net>scaler

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	6
Optimieren der Leistung von NetScaler VPX auf VMware ESX, Linux KVM und Citrix Hyper- visors	14
Unterstützung für die Erhöhung des NetScaler VPX-Speicherplatzes	31
NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in der Cloud anwenden	34
Verbessern der SSL-TPS-Leistung auf Public-Cloud-Plattformen	69
Gleichzeitiges Multithreading für NetScaler VPX in öffentlichen Clouds konfigurieren	70
NetScaler Sanity Checker-Tool	74
Installieren einer NetScaler VPX Instanz auf einem Bare-Metal-Server	76
Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor/XenServer	77
Konfigurieren von VPX-Instanzen für die Verwendung von Single-Root-I/O-Virtualisierungs- Netzwerkschnittstellen (SR-IOV)	80
Installieren einer NetScaler VPX-Instanz auf VMware ESX	86
Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der VMXNET3- Netzwerkschnittstelle	91
Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnitt	stelle104
Konfigurieren Sie einen NetScaler VPX auf dem ESX-Hypervisor, um Intel QAT für die SSL- Beschleunigung im SR-IOV-Modus zu verwenden	122
Migration des NetScaler VPX von E1000 auf SR-IOV- oder VMXNET3-Netzwerkschnittstellen	126
Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der PCI-Passthrough- Netzwerkschnittstelle	127
Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem VMware ESX Hypervisor	130
Installieren einer NetScaler VPX-Instanz in der VMware Cloud auf AWS	140

Installieren Sie eine NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server	143
Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform	148
Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf der Linux-KVM- Plattform	149
Bereitstellen der NetScaler VPX Instanz mithilfe von OpenStack	154
NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitstellen	163
Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerksch	nittstellen178
Konfigurieren Sie einen NetScaler VPX auf dem KVM-Hypervisor, um Intel QAT für die SSL- Beschleunigung im SR-IOV-Modus zu verwenden	189
Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von PCI-Passthrough- Netzwerkschnittstellen	195
Stellen Sie die NetScaler VPX-Instanz mithilfe des virsh Programms bereit	199
Verwalten der NetScaler VPX Gast-VMs	203
Stellen Sie die NetScaler VPX-Instanz mit SR-IOV auf OpenStack bereit	206
Konfigurieren Sie eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS-DPDK- basierten Hostschnittstellen	213
Anwenden der NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem KVM-Hypervisor	223
NetScaler VPX auf AWS	225
AWS-Terminologie	228
AWS-VPX-Unterstützungsmatrix	231
Einschränkungen und Nutzungsrichtlinien	234
Voraussetzungen	236
AWS IAM-Rollen auf der NetScaler VPX-Instanz konfigurieren	238
So funktioniert eine NetScaler VPX-Instanz auf AWS	250
Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS	251

Szenario: Standalone-Instanz	257
Download einer NetScaler VPX-Lizenz	266
Lastausgleichsserver in verschiedenen Availability Zones	273
So funktioniert Hochverfügbarkeit auf AWS	274
Bereitstellen eines VPX-HA-Paar in derselben AWS-Verfügbarkeitszone	276
Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen	288
Bereitstellen eines VPX Hochverfügbarkeitspaars mit elastischen IP-Adressen in ver- schiedenen AWS-Zonen	289
Bereitstellen eines VPX Hochverfügbarkeitspaars mit privaten IP-Adressen in verschiede- nen AWS-Zonen	294
Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts	307
Schützen Sie das AWS API Gateway mithilfe der NetScaler Web App Firewall	311
Fügen Sie den Back-End-Dienst AWS Autoscaling hinzu	315
NetScaler GSLB auf AWS bereitstellen	320
Stellen Sie NetScaler Web App Firewall auf AWS bereit	337
Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnitt	stelle362
Konfigurieren einer NetScaler VPX-Instanz für die Verwendung von Enhanced Networking	265
	365
Aktualisieren einer NetScaler VPX-Instanz auf AWS	365
Problembehandlung bei einer VPX-Instanz in AWS	371
AWS FAQs	372
Bereitstellen einer NetScaler VPX Instanz unter Microsoft Azure	376
Azure-Terminologie	381
Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure	385
Eigenständige NetScaler VPX-Instanz konfigurieren	388

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren	402
Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren	409
Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzw- erkkarten über PowerShell-Befehle	420
NetScaler-Hochverfügbarkeitspaar auf Azure mit ALB im Floating IP-Deaktiviert-Modus bereitstellen	432
Stellen Sie eine private NetScaler for Azure DNS-Zone bereit	453
Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von Azure Accelerated Networking	475
Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage mit Azure ILB	492
Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage für mit dem Internet verbundene Anwendungen	505
Hochverfügbarkeitssetup mit externen und internen Load Balancern von Azure gle- ichzeitig konfigurieren	516
Installieren Sie eine NetScaler VPX-Instanz auf Azure VMware Solution	522
Eigenständige NetScaler VPX-Instanz auf der Azure VMware-Lösung konfigurieren	538
NetScaler VPX-Hochverfügbarkeitssetups auf Azure VMware-Lösung konfigurieren	540
Azure-Routenserver mit NetScaler VPX HA-Paar konfigurieren	542
Back-End-Azure-Autoscaling-Dienst hinzufügen	546
Azure-Tags für NetScaler VPX Bereitstellung	555
Konfigurieren von GSLB auf NetScaler VPX-Instanzen	560
Konfigurieren Sie GSLB in einem aktiven Standby-Hochverfügbarkeits-Setup	569
NetScaler GSLB auf Azure bereitstellen	574
NetScaler Web App Firewall auf Azure bereitstellen	589
Konfigurieren der Intranet-IP für Adresspools für eine NetScaler Gateway-App	615

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz über PowerShell- Befehle konfigurieren	617
Zusätzliche PowerShell -Skripts für die Azure-Bereitstellung	625
Erstellen Sie ein Support-Ticket für die VPX-Instanz in Azure	641
Häufig gestellte Fragen zu Azure	643
Bereitstellen einer NetScaler VPX Instanz auf der Google Cloud Platform	644
Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform	659
Stellen Sie ein VPX Hochverfügbarkeitspaar mit externer statischer IP-Adresse auf der Google Cloud Platform bereit	661
Einzelnes NIC-VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereitstellen	672
Stellen Sie ein VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereit	682
NetScaler VPX-Instanz auf Google Cloud VMware Engine bereitstellen	691
Back-End-GCP-Autoscaling-Dienst hinzufügen	711
Unterstützung für VIP-Skalierung für NetScaler VPX-Instanz auf GCP	717
Problembehandlung bei einer VPX-Instanz auf GCP	724
Jumbo-Frames auf NetScaler VPX-Instanzen	725
Bereitstellung und Konfigurationen von NetScaler automatisieren	727
Häufig gestellte Fragen	730

NetScaler VPX-Unterstützungsmatrix

June 12, 2025

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-			
	VeröffentlichungsdatE6Xi-Build-		NetScaler VPX	
ESXi-Version	(YYYY/MM/DD)	Nummer	Version	Leistungsbereich
ESXi 8.0 Update	10.04.2025	24674464	14.1-43.x und	
3e			höhere Builds	
ESX 8.0-Update	2025/03/04	24585383	14.1-38.x und	10 Mbit/s bis 100
2d			höhere Builds	Gbit/s
ESXi 8.0 Update	23.01.2025	24414501	14.1-29.x und	·
3c			höhere Builds	
ESXi 8.0 Update	17.09.2024	24280767	14.1-17.x und	
3b			höhere Builds	
ESXi 8.0 Update 3	2024/06/25	24022510	14.1-17.x und	
			höhere Builds	
VPX 10, VPX 25,	_	23825572	14.1-17.x und	
VPX 200, VPX			höhere Builds	
1000, VPX 3000,				
VPX 5000, VPX				
8000, VPX 10 G,				
VPX 15 G. VPX				
25G. VPX 40G. VPX				
100G				
ESXi 8.0 update	2024/02/29	23305546	14.1-4.x und	
2b			höhere Builds	
ESXi 8.0 Update 2	2023/09/21	22380479	14.1-4.x und	
·			höhere Builds	
ESXi 8.0-	2023/04/18	21495797	14.1-4.x und	
Aktualisierung 1			höhere Builds	
ESXi 8.0c	2023/03/30	21493926	14.1-4.x und	
	,,		höhere Builds	

	ESXi-						
	Veröffentlichung	sdatE£67Xi-Build-	NetScaler VPX	NetScaler VPX			
ESXi-Version	(YYYY/MM/DD)	Nummer	Version	Leistungsbereich			
ESXi 8.0	2022/10/11	20513097	14.1-4.x und				
			höhere Builds				
ESXi 7.0 Update	2025/03/04	24585291	14.1-29.x und				
3s			höhere Builds				
ESXi 7.0 Update	2024/12/12	24411414	14.1-29.x und				
3r			höhere Builds				
ESXi 7.0 Update	_	23794027	14.1-17.x und				
30			höhere Builds				
ESXi 7.0 update	_	23307199	14.1-4.x und				
Зр			höhere Builds				
ESXi 7.0 Update	2023/09/28	22348816	14.1-4.x und				
3m			höhere Builds				
ESXi 7.0	2023/07/06	21930508	14.1-8.x und				
Aktualisierung 3n			höhere Builds				
ESXi 7.0 Update	2023/05/03	21686933	14.1-4.x und				
3m			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	450070	10 Mbit/s bis 100 Gbit/s
Ubuntu 16.04, Ubuntu 18.04,		
Ubuntu 22.04		

Wichtige Hinweise:

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

 Die VPX-Instanz ist f
ür Hypervisor Releaseversionen in Tabelle 1–4 und nicht f
ür Patch-Releases innerhalb einer Version qualifiziert. Es wird jedoch erwartet, dass die VPX-Instanz nahtlos mit Patch-Versionen einer unterst
ützten Version funktioniert. Wenn dies nicht der Fall ist, öffnen Sie einen Supportfall f
ür 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 h

 ängen 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 ES	SX			
^^Funk	tionen		~~				۸۸	۸۸		
* Interfa	ceBV	SR-	PV	SR-	Emul	iertPCI-	PV	PV	SR-	PCI-
→		IOV		IOV		Passtł	nrough		IOV	Passthrough
Multi- PE- Unters	Ja tützung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

NetScaler VPX 14.1

^^Funkt	ionen									
\checkmark	٨٨		۸۸				٨٨	٨٨		
Clusteri Unterst	n g: ützung	Ja¹	Ja	Ja¹	Ja	Ja	Ja	Ja	Ja¹	Ja
VLAN- Tagging	Ja	Ja	Ja	Ja	Ja	Ja	Ja (nur bei 2012R2)	Ja	Ja	Ja
Erkenne von Link-	enNein²	Ja ³	Nein ²	Ja ³	Nein ²	Ja ³	Nein ²	Nein ²	Ja ³	Ja³
Ereignis	sen/HAN	lon								
Konfigu der Schnitts len- para- meter	raltion stel-	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
Statisch LA	ela²	Ja³	Ja²	Nein	Ja²	Ja³	Ja²	Ja²	Ja ³	Ja³
LACP	Nein	Ja³	Ja²	Nein	Ja²	Ja³	Nein	Ja²	Ja³	Ja³
Statisch CLAG	e Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
LACP CLAG	Nein	Nein	Ja²	Nein	Ja²	Ja³	Nein	Ja²	Ja³	Ja³
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 ↓	٨٨	^^	^^
Multi-PE-	Ja	Ja	Ja
Unterstützung			
Clustering-	Nein	Nein	Nein
Unterstützung			
VLAN-Tagging	Nein	Nein	Nein
Erkennen von Link-	Nein ²	Nein ²	Nein ²
Ereignissen/HAMon			
Konfiguration der	Nein	Nein	Nein
Schnittstellenpara-			
meter			
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 Link-Ereignis (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 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-, SRIOVund ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn versucht wird, Hot-Removal durchzuführen.

Unterstützte Browser

Informationen zu unterstützten Browsern für den Zugriff auf die NetScaler-GUI-Versionen 14.1 und 13.1 finden Sie unter Kompatible Browser.

Plattformen	Intel-Prozessor	AMD-Prozessor
Citrix Hypervisor	Ja	Nein
ESXi-Hypervisor	Ja	Ja
Hyper-V	Ja	Nein
KVM	Ja	Nein
AWS	Ja	Ja
Azure	Ja	Ja
GCP	Ja	Ja

Unterstützte Prozessoren für NetScaler VPX

Unterstützte Netzwerkkarten für NetScaler VPX

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/> SRIOV VF	Intel XL7X1010/XL710/XXV710 PCI- Passthrough- Modus
^^Plattforme	en					
\checkmark	٨٨	٨٨	٨٨	~ ~	٨٨	٨٨
Citrix Hypervisor	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Ja	Nein
ESXi-	Nein	Ja	Nein	Ja	Nein	Ja
Hypervisor Hyper-V	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nein	Nein	Nein
KVM	Nein	Ja	Ja	Ja	Ja	Nein
AWS	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Nicht verfügbar	Nicht verfügbar
Azure	Ja	Ja	Ja	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
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 Citrix Ready-Partnerseite.
- 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

April 1, 2025

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 einer VMNIC zu ermitteln, melden Sie sich lokal oder remote beim Host an und geben Sie Folgendes ein:

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

 Informationen zum Festlegen der NUMA- und vCPU-Affinität f
ür 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:

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

- Für ESX ab Version 6.0:

```
1 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:

1

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 2.2.2.2 255.255.0
```

• 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:

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

- Für ESX ab Version 6.0:

1 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:

```
1 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:

```
1 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 SANbasierten 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 f
 ür die VM, der sie zugewiesen wurden. Diese Option zeigt in Hypervisor- und Cloud-Umgebungen einen h
 öheren Prozentsatz f
 ür 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.

[root@localhost ~]# lstopo-no-graphics
Machine (12808)
Socket L#0 + L3 L#0 (20MR)
L2 L#0 (256KB) + L1d L#0 (32KB) + L1i L#0 (32KB) + Core L#0 + PU L#0 (P#0)
L2 L#1 (256KB) + L1d L#1 (32KB) + L1i L#1 (32KB) + Core L#1 + PU L#1 (P#1)
L2 L#2 (256KB) + L1d L#2 (32KB) + L1i L#2 (32KB) + Core L#2 + PU L#2 (P#2)
L2 L#3 (256KB) + L1d L#3 (32KB) + L1i L#3 (32KB) + Core L#3 + PU L#3 (P#3)
L2 L#4 (256KB) + L1d L#4 (32KB) + L11 L#4 (32KB) + Core L#4 + PU L#4 (P#4)
L2 L#5 (256KB) + L1d L#5 (32KB) + L11 L#5 (32KB) + Core L#5 + PU L#5 (P#5)
L2 L#6 (256KB) + L1d L#6 (32KB) + L11 L#6 (32KB) + Core L#6 + PU L#6 (P#6)
L2 L#/ (230KD) + L10 L#/ (32KD) + L11 L#/ (32KD) + C010 L#/ + P0 L#/ (P#/) HostBridge L#0
PCIBridge
PCI 8086:1521
Net L#0 "enol"
PCI 8086:1521
Net L#1 "eno2"
PCIBridge
PCI 8085:1584
PCTPridee
PCI 8086:1584
Net L#3 "ens4"
PCI 8086:8d62
Block L#4 "sda"
Block L#5 "sdb"
PCIBridge
PCT 1a03-2000
GPU L#6 "card0"
GPU L#7 "controlD64"
PCT_8086+8d92
NUMANode L#1 (P#1 64GB)
Socket L#1 + L3 L#1 (20MB)
L2 L#8 (200B) + L10 L#8 (34AB) + L11 L#8 (34AB) + COFE L#8 + PU L#8 (P#8) 12 L#9 (256KB) + L10 L#9 (32AB) + L11 L#8 (32AB) + COFE L#8 + PU L#8 (P#8)
L2 L#10 (256KB) + L1d L#10 (32KB) + L11 L#10 (32KB) + Core L#10 + PU L#10 (P#10)
L2 L#11 (256KB) + L1d L#11 (32KB) + L11 L#11 (32KB) + Core L#11 + PU L#11 (P#11)
L2 L#12 (256KB) + L1d L#12 (32KB) + L1i L#12 (32KB) + Core L#12 + PU L#12 (P#12)
L2 L#13 (256KB) + L1d L#13 (32KB) + L1i L#13 (32KB) + Core L#13 + PU L#13 (P#13)
L2 L#14 (256KB) + L1d L#14 (32KB) + L11 L#14 (32KB) + Core L#14 + PU L#14 (P#14)
L2 L#15 (256KB) + L1d L#15 (32KB) + L11 L#15 (32KB) + Core L#15 + PU L#15 (P#15)
DCTR://do
PCI 8086:1584
Net L#8 "ens2"
PClBridge
PCI 8086:10fb
Net L#9 "enslf0"
PUI 8080:10TD
DCT FFFF.FFFF
Net L#11 "enp131s16"
[root@localhost ~]# modprobe kvm-intel acpienv=N
[rest0]eee]heet]#]e

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.

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

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

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

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

2. Fügen Sie das folgende Tag hinzu:

- 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



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

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

1 mpstat -P ALL 5

inux 3.	10.0	-123.e	17.x86_	64 (local	host.lo	caldomain)	0.	5/17/201	6 _	x86_64_		16 CPU)
2:26:20	PM	CPU	<pre>%usr</pre>	<pre>%nice</pre>	%sys	<pre>%iowait</pre>	\$irg	%soft	<pre>%steal</pre>	%guest	%gnice	\$idle
2:26:25	PM	all	0.24	0.00	1.67	0.00	0.00	0.00	0.00	17,32	0.00	80.78
2:26:25	PM		0.20	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	98.80
2:26:25	PM		0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.60
2:26:25	PM		0.20	0.00	0.40	0.00	0.00	0.00	0.00	0.00	0.00	99.40
2:26:25	PM		0.00	0.00	0.20	0.00	0.00	0,00	0.00	0.00	0.00	99.80
2:26:25	PM	4	0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.60
2:26:25	PM		0.60	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.20
2:26:25	PM		0.40	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	99.60
2:26:25	PM		1.62	0.00	1.42	0.00	0.00	0.00	0.00	0.00	0.00	96.90
2:26:25	PM		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
2:26:25	PM		0.00	0.00	7.60	0.00	0.00	0.00	0.00	92.40	0.00	0.00
2:26:25	PM	10	0.20	0.00	7.00	0.00	0.00	0.00	0.00	92,80	0.00	0.00
2:26:25	PM	11	0.00	0.00	8.60	0.00	0.00	0.00	0.00	91.40	0.00	0.00
2:26:25	PM	12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
2:26:25	PM	13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM	14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0
2:26:25	PM	15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.0

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:

1	virsh	vcpupin	<vpx name=""> <vcpu id=""> <pcpu number=""></pcpu></vcpu></vpx>
2	virsh	vcpupin	NetScaler-VPX-XML 0 8
3	virsh	vcpupin	NetScaler-VPX-XML 1 9
4	virsh	vcpupin	NetScaler-VPX-XML 2 10
5	virsh	vcpupin	NetScaler-VPX-XML 3 11

- 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

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

2. Fügen Sie das folgende Tag hinzu:

- 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 vC-PUs 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

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

```
1 echo 0000000f > /proc/irq/55/smp_affinity
2 0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
only be scheduled on pCPUs 0 - 3
```

• 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:

- WTM-TV MAMP SALARA NUTY)
 0
 ×

 Serve Vew Toke Hep
 0
 ×

 Serve Vew Toke Hep
 0
 ×
 0

 Serve Vew Toke Hep
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
- 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-<pidof-qemu>).
- 3. Binden Sie die vHost-Prozesse mit dem folgenden Befehl an die zuvor identifizierten physischen Kerne in der NUMA-Domäne:

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

Beispiel

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

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:

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

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":

```
1 xl info -n
```

Pin vCPUs von VPX an physische Kerne.

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

Überprüfen Sie die Bindung von vCPUs.

1 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:

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

Im folgenden Beispiel zeigen diese Werte an:

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

[root@xenserve	r-uu	ffyqlx ~]	# xl lis	t					
Name				I	D	Mem	VCPUs	State	e Time(s)
Domain-0					0	4092	8	r	633321.0
Sai_VPX					5	8192	4	r	1529471.0
[root@xenserve	r-uu	ffyqlx ~]	#						
[root@xenserve	r-uu	ffyqlx ~]	#						
[root@xenserve	r-uu	ffyqlx ~]	# ps -ax	grep "v	if	5"			
Warning: bad s	yntax	x, perhap	s a bogu	s '-'? See		usr/sl	hare/d	loc/procps-3	3.2.7/FAQ
20447 pts/6	S+	0:00	grep vif	5					
29187 ?	S	1:09	[vif5.0-	guest-rx]					
29188 ?	S	0:00	[vif5.0-	dealloc]					
29189 ?	S	201:33	[vif5.1-	guest-rx]					
29190 ?	S	80:51	[vif5.1-	dealloc]					
29191 ?	S	0:20	[vif5.2-	guest-rx]					
29192 ?	S	0:00	[vif5.2-	dealloc]					
[root@xenserve	r-uu:	ffyqlx ~]	#						

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

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

Beispiel

1 taskset -pc 1 29189

Unterstützung für die Erhöhung des NetScaler VPX-Speicherplatzes

March 20, 2025

NetScaler VPX unterstützt einen Standardspeicherplatz von 20 GB. Wenn Sie aus verschiedenen Gründen auf Einschränkungen der Datenträgergröße stoßen, stehen die folgenden Optionen zur Verfügung, um den VPX-Speicherplatz zu erhöhen:

- Erhöhen Sie manuell die Größe des primären Datenträgers
- Erhöhen Sie dynamisch die Größe des primären Datenträgers
- Einen sekundären Datenträger hinzufügen

Hinweis:

Die Möglichkeit, den NetScaler VPX-Festplattenspeicherplatz zu erhöhen, ist sowohl für VPX-Bereitstellungen vor Ort als auch für VPX-Cloud-Bereitstellungen verfügbar. Die Größenänderung der primären Festplatte von NetScaler VPX wird bei Verwendung des SDX-Verwaltungsdienstes nicht unterstützt.

Erhöhen Sie die Größe des primären Datenträgers auf NetScaler VPX manuell

Befolgen Sie diese Schritte, um die Größe der primären VPX-Festplatte mithilfe eines Hypervisors oder einer Cloud-Plattform manuell zu erhöhen:

- 1. Fahren Sie die VM herunter.
- 2. Erweitern Sie die Standardfestplattengröße von 20 GB auf einen höheren Wert, beispielsweise 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. Melden Sie sich mit dem Befehl boot -s im Einzelbenutzermodus an.
- 5. Überprüfen Sie den Speicherplatz. Sie können den neu zugewiesenen Speicherplatz mit dem Befehl gpart show überprüfen.
- 6. Notieren Sie sich den Partitionsnamen. Im folgenden Beispiel ist die VM-Partition da0.
- 7. Ändern Sie die Größe der Festplattenpartition 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 einzuschließen.

Beispiel

growfs /dev/da0s1e

10. Starten Sie die VM neu und überprüfen Sie den erhöhten Speicherplatz mit dem Befehl df −h in der Shell-Eingabeaufforderung.

Erhöhen Sie dynamisch die Größe des primären Datenträgers auf NetScaler VPX

Administratoren können die primäre Festplattengröße auf NetScaler VPX dynamisch von 20 GB auf bis zu 1 TB erhöhen. Bei jeder weiteren Erhöhung ist eine nochmalige Erweiterung auf bis zu 1 TB möglich. Stellen Sie sicher, dass Sie die VM jedes Mal herunterfahren, wenn Sie die Größe der primären Festplatte erhöhen. Dadurch kann das System die neue Festplattengröße richtig erkennen, die Partitionstabelle aktualisieren und die Systemstabilität aufrechterhalten. Um den Speicherplatz zu erhöhen, erweitern Sie die primäre Festplattengröße in der jeweiligen Cloud- oder Hypervisor-Benutzeroberfläche um mindestens 1 GB.

Hinweis:

Sie können nur die Größe der Datenträger erhöhen. Sobald die neue Größe zugewiesen ist, kön-

nen Sie sie später nicht mehr verringern. Erhöhen Sie daher die Größe der Datenträger nur, wenn dies unbedingt erforderlich ist.

Einen sekundären Datenträger hinzufügen

Sie können den Speicherplatz auf der NetScaler VPX-Instanz erhöhen, indem Sie eine sekundäre Festplatte hinzufügen. Wenn Sie die sekundäre Festplatte anschließen, wird das Verzeichnis /var/ crash automatisch auf dieser Festplatte gemountet. Die sekundäre Festplatte wird zum Speichern von Kerndateien und Protokollen verwendet. Vorhandene Verzeichnisse für Core-Dateien und Log-Dateien funktionieren weiterhin wie bisher.

Hinweis:

Erstellen Sie vor dem Downgrade des NetScaler-Geräts ein externes Backup, 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 einen sekundären Datenträger an VPX-Instanzen anzuhängen, die auf Azure bereitgestellt werden, stellen Sie sicher, dass die Azure-VM-Größen über einen lokalen temporären Datenträger verfügen. Weitere Informationen finden Sie unter Azure-VM-Größen ohne lokalen temporären Datenträger.

AWS-Dokumentation

GCP-Dokumentation

Warnung:

Nach dem Hinzufügen einer Festplatte zu VPX schlagen einige Skripts, die mit auf die neue Festplatte verschobenen Dateien arbeiten, unter den folgenden Bedingungen möglicherweise fehl:

• Verwenden Sie den Shell-Befehl link , um Hardlinks zu den Dateien zu erstellen, die auf die neue Festplatte verschoben wurden.

Ersetzen Sie alle diese Befehle durch $\ln -s$, um einen symbolischen Link zu verwenden. Aktualisieren Sie auch die fehlerhaften Skripte entsprechend.

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.

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

Hinweis:

Der reine AWS-IMDSv2-Modus für die Preboot-Benutzerdatenfunktion wird ab NetScaler VPX Version 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 \
1
2
    --image-id ami-0abcdef1234567890 \
3
        --instance-type t2.micro \
4
        --count 1 
        --subnet-id subnet-08fc749671b2d077c \
5
        --key-name MyKeyPair \
6
        --security-group-ids sg-0b0384b66d7d692f9 \
7
8
        --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.

Home > Virtual machines >				
Create a virtual machine	e			
Basics Disks Networking Man	agement Advanced	Tags	Review + create	
Add additional configuration, agents, script	s or applications via virtual	machine	extensions or cloud-init.	
Extensions				
Extensions provide post-deployment config	uration and automation.			
Extensions ()	Select an extension to insta	all		
Custom data				
Pass a script, configuration file, or other dat the VM in a known location. Learn more ab	a into the virtual machine w out custom data for VMs 🖄	vhile it is 7	being provisioned. The data will be saved on	
Custom data				
Custom data on the selected image will	be processed by cloud-init. I	Learn mor	re about custom data and cloud init 🖻	
Host				
Azure Dedicated Hosts allow you to provisi Azure subscription. A dedicated host gives choose VMs from your subscription that wi of the host. Learn more	on and manage a physical s you assurance that only VM Il be provisioned on the hos	erver wit Is from yo st, and the	hin our data centers that are dedicated to yo our subscription are on the host, flexibility to e control of platform maintenance at the leve	ur I
Host group 🕕	No host group found			~

Bereitstellen von Preboot-Benutzerdaten mit der Azure CLI

Geben Sie den folgenden Befehl in die Azure CLI ein:

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

Beispiel



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.

	Security	DIGINO		
Description (Opt	iional)			
Deletion protect Deletion protect Deletion Delet	ion etion protection on protection i	on s enabled, i	instance cannot b	e deleted. Learn more
Reservations Use an existing	reservation wh	en creating	this VM instance	
Automatically	use created	reservatio	n	•
Automation				
Automation Startup script (C You can choose restarts. Startup services are run	optional) to specify a st scripts can be ning within the	artup scrip e used to in e virtual ma	t that will run whe stall software and chine. Learn more	n your instance boots up or updates, and to ensure that
Automation Startup script (C You can choose restarts. Startup services are run	lptional) to specify a st scripts can be ning within the	artup scrip e used to in virtual ma	t that will run whe stall software and chine. Learn more	n your instance boots up or updates, and to ensure that
Automation Startup script (C You can choose restarts. Startup services are run Metadata (Optio You can set cus metadata. This i be queried by yo	optional) to specify a st scripts can be ning within the nal) tom metadata s useful for pa ur code on the	for an insta instance. I	t that will run whe stall software and chine. Learn more ance or project our pitrary values to yo Learn more	n your instance boots up or updates, and to ensure that side of the server-defined bur project or instance that can
Automation Startup script (C You can choose restarts. Startup services are run Metadata (Optio You can set cus metadata. This i be queried by yo Key	Iptional) to specify a st scripts can be ning within the nal) tom metadata s useful for pa ur code on the	for an insta sing in art sing in art sing in art instance. I	t that will run whe stall software and chine. Learn more ance or project our pitrary values to yo Learn more	n your instance boots up or updates, and to ensure that tside of the server-defined bur project or instance that can

Stellen Sie Preboot-Benutzerdaten mit der gcloud CLI bereit

Geben Sie den folgenden Befehl in die GCP CLI ein:

1 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:

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

Beispiel 2:

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

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

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:

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

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

> sn ns	1p							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
_								
1)	10.160.0.72		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	5.0.0.1		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	4.0.0.101		VIP	Active	Enabled	Enabled	Enabled	Enabled
Done								
> sh vl	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::4001	:aff:fea0:48/64					
	Interfaces : 1/1	1/2 LO/1						
2)	VLAN ID: 5	VLAN Alias Name:						
	IPs :							
	5.0.0.1	Mask: 255.255.25	5.0					
3)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 0/1							
	IPs :							
	10.160.0.72	Mask: 25	5.255.240.0					
Done								



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.

:NS-SCRIPTS>	
<script></th><th></th></tr><tr><td>#Shell script</td><td></td></tr><tr><td>echo "Running script 1" > /var/script-1.output</td><td></td></tr><tr><td>date >> /var/script-1.output</td><td></td></tr><tr><td></CONTRACTS</td><td>1</td></tr><tr><td>/var/ </SCRIPT-TARGET-LOCATION></td><td>ľ</td></tr><tr><td>sh /var/script-1.sh</SCRIPT-NS-BOOTUP> </script> <td></td>	

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

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

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

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

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.

<script> #Shell script acho "Pupping script 1" > /var/script-1 output</th><th>script-1.sh</th></tr><tr><th><pre>stop Rdming Script 1 > /var/script-1.output atg >> /var/script-1.output </SCRIPT-CONTENT> script-1.sh </SCRIPT-NAME> /var/ </SCRIPT-TARGET-LOCATION> sh /var/script-1.sh</SCRIPT-NS-BOOTUP> </script>	€ file-2.txt
<pre></pre>	NS Consumer module should consume this

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

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

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:



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.

> sh licenseserv	ver		
License	Server: 10.102.38.214	Port: 2800	Status:
Done			
>			
>			

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 & lt; SKIP-DEFAULT-BOOTSTRAP> und & lt; NEW-BOOTSTRAP-SEQUENCE> Tags an.

SKIP-DEFAULT-	NEW-BOOTSTRAP-	
BOOTSTRAP	SEQUENCE	Bootstrap-Verhalten
A	JA	Das standardmäßige
		Bootstrapping-Verhalten wird
		übersprungen, und eine neue
		benutzerdefinierte
		Bootstrap-Sequenz im
		<ns-bootstrap></ns-bootstrap>
		Abschnitt wird ausgeführt.
JA	NEIN	Das standardmäßige
		Bootstrapping-Verhalten wird
		übersprungen. Die im
		<ns-config></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.



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.

Network Interface eth1

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

Network interface eth0

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

Network Interface eth2

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

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

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.



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.

👤 Overview	
Activity log	vsk-server-nic: vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
🔷 Tags	ipconfig1 (Primary) V
Diagnose and solve problems	Network Interface Vsk-server-nic3 ective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/default NIC Public IP: 52.172.10.59 NIC Private IP: 172.27.0.53 Accelerated networking: Disabled
2 Networking	Inbound port rules Outbound port rules Application security groups Load balancing
~ ~ ·	
Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration 🔘
🗳 Tags	ipconfig1 (Primary) V
Diagnose and solve problems	Network Interface: VSk-client-nic3 :tive security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southindia/vsk-client-subnet NIC Public IP: 52.172.10.184 NIC Private IP: 172.27.1.53 Accelerated networking: Disabled
Retworking	Inbound port rules Outbound port rules Application security groups Load balancing
Verview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration O
🗳 Tags	ipconfig1 (Primary)
Diagnose and solve problems	Network Interfi Vsk-mgmt-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-server-subnet NIC Public IP: 104.211.241.141 NIC Private IP: 172.27.2.53 Accelerated networking: Disabled
Retworking	Inbound port rules Outbound port rules Application security groups Load balancing

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.

	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
.)	172.27.2.53	0	NetScaler IP	Active	Enabled	Enabled	NA	Enable
2)	172.27.0.53		SNIP	Active	Enabled	Enabled	NA	Enable
)	172.27.1.53		VIP	Active	Enabled	Enabled	Enabled	Enable
Done								
sh v	lan							
۰ ۱	VIAN TD. 1							
	Link-local IPv6	addr: fe80::20d:	Saff.fec9.c26c/64					
	Interfaces • 0/1	1/1 TO/1	5411.12C5.C20C/ 04					
	incertaces : 0/1							
	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2	2						
	IPs :							
	172.27.2.53	B Mask: 25	5.255.255.0					
Done								
sh r	oute							
	Network	Netmagl	Cotorrow /OrmodTD	377 7 N	State			
	NCOWOLK	Necillasi	Galeway/Ownedip	VLAIN	State	Irarric D	omain Ty	/pe
						Iraffic D	omain Ty	/pe
	0.0.0.0	0.0.0.0	172.27.2.1	0 0	UP	0	omain Ty ST#	npe ATIC
)	0.0.0.0	0.0.0.0 255.0.0.0	172.27.2.1 127.0.0.1	0 0	UP UP	0 0	omain Ty STP PEF	ATIC ATIC AMANENT
))	0.0.0.0 127.0.0.0 172.27.0.0	0.0.0.0 255.0.0.0 255.255.255.0	172.27.2.1 127.0.0.1 172.27.0.53	0 0 0	UP UP UP	0 0 0	omain Ty STP PEF DIF	/pe ATIC AMANENT RECT
	0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0	0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0	172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53	0 0 0 0 0	UP UP UP UP UP	0 0 0 0 0 0	omain Ty STZ PEF DIF DIF	/pe ATIC AMANENT RECT RECT
	0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0	 0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0	172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53	0 0 0 0 0 0	UP UP UP UP UP UP	0 0 0 0 0 0 0 0	omain Ty ST2 PEF DIF DIF DIF	/pe ATIC AMANENT AECT AECT AECT
)))))		0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.0.0	172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1	0 0 0 0 0 0 0 0	UP UP UP UP UP UP UP	0 0 0 0 0 0 0 0 0 0	omain Ty STZ PEF DIF DIF DIF STZ	ADE ATIC AMANENT RECT RECT RECT ATIC
	0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0 169.254.0.0 168.63.129.16	 0.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.255.255	172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1 172.27.0.1	0 0 0 0 0 0 0 0 0	UP UP UP UP UP UP UP UP	0 0 0 0 0 0 0 0 0 0 0 0 0	omain Ty STZ PEF DIF DIF DIF STZ STZ	ADE ATIC RMANENT RECT RECT RECT ATIC ATIC
)))))	0.0.0.0 127.0.0.0 172.27.0.0 172.27.1.0 172.27.2.0 169.254.0.0 168.63.129.16 169.254.169.254	 0.0.0.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.00 255.255.255.255 255.255.255.255	172.27.2.1 127.0.0.1 172.27.0.53 172.27.1.53 172.27.2.53 172.27.0.1 172.27.0.1 172.27.0.1	0 0 0 0 0 0 0 0 0 0	UP UP UP UP UP UP UP UP UP UP	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	omain Ty STA PEF DIF DIF DIF STA STA STA	ADE ATIC RMANENT RECT RECT RECT ATIC ATIC

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.



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:

Net	work in	terfaces							
N	ame	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier 🎲	IP forwarding	Network details
ni	ic0	default	default	10.160.0.71	-	35.244.56.180 (ephemeral)	Premium	Off	View details
ni	ic1	vsk-vpc-network-1	asia-south1-subnet-1	10.128.0.40	_	35.244.40.113 (ephemeral)	Premium		View details
ni	ic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.27	-	34.93.241.147 (ephemeral)	Premium		View details
Pub	olic DNS	S PTR Record							
No	ne								

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	Туре	Mode	Arp	Icmp	Vserver	State
1) 2) 3) Done	10.128.4.27 10.160.0.71 10.128.0.40	0 0 0	NetScaler IP SNIP VIP	Active Active Active Active	 Enabled Enabled Enabled	Enabled Enabled Enabled	NA NA Enabled	Enabled Enabled Enabled
> sh vl	an							
1)	VLAN ID: 1 Link-local IPv6 addr: fe80::4001:aff:fea0:47/64 Interfaces : 0/1 1/1 LO/1							
2)	VLAN ID: 10 Interfaces : 1/2 IPs : 10.128.4.27	VLAN Alias Name: Mask: 25	5.255.255.0					
Done	1175							
> 311 IO	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main Ty	pe
1)	0.0.0.0	0.0.0.0	10.128.4.1		UP		STA	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
3)	10.128.0.0	255.255.255.0	10.128.0.40		UP		DIR	ECT
4)	10.128.4.0	255.255.255.0	10.128.4.27	0	UP	0	DIR	ECT
5) Done	10.160.0.0	255.255.240.0	10.160.0.71		UP		DIR	ECT
> []								

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	ain							
- 511 115	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp Vs	erver	State
1)	172.31.52.88		NetScaler IP	Active	Enabled	Enabled NA		Enabled
2)	172.31.76.177		SNIP	Passive	Enabled	Enabled NA		Enabled
3)	172.31.5.155		VIP	Passive	Enabled	Enabled En	abled	Enabled
Done								
> sh vl	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::839:	e2ff:feaf:4a9e/64					
	Interfaces : 1/1	. 1/3 LO/1						
21	VIAN TD. 10	VIAN Alian Name						
2)	Toterfaces : 1/2	VLAN AIIas Name.						
	TDa .							
	172 31 52 9	8 Maele 25	5 255 240 0					
Done	1/2.01.02.0	io nask. 25	5.255.240.0					
> sh ro	ute							
- 511 20	Network	Netmask	Gatewav/OwnedIP	VLAN	State	Traffic Doma	in Tv	pe
1)	0.0.0.0	0.0.0.0	172.31.48.1		UP		STA	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
3)	172.31.0.0	255.255.240.0	172.31.5.155		UP		DIR	ECT
4)	172.31.48.0	255.255.240.0	172.31.52.88		UP		DIR	ECT
5)	172.31.64.0	255.255.240.0	172.31.76.177		UP		DIR	ECT
6)	172.31.0.2	255.255.255.255	172.31.48.1		UP		STA	TIC
Done								
>								

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)



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.

Overview	A
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration O
🗳 Tags	ipconfig1 (Primary) V
Diagnose and solve problems	Network Interfai Vsk-mgmt-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-server-subnet NIC Public IP: 104.211.241.141 NIC Private IP: 172.27.2.53 Accelerated networking: Disable
Networking	Inbound port rules Outbound port rules Application security groups Load balancing
Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration (0)
🔷 Tags	ipconfig1 (Primary)
Diagnose and solve problems	Stework Interface: vsk-client-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-client-subnet NIC Public IP: 52.172.10.184 NIC Private IP: 172.27.1.53 Accelerated networking: Disable
Networking	Inbound port rules Outbound port rules Application security groups Load balancing

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

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.

> sii iis	ip Ipaddress	Traffic Domain	Tvpe	Mode	Arp	Icmp 1	Vserver	State
1)	172.27.2.53		NetScaler IP	Active	Enabled	Enabled 1	AN	Enable
2)	172.27.0.53		SNIP	Active	Enabled	Enabled 1	AN	Enable
3)	172.27.1.53		VIP	Active	Enabled	Enabled H	Enabled	Enable
Done								
> sh vla	an							
1.5	WINN TD. 1							
1)	VLAN ID: 1		2-55-5026-/64					
	Link-local IPV6	addr: 1680::20d:	3aII:IEC9:C26C/64					
	Interfaces : 0/1	1/1 L0/1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	172.27.2.53	Mask: 25	5.255.255.0					
Done								
> sh rou	ate							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Dor	main Ty	pe
1)	0.0.0.0	0.0.0.0	172.27.2.1		UP		ST	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PEF	MANENT
3)	172.27.0.0	255.255.255.0	172.27.0.53		UP		DIF	ECT
4)	172.27.1.0	255.255.255.0	172.27.1.53		UP		DIF	ECT
5)	172.27.2.0	255.255.255.0	172.27.2.53		UP		DIF	ECT
6)	169.254.0.0	255.255.0.0	172.27.0.1		UP		STA	TIC
7)	168.63.129.16	255.255.255.255	172.27.0.1		UP		STA	TIC
8)	169.254.169.254	255.255.255.255	172.27.0.1		UP		STA	TIC
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)



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									
1	Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier 📀	IP forwarding	Network details
1	nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	-	34.93.216.90 (ephemeral)	Premium	Off	View details
1	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
1	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 <NS -BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen" ausführen, um die Subnetzmaske zu überprüfen.

ai							
Inaddress	Traffic Domain	Type	Mode	Arn	Temp V	server	State
10.128.4.31	0	NetScaler IP	Active	Enabled	Enabled N	A	Enabled
10.160.0.75	0	SNTP	Passive	Enabled	Enabled N	Ά	Enabled
10.128.0.43	0	VTP	Passive	Enabled	Enabled E	nabled	Enabled
10112010110	<u> </u>	122	1000110	Dirabled	Ditabled D	10.0200	21100200
an							
VLAN ID: 1							
Link-local IPv6	addr: fe80::4001	:aff:fea0:4b/64					
Interfaces : 0/1	1/1 LO/1						
VLAN ID: 10	VLAN Alias Name:						
Interfaces : 1/2							
IPs :							
10.128.4.31	Mask: 25	5.255.255.0					
oute							
Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Dom	ain Ty	pe
0.0.0.0	0.0.0.0	10.128.4.1		UP		STA	TIC
127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
10.128.0.0	255.255.255.0	10.128.0.43		UP		DIR	ECT
10.128.4.0	255.255.255.0	10.128.4.31		UP		DIR	ECT
10.160.0.0	255.255.255.0	10.160.0.75		UP		DIR	ECT
	<pre>g ip Ipaddress 10.128.4.31 10.160.0.75 10.128.0.43 an VLAN ID: 1 Link-local IPv6 Interfaces : 0/1 VLAN ID: 10 Interfaces : 1/2 IPs : 10.128.4.31 oute Network 0.0.00 127.0.00 10.128.0.0 10.128.4.0 10.160.0.0</pre>	s ip Ipaddress Traffic Domain 10.128.4.31 0 10.160.0.75 0 10.128.0.43 0 Tan VLAN ID: 1 Link-local IPv6 addr: fe80::4001 Interfaces : 0/1 1/1 LO/1 VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 10.128.4.31 Mask: 25 Network Netmask 0.0.0.0 0.0.00 127.0.0.0 255.0.0.0 10.128.4.0 255.255.0 10.128.4.0 255.255.0 10.160.0.0 255.255.0	s ip Ipaddress Traffic Domain Type 	ip Ipaddress Traffic Domain Type Mode 10.128.4.31 0 NetScaler IP Active 10.160.0.75 0 SNIP Passive 10.128.0.43 0 VIP Passive an VLAN ID: 1 Link-local IPv6 addr: fe80::4001:aff:fea0:4b/64 Interfaces : 0/1 1/1 L0/1 VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 10.128.4.31 Mask: 255.255.255.0 Oute Network Netmask Gateway/OwnedIP VLAN 0.0.0.0 0.0.0.0 10.128.4.1 0 127.0.0.0 255.255.255.0 10.128.0.43 0 10.128.4.0 255.255.255.0 10.128.0.43 0 10.128.4.0 255.255.255.0 10.128.0.43 0 10.128.0.0 255.255.255.0 10.128.0.43 0 10.128.4.0 255.255.255.0 10.128.4.31 0 10.128.4.0 255.255.255.0 10.128.4.31 0 10.160.0.0 255.255.255.0 10.128.4.31 0	ip Ipaddress Traffic Domain Type Mode Arp 10.128.4.31 0 NetScaler IP Active Enabled 10.160.0.75 0 SNIP Active Enabled 10.128.0.43 0 VIP Active Enabled an VLAN ID: 1 Interfaces : 0/1 1/1 LO/1 VLAN Alias Name: Interfaces : 1/2 IPs : INTERfaces : 1/2 VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : INTERfaces : 1/2 IPs : INTERfaces : 1/2 IPs : 10.128.4.31 Mask: 255.255.255.0 0 UP INTERfaces : 1/2 0.0.0.0 0.0.0.0 10.128.4.1 0 UP 127.0.0.0 255.00.0 127.0.0.1 0 UP 10.128.0.0 255.255.255.0 10.128.0.43 0 UP 10.128.4.0 255.255.255.0 10.128.0.43 0 UP 10.128.4.0 255.255.255.0 10.128.0.43 0 UP	ip Traffic Domain Type Mode Arp Icmp V 10.128.4.31 0 NetScaler IP Active Enabled Nabled N 10.128.0.43 0 VIP Passive Enabled Enabled N 10.128.0.43 0 VIP Passive Enabled Enabled N an VLAN ID: 1 Link-local IPv6 addr: fe80::4001:aff:fea0:4b/64 Passive Enabled Enabled	ip Traffic Domain Type Mode Arp Icmp Vserver 10.128.4.31 0 NetScaler IF Active Enabled Enabled NA 10.128.4.31 0 SNIP Passive Enabled Enabled NA 10.128.0.43 0 VIP Passive Enabled Enabled NA 10.128.0.43 0 VIP Passive Enabled Enabled

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. NetScaler VPX 14.1



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

1	<ns-pre-boot-config></ns-pre-boot-config>
2	<ns-config></ns-config>
3	
4	set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
5	add route 0.0.0.0 0.0.0.0 172.31.48.1
6	set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
7	add route 172.31.0.2 255.255.255.255 172.31.48.1
8	
9	enable ns feature WL SP LB RESPONDER
10	add server 5.0.0.201 5.0.0.201
11	add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
	maxClient 0 -maxReq 0 -cip DISABLED -usip NO -
	useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -
	CKA NO -TCPB NO -CMP NO
12	add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
	persistenceType NONE -cltTimeout 180
13	
14	
15	
16	<ns-bootstrap></ns-bootstrap>
17	<skip-default-bootstrap>YES</skip-default-bootstrap>
18	<new-bootstrap-sequence> NO </new-bootstrap-sequence>
19	
20	
21	
22	

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.

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

Network Interface eth2	
Interface ID	eni-09e55a6cfb791e68d
VPC ID Attachment Owner	Vpc-60258602 566658252593
Attachment Status	attached
Attachment Time	Fri Jan 01 11:11:33 GMT+530 2021
Delete on Terminate	false
Private IP Address	172.31.76.177 @
Private DNS Name	ip-172-31-76-177.ap-south-1.compute.internal 但

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	lp							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
	172.31.52.88		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
	4.0.0.101		VIP	Active	Enabled	Enabled	Enabled	Enabled
one								
sh vl	an							
	VLAN ID: 1							
	Link-local IPv6	addr: fe80::839:	e2ff:feaf:4a9e/64					
	Interfaces : 1/1	1/3 LO/1						
	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	172.31.52.8	8 Mask: 25	5.255.240.0					
one								
sh ro	ute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main Ty	npe
	0.0.0.0	0.0.0.0	172.31.48.1		UP		STA	TIC
	127.0.0.0	255.0.0.0	127.0.0.1		UP		PEF	RMANENT
	172.31.48.0	255.255.240.0	172.31.52.88		UP		DIF	RECT
	172.31.0.2	255.255.255.255	172.31.48.1		UP		STA	TIC
one								

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

NetScaler VPX 14.1

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.



15

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 -CLTIIMEOUT 180 -SVEIIMEOUT 360 -CKA NO -ICPB NO -CMP NO
17	add lb vserver preboot v4 101 HTTP 4.0.0.101 80 -
	persistenceType NONE -cltTimeout 180
18	
19	
20	
21	<ns-bootstrap></ns-bootstrap>
22	
23	<skip-default-bootstrap>YES</skip-default-bootstrap>
24	<new-bootstrap-sequence> NO </new-bootstrap-sequence>
25	
26	
27	
28	

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.

,	\ll \mathscr{S} Attach network interface \mathscr{S} Detach network interface
Overview	A
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
🗳 Tags	ipconfig1 (Drimap)
Diagnose and solve problems	Network Interface Vsk-server-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/default NIC Public IP: 104.211.220.9 NIC Private IP: 172.27.0.61 Accelerated networking: Disabled
Networking	Inbound port rules Outbound port rules Application security groups Load balancing
🖋 Connect	
Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
🗳 Tags	ipconfig1 (Primary)
Diagnose and solve problems	Network Interface Vsk-client-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southindia/vsk-client-subnet NIC Public IP: 52.172.2.48 NIC Private IP: 172.27.1.61 Accelerated networking: Disabled
Retworking	Inbound port rules Outbound port rules Application security groups Load balancing
Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
🗳 Tags	Ipcontig i (Primary)
Diagnose and solve problems	Network Interfa Vsk-mgmt-nic3 Effective security rules Topology
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-server-subnet NIC Public IP: 52.172.47.251 NIC Private IP: 172.27.2.61 Accelerated networking: Disabled
Retworking	Inbound port rules Outbound port rules Application security groups Load balancing
d. Connect	

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.

511 110	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp V	Vserver	State
)	172.27.2.61	0	NetScaler IP	Active	Enabled	Enabled 1	ANA	Enabl
)	172.27.0.61		SNIP	Active	Enabled	Enabled 1	AN	Enabl
Done	4.0.0.101	0	VIP	Active	Enabled	Enabled H	Enabled	Enabl
sh vl	an							
	VLAN ID: 1							
	Link-local IPv6	addr: fe80::20d:3	Baff:fec9:9076/64					
	Interfaces : 0/1	1/1 LO/1						
	VLAN ID: 5	VLAN Alias Name:						
	VLAN ID: 10	VLAN Alias Name:						
	VLAN ID: 10 Interfaces : 1/2	VLAN Alias Name:						
	VLAN ID: 10 Interfaces : 1/2 IPs :	VLAN Alias Name:						
	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61	VLAN Alias Name: Mask: 25	5.255.255.0					
one	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61	VLAN Alias Name: Mask: 25	5.255.255.0					
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 wute	VLAN Alias Name: Mask: 25	5.255.255.0					
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 ute Network	VLAN Alias Name: Mask: 255 Netmask	5.255.255.0 Gateway/OwnedIP	VLAN	State	Traffic Dom	nain Ty	pe
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 ute Network 0.0.0.0	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0	5.255.255.0 Gateway/OwnedIP 	VLAN 0	State UP	Traffic Dom 	nain Ty STA	pe TIC
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 wite Network 0.0.0.0 127.0.0.0	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0 255.0.0.0	5.255.255.0 Gateway/OwnedIP 	VLAN 0 0	State UP UP	Traffic Dom 0 0	main Ty STA PER	pe TIC MANENT
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 ute Network 0.0.0.0 127.0.0.0 172.27.0.0	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0 255.0.0.0 255.255.255.0	Gateway/OwnedIP 	VLAN 0 0 0	State UP UP UP	Traffic Dom 0 0	main Ty; STA PER DIR	pe TIC MANENT ECT
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 wte Network 0.0.0.0 127.0.00 172.27.0.0 172.27.2.0	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0	Gateway/OwnedIP 	VLAN 0 0 0 0	State UP UP UP UP	Traffic Dom 	main Ty STA PER DIR DIR	pe TIC MANENT ECT ECT
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 wtte Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.2.0 169.254.0.0	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0 255.255.255.0 255.255.0 255.255.0	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.61 172.27.2.61 172.27.0.1	VLAN 0 0 0 0 0	State UP UP UP UP UP UP	Traffic Dom 0 0 0 0 0	main Ty; STA PER DIR DIR STA	pe TIC MANENT ECT ECT TIC
one sh ro	VLAN ID: 10 Interfaces : 1/2 IPs : 172.27.2.61 wtte Network 0.0.0.0 127.0.0.0 172.27.0.0 172.27.2.0 169.254.0.0 168.63.129.16	VLAN Alias Name: Mask: 255 Netmask 0.0.0.0 255.255.255.0 255.255.0 255.255.0 255.255.00	Gateway/OwnedIP 172.27.2.1 127.0.0.1 172.27.0.61 172.27.0.1 172.27.0.1 172.27.0.1	VLAN 0 0 0 0 0 0 0	State UP UP UP UP UP UP UP	Traffic Dom 0 0 0 0 0 0	main Ty STA PER DIR DIR STA STA	pe TIC MANENT ECT ECT TIC TIC

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:

1	<ns-pre-boot-config></ns-pre-boot-config>
2	
3	<ns-config></ns-config>
4	
5	set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
6	add route 0.0.0.0 0.0.0.0 10.128.0.1
7	set ns config -nsvlan 10 -ifnum 1/1 -tagged NO
8	
9	enable ns feature WL SP LB RESPONDER
10	add server 5.0.0.201 5.0.0.201
11	add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
	maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
	YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
	NO -CMP NO
12	add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
	persistenceType NONE -cltTimeout 180
13	
14	
15	
16	<ns-boutstrap></ns-boutstrap>
1/	<pre><skip-defauli-booistrap>YES</skip-defauli-booistrap></pre>
18	<pre><new-booistrap-sequence> NO </new-booistrap-sequence></pre>
19	
20	
21	

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) 2)	10.128.0.2 4.0.0.101	0 0	NetScaler IP VIP	Active Active	Enabled Enabled	Enabled Enabled	NA Enabled	Enabled Enabled
> sh vl	an							
1)	VLAN ID: 1 Link-local IPv6 Interfaces : 0/1	addr: fe80::4001 1/2 LO/1	:aff:fea0:4a/64					
2)	VLAN ID: 10 Interfaces : 1/1 IPs : 10.128.0.2	VLAN Alias Name: Mask: 25	5.255.255.0					
Done								
> sh ro	Network	Netmask	Gatewav/OwnedIP	VLAN	State	Traffic D	omain T	vpe
1)	0.0.0.0	0.0.0.0	10.128.0.1		UP		ST	ATIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PE	RMANENT
3) Done	10.128.0.0	255.255.255.0	10.128.0.2	0	UP	0	DI	RECT

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:

1 show cpuparam

Beispiel

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

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

4. 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.

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

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

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

Problembehandlung

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

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

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.

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

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

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

NetScaler Sanity Checker-Tool

October 17, 2024

Das Sanity Checker-Tool bewertet den Zustand und die Leistung von NetScaler, und identifiziert auch die allgemeinen Konfigurationsprobleme.

Hinweis:

Derzeit wird das NetScaler Sanity Checker-Tool nur für die AWS-Cloud unterstützt.

Das NetScaler Sanity Checker-Tool führt auch die folgenden Aktivitäten aus:

• Validiert HA-Topologie, Netzwerke, Lizenzierung und Berechtigungen.

- Rationalisiert den Fehlerbehebungsprozess.
- Ermöglicht die schnelle Lösung von Problemen, die in öffentlichen Clouds beobachtet wurden.
- Generiert Ergebnisse in mehreren Formaten wie Klartext-Logs, JSON und HTML.

NetScaler Sanity Checker-Tool für AWS

Das NetScaler Sanity Checker-Tool deckt je nach Bereitstellungstyp die folgenden Validierungen ab.

Eigenständige		
HA-Bereitstellungen und		
HA-Bereitstellungen in derselben Zone	Mehrzonen-HA-Bereitstellung mit elastischen IP-Adressen	Mehrzonen-HA-Bereitstellung mit privaten IP-Adressen
 Überprüfung der IAM-Berechtigungen Lizenzüberprüfung Speicherüberprüfung Überprüfung der Metadaten-Route Überprüfung der DNS-Auflösung EC2-Endpunktprüfung Standard-Gateway- Check VLAN- Konfigurationsprüfung ARP-Prüfung SysID-Überprüfung Cloudhadaemon- 	 Überprüfung der IAM-Berechtigungen Schnittstellenüberprüfung EIP-Überprüfung INC-Modusüberprüfung IPSet-Überprüfung 	 Überprüfung der IAM-Berechtigungen Schnittstellenüberprüfung Routenüberprüfung Geräteindexüberprüfung Src/Dst-Überprüfung

Führen Sierdas Sanity Checker-Tool mit NetScaler CLI aus

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Nach dem Ausführen des Sanity Checker-Tools werden die folgenden Dateien in den Formaten JSON und HTML generiert.

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

Diese Dateien enthalten die detaillierten Ergebnisse der durchgeführten Prüfungen, anhand derer potenzielle Probleme identifiziert und analysiert werden können.

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/XenServer

January 15, 2025

Um VPX-Instanzen auf dem Citrix Hypervisor/XenServer zu installieren, müssen Sie zuerst den Hypervisor auf einer Maschine 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.





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 Informationen finden Sie in der
	BIOS-Dokumentation.
RAM	3 GB
Speicherplatz	Lokal angeschlossener Speicher (PATA, SATA,
Spelenerplatz	SCSI) mit 40 GB Speicherplatz.
	Anmerkung: Bei der Hypervisor-Installation
Netzwerkkarte	king tifebit/genetiketitenempfohlen: zwei
	hybet/ssbettwststeaetengsdomäne erstellt. Der
	verbleibende Speicherplatz ist für die NetScaler

Weitere Informationen finden Sie in der XenServer-Weiterte Und andere virtuelle Maschinen

verfügbar. 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|

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)

January 30, 2025

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

Für die Netzwerkkarten Intel X710 10G und Intel XL710 40G gelten die folgenden Einschränkungen:

- 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:

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.

1 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.

```
1 xe pif-list
2
3 uuid ( R0) : e2874343-f1de-1fa7-8fef-98547c348783
4 device ( R0): eth18
5 currently-attached ( R0): true
6 VLAN ( R0): -1
7 network-uuid ( R0): 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:

```
1 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:

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

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

Hinweis:

Die NIC-Indexnummer der VM muss mit 0 beginnen.

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

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

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.

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

Beispiel

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.

Andere Referenzen

SR-IOV-fähige NICs Fügen Sie ein SR-IOV-Netzwerk hinzu

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 ESX i 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
RAM	AMD-Prozessoren. 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.

Komponente	Voraussetzung
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 1 GB, 2 GB empfohlen
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-Passthroughund 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.

/irtual Hardware VM C	Options SDRS Rules	VA	pp Optio	ns		
CPU	2	•	0			
Memory	2048	-	MB	-)	
🔚 Hard disk 1	20	*	GB	-)	
SCSI controller 0	LSI Logic Parallel					
🕨 🗾 Network adapter 1	VM Network			-	Connect	
🕨 ় Network adapter 2	1/2			-	Connect	
Video card	Specify custom settin	gs		-		
VMCI device						
 Other Devices 						
Upgrade	Schedule VM Comp	atib	ility Upgr	ade		
New device:	Select			•	Add	
Compatibility: ESXi 5.5 an	d later (VM version 10)				ОК	Cance

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

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

5. 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.

	ons	vApp Opti	SDRS Rules	VM Options	irtual Hardware		
	0	•	4		🔲 *CPU		
1	Sockets:	-	1	ocket	Cores per So		
		ot Add	Enable CPU	g	CPU Hot Plu		
-)	MHz	•	0		Reservation		
·)	MHz	MHz	Current value:		Limit		
1	4000	ИНZ	Minimum:		Shares		
Adva	juest	96 MHz	Maximum:		CPUID Mask		
ion to the	ted virtualiza	are assist	Expose hard	tualization	Hardware virtualization		
counters	performanc	ed CPU p	🗌 Enable virtua	counters	Performance		
I CPUs	s: Active 24 (logi	ing Status Us:	Hyperthre: Available (ffinity	Scheduling Affinity		
Add	-		Select	evice:	New d		

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

Virtual Hardware VM Options	SDRS Rules	vApp Op	tions		
- 🔲 *CPU	4	-	0		
Cores per Socket	1	-	Sockets:	4	
CPU Hot Plug	Enable CPU H	ot Add			
Reservation (*)	8396	-	MHz	-	
Limit	Unlimited	-	MHz	-	
Shares	Current value: Ur	nlimited	4000	-	
CPUID Mask	Minimum: 8396 MHz		guest 🖌 A		dvar
Hardware virtualization	Maximum: Ur	nlimited	sted virtuali	zation to t	the
Performance counters	📃 Enable virtualiz	zed CPU	performan	ce counte	ers
Scheduling Affinity	Hyperthread Available CF	ing Statu PUs:	ıs: Active 24 (lo <u>c</u>	gical CPU	ls)
New device:	Select			Add	

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

Virtual Hardware VM Optio	ons	SDRS Rules	vApp	Optio	ons			
🕶 🔲 *CPU		4		•	0			-
Cores per Socket	(1		-	Sockets	: 4		
CPU Hot Plug	1	Enable CPU	Hot Ad	d				
Reservation (*)		8396		•	MHz	-		
Limit	Γ	Unlimited		-	MHz	-		
Shares (*)	ĺ	Custom	- 20	-	4000	-		
CPUID Mask	ĺ	Expose the NX/	XD fl	Minim	num 0		Adva	n
Hardware virtualization	n [Expose hard	vare 1	Maxin	num 100	00	n to the	9
Performance counters		Enable virtua	lized C	PU p	erformar	nce co	ounters	
Scheduling Affinity	Ş	Hyperthrea Available C Select logical pr	ding S PUs: ocess	tatus or affi	: Active 24 (Io nity for th	gical iis virt	CPUs) tual ma	30
New device:		Select -			-	ł	\dd	1

- 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 = 4×4 GB = 16 GB.

		IS	io	Opt	vApp	SDRS Rules	VM Options	tual Hardware
		•	6	-		4		🕽 *CPU
								м *Метогу
	-	MB		-		8396		RAM (*)
	-	МВ		-		0		Reservation
	(ed)	(All lock	or	nem	uestm	🔄 Reserve all g		
	-	МВ		•		Unlimited		Limit
	-	83960		-		Normal		Shares
						Enable	Plug	Memory Hot
	-	GB		*		20		Hard disk 1
					el	LSI Logic Paralle	ler 0	SCSI control
⊡ Co	-					VM Network	pter 1	Network ada
⊡ Co	•					1/2	pter 2	Network ada
dd	P		81			Select -	evice:	New d

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.

al Hardware VM Optio	ns SDRS Rules	s VApp Op	tions		
*CPU	4	•	0		
*Memory		1.1			
RAM (*)	8192	-	MB	-	
Reservation (*)	8192	*	MB	-	
	✓ Reserve al	lguestmem	ory (All loc	ked)	
Limit	Unlimited	-	MB	-	
Shares	Normal	-	81920	-	
Memory Hot Plug	Enable				
Hard disk 1	20	*	GB	-	
SCSI controller 0	LSI Logic Par	allel			
Network adapter 1	VM Network			-	Co
Network adapter 2	1/2			•	Co
New device:	Sele	ct		Add	

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

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

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

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

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

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

- 8. 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.

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

- 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 rface VMXNE	1500 T3	00:0c:29:89:1d:0e	NetScaler Vir	
6	2	1/1	9000	00:0c:29:89:1d:18	NetScaler Vir	
		THUCC, WHATE	10			

_ _ -

_ _ _

7	3	1/2	9000	00:0c:29:89:1d:22	NetScaler Vir
0	4	rface, VMX	NET3	00 • 0 = • 20 • 00 • 1 = • 0 =	Neterslevel controls
8	4	interface	9000	00:0c:29:89:1d:0e	Netscaler Loopback

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 f
 ür SR-IOV VF-Schnittstelle
 über ip link Befehl wird nicht unterst
 ützt

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.

vmware [®] vSphere V	Web Client ते≣	کا Adr	ninistrator@VSPHERE	LOCAL 👻 H	lelp -
Navigator I	№ 10.102.38.201 Actions ▼				=*
Home	Getting Started Summary Mo	nitor Manage Related	Objects		
Image: Constraint of the second se	Settings Networking Storage	Alarm Definitions Tags	Permissions		
 ▼ Im VPX ▶ Im 10.102.100.10€ ▶ Im 10.102.38.201 	•• Virtual switches	Physical adapters	Q Filter		•
 10.217.195.204 10.217.195.220 	VMkernel adapters	Observed IP ranges	Wake on LAN Support	SR-IOV Status	-
	TCP/IP configuration	No networks	No	Disabled Disabled	
	Advanced	No networks	No	Enabled	
		No networks	No	Disabled	::
		No networks	No	Disabled	100
		No networks	No ::	Disabled •	•

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

vmware [®] vSpher	e Web Client ते≣	Ŭ L A	dministrator@VSPHERE	LOCAL 👻	Help
Navigator	🖡 🔂 10.102.38.201 Actions 👻				=*
Home	Getting Started Summary M	Ionitor Manage Related	l Objects		
▼ 2 10.102.38.250	Settings Networking Storage	Alarm Definitions Tags	Permissions		
 VPX 10.102.100.1 10.102.38.20 	06 ** 1 Virtual switches	Physical adapters	· (Q. Filter		•
 10.217.195.2 10.217.195.2 	VMkernel adapters	Observer P ranges	Wake on LAN Support	SR-IOV Status	-
	Physical adapters	No networks	No	Disabled	
	TCP/IP configuration	No networks	No	Disabled	
	Advanced	No networks	No	Enabled	
		No networks	No	Disabled	
		No networks	No	Disabled	
		No networks	No	Disabled	+
		4			Þ
		Physical network adapter	r: vmnic5 DP LLDP Intel Corj 10 Gigab Network	ooration 82599 it Dual Port Connection	•
		Name	vmnic5		

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

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

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

💌 vmnic5 - Edit Settings		?
Configured speed, Duplex:	Auto negotiate	•
SR-IOV		
SR-IOV is a technology that allows multiple virtual machines to use the same PCI device as a virtual pass-through device.		
Number of virtual functions:	1	*
Changes will not take effect until the system is restarted.		
	ОК	Cancel

- 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 Clusteraus.
- 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**.

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

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

Virtual Hardware VM C	ptions SDRS Rules	VApp Op	tions	
CPU	2	• 0		
Memory	2048	- MB	•]	
🕨 🛄 Hard disk 1	20	GB		
SCSI controller 0	LSI Logic Parallel			
🕨 ় Network adapter 1	VM Network		👻 🗹 Connect	
🕨 属 Network adapter 2	1/2		Connect	
Video card	Specify custom setting	gs		
VMCI device				
Other Devices				
Upgrade	🗌 Schedule VM Comp	atibility Up	grade	
New device:	Select		Add	
	12212 2220 12 222		17	Vir

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

/irtual Hardware VM Option:	s SDRS Rules vApp Options
T *CPU	4 🕞 🛈
Cores per Socket	1 Sockets: 4
CPU Hot Plug	Enable CPU Hot Add
Reservation	0 🔹 MHz 💌
Limit	Unlimited
Shares	Normal + 4000 -
CPUID Mask	Expose the NX/XD flag to guest - Advanced
Hardware virtualization	Expose hardware assisted virtualization to the guest OS
Performance counters	Enable virtualized CPU performance counters
Scheduling Affinity	Hyperthreading Status: Active Available CPUs: 24 (logical CPUs) Select logical processor affinity for this virtual machine. Use '-' for ranges and ',' to separate values. For example, "0, 2, 4- 7" would indicate processors 0, 2, 4, 5, 6 and 7. Clear the string to remove affinity settings.
CPU/MMU Virtualization	Automatic - ESXi can automatically determine if a virtual machine should use
New device:	Select Add

- 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.

		ptions	vApp Op	SDRS Rules	VM Options	irtual Hardware	
		0	•	4		T *CPU	
	ckets: 4	Sock	-	1	ocket	Cores per So	
		_	J Hot Add	Enable CPI	g	CPU Hot Plu	
)	Hz 🚽	MHz	-	0		Reservation	
)	Hz 🗸	MHz	: 0 MHz	Current value		Limit	
	• 000	4000	0 MHz	Minimum:		Shares	
Adva	it 🚽	guest	8396 MHz	Maximum:	:	CPUID Mask	
on to the	virtualizatio	isted virt	dware assi	Expose har	tualization	Hardware vir	
ounters	ormance c	J perforn	alized CPU	📃 Enable virtu	counters	Performance	
CPUs)	Active 24 (logical	tus: Act 24	eading Stat CPUs:	Hyperthro Available	Affinity	Scheduling A	
Add	•		:t	Selec	evice:	New d	

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

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

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

Virtual Hardware VM Option:	SDRS Rules V	App Opt	ions		
- 🔲 *CPU	4	•	0		
Cores per Socket	1	-	Sockets	: 4	
CPU Hot Plug	Enable CPU Ho	ot Add			
Reservation (*)	8396	-	MHz	-	
Limit	Unlimited	-	MHz	-	
Shares (*)	Custom		4000	-	
CPUID Mask	Expose the NX/XD fl Minimum				Adva
Hardware virtualization	Expose hardwa	00	n to the		
Performance counters	Enable virtualize	ed CPU	performar	nce co	ounters
Scheduling Affinity	Hyperthreadin Available CPU Select logical proc	ng Statu Us: essor af	s: Active 24 (Io finity for th	gical iis viri	CPUs) tual ma
New device:	Select		-	-	Add

- 6. 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.

irtual Hardware VM Op	otions	SDRS Rules	vApp Opt	ions			
T *CPU		4	 •	0			
Memory			5 pr				
RAM (*)		8396	-	MB	-		
Reservation		0	-	MB	-		
		Reserve all g	uest mem	ory (All loc	ked)		
Limit		Unlimited 🗸		MB	-		
Shares		Normal	83960	-			
Memory Hot Plug		Enable					
🛄 Hard disk 1		20	A 7	GB	-		
🛃 SCSI controller 0		LSI Logic Parall	el				
🗾 Network adapter 1		VM Network			-	⊡ c	0
📕 Network adapter 2		1/2 🔍					0
New device:	_	Select			A	\dd	1

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.

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

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

		1	2				1
/irtual Hardware	VM Options	SDRS Rules	vApp Opti	ons			
CPU *CPU		4	•	0			
Memory							
RAM (*)		8192	•	MB	-		
Reservation	(*)	8192	•	MB	-		
		🔄 Reserve all g	uestmemo	ory (All loci	ked)		
Limit		Unlimited 👻		MB	-		
Shares		Normal 😽 81					
Memory Hot	Plug	Enable					-
Hard disk 1		20 A GB					
G SCSI control	er 0	LSI Logic Parall	el				
🗾 Network ada	pter 1	VM Network			+	🗹 Co	0
Network adapter 2		1/2				√ Co	D
New d	evice:	Select			A	dd	1
				-		•	

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

Virtual Hardware	VM Options	SDRS Rules	vApp Opti	ions		
🕨 🔲 *CPU		4	•	0		
🕶 🌃 *Memory						
RAM (*)		8192	-	MB	-	
Reservation (*)		8192	-	MB	-	
		🔄 Reserve all g	uestmem	ory (All loc	ked)	
Limit		Unlimited 👻		MB	-	
Shares (*)		Custom 🚽 🖓		00000	-	
Memory Hot Plug		Enable Minimu		mum 1		
🕨 🛄 Hard disk 1	📑 Hard disk 1		Maximum 1000			
🛛 🛃 SCSI controll	er 0	LSI Logic Parall	el			
🕨 🗾 Network ada	pter 1	VM Network			-	[Co
Network ada	pter 2	1/2			-	[Co
New d	evice:	Select			Add	

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

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

- 8. 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.

🗗 NSVPX-ESX - Edit Settings		?₩
Virtual Hardware VM Options	SDRS Rules vApp Options	
🕨 🛄 Hard disk 1	20 GB	•
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
▶ 飅 Network adapter 1	VM Network 🗸 🗸 Connect	1.0
▶ 飅 Network adapter 2	VM Network 2	
▶ 🛄 Video card	Specify custom settings	
▶ ∰ VMCI device		
▶ Other Devices		
👻 飅 New Network	CITRIX_PG1 (DVS_SRIOV_CITRIX)	
Status	Connect At Power On	
Port ID		::
Adapter Type	SR-IOV passthrough	
	E1000 Is are unavailable when	1
	SR-IOV passthrough Sent. You cannot	
	VMXNET 3	
Physical function	vmnic4 0000:03:00.0 Intel Corp	
MAC Address	Automatic 🗸	
Guest OS MTU Change	Disallow -	•
New device:	Metwork - Add	
Compatibility: ESXi 6.0 and later ((VM version 11) OK Ca	incel

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

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

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

- 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.

NOVPA-ESA-DEMO - Eail Setting	3	1		
/irtual Hardware VM Options S	DRS Rules VApp Options			
VMware Tools	Expand for VMware Tools settings	•		
Power management	Expand for power management settings			
Boot Options	Expand for boot options	T		
Advanced				
Settings	Disable acceleration			
	Leadie logging			
Debugging and statistics	Run normally	J		
Swap file location	 Default Use the settings of the cluster or host containing the virtual machine. 			
	 Virtual machine directory Store the swap files in the same directory as the virtual machine. 			
	Datastore specified by host Store the swap files in the datastore specified by the host to be used for swap files. If not possible, store the swap files in the same directory as the virtual machine. Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines.	40		
Configuration Parameters	Edit Configuration	1		
Latency Sensitivity	High 🔹 🚯 🛕 Check CPU reservation 🚯			
	Low			
	Normal			
ompatibility: ESXi 5.5 and later 0/M	Medium	4		

- 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

4					
5	1	0/1	1500	00:0c:29:1b:81:0b	NetScaler Virtual
6	2	10/1	1500	00:50:56:9f:0c:6f	Intel 82599 10G VF
	Interface				
7	3	10/2	1500	00:50:56:9f:5c:1e	Intel 82599 10G VF
0		Interface	1500		T. I. J. 00500 100 VE
8	4	10/3 Interface	1500	00:50:56:97:02:10	Intel 82599 10G VF
9	5		1500	00.50.56.9f.5a.1d	Intel 82599 106 VE
J	5	Interface	1300	00.30.30.31.34.14	111111111111111111111111111111111111111
10	6	10/5	1500	00:50:56:9f:4e:0b	Intel 82599 10G VF
		Interface			
11	7	L0/1	1500	00:0c:29:1b:81:0b	Netscaler Loopback
		interface			
12	Do	one			
13	> :	show inter 10	/1		
14	1)	Interfa	ce 10/1 (1	Intel 82599 10G VF Inte	rface) #1
15		flags=0	xe460 <en< td=""><td>ABLED, UP, UP, HAMON, 8</td><td>02.1q></td></en<>	ABLED, UP, UP, HAMON, 8	02.1q>
16		MTU=150 h21m	0, native 153s	vlan=55, MAC=00:50:56:	9f:0c:6f, uptime 0
17		Actual: thro	media FII ughput 10	BER, speed 10000, duple: 000	x FULL, fctl NONE,
18		LLDP Mo	de: NONE,	LR Pri	ority: 1024
19			,		
20		RX: Pkt Stal	s(83802074 ls(0)	42) Bytes(860888485431)	Errs(0) Drops(2527)
21		TX: Pkt Stal	s(8381499 ls(0)	54) Bytes(860895860507)	Errs(0) Drops(0)
22		NIC: In (0)	Disc(0) 0	utDisc(0) Fctls(0) Stal	ls(0) Hangs(0) Muted
23		Bandwid	th thresh	olds are not set.	
24	Do	one			

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**.

1	Create / Register VM 📑 Console 🕨 Power on 🔲 Power off	
□	Virtual machine ~	Status ~
☑.	🔂 ns1	📀 Normal
Ο.	ns2	📀 Normal
□	ns4	Normal
Ο.	ns3	Normal
□	🔂 ns5	📀 Normal
Qu	ick filters v	



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

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

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

Network Adapter 2	PG1-v1	Connect	\otimes
Uideo Card	Specify custom settings	~	
PCI device 1	c6xx QAT VF - 0000:1a:01.0	~	8
PCI device 2	c6xx QAT VF - 0000:1b:01.0	~	
PCI device 3	c6xx QAT VF - 0000:1a:01.1	~	
PCI device 4		~	
PCI device 5	c6xx QAT VF - 0000:1b:01.1	~	
PCI device 6	c6xx QAT VF - 0000:1b:01.2	~	
PCI device 7		~	8
New PCI device	c6xx QAT VF - 0000:1a:01.4	~	⊗

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.

> stat ssl	
SSL Summary	
# SSL cards present	1
# SSL cards UP	1
SSL engine status	1

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

April 1, 2025

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**.

All PCI Devices					
·				Q Fi	Iter -
ID		Status	Vendor Name	Device Name	ESX Name
✓ 0000:05:00.	3	Available	Intel Corporation	Ethernet Controll	A
☑ 🚾 0000:05:00.	☑ 🜆 0000:05:00.0		Intel Corporation	Ethernet Controll	
00:000 📷 🗌	:1A.0	Unavailable	Intel Corporation	Wellsburg USB	
▼ 0000:00:1C	.4	Not Configurable	Intel Corporation	Wellsburg PCI E	
▼ 0000:09:	.00.0	Not Configurable	ASPEED Techn	AST1150 PCI-to	
0 📷 🗌	0.00:0A:00.0	Unavailable	ASPEED Techn	ASPEED Graphi	
000:00 📷	:1D.0	Unavailable	Intel Corporation	Wellsburg USB	
▼ 0000:80:03	.0	Not Configurable	Intel Corporation	Haswell-E PCI E	
1 device will become a	vailable when this ho	ost is rebooted.		00500ED 40 0	
0000:00:01.0					
This device cannot be	made available for V	'Ms to use			
Name	Haswell-E PCI Exp	ress Root Port 1	Vendor Name	Intel Corporation	
Device ID	2F02		Vendor ID	8086	
Subdevice ID	0		Subvendor ID	0	
Class ID	604				
Bus Location					
ID	0000:00:01.0		Slot	1	
Bus	0		Function	0	
				E 1	OK Cancel

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.

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

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.

NSVPX-ESX-DEMO - Edit S	ettings			(?) ₩
Virtual Hardware VM Options	SDRS Rules	vApp Options		
▶ 🔲 CPU	2	• 0		
▶ Image Memory	4096	▼ MB	•	
▶ 🛄 Hard disk 1	20	GB	•	
▶ G SCSI controller 0	LSI Logic Paralle	4816		
▶ m Network adapter 1	VM Network		✓ Connect	
▶ Uideo card	Specify custom	settings	•	
▶ ∰ VMCI device				
 Other Devices 				
✓ New PCI device	0000:05:00.3 1	tel Corporation Ethe	•	
Physical PCI/PCIe device	0000:05:00.3 In 10GbE SFP+	el Corporation Ethern	et Controller X710 for	
	Note: Some PCI/PCIe par suspend, mig such virtual r	virtual machine operati asthrough devices are rate with vMotion, or t nachines.	ions are unavailable when present. You cannot ake or restore snapshots of	,
New device:	🛅 PCI De	vice 🔹	Add	
Compatibility: ESXi 6.0 and later	(VM version 11)		ОК	Cancel

5. 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

April 1, 2025

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 & lt; NS-CONFIG> section:

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

 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 userdataverwendet 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
1
2
     drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
     root@ubuntu:~/sai/14jul2021#
3
4
     root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
5
     -rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
6
     root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
          ./esx_preboot_userdata
     I: -input-charset not specified, using utf-8 (detected in locale
7
         settings)
8
     Total translation table size: 0
9
     Total rockridge attributes bytes: 0
     Total directory bytes: 112
10
     Path table size(bytes): 10
11
     Max brk space used 0
13
     176 extents written (0 MB)
14
     root@ubuntu:~/sai/14jul2021# ls -lh
15
     total 356K
     drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
16
17
     -rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.
        iso
18
19
     root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
     root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
        preboot_userdata_155_193
21
     I: -input-charset not specified, using utf-8 (detected in locale
         settings)
     Total translation table size: 0
22
     Total rockridge attributes bytes: 0
24
     Total directory bytes: 112
25
     Path table size(bytes): 10
26
     Max brk space used 0
     176 extents written (0 MB)
27
```

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

🔁 New virtual machine - sai-test-iso						
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options Select deployment options					
5 Ready to complete	Network mappings	VM Network VM N	letwork		Ŷ	
	Disk provisioning	Thin O Thick				
	Power on automatically	D				
vm ware [®]						
			Back	Next	Finish	Cancel

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

🖻 Edit settings - sai-test-iso (ESXi 5.1	virtual n	nachine)		
Virtual Hardware VM Options				
🔜 Add hard disk 🛛 🎫 Add network a	dapter	Add other device		
+ 🔲 CPU	2	CD/DVD drive		
h Mamory		Floppy drive		
- Meriory	2	serial port		
Hard disk 1	20	Parallel port		0
SCSI Controller 0	19	USB controller		0
		💼 USB device		
Mill Network Adapter 1	VM	Sound controller	V Connect	0
🕨 🛄 Video Card	Spe	PCI device	~	
		Dynamic PCI device		
		VAL SCSI controller	-	
			Save	Cancel

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

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

6. Select a Datastore in the vSphere Client.

😡 Datastore browser				
🛉 Upload 📑 Download	🙀 Delete 🛛 🔒 Move 👔 Co	py 🏾 🎦 Create dir	rectory 🛛 🤁 Refresh	
datastore1	៉ .sdd.sf	💿 esx		
៉ vmimages	៉ centosiso	🍥 pre		
	늘 centosnirmal_225	🍥 pre	esx_preboot_userdata.i	
	늘 fips-t1	🔞 pre	Wednesday, July 14, 2	
	ips1	🍥 pre		
	៉ sai-test-iso	i pre		
	🚞 sai-test-rs130	sai		
	📺 sai-vpx-2	<u></u> sai		
	៉ sai-vpx-test	sai		
	🚞 sai-vpx3	🔂 sai		
	៉ Shreesh-blx-centos	sai		
	៉ Venkata	vm		
		i vm		
		III 📄 vm III		111
[datastore1] sai-vpx-2/esx	_preboot_userdata.iso			
			Sel	ect Cancel

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:

1	base64	<userdata-filename> > <outuput-file></outuput-file></userdata-filename>	
Beispiel			
1	base64	<pre>esx_userdata.xml > esx_userdata_b64</pre>	
root@ubu	ntu:~/sai/	l4jul2021# base64 esx_userdata.xml > esx_userdata_b64	
root@ubu root@ubu PE5TLVBSI	ntu:~/sai/ ntu:~/sai/ RS1CT09ULU	4]UL2021# [4jul2021# cat esx_userdata_b64 YPT&ZJRz4KICAgIDx0Uv1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw	
LjAuMC4w ICAgICAg	IDEwLjEwMi ICAgICA8U0	120C4xCiagICA8L05TLUNPTkZJRz4KCiagICA8T1MtQk9PVFNUUkFQPgog LJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U	
U1RSQVA+0 VFJBUC1TH	CiAgICAgIC RVFVRU5DRT	\glCAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFP11FUZwvTkVXLUJPT1RT iKCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg ZBOULT1VNPiBLGCgwIDwySU5UPVLCQUNFLU5VTT4KICAgICAgICAgICAg	
ICAgIDxJU QVNLPiAy	JD4gICAgMT NTUuMjU1Lj	AuMTAyLjM4LjIXOSABLOlQPgogICAgICAgICAgICAGICAGPFNVQk5FVCIN IINS4wIDwvUlVCTkVULU1BUOs+CiAgICAgICAGC9NR01ULU10VEVSRkFD	
RS1DT05G	SUc+CiAgIC	A8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+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:

1	<productsection></productsection>
2	
3	<info>Information about the installed software</info>
4	<product>NSVPX-VSK Template</product>
5	<vendor>Citrix</vendor>
6	<vendorurl>www.citrix.com</vendorurl>
7	<category> Preboot Userdata </category>

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

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

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

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

Please d	change the defaul	t NSROOT passwor	d.					
Enter ne	ew password:							
Please :	re-enter your pas	sword:						
Done								
> sh ns	ver							
	NetScaler NS13.0	: Build 83,9005.	nc. Date: Jul 13	2021. 02:	56:05	(64-bit)		
Done						(01 220)		
> sh ns	in							
	Inaddress	Traffic Domain	Type	Mode	Arn	Temp	Vserver	S
tate	ipadaress	fidilie bomain	1150	11040	111-12	remp	VSCLVCL	0
Cace								
1 \	10 102 38 219		NotScolor TR	Activo	Enabled	Enabled	N7	F
1)	10.102.30.219		NetStater if	ACCIVE	Enabled	Enabled	NA	E
Dono								
Done								
> sn rot	Natural	Matwaals	Cotowood D	777 7 N	Otata		empin Dr	
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic D	omain Ty	pe
1 \			10 102 29 1	0				
1)	0.0.0.0	0.0.0.0	10.102.30.1		UP		511	VI. T
	127 0 0 0	255 0 0 0	107 0 0 1		IID		DBI	
2)	127.0.0.0	255.0.0.0	127.0.0.1		02		PEI	(PLA
NENT	10 100 30 0		10 100 30 010				D.T.T	
ວ) ຫ	10.102.38.0	200.200.200.0	10.102.38.219		0P		DIE	(EC
T								

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.

- 2. Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:
 - In Linux, use the following command:

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

Beispiel

1	base64	esx_userdata.x	<pre>(ml > esx_userdata_b64</pre>
root@ubu	untu:~/sai/	14jul2021# base64 e	sx userdata.xml > esx userdata b64
root@ubu	untu:~/sai/	14jul2021#	
root@ubu	untu:~/sai/	14jul2021# cat esx_	userdata_b64
PE5TLVB	SRS1CT09ULU	NPTkZJRz4KICAgIDxOU	y1DT05GSUc+Cg1hZGQgcm91dGUgMC4wLjAuMCAw
LjAuMC4	wIDEwLjEwMi	4zOC4xCiAgICA8L05TL	UNPTkZJRz4KCiAgICA8T1MtQk9PVFNUUkFQPgog
ICAgICAg	gICAgICA8U0	tJUC1ERUZBVUxULUJPT	1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
U1RSQVA-	+CiAgICAgIC	AgICAgIDxORVctQk9PV	FNUUkFQLVNFUVVFTkNFP11FUzwvTkVXLUJPT1RT
VFJBUC1	IRVFVRU5DRT	4KCiAgICAgICAgPE1HT	VQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
ICAGICA	gIDxJTlRFUk	ZBQ0UtTlVNPiBldGgwI	DwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
ICAgIDx	JUD4gICAgMT	AuMTAyLjM4LjIxOSA8L	01QPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
QVNLPiA	yNTUuMjU1Lj	I1NS4wIDwvU1VCTkVUL	U1BU0s+CiAgICAgICAgPC9NR01ULU1OVEVSRkFD
RS1DT050	GSUc+CiAgIC	A8L05TLUJPT1RTVFJBU	D4KPC90Uy1QUkUtQk9PVC1DT05GSUc+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:

1	<productsection></productsection>
2	
3	<info>Information about the installed software</info>
4	<product>NSVPX-VSK Template</product>
5	<vendor>Citrix</vendor>
6	<vendorurl>www.citrix.com</vendorurl>
7	<category> Preboot Userdata </category>
8	
9	<property ovf:<br="" ovf:key="guestinfo.userdata" ovf:type="string">userConfigurable="true" ovf:value=""></property>
10	
11	<label>Userdata</label>
12	<description> Userdata for ESX VPX </description>
13	
14	
15	

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

1	<productsection></productsection>
2	
3	<info>Information about the installed software</info>
4	<product>NSVPX-VSK Template</product>
5	<vendor>Citrix</vendor>
6	<vendorurl>www.Citrix.com</vendorurl>
7	<category> Preboot Userdata </category>
8	<property ovf:<="" ovf:key="guestinfo.userdata" ovf:type="string" td=""></property>
	userConfigurable="true"
9	ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+
	CglhZGQgcm91dGUgMC4wLjAuMCAw
10	LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQ

1

11	ICAgICAgICAgICA8U0tJUC1ERUZBVU×ULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQ	/VMVC
12	U1RSQVA+ CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLU	JPT1F
13	VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KI	CAgIC
14	ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgI	CAgIC
15	ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgICAgP	-NVQk
16	QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+ CiAgICAgICAgPC9NR01ULUlOVEVSRkFD	
17	RS1DT05GSUc+ CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+ Cg==">	
18		
19	<label>Userdata</label>	
20	<pre><description> Userdata for ESX VPX </description></pre>	
21 22		
23		

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

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

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

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

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.
- 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/a rticle/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 importierene.
- 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"?>
1
2
3
     <Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment
         /1`"
4
5
     xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"
6
     oe:id=""
7
8
     xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">
9
10
     <PlatformSection>
11
12
13
     <Kind>HYPER-V</Kind>
14
15
     <Version>2013.1</Version>
16
17
     <Vendor>CITRIX</Vendor>
18
19
     <Locale>en</Locale>
20
21
     </PlatformSection>
22
23
     <PropertySection>
24
25
     <property oe:key="com.citrix.netscaler.ovf.version" oe:value="</pre>
         1.0"/>
     <property oe:key="com.citrix.netscaler.platform" oe:value="</pre>
27
         NS1000V"/>
28
29
     <property oe:key="com.citrix.netscaler.orch\_env" oe:value="</pre>
         cisco-orch-env"/>
30
```

- 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 Einstellungenaus. Sie können auch die virtuelle Appliance auswählen und dann mit der rechten Maustaste klicken und Einstellungenauswählen. 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 ausethool -K eth6 lro aus

Beispiel:

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

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.

1	[root@localhost	<pre>~]# brctl show eth6_br</pre>		
2				
3	bridge name	bridge id	STP enabled	interfaces
4				
5	eth6_br	8000.00e0ed1861ae	no	eth6
6				
7				vnet0
8				
9				vnetz
11	[reat0]acalhact]#		
11	Lionrerocariosi	- ~]#		

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.

```
1ethtool -K vnet0 gro off2ethtool -K vnet2 gro off3ethtool -K vnet0 lro off4ethtool -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.

```
[root@localhost ~]# ifconfig eth6 promisc
1
2
     [root@localhost ~]# ifconfig eth6
3
     eth6
                Link encap:Ethernet HWaddr 78:2b:cb:51:54:a3
                 inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
4
5
                 UP BROADCAST RUNNING PROMISC MULTICAST MTU:9000 Metric
                     :1
                 RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
6
                 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
     [root@localhost ~]#
11
```

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 Open-Stack 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 Standard-mechanismus, 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"?>
2
3
     <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"</pre>
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4
5
     oe:id=""
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
6
7
     xmlns:cs="http://schemas.citrix.com/openstack">
     <PlatformSection>
8
9
     <Kind></Kind>
     <Version>2016.1</Version>
11
     <Vendor>VPX</Vendor>
12
     <Locale>en</Locale>
13
     </PlatformSection>
14
     <PropertySection>
     <property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
15
     <property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
16
17
     <property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-</pre>
         orch-env"/>
     <property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"</pre>
18
         />
     <property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="</pre>
19
         255.255.255.0"/>
     <property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="</pre>
         10.1.2.1"/>
21
     </PropertySection>
22
      <cs:ScriptSection>
23
         <cs:Version>1.0</cs:Version>
24
           <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack</pre>
              " xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
               <Scripts>
25
26
                 <Script>
27
                        <Type>shell</Type>
28
                        <Parameter>X Y</Parameter>
29
                      <Parameter>Z</Parameter>
                      <BootScript>before</BootScript>
                         <Text>
31
32
                               #!/bin/bash
                               echo "Hi, how are you" $1 $2 >> /var/sample.
                                   txt
                         </Text>
34
35
                 </Script>
                 <Script>
37
                        <Type>python</Type>
                        <BootScript>after</BootScript>
39
                         <Text>
40
                              #!/bin/python
41
      print("Hello");
42
                         </Text>
43
                 </Script>
         <Script>
44
45
                        <Type>perl</Type>
46
                        <BootScript>before</BootScript>
47
                         <Text>
48
                              !/usr/bin/perl
```

```
my $name = "VPX";
49
50
      print "Hello, World $name !\n";
51
                        </Text>
                 </Script>
52
53
                 <Script>
54
                      <Type>nscli</Type>
                      <BootScript>after</BootScript>
                      <Text>
57
                       add vlan 33
58
      bind vlan 33 -ifnum 1/2
59
                      </Text>
                 </Script>
61
               </Scripts>
          </ScriptSettingSection>
62
63
      </cs:ScriptSection>
64
     </Environment>
       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

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

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

Abbildung 1: Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance imagecreate.

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

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 Instanzenaus.
- 3. Klicken Sie im Instanzen Bedienfeld auf **Instanz starten**, um den Instanzentart-Assistenten zu öffnen.

ject	Ψ.	Ins	tances							,			
Compute	Ŧ	Ins	tances			Filter			Q Faur	(+u	unch Instance	Set Reb	et instances
Dveniew			Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Uptime	Actions
folumes	~		dicp	NS-VPX- 10-5-49-3	10.0.0.5	m1.medium 4GB RAM 2 VCPU 40.0GB Disk		Active	nova	None	Running	1 hour, 50 minutes	Create Snapshot
nages			NS1000+- 10-5-4	NS-VPX- 10-5-49-3	10.0.0.4	m1.medium 4G8 RAM 2 VCPU 40.0G8 Disk		Active	nova	None	Running	1 hour, 57 minutes	Create Snapshot
letwork	•		NS1000+10-5	NS-VPX- 10-5-49-3	10.0.0.2	m1.medium 4G8 RAM 2 VCPU		Active	nova	None	Running	2 hours, 16 minutes	Create Snapshot

- 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

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

5. 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**.

Import Key Pair		×
Key Pair Name *		
NewKey	Description:	
Public Key *	Key Pairs are how you login to your instance after it is launched.	
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCIZih	Choose a key pair name you will recognise and paste your SSH public key into the space provided.	
03te1EnvL38iGXbjlByc2+oBV7ZIERiYQEtk2UfM+ EtJJlcx92m4aIn1RlgEvukXECHjXGqfQXVI06pyim	SSH key pairs can be generated with the ssh-keyge command:	
KRWigXhI+h+tvPGS4iltJ3uWKwfh1PDGYkmgAik osA955L+W9ngVloVyaK40OuAqYCTwIQNBKVuZ	ssh-keygen -t rsa -f cloud.key	
EcvsxOvhdb3LW9YADAVnihVK4NLeBc4HIsFeHI 5UY0IYyGk7aW/2SXizkwRqZ8cX1Oba0XoDiCYN apRVOT6FB//yknvu+BSVF4v0og3	This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.	9
	After launching an instance, you login using the private key (the username might be different depending on the image you launched):	9
	ssh -i cloud.key <username>@<instance_ip></instance_ip></username>	
	Cancel Import Key Pa	ir

- 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 configdrive und klicken Sie auf **Starten**.

Launch Instance								
Details *	Access & Security	Networking *	Post-Creation	Advanced Options				
Disk Partition	0		Specify advan	nced options to use when	launching an			
Automatic		Ψ	instance.					
🕑 Configurati	on Drive 🥝							
				Ca	ancel Launch			

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:

```
openstack server create --flavor FLAVOR_ID --image IMAGE ID --
1
       key-name KEY_NAME
    --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id
2
       =net-uuid
    INSTANCE_NAME
3
4
    openstack server create --image VPX-ToT-Image --flavor m1.medium
         --user-data
    ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6
5
       -3efd44b761b9
    VPX-ToT
6
```

Abbildung 2: Die folgende Abbildung zeigt eine Beispielausgabe.

+	
Field	Value
/ OS-DCF:diskConfig	I MANUAL
OS-EXT-AZ:availability zone	
0S-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor hostname	None
0S-EXT-SRV-ATTR: instance name	instance-000001c2
0S-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
0S-EXT-STS:vm_state	building
0S-SRV-USG: Launched at	None
0S-SRV-USG:terminated at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtg7N8Z6
config drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
kev name	None
name	IVPX-ToT
os-extended-volumes:volumes attached	
progress	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

January 28, 2025

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

Beispiel:

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

Eine typische NetScaler VPX-Bereitstellung auf KVM umfasst die folgenden Schritte:

- Überprüfen der Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz
- Provisioning der NetScaler VPX-Instanz mithilfe eines RAW-Images
- Provisioning der NetScaler VPX-Instanz mithilfe eines QCOW2-Images
- Hinzufügen weiterer 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
3 <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`</pre>
```

4	xmlns·xsi="`http://www.w3.org/2001/XMLSchema-instance"`
6	
7	oe:id=""
8 9	<pre>xmlns="`http://schemas.dmtf.org/ovf/environment/1"`</pre>
10 11 12	<pre>xmlns:cs="`http://schemas.citrix.com/openstack">`</pre>
13 14	<platformsection></platformsection>
15 16	<kind></kind>
17 18	<version>2016.1</version>
19 20	<vendor>VPX</vendor>
21 22	<locale>en</locale>
23 24	
25 26	<propertysection></propertysection>
27 28	<property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"></property>
29 30	<property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"></property>
31 32	<property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"></property>
33	<property <br="" oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22">/></property>
34	
35	<property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
255.255.255.0"></property>
36	
37	<property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
10.1.2.1"></property>
38	
39 40	
41	

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:

- 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.

V? localhost.localdomain:6 (admin)		
Activities WWirtual Machine Ma	nager	Thu 02:24 🌱
		Virtual Machine Manager
File Edit View Help		
🔛 🗐 Open 🗇 💷 🖪 🗸		
Name		
Localhost (GEMU)		
Connect		
Disconn	ct	
Delete		
Dgtails		
x		

- 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**.

🕐 localhost.localdomain:6 (admin)		
Activities WWirtual Machin	e Manager	Virtual Machine Manager
File Edit View Help		
🔛 🗏 Open ⊳ 💷 💽	V.	
Name		
localhost (GEMU)	New VM	
	Create a new virtual machine Step 1 of 4	
	Enter your virtual machine details Name: NetScaler-VPX Connection: localhost (QEMU/KVM)	
	Choose how you would like to install the operating system Local install media (ISO image or CDROM) Network Install (HTTP, FTP, or NFS) Network Boot (PXE) 	
	Import existing disk image Cancel Back Forward	

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**.

VC localhost.localdomain:6 (admin)		
(Virtual Machine Manager
File Edit View Help		
📔 🗍 🛄 Open 🗈 🔢 👩 🛩		
Name		
localhost (QEMU)	New VM	
	Create a new virtual machine Step 2 of 4	
	Provide the existing storage path: /(ibvirt/images/NSVPX-KVM-10.1-118.7_nc.raw) Browse	e
	Choose an operating system type and version OS type: UNIX Version: FreeBSD 6.x	
	Cancel Back Forward	

- 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

V localhost.localdomain:6 (admin)		
·	Virtual Mac	hine Manager
File Edit View Help		
🔛 🗐 Open 🗈 🔟 🖻 👻		
Name		
localhost (QEMU)	New VM	
	Create a new virtual machine Step 3 of 4 Choose Memory and CPU settings Memory (RAM): 2048 MB Up to 96658 MB available on the host CPUs: 20 Up to 12 available Cancel Back Forward	
*[

 Wählen Sie die Schaltfläche Anpassen der Konfiguration vor der Installation Kontrollkästchen. 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.

Ibost (OEMLI)		
most (acrio)	New VM	
	Create a new virtual machine Step 4 of 4	
	Ready to begin installation of NetScaler-VPX	
	OS: FreeBSD 6.x	
	Memory: 2048 MB	
	CPUs: 2	
	Storage: 20.0 GB /var/lib/lib/virt/images/NSVPX-KVM-10.1-118.7_n	
	☑ Customize configuration before install	
	Virtual network 'default': NAT	
	☑ Set a fixed MAC address	
	52:54:00:0d:22:cb	
	Virt Type: kvm	
	Architecture: x86_64	
	Cancel Back Finish	

- 8. Wählen Sie eine Netzwerkkarte aus, und stellen Sie die folgende Konfiguration bereit:
 - Quellgerät- ethX macvtap oder Bridge
 - Geräte-Modell—virtio
 - Quellmodus—Brücke

Image: Source device Virtual Network Interface Image: Source device Fost device p255p1 : macvtap Image: Source device Virtual content Image: Source device Fost device p255p1 : macvtap Image: Source device Virtual content Image: Source device Fost device p255p1 : macvtap Image: Source device Virtual content Image: Source device Fost device Image: Source device Virtual port Image: Source device Virtual port	
Console Video	

- 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 das Ankreuzfeld **qcow2** Bild in **Schritt 5**.

2. Wählen Sie **Disk 1** und klicken Sie auf **Erweiterte Optionen**.

3.	Wählen Sie qcow2	aus der Dropdowr	liste Speicherformat aus.
----	-------------------------	------------------	---------------------------

rtual Disk Farget device: Source path: /h Storage size: 78 Readonly: Sharaahla: 7	sk 1 ome/dummy_ 18.25 MB	dut/NSVPX-	KVM-11.1-12.5_nc.qa	
rtual Disk Target device: Source path: /h Storage size: 78 Readonly: Sharaahla: 7	<mark>sk 1</mark> ome/dummy_ 18.25 MB	dut/NSVPX-	KVM-11.1-12.5_nc.qc	
 ✓ Advanced opti Disk bus: Serial number: Storage format: ✓ Performance of Cache mode: IO mode: IO Tuning 	ons default 🗢 qcow2 options efault 🗢)		UW
Read: 0	T A	0	5/500	
Write: 0		6		
Cotal: 0				
	Disk bus: Serial number: itorage format: Performance of ache mode: de IO mode: de IO mode: de IO Tuning KByt ead: 0 vrite: 0 otal: 0 Tip: 'source' r while 'target' r	Disk bus: default Serial number: torage format: qcow2 Performance options tache mode: default IO mode: default IO mode: default IO mode: default VIO Tuning KBytes/Sec ead: 0 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Disk bus: default Serial number: torage format: qcow2 Performance options tache mode: default IO mode: default III mode: default III mode: default III mode: default III mode: default III mode: default III mode: default I	Disk bus: default Disk bus: default Serial number: storage format: qcow2 Performance options cache mode: default IO mode: default IO mode: default IO mode: default VIO Tuning KBytes/Sec IOPS/Sec ead: 0 Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS

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.
- 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.

e Virtual Machine View Send	l Key				
0 - 0 - 5					
Aug 11 10:14:55 <local(< th=""><td>9.alert> ns restar</td><td>t[2578]: Restar</td><td>t: ∕netsca</td><td>ler/nsstar</td><td>t.sh</td></local(<>	9.alert> ns restar	t[2578]: Restar	t: ∕netsca	ler/nsstar	t.sh
exited normally. Exit	code (0) 2 alents no nestan	+[2578]: Succ	م م الالسام	anagistana	4
h Pitboss	9.alert/ HS restar	·[[2370], 3000	essiully a	eregistere	α ωις
login: nsroot					
Password:		DOOT LOCIN (
Comuriant (c) 1992-2013	notice> ns login; 3 The FreeBSD Proi	RUUI LUGIN (NSP)	OOT) UN TT	yv⊎	
Copyright (c) 1979, 198	80, 1983, 1986, 19	88, 1989, 1991,	1992, 199	3, 1994	
The Regents of	the University of	California. Al	l rights r	eserved.	
Done					
> sh ip	Traffic Devision	Tune	Mada	A	Inner
Userver State	IPAILIC DUMAIN	туре	noae	нгр	ıcmh
1) 10.1.2.22	Θ	NetScaler IP	Active	Enabled	Enab
led NA Enabled					
> Aug 11 10:15:13 < loca	alA alert> ns rest	art[25781: Ns	shutdoum l	ock releas	ed t
_					

 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.



in der Kopfzeile, um die Details der virtuellen Hardware anzuzeigen.

4. Klicken Sie auf Hardware hinzufügen. Wählen Sie im Fenster Neue virtuelle Hardware hinzufügenim 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 "Name 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.

Overview Performance Processor Memory Boot Options IDE Disk 1 NIC :0d:22:cb NIC :a9:77:fc Mouse Display VNC Sound: ich6 Serial 1 Video Controller USB Controller IDE	Image Image Image Image Graphics Sound Serial Image Parallel Image Channel USB Host Device PCI Host Device Video Filesystem Smartcard USB Redirection	Add New Virtual Hardware Network Please indicate how you'd like to connect your new virtual network device to the host network. Host device: Specify shared device name Bridge name: bridge1 MAC address: S2:54:00:c3:9a:22 Device model: virtio Cancel Finish
	▷ Security	

- iii. Gerätemodell—virtio.
- iv. Klicken Sie auf **Fertig stellen**.
- b) Für MacVtap
 - i. Host-Gerät Wählen Sie die physische Schnittstelle aus dem Menü aus.
 - ii. Gerätemodell—virtio.

		Add New Vi	tual Hardware
	Storage	Network	
9	Network		
0	Input	Please indicate how	/ you'd like to connect your
2	Graphics	new virtual networ	k device to the host network.
	Sound	Host device:	Host device macutan2 : macutan
-	Serial		
~	Parallel	MAC address:	☑ 52:54:00:fb:bb:e5
~	Channel		
33	USB Host Device	Device model:	VITTIO
33	PCI Host Device		
<u>_</u>	Video		
F	Watchdog		
	Filesystem		
2	Smartcard		
			Cancel Finish

iii. Klicken Sie auf **Fertig stellen**. Sie können die neu hinzugefügte NIC im Navigationsbereich anzeigen.

		NetS	caler-VPX Virtual	Machin	e		-
ile	Virtual Machine View	Send Key					
	3 > 11 8	× [
<u>.</u>	Overview	Virtual Network	Interface				
44 11	Performance Processor	Source device:	Host device p1p1	: macvta	ap 🗘		
-	Memory	Device model:	virtio	\$			
33	Boot Options	MAC address:	52:54:00:a9:77:fc				
	IDE Disk 1	Source mode:	Default				
2	NIC :a9:77:fc	Virtual port	VEPA				
5	Mouse		Bridge				
2	Display VNC		Private				
J.	Sound: ich6		Passthrough				
2	Serial 1						
	Video						
	Controller USB						
	Controller IDE						
_							
	Add Hardware				Remove	Cancel	Apply

- 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

January 15, 2025

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

Weitere Informationen finden Sie unter Unterstützte Netzwerkkarten für NetScaler VPX.

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
 Fügen Sie die Netzwerkkarte zum KVM-Host hinzu. 	-	-
 Laden Sie den neuesten Intel-Treiber herunter und installieren Sie ihn. 	IXGBE-Treiber	l40E-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). Wenn Sie eine frühere Version	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). Wenn Sie eine frühere Version
 Aktivieren Sie SR-IOV Virtual Functions (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. 	<pre>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>/</number_of_vfs> </pre>	<pre>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>/</number_of_vfs> </pre>
	device/sriov_numvfs. Siehe Beispiel in Abbildung 2.	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
 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.

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

Abbildung 2: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel X710 10G- und XL710 40G-NICs.

roccabarca
root@ubuntu:~# lspci grep 710
03:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 01)
03:06.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:06.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0a.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
03:0e.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 01)
82:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 02)
82:00.1 Ethernet controller: Intel Corporation Ethernet Controller XL 710 for 40GbE QSFP+ (rev 02)
82:02.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:02.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
82:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)
root@ubuntu:~#

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 hinzufügenaus.

MI		Demo_VPX on QEMU/KVM	↑ _ □ X
File	Virtual Machine View Send	New Virtual Hardware Add New Virtual Hardware Storage • Create a disk image for the virtual machine 20.0 - + GiB 748.9 GiB available in the default location • Select or create custom storage Manage Device type: Disk device Bus type: IDE • Advanced options	
	Seria Smartcard Chai USB Redirection Vide RNG Cont Cont Cont Cont Controller VirtlO Serial USB Redirector 1 USB Redirector 2	⊘ Cancel √ Finish	

- 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

20		Add New Virtual Hardware
St.	orage	PCI Device
📑 Co	ontroller	
Ne Ne	etwork	Host Device:
📋 Inj	put	טטטט:סט:בו:א וחלא Corporation כאדע/אש series chipset Thermal Subsystem
- Gr	aphics	0000:01:00:0 Intel Corporation I350 Gigabit Network Connection (Interface e
📑 So	und	0000:01:00:1 Intel Corporation I350 Gigabit Network Connection (Interface e
Se	rial	0000:02:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Conne
🗗 Pa	rallel	0000:02:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Conne
🗗 Co	onsole	0000:02:10:0 Intel Corporation 82599 Ethernet Controller Virtual Function
🗗 Ch	annel	0000:02:10:1 Intel Corporation 82599 Ethernet Controller Virtual Function
🔏 US	5B Host Device	0000:03:00:0 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel Control of
💑 PC	CI Host Device	0000:03:00:1 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel
Vie	deo	0000:03:00:2 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel Control of
📑 Wa	atchdog	0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (Intel Control of
Fil	esystem	0000:06:00:0 ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge
🗟 Sn	nartcard	0000:07:00:0 ASPEED Technology, Inc. ASPEED Graphics Family
🛞 US	5B Redirection	0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
💭 ТР	M	0000:7F:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
🔏 RN	IG	0000:7F:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
🔏 Pa	nic Notifier	0000:7F:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 4
		(2) Cancel √ Finish
	odiractor 1	

Abbildung 5: VF für Intel XL710 40G NIC

<u>000</u>		Add New Virtual Hardware	↑ ×
	Storage Controller Network	PCI Device Host Device:	
	Input Graphics Sound Serial Parallel Console	0000:02:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Cor 0000:02:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Cor 0000:03:00:0 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:1 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:2 Intel Corporation Ethernet Controller X710 for 10GbE SFP+	nne Ine (Int) (Int) (Int)
	Channel USB Host Device PCI Host Device Video Watchdog Filesystem Smartcard USB Redirection TPM RNG Panic Notifier	0000:03:06:0 Intel Corporation XL710/X710 Virtual Function 0000:03:06:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:0 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:2 Intel Corporation XL710/X710 Virtual Function 0000:03:0A:3 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:0 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:1 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:2 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:3 Intel Corporation XL710/X710 Virtual Function	
		Cancel	ish

Additiong 6: VF fur intel X/22 10G-N	: VF für Intel X722 10G	-NIC
--------------------------------------	-------------------------	------

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

- 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.

MM				Demo_VPX on QEMU/KVM		↑ - □ ×
File	Virtual	Machine View	w Send Key			
		> 🚺 🕘 🔹				
	> shou	J interface	summary			
		Interface	MTU	MAC	Suffix	
	1	0/1	1500	52:54:00:7f:81:87	NetScaler Virtual Interfac	е
	2	10/1	1500	8e:e7:e7:06:50:3f	Intel 82599 10G VF Interfa	се
	3	10/2	1500	8e:1a:71:cc:a8:3e	Intel 82599 10G VF Interfa	се
	4	L0/1	1500	52:54:00:7f:81:87	Netscaler Loopback interfa	се
	Done >					

Abbildung 7. Entfernen einer bestehenden SSD ohne RAID **Abbildung 7.** Zusammenfassung der Ausgangsdaten für Intel X710- und XL710-NICs.

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

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 \\<interface\\_name\\&#062; vf \\&#060;VF\\_id
\\&#062; spoofchk off*
```

Ort:

- interface_name —ist der Schnittstellenname.
- vf_ID —ist die virtuelle Funktions-ID.

Beispiel:

Terminal - root@ubuntu: /etc 🗘 .	
File Edit View Terminal Tabs Help	
root@ubuntu:/etc# ip link show ens3f0	
6: ens3f0: <broadcast,multicast,up,lower up=""> mtu 1500 gdisc mg state UP mode DEFAULT group default glen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7e brd ff:ff:ff:ff:ff:ff	
vf 0 MAC 8e:e7:e7:06:50:3f, spoof checking on, link-state auto	
root@ubuntu:/etc#	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip_link_show_ens3f1	
7: ens3f1: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default glen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff	
vf θ MAC 8e:la:71:cc:a8:3e, spoof checking on, link-state auto	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip link set ens3f0 vf θ spoofchk off	
root@ubuntu:/etc# ip link show ens3f0	
6: ens3f0: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default glen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7e brd ff:ff:ff:ff:ff:ff	
vf θ MAC 8e:e7:e7:06:50:3f, spoof checking off, link-state auto	
root@ubuntu:/etc# ip link set ens3f1 vf θ spoofchk off	
root@ubuntu:/etc# ip link show ens3f1	
7: ens3f1: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default glen 1000</broadcast,multicast,up,lower>	
link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff:ff	
vf θ MAC 8e:la:71:cc:a8:3e, spoof checking off, link-state auto	
root@ubuntu:/etc#	

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

 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).

root@venkat-Super-Server:~#	adf_ctl sta	tus		
Checking status of all device	ces.			
There is 47 QAT acceleration	n device(s) in	the system:		
gat_dev8 - type: c6xx, ins	st_id: 0, nod	e_id: 0, bsf	: 6660:1a:86.0, #ac	cel: 5 Aengines: 10 state: up
gat_dev1 - type: c6xx, ins	st_id: 1, nod	e_id: 8, bsf	: 6660:1b:80.0, #ac	cel: 5 #engines: 10 state: up
gat_dev2 - type: c6xx, ins	st_id: 2, nod	e_id: 0, bsf	: 6660:1c:80.0, #ac	cel: 5 #engines: 10 state: up
gat_dev3 - type: c6xxvf,	inst_id: 0, n	ode_id: 0, b	sf: 0000:1a:01.0, #	accel: 1 #engines: 1 state: up
gat_dev4 - type: c6xxvf, 1	inst_id: 1, n	ode_id:0, b	sf: 0000:1a:01.7, #	accel: 1 #engines: 1 state: up
gat_dev5 - type: c6xxvf, 1	inst_id: 2, n	ode_id:0, b	sf: 0000:1a:01.1, #	accel: 1 #engines: 1 state: up
qat_dev6 - type: c6xxvf,	inst_id: 3, n	ode_id: 0, b	sf: 0000:1a:02.0, #	accel: 1 #engines: 1 state: up
gat_dev7 - type: c6xxvf, 1	inst_id: 4, n	ode_id:0, b	sf: 6000:1a:01.2, #	accel: 1 #engines: 1 state: up
qat_dev8 - type: c6xxvf, 1	inst_id: 5, n	ode_id:0, b	sf: 6000:1a:01.3, #	accel: 1 #engines: 1 state: up
qat_dev9 - type: c6xxvf,	inst_id: 6, n	ode_id: 0, b	sf: 0000:1a:02.1, #	accel: 1 #engines: 1 state: up
qat_dev10 - type: c6xxvf,	inst_id: 7,	node_id: 0,	bsf: 0000:1a:01.4,	#accel: 1 #engines: 1 state: up
qat_dev11 - type: c6xxvf,	inst_id: 8,	node_id: 0, I	bsf: 0000:1a:01.5,	#accel: 1 #engines: 1 state: up
qat_dev12 - type: c6xxvf,	inst_id: 9, i	node_id: 0, 1	bsf: 0000:1a:02.2,	<pre>#accel: 1 #engines: 1 state: up</pre>
qat_dev13 - type: c6xxvf,	inst_id: 10,	node_id: 0,	bsf: 0000:1a:01.6,	#accel: 1 #engines: 1 state: up
qat_dev14 - type: c6xxvf,	inst_id: 11,	node_id: 0,	bsf: 0000:1a:02.3,	#accel: 1 #engines: 1 state: up
qat_dev15 - type: c6xxvf,	inst_id: 12,	node_id: 0,	bsf: 0000:1a:02.4,	#accel: 1 #engines: 1 state: up
qat_dev16 - type: c6xxvf,	inst_id: 13,	node_id: 0,	bsf: 0000:1a:02.5,	#accel: 1 #engines: 1 state: up
qat_dev17 - type: c6xxvf,	inst_id: 14,	node_id: 0,	bsf: 0000:1a:02.6,	#accel: 1 #engines: 1 state: up
qat_dev18 - type: c6xxvf,	inst_id: 15,	node_id: 0,	bsf: 0000:1a:02.7,	#accel: 1 #engines: 1 state: up
qat_dev19 - type: c6xxvf,	inst_id: 16,	node_id: 0,	bsf: 0000:1b:01.0,	#accel: 1 #engines: 1 state: up
qat_dev20 - type: c6xxvf,	inst_id: 17,	node_id: 0,	bsf: 0000:1b:01.1,	#accel: 1 #engines: 1 state: up
qat_dev21 - type: c6xxvf,	inst_id: 18,	node_id: 0,	bsf: 0000:1b:01.2,	#accel: 1 #engines: 1 state: up
qat_dev22 - type: c6xxvf,	inst_id: 19,	node_id: 0,	bsf: 0000:1b:01.3,	#accel: 1 #engines: 1 state: up
qat_dev23 - type: c6xxvf,	inst_id: 20,	node_id: 0,	bsf: 0000:1b:01.4,	#accel: 1 #engines: 1 state: up
qat_dev24 - type: c6xxvf,	inst_id: 21,	node_id: 0,	bsf: 0000:1b:01.5,	#accel: 1 #engines: 1 state: up
qat_dev25 - type: c6xxvf,	inst_id: 22,	node_1d: 0,	bsf: 0000:1b:01.6,	#accel: 1 #engines: 1 state: up
qat_dev26 - type: c6xxvf,	inst_id: 23,	node_id: 0,	bsf: 0000:1b:01.7,	#accel: 1 #engines: 1 state: up
qat_dev27 - type: c6xxvf,	inst_id: 24,	node_id: 0,	bsf: 0000:1b:02.0,	#accel: 1 #engines: 1 state: up
qat_dev28 - type: c6xxvf,	inst_id: 25,	node_id: 0,	bsf: 0000:1b:02.1,	#accel: 1 #engines: 1 state: up
qat_dev29 - type: c6xxvf,	inst_id: 26,	node_id: 0,	bsf: 0000:1b:02.2,	#accel: 1 #engines: 1 state: up
qat_dev30 - type: c6xxvf,	inst_id: 27,	node_id: 0,	bsf: 0000:1b:02.3,	#accel: 1 #engines: 1 state: up
qat_dev31 - type: c6xxvf,	inst_id: 28,	node_id: 0,	bsf: 0000:1b:02.4,	#accel: 1 #engines: 1 state: up
qat_dev32 - type: c5xxvf,	inst_id: 29,	node_id: 0,	bsf: 0000:1b:02.5,	#accel: 1 #engines: 1 state: up
qat_dev33 - type: c6xxvf,	inst_id: 30,	node_id: 0,	bsf: 0000:1b:02.6,	#accel: 1 #engines: 1 state: up
qat_dev34 - type: c6xxvF,	inst_id: 31,	node_id: 0,	bsf: 0000:1b:02.7,	#accel: 1 #engines: 1 state: up
qat_dev39 - type: c6xxvf,	inst_id: 32,	node_1d: 0,	bsf: 0000:1c:01.4,	#accel: 1 #engines: 1 state: up
qat_dev40 - type: c6xxvf,	inst_id: 33,	node_id: 0,	bsf: 0000:1c:01.5,	#accel: 1 #engines: 1 state: up
qat_dev41 - type: c6xxvf,	inst_id: 34,	node_id: 0,	bsf: 0000:1c:01.6,	#accel: 1 #engines: 1 state: up
qat_dev42 - type: c6xxvf,	inst_id: 35,	node_id: 0,	bsf: 0000:1c:01.7,	#accel: 1 #engines: 1 state: up
qat_dev43 - type: c6xxvf,	inst_id: 36,	node_id: 0,	bsf: 0000:1c:02.0,	#accel: 1 #engines: 1 state: up
qat_dev44 - type: c6xxvf,	inst_id: 37,	node_id: 0,	bsf: 0000:1c:02.1,	#accel: 1 #engines: 1 state: up
qat_dev45 - type: c6xxvf,	inst_id: 38,	node_id: 0,	bsf: 0008:1c:02.2,	#accel: 1 #engines: 1 state: up
qat_dev46 - type: c6xxvf,	inst_1d: 39,	node_1d: 0,	bsf: 0000:1c:02.3,	#accel: 1 #engines: 1 state: up
qat_dev47 - type: c6xxvf,	inst_id: 40,	node_id: 0,	bsf: 0000:1c:02.4,	#accel: 1 #engines: 1 state: up
qat_dev48 - type: c6xxvf,	inst_id: 41,	node_id: 0,	bsf: 0000:1c:02.5,	#accel: 1 #engines: 1 state: up
qat_dev49 - type: c6xxvf,	inst_id: 42,	node_id: 0,	bsf: 0000:1c:02.6,	#accel: 1 #engines: 1 state: up
qat_dev50 - type: c6xxvf,	inst_id: 43,	node_id: 0,	bsf: 0000:1c:02.7,	#accel: 1 #engines: 1 state: up
rootgvenkat-Super-Server:~#				

- 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.

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

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.

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

3. Klicken Sie im Fenster virtual_machine im KVM -Fenster auf das I-Symbol.

DEM			Demo_VPX on QEMU/KVM	+ ×
File	Virtual Machine View	Send Key		
	🕐 🕨 🖉 🔹	6		<mark>م</mark> ۲
	Overview	Basic Details	i	
4-	Performance	Name:	Demo_VPX	
	CPUs	UUID:	2f82dfa1-ae7d-46bf-b63f-833387798cf0	
-	Memory	Status:	Shutoff (Destroyed)	
	Boot Options	Title:		
2	IDE Disk 1	Description:		
-	NIC :7f:81:87			
	Mouse			
	Keyboard			
	Display VNC	Hypervisor D	etails	
	Sound: ich6	Hypervisor:	KVM	
6	Serial 1	Architecture:	: x86_64	
6	Channel spice	Emulator:	/usr/bin/kvm-spice	
	Video QXL	Firmware:	BIOS	
	Controller USB	chipset.	14401 A	
	Controller PCI			
	Controller IDE		N.	
	Controller VirtlO Serial		N	
*	USB Redirector 1			
P	USB Redirector 2			
	-Add Hardware		Cancel	Apply

- 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**.

e Virtual Machine V	iew Send Key	
	Add New Virtual Hardware	• >
Oven Storage Oven Control Perfo Input CPUs Input Mem Sound Boot Serial VirtlC Paralle Mous Consol Displ Video Video Video Video Filesys Contr Smartc Contr PANG	PCI Device Iler rk Host Device: 0000:00:1C:4 Intel Corporation C610/X99 series chipset 0000:00:1D:0 Intel Corporation C610/X99 series chipset 0000:00:1F:0 Intel Corporation C610/X99 series chipset 0000:00:1F:10 Intel Corporation C610/X99 series chipset 0000:00:1F:2 Intel Corporation C610/X99 series chipset 0000:00:1F:3 Intel Corporation C610/X99 series chipset 0000:01:F:6 Intel Corporation C610/X99 series chipset 0000:01:00:0 Intel Corporation C610/X99 series chipset 0000:01:F:6 Intel Corporation C610/X99 series chipset 0000:01:00:0 Intel Corporation C610/X99 series chipset 0000:01:00:0 Intel Corporation C610/X99 series chipset 0000:01:00:0 Intel Corporation Secondary 0000:01:00:0 Intel Corporation I350 Gigabit Network Corporation Secondary 0000:01:00:0 Intel Corporation Ethernet Controller XL710 0000:05:00:0 Intel Corporation Ethernet Controller XL710 0000:05:00:0 Intel Corporation Ethernet Controller XL710 0000:07:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/C0 0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/C0 0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/C0 0000:7F:08:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/C0 0000:7F:08:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/	PCI Express Root Por USB Enhanced Host LPC Controller 6-Port SATA Controlle SMBus Controller Thermal Subsystem nnection (Interface e o for 40GbE QSFP+ (0 for 40GbE QSFP+ (PCI Bridge 5 Family ore i7 QPI Link 0 ore i7 QPI Link 0 ore i7 R3 QPI Link 0 ore i7 R3 QPI Link 0

- 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:



Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

 Suffi×
پ Suffix
Suffix
Suffix
:3f:57:7c NetScaler Virtual Interface
:8e:b8:2d Intel XL710, SR, 10 Gbit
:8e:b8:2e Intel XL710, SR, 10 Gbit
:9e:d8:d9 Intel XL710 40Gbit Interface
:3f:57:7c Netscaler Loopback interface

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 1 2

```
NSVPX-KVM-10.1-117_nc.xml
3
```

```
NSVPX-KVM-10.1-117_nc.raw
```

```
4
   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 f
ür das Datentr
ägerimage an. Der Dateipfad muss absolut sein. Sie k
önnen 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

```
1 <name>NetScaler-VPX</name>
2 <mac address='52:54:00:29:74:b3'/>
3 <source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
```

Geben Sie den absoluten QCOW2-Datenträgerimagequellpfad an, und definieren Sie den Treibertyp als **qcow2**, wie im folgenden Beispiel gezeigt:

Beispiel

```
1 <name>NetScaler-VPX</name>
2 <mac address='52:54:00:29:74:b3'/>
3 <driver name ='qemu' type='qcow2'/>
4 <source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
```

- 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

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

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

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

7. Verbinden der Gast-VM über die Konsole:

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

Beispiel

1 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

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

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

5 </interface>

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.

V localhost.localdomain:6 (admin) Activities	chine Manager	Thu 03:07
		Virtual Machine Manager
File Edit View Help		
🔛 📃 🗮 Open 🔃 🛛		
Name		
✓ localhost (GEMU)		
NetScaler-VPX Running	Run	
	Pause	
	Shut Down 💙	Beboot
	Clone	Shut Down
	Migrate	Eorce Off
	Delete	Sa <u>x</u> e
	Open	
<[

• 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:

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

• 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

1	virsh	shutdown	NetScaler-VPX
2	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:

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.

S	Terminal - root@ubuntu: /etc	+ - • ×
File Edit View Terminal Tabs Help		
root@ubuntu:/etc# echo 1 > /sys/class/net/en	s3f0/device/sriov_numvfs	
root@ubuntu:/etc# echo 1 > /sys/class/net/en	s3f1/device/sriov_numvfs	
root@ubuntu:/etc# lspci grep 82599		
02:00.0 Ethernet controller: Intel Corporati	on 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	
02:00.1 Ethernet controller: Intel Corporati	.on <pre>82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)</pre>	
02:10.0 Ethernet controller: Intel Corporati	on 82599 Ethernet Controller Virtual Function (rev 01)	
02:10.1 Ethernet controller: Intel Corporati	on 82599 Ethernet Controller Virtual Function (rev 01)	
root@ubuntu:/etc# 👢		

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:

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

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

Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.

+ •	Property	+-	Value
	checksum container_format created_at disk_format hw_disk_bus id min_disk min_ram name owner protected size status tags updated_at virtual_size visibility		735dae4ea6e46e39ed3f0acfba02e755 bare 2017-02-16T10:03:29Z qcow2 ide aeaa13e9-b49b-411c-ab54-c61820a8e2f3 0 0 NSVPX-KVM-12.0-26.2 06c41a73b32f4b48af55359fd7d3502c False 717946880 active [] 2017-02-16T10:03:38Z None 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.

PropertyValueI PropertyValueI OS-DCF:diskConfigMANUALI OS-EXT-AZ:availability_zone-I OS-EXT-AZ:availability_zone-I OS-EXT-SRV-ATTR:host-I OS-EXT-SRV-ATTR:hypervisor_hostname-I OS-EXT-SRV-ATTR:hypervisor_hostname-I OS-EXT-SRV-ATTR:hypervisor_hostname-I OS-EXT-SRV-ATTR:hypervisor_hostname-I OS-EXT-SRV-ATTR:hypervisor_hostname-I OS-EXT-STS:tosk_stateI schedulingI OS-EXT-STS:tosk_statebuildingI OS-SRV-USG:launched_at-I oC-SRV-USG:launched_at-I accessIPv4-I accessIPv4-I adninPass43EjPdMSshLzI config_driveI TrueI created2017-02-20T11:53:37ZI flavorm1.medium (3)I hostId-I id699f6968-aab9-463c-b619-d58c73db3187I imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)I key_namemetadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	_		
OS-DCF:diskConfigMANUALOS-DCF:diskConfigMANUALOS-EXT-AZ:availability_zone-OS-EXT-SRV-ATTR:host-OS-EXT-SRV-ATTR:hypervisor_hostnameinstance-0000003cOS-EXT-SRV-ATTR:instance_nameinstance-0000003cOS-EXT-STS:power_state0OS-EXT-STS:task_stateischedulingOS-EXT-STS:tow_statebuildingOS-EXT-STS:task_stateischedulingOS-SRV-USG:launched_at-I accessIPv4-accessIPv4-adminPass43EjPdMSshLzcorfig_driveTruecreated2017-02-20T11:53:37Zflavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	+ -	Property	Value I
OS-EXT-AZ:availability_zoneInstanceOS-EXT-SRV-ATTR:host-OS-EXT-SRV-ATTR:hypervisor_hostname-OS-EXT-SRV-ATTR:instance_nameinstance-0000003cOS-EXT-SRV-ATTR:instance_name0OS-EXT-STS:power_state0OS-EXT-STS:task_stateschedulingOS-EXT-STS:task_statebuildingOS-SRV-USG:launched_at-IaccessIPv4IaccessIPv4IaccessIPv4Iconfig_driveI flavorm1.medium (3)hostId-I6b9f6968-aab9-463c-b619-d58c73db3187I mageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-100os-extended-volumes:volumes_attached[]progress0	•••	OS-DCE:diskConfig	ΜΔΝΙΙΔΙ
OS-EXT-SRV-ATTR:histore_nome-OS-EXT-SRV-ATTR:hypervisor_hostnameinstance-0000003cOS-EXT-SRV-ATTR:instance_nameinstance-0000003cOS-EXT-STS:power_state0OS-EXT-STS:m_statebuildingOS-SRV-USG:launched_at-I-OS-SRV-USG:terminated_at-accessIPv4-accessIPv6-adminPass43EjPdMSshLzconfig_driveTruecreated2017-02-20T11:53:37Zflavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187image-metadata{}nameNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)os-extended-volumes:volumes_attached[]progress0		OS-EXT-AZ:availability zone	
OS-EXT-SRV-ATTR:hypervisor_hostname-OS-EXT-SRV-ATTR:instance_nameinstance-0000003cOS-EXT-STS:power_state0OS-EXT-STS:task_stateschedulingOS-EXT-STS:vm_statebuildingOS-SRV-USG:launched_at-I accessIPv41accessIPv61adminPass43EjPdM5shLzconfig_drive1reated2017-02-20T11:53:37Zflavorm1.medium (3)hostId1id6b9f6968-aab9-463c-b619-d58c73db3187imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]	i	0S-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:instance_nameinstance-0000003cOS-EXT-SRV-ATTR:instance_name0OS-EXT-STS:power_state0OS-EXT-STS:task_stateschedulingOS-SRV-USG:launched_at-OS-SRV-USG:terminated_at-accessIPv4-accessIPv6-adminPass43EjPdM5shLzconfig_driveTruecreated2017-02-20T11:53:372flavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	i	0S-EXT-SRV-ATTR: hypervisor hostname	
OS-EXT-STS:power_state0OS-EXT-STS:task_stateschedulingOS-EXT-STS:vm_statebuildingOS-SRV-USG:launched_at-OS-SRV-USG:terminated_at-accessIPv4accessIPv6adminPass43EjPdM5shLzconfig_driveTruecreated2017-02-20T11:53:37Zflavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	i	0S-EXT-SRV-ATTR:instance name	instance-000003c
OS-EXT-STS:task_stateschedulingOS-EXT-STS:vm_statebuildingOS-SRV-USG:launched_at-OS-SRV-USG:terminated_at-accessIPv4-accessIPv6-adminPass43EjPdM5shLzconfig_driveTruecreated2017-02-20T11:53:37Zflavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187imageNVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	i	0S-EXT-STS:power_state	0
OS-EXT-STS:vm_statebuildingOS-SRV-USG:launched_at-OS-SRV-USG:terminated_at-accessIPv4-accessIPv6-adminPass43EjPdM5shLzconfig_driveTruecreated2017-02-20T11:53:37Zflavorm1.medium (3)hostId-id6b9f6968-aab9-463c-b619-d58c73db3187imageNSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)key_name-metadata{}nameNSVPX-10os-extended-volumes:volumes_attached[]progress0	i	0S-EXT-STS:task state	scheduling
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 - name NSVPX-10 os-extended-volumes:volumes_attached [] progress 0	i	OS-EXT-STS:vm_state	building
OS-SRV-USG:terminated_at - accessIPv4 - 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	i	0S-SRV-USG: Jaunched at	-
accessIPv4 accessIPv6 adminPass 43EjPdM5shLz config_drive created 2017-02-20T11:53:37Z flavor 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	i	OS-SRV-USG:terminated at	-
accessIPv6 adminPass config_drive created created constid id id image key_name name NSVPX-10 os-extended-volumes:volumes_attached [] progress	i	accessIPv4	
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	i	accessIPv6	
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	i	adminPass	43EiPdM5shLz
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	i	config drive	True
flavor m1.medium (3) hostId i 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	l	created	2017-02-20T11:53:37Z
hostId id id image image key_name metadata name os-extended-volumes:volumes_attached [] progress	l	flavor	m1.medium (3)
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	1	hostId	
image I NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1) key_name I - metadata I {} name I NSVPX-10 os-extended-volumes:volumes_attached [] progress 0	1	id	6b9f6968-aab9-463c-b619-d58c73db3187
key_name - metadata {} name NSVPX-10 os-extended-volumes:volumes_attached [] progress 0	1	image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
metadata {} name NSVPX-10 os-extended-volumes:volumes_attached [] progress 0	1	key_name	-
I name I NSVPX-10 I os-extended-volumes:volumes_attached [] I progress I 0	I	metadata	8
os-extended-volumes:volumes_attached [] progress 0	I	name	NSVPX-10
progress 0	I	os-extended-volumes:volumes_attached	
	I	progress	0
i security_groups i default	l	security_groups	default
status I BUILD	I	status	BUILD
l tenant_id 06c41a73b32f4b48af55359fd7d3502c	I	tenant_id I	06c41a73b32f4b48af55359fd7d3502c
updated 2017-02-20T11:53:38Z	I	updated I	2017-02-20T11:53:38Z
luser_id 418524f7101b4f0389ecbb36da9916b5	1	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"?>
1
2
     <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
        11
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3
     oe:id=""
4
5
     xmlns="http://schemas.dmtf.org/ovf/environment/1">
     <PlatformSection>
6
7
     <Kind>NOVA</Kind>
8
     <Version>2013.1</Version>
9
     <Vendor>Openstack</Vendor>
10
     <Locale>en</Locale>
     </PlatformSection>
11
12
     <PropertySection>
13
     <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="</pre>
        1.0"/>
     <property oe:key="com.citrix.netscaler.platform" oe:value="vpx"</pre>
14
        />
15
     citrix.com 4
16
     <property oe:key="com.citrix.netscaler.orch_env"</pre>
17
     oe:value="openstack-orch-env"/>
18
     <property oe:key="com.citrix.netscaler.mgmt.ip"</pre>
19
     oe:value="10.1.0.100"/>
20
     <Property oe:key="com.citrix.netscaler.mgmt.netmask"
```

```
21 oe:value="255.255.0.0"/>
22 <Property oe:key="com.citrix.netscaler.mgmt.gateway"
23 oe:value="10.1.0.1"/>
24 </PropertySection>
25 </Environment>
```

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

```
4: enp8s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT qlen 1000
link/ether 00:1b:21:7b:d7:88 brd ff:ff:ff:ff:ff
vf 0 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 1 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 2 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 3 MAC fa:16:3e:1e:0b:ee, spoof checking on, link-state auto, trust off
vf 4 MAC fa:16:3e:0d:05:62, spoof checking on, link-state auto, trust off
vf 5 MAC fa:16:3e:0d:05:62, spoof checking on, link-state auto, trust off
vf 6 MAC fa:16:3e:db:ea:b3, vlan 10 spoof checking on, link-state auto, trust off
vf 7 MAC 00:00:00:00:00:00; 00; 00; 00, spoof checking on, link-state auto, trust off
```

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

[root@localhost ~]# ip link show enp8s0f0
4: enp8s0f0: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP mode DEFAULT qlen 1000</broadcast,multicast,up,lower_up>
link/ether 00:1b:21:7b:d7:88 brd ff:ff:ff:ff:ff:ff
vf 0 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 1 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 2 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
vf 3 MAC fa:16:3e:1e:0b:ee, spoof checking on, link-state auto, trust off
vf 4 MAC fa:16:3e:0d:05:62, spoof checking on, link-state auto, trust off
vf 5 MAC 5e:46:0d:79:de:f8 spoof checking on, link-state auto, trust off
vf 6 MAC fa:16:3e:db:ea:b3, spoof checking on, link-state auto, trust off
vr / MAC 00:00:00:00:00:00; spoor checking on, link-state auto, trust off

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

RHOS-Befehl:

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:

```
1 > $0VS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
user1 mtu_request=9000
2 
3 > $0VS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-
user2 mtu_request=9000
4 
5 chmod g+w /usr/local/var/run/openvswitch/vhost*
```

RHOS-Befehl:

```
1 ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
	type=dpdkvhostuser -- set Interface vhost-user1 mtu_request=9000
2 ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
	type=dpdkvhostuser -- set Interface vhost-user2 mtu_request=9000
4 5 chmod g+w /var/run/openvswitch/vhost*
```

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 \
1
2
3
     -object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages
         ,share=on -numa node,memdev=mem ∖
4
5
     -mem-prealloc -smp sockets=1, cores=2 -drive file=<absolute-path-to-
        disc-image-file>, if=none, id=drive-ide0-0-0, format=<disc-image-
         format> \
6
     -device ide-drive, bus=ide.0, unit=0, drive=drive-ide0-0-0, id=ide0-0-0,
7
        bootindex=1 \
8
9
     -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
```
```
-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
        bus=pci.0,addr=0x3 \
12
     -chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
13
        user1> \
14
     -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
15
        virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
16
17
     -chardev socket, id=char1, path=</usr/local/var/run/openvswitch/vhost-
        user2> \
18
     -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
19
        virtio-net
20
21
     pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
22
23
     --nographic
```

Verwenden Sie für RHOS die folgende XML-Beispieldatei, um die NetScaler VPX-Instanz mithilfe von bereitzustellen virsh.

```
1
     <domain type='kvm'>
2
       <name>dpdk-vpx1</name>
3
4
        <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
5
6
7
        <memory unit='KiB'>16777216</memory>
8
9
        <currentMemory unit='KiB'>16777216</currentMemory>
11
        <memoryBacking>
12
         <hugepages>
13
14
15
            <page size='1048576' unit='KiB'/>
16
17
          </hugepages>
18
        </memoryBacking>
19
20
        <vcpu placement='static'>6</vcpu>
21
22
23
        <cputune>
24
25
         <shares>4096</shares>
27
         <vcpupin vcpu='0' cpuset='0'/>
28
29
         <vcpupin vcpu='1' cpuset='2'/>
          <vcpupin vcpu='2' cpuset='4'/>
31
```

32	
33	<vcpupin cpuset="6" vcpu="3"></vcpupin>
34	
35	<emulatorpin cpuset="0,2,4,6"></emulatorpin>
36	
37	
30	
40	
41	<memory mode="strict" nodeset="0"></memory>
42	
43	
44	
45	<resource></resource>
46	
47	<partition>/machine</partition>
40 49	
50	
51	<os></os>
52	
53	<type arch="x86_64" machine="pc-i440fx-rhel7.0.0">hvm</type>
54	
55	<boot dev="hd"></boot>
56	
58	1037
59	<features></features>
60	
61	<acpi></acpi>
62	
63	<apic></apic>
65	
66	
67	<cpu check="full" match="minimum" mode="custom"></cpu>
68	
69	<model fallback="allow">Haswell-noTSX</model>
70	(verder) Intel (verder)
72	<pre><vendor>intet</vendor></pre> /vendor>
73	<topology_sockets='1'_cores='6'_threads='1'></topology_sockets='1'_cores='6'_threads='1'>
74	
75	<feature name="ss" policy="require"></feature>
76	
77	<teature name="pcid" policy="require"></teature>
70	(feature policy=!require! name=!bypervisor!/)
80	steature potrey-require name- hypervisor //
81	<feature name="arat" policy="require"></feature>
82	
83	<domain type="kvm"></domain>
84	

85	<name>dpdk-vpx1</name>
86	wide add a the the the the state action and the state of
88	<pre><uuuuvaeub844b=16bc=46e6=a4c6=363111208806< pre="" uu1uv<=""></uuuuvaeub844b=16bc=46e6=a4c6=363111208806<></pre>
89	<pre><memory unit="KiB">16777216</memory></pre>
90	
91	<currentmemory unit="KiB">16777216</currentmemory>
92	
93	<memorybacking></memorybacking>
94	
95	<hugepages></hugepages>
96	(nogo cizo-110405761 unit-1KiPL/N
97	spage size- 1048576 ulite- Kib //
99	
100	1.1.1.2.0.2.2.2.2.
101	
102	
103	<vcpu placement="static">6</vcpu>
104	
105	<cputune></cputune>
107	(charac) (0) (charac)
108	Shares/4030(/ Shares/
109	<vcpupin cpuset="0" vcpu="0"></vcpupin>
110	shah sha shasa sh
111	<vcpupin cpuset="2" vcpu="1"></vcpupin>
112	
113	<vcpupin cpuset="4" vcpu="2"></vcpupin>
114	
115	<vcpupin cpuset="16772</td" vcpu="13"></vcpupin>
117	<pre><emulatorpin cpuset="0.2.4.6"></emulatorpin></pre>
118	
119	
120	
121	<numatune></numatune>
122	
123	<memory hodeset="0" mode="strict"></memory>
124	
125	
127	<resource></resource>
128	
129	<partition>/machine</partition>
130	
131	
132	
133	NUS2
134	<pre>stype arch='x86\ 64' machine='nc-i440fy-rhel7 0 0'>hym</pre>
136	cype aren xee(_er maenne pe interver neerver viviley cype)
137	<boot dev="hd"></boot>

138	
139	
140	
141	<features></features>
142	
143	<acpi></acpi>
144	
145	<apic></apic>
146	
147	
148	
149	<cpu check="full" match="minimum" mode="custom"></cpu>
150	
151	<model fallback="allow">Haswell-noTSX</model>
152	
153	<vendor>Intel</vendor>
154	
155	<topology cores="6" sockets="1" threads="1"></topology>
156	
157	<feature name="ss" policy="require"></feature>
158	
159	<feature name="pcid" policy="require"></feature>
160	
161	<feature name="hypervisor" policy="require"></feature>
162	
163	<feature name="arat" policy="require"></feature>
164	
165	<feature name="tsc_adjust" policy="require"></feature>
166	
167	<reature name="xsaveopt" policy="require"></reature>
168	(feature relievely any inclusion induction 1/2)
159	<reature name="popeigb" policy="require"></reature>
171	
172	<pre>Niuliid></pre>
172	<pre>Kcoll id=101 cpus=10-51 momory=1167772161 upit=1KiR1 momAccoss=</pre>
TIS	shared!/>
174	
175	
176	
177	
178	() cpu/
179	<clock offset="utc"></clock>
180	
181	<pre><on\ noweroff="">destrov</on\></pre>
182	
183	<pre><on\ reboot="">restart</on\></pre>
184	
185	<pre><on\ crash="">destrov</on\></pre>
186	
187	<devices></devices>
188	
189	<emulator>/usr/libexec/qemu-kvm</emulator>

190 191 <disk type='file' device='disk'> 192 <driver name='qemu' type='qcow2' cache='none'/> 193 194 <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/> 196 <target dev='vda' bus='virtio'/> 197 199 <address type='pci' domain='0x0000' bus='0x00' slot='0x07'</pre> function='0x0'/> </disk> <controller type='ide' index='0'> 204 <address type='pci' domain='0x0000' bus='0x00' slot='0x01' 205 function='0x1'/> 206 </controller> 207 208 <controller type='usb' index='0' model='piix3-uhci'> <address type='pci' domain='0x0000' bus='0x00' slot='0x01' 211 function='0x2'/> 212 213 </controller> 214 <controller type='pci' index='0' model='pci-root'/> 215 216 217 <interface type='direct'> 218 <mac address='52:54:00:bb:ac:05'/> 219 <source dev='enp129s0f0' mode='bridge'/> 221 222 223 <model type='virtio'/> 224 <address type='pci' domain='0x0000' bus='0x00' slot='0x03' 225 function='0x0'/> 227 </interface> 229 <interface type='vhostuser'> 230 <mac address='52:54:00:55:55:56'/> <source type='unix' path='/var/run/openvswitch/vhost-user1'</pre> 233 mode='client'/> 234 <model type='virtio'/> 236 <address type='pci' domain='0x0000' bus='0x00' slot='0x04'

220	<pre>tunction='0x0'/></pre>
220	(/interface)
235	<pre>//interface/</pre>
240	(interface type=)/hestuser!>
241	Vincerrace cype- viloscuser /
242	(mag. addross=152:54:00:20:22:641/)
243	<pre></pre>
244	Courses type=lupix1 path=1/yar/rup/epepyewitch/ybect_ucor21
243	mode='client'/>
246	
247	<model type="virtio"></model>
248	Kaddrass type=lacil demain=l0y00001 bys=l0y001 slot=l0y051
249	function='0x0'/>
250	
251	
252	(interface type=lybectycerl)
253	<pre><intertace type="`vnostuser'"></intertace></pre>
254	(mag. addross-152+54+00+20+22+741/)
200	<pre></pre>
250	Courses type=lupix1 path=1/yar/rup/openycwitch/ybect_ucor21
251	mode='client'/>
250	(model type=lyistic1/)
255	
261	<address <br="" bus="0x00" domain="0x0000" slot="0x06" type="pci">function='0x0'/></address>
262	, ,
263	
264	
265	<interface type="vhostuser"></interface>
266	
267	<mac address="52:54:00:2a:32:84"></mac>
268	
269	<source <br="" path="/var/run/openvswitch/vhost-user4" type="unix"/> mode='client'/>
270	
271	<model type="virtio"></model>
272	
273	<address <br="" bus="0x00" domain="0x0000" slot="0x09" type="pci">function='0x0'/></address>
274	
275	
276	
277	<serial type="pty"></serial>
278	
279	<target port="0"></target>
280	
281	
282	
283	<console type="pty"></console>

```
284
             <target type='serial' port='0'/>
          </console>
287
288
289
          <input type='mouse' bus='ps2'/>
290
291
          <input type='keyboard' bus='ps2'/>
292
293
          <graphics type='vnc' port='-1' autoport='yes'>
294
             type='address'/>
295
296
297
          </graphics>
299
          <video>
             <model type='cirrus' vram='16384' heads='1' primary='yes'/>
301
302
             <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
                function='0x0'/>
304
          </video>
306
          <memballoon model='virtio'>
             <address type='pci' domain='0x0000' bus='0x00' slot='0x08'</pre>
                function='0x0'/>
310
          </memballoon>
311
312
        </devices>
313
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
```

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:

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

```
12 12 12 14 10.102.38.216 </IP>
14 14 15 16 17
18 17 17
```

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 userdataverwendet 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.

```
Total translation table size: 0
7
8
    Total rockridge attributes bytes: 0
9
    Total directory bytes: 0
    Path table size(bytes): 10
10
11
   Max brk space used O
12
    175 extents written (0 MB)
13
    root@ubuntu:~/sai/19oct#
14
    root@ubuntu:~/sai/19oct# ls -lh
15
    total 356K
16
    -rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
17
     -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
```

- 3. 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

April 1, 2025

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 Lizenzierungsoption für NetScaler VPX-Instanzen, die auf AWS ausgeführt werden, ist Bring Your Own License (BYOL).

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
- Entdecken Sie den Vorteil von NetScaler und AWS

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.
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.

Begriff	Definition
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.
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.

Begriff	Definition
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.
Automatische Skalierung	Ein Webservice zum automatischen Starten oder
Ū.	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

January 15, 2025

In den folgenden Tabellen sind die unterstützten VPX-Angebote, AWS-Regionen, Instanztypen und Services aufgeführt.

Tabelle 1: Unterstützte VPX-Angebote auf AWS

Unterstützte VPX-Angebote

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 (Melbourne)

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)

Unterstützte AWS Regionen EU (Frankfurt) EU (Irland) EU (London) EU (Daris) EU (Paris) EU (Mailand) Südamerika (São Paulo) AWS GovCloud (USA-Ost) AWS GovCloud (USA, West) AWS Streng geheim (C2S) Naher Osten (Bahrain) Naher Osten (VAE) Afrika (Kapstadt) C2S

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

c6 Zoll groß, c6 Zoll xgroß, c6 Zoll 2 xgroß, c6 Zoll 4 xgroß, c6 Zoll 8 xgroß, c6 Zoll 12 xgroß, c6 Zoll 16 xgroß, c6 Zoll 24 xgroß, c6 Zoll 32 xgroß

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

Unterstützte AWS-Instanztypen

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

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.

Empfohlene AWS-Instanz
m5.xGroß
m5.2xGroß

VPX mit gepoolter oder flexibler Lizenzierung	
(Bandbreitenlizenzen)	Empfohlene AWS-Instanz
5-8 Gbit/s	c5n.4xGroß
8-25 Gbit/s	c5n.9xGroß

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 nsvlanfinden Sie unter Konfigurieren von NSVLAN.

 In der AWS-Konsole kann die vCPU-Auslastung, die f
ür eine VPX-Instanz auf der Registerkarte Überwachung angezeigt wird, hoch sein (bis zu 100 Prozent), selbst wenn die tats
ächliche Auslastung wesentlich geringer ist. Um die tats
ächliche 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-, SRIOVund 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",
1
2
```

- "ec2:AssignPrivateIpAddresses", "ec2:AssignIpv6Addresses", 3
- 4 "ec2:UnassignIpv6Addresses",
 5 "iam:SimulatePrincipalPality "iam:SimulatePrincipalPolicy",
- "iam:GetRole", 6
- "ec2:CreateTags" 7

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
1
     "ec2:DescribeAddresses",
2
     "ec2:AssociateAddress",
3
     "ec2:DisassociateAddress",
4
5
6
     "iam:SimulatePrincipalPolicy",
     "iam:GetRole",
6
     "ec2:CreateTags"
7
```

HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

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

HA-Paar mit privaten IP- und Elastic IP-Adressen über verschiedene AWS-Zonen hinweg:

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

Autoscaling des AWS-Backends:

```
"ec2:DescribeInstances",
1
       "autoscaling:*",
2
3 "sns:CreateTopic",
4 "sns:DeleteTopic",
5 "sns:ListTopics",
6 "sns:Subscribe",
```

```
7 "sqs:CreateQueue",
8 "sqs:ListQueues",
9 "sqs:DeleteMessage",
10 "sqs:GetQueueAttributes",
11 "sqs:SetQueueAttributes",
12 "iam:SimulatePrincipalPolicy",
13 "iam:GetRole",
14 "ec2:CreateTags"
```

Hinweis:

- Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen f
 ür 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

April 1, 2025

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:

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

HA-Paar mit IPv6-Adressen in derselben AWS-Zone:

```
    "ec2:DescribeInstances",
    "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",
1
2
    "ec2:DescribeAddresses".
    "ec2:AssociateAddress",
3
    "ec2:DisassociateAddress",
4
    "ec2:DescribeRouteTables",
5
    "ec2:DeleteRoute",
6
7
   "ec2:CreateRoute",
8
   "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
9
    "iam:GetRole"
```

Autoscaling des AWS-Backends:

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

New EC2 Experience X	Instances (1) Info
EC2 Dashboard	Q. Find instance by attribute or tag (case-sensitive) < 1 > ③
EC2 Global View	Name V Instance ID Instance state V Instance type V Status check Alarm status Availability Zone
Events	adc i-0cc53b7cdd39f9621 Ø Running Q m5.xlarge Ø 2/2 checks passed No alarms + us-east-1a
Tags	
Limits	
▼ Instances	
Instances New	
Instance Types	
Launch Templates	
Spot Requests	
Savings Plans	Select an instance \otimes X
Reserved Instances New	
Dedicated Hosts	
Scheduled Instances	
Capacity Reservations	
▼ Images	
AMIs New	
AMI Catalog	
Elastic Block Store	
Volumes	

3. Navigieren Sie zu Aktionen > Sicherheit > IAM-Rolle ändern.

🔘 New EC2 Experience 🗸 🗸	Instances (1/1) Info	C	Connect	Instance state	Actions 🔺	Launch in	stances	•
Tell us what you think	Q Find instance by attribute or tag (case-sensitive)				Connect		1	> @
EC2 Dashboard					View details			
EC2 Global View	✓ Name ♥ Instance ID	Instance state	⊽ Insta	nce type	IS che Manage instanc	e state	ailabi	lity Zone
Events	adc i-0cc53b7cdd39f962	21 🕢 Running 🔍 G	रे m5.x	large 📀 2/	/2 che		-east-1	la
Tags					Networking	95		
Limits				channe and it	Networking			
				Change security group	ps Security			
Instances				Get Windows passwor	rd Image and tem	plates		
Instances New			L	Modify IAM role	Monitor and tr	oubleshoot	•	
Instance Types								
Launch Templates								
Spot Requests			=					
Savings Plans	Instance: i-0cc53b7cdd39f9621 (adc)	Instance: i-0cc53b7cdd39f9621 (adc) 💿					⊚ ×	
Reserved Instances New	Detaile Country Networking Storage							
Dedicated Hosts	Details Security Networking Storage	Status checks Monito	oring	rags				
Scheduled Instances	▼ Instance summary Info							
Capacity Reservations	Instance ID	Public IPv4 address		Pri	ivate IPv4 addresses			
	i-0cc53b7cdd39f9621 (adc)	52.3.230.117 open add	ress 🖸	6	10.10.1.160			
Images	IPv6 address	Instance state		Pu	ublic IPv4 DNS			
AMIs New	-	⊘ Running		-				
AMI Catalog	Hostname type	Private IP DNS name (IPv4 or	alv)					
Elastic Block Store	IP name: ip-10-10-1-160.ec2.internal	D ip-10-10-1-160.ec2.inte	rnal					
Volumes	Answer private resource DNS name	Instance type		Ela	astic IP addresses			

- 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.

Addify IAM role into tach an IAM role to your instance.	
Instance ID ☐ I-Occ53b7cdd39f9621 (adc) AM role deter an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are write matched to your instance. Choose IAM role If you choose No IAM Role, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?	
Cancel Update IAM role	
	Addify IAM role two ttach an IAM role to your instance. Instance ID C I-occ53b7cdd39f9621 (adc) AM role entremity attached to your instance or create a new role if you haven't created any. The role you select replaces any roles that are entremity attached to your instance or create a new role if you haven't created any. The role you select replaces any roles that are entremity attached to your instance. C Coose IAM role If you choose No IAM Role, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance? M role IAM role C Create new IAM role IAM role IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance? M role IAM role

b) Klicken Sie auf der Seite Rollen auf Rolle erstellen.

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

c) Wählen Sie AWS-Service unter Trusted Entity Type und EC2 unter Common Use Cases

aus und klicken Sie dann auf Weiter.

Allow AVVS service Allow AVVS services like EC2, Lambda, or others to partiam actions in this account.	AWS account Allow entities in other AWS account belonging to you or a Brd party to perform actions in this account.	 Web identity Allows users todevaled by the specified external web identity provider to assume this role to perform actions in this account. 	
SAMIL 2.0 federation Abov users indensised with SAMI, 2.0 from a corporate directory to perform actions in this account.	Custom trust policy Create a custom trust policy to enable others to perform actions in this account.		
Use case Allow an AWS service like EC2, Lambda, or o	thers to perform actions in this account.		
Use case Afove an AWS service like EC2, Lambda, or o Common use cases © EC2 Adows EC2 instances to call AWS service	thers to perform actions in this account.		
Use case Alow an AVRS service like EC2, Lambde, or / Common use cases C2 Alows EC2 Instances to call AVRS servic Alows Lambda Alows Lambda Uncitors to call AVRS servic	there to perform actions in this account. as on your behalf. release on your behalf.		
Use case Allow an AVVS service like EC2, Lambda, or o Common use cases D CO Allow EC2 Instances to call AVVS servic Allows Lambda functions to call AVVS services: Use cases for other AVVS services:	thes to perform actions in this account, as on your ballant, invices on your ballant,		

d) Klicken Sie auf der Seite "Berechtigungen hinzufügen "auf Richtlinie erstellen.

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

e) Klicken Sie auf den **JSON-Tab**, um den JSON-Editor zu öffnen.

policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more			
Visual editor JSON		Import managed polic	
1 • { 2 "Version": "20: 3 "Statement": [4 }	12-10-17",]		

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:

```
1 {
2 
3 "Version": "2012-10-17",
4 "Statement": [
5 {
6
```

```
"Sid": "VisualEditor0",
8
                  "Effect": "Allow",
9
                  "Action": [
10
                       "ec2:DescribeInstances",
                       "autoscaling:*",
11
                       "sns:CreateTopic",
12
                       "sns:DeleteTopic",
13
                       "sns:ListTopics",
14
                       "sns:Subscribe",
15
                       "sqs:CreateQueue",
                       "sqs:ListQueues",
17
18
                       "sqs:DeleteMessage",
19
                       "sqs:GetQueueAttributes",
                       "sqs:SetQueueAttributes"
                       "iam:SimulatePrincipalPolicy",
21
                       "iam:GetRole"
22
23
                  ],
                  "Resource": "*"
24
               }
25
26
27
          ]
      }
28
```

Stellen Sie sicher, dass das Schlüsselwertpaar "Version", das Sie angeben, mit dem identisch ist, das automatisch von AWS generiert wird.

g) Klicken Sie auf Weiter: Überprüfen.

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

h) Geben Sie auf der Registerkarte **Richtlinie überprüfen** der Richtlinie einen gültigen Namen und klicken Sie auf **Richtlinie erstellen**.

					1 2 3
Review policy					
Name* ba	ackend_autoscaling_policy				
Use	alphanumeric and '+=,.@' charac	ters. Maximum 128 characters.			
Description					
2000 April 10					
					lh
Max	imum 1000 characters. Use alphar	umeric and '+=,.@' characters.			
Summary	a				
C	J, Filter				
Se	ervice 👻	Access level	Resource	Request c	ondition
A	llow (5 of 338 services) Show	v remaining 333			
EC	02	Limited: List	All resources	None	
EC	C2 Auto Scaling	Full access	All resources	None	
IA	м	Limited: Read	All resources	None	
St	NS	Limited: List, Write	All resources	None	
so	QS	Limited: Read, Write	All resources	None	
Tags	V		A Malua		
	Ney		- Value		Ŷ
		No ta	gs associated with the resource.		

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**.

Add permissions us	
Persbalan publica (UNIX) we	O Downey only (7)
	< 1 0 0 4 5 6 7 - M 3 0
W Poly-part (7 V Qu V Receipts	
B Dissocratery, data.	
Bacted Jacket Jacket Control (1997)	© tree for
0 ************************************	
a Sumary w	11.
© Chattendetten_ date.	
0 0 bashundrinenge. bashun	
3 Bardinectoreat., Adj m., Posta nativity scene to MS liket forvat size Adj Marganet Grauk.	
B Annueviliante Ras. Addi e Previde and only assess in Annueviliante due and only assess in Annueviliante due and Schurzer and Constant.	
© Ø Hollakonspisor F Akti e Akti e Akti e Nexiste ite all angle is the first biologican software software indexes to the single biological software indexes indexes indexes indexes to the single biological software indexes ind	
O B ANXECCIMING. ARE N. Advisition assess to BIC Overlay.	
© 🖞 Avids Diadeat. Alt s. Proto ready assess is M3 517 Dist.	
(i) B Audushiphawal. AND s AND s Poolski seb orly assess UA-to Stating on Te-AND Manapuret Counts.	
B Ananoldification, Arti R., Prode score of angle 5 article 10 and experience (IN).	
0.0 Execution for a Mit . Some and day locate to find the based on the later series	
0. 🜒 unaverlight das . All n. – Projek far press ta deserv für sich all für deserver in meis	
O Begenchar Ald m. Day polycywate permissions to insulational and models taxan in the Ald annuel Tay polycy das makeds for one to content Mill separation mode and enough taxan.	
(i) Ø investel D'Aldrea. All n Prosides M access to Antonni UC via the MMI Riscopport Organia.	
(1) 🚯 (menulargen)a. ART Problem mårbelte avsets i ART.Bonnik Menger vå te	
🛞 🚯 Jakoba Thogodhag	
🛞 🖗 Januar Caulifation Alti K	
Ng parakalasi kazalap yalikala a. Ng parakalasi kazalap yalikala a.	
	Cancel Percent Real

j) Geben Sie der Rolle auf der Seite **Name, Überprüfung und Erstellen** einen gültigen Namen.

Step 1 Select trusted entity	Name, review, and create	
Step 2 Add permissions	Role details	
Step 3	Role name Enter a meaningful name to identify this role.	
Name, review, and create	ADC_IAMRole	
	Maximum 64 characters. Use alphanumeric and '+=,,@' characters.	
	Description Add a short explanation for this role.	
	Allows EC2 instances to call AWS services on your behalf.	
	Maximum 1000 characters. Use alphanumeric and '+=,	
	Step 1: Select trusted entities	Edit
	<pre>1 - [{</pre>	

k) Klicken Sie auf Rolle erstellen.

Step 2: Add permissions			Ed
Permissions policy summary			
Policy name C*	⊽Туре	✓ Attached as	
backend_autoscaling_policy	Customer managed	Permissions policy	
Add togo (Ontional)			
Add tags (Optional)			
lags are key-value pairs that you can add to AWS re	asources to help identify, organize, or search for resources.		
No tags associated with the resource.	sources to help identify, organize, or search for resources.		
No tags associated with the resource.	sources to help identity, organize, or search for resources.		
No tags associated with the resource.	sources to help identity, organize, or search for resources.		
No tags are key-value pairs that you can add to AWS read and the AWS read and the second term of term	sources to help identity, organize, or search for resources.		

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.

Modify IAM role Info			
Attach an IAM role to your instance.			
Instance ID			
-			
D i-099f319d4e89f0ca2 (adc)			
D 1-099f319d4e89f0ca2 (adc)			
I-099f319d4e89f0ca2 (adc) IAM role Select an IAM role to attach to your instance or create a new role il currently attached to your instance.	you haven't created as	y. The role y	ou select replaces any roles that
H-999f319d4e89f0ca2 (adc) IAM role Select an IAM role to attach to your instance or create a new role il urmenty attached to your instance. Choose IAM role	you haven't created ar	y. The role y	ou select replaces any roles that
GP I-099f319d4e89f0ca2 (adc) IAM role Select an IAM role to attach to your instance or create a new role il urrently attached to your instance. Choose IAM role Q	you haven't created a	y. The role y	Create new IAM role [2
I-O99f319d4e89f0ca2 (adc) IAM role Select an Irk role to attach to your instance or create a new role il currently attached to your instance. Choose IAM role Q No IAM Role	you haven't created ar	y. The role y	ou select replaces any roles that Create new IAM role [2 will be removed. Are you

7. Klicken Sie auf IAM-Rolle aktualisieren.

Modify IAM role Info	78.
and a second to your materia	1991
nstance ID	
🗇 i-00c340e20506a5b6e (N	letScaler Gateway)
AM role	
elect an IAM role to attach to yo urrently attached to your instance	ur instance or create a new role if you haven't created any. The role you select replaces any roles that are te.
ADC_IAMRole	Create new IAM role 🗹

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.

Identity and Access X Management (IAM)			Delete
Dashboard	Allows EC2 instances to call AWS services on your be	shalf.	
 Access management User groups 	Summary		Edit
Users	Creation date	ARN	Instance profile ABN
Roles	July 18, 2022, 19:37 (UTC+05:30)	2 arn:aws:iam::999910688552:role/ADC_IAMRole	입 arn:aws:iam::999910688552:instance-profile/AD
Policies			C_IAMRole
Identity providers	Last activity	Maximum session duration	
Account settings	7 days ago	1 hour	
 Access reports Access analyzer Archive rules 	Permissions Trust relationships Tag	s Access Advisor Revoke sessions	
Analyzers			
Settings	Permissions policies (1)	2 Simulat	Remove Add permissions 🔻
Credential report	You can attach up to 10 managed policies.		
Organization activity	Q Filter policies by property or policy name and	l press enter	< 1 > 🔘
Service control policies (SCPs)			
	Policy name C*	▽ Туре	▽ Description
Related consoles	□	Customer managed	

2. Wählen Sie in der IAM-Policy Simulator-KonsoleExisting PoliciesalsModus aus.

IAM Policy Simulator	Mode : Existing Policies -	assumed- role/AWSReservedSSO_ITManagedOwnerAccess_cb7438e0bc5b							
			Existing Policies		/subhojitg -				
Users, Groups, and Roles	Policy Simulator		New Policy						
Users V Filter	Select service Select a	Select All	Deselect All	Reset Contexts	Clear Results	Run Simulation			
There are no users associated with this account.	Global Settings General Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]								
Service Action			Resource Type	Simulation Resource	Permission				

3. Wählen Sie auf der Registerkarte **Benutzer, Gruppen und Rollen** die Option **Rollen** aus dem Dropdownmenü aus und wählen Sie eine vorhandene Rolle aus.

IAM Policy Simulator Mode : Existing Policies -				s •			2			
	Users, Groups, and Roles Policy Simulator						_			
	Roles V Filter	Select service -	Select actions	*	Select All	Deselect All		Reset Contexts	Clear Results	Run Simulation
	ADC IAMBole	► Global Settings ①								
	aws-controltower-AdministratorExecuti	Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]								
	aws-controltower-ConfigRecorderRole	Service	Act	ion		Resource Type	Simula	tion Resource	Permission	
	aws-controltower-ForwardSnsNotificati									

4. Nachdem Sie die vorhandene Rolle ausgewählt haben, wählen Sie die darunter befindliche Richtlinie aus.

IAM Policy Simulator			Mode : Existing Policies	•				
Policies Back Create New Policy	Policy Simulato	r						
Selected role: ADC_IAMRole	Select service 🔻	Select actions 🔹	Select All Deselect All	Reset Contexts	Clear Results Run Simulation			
AWS Organizations SCPs	Global Settings ①							
Service control policies (SCPs) applied to your account can impact your access to AWS services.	Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]							
Learn more.	Service	Action	Resource Type	Simulation Resource	Permission			
IAM Policies								
Filter								
backend_autoscaling_policy								
Custom IAM Policies								
There are no policies to display!								
Permissions Boundary Policy								
You can simulate a maximum of one permissions boundary policy per user or role.								
There are no policies to display!								

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.

Policies Back	Policy Simulator					
Editing policy: backend_autoscaling_policy	Amazon EC2 A 💌	Select actions 🔹	Select All Deselect All	Reset 0	Contexts Clear Results	Run Simulatio
<pre>Editing policy: backend_autoscaling_policy { 'Version': '2012-10-17', 'Statement': [{ 'Statement': /Ailow', 'Action': [</pre>	Global Settings Action Settings and Service	Attachinstances Attachinstances BatchPutSchaduledUp CreateLanchConfigur DeleteTags DescribeAutoScalingGr PutNottificationConfigur RecordLifecycleAction SetInstanceProtection	AttachLoadBalancerTar CancelInstanceRefresh CreateOrUpdateTags DeleteNotIficationConfi DeleteNotIficationConfi DeleteNotIficationConfi DescribeAutoScalingIn DescribeAutoScalingIn DescribeAutoScalingProces DescribeScalingProces DescribeWarmPool DisableMetricScOlection ExitStandby PutScalingPoley ResumeProcesses StartInstanceRefresh	AttachLoadBalancers CompleteLifecycleAction DeleteAutoScalingGroup DeletePolicy DescribeActoScalingGroup DescribeActoScalingGroup DescribeActoScalingGroup DescribeActoScalingGroup DescribeActoScalingGroup DescribeActoScalingGroup DetachInstances EnableMetricsCollection GetPredictiveScalingFo PutScheduledUpdateG SetDesiredCapacity SuspendProcesses	BatchDeleteScheduled CreateAutoScalingGroup DeleteScheduled CreateAutoScalingGroup DeleteScheduledAction DescribeAduletAction DescribeAd	

6. Klicken Sie auf **Simulation ausführen**.

Policies	Policy Simulator					
Editing policy: backend_autoscaling_policy	Amazon EC2 A 🔻 61 Actio	on(s) sel Select All	Deselect All	Reset Contexts	Clear Results Run Simulation	
{ "Version": "2012-10-17", "Statement": [Global Settings ① Action Settings and Result 	Its [61 actions selected. 0 actions	not simulated. 61 action	ns allowed. 0 actions denied.]		
{ "Sid": "VisualEditor0",	Service	Action	Resource Type	Simulation Resource	Permission	
"Effect": "Allow", "Action": [Amazon EC2 Auto Scaling	AttachInstances	autoScalingGroup	•	allowed 1 matching statements.	
"ec2:DescribeInstances",	Amazon EC2 Auto Scaling	AttachLoadBalancerTargetGr	autoScalingGroup		allowed 1 matching statements.	
"autoscaling:"", "sns:CreateTopic",	Amazon EC2 Auto Scaling	AttachLoadBalancers	autoScalingGroup	•	allowed 1 matching statements.	
"sns:DeleteTopic", "sns:ListTopics",	Amazon EC2 Auto Scaling	BatchDeleteScheduledAction	autoScalingGroup	•	allowed 1 matching statements.	
"sns:Subscribe", "sqs:CreateQueue",	Amazon EC2 Auto Scaling	BatchPutScheduledUpdateG	autoScalingGroup	•	allowed 1 matching statements.	
"sqs:ListQueues", "sqs:DeleteMessage",	Amazon EC2 Auto Scaling	CancelInstanceRefresh	autoScalingGroup	•	allowed 1 matching statements.	
"sqs:GetQueueAttributes",	Amazon EC2 Auto Scaling	CompleteLifecycleAction	autoScalingGroup	•	allowed 1 matching statements.	
"iam:SimulatePrincipalPolicy",	Amazon EC2 Auto Scaling	CreateAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.	
],	Amazon EC2 Auto Scaling	CreateLaunchConfiguration	launchConfiguration	•	allowed 1 matching statements.	
"Resource": "*" }	Amazon EC2 Auto Scaling	CreateOrUpdateTags	autoScalingGroup	•	allowed 1 matching statements.	
))	Amazon EC2 Auto Scaling	DeleteAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.	
	Amazon EC2 Auto Scaling	DeleteLaunchConfiguration	launchConfiguration		allowed 1 matching statements.	
	Amazon EC2 Auto Scaling	DeleteLifecycleHook	autoScalingGroup		allowed 1 matching statements.	
	Amazon EC2 Auto Scaling	DeleteNotificationConfiguration	autoScalingGroup		allowed 1 matching statements.	

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

April 1, 2025

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 oder mehrere Subnetze f
 ür 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 f
 ür 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.

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

- 2. 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

April 1, 2025

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	Eine öffentliche IP-Adresse und
	Management-Datenverkehrs (NSIP)	eine private IP-Adresse
eth1	Dient clientseitigem Datenverkehr (VIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth2	Kommuniziert mit	Eine öffentliche IP-Adresse
	Back-End-Servern (SNIP)	(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 Inhalts**bereitstellung > 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 10.0.0/16 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.

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

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.

Create Subnet					×
Use the CIDR format to spec netmask and /28 netmask. A	cify your subnet's IP address bloc Ilso, note that a subnet can be th	ck (e.g., 10.0.0.0/2 e same size as yo	4). Note that block sizes must ur VPC. An IPv6 CIDR block m	be between a /1 hust be a /64 CID	6 R block.
Name tag	NSDoc-client	0			
VPC	vpc-ac9ad2c5 NSDoc 💠 🕄)			
VPC CIDRs	CIDR	Status	Status Reason		
	10.0.0/16	associated			
Availability Zone	ap-south-1a				
IPv4 CIDR block	10.0.1.0/24	0			
			(Cancel Yes,	Create

3. Wiederholen Sie die Schritte, um ein weiteres Subnetz für Back-End-Server zu erstellen.

Create Subnet					×
Use the CIDR format to spec netmask and /28 netmask. A	ify your subnet's IP address Iso, note that a subnet can b	block (e.g., 10.0.0 be the same size as	.0/24). Note th s your VPC. Ar	at block sizes must be betw IPv6 CIDR block must be a	veen a /16 a /64 CIDR block.
Name tag	NSDoc-server		0		
VPC	vpc-ac9ad2c5 NSDoc \$	0			
VPC CIDRs	CIDR	Status	St	atus Reason	
	10.0.0/16	associated			
Availability Zone	No Preference 🛟 🛈				
IPv4 CIDR block	10.0.2.0/24		0		
				Cancel	Yes, Create

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**.

Create Route Table							
A route table specifies how p and your VPN connection.	packets are forwarded between the subnets	within your VPC, the Internet,					
Name tag VPC	0						
		Cancel 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.

	rtb-4329082a NSDoc-internet-traffic										
Summar	y Routes	Subne	et Association	Route	Propagation	Tags					
Cancel	Save										
Associate	Subnet		IPv4 CIDR	IPv6 CIDR	Current Route	Table					
	subnet-c4ce9aad	NSDoc-MGMT	10.0.0/24	-	rtb-735a7b1a						
	subnet-31ce9a58	NSDoc-client	10.0.1.0/24	-	Main						
	subnet-d0cd99b9	NSDoc-server	10.0.2.0/24	-	Main						

- 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**.

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

10. 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.
- 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

Services - Resource	Groups	* *						⊈ nirm	alanaj @ nirmalanaj ~	Mumbai 🛩	Support •
1. Choose AMI 2. Choose Instance Type	3. Co	onfigure Instance 4. Add Storage	5. Add Tags (. Config	jure Security Group	7. Review					
Step 3: Configure Instance Details											
more.	ornorna.	rou carriadron manipie metanoea	nom are same ran,	reques	n opor matarioso te	rane advartage	or the lower pr	ionig, assign	an access manageme		instance, and
Number of instances		1	Launch into Auto §	caling	Group (1)						
	U.										- 1
Purchasing option	()	Request Spot instances									- 1
Network					Create new VD	<u>,</u>					
	U.	vpc-acead2c5 NSDoc			Create new vPC						
Subnet	1	subnet-c4ce9aad NSDoc-MGMT 251 IP Addresses available	ap-south-1a	0	Create new sub	net					
Auto-assign Public IP		Enable		•							- 1
Placement group		No placement group									
- Flacement group	U	No precentent group									
IAM role	(i)	None		C Create new IAM role							
				_							- 1
Shutdown behavior		Stop		0							
Enable termination protection		Protect against accidental ter	mination								
Monitoring	(i)	Enable CloudWatch detailed	monitoring								
	-	Additional charges apply.									
EBS-optimized instance		Launch as EBS-optimized ins	stance	_							
Tenancy		Shared - Run a shared hardware inst Additional charges will apply for	ance	0							
		reading on all do will apply to	council terrarioy.								
							Cancel	Previous	Beview and Laun	ch Next	Add Storage
							Gander	revious	Line reaction and Cault	Next	Had otorage

- 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**.

Select an existing key pair or create a new key pair	×
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is requir to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you securely SSH into your instance.	ed u to
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.)
Choose an existing key pair	
Select a key pair	
NSDOCKeypair	
I acknowledge that I have access to the selected private key file (NSDOCKeypair.pem), and	
that without this file, I won't be able to log into my instance.	
Cancel Launch Instances	8

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**.

Create Netwo	ork l	nterface		×
Description	(j)	NSDoc-VIP-NIC		
Subnet	(j)	subnet-31ce9a58 ap-south-1a NSDoc-client		
Private IP	(j)	auto assign		
Security groups	(i)	sg-05e3186d - NetScaler VPX - Customer Licensed-12-0-41-23-Auto sg-d2946fba - default - default VPC security group		
			Cancel	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**.

	Name	Network Interna	Subnet ID	VPCID	Zone	Ť	Security groups		
	NSDoc-VIP	eni-3c843657	subnet-31ce9a	vpc-ac9ad2c5	ap-south-1	а	default		
	NSDoc-SNIP	eni-3e8b3955	subnet-d0cd99	vpc-ac9ad2c5	ap-south-1	а	default		
		eni-dd1cacb6	subnet-9d43f6f4	vpc-52ab033b	ap-south-1	а	FreeBSD 11-11-0-R		
	NSDoc-NSIP	eni-878133ec	subnet-c4ce9aad	vpc-ac9ad2c5	ap-south-1	а	NetScaler VPX - Cu		
		eni-2da8a261	subnet-fe6882h3	vpc-52ab033b	an-south-1	h			
		eni-e0f9128b	Attach Network Interface						
		eni-0e55e565							
		eni-1fa9ef53	Network Interfa	ace: eni-3e8b3	955				
		eni-23ff4a48	Instance	ID: i-0296946	19cd5b71ec - NSI	Doc-VM	(running)		
		eni-45fb4e2e							
		eni-76f84d1d							
		eni-72ff183d				Cance	Attach		
0									

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**.

Associate address		
Select the instance OR network interface to	which you want to associate this Elastic	IP address (13.126.158.205)
Resource type	Instance	
	 Network interface 	
Network interface	eni-878133ec	- C
Private IP	Q Filter by attributes	C 0
Reassociation	eni-0e55e565 eni-dd1cacb6 eni-76f84d1d	tached 🚯
Warning If you associate an Elastic IP ad	eni-72ff183d eni-878133ec NSDoc-NSI eni-23ff4a48 eni-1509ef53	ress is released. Learn more.
* Required	eni-2da8a261	Cancel Associate

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

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 unterhttps://support.citrix.com/s/article/CTX2559 59-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US

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.

 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.

Velcome to	
Backup and	Restore
he backup and restore sed to restore the Citrix	unctionality of the Citrix ADC appliance allows you to create a backup file of the Citrix ADC configurations. This file can later be ADC configurations to the previous state.
o create a backup, click	the "Backup" link shown below. When required, select one of the backups and restore the appliance.

- c) Geben Sie auf der Seite "Backup/Import "die folgenden Details ein:
 - Name Name der Sicherungsdatei.
 - Level Wählen Sie die Backup-Level als Fullaus.
 - Kommentar Geben Sie eine kurze Beschreibung des Backup an.

Backup/Imp	ort
 Orresta 	
Create	
Citrix ADC Ver	sion 50.19.nc. Date: Sep 25 2023. 21:28:29 (64-bit)
File Name	
fullbacku	p
l evel*	
Full	\sim (i)
Comment	
None	
Backup	Cancel
Васкир	Cancer

System > Backup and Restore > Backup/Import

d) Klicken Sie auf **Backup**. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf Ihren lokalen Computer herunterladen.

System > Backup and Restore				
Backup and Resto	ore 🕕			
Backup/Import Delete	✓ Select Action Download	= Download		
${\sf Q}$ Click here to search or you can ϵ	Restore	at		()
FILE NAME	LEVEL	CREATED BY	CREATION TIME	♦ SIZE (IN KB)
fullbackup.tgz	Full	nsroot	Wed Oct 4 15:01:42 2023	2117 KB
Total 1			25 Per Page	✓ Page 1 of 1 < ▶

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.

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

Backup/Import	
Create Import	
File Name*	_
Choose File 🗸	🚺 🌗 Please choose file
Local	-
Appliance Cancel	

- d) Wählen Sie die Datei aus.
- e) Wählen Sie im Dropdownmenü Aktion auswählen die Option Wiederherstellen aus.

System > Ba	ackup and Restore								
Backup	and Resto	ore	D						
Backup/Im	port Delete	✓ Select Down Rest	ct Action nload pre	Resto	bre				()
	FILE NAME		LEVEL		CREATED BY	CREATION TIME		SIZE (IN KB)) \$
	fullbackup.tgz		Full		nsroot	Wed Oct 4 15:01:42 203	23	2117 KB	
Total 1						25 Pe	er Page 🗸 Pag	ge 1 of 1	•

f) Überprüfen Sie auf der Seite **Wiederherstellen** die Dateidetails und klicken Sie auf **Wiederherstellen**.

← Restore

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

- g) 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-Portalsowohl 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 > Anhängenklicken. Geben Sie den Namen der EC2-Instanz ein, an den die Netzwerkschnittstelle angeschlossen werden muss.

New EC2 Experience Tell us what you think	Network interfaces (1/1			
EC2 Dashboard New				
Events				
Tags		Attach network interface	×	
Limits				
▼ Instances		Network interface		
Instances New		eni-0432953739657651e		
Instance Types		Instance		
Launch Templates		Choose an instance	•	
Spot Requests				
Savings Plans			Cancel Attach	
Reserved Instances New				
Dedicated Hosts				
Scheduled Instances				
Capacity Reservations				

- 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 3vermerkt sind.
- h) Aktivieren Sie das Kontrollkästchen Neuzuweisung sekundärer privater IP-Adressen zulassen.
- i) Klicken Sie auf **Speichern**.

aws	Services 🔻 🔍 🔍	Search for services, featu	ures, marketplace products, and docs	[Alt+S]	
	IPv4 addresses				
	Private IP address	Public IP address			
	192.168.1.180	3.209.165.4	Unassign		
	192.168.1.121		Undo		
	192.168.1.243		Undo		
	Assign new IP address	5			
	 Allow secondary private II Allows you to reassign a privat instance or network interface. 	Pv4 addresses to be reassi te IPv4 address that is assigne	gned d to this network interface to another		
				Control	Course

- 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 f
 ür die Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse f
 ür Sie ausw
 ählen 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 Instanzbeschreibungwerden 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:

Konfigurieren Sie als Nächstes VIP und SNIP.

Geben Sie für VIP Folgendes ein:

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

Geben Sie für SNIP Folgendes ein:

1 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:

1 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:

```
1 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:

```
1 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 HAFailover 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 Kundenlizenziertaus.
- 6. Klicken Sie auf Weiter, um zu abonnieren.
- 7. Überprüfen Sie die Details auf der Seite **Abonnieren** und klicken Sie **auf Configuration fort-setzen**.
- 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.

Step 2 Specify stack details Prerequisite - Prepare template Step 3 Configure stack options Prepare template Step 4 Review Template is ready Use a sample template Step 4 Review Specify template Is a JSON or VAML file that describes your stack's resources and properties. Template is a JSON or VAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Upload a template file Amazon S3 URL Upload a template file Amazon S3 URL thttps://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-454	1 cify template	Create stack
Step 3 Configure stack options Prepare template Every stack is based on a template. A template is a JSON or VAML file that contains configuration information about the AWS resources you want to include in the Step 4 Review Image: Create template is ready Use a sample template Create template in Designer Step 4 Review Specify template Template is a JSON or VAML file that describes your stack's resources and properties. Template is a JSON or VAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Image: Upload a template file Amazon S3 URL Upload a template file Amazon S3 URL that the the template-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-455	2 cify stack details	Prerequisite - Prepare template
Configure stack options • Template is ready • Use a sample template • Create template in Designer • Create template • Create template in Designer • Create template • Create template • Cre	3	Prepare template Every stack is based on a template. A template is a JSON or VAML file that contains configuration information about the AWS resources you want to include in the stack.
Step 4 Review Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL Amazon S3 URL Inttps://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-455	figure stack options	Template is ready Use a sample template Create template in Designer
Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. • Amazon S3 URL • Amazon S3 URL • Amazon S3 URL • Intps://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-455	4	
Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL Upload a template file Amazon S3 URL Inttps://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-455	ew	
Amazon S3 URL Upload a template file Amazon S3 URL https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-455 temps 67 centre UP	ew	Specify template A template is a JSON or YAML file that describes your stack's resources and properties.
Amazon S3 URL https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-45	ew	Specify template A template is a JSON or VAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon 53 URL where it will be stored.
https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-45	ew	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL
Amount C7 terrolate UDI	ew	Specify template A template is a JSON or VAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL Amazon S3 URL
Amazon SS template URL	ew	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Amazon S3 URL Upload a template file Amazon S3 URL https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-45b4-8bb

- 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 Instanztypaus.
 - 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 Jaeingestellt. Wenn Sie diese Option deaktivieren möchten, wählen Sie Neinaus.

Weitere Informationen zu CloudWatch-Metriken finden Sie unter [Überwachen Sie Ihre Instanzen mit Amazon CloudWatch] (#monitor-your-instances-using-amazoncloudWatch).

- Führen Sie unter **Optionale Konfiguration**Folgendes aus:
 - Standardmäßig lautet die: Soll den Verwaltungsschnittstellen eine öffentliche IP (EIP) zugewiesen werden? Option ist auf Neineingestellt.
 - Standardmäßig lautet die Adresse . Soll der Clientschnittstelle eine öffentliche IP (EIP) zugewiesen werden? Option ist auf Neineingestellt.

Step 1 Specify template	Specify stack details
Step 2 Specify stack details	Stack name
	Stack name
Step 3	Enter a stack name
Configure stack options	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Step 4	
Review	Parameters Parameters are defined in your template and allow you to input custom values when you create or update a stack.
	Network Configuration
	VPC ID to deploy the resources
	· · · · · · · · · · · · · · · · · · ·
	Address range to access Management interfaces via SSH, HTTP; HTTPS ports Must be a valid IP CDR range of the form xxxxx/x
	Subnet ID associated with Primary and Secondary ADCs Management interface
	Subnet ID associated with Primary and Secondary ADCs Client interface (Traffic coming from `client` to the `ADC VIP`)
	Subnet ID associated with Primary and Secondary ADCs Client Interface (Traffic leaving from the 'ADC SNIP' to the 'backend')
	V0/Tensor:
	default
	Versions T
	Citrix ADC Configuration
	m5.xlaroe
	Keypair to associate to ADCs
	Publish custom metrics to CloudWatch?
	Yes
	Optional Configuration Should PublicIP(EIP) be assigned to management interfaces? If not specified, the private jo will be auto assigned
	No
	Should PubliciP(EIP) be assigned to client interface?

- 14. Klicken Sie auf **Weiter**.
- 15. Die Seite **Stack-Optionen konfigurieren** wird angezeigt. Dies ist eine optionale Seite.

aws Services V										
Step 1 Specify template	Configure stack options									
Step 2 Specify stack details	Tags You can specify tags (Rey-value pairs) to report to resources in your stack. You can add up to 50 unique tags for each stack. Learn more [
Step 3 Configure stack options	Kay Value R									
Step 4 Review	m 0 V e									
	Add tag									
	Permissions Choose an UM role to explicitly define hew Cloudformation can create, modify, or delete resources in the stack. If you don't choose a role, Cloudformation uses permissions based on your user credentials. Learn more 🔁									
	IAM role - optional Observed for Claudformation to use for all operations performed on the stack.									
	Advanced options									
	You can set additional options for your stack, like notification options and a stack policy. Learn more C									
	Rollback configuration Specify slaves for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. Laarn more									
	Notification options									
	Stack creation options									
	Cancel Previous Next									

- 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.

C Stacks (1)	© × < 1 >	Stack info Events 1 Events (38)	Resources	Outputs Parameters	Delete Template Change sets	Update Stack actions V
2020-10-28 13:42:49 UTC+0530 CREATE_COMPLETE	0	Q. Search events				
		Timestamp		Logical ID	Status	Status reason
		2020-10-28 13:45:59 UTC+053	0		CREATE_COMPLETE	
		2020-10-28 13:45:56 UTC+053	0	SecondaryInstance	O CREATE_COMPLETE	
		2020-10-28 13:45:39 UTC+053	0	SecondaryInstance	CREATE_IN_PROGRESS	Resource creation Initiated
		2020-10-28 13:45:37 UTC+053	0	SecondaryInstance	CREATE_IN_PROGRESS	
		2020-10-28 13:45:34 UTC+053	0	PrimaryInstance	CREATE_COMPLETE	
		2020-10-28 13:45:18 UTC+053	0	PrimaryInstance	CREATE_IN_PROGRESS	Resource creation Initiated
		2020-10-28 13:45:15 UTC+053	0	PrimaryInstance	CREATE_IN_PROGRESS	
		2020-10-28 13:45:13 UTC+053	0		CREATE_COMPLETE	
		2020-10-28 13:43:22 UTC+053	0	PrimaryManagementENI	CREATE_COMPLETE	

- 21. 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 Benutzernamennsroot 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.

Nodes	5 2											
Add	Edit	Delete	Statist	tics	Select Actio	n V	·					
	ID	÷ IP A	DDRESS		HOST NAME		MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE		SYNCHRONIZAT
	0						Primary	• UP	DISABLED	ENABLED		-NA-
	1						Secondary	• UP	DISABLED	SUCCESS		-NA-
Total 2											2	5 Per Page 🗸 🗸

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.

testfarhan-PrimaryInstance	i-0bb6e330c2b51d145	⊘ Running @@	⊇ m5.xlarge	 Initializing 	No alarms	us-east-1b	-
testfarhan-SecondaryInstance	i-02ad0511c02899312	⊘ Running @ €	ට, m5.xlarge	⊘ 2/2 checks …	No alarms	us-east-1b	-
nce: i-0bb6e330c2b51d145 (testfarhan-Primar	yInstance)	-					
etails Security Networking Storag	ge Status Checks Mor	atoring Tag	IS				
				Add to dashboard 1h	3h 12h 10	d 3d 1w custom	. 2 💶
CPU utilization (%) Percent 27 15.5 0 07:30 07:45 08:00 08:15 08:30	Status check failed (any Count 0.5 0 07:30 07:45 08:00	08:15 08:30	Status check Count 1 0.5 0 07:30 07:4	failed (instance) (cou 15 08:00 08:15 08:30	Status c Count 1 0.5 0 07:30	heck failed (syst	em) (count) 08:15 08:30
i-Obb6e330c2b51d145 (testfarhan-PrimaryInstar	i-Obb6e330c2b51d145 (testfarf	an-PrimaryInstar	i-0bb6e330c2b5	1d145 (testfarhan-PrimaryInstar	i-Obb6e	330c2b51d145 (testfarh	an-PrimaryInstar
Network in (bytes)	Network out (bytes)		Network pack	(count)	Networ	k packets out (co	unt)
Bytes	Bytes		Count		Count		
150k	2044		473		478		-

5. Klicken Sie unter Alle Metriken auf Ihre Instanz-ID.

All metrics	Graphed metrics	Graph options	Source
All >	<i-01c50c91dd353< td=""><td>7d7a> Q Search</td><td>for any metric</td></i-01c50c91dd353<>	7d7a> Q Search	for any metric
5 Metrics			
CPU			
2 Metrics			
Throughp	put		
2 Metrics			

- 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-

Untitled g	raph 🖉				1h 3h	12h 1d	3d	1w custom (2	2w) -	Line	- A	ctions *	3.	0
Percent														
3.7														
2.32														
0.933 04/2	26 04/27 04/28	04/29	04/30	05/01	05/02	05/0	03	05/04	05/05	05/06	05/07	05/08	05/09	
Managem	ent CPU usage 📒 Packet CPU us	age												
All metrics	All metrics Graphed metrics (2) Graph options Source													
O Add a math expression O Statistic: Average v Period: 5 Minutes v Remove all														
•	Label		Details						Sta	atistic	Period	Y Axis	Actio	ns
	Management CPU usage			<-0630alled	eldial3ca	• Mana	igemer	nt CPU usage •.	Ave	erage	5 Minutes	< >	46	0
 Image: Image: Ima	Packet CPU usage			<-0130aled	e4d4a43ca>	Pack	et CPL	usage • CPU:.	Ave	erage	5 Minutes	< >	∆ 4	0

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 <server_type&#062; vserver &#060;vserver_name&#062;
<protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -
ipset \\<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 Benutzernamensroot 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.

Load Balancing Virtual Server Export as a Template

Basic Settings									
Name Protocol State IP Address Port Traffic Domain	vserver1 HTTP DOWN 192.168.2.129 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster	- NONE IP 1 ipset123 PASSIVE ENABLED NO						

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



Before failover

After failover

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.

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

5. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären.

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

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:

```
1
     {
2
          "Version": "2012-10-17",
3
          "Statement": [
4
5
              {
6
7
                  "Action": [
                       "ec2:DescribeInstances",
8
                       "ec2:DescribeAddresses",
9
                       "ec2:AssociateAddress",
10
                       "ec2:DisassociateAddress",
11
12
                       "ec2:DescribeRouteTables",
                       "ec2:DeleteRoute",
13
                       "ec2:CreateRoute",
14
                       "ec2:ModifyNetworkInterfaceAttribute",
                       "iam:SimulatePrincipalPolicy",
16
                       "iam:GetRole"
17
18
                  ],
                  "Resource": "*",
19
                  "Effect": "Allow"
20
               }
21
22
23
         ]
      }
24
```

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:

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

Route Tables > Edit routes

Edit routes

Destination	Target		
192.168.0.0/16	local		
0.0.0/0	igw-0b6da15e72de5729e 🔹		
10.10.10.0/24	eni-09ad18f01f854b8ab 🗸		
5500/16	ani 00ad19f01f95/b8ab		

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 Benutzernamensroot und Instanz-ID als Kennwort an.
- 3. Navigieren Sie zu Konfiguration > System > Hochverfügbarkeitund 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.

G Load Balancing Virtual Server

Load Balancing Virtual Server Export as a Template										
Basic Settings										
Name Protocol State IP Address Port Traffic Domain	My LB HTTP • UP 10.10.10 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- NONE IP 1 - PASSIVE ENABLED NO							
Services and Service Groups										
1 Load Balan	ing Virtual Server Service Binding									

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",
4
           "Statement": [
5
               {
6
                    "Sid": "VisualEditor0",
7
                    "Effect": "Allow",
8
                    "Action": [
9
10
                         "ec2:CreateRoute",
                        "ec2:DeleteRoute",
11
                        "ec2:DescribeRouteTables"
12
                    ],
13
                    "Resource": "*"
14
15
                }
16
           ]
17
18
        }
```

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 Roleaus.
- 3. Wählen Sie ein anderes AWS-Konto.

 Create role

 Select type of trusted entity

 Image: Provide and others

 Image: Provide and others

 Image: Provide and other

 Image: Provide

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.

Q Search Menu		AWS						
Favorites	\sim	Configuration Summary	Configure Cloud Parameters					
AWS	~	No Cloud Profile	Change Cloud Parameters					
Cloud Profile								
System	>							
AppExpert	>							

2. Geben Sie auf der Seite **AWS-Cloud-Parameter konfigurieren** den Wert für das Feld **RoleARN** ein.

← Configure AWS Cloud Parameters

r	neo.rolearn		
	errtfvf		

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:

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.

TRANSIT	<	,								
GATEWAYS	Transit Gat	Transit Gateway Route Table: fow-rfb-09/12ca61473654a7								
Transit Gateways										
Transit Gateway	Details	Associations	Propagations	Prefix list references	Routes	Tags				
Attachments										
Transit Gateway	The table	e below will return	a maximum of 100	0 routes. Narrow the filter	or use expor	rt routes to view more routes.				
Route Tables	Create	static route								
Transit Gateway	<u></u>									
Multicast	Q Filt	I< < 1 to 3 of 3 > >I								

4. Erstellen Sie eine statische Route, bei der CIDR auf Ihr privates VIPS-Subnetz und die Anschlusspunkte auf die VPC mit NetScaler VPX verweist.

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

5. Klicken Sie auf Statische Route erstellenund 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 Netzwerkund 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.
- 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.

- 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:
 - 1 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.

3. Fügen Sie Richtlinien zum Umschreiben für die Umschreibaktionen hinzu.

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

4. 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 GracefulTimeout 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/use rguide/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:

```
{
1
2
3
           "Version": "2012-10-17",
4
           "Statement": \[
5
            {
6
                   "Action": \[
7
                       "ec2:DescribeInstances",
8
9
                        "ec2:DescribeNetworkInterfaces",
10
                        "ec2:DetachNetworkInterface",
                       "ec2:AttachNetworkInterface",
11
                       "ec2:StartInstances",
12
13
                        "ec2:StopInstances",
                        "ec2:RebootInstances",
14
15
                        "autoscaling:\*",
                        "sns:\*",
16
```

17				"sqs:*"
18				
19				"iam: SimulatePrincipalPolicy"
20				"iam: GetRole "
21				\],
22				"Resource": "*",
23				"Effect": "Allow"
24			}	
25				
26	١	\]		
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 nsrootbei der VPX-Instanz an.
- Navigieren Sie zu System > AWS > Cloud-Profil und klicken Sie auf Hinzufügen.
 Die Konfigurationsseite " Cloud-Profil erstellen "wird angezeigt.

← Create Cloud Profile

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

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.

Q Search Menu		AWS > Cloud Profile									
Favorites	~ (Cloud Profile 1									
AWS	~	Add Edit Delete									
Cloud Profile		Q Click here to search or you can enter Key : Value format									
System	>		NAME \$	AUTO SCALE GROUP	LOAD BALANCING VIRTUAL SERVER	AUTO SCALE GROUP PF	ROTOCOL 🔅	GRACEFUL			
AppExpert	>		test-cloudprofile	_test-script_80	_CP_test-cloudprofile_192.168.2.53_LB_	HTTP		NO			
Traffic Management	>	Total 1				25 Per Page 🗸 Pa	age 1 of 1				
Optimization	>										

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

April 1, 2025

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.

- Melden Sie sich bei derAWS-Benutzergruppean und navigieren Sie zuEC2 > NETWORK & SE-CURITY > 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 derAWS-Benutzergruppean und navigieren Sie zuEC2 > 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-Benutzergruppean 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.

```
    Melden Sie sich bei der**AWS-Benutzergruppe**an und navigieren Sie
zu**EC2 > NETWORK & SECURITY > Elastic IPs**.
    Klicken Sie auf**Neue Adresse**zuweisen, um eine elastische IP-
Adresse zu erstellen.
    Konfigurieren Sie die Elastic IP so, dass sie auf den Benutzer
verweist, der die NetScaler-Instanz in AWS ausführt.
    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-Benutzergruppean und navigieren Sie zuEC2 > LOAD BAL-ANCING > 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 f
 ür die Verarbeitung einer Client-Anfrage auswählt und die IP-Adresse des ausgewählten Rechenzentrums f
 ür alle nachfolgenden DNS-Anfragen weiterleitet. Wenn die konfigurierte Persistenz f
 ür eine Site gilt, die DOWN ist, verwendet der GSLB-Knoten eine GSLB-Methode, um eine neue Site auszuwählen, und die neue Site wird f
 ür 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 drei oben genannten 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 unter<u>Erste Schritte</u>

- 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 Style-Book, 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 zuAnwendungen > 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 zum Bereitstellen von NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen von NetScaler VPX-Instanzen auf AWS.

Informationen zum Konfigurieren von GSLB mit StyleBooks finden Sie unter Verwenden von Style-Books 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.

Stellen Sie NetScaler Web App Firewall auf AWS bereit

October 17, 2024

Die NetScaler Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Kundenservern und Kundenbenutzern installiert werden, normalerweise hinter dem Router oder der Firewall des Kundenunternehmens. NetScaler Web App Firewall muss an einem Ort installiert werden, an dem sie den Datenverkehr zwischen den Webservern und dem Hub oder Switch abfangen kann, über den Benutzer auf diese Webserver zugreifen. Die Benutzer konfigurieren das Netzwerk dann so, dass Anforderungen an die Web Application Firewall anstatt direkt an ihre Webserver und Antworten an die Web Application Firewall anstatt direkt an ihre Benutzer gesendet werden. Die Web Application Firewall filtert diesen Datenverkehr, bevor sie ihn an sein endgültiges Ziel weiterleitet. Dabei werden sowohl der interne Regelsatz als auch die Benutzerergänzungen und -änderungen verwendet. Es blockiert oder macht alle Aktivitäten unschädlich, die es als schädlich erkennt, und leitet dann den verbleibenden Verkehr an den Webserver weiter. Das vorhergehende Bild bietet einen Überblick über den Filtervorgang.

Weitere Informationen finden Sie unter Funktionsweise der NetScaler Web App Firewall.

Architektur für NetScaler Web App Firewall auf AWS für die Produktionsbereitstellung

Das Bild zeigt eine Virtual Private Cloud (VPC) mit **Standardparametern**, die eine NetScaler Web App Firewall-Umgebung in der AWS-Cloud erstellt.



In einer Produktionsbereitstellung werden die folgenden Parameter für die NetScaler Web App Firewall-Umgebung eingerichtet:

- Diese Architektur setzt die Verwendung einer AWS CloudFormation-Vorlage voraus.
- Eine VPC, die sich über zwei Availability Zones erstreckt und gemäß den Best Practices von AWS mit zwei öffentlichen und vier privaten Subnetzen konfiguriert ist, um Ihnen Ihr eigenes virtuelles Netzwerk auf AWS mit einem /16 Classless Inter-Domain Routing (CIDR) -Block (ein Netzwerk mit 65.536 privaten IP-Adressen) zur Verfügung zu stellen.
- Zwei Instanzen der NetScaler Web App Firewall (primär und sekundär), eine in jeder Availability Zone.
- Drei Sicherheitsgruppen, eine für jede Netzwerkschnittstelle (Management, Client, Server), die als virtuelle Firewalls dienen, um den Datenverkehr für die zugehörigen Instanzen zu steuern.
- **Drei Subnetze**für jede Instanz eines für die Verwaltung, eines für den Client und eines für den Back-End-Server.
- Ein **Internet-Gateway**, das mit der VPC verbunden ist, und eine Routing-Tabelle für öffentliche Subnetze, die öffentlichen Subnetzen zugeordnet ist, um den Zugriff auf das Internet zu ermöglichen. Dieses Gateway wird vom Web App Firewall-Host zum Senden und Empfangen von Datenverkehr verwendet. Weitere Informationen zu Internet-Gateways finden Sie unter: Internet-Gateways.
- **5 Routing-Tabellen** eine öffentliche Routing-Tabelle, die den Client-Subnetzen der primären und sekundären Web App Firewall zugeordnet ist. Die verbleibenden 4 Routing-Tabellen sind

mit jedem der 4 privaten Subnetze verknüpft (Management- und serverseitige Subnetze der primären und sekundären Web App Firewall). *

- AWS Lambda in Web App Firewall kümmert sich um Folgendes:
 - Konfiguration von zwei Web App Firewall in jeder Verfügbarkeitszone des HA-Modus
 - Ein Beispiel f
 ür ein Web App Firewall-Profil erstellen und diese Konfiguration somit in Bezug auf die Web App Firewall
 übertragen
- In den öffentlichen Subnetzen zwei verwaltete Network Address Translation (NAT) -Gateways, um ausgehenden Internetzugriff für Ressourcen in öffentlichen Subnetzen zu ermöglichen.

Hinweis:

Die CFT Web App Firewall-Vorlage, die die NetScaler Web App Firewall in einer vorhandenen VPC bereitstellt, überspringt die mit Sternchen markierten Komponenten und fordert Benutzer zur Eingabe ihrer vorhandenen VPC-Konfiguration auf.

Backend-Server werden von der CFT nicht bereitgestellt.

Kosten und Lizenzierung

Die Benutzer sind für die Kosten der AWS-Services verantwortlich, die bei der Ausführung von AWS-Bereitstellungen verwendet werden. Die AWS CloudFormation-Vorlagen, die für diese Bereitstellung verwendet werden können, enthalten Konfigurationsparameter, die Benutzer bei Bedarf anpassen können. Einige dieser Einstellungen, wie der Instance-Typ, wirken sich auf die Bereitstellungskosten aus. Kostenvoranschläge finden Sie auf den Preisseiten für jeden von ihnen verwendeten AWS-Service. Die Preise können sich ändern.

Für eine NetScaler Web App Firewall auf AWS ist eine Lizenz erforderlich. Um NetScaler Web App Firewall zu lizenzieren, müssen Benutzer den Lizenzschlüssel in einem S3-Bucket platzieren und seinen Speicherort angeben, wenn sie die Bereitstellung starten.

Hinweis:

Wenn Benutzer das Lizenzmodell Bring Your Own License (BYOL) wählen, sollten sie sicherstellen, dass sie eine AppFlow-Funktion aktiviert haben. Weitere Informationen zur BYOL-Lizenzierung finden Sie unter: AWS Marketplace/Citrix VPX– Kundenlizenziert.

Die folgenden Lizenzoptionen sind für die Citrix ADC Web App Firewall verfügbar, die auf AWS ausgeführt wird. Benutzer können ein AMI (Amazon Machine Image) basierend auf einem einzigen Faktor wie dem Durchsatz auswählen.

- **Lizenzmodell**: Pay as You Go (PAYG, für die Produktionslizenzen) oder Bring Your Own License (BYOL, für das vom Kunden lizenzierte AMI Citrix ADC Pooled Capacity). Weitere Informationen zur gepoolten Kapazität von Citrix ADC finden Sie unter: Citrix ADC Pooled Capacity.
 - Für BYOL gibt es 3 Lizenzierungsmodi:
 - * NetScaler Pool-Kapazität konfigurieren: Konfigurieren Sie die gepoolte Kapazität von Citrix ADC
 - * NetScaler VPX Check-in- und Checkout-Lizenzierung (CICO): Citrix ADC VPX Ein- und Auscheck-Lizenzierung

Tipp:

Wenn Benutzer die CICO-Lizenzierung mit den Anwendungsplattformtypen VPX-200, VPX-1000, VPX-3000, VPX-5000 oder VPX-8000 wählen, sollten sie sicherstellen, dass auf ihrem NetScaler Console-Lizenzserver dieselbe Durchsatzlizenz vorhanden ist.

* NetScaler virtuelle CPU-Lizenzierung: NetScaler virtuelle CPU-Lizenzierung

Hinweis:

Wenn Benutzer die Bandbreite einer VPX-Instanz dynamisch ändern möchten, sollten sie eine BYOL-Option wählen, z. B. **NetScaler Pool Capacity**, mit der sie die Lizenzen von der NetScaler Console aus zuweisen können, oder sie können die Lizenzen entsprechend der Mindest- und Maximalkapazität der Instanz bei Bedarf und ohne Neustart von NetScaler auschecken. Ein Neustart ist nur erforderlich, wenn Benutzer die Lizenzversion ändern möchten.

- Durchsatz: 200 MBit/s oder 1 GBit/s
- Paket: Premium

Bereitstellungsoption

Dieser Bereitstellungshandbuch bietet zwei Bereitstellungsoptionen:

- Die erste Option ist die Bereitstellung mithilfe eines Schnellstarthandbuchformats und der folgenden Optionen:
 - Stellen Sie NetScaler Web App Firewall in einer neuen VPC bereit (durchgängige Bereitstellung). Diese Option erstellt eine neue AWS-Umgebung, die aus der VPC, Subnetzen, Sicherheitsgruppen und anderen Infrastrukturkomponenten besteht, und stellt dann NetScaler Web App Firewall in dieser neuen VPC bereit.

- Stellen Sie NetScaler Web App Firewall in einer vorhandenen VPC bereit. Diese Option stellt die NetScaler Web App Firewall in der vorhandenen AWS-Infrastruktur des Benutzers bereit.
- Die zweite Option besteht darin, die Web App Firewall StyleBooks mithilfe der NetScaler Console bereitzustellen

AWS-Schnellstart

Schritt 1: Melden Sie sich beim AWS-Benutzerkonto an

- Melden Sie sich beim Benutzerkonto bei AWS: AWS mit einer IAM-Benutzerrolle (Identity and Access Management) an, die über die erforderlichen Berechtigungen verfügt, um ein Amazon-Konto (falls erforderlich) zu erstellen oder sich bei einem Amazon-Konto anzumelden.
- Verwenden Sie die Regionsauswahl in der Navigationsleiste, um die AWS-Region auszuwählen, in der Benutzer Hochverfügbarkeitszonen bereitstellen möchten.
- Stellen Sie sicher, dass das AWS-Benutzerkonto korrekt konfiguriert ist. Weitere Informationen finden Sie im Abschnitt Technische Anforderungen in diesem Dokument.

Schritt 2: Abonnieren Sie das NetScaler Web App Firewall AMI

- Für diese Bereitstellung ist ein Abonnement des AMI für NetScaler Web App Firewall im AWS Marketplace erforderlich.
- Melden Sie sich beim AWS-Benutzerkonto an.
- Öffnen Sie die Seite für das NetScaler Web App Firewall-Angebot, indem Sie einen der Links in der folgenden Tabelle auswählen.
 - Wenn Benutzer die Schnellstartanleitung zur Bereitstellung der NetScaler Web App Firewall in Schritt 3 unten starten, verwenden sie den NetScaler Web App Firewall Image-Parameter, um das Paket und die Durchsatzoption auszuwählen, die ihrem AMI-Abonnement entspricht. Die folgende Liste zeigt die AMI-Optionen und die entsprechenden Parametereinstellungen. Die VPX AMI-Instanz benötigt mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher.

Hinweis:

Informationen zum Abrufen der AMI-ID finden Sie auf der Seite NetScaler Products on AWS Marketplace auf GitHub: Citrix Products on AWS Marketplace.

AWS Marketplace AMI

- NetScaler Web Application Firewall (Web App Firewall) 200 MBit/s: Citrix Web App Firewall) 200 MBit/s
- NetScaler Web Application Firewall (Web App Firewall) 1000 MBit/s: Citrix Web App Firewall (Web App Firewall) –1000 MBit/s
- Wählen Sie auf der AMI-Seite Continue to Subscribe.

😭 aws m	arketplace	National and Marce	ion Mandan Antidaet	VacCoudiat		Bullets 6		Amore Mith Car	100.0
0	itrix	Citrix Web / By: Citrix Systems, Linux/Unix	App Firewall	(WAF) - 20 ier: 130-47.34 iews	0 Mbps		Continue to 1 Save to Typical Ter \$2.15 Tetral pricing are into herbit on mit darpp Verginal View Detail	Subscribe Lat al Price /hr excelfor services in US East (%	
	Overview	Pr	icing	Usage		Support		Reviews	
	Product Over the Web App Frewall (he and protections for m ublic facing assets, link reputation based brain interce authentication, so blicles. Using beth basis roundes comprehensive reactions time. By antern starmated learning med reclose time. By actem this WAF adapts to applications. Center WW F bodies, including PC implates, it has never b	BEVIEW WAP) is an enterprise g odem applications. Citio using websites, web ap- ing, Bot mitigation, OW 6 protection and mere- strong SSL/TLS ciphens, cas web as advanced W protection for your app protection for your app related dynamic profi etically learning how a application even as attent of ma- tedpa with comptions to 1.055, HIBNA, and mere- eren easier to get up am	rade salution offering is WAF mitigates the os, and APIs. Citrix W MSP Top 10 application APIs included are op TLS 1.3, rate limiting AP protections, Citris lications with unparts inclus. Further, using liling, Citris WAF save protected application ellopens deploy and a related or all major regulator is with our CloudForm d running quickly. With	e state of cats against AF includes ion threats forms to a and nowrite www/ clobed case an types weeks, doer the ry standards nation th auto	Highlights • Comprehensive App powerful ADC platfor cleut, physical, virtu enables comaintenry applications and we security frem Layer protection ensures y vulnerable. • Secure your Website applications is more Citris WW includes 1 reputation based fill	Security Cibic 1 m - a single co- al, bare-metal, across your hyt dr.Raws. Helioti to Layer 7 and ou don't have t s, Apps, and AP than just bails than just bails than just bails	WAF is based on the or base across and containers that old multi-cloud capplication of built-in-API a warry about being % Securing Waf-functionality. Annote WAF, IP pation,		

• Lesen Sie sich die Allgemeinen Geschäftsbedingungen für die Softwarenutzung durch und wählen Sie dann **Nutzungsbedingungen akzeptieren**.



Hinweis:

Benutzer erhalten eine Bestätigungsseite und eine E-Mail-Bestätigung wird an den Kontoinhaber gesendet. Detaillierte Anweisungen zum Abonnement finden Sie unter Erste Schritte in der AWS Marketplace-Dokumentation: Erste Schritte.

 Wenn der Abonnementprozess abgeschlossen ist, verlassen Sie den AWS Marketplace ohne weitere Maßnahmen. Stellen Sie die Software nicht über AWS Marketplace bereit – Benutzer stellen das AMI mit der Schnellstartanleitung bereit.

Schritt 3: Starten Sie den AWS Schnellstart

- Melden Sie sich beim AWS-Benutzerkonto an und wählen Sie eine der folgenden Optionen, um die AWS CloudFormation-Vorlage zu starten. Hilfe bei der Auswahl einer Option finden Sie weiter oben in diesem Handbuch unter Bereitstellungsoptionen.
 - Stellen Sie NetScaler VPX in einer neuen VPC auf AWS bereit, indem Sie eine der AWS CloudFormation-Vorlagen verwenden, die Sie hier finden:
 - * Citrix/Citrix-ADC-AWS-CloudFormation/Templates/Hochverfügbarkeit/Across-Availability-Zone
 - * Citrix/Citrix-ADC-AWS-CloudFormation/Templates/Hochverfügbarkeit/Gleiche Availability-Zone

Wichtig:

Wenn Benutzer NetScaler Web App Firewall in einer vorhandenen VPC bereitstellen, müssen sie sicherstellen, dass sich ihre VPC über zwei Availability Zones erstreckt, mit einem öffentlichen und zwei privaten Subnetzen in jeder Availability Zone für die Workload-Instances, und dass die Subnetze nicht gemeinsam genutzt werden. Dieser Bereitstellungshandbuch unterstützt keine freigegebenen Subnetze. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten VPCs. Diese Subnetze benötigen NAT-Gateways in ihren Routing-Tabellen, damit die Instances Pakete und Software herunterladen können, ohne sie dem Internet auszusetzen. Weitere Informationen zu NAT-Gateways finden Sie unter NAT-Gateways. Konfigurieren Sie die Subnetze so, dass sich die Subnetze nicht überlappen.

Benutzer sollten außerdem sicherstellen, dass die Domänennamenoption in den DHCP-Optionen wie in der Amazon VPC-Dokumentation erläutert konfiguriert ist, die hier zu finden ist: DHCP-Optionssätze DHCP-Optionssätze. Benutzer werden aufgefordert, ihre VPC-Einstellungen einzugeben, wenn sie die Schnellstartanleitung starten.

- Jede Bereitstellung dauert etwa 15 Minuten.
- Überprüfen Sie die AWS-Region, die in der oberen rechten Ecke der Navigationsleiste angezeigt wird, und ändern Sie sie gegebenenfalls. Hier wird die Netzwerkinfrastruktur für die Citrix Web App Firewall aufgebaut. Die Vorlage wird standardmäßig in der Region USA Ost (Ohio) eingeführt.

Hinweis:

Diese Bereitstellung umfasst NetScaler Web App Firewall, die derzeit nicht in allen AWS-Regionen

unterstützt wird. Eine aktuelle Liste der unterstützten Regionen finden Sie in den AWS Service Endpoints: AWS Service Endpoints.

- Behalten Sie auf der Seite **Vorlage auswählen** die Standardeinstellung für die Vorlagen-URL bei, und wählen Sie dann Weiter aus.
- Geben Sie auf der Seite **Details angeben** den Stack-Namen nach Benutzerkomfort an. Überprüfen Sie die Parameter für die Vorlage. Geben Sie Werte für die Parameter an, die eine Eingabe erfordern. Überprüfen Sie für alle anderen Parameter die Standardeinstellungen, und passen Sie sie nach Bedarf an.
- In der folgenden Tabelle werden die Parameter nach Kategorie aufgelistet und für die Bereitstellungsoption separat beschrieben:
- Parameter für die Bereitstellung von NetScaler Web App Firewall in einer neuen oder vorhandenen VPC (Bereitstellungsoption 1)
- Wenn Benutzer die Überprüfung und Anpassung der Parameter abgeschlossen haben, sollten sie Weiter wählen.

Parameter für die Bereitstellung von NetScaler Web App Firewall in einer neuen VPC

Parameter-Bezeichnung			
(Name)	Standard	Beschreibung	
Primäre Availability Zone	Erfordert Eingaben	Die Availability Zone für die	
(PrimaryAvailabilityZone)		primäre NetScaler Web App	
		Firewall-Bereitstellung	
Sekundäre Availability Zone	Erfordert Eingaben	Die Availability Zone für die	
(SecondaryAvailabilityZone)		Bereitstellung der sekundären	
		NetScaler Web App Firewall	
VPC CIDR (VPCCIDR)	10.0.0/16	Der CIDR-Block für die VPC.	
		Muss ein gültiger	
		IP-CIDR-Bereich der Form	
		x.x.x.x/x sein.	
Remote-SSH-CIDR-IP	Erfordert Eingaben	Der IP-Adressbereich, der SSH	
(Verwaltung)		an die EC2-Instance senden	
(RestrictedSSHCIDR)		kann (Port: 22).	

VPC-Netzwerkkonfiguration

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
		Wenn Sie beispielsweise
		alle IP. Adressen mithilfe von
		SSH oder PDP auf die
		Benutzerinstanz zugreifen
		Hinweis: Autorisieren Sie nur
		eine bestimmte IP-Adresse
		oder einen bestimmten
		Adressbereich für den Zugriff
		auf die Benutzerinstanz, da die Verwendung in der Produktion unsicher ist.
Remote-HTTP-CIDR-IP	0.0.0/0	Der IP-Adressbereich, der HTTP
(Client)		zur EC2-Instance senden kann
(RestrictedWebAppCIDR)		(Port: 80)
Remote-HTTP-CIDR-IP (Client) (RestrictedWebAppCIDR)	0.0.0.0/0	Der IP-Adressbereich, der HTTP zur EC2-Instance senden kann (Port: 80)
CIDR für das primäre	10 0 1 0/24	Der CIDR-Block für das primäre
Management des privaten Subnetzes (PrimaryManage- mentPrivateSubnetCIDR)	10.0.1.0/21	Management-Subnetz befindet sich in Availability Zone 1.
Primäre Verwaltung Private	_	Private IP, die der primären
IP (PrimaryManagementPri- vateIP)		Management-ENI zugewiesen wurde (das letzte Oktett muss zwischen 5 und 254 liegen) aus dem CIDR des primären Management-Subnetzes.
CIDR für das öffentliche	10.0.2.0/24	Der CIDR-Block für das primäre
Subnetz des primären Clients		Client-Subnetz befindet sich in
(PrimaryClientPublicSubnet- CIDR)		Availability Zone 1.

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Private IP des primären Clients (PrimaryClientPrivateIP)		Private IP, die dem primären Client ENI zugewiesen wurde (das letzte Oktett muss zwischen 5 und 254 liegen) von der primären Client-IP aus dem primären Client-Subnetz-CIDR.
Privates Subnetz-CIDR des Primärservers (PrimaryServer- PrivateSubnetCIDR)	10.0.3.0/24	Der CIDR-Block für den Primärserver befindet sich in Availability Zone 1.
Private IP des Primärservers (PrimaryServerPrivateIP)		Private IP, die dem Primärserver-ENI (letztes Oktett muss zwischen 5 und 254 liegen) vom Primärserver-Subnetz-CIDR zugewiesen.
Secondary Management Privates Subnetz CIDR (SecondaryManagementPri- vateSubnetCIDR)	10.0.4.0/24	Der CIDR-Block für das sekundäre Management-Subnetz befindet sich in Availability Zone 2.
Sekundäre Verwaltung Private IP (SecondaryManage- mentPrivateIP)		Private IP, die dem Secondary Management ENI zugewiesen wurde (das letzte Oktett muss zwischen 5 und 254 liegen). Es würde sekundäre Management-IP aus dem Secondary Management Subnet CIDR zuweisen.
CIDR für das öffentliche Subnetz des sekundären Clients (SecondaryClient- PublicSubnetCIDR)	10.0.5.0/24	Der CIDR-Block für das sekundäre Client-Subnetz befindet sich in Availability Zone 2.

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Private IP des sekundären	_	Private IP, die dem Secondary
Clients		Client ENI zugewiesen wurde
(SecondaryClientPrivateIP)		(das letzte Oktett muss
		zwischen 5 und 254 liegen). Es
		würde die sekundäre Client-IP
		aus dem Secondary Client
		Subnet CIDR zuweisen.
Privates Subnetz-CIDR für	10.0.6.0/24	Der CIDR-Block für das
sekundäre Server (Secondary-		sekundäre Serversubnetz
ServerPrivateSubnetCIDR)		befindet sich in Availability
		Zone 2.
Private IP des sekundären	—	Private IP, die dem Secondary
Servers		Server ENI zugewiesen wurde
(SecondaryServerPrivateIP)		(das letzte Oktett muss
		zwischen 5 und 254 liegen). Es
		würde die sekundäre Server-IP
		aus dem sekundären
		Server-Subnetz-CIDR zuweisen.
VPC-Tenancy-Attribut	Standard	Die zulässige Tenancy von
(VPCTenancy)		Instances, die in der VPC
		gestartet wurden. Wählen Sie
		Dedicated Tenancy, um
		EC2-Instances für einen
		einzelnen Kunden zu starten.

Bastion-Host-Konfiguration

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Bastion Host erforderlich	Nein	Standardmäßig wird kein
(LinuxBastionHostEIP)		Bastion-Host konfiguriert.
		Wenn Benutzer sich jedoch für
		eine Sandbox-Bereitstellung
		entscheiden möchten, wählen
		Sie im Menü Ja aus. Dadurch
		würde ein Linux-Bastion-Host
		im öffentlichen Subnetz mit
		einer EIP bereitgestellt, die
		Benutzern Zugriff auf die
		Komponenten im privaten und
		öffentlichen Subnetz gewährt.

Konfiguration der NetScaler Web App Firewall

Parameter-Bezeichnung			
(Name)	Standard	Beschreibung	
Name des Schlüsselpaars	Erfordert Eingaben	Ein öffentliches/privates	
(KeyPairName)		Schlüsselpaar, das es	
		Benutzern ermöglicht, sich	
		nach dem Start sicher mit der	
		Benutzerinstanz zu verbinden.	
		Dies ist das Schlüsselpaar, das	
		Benutzer in ihrer bevorzugten	
		AWS-Region erstellt haben.	
		Weitere Informationen finden	
		Sie im Abschnitt Technische	
		Anforderungen.	

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
NetScaler Instanztyp	m4.xlarge	Der EC2-Instance-Typ, der für
(CitrixADCInstanceType)		die ADC-Instances verwendet
		werden soll. Stellen Sie sicher,
		dass der gewählte Instance-Typ mit den auf dem
		AWS-Marktplatz verfügbaren
		Instance-Typen übereinstimmt.
		da sonst die CFT
		möglicherweise fehlschlägt.
NetScaler ADC AMI-ID	_	Das AWS Marketplace AMI, das
(CitrixADCImageID)		für die Bereitstellung der
		NetScaler Web App Firewall
		verwendet werden soll. Dies
		muss mit den AMI-Benutzern
		übereinstimmen, die in Schritt
		2 abonniert wurden.
NetScaler ADC VPX IAM-Rolle	_	Diese Vorlage:
(iam:GetRole)		AWS-Quickstart/Quickstart-
		Citrix-ADC-VPX/Templates
		erstellt die IAM-Rolle und das
		für NetScaler VPX erforderliche
		Instanzprofil. Wenn das Feld
		leer gelassen wird, erstellt CFT
		die erforderliche IAM-Rolle.
Kunde PublicIP (EIP)	Nein	Wählen Sie "Ja", wenn
(ClientPublicEIP)		Benutzer der
		Client-Netzwerkschnittstelle
		eine öffentliche EIP zuweisen
		möchten. Andernfalls haben
		Benutzer auch nach der
		Bereitstellung immer noch die
		Möglichkeit, sie bei Bedarf
		später zuzuweisen.

Konfiguration der Pooled Lizenzierung

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Gepoolte NetScaler Console-Lizenzierung	Nein	Wenn Sie die BYOL-Option für die Lizenzierung wählen, wählen Sie in der Liste Ja aus. Auf diese Weise können Benutzer ihre bereits gekauften Lizenzen hochladen. Bevor Benutzer beginnen, sollten sie NetScaler ADC Pooled Capacity konfigurieren, um sicherzustellen, dass die gepoolte NetScaler Console-Lizenzierung verfügbar ist, siehe NetScalerPooled Capacity
		konfigurieren
Erreichbare NetScaler Console//NetScaler Console Agent IP	Erfordert Eingaben	Unabhängig davon, ob Benutzer NetScaler Console vor Ort oder einen Agenten in der
		Cloud bereitstellen, stellen Sie bei der Option Kundenlizenz sicher, dass Sie eine erreichbare NetScaler Console-IP haben, die dann als Eingabeparameter verwendet wird.
Lizenzierungsmodus	Optional	Lizenzierungsmodi wählen Konfigurieren Sie NetScaler Pooled Capacity. Weitere Informationen finden Sie unter Konfigurieren der gepoolten Kapazität von Citrix ADC NetScaler VPX-Lizenzierung zum Ein- und Auschecken (CICO). Weitere Informationen finden Sie unter Citrix ADC VPX Check-in and Check-Out Lizenzierung NetScaler virtuelle
© 1999–2025 Cloud Software Gr	oup, Inc. All rights reserved.	CPU-Lizenzierung. Weiterg ₅₀ Informationen finden Sie unter Citrix ADC Virtual CPU-Lizenzierung

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Lizenzbandbreite in MBit/s	0 MBit/s	Nur wenn der Lizenzmodus
		Pooled-Licensing ist, kommt
		dieses Feld ins Spiel. Es weist
		eine anfängliche Bandbreite
		der Lizenz in MBit/s zu, die
		nach der Erstellung von
		BYOL-ADCs zugewiesen werden
		soll. Es sollte ein Vielfaches von
		10 MBit/s sein.
Lizenzversion	Premium	Die Lizenzversion für den
		Lizenzmodus Pooled Capacity
		ist Premium .
Plattformtyp der Appliance	Optional	Wählen Sie den erforderlichen
		Appliance-Plattformtyp nur
		dann, wenn sich Benutzer für
		den CICO-Lizenzmodus
		entscheiden. Benutzer erhalten
		die aufgelisteten Optionen:
		VPX-200, VPX-1000, VPX-3000,
		VPX-5000, VPX-8000.
Lizenzversion	Premium	Die Lizenzversion für
		vCPU-basierte Lizenzen ist
		Premium.

AWS-Schnellstart-Konfiguration

Hinweis:

Wir empfehlen Benutzern, die Standardeinstellungen für die beiden folgenden Parameter beizubehalten, es sei denn, sie passen die Vorlagen für die Schnellstartanleitung für ihre eigenen Bereitstellungsprojekte an. Wenn Sie die Einstellungen dieser Parameter ändern, werden die Code-Referenzen automatisch aktualisiert, sodass sie auf eine neue Position in der Schnellstartanleitung verweisen. Weitere Informationen finden Sie im AWS Schnellstart Guide Contributor's Guide hier: AWS Schnellstarts/Option 1 – Adopt a Schnellstart.

Parameter-Bezeichnung		
(Name)	Standard	Beschreibung
Schnellstartanleitung S3	aws-quickstart	Die S3-Bucket-Benutzer, die für
Bucket-Name		ihre Kopie der Schnellstart
(QSS3BucketName)		Guide-Assets erstellt wurden,
		wenn Benutzer die
		Schnellstartanleitung für ihren
		eigenen Gebrauch anpassen
		oder erweitern möchten. Der
		Bucket-Name kann Zahlen,
		Kleinbuchstaben,
		Großbuchstaben und
		Bindestriche enthalten, sollte
		aber nicht mit einem
		Bindestrich beginnen oder
		enden.
Schnellstartanleitung	quickstart-citrix-adc-vpx/	Das Präfix des
S3-Schlüsselpräfix		S3-Schlüsselnamens aus
(QSS3KeyPrefix)		Objektschlüssel und
		Metadaten: Objektschlüssel
		und Metadatenwird verwendet,
		um einen Ordner für die
		Benutzerkopie von Schnellstart
		Guide-Assets zu simulieren,
		wenn Benutzer die
		Schnellstartanleitung für ihren
		eigenen Gebrauch anpassen
		oder erweitern möchten.
		Dieses Präfix kann Zahlen,
		Kleinbuchstaben,
		Großbuchstaben, Bindestriche
		und Schrägstriche enthalten.

- Auf der Seite Optionen können Benutzer ein Ressourcen-Tag oder ein Schlüssel-Wert-Paar für Ressourcen in Ihrem Stack angeben und erweiterte Optionen festlegen. Weitere Informationen zu Ressourcen-Tags finden Sie unter Ressourcen-Tag. Weitere Informationen zum Festlegen von AWS CloudFormation-Stack-Optionen finden Sie unter Festlegen von AWS CloudFormation-Stack-Optionen. Wenn Benutzer fertig sind, sollten sie Weiterwählen.
- Überprüfen und bestätigen Sie auf der Seite Überprüfen die Vorlageneinstellungen. Aktivieren

Sie unter **Funktionen**die beiden Kontrollkästchen, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt und möglicherweise die Fähigkeit zum automatischen Erweitern von Makros erfordert.

- Wählen Sie Erstellen, um den Stack bereitzustellen.
- Überwachen Sie den Status des Stacks. Wenn der Status **CREATE_COMPLETE** #lautet, ist die NetScaler Web App Firewall-Instanz bereit.
- Verwenden Sie die URLs, die auf der Registerkarte **Ausgaben** für den Stapel angezeigt werden, um die erstellten Ressourcen anzuzeigen.

Ossilfernation > Stads > quidstart-soft				
🗆 Stacks (1) 🛛 🔿	Stack info Events Resources	Outputs Parameters	Template Change sets	
Q, Filter by stack name				
Active	Outputs (16)			σ
Qukkstart-waf-ik DEB-05-04 (1541-01 UTC-0030 © GMARE, COMPLETE	Q, Search extruits			•
	Key A	Value v	Description v	Export name
	CientiecurityGroupID	sg-0056eb125c9c3a264	Security group ID for client ADC DNs	
	HanagementSecurityGroupID	19-08c5c20x6a382206d	Security group ID for management ADC DNs	
	PrimaryA0Omtanoe0	1-068041192385c9084	Primary ADC instance ID	
	PrimaryClientPrivateVP	10.0.2.118	Primary Client private VIP	
	PrimaryClientPublicSubnetID	subret-025745e2b66d13d59	Primary Client public subret ID	
	PrimaryManagementPrivatehSIP	10.0.1.149	Primary Management private NSIP	
	PrimaryManagementPrivateSubnetD	subret-0810b54%x8925813	Primary Management private subnet ID	
	PrimaryServerHivataSubnettD	subnet-071053012154ec15c	Primary Server private subnet ID	
	SecondaryADCrestance/0	1-0x5649%293864504	Secondary ADC instance (D	
	SecondaryClientPrivate/HP	1085.231	Secondary Client private VP	
	SecondaryCliettPublicSubnetD	subnet-07se1cd7905845aec	Secondary Client public subnet ID	
	SecondaryManagementPrivateNSIP	10.0.4.213	Secondary Management private NSIP	
	SecondaryManagementPrivateSubnetID	subnet-00/82966635548/22	Secondary Management private subnet ID	
	SecondaryServerPrivateSubnettD	subnet-030018e63558h463	Secondary Server private subnet ID	
	ServerSecurityGroup@	sg-0s299htSeaft(Secd?	Security group 10 for server ADC ENIs	
	VPOD	vpc-06a7v8rtva0x25#lok	VPC/D	

Schritt 4: Testen Sie die Bereitstellung

Wir bezeichnen die Instanzen in dieser Bereitstellung als **primär** und **sekundär**. Jeder Instanz sind unterschiedliche IP-Adressen zugeordnet. Wenn der Schnellstart erfolgreich bereitgestellt wurde, durchläuft der Datenverkehr die primäre NetScaler Web App Firewall-Instanz, die in Availability Zone 1 konfiguriert ist. Unter Failover-Bedingungen, wenn die primäre Instanz nicht auf Clientanfragen reagiert, übernimmt die sekundäre Web App Firewall-Instanz die Leitung.

Die Elastic IP-Adresse der virtuellen IP-Adresse der primären Instance wird auf die sekundäre Instance migriert, die als neue primäre Instanz übernimmt.

Im Failover-Prozess führt NetScaler Web App Firewall Folgendes aus:

- NetScaler Web App Firewall überprüft die virtuellen Server, an die IP-Sätze angehängt sind.
- NetScaler Web App Firewall findet die IP-Adresse, der eine öffentliche IP-Adresse zugeordnet ist, aus den beiden IP-Adressen, die der virtuelle Server abhört. Eine, die direkt an den virtuellen Server angeschlossen ist, und eine, die über den IP-Satz angeschlossen ist.
- NetScaler Web App Firewall ordnet die öffentliche Elastic IP-Adresse wieder der privaten IP-Adresse zu, die zur neuen primären virtuellen IP-Adresse gehört.

Gehen Sie wie folgt vor, um die Bereitstellung zu überprüfen:

• Mit der primären Instance verbinden

Zum Beispiel mit einem Proxy-Server, einem Jump-Host (einer Linux/Windows/FW-Instanz, die in AWS ausgeführt wird, oder dem Bastion-Host) oder einem anderen Gerät, das mit dieser VPC erreichbar ist, oder einem Direct Connect, wenn es um lokale Konnektivität geht.

• Führen Sie eine Auslöseaktion durch, um ein Failover zu erzwingen, und überprüfen Sie, ob die sekund

Tipp:

Um die Konfiguration in Bezug auf NetScaler Web App Firewall weiter zu überprüfen, führen Sie den folgenden Befehl aus, nachdem Sie eine Verbindung zur **primären NetScaler Web App Firewall-Instanz hergestellt haben**:

Sh appfw profile QS-Profile

Stellen Sie mithilfe des Bastion-Hosts eine Verbindung zum NetScaler Web App Firewall HA-Paar her

Wenn sich Benutzer für die Sandbox-Bereitstellung entscheiden (z. B. als Teil von CFT entscheiden sich Benutzer für die Konfiguration eines Bastion Hosts), wird ein in einem öffentlichen Subnetz bereitgestellter Linux-Bastion-Host für den Zugriff auf die Web App Firewall-Schnittstellen konfiguriert.

In der AWS CloudFormation-Konsole, auf die Sie durch Anmeldung zugreifen können: Melden Sie sich an, wählen Sie den Master-Stack und suchen Sie auf der Registerkarte **Outputs** den Wert von **LinuxBastionHostEIP1**.

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

- Der Wert des Schlüssels**PrivateManagementPrivateNSIP** und **PrimaryADCInstanceID**, der in den späteren Schritten für SSH in den ADC verwendet werden soll.
- Wählen Sie Dienste.
- Wählen Sie auf der Registerkarte **Compute EC2** aus.
 - Wählen Sie unter **Resources** die Option **Running Instances**.
 - Notieren Sie sich auf der Registerkarte Description der primären Web App Firewall-Instanz die öffentliche IPv4-IP-Adresse. Benutzer benötigen diese IP-Adresse, um den SSH-Befehl zu erstellen.

tost-tag	p-citrix-adc-master-eu-ce	ntral-1-97a6acc9-Wo	wkLoad51	ack-XYC4-PrimaryADC	Instance-1XIO05VH2MRAWG I	himary	i-07197878fc2cafaed	m4.xlarge
tost-lag	politrix-ado-master-eu-ce	intral-1-97a6acc9-Wo	rkLoad5t	ack-XY-SecondaryADC	Instance-NV30OQYJ9DBJ Sec	ondary	i-0d671adb4736167	m4.xlarge
Instance:	-07197878fc2cafaed RAWG Primary) E	(tcat-tag-citrix-adc lastic IP: 3.122.141	c-master 1.245	eu-central-1-97a6a	cc9-WorkLoadStack-XYC4	-PrimaryA	DCInstance-	880
Description	Status Checks	Monitoring	Tegs	Usage Instructions				
	Instance ID	i-07197878fc2cafaed		Public DNS (Pv4)				
	Instance state	running			IPv4 Public IP	3.122.141	.245	
	Instance type	m4.xlarge			IPr6 IPs			
	Eastic IPs	3.122.141.245*			Private DNS	ip-10-0-1 1.comput	-61.eu-central- e.internal	
	Availability zone	eu-central-1a			Private IPs	10.0.3.10	4, 10.0.1.81, 10.0.2.23	
	Security groups	toat-tag-citrix-ado- 1-97a6acc9-WorkL SecurityGroupStad	master-ex .oad5tack R-	-central- XYC4-	Secondary private IPs			

 Führen Sie den Befehl aus, um den Schlüssel im Benutzer-Schlüsselbund zu speichern sshadd -K [your-key-pair].pem Unter Linux müssen Benutzer möglicherweise das -K Flag weglassen.

• Melden Sie sich mit dem folgenden Befehl beim Bastion-Host an und verwenden Sie dabei den Wert für **LinuxBastionHostEIP1**, den Benutzer in Schritt 1 notiert haben.

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

• Vom Bastion-Host aus können Benutzer mit SSH eine Verbindung zur primären Web App Firewall-Instanz herstellen.

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

Kennwort: [Primäre ADC-Instanz-ID]

```
[ubuntu@ip-10-0-5-243:~$ ssh nsroot@10.0.1.91
ø
                                                #
#
     WARNIND: Access to this system is for authorized users only
                                                #
      Disconnect IMMEDIATELY if you are not an authorized user!
ø
                                                11
ž
                                                #
Last login: Thu Oct 31 19:31:49 2019 from 10.0.5.243
Done
>
```

Jetzt sind Benutzer mit der primären NetScaler Web App Firewall-Instanz verbunden. Um die verfügbaren Befehle anzuzeigen, können Benutzer den Befehl help ausführen. Um die aktuelle HA-Konfiguration anzuzeigen, können Benutzer den Befehl show HA node ausführen.

NetScaler-Konsole

NetScaler Application Delivery Management Service bietet eine einfache und skalierbare Lösung für die Verwaltung von NetScaler-Bereitstellungen, zu denen NetScaler MPX, NetScaler VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler SDX, NetScaler ADC CPX und NetScaler SD-WAN-Appliances gehören, die on-premises oder in der Cloud bereitgestellt werden.

Die NetScaler Console Service-Dokumentation enthält Informationen zu den ersten Schritten mit dem Dienst, eine Liste der vom Dienst unterstützten Funktionen und die für diese Servicelösung spezifische Konfiguration.

Weitere Informationen finden Sie unter NetScaler Console Overview.

Bereitstellung von NetScaler VPX-Instanzen auf AWS mithilfe der NetScaler Console

Wenn Kunden ihre Anwendungen in die Cloud verlagern, werden die Komponenten, die Teil ihrer Anwendung sind, zunehmen, werden stärker verteilt und müssen dynamisch verwaltet werden.

Weitere Informationen finden Sie unter Provisioning NetScaler VPX Instances auf AWS.

NetScaler Web App Firewall und OWASP Top 10 – 2017

Das Open Web Application Security Project: OWASP hat die OWASP Top 10 für 2017 für die Sicherheit von Webanwendungen veröffentlicht. Diese Liste dokumentiert die häufigsten Sicherheitslücken in Webanwendungen und ist ein guter Ausgangspunkt für die Bewertung der Websicherheit. Hier wird detailliert beschrieben, wie die NetScaler Web App Firewall (Web App Firewall) konfiguriert wird, um diese Fehler zu beheben. Web App Firewall ist als integriertes Modul in der NetScaler (Premium Edition) sowie als komplette Palette von Appliances verfügbar.

Das vollständige OWASP Top 10-Dokument ist unter OWASPTop Ten verfügbar.

Signaturen bieten die folgenden Bereitstellungsoptionen, um Benutzern zu helfen, den Schutz von Benutzeranwendungen zu optimieren:

- Negatives Sicherheitsmodell: Beim negativen Sicherheitsmodell verwenden Benutzer zahlreiche vorkonfigurierte Signaturregeln, um die Leistungsfähigkeit des Mustervergleichs anzuwenden, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen. Benutzer blockieren nur das, was sie nicht wollen, und lassen den Rest zu. Benutzer können ihre eigenen Signaturregeln hinzufügen, die auf den spezifischen Sicherheitsanforderungen von Benutzeranwendungen basieren, um ihre eigenen maßgeschneiderten Sicherheitslösungen zu entwerfen.
- Hybrides Sicherheitsmodell: Zusätzlich zur Verwendung von Signaturen können Benutzer positive Sicherheitsüberprüfungen verwenden, um eine Konfiguration zu erstellen, die sich ideal für Benutzeranwendungen eignet. Verwenden Sie Signaturen, um zu blockieren, was Benutzer nicht möchten, und setzen Sie positive Sicherheitsprüfungen durch, um durchzusetzen, was zulässig ist

Um Benutzeranwendungen mithilfe von Signaturen zu schützen, müssen Benutzer ein oder mehrere Profile für die Verwendung ihres Signaturobjekts konfigurieren. In einer hybriden Sicherheitskonfiguration werden die SQL-Injection- und Cross-Site-Scripting-Muster sowie die SQL-Transformationsregeln im Benutzersignaturobjekt nicht nur von den Signaturregeln verwendet, sondern auch von den positiven Sicherheitsüberprüfungen, die im Profil der Web Application Firewall konfiguriert sind, das den signatures-Objekt.

Die Web Application Firewall untersucht den Verkehr zu benutzergeschützten Websites und Webdiensten, um Datenverkehr zu erkennen, der mit einer Signatur übereinstimmt. Eine Übereinstimmung wird nur ausgelöst, wenn jedes Muster in der Regel mit dem Datenverkehr übereinstimmt. Wenn eine Übereinstimmung auftritt, werden die angegebenen Aktionen für die Regel aufgerufen. Benutzer können eine Fehlerseite oder ein Fehlerobjekt anzeigen, wenn eine Anfrage blockiert wird. Protokollmeldungen können Benutzern helfen, Angriffe auf Benutzeranwendungen zu erkennen. Wenn Benutzer Statistiken aktivieren, verwaltet die Web Application Firewall Daten zu Anforderungen, die mit einer Signatur oder Sicherheitsüberprüfung der Web Application Firewall übereinstimmen.

Wenn der Datenverkehr sowohl mit einer Signatur als auch mit einer positiven Sicherheitsprüfung

übereinstimmt, werden die restriktiveren der beiden Aktionen durchgesetzt. Wenn beispielsweise eine Anforderung mit einer Signaturregel übereinstimmt, für die die Blockaktion deaktiviert ist, aber die Anforderung auch mit einer positiven SQL Injection Sicherheitsprüfung übereinstimmt, für die die Aktion blockiert ist, wird die Anforderung blockiert. In diesem Fall wird die Signaturverletzung möglicherweise als [nicht blockiert] protokolliert, obwohl die Anforderung durch die SQL-Injection-Prüfung blockiert wird.

Anpassung: Falls erforderlich, können Benutzer ihre eigenen Regeln zu einem Signatur-Objekt hinzufügen. Benutzer können die SQL/XSS-Muster auch anpassen. Die Option, eigene Signaturregeln hinzuzufügen, die auf den spezifischen Sicherheitsanforderungen von Benutzeranwendungen basieren, gibt Benutzern die Flexibilität, ihre eigenen maßgeschneiderten Sicherheitslösungen zu entwerfen. Benutzer blockieren nur das, was sie nicht wollen, und lassen den Rest zu. Ein bestimmtes Fast-Match-Muster an einem bestimmten Ort kann den Verarbeitungsaufwand erheblich reduzieren, um die Leistung zu optimieren. Benutzer können SQL-Injection- und Cross-Site-Scripting-Muster hinzufügen, ändern oder entfernen. Integrierte RegEx- und Expressions-Editoren helfen Benutzern dabei, Benutzermuster zu konfigurieren und ihre Richtigkeit zu überprüfen.

NetScaler Web App Firewall

Web App Firewall ist eine Lösung für Unternehmen, die hochmodernen Schutz für moderne Anwendungen bietet. NetScaler Web App Firewall mindert Bedrohungen für öffentlich zugängliche Ressourcen wie Websites, Webanwendungen und APIs. Die NetScaler Web App Firewall umfasst IP-Reputationsbasierte Filterung, Bot-Abwehr, Schutz vor OWASP Top 10-Anwendungsbedrohungen, Layer-7-DDoS-Schutz und mehr. Ebenfalls enthalten sind Optionen zur Durchsetzung der Authentifizierung, starke SSL/TLS-Chiffren, TLS 1.3, Ratenbegrenzung und Rewrite-Richtlinien. NetScaler Web App Firewall verwendet sowohl grundlegende als auch erweiterte Web App Firewall-Schutzmaßnahmen und bietet umfassenden Schutz für Ihre Anwendungen mit beispielloser Benutzerfreundlichkeit. Es ist eine Frage von Minuten, bis Sie loslegen können. Darüber hinaus spart NetScaler Web App Firewall den Benutzern durch die Verwendung eines automatisierten Lernmodells, das als dynamisches Profiling bezeichnet wird, wertvolle Zeit. Indem die Web App Firewall automatisch lernt, wie eine geschützte Anwendung funktioniert, passt sie sich an die Anwendung an, auch wenn Entwickler die Anwendungen bereitstellen und ändern. NetScaler Web App Firewall hilft bei der Einhaltung aller wichtigen behördlichen Standards und Gremien, einschließlich PCI-DSS, HIPAA und mehr. Mit unseren CloudFormation-Vorlagen war es noch nie so einfach, schnell einsatzbereit zu sein. Mit Auto Scaling können Benutzer sicher sein, dass ihre Anwendungen auch bei wachsendem Datenverkehr geschützt bleiben.

Bereitstellungsstrategie der Web App Firewall

Der erste Schritt bei der Bereitstellung der Webanwendungs-Firewall besteht darin, zu bewerten, welche Anwendungen oder spezifischen Daten maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und für welche die Sicherheitsinspektion sicher umgangen werden kann. Dies hilft Benutzern dabei, eine optimale Konfiguration zu finden und geeignete Richtlinien und Verbindungspunkte zur Trennung des Datenverkehrs zu entwerfen. Beispielsweise möchten Benutzer möglicherweise eine Richtlinie konfigurieren, um die Sicherheitsinspektion von Anfragen nach statischen Webinhalten wie Bildern, MP3-Dateien und Filmen zu Bypass, und eine andere Richtlinie konfigurieren, um erweiterte Sicherheitsprüfungen auf Anfragen nach dynamischen Inhalten anzuwenden. Benutzer können mehrere Richtlinien und Profile verwenden, um unterschiedliche Inhalte derselben Anwendung zu schützen.

Der nächste Schritt besteht darin, die Bereitstellung zu planen. Erstellen Sie zunächst einen virtuellen Server und führen Sie Testverkehr durch diesen aus, um sich ein Bild von der Geschwindigkeit und Menge des Datenverkehrs zu machen, der durch das Benutzersystem fließt.

Stellen Sie dann die Web App Firewall bereit. Verwenden Sie die NetScaler-Konsole und das Web App Firewall StyleBook, um die Web App Firewall zu konfigurieren. Einzelheiten finden Sie im Abschnitt StyleBook weiter unten in diesem Handbuch.

Nachdem die Web App Firewall mit dem Web App Firewall StyleBook bereitgestellt und konfiguriert wurde, besteht ein nützlicher nächster Schritt darin, die NetScaler ADC Web App Firewall und OWASP Top 10 zu implementieren.

Schließlich sind drei der Web App Firewall-Schutzmaßnahmen besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger verwendet als alle anderen. Daher sollten sie bei der ersten Bereitstellung implementiert werden.

NetScaler-Konsole

Die NetScaler-Konsole bietet eine skalierbare Lösung zur Verwaltung von NetScaler ADC-Bereitstellungen, zu denen NetScaler ADC MPX, NetScaler ADC VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler ADC SDX, NetScaler ADC CPX und NetScaler SD-WAN-Appliances gehören, die on-premises oder in der Cloud bereitgestellt werden.

Analyse- und Verwaltungsfunktionen für NetScaler-Konsolenanwendungen

Die Funktionen, die auf der NetScaler-Konsole unterstützt werden, sind der Schlüssel zur NetScaler Console-Rolle in App Security.

Weitere Informationen zu Funktionen finden Sie unter Funktionen und Lösungen.
Voraussetzungen

Bevor Benutzer versuchen, eine VPX-Instanz in AWS zu erstellen, sollten sie sicherstellen, dass die Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter Voraussetzungen:

Einschränkungen und Nutzungsrichtlinien

Die unter Einschränkungen und Nutzungsrichtlinien verfügbaren Einschränkungen und Nutzungsrichtlinien gelten beim Bereitstellen einer Citrix ADC VPX-Instanz auf AWS.

Technische Anforderungen

Bevor Benutzer die Schnellstartanleitung starten, um mit einer Bereitstellung zu beginnen, muss das Benutzerkonto wie in der folgenden Ressourcentabelle angegeben konfiguriert werden. Andernfalls schlägt die Bereitstellung möglicherweise fehl.

Ressourcen

Melden Sie sich bei Bedarf beim Amazon-Benutzerkonto an und fordern Sie hier eine Erhöhung des Servicelimits für die folgenden Ressourcen an: AWS/Anmelden. Möglicherweise müssen Sie dies tun, wenn Sie bereits über eine vorhandene Bereitstellung verfügen, die diese Ressourcen verwendet, und Sie glauben, dass Sie bei dieser Bereitstellung die Standardlimits überschreiten könnten. Standardlimits finden Sie in den AWS-Servicekontingenten in der AWS-Dokumentation: AWS Service Quotas.

Der AWS Trusted Advisor, zu finden hier: AWS/Sign in, bietet eine Überprüfung der Service-Limits, die die Nutzung und Einschränkungen für einige Aspekte einiger Services anzeigt.

Ressource	Diese Bereitstellung verwendet			
VPCs	1			
Elastische IP-Adressen	0/1 (für Bastion-Gastgeber)			
IAM-Sicherheitsgruppen	3			
IAM-Rollen	1			
Subnetze	6 (3/Verfügbarkeitszone)			
Internet-Gateway	1			
Routen-Tabellen	5			
Web App Firewall VPX-Instanzen	2			

Ressource	Diese Bereitstellung verwendet
Bastion-Wirt	0/1
NAT-Gateway	2

Regionen

NetScaler Web App Firewall auf AWS wird derzeit nicht in allen AWS-Regionen unterstützt. Eine aktuelle Liste der unterstützten Regionen finden Sie unter AWS Service Endpoints in der AWS-Dokumentation: AWS Service Endpoints.

Weitere Informationen zu AWS-Regionen und warum Cloud-Infrastruktur wichtig ist, finden Sie unter: Globale Infrastruktur.

Schlüssel-Paar

Stellen Sie sicher, dass mindestens ein Amazon EC2-Schlüsselpaar im AWS-Benutzerkonto in der Region vorhanden ist, in der Benutzer mithilfe der Schnellstartanleitung eine Bereitstellung planen. Notieren Sie sich den Namen des Schlüsselpaars. Benutzer werden während der Bereitstellung zur Eingabe dieser Informationen aufgefordert. Um ein Schlüsselpaar zu erstellen, folgen Sie den Anweisungen für Amazon EC2-Schlüsselpaare und Linux-Instances in der AWS-Dokumentation: Amazon EC2-Schlüsselpaare und Linux-Instances.

Wenn Benutzer die Schnellstartanleitung zu Test- oder Machbarkeitszwecken bereitstellen, empfehlen wir, dass sie ein neues Schlüsselpaar erstellen, anstatt ein Schlüsselpaar anzugeben, das bereits von einer Produktionsinstanz verwendet wird.

Referenzen

- HTML-SQL-Injektionsprüfung
- XML-SQL-Injektionsprüfung
- Den HTML Cross-Site Scripting Check über die Befehlszeile konfigurieren
- Siteübergreifende XML-Skriptprüfung
- Verwenden der Befehlszeile zur Konfiguration der Sicherheitsüberprüfung für den Pufferüberlauf
- Signaturobjekt hinzufügen oder entfernen
- Konfiguration oder Änderung eines Signature-Objekts

- Aktualisierung eines Signaturobjekts
- Integration von Snort-Regeln
- Bot-Erkennung
- Bereitstellen einer NetScaler VPX Instanz unter Microsoft Azure

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	Øa:1e:2e:17:a2:37	Intel 82599 10G VF Interface			
2	L0/1	1500	Øa:1e:2e:17:a2:37	Netscaler Loopback interface			

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

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 \\<instance
\\_id\\> --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 \\<
instance\\_id\\> --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 --stribute sriovNetSupport
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.



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.

	Interface	MTU	MAC	Suffix
1	10/1	1500	Øa:1e:2e:17:a2:37	Intel 82599 10G VF Interface
2	10/2	1500	0a:df:17:0a:fe:83	Intel 82599 10G VF Interface
8	10/3	1500	@a:de:5d:31:bf:c3	Intel 82599 10G VF Interface
1	L0/1	1500	Øa:1e:2e:17:a2:37	Netscaler Loopback interface

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/aboutaws/whats-new/2016/06/introducing-elastic-network-adapter-ena-the-next-generation-networkinterface-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 Hochverfügbarkeitskonfigura tion 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:

- 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:

```
    [WARNING]:Force Failover may cause configuration loss, peer
health not optimum. Reason(s):
    HA version mismatch
    HA heartbeats not seen on some interfaces
    Please confirm whether you want force-failover (Y/N)?
```

Die Warnmeldung wird angezeigt, da die Systemsoftware der beiden VPX-Instanzen nicht HAkompatibel 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 f
 ür die Warnmeldung ein, um den Failover-Vorgang zu best
 ätigen:
 - 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)?
	γ

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:

```
1 > remove ha node 30
2 Done
3 > save config
4 Done
```

Geben Sie an der Eingabeaufforderung der neuen Instanz (neuer Primärknoten) Folgendes ein:

```
1> remove ha node 102Done3> save config4Done
```

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.

NetScaler VPX 14.1

Q Search in Menu		System / System Information	
AWS	>	System	
System	\sim		
Licenses		System Information System Sessions 1 System Network	
Settings		System Upgrade Reboot Migration Statistics Call Home	
Diagnostics			
High Availability	>	System Information	
NTP Servers		Citrix ADC IP Address	
Reports		Netmask	
Profiles		Node	Standalone
Partition Administration	>	Technical Support PIN	Coordinated Universal Time
User Administration	>	System Time	Wed, 18 Dec 2019 06:16:59 UTC
Authentication	(Last Config Changed Time	Wed, 18 Dec 2019 06:16:40 UTC
Auditing	(Last Config Saved Time	Wed, 18 Dec 2019 05:41:16 UTC
SNMP		Hardware Information	
AppElow	<u> </u>		
Appriow	• >	Platform	NetScaler Virtual Appliance 450040
Cluster	>	Manufactured on	2/17/2009
Network	>	CPU	2305 MHZ
Web Interface	>	DI JSDH	
WebFront	>	Encoded serial no	
Backup and Restore		Citrix ADC UUID	
Encryption Keys			

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

March 20, 2025

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.

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

Für eine NetScaler VPX-Instanz in Azure ist eine gültige Lizenz erforderlich. Für NetScaler VPX-Instanzen, die in Azure ausgeführt werden, sind folgende Lizenzierungsoptionen verfügbar:

- Bringen Sie Ihre eigene Lizenz mit (BYOL): Um die BYOL-Option zu verwenden, gehen Sie folgendermaßen vor:
 - Verwenden Sie das Lizenzierungsportal auf der NetScaler-Website, um eine gültige Lizenz zu generieren.
 - Laden Sie die generierte Lizenz auf die Instanz hoch.
- NetScaler VPX Check-in- und Check-out-Lizenz: Mit diesem Lizenzmodell können Sie eine Lizenz aus einem Pool verfügbarer Lizenzen auschecken und wieder einchecken, wenn sie nicht mehr benötigt wird. Weitere Informationen und detaillierte Anweisungen finden Sie unter NetScaler VPX Check-in- und Check-out-Lizenz.

Hinweis:

- Die abonnementbasierte Lizenzierung wird für NetScaler VPX-Instanzen in Azure nicht mehr unterstützt.
- Führen Sie einen Warm-Neustart durch, bevor Sie Konfigurationsänderungen an der NetScaler VPX-Instanz vornehmen, um die richtige NetScaler VPX-Lizenz zu aktivieren.

VPX-Leistung und empfohlene Azure-Instanztypen

Für die gewünschte VPX-Leistung werden die folgenden Azure-Instanztypen empfohlen.

VPX- Leistung	Azure-Insta	inztypen VPX 3		
	VPX 1	Netzw-	VPX bis zu	
	NIC/2 NIC	erkkarte	8 NIC	
Bis zu 200 Mbit/s	Standard_[D2 S<u>t</u>av5 dard_	_D8 S<u>t</u>av5 dard_D16_v5	
Bis zu 1 Gbit/s	Standard_[04 S<u>t</u>av5 dard_	_D8 \$<u>t</u>av5 dard_D16_v5	
Bis zu 5 Gbit/s	Standard_[∑8 \$tâ<u>n</u>vda rd_	_D8\$515a <u>n</u> %15ard_DS94t_an2dard_D8\$515a <u>n</u> %15ard_D8\$515a <u>n</u> %15ard_DS94t_an2dard_D16_	_v5
Bis zu 10 Gbit/s	Standard_I	D8 S<u>t</u>av5 dard_	_D8 S tan5dard_D16_v5	

Punkte zu beachten

- Azure unterstützt VPX-Durchsatz von bis zu 10 Gbit/s. Weitere Informationen finden Sie im NetScaler VPX-Datenblatt.
- Um eine optimale Leistung auf NetScaler VPX-Instanzen mit einem Durchsatz von mehr als 1 GBit/s zu erzielen, müssen Sie den beschleunigten Azure-Netzwerkbetrieb aktivieren. Es wird empfohlen, zu diesem Zweck einen Azure-Instanztyp zu verwenden, der den beschleunigten Netzwerkbetrieb unterstützt. Weitere Informationen zum Konfigurieren des beschleunigten Netzwerkbetriebs finden Sie unter Konfigurieren einer NetScaler VPX-Instanz für die Verwendung des beschleunigten Azure-Netzwerkbetriebs.
- 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.

- 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.

IPv6-Unterstützung für die NetScaler VPX-Instanz in Azure

Die eigenständige NetScaler VPX-Instanz unterstützt 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
- 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.

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 Netzwerk 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. 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 konfigurierten 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

January 15, 2025

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

=	New	_ 🗖 ×	Management	_ 🗖 ×
+ New			2	
Resource groups	Search the marketplace	الد ممک	FFATURED APPS	الد ممک
All resources				<u> </u>
1 Decent	Virtual Machines	>	Resource grou	
wecent	Web + Mobile	>	application toget	her
🔇 App Services	Data + Storage	>		
SQL databases	Data + Analytics	>	Backup and Sit (OMS)	e Recovery
👰 Virtual machines (classic)	Internet of Things	>	A backup and dis solution to safegu	aster recovery Iard applications
👱 Virtual machines	Networking	>	Automation	
👶 Cloud services (classic)	Media + CDN	>	Automate the ma	nagement of your mises resources
🕆 Subscriptions	Hybrid Integration	>	_	
Browse >	Security + Identity	>	Scheduler Run jobs on simp	le or complex
	Developer Services	>	recurring schedul	es.
	Management	\geq	Kov Vault	
	Intelligence	>	Enhance data pro	tection and
	Containara			

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

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

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**.

NetScalerVNet - Subnets						*	_	×
virtual network	🕂 Subnet	- Gate	way subnet					
Search (Ctrl+/)	Search :	ubnets						1
	NAME	^	ADDRESS RANGE	^	AVAILABLE ADDR ^	SECURITY GROUP	^	
	NSFrontEn	ł	22.22.1.0/24		251	-		
1093								
SETTINGS								
↔ Address space								
 Connected devices 								
<↔ Subnets								

- 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 Dropdownliste
- 3. Klicken Sie auf **Erstellen**.

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

		_ 🗖 ×		_ = ×
+ New	New		Data + S	Storage
Resource groups			*	Data Lake Store (preview) Hyper-scale repository for big data analytic workloads
All resources	MARKETPLACE	See all	PREVIEW	
🕒 Recent	Virtual Machines	>		SQL Data Warehouse (preview) Fully elastic, managed, and
🔕 App Services	Web + Mobile	<u> </u>	SQL PREVIEW	parallelized relational database. Analyze and scale in seconds.
👼 SQL databases	Data + Storage	>		Azure DocumentDB
🧕 Virtual machines (classic)	Internet of Things	>		Scalable and managed NoSQL document database service for modern cloud applications.
Virtual machines	Networking	>		Storago account
Cloud services (classic)	Media + CDN	>		Use Blobs, Tables, Queues, and Files for reliable, economical cloud
💡 Subscriptions	Hybrid Integration	>		storage.
Browse 🖒	Security + Identity	>	2	Redis Cache Distributed, in-memory Redis Cache
	Developer Services		×	service for modern cloud applications
	Management	>		Azure Search
	Intelligence	>		Search-as-a-service solution
	Containers	>		

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.

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

- 4. 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**.

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

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.

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.

≡		_ D ×		* _ D ×
+ New	New		NETWOF	Marketplace
	✓ NetScaler	×	RKING	
() Resource groups	MARKETPLACE			
All resources	Virtual Machines	<u> </u>		Everything
🕒 Recent	Web + Mobile	>		Virtual Machines
🔇 App Services	Data + Storage	>		Web + Mobile
👼 SQL databases	Data + Analytics	>		Data + Storage
Virtual machines (classic)	Internet of Things	>		Data + Analytics
🧕 Virtual machines	Networking	>		Internet of Things
Cloud services (classic)	Media + CDN	>		Networking
📍 Subscriptions	Hybrid Integration	>		Media + CDN
Browse >	Security + Identity	>		Hybrid Integration
	Developer Services	>		Security + Identity
	Management	>		Developer Services
	Containers	>		Management
	RECENT			Intelligence
	Traffic Manager profile			Containers
	Microsoft			
	Resource group Microsoft			

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**.

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

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	Bedient den
	IP-Adresse; statische private	Verwaltungsverkehr
	IP-Adresse	
ipconfig2	Statische öffentliche	Dient dem clientseitigen
	IP-Adresse; statische private	Datenverkehr
	Adresse	
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.

Virtual machines 💉 🗙 brahasitaramanathancitrix (Default Directory)	NSDoc0330VM - Network in Virtual machine	nterfaces	* ×
+ Add ■■ Columns 🕐 Refresh	Search (Ctrl+/)		
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Switch directories	Q Overview	NAME ^ PUBLIC IP ADDRE ^ PRIVATE IP ADDR ^ SECURITY GR	OUP ^
nsdoc 1 itans	Activity log	nsdoc0330vm923 13.78.187.150 192.0.0.4 NSDoc0330	VM-nsg
NAME V	Access control (IAM)		
I NSDoc0330VM •••	Tags		
	X Diagnose and solve problems		
	SETTINGS		
	🔯 Availability set		
	aisks		
	Extensions		
	Retwork interfaces		
	👤 Size		

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.

nsdoc0330vm923 - IP config	urations	
Search (Ctrl+/)	+ Add R Save X Discard	
 Overview Activity log Access control (IAM) 	IP forwarding settings IP forwarding Virtual network	
🛷 Tags	IP configurations * Subnet	
SETTINGS		
IP configurations	Search IP configurations	IP VERSION
DNS servers	inconfig1	IDv/
Network security group	ipcomgr	117 V44
Properties		

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.

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

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**.

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

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

Schritt 2: Konfigurieren von NetScaler-eigenen IP-Adressen

Konfigurieren Sie die NetScaler-eigenen IP-Adressen mit der GUI oder des Befehlsadd ns ip. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren

April 1, 2025

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 aktivpassiven 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**.

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

5. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.

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

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.

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

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.

	🕂 Add		
	○ Search frontend IP configu	irations	
	NAME		P ADDRESS
Activity log			
Access control (IAM)			04.40.00.190 (alb-publicip)
🧳 Tags			
🗙 Diagnose and solve problems			
SETTINGS			
Frontend IP configuration			

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.

Create a resource	NetScaler 12.1 HA using Availability Zones
	Litrix

- 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?

^{Home} > № Create	New > Marketplace > Everything : NetScaler 12.1 HA using	A	Scaler X	12.1 HA using Av Basics	vailability Zones > Create NetScaler 12.1 HA us
1	Basics Configure basic settings	>			This deployment requires Azure region supporting Availability Zones. Selecting a region that does not support Availability Zones will
2	General Settings Configure the General settings	>		U	result in deployment failure. Refer to the <u>list</u> of Azure regions supporting Availability Zones.
3	Network Settings Configure the Network settings	>		Subscriptio	on
4	Summary NetScaler 12.1 HA using Availa	>		* Resource	e group 🕦 e new 🔵 Use existing
5	Buy	>		* Location East US 2	2 ~

- 4. 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.

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

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 Maschinenan.
- 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

January 15, 2025

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktivpassiven 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) onthält:	Management IP ist mit IPConfig5 konfiguriert, die eine öffentliche IP (pip3) und eine private IP (12 5 2 26) onthält:
	nic1; Mgmtsubnet=12.5.2.0/24	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;	Clientseitige IP ist mit IPConfig7 konfiguriert, die eine private IP (12.5.1.28) enthält; nic5;
	frontendSubet=12.5.1.0/24 enthält	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	Serverseitige IP ist mit IPConfig8 konfiguriert, die eine private IP (12.5.3.28) enthält; nic6;
	enthält	BackendSubnet=12.5.3.0/24
-	Regeln und Ports für NSG sind SSH (22), HTTP (80), HTTPS (443)	-

Parametereinstellungen

In diesem Szenario werden die folgenden Parametereinstellungen verwendet:

1	<pre>\$locName= "South east Asia"</pre>
3	<pre>\$rgName = "MulitIP-MultiNIC-RG"</pre>
5	<pre>\$nicName1= "VM1-NIC1"</pre>
6 7	<pre>\$nicName2 = "VM1-NIC2"</pre>
8 9 10	<pre>\$nicName3= "VM1-NIC3"</pre>
10 11 12	<pre>\$nicName4 = "VM2-NIC1"</pre>
12	<pre>\$nicName5= "VM2-NIC2"</pre>
14 15 16	<pre>\$nicName6 = "VM2-NIC3"</pre>
10	<pre>\$vNetName = "Azure-MultiIP-ALB-vnet"</pre>
10	<pre>\$vNetAddressRange= "12.5.0.0/16"</pre>
20 21 22	<pre>\$frontEndSubnetName= "frontEndSubnet"</pre>
23	<pre>\$frontEndSubnetRange= "12.5.1.0/24"</pre>
2 4 25 26	<pre>\$mgmtSubnetName= "mgmtSubnet"</pre>
27	<pre>\$mgmtSubnetRange= "12.5.2.0/24"</pre>
29 30	<pre>\$backEndSubnetName = "backEndSubnet"</pre>
31 32	<pre>\$backEndSubnetRange = "12.5.3.0/24"</pre>
33 34	<pre>\$prmStorageAccountName = "multiipmultinicbstorage"</pre>
35	<pre>\$avSetName = "multiple-avSet"</pre>
37 38	<pre>\$vmSize= "Standard_DS4_V2"</pre>
39 40	<pre>\$publisher = "Citrix"</pre>
41 42	<pre>\$offer = "netscalervpx-120"</pre>
43 44	\$sku = "netscalerbyol"
45 46	<pre>\$version="latest"</pre>
47 48	<pre>\$pubIPName1="VPX1MGMT"</pre>
49	<pre>\$pubIPName2="VPX2MGMT"</pre>

50	
51	\$pubIPName3="ALBPIP"
52	ÉdemNeme 1 - II v pv 1 dpc II
53 54	\$dolinaliet="vpxtdls"
55	\$domName2="vpx2dns"
56	
57	\$domName3="vpxalbdns"
58	
59	\$vmNamePrefix="VPXMultiIPALB"
60 61	<pre>cocDickSuffix1="comultiinalbdickdb1"</pre>
62	
63	<pre>\$osDiskSuffix2="osmultiipalbdiskdb2"</pre>
64	
65	<pre>\$lbName= "MultiIPALB"</pre>
66	
67	<pre>\$frontEndConfigName1= "FrontEndIP"</pre>
69	<pre>\$backendPoolName1= "BackendPoolHttp"</pre>
70	
71	<pre>\$lbRuleName1= "LBRuleHttp"</pre>
72	
73	<pre>\$healthProbeName= "HealthProbe"</pre>
74	
75 76	\$nsgName="NSG-Mult11P-ALB"
77	Śrule1Name="Inbound-HITP"
78	
79	<pre>\$rule2Name="Inbound-HTTPS"</pre>
80	
81	<pre>\$rule3Name="Inbound-SSH"</pre>

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.

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
$prmStorageAccount=New-AzureRMStorageAccount -Name
$prmStorageAccountName -ResourceGroupName $rgName -Type
Standard_LRS -Location $locName
$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
     $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
13
        Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 120
14
15
     -SourceAddressPrefix Internet -SourcePortRange * -
16
        DestinationAddressPrefix * -DestinationPortRange 22
17
18
     $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
        Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
        $rule3
```

Erstellen Sie ein virtuelles Netzwerk und drei Subnetze.

```
5
6
     $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
7
         $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
     $subnetName="backEndSubnet"
21
22
23
     \$subnet2=\$vnet.Subnets|?{
24
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
     $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
7
         Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
         $pip1 -Primary
8
9
10
     $IPConfigName3="IPConfig-3"
11
     $IPAddress="12.5.1.27"
13
14
15
     $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
16
         Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
     $IPConfigName4 = "IPConfig-4"
19
20
21
22
     $IPAddress = "12.5.3.24"
23
24
25
     $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
          -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie IP-Konfigurationen für VPX2.

```
$IpConfigName5 = "IPConfig5"
1
2
3
     $IPAddress="12.5.2.26"
4
5
6
     $IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
7
         Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
         $pip2 -Primary
8
9
     $IPConfigName7="IPConfig-7"
10
11
12
     $IPAddress="12.5.1.28"
13
14
15
16
     $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
         Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
     $IPConfigName8="IPConfig-8"
19
20
21
22
     $IPAddress="12.5.3.28"
```

```
23
24
25 $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
        Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie Netzwerkkarten für VPX1.

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

Erstellen Sie Netzwerkkarten für VPX2.

```
$nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
1
        $rgName -Location $locName -IpConfiguration $IpConfig5 -
        NetworkSecurityGroupId $nsg.Id
2
3
Δ
    $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig7 -
        NetworkSecurityGroupId $nsg.Id
5
6
7
    $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
        $rgName -Location $locName -IpConfiguration $IpConfig8 -
        NetworkSecurityGroupId $nsg.Id
```

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

```
1 $suffixNumber = 1
2
3 $vmName=$vmNamePrefix + $suffixNumber
4
```

5	<pre>\$vmConfig=New-AzureRMVMConfig -VMName \$vmName -VMSize \$vmSize - AvailabilitySetId \$avSet.Id</pre>
6	
7	<pre>\$cred=Get-Credential -Message "Type the name and password for VPX login."</pre>
8	
9	<pre>\$vmConfig=Set-AzureRMVMOperatingSystem -VM \$vmConfig -Linux - ComputerName \$vmName -Credential \$cred</pre>
10	
11	\$vmConfig=Set-AzureRMVMSourceImage -VM \$vmConfig -PublisherName \$publisher -Offer \$offer -Skus \$sku -Version \$version
12	
13	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic1 .Id -Primary</pre>
14	
15	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic2 .Id</pre>
16	
17	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic3 .Id</pre>
18	
19	ŚosDiskName=ŚvmName + "-" + ŚosDiskSuffix1
20	
20	<pre>\$osVhdUri=\$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +</pre>
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
    $vmName=$vmNamePrefix + $suffixNumber
5
6
7
     $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
8
        AvailabilitySetId $avSet.Id
9
10
     $cred=Get-Credential -Message "Type the name and password for VPX
11
        login."
12
13
14
     $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
```

```
ComputerName $vmName -Credential $cred
15
16
     $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
17
         $publisher -Offer $offer -Skus $sku -Version $version
18
19
20
     $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
         Primary
23
     $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
     $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
26
27
28
     $osDiskName=$vmName + "-" + $osDiskSuffix2
29
31
     $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
32
         /" + $osDiskName + ".vhd"
34
     $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
35
          $osVhdUri -CreateOption fromImage
37
38
     Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
          -Name $sku
40
     New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
41
         $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
      $nic3.IPConfig
8
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 255.255.0 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 aktivpassiven 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-Befehlenein 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**.

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

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.

Create a virtual machine

Basics	Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create

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

Project details

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

Subscription * (i)	V	
Resource group * (i)	(New) demo	٦
	Create new	_
Instance details		
Virtual machine name * 🕕	vm1-demo 🗸	
Region * (i)	US) East US	
Availability options (i)	Availability zone	
Availability zone * ①	Zones 1 ~	
Review + create < Previ	ous Next : Disks >	

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.

Create a virtual machine

 Basics
 Disks
 Networking
 Management
 Monitoring
 Advanced
 Tags
 Review + create

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

Network interface

Learn more 🗹

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

Virtual network * 🕕	(new) vm1-demo-vnet	\sim
	Create new	
Subnet * 🔅	(new) default (10.2.0.0/24)	\sim
Public IP 🕕	(new) vm1-demo-ip	\sim
	Create new	
NIC network security group 🕕	O None	
	Basic	
	◯ Advanced	
Public inbound ports * 🛈	○ None	
	Allow selected ports	
Select inbound ports *	SSH (22)	\sim
	This will allow all IP addresses to access your virtual machine. This is or recommended for testing. Use the Advanced controls in the Networking ta create rules to limit inbound traffic to known IP addresses.	nly Ib to
Delete public IP and NIC when VM is deleted ①		
Enable accelerated networking 🔅		
Load balancing		
You can place this virtual machine in the	backend pool of an existing Azure load balancing solution. Learn more $ec d$	
Load balancing options (i)	None	
, in the second s	Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flu	DWS.
	Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.	

4. Klicken Sie auf Weiter: Überprüfen + erstellen.

< Previous

Review + create

Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**.

Next : Management >

Create a virtual machine

✓ Validation past	ssed	
Basics Disks	Networking Man	nagement Monitoring Advanced Tags Review + create
i Cost given b	elow is an estimate and no	ot the final price. Please use Pricing calculator a for all your pricing needs.
Price		
NetScaler ADC 14	4.1	Not covered by credits ①
by Cloud Software Terms of use Priv	Group acy policy	2.3000 USD/hr
1 X Standard DS2	2 v2	Subscription credits apply ①
by Microsoft		0.0880 USD/hr
Terms of use Priv	acy policy	Pricing for other VM sizes
		1
TERMS		
By clicking "Create above; (b) authoriz billing frequency a	", I (a) agree to the legal re Microsoft to bill my cu is my Azure subscription:	I terms and privacy statement(s) associated with the Marketplace offering(s) listed urrent payment method for the fees associated with the offering(s), with the same ; and (c) agree that Microsoft may share my contact, usage and transactional
provide rights for	he provider(s) of the offe third-party offerings. See	ering(s) for support, billing and other transactional activities. Microsoft does not the Azure Marketplace Terms for additional details.
provide rights for t Name	he provider(s) of the offe third-party offerings. See	ering(s) for support, billing and other transactional activities. Microsoft does not a the Azure Marketplace Terms for additional details.
provide rights for a	he provider(s) of the offe third-party offerings. See	ering(s) for support, billing and other transactional activities. Microsoft does not e the Azure Marketplace Terms for additional details.
provide rights for Name Preferred e-mail a	he provider(s) of the offe third-party offerings. See ddress	ering(s) for support, billing and other transactional activities. Microsoft does not e the Azure Marketplace Terms for additional details.
provide rights for Name Preferred e-mail a Preferred phone n	he provider(s) of the offe third-party offerings. See ddress umber	ering(s) for support, billing and other transactional activities. Microsoft does not a the Azure Marketplace Terms for additional details.
provide rights for Name Preferred e-mail a Preferred phone n	he provider(s) of the offe third-party offerings. See ddress umber	ering(s) for support, billing and other transactional activities. Microsoft does not a the Azure Marketplace Terms for additional details.
Preferred e-mail at Preferred phone n	he provider(s) of the offe third-party offerings. See ddress umber It SSH port(s) open to the cs tab.	ering(s) for support, billing and other transactional activities. Microsoft does not a the Azure Marketplace Terms for additional details.

5. Nachdem die Bereitstellung abgeschlossen ist, klicken Sie auf **Go to Resource**, um die Konfigurationsdetails zu sehen.

Overview	Vour deployment is complete
nputs	V Four deployment is complete
lutoute	Deployment name: CreateVm-citrix.netscalervpx-141-netscaler5000 Start time: 8/9/2023, 11:41:20 AM
Julputs	Subscription: Correlation ID: 902798eb-f8b1-4c0a-a6bb-efe734476f71
emplate	heading group, denie
	✓ Deployment details
	∧ Next steps
	Setup auto-shutdown Recommended
	Monitor VM health, performance and network dependencies Recommended
	Run a script inside the virtual machine . Recommended
	Go to resource Create another VM

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.

Home > vm1-demo | Networking >

Create network interface

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

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.

Create load balancer

Project details	
Subscription *	
Resource group *	demo 🗸
	Cleate new
Instance details	
Name *	alb1 🗸
Region *	Southeast Asia
SKU * (i)	• Standard
	Gateway
	O Basic
Type * 🛈	Public
	O Internal
Tier *	Regional
	🔿 Global
Review + create < Previous	Next : Frontend IP configuration > Download a template for automation RGi

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.

Basics	Frontend IP configuration	Backend pools	Inbound rules	Outbound rules	Tags	Review + create
A fronten	d IP configuration is an IP addres	ss used for inbound	and/or outbound co	ommunication as defi	ned withi	n load balancing, inbound NAT, and outbound rules.
+ Add	a frontend IP configuration]				
Name ´	¢↓	-		IP a	address ´	L1
Add a fr	ontend IP to get started					

Add frontend IP configuration	\times
Name *	
alb-frontend	\checkmark
IP version	
● IPv4 ○ IPv6	
IP type	
IP address () IP prefix	
Public IP address *	
(New) alb-public-ip	\checkmark
Create new	
Gateway Load balancer (i)	
None	\sim



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.

Create load balancer

Basics	Frontend IP configuration	Backend pools In	bound rules Outbound rul	es Tags Review + creat	e				
A backen	A backend pool is a collection of resources to which your load balancer can send traffic. A backend pool can contain virtual machines, virtual machine s								
+ Add	d a backend pool								
Name	Virtua	al network	Resource Name	Network interface	IP address				
Name \checkmark alb-	Virtua-backend-pool	al network	Resource Name	Network interface	IP address				
Name	-backend-pool vm1-o	al network demo-vnet	Resource Name	Network interface	IP address 10.2.0.4				

5. Klicken Sie auf der Registerkarte Eingehende Regeln auf Load Balancing-Regel hinzufügenund 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.

Add load balancing rule

alb1

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

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

 \times

6. Klicken Sie auf **Review + Erstellen**. Nachdem die Überprüfung erfolgreich war, klicken Sie auf **Erstellen**.

Create load balancer Validation passed Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Review + create Tags Basics Subscription Resource group demo Name alb1 Southeast Asia Region SKU Standard Regional Tier Public Type Frontend IP configuration alb-frontend Frontend IP configuration name Frontend IP configuration IP address To be created Backend pools Backend pool name alb-backend-pool Inbound rules Load balancing rule name lb-rule1 Health probe name health-probe1 Outbound rules None Tags None Create < Previous Next > Download a template for automation RGive feedback

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**.

← Create HA Node

Remote Node IP Address*		
10 . 4 . 1 . 5	0	
Configure remote system to part	icipate High Availability setup	,
Turn Off HA Monitor interface/cl	tannels that are down	
🥑 Turn en INC(Independent Netwo	rk Configuration) mode on self	t node ()
Remote System Login Credential		
User Name		
Pessword		
Secure Access		

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**.

숙 Create HA Node

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

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.

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

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**.

System > Not	twork > IPs >	IPV4s												
IPs													Ş	F.
IPV4s 🖪	IPV6s 1	Port A	Allocation											
Add Ed	lit Delete	Statis	stics Sele	et Acti	an 🗸									
Q Click here t	to search or you ca	n enter K	(ey : Value format											()
	IP ADDRESS		STATE		TYPE	MODE	ARP	ICMP	VIRTUAL S	ERVER		TRAFFIC DOMAIN		
	10.4.3.4		ENABLED		Subnet IP	Active	ENABLED	ENABLED	-N/A-					0
	10.4.2.5		ENABLED		Virtual IP	Active	ENABLED	ENABLED	ENABLED					0
	10.4.2.4		ENABLED		Virtual IP	Active	ENABLED	ENABLED	ENABLED					0
	10.4.1.4		ENABLED		NetScaler IP	Active	ENABLED	ENABLED	-N/A-					0
Total 4										25 Per Page	~	Page 1 of 1	۰.	

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.
 - System > Network > IPs > IPV4s C 😭 IPs IPV4s 3 IPV6s 1 Port Allocation Add Edit Delete Statistics TYPE MODE ARP VIRTUAL SERVER ICMP TRAFFIC DOMAIN ENABLED Subnet IP Active ENABLED -N/A-0 0.4.2.5 ENABLED Virtual IP ENABLED ENABLED ENABLED 10.4.1.5 ENABLED NetScaler IP Active ENABLED ENABLED -N/A-0 Total 3 25 Per Page

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:

c) Klicken Sie auf Erstellen.

- 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.

← Create IP Set	IPV4s 🕘							С×
North Control of Contr	Add Edit Delete	Statistics Select A	ctionv					
ipuett ()	Q. Click here to search or you can entr	er Key::Value format						0
Traffic Domain	IP ADDRESS	5 : TRAFFIC DOMAIN	OWNER NODE	STATE :	TYPE :	MODE : ARP	: ICMP	: VIRTUAL SERVER :
And V	10.4.1.4	0	ALL NODES (255)	ENABLED	NetScalar IP	Active ENAB	ED ENABLED	-N/A-
p.(0 10.4.2.4	0	ALL NODES (255)	ENABLED	Virtual IP	Active ENAB	ED ENABLED	ENABLED
1944 1940	10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Active ENAB	ED ENABLED	ENABLED
	0.4.3.4	0	ALL NODES (255)	ENABLED	Subnet IP	Active ENAB	ED ENABLED	-N/A-
Insert Daixte	Total 4						25 Per Page 🗸	Page 1 of1
IP ADDRESS No turu	Insert Close							
Cruce Close								

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.

← Create IP Set	IPV4s 3									G×
Name*	Add Edit	Add Edit Delete Statistics Select Action								
ipset1	Q. Click here to searc	here to search or you can enter Key : Value format								
Traffic Domain		IP ADDRESS 0	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER
		10.4.1.5	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
10.4 D.4		10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED
15-6-4 15-6.0		10.4.3.5	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
Insert Delete	Total 3							25 Per Pa	se 🗡 Page	1 of 1 🚽 🕨
IP ADDRESS	Insert	Close								
Nostems										

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.

← Load Balancing Virtual Server

Basic Settings		
Create a virtual server by specifying a name, an IP i area network (LAN) or wide area network (WAN), th You can configure multiple virtual servers to receive Nermet	address, a port, and a protocol type. If an application is accessible fro te VIP is usually a private (ICANN: non-routable) IP address, e client requests, thereby increasing the availability of rosources to p	m the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local rocess client requests.
vi (i)		
Destaced		
HTTP		
IP Address Type*		
IP Address V		
IP Address*		
10 . 4 . 2 . 4		
Port"		
80 ()		
Iraffic Doman UP Range IP Set settings UP ust UP us	Add	Vertual Server State Infil Seale AppTox Logsins Tetain Connections on Cluster
IPSet Ippet1 V Redirection Mode* P Based V	Add Edit ()	
Listen Priority		

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 5konfigurierten Dienst aus und klicken Sie auf "Binden".

NetScaler VPX 14.1

6 Lood	Ralancing Virtual Server	Service Bind	ng > Service							
n Luau		Service	0							×
		Select	Add Edit							
		Q. Clickhere t	o search or you can enter Key : Value format							0
		0	NAME	STATE :	IP ADDRESS/DOMAIN NAME	TRAFFIC DOMAIN	PORT :	PROTOCOL :	MAX CLIENTS :	MAX REQU
	DOWN 10124		azurelbdhsservice0	• UP	168.63.129.16	0	53	DNS	0	
			sl	●UP	10.4.3.6	0	80	HTTP	0	
			2	●UP	10.4.3.7	0	80	HTTP	0	
		Total 3						25 Per Page	⊻ Page 1 of1	$\prec \rightarrow$

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.

Q Search Menu		System > High Availability > Nodes						
Favorites	×	Nodes 🕐						C 😭
AZURE	>	Add Edit Delete Statistics	Select Action 🖂					
System	\sim	D D : IP ADDRESS	Force Synchronization STER STATE	: NODE STATE	: IND :	SYNCHRONIZATION STATE :	SYNCHRONIZATION HAILURE REASON	
Licenses		0 10.4.1.4	citro-ado-1 Primery	O UP	ENABLED	ENABLED	-N/I-	
Settings		1 10435	Torce Failzver	• UP	FNARLED	SUCCESS	NA .	
Diagnostics		lotal 2					25 Per Page ∨ Page I of I	
High Availability	\sim							
Nodes								
Route Monitors								

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).

Home > mysite.net									
mysite.net							\$? >		
	$\overset{\bullet}{\bullet} \text{Record set} \rightarrow \text{Mov}$	ve 菌 Delete zone 💍	Refresh						
Overview	Resource group (change) gslb_phase2			Name server 1 -	Name server 1 -				
Activity log	Subscription (change)	pagawai@strik.com		Name server 2 -					
Access control (IAM)	Subscription ID 764bc6a9-7927-4311-8et	57-ed073090cea3	Name server 3	Name server 3					
 lags Diagnose and solve problems 				Name server 4					
Settings	Tags (change) Click here to add tags								
Properties				*					
Locks	✓ Search record sets								
Automation script	NAME	ТҮРЕ	TTL	VALUE	ALIAS RESOURCE TYPE	ALIAS TARGET			
Monitoring				Email: azuredns-ho Host: internal.clou					
🔑 Alerts	@	SOA	3600	Refresh: 3600 Retry: 300					
Metrics				Expire: 2419200 Minimum TTL: 300 Serial number: 1					
Support + troubleshooting									
New support request									

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.

Virtual network							
	« 👌 Refr	esh 🔶 Move 📋 [Delete				
-> Overview	Resource GSLB_Ph	egroup (<u>change</u>) ase2		Address space 10.8.0.0/16			
Activity log	Location			DNS servers			
Access control (IAM)	Subscrip	tion (change)		10.8.0.6			
Tags	NO W	lations Of annual ages	elêdirîk.com				
Ciagnose and solve problems	Subscrip 764bc6a	tion ID 9-7927-4311-8e67-ed0	73090cea3				
ettings	Tags (cha	inge)					
> Address space	_ Click here	to add tags		*			
Connected devices	Conne	cted devices					
> Subnets	,⊅ Sea	rch connected devices					
DDoS protection	DEVICE		↑↓ ТҮРЕ	1 IP ADDRESS		SUBNET	
Firewall (Preview)	nsvnet	a210	Network interface	10.8.0.4		default	
DNS servers	nsvnet	a210	Network interface	10.8.0.5		default	
2 Peerings	dosfor	warder962	Network interface	10.8.0.6		default	
Service endpoints	dilbroi			10.8.0.7		default	
	clienty	neta27	Network interface				
Properties	clientv	neta27	Network interface	10.0.0.7			
Properties Cocks Come > Virtual_Network_B_10_9 Virtual_Network_B_10_9	Azure2	neta27 AwsGW	Network interface Virtual network gateway	-		GatewaySubnet	
Properties Locks Virtual_Network_B_10_9 Virtual_Network_B_U_9 Virtual_network	clientv Azure2	neta27 AwsGW	Network interface Virtual network gateway	-		GatewaySubnet	,
Properties Locks Ome > Virtual_Network_B_10_9 Virtual_Network_B_ Virtual_network Search (Ctrl+/)	10_9	sh → Move 🍈 D	Network interface Virtual network gateway	-		GatewaySubnet	;
Properties Locks Virtual_Network_B_10_9 Virtual_Network_B Virtual_network Search (Clrl+/) Voreview	10_9 « Č Refre GSLB_Ph/	sh → Move III D group (change) sse2	Network interface Virtual network gateway	- - Address space 10.9.0.0/16		GatewaySubnet	
Properties Locks Overview Averview Activity log Properties	Clientv Azure2	sh → Move iii D group (<u>changs</u>) sse2	Network interface Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	;
Properties Locks Ortual_Network_B_10_9 Virtual_Network_B_ Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM)	Clientvi Azure2	sh → Move 10 D group (change) se2	Network interface Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
Properties Cocks Virtual_Network_B_10_9 Virtual_Network_B_ Virtual_network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags	10_9 « Č Refre Resource GSLB_Pha Location West US Subscript	sh → Move 🛍 D group (change)	Network interface Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	
Properties Cocks Virtual_Network_B_10_9 Virtual_Network_B_ Virtual_network Search (Ctrl+/) Overview Activity log Activity log Access control (IAM) Tags Diagnose and solve problems	10_9	sh → Move 1 D group (change) ise2 ion (change) ion ID -7927-4311-8e67-ed07	Network interface Virtual network gateway elete elete	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
Properties Cocks Properties Cocks Proventies Virtual_Network_B_10_9 Virtual_Network_B_ Virtual_network Cocks Co	10_9	sh → Move iii D group (change) ion (change) ion ID -7927-4311-8e67-ed07 nge)	Network interface Virtual network gateway elete 23090cea3	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
Properties Cocks Properties Cocks Cocks Properties Virtual_Network_B_10_9 Virtual_network Virtual_network Cocks Cock	10_9	sh → Move iii D group (change) ion (change) ion (change) ion 12D r927-4311-8e67-ed07 nge) to add tags	Network interface Virtual network gateway elete '3090cea3	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
Properties Locks Virtual_Network_B_10_9 Virtual_network Virtual_network Search (Ctrl+,) Overview Activity log Access control (IAM) Tags Diagnose and solve problems tttings Address space Connected devices	II0_9 « V Refre GSLB_Pha Location West US Subscript Subscript T64bc6as Tags (cha Click here Conne-	sh → Move III D group (change) ion (change) ion ID .7927-4311-8e67-ed07 nge) to add tags cted devices	Network interface Virtual network gateway elete	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
 Properties Locks come > Virtual_Network_B_10_9 Virtual_network Virtual_network Search (Clrl+.) Overview Activity log Access control (IAM) Tags Diagnose and solve problems sttings Address space Connected devices Subnets 	10_9 « Conner Subscript Subscript Subscript Conner Conner Sear	sh → Move III D group (change) ion (change) ion (change) ion ID -7927-4311-8e67-ed07 nge) to add tags cted devices ch connected devices	Network interface Virtual network gateway elete '3090cea3	Address space 10.9.0.0/16 DNS servers 10.9.0.6		GatewaySubnet	,
 Properties Locks ome > Virtual_Network_B_10_9 Virtual_network Search (Clrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems sttings Address space Connected devices Subnets DDoS protection 	I0_9 « Č Refre Resource GSLB_PhA Location West US Subscript Subscript Goldscraft Conne Sear Device	sh → Move III D group (change) ion (change) ion (change) ion add tags cted devices cted devices	Network interface Virtual network gateway elete '3090cea3	Address space 10.9.0.0/16 DNS servers 10.9.0.6	P4	GatewaySubnet	,
 Properties Locks Virtual_Network_B_10_9 Virtual_Network_B Virtual_network Virtual_network Virtual_network Activity log Access control (IAM) Tags Access control (IAM) Tags Diagnose and solve problems ettings Address space Connected devices Subnets DDoS protection Firewall (Preview) 	ID_9 « Connee Subscript Tags (cha Connee Connee Seer DEVICE Serverv	AwsGW	Network interface Virtual network gateway elete elete '3090cea3 '5 TYPE Network interface	Address space 10.9.0.0/16 DNS servers 10.9.0.6 * * 10.9.0.4	¢4	GatewaySubnet GatewaySubnet SUBNET default	,
 Properties Locks Come > Virtual_Network_B_10_9 Virtual_Network_B Virtual_network D Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Access control (IAM) Tags Diagnose and solve problems ettings Address space Connected devices Subnets DDoS protection Firewall (Preview) DNS servers 	I0_9	sh → Move i D group (change) ion (change) ion (change) ion (change) to add tags cted devices ch connected devices hetb216 etb294	Network interface Virtual network gateway elete elete '3090cea3 ' TYPE Network interface Network interface	Address space 10.9.0.0/16 DNS servers 10.9.0.6	¢4	GatewaySubnet GatewaySubnet	,
 Properties Locks Come > Virtual_Network_B_10_9 Virtual_Network_BVertual_Network_BVertual_network O Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Access control (IAM) Tags Diagnose and solve problems ettings Address space Connected devices Subnets DDoS protection Firewall (Preview) DNS servers Peerings 	10_9	sh → Move i D group (change) ion (change) ion (change) ion 2727-4311-8e67-ed07 nge) to add tags cted devices cted devices cted devices cted devices	Network interface Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6 * * * * * * * * * * * *	÷.	GatewaySubnet Ga	
 Properties Locks Locks Virtual_Network_B_10_9 Virtual network Virtual network O Search (Ctrl+/) Osearch (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems ettings Address space Connected devices Subnets DoDS protection Firewall (Preview) DNS servers Peerings Service endpoints 	10_9	sh → Move D AwsGW sh → Move D Group (change) ion (change) ion (change) ion 10 -7927-4311-8e67-ed07 nge) to add tags cted devices cted devices etb216 etb294 ardervnetb709	Network interface Virtual network gateway	Address space 10.9.0.0/16 DNS servers 10.9.0.6 * IP ADDRESS 10.9.0.4 10.9.0.5 10.9.0.5	¢4	GatewaySubnet GatewaySubnet	,

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.

Vnet_A_to_E	} _8]
R Save X Di	iscard 🧰 Delete	
Name		
Vnet_A_to_B		
Peering status		
Connected		
Provisioning state		
Succeeded		
Peer details		
Address space		
10.9.0.0/16		
Virtual network		
Virtual_Network_B	_10_9	
Configuration		
Allow virtual potw		
Disabled Enal		
 Allow forward 	ed traffic 🚯	
✓ Allow gateway	y transit 🕦	
Use remote a	ateways 🕦	

Die folgende Abbildung zeigt das erfolgreiche Peering von VNet A zu VNet B.

Home > Virtual_Network_A_10_8 - Peer	rings			
Virtual_Network_A_10_8	3 - Peerings			
	< Add			
<> Overview	Search peerings			
Activity log	NAME	PEERING STATUS	PEER	GATEWAY 1
Access control (IAM)	Vnet_A_to_B	Connected	Virtual_Network_B_10_9	Enabled
🛹 Tags				

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)					
		Ho	ome > Virtual_Network_B_*	10_9 - Peerin	gs	
		<u></u>	Virtual_Network	_B_10_9 -	Pee	erings
		2) Search (Ctrl+/)	«	-	- Add
		\Leftrightarrow	Overview			𝒫 Search peering
		=	Activity log			NAME
		•	Access control (IAM)			Vnet_B_to_A
Die fo	lgende Abbildung zeigt das erfolgreiche Peering von VNet B zu VNet A	-	Tags		La	

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.

- 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

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

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:



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 "ptm.mysite.net" {
9
10
               type forward;
11
               forwarders {
12
13
     10.8.0.5;
                 }
14
     ;
           }
15
16
     ;
```

Denn mysite.netwir 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:

Ġ Load Balancing Service	ancing Service
--------------------------	----------------

Service Name*					
s_adns	?				
O New Server					
Server*					
10.8.0.5 (10.8.0.5)	\sim				
Protocol*					
ADNS	\sim				
Port*					
53					
æ	Load	Ba	lanci	na	Service
---	------	----	-------	-----	---------
	Louu	Du	anci	''Y	Jervice

	basic settings	
S	Service Name*	
	ADNS_TCP	
(New Server Existing Server	
I	P Address*	
	10 . 8 . 0 . 5	
F	Protocol*	
	ADNS_TCP V	
F	Port*	
	53	
Þ	More	
Q Search in Menu	Traffic Management / Load Balancing / Services / Services	
System	Services	
Traffic Management	 Services 2 Auto Detected Services 0 Internal Services 7 	
Load Balancing	✓ Add Edit Delete Statistics No action ✓	Search 🗸
Virtual Servers ☆ Services	Name State IP Address/Domain Name Port Protocol Max Clients Max Requests Cache T	Type Traffi <u>c Don</u>
Service Groups	azurelbdnsservice0 DOWN 168.63.129.16 53 DNS 0 0 SERVER	
Monitors	□ s_adns ●UP 10.8.0.5 53 ADNS 0 0 SERVER	

GSLB-Sites hinzufügen

- 1. Fügen Sie lokale und Remote-Sites hinzu, zwischen denen GSLB konfiguriert wird.
- 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.

Name*	_
s1	0
Туре	_
LOCAL V	
Site IP Address*	
10 . 8 . 0 . 5]
Public IP Address	
10 . 8 . 0 . 5]
Parent Site Backup Parent Sites Parent Site Name	
~]
Trigger Monitors*	J
ALWAYS V]
Cluster IP	
Public Cluster IP	
NAPTR Replacement Suffix	
Metric Exchange	
Network Metric Exchange	2
Persistence Session Entry	Exchang

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

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.

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

Server Name*	
10.8.0.6	\sim
Server IP*	
10 . 8 . 0 . 6	
Public IP	
10 . 8 . 0 . 6	
Public Port	
80	
 Enable after Creating 	
🖌 Enable Health Monitoring	
AppFlow Logging	
Comments	

- 5. Nachdem Sie den Dienst erstellt haben, wechseln Sie im GSLB-Dienst zur Registerkarte **Erweit**erte Einstellungen .
- 6. Klicken Sie auf **Monitor hinzufügen**, um den GSLB-Dienst mit einem HTTP-Monitor zu

	GSLB Service Load Balancing Monitor Binding								
	Add Binding	g Edit Bi	nding	Unbind	Edit Monitor				
		Monitor Name		Weight	State	Current State	Las		
ndon und don Dionststatus aufzurufon		http		1	true	●UP	Suc		
iden und den Dienststatus aufzururen.									

7. Sobald Sie sich mit dem HTTP-Monitor verbinden, wird der Status der Dienste als UP markiert,

Q Search in Menu		Traffic Management / GSLB / GSLB Services							
System > AppExpert > Traffic Management ~		GSLB Services							
		Add	Edit Delete	Statistics	No action 🗸 🗸				
Load Balancing	>		Name	State	Effective State	IP Address	Port		
Content Switching	<u> </u>		service_vnetA	OUP	DOWN	10.8.0.6	80		
Cache Redirection	•		service_vnetB	• UP	DOWN	10.9.0.4	80		
DNS	>		service_Aws	• UP	DOWN	10.12.0.31	80		

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.

GSLB Virtual Server

Basic Settings	
Name*	
vserver_m	
DNS Record Type*	
Α 🗸	
Service Type*	
HTTP V	
Enable after Creating	
AppFlow Logging	
When this Virtual Server is DOWN	
Do not send any service's IP address in response	e (EDR)
When this Virtual Server is UP	
Send all "active" service IPs' in response (MIR)	
EDNS Client Subnet	
Respond with ECS option in the response for a l	DNS query with ECS
Validate ECS address is a private or unroutable a	address

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.

GSLB Virtual Server Domain Binding										
GSLB Virtual Server Domain Binding										
Add Binding Edit Bindin	g Unbind	Show B								
FQDN	TTL (secs)	Backup IP	Cookie Domain	Cookie Time-out (mins)	Site Domain TTL (secs)					
rr.ptm.mysite.net	5			0	3600					
Close										

- 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.

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

Nach dem Binden der GSLB-Dienste und der Domäne an den virtuellen Server wird es wie in der folgenden Abbildung dargestellt angezeigt:

GSLB Virtual Server

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

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.

NetScaler VPX 14.1

Q Search in Menu		Traffic Manage	ment / GSLB / GSLB Virtual Serve	rs		
System >		GSLB Vi	rtual Servers			
AppExpert	>					
Traffic Management	\sim	Add	dit Delete Statistics	No action 🗸		
☆ Load Balancing	>	•	Name	State	Protocol	% Health
Content Switching	•		vserver_rr	• UP	HTTP	100.00% 3 UP/0 DOWN
Cache Redirection	<u> </u>		vserver_sp	● UP	HTTP	100.00% 3 UP/0 DOWN

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.

\equiv Microsoft Azure	ho Search resources, services, and do	ocs (G+/)	D 🖓	🖓 🅸 ? 😊
Home >				
Marketplace				
Recently created	🔎 Citrix ADC	X Pricing : All X Oper	rating System : All 🗙 Publisher T	ype:All 🗙
Service Providers		Offer Type : All X	Publisher name : All $ imes$	
Private Offers	Showing All Results			
Categories				
	citrix.	citrix.	citrix.	citrix.
Get Started	Citrix ADC 13.0	Citrix ADC	Citrix ADC 13.0 - Azure Stack	Citrix ADC VPX FIPS
AI + Machine Learning				
Analytics	Citrix	Citrix	Citrix	Citrix
, analy and	Virtual Machine	Azure Application	Virtual Machine	Virtual Machine
Blockchain	Citrix Application Delivery Controller:	Citrix Application Delivery Controller:	Citrix Application Delivery Controller:	Citrix Application Delivery Contr
Compute	Load Balancer, SSL VPN, WAF & SSO	Load Balancer, SSL VPN, WAF & SSO	Load Balancer, SSL VPN, WAF & SSO	Load Balancer, SSL VPN, WAF &
*				
	Software plan starts at	Price varies	Bring your own liconco	Rring your own license
	rice		bring your own license	bring your own license
	Create 🗸 🛇	Create 🗸 💙	Create 🗸 💙	Create 🗸

3. Wählen Sie einen NetScaler-Plan ohne FIPS zusammen mit der Lizenz aus und klicken Sie auf **Erstellen**.

	Microsoft Azure	Search resources, services,	and docs (G+/)		▶_	Ę
Home						
NetS	caler ADC 14	l.1 ☆ …				
netisca	NetScale	er ADC 14.1 🗢 Add	to Favorites			
	Cloud Software	Group Virtual Machine				
	Free trial					
	Plan					
	NetScaler ADC	14.1 VPX Bring Your O 🗸	Create	Start with a pre-set configuration		
	Want to deploy	programmatically? Get started				
Overv	iew Plans + Pricing	3 Usage Information + Su	oport Ratir	ıgs + Reviews		
NetSc and pr the hy	ler ADC (formerly NetS icing flexibility to meet brid cloud.	caler) is an enterprise-grade app your business' unique needs. De	plication deliver esigned to provi	y controller that delivers your applications q de operational consistency and a smooth us	uickly, reli er experie	ably, ence,

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

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.

Home > NetScaler ADC 14.1 >

Create a virtual machine

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

5. 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.

Define network connectivity for your virtual machine by configuring network inter inbound and outbound connectivity with security group rules, or place behind an Learn more Network interface When creating a virtual machine, a network interface will be created for you. Virtual network * ① (new) vpx-aan-vnet Create new Subnet * ① (new) default (10.6.0.0/24) Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None ● Basic △ Advanced Public inbound ports * ① None ● Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traff	erface card (NIC) settings. You can control por n existing load balancing solution.
Network interface When creating a virtual machine, a network interface will be created for you. Virtual network * ① (new) vpx-aan-vnet Create new Subnet * ① (new) default (10.6.0.0/24) Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None ● Basic Advanced Public inbound ports * ① None ● Allow selected ports SsH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered	
When creating a virtual machine, a network interface will be created for you. Virtual network * ① (new) vpx-aan-vnet Create new Subnet * ① (new) default (10.6.0.0/24) Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None ● Basic ○ Advanced Public inbound ports * ① None ● Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered for testing.	
Virtual network * ① (new) vpx-aan-vnet Create new Subnet * ① Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None Basic Advanced Public inbound ports * ① None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered	
Initial network Image: Subnet *	
Subnet * ① (new) default (10.6.0.0/24) Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None Basic Advanced Public inbound ports * ① None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered	
Public IP ① (new) vpx-aan-ip Create new NIC network security group ① None Basic Advanced Public inbound ports * None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered	
Public IP () (new) vpx-aan-ip Create new NIC network security group () None Basic Advanced Public inbound ports * () None Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use the create rules to limit inbound traffered to the set of the se	
NIC network security group NIC network security group None Advanced None Allow selected ports Select inbound ports * Select inbound ports * Select inbound ports * Select inbound ports * None This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traffered	
NIC network security group NOne Basic Advanced Public inbound ports * None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traff	
 Basic Advanced Public inbound ports * None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use the create rules to limit inbound traffic 	
Public inbound ports * None None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traff	
Public inbound ports * None Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use to create rules to limit inbound traff	
Allow selected ports Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use th create rules to limit inbound traff	
Select inbound ports * SSH (22) This will allow all IP addresses to recommended for testing. Use the create rules to limit inbound trafference in the second secon	
This will allow all IP addresses to recommended for testing. Use the create rules to limit inbound trafference in the create rules to l	
	to access your virtual machine. This is only the Advanced controls in the Networking tab to ffic to known IP addresses.
Delete public IP and NIC when VM is deleted ①	
Enable accelerated networking 🕕 🔽	
Load balancing	
You can place this virtual machine in the backend pool of an existing Azure load b	balancing solution. Learn more 🗹
Load balancing options (i)	
Azure load balancer	
Supports all TCP/UDP network tra	
Web traffic load balancer for HTT	raffic, port-forwarding, and outbound flows.
Load balancing options () None	balancing solution. Learn more d
	raffic port-forwarding and outbound flows
Application gateway Web traffic load balancer for HTT	raffic, port-forwarding, and outbound flows.
Web traffic load balancer for HTT	raffic, port-forwarding, and outbound flows.

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.

≡ Microsoft Azure 🖉 Search	n resources, services, and docs (G+/)		; 🗘 🐵	? 🙂
Home > citrix.netscalervpx-1vm-3nic-20	0210204125107 > test-aan- > citrix.netscalervpx-1vm-3nic-20210204	4125107 >		
✓ Search (Ctrl+/) «	$+$ Add $\equiv\equiv$ Edit columns 📋 Delete resource group 🖒 Refresh	🛓 Export to CSV 🥳	Open query	🖉 Assign t
😥 Overview	↑ Essentials			
Activity log	Subscription (change) NSDev Platform CA	Deployments 2 Succeeded		
Access control (IAM)	Subscription ID	Location		
🔷 Tags	/64bc6a9-/92/-4311-8e6/-ed0/3090cea3	South India		
🗲 Events	Tags (change) Click here to add tags			
Settings	Filter for any field Type == all × Location == all ×	+ Add filter		
1 Deployments	Showing 1 to 22 of 22 records. Show hidden types ①		No grouping	
Security				
Policies	Name ↑↓	Type ↑↓	_	Location
🔁 Properties	Citrix-adc-vpx-0	Virtual machine		South Ce
🔒 Locks	< Previous Page 1 V of 1 Next >			

 Um die Konfigurationen f
ür beschleunigte Netzwerke zu
überpr
üfen, w
ählen Sie Virtuelle Maschine > Netzwerk
aus. Der Status "Beschleunigtes Netzwerk" wird f
ür jede Netzwerkkarte als Aktiviert oder
Deaktiviert** angezeigt.

■ Microsoft Azure	resources, services, and doc	s (G+/)		D. [7	₽ @ ?	©
Home > citrix.netscalervpx-1vm-3nic-202 citrix-adc-vpx-0 Virtual machine	10204125107 > test-aan tworking & Attach network inter	·	rvpx-1vm-3nic-20210204125107 rk interface	> test-aan	> citrix-adc-v	px-0
Overview Activity log Access control (IAM) Tans	citrix-adc-vpx-nic01-0	citrix-adc-vpx-nic1	1-0 citrix-adc-vpx-nic12-0	C	3	
 Diagnose and solve problems Settings Naturalization 	Network Interface Virtual network/subnet: Accelerated netwo	: citrix-adc-vpx-nic01 citrix-adc-vox-virtual-net rking: Enabled	-0 Effective security rules twork/01-management-subnet	Topology NIC Public IP: 1	3.66.88.43 NI	C Private IP: 172.17.40.5
retworking Connect Disks	Network security of Impacts 0 subnets,	Outbound port rules group citrix-adc-vpx-nic 1 network interfaces	Application security groups	Load balan hterface: citrix-a	cing adc-vpx-nic01-0)	Add inbound p
Size Security Advisor recommendations	Priority 1022	Name A ssh-22-rule	Port 22	Protocol TCP	Source	Destination

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:**

Hinweis:

Stellen Sie sicher, dass Sie die VM beenden, bevor Sie Accelerated Networking mit Azure Power-Shell 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.

Wenn Sie sich im Bash-Modus befinden, wechseln Sie in den PowerShell-Modus.



2. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

1 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:

```
1 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:

```
1 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.

■ Microsoft Azure	h resources, services, and doo	is (G+/)			₽ 🕸 ? 😳	
Home > citrix.netscalervpx-1vm-3nic-20	0210204125107 > test-aar	· > citrix.netscalerv	ox-1vm-3nic-202102041251	107 > test-aan	> citrix-adc-vpx-0	
citrix-adc-vpx-0 N	etworking					
	🖉 Attach network inter	face ್ರ ^{ರ್} Detach network	interface			
Overview		_				
 Activity log 	citrix-adc-vpx-nic01-0	citrix-adc-vpx-nic11-	0 citrix-adc-vpx-nic12-0			
Access control (IAM)	IP configuration (i)	_		L3		
🗳 Tags	nsip (Primary)	\sim				
Diagnose and solve problems	Network Interface	citrix-adc-vpx-nic01-0	Effective security rules	Topology		
Settings	Virtual network/subnet Accelerated netwo	citrix-adc-vpx-virtual-netwo rking: Enabled	ork/01-management-subnet	NIC Public IP: 13.6	6.88.43 NIC Private	e IP: 172.17.40.5
2 Networking						
S Connect	Inbound port rules	Outbound port rules	Application security grou	ps Load balancin	g	
B Disks	Network security Impacts 0 subnets,	group citrix-adc-vpx-nic0 1 network interfaces	1-nsg-0 (attached to netwo	rk interface: citrix-adc	-vpx-nic01-0)	Add inbound p
💶 Size	Priority	Name	Port	Protocol	Source	Destinatio
Security	1022	▲ ssh-22-rule	22	TCP	Internet	Any
Advisor recommendations						

Im folgenden Beispiel sehen Sie, dass Accelerated Networking **deaktiviert**ist.

	Microsoft Azure	𝒫 Search re	esources, services, and do	cs (G+/)		E E	0 @ ? ©	
Hor	ne > citrix-adc-vpx-0							
Ŕ	citrix-adc-vpx	- 0 Net	tworking					×
٩	Search (Ctrl+/)	~	🖉 Attach network inte	erface 🖉 Detach network in	nterface			
ጽ	Access control (IAM)	*						
0	Tags	- 11	citrix-adc-vpx-nic01-	0 citrix-adc-vpx-nic11-0	citrix-adc-vpx-nic12-	0		
Þ	Diagnose and solve problem:	5	IP configuration ①	-				
Sett	ings		nsip (Primary)	\sim				
2	Networking		Network Interfac	e: citrix-adc-vpx-nic01-0	Effective security rule	s Topology		
ø	Connect		Virtual network/subnet Accelerated network	t: citrix-adc-vpx-virtual-networ orking: Disabled	k/01-management-subnet	t NIC Public IP: 13.6	6.88.43 NIC Private IF	2: 172.17.40.5
8	Disks							
•	Size		Inbound port rules	Outbound port rules	Application security gro	oups Load balanci	ng	
٢	Security		Network security	group citrix-adc-vpx-nic01-	nsg-0 (attached to netw	ork interface: citrix-ad	c-vpx-nic01-0)	Add inbound port rule
	Advisor recommendations		Impacts 0 subnets	, 1 network interfaces				
	Extensions		Priority	Name	Port	Protocol	Source	Destination
6	Continuous delivery		1022	▲ ssh-22-rule	22	TCP	Internet	Any
		-	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork -

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</up,loopback,running,multicast>
options=3 <rxcsum,txcsum></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></performnud,accept_rtadv>
0/1: flags=8843 <up,broadcast,running,simplex,multicast> metric 0 mtu 1500</up,broadcast,running,simplex,multicast>
options=80019 <rxcsum,vlan_mtu,vlan_hwtagging,linkstate></rxcsum,vlan_mtu,vlan_hwtagging,linkstate>
ether 00:0d:3a:98:71:be
inet 172.16.27.11 netmask 0xfffff00 broadcast 172.16.27.255
inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
nd6 options=3 <performnud,accept_rtadv></performnud,accept_rtadv>
media: Ethernet autoselect (10Gbase-T <full-duplex>)</full-duplex>
status: active
1/1: flags=8802 <broadcast,simplex,multicast> metric 0 mtu 1500</broadcast,simplex,multicast>
options=80019 <rxcsum,vlan_mtu,vlan_hwtagging,linkstate></rxcsum,vlan_mtu,vlan_hwtagging,linkstate>
ether 00:22:48:1c:99:3e
media: Ethernet autoselect (10Gbase-T <full-duplex>)</full-duplex>
status: active
50/1: flags=8842 <broadcast,running,simplex,multicast> metric 0 mtu 1500</broadcast,running,simplex,multicast>
options=900b8 <vlan_mtu,vlan_hwtagging,jumbo_mtu,vlan_hwcsum,vlan_hwfilter,linkstate></vlan_mtu,vlan_hwtagging,jumbo_mtu,vlan_hwcsum,vlan_hwfilter,linkstate>
ether 00:22:48:1c:99:3e
media: Ethernet autoselect (<unknown subtype="">)</unknown>
status: activo

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).



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

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).

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

flags=0xe460 <ENABLED, UP. UP. 802.1g>

MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d uptime 10h49m11s
1)
           Actual: media FIBER, speed NONE, duplex FULL, tctl NONE, throughput
n
           LLDP Mode: NONE,
                                                              LR Priority: 1024
           RX: Pkts(1135870) Bytes(1487381079) Errs(0) Drops(0) Stalls(0)
           TX: Pkts(1143020) Bytes(143165922) Errs(0) Drops(0) Stalls(0)
NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
 Done
```

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.
 - 1 add vlan 20
- 2. Binden Sie ein VLAN an die PV-Schnittstelle.

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

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

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.

	HA-ILB ☆ Resource group										
»	$+$ Add $\equiv\equiv$ Edit columns 🛍 Delete resource group 🖒	Refresh 🞍 Export to CSV 😚 Open query	🛛 🧔 Assign ta								
	∧ Essentials										
	Subscription (change):										
	Subscription ID : 764bcdar9-3123-4311-6a63-ed0734996cm	a									
	Tags (change) : Click here to add tags										
	Filter by name Type == (all) X Location	== (all) \times + Add filter									
	Showing 1 to 20 of 20 records. Show hidden types ①										
	\square Name \uparrow_{\downarrow}	Туре ↑↓	Location \uparrow_{\downarrow}								
	ADC-Availability-Set	Availability set	West US 2								
	📄 💠 ADC-Azure-Load-Balancer	Load balancer	West US 2								
	P ADC-VPX-0	Virtual machine	West US 2								
	📄 🛅 ADC-VPX-0-management-public-ip	Public IP address	West US 2								
	ADC-VPX-1	Virtual machine	West US 2								
	📄 🛅 ADC-VPX-1-management-public-ip	Public IP address	West US 2								
	ADC-VPX-NIC-0-01	Network interface	West US 2								
	ADC-VPX-NIC-0-11	Network interface	West US 2								
_	ADC-VPX-NIC-0-12	Network interface	West US 2								
	ADC-VPX-NIC-1-01	Network interface	West US 2								
	ADC-VPX-NIC-1-11	Network interface	West US 2								
	ADC-VPX-NIC-1-12	Network interface	West US 2								
_	ADC-VPX-NSG-0-01	Network security group	West US 2								
	ADC-VPX-NSG-0-11	Network security group	West US 2								
	ADC-VPX-NSG-0-12	Network security group	West US 2								
	ADC-VPX-NSG-1-01	Network security group	West US 2								

4. 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 ip								
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
1)	10.11.0.5		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.11.1.5		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.4		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								

> sh ha	node
1)	Node ID: 0
	IP: 10.11.0.5 (ADC-VPX-0)
	Node State: UP
	Master State: Primary
	Fail-Safe Mode: OFF
	INC State: ENABLED
	Sync State: ENABLED
	Propagation: ENABLED
	Enabled Interfaces : 0/1 1/1 1/2
	Disabled Interfaces : None
	HA MON ON Interfaces : None
	HA HEARTBEAT OFF Interfaces : None
	Interfaces on which heartbeats are not seen : $1/1 \ 1/2$
	Interfaces causing Partial Failure: None
	SSL Card Status: NOT PRESENT
	Sync Status Strict Mode: DISABLED
	Hello Interval: 200 msecs
	Dead Interval: 3 secs
	Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)	Node ID: 1
	IP: 10.11.0.4
	Node State: UP
	Master State: Secondary
	Fail-Safe Mode: OFF
	INC State: ENABLED
	Sync State: SUCCESS
	Propagation: ENABLED
	Enabled Interfaces : 0/1 1/1 1/2
	Disabled Interfaces : None
	HA MON ON Interfaces : None
	HA HEARTBEAT OFF Interfaces : None
	Interfaces on which heartbeats are not seen : $1/1 \ 1/2$
	Interfaces causing Partial Failure: None
	SSL Card Status: NOT PRESENT
Done	

Auf dem sekundären Knoten (ADC-VPX-1)

> sh ip								
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
1)	10.11.0.4		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.11.1.6		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.5		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								
s 📕								



- 5. Nachdem die primären und sekundären Knoten aktiv sind und der Synchronisierungsstatus ER-FOLGREICHist, 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**.

≡ Microsoft Azure	𝒫 Search resources, services, and docs (G+/)	<u>ک</u>	Ŗ	© ©					
Home > Test_HA_Deployment > ADC-Azure-Load-Balancer ADC-Azure-Load-Balancer Frontend IP configuration									
Search (Ctrl+/) Overview									
Activity log	Name IP address		Ri	ules count					
 Access control (IAM) Tags 	ADC-Load-Balancer-Frontend-IP-Configuration-rule 10.11.1.4		1						
🤌 Diagnose and solve problem	ns								

7. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung beim Erstellen der LB-Regel, Back-End-Pools und Gesundheitsproben.

SE ADC-Azure-Load-Balancer Load balancing rules										
Ø Search (Ctrl+/) ≪	+ Add									
Activity log	P Search load balancing rul									
Access control (IAM)	Name	↑↓ Load balancing rule	↑↓ Backend pool	¢ψ	Health probe \uparrow_\downarrow					
🤣 Tags	lbRule1	IbRule1 (TCP/80)	ADC-Load-Balancer-Ba	kend-rule	ADC-Load-Balancer-Health-Probe-rule	ŀ				
Diagnose and solve problems										
Settings										
Frontend IP configuration										
Backend pools										
Health probes										
i≡ Load balancing rules										

• Die LB-Regel (LBrule1) verwendet standardmäßig Port 80.

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

lbRule1	
ADC-Azure-Load-Balancer	
🔚 Save 🗙 Discard 🔟 Delete	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination access a group of backand and instances. Only backand instances that the backth problem	
considers healthy receive new traffic.	
Name *	
IP Version *	
● IPv4	
Frontend IP address * ①	
10 11 1 4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule)	$\mathbf{\mathbf{v}}$
Protocol	
Port *	
443	
Backend port * ①	
443	
Backand pool	
ADC Load Balancer Backand rule (2 virtual machinee)	
	~
Health probe ①	
ADC-Load-Balancer-Health-Probe-rule (TCP:9000)	\sim
None	\sim
Idle timeout (minutes) ①	
0	4
Floating IP ①	
Enabled	

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.

Home > HA-ILB > ADC-Azure-Load-Balancer							
BADC-Azure-Lo	oad-B	alancer Frontend IP configuration					
		🕂 Add 🖒 Refresh					
Activity log	•	Q Filter by name					
Access control (IAM)		Name	IP address				
🔶 Tags		ADC-Load-Balancer-Frontend-IP-Configuration-rule	10.11.1.4				
Diagnose and solve problem	ns						
Settings	•						
Frontend IP configuration							

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**.

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

3. 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.

Home > HA-ILB > ADC-Azure-Load-Balancer								
ADC-Azure-Load-Balancer Frontend IP configuration Load balancer								
		+ Add 💍 Refresh						
💠 Overview		Q Filter by pame						
Activity log			10 11					
Access control (IAM)		Name	IP address		Rules count			
		ADC-Load-Balancer-Fronte	10.11.1.4		1			
🔶 Tags		II B-Front-End-IP-2	10.11.1.7		0			
Diagnose and solve problems								

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.

Home > HA-ILB > ADC-Azure-Load-Balancer > Add load balancing rule ADC-Azure-Load-Balancer	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.	
0	
Name *	
lbrule2 ~	
IP Version * IPv4 IPv6 Frontend IP address * ①	
10.11.1.7 (ILB-Front-End-IP-2)	
Protocol TCP UDP Port * 3 443	
Backend port	
443 ~	
Backend pool ①	
ADC-Load-Balancer-Backend-rule (2 virtual machines)	
ADC-Load-Balancer-Health-Probe-rule (ICP:9000)	
Session persistence ①	
None V	
Idle timeout (minutes)	
6	
Floating IP ①	
Disabled Enabled	
ОК	

6. Jetzt zeigt die **Frontend-IP-Konfiguration** die angewendete LB-Regel an.
| Hom | he > HA-ILB > ADC-Azure-Loa
ADC-Azure-Load
Load balancer | ad-Balan
d-Bal | ^{cer}
ancer Frontend IP configu | iration | | |
|---------|--|-------------------|--|------------|-------|-------|
| م | Search (Ctrl+/) | | $+$ Add \circlearrowright Refresh | | | |
| | Overview | ^ | O Eilter by name | | | |
| | Activity log | | Name | IP address | Rules | count |
| | Access control (IAM) | | ADC-Load-Balancer-Frontend-IP-Configurati | 10.11.1.4 | 1 | |
| - | Tags | | ILB-Front-End-IP-2 | 10.11.1.7 | 1 | |
| ß | Diagnose and solve problems | | | | | |
| Set | tings | | | | | |
| | Frontend IP configuration | | | | | |

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.

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

5. Klicken Sie auf Weiter: VM-Konfigurationen.

Basics	VM Configurations	Network and Additional Settings Review + create	
Project d	etails		
Select the manage a	subscription to manage o Il your resources.	deployed resources and costs. Use resource groups like folders to organize and	
Subscripti	on * 🛈	xm-test-cs-shared	\sim
Re	esource group * i	(New) Test_HA_Internet Create new	\checkmark
Instance	details		
Region *	0	South India	\sim
Citrix ADC	Release Version * 🛈	12.113.0	
License Sul	bscription 🛈	Bring Your Own License	
Virtual Ma	chine name * 🛈	citrix-adc-vpx	
Administr	ator account		
Username	* (i)	praveenk	~
Authentica	tion type * 🕡	Password SSH Public Key	
Password *	· (i)	•••••	~
Confirm pa	assword *		V Passwor
Review	+ create < Prev	vious Next : VM Configurations >	

- 6. Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:
 - Konfigurieren Sie das Suffix für den öffentlichen IP-Domainnamen
 - Azure Monitoring Metricsaktivieren oder deaktivieren
 - BackendAutoscale aktivieren oder deaktivieren
- 7. Klicken Sie auf Weiter: Netzwerk- und Zusatzeinstellungen

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

8. Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Startdiagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

	vivi conligurations	Network and Additional Settings Review + create	
Boot diag	inostics		
Diagnostic	storage account * 🕡	(new) citrixadcvpxd7a2c4d49e	\sim
		Create New	
Network	Settings		
Configure	e virtual networks		
Virtual net	work * 🛈	(new) citrix-adc-vpx-virtual-network	\sim
		Create new	
Managem	ent Subnet * 🕠	(new) 01-management-subnet (10.17.4.0/24)	\sim
Client Sub	net * 🛈	(new) 11-client-subnet (10.17.5.0/24)	~
Server Sub	onet * 🛈	(new) 12-server-subnet (10.17.6.0/24)	~
Public IP	(Management)		
Managem	ent Public IP (NSIP) * 🕕	(new) citrix-adc-vpx-nsip	~
2		Create new	
Managem	ent Domain Name 🛈	citrix-adc-vpx-nsip-d7a2c4d49e	~
Managem	ent Domain Name 🛈	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.	cloudapp.azure.cor
Managem Public IP	ent Domain Name ① (Clientside)	citrix-adc-vpx-nsip-d7a2c4d49e .southindia.	cloudapp.azure.cor
Managem Public IP Clientside	ent Domain Name ① (Clientside) Public IP (VIP) * ④	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip	<pre>cloudapp.azure.con</pre>
Managem Public IP Clientside	ent Domain Name ① (Clientside) Public IP (VIP) * ③	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new	<pre>cloudapp.azure.com</pre>
Managem Public IP Clientside Clientside	ent Domain Name ① (Clientside) Public IP (VIP) * ④ Domain Name ④	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e	<pre>cloudapp.azure.com</pre>
Managem Public IP Clientside Clientside	ent Domain Name ① (Clientside) Public IP (VIP) * ④ Domain Name ④	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia.	<pre>cloudapp.azure.con </pre>
Managem Public IP Clientside Clientside Public Inb	ent Domain Name ① (Clientside) Public IP (VIP) * ④ Domain Name ④	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only)	<pre>cloudapp.azure.con </pre>
Managem Public IP Clientside Clientside Public Inb Ports open	ent Domain Name ① (Clientside) Public IP (VIP) * ④ Domain Name ④ pound Ports (Management for Management public I	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only) P ① None	<pre>cloudapp.azure.cor </pre>
Managem Public IP Clientside Clientside Public Inb Ports open	ent Domain Name ① (Clientside) Public IP (VIP) * ④ Domain Name ④ pound Ports (Management for Management public I	citrix-adc-vpx-nsip-d7a2c4d49e .southindia. (new) citrix-adc-vpx-vip Create new citrix-adc-vpx-vip-d7a2c4d49e .southindia. ent only) P () None () ssh (22)	Cloudapp.azure.cor

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.

Home > citrix.netscalervpx-1vm-3nic-20201006140352 >

🕂 Add 💷 Edit columns 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV	$\%$ $\%$ Open query $\%$ Assign tags $ ightarrow$ Move \sim
✓ Essentials	
Filter by name Type == all X Location == all X ⁺ Add filter	
Showing 1 to 23 of 23 records. 🔲 Show hidden types 🛈	
Name 1	Type ↑↓
citrix-adc-vpx-0	Virtual machine
eitrix-adc-vpx-0_OsDisk_1_6749f4a73c534051b0602ba6e3ec2cf8	Disk
📃 🖳 citrix-adc-vpx-1	Virtual machine
eitrix-adc-vpx-1_OsDisk_1_8fde7770497b4dbdba385715e81505c9	Disk
citrix-adc-vpx-nic01-0	Network interface
itrix-adc-vpx-nic01-1	Network interface
🗌 🌻 citrix-adc-vpx-nic01-nsg-0	Network security group
📄 🎈 citrix-adc-vpx-nic01-nsg-1	Network security group
🕼 citrix-adc-vpx-nic11-0	Network interface
🕼 citrix-adc-vpx-nic11-1	Network interface
🗌 💎 citrix-adc-vpx-nic11-nsg-0	Network security group
🗌 🎈 citrix-adc-vpx-nic11-nsg-1	Network security group
C itrix-adc-vpx-nic12-0	Network interface
🗌 🌆 citrix-adc-vpx-nic12-1	Network interface
Citrix-adc-vpx-nic12-nsg-0	Network security group
Citrix-adc-vpx-nic12-nsg-1	Network security group
Citrix-adc-vpx-nsip-0	Public IP address
citrix-adc-vpx-nsip-1	Public IP address
🗌 🧰 citrix-adc-vpx-vip	Public IP address
C 🔷 citrix-adc-vpx-vip-load-balancer	Load balancer
C +> citrix-adc-vpx-virtual-network	Virtual network
🔲 🖪 vitriv ada yay ya availability sat	Availability set

- 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 citrixadc-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	Туре	Mode	Arp	Icmp	Vserver	State
1.\	10 18 0 4		NetSceler TD	Active	 Enabled			Fnabled
2)	10.18.1.5	0	SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.18.2.4		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								
> _h h								
> sn n	a node							
T)	Node ID:	0 10 0 1 (==						
	IF: I Nodo Stata:	U.10.U.4 (ns-	vpx0)					
	Node State:	UP Deimoni						
	Master Stat	e: Frimary						
	TNC State	ENABLED						
	INC State:	ENABLED						
	Sync State:	ENABLED						
	Fropagation Enabled Int	arfaces : 0/1	1/1 1/2					
	Disphled Int	torfogog : No	1/1 1/2					
	Disabled interfaces : None							
	HA HEADTREA	T OFF Interfa	ces · None					
	Interfaces	on which hear	theats are not	- seen ·	1/1 1/	2		
	Interfaces	causing Parti	al Failure: No	ne.	-///	4		
	SSL Card St	atus: NOT PRF	SENT					
	Sync Status	Strict Mode:	DISABLED					
	Hello Inter	val: 200 msec	3					
	Dead Interv	al: 3 secs						
	Node in thi	s Master Stat	e for: 0:3:34:	21 (dav	s:hrs:m	in:sec)		
2)	Node ID:	1		· -				
	IP: 1	0.18.0.5						
	Node State:	UP						
	Master Stat	e: Secondary						
	Fail-Safe M	ode: OFF						
	INC State:	ENABLED						
	Sync State:	SUCCESS						
	Propagation	: ENABLED						
	Enabled Int	erfaces : 0/1	1/1 1/2					
	Disabled In	terfaces : No	ne					
	HA MON ON I	nterfaces : N	one					
	HA HEARTBEA	T OFF Interfa	ces : None					
	Interfaces	on which hear	tbeats are not	: seen :	1/1 1/2	2		
	Interfaces	causing Parti	al Failure: No	one				
	SSL Card St	atus: NOT PRE	SENT					
Done								

Auf dem sekundären Knoten (citrix-adc-vpx-1)



- 12. Nachdem der primäre und sekundäre Knoten UP sind und der Synchronisierungsstatus **ER-FOLG**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**.

Home > Test_HA_Template > alb Frontend IP con Load balancer	figuration			×
P Search (Ctrl+/) ≪	+ Add 🕐 Refresh			
Overview	Filter by name			_
Activity log	Name	IP address	Rules count	
Access control (IAM)	ipconf-11	52.172.55.197 (alb-publicip)	1	
Tags				
Diagnose and solve problems				
Settings				
Frontend IP configuration				
Backend pools				

14. Fügen Sie die eingehende Sicherheitsregel für den virtuellen Serverport 443 in der Netzwerksicherheitsgruppe der beiden Client-Schnittstellen hinzu.

Home > Test_HA_Template > ns-vpx-n	iic0-11 >								
• ns-vpx-nic-nsg0-11 Network security group	Â								×
₽ Search (Ctrl+/) «	$ ightarrow$ Move \lor 📋 I	Delete 💍 Refresh							
Overview									
Activity log	Resource group (char	nge) : Test_HA_Template			Custom security	rules:2 inb	ound, 0 outbour	nd	
Access control (IAM)	Location	: South India			Associated with	: 0 sub	onets, 1 network	interfaces	
Taos	Subscription (change) : xm-test-cs-shared							
Diagnose and solve problems	Subscription ID	: db99d808-6e89-480	a-96ae-3275fe	e61eed4					
Diagnose and some problems	Tags (change)	: Click here to add tag	s						
Settings	Inbound security rul	les							
📩 Inbound security rules	Priority	Name		Port	Protocol	Sourc	e	Destination	Action
🖈 Outbound security rules	1000	🔺 default-allow-ssh		22	TCP	Any		Any	Allow
Network interfaces	1010	Port_443		443	TCP	Any		Any	Allow
<-> Subnets	65000	AllowVnetInBound		Any	Any	Virtua	INetwork	VirtualNetwork	Allow
Properties	65001	AllowAzureLoadBalanc	erInBound	Any	Any	Azure	LoadBalancer	Any	Allow
A Locks 👻									
ns-vpx-nic-nsg1-11 Network security group fearch (Ctrl+/) «	↔ Move $∨$ 1 Def	lete 🖒 Refresh							×
💎 Overview 🄶									
Activity log	Resource group (change	e) : Test_HA_Template			Custom security	rules : 2 inbo	und, 0 outbound		
Access control (IAM)	Location	: South India			Associated with	: 0 subn	ets, 1 network inf	terfaces	
Tags	Subscription (change)	: <u>xm-test-cs-shared</u> (<u>h</u>							
Diagnose and solve problems	Subscription ID Tags (change)	: db99d808-6e89-480a-96 : Click here to add tags	bae-3275te61e	ed4					
Settings	Inbound security rules								
inbound security rules	Priority	Name	Port	Protocol	Source		Destination	Action	
Outbound security rules	1000	▲ default-allow-ssh	22	TCP	Any		Any	Allow	
Network interfaces	1010	Port_443	443	TCP	Any		Any	Allow	
Subnets	65000	AllowVnetInBound	Any	Any	VirtualN	letwork	VirtualNetwork	k 🔮 Allow	
Properties	65001	AllowAzureLoadBalancer	Any	Any	AzureLo	adBalancer	Any	Allow	
🔒 Locks	65500	DenyAllInBound	Any	Any	Any		Any	Ø Deny	
😫 Export template									

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.

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

16. 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

```
1 enable feature aaa LB SSL SSLVPN
2 add ip 52.172.55.197 255.255.0 -type VIP
3 add vpn vserver vpn_ssl SSL 52.172.55.197 443
4 add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
5 bind ssl vserver vpn_ssl -certkeyName ckp
```

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 Internaus. 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. Home > ansible_rg_ganeshb_1611818039 > New > Load Balancer >

Create load balancer

Project details		
Subscription *		\checkmark
Resource group *	Create new	\checkmark
Instance details		
Name *	internal-load-balancer	\checkmark
Region *	(US) West US 2	\sim
Туре * 🛈	Internal O Public	
SKU * 🕕	● Basic 🔵 Standard	
Configure virtual network.		
Virtual network * ①	automation_network	\checkmark
Subnet *	ClientSubnet (192.168.2.0/24) Manage subnet configuration	\checkmark
IP address assignment *	🔿 Static 💿 Dynamic	
Review + create < Previous	Next : Tags > Download a template for automation	

• Um einen externen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Public** und erstellen Sie hier die öffentliche IP-Adresse.

Microsoft Azure	
me > Load balancing - he Create load ba	الع me choose (Preview) > اlancer
Туре * 🛈	O Internal Public
SKU * 🛈	• Standard O Basic
	 Microsoft recommends Standard SKU load balancer for production workloads. Learn more about pricing differences between Standard and Basic SKU 3
Tier *	Regional Global
Public IP address Public IP address * ①	• Create new Use existing
Public IP address name *	
Public IP address SKU	Standard
IP address assignment	O Dynamic 🔘 Static
Availability zone *	✓
Add a public IPv6 address	1 No Yes
Routing preference (i)	Microsoft network Internet
Review + create	< Previous Next : Tags > Download a template for automation

1. 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.

••	new-alb-ilb Frontend IP configuration							
2	Search (Cmd+/)	🕂 Add 💍 Refresh						
	Overview	Filter by name						
-	Activity log	Name	IP address	Rules count				
ጵ	Access control (IAM)	LoadBalancerFrontEnd	52 172 96 71 (in-alb-ilb)	0				
Ø	Tags	Eoaubalancemontena		·				
Þ	Diagnose and solve problems							
Set	tings							
•••	Frontend IP configuration							
Ņ	Backend pools							
P	Health probes							
≝≡	Load balancing rules							
ð	Inbound NAT rules							
•								

- 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.

```
1 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.

1 bind lb vserver <name> <serviceName>

Beispiel

1 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.

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

Beispiel

1 add nsip 52.172.96.71 -type vip

2. Fügen Sie ein IPSet sowohl auf primären als auch auf sekundären Knoten hinzu.

1 add ipset <name>

Beispiel

1 add ipset ipset1

3. Binden Sie IP-Adressen an den IP-Satz.

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

Beispiel

1 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

1 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 Marketplacenach 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 f
 ür das virtuelle Netzwerksicher, 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.

Azure settings		
Subscription * (i)		\checkmark
Resource aroup * (i)		\checkmark
	Create new	
ocation * (i)	(US) East US	\checkmark
General		
Resource name * 🛈	avs-cloud1	~
KU * 🛈	AV36 Node	\checkmark
SXi hosts * ①	0	3
		\$11,929.68
Address block * ①	192.168.0.0/20	
firtual Network	avs-cloud-vnet1	\checkmark
	Create new Only Virtual Networks with a valid subnet with are available for selection. For details about a network, refer to details here	h the name "GatewaySubnet" dding subnet in a virtual

- 4. Klicken Sie auf **Review + Erstellen**.
- 5. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.

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

6. Klicken Sie auf **Erstellen**. Der Provisioning-Prozess der Private Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt wird.

Home >							
Microsoft.AVS-20210609092342 Overview ∞ × Deployment × ×							
	Delete 🛇 Cancel 🕕 Redeploy 💍 Refresh						
👶 Overview	Ø We'd love your feedbackt →						
😫 Inputs							
š≡ Outputs	Your deployment is complete						
📄 Template	Deployment name: MicrosoftAVS-20210609092342 Subscription: Resource group: avs-cloud-new Correlation ID: 7330c8b1-6d0b-4dcd-aa8d-aef81b1l						
	✓ Deployment details (Download)						
	∧ Next steps						
	Go to resource						

7. Klicken Sie auf **Gehe zu Ressource**, um die erstellte Private Cloud zu überprüfen.

Search (Cmd+/) « Overview	Delete Essentials Resource group (change)		JSON Vie
Overview	∧ Essentials Resource group (change)		JSON Vie
	Resource group (change)		
Activity log	avs-cloud-new	ESXi hosts 3	
Access control (IAM)	Status Succeeded	Primary peering subnet 192.168.0.232/30	
Diagnose and solve problems	Location East US	Secondary peering subnet 192.168.0.236/30	
Settings	Subscription (change)	Private Cloud Management network 192.168.0.0/26	
Locks	Subscription ID	vMotion network 192.168.1.128/25	
Manage	/640c6a9-7927-4311-6667-ed075090ceas		
Connectivity	Tags (change) Click here to add tags		

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-Portalund klicken Sie auf Ressource erstellen.



2. Suchen Sie nach Microsoft Windows 10 und klicken Sie auf Erstellen.

Home > Create a resource >	
Microsoft Windows 10 🖈 … Microsoft Corporation	×
Microsoft Windows 10 Create Start with a pre-set configuration	
Overview Plans Usage Information + Support Reviews	
This software is provided by Microsoft. Use of this software in Microsoft Azure is not permitted except under a volume licensing agreement wit Create, I acknowledge that I or the company I work for is licensed to use this software under a volume licensing agreement with Microsoft and will be subject to that agreement.	ith Microsoft. By clicking I that the right to use it

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.

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

- 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.

All services > Resource groups > Oviv	ekc-avs-demo > avs-cloud		
avs-cloud Identity	\$ ···		×
✓ Search (Ctrl+/) « ✓ Taos	Login credentials		
e logo	vCenter credentials		
Diagnose and solve problems	Web client URL ①	https://192.168.0.2/	Conv to clinhoard
Settings	Admin username ①	cloudadmin@vsphere.local	
🔒 Locks	Admin password		
Manage	. and particular C		
Connectivity	Certificate thumbprint ①	B237D65A11B69C2907A35856E3CDB7A12B0BA2FE	Ø
	NSX-T Manager credentials		
	Web client URL ①	https://192.168.0.3/	D.
Clusters			
Workload Networking	Admin username ()	admin	Ø
i Segments	Admin password ①		
TT DHCP	Certificate thumbprint ①	2362FAA1F4CAE9952646F2B62DF1BB87AC7CF368	۵
Port mirroring			

2. Starten Sie den vSphere-Client, indem Sie die vCenter-Webclient-URL eingeben.

$\leftarrow \rightarrow$ C \land Not secure https://192.16	8.0.2
vm ware [.]	
Getting Started	
The vSphere Flash-based Web Client is deprecated in vSp switching to the all-new modern HTML5-based vSphere cl reverting to the Flash-based Web Client when necessary.	phere 6.7. We recommend lient as the primary client and only
LAUNCH VSPHERE & IENT (HTML5)	
LAUNCH VSPHERE WEB CLIENT (FLEX)	Deprecated
Documentation	
VMware vSphere Documentation Center	
Functionality Updates for the vSphere Client (HTML5)	

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.

vSphere - vc.de7510d9c7d8485	× +						- o ×
← → C ▲ Not secur	e https://192.168.0.2/ui/#?exter	sionId=vsphere.core.inventory.s	erverObjectViewsExtensio	on&objectId=urn:vm/	omi:Folder:group-d1:d	77ece11-494 🏠 🐒	i @ 🔋 …
vm vSphere Client M	enu 🗸 🛛 📿 Search in all enviro	onments			C @~	cloudadmin@VSPHERE	LOCAL Y
	🗗 vc.de7510d9c7d848	35cb31194.eastus.avs.a	ZURE.COM	ons 🗸			
🖉 vc.de7510d9c7d8485cb311	Summary Monitor Configur	e Permissions Datacenters	Hosts & Clusters	VMs Datastores	Networks Linked	Center Server Systems	Extensions
 Cluster-1 esx03-r09.p03.de7 esx04-r02.p03.de7 esx14-r15.p03.de75 	Virtual Machines: Hosts:					CPU Used 13.07 CHz Mamory Used 235.83 GB Storage Used 5.82 TB	Free 234.79 GHz * Capachy: 247.86 GHz Free: 1.45 TB Capachy: 1.68 TB Free: 31.61 TB Capachy: 38.42 TB
	Custom Attributes		^	Tags			^
	Attribute	Value		Assigned Teg	Category	Description	
	4			4			
Recent Tasks Alarms			the Basser De Wander,				*
Target Verde75	 ✓ Status 10d9c7d84 ✓ Completed 	Details V Initiato HCX Disaster Recovery Plugin VSPH (com.ymware.hybridity.	er v Queuer ERELOCALivsph 10 ms	d For v Sta	rt Time ↓ v c	5/02/2021, 3:17:19 PM	de7510d9c7d8485c

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

> Hinzufügenaus. 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.

All services > Resource groups > Oviv	ekc-avs-demo > avs-cloud				Add segment	×	
avs-cloud Segmer	nts 🖈 …						
P Search (Ctrl+/) ≪	🕂 Add 🗐 Delete 💍 Refre	sh					1
Overview	P Filter by name	Name : All IP Address :	all a		Segment name *	~	
Activity log	Francisco (*	Connected automau \$1	Colomba ID Co.	DHICD +	Connected automatic		
Access control (IAM)		Connected gateway 14	Galeway IP 1.	UNCER	Connected gateway		
Tags	TNT22-HCK-UPUNK	TNT22-T1	192.168.3.1/26		T1 TNT22-T1		
Diagnose and solve problems					Туре		
Settings					Overlay segment		
🔒 Locks					Subnet		
Manane					Gateway *		
Connertuitu					192.168.4.1/24	×	
Identity					DHCP rappes (actional)	Example: 10.1.1.1/24	
Clusters					Enter DHCP ranges		
Workload Networking							
Ke Segments							l
T DHCP							
Port mirroring						Example: 10.1.1.0/24 or 10.1.1.10-10.1.1.100	
O DNS							,
		~			OX Cancel		

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.

services > Resource groups > Oviv	ekc-avs-demo > avs-cloud	
avs-cloud Identity	\$	
Search (Ctrl+/) «	Login credentials	
Tags	Conter medentials	
Diagnose and solve problems	Web client URL ①	https://192.168.0.2/
ings	Admin username ①	cloudadmin@vsphere.local
Locks	Admin annual O	
nage	Admin password	
Connectivity	Certificate thumbprint ①	B237D65A11B69C2907A35856E3CD87A12B0BA2FE
Identity	NSX-T Manager credentials	
Clusters	Web client URL ①	https://192.168.0.3/
	Admin username ①	admin
kload Networking	Admin assessed ()	TN .
Segments	Admin password	
DHCP	Certificate thumbprint ①	2362FAA1F4CAE9952646F2B62DF1BB87AC7CF368
Port mirroring		
0.115		

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.

🖻 💋 vSphere - vc.de7510d9c7d8485 x		NSX		× +						-
\leftarrow \rightarrow C \blacktriangle Not secure	https	://192	.168.0	0.3/nsx/#/app/networks/segments/	module/home			ť	ð ≦	œ
vm NSX-T							Q	¢		
Home Networking Securi	ity	Invent	tory	Plan & Troubleshoot System	Advanced Networking & Security					
Network Overview Connectivity		SEGM		SEGMENT PROFILES		EXPAND ALL	Filter by	Name, P	ath or more	e
🔁 Tier-0 Gateways				Segment Name	Connected Gateway & Type		Subnet	ts	Status	Т
🔁 Tier-1 Gateways	÷	>	~	client	TNT22-T1 Tier1 - Flexible		1		• Up	C
🝕 Segments	÷	>	4	management	TNT22-T1 Tier1 - Flexible		1		• Up	С
Network Services	-	>	¢	server	TNT22-T1 Tierl - Flexible		1		• Up	С
VPN	-	>	0 6	TNT22-HCX-UPLINK	TNTZZ-TTTTTETT - Flexible		1		Up Up	C
- NAT	:	>	4	TNT22-T0-PRIVATE01-LS	None - Flexible				• Up	C
 Load Balancing Forwarding Policies 	:	>	~	TNT22-T0-PRIVATE02-LS	None - Flexible				• Up	C

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**.

e of sphere - NSV9X-ESX-13.0-7 ← → C ▲ Not sect	9.6- x a NSX ure https ://19	× + 92.168.0.2/ui/#?extensionId=vsphere	core.inventory.serverObjectViewsExtension&	cobjectId=umvmomi/VirtualMachine.vm-53:d776
Vin Vophere Clent	B NSV	Edit Settings NSVPX-E	5X-13.0-79.64_nc_64	
 Cluster-1 esx03-r09.p03.de7 esx04-r02.p03.de7 esx04-r05.p03.de75 	Powe	> CPU > Memory	2 ~	0
	Launch Wo Launch Ren	> Hard disk 1 > SCSI controller 0	20 GB ~ LSI Logic Parallel	
	VM Hard	Network adapter 1 New Network *	management ~	Connect
	Related 0	> New Network *	server 🗸	Connect
	Clust	> Video card	Specify custom settings $ \sim $	
	Host	VMCI device	Device on the virtual machine PCI bus virtual machine communication interfe	s that provides support for the ace
ecent Tasks Alarms		> Other	Additional Hardware	
estoy OVF template Profest OVF package Cust	*X.ESX.I3.0-7 er-1			CANCEL CANCEL SS 02:202

7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.

■ ■ 9	 1 Select an OVF template 2 Select a name and folder 	Ready to complete Click Finish to start creat	tion.
DDC-Datacenter	 ✓ 3 Select a compute resource ✓ 4 Review details 	Rectification to as	
esx03-r09.p03.de7	✓ 5 Select storage ✓ 6 Select networks	Provisioning type	Deploy from template
esx34-r15.p03.de75	7 Ready to complete	Tampinta name	N3VPA-E3X-13.0-79.04_10_04
		Permission of size	N5VPX-E5X-13.0-79.64_NC_64
		Download Size	599.9 MB
		size on disk	20.0 GB
		Folder	SDDC-Datacenter
		Resource	Cluster-1
		Storage mapping	1
		All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
		Network mapping	1
		VM Network	management
Tasks Alarms		IP allocation settings	
· · Target		IP protocol	IPV4
F package		10 clinical inter	

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.

VSphere - NSV	PX-ESX-13.0-79.6 × NSX	× +	
vm vSphere Cl	Actions - NSVPX-ESX-13.0-79.64_m.	22 UV * EXcertationinu * spinelezui e universitori y sei veri objecti viewsckietrationicuologiectio * unitivimonii virtualamachine viri * sud / rece i e e all exercisionisote	ISPHERELOCAL V
vc.de7510d9c7d8	Guest OS Snapshots Open Remote Console	Imposer Off. off Fall + 2 Imposed off Fall + 2 astores Networks	
 Cluster-1 esx03-r09 esx04-r02 	Clone	4-bit) Shut Down Scient (S = 11 + 0 /M version 9) Shut Down Scient (S = 11 + 0 /M version 9) Shut Down Scient (S = 11 + 12 + 12 + 12 + 12 + 12 + 12 + 12	CPU USAGE O HZ MEMORY USAGE
esx14-r15.c	VM Policies	DYs Name: P Addresses: Host: esx04+02.p03.de7510d9c7d8485cb31194.eastus.avs.azure.com	STORAGE USAGE 40.83 GB
	Compatibility Export System Logs	▼ Notes	^
	Edit Settings Move to folder Dename	Custor-1	^
	Edit Notes Tags & Custom Attributes	est/04-02.p03.de7510d907d8485cb31194.east. Antibule Value Value	1
Recent Tasks Ala Task Name v Reconfigure virtual	Add Permission Alarms	✓ Deals ✓ Interar ✓ Queued For ✓ Sout Time ↓ ✓ Competion Time	 ✓ Server
machine Deploy OVF template	Remove from Inventory Delete from Disk	ed VSPHERELOCAL/cloud 4 ms 05/02/2021, 41108 PM 05/02/2021, 41108 PM ed VSPHERELOCAL/cpsd 3 ms 05/02/2021, 402 PM 05/02/2021, 402 PM 05/02/2021, 402 PM	M vc.de7510d9c7d8485c.

9. Sie sind jetzt vom vSphere-Client aus mit der NetScaler VM verbunden.

				-					_
VSphere - NS	SVPX-E5X-13.0-79.64	NSVPX-ESX-1	3.0-79.64_nc_64 x	NSX		× -	t	-	o ×
$\leftrightarrow \rightarrow G$	Not secure	https://192.168.0	0.2/ui/webconso	le.html?vmId=v	/m-53&vmName=	NSVP	PX-ESX-13.0-79.64_nc_64&serverGuid=d77ece11-4945-4ee5-bb8e-17b4 S S	•	\$ ···
NSVPX-ESX-13.0-79	9.64_nc_64						Enforce US Keyboard Layout View Fullscreen Se	nd Ctrl+/	Alt+Delete
	NetScal	er has st	tarted s	uccessf	ully				
	Start a	dditional	l daemon	s: m ay	2 16:12:	:54	(local@.err> ns nsconfiga: _dispatch()		
	Mau 2	10 passau 16:12:54	Jocal A	orr) n	s neconfi	iad	: disnatch(): Specified parameters are		
	not an	inlicable	for thi	s tune	of SSL nr	rof	ile.		
	May 2	16:12:54	<loca10< td=""><td>.err> n</td><td>s nsconfi</td><td>iad</td><td>: _dispatch(): Invalid rule.</td><td></td><td></td></loca10<>	.err> n	s nsconfi	iad	: _dispatch(): Invalid rule.		
	May 2	16:12:54	<local0< td=""><td>.err> n</td><td>s last me</td><td>ess</td><td>age repeated 2 times</td><td></td><td></td></local0<>	.err> n	s last me	ess	age repeated 2 times		
	May 2	16:12:55	<local0< td=""><td>.err> n</td><td>s nsconfi</td><td>igd</td><td>: _dispatch(): No such resource</td><td></td><td></td></local0<>	.err> n	s nsconfi	igd	: _dispatch(): No such resource		
	May 2	16:12:55	<local0< td=""><td>.err> n</td><td>s nsconfi</td><td>igd</td><td>: _dispatch(): No such policy exists</td><td></td><td></td></local0<>	.err> n	s nsconfi	igd	: _dispatch(): No such policy exists		
	Monit ⊾	ionit daer	10n at 1	000 ама	kened				
	Mari 2	16.12.55	(100010		a laat w		are repeated 4 times		
	Mau 2	16:12:55		.err> m	S last Me	ess thd	aye repeated 4 times		
	-2.	10.13.00	Auser.c	1117 115	sysnear	t nu	· systa 450010, frai aevice feau failea		
	May 2	16:13:00	<loca10< td=""><td>.err> n</td><td>s nscolle</td><td>ect</td><td>: ns copyfile(): Not able to get info o</td><td></td><td></td></loca10<>	.err> n	s nscolle	ect	: ns copyfile(): Not able to get info o		
	f file	/var/log/	∕db∕defa	ult/nsd	evmap.txt	t :	No such file or directory		
	Mau 2	16:13:01	(local@	err) n	e neumond	4 F 1	6391: nsumond daemon started		

10. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

1 ssh nsroot@<management IP address>

Beispiel

```
1 ssh nsroot@192.168.4.5
```

11. Sie können die ADC-Konfiguration mit dem Befehl show ns ip überprüfen.

D Ope	nSSH SSH client							
Done sh ns	ip Ipaddress	Traffic Domain	Туре	Rode	Arp	Icmp	Vserver	State
1) 2) 1) Done	192.168.4.5 192.168.5.5 192.168.6.5		NetScaler IP VIP SNIP	Active Active Active	Enabled Enabled Enabled	Enabled Enabled Enabled	NA Enabled NA	Enabled Enabled Enabled
		٠						

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 f
 ür den Zugriff auf und die Verwaltung der Azure VMware-L
 ösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-L
 ösung.
- 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.

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

Beispiel

1 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.

1 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.
	1	bind	lb	vserver	<nam< th=""><th>ie></th><th><servicename></servicename></th></nam<>	ie>	<servicename></servicename>
B	eispie	ι					
	1	bind	lb	vserver	lb1	web	oserverl

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.

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

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 f
 ür den Zugriff auf und die Verwaltung der Azure VMware-L
 ösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-L
 ösung.
- 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:

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

Beispiel-IP-Konfiguration für die sekundäre ADC-Instanz:

```
1 NSIP: 10.0.0.5/24
2 SNIP on 1/1: 10.0.1.5/24
3 SNIP on 1/2: 10.0.2.5/24
4 VIP: 172.168.1.1/32
```

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.

= Microsoπ Azure	Search resources, services, and docs (G+/)	CITRIX (CITRIX.ONMICROSOFT.C
Home > Resource groups > Azure	puteserverIntegration >	
Route Server	x 🛪 …	×
Search (Ctrl+/)	« 🔟 Delete	
😵 Overview	▲ ▲ Essentials	JSON View
Activity log	Resource group : <u>AzurerouteserverIntegration</u> Status	: Succeeded
Access control (IAM)	Location : eastus Virtual	Network / Subnet : RSvnet/RouteServerSubnet
🔷 Tags	Subscription ASN	: 65515
	Subscription ID Peer Ip	s : 10.0.3.4, 10.0.3.5
Settings	Tags (edit) : <u>Click here to add tags</u>	
💼 Configuration		
Peers		
Properties 1		
🔒 Locks		
Monitor		
Sconnection monitor		
Monitoring		
Metrics		
Automation		
🖧 Tasks (preview)		
Export template		

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.

Home > Resource groups > A	AzurerouteserverIntegration $>$ myRc	uteServer			
myRouteServe	er∣Peers ☆ …				×
	« 🕂 Add 🖒 Refresh				
S Overview	Name	↑↓ ASN	↑↓ IPv4 Address	↑↓ Provisioning State	↑↓
Activity log	ADC0	400	10.0.1.4	Succeeded	
^P _R Access control (IAM)	ADC1	500	10.0.1.5	Succeeded	
🧳 Tags					
Settings					

3. 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:

```
1
     enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
     enable ns feature LB BGP
2
     add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -
3
        dynamicRouting ENABLED
4
     VTYSH
5
     configure terminal
     router BGP 400
6
7
     timers bgp 1 3
8
     neighbor 10.0.3.4 remote-as 65515
9
     neighbor 10.0.3.4 advertisement-interval 3
10
     neighbor 10.0.3.4 fall-over bfd
11
     neighbor 10.0.3.5 remote-as 65515
12
     neighbor 10.0.3.5 advertisement-interval 3
13
     neighbor 10.0.3.5 fall-over bfd
14
     address-family ipv4
15
     redistribute kernel
16
     redistribute static
```

5. Konfigurieren Sie das dynamische Routing in der sekundären ADC-Instanz.

Beispielkonfiguration:

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

6. 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.

```
1 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 -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 Identitätaus.
- 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.

Home > new-test-14.1	
new-test-14.1 Ide Virtual machine	entity 🛪 …
₽ Search	System assigned User assigned
👤 Size	
Ø Microsoft Defender for Cloud	A system assigned managed identity is restricted to one per resource and is tied to the inecycle of this resource, you can grant permiss using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have
Advisor recommendations	Save X Discard () Refresh
Extensions + applications	
Natiability + scaling	Status (i)
💼 Configuration	Off On
😢 Identity	
Properties	
🔒 Locks	
Operations	
≯ Bastion	

Sobald der Status gespeichert ist, sehen Sie, dass ein Dienstprinzipalobjekt erstellt und der VM zugewiesen wird.

5. Klicken Sie auf Azure-Rollenzuweisungen.

Home > new-test-14.1	
new-test-14.1 Identi Virtual machine	ty ★ ··· ×
Search «	System assigned User assigned
😫 Disks	A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.
Size	
Ø Microsoft Defender for Cloud	E zave V Discalo O Kellezu V Got leedback.
Advisor recommendations	
Extensions + applications	Off On
Availability + scaling	Object (original) ID 0
💼 Configuration	78dc5c36-814f-44f0-a238-ccd992caae86
🚷 Identity	Permissions ①
Properties	Azure role assignments
🔒 Locks	
Operations	This resource is registered with Microsoft Entra ID. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures.
💉 Bastion	

- 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.

Home > new-test-14.1 Identity >		Add role assignment (Preview)		
Azure role assignments				
+ Add role assignment (Preview)	sch	Scope ①		
If this identity has role assignments that you do	n't have permission to re	Resource group Subscription		
Subscription *	_	Resource group ①		
Role R	esource Name	tahaj-test-ipconfig		
No role assignments found for the selected sub	scription.	Role () Contributor ()		
		Learn more about RBAC		
		Save Discard		

Auf der Seite mit den **Azure-Rollenzuweisungen** wird die verwaltete Identität angezeigt, die Sie erstellt haben.

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

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**.

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

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.

← Set Credentials

Tenant ID	
Application ID	
Application Secret	
OK Cancel	

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.

Q Search Menu	AZURE > Cloud Profile
Favorites ~	Cloud Profile 💿
AZURE ~	Add Edit Delete
Cloud Profile	Q Click here to search or you can enter Key : Value format
System >	NAME © AUTO SCALE SETTING © LOAD BALANCING VIRTUAL SERVER
AppExpert >	No items

Die Konfigurationsseite " Cloud-Profil erstellen "wird angezeigt.

← Create Cloud Profile

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

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 Portsicher, 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.

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

Apply	Discard changes

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.

Create Cloud Profile

Name

Virtual Server IP Address*

52.169.111.203

Туре

AZURETAGS

Azure Tag Name

Azure Tag Value

Azure Poll Periods

60

Load Balancing Server Protocol

HTTP

Load Balancing Server Port

80

Azure Tag Setting*

Azure Tag Setting Protocol

HTTP

Azure Tag Setting Port

80

Create

Close

- 1. 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.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>`
    -port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
```

Wichtig:

Sie müssen alle Konfigurationen speichern, da die Konfigurationen andernfalls nach dem Neustart der Instanz verloren gehen. Geben Sie save configein.

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
          Name: MyTagCloudProfile Type: azuretags
2
    1)
                                                           VServerName:
        MyTagVServer ServiceType: HTTP
                                             IPAddress: 52.178.209.133
       Port: 80
                                ServiceGroupName: MyTagsServiceGroup
       BoundServiceGroupSvcType: HTTP
3
          Vsvrbindsvcport: 80
                                  AzureTagName: myTagName AzureTagValue
             : myTagValue AzurePollPeriod: 60
                                                  GraceFul: NO
                        Delay: 60
```

Um ein Cloud-Profil zu entfernen, geben Sie rm Cloud-Profil ein < 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:

1 #> 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

```
1 #> shell
```

Verwenden Sie den folgenden Befehl, um den rain_tags-Prozess zu beenden:

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

January 15, 2025

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.



Region 2 (Resource Group 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.

\$location="West Central US" 1 2 3 \$vnetName="NSVPX-vnet" 4 \$RGName="multiIP-RG" 5 6 7 \$prmStorageAccountName="multiipstorageaccnt" 8 \$avSetName="MultiIP-avset" 9 10 11 \$vmSize="Standard_DS3_V2"

Hinweis:

Die Mindestanforderung für eine VPX-Instanz sind 2 vCPUs und 2 GB RAM.

1 2	<pre>\$publisher="citrix"</pre>
- 3 4	<pre>\$offer="netscalervpx111"</pre>
5	\$sku="netscalerbyol"
7 8	<pre>\$version="latest"</pre>
9 10	<pre>\$vmNamePrefix="MultiIPVPX"</pre>
11 12	<pre>\$nicNamePrefix="MultiipVPX"</pre>
13 14	<pre>\$osDiskSuffix="osdiskdb"</pre>
15 16	<pre>\$numberOfVMs=1</pre>
17 18	<pre>\$ipAddressPrefix="10.0.0."</pre>
19 20	<pre>\$ipAddressPrefix1="10.0.1."</pre>
21 22	<pre>\$ipAddressPrefix2="10.0.2."</pre>
23 24	<pre>\$pubIPName1="MultiIP-pip1"</pre>
25 26	<pre>\$pubIPName2="MultiIP-pip2"</pre>
27 28	<pre>\$IpConfigName1="IPConfig1"</pre>
29 30	\$IPConfigName2="IPConfig-2"
31 32	\$IPConfigName3="IPConfig-3"
33	\$IPConfigName4="IPConfig-4"

```
34
35 $frontendSubnetName="default"
36
37 $backendSubnetName1="subnet\_1"
38
39 $backendSubnetName2="subnet\_2"
40
41 $suffixNumber=10
```

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

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

Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

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

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.

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

3. Rufen Sie Subnetze ab.

```
1 $frontendSubnet=$vnet.Subnets|?{
2 $_.Name -eq $frontendSubnetName }
3
4 $backendSubnet1=$vnet.Subnets|?{
5 $_.Name -eq $backendSubnetName1 }
6
7 $backendSubnet2=$vnet.Subnets|?{
8 $_.Name -eq $backendSubnetName2 }
```

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

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

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

NIC 1/1 erstellen

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

NIC 1/2 erstellen

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

VM-Konfigurationsobjekt erstellen

```
    $vmName=$vmNamePrefix
    $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
AvailabilitySetId $avSet.Id
```

Anmeldeinformationen abrufen und Betriebssystemeigenschaften festlegen

1	<pre>\$cred=Get-Credential -Message "Type the name and password for VPX</pre>
	login."
2	<pre>\$vmConfig=Set-AzureRMVMOperatingSystem -VM \$vmConfig -Linux -</pre>
	ComputerName \$vmName -Credential \$cred
3	\$vmConfig=Set-AzureRMVMSourceImage -VM
	\$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

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

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 verwen	dete IP-Adressen In VM1	verwendete IP-Adressen
--------------------------	-------------------------	------------------------

Netzwerkkarte	Private IP	Öffentliche IP (PIP)	Beschreibung
0/1	10.0.0.10	PIP1	Als NSIP
			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 svcl 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

```
2 Add nsip 20.0.2.10 255.255.255.0
3 add service svc1 20.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 20.0.1.11 80
5 Add service s1 20.0.2.90 http 80
6 Add service s2 20.0.2.91 http 80
7 Bind lb vs v1 s[1-2]
```

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.

1	enable ns feature LB GSLB
2	add gslb site site1 10.0.1.10 -publicIP PIP2
3	add gslb site site2 20.0.1.10 -publicIP PIP5
4	add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
	PIP3 -publicPort 80 -siteName site1
5	add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP
	PIP6 -publicPort 80 -siteName site2
6	add gslb vserver gslb_http_vip1 HTTP
7	bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
8	bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
9	bind gslb vserver gslb_http_vip1 -domainName_www.gslbindia.com -TTL 5

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 Complianceund 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



Region 2 (Resource Group 2)

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.

1	<pre>\$locName="South east Asia"</pre>
2	
3	\$rgName="MulitIP-MultiNIC-RG"
4	
5	<pre>\$pubIPName4="PIPFORGSLB1"</pre>
6	
7	\$domName4="vpxgslbdns"
8	
9	<pre>\$lbName="MultiIPALB"</pre>
10	
11	<pre>\$frontEndConfigName2="FrontEndIP2"</pre>
12	
13	<pre>\$backendPoolName1="BackendPoolHttp"</pre>
14	
15	<pre>\$lbRuleName2="LBRuleGSLB1"</pre>
16	
17	<pre>\$lbRuleName3="LBRuleGSLB2"</pre>
18	
19	<pre>\$lbRuleName4="LBRuleDNS"</pre>

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

Schritt 2. Erstellen Sie LB-Regeln und aktualisieren Sie die vorhandene ALB.

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
1
        $rgName
2
3
     $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
4
        LoadBalancer $alb -Name $frontEndConfigName2
5
6
7
     $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
        LoadBalancer $alb -Name $backendPoolName1
8
9
10
     $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
        Name $healthProbeName
11
13
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
        BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
14
15
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
        BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
17
18
```

19 \\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \\$lbRuleName4 -BackendAddressPool \\$backendPool -FrontendIPConfiguration \ \$frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort 53 -Probe \\$healthprobe -EnableFloatingIP | Set-AzureRmLoadBalancer

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

Verwandte Ressourcen:

Konfigurieren von GSLB auf NetScaler VPX-Instanzen

Globaler Serverlastausgleich

NetScaler GSLB auf Azure bereitstellen

April 9, 2025

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 auf der Welt Sie sich 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)

GSLB DBS verwendet den FQDN des Benutzers ALB, um die GSLB-Dienstgruppen dynamisch zu aktualisieren und die Back-End-Server einzuschließen, 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 DNS-fähige Diensterkennung, um die Mitgliedsdienstressourcen des in der Autoscale-Gruppe identifizierten DBS-Namespace zu bestimmen.

Das folgende Bild zeigt die NetScaler GSLB DBS Autoscale-Komponenten mit Cloud Load Balancern:



Voraussetzungen für Azure GSLB

Zu den Voraussetzungen für die NetScaler GSLB-Dienstgruppen gehören eine funktionierende Microsoft Azure-Umgebung sowie das Wissen und die Fähigkeit, Linux-Webserver, NetScaler-Geräte innerhalb von Azure, öffentliche IP-Adressen und Azure Load Balancer (ALB) 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-xxxxxxx.australiaeast.cloudapp.
azure.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.
| ≡ Microsoft Azure | | $\mathcal P$ Search resources, services, and docs (G+/) | |
|---|--|---|--|
| Home > Create a resource > Marketpla | ce > Load Balancer > | | |
| Create load balancer | | | |
| Azure load balancer is a layer 4 load balancer
balancers uses a hash-based distribution a
destination port, protocol type) hash to ma
accessible via public IP addresses, or intern
Network Address Translation (NAT) to rout | backend pools indound rules of
cer that distributes incoming traffic among
Igorithm. By default, it uses a 5-tuple (sour
ap traffic to available servers. Load balance
hal where it is only accessible from a virtual
e traffic between public and private IP add | healthy virtual machine instances. Load
ce IP, source port, destination IP,
rs can either be internet-facing where it is
network. Azure load balancers also support
resses. Learn more. | |
| Project details | | | |
| Subscription * | | \checkmark | |
| Resource group * | Create new | ~ | |
| Instance details | | | |
| Name * | ALB | ✓ | |
| Region * | East US 2 | \checkmark | |
| SKU* 🛈 | Standard Gateway Basic | | |
| Туре * 🛈 | Public Internal | | |
| Tier * | Regional Global | | |
| Review + create < Previous | Next : Frontend IP configuration > | Download a template for automation RGive feedback | |

3. Fügen Sie die erstellten NetScaler-Back-End-Pools hinzu.

Home > tahaj-test > ALB							
ALB Backend pool	s ☆						
© Search «	+ Add 💍 Refresh						
Overview							
Activity log	The backend pool is a critical compo	nent of the load balancer. The ba	ckend pool defines the group of res	urces that will			
Access control (IAM)	serve traffic for a given load-balancin	ng rule. Learn more. 🕫	p p p p p				
Tags	Q	Add filter					
X Diagnose and solve problems							
iettings	Backend pool	Resource Name	IP address	Network interface	Availability zone	Rules count	Resource Status
Frontend IP configuration							
Backend pools							
Health probes							
Load balancing rules							
Inbound NAT rules							
Properties							
Locks							
Monitoring							
V Insights							
 Diagnostic settings 							
🗜 Logs							
Alerts							
Metrics							

4. Erstellen Sie eine Integritätsprüfung für Port 80.

Erstellen Sie eine Lastenausgleichsregel mit der vom Lastenausgleich 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

\equiv Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)				
Home > tahaj-test > ALB Load balancing rules >						
Add load balancing rule						
A load balancing rule distributes incoming backend pool instances. Only backend inst	traffic that is sent to a selected IP address a ances that the health probe considers health	nd port combination across a group of y receive new traffic.				
Name *	lb_rule2					
IP Version *	IPv4					
	O IPv6					
Frontend IP address * (i)	frontend_ip (10.1.0.7)	~				
Backend pool * (i)	backend_pool					
High availability ports 🛈						
Protocol	● TCP					
	O UDP					
Port *	80					
Backend port * (i)	80					
Health probe * 🕕	Select an existing probe	~				
Carrier considerate O	Create new					
Session persistence ()	None					
Frankla TCD Deset	4					
Enable TCP Reset						
Save Cancel						

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, NetScaler entweder mit einem Nameserver oder einem virtuellen DNS-Server zu konfigurieren, über den die ALB-Domänen für die DBS-Dienstgruppen 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.

← Create Server

elb-virginia	()	
🔵 IP Address 🛛 💿 Domain Name		
FQDN*		
elb-virginia-1948532428-us-eas		
Traffic Domain		
	Add	Edit
Translation IP Address		
Translation Mask		
Resolve Retry (secs)	_	
IPv6 Domain		
Enable after Creating		
A	/	
Comments		

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. Konfigurieren Sie die Site als übergeordnete Site und stellen Sie sicher, dass die **Trigger-Monitore** IMMER auf **und**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.

← Create GSLB Site

Name*	
asia-site	\bigcirc
Туре	
REMOTE	\sim ()
Site IP Address*	
172 . 35 . 88 . 90	()
Public IP Address	
18 . 232 . 14 . 212	()
Parent Site Backup Parent Sit Parent Site Name	tes
GSLBSite1	Ý Ō
Trigger Monitors*	
ALWAYS	/
Cluster IP	_
Public Cluster IP	
NAPTR Replacement Suffix	
Metric Exchange	
Vetwork Metric Exchange	
Persistence Session Entry Exchange	
Create Close	

- 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 Statusund Integritätsüberwachung aktivieren. Klicken Sie auf**OK**, um die Dienstgruppe zu erstellen.

← GSLB Service Group

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

7. Klicken Sie auf**Service Group Members**und wählen Sie**Serverbasiert**aus. Wählen Sie den jeweiligen ALB aus, der zu Beginn der Laufanleitung konfiguriert wurde. Konfigurieren Sie den Datenverkehr so, dass er über Port 80 geht. Klicken Sie auf **Erstellen**.

Create Service Group Me	mber
IP Based Server Based	
Select Server*	
elb-nvirginia	> Add Edit ()
Port*	
80	$(\mathbf{\hat{l}})$
Weight	
1	
Order	
Site Prefix	
✓ State	
Create Close	

Die Servicegruppenmitgliedsbindung wird mit 2 Instanzen aufgefüllt, die sie vom ALB empfängt.

GSLB Servicegroup Member Binding								×				
Add	Edit Unbind	Monitor Details	No action 🗸									
${\sf Q}$ Click here	to search or you can enter Key	: Value format										î
	IP ADDRESS	SERVER NAME	PORT \$	WEIGHT	ORDER 4		HASH ID		STATE \$	SERVICE STATE	SITE PREFIX	
	10.100.234.12	10.100.234.12	80	1					ENABLED	UP		
	54.252.154.72	elb-nvirginia	80	1	1				ENABLED	UP		
Close												

- 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.

← GSLB Virtual Server

Indille	
GV2	Î
DNS Record Type*	
А	\sim
Service Type*	
НТТР	\sim
Consider Effective State	
NONE	\sim ()
Toggle Order	
ASCENDING	\sim (i)
Order Threshold	
Order Threshold AppFlow Logging	
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's	OWN
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF	OWN s IP address in response (EDR) P
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II	OWN s IP address in response (EDR) P IPs' in response (MIR)
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet	OWN s IP address in response (EDR) P IPs' in response (MIR)
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet Respond with ECS option	OWN s IP address in response (EDR) P IPs' in response (MIR) n in the response for a DNS query with ECS
 ✓ AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet Respond with ECS option Validate ECS address is a 	OWN s IP address in response (EDR) P IPs' in response (MIR) n in the response for a DNS query with ECS a private or unroutable address
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments	OWN s IP address in response (EDR) P IPs' in response (MIR) n in the response for a DNS query with ECS a private or unroutable address
 ✓ AppFlow Logging When this Virtual Server is D0 Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments 	OWN s IP address in response (EDR) P IPs' in response (MIR) n in the response for a DNS query with ECS a private or unroutable address
Order Threshold AppFlow Logging When this Virtual Server is DO Do not send any service's When this Virtual Server is UF Send all "active" service II EDNS Client Subnet Respond with ECS option Validate ECS address is a Comments	OWN s IP address in response (EDR) P IPs' in response (MIR) n in the response for a DNS query with ECS a private or unroutable address

l

- 12. Sobald der virtuelle GSLB-Server erstellt wurde, klicken Sie auf**No GSLB Virtual Server Ser**viceGroup Binding.
 - ← GSLB Virtual Server

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

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.

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

14. Konfigurieren Sie die Domänenbindung für virtuelle GSLB-Server, indem Sie aufKeine GSLB-Domainbindung für virtuelle Serverklicken. Konfigurieren Sie den FQDN und binden Sie ihn. Behalten Sie für die anderen Parameter die Standardeinstellungen bei.

Domain Binding	
FQDN*	
www.gslbdbs.com	0
TTL (secs)	
5]
Backup IP	
	1
Cookie Domain	
	1
Cookie Time-out (mins)	_
0	1
Site Domain TTL (secs)	
3600	1
Bind Close	

- 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.

← Load Balancing Service

Service Name*	
adns	(\mathbf{i})
New Server Existing Server	
IP Address*	
172 . 31 . 27 . 121	()
Protocol*	
ADNS	v (j)
Port*	
53	
More	

- 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.

C. Sandi Interve		Traffic Manag	ement / 4518 /	ESL8 Virtual Servers			
ANS	GSLB Virtual Servers					0 😭	
Symen.			The part and the				
Applopent	>	Add	Edit Delet	Statistics No action	~		Search 🛩
Tuffic Management	~		Name	Bath	Polocal	X. Handlin	
Load Balancing	>	000		• LP	1072	100.00%.4 UP/0 DOWN	
Content Switching	• •						
Cache Redirection	• •						
046							
GSLB	~						
Cashboard							
 Virtual Servers 							
Services.							

Andere Ressourcen

Globaler NetScaler Lastausgleich für Hybrid- und Multi-Cloud-Bereitstellungen

NetScaler Web App Firewall auf Azure bereitstellen

October 17, 2024

NetScaler Web App Firewall ist eine Lösung der Enterprise-Klasse, die moder nsten Schutz für moder ne Anwendungen bietet. NetScaler Web App Firewall mindert Bedrohungen für öffentlich zugängliche Ressourcen wie Websites, Webanwendungen und APIs. Die NetScaler Web App Firewall umfasst IP-Reputationsbasierte Filterung, Bot-Abwehr, Schutz vor OWASP Top 10-Anwendungsbedrohungen, Layer-7-DDoS-Schutz und mehr. Ebenfalls enthalten sind Optionen zur Durchsetzung der Authentifizierung, starke SSL/TLS-Chiffren, TLS 1.3, Ratenbegrenzung und Rewrite-Richtlinien. NetScaler Web App Firewall verwendet sowohl grundlegende als auch erweiterte WAF-Schutzmaßnahmen und bietet umfassenden Schutz für Ihre Anwendungen mit beispielloser Benutzerfreundlichkeit. Es ist eine Frage von Minuten, bis Sie loslegen können. Darüber hinaus spart NetScaler Web App Firewall den Benutzern durch die Verwendung eines automatisierten Lernmodells, das als dynamisches Profiling bezeichnet wird, wertvolle Zeit. Indem NetScaler Web App Firewall automatisch lernt, wie eine geschützte Anwendung funktioniert, passt sie sich der Anwendung an, selbst wenn Entwickler die Anwendungen bereitstellen und ändern. NetScaler Web App Firewall hilft bei der Einhaltung aller wichtigen behördlichen Standards und Gremien, einschließlich PCI-DSS, HIPAA und mehr. Mit unseren CloudFormation-Vorlagen war es noch nie so einfach, schnell einsatzbereit zu sein. Mit Auto Scaling können Benutzer sicher sein, dass ihre Anwendungen auch bei wachsendem Datenverkehr geschützt bleiben.

Die NetScaler Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Kundenservern und Kundenbenutzern installiert werden, normalerweise hinter dem Router oder der Firewall des Kundenunternehmens. Weitere Informationen finden Sie unter Einführung in NetScaler Web App Firewall.

NetScaler Web App Firewall Bereitstellungsstrategie

1. Der Einsatz der Web Application Firewall dient der Bewertung, welche Anwendungen oder spezifischen Daten maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und für welche Sicherheitsüberprüfungen sicher umgangen werden können. Dies hilft Benutzern dabei, eine optimale Konfiguration zu finden und geeignete Richtlinien und Verbindungspunkte zur Trennung des Datenverkehrs zu entwerfen. Beispielsweise möchten Benutzer möglicherweise eine Richtlinie konfigurieren, um die Sicherheitsinspektion von Anfragen nach statischen Webinhalten wie Bildern, MP3-Dateien und Filmen zu Bypass, und eine andere Richtlinie konfigurieren, um erweiterte Sicherheitsprüfungen auf Anfragen nach dynamischen Inhalten anzuwenden. Benutzer können mehrere Richtlinien und Profile verwenden, um unterschiedliche Inhalte derselben Anwendung zu schützen.

- 2. Erstellen Sie als Grundlage für die Bereitstellung einen virtuellen Server und führen Sie Testdatenverkehr durch diesen aus, um sich ein Bild von der Geschwindigkeit und Menge des Datenverkehrs zu machen, der durch das Benutzersystem fließt.
- 3. Stellen Sie die Web Application Firewall bereit. Verwenden Sie NetScaler ADM und das Web Application Firewall StyleBook, um die Web Application Firewall zu konfigurieren. Einzelheiten finden Sie im Abschnitt StyleBook weiter unten in diesem Handbuch.
- 4. Implementieren Sie die NetScaler Web App Firewall und OWASP Top Ten.

Die drei Schutzmaßnahmen der Web Application Firewall sind besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger eingesetzt als alle anderen. Daher sollten sie bei der ersten Bereitstellung implementiert werden. Sie sind:

- **HTML Cross-Site Scripting**: Untersucht Anfragen und Antworten auf Skripte, die versuchen, auf Inhalte auf einer anderen Website als der, auf der sich das Skript befindet, zuzugreifen oder diese zu ändern. Wenn diese Prüfung ein solches Skript findet, macht sie das Skript entweder unschädlich, bevor die Anfrage oder Antwort an ihr Ziel weitergeleitet wird, oder sie blockiert die Verbindung.
- **HTML-SQL-Injection**: Untersucht Anfragen, die Formularfelddaten enthalten, auf Versuche, SQL-Befehle in eine SQL-Datenbank einzufügen. Wenn diese Prüfung injizierten SQL-Code erkennt, blockiert sie entweder die Anfrage oder macht den injizierten SQL-Code unschädlich, bevor die Anfrage an den Webserver weitergeleitet wird.

Hinweis:

Stellen Sie sicher, dass Ihre Web App Firewall korrekt konfiguriert ist, damit die folgenden Bedingungen in Ihrer Konfiguration gelten:

- >* Wenn Benutzer die HTML Cross-Site Scripting-Pr
 üfung oder die HTML SQL Injection-Pr
 üfung (oder beide) aktivieren.
- >

>* Benutzergeschützte Websites akzeptieren Datei-Uploads oder enthalten Webformulare, die große POST-Textdaten enthalten können.

Weitere Informationen zum Konfigurieren der Web Application Firewall zur Behandlung dieses Falls finden Sie unter Konfigurieren der Anwendungsfirewall: Konfigurieren der Web App Firewall.

• **Pufferüberlauf**: Untersucht Anfragen, um Versuche zu erkennen, einen Pufferüberlauf auf dem Webserver zu verursachen.

Konfiguration der Web Application Firewall

Stellen Sie sicher, dass die NetScaler Web App Firewall bereits aktiviert ist und ordnungsgemäß funktioniert. Es wird empfohlen, NetScaler Web App Firewall mit dem Web Application Firewall StyleBook zu konfigurieren. Für die meisten Benutzer ist dies die einfachste Methode, die Web Application Firewall zu konfigurieren, und sie wurde entwickelt, um Fehler zu vermeiden. Sowohl die GUI als auch die Befehlszeilenschnittstelle richten sich an erfahrene Benutzer, hauptsächlich um eine bestehende Konfiguration zu ändern oder erweiterte Optionen zu verwenden.

SQL-Einschleusung

Die HTML-SQL-Injection-Prüfung der NetScaler Web App Firewall bietet spezielle Schutzmaßnahmen gegen die Injektion von nicht autorisiertem SQL-Code, der die Sicherheit von Benutzeranwendungen beeinträchtigen könnte. NetScaler Web App Firewall untersucht die Anforderungsnutzlast für injizierten SQL-Code an drei Stellen: 1) POST-Text, 2) Header und 3) Cookies. Weitere Informationen finden Sie unter HTML-SQL-Injection-Prüfung.

Siteübergreifendes Scripting

Die Prüfung HTML Cross-Site Scripting (Cross-Site Scripting) untersucht sowohl die Header als auch die POST-Texte von Benutzeranfragen auf mögliche Cross-Site-Scripting-Angriffe. Findet es ein Cross-Site-Script, modifiziert (transformiert) es entweder die Anfrage, um den Angriff unschädlich zu machen, oder blockiert die Anfrage. Weitere Informationen finden Sie unter HTML-Cross-Site-Scripting-Prüfung.

Überprüfung des Pufferüberlaufs

Die Pufferüberlaufprüfung erkennt Versuche, einen Pufferüberlauf auf dem Webserver zu verursachen. Wenn die Web Application Firewall feststellt, dass die URL, die Cookies oder der Header länger als die konfigurierte Länge sind, blockiert sie die Anfrage, da dies zu einem Pufferüberlauf führen kann. Weitere Informationen finden Sie unter Pufferüberlaufprüfung.

Virtuelles Patchen/Signaturen

Die Signaturen enthalten spezifische, konfigurierbare Regeln, um den Schutz von Benutzerwebsites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das Bestandteil eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Ein umfangreicher Satz vorkonfigurierter integrierter oder systemeigener Regeln bietet eine einfach zu bedienende Sicherheitslösung, die das Potenzial des Muster-

abgleichs nutzt, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen. Weitere Informationen finden Sie unter Signaturen.

Die NetScaler Web App Firewall unterstützt sowohl die **automatische als auch die manuelle Aktualisierung** von Signaturen. Wir empfehlen außerdem die **automatische Aktualisierung** für Signaturen zu aktivieren, um auf dem neuesten Stand zu bleiben.



Automatic signatures updates

Diese Signaturdateien werden in der AWS-Umgebung gehostet, und es ist wichtig, den ausgehenden Zugriff auf NetScaler-IP-Adressen von Netzwerk-Firewalls aus zuzulassen, um die neuesten Signaturdateien abzurufen. Die Aktualisierung von Signaturen auf dem NetScaler während der Verarbeitung von Echtzeitverkehr hat keine Auswirkung.

Analysen zur Anwendungssicherheit

Das**Application Security Dashboard**bietet einen ganzheitlichen Überblick über den Sicherheitsstatus von Benutzeranwendungen. Es zeigt beispielsweise wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen und Bedrohungsindizes. Das Anwendungssicherheits-Dashboard zeigt auch angriffsbezogene Informationen wie Syn-Attacken, Angriffe auf kleine Fenster und DNS-Flood-Angriffe für den entdeckten NetScaler an.

Hinweis:

Um die Metriken des Anwendungssicherheits-Dashboards anzuzeigen, sollte AppFlow for Security Insight auf den NetScaler-Instanzen aktiviert sein, die Benutzer überwachen möchten.

So zeigen Sie die Sicherheitsmetriken einer NetScaler-Instanz im Anwendungssicherheits-Dashboard an:

- 1. Melden Sie sich mit den Administratoranmeldeinformationen bei NetScaler ADM an.
- 2. Navigieren Sie zu**Applications > App Security Dashboard**und wählen Sie die Instanz-IP-Adresse aus der Geräteliste aus.

Benutzer können die im Application Security Investigator gemeldeten Unstimmigkeiten weiter untersuchen, indem sie auf die im Diagramm dargestellten Blasen klicken.

Zentralisiertes Lernen auf ADM

NetScaler Web App Firewall schützt Benutzer-Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site Scripting (XSS). Um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz zu bieten, müssen Benutzer ihren Datenverkehr auf Bedrohungen und verwertbare Echtzeitdaten zu Angriffen überwachen. Manchmal kann es sich bei den gemeldeten Angriffen um falsch positive Ergebnisse handeln, und diese müssen ausnahmsweise angegeben werden.

Das zentralisierte Lernen auf NetScaler ADM ist ein sich wiederholender Musterfilter, der es WAF ermöglicht, das Verhalten (die normalen Aktivitäten) von Benutzer-Webanwendungen zu erlernen. Basierend auf der Überwachung generiert die Engine eine Liste mit vorgeschlagenen Regeln oder Ausnahmen für jede Sicherheitsüberprüfung, die auf den HTTP-Verkehr angewendet wird.

Es ist viel einfacher, Entspannungsregeln mithilfe der Learning Engine bereitzustellen, als sie manuell als notwendige Entspannungen bereitzustellen.

Um die Lernfunktion bereitzustellen, müssen Benutzer zunächst ein Web Application Firewall-Profil (Satz von Sicherheitseinstellungen) auf dem Benutzer NetScaler konfigurieren. Weitere Informationen finden Sie unter Erstellen von Web App Firewall-Profilen.

NetScaler ADM generiert für jede Sicherheitsprüfung eine Liste mit Ausnahmen (Lockerungen). Als Administrator können Sie die Liste der Ausnahmen in NetScaler ADM überprüfen und entscheiden, ob Sie die Bereitstellung durchführen oder überspringen möchten.

Mit der WAF-Lernfunktion in NetScaler ADM können Sie:

- Konfigurieren Sie ein Lernprofil mit den folgenden Sicherheitsüberprüfungen.
 - Pufferüberlauf
 - Siteübergreifendes HTML-Scripting

Hinweis:

1 2

Die standortübergreifende Skriptbeschränkung gilt nur für FormField. - HTML-SQL-Injektion

> **Hinweis:**

```
>

    > Für die HTML-SQL-Injection-Prüfung müssen Benutzer `set -
    sqlinjectionTransformSpecialChars ON` und `set -sqlinjectiontype
    sqlspclcharorkeywords` in NetScaler konfigurieren.
```

- Überprüfen Sie die Lockerungsregeln in NetScaler ADM und entscheiden Sie, ob die erforderlichen Maßnahmen ergriffen werden sollen (Bereitstellen oder Überspringen).
- Erhalten Sie die Benachrichtigungen per E-Mail, Slack und ServiceNow.

• Verwenden Sie das Dashboard, um Details zur Entspannung anzuzeigen.

So verwenden Sie das WAF-Lernen in NetScaler ADM:

- 1. Das Lernprofil konfigurieren: Das Lernprofilkonfigurieren
- 2. Siehe die Entspannungsregeln: Entspannungsregeln und Leerlaufregeln anzeigen
- 3. Verwenden Sie das WAF-Lern-Dashboard: WAF-Lern-Dashboard anzeigen

StyleBooks

StyleBooks vereinfachen die Verwaltung komplexer NetScaler-Konfigurationen für Benutzeranwendungen. Ein StyleBook ist eine Vorlage, mit der Benutzer NetScaler-Konfigurationen erstellen und verwalten können. Hier geht es den Benutzern hauptsächlich um das StyleBook, mit dem die Web Application Firewall bereitgestellt wird. Weitere Informationen zu StyleBooks finden Sie unter Style-Books.

Analytik von Sicherheitseinblicken

Web- und Webdienstanwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Benutzer Einblicke in Art und Ausmaß vergangener, gegenwärtiger und drohender Bedrohungen, verwertbare Echtzeitdaten zu Angriffen und Empfehlungen für Gegenmaßnahmen. Security Insight bietet eine zentrale Lösung, mit der Benutzer den Sicherheitsstatus von Benutzeranwendungen beurteilen und Korrekturmaßnahmen zum Schutz von Benutzeranwendungen ergreifen können. Weitere Informationen finden Sie unter Security Insight.

Erhalten Sie detaillierte Informationen über Sicherheitsverletzungen

Benutzer möchten möglicherweise eine Liste der Angriffe auf eine Anwendung einsehen und Einblicke in die Art und Schwere der Angriffe, die von der ADC-Instanz ergriffenen Maßnahmen, die angeforderten Ressourcen und die Quelle der Angriffe erhalten.

Beispielsweise möchten Benutzer möglicherweise ermitteln, wie viele Angriffe auf Microsoft Lync blockiert wurden, welche Ressourcen angefordert wurden und welche IP-Adressen die Quellen haben.

Klicken Sie im**Security Insight-Dashboard**auf**Lync > Gesamtzahl der Verstöße**. Klicken Sie in der Tabelle in der Spaltenüberschrift**Aktion**ausgeführt auf das Filtersymbol, und wählen Sie dann**Blockiert**aus.

1	ppleation	Summary			Action Taken 1						
	Security Check Volation	Severity 🖓	Weistine Category 🖓	Action Taken V	Bached NorBicked	9	Location	Signature Violation	Visiation Name	Same Violation Violat	found in
ï	Sec UR	Critical	Broken Authentication and Section Management	Buched	hardsmad	without I have					Form Trail
ï	Sec URL	Critical	Boles Authentication and Seulon Management	Docked		w//testChird					Form Field
	Sec. URL	Critical	Broten duthentication and Section Management	Docked	Mp.010.102.43.0	Current and					form field
	Sec 185	Cillual	Broken Authentication and Sectors Management	Doched	Mp. 75. 15.41.6	(w//testil.html					Form Field
	Set UK.	Critical	Broken Authentication and Section Menagement	Doded	Mp.(10.10.41.6	/wi/featUnied					Form Field
	Set URL	Critical	Briten Authentication and Section Management	Disting	Mp.(70.10.41.0	(without hind					Form Field
	Sec. We	Critical	Broten Authentication and Sectors Management	Doched	Mp.(10.10.41.6	Var/Teal? Med					Form Field
	Sec URL	Citical	Broken Authentication and Section Menagement	Disting	Mp./70.10.41.6	2/wi/featUnied					Form Field
	Set URL	Citical	Broken Authentication and Section Menagement	Disted	Mp.(70.10.41.6	/w/test0.tend					Form Field
	244.055	Critical	Broken Authentication and Section Management	Ducked	Mp.(10.10.41.6	/without interd					Form Field
	Sec URL	Citical	Broken Authentication and Section Management	Bisched	Mp.010.101424	/wi/heat11.html					Form Frank
	Sec. 100	Called	Bookers Authentication and Service Mercarameter	Rindard	Manufacture and state	National Distance					From Date

Informationen zu den Ressourcen, die angefordert wurden, finden Sie in der Spalte**URL**. Informationen zu den Quellen der Angriffe finden Sie in der Spalte**Client-IP**.

Details zum Protokollausdruck anzeigen

NetScaler verwendet Protokollausdrücke, die mit dem Application Firewall-Profil konfiguriert sind, um Maßnahmen gegen Angriffe auf eine Anwendung im Benutzerunternehmen zu ergreifen. In **Security Insight**können Benutzer die Werte anzeigen, die für die von der ADC-Instanz verwendeten Protokollausdrücke zurückgegeben wurden. Zu diesen Werten gehören Anforderungsheader, Anforderungstext und so weiter. Zu diesen Werten gehören Anforderungsheader, Anforderungstext usw. Zusätzlich zu den Werten für den Protokollausdruck können Benutzer auch den Namen des Protokollausdrucks und den Kommentar für den Protokollausdruck anzeigen, der im Application Firewall-Profil definiert ist, das die ADC-Instanz verwendet hat, um Maßnahmen gegen den Angriff zu ergreifen.

Voraussetzungen:

Stellen Sie sicher, dass Benutzer:

- Konfigurieren Sie Protokollausdrücke im Application Firewall-Profil. Weitere Informationen finden Sie unter Application Firewall.
- Aktivieren Sie die auf Protokollausdrücken basierenden Security Insights-Einstellungen in NetScaler ADM. Führen Sie folgende Schritte aus:
 - Navigieren Sie zuAnalytics > Einstellungenund klicken Sie aufFunktionen f
 ür Analytics aktivieren.
 - Wählen Sie auf der Seite "Features für Analyticsaktivieren" im Abschnitt "Auf Logausdruck basierende Security InsightSetting" die Option "Enable Security Insight" aus

 Enable Features for Analytics
Multihop Settings
Enable the MultiPage Instance If the relevant displayment has more than one NetStater appliance or NetStater Cateway appliance between a single client and a server connection. NetScale MAS analyses the number of hops for herScaler Genway appliances through which the ICA connections pars. NetScaler MAS also enlines and constitutes the AppFore records from all the appliances. United MultiPage ()
Adapiter Trenchald Britiegs
Enable the adaptive threshold functionality feature to send a systep message to the systep server if the maximum number of hits on a UHL is greater than the threshold value set. The feature dynamically sets the threshold value in NetScare MMS for the maximum inumber of hits on each URL.
English Alaphie Transmit
YCP isolght Settings
Enable the TCP month feature of NetScales MAI to provide an easy and ecalable solution for monitoring the methods of the optimization techniques and congestion control statistics (a algorithmic used in NetScales appliances to avaid retwent congestion in data transmission
web insight Settings
Proble life Web Insight Realise is allow Redicate MAX to retrieve the performance reports of web applications (had informing and context in printial receiption being served) that are bound to the Nethanian ASC, Web Insight analysis visibility into enterprise web applications and allows IT administrators to manitor all web applications being served by the Nethanian ASC Web Insight and Interfere monotoring of applications. The Nethan Interference in the Interference i
Lag Expression Based Resurity insights Settings
trable Log Expression-based Security insights to report log expression data-configured with Application Rewell profile.
OK Cost

Beispielsweise möchten Sie möglicherweise die Werte des Protokollausdrucks anzeigen, der von der ADC-Instanz für die Aktion zurückgegeben wurde, die sie bei einem Angriff auf Microsoft Lync im Benutzerunternehmen ausgeführt hat.

Navigieren Sie im **Security Insight-Dashboard**zu**Lync** > **Gesamtzahl der Verstöße**. Klicken Sie in der Tabelle Anwendungszusammenfassung auf die URL, um die vollständigen Details des Verstoßes auf der Seite**Informationen zur Verletzung**anzuzeigen, einschließlich des Namens des Protokollausdrucks, des Kommentars und der von der ADC-Instanz für die Aktion zurückgegebenen Werte.

Gatzway Insight	>	Mielstien Jeferre	atlan				
 Security resigns 		violation inform	ation			~)
Settings				Violation	Information	n	
Trubisheeting							
Contraction		Attack Time	NA				
		Signature Volation					
System		Violation Name					
Downloads		Violation value					
		Security Check Violation	Start L	JR1,			
		Violation Category	Broker	n Authentication and Session Ma	nagement		
		Threat Index	5				
		Severity	Mediu	m			
		Action Taken	Blocke	ed .			
		URL	MIPO	/10.102.40.345/csrf_fh/fh/Wu/vow?f	field1=asfasd		
		Pound in	Other	Location			
		Client IP	10.503	1.63.79			
		Location	Banga	lane			
		Total Attacks	1				
			_				_
		Log Expression Name		Log Expression Comment	Log Expression	lan Walue	
		L6D/907		http request contains keyword	false		
		LSEXPRO		http request contains header	faise		
		LGEXPRE		http method expression	GET./csrt_Mc/ User-Agent: c OpenSiL/0.9 Hest: 33.182/ Accept: "/"	MC/NUM/Well-Actabl HTP/1.3 LV77327 UB6, 64-pc-Ima-gro/Hbcurl/7.19.7 Bk sib/1.2.2.3 Holen/1.15 00345	
		LGD/PR0		http method expression	true		
		LGEXPRE		http request contains header			
		LSEXPRI		http:request.header.contains-u ueragent	ouri/7.15/7.04 2/b/1.2.3.3 ib	86.,54-pt-linux-gnu) Ibcurl/7.19.7 Open55L/0.9-8k x8h/1.15	
		LGD/PR2		http method expression	false		
		LGD/PRS		http method expression			
				MATTER.	Medium.	Roken Authentication and Sevices Management	

Ermitteln Sie den Sicherheitsindex, bevor Sie die Konfiguration bereitstellen. Sicherheitsverletzungen treten auf, nachdem Benutzer die Sicherheitskonfiguration auf einer ADC-Instanz bereitgestellt haben. Benutzer möchten jedoch möglicherweise die Wirksamkeit der Sicherheitskonfiguration bewerten, bevor sie sie bereitstellen.

Beispielsweise möchten Benutzer möglicherweise den Sicherheitsindex der Konfiguration für die SAP-Anwendung auf der ADC-Instanz mit der IP-Adresse 10.102.60.27 bewerten.

Klicken Sie im **Security Insight-Dashboard** unter **Geräte** auf die IP-Adresse der ADC-Instanz, die Benutzer konfiguriert haben. Benutzer können sehen, dass sowohl der Bedrohungsindex als auch die Gesamtzahl der Angriffe 0 sind. Der Bedrohungsindex spiegelt direkt die Anzahl und Art der Angriffe auf die Anwendung wider. Keine Angriffe bedeuten, dass die Anwendung keiner Bedrohung ausgesetzt ist.

E 104	*	1 Adarbay 2016 10:20:20 - 2 Feb	inung 2016 10,00 25				
Overview Applications to Cattook Applica	analiigheat Threat Ind Ban kas Higheat Critic	m & Lowest Safety Index a Attacks		Mill of Lysten Security of 10.102	10.71 Device in Net Compliant		
Applicati	ons					48.0	etty -
			Thread Index	Safety Index	Total Alberto	Devices	
Lyne			Level a	Level 2	4932	10.102.01.75	
Sup			Level 0	Level 3		Threat Index	
Outloo			Level #	Level &		AS No.	
ShareP	via		Level #	Level 4		Mastum	
			9			Safety Index	

Klicken Sie auf**SAP > Safety Index > SAP_Profile**und bewerten Sie die angezeigten Sicherheitsindexinformationen.

application Summary			
Total Visitetiese	Violations By Severity Critical 5546	Wainteen By Action Blocked 5846	Violations By Category Cross alte Scripting \$846
Thread index Long 6 🙆 Galley brains			
laty index Summary			
Application Fermal Signatures: 1295/1300 Net Security Check: 1/14 Net	i Configuration Configurad Configurad	System 5 6/10 Not	configured
Application Firewall Configuration	New	Safety Bales	
Level 2	append.		
NetScaler System Security Level 2			

In der Zusammenfassung der Anwendungsfirewall können Benutzer den Konfigurationsstatus verschiedener Schutzeinstellungen einsehen. Wenn eine Einstellung auf Protokollierung gesetzt ist oder wenn eine Einstellung nicht konfiguriert ist, wird der Anwendung ein niedrigerer Sicherheitsindex zugewiesen.

Security Check	Lavel 3	Signatures Holistics	Land 1
	Biochert (4) Rev Biochert (4) Onabled (4)		Bischool (0) Bischool (0) Bischool (0) Bischool (1)
Prostan Exem		Configuration Status	
XMR, Yarlukeisen		Net Certigunal	
104, SDAFFeeR		Not Configured	
AND BELOWARD		Rent Carrileguereal	
1048, 1022		Not Certificanted	

Sicherheitsverstöße

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. Mit NetScaler ADM können Sie verwertbare Details zu Verstößen visualisieren, um Anwendungen vor Angriffen zu schützen.

Details zu Sicherheitsverletzungen bei Anwendungen anzeigen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfälliger für Angriffe geworden. Mit NetScaler ADM können Benutzer Details zu Verstößen visualisieren, die Konsequenzen nach sich ziehen, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu **Sicherheit** >Sicherheitsverstöße^{**}, um eine zentrale Lösung für Folgendes zu finden:

- Greifen Sie auf die Sicherheitsverletzungen der Anwendung basierend auf ihren Kategorien wie**Netzwerk,Bot**und**WAF**zu
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern

Um die Sicherheitsverletzungen in NetScaler ADM anzuzeigen, stellen Sie Folgendes sicher:

- Benutzer haben eine Premium-Lizenz für den NetScaler (für WAF- und BOT-Verstöße).
- Benutzer haben eine Lizenz für die virtuellen Load-Balancing- oder Content Switching-Server (für WAF und BOT) beantragt. Weitere Informationen finden Sie unter Lizenzierung auf virtuellen Servern verwalten.
- Benutzer können weitere Einstellungen aktivieren. Weitere Informationen finden Sie in dem Verfahren, das im Abschnitt Einrichtung der NetScaler-Produktdokumentation verfügbar ist: Einrichtung.

Kategorien von Verstößen

NetScaler ADM ermöglicht Benutzern die Anzeige der in Alle Verstößeverfügbaren Verstöße:

einrichten

Stellen Sie bei Verstößen sicher, dass**Metrics Collector** aktiviert ist. Standardmäßig ist**Metrics Collector** auf dem NetScaler aktiviert. Weitere Informationen finden Sie unterIntelligente App-Analyse konfigurieren.

Ermöglichen Sie erweiterte Sicherheitsanalysen

- Navigieren Sie zuNetzwerke>Instances>NetScaler, und wählen Sie den Instanztyp aus. Zum Beispiel MPX.
- Wählen Sie die NetScaler-Instanz aus und wählen Sie in der Liste**Aktion auswählen** die Option Analytics**konfigurieren**aus.
- Wählen Sie den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
- Gehen Sie im Fenster " Analysen aktivieren "wie folgt vor:
 - Wählen Sie**Web Insight**aus. Nachdem Benutzer Web Insight ausgewählt haben, wird die schreibgeschützte**Advanced Security Analytics-Option**automatisch aktiviert.

Hinweis:

Die Option**Advanced Security Analytics** wird nur für Premium-lizenzierte ADC-Instanzen angezeigt.

- Wählen Sie Logstream als Transportmodus
- Der Ausdruck ist standardmäßig wahr
- Klicken Sie auf **OK**

Enable Analytics	×
Selected Virtual Server - Load Balancing: 1	
Veb Insight	
Client Side Measurement	
Security Insight	
Bot Insight	
Advanced Security Analytics	
Advanced Options	
For ADC version less than 12.0 IPFIX is default Transport mode.	
Transport Mode	
Logstream OIPTIX	
Instance level options	
Enable HTTP X-Forwarded-For	
Citrix Gateway	
	_
Expression Configuration	_
OK Close	

Einstellungen für Web-Transaktionen aktivieren

• Navigieren Sie zu**Analytics>Einstellungen**.

Die Seite "Einstellungen "wird angezeigt.

- Klicken Sie auf Funktionen für Analytics aktivieren.
- Wählen Sie unter Einstellungen für Webtransaktionen die Option Alleaus.

 Enable Features for Analytics
Multing Institut
Enable the Wolfman Nature II the industry displayment has more than one Chin Addressing appliance between a single direct and unever connection. Chin ADM analyses the number of hops for Chin Satteway appliances through which the Chin connections pain. Chin ADM also saftees and connections the Appliances. (()) Satteway appliances through which the Chin Chin AdM also saftees and connections the Appliances and the appliances.
32 helph brillion
Evable the Y2 might have of D1x ADH's provide an easy and solidalit solidar for monitoring the metrics of the sphringston techniques and corgention control strengting for algorithms) and in D1x ADH appliances to assol screepedan in data termination.
Educate S2 regin
Web heavings
Evalue for Web maph hautors to disc Dish-Shiftis intrinse the performance reports of web applications (busi-indexing enclosered) that an isolation the Disn AGL. Web insight evalues shifting intra-interprise web applications and about it applications.
Mich Texture Exercises
Enable Web Transactions Tradew to allow Chris ADM to retria Web transactions from Chris ADK. Enable Web Transactions Assertation:
Insurity hulplin Lettings
Endbit op Spension based lacunts insiden to report to exponsion data-configured with Application Freewall profile. This will help use to see detailed togging
OM DESE

• Klicken Sie auf **Ok**.

Dashboard für Sicherheitsverletzungen

Im Dashboard für Sicherheitsverletzungen können Benutzer Folgendes einsehen:

• Die Gesamtzahl der Verstöße trat in allen NetScaler und Anwendungen auf. Die Gesamtzahl der Verstöße wird basierend auf der ausgewählten Zeitdauer angezeigt.

Security Wolations	6476.5012 60.000	9016/9020 23:00:00	v

• Gesamtzahl der Verstöße in jeder Kategorie.

Network	Bot	WAF
No violations detected	52K violations	55 violations

• Gesamtzahl der betroffenen ADCs, der Gesamtzahl der betroffenen Anwendungen und der häufigsten Verstöße, basierend auf der Gesamtzahl der Fälle und der betroffenen Anwendungen.

ADCr.Athenet Applications.Athened 5 7	
Top Violations Text on the associate of increases and the affinited applications: COLAR 200 9 9 9 9 9 9 9 9 9 9 9 9 9	Solvers (\$1.2) 507 Voldoves Understeller topical transfer topical transfer

Weitere Informationen zu Verstößen finden Sie unter Alle Verstöße.

Bot-Einblick

Konfigurieren Sie BOT Insight in NetScaler. Weitere Informationen finden Sie unter Bot.

Bots ansehen

Klicken Sie auf den virtuellen Server, um die Anwendungszusammenfassung anzuzeigen

I Meenting Refer to the second of the sec	t_vserver				C 12
	1 Murch *	23 March 2021 52:56:53 - 23, April 2020	0.1258/50		0 00
Amage RFS BO2 Bob By Seeting High 4108 K Larget Bot Caragory Linget Bot Source Unknown 41.55 K Larget Bot Source Unknown 41.55 K Amage K Bot Tuffk 8.52K Critical Teereity Mitcle • Medure Isoenity Mitcle • Low Seeting Mitcle	oplication Summary 🌒				
	Average RPS 0.02	Bots by Severity High: 41.08 K	Largest Bot Category	Largest Geo Source Unichown 41.33 K	Average N Bot Traffic 84,52%
Collocal Severity Alikado. Medium Severity Alikado. Ord Ord			a care		
Cutical Severity Attacks)	Ĩ	<u> 7</u>		
	Critical Senerity Attacks 🗧 Medi	un Severity Attacks 👋 Low Severity A	Radis		
Med d d A DEC CATEGORY TODAL & # DECPTED : # CATCON I # ALLOWED : # MATE LIMIT : # REDRIECT : # LOO Mediana (1)					
NOT CATEGORY TOTM, I # DROPPED # CAPTCHA # ALLOWED # RATE-LIMIT # REDRECT # PLOG Mini Turn 2 ¹¹ 4.0000 4.0000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2/7		•		 Inselfs (assist) (2010) The Confidence (2010) 	49 8
NOT CATISONY TODIL: # PORPHID # PALLOWID # MATE LIMIT # REDRECT # PALLOW MORE THAN 1000000000000000000000000000000000000	od I	8		 South South (1993) South South (1993) South South (1993) 	-
Home ALMON ALMON B B B B B B D <thd< th=""> D <thd< th=""> D <thd< th=""> D D D</thd<></thd<></thd<>	aal	0		 Andre Sanderfer (1993) Andre Sanderfer (1993) Andre Sanderfer (1993) 	
20 6 6 6 6 0 0 20	eef				# REDRECT # 100
	eed d		TODIL #DROPPID #GAPTCHA 4088 4088 0		2 # HEDHECT 1 # LOG 0 0

- 1. Enthält die Zusammenfassung der Anwendung, z. B.:
 - **Durchschnittliche RPS** Gibt die durchschnittlichen Bot-Transaktionsanfragen pro Sekunde (RPS) an, die auf virtuellen Servern empfangen wurden.
 - Bots nach Schweregrad Zeigt an, dass basierend auf dem Schweregrad die höchsten Bot-Transaktionen stattgefunden haben. Der Schweregrad wird nach Kritisch, Hoch, Mittelund Niedrigkategorisiert.

Wenn die virtuellen Server beispielsweise 11770 Bots mit hohem Schweregrad und 1550 Bots mit kritischem Schweregrad aufweisen, zeigt NetScaler ADM **Kritisch 1,55 K**unter**Bots nach Schweregrad**an.

• **Größte Bot-Kategorie** – Gibt an, dass basierend auf der Bot-Kategorie die meisten Bot-Angriffe stattgefunden haben.

Wenn die virtuellen Server beispielsweise 8000 blockierte Bots, 5000 zugelassene Bots und 10000 Bots mit überschrittener Rate Limit haben, zeigt NetScaler ADM unter**Größte Bot-KategorieRate Limit überschritten 10 K**an.

• **Größte Geoquelle** – Gibt an, dass je nach Region die meisten Bot-Angriffe stattfanden.

Wenn die virtuellen Server beispielsweise 5000 Bot-Angriffe in Santa Clara, 7000 Bot-Angriffe in London und 9000 Bot-Angriffe in Bangalore aufweisen, zeigt NetScaler ADM**Bangalore 9** Kunter**Größte Geo-Quelle**an.

- Durchschnittlicher Bot-Traffic in% Gibt die menschliche Bot-Rate an.
- 2. Zeigt den Schweregrad der Bot-Angriffe basierend auf Standorten in der Kartenansicht an
- 3. Zeigt die Arten von Bot-Angriffen an (Gut, Schlecht und alle)
- 4. Zeigt die Gesamtzahl der Bot-Angriffe zusammen mit den entsprechenden konfigurierten Aktionen an. Wenn Sie beispielsweise Folgendes konfiguriert haben:
 - IP-Adressbereich (192.140.14.9 bis 192.140.14.254) als Blocklisten-Bots und Auswahl von Löschen als Aktion für diese IP-Adressbereiche
 - IP-Bereich (192.140.15.4 bis 192.140.15.254) als Blocklisten-Bots und ausgewählt, um eine Protokollnachricht als Aktion für diese IP-Bereiche zu erstellen

In diesem Szenario zeigt NetScaler ADM Folgendes an:

- Gesamtzahl der blockierten Bots
- Gesamtzahl Bots unter Dropped
- Gesamtzahl der Bots unter Log

CAPTCHA-Bots ansehen

Auf Webseiten sollen CAPTCHAs erkennen, ob der eingehende Traffic von einem Menschen oder einem automatisierten Bot stammt. Um die CAPTCHA-Aktivitäten in NetScaler ADM anzuzeigen, müssen Benutzer CAPTCHA als Bot-Aktion für IP-Reputation und Techniken zur Erkennung von Gerätefingerabdrücken in einer NetScaler ADM-Instanz konfigurieren. Weitere Informationen finden Sie unter:Bot-Verwaltung konfigurieren.

Die folgenden CAPTCHA-Aktivitäten werden von NetScaler ADM in Bot Insight angezeigt:

- **Captcha-Versuche überschritten** Gibt die maximale Anzahl von CAPTCHA-Versuchen an, die nach Anmeldefehlern unternommen wurden
- **Captcha-Client stummgeschaltet** Gibt die Anzahl der Client-Anfragen an, die verworfen oder umgeleitet wurden, da diese Anfragen zuvor mit der CAPTCHA-Herausforderung als fehlerhafte Bots erkannt wurden
- Mensch Bezeichnet die Captcha-Eingaben, die von menschlichen Benutzern vorgenommen wurden
- Ungültige Captcha-Antwort- Gibt die Anzahl der falschen CAPTCHA-Antworten an, die vom Bot oder Menschen empfangen wurden, wenn NetScaler eine CAPTCHA-Herausforderung sendet

BOT CATEGORY	TOTAL ATTACKS 🔅	# DROPPED 🔅	# CAPTO IA 😳	# ALLOWED 🔅	# RATE LIMIT	# REDIRECT 🔅	#LOG 0
Captche Attempts Exceeded	11	11	0	0	0	0	0
Captche Client Muted	z	0	0	0	0	2	0
Cowler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Involid Captcha Response	40	33	0	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Scraper Search Engine	33 155	33 155	0 0	0 0	0	0	0 0
Scraper Search Engine Site Monitor	33 155 57	33 155 57	0 0	0 0	0 0	0	0 0 0
Scaper Search Engine Site Monitor Teel	33 155 57 82	33 155 57 82	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
Scaper Search Engine Site Monitor Teel Uncategorized	33 155 57 82 0	33 155 57 82 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0

Botfallen ansehen

Um Bot-Traps in NetScaler ADM anzuzeigen, müssen Sie die Bot-Trap in NetScaler konfigurieren. Weitere Informationen finden Sie unter:Bot-Verwaltung konfigurieren.

pplications	5								1.00	any in	ar Berte	~	Instances
fasal Bots on In	stance 18.3	06154240	are 9.77 K										BUR, 340 (30.304.254.340)
	Total Bots	Total Human Browsets	Bot Human Ratio	Signatured Bots	Fingerprint ed Stats	Rate Receil Bots	ar Reputation Bots	Whitefair Bots	Backler Bots	Bot Tape	175.844		
test_Ib1	440	0	300:0	0	0	0	0	0	0	0	440		
test_vserve	9.33 K	•	100:0		•	0	0	•	0	5	9.32 K		

Um die Botfalle zu identifizieren, ist auf der Webseite ein Skript aktiviert, das vor Menschen verborgen ist, aber nicht vor Bots. NetScaler ADM identifiziert und meldet die Bot-Traps, wenn dieses Skript von den Bots aufgerufen wird.

Klicken Sie auf den virtuellen Server und wählen Sie Zero Pixel Request

BOT CATEGORY	TOTAL :	# DROPPED :	JE CAPICHA 0	# ALLOWED 0	# RATE LIMIT	# REDIRECT 0	1106 0
Invalid DeviceRP	33450	33450	0	0	0	0	0
Zero Pixel Request	245	0	0	0	0	0	246
Human	100	0	0	100	0	0	0

Bot-Details anzeigen

Weitere Informationen erhalten Sie, indem Sie unter **Bot-Kategorie auf den Bot-Angriffstyp**klicken.

Die Details wie Angriffszeit und Gesamtzahl der Bot-Angriffe für die ausgewählte Captcha-Kategorie werden angezeigt.

ina ja Bantinnäght ja penne, Ba ja Bent-Mitach Category			
Bot Category - "Capitcha Attempts Exceeded"	×	Last 1 Month	v Search
ineline Details		17 War 2020, 1110	10.16 Apr 2020, 11.10
E			

Benutzer können das Balkendiagramm auch ziehen, um den spezifischen Zeitraum auszuwählen, der bei Bot-Angriffen angezeigt werden soll.



Um weitere Informationen zum Bot-Angriff zu erhalten, klicken Sie zum Erweitern.

	27627M	1.00	87.96	Marrie .	100.000	an once of	APRIL 10	LOCAL DESIGNATION OF	MONTON.	
	140.003		**	1004	-	market .	Market .	Respire	Ass. 34, 361	
×	50p 09 0248 P.,	101021.88	Bad	onball	Drap	BLICKLIST	BlackLST	Bangatore	/0448_03_031-	
	Instance IP: 30.00 HTTP Request UR Region: Kamataka	6354240 Er/bleck_list_test.ht	imi	Total Cour Paul	Bots: 1 stry Code: IN le Name: bot_profit					
	-	-	-	1004	-	Barbaro	Ballot	Respire	Ast, 16, 261.	

- Instanz-IP Gibt die IP-Adresse der NetScaler-Instanz an.
- **Gesamtzahl der Bots** Gibt an, dass die Gesamtzahl der Bot-Angriffe für diesen bestimmten Zeitraum stattgefunden hat.
- HTTP-Anforderungs-URL Gibt die URL an, die für Captcha-Berichte konfiguriert ist.
- Landesvorwahl Gibt das Land an, in dem der Bot-Angriff stattgefunden hat.
- **Region** Gibt die Region an, in der der Bot-Angriff stattgefunden hat.
- **Profilname** Gibt den Profilnamen an, den Benutzer bei der Konfiguration angegeben haben.

Erweiterte Suche

Benutzer können auch das Suchtextfeld und die Zeitdauerliste verwenden, wo sie Bot-Details gemäß den Benutzeranforderungen anzeigen können. Wenn Benutzer auf das Suchfeld klicken, erhalten sie im Suchfeld die folgende Liste mit Suchvorschlägen.

• Instanz-IP – IP-Adresseder NetScaler-Instanz.

- **Client-IP** Client-IP-Adresse.
- Bot-Typ Bot-Typ wie Gut oder Schlecht.
- Schweregrad Schweregrad des Bot-Angriffs.
- Aktionergriffen –Maßnahmen, die nach dem Bot-Angriff ergriffen wurden, z. B. Drop, Keine Aktion, Redirect.
- **Bot-Kategorie** Kategorie des Bot-Angriffs wie Blockliste, Zulassungsliste, Fingerabdruck. Basierend auf einer Kategorie können Benutzer ihr eine Bot-Aktion zuordnen.
- **Bot-Detection** Bot-Erkennungstypen (Blockliste, Zulassungsliste usw.), die Benutzer auf NetScaler konfiguriert haben.
- Standort Region/Land, in dem der Bot-Angriff stattgefunden hat
- Request-url URL, die die möglichen Bot-Angriffe enthält

Benutzer können in den Benutzersuchabfragen auch Operatoren verwenden, um den Fokus der Benutzersuche einzugrenzen. Zum Beispiel, wenn Benutzer alle bösartigen Bots sehen möchten:

- Klicken Sie auf das Suchfeld und wählen Sie Bot-Type
- Klicken Sie erneut auf das Suchfeld und wählen Sie den Operator =
- Klicken Sie erneut auf das Suchfeld und wählen Sie Schlecht
- Klicken Sie auf**Suchen**, um die Ergebnisse anzuzeigen



Ungewöhnlich hohe Anfragerate

Benutzer können den eingehenden und ausgehenden Verkehr von oder zu einer Anwendung steuern. Ein Bot-Angriff kann eine ungewöhnlich hohe Anforderungsrate verursachen. Wenn Benutzer beispielsweise eine Anwendung so konfigurieren, dass sie 100 Anfragen pro Minute zulässt, und wenn Benutzer 350 Anfragen beobachten, handelt es sich möglicherweise um einen Bot-Angriff.

Mithilfe des Indikators**Ungewöhnlich hohe Anforderungsrate**können Benutzer die ungewöhnliche Anforderungsrate analysieren, die an die Anwendung eingegangen ist.

VIOLATION DETAILS						
Dependive Client Connections 4	Unusually High Req	uest Rate measurement				
Unusually High Request Rate 2	Admonstration from u	uol Request rate on a eserver	indicates passibility of an	INFARMS.		
2 Apr 101 10 arm Behaviour based	What Happened					
Unusually Large Download V. at	Last Occurred time	Total Occurrences	Applications Affects	ed.		
Non-Dy-112-21 Behavior based	E3 Apr 8:30 am	7	1			
Simularly Large Uplead Value 19						
T-lpr 10.01 arts Behaviour based	Event Details					
	Affected Application	na_101_01_01_010101	117.58) (P)			
	Request Rate					
	1.00					Read years
						1111
		\sim	~			
		1944 X244	15.64	14 MA	in a	447 HT 04

UnterVeranstaltungsdetailskönnen Benutzer Folgendes anzeigen:

- Die betroffene Anwendung. Benutzer können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Die Grafik zeigt alle Verstöße
- Zeitpunkt des Auftretens des Verstoßes
- Die Erkennungsmeldung für den Verstoß, in der die Gesamtzahl der eingegangenen Anfragen und der Prozentsatz der eingegangenen Anfragen angegeben sind, die über den erwarteten Anforderungen liegen
- Der akzeptierte Bereich der erwarteten Anforderungsraten reicht von der Anwendung ab

Bot-Erkennung

Das NetScaler Bot-Managementsystem verwendet verschiedene Techniken, um den eingehenden Bot-Verkehr zu erkennen. Die Techniken werden als Erkennungsregeln verwendet, um den Bot-Typ zu erkennen.

Konfiguration des Bot-Managements mithilfe der GUI Benutzer können das NetScaler-Bot-Management konfigurieren, indem sie zuerst die Funktion auf der Appliance aktivieren. Weitere Informationen finden Sie unter Bot-Erkennung.

IP-Reputation

IP-Reputation ist ein Tool, das IP-Adressen identifiziert, die unerwünschte Anfragen senden. Mithilfe der IP-Reputationsliste können Sie Anfragen ablehnen, die von einer IP-Adresse mit einem schlechten Ruf kommen.

IP-Reputation mithilfe der GUI konfigurieren Diese Konfiguration ist eine Voraussetzung für die Bot-IP-Reputationsfunktion. Weitere Informationen finden Sie unter IP-Reputation.

Automatisches Update für Bot-Signaturen Die statische Bot-Signaturtechnik verwendet eine Signatur-Suchtabelle mit einer Liste guter und schlechter Bots. Weitere Informationen finden Sie unter Automatische Signaturaktualisierung.

Die zehn besten Adressen von NetScaler Web App Firewall und OWASP – 2021

Das Open Web Application Security Project (OWAP) hat die OWASP Top 10 für 2021 für die Sicherheit von Webanwendungen veröffentlicht. Diese Liste dokumentiert die häufigsten Sicherheitslücken in Webanwendungen und ist ein guter Ausgangspunkt für die Bewertung der Websicherheit. In diesem Abschnitt wird erklärt, wie Sie die NetScaler Web App Firewall konfigurieren, um diese Fehler zu beheben. WAF ist als integriertes Modul in NetScaler (Premium Edition) und einer kompletten Palette von Appliances verfügbar.

Die 10 besten OWASP 2021	Funktionen der NetScaler Web App Firewall
A1:2021 Fehlerhafte Zugriffssteuerung	AAA, Autorisierungssicherheitsfunktionen im
	AAA-Modul von NetScaler, Formularschutz und
	Cookie-Manipulationsschutz, StartURL und
	ClosureURL
A2:2021 - Kryptografische Fehler	Kreditkartenschutz, Safe Commerce,
	Cookie-Proxying und Cookie-Verschlüsselung
A3:2021- Einschleusung	Verhinderung von Injektionsangriffen (SQL oder
	andere benutzerdefinierte Injektionen wie OS
	Command Injection, XPath Injection und
	LDAP-Injection), Signaturfunktion zur
	automatischen Aktualisierung

Das vollständige OWASP Top 10-Dokument ist unter OWASPTop Ten verfügbar.

Die 10 besten OWASP 2021	Funktionen der NetScaler Web App Firewall
A5:2021 Fehlkonfiguration der Sicherheit	Dieser Schutz umfasst WSI-Prüfungen,
	XML-Nachrichtenvalidierung und
	XML-SOAP-Fehlerfilterprüfung
A6:2021 – Sicherheitslücke und veraltete	Berichte über Sicherheitslücken, Vorlagen für die
Komponenten	Anwendungs-Firewall und benutzerdefinierte
	Signaturen
A7:2021 – Fehler bei Identifizierung und	AAA, Schutz vor Cookie-Manipulation,
Authentifizierung	Cookie-Proxying, Cookie-Verschlüsselung,
	CSRF-Tagging, SSL verwenden
A8:2021 – Fehler bei der Software- und	XML-Sicherheitsprüfungen, GWT-Inhaltstyp,
Datenintegrität	benutzerdefinierte Signaturen, Xpath für JSON und XML
A9:2021 – Fehler bei der	Benutzerkonfigurierbares benutzerdefiniertes
Sicherheitsprotokollierung und Überwachung	Protokollierungs-, Verwaltungs- und
	Analysesystem

A1:2021 Fehlerhafte Zugriffssteuerung

Einschränkungen dessen, was authentifizierte Benutzer tun dürfen, werden oft nicht ordnungsgemäß durchgesetzt. Angreifer können diese Sicherheitslücken ausnutzen, um auf nicht autorisierte Funktionen und Daten zuzugreifen, z. B. auf Konten anderer Benutzer zuzugreifen, vertrauliche Dateien einzusehen, Daten anderer Benutzer zu ändern und Zugriffsrechte zu ändern.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die AAA-Funktion, die Authentifizierung, Autorisierung und Prüfung für den gesamten Anwendungsverkehr unterstützt, ermöglicht es einem Site-Administrator, die Zugriffskontrollen mit der ADC-Appliance zu verwalten.
- Die Sicherheitsfunktion Autorisierung im AAA-Modul der ADC-Appliance ermöglicht es der Appliance, zu überprüfen, auf welche Inhalte auf einem geschützten Server sie jedem Benutzer Zugriff gewähren soll.
- Konsistenz von Formularfeldern: Wenn Objektreferenzen als versteckte Felder in Formularen gespeichert werden, können Sie mithilfe der Konsistenz von Formularfeldern überprüfen, ob diese Felder bei nachfolgenden Anfragen nicht manipuliert werden.
- Cookie-Proxying und Cookie-Konsistenz: Objektreferenzen, die in Cookie-Werten gespeichert sind, können mit diesen Schutzmaßnahmen validiert werden.

• URL-Prüfung mit URL-Schließung starten: Ermöglicht Benutzern den Zugriff auf eine vordefinierte Zulassungsliste von URLs. Die URL-Schließung erstellt eine Liste aller URLs, die während der Benutzersitzung in gültigen Antworten gesehen wurden, und ermöglicht automatisch den Zugriff darauf während dieser Sitzung.

A2:2021 - Kryptografische Fehler

Viele Webanwendungen und APIs schützen sensible Daten wie Finanzen, Gesundheitswesen und personenbezogene Daten nicht ordnungsgemäß. Angreifer können solche schlecht geschützten Daten stehlen oder ändern, um Kreditkartenbetrug, Identitätsdiebstahl oder andere Verbrechen zu begehen. Sensible Daten können ohne zusätzlichen Schutz, z. B. Verschlüsselung im Ruhezustand oder bei der Übertragung, gefährdet werden und erfordern besondere Vorsichtsmaßnahmen, wenn sie mit dem Browser ausgetauscht werden.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die Web Application Firewall schützt Anwendungen davor, sensible Daten wie Kreditkartendaten preiszugeben.
- Sensible Daten können im Safe Commerce-Schutz als sichere Objekte konfiguriert werden, um eine Offenlegung zu vermeiden.
- Alle sensiblen Daten in Cookies können durch Cookie-Proxying und Cookie-Verschlüsselung geschützt werden.

A3:2021- Einschleusung

Injektionsfehler wie SQL-, NoSQL-, OS- und LDAP-Injection treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die feindlichen Daten des Angreifers können den Interpreter dazu verleiten, unbeabsichtigte Befehle auszuführen oder ohne entsprechende Autorisierung auf Daten zuzugreifen.

XSS-Fehler treten auf, wenn eine Anwendung nicht vertrauenswürdige Daten ohne ordnungsgemäße Validierung oder Escaping in eine neue Webseite einfügt oder eine bestehende Webseite mithilfe einer Browser-API, die HTML oder JavaScript erstellen kann, mit vom Benutzer bereitgestellten Daten aktualisiert. XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, die Benutzersitzungen kapern, Websites verunstalten oder den Benutzer auf bösartige Websites umleiten können.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die Funktion zur Verhinderung von SQL-Injection schützt vor häufigen Injection-Angriffen. Zum Schutz vor jeder Art von Injektionsangriffen, einschließlich XPath und LDAP, können benutzerdefinierte Injektionsmuster hochgeladen werden. Dies gilt sowohl für HTML- als auch für XML-Nutzlasten.
- Die Funktion zur automatischen Aktualisierung der Signatur hält die Injektionssignaturen auf dem neuesten Stand.
- Die Funktion zum Schutz von Feldformaten ermöglicht es dem Administrator, jeden Benutzerparameter auf einen regulären Ausdruck zu beschränken. Sie können beispielsweise erzwingen, dass ein PLZ-Feld nur ganze Zahlen oder sogar fünfstellige Ganzzahlen enthält.
- Die Konsistenz von Formularfeldern überprüft jedes übermittelte Benutzerformular anhand der Signatur des Benutzersitzungsformulars, um die Gültigkeit aller Formularelemente sicherzustellen.
- Pufferüberlaufprüfungen stellen sicher, dass die URL, Header und Cookies in den richtigen Grenzwerten sind, sodass Versuche, große Skripts oder Code einzufügen, blockiert werden.
- Der XSS-Schutz schützt vor gängigen XSS-Angriffen. Benutzerdefinierte XSS-Muster können hochgeladen werden, um die Standardliste der zulässigen Tags und Attribute zu ändern. Die ADC WAF verwendet eine Positivliste zulässiger HTML-Attribute und -Tags, um XSS-Angriffe zu erkennen. Dies gilt sowohl für HTML- als auch für XML-Nutzlasten.
- ADC WAF blockiert alle Angriffe, die im OWASP XSS Filter Evaluation Cheat Sheet aufgeführt sind.
- Die Feldformatprüfung verhindert, dass ein Angreifer unangemessene Webformulardaten sendet, was ein potenzieller XSS-Angriff sein kann.
- Konsistenz von Formularfeldern.

A5:2021 - Fehlkonfiguration der Sicherheit

Eine Fehlkonfiguration der Sicherheit ist das am häufigsten auftretende Problem. Dies ist häufig auf unsichere Standardkonfigurationen, unvollständige oder improvisierte Konfigurationen, offenen Cloud-Speicher, falsch konfigurierte HTTP-Header und ausführliche Fehlermeldungen mit vertraulichen Informationen zurückzuführen. Alle Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen nicht nur sicher konfiguriert sein, sondern sie müssen auch rechtzeitig gepatcht und aktualisiert werden.

Viele ältere oder schlecht konfigurierte XML-Prozessoren werten externe Entitätsreferenzen in XML-Dokumenten aus. Externe Entitäten können verwendet werden, um interne Dateien mithilfe des Datei-URI-Handlers, interner Dateifreigaben, interner Portscans, Remotecodeausführung und Denial-of-Service-Angriffe offenzulegen.
NetScaler Web App Firewall-Schutzmaßnahmen

- Der von der Application Firewall generierte PCI-DSS-Bericht dokumentiert die Sicherheitseinstellungen auf dem Firewall-Gerät.
- Berichte der Scan-Tools werden in ADC-WAF-Signaturen konvertiert, um Sicherheitsfehlkonfigurationen zu behandeln.
- Die NetScaler Web App Firewall Web Application Firewall unterstützt Cenzic, IBM AppScan (Enterprise und Standard), Qualys, TrendMicro, WhiteHat und benutzerdefinierte Schwachstellen-Scan-Berichte.
- Zusätzlich zur Erkennung und Blockierung gängiger Anwendungsbedrohungen, die für Angriffe auf XML-basierte Anwendungen (d. h. Cross-Site Scripting, Befehlsinjektion usw.) angepasst werden können.
- Die NetScaler Web App Firewall Web Application Firewall umfasst eine Vielzahl von XMLspezifischen Sicherheitsvorkehrungen. Dazu gehören die Schemavalidierung zur gründlichen Überprüfung von SOAP-Nachrichten und XML-Payloads sowie eine leistungsstarke Prüfung von XML-Anhängen zum Blockieren von Anhängen, die schädliche ausführbare Dateien oder Viren enthalten.
- Automatische Methoden zur Überprüfung des Datenverkehrs blockieren XPath-Injection-Angriffe auf URLs und Formulare, die darauf abzielen, Zugriff zu erlangen.
- Die NetScaler Web App Firewall Web Application Firewall vereitelt auch verschiedene DoS-Angriffe, darunter externe Entitätsverweise, rekursive Expansion, übermäßige Verschachtelung und bösartige Nachrichten, die entweder lange oder viele Attribute und Elemente enthalten.

A6:2021 – Anfällige und veraltete Komponenten

Komponenten wie Bibliotheken, Frameworks und andere Softwaremodule werden mit denselben Rechten wie die Anwendung ausgeführt. Wenn eine anfällige Komponente ausgenutzt wird, kann ein solcher Angriff zu schwerwiegenden Datenverlusten oder Serverübernahmen führen. Anwendungen und APIs, die Komponenten mit bekannten Sicherheitslücken verwenden, können die Anwendungsabwehr untergraben und verschiedene Angriffe und Auswirkungen ermöglichen.

NetScaler Web App Firewall-Schutzmaßnahmen

- Wir empfehlen, die Komponenten von Drittanbietern auf dem neuesten Stand zu halten.
- Sicherheitslücken-Scan-Berichte, die in ADC-Signaturen umgewandelt werden, können verwendet werden, um diese Komponenten virtuell zu patchen.

- Anwendungsfirewall-Vorlagen, die für diese anfälligen Komponenten verfügbar sind, können verwendet werden.
- Benutzerdefinierte Signaturen können an die Firewall gebunden werden, um diese Komponenten zu schützen.

A7:2021 - Fehlerhafte Authentifizierung

Anwendungsfunktionen im Zusammenhang mit Authentifizierung und Sitzungsmanagement werden häufig falsch implementiert, sodass Angreifer Passwörter, Schlüssel oder Sitzungstoken kompromittieren oder andere Implementierungsfehler ausnutzen können, um vorübergehend oder dauerhaft die Identitäten anderer Benutzer anzunehmen.

NetScaler Web App Firewall-Schutzmaßnahmen

- Das NetScaler AAA-Modul führt die Benutzerauthentifizierung durch und bietet Single Sign-On-Funktionalität für Back-End-Anwendungen. Dies ist in die NetScaler AppExpert Policy-Engine integriert, um benutzerdefinierte Richtlinien auf der Grundlage von Benutzer- und Gruppeninformationen zu ermöglichen.
- Mithilfe von SSL-Offloading- und URL-Transformationsfunktionen kann die Firewall Websites auch dabei unterstützen, sichere Transportschichtprotokolle zu verwenden, um den Diebstahl von Sitzungstoken durch Netzwerk-Sniffing zu verhindern.
- Cookie-Proxying und Cookie-Verschlüsselung können eingesetzt werden, um den Diebstahl von Cookies vollständig zu verhindern.

A8:2021 – Fehler bei der Software- und Datenintegrität

Eine unsichere Deserialisierung führt häufig zur Ausführung von Code aus der Ferne. Auch wenn Deserialisierungsfehler nicht zur Remotecodeausführung führen, können sie für Angriffe verwendet werden, darunter Replay-Angriffe, Injection-Angriffe und Angriffe zur Rechteeskalation.

NetScaler Web App Firewall-Schutzmaßnahmen

- JSON-Nutzlastinspektion mit benutzerdefinierten Signaturen.
- XML-Sicherheit: schützt vor XML Denial of Service (xDoS), XML SQL und Xpath Injection und Cross-Site Scripting, Formatprüfungen, Einhaltung von WS-I-Grundprofilen und Überprüfung von XML-Anhängen.
- Feldformatprüfungen sowie Cookie-Konsistenz und Feldkonsistenz können verwendet werden.

A9:2021 – Fehler bei der Sicherheitsprotokollierung und Überwachung

Eine unzureichende Protokollierung und Überwachung in Verbindung mit einer fehlenden oder ineffektiven Integration in die Reaktion auf Vorfälle ermöglichen es Angreifern, Systeme weiter anzugreifen, ihre Persistenz aufrechtzuerhalten, auf mehr Systeme umzusteigen und Daten zu manipulieren, zu extrahieren oder zu zerstören. Die meisten Studien zeigen, dass die Zeit bis zur Entdeckung eines Verstoßes über 200 Tage beträgt, was in der Regel eher von externen Parteien als von internen Prozessen oder Überwachungen erkannt wird.

NetScaler Web App Firewall-Schutzmaßnahmen

- Wenn die Protokollaktion für Sicherheitsprüfungen oder Signaturen aktiviert ist, enthalten die resultierenden Protokollmeldungen Informationen über die Anfragen und Antworten, die die Anwendungsfirewall beim Schutz Ihrer Websites und Anwendungen beobachtet hat.
- Die Anwendungsfirewall bietet den Komfort, die integrierte ADC-Datenbank zu verwenden, um die Standorte zu identifizieren, die den IP-Adressen entsprechen, von denen bösartige Anfragen stammen.
- Ausdrücke im Standardformat (PI) bieten die Flexibilität, die in den Protokollen enthaltenen Informationen anzupassen, wobei die Option besteht, die spezifischen Daten hinzuzufügen, die in den von der Anwendungs-Firewall generierten Protokollmeldungen erfasst werden sollen.
- Die Anwendungsfirewall unterstützt CEF-Protokolle.

Referenzen

- HTML-SQL-Injektionsprüfung
- XML-SQL-Injektionsprüfung
- Den HTML Cross-Site Scripting Check über die Befehlszeile konfigurieren
- Siteübergreifende XML-Skriptprüfung
- Verwenden der Befehlszeile zur Konfiguration der Sicherheitsüberprüfung für den Pufferüberlauf
- Signaturobjekt hinzufügen oder entfernen
- Konfiguration oder Änderung eines Signature-Objekts
- Aktualisierung eines Signaturobjekts
- Integration von Snort-Regeln
- Bot-Erkennung

• Bereitstellen einer NetScaler VPX Instanz unter Microsoft Azure

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.

 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.

NSDoc0330VM - Network ir	nterfaces	
	Search network interfaces	
ags 🗸	NAME	^ PUBLIC IP ADD
X Diagnose and solve problems	nsdoc0330vm923	13.78.187.15
SETTINGS		
👰 Availability set		
😑 Disks		
Extensions		
R Network interfaces		
Size		

2. Klicken Sie auf IP-Konfigurationen, und klicken Sie dann auf Hinzufügen.

Microsoft Azure NSDoc0330VM - Network interfaces > nsdoc0330vm923 - IP configurations						
	≡ Insdoc0330vm923 - IP configurations					
+		🛨 Add 🖪 Si	ave 🗙 Discard			
	Overview	IP forwarding s	ettings			
	Activity log	Virtual network			NSDoc0330VNET	
	Access control (IAM)					
٩	nags 🖉	IP configuration	ns		Frontend (192.0.0.0/24)	
8	SETTINGS				Hontena (152.0.0.0/24)	
2	IP configurations		nfigurations			
	DNS servers	NAME	IP VERSION	ТҮРЕ	PRIVATE IP ADDRE	
*	🔋 Network security group	ipconfig1	IPv4	Primary	192.0.0.4 (Static)	
Ŷ		ipconfig2	IPv4	Secondary	192.0.0.5 (Static)	
		ipconfig3	IPv4	Secondary	192.0.0.6 (Static)	

3. Geben Sie die erforderlichen Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf **OK**.

Add IP configuration	
* Name	
PrivateIP5	~
Туре	
Primary Secondary	
Primary IP configuration already exists	
Private IP address settings	
Allocation	
Dynamic Static	
* IP address	
192.0.0.8	~
Public ID address	
Disabled Enabled	
ок	

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

January 15, 2025

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.

```
1
     $locName="westcentralus"
2
3
     $rgName="Azure-MultiIP"
4
     $nicName1="VM1-NIC1"
5
6
7
     $vNetName="Azure-MultiIP-vnet"
8
     $vNetAddressRange="11.6.0.0/16"
9
     $frontEndSubnetName="frontEndSubnet"
11
     $frontEndSubnetRange="11.6.1.0/24"
13
14
     $prmStorageAccountName="multiipstorage"
15
16
     $avSetName="multiip-avSet"
17
18
19
     $vmSize="Standard\_DS4\_V2" (This parameter creates a VM with up to
         four NICs.)
```

Hinweis:

Die Mindestanforderung für eine VPX-Instanz sind 2 vCPUs und 2 GB RAM.

```
1
     $publisher="Citrix"
2
     $offer="netscalervpx110-6531" (You can use different offers.)
3
4
     $sku="netscalerbyol" (According to your offer, the SKU can be
5
        different.)
6
     $version="latest"
7
8
9
     $pubIPName1="PIP1"
10
     $pubIPName2="PIP2"
11
12
13
     $domName1="multiipvpx1"
14
```

\$domName2="multiipvpx2" 15 16 \$vmNamePrefix="VPXMultiIP" 17 18 \$osDiskSuffix="osmultiipalbdiskdb1" 19 21 **Network Security Group (NSG)-related information**: 23 \$nsgName="NSG-MultiIP" 24 \$rule1Name="Inbound-HTTP" 26 27 \$rule2Name="Inbound-HTTPS" 28 \$rule3Name="Inbound-SSH" 29 31 \$IpConfigName1="IPConfig1" 32 \$IPConfigName2="IPConfig-2" 33 34 \$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 -Quelladresspräfix Internet
-Quellportbereich * -Zieladresspräfix * -Zielportbereich 80
```

```
$rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
Beschreibung "HTTPS zulassen" -Zugriff zulassen -Protokoll TCP
-Richtung eingehend -Priorität 110 -Quelladresspräfix Internet
-Quellportbereich * -Zieladresspräfix * -Zielportbereich 443
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
Beschreibung "SSH zulassen" -Zugriff zulassen -Protokoll TCP -
Richtung eingehend -Priorität 120 -Quelladresspräfix Internet -
Quellportbereich * -Zieladresspräfix * -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.

```
$IPAddress1="11.6.1.27"
1
    $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
2
        Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress
        $pip1 - Primary
3
    $IPAddress2="11.6.1.28"
    $IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
4
        Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress
        $pip2
5
    $IPAddress3="11.6.1.29"
    $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
6
        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="<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&gt;" $saType="&lt;storage
account type>",gebenSieeinesan:Standard_LRS,Standard_GRS,Standard_RAGRS
oder Premium_LRS Neues AzureRmStorageAccount -Name $saName -
Ressourcengruppenname $rgName -Typ $saType -Standort $locName
```

Zum Beispiel:

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
```

```
    $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
```

```
1 $nicName="frontendNIC"
```

```
3 $domName="vpxazure"
4
5 $pip = New-AzureRmPublicIpAddress -Name $nicName -
ResourceGroupName $rgName -DomainNameLabel $domName -Location
        $locName -AllocationMethod Dynamic
6
7 $nic = New-AzureRmNetworkInterface -Name $nicName -
ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
Subnets\[0\].Id -PublicIpAddressId $pip.Id
```

c) NIC 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 -AvailabilitySetIc
$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
     $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/
11
        " + $diskName + ".vhd"
12
     $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri
13
        $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="<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
```

```
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.

\$vnetName = "LBVnet" 1 2 3 \$FrontendAddressPrefix="10.0.1.0/24" 4 \$BackendAddressPrefix="10.0.2.0/24" 5 6 7 \$vnetAddressPrefix="10.0.0/16" 8 9 \$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix \$FrontendAddressPrefix 10 11 \$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix \$BackendAddressPrefix 12 13 \$vnet=New-AzureRmVirtualNetwork -Name \$vnetName -ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet

Hinweis:

Wählen Sie den Parameterwert AddressPrefix entsprechend Ihren Anforderungen.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-Endund 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] .ld 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. 1 2

```
$pubName="PublicIp1"
```

```
3 $publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
ResourceGroupName $rgName -Location $locName -
AllocationMethod Static -DomainNameLabel nsvpx
```

Hinweis:

Überprüfen Sie die Verfügbarkeit des Wertes für DomainNameLabel.

1	\$FIPName = "ELBFIP"
2	
3	<pre>\$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig - Name \$FIPName -PublicIpAddress \$publicIP1</pre>
4	
5	\$BEPool = "LB-backend-Pool"
6	
7	<pre>\$beaddresspool1= New- AzureRmLoadBalancerBackendAddressPoolConfig -Name \$BEPool</pre>

6. Erstellen eines Gesundheitstasters

Erstellen Sie einen TCP-Integritätstest mit Port 9000 und Intervall 5 Sekunden.

```
1 $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.

```
1 $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.	
1	<pre>\$inboundNATRule1= New- AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1 -FrontendIpConfiguration \$frontendIP1 -Protocol TCP -FrontendPort 22 -BackendPort 22</pre>
2	
3	<pre>\$inboundNATRule2= New- AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 - FrontendIpConfiguration \$frontendIP1 -Protocol TCP - FrontendPort 10022 -BackendPort 22</pre>

9. Erstellen einer Load Balancer-Entität

Erstellen Sie den Load Balancer und fügen Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Probe-Konfigurationen) zusammen.

```
1 $lbName="ELB"
2
3 $NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -
Name $lbName -Location $locName -InboundNatRule
$inboundNATRule1, $inboundNATRule2 -FrontendIpConfiguration
$frontendIP1 -LoadBalancingRule $lbrule1 -BackendAddressPool
$beAddressPool1 -Probe $healthProbe
```

10. Erstellen einer Netzwerkkarte

Erstellen Sie zwei Netzwerkkarten und verknüpfen Sie jede Netzwerkkarte mit jeder VPX-Instanz

a) NIC1 mit VPX1

```
1
     $nicName="NIC1"
2
3
     $lbName="ELB"
4
5
     $bePoolIndex=0
6
     \times Rule indexes starts from 0.
7
8
     $natRuleIndex=0
9
10
11
     $subnetIndex=0
12
13
     \* Frontend subnet index
14
15
     $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
         $rgName
16
17
     $nic1=New-AzureRmNetworkInterface -Name $nicName -
         ResourceGroupName $rgName -Location $locName -Subnet $vnet.
         Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
```

```
BackendAddressPools\[$bePoolIndex\] -
LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
\]
```

b) NIC2 mit VPX2

Zum Beispiel:

1	<pre>\$nicName="NIC2"</pre>
2	
3	<pre>\$lbName="ELB"</pre>
4	
5	\$bePoolIndex=0
6	
(\$natRuleIndex=1
8	At Second Tabaund NAT (SSU) rule we need to use
9	(* Second Inbound NAT (SSR) rule we need to use
11	`\$subnetIndex=0
12	
13	<pre>* Frontend subnet index</pre>
14	
15	<pre>\$lb=Get-AzureRmLoadBalancer -Name \$lbName -ResourceGroupName \$rgName</pre>
16	
17	<pre>\$nic2=New-AzureRmNetworkInterface -Name \$nicName - ResourceGroupName \$rgName -Location \$locName -Subnet \$vnet. Subnets\[\$subnetIndex\] -LoadBalancerBackendAddressPool \$lb. BackendAddressPools\[\$bePoolIndex\] - LoadBalancerInboundNatRule \$lb.InboundNatRules\[\$natRuleIndex\]</pre>

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

```
$vmName="VPX1"
1
2
3
     $vmSize="Standard\_A3"
4
5
     $pubName="citrix"
6
     $offerName="netscalervpx110-6531"
7
8
9
     $skuName="netscalerbyol"
10
11
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
         ResourceGroupName $rgName
12
```

```
$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
13
        AvailabilitySetId $avset.Id
14
     $cred=Get-Credential -Message "Type Credentials which will be
15
        used to login to VPX instance"
     $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
17
         $vmName -Credential $cred -Verbose
18
19
     $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
20
     $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id
21
22
     $diskName="dynamic"
23
24
25
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
26
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
27
        vhds1/" + $diskName + ".vhd"
28
29
     $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
         $osDiskUri1 -CreateOption fromImage
31
     Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
         $offerName -Name $skuName
33
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm1
```

b) NetScaler VPX-Instanz 2

```
$vmName="VPX2"
1
2
3
     $vmSize="Standard\_A3"
4
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
5
        ResourceGroupName $rgName
6
     $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
9
     $cred=Get-Credential -Message " Type Credentials which will be
        used to login to VPX instance "
10
     $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
11
        $vmName -Credential $cred -Verbose
12
     $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
13
        Offer $offerName -Skus $skuName -Version "latest"
14
```

```
$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
15
16
     $diskName="dynamic"
17
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
21
        vhds2/" + $diskName + ".vhd"
22
23
     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
         $osDiskUri1 -CreateOption fromImage
24
     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
25
         $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $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="\\<resource group name\\&#062;"
$locName="\\&#060;location name, such as West US\\&#062;"
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="<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:

```
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 $vnetAddressPrefix="10.0.0.0/16"
4
5 $FrontendAddressPrefix="10.0.1.0/24"
6
7 $BackendAddressPrefix="10.0.2.0/24"
8
```

9	<pre>\$vnet=New-AzureRmVirtualNetwork -Name \$vnetName - ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet\`</pre>
10	
11	
	frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix \$FrontendAddressPrefix
12	
13	<pre>\$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name</pre>
	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-Endund 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.

```
1 $inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
Protocol TCP -FrontendPort 3441 -BackendPort 3389
2
3 $inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol
TCP -FrontendPort 3442 -BackendPort 3389
```

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.

```
1 $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.

```
1 $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.

```
1 $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.

```
1 $backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
   $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
   10.0.2.7 -Subnet $backendSubnet -
   LoadBalancerBackendAddressPool $nrplb.BackendAddressPools
   \[0\] -LoadBalancerInboundNatRule $nrplb.InboundNatRules
   \[1\].
```

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:

1 2	\$∨mName="VPX1"
3	<pre>\$vmSize="Standard_A3"</pre>
5	\$avSet=Get-AzureRmAvailabilitySet -Name \$avName - ResourceGroupName \$rgName
7	\$vm1=New-AzureRmVMConfig -VMName \$vmName -VMSize \$vmSize - AvailabilitySetId \$avset.Id
9	<pre>\$cred=Get-Credential -Message "Type Credentials which will be used to login to VPX instance"</pre>
10	\$vm1=Set-AzureRmVMOperatingSystem -VM \$vm1 -Linux -ComputerName \$vmName -Credential \$cred -Verbose
12	<pre>\$vm1=Set-AzureRmVMSourceImage -VM \$vm1 -PublisherName \$pubName - Offer \$offerName -Skus \$skuName -Version "latest"</pre>
14 15 16	<pre>\$vm1=Add-AzureRmVMNetworkInterface -VM \$vm1 -Id \$backendnic1.Id</pre>
17 18	\$diskName="dynamic"
19	<pre>\$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName \$rgName -Name \$saName</pre>
20 21	<pre>\$osDiskUri1=\$storageAcc.PrimaryEndpoints.Blob.ToString() + " vhds1/" + \$diskName + ".vhd"</pre>
22 23	\$vm1=Set-AzureRmVMOSDisk -VM \$vm1 -Name \$diskName -VhdUri \$osDiskUri1 -CreateOption fromImage
24 25	Set-AzureRmVMPlan -VM \$vm1 -Publisher \$pubName -Product \$offerName -Name \$skuName
26 27	New-AzureRmVM -ResourceGroupName \$rgName -Location \$locName -VM \$vm1

b) NetScaler VPX-Instanz 2

```
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
     $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
15
16
17
     $diskName="dynamic"
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
20
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName + ".vhd"
     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
25
        $offerName -Name $skuName
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.

Erstellen Sie ein Support-Ticket für die VPX-Instanz in Azure

January 15, 2025

Wenn Sie Probleme mit Ihrer NetScaler VPX-Instanz in Azure haben, können Sie zur Problembehandlung ein Supportticket im NetScaler-Support-Portal.

Um ein Support-Ticket zu erstellen, stellen Sie Folgendes sicher:

- Ihr Netzwerk ist verbunden.
- Sie haben Ihre Azure-Kontonummer, den Support-PIN-Code des abonnementbasierten NetScaler-Angebots, das Sie in Azure bereitgestellt haben, und das serielle Azure-Protokoll zur Hand.
 - Den Support-PIN-Code finden Sie auf der **Seite "Systeme**" in der VPX-GUI.

Dashboard	Configuration	Reporting Documentation Downloads	¢
Q Search Menu		System > System Information	
Favorites	~	System	
AZURE	>	System Information System Sessions 2 System Network	
System	~	System Upgrade Reboot Migration Statistics Call Home NetScaler ADM Service Connect	
Licenses		System Information	
Settings			
Diagnostics		NetScaler ADC IP Address	
High Availability		Netmask 255.255.0	
High Availability	y -	Node Standalone	
NTP Servers		Technical Support PIN	
Reports		Time Zone Coordinated Universal Time	
hepoirto		System Time Fri, 24 Nov 2023 09:58:26 UTC	
Reporting Conf	figs	Last Contig Changed Time Fri, 24 Nov 2023 09:55:45 UTC	
Profiles		Last Config Saved Lime Fri, 24 Nov 2023 09:56:00 UTC	
Destition Admin	sistentian	Hardware Information	

- Sie finden das serielle Protokoll im Azure-Portal (Boot-Diagnose -Bereich Ihrer VM).

Virtual machine	() Pafrach (Sottings (Traublackapt
	Verresh 😓 Settings 🧭 Houbleshoot
Run command	Screenshot Serial log
lonitoring	Updated: Friday, 8 September 2023 at 6:15:06 AM UTC Download serial log
P Insights	ער ער ער ער ער ער ער ער ער אי
Alerts	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
- Alera	-\/-\/-\/-\//-\//-\//-\//-\//-\//-\//-\
Metrics	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Disgnastic settings	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Diagnostic settings	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Logs	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
-	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Connection monitor (classic)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Marth a sha	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
WORKDOOKS	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-
	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
utomation	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Tasks (proviou)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
 Tasks (preview) 	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Export template	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
elp	
- F	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
Resource health	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
	-\/-\/-\//-\//-\//-\//-\//-\//-\//
Boot diagnostics	-\/-\/-\//-\//-\//-\//-\//-\//-\//

Wenn Sie alle Informationen zur Hand haben, wenden Sie sich an den NetScaler-Support. Sie werden aufgefordert, Ihren Namen und Ihre E-Mail-Adresse anzugeben.

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 zuNetScaler 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

January 30, 2025

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	Management-Netzwerk
	Verwaltungsdatenverkehr	
	(NetScaler IP)	
NIC 1	Dient clientseitigem	Kunden-Netzwerk
	Datenverkehr (VIP)	
NIC 2	Kommuniziert mit	Back-End-Server-Netzwerk
	Back-End-Servern (SNIP)	

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**.

Create a VPC network Name Vexmgmt Vexmgmt Vexeription (Optional) management ygc Subnets Subnets Subnets leave a subnet in each region, or click Custom to manually define the subnets. Learn more Subnet creation mode Custom Automatic New subnet Add a description Region Paddress range O O O Casets Private Google access O O Casets Custom Casets Custom Coulding mode Private Google access O Custom Add subnet Vexmic routing mode Custom Cust	• netsca	er-vpx-platform-eng 🔻	
Name vpxmgmt Description (Optional) management ygc Subnets Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more Subnet creation mode Custom Automatic New subnet Name Name Image: Subnet creation mode Custom Automatic New subnet Add a description Region Image: State scandary IP IP address range Ip: 168.30.0/24 Create secondary IP range Private Google access Image: State scandary IP range Image: State scandary	(Cre	ate a VPC network	
vpxmgmt Description (Optional) management ygc Subnets Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the ubunets. Learn more Subnet creation mode Custom Automatic Name @ vpxmgmtsubnet Add a description Region @ asia-east1 IP address range @ 192.168.30.0/24 Create secondary IP range Private Google access @ @ On Off Flow logs On On On Regional Cloud Routers will learn routes only in the region in which they were created Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Name 🕜		
Description (Optional) management ypc Subnets Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more Subnet creation mode Custom Automatic New subnet	vpxmgmt		
management ypc Subnets Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more Subnet creation mode Custom Automatic New subnet New subnet New subnet Name Vyxmgmtsubnet Add a description Region asia-east1 P address range 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Flow logs On Private Google access rivate Google access Private Google	Description	Optional)	
Subnets Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more Custom Automatic New Subnet Automatic New Subnet Name Automatic New Subnet Name	managem	ent ypç	
Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more Subnet creation mode Custom Automatic New Subnet	Subnets		
Subnet creation mode Custom Automatic New subnet Automatic Name	Subnets let y Automatic to subnets. <mark>Lea</mark>	ou create your own private cloud topology within Google Cloud. Click create a subnet in each region, or click Custom to manually define the n more	
New subnet Name Vpxmgmtsubnet Add a description Region asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access Image: I	Subnet crea	ion mode	
New subnet Name Name	Custom	Automatic	
Name	New subne	t 💼	^
vpxmgmtsubnet Add a description Region @ asia-east1 IP address range @ 192.168.30.0/24 Create secondary IP range Private Google access @ Image: Image of the secondary IP range Private Google access @ Image: Image of the secondary IP range Private Google access @ Image: Image: Image of the secondary IP range Private Google access @ Image: Image: Image: Image of the secondary IP range Private Google access @ Image: Image: Image: Image of the secondary IP range Image: Image: Image: Image of the secondary IP range Image: Image	Name 📀		
Add a description Region asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Flow logs On Off Done Cancel // Add subnet // Add subnet // Add subnet // Create secondary iP range // Add subnet // Cancel	vpxmgm	subnet	
Add a description Region © asia-east1 IP address range © 192.168.30.0/24 Create secondary IP range Private Google access @ On Off Flow logs On Off Flow logs On Off Done Cancel Let a second provide a state of the second provide state o	Add a day	inter-	
Region asia-east1 IP address range 192.168.30.0/24 Create secondary IP range Private Google access Image: Image of the im	Add a desc	nption	
asia-east1 IP address range I92.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On Off Flow logs On Off Done Cancel Lance Lance /b>	Region 🕑	-	
IP address range	asia-east	1	•
192.168.30.0/24 Create secondary IP range Private Google access On Off Flow logs On On Off Done Cancel Add subnet Ynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	IP address	range 🕜	
Create secondary IP range Private Google access On Off Flow logs On Off Done Cancel Add subnet Yynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	192.168.	30.0/24	
Private Google access On Off Flow logs On On Off Done Cancel Add subnet Vynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Create sec	ondary IP range	
 On Off Flow logs On Off Done Cancel Done Cancel Add subnet Add subnet Segional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router Orocto Cancel	Private Go	gle access 🕖	
 On Off Flow logs On Off Done Cancel + Add subnet Dynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router 			
Flow logs On On Of Cancel Flow logs	 On Off 		
Flow logs On Off Done Cancel Let a constrain the second seco			
On Off Done Cancel Add subnet	Flow logs		
Done Cancel Add subnet Dynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router Create	 On Off 		
Add subnet	Done	Cancel	
Add subnet Oynamic routing mode Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router Create			
Opnamic routing mode Image: Constant of the second sec		+ Add subnet	
Regional Cloud Routers will learn routes only in the region in which they were created Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Dynamic rou	ting mode 📀	
Global Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	 Regiona 		
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router	Gloud Ro Global	uters will learn routes only in the region in which they were created	
Crancel	Global ro VPN or in	uting lets you dynamically learn routes to and from all regions with a sin terconnect and Cloud Router	ngle
	Croate	Cancel	
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 asiaeast1 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.

😔 netscaler-vp	x-platform-eng 👻									
← Create	a firewall rule									
Firewall rules con incoming traffic f	trol incoming or outgoing traffic to an instance. By default, rom outside your network is blocked. Learn more									
Name 📀										
vpxmgmtingressrule										
Description (Option	nal)									
management tra	ffic ingress rules									
Logs Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more										
Off										
Network										
vpxmgmt	•									
Priority 🕜 Priority can be 0 - 6	5535 Check priority of other firewall rules									
1000										
Ingress Egress Action on match Allow Deny Targets										
All instances in t	he network 👻									
Source filter 🕜										
IP ranges	•									
Source IP ranges	0									
0.0.0/0 😢										
Out and a survey film										
None	er 🕑									
None										
Protocols and port Allow all Specified prot	s 😨									
🗹 tcp :	22, 80, 443									
udp :	all									
Other protocols										
protoco	ols, comma separated, e.g. ah, sctp									
Y Dischla mile										
 Disable rule 										
Create	el									

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.

≡ Google Cloud			
🖄 Marketplace			Q NetScaler VPX X
Marketplace > "NetScaler V	'PX"		
Marketplace home		2 results	
★ Your products★ Your orders		net)scaler.	NetScaler VPX FIPS - Customer Licensed Citrix Systems, Inc. NetScaler VPX FIPS (formerly Citrix ADC) is an enterprise grade application delivery controller that delivers your applications quickly, reliably, and
= Filter Type to filter			securely, with the deployment and pricing flexibility to meet your business' unique needs. Designed to provide operational consistency and a smooth user experience, NetScaler eases your transition to the hybrid cloud. NetScaler VPX FIPS is in NIST process for FIPS 140-2 Level 1
Category	^	netoscaler	NetScaler VPX - Customer Licensed
Security Networking	(1)		NetScaler (formerly Citrix ADC) is an enterprise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to meet your business' unique needs. Designed to provide operational consistency and a smooth user expressions. Reference sees your transition to the bubrid cloud. Why NatScaler offers high performance with fast application.
Туре	^		
Virtual machines	(2)		
Price	^		
BYOL	(2)		

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 NICO.
- 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**.

÷	Create a VPC network
Name	0
vpxm	gmt
Descrip	ption (Optional)
mana	sgement ypp
Subn	ets
Subnet Autom	s let you create your own private cloud topology within Google Cloud. Click alic to create a subnet in each region, or click Custom to manually define the
Subnet	s Learn more
Cust	am Automatic
New s	ubnet 🔋 🧥
Name	0
vpx	mgmtsubnet
Add a	description
Denin	
asia	Least]
a since	
IP ad	fress range 💿
192	168.30.0/24
Creat	e secondary IP range
Priva	te Google access 💿
0	2
Õõ	ff
Flow	lags
ŏ	rr
Dor	Cancel
	h strategy
	T Aug sublict
Dynam	ic routing mode
Glo	su voltero wai reala rottes ony in the region in which they were created
Glo	bal routing lets you dynamically learn routes to and from all regions with a single

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.

NetScaler VPX 14.1

🔹 netscaler-vpx-platform-eng 👻
Create a firewall rule
Firewall rules control incoming or outgoing traffic to an instance. By default,
incoming traffic from outside your network is blocked. Learn more
vpxmgmtingressrule
Description (Optional)
management tramc ingress rules
Logs Turning on frewall logs can generate a large number of logs which can increase costs in Stockfirer, Learn more
• on
Network 💿
vpixmgmt +
Priority Priority Priority can be 0 - 65535 Check priority of other firewall rules
1000
Ingress Action on match Adviou Allow Dony
All instances in the network
An instances in one network
Source filter
ir tursjua
Source IP ranges
0.0.0.0/0 🕲
Second source filter 💿
None *
Protocols and ports Allow all Specified protocols and ports
✓ tcp: 22,80,443
udp: all
Other protocols
protocols, comma separated, e.g. ah, sctp
➢ Disable rule
Create Cancel

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**.

۲	Compute Engine	Images	[+] CREATE IMAGE	C REFRESH	-	CREATE INSTANCE		⊖ DEPRECAT
	VM instances							
6 14	Instance groups	= Filter images					0	Columns 👻
	Instance templates							
日	Sole tenant nodes	<< Previous 1	2 Next >>					
٥	Disks	Name		Siz	ze	Created by		
٥	Snapshots	✓ ✓ nsvpx-12-1-5	0-9	20	GB			
	Images							

4. Wählen Sie einen Instanztyp mit zwei vCPUs aus (Mindestanforderung für ADC).

÷	Create an instance							
To cr	eate a VIM instance, select one of the options:		Name © Name is permanent					
A	New VM Instance Create a single VM instance from scratch	Labels © (Optional) shuddown : no						
ŧ	New VM instance from template Create a single VM instance from an existing template		+ Add label Region () Region is permanent Us-east1 (South Carolina) Us-east1-b					
н Ц	New VM instance from machine image Create a single VM Instance from an existing machine image Marketplace Deploy a ready-to-go solution onto a VM instance	E	Machine configuration Machine family General-purpose Compute-optimized Machine types for common workloads, optimized for cost and flexibility Series N1 • Powered by Intel Skylake CPU plotform or one of its predecessors Machine type Intestandard-2 (2 xCPU, 7.5 GB memory) vCPU Memory GPUs 2 7.5 GB * Confidential VM service Enable the Confidential Computing service on this VM instance. Container Optoy a container image to this VM instance. Learn more					

- 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 NICO-Schnittstelle.
- 3. Geben Sie im Feld **Alias-IP-Bereich** die Alias-IP-Adressen ein.

 VM instance details 	/ EDIT	也 RESET	CREATE MACHINE IMAGE	E) CREAT
Vetwork interfaces 🛞				
Network interface		^		
You must stop the VM instance to edit ne Network	twork, subnetwork or internal	IP address		
automationmgmtnetwork		*		
Subnetwork 💮				
mgmtsubnet (192.168.1.0/24)		*		
Internal IP 192.168.1.50 Internal IP type				
Ephemeral		-		
Alias IP ranges Subnet range	Alias IP range 💿			
Primary (192.168.1.0/24) *	192.168.1.3/32	×		
Primary (192.168.1.0/24) *	192.168.1.7/32	×		
+ Add II	P range			
 Hide alias IP ranges External IP (0) 				
Ephemeral		*		
Network Service Tier Premium (Current project-level Standard (us-east1)	tier, change) 💿			
off				
5.12 BIG DTD B			1	

- 4. Klicken Sie auf **Fertig**und dann auf **Speichern**.
- 5. Überprüfen Sie die Alias-IP-Adressen auf der Detailseite der VM-Instanz.

()	VM instance details	10		CREATE MACHINE IMAG	RE 🐴 CREATE SIMILAR	E STOP	II SUSPEND	B DELET
[]] Eral	ble-connecting to serial parts 6							
Logs David Li Serial pr C More	ogging art 1 (consolie) e							
Instance 254353	NJ 444822010637222							
Mashine mi-stand	fige dat62 (2 vOPUs, 7.5 68 memory	ð						
Reservat	ian fically choose							
CPU juli Intel His	fam. Auril							
Display of Turn on 1	device a display device if you want to use : a conducting device	ronen capitring e	nd recording tools.					
Zone Lo sepi1	1.6							
Lubels shuttle	tem no							
Creation Feb 22,	time 2021, 6:19:01 PM							
Network	Interfaces Network	Submetwork	Primary internal IP	Alias IP ranges	External IP	Network Tiler 💮	IP forwarding	Network details
nic3	automationingentrietwork	ingritazioni	192.168.1.50	192.148.1.3/32, 192.168.1.7/32	104.196.190.91 (epheneral)	Premium	Off	View details
Public D	NS PTR Record							

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 > IPv4sund klicken Sie auf Hinzufügen.

CİTIX.) from	m Market	place							HA Status Piot configured	Partition 👃 default	naraet ~
Dashboard	Configurat	ion Re	porting D	scumentation	Downloads						¢
Q, Search in Menu		System >	Network > IPs ->	IPV45							
Geogle Cloud Platform	>	IDe									0.0
Bystem	~	IF 8									0.14
Licenses		12V4a 🥌	PV8x 1								
Sottings		Ann	Edit Delete	Statistics No.	last Astrony						
Diagnostics		<u> </u>									
High Availability	>	Q Cickie	re to search or you to	en ender Keyl: Value Iorris	t						0
NTP Servers			IP AEDRESS	STATE D	TIPE	: MODE	A102	1 KMP	URBLAL SERVER	TRAFFI	C DOMAIN I
Reports			192.168.1.7	ENABLED	Satnel P	Active	ENABLED	ENABLED	-10 A-		0
Profiles			192.198.1.3	ENABLED	VP to all IP	Action	ENABLED	ENABLED	ENABLED		D
Partition Administrati	con)		192,168,150	ENABLED	NetSceler P	Active	ENABLED	ENABLED	-10 A-		0
User Administration	>	Total 3							25 Per Page	✓ Page 1 4	n - E
Authentication	>										
Authing	2										

- 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.

Dashboard Configuration Reporting Documentation Downloads Load Balancing Virtual Server Basic Settings Create a virtual server by specifying a name, an IP address, a part, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address. IP address. If the application is accessible only from the local area network (LAK) or wide area network (WAN), the VIP is usually a private ICAKNI non-mutable) IP address. You can configure multiple virtual servers to receive client requests, thereby incre-0 vser1 Protocol/ HTTP IP Address Type* IP Adds 2 Addisord 192.168.1.3 0 0 80 Cancel

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:

Hinweis:

&lt; instance-name> -adcinternal ist der Name der Zielinstanz, die gelöscht werden muss.

NetScaler VPX-Lizenzierung

Für eine NetScaler VPX-Instanz auf GCP ist eine gültige Lizenz erforderlich. Die Lizenzierungsoption für NetScaler VPX-Instanzen, die auf GCP ausgeführt werden, lautet wie folgt:

Bringen Sie Ihre eigene Lizenz mit (BYOL): Um die BYOL-Option zu verwenden, gehen Sie folgendermaßen vor:

- Verwenden Sie das Lizenzierungsportal auf der NetScaler-Website, um eine gültige Lizenz zu generieren.
- Laden Sie die generierte Lizenz auf die Instanz hoch.
- NetScaler VPX Check-in- und Check-out-Lizenz: Mit diesem Lizenzmodell können Sie eine Lizenz aus einem Pool verfügbarer Lizenzen auschecken und wieder einchecken, wenn sie nicht mehr benötigt wird. Weitere Informationen und detaillierte Anweisungen finden Sie unter NetScaler VPX Check-in- und Check-out-Lizenz.

Hinweis:

Die abonnementbasierte Lizenzierung wird für NetScaler VPX-Instanzen auf GCP nicht mehr unterstützt.

Unterstützte NetScaler VPX-Angebote auf GCP

In der folgenden Tabelle sind die unterstützten NetScaler VPX-Angebote auf GCP aufgeführt.

Unterstützte VPX-Angebote

NetScaler VPX – Kundenlizenz

NetScaler VPX FIPS – Kundenlizenz

Unterstützte GCP-Maschinentypfamilien

Maschinentypfamilie	Mindestmaschinentyp
Allzweckmaschinen	e2-mittel, e2-Standard-2, e2-Highmem-2,
	n1-Standard-2, n1-Highmem-2, n2-Standard-2,
	n2-Highmem-2, n2d-Standard-2,
	n2d-Highmem-2
Rechenoptimierte Maschinen	c2-Standard-4, c2d-Standard-2, c2d-Highmem-2

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 <u>NetScaler GDM Templates</u>.

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 useast1-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.

```
Identity and API access @
Service account @
Compute Engine default service ac
Access scopes @
Allow default access
Allow full access to all Cloud AP
Set access for each API
```

Firewall 🙆

- 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:

1	REQUIRED_INSTANCE_IAM_PERMS = [
2	
3	"compute.addresses.use",
4	"compute.forwardingRules.list",
5	"compute.forwardingRules.setTarget",
6	"compute.instances.setMetadata"
7	"compute.instances.addAccessConfig",
8	"compute.instances.deleteAccessConfig",
9	"compute.instances.get",
10	"Compute.instances.list",
11	"compute.networks.useExternalIp",
12	"compute.subnetworks.useExternalIp",
13	"compute.targetInstances.list",
14	"compute.targetInstances.use",
15	"compute.targetInstances.create",
16	"compute.zones.list",
17	"compute.zoneOperations.get",
18]

• 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:

1 "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 > Ex-terne IP**und klicken Sie auf **IP-Adresse erstellen**.

Network interface	^
Network	
Subnetwork clientvpc-ss-subnet	
Internal IP	
Internal IP type	
Ephemeral	•
℅ Show alias IP ranges	
External IP 💿	
None	
Ephemeral	
vpxpublic (35.229.255.208)	
Premium tier	-
Create IP address	
And the second s	

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.

System / High Availability / Nodes									
Nodes 🝳	Nodes 2								
Add Edit	Delete Statistics	Select Action 🗸							
ID ¢	IP ADDRESS 🔅 HOST NAME 🗘	MASTER STATE	NODE STATE	INC \bigcirc	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REASON			
0	192.168.1.3	Primary	• UP	ENABLED	ENABLED	-NA-			
1	192.168.1.66	Secondary	• UP	ENABLED	SUCCESS	-NA-			
Total 2					25 Per	Page 🗸 Page 1 of 1 < 🕨			

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**.

IPs								
IPV4s 4	IPV6s 1							
Add Edit Delete Statistics Select Action \(\neq \)								
Q Click here to search or you can enter Key : Value format								
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER C TRAFFIC DOMAIN	
Secondary VIP	192.168.2.54	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0
Primary SNIP	192.168.3.7	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
Primary VIP	192.168.2.37	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0
	192.168.1.3	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
Total 4	*						25 Per Page V Page 1 of 1	\rightarrow

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**.

IPs								
IPV4s 3	IPV6s 1							
Add E	dit Delete	Statistics	Select Action \checkmark					
Q Click here to	search or you can enter	Key : Value format						(i)
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP	CMP.	VIRTUAL SERVER C TRAFFIC DOMAIN	
Secondary SNIP	192.168.3.76	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
Secondary VIP	192.168.2.54	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED	0
	192.168.1.66	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
Total 3							25 Per Page ∨ Page 1 of 1 <	

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.

NetScaler VPX 14.1

Citrix ADC V	PX Express (Fre	emium)						HA Status Primary	Partition , default	" ns	root ~
Dashboard	Configuration	Reporting	Documentation	Downloads							۰
	Set	IPV4s	D								С×
		Add	Edit Delete	Statistics	Select Action >>						
		Q Click here	to search or you can enter Ke	y : Value format							0
			IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE	MODE 0	ARP 0	ICMP	VIRTUA
		Ada	192.168.1.3	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
			192.168.2.37	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLE
			192.168.3.7	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
			192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLE
		Total 4						25 Per Pa	ge 🗸 Page	1 of 1	\rightarrow
		Inster	Close								
										(9

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.

Dashboard	Configuration	Reporting	Documentation	Downloads							۰	
G Create IP	Set	IPV4s	0								C	×
Name*		Add	Edit Delete	Statistics	Select Action							
ipset1		Q Click her	e to search or you can enter K	ey : Value format								()
Traffic Domain			IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP		VIRTUA
		Adt	192.168.1.66	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED		-N/A-
IDual IDual			192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED		ENABL
11794 11790			192.168.3.76	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED		-N/A-
Insert Del		Total 3						25 Per Pag	e 🗸 Page	1 of 1	4	►
IP ADDRES		Insert	Close									
No items		_										
Create												

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 5konfigurierten 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.

1 add ha node 1 <sec_ip> -inc ENABLED

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

1 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.

```
1 add ns ip <primary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_vip> <subnet> -type VIP
4
5 add ns ip <primary_snip> <subnet> -type SNIP
```

primary_vip 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.

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 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:

```
1 add ipset <ipsetname>
2 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:

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:

1 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.



Firewall

- 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:

1	<pre>REQUIRED_INSTANCE_IAM_PERMS = [</pre>
2	"compute.forwardingRules.list",
3	"compute.forwardingRules.setTarget",
4	"compute.instances.setMetadata",
5	"compute.instances.get",

- "compute.instances.list", 6 7 "compute.instances.updateNetworkInterface", "compute.targetInstances.list", 8 9 "compute.targetInstances.use", "compute.targetInstances.create", 10 11 "compute.zones.list", "compute.zoneOperations.get", 12 13]
- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie Private Google Access im VPC-

	Add a subnet	
	Name 😡 Name is permanent	
	management-subnet	
	Add a description	
	VPC Network	
	automationmgmtnetwork	
	Region 🛞	
	us-east1	*
	Reserve for Internal HTTP(S) Load Balancing	
	On Off	
	IP address range 🕡	
	192.168.2.0/24	
	Create secondary IP range	
	Private Google access 🛞	
	On Off	
	Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a lar number of long, which can increase costs in Stackdiver Learn more	ge
	• on	
	CANCEL	ADD
upnetz 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:

- 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.

You must stop the VM instance to	edit network, subnetwork or internal IP addr	ess
Network 🕜		
automationmgmtnetwork		Ŧ
Subnetwork 🕜		
mgmtsubnet (192.168.1.0/24,	us-east1)	-
Internal IP 192.168.1.71		
Internal IP type		
Ephemeral		-
Subnet ranges	Alias IP range	
Primary (192.168.1.0/24)	· 192.168.1.5/32	Primary Client Alias
Primary (192.168.1.0/24)	▼ 192.168.1.6/32	Primary Server Alia
+	Add IP range	
 Uide elies ID renges 		
 Fide allas in faliges 		
External IP 💿		
		*
Ephemeral		
Ephemeral Network Service Tier		
Ephemeral Network Service Tier Premium (Current projee Standard (us-east1)	ct-level tier, change) 📀	
Ephemeral Network Service Tier Premium (Current projec Standard (us-east1)	ct-level tier, change) 💿	
Ephemeral Network Service Tier • Premium (Current projection of the second of the se	ct-level tier, change) 💿	
Ephemeral Network Service Tier Premium (Current project Standard (us-east1) Pforwarding Dff Public DNS PTR Record Enable	ct-level tier, change) 📀	

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.

Network interface		^
You must stop the VM instance to edit n Network	etwork, subnetwork or internal IP address	
automationmgmtnetwork		-
Subnetwork 🛞		
mgmtsubnet (192.168.1.0/24, us-e	ast1)	-
Internal IP 192.168.1.76		
Ephemeral		*
Alias IP ranges	Secondary Subnet IP(SNIP)	
Subnet range	Alias IP range 🛞	
Primary (192.168.1.0/24) -	192.168.1.7/32	х
+ Add	IP range	•
Hide alias IP ranges External IP @		
Ephemeral		-
Network Service Tier Premium (Current project-levent Standard (us-east1) Prorwarding	el tier, change) 🐵	
Dublic DNP DTD Decord		
Enable		
PTR domain name		
Done Cancel		

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.

k

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.

System >	High Availa	bility > Nodes						
Node	s 2							
Add	Edit	Delete Statis	Selec	ct Action \checkmark				
	ID ¢	IP ADDRESS 🔅	HOST NAME 🔅	MASTER STATE	NODE STATE	INC ‡	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REA
	0	192.168.1.71		Primary	• UP	ENABLED	ENABLED	-NA-
	1	192.168.1.76		Secondary	• UP	ENABLED	SUCCESS	-NA-
Total 2							25 Per Page	✓ Page 1 of 1 < ▶

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.

System > Network > IPs > IPV4s									
IPs								$\langle z \rangle$	F
IPV4s 3	IPV6s 1								
Add Edit Delete Statistics									
Q Click here	to search or you can	n enter Key : Value format							(j)
	IP ADDRESS		TYPE		ARP 0	ICMP	VIRTUAL SERVER	TRAFFIC DOMAIN	
Primary SNIP	192.168.1.6	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-		0
Primary VIP	192.168.1.5	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED		0
	192.168.1.71	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-		0
Total 3							25 Per Page 🗸 Pa	age 1 of 1 🔍	
									k

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**.

System > Network > IPs > IPV4s								
IPs								
IPV4s 3 IPV6s 1								
Add Edit Delete Statistics Select Action \u2274								
\boldsymbol{Q} Click here to search or you can enter Key : Value format			0					
IP ADDRESS 🗘 STATE 🌣 TYPE			SERVER					
Secondary SNIP 192.168.1.7 ●ENABLED Subnet	IP Active ENABLED	ENABLED -N/A-	0					
□ 192.168.1.76 ● ENABLED NetScal	er IP Active ENABLED	ENABLED -N/A-	0					
Primary VIP 192.168.1.5 ●ENABLED Virtual I	P Passive ENABLED	ENABLED ENABLE	D 0					
Total 3		25 Per	Page V Page 1 of 1					

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**.

¬ Load Balancing Virtual Server

Basic Settings	
Create a virtual server by specifyin IP address. If the application is acc You can configure multiple virtual s Name*	g a name, an IP address, a port, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address is a public essible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. ervers to receive client requests, thereby increasing the availability of resources to process client requests.
lb-vserver1	0
Protocol*	
HTTP	~
IP Address Type*	
IP Address	\checkmark
IP Address*	
192.168.1.5	0
Port*	
80	
More	
OK Cancel)

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 4konfigurierten 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.

1 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:

1 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.

1 add ns ip <primary_server_alias_ip> <subnet> -type SNIP

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

1 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.

1 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:

1 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:

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.

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.

```
Identity and API access 
Service account 
Compute Engine default service acc
Access scopes 
Allow default access
Allow full access to all Cloud AP
Set access for each API
```

Firewall

- 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:

1	REQUIRED_INSTANCE_IAM_PERMS = [
2	"compute.forwardingRules.list",
3	"compute.forwardingRules.setTarget",
4	"compute.instances.setMetadata",
5	"compute.instances.get",
6	"compute.instances.list",
7	"compute.instances.updateNetworkInterface",
8	"compute.targetInstances.list",
9	"compute.targetInstances.use",
10	"compute.targetInstances.create",
11	"compute.zones.list",
12	"compute.zoneOperations.get",
13]

• 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:

```
1 REQUIRED_INSTANCE_IAM_PERMS = [
2 "compute.addresses.use"
3 "compute.instances.addAccessConfig",
4 "compute.instances.deleteAccessConfig",
5 "compute.networks.useExternalIp",
6 "compute.subnetworks.useExternalIp",
7 ]
```

• Wenn Ihre VMs keinen Internetzugang haben, müssen Sie Private Google Access im Verwal-
Γ	
	Add a subnet
	Name 💿
	management-subnet
	Add a description
	VPC Network
	automationmgmtnetwork
	Region 🛞
	us-east1 -
	Reserve for Internal HTTP(S) Load Balancing 0
	On Off
	IP address range 🛞
	192.168.2.0/24
	Create secondary IP range
	Private Google access 🛞
	On Off
	Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more
	On Off
tungssubnetz aktivieren.	CANCEL ADD

• 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.

NetScaler VPX 14.1

Anisonationagenteetwork Subnetwork Network interface	VM instance deta	ails	/ EDIT	心 RESET	🗒 CREATE SIM			
Jan 16, 2020, 4300-22 PM Network interface nic0: automationmgminetwork mgmtsubnet Network interface <	creation time							
vetwork interfaces nic0: automationmgmtnetwork mgmtsubnet Network interface Network sudomationalisetnetwork Subortvork, calentsubnet Internal IP 122.168.2.65 External IP External IP Subort range Primary (192.168.2.0/24) External IP Cancel None Inic2: automationservenetwork serversubnet vetwork interface vetwork interface Network interface Alias IP ranges Subort range Primary (192.168.2.0/24) External IP None Inc2: automationservenetwork serversubnet vetwork interface automationservenetwork serversubnet Vetwork interface Internal IP d< th=""><th>an 16, 2020, 4:00:22 PM</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td<>	an 16, 2020, 4:00:22 PM							
nic2: automationngmtnetwork mgmtsubnet Network Network automationalisentnetwork Subnet range Ephemeral Trimary (1921.16.8.2.0/24) Example: 10.0.1.0/24 or /32 Primary (1921.68.2.0/24) Example: 10.0.1.0/24 or /32 Alda IP ranges Subnet range Alda IP ranges Come Alda IP ranges Internal IP Pirimary (1921.16.8.2.0/24) Example: 10.0.1.0/24 or /32 Alda IP ranges Come < th=""><th>letwork interfaces 💿</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>	letwork interfaces 💿							
Network interface	nic0: automationmgmtnetwork	k mgmtsubnet		1				
Network automationclientnetwork Subnetwork cientrationet Totals IP ranges Subnet range Primary (192.168.2.0/24) + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Enternal IP 0 ne Cancel None nic2: automationspervemetwork serversubnet Verticationspervemetwork subnetwork of automationspervemetwork subnetwork none vatomationspervemetwork subnetwork none vatomationspervemetwork subnetwork note vatomationspervemetwork subnetwork none vatomationspervemetwork subnetwork none vatomationspervemetwork subnetwork none vatomationspervemetwork none none	Network interface			^				
Network clentsubnet Internal P 192:168.2.65 Internal P type Ephemeral Alias IP ranges Subnet range Pirimary (192:168.2.0/24) ↓ Example: 10.0.1.0/24 or /32 ↓ Add IP range Subnet range Pirimary (192:168.2.0/24) ↓ Example: 10.0.1.0/24 or /32 ↓ Add IP range Subnet range ternal IP None	Natural							
Subnetwork clientsubnet Internal IP 192.168.2.65 Internal IP type Ephenneral Alias IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range Example: 10.0.1.0/24 or /32 + Add IP range 	automationclientnetwork							
ciertsubnet Internal IP 192.168.2.65 Internal IP type Ephemeral Alias IP ranges Subnet range Primary (192.168.2.0/24) Lista IP range Subnet range Primary (192.168.2.0/24) Lista IP ranges Subnet range Primary (192.168.1.62) None Nationationargentnetwork None None None None None Vew details	Subnetwork							
Internal IP 192.168.2.65 Internal IP type Ephemeral Alias IP range Example: 10.0.1.0/24 or /32 Alias IP	clientsubnet							
192.168.2.65 internal IP type Ephemeral Alias IP range Kample: 10.0.1.0/24 or /32 Alias IP range Example: 10.0.1.0/24 or /32 Add IP range Alias IP range Alias IP range Add IP rang	Internal IP	_						
internal IP type Ephemerai Alias IP ranges Subnet range Primary (192.168.2.0/24) Example: 10.0.1.0/24 or /32 + Add IP range Reternal IP None Inic2: automationservernetwork serversubnet v work imerfaces and mationangmitnetwork Inic2: automationservernetwork 12: automationservernetwork 12: automationservernetwork 12: automationservernetwork 12: automationservernetwork 12: automationservernetwork 12: 10: 10: 10: 10: 10: 10: 10: 10: 10: 10	192.168.2.65							
Ephemeral Alias IP ranges Subnet range Primary (192.168.2.0/24) Example: 10.0.1.0/24 or /32 + Add IP range Remain IP @ None Done Cancel inc2: automationservernetwork serversubnet verkinterfaces and material in Parity internal IP Alias IP ranges External IP @ None verkinterfaces and material interfaces and material interfaces and material interfaces and cha-instance1-ip1 (35.185.108.124) Premium Off View details ia automationisintnetwork ci automationisintnetwork serversubnet 12 automationiservernetwork	Internal IP type							
Alias IP ranges Subnet range Primary (192.168.2.0/24) Add IP range Add IP range Hide alias IP ranges External IP Tone Inc2: automationservemetwork serversubnet work interfaces are Network Serversubnet 192.168.1.62 - add-ha-instance1-ip1 (35.185.108.124) Premium Off View details into automationingmtnetwork dilentsubnet 192.168.2.8 192.168.2.7/32 None None View details View details	Ephemeral			•				
Alias IP ranges Subnet range Primary (192.168.2.0/24) Example: 10.0.1.0/24 or /32 + Add IP range Alias IP range Hide alias IP ranges External IP								
Subnet renge Primary (192.168.2.0/24) Example: 10.0.1.0/24 or /32 + Add IP range + Add IP range * Hide alias IP ranges External IP IP None inc2: automationservernetwork serversubnet * Network Titer © None and Network Subnetwork Primary internal IP Alias IP ranges None ************************************	Alias IP ranges	Alian ID						
Immediately (view countering))))))))))))))))))))))))))))))))))))	Primary (192 168 2 0/24)	Framo	le: 10.0.1.0/24 or /5	2 X				
→ Add IP range > Hide alias IP ranges External IP None ToDone Cancel	Finnary (152.100.2.0/24)	Compl	C. 10.0.1.0/24 01/0	^				
A Hide alias IP ranges External IP None Tone Cancel	+	 Add IP range 						
External IP None Done Cancel nic2: automationservernetwork serversubnet None View details Niew None Niew None View details Niew None View details	A Hide alias IP ranges							
None Image: State and State an	External IP							
Torregular Done Cancel Inic2: automationservemetwork serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet Image: Subnetwork Serversubnet IP Alias IP ranges External IP Network Tier @ IP forwarding Network details ic0 automationingmtinetwork mgmtsubnet 192.168.1.62 - adc-ha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationclientnetwork clientsubnet 192.168.2.7/32 None View details ic2 automationservernetwork serversubnet 192.168.3.8 - None View details	None			•				
Done Cancel nic2: automationservernetwork serversubnet Image: Subnetwork s								
nic2: automationservernetwork serversubnet twork interfaces ame Network Subnetwork Primary internal IP Allas IP ranges External IP Network Tier IP IP forwarding Network details ic0 automationsmgmtnetwork mgmtsubnet 192.168.1.62 – adocha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationclientnetwork clientsubnet 192.168.2.8 192.168.2.732 None View details ic2 automationservernetwork serversubnet 192.168.3.8 – None View details	Done Cancel							
nic2: automationservernetwork serversubnet mork interfaces ame Network Subnetwork Primary internal IP Alias IP ranges External IP Network Tir © IP forwarding Network details ic0 automationngmtnetwork mgmtsubnet 192.168.1.62 – adecha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationclientnetwork clientsubnet 192.168.2.8 192.168.2.732 None View details ic2 automationservernetwork serversubnet 192.168.3.8 – None View details								
nic2: automationservernetwork serversubnet work interfaces iame Network Subnetwork Primary internal IP Alias IP ranges External IP Network Tire IP forwarding Network details ic0 automationsmyntnetwork mgmtsubnet 192.168.1.62 - adocha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationclientnetwork clientsubnet 192.168.2.8 192.168.2.732 None View details ic2 automationservernetwork serversubnet 192.168.3.8 - None View details				. 1				
twork interfaces Subnetwork Primary internal IP Alias IP ranges External IP Network Tire () IP forwarding Network details ic0 automationingmtnetwork mgmtsubnet 192.168.1.62 - adc-ha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationinclientnetwork clientsubnet 192.168.2.732 None View details ic2 automationsevernetwork seversubnet 192.168.3.8 - None View details	nic2: automationservernetwor	k serversubnet		/				
twork interfaces Subnetwork Primary internal IP Alias IP ranges External IP Network Tie @ IP forwarding Network details ic0 automationingmtnetwork mgmtsubnet 192.168.1.62 - adcha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationiclientnetwork clientsubnet 192.168.2.83 192.168.2.732 None View details ic2 automationservernetwork serversubnet 192.168.3.8 - None View details								
icO automationmgmtnetwork mgmtsubnet 192.168.1.62 – adc-ha-instance1-ip1 (35.185.108.124) Premium Off View details ic1 automationclientnetwork clientsubnet 192.168.2.8 192.168.2.732 None View details ic2 automationservemetwork serversubnet 192.168.3.8 – None View details	work interfaces ame Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
ic1 automationclientnetwork clientsubnet 192.168.2.8 192.168.2.7/32 None View details ic2 automationservemetwork serversubnet 192.168.3.8 - None View details	c0 automationmgmtnetwork	mgmtsubnet	192.168.1.62	-	adc-hainstance1-ip1 (35.185.108.124)	Premium	Off	View details
ic2 automationservernetwork serversubnet 192.168.3.8 - None View details	c1 automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
	c2 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.

System >	High Availa	ability > Nodes												
Node	Nodes 🞱													
Add Edit Delete Statistics Select Action ~														
	ID 0	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC 0	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE RE						
	0	192.168.1.62		Primary	• UP	ENABLED	ENABLED	-NA-						
	1	192.168.1.6		Secondary	• UP	ENABLED	SUCCESS	-NA-						

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 IPSetaus 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**.

System > Network > IPs > IPV4s														
Ps											ζ_{a}	F		
IPV4s 3	IPV6s 1													
Add Edit Delete Statistics Select Action														
Q Click here to	search or you ca	n ente	er Key : Value f	ormat										í
	IP ADDRESS		STATE		TYPE		MODE		ARP		ICMP	VIRTUAL SERVER 0 TRA	AFFIC DOMAIN	
Primary VIP	192.168.2.7		ENABLED		Virtual IP		Active		ENABLED		ENABLED	ENABLED		0
	192.168.1.62		ENABLED		NetScaler IP		Active		ENABLED		ENABLED	-N/A-		0
Primary SNIP	192.168.3.8		ENABLED		Subnet IP		Active		ENABLED		ENABLED	-N/A-		0
Total 3												25 Per Page 🗸 Page	1 of 1 🔍	•

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**.

System > Network > IPS > IPV4s											
IPs								"			
IPV4s 3	IPV6s 1										
Add Edit Delete Statistics Select Action											
Q Click here to	search or you can en	ter Key : Value format						Ô			
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER	N ÷			
	192.168.1.6	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0			
Seconary SNIP	192.168.3.7	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0			
Primary VIP	192.168.2.7	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED	0			
Total 3							25 Per Page ∨ Page 1 of 1 <	•			

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**.
 - G Load Balancing Virtual Server

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.	Basic Settings		
Name* Ib-vserver1 Protocol* HTTP P Address Type* IP Address IP Address* 192 . 168 . 2 . 5 Ort* 80	Create a virtual server by specifying a address. If the application is accessible You can configure multiple virtual serv	name, a e only fr vers to r	n IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP om the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. eceive client requests, thereby increasing the availability of resources to process client requests.
Ib-vserver1 ① Protocol*	Name*		
Protocol* HTTP PAddressType* P Address P Address* 192 . 168 . 2 . 5 Port* 80 More Cancel	lb-vserver1		0
HTTP PAdressType* PAdress* 192 . 168 . 2 . 5 Port* 80 More Kore	Protocol*		
IP Address Type* IP Address IP Address* 192 . 168 . 2 . 5 Ort* 80 > More	HTTP	~	
IP Address IP Address* 192 . 168 . 2 . 5 Ort* 80 ▶ More	IP Address Type*		
IP Address*	IP Address	\sim	
192 . 168 . 2 . 5 ① Port* 80 ▶ More ▲	IP Address*		
Port* 80 More OK Cancel	192 . 168 . 2 . 5		0
80 Verified Action Cancel	Port*		
More Cancel	80		
OK Cancel	▶ More		
	OK Cancel		*

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 4konfigurierten 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.

1 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:

1 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.

1 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:

1 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:

1

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:

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:

1 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:

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.

NetScaler VPX-Instanz auf Google Cloud VMware Engine bereitstellen

October 17, 2024

NetScaler VPX 14.1

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 Pointto-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.

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

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

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.

Google	Cloud VMware Engin	e			0	B)	\$\$ I	c? 🙁
Home Resources	Welcome to Go	ogle Cloud VMware E	ngine. Create your fir New Priv	st Private Cloud, or t	ry one of the commo	on task:	s belov	w.
Activity Account				2				
			Comm	on Tasks				
	Launch vSphere client	Create a Private Cloud	Add nodes to a Private Cloud	کی Connect via VPN	Allocate Public IP		Manage	e Users

- 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.

	 Create Private Cloud ③ 			
3	Private Cloud name *			
1e	Name your Private Cloud			
} rces	Location *			
5	asia-northeast1 > v-zone-a > VE Placement Group 2	•		
ork	Node type *			
5	ve1-standard-72			
ty	2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM 19.2 TB Raw, 3.2 TB Cache (All-Flash)			
nt	Multi Node Single Node			
	Nada asunt *			
	3			
	(3 to 8)			
	O Customize Cores			
	vSphere/vSAN subnets CIDR range *			
	CIDR block prefix		22	•
	HCX Deployment Network CIDR range			

3. Klicken Sie auf Überprüfen und erstellen.

4. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.

Google	e Cloud VMware Engine
	← Create Private Cloud ⑦
Home	Good news! Your Priva
â	Compute Node Type Edit
Resources	ve1-standard-72
Network	Model: PCSN-ULT-1ND CPU: 2x2.6 GHz, 36 Cores (72 HT) RAM: 788 GB Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
伯比 Activity	Private Cloud Size Edit
(Q)	1 Node
Account	Total CPU: 36 Cores Total RAM: 768 GB Total Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
	Location Edit
	asia-northeast1 > v-zone-a > VE Placement Group 2
	Advanced Options Edit
	Cores per node: 36
	HCX Deployment Network CIDR range
	10.231.8.0/26
	Create Previous Cancel

- 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.

Googl	e Cloud VMware Engine				0 4	\$	d ⁰	8
	Resources							
6 Home	Private Clouds (1)						New Priv	ate Cloud
	u Download as CSV				Column setting	41	Selected	filters (0)
Resources	Name	Clusters	\$ Total Nodes	\$ Location		÷	State	
ل Network	vps-gene-demo	1	1	asia-northeast1 > v-zone-a > VE Placement Group	2		• Prov	isioning

- 7. 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-Anmeldeinformationenauf Anzeigen.

Googl	Google Cloud VMware Engine												
	Resources												
Home	🔶 gcp-vmwa	re-demo	lemo										
Resources	SUMMARY	CLUSTERS	SUBNETS	ACTIVITY	VSPHERE MANAGEN								
Network Activity Account	Ba	asic Info	N 8 (1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Name gcp-vmware-demo Clusters L VSphere/vSAN subi L0.231.0.0/22 VCenter login info View Reset passwor	nets CIDR range rd								

2. Notieren Sie sich die vCenter-Anmeldeinformationen.

Google (Google Cloud VMware Engine									
	← vCenter login									
Home	User name									
Resources	CloudOwner@gve.local	Сору								
्रि Network	Password									
Activity	****	Сору								

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.

Googl	e Cloud VMware Engine				0 4	¢ 🖇	۵
	Resources						
Home	← gcp-vmware-demo				C LAUNCH VSPHERE CLIEN	T 💮 ADD NO	DDES
6	SUMMARY CLUSTERS SUBNETS	ACTIVITY	VSPHERE MANAGEMENT NETWORK	ADVANCED VCENTER SETTINGS DNS CONFIGURATION			
Resources	🗄 Download as CSV				1]]. Selected filters ((0)
Network	Type	÷	Version	‡ FQDN	\$ IP Address		\$
æ	vCenter Server Appliance		7.0.2.19272235	vcsa-126870/3712/c5.asia-northeast1.gve.goog	10.231.0.6		
Activity	NSX Manager		-	max-127044/3712(c5.asia-northeast1.gvs.goog	10.231.0.11		
0	HCX		-	hox-127045.f3712/c5.asia-northeast1.gve.goog	10.231.0.13		
Account	ESIG	*	7.0.2.18836573	essi-126865.f3712fc5.asia-northeast1.gve.goog	10.231.0.15		
	DNS Server 2		-	ns2-126869.f3712fc5.asia-northeast1.gve.goog	10.231.0.9		
	DNS Server 1		-	ns1-126868.f3712fc5.asia-northeast1.gve.goog	10.231.0.8		

4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens vCenter-Anmeldeinformationen bei VMware vSphere an.

VMwa	are [®] vSp	here	
ovemple@d	main local		
Password	main.iocal		
Use Wind	ows session authe	entication	
	LOGIN	N	

5. Im vSphere Client können Sie die ESXi-Hosts überprüfen, die Sie im GCVE Portal erstellt haben.

vm	vSphere Client															·
(])	Ø E 🤅	2		🔊 vcsa-	126870.f	3712fc5.a	isia-northe	ast1.gve.gc		v	Datastosos	Notworks	i blad uffenter for er forstemr	Extensions	lindates	
~ E	Datacenter	2fc5.asia-northeastl	ave.0000		Version: Build:	7.0.2 19272235	Permissions	DataCenters	Hosts & Clusters	VMS	Datastores	Networks	Linked vuenter server systems	Extensions	CPU User 14.31 CHz C	Press: 79.08 Girls
3	 esxi-128865137127c5.asta-northeasti.gve.goog 			[[]	Custeric 1 Hosts 1 Viriaai Machines 0				Morway Used: 150.67 GB C	Free: 009.50 GB Reportly: 766.26 GB Proc. 18.78 TB						
		*													Used: 1.69 TB	Capacity: 17.47 TD

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.

Status Operational
Location asia-northeast1 > v-zone-a > VE Placement Group 2
Expandable No
NSX-T login info <u>View</u> Reset password

2. Notieren Sie sich die NSX-T-Anmeldeinformationen.

Google Cloud VMware Engine									
	← NSX-T login								
Home	User name admin	Сору							
Network Activity	Password	<u>Сору</u>							

3. Starten Sie NSX Manager, indem Sie zu **VSPHERE MANAGEMENT NETWORK** navigieren und auf den **NSX Manager-FQDN** klicken.

Googl	e Cloud VMware Engine					
	Resources					
Home	← gcp-vmware-demo					₽ LAUNC
6	SUMMARY CLUSTERS	SUBNETS ACTIVITY	VSPHERE MANAGEMENT NETWORK	ADVANCED VCENTER SETTINGS DNS CONFIGURATION		
Resources	🛃 Download as CSV					
Network	Туре		Version	FQDN	相 🗢	IP Address
æ	vCenter Server Appliance		7.0.2.19272235	vcsa-126870.f3712fc5.asia-northeast1.gve.goog		10.231.0.6
Activity	NSX Manager			nsx-127044/3712fc5.asia-northeast1.ave.aooa		10.231.0.11
0	нсх			hcx-127045./3712fc5.asia-northeast nove.goog		10.231.0.13
(음급) Arcount	ESXi		7.0.2.18836573	esxi-126865.f3712fc5.asia-northeast1.gve.goog		10.231.0.15
Account	DNS Server 2			ns2-126869.f3712fc5.asia-northeast1.gve.goog		10.231.0.9
	DNS Server 1		**	ns1-126868.f3712fc5.asia-northeast1.gve.goog		10.231.0.8

4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens angegebenen Anmeldeinformationen beim NSX Manager an.

VMware® NSX-T™								
Username								
Password								
LOG IN								

- 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.
- 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.

vm NSX-T						Q	Ļ	. ()· ·	×	admin	
Home Networking Secur									•			
*	DHCP											
Network Overview												
関 Network Topology												
Connectivity					Server IP Address							
😝 Tier-O Gateways		management-client-dhq			(10.220.1254/24 ×) Enter IP Addresses	86400						
Tier-1 Gateways												
Segments		Edaa (lustar #			Edites							
Network Services			edge-cluster									
() VPN			Max 30 allowed. Clic									
EVPN Tenant												
B NAT		CANCEL										

14. Wiederholen Sie die Schritte 6 bis 13 für den Server-DHCP-Bereich.

vm NSX-T							O,	¢ 0.	*	admin
Home Networking Secur									POLICY	MANAGER
*	DHCP									0
(2) Network Overview										
🙀 Network Topology										re =
Connectivity										
# Tier-O Gateways		server-dhcp		DHCP Server 🗸	10.220.2.254/24 × Enter IP Addresses	86400				
Tier-1 Gateways										
Segments										
Natwork Services			edge-cluster							
(VPN			Max 30 allowed. Clk	Scope						
S EVPN Tenant										
- NAT		SAVE CANCEL								

- 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

Überlagerung**.

Transportzonenliste**TZ-OVERLAY aus

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.

Segments Segments S	egment Profiles Edge Bridge Pro	files Metadata Proxies									
ADD SEGMENT	ADD SEGMENT										
	Segment Name	Connected Gateway		Transport Zone	Subnets		Ports				
	management-client-segme *	Tieri Tieri		TZ-OVERLAY ~	10.230.11/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. 1c7e.1206.db42:1/48 SET DYCP CONFIG						

22. Klicken Sie auf **DHCP-Konfiguration festlegen**und geben Sie Werte für das Feld **DHCP-Bereiche** an.

Set DHCP (Config			×
Segment mana	agement-client-segment			
IPV4 Gateway	10.230.1.1/24 #DHCP Ranges ()	IPV6 Gateway	Not Set #DHCP Ranges 🧿	
DHCP Type *	Local DHCP Server 🗸 🛈	DHCP Profile *	management-client-dhcp	
IPv4 Server				
	ptions			
DHCP Config	C Enabled			
DHCP Server	10.230.1.254/24			
Address *	CIDR e.g. 10.22.12.2/23			
DHCP Ranges	99 Maximum Format 172.16.14.10-172.16.14 range to avoid duplicate IP address allocati	100 or 172.16.14.0/24 Please verify th on		
10.230.1.10-10.230.1	1.100 ×			
Enter DHCP Rang	jes			
Lease Time	Default value is 86400			
(aeconda)				
DNS Servers	Enter IP Addresses			
				R

- 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**.

Edit Settings NSVPX-ESX-13.1	-24.38_nc_64	>
Virtual Hardware VM Options		
		ADD NEW DEVICE ~
> CPU	2 ~	١
> Memory	2	✓ GB ✓
> Hard disk 1	20 GB	×
> SCSI controller 0	LSI Logic Parallel	
✓ Network adapter 1	management-client-segmer	nt 🗸
Status	Connect At Power On	
Port ID	372795cc-b049-47b4-b9	
Adapter Type	VMXNET 3 🗸	
DirectPath I/O	Enable	
Shares	Normal ~ 50	~
Reservation	° T	✓ Mbit/s ✓
Limit	Unlimited	✓ Mbit/s ✓

✓ New Network *	server-segment v
Status	Connect At Power On
Adapter Type	VMXNET 3 ~
DirectPath I/O	Z Enable
Shares	Normal V 50 V
Reservation	0
Limit	Unlimited V Mbit/s V
MAC Address	Automatic ~
> Video card	Specify custom settings ~
VMCI device	
	CANCEL

7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance in der VMware Cloud zu beginnen.

1 Select an OVF template 2 Select a name and folder 3 Select a compute resource 4 Review details 5 Select storage 6 Select networks 7 Ready to complete	×
Name NsVPX-EsX-13.1-24.38_nc_64 2 Select a name and folder Template name NSVPX-ESX-13.1-24.38_nc_64 3 Select a compute resource Download size 661.4 MB 4 Review details Size on disk 20.0 GB 5 Select storage Folder Workload VMs 6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: roanDatastore; Format: As defined in the VM storage policy	- I
3 Select a compute resource Download size 661.4 MB 4 Review details Size on disk 20.0 GB 5 Select storage Folder Workload VMs 6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: Format: As defined in the VM storage policy	-
3 Select a complete resource bownidad size boli 4 MB 4 Review details Size on disk 20.0 GB 5 Select storage Folder Workload VMs 6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: Format: As defined in the VM storage policy	-
4 Review details Size on disk 20.0 GB 5 Select storage Folder Workload VMs 6 Select networks Resource Workload 7 Ready to complete All disks Datastore: roanatastore; Format: As defined in the VM storage policy	
Folder Workload VMs 5 Select storage Resource Workload 6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: Format: As defined in the VM storage policy	
5 Select storage Resource Workload 6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: vsanDatastore; Format: As defined in the VM storage policy	
6 Select networks Storage mapping 1 7 Ready to complete All disks Datastore: vsanDatastore; Format: As defined in the VM storage policy	
7 Ready to complete All disks Datastore: vsanDatastore; Format: As defined in the VM storage policy Network manping 1	
Network mapping 1	
rector inspiring	
VM Network management-client-segment	
IP allocation settings	
IP protocol IPV4	
IP allocation Static - Manual	
CANCEL BACK FINISH	

 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.

VSphere - NSV	PX-ESX-13.0-79.6 × NSX	x +	- 0
$\leftarrow \rightarrow $ C	Not secure https://192.168/	$eq:linearized_linearized$	6 6 6
Jan JuSobere Cl	Actions - NSVPX-ESX-13.0-79.64_n_	In all ansienements	EDVEDE LOCAL N
vapriere ci	Power &	Power On christelle B	SPIERELUURL Y
	Guest OS	Power Off	
	Snapshots	II Suspend cbit + all + 2	
 vc.de7510d9c7d8 SDDC-Datacent 	😴 Open Remote Console	astores Networks	
V 🚺 Cluster-1	🚓 Migrate	4-bit)	CPU USAGE
esx03-r09 esx04-r02 esx14-r15.c	Clone	P Declari Class III alled	MEMORY USAGE
	Fault Tolerance	DNS Name:	ов
	VM Policies	P Addresses: Host: esx04-r02.p03.de7510d9c7d8485cb31194.eastus.avs.azure.com	STORAGE USAG
	Template		40.83 GB
	Compatibility		
	Export System Logs	✓ Notes	^
	🚱 Edit Settings	Edit Notes	
	Move to folder	^	
	Rename	Custor Attributes	^
	Edit Notes	esx04-r02.p03.de7510d9c7d8485cb31194.east	
	Tags & Custom Attributes	& client	
Recent Tasks Ala	Add Permission		
Task Name	Alarms	v Details v Initiator v Queued For v Start Time ↓ v Completion Time	 Server
Reconfigure virtual	Remove from Inventory	ed VSPHERELOCALIcioud 4 ms 05/02/2021, 4:108 PM 05/02/2021, 4:108 PM	vc.de7510d9c7d8485c
Deploy OVF template	Delete from Disk	ed VSPHERE LOCAL/vprd 3 ms 05/02/2021, 4:08:26 PM 05/02/2021, 4:09:12 PH	4 vc.de7510d9c7d8485c

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.

11. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
1 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.

Done is a kp is		
1) DIX 566.4.5 & Second P Active Fronthed Exciled 1) DIX 566.5.5 0 VP Active Fronthed Exciled 1) DIX 566.5.0 SHEP Active Fronthed Enabled N Down 0 *	Vserver St	itate
*	NA En Enabled En NA En	nables nables nables

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.

Google	e Cloud VMware E	ngine									0	ą	¢	ß	۲
	Network														
ß	FIREWALL TABLES	SUBNETS	PUBLIC IPS	VPN GATEWAYS	DNS CONFIGURA	TION	PRIVATE CONNECTION	REGIONAL	SETTINGS						
	Regional Settings													Ado	Region
Resources	🕁 Download as CSV										Column :	ettings	机 5	elected (ilters (0)
Retwork	Region		≑ Re	gion Status	\$	Internet	t Access	\$	Public IP Se	rvice	\$ Edge Se	vices CI	DR		\$

- 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**.

Goog	e Cloud VMware Engine						0	4)	\$ ¢ (Ð
	Network									
ß	FIREWALL TABLES SUBNE	IS PUBLIC IPS	VPN GATEWAYS	DNS CONFIGURATION	PRIVATE CONNECTION	REGIONAL SETTINGS				
	Public IPs (0)								Alle	5
Researces										1

- 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**.

Google	e Cloud VMware Engine								
	← Allocate Public IP ③								
Home	Name * 🐵								
6	vpx-management-public-ip								
Resources	Location *								
0	asia-northeast1 -								
ිදුර Network	Private cloud *								
	gcp-vmware-demo -								
(Th) Activity	Attached local address * 💿								
Activity	10.230.1.10								
Account	You need to open Firewall ports to enable traffic on this IP address through the Firewall Table feature.								
	Submit Cancel								

- 5. 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.



Firewall 🙆

- 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:

1	REQUIRED_INSTANCE_IAM_PERMS = [
2	"compute.instances.get",
3	"compute.instanceGroupManagers.get",
4	<pre>"compute.instanceGroupManagers.list",</pre>
5	"compute.zones.list",
6	"logging.sinks.create",
7	"logging.sinks.delete",
8	"logging.sinks.get",
9	"logging.sinks.list",
10	"logging.sinks.update",
11	"pubsub.subscriptions.consume",
12	"pubsub.subscriptions.create",
13	"pubsub.subscriptions.delete",
14	"pubsub.subscriptions.get",
15	"pubsub.topics.attachSubscription",
16	"pubsub.topics.create",
17	"pubsub.topics.delete",
18	"pubsub.topics.get",
19	"pubsub.topics.getIamPolicy",
20	"pubsub.topics.setIamPolicy",
21]

- 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 nsrootbei 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.

me			
DemoCloudProfile			
tual Server IP Address*			
192.168.2.24	\sim		
ad Balancing Server Protocol			
HTTP	\sim		
ad Balancing Server Port			
80			
to Scale Group*			
ansible-mig-defaultuser-1585300924	l-: 🗸		
to Scale Group Protocol			
HTTP	\sim		
to Scale Group Port			
80			

- 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**.

Q Search in Menu		Google Cloud	Platform / Cloud Pro	file				
Google Cloud Platform	\sim	Cloud F	Profile 💶				G	F
🕸 Cloud Profile								
System	>	Add	Edit Delete					
AppExpert	>	Q Click here	to search or you can ent	er Key : Value format				(i)
Traffic Management	>							
Optimization		\checkmark	NAME	AUTO SCALE GROUP	LOAD BALANCING VIRTUAL SERV	ER 🤤	AUTO SCALE GROUP PROTOCO	JL ≑
Security		\checkmark	DemoCloudProfile	ansible-mig-defaultuser-1585300924-1	_CP_DemoCloudProfile_192.168	2.24_LB_	HTTP	
Security								
Authentication	>	Total 1				25 Per Page	✓ Page 1 of 1 <	•

Die Konfigurationsseite " Cloud-Profil erstellen "wird angezeigt.

G Create Cloud Profile

Name	
DemoCloudProfile	
Virtual Server IP Address*	
192.168.2.24	\sim
Load Balancing Server Protocol	
HTTP	\sim
Load Balancing Server Port	
80	
Auto Scale Group*	
ansible-mig-defaultuser-1585300924-	-: ~
Auto Scale Group Protocol	
НТТР	\sim
Auto Scale Group Port	
80	

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.

Q Search in Menu		Google Cloud	Platform / Cloud Pro	ofile				
Google Cloud Platform	\sim	Cloud Profile 1						C 📑
Cloud Profile								
System	>	Add Edit Delete						
AppExpert	>	Q Click here to search or you can enter Key : Value format					(j)	
Traffic Management	>		NAME	AUTO SCALE GROUP	÷ LC	OAD BALANCING VIRTUAL SERVER	AUTO SCALE GROUP PRO	TOCOL 🔅
Optimization		•	Deve Claud Dev Gla					
Security	>		DemocloudProfile	ansible-mig-defaultuser-1585300924-1	_(CP_DemociouaPronie_192.168.2.24_LB_	HIIP	
Authentication	>	Total 1				25 Per Pa	ge V Page 1 of 1	

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:

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.list",
3	"compute.addresses.get",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.instances.use",
10	"compute.subnetworks.use",
11	"compute.targetInstances.create"
12	"compute.targetInstances.get"
13	"compute.targetInstances.use",
14]

- 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:

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.list",
3	"compute.addresses.get",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.instances.use",
10	"compute.subnetworks.use",
11	"compute.targetInstances.create",
12	"compute.targetInstances.list",
13	"compute.targetInstances.use",
14]

• Wenn Sie die VIP-Skalierung in einem Hochverfügbarkeitsmodus verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.get",
3	"compute.addresses.list",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.forwardingRules.setTarget"
10	"compute.instances.use",
11	"compute.instances.get",
12	"compute.instances.list",
13	"compute.instances.setMetadata",
14	"compute.subnetworks.use",
15	"compute.targetInstances.create",
16	"compute.targetInstances.list",
17	"compute.targetInstances.use",
18	"compute.zones.list",
10	1

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

VM instance	details	/ EDIT	레 RESET	+ CRE
Select a shielded image to u Turn on all settings for the m Turn on Secure Boot (Turn on vTPM @ Turn on Integrity Moni	se shielded VM features. nost secure configuration			
Availability policies				
Preemptibility				
Off (recommended)				
On host maintenance				
Migrate VM instance (ree	commended)		•	
Automatic restart				
On (recommended)				
Custom metadata				
vips	{		/ ×	
	+ Add item			
SSH Keys Block project-wide SSI When checked, project-v You have 0 SSH keys Show and edit	H keys vide SSH keys cannot acc	cess this instanc	e Learn more	
Service account				
You must stop the VM instar	nce to edit its service acc	ount		
416809692761-compute@	developer.gserviceaco	count.com		
Cloud API access scopes				
You must stop the VM instar	nce to edit its API access	scopes		
Allow full access to all Clo	oud APIs			
Save Cancel				

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.

Q Search in Menu		Traffic Management / Load Balancing / Virtual Servers			
Google Cloud Platform	>	Virtual Servers			
System	>				
AppExpert	>	Add Edit Delete Enable Disable	Rename	Statistics	Select
Traffic Management	\sim	Q Click here to search or you can enter Key : Value format			
Load Balancing	\sim				
😭 Virtual Servers		NAME	STATE 0	EFFECTIVE STATE	IP A
Services		gcplbdnsvserver	• UP	UP	0.0.0
Service Groups		lbv2	• UP	• UP	10.3
Monitors		v1	DOWN	DOWN	10.2
Metric Tables		Demo-vServer	• DOWN	• DOWN	34.9
Servers		Total 4			

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**.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an app address is a public IP address. If the application is accessible only from the local area network (L (ICANN non-routable) IP address.

You can configure multiple virtual servers to receive client requests, thereby increasing the avail

Demo-vServer		
Protocol*		
HTTP	\sim	
IP Address Type*		
IP Address	\sim	
IP Address*		
34 . 93 . 61 . 42	()	
Port*		
80		

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**.

Coad Balancing Service

Basic Settings	
Service Name*	
Demo-Service	(j)
New Server Existing Server	
10 . 30 . 1 . 54	í
Protocol*	
НТТР	\sim
Port*	
80	

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.

	Load Balan Basic Settin	cing Virtual Server Export as a Template			/
N Pi SI IP Pi Tř	lame rotocol tate > Address ort raffic Domain	Demo-vServer HTTP ● DOWN 34.93.61.42 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- NONE IP 1 - PASSIVE ENABLED NO	
	Services and	d Service Groups			
	No Load Bala	ncing Virtual Server Service Binding			>
	No Load Bala	ncing Virtual Server ServiceGroup Binding			>

4. Wählen Sie den in Schritt 3konfigurierten Dienst aus und klicken Sie auf "Binden".

,	
Service Binding	
Select Service*	
Demo-Service	> Add Edit ()
Binding Details	
Weight	

5. Speichern Sie die Konfiguration.

Problembehandlung bei einer VPX-Instanz auf GCP

January 15, 2025

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**.

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.

NetScaler VPX 14.1

Q Search in Menu		System / System Information
Google Cloud Platform	>	System
System	\sim	System
🖕 🟠 Licenses		System Information System Sessions 1 System Network
Settings		System Upgrade Reboot Migration Statistics Call Home Citrix ADM Service Connect
Diagnostics		
High Availability	>	System Information
NTP Servers		
Reports		Citrix ADC IP Address 10.160.15.230
Profiles		Netmask 255.255.240.0
		Node Standalone
Partition Administration	>	Technical Support PIN 4051153
User Administration	>	Time Zone Coordinated Universal Time
Authentication	>	System Time Sat, 11 Jul 2020 01:56:22 UTC
Auditing	>	Last Config Changed Time Sat, 11 Jul 2020 01:53:09 UTC
SNMP	>	Last Config Saved Time Sat, 11 Jul 2020 01:53:12 UTC
AppFlow	• >	Hardware Information
Cluster	>	

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:

- 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.
- 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:

- 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.
- 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

January 15, 2025

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?

Ja, das Hinzufügen von CPU-Kernen kann die Leistung von NetScaler VPX verbessern, vorausgesetzt, die NetScaler VPX-Instanz ist für die zusätzlichen vCPUs lizenziert. NetScaler VPX kann je nach Konfiguration und Leistungsstufe bis zu 20 vCPUs unterstützen (für eine Leistung von 41 Gbit/s –100 Gbit/s). Mehr vCPUs können dazu beitragen, den Durchsatz zu erhöhen, insbesondere in Hochleistungsszenarien. Die Auswirkungen auf die Leistung hängen jedoch auch von Faktoren wie den Netzwerktreibern (z. B. PCI-Passthrough oder SR-IOV) und der spezifischen Arbeitslast ab. Informationen zur Anzahl der für verschiedene VPX-Leistungsstufen unterstützten vCPUs finden Sie im NetScaler VPX-Datenblatt.

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 | Informationen zu den Prozessoranforderungen Ihrer VPX-Plattform finden Sie in der [Unterstützte Prozessoren für NetScaler VPX](/de-de/vpx/current-release/supported-hypervisorsfeatures-limitations.html#supported-processors-for-netscaler-vpx) Tisch. |

| 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|Verwenden Sie eine Netzwerkkarte, die mit Ihrem Hypervisor kompatibel ist. Weitere Informationen finden Sie unter [Unterstützte Netzwerkkarten für NetScaler VPX](/de-de/vpx/currentrelease/supported-hypervisors-features-limitations.html#supported-nics-for-netscaler-vpx).|

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.
- Ab Version NetScaler 13.1 unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi-Hypervisor AMD EPYC-Prozessoren.

Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

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?

Bei vielen Servern sind Virtualisierungsunterstützungsfunktionen (wie VT-x oder AMD-V) in den BIOS-Einstellungen standardmäßig deaktiviert. Bevor Sie zu dem Schluss kommen, dass Sie NetScaler VPX nicht ausführen können, überprüfen Sie die BIOS-Konfiguration. Wenn die Virtualisierungsunterstützung deaktiviert ist, müssen Sie sie möglicherweise im BIOS aktivieren, um sicherzustellen, dass Ihr Server virtualisierte Anwendungen wie NetScaler VPX ordnungsgemäß ausführen kann.

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?

Jeder NetScaler VPX-Instanz müssen mindestens 2 GB Speicher zugewiesen werden. Das NetScaler VPX-Disk-Image ist auf 20 GB ausgelegt, um Wartungsanforderungen gerecht zu werden, einschließlich Platz zum Speichern von bis zu 4 GB Core-Dumps sowie Protokoll- und Ablaufverfolgungsdateien. 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.

Die folgenden Werte stellen den Speicherplatz dar, der bestimmten Verzeichnissen auf der NetScaler VPX-Instanz zugeordnet ist:

- /Flash = 965 MB
- /var = 14G

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 "In -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.
- 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.

net>scaler

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

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