-Instanz überwacht, indem alle 5 Sekunden eine Integritätsprobe an primäre und sekundäre Instanzen gesendet wird.

In diesem Setup reagiert nur der primäre Knoten auf Integritätssonden und der sekundäre nicht. Sobald der Primärserver die Antwort an den Integritätstest sendet, beginnt die ALB den Datenverkehr an die Instanz zu senden. Wenn die primäre Instance zwei aufeinanderfolgende Integritätstests verpasst, leitet ALB den Datenverkehr nicht an diese Instance weiter. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failover-Zeit, die für den Wechsel des Datenverkehrs dauern kann, kann maximal 13 Sekunden betragen.

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Die folgenden Optionen sind für eine Bereitstellung mit mehreren NICs mit hoher Verfügbarkeit verfügbar:

- Hohe Verfügbarkeit mit dem Azure-Verfügbarkeitssatz
- Hochverfügbarkeit mit Azure Availability Zones

Weitere Informationen zu Azure Availability Set und Availability Zones finden Sie in der Azure-Dokumentation Verwalten der Verfügbarkeit virtueller Linux-Maschinen.

Hochverfügbarkeit mit Verfügbarkeitssatz

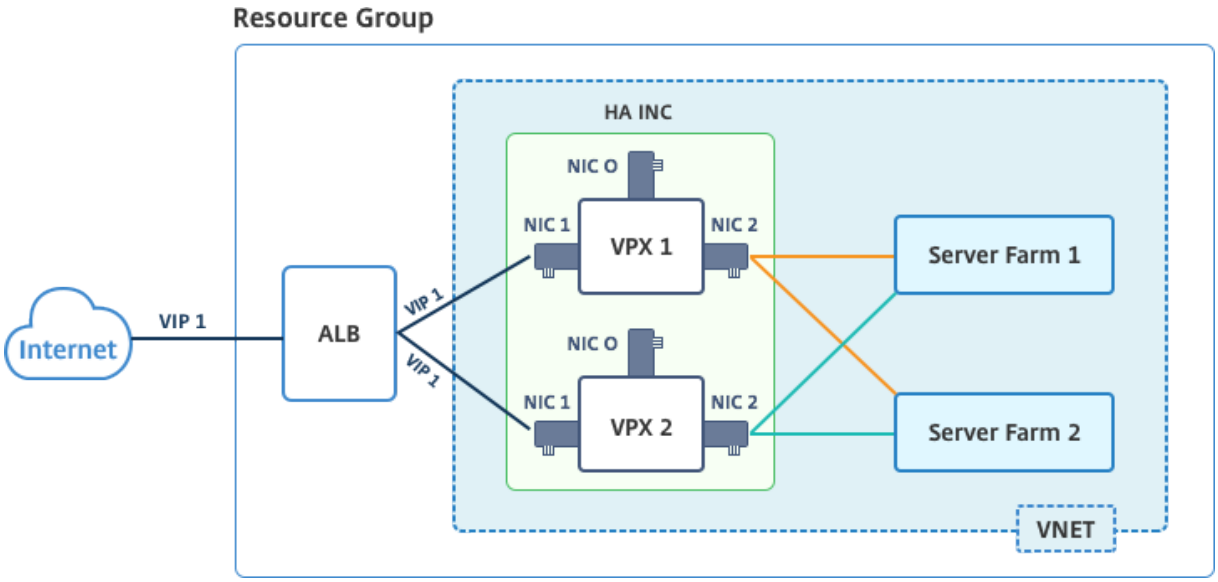
Ein Hochverfügbarkeits-Setup, das ein Verfügbarkeitsset verwendet, muss die folgenden Anforderungen erfüllen:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) im Direct Server Return (DSR) -Modus

Der gesamte Datenverkehr geht durch den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis:**
>
> Damit eine NetScaler VPX-Hochverfügbarkeitsbereitstellung in der Azure-Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden VPX-Knoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Abbildung: Beispiel für eine Bereitstellungsarchitektur mit hoher Verfügbarkeit unter Verwendung von Azure Availability Set



In einer aktiv-passiven Bereitstellung werden die öffentlichen IP-Adressen (PIP) von ALB Frontend als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

Sie können ein VPX-Paar im aktiv-passiven Hochverfügbarkeitsmodus auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **NetScaler VPX-Standardvorlage für hohe Verfügbarkeit**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.
- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar im aktiv-passiven HA-Setup mithilfe der Citrix Vorlage bereitgestellt wird. Wenn Sie PowerShell-Befehle verwenden möchten, finden Sie weitere Informationen unter Konfigurieren eines HA-Setups mit mehreren IP-Adressen und Netzwerkkarten mithilfe von PowerShell-Befehlen.

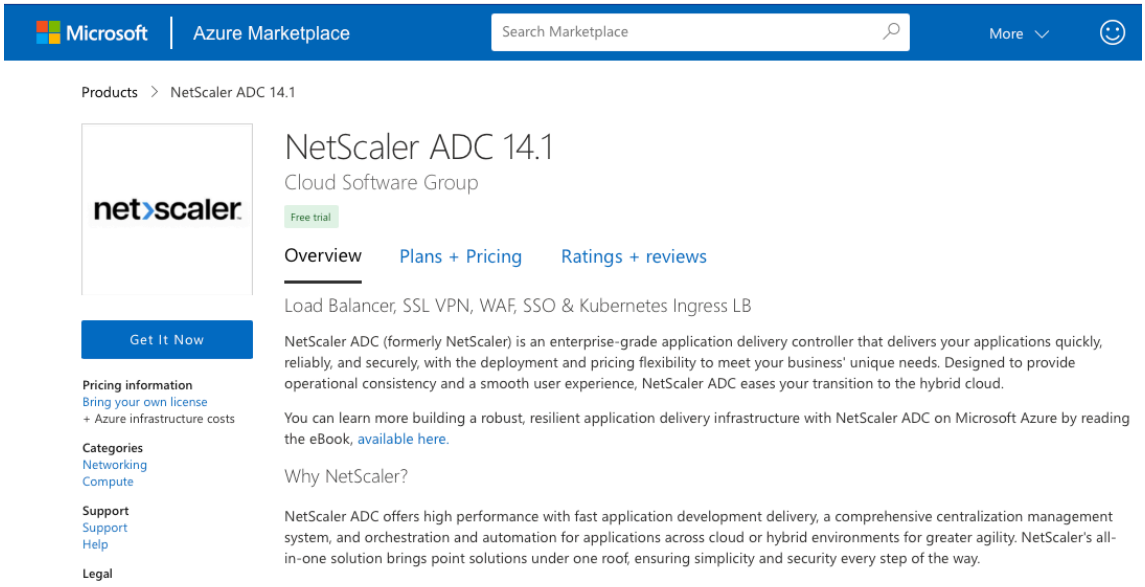
Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage

Mithilfe der Standardvorlage können Sie schnell und effizient ein Paar VPX-Instances im HA-INC-Modus bereitstellen. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für Verwaltungs-, Client- und serverseitigen Datenverkehr, und jedes Subnetz verfügt über zwei Netzwerkkarten für beide VPX-Instanzen.

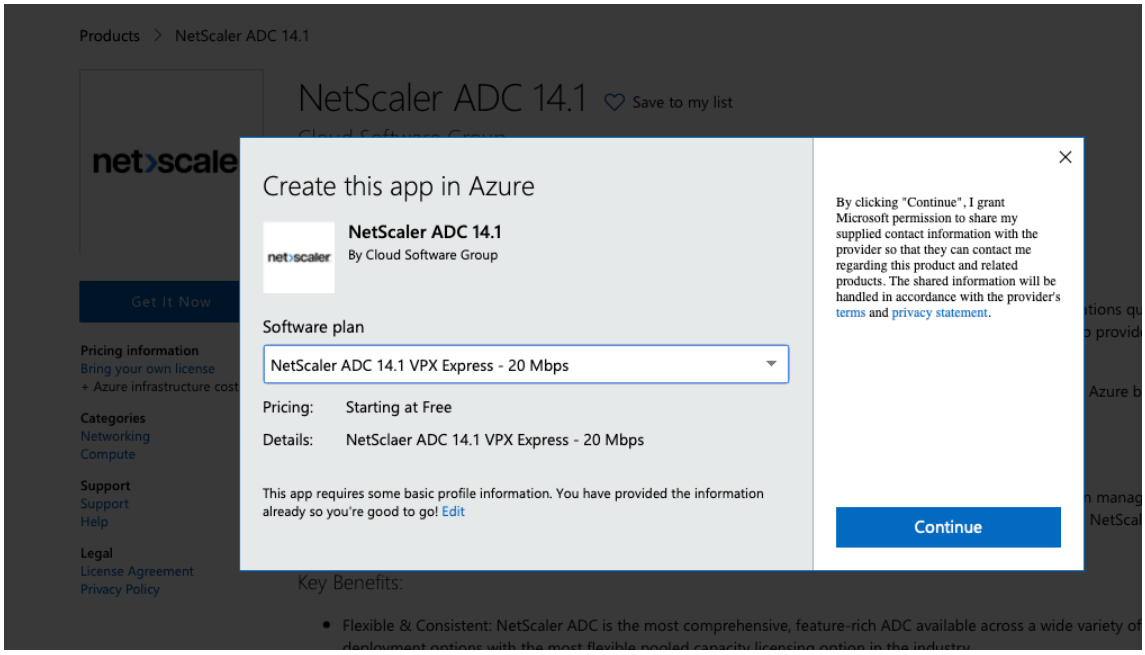
Sie können die NetScaler HA Pair Vorlage im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein VPX-Paar mit hoher Verfügbarkeit bereitzustellen, indem Sie Azure-Verfügbarkeitssätze verwenden.

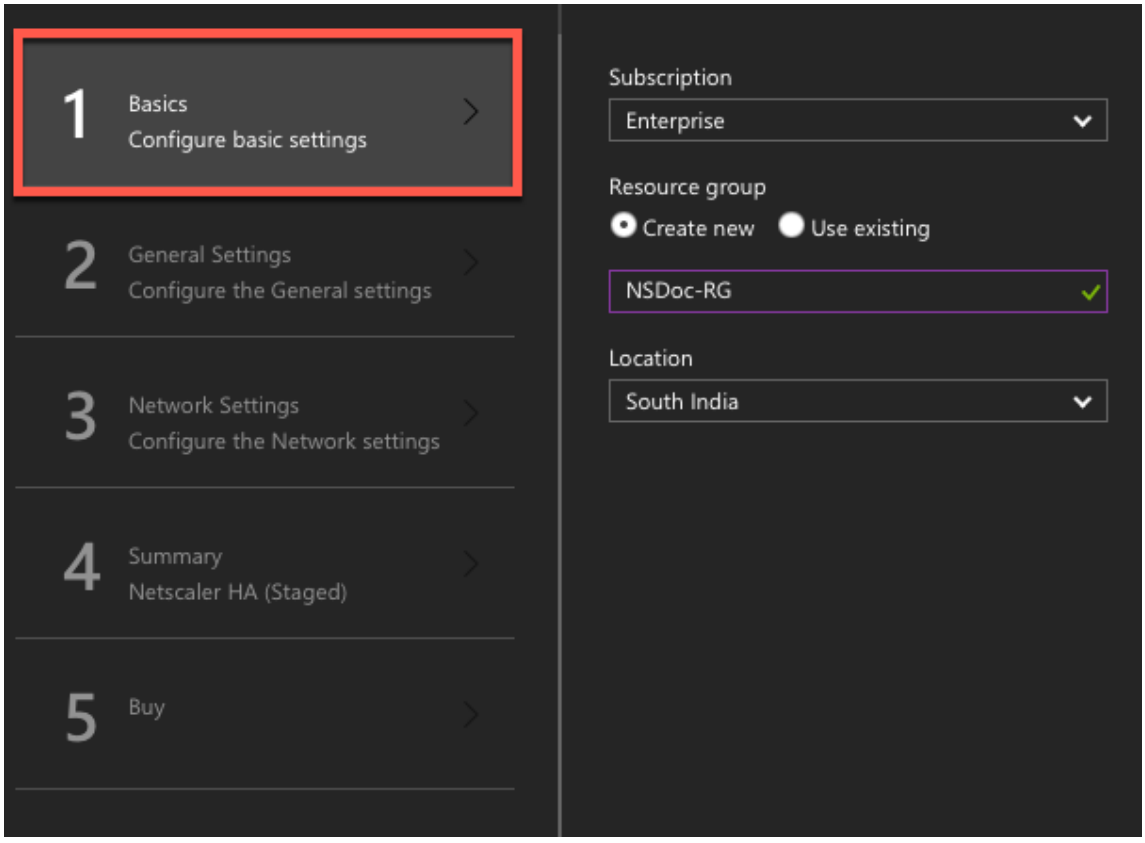
1. Suchen Sie in Azure Marketplace nach **NetScaler**.



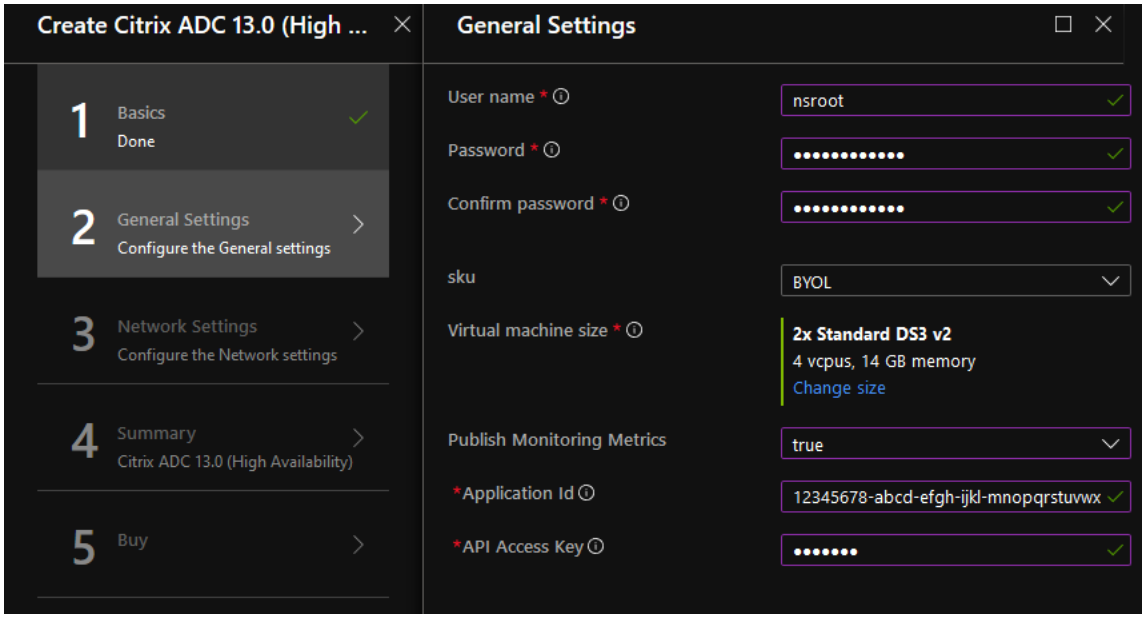
2. Klicken Sie auf **JETZT HOLEN**.
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe und wählen Sie **OK**.

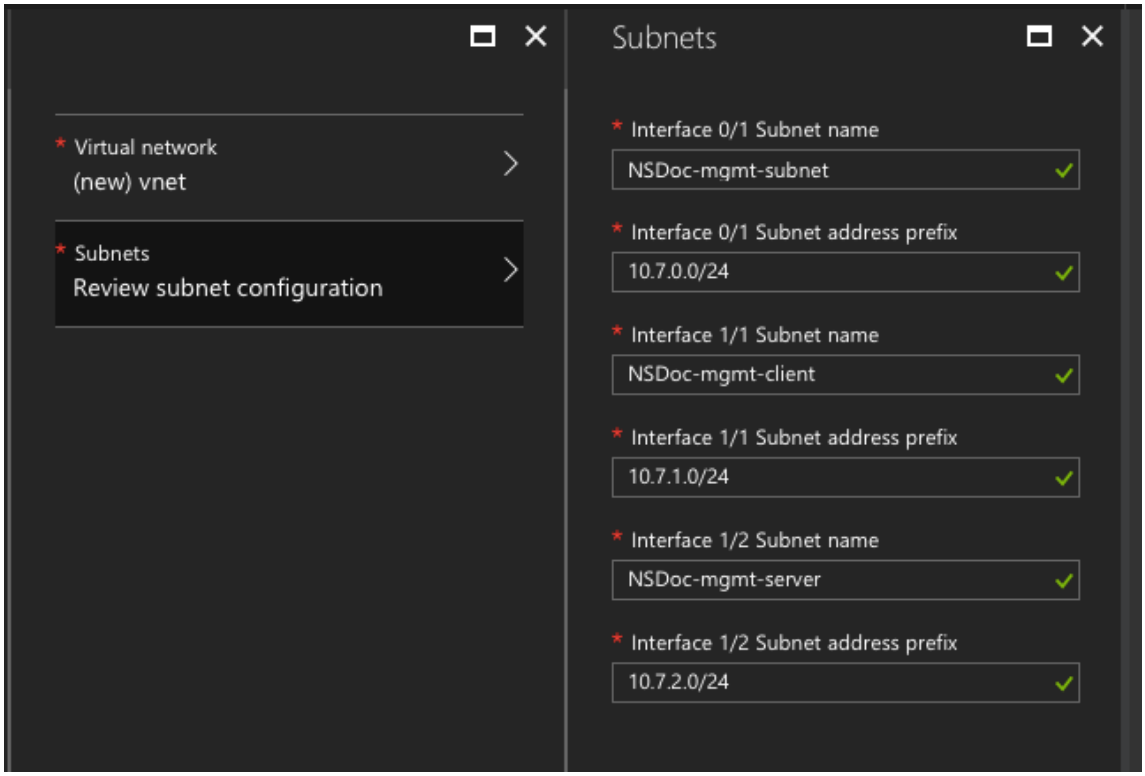


5. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.



> **Hinweis:**
>
> Die Option „ **Monitoring-Metriken veröffentlichen** “ist standardmäßig auf **„False** “gesetzt. Wenn Sie diese Option aktivieren möchten, wählen Sie **True**aus. Erstellen Sie eine Azure Active Directory (ADD) -Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können. Weisen Sie der neu erstellten AAD-Anwendung die Rolle der Mitwirkenden zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals, die auf Ressourcen zugreifen können.

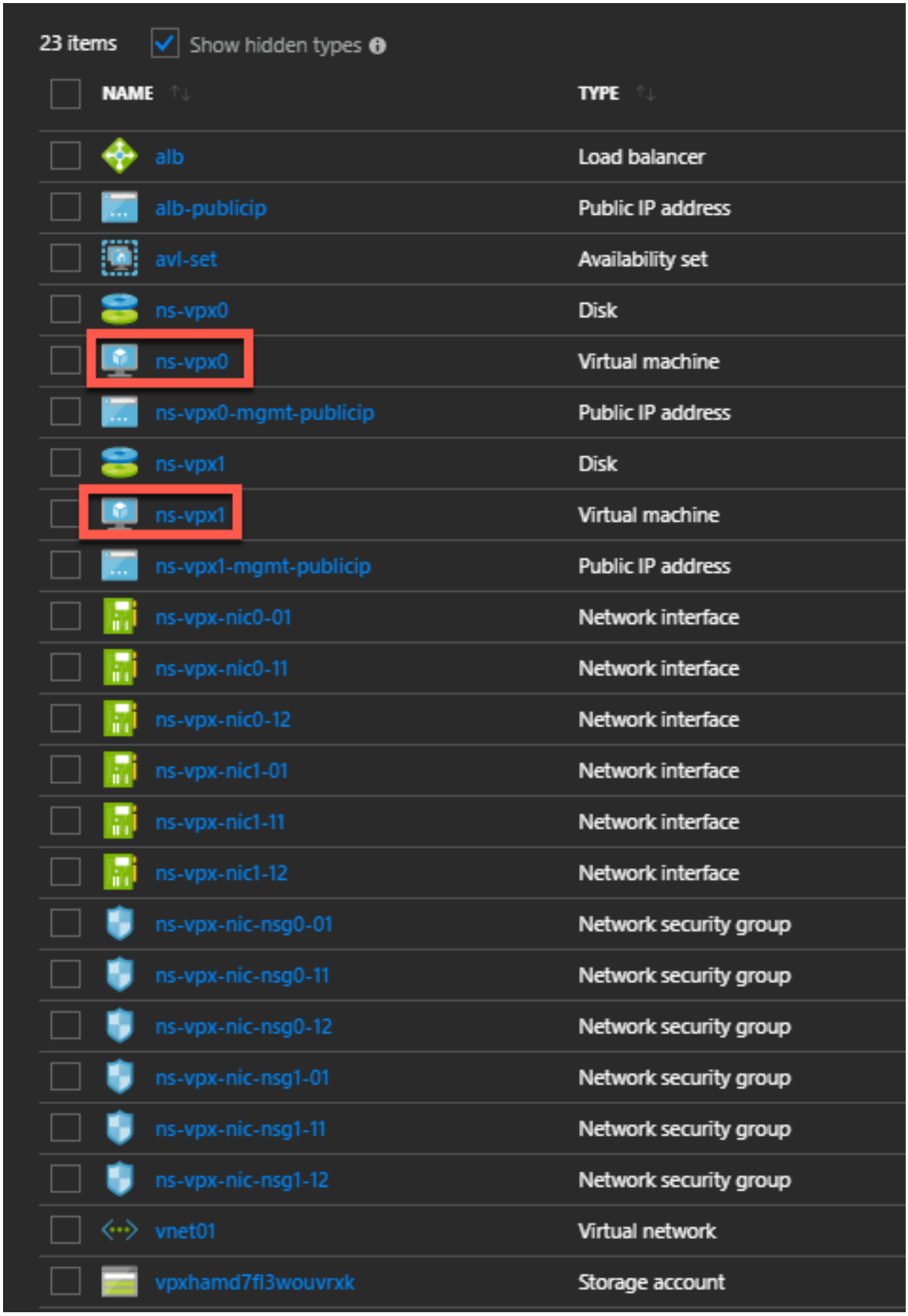
6. Die Seite **“Netzwerkeinstellungen** “wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.



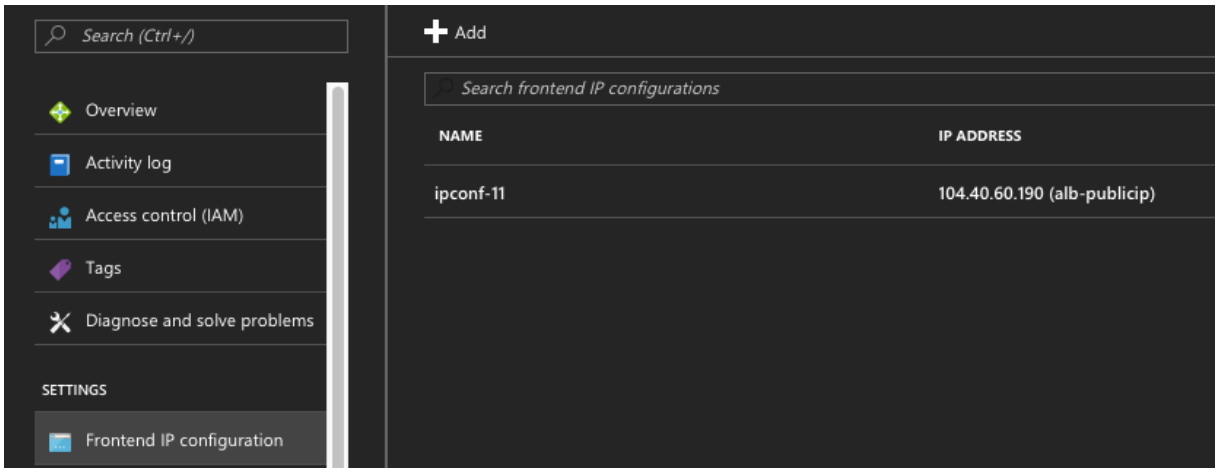
7. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie zur Bestätigung **OK** .
8. Die Seite „ **Kaufen** “wird angezeigt. Wählen Sie **Kaufen** aus, um die Bereitstellung abzuschließen.

Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die **Ressourcengruppe** im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.



Als Nächstes müssen Sie den virtuellen Lastausgleichsserver mit der **öffentlichen IP-Adresse (PIP) des ALB mit der Frontend-IP-Adresse (PIP)**auf dem primären Knoten konfigurieren. Um das ALB PIP zu finden, wählen Sie ALB > **Frontend-IP-Konfiguration**.



Weitere Informationen zur Konfiguration des virtuellen Load-Balancing-Servers finden Sie im Abschnitt **Ressourcen** .

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastausgleichs

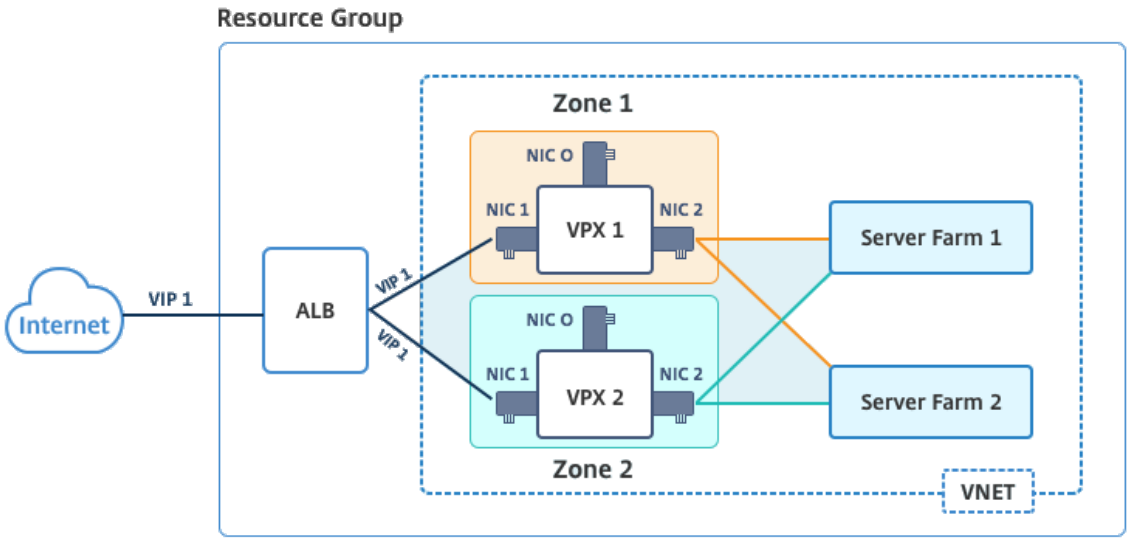
Verwandte Ressourcen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Hohe Verfügbarkeit mithilfe von Availability Zones

Azure Availability Zones sind fehlerisolierte Standorte in einer Azure-Region, die redundante Stromversorgung, Kühlung und Netzwerke bieten und die Ausfallsicherheit erhöhen. Nur bestimmte Azure-Regionen unterstützen Availability Zones. Weitere Informationen zu Regionen, die Availability Zones unterstützen, finden Sie in der Azure-Dokumentation Was sind Availability Zones in Azure?.

Diagramm: Beispiel für eine Hochverfügbarkeitsbereitstellungsarchitektur mit Azure Availability Zones



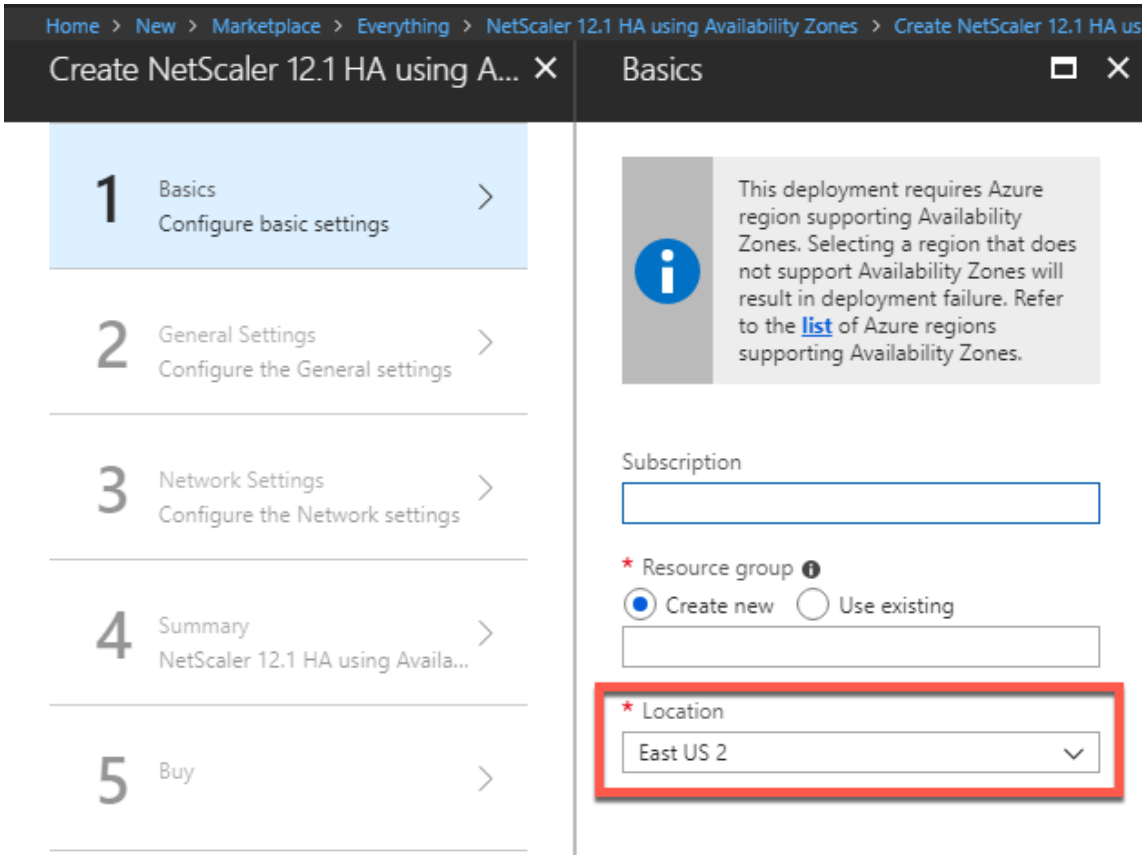
Sie können ein VPX-Paar im Hochverfügbarkeitsmodus bereitstellen, indem Sie die Vorlage „NetScaler 13.0 HA using Availability Zones“verwenden, die im Azure Marketplace verfügbar ist.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein hochverfügbarkeitsfähiges VPX-Paar mithilfe von Azure Availability Zones bereitzustellen.

1. Wählen Sie in Azure Marketplace die Citrix Lösungsvorlage aus, und starten Sie sie.

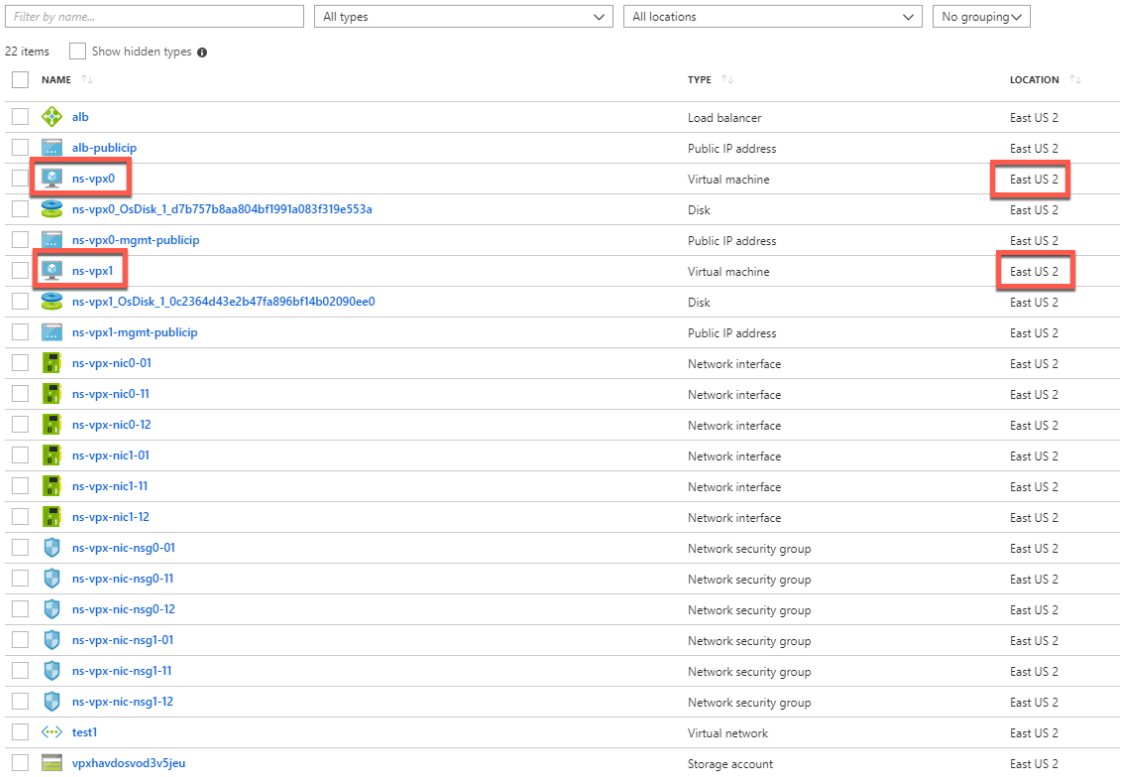
2. Stellen Sie sicher, dass der Bereitstellungstyp Resource Manager ist, und wählen Sie **Erstellen**aus.
3. Die Seite **Grundlagen** wird angezeigt. Geben Sie die Details ein und klicken Sie auf **OK**.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie eine Azure-Region auswählen, die Verfügbarkeitszonen unterstützt. Weitere Informationen zu Regionen, die Availability Zones unterstützen, finden Sie in der Azure-Dokumentation Was sind Availability Zones in Azure?



4. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.
5. Die Seite mit den **Netzwerkeinstellungen** wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.
6. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie zur Bestätigung **OK** .
7. Die Seite „ **Kaufen** “wird angezeigt. Wählen Sie **Kaufen** aus, um die Bereitstellung abzuschließen.

   Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die **Ressourcengruppe** aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools, Integritätstests usw. im Azure-Portal anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt. Sie können den Standort auch in der Spalte **Standort** sehen.



Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Überwachen Sie Ihre Instanz mit Metriken in Azure Monitor

Sie können Metriken auf der Azure Monitor-Datenplattform verwenden, um eine Reihe von NetScaler VPX-Ressourcen wie CPU, Speicherauslastung und Durchsatz zu überwachen. Der Metrics-Dienst überwacht NetScaler VPX-Ressourcen, die auf Azure ausgeführt werden, in Echtzeit. Sie können den **Metrics Explorer** verwenden, um auf die gesammelten Daten zuzugreifen. Weitere Informationen finden Sie unter Übersicht über Azure Monitor-Metriken.

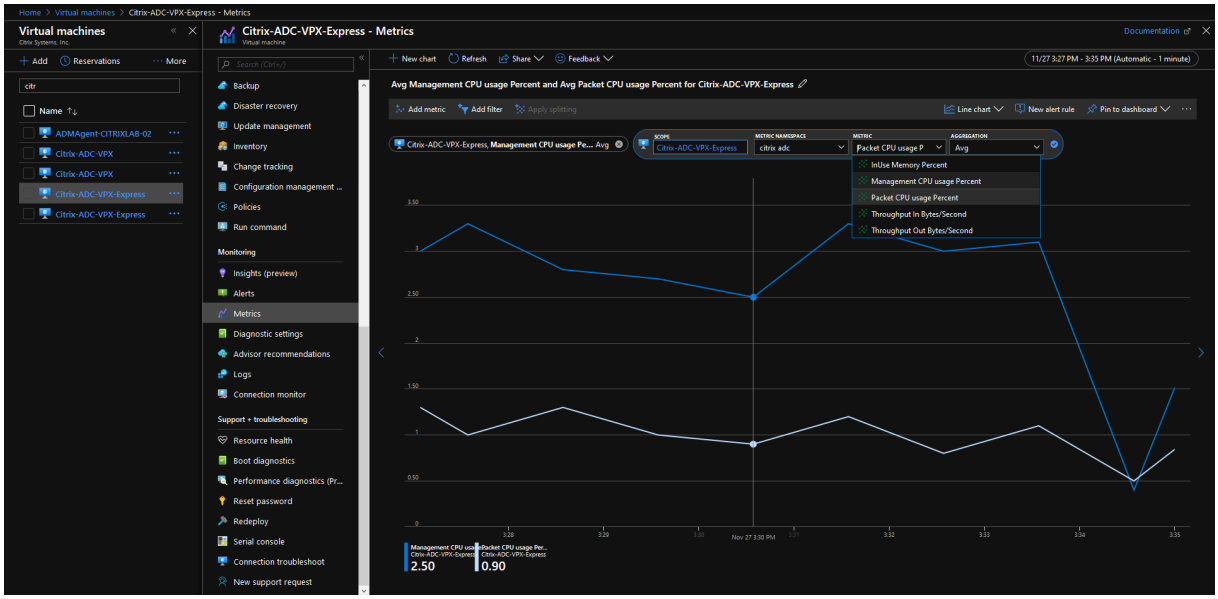
Punkte zu beachten

- Wenn Sie mithilfe des Azure Marketplace-Angebots eine NetScaler VPX-Instanz in Azure bereitstellen, ist der Metrics-Dienst standardmäßig deaktiviert.
- Der Metrics-Dienst wird in Azure CLI nicht unterstützt.
- Metriken sind für CPU (Verwaltung und Paket-CPU-Auslastung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

So zeigen Sie Metriken im Azure-Monitor an

Gehen Sie folgendermaßen vor, um Metriken im Azure-Monitor für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **Azure Portal > Virtuelle Maschinen**an.
2. Wählen Sie die virtuelle Maschine aus, die der primäre Knoten ist.
3. Klicken Sie im Abschnitt **Überwachung** auf **Metriken**.
4. Klicken Sie im Dropdownmenü **Metric Namespace** auf **NetScaler**.
5. Klicken Sie im Dropdownmenü **Alle Metrikenin Metriken** auf die Metriken, die Sie anzeigen möchten.
6. Klicken Sie auf **Metrik hinzufügen**, um eine weitere Metrik im selben Diagramm anzuzeigen. Verwenden Sie die Diagrammoptionen, um Ihr Diagramm anzupassen.



Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle

October 17, 2024

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Für eine aktiv-passive Bereitstellung sind folgende Voraussetzungen erforderlich:

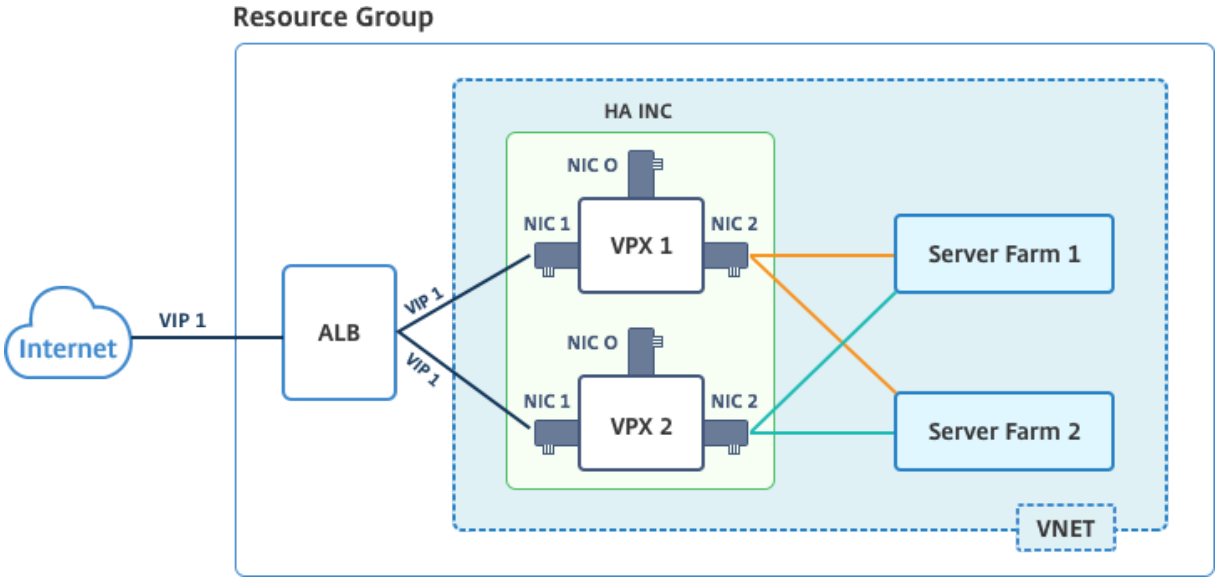
- Eine HA Independent Network Configuration (INC) Konfiguration

- Der Azure Load Balancer (ALB) im Direct Server Return (DSR) -Modus

Der gesamte Datenverkehr geht durch den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis:**
>
> Damit eine NetScaler VPX Hochverfügbarkeitsbereitstellung in einer Azure-Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden Hochverfügbarkeitsknoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Diagramm: Beispiel einer aktiv-passiven Bereitstellungsarchitektur



In einer aktiven und passiven Bereitstellung werden die ALB Floating Public IP (PIP) Adressen als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

ALB überwacht jede VPX-Instanz, indem es alle 5 Sekunden den Integritäts-Sonde sendet, und leitet den Datenverkehr nur an diese Instanz um, die die Reaktion der Integritätssonden in regelmäßigen Intervallen sendet. In einem HA-Setup reagiert der primäre Knoten auf Gesundheitssonden und sekundäre nicht. Wenn die primären Instanzen zwei aufeinanderfolgende Gesundheitssonden verpassen, leitet ALB den Datenverkehr nicht zu dieser Instanz um. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failoverzeit, die für die Umschaltung des Datenverkehrs benötigt wird, kann maximal 13 Sekunden betragen.

Sie können ein VPX-Paar im aktiv-passiven HA-Setup auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **NetScaler VPX Standard-Vorlage für hohe Verfügbarkeit**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.
- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar in aktiv-passiven HA-Setup mithilfe von PowerShell Befehlen bereitgestellt wird. Wenn Sie die NetScaler VPX Standard-HA-Vorlage verwenden möchten, lesen Sie Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs.

Konfigurieren Sie HA-INC-Knoten mit PowerShell-Befehlen

Szenario: HA-INC PowerShell Bereitstellung

In diesem Szenario stellen Sie ein NetScaler VPX-Paar bereit, indem Sie die in der Tabelle angegebene Topologie verwenden. Jede VPX-Instanz enthält drei Netzwerkkarten, wobei jede Netzwerkkarte in einem anderen Subnetz bereitgestellt wird. Jeder NIC wird eine IP-Konfiguration zugewiesen.

ALB	VPX1	VPX2
ALB ist mit öffentlicher IP 3 (pip3) verbunden	Management IP ist mit IPConfig1 konfiguriert, die eine öffentliche IP (pip1) und eine private IP (12.5.2.24) enthält; nic1; Mgmtsubnet=12.5.2.0/24	Management IP ist mit IPConfig5 konfiguriert, die eine öffentliche IP (pip3) und eine private IP (12.5.2.26) enthält; nic4; Mgmtsubnet=12.5.2.0/24
LB-Regeln und Port konfiguriert sind HTTP (80), SSL (443), Health Probe (9000)	Clientseitige IP ist mit IPConfig3 konfiguriert, die eine private IP (12.5.1.27); nic2; frontendSubet=12.5.1.0/24 enthält	Clientseitige IP ist mit IPConfig7 konfiguriert, die eine private IP (12.5.1.28) enthält; nic5; frontendSubet=12.5.1.0/24
-	Serverseitige IP ist mit IPConfig4 konfiguriert, die eine private IP (12.5.3.24); nic3; BackendSubnet=12.5.3.0/24 enthält	Serverseitige IP ist mit IPConfig8 konfiguriert, die eine private IP (12.5.3.28) enthält; nic6; BackendSubnet=12.5.3.0/24
-	Regeln und Ports für NSG sind SSH (22), HTTP (80), HTTPS (443)	-

Parametereinstellungen

Die folgenden Parametereinstellungen werden in diesem Szenario verwendet.

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$Publisher = “Citrix”

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=”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=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Führen Sie die folgenden Schritte mithilfe von PowerShell Befehlen aus, um die Bereitstellung abzuschließen:

1. Erstellen einer Ressourcengruppe, eines Speicherkontos und eines Verfügbarkeitssatzes
2. Erstellen einer Netzwerksicherheitsgruppe und Hinzufügen von Regeln
3. Erstellen eines virtuellen Netzwerks und drei Subnetze
4. Öffentliche IP-Adressen erstellen
5. Erstellen von IP-Konfigurationen für VPX1
6. Erstellen von IP-Konfigurationen für VPX2
7. Erstellen von Netzwerkkarten für VPX1
8. Erstellen von Netzwerkkarten für VPX2
9. VPX1 erstellen
10. VPX2 erstellen
11. ALB erstellen

Erstellen Sie eine Ressourcengruppe, ein Speicherkonto und ein Verfügbarkeitsset.

```
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
```

Erstellen Sie eine Netzwerksicherheitsgruppe und fügen Sie Regeln hinzu.

```
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
```

Erstellen Sie ein virtuelles Netzwerk und drei Subnetze.

```
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 }
```

Erstellen Sie öffentliche IP-Adressen.

```
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
```

Erstellen Sie IP-Konfigurationen für VPX1.

```
1    $IpConfigName1 = "IPConfig1"
2
3
4    $IPAddress = "12.5.2.24"
5
6
7    $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
        Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
        $pip1 -Primary
8
9
```



```
$IPConfigName3="IPConfig-3"


$IPAddress="12.5.1.27"


$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName4 = "IPConfig-4"


$IPAddress = "12.5.3.24"


$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
     -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie IP-Konfigurationen für VPX2.

```
$IpConfigName5 = "IPConfig5"


$IPAddress="12.5.2.26"


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
    $pip2 -Primary


$IPConfigName7="IPConfig-7"


$IPAddress="12.5.1.28"


$IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName8="IPConfig-8"


$IPAddress="12.5.3.28"


$IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie Netzwerkkarten für VPX1.


```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig1 -
    NetworkSecurityGroupId $nsg.Id


$nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig3 -
    NetworkSecurityGroupId $nsg.Id


$nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig4 -
    NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie Netzwerkkarten für VPX2.

```
$nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig5 -
    NetworkSecurityGroupId $nsg.Id


$nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig7 -
    NetworkSecurityGroupId $nsg.Id


$nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig8 -
    NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie VPX1.

Dieser Schritt umfasst die folgenden Teilschritte:

- VM-Konfigurationsobjekt erstellen
- Festlegen der Anmeldeinformationen, des Betriebssystems und des Images
- Netzwerkkarten hinzufügen
- Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
    $suffixNumber = 1

    $vmName=$vmNamePrefix + $suffixNumber

    $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avSet.Id

    $cred=Get-Credential -Message "Type the name and password for
        VPX login."

    $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
        ComputerName $vmName -Credential $cred
```



```
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
```

Erstellen Sie 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  ```
```

Geben Sie die folgenden Befehle ein, um private und öffentliche IP-Adressen anzuzeigen, die den Netzwerkkarten zugewiesen sind:

```
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 ```
```

Erstellen Sie Azure-Lastenausgleich (ALB).

Dieser Schritt umfasst die folgenden Teilschritte:

- Frontend-IP-Konfiguration erstellen
- Erstellen eines Integritätstests
- Back-End-Adresspool erstellen
- Erstellen von Lastenausgleichsregeln (HTTP und SSL)
- Erstellen Sie ALB mit Front-End-IP-Konfiguration, Back-End-Adresspool und LB-Regel
- Verknüpfen Sie IP-Konfiguration mit Back-End-Pools

```
$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
```

Nachdem Sie das NetScaler VPX-Paar erfolgreich bereitgestellt haben, melden Sie sich bei jeder VPX-Instanz an, um HA-INC- sowie SNIP- und VIP-Adressen zu konfigurieren.

1. Geben Sie den folgenden Befehl ein, um HA-Knoten hinzuzufügen.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Fügen Sie private IP-Adressen von clientseitigen Netzwerkkarten als SNIPs für VPX1 (NIC2) und VPX2 (NIC5) hinzu


```
füge nsip privateIPofNIC2 255.255.255.0 hinzu -Typ SNIP füge nsip
 privateIPofNIC5 255.255.255.0 hinzu -Typ SNIP
```

3. Fügen Sie einen virtuellen Lastenausgleichsserver auf dem primären Knoten mit Front-End-IP-Adresse (öffentliche IP) von ALB hinzu.

```
add lb virtual server v1 HTTP FrontEndIPofALB 80
```

Verwandte Ressourcen:

Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

NetScaler-Hochverfügbarkeitspaar auf Azure mit ALB im Floating IP-Deaktiviert-Modus bereitstellen

October 17, 2024

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede Netzwerkkarte kann viele IP-Adressen enthalten.

Für eine aktiv-passive Bereitstellung sind folgende Voraussetzungen erforderlich:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) mit:
  - Floating IP-fähiger Modus oder Direct Server Return (DSR) -Modus
  - Floating-IP-Modus deaktiviert

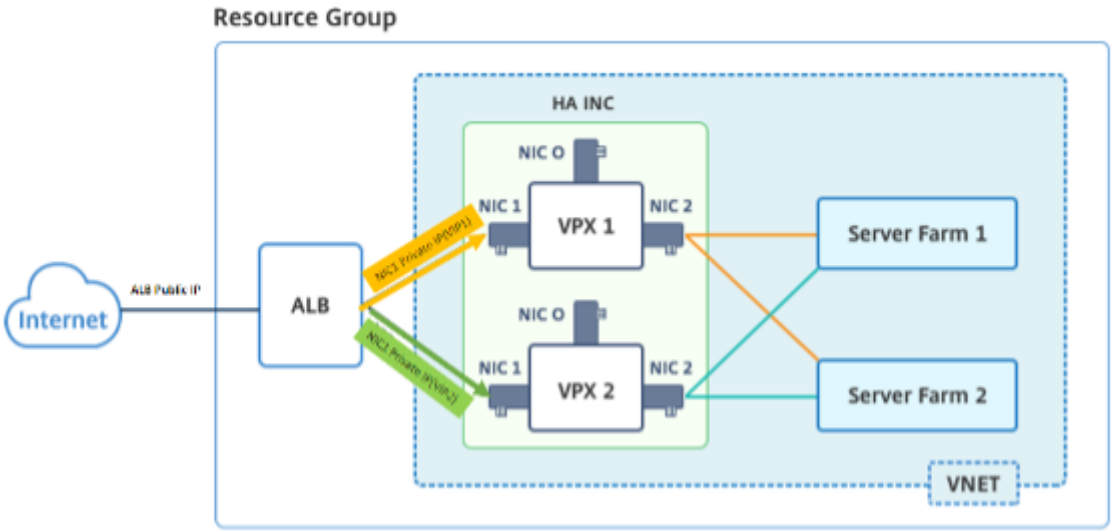
Weitere Informationen zu ALB Floating-IP-Optionen finden Sie in der Azure-Dokumentation.

Wenn Sie ein VPX-Paar in einem Aktiv-Passiv-HA-Setup auf Azure mit aktivierter ALB-Floating-IP bereitstellen möchten, lesen Sie . Konfigurieren Sie mithilfe von PowerShell-Befehleneinein Hochverfügbarkeits-Setup mit mehreren IP-Adressen und NICs.

HA-Bereitstellungsarchitektur mit ALB im Floating-IP-deaktivierten Modus

Bei einer Aktiv-Passiv-Bereitstellung werden die privaten IP-Adressen der Client-Schnittstelle jeder Instanz als VIP-Adressen in jeder VPX-Instanz hinzugefügt. Konfiguration im HA-INC-Modus mit VIP-Adressen, die über IPset geteilt werden und SNIP-Adressen instanzspezifisch sind. Der gesamte Datenverkehr durchläuft die primäre Instanz. Die sekundäre Instanz befindet sich im Standby-Modus, bis die primäre Instanz ausfällt.

Diagramm: Beispiel einer aktiv-passiven Bereitstellungsarchitektur



Voraussetzungen

Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Arbeiten einer NetScaler-Appliance. Weitere Informationen finden Sie in der NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie im ADC-Netzwerk.
- Azure Load Balancer und Konfiguration der Lastenausgleichsregeln. Konfiguration von Azure Load Balancer und Load Balancing-Regeln Weitere Informationen finden Sie in der Azure ALB-Dokumentation.

So stellen Sie ein VPX HA-Paar auf Azure mit deaktivierter ALB Floating-IP bereit

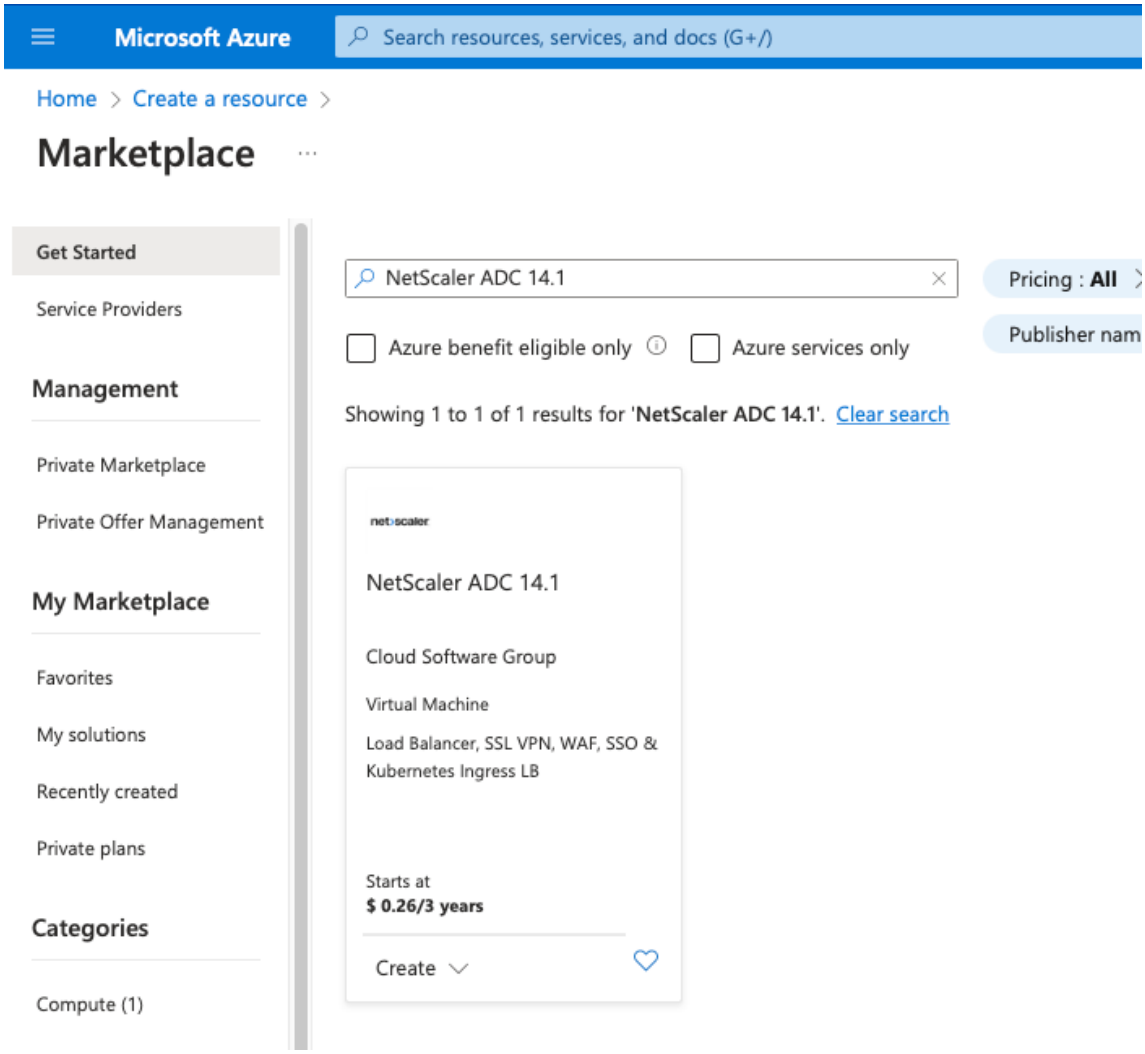
Hier finden Sie eine Zusammenfassung der Schritte zur HA- und ALB-Bereitstellung:

1. Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) in Azure bereit.
2. Fügen Sie auf beiden Instanzen eine Client- und Server-Netzwerkkarte hinzu.
3. Stellen Sie eine ALB mit Load Balancing-Regel bereit, deren Floating-IP-Modus deaktiviert ist.
4. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI.

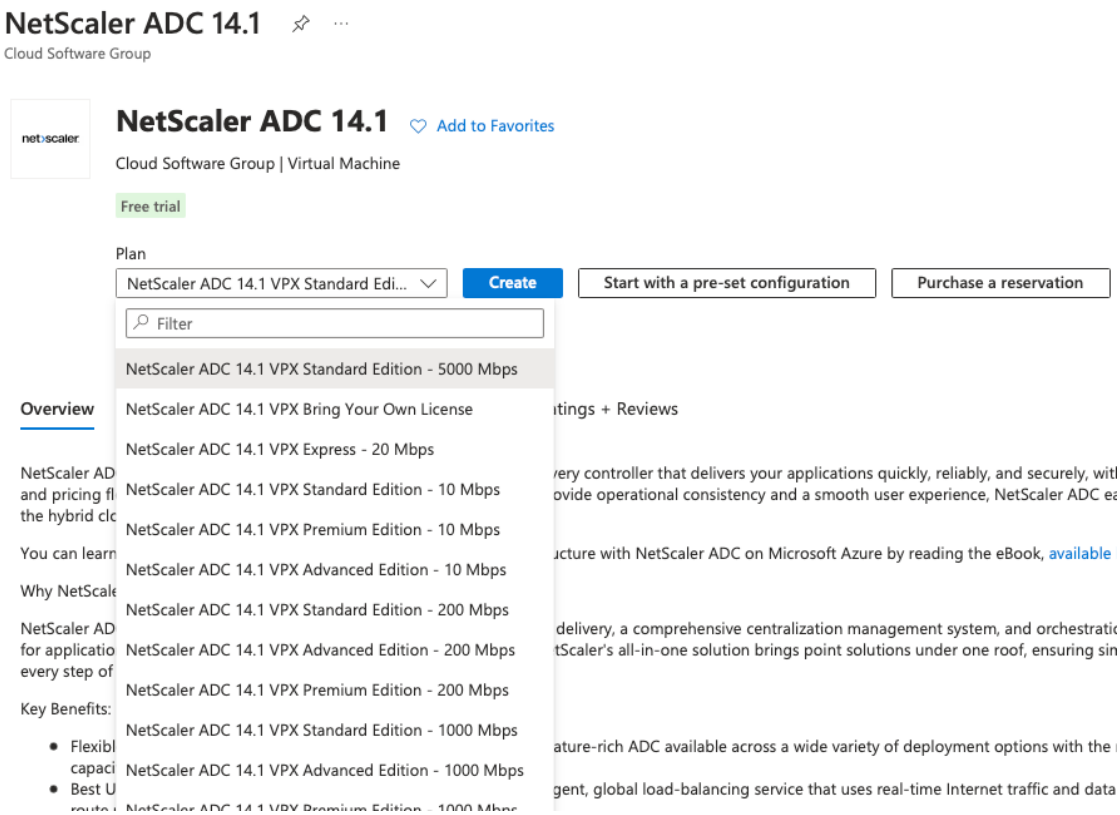
Schritt 1. Stellen Sie zwei VPX-Instanzen auf Azure bereit.

Erstellen Sie zwei VPX-Instanzen, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie die NetScaler-Version aus Azure Marketplace aus (in diesem Beispiel wird NetScaler Version 13.1 verwendet).

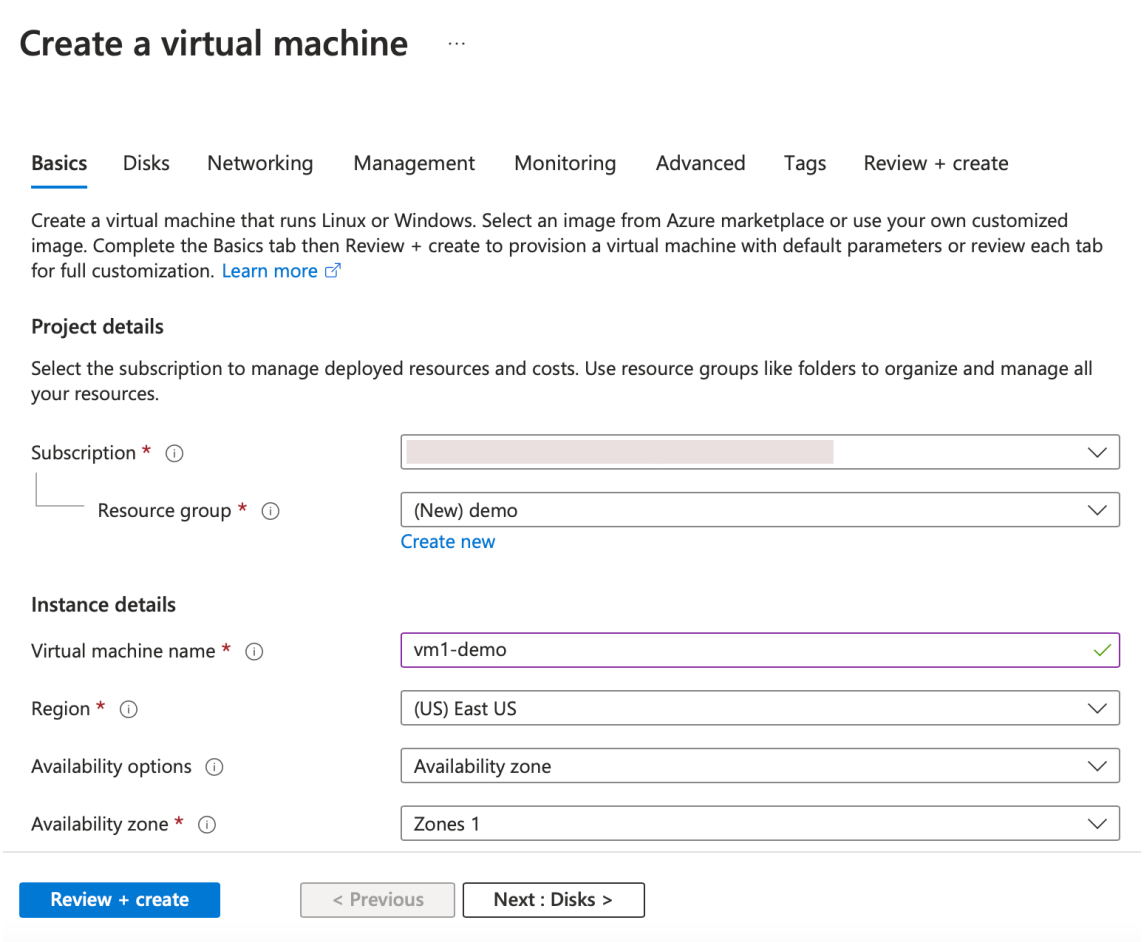


2. Wählen Sie den erforderlichen ADC-Lizenzierungsmodus aus und klicken Sie auf **Erstellen**.



Die Seite **Virtuelle Maschine erstellen** wird geöffnet.

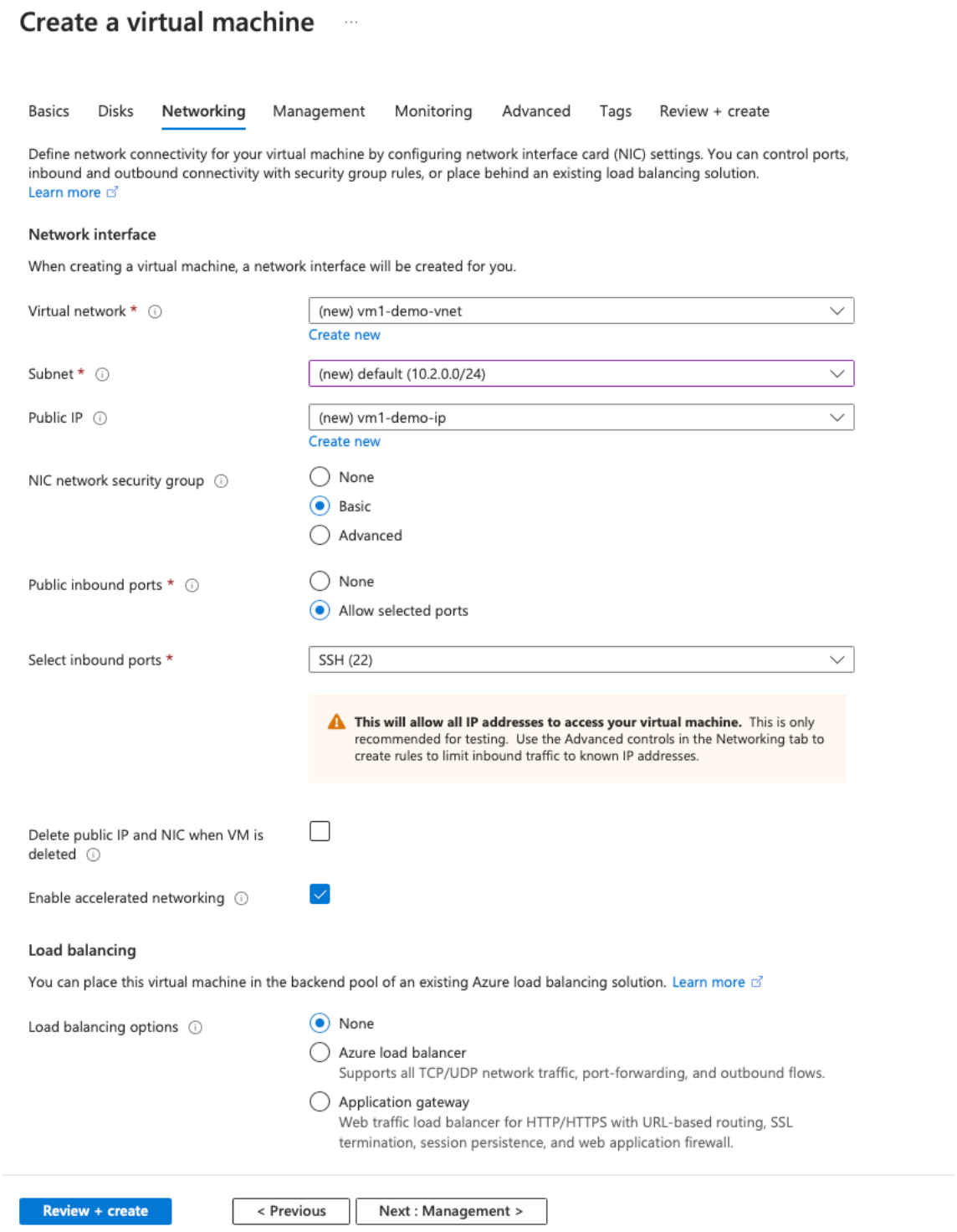
3. Geben Sie auf jeder Registerkarte die erforderlichen Informationen ein: Grundlagen, Festplatten, Netzwerke, Verwaltung, Überwachung, Erweitert und Tags, um eine erfolgreiche Bereitstellung zu gewährleisten.



Erstellen Sie auf der Registerkarte **Netzwerk** ein neues virtuelles Netzwerk mit 3 Subnetzen, jeweils eines für: Verwaltungs-, Client- und Server-Netzwerkkarten. Andernfalls können Sie auch ein vorhandenes virtuelles Netzwerk verwenden. Die Management-NIC wird während der VM-Bereitstellung erstellt. Client- und Server-Netzwerkkarten werden erstellt und angehängt, nachdem die VM erstellt wurde. Für die Netzwerksicherheitsgruppe NIC können Sie eine der folgenden Aktionen ausführen:

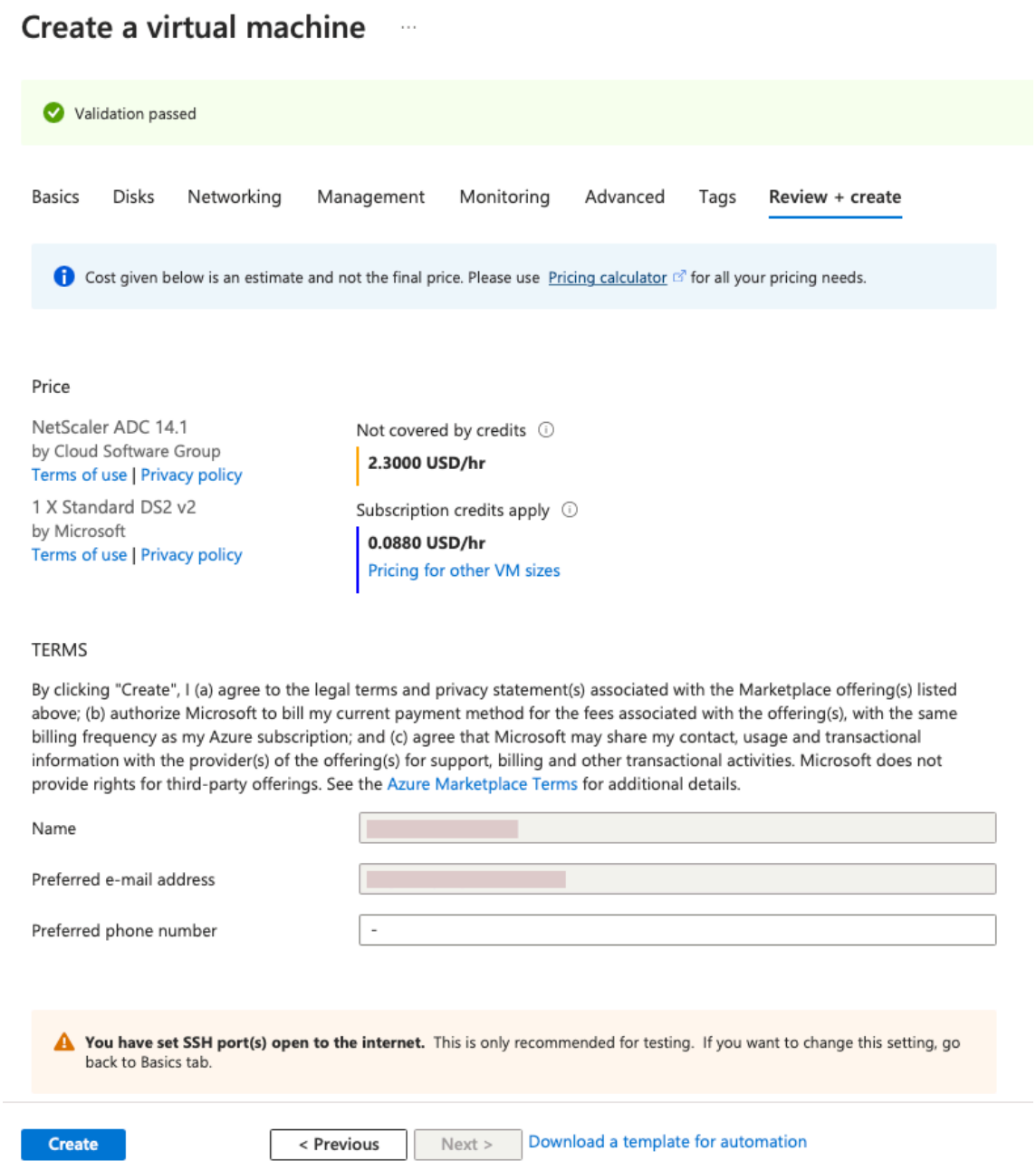
- Wählen Sie **Erweitert** aus und verwenden Sie eine vorhandene Netzwerksicherheitsgruppe, die Ihren Anforderungen entspricht.
- Wählen Sie **Basic** und dann die erforderlichen Ports aus.

> **Hinweis:**
>
> Sie können die Einstellungen der Netzwerksicherheitsgruppe auch ändern, nachdem die VM-Bereitstellung abgeschlossen ist.

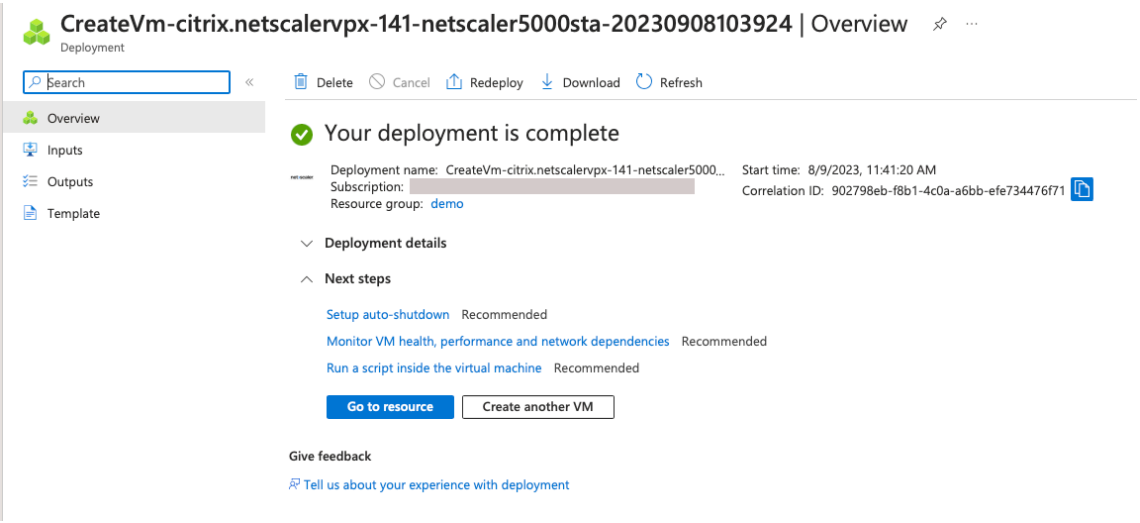


4. Klicken Sie auf Weiter: **Überprüfen + erstellen**.

   Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**.



5. Nachdem die Bereitstellung abgeschlossen ist, klicken Sie auf **Go to Resource**, um die Konfigurationsdetails zu sehen.



Stellen Sie auf ähnliche Weise eine zweite NetScaler VPX-Instanz bereit.

Schritt 2. Fügen Sie auf beiden Instanzen Client- und Server-Netzwerkkarten hinzu.

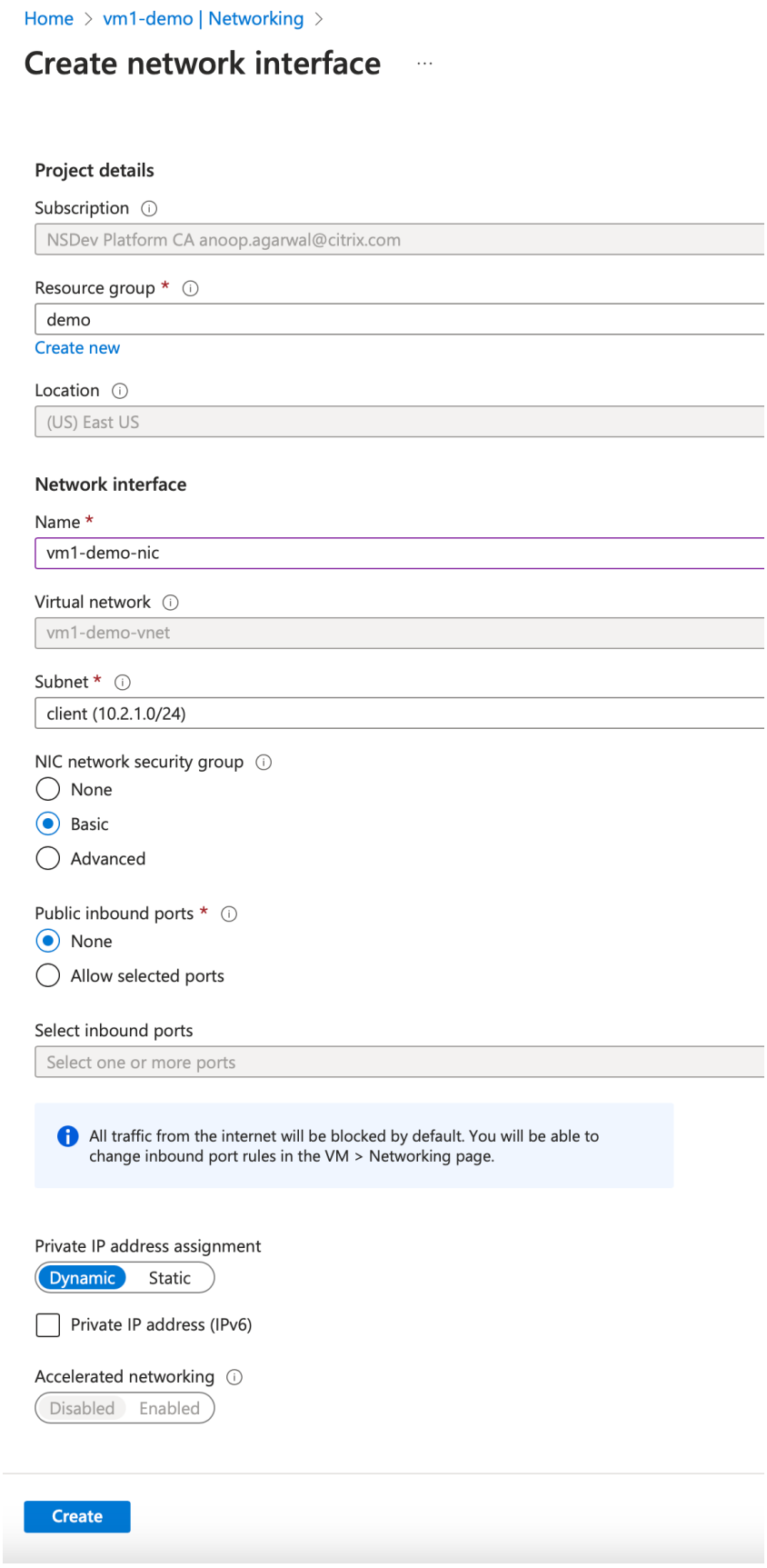
> **Hinweis:**
>
> Um weitere Netzwerkkarten anzuhängen, müssen Sie zuerst die VM beenden. Wählen Sie im Azure-Portal die VM aus, die Sie beenden möchten. Klicken Sie auf der Registerkarte **Overview** auf **Stop**. Warten Sie, bis der Status als **Gestoppt angezeigt wird**.

Gehen Sie folgendermaßen vor, um eine Client-Netzwerkkarte zur primären Instanz hinzuzufügen:

1. Navigieren Sie zu **Netzwerk > Netzwerkschnittstelle anhängen**.

   Sie können eine vorhandene Netzwerkkarte auswählen oder eine neue Schnittstelle erstellen und anfügen.

2. Für die Netzwerksicherheitsgruppe NIC können Sie eine vorhandene Netzwerksicherheitsgruppe verwenden, indem Sie **Erweitert** auswählen, oder eine erstellen, indem Sie **Basic**auswählen.



Um eine Server-Netzwerkkarte hinzuzufügen, führen Sie dieselben Schritte wie beim Hinzufügen einer Client-Netzwerkkarte aus.

An die NetScaler VPX-Instanz sind alle drei Netzwerkkarten (Management-NIC, Client-NIC und Server-NIC) angeschlossen.

Wiederholen Sie die vorherigen Schritte zum Hinzufügen von Netzwerkkarten auf der sekundären Instanz.

Nachdem Sie die Netzwerkkarten auf beiden Instanzen erstellt und angehängt haben, starten Sie beide Instanzen neu, indem Sie zu **Übersicht > Start**gehen.

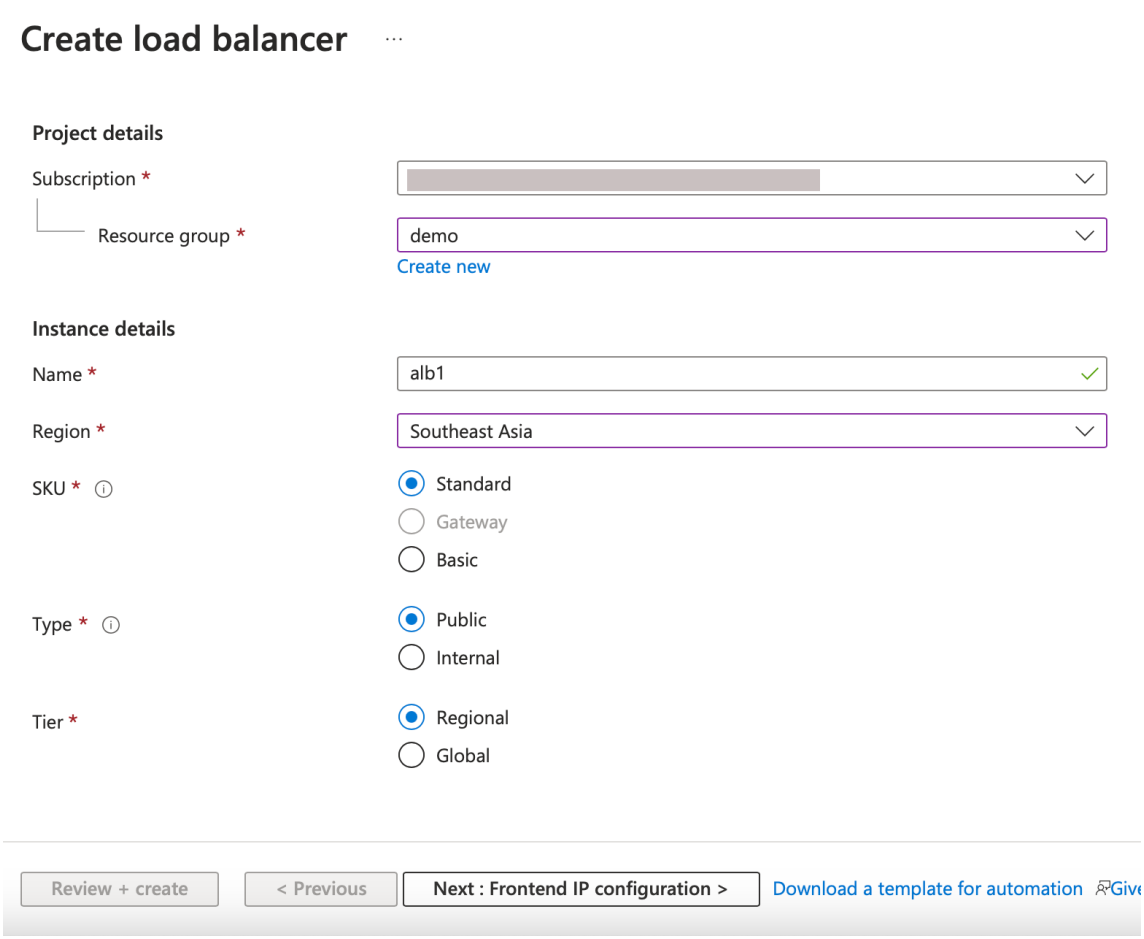
> **Hinweis:**
>
> Sie müssen den Datenverkehr durch den Port in der eingehenden Client-NIC-Regel zulassen, die später verwendet wird, um einen virtuellen Lastausgleichsserver beim Konfigurieren der NetScaler VPX-Instanz zu erstellen.

Schritt 3. Stellen Sie eine ALB mit Load Balancing-Regel bereit, deren Floating-IP-Modus deaktiviert ist.

Gehen Sie folgendermaßen vor, um die Konfiguration von ALB zu starten:

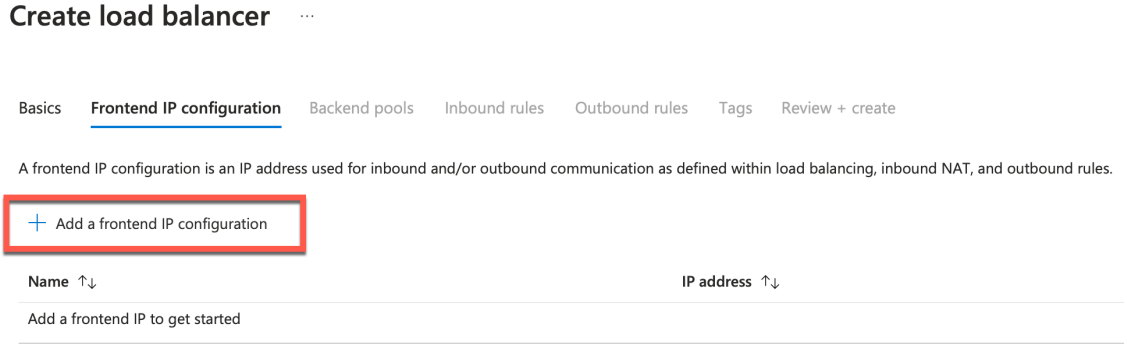
1. Gehen Sie zur Seite **Load Balancers** und klicken Sie auf **Erstellen**.
2. Geben **Sie auf der Seite Load Balancer erstellen** die Details nach Bedarf ein.

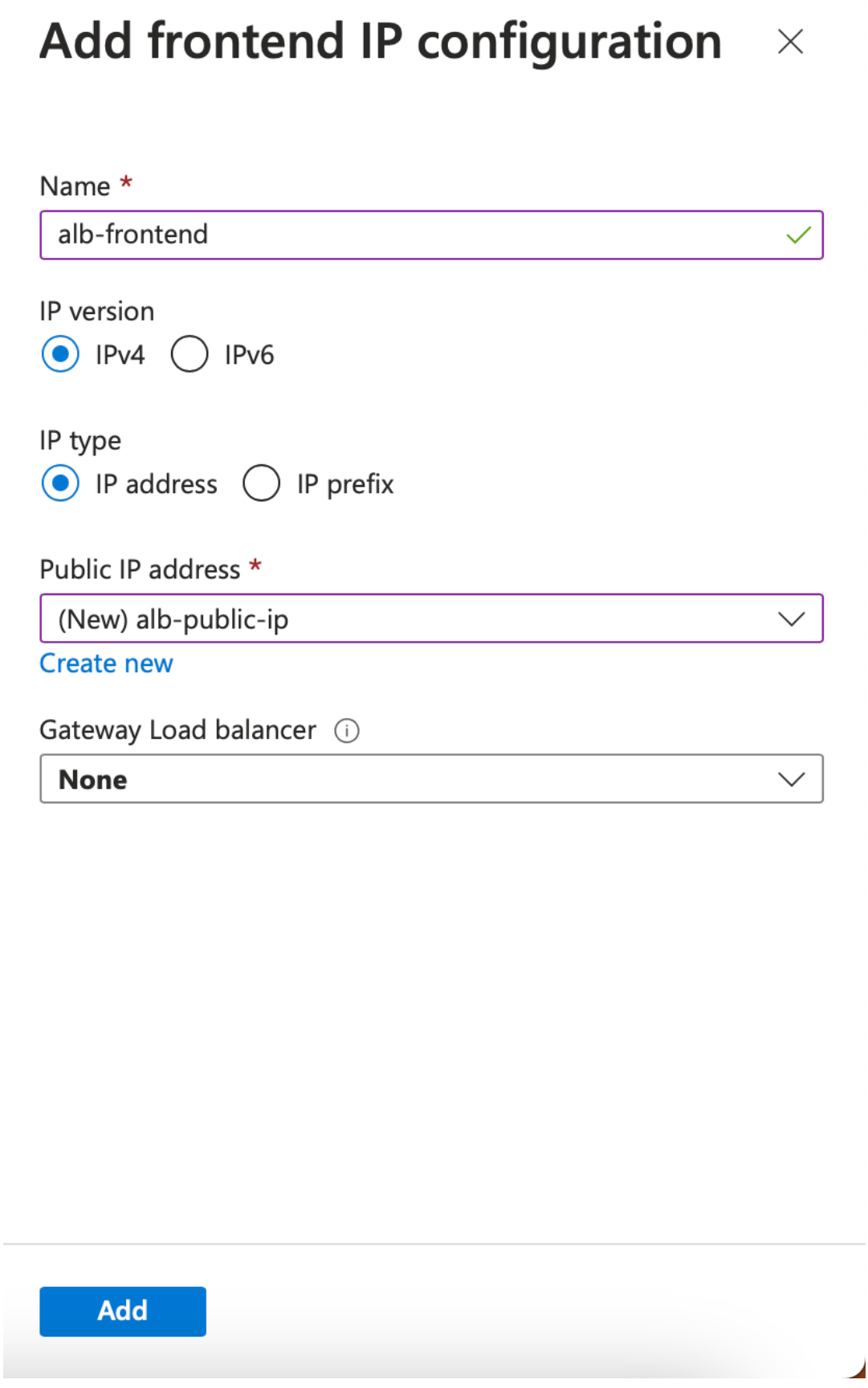
   Im folgenden Beispiel stellen wir einen regionalen öffentlichen Load Balancer der Standard-SKU bereit.



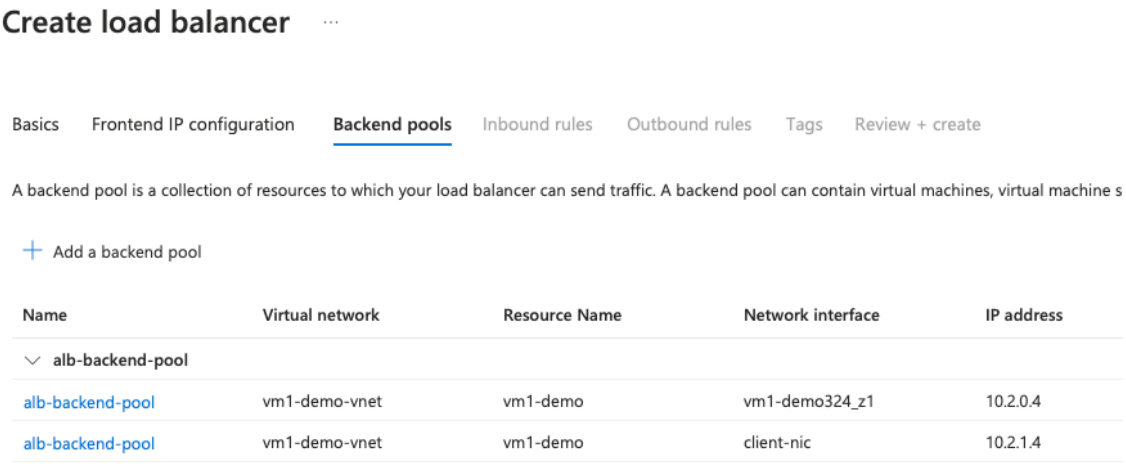
> **Hinweis:**
>
> Alle öffentlichen IPs, die an die NetScaler VMs angeschlossen sind, müssen dieselbe SKU wie die von ALB haben. Weitere Informationen zu ALB-SKUs finden Sie in der Dokumentation der Azure Load Balancer-SKUs.

3. Erstellen Sie auf der Registerkarte **Frontend-IP-Konfiguration** entweder eine IP-Adresse oder verwenden Sie eine vorhandene IP-Adresse.

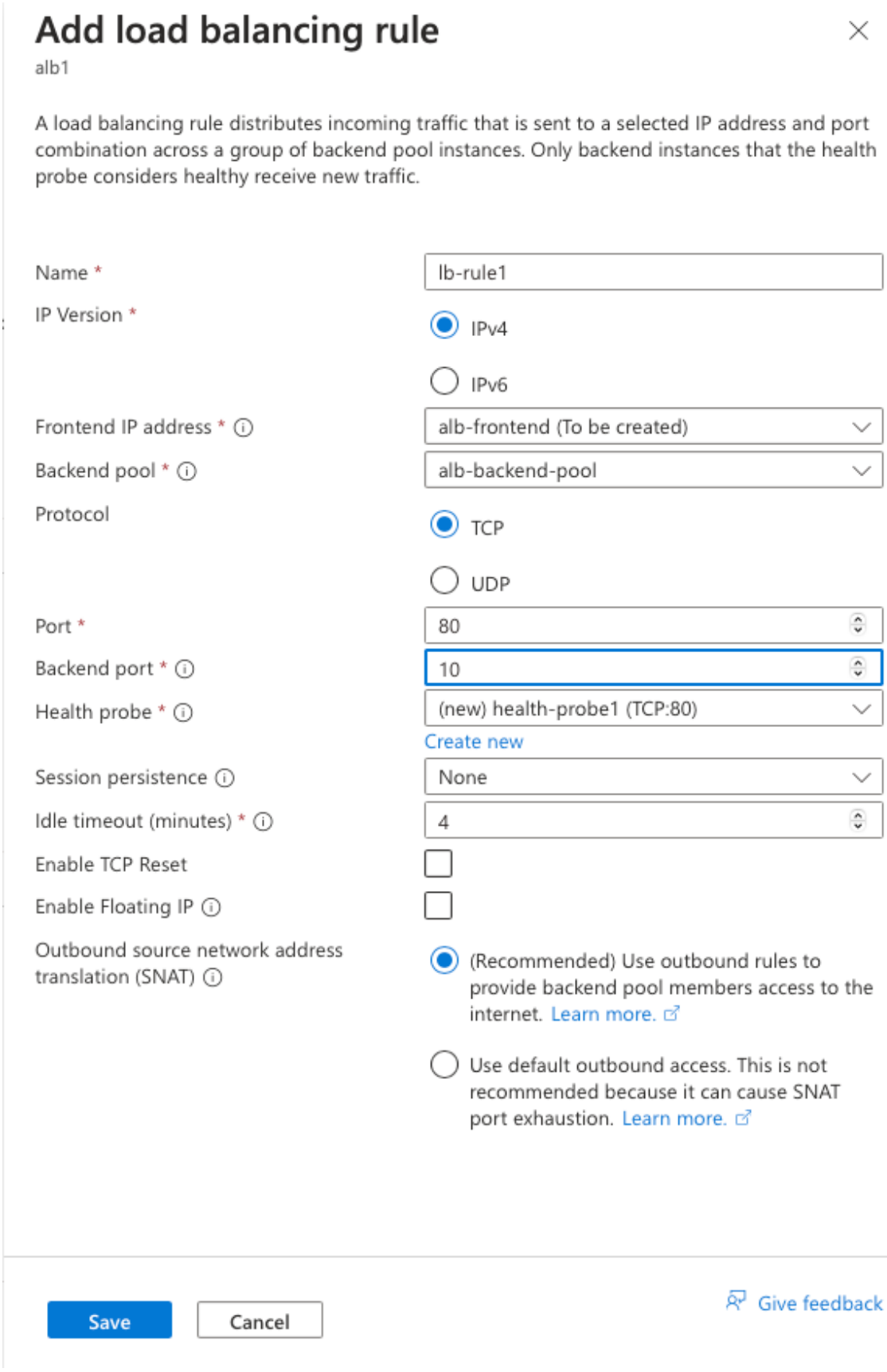




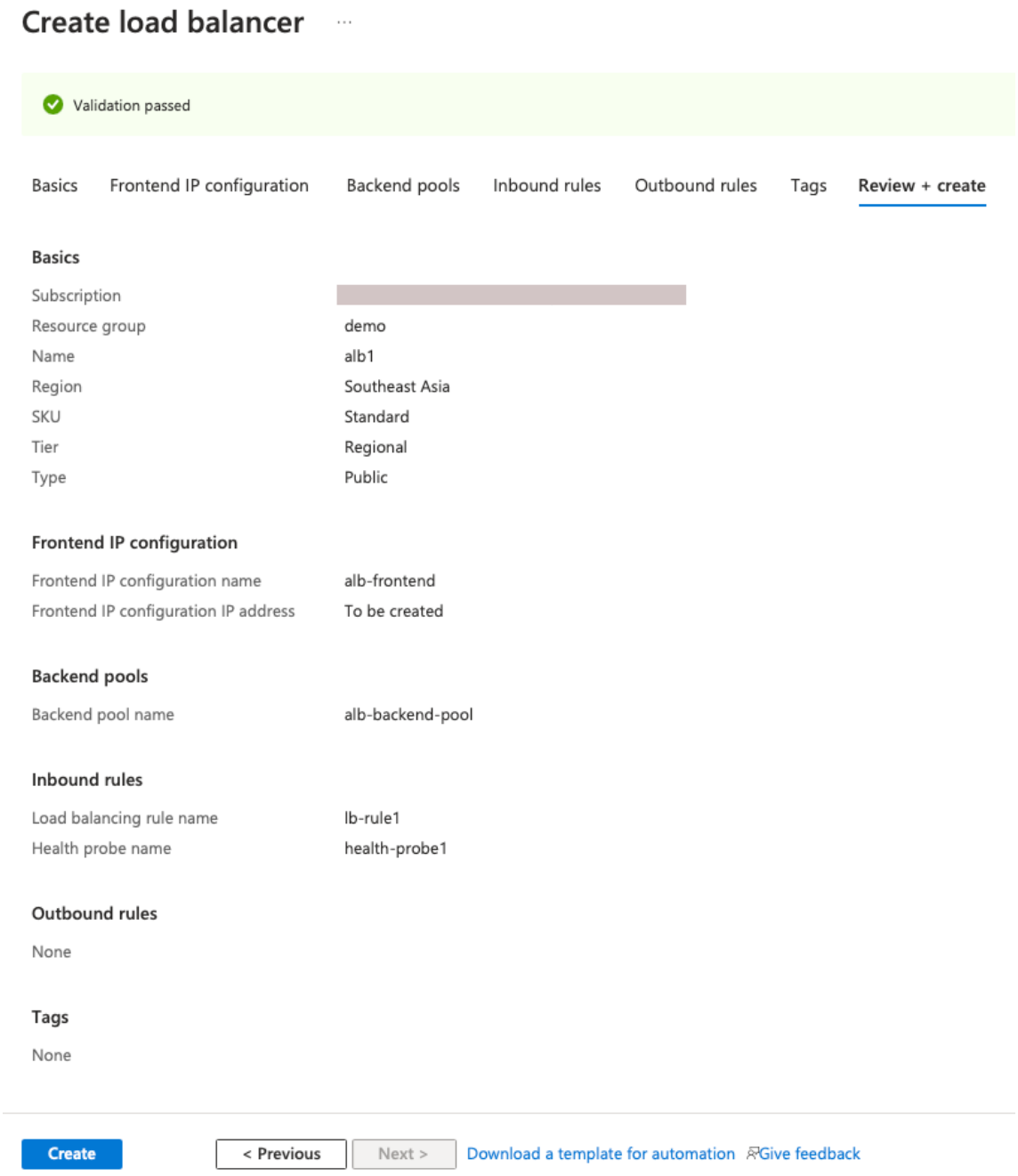
4. Wählen Sie auf der Registerkarte **Backend-Pools** die NIC-basierte Backend-Poolkonfiguration aus und fügen Sie die Client-NICs der beiden NetScaler VMs hinzu.



5. Klicken Sie auf der Registerkarte **Eingehende Regeln** auf **Load Balancing-Regel hinzufügen**und geben Sie die Frontend-IP-Adresse und den Backend-Pool an, die in den vorherigen Schritten erstellt wurden. Wählen Sie das Protokoll und den Port basierend auf Ihren Anforderungen aus. Erstellen oder verwenden Sie eine vorhandene Gesundheitssonde. Deaktivieren Sie das Kontrollkästchen **Floating IP** aktivieren.



6. Klicken Sie auf **Review + Erstellen**. Nachdem die Überprüfung erfolgreich war, klicken Sie auf **Erstellen**.



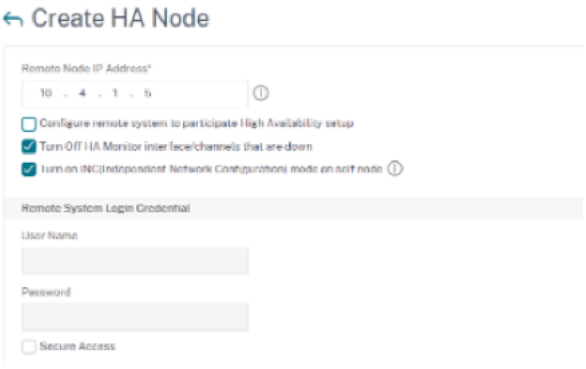
Schritt 4. Konfigurieren Sie HA-Einstellungen auf beiden NetScaler VPX-Instanzen mithilfe der NetScaler GUI.

Nachdem Sie die NetScaler VPX-Instanzen in Azure erstellt haben, können Sie HA mithilfe der NetScaler GUI konfigurieren.

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

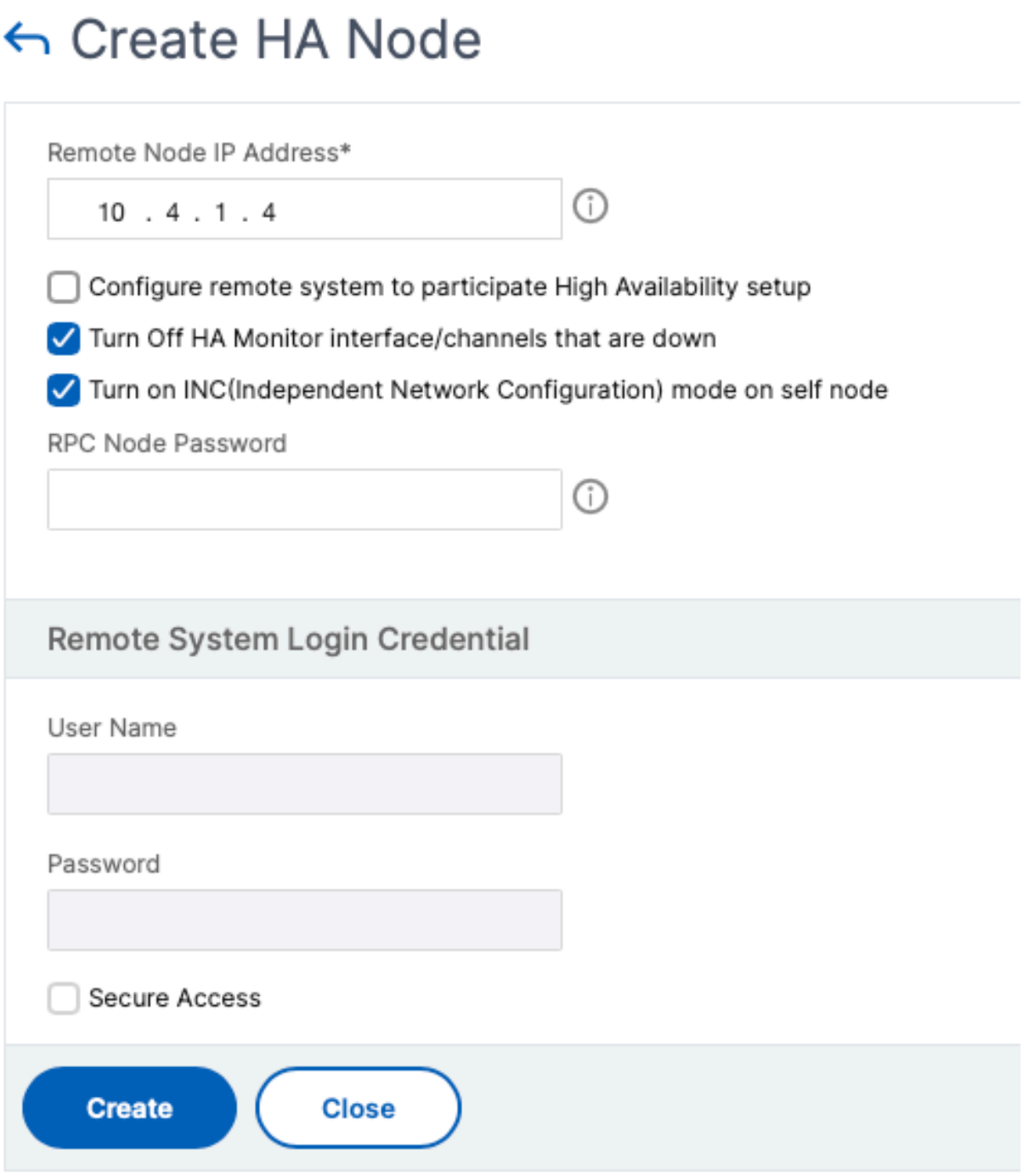
Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem bei der Bereitstellung der Instanz angegebenen Benutzernamen und Kennwort von `nsroot` an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node-IP-Adresse** die private IP-Adresse der Management-NIC der sekundären Instanz ein, z. B.: 10.4.1.5.
4. Aktivieren Sie das Kontrollkästchen **INC-Modus (Independent Network Configuration) auf eigenem Knoten** einschalten.
5. Klicken Sie auf **Erstellen**.



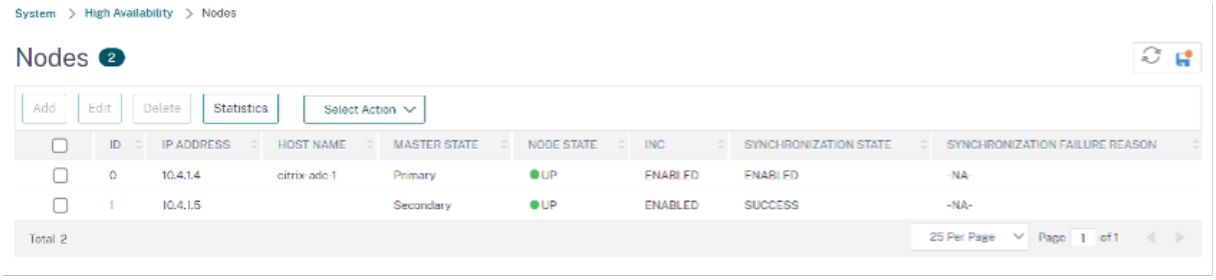
Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem bei der Bereitstellung der Instanz angegebenen Benutzernamen und Kennwort von `nsroot` an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node-IP-Adresse** die private IP-Adresse der Management-NIC der primären Instanz ein, z. B.: 10.4.1.4.
4. Aktivieren Sie das Kontrollkästchen **INC-Modus (Independent Network Configuration) auf eigenem Knoten** einschalten.
5. Klicken Sie auf **Erstellen**.



Bevor Sie fortfahren, stellen Sie sicher, dass der **Synchronisierungsstatus** der sekundären Instanz auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

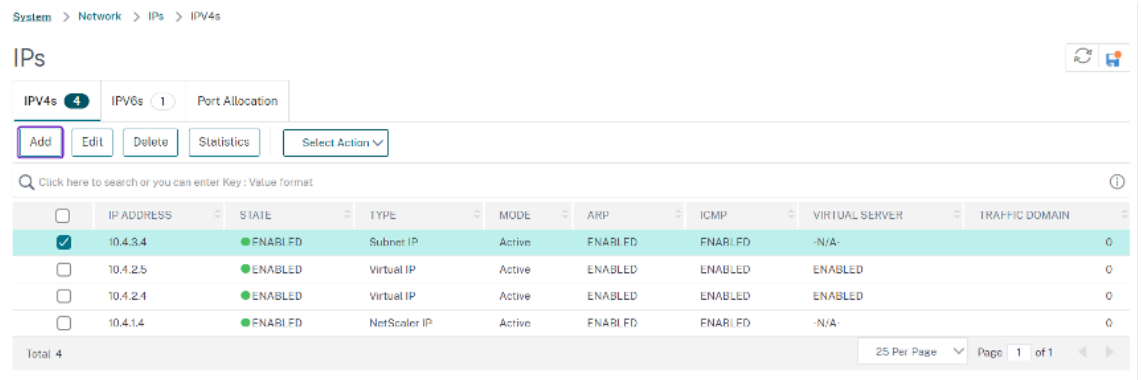
> **Hinweis:**
>
> Jetzt hat die sekundäre Instanz dieselben Anmeldeinformationen wie die primäre Instanz.



Schritt 2. Fügen Sie auf beiden Instanzen virtuelle IP-Adresse und Subnetz-IP-Adresse hinzu.

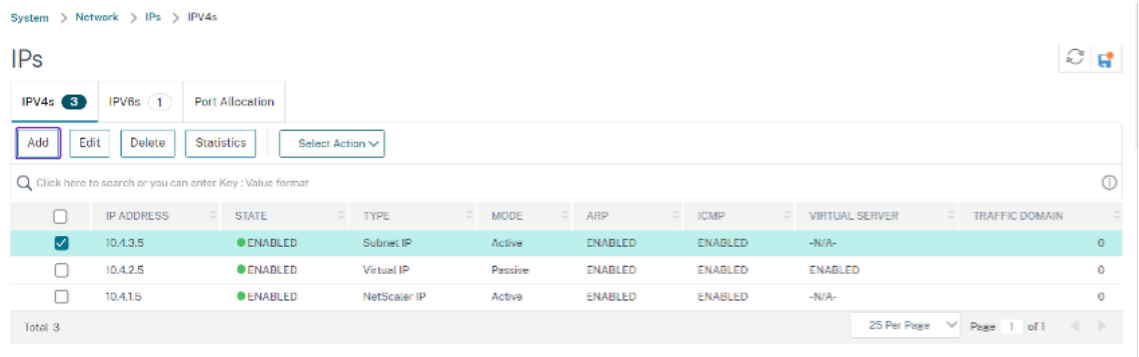
Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die private IP-Adresse der Client-NIC der primären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Server-NIC der primären Instanz und die für das Serversubnetz in der primären Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

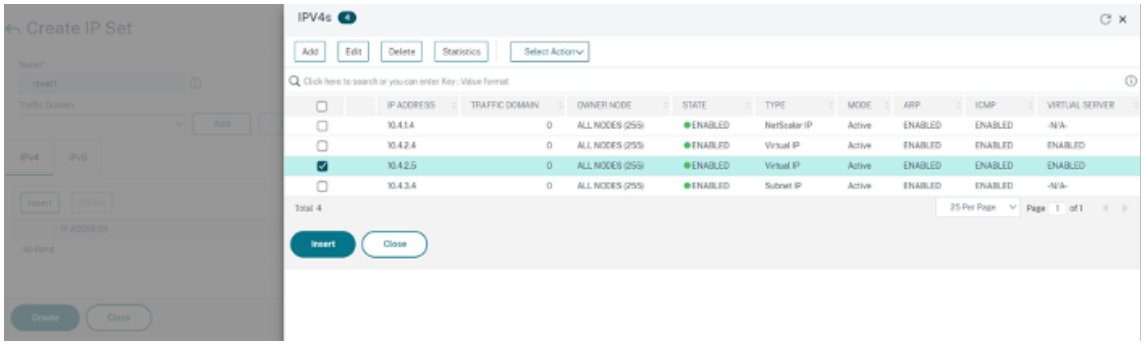
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Server-NIC der sekundären Instanz und die für das Serversubnetz in der sekundären Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Schritt 3: Fügen Sie IP-Set hinzu und binden Sie die IP, die an den sekundären VIP auf beiden Instanzen festgelegt ist.

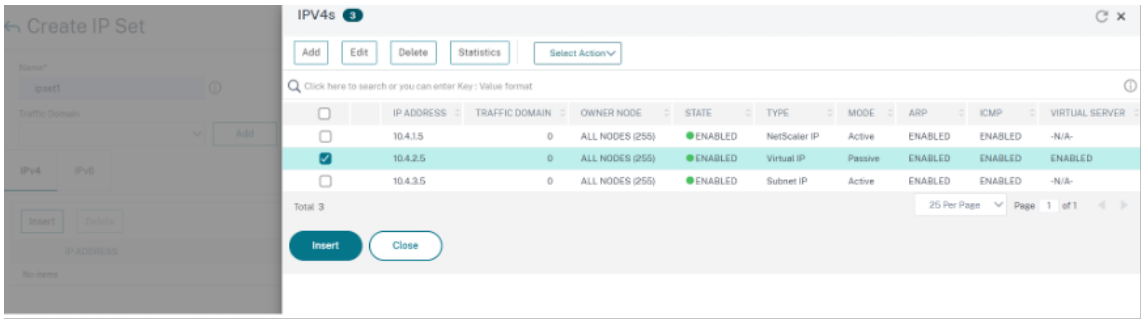
Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. **Schritt 2.** Fügen Sie den IP-Satz in beiden Instanzen hinzu.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

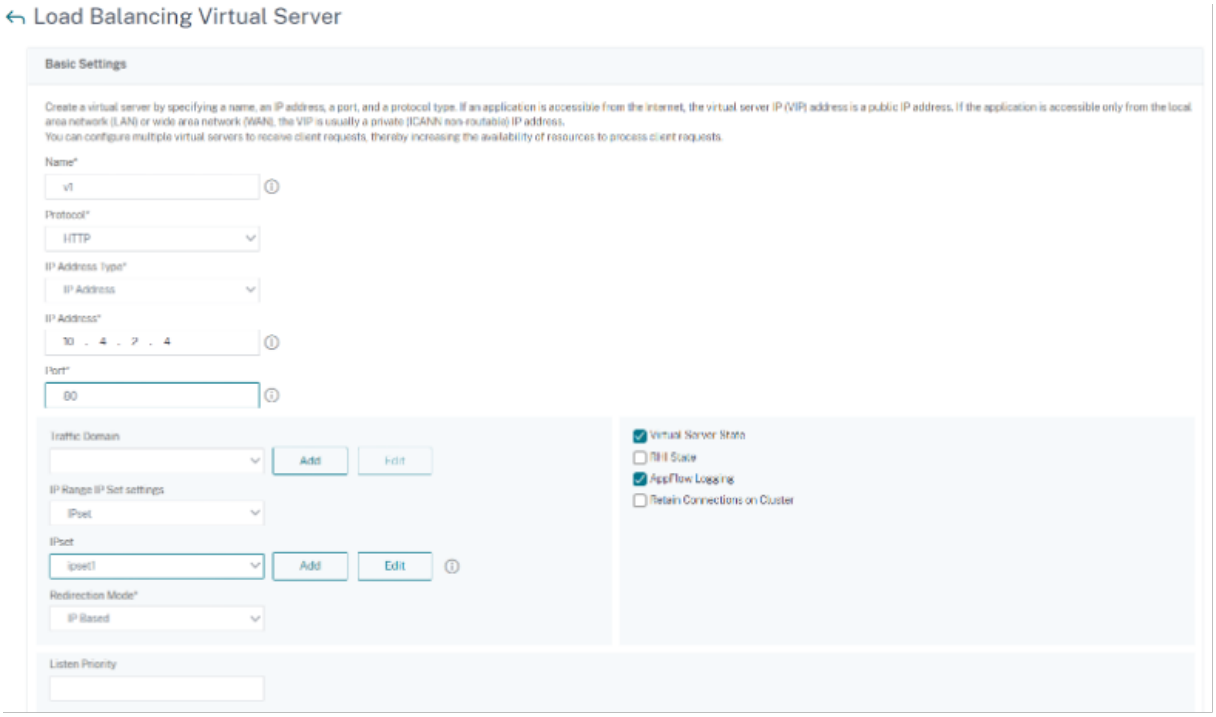
1. **Schritt 2.** Fügen Sie den IP-Satz in beiden Instanzen hinzu.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der Seite **IPv4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



> **Hinweis:**
>
> Der Name des IP-Sets muss sowohl auf der primären als auch auf der sekundären Instanz identisch sein.

Schritt 4. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf der primären Instanz.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäres VIP) und Port hinzu.
3. Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen**, wählen Sie im Dropdownmenü **IPset** aus und geben Sie das in **Schritt 3** erstellte IPset ein.
4. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

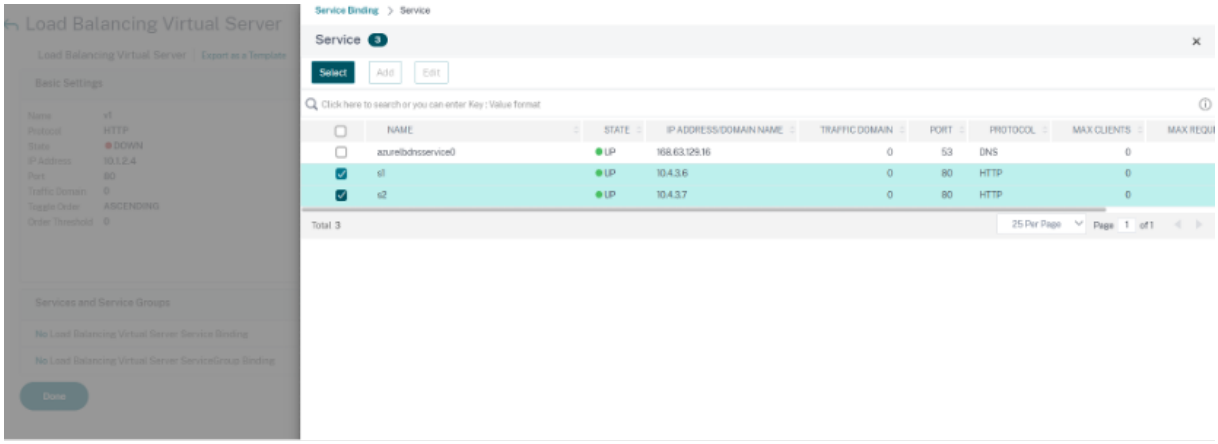


Schritt 5. Fügen Sie der primären Instanz einen Dienst oder eine Servicegruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 6. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf der primären Instanz.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 4**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 5**konfigurierten Dienst aus und klicken Sie auf "**Binden**".



Schritt 7: Speichern Sie die Konfiguration.

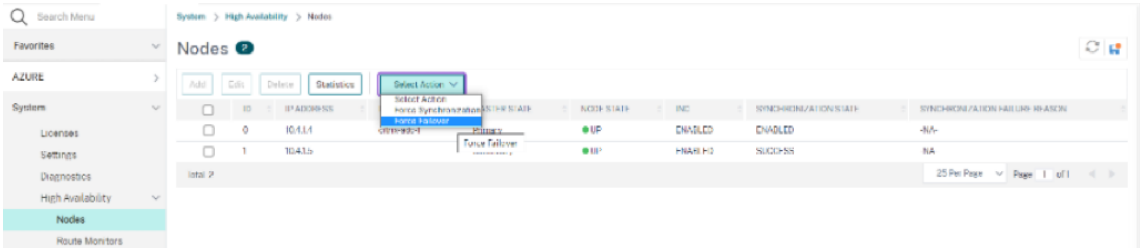
Andernfalls geht die gesamte Konfiguration nach einem Neustart oder einem sofortigen Neustart verloren.

Schritt 8: Überprüfen Sie die Konfiguration.

Stellen Sie sicher, dass die ALB-Frontend-IP-Adresse nach einem Failover erreichbar ist.

1. Kopieren Sie die ALB-Frontend-IP-Adresse.
2. Fügen Sie die IP-Adresse in den Browser ein und stellen Sie sicher, dass die Backend-Server erreichbar sind.
3. Führen Sie auf der primären Instanz Failover durch:

   Navigieren Sie in der NetScaler GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.



4. Stellen Sie sicher, dass Backend-Server nach einem Failover über die zuvor verwendete ALB-Frontend-IP erreichbar sind.

Stellen Sie eine private NetScaler for Azure DNS-Zone bereit

October 17, 2024

Azure DNS ist ein Dienst in der Microsoft Azure-Infrastruktur zum Hosten von DNS-Domänen und zur Bereitstellung von Namensauflösung.

Private Azure DNS-Zonen sind ein Dienst, der sich auf die Auflösung von Domainnamen in einem privaten Netzwerk konzentriert. Mit privaten Zonen können Kunden ihre eigenen benutzerdefinierten Domainnamen anstelle der derzeit von Azure bereitgestellten Namen verwenden.

NetScaler, die führende Lösung für die Anwendungsbereitstellung, eignet sich am besten für die Bereitstellung von Lastenausgleichs- und GSLB-Funktionen für eine private Azure DNS-Zone. Durch das Abonnement der Azure DNS Private Zone kann sich das Unternehmen auf die Leistung und Intelligenz von NetScaler Global Server Load Balancing (GSLB) verlassen, um den Intranetverkehr auf Workloads in mehreren Regionen und über Rechenzentren zu verteilen, die über sichere VPN-Tunnel verbunden sind. Diese Zusammenarbeit garantiert Unternehmen den nahtlosen Zugriff auf einen Teil ihrer Arbeitslast, den sie in die Azure Public Cloud verlagern möchten.

Überblick über Azure DNS

Das Domain Name System (DNS) ist für die Übersetzung oder Auflösung eines Dienstnamens in seine IP-Adresse verantwortlich. Azure DNS ist ein Hosting-Service für DNS-Domänen und bietet Namensauflösung mithilfe der Microsoft Azure-Infrastruktur. Azure DNS unterstützt nicht nur mit dem Internet verbundene DNS-Domänen, sondern jetzt auch private DNS-Domänen.

Azure DNS bietet einen zuverlässigen, sicheren DNS-Dienst zur Verwaltung und Auflösung von Domainnamen in einem virtuellen Netzwerk, ohne dass eine benutzerdefinierte DNS-Lösung erforderlich ist. Durch die Verwendung von privaten DNS-Zonen können Sie anstelle der von Azure bereitgestellten Namen Ihre eigenen benutzerdefinierten Domainnamen verwenden. Mithilfe benutzerdefinierter Domainnamen können Sie Ihre virtuelle Netzwerkarchitektur optimal an die Bedürfnisse Ihres Unternehmens anpassen. Es bietet die Namensauflösung für virtuelle Maschinen (VMs) innerhalb eines virtuellen Netzwerks und zwischen virtuellen Netzwerken. Außerdem können Kunden Zonennamen mit einer Split-Horizon-Ansicht konfigurieren, sodass eine private und eine öffentliche DNS-Zone einen gemeinsamen Namen haben können.

Warum NetScaler GSLB für Azure DNS Private Zone?

In der heutigen Welt möchten Unternehmen ihre Workloads von lokalen Workloads auf die Azure-Cloud verlagern. Der Übergang zur Cloud ermöglicht es ihnen, die Markteinführungszeit, die Kapitalaufwand/den Preis, die einfache Implementierung und die Sicherheit zu nutzen. Der Azure DNS Private Zone Service bietet ein einzigartiges Angebot für Unternehmen, die einen Teil ihrer Workloads in die Azure Cloud verlagern. Diese Unternehmen können ihren privaten DNS-Namen, den sie jahrelang in lokalen Bereitstellungen hatten, erstellen, wenn sie den Private Zone Service nutzen. Bei diesem Hybridmodell von Intranet-Anwendungsservern, die sich lokal und in der Azure-Cloud befinden und

über sichere VPN-Tunnel verbunden sind, besteht die einzige Herausforderung darin, einen nahtlosen Zugriff auf diese Intranetanwendungen zu haben. NetScaler löst diesen einzigartigen Anwendungsfall mit seiner globalen Lastenausgleichsfunktion, die den Anwendungsdatenverkehr an die optimalsten verteilten Workloads/Server entweder vor Ort oder in der Azure-Cloud weiterleitet und den Integritätsstatus des Anwendungsservers bereitstellt.

Anwendungsfall

Benutzer in einem lokalen Netzwerk und in verschiedenen Azure-VNets können eine Verbindung zu den optimalsten Servern in einem internen Netzwerk herstellen, um auf die erforderlichen Inhalte zuzugreifen. Dadurch wird sichergestellt, dass die Anwendung immer verfügbar ist, die Kosten optimiert werden und die Benutzererfahrung gut ist. Azure Private Traffic Management (PTM) ist hier die Hauptanforderung. Azure PTM stellt sicher, dass die DNS-Abfragen der Benutzer zu einer geeigneten privaten IP-Adresse des Anwendungsservers aufgelöst werden.

Lösung für Anwendungsfälle

NetScaler enthält die GSLB-Funktion (Global Server Load Balancing), um die Azure PTM-Anforderungen zu erfüllen. GSLB verhält sich wie ein DNS-Server, der die DNS-Anfragen empfängt und die DNS-Anfrage in eine geeignete IP-Adresse auflöst, um Folgendes bereitzustellen:

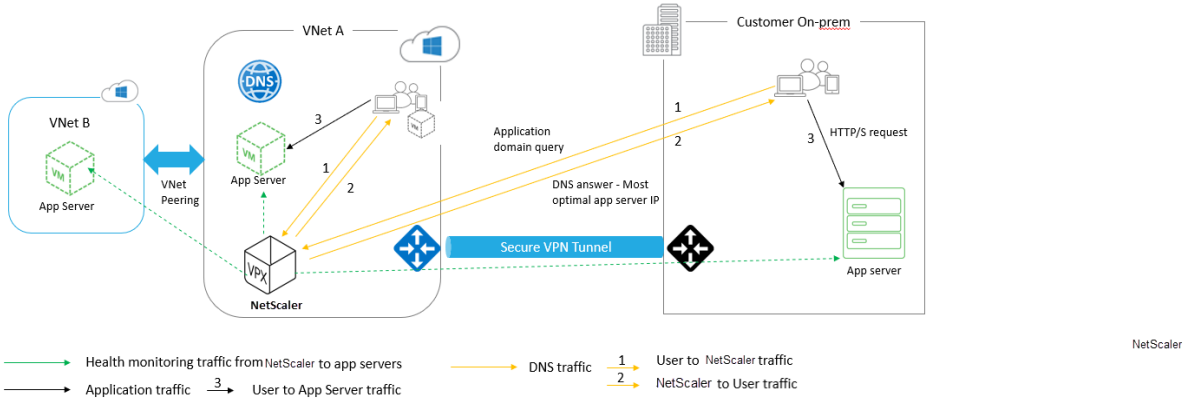
- Reibungsloser DNS-basierter Failover.
- Schrittweise Migration von On-Premise zur Cloud.
- A/B-Tests einer neuen Funktion.

Unter den vielen unterstützten Lastausgleichsmethoden können die folgenden Methoden in dieser Lösung nützlich sein:

1. Runde Robin
2. Statische Nähe (standortbasierte Serverauswahl). Es kann auf zwei Arten eingesetzt werden:
    a) Auf EDNS Client Subnet (ECS) basierendes GSLB auf NetScaler.
    b) Stellen Sie für jedes virtuelle Netzwerk einen DNS-Forwarder bereit.

Topologie

Die folgende Abbildung zeigt die NetScaler GSLB-Bereitstellung für eine private Azure-DNS-Zone.



Ein Benutzer kann auf jeden Anwendungsserver entweder in Azure oder vor Ort zugreifen, der auf der NetScaler GSLB-Methode in einer privaten Azure-DNS-Zone basiert. Der gesamte Datenverkehr zwischen dem lokalen und dem virtuellen Azure-Netzwerk erfolgt ausschließlich über einen sicheren VPN-Tunnel. Anwendungsverkehr, DNS-Verkehr und Überwachungsverkehr werden in der vorherigen Topologie angezeigt. Abhängig von der erforderlichen Redundanz können NetScaler und DNS-Forwarder in den virtuellen Netzwerken und Rechenzentren eingesetzt werden. Der Einfachheit halber wird hier nur ein NetScaler angezeigt, aber wir empfehlen mindestens einen Satz NetScaler und DNS-Forwarder für die Azure-Region. Alle Benutzer-DNS-Abfragen werden zunächst an den DNS-Forwarder weitergeleitet, für den Regeln für die Weiterleitung der Anfragen an einen geeigneten DNS-Server definiert sind.

Konfiguration von NetScaler für die private Azure DNS-Zone

Getestete Produkte und Versionen:

Product	Version
Azure	Cloud-Abonnement
NetScaler VPX	BYOL (Bringen Sie Ihre eigene Lizenz mit)

> **Hinweis:**
>
> Die Bereitstellung wurde getestet und bleibt mit NetScaler Version 12.0 und höher unverändert.

Voraussetzungen

Im Folgenden sind allgemeine Voraussetzungen aufgeführt.

- Microsoft Azure-Portalkonto mit einem gültigen Abonnement.

- Stellen Sie die Konnektivität (Secure VPN Tunnel) zwischen On-Prem und Azure Cloud sicher. Informationen zum Einrichten eines sicheren VPN-Tunnels in Azure finden Sie unter Schritt für Schritt: Konfiguration eines Site-to-Site-VPN-Gateways zwischen Azure und on-premises.

Lösungsbeschreibung

Wenn Sie eine Anwendung hosten möchten, die private Azure-DNS-Zone (rr.ptm.mysite.net), die auf HTTPs läuft und in Azure und lokal mit Intranetzugriff bereitgestellt wird, der auf der Round-Robin-GSLB-Lastenausgleichsmethode basiert. Um diese Bereitstellung zu erreichen, aktivieren Sie GSLB für die private Azure-DNS-Zone mit NetScaler, die aus den folgenden Konfigurationen besteht:

1. Konfigurieren Sie das Azure- und On-Premises-Setup.
2. NetScaler-Appliance im virtuellen Azure-Netzwerk.

Azure- und On-Premises-Setup konfigurieren

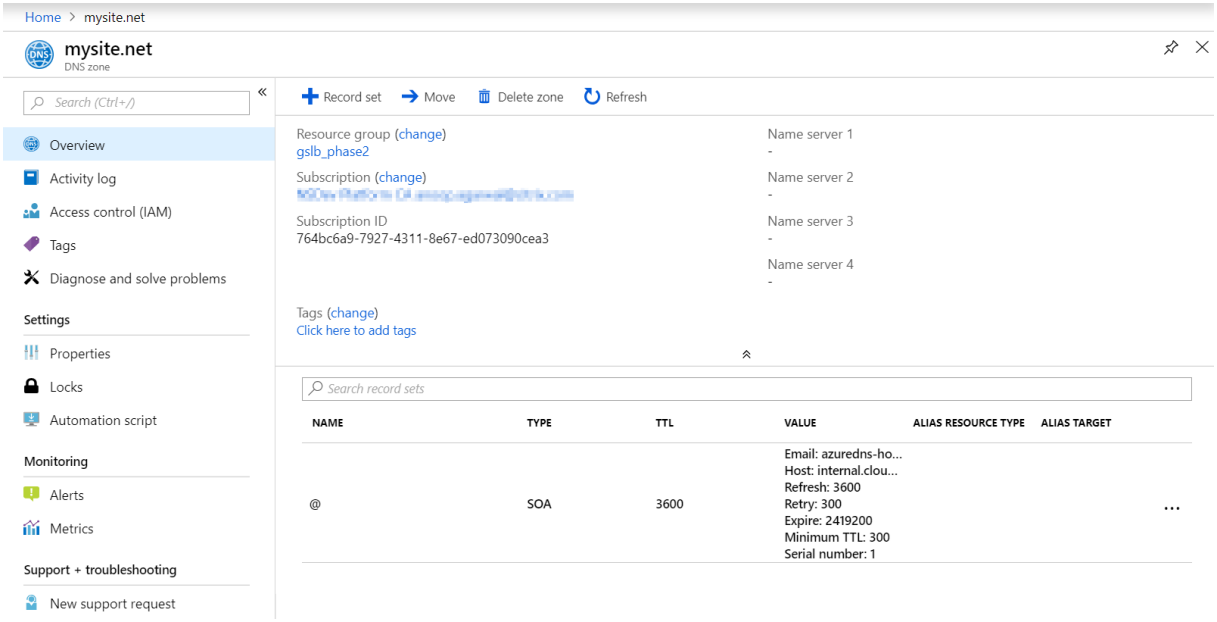
Richten Sie, wie in der Topologie gezeigt, das virtuelle Azure-Netzwerk (in diesem Fall VNet A, VNet B) und das lokale Setup ein.

1. Erstellen Sie eine private Azure-DNS-Zone mit dem Domainnamen (mysite.net).
2. Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.
3. Stellen Sie App Server, DNS-Forwarder, Windows 10 Pro-Client und NetScaler in VNet A bereit.
4. Stellen Sie einen App Server bereit und stellen Sie einen DNS-Forwarder bereit, falls sich Clients in VNet B befinden.
5. Stellen Sie einen App-Server, eine DNS-Weiterleitung und einen Windows 10 Pro-Client vor Ort bereit.

Private Azure-DNS-Zone

Erstellen Sie eine private Azure-DNS-Zone mit einem Domainnamen.

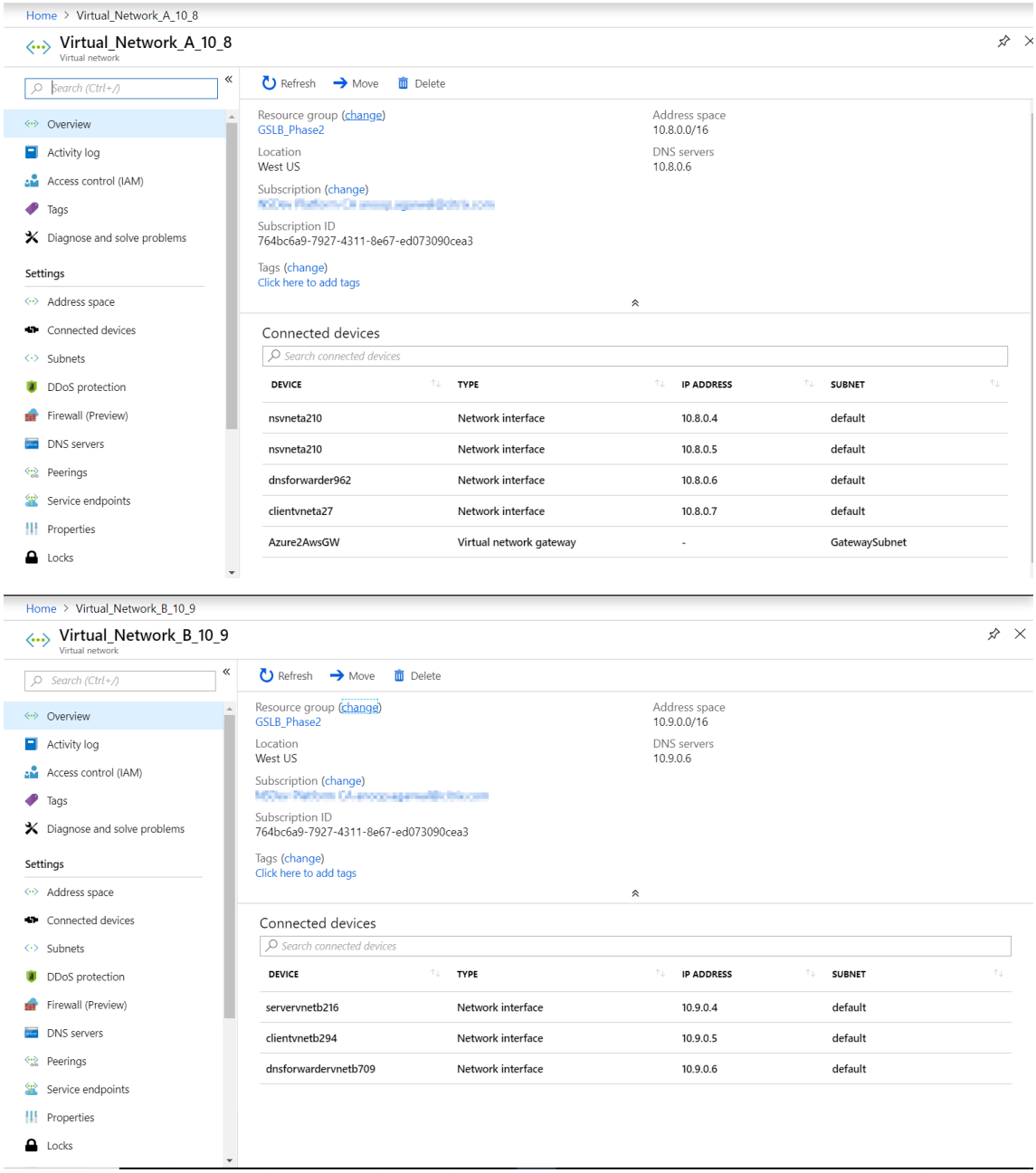
1. Melden Sie sich im Azure-Portal an und wählen Sie ein Dashboard aus oder erstellen Sie es.
2. Klicken Sie auf **Ressource erstellen und suchen Sie nach der DNS-Zone, um eine** private Azure-DNS-Zone mit dem Domänennamen (mysite.net) zu erstellen (in diesem Fall mysite.net).



Virtuelle Azure-Netzwerke (VNet A, VNet B) im Hub-and-Spoke-Modell

Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.

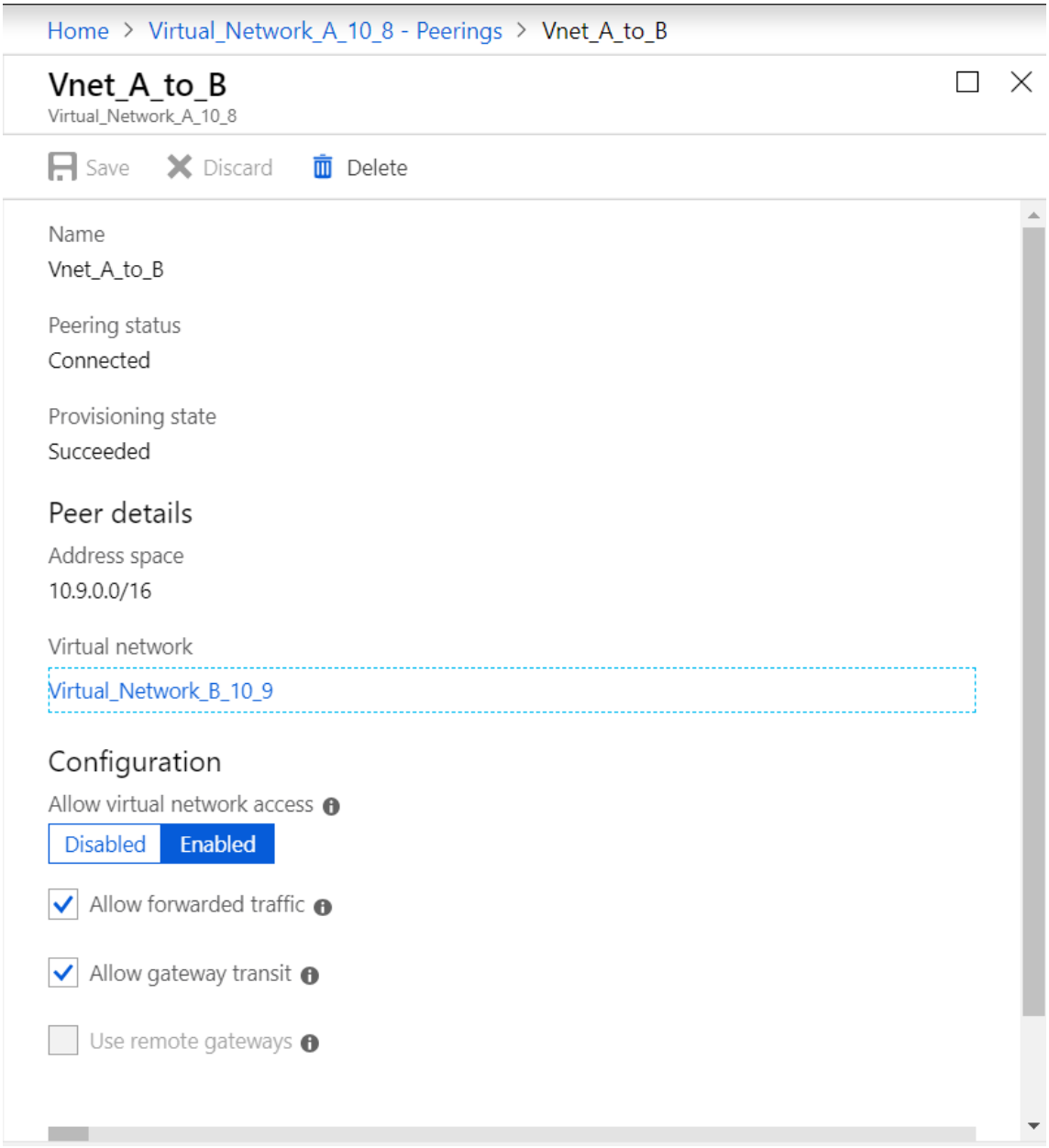
1. Erstellen Sie zwei virtuelle Netzwerke.
2. Wählen Sie dasselbe Dashboard aus, klicken Sie auf **Ressource erstellen** und suchen Sie nach virtuellen Netzwerken, um zwei virtuelle Netzwerke, nämlich VNet A und VNet B, in derselben Region zu erstellen und sie miteinander zu verbinden, um ein Hub-and-Spoke-Modell zu bilden, wie in der folgenden Abbildung gezeigt. Weitere Informationen zum Einrichten einer Hub-and-Spoke-Topologie finden Sie unter Implementieren einer Hub-Spoke-Netzwerktopologiein Azure.



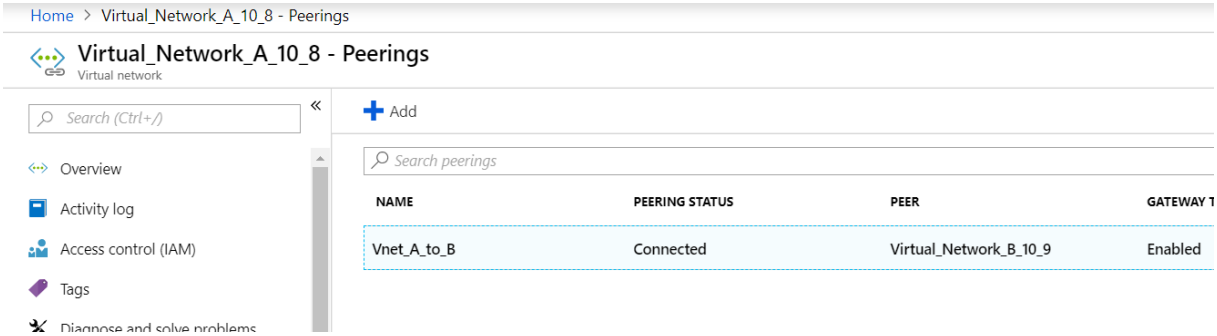
Peering von VNet A zu VNet B

Um VNet A und VNet B miteinander zu verbinden:

1. Klicken Sie im **Einstellungsmenü** von VNet A und **Peer-VNet B auf Peerings** .
2. Aktivieren **Sie Weitergeleiteten Verkehrzulassen und Gateway-Transit** zulassen, wie in der folgenden Abbildung gezeigt.



Die folgende Abbildung zeigt das erfolgreiche Peering von VNet A zu VNet B.



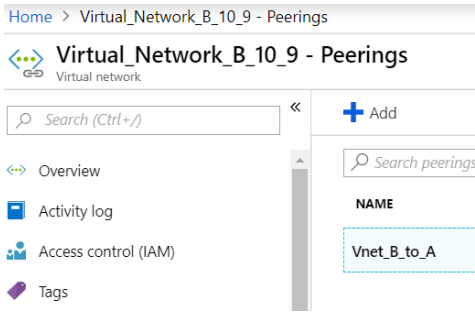
Peering von VNet B zu VNet A

Zum Peering von VNet B und VNet A:

1. Klicken Sie im **Einstellungsmenü** von VNet B und **Peer-VNet A auf Peerings** .
2. Aktivieren **Sie Weitergeleiteten Verkehr zulassen** und verwenden Sie Remote-Gateways, wie in der folgenden Abbildung gezeigt.

```
1 ![VNet B to A](/en-us/vpx/media/image-07.png)
```

Die folgende Abbildung zeigt das erfolgreiche Peering von VNet B zu VNet A.



App-Server, DNS-Forwarder, Windows 10 Pro-Client und NetScaler in VNet A bereitstellen

Wir besprechen kurz den App-Server, den DNS-Forwarder, den Windows 10 Pro-Client und NetScaler auf VNet A.

1. Wählen Sie dasselbe Dashboard aus und klicken Sie **auf Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP aus dem VNet A-Subnetz zu.

App-Server App-Server ist nichts anderes als der Webserver (HTTP-Server), auf dem ein Ubuntu-Server 16.04 als Instanz auf der Azure- oder lokalen VM bereitgestellt wird. Um ihn als Webserver einzurichten, geben Sie an der Befehlszeile Folgendes ein:

```
sudo apt install apache2
```

Windows 10 Pro-Client Starten Sie die Windows 10 Pro-Instanz als Client-Computer auf VNet A und lokal.

NetScaler NetScaler ergänzt die private Zone von Azure DNA durch Health Check und Analytics von NetScaler MAS. Starten Sie je nach Ihren Anforderungen einen NetScaler vom Azure Marketplace aus. Hier haben wir NetScaler (BYOL) für diese Bereitstellung verwendet.

Für die detaillierten Schritte zur Bereitstellung von NetScaler auf Microsoft Azure. Siehe Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure.

Verwenden Sie nach der Bereitstellung NetScaler IP, um NetScaler GSLB zu konfigurieren.

DNS-Weiterleitung Es wird verwendet, um die Client-Anfragen von gehosteten Domänen weiterzuleiten, die an NetScaler GSLB (ADNS IP) gebunden sind. Starten Sie einen Ubuntu-Server 16.04 als Linux-Instanz (Ubuntu-Server 16.04) und finden Sie unter der folgenden URL, wie Sie ihn als DNS-Forwarder einrichten.

> **Hinweis:**
>
> Für die Round Robin GSLB-Lastausgleichsmethode ist ein DNS-Forwarder für die Azure-Region ausreichend, aber für Static Proximity benötigen wir einen DNS-Forwarder pro virtuellem Netzwerk.

1. Ändern Sie nach der Bereitstellung der Forwarder die DNS-Servereinstellungen des virtuellen Netzwerks A von Standard auf Benutzerdefiniert mit VNet A-DNS-Forwarder-IP, wie in der folgenden Abbildung gezeigt.
2. Ändern Sie die `named.conf.options` Datei in VNet A DNS-Forwarder, um Weiterleitungsregeln für Domain (mysite.net) und Subdomain (ptm.mysite.net) zur ADNS-IP von NetScaler GSLB hinzuzufügen.
3. Starten Sie den DNS-Forwarder neu, um die in der Datei `named.conf.options` vorgenommenen Änderungen widerzuspiegeln.

DNS-Forwarder-Einstellungen für VNet A

```
      zone "mysite.net" {

                  type forward;
      forwarders {
  168.63.129.16;  }
;
       }
;
      zone "ptm.mysite.net" {

          type forward;
          forwarders {
  10.8.0.5;  }
;
       }
;
```

> **Hinweis:**
>
> Verwenden Sie für die Zonen-IP-Adresse der Domäne („mysite.net“) die DNS-IP-Adresse Ihrer

> Azure-Region. Verwenden Sie für die IP-Adresse der Subdomain (“ptm.mysite.net”) Zone alle ADNS-IP-Adressen Ihrer GSLB-Instanzen.

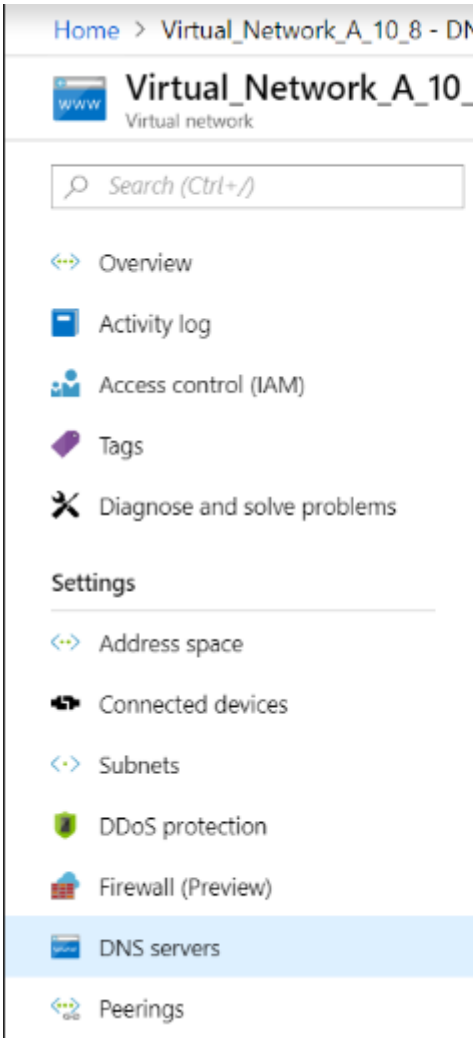
Stellen Sie einen App-Server und einen DNS-Forwarder bereit, wenn sich Clients in VNet B befinden

1. Wählen Sie für das virtuelle Netzwerk B dasselbe Dashboard aus und klicken Sie auf **Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP aus dem VNet B-Subnetz zu.
3. Starten Sie den App-Server und den DNS-Forwarder, wenn ein statischer Proximity-GSLB-Lastenausgleich ähnlich wie bei VNet A besteht.
4. Bearbeiten Sie die DNS-Forwarder-Einstellungen von VNet B `named.conf.options` wie in der folgenden Einstellung gezeigt:

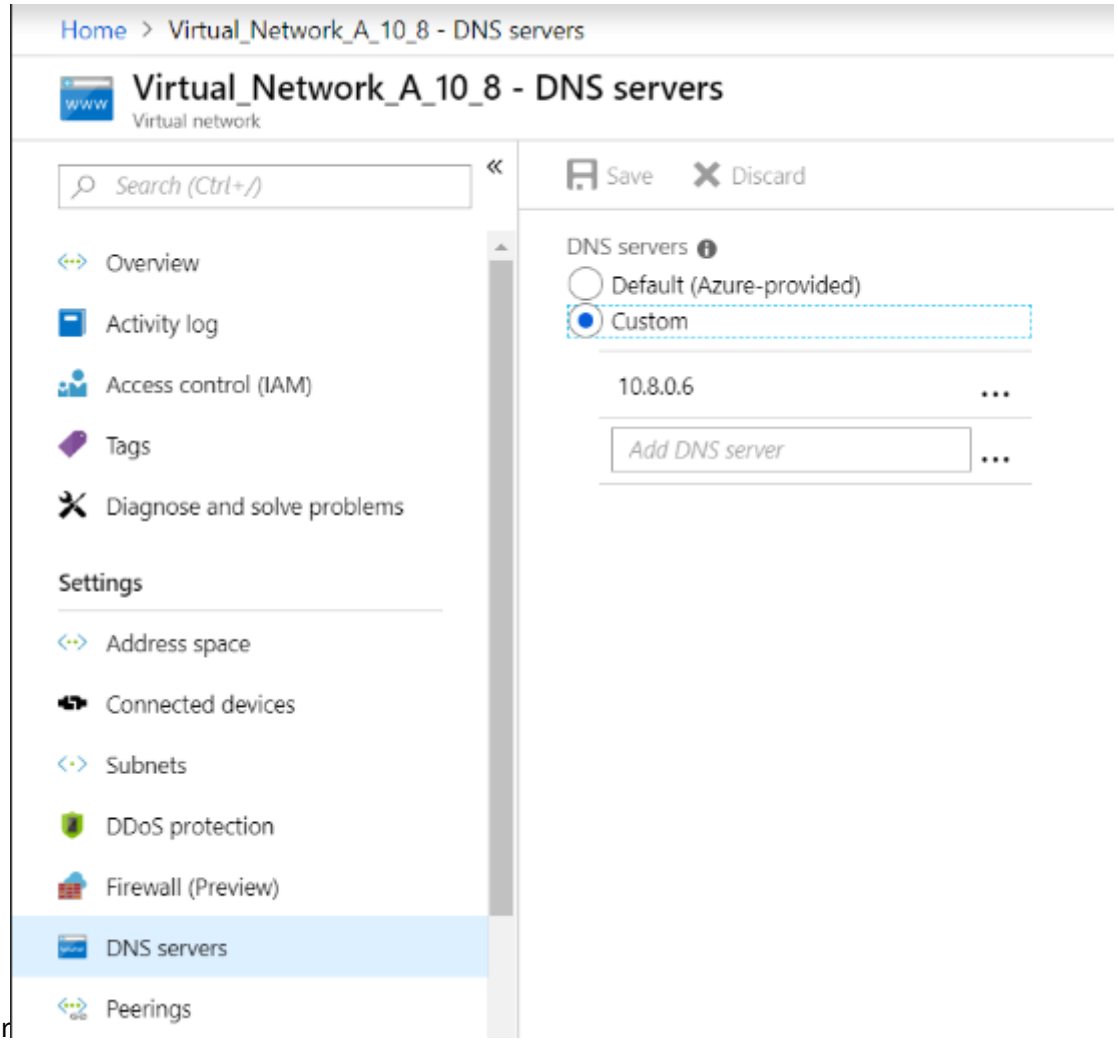
   DNS-Forwarder-Einstellungen für VNet B:

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


Die folgende Abbildung zeigt die DNS-Forwarder-Einstellungen von VNet B:



DNS-Server



App-Server, DNS-Forwarder und Windows 10 Pro-Client lokal bereitstellen

1. Starten Sie für lokale Umgebungen die VMs auf Bare Metal und verwenden Sie den App-Server, den DNS-Forwarder und den Windows 10 Pro-Client, der VNet A ähnelt.
2. Bearbeiten Sie die lokalen DNS-Forwarder-Einstellungen `named.conf.options` wie im folgenden Beispiel gezeigt.

Lokale DNS-Forwarder-Einstellungen

```
      zone "mysite.net" {

                  type forward;
                  forwarders {
 10.8.0.6;  }
;
       }
;
```



```
 9        zone "ptm.mysite.net" {
10
11            type forward;
12            forwarders {
13     10.8.0.5;  }
14    ;
15          }
16    ;
```

Denn `mysite.net`wir haben die DNS-Forwarder-IP von VNet A anstelle der IP des privaten DNS-Zonenservers von Azure angegeben, da es sich um eine spezielle IP-Adresse handelt, die von lokal aus nicht erreichbar ist. Daher ist diese Änderung in der DNS-Forwarder-Einstellung von On-premises erforderlich.

Konfigurieren Sie den NetScaler im virtuellen Azure-Netzwerk

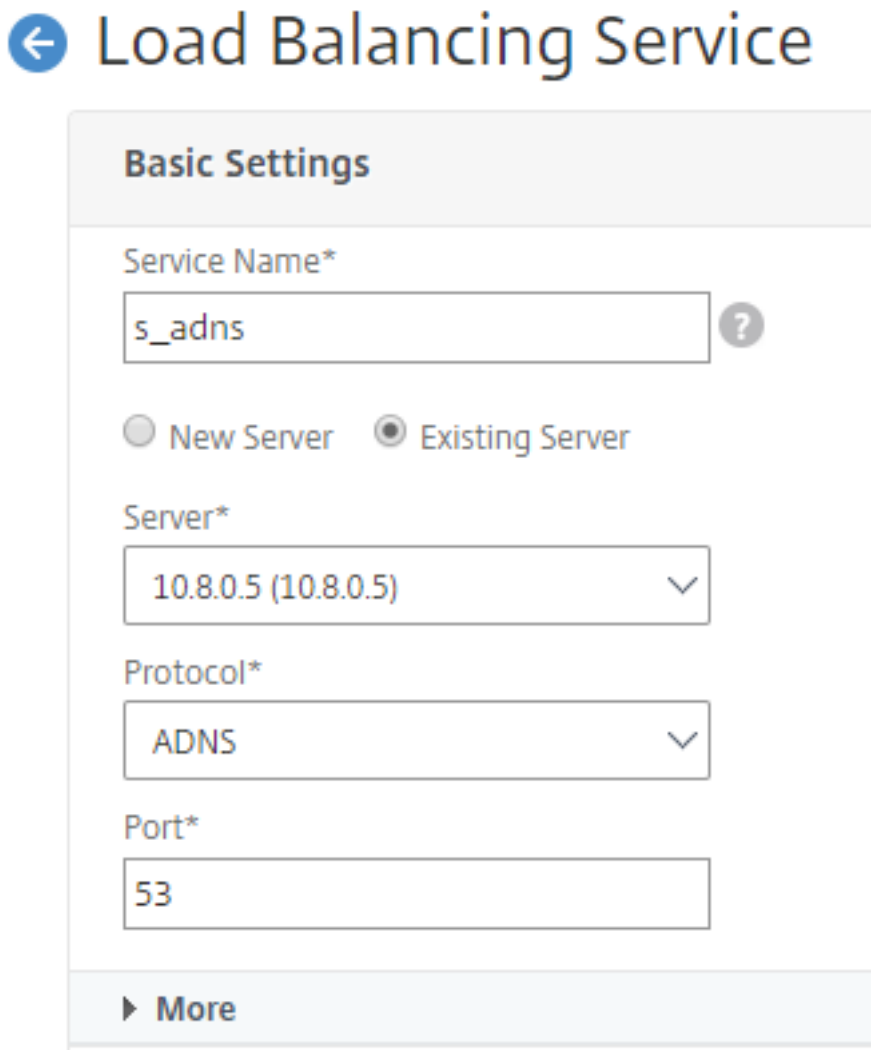
Wie in der Topologie gezeigt, stellen Sie NetScaler im virtuellen Azure-Netzwerk (in diesem Fall VNet A) bereit und greifen Sie über die NetScaler-GUI darauf zu.

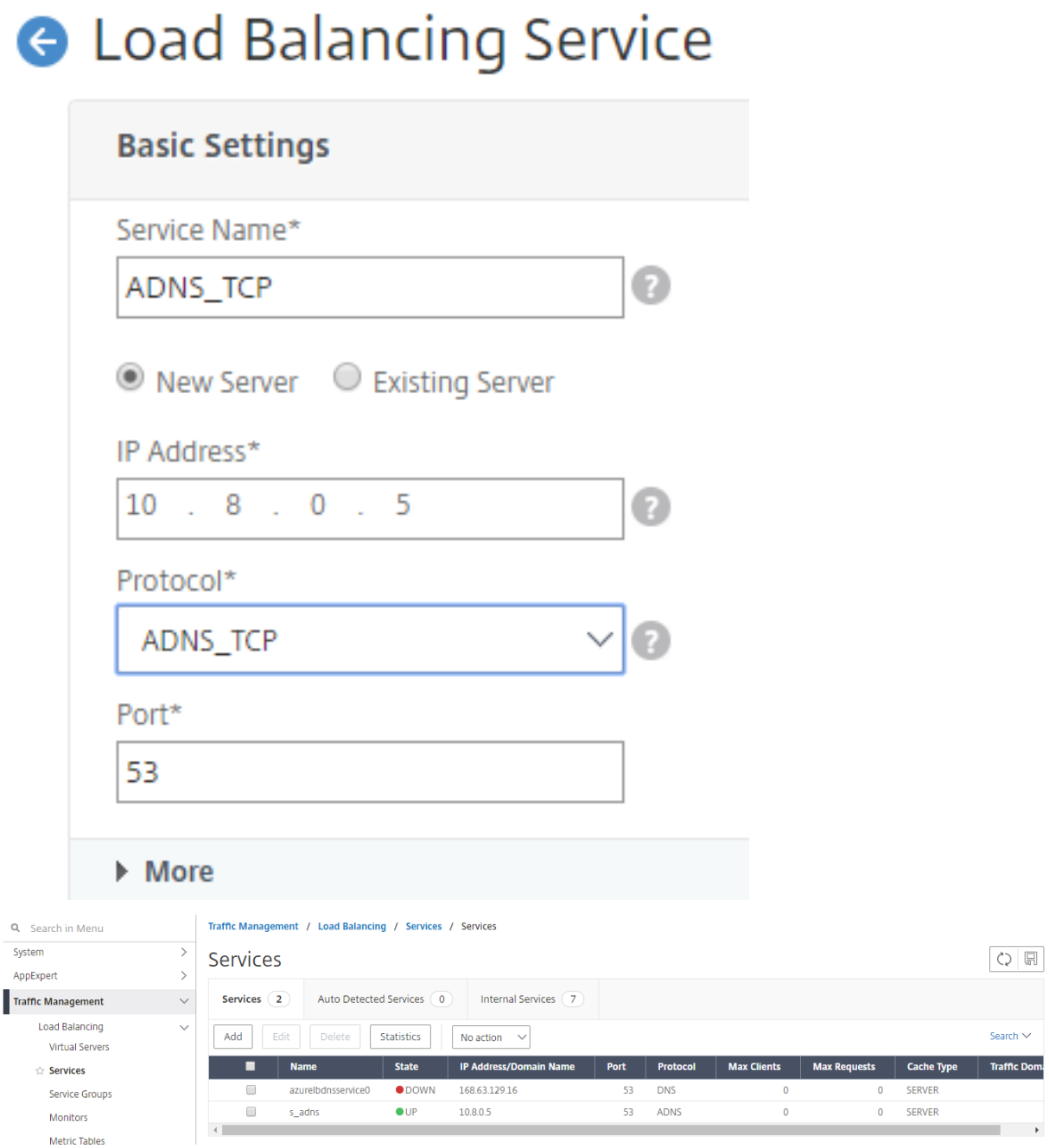
Konfiguration von NetScaler GSLB

1. Erstellen Sie einen ADNS-Dienst.
2. Erstellen Sie lokale und Remote-Sites.
3. Erstellen Sie Dienste für die lokalen virtuellen Server.
4. Erstellen Sie virtuelle Server für die GSLB-Dienste.

ADNS-Dienst hinzufügen

1. Melden Sie sich bei der NetScaler-GUI an.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > Load Balancing > Services**.
3. Fügen Sie einen Dienst hinzu. Wir empfehlen Ihnen, den ADNS-Dienst sowohl in TCP als auch in UDP zu konfigurieren, wie in der folgenden Abbildung gezeigt:

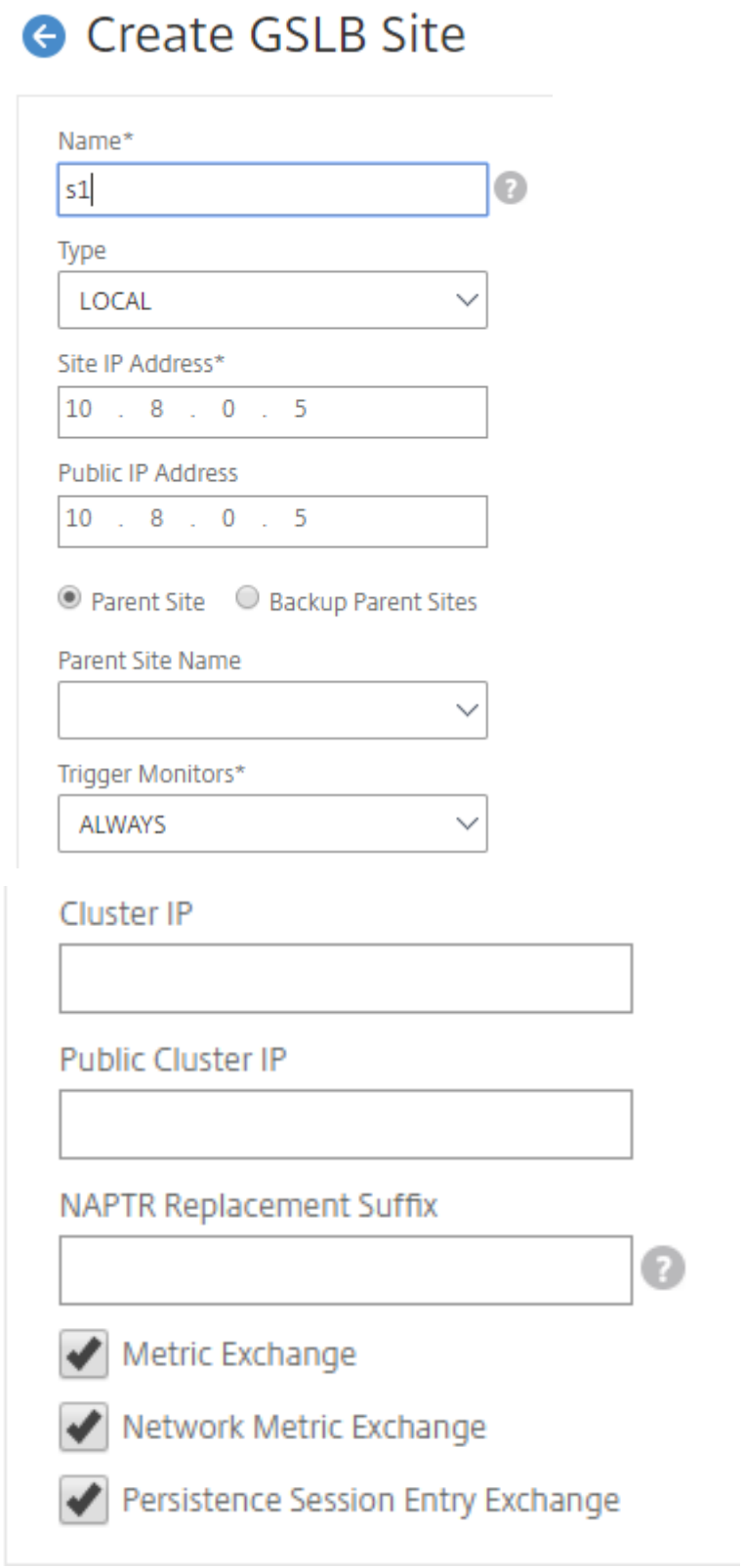


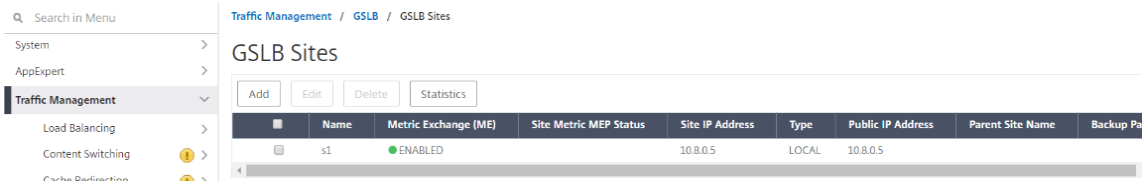


GSLB-Sites hinzufügen

1. Fügen Sie lokale und Remote-Sites hinzu, zwischen denen GSLB konfiguriert wird.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Datenverkehrsverwaltung > GSLB > GSLB-Sites** . Fügen Sie eine Site hinzu, wie im folgenden Beispiel gezeigt, und wiederholen Sie das gleiche Verfahren für andere Sites. Fügen Sie eine Site wie im folgenden Beispiel gezeigt

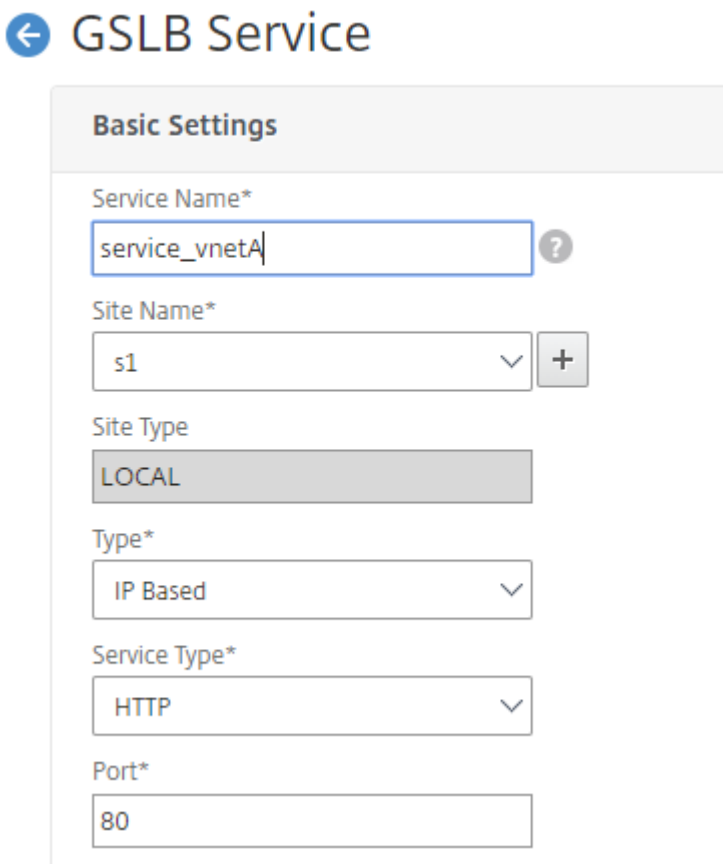
hinzu und wiederholen Sie den gleichen Vorgang für andere Sites.



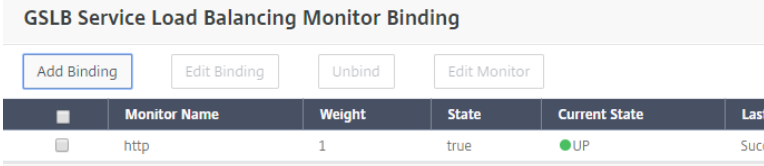


GSLB-Dienste hinzufügen

1. Fügen Sie GSLB-Dienste für die lokalen und virtuellen Remote-Server hinzu, die den Lastenausgleich für App-Server ermöglichen.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Services**.
3. Fügen Sie die Dienste wie in den folgenden Beispielen gezeigt hinzu.
4. Binden Sie den HTTP-Monitor, um den Serverstatus zu überprüfen.

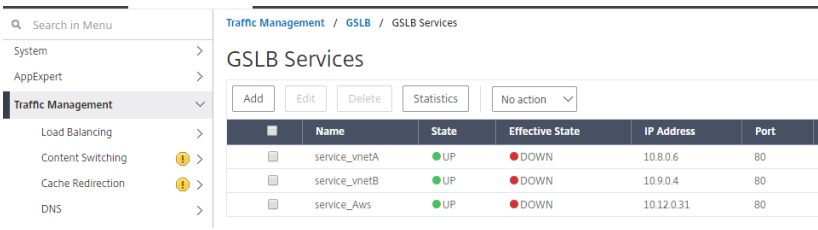


5. Nachdem Sie den Dienst erstellt haben, wechseln Sie im GSLB-Dienst zur Registerkarte **Erweiterte Einstellungen** .
6. Klicken Sie auf **Monitor hinzufügen**, um den GSLB-Dienst mit einem HTTP-Monitor zu verbinden und den Dienststatus aufzurufen.



7. Sobald Sie sich mit dem HTTP-Monitor verbinden, wird der Status der Dienste als UP markiert,

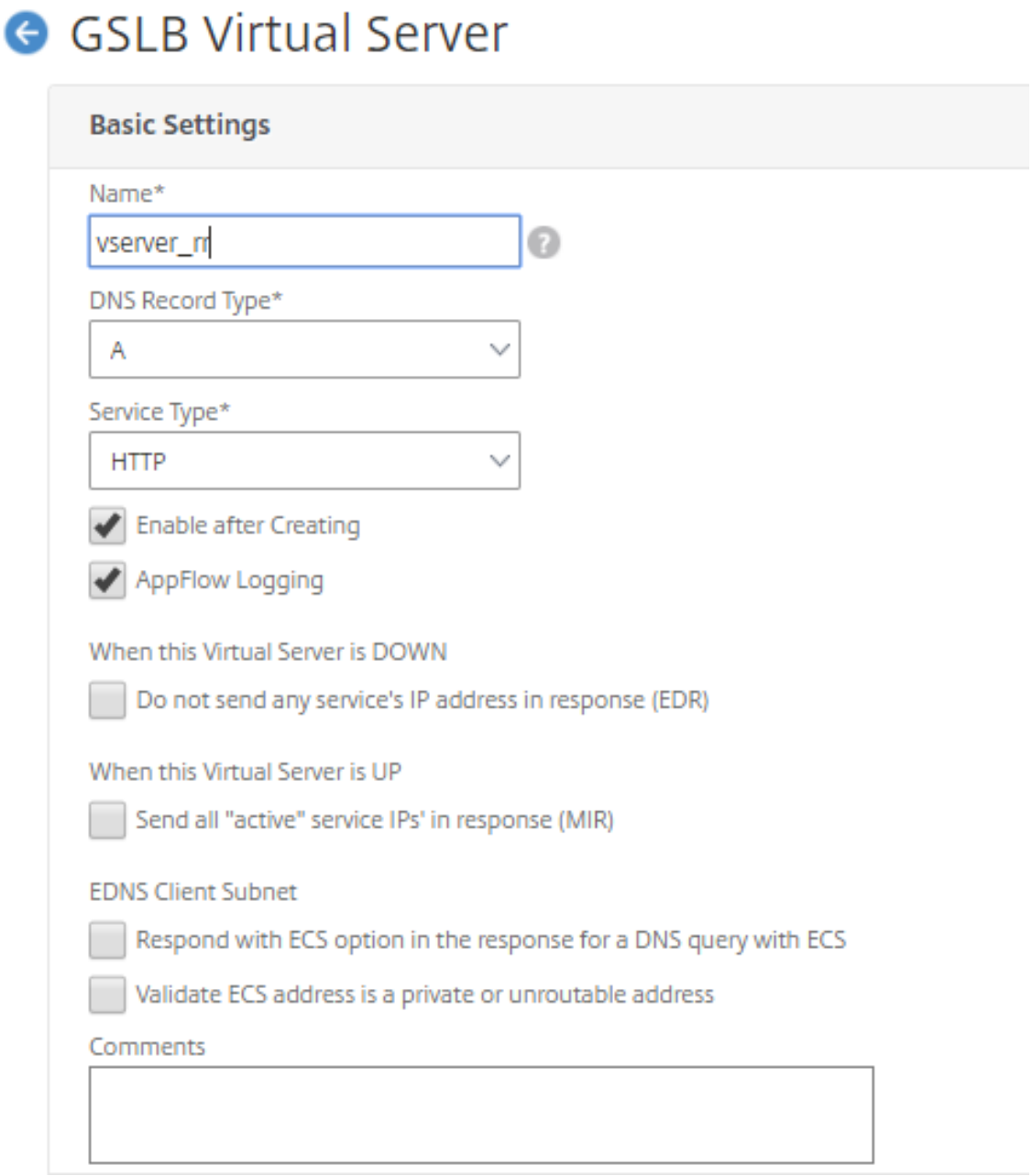
wie in der folgenden Abbildung gezeigt:



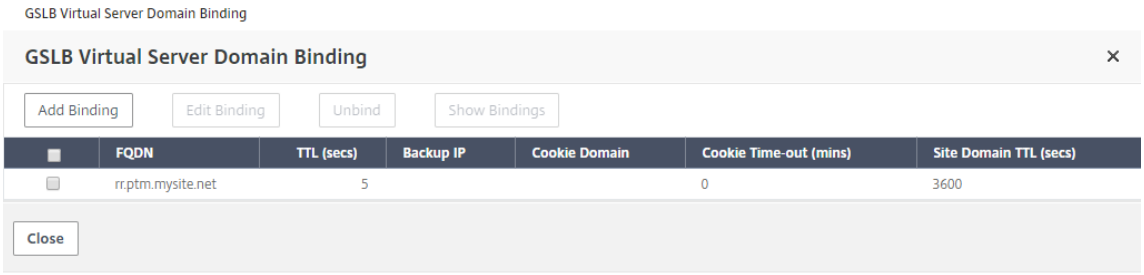
Virtuellen GSLB-Server hinzufügen

Fügen Sie einen virtuellen GSLB-Server hinzu, über den auf die Alias-GSLB-Dienste der App-Server zugegriffen werden kann.

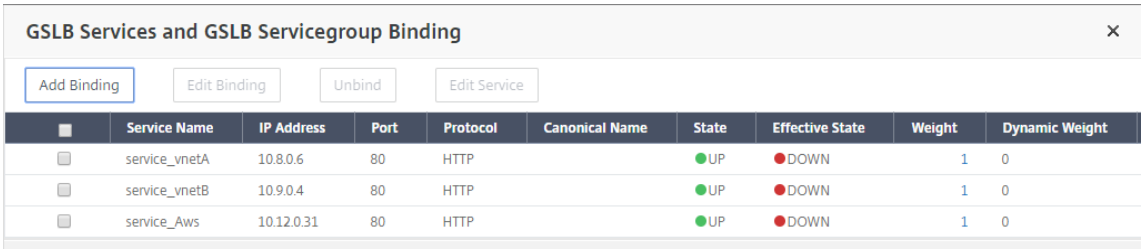
1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Virtual Servers**.
2. Fügen Sie die virtuellen Server hinzu, wie im folgenden Beispiel gezeigt.
3. Binden Sie GSLB-Dienste und den Domainnamen daran.



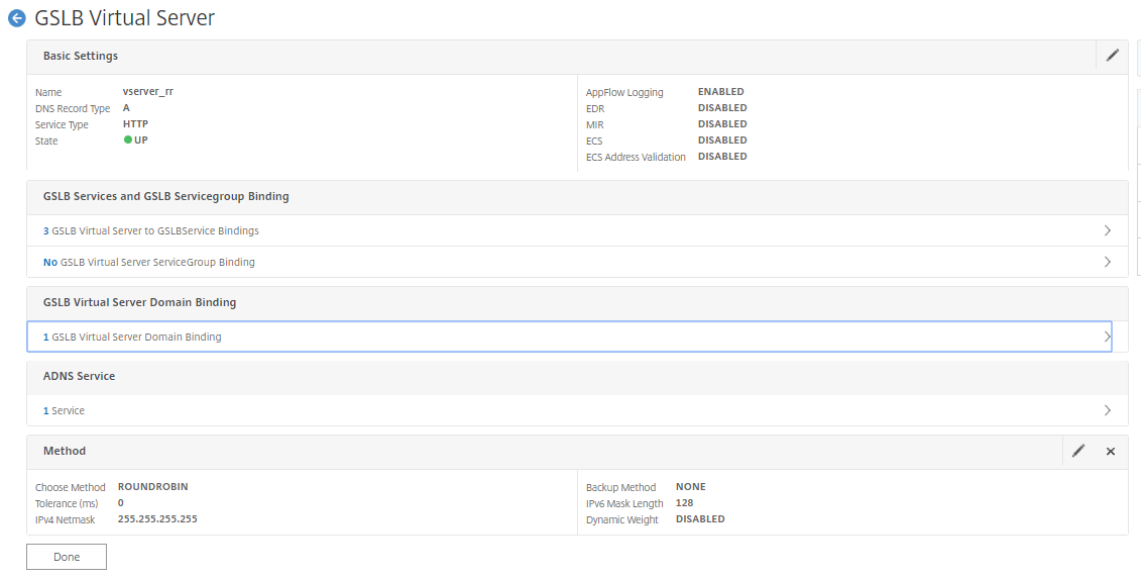
4. Nachdem Sie den virtuellen GSLB-Server erstellt und die entsprechende Lastausgleichsmethode ausgewählt haben (in diesem Fall Round Robin), binden Sie GSLB-Dienste und -Domänen, um den Schritt abzuschließen.



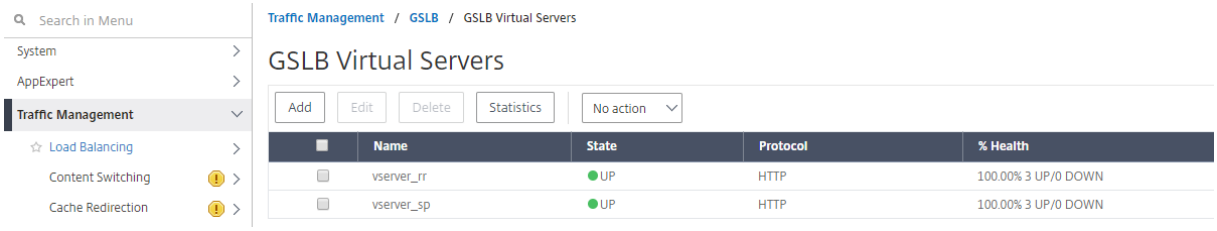
5. Gehen Sie auf dem virtuellen Server zur Registerkarte **Erweiterte Einstellungen** und klicken Sie auf die Registerkarte **Domänen hinzufügen**, um eine Domain zu binden.
6. Gehen Sie zu **Advanced > Services** und klicken Sie auf den Pfeil, um einen GSLB-Dienst zu binden und alle drei Dienste (VNet A, VNet B, On-Premise) an den virtuellen Server zu binden.



Nach dem Binden der GSLB-Dienste und der Domäne an den virtuellen Server wird es wie in der folgenden Abbildung dargestellt angezeigt:



Überprüfen Sie, ob der virtuelle GSLB-Server aktiv und zu 100% fehlerfrei ist. Wenn der Monitor anzeigt, dass der Server aktiv und fehlerfrei ist, bedeutet dies, dass die Websites synchronisiert sind und Back-End-Dienste verfügbar sind.



Um die Bereitstellung zu testen, greifen Sie entweder `rr.ptm.mysite.net` vom Cloud-Client-Computer oder vom lokalen Client-Computer auf die Domain-URL zu. Wenn Sie über einen Cloud-Windows-Client-Computer darauf zugreifen, stellen Sie sicher, dass auf den on-premises App-Server in einer privaten DNS-Zone zugegriffen wird, ohne dass DNS-Lösungen von Drittanbietern oder benutzerdefinierte DNS-Lösungen erforderlich sind.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von Azure Accelerated Networking

October 17, 2024

Accelerated Networking ermöglicht die virtuelle Funktions- (VF) -Netzwerkkarte (Single Root I/O Virtualization, SR-IOV) für eine virtuelle Maschine, wodurch die Netzwerkleistung verbessert wird. Sie können diese Funktion bei hohen Workloads verwenden, bei denen Daten mit höherem Durchsatz bei zuverlässigem Streaming und geringerer CPU-Auslastung gesendet oder empfangen werden müssen. Wenn eine NIC mit beschleunigter Vernetzung aktiviert ist, bündelt Azure die vorhandene para-virtualisierte (PV) -Schnittstelle der NIC mit einer SR-IOV VF-Schnittstelle. Die Unterstützung der SR-IOV VF-Schnittstelle ermöglicht und verbessert den Durchsatz der NetScaler VPX-Instanz.

Accelerated Networking bietet die folgenden Vorteile:

- Niedrigere Latenz
- Höhere Leistung von Paketen pro Sekunde (pps)
- Verbesserter Durchsatz
- Reduzierter Jitter
- Verminderte CPU-Auslastung

> **Hinweis:**
>
> Azure Accelerated Networking wird auf NetScaler VPX-Instanzen ab Version 13.0 Build 76.29 unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Ihre VM-Größe den Anforderungen für Azure Accelerated Networking entspricht.
- Stoppen Sie VMs (einzeln oder in einem Verfügbarkeitssatz), bevor Sie beschleunigtes Netzwerk auf einer beliebigen Netzwerkkarte aktivieren.

Einschränkungen

Accelerated Networking kann nur für einige Instance-Typen aktiviert werden. Weitere Informationen finden Sie unter Unterstützte Instance-Typen.

Unterstützte NICs für beschleunigtes Networking

Azure bietet Mellanox ConnectX3-, ConnectX4- und ConnectX5-NICs im SR-IOV-Modus für beschleunigte Netzwerke.

Wenn Accelerated Networking auf einer NetScaler VPX-Schnittstelle aktiviert ist, bündelt Azure entweder die ConnectX3-, ConnectX4- oder ConnectX5-Schnittstelle mit der vorhandenen PV-Schnittstelle einer NetScaler VPX-Appliance.

Weitere Informationen zum Aktivieren von Accelerated Networking vor dem Anfügen einer Schnittstelle an eine VM finden Sie unter Erstellen einer Netzwerkschnittstelle mit beschleunigtem Netzwerk.

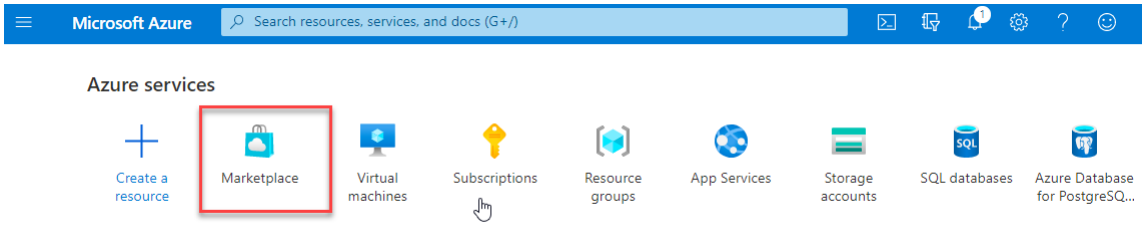
Weitere Informationen zum Aktivieren von beschleunigten Netzwerken auf einer vorhandenen Schnittstelle auf einer VM finden Sie unter Aktivieren vorhandener Schnittstellen auf einer VM.

So aktivieren Sie beschleunigtes Networking auf einer NetScaler VPX-Instanz mithilfe der Azure-Konsole

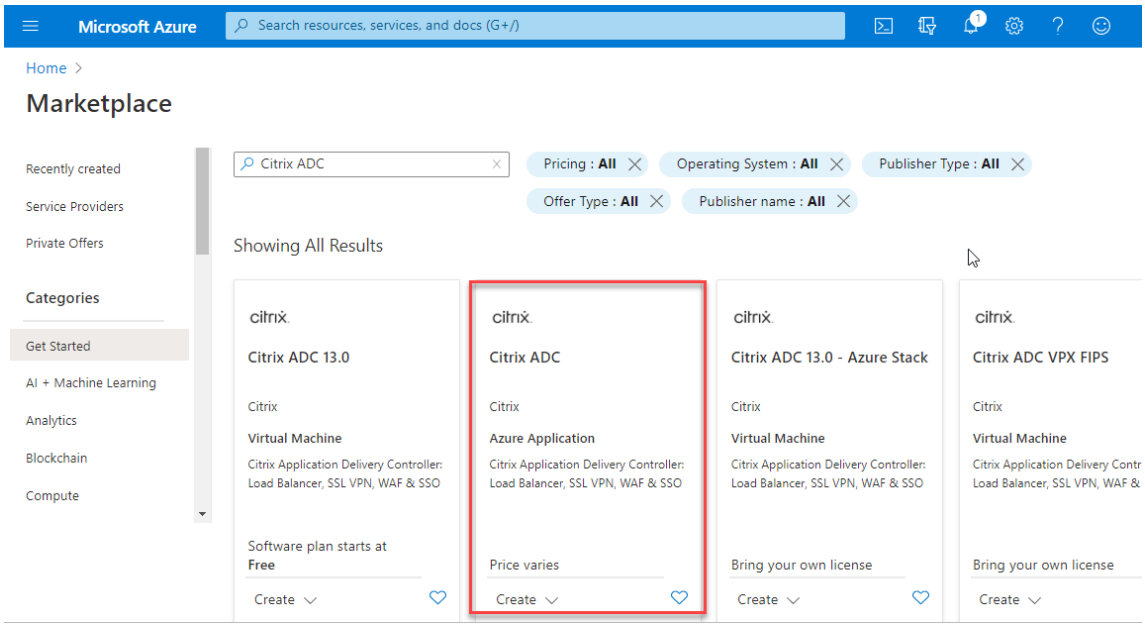
Sie können beschleunigte Netzwerke auf einer bestimmten Schnittstelle mithilfe der Azure-Konsole oder der Azure PowerShell aktivieren.

Gehen Sie wie folgt vor, um beschleunigtes Networking mithilfe von Azure-Verfügbarkeitssätzen oder Availability Zones zu aktivieren.

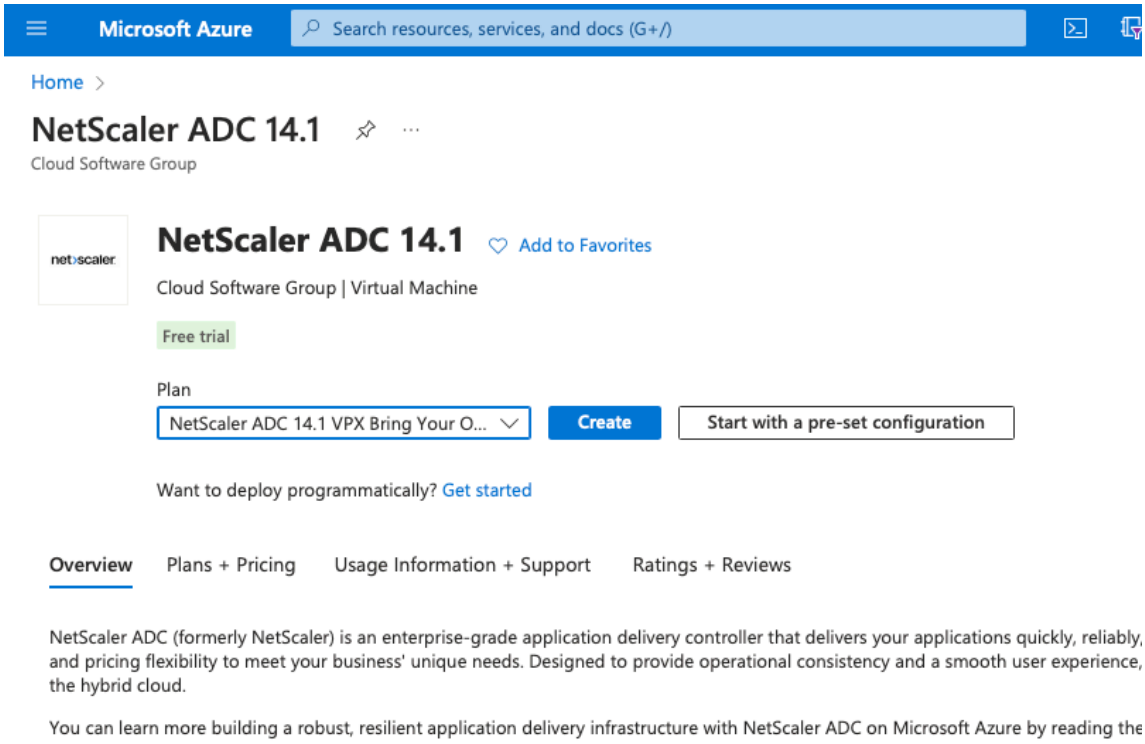
1. Melden Sie sich beim Azure-Portalan und navigieren Sie zu **Azure Marketplace**.



2. Suchen Sie im **Azure Marketplace** nach **NetScaler**.

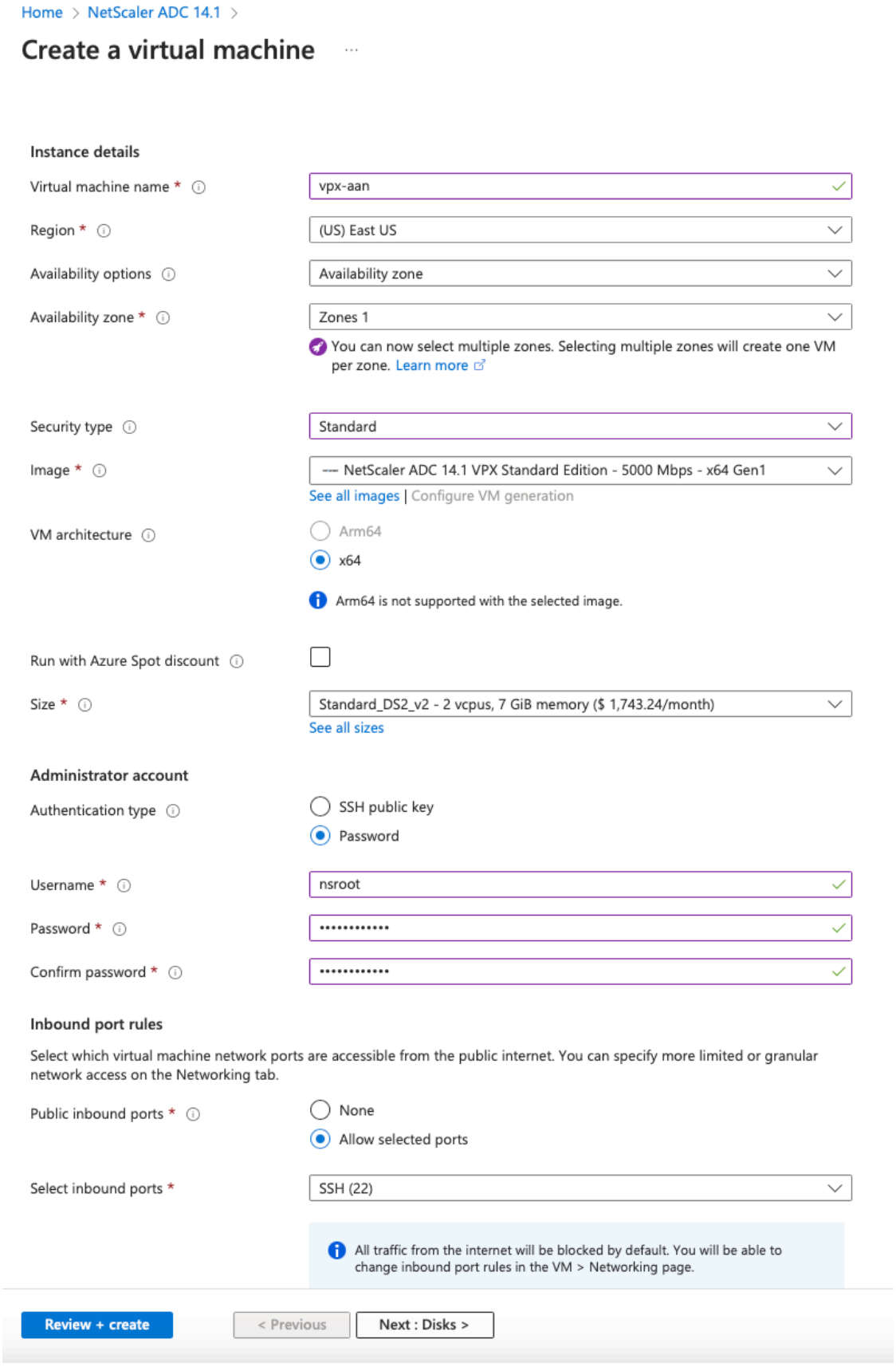


3. Wählen Sie einen NetScaler-Plan ohne FIPS zusammen mit der Lizenz aus und klicken Sie auf **Erstellen**.



Die Seite **NetScaler erstellen** wird angezeigt.

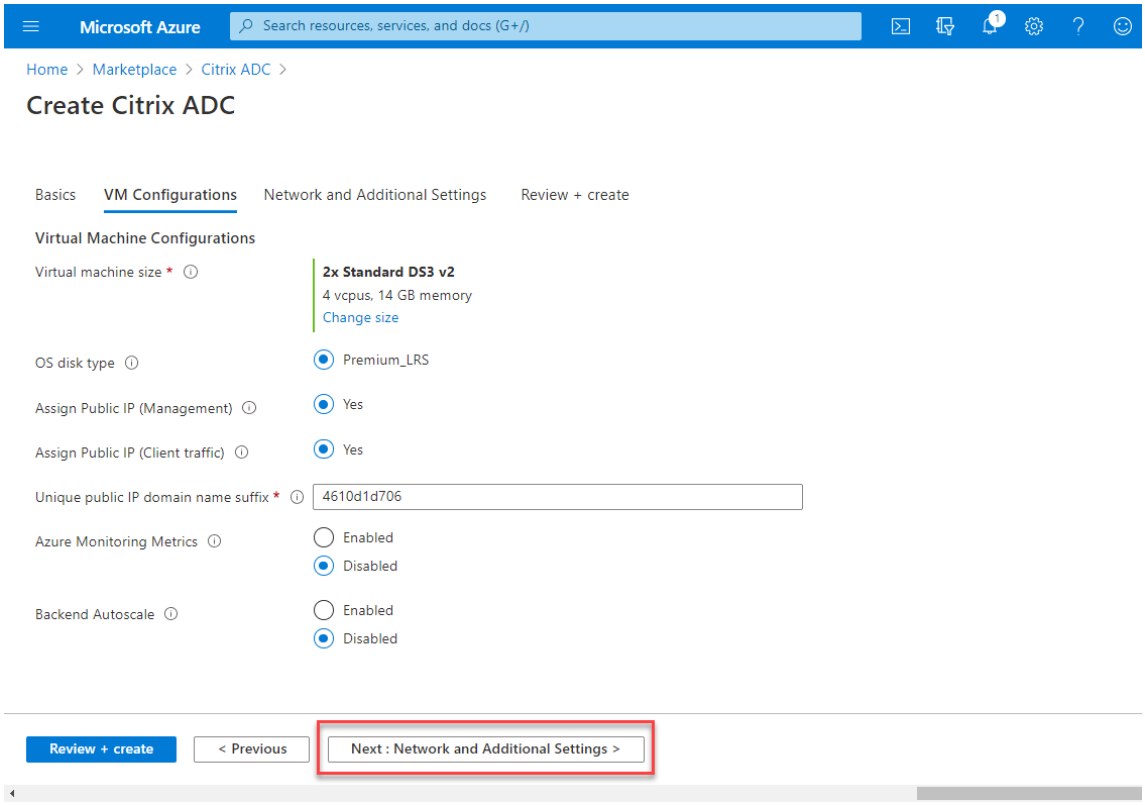
4. Erstellen Sie auf der Registerkarte **Grundlagen** eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



5. Klicken Sie auf **Weiter: VM-Konfigurationen**.

   Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:

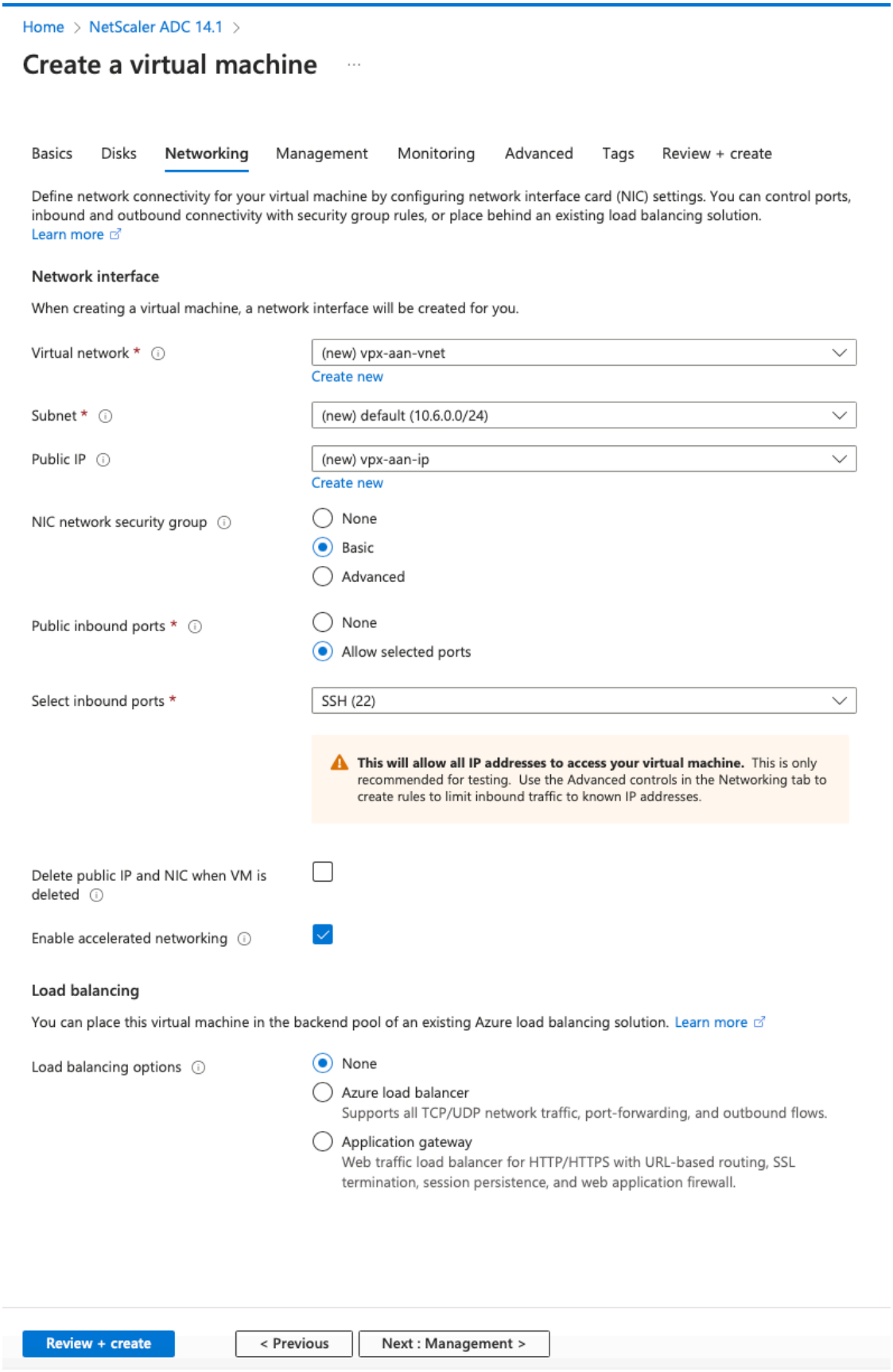
   a) Konfigurieren Sie ein öffentliches IP-Domänennamensuffix.
   b) Aktivieren oder deaktivieren Sie **Azure Monitoring-Metriken**.
   c) Aktivieren oder deaktivieren Sie **Backend Autoscale**.



6. Klicken Sie auf **Weiter: Netzwerk und Zusätzliche Einstellungen**.

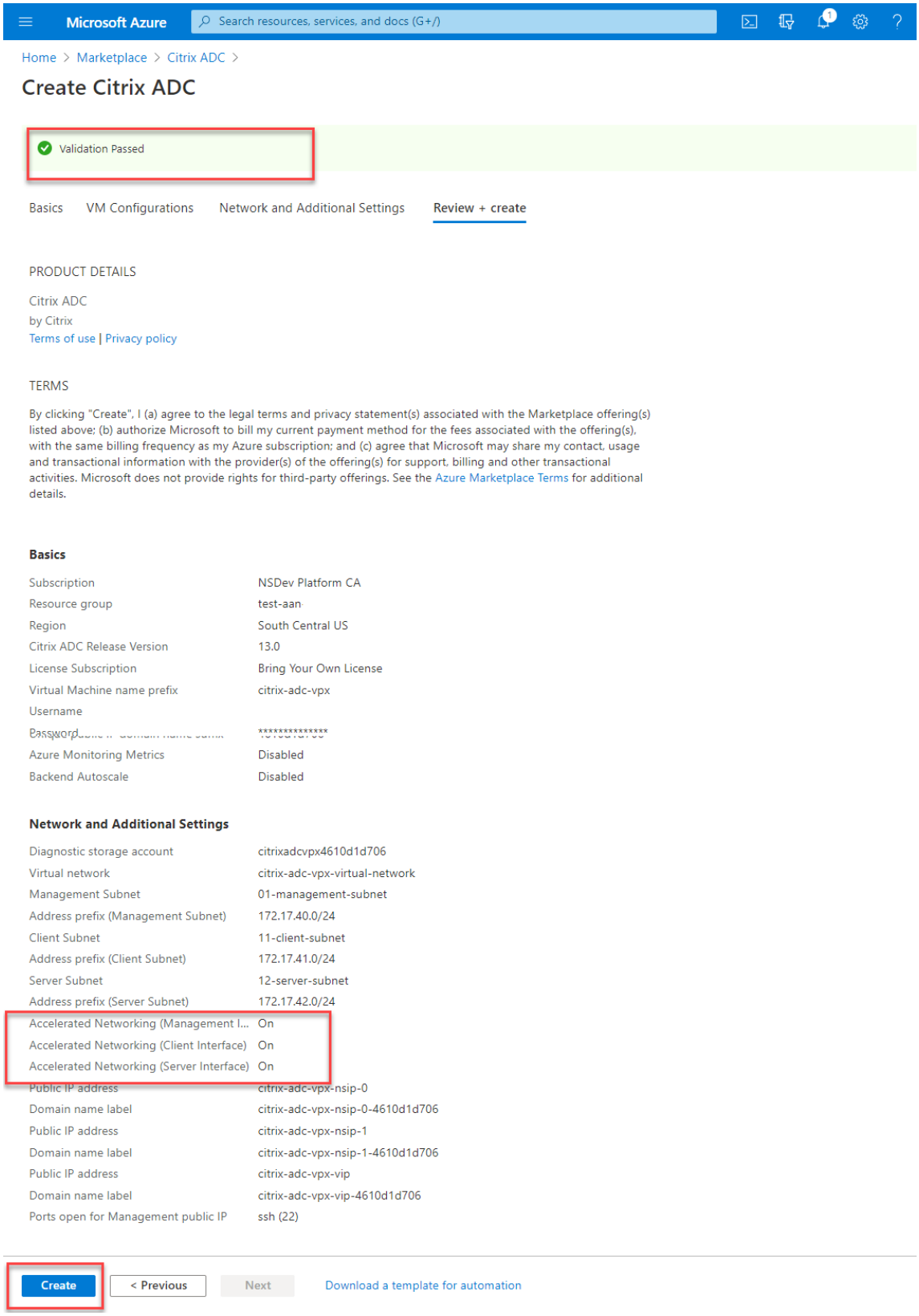
   Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Boot-Diagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

   Im Abschnitt **Accelerated Networking** haben Sie die Möglichkeit, das beschleunigte Netzwerk separat für die Verwaltungsschnittstelle, die Client-Schnittstelle und die Serverschnittstelle zu aktivieren oder zu deaktivieren.



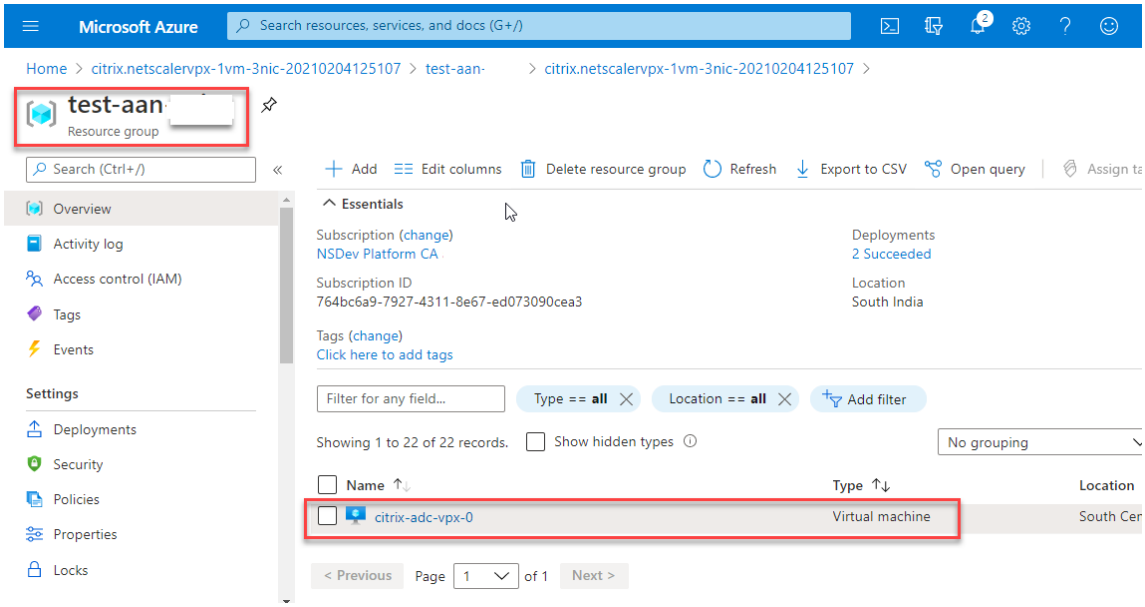
7. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

   Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**. Es kann einige Zeit dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt ist.

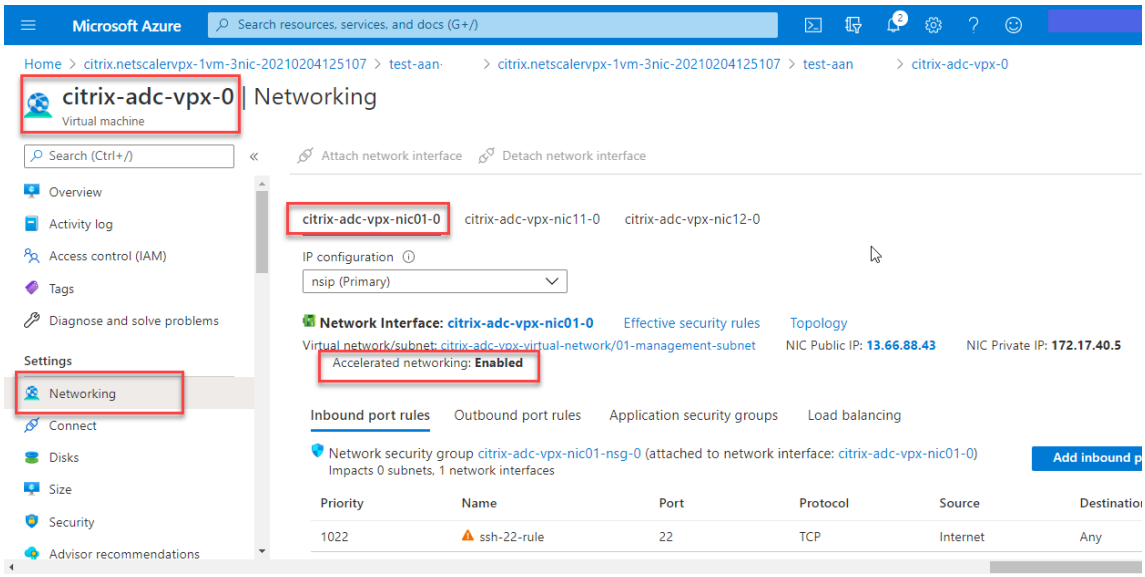


8. Wählen Sie nach Abschluss der Bereitstellung die **Ressourcengruppe** aus, um die Konfigura-

tionsdetails zu sehen.



9. Um die Konfigurationen für beschleunigte Netzwerke zu überprüfen, wählen Sie **Virtuelle Maschine > Netzwerk**aus. Der Status “Beschleunigtes Netzwerk”wird für jede Netzwerkkarte als **Aktiviert oder**Deaktiviert** angezeigt.



Aktivieren Sie beschleunigtes Networking mit Azure PowerShell

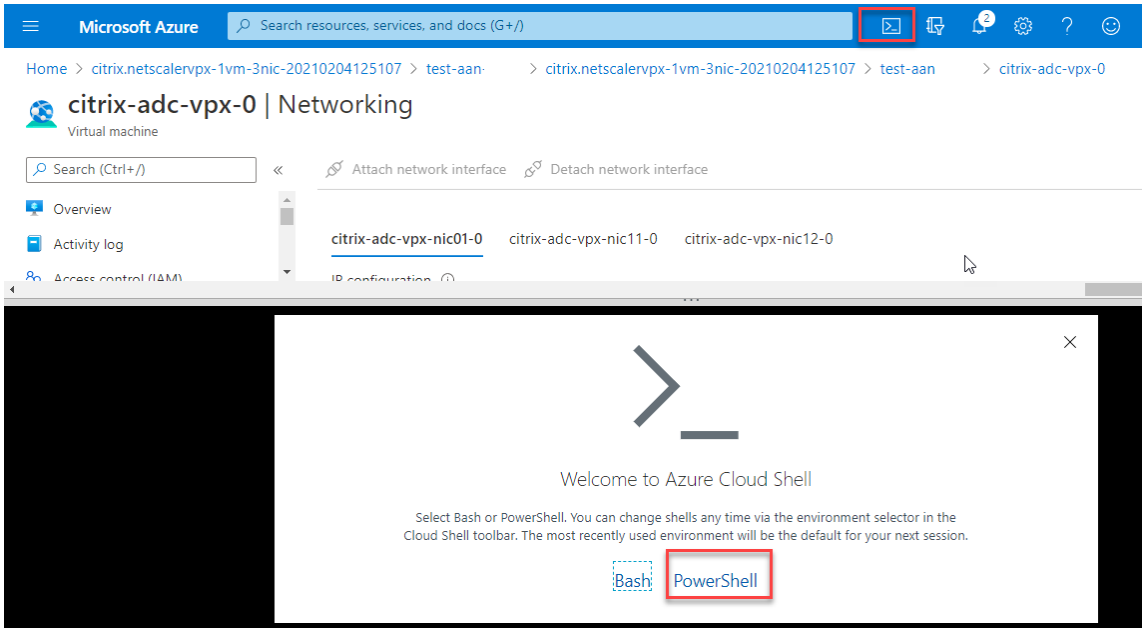
Wenn Sie nach der VM-Erstellung beschleunigte Netzwerke aktivieren müssen, können Sie dies mit Azure PowerShell tun.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die VM beenden, bevor Sie Accelerated Networking mit Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um beschleunigtes Networking mithilfe von Azure PowerShell zu aktivieren.

1. Navigieren Sie zum **Azure-Portal**und klicken Sie auf das **PowerShell-Symbol** in der rechten oberen Ecke.

   > **Hinweis:**
   >
   > Wenn Sie sich im Bash-Modus befinden, wechseln Sie in den PowerShell-Modus.



2. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
az network nic update --name <nic-name> --accelerated-networking
    [true | false] --resource-group <resourcegroup-name>
```

   Der Parameter Accelerated Networking akzeptiert einen der folgenden Werte:

   - **True:** Aktiviert beschleunigtes Netzwerk auf der angegebenen NIC.
   - **False:** Deaktiviert das beschleunigte Netzwerk auf der angegebenen Netzwerkkarte.

   So aktivieren Sie beschleunigtes Netzwerk auf einer bestimmten NIC:

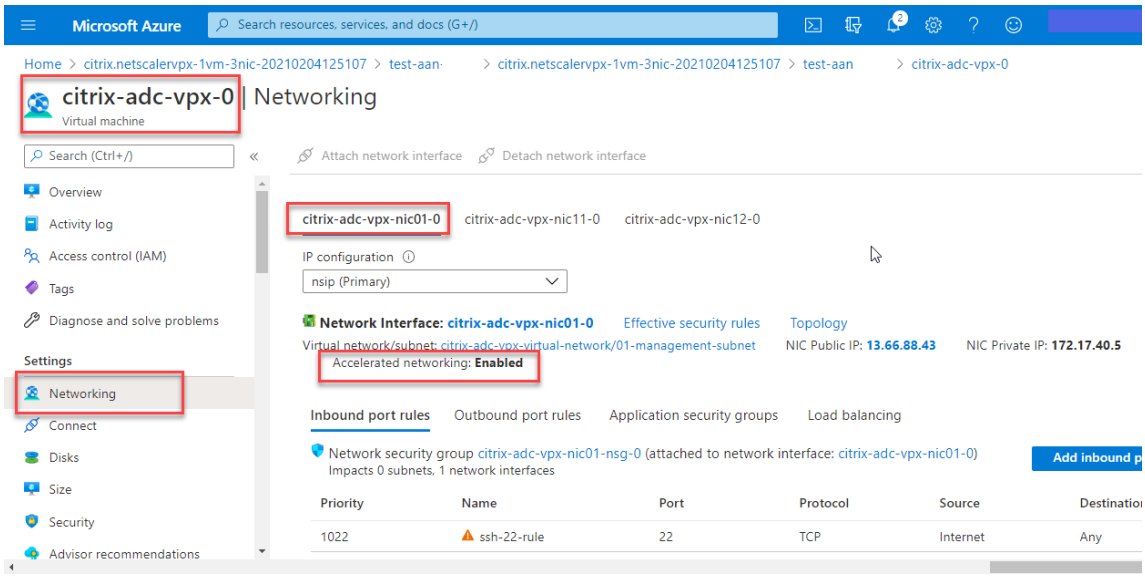
```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking true --resource-group rsgp1-aan
```

   So deaktivieren Sie das beschleunigte Netzwerk auf einer bestimmten NIC:

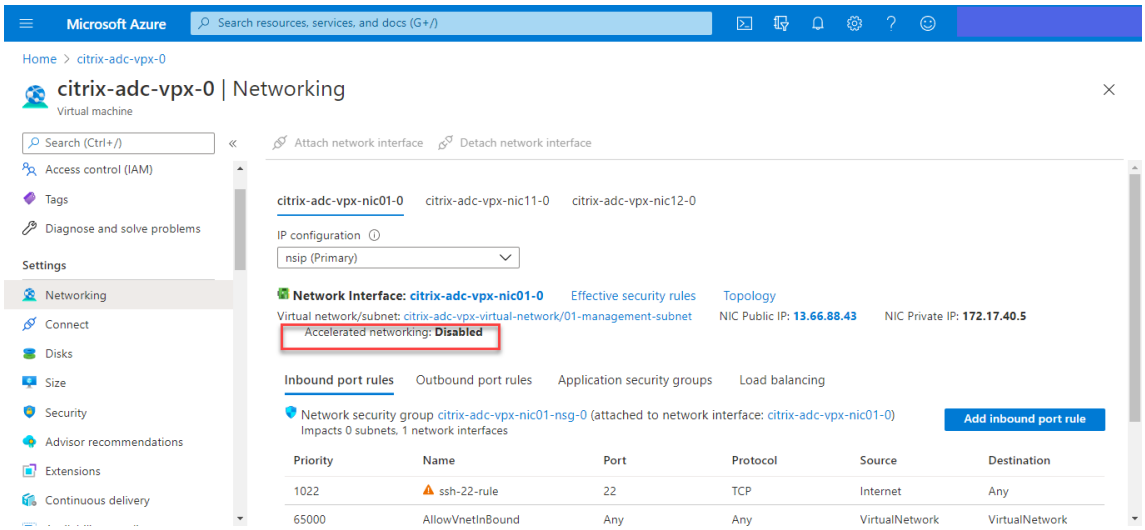

```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking false --resource-group rsgp1-aan
```

3. Um zu überprüfen, ob der Status Beschleunigtes Netzwerk nach Abschluss der Bereitstellung angezeigt wird, navigieren Sie zu **VM > Netzwerk**.

   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **aktiviert**ist.



   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **deaktiviert**ist.



Um beschleunigte Netzwerke auf einer Schnittstelle mithilfe der FreeBSD-Shell von NetScaler zu überprüfen

Sie können sich bei der FreeBSD-Shell von NetScaler anmelden und die folgenden Befehle ausführen, um den Status des beschleunigten Netzwerks zu überprüfen.

Beispiel für ConnectX3 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe „ifconfig“der Mellanox ConnectX3-NIC. Der “50/n” zeigt die VF-Schnittstellen der Mellanox ConnectX3-NICs an. 0/1 und 1/1 stehen für die PV-Schnittstellen der NetScaler VPX-Instanz. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX3-VF-Schnittstelle (50/1) dieselben MAC-Adressen haben (00:22:48:1 c: 99:3 e). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind.

```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Beispiel für ConnectX4 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe „ifconfig“der Mellanox ConnectX4-NIC. Der “100/n” zeigt die VF-Schnittstellen der Mellanox ConnectX4-NICs an. 0/1, 1/1 und 1/2 stehen für die PV-Schnittstellen der NetScaler VPX-Instanz. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX4-VF-Schnittstelle (100/1) dieselben MAC-Adressen haben (00:0d:3a:9b:f2:1d). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind. In ähnlicher Weise haben die PV-Schnittstelle (1/2) und die CX4-VF-Schnittstelle (100/2) dieselben MAC-Adressen (00:0 d:3a:1e:d 2:23).

```
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 0xffffff00 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
```

Um beschleunigte Netzwerke auf einer Schnittstelle mithilfe von ADC CLI zu überprüfen

Beispiel für ConnectX3 NIC:

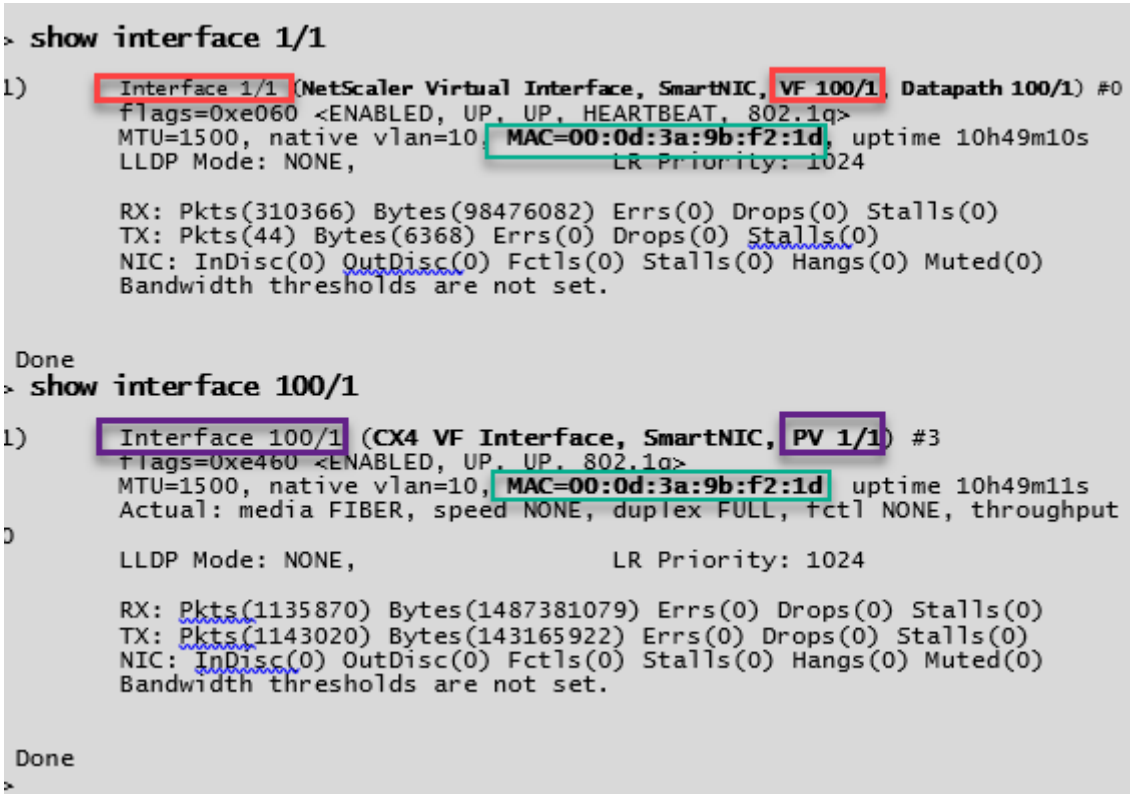
Die folgende Befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 50/1 gebündelt ist, bei der es sich um eine SR-IOV-VF-NIC handelt. Die MAC-Adressen der 1/1- und 50/1-

NICs sind identisch. Nachdem das beschleunigte Netzwerk aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 50/1-Schnittstelle gesendet, bei der es sich um eine ConnectX3-Schnittstelle handelt. Sie können sehen, dass der Ausgang „Show Interface“der PV-Schnittstelle (1/1) auf den VF (50/1) zeigt. In ähnlicher Weise zeigt die Ausgabe „Show Interface“der VF-Schnittstelle (50/1) auf die PV-Schnittstelle (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=0xe460 <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.
```

Beispiel für ConnectX4 NIC:

Die folgende Befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 100/1 gebündelt ist, bei der es sich um eine SR-IOV-VF-NIC handelt. Die MAC-Adressen der 1/1- und 100/1-NICs sind identisch. Nachdem das beschleunigte Netzwerk aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 100/1-Schnittstelle gesendet, bei der es sich um eine ConnectX4-Schnittstelle handelt. Sie können sehen, dass der Ausgang „Show Interface“der PV-Schnittstelle (1/1) auf den VF (100/1) zeigt. In ähnlicher Weise zeigt die Ausgabe „Show Interface“der VF-Schnittstelle (100/1) auf die PV-Schnittstelle (1/1).



Zu beachtende Punkte in NetScaler

- Die PV-Schnittstelle wird als primäre oder Hauptschnittstelle für alle erforderlichen Operationen betrachtet. Konfigurationen dürfen nur an PV-Schnittstellen durchgeführt werden.
- Alle „Set“-Operationen auf einer VF-Schnittstelle sind blockiert, mit Ausnahme der folgenden:
  - Schnittstelle aktivieren
  - Schnittstelle deaktivieren
  - Schnittstelle zurücksetzen
  - Statistiken löschen

  > **Hinweis:**
  >
  > Citrix empfiehlt, dass Sie keine Operationen auf der VF-Schnittstelle ausführen.

- Sie können die Bindung der PV-Schnittstelle an die VF-Schnittstelle mit dem `show interface` Befehl überprüfen.
- Ab NetScaler Version 13.1-33.x kann eine NetScaler VPX-Instanz dynamische NIC-Entfernungen und das erneute Anhängen der entfernten NICs in Azure Accelerated Networking nahtlos verarbeiten. Azure kann die SR-IOV VF-NIC von Accelerated Networking für ihre Host-Wartungsaktivitäten entfernen. Immer wenn eine Netzwerkkarte aus der Azure-VM entfernt

wird, zeigt die NetScaler VPX-Instanz den Schnittstellenstatus als „Link Down“an und der Datenverkehr fließt nur über die virtuelle Schnittstelle. Nachdem die entfernte Netzwerkkarte wieder angeschlossen wurde, verwenden die VPX-Instanzen die erneut verbundene SR-IOV-VF-Netzwerkkarte. Dieser Vorgang erfolgt nahtlos und erfordert keine Konfiguration.

Konfigurieren Sie ein VLAN zu einer PV-Schnittstelle

Wenn eine PV-Schnittstelle an ein VLAN gebunden ist, ist die zugehörige beschleunigte VF-Schnittstelle auch an dasselbe VLAN wie die PV-Schnittstelle gebunden. In diesem Beispiel ist die PV-Schnittstelle (1/1) an VLAN (20) gebunden. Die VF-Schnittstelle (100/1), die mit der PV-Schnittstelle (1/1) gebündelt ist, ist ebenfalls an VLAN 20 gebunden.

Beispiel

1. Erstellen Sie ein VLAN.

```
add vlan 20
```

2. Binden Sie ein VLAN an die PV-Schnittstelle.

```
bind vlan 20 –ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2
```

> **Hinweis:**
>
> VLAN-Bindungsvorgänge sind auf einer beschleunigten VF-Schnittstelle nicht zulässig.

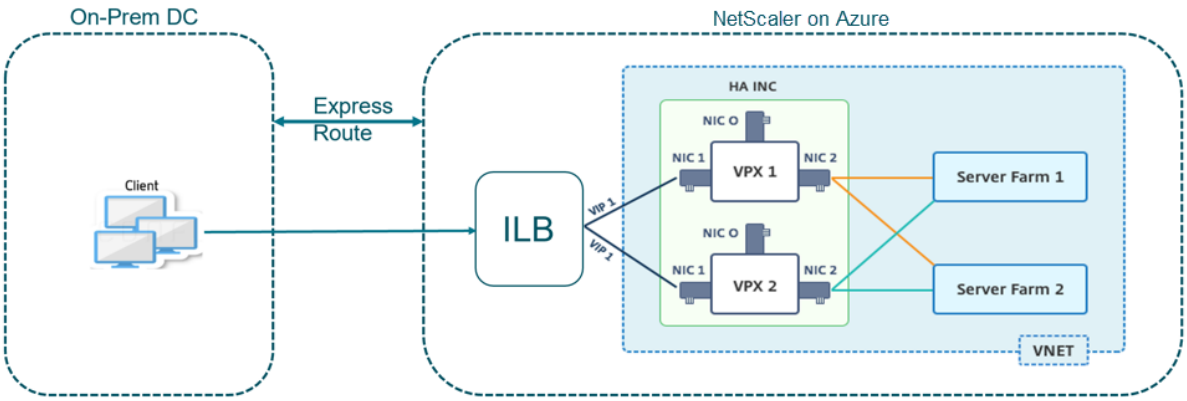
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
```


Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage mit Azure ILB

October 17, 2024

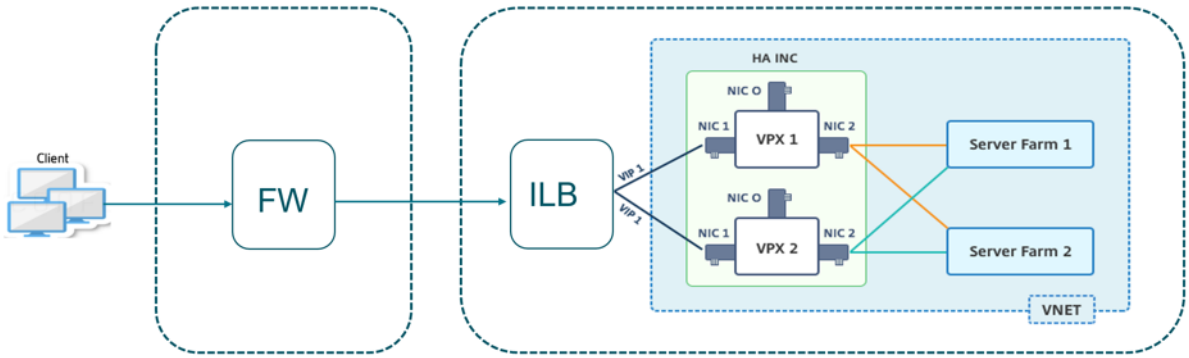
Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für Intranetanwendungen verwenden. Der Azure Internal Load Balancer (ILB) verwendet eine interne oder private IP-Adresse für das Frontend, wie in Abbildung 1 dargestellt. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze dienen der Verwaltung, des Clients und des serverseitigen Datenverkehrs, wobei jedes Subnetz zu einer anderen Netzwerkkarte auf jedem Gerät gehört.

Abbildung 1: NetScaler HA-Paar für Clients in einem internen Netzwerk



Sie können diese Bereitstellung auch verwenden, wenn sich das NetScaler HA-Paar hinter einer Firewall befindet, wie in Abbildung 2 dargestellt. Die öffentliche IP-Adresse gehört zur Firewall und ist mit NAT der Front-End-IP-Adresse der ILB verbunden.

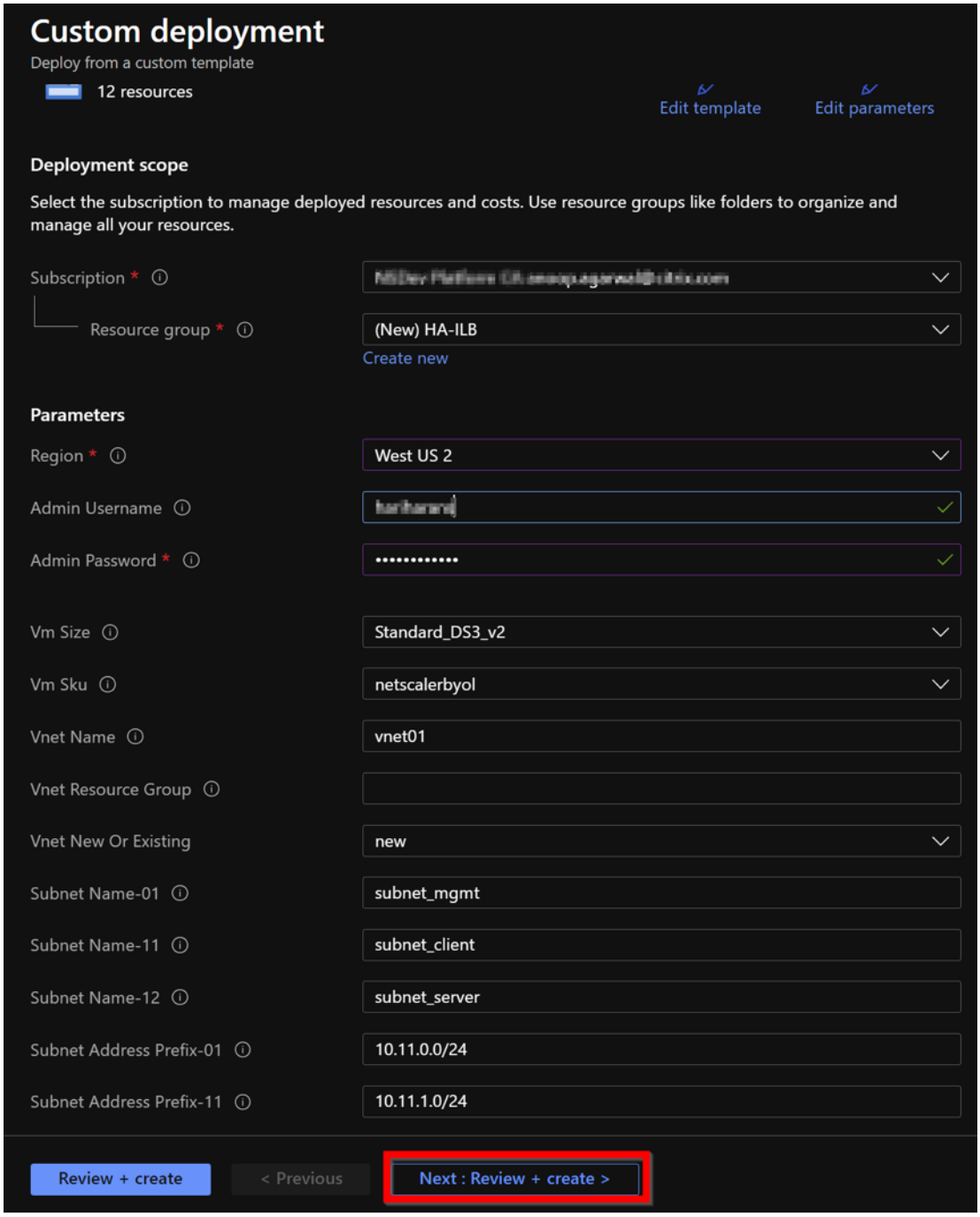
Abbildung 2: NetScaler HA-Paar mit Firewall mit öffentlicher IP-Adresse



Sie können die NetScaler HA-Paarvorlage für Intranetanwendungen im Azure-Portalabrufen

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets bereitzustellen.

1. Navigieren Sie im Azure-Portal zur Seite **Benutzerdefinierte Bereitstellung** .
2. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Region, den Admin-Benutzernamen, das Admin-Kennwort, den Lizenztyp (`VM sku`) und andere Felder ein.

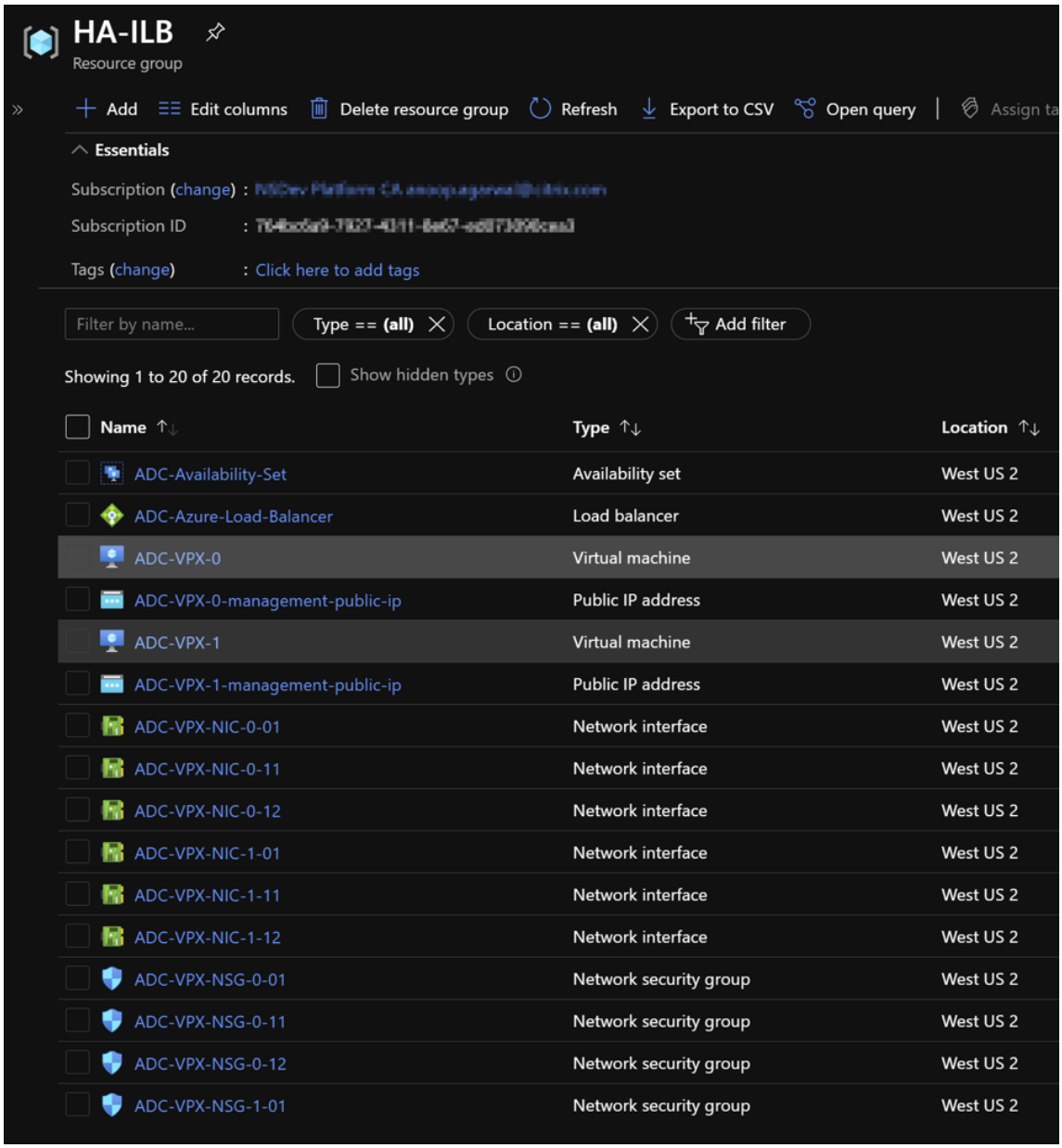


3. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

   Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar erscheint als ADC-VPX-0 und ADC-VPX-1.

   Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

   Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.



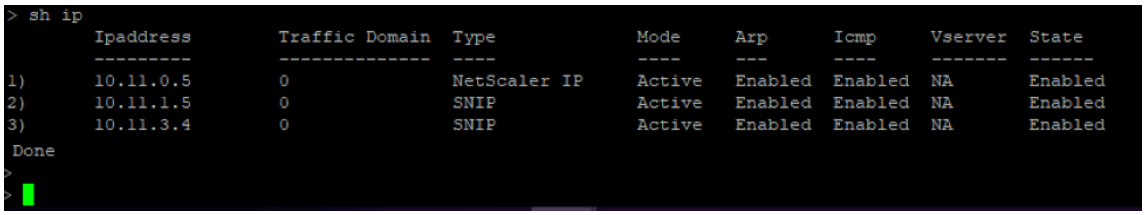
4. Melden Sie sich bei den Knoten **ADC-VPX-0** und **ADC-VPX-1** an, um die folgende Konfiguration

zu überprüfen:

- NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
- Auf den primären (ADC-VPX-0) und sekundären (ADC-VPX-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird für die Reaktion auf ILB-Prüfpunkte verwendet und das andere SNIP (Serversubnetz) wird für die Back-End-Server-Kommunikation verwendet.

> **Hinweis:**
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adresse der ADC-VPX-0- und ADC-VPX-1-VMs im selben Subnetz, im Gegensatz zu der klassischen lokalen ADC HA-Bereitstellung, bei der beide gleich sind. Um Bereitstellungen zu unterstützen, wenn sich das VPX-Paar SNIP in verschiedenen Subnetzen befindet oder wenn sich der VIP nicht im selben Subnetz wie ein SNIP befindet, müssen Sie entweder Mac-Based Forwarding (MBF) aktivieren oder jedem VPX-Knoten eine statische Host-Route für jeden VIP hinzufügen.

Auf dem primären Knoten (ADC-VPX-0)




```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

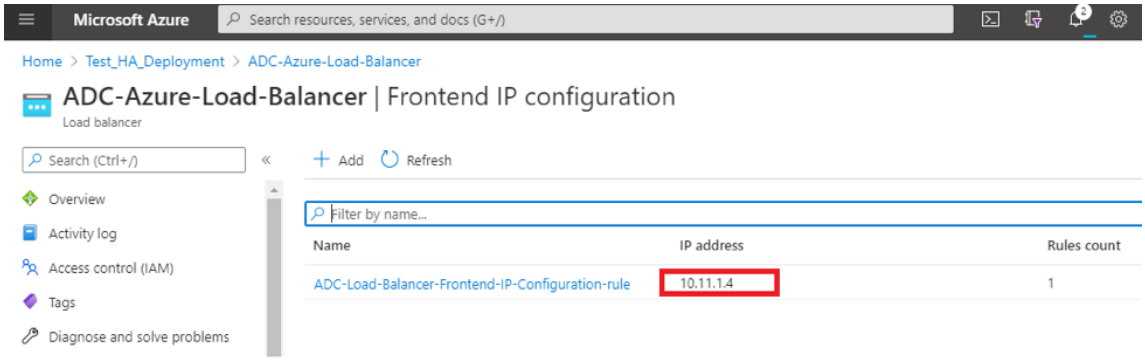
Auf dem sekundären Knoten (ADC-VPX-1)

```
> sh ip
        Ipaddress       Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------       --------------  ----            ----     ---      ----     -------  ------
1)      10.11.0.4       0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.6       0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.5       0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

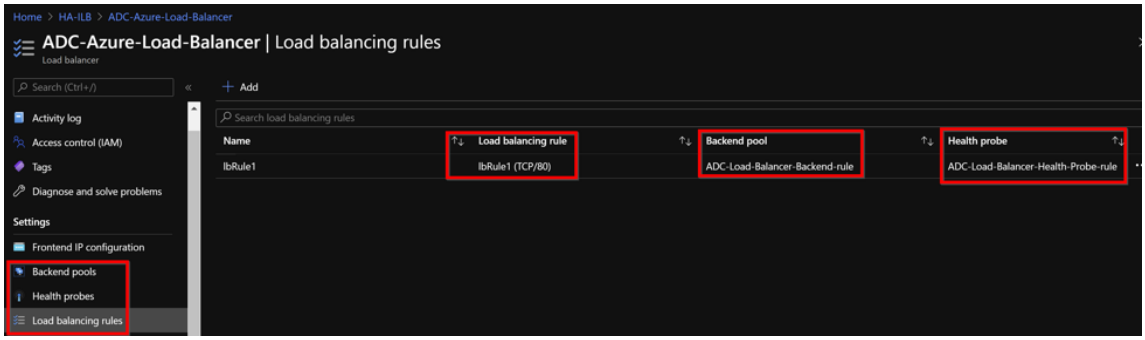


```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

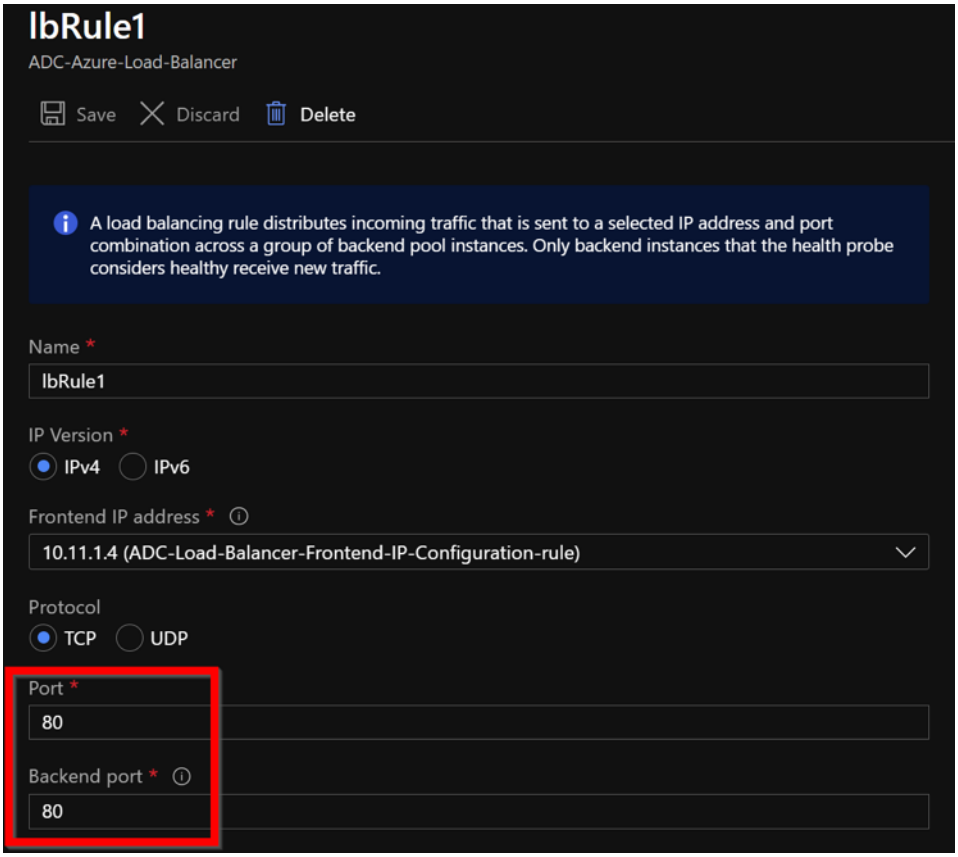
5. Nachdem die primären und sekundären Knoten aktiv sind und der Synchronisierungsstatus **ERFOLGREICH**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem Primärknoten (ADC-VPX-0) mit der privaten Floating IP (FIP) -Adresse des ADC Azure Load Balancers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
6. Um die private IP-Adresse des ADC Azure Load Balancers zu finden, navigieren Sie zum **Azure-Portal > ADC Azure Load Balancer > Frontend IP-Konfiguration**.



7. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung beim Erstellen der LB-Regel, Back-End-Pools und Gesundheitsproben.

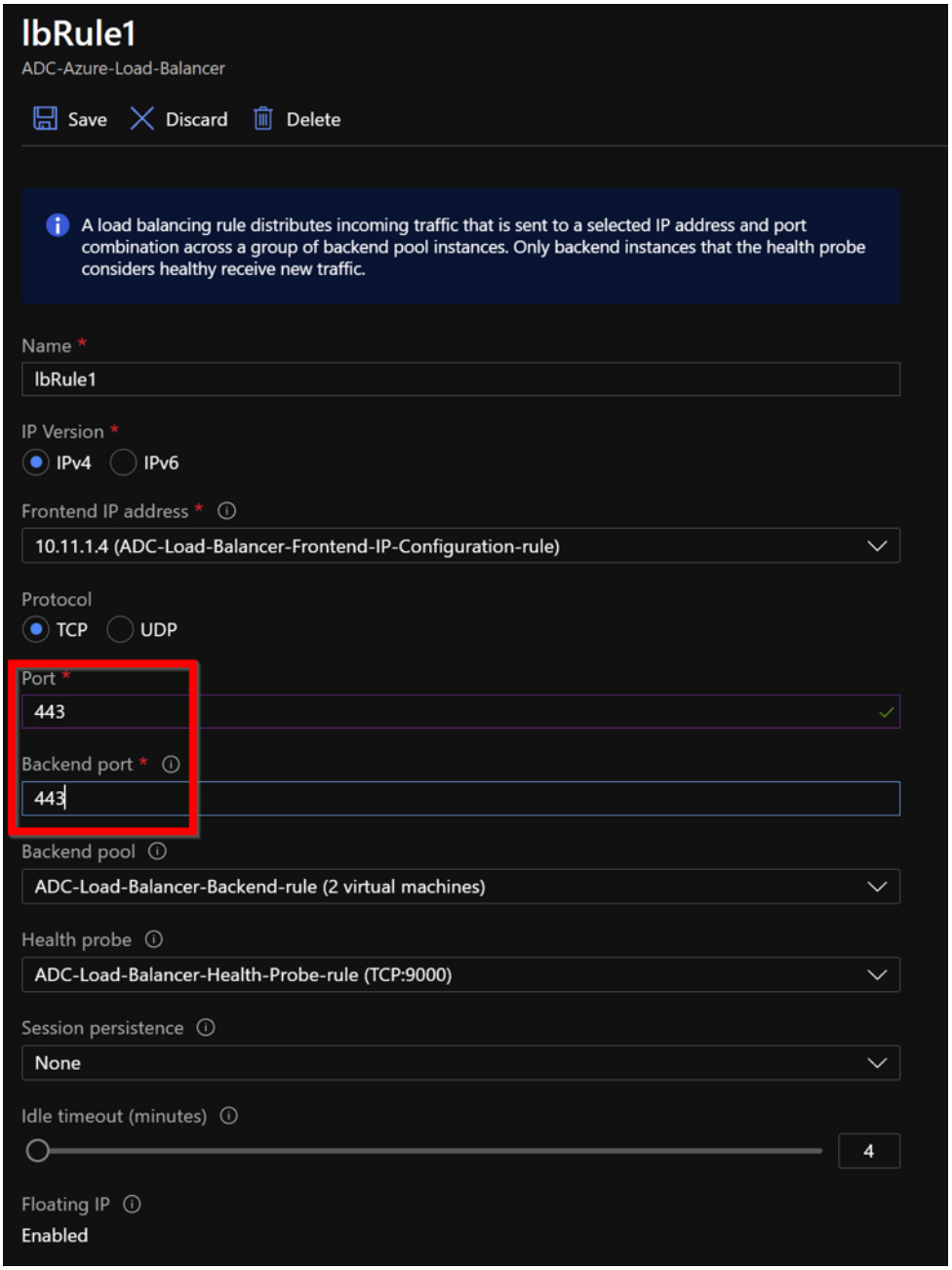


- Die LB-Regel (LBrule1) verwendet standardmäßig Port 80.



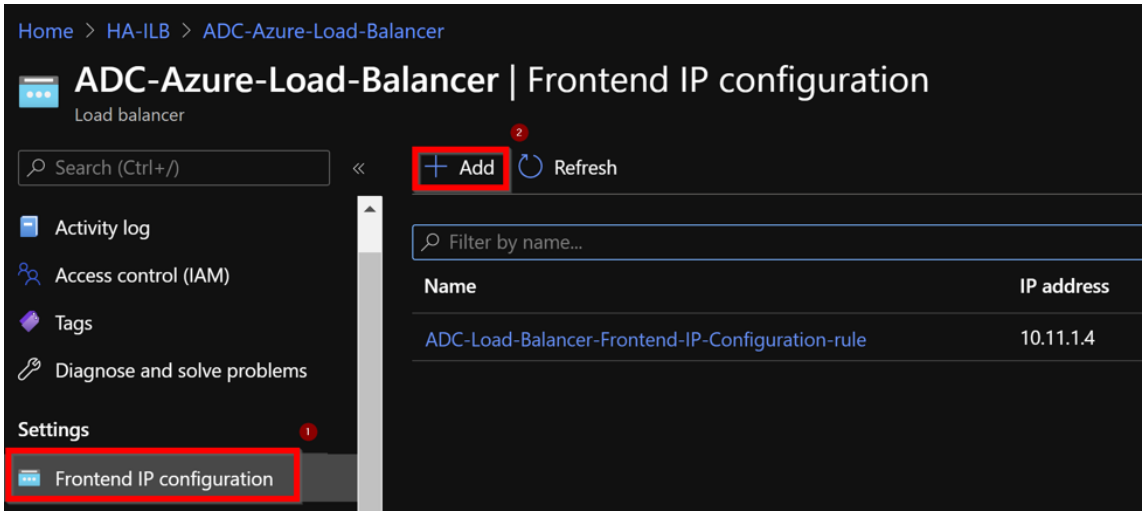
- Bearbeiten Sie die Regel, um Port 443 zu verwenden, und speichern Sie die Änderungen.

  > **Hinweis:**
  >
  > Für eine verbesserte Sicherheit empfiehlt Citrix, den SSL-Port 443 für den virtuellen LB-Server oder den virtuellen Gateway-Server zu verwenden.

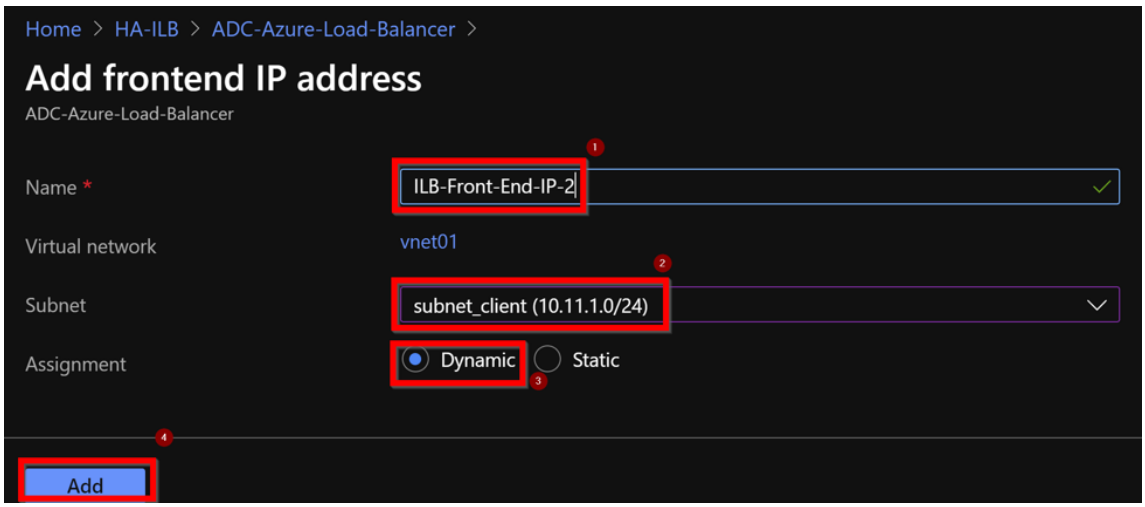


Gehen Sie wie folgt vor, um weitere VIP-Adressen zum ADC hinzuzufügen:

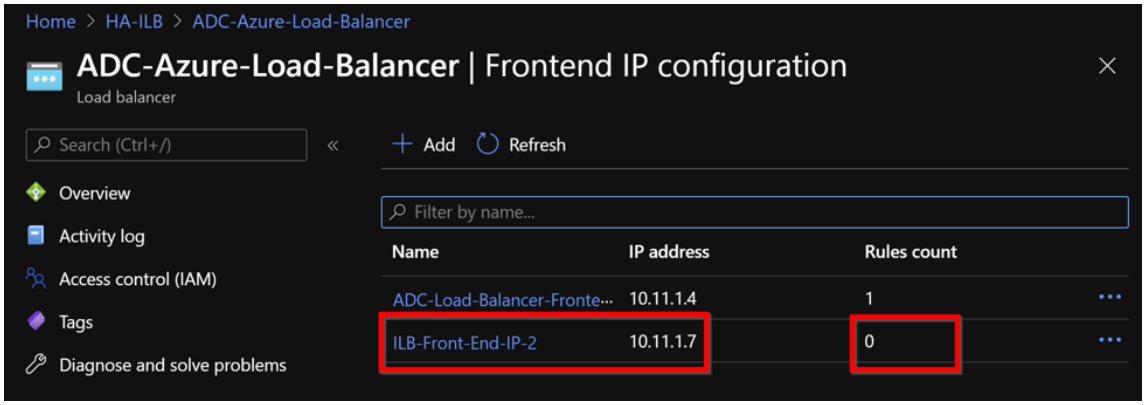
1. Navigieren Sie zu **Azure Load Balancer > Frontend-IP-Konfiguration**, und klicken Sie auf **Hinzufügen**, um eine neue interne Load Balancer-IP-Adresse zu erstellen.



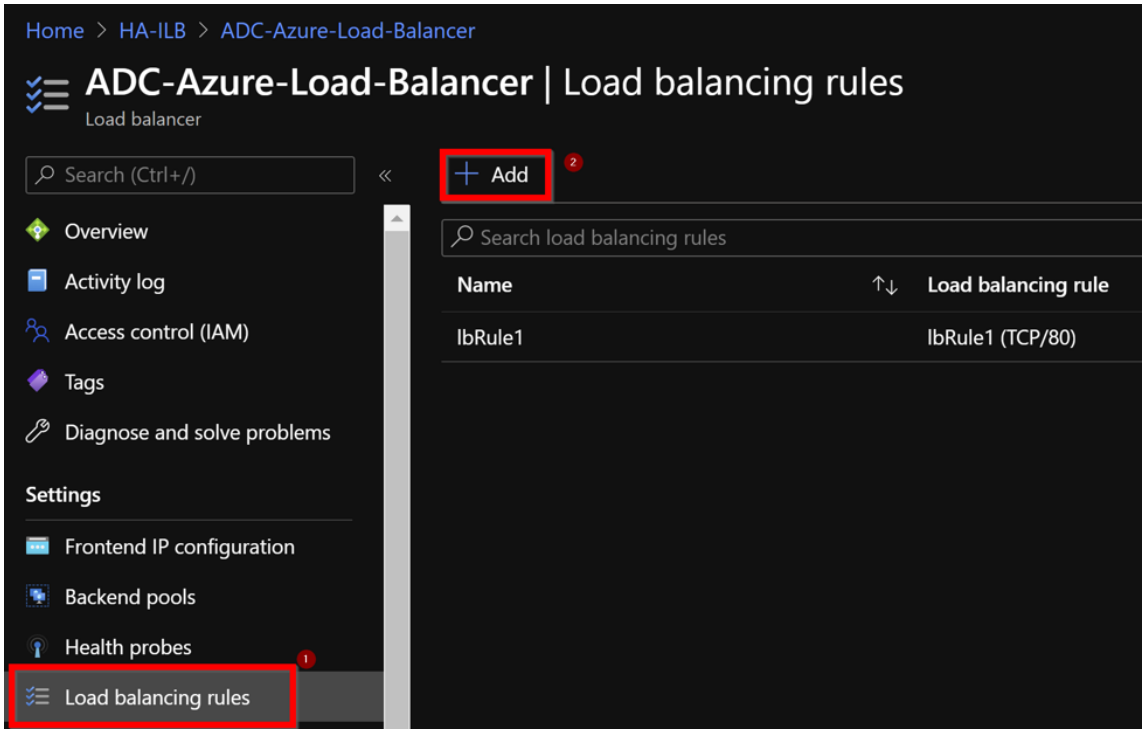
2. Geben Sie auf der Seite **Frontend-IP-Adresse hinzufügen** einen Namen ein, wählen Sie das Client-Subnetz aus, weisen Sie entweder dynamische oder statische IP-Adresse zu und klicken Sie auf **Hinzufügen**.



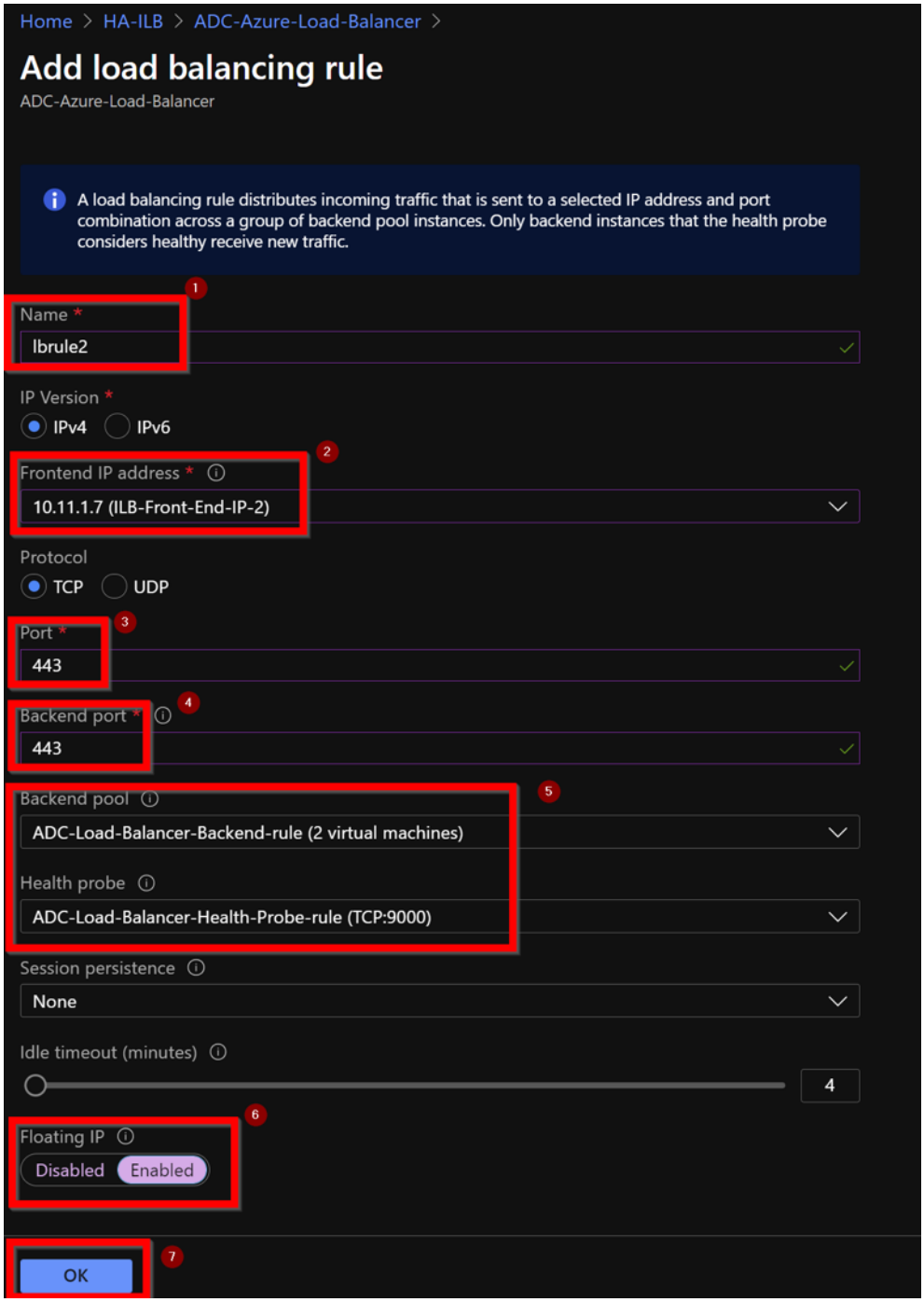
3. Die Front-End-IP-Adresse wird erstellt, aber eine LB-Regel ist nicht zugeordnet. Erstellen Sie eine neue Lastausgleichsregel, und verknüpfen Sie sie mit der Front-End-IP-Adresse.



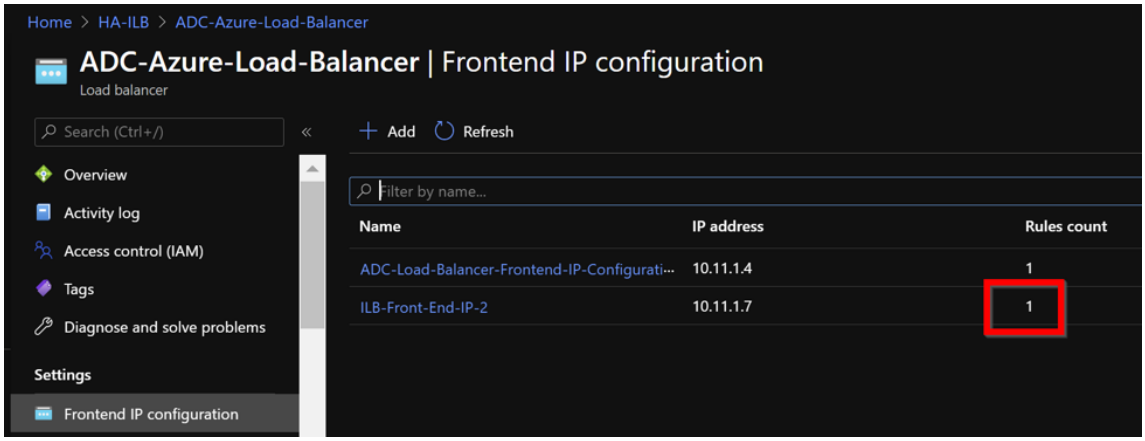
4. Wählen Sie auf der Seite **Azure Load Balancer** die Option **Load Balancing-Regeln**aus, und klicken Sie dann auf **Hinzufügen**.



5. Erstellen Sie eine neue LB-Regel, indem Sie die neue Front-End-IP-Adresse und den Port auswählen. Das**Floating-IP-Feld** muss auf **Enabled**gesetzt sein.



6. Jetzt zeigt die **Frontend-IP-Konfiguration** die angewendete LB-Regel an.



Beispiel-Konfiguration

Führen Sie zum Konfigurieren eines virtuellen Gateway-VPN-Servers und eines virtuellen Lastausgleichsservers die folgenden Befehle auf dem primären Knoten aus (ADC-VPX-0). Die Konfiguration synchronisiert sich automatisch mit dem sekundären Knoten (ADC-VPX-1).

Gateway Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
```

Beispielkonfiguration für den Lastausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
```

Sie können jetzt mit dem vollqualifizierten Domänennamen (FQDN), der mit der internen IP-Adresse von ILB verknüpft ist, auf den Lastausgleich- oder virtuellen VPN-Server zugreifen.

Weitere Informationen zur Konfiguration des virtuellen Load-Balancing-Servers finden Sie im Abschnitt **Ressourcen** .

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastausgleichs

Verwandte Ressourcen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage für mit dem Internet verbundene Anwendungen

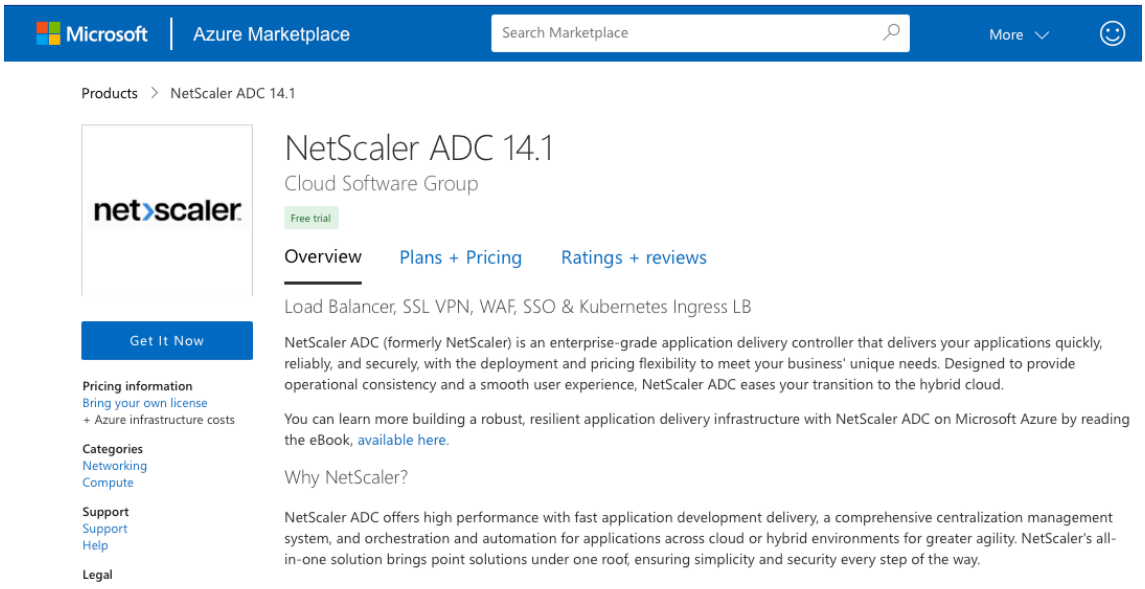
October 17, 2024

Sie können schnell und effizient ein Paar von VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für internetfähige Anwendungen verwenden. Der Azure Load Balancer (ALB) verwendet eine öffentliche IP-Adresse für das Frontend. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für den Management-, Client- und serverseitigen Verkehr bestimmt. Jedes Subnetz hat zwei Netzwerkkarten für beide VPX-Instanzen.

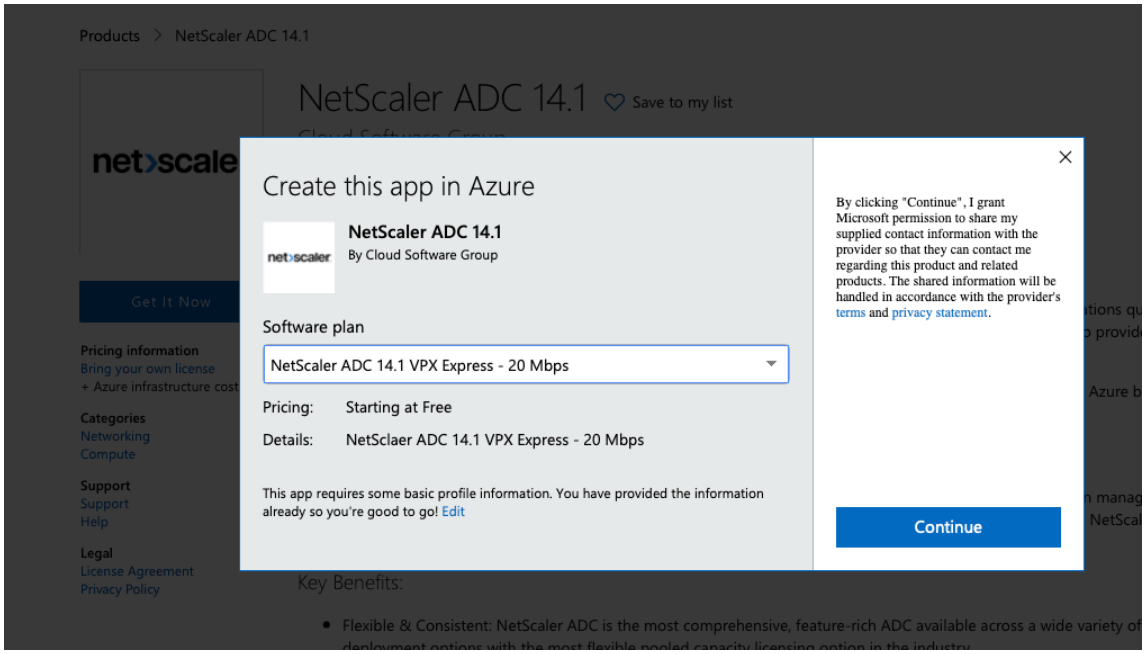
Sie können die NetScaler HA-Paar-Vorlage für internetorientierte Anwendungen im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets oder Availability Zone bereitzustellen.

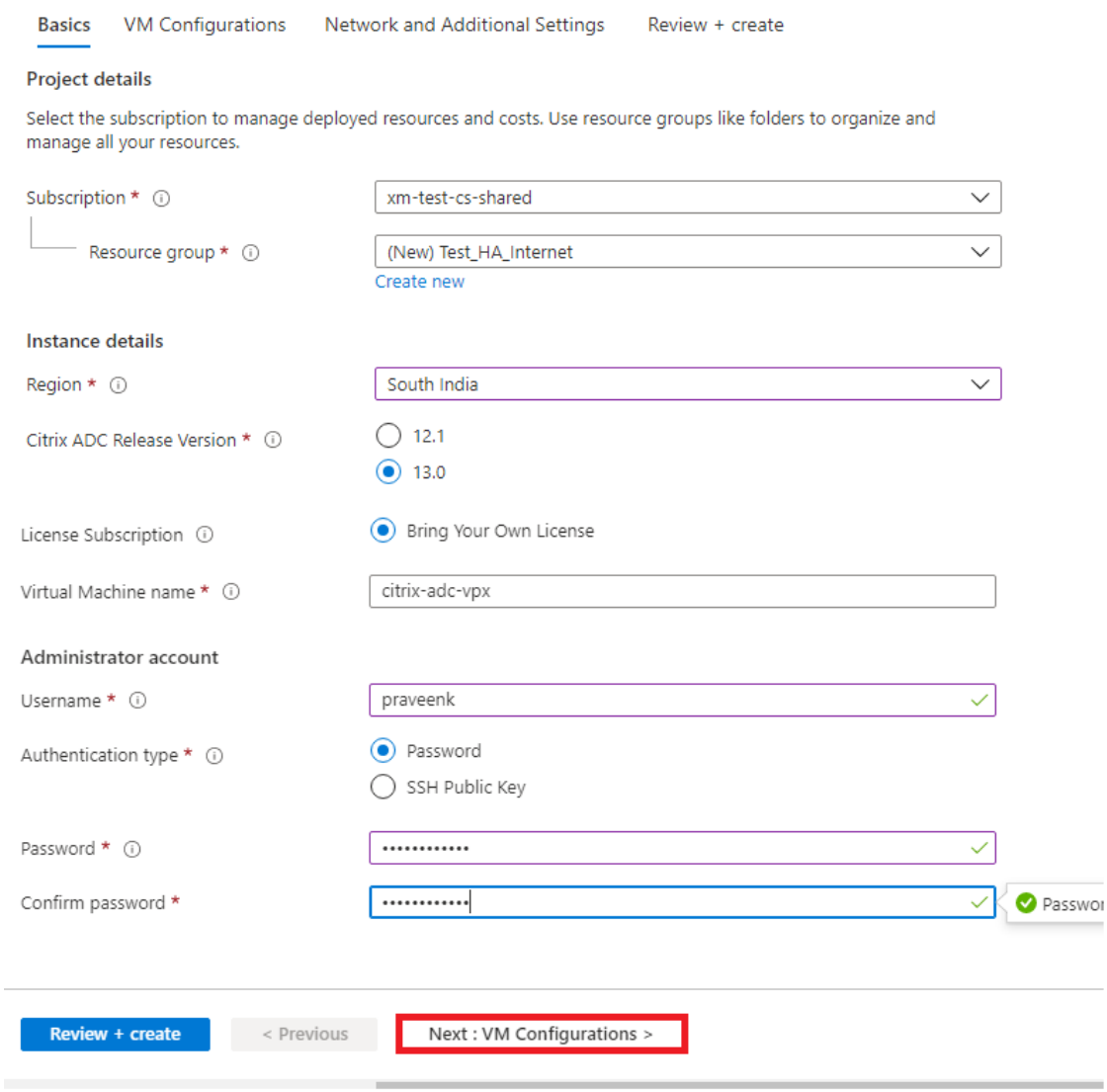
1. Suchen Sie im Azure Marketplace nach **NetScaler**.
2. Klicken Sie auf **JETZT HOLEN**.



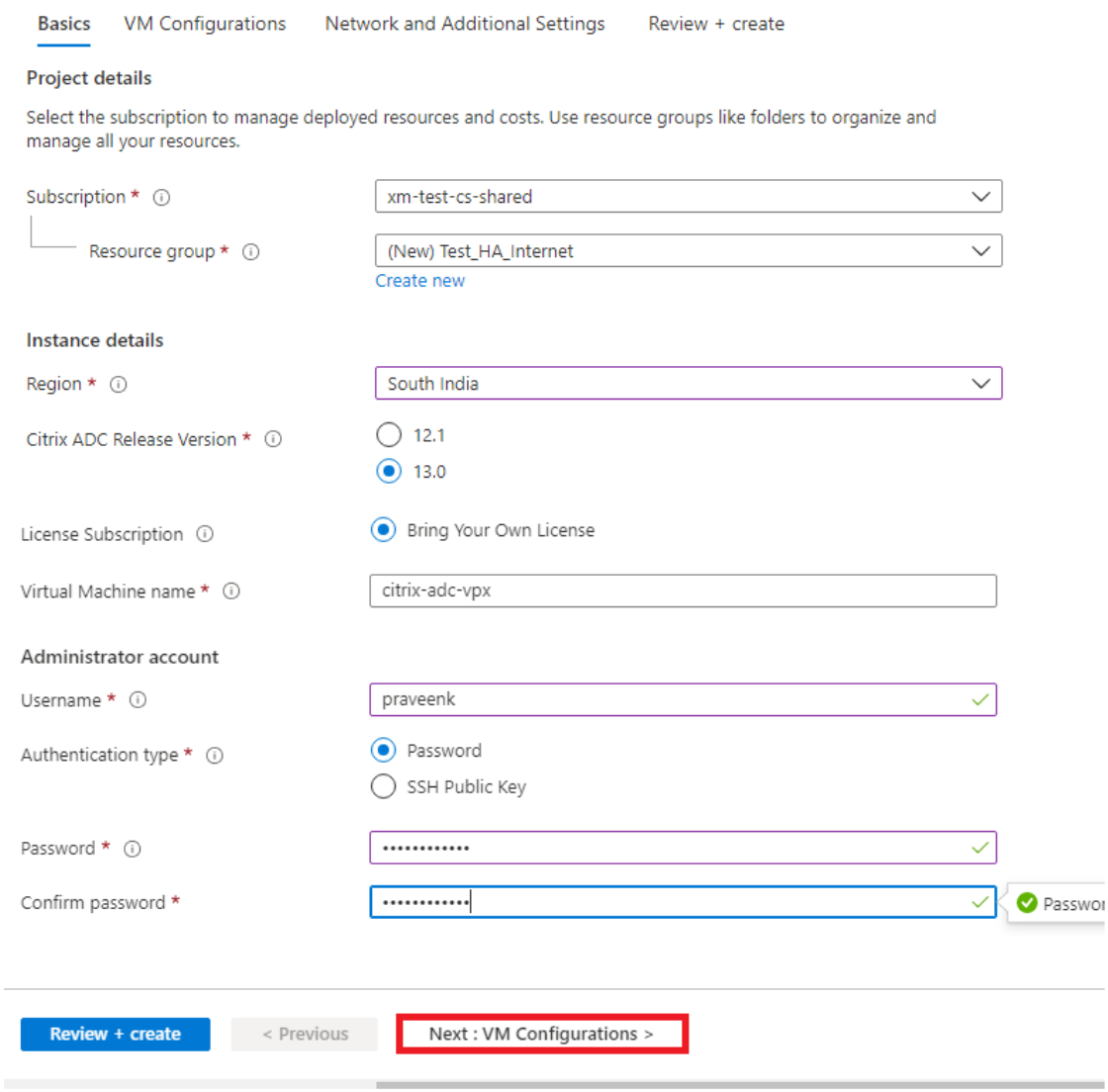
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



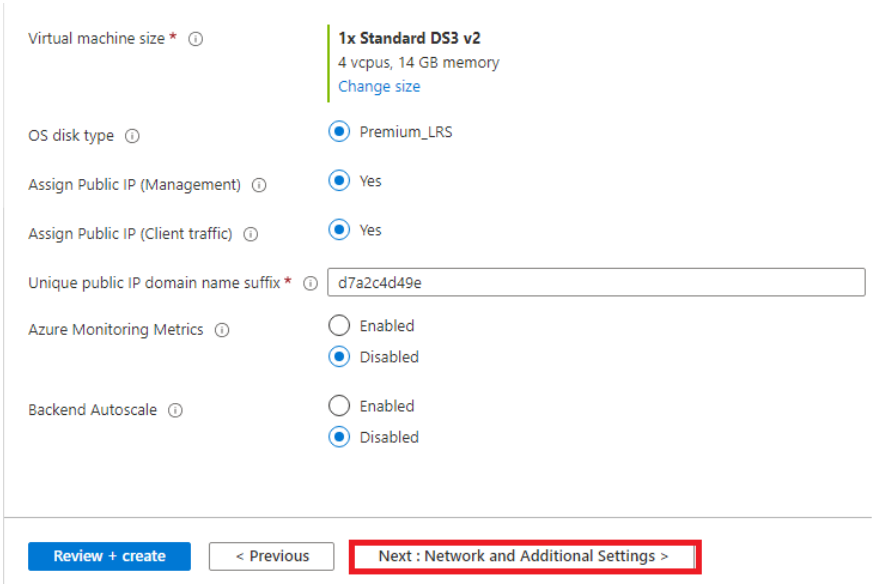
5. Klicken Sie auf **Weiter: VM-Konfigurationen**.



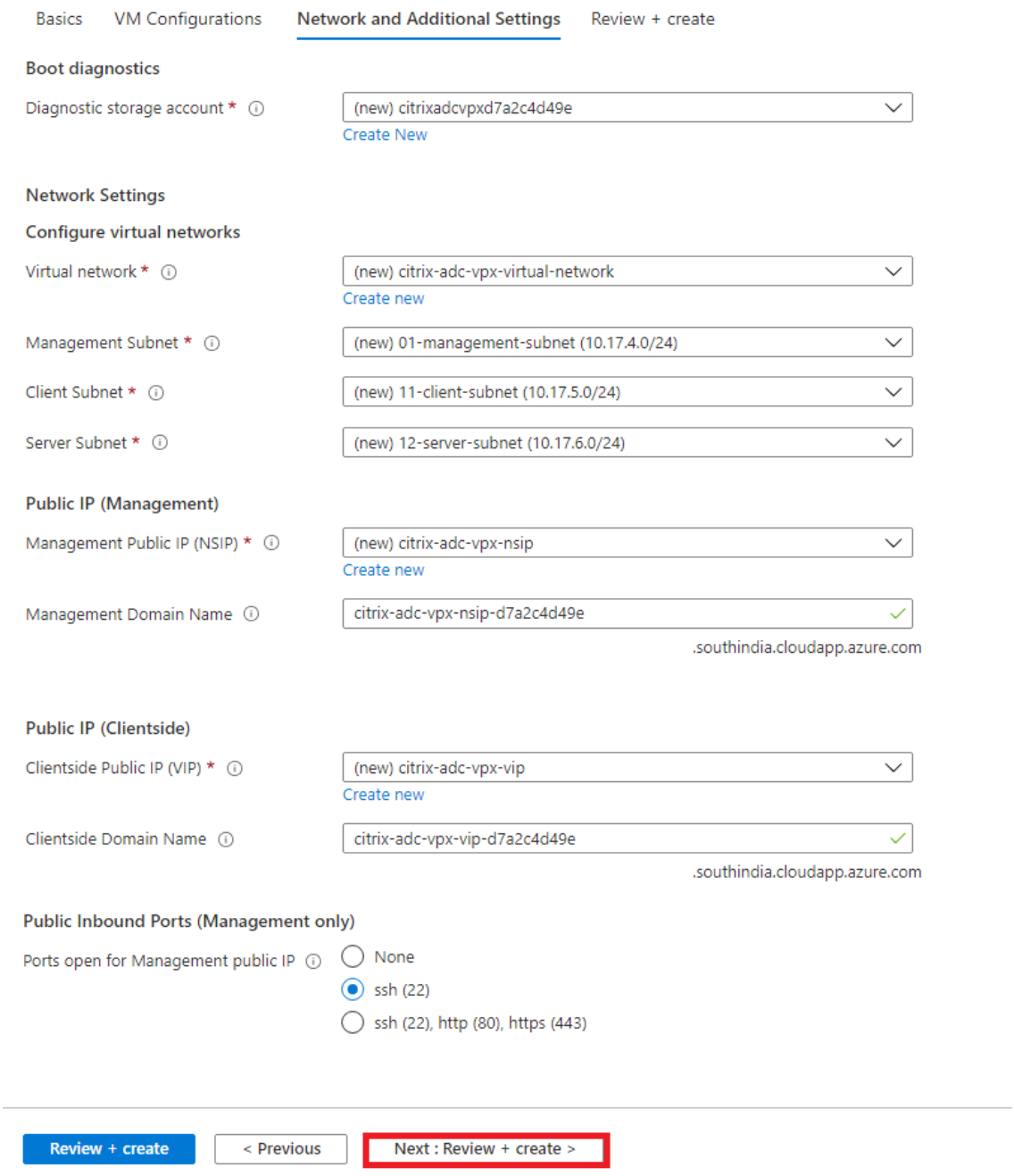
6. Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:

   - Konfigurieren Sie das Suffix für den öffentlichen IP-Domainnamen
   - **Azure Monitoring Metrics**aktivieren oder deaktivieren
   - **Backend**Autoscale aktivieren oder deaktivieren

7. Klicken Sie auf **Weiter: Netzwerk- und Zusatzeinstellungen**



8. Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Startdiagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.



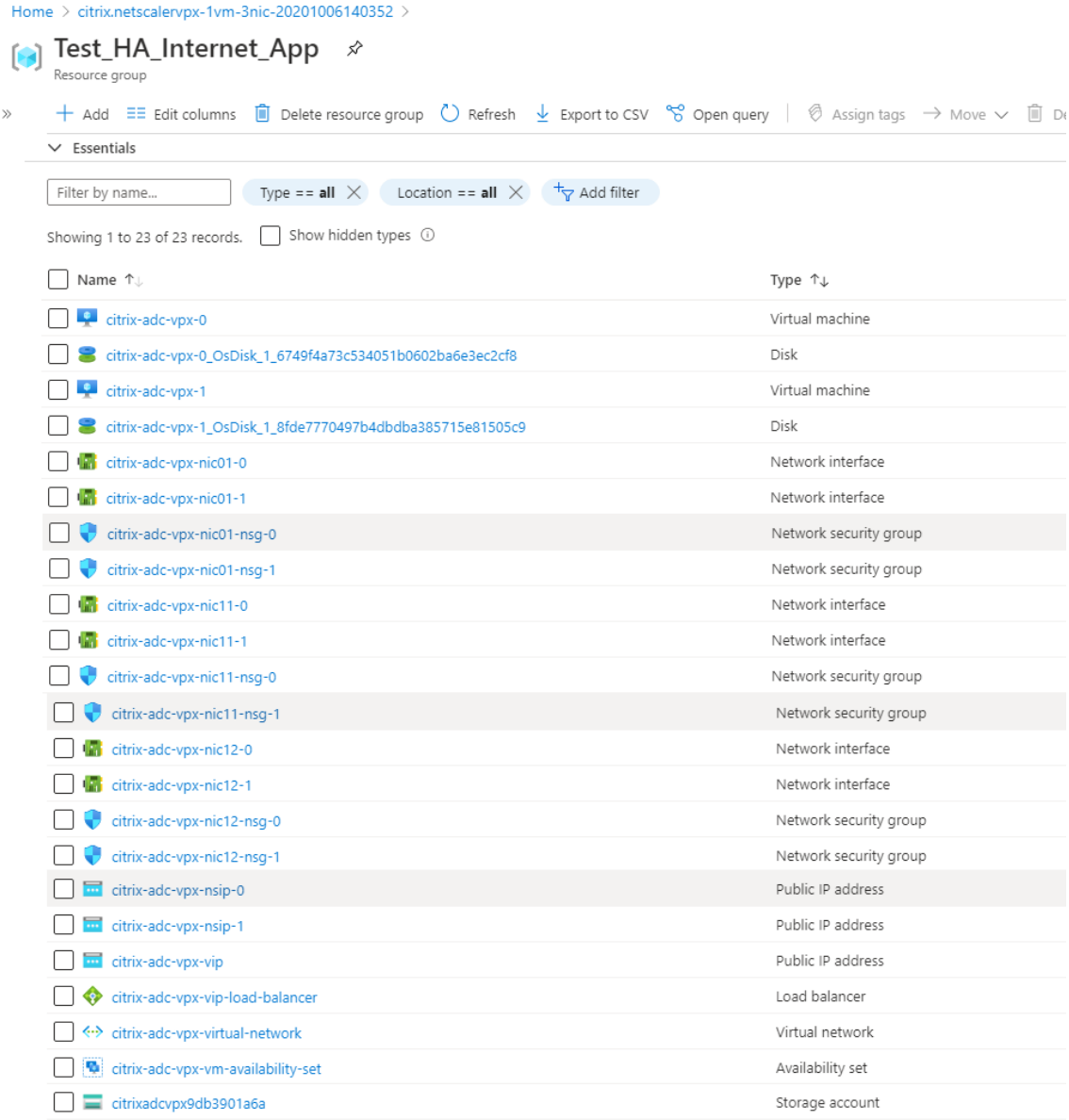
9. Klicken Sie auf **Weiter: Überprüfen + erstellen**.
10. Überprüfen Sie die Grundeinstellungen, die VM-Konfiguration, das Netzwerk und die zusätzlichen Einstellungen und klicken Sie auf **Erstellen**.

    Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Health Probes anzuzeigen.

Das Hochverfügbarkeitspaar wird als **citrix-adc-vpx-0** und **citrix-adc-vpx-1**angezeigt.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.



11. Sie müssen sich an den Knoten **citrix-adc-vpx-0** und **citrix-adc-vpx-1** anmelden, um die folgende Konfiguration zu validieren:

    - NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
    - Auf den primären (citrix-adc-vpx-0) und sekundären (citrix-adc-vpx-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird für die Beantwortung

der ALB-Sonden verwendet und das andere SNIP (Serversubnetz) wird für die Backend-Serverkommunikation verwendet.

> **Hinweis:**
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adressen der VMs citrix-adc-vpx-0 und citrix-adc-vpx-1, im Gegensatz zur klassischen on-premises ADC-Hochverfügbarkeitsbereitstellung, bei der beide gleich sind.

Auf dem primären Knoten (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

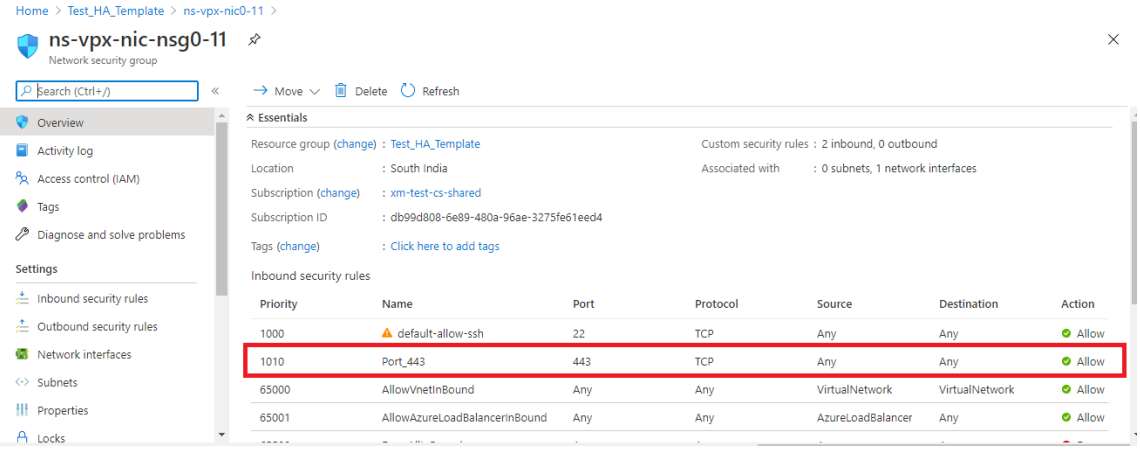
Auf dem sekundären Knoten (citrix-adc-vpx-1)

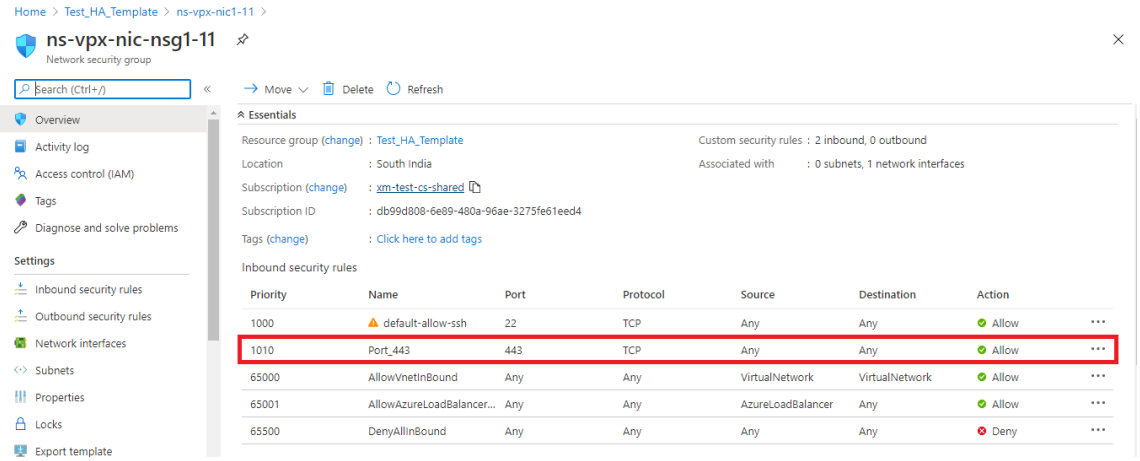

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

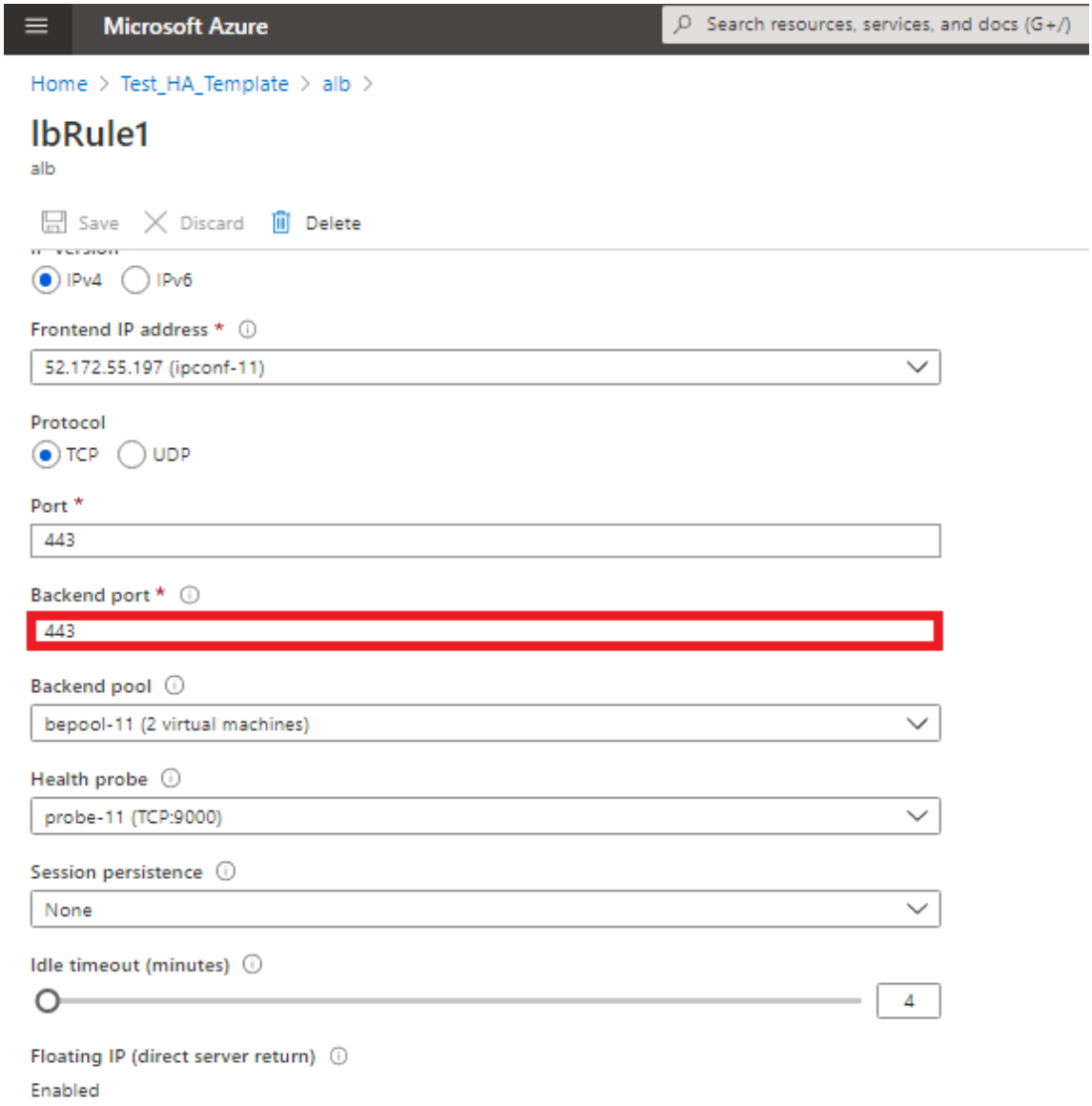
12. Nachdem der primäre und sekundäre Knoten UP sind und der Synchronisierungsstatus **ERFOLG**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem primären Knoten (citrix-adc-vpx-0) mit der öffentlichen IP-Adresse des virtuellen ALB-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
13. Um die öffentliche IP-Adresse des virtuellen ALB-Servers zu finden, navigieren Sie zum **Azure-Portal > Azure Load Balancer > Frontend IP-Konfiguration**.

14. Fügen Sie die eingehende Sicherheitsregel für den virtuellen Serverport 443 in der Netzwerksicherheitsgruppe der beiden Client-Schnittstellen hinzu.

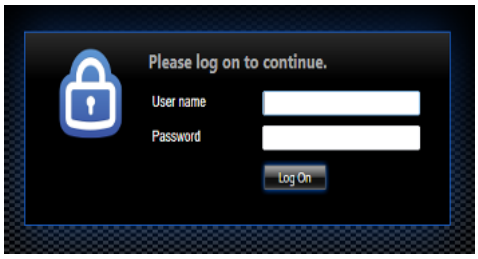




15. Konfigurieren Sie den ALB-Port, auf den Sie zugreifen möchten, und erstellen Sie eine Sicherheitsregel für eingehenden Datenverkehr für den angegebenen Port. Der Backend-Port ist Ihr virtueller Load-Balancing-Serverport oder der virtuelle VPN-Serverport.



16. Jetzt können Sie über den vollqualifizierten Domänennamen (FQDN), der der öffentlichen ALB-IP-Adresse zugeordnet ist, auf den virtuellen Lastausgleichsserver oder den virtuellen VPN-Server zugreifen.



Beispiel-Konfiguration

Führen Sie zum Konfigurieren eines virtuellen Gateway-VPN-Servers und eines virtuellen Lastausgleichsservers die folgenden Befehle auf dem primären Knoten aus (ADC-VPX-0). Die Konfiguration synchronisiert sich automatisch mit dem sekundären Knoten (ADC-VPX-1).

Gateway Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
```

Beispielkonfiguration für den Lastausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
```

Sie können jetzt über den FQDN, der der öffentlichen IP-Adresse von ALB zugeordnet ist, auf den virtuellen Loadbalancing- oder VPN-Server zugreifen.

Im Abschnitt **Ressourcen** finden Sie weitere Informationen zur Konfiguration des virtuellen Lastausgleichsservers.

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Virtuelle Server erstellen
- Einrichten des grundlegenden Lastausgleichs

Hochverfügbarkeitssetup mit externen und internen Load Balancern von Azure gleichzeitig konfigurieren

October 17, 2024

Das Hochverfügbarkeitspaar auf Azure unterstützt sowohl externe als auch interne Load Balancer gleichzeitig.

Sie haben die folgenden zwei Möglichkeiten, ein Hochverfügbarkeitspaar mit externen und internen Load Balancern von Azure zu konfigurieren:

- Verwenden von zwei virtuellen LB-Servern auf der NetScaler Appliance.
- Verwenden eines virtuellen LB-Servers und eines IP-Sets. Der einzelne virtuelle LB-Server dient Datenverkehr zu mehreren IPs, die durch das IPSet definiert sind.

Führen Sie die folgenden Schritte aus, um ein Hochverfügbarkeitspaar in Azure zu konfigurieren, wobei sowohl externe als auch interne Load Balancer gleichzeitig verwendet werden:

Verwenden Sie für die Schritte 1 und 2 das Azure-Portal. Verwenden Sie für die Schritte 3 und 4 die NetScaler VPX GUI oder die CLI.

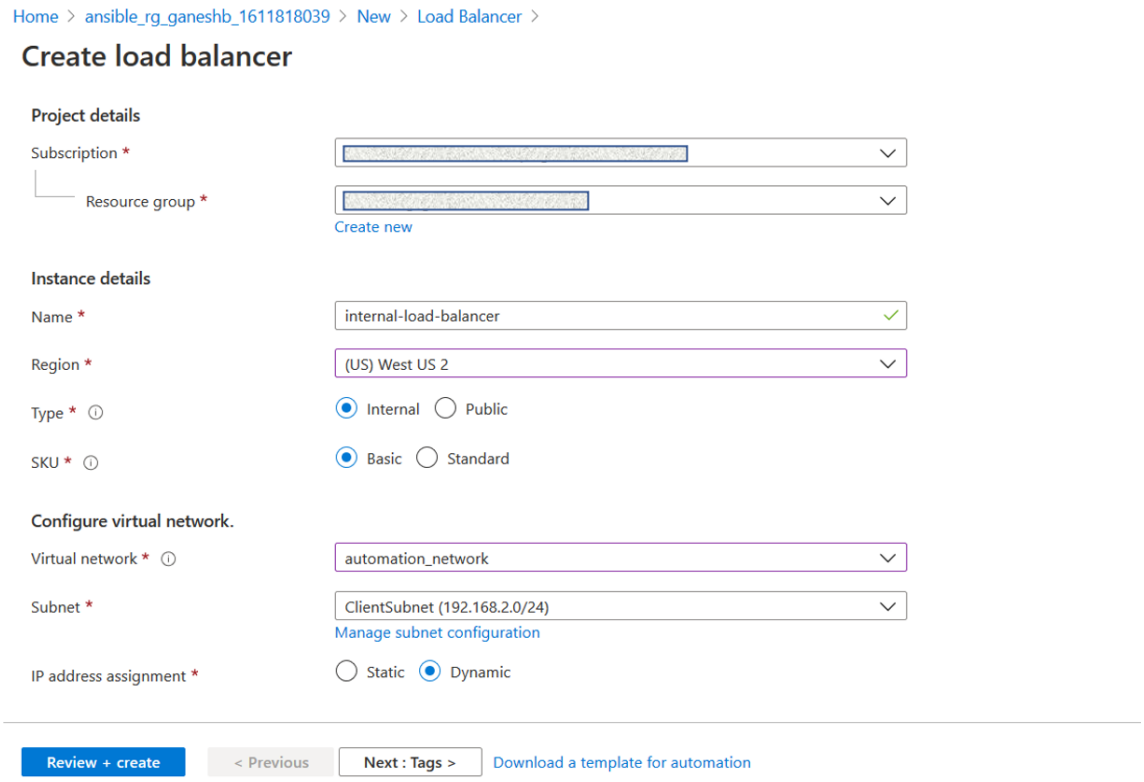
Schritt 1. Konfigurieren Sie einen Azure Load Balancer, entweder einen externen oder einen internen Load Balancer.

Weitere Informationen zum Konfigurieren einer Hochverfügbarkeitseinrichtung mit externen Azure Load Balancern finden Sie unter Konfigurieren einer Hochverfügbarkeitseinrichtung mit mehreren IP-Adressen und einer Netzwerkkarte.

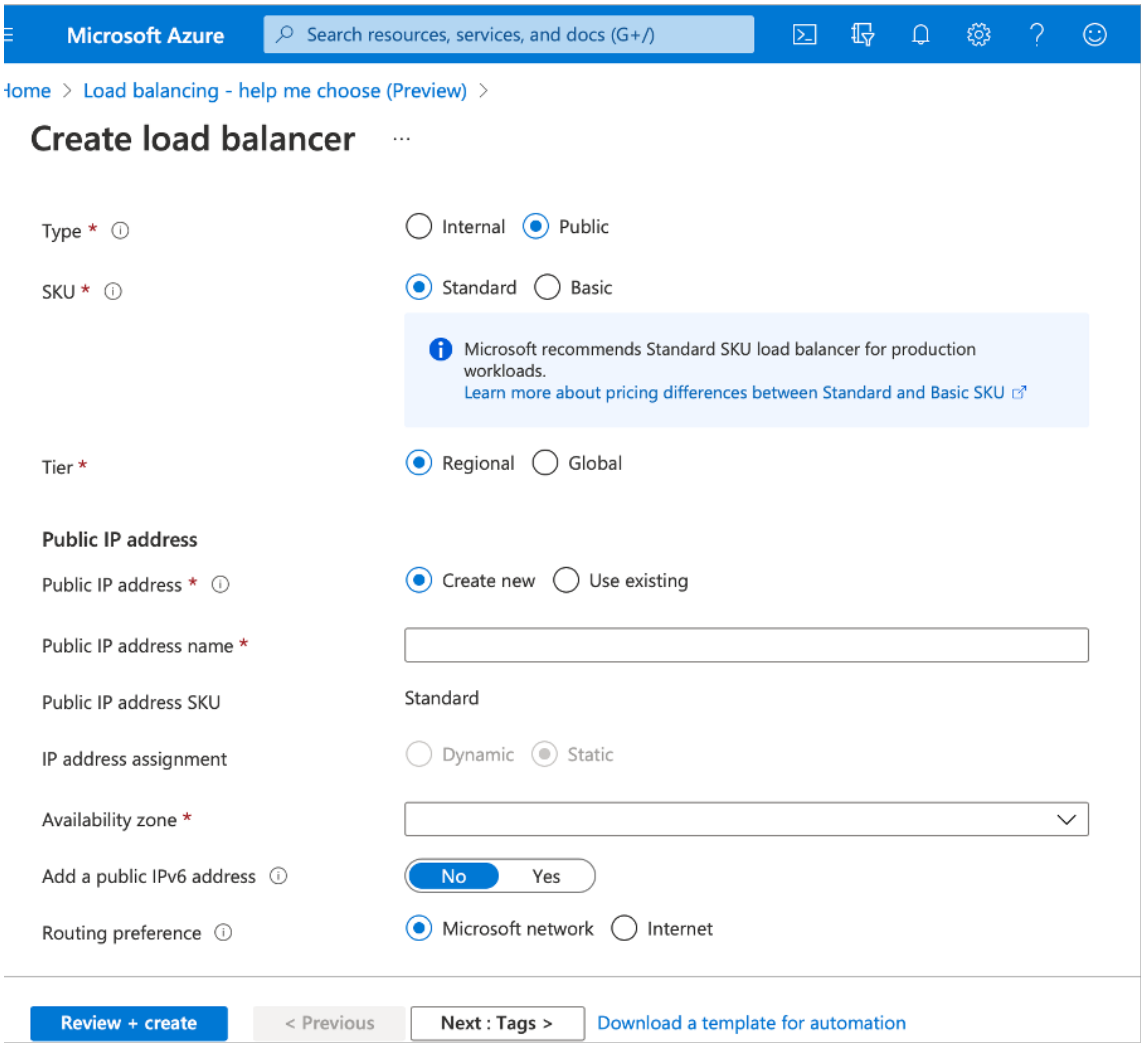
Weitere Informationen zum Konfigurieren eines Hochverfügbarkeits-Setups mit internen Azure-Lastenausgleichsmodulen finden Sie unter Konfigurieren von HA-INC-Knoten mithilfe der NetScaler-Vorlage für Hochverfügbarkeit mit Azure ILB.

Schritt 2. Erstellen Sie einen zusätzlichen Load Balancer (ILB) in Ihrer Ressourcengruppe. Wenn Sie in Schritt 1 einen externen Load Balancer erstellt haben, erstellen Sie jetzt einen internen Load Balancer und umgekehrt.

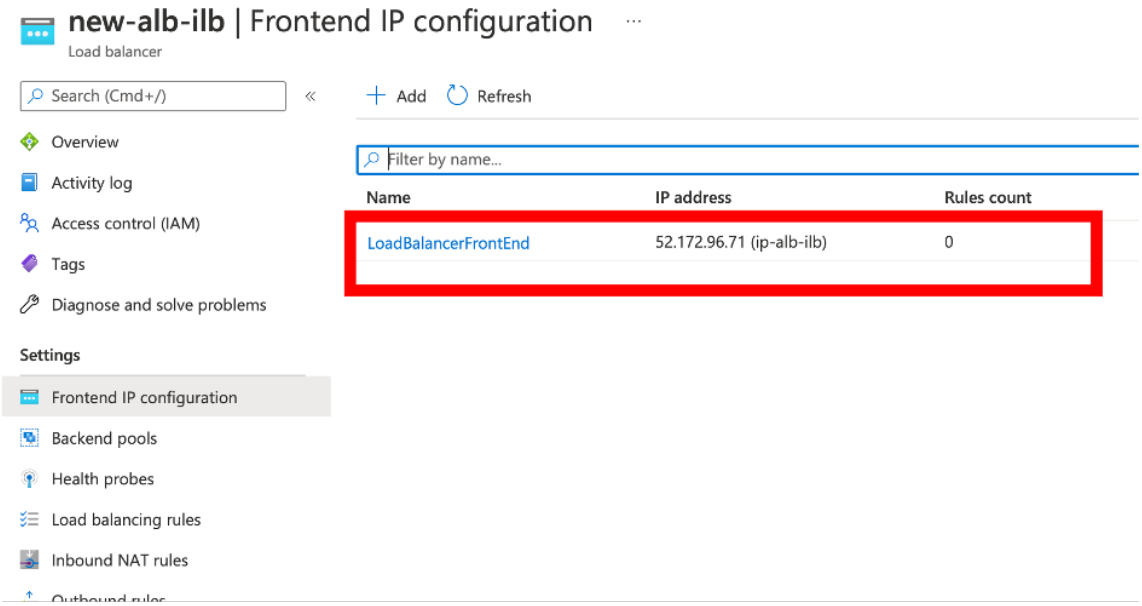
- Um einen internen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Intern**aus. Für das Feld **Subnet** müssen Sie Ihr NetScaler Client-Subnetz auswählen. Sie können eine statische IP-Adresse in diesem Subnetz angeben, vorausgesetzt, es gibt keine Konflikte. Wählen Sie andernfalls die dynamische IP-Adresse aus.



- Um einen externen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Public** und erstellen Sie hier die öffentliche IP-Adresse.



1. Nachdem Sie den Azure Load Balancer erstellt haben, navigieren Sie zur **Frontend-IP-Konfiguration** und notieren Sie sich die hier angezeigte IP-Adresse. Sie müssen diese IP-Adresse verwenden, während Sie den virtuellen ADC Load Balancing Server wie in Schritt 3 erstellen.



2. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung bei der Erstellung der LB-Regel, Back-End-Pools und Integritätstests.
3. Fügen Sie die Client-NICs mit hoher Verfügbarkeit zum Backend-Pool für die ILB hinzu.
4. Erstellen Sie eine Gesundheitssonde (TCP, 9000-Port)
5. Erstellen Sie zwei Load Balancing-Regeln:
    - Eine LB-Regel für HTTP-Datenverkehr (Webapp-Anwendungsfall) auf Port 80. Die Regel muss auch den Backend-Port 80 verwenden. Wählen Sie den erstellten Backend-Pool und die Integritätsprobe aus. Floating IP muss aktiviert sein.
    - Eine weitere LB-Regel für HTTPS- oder CVAD-Datenverkehr auf Port 443. Der Prozess ist der gleiche wie der HTTP-Datenverkehr.

Schritt 3. Erstellen Sie auf dem primären Knoten des NetScaler-Geräts einen virtuellen Lastausgleichsserver für ILB.

1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

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

Beispiel

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```

> **Hinweis:**

> Verwenden Sie die Frontend-IP-Adresse des Load Balancers, die mit dem zusätzlichen Load Balancer verknüpft ist, den Sie in Schritt 2 erstellen.

2. Binden Sie einen Dienst an einen virtuellen Lastenausgleichsserver.

```
bind lb vserver <name> <serviceName>
```

Beispiel

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

Weitere Informationen finden Sie unter Einrichten des grundlegenden Lastenausgleichs

Schritt 4: Alternativ zu Schritt 3 können Sie mit IPSets einen virtuellen Lastausgleichsserver für ILB erstellen.

1. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu.

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

Beispiel

```
add nsip 52.172.96.71 -type vip
```

2. Fügen Sie ein IPSet sowohl auf primären als auch auf sekundären Knoten hinzu.

```
add ipset <name>
```

Beispiel

```
add ipset ipset1
```

3. Binden Sie IP-Adressen an den IP-Satz.

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

Beispiel

```
bind ipset ipset1 52.172.96.71
```

4. Stellen Sie den vorhandenen virtuellen LB-Server so ein, dass er das IPSet verwendet.

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

Beispiel

```
set lb vserver vserver_name -ipset ipset1
```

Weitere Informationen finden Sie unter Konfigurieren eines virtuellen Multi-IP-Servers.

Installieren Sie eine NetScaler VPX-Instanz auf Azure VMware Solution

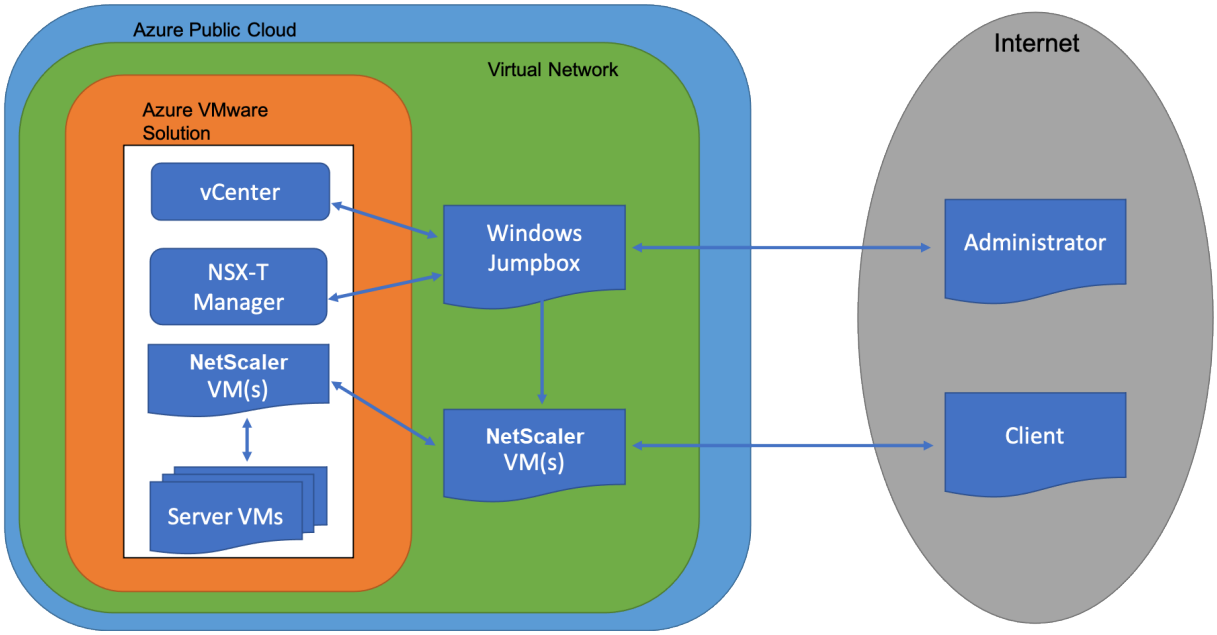
October 17, 2024

Azure VMware Solution (AVS) bietet Ihnen private Clouds, die vSphere-Cluster enthalten, die aus einer dedizierten Bare-Metal-Azure-Infrastruktur basieren. Die minimale Erstbereitstellung beträgt drei Hosts, aber zusätzliche Hosts können einzeln hinzugefügt werden, bis zu maximal 16 Hosts pro Cluster. Alle bereitgestellten Private Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

Mit der VMware Cloud (VMC) auf Azure können Sie Cloud-softwaredefinierte Rechenzentren (SDDC) auf Azure mit der Anzahl der gewünschten ESX-Hosts erstellen. Der VMC auf Azure unterstützt NetScaler VPX-Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert ähnlich wie die ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt die Azure VMware-Lösung in der Azure Public Cloud, auf die ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mit der Azure VMware-Lösung erstellen, verwalten und konfigurieren. Der Administrator kann von einer Windows Jumpbox aus auf das webbasierte vCenter und den NSX-T Manager des AVS zugreifen. Sie können die NetScaler VPX-Instanzen (eigenständige oder Hochverfügbarkeitspaar) und Server-VMs in Azure VMware Solution mit vCenter erstellen und das entsprechende Netzwerk mit NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf AVS funktioniert ähnlich dem lokalen VMware-Host-Cluster. AVS wird von einer Windows Jumpbox aus verwaltet, die im selben virtuellen Netzwerk erstellt wird.

Ein Client kann nur auf den AVS-Dienst zugreifen, indem er sich mit dem VIP von ADC verbindet. Eine andere NetScaler VPX-Instanz außerhalb von Azure VMware Solution, aber im selben virtuellen Azure-Netzwerk, hilft dabei, den VIP der NetScaler VPX-Instanz in Azure VMware Solution als Dienst hinzuzufügen. Je nach Anforderung können Sie die NetScaler VPX-Instanz so konfigurieren, dass sie Dienste über das Internet bereitstellt.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.
- Weitere Informationen zum Erstellen einer Windows Jump Box-VM für den Zugriff und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware Solution
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- VPX-Lizenzdateien abrufen.
- Virtuelle Maschinen (VMs), die in die Azure VMware Solution Private Cloud erstellt oder migriert wurden, müssen an ein Netzwerksegment angeschlossen sein.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX NCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> **Hinweis:**
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Systemvoraussetzungen für die Installation des OVF-Tools beschrieben.

Tabelle 2. Systemvoraussetzungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide”http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

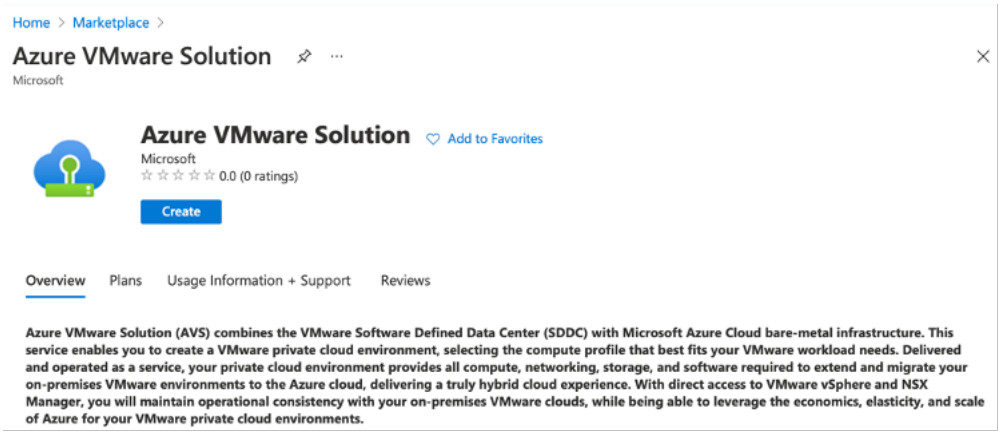
Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

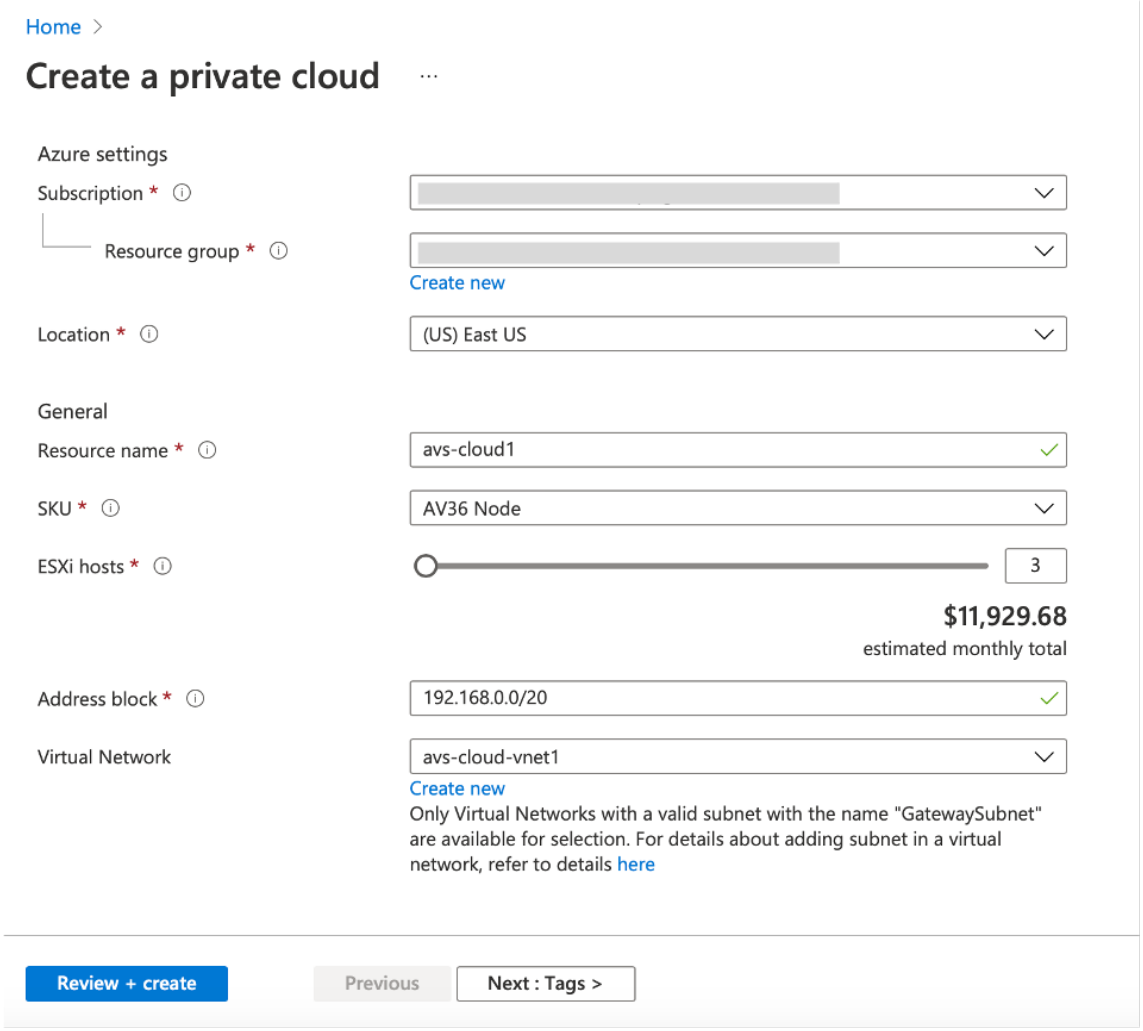
Bereitstellen von Azure VMware-Lösung

1. Melden Sie sich bei Ihrem Microsoft Azure-Portalan und navigieren Sie zu **Azure Marketplace**.
2. Suchen Sie im **Azure Marketplace**nach **Azure VMware Solution** und klicken Sie auf **Erstellen**.

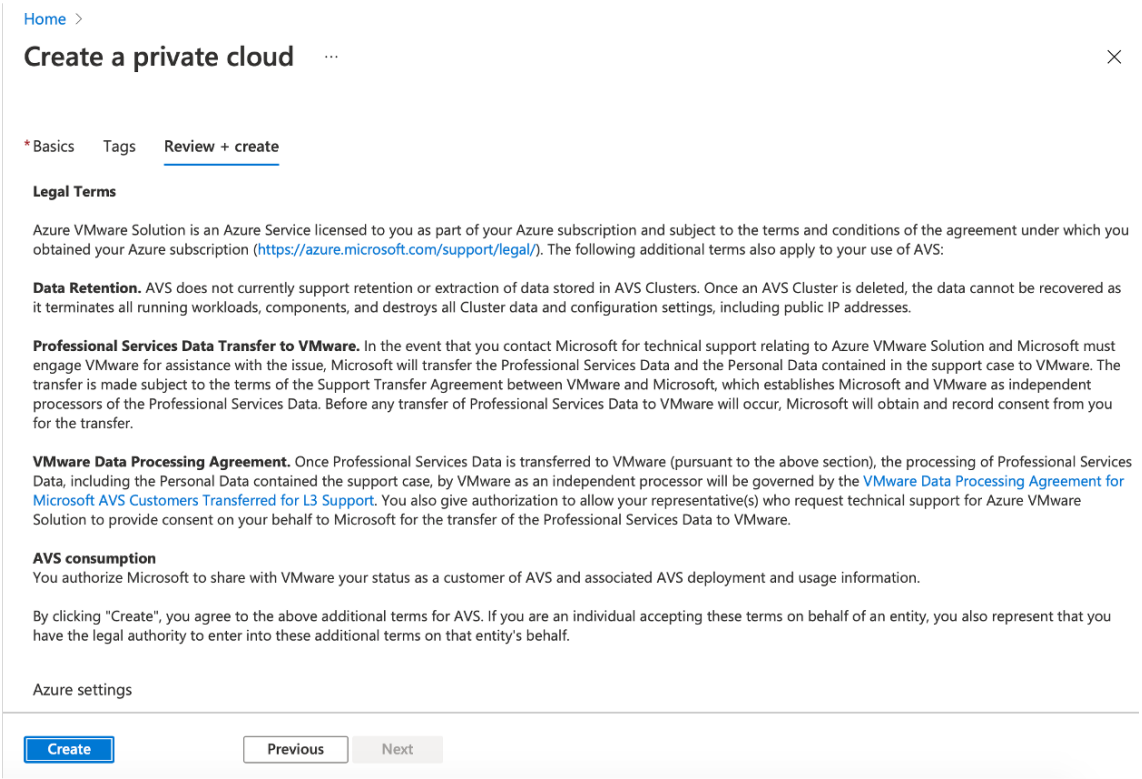


3. Geben **Sie auf der Seite Private Cloud erstellen** die folgenden Details ein:
    - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer Private Cloud zu erstellen.
    - Verwenden Sie für das Feld **Adressblock/22** Adressraum.
    - Stellen Sie für das **virtuelle Netzwerk**sicher, dass sich der CIDR-Bereich nicht mit einem Ihrer on-premises oder anderen Azure-Subnetze (virtuelle Netzwerke) oder mit dem Gateway-Subnetz überschneidet.

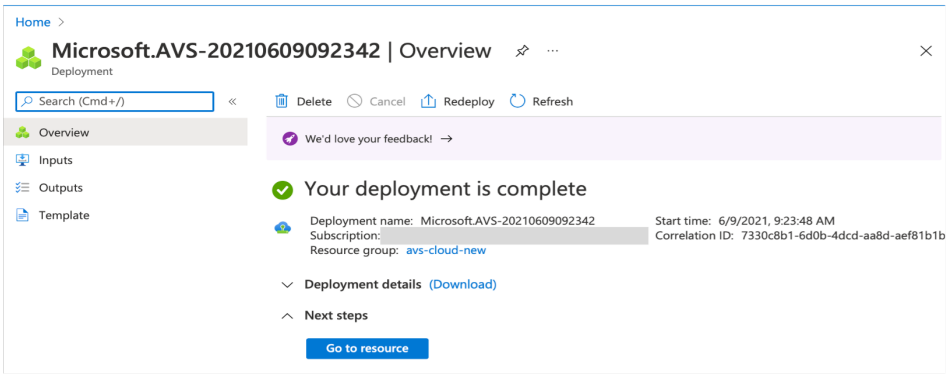
- Das Gateway-Subnetz wird verwendet, um die Verbindung mit Private Cloud weiterzuleiten.



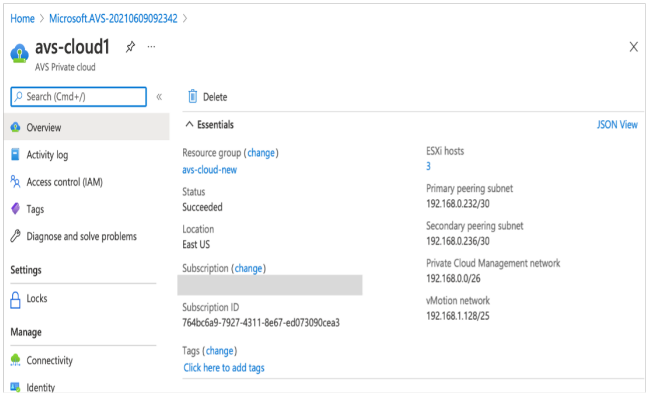
4. Klicken Sie auf **Review + Erstellen**.
5. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.



6. Klicken Sie auf **Erstellen**. Der Provisioning-Prozess der Private Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt wird.



7. Klicken Sie auf **Gehe zu Ressource**, um die erstellte Private Cloud zu überprüfen.



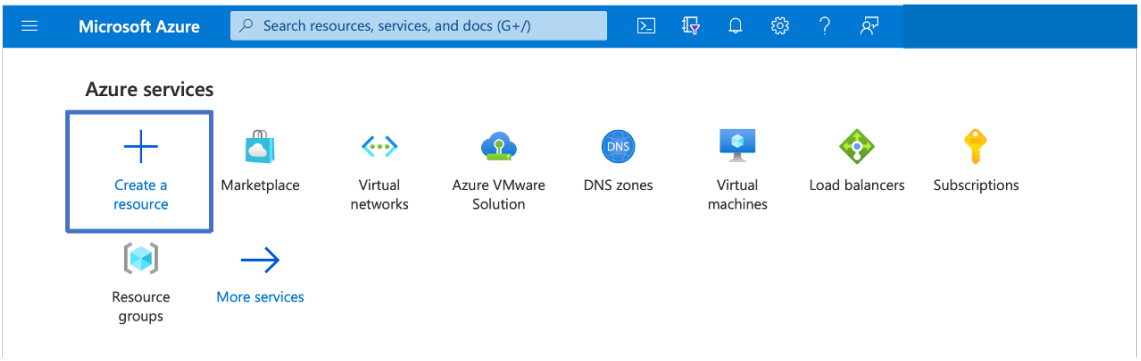
> **Hinweis:**
>
> Um auf diese Ressource zugreifen zu können, benötigen Sie eine VM in Windows, die als Sprungbox fungiert.

Verbinden Sie sich mit einer virtuellen Azure-Maschine unter Windows

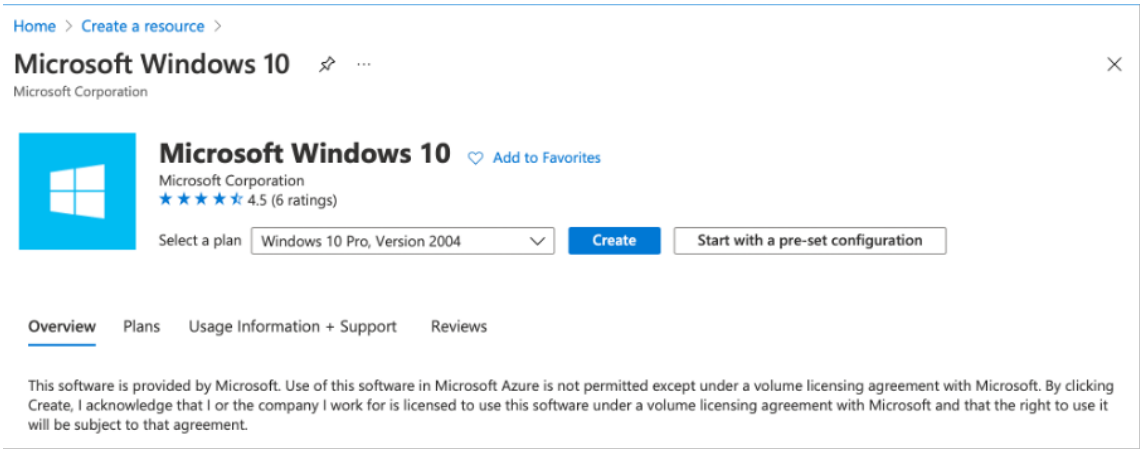
Dieses Verfahren zeigt Ihnen, wie Sie das Azure-Portal verwenden, um eine virtuelle Maschine (VM) in Azure bereitzustellen, auf der Windows Server 2019 ausgeführt wird. Um Ihre VM in Aktion zu sehen, rdp dann auf die VM und installieren den IIS-Webserver.

Um auf die von Ihnen erstellte Private Cloud zugreifen zu können, müssen Sie eine Windows Jump-Box innerhalb desselben virtuellen Netzwerks erstellen.

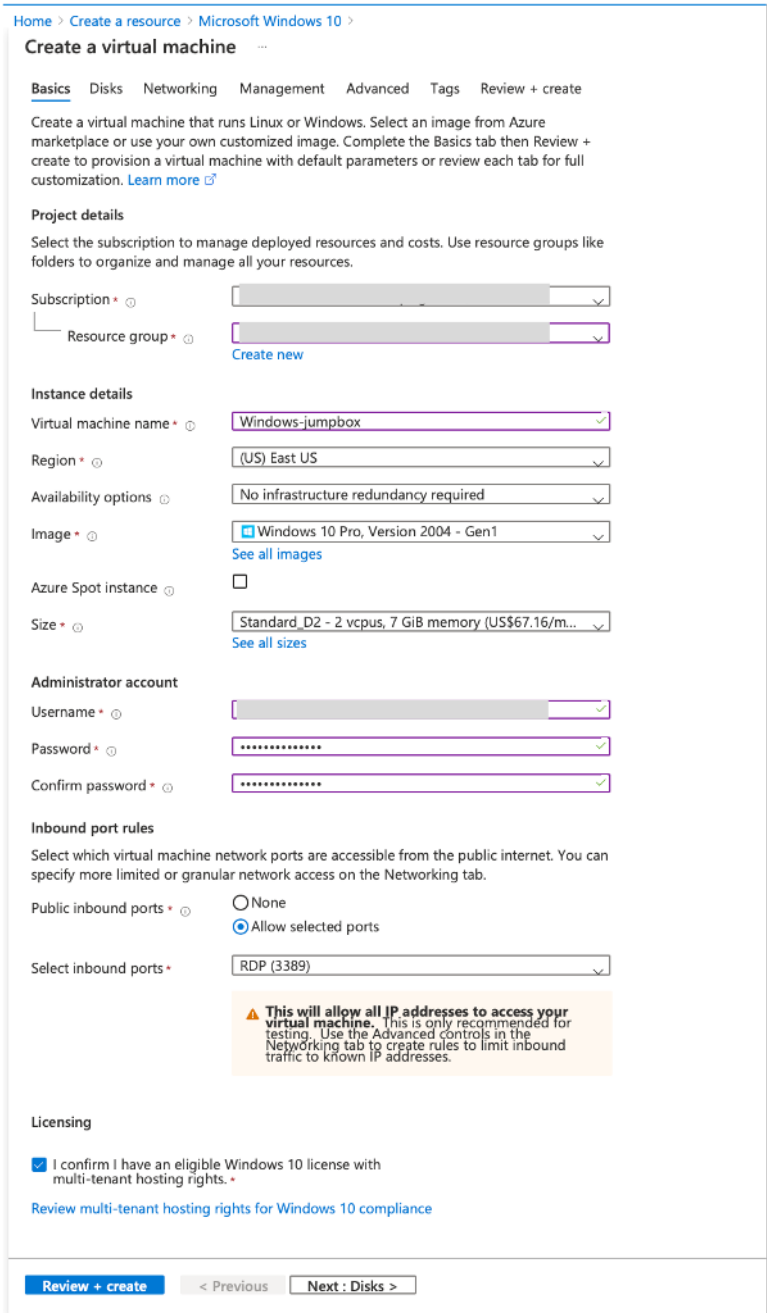
1. Wechseln Sie zum **Azure-Portal**und klicken Sie auf **Ressource erstellen**.



2. Suchen Sie nach **Microsoft Windows 10**und klicken Sie auf **Erstellen**.



3. Erstellen Sie eine virtuelle Maschine (VM), auf der Windows Server 2019 ausgeführt wird. Die Seite "**Virtuelle Maschine erstellen** "wird angezeigt. Geben Sie alle Details auf der Registerkarte **Grundlagen** ein und aktivieren Sie das Kontrollkästchen **Lizenzierung** . Belassen Sie die verbleibenden Standardeinstellungen und wählen Sie dann unten auf der Seite die Schaltfläche **Review + erstellen** .



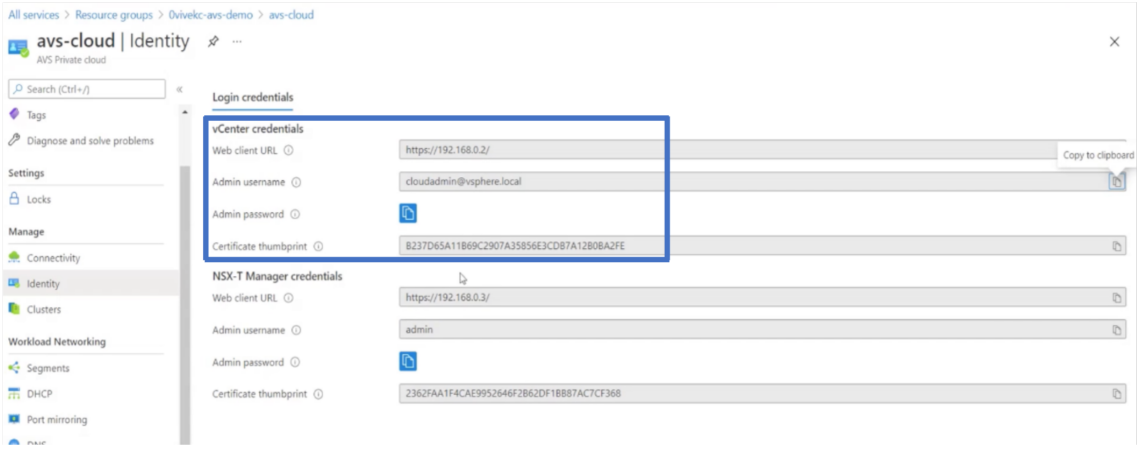
4. Nachdem die Validierung ausgeführt wurde, klicken Sie unten auf der Seite auf die Schaltfläche **Erstellen** .
5. Wählen Sie nach Abschluss der Bereitstellung **Gehe zu Ressource**aus.
6. Wechseln Sie zu der von Ihnen erstellten Windows-VM. Verwenden Sie die öffentliche IP-Adresse der Windows-VM und stellen Sie eine Verbindung mit RDP her.

   Verwenden Sie die Schaltfläche **Verbinden** im Azure-Portal, um eine Remotedesktop-Sitzung (RDP) von einem Windows-Desktop aus zu starten. Zuerst stellen Sie eine Verbindung mit der virtuellen Maschine her und melden sich dann an.

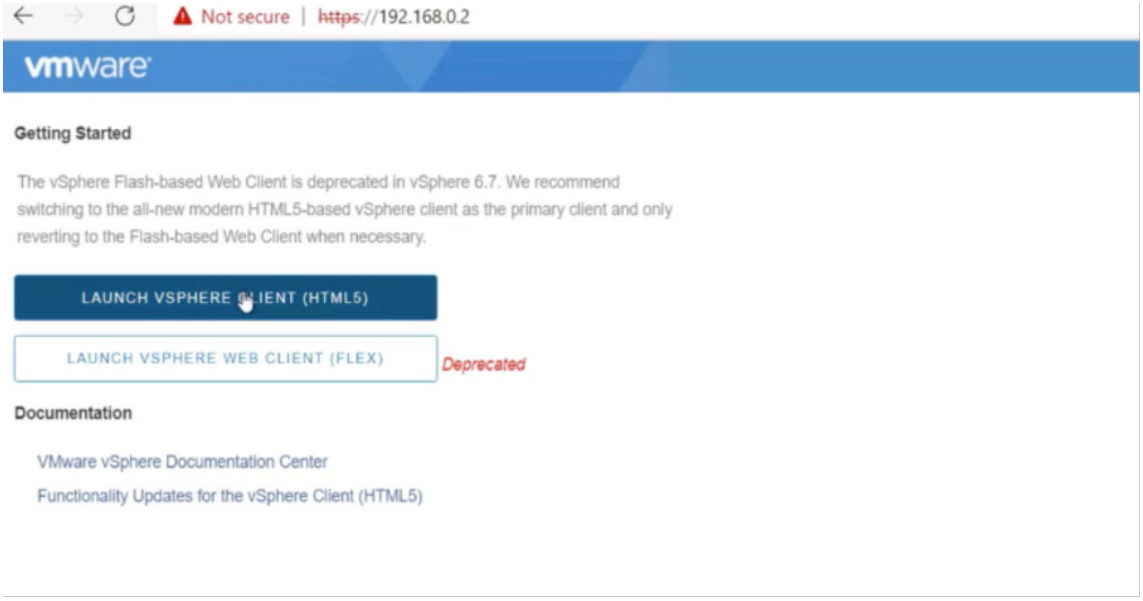
Um eine Verbindung mit einer Windows-VM von einem Mac aus herzustellen, müssen Sie einen RDP-Client für Mac wie Microsoft Remote Desktop installieren. Weitere Informationen finden Sie unter Herstellen und Melden Sie sich bei einer virtuellen Azure-Maschine unter Windowsan.

Greifen Sie auf Ihr Private Cloud vCenter Portal zu

1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die vCenter-Anmeldeinformationen.

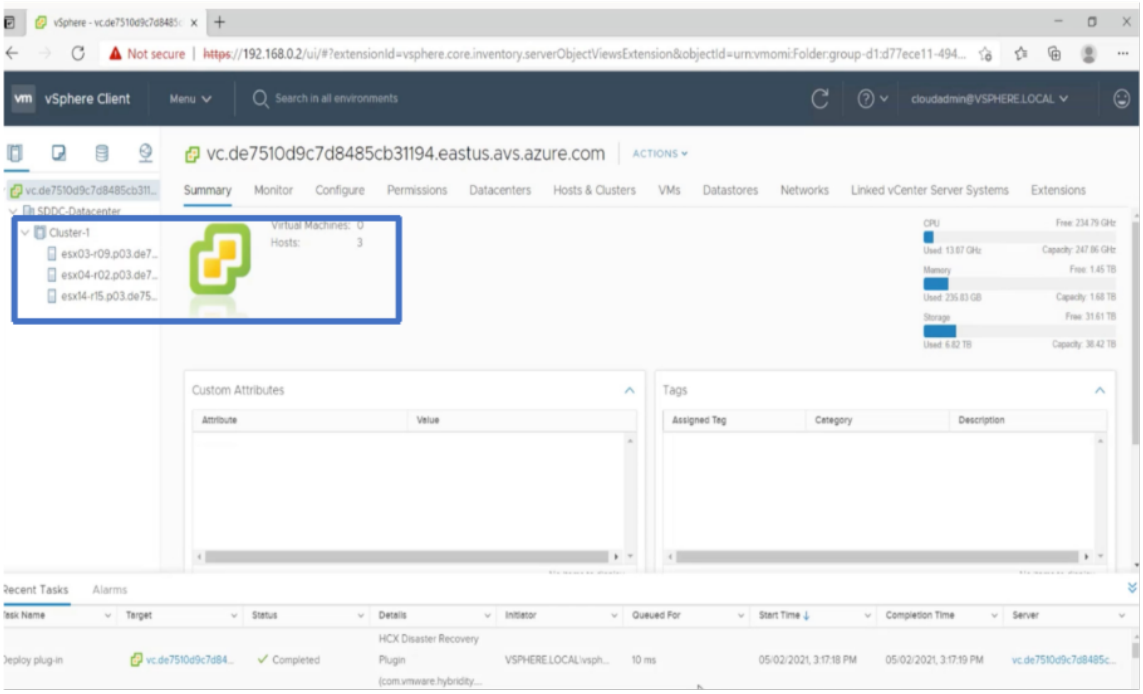


2. Starten Sie den vSphere-Client, indem Sie die vCenter-Webclient-URL eingeben.



3. Melden Sie sich mit den vCenter-Anmeldeinformationen Ihrer Azure VMware Solution Private Cloud bei VMware vSphere an.

4. Im vSphere-Client können Sie die ESXi-Hosts überprüfen, die Sie im Azure-Portal erstellt haben.



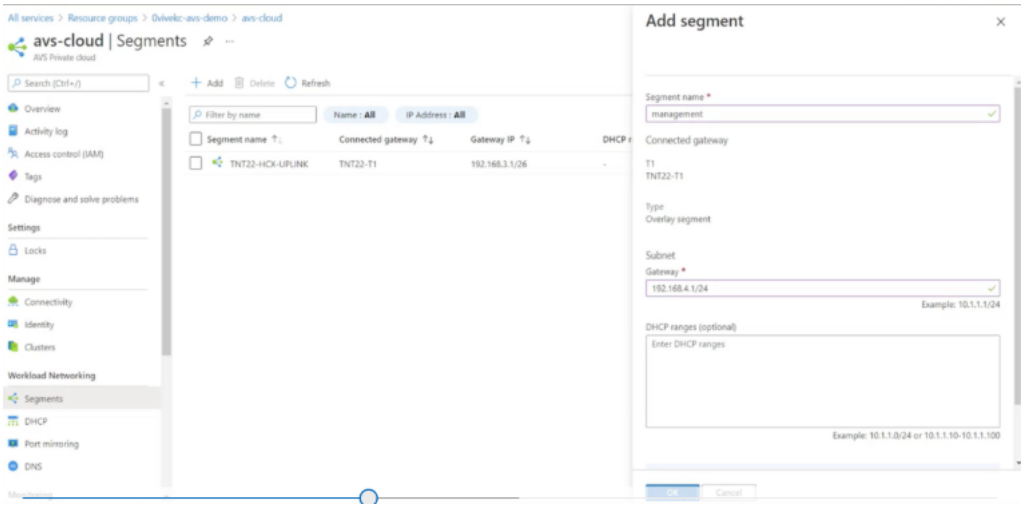
Weitere Informationen finden Sie unter Zugriff auf Ihr Private Cloud vCenter-Portal.

Erstellen Sie ein NSX-T-Segment im Azure-Portal

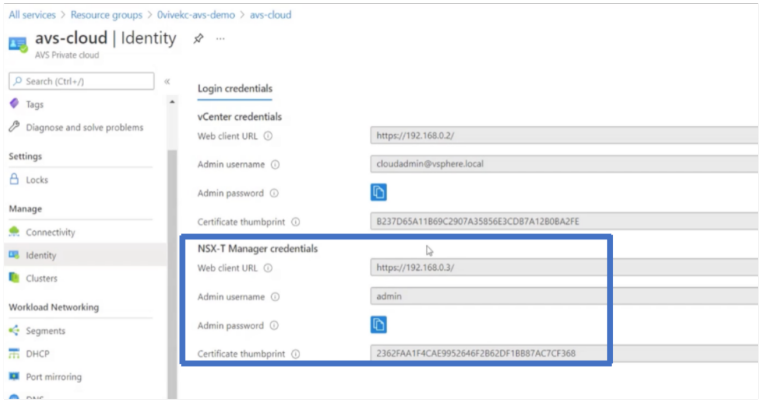
Sie können ein NSX-T-Segment über die Azure VMware Solution Console im Azure-Portal erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads

in diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment erstellt haben, wird es in NSX-T Manager und vCenter angezeigt.

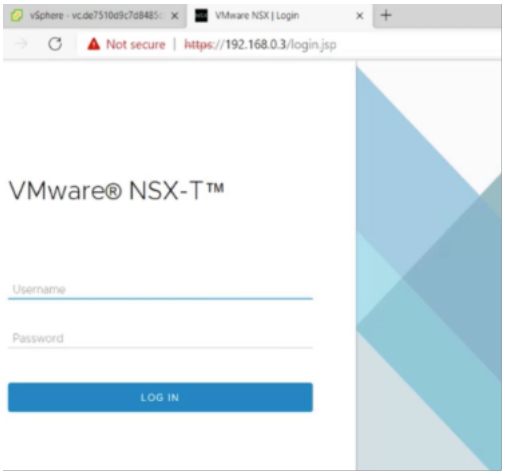
1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Workload-NetzwerkSegmente > Hinzufügen**aus. Geben Sie die Details für das neue logische Segment ein und wählen Sie**OK**aus. Sie können drei separate Segmente für Client-, Management- und Server-Schnittstellen erstellen.



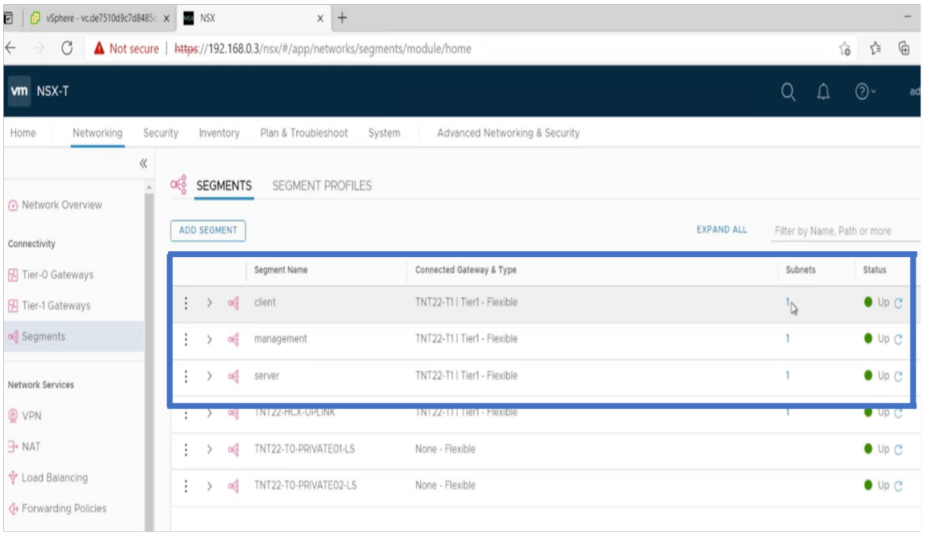
2. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die Anmeldeinformationen von NSX-T Manager.



3. Starten Sie den VMware NSX-T Manager, indem Sie die URL des NSX-T-Webclients eingeben.



4. Im NSX-T-Manager unter **Netzwerk > Segmente**sehen Sie alle Segmente, die Sie erstellt haben. Sie können die Subnetze auch überprüfen.



Weitere Informationen finden Sie unter Erstellen eines NSX-T-Segments im Azure-Portal.

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie VMware Software-Defined Data Center (SDDC) installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware-Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

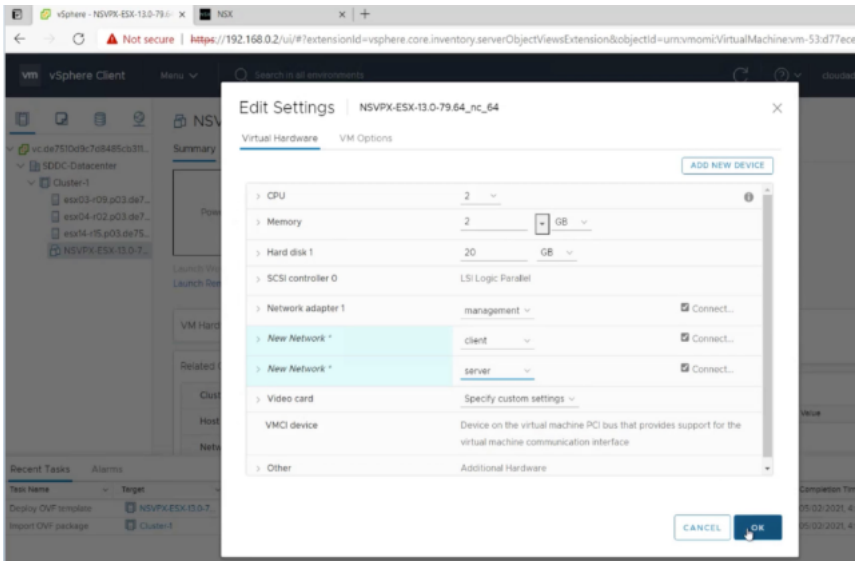
Um NetScaler VPX-Instanzen in der VMware Cloud zu installieren, führen Sie die folgenden Schritte in Windows Jumpbox VM aus:

1. Laden Sie die Setup-Dateien der NetScaler VPX-Instanz für den ESXi-Host von der NetScaler-Downloadseite herunter.

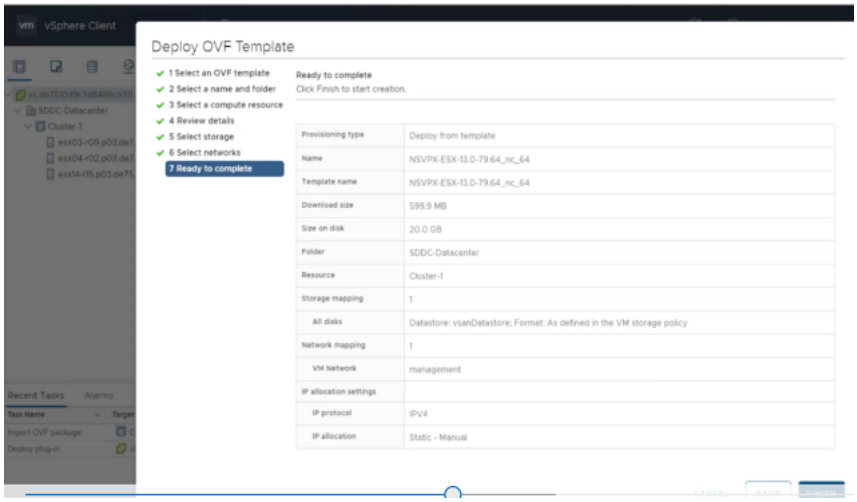
2. Öffnen Sie VMware SDDC in der Windows Jumpbox.
3. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlagebereitstellen im Feld Aus Datei bereitstellen**zu dem Speicherort, an dem Sie die Setupdateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf**Weiter**.

   > **Hinweis:**
   >
   > Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die Azure-Infrastruktur begrenzt und ist möglicherweise in Azure VMware Solution nicht verfügbar.

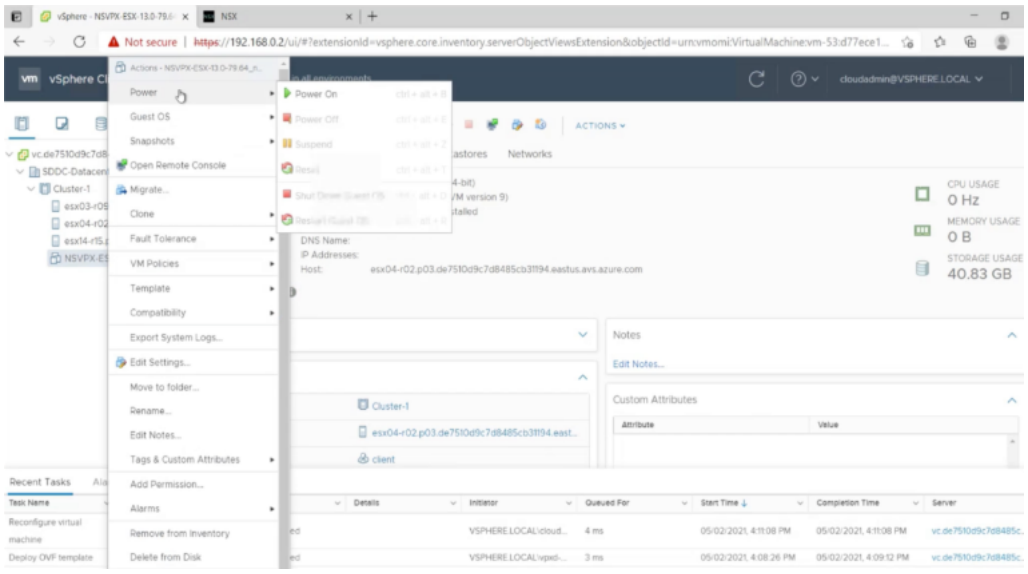
6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **OK**.



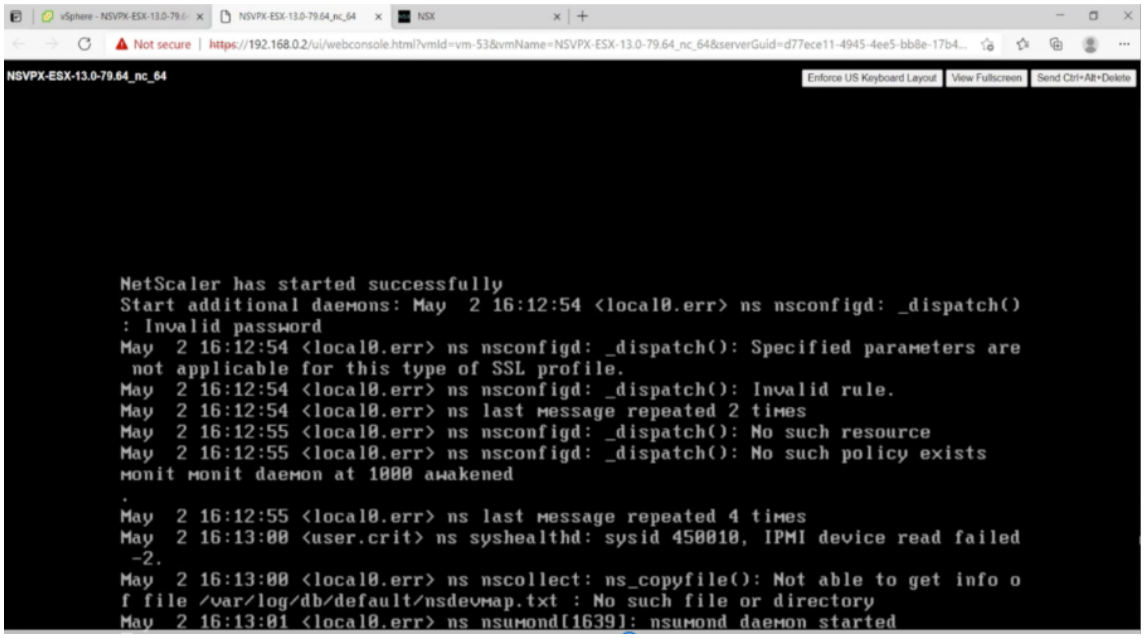
7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.



8. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.



9. Sie sind jetzt vom vSphere-Client aus mit der NetScaler VM verbunden.



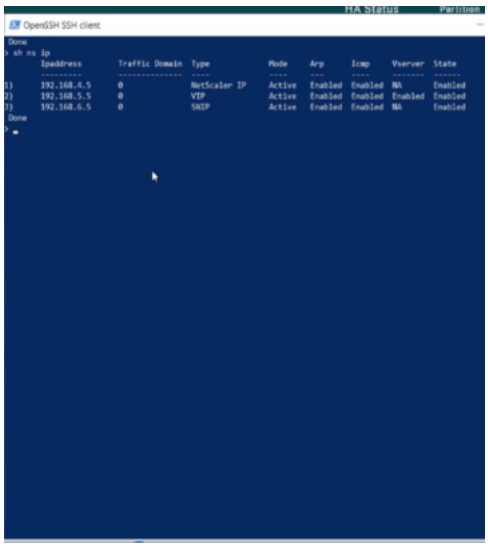
10. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
ssh nsroot@<management IP address>
```

Beispiel

```
ssh nsroot@192.168.4.5
```

11. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

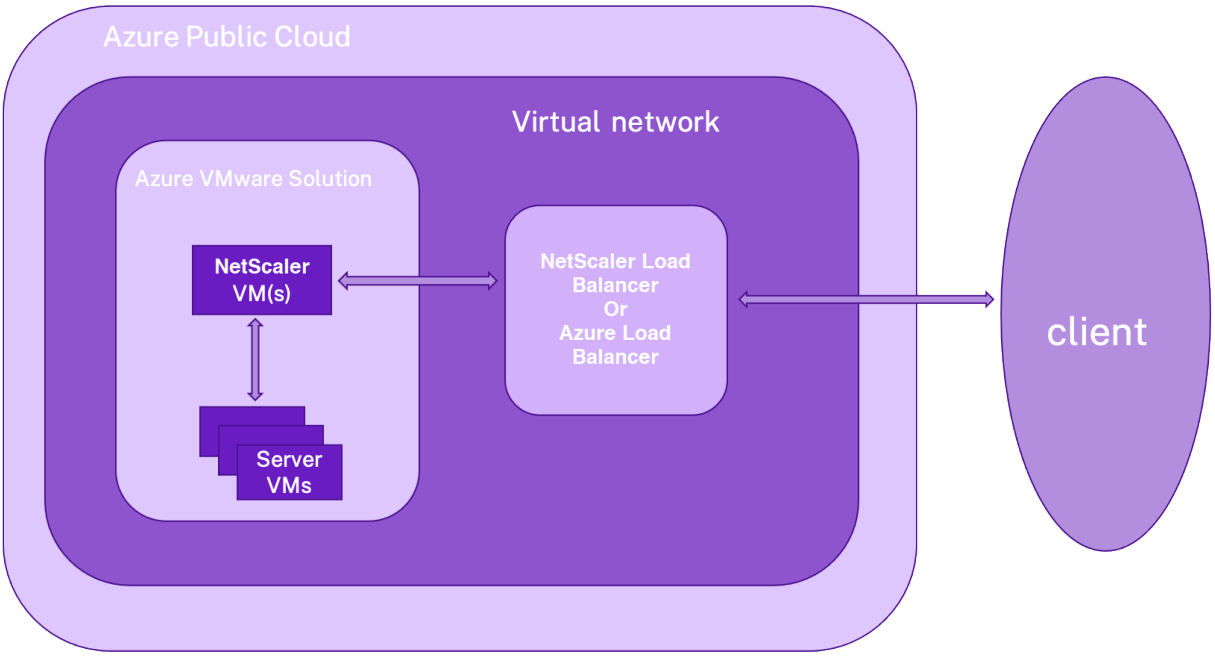


Eigenständige NetScaler VPX-Instanz auf der Azure VMware-Lösung konfigurieren

October 17, 2024

Sie können eine eigenständige NetScaler VPX-Instanz auf der Azure VMware-Lösung (AVS) für internetfähige Anwendungen konfigurieren.

Das folgende Diagramm zeigt die eigenständige NetScaler VPX-Instanz auf Azure VMware Solution. Ein Client kann auf den AVS-Dienst zugreifen, indem er eine Verbindung zur virtuellen IP-Adresse (VIP) von NetScaler innerhalb des AVS herstellt. Sie können dies erreichen, indem Sie einen NetScaler Load Balancer oder die Azure Load Balancer-Instanz außerhalb von AVS, jedoch im selben virtuellen Azure-Netzwerk bereitstellen. Konfigurieren Sie den Load Balancer für den Zugriff auf den VIP der NetScaler VPX-Instanz innerhalb des AVS-Dienstes.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.

- Weitere Informationen zum Erstellen einer Windows Jumpbox-VM für den Zugriff auf und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-Lösung.
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- Weitere Informationen zum Installieren einer NetScaler VPX-Instanz in der VMware-Cloud finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware-Cloud.

Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des NetScaler Load Balancer

Befolgen Sie diese Schritte, um die eigenständige NetScaler VPX-Instanz auf AVS für internetorientierte Anwendungen mithilfe des NetScaler Load Balancer zu konfigurieren.

1. Stellen Sie eine NetScaler VPX-Instanz in der Azure Cloud bereit. Weitere Informationen finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass es im selben virtuellen Netzwerk wie die Azure VMware Cloud bereitgestellt wird.

2. Konfigurieren Sie die NetScaler VPX-Instanz für den Zugriff auf die VIP-Adresse von NetScaler VPX, das auf AVS bereitgestellt wird.

   a) Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

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

   Beispiel

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   ```

   b) Fügen Sie einen Dienst hinzu, der eine Verbindung zum VIP von NetScaler VPX herstellt, der auf AVS bereitgestellt wird.

   ```
   add service <name> <ip> <serviceType> <port>
   ```

   Beispiel

   ```
   add service webserver1 192.168.4.10 HTTP 80
   ```

   c) Binden Sie einen Dienst an den virtuellen Lastausgleichsserver.


```
bind lb vserver <name> <serviceName>
```

Beispiel

```
bind lb vserver lb1 webserver1
```

Konfigurieren der eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des Azure Load Balancer

Befolgen Sie diese Schritte, um die eigenständige NetScaler VPX-Instanz auf AVS für internetorientierte Anwendungen mithilfe des Azure Load Balancer zu konfigurieren.

1. Konfigurieren Sie eine Azure Load Balancer-Instanz in der Azure-Cloud. Konfigurieren Sie eine Azure Load Balancer-Instanz in Azure Cloud Weitere Informationen finden Sie in der Azure-Dokumentation zum Erstellen des Load Balancers.
2. Fügen Sie die VIP-Adresse der NetScaler VPX-Instanz, die auf AVS bereitgestellt wird, zum Backend-Pool hinzu.

   Der folgende Azure-Befehl fügt eine Back-End-IP-Adresse zum Back-End-Adresspool des Lastenausgleichs hinzu.

```
az network lb address-pool address add
                                    --resource-group <Azure VMC
                                       Resource Group>
                                    --lb-name <LB Name>
                                    --pool-name <Backend pool
                                       name>
                                    --vnet <Azure VMC Vnet>
                                    --name <IP Address name>
                                    --ip-address <VIP of ADC in
                                       VMC>
```

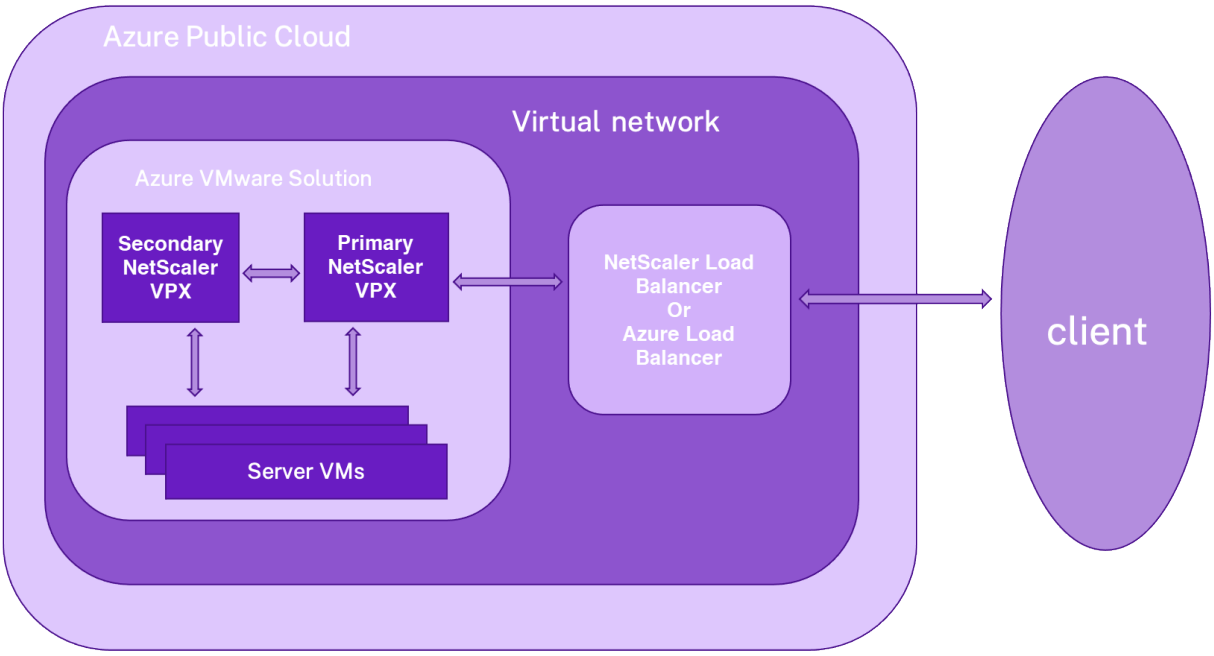
> **Hinweis:**
>
> Stellen Sie sicher, dass der Azure Load Balancer im selben virtuellen Netzwerk wie die Azure VMware-Cloud bereitgestellt wird.

NetScaler VPX-Hochverfügbarkeitssetups auf Azure VMware-Lösung konfigurieren

October 17, 2024

Sie können ein NetScaler VPX HA-Setup auf Azure VMware-Lösung (AVS) für internetfähige Anwendungen konfigurieren.

Das folgende Diagramm zeigt das NetScaler VPX HA-Paar auf AVS. Ein Client kann auf den AVS-Dienst zugreifen, indem er sich mit dem VIP des primären ADC-Knotens innerhalb des AVS verbindet. Sie können dies erreichen, indem Sie einen NetScaler Load Balancer oder die Azure Load Balancer-Instanz außerhalb von AVS, jedoch im selben virtuellen Azure-Netzwerk bereitstellen. Konfigurieren Sie den Load Balancer für den Zugriff auf den VIP des primären ADC-Knotens innerhalb des AVS-Dienstes.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.
- Weitere Informationen zum Erstellen einer Windows Jumpbox-VM für den Zugriff auf und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-Lösung.
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware-Lösung.

Konfigurationsschritte

Befolgen Sie diese Schritte, um das NetScaler VPX Hochverfügbarkeitssetup in AVS für internetfähige Anwendungen zu konfigurieren.

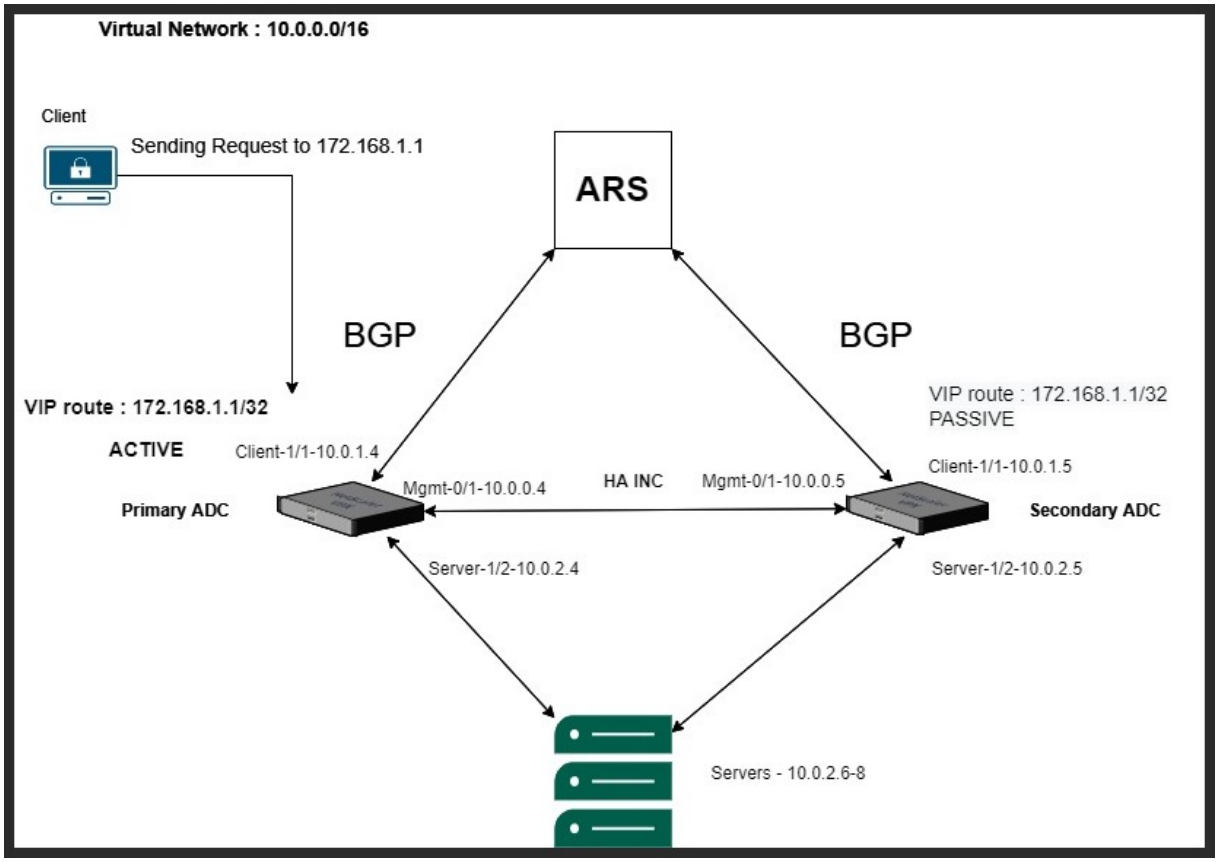
1. Erstellen Sie zwei NetScaler VPX-Instanzen in der VMware Cloud. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware-Cloud.
2. Konfigurieren Sie das NetScaler HA-Setup. Weitere Informationen finden Sie unter Konfigurieren von Hochverfügbarkeit.
3. Konfigurieren Sie das NetScaler HA-Setup so, dass es für internetorientierte Anwendungen zugänglich ist.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mit dem NetScaler-Load Balancer finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mit dem NetScaler-Load Balancer.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mit dem Azure Load Balancer finden Sie unter Konfigurieren der eigenständigen NetScaler VPX-Instanz auf AVS mit dem Azure Load Balancer.

Azure-Routenserver mit NetScaler VPX HA-Paar konfigurieren

October 17, 2024

Sie können den Azure-Routenserver mit der NetScaler VPX-Instanz konfigurieren, um die mit dem virtuellen Netzwerk konfigurierten VIP-Routen mit dem BGP-Protokoll auszutauschen. Der NetScaler kann im Standalone- oder HA-INC-Modus bereitgestellt und dann mit BGP konfiguriert werden. Für diese Bereitstellung ist kein Azure Load Balancer (ALB) vor dem ADC HA-Paar erforderlich.

Das folgende Diagramm zeigt, wie eine VPX HA-Topologie in den Azure-Routenserver integriert ist. Jede der ADC-Instanzen verfügt über 3 Schnittstellen: eine für die Verwaltung, eine für den Client-Datenverkehr und eine für den Serververkehr.



Das Topologiediagramm verwendet die folgenden IP-Adressen.

Beispiel-IP-Konfiguration für die primäre ADC-Instanz:

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

Beispiel-IP-Konfiguration für die sekundäre ADC-Instanz:

```
NSIP: 10.0.0.5/24
SNIP on 1/1: 10.0.1.5/24
SNIP on 1/2: 10.0.2.5/24
VIP: 172.168.1.1/32
```

Voraussetzungen

Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

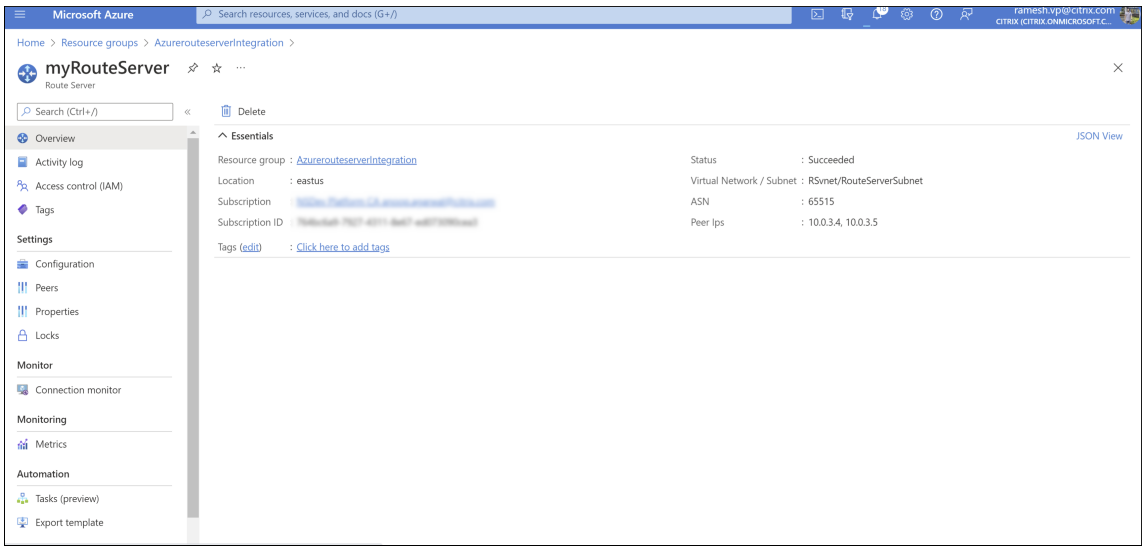
- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.

- Überblick über Azure Route Server. Weitere Informationen finden Sie unter Was ist Azure Route Server?.
- Arbeiten einer NetScaler-Appliance. Weitere Informationen finden Sie in der NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie im ADC-Netzwerk.

So konfigurieren Sie einen Azure-Routenserver mit einem NetScaler VPX HA-Paar

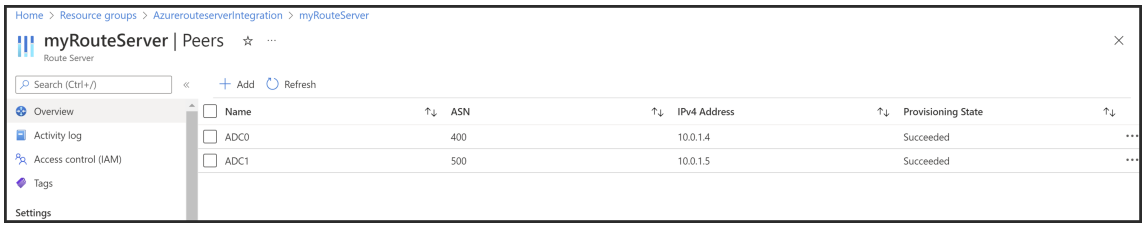
1. Erstellen Sie einen Routenserver im Azure-Portal. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines Routenservers mithilfe des Azure-Portals.

   Im folgenden Beispiel wird das Subnetz 10.0.3.0/24 für die Bereitstellung des Azure-Servers verwendet. Sobald der Routenserver erstellt wurde, rufen Sie die IP-Adressen des Routenservers ab, zum Beispiel: 10.0.3.4, 10.0.3.5.



2. Richten Sie Peering mit einer virtuellen Netzwerkanwendung (NVA) im Azure-Portal ein. Fügen Sie Ihre NetScaler VPX-Instanz als NVA hinzu. Weitere Informationen finden Sie unter Einrichten von Peering mit NVA.

   Im folgenden Beispiel werden das ADC-SNIP auf 1/1-Schnittstellen 10.0.1.4 und 10.0.1.5 und die ASN: 400 und 500 beim Hinzufügen des Peers verwendet.



3. Fügen Sie zwei NetScaler VPX-Instanzen für die HA-Konfiguration hinzu.

Führen Sie hierzu die folgenden Schritte aus:

a) Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) in Azure bereit.
b) Fügen Sie auf beiden Instanzen eine Client- und Server-Netzwerkkarte hinzu.
c) Konfigurieren Sie HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI.

4. Konfigurieren Sie das dynamische Routing in der primären ADC-Instanz.

   Beispielkonfiguration:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -
   dynamicRouting ENABLED
VTYSH
configure terminal
router BGP 400
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
```

5. Konfigurieren Sie das dynamische Routing in der sekundären ADC-Instanz.

   Beispielkonfiguration:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -
   dynamicRouting ENABLED
VTYSH
configure terminal
router BGP 500
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
```

6. Überprüfen Sie die BGP-Peers, die mithilfe der BGP-Befehle in der VTY-Shell-Schnittstelle eingerichtet wurden. Weitere Informationen finden Sie unter Überprüfen der BGP-Konfiguration.


```
show ip bgp neighbors
```

7. Konfigurieren Sie den virtuellen LB-Server in der primären ADC-Instanz.

   Beispielkonfiguration:

```
add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute
   ENABLED
add lbvserver v1 HTTP 172.16.1.1 80
add service s1 10.0.2.6 HTTP 80
bind lbvserver v1 s1
enable ns feature lb
```

   Ein Client im selben virtuellen Netzwerk wie die NetScaler VPX-Instanz kann jetzt auf den virtuellen LB-Server zugreifen. In diesem Fall kündigt die NetScaler VPX-Instanz die VIP-Route an den Azure-Routenserver an.

Back-End-Azure-Autoscaling-Dienst hinzufügen

October 17, 2024

Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen hochskalieren. Unabhängig davon, ob die Nachfrage nachlässt, müssen Sie herunterfahren, um die unnötigen Kosten ungenutzter Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

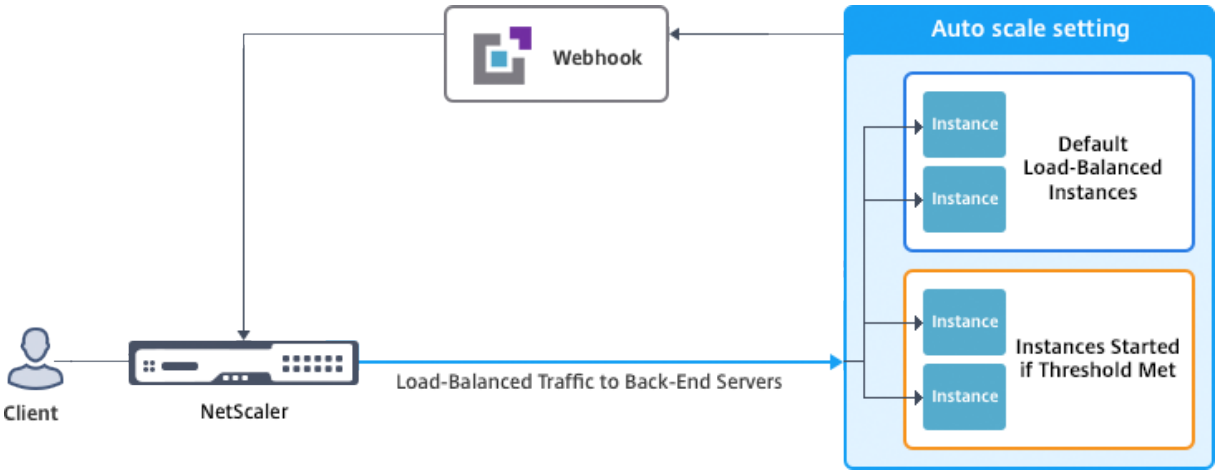
Sie können Autoscale mit Azure VM Scale Sets (VMSS) für die eigenständige VPX Multi-IP-Bereitstellung und Hochverfügbarkeitsbereitstellung auf Azure verwenden.

Die NetScaler VPX-Instanz ist in die Azure VMSS- und Autoscale-Funktion integriert und bietet die folgenden Vorteile:

- Lastverteilung und Verwaltung: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die NetScaler VPX-Instanz erkennt automatisch die Einstellung VMSS Autoscale in demselben virtuellen Netzwerk, in dem die VPX-Instanz bereitgestellt wird, oder in den virtuellen Peered-Netzwerken, die sich im selben Azure-Abonnement befinden. Sie können die Einstellung VMSS Autoscale auswählen, um die Last auszugleichen.

Dies geschieht durch die automatische Konfiguration der virtuellen NetScaler-IP-Adresse und Subnetz-IP-Adresse auf der VPX-Instanz.

- Hochverfügbarkeit: Erkennt Autoscale-Gruppen und gleicht Server aus.
- Bessere Netzwerkverfügbarkeit: Die VPX-Instanz unterstützt Back-End-Server in verschiedenen virtuellen Netzwerken (VNETs).



Weitere Informationen finden Sie im folgenden Azure-Thema

- Dokumentation zu Skalierungssätzen für virtuelle Maschinen
- Überblick über Autoscale in virtuellen Maschinen, Cloud-Diensten und Web-Apps von Microsoft Azure

Voraussetzungen

- Lesen Sie die Azure-bezogenen Nutzungsrichtlinien. Weitere Informationen finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure.
- Erstellen Sie je nach Anforderung eine oder mehrere NetScaler VPX -Instanzen mit drei Netzwerkschnittstellen in Azure (eigenständige oder hochverfügbare Bereitstellung).
- Öffnen Sie den TCP 9001-Port in der Netzwerksicherheitsgruppe der 0/1-Schnittstelle der VPX-Instanz. Die VPX-Instanz verwendet diesen Port, um die Scale-Out- und Scale-In-Benachrichtigung zu empfangen.
- Erstellen Sie eine Azure-VMSS im selben virtuellen Netzwerk, in dem die NetScaler VPX-Instanz bereitgestellt wird. Wenn die VMSS- und NetScaler VPX-Instanz in verschiedenen virtuellen Azure-Netzwerken bereitgestellt werden, müssen die folgenden Bedingungen erfüllt sein:
  - Beide virtuellen Netzwerke müssen im selben Azure-Abonnement enthalten sein.
  - Die beiden virtuellen Netzwerke müssen mithilfe der Peering-Funktion für virtuelle Netzwerke von Azure verbunden werden.

Wenn Sie keine vorhandene VMSS-Konfiguration haben, führen Sie die folgenden Aufgaben aus:

a) Erstellen eines VMSS

b) Autoscale auf VMSS aktivieren

c) Erstellen Sie Scale-In- und Scale-Out-Richtlinien in der VMSS-Autoscale-Einstellung

Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.

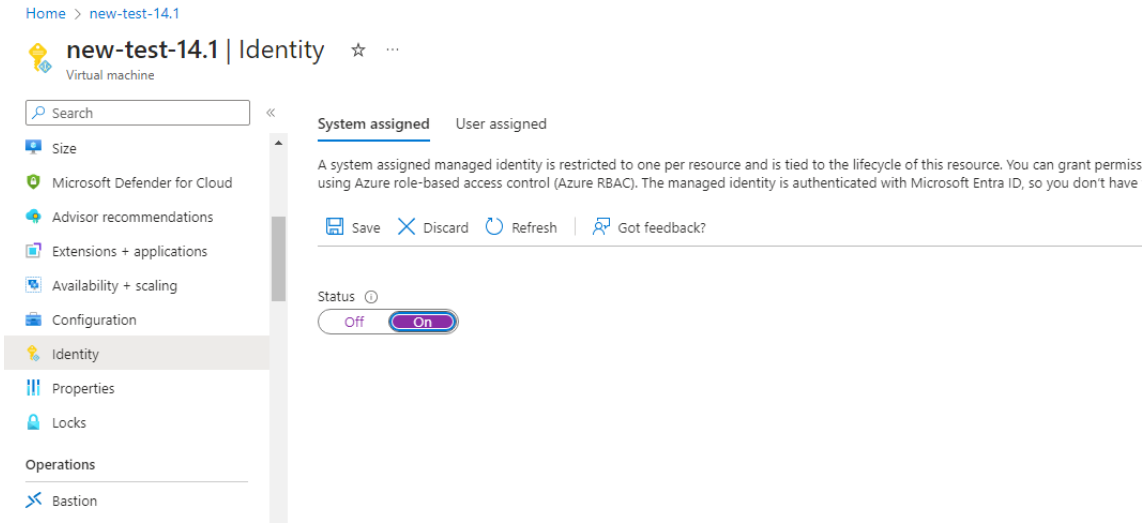
- NetScaler VPX unterstützt VMSS nur mit einheitlicher Orchestrierung. VMSS mit flexibler Orchestrierung wird nicht unterstützt. Weitere Informationen finden Sie unter Orchestrierungsmodi für Virtual Machine Scale Sets in Azure.
- Ab NetScaler Version 14.1-12.x unterstützt NetScaler VPX verwaltete Identitäten in der Azure-Cloud. Verwaltete Identitäten verknüpfen einen Service Principal mit einer Azure-Ressource wie einer virtuellen Maschine. Mit verwalteter Identität müssen Sie die Cloud-Anmeldeinformationen (Anwendungs-ID, Anwendungsgeheimnis und Mandanten-ID) nicht verwalten, wodurch Sicherheitsrisiken vermieden werden. Derzeit unterstützt NetScaler VPX nur die vom System zugewiesene und eine einem einzelnen Benutzer zugewiesene verwaltete Identität. Mehreren Benutzern zugewiesene verwaltete Identität wird nicht unterstützt.

  Für NetScaler-Versionen vor 14.1-12.x müssen Sie die Cloud-Anmeldeinformationen in NetScaler VPX manuell über Azure Active Directory (AAD) verwalten. Weisen Sie der neu erstellten AAD-Anwendung eine Mitwirkende Rolle zu. Die Cloud-Anmeldeinformationen müssen nach Ablauf regelmäßig neu erstellt werden. Weitere Informationen finden Sie unter Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipalers.

  Wenn Sie verwaltete Identität auf der Azure-Konsole und Cloud-Anmeldeinformationen in NetScaler konfigurieren, hat verwaltete Identität Vorrang vor Cloud-Anmeldeinformationen.

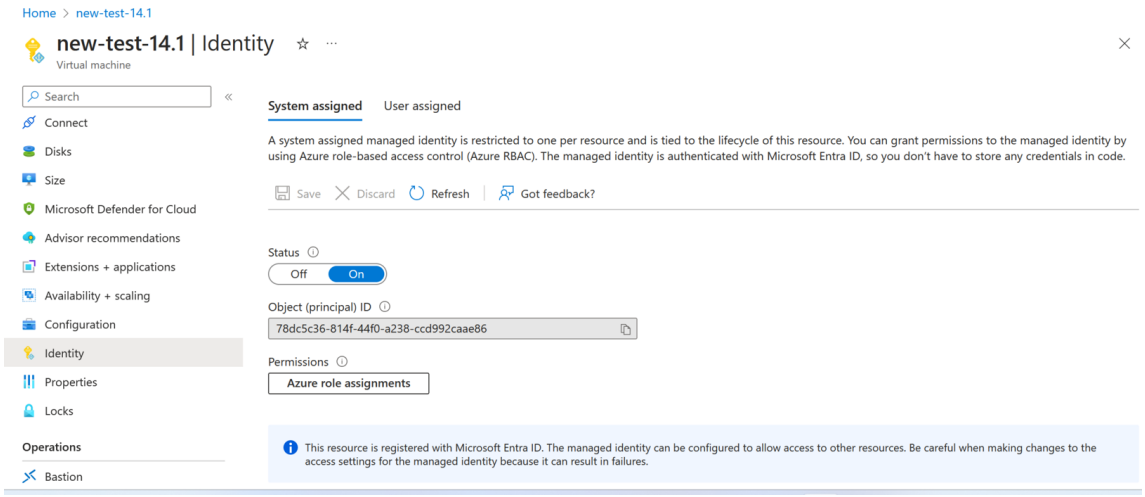
Eine verwaltete Identität auf einer virtuellen Maschine konfigurieren

1. Melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu Ihrer virtuellen Maschine und wählen Sie **Identität**aus.
3. Wählen Sie je nach Ihren Anforderungen entweder „ **System zugewiesen**“**oder „Benutzer zugewiesen**“.
4. Wählen Sie unter **Status**die Option **An** aus und klicken Sie dann auf **Speichern**.



Sobald der Status gespeichert ist, sehen Sie, dass ein Dienstprinzipalobjekt erstellt und der VM zugewiesen wird.

5. Klicken Sie auf **Azure-Rollenzuweisungen**.



6. Wählen **Sie im Fenster Rollenzuweisung hinzufügen** einen Bereich aus. Sie können aus den folgenden Optionen wählen:

   - Abonnement

     Wenn sich VMSS und VM in unterschiedlichen Ressourcengruppen befinden, verwenden Sie **Abonnement** als Bereich.

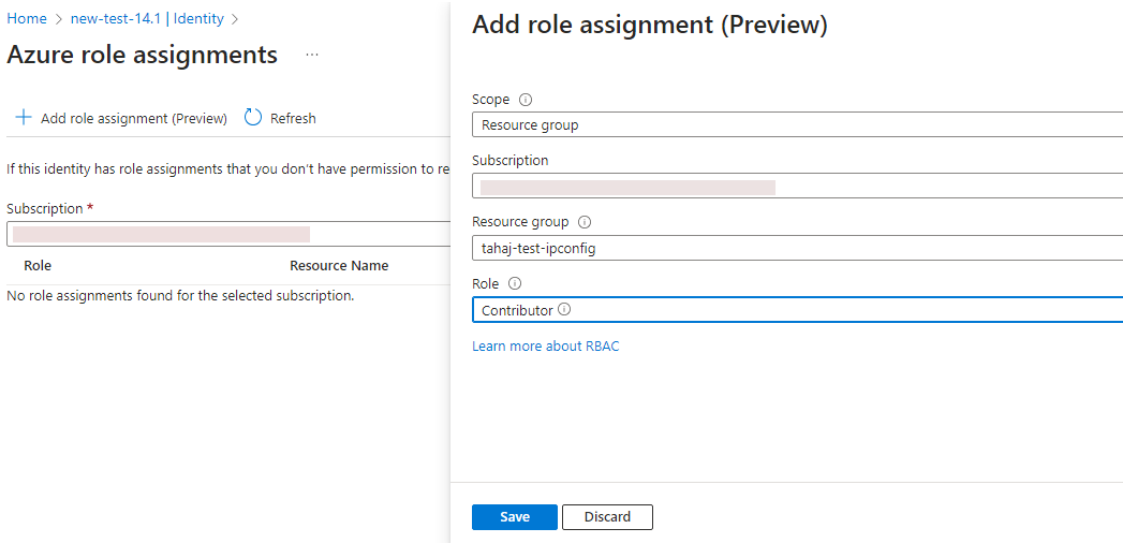
   - Ressourcengruppe

     Wenn sich die VMSS in derselben Ressourcengruppe wie Ihre VM befindet, verwenden Sie die **Ressourcengruppe** als Bereich.

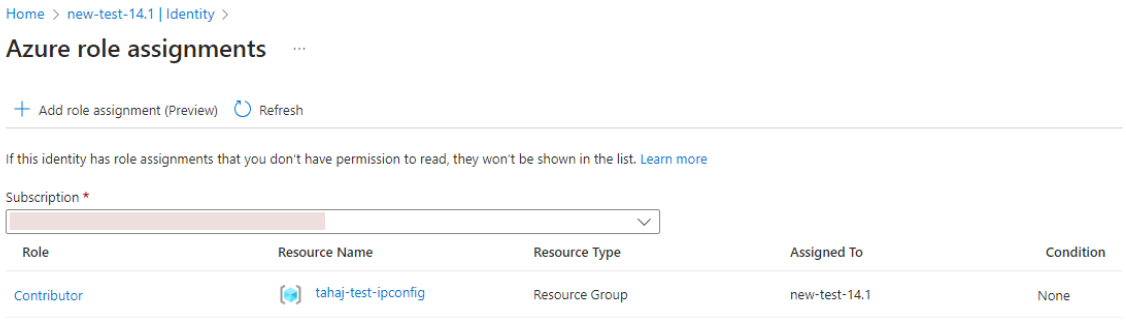
   - Schlüssel-Tresor

- Speicher
- SQL

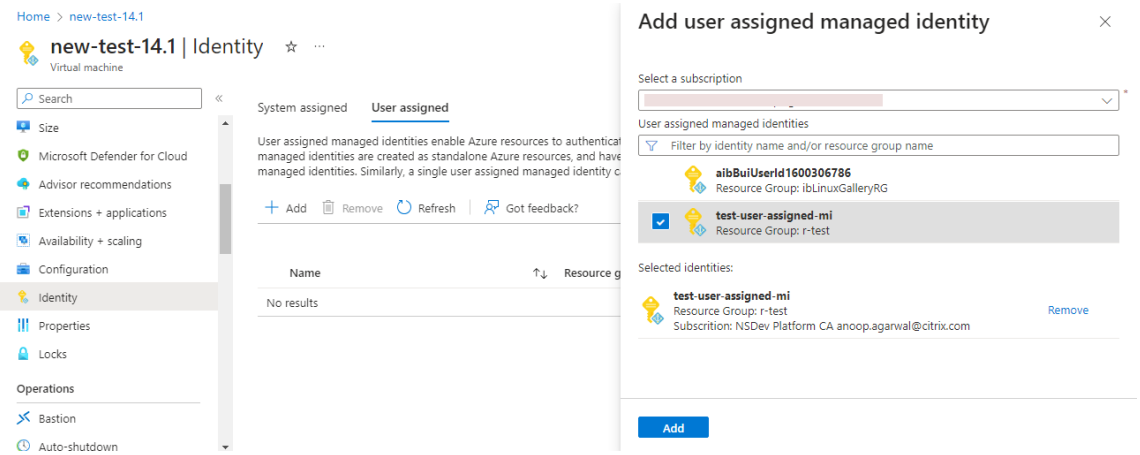
Füllen Sie auf der Grundlage Ihrer Bereichsauswahl die Details für andere Felder aus. Weisen Sie eine **Mitwirkendenrolle** zu und **speichern Sie** die Konfiguration.



Auf der Seite mit den **Azure-Rollenzuweisungen** wird die verwaltete Identität angezeigt, die Sie erstellt haben.



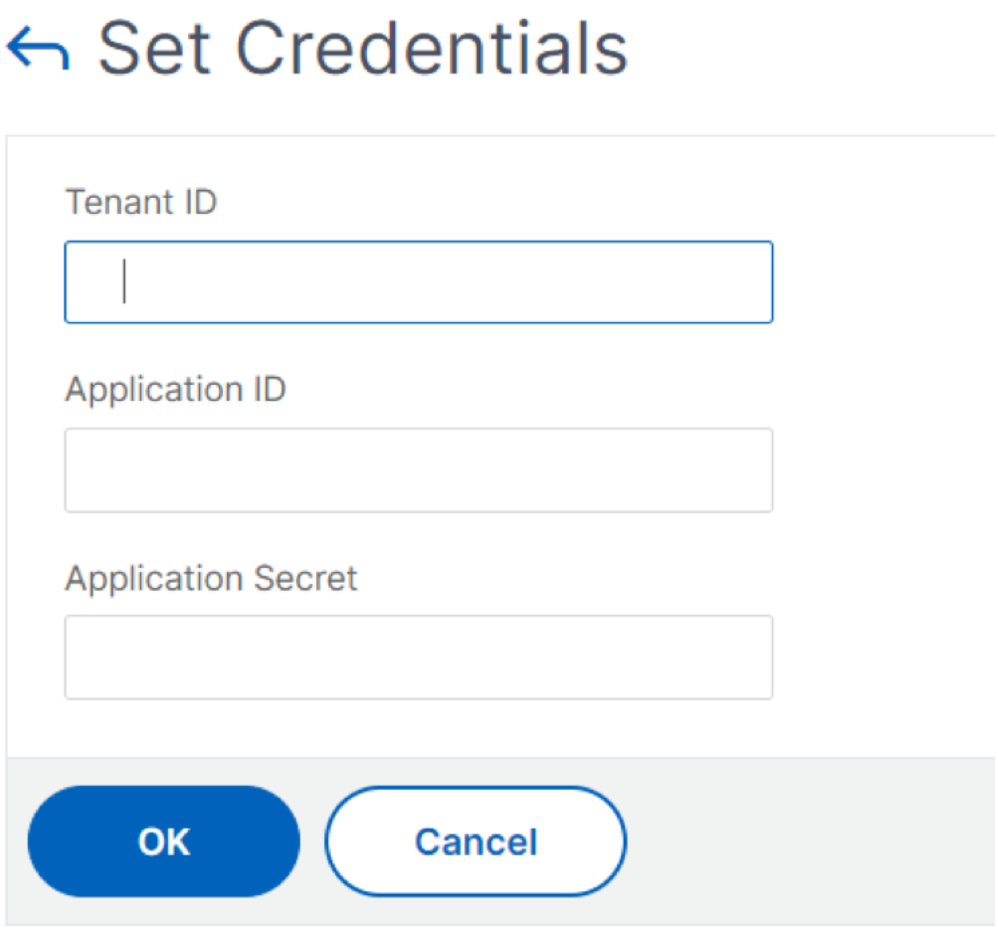
7. Um eine vom Benutzer zugewiesene verwaltete Identität zu erstellen, wählen Sie ein Abonnement aus, wählen Sie eine vom Benutzer zugewiesene verwaltete Identität aus und klicken Sie auf **Hinzufügen**.



Hinzufügen von VMSS zu einer NetScaler VPX-Instanz

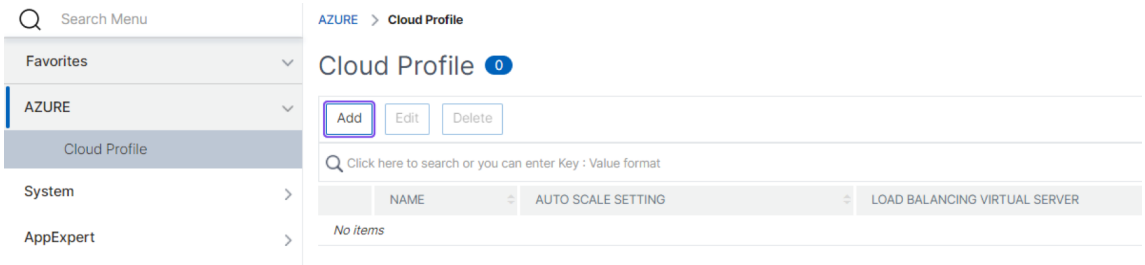
Gehen Sie wie folgt vor, um der VPX-Instanz die Autoscale-Einstellung hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an.
2. Navigieren Sie zu **Konfiguration > Azure > Anmeldeinformationen festlegen**. Fügen Sie die erforderlichen Azure-Anmeldeinformationen hinzu, damit die Autoscale-Funktion funktioniert.

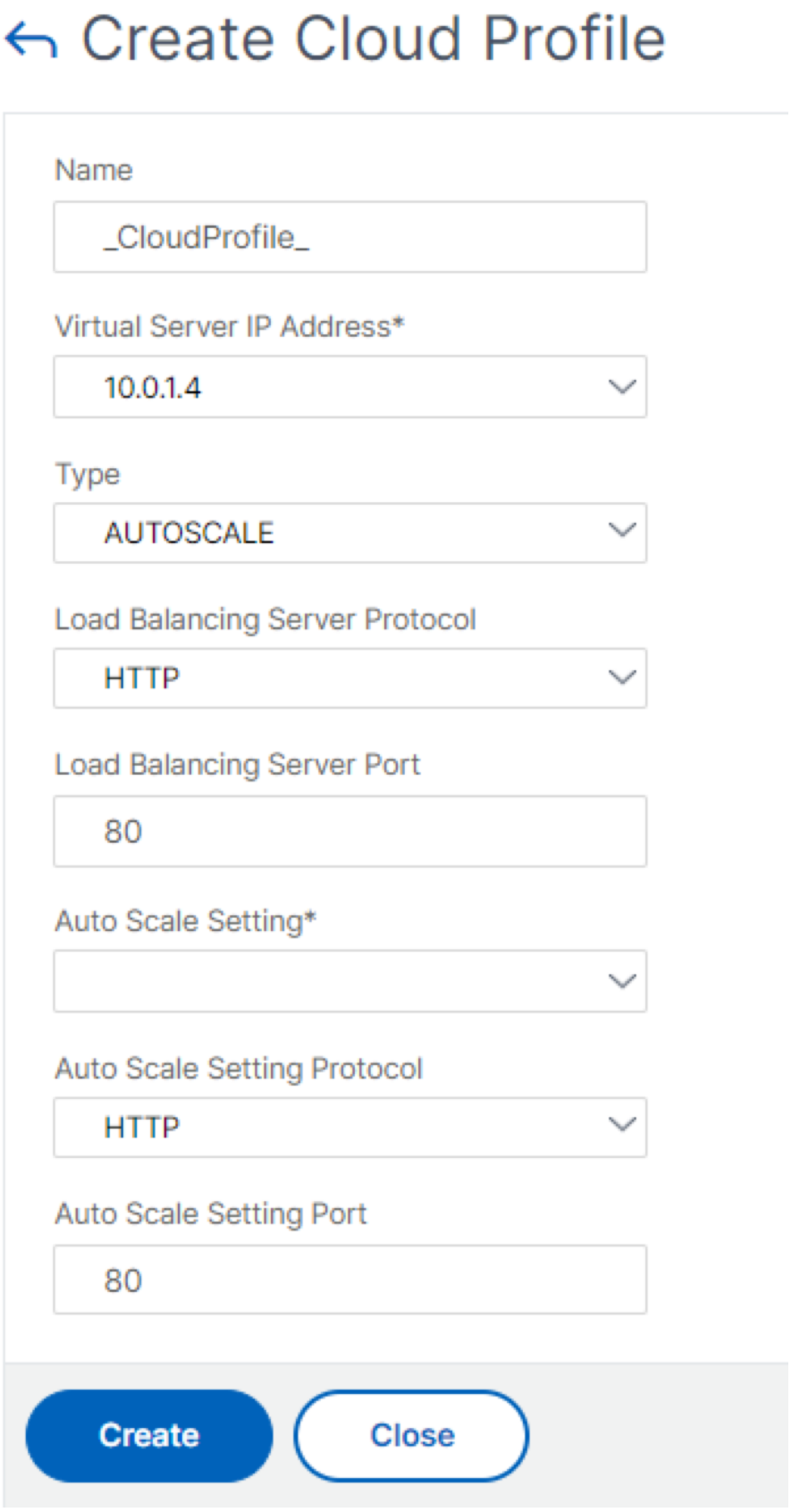


> **Hinweis:**
>
> Wenn Sie Azure Managed Identity verwenden, müssen Sie keine Anmeldeinformationen festlegen.

3. Gehen Sie zu **System > Azure > Cloud-Profil** und klicken Sie auf **Hinzufügen**, um ein Cloud-Profil zu erstellen.



Die Konfigurationsseite „ **Cloud-Profil erstellen** “wird angezeigt.



Das Cloud-Profil erstellt einen virtuellen NetScaler-Load-Balancing-Server und eine Dienstgruppe mit Mitgliedern (Servern) als Server der Auto Scaling Group. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

Punkte, die beim Erstellen eines Cloud-Profils berücksichtigt werden müssen

- Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
- Die Autoscale-Einstellung wird von der VMSS-Instanz, die entweder im selben virtuellen Netzwerk oder in virtuellen Peering-Netzwerken mit der NetScaler VPX-Instanz verbunden ist, vorab ausgefüllt. Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.
- Stellen Sie bei der Auswahl des **Auto Scale Setting Protocol** und des **Auto Scale Setting Port**sicher, dass Ihre Server die Protokolle und Ports überwachen und dass Sie den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Bei Autoscaling vom Typ SSL-Protokoll ist der virtuelle Load Balancing-Server oder die Servicegruppe nach dem Erstellen des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

> **Hinweis:**
>
> Ab NetScaler Version 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung verschiedener Ports) mit demselben VMSS in Azure erstellen. Daher unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

Um Informationen zur automatischen Skalierung im Azure-Portal anzuzeigen, wechseln Sie zu **Skalierungssätze für virtuelle Maschinen** und wählen Sie **Skalierungssatzfür virtuelle Maschinen** > **Skalierung** aus.

Referenzen

Informationen zur automatischen Skalierung von NetScaler VPX in Microsoft Azure mithilfe von NetScaler Application Delivery and Management finden Sie unter Azure Autoscale mithilfe von NetScaler ADM.

Azure-Tags für NetScaler VPX Bereitstellung

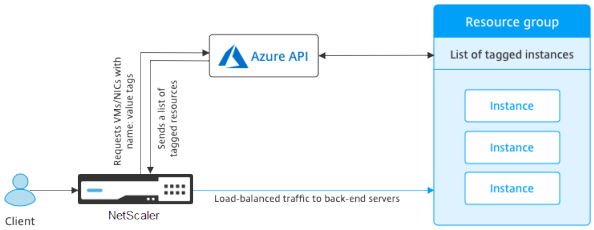
October 17, 2024

Im Azure-Cloud-Portal können Sie Ressourcen mit einem Namen: Wertepaar (wie Abt: Finance) kennzeichnen, um Ressourcen zwischen Ressourcengruppen und innerhalb des Portals über Abonnements hinweg zu kategorisieren und anzuzeigen. Tagging ist hilfreich, wenn Sie Ressourcen für die Abrechnung, Verwaltung oder Automatisierung organisieren müssen.

So funktioniert das Azure-Tag für die VPX-Bereitstellung

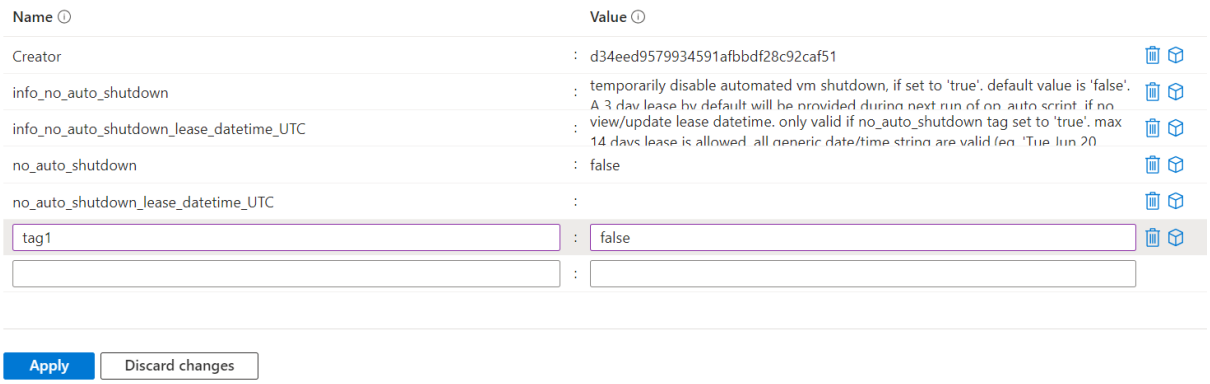
Für eigenständige NetScaler VPX-Instanzen und Hochverfügbarkeitsinstanzen, die in Azure Cloud bereitgestellt werden, können Sie jetzt Lastausgleichsdienstgruppen erstellen, die einem Azure-Tag zugeordnet sind. Die VPX-Instanz überwacht ständig virtuelle Azure-Computer (Back-End-Server) und Netzwerkschnittstellen (NICs) oder beides mit dem entsprechenden Tag und aktualisiert die Servicegruppe entsprechend.

Die VPX-Instanz erstellt die Dienstgruppe, die die Back-End-Server mit Tags ausgleicht. Die Instanz fragt die Azure-API nach allen Ressourcen ab, die mit einem bestimmten Tagnamen und Tag-Wert gekennzeichnet sind. Abhängig vom zugewiesenen Abfragezeitraum (standardmäßig 60 Sekunden) fragt die VPX-Instanz regelmäßig die Azure-API ab und ruft die verfügbaren Ressourcen mit dem in der VPX-GUI zugewiesenen Tag-Namen und den Tag-Werten ab. Immer wenn eine VM oder NIC mit dem entsprechenden Tag hinzugefügt oder gelöscht wird, erkennt der ADC die entsprechende Änderung und fügt die VM- oder NIC-IP-Adresse automatisch zur Dienstgruppe hinzu oder löscht sie aus der Dienstgruppe.



Voraussetzungen

Bevor Sie NetScaler Load Balancing-Dienstgruppen erstellen, fügen Sie den Servern in Azure ein Tag hinzu. Sie können das Tag entweder der virtuellen Maschine oder der Netzwerkkarte zuweisen.



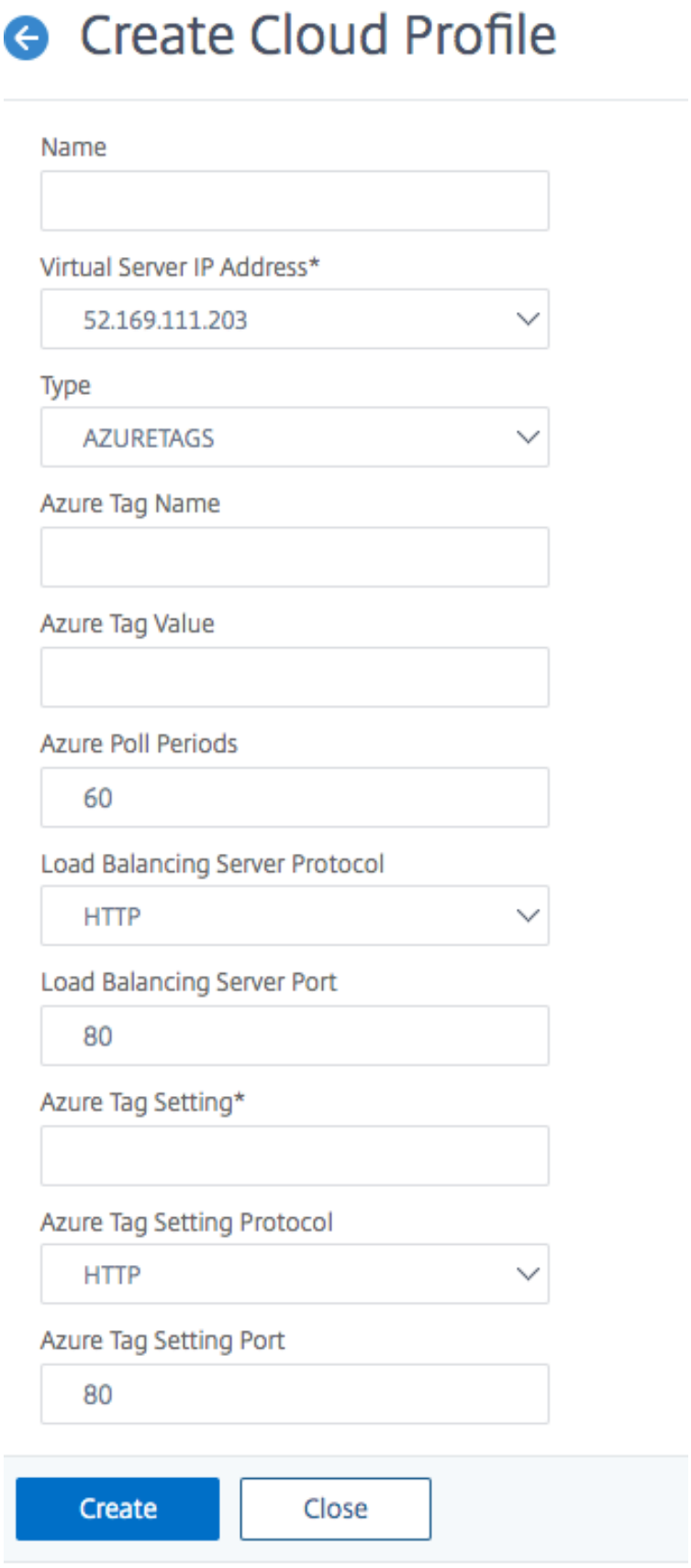
Weitere Informationen zum Hinzufügen von Azure-Tags finden Sie unter Microsoft-Dokument Verwenden Sie Tags zum Organisieren Ihrer Azure-Ressourcen.

> **Hinweis:**
>
> ADC-CLI-Befehle zum Hinzufügen von Azure-Tageinstellungen unterstützen Tag-Namen und Tag-Werte, die nur mit Ziffern oder Buchstaben und nicht mit anderen Tastaturzeichen beginnen.

So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX-GUI hinzu

Sie können das Azure-Tag-Cloud-Profil zu einer VPX-Instanz hinzufügen, indem Sie die VPX-GUI verwenden, sodass die Instanz die Back-End-Server mithilfe des angegebenen Tags ausgleichen kann. Führen Sie folgende Schritte aus:

1. Gehen Sie in der VPX-GUI zu **Konfiguration > Azure > Cloud-Profil**.
2. Klicken Sie auf Hinzufügen, um ein Cloud-Profil zu erstellen. Das Cloud-Profilfenster wird geöffnet.



1. Geben Sie Werte für die folgenden Felder ein:

   - Name: Füge einen Namen für dein Profil hinzu
   - IP-Adresse des virtuellen Servers: Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
   - Typ: Wählen Sie im Menü AZURETAGS.
   - Azure-Tag-Name: Geben Sie den Namen ein, den Sie den VMs oder NICs im Azure-Portal zugewiesen haben.
   - Azure-Tag-Wert: Geben Sie den Wert ein, den Sie den VMs oder Netzwerkkarten im Azure-Portal zugewiesen haben.
   - Azure-Abfragezeiträume: Standardmäßig beträgt der Abfragezeitraum 60 Sekunden, was dem Mindestwert entspricht. Sie können es entsprechend Ihren Anforderungen ändern.
   - Load Balancing Server Protocol: Wählen Sie das Protokoll aus, das Ihr Load Balancer überwacht.
   - Load Balancing-Server-Port: Wählen Sie den Port aus, auf dem Ihr Load Balancer lauscht.
   - Azure-Tag-Einstellung: Der Name der Dienstgruppe, die für dieses Cloud-Profil erstellt wird.
   - Azure Tag Setting Protocol: Wählen Sie das Protokoll aus, das Ihre Backend-Server abhören.
   - Azure Tag Setting Port: Wählen Sie den Port aus, den Ihre Back-End-Server abhören.

2. Klicken Sie auf **Erstellen**.

Ein virtueller Load-Balancer-Server und eine Dienstgruppe werden für die markierten VMs oder NICs erstellt. Um den virtuellen Load Balancer-Server zu sehen, navigieren Sie in der VPX-GUI zu **Traffic Management > Load Balancing > Virtual**Servers.

So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX CLI hinzu

Geben Sie den folgenden Befehl in der NetScaler CLI ein, um ein Cloud-Profil für Azure-Tags zu erstellen.

```
add cloud profile `<profile name>` -type azuretags -vServerName `<
   vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>`
    -port 80 -serviceGroupName `<service group name>` -
   boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
   Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
```


> **Wichtig:**
>
> Sie müssen alle Konfigurationen speichern, da die Konfigurationen andernfalls nach dem Neustart der Instanz verloren gehen. Geben Sie `save config` ein.

Beispiel 1: Hier ist ein Beispielbefehl für ein Cloud-Profil für den HTTP-Verkehr aller Azure-VMs/NICs, die mit dem Paar „myTagName/myTagValue“gekennzeichnet sind:

```
1   add cloud profile MyTagCloudProfile -type azuretags -vServerName
       MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
       serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
        -vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue
       myTagValue -azurePollPeriod 60
2   Done
```

Um das Cloud-Profil anzuzeigen, geben Sie ein `show cloudprofile`.

Beispiel 2: Der folgende CLI-Befehl druckt Informationen über das neu hinzugefügte Cloud-Profil in Beispiel 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
```

Um ein Cloud-Profil zu entfernen, geben Sie rm Cloud-Profil ein &`lt;cloud profile name>`

Beispiel 3: Mit dem folgenden Befehl wird das in Beispiel 1 erstellte Cloud-Profil entfernt.

```
1   > rm cloudprofile MyTagCloudProfile
2     Done
```

Problembehandlung

Problem: In sehr seltenen Fällen kann der CLI-Befehl “rm cloud profile”die Dienstgruppe und Server, die mit dem gelöschten Cloud-Profil verknüpft sind, möglicherweise nicht entfernen. Dies geschieht, wenn der Befehl Sekunden vor Ablauf des Abfragezeitraums des gelöschten Cloud-Profils ausgegeben wird.

Lösung: Löschen Sie die verbleibenden Dienstgruppen manuell, indem Sie den folgenden CLI-Befehl für jede der verbleibenden Dienstgruppen eingeben:

```
1   #> rm servicegroup <serviceGroupName>
```


Entfernen Sie auch jeden der verbleibenden Server, indem Sie den folgenden CLI-Befehl für jeden der verbleibenden Server eingeben:

```
#> rm server <name>
```

Problem: Wenn Sie einer VPX-Instanz über die Befehlszeilenschnittstelle eine Azure-Tag-Einstellung hinzufügen, wird der rain_tags-Prozess nach einem Warmneustart weiterhin auf einem HA-Paar-Node ausgeführt.

Lösung: Beenden Sie den Prozess auf dem sekundären Knoten nach einem warmen Neustart manuell. Von der CLI des sekundären HA-Knotens beenden Sie die Shell-Eingabeaufforderung

```
#> shell
```

Verwenden Sie den folgenden Befehl, um den rain_tags-Prozess zu beenden:

```
# PID=`ps -aux | grep rain_tags | awk '{
print $2 }
'`; kill -9 $PID
```

Problem: Back-End-Server sind möglicherweise nicht erreichbar und werden von der VPX-Instanz als DOWN gemeldet, obwohl sie gesund sind. **Lösung**: Stellen Sie sicher, dass die VPX-Instanz die getaggte IP-Adresse erreichen kann, die dem Back-End-Server entspricht. Bei einer getaggten NIC handelt es sich hierbei um die NIC-IP-Adresse. Bei einer getaggten VM handelt es sich dabei um die primäre IP-Adresse der VM. Wenn sich die VM/NIC in einem anderen Azure VNet befindet, stellen Sie sicher, dass VNet-Peering aktiviert ist.

Konfigurieren von GSLB auf NetScaler VPX-Instanzen

October 17, 2024

NetScaler Appliances, die für den Global Server Load Balancing (GSLB) konfiguriert sind, bieten Disaster Recovery und kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Fehlerpunkten in einem WAN schützen. GSLB kann die Last über Rechenzentren hinweg ausgleichen, indem sie Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder an überlebende Rechenzentren bei einem Ausfall weiterleitet.

In diesem Abschnitt wird beschrieben, wie Sie GSLB auf VPX-Instanzen auf zwei Standorten in einer Microsoft Azure-Umgebung mithilfe von Windows PowerShell Befehlen aktivieren.

> **Hinweis:**
>
> Weitere Informationen zu GSLB finden Sie unter Globaler Server-Lastenausgleich.

Sie können GSLB für eine NetScaler VPX-Instanz in Azure in zwei Schritten konfigurieren:

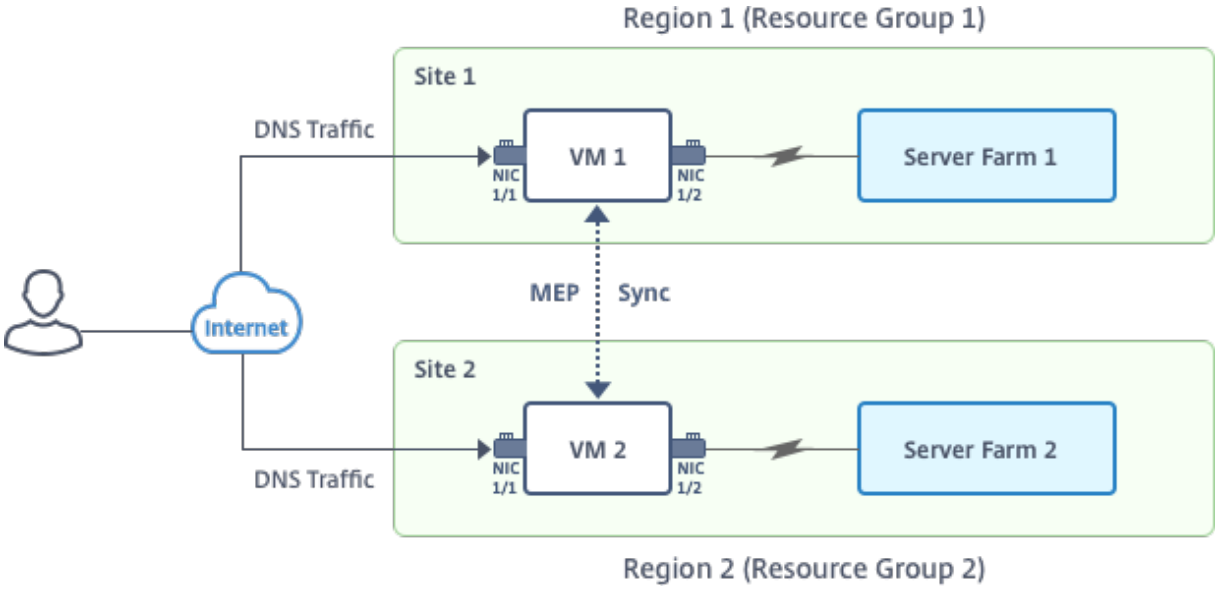
1. Erstellen Sie auf jeder Site eine VPX-Instanz mit mehreren Netzwerkkarten und mehreren IP-Adressen.
2. Aktivieren Sie GSLB für die VPX-Instanzen.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren mehrerer Netzwerkkarten und IP-Adressen finden Sie unter: Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen

Szenario

Dieses Szenario umfasst zwei Standorte —Standort 1 und Standort 2. Jeder Standort verfügt über eine VM (VM1 und VM2), die mit mehreren NICs, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung. GSLB-Setup an zwei Standorten implementiert –Standort 1 und Standort 2.



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Jede NIC kann mehrere private und öffentliche IP-Adressen haben. Die Netzwerkkarten sind für die folgenden Zwecke konfiguriert.

- NIC 0/1: zur Bedienung des Management-Datenverkehrs
- NIC 1/1: zur Bedienung des clientseitigen Datenverkehrs
- NIC 1/2: Kommunikation mit Back-End-Servern

Informationen zu den IP-Adressen, die in diesem Szenario auf jeder Netzwerkkarte konfiguriert sind, finden Sie im Abschnitt Details zur IP-Konfiguration .

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für dieses Szenario in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard\_DS3\_V2"
```

> **Hinweis:**
>
> Die Mindestanforderung für eine VPX-Instanz sind 2 vCPUs und 2 GB RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"
```



```
32
33    $IPConfigName4="IPConfig-4"
34
35    $frontendSubnetName="default"
36
37    $backendSubnetName1="subnet\_1"
38
39    $backendSubnetName2="subnet\_2"
40
41    $suffixNumber=10
```

Erstellen einer virtuellen Maschine

Führen Sie die Schritte 1 bis 10 aus, um VM1 mit mehreren Netzwerkkarten und mehreren IP-Adressen zu erstellen, indem Sie PowerShell-Befehle verwenden:

1. Ressourcengruppe erstellen
2. Erstellen eines Speicherkontos
3. Verfügbarkeitssatz erstellen
4. Virtuelles Netzwerk erstellen
5. Öffentliche IP-Adresse erstellen
6. NICs erstellen
7. VM-Konfigurationsobjekt erstellen
8. Anmeldeinformationen abrufen und Betriebssystemeigenschaften für die VM festlegen
9. Netzwerkkarten hinzufügen
10. Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

Nachdem Sie alle Schritte und Befehle zum Erstellen von VM1 abgeschlossen haben, wiederholen Sie diese Schritte, um VM2 mit spezifischen Parametern zu erstellen.

Ressourcengruppe erstellen

```
1    New-AzureRMResourceGroup -Name $RGName -Location $location
```

Erstellen eines Speicherkontos

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


Verfügbarkeitssatz erstellen

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

Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix "10.0.0.0/24"
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix "10.0.1.0/24"
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
```

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.

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

3. Rufen Sie Subnetze ab.

```
$frontendSubnet=$vnet.Subnets|?{
$_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName2 }
```

Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
```

NICs erstellen

NIC 0/1 erstellen

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$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
```

NIC 1/1 erstellen

```
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
```

NIC 1/2 erstellen

```
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
```

VM-Konfigurationsobjekt erstellen

```
1   $vmName=$vmNamePrefix
2   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avSet.Id
```

Anmeldeinformationen abrufen und Betriebssystemeigenschaften festlegen

```
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
```

Netzwerkkarten hinzufügen


```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
```

Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
    /" +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
     $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
     -Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
```

> **Hinweis:**
>
> Wiederholen Sie die Schritte 1 bis 10, die unter “Erstellen von VMs mit PowerShell-Befehlen erstellen”aufgeführt sind, um VM2 mit Parametern zu erstellen, die für VM2 spezifisch sind.

IP-Konfigurationsdetails

Die folgenden IP-Adressen werden verwendet.

Tabelle 1. In VM1 verwendete IP-Adressen In VM1 verwendete IP-Adressen

Netzwerkkarte	Private IP	Öffentliche IP (PIP)	Beschreibung
0/1	10.0.0.10	PIP1	Als NSIP (Management-IP) konfiguriert
1/1	10.0.1.10	PIP2	Als SNIP/GSLB Site IP konfiguriert
-	10.0.1.11	-	Als LB-Server-IP konfiguriert. Öffentliche IP ist nicht verpflichtend

Netzwerkkarte	Private IP	Öffentliche IP (PIP)	Beschreibung
1/2	10.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Tabelle 2. In VM2 verwendete IP-Adressen

Netzwerkkarte	Interne IP	Öffentliche IP (PIP)	Beschreibung
0/1	20.0.0.10	PIP4	Als NSIP (Management-IP) konfiguriert
1/1	20.0.1.10	PIP5	Als SNIP/GSLB Site IP konfiguriert
-	20.0.1.11	-	Als LB-Server-IP konfiguriert. Öffentliche IP ist nicht verpflichtend
1/2	20.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Hier finden Sie Beispielkonfigurationen für dieses Szenario, die die IP-Adressen und anfänglichen LB-Konfigurationen zeigen, die über die NetScaler VPX CLI für VM1 und VM2 erstellt wurden.

Hier ist eine Beispielkonfiguration auf 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]
```

Hier ist eine Beispielkonfiguration auf VM2.

```
1   add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
```



```
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
```

Konfigurieren von GSLB-Sites und anderen Einstellungen

Führen Sie die im folgenden Thema beschriebenen Aufgaben aus, um die beiden GSLB-Sites und andere erforderliche Einstellungen zu konfigurieren:

Globaler Serverlastausgleich

Hier ist ein Beispiel für eine GSLB-Konfiguration auf VM1 und VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
   PIP3 -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP
   PIP6 -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Sie haben GSLB auf NetScaler VPX-Instanzen konfiguriert, die in Azure ausgeführt werden.

Notfallwiederherstellung

Katastrophe ist eine plötzliche Störung der Geschäftsfunktionen, die durch Naturkatastrophen oder durch Menschen verursachte Ereignisse verursacht werden. Katastrophen wirken sich auf den Betrieb des Rechenzentrums aus. Danach müssen die am Katastrophenort verlorenen Ressourcen und Daten vollständig neu aufgebaut und wiederhergestellt werden. Der Verlust von Daten oder Ausfallzeiten im Rechenzentrum ist entscheidend und reduziert die Business Continuity.

Eine der Herausforderungen, vor denen Kunden heute stehen, besteht darin, zu entscheiden, wo sie ihren DR-Standort platzieren möchten. Unternehmen suchen nach Konsistenz und Leistung, unabhängig von zugrunde liegenden Infrastruktur- oder Netzwerkfehlern.

Mögliche Gründe, warum sich viele Unternehmen für eine Migration in die Cloud entscheiden, sind:

- Ein Rechenzentrum vor Ort ist sehr teuer. Durch die Nutzung der Cloud können die Unternehmen Zeit und Ressourcen für die Erweiterung ihrer eigenen Systeme sparen.

- Viele der automatisierten Orchestrierungen ermöglichen eine schnellere Wiederherstellung
- Replizieren Sie Daten, indem Sie kontinuierlichen Datenschutz oder kontinuierliche Snapshots bereitstellen, um sich vor Ausfällen oder Angriffen zu schützen.
- Unterstützen Sie Anwendungsfälle, in denen Kunden viele verschiedene Arten von Compliance- und Sicherheitskontrollen benötigen, die bereits in den Public Clouds vorhanden sind. Diese machen es einfacher, die von ihnen benötigte Compliance zu erreichen, als ihre eigenen zu erstellen.

Ein für GSLB konfigurierter NetScaler leitet den Datenverkehr an das am wenigsten ausgelastete oder leistungsstärkste Rechenzentrum weiter. Diese Konfiguration, die als aktiv-aktives Setup bezeichnet wird, verbessert nicht nur die Leistung, sondern bietet auch eine sofortige Notfallwiederherstellung, indem Datenverkehr an andere Rechenzentren weitergeleitet wird, wenn ein Rechenzentrum, das Teil des Setups ist, ausfällt. NetScaler spart Kunden dadurch wertvolle Zeit und Geld.

Bereitstellung mehrerer Netzwerkkarten (drei Netzwerkkarten) für die Notfallwiederherstellung

Kunden würden möglicherweise eine Bereitstellung mit drei Netzwerkkarten bereitstellen, wenn sie in einer Produktionsumgebung eingesetzt werden, in der Sicherheit, Redundanz, Verfügbarkeit, Kapazität und Skalierbarkeit entscheidend sind. Bei dieser Bereitstellungsmethode sind Komplexität und einfache Verwaltung für die Benutzer kein kritisches Problem.

Multi-IP-Bereitstellung mit einer Netzwerkkarte für die Notfallwiederherstellung

Kunden stellen die Bereitstellung möglicherweise mithilfe einer einzigen Netzwerkkarte bereit, wenn sie die Bereitstellung in einer Umgebung außerhalb der Produktionsumgebung vornehmen, und zwar aus den folgenden Gründen:

- Sie richten die Umgebung für Tests ein, oder sie stellen eine neue Umgebung vor der Bereitstellung in der Produktion bereit.
- Schnelle und effiziente Bereitstellung direkt in der Cloud.
- Sie sind auf der Suche nach der Einfachheit einer einzelnen Subnetzkonfiguration.

Konfigurieren Sie GSLB in einem aktiven Standby-Hochverfügbarkeits-Setup

October 17, 2024

Sie können den globalen Serverlastenausgleich (GSLB) bei der HA-Bereitstellung im aktiven Standby in Azure in drei Schritten konfigurieren:

1. Erstellen Sie ein VPX HA-Paar auf jeder GSLB-Site. Informationen zum Erstellen eines HA-Paares finden Sie unter Konfigurieren einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und Netzwerkkarten .
2. Konfigurieren Sie den Azure Load Balancer (ALB) mit der Front-End-IP-Adresse und -Regeln, um GSLB- und DNS-Datenverkehr zuzulassen.

   Dieser Schritt beinhaltet die folgenden Teilschritte. Das Szenario in diesem Abschnitt enthält die PowerShell-Befehle, die zum Ausführen dieser Teilschritte verwendet werden.

   a. Erstellen Sie ein Front-End-`IPconfig` für die GSLB-Site.

   b. Erstellen Sie einen Back-End-Adresspool mit der IP-Adresse der NIC 1/1 der Knoten in HA.

   c. Erstellen Sie Lastenausgleichsregeln für Folgendes:

   ```
   TCP/3009 – gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

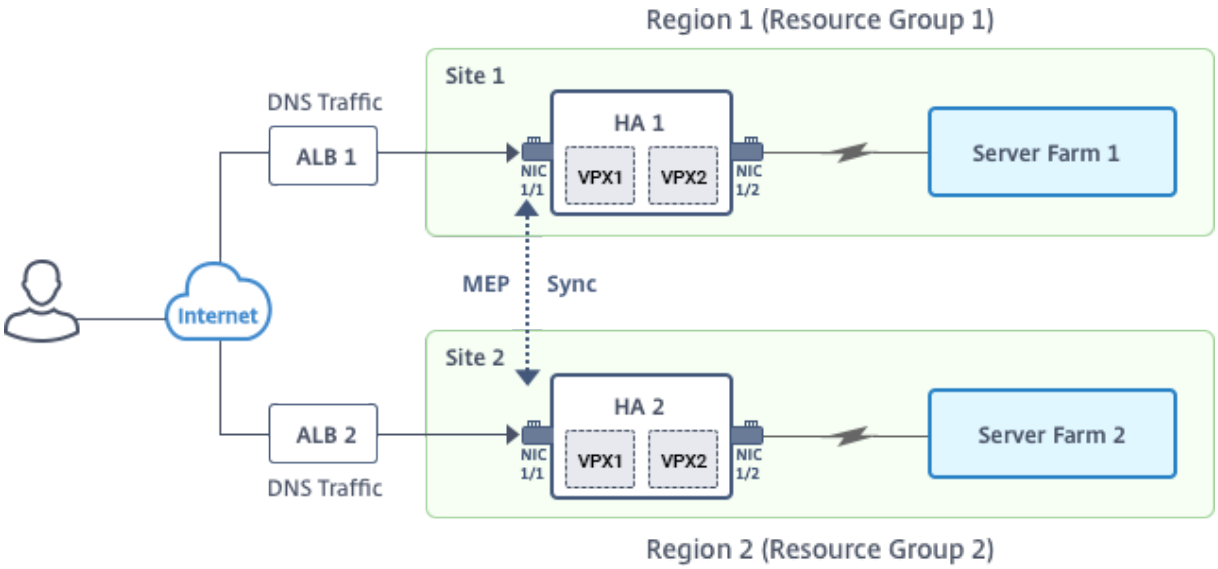
   d. Ordnen Sie den Back-End-Adresspool mit den in Schritt c erstellten LB-Regeln zu.

   e. Aktualisieren Sie die Netzwerksicherheitsgruppe von NIC 1/1 der Knoten in beiden HA-Paaren, um den Datenverkehr für TCP 3008-, TCP 3009- und UDP 53-Ports zuzulassen.
3. Aktivieren Sie GSLB auf jedem HA-Paar.

Szenario

Dieses Szenario umfasst zwei Standorte —Standort 1 und Standort 2. Jeder Standort verfügt über ein HA-Paar (HA1 und HA2), das mit mehreren Netzwerkkarten, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung: GLSB auf Active-Standy HA-Bereitstellung in Azure



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Die Netzwerkkarten sind für die folgenden Zwecke konfiguriert.

NIC 0/1: zur Bedienung des Management-Datenverkehrs

NIC 1/1: zur Bedienung des clientseitigen Datenverkehrs

NIC 1/2: Kommunikation mit Back-End-Servern

Parameter-Einstellungen

Im Folgenden finden Sie Beispielparametereinstellungen für den ALB. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"

$lbRuleName3="LBRuleGSLB2"

$lbRuleName4="LBRuleDNS"
```



```
20
21   $healthProbeName="HealthProbe"
```

Konfiguration von ALB mit der Front-End-IP-Adresse und Regeln, um GSLB- und DNS-Verkehr zuzulassen

Schritt 1. **Erstellen einer öffentlichen IP für GSLB-Site-IP**

```
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
```

Schritt 2. **Erstellen Sie LB-Regeln und aktualisieren Sie die vorhandene ALB**.

```
1   $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName
2
3
4   $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2
5
6
7   $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1
8
9
10  $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName
11
12
13  \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
    BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
14
15
16  \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
    BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
17
18
```



```
\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName4 -
   BackendAddressPool \$backendPool -FrontendIPConfiguration  \
   $frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort
    53 -Probe \$healthprobe -EnableFloatingIP  | Set-
   AzureRmLoadBalancer
```

Aktivieren von GSLB für jedes Hochverfügbarkeitspaar

Jetzt haben Sie zwei Front-End-IP-Adressen für jedes ALB: ALB 1 und ALB 2. Eine IP-Adresse ist für den virtuellen LB-Server und die andere für die GSLB-Site-IP.

HA 1 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB1 (für virtuellen LB-Server)
- PIPFORGSLB1 (GSLB IP)

HA 2 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB2 (für virtuellen LB-Server)
- PIPFORGSLB2 (GSLB IP)

Die folgenden Befehle werden für dieses Szenario verwendet.

```
enable ns feature LB GSLB

add service dnssvc PIPFORGSLB1 ADNS 53

add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1

add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2

add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
   publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
   publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Verwandte Ressourcen:

Konfigurieren von GSLB auf NetScaler VPX-Instanzen

Globaler Serverlastausgleich

NetScaler GSLB auf Azure bereitstellen

October 17, 2024

Angesichts der steigenden Nachfrage möchten Unternehmen, die ein lokales Rechenzentrum für regionale Kunden betreiben, mithilfe der Azure-Cloud weltweit skalieren und bereitstellen. Mit NetScaler auf der Seite des Netzwerkadministrators können Sie das GSLB StyleBook verwenden, um Anwendungen sowohl vor Ort als auch in der Cloud zu konfigurieren. Sie können dieselbe Konfiguration mit NetScaler ADM in die Cloud übertragen. Je nach Nähe zu GSLB können Sie entweder lokale oder Cloud-Ressourcen erreichen. Dies ermöglicht Ihnen ein nahtloses Erlebnis, egal wo Sie sich auf der Welt befinden.

DBS-Übersicht

NetScaler GSLB unterstützt die Verwendung von Domain-Based Services (DBS) für Cloud-Load Balancer. Dies ermöglicht die automatische Erkennung dynamischer Cloud-Dienste mithilfe einer Cloud-Load-Balancer-Lösung. Diese Konfiguration ermöglicht es dem NetScaler, GSLB DBS in einer Active-Active-Umgebung zu implementieren. DBS ermöglicht die Skalierung von Back-End-Ressourcen in Microsoft Azure-Umgebungen ab der DNS-Erkennung. Dieser Abschnitt behandelt die Integration zwischen NetScalers in der Azure Autoscale-Umgebung.

Domänennamenbasierte Dienste mit Azure Load Balancer (ALB)

GLSB DBS verwendet den FQDN des ALB des Benutzers, um die GSLB-Dienstgruppen dynamisch zu aktualisieren, sodass sie die Backend-Server einschließen, die in Azure erstellt und gelöscht werden. Um diese Funktion zu konfigurieren, verweist der Benutzer den Citrix ADC auf seinen ALB, um ihn dynamisch an verschiedene Server in Azure weiterzuleiten. Sie können dies tun, ohne den Citrix ADC jedes Mal manuell aktualisieren zu müssen, wenn eine Instanz in Azure erstellt und gelöscht wird. Die Citrix ADC DBS-Funktion für GSLB-Dienstgruppen verwendet die DNS-fähige Diensterkennung, um die Mitgliedsdienstressourcen des DBS-Namespaces zu ermitteln, der in der Autoscale-Gruppe identifiziert wurde.

Das folgende Bild zeigt die Autoscale-Komponenten von NetScaler GSLB DBS mit Cloud-Loadbalancern:

Voraussetzungen für Azure GSLB

Zu den Voraussetzungen für die NetScaler GSLB-Servicegruppen gehört eine funktionierende Microsoft Azure-Umgebung mit dem Wissen und der Fähigkeit, Sicherheitsgruppen, Linux-Webserver, NetScaler-Appliances innerhalb von AWS, Elastic IPs und Elastic Load Balancers (ELB) zu konfigurieren.

- Die GSLB DBS Service-Integration erfordert NetScaler Version 12.0.57 für Microsoft Azure-Loadbalancer-Instanzen.
- GSLB-Dienstgruppenentität: NetScaler Version 12.0.57.
- Die GSLB-Servicegruppe wird eingeführt, die die automatische Skalierung mithilfe von DBS Dynamic Discovery unterstützt.
- DBS-Feature-Komponenten (domänenbasierter Dienst) müssen an die GSLB-Dienstgruppe gebunden sein.

Beispiel

```
```

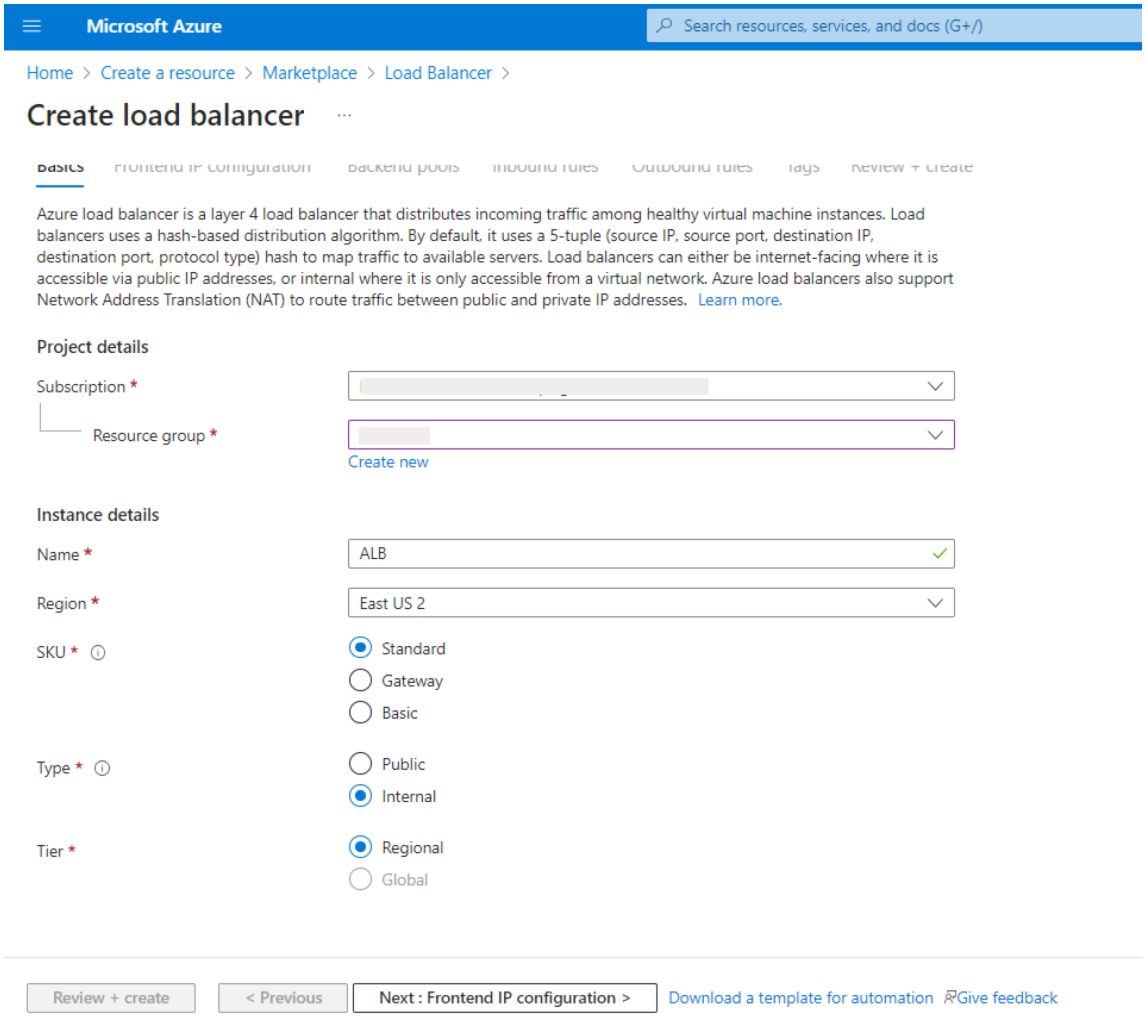
```
    > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
      amazonaws.com
    > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName
      sydney
    > bind gslb serviceGroup sydney_sg sydney_server 80
```

```
```

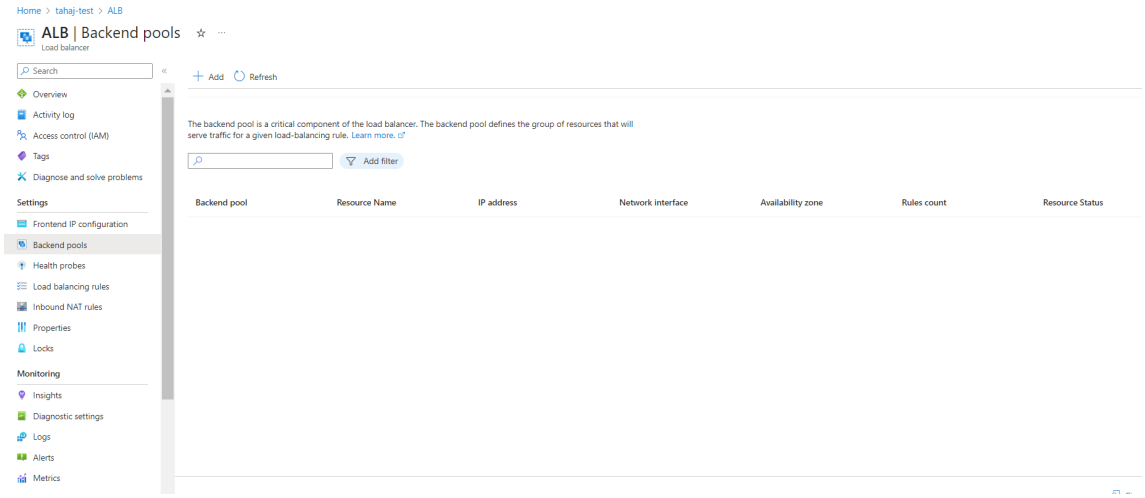
Azure-Komponenten konfigurieren

1. Melden Sie sich beim Benutzer Azure Portal an und erstellen Sie eine neue virtuelle Maschine aus einer NetScaler-Vorlage.

2. Erstellen Sie einen Azure Load Balancer.



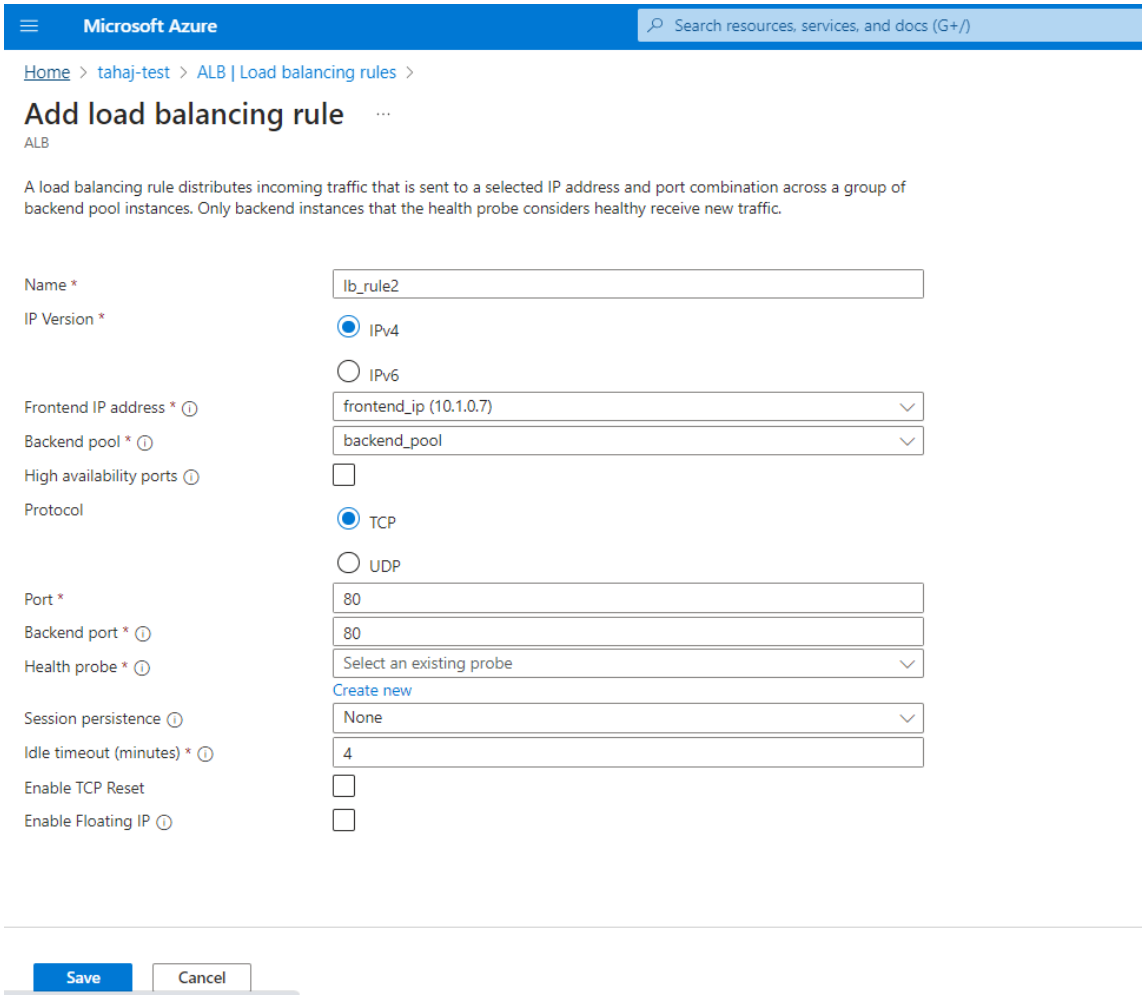
3. Fügen Sie die erstellten NetScaler-Back-End-Pools hinzu.



4. Erstellen Sie eine Integritätsprüfung für Port 80.

Erstellen Sie eine Load-Balancing-Regel unter Verwendung der vom Load Balancer erstellten Front-End-IP.

- Protokoll: TCP
- Back-End-Port: 80
- Back-End-Pool: NetScaler wurde in Schritt 1 erstellt
- Health Probe: In Schritt 4 erstellt
- Sitzungsbeständigkeit: Keine



Konfigurieren Sie den domänenbasierten Dienst NetScaler GSLB

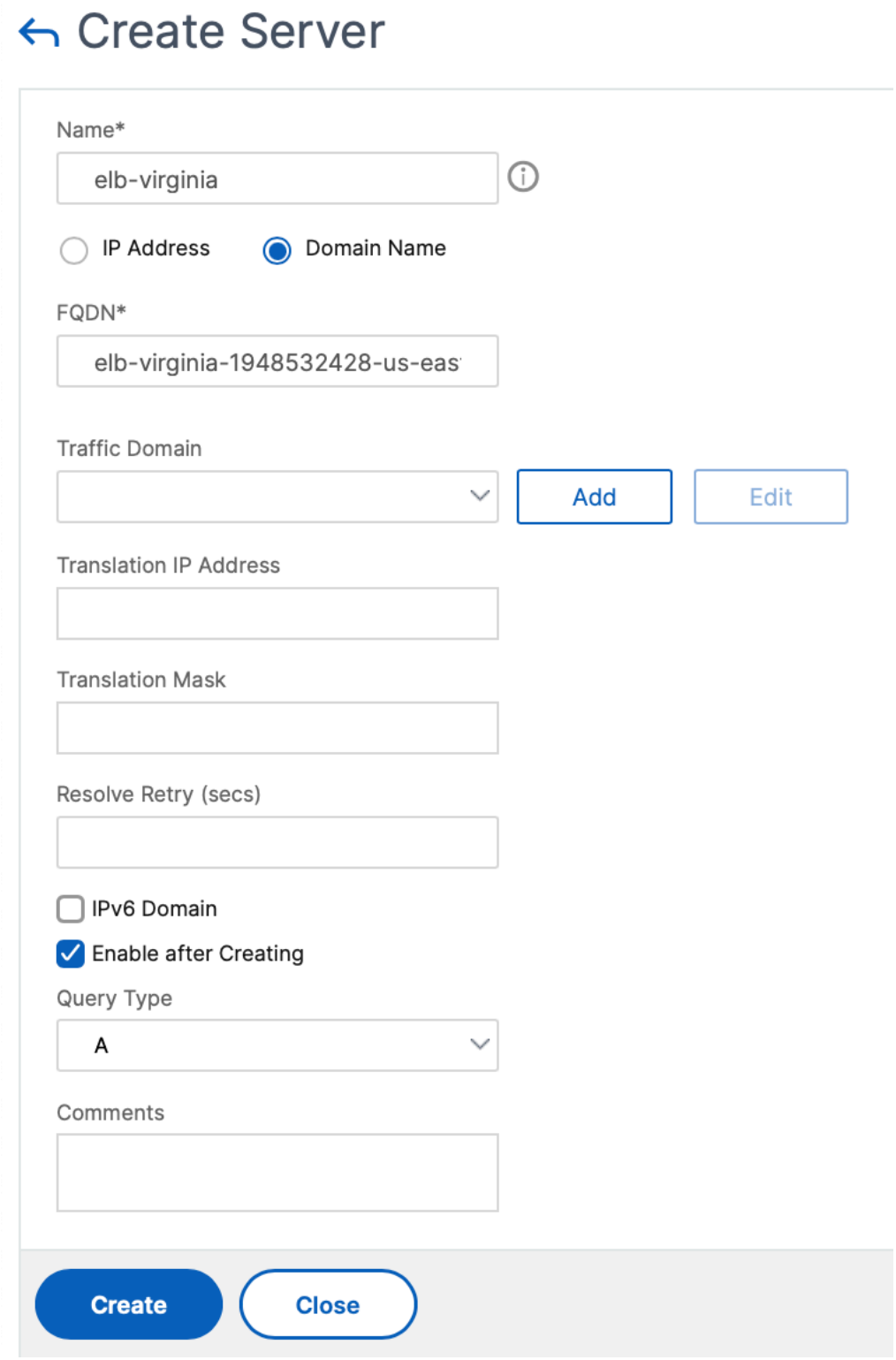
Die folgenden Konfigurationen fassen zusammen, was erforderlich ist, um domänenbasierte Dienste für die automatische Skalierung von ADCs in einer GSLB-fähigen Umgebung zu aktivieren.

- Konfigurationen für die Datenverkehrsverwaltung
- GSLB-Konfigurationen

Konfigurationen für die Datenverkehrsverwaltung

> **Hinweis:**
>
> Es ist erforderlich, den NetScaler entweder mit einem Nameserver oder einem virtuellen DNS-Server zu konfigurieren, über den die ELB /ALB-Domänen für die DBS-Servicegruppen aufgelöst werden. Weitere Informationen zu Nameservern oder virtuellen DNS-Servern finden Sie unter: DNS-Nameserver

1. Navigieren Sie zu**Traffic Management > Load Balancing > Server**.
2. Klicken Sie auf**Hinzufügen**, um einen Server zu erstellen, und geben Sie einen Namen und einen FQDN an, die dem A-Eintrag (Domänenname) in Azure für die ALB entsprechen.



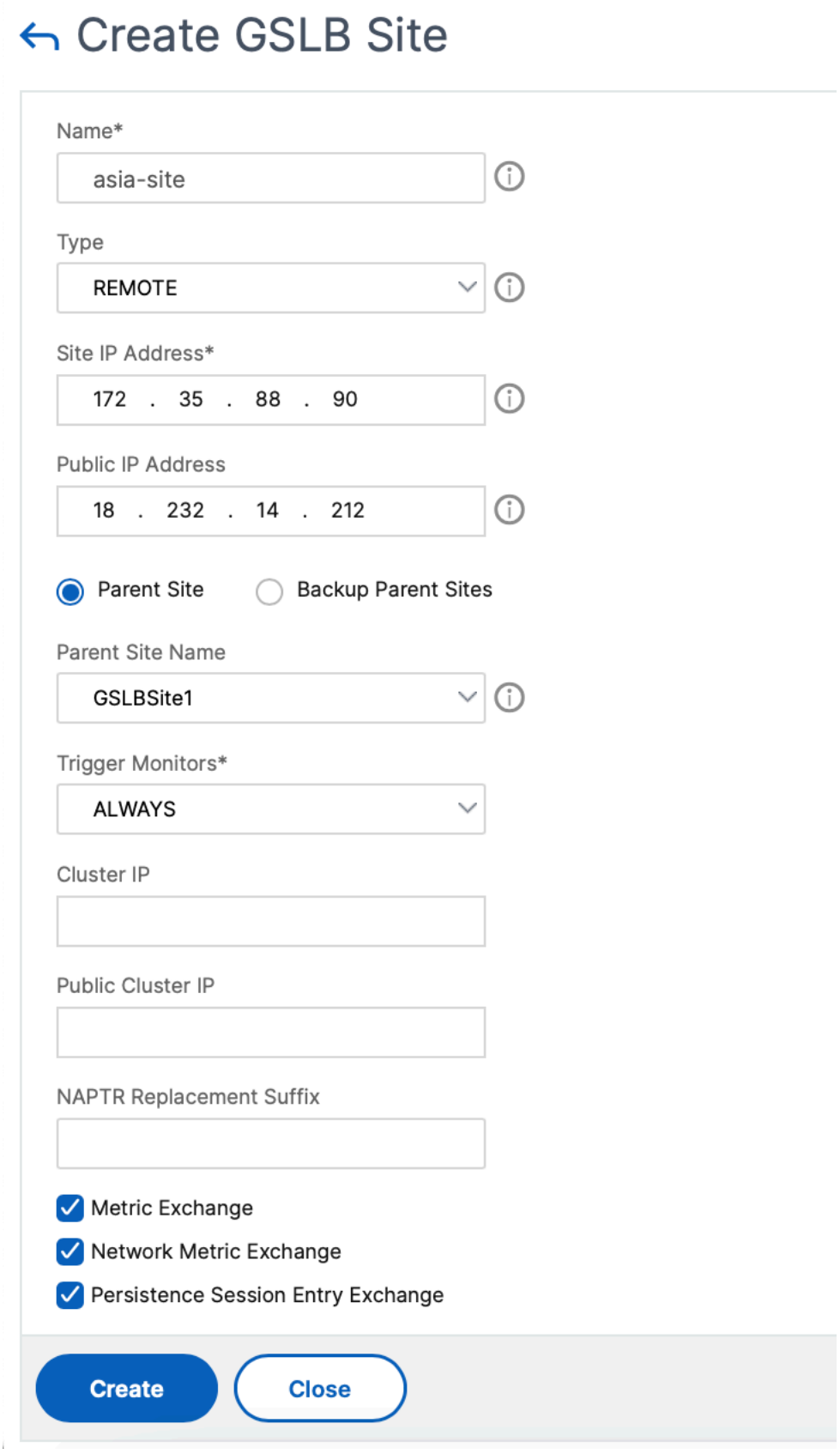
3. Wiederholen Sie Schritt 2, um die zweite ALB aus der zweiten Ressource in Azure hinzuzufügen.

GSLB-Konfigurationen

1. Klicken Sie auf **Fügen Sie**hinzu, um eine GSLB-Site zu konfigurieren.
2. Geben Sie die Details für die Konfiguration der GSLB-Site an

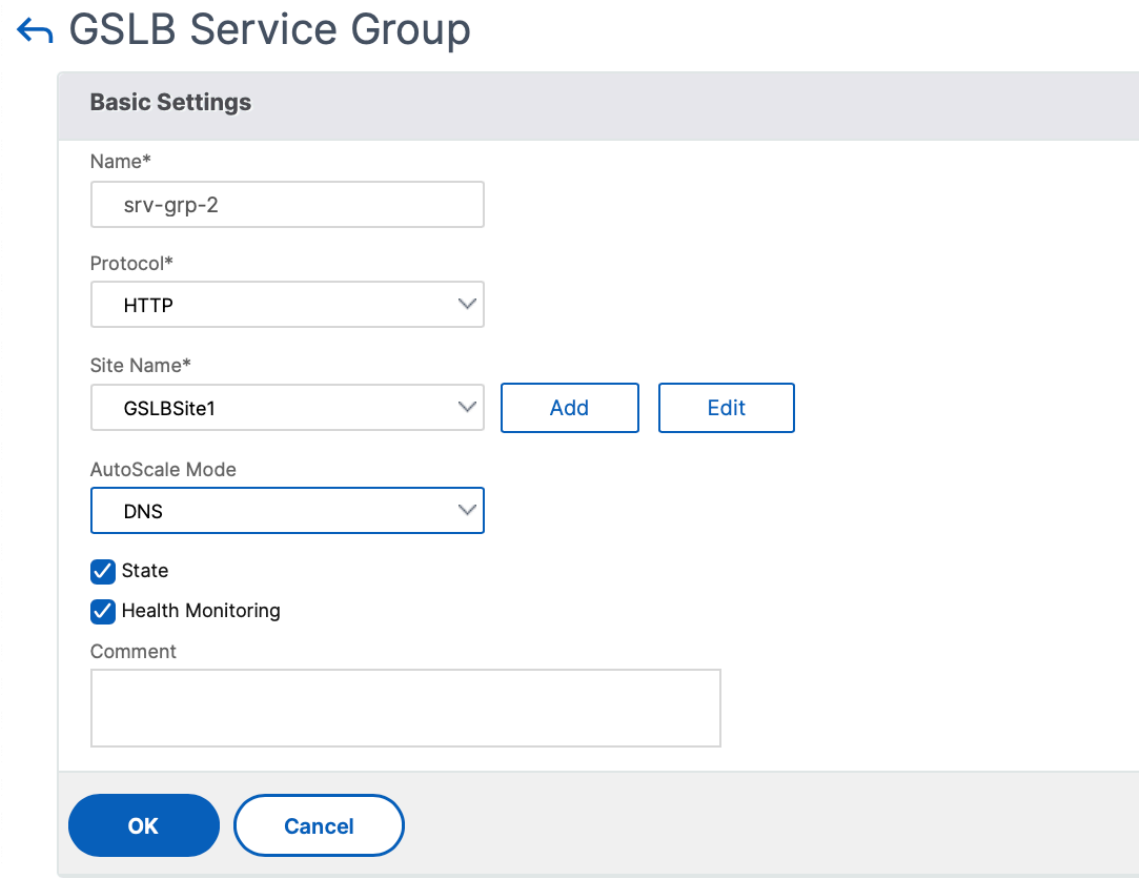
   Benennen Sie die Site. Der Typ wird als remote oder lokal konfiguriert, je nachdem, auf welchem NetScaler Sie die Site konfigurieren. Die Site-IP-Adresse ist die IP-Adresse für die GSLB-Site. Die GSLB-Site verwendet diese IP-Adresse, um mit den anderen GSLB-Sites zu kommunizieren. Die öffentliche IP-Adresse ist erforderlich, wenn Sie einen Cloud-Dienst verwenden, bei dem eine bestimmte IP-Adresse auf einer externen Firewall oder einem NAT-Gerät gehostet wird. Die Site sollte als übergeordneter Standort konfiguriert werden. Stellen Sie sicher, dass die **Trigger-Monitore** auf **ALWAYS**eingestellt sind. Stellen Sie außerdem sicher, dass Sie die drei Kästchen unten für **Metric Exchange**, **Network Metric Exchange**und **Persistence Session Entry Exchange**aktivieren.

   Wir empfehlen Ihnen, den **Trigger-Monitor** auf **MEPDOWN**einzustellen. Weitere Informationen finden Sie unterKonfigurieren einer GSLB-Dienstgruppe.

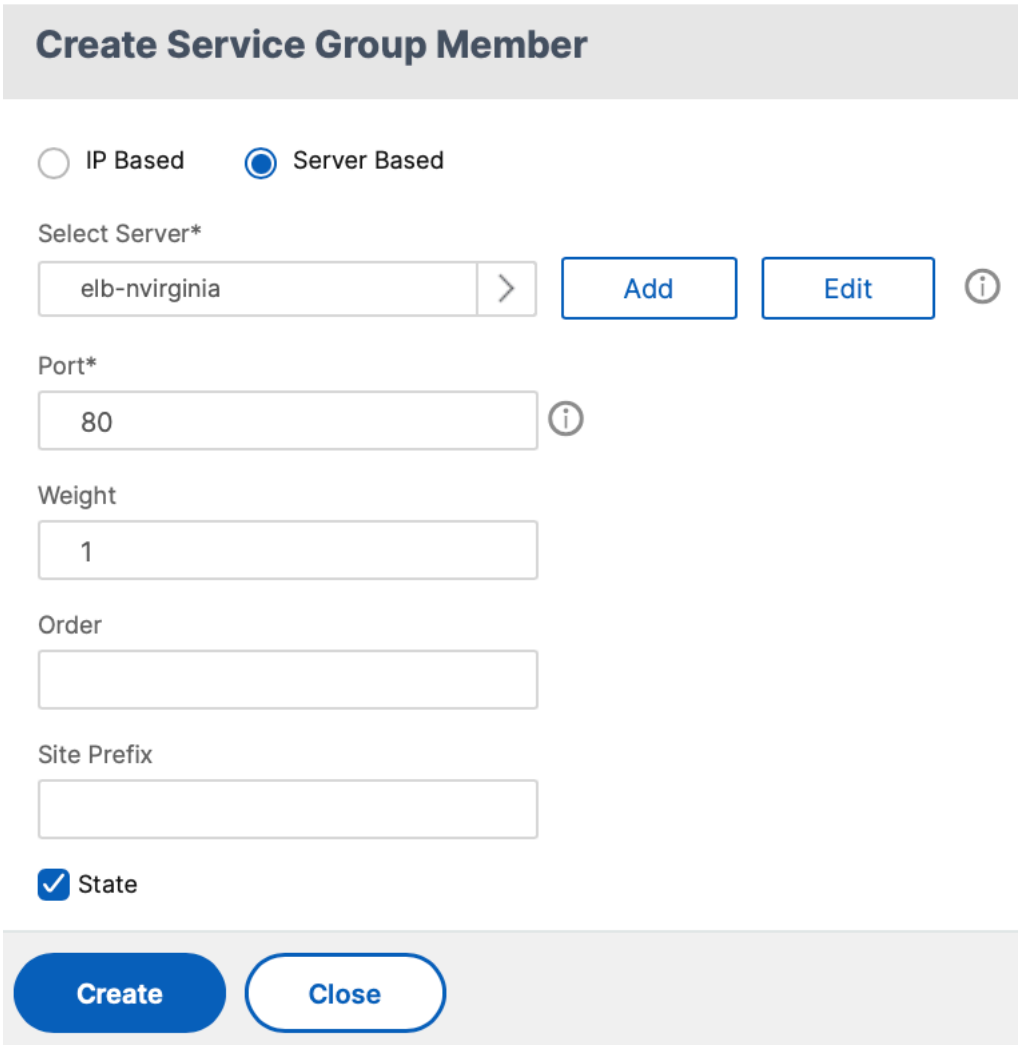


3. Klicken Sie auf **Erstellen**.
4. Navigieren Sie zu **Traffic Management > GSLB > Dienstgruppen**.
5. Klicken Sie auf **Hinzufügen**, um eine Dienstgruppe hinzuzufügen.
6. Geben Sie die Details zur Konfiguration der Dienstgruppe an

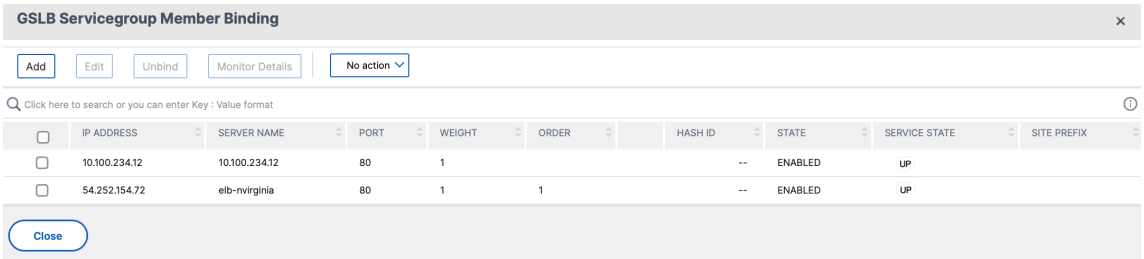
   Benennen Sie die Dienstgruppe und verwenden Sie das HTTP-Protokoll. Wählen Sie unter **Site-Name** die entsprechende Site aus, die Sie erstellt haben. Stellen Sie sicher, dass Sie den automatischen Skalierungsmodus als DNS konfigurieren und die Kontrollkästchen für die Status- und Integritätsüberwachung aktivieren. Klicken Sie auf**OK**, um die Dienstgruppe zu erstellen.



7. Klicken Sie auf**Service Group Members**und wählen Sie**Serverbasiert**aus. Wählen Sie den jeweiligen ELB aus, der zu Beginn der Run-Anleitung konfiguriert wurde. Konfigurieren Sie den Datenverkehr so, dass er über Port 80 geht. Klicken Sie auf **Erstellen**.



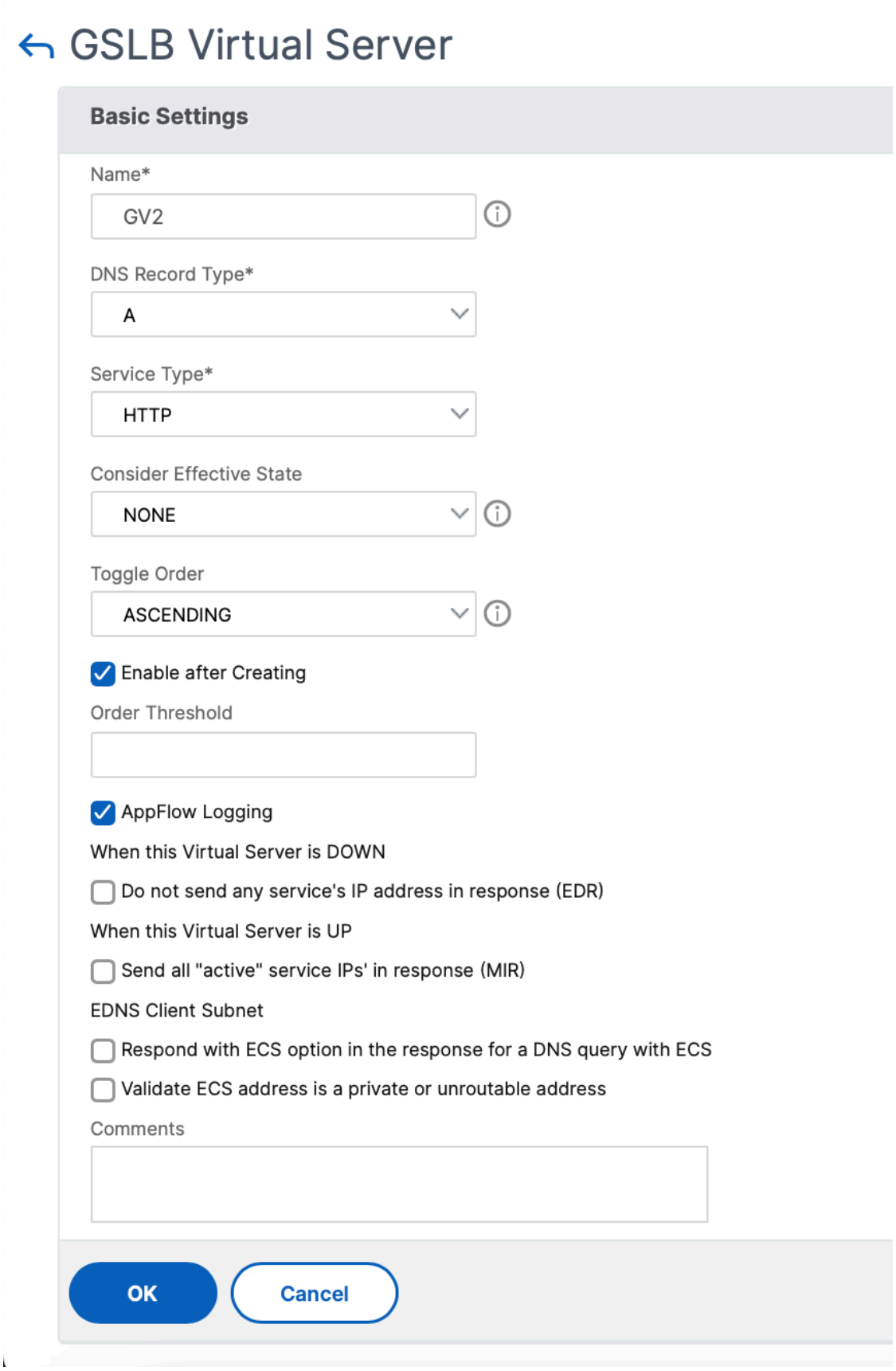
Die Dienstgruppenmitgliederbindung sollte mit 2 Instanzen aufgefüllt werden, die sie vom ELB empfängt.



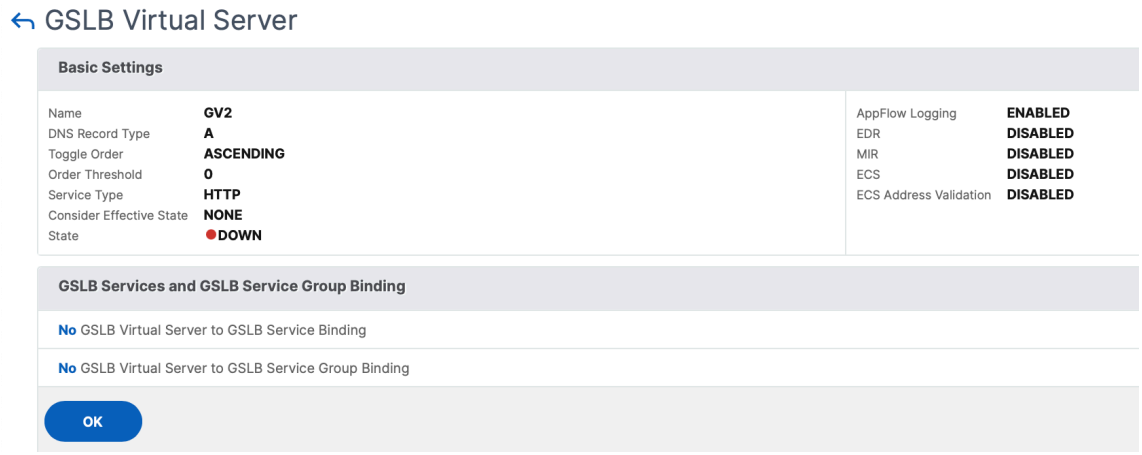
8. Wiederholen Sie die Schritte 5 und 6, um die Dienstgruppe für den zweiten Ressourcenstandort in Azure zu konfigurieren. (Dies kann über dieselbe NetScaler GUI erfolgen).
9. Um einen virtuellen GSLB-Server einzurichten. Navigieren Sie zu **Traffic Management > GSLB > Virtuelle Server**.
10. Klicken Sie auf**Hinzufügen**, um den virtuellen Server zu erstellen.

11. Geben Sie die Details zur Konfiguration des virtuellen GSLB-Servers an.

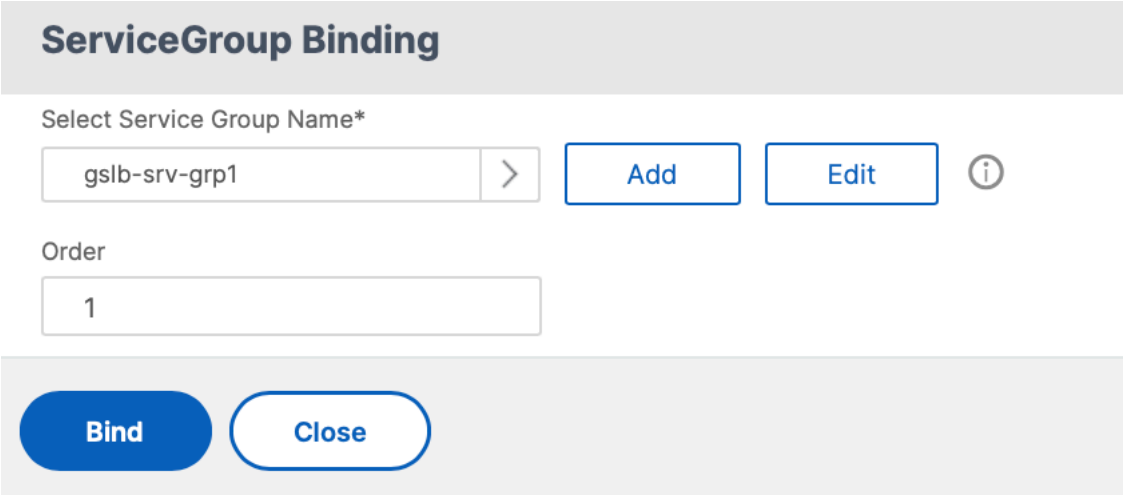
    Nennen Sie den Server, DNS-Datensatztyp ist als A, Diensttyp als HTTP festgelegt, und aktivieren Sie die Kontrollkästchen Nach dem Erstellen aktivieren und AppFlow-Protokollierung. Klicken Sie auf**OK**, um den virtuellen GSLB Server zu erstellen.



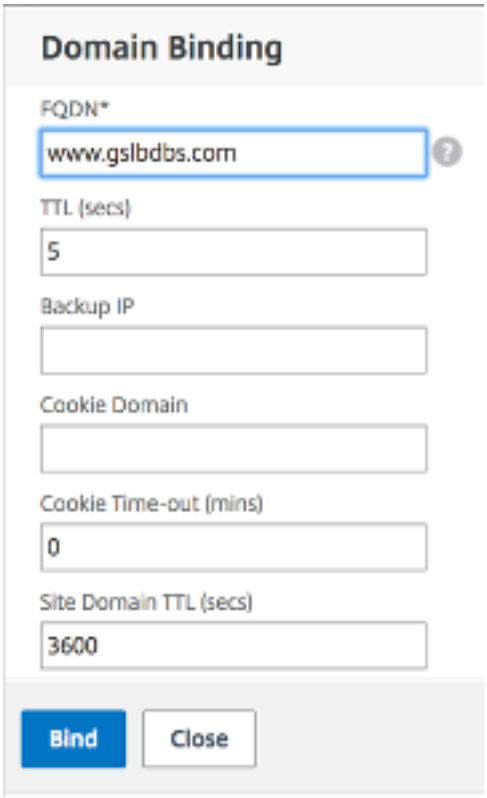
12. Sobald der virtuelle GSLB-Server erstellt wurde, klicken Sie auf**No GSLB Virtual Server ServiceGroup Binding**.



13. Verwenden**Sie unter**ServiceGroup Binding**die Option Select Service Group Name** , um die Dienstgruppen auszuwählen und hinzuzufügen, die in den vorherigen Schritten erstellt wurden.

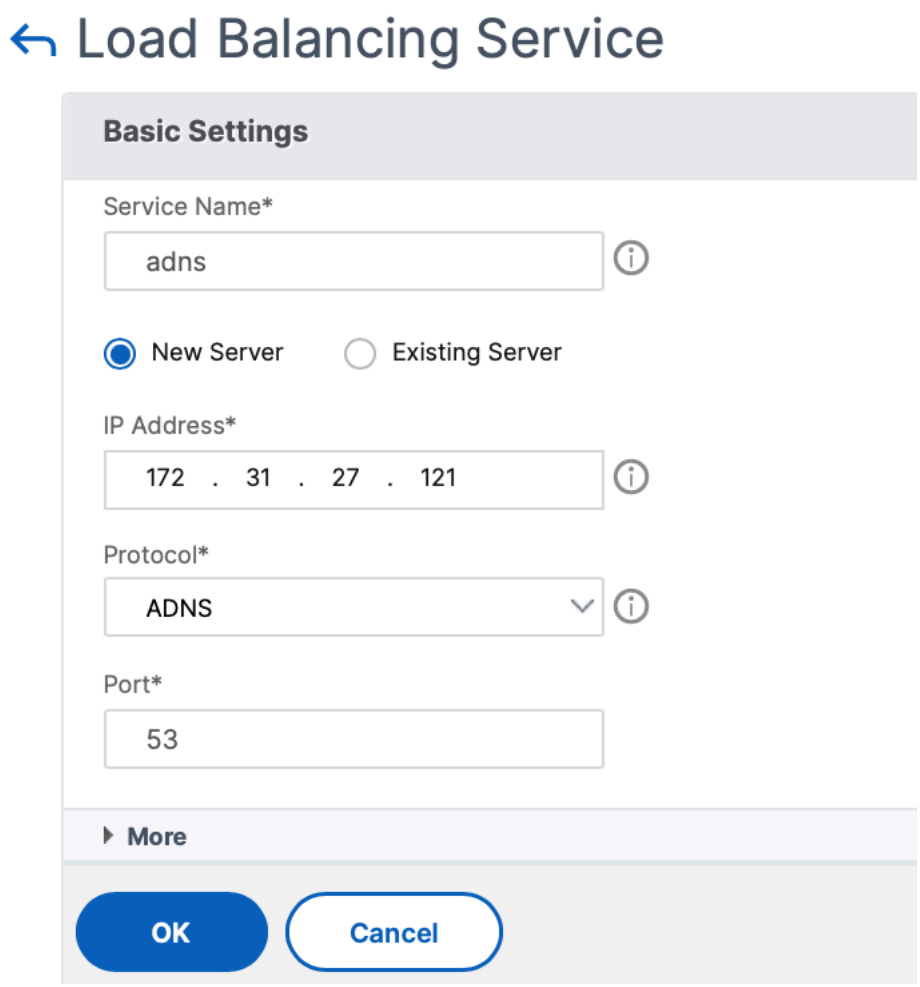


14. Konfigurieren Sie die Domänenbindung für virtuelle GSLB-Server, indem Sie auf**Keine GSLB-Domainbindung für virtuelle Server**klicken. Konfigurieren Sie den FQDN und binden Sie ihn. Behalten Sie die Standardeinstellung für andere Parameter bei.



15. Konfigurieren Sie den ADNS-Dienst, indem Sie auf**Kein Dienst**klicken.
16. Geben Sie die Details an, um den Load Balancing-Dienst zu konfigurieren.

    Fügen Sie einen **Dienstnamen**hinzu, klicken Sie auf**Neuer Server**und geben Sie die **IP-Adresse** des ADNS-Servers ein. Wenn der Benutzer ADNS bereits konfiguriert ist, können Benutzer**Existing Server**und dann den Benutzer ADNS aus dem Drop-down-Menü auswählen. Stellen Sie sicher, dass das Protokoll ADNS ist und der Datenverkehr so konfiguriert ist, dass er über Port 53 fließt.



17. Konfigurieren Sie die **Methode** als **Least Connection** und die Backup-Methode als **Round Robin**.
18. Klicken Sie auf**Fertig**und stellen Sie sicher, dass der virtuelle GSLB-Server des Benutzers als Up angezeigt wird.

Andere Ressourcen

Globaler NetScaler Lastausgleich für Hybrid- und Multi-Cloud-Bereitstellungen

Konfigurieren der Intranet-IP für Adresspools für eine NetScaler Gateway-App

October 17, 2024

In einigen Situationen benötigen Benutzer, die eine Verbindung mit dem NetScaler Gateway -Plug-In herstellen, eine eindeutige IP-Adresse für eine NetScaler Gateway-Appliance. Wenn Sie Adresspools (auch als IP-Pooling bezeichnet) für eine Gruppe aktivieren, kann die NetScaler Gateway-Appliance jedem Benutzer einen eindeutigen IP-Adressalias zuweisen. Sie konfigurieren Adresspools mithilfe von Intranet-IP (IIP) -Adressen.

Sie können Adresspools auf einer in Azure bereitgestellten NetScaler Gateway -Appliance konfigurieren, indem Sie diese zweistufige Vorgehensweise ausführen:

- Registrieren der privaten IP-Adressen, die im Adresspool verwendet werden, in Azure
- Konfigurieren von Adresspools in der NetScaler Gateway Appliance

Registrieren einer privaten IP-Adresse im Azure-Portal

In Azure können Sie eine NetScaler VPX-Instanz mit mehreren IP-Adressen bereitstellen. Sie können einer VPX-Instanz auf zwei Arten IP-Adressen hinzufügen:

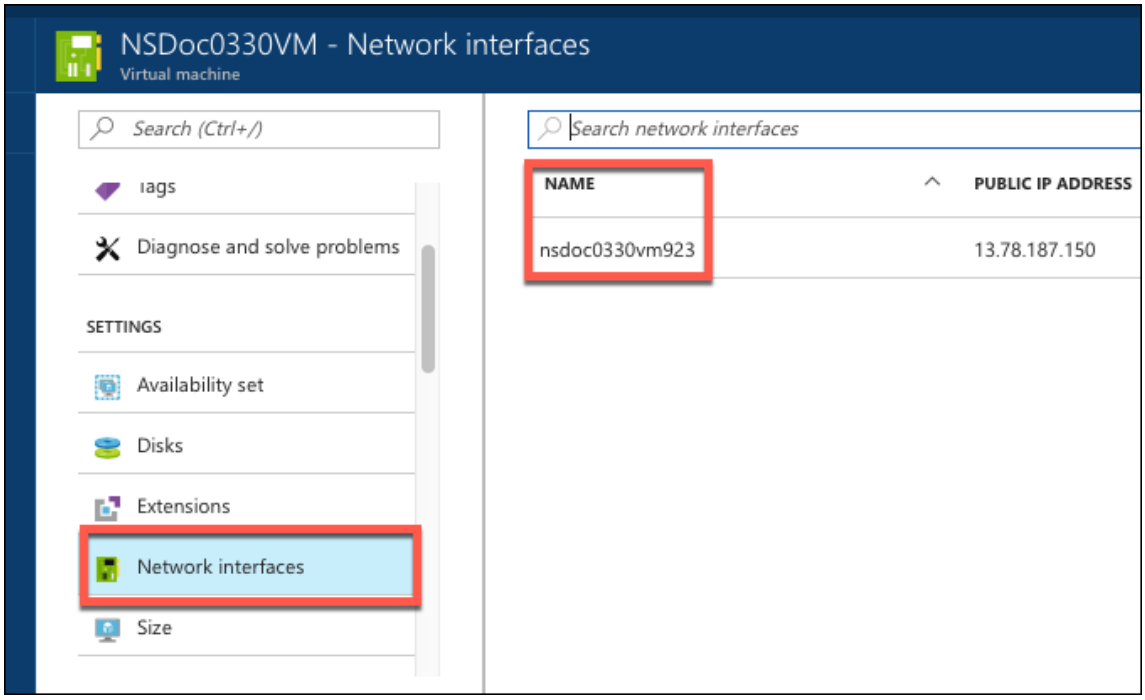
a. Beim Provisioning einer VPX-Instanz

Weitere Informationen zum Hinzufügen mehrerer IP-Adressen beim Bereitstellen einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine eigenständige NetScaler-Instanz. Informationen zum Hinzufügen von IP-Adressen mithilfe von PowerShell-Befehlen beim Bereitstellen einer VPX-Instanz finden Sie unter . Konfigurieren Sie mehrere IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

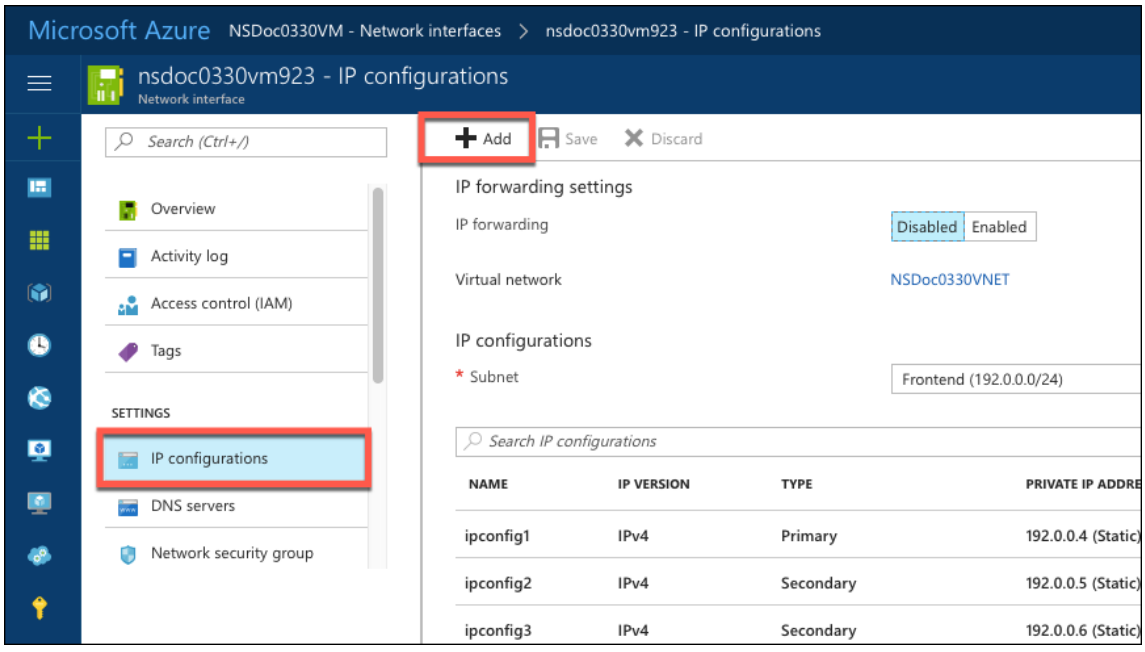
b. Nach der Provisioning einer VPX-Instanz

Nachdem Sie eine VPX-Instanz bereitgestellt haben, führen Sie diese Schritte aus, um eine private IP-Adresse im Azure-Portal zu registrieren, das Sie als Adresspool in der NetScaler Gateway-Appliance konfigurieren.

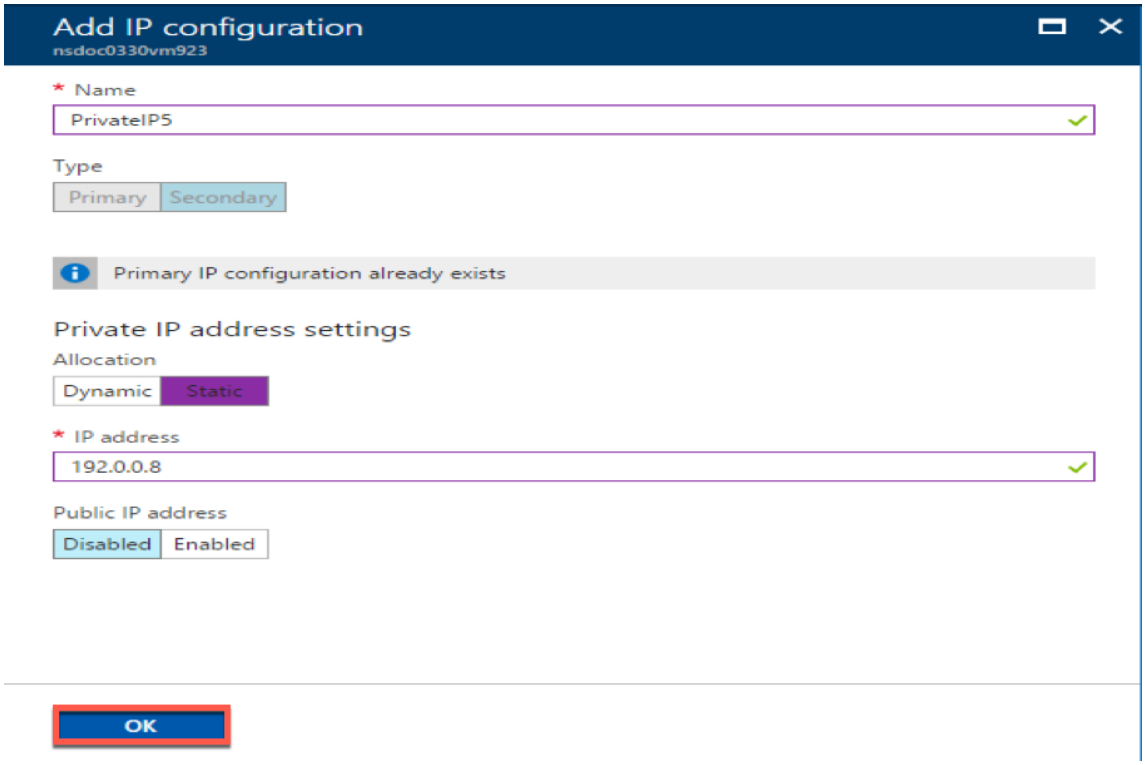
1. Wechseln Sie in Azure Resource Manager (ARM) zur bereits erstellten NetScaler VPX-Instanz > **Netzwerkschnittstellen**. Wählen Sie die Netzwerkschnittstelle, die an ein Subnetz gebunden ist, zu dem das IIP gehört, das Sie registrieren möchten.



2. Klicken Sie auf **IP-Konfigurationen**, und klicken Sie dann auf **Hinzufügen**.



3. Geben Sie die erforderlichen Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf **OK**.



Konfigurieren von Adresspools in der NetScaler Gateway Appliance

Weitere Informationen zum Konfigurieren von Adresspools auf dem NetScaler Gateway finden Sie unter Konfigurieren von Adresspools.

> **Einschränkung:**
>
> Sie können einen Bereich von IIP-Adressen nicht an Benutzer binden. Jede IIP-Adresse, die in einem Adresspool verwendet wird, muss registriert sein.

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz über PowerShell-Befehle konfigurieren

October 17, 2024

In einer Azure-Umgebung kann eine virtuelle NetScaler VPX-Appliance mit mehreren NICs bereitgestellt werden. Jede Netzwerkkarte kann mehrere IP-Adressen haben. In diesem Abschnitt wird beschrieben, wie Sie eine NetScaler VPX-Instanz mit einer einzelnen Netzwerkkarte und mehreren IP-Adressen mithilfe von PowerShell-Befehlen bereitstellen. Sie können dasselbe Skript für die Multi-NIC- und Multi-IP-Bereitstellung verwenden.

> **Hinweis:**
>
> In diesem Dokument bezieht sich IP-Config auf ein Paar von IP-Adressen, öffentliche IP und private IP, die mit einer einzelnen Netzwerkkarte verknüpft sind. Weitere Informationen finden Sie im Abschnitt Azure-Terminologie .

Anwendungsfall

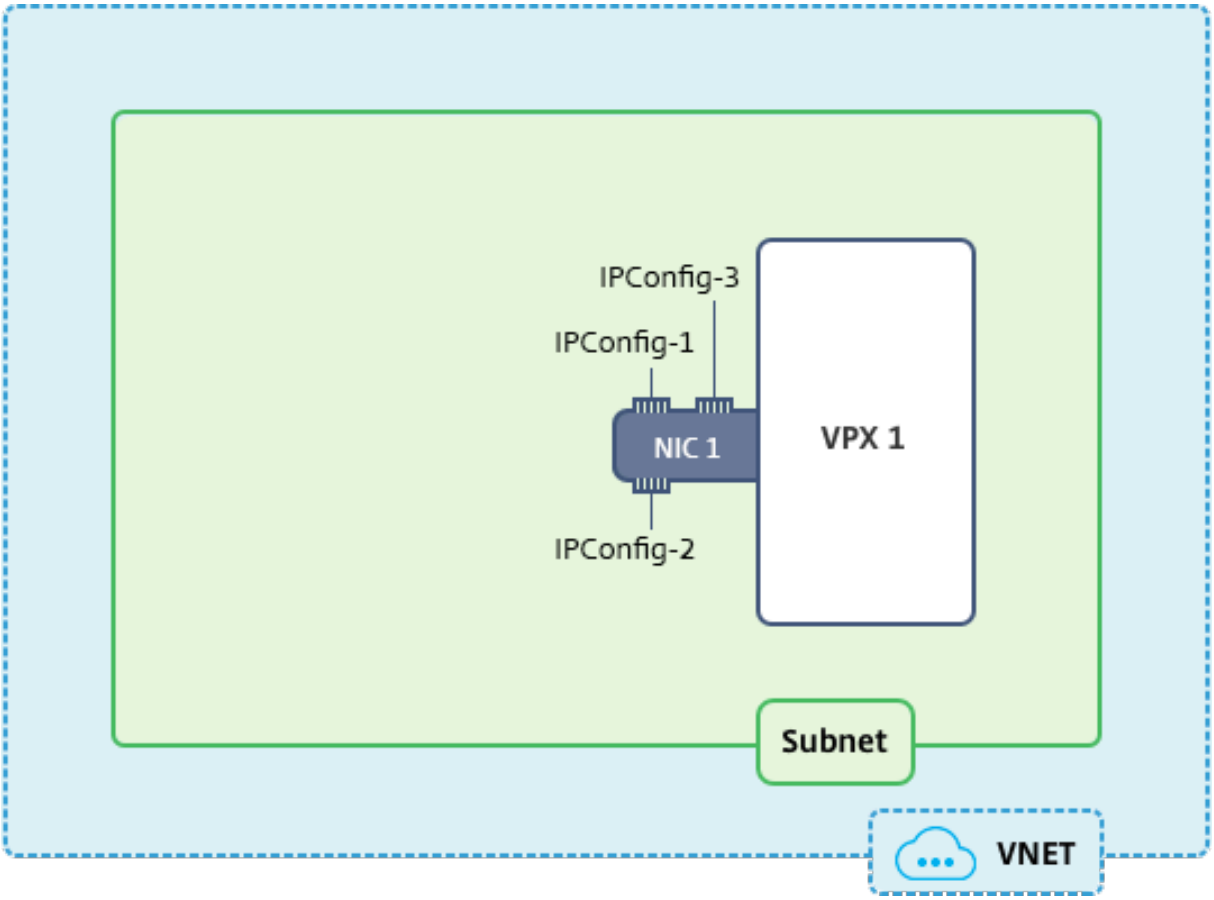
In diesem Anwendungsfall ist eine einzelne Netzwerkkarte mit einem virtuellen Netzwerk (VNET) verbunden. Die Netzwerkkarte ist drei IP-Konfigurationen zugeordnet, wie in der folgenden Tabelle dargestellt.

IP-Konfiguration	Verbunden mit
IPConfig-1	Statische öffentliche IP-Adresse; statische private IP-Adresse
IPConfig-2	Statische öffentliche IP-Adresse; statische private Adresse
IPConfig-3	Statische private IP-Adresse

> **Hinweis:**
>
> ipConfig-3 ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis:**
>
> In einer Multi-Nic, Multi-IP Azure NetScaler VPX-Bereitstellung wird die private IP-Adresse, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als Verwaltungs-NSIP-Adresse der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIPs oder SNIPs mit dem `add ns ip` Befehl hinzugefügt werden, wie von Ihren Anforderungen festgelegt.

Im Folgenden finden Sie die Schritte, die zum Konfigurieren mehrerer IP-Adressen für eine virtuelle NetScaler VPX Appliance im Standalone-Modus erforderlich sind:

1. Ressourcengruppe erstellen
2. Speicherkonto erstellen
3. Verfügbarkeitsset erstellen
4. Netzwerkdienstgruppe erstellen
5. Virtuelles Netzwerk erstellen
6. Öffentliche IP-Adresse erstellen
7. IP-Konfiguration zuweisen
8. NIC erstellen
9. Erstellen Sie NetScaler VPX-Instanz

10. NIC-Konfigurationen überprüfen
11. VPX-seitige Konfigurationen überprüfen

Skript

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für den Anwendungsfall in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

$locName=”westcentralus”

$rgName=”Azure-MultiIP”

$nicName1=”VM1-NIC1”

$vNetName=”Azure-MultiIP-vnet”

$vNetAddressRange=”11.6.0.0/16”

$frontEndSubnetName=”frontEndSubnet”

$frontEndSubnetRange=”11.6.1.0/24”

$prmStorageAccountName=”multiipstorage”

$avSetName=”multiip-avSet”

$vmSize=”Standard_DS4_v2”(Dieser Parameter erstellt eine VM mit bis zu vier NICs.)

Hinweis: Die Mindestanforderung für eine VPX-Instanz ist 2 vCPUs und 2 GB RAM.

$Publisher = “Citrix”

$offer=”netscalervpx110-6531”(Sie können andere Angebote verwenden.)

$sku=”netscalerbyol”(Je nach Ihrem Angebot kann die SKU unterschiedlich sein.)

$version=”latest”

$pubIPName1=”PIP1”

$pubIPName2=”PIP2”

$domName1=”multiipvpx1”

$domName2=”multiipvpx2”

$vmNamePrefix=”VPXMultiIP”

$osDiskSuffix=”osmultiipalbdiskdb1”

Informationen zur Netzwerksicherheitsgruppe (NSG):

$nsgName=”NSG-MultiIP”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Ressourcengruppe erstellen

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Speicherkonto erstellen

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Verfügbarkeitsset erstellen

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
 $rgName -Location $locName
```

4. Netzwerksicherheitsgruppe erstellen

1. Fügen Sie Regeln hinzu. Sie müssen der Netzwerksicherheitsgruppe eine Regel für jeden Port hinzufügen, der Datenverkehr bedient.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
   Beschreibung „HTTP zulassen“ -Zugriff zulassen -Protokoll TCP
   -Richtung eingehend -Priorität 101 -Quelladressspräfix Internet
    -Quellportbereich * -Zieladressspräfix * -Zielportbereich 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
   Beschreibung „HTTPS zulassen“ -Zugriff zulassen -Protokoll TCP
   -Richtung eingehend -Priorität 110 -Quelladressspräfix Internet
    -Quellportbereich * -Zieladressspräfix * -Zielportbereich 443
   ```



```
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
Beschreibung „SSH zulassen“ -Zugriff zulassen -Protokoll TCP -
Richtung eingehend -Priorität 120 -Quelladressspräfix Internet -
Quellportbereich * -Zieladressspräfix * -Zielportbereich 22
```

2. Erstellen Sie ein Netzwerksicherheitsgruppenobjekt.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName
-Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
$rule3
```

5. Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$frontEndSubnetName -AddressPrefix $frontEndSubnetRange
```

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
 $rgName -Location $locName -AddressPrefix $vNetAddressRange -
Subnet $frontendSubnet
```

3. Rufen Sie Subnetze ab.

```
$subnetName="frontEndSubnet" $subnet1=$vnet.Subnetze|?{ $_.Name -
eq $subnetName }
```

6. Öffentliche IP-Adresse erstellen

```
$pip1=Neue-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
 $rgName -DomainNameLabel $domName1 -Standort $locName -AllocationMethod
 Statisch$pip2=Neue-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupNam
 $rgName -DomainNameLabel $domName2 -Standort $locName -AllocationMethod
 Statisch
```

> **Hinweis:**
>
> Prüfen Sie vor der Verwendung die Verfügbarkeit von Domainnamen.
>
> Die Zuordnungsmethode für IP-Adressen kann dynamisch oder statisch sein.

7. IP-Konfiguration zuweisen

Berücksichtigen Sie in diesem Anwendungsfall die folgenden Punkte, bevor Sie IP-Adressen zuweisen:

- ipConfig-1 gehört zum Subnetz1 von VPX1.
- ipConfig-2 gehört zum Subnetz 1 von VPX1.
- ipConfig-3 gehört zum Subnetz 1 von VPX1.

> **Hinweis:**
>
> Wenn Sie einer NIC mehrere IP-Konfigurationen zuweisen, muss eine Konfiguration als primäre zugewiesen werden.

```
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
```

Verwenden Sie eine gültige IP-Adresse, die Ihren Subnetzanforderungen entspricht, und überprüfen Sie deren Verfügbarkeit.

8. NIC erstellen

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
 $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,
$IPConfig3 -NetworkSecurityGroupId $nsg.Id
```

9. NetScaler VPX-Instanz erstellen

1. Initialisieren Sie Variablen.

   ```
   $suffixNumber = 1 $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Erstellen Sie ein VM-Konfigurationsobjekt.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
   AvailabilitySetId $avSet.Id
   ```


3. Legen Sie Anmeldeinformationen, Betriebssystem und Image fest.

```
$cred=Get-Credential -Message „Geben Sie den Namen und das
Passwort für die VPX-Anmeldung ein.“$vmConfig=Set-AzureRMVMOperatingSystem
 -VM $vmConfig -Linux -ComputerName $vmName -Anmeldeinformationen
 $cred$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
 $publisher -Angebot $offer -Skus $sku -Version $version
```

4. Fügen Sie NIC hinzu.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
Id -Primary
```

> **Hinweis:**
>
> Bei einer NetScaler VPX-Bereitstellung mit mehreren Netzwerkkarten muss eine Netzwerkkarte die primäre sein. Daher muss beim Hinzufügen dieser Netzwerkkarte zur NetScaler VPX-Instanz „-Primary“angehängt werden.

5. Geben Sie den Betriebssystemdatenträger an und erstellen Sie VM.

```
$osDiskName=$vmName + „-“ + $osDiskSuffix1$osVhdUri=$prmStorageAccount
.PrimaryEndpoints.Blob.ToString()+ "vhds/"+ $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -
VhdUri $osVhdUri -CreateOption fromImage   Set-AzureRmVMPlan -VM
$vmConfig -Herausgeber $publisher -Produkt $offer -Name $sku Neu-
AzureRMVM -VM $vmConfig -Ressourcengruppenname $rgName -Standort
$locName
```

10. Überprüfen Sie die NIC-Konfigurationen

Nachdem die NetScaler VPX-Instanz gestartet ist, können Sie mit dem folgenden Befehl die den `IPConfigs` der NetScaler VPX-NIC zugewiesenen IP-Adressen überprüfen.

```
$nic.IPConfig
```

11. Überprüfen Sie die VPX-seitigen Konfigurationen

Wenn die NetScaler VPX-Instanz gestartet wird, wird eine private IP-Adresse, die mit `IPconfig` der primären Netzwerkkarte verknüpft ist, als NSIP-Adresse hinzugefügt. Die verbleibenden privaten IP-Adressen müssen gemäß Ihren Anforderungen als VIP- oder SNIP-Adressen hinzugefügt werden. Verwenden Sie den folgenden Befehl.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```


Sie haben jetzt mehrere IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus konfiguriert.

Zusätzliche PowerShell -Skripts für die Azure-Bereitstellung

October 17, 2024

Dieser Abschnitt enthält die PowerShell Cmdlets, mit denen Sie die folgenden Konfigurationen in Azure PowerShell ausführen können:

- Bereitstellung einer eigenständigen NetScaler VPX-Instanz
- Bereitstellung eines NetScaler VPX-Paars in einem Hochverfügbarkeits-Setup mit einem externen Azure-Load Balancer
- Stellen Sie ein NetScaler VPX-Paar in einem Hochverfügbarkeits-Setup mit dem internen Azure-Load Balancer bereit

Weitere Informationen zu Konfigurationen, die Sie mithilfe von PowerShell Befehlen ausführen können, finden Sie in den folgenden Themen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle
- Konfigurieren von GSLB auf NetScaler VPX-Instanzen
- Konfigurieren von GSLB auf einem NetScaler Active-Standby Hochverfügbarkeitssetup
- Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalonemodus über PowerShell-Befehle

Bereitstellung einer eigenständigen NetScaler VPX-Instanz

1. **Erstellen einer Ressourcengruppe**

   Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancer dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="&lt;resource group name&gt;" $locName="&lt;location name
   , such as West US&gt;   Neue AzureRmResourceGroup -Name $rgName -
   Standort $locName
   ```

   Zum Beispiel:


```
$rgName = "ARM-VPX"
$locName = "West US"
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>" $saType="<storage account type>"`, geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS` `Neues AzureRmStorageAccount -Name $saName -Ressourcengruppenname $rgName -Typ $saType -Standort $locName`

   Zum Beispiel:

   ```
   $saName="vpxstorage"
   $saType="Standard\_LRS"
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
      $rgName -Type $saType -Location $locName
   ```

3. **Erstellen eines Verfügbarkeitssatzes**

   Verfügbarkeitssatz hilft, Ihre virtuellen Maschinen während Ausfallzeiten verfügbar zu halten, z. B. Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
   $rgName -Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

   ```
   $FrontendAddressPrefix= „10.0.1.0/24“ $BackendAddressPrefix=
   „10.0.2.0/24“ $vnetAddressPrefix= „10.0.0.0/16“ $frontendSubnet
   =New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -
   AddressPrefix $FrontendAddressPrefix $backendSubnet=New-AzureRmVirtualNetwo
    -Name backendSubnet -AddressPrefix $BackendAddressPrefix Neues
   AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
    -Standort $locName -Adresspräfix $vnetAddressPrefix -Subnetz
   $frontendSubnet,$backendSubnet
   ```

   Zum Beispiel:


```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vnetAddressPrefix
    -Subnet $frontendSubnet,$backendSubnet
```

5. **Erstellen einer Netzwerkkarte**

   Erstellen Sie eine NIC und verknüpfen Sie die NIC mit der NetScaler VPX-Instanz. Das in der obigen Prozedur erstellte Front-End-Subnetz wird bei 0 indiziert und das Back-End-Subnetz wird bei 1 indiziert. Erstellen Sie nun NIC auf eine der drei folgenden Arten:

   a) *NIC mit öffentlicher IP-Adresse*

   ```
   $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 mit öffentlicher IP und DNS Label*

   ```
   $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
   ```

   Bevor Sie $domName zuweisen, überprüfen Sie, ob es verfügbar ist oder nicht, indem Sie den Befehl verwenden:

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -
   Location $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
    $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
   ].Id -PublicIpAddressId $pip.Id
   ```

   Zum Beispiel:

   ```
   $nicName="frontendNIC"

   $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 mit dynamischer öffentlicher Adresse und statischer privater IP-Adresse*

Stellen Sie sicher, dass die private (statische) IP-Adresse, die Sie der VM hinzufügen, den gleichen Bereich haben muss wie die des angegebenen Subnetzes.

```
$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. **Erstellen eines virtuellen Objekts**

```
$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. **Holen Sie sich das NetScaler VPX-Image**

```
$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."
```

Geben Sie Ihre Anmeldeinformationen an, die für die Anmeldung bei VPX verwendet werden

```
$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
```

Zum Beispiel:

```
$pubName="citrix"
```

Mit dem folgenden Befehl werden alle Angebote von Citrix angezeigt:

```
1   Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
        Select Offer
2
3   $offerName="netscalervpx110-6531"
```

Der folgende Befehl wird verwendet, um die vom Herausgeber angebotene SKU für einen bestimmten Angebotsnamen zu kennen:

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -
Offer $offerName | Select Skus
```

8. **Erstellen Sie eine virtuelle Maschine**

```
$diskName="<name identifier for the disk in Azure storage, such
as OSDisk>"
```

Zum Beispiel:

```
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
```

Wenn Sie VM aus Images erstellen, die auf Marketplace-Site vorhanden sind, verwenden Sie den folgenden Befehl, um den VM-Plan anzugeben:

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName
 -Name $skuName
```



```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
$vm
```

Bereitstellung eines NetScaler VPX-Paars in einem Hochverfügbarkeits-Setup mit einem externen Azure-Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Erstellen einer Ressourcengruppe**

   Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle, die zum Erstellen eines Load Balancer verwendet werden, dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="<resource group name>"
   ```

   ```
   $locName="<location name, such as West US>"
   ```

   ```
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   1   $rgName = "ARM-LB-NS"
   2
   3   $locName = "West US"
   4
   5   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   ```
   $saName="<storage account name>"
   ```

   ```
   $saType="&lt;storage account type&gt;"
   ```
   , geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

   ```
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
   $rgName -Type $saType -Location $locName
   ```

   Zum Beispiel:

   ```
   1   $saName="vpxstorage"
   2
   3   $saType="Standard_LRS"
   4
   5   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
          $rgName -Type $saType -Location $locName
   ```


3. **Erstellen eines Verfügbarkeitssatzes**

   Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
   $rgName -Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

   ```
   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
   ```

   > **Hinweis:**
   >
   > Wählen Sie den Parameterwert AddressPrefix entsprechend Ihren Anforderungen.

   Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

   Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

   Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Konfigurieren der Front-End-IP-Adresse und Erstellen eines Back-End-Adress-Pools**

   Konfigurieren Sie eine Front-End-IP-Adresse für den eingehenden Load Balancer Netzwerkverkehr und erstellen Sie einen Back-End-Adresspool, um den Lastausgleichsverkehr zu empfangen.


```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -
    AllocationMethod Static -DomainNameLabel nsvpx
```

> **Hinweis:**
>
> Überprüfen Sie die Verfügbarkeit des Wertes für DomainNameLabel.

```
        $FIPName = "ELBFIP"

        $frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -
            Name $FIPName -PublicIpAddress $publicIP1

        $BEPool = "LB-backend-Pool"

        $beaddresspool1= New-
            AzureRmLoadBalancerBackendAddressPoolConfig -Name
            $BEPool
```

6. **Erstellen eines Gesundheitstasters**

   Erstellen Sie einen TCP-Integritätstest mit Port 9000 und Intervall 5 Sekunden.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
```

7. **Erstellen einer Lastausgleichsregel**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie Lastenausgleich arbeiten.

   Zum Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst Lastenausgleich zu verwenden.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -
    FrontendPort 80 -BackendPort 80
```

8. **Erstellen eingehender NAT-Regeln**

   Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastausgleich haben.

   Zum Beispiel beim Erstellen eines SSH-Zugriffs auf eine NetScaler VPX Instanz.

   > **Hinweis:**
   >
   > Das Tripel Protokoll-FrontEndPort-BackendPort darf für zwei NAT-Regeln nicht identisch

sein.

```
$inboundNATRule1= New-
    AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1
        -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-
    AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 -
    FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
```

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer und fügen Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Probe-Konfigurationen) zusammen.

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -
    Name $lbName -Location $locName -InboundNatRule
    $inboundNATRule1, $inboundNATRule2 -FrontendIpConfiguration
    $frontendIP1 -LoadBalancingRule $lbrule1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe
```

10. **Erstellen einer Netzwerkkarte**

    Erstellen Sie zwei Netzwerkkarten und verknüpfen Sie jede Netzwerkkarte mit jeder VPX-Instanz

    a) NIC1 mit VPX1

    Zum Beispiel:

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

\* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

\* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic1=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
```



```
        BackendAddressPools\[$bePoolIndex\] -
        LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
        \]
```

b) NIC2 mit VPX2

Zum Beispiel:

```
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. **Erstellen von NetScaler VPX-Instanzen**

    Erstellen Sie zwei NetScaler VPX-Instanzen als Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe und hängen Sie sie an den externen Load Balancer an.

    a) NetScaler VPX-Instanz 1

    Zum Beispiel:

```
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
```



```
$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
     -Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds1/" + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
    $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
```

b) NetScaler VPX-Instanz 2

Zum Beispiel:

```
$vmName="VPX2"

$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

```



```
$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
    -Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
   vhds2/" + $diskName  + ".vhd"

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
   $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
   $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
   $vm2
```

12. **Konfigurieren der virtuellen Maschinen**

    Wenn beide NetScaler VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden NetScaler VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Active-Active: Führen Sie dieselben Konfigurationsbefehle auf der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    b) Active-Passive: Führen Sie diesen Befehl in der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    ```
    add ha node #nodeID <nsip of other NetScaler VPX>
    ```

    Führen Sie im Aktiv-Passiv-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

Stellen Sie ein NetScaler VPX-Paar in einem Hochverfügbarkeits-Setup mit dem internen Azure-Load Balancer bereit

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Erstellen einer Ressourcengruppe**

   Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancer dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="\\&#060;resource group name\\&#062;"

   $locName="\\&#060;location name, such as West US\\&#062;"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```


Zum Beispiel:

```
$rgName = "ARM-LB-NS"

$locName = "West US"

New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

   ```
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
   $rgName -Type $saType -Location $locName
   ```

   Zum Beispiel:

   ```
   $saName="vpxstorage"

   $saType="Standard_LRS"

   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
      $rgName -Type $saType -Location $locName
   ```

3. **Erstellen eines Verfügbarkeitssatzes**

   Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
   $rgName -Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

   ```
   $vnetName = "LBVnet"

   $vnetAddressPrefix="10.0.0.0/16"

   $FrontendAddressPrefix="10.0.1.0/24"

   $BackendAddressPrefix="10.0.2.0/24"

   ```



```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -
    ResourceGroupName $rgName -Location $locName -AddressPrefix
    $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet\`

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
```

> **Hinweis:**
>
> Wählen Sie den Parameterwert AddressPrefix entsprechend Ihren Anforderungen.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Erstellen eines Backend-Adresspool**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -
Name "LB-backend"
```

6. **Erstellen von NAT-Regeln**

   Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastausgleich haben.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
    Protocol TCP -FrontendPort 3441 -BackendPort 3389

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol
    TCP -FrontendPort 3442 -BackendPort 3389
```

   Verwenden Sie Front-End-und Back-End-Ports nach Ihren Anforderungen.

7. **Erstellen eines Gesundheitstasters**

   Erstellen Sie einen TCP-Integritätstest mit Port 9000 und Intervall 5 Sekunden.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
    HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5
     -ProbeCount 2
```

8. **Erstellen einer Lastausgleichsregel**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie Lastenausgleich arbeiten.

Beispiel:

Sie können das folgende Beispiel verwenden, um den HTTP-Dienst Lastenausgleich zu verwenden.

```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -
    FrontendPort 80 -BackendPort 80
```

Verwenden Sie Front-End-und Back-End-Ports nach Ihren Anforderungen.

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer und fügen Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Probe-Konfigurationen) zusammen.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -
    Name "InternalLB" -Location $locName -FrontendIpConfiguration
     $frontendIP -InboundNatRule $inboundNATRule1,
    $inboundNatRule2 -LoadBalancingRule $lbrule -
    BackendAddressPool $beAddressPool -Probe $healthProbe
```

10. **Erstellen einer Netzwerkkarte**

    Erstellen Sie zwei Netzwerkkarten und ordnen Sie jede Netzwerkkarte jeder NetScaler VPX-Instanz zu

```
$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\[0\]
```

    Diese Netzwerkkarte ist für NetScaler VPX 1. Die Private IP muss sich im selben Subnetz befinden wie die des hinzugefügten Subnetzes.

```
$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
    \[1\].
```

    Diese NIC ist für NetScaler VPX 2. Der Parameter `Private IPAddress` kann jede private IP gemäß Ihrer Anforderung haben.

11. **Erstellen von NetScaler VPX-Instanzen**

    Erstellen Sie zwei VPX-Instanzen, die Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe sind, und fügen Sie sie dem internen Lastausgleichsdienst hinzu.

a) NetScaler VPX-Instanz 1

Zum Beispiel:

```
$vmName="VPX1"

$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be
    used to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
     -Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds1/" + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
    $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
```

b) NetScaler VPX-Instanz 2

Zum Beispiel:

```
$vmName="VPX2"

$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$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() + "
        vhds2/" + $diskName  + ".vhd"
22
23  $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25  Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
        $offerName -Name $skuName
26
27  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm2
```

12. **Konfigurieren der virtuellen Maschinen**

    Wenn beide NetScaler VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden NetScaler VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Active-Active: Führen Sie dieselben Konfigurationsbefehle auf der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    b) Active-Passive: Führen Sie diesen Befehl in der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    ```
    add ha node #nodeID <nsip of other NetScaler VPX>
    ```

    Führen Sie im Aktiv-Passiv-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

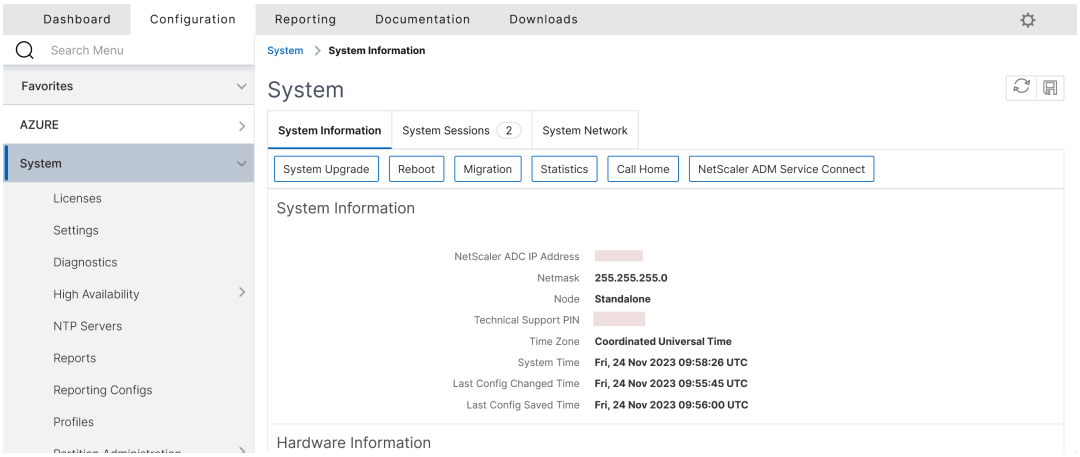
Create a support ticket for the VPX instance on Azure

April 23, 2024

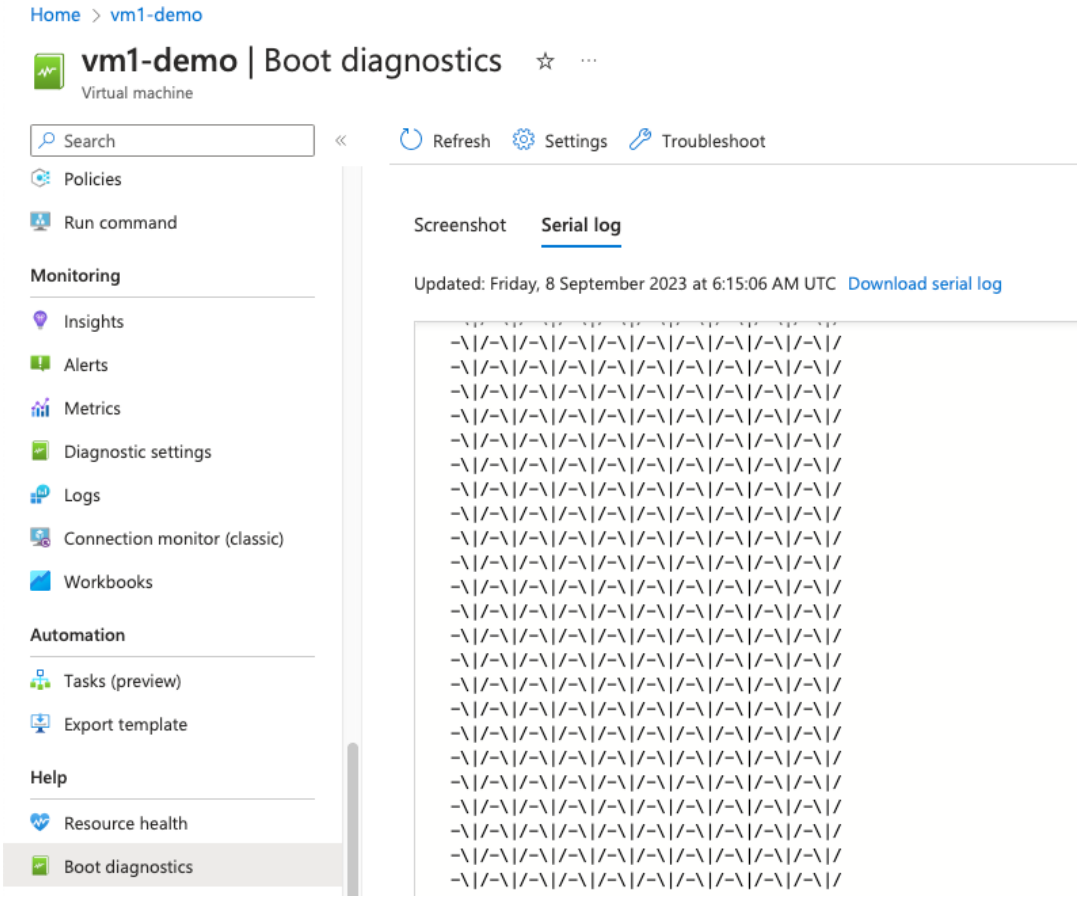
If you're experiencing issues with your NetScaler VPX instance on Azure, for troubleshooting, you can create a support ticket in the NetScaler support portal.

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.

Häufig gestellte Fragen zu Azure

October 17, 2024

- **Unterscheidet sich das Upgrade-Verfahren der im Azure Marketplace installierten NetScaler VPX-Instanz vom on-premises Upgrade-Verfahren?**

  Nein. Sie können Ihre NetScaler VPX-Instanz in der Microsoft Azure-Cloud mithilfe der standardmäßigen NetScaler VPX-Upgrade-Verfahren auf NetScaler VPX Version 11.1 oder höher aktualisieren. Sie können das Upgrade entweder mithilfe von GUI- oder CLI-Verfahren durchführen. Verwenden Sie für neue Installationen das NetScaler VPX Image für die Microsoft Azure-Cloud.

Um die NetScaler VPX-Upgrade-Builds herunterzuladen, gehen Sie zu NetScaler Downloads > NetScaler Firmware**.**

- **Wie korrigiert man MAC-Bewegungen und Interface-Stummutes, die auf NetScaler VPX-Instanzen auf Azure gehostet werden?**

  In der Azure Multi-NIC-Umgebung zeigen alle Datenschnittstellen standardmäßig MAC-Bewegungen und Schnittstellenstummschaltung an. Um MAC-Verschiebungen und Schnittstellen-Stummschaltung in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden.

  Weitere Informationen finden Sie im Artikel CTX224626 .

Bereitstellen einer NetScaler VPX Instanz auf der Google Cloud Platform

October 17, 2024

Sie können eine NetScaler VPX-Instanz auf der Google Cloud Platform (GCP) bereitstellen. Mit einer VPX-Instanz in GCP können Sie die Vorteile der GCP-Cloud-Computing-Funktionen nutzen und Citrix Load Balancing und Traffic-Management-Funktionen für Ihre geschäftlichen Anforderungen nutzen. Sie können VPX-Instanzen in GCP als eigenständige Instanzen bereitstellen. Sowohl einzelne NIC- als auch Multi-NIC-Konfigurationen werden unterstützt.

Unterstützte Features

Alle Premium-, Advanced- und Standardfunktionen werden auf der GCP basierend auf dem verwendeten Lizenz-/Versionstyp unterstützt.

Einschränkung

- IPv6 wird nicht unterstützt.

Hardwareanforderungen

Die VPX-Instanz in GCP muss mindestens 2 vCPUs und 4 GB RAM haben.

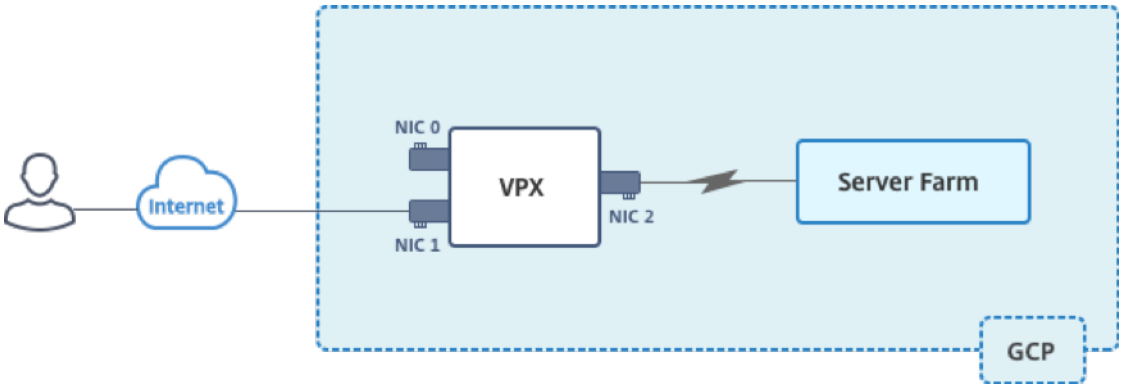
Punkte zu beachten

Berücksichtigen Sie die folgenden GCP-spezifischen Punkte, bevor Sie mit der Bereitstellung beginnen.

- Nach dem Erstellen der Instanz können Sie keine Netzwerkschnittstellen hinzufügen oder entfernen.
- Erstellen Sie für eine Multi-NIC-Bereitstellung separate VPC-Netzwerke für jede Netzwerkkarte. Eine Netzwerkkarte kann nur mit einem Netzwerk verknüpft werden.
- Für eine Single-NIC-Instanz erstellt die GCP-Konsole standardmäßig ein Netzwerk.
- Für eine Instanz mit mehr als zwei Netzwerkschnittstellen sind mindestens 4 vCPUs erforderlich.
- Wenn IP-Weiterleitung erforderlich ist, müssen Sie die IP-Weiterleitung aktivieren, während Sie die Instanz erstellen und die Netzwerkkarte konfigurieren.

Szenario: Bereitstellung einer eigenständigen NetScaler VPX-Instanz mit mehreren Netzwerkkarten und mehreren IPs

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-Instanz in GCP bereitgestellt wird. In diesem Szenario erstellen Sie eine eigenständige VPX-Instanz mit vielen NICs. Die Instanz kommuniziert mit Back-End-Servern (der Serverfarm).



Erstellen Sie drei NICs, um den folgenden Zwecken zu dienen.

Netzwerkkarte	Zweck	Verbunden mit VPC-Netzwerk
NIC 0	Dient Verwaltungsdatenverkehr (NetScaler IP)	Management-Netzwerk
NIC 1	Dient clientseitigem Datenverkehr (VIP)	Kunden-Netzwerk

Netzwerkkarte	Zweck	Verbunden mit VPC-Netzwerk
NIC 2	Kommuniziert mit Back-End-Servern (SNIP)	Back-End-Server-Netzwerk

Richten Sie die erforderlichen Kommunikationswege zwischen den folgenden ein:

- NetScaler VPX-Instanz und die Back-End-Server.
- NetScaler VPX-Instanz und die externen Hosts im öffentlichen Internet.

Zusammenfassung der Bereitstellungsschritte

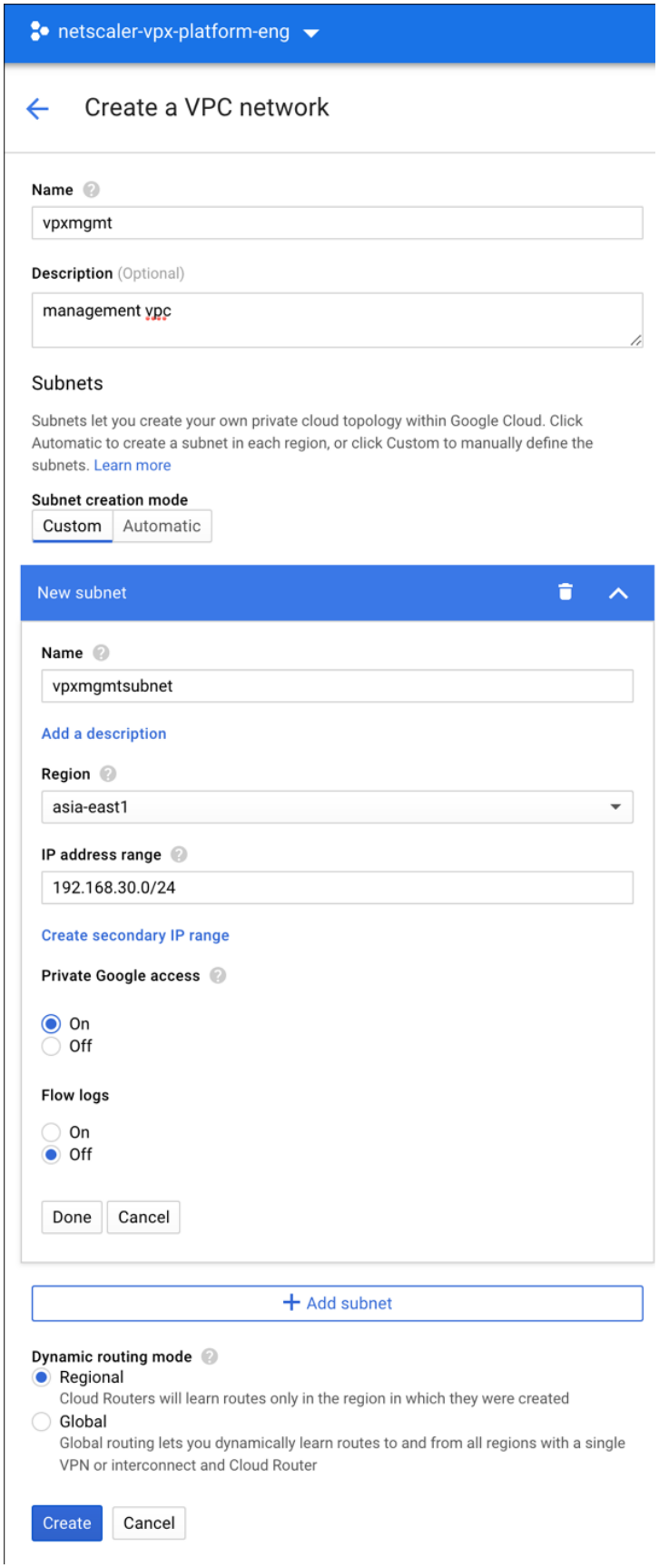
1. Erstellen Sie drei VPC-Netzwerke für drei verschiedene NICs.
2. Schritt 2: Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit drei NICs.

Wählen Sie die NetScaler VPX-Instanz aus dem GCP Marketplace aus.

> **Hinweis:**
>
> Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Fügen Sie der VPX-Instanz Alias-IP-Adressen hinzu.

Erstellen Sie drei VPC-Netzwerke, die mit Verwaltungs-NIC, Client-NIC und Server-NIC verknüpft sind. Um ein VPC-Netzwerk zu erstellen, melden Sie sich bei **Google-Konsole > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**an. Füllen Sie die erforderlichen Felder aus, wie in der Bildschirmaufnahme gezeigt, und klicken Sie auf **Erstellen**.

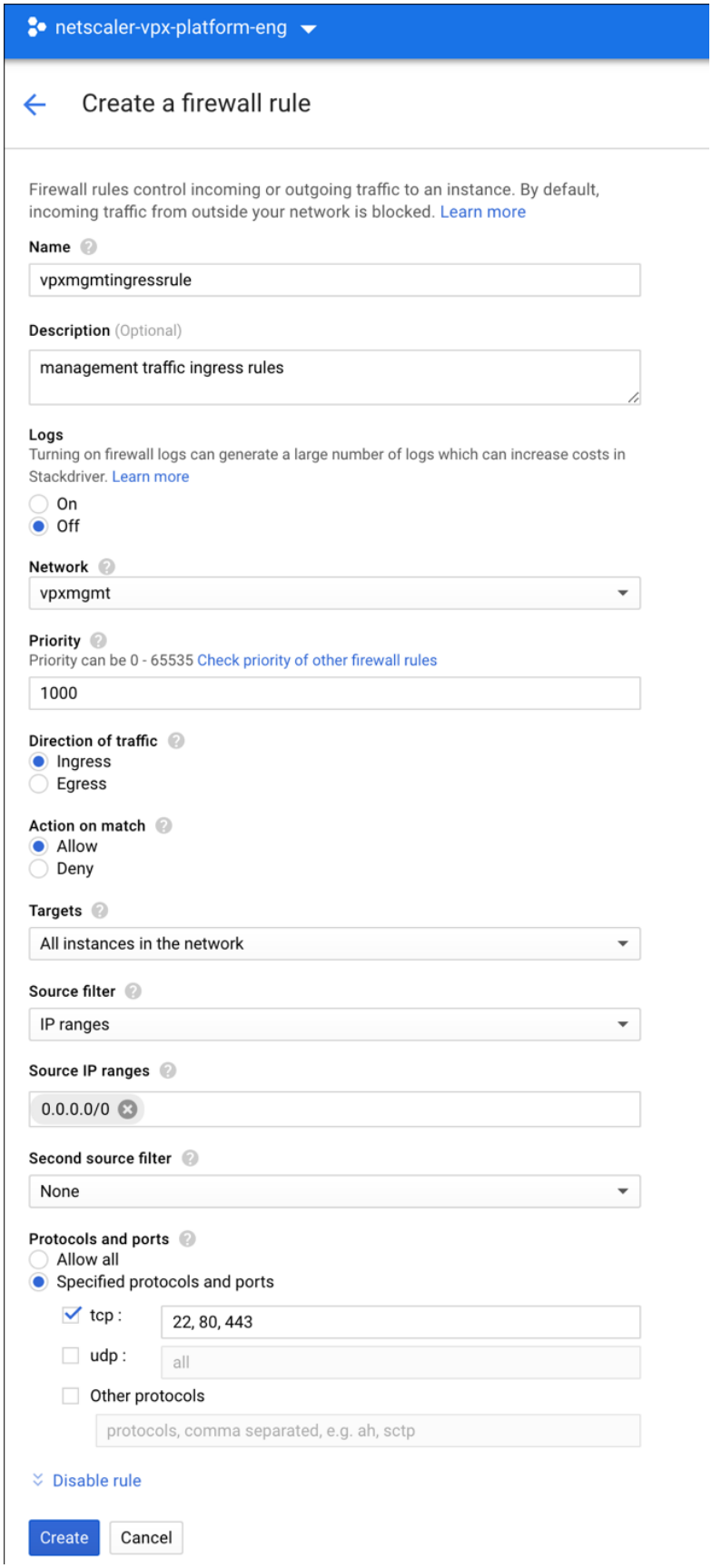


Erstellen Sie in ähnlicher Weise VPC-Netzwerke für client- und serverseitige Netzwerkkarten.

> **Hinweis:**
>
> Alle drei VPC-Netzwerke müssen sich in derselben Region befinden, die in diesem Szenario asia-east1 ist.

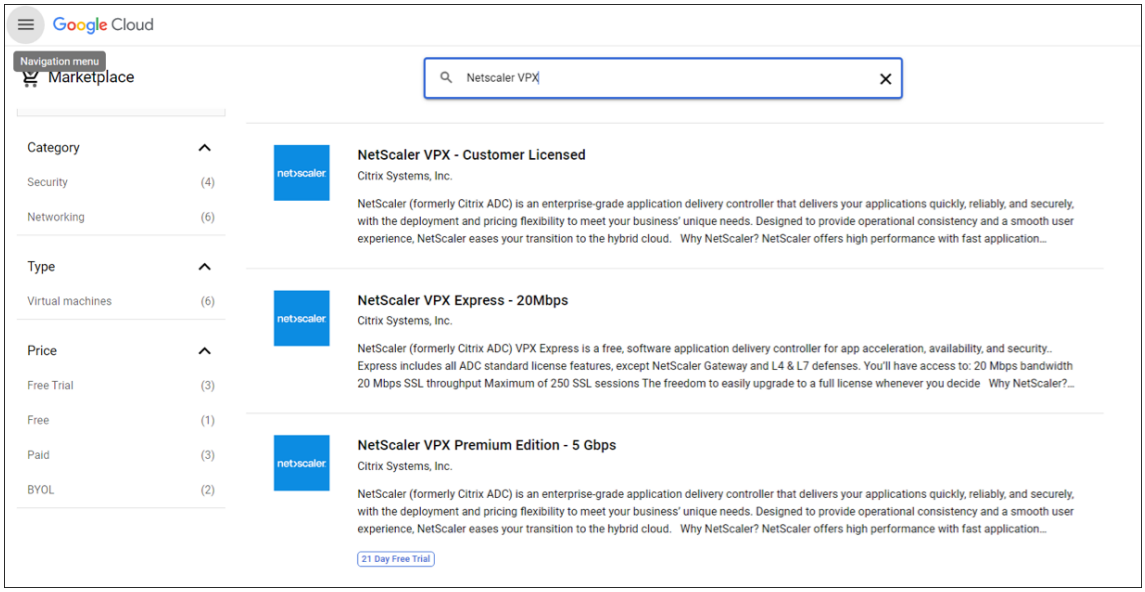
Schritt 2. Schritt 2: Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für jedes VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.

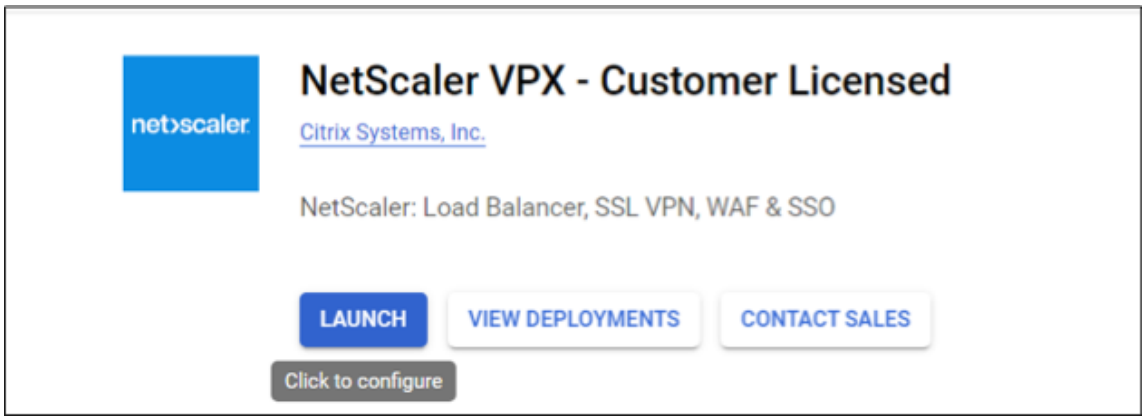


Schritt 3. Fügen Sie VIP und SNIP in der VPX-Instanz hinzu.

1. Melden Sie sich an der GCP-Konsole an.
2. Navigieren Sie zum GCP Marketplace.
3. Wählen Sie ein Abonnement aus, das Ihren Anforderungen entspricht.



4. Klicken Sie für das ausgewählte Abonnement auf **Starten**.



5. Füllen Sie das Bereitstellungsformular aus und klicken Sie auf **Bereitstellen**.

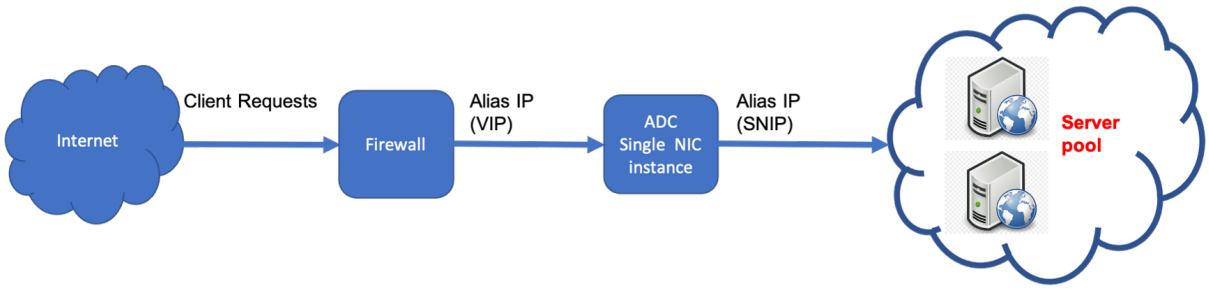
> **Hinweis:**
>
> Verwenden Sie die in **Schritt 1**erstellten VPC-Netzwerke.

6. Die bereitgestellte Instanz wird unter **Compute Engine > VM-Instanzen** angezeigt.

   Verwenden Sie die GCP SSH oder die serielle Konsole, um die VPX-Instanz zu konfigurieren und zu verwalten.

Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzigen NIC

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-Instanz mit einer einzigen Netzwerkkarte in GCP bereitgestellt wird. Die Alias-IP-Adressen werden verwendet, um diese Bereitstellung zu erreichen.



Erstellen Sie eine einzelne NIC (NIC0) für folgende Zwecke:

- Behandeln Sie den Verwaltungsdatenverkehr (NetScaler IP) im Verwaltungsnetzwerk.
- Behandeln Sie clientseitigen Datenverkehr (VIP) im Clientnetzwerk.
- Kommunizieren Sie mit Back-End-Servern (SNIP) im Back-End-Server-Netzwerk.

Richten Sie die erforderlichen Kommunikationswege zwischen den folgenden ein:

- Instanz und die Back-End-Server.
- Instanz und die externen Hosts im öffentlichen Internet.

Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie ein VPC-Netzwerk für NIC0.
2. Schritt 2: Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit einer einzigen NIC.
4. Fügen Sie Alias-IP-Adressen zu VPX hinzu.
5. Fügen Sie VIP und SNIP auf VPX hinzu.
6. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.
7. Fügen Sie der Instanz einen Dienst oder eine Servicegruppe hinzu.
8. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver der Instanz.

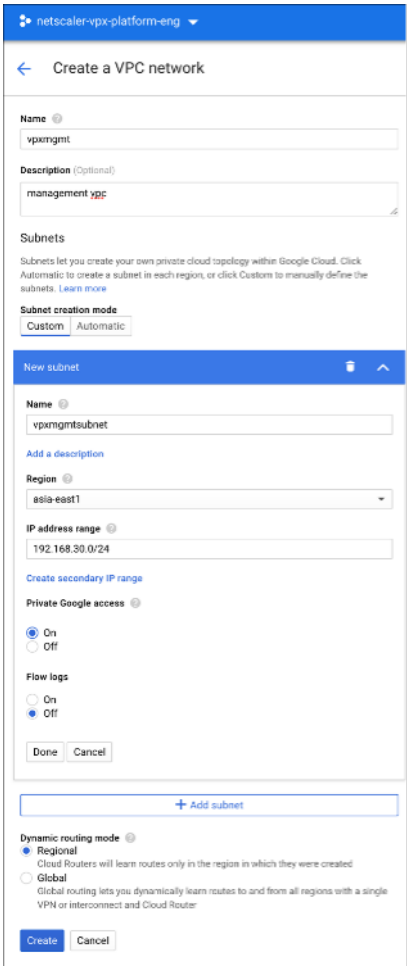
> **Hinweis:**
>
> Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Fügen Sie der VPX-Instanz einen Dienst oder eine Dienstgruppe hinzu.

Erstellen Sie ein VPC-Netzwerk, das Sie mit NIC0 verknüpfen möchten.

Gehen Sie folgendermaßen vor, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei **GCP Console an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.



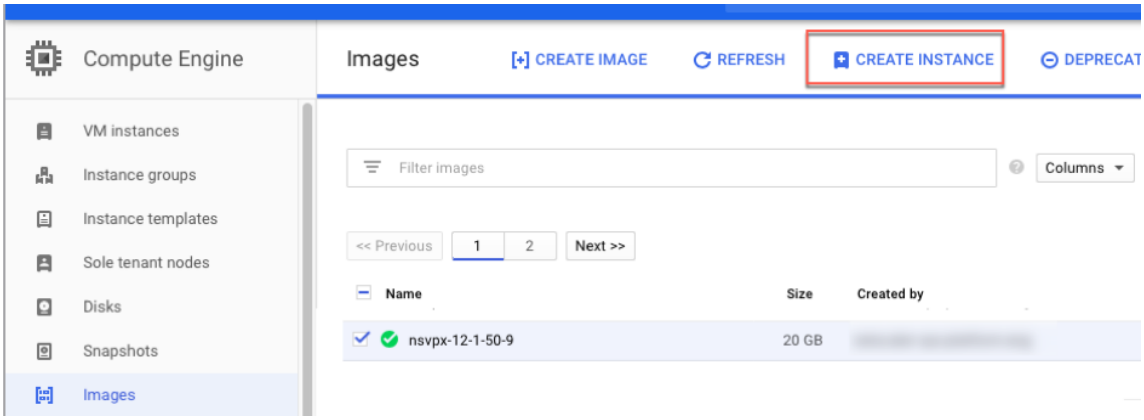
Schritt 2. Schritt 2: Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für das VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.

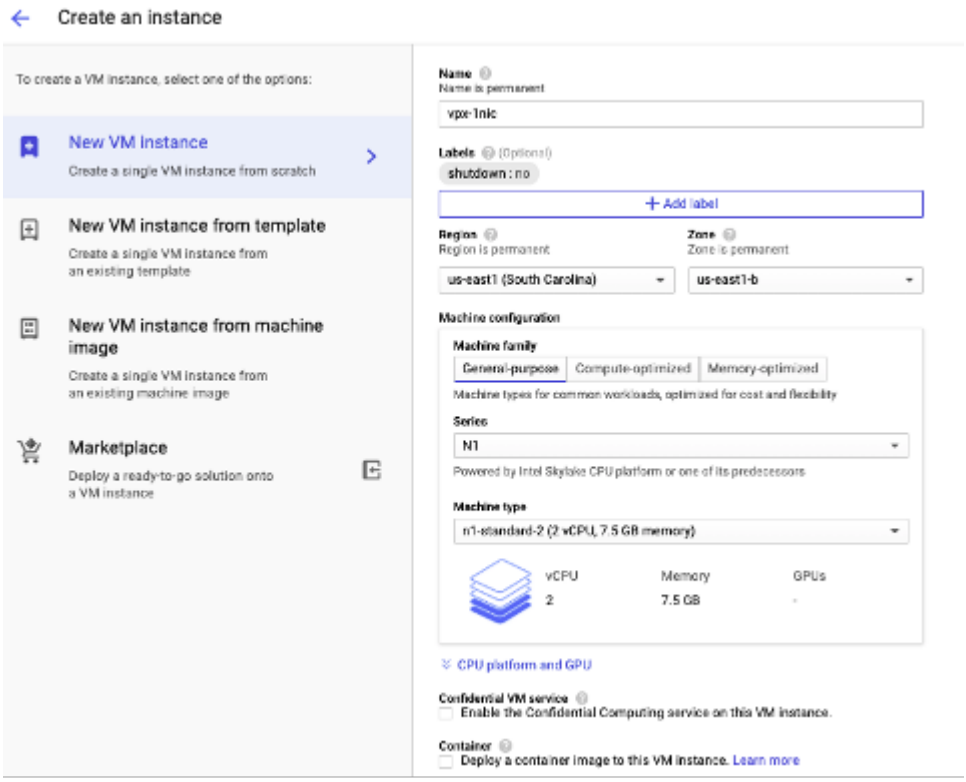
Schritt 3. Schritt 3: Erstellen Sie eine Instanz mit einer einzelnen NIC.

Gehen Sie folgendermaßen vor, um eine Instanz mit einer einzelnen NIC zu erstellen:

1. Melden Sie sich an der **GCP-Konsole** an.
2. Zeigen Sie unter **Compute** mit der Maus auf **Compute Engine** und wählen Sie **Images** aus.
3. Wählen Sie das Image aus und klicken Sie auf **Instanz erstellen**.



4. Wählen Sie einen Instanztyp mit zwei vCPUs aus (Mindestanforderung für ADC).



5. Klicken Sie im Fenster **Verwaltung, Sicherheit, Datenträger, Netzwerk** auf die Registerkarte **Netzwerk**.
6. Klicken Sie unter **Netzwerkschnittstellen** auf das Symbol **Bearbeiten**, um die Standard-Netzwerkkarte zu bearbeiten.
7. Wählen Sie im Fenster **Netzwerkschnittstellen** unter **Netzwerk** das VPC-Netzwerk aus, das Sie erstellt haben.
8. Sie können eine statische externe IP-Adresse erstellen. Klicken Sie unter den **Externen IP-Adressen** auf **IP-Adresse erstellen**.
9. Fügen Sie im Fenster **Statische Adresse reservieren** einen Namen und eine Beschreibung hinzu und klicken Sie auf **Reservieren**.
10. Klicken Sie auf **Erstellen**, um die VPX-Instanz zu erstellen. Die neue Instanz wird unter VM-Instanzen angezeigt.

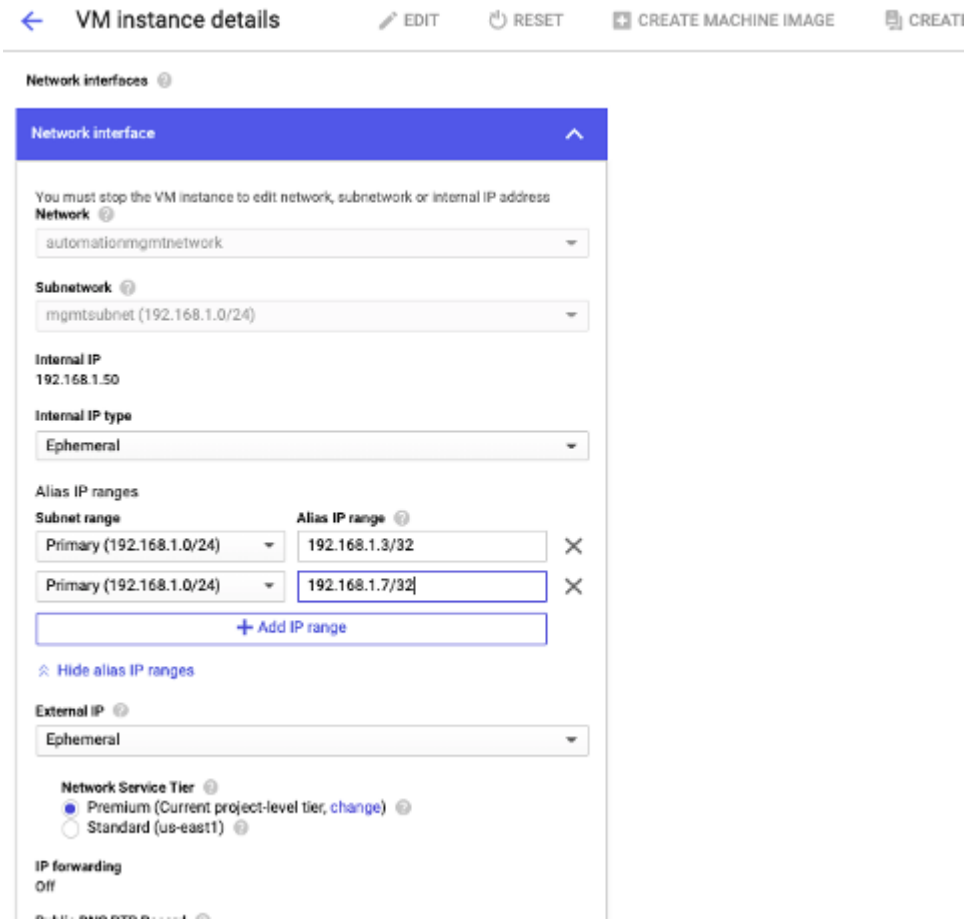
Schritt 4. Fügen Sie der VPX-Instanz Alias-IP-Adressen hinzu.

Weisen Sie der VPX-Instanz zwei Alias-IP-Adressen zu, die als VIP- und SNIP-Adressen verwendet werden sollen.

> **Hinweis:**
>
> Verwenden Sie nicht die primäre interne IP-Adresse der VPX-Instanz, um den VIP oder SNIP zu konfigurieren.

Gehen Sie folgendermaßen vor, um eine Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster der **Netzwerkschnittstelle** die NIC0-Schnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die Alias-IP-Adressen ein.

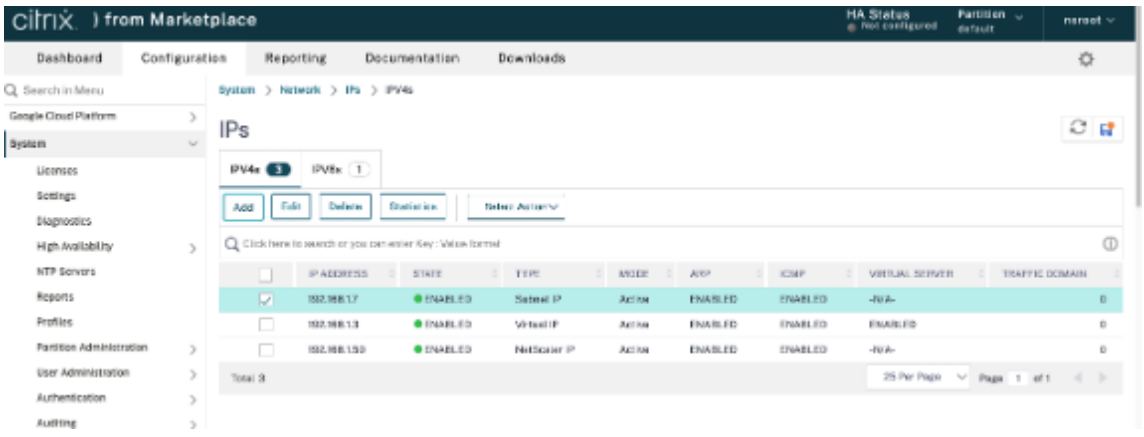


4. Klicken Sie auf **Fertig**und dann auf **Speichern**.
5. Überprüfen Sie die Alias-IP-Adressen auf der **Detailseite der VM-Instanz** .

Schritt 5. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

Fügen Sie in der VPX-Instanz die IP-Adresse des Client-Alias und die IP-Adresse des Serveralias hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **System > Netzwerk > IPs > IPv4s**und klicken Sie auf **Hinzufügen**.



2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):

   - Geben Sie die Client-Alias-IP-Adresse und Netzmaske ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.
   - Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   - Klicken Sie auf **Erstellen**.

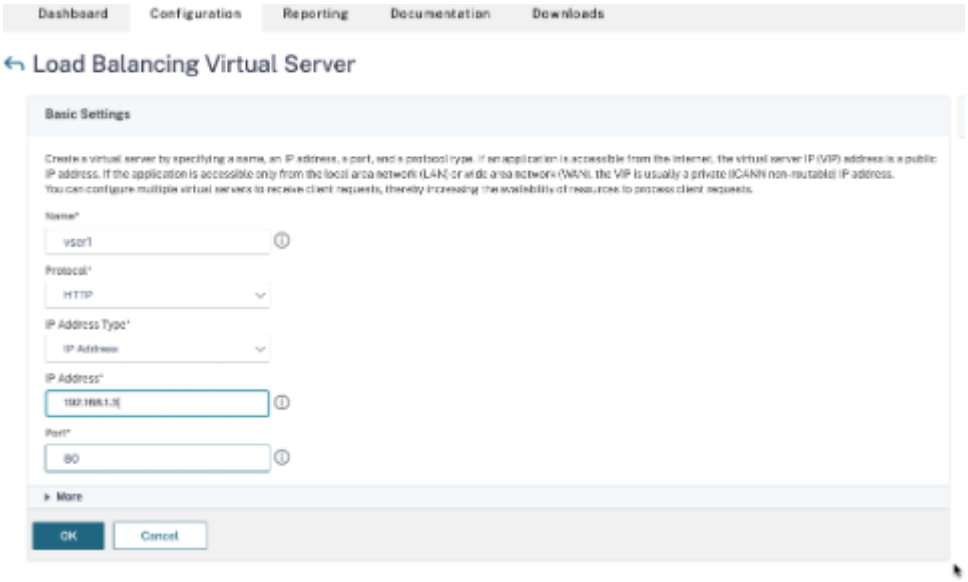
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:

   - Geben Sie die IP-Adresse und Netzmaske des Server-Alias ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.

- Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
- Klicken Sie auf **Erstellen**.

Schritt 6. Binden Sie die Service/Dienstgruppe an den virtuellen Load Balancing Server in der Instanz.

1. Navigieren Sie in der NetScaler-GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Clientalias-IP) und Port hinzu.
3. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.



Schritt 7: Fügen Sie der VPX-Instanz einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **Konfiguration > Traffic Management > Load Balancing > Services**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

Schritt 8: Binden Sie den Dienst/die Dienstgruppe an den virtuellen Lastenausgleichsserver auf der Instanz.

1. Navigieren Sie in der GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 6**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Fenster **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 7**konfigurierten Dienst aus und klicken Sie auf **Binden**.

Hinweise zu beachten, nachdem Sie die VPX-Instanz auf GCP bereitgestellt haben

- Melden Sie sich beim VPX mit Benutzernamen `nsroot` und Instanz-ID als Kennwort an. Ändern Sie an der Eingabeaufforderung das Kennwort und speichern Sie die Konfiguration.
- Um ein Paket für den technischen Support zu sammeln, führen Sie den Befehl `shell /netscaler/showtech_cloud.pl` anstelle des üblichen `show techsupport` aus.
- Löschen Sie nach dem Löschen einer NetScaler VM von der GCP-Konsole auch die zugehörige interne Zielinstanz von NetScaler. Gehen Sie dazu zur gcloud CLI und geben Sie den folgenden Befehl ein:

```
gcloud compute -q  target-instances delete <instance-name>-
   adcinternal --zone <zone>
```

> **Hinweis:**
>
> <instance-name>-adcinternal ist der Name der Zielinstanz, die gelöscht werden muss.

NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz auf GCP benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf GCP ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: NetScaler VPX Appliances sind als kostenpflichtige Instanzen auf dem GCP-Marktplatz verfügbar. Abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet. Die folgenden VPX-Modelle und Lizenz-Editionen sind auf dem GCP-Marktplatz verfügbar.

Unterstützte VPX-Leistung
NetScaler VPX Advanced – 200 Mbit/s
NetScaler VPX Premium –1 Gbit/s
NetScaler VPX Premium –5 Gbit/s
NetScaler VPX Express –20 Mbit/s
NetScaler VPX –Kundenlizenz
NetScaler VPX FIPS –Kundenlizenz

- **Bringen Sie Ihre eigene Lizenz (BYOL) mit**: Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, finden Sie weitere Informationen im VPX-Lizenzierungsleitfaden unter http://support.citrix.com/article/CTX122426. Sie müssen:

  - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.

- **NetScaler VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter NetScaler VPX Check-In/Auschecken Lizenzierung.

VPX Express für lokale und Cloud-Bereitstellungen erfordert keine Lizenzdatei. Weitere Informationen zu NetScaler VPX Express finden Sie im Abschnitt "NetScaler VPX Express-Lizenz"in der Übersicht über die NetScaler Lizenzierung.

GDM-Vorlagen zur Bereitstellung einer NetScaler VPX-Instanz

Sie können eine NetScaler VPX Google Deployment Manager (GDM) -Vorlage verwenden, um eine VPX-Instanz auf GCP bereitzustellen. Weitere Informationen finden Sie unter NetScaler GDM Templates.

NetScaler Marketplace-Images

Sie können die Images in GDM-Vorlagen verwenden, um die NetScaler-Appliance aufzurufen.

In der folgenden Tabelle sind die Images aufgeführt, die auf dem GCP Marketplace verfügbar sind.

Release	Imagename	Imageort
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

Release	Imagename	Imageort
14.1	citrix-adc-vpx-byol-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-14-1-21-57

Ressourcen

- Erstellen von Instanzen mit mehreren Netzwerkschnittstellen
- Erstellen und Starten einer VM-Instanz

Verwandte Informationen

- Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform

Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform

October 17, 2024

Sie können zwei NetScaler VPX-Instanzen auf der Google Cloud Platform (GCP) als aktives und passives Paar mit hoher Verfügbarkeit (HA) konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Die Knoten müssen sich in derselben Region befinden; sie können sich jedoch entweder in derselben Zone oder in verschiedenen Zonen befinden. Weitere Informationen finden Sie unter Regionen und Zonen.

Jede VPX-Instanz benötigt mindestens drei IP-Subnetze (Google VPC-Netzwerke):

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Backend-Subnetz (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz.

Sie können ein VPX-Hochverfügbarkeitspaar mit den folgenden Methoden bereitstellen:

- Verwendung externer statischer IP-Adresse
- Private IP-Adresse verwenden
- Verwendung von Single-NIC-VMs mit privater IP-Adresse

GDM-Vorlagen zum Bereitstellen eines VPX-Hochverfügbarkeitspaars auf GCP

Sie können eine NetScaler Google Deployment Manager (GDM) -Vorlage verwenden, um ein VPX-Hochverfügbarkeitspaar auf GCP bereitzustellen. Weitere Informationen finden Sie unter NetScaler GDM Templates.

Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP

Sie können ein VPX Hochverfügbarkeitspaar auf dem GCP mithilfe von Weiterleitungsregeln bereitstellen.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Voraussetzungen

- Die Weiterleitungsregeln müssen sich in derselben Region wie die VPX-Instanzen befinden.
- Zielinstanzen müssen sich in derselben Zone wie die VPX-Instanz befinden.
- Die Anzahl der Zielinstanzen für primäre und sekundäre Knoten muss übereinstimmen.

Beispiel

Sie haben ein hochverfügbarkeitsstarkes Paar in der `us-east1` Region mit primärem VPX in `us-east1-b` Zone und sekundärem VPX in `us-east1-c` Zone. Eine Weiterleitungsregel wird für den primären VPX mit der Zielinstanz in `us-east1-b` Zone konfiguriert. Konfigurieren Sie eine Zielinstanz für die sekundäre VPX in `us-east1-c` Zone, um die Weiterleitungsregel bei Failover zu aktualisieren.

Einschränkungen

In der Hochverfügbarkeitsbereitstellung von VPX werden nur Weiterleitungsregeln unterstützt, die mit Zielinstanzen am Backend konfiguriert sind.

Stellen Sie ein VPX Hochverfügbarkeitspaar mit externer statischer IP-Adresse auf der Google Cloud Platform bereit

October 17, 2024

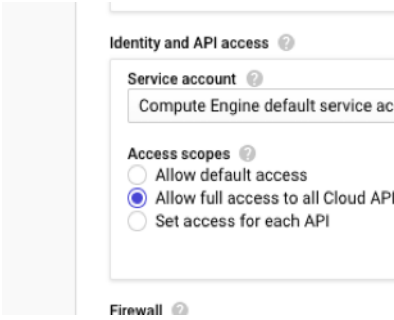
Sie können ein VPX-Paar mit hoher Verfügbarkeit auf GCP mit einer externen statischen IP-Adresse bereitstellen. Die Client-IP-Adresse des primären Knotens muss an eine externe statische IP-Adresse gebunden sein. Beim Failover wird die externe statische IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr fortgesetzt werden kann.

Eine statische externe IP-Adresse ist eine externe IP-Adresse, die für Ihr Projekt reserviert ist, bis Sie es freigeben möchten. Wenn Sie eine IP-Adresse für den Zugriff auf einen Dienst verwenden, können Sie diese IP-Adresse so reservieren, dass nur Ihr Projekt sie verwenden kann. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise unter „Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform“. Diese Informationen gelten auch für HA-Bereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.



- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.
- Stellen Sie sicher, dass die mit Ihrem GCP-Dienstkonto verknüpfte IAM-Rolle die folgenden IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
```



```
    "compute.instances.get",
    "Compute.instances.list",
    "compute.networks.useExternalIp",
    "compute.subnetworks.useExternalIp",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.targetInstances.create",
    "compute.zones.list",
    "compute.zoneOperations.get",
    ]
```

- Wenn Sie Alias-IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
    "compute.instances.updateNetworkInterface"
```

- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die in Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaare auf GCP genannten Einschränkungen und Anforderungen, um sie beim Failover auf den neuen Primärknoten zu aktualisieren.

So stellen Sie ein VPX HA-Paar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der HA-Bereitstellungsschritte:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen über die NetScaler GUI- oder ADC-CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

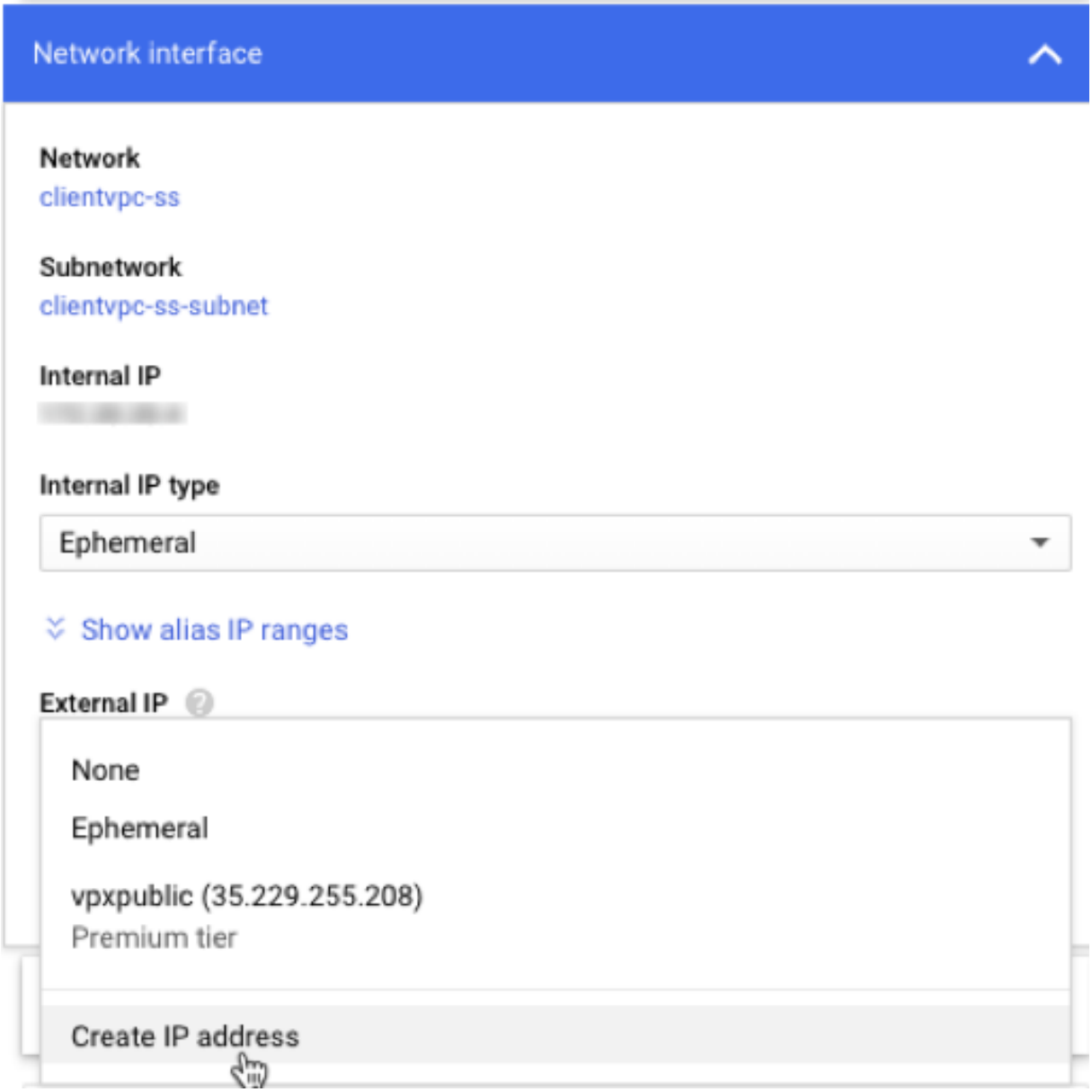
1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **VPC-Netzwerke erstellen** unter Eine NetScaler VPX-Instanz auf Google Cloud Platform bereitstellen.

Schritt 2. Erstellen Sie zwei VPX-Instanzen

Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte in Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPsbefolgen.

> **Wichtig:**
>
> Weisen Sie der Client-IP-Adresse (VIP) des primären Knotens eine statische externe IP-Adresse zu. Sie können eine vorhandene reservierte IP-Adresse verwenden oder eine neue erstellen. Um eine statische externe IP-Adresse zu erstellen, navigieren Sie zu **Netzwerkschnittstelle > Externe IP**und klicken Sie auf **IP-Adresse erstellen**.



Wenn nach dem Failover der alte primäre neue sekundäre wird, wird die statische externe IP-Adresse

von der alten primären IP-Adresse verschoben und an den neuen primären Server angeschlossen. Weitere Informationen finden Sie im Google Cloud-Dokument Reservieren einer statischen externen IP-Adresse.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die VIP- und SNIP-Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie HA über die NetScaler GUI für CLI konfigurieren.

Konfigurieren von HA mit der GUI **Schritt 1.** Fügen Sie einen virtuellen Lastausgleichsserver hinzu. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

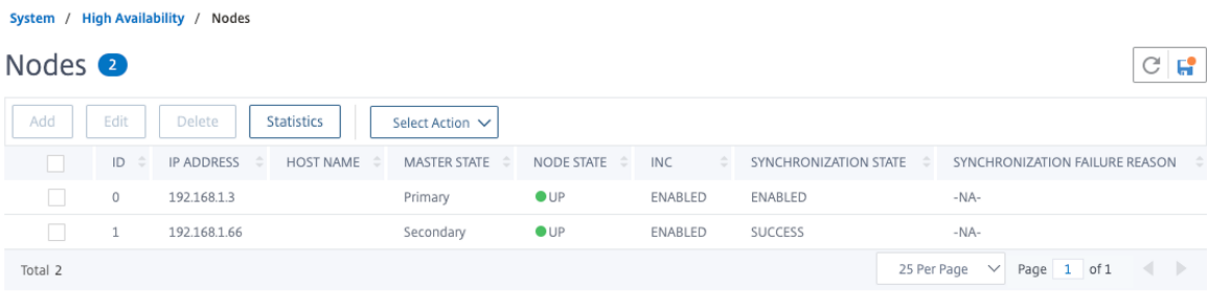
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

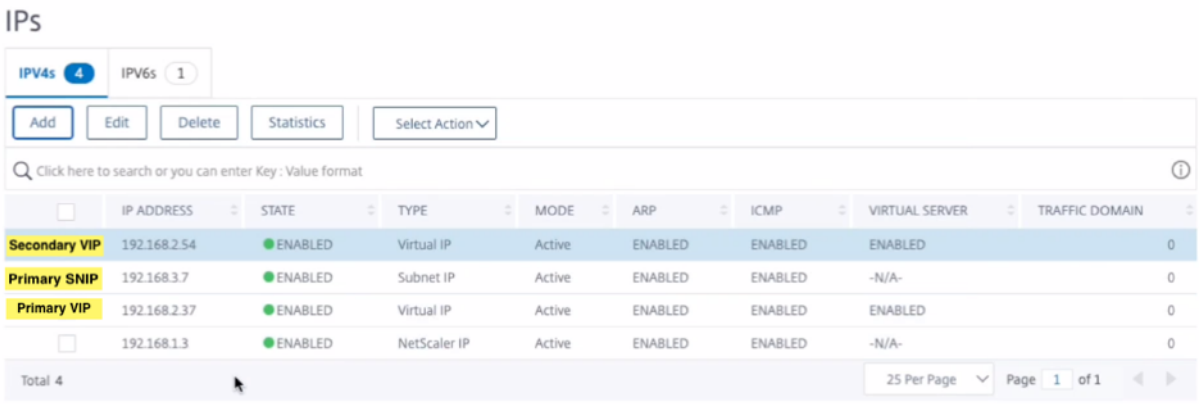


> **Hinweis:**
>
> Jetzt hat der sekundäre Knoten die gleichen Anmeldeinformationen wie der primäre Knoten.

Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen , wählen Sie im Dropdownmenü IPSet**aus und geben Sie das in**Schritt 3**erstellte IPSet ein.

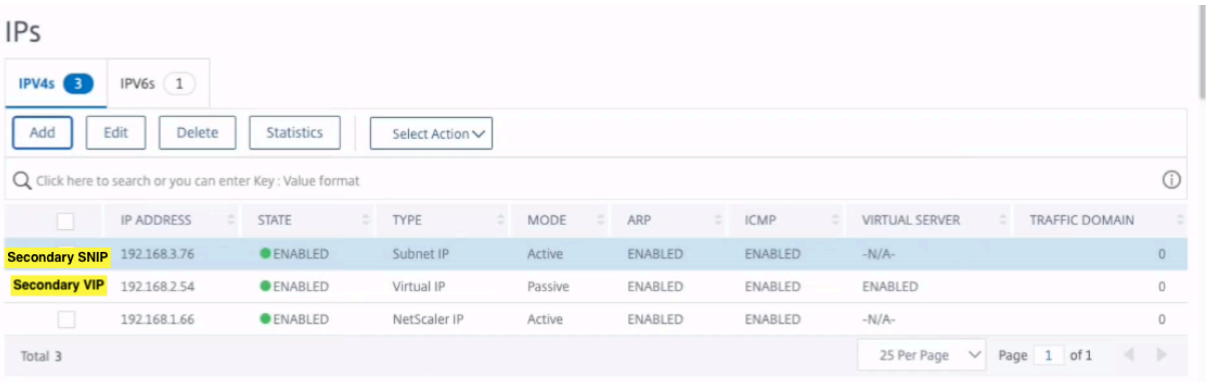
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
    b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz in der primären Instanz konfiguriert ist.
    b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
    b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.



Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz in der sekundären Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.

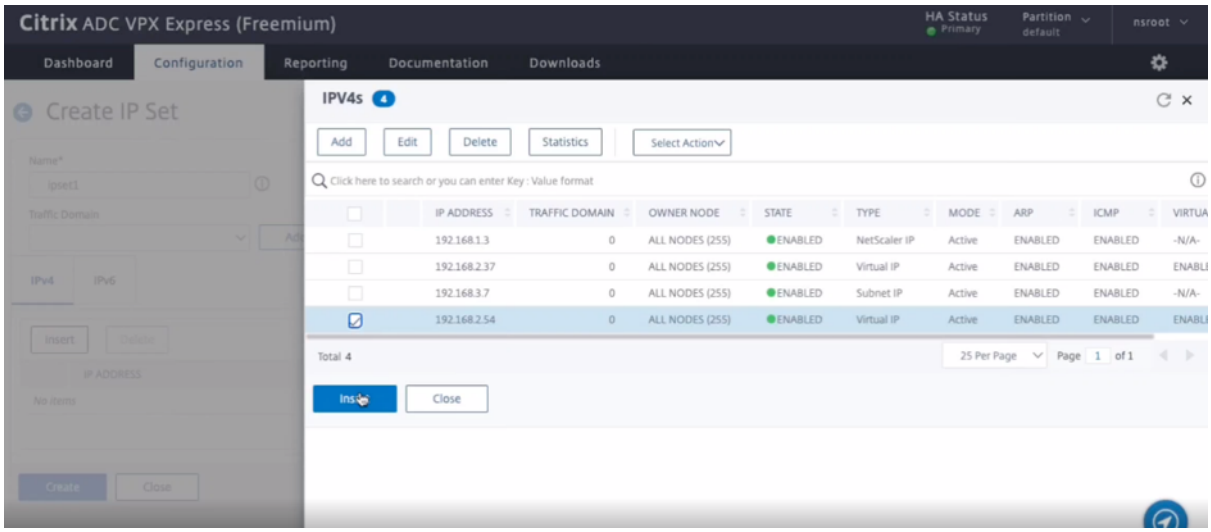


Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. Schritt 3: Fügen Sie IP-Set hinzu und binden Sie die IP, die an den sekundären VIP auf beiden Instanzen festgelegt ist.

Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

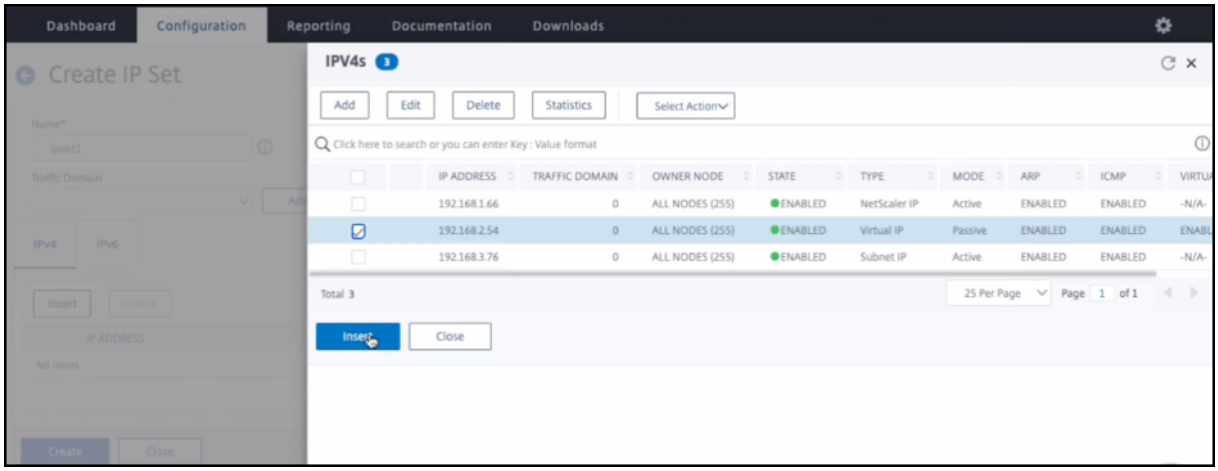
1. **Schritt 2.** Fügen Sie den IP-Satz in beiden Instanzen hinzu.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.

3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

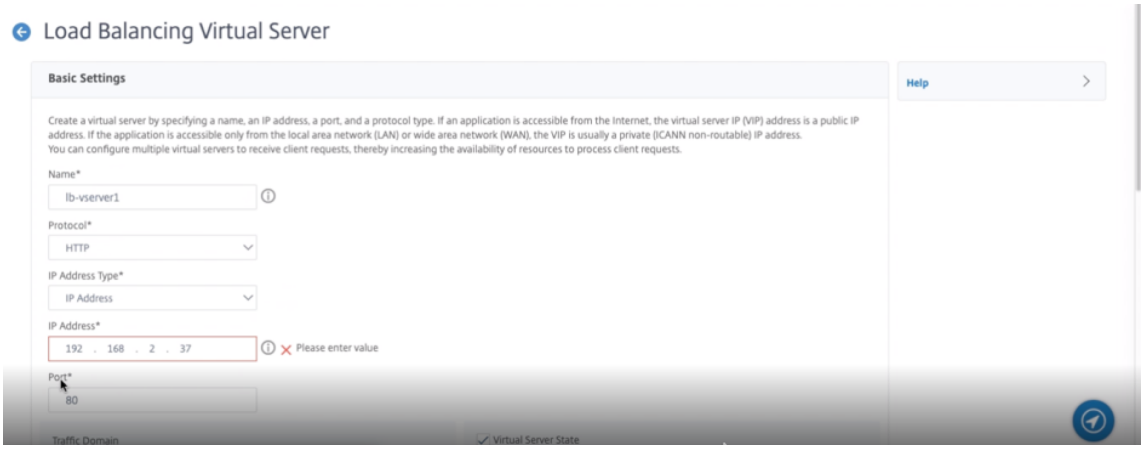
1. **Schritt 2.** Fügen Sie den IP-Satz in beiden Instanzen hinzu.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



> **Hinweis:**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Überprüfen Sie die Konfiguration. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf der primären Instanz.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäres VIP) und Port hinzu.



3. Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen**, wählen Sie im Dropdownmenü **IPset** aus und geben Sie das in **Schritt 3** erstellte IPset ein.
4. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

Schritt 5. Speichern Sie die Konfiguration. **Schritt 5.** Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 6. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 4**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 5**konfigurierten Dienst aus und klicken Sie auf "**Binden**".

Speichern Sie die Konfiguration. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die externe statische IP des alten primären VIP wechselt zum neuen sekundären VIP.

Konfigurieren der Hochverfügbarkeit mit CLI **Schritt 1.** Fügen Sie einen virtuellen Lastausgleichsserver hinzu. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

`prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Klicken Sie auf **Mehr**. **Schritt 2.** Fügen Sie auf beiden Knoten virtuelle und Subnet-IPs hinzu.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz.

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

`primary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

`secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. Fügen Sie einen IP-Satz hinzu und binden Sie ihn an den sekundären VIP auf beiden Instanzen.

Geben Sie auf dem primären Knoten den folgenden Befehl ein:

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
```


Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
1   add ipset <ipsetname>
2   bind ipset <ipsetname> <secondary VIP>
```

> **Hinweis:**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Überprüfen Sie die Konfiguration. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

Geben Sie den folgenden Befehl ein:

```
1   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <
       port> -ipset <ipset_name>
```

Schritt 5. Speichern Sie die Konfiguration. Fügen Sie der primären Instanz einen Dienst oder eine Servicegruppe hinzu.

Geben Sie den folgenden Befehl ein:

```
1   add service <service_name> <service_ip_address> <protocol> <port>
```

Schritt 6. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie die Service/Dienstgruppe an den virtuellen Lastenausgleichsserver auf der primären Instanz.

Geben Sie den folgenden Befehl ein:

```
1   bind <server_type> vserver <vserver_name> <service_name>
```

> **Hinweis:**
>
> Geben Sie den Befehl `save config` ein, um die Konfiguration zu speichern. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Schritt 7. Überprüfen Sie die Konfiguration. Überprüfen Sie die Konfiguration.

Stellen Sie sicher, dass die an die primäre Client-NIC angehängte externe IP-Adresse bei einem Failover zur sekundären IP-Adresse wechselt.

1. Stellen Sie eine cURL-Anfrage an die externe IP-Adresse und stellen Sie sicher, dass sie erreichbar ist.
2. Führen Sie auf der primären Instanz Failover durch:

   Navigieren Sie in der GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.

   Geben Sie in der CLI den folgenden Befehl ein:


```
force ha failover -f
```

Navigieren Sie auf der GCP-Konsole zur sekundären Instanz. Die externe IP-Adresse muss nach dem Failover auf die sekundäre Client-NIC verschoben worden sein.

3. Stellen Sie eine cURL-Anforderung an die externe IP aus und stellen Sie sicher, dass sie wieder erreichbar ist.

Einzelnes NIC-VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereitstellen

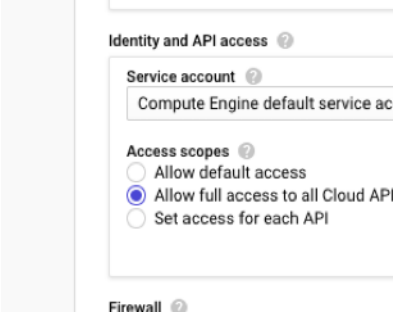
October 17, 2024

Sie können ein einzelnes NIC-VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP-Adresse (VIP) muss als Alias-IP-Adresse auf dem Primärknoten konfiguriert werden. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann. Die Subnetz-IP-Adressen (SNiPs) für jeden Knoten müssen ebenfalls als Alias-IP-Bereich konfiguriert werden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise unter „Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform“. Diese Informationen gelten auch für Bereitstellungen mit hoher Verfügbarkeit.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



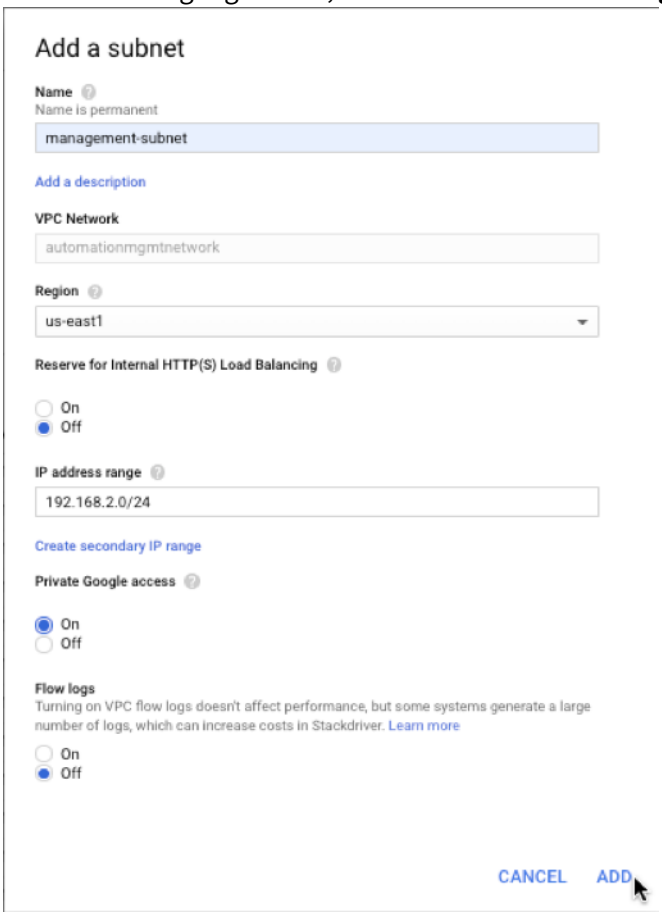
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
```



```
    "compute.forwardingRules.setTarget",
    "compute.instances.setMetadata",
    "compute.instances.get",
    "compute.instances.list",
    "compute.instances.updateNetworkInterface",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.targetInstances.create",
    "compute.zones.list",
    "compute.zoneOperations.get",
    ]
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Private Google Access** im VPC-Subnetz aktivieren.



- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die in Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaare auf GCP genannten Einschränkungen und Anforderungen, um sie beim Failover auf den neuen Primärknoten zu aktualisieren.

So stellen Sie ein VPX Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier finden Sie eine Zusammenfassung der Schritte zur Bereitstellung eines HA-Paars mit einer einzelnen Netzwerkkarte:

1. Fügen Sie der VPX-Instanz einen Dienst oder eine Dienstgruppe hinzu.
2. Erstellen Sie zwei VPX-Instanzen (primärer und sekundärer Knoten) in derselben Region. Sie können sich in derselben Zone oder verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen über die NetScaler GUI- oder ADC-CLI-Befehle.

Schritt 1. Erstellen Sie ein VPC-Netzwerk

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich an der **Google-Konsole an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **VPC-Netzwerke erstellen** unter Eine NetScaler VPX-Instanz auf Google Cloud Platform bereitstellen.

Schritt 2. Erstellen Sie zwei VPX-Instanzen

Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte 1 bis 3 unter Szenario befolgen: Stellen Sie eine eigenständige VPX-Instanz mit einer Netzwerkkartebereit.

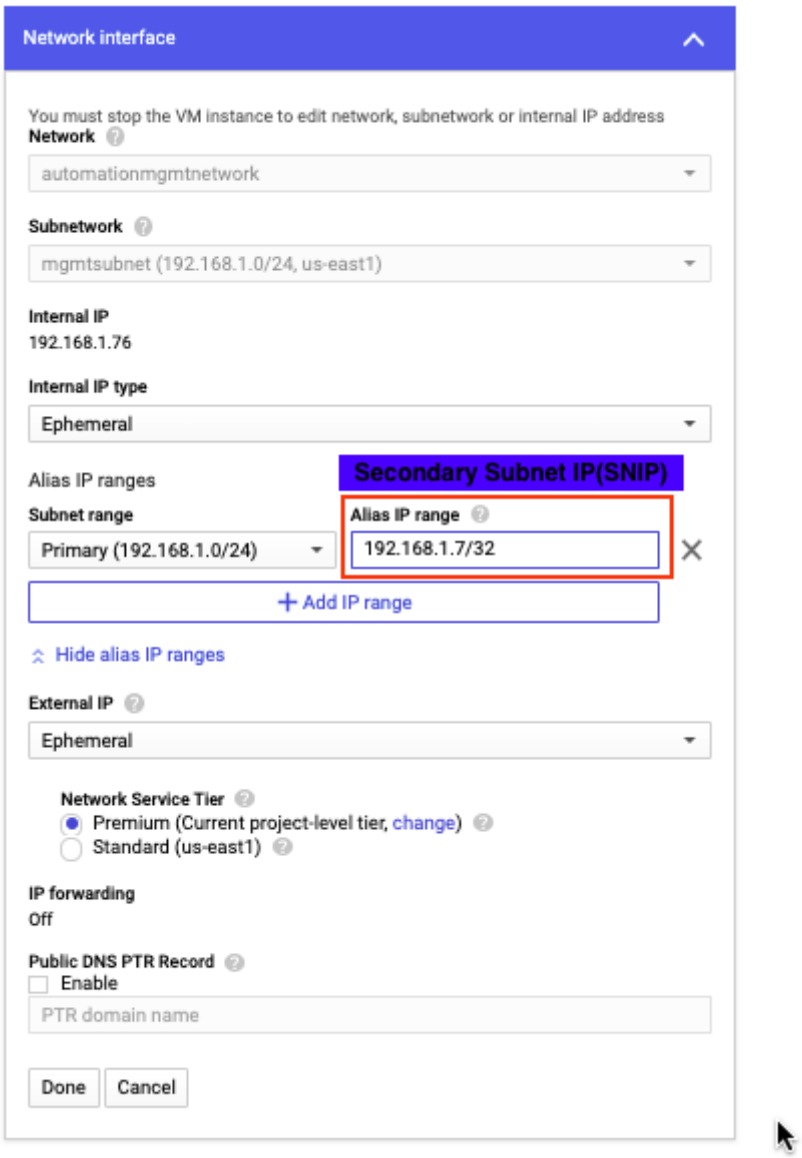
> **Wichtig:**
>
> Weisen Sie nur dem primären Knoten eine Client-Alias-IP-Adresse und primären und sekundären Knoten Server-Alias-IP-Adressen zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um VIP oder SNIP zu konfigurieren.

Gehen Sie auf dem primären Knoten wie folgt vor, um Client- und Server-Alias-IP-Adressen zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias-IP-Bereich** die IP-Adresse des Client-Alias ein.
4. Klicken Sie auf **IP-Bereich hinzufügen** und geben Sie die Server-Alias-IP-Adresse ein.

Gehen Sie auf dem sekundären Knoten wie folgt vor, um eine Serveralias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias-IP-Bereich** die Serveralias-IP-Adresse ein.



Nach dem Failover, wenn der alte primäre zum neuen sekundären wird, wird die Client-Alias-IP-Adresse vom alten primären verschoben und an den neuen primären angehängt.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die Virtual (VIP) und Subnet IP (SNIP) -Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler-GUI oder CLI konfigurieren.

Konfigurieren der Hochverfügbarkeit mit der GUI

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu. **Schritt 1.** Richten Sie die Hochverfügbarkeit im Modus INC Enabled auf beiden Knoten ein.

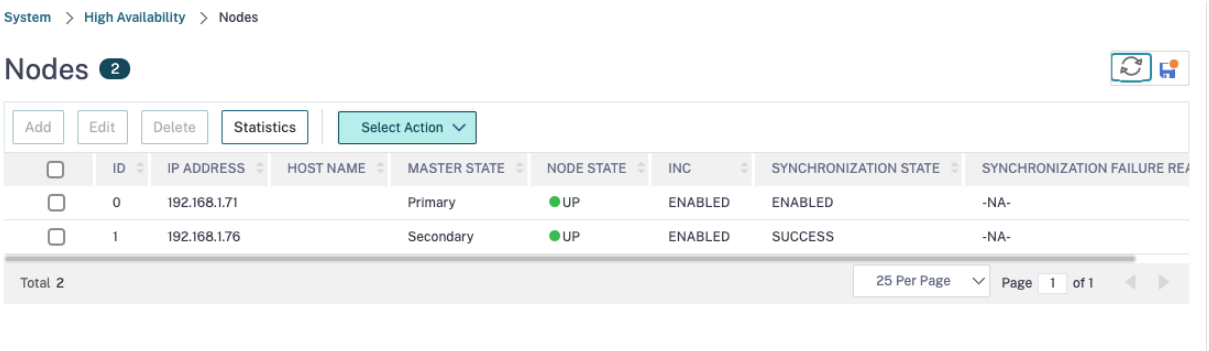
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

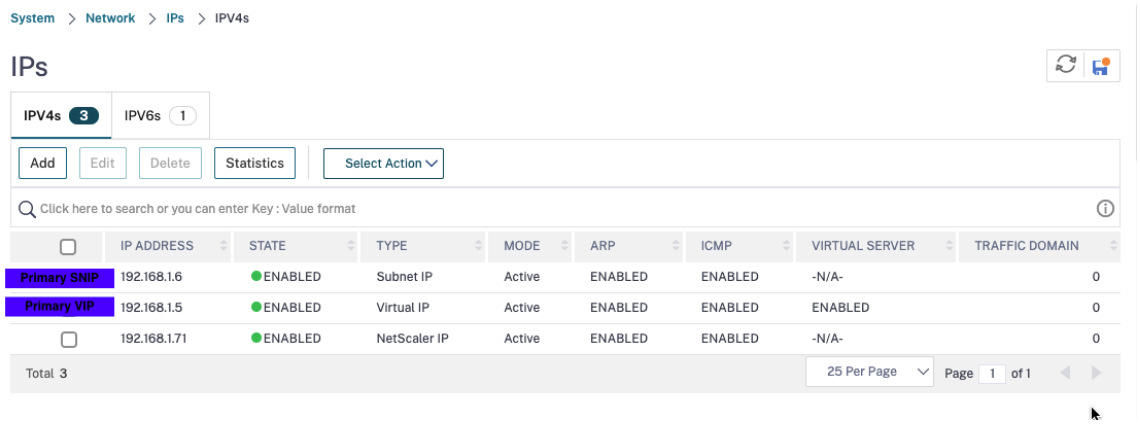


> **Hinweis:**
>
> Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, hat der sekundäre Knoten dieselben Anmeldeinformationen wie der primäre Knoten.

Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen , wählen Sie im Dropdownmenü IPSet**aus und geben Sie das in**Schritt 3**erstellte IPSet ein.

Führen Sie auf dem primären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:
   a) Geben Sie die Serveralias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



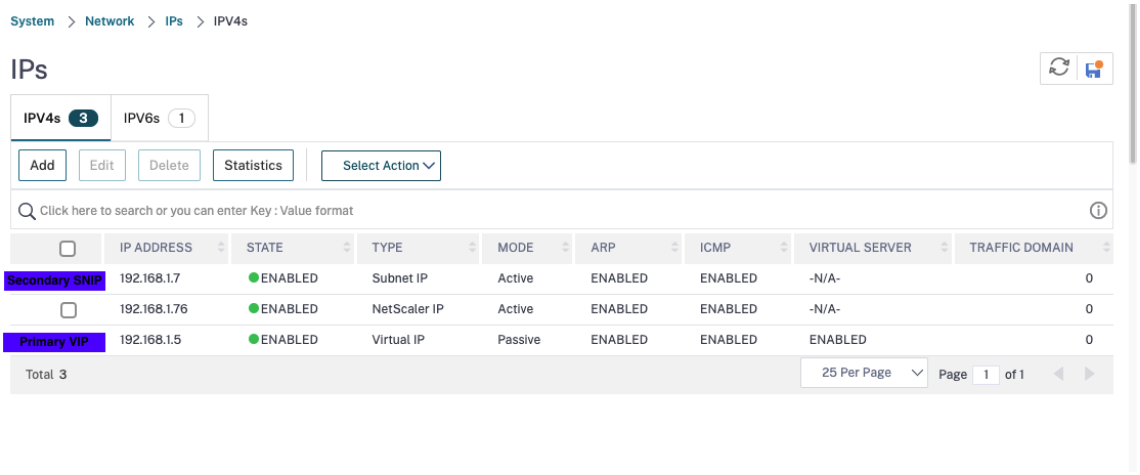
Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.

c) Klicken Sie auf **Erstellen**.

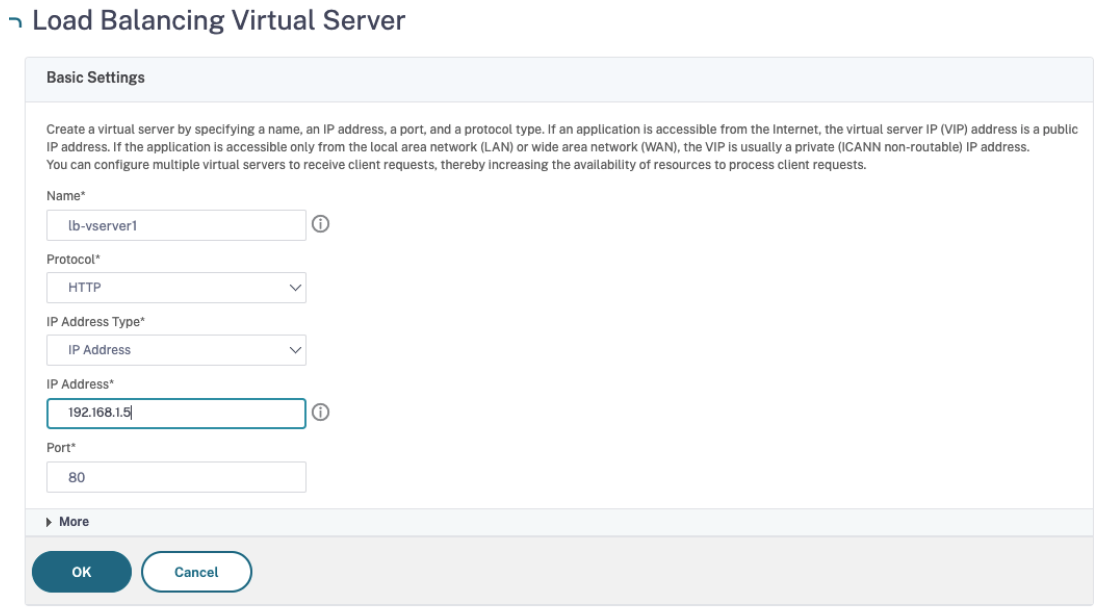
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:

   a) Geben Sie die Serveralias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der sekundären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. **Schritt 3.** Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Clientalias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.



Schritt 4. Überprüfen Sie die Konfiguration. **Schritt 5.** Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 5. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 3**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 4**konfigurierten Dienst aus und klicken Sie auf "**Binden**".

Schritt 6. Speichern Sie die Konfiguration. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die Client-Alias-IP (VIP) vom alten Primärknoten wird auf den neuen Primärknoten verschoben.

Konfigurieren Sie Hochverfügbarkeit über die CLI

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu. **Schritt 1.** Richten Sie in beiden Instanzen die Hochverfügbarkeit im **INC-aktivierten** Modus mithilfe der NetScaler CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

Der `sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

Der `prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Klicken Sie auf **Mehr**. **Schritt 2.** Fügen Sie VIP und SNIP sowohl auf dem primären als auch auf dem sekundären Knoten hinzu.

Geben Sie die folgenden Befehle auf den primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <primary_server_alias_ip> <subnet> -type SNIP
```

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Serversubnetz in der VM-Instanz konfiguriert sind.

Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. **Schritt 3.** Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```


Schritt 4. Überprüfen Sie die Konfiguration. **Schritt 5.** Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
```

Schritt 5. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
```

> **Hinweis:**
>
> Geben Sie den Befehl `save config` ein, um die Konfiguration zu speichern. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Stellen Sie ein VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereit

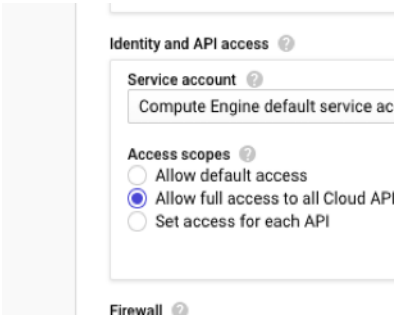
October 17, 2024

Sie können ein VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP (VIP) muss als Alias-IP-Adresse auf dem primären Knoten konfiguriert sein. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise unter „Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform“. Diese Informationen gelten auch für Bereitstellungen mit hoher Verfügbarkeit.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.



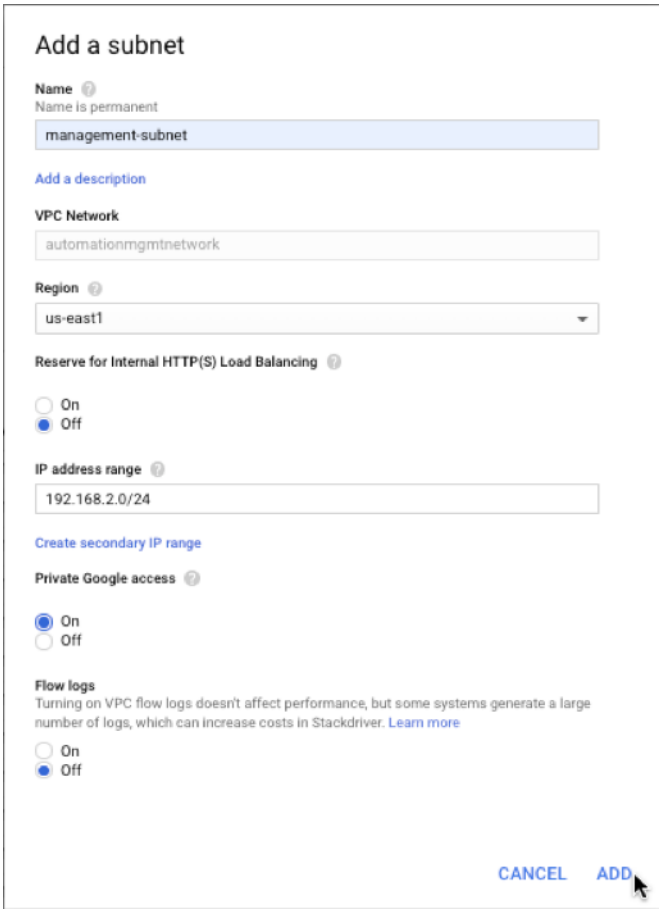
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
```

- Wenn Sie externe IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.addresses.use"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
]
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Private Google Access** im Verwal-



tungssubnetz aktivieren.

- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die in Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaare auf GCP genannten Einschränkungen und Anforderungen, um sie beim Failover auf den neuen Primärknoten zu aktualisieren.

So stellen Sie ein VPX Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der Bereitstellungsschritte für hohe Verfügbarkeit:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie Hochverfügbarkeitseinstellungen für beide Instanzen mit den Befehlen NetScaler-GUI oder ADC CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **VPC-Netzwerke erstellen** unter Eine NetScaler VPX-Instanz auf Google Cloud Platform bereitstellen.

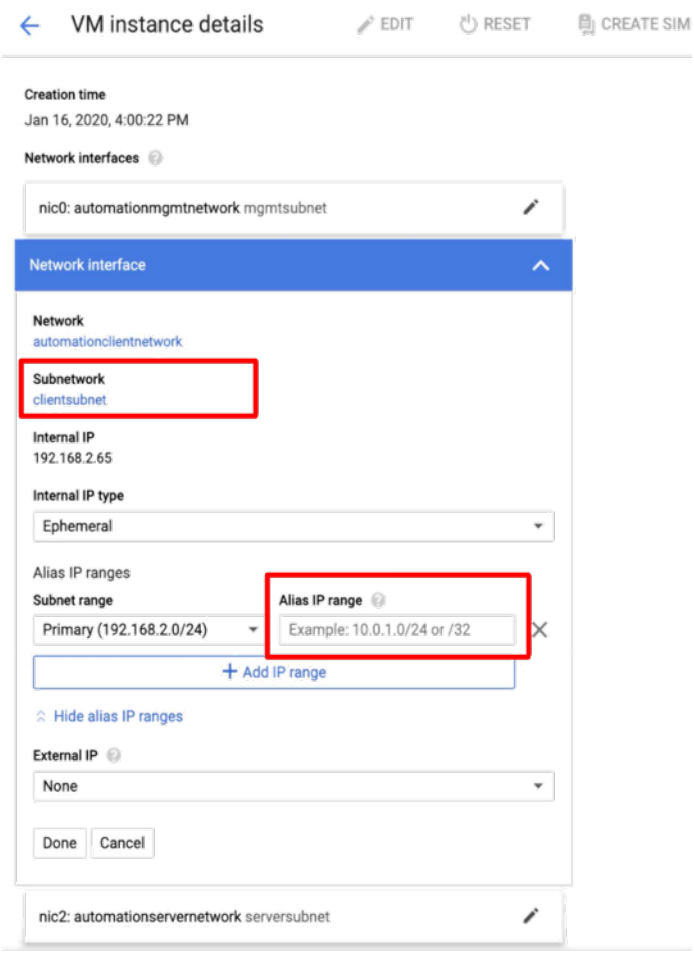
Schritt 2. Erstellen Sie zwei VPX-Instanzen

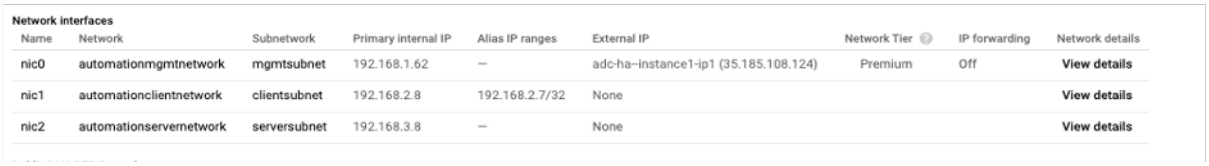
Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte in Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPsbefolgen.

> **Wichtig:**
>
> Weisen Sie dem primären Knoten eine Client-Alias-IP-Adresse zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um den VIP zu konfigurieren.

Führen Sie die folgenden Schritte aus, um eine Client-Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Clientschnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die IP-Adresse des Client-Alias ein.





Network interfaces

Name	Network	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

Nach dem Failover, wenn der alte Primär zur neuen Sekundärgruppe wird, wechseln die Alias-IP-Adressen von der alten primären und sind an den neuen Primärbereich angehängt.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die Virtual (VIP) und Subnet IP (SNIP) -Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler-GUI oder CLI konfigurieren.

Konfigurieren der Hochverfügbarkeit mit der GUI

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu. **Schritt 1.** Richten Sie die Hochverfügbarkeit im Modus INC Enabled auf beiden Knoten ein.

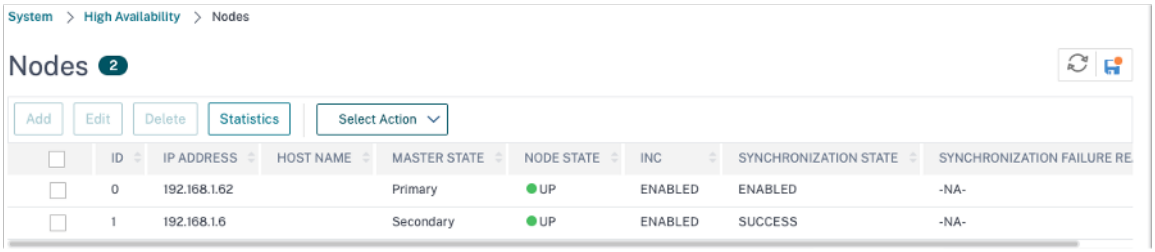
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.



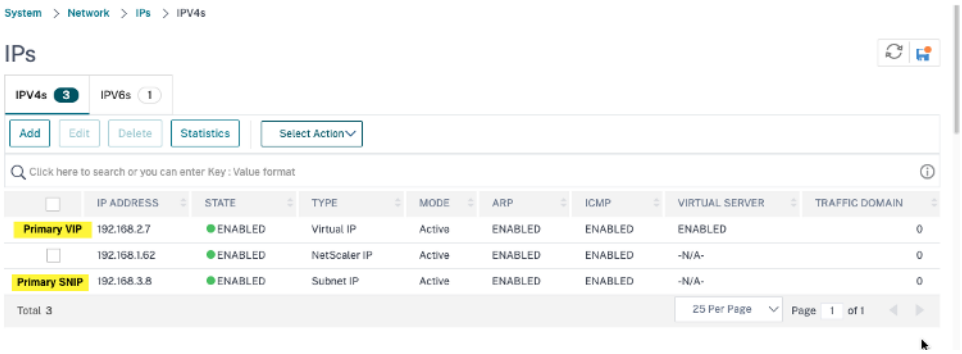
Hinweis:

Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, hat der sekundäre Knoten dieselben Anmeldeinformationen wie der primäre Knoten.

Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen , wählen Sie im Dropdownmenü IPSet**aus und geben Sie das in**Schritt 3**erstellte IPSet ein.

Führen Sie auf dem primären Knoten die folgenden Schritte aus:

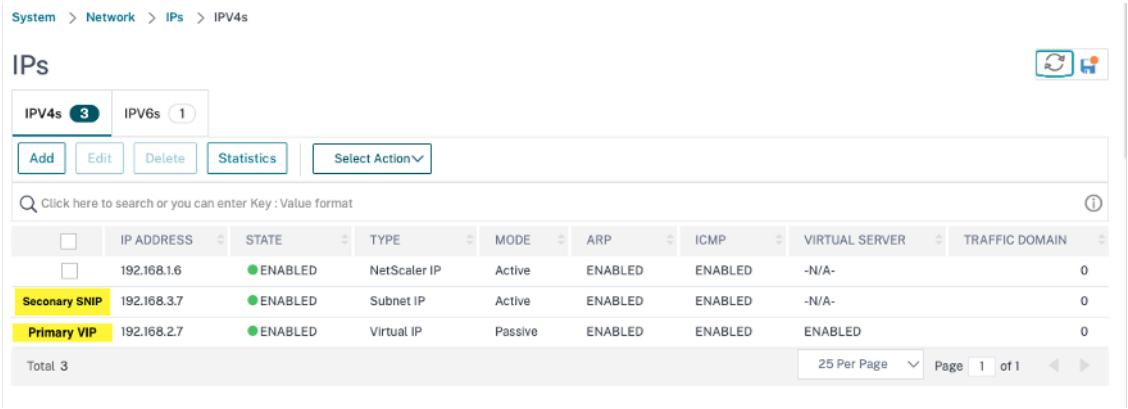
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

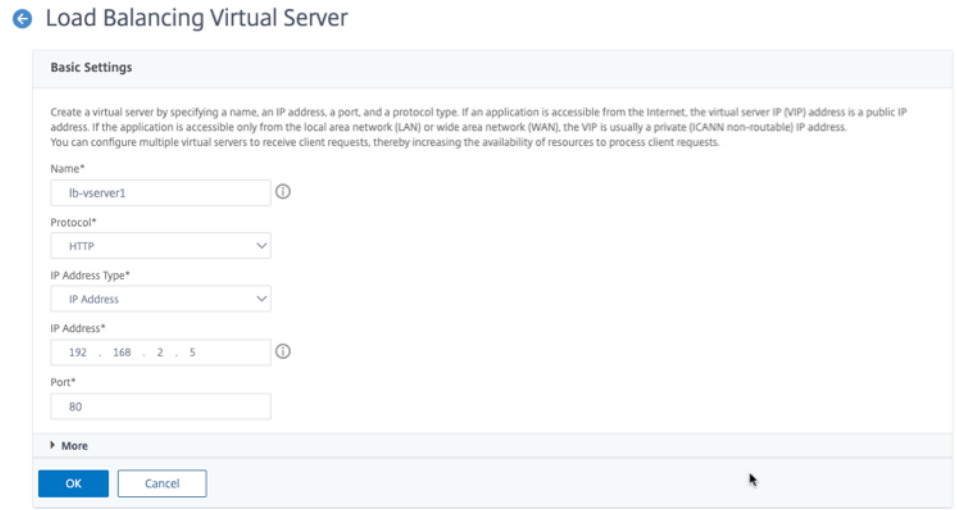
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.

c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. **Schritt 3.** Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Clientalias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.



Schritt 4. Überprüfen Sie die Konfiguration. **Schritt 5.** Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 5. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 3**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 4**konfigurierten Dienst aus und klicken Sie auf "**Binden**".

Schritt 5. Speichern Sie die Konfiguration. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die Client-Alias-IP (VIP) und die Server-Alias-IP (SNIP) von der alten primären wechselt zur neuen primären.

Konfigurieren Sie Hochverfügbarkeit über die CLI

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu. **Schritt 1.** Richten Sie in beiden Instanzen die Hochverfügbarkeit im **INC-aktivierten** Modus mithilfe der NetScaler CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

Der `sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

Der `prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Klicken Sie auf **Mehr**. Fügen Sie auf beiden Knoten VIP und SNIP hinzu.

Geben Sie die folgenden Befehle auf den primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <primary_snip> <subnet> -type SNIP
```

Der `primary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```


> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

Der `secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

> **Hinweis:**
>
> Geben Sie die IP-Adresse und Netzmaske ein, die für das Serversubnetz in der VM-Instanz konfiguriert sind.

Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. **Schritt 3.** Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```

Schritt 4. Überprüfen Sie die Konfiguration. **Schritt 5.** Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
```

Schritt 5. Speichern Sie die Konfiguration. **Schritt 6** Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
```

> **Hinweis:**
>
> Geben Sie den Befehl `save config` ein, um die Konfiguration zu speichern. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

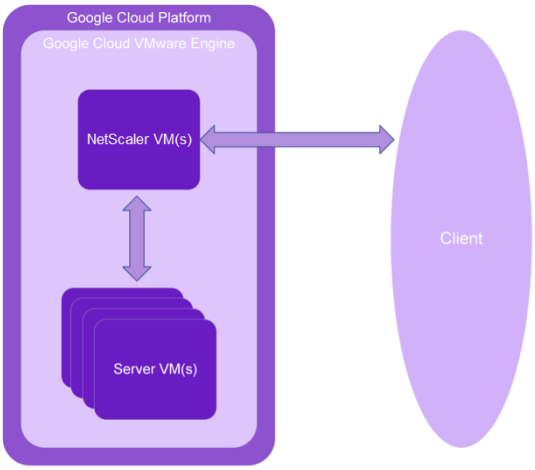
NetScaler VPX-Instanz auf Google Cloud VMware Engine bereitstellen

October 17, 2024

Google Cloud VMware Engine (GCVE) bietet Ihnen Private Clouds, die vSphere-Cluster enthalten, die aus einer dedizierten Bare-Metal-Infrastruktur der Google Cloud Platform erstellt wurden. Die minimale anfängliche Bereitstellung beträgt drei Hosts, es können jedoch nacheinander zusätzliche Hosts hinzugefügt werden. Alle bereitgestellten Private Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

GCVE ermöglicht es Ihnen, Cloud Software Defined Data Center (SDDC) auf der Google Cloud Platform mit der gewünschten Anzahl von ESX-Hosts zu erstellen. GCVE unterstützt NetScaler VPX-Bereitstellungen. GCVE bietet eine gleiche Benutzeroberfläche wie das lokale vCenter. Es funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt den GCVE auf der Google Cloud Platform, auf den ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mithilfe von GCVE erstellen, verwalten und konfigurieren. Der Administrator kann über eine OpenVPN-Verbindung auf das webbasierte vCenter und NSX-T Manager des GCVE zugreifen. Sie können die NetScaler VPX-Instanzen (eigenständig oder HA-Paar) und Server-VMs innerhalb von GCVE mithilfe von vCenter erstellen und das entsprechende Netzwerk mit NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf GCVE funktioniert ähnlich wie der lokale VMware-Hostcluster. GCVE kann über eine OpenVPN-Verbindung zur Verwaltungsinfrastruktur verwaltet werden.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Weitere Informationen zu Google Cloud VMware Engine und ihren Voraussetzungen finden Sie in der Dokumentation zu Google Cloud VMware Engine.
- Weitere Informationen zum Bereitstellen von Google Cloud VMware Engine finden Sie unter Bereitstellen einer privaten Cloud VMware Engine Cloud.
- Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Private Cloud über ein Point-to-Site-VPN-Gateway für den Zugriff auf und die Verwaltung von Google Cloud VMware Engine

finden Sie unter Zugriff auf eine private Cloud VMware Engine-Cloud.

- Laden Sie auf dem VPN-Clientcomputer die Setupdateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Google Cloud VMware Engine.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzierungsübersicht.
- Virtuelle Maschinen (VMs), die in die GCVE Private Cloud erstellt oder in diese migriert wurden, müssen mit einem Netzwerksegment verbunden sein.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX NCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> **Hinweis:**
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Mindestsystemanforderungen für die Installation des OVF-Tools beschrieben.

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei "OVF Tool User Guide"http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei "OVF Tool User Guide" http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

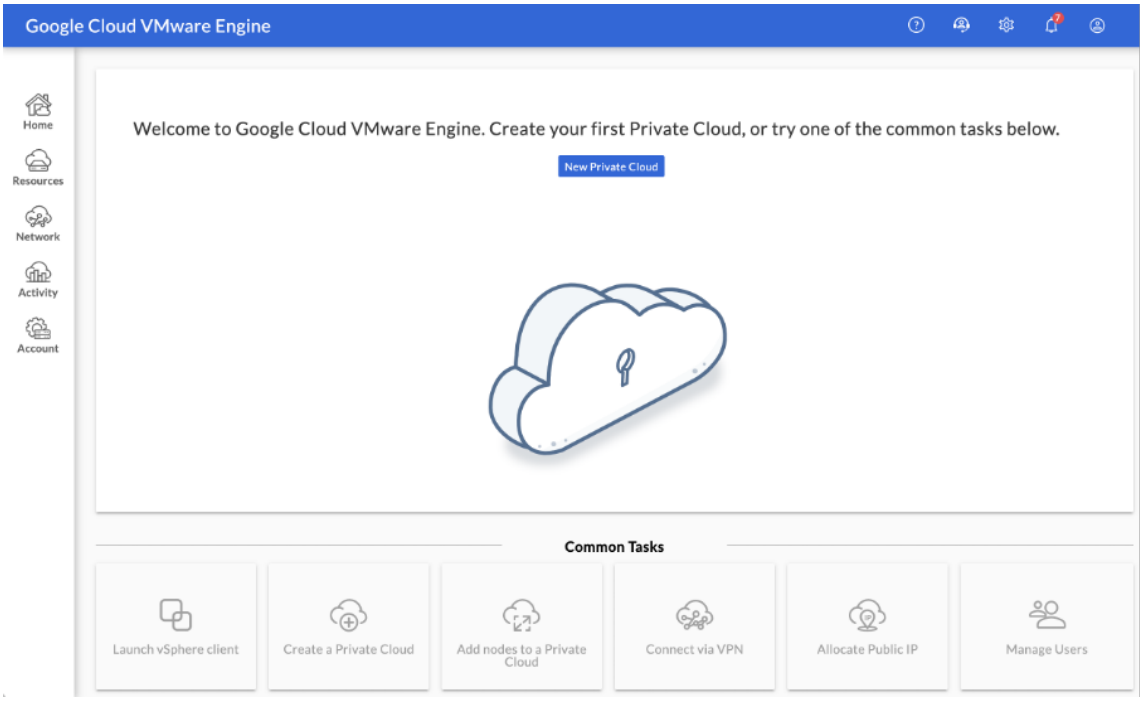
Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

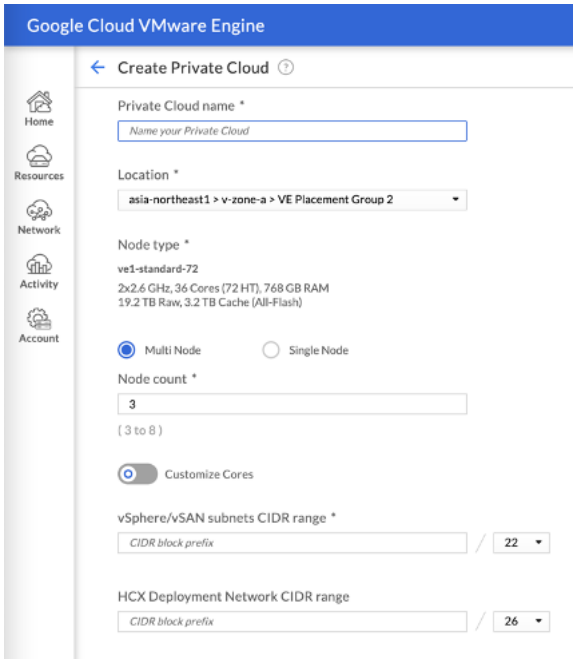
Google Cloud VMware Engine bereitstellen

1. Melden Sie sich bei Ihrem GCVE-Portal an und navigieren Sie zu **Home**.

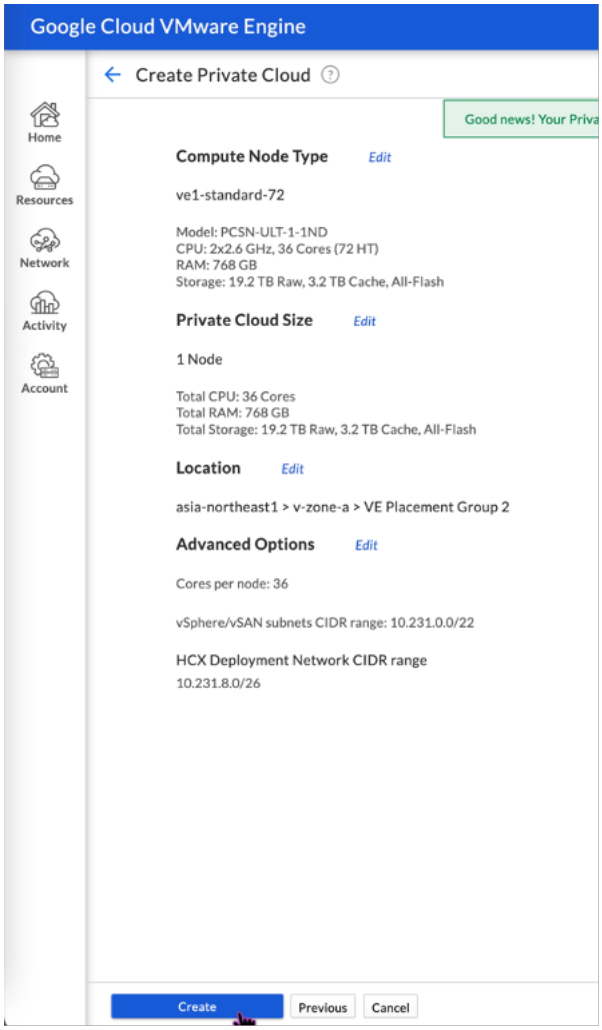


2. Geben Sie auf der Seite **Neue Private Cloud** die folgenden Details ein:

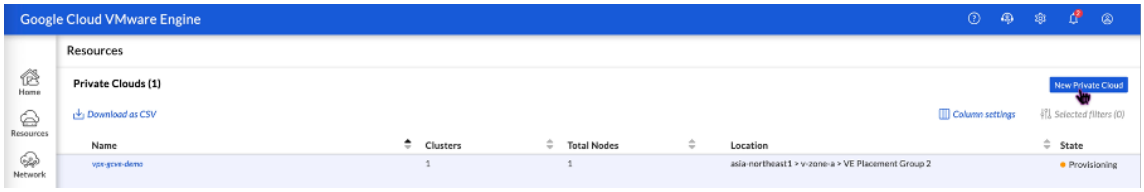
   - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer Private Cloud zu erstellen.
   - Verwenden Sie für das Feld **CIDR-Bereich des vSphere/vSAN-Subnetzes** den Adressraum /22.
   - Verwenden Sie für das Feld **CIDR-Bereich des HCX Deployment Network** den Adressraum /26.
   - Stellen Sie für das virtuelle Netzwerk sicher, dass sich der CIDR-Bereich nicht mit Ihren on-premises oder anderen GCP-Subnetzen (virtuellen Netzwerken) überschneidet.



3. Klicken Sie auf **Überprüfen und erstellen**.
4. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.



5. Klicken Sie auf **Erstellen**. Der Private Cloud-Bereitstellungsprozess wird gestartet. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt ist.
6. Gehen Sie zu **Ressourcen**, um die erstellte Private Cloud zu überprüfen.

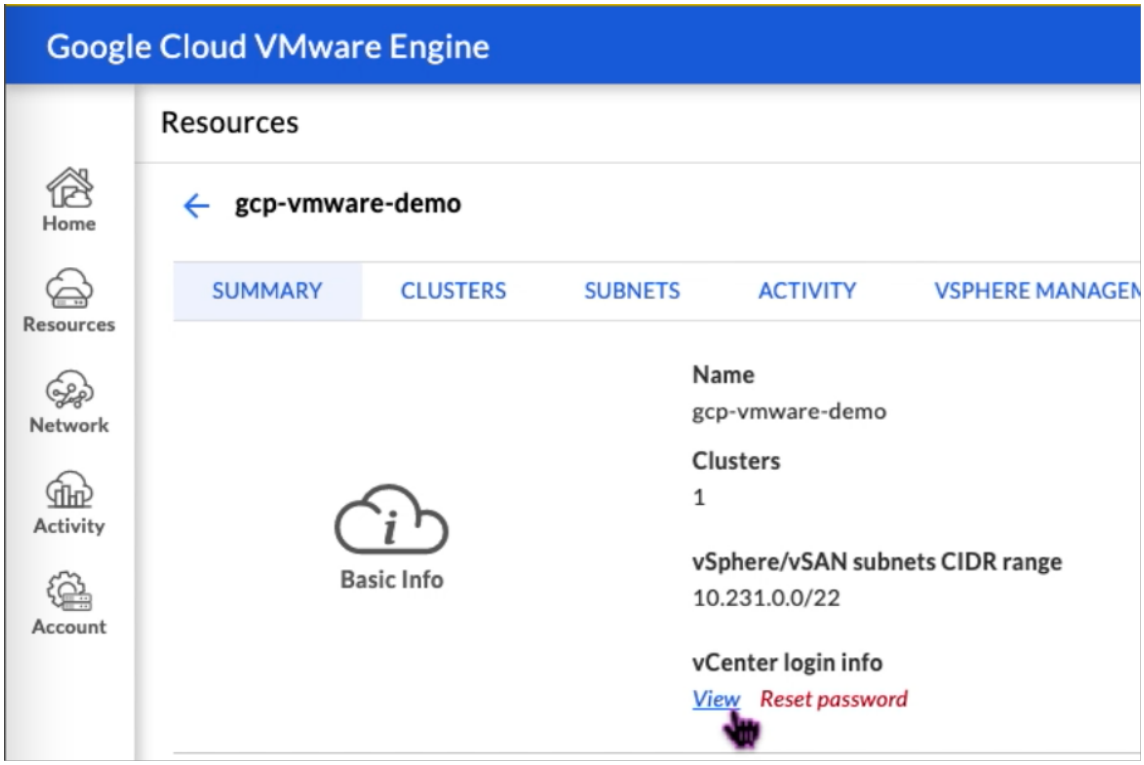


7. Um auf diese Ressource zugreifen zu können, müssen Sie über Point-to-Site-VPN eine Verbindung zu GCVE herstellen. Weitere Informationen finden Sie in der folgenden Dokumentation:

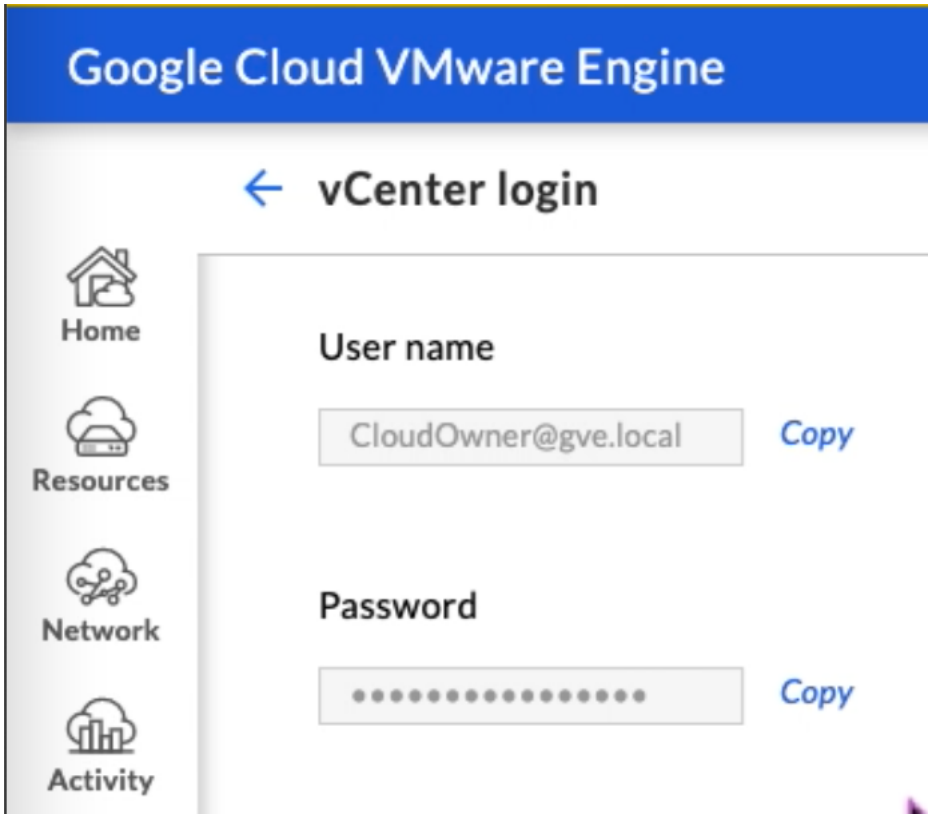
   - VPN-Gateways
   - Verbindung über VPN herstellen

Greifen Sie auf Ihr Private Cloud vCenter Portal zu

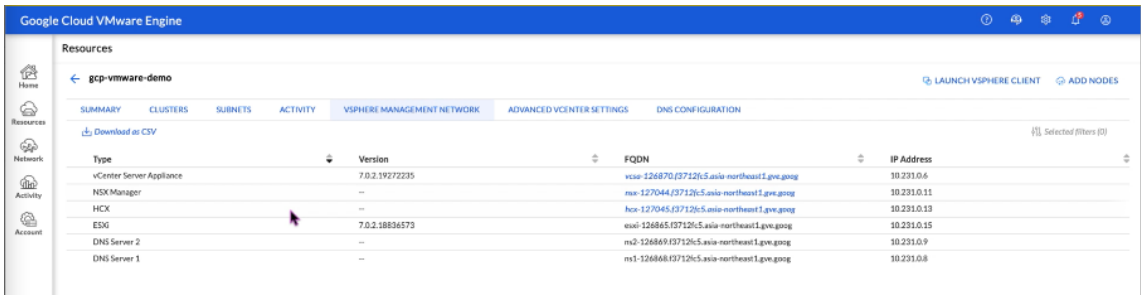
1. Navigieren Sie zu Ihrer privaten Cloud VMware Engine Cloud. Klicken Sie auf der Registerkarte **ZUSAMMENFASSUNG** unter **vCenter-Anmeldeinformationen**auf **Anzeigen**.



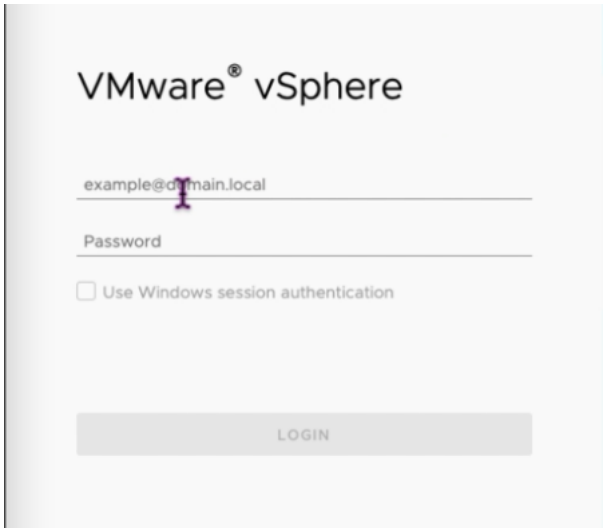
2. Notieren Sie sich die vCenter-Anmeldeinformationen.



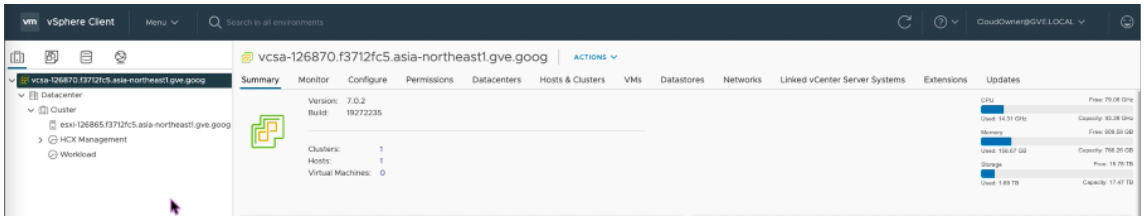
3. Starten Sie den vSphere Client, indem Sie auf **LAUNCH VSPHERE CLIENT** klicken, oder navigieren Sie zu **VSPHERE MANAGEMENT NETWORK** und klicken Sie auf den **vCenter Server Appliance**-FQDN.



4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens vCenter-Anmeldeinformationen bei VMware vSphere an.



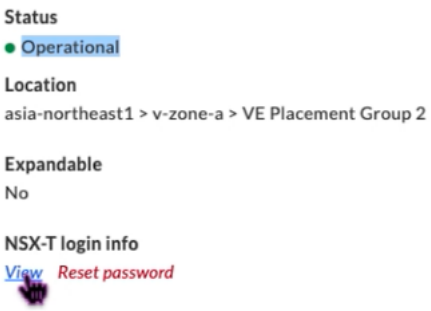
5. Im vSphere Client können Sie die ESXi-Hosts überprüfen, die Sie im GCVE Portal erstellt haben.



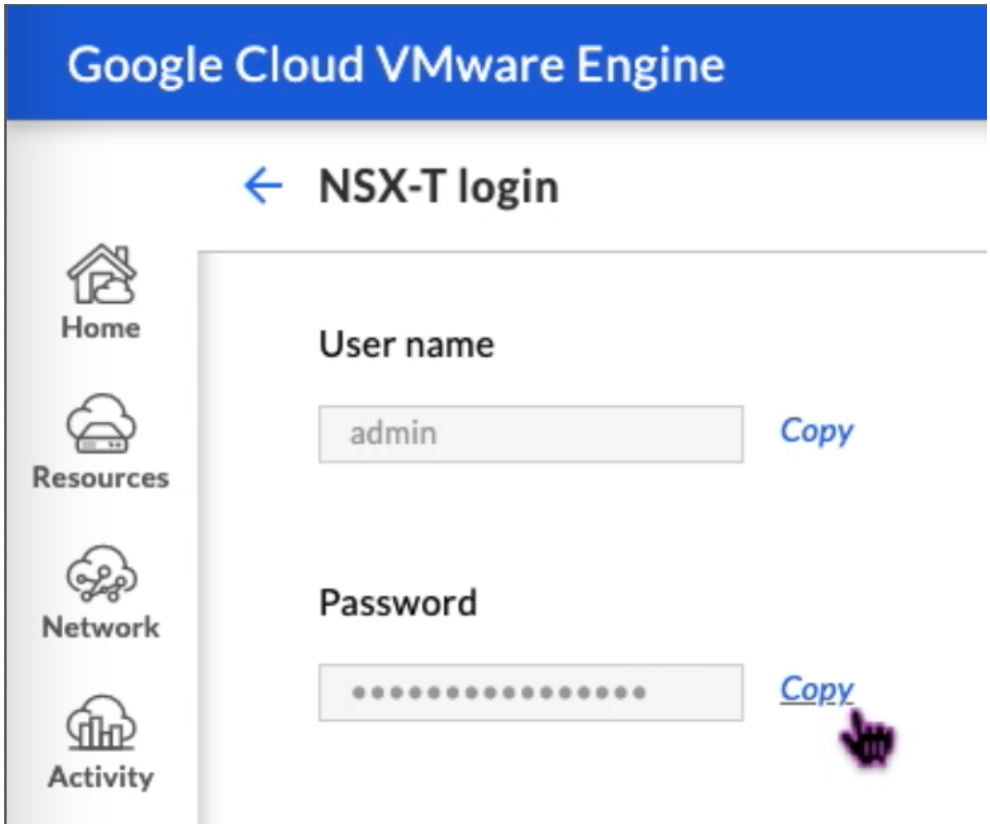
Erstellen eines NSX-T-Segments im GCVE NSX-T-Portal

Sie können ein NSX-T-Segment über NSX Manager in der Google Cloud VMware Engine-Konsole erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads in diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment erstellt haben, wird es in vCenter angezeigt.

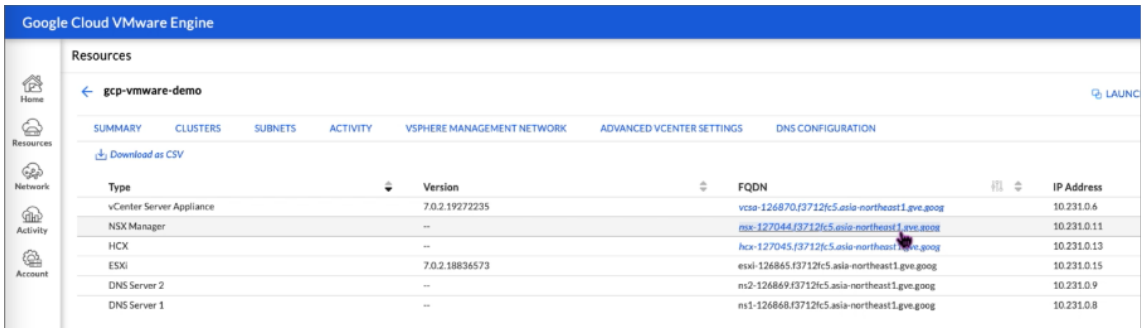
1. Wählen Sie in Ihrer GCVE Private Cloud unter **Zusammenfassung -> NSX-T-Anmeldeinformationen**die Option **Anzeigen**aus.



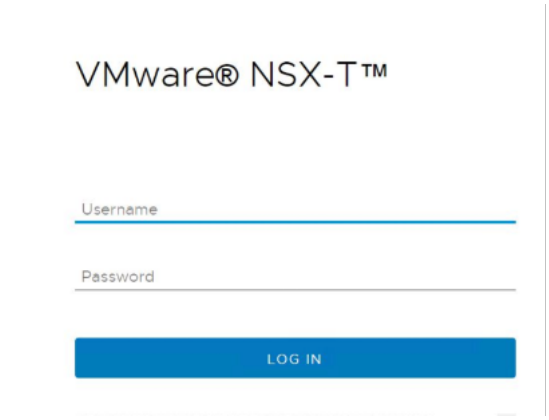
2. Notieren Sie sich die NSX-T-Anmeldeinformationen.



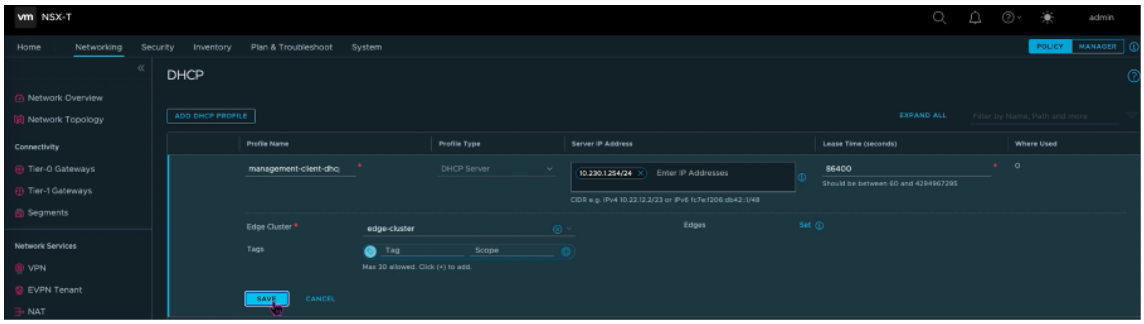
3. Starten Sie NSX Manager, indem Sie zu **VSPHERE MANAGEMENT NETWORK** navigieren und auf den **NSX Manager-FQDN** klicken.



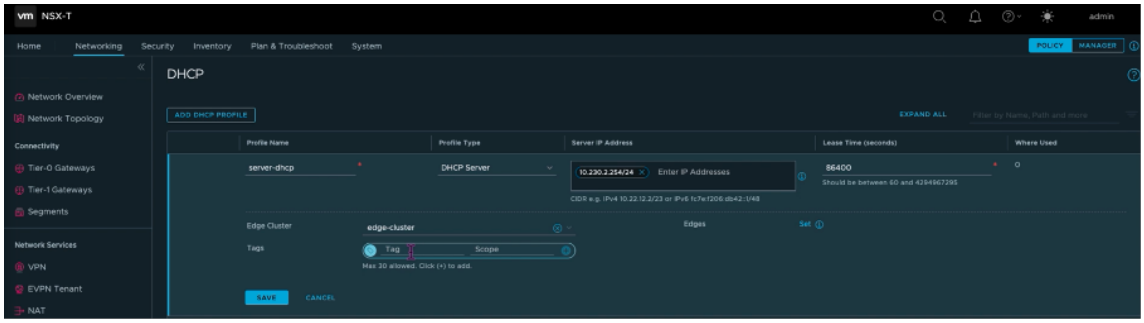
4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens angegebenen Anmeldeinformationen beim NSX Manager an.



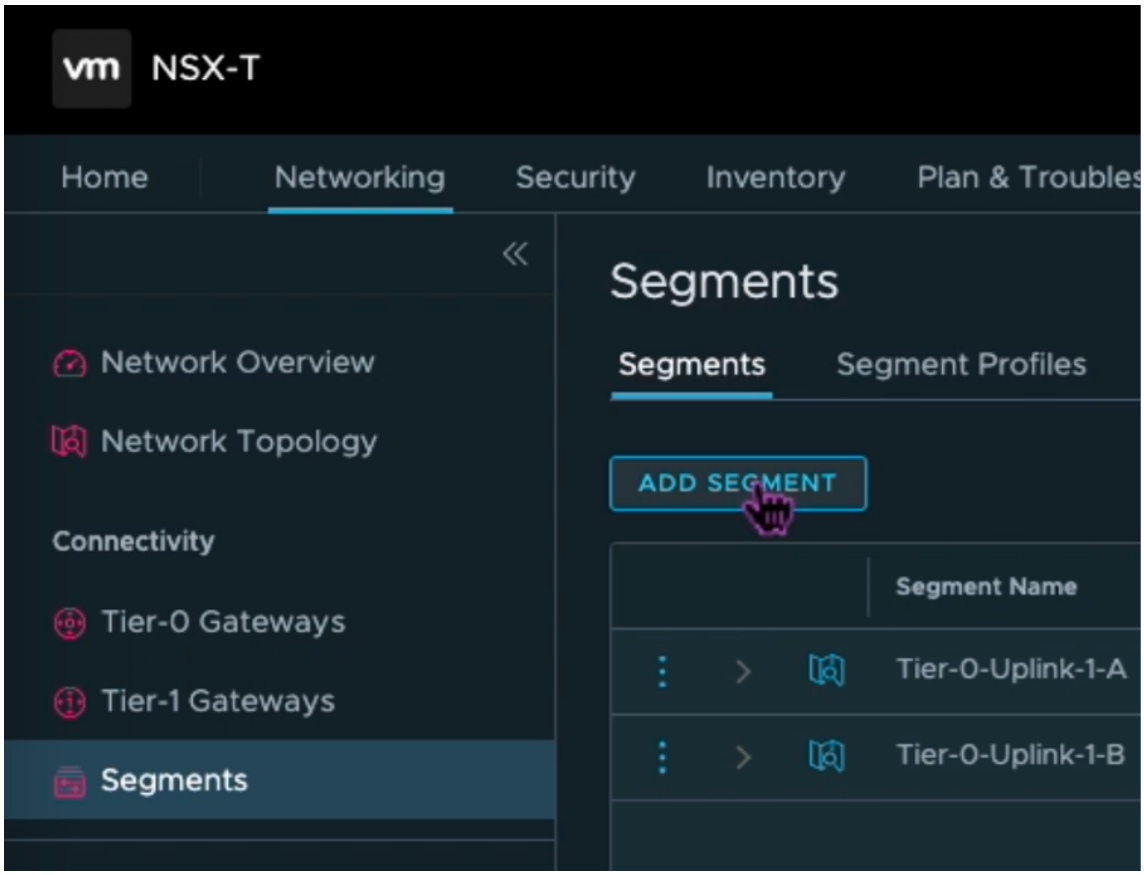
5. Richten Sie den DHCP-Service für die neuen Segmente oder Subnetze ein.
6. Bevor Sie ein Subnetz erstellen können, richten Sie einen DHCP-Dienst ein.
7. Gehen Sie in NSX-T zu **Netzwerk > DHCP**. Das Netzwerk-Dashboard zeigt an, dass der Dienst ein Tier-0- und ein Tier-1-Gateway erstellt.
8. Um mit der Bereitstellung eines DHCP-Servers zu beginnen, klicken Sie auf **DHCP-Profil hinzufügen**.
9. Geben Sie im Feld DHCP-Name einen Namen für das **Client-Management-Profil** ein.
10. Wählen Sie **DHCP-Server** als Profiltyp aus.
11. Geben Sie in der Spalte **Server-IP-Adresse** einen IP-Adressbereich für den DHCP-Dienst an.
12. Wählen Sie Ihren **Edge Cluster aus**.
13. Klicken Sie auf **Save**, um den DHCP-Dienst zu erstellen.



14. Wiederholen Sie die Schritte 6 bis 13 für den Server-DHCP-Bereich.



15. Erstellen Sie zwei separate Segmente: eines für Client- und Management-Schnittstellen und eines für Serverschnittstellen.
16. Gehen Sie in NSX-T zu **Netzwerk > Segmente**.
17. Klicken Sie auf **Add Segment**.

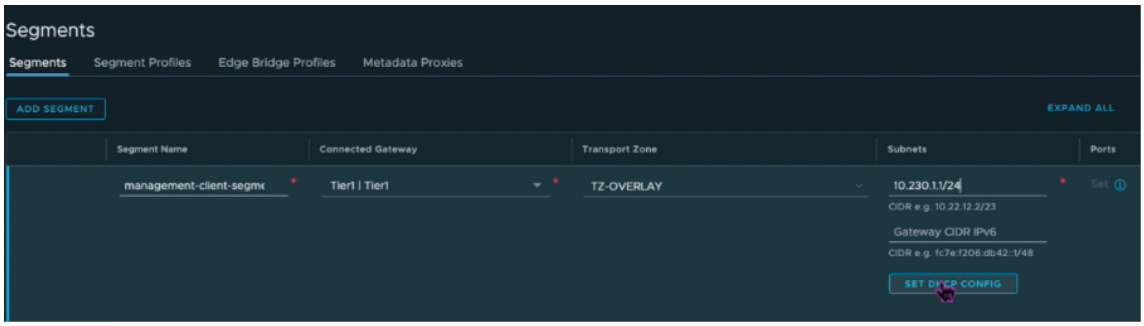


18. Geben Sie im Feld **Segmentname** einen Namen für Ihr **Kundenmanagement-Segment** ein.
19. Wählen Sie in der Liste **Verbundenes GatewayTier1** aus, um eine Verbindung zum Tier-1-Gateway herzustellen.

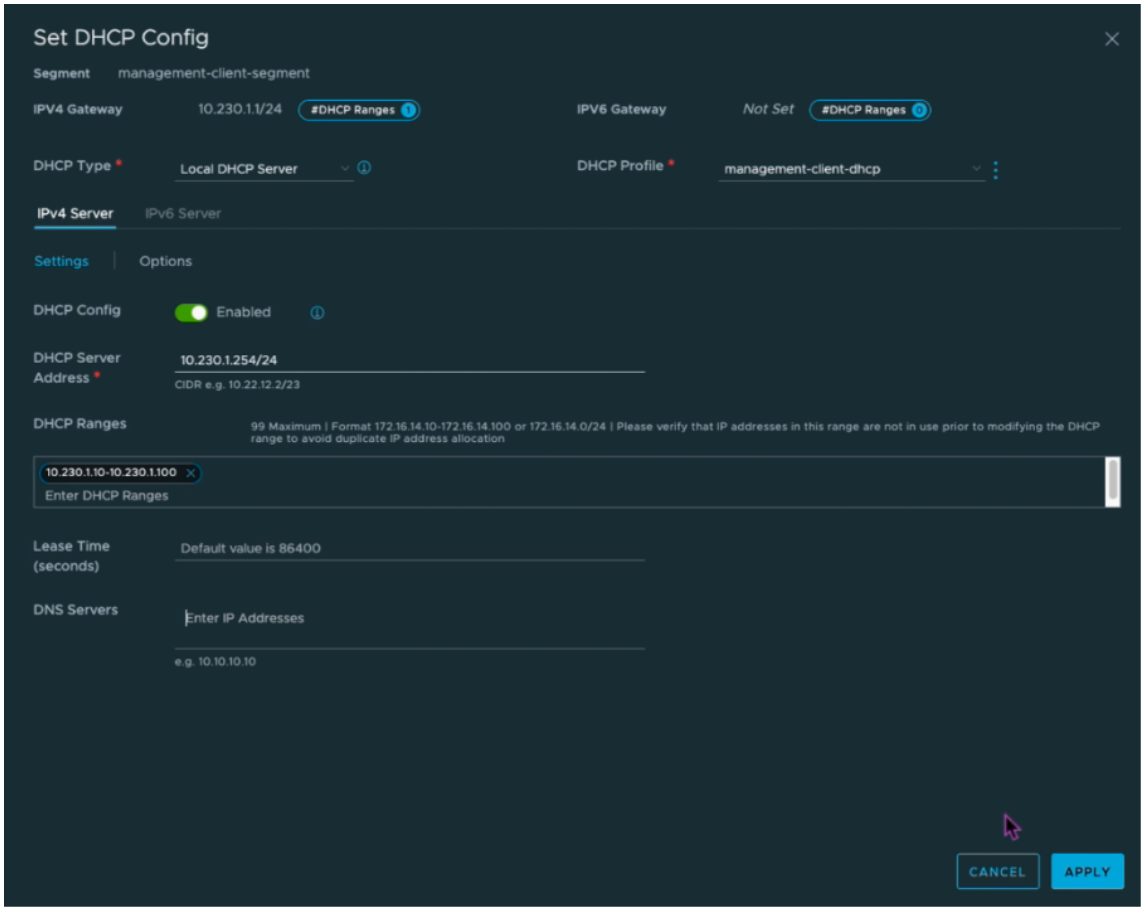
Wählen Sie in der **Transportzonenliste**TZ-OVERLAY aus Überlagerung**.

20.

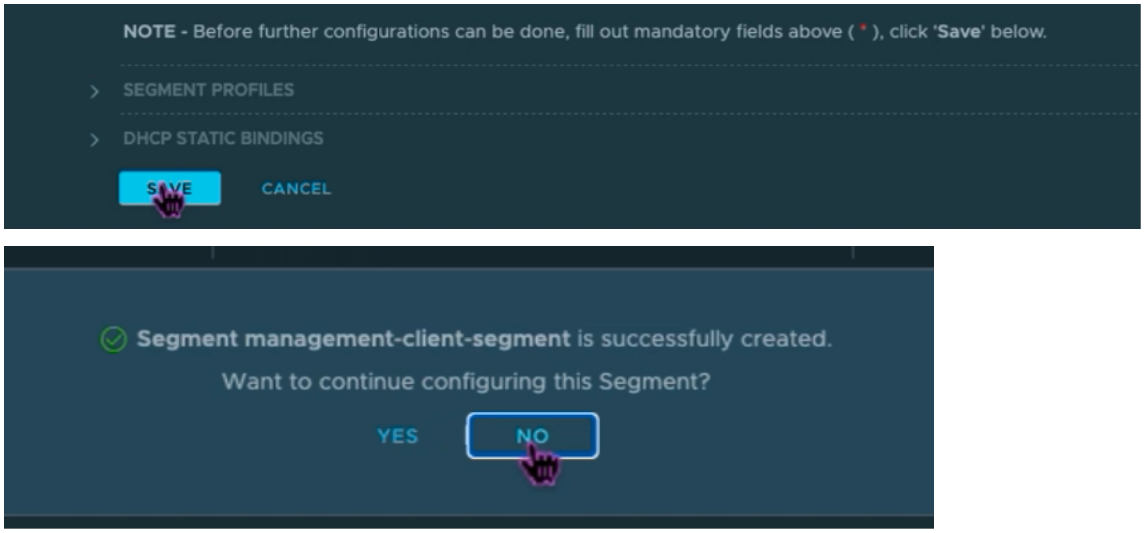
21. Geben Sie in der Spalte **Subnetze** den Subnetzbereich ein. Geben Sie den Subnetzbereich mit **.** 1 als letztes Oktett an. Beispiel: 10.12.2.1/24.



22. Klicken Sie auf **DHCP-Konfiguration festlegen**und geben Sie Werte für das Feld **DHCP-Bereiche** an.



23. Klicken Sie auf **Übernehmen**, um Ihre DHCP-Konfiguration zu
24. Klicken Sie auf **Speichern**.



25. Wiederholen Sie die Schritte 17 bis 24 auch für das Serversegment.
26. Sie können diese Netzwerksegmente jetzt in vCenter auswählen, wenn Sie eine VM erstellen.

Weitere Informationen finden Sie unter Erstellen Ihres ersten Subnetzes.

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie Private Cloud auf GCVE installiert und konfiguriert haben, können Sie das vCenter verwenden, um virtuelle Appliances auf der VMware Engine zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge der in der Private Cloud verfügbaren Ressourcen ab.

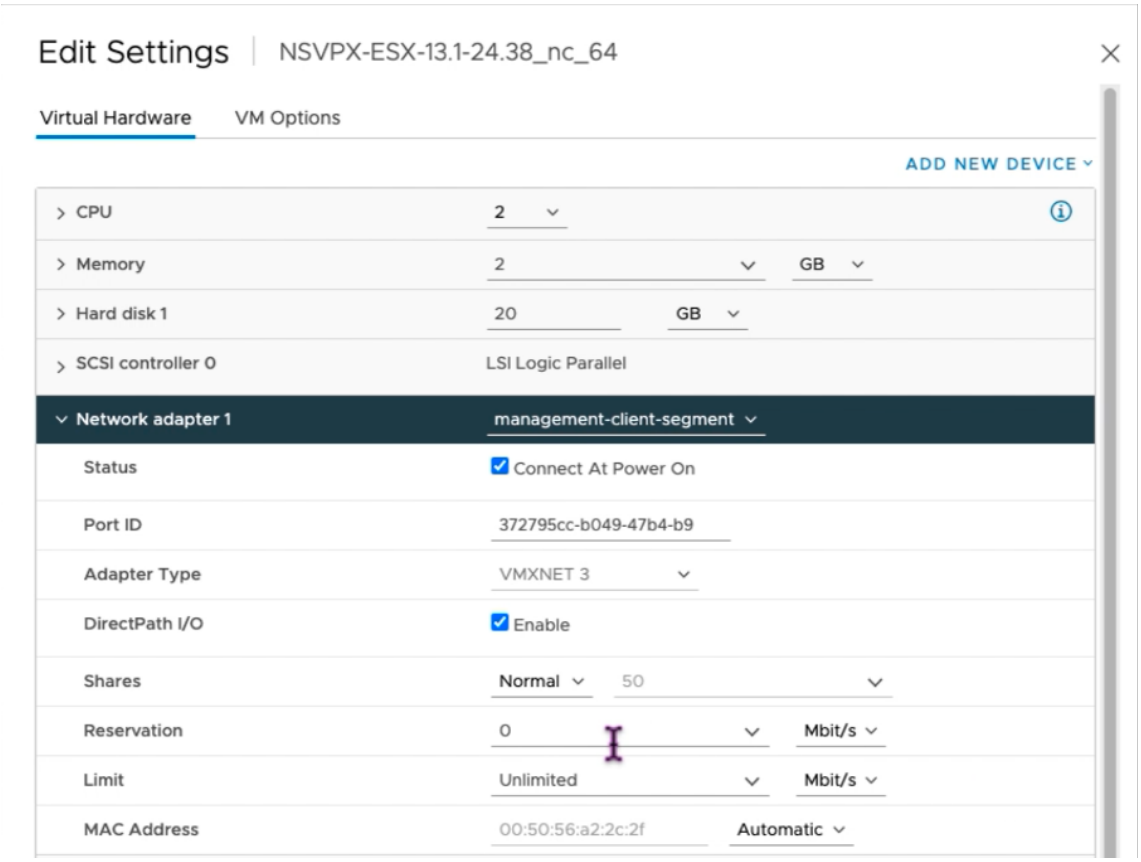
Um NetScaler VPX-Instanzen in Private Cloud zu installieren, führen Sie die folgenden Schritte auf einem Desktop aus, der mit dem Point-to-Site-VPN der Private Cloud verbunden ist:

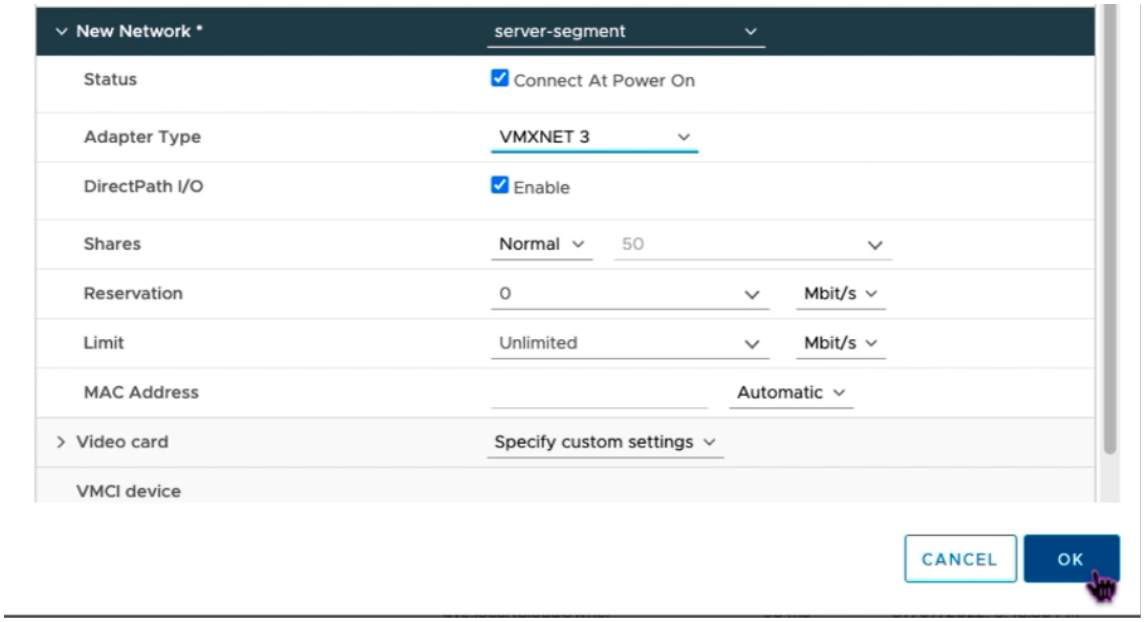
1. Laden Sie die Setup-Dateien der NetScaler VPX-Instanz für den ESXi-Host von der NetScaler-Downloadseite herunter.
2. Öffnen Sie VMware vCenter in einem Browser, der mit Ihrem Point-to-Site-VPN der Private Cloud verbunden ist.
3. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.

5. Navigieren Sie im Dialogfeld **OVF-Vorlagebereitstellen im Feld Aus Datei bereitstellen**zu dem Speicherort, an dem Sie die Setupdateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf**Weiter**.

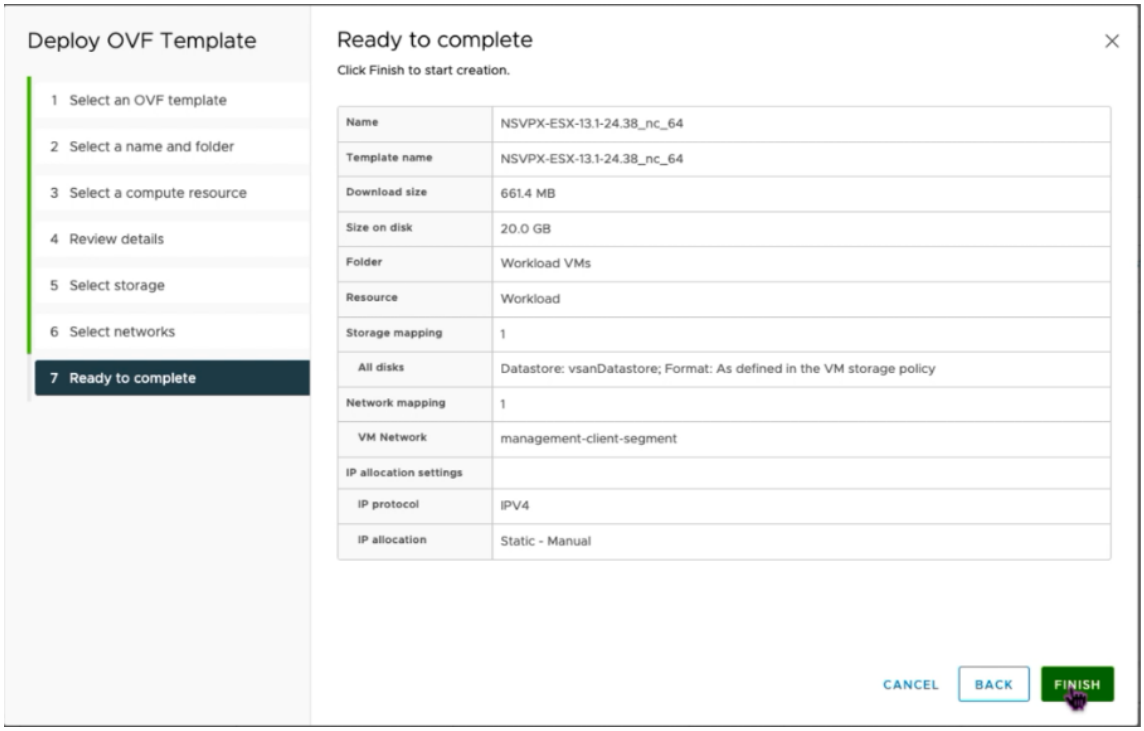
   > **Hinweis:**
   >
   > Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die GCP-Infrastruktur begrenzt und in Google Cloud VMware Engine möglicherweise nicht verfügbar.

6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf NSX-T Manager konfiguriert haben. Klicken Sie auf **OK**.

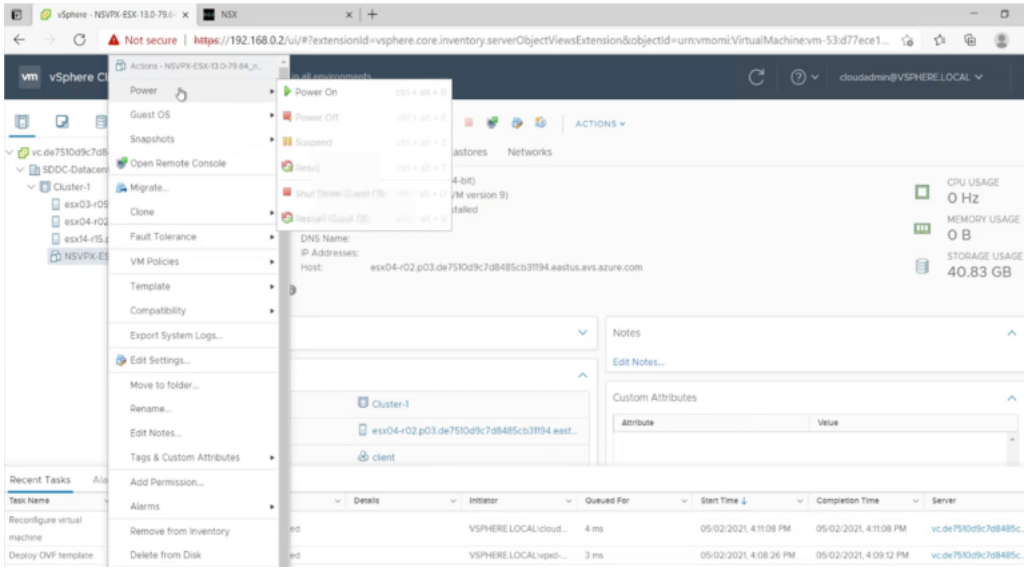




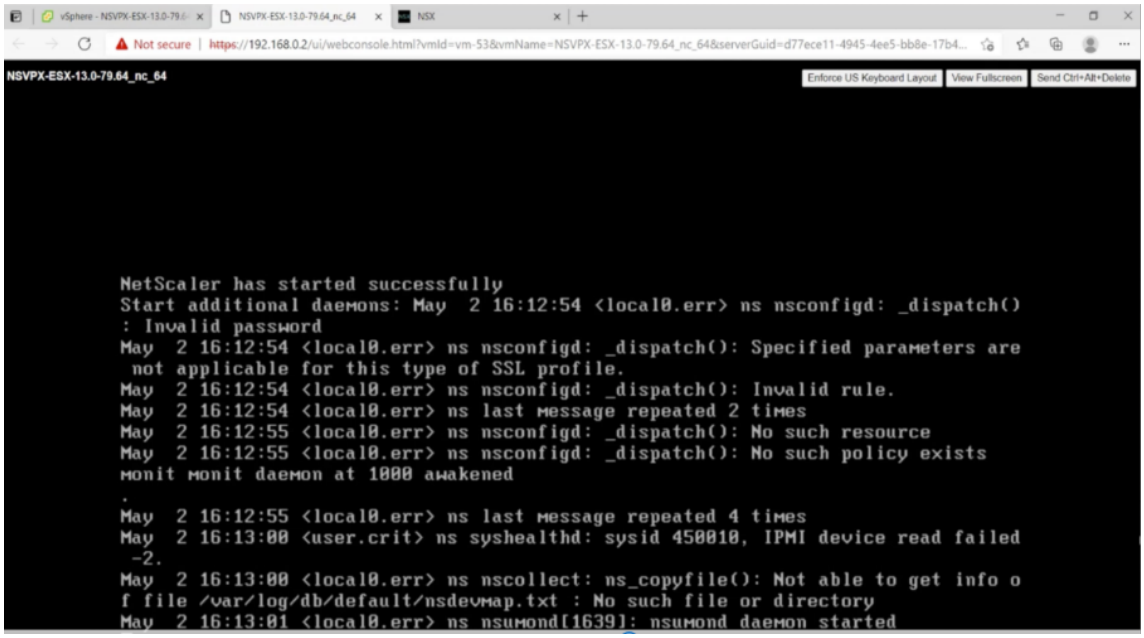
7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance in der VMware Cloud zu beginnen.



8. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Web-Konsole starten**, um einen Konsolenport zu emulieren.



9. Sie sind jetzt vom vSphere-Client aus mit der NetScaler VM verbunden.



10. Legen Sie beim ersten Start die Verwaltungs-IP und das Gateway für die ADC-Instanz fest.


```
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
```

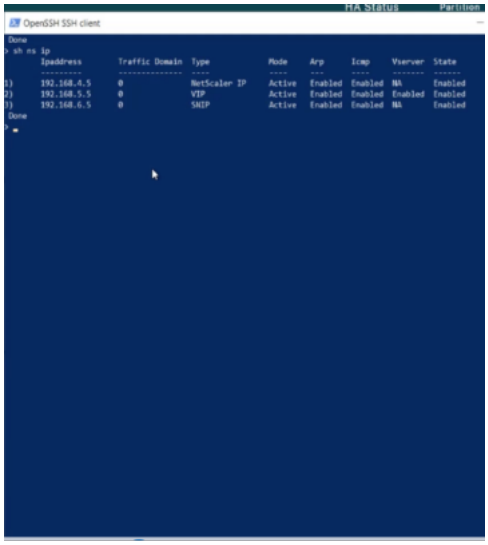
11. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
ssh nsroot@<management IP address>
```

Beispiel

```
ssh nsroot@10.230.1.10
```

12. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

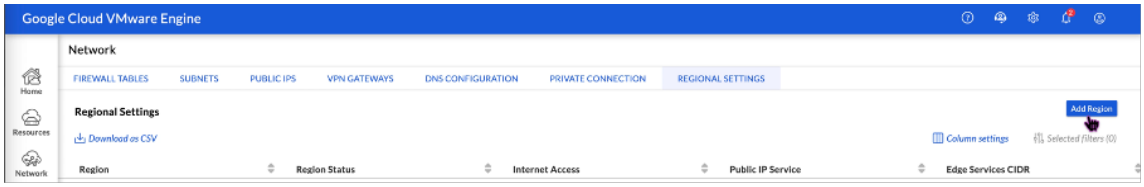


Weisen Sie einer NetScaler VPX-Instanz in der VMware-Cloud eine öffentliche IP-Adresse zu

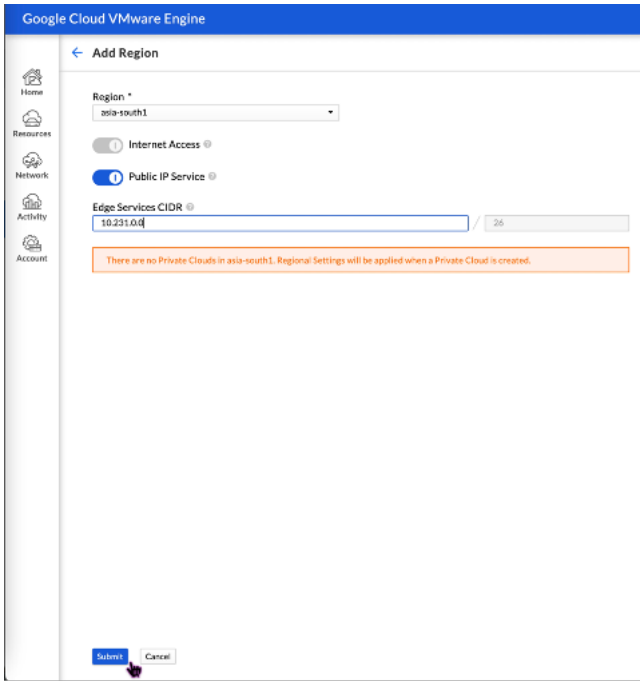
Nachdem Sie die NetScaler VPX-Instanz auf GCVE installiert und konfiguriert haben, müssen Sie der Clientschnittstelle eine öffentliche IP-Adresse zuweisen. Stellen Sie vor dem Zuweisen öffentlicher IP-Adressen zu Ihren VMs sicher, dass der öffentliche IP-Dienst für Ihre Google Cloud-Region aktiviert ist.

Gehen Sie folgendermaßen vor, um den öffentlichen IP-Dienst für eine neue Region zu aktivieren:

1. Navigieren Sie in der GCVE Console zu **Netzwerk > REGIONALE EINSTELLUNGEN > Region hinzufügen**.



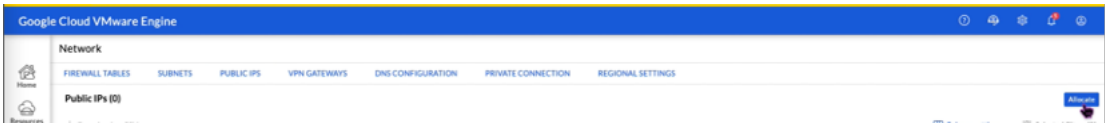
2. Wählen Sie Ihre Region aus und aktivieren Sie **den Internetzugriff und denöffentlichen IP-Dienst**.
3. Weisen Sie einen Edge-Services-CIDR zu und stellen Sie sicher, dass sich der CIDR-Bereich nicht mit Ihren on-premises oder anderen GCP/GCVE-Subnetzen (virtuellen Netzwerken) überschneidet.



4. Der öffentliche IP-Dienst wird in wenigen Minuten für die ausgewählte Region aktiviert.

Um der Clientschnittstelle auf der NetScaler VPX-Instanz auf GCVE eine öffentliche IP zuzuweisen, führen Sie die folgenden Schritte im GCVE Portal aus:

1. Navigieren Sie in der GCVE Console zu **Netzwerk > PUBLIC IPS > Allocate**.



2. Geben Sie einen Namen für die öffentliche IP ein. Wählen Sie Ihre Region und wählen Sie die Private Cloud aus, in der die IP verwendet werden soll.
3. Geben Sie die private IP für die Schnittstelle an, der die öffentliche IP zugeordnet werden soll. Dies ist die **private IP** für Ihre **Client-Schnittstelle** .
4. Klicken Sie auf **Submit**.

5. Public IP ist in wenigen Minuten einsatzbereit.
6. Sie müssen Firewall-Regeln hinzufügen, um den Zugriff auf die öffentliche IP zu ermöglichen, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter Firewallregeln.

Back-End-GCP-Autoscaling-Dienst hinzufügen

October 17, 2024

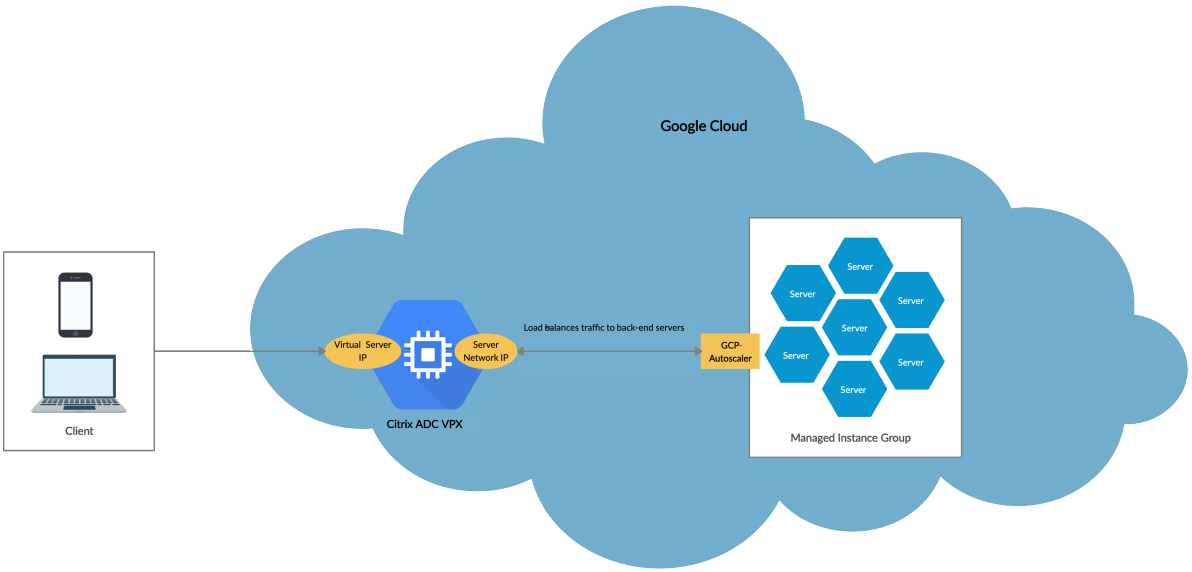
Ein effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen, abhängig von den Anwendungsanforderungen. Um der steigenden

Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Wenn die Nachfrage nachlässt, müssen Sie herunterfahren, um unnötige Kosten durch nicht ausgelastete Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die NetScaler VPX-Instanz ist in den GCP Autoscaling-Dienst integriert und bietet die folgenden Vorteile:

- **Lastverteilung und Verwaltung**: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch verwaltete Instanzgruppen im Back-End-Subnetz und ermöglicht es Ihnen, die verwalteten Instanzgruppen auszuwählen, um die Last auszugleichen. Die virtuellen IP-Adressen und Subnetz-IP-Adressen werden auf der VPX-Instanz automatisch konfiguriert.
- **Hochverfügbarkeit**: Erkennt verwaltete Instanzgruppen, die sich über mehrere Zonen erstrecken, und verteilt die Serverlast.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Backend-Server auf denselben Platzierungsgruppen
  - Backend-Server in verschiedenen Zonen

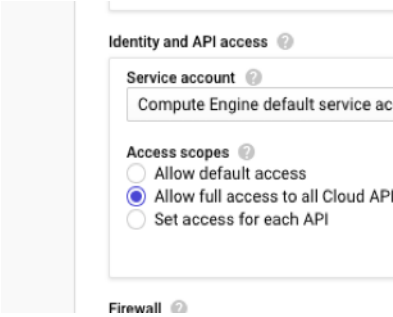
Dieses Diagramm zeigt, wie der GCP Autoscaling-Dienst in einer NetScaler VPX-Instanz funktioniert, die als virtueller Lastausgleichsserver fungiert.



Voraussetzungen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

- Erstellen Sie eine NetScaler VPX Instanz auf GCP entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer NetScaler VPX-Instanz finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.
  - Weitere Informationen zum Bereitstellen von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.instances.get",
"compute.instanceGroupManagers.get",
"compute.instanceGroupManagers.list",
"compute.zones.list",
"logging.sinks.create",
"logging.sinks.delete",
"logging.sinks.get",
"logging.sinks.list",
"logging.sinks.update",
"pubsub.subscriptions.consume",
"pubsub.subscriptions.create",
"pubsub.subscriptions.delete",
"pubsub.subscriptions.get",
"pubsub.topics.attachSubscription",
"pubsub.topics.create",
"pubsub.topics.delete",
"pubsub.topics.get",
"pubsub.topics.getIamPolicy",
"pubsub.topics.setIamPolicy",
]
```

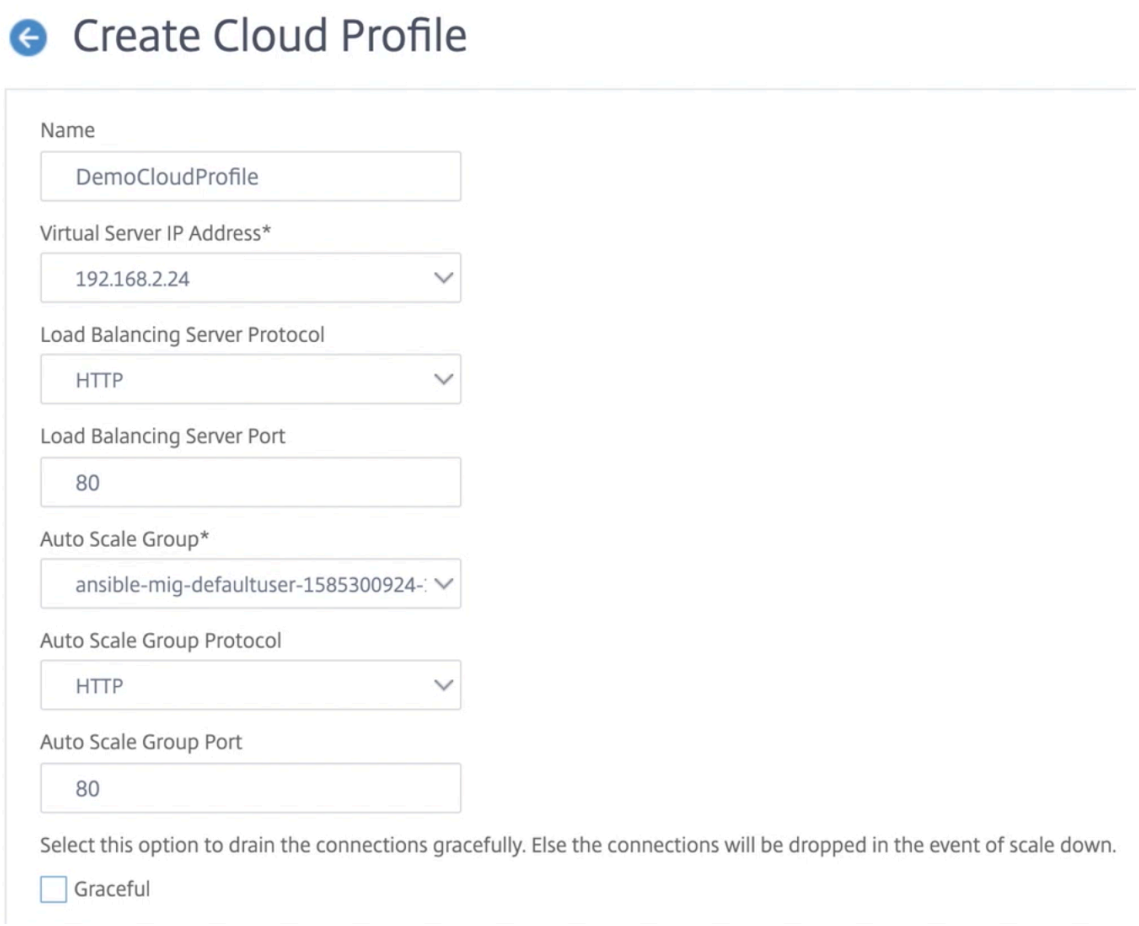
- Um Autoscaling einzurichten, stellen Sie sicher, dass Folgendes konfiguriert ist:
  - Instanzvorlage

- Verwaltete Instanzgruppe
- Autoscaling-Richtlinie

Fügen Sie den GCP Autoscaling-Dienst zu einer NetScaler VPX-Instanz hinzu

Sie können den Autoscaling-Dienst mit einem einzigen Klick zu einer VPX-Instanz hinzufügen, indem Sie die GUI verwenden. Gehen Sie wie folgt vor, um den Autoscaling-Dienst zur VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für `nsroot`bei der VPX-Instanz an.
2. Wenn Sie sich zum ersten Mal bei der NetScaler VPX-Instanz anmelden, wird die standardmäßige Cloud-Profilseite angezeigt. Wählen Sie im Dropdownmenü die von GCP verwaltete Instanzgruppe aus und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen.

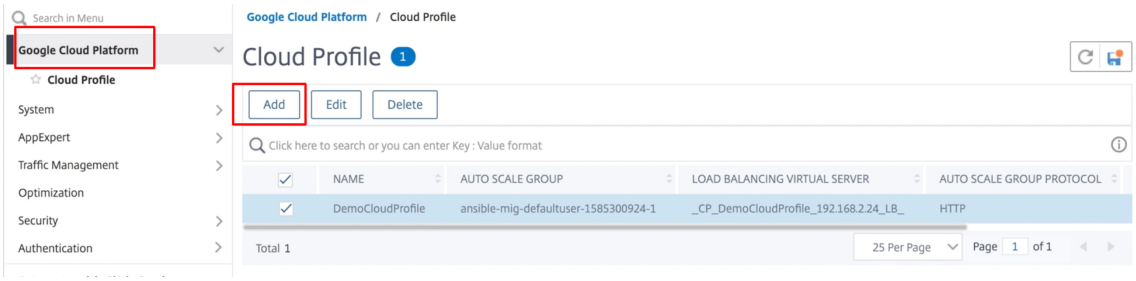


- Das Feld **IP-Adresse des virtuellen Servers** wird automatisch von allen IP-Adressen ausgefüllt, die den Instanzen zugeordnet sind.
- Die **Autoscale Group** wird aus der verwalteten Instanzgruppe vorausgefüllt, die für Ihr GCP-Konto konfiguriert ist.

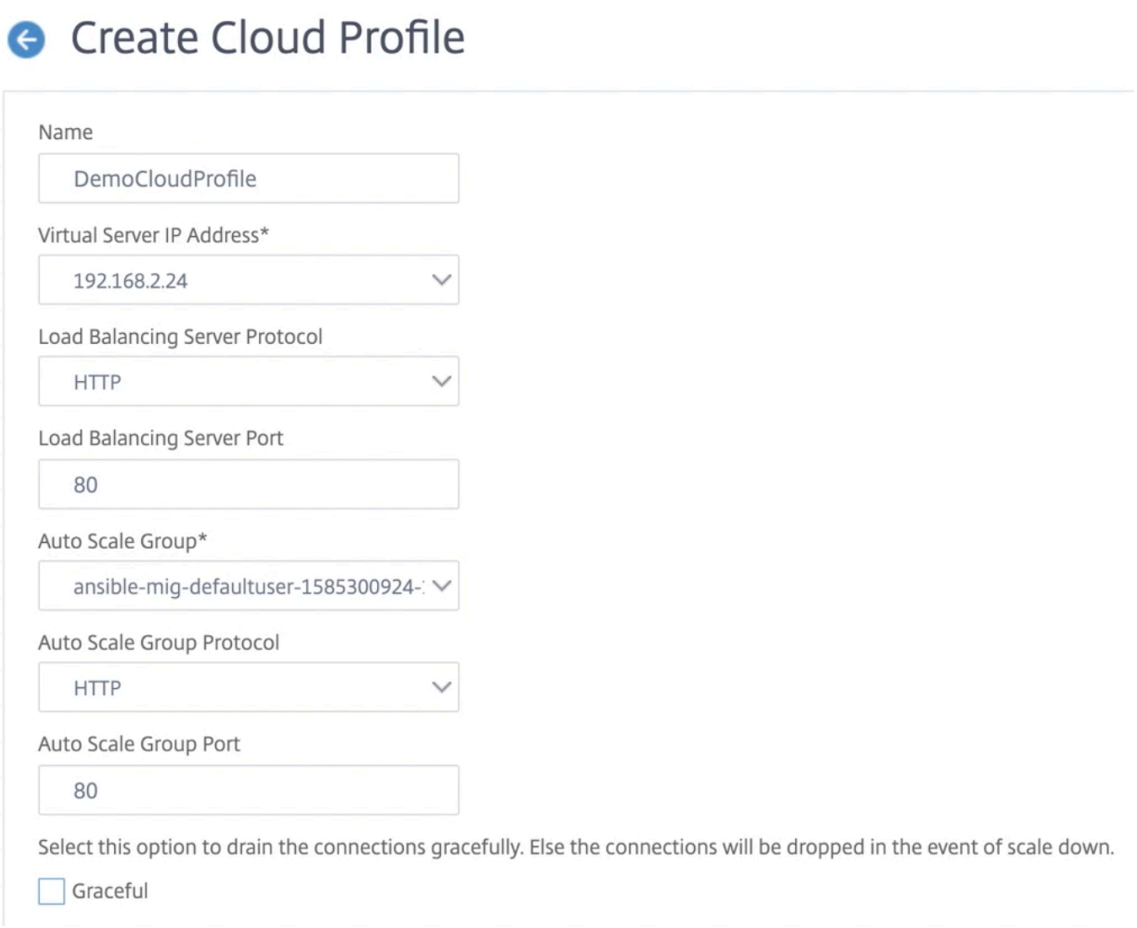
- Stellen Sie bei der Auswahl von **Autoscale Group Protocol** und **Autoscale Group Port**sicher, dass die Server das konfigurierte Protokoll und die konfigurierten Ports überwachen. Binden Sie den richtigen Monitor in der Servicegruppe. Standardmäßig wird der TCP-Monitor verwendet.
- Deaktivieren Sie das Kontrollkästchen **Graceful**, da es nicht unterstützt wird.

> **Hinweis:**
>
> Bei Autoscaling des SSL-Protokolltyps ist der virtuelle Lastausgleichsserver oder die Servicegruppe nach der Erstellung des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

3. Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie in der GUI zu **System > Google Cloud Platform > Cloud-Profil** und klicken Sie auf **Hinzufügen**.

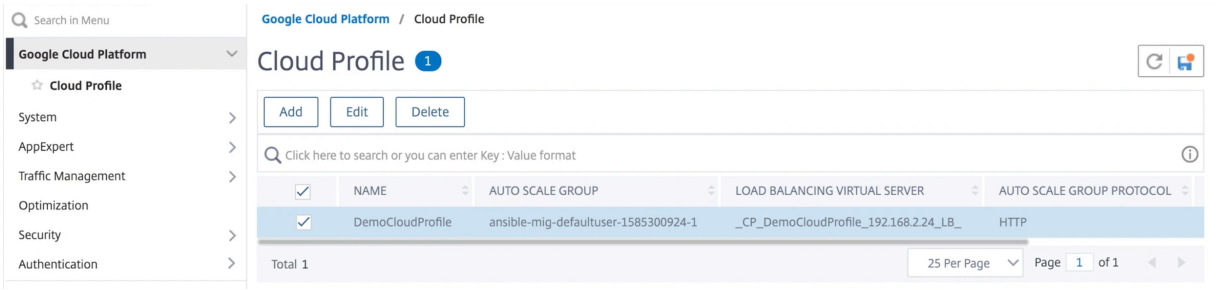


Die Konfigurationsseite „ **Cloud-Profil erstellen** “wird angezeigt.



Cloud Profile erstellt einen virtuellen NetScaler Loadbalancing-Server und eine Dienstgruppe mit Mitgliedern als Servern der verwalteten Instanzgruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

> **Hinweis:**
>
> Ab NetScaler Version 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung verschiedener Ports) mit derselben verwalteten Instanzgruppe in GCP erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.



Unterstützung für VIP-Skalierung für NetScaler VPX-Instanz auf GCP

October 17, 2024

Eine NetScaler-Appliance befindet sich zwischen den Clients und den Servern, sodass Clientanfragen und Serverantworten sie durchlaufen. In einer typischen Installation stellen virtuelle Server, die auf der Appliance konfiguriert sind, Verbindungspunkte bereit, die Clients für den Zugriff auf die Anwendungen hinter der Appliance verwenden. Die Anzahl der öffentlichen virtuellen IP-Adressen (VIP), die für eine Bereitstellung benötigt werden, variiert von Fall zu Fall.

Die GCP-Architektur schränkt jede Schnittstelle der Instanz ein, die mit einer anderen VPC verbunden werden soll. Eine VPC auf GCP ist eine Sammlung von Subnetzen, und jedes Subnetz kann sich über Zonen einer Region erstrecken. Darüber hinaus legt GCP die folgende Einschränkung vor:

- Es gibt eine 1:1 -Zuordnung der Anzahl öffentlicher IP-Adressen zur Anzahl der NICs. Einer NIC kann nur eine öffentliche IP-Adresse zugewiesen werden.
- An einem Instanztyp mit höherer Kapazität können maximal 8 NICs angeschlossen werden.

Zum Beispiel kann eine n1-Standard-2-Instanz nur 2 NICs haben, und die öffentlichen VIPs, die hinzugefügt werden können, sind auf 2 beschränkt. Weitere Informationen finden Sie unter VPC-Ressourcenkontingente.

Um höhere Maßstäbe öffentlicher virtueller IP-Adressen auf einer NetScaler VPX-Instanz zu erreichen, können Sie die VIP-Adressen als Teil der Metadaten der Instanz konfigurieren. Die NetScaler VPX-Instanz verwendet intern Weiterleitungsregeln, die von der GCP bereitgestellt werden, um eine VIP-Skalierung zu erreichen. Die NetScaler VPX-Instanz bietet auch Hochverfügbarkeit für die konfigurierten VIPs. Nachdem Sie VIP-Adressen als Teil der Metadaten konfiguriert haben, können Sie einen virtuellen LB-Server mit derselben IP konfigurieren, die zum Erstellen der Weiterleitungsregeln verwendet wird. Daher können wir Weiterleitungsregeln verwenden, um die Einschränkungen zu mildern, die wir bei der Skalierung bei der Verwendung öffentlicher VIP-Adressen auf einer NetScaler VPX-Instance auf GCP haben.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Punkte zu beachten

- Google berechnet einige zusätzliche Kosten für jede virtuelle IP-Weiterleitungsregel. Die tatsächlichen Kosten hängen von der Anzahl der erstellten Einträge ab. Die damit verbundenen Kosten entnehmen Sie den Google-Preisdokumenten.
- Die Weiterleitungsregeln gelten nur für öffentliche VIPs. Sie können Alias-IP-Adressen verwenden, wenn die Bereitstellung private IP-Adressen als VIPs benötigt.

- Sie können Weiterleitungsregeln nur für die Protokolle erstellen, die den virtuellen LB-Server benötigen. VIPs können im laufenden Betrieb erstellt, aktualisiert oder gelöscht werden. Sie können auch einen neuen virtuellen Lastausgleichsserver mit derselben VIP-Adresse, jedoch mit einem anderen Protokoll hinzufügen.

Vorbereitung

- Die NetScaler VPX-Instanz muss auf GCP bereitgestellt werden.
- Die externe IP-Adresse muss reserviert werden. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]
```

- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Wenn Sie VIP-Skalierung auf einer eigenständigen VPX-Instanz verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
]
```


- Wenn Sie die VIP-Skalierung in einem Hochverfügbarkeitsmodus verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.use",
"compute.instances.get",
"compute.instances.list",
"compute.instances.setMetadata",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.zones.list",
]
```

> **Hinweis:**
>
> Wenn Ihr Dienstkonto in einem Hochverfügbarkeitsmodus keine Eigentümer- oder Bearbeiterrollen hat, müssen Sie die **Rolle Dienstkontobenutzer** zu Ihrem Dienstkonto hinzufügen.

Konfigurieren externer IP-Adressen für die VIP-Skalierung auf der NetScaler VPX-Instanz

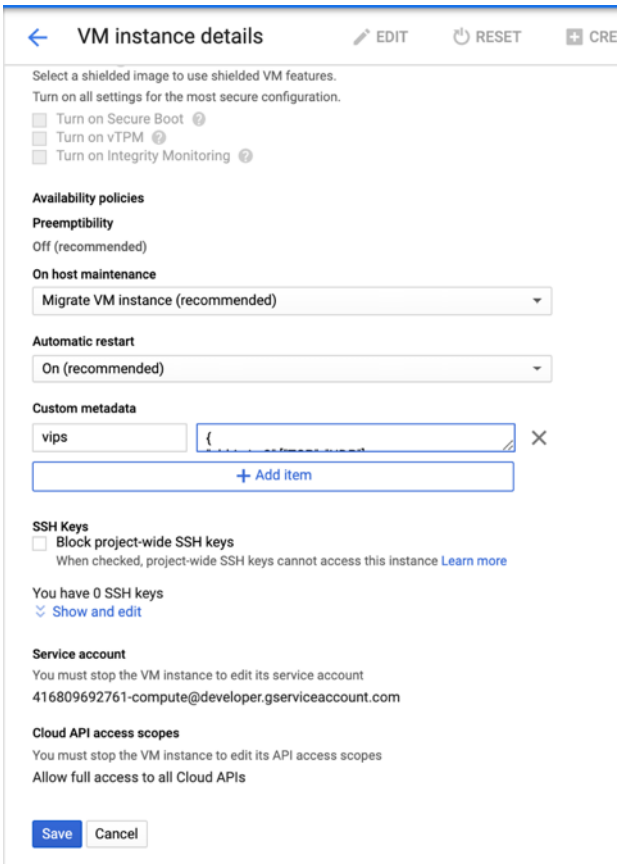
1. Navigieren Sie in der Google Cloud Console zur Seite **VM-Instanzen** .
2. Erstellen Sie eine neue VM-Instanz oder verwenden Sie eine vorhandene Instanz.
3. Klicken Sie auf den Instanznamen. Klicken Sie auf der **Detailseite der VM-Instanz** auf **Bearbeiten**.
4. Aktualisieren Sie die **benutzerdefinierten Metadaten**, indem Sie Folgendes eingeben:
   - Schlüssel = vips
   - Value = Geben Sie einen Wert im folgenden JSON-Format an:

     { “Name der externen reservierten IP”: [Liste der Protokolle], }

   GCP unterstützt die folgenden Protokolle:

   - AH

- ESP
- ICMP
- SCT
- TCP
- UDP



Weitere Informationen finden Sie unter Benutzerdefinierte Metadaten.

Beispiel für benutzerdefinierte Metadaten:

{ “external-ip1-name”:[“TCP”, “UDP”], “external-ip2-name”:[“ICMP”, “AH”] }

In diesem Beispiel erstellt die NetScaler VPX-Instanz intern eine Weiterleitungsregel für jedes IP-Protokollpaar. Die Metadateneinträge werden den Weiterleitungsregeln zugeordnet. Dieses Beispiel hilft Ihnen zu verstehen, wie viele Weiterleitungsregeln für einen Metadateneintrag erstellt werden.

Vier Weiterleitungsregeln werden wie folgt erstellt:

a) external-ip1-Name und TCP
b) external-ip1-Name und UDP
c) external-ip2-name und ICMP
d) external-ip2-name und AH

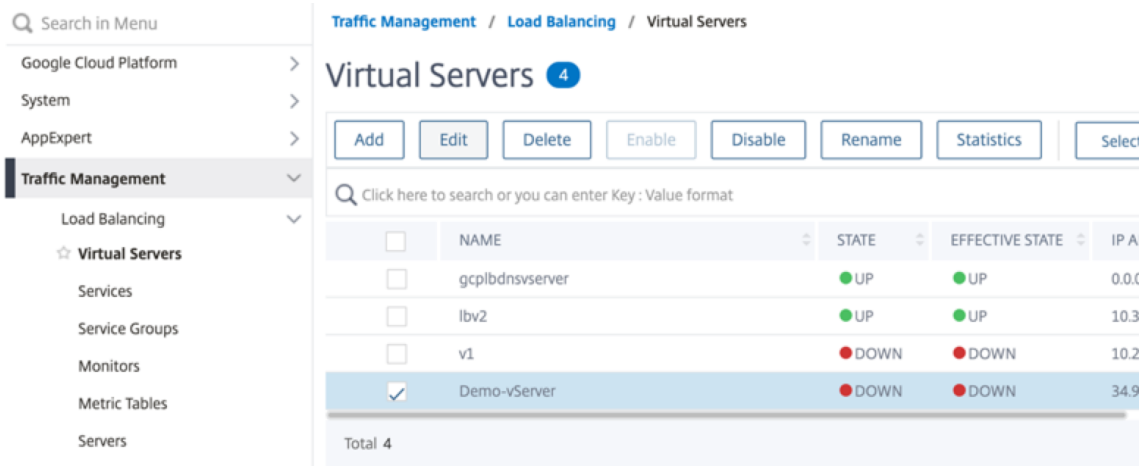
> **Hinweis:**
>
> Im HA-Modus müssen Sie benutzerdefinierte Metadaten nur für die primäre Instanz hinzufügen. Beim Failover werden die benutzerdefinierten Metadaten mit dem neuen Primärgerät synchronisiert.

5. Klicken Sie auf **Speichern**.

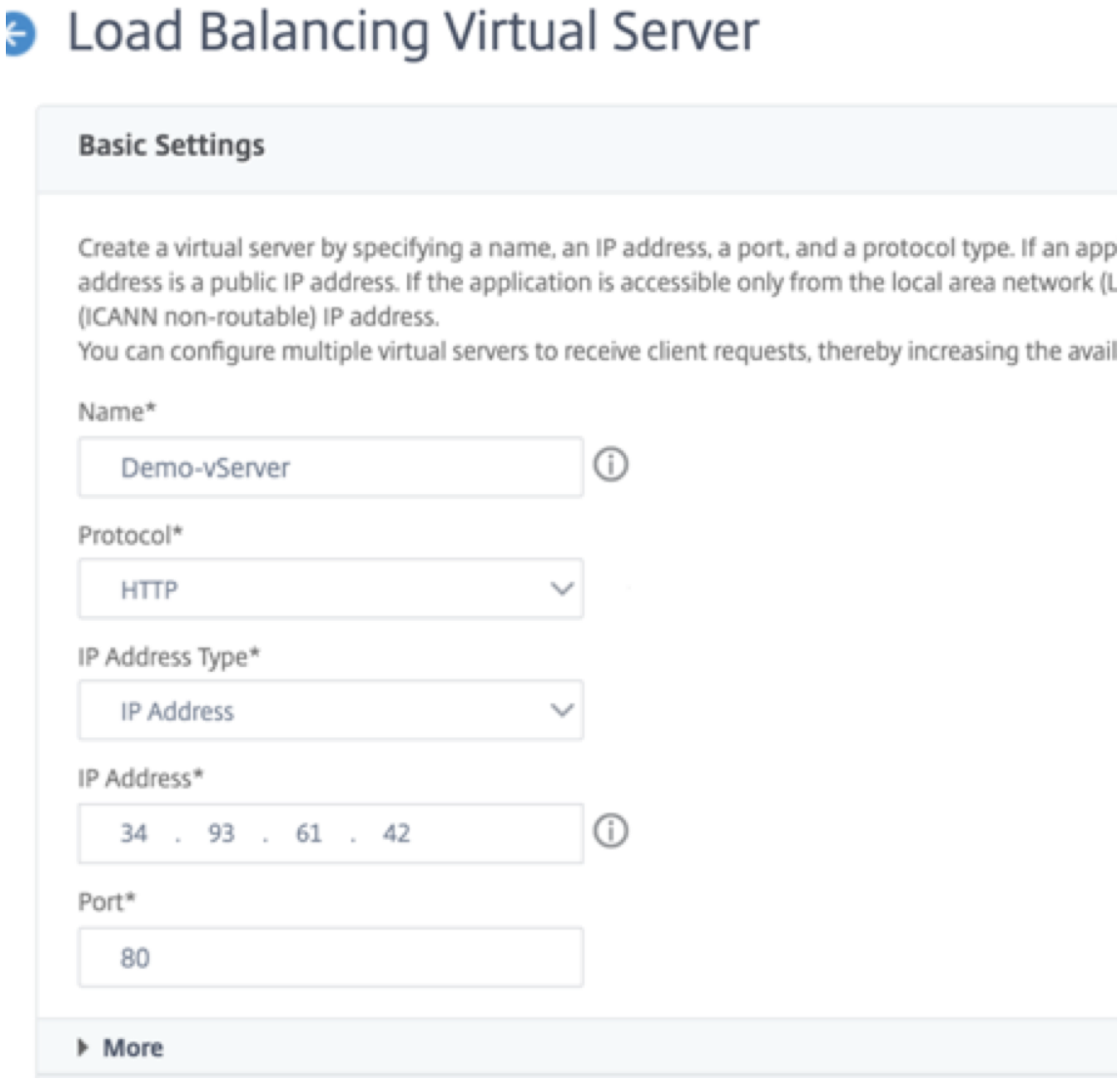
Einrichten eines virtuellen Lastausgleichsservers mit externer IP-Adresse auf einer NetScaler VPX-Instanz

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.

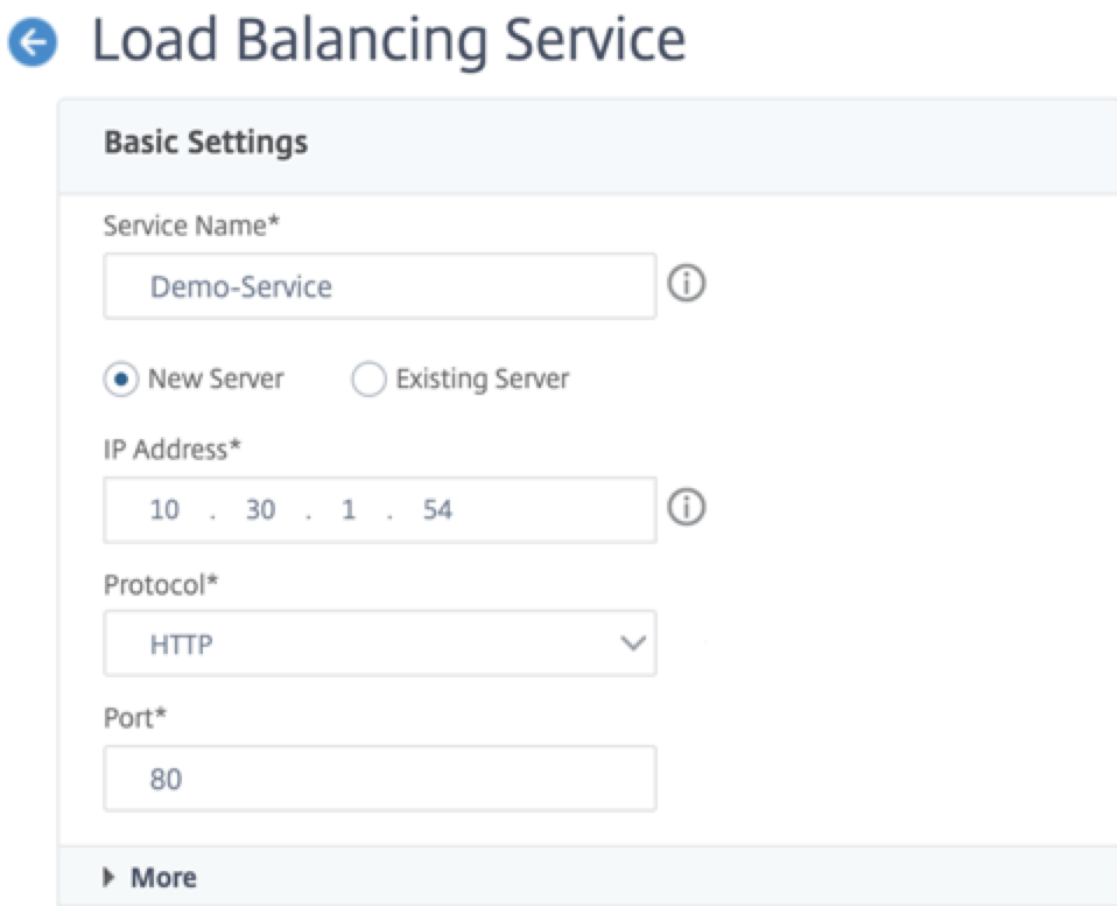


2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Externe IP-Adresse der Weiterleitungsregel, die als VIP auf ADC hinzugefügt wird) und Port hinzu, und klicken Sie auf **OK**.



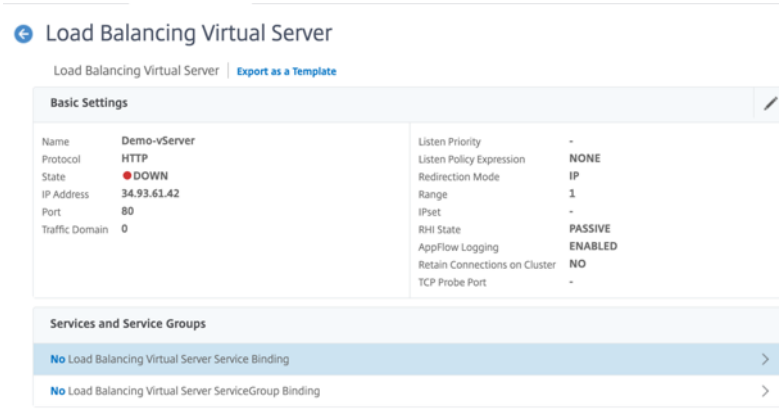
Klicken Sie auf **Mehr**. Fügen Sie einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

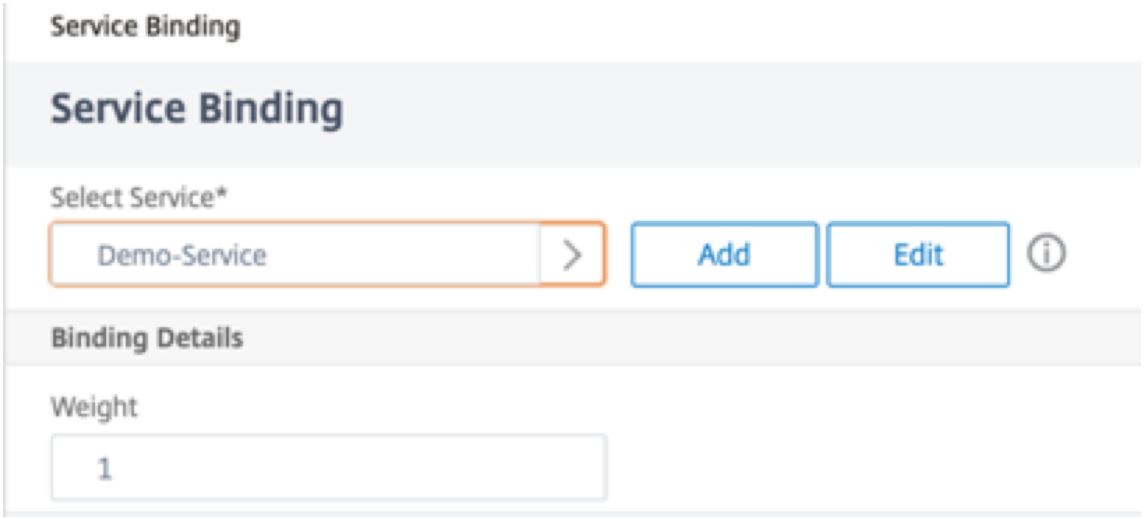


Schritt 3. Fügen Sie einen virtuellen Server in der primären Instanz hinzu. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 1**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.



4. Wählen Sie den in **Schritt 3**konfigurierten Dienst aus und klicken Sie auf "**Binden**".



5. Speichern Sie die Konfiguration.

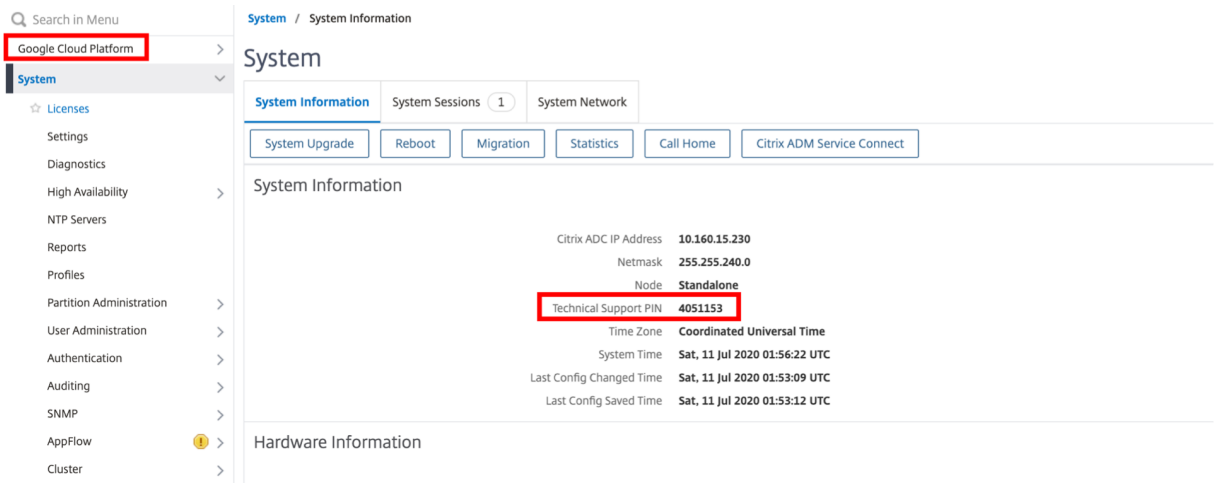
Problembehandlung bei einer VPX-Instanz auf GCP

October 17, 2024

Die Google Cloud Platform (GCP) bietet Konsolenzugriff auf eine NetScaler VPX-Instanz. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz einzusehen, greifen Sie auf die Konsole zu und überprüfen Sie die **Systemprotokolldateien**.

NetScaler unterstützt gebührenpflichtige NetScaler VPX-Instances (Utility-Lizenz mit Stundengebühr) auf GCP. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer GCP-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support. Sie werden gebeten, Ihren Namen und Ihre E-Mail-Adresse anzugeben. Um die Support-PIN zu finden, melden Sie sich an der VPX-GUI an und navigieren Sie zur **Systemseite** .

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



Jumbo-Frames auf NetScaler VPX-Instanzen

October 17, 2024

NetScaler VPX-Appliances unterstützen das Empfangen und Senden von Jumbo-Frames mit bis zu 9216 Byte an IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen als dies mit der standardmäßigen IP-MTU-Größe von 1500 Byte möglich ist.

Eine NetScaler-Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo zu Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Jumbo bis Non-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.
- Von Non-Jumbo zu Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.

Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer NetScaler Appliance.

Unterstützung für Jumbo Frames ist auf NetScaler VPX -Appliances verfügbar, die auf den folgenden Virtualisierungsplattformen ausgeführt werden:

- VMware ESX
- Linux-KVM-Plattform
- Citrix XenServer

- Amazon Web Services (AWS)

Jumbo-Frames auf VPX-Appliances funktionieren ähnlich wie Jumbo-Frames auf MPX-Appliances. Weitere Informationen zu Jumbo Frames und ihren Anwendungsfällen finden Sie unter Konfiguration von Jumbo Frames auf MPX-Appliances. Die Anwendungsfälle von Jumbo-Frames auf MPX-Appliances gelten auch für VPX-Appliances.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf VMware ESX ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf dem VMware ESX-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501-9000 ein. Verwenden Sie die CLI oder GUI, um die MTU-Größe festzulegen. Die NetScaler VPX-Appliances, die auf VMware ESX laufen, unterstützen das Empfangen und Senden von Jumbo-Frames, die nur bis zu 9000 Byte an IP-Daten enthalten.
2. Legen Sie die gleiche MTU-Größe auf den entsprechenden physischen Schnittstellen des VMware ESX-Servers mithilfe der Verwaltungsanwendungen fest. Weitere Informationen zum Festlegen der MTU-Größe auf den physischen Schnittstellen von VMware ESX finden Sie unter http://vmware.com/.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf dem Linux-KVM-Server ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf einem Linux-KVM-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich 1501—9216 ein. Verwenden Sie die NetScaler VPX CLI oder GUI, um die MTU-Größe festzulegen.
2. Stellen Sie dieselbe MTU-Größe auf den entsprechenden physischen Schnittstellen eines Linux-KVM-Servers ein, indem Sie dessen Verwaltungsanwendungen verwenden. Weitere Hinweise zum Festlegen der MTU-Größe auf den physischen Schnittstellen von Linux-KVM finden Sie unter. http://www.linux-kvm.org/

Konfigurieren Sie Jumbo-Frames für eine VPX-Instanz, die auf Citrix XenServer ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf Citrix XenServer ausgeführt wird:

1. Stellen Sie mithilfe von XenCenter eine Verbindung zum XenServer her.
2. Fahren Sie alle VPX-Instanzen herunter, die die Netzwerke verwenden, für die die MTU geändert werden muss.
3. Wählen Sie auf der Registerkarte **Netzwerk** das Netzwerk —Netzwerk 0/1/2 aus.
4. Wählen Sie **Eigenschaften** und bearbeiten Sie MTU.

Nachdem Sie die Jumbo-Frames auf dem XenServer konfiguriert haben, können Sie die Jumbo-Frames auf der ADC-Appliance konfigurieren. Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer NetScaler Appliance.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die in AWS ausgeführt wird

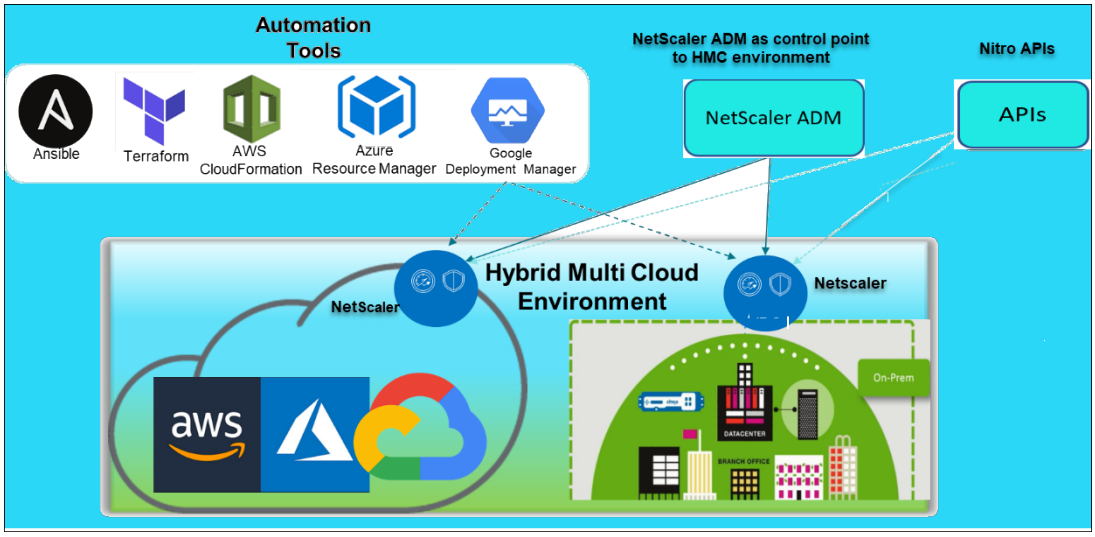
Konfiguration auf Hostebene ist für VPX unter Azure nicht erforderlich. Um Jumbo Frames auf VPX zu konfigurieren, befolgen Sie die Schritte unter Konfigurieren von Jumbo Frames Support auf einer NetScaler Appliance.

Bereitstellung und Konfigurationen von NetScaler automatisieren

October 17, 2024

NetScaler bietet mehrere Tools zur Automatisierung Ihrer ADC-Bereitstellungen und Konfigurationen. Dieses Dokument enthält eine kurze Zusammenfassung verschiedener Automatisierungstools und Verweise auf verschiedene Automatisierungsressourcen, mit denen Sie ADC-Konfigurationen verwalten können.

Die folgende Abbildung bietet einen Überblick über die NetScaler-Automatisierung in einer Hybrid-Multi-Cloud-Umgebung (HMC).



Automatisieren Sie NetScaler mit NetScaler ADM

NetScaler ADM fungiert als Automatisierungskontrollpunkt für Ihre verteilte ADC-Infrastruktur. NetScaler ADM bietet umfassende Automatisierungsfunktionen, von der Bereitstellung bis zur Aktualisierung von ADC-Geräten. Im Folgenden sind die wichtigsten Automatisierungsfunktionen von ADM aufgeführt:

- Provisioning von NetScaler VPX-Instanzen auf AWS
- Provisioning von NetScaler VPX-Instanzen auf Azure
- StyleBooks
- Konfigurationsaufträge
- Konfigurationsaudit
- ADC-Aktualisierungen
- SSL Zertifikatsverwaltung
- Integrationen - GitHub, ServiceNow, Integrationen von Ereignisbenachrichtigungen

NetScaler ADM-Blogs und Videos zur Automatisierung

- Anwendungsmigrationen mit StyleBooks
- Integrieren Sie ADC-Konfigurationen mit CI/CD mithilfe von ADM StyleBooks
- Vereinfachung der Public Cloud NetScaler-Bereitstellungen durch ADM
- 10 Möglichkeiten, wie der NetScaler ADM-Dienst einfachere NetScaler-Upgrades unterstützt

NetScaler ADM bietet für seine verschiedenen Funktionen auch APIs, die NetScaler ADM und NetScaler als Teil der gesamten IT-Automatisierung integrieren. Weitere Informationen finden Sie unter NetScaler ADM Service-APIs.

Automatisieren Sie NetScaler mit Terraform

Terraform ist ein Tool, das Infrastruktur als Code-Ansatz zur Bereitstellung und Verwaltung von Cloud, Infrastruktur oder Service verwendet. NetScaler-Terraform-Ressourcen sind in GitHub zur Verwendung verfügbar. Lesen Sie GitHub für eine ausführliche Dokumentation und Verwendung.

- NetScaler Terraform-Module zur Konfiguration von ADC für verschiedene Anwendungsfälle wie Load Balancing und GSLB
- Terraform Cloud-Skripts zur Bereitstellung von ADC in AWS
- Terraform-Cloud-Skripts zur Bereitstellung von ADC in Azure
- Terraform-Cloud-Skripte zur Bereitstellung von ADC in GCP
- Blau-grüne Bereitstellung mit NetScaler VPX und Azure-Pipelines

Blogs und Videos auf Terraform für die ADC-Automatisierung

- Automatisieren Sie Ihre NetScaler-Bereitstellungen mit Terraform
- Bereitstellung und Konfiguration von ADC im HA-Setup in AWS mithilfe von Terraform

Automatisieren Sie NetScaler mit Consul-Terraform-Sync

Mit dem NetScaler Consul-Terraform-Sync (CTS) -Modul können Anwendungsteams automatisch neue Instanzen von Diensten zu NetScaler hinzufügen oder entfernen. Es ist nicht erforderlich, manuelle Tickets für IT-Administratoren oder Netzwerkteams zu erheben, um die erforderlichen Änderungen der ADC-Konfiguration vorzunehmen.

- NetScaler Consul-Terraform-Sync-Modul für die Automatisierung der Netzwerkinfrastruktur
- Gemeinsames Webinar von Citrix-HashiCorp: Dynamisches Networking mit Consul-Terraform-Sync für Terraform Enterprise und NetScaler

Automatisieren Sie NetScaler mit Ansible

Ansible ist ein Open-Source-Tool zur Softwarebereitstellung, Konfigurationsverwaltung und Anwendungsbereitstellung, das die Infrastruktur als Code ermöglicht. NetScaler Ansible-Module und Beispiel-Playbooks können in GitHub zur Verwendung gefunden werden. Lesen Sie GitHub für eine ausführliche Dokumentation und Verwendung.

- Ansible-Module zur Konfiguration von ADC
- Dokumentation/Referenzhandbuch zu ADC Ansible-Modulen
- Ansible-Module für ADM

Citrix ist ein zertifizierter Ansible Automation Partner. Benutzer mit einem Red Hat Ansible Automation Platform-Abonnement können von Red Hat Automation Hubaus auf NetScaler Collections zugreifen.

Automatisierungsblogs von Terraform und Ansible

- Citrix wurde zum HashiCorp-Integrationspartner des Jahres ernannt
- Citrix ist jetzt zertifizierter Red Hat Ansible Automation Platform Partner
- Terraform und Ansible Automation für App-Bereitstellung und Sicherheit

Public-Cloud-Vorlagen für ADC-Bereitstellungen

Öffentliche Cloudvorlagen vereinfachen die Bereitstellung Ihrer Bereitstellungen in Public Clouds. Für verschiedene Umgebungen stehen verschiedene NetScaler-Vorlagen zur Verfügung. Einzelheiten zur Verwendung finden Sie in den jeweiligen GitHub-Repositorys.

AWS-CFTs:

- CFTs zur Bereitstellung von NetScaler VPX auf AWS

Azure Resource Manager (ARM)-Vorlagen:

- ARM-Vorlagen zur Bereitstellung von NetScaler VPX auf Azure

Google Cloud-Bereitstellungsmanager (GDM) -Vorlagen:

- GDM-Vorlagen zur Bereitstellung von NetScaler VPX bei Google

Videos auf Vorlagen

- Bereitstellen von NetScaler HA in AWS mithilfe der CloudFormation-Vorlage
- Bereitstellen von NetScaler HA über Availability Zones hinweg mit AWS QuickStart
- NetScaler HA-Bereitstellung in GCP mit GDM-Vorlagen

NITRO-APIs

Mit dem NetScaler NITRO-Protokoll können Sie die NetScaler-Appliance programmgesteuert konfigurieren und überwachen, indem Sie Schnittstellen für den Representational State Transfer (REST) verwenden. Daher können NITRO-Anwendungen in jeder Programmiersprache entwickelt werden. Für Anwendungen, die in Java oder .NET oder Python entwickelt werden müssen, werden NITRO-APIs durch relevante Bibliotheken bereitgestellt, die als separate Software Development Kits (SDKs) gepackt sind.

- NITRO-API-Dokumentation
- Beispiel einer ADC-Anwendungsfallkonfiguration mit NITRO API

Häufig gestellte Fragen

October 17, 2024

Der folgende Abschnitt hilft Ihnen bei der Kategorisierung der FAQs basierend auf Citrix Application Delivery Controller (ADC) VPX.

- Feature und Funktionalität
- Verschlüsselung
- Preisgestaltung und Verpackung
- NetScaler VPX Express und 90 Tage kostenlose Testversion
- Hypervisor
- Kapazitätsplanung oder -größe
- Systemanforderungen
- Weitere technische FAQs

Feature und Funktionalität

Was ist NetScaler VPX?

NetScaler VPX ist eine virtuelle ADC-Appliance, die auf einem Hypervisor gehostet werden kann, der auf Industriestandard-Servern installiert ist.

Enthalten NetScaler VPX alle Funktionen zur Optimierung von Webanwendungen als ADC-Appliances?

Ja. NetScaler VPX umfasst alle Lastausgleich, Datenverkehrsverwaltung, Anwendungsbeschleunigung, Anwendungssicherheit (einschließlich NetScaler Gateway und Citrix Application Firewall) und Offload-Funktionen. Einen vollständigen Überblick über die Funktion und Funktionalität von NetScaler finden Sie unter Anwendungsbereitstellung auf Ihre Weise.

Gibt es Einschränkungen bei der Citrix Application Firewall bei der Verwendung auf NetScaler VPX?

Citrix Application Firewall auf NetScaler VPX bietet denselben Sicherheitsschutz wie auf NetScaler-Appliances. Die Leistung oder der Durchsatz von Citrix Application Firewall variiert je nach Plattform.

Gibt es Unterschiede zwischen NetScaler Gateway auf NetScaler VPX und NetScaler Gateway auf NetScaler-Appliances?

Funktionell sind sie identisch. NetScaler Gateway auf NetScaler VPX unterstützt alle NetScaler Gateway-Funktionen, die in NetScaler Softwareversion 14.1 verfügbar sind. Da NetScaler-

Appliances jedoch dedizierte SSL-Beschleunigungshardware bieten, bietet sie eine größere SSL-VPN-Skalierbarkeit als eine NetScaler VPX-Instanz.

Abgesehen von dem offensichtlichen Unterschied, dass NetScaler VPX auf einem Hypervisor ausgeführt werden kann, wie unterscheidet es sich von physischen NetScaler Appliances?

Es gibt zwei Hauptbereiche, in denen Kunden Verhaltensunterschiede feststellen. Das erste ist, dass NetScaler VPX nicht die gleiche Leistung bieten kann wie viele NetScaler-Appliances. Das zweite ist, dass NetScaler-Appliances zwar über eine eigene L2-Netzwerkfunktionalität verfügen, NetScaler VPX jedoch für seine L2-Netzwerkdienste auf den Hypervisor angewiesen ist. Im Allgemeinen schränkt dies nicht ein, wie der NetScaler VPX bereitgestellt werden kann. Es kann bestimmte L2-Funktionen geben, die auf einer physischen NetScaler-Appliance konfiguriert sind und auf dem zugrunde liegenden Hypervisor konfiguriert werden müssen.

Wie spielt NetScaler VPX eine Rolle auf dem Markt für Anwendungsbereitstellung?

NetScaler VPX ändert das Spiel auf dem Markt für Anwendungsbereitstellung auf folgende Weise:

- Indem eine NetScaler-Appliance noch erschwinglicher wird, ermöglicht NetScaler VPX jeder IT-Organisation, eine NetScaler-Appliance bereitzustellen. Dies ist nicht nur für ihre geschäftskritischsten Webanwendungen gedacht, sondern für alle ihre Webanwendungen.
- NetScaler VPX ermöglicht es Kunden, Netzwerk und Virtualisierung in ihren Rechenzentren weiter zu konvergieren. NetScaler VPX kann nicht nur zur Optimierung von Webanwendungen verwendet werden, die auf virtualisierten Servern gehostet werden. Darüber hinaus kann die Bereitstellung von Webanwendungen selbst zu einem virtualisierten Service werden, der einfach und schnell überall bereitgestellt werden kann. IT-Organisationen verwenden die Standard-Rechenzentrumsprozesse für Aufgaben wie Bereitstellung, Automatisierung und Rückladung für die Infrastruktur zur Bereitstellung von Webanwendungen.
- NetScaler VPX eröffnet neue Bereitstellungsarchitekturen, die nicht praktisch sind, wenn nur physische Appliances verwendet werden. NetScaler VPX und NetScaler MPX Appliances können als Basis verwendet werden, die auf die individuellen Bedürfnisse der jeweiligen Anwendung zugeschnitten sind, um prozessorintensive Aktionen wie Komprimierung und Anwendungsfirewall zu verarbeiten. Am Rechenzentrumsrand übernehmen NetScaler MPX-Appliances netzwerkweite Aufgaben mit hohem Volumen wie die anfängliche Datenverkehrsverteilung, SSL-Verschlüsselung oder Entschlüsselung, Denial-of-Service-Angriffsprävention (DoS) und den globalen Lastausgleich. Die Kopplung von leistungsstarken NetScaler MPX-Appliances mit der einfach bereitzustellenden virtuellen NetScaler VPX Appliance bringt beispiellose Flexibilität und Anpassungsfunktionen für moder ne, große Rechenzentrumsumgebungen und reduziert gleichzeitig die Gesamtkosten für Rechenzentren.

Wie passt NetScaler VPX in unsere Citrix Delivery Center-Strategie?

Mit der Verfügbarkeit von NetScaler VPX ist das gesamte Citrix Delivery Center-Angebot als virtualisiertes Angebot verfügbar. Das gesamte Citrix Delivery Center profitiert von den leistungsstarken Verwaltungs-, Bereitstellungs-, Überwachungs- und Berichtsfunktionen, die in Citrix XenCenter verfügbar sind. Dies kann schnell in fast jeder Umgebung eingesetzt und von überall aus zentral verwaltet werden. Mit einer integrierten, virtualisierten Anwendungsbereitstellungsinfrastruktur können Unternehmen Desktops, Client-Server-Anwendungen und Webanwendungen bereitstellen.

Verschlüsselung

Unterstützt NetScaler VPX SSL-Offload?

Ja. NetScaler VPX führt jedoch die gesamte SSL-Verarbeitung in Software durch, sodass NetScaler VPX nicht die gleiche SSL-Leistung wie NetScaler-Appliances bietet. NetScaler VPX kann bis zu 750 neue SSL-Transaktionen pro Sekunde unterstützen.

Beschleunigen SSL-Karten von Drittanbietern, die auf dem Server installiert sind, auf dem NetScaler VPX gehostet wird, die SSL-Verschlüsselung oder -Entschlüsselung?

Nein. Die Unterstützung von SSL-Karten von Drittanbietern kann den NetScaler VPX nicht bestimmten Hardwareimplementierungen zuordnen. Dies verringert die Fähigkeit eines Unternehmens, NetScaler VPX flexibel überall im Rechenzentrum zu hosten. NetScaler MPX-Appliances müssen verwendet werden, wenn mehr SSL-Durchsatz erforderlich ist, als NetScaler VPX bietet.

Unterstützt NetScaler VPX dieselben Verschlüsselungsverschlüsselungen wie physische NetScaler-Appliances?

VPX unterstützt alle Verschlüsselungsverschlüsselungen als physische NetScaler-Appliances, mit Ausnahme der ECDSA.

Was ist der SSL-Transaktionsdurchsatz von NetScaler VPX?

Informationen zum Durchsatz von SSL-Transaktionen finden Sie im NetScaler VPX Datenblatt.

Preisgestaltung und Verpackung

Wie ist NetScaler VPX verpackt?

Die Auswahl von NetScaler VPX ähnelt der Auswahl von NetScaler-Appliances. Zunächst wählt der Kunde die NetScaler Edition basierend auf seinen Funktionsanforderungen aus. Anschließend wählt der Kunde die spezifische NetScaler VPX -Bandbreitenstufe basierend auf den Durchsatzanforderungen aus. NetScaler VPX ist in Standard-, Advanced- und Premium-Editionen verfügbar. NetScaler VPX bietet von 10 Mbit/s (VPX 10) bis 100 Gbit/s (VPX 100G). Weitere Details finden Sie im NetScaler VPX Datenblatt.

Ist der Preis für NetScaler VPX für alle Hypervisoren gleich?

Ja.

Werden dieselben NetScaler-SKUs für VPX auf allen Hypervisoren verwendet?

Ja.

Kann eine NetScaler VPX-Lizenz von einem Hypervisor auf einen anderen verschoben werden (z. B. von VMware auf Hyper-V)?

Ja. NetScaler VPX-Lizenzen sind unabhängig vom zugrunde liegenden Hypervisor. Wenn Sie sich entscheiden, die virtuelle NetScaler VPX-Maschine von einem Hypervisor auf einen anderen zu verschieben, müssen Sie keine neue Lizenz erwerben. Möglicherweise müssen Sie jedoch die vorhandene NetScaler VPX-Lizenz neu hosten.

Können NetScaler VPX-Instanzen aktualisiert werden?

Ja. Sowohl die Durchsatzbeschränkungen als auch die NetScaler Family Edition können aktualisiert werden. Upgrade-SKUs für beide Upgrade-Typen sind verfügbar.

Wie viele Lizenzen benötige ich, wenn ich NetScaler VPX in einem Hochverfügbarkeitspaar bereitstellen möchte?

Wie bei physischen NetScaler-Appliances erfordert eine NetScaler-Hochverfügbarkeitskonfiguration zwei aktive Instanzen. Daher muss der Kunde zwei Lizenzen erwerben.

NetScaler VPX Express und 90 Tage kostenlose Testversion

Enthalten NetScaler VPX Express alle NetScaler-Standardfunktionen? Umfasst es NetScaler Gateway und Load Balancing für Citrix Virtual Apps (ehemals XenApp), Webinterface und XML-Broker?

Ja. NetScaler VPX Express umfasst die volle NetScaler Premium-Funktionalität. Ab der NetScaler-Version 14.1–29.65 hat NetScaler das Verhalten von VPX Express geändert.

Benötigt NetScaler VPX Express eine Lizenz?

Mit der neuesten Version von NetScaler VPX Express (14.1–29.65 und höher) ist die Nutzung von VPX Express kostenlos und erfordert für die Installation oder Nutzung keine Lizenzdatei. Es ist keinerlei Verpflichtung erforderlich. Wenn Sie bereits über eine VPX Express-Lizenz verfügen, bleibt das vorherige Lizenzierungsverhalten bestehen. Wenn Sie jedoch die vorhandene VPX Express-Lizenzdatei entfernen und Version 14.1–29.65 oder höher verwenden, gilt das aktualisierte VPX Express-Verhalten.

Lauf die NetScaler VPX Express-Lizenz ab?

Beim neuen VPX express gibt es keine Lizenz und kein Ablaufdatum. Wenn Sie bereits eine VPX-Express-Lizenz besitzen, erlischt die Lizenz ein Jahr nach dem Download.

Unterstützt NetScaler VPX Express dieselben Verschlüsselungsverschlüsselungen wie NetScaler MPX-Appliances?

Für die allgemeine Verfügbarkeit sind dieselben starken Verschlüsselungsverschlüsselungen, die auf NetScaler-Appliances unterstützt werden, für NetScaler VPX und NetScaler VPX Express verfügbar. Es unterliegt denselben Import- oder Exportvorschriften.

Kann ich technische Supportfälle für NetScaler VPX Express einreichen?

Nein. Benutzer von NetScaler VPX Express können sowohl das NetScaler VPX Knowledge Center nutzen als auch in den Diskussionsforen die Community um Hilfe bitten.

Kann NetScaler VPX Express auf eine Einzelhandelsversion aktualisiert werden?

Ja. Erwerben Sie einfach die NetScaler VPX-Einzelhandelslizenz, die Sie benötigen, und wenden Sie dann die entsprechende Lizenz auf die NetScaler VPX Express-Instanz an.

Hypervisor

Welche VMware-Versionen unterstützt NetScaler VPX?

NetScaler VPX unterstützt VMware ESX und ESXi für Versionen 3.5 oder höher. Weitere Informationen finden Sie unter Supportmatrix und Nutzungsrichtlinien

Wie viele virtuelle Netzwerkschnittstellen können Sie für VMware einem VPX zuweisen?

Sie können einem NetScaler VPX bis zu 10 virtuelle Netzwerkschnittstellen zuweisen.

Wie können wir von vSphere auf die NetScaler VPX-Befehlszeile zugreifen?

Der VMware vSphere-Client bietet über eine Konsolenregisterkarte integrierten Zugriff auf die NetScaler VPX-Befehlszeile. Sie können auch jeden SSH- oder Telnet-Client verwenden, um auf die Befehlszeile zuzugreifen. Sie können die NSIP-Adresse des NetScaler VPX im SSH- oder Telnet-Client verwenden.

Wie können Sie auf die NetScaler VPX GUI zugreifen?

Um auf die NetScaler VPX GUI zuzugreifen, geben Sie die NSIP des NetScaler VPX, beispielsweise `http://NSIP address`, in das Adressfeld eines beliebigen Browsers ein.

Können zwei NetScaler VPX-Instanzen, die auf demselben VMware ESX installiert sind, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja, aber es wird nicht empfohlen. Ein Hardwarefehler würde sich auf beide NetScaler VPX-Instanzen auswirken.

Können zwei NetScaler VPX-Instanzen, die auf zwei verschiedenen VMware ESX-Systemen ausgeführt werden, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja. Es wird in einem Hochverfügbarkeits-Setup empfohlen.

Werden für die VMware interface-bezogene Ereignisse auf NetScaler VPX unterstützt?

Nein. Schnittstellenbezogene Ereignisse werden nicht unterstützt.

Werden für die VMware getaggte VLANs auf NetScaler VPX unterstützt?

Ja. NetScaler-markierte VLANs werden ab Version 11.0 und höher von NetScaler VPX unterstützt. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

Werden Link-Aggregation und LACP für VMware auf NetScaler VPX unterstützt?

Nein. Link Aggregation und LACP werden für NetScaler VPX nicht unterstützt. Die Link-Aggregation muss auf VMware-Ebene konfiguriert werden.

Wie greifen wir auf die NetScaler VPX-Dokumentation zu?

Die Dokumentation ist über die NetScaler VPX GUI verfügbar. Nachdem Sie sich angemeldet haben, wählen Sie die Registerkarte **Dokumentation**.

Kapazitätsplanung oder -größe

Welche Leistung kann ich mit NetScaler VPX erwarten?

NetScaler VPX bietet eine gute Leistung. Ein bestimmtes Leistungsniveau, das mit NetScaler VPX erreicht werden kann, finden Sie im NetScaler VPX Datenblatt.

Wie können wir die maximale Leistung einer NetScaler Instanz schätzen, da die CPU-Leistung des Servers variiert?

Die Verwendung einer schnelleren CPU kann zu einer höheren Leistung führen (bis zu dem von der Lizenz zulässigen Maximum), während die Verwendung einer langsameren CPU die Leistung sicherlich einschränken kann.

Sind NetScaler VPX Bandbreiten- oder Durchsatzbeschränkungen für eingehenden Datenverkehr oder sowohl eingehenden als auch ausgehenden Datenverkehr?

NetScaler VPX-Bandbreitenbeschränkungen werden nur für den Datenverkehr durchgesetzt, der an den NetScaler eingeht, unabhängig davon, ob der Anforderungsverkehr oder der Antwortverkehr erfolgt. Dies zeigt an, dass ein NetScaler VPX-1000 (zum Beispiel) sowohl 1 Gbit/s eingehenden Datenverkehr als auch 1 Gbit/s ausgehenden Datenverkehr gleichzeitig verarbeiten kann. Eingehender und ausgehender Datenverkehr ist nicht identisch mit Anforderungs- und Antwortdatenverkehr. Für den NetScaler ist sowohl der Datenverkehr, der von Endpunkten (Anforderungsverkehr) kommt, als auch Datenverkehr von Ursprungsservern (Antwortverkehr) “eingehend”(d. h.

Können mehrere Instanzen von NetScaler VPX auf demselben Server ausgeführt werden?

Ja. Stellen Sie jedoch sicher, dass der physische Server über genügend CPU- und E/A-Kapazität verfügt, um die gesamte auf dem Host ausgeführte Arbeitslast zu unterstützen, da sonst die Leistung von NetScaler VPX beeinträchtigt werden kann.

Wenn mehr als eine Instanz von NetScaler VPX auf einem physischen Server ausgeführt wird, was ist die Mindestanforderungen für die Hardware pro NetScaler VPX-Instanz?

Jeder NetScaler VPX Instanz muss 2 GB physischen RAM, 20 GB Speicherplatz und 2 vCPUs zugewiesen werden. Für kritische Bereitstellungen empfehlen wir 2 GB RAM für VPX nicht, da das System in einer Umgebung mit begrenztem Arbeitsspeicher betrieben wird. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen. Es werden 4 GB RAM oder 8 GB RAM empfohlen.

> **Hinweis:**
>
> Der NetScaler VPX ist eine latenzempfindliche, leistungsstarke virtuelle Appliance. Um die erwartete Leistung zu erzielen, benötigt die Appliance eine vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert werden. Wenn der Host diese Anforderungen nicht erfüllt, treten Probleme wie Hochverfügbarkeitsfailover, CPU-Anstieg innerhalb der VPX-Instanz, Trägheit beim Zugriff auf die VPX CLI, Absturz des Pitboss-Daemons, Paketausfälle und ein niedriger Durchsatz auf.
>
> Stellen Sie sicher, dass jede VPX-Instanz die vordefinierten Bedingungen erfüllt.

Kann ich NetScaler VPX und andere Anwendungen auf demselben Server hosten?

Ja. Beispielsweise können NetScaler VPX, Citrix Virtual Apps Webinterface und Citrix Virtual Apps XML Broker alle virtualisiert werden und auf demselben Server ausgeführt werden. Stellen Sie für eine optimale Leistung sicher, dass der physische Host über genügend CPU- und E/A-Kapazität verfügt, um alle laufenden Workloads zu unterstützen.

Wird das Hinzufügen von CPU-Kernen zu einer einzelnen NetScaler VPX-Instanz die Leistung dieser Instanz erhöhen?

Abhängig von der Lizenz kann eine NetScaler VPX Instanz heute bis zu 4 vCPU verwenden. Das Hinzufügen einer zusätzlichen CPU zu einer NetScaler VPX-Instanz, die mehr CPUs verwenden kann, erhöht die Leistung.

Warum sieht NetScaler VPX so aus, als würde er mehr als 90% der CPU verbraucht, obwohl er im Leerlauf ist?

Es ist normales Verhalten und NetScaler-Appliances zeigen das gleiche Verhalten. Um die tatsächliche Ausdehnung der NetScaler VPX CPU-Auslastung anzuzeigen, verwenden Sie den Befehl stat CPU in der NetScaler CLI oder zeigen Sie die NetScaler VPX CPU-Auslastung von der NetScaler GUI an. Die NetScaler Paketverarbeitungs-Engine ist immer "auf der Suche nach Arbeit", auch wenn keine Arbeit zu tun ist. Daher tut es alles, um die Kontrolle über die CPU zu übernehmen und sie nicht freizugeben. Auf einem Server, der mit NetScaler VPX und sonst nichts installiert ist, ergibt sich (aus der Sicht des Hypervisors), dass NetScaler VPX die gesamte CPU verbraucht. Ein Blick auf die CPU-Auslastung von "innerhalb von NetScaler"(über die Befehlszeilenschnittstelle oder der GUI) liefert ein Bild der verwendeten NetScaler VPX CPU-Kapazität.

Systemanforderungen

Was sind die Mindestanforderungen an die Hardware für NetScaler VPX?

In der folgenden Tabelle werden die Mindestanforderungen an die Hardware für NetScaler VPX erläutert.

Typ	Anforderungen
Prozessor	Dual-Core-Server mit Intel Xeon oder AMD EPYC.
Speicher	Mindestens 2 GB. Es werden jedoch 4 GB empfohlen.
Datenträger	Mindestens 20 GB Festplatte.
Hypervisor	Citrix Hypervisor 5.6 oder höher, VMware ESX/ESXi 3.5 oder höher oder Windows Server 2008 R2 mit Hyper-V
Netzwerk-Konnek	Mindestens 100 Mbit/s, aber 1 Gbit/s wird empfohlen.
Netzwerkkarte	Eine NIC, die mit dem von Ihnen verwendeten Hypervisor kompatibel ist.

> **Hinweis:**
>
> Für kritische Bereitstellungen werden 4 GB Arbeitsspeicher für NetScaler VPX bevorzugt. Mit 2 GB Arbeitsspeicher arbeitet NetScaler VPX in einer Umgebung mit beschränktem Arbeitsspeicher. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen.

Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

> **Hinweis:**
>
> Ab Version NetScaler 13.1 unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi-Hypervisor AMD EPYC-Prozessoren.

Was ist der Intel VT-x?

Diese Funktionen, die manchmal auch als “Hardwareunterstützung”oder “Virtualisierungshilfe”bezeichnet werden, leiten sensible oder privilegierte CPU-Befehle, die vom Gastbetriebssystem ausgeführt werden, an den Hypervisor ab. Dies vereinfacht das Hosten von Gastbetriebssystemen (BSD für einen NetScaler VPX) auf dem Hypervisor.

Wie üblich sind VT-x?

Praktisch können alle Server, die innerhalb der letzten zwei Jahre ausgeliefert wurden, VT-x unterstützen. Viele Server werden mit deaktivierter Virtualisierungsunterstützung im BIOS ausgeliefert. Bevor Sie davon ausgehen, dass Sie NetScaler VPX nicht ausführen können, prüfen Sie, ob Sie diese Einstellung auf dem Server ändern müssen.

Gibt es eine Hardwarekompatibilitätsliste (HCL) für NetScaler VPX?

Solange der Server Intel VT-x unterstützt, muss NetScaler VPX auf jedem Server laufen, der mit dem zugrunde liegenden Hypervisor kompatibel ist. Eine umfassende Liste der unterstützten Plattformen finden Sie in der Hypervisor-HCL.

Auf welcher Version von NetScaler OS basiert NetScaler VPX?

NetScaler VPX basiert auf NetScaler 9.1 oder höheren Versionen.

Da NetScaler VPX auf BSD läuft, kann es nativ auf einem Server mit installiertem BSD Unix ausgeführt werden?

Nein. NetScaler VPX erfordert die Ausführung des Hypervisors. Detaillierte Hypervisor-Unterstützungen finden Sie im Datenblatt von NetScaler VPX.

Weitere technische FAQs

Funktioniert die Link-Aggregation auf einem physischen Server mit mehreren Netzwerkkarten?

LACP wird nicht unterstützt. Für den Citrix Hypervisor wird die statische Link-Aggregation unterstützt und hat Grenzen von vier Kanälen und sieben virtuellen Schnittstellen. Für VMware wird die statische Link-Aggregation in NetScaler VPX nicht unterstützt, kann aber auf VMware-Ebene konfiguriert werden.

Wird MAC-basierte Weiterleitung (MBF) auf VPX unterstützt? Gibt es Änderungen gegenüber der Implementierung der NetScaler-Appliance?

MBF wird unterstützt und verhält sich genauso wie bei der NetScaler-Appliance. Der Hypervisor schaltet grundsätzlich alle von NetScaler VPX empfangenen Pakete nach außen und umgekehrt.

Wie wird der NetScaler VPX-Upgrade-Prozess durchgeführt?

Upgrades werden genauso ausgeführt wie für NetScaler-Appliances: Laden Sie eine Kerneldatei herunter und verwenden Sie install ns oder das Upgrade-Dienstprogramm in der Benutzeroberfläche.

Wie werden Flash- und Datenträgerspeicher zugewiesen? Können wir es ändern?

/Flash = 965 MB /var = 14G Jeder NetScaler VPX-Instanz müssen mindestens 2 GB Speicher zugewiesen werden. Das NetScaler VPX Disk-Image hatte eine Größe von 20 GB für Wartungszwecke, z. B. Platz für die Aufnahme und Speicherung von bis zu 4 GB Core-Dumps sowie Protokoll- und Trace-Dateien. Obwohl es möglich wäre, ein kleineres Datenträgerimage zu generieren, ist dies derzeit nicht geplant. `/flash` und `/var` sind beide im selben Datenträgerimage. Sie werden aus Kompatibilitätsgründen als separate Dateisysteme aufbewahrt. Ausführliche Empfehlungen zur Speicherzuweisung finden Sie im NetScaler VPX-Datenblatt.

Können wir eine neue Festplatte hinzufügen, um den Speicherplatz auf der NetScaler VPX-Instanz zu erhöhen?

Ja. Ab NetScaler Release 13.1 Build 21.x haben Sie die Möglichkeit, den Speicherplatz auf der NetScaler VPX-Instanz zu vergrößern, indem Sie einen zweiten Datenträger hinzufügen. Wenn Sie den zweiten Datenträger bereitstellen, wird das Verzeichnis "/var/crash"automatisch auf diesem Datenträger bereitgestellt. Der zweite Datenträger wird zum Speichern von Kerndateien und zum Protokollieren verwendet. Bestehende Verzeichnisse, die zum Speichern von Kern- und Protokolldateien verwendet werden, funktionieren weiterhin wie zuvor.

> **Hinweis:**
>
> Nehmen Sie beim Downgrade der NetScaler-Appliance ein externes Backup vor, um Datenverlust zu vermeiden.

Informationen zum Anschließen eines neuen Festplattenlaufwerks (HDD) an eine NetScaler VPX-Instanz in einer Cloud finden Sie in den folgenden Abschnitten:

- Azure-Dokumentation

> **Hinweis:**
>
> Um eine sekundäre Festplatte an in Azure bereitgestellte NetScaler VPX-Instanzen anzuschließen, stellen Sie sicher, dass die Azure-VM-Größen über eine lokale temporäre Festplatte verfügen. Weitere Informationen finden Sie unter Azure-VM-Größen ohne lokalen temporären Datenträger.

- AWS-Dokumentation
- GCP-Dokumentation

> **Warnung:**
>
> Nachdem Sie NetScaler VPX eine neue Festplatte hinzugefügt haben, schlagen einige der Skripts, die mit Dateien arbeiten, die auf die neue Festplatte verschoben werden, unter den folgenden Bedingungen möglicherweise fehl:
>
> Wenn Sie den Shell-Befehl "Link"verwenden, um feste Links zu den Dateien zu erstellen, die auf eine neue Festplatte verschoben wurden.
>
> Ersetzen Sie alle diese Befehle durch "ln -s", um einen symbolischen Link zu verwenden. Ändern Sie auch die fehlgeschlagenen Skripte entsprechend.

Kann ich die Größe der primären Festplatte von NetScaler VPX erhöhen?

Ab NetScaler Version 14.1 Build 21.x können Administratoren die Größe des primären Datenträgers auf NetScaler VPX dynamisch von 20 GB auf 1 TB gleichzeitig erhöhen. Und beim nächsten Mal können Sie wieder auf bis zu 1 TB erhöhen. Um den Speicherplatz zu erhöhen, erweitern Sie die Größe des primären Datenträgers in der jeweiligen Cloud- oder Hypervisor-Benutzeroberfläche auf mindestens 1 GB.

> **Hinweis:**
>
> Sie können nur die Größe der Datenträger erhöhen. Sobald die neue Größe zugewiesen ist, können Sie sie später nicht mehr verringern. Erhöhen Sie daher die Größe der Datenträger nur, wenn dies unbedingt erforderlich ist.

Wie erhöhe ich manuell die Größe des primären Datenträgers auf NetScaler VPX?

Gehen Sie wie folgt vor, um die Größe des primären VPX-Datenträgers von einem Hypervisor oder einer Cloud aus manuell zu erhöhen:

1. Fahren Sie die VM herunter.

2. Erweitern Sie die Standarddatenträgergröße von 20 GB auf einen höheren Wert. Zum Beispiel 20 GB bis 30 GB oder 40 GB. Erweitern Sie für Azure die Standarddatenträgergröße von 32 GB auf 64 GB.
3. Schalten Sie die VM ein und geben Sie die Startaufforderung ein.
4. Loggen Sie sich mit dem Befehl "boot -s"in den Einzelbenutzermodus ein.
5. Überprüfen Sie den Speicherplatz. Sie können den neu zugewiesenen Speicherplatz mit dem Befehl "gpart show"überprüfen.
6. Notieren Sie sich den Partitionsnamen. Die VM-Partition ist beispielsweise da0.
7. Ändern Sie die Größe der Datenträgerpartition mit dem Befehl "gpart resize".

   Beispiel: Ändern wir die Größe der MBR-Partition da0, um 10 GB freien Speicherplatz einzuschließen, indem wir den folgenden Befehl ausführen.

   ```
   gpart resize -i 1 da0
   ```

8. Fügt den freien Speicherplatz mit der letzten Partition zusammen.

   Beispiel

   ```
   gpart resize -i 5 da0s1
   ```

9. Erweitern Sie das Dateisystem mit dem Befehl "growfs", um neu zugewiesenen freien Speicherplatz einzubeziehen.

   Beispiel

   ```
   growfs /dev/ada0s1e
   ```

10. Starten Sie die VM neu und überprüfen Sie den erhöhten Speicherplatz mit dem Befehl "df -h" an der Shell-Eingabeaufforderung.

Was können wir erwarten, dass die NetScaler VPX Build-Nummerierung und die Interoperabilität mit anderen Builds berücksichtigt werden?

NetScaler VPX hat eine ähnliche Build-Nummerierung wie die 9.1. Cl (klassisch) und 9.1. Nc (NCore) -Versionen, zum Beispiel 9.1_97.3.vpx, 9.1_97.3.nc und 9.1_97.3.cl.

Kann der NetScaler VPX Teil eines Hochverfügbarkeitssetups mit einer NetScaler-Appliance sein?

Keine unterstützte Konfiguration.

Befinden sich alle in NetScaler VPX sichtbaren Schnittstellen in direktem Zusammenhang mit der Anzahl der Schnittstellen auf dem Hypervisor?

Nein. Sie können bis zu sieben Schnittstellen (10 für VMware) über das NetScaler VPX Konfigurationsprogramm mit nur einer physischen Netzwerkkarte auf dem Hypervisor hinzufügen.

Kann Citrix Hypervisor XenMotion oder VMware vMotion oder Hyper-V Livemigration verwendet werden, um aktive Instanzen von NetScaler VPX zu verschieben?

NetScaler VPX unterstützt keine Hyper-V-Livemigration. vMotion wird ab NetScaler Version 13.0 unterstützt. Live-Migration (früher XenMotion) wird ab der NetScaler Version 14.1 Build 17.38 unterstützt.