net>scaler

NetScaler VPX 14.1

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントの コンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は 機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合 があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使い の Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該 当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての 契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明 示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。 機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負 わないものとします。

Contents

NetScaler VPX サポートマトリックス	6
VMware ESX、Linux KVM、および Citrix Hypervisor で NetScaler ADC VPX のパフォーマンスを最 適化する	21
NetScaler VPX のディスク容量を増やすためのサポート	37
NetScaler VPX 構成をクラウドで NetScaler アプライアンスの最初の起動時に適用する	39
パブリッククラウドプラットフォームでの SSL-TPS パフォーマンスを向上させる	74
パブリッククラウド上の NetScaler VPX 同時マルチスレッドを構成する	75
NetScaler サニティチェッカーツール	79
NetScaler VPX インスタンスをベアメタルサーバーにインストールする	80
Citrix Hypervisor/XenServer への NetScaler VPX インスタンスのインストール	81
シングルルート I/O 仮想化 (SR-IOV) ネットワークインターフェイスを使用するように VPX インスタンスを 構成する	85
VMware ESX に Citrix ADC VPX インスタンスをインストールする	90
VMXNET3 ネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する	95
SR-IOV ネットワークインターフェイスの使用を NetScaler ADC VPX インスタンスで構成する	107
SR-IOV モードでの SSL アクセラレーションにインテル QAT を使用するように ESX ハイパーバイザー上の NetScaler VPX を構成する	125
E1000 から SR-IOV または VMXNET3 ネットワークインターフェイスへの NetScaler VPX の移行	129
PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する	129
VMware ESX ハイパーバイザーでの NetScaler ADC アプライアンスの初回起動時に NetScaler ADC VPX の構成を適用する	133
AWS の VMware クラウドに Citrix ADC VPX インスタンスをインストールする	143
Microsoft Hyper-V サーバーに NetScaler VPX インスタンスをインストールします	145
Linux-KVM プラットフォームへの Citrix ADC VPX インスタンスのインストール	150

Linux-KVM プラットフォームに Citrix ADC VPX インスタンスをインストールするための前提条件	151
OpenStack を使用して Citrix ADC VPX インスタンスをプロビジョニングする	156
仮想マシンマネージャーを使用して NetScaler VPX インスタンスをプロビジョニングします	165
SR-IOV ネットワークインターフェースを使用するように NetScaler VPX インスタンスを構成する	180
SR-IOV モードでの SSL アクセラレーションに Intel QAT を使用するように KVM ハイパーバイザー上の NetScaler VPX を構成します	190
PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する	194
virsh プログラムを使用して NetScaler ADC VPX インスタンスをプロビジョニングする	199
NetScaler VPX ゲスト仮想マシンの管理	203
OpenStack 上で SR-IOV を使用して NetScaler VPX インスタンスをプロビジョニングします	206
KVM 上の NetScaler VPX インスタンスが OVS DPDK ベースのホストインターフェイスを使用するように 構成する	212
KVM ハイパーバイザーでの NetScaler ADC アプライアンスの初回起動時に NetScaler ADC VPX の構成 を適用する	222
AWS での NetScaler VPX	224
AWS 用語	227
AWS-VPX サポートマトリックス	229
制限事項と使用ガイドライン	232
前提条件	234
NetScaler VPX インスタンスで AWS IAM ロールを設定します	236
AWS 上の NetScaler VPX インスタンスの仕組み	246
NetScaler VPX スタンドアロンインスタンスを AWS にデプロイする	248
シナリオ:スタンドアロンインスタンス	253
NetScaler VPX ライセンスをダウンロードする	262
異なる可用性ゾーンでの負荷分散サーバー	268

AWS での高可用性の機能	268
同じ AWS 可用性ゾーンに VPX HA ペアを展開する	271
異なる AWS アベイラビリティーゾーンでの高可用	282
異なる AWS ゾーンに Elastic IP アドレスを使用した VPX 高可用性ペアをデプロイする	283
異なる AWS ゾーンにプライベート IP アドレスを使用して VPX 高可用性ペアを展開する	288
AWS Outpost で NetScaler VPX インスタンスを展開する	301
NetScaler Web App Firewall を使用して AWS API ゲートウェイを保護	305
バックエンドの AWS Autoscaling サービスを追加する	308
NetScaler GSLB を AWS に展開	313
AWS への NetScaler Web App Firewall デプロイ	328
SR-IOV ネットワークインターフェイスの使用を NetScaler ADC VPX インスタンスで構成する	350
AWS ENA での拡張ネットワークの使用を Citrix ADC VPX インスタンスで構成する	353
AWS 上の NetScaler VPX インスタンスのアップグレード	354
AWS での VPX インスタンスのトラブルシューティング	358
AWS に関するよくある質問	359
Microsoft Azure で NetScaler VPX インスタンスを展開する	362
Azure 用語集	367
Microsoft Azure 上の NetScaler ADC VPX インスタンスのネットワークアーキテクチャ	370
NetScaler VPX スタンドアロンインスタンスを構成する	373
NetScaler VPX スタンドアロンインスタンスに複数の IP アドレスを構成する	387
複数の IP アドレスと NIC を使用して高可用性設定を構成する	393
PowerShell コマンドを使用して複数の IP アドレスと NIC を使用して高可用性セットアップを構成する	403
フローティング IP 無効モードの ALB を使用して Azure に NetScaler 高可用性ペアをデプロイする	415
Azure DNS プライベートゾーン用 NetScaler デプロイ	436

Azure アクセラレーションネットワークを使用するように NetScaler VPX インスタンスを構成する	456
Azure ILB で NetScaler 高可用性テンプレートを使用して HA-INC ノードを構成する	471
インターネット向けアプリケーション用の NetScaler 高可用性テンプレートを使用して HA-INC ノードを 構成する	484
Azure 外部および内部ロードバランサーで同時に高可用性セットアップを構成する	495
Azure VMware ソリューションに NetScaler VPX インスタンスをインストールする	499
Azure VMware ソリューションでスタンドアロンの NetScaler ADC VPX インスタンスを構成する	516
Azure VMware ソリューションで Citrix ADC VPX の高可用性セットアップを構成する	518
NetScaler VPX HA ペアで Azure ルートサーバーを構成する	520
バックエンドの Azure 自動スケーリングサービスを追加	524
NetScaler VPX 展開用の Azure タグ	531
NetScaler VPX インスタンスで GSLB を構成する	537
アクティブ / スタンバイの高可用性セットアップで GSLB を構成する	546
Azure に NetScaler GSLB を展開	549
NetScaler Web App Firewall を Azure にデプロイする	565
NetScaler Gateway アプライアンスのアドレスプールのイントラネット IP を構成する	588
PowerShell コマンドを使用して、NetScaler VPX スタンドアロンインスタンスに複数の IP アドレスを 構成する	591
Azure 展開の追加の PowerShell スクリプト	599
Azure で VPX インスタンスのサポートチケットを作成する	615
Azure に関するよくある質問	616
Google Cloud Platform への NetScaler ADC VPX インスタンスのデプロイ	617
VPX の高可用性ペアを Google Cloud Platform に展開する	632
Google Cloud Platform に外部の静的 IP アドレスを指定した VPX 高可用性ペアをデプロイする	634

Google Cloud Platform にプライベート IP アドレスを指定した 1 つの NIC VPX 高可用性ペアをデプロ イします	643
プライベート IP アドレスを持つ VPX 高可用性ペアを Google Cloud Platform にデプロイする	652
Google Cloud VMware Engine に NetScaler VPX インスタンスをインストールする	661
バックエンドの GCP Auto Scaling サービスを追加する	680
GCP 上の NetScaler VPX インスタンスの VIP スケーリングサポート	685
GCP での VPX インスタンスのトラブルシューティング	692
NetScaler VPX インスタンスのジャンボフレーム	693
NetScaler の導入と構成を自動化する	694
よくある質問	698

NetScaler VPX サポートマトリックス

June 12, 2025

このドキュメントでは、NetScaler VPX インスタンスでサポートされているさまざまなハイパーバイザーと機能に ついて説明します。また、使用上のガイドラインと既知の制限事項についても説明します。

VMware ESX ハイパーバイザー上の VPX インスタンス

	/°			
ESX	iフ			
の	NetScaler			
esxi e	SM/PX-			
バリビ	ごバマ			
— — ม	ィーン			
ジスド	・ジス			
∃ 日 番	育 ヨ 範			
ン (年月	月四囲			
ESX02!	36741 64			
8.0年	43.x			
ア4	_以 10Mbps~			
ッ 月	_降 100Gbps			
プ 10	Ø			
デ日	Е			
_	ル			
۲	۲			
3e				
ESX02	54/1025/16/2 13			
8.0	38.x			
up-	と			
date	そ			
3d	れ			
	以			
	降			
	Ø			
	ビ			
	ル			
	ド			

/ <u>^</u>			
ESXi フ			
の NetScaler			
esxi esxip x.			
バリビバマ			
ーールーン			
ジスドジス			
ョ 日 番 ョ 範			
ン (年月) 知囲			
ESXD2340004/12-031			

8.0	29.x
ア	以
ッ	降
プ	の
デ	ビ
_	ル
۲	ド
3c	
ESX024	2090/11 -677
8.0	17.x
8.0 ア	17.x と
8.0 ア ツ	17.x と そ
8.0 ア ツ プ	17.x と そ れ
8.0 ア ッ プ デ	17.x と そ れ 以
8.0 ア ッ プ デ ー	17.x と そ れ 以 降
8.0 ア ッ プ デ ト	17.x と そ れ 以 降 の
8.0 ア ッ プ デ ー ト 3b	17.x と そ れ 以 降 の ビ

ド

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

	<i>\</i> ۲					
E:	SXi フ					
の	NetScaler					
ESXI	ESM/PX-					
バリ	ビバマ					
	・ルーン					
ジス	ドジス					
ヨΒ	番ョ範					
ン (生	F月/2019					
ESXI	0 24/025/5 50					
8.0	17.x					
ア	ک					
ッ	そ					
プ	れ					
デ	以					
_	降					
۲	の					
3	ビ					
	ル					
	۴					
ESXi	ハ XenS&MMerrare	Mic術ostoffeeatures	イ PVSRPVSI	R≖ P CP VP	VSRPCI	Multiは は
8.0	イ上 ESX	Нурвек₀ ^^ ^^ △^ △^_ — — — — — — — — —	ン IOV IO	モパ	۱OV	PE い い い
ア	パの上	V 的	タ	ュス	ス	の
ッ	— VPX の	上 KVM	_	レス	ス	サ
プ	バ VPX	の上	フ	ール	ル	ポ
デ	1	VPXo	I	ト ー	—	_
—	ザ	VPX	—			۲
F	_		ス			
2b	\rightarrow		→			

Л		
ESXi フ		
の NetScaler		
esxi esxipx-		
バリビバマ		
ーールーン		
ジスドジス		
ョ 日 番 ョ 範		
ン (年月) 旧囲		

ESX024	3 /30925/12-9 6
--------	------------------------

8.0 4.x ア お よ ッ プ び そ デ _ れ ۲ 以 2 降 の ビ ル ド ESX023/30390/12-119 8.0 4.x ア お ッ よ プ び デ そ _ れ ۲ 以 降 2 の ビ

ルド

パ			
ESXi フ			
の NetScaler			
esxi esxip x.			
バリビバマ			
ーールーン			
ジスドジス			
ョ日番ョ範			
ン (年月) 2日 囲			
ESXD23/1945/11-987			

8.0	4.x
ア	お
ッ	よ
プ	び
デ	そ
_	れ
۲	以
1	降
	の
	ビ
	ル
	۲
ESX023	/ 1988/13-10 6
ES XD23 8.0c	/ 10983/13520 6 4.x
ES XD23 8.0c	/1983/13:20 6 4.x お
ES X D 23 8.0c	/1983/193206 4.x お よ
ES X D 23 8.0c	/1383/13206 4.x お よ び
ES X D 23 8.0c	/1988/15:20 6 4.x お よ び そ
ES X D 23 8.0c	/1988/1520 6 4.x お よ び そ れ
ES X D 23 8.0c	ADBRABD6 4.x お よ び そ れ 以
ES X D 23 8.0c	ADBRABD6 4.x お よ び そ れ 以 降
ES X D 23 8.0c	ADBRABDO 4.x お よ び そ れ 以 降 の
ES X D 23 8.0c	4088/1820 6 4.x およびそれ以降のビ

ド

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

٦N°			
ESXi フ			
の NetScaler			
ESXI ESXIPX-			
バリビバマ			
ーールーン			
ジスドジス			
ョ 日 番 ョ 範			
ン (年月) 旧囲			
ESXD220/5140310-97			

8.0 4.x お よ び そ れ 以 降 の ビ ル ド ESX0254/085/10941 7.0 29.x ア 以 ッ 降 プ の デ ビ ル

- ー ル ト ド
- 3s

	/۲					
ES	SXi フ					
の	NetScaler					
ESXI	ESM/PX-					
バリ	ビバマ					
	ルーン					
ジス	ドジス					
ヨ日	番ョ範					
ン (年	周阳田					
ESXI) 24/<u>11421/14-</u>2 4					
7.0	29.x					
ア	以					
ッ	降					
プ	Ø					
デ	ビ					
_	ル					
۲	۲					
3r						
ESXi	ハ XenSMMerrare	Micৈπo∣stofffeatures	イ PV	SRPVSR≖ PC P V	PVSRPCI	Multik k
7.0	イ上 ESX	Ну р ељ/^^ ^^ <u></u> ^^	ン	IOV IOVE パ	۱ ΟV %	PE い い い
ア	パの上	V 的	タ	ュス	ス	の
ッ	— VPX の	上 KVM	—	レス	ス	サ
プ	バ VPX	の上	フ	ール	ル	ポ
デ	イ	VPXo	т	ト −	_	_
_	ザ	VPX	_			۲
۲	_		ス			
3q	→		→			
•						

パ ESXi フ の NetScaler SXi ESMPX- ベローンン スドジス 日番 = 範 (年用)/四囲 SXi 2330711-99 0- 4.x pル お aTe6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド S SD22/04/3286 0 4.x p- お ate よ 2 び そ れ れ 以 降 の ビ ノ ル ド
ESXi フ の Net& Scaler SXi ESMPX- ベリビバマ - ルーン ジスドジス 日番ョ範 · (年月) / 四囲 SXi 2330711-99 0- 4.x pル お arte6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SSU22/VE/BEØ 0 4.x p- お ate よ o び そ れ れ 以 降 の に 天
の Net&Galer SXI ESMPX- ド ビバマ マルーン マボジス マボジス 日番ョ範 *(年月)/日囲 SXi 233071199 ハー 4.x pル お a都e6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SZD230498960 0 4.x p- お ate よ ウ び そ ハ ド
SXI ESMPX- ぶ リビ バマ - ルーン ズ ド ジス 白 番 ョ 範 (年月) / 日囲 SXI 2330711-99 4.x pル お a都e6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD22/UP(DBC 0 4.x p- お ate よ - び そ れ 以 降 の ビ り、 び そ れ 以 ド
 バマベマ バマジス スドジス 日番 = 範 (年月)/40円 SXi 2330711-99 .0- 4.x pル お a都e6、よ pレ び - そ ル れ 8.0、以 レ び - そ ル れ 8.0、以 レ ビ 9.3 ル ド SZD23509(996) 0 4.x p- お ate よ 0 び そ れ 以 降 0 び そ れ 以 降 0 び 6 7 8 8 10 10 11 12 12 12 13 14 15 14 15 15 16 17 18 18 18 18 19 19 19 10 10 10 11 11 12 12 12 13 14 15 14 15 15 16 16 17 18 18 18 18 19 19 19 10 10 10 11 11 12 12 12 13 14 14 15 16 16 17 18 18 18 18 18 18 18 18 18 18 18 18 19 19 19 10 10 10 10 10 10 11 11 12 12 13 14 14 15 16 16 16 17 17 18
- ルーン スドジス 日番 = 範 · (年月)/2月 SXi 233071199 0- 4.x pル お a型66、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD22,50495286 0 4.x p- お ate よ つ び それ れ 以 降 の ビ り、 が そ れ 以 下 SXD23,5045528 0 4.x p- お ate よ つ び それ れ 以 下 SXD23,5045528 0 7 それ れ い た 5 7 7 7 7 7 7 7 7 7 7 7 7 7
² スドジス 日番ョ範 · (年月)/20日 SXi 2330711-99 .0- 4.x pル お a和e6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD22,5049(9296 0 4.x p- お ate よ つ び それれいいい 降 の ビ ル ド
日番 当範 (年月) / (年月) / (1000 / (
<pre>Y (年期)/日囲 SXi 2330711-99 O- 4.x pル お a和e6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD23/D09/9286 O 4.x p- お ate よ D び そ れ 以 降 の ビ ル ド</pre>
SXi 2330711-99 .0- 4.x pル お a和e6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD22704909266 0 4.x p- お ate よ つ び そ れ 以 降 の ビ り、 ド
N 4.x pル お a種6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド S XD23/049/9286 0 4.x p- お ate よ つ び そ れ 以 降 の ビ り、 ド
pル お afe6、よ pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド S XD23/J99(9286 0 4.x p- お ate よ o び そ れ 以 降 の ビ ル
F ¹¹
pレ び - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD22/J99/B286 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル ド
F・ こ - そ ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SZD23/DB/B2B6 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル ド
ル れ 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD23/D9/9286 .0 4.x p- お ate よ c び そ れ 以 降 の ビ ル
No. 102 8.0、以 レ 降 - の ル ビ 9.3 ル ド SXD232504962866 .0 4.x p- お ate よ つ び そ れ 以 降 の ビ ル ド
レ 降 - の ル ビ 9.3 ル ド SXID23/JONE/B2B6 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル ド
レ ド - の ル ビ 9.3 ル ド SXD23/349(9386 .0 4.x p- お ate よ つ び そ れ 以 降 の ビ ル ド
・・ ル ビ 9.3 ル ド SXD23/349/3286 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル ド
9.3 ル ド SXD223/049/9386 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル
ド SXD23,5049,6236 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル
SXD232,5049,6286 .0 4.x p- お ate よ o び そ れ 以 降 の ビ ル ド
p- お ate よ o び そ れ 以 降 の ビ ル
ate よ o び そ れ 以 降 の ビ ル
- び それ 以 降 の ビ ル
それ れ 以 降 の ビ ル ド
- れ 以 降 の ビ ル ド
、 以 降 の ビ ル ド
降 の ビ ル ド
の ビ ル ド
ビル
ド
۲

	١Ŷ				
ESX	(i フ				
の	Net&caler				
ESX/I E	es x px-				
バリヒ	ビバマ				
— — J	レーン				
ジスト	ドジス				
ヨ日看	番 ヨ 範				
ン (年春	新 /知囲				
ES%202	3/9030/16/68				
7.0	8.x				
up-	ک				
date	そ				
3n	れ				
	以				
	降				
	の				
	Ľ				
	ル				
	ド				
ESX02	2 3/026/10/3 3				
7.0	4.x				
up-	お				
date	よ				
3m	び				
	そ				
	れ				
	以				
	降				
	の				
	ビ				
	ル				
	ĸ				

各 ESXi パッチサポートは、前の表で指定されている NetScaler VPX バージョンで検証されており、NetScaler VPX 14.1 バージョンのすべての上位ビルドに適用されます。

使用ガイドラインの詳細については、「VMware ESXi ハイパーバイザーの使用ガイドライン」を参照してくださ

ιı°

XenServer または **Citrix Hypervisor** 上の **VPX** インスタンス

KenServer または Citrix						
Hypervisor のバージョン	SysID	パフォーマンス範囲				
8.4、NetScaler VPX バージョン	450000	10Mbps~40Gbps				
14.1 ビルド 17.x 以降からサポート						
8.2、NetScaler VPX バージョン						
13.0 ビルド 64.x 以降でサポート						
8.0, 7.6, 7.1						

Microsoft Hyper-V上の VPX インスタンス

Hyper-V 版	SysID	パフォーマンス範囲
2016, 2019	450020	10Mbps~3Gbps

Nutanix AHV o VPX インスタンス

NetScaler VPX は、Citrix Ready パートナーシップを通じて Nutanix AHV でサポートされています。Citrix Ready は、ソフトウェアおよびハードウェアのベンダーが自社製品を開発し、デジタルワークスペース、ネットワーキング、 および分析用の NetScaler テクノロジーと統合するのを支援するテクノロジーパートナープログラムです。

NetScaler VPX インスタンスを Nutanix AHV にデプロイする段階的な方法の詳細については、「Nutanix AHV への NetScaler VPX デプロイ」を参照してください。

サードパーティサポート:

NetScaler 環境での特定のサードパーティ(Nutanix AHV)の統合で問題が発生した場合は、サードパーティパー トナー(Nutanix)に直接サポートインシデントをオープンしてください。

パートナーが問題が NetScaler にあると判断した場合、パートナーは NetScaler サポートに連絡してさらにサポー トを受けることができます。問題が解決するまで、パートナーの専任技術者が NetScaler サポートチームと協力しま す。

汎用 **KVM** 上の **VPX** インスタンス

汎用 KVM バージョン	SysID	パフォーマンス範囲
RHEL 7.6、RHEL 8.0、RHEL 9.3	450070	10Mbps~100Gbps
Ubuntu 16.04、Ubuntu 18.04、		
Ubuntu 22.04		

注意事項:

KVM ハイパーバイザーを使用するときは、次の点を考慮してください。

- VPX インスタンスは、表 1-4 に記載されている Hypervisor リリースバージョンに対して認定されており、バ ージョン内のパッチリリースには適していません。ただし、VPX インスタンスは、サポートされているバージ ョンのパッチリリースとシームレスに動作することが期待されます。そうでない場合は、トラブルシューティ ングとデバッグのためのサポートケースを記録します。
- RHEL 7.6 を使用する前に、KVM ホストで以下のステップを完了します。
 - /etc/default/grubを編集して"kvm_intel.preemption_timer=0"をGRUB_CMDLINE_LINUX 変数に追加します。
 - 2. コマンド"# grub2-mkconfig -o /boot/grub2/grub.cfg"でgrub.cfgを再生成し ます。
 - 3. ホストマシンを再起動します。
- Ubuntu 18.04 を使用する前に、KVM ホストで以下のステップを完了してください。
 - /etc/default/grubを編集して"kvm_intel.preemption_timer=0"をGRUB_CMDLINE_LINUX 変数に追加します。
 - 2. コマンド"# grub-mkconfig -o /boot/grub/grub.cfg "で grub.cfg を再生成し ます。
 - 3. ホストマシンを再起動します。

パブリッククラウド上の **VPX** インスタンス

パブリッククラウド	SysID	パフォーマンス範囲
AWS	450040	10Mbps~30Gbps
Azure	450020	10 Mbps \sim 10 Gbps
GCP	450070	10 Mbps \sim 10 Gbps

ハイパーバイザーでサポートされる **VPX** 機能

ハイパーバイ	XenServer 上の VPX	VMware ESX 上の VPX
ザー→		

^^ 特徴	▲ 特徴									
\checkmark	~~		٨٨				٨٨	٨٨		
インタ −フェ イス →	PV	SR- IOV	PV	SR- IOV	エミュ レート	PCI パ ススル ー	PV	PV	SR- IOV	PCI パ ススル ー
マルチ PE サ ポート	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
クラス タリン グのサ ポート	Yes	はい ¹	Yes	はい ¹	Yes	Yes	Yes	Yes	はい 1	Yes
VLAN タグ付 け	Yes	Yes	Yes	Yes	Yes	Yes	はい (2012R2 のみ)	Yes	Yes	Yes
リンク イベン トの検 出 /HAM	いいえ 2 on	はい ³	いいえ 2	はい ³	いいえ 2	はい ³	いいえ 2	いいえ 2	はい ³	はい ³
インタ ーフェ ースパ ラメー 定	いいえ	いいえ	いいえ	いいえ	いいえ	Yes	いいえ	いいえ	いいえ	Yes
静的 LA	はい ²	はい ³	はい ²	いいえ	はい ²	はい ³	はい ²	はい ²	はい ³	はい ³
LACP	いいえ	はい ³	はい ²	いいえ	はい ²	はい ³	いいえ	はい ²	はい ³	はい ³
静的 CLAG	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

\checkmark	~~		٨٨				~~	~~		
LACP クラグ	いいえ	いいえ	はい ²	いいえ	はい ²	はい ³	いいえ	はい ²	はい ³	はい ³
ホット プラグ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

パブリッククラウドでサポートされる VPX 機能

パブリック クラウド →	AWS 上の VPX	Azure 上の VPX	GCP 上の VPX
	٨٨	٨٨	٨٨
マルチ PE サポート	Yes	Yes	Yes
クラスタリングのサポート	いいえ	いいえ	いいえ
VLAN タグ付け	いいえ	いいえ	いいえ
リンクイベントの検	いいえ 2	いいえ 2	いいえ ²
出/HAMon			
インターフェースパラメー タの設定	いいえ	いいえ	いいえ
静的 LA	いいえ	いいえ	いいえ
LACP	いいえ	いいえ	いいえ
静的 CLAG	いいえ	いいえ	いいえ
LACP クラグ	いいえ	いいえ	いいえ
ホットプラグ	Yes	いいえ	いいえ

前述の2つの表で使われている上付き文字(1、2、3)は、以下の点とそれぞれの番号を示しています:

- 1. SRIOV では、バックプレーンではなく、クライアント側およびサーバ側インターフェイス用のクラスタリング サポートを利用できます。
- 2. インターフェイスダウンイベントは NetScaler VPX インスタンスには記録されません。
- 3. スタティック LA の場合、物理ステータスが DOWN のインターフェイスでトラフィックが送信される場合も あります。

次の点は、前述の2つの表で取り込まれたそれぞれの機能に適用されます:

- LACP の場合、ピアデバイスは LACP タイムアウトメカニズムに基づいてインターフェイス DOWN イベント を認識します。
 - 短いタイムアウト:3秒
 - 長いタイムアウト: 90秒
- LACP では、VM 間でインターフェイスを共有しないでください。
- 動的ルーティングの場合、リンクイベントは検出されないため、コンバージェンス時間はルーティングプロト コルによって異なります。
- モニタ対象スタティックルート機能は、ルータの状態が VLAN ステータスに依存するため、モニタをスタティ ックルートにバインドしないと失敗します。VLAN ステータスは、リンクステータスによって異なります。
- リンク障害がある場合、高可用性では部分的な障害検出は行われません。リンク障害があると、高可用性の分割脳の状態が発生する可能性があります。
 - VPX インスタンスからリンクイベント (無効化、有効化、リセット) が生成されても、リンクの物理ステ ータスは変更されません。静的 LA の場合、ピアによって開始されたトラフィックはすべてインスタン スでドロップされます。
 - VMware ESX で VLAN タグ付け機能を動作させるには、VMware ESX サーバーの vSwitch でポート グループの VLAN ID を 1 ~4095 に設定します。
- ホットプラグは、ENA インターフェイスを備えた VPX インスタンスではサポートされていないため、ホット プラグを試みるとインスタンスの動作が予測できない場合があります。ホットアドは、AWS 上の NetScaler を使用する PV および SRIOV インターフェイスでのみサポートされます。
- AWS ウェブコンソールまたは AWS CLI インターフェイスを介したホット削除は、NetScaler の PV、SRIOV、 および ENA インターフェイスではサポートされていません。ホット削除を試みると、インスタンスの動作が 予測できなくなる可能性があります。

サポートされているブラウザー

NetScaler GUI バージョン 14.1 および 13.1 にアクセスするためにサポートされているブラウザについては、「互換 性のあるブラウザ」を参照してください。

NetScaler VPX でサポートされているプロセッサ

プラットフォーム	Intel プロセッサ	AMD プロセッサ
Citrix Hypervisor	Yes	いいえ

プラットフォーム	Intel プロセッサ	AMD プロセッサ
ESXi ハイパーバイザー	Yes	Yes
Hyper-V の	Yes	いいえ
KVMの	Yes	いいえ
AWS	Yes	Yes
Azure	Yes	Yes
GCP	Yes	Yes

NetScaler VPX でサポートされている NIC

次の表は、VPX プラットフォームまたはクラウドでサポートされている NIC の一覧です。

NIC →	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/) SRIOV VF	Intel KL7X1010/XL710/XXV710 PCI パススル ーモード
^^ プラット						
フォーム↓	~~	~~	٨٨	٨٨	~~	٨٨
Citrix Hypervisor	-	-	-	Yes	Yes	いいえ
ESXi ハイパ ーバイザー	いいえ	Yes	いいえ	Yes	いいえ	Yes
Hyper-V の	-	-	-	いいえ	いいえ	いいえ
KVM の	いいえ	Yes	Yes	Yes	Yes	いいえ
AWS	-	-	-	Yes	-	-
Azure	Yes	Yes	Yes	-	-	-
GCP	-	-	-	-	-	-

その他の参考文献

- Citrix Ready 製品については、Citrix Ready Marketplaceにアクセスしてください
- Citrix Ready 製品のサポートについては、Citrix Ready パートナー ページを参照してください。

• VMware ESX ハードウェアバージョンについては、VMware Tools のアップグレードを参照してください。

VMware ESX、Linux KVM、および **Citrix Hypervisor** で **NetScaler ADC VPX** のパフォーマンスを最適化する

April 1, 2025

NetScaler VPX のパフォーマンスは、ハイパーバイザー、割り当てられたシステムリソース、およびホスト構成に よって大きく異なります。To achieve the desired performance, first follow the recommendations in the VPX data sheet, and then further optimize it using the best practices provided in this document.

VMware ESX ハイパーバイザー上の NetScaler ADC VPX インスタンス

このセクションでは、構成可能なオプションと設定、および VMware ESX ハイパーバイザー上の NetScaler ADC VPX インスタンスの最適なパフォーマンスを実現するのに役立つその他の推奨事項について説明します。

- Recommended configuration on ESX hosts
- E1000 ネットワークインターフェイスを備えた NetScaler ADC VPX
- VMXNET3 ネットワークインターフェイスを備えた NetScaler ADC VPX
- SR-IOV および PCI パススルーネットワークインターフェイスを備えた NetScaler ADC VPX

Recommended configuration on ESX hosts

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

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

-Vmnic の NUMA アフィニティを見つけるには、ローカルまたはリモートでホストにログインし、次のよう に入力します。

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

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

E1000 ネットワークインターフェイスを備えた NetScaler ADC VPX

Perform the following settings on the VMware ESX host:

- On the VMware ESX host, create two vNICs from one pNIC vSwitch. 複数の vNIC は、ESX ホストに 複数の受信 (Rx) スレッドを作成します。This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX command:
 - For ESX version 5.5:

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

- For ESX version 6.0 onwards:

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

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

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

注

Make sure that you reboot the VMware ESX host to apply the updated settings.

Two vNICs per pNIC deployment

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



NetScaler VPX 構成例:

前のサンプルトポロジに示した展開を実現するには、NetScaler VPX インスタンスで次の構成を実行します。

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

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

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

1 bind vlan 3 -ifnum 1/2 - tagged
2 bind vlan 3 -IPAddress 2.2.2.2 255.255.25.0

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

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

Make sure that you include the following two entries in the route table:

- 1.1.1.0/24 subnet with gateway pointing to SNIP 1.1.1.2
- 2.2.2.0/24 subnet with gateway pointing to SNIP 2.2.2.2

VMXNET3 ネットワークインターフェイスを備えた NetScaler ADC VPX

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

- Create two vNICs from one pNIC vSwitch. 複数の vNIC により、ESX ホストに複数の Rx スレッドが作成されます。This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX commands:
 - For ESX version 5.5:

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

- For ESX version 6.0 onwards:

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

On the VMware ESX host, perform the following configuration:

- On the VMware ESX host, create two vNICs from 1 pNIC vSwitch. Multiple vNICs create multiple Tx and Rx threads in the ESX host. This increases the Tx and Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase Tx throughput of a vNIC, use a separate Tx completion thread and Rx threads per device (NIC) queue. 次のコマンドを使用します:

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

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

1 ethernetX.ctxPerDev = "1"

• 仮想マシンの構成に次の設定を追加して、vNIC あたり最大 8 つの送信スレッドを使用するように仮想マシン を構成します。

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

vNIC あたりの送信スレッド数を増やすと、ESX ホストでより多くの CPU リソース (最大 8 つ) が必要 になります。前述の設定を行う前に、十分な CPU リソースが使用可能であることを確認してください。

注

Make sure that you reboot the VMware ESX host to apply the updated settings.

You can configure VMXNET3 as a **Two vNICs per pNIC** deployment. 詳細については、「物理 NIC 展開ごと に 2 つの vNIC」を参照してください。

VMware ESX で VMXNET3 デバイス用のマルチキューと RSS サポートを設定します デフォルトでは、 VMXNET3 デバイスは 8 つの Rx キューと Tx キューのみをサポートします。VPX の vCPU の数が 8 を超えると、 VMXNET3 インターフェイスに設定されている Rx キューと Tx キューの数は、デフォルトで1に切り替わります。 ESX の特定の構成を変更することで、VMXNET3 デバイス用に最大 19 個の Rx キューと Tx キューを設定できます。 このオプションにより、パフォーマンスが向上し、VPX インスタンスの vCPU 間でパケットが均一に分散されま す。

注

NetScaler リリース 13.1 ビルド 48.x 以降、NetScaler VPX は VMXNET3 デバイスの ESX 上で最大 19 個の Rx キューと Tx キューをサポートします。

前提条件:

ESX で VMXNET3 デバイス用に最大 19 個の Rx キューと Tx キューを構成するには、次の前提条件が満たされてい ることを確認してください。

- NetScaler VPX バージョンは 13.1 ビルド 48.X 以降です。
- NetScaler VPX は、VMware ESX 7.0 以降でサポートされているハードウェアバージョン 17 以降の仮想マシンで構成されます。

8 つ以上の Rx キューと Tx キューをサポートするように VMXNET3 インターフェイスを設定します。

- 1. 仮想マシンの構成ファイル (.vmx) ファイルを開きます。
- ethernetX.maxTxQueuesおよびethernetX.maxRxQueuesの値を設定して Rx キューと TX キューの数を指定します(X は設定する仮想 NIC の数)。設定するキューの最大数は、仮想マシンの vCPU 数 を超えてはいけません。

キューの数を増やすと、ESX ホストのプロセッサオーバーヘッドも増加します。したがって、キューを 増やす前に、ESX ホストに十分な CPU リソースがあることを確認してください。キューの数がパフォ ーマンスのボトルネックになっている場合は、サポートされるキューの最大数を増やすことができます。 このような場合は、キューの数を徐々に増やすことをお勧めします。たとえば、8 から 12、次に 16 へ、 そして 20 へ、というようになります。最大値まで直接上げるのではなく、各設定でパフォーマンスを評 価してください。

SR-IOV および PCI パススルーネットワークインターフェイスを備えた NetScaler ADC VPX

SR-IOV および PCI パススルー ネットワーク インターフェイスを使用して NetScaler VPX の高パフォーマンスを実現するには、「ESX ホストでの推奨構成」を参照してください。

VMware ESXi ハイパーバイザーの使用ガイドライン

• NetScaler VPX インスタンスをサーバーのローカル ディスクまたは SAN ベースのストレージ ボリュームに 展開することをお勧めします。

『VMware vSphere 6.5 のパフォーマンスのベストプラクティス』ドキュメントの「VMware ESXi CPU に関する考慮事項」セクションを参照してください。ここに抽出があります:

- CPU またはメモリのデマンドが高い仮想マシンを、オーバーコミットされたホストまたはクラスタにデプロ イすることは推奨されません。
- ほとんどの環境では、ESXiは、仮想マシンのパフォーマンスに影響を与えることなく、かなりのレベルの CPUオーバーコミットメントを許可します。ホストでは、そのホスト内の物理プロセッサコアの総数よりも 多くの vCPUを実行できます。
- ESXi ホストが CPU 飽和状態になった場合、つまり、仮想マシンおよびホスト上のその他の負荷がホストにあるすべての CPU リソースを要求すると、レイテンシの影響を受けやすいワークロードがうまく動作しない可能性があります。この場合、たとえば、一部の仮想マシンをパワーオフするか、別のホストに移行する(または DRS に自動的に移行させる)ことで、CPU 負荷を軽減します。
- NetScaler では、仮想マシンで ESXi ハイパーバイザーの最新の機能セットを利用するには、最新のハードウェア互換性バージョンを使用することをお勧めします。ハードウェアと ESXi のバージョンの互換性に関する 詳細については、VMwareのドキュメントを参照してください。
- NetScaler VPX は、レイテンシーに敏感で高性能な仮想アプライアンスです。期待どおりのパフォーマンス を実現するには、アプライアンスに vCPU の予約、メモリの予約、および vCPU のホストへのピンニングが 必要です。また、ホスト上でハイパースレッディングを無効にする必要があります。ホストがこれらの要件を 満たしていない場合、次の問題が発生する可能性があります:
 - 高可用性フェイルオーバー

- VPX インスタンス内の CPU スパイク
- VPX CLI へのアクセスが遅い
- ピットボスデーモンクラッシュ
- パケットドロップ
- 低スループット
- Hypervisor は、次の 2 つの条件のいずれかが満たされると、過剰プロビジョニングと見なされます:
 - ホストにプロビジョニングされた仮想コア (vCPU) の総数が、物理コア (pCPU) の総数を超えています。
 - プロビジョニングされた仮想マシンの合計数は、pCPU の合計数よりも多くの vCPU を消費します。

インスタンスが過剰プロビジョニングされている場合、ハイパーバイザーのスケジューリングオーバー ヘッド、バグ、またはハイパーバイザーの制限により、ハイパーバイザーがインスタンスのリザーブド リソース(CPU、メモリなど)を保証しない場合があります。この動作により、NetScaler の CPU リ ソースが不足し、「使用上のガイドライン」の最初のポイントで説明した問題が発生する可能性がありま す。管理者は、ホストにプロビジョニングされた vCPU の総数が PCU の総数以下になるように、ホス トのテナンシーを減らすことをお勧めします。

例

ESX ハイパーバイザーの場合、esxtopコマンド出力で VPX vCPU の%RDY%パラメーターが 0 より 大きい場合、ESX ホストにはスケジューリングオーバーヘッドがあると言われ、VPX インスタンスにレ イテンシー関連の問題が発生する可能性があります。

このような状況では、%RDY%が常に0に戻るように、ホストのテナンシーを減らします。または、ハイ パーバイザーベンダーに連絡して、リソース予約が受け付けられない理由を優先順位付けしてください。

パケットエンジンの **CPU** 使用率を制御するコマンド

ハイパーバイザーおよびクラウド環境における VPX インスタンスのパケットエンジン(非管理)CPU 使用率の動作 を制御するには、2 つのコマンド(set ns vpxparamおよびshow ns vpxparam)を使用できます:

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

各 VM が、別の VM に割り当てられているが、使用されていない CPU リソースを使用できるようにします。

Set ns vpxparam $N \ni X - \varphi$:

-cpuyield: 割り当てられているが未使用の CPU リソースを解放または解放しません。

- はい: 割り当てられているが未使用の CPU リソースを別の VM で使用できるようにします。
- いいえ:割り当てられた VM のすべての CPU リソースを予約します。このオプションは、ハイパーバイ ザーおよびクラウド環境で VPX CPU 使用率が高いことを示します。
- デフォルト: いいえ。

```
注
```

すべての NetScaler VPX プラットフォームで、ホストシステム上の vCPU 使用率は 100% です。 set ns vpxparam -cpuyield YES コマンドを使用してこの使用方法を無効にしてください。

クラスタノードを「yield」に設定する場合は、CCO で次の追加設定を実行する必要があります:

- クラスターが形成されると、すべてのノードが「yield=DEFAULT」に設定されます。
- すでに「yield=Yes」に設定されたノードを使用してクラスターが形成されている場合、ノードは「DEFAULT」のイールドを使用してクラスターに追加されます。

注

クラスタノードを「yield=YES」に設定する場合は、クラスタの形成後にのみ構成でき、クラスタが形成される前には設定できません。

-**masterclockcpu1**: メインクロックソースを CPU0 (管理 CPU) から CPU1 に移動できます。このパラメ ータには、次のオプションがあります。

- はい: 仮想マシンがメインクロックソースを CPU0 から CPU1 に移動できるようにします。
- いいえ:VM はメインクロックソースに CPU0 を使用します。デフォルトでは、CPU0 がメインクロック ソースです。
- show ns vpxparam

このコマンドは、現在のvpxparam設定を表示します。

Linux-KVM プラットフォーム上の NetScaler ADC VPX インスタンス

このセクションでは、構成可能なオプションと設定、および Linux-KVM プラットフォーム上の NetScaler ADC VPX インスタンスの最適なパフォーマンスを達成するのに役立つその他の推奨事項について説明します。

- KVM のパフォーマンス設定
- PV ネットワークインターフェイスを備えた NetScaler ADC VPX
- SR-IOV およびフォートビルの PCIe パススルーネットワークインターフェイスを備えた NetScaler ADC VPX

KVM のパフォーマンス設定

KVM ホストで次の設定を行います。

lstopoコマンドを使用して、NIC の NUMA ドメインを検索します。

Make sure that memory for the VPX and the CPU is pinned to the same location. VPX と CPU のメモリ が同じ場所に固定されていることを確認します。次の出力では、10G NIC「ens2」は NUMA ドメイン #1 に関連付 けられています。

[root@localhost ~]# lstopo-no-graphics Machine (128GB) NUMANode L#0 (P#0 64GB) Socket L#0 + L3 L#0 (20MB) L2 L#0 (256KB) + L1d L#0 (32KB) + L11 L#0 (32KB) + Core L#0 + PU L#0 (P#0) L2 L#1 (256KB) + L1d L#1 (32KB) + L11 L#1 (32KB) + Core L#2 + PU L#1 (P#1) L2 L#3 (256KB) + L1d L#3 (32KB) + L11 L#1 (32KB) + Core L#2 + PU L#2 (P#2) L2 L#3 (256KB) + L1d L#3 (32KB) + L11 L#3 (32KB) + Core L#3 + PU L#2 (P#2) L2 L#3 (256KB) + L1d L#3 (32KB) + L11 L#4 (32KB) + Core L#3 + PU L#3 (P#3) L2 L#4 (256KB) + L1d L#4 (32KB) + L11 L#4 (32KB) + Core L#5 + PU L#3 (P#3) L2 L#6 (256KB) + L1d L#6 (32KB) + L11 L#6 (32KB) + Core L#5 + PU L#5 (P#5) L2 L#6 (256KB) + L1d L#7 (32KB) + L11 L#7 (32KB) + Core L#7 + PU L#7 (P#7) HostEridge L#0 HostBridge L#0 lostBridge L#0 PCIBridge PCI 8086:1521 Net L#0 "enol" PCI 8086:1521 Net L#1 "eno2" PCIBridge PCI 8086:1584 Net L#2 "ens3" PCIBridge Net L#2 "ens3 PCIBridge PCI 8086:1584 Net L#3 "ens4 PCI 8086:8d62 Block L#4 "sda" Block L#5 "sdb" PCIBridge "ens4" PCIBridge PCIBridge PCI 1a03:2000 GPU L#6 "card0" GPU L#7 "controlD64" NUMANode L#1 (P#1 64GB) MANOGE (#1 (##1 0408) 12 L#8 (256KB) + L1d L#8 (32KB) + L11 L#8 (32KB) + Core L#8 + PU L#8 (P#8) 12 L#8 (256KB) + L1d L#9 (32KB) + L11 L#9 (32KB) + Core L#0 + PU L#9 (P#9) 12 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#10 (P#11) L2 L#11 (256KB) + L1d L#11 (32KB) + L11 L#12 (32KB) + Core L#12 + PU L#12 (P#12) L2 L#13 (256KB) + L1d L#13 (32KB) + L11 L#12 (32KB) + Core L#12 + PU L#12 (P#12) L2 L#13 (256KB) + L1d L#13 (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#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) HostBridde L#6 HostBridge L#6 CIBrida PCI 8086:1584 PCI 8086:1584 Net L#8 "ens2" CIBridge PCI 8086:10fb Net L#9 "ens1f0" PCI 8086:10fb Net L#10 "enslfl PCI ffff:fff Net L#11 "enp131s16" [root@localhost ~]# modprobe kvm-intel acpienv=N

NUMA ドメインから VPX メモリを割り当てます。

numactlコマンドは、メモリの割り当て元の NUMA ドメインを示します。次の出力では、NUMA ノード #0 から 約 10 GB の RAM が割り当てられています。



NUMA ノードマッピングを変更するには、次の手順に従います。

1. ホスト上の VPX の.xml を編集します。

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

2. 次のタグを追加します。

- 3. VPX をシャットダウンします。
- 4. 次のコマンドを実行します:

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

このコマンドは、NUMA ノードマッピングを使用して VM の構成情報を更新します。

5. VPX の電源をオンにします。次に、ホスト上のnumactl –hardwareコマンド出力を確認して、VPX の 更新されたメモリ割り当てを確認します。

[root	:@1	Loca	alho	ost	c ^	-]:	# 1	nur	nac	:t]	L -	ha	ardı	var	e
avail	Lak	ole	: 2	nc	ode	23	()	0-1	L)						
node	0	cpu	18:	0	1	2	3	4	5	6	7				
node	0	si	ze:	65	542	29	MI	3							
node	0	fre	ee:	65	542	29	MI	3							
node	1	cpu	13:	8	9	1	0 1	11	12	1	13	14	15		
node	1	siz	ze:	65	553	36	MI	3							
node	1	fre	ee:	55	585	54	MI	3							
node	di	ista	ance	28											
node		0	1												
0:	1	0	21												
1:	2	21	10												
[root	:@1	Loca	alho	ost	5 1	-]:	ŧ.								

VPX の vCPU を物理コアにピン留めします。

• VPX の vCPU から pCPU へのマッピングを表示するには、次のコマンドを入力します。

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

vCPU0~4は物理コア8~11にマッピングされます。

• 現在の pCPU 使用率を表示するには、次のコマンドを入力します。

1	m	pstat	с -РА	LL 5								
x005910	aslb	oot oo	mul#_mo.	arat D 7								
inux 3.1	10.0	-123.e	17.x86_(64 (local	host.lo	ocaldomain)	05	5/17/201	6 _	x86_64_		16 CPU)
2:26:20	PM	CPU	\$usr	\$nice	%sys	<pre>%iowait</pre>	%irg	%soft	<pre>%steal</pre>	%guest	%gnice	<pre>%idle</pre>
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
1:26:25	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
:26:25	PM		0.00	0.00	0,20	0.00	0.00	0.00	0.00	0.00	0.00	99.80
:26:25	PM	4	0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.60
:26:25	PM		0.60	0.00	0.20	0.00	0.00	0.00	0.00	0.00	0.00	99.20
: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	96.96
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	\mathbf{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	100.00
2:26:25	PM	14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00
2:26:25	PM	15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00

この出力では、8 は管理 CPU、9~11 はパケットエンジンです。

- vCPU を pCPU 固定に変更するには、2 つのオプションがあります。
 - 次のコマンドを使用して、VPX の起動後に実行時に変更します。

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

- VPX に静的な変更を加えるには、前と同じように次のタグを付けて・xmlファイルを編集します。
 - 1. ホスト上の VPX の.xml ファイルを編集します。

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

2. 次のタグを追加します。

- 3. VPX をシャットダウンします。
- 4. 次のコマンドを使用して、NUMA ノードマッピングを使用して VM の設定情報を更新します。

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

5. VPXの電源をオンにします。次に、ホスト上のvirsh vcpupin <VPX name>コ マンド出力をチェックして、更新された CPU ピン接続を確認します。

ホスト割り込みオーバーヘッドを排除します。

• kvm_statコマンドを使用して VM_EXITS を検出します。

ハイパーバイザーレベルでは、ホスト割り込みは、VPX の仮想 CPU が固定されているのと同じ pCPU にマッ ピングされます。これにより、VPX 上の vCPU が定期的に追い出される可能性があります。

ホストを実行している仮想マシンによって実行された VM の終了を確認するには、kvm_statコマンドを使用します。

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

1+M の順の値が大きいほど、問題があることを示します。

単一の VM が存在する場合、予想される値は 30~100 K です。それ以上の場合は、同じ pCPU にマップされ たホスト割り込みベクターが 1 つ以上あることを示している可能性があります。

• ホスト割り込みを検出し、ホスト割り込みを移行します。

「/proc/interrupts」ファイルのconcatenateコマンドを実行すると、すべてのホスト割り込みマッピン グが表示されます。1 つ以上のアクティブな IRQ が同じ pCPU にマップされている場合、対応するカウンタ が増分します。

NetScaler VPX の pCPU と重複する割り込みを未使用の pCPU に移動します。

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

• IRQ バランスを無効にします。

IRQ バランスデーモンを無効にして、その場で再スケジュールが実行されないようにします。

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

必ずkvm_statコマンドを実行して、カウンタの数が多くないことを確認します。

PV ネットワークインターフェイスを備えた NetScaler ADC VPX

準仮想化(PV)、SR-IOV、および PCIe パススルーネットワークインターフェイスは、物理 NIC ごとに **2** つの **vNIC** 展開として設定できます。詳細については、「物理 NIC 展開ごとに 2 つの vNIC」を参照してください。

PV (virtio) インターフェイスの最適なパフォーマンスを得るには、次の手順に従います。

- PCIe スロット/NIC が属する NUMA ドメインを特定します。
- VPX のメモリと vCPU は、同じ NUMA ドメインにピン接続する必要があります。
- 仮想ホストスレッドは、同じ NUMA ドメイン内の CPU にバインドする必要があります。

仮想ホストスレッドを対応する CPU にバインドします。

1. トラフィックが開始されたら、ホストでtopコマンドを実行します。

MTPuTTY (Multi-Tabbed PuTTY)		- 0 ×
Server View Tools Help		
🔙 🖴 😵 - 📰 🛄		
g / Start page X root@localhost:~ X root@localhost:~ X root@	@ubuntu: ~ X / root@localhost:~ X / root@ubuntu: ~ X	-
top - 14:48:08 up 6 days, 17 min, 4 user	rs, load average: 1.46, 0.42, 0.65	^
Tasks: 486 total, 3 running, 483 sleepi	ing, 0 stopped, 0 zombie	
%Cpu(s): 4.1 us, 5.1 sy, 0.0 ni, 89.2	id, 0.0 wa, 0.0 hi, 1.7 si, 0.0 st	
KiB Mem: 13175540+total, 6496624 used,	12525878 free, 884 buffers	
KIB Swap: 4194300 total, 0 used,	4194300 Iree. 2086468 Cachea Mem	
PID USER PR NI VIRT RES	SHR S &CPU &MEM TIME+ COMMAND	P
29824 gemu 20 0 12.786g 742864 8	8040 S 139.2 0.6 8789:04 gemu-kym	11
29838 root 20 0 0 0	0 R 100.0 0.0 5659:06 vhost-29824	8
29837 root 20 0 0 0	0 R 99.7 0.0 5659:25 vhost-29824	1
3063 root 20 0 1073944 23992 9	9396 s 1.7 0.0 111:58.18 libvirtd	0
1070 root 39 19 0 0	0 S 1.0 0.0 91:35.98 kipmi0	14
27439 test 20 0 2710032 1.159g 25	5868 S 0.7 0.9 45:35.56 virt-manager	7
16500 root 20 0 0 0	U S 0.3 0.0 0116.96 KWorker/2510	25
2 root 20 0 0 0	0.9 0.0 0.0 0.0 0.13.69 Systemu	13
3 root 20 0 0 0	0 S 0.0 0.0 384-17 42 Kenft rad/0	0
5 root 0 -20 0 0	0 S 0.0 0.0 0:00.00 kworker/0:0H	Ő
6 root 20 0 0 0	0 S 0.0 0.0 0:00.00 kworker/u64:0	18
8 root rt 0 0 0	0 S 0.0 0.0 0:03.02 migration/0	0
9 root 20 0 0 0	0 s 0.0 0.0 0:00.00 rcu_bh	2
10 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/0	0
11 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/1	0
12 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcub/2	0
13 FOOT 20 0 0 0		0
15 root 20 0 0 0		ő
16 root 20 0 0 0	0 \$ 0.0 0.0 0:00.00 rcuob/6	ŏ
17 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/7	0
18 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/8	9
19 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/9	0
20 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/10	0
21 root 20 0 0 0	0 S 0.0 0.0 0:00.00 rcuob/11	0
22 root 20 0 0 0	0 S 0.0 0.0 0:00.00 FCtop/12	0
		ENG 14:48
I'm Cortana. Ask me anything.		IN 11-07-2016

- 2. 仮想ホストプロセス (vhost-<pid-of-qemu>という名前) アフィニティを識別します。
- 3. 次のコマンドを使用して、前に特定した NUMA ドメインの物理コアに vHost プロセスをバインドします。

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

例

- 1 taskset pc 12 29838
- 4. NUMA ドメインに対応するプロセッサコアは、次のコマンドで識別できます。

1	root@localhost ~]# virsh capabilities grep cpu
2	<pre>Ccpu></pre>
3	
4	<cpus num="8"></cpus>
5	<cpu core_id="0" id="0" siblings="0" socket_id="0"></cpu>
6	<cpu core_id="1" id="1" siblings="1" socket_id="0"></cpu>
7	<cpu core_id="2" id="2" siblings="2" socket_id="0"></cpu>
8	<cpu core_id="3" id="3" siblings="3" socket_id="0"></cpu>
9	<cpu core_id="4" id="4" siblings="4" socket_id="0"></cpu>
10	<cpu core_id="5" id="5" siblings="5" socket_id="0"></cpu>
11	<cpu core_id="6" id="6" siblings="6" socket_id="0"></cpu>
12	<cpu core_id="7" id="7" siblings="7" socket_id="0"></cpu>
13	

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

QEMU プロセスを対応する物理コアにバインドします。

- 1. QEMU プロセスが実行されている物理コアを特定します。詳細については、前述の出力を参照してください。
- 2. 次のコマンドを使用して、vCPU をバインドするのと同じ物理コアに QEMU プロセスをバインドします。

1 taskset - pc 8-11 29824

SR-IOV およびフォートビルの PCIe パススルーネットワークインターフェイスを備えた NetScaler ADC VPX

SR-IOV および Fortville PCIe パススルーネットワークインターフェイスのパフォーマンスを最適化するには、次の 手順を実行します。

- PCle スロット/NIC が属する NUMA ドメインを特定します。
- NetScaler VPX のメモリと vCPU は、同じ NUMA ドメインに固定する必要があります。

Linux KVM の vCPU およびメモリピンニング用のサンプル VPX XML ファイル:

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

18 19 </domain>

Citrix Hypervisor 上の NetScaler ADC VPX インスタンス

このセクションでは、構成可能なオプションと設定、および Citrix Hypervisors 上の NetScaler ADC VPX インス タンスの最適なパフォーマンスを達成するのに役立つその他の推奨事項について説明します。

- Citrix Hypervisor のパフォーマンス設定
- SR-IOV ネットワークインターフェイスを備えた NetScaler ADC VPX
- 準仮想化インターフェイスを備えた NetScaler ADC VPX

Citrix Hypervisor のパフォーマンス設定

「xl」コマンドを使用して NIC の NUMA ドメインを見つけます。

1 xl info -n

VPX の vCPU を物理コアにピン留めします。

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

vCPUのバインドをチェックします。

1 xl vcpu-list

8 個を超える仮想 CPU を NetScaler ADC 仮想マシンに割り当てます。

8個を超える仮想 CPU を構成するには、Citrix Hypervisor コンソールから次のコマンドを実行します。

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

SR-IOV ネットワークインターフェイスを備えた NetScaler ADC VPX

SR-IOV ネットワークインターフェイスの最適なパフォーマンスを得るには、次の手順を実行します。

- PCle スロットまたは NIC が接続されている NUMA ドメインを特定します。
- VPX のメモリと vCPU を同じ NUMA ドメインに固定します。
- ドメイン 0 vCPU を残りの CPU にバインドします。
準仮想化インターフェイスを備えた NetScaler ADC VPX

最適なパフォーマンスを得るには、他の PV 環境と同様に、pNIC ごとに 2 つの vNIC、および pNIC 構成ごとに 1 つの vNIC を推奨します。

準仮想化 (netfront) インターフェイスの最適なパフォーマンスを実現するには、次の手順を実行します。

- PCle スロットまたは NIC が属する NUMA ドメインを特定します。
- VPX のメモリと vCPU を同じ NUMA ドメインに固定します。
- ドメイン 0 vCPU を同じ NUMA ドメインの残りの CPU にバインドします。
- 仮想 NIC のホスト Rx/Tx スレッドをドメイン 0 vCPU に固定します。

ホストスレッドをドメイン **0 vCPU** にピン留めします。

- 1. Citrix Hypervisor ホスト シェルで xl list コマンドを使用して、NetScaler VPX の Xen-ID を見つけ ます。
- 2. 次のコマンドを使用して、ホストスレッドを識別します。

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

次の例では、これらの値は次のことを示しています。

- vif5.0 -XenCenter で VPX に割り当てられた最初のインターフェイス(管理インターフェイス)のスレッド。
- vif5.1 -VPX に割り当てられた2番目のインターフェースのスレッドなど。

[root@	xenserv	er-uuf	fyqlx ~]	# xl lis	t					
Name						ID	Mem	VCPUs	State	Time(s)
Domain	n-0				_	0	4092	8	r	633321.0
Sai VE	2X					5	8192	4	r	1529471.0
[root@	xenserv	er-uuf	fyqlx ~]	#	L					
[root@	xenserv	er-uuf	fyqlx ~]	#						
[root@	xenserv	er-uuf	fyqlx ~]	# ps -ax	grep	"vif	5"			
Warnin	ng: bad	syntax,	, perhap	os a bogu	s '-'?	See /	usr/sł	nare/doc	/procps-3.	2.7/FAQ
20447	pts/6	S+	0:00	grep vif	5					
29187	?	S	1:09	[vif5.0-	guest-r	x]				
29188	?	S	0:00	[vif5.0-	dealloc]				
29189	?	S	201:33	[vif5.1-	guest-r	x]				
29190	?	S	80:51	[vif5.1-	dealloc]				
29191	?	S	0:20	[vif5.2-	guest-r	x]				
29192	?	S	0:00	[vif5.2-	dealloc]				
[root@	xenserv	er-uuf:	fyqlx ~]	#						

3. 次のコマンドを使用して、スレッドをドメイン 0 vCPU に固定します。

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

例

1 taskset -pc 1 29189

NetScaler VPX のディスク容量を増やすためのサポート

March 20, 2025

NetScaler VPX は、20 GB のデフォルトのディスク容量をサポートしています。さまざまな理由でディスクサイズ の制約が発生した場合は、次のオプションを使用して VPX のディスク容量を増やすことができます:

- プライマリディスクサイズを手動で増やす
- プライマリディスクサイズを動的に増やす
- •2台目のディスクを追加

注

NetScaler VPX ディスク容量を増やす機能は、VPX オンプレミスと VPX クラウド展開の両方で利用できます。 SDX 管理サービスを使用した NetScaler VPX プライマリ ディスクのサイズ変更はサポートされていません。

NetScaler VPX プライマリディスクサイズを手動で増やしてください

ハイパーバイザーまたはクラウド プラットフォームを使用して VPX プライマリ ディスクのサイズを手動で増やすに は、次の手順に従います。

- 1. VM をシャットダウンします。
- 2. デフォルトのディスク サイズを 20 GB から 30 GB や 40 GB などのより高い値に拡張します。Azure の場合、 デフォルトのディスク サイズを 32 GB から 64 GB に拡張します。
- 3. VM の電源を入れ、ブートプロンプトを入力します。
- 4. boot -s コマンドを使用してシングル ユーザー モードにログインします。
- 5. ディスク容量を確認してください。gpart show コマンドを使用して、新しく割り当てられたディスク領 域を確認できます。
- 6. パーティション名を書き留めておきます。次の例では、VM パーティションは da0 です。
- 7. gpart resize コマンドを使用してディスク パーティションのサイズを変更します。

例:次のコマンドを実行して、da0 MBR パーティションのサイズを変更し、10 GB の空き領域を含めます。 gpart resize -i 1 da0

8. 空き領域を最後のパーティションにマージします。

例 gpart resize -i 5 da0s1 growfs コマンドを使用して、新しく割り当てられた空き領域を含むようにファイルシステムを拡張します。
 例

growfs /dev/da0s1e

10. VM を再起動し、シェル プロンプトで df -h コマンドを使用して、増加したディスク領域を確認します。

NetScaler VPX プライマリディスクサイズを動的に増やす

管理者は、NetScaler VPX のプライマリ ディスク サイズを一度に 20 GB から最大1 TB まで動的に増やすことがで きます。その後の増加ごとに、最大1 TB まで再度拡張できます。プライマリ ディスクのサイズを増やすたびに、必 ず VM をシャットダウンしてください。これにより、システムは新しいディスク サイズを適切に認識し、パーティシ ョン テーブルを更新し、システムの安定性を維持できます。ディスク容量を増やすには、それぞれのクラウドまたは ハイパーバイザー UI でプライマリ ディスクのサイズを少なくとも1 GB 拡張します。

注

ディスクのサイズを増やすことしかできません。新しいサイズを割り当てると、後でサイズを減らすことはで きません。そのため、必要な場合にのみディスクサイズを増やしてください。

2 台目のディスクを追加

セカンダリ ディスクを追加することで、NetScaler VPX インスタンスのディスク容量を増やすことができます。セ カンダリ ディスクを接続すると、/var/crash ディレクトリがこのディスクに自動的にマウントされます。セカ ンダリ ディスクは、コア ファイルとログを保存するために使用されます。コア ファイルとログ ファイル用の既存の ディレクトリは、これまでどおり機能し続けます。

注

データの損失を避けるために、NetScaler アプライアンスをダウングレードする前に外部バックアップを作成 してください。

クラウド上の NetScaler VPX インスタンスに新しいハードディスクドライブ(HDD)を接続する方法については、 以下を参照してください。

• Azure ドキュメンテーション

注

Azure にデプロイされた VPX インスタンスにセカンダリディスクを接続するには、Azure VM のサイズ にローカルの一時ディスクがあることを確認してください。詳細については、「ローカル一時ディスクな しの Azure VM サイズ」を参照してください。

- AWS ドキュメント
- GCP ドキュメント

警告:

VPX に HDD を追加した後、新しい HDD に移動されたファイルに対して機能する一部のスクリプトが、次の条件下で失敗する可能性があります。

• link シェル コマンドを使用して、新しい HDD に移動されたファイルへのハード リンクを作成します。

シンボリック リンクを使用するには、このようなコマンドをすべて ln -s に置き換えます。また、失敗した スクリプトもそれに応じて更新します。

NetScaler VPX 構成をクラウドで NetScaler アプライアンスの最初の起動時に適用 する

October 17, 2024

NetScaler VPX 構成は、クラウド環境での NetScaler アプライアンスの最初の起動時に適用できます。このステージは、このドキュメントでプレブートステージとして取り上げられています。したがって、ADC プールライセンスなどの特定のケースでは、特定の VPX インスタンスがはるかに短時間で起動されます。この機能は、Microsoft Azure、 Google Cloud Platform、および AWS クラウドで使用できます。

ユーザーデータとは何ですか

クラウド環境で VPX インスタンスをプロビジョニングする場合、ユーザーデータをインスタンスに渡すオプションが あります。ユーザーデータを使用すると、一般的な自動設定タスクの実行、インスタンスの起動動作のカスタマイズ、 インスタンスの起動後にスクリプトを実行できます。最初の起動時に、NetScaler VPX インスタンスは次のタスクを 実行します。

- ユーザーデータを読み取ります。
- ユーザーデータで提供される構成を解釈します。
- 新しく追加された構成をブート時に適用します。

クラウドインスタンスでプレブートユーザーデータを提供する方法

プレブートユーザーデータを XML 形式でクラウドインスタンスに提供できます。クラウドによって、ユーザーデー タを提供するためのインターフェースが異なります。

AWS コンソールを使用してプレブートユーザーデータを提供する

AWS コンソールを使用して NetScaler VPX インスタンスをプロビジョニングする場合は、[インスタンスの詳細の 構成] > [詳細の詳細] に移動し、[ユーザーデータ] フィールドにプレブートユーザーデータ構成を指定します。

各手順の詳細な手順については、「AWS Web コンソールを使用して AWS に NetScaler VPX インスタンスをデプロ イする」を参照してください。詳細については、AWS ドキュメントの「インスタンスの起動」を参照してください。

aws Services	Reso	urce 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: Configure Ins	tance l	Details
Domain join direc	tory (j)	No directory C Create new directory
IAM	role (j)	None Create new IAM role
Shutdown beha	vior (j)	Stop 🔮
Stop - Hibernate beha	vior (j)	Enable hibernation as an additional stop behavior
Enable termination protec	tion (j)	Protect against accidental termination
Monito	ring (i)	Enable CloudWatch detailed monitoring Additional charges apply.
Tena	ancy (j)	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
Credit specifica	tion (j)	Unlimited Additional charges may apply
File syst	ems (j)	Add file system C Create new file system
 Advanced Details 		
Metadata access	sible (j	Enabled 4
Metadata ver	sion (j)	V1 and V2 (token optional)
Metadata token res <mark>ponse hop l</mark>	limit 👔	1
User	data 🕧	
		(Optional)
÷		

汪

プリブートユーザーデータ機能の AWS IMDSv2 専用モードは、NetScaler VPX リリース 13.1.48.x 以降のリ リースでサポートされています。

AWS CLI を使用してプレブートユーザーデータを提供する

AWS CLI で次のコマンドを入力します。

```
1 aws ec2 run-instances \
2 --image-id ami-0abcdef1234567890 \
3 --instance-type t2.micro \
```

```
4 --count 1 \
5 --subnet-id subnet-08fc749671b2d077c \
6 --key-name MyKeyPair \
7 --security-group-ids sg-0b0384b66d7d692f9 \
8 --user-data file://my_script.txt
```

詳細については、インスタンスの実行に関するAWS ドキュメントを参照してください。

詳細については、インスタンスユーザーデータの使用に関するAWS ドキュメントを参照してください。

Azure コンソールを使用してプリブートユーザーデータを提供する

Azure コンソールを使用して NetScaler VPX インスタンスをプロビジョニングする場合は、[仮想マシンの作成] > [詳細設定] タブに移動します。[カスタムデータ] フィールドに、プリブートユーザーデータの構成を指定します。

Home > 1	list. al	machines	
nome /	virtuai	machines	/

Create a virtual machine

Basics	Disks	Networking	Management	Advanced	Tags	Review + create			
Add add	Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.								
Extensio	Extensions								
Extensions provide post-deployment configuration and automation.									
Extensio	Extensions ① Select an extension to install								
Custom	data								
Pass a sc the VM i	ript, config n a known	guration file, or of location. Learn n	her data into the vinore about custom	irtual machine v data for VMs o	vhile it is	being provisioned. The data will be	saved on		
Custom	data								
() c	ustom data	on the selected in	age will be processe	ed by cloud-init.	Learn mor	e about custom data and cloud init 🗗			
Host									
Azure De Azure su choose V of the ho	Host Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more								
Host gro	up 🕕		No host g	group found			\sim		

Azure CLI を使用してプリブートユーザーデータを提供する

Azure CLI で次のコマンドを入力します。

1 az vm create \

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

例

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

カスタムデータまたはプリブート設定をファイルとして「―custom-data」パラメータに渡すことができます。この 例では、ファイル名は **MyCloudInitScript.txt** です。

詳細については、Azure CLI のドキュメントを参照してください。

GCP コンソールを使用してプレブートユーザーデータを提供する

GCP コンソールを使用して NetScaler VPX インスタンスをプロビジョニングする場合は、インスタンスのプロパテ ィを入力します。管理、セキュリティ、ディスク、ネットワーキング、単独テナンシを展開します。[管理] タブに移 動します。[自動化] セクションで、[スタートアップスクリプト] フィールドにプリブートユーザーデータ設定を指定 します。

GCP を使用して VPX インスタンスを作成する方法の詳細については、「Google Cloud Platform に NetScaler VPX インスタンスをデプロイする」を参照してください。

	Security	Disks	Networking	Sole Tenancy
Description (Opt	tional)			
				1
Deletion protect Enable dele When deleti	ion etion protection on protection is	on s enabled, i	nstance cannot be	e deleted. Learn more
Reservations Use an existing (reservation wh	en creating	this VM instance	
Automatically	use created	reservatio	n	-
Automation				
Startup script (0)ptional)			
Startup script (C You can choose restarts. Startup services are run	Optional) to specify a st scripts can be ning within the	artup scrip used to in virtual mae	t that will run whe stall software and chine. Learn more	n your instance boots up or updates, and to ensure that
Startup script (C You can choose restarts. Startup services are run	Optional) to specify a st o scripts can be ning within the	artup scrip used to in virtual mae	t that will run whe stall software and chine. Learn more	n your instance boots up or updates, and to ensure that
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 o scripts can be ning within the onal) tom metadata is useful for pa our code on the	artup scrip e used to in virtual mar for an insta ssing in art instance. I	t that will run whe stall software and chine. Learn more ance or project out jitrary 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
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	optional) to specify a st o scripts can be ning within the onal) tom metadata is useful for pa our code on the	artup scrip used to in virtual mar for an insta ssing in art instance. I /alue	t that will run whe stall software and chine. Learn more ance or project out pitrary values to yo Learn more	n your instance boots up or updates, and to ensure that tside of the server-defined pur project or instance that can

gcloud CLI を使用してプレブートユーザーデータを提供する

GCP CLI で次のコマンドを入力します。

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

metadata-from-file -に格納されているファイルから値またはユーザーデータを読み取ります。.

詳細については、gcloud CLI ドキュメントを参照してください。

プレブートユーザーデータ形式

プレブートユーザーデータは XML 形式でクラウドインスタンスに提供する必要があります。起動時にクラウドイン フラストラクチャを介して提供される NetScaler プレブートユーザーデータは、次の 4 つのセクションで構成され ます。

- NetScaler 構成は<NS-CONFIG>タグで表されます。
- ・ <NS-BOOTSTRAP>タグで表される NetScaler をカスタムブートストラップします。

- <NS-SCRIPTS>タグで表される NetScaler にユーザースクリプトを保存する。
- <NS-LICENSE-CONFIG>タグで表されるプールライセンス構成。

前の 4 つのセクションは、ADC のプレブート構成内で任意の順序で提供できます。プリブートユーザーデータを提供 しながら、次のセクションに示す書式に厳密に従うようにしてください。プリブート ユーザー データを提供する際 は、次のセクションに示すフォーマットに厳密に従ってください。

注

次の例に示すように、プレブートユーザーデータ構成全体を**<NS-PRE-BOOT-CONFIG>**タグで 囲む必要があります。

例1:

1	<ns-pre-boot-config></ns-pre-boot-config>	
2	<ns-config></ns-config>	
3	<ns-bootstrap></ns-bootstrap>	
4	<ns-scripts></ns-scripts>	
5	<ns-license-config></ns-license-config>	
6		

例 **2**:

1	<ns-pre-boot-config></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-CONFIG>タグを使用して、プレブート段階で VPX インスタンスに適用する必要がある特定の NetScaler VPX 構成を指定します。

注

<NS-CONFIG>セクションには、有効な ADC CLI コマンドが必要です。CLI は、構文エラーまた は形式について検証されません。

NetScaler 構成

<NS-CONFIG>タグを使用して、プレブート段階で VPX インスタンスに適用する必要がある特定の NetScaler VPX 構成を指定します。

注

<NS-CONFIG>セクションには、有効な ADC CLI コマンドが必要です。CLI は、構文エラーまた は形式について検証されません。

例

次の例では、<NS-CONFIG>セクションに設定の詳細を示します。ID「5」の VLAN が設定され、SNIP (5.0.0.1) にバインドされます。負荷分散仮想サーバー (4.0.0.101) も構成されています。

<NS-PRE-BOOT-CONFIG> <pr

</NS-PRE-BOOT-CONFIG>

前のスクリーンショットに示した設定をここからコピーできます。

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	

NetScaler VPX インスタンスは、次の図に示すように、<NS-CONFIG>セクションに適用された構成を 表示します。



ユーザースクリプト

<NS-SCRIPTS>タグを使用して、NetScaler VPX インスタンスに保存して実行する必要があるスクリ プトを指定します。

<NS-SCRIPTS>タグには多数のスクリプトを含めることができます。各スクリプトは<SCRIPT >タグ内に含める必要があります。各<SCRIPT>セクションは1つのスクリプトに対応し、次のサ ブタグを使用してスクリプトの詳細をすべて含みます。各 <SCRIPT>セクションは1つのスクリプトに 対応し、次のサブタグを使用してスクリプトの詳細がすべて含まれています。

- ・ <SCRIPT-NAME>:保存する必要のあるスクリプトファイルの名前を示します。
- **<SCRIPT-CONTENT>:**保存する必要のあるファイルの内容を示します。
- <SCRIPT-TARGET-LOCATION>:このファイルを保存する必要がある指定されたターゲットの場所を示します。ターゲットの場所が指定されていない場合、デフォルトでは、ファイルまたはスクリプトは「/nsconfig」ディレクトリに保存されます。
- ・ <SCRIPT-NS-BOOTUP>:スクリプトの実行に使用するコマンドを指定します。
 - <SCRIPT-NS-BOOTUP>セクションを使用する場合、セクションで提供されるコマンドは「/nsconfig/nsafter.sh」に保存され、コマンドは「nsafter.sh」実行の一部としてパケットエンジンが起動した後に実行されます。
 - <SCRIPT-NS-BOOTUP>セクションを使用しない場合、スクリプトファイルは指定した ターゲットの場所に保存されます。

例 **1**:

この例では、<NS-SCRIPTS>タグには script-1.sh というスクリプトの詳細が 1 つだけ含まれていま す。「script-1.sh」スクリプトは「/var」ディレクトリに保存されます。スクリプトは指定された内容で読み込まれ、 パケットエンジンの起動後に「sh /var/script-1.sh」コマンドで実行されます。

<script></th><th></th></tr><tr><td></td><td></td></tr><tr><td>#Shell script</td><td></td></tr><tr><td>echo "Running scri</td><td>pt 1" > /var/script-1.output</td></tr><tr><td>date >> /var/script-</td><td>-1.output</td></tr><tr><td></SCRIPT-CONTENT></td><td></td></tr><tr><td><pre>SCRIPT-NAME> script-</pre></td><td>1.sh </SCRIPT-NAME></td></tr><tr><td>SCRIPT-TARGET-LOCAT</td><td>ION> /var/ </SCRIPT-TARGET-LOCATION></td></tr><tr><td>SCRIPT-NS-BOOTUP>st</td><td>h /var/script-1 sh</SCRIPT-NS-BOOTUP></td></tr><tr><td></script> <td></td>	

</NS-PRE-BOOT-CONFIG>

前のスクリーンショットに示した設定をここからコピーできます。

```
<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>
11
                    /var/ </SCRIPT-TARGET-</pre>
                      LOCATION>
                   sh /var/script-1.sh</SCRIPT-NS-</pre>
                      BOOTUP>
13
            </SCRIPT>
14
        </NS-SCRIPTS>
15
    </NS-PRE-BOOT-CONFIG>
```

次のスナップショットでは、「script-1.sh」スクリプトが「/var/」ディレクトリに保存されていることを確認できま す。「Script-1.sh」スクリプトが実行され、出力ファイルが適切に作成されます。





次の例では、<NS-SCRIPTS>タグに2つのスクリプトの詳細が含まれています。

- 最初のスクリプトは「script-1.sh」として「/var」ディレクトリに保存されます。スクリプトは指定された内容で読み込まれ、パケットエンジンの起動後にコマンド「sh /var/script-1.sh」で実行されます。
- 2番目のスクリプトは「file-2.txt」として「/var」ディレクトリに保存されます。このファイルには、指定され たコンテンツが入力されます。しかし、ブートアップ実行コマンド<SCRIPT-NS-BOOTUP>が 提供されていないため、実行されません。

< <u>SCRIPT></u>	script-1.sh
shell script cho "Running script 1" > /var/script-1 output	
ate >> /var/script-1.output	
	N
script-1.sh	12
<pre><script-target-location> /var/ </script-target-location></pre>	
sh /var/script-1.sh	file-2.txt
<th></th>	
< CODIDTS	
his script has no execution point. It will just be saved at the target location. N	S Consumer module should consume this
ript/file.	
file-2.txt	
/var/	

前のスクリーンショットに示した設定をここからコピーできます。

```
1 <NS-PRE-BOOT-CONFIG>
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
                  This script has no execution point.
17
                  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>
```

次のスナップショットでは、script-1.sh と file-2.txt が「/var/」ディレクトリに作成されていることを確認できま す。Script-1.sh が実行され、出力ファイルが適切に作成されます。

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/scrip	t-l.sh			
#Shell script				
echo "Running script 1"	> /var/script-l.output			
date >> /var/script-1.0	utput			
root@ns#				
root@ns# cat /var/scrip	t-1.output			
Running script 1				
Wed Jan 6 05:08:56 UTC	2021			
root@ns#				
root@ns#				
root@ns# cat /var/file-:	2.txt			
This script has no exect	ution point.			
It will just be saved a	t the target location			
NS Consumer module shou	ld consume this script/f:	ile		
root@ns#				
root@ns#				

ライセンス

VPX インスタンスの起動中に NetScaler プールライセンスを適用するには、<NS-LICENSE-CONFIG& gt;タグを使用します。<NS-LICENSE-CONFIG>セクション内の<LICENSE-COMMANDS >タグを使用して、プールされたライセンスコマンドを指定します。これらのコマンドは構文的に有効である必 要があります。

標準のプールライセンスコマンドを使用して、<LICENSE-COMMANDS>セクションで、ライセンスタ イプ、容量、ライセンスサーバーなどのプールされたライセンスの詳細を指定できます。詳細については、「NetScaler プール容量ライセンスの構成」を参照してください。

<NS-LICENSE-CONFIG>を適用した後、VPX は起動時に要求されたエディションを起動し、VPX は ライセンスサーバから構成されたライセンスをチェックアウトしようとします。

- ライセンスのチェックアウトが成功すると、構成された帯域幅が VPX に適用されます。
- ライセンスのチェックアウトに失敗した場合、約10~12分以内にライセンスはライセンスサーバから取得されません。その結果、システムがリブートし、ライセンスなしの状態になります。

例

次の例では、<NS-LICENSE-CONFIG>を適用した後、VPX は起動時にプレミアムエディションを起 動し、VPX はライセンスサーバ(10.102.38.214)から構成されたライセンスをチェックアウトしようとします。

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

前のスクリーンショットに示した設定をここからコピーできます。

1	<ns-pre-boot-config></ns-pre-boot-config>
2	<ns-license-config></ns-license-config>
3	<license-commands></license-commands>
4	add ns licenseserver 10.102.38.214 -port 2800
5	set ns capacity -unit gbps -bandwidth 3 edition platinum
6	
7	
8	

次の図に示すように、「ライセンスサーバーの表示」コマンドを実行し、ライセンスサーバー(10.102.38.214)が VPX に追加されていることを確認します。

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

ブートストラッピング

<NS-BOOTSTRAP>タグを使用して、カスタムブートストラップ情報を指定します。<NS -BOOTSTRAP>セクション内では、<SKIP-DEFAULT-BOOTSTRAP>タグと<NEW-BOOTSTRAP-SEQUENCE>タグを使用できます。このセクションでは、デフォルトのブートストラップを 回避するかどうかを NetScaler アプライアンスに通知します。デフォルトのブートストラップが回避される場合、こ のセクションでは、新しいブートストラップシーケンスを提供するオプションを提供します。

デフォルトのブートストラップ構成

NetScaler アプライアンスのデフォルトのブートストラップ構成は、次のインターフェイスの割り当てに従います。

- EthO -特定の NSIP アドレスを持つ管理インターフェイス。
- Eth1 -特定の VIP アドレスを持つクライアント向けインターフェイス。
- Eth2 -特定の SNIP アドレスを持つサーバー側インターフェイス。

ブートストラップ構成をカスタマイズする

デフォルトのブートストラップシーケンスをスキップして、NetScaler VPX インスタンスに新しいブートストラッ プシーケンスを指定することができます。<NS-BOOTSTRAP>タグを使用して、カスタムブートストラ ップ情報を指定します。たとえば、管理インターフェイス (NSIP)、クライアント側インターフェイス (VIP)、およ びサーバー側インターフェイス (SNIP) が常に特定の順序で提供されるデフォルトのブートストラップを変更できま す。

次の表に、<SKIP-DEFAULT-BOOTSTRAP>および<NEW-BOOTSTRAP-SEQUENCE> ;タグで許可されるさまざまな値を使用したブートストラップ動作を示します。

SKIP-DEFAULT-	NEW-BOOTSTRAP-	
BOOTSTRAP	SEQUENCE	ブートストラップ動作
はい	はい	デフォルトのブートストラップ動作
		はスキップされ、
		<ns-bootstrap>セ</ns-bootstrap>
		クションで提供される新しいカスタ
		ムブートストラップシーケンスが実
		行されます。
はい	いいえ	デフォルトのブートストラップ動作
		はスキップされま
		す。「 <ns-config>」</ns-config>
		セクションに記載されているブート
		ストラップコマンドが実行されます。

ブートストラップ構成は、次の3つの方法でカスタマイズできます。

- インターフェイスの詳細のみを入力します。
- IP アドレスとサブネットマスクとともにインターフェイスの詳細を指定します。
- <NS-CONFIG>セクションにブートストラップ関連のコマンドを入力します。

方法 1: インターフェイスの詳細のみを指定してカスタムブートストラップ

管理インターフェイス、クライアント向けインターフェイス、およびサーバ側インターフェイスは指定しますが、その IP アドレスとサブネットマスクは指定しません。IP アドレスとサブネットマスクは、クラウドインフラストラク チャのクエリによって設定されます。

AWS のカスタムブートストラップの例

次の例に示すように、カスタムブートストラップシーケンスを指定します。詳細については、「クラウドインスタンス でプレブートユーザーデータを提供する方法」を参照してください。Eth2 インターフェイスは、管理インターフェイ ス (NSIP) として、Eth1 インターフェイスをクライアントインターフェイス (VIP) として、Eth0 インターフェイ スをサーバインターフェイス (SNIP) として割り当てます。<NS-BOOTSTRAP>セクションには、イン ターフェイスの詳細のみが含まれ、IP アドレスとサブネットマスクの詳細は含まれません。



VM インスタンスの作成後、AWS ポータルで、ネットワークインターフェイスのプロパティを次のように確認できます。

- 1. [AWS Portal] > [EC2 インスタンス] に移動し、カスタムブートストラップ情報を指定して作成したインス タンスを選択します。
- 2. [説明] タブでは、次の図に示すように、各ネットワークインタフェースのプロパティを確認できます。

Network Interface eth1	
Interface ID	<u>eni-021961099be6815eb</u>
VPC ID Attachment Owner	vpс-об258с02 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 VPC ID Attachment Owner Attachment Status Attachment Time Delete on Terminate Private IP Address Private DNS Name	<u>eni-039e5f3329cd879e9</u> 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- 1.compute.internal
Network Interface eth2	
Interface ID VPC ID Attachment Owner Attachment Status Attachment Time Delete on Terminate Private IP Address Private DNS Name	eni-09e55a6cfb791e68d vpc-6b258c02 566658252593 attached Fri Jan 01 11:11:33 GMT+530 2021 false 172.31.76.177 @ ip-172-31-76-177.ap-south-1.compute.internal @

ADC CLI でshow nsipコマンドを実行し、ADC アプライアンスの初回起動時に NetScalerVPX インスタンスに 適用されるネットワークインターフェイスを確認できます。

NetScaler VPX 14.1

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

Azure のカスタムブートストラップの例

次の例に示すように、カスタムブートストラップシーケンスを指定します。詳細については、「クラウドインスタンス でプレブートユーザーデータを提供する方法」を参照してください。Eth1 インターフェイスは管理インターフェイス (NSIP)、クライアントインターフェイス (VIP) として Eth0 インターフェイス、サーバインターフェイス (SNIP) として Eth2 インターフェイスが割り当てられます。<NS-BOOTSTRAP>セクションには、インターフ ェイスの詳細のみが含まれ、IP アドレスとサブネットマスクの詳細は含まれません。



NetScaler VPX インスタンスが 3 つのネットワークインターフェイスで作成されていることがわかります。Azure Portal > VM インスタンス > ネットワークに移動し、次の図に示すように 3 つの NIC のネットワークプロパティを 確認します。



ADC CLI でshow nsipコマンドを実行し、<NS-BOOTSTRAP>セクションで指定された新しいブー

トストラップシーケンスが適用されていることを確認できます。「show route」コマンドを実行して、サブネットマ スクを確認できます。

> sh na	s ip							
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
L)	172.27.2.53	0	NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	172.27.0.53		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	172.27.1.53		VIP	Active	Enabled	Enabled	Enabled	Enabled
Done								
> sh v]	Lan							
1.	VIAN TD. 1							
1	Tink-local TDue	addr. fa8020d.	3aff.fac9.c26c/64					
	Interfaces · 0/1	1/1 10/1	5411.1005.0200/01					
	interfaces . 0/1	1/1 10/1						
	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2	2						
	IPs :							
	172.27.2.53	B Mask: 25	5.255.255.0					
Done								
sh ro	oute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic D	omain Ty	pe
	0.0.0.0	0.0.0.0	172.27.2.1		UP		ST	TIC
	127.0.0.0	255.0.0.0	127.0.0.1		UP		PEF	MANENT
	172.27.0.0	255.255.255.0	172.27.0.53		UP		DIF	ECT
	172.27.1.0	255.255.255.0	172.27.1.53		UP		DIF	ECT
)	172.27.2.0	255.255.255.0	172.27.2.53		UP		DIF	ECT
	169.254.0.0	255.255.0.0	172.27.0.1		UP		STA	TIC
			120 02 0 1		TTD		ST7	TT CI
)	168.63.129.16	255.255.255.255	1/2.2/.0.1		UE		JIF	
)	168.63.129.16 169.254.169.254	255.255.255.255	172.27.0.1		UP		STA	TIC

GCP のカスタムブートストラップの例

次の例に示すように、カスタムブートストラップシーケンスを指定します。詳細については、「クラウドインスタンス でプレブートユーザーデータを提供する方法」を参照してください。Eth2 インターフェイスは、管理インターフェイ ス (NSIP) として、Eth1 インターフェイスをクライアントインターフェイス (VIP) として、Eth0 インターフェイ スをサーバインターフェイス (SNIP) として割り当てます。<NS-B00TSTRAP>セクションには、イン ターフェイスの詳細のみが含まれ、IP アドレスとサブネットマスクの詳細は含まれません。

<new-bootstrap-sequence>YES<</new-bootstrap-sequence>	/NEW-BOOTSTRA	P-SEQUENCE>	
<mgmt-interface-config></mgmt-interface-config>			
<interface-num><u>eth1</u><td>ERFACE-NUM></td><td></td><td></td></interface-num>	ERFACE-NUM>		
<client-interface-config></client-interface-config>		_	
<interface-num> eth0 <td>ERFACE-NUM></td><td></td><td></td></interface-num>	ERFACE-NUM>		
<server-interface-config></server-interface-config>		-	
<interface-num> eth2 <td>ACE-NUM></td><td></td><td></td></interface-num>	ACE-NUM>		

GCP ポータルで VM インスタンスを作成した後、ネットワークインターフェイスのプロパティを次のように確認で きます。

- 1. カスタムブートストラップ情報を指定して、作成したインスタンスを選択します。
- 2. ネットワークインターフェイスのプロパティに移動し、NIC の詳細を次のように確認します。

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

ADC CLI でshow nsipコマンドを実行し、ADC アプライアンスの初回起動時に NetScalerVPX インスタンスに 適用されるネットワークインターフェイスを確認できます。

s ip Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State			
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			
lan										
<pre>1) VLAN ID: 1 Link-local IPv6 addr: fe80::4001:aff:fea0:47/64 Interfaces : 0/1 1/1 LO/1</pre>										
VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 10.128.4.27 Mask: 255.255.2										
ute										
Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main Ty	pe			
0.0.0.0 127.0.0.0 10.128.0.0 10.128.4.0 10.160.0.0	0.0.0.0 255.0.0.0 255.255.255.0 255.255.255.0 255.255.240.0	10.128.4.1 127.0.0.1 10.128.0.40 10.128.4.27 10.160.0.71		UP UP UP UP UP		STA PER DIR DIR DIR	 TIC MANENT ECT ECT ECT			
	s ip Ipaddress 10.128.4.27 10.160.0.71 10.128.0.40 Ian VLAN ID: 1 Link-local IPv6 Interfaces : 0/1 VLAN ID: 10 Interfaces : 1/2 IPs : 10.128.4.2 Dute Network 0.0.0.0 127.0.0.0 10.128.4.0 10.160.0.0	s ip Ipaddress Traffic Domain 10.128.4.27 0 10.160.0.71 0 10.128.0.40 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 : 10.128.4.27 Mask: 25 Dute Network Netmask 0.0.0.0 0.0.00 127.0.0.0 255.255.0 10.128.4.0 255.255.0 10.160.0.0 255.255.240.0	s ip Ipaddress Traffic Domain Type 10.128.4.27 0 NetScaler IP 10.160.0.71 0 SNIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.0.40 0 VIP 10.128.1 IPV6 addr: fe80::4001:aff:fea0:47/64 Interfaces : 0/1 1/1 LO/1 VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 10.128.4.27 Mask: 255.255.255.0 10.128.4.21 Mask: 255.255.255.0 10.128.4.1 127.0.0.0 255.0.0.0 127.0.0.1 10.128.4.0 255.255.255.0 10.128.0.40 10.128.4.0 255.255.255.0 10.128.4.27 10.160.0.0 255.255.240.0 10.160.0.71	ip Ipaddress Traffic Domain Type Mode 10.128.4.27 0 NetScaler IP Active 10.160.0.71 0 SNIP Active 10.128.0.40 0 VIP Active 10.128.0.40 0 VIP Active active Node Active Active 10.128.0.40 0 VIP Active active Netmask Active Active active Netmask Gateway/OwnedIP VLAN VLAN ID: 10 VLAN Alias Name: Interfaces : 1/2 IPs : 10.128.4.27 Mask: 255.255.255.0 Mask: 255.255.255.0 0 oute Network Netmask Gateway/OwnedIP VLAN 127.0.0.0 255.0.0.0 127.0.0.1 0 0 10.128.0.0 255.255.255.0 10.128.0.40 0 0 10.128.4.0 255.255.255.0 10.128.4.27 0 0 10.160.0.0 255.255.240.0 10.160.0.71 0	ip Ipaddress Traffic Domain Type Mode Arp 10.128.4.27 0 NetScaler IP Active Enabled 10.160.0.71 0 SNIP Active Enabled 10.128.0.40 0 VIP Active Enabled 10.128.0.40 0 VIP Active Enabled Active Enabled Active Enabled Active Inabled Active Enabled Active Inabled Active Enabled Active Inabled Active Enabled Active Inabled Interfaces: Interfaces: Interfaces: VLAN ID: 10 VLAN Alias Name: Interfaces: Interfaces: Interfaces: IPs : 10.128.4.27 Mask: 255.255.255.0 Interfaces: Interfaces: 0.0.0.0 0.0.0.0 10.128.4.1 0 UP Interfaces: Inte	ip Ipaddress Traffic Domain Type Mode Arp Icmp Icmp 10.128.4.27 0 NetScaler IP Active Enabled Enabled Indicate the state 10.160.0.71 0 SNIP Active Enabled Enabled Indicate the state 10.128.0.40 0 VIP Active Enabled Enabled Indicate an VLAN ID: 1 Link-local IPv6 addr: fe80::4001:aff:fea0:47/64 Active Enabled Indicate Interfaces : 0/1 1/1 LO/1 VLAN Alias Name: Interfaces : 1/2 IFs : 10.128.4.27 Mask: 255.255.255.0 Network Netmask Gateway/OwnedIP VLAN State Traffic Domestic 0.0.0.0 0.0.0.0 10.128.4.1 0 UP 0 127.0.0.0 255.0.0.0 127.0.0.1 0 UP 0 10.128.4.0 255.255.255.0 10.128.0.40 0 UP 0 10.128.4.0 255.255.255.0 10.128.4.27 0 UP 0 10.128.4.0 255.255.240.0 10.160.0.71 0 UP 0 <td>ip Traffic Domain Type Mode Arp Icmp Vserver 10.128.4.27 0 NetScaler IP Active Enabled Enabled NA 10.128.0.40 0 VIP Active Enabled Enabled</td>	ip Traffic Domain Type Mode Arp Icmp Vserver 10.128.4.27 0 NetScaler IP Active Enabled Enabled NA 10.128.0.40 0 VIP Active Enabled Enabled			

方法 2: インターフェイス、IP アドレス、およびサブネットマスクを指定してカスタムブートストラップ

管理インターフェイス、クライアント向けインターフェイス、およびサーバ向けインターフェイスと IP アドレスとサ ブネットマスクを指定します。

AWS のカスタムブートストラップの例

次の例では、デフォルトのブートストラップをスキップして、NetScaler アプライアンスの新しいブートストラップ シーケンスを実行します。新しいブートストラップシーケンスでは、次の詳細を指定します。

- ・管理インターフェイス: インターフェイス-Eth1、NSIP-172.31.52.88、およびサブネットマスク-255.255.240.0
- クライアント側インターフェイス:インターフェイス-Eth0、VIP-172.31.5.155、およびサブネットマス ク-255.255.240.0。
- ・サーバー側インターフェイス: インターフェイス-Eth2、SNIP-172.31.76.177、サブネットマスク-255.255.240.0。



ADC CLI でshow nsipコマンドを実行し、<NS-BOOTSTRAP>セクションで指定された新しいブー トストラップシーケンスが適用されていることを確認できます。「show route」コマンドを実行して、サブネットマ スクを確認できます。

> sh ns	ip							
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp V:	server	State
1)	172.31.52.88	0	NetScaler IP	Active	Enabled	Enabled N	A	Enabled
2)	172.31.76.177	0	SNIP	Passive	Enabled	Enabled N	A	Enabled
3)	172.31.5.155	0	VIP	Passive	Enabled	Enabled En	nabled	Enabled
Done								
> sh vl	an							
1)	VIAN TD. 1							
±)	Link-local IPv6	addr: fe80:.839.						
	Interfaces : 1/1	1/3 10/1	2211.1001.1000/01					
	1.0001140000 1 1/1	1,0 10,1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	172.31.52.8	8 Mask: 25	5.255.240.0					
Done								
> sh ro	oute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Doma	ain Ty	pe
1)	0.0.0.0	0.0.0.0	172.31.48.1	0	 UP	0	STA	 TTC
2)	127.0.0.0	255.0.0.0	127.0.0.1	0	UP	0	PER	MANENT
3)	172.31.0.0	255.255.240.0	172.31.5.155	0	UP	0	DIR	ECT
4)	172.31.48.0	255.255.240.0	172.31.52.88	0	UP	0	DIR	ECT
5)	172.31.64.0	255.255.240.0	172.31.76.177	0	UP	0	DIR	ECT
6)	172.31.0.2	255.255.255.255	172.31.48.1		UP		STA	TIC
Done								
S .								

Azure のカスタムブートストラップの例

次の例では、ADC の新しいブートストラップシーケンスが記述され、デフォルトのブートストラップがスキップされ ます。インターフェイスの詳細と IP アドレスとサブネットマスクを次のように指定します。

- 管理インターフェイス (eth2)、NSIP (172.27.2.53)、およびサブネットマスク (255.255.255.0)
- クライアント側インターフェイス (eth1)、VIP (172.27.1.53)、およびサブネットマスク (255.255.255.0)
- ・ サーバー側インターフェイス (eth0)、SNIP (172.27.0.53)、およびサブネットマスク (255.255.255.0)



NetScaler VPX インスタンスが 3 つのネットワークインターフェイスで作成されていることがわかります。Azure Portal > VM インスタンス > ネットワークに移動し、次の図に示すように 3 つの NIC のネットワークプロパティを

確認します。

菒 Overview		
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3	
Access control (IAM)	IP configuration 🔘	
🔷 Tags	ipconfig1 (Primary)	
Diagnose and solve problems	Network Interfa 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 Ac	celerated networking: Disabled
Networking	Inbound port rules Outbound port rules Application security groups Load balancing	
Overview		
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3	
Access control (IAM)	IP configuration 🔘	
🗳 Tags	ipconfig1 (Primary)	
Diagnose and solve problems	Network Interface: vsk-client-nic3 Effective security rules Topology	
Settings	Virtual network/subnet: vsk-mgmt-vnet-southIndia/vsk-client-subnet NIC Public IP: 52.172.10.184 NIC Private IP: 172.27.1.53 Ac	ccelerated networking: Disabled
Networking	Inbound port rules Outbound port rules Application security groups Load balancing	

Overview	
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration 🔘
🗳 Tags	ipconfig1 (Primary)
Diagnose and solve problems	Network Interface Vsk-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
d	A

ADC CLI でshow nsipコマンドを実行し、<NS-BOOTSTRAP>セクションで指定された新しいブー トストラップシーケンスが適用されていることを確認できます。「show route」コマンドを実行して、サブネットマ スクを確認できます。

> sn ns	lp							
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
1)	172.27.2.53	0	NetScaler TP	Active	 Enabled	Fnabled	 ND	Enabled
-) 2)	172 27 0 53		SNTD	Active	Enabled	Enabled	NA	Enabled
2)	172.27.0.55		VTD	Active	Enabled	Enabled	Fnablad	Enabled
Done	172.27.1.33		VIE	ACCIVE	Enabled	Enabled	LIIADICU	Enabled
> sh vla	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::20d:3	3aff:fec9:c26c/64					
	Interfaces : 0/1	1/1 LO/1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	172.27.2.53	Mask: 25	5.255.255.0					
Done								
> sh rou	ite							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	main Ty	pe
1.5			150 05 0 1					
1)	0.0.0.0	0.0.0.0	1/2.2/.2.1		UP		514	
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENI
3)	172.27.0.0	255.255.255.0	172.27.0.53		UP		DIR	ECT
4)	172.27.1.0	255.255.255.0	172.27.1.53	0	UP	0	DIR	ECT
5)	172.27.2.0	255.255.255.0	172.27.2.53	0	UP	0	DIR	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								

GCPのカスタムブートストラップの例

次の例では、ADC の新しいブートストラップシーケンスが記述され、デフォルトのブートストラップがスキップされ ます。インターフェイスの詳細と IP アドレスとサブネットマスクを次のように指定します。

- 管理インターフェイス (eth2)、NSIP (10.128.4.31)、およびサブネットマスク (255.255.255.0)
- クライアント側インターフェイス (eth1)、VIP (10.128.0.43)、およびサブネットマスク (255.255.255.0)
- ・ サーバ側インターフェイス (eth0)、SNIP (10.160.0.75)、およびサブネットマスク (255.255.255.0)



カスタムブートストラップを使用して GCP ポータルで VM インスタンスを作成した後、ネットワークインターフェ イスのプロパティを次のように確認できます。

- 1. カスタムブートストラップ情報を指定して、作成したインスタンスを選択します。
- 2. ネットワークインターフェイスのプロパティに移動し、NIC の詳細を次のように確認します。

Netw	work interfaces							
Nar	ne Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier 🔞	IP forwarding	Network details
nic	0 default	default	vsk-defnw-st-ip1 (10.160.0.75)	-	34.93.216.90 (ephemeral)	Premium	Off	View details
nic	1 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
nic	2 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

ADC CLI でshow nsipコマンドを実行し、<NS-BOOTSTRAP>セクションで指定された新しいブー トストラップシーケンスが適用されていることを確認できます。「show route」コマンドを実行して、サブネットマ スクを確認できます。

> sh ns	; ip							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp V	server	State
1)	10.128.4.31		NetScaler IP	Active	Enabled	Enabled N	A	Enabled
2)	10.160.0.75		SNIP	Passive	Enabled	Enabled N	A	Enabled
3)	10.128.0.43		VIP	Passive	Enabled	Enabled En	nabled	Enabled
Done								
> sh vl	.an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::4001	:aff:fea0:4b/64					
	Interfaces : 0/1	1/1 LO/1						
2)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	10.128.4.31	Mask: 25	5.255.255.0					
Done								
> sh ro	oute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Doma	ain Ty	pe
1)	0.0.0.0	0.0.0.0	10.128.4.1	0	UP	0	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	10.128.0.43		UP		DIR	ECT
4)	10.128.4.0	255.255.255.0	10.128.4.31		UP		DIR	ECT
5)	10.160.0.0	255.255.255.0	10.160.0.75		UP		DIR	ECT
Done								
>								

方法 3: <NS-CONFIG> セクションにブートストラップ関連のコマンドを指定して、カスタム ブートストラップ

ブートストラップ関連のコマンドについては、<NS-CONFIG>セクションを参照してください。< NS-BOOTSTRAP>セクションでブートストラップコマンドを実行するには、<NS-CONFIG>セ クションで<NEW-BOOTSTRAP-SEQUENCE>を「No」と指定する必要があります。NSIP、デフォル トルート、および NSVLAN を割り当てるコマンドも指定する必要があります。さらに、使用するクラウドに関連す るコマンドも提供します。

カスタムブートストラップを提供する前に、クラウドインフラストラクチャが特定のインターフェイス構成をサポー トしていることを確認してください。

AWS のカスタムブートストラップの例

この例では、ブートストラップ関連のコマンドを<NS-CONFIG>セクションで提供しています。 <NS-BOOTSTRAP>セクションは、デフォルトのブートストラップがスキップされ、<NS-CONFIG>セクションで提供されるカスタムブートストラップ情報が実行されることを示します。NSIPの作 成、デフォルトルートの追加、および NSVLAN の追加を行うコマンドも指定する必要があります。 NetScaler VPX 14.1

<ns-f< th=""><th>PRE-BOOT-CONFIG> NS-CONFIG></th><th>Bootstrap relate</th><th>ed commands</th></ns-f<>	PRE-BOOT-CONFIG> NS-CONFIG>	Bootstrap relate	ed commands					
	set ns config -IPAddress <u>172.31.52.88</u> -netmask add route 0.0.0.0 0.0.0.0 172.31.48.1 set ns config -nsvlan 10 -ifnum 1/2 -tagged NO	255.255.240.0						
	add route 172.31.0.2 255.255.255.255 172.31.4	8.1	route to DNS server is added					
useproxypor	enable ns feature WL SP LB RESPONDER add server 5.0.0.201 5.0.0.201 add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType NONE -cltTimeout 180							
<	NS-BOOTSTRAP> <skip-default-bootstrap>YES<new-bootstrap-sequence> NO /NS-BOOTSTRAP></new-bootstrap-sequence></skip-default-bootstrap>	ULT-BOOTSTRAP> OOTSTRAP-SEQUE	NCE>					
<td>S-PRE-BOOT-CONFIG></td> <td></td> <td></td>	S-PRE-BOOT-CONFIG>							

前のスクリーンショットに示した設定をここからコピーできます。

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	

VM インスタンスの作成後、AWS ポータルで、ネットワークインターフェイスのプロパティを次のように確認できます。

- 1. [**AWS Portal**] > [EC2 インスタンス] に移動し、カスタムブートストラップ情報を指定して作成したインス タンスを選択します。
- 2. [説明] タブでは、次の図に示すように、各ネットワークインタフェースのプロパティを確認できます。

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	<u>172.31.52.88</u>
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	<u>eni-09e55a6cfb791e68d</u>
Attachment Owner	566658252593
Attachment Status Attachment Time	attached Fri Jan 01 11:11:33 GMT+530 2021
Delete on Terminate	false
Private IP Address Private DNS Name	172.31.76.177 @ ip-172-31-76-177.ap-south-1.compute.internal ^企

ADC CLI でshow nsipコマンドを実行し、ADC アプライアンスの初回起動時に NetScalerVPX インスタンスに 適用されるネットワークインターフェイスを確認できます。

> sh ns	ip										
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State			
1)	172.31.52.88		NetScaler IP	Active	Enabled	Enabled	NA	Enabled			
2)	4.0.0.101		VIP	Active	Enabled	Enabled	Enabled	Enabled			
Done											
> sh vl	an										
1)	VLAN ID: 1										
	Link-local IPv6	addr: fe80::839:6	e2ff:feaf:4a9e/64								
	Interfaces : 1/1 1/3 LO/1										
2)	VLAN ID: 10	VLAN Alias Name:									
	Interfaces : 1/2										
	IPs :										
	172.31.52.8	8 Mask: 255	5.255.240.0								
Done											
> sh ro	ute										
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic D	omain T	ype			
1)	0.0.0.0	0.0.0.0	172.31.48.1		UP		ST	ATIC			
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PE	RMANENT			
3)	172.31.48.0	255.255.240.0	172.31.52.88		UP		DI	RECT			
4)	172.31.0.2	255.255.255.255	172.31.48.1		UP		ST	ATIC			
Done											
>											

Azure のカスタムブートストラップの例

この例では、ブートストラップ関連のコマンドを<NS-CONFIG>セクションで提供しています。<NS-BOOTSTRAP>セクションは、デフォルトのブートストラップがスキップされ、<NS-CONFIG>セクションで提供されるカスタムブートストラップ情報が実行されることを示します。

注

Azure クラウドの場合、インスタンスメタデータサーバー (IMDS) と DNS サーバーはプライマリインターフェイス (Eth0) を介してのみアクセスできます。したがって、Eth0 インターフェイスが管理インターフェイス

(NSIP) として使用されない場合、EthO インターフェイスは、少なくとも IMDS または DNS アクセスを動作 させるには、SNIP として設定する必要があります。EthO のゲートウェイを経由する IMDS エンドポイント (169.254.169.254) および DNS エンドポイント(168.63.129.16)へのルートも追加する必要があります。



```
1 <NS-PRE-BOOT-CONFIG>
2
3
        <NS-CONFIG>
4
5
             set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
6
             add route 0.0.0.0 0.0.0.0 172.27.2.1
7
             set ns config -nsvlan 10 -ifnum 1/2 -tagged NO
             add ns ip 172.27.0.61 255.255.255.0 -type SNIP
8
9
             add route 169.254.169.254 255.255.255.255 172.27.0.1
             add route 168.63.129.16 255.255.255.255 172.27.0.1
11
             add vlan 5
12
             bind vlan 5 - IPAddress 5.0.0.1 255.255.255.0
13
             enable ns feature WL SP LB RESPONDER
14
             add server 5.0.0.201 5.0.0.201
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 -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
```

```
NO -CMP NO
17
             add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
                 persistenceType NONE -cltTimeout 180
18
         </NS-CONFIG>
19
21
         <NS-BOOTSTRAP>
22
23
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24
         <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26
         </NS-BOOTSTRAP>
27
     </NS-PRE-BOOT-CONFIG>
28
```

NetScaler VPX インスタンスが 3 つのネットワークインターフェイスで作成されていることがわかります。Azure Portal > VM インスタンス > ネットワークに移動し、次の図に示すように 3 つの NIC のネットワークプロパティを 確認します。

✓ Search (Ctrl+/)	« \mathscr{S} Attach network interface \mathscr{S} Detach network interface
👤 Overview	^
Activity log	vsk-server-nic3 vsk-client-nic3 vsk-mgmt-nic3
Access control (IAM)	IP configuration ①
Tags	ipsonfig1 (Drimany)
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
Retworking	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
2 Networking	Inbound port rules Outbound port rules Application security groups Load balancing
Overview	
Activity log	vsk-server-nica vsk-client-nica vsk-mgmt-nica
Access control (IAM)	IP configuration ()
🔷 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
Networking	Inbound port rules Outbound port rules Application security groups Load balancing
Ø. Connect	

ADC CLI でshow nsipコマンドを実行し、<NS-BOOTSTRAP>セクションで指定された新しいブー トストラップシーケンスが適用されていることを確認できます。「show route」コマンドを実行して、サブネットマ スクを確認できます。

> sh ns	s ip Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp Vs	erver	State
1)	172.27.2.61	0	NetScaler IP	Active	Enabled	Enabled NA		Enabled
2)	172.27.0.61		SNIP	Active	Enabled	Enabled NA		Enabled
3) Done	4.0.0.101	0	VIP	Active	Enabled	Enabled En	abled	Enabled
> sh vl	an							
1)	VLAN ID: 1							
	Link-local IPv6	addr: fe80::20d:	3aff:fec9:9076/64					
	Interfaces : 0/1	1 1/1 LO/1						
2)	VLAN ID: 5	VLAN Alias Name:						
3)	VLAN ID: 10	VLAN Alias Name:						
	Interfaces : 1/2							
	IPs :							
	172.27.2.61	Mask: 25	5.255.255.0					
Done								
> sh ro	ute							
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Doma	in Ty	pe
1)	0.0.0.0	0.0.0.0	172.27.2.1	0	UP	0	STA	TIC
2)	127.0.0.0	255.0.0.0	127.0.0.1		UP		PER	MANENT
3)	172.27.0.0	255.255.255.0	172.27.0.61		UP		DIR	ECT
4)	172.27.2.0	255.255.255.0	172.27.2.61		UP		DIR	ECT
5)	169.254.0.0	255.255.0.0	172.27.0.1		UP		STA	TIC
6)	168.63.129.16	255.255.255.255	172.27.0.1		UP		STA	TIC
7)	169.254.169.254	255.255.255.255	172.27.0.1		UP		STA	TIC
Done								

GCP のカスタムブートストラップの例

この例では、ブートストラップ関連のコマンドを<NS-CONFIG>セクションで提供しています。<NS-BOOTSTRAP>セクションは、デフォルトのブートストラップがスキップされ、<NS-CONFIG>セクションで提供されるカスタムブートストラップ情報が適用されることを示します。


前のスクリーンショットに示した設定をここからコピーできます。

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

カスタムブートストラップを使用して GCP ポータルで VM インスタンスを作成した後、ネットワークインターフェ イスのプロパティを次のように確認できます。

1. カスタムブートストラップ情報を指定して、作成したインスタンスを選択します。

2. [Network Interface] プロパティに移動し、図に示すように NIC の詳細を確認します。

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)

ADC CLI で**show nsip**コマンドを実行し、**ADC** アプライアンスの最初の起動時に前の<NS-CONFIG& gt;セクションで説明した設定が適用されていることを確認できます。

> sh ns	ip Ipaddress	Traffic Domain	Туре	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 1/2 LO/1	:aff:fea0:4a/64					
2)	VLAN ID: 10 Interfaces : 1/1 IPs : 10.128.0.2	VLAN Alias Name: L Mask: 25	5.255.255.0					
Done								
> sh ro	ute Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	omain Ty	/pe
1)	0.0.0.0	0.0.0.0	10.128.0.1		UP		ST	ATIC
3)	10.128.0.0	255.255.255.0	10.128.0.2		UP	0	DI	RECT

AWS および Azure での NIC のアタッチとデタッチによる影響

AWS と Azure には、ネットワークインターフェイスをインスタンスにアタッチし、ネットワークインターフェイス をインスタンスからデタッチするオプションが用意されています。インターフェイスをアタッチまたはデタッチする と、インターフェイスの位置が変わることがあります。そのため、Citrix では NetScaler VPX インスタンスからイ ンターフェイスをデタッチしないことをお勧めします。カスタムブートストラップが構成されているときにインター フェイスをデタッチまたは接続すると、NetScaler VPX インスタンスは、管理インターフェイスの位置で新しく使用 可能なインターフェイスのプライマリ IP を NSIP として再割り当てします。デタッチしたインターフェイスの後に 使用可能なインターフェイスがない場合は、最初のインターフェイスが NetScaler VPX インスタンスの管理インタ ーフェイスになります。

たとえば、NetScaler VPX インスタンスは、Eth0(SNIP)、Eth1(NSIP)、および Eth2(VIP)の 3 つのインター フェイスで起動されます。管理インターフェイスであるインスタンスから Eth1 インターフェイスをデタッチすると、 ADC は次の使用可能なインターフェイス (Eth2) を管理インターフェイスとして設定します。そのため、NetScaler VPX インスタンスには引き続き Eth2 インターフェイスのプライマリ IP を介してアクセスされます。Eth2 も使用で きない場合は、残りのインターフェイス (Eth0) が管理インターフェイスになります。そのため、NetScaler VPX インスタンスには引き続きアクセスできます。

Eth0 (SNIP)、Eth1 (VIP)、Eth2 (NSIP) の異なるインターフェイスの割り当てを考えてみましょう。Eth2 (NSIP) をデタッチすると、Eth2 の後に新しいインターフェイスが使用できないため、最初のインターフェイス (Eth0) が 管理インターフェイスになります。

パブリッククラウドプラットフォームでの SSL-TPS パフォーマンスを向上させる

October 17, 2024

パケットエンジン (PE) の重みを均等に分散することで、AWS と GCP クラウドで SSL-TPS のパフォーマンスを向 上させることができます。この機能を有効にすると、HTTP スループットが約 10 ~12% わずかに低下する可能性が あります。

AWS および GCP クラウドでは、10~16 個の vCPU を持つ NetScaler ADC VPX インスタンスでは、PE の重みが デフォルトで均等に分散されるため、パフォーマンスの向上は見られません。

注

Azure クラウドでは、PE の重みはデフォルトで均等に分散されます。この機能によって Azure インスタンスのパフォーマンスは向上しません。

NetScaler CLI を使用して PE モードを構成する

PE モードを設定したら、設定変更を有効にするためにシステムをリブートする必要があります。

コマンドプロンプトで入力します:

1 set cpuparam pemode [CPUBOUND | Default]

PE モードが CPUBOUND に設定されている場合、PE の重みは均等に分散されます。PE モードが DEFAULT に設 定されている場合、PE の重みはデフォルト値に設定されます。PE モードが DEFAULT に設定されている場合、PE の重みはデフォルト値に設定されます。

注

このコマンドはノード固有です。高可用性またはクラスタセットアップでは、各ノードでコマンドを実行する 必要があります。CLIP でコマンドを実行すると、次のエラーが発生します。CLIP では操作は許可されてい ません

設定されている PE モードの状態を表示するには、次のコマンドを実行します。

1 show cpuparam

例

1	> show cpupa	ram
2	Pemode:	CPUBOUND
3	Done	

クラウド内の NetScaler ADC アプライアンスの初回起動時に PE モード構成を適用する

クラウド内の NetScaler ADC アプライアンスの初回起動時に PE モード構成を適用するには、カスタムスクリプト を使用して/nsconfig/.cpubound.confファイルを作成する必要があります。詳細については、「クラウ ド内の NetScaler アプライアンスの初回起動時に NetScaler VPX 構成を適用する」を参照してください。

パブリッククラウド上の NetScaler VPX 同時マルチスレッドを構成する

October 17, 2024

NetScaler は、管理とデータプレーン機能にさまざまな専用コアを使用します。通常、1 つのコアが管理プレーン機能に割り当てられます。使用可能な残りのコアはデータプレーン機能に割り当てられます。

以下の画像は、4 コアの NetScaler VPX を簡略化した図を示しています。

図1: インライン展開図1: 4 コアシステムでの NetScaler 管理とデータプレーンワークロード



上の図は、使用可能なコア全体にわたる NetScaler 機能の分布を示していますが、基盤となるハードウェアを必ずし も正確に表しているわけではありません。最新の x86 CPU のほとんどは、Intel ハイパースレッディング(HT)ま たは AMD 同時マルチスレッディング(SMT)として商業的に知られている機能により、物理コアあたり 2 つの論理 コアを備えています。

次の画像は、SMT が無効になっている最新の CPU 上で実行されている NetScaler VPX を示しています。各 CPU コ アは、一般にスレッドと呼ばれる 2 つ以上の論理 CPU に分割されます。各スレッドには、それぞれ独自の複製リソー スセットとパーティション化されたリソースの一部があり、兄弟スレッドと共有リソースをめぐって競合します。 図 2: 図 2: SMT を無効にした 4 コア/8 スレッドシステムでの NetScaler 管理とデータプレーンワークロード



次の画像は、SMT が有効になっている最新の CPU 上で実行されている NetScaler VPX を示しています。

図 5. 図 3: SMT が有効になっている 4 コアシステムでの NetScaler 管理とデータプレーンワークロード



SMT を有効にすると、次の点で NetScaler のパフォーマンスが向上します:

- すべての物理コアでデータプレーン機能を実行しています。
- 管理プレーン機能を兄弟スレッドに移動します。
- 管理プレーン機能がデータプレーン機能のパフォーマンスを損なうことを防ぐために、柔軟なリソース制限メ カニズムを導入しました。

SMT サポートマトリックス

SMT をサポートする VPX プラットフォーム、クラウドインスタンスタイプ、NetScaler のバージョンを次の表に示 します。

|VPX プラットフォーム|インスタンスタイプ|NetScaler VPX バージョン|

|-----|-----|

|AWS|M5, m5n, c5, c5n | 14.1-12.x およびそれ以降|

|Azure|ハイパースレッディングを使用するすべてのインスタンスファミリー (DS_v4 など)|14.1-12.x およびそ れ以降|

|GCP|e2 インスタンス|14.1-12.x およびそれ以降|

注

SMT 機能を有効にすると、サポートされているタイプの NetScaler VPX パフォーマンスが向上します。

制限事項

SMT 機能により、NetScaler アプライアンスが利用できる仮想 CPU の数が実質的に倍増します。NetScaler アプ ライアンスがライセンス制限を使用できるようにするには、ライセンス制限を考慮する必要があります。

たとえば、図3に示されている NetScaler VPX について考えてみます。スループットベースのライセンスを使用す る場合、8個の vCPU を有効にするには、SMT 機能を備えた 10 Gbps 以上のライセンスが必要です。以前は、4つ の vCPU を有効にするには1 Gbps のライセンスで十分でした。vCPU ライセンスを使用する場合、正常に動作する ためには、2 倍の数の vCPU のライセンスをチェックアウトするように NetScaler VPX を構成する必要があります。 このトピックに関する詳細なガイダンスについては、NetScaler テクニカルサポートにお問い合わせください。

SMT を設定して下さい

SMT 機能を有効にする前に、プラットフォームがこの機能をサポートしていることを確認してください。前のセクションのサポートマトリックスの表を参照してください。

SMT 機能を有効にするには、次の手順に従います:

- 1.「/nsconfig」ディレクトリの下に名前.smt_handlingの空のファイルを作成します。
- 2. 現在の設定を保存します。
- 3. NetScaler VPX インスタンスを再起動します。

```
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. 再起動後、NetScaler は機能が使用可能で有効であることを示します。

```
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
```

SMT 機能を無効にするには、次の手順に従います:

- 1. .smt_handling ファイルを削除します。
- 2. NetScaler VPX インスタンスを再起動します。

```
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. 再起動後、NetScaler は機能が使用可能だが無効になっていることを示します。

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

トラブルシューティング

sysctl シェルコマンドを実行して、SMT 機能のステータスを確認します。

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

このコマンドは、次の出力のいずれかを返すことができます。

• SMT 機能がありません。

sysctlコマンドは出力を返しません。

• SMT 機能はサポートされていません。

SMT 機能は次のいずれかの理由でサポートされていません:

- お使いの NetScaler VPX は 13.1-48.x または 14.1-12.x より古いです。
- お使いのクラウドは SMT をサポートしていません。
- お使いの VM インスタンスタイプは SMT をサポートしていません。たとえば、vCPU 数が 8 を超えています。

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

• SMT 機能はサポートされていますが、有効になっていません。

```
1 > shell sysctl -a | grep smt_handling
2 netscaler.smt_handling_platform: 1 (available)
```

3 netscaler.smt_handling: 0 (not enabled)
4 netscaler.smt_handling_active: 0 (not active)

NetScaler サニティチェッカーツール

October 17, 2024

サニティチェッカーツールは NetScaler の健全性とパフォーマンスを評価します。 また、一般的な構成の問題も特定します。

注

現在、NetScaler サニティチェッカーツールは AWS クラウドでのみサポートされています。

NetScaler サニティチェッカーツールは次のアクティビティも実行します:

- HA トポロジ、ネットワーク、ライセンス、権限を検証します。
- トラブルシューティングプロセスを合理化します。
- パブリッククラウドで発生した問題を迅速に解決できます。
- プレーンテキストログ、JSON、HTML など、複数の形式で結果を生成します。

AWS 向け NetScaler サニティチェッカーツール

NetScaler サニティチェッカーツールは、展開タイプに基づいて以下の検証を行います。

スタンドアロンと同一ゾーンの HA	エラスティック IP アドレスを使用し	プライベート IP アドレスを使用する
デプロイメント	たマルチゾーン HA デプロイ	マルチゾーン HA 展開
 IAM 権限の検証 ライセンスチェック ストレージチェック メタデータのルートチェック DNS 解像度チェック EC2 エンドポイントチェック デフォルトゲートウェイチェック ゲLAN 構成チェック ARP チェック システム ID チェック Cloudbadaemon チェック 	 IAM 権限の検証 インターフェースチェック EIP チェック INC モードチェック IPSet チェック 	 IAM 権限の検証 インターフェースチェック ルートチェック デバイスインデックスチェック ソース/日付チェック

スタンドアロンと同一ゾーンの HA エラスティック IP アドレスを使用し プライベート IP アドレスを使用する デプロイメント たマルチゾーン HA デプロイ マルチゾーン HA 展開

NetScaler CLI を使用してサニティチェッカーツールを実行する

コマンドプロンプトで次のように入力します:

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

サニティチェッカーツールを実行すると、次のファイルが JSON 形式と HTML 形式で生成されます。

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

これらのファイルには、実行されたチェックの詳細な結果が含まれており、潜在的な問題の特定と分析に使用できま す。

NetScaler VPX インスタンスをベアメタルサーバーにインストールする

October 17, 2024

ベアメタルとは、クラウド環境に完全に統合された、物理的に分離された完全専用の物理サーバーです。シングルテ ナントサーバーとも呼ばれます。シングルテナントを使用すると、ノイズの多いネイバー効果を回避できます。ベア メタルでは、自分が唯一のユーザーなので、ノイズの多いネイバー効果は発生しません。

ハイパーバイザーがインストールされたベアメタルサーバーは、サーバー上に仮想マシンを作成するための管理スイ ートを提供します。ハイパーバイザーはアプリケーションをネイティブに実行しません。その目的は、ワークロード を個別の仮想マシンに仮想化して、仮想化の柔軟性と信頼性を高めることです。

NetScaler VPX インスタンスをベアメタルサーバーにインストールするための前提条件

ベアメタルサーバーは、それぞれのハイパーバイザーのすべてのシステム要件を満たすクラウドベンダーから入手す る必要があります。

NetScaler VPX インスタンスをベアメタルサーバーにインストールします

NetScaler VPX インスタンスをベアメタルサーバーにインストールするには、まずクラウドベンダーから十分なシ ステムリソースを備えたベアメタルサーバーを入手する必要があります。そのベアメタルサーバーでは、NetScaler VPX インスタンスを展開する前に、Linux KVM、VMware ESX、Citrix Hypervisor、Microsoft Hyper-V などの サポートされているハイパーバイザーのいずれかをインストールして構成する必要があります。

NetScaler VPX インスタンスでサポートされているさまざまなハイパーバイザーと機能のリストの詳細について は、「サポート マトリックスと使用ガイドライン」を参照してください。

さまざまなハイパーバイザーに NetScaler ADC VPX インスタンスをインストールする方法の詳細については、それ ぞれのドキュメントを参照してください。

- Citrix Hypervisor: 「Citrix Hypervisor に NetScaler VPX インスタンスをインストールする」を参照してください。
- VMware ESX: 「VMware ESX に NetScaler VPX インスタンスをインストールする」を参照してください。
- Microsoft Hyper-V: 「Microsoft Hyper-V サーバーに NetScaler VPX インスタンスをインストールする」 を参照してください。
- Linux KVM プラットフォーム: 「Linux-KVM プラットフォームに NetScaler VPX インスタンスをインスト ールする」を参照してください。

Citrix Hypervisor/XenServer への NetScaler VPX インスタンスのインストール

January 15, 2025

Citrix Hypervisor/XenServer に VPX インスタンスをインストールするには、まず、適切なシステムリソースがあ るマシンにハイパーバイザーをインストールする必要があります。NetScaler VPX インスタンスのインストールを 実行するには、Citrix XenCenter を使用します。Citrix XenCenter は、ネットワーク経由で Hypervisor ホストに 接続できるリモートマシンにインストールする必要があります。

Hypervisor の詳細については、Citrix Hypervisor のドキュメントを参照してください。

次の図は、Hypervisor 上の NetScaler ADC VPX インスタンスのベアメタルソリューションアーキテクチャを示しています。

図. Citrix Hypervisor/XenServer 上の NetScaler VPX インスタンス



Hypervisor に NetScaler ADC VPX インスタンスをインストールするための前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- 最小要件を満たすハードウェアに Hypervisor バージョン 6.0 以降をインストールします。
- 最小システム要件を満たす管理ワークステーションに XenCenter をインストールします。
- 仮想アプライアンスのライセンスファイルを取得します。仮想アプライアンス ライセンスの詳細については、『NetScaler ライセンス ガイド』を参照してください。

Hypervisor のハードウェア要件

次の表は、NetScaler VPX インスタンスを実行するハイパーバイザープラットフォームの最小ハードウェア要件を示しています。

テーブル 1. nCore VPX インスタンスを実行する Hypervisor の最小システム要件

コンポーネント	条件
CPU	仮想化アシスト (Intel-VT) が有効になっている 64 ビッ
	ト x86 CPU が 2 つ以上あります。NetScaler VPX イン
	スタンスを実行するには、Hypervisor ホストで仮想化
	のハードウェアサポートを有効にする必要があります。
	仮想化サポートの BIOS オプションが無効になっていな
	いことを確認してください。詳細については、BIOS の
	ドキュメントを参照してください。
RAM	3 GB
ディフク領域	40 GB のディスク容量を持つローカル接続ストレージ
ノュヘノ浪域	(PATA、SATA、SCSI)。
	手記:ハイパーバイザーをインストールすると、ハイパ
NIC	LGEPSFULSよ基準備標:シアク用にをPBNSパーティシ
	ョンが作成されます。残りのスペースは、NetScaler
	VPX インスタンスやその他の仮想マシンに使用できま
詳細については、XenServer のドキュメント.	す。

次の表に、Hypervisor が各 nCore VPX 仮想アプライアンスに提供する必要がある仮想コンピューティングリソー スを示します。

テーブル 2. nCore VPX インスタンスの実行に必要な最小仮想コンピューティングリソース

注

NetScaler VPX インスタンスを本番環境で使用する場合、スケジューリング動作とネットワーク遅延を改善するために、(仮想マシンプロパティの) CPU 優先度を最高レベルに設定することを Citrix では推奨しています。

XenCenter のシステム要件

XenCenter は、Windows のクライアントアプリケーションです。Hypervisor ホストと同じマシンでは実行でき ません。最小システム要件と XenCenter のインストールについて詳しくは、Hypervisor に関する次のドキュメン トを参照してください。

- システム要件
- インストール

XenCenter を使用して NetScaler VPX インスタンスをハイパーバイザーにインストールする

Hypervisor と XenCenter をインストールして構成したら、XenCenter を使用して Hypervisor に仮想アプライ アンスをインストールできます。インストールできる仮想アプライアンスの数は、Hypervisor を実行しているハー ドウェアで使用可能なメモリの量によって異なります。

XenCenter を使用して Hypervisor に NetScaler ADC VPX インスタンスをインストールするには、次の手順に従 います。

- 1. ワークステーションで XenCenter を起動します。
- 2. [サーバー] メニューの [追加] を選択します。
- 3. [新規サーバーの追加]ダイアログボックスのホスト名テキストボックスに、接続するハイパーバイザーの IP アドレスまたは DNS 名を入力します。
- 4. [User Name] ボックスと [Password] ボックスに管理者資格情報を入力して、[Connect] をクリック します。Hypervisor 名がナビゲーションペインに表示され、Hypervisor が接続されていることを示します。
- 5. ナビゲーションペインで、NetScaler VPX インスタンスをインストールする Hypervisor の名前をクリック します。
- 6. [VM] メニューの [Import] を選択します。
- インポートダイアログボックスのインポートファイル名で、NetScaler VPX インスタンス・xvaイメージフ ァイルを保存した場所を参照します。[エクスポートされた仮想マシン] オプションが選択されていることを確 認し、[次へ] をクリックします。
- 8. 仮想アプライアンスをインストールするハイパーバイザーを選択し、[次へ]をクリックします。
- 9. 仮想アプライアンスを保存するローカルストレージリポジトリを選択して [**Import**] をクリックし、インポ ート処理を開始します。
- **10.** 必要に応じて、仮想ネットワークインターフェイスを追加、変更、または削除できます。完了したら [**Next**] をクリックします。
- 11. [完了]をクリックしてインポートプロセスを完了します。

注

インポート処理の状態を参照するには、[Log] タブをクリックします。

12. 別の仮想アプライアンスをインストールする場合は、手順5~11を繰り返します。

注

VPX インスタンスの初期構成後、アプライアンスを最新のソフトウェアリリースにアップグレードする場合は、「システムソフトウェアのアップグレードまたはダウングレード」を参照してください。

シングルルート I/O 仮想化 (SR-IOV) ネットワークインターフェイスを使用するように VPX インスタンスを構成する

January 30, 2025

NetScaler VPX インスタンスを Citrix Hypervisor にインストールして構成したら、SR-IOV ネットワークインタ ーフェイスを使用するように仮想アプライアンスを構成できます。

次の NIC がサポートされています。

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

制限事項

Citrix Hypervisor は、SR-IOV インターフェイスの一部の機能をサポートしていません。Intel 82599、Intel X710、 および Intel XL710 NIC の制限は、次のセクションに記載されています。

Intel 82599 NIC の制限事項

Intel 82599 NIC は次の機能をサポートしていません。

- L2 モード切り替え
- クラスタリング
- 管理パーティション化 [共有 VLAN モード]
- 高可用性 [アクティブ/アクティブモード]
- ジャンボフレーム
- クラスター環境の IPv6 プロトコル

Intel X710 10G および Intel XL710 40G NIC の制限事項

Intel X710 10G および Intel XL710 40G NIC には次の制限があります。

- L2 モードの切り替えはサポートされていません。
- 管理パーティショニング(共有 VLAN モード)はサポートされていません。
- クラスタでは、XL710 NIC がデータ・インタフェースとして使用されている場合、ジャンボフレームはサポートされません。
- インターフェイスが切断され、再接続されると、インターフェイスリストが順序変更されます。

- スピート、デュプレックス、オートネゴシエーションなどの Interface パラメーター構成はサポートされません。
- Intel X710 10 G と Intel XL710 40G NIC の両方で、インターフェイスは 40/x インターフェイスとして表示 されます。
- VPX インスタンスでサポートできる Intel X710/XL710 SR-IOV インターフェイスは 16 個までです。

```
注
```

Intel X710 10G および Intel XL710 40G NIC が IPv6 をサポートするには、Citrix Hypervisor ホストで次のコマンドを入力して、仮想機能(VF)のトラストモードを有効にします。

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

例

ip link set ens785f1 vf 0 trust on

Intel 82599 NIC の前提条件

Citrix Hypervisor ホストで、次のことを確認してください。

- インテル 82599 NIC (NIC) をホストに追加します。
- /etc/modprobe.d/blacklist.conf ファイルに次のエントリを追加して、ixgbevfドライバを一覧表示 することを禁止します。

blacklist ixgbevf

 /etc/modprobe.d/blacklist.conf ファイルで、以下のエントリを追加して、SR-IOV Virtual Functions (VF) を有効にします。

options ixgbe max_vfs=*<number_of_VFs>*

ここで、<number_VFs>は、作成する SR-IOV VF の数です。

• BIOS で SR-IOV が有効になっていることを確認します。

```
注
IXGBE ドライバーのバージョン 3.22.3 をお勧めします。
```

Citrix Hypervisor ホストを使用して、**Intel 82599 SR-IOV VF** を **NetScaler VPX** インスタンスに 割り当てます

Intel 82599 SR-IOV VF を NetScaler VPX インスタンスに割り当てるには、次の手順に従います。

1. Citrix Hypervisor ホストで、次のコマンドを使用して SR-IOV VF を Citrix ADC VPX インスタンスに割り 当てます。 **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>*

各項目の意味は次のとおりです:

- *<Xen host UUID*>Citrix Hypervisor の UUID です。
- *<NetScaler VM UUID>*は、NetScaler VPX インスタンスの UUID です。
- ・ <interface name> は SR-IOV VF のインターフェイスです。
- <MAC address > は SR-IOV VF の MAC アドレスです。
- 注

args: mac= パラメータで使用する MAC アドレスを指定します。指定しない場合、iovirtスクリ プトはランダムに MAC アドレスを生成して割り当てます。また、リンクアグリゲーションモードで SR-IOV VF を使用する場合は、必ず MAC アドレスを 00:00:00:00:00 と指定します。

2. NetScaler VPX インスタンスを起動します。

Citrix Hypervisor ホストを使用して、**Intel 82599 SR-IOV VF** を **NetScaler VPX** インスタンスに 割り当て解除します

正しくない SR-IOV VF を割り当てた場合、または割り当てられた SR-IOV VF を変更する場合は、SR-IOV VF を Citrix ADC VPX インスタンスに割り当て解除して再割り当てする必要があります。

NetScaler VPX インスタンス に割り当てられた SR-IOV ネットワークインターフェイスの割り当てを解除するには、 次の手順に従います。

1. Citrix Hypervisor ホストで、次のコマンドを使用して SR-IOV VF を Citrix ADC VPX インスタンスに割り 当て、NetScaler VPX インスタンスを再起動します。

xe host-call-plugin plugin=iovirt **host-uuid**=*Xen_host_UUID>***fn**=unassign_all **args:uuid**=*Netscaler_VM_*し 各項目の意味は次のとおりです:

- *<Xen_host_UUID>*-Citrix Hypervisor ホストの UUID。
- *<Netscaler_VM_UUID>*-NetScaler VPX インスタンスの UUID
- 2. NetScaler VPX インスタンスを起動します。

Citrix Hypervisor ホストを使用して、**Intel X710/XL710 SR-IOV VF** を **NetScaler VPX** インスタ ンスに割り当てます

Intel X710/XL710 SR-IOV VF を NetScaler VPX インスタンスに割り当てるには、次の手順に従います。

1. Citrix Hypervisor ホストで次のコマンドを実行して、ネットワークを作成します。

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

例

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

2. SR-IOV ネットワークを構成する NIC の PIF ユニバーサルー意識別子 (UUID) を決定します。

3. ネットワークを SR-IOV ネットワークとして設定します。次のコマンドは、新しく作成された SR-IOV ネット ワークの UUID も返します。

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

例

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

SR-IOV ネットワークパラメーターの詳細情報を取得するには、次のコマンドを実行します。

4. 仮想インターフェイス (VIF) を作成し、ターゲット VM にアタッチします。

注

VM の NIC インデックス番号は 0 で始まる必要があります。

VM UUID を見つけるには、次のコマンドを使用します。

```
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
```

Citrix Hypervisor ホストを使用して **NetScaler** インスタンスから **Intel X710/XL710 SR-IOV VF** を削除します

NetScaler VPX インスタンスから Intel X710/XL710 SR-IOV VF を削除するには、次の手順に従います。

- 1. 破棄する VIF の UUID をコピーします。
- 2. VIF を破棄するには、Citrix Hypervisor ホスト上で以下のコマンドを実行します。

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

例

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

SR-IOV インターフェイスでのリンクアグリゲーションの設定

SR-IOV 仮想機能 (VF) をリンクアグリゲーションモードで使用するには、作成した仮想機能のスプーフィングチェッ クを無効にする必要があります。

Citrix Hypervisor ホストで、次のコマンドを使用してスプーフィングチェックを無効にします。

ip リンクセット ** <interface_name>vf ** <VF_id>spoofchk オフ

各項目の意味は次のとおりです:

- <interface_name> は、インターフェイス名です。
- <VF_id> は、仮想機能 ID です。

作成したすべての仮想機能のスプーフィングチェックを無効にした後、NetScaler VPX インスタンスを再起動し、リ ンクアグリゲーションを設定します。手順については、「リンク集約の設定」を参照してください。

重要:

SR-IOV VF を Citrix ADC VPX インスタンスに割り当てるときは、VF の MAC アドレス 00:00:00:00:00 を必 ず指定してください。

SR-IOV インターフェイスで VLAN を設定します

SR-IOV 仮想機能に VLAN を設定できます。手順については、「VLAN の設定」を参照してください。

重要:

Citrix Hypervisor ホストに VF インターフェイスの VLAN 設定が含まれていないことを確認してください。

その他の参考資料

SR-IOV 対応 NIC

SR-IOV ネットワークを追加する

VMware ESX に Citrix ADC VPX インスタンスをインストールする

October 17, 2024

NetScaler VPX インスタンスを VMware ESX にインストールする前に、VMware ESX サーバーが適切なシステ ムリソースを備えたマシンにインストールされていることを確認してください。NetScaler VPX インスタンスを VMware ESXi にインストールするには、VMware vSphere クライアントを使用します。これらのクライアントソフ トウェアは、ネットワーク経由で VMware ESX に接続できるリモートマシンにインストールする必要があります。

このセクションでは、以下のトピックについて説明します。

- 前提条件
- VMware ESX に Citrix ADC VPX インスタンスをインストールする

重要:

NetScaler VPX インスタンスで標準の VMware Tools をインストールしたり、VMware Tools バージョンを アップグレードしたりすることはできません。NetScaler VPX インスタンス用の VMware ツールは、Citrix ADC ソフトウェアリリースの一部として提供されます。

前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- 最小要件を満たすハードウェアに VMware ESX をインストールします。
- 最小システム要件を満たす管理用のワークステーションに VMware Client をインストールします。
- NetScaler VPX アプライアンスセットアップファイルをダウンロードします。
- 仮想スイッチを作成し、物理 NIC を仮想スイッチに接続します。
- ポートグループを追加し、仮想スイッチに接続します。

- ポートグループを VM に接続します。
- VPX ライセンスファイルを入手します。NetScaler VPX インスタンスライセンスの詳細については、「ライセンスの概要」を参照してください。

VMware ESX のハードウェア要件

次の表では、NetScaler VPX nCore 仮想アプライアンスを実行している VMware ESX サーバーの最小システム要件について説明します。

コンポーネント	条件
СРИ	仮想化アシスト (Intel-VT) が有効になっている 64 ビッ
	ト x86 CPU が 2 つ以上あります。NetScaler VPX イン
	スタンスを実行するには、仮想化のハードウェアサポー
	トが VMware ESX ホストで有効になっている必要があ
	ります。仮想化サポートの BIOS オプションが無効にな
	っていないことを確認します。詳しくは、BIOS のドキ
	ュメントを参照してください。NetScaler 13.1 リリー
	ス以降、VMware ESXi ハイパーバイザー上の
	NetScaler VPX インスタンスは AMD プロセッサをサポ
	ートしています。
RAM	2GB VPX。2 ギガバイトの VPX 重要な展開では、シス
	テムがメモリに制約のある環境で動作するため、VPX に
	2 GB の RAM を使用することはお勧めしません。これに
	より、スケール、パフォーマンス、または安定性に関連
	する問題が発生する可能性があります。推奨されるのは
	4 GB の RAM または 8 GB の RAM です。
ディスク領域	ESXi をセットアップするための VMware の最小サーバ
	要件よりも 20 GB 多くなっています。サーバの最小要件
	については、VMware のマニュアルを参照してください。
ネットワーク	1Gbps NIC (NIC)1つ、1Gbps NIC を2つ推奨

表 1. NetScaler VPX インスタンスを実行する VMware ESX サーバーの最小システム要件

VMware ESX のインストールについては、http://www.vmware.com/を参照してください。

SR-IOV ネットワークインターフェイスまたは PCI パススルーをサポートするには、次のプロセッサと設定が有効に なっていることを確認してください。

- Intel VT をサポートする Intel ・プロセッサー
- AMD-V をサポートする AMD プロセッサー

• 入出力メモリ管理ユニット (IOMMU) または SR-IOV が BIOS で有効になっています

SR-IOV モードでは次の NIC がサポートされます。

- Mellanox ConnectX-4 NIC (Citrix ADC リリース 13.1-42.x 以降)
- Intel 82599 NIC

次の表に、VMware ESX サーバが各 VPX nCore 仮想アプライアンスに対して提供する必要がある仮想コンピューティングリソースを示します。

表 2. NetScaler VPX インスタンスの実行に必要な最小限の仮想コンピューティングリソース

```
これは、ハイパーバイザーのディスク要件に加えて必要になります。
```

VPX 仮想アプライアンスを本番環境で使用するには、完全なメモリ割り当てを予約する必要があります。少なくとも ESX の 1 つの CPU コアの速度に等しい CPU サイクル (MHz) を予約する必要があります。

VMware vSphere クライアントのシステム要件

VMware vSphere Client は、Windows および Linux の各オペレーティングシステムで実行できるクライアント アプリケーションです。VMware ESX サーバと同じマシンでは実行できません。次の表は、最小システム要件を示し ています。

表 3. VMware vSphere クライアントインストールの最小システム要件

コンポーネント	条件
オペレーティングシステム	VMware からの詳細な要件については、 http://kb.vmware.com/で「vSphere 互換性マトリ ックス」PDF ファイルを検索してください。
CPU	750 MHz。1 ギガヘルツ (GHz) 以上推奨
RAM	1GB. 2GB を推奨
NIC (NIC)	100Mbps 以上の NIC。

OVF ツール 1.0 のシステム要件

Open Virtualization Format Tool (OVF Tool) は、Windows および Linux システムで実行できるクライアント アプリケーションです。VMware ESX サーバと同じマシンでは実行できません。次の表は、最小システム要件を示し ています。

表 4. OVF ツールのインストールに必要な最小システム要件

コンポーネント	条件
オペレーティングシステム	VMware からの詳細な要件については、
	http://kb.vmware.com/で『OVF ツールユーザーガ
	イド』の PDF ファイルを検索してください。
CPU	最低 750MHz、1GHz 以上推奨
RAM	最小1GB、推奨2GB
NIC (NIC)	100Mbps 以上の NIC。

OVF のインストールについては、http://kb.vmware.com/で『OVF ツールユーザーガイド』の PDF ファイルを検 索してください。

NetScaler VPX セットアップファイルのダウンロード

VMware ESX 用の NetScaler VPX インスタンスセットアップパッケージは、オープン仮想マシン(OVF)フォーマット標準に準拠しています。これらのファイルは、Citrix Web サイトからダウンロードできます。ログオンするには、Citrix アカウントが必要です。Citrix アカウントをお持ちでない場合は、http://www.citrix.comのホームページにアクセスし、[新規ユーザー] リンクをクリックし、指示に従って Citrix アカウントを作成します。

ログオンしたら、Citrix のホームページから次のパスをナビゲートします。

Citrix.com > ダウンロード > NetScaler > 仮想アプライアンス。

次のファイルを、ESX サーバーと同じネットワーク上のワークステーションにコピーします。3 つのファイルをすべ て同じフォルダーにコピーします。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (た と え ば、nsvpx-esx-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (たとえば、nsvpx-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf(たとえば、nsvpx-esx-13.0-71.44_nc_64.mf)

VMware ESX に Citrix ADC VPX インスタンスをインストールする

VMware ESX をインストールして構成したら、VMware vSphere Client を使用して VMware ESX サーバーに仮 想アプライアンスをインストールします。インストールできる仮想アプライアンスの数は、VMware ESX を実行す るハードウェアで使用可能なメモリの量によって決まります。

VMware vSphere クライアントを使用して NetScaler VPX インスタンスを VMware ESX にインストールするに は、以下の手順に従ってください。

- 1. ワークステーション上で VMware vSphere Client を起動します。
- 2. [IP address / Name] テキストボックスに、接続する VMware ESX サーバーの IP アドレスを入力します。
- 3. [ユーザー名] テキストボックスと [パスワード] テキストボックスに、管理者の認証情報を入力し、[ログイン] をクリックします。
- 4. [File] メニューの [Deploy OVF Template] を選択します。
- 5. [**OVF** テンプレートのデプロイ] ダイアログボックスの [ファイルからデプロイ] で、NetScaler VPX インス タンスセットアップファイルを保存した場所を参照し、.ovf ファイルを選択して、[次へ] をクリックします。
- 仮想アプライアンス OVF テンプレートに示されるネットワークを、ESX ホストで構成したネットワークにマップします。[Next] をクリックして、VMware ESX への仮想アプライアンスのインストールを開始します。 インストールが完了すると、ポップアップウィンドウによって正常にインストールされたことが通知されます。
- 7. これで、NetScaler VPX インスタンスを起動する準備ができました。ナビゲーションペインで、インストー ルした Citrix ADC VPX インスタンスを選択し、右クリックメニューから [パワーオン] を選択します。
- 8. 仮想マシンを起動したら、コンソールから Citrix ADC IP、ネットマスク、およびゲートウェイアドレスを設 定します。設定が完了したら、コンソールで [**Save and Quit**] オプションを選択します。
- 9. 別の仮想アプライアンスをインストールするには、ステップ6からステップ8までを繰り返します。

注

デフォルトでは、NetScaler VPX インスタンスは E1000 ネットワークインターフェイスを使用します。

インストール後、vSphere クライアントまたは vSphere Web Client を使用して VMware ESX 上の仮想ア プライアンスを管理できます。

VMware ESX で VLAN タグ付けを有効にするには、vSwitch でポート グループの VLAN ID をすべて (4095) に設定します。vSwitch で VLAN ID を設定する詳細な手順については、VMware のドキュメントを参照して ください。

VMware vMotion を使用して Citrix ADC VPX インスタンスを移行する

VMware vSphere vMotion を使用して、NetScaler VPX インスタンスを移行できます。

使用上のガイドラインに従ってください。

• VMware は、PCI パススルーおよび SR-IOV インターフェイスで構成された仮想マシンでは vMotion 機能を サポートしていません。

- サポートされているインターフェイスは、E1000 と VMXNET3 です。VPX インスタンスで vMotion を使用 するには、サポートされているインターフェイスでインスタンスが設定されていることを確認します。
- VMware vMotion を使用してインスタンスを移行する方法の詳細については、VMware のドキュメントを参照してください。

VMXNET3 ネットワークインターフェイスを使用するように NetScaler VPX インス タンスを構成する

October 17, 2024

VMware ESX に NetScaler VPX インスタンスをインストールして構成したら、VMware vSphere Web クライア ントを使用して、VMXNET3 ネットワークインターフェイスを使用するように仮想アプライアンスを構成できま す。

VMware vSphere Web クライアントを使用して VMXNET3 ネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成するには:

- 1. vSphere Web クライアントで、ホストとクラスタを選択します。
- 2. 次のように、NetScaler VPX インスタンスの互換性設定を ESX にアップグレードします。
 - a. NetScaler VPX インスタンスの電源を切ります。

b. NetScaler VPX インスタンスを右クリックし、「互換性」>「仮想マシンの互換性のアップグレード」を選択します。

c. 「仮想マシンの互換性の設定」ダイアログボックスで、「互換性」ドロップダウンリストから「ESXi 5.5 以降」を選択し、「OK」をクリックします。

3. NetScaler VPX インスタンスを右クリックし、[設定の編集] をクリックします。

(intual Handwara VMC	Potions SDBS Bulas	LuA	nn Ontion	2		~
		VA	pp Option	5		
CPU	2	-	0			
Memory	2048	-	MB	-		
📇 Hard disk 1	20	*	GB	-		
G 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	batibil	lity Upgra	de		
Newboli						

4. [<virtual_appliance> 設定の編集] ダイアログボックスで、[CPU] セクションをクリックします。

/irtual Hardware VM Options	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
New device:	Select Add

5. [CPU] セクションで、以下を更新します。

- CPU の数
- ソケット数
- 予約
- 上限
- 共有

値を次のように設定します:

a. CPU ドロップダウンリストで、仮想アプライアンスに割り当てる CPU の数を選択します。

b. [予約] ドロップダウンリストで、最大値として表示される番号を選択します。

c. (オプション) [CPU ホットプラグ] フィールドで、[CPU ホットアドを有効にする] チェックボックスをオ ンまたはオフにします。

注

Citrix では、デフォルト (無効) を受け入れることをお勧めします。

d. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

-		ons	Opti	vApp	SDRS Rules	VM Options	Virtual Hardware
		0	•		4		🗸 📕 *CPU
	4	Sockets:	-		1	ocket	Cores per So
			d	J Hot Ad	Enable CPU	g	CPU Hot Plu
	-	MHz	-		0		Reservation
	-	MHz		: 0 MHz	Current value		Limit
1	-	4000		0 MHz	Minimum:		Shares
Advar	-	guest	Hz	8396 M	Maximum:		CPUID Mask
n to the	zatio	ted virtualiz	ssis	dware a:	Expose har	tualization	Hardware vir
ounters	ce co	performan	PUp	alized C	🗌 Enable virtu	counters	Performance
CPUs)	ical	s: Active 24 (log	tatus	eading S CPUs:	Hyperthre Available	ffinity	Scheduling /
\dd	ŀ	 +]		:t	Selec	evice:	New d

e. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

Virtual Hardware	VM Options	SDRS Rules	vApp Op	otions		
🕶 🔲 *CPU		4	-	0		
Cores per So	cket	1	-	Sockets:	4	
CPU Hot Plug	i I	Enable CP	J Hot Add			
Reservation	(*)	8396	-	MHz	-	
Limit		Unlimited	-	MHz	•	
Shares		Current value	: Unlimited	4000	1	
CPUID Mask	CPUID Mask		Minimum: 8396 MHz		→ Adv	a
Hardware virt	ualization	Maximum:	Unlimited	s <mark>t</mark> ed virtuali	zation to th	he
Performance	counters	📃 Enable virtu	alized CPU	performan	ce counte	rs
Scheduling A	finity	Hyperthre Available	eading Stati CPUs:	us: Active 24 (log	gical CPUs	s)
New de	evice:	Selec	:t	-	Add	

f. [共有] ドロップダウンリストで、[カスタム] を選択し、最大値として表示される数を指定します。

Virtual Hardware V	M Options	SDRS Rules	vApp Opt	ions			
🕶 🔲 *CPU		4	•	0			
Cores per Socket		1	Sockets: 4				
CPU Hot Plug		Enable CPU I	Hot Add				
Reservation (*)		8396		MHz	-		
Limit		Unlimited	-	MHz	-		
Shares (*) CPUID Mask		Custom		4000	-		
				linimum 0 Adva			n
Hardware virtua	lization	Expose hardv	mum 10000 n to th			9	
Performance co	unters	Enable virtualized CPU performance counters					
Scheduling Affin	ity	Hyperthrea Available C Select logical pro	ding Statu PUs: pcessor al	s: Active 24 (log finity for th	gical is virt	CPUs) ual ma	1
New devi	ce:	Select -		-	A	dd	

6. [メモリ] セクションで、次の項目を更新します。

- メモリのサイズ
- 予約
- 上限
- 共有

値を次のように設定します:

a. [RAM] ドロップダウンリストで、RAM のサイズを選択します。これは vCPU の数 x 2 GB でなければなりません。たとえば、vCPU の数が 4 の場合、RAM は 4 x 2 GB = 8 GB でなければなりません。

注

NetScaler VPX アプライアンスの Advanced または Premium エディションの場合は、各 vCPU に 4 GB の RAM を割り当てるようにしてください。たとえば、vCPU の数が 4 の場合、RAM = 4×4GB = 16GB になります。

tual Hardware VM Optio	ons	SDRS Rules	vApp O	pti	ons			
* CPU	(4		-)	0			-
Kemory								
RAM (*)		8396		-)	MB	-	ĺ	
Reservation		0		-)	MB	-		
	[Reserve all g	uestme	mo	ory (All loci	(ed)		
Limit		Unlimited		-	MB	-		
Shares		Normal		-)	83960	-		
Memory Hot Plug	1	Enable						
Hard disk 1		20			GB	-	ĺ	
SCSI controller 0		LSI Logic Parall	el					
🗾 Network adapter 1		VM Network			-	⊡ c	;0	
Network adapter 2	(1/2				•	⊻ c	;0
New device:		Select			_	1	Add	

b. [予約] ドロップダウンリストで、メモリ予約の値を入力し、[すべてのゲストメモリを予約する (すべてのロック済み)] チェックボックスをオンにします。メモリ予約は vCPU の数 x 2 GB である必要があります。たと えば、vCPU の数が 4 の場合、メモリ予約は 4 x 2 GB = 8 GB である必要があります。

注

NetScaler VPX アプライアンスの Advanced または Premium エディションの場合は、各 vCPU に 4 GB の RAM を割り当てるようにしてください。たとえば、vCPU の数が 4 の場合、RAM = 4×4GB = 16GB になります。

/irtual Hardware VM Optio	ons	SDRS Rules	vApp Opt	ions			
T *CPU		4	-	0			
Memory							
RAM (*)		8192	-	MB	-		
Reservation (*)		8192	*	MB	-		
		Z Reserve all g	uestmem	ory (All loc	ked)		
Limit		Unlimited	-	MB	-		
Shares	(Normal	-	81920	-		
Memory Hot Plug	Ľ] Enable					
🕨 🛄 Hard disk 1		20	×	GB	-		
G SCSI controller 0	L	SI Logic Parall	el				
🕨 飅 Network adapter 1		VM Network			-	СC	0
📕 Network adapter 2	(1/2			•	∎c	0
New device:		Select		-	A	dd	1

c. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

irtual Hardware VM Optio	ons SDRS Rule	s VApp Op	tions		
CPU *CPU	4		0		
Memory					
RAM (*)	8192	-	MB	•	
Reservation (*)	8192	-	MB	-	
	Reserve al	Iguestmen	nory (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	VM Network			✓ Co
Metwork adapter 2	1/2			•	Z Co
New device:	Sele	ct		Ad	d

d. [共有] ドロップダウンリストで、[カスタム] を選択し、最大値として表示される数を指定します。

Virtual Hardware VM Option	s SDRS Rules	vApp Opti	ons		
• 🔲 *CPU	4	•	0		
Memory					
RAM (*)	8192	-	MB	-	
Reservation (*)	8192	-	MB	-	
	Reserve all g	guestmem	ory (All loci	ked)	
Limit	Unlimited	-	MB	-	
Shares (*)	Custom	-	00000	-	
Memory Hot Plug	Enable	Minir	num 1		
- 🛄 Hard disk 1	20	Maxi	mum 100(00	
G SCSI controller 0	LSI Logic Paral	lel			
🗾 Network adapter 1	VM Network			$\left \cdot \right $	∎ co
Network adapter 2	1/2			•	⊻ Co
New device:	Select			A	bb

7. VMXNET3 ネットワークインターフェイスを追加します。[新しいデバイス] ドロップダウンリストから [ネットワーク] を選択し、[追加] をクリックします。

🔂 NSVPX-DEMO - Edit S	ettings	(? »
Virtual Hardware VM O	ptions SDRS Rules vA	App Options
▶ ■ *CPU	4	• 0
► Memory	New Hard Disk	▼ MB ▼
Hard disk 1	Existing Hard Disk	GB V
▶ G SCSI controller 0	🖧 RDM Disk	
Network adapter 1	Network	Connect
Network adapter 2		Connect
🕨 🛄 Video card	CD/DVD Drive	tings 🗸
► 🎲 VMCI device	Floppy Drive	
 Other Devices 	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 an	d later (VM version 10)	OK Cancel

8. [New Network] セクションのドロップダウンリストからネットワークインターフェイスを選択し、次の操作 を行います。

a. [アダプタ タイプ] ドロップダウン リストで、[VMXNET3] を選択します。

重要:

デフォルトの E1000 ネットワークインターフェイスと VMXNET3 は共存できないため、E1000 ネット ワークインターフェイスの削除を確認して、VMXNET3 (0/1) を管理インターフェイスとして使用しま す。

🚯 NSVPX-ESX - Edit Settings		? ₩
Virtual Hardware VM Options	SDRS Rules VApp Options	
> 🔲 CPU	4 • •	
▶ 🌆 Memory	8192 • MB •	
▶ 🛄 Hard disk 1	20 GB V	
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
▶ 飅 Network adapter 1	VM Network	
▶ 🛄 Video card	Specify custom settings	
▶ i 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 -	
	VINANET 5	
New device:	Metwork - Add	
Compatibility: ESXi 6.0 and later (VM version 11) OK C	ancel

- 9. [作成]または[**OK**]をクリックします。
- 10. NetScaler VPX インスタンスをパワーオンします。
- 11. NetScaler VPX インスタンスの電源が入ったら、次のコマンドを使用して構成を確認できます。

インターフェイスの概要を表示

出力には、設定したすべてのインターフェイスが表示されている必要があります。

1	> :	show int	t erface summary			
~						
3		Inte	erface MTU	MAC	Suffix	
4						
5	1	0/1	1500	00:0c:29:89:1d:0e	NetScaler Vir	
		rface,	VMXNET3			
6	2	1/1	9000	00:0c:29:89:1d:18	NetScaler Vir	
		rface,	VMXNET3			
7	3	1/2	9000	00:0c:29:89:1d:22	NetScaler Vir	
		rface,	VMXNET3			

8 4 LO/1 9000 00:0c:29:89:1d:0e Netscaler Loopback interface

注

VMXNET3 インターフェイスを追加して NetScaler VPX アプライアンスを再起動すると、VMware ESX ハイ パーバイザーによって NIC が VPX アプライアンスに提示される順序が変更されることがあります。そのため、 ネットワークアダプター1が常に 0/1 のままであるとは限らず、その結果 VPX アプライアンスに対する管理接 続が失われることがあります。この問題を回避するには、ネットワークアダプターの仮想ネットワークを変更 します。

これは VMware ESX ハイパーバイザの制限です。

VMXNET3 ネットワークインターフェイスの受信リングサイズの設定

VMware ESX の VMXNET3 ネットワークインターフェイスの受信リングサイズを増やすことができます。リングサ イズを大きくすると、トラフィックの突然のバーストが発生したときのパケットドロップが減少します。

注

この機能は、リリース 14.1 ビルド 14.x 以降で使用できます。

VMXNET3 ネットワークインターフェイスのリングサイズを設定するには

コマンドプロンプトで入力します:

set interface id [-ringsize *positive_integer*]

VMXNET3 インターフェイスに設定できる最大リングサイズは 2048 です。固定リングタイプのみがサポートされて います。設定を有効にするには、構成を保存して NetScaler VPX インスタンスを再起動する必要があります。

SR-IOV ネットワークインターフェイスの使用を NetScaler ADC VPX インスタンス で構成する

October 17, 2024

VMware ESX に Citrix ADC VPX インスタンスをインストールして構成した後、VMware vSphere Web クライア ントを使用して、シングルルート I/O 仮想化 (SR-IOV) ネットワークインターフェイスを使用するように仮想アプラ イアンスを構成できます。
制限事項

SR-IOV ネットワークインターフェイスで構成された NetScaler VPX には、以下の制限事項があります。

- 次の機能は、ESX VPX 上の Intel 82599 10G NIC を使用する SR-IOV インターフェイスではサポートされて いません。
 - L2 モード切り替え
 - スタティックリンク集約および LACP
 - クラスタリング
 - 管理パーティション化 [共有 VLAN モード]
 - 高可用性 [アクティブ/アクティブモード]
 - ジャンボフレーム
 - IPv6
- KVM VPX 上の Intel 82599 10G NIC を搭載した SR-IOV インターフェイスでは、次の機能はサポートされ ていません。
 - スタティックリンク集約および LACP
 - L2 モード切り替え
 - クラスタリング
 - 管理パーティション化 [共有 VLAN モード]
 - 高可用性[アクティブ-アクティブモード]
 - ジャンボフレーム
 - IPv6
 - ip linkコマンドによる SR-IOV VF インターフェイスのハイパーバイザでの VLAN 設定はサポート されていません

前提要件

- 必ず ESX ホストに次のいずれかの NIC を追加してください。
 - Intel 82599 NIC、IXGBE ドライバーバージョン 3.7.13.7.14iov 以降が推奨されます。
 - Mellanox ConnectX-4 NIC
- ホスト物理アダプタで SR-IOV を有効にします。

以下の手順に従って、ホスト物理アダプタで SR-IOV を有効にします。

- 1. vSphere Web クライアントで、ホストに移動します。
- [管理]>[ネットワーク] タブで、[物理アダプター]を選択します。[SR-IOV Status] フィールドに、物 理アダプターが SR-IOV をサポートしているかどうかが表示されます。

Navigator I	🔂 10.102.38.201 Actions 👻			-
Home	Getting Started Summary M	onitor Manage Relate	d Objects	
Image: Constraint of the second sec	Settings Networking Storage	Alarm Definitions Tags	Permissions	
▼ Im VPX ▶ Im 10.102.100.106 ▶ Im 10.102.38.201	√ Virtual switches	Physical adapters		
10.217.195.204	VMkernel adapters	Observed IP ranges	Wake on LAN Support	SR-IOV Status
10.217.195.220	Physical adapters	No networks	No	Disabled
TCP/IP configurat	TCP/IP configuration	No networks	No	Disabled
	Advanced	No networks	No	Enabled
	Advanced	No networks No networks	No No	Enabled Disabled
	Advanced	No networks No networks No networks	No No No	Enabled Disabled Disabled

3. 物理アダプタを選択し、鉛筆アイコンをクリックして [設定の編集] ダイアログボックスを開きます。

vmware [®] vSphere	e Web Client † ≘	Õ L A	dministrator@VSPHERE	LOCAL - Help
Navigator	🔂 10.102.38.201 Actions 👻			≡▼
Home	Getting Started Summary	Monitor Manage Relate	d Objects	
▼ 🖓 10.102.38.250	Settings Networking Storag	e Alarm Definitions Tags	Permissions	
VPX ► ■ 10.102.100.10 ► ■ 10.102.38.20	06 1 Virtual switches	Physical adapters	A Filter	•
 10.217.195.20 10.217.195.20 	04 VMkernel adapters	Observer P ranges	Wake on LAN Support	. SR-IOV Status
M 10.217.155.2	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 👻
		•		•
		Physical network adapte	er: vmnic5	
		All Properties Cl	DP LLDP	
		Adapter	Intel Cor 10 Gigal Network	poration 82599 Abit Dual Port Connection
		Name	vmnic5	::

4.「SR-IOV」で、「ステータス」ドロップダウンリストから「有効」を選択します。

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	ows multiple virtual machines a virtual pass-through device.
Glatus.	Enabled
Number of virtual functions:	Disabled
📌 Changes will not take effec	t until the system is restarted.
	OK Cancel

5. [仮想関数の数] フィールドに、アダプタに対して構成する仮想関数の数を入力します。

💌 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:	lows multiple virtual machines s a virtual pass-through device. Enabled	
Number of virtual functions:	1	Ì
📌 Changes will not take effec	t until the system is restarted.	
	OK Canc	el

- 6. [作成]または[**OK**]をクリックします。
- 7. ホストを再起動します。
- 分散仮想スイッチ (DVS) とPortgroupsを作成します。手順については、VMwareのドキュメントを参照 してください。

```
注
```

Citrix は、DVS およびPortgroupsでのみ SR-IOV 構成を認定しています。

VMware vSphere Web クライアントを使用して SR-IOV ネットワークインターフェイスを使用するように Citrix ADC VPX インスタンスを構成するには:

- 1. vSphere Web クライアントで、ホストとクラスタを選択します。
- 2. 次のように、NetScaler VPX インスタンスの互換性設定を ESX 5.5 以降にアップグレードします。

a. NetScaler VPX インスタンスの電源を切ります。

b. NetScaler VPX インスタンスを右クリックし、「互換性」>「仮想マシンの互換性のアップグレード」を選択します。

c. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

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	

3. NetScaler VPX インスタンスを右クリックし、[設定の編集] をクリックします。

/irtual Hardware VM C	ontions SDRS Rules	VA	nn Ontion	_		
			pp option	<u> </u>		
CPU	2		0			
Memory	2048	•	MB	-)	
🛄 Hard disk 1	20	*	GB	-)	
G SCSI controller 0	LSI Logic Parallel					
属 Network adapter 1	VM Network			-	🗹 Connect	
📕 Network adapter 2	1/2			-	Connect	
Uideo card	Specify custom settin	gs		-)	
🔅 VMCI device						
Other Devices						
Upgrade	Schedule VM Comp	atibi	lity Upgrad	de		
200 St (0	Select		_	-	Add	
New device:		1		_		

4. [**<virtual_appliance> 設定の編集] ダイアログボックスで、[CPU**] セクションをクリックします。

/irtual Hardware VM Options	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
New device:	Select Add

5. [CPU] セクションで、次の設定を更新します。

- CPU の数
- ソケット数
- 予約
- 上限
- 共有

値を次のように設定します:

a. **CPU** ドロップダウンリストで、仮想アプライアンスに割り当てる CPU の数を選択します。

b. [予約] ドロップダウンリストで、最大値として表示される番号を選択します。

c. (オプション)「**CPU** ホットプラグ」フィールドで、「**CPU** ホットアドを有効にする」チェックボックスをオ ンまたはオフにします。

注

Citrix では、デフォルト (無効) を受け入れることをお勧めします。

d. [共有] ドロップダウンリストで、[カスタム] を選択し、最大値として表示される数値を選択します。

		ions	vApp Opti	SDRS Rules	VM Options	/irtual Hardware
		0	-	4		T *CPU
2	ets: 4	Socket	-	1	ocket	Cores per So
			lot Add	Enable CPU	g	CPU Hot Plu
)	-	MHz	-	D		Reservation
)	•	MHz	MHz	Current value:		Limit
)	0 -	4000	MHz	Minimum:		Shares
Adva	+	guest	396 MHz	Maximum:	:	CPUID Mask
on to th	ualizatio	ted virtu:	are assis	Expose hard	tualization	Hardware vir
counter	nance c	performa	zed CPU (Enable virtua	counters	Performance
I CPUs	ive (logical	s: Activ 24 (I	ding Statu: PUs:	Hyperthre Available (Affinity	Scheduling A
Add	٩ <u>(</u>			Select	evice:	New d

e. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

Virtual Hardware	VM Options	SDRS Rules	vApp Op	tions	
🕶 🔲 *CPU		4	-	0	
Cores per Soc	:ket	1	-) Sockets:	4
CPU Hot Plug		Enable CPU	J Hot Add		
Reservation (*)	8396	-	MHz	-
Limit		Unlimited		MHz	-
Shares		Current value: Unlimited		4000	-
CPUID Mask		Minimum:	8396 MHz	guest	+ Adva
Hardware virtu	alization	Maximum:	Unlimited	ted virtualiz	zation to th
Performance of	counters	📃 Enable virtu	alized CPU	performan	ce counter:
Scheduling Af	finity	Hyperthre Available	ading Stati CPUs:	us: Active 24 (log	ical CPUs
New de	vice:	Selec	t	.	Add

f. [共有] ドロップダウンリストで、[カスタム] を選択し、最大値として表示される数を指定します。

Virtual Hardware VM Opti	ons	SDRS Rules	vApp	Optio	ons		
▼ 🔲 *CPU	(4		•	0		
Cores per Socket	1	1		•	Sockets:	4	
CPU Hot Plug	1	Enable CPU	Hot Ad	1			
Reservation (*)		8396		•	MHz	-	
Limit	[Unlimited		•	MHz	-	
Shares (*)		Custom		•	4000	-	
CPUID Mask		Expose the NX/	XD fl	linin	num 0		Adva
Hardware virtualization	n [Expose hard	ware N	laxir	num 1000	00	n to th
Performance counters	s [🗌 Enable virtua	lized C	PU p	erforman	ce co	ounters
Scheduling Affinity		Hyperthrea Available C Select logical pr	iding Si PUs: ocesso	tatus or affi	: Active 24 (loc nity for thi	gical is vir	CPUs) tual ma
New device:	/	Select		15.5	-	4	\dd

6. [メモリ] セクションで、次の設定を更新します。

- メモリのサイズ
- 予約
- 上限
- 共有

値を次のように設定します:

a. [**RAM**] ドロップダウンリストで、RAM のサイズを選択します。これは vCPU の数 x 2 GB でなければなり ません。たとえば、vCPU の数が 4 の場合、RAM = 4×2GB = 8GB になります。

注

NetScaler VPX アプライアンスの Advanced または Premium エディションの場合は、各 vCPU に 4 GB の RAM を割り当てるようにしてください。たとえば、vCPU の数が 4 の場合、RAM = 4×4GB = 16GB になります。

ns SDRS Rules vA	App Opti	ons			
4	-	0			-
-					
8396	-	MB	-	ĺ	
0	-	MB	-)	
Reserve all gues	stmemo	ory (All loc	ked)		
Unlimited	•	МВ	-		
Normal	-	83960	-		
Enable					
20		GB	-		
LSI Logic Parallel					
VM Network			-	j ⊡ c	:0
1/2			-	⊡ c	0
Select			1	Add	1

b. [予約] ドロップダウンリストで、メモリ予約の値を入力し、[すべてのゲストメモリを予約する (すべてのロック済み)] チェックボックスをオンにします。メモリ予約は vCPU の数 x 2 GB である必要があります。たと えば、vCPU の数が 4 の場合、メモリ予約は 4 x 2 GB = 8 GB である必要があります。

注

NetScaler VPX アプライアンスの Advanced または Premium エディションの場合は、各 vCPU に 4 GB の RAM を割り当てるようにしてください。たとえば、vCPU の数が 4 の場合、RAM = 4×4GB = 16GB になります。

/irtual Hardware VM C	ptions	SDRS Rules	vApp Opt	ions		
CPU *CPU		4	-	0		
*Memory						
RAM (*)		8192	-	MB	-	
Reservation (*)		8192		MB	-	
		🗸 Reserve all g	juestmem	ory (All loc	ked)	
Limit		Unlimited	•	MB	-	
Shares		Normal	-	81920	-	
Memory Hot Plug		Enable				
🛄 Hard disk 1		20	A T	GB	-	
G SCSI controller 0		LSI Logic Parall	el			
Metwork adapter 1		VM Network			-	∎c
Network adapter 2		1/2			•	√ c
New device:	<u></u>	Select			A	dd

c. [制限] ドロップダウンリストで、最大値として表示されている数値を選択します。

		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		81920			
Memory Hot Plug		Enable					-
Hard disk 1		20 A GB		GB	-		
G SCSI control	er 0	LSI Logic Parall	el				
🕨 🧮 Network adapter 1		VM Network			+	🗹 Co	0
Network adapter 2		1/2				√ Co	D
New d	evice:	Select			A	dd	1
				-		•	

d. [物理機能]ドロップダウンリストで、Portgroupにマップされている物理アダプタを選択します。

Virtual Hardware VM	Options	SDRS Rules	vApp Opt	ions		
🕨 🔲 *CPU		4	•	0		
- 🌆 *Memory						
RAM (*)		8192	-	MB	-	
Reservation (*)		8192	-	MB	-	
		🔄 Reserve all g	uestmem	ory (All loc	ked)	
Limit		Unlimited		MB	-	
Shares (*)		Custom	-	00000	-	
Memory Hot Plug		Enable	Minii	mum 1		
🕨 🛄 Hard disk 1		20	Maximum 10000			
🖌 🛃 SCSI controller 0		LSI Logic Parall	el			
🕨 📷 Network adapter 1		VM Network			-	🗹 Co
🕨 🧮 Network adapter :	2	1/2			•	Co
New device	e: [Select			A	bb

 SR-IOV ネットワークインターフェイスを追加します。[新しいデバイス] ドロップダウンリストから [ネット ワーク] を選択し、[追加] をクリックします。

/irtual Hardware VM Op	otions	SDRS Rules v	App Optic	ons			
CPU		4	-	0			
Hard disk 1	A N	ew Hard Disk kisting Hard Disk DM Disk	•	GB			
Network adapter 1	n N	etwork	Jk-DVS	1)	- -	Connect	8
Status Port ID) C	D/DVD Drive oppy Drive	r On				
Adapter Type	000 SI ▲ P: ∦ H ₩ U	erial Port arallel Port ost USB Device SB Controller	ual mac ough de ite with nachine	chine ope evices ar vMotion, s.	eration re pres or take	s are unavaila sent. You cann e or restore sn	ble when ot apshots
Physical function MAC Address Guest OS MTU Cha	SI	CSI Device CI Device			•	Automatic	•
Video card	ାଡ଼ି S S	CSI Controller	tings		•	/	
New device:		属 Network		-	A	dd	

8. [新しいネットワーク] セクションで。ドロップダウンリストから、作成したPortgroupを選択し、次の操作を行います。

a.b.「ソケットあたりのコア数」ドロップダウンリストで、ソケット数を選択します。

Virtual Hardware VM Options	SDRS Rules VApp Options			
Hard disk 1	20 • GB •			
SCSI controller 0	LSI Logic Parallel			
Metwork adapter 1	VM Network			
Network adapter 2	VM Network 2			
Video card	Specify custom settings			
VMCI device				
 Other Devices 				
🕫 🏧 New Network	CITRIX_PG1 (DVS_SRIOV_CITRIX)			
Status	Connect At Power On			
Port ID		::		
Adapter Type	SR-IOV passthrough			
	E1000 is are unavailable when			
	SR-IOV passthrough e or restore snapshots			
Divisional Association				
Physical function	vmnic4 0000:03:00.0 Intel Corp 👻			
MAC Address	Automatic V			
Guest OS MTO Change	Disallow	•		
New device:	Network - Add			
Compatibility: ESXi 6.0 and later	(VM version 11) OK Ca	ancel		

b. [物理機能] ドロップダウンリストで、Portgroupにマップされている物理アダプタを選択します。

NSVPX-ESX - Edit Settin	igs (? ••
Virtual Hardware VM Opt	ons SDRS Rules vApp Options	
🕨 🛄 Hard disk 1	20 GB	•
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
▶ 飅 Network 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	
Guest OS MTU Chan	ge Disallow 🔹	-
New device:	💌 Network 💌 Add	
Compatibility: ESXi 6.0 and	ater (VM version 11) OK Cano	el

c. ゲスト OS の MTU 変更ドロップダウンリストで、「許可」を選択します。

- 9. [-設定の編集 <virtual_appliance>] ダイアログボックスで、[仮想マシンオプション] タブをクリックしま す。
- 10. [仮想マシンオプション]タブで、[詳細設定]セクションを選択します。[遅延感度]ドロップダウンリストか ら、[高]を選択します。

NSVPX-ESX-DEMO - Edit Setti	ngs	(1	
Virtual Hardware VM Options	SDRS Rules	vApp Options	
VMware Tools	Ex	pand for VMware Tools settings	*
Power management	Ex	pand for power management settings	
Boot Options	Ex	pand for boot options	F
 Advanced 			
Settings	Disable	acceleration ogging	
Debugging and statistics	Run norm	ally 🗸 🗸	1
Swap file location	 Default Use the machine Virtual n 	settings of the cluster or host containing the virtual a. hachine directory	
	Store the machine	e swap files in the same directory as the virtual).	
	Datasto Store the used for same di is not vis vMotion	re specified by host e swap files in the datastore specified by the host to be swap files. If not possible, store the swap files in the rectory as the virtual machine. Using a datastore that sible to both hosts during vMotion might affect the performance for the affected virtual machines.	4
Configuration Parameters		Edit Configuration	1L
Latency Sensitivity	High	🔹 🚯 🔥 Check CPU reservation	
	Low Normal Medium		
Compatibility: ESXi 5.5 and later (V	High	OK Cance	el

- 11. [作成]または [**OK**]をクリックします。
- 12. NetScaler VPX インスタンスをパワーオンします。
- 13. NetScaler VPX インスタンスの電源が入ったら、次のコマンドを使用して構成を確認できます。

インターフェイスの概要を表示

出力には、設定したすべてのインターフェイスが表示されている必要があります。

1	> show interface	summary			
2 3 4	Interface	MTU	MAC	Suffix	

5	1	0/1	1500	00:0c:29:1b:81:0b	NetScaler Virtual			
		Interface						
6	2	10/1	1500	00:50:56:9f:0c:6f	Intel 82599 10G VF			
		Interface						
7	3	10/2	1500	00:50:56:9f:5c:1e	Intel 82599 10G VF			
		Interface						
8	4	10/3	1500	00:50:56:9f:02:1b	Intel 82599 10G VF			
		Interface						
9	5	10/4	1500	00:50:56:9f:5a:1d	Intel 82599 10G VF			
		Interface						
10	6	10/5	1500	00:50:56:9f:4e:0b	Intel 82599 10G VF			
		Interface						
11	7	L0/1	1500	00:0c:29:1b:81:0b	Netscaler Loopback			
		interface						
12	Do	one						
13	> :	show inter 10	0/1					
14	1) Interface 10/1 (Intel 82599 10G VF Interface) #1							
15	flags=0xe460 <enabled, 802.1g="" hamon,="" up,=""></enabled,>							
16	MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0							
		h21ı	m53s					
17		Actual	media FI	BER, speed 10000, duple	ex FULL, fctl NONE,			
	throughput 10000							
18		LLDP Mc	ode: NONE,	LR Pri	ority: 1024			
19								
20		RX: Pkt	s(8380207	42) Bytes(860888485431)	Errs(0) Drops(2527)			
		Sta	lls(0)					
21		TX: Pkt	s(8381499	54) Bytes(860895860507)	Errs(0) Drops(0)			
		Sta	lls(0)					
22		NIC: Ir	Disc(0) 0	utDisc(0) Fctls(0) Stal	ls(0) Hangs(0) Muted			
		(0)			C			
23		Bandwid	th thresh	olds are not set.				
24	D	one						

SR-IOV モードでの SSL アクセラレーションにインテル QAT を使用するように ESX ハ イパーバイザー上の NetScaler VPX を構成する

October 17, 2024

VMware ESX ハイパーバイザー上の NetScaler VPX インスタンスは、Intel QuickAssist Technology (QAT) を 使用して NetScaler SSL パフォーマンスを高速化できます。インテル QAT を使用すると、レイテンシーの高い暗号 処理をすべてチップにオフロードできるため、1 つまたは複数のホスト CPU を解放して他のタスクを実行できるよ うになります。

以前は、NetScaler データパスの暗号化処理はすべて、ホスト vCPU を使用するソフトウェアで行われていました。

注

現在、NetScaler VPX はインテル QAT ファミリーの C62x チップモデルのみをサポートしています。この機 能は、NetScaler リリース 14.1 ビルド 8.50 以降でサポートされています。

前提条件

- ESX ホストには、1 つ以上のインテル C62x (QAT) チップが搭載されています。
- NetScaler VPX は VMware ESX のハードウェア要件を満たしています。詳細については、「VMware ESX に NetScaler VPX インスタンスをインストールする」を参照してください。

制限事項

個々の VM 用に暗号ユニットや帯域幅を予約する規定はありません。Intel QAT ハードウェアで使用可能なすべての 暗号ユニットは、QAT ハードウェアを使用するすべての VM で共有されます。

インテル **QAT** を使用するためのホスト環境のセットアップ

- インテルが提供する C62x シリーズ (QAT) チップモデル用 VMware ドライバーを VMware ホストにダウン ロードしてインストールします。インテルパッケージのダウンロードとインストール手順の詳細については、 VMware 用インテルクイックアシストテクノロジードライバーを参照してください。
- 2. ESX ホストで SR-IOV を有効にします。
- 3. 仮想マシンを作成します。仮想マシンを作成するときは、パフォーマンス要件を満たす適切な数の PCI デバイ スを割り当てます。

注

各 C62x (QAT) チップには、最大 3 つの個別の PCI エンドポイントを設定できます。各エンドポイントは VF の論理的な集合であり、チップの他の PCI エンドポイントと帯域幅を均等に共有します。各エンドポイントに は、最大 16 個の PCI デバイスとして表示される VF を最大 16 個設定できます。これらのデバイスを VM に追 加すると、QAT チップを使用して暗号アクセラレーションを実行できます。

注意事項

- 仮想マシンの暗号化要件が複数の QAT PCI エンドポイント/チップを使用することである場合は、対応する PCI デバイス/VF をラウンドロビン方式で選択して対称的に配信することをお勧めします。
- 選択する PCI デバイスの数は、ライセンスされている vCPU の数 (管理 vCPU 数は含まない) と同じにすることをお勧めします。利用可能な vCPU 数よりも多くの PCI デバイスを追加しても、必ずしもパフォーマンスが向上するわけではありません。

例

3 つのエンドポイントを持つ1 つの Intel C62x チップを搭載した ESX ホストを考えてみましょう。6 個の vCPU を搭載した VM をプロビジョニングする場合、各エンドポイントから2 つの VF を選択し、それらを VM に割り当てます。このような割り当てにより、仮想マシンの暗号ユニットを効果的かつ均等に分散でき ます。使用可能な vCPU の合計のうち、デフォルトで1 つの vCPU が管理プレーン用に予約され、残りの vCPU はデータプレーン PE で使用できます。

vSphere ウェブクライアントを使用して QAT 仮想マシンを VPX に割り当てる

1. vSphere Web Client で、仮想マシンが配置されている ESX ホストに移動し、[パワーオフ] をクリックしま す。

Treate / Register VM 📑 Console 🕨 Power on Power off	C Refresh 🛛 🌼 Actions	
. Virtual machine	~	Status ~
🗹. 🔂 nst		📀 Normal
		📀 Normal
🗆 🍈 ns4		Normal
🗆 🍈 ns3		Normal
🗔., 👘 ns5		📀 Normal
Quick filters V		



2. [アクション]>[設定の編集]>[他のデバイスの追加]に移動し、[PCI デバイス]を選択します。

🖻 Edit settings - ns1 (ESXi 6.5 virtual ma	achine)						
Virtual Hardware VM Options							
🔜 Add hard disk 🛛 🎫 Add network ad	apter	🚍 A	Add other device				
► 🔲 CPU	5	0	CD/DVD drive				
h The Momony			Floppy drive				
P mm Mernory	12	010	Serial port				
► → Hard disk 1	20	B	Parallel port				8
► SCSI Controller 0		÷¢	USB controller				0
	LOIT	1	USB device	~			
Metwork Adapter 1	VMI	۲	Sound controller	~	Connect		0
Network Adapter 2	PG1)an	PCI device	~	Connect		8
▶ Uideo Card	Spe		Dynamic PCI device				
1	opo	¢	SCSI controller	-			
PCI device 1	C6X0	SATA	SATA controller			\sim	\otimes
PCI device 2	c6xx	1	NVMe controller	J		~	
						Save	Cancel

3. 新しく追加した PCI デバイスに、c6xx QAT VF を割り当て、設定を保存します。

Network Adapter 2	PG1-v1	🗸 🗹 Conn	ect	\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		~	8
PCI device 3	c6xx QAT VF - 0000:1a:01.1		~	8
PCI device 4			~	8
E PCI device 5	c6xx QAT VF - 0000:1b:01.1		~	8
E PCI device 6			~	8
E PCI device 7	c6xx QAT VF - 0000:1b:01.3		~	8
Mew PCI device	c6xx QAT VF - 0000:1a:01.4		~	8

- 4. VM を再度パワーオンします。
- 5. NetScaler CLI でstat sslコマンドを実行して SSL の概要を表示し、QAT VF を VPX に割り当てた後に

SSL カードを確認します。

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

展開について

このデプロイメントは、次のコンポーネント仕様でテストされました:

- **NetScaler VPX** バージョンとビルド:14.1-8.50
- VMware ESXi バージョン:7.0.3 (ビルド 20036589)
- VMware 用インテル C62x QAT ドライバーバージョン:1.5.1.54

E1000 から SR-IOV または VMXNET3 ネットワークインターフェイスへの

NetScaler VPX の移行

October 17, 2024

2018年5月24日

E1000 ネットワークインターフェイスを使用する既存の NetScaler VPX インスタンスを、SR-IOV または VMXNET3 ネットワークインターフェイスを使用するように構成できます。

既存の NetScaler VPX インスタンスを SR-IOV ネットワーク インターフェイスを使用するように構成するに は、「SR-IOV ネットワーク インターフェイスを使用するように NetScaler VPX インスタンスを構成する」を参照し てください。

VMXNET3 ネットワーク インターフェイスを使用するように既存の NetScaler VPX インスタンスを構成するに は、「VMXNET3 ネットワーク インターフェイスを使用するように NetScaler VPX インスタンスを構成する」を参 照してください。

PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX イン スタンスを構成する

April 1, 2025

概要

VMware ESX Server に NetScaler VPX インスタンスをインストールして構成したら、vSphere Web Client を使 用して、PCI パススルーネットワークインターフェイスを使用するように仮想アプライアンスを構成できます。

PCI パススルー機能では、ゲスト仮想マシンからホストに接続された物理 PCI および PCIe デバイスに直接アクセス できます。

前提条件

- ホストの Intel XL710 NIC のファームウェアバージョンは、5.04 です。
- ホストに接続され構成されている PCI パススルーデバイス
- サポートされている NIC:
 - Intel X710 10G NIC
 - Intel XL710 デュアルポート 40G NIC
 - Intel XL710 シングルポート 40G NIC
 - Intel XXV710 デュアルポート 25G NIC

ホスト上のパススルー・デバイスの構成

仮想マシンでパススルー PCI デバイスを構成する前に、ホストマシン上でそれを構成する必要があります。ホストで パススルーデバイスを構成するには次の手順を実行します。

- 1. vSphere Web クライアントのナビゲーターパネルからホストを選択します。
- 2. 管理 > 設定 > PCI デバイス をクリックします。すべての利用可能なパススルーデバイスが表示されます。
- 3. 構成するデバイスを右クリックし、[Edit] をクリックします。
- 4.「PCI デバイスの可用性の編集」ウィンドウが表示されます。
- 5. パススルーに使用するデバイスを選択し、[**OK**] をクリックします。

All PCI Devices						
Q Filter -						
ID		Status	Vendor Name	Device Name	ESX Name	
✓ 1 0000:05:00.	3	Available	Intel Corporation	Ethernet Controll	*	
✓ 1 0000:05:00.	.0	Available	Intel Corporation	Ethernet Controll		
00:000 📷 📃	:1A.0	Unavailable	Intel Corporation	Wellsburg USB		
▼ 0000:00:10	.4	Not Configurable	Intel Corporation	Wellsburg PCI E		
▼ 0000:09	:00.0	Not Configurable	ASPEED Techn	AST1150 PCI-to		
0 📷 📃	000:0A:00.0	Unavailable	ASPEED Techn	ASPEED Graphi		
00:000 📷 📃	:1D.0	Unavailable	Intel Corporation	Wellsburg USB		
- 0000:80:03	.0	Not Configurable	Intel Corporation	Haswell-E PCI E	T	
1 device will become a	vailable when this h	ost is rebooted.		0050055 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		
					OK Cancel	
					Cancel	

6. ホストマシンを再起動します。

NetScaler VPX インスタンスでパススルーデバイスを構成する

次の手順に従って、NetScaler VPX インスタンスでパススルー PCI デバイスを構成します。

- 1. 仮想マシンの電源を切ります。
- 2. 仮想マシンを右クリックし、[設定の編集]を選択します。
- 3. [仮想ハードウェア] タブで、[新しいデバイス] ドロップダウンメニューから [PCI デバイス] を選択し、[追加] をクリックします。

B NSVPX-ESX-DEMO -	Edit Settings		(?) ₩
Virtual Hardware VM C	Options SDRS Rule	es vApp Options	
F 🔲 CPU	2	• 0	
► III Memory	4096	▼ MB ▼	
▶ → Hard disk 1	20	GB v	
▶ ☑ SCSI controller 0	LSI Logic Parallel		
Network adapter 1	VM Network	Connect	
Video card	Specify custom set	tings 🛛	
VMCI device			
 Other Devices 			
New device:	PCI	Device Add	
Compatibility: ESXi 6.0 an	nd later (VM version 1	1) ОК	Cancel

4. [New PCI device] を展開し、ドロップダウンリストから仮想マシンに接続するパススルーデバイスを選択し、[OK] をクリックします。

注

VMXNET3 ネットワークインターフェイスと PCI パススルーネットワークインターフェイスは共存できません。

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

5. ゲスト仮想マシンの電源を入れます。

PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX を構成する手順を完了しました。

VMware ESX ハイパーバイザーでの NetScaler ADC アプライアンスの初回起動時に NetScaler ADC VPX の構成を適用する

April 1, 2025

NetScaler VPX 構成は、VMware ESX ハイパーバイザーでの NetScaler ADC アプライアンスの初回起動時に適 用できます。Therefore in certain cases, a specific setup or VPX instance is brought up in much lesser

time.

プレブートユーザーデータとその形式について詳しくは、クラウドでの NetScaler ADC アプライアンスの初回起動 時に NetScaler ADC VPX 構成を適用するを参照してください。

注

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

How to provide preboot user data on ESX hypervisor

Web クライアントまたは vSphere クライアントから ESX ハイパーバイザーのプレブートユーザーデータを提供するには、次の 2 つの方法があります。

- Using CD/DVD ISO
- Using OVF Property

Provide user data using CD/DVD ISO

VMware vSphere クライアントを使用すると、CD/DVD ドライブを使用して ISO イメージとしてユーザーデータ を VM に注入できます。

CD/DVD ISO を使用してユーザーデータを提供するには、次の手順に従います。

 プレブートユーザーデータコンテンツを含むファイル名userdataでファイルを作成します。For more information on the content of the <NS-CONFIG> tag, see Sample <NS-CONFIG > section.

```
注
ファイル名は厳密に userdataとして使用する必要があります。
```

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

3. 標準の展開プロセスを使用して NetScaler ADC VPX インスタンスをプロビジョニングし、仮想マシンを作成 します。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 Network			Ý	
	Disk provisioning	Thin O Thick				
	Power on automatically	D				
vmware						
			Back	Next	Finish	Cancel

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

🔁 Edit settings - sai-test-iso (ESXi 5.1 virtual machine)					
Virtual Hardware VM Options					
🔜 Add hard disk 🛛 🔳 Add network ad	apter	Add other device			
+ 🔲 CPU	2	CD/DVD drive			
k Memory		Floppy drive			
, menory	2	Serial port			
۱ 🛄 Hard disk 1	20	Parallel port		٢	
+ 🐼 SCSI Controller 0		USB controller		0	
		E USB device		0	
Network Adapter 1	VM	Sound controller	V Connect	0	
🕨 🌉 Video Card	Spe	B PCI device	~		
		Dynamic PCI device			
			-		
			Save	Cancel	

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

r.

🔁 Edit settings - sai-test-iso (ESXI 5.1 virtual machine)					
Virtual Hardware VM Options					
🔜 Add hard disk 🛛 🎫 Add network ad	lapter 🛛 🚊 Add other device				
+ 🔲 CPU	2 ~ ()				
• 🎆 Memory	2 GB ~				
+ 🔜 Hard disk 1	20 GB ~		۵		
SCSI Controller 0	LSI Logic Parallel		٢		
INN Network Adapter 1	VM Network	Connect	٢		
I is New CD/DVD Drive	Host device	🗸 🗹 Connect	٥		
▶ 🛄 Video Card	Datastore ISO file				
		Save	Cancel		

6. Select a Datastore in the vSphere Client.

Upload	d 🚯 Delete 🔒 Move 陷 C	opy 🔭 Create dir	ectory C Refresh	
datastore1	isdd.sf	🔕 esx		
៉ vmimages	៉ centosiso	i pre	9	
	🚞 centosnirmal_225	i pre	esx_preboot_userdata.i	
	៉ fips-t1	i pre	352 KB Wednesday, July 14, 2	
	🚞 fips1	i pre		
	៉ sai-test-iso	i pre		
	🚞 sai-test-rs130	sai		
	📺 sai-vpx-2	📃 sai		
	ai-vpx-test	sai		
	늘 sai-vpx3	🌇 sai		
	i Shreesh-blx-centos	sai		
	៉ Venkata	vm		
		vm		
	11	III 📄 vm III		
[datastore1] sai-vpx-2/e	sx_preboot_userdata.iso			
			Select	Cancel

7. Power on the VM.

ESX Web クライアントの OVF プロパティを使用してユーザーデータを提供

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.

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

1	<pre>base64 <userdata-filename> > <outuput-file></outuput-file></userdata-filename></pre>
(51)	
1	base64 esx_userdata.xml > esx_userdata_b64
root@ub root@ub	untu:~/sai/l4jul2021# base64 esx_userdata.xml > esx_userdata_b64 untu:~/sai/l4jul2021#
root@ub	untu:~/sai/14jul2021# cat esx_userdata_b64
PE5TLVB	SRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+Cg1hZGQgcm91dGUgMC4wLjAuMCAw
LjAuMC4	wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
ICAGICA	GICAGICAGICAGICAGIDXORVGXULUJPTIKIVFJBUD52KVM8LINLSVALKEVGQVVMVCICTU90 +CiAGICAGICAGICAGIDXORVG+OkQDVFNUUkFOLVNFUVVFTkNFD]]FUzuvTkVXLUIPT1RT
VFJBUC1	TRVFVRU5DRT4KCiAaICAaICAaICAAPE1HTVOtSU5URVJGOUNFLUNPTkZJRz4KICAaICAaICAa
ICAgICA	gIDxJT1RFUkZBQ0UtT1VNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
ICAgIDx	JUD4gICAgMTAuMTAyLjM4LjIxOSA8L01QPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
QVNLPiA	yNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULU10VEVSRkFD
RS1DT05	GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+Cg==

- Use online tools to encode user data content, for example, Base64 Encode and Decode.
- 3. ESX ハイパーバイザー上の NetScaler ADC **VPX** インスタンスの **OVF** テンプレートに製品セクションを含めます。

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 o	change the defaul	t NSROOT password	d.						
Enter ne	ew password:								
Please :	re-enter your pas	sword:							
Done									
> sh ns	ver								
	NetScaler NS13.0	: Build 83.9005.1	nc. Date: Jul 13	2021. 02:	56:05	(64-bit)			
Done						(01 220)			
> sh ns	in								
/ 511 115	Traddress	Traffic Domain	Trance	Mode	Arn	Temp	Veerve	sr.	Q
tato	ipaddiess	ITATIIC Domain	TAbe	noue	мр	remp	VSELVE	2 L.	5
Late									
1.	10 100 00 010						373		-
,,	10.102.38.219		NetScaler IP	ACLIVE	Enabled	Fuabled	NA		F.
nabled									
Done									
> sh rou	ute								
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic D	omain	тур)e
1)			10 102 20 1						. —
±)	0.0.0.0	0.0.0.0	10.102.30.1		0F		-	TUT	
C O	107 0 0 0	0.5.5 0 0 0	107 0 0 1				-		
2)	127.0.0.0	255.0.0.0	127.0.0.1		0P		F	/ERM	IA
NENT		055 055 055 0							
3)	10.102.38.0	255.255.255.0	10.102.38.219		UP		E	DIRE	C
T									
Description									

ESX vSphere クライアントの OVF プロパティを使用してユーザーデータを提供

ESX vSphere クライアントから OVF プロパティを使用してユーザーデータを提供するには、次の手順に従います。

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>
                      10.102.38.219 </IP>
                < 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>
```

```
例
```

1	base64	esx_userdata.xml	> esx_userdata_b64
root@ubu	untu:~/sai/	14jul2021# base64 esx	userdata.xml > esx userdata b64
root@ubu	untu:~/sai/	14jul2021#	
root@ubu	untu:~/sai/	14jul2021# cat esx_use	erdata_b64
PE5TLVBS	SRS1CT09ULU	NPTkZJRz4KICAgIDxOUy1D	T05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
LjAuMC4v	wIDEwLjEwMi	4zOC4xCiAgICA8L05TLUNE	TkZJRz4KCiAgICA8T1MtQk9PVFNUUkFQPgog
ICAGICAG	gICAgICA8U0	tJUC1ERUZBVUxULUJPT1R1	VFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
U1RSQVA-	+CiAgICAgIC	AgICAgIDxORVctQk9PVFNU	UUkFQLVNFUVVFTkNFP11FUzwvTkVXLUJPT1RT
VFJBUC1	IRVFVRU5DRT	4KCiAgICAgICAgPE1HTVQt	SU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
ICAgICAg	gIDxJTlRFUk	ZBQ0UtTlVNPiBldGgwIDwv	SU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
ICAgIDxJ	JUD4gICAgMT	AuMTAyLjM4LjIxOSA8L01Q	PgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
QVNLPiAy	yNTUuMjU1Lj	I1NS4wIDwvU1VCTkVULU1E	3U0s+CiAgICAgICAgPC9NR01ULU10VEVSRkFD
RS1DT050	GSUc+CiAqIC	A8L05TLUJPT1RTVFJBUD4K	PC90Uy1QUkUtQk9PVC1DT05GSUc+Cg==

- Use online tools to encode user data content, for example, Base64 Encode and Decode.
- 3. ESX ハイパーバイザー上の NetScaler ADC **VPX** インスタンスの **OVF** テンプレートに製品セクションを含めます。

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" pre=""></property>
	userConfigurable="true"
9	ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDx0Uy1DT05GSUc+
	CglhZGQgcm91dGUgMC4wLjAuMCAw
10	LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQ

11	ICAgICAgICAgICA8U0tJUC1ERUZBVU×ULUJPT1RTVFJBUD5ZRVM8L1NLSVAtR	EVGQVVMVC
12	U1RSQVA+ CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTk	VXLUJPT1
13	VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz	4KICAgIC
14	ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KIC	CAgICAgIC
15	ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgIC	CAgPFNVQk
16	QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+ CiAgICAgICAgPC9NR01ULUlOVEVSRkFD	
17	RS1DT05GSUc+ CiAgICA8L05TLUJPT1RTVFJBUD4KPC90Uy1QUkUtQk9PVC1DT05GSUc+ Cg==">	
18	Ŭ	
19	<label>Userdata</label>	
20	<pre><description> Userdata for ESX VPX </description></pre>	
21		
22		
23		

5. 次のように ovf:transport="com.vmware.guestInfo"、プロパティを仮想ハードウェアセ クションに追加します。

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

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

Please (Enter ne	change the defaul ew password: re-enter your pas	t NSROOT password	1.						
Done	ro chitor jour pub	5.102.01							
> sh ns	ver								
	NetScaler NS13.0	: Build 83.9005.r	nc, Date: Jul 13	2021, 02:	56:05	(64-bit)			
Done									
> sh ns	ip								
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserve	er	S
tate									
1)	10.102.38.219	0	NetScaler IP	Active	Enabled	Enabled	NA		E
nabled Done									
> sh rou	ute								
	Network	Netmask	Gateway/OwnedIP	VLAN	State	Traffic Do	omain	Тур	e
1) C	0.0.0.0	0.0.0.0	10.102.38.1		UP		S	TAT	I
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		Ι	DIRE	С

AWS of VMware クラウドに Citrix ADC VPX インスタンスをインストールする

October 17, 2024

AWS 上の VMware クラウド (VMC) を使用すると、必要な数の ESX ホストを使用してクラウドソフトウェア定義デ ータセンター (SDDC) を AWS 上に作成できます。AWS 上の VMC は、NetScaler VPX デプロイをサポートしてい ます。VMC は、オンプレミスの vCenter と同じユーザー・インタフェースを提供します。ESX ベースの Citrix ADC VPX デプロイメントと同じように機能します。

前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- 1 つの VMware SDDC が少なくとも1つのホストに存在している必要があります。
- NetScaler VPX アプライアンスセットアップファイルをダウンロードします。
- 仮想マシンが接続する適切なネットワークセグメントを VMware SDDC 上に作成します。
- VPX ライセンスファイルを入手します。NetScaler VPX インスタンス ライセンスの詳細については、 NetScaler VPX ライセンス ガイド (</en-us/licensing/licensing-guide-for-netscaler.html>) を参照し てください。

VMware クラウドのハードウェア要件

次の表に、VMware SDDC が各 VPX nCore 仮想アプライアンスに対して提供する必要がある仮想コンピューティン グリソースを示します。

表 1. NetScaler VPX インスタンスの実行に必要な最小限の仮想コンピューティングリソース

コンポーネント	条件
メモリ	2 GB
仮想 CPU(VCPU)	2
仮想ネットワークインターフェイス	VMware SDDC では、VPX ハードウェアをバージョン7 以上にアップグレードすると、最大 10 個の仮想ネット ワーク インターフェイスをインストールできます。
ディスク領域	20GB

注

これは、ハイパーバイザーのディスク要件に加えて必要になります。

VPX 仮想アプライアンスを実稼働で使用するには、フルメモリ割り当てを予約する必要があります。
OVF ツール 1.0 のシステム要件

Open Virtualization Format Tool (OVF Tool) は、Windows および Linux システムで実行できるクライアント アプリケーションです。次の表は、最小システム要件を示しています。

表 2. OVF ツールのインストールに必要な最小システム要件

コンポーネント	条件
オペレーティングシステム	VMware からの詳細な要件については、 http://kb.vmware.com/で『OVF ツールユーザーガ イド』の PDF ファイルを検索してください。
CPU	最低 750MHz、1GHz 以上推奨
RAM	最小1GB、推奨2GB
NIC	100Mbps 以上の NIC。

OVF のインストールについては、http://kb.vmware.com/で『OVF ツールユーザーガイド』の PDF ファイルを検 索してください。

NetScaler VPX セットアップファイルのダウンロード

VMware ESX 用の NetScaler VPX インスタンスセットアップパッケージは、オープン仮想マシン(OVF)フォーマット標準に準拠しています。これらのファイルは、Citrix Web サイトからダウンロードできます。ログオンするには、Citrix アカウントが必要です。Citrix アカウントをお持ちでない場合は、http://www.citrix.comのホームページにアクセスしてください。[新しいユーザー] リンクをクリックし、指示に従って新しい Citrix アカウントを作成します。

ログオンしたら、Citrix のホームページから次のパスをナビゲートします。

Citrix.com > ダウンロード > NetScaler > 仮想アプライアンス。

次のファイルを、ESX サーバーと同じネットワーク上のワークステーションにコピーします。3 つのファイルをすべ て同じフォルダーにコピーします。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (例えば、NSVPX-ESX-13.0-79.64disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (例えば、NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf(例えば、NSVPX-ESX-13.0-79.64.mf)

VMware クラウドへの Citrix ADC VPX インスタンスのインストール

VMware SDDC をインストールして設定したら、SDDC を使用して VMware クラウドに仮想アプライアンスをイン ストールできます。インストールできる仮想アプライアンスの数は、SDDC で使用可能なメモリの量によって異なり ます。

NetScaler VPX インスタンスを VMware クラウドにインストールするには、次の手順に従います。

- 1. ワークステーションで VMware SDDC を開きます。
- 2. [ユーザー名] テキストボックスと [パスワード] テキストボックスに、管理者の認証情報を入力し、[ログイン] をクリックします。
- 3. [File] メニューの [Deploy OVF Template] を選択します。
- 4. [**OVF** テンプレートのデプロイ] ダイアログボックスの [ファイルからデプロイ] で、NetScaler VPX インス タンスセットアップファイルを保存した場所を参照し、.ovf ファイルを選択して、[次へ] をクリックします。

注: デフォルトでは、NetScaler VPX インスタンスは E1000 ネットワークインターフェイスを使用し ます。VMXNET3 インターフェイスで ADC を展開するには、E1000 ではなく VMXNET3 インターフェ イスを使用するように OVF を変更します。

- 5. 仮想アプライアンス OVF テンプレートに表示されるネットワークを、VMware SDDC で設定したネットワー クにマッピングします。[次へ] をクリックして VMware SDDC への仮想アプライアンスのインストールを開 始します。
- これで、NetScaler VPX インスタンスを起動する準備ができました。ナビゲーションペインで、インストー ルした Citrix ADC VPX インスタンスを選択し、右クリックメニューから [パワーオン]を選択します。コン ソールポートをエミュレートするには、[Console] タブをクリックします。
- 7. 別の仮想アプライアンスをインストールする場合は、ステップ6から繰り返します。
- 8. 管理ネットワークとして選択した同じセグメントから管理 IP アドレスを指定します。ゲートウェイには同じ サブネットが使用されます。
- 9. VMware SDDC では、ネットワークセグメントに属するすべてのプライベート IP アドレスに対して NAT ル ールとファイアウォールルールを明示的に作成する必要があります。

Microsoft Hyper-V サーバーに NetScaler VPX インスタンスをインストールします

October 17, 2024

NetScaler VPX インスタンスを Microsoft Windows Server にインストールするには、まず、十分なシステムリ ソースを備えたマシンに、Hyper-V ロールを有効にした Windows Server をインストールする必要があります。 Hyper-V の役割をインストールするときは、仮想ネットワークを作成するために Hyper-V で使用されるサーバー 上の NIC を必ず指定してください。一部の NIC は、ホスト用に確保できます。Hyper-V マネージャーを使用して NetScaler VPX インスタンスのインストールを実行します。

Hyper-V 用の NetScaler ADC VPX インスタンスは、仮想ハードディスク(VHD)形式で配信されます。CPU、ネ ットワークインターフェイス、ハードディスクのサイズと形式などの要素について、デフォルト構成が格納されてい ます。NetScaler VPX インスタンスをインストールしたら、仮想アプライアンスにネットワークアダプタを構成し、 仮想 NIC を追加してから、NetScaler IP アドレス、サブネットマスク、およびゲートウェイを割り当てて、仮想ア プライアンスの基本構成を完了できます。

VPX インスタンスの初期構成後、アプライアンスを最新のソフトウェアリリースにアップグレードする場合は、 NetScaler VPX スタンドアロンアプライアンスのアップグレードを参照してください。

注

ISIS(Intermediate System-to-Intermediate System)プロトコルは、Hyper-V 2012 プラットフォーム 上でホストされる NetScaler VPX 仮想アプライアンスではサポートされません。

NetScaler VPX インスタンスを Microsoft サーバーにインストールするための前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- Windows サーバーで Hyper-V ロールを有効にします。詳しくは、http://technet.microsoft.com/enus/library/ee344837(WS.10).aspxを参照してください。
- 仮想アプライアンスセットアップファイルをダウンロードします。
- NetScaler VPX インスタンスのライセンスファイルを取得します。NetScaler VPX インスタンスライセンスの詳細については、https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-installcitrix-netscaler-vpx-licenses?language=en_USの『NetScaler VPX ライセンスガイド』を参照してください。

Microsoft のサーバハードウェア要件

次の表は、Microsoft サーバーの最小システム要件を示しています。

表 1. Microsoft サーバーの最小システム要件

コンポーネント	条件
CPU	1.4GHz 64 ビットプロセッサ
RAM	8 GB
ディスク領域	32GB 以上

次の表は、各仮想コンピューティングリソースの一覧です。NetScaler VPX インスタンス。

コンポーネント	条件
RAM	4 GB
仮想 CPU	2
ディスク領域	20GB
仮想ネットワーク インターフェイス	1

表 2. NetScaler VPX インスタンスの実行に必要な最小限の仮想コンピューティングリソース

NetScaler VPX セットアップファイルをダウンロードする

Hyper-V 用の NetScaler ADC VPX インスタンスは、仮想ハードディスク(VHD)形式で配信されます。これらの ファイルは、Citrix Web サイトからダウンロードできます。ログインするには Citrix アカウントが必要です。Citrix アカウントをお持ちでない場合は、http://www.citrix.comのホームページにアクセスし、[サインイン] > [マイア カウント] > [**Citrix** アカウントの作成] の順にクリックし、手順に従って Citrix アカウントを作成します。

NetScaler VPX インスタンスのセットアップファイルをダウンロードするには、次の手順に従います。

- 1. Web ブラウザーで、http://www.citrix.com/に移動します。
- 2. ユーザー名とパスワードを使用してサインインします。
- 3. [Downloads] をクリックします。
- 4.「製品の選択」ドロップダウンメニューで、「NetScaler (NetScaler ADC)」を選択します。
- 5. 「NetScaler リリース X.X」>「仮想アプライアンス」で、「NetScaler VPX リリース X.X」をクリックしま す。
- 6. 圧縮ファイルをサーバーにダウンロードします。

NetScaler VPX インスタンスを Microsoft のサーバーにインストールします

Microsoft Server で Hyper-V ロールを有効にし、仮想アプライアンスファイルを抽出したら、Hyper-V Manager を使用して NetScaler ADC VPX インスタンスをインストールできます。仮想マシンをインポートしてから仮想 NIC を構成し、Hyper-V によって作成された仮想ネットワークに関連付ける必要があります。

最大 8 つの仮想 NIC を構成できます。物理 NIC が DOWN になっても、同じホスト(サーバー)上の他の仮想アプラ イアンスと通信できるため、仮想アプライアンスでは仮想 NIC は UP と見なされます。

注

仮想アプライアンスの実行中は、設定を変更することができません。仮想アプライアンスをシャットダウンし てから変更を行います。 **Hyper-V** マネージャーを使用して **NetScaler VPX** インスタンスを **Microsoft** サーバーにインストールするに は:

- Hyper-V マネージャーを起動するには、[スタート]ボタンをクリックし、[管理ツール]をポイントして、[Hyper-V マネージャー]をクリックします。
- 2. ナビゲーションペインの **Hyper-V Manage**r で、NetScaler VPX インスタンスをインストールするサーバ ーを選択します。
- 3. [アクション]メニューで、[仮想マシンのインポート]をクリックします。
- 【仮想マシンのインポート】ダイアログボックスの [場所] で、NetScaler VPX インスタンスのソフトウェア ファイルを含むフォルダーのパスを指定し、[仮想マシンをコピー(新しい一意の ID を作成)]を選択します。 このフォルダーは、Snapshots フォルダー、Virtual Hard Disks フォルダー、および Virtual Machines フ ォルダーを格納する親フォルダーです。

注

圧縮ファイルを受け取った場合は、フォルダーへのパスを指定する前に、フォルダーにファイルを展開することを確認します。

1. [インポート] をクリックします。

- 2. インポートした仮想アプライアンスが [仮想マシン]の下に表示されていることを確認します。
- 3. 別の仮想アプライアンスをインストールするには、手順2~6を繰り返します。

重要:

手順4で、必ずファイルを別のフォルダーに解凍してください。

Hyper-V で NetScaler ADC VPX インスタンスを自動プロビジョニングする

NetScaler VPX インスタンスの自動プロビジョニングはオプションです。自動プロビジョニングを実行しない場合 は、NetScaler 仮想アプライアンスによって IP アドレスなどを構成するためのオプションが提供されます。

Hyper-V で NetScaler ADC VPX インスタンスを自動プロビジョニングするには、次の手順に従います。

1. 例に示されている説明に従い、XML ファイルを使用して ISO9660 準拠の ISO イメージを作成します。xml ファイルの名前が **userdata** であることを確認してください。

XML ファイルから ISO ファイルを作成するには、以下を使用します。

- PowerISO などの任意の画像処理ツール。
- Linux の mkisofsコマンド。

0	
7	oe:id=""
0	<pre>xmlnc=`"http://schomas.dmtf.org/ovf/onvironmont/1`"></pre>
10	xiiiths- iittp://scheilas.uliti.org/ovi/environilent/1 /
11	<platformsection></platformsection>
12	
13	<kind>HYPER-V</kind>
14	
15	<version>2013.1</version>
15	(Venders) CITETY (Venders)
10	<pre><vendor>Clikix</vendor></pre>
10	
20	
21	
22	
23	<propertysection></propertysection>
24	
25	<property oe:key="com.citrix.netscaler.ovf.version" oe:value=" 1.0"></property>
26	
27	<property oe:key="com.citrix.netscaler.platform" oe:value="
NS1000V"></property>
28	
29	<property oe:key="com.citrix.netscaler.orch_env" oe:value="
cisco-orch-env"></property>
30	
31	<property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
10.102.100.122"></property>
32	
33	<property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
255.255.255.128"></property>
34	
35	<property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
10.102.100.67"></property>
36	
37	

- 2. ISO イメージを Hyper-V Server にコピーします。
- インポートした仮想アプライアンスを選択し、[アクション]メニューで[設定]を選択します。仮想アプライアンスを選択し、右クリックして[設定]を選択することもできます。選択した仮想アプライアンスの[設定]ウィンドウが表示されます。
- 4.「設定」ウィンドウの「ハードウェア」セクションで、「IDE Controller」をクリックします。
- 5. 右側のウィンドウペインで、「**DVD Drive**」を選択し、「追加」をクリックします。DVD ドライブは、左側の ウィンドウペインの **IDE** コントローラセクションに追加されます。
- 6. 手順 5 で追加した **DVD** ドライブを選択します。右側のウィンドウペインで [イメージファイル] ラジオボタ ンを選択し、[参照] をクリックして、手順 2 で Hyper-V サーバにコピーした ISO イメージを選択します。

7. [適用] をクリックします。

注

次の場合、仮想アプライアンスインスタンスはデフォルトの IP アドレスで起動します。

- DVD ドライブがアタッチされているのに、ISO ファイルが提供されていない。
- ISO ファイルにはユーザーデータファイルは含まれていません。
- ユーザーデータのファイル名または形式が正しくありません。

NetScaler VPX インスタンスで仮想 NIC を構成するには、次の手順に従います。

- 1. インポートした仮想アプライアンスを選択し、[アクション]メニューで[設定]を選択します。
- 2. [設定]ダイアログボックスの左ペインの <virtual appliance name>[ハードウェアの追加] をクリックしま す。
- 3. 右ペインで、デバイスのリストから [ネットワークアダプター]を選択します。
- 4. [追加] をクリックします。
- 5. 左ペインに [Network Adapter (not connected)] が表示されていることを確認します。
- 6. 左ペインでネットワークアダプターを選択します。
- 7. 右側のペインの [ネットワーク] メニューから、アダプターを接続する仮想ネットワークを選択します。
- 8. 使用する他のネットワークアダプタの仮想ネットワークを選択するには、手順6と7を繰り返します。
- 9. [適用] をクリックしてから、[**OK**] をクリックします。

NetScaler VPX インスタンスを構成するには:

- 1. 前にインストールした仮想アプライアンスを右クリックし、[開始]を選択します。
- 2. 仮想アプライアンスをダブルクリックして、コンソールにアクセスします。
- 3. 仮想アプライアンスの NetScaler IP アドレス、サブネットマスク、およびゲートウェイを入力します。

仮想アプライアンスの基本構成が完了しました。Web ブラウザーで IP アドレスを入力して、仮想アプライアンスに アクセスします。

注

仮想マシン(VM)テンプレートを使用して、SCVMM を使用して NetScaler ADC VPX インスタンスをプロビ ジョニングすることもできます。

NetScaler VPX インスタンスで Microsoft Hyper-V NIC チーミングソリューションを使用する場合、詳細に ついては、記事 CTX224494 を参照してください。

Linux-KVM プラットフォームへの Citrix ADC VPX インスタンスのインストール

October 17, 2024

Linux-KVM プラットフォーム用の Citrix ADC VPX を設定するには、グラフィカル仮想マシンマネージャ(仮想マ ネージャ)アプリケーションを使用できます。Linux-KVM コマンドラインを使用する場合は、virsh プログラム を使用できます。

KVM Module および QEMU のような仮想化ツールを使って、適切なハードウェアにホスト Linux オペレーティン グシステムをインストールする必要があります。ハイパーバイザー上で展開できる仮想マシン(VM)の数はアプリケ ーション要件および選択されたハードウェアにより異なります。

NetScaler VPX インスタンスをプロビジョニングしたら、より多くのインターフェイスを追加できます。

制限事項と使用ガイドライン

一般的な推奨事項

予測できない動作を回避するには、次の推奨事項を適用します。

- VPX 仮想マシンに関連付けられている VNet インターフェイスの MTU を変更しないでください。インターフ ェイスモードや CPU などの構成パラメータを変更する前に、VPX VM をシャットダウンします。
- VPX VM を強制的にシャットダウンしないでください。つまり、【強制オフ] コマンドは使用しないでください。
- ホスト Linux 上で指定された任意の構成は、Linux ディストリビューションの設定によってそのまま維持されたり、維持されなかったりします。これらの構成を維持するよう選択して、ホスト Linux オペレーティングシステムのリブートにおける一貫した動作を確保できます。
- NetScaler パッケージはプロビジョニングされた各 NetScaler VPX インスタンスに対して一意である必要が あります。

制限事項

• KVM 上で動作する VPX インスタンスのライブマイグレーションはサポートされていません。

Linux-KVM プラットフォームに **Citrix ADC VPX** インスタンスをインストールするた めの前提条件

October 17, 2024

NetScaler VPX インスタンスで実行されている Linux-KVM サーバーの最小システム要件を確認します。

CPU 要件:

• Intel VT-X プロセッサーに含まれるハードウェア仮想化機能を備えた 64 ビット x86 プロセッサー。

CPU が Linux ホストをサポートしているかどうかをテストするには、ホスト Linux シェルプロンプトで次のコマン ドを入力します。

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

前の拡張機能の BIOS 設定が無効になっている場合は、BIOS でそれらを有効にする必要があります。

- ホスト Linux に 2 つ以上の CPU コアを指定します。
- プロセッサ速度に対する特定の推奨設定はありませんが、速度が速ければ速いほど VM アプリケーションのパフォーマンスはよくなります。

メモリ (RAM) 要件:

ホスト Linux カーネルに対して 4GB 以上。VM が必要とするメモリを追加します。

ハードディスク要件:

ホスト Linux カーネルおよび VM 要件の領域を計算します。単一の NetScaler VPX VM は 20GB のディスク領域を 必要とします。

ソフトウェア要件

使用されるホストカーネルは、リリース 2.6.20 以降で、すべての仮想化ツールがある 64 ビットの Linux カーネル である必要があります。3.6.11-4 以降といったより新しいカーネルを推奨します。

Red Hat、CentOS、Fedora などの多くの Linux ディストリビューションでは、カーネルのバージョンと関連する 仮想化ツールのテストが行われています。

ゲスト VM のハードウェア要件

NetScaler VPX でサポートされるハードディスクの種類は IDE と virtIO です。ハードディスクの種類は、NetScaler パッケージに含まれる XML ファイルで構成されています。

ネットワーク要件

NetScaler VPX は、VirtIO 準仮想化、SR-IOV、および PCI パススルーネットワークインターフェイスをサポートします。

サポートされるネットワークインターフェースの詳細については、以下を参照してください。

- 仮想マシンマネージャーを使用して NetScaler VPX インスタンスをプロビジョニングします
- SR-IOV ネットワークインターフェースを使用するように NetScaler VPX インスタンスを構成する
- PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する

ソースインターフェイスおよびモード

ソースデバイスの種類は、Bridge または MacVTap のいずれかにできます。MacvTap では、VEPA モード、ブリッジ、プライベート、パススルーの 4 つのモードが可能です。次のように、使用できるインターフェイスのタイプとサポートされているトラフィックタイプを確認します。

ブリッジ:

- Linux Bridge。
- 正しい設定を選択したり、IPtable サービスを無効にしたりしないと、ホスト Linux のEbtablesおよびiptables設定によってブリッジのトラフィックがフィルタリングされることがあります。

MacV タップ **(VEPA** モード):

- パフォーマンスは Bridge より向上します。
- 同じ下位デバイスからのインターフェイスを VM 間で共有できます。
- 仮想マシン間通信(同じ
- 下位のデバイスは、アップストリームスイッチまたはダウンストリームスイッチが VEPA モードをサポートしている場合にのみ可能です。

MacVTap (プライベートモード):

- パフォーマンスは Bridge より向上します。
- 同じ下位デバイスからのインターフェイスを VM 間で共有できます。
- 同じ下位デバイスを使った内部 VM 通信を実行できません。

MacVTap (ブリッジモード):

- Bridge と比べてよい。
- 同じ下位デバイスのインターフェイスは、VM 間で共有できます。
- 下位のデバイスリンクがアップしている場合は、同じ下位デバイスを使用する VM 間通信が可能です。

MacVTap (パススルーモード**)**:

- Bridge と比べてよい。
- 同じ下位デバイスのインターフェイスは、仮想マシン間で共有できません。
- 1 つの VM のみ、下位デバイスを使用できます。

注

VPX インスタンスによる最高のパフォーマンスを得るには、ソース インターフェイスで gro および lro 機 能がオフになっていることを確認します。

送信元インターフェイスのプロパティ

ソースインターフェイスの Generic-receive-offload(gro)および大規模受信オフロード(lro)機能をオフに します。groおよびlro機能をオフにするには、ホスト Linux シェルプロンプトで次のコマンドを実行します。

```
ethtool -K eth6 gro &dtate thool -K eth6 lro data
```

例:

1	[root@localhost ~]# ethtool -K eth6
2	
3	Offload parameters for eth6:
4	
5	rx-checksumming: on
6	
7	tx-checksumming: on
8	
9	scatter-gather: on
10	
11	tcp-segmentation-offload: on
12	
13	udp-fragmentation-offload: off
14	
15	generic-segmentation-offload: on
16	
1/	generic-receive-offload: off
18	
19	large-receive-ottload: ott
20	ry ylan offload, an
21	
22	tx-vlan-offload, on
23	
25	ntunle-filters. off
25	incupte inters. On
27	receive-bashing. on
28	receive nasiring. on
29	[root@localhost ~]#

例:

次の例のように、ホスト Linux ブリッジをソースデバイスとして使用する場合、ホストとゲスト VM を接続する仮想 インターフェイスである VNet インターフェイスでlro機能をオフにする必要があります。

1	[root@localhost	: ~]# brctl show eth6_br		
2				
3	bridge name	bridge id	SIP enabled	interfaces
5	eth6_br	8000.00e0ed1861ae	no	eth6
6	_			
7				vnet0
8				
9				vnet2
11	[root@localhost	: ~]#		

上記の例では、2 つの仮想インターフェイスは eth6_br から派生し、vnet0 および vnet2 として表されます。次の コマンドを実行して、これらのインターフェイスのgro機能とlro機能をオフにします。

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

無差別モード

次の機能を動作させるには、無差別モードを有効にする必要があります。

- L2 モード
- マルチキャストトラフィック処理
- ブロードキャスト
- IPV6 トラフィック
- 仮想 MAC
- 動的ルーティング

次のコマンドを使用して、無差別モードを有効にします。

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

必要なモジュール

ネットワークパフォーマンスを向上させるには、Linux ホストに vhost_net モジュールが存在することを確認して ください。vhost_net モジュールの存在を確認するには、Linux ホストで次のコマンドを実行します。

1 lsmod | grep "vhost_net"

vhost_net がまだ実行されていない場合は、次のコマンドを入力して実行します。

1 modprobe vhost_net

OpenStack を使用して Citrix ADC VPX インスタンスをプロビジョニングする

October 17, 2024

OpenStack 環境で Citrix ADC VPX インスタンスをプロビジョニングするには、**Nova** ブートコマンド(OpenStack CLI) または Horizon (OpenStack ダッシュボード)を使用します。

VPX インスタンスをプロビジョニングします。オプションで、コンフィグドライブのデータを使用します。「構成ドラ イブ」とは、インスタンスの起動時に CD-ROM デバイスとしてアタッチされる特殊な構成ドライブを指します。こ の構成ドライブは、管理 IP アドレス、ネットワークマスク、デフォルトゲートウェイなど、ネットワーク構成を渡す ためや、顧客スクリプトを注入するために使用できます。

NetScaler アプライアンスでは、デフォルトの認証方式はパスワードベースです。現在、OpenStack 環境上の Citrix ADC VPX インスタンスでは、SSH キーペア認証メカニズムがサポートされています。

キーペア (公開鍵と秘密キー) は、公開鍵暗号化メカニズムを使用する前に生成されます。Horizon、Windows 用 Puttygen.exe、Linux 環境用ssh-keygen など、さまざまなメカニズムを使用して、キーペアを生成できます。 キーペアの生成について詳しくは、それぞれの方式のオンラインドキュメントを参照してください。

キーペアが利用可能になったら、権限のあるユーザーがアクセスできる安全な場所に秘密鍵をコピーします。 OpenStack では、Horizon または Nova ブートコマンドを使用して、VPX インスタンスにパブリックキーをデプ ロイできます。OpenStack を使用して VPX インスタンスをプロビジョニングすると、まず特定の BIOS 文字列 を読み取って、インスタンスが OpenStack 環境で起動していることを検出します。この文字列は「OpenStack Foundation」であり、Red Hat Linux ディストリビューションの場合は、/etc/nova/release に保存されます。こ れは、KVM ハイパーバイザープラットフォームに基づくすべての OpenStack 実装で利用できる標準的なメカニズ ムです。ドライブには特定の OpenStack ラベルが必要です。

ネットワ — ク構成、カスタムスクリプト、および SSH キーペアが提供されている場合は、構成ドライブが検出され ると、インスタンスがそれらを読み取ろうとします。

ユーザーデータファイル

NetScaler VPX インスタンスは、ユーザーデータファイルとも呼ばれるカスタマイズされた OVF ファイルを使用して、ネットワーク構成、カスタムスクリプトを注入します。このファイルは、構成ドライブの一部として提供されます。次に、カスタマイズされた OVF ファイルの例を示します。

```
1 ...
    <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
    <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"</pre>
3
4
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5 oe:id=""
   xmlns="http://schemas.dmtf.org/ovf/environment/1"
6
7
    xmlns:cs="http://schemas.citrix.com/openstack">
8
    <PlatformSection>
    <Kind></Kind>
9
```

```
<Version>2016.1</Version>
10
11
     <Vendor>VPX</Vendor>
12
     <Locale>en</Locale>
13
     </PlatformSection>
14
     <PropertySection>
15
     <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
      <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"/>
18
     <property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"</pre>
         />
     <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>
20
         10.1.2.1"/>
21
     </PropertySection>
22
       <cs:ScriptSection>
         <cs:Version>1.0</cs:Version>
23
           <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack</pre>
24
               " xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
25
               <Scripts>
                 <Script>
26
27
                        <Type>shell</Type>
28
                        <Parameter>X Y</Parameter>
29
                       <Parameter>Z</Parameter>
                       <BootScript>before</BootScript>
                         <Text>
                               #!/bin/bash
                               echo "Hi, how are you" $1 $2 >> /var/sample.
33
                                   txt
                         </Text>
34
                 </Script>
35
                 <Script>
37
                        <Type>python</Type>
                        <BootScript>after</BootScript>
38
39
                         <Text>
40
                              #!/bin/python
       print("Hello");
41
42
                         </Text>
43
                 </Script>
44
         <Script>
45
                        <Type>perl</Type>
                        <BootScript>before</BootScript>
46
47
                         <Text>
48
                              !/usr/bin/perl
       my $name = "VPX";
49
       print "Hello, World $name !\n" ;
50
51
                         </Text>
52
                 </Script>
53
                  <Script>
54
                       <Type>nscli</Type>
55
                       <BootScript>after</BootScript>
                       <Text>
```

```
add vlan 33
57
58
     bind vlan 33 -ifnum 1/2
59
                 </Text>
             </Script>
61
           </Scripts>
        </ScriptSettingSection>
    </cs:ScriptSection>
   </Environment>
64
65
      前のOVFファイルでは、「PropertySection」はNetScalerネットワーク構成
     に 使 用 さ れ 、 \<cs:ScriptSection> は す べ て の ス ク リ プ ト を 囲 む た め に 使 用
     されます。 \ \</Scripts> タグは、すべてのスクリプトをまとめるのに使
     われます。 各スクリプトは \<Script> \</Script>タグの間に定義されてい
     ます。 各スクリプトタグには、従属するフィールドやタグがあります。
```

a) <Type>: スクリプトタイプの値を指定します。指定可能な値: Shell/Perl/Python/NSLCI (NetScaler CLI ス クリプトの場合)

b) <Parameter>: スクリプトにパラメーターを指定します。各スクリプトでは、複数の <Parameter> タグを使用 できます。

c) <BootScript>: スクリプト実行ポイントを指定します。このタグに指定できる値: 前/後。「before」は、PE がア ップする前にスクリプトを実行することを指定します。「after」は、PE が起動した後にスクリプトが実行されること を指定します。

d) <Text>: スクリプトの内容を貼り付けます。

注

現在、VPX インスタンスはスクリプトのサニタイズを処理しません。管理者は、スクリプトの有効性を確認す る必要があります。

すべてのセクションを表示する必要はありません。空の「PropertySection」を使用して最初のブート時に実 行するスクリプトのみを定義するか、

OVF ファイル(ユーザーデータファイル)の必要なセクションが入力されたら、そのファイルを使用して VPX インスタンスをプロビジョニングします。

ネットワーク構成

ネットワーク構成の一部として、VPX インスタンスは以下を読み込みます。

- 管理 IP アドレス
- ネットワークマスク
- デフォルトゲートウェイ

パラメーターは、正常に読み取られると、インスタンスをリモートで管理できるように NetScaler 構成に移入されま す。パラメーターが読み取られない場合、または構成ドライブが存在しない場合は、インスタンスが以下のデフォル トの処理を実行します。

- DHCP から IP アドレス情報を取得する。
- DHCP で障害が発生するか、タイムアウトした場合、インスタンスはデフォルトのネットワーク設定 (192.168.100.1/16) で起動します。

カスタマースクリプト

VPX インスタンスでは、初期プロビジョニング中にカスタムスクリプトを実行できます。アプライアンスは、シェル、 Perl、Python、および Citrix ADC CLI コマンドタイプのスクリプトをサポートしています。

SSH キーペア認証

VPX インスタンスは、インスタンスメタデータの一部として構成ドライブ内で利用可能なパブリックキーをその 「authorized_keys」ファイルにコピーします。これにより、ユーザーが秘密キーを使用してインスタンスにアクセ スできるようになります。

注

SSH キーが提供されると、デフォルトの認証情報(nsroot/nsroot)は機能しなくなります。パスワードベー スのアクセスが必要な場合は、それぞれの SSH プライベートキーでログオンし、手動でパスワードを設定しま す。

はじめに

OpenStack 環境で VPX インスタンスをプロビジョニングする前に、.tgz ファイルから.qcow2ファイルを抽出し てビルドします。

qcow2 イメージからの OpenStack イメージ。以下の手順を実行します:

1. 次のコマンドを入力して、.tqzファイルから.qcow2ファイルを抽出します。

```
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. 次のコマンドを入力して、手順1で抽出した.qcoz2ファイルを使用して OpenStack イメージをビルドします。

図 1 : 次の図に、	glance	mage-create コマンドの	出力例を示します。
--------------------	--------	-------------------	-----------

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

VPX インスタンスのプロビジョニング

VPX インスタンスをプロビジョニングするには、次のいずれかの方法を使用します。

- Horizon (OpenStack ダッシュボード)
- Nova boot コマンド (OpenStack CLI)

OpenStack ダッシュボードを使用して VPX インスタンスをプロビジョニングする

Horizon を使用して VPX インスタンスをプロビジョニングするには、次の手順に従います。

- 1. OpenStack ダッシュボードにログオンします。
- 2. ダッシュボードの左側にある [プロジェクト] パネルで、[インスタンス] を選択します。
- 3. [インスタンス] パネルで、[インスタンスの起動] をクリックして、[インスタンスの起動] ウィザードを開きま す。

oject	~	Inst	tances										
Compute	×	Inst	tances			Filter			Q Flor	••	unch Instance	Set Reb	oof instances
Overview			Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Uptime	Actions
Volumes	1		dhcp	NS-VPX- 10-5-49-3	10.0.0.5	m1.medium 4GB RAM 2 VCPU 40.0GB Disk		Active	nova	None	Running	1 hour, 50 minutes	Create Snapshot Nore
Images			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 Mon
Access & Security Network	•		NS1000+10-5	NS-VPX- 10-5-49-3	10.0.0.2	m1.medium 4G8 RAM 2 VCPU 40 0G8 Disk		Active	nova	None	Running	2 hours, 16 minutes	Create Snapshot More

- 4. インスタンスの起動ウィザードで、次のような詳細を入力します。
 - a) Instance Name インスタンス名
 - b) Flavor インスタンスのフレーバー(種類)
 - c) Instance Count インスタンスの数
 - d) Instance Boot Source インスタンスの起動ソース
 - e) イメージ名

Details *	Access & Security *	Networking *	Post-Creation Adv	anced Options
Availability Z	one:		Specify the details for law	nching an instance
nova		•	The chart below shows th	e resources used by this project
Instance Nam	ne: *		in relation to the project'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. 次の手順を実行して、Horizon を介して新しいキーペアか既存のキーペアを展開します。

a) 既存のキーペアがない場合は、既存の方式を使用してキーを作成します。既存のキーがある場合は、この手順はスキップします。

- b) 公開キーの内容をコピーします。
- c) [Horizon] > [インスタンス] > [新しいインスタンスの作成] の順に選択します。
- d) [アクセスとセキュリティ] をクリックします。
- e) [**Key Pair**] ドロップダウンメニューの隣にある [+] 記号をクリックし、表示されるパラメータの値を入力 します。
- f) 公開鍵の内容を 公開鍵 ボックスに貼り付け、鍵に名前を付け、[鍵 ペアのインポート] をクリックします。

Key Pair Name *	Description:
NewKey	Description.
Public Key *	Key Pairs are how you login to your instance after it is launched.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjZjh mEducHd8almy/CPXO6/JupOPOM92d-NOv-7417	 Choose a key pair name you will recognise and paste your SSH public key into the space provided.
03te1FrwL38iGXbilByc2+oBV7ZIFRiYQEtk2UfM+ EtJJlcx92m4aln1RlgFvukXECHiXGqfQXVI06pyim	SSH key pairs can be generated with the ssh-keygen command:
KRWigXhl+h+tvPGS4iltJ3uWKwfh1PDGYkmgAik osA955L+W9ngVloVyaK40OuAqYCTwlQNBKVuZ GBQ4H9a Jaim01 oBw5u458/ Jbil8qNC+QYw5S2w	ssh-keygen -t rsa -f cloud.key
EcvsxOvhdb3LW9YADAVnihVK4NLeBc4HIsFeHI 5UY0IYyGk7aW/2SXjzkwRqZ8cX1Oba0XoDiCYN apP/OTEEB//wknsit#BSVE4v0ng3	 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
Servers, S. Trais, Services	After launching an instance, you login using the private key (the username might be different depending on the image you launched):
	ssh -i cloud.key <username>@<instance_ip></instance_ip></username>

- ウィザードの [ポスト作成] タブをクリックします。[カスタマイズスクリプト] で、ユーザーデータファイルの コンテンツを追加します。ユーザーデータファイルには、VPX インスタンスの IP アドレス、ネットマスクと ゲートウェイの詳細、およびカスタマースクリプトが含まれます。
- 7. キーペアを選択またはインポートした後、config-drive オプションをチェックし、**Launch** をクリックしま す。

Launch Instance					
Details *	Access & Security	Networking *	Post-Creation	Advanced Options	
Disk Partition	0		Specify advar	nced options to use when	n launching an
Automatic •		instance.			
 Configurati 	on Drive 😧				
				C	ancel Launch

OpenStack CLIを使用して VPX インスタンスをプロビジョニングする

OpenStack CLI を使用して VPX インスタンスをプロビジョニングするには、次の手順に従います。

1. qcow2 からイメージを作成するには、次のコマンドを入力します。

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

2. インスタンスを作成するイメージを選択するには、次のコマンドを入力します。

openstack image list | more

3. 特定のフレーバーのインスタンスを作成するには、次のコマンドを入力して、リストからフレーバー ID/名前 を選択します。

openstack flavor list

NIC を特定のネットワークに接続するには、次のコマンドを入力して、ネットワークリストからネットワーク
 ID を選択します。

openstack network list

5. インスタンスを作成するには、次のコマンドを入力します。

1	openstack server createflavor FLAVOR_IDimage IMAGE_ID
	key-name KEY_NAME
2	user-data USER_DATA_FILE_PATHconfig-drive Truenic net-id
	=net-uuid
3	INSTANCE_NAME
4	openstack server createimage VPX-ToT-Imageflavor m1.medium
	user-data
5	ovf.xmlconfig-drive Truenic net-id=2734911b-ee2b-48d0-a1b6
	-3efd44b761b9
6	VPX-ToT

図 2: 次の図は、出力例を示しています。

+	+
Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
0S-EXT-SRV-ATTR:host	None
0S-EXT-SRV-ATTR:hypervisor hostname	None
0S-EXT-SRV-ATTR:instance name	instance-000001c2
OS-EXT-STS:power_state	i Ø
0S-EXT-STS:task state	, scheduling
OS-EXT-STS:vm state	building
0S-SRV-USG:launched at	l 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)
key_name	None
name	IVPX-ToT
<pre>os-extended-volumes:volumes_attached</pre>	1 []
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	1
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935
4	

仮想マシンマネージャーを使用して NetScaler VPX インスタンスをプロビジョニング します

January 28, 2025

Virtual Machine Manager は、VM ゲストを管理するためのデスクトップツールです。これによって新しい VM ゲ ストおよびさまざまな種類のストレージを作成し、仮想ネットワークを管理できます。組み込み VNC ビューアーに より VM ゲストのグラフィカルコンソールにアクセスして、ローカルまたはリモートでパフォーマンス統計を閲覧で きます。

優先 Linux ディストリビューションをインストールした後、KVM 仮想化を有効にして、仮想マシンのプロビジョニ ングを処理できます。

仮想マシンマネージャーを使用して NetScaler VPX インスタンスをプロビジョニングする場合、2 つのオプション があります。

- 手動で IP アドレス、ゲートウェイ、およびネットマスクを入力する
- IP アドレス、ゲートウェイ、ネットマスクを自動的に割り当てる (自動プロビジョニング)

NetScaler VPX インスタンスのプロビジョニングには、次の2種類のイメージを使用できます。

- RAW
- QCOW2

NetScaler VPX RAW イメージを QCOW2 イメージに変換して、NetScaler VPX インスタンスをプロビジョニング できます。RAW イメージを QCOW2 イメージに変換するには、次のコマンドを入力します。

qemu-img convert -0 qcow2 original-image.raw image-converted.qcow2

例:

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

KVM での一般的な NetScaler VPX 展開には、次の手順があります。

- NetScaler VPX インスタンスの自動プロビジョニングの前提条件の確認
- RAW イメージを使用した NetScaler VPX インスタンスのプロビジョニング
- QCOW2 イメージを使用した NetScaler VPX インスタンスのプロビジョニング
- 仮想マシンマネージャを使用して VPX インスタンスにインタフェースを追加する

NetScaler VPX インスタンスの自動プロビジョニングの前提条件を確認する

自動プロビジョニングはオプション機能であり、CDROM ドライブからのデータの使用を伴います。この機能が有効 になっている場合は、初期セットアップ時に、NetScaler VPX インスタンスの管理 IP アドレス、ネットワークマス ク、およびデフォルトゲートウェイを入力する必要があります。

VPX インスタンスを自動プロビジョニングする前に、次のタスクを完了する必要があります。

- 1. カスタマイズされたオープン仮想化形式 (OVF) XML ファイルまたはユーザーデータファイルを作成します。
- 2. オンラインアプリケーション(たとえば、PowerISO)を使用して、OVF ファイルを ISO イメージに変換します。
- 3. セキュアコピー (SCP) ベースのツールを使用して、ISO イメージを KVM ホストにマウントします。

サンプル **OVF XML** ファイル:

次に、OVF XML ファイルの内容の例を示します。このファイルをサンプルとして使用して、ファイルを作成することができます。

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
1
2
3
     <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`</pre>
4
     xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`
5
6
7
     oe:id=""
8
     xmlns="`http://schemas.dmtf.org/ovf/environment/1"`
9
10
     xmlns:cs="`http://schemas.citrix.com/openstack">`
11
12
     <PlatformSection>
13
14
```

15 16	<kind></kind>
10 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	(Decembra contraction of the interception ment in the classical sector)
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	

前述の OVF XML ファイルでは、NetScaler ネットワーク構成に「PropertySection」が使用されています。ファ イルを作成するときには、この例の最後で強調表示されている、パラメーターの値を指定します。

- 管理 IP アドレス
- ネットマスク
- Gateway

```
重要
```

OVF ファイルが適切に XML 形式になっていない場合、VPX インスタンスにはファイルに指定されている値で はなく、デフォルトのネットワーク構成が割り当てられます。

RAW イメージを使用して NetScaler VPX インスタンスをプロビジョニングします

Virtual Machine Manager では、RAW イメージを使用して NetScaler VPX インスタンスをプロビジョニングできます。

仮想マシンマネージャーを使用して NetScaler VPX インスタンスをプロビジョニングするには、次の手順に従います。

- 仮想マシンマネージャー (アプリケーション>システムツール>バーチャルマシンマネージャー)を開き、[認証] ウィンドウにログオン資格情報を入力します。
- 新しい NetScaler VPX インスタンスを作成するには、 アイコンをクリックするか、localhost (QEMU) を右クリックします。

Ve localhost.localdomain:6 (admin	n)		- 0 💌
Activities Wirtual	Machine Manager		Thu 02:24 🖌
			Virtual Machine Manager
File Edit View Help			
🔛 🗏 Open 🗇 💠	·		
Name			
Localhost (GEMU)	Mary		
	Connect		1
	Disconnect		
	Delete		
	Dgtails		
x			

- 3. 名前テキストボックスに、新しい仮想マシンの名前 (たとえば、NetScaler-VPX) を入力します。
- 4. [新規 VM] ウィンドウの [オペレーティングシステムのインストール方法を選択] で [既存のディスクイメージをインポートする] を選択し、[転送] をクリックします。

V localhost.localdomain6 (admin) Activities	nager	Thu 02:26 Virtual Machine Manager
File Edit View Help		
🔛 🗐 Open 🗇 💷 🖪 👻		
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.「既存のストレージパスを指定」フィールドで、画像へのパスをナビゲートします。オペレーティングシステム 種類に UNIX、バージョンとして FreeBSD 6.x を選択します。次に、「進む」をクリックします。

V 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: /libvirt/images/NSVPX-KVM-10.1-118.7_nc.raw Browse	
	Choose an operating system type and version OS type: UNIX Version: FreeBSD 6.x Cancel Back Forward	-

- 6.「メモリと **CPU** の設定を選択」で次の設定を選択し、「転送」をクリックします。
 - メモリ (RAM) -2048MB
 - CPU -2

V localhost.localdomain:6 (admin)		
		Virtual Machine Manager
File Edit View Help		
🞑 🗐 Open ⊳ 🔟 👩 🗸		
Name		
localhost (GEMU)		
	New VM	
	Create a new virtual machine Step 3 of 4	
	Choose Memory and CPU settings	1
	Memory /PAM): 2048 MB	
	Lin to 96658 M8 available on the host	
	Linta 12 malable	
	OP TO AL BREAK	
	Court But Ecourt	
	Cancet Back Porward	
•	*	

 を選択します。インストール前に構成をカスタマイズする チェックボックスを選択します。オプションで、[詳細オプション] で MAC アドレスをカスタマイズできます。選択した Virt タイプが KVM で、選択されたア ーキテクチャが x86_64 であることを確認します。[完了] をクリックします。

acalbert (OEMLI)		
ocaniosc (acciso)	New VM	
	Create a new virtual machine Step 4 of 4	
	Ready to begin installation of NetScaler-VPX	
	OS: FreeBSD 6.x Install: Import existing OS image	
	Memory: 2048 MB	
	CPUs: 2	
	Storage: 20.0 GB /var/Lb/Lb/vt/mages/NSVPX-KVM-10.1-118.7_n	
	✓ Advanced options	
	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. NIC を選択し、次の構成を指定します。
 - Y-スデバイス: ethX macvtap またはブリッジ
 - デバイスモデル—virtio
 - ソースモード Bridge

- 9. [適用] をクリックします。
- VPX インスタンスを自動プロビジョニングする場合は、このドキュメントの「CDROM ドライブを接続して 自動 Provisioning を有効にする」セクションを参照してください。それ以外の場合は、[インストレーショ ンを開始] をクリックします。KVM で Citrix ADC VPX をプロビジョニングしたら、インターフェイスを追加 できます。

QCOW2 イメージを使用して Citrix ADC VPX インスタンスをプロビジョニングする

仮想マシンマネージャーを使用すると、QCOW2 イメージを使用して NetScaler VPX インスタンスをプロビジョニ ングできます。

QCOW2 イメージを使用して Citrix ADC VPX インスタンスをプロビジョニングするには、次の手順に従います。

- 1. RAW イメージを使用した Citrix ADC ****VPX** インスタンスのプロビジョニングの手順 **1**~ステップ **8** に従い ます **。
 - 注 必ず **QCOW2** の の画像 ステップ **5**.
- 2. Disk1を選択し、[詳細オプション]をクリックします。

3. [ストレージ形式] ドロップダウンリストから [qcow2] を選択します。

48	test Virtual Machine	_ + ×
🞻 Begin Installation 🛛 💥 Can	el	
Overview Processor Memory Boot Options Input Input Display Spice Sound: default Console Channel Video Default	Virtual Disk Target device: Disk1 Source path: /home/dummy_dut/NSVPX-KVM-11.1-12.5_nc.qcow Storage size: 788.25 MB Readonly: □ Shareable: □ ◇ Advanced options Disk bus: default ◇ Serial number: Storage format: qcow2 ◇ Performance options Cache mode: default ◇ IO mode: default ◇ X IO Timing	
	Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS	

4. [**Apply**] をクリックし、次に [**Begin Installation**] をクリックします。KVM で Citrix ADC VPX をプロビ ジョニングしたら、インターフェイスを追加できます。

CD-ROM ドライブを接続して自動プロビジョニングを有効にする

- 1. ハードウェアの追加 > ストレージ > デバイスタイプ > CDROM デバイスをクリックします。
- 2. [管理] をクリックし、 [NetScaler VPX インスタンスの自動プロビジョニングの前提条件] セクションで マウントした正しい ISO ファイルを選択し、 [完了] をクリックします。NetScaler VPX インスタンスの [Resources] の下に新しい CDROM が作成されます。



3. VPX インスタンスの電源をオンにすると、スクリーンショットの例で示すように、OVF ファイルで提供され ているネットワーク構成を使用して自動プロビジョニングが行われます。

_	Кеу				
) 🚺 🕨 🛄 🕑 🔹 🕞					
Aum 11 10:14:55 ≮local0).alert> ns restar	t[2578]: Restar	•t: ∠netsca	ler/nsstar	t.sh
exited normally. Exit	code (0)	villorol. noovar	0. / 100000	1017 100 001	0.01
Aug 11 10:14:55 <local6< td=""><td>).alert> ns restar</td><td>t[2578]: Succ</td><td>essfully d</td><td>eregistere</td><td>d wit</td></local6<>).alert> ns restar	t[2578]: Succ	essfully d	eregistere	d wit
h Pitboss					
login: nsroot					
Password:					
Aug 11 10:15:04 (auth.r	iotice> ns login: 3 The FreeRSD Proj	RUUT LUGIN (nsr	oot) UN tt	yv0	
Conuright (c) 1979, 198	RA. 1983. 1986. 19	ест. 88. 1989. 1991.	1992. 199	3. 1994	
Copyright (c) 1979, 198 The Regents of	30, 1983, 1986, 19 the University of	ect. 88, 1989, 1991, California. Al	1992, 199 l rights r	3, 1994 eserved.	
Copyright (c) 1979, 198 The Regents of	30, 1983, 1986, 19 the University of	ect. 88, 1989, 1991, California. Al	1992, 199 rights r	3, 1994 eserved.	
Copyright (c) 1979, 198 The Regents of Done S sh in	30, 1983, 1986, 19 the University of	ect. 88, 1989, 1991, California. Al	1992, 199 1 rights r	3, 1994 eserved.	
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress	30, 1983, 1986, 19 the University of Traffic Domain	ест. 88, 1989, 1991, California. Al Туре	1992, 199 1 rights r Mode	3, 1994 eserved. Arp	Істр
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress Vserver State	30, 1983, 1986, 19 the University of Traffic Domain	ест. 88, 1989, 1991, California. Al Туре	1992, 199 1 rights r Mode	3, 1994 eserved. Arp	Icmp
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress Userver State	Traffic Domain	ECL. 88, 1989, 1991, California. Al Type 	1992, 1993 I rights r Mode	3, 1994 eserved. Arp 	Icmp
Copyright (c) 1979, 198 The Regents of Done > sh ip Userver State 	00, 1983, 1986, 19 the University of Traffic Domain 	California. Al Type NetScaler IP	1992, 1993 I rights r Mode Active	3, 1994 eserved. Arp Enabled	Icmp Enab
Copyright (c) 1979, 198 The Regents of Done > sh ip Userver State 	00, 1983, 1986, 19 the University of Traffic Domain 	California. Al Type NetScaler IP	1992, 1993 I rights r Mode Active	3, 1994 eserved. Arp Enabled	Icmp Enab
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress Userver State 	0, 1983, 1986, 19 the University of Traffic Domain 0	ECL. 88, 1989, 1991, California. Al Type NetScaler IP	1992, 1993 I rights r Mode Active	3, 1994 eserved. Arp Enabled	Icmp Enab
Copyright (c) 1979, 198 The Regents of Done > sh ip Upaddress Vserver State 	09. 1983, 1996, 19 the University of Traffic Domain 0 allO.alert> ns rest	ect. 88, 1989, 1991, California. Al Type NetScaler IP art[2578]: Ns	1992, 1993 I rights r Mode Active sshutdown I	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab sed !
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress Vserver State 	00, 1983, 1996, 19 the University of Traffic Domain 0 allO.alert> ns rest	ect. 88, 1989, 1991, California. Al Type NetScaler IP art[2578]: Ns	1992, 1993 I rights r Mode Active sshutdown I	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab sed !
Copyright (c) 1979, 198 The Regents of Done > sh ip Ipaddress Userver State 	09. 1983, 1996, 19 the University of Traffic Domain 0 alO.alert> ns rest	ect. 88, 1989, 1991, California. Al Type NetScaler IP art[2578]: Ns	1992, 1993 I rights r Mode Active sshutdown I	3, 1994 eserved. Arp Enabled ock releas	Icmp Enab :ed !

 自動プロビジョニングが失敗した場合、インスタンスはデフォルトの IP アドレス(192.168.100.1)で起動 します。その場合は、初期設定を手動で完了する必要があります。詳細については、「ADC を初めて構成する」 を参照してください。

仮想マシンマネージャーを使用して、NetScaler VPX インスタンスにインターフェイスを追加する

KVM で NetScaler VPX インスタンスをプロビジョニングしたら、インターフェイスを追加できます。

インターフェイスを追加するには、次の手順を実行します。

- 1. KVM の上で動作している NetScaler VPX インスタンスをシャットダウンします。
- 2. VPX インスタンスを右クリックし、ポップアップメニューから [Open] を選択します。
- 3. ヘッダーの アイコンをクリックすると、仮想ハードウェアの詳細が表示されます。
- 4. [ハードウェアの追加] をクリックします。[Add New Virtual Hardware] ウィンドウで、ナビゲーション メニューから [Network] を選択します。



- 5. [Host Device] フィールドで、物理インターフェイスの種類を選択します。ホストデバイスの種類は、Bridge または MacVTap のいずれかにできます。macvTap の場合、VEPA モード、ブリッジ、プライベート、パス スルーの 4 つのモードが可能です。
 - a) Bridge の場合
 - i. ホストデバイス—「共有デバイス名の指定」オプションを選択します。
 - ii. KVM ホストで構成される Bridge 名を指定します。

```
注
KVM ホストに Linux ブリッジを設定し、物理インターフェイスをブリッジにバインドし、
ブリッジを UP 状態にしていることを確認します。
```



iii. デバイスモデル-virtio。

iv. [完了] をクリックします。

- b) MacVTap 用
 - i. ホストデバイス-メニューから物理インターフェイスを選択します。
 - ii. デバイスモデル-virtio。

		Add New Vi	irtual	Hardware	•			
2	Storage	Network						
F	Network	Network						
	Input	Please indicate how	w you'	d like to co	onnect	your		
	Graphics	new virtual netwo	rk devi	ce to the l	host ne	twork.		
F	Sound	Host device:	Hos	t device m	acvtap	2 : macvtap	0	
=	Serial							
	Parallel	MAC address:		52:54:00:	fb:bb:e	5		
1	Channel	Device model:	virti	0				
3	USB Host Device	Device model.				<u> </u>		
à	PCI Host Device							
	Video							
ſ	Watchdog							
	Filesystem							
2	Smartcard							
					ſ	Grand	ר ה	r
						Cancel		L

iii. [完了]をクリックします。ナビゲーションペインで新しく追加された NIC を見ることができます。

		NetS	caler-VPX Virtual	Mach	ine			
ile	Virtual Machine View	Send Key						
		× [
5	Overview	Virtual Network	Interface					
	Performance	Source device:	Host device p1p1	: macv	tap	0		
	Processor	Davies medale		^	-			
9.s	Memory Reat Options	Device model:	virtio	~				
32	Boot Options	MAC address:	52:54:00:a9:77:fc					
	IDE Disk I	Source mode:	Default					
	NIC ::00:22:00	h	VEPA					
er à	Micca9.77.ic	P Virtual port	Bridge					
	Display VNC		Private					
j	Sound: ich6		Passthrough					
2	Serial 1							
<u>y</u>	Video							
	Controller USB							
	Controller IDE							
					_			
	Add Hardware				R	emove	Cancel	Apply

- iv. 新しく追加された NIC を選択して、この NIC の Source モードを選択します。利用可能なモード は VEPA、Bridge、Private、および Passthrough です。インターフェイスとモードについて詳 しくは、「ソースインターフェイスおよびモード」を参照してください
- V. [適用] をクリックします。
- 6. VPX インスタンスを自動プロビジョニングする場合は、このドキュメントの「自動プロビジョニングを有効に するための構成ドライブの追加」セクションを参照してください。それ以外の場合は、VPX インスタンスをパ ワーオンして初期構成を手動で完了します。

重要:

スピード、デュプレックス、オートネゴシエーションなどの Interface パラメーター構成はサポートされません。
SR-IOV ネットワークインターフェースを使用するように NetScaler VPX インスタン

スを構成する

January 15, 2025

Linux-KVM プラットフォームで実行される NetScaler VPX インスタンスは、次の NIC でシングルルート I/O 仮想 化(SR-IOV)を使用して構成できます。

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- インテル X722 10G

詳細については、以下を参照してください。NetScaler VPX でサポートされている NIC.

このセクションでは、次の方法について説明します。

- SR-IOV ネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する
- SR-IOV インターフェイスで静的 LA/LACP を構成する
- SR-IOV インターフェイスで VLAN を構成する

制限事項

インテル 82599、X710、XL710、X722 の NIC を使用する場合は、制限事項に留意してください。次の機能はサポートされません。

インテル 82599 NIC の制限事項:

- L2 モード切り替え
- 管理パーティション化(共有 VLAN モード)
- 高可用性(アクティブ/アクティブモード)
- ジャンボフレーム。
- IPv6: SR-IOV インターフェイスが1つ以上ある場合は、VPX インスタンスで最大 30 個までの一意の IPv6 アドレスのみを設定できます。
- ip linkコマンドによる SRIOV VF インターフェイスのハイパーバイザでの VLAN 設定はサポートされて いません。
- スピート、デュプレックス、オートネゴシエーションなどの Interface パラメーター構成はサポートされません。

インテル X710 10G、インテル XL710 40G、インテル X722 10G NIC の制限事項:

- L2 モード切り替え
- 管理パーティション化(共有 VLAN モード)

- クラスタでは、XL710 NIC がデータ・インタフェースとして使用されている場合、ジャンボフレームはサポートされません。
- インターフェイスが切断され、再接続されると、インターフェイスリストが順序変更されます。
- スピート、デュプレックス、オートネゴシエーションなどの Interface パラメーター構成はサポートされません。
- インターフェイス名は、Intel X710 10G、Intel XL710 40G、Intel X722 10G NIC の場合は 40/X
- VPX インスタンスでは、最大 16 個のインテル XL710/X710/X722 SRIOV または PCI パススルーインターフ ェイスをサポートできます。

```
注
```

Intel X710 10G、Intel XL710 40G、および Intel X722 10G NIC で IPv6 をサポートするには、KVM ホスト で次のコマンドを入力して、仮想機能 (VF) の信頼モードを有効にする必要があります。

ip link set <PNIC> <VF> trust on

例

ip link set ens785f1 vf 0 trust on

前提条件

SR-IOV ネットワークインターフェイスを使用するように NetScaler VPX インスタンスを構成する前に、次の前提 条件となるタスクを完了してください。対応するタスクを完了する方法の詳細については、「NIC」列を参照してくだ さい。

タスク	Intel 82599 NIC	インテル X710、XL710、X722 NIC
 NIC を KVM ホストに追加します。 最新の Intel ドライバーをダウンロードしてインストールします 	- IXGBE ドライバー	- 140E ドライバー
しょす。 1. KVM ホスト上のドライバー をブロック リストに追加しま す。	/etc/modprobe.d/blacklist.conf ファイルに次のエントリを追加しま す。blacklist ixgbevf。 IXGBE ドライバーのバージョン 4.3.15 を使用します (推奨)。	/etc/modprobe.d/blacklist.conf ファイルに次のエントリを追加しま す。blacklist i40evf。 i40e ドライバーのバージョン 2.0.26 を使用します(推奨)。

タスク	Intel 82599 NIC	インテル X710、XL710、X722 NIC
 KVM ホストで SR-IOV 仮想 機能 (VF) を有効にします。 次の 2 つの列の両方のコマン ドで、number_of_VFs = 作成する仮想 VF の数。 device_name = インタ ーフェイス名です。 VF の作成に使用したコマン 	以前のバージョンのカーネル 3.8 を 使用している場合は、次のエントリ を /etc/modprobe.d/ixgbe ファ イルに追加し、KVM ホストを再起動 します。options ixgbe max_vfs=< number_of_VFs>。カー ネル 3.8 以降を使用している場合は、 次のコマンドを使用して VF を作成 します。echo < number_of_VFs> > ; /sys/class/net/< device_name>/ device/sriov_numvfs。図 1の例を参照してください。 図 3 の例を参照してください。	以前のバージョンのカーネル 3.8 を 使用している場合は、 /etc/modprobe.d/i40e.conf ファ イルに次のエントリを追加し、KVM ホストを再起動します。options i40e max_vfs=< number_of_VFs>。カー ネル 3.8 以降を使用している場合は、 次のコマンドを使用して VF を作成 します。echo< number_of_VFs> > ; /sys/class/net/< device_name>/ device/sriov_numvfs。図 2 の例を参照してください。 図 3 の例を参照してください。

ドを rc.local ファイルに追加

して、VF を永続化します。

重要:

SR-IOV VF を作成するときは、MAC アドレスを VF に割り当てないようにしてください。

図 1: インテル 82599 10G NIC の KVM ホストで SR-IOV VF を有効にする

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

図 2: インテル X710 10G および XL710 40G NIC の KVM ホストで SR-IOV VF を有効にする

rooteubuntu: # lenci Lamon 710	DIGINAL
roteduritu.~# tspet i grep /10	
03:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP	+ (rev 01)
03:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP	+ (rev 01)
03:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP	+ (rev 01)
03:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP	+ (rev 01)
03:06.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:06.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0a.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0a.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0a.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0a.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0e.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0e.1 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0e.2 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
03:0e.3 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 01)	
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QS	FP+ (rev 01)
82:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QS	FP+ (rev 02)
82:00.1 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QS	FP+ (rev 02)
82:02.0 Ethernet controller: Intel Corporation XL710/X710 Virtual Function (rev 02)	
82:02.1 Ethernet controller: Intel Corporation XL 710 /X 710 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:~#	

図 3: インテル X722 10G NIC の KVM ホストで SR-IOV VF を有効にする

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

図 4: VF を永続的にする



SR-IOV ネットワークインターフェイスの使用を NetScaler ADC VPX インスタンスで構成する

仮想マシンマネージャを使用して SR-IOV ネットワークインターフェイスを使用するように NetScaler ADC VPX イ ンスタンスを構成するには、次の手順を実行します。

- 1. NetScaler VPX インスタンスの電源を切ります。
- 2. NetScaler VPX インスタンスを選択して、[Open] をクリックします。



3. <virtual machine on KVM> ウィンドウで、i アイコンを選択します。

BEM			Demo_VPX on QEMU/KVM	+ - • ×
File	Virtual Machine View	Send Key		
	🕐 🕨 🚺 🖉 🔹	6		a 12
	Overview	Basic Details		
-1/	Performance	Name:	Demo_VPX	
	CPUs	UUID:	2f82dfa1-ae7d-46bf-b63f-833387798cf0	
	Memory	Status:	Shutoff (Destroyed)	
20	Boot Options	Title:		
0	IDE Disk 1	Description:		
	NIC :7f:81:87			
	Mouse			
	Keyboard			
	Display VNC	Hypervisor D	etails	
	Sound: ich6	Hypervisor:	KVM	
	Serial 1	Architecture:	x86_64	
2	Channel spice	Emulator:	/usr/bin/kvm-spice	
	Video QXL	Firmware:	BIOS	
	Controller USB	chipset.	1440FA	
	Controller PCI			
	Controller IDE			
	Controller VirtlO Serial		^	
1	USB Redirector 1			
1	USB Redirector 2			
	Add Hardware			Cancel Apply

4. [ハードウェアの追加]を選択します。

MM		Demo_VPX on QEMU/KVM	↑ _ □ X
File	Virtual Machine View Send	Key	
		Add New Virtual Hardware	ع ع
	Ove Storage Perfi Controller Perfi Network Input Graphics Boot Sound Boot Parallel IDE Parallel NIC Console Mou USB Host Device Keyt PCI Host Device Sour Watchdog Sour Filesystem Seria Smartcard Char USB Redirection Vide Panic Notifier Cont Smartcard USB Redirector 1 USB Redirector 1	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	

- 5. [新しい仮想ハードウェアの追加] ダイアログボックスで、次の操作を行います。
 - a) [PCI ホストデバイス] を選択します。
 - b) [Host Device] セクションで、作成した VF を選択して、 [Finish] をクリックします。

図 **4**: インテル 82599 10G NIC の VF

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



<u>191</u>		Add New Virtual Hardware	\uparrow \times
	Storage Controller Network	PCI Device Host Device:	
	Graphics Sound Serial Parallel Console Channel USB Host Device	0000:02:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Con 0000:02:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Con 0000:03:00:0 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:1 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:2 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+ 0000:03:00:3 Intel Corporation Ethernet Controller X710 for 10GbE SFP+	ine Inti (Inti (Inti (Inti
	PCI Host Device Video Watchdog Filesystem Smartcard USB Redirection TPM RNG Panic Notifier	0000:03:06:1 listel 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 0000:03:0E:0 Intel Corporation XL710/X710 Virtual Function 0000:03:0E:1 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 🗸 🗸 Fin	ish

図 6 : イン	√テル X722	10G N	NICの	VF
-----------------	----------	-------	------	----

age troller vork t ohics nd al llel	PCI Device Host Device: U000:81:02:6 Intel Corporation XL710/X710 Virtual Function (Interface enp12) 0000:81:02:7 Intel Corporation XL710/X710 Virtual Function (Interface enp12) 0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12) 0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12)
troller vork t phics nd al llel	Host Device: 0000:81:02:6 Intel Corporation XL/10/X/10 Virtual Function (Interface enp12 0000:81:02:7 Intel Corporation XL/10/X710 Virtual Function (Interface enp12 0000:81:03:0 Intel Corporation XL/10/X710 Virtual Function (Interface enp12 0000:81:03:1 Intel Corporation XL/10/X710 Virtual Function (Interface enp12
vork t ohics nd al Ilel	Host Device: 0000:81:02:6 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:02:7 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12
t bhics nd al Ilel	0000:81:02:6 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:02:7 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12
ohics nd al Ilel	0000:81:02:7 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12
nd al IIel	0000:81:03:0 Intel Corporation XL710/X710 Virtual Function (Interface enp12 0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12
al Ilel	0000:81:03:1 Intel Corporation XL710/X710 Virtual Function (Interface enp12
llel	이 이 이 것 같은 것 같은 것 같은 것 같은 것 같이 다 있는 것 같은 것 같이 있는 것 같은 것 같이 있는 것 같이 없는 것 같이 있는 것 같이 없는 것 같이 없 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 것 같이 않는 것 같이 없는 것 같이 없다. 것 같이 없는 것 같이 없다. 같이 없는 것 같이 없다. 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 않은 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 않는 것 같이 않는 것 같이 없는 것 같이 없는 것 같이 없다. 것 같이 않는 것 같이 없는 것 같이 없는 것 같이 없는 것 같이 없다. 않는 것 같이 없는 것 같이 없다. 않는 것 같이 않는 것 같이 않는 것 같이 않는 것 같이 없다. 않는 것 같이 않는 것 같이 없다. 않는 것 같이 않 않는 것 같이 않는 않 않이 않는 것 같이 않 않는 것 같이 않는 것 같이 않는 것 같이 않이 않이 않는 것 같이 않는 것 같이 않이 않이 않이 않는 것 같이 않는 것 같이 않이 않 않이 않 않이 않 않이 않 않이 않 않이 않이
	0000:82:00:0 Intel Corporation
sole	0000:83:03:0 Intel Corporation
nnel	0000:84:00:0 Intel Corporation (Interface enp132s0f0)
Host Device	0000:84:00:1 Intel Corporation (Interface enp132s0f1)
lost Device	0000:84:02:0 Intel Corporation (Interface enp132s2)
0	0000:84:0A:0 Intel Corporation (Interface enp132s10)
chdog	0000:FF:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
ystem	0000:FF:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
rtcard	0000:FF:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI Link 0
Redirection	0000:FF:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 8
	0000:FF:0B:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 8
i.	0000:FF:0B:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 QPI Link 0 8
c Notifier	0000:FF:0C:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 Unicast Regist
F	Redirection Notifier

- 6. 手順4と5を繰り返し、作成したVFを追加します。
- 7. NetScaler VPX インスタンスをパワーオンします。
- 8. NetScaler VPX インスタンスがパワーオンしたら、次のコマンドを使用して構成を確認します。

1 show **interface** summary

構成したすべてのインターフェイスが出力に表示されます。

図 6: インテル 82599 NIC の出力サマリー

UUM				Demo_VPX on QEMU/KVM		↑ _ □ ×
File	Virtua	Machine View	w Send Key			
		• • • •				
	> sho	w interface	summary			
		Interface	MTU	MAC	Suffix	
	1	0/1	1500	52:54:00:7f:81:87	NetScaler Virtual Interfa	ce
	2	10/1	1500	8e:e7:e7:06:50:3f	Intel 82599 10G VF Interf	ace
	3	10/2	1500	8e:1a:71:cc:a8:3e	Intel 82599 10G VF Interf	ace
	4	L0/1	1500	52:54:00:7f:81:87	Netscaler Loopback interfa	ace
	Done >					

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

図 7 . インテル X710 および XL710 NIC 0	の出力サマ	リー。
--	-------	-----

SR-IOV インターフェイスでスタティック LA/LACP を設定する

重要:

SR-IOV VF を作成する場合、MAC アドレスを VF に割り当てていないことを確認してください。

リンクアグリゲーションモードで、SR-IOV VF を使用するには、作成した VF のなりすましチェックを無効にします。 KVM ホストでなりすましチェックを無効にするには、以下のコマンドを使用します。

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

各項目の意味は次のとおりです:

- Interface_name -インターフェイス名です。
- VF_id -Virtual Function ID です。

佦	٠
12.1	٠

Terminal - root@ubuntu: /etc	- E ×
File Edit View Terminal Tabs Help	
<pre>root@ubuntu:/etc# ip link show ens3f0 6: ens3f0: <broadcast,multicast,up,lower up=""> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 0c:c4:7a:b0:50:7e brd ff:ff:ff:ff:ff vf 0 MAC 8e:e7:e7:e0:50:3f, spoof checking on, link-state auto</broadcast,multicast,up,lower></pre>	
root@ubuntu:/etc#	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip link snow ens311	
7: ens311: <broadcasy,multicast,up,lower up=""> mtu 1500 gdisc mq state UP mode DEFAULT group default glen 1000 link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff:ff:ff vf 0 MAC 8e:la:7l:cc:a8:3e, spoof checking on, link-state auto</broadcasy,multicast,up,lower>	
root@ubuntu:/etc#	
root@ubuntu:/etc# ip link set ens3f0 vf θ spoofchk off	
root@ubuntu:/etc# ip_link_show_ens3f0	
6: ens3f0: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 0c:c4:7a:bd:50:7e brd ff:ff:ff:ff:ff:ff:ff vf 0 MAC 8e:e7:e7:e0:550:3f, spoof checking off, link-state auto</broadcast,multicast,up,lower_up>	
root@ubuntu:/etc# ip link set ens3f1 vf θ spoofchk off	
root@ubuntu:/etc# ip link show ens3f1	
7: ens3f1: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 0c:c4:7a:bd:50:7f brd ff:ff:ff:ff:ff:ff</broadcast,multicast,up,lower_up>	
vf 0 MAC 8e:la:71:cc:a8:3e, spoof checking off, link-state auto	
root@ubuntu:/etc#	

作成したすべての VF のなりすましチェックを無効にします。NetScaler VPX インスタンスを再起動し、リンクアグ リゲーションを構成します。詳細な手順については、リンク集約の設定を参照してください。

SR-IOV インターフェイスで VLAN を構成する

SR-IOV VF で VLAN を構成できます。詳細な手順については、VLAN の設定を参照してください。

重要:

KVM ホストに VF インターフェイスの VLAN 設定が含まれていないことを確認してください。

SR-IOV モードでの **SSL** アクセラレーションに **Intel QAT** を使用するように **KVM** ハ イパーバイザー上の **NetScaler VPX** を構成します

October 17, 2024

Linux KVM ハイパーバイザー上の NetScaler VPX インスタンスは、Intel クイックアシストテクノロジー(QAT) を使用して NetScaler SSL のパフォーマンスを高速化できます。インテル QAT を使用すると、レイテンシーの高い 暗号処理をすべてチップにオフロードできるため、1 つまたは複数のホスト CPU を解放して他のタスクを実行でき るようになります。

以前は、NetScaler データパスの暗号化処理はすべて、ホスト vCPU を使用するソフトウェアで行われていました。

注

現在、NetScaler VPX はインテル QAT ファミリーの C62x チップモデルのみをサポートしています。この機能は、NetScaler リリース 14.1 ビルド 8.50 以降でサポートされています。

前提条件

• Linux ホストには、マザーボードに直接統合されているか、外部 PCI カードに追加された Intel QAT C62x チップが搭載されています。

Intel QAT C62x シリーズ モデル: C625、C626、C627、C628。これらの C62x モデルのみに公開キー暗号 化 (PKE) 機能が含まれています。その他の C62x バリアントは PKE をサポートしていません。

• NetScaler VPX は、VMware ESX のハードウェア要件を満たしています。詳細については、「Linux KVM プ ラットフォームに NetScaler VPX インスタンスをインストールする」を参照してください。

制限事項

個々の VM 用に暗号ユニットや帯域幅を予約する規定はありません。Intel QAT ハードウェアで使用可能なすべての 暗号ユニットは、QAT ハードウェアを使用するすべての VM で共有されます。 インテル QAT を使用するためのホスト環境のセットアップ

 Linux ホストに C62x シリーズ (QAT) チップモデル用の Intel 提供のドライバーをダウンロードしてイン ストールします。Intel パッケージのダウンロードとインストール手順の詳細については、Linux 用 Intel QuickAssist テクノロジー・ドライバーを参照してください。readme ファイルはダウンロードパッケージ に含まれています。ダウンロード パッケージの一部として readme ファイルが提供されます。このファイル には、パッケージをコンパイルしてホストにインストールする手順が記載されています。

ドライバをダウンロードしてインストールしたら、次の健全性チェックを行います:

- C62x チップの数に注意してください。各 C62x チップには、最大 3 つの PCle エンドポイントがあります。
- すべてのエンドポイントが稼働していることを確認します。adf_ctl status コマンドを実行して、すべての PF エンドポイント (最大 3 つ)のステータスを表示します。

```
1 root@Super-Server:~# adf_ctl status
2
3 Checking status of all devices.
4 There is 51 QAT acceleration device(s) in the system
5 qat_dev0 - type: c6xx, inst_id: 0, node_id: 0, bsf:
        0000:1a:00.0, #accel: 5 #engines: 10 state: up
6 qat_dev1 - type: c6xx, inst_id: 1, node_id: 0, bsf:
        0000:1b:00.0, #accel: 5 #engines: 10 state: up
7 qat_dev2 - type: c6xx, inst_id: 2, node_id: 0, bsf:
        0000:1c:00.0, #accel: 5 #engines: 10 state: up
```

• すべての QAT エンドポイントで SRIOV (VF サポート) を有効にします。

```
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
```

- すべての VF が表示されていることを確認します(エンドポイントあたり 16 VF、合計 48 VF)。
- adf_ctl status コマンドを実行して、各 Intel QAT チップのすべての PF エンドポイント (最大 3 つ) と VF が稼働していることを確認します。この例では、システムには C62x チップが1つしかありません。 つまり、合計で 51 のエンドポイント (3+48 の VF) があります。

root@venkat-Super-Server:~#	adf_ctl star	tus				
Checking status of all devices.						
There is 47 GAT acceleration	n device(s) in	the system:				
gat dev8 - type: c6xx, ind	st id: 0. nod	e id: 0. bsf	: 6660:1a:60.0. #ac	cel: 5 Aengines: 10 state: up		
gat dev1 - type: c6xx, int	st id: 1. nod	e id: 8. bsf	: 6969:1b:86.0, #ac	cel: 5 #engines: 10 state: up		
gat dev2 - type: c6xx, inc	st id: 2. nod	e id: 0. bsf	: 6869:1c:80.0, fac	cel: 5 deorines: 10 state: un		
nat dev3 - type: c6xxvf.	inst id: 0. n	ode id: 0. b	sf: 0000:1a:01.0. 4	accel: 1 #engines: 1 state: up		
gat deu4 - tupe: c6xxuf.	inst id: 1. m	ode id: 0, h	sf: 0000:10:01.7. #	accel: 1 #engines: 1 state: un		
gat dau5 - tupe: c5xxuf.	inst id: 2, n	ode id: 0, b	sf: 0000:1a:01.1. #	accel: 1 tengines: 1 state: up		
nat deug = tune: c6xxuf.	inst id: 1. m	ode id: 0, b	sf: 0000:1a:02.0. 4	accel: 1 #engines: 1 state: up		
nat dev7 - tune: c6xxvf.	inst id: 4. m	ode id: 0. b	sf: 6000:10:01.2. 4	accel: 1 #engines: 1 state: un		
gat days - type: coxyuf.	inst id: 5. n	ode id: 0, b	sfr 6000:10:01.3. #	accel: 1 tengines: 1 state: up		
nat daug - tupe: c6xxvf.	inst id: 6, m	ode id: 0, b	sf: 0000:1a:02.1. #	accel: 1 #engines: 1 state: up		
nat daula - tuna: covuf	inst id- 7	node id: 0	hof: 0000:10:001 4	kaccal: 1 Kangines: 1 state: un		
ast deull - tune: covruf.	inst id: 8.	node id: 0,	hef: 0000110101.5.	taccel: 1 tengines: 1 state: un		
nat deul2 = tune: c5xxuf.	inst id: 9, 1	node id: 0, 1	hef: 0000:10:02.2.	taccel: 1 tengines: 1 state: up		
nat dauli = tuna: civeuf	inst id: 10	node id: 0	hef: 0000110-01 6	Harcal: 1 Hangines: 1 state: up		
nat devid - tune: coxvef	inst id: 11.	node id: 0.	hef: 0888:1a:02.3	Haccel: 1 Hengines: 1 state: up		
ast dauls - tuna: c5yvuf	inst id: 12	node id: 0	hef: 0000:1a:02.4	Faccal: 1 Fendines: 1 state: up		
mat daul6 = tuna: c5xxuf	inst_id: 12,	node_id: 0	bef: 0000:10:02.4;	Maccel: 1 Mengines: 1 state: up		
nat daul7 - tunat covvuf	inst id: 14.	node id: 0	hef: 0888:1a:02.5;	Harcel: 1 Hengines: 1 state: up		
ast douls - tuno: cfrout	inst_id: 15	node_id: 0,	hef: 0000:10:02.7	Faccal: 1 Fangines: 1 state: up		
ast dau19 - tuna: cSxxuf	inst_id: 15,	node_id: 0,	bef: 0000:1b-01 0	saccel: 1 sengines: 1 state: up		
ast double - type: coxver,	finst_fdt 17	node id: 0	bef: 0000:10:01.0;	Receil: 1 Rengines: 1 state: up		
ast doubl - tupor coxver,	fact id: 19	node_id: 0	bef: 0000:10:01.1	Faccel: 1 Fengines: 1 state: up		
qat_dev21 - type: coxxvf,	doct dd: 10	node_id: 0,	baf: 0000:10:01.2,	Faccal: 1 Fendines: 1 state: up		
gat_dev22 - type: coxxvf,	inst_id: 20	node_id: 0,	bef: 0000:10:01.3,	Maccel: 1 Mengines: 1 state: up		
gat_dev2a - type: coxxvr;	fact fd: 20,	node_id: 0	bef: 0000:10:01.4;	Faccel: 1 Fengines: 1 state: up		
dat_dav24 - type: coxvvr,	doct id: 22	node_id: 0,	bar: 0000:10:01.5,	Faccel: 1 Fengines: 1 state: up		
gat_dev25 - type: cokkvi,	inst_id: 22,	node_id: 0,	bef: 0000:10:01.0,	waccet: 1 wengines: 1 state: up		
gat_dev26 - type: coxxvr,	inst_10: 23,	node_id: 0,	bef: 0000:10:01.1,	Maccel: 1 Mengines: 1 state: up		
dat_dev2r - type: coxvvr,	inst_10: 24,	node_10: 0,	bar: 0000:10:02.0,	Faccel: 1 Fengines: 1 state: up		
qac_dev26 - type: coxxv1,	doct dd: 25,	node_id: 0,	baf: 0000:10:02.1,	faccal: 1 fondines: 1 state: up		
gat_dev10 - type: coxxvr,	inst_id: 20,	node_id: 0,	bof: 0000:10:02.2;	Maccel: 1 Mengines: 1 state: up		
est doubt - type: coxver,	foot fd: 20	node_fd; 0	bef: 0000:10:02.3;	Faccel: 1 Fengines: 1 state: up		
qat_dev31 - type: coxxvr,	doct dd: 20,	node_id: 0,	baf: 0000:10:02.4,	faccel: 1 fengines: 1 state: up		
qac_dev32 - type: coxxv1,	inst_id: 29,	mode_id: 0,	baf: 0000:10:02.5,	faccal: 1 forgines: 1 state: up		
gat_dev3a - type: coxxvr,	inst_id: 30,	node_10: 0,	bef: 0000:10:02.0;	Faccel: 1 Fengines: 1 state: up		
gat_dev34 - type: caxxvr,	fact id: 22	node_id: 0,	bar: 0000:10:02.1,	Faccel: 1 Fengines: 1 state: up		
qac_devis - cyper coxxvi,	doct dde 32,	node_id: 0,	baf: 0000.1c.01.5	faccel: 1 fengines: 1 state: up		
dat_dev46 - type: c6xxvr,	inst_10: 33,	nobe_10: 0,	bof: 0000:10:01.5,	Waccet: 1 Wengines: 1 state: up		
ast doud? - tupo: coxxvf,	inst_10: 34,	nose_10: 0,	bef: 0000:1c:01.7	Faccel: 1 Fengines: 1 state: up		
qac_dev42 - type: coxxvf,	doct dd: 35,	node_id: 0,	bar: 0000:10:01.r.	faccel: 1 fengines: 1 state: up		
dat_dev43 - type: c6kkvr,	inst_id: 30,	nobe_10: 0,	bsf: 0000.1c.02.0,	waccet: 1 vengines: 1 state: up		
gat_dev44 - type: coxxvf,	fact (d) 20	nose_10: 0,	bsf: 0000:10:02.2	Waccet: 1 Wengines: 1 state: up		
ast douds - type: caxevr,	inst_id: 30,	node_id: 0,	bat: 0000:1c:02.2,	Faccal: 1 Fendines: 1 state: up		
dat_dav45 - type: cskkvr,	inst_10: 39,	node_id: 0,	baf: 0000:10:02.3,	#accel: 1 #engines: 1 state: up		
gat_deud8 - type: c6xxvr,	inst_10: 48,	node_id: 0,	bef: 0000:10:02.4,	Maccel: 1 Mengines: 1 state: Up		
qat_dev4a - type: c6xxvf,	inst_10: 41,	node_10: 0,	bof: 0000:1c:02.5,	Faccel: 1 Pengines: 1 state: up		
gat_dev49 - type: c6xxvr,	dost id: 42,	node_id: 0,	bef: 0000:1c:02.6,	faccel: 1 Fengines: 1 state: up		
rootOvenkat_Super_Servertet	1115 C_101 43,	10000_101 0,	0511 000011C10211	vaccett i venginest i state: up		
roo cavelina c -auper -aerver;						

- 2. Linux ホストで SR-IOV を有効にしてください。
- 3. 仮想マシンを作成します。仮想マシンを作成するときは、パフォーマンス要件を満たす適切な数の PCI デバイ スを割り当てます。

注

各 C62x (QAT) チップには、最大 3 つの個別の PCI エンドポイントを設定できます。各エンドポイントは VF の論理的な集合であり、チップの他の PCI エンドポイントと帯域幅を均等に共有します。各エンドポイントに は、最大 16 個の PCI デバイスとして表示される VF を最大 16 個設定できます。これらのデバイスを VM に追 加して、QAT チップを使用して暗号アクセラレーションを行います。

注意事項

• 仮想マシンの暗号化要件が複数の QAT PCI エンドポイント/チップを使用することである場合は、対応する PCI デバイス/VF をラウンドロビン方式で選択して対称分散を行うことをお勧めします。 選択する PCI デバイスの数は、ライセンスされている vCPU の数と同じにすることをお勧めします (管理 vCPU 数は含まない)。利用可能な vCPU 数よりも多くの PCI デバイスを追加しても、必ずしもパフォーマン スが向上するわけではありません。

例

3 つのエンドポイントを備えた 1 つの Intel C62x チップを搭載した Linux ホストを考えてみましょう。6 個 の vCPU を搭載した VM をプロビジョニングする場合、各エンドポイントから 2 つの VF を選択し、それらを VM に割り当てます。この割り当てにより、仮想マシンの暗号ユニットを効果的かつ均等に分配できます。使 用可能な vCPU の合計のうち、デフォルトで 1 つの vCPU が管理プレーン用に予約され、残りの vCPU はデ ータプレーン PE で使用できます。

Linux KVM ハイパーバイザーにデプロイされた NetScaler VPX に QAT VF を割り当てる

- 1. Linux KVM Virtual Machine Manager で、仮想マシン (NetScaler VPX) の電源がオフになっていることを 確認します。
- 2. [ハードウェアの追加] > [PCI ホストデバイス] に移動します。
- 3. Intel QAT VF を PCI デバイスに割り当てます。



4. [完了] をクリックします。

5. 前述の手順を繰り返して、1 つ以上の Intel QAT VF を NetScaler VPX インスタンスに割り当てます。なぜな ら、1 つの vCPU が管理プロセス用に予約されているからです。

仮想マシンあたりの QAT 仮想マシンの数 = 仮想 CPU の数-1

- 6. Power on the VM.
- 7. NetScaler CLI でstat sslコマンドを実行して SSL サマリーを表示し、QAT VF を NetScaler VPX に割 り当てた後に SSL カードを確認します。

この例では、5 つの vCPU を使用しました。つまり、4 つのパケットエンジン (PE) です。

Press Control_L+Alt_L to re	lease pointer. vpx-kvm-14.1 on Q	QEMU/KVM 😑 🖲
File Virtual Machine View Send Key		
📃 🕜 🕨 🔟 💆 👻 🖻		
SSL Summary		
# SSL cards present	4	
# SSL cards UP	4	
SSL engine status	1	
SSL sessions (Rate)	Θ	
Crypto Utilization(%)		
Asymmetric Crypto Utilization	0.00	
Symmetric Crypto Utilization	0.00	
System		
Transactions	Rate (/s)	Total
SSL transactions	Θ	0
SSLv3 transactions	Θ	Θ

展開について

このデプロイメントは、次のコンポーネント仕様でテストされました:

- **NetScaler VPX** バージョンとビルド:14.1-8.50
- **Ubuntu** バージョン: 18.04、カーネル 5.4.0-146
- Linux 用インテル **C62x QAT** ドライバーのバージョン:L.4.21.0-00001

PCI パススルーネットワークインターフェイスを使用するように NetScaler VPX イン スタンスを構成する

October 17, 2024

Linux-KVM プラットフォームに NetScaler VPX インスタンスをインストールして構成したら、仮想マシンマネー ジャーを使用して、PCI パススルーネットワークインターフェイスを使用するように仮想アプライアンスを構成でき ます。

前提条件

- KVM ホスト上のインテル XL710 NIC (NIC) のファームウェア・バージョンは 5.04 です。
- KVM ホストは、IOMMU (Input-Output Memory Management Unit) と Intel VT をサポートし、これらは KVM ホストの BIOS で有効になっています。KVM ホストで IOMMU を有効にするには、/boot/-grub2/grub.cfg ファイルに次のエントリを追加します。
- 次のコマンドを実行して KVM ホストを再起動します。grub2-MKConfig -- o /boot/grub2/grub.cfg

仮想マシンマネージャーを使用して PCI パススルーネットワークインターフェイスを使用するように NetScaler ADC VPX インスタンスを構成するには:

- 1. NetScaler VPX インスタンスの電源を切ります。
- 2. NetScaler VPX インスタンスを選択し、[開く]をクリックします。



3. KVM> o virtual_machine ウィンドウで、i アイコンをクリックします。

MI			Demo_VPX on QEMU/KVM	+ _ = X
File	Virtual Machine View	Send Key		
	🕐 🕨 🖉 🔹	6		<mark>ه</mark> م
	Overview	Basic Details		
-A-	Performance	Name:	Demo_VPX	
	CPUs	UUID:	2f82dfa1-ae7d-46bf-b63f-833387798cf0	
	Memory	Status:	Shutoff (Destroyed)	
	Boot Options	Title:		
0	IDE Disk 1	Description:		
₽	NIC :7f:81:87			
	Mouse			
	Keyboard			
	Display VNC	Hypervisor D	etails	
	Sound: ich6	Hypervisor:	KVM	
2	Serial 1	Architecture:	x86_64	
2	Channel spice	Emulator:	/usr/bin/kvm-spice	
	Video QXL	Firmware:	BIOS	
	Controller USB	chipset:	1440FA	
	Controller PCI			
	Controller IDE		N	
	Controller VirtlO Serial		· · ·	
1	USB Redirector 1			
*	USB Redirector 2			
	-Add Hardware		Cancel	Apply

- 4. [ハードウェアの追加]をクリックします。
- 5. [新しい仮想ハードウェアの追加] ダイアログボックスで、次の操作を行います。
 - a. [**PCI** ホストデバイス] を選択します。
 - b. [ホストデバイス] セクションで、インテル XL710 物理機能を選択します。
 - **c.** [完了] をクリックします。

<i>a</i>				Demo_VPX on QEMU/KVM	↑ _ □ ×
File	Virtual	Mac	hine View Send K	ey	
	1	003		Add New Virtual Hardware	↑ ×
	Oven		Storage Controller	PCI Device	
	Perfo CPUs Memo	0	Input Graphics Sound	0000:00:1C:4 Intel Corporation C610/X99 series chipset PCI Expres 0000:00:1D:0 Intel Corporation C610/X99 series chipset USB Enhan 0000:00:1F:0 Intel Corporation C610/X99 series chipset LPC Contro	ss Root Por nced Host Iller
	Boot VirtIC Mous		Serial Parallel Console Channel	0000:00:1F:2 Intel Corporation C610/X99 series chipset 6-Port SAT/ 0000:00:1F:3 Intel Corporation C610/X99 series chipset SMBus Cor 0000:00:1F:6 Intel Corporation C610/X99 series chipset Thermal So 0000:01:00:0 Intel Corporation I350 Gigabit Network Connection (I	A Controlle htroller ubsystem nterface e
	Displ Seria Videc Contr		USB Host Device PCI Host Device Video Watchdog Filesystem Smartcard	0000:01:00:1 Intel Corporation I350 Gigabit Network Connection (I 0000:03:00:0 Intel Corporation Ethernet Controller XL710 for 40Gb 0000:05:00:0 Intel Corporation Ethernet Controller XL710 for 40Gb 0000:09:00:0 ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge 0000:0A:00:0 ASPEED Technology, Inc. ASPEED Graphics Family 0000:7F:08:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI	nterface e E QSFP+ (E QSFP+ (Link 0
	Contr		USB Redirection TPM RNG Panic Notifier	0000:7F:08:2 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI 0000:7F:08:3 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 QPI 0000:7F:0B:0 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 C 0000:7F:0B:1 Intel Corporation Xeon E7 v3/Xeon E5 v3/Core i7 R3 C	Link 0 Link 0 QPI Link 0 QPI Link 0
	Add H	ardw	are	Cancel	Finish

- 6. 手順4と5を繰り返して、インテル XL710 物理関数を追加します。
- 7. NetScaler VPX インスタンスをパワーオンします。
- 8. NetScaler VPX インスタンスの電源が入ったら、次のコマンドを使用して構成を確認できます。



出力には、設定したすべてのインターフェイスが表示されている必要があります。

	Press Control_L+Alt_L to release pointer. NetScaler-VPX on QEMU/KVM						
File	Virtual	Machine View	/ Send Key				
	8	⊳ 00	•	6		¢	
	> show interface summary						
		Interface	MTU	MAC	Suffix		
	1	0/1	1500	52:54:00:3f:57:7c	NetScaler Virtual Interface		
	2	10/1	1500	0c:c4:7a:8e:b8:2d	Intel XL710, SR, 10 Gbit		
	3	10/2	1500	0c:c4:7a:8e:b8:2e	Intel XL710, SR, 10 Gbit		
	4	40/1	1500	3c:fd:fe:9e:d8:d9	Intel XL710 40Gbit Interface		
	5	L0/1	1500	52:54:00:3f:57:7c	Netscaler Loopback interface		
	Done >						

virsh プログラムを使用して **NetScaler ADC VPX** インスタンスをプロビジョニング する

October 17, 2024

virshプログラムは VM ゲストを管理するためのコマンドラインツールです。その機能性は Virtual Machine Manager に似ています。これにより VM Guest の状態(開始、停止、一時停止など)を変更でき、新しい Guests およびデバイスをセットアップして、既存の構成を編集できます。virshプログラムは、VM ゲスト管理操作のスク リプト作成にも役立ちます。

virshプログラムを使用して NetScaler ADC VPX をプロビジョニングするには、次の手順に従います。

- tar コマンドを使用して、NetScaler VPX パッケージを解凍します。nsvpx-kvm-*_nc.tgz パッケージには、 次のコンポーネントが含まれています。
 - VPX 属性 [NSVPX-KVM-*_nc.xml] を指定するドメイン XML ファイル
 - NS-VM ディスクイメージ [Checksum.txt] のチェックサム
 - NS-VM Disk Image [NSVPX-KVM-*_nc.raw]

例

```
1 tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
```

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

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

```
4 checksum.txt
```

 NSVPX-KVM-*_nc.xml XMLファイルを\\<DomainName\\>-NSVPX-KVM-*_nc.xmlという名前のファイルにコピーします。<DomainName>は仮想マシンの名前でも あります。例

```
1 cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc
.xml
```

- 3. \\<DomainName\\>-NSVPX-KVM-*_nc.xmlファイルを編集して、次の パラメータを指定します。
 - name 名前を指定します。
 - Mac MAC アドレスを指定します。

```
注
ドメイン名と MAC アドレスは一意である必要があります。
```

 source file:ディスクイメージの絶対ソースパスを指定します。ファイルパスは絶対パスである必要が あります。RAW イメージファイルまたは QCOW2 イメージファイルのパスを指定することができます。

RAW イメージファイルを指定する場合は、次の例のようにディスクイメージソースパスを指定します。

例

```
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'/>
```

次の例に示すように、絶対 QCOW2 ディスクイメージソースパスを指定し、ドライバタイプを **qcow2** と定義します。

例

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

- 4. \\<DomainName\\>-NSVPX-KVM-*_nc.xmlファイルを編集して、ネットワークの詳細を構成します。
 - source dev インターフェースを指定します。
 - mode モードを指定します。デフォルトのインターフェイスは Macvtap ブリッジです。

例: モード:macvTap Bridge ターゲットインターフェイスをethxに設定し、モードをブリッジモデルタイ プvirtioに設定

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	

ここで、eth0 は仮想マシンに接続された物理インターフェイスです。

5. 次のコマンドを使用して、\\<DomainName\\>-NSVPX-KVM-*_nc.xmlフ ァイル内の VM 属性を定義します。

virsh define \<DomainName\>-NSVPX-KVM-*_nc.xml

例

virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml

6. 次のコマンドを入力して VM を起動します。

virsh start \[\<DomainName\> | \<DomainUUID\>\]

例

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

7. コンソール経由でゲスト VM を接続します。

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

例

1 virsh console NetScaler-VPX

virsh プログラムを使用して NetScaler ADC VPX インスタンスにインターフェイスを追加する

KVM 上で NetScaler VPX をプロビジョニングした後、追加のインターフェイスを付加できます。

インターフェイスを追加するには、次の手順を実行します。

- 1. KVM の上で動作している NetScaler VPX インスタンスをシャットダウンします。
- 次のコマンドを使用して、\\<DomainName\\>-NSVPX-KVM-*_nc.xmlフ ァイルを編集します。

virsh edit \[\<DomainName\> | \<DomainUUID\>\]

 3. \\<DomainName\\>-NSVPX-KVM-*_nc.xmlファイルに、次のパラメー タを追加します。

a) MacVTap 用

- Interface type インターフェイスの種類として「direct」を指定します。
- MAC アドレス: MAC アドレスを指定し、MAC アドレスがインターフェイス全体で一意であることを確認します。
- source dev インターフェイス名を指定します。
- mode-モードを指定します。サポートされているモードは、ブリッジ、VEPA、プライベート、パススルーです。
- モデルタイプ-モデルタイプを次のように指定します。virtio

例

モード: MacVTap Pass-through

ターゲットインターフェースを次のように設定します ethx、モードとして 橋梁、モデルタイプとして ヴィ ルティオ

ここで eth1 は仮想マシンに接続された物理インターフェイスです。

b) ブリッジモード用

注

KVM ホストに Linux ブリッジを設定し、物理インターフェイスをブリッジにバインドし、ブリッジを UP 状態にしていることを確認します。

- Interface type インターフェイスの種類として「bridge」を指定します。
- MAC アドレス: MAC アドレスを指定し、MAC アドレスがインターフェイス全体で一意であるこ とを確認します。
- source dev ブリッジ名を指定します。
- モデルタイプ-モデルタイプを次のように指定します。virtio

例: Bridge Mode

NetScaler VPX ゲスト仮想マシンの管理

October 17, 2024

仮想マシンマネージャと virshプログラムを使用して、仮想マシンゲストの起動または停止、新しいゲストとデバ イスの設定、既存構成の編集、仮想ネットワークコンピューティング (VNC) によるグラフィカルコンソールへの接続 などの管理タスクを実行できます。

仮想マシンマネージャーを使用して VPX ゲスト仮想マシンを管理する

• VM ゲストを一覧表示する

Virtual Machine Manager のメインウィンドウには、接続される各 VM ホストサーバのすべての VM Guests の一覧が表示されます。各仮想マシンゲストエントリには、仮想マシンの名前と、アイコンに表示されるステ ータス(実行中、一時停止、またはシャットオフ)が含まれます。

グラフィカルコンソールを開く

VM Guest に対してグラフィカルコンソールを開いて、VNC 接続介して物理的ホストと通信するようにマシ ンと相互通信できます。Virtual Machine Manager でグラフィカルコンソールを開くには、VM Guest エン トリーを右クリックして、ポップアップメニューで [オープン] オプションを選択します。

• ゲストの起動とシャットダウン

Virtual Machine Manager から VM Guest を開始または停止できます。VM の状態を変更するには、VM Guest エントリーを右クリックして、ポップアップメニューで [Run] または [Shut Down] オプションの いずれかを選択します。

V localhost.localdomain:6 (admin)			
Activities WWirtual Mac	chine Manager		Thu 03:07
			Virtual Machine Manager
File Edit View Help			
🔛 📃 Open 🗈 🛛 🛛	a ~		
Name			
✓ localhost (GEMU)			
NetScaler-VPX Running	Run		
	Pause		
	Shut Down 💙	Reboot	
	Clone	Shut Down	
	Migrate	Eorce Off	
	Delete	Sa <u>v</u> e	
	Open		
< l			,

• ゲストを再起動

Virtual Machine Manager から VM Guest を再起動できます。VM を再起動するには、VM Guest エントリ ーを右クリックして、ポップアップメニューで [Shut Down] > [Reboot] を選択します。

• ゲストを削除する

デフォルトでは、VM Guest を削除すると XML 構成が消去されます。また、ゲストのストレージファイルを 削除できます。これを実行して、完全にそうすることはゲストを消します。

- 1. Virtual Machine Manager で、VM Guest エントリーを右クリックします。
- 2. ポップアップメニューで [Delete from] を選択します。確認ウィンドウが開きます。

注

削除オプションは、VM ゲストがシャットダウンされている場合にのみ有効になります。

- 3. [削除] をクリックします。
- 完全にゲストを消去するには、[Delete Associated Storage Files] チェックボックスをオンにして、 関連付けられた.raw ファイルを削除します。

virsh プログラムを使用して NetScaler ADC VPX ゲスト仮想マシンを管理する

• VM ゲストとその現在の状態を一覧表示します。

ゲストに関する情報を表示するためにvirshを使用するには

virsh list --all

コマンド出力はすべてのドメインとその状態を表示します。出力例:

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	

• virshコンソールを開きます。

```
ゲスト仮想マシンをコンソールから接続します。
```

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

例

```
virsh console NetScaler-VPX
```

ゲストを起動してシャットダウンします。

```
Guest は DomainName または Domain-UUID を使って開始できます。
```

```
virsh start [<DomainName> | <DomainUUID>]
```

```
例
```

```
virsh start NetScaler-VPX
```

ゲストをシャットダウンするには:

virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]

例

```
virsh shutdown NetScaler-VPX
```

• ゲストを再起動

virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]

例

```
virsh reboot NetScaler-VPX
```

ゲストを削除する

ゲスト仮想マシンを削除するには、削除コマンドを実行する前に、ゲストをシャットダウンして-NSVPX-KVM <DomainName>- * _nc.xml を定義解除する必要があります。 virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]

例

```
    virsh shutdown NetScaler-VPX
    virsh undefine NetScaler-VPX
```

注

削除コマンドではディスク イメージ ファイルは削除されないため、手動で削除する必要があります。

OpenStack 上で **SR-IOV** を使用して **NetScaler VPX** インスタンスをプロビジョニ ングします

October 17, 2024

OpenStack で、シングルルート I/O 仮想化(Single-Root I/O Virtualization: SR-IOV)テクノロジを使用する 高パフォーマンスの NetScaler VPX インスタンスを展開できます。

OpenStack で、3 つの手順で、SR-IOV テクノロジを使用する NetScaler VPX インスタンスを展開できます。

- ホスト上で SR-IOV Virtual Functions (VF) を有効にします。
- VF を構成し、OpenStack で使用できるようにします。
- OpenStack で NetScaler VPX をプロビジョニングします。

前提条件

次のことを確認してください:

- インテル 82599 NIC (NIC) をホストに追加します。
- 最新の IXGBE ドライバーをダウンロードしてインストールします。
- ホスト上の IXGBEVF ドライバをブロックリストします。/etc/modprobe.d/blacklist.conf ファイルに次のエントリを追加します。ブロックリストixgbevf

注

ixgbeドライバーのバージョンは 5.0.4 以上でなければなりません。

ホストで SR-IOV VF を有効にする

SR-IOV VF を有効にするには、次のいずれかの手順を実行します。

- <number_of_VFs>3.8 より前のカーネルバージョンを使用している場合は、/etc/modprobe.d/ixgbe フ ァイルに次のエントリを追加し、ホストを再起動します。オプション ixgbe max_vfs=
- カーネル 3.8 以降のバージョンを使用している場合、以下のコマンドを使用して VF を作成します。

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

各項目の意味は次のとおりです:

- number_of_VFs は、作成する Virtual Function の数です。
- device_name はインターフェイス名です。

重要:

1

SR-IOV VF を作成する場合、MAC アドレスを VF に割り当てないようにしてください。

次に、作成している 4 つの VF の例を示します。

Terminal - root@ubuntu: /etc	+ - • ×
File Edit View Terminal Tabs Help	1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 -
root@ubuntu:/etc# echo 1 > /sys/class/net/ens3f0/device/sriov_numvfs	
root@ubuntu:/etc# echo 1 > /sys/class/net/ens3f1/device/sriov_numvfs	
root@ubuntu:/etc# lspci grep 82599	
02:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	
02:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	
02:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)	
02:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)	
root@ubuntu:/etc# &	

VF を永続的にし、VF の作成に使用したコマンドを **rc.local** ファイルに追加します。rc.local ファイルの内容を示 す例を次に示します。



詳細については、このインテル SR-IOV 構成ガイドを参照してください。

OpenStack で VF を設定して利用できるようにする

以下のリンクに記載されている手順に従って、OpenStack で SR-IOV を設定します: https://wiki.openstack.o rg/wiki/SR-IOV-Passthrough-For-Networking。

OpenStack で Citrix ADC VPX インスタンスをプロビジョニングする

OpenStack CLI を使用して、OpenStack 環境で Citrix ADC VPX インスタンスをプロビジョニングできます。

VPX インスタンスをプロビジョニングします。オプションで、コンフィグドライブのデータを使用します。「構成ドラ イブ」とは、インスタンスの起動時にアタッチされる特殊な構成ドライブを指します。この構成ドライブを使用して、 インスタンスのネットワーク設定を構成する前に、管理 IP アドレス、ネットワークマスク、デフォルトゲートウェイ などのネットワーク構成情報をインスタンスに渡すことができます。

OpenStack が VPX インスタンスをプロビジョニングする場合、まず OpenStack を示す特定の BIOS 文字列 (OpenStack ファウンデーション)を読み取ることによって、インスタンスが OpenStack 環境で起動しているこ とを検出します。Red Hat Linux ディストリビューションの場合、この文字列は/etc/nova/release に保存されま す。これは、KVM ハイパーバイザープラットフォームに基づくすべての OpenStack 実装で使用できる標準メカ ニズムです。ドライブには特定の OpenStack ラベルが必要です。構成ドライブが検出されると、インスタンスは nova boot コマンドで指定されたファイル名から次の情報を読み取ろうとします。以下の手順では、このファイル を「userdata.txt」と呼びます。

- 管理 IP アドレス
- ネットワークマスク
- デフォルトゲートウェイ

パラメーターが正しく読み取られると、それらの値が NetScaler スタックに適用されます。これにより、インスタン スをリモートから管理できるようになります。パラメーターが読み取られない場合、または構成ドライブが存在しな い場合は、インスタンスが以下のデフォルトの処理を実行します。

- DHCP から IP アドレス情報を取得する。
- DHCP から情報を取得できない場合は、デフォルトのネットワーク構成として 192.168.100.1/16 を使用する。

CLI を使用して OpenStack 上の NetScaler VPX インスタンスをプロビジョニングします

OpenStack 環境で VPX インスタンスをプロビジョニングするには、OpenStack の CLI を使用します。次に、 OpenStack で Citrix ADC VPX インスタンスをプロビジョニングする手順の概要を示します。

- 1. .tgz ファイルから.qcow2ファイルを抽出する
- 2. qcow2 イメージから OpenStack イメージを作成する
- 3. VPX インスタンスのプロビジョニング

OpenStack 環境で VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. 抽出します。次のコマンドを入力して、.tqzファイルからqcow2ファイルを抽出します。

2 tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz

¹ tar xvzf <TAR file>

```
3 NSVPX-KVM.xml
```

```
4 NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. 次のコマンドを入力して、手順1で抽出した・qcoz2ファイルを使用して OpenStack イメージをビルドします。

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

下図は、glance image-create コマンドの出力例です。

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

3. OpenStack イメージが作成されたら、NetScaler VPX インスタンスをプロビジョニングします。

nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true -userdata ./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-02086a6bdee2 NSVPX-10

前述のコマンドでは、userdata.txt は、VPX インスタンスの IP アドレス、ネットマスク、デフォルトゲ

ートウェイなどの詳細を含むファイルです。ユーザーデータファイルは、ユーザーカスタマイズ可能なフ ァイルです。NSVPX-KVM-12.0-26.2 は、プロビジョニングする仮想アプライアンスの名前です。—NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 は OpenStack VF です。

+ Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	I I I I I I I I I I I I I I I I I I I
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling I
OS-EXT-STS:vm_state	building I
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	I I I I I I I I I I I I I I I I I I I
accessIPv6	
adminPass	43EjPdM5shLz I
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	I I I I I I I I I I I I I I I I I I I
l id l	6b9f6968-aab9-463c-b619-d58c73db3187
l image l	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	8
name I	NSVPX-10
os-extended-volumes:volumes_attached	
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
luser_id	418524f7101b4f0389ecbb36da9916b5

次の図に、nova boot コマンドの出力例を示します。

次の図は、userdata.txt ファイルのサンプルです。タグ内の値は、ユーザーが設定可能な値で、IP アドレス、 ネットマスク、デフォルトゲートウェイなどの情報を保持します。

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
1
     <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
2
        11
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3
4
    oe:id=""
5
    xmlns="http://schemas.dmtf.org/ovf/environment/1">
6
    <PlatformSection>
7
     <Kind>NOVA</Kind>
    <Version>2013.1</Version>
8
9
    <Vendor>Openstack</Vendor>
    <Locale>en</Locale>
11
     </PlatformSection>
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
        />
     citrix.com 4
15
     <property oe:key="com.citrix.netscaler.orch_env"</pre>
16
```

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

サポートされているその他の構成:ホストからの SR-IOV VF 上の VLAN の作成と削除

SR-IOV VF 上の VLAN を作成するには、次のコマンドを入力します。

ip link show enp8s0f0 vf 6 vlan 10

前述のコマンドでは、「enp8s0f0」は物理機能の名前です。

例: vf6で作成された VLAN 10

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

SR-IOV VF 上の VLAN を削除するには、次のコマンドを入力します。

ip link show enp8s0f0 vf 6 vlan 0

例: VLAN 10、vf6から削除された

[root@localhost ~]# ip link show enp8s0f0	
4: enp8s0f0: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP mode DEFAULT qle</broadcast,multicast,up,lower_up>	n 1000
link/ether 00:1b:21:7b:d7:88 brd ff:ff:ff:ff:ff:ff	
vf 0 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off	
vf 1 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off	
vf 2 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off	
vf 3 MAC fa:16:3e:1e:0b:ee, spoof checking on, link-state auto, trust off	
vf 4 MAC fa:16:3e:0d:05:62, spoof checking on, link-state auto, trust off	
vf 5 MAC 50:46:00:79: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	
VI / MAC 00:00:00:00:00; spoor checking on, link-state auto, trust off	

これらの手順により、SRIOV テクノロジを使用する NetScaler VPX インスタンスを OpenStack 上で展開する方法 が完了します。

KVM 上の NetScaler VPX インスタンスが OVS DPDK ベースのホストインターフェ イスを使用するように構成する

October 17, 2024

KVM (Fedora と RHOS) で実行されている NetScaler VPX インスタンスを Open vSwitch (OVS) と Data Plane Development Kit (DPDK) を使用するように構成して、ネットワークパフォーマンスを向上させることができま す。このドキュメントでは、KVM ホスト上の OVS-DPDK によって公開されるvhost-user ポートで動作するよ うに NetScaler ADC VPX インスタンスを構成する方法について説明します。

OVS は、オープンソースの Apache 2.0 ライセンスでライセンスされている多層仮想スイッチです。DPDK は、高 速パケット処理のためのライブラリとドライバのセットです。

以下のバージョンの Fedora、RHOS、OVS、および DPDK は、NetScaler VPX インスタンスを設定するために認 定されています。

Fedora	RHOS
Fedora 25	RHOS 7.4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

前提条件

DPDK をインストールする前に、ホストに 1GB の巨大なページがあることを確認してください。

詳細については、この DPDK システム要件ドキュメントを参照してください。OVS DPDK ベースのホストインター フェイスを使用するように KVM で NetScaler ADC VPX インスタンスを構成するために必要な手順の概要は次のと おりです。

- DPDK をインストールします。
- OVS を構築し、インストールします。
- OVS ブリッジを作成します。
- OVS ブリッジに物理インターフェイスを接続します。
- OVS データパスにvhost-userポートを接続します。
- OVS-DPDK ベースのvhost-userポートで KVM-VPX をプロビジョニングします

DPDK のインストール

DPDK をインストールするには、この Open vSwitch with DPDK ドキュメントに記載されている指示に従ってく ださい。

OVS のビルドとインストール

OVS のダウンロードページから OVS をダウンロードします。次に、DPDK データパスを使用して OVS をビルドお よびインストールします。「Open vSwitch のインストール 」ドキュメントに記載されている手順に従います。 詳細については、「DPDK 入門ガイド for Linux」を参照してください。

OVS ブリッジの作成

必要に応じて、Fedora コマンドか RHOS コマンドを入力して、OVS ブリッジを作成します。

Fedora コマンド:

RHOS コマンド:

1 ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev

物理インターフェイスを OVS ブリッジに接続します

ポートを DPDK にバインドし、次の Fedora または RHOS コマンドを入力して OVS ブリッジにアタッチします。

Fedora コマンド:

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 コマンド:

オプションの一部として表示される dpdk-devargs は、それぞれの物理 NIC の PCI BDF を指定します。

OVS データパスに vhost-user ポートを接続する

OVS データパスにvhost-userポートを接続するには、次の Fedora または RHOS コマンドを入力します。

Fedora コマンド:

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

RHOS コマンド:

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

OVS-DPDK ベースの vhost-user ポートを持つ KVM-VPX のプロビジョニング

次の QEMU コマンドを使用して、CLI からのみ、OVS-DPDK ベースの vhost-user ポートを持つ Fedora KVM 上の VPX インスタンスをプロビジョニングできます。**Fedora** コマンド:

```
1
     qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \
2
3
     -object memory-backend-file, id=mem, size=4096M, mem-path=/dev/hugepages
         ,share=on -numa node,memdev=mem \
4
5
     -mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-
        disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-</pre>
         format> \
6
     -device ide-drive, bus=ide.0, unit=0, drive=drive-ide0-0-0, id=ide0-0-0,
7
        bootindex=1 \
8
9
     -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
     -device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
11
         bus=pci.0,addr=0x3 \
12
     -chardev socket, id=char0, path=</usr/local/var/run/openvswitch/vhost-
13
        user1> \
14
     -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
15
        virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
17
     -chardev socket, id=char1, path=</usr/local/var/run/openvswitch/vhost-
        user2> \
```

```
18
19 -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
    virtio-net
20
21 pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
22
23 --nographic
```

RHOS の場合は、次のサンプル XML ファイルを使用して、virshを使用して NetScaler ADC VPX インスタンス をプロビジョニングします。

1	<domain type="kvm"></domain>
2	<name>dpdk-vpx1</name>
4	
5 6	<uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
7	<memory unit="KiB">16777216</memory>
9	<currentmemory unit="KiB">16777216</currentmemory>
10	<memorybacking></memorybacking>
12	<hugepages></hugepages>
14 15	<page size="1048576" unit="KiB"></page>
16	
18 19 20	
20 21 22	<vcpu placement="static">6</vcpu>
23 24	<cputune></cputune>
25	<shares>4096</shares>
27	<vcpupin cpuset="0" vcpu="0"></vcpupin>
29	<vcpupin cpuset="2" vcpu="1"></vcpupin>
31 32	<vcpupin cpuset="4" vcpu="2"></vcpupin>
33 34	<vcpupin cpuset="6" vcpu="3"></vcpupin>
35 36	<emulatorpin cpuset="0,2,4,6"></emulatorpin>
37 38	
39 40	<numatune></numatune>
41 42	<memory mode="strict" nodeset="0"></memory>
43	
----------	---
44	<resource></resource>
46	
47	<partition>/machine</partition>
48 49	
50	
51	<os></os>
52	
53 54	<type arch="x86_64" machine="pc-i440fx-rhel7.0.0">hvm</type>
55	<pre><boot dev="hd"></boot></pre>
56	
57	
59	<features></features>
60	
61	<acpi></acpi>
62	(apic/)
64	<pre>xapic/></pre>
65	
66	
67 68	<pre><cpu check="tull" match="minimum" mode="custom"></cpu></pre>
69	<model fallback="allow">Haswell-noTSX</model>
70	
71	<vendor>Intel</vendor>
73	<topology cores="6" sockets="1" threads="1"></topology>
74	
75	<feature name="ss" policy="require"></feature>
76	<pre><feature name="ncid" policy="require"></feature></pre>
78	
79	<feature name="hypervisor" policy="require"></feature>
80 81	(feature policy=!require! name=!arat!/)
82	creature potrey-require name-arat //
83	<domain type="kvm"></domain>
84	
85 86	<name>apak=vpx1</name>
87	<uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88	
89	<memory unit="KiB">16777216</memory>
91	<currentmemory unit="KiB">16777216</currentmemory>
92	
93	<memorybacking></memorybacking>
94 95	<hugepages></hugepages>

<page size='1048576' unit='KiB'/> </hugepages> </memoryBacking> <vcpu placement='static'>6</vcpu> <cputune> <shares>4096</shares> <vcpupin vcpu='0' cpuset='0'/> <vcpupin vcpu='1' cpuset='2'/> <vcpupin vcpu='2' cpuset='4'/> <vcpupin vcpu='3' cpuset='6'/> <emulatorpin cpuset='0,2,4,6'/> </cputune> <numatune> <memory mode='strict' nodeset='0'/> </numatune> <resource> <partition>/machine</partition> </resource> <os> <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type> <boot dev='hd'/> </os> <features> <acpi/> <apic/> </features>

149	<cpu check="full" match="minimum" mode="custom"></cpu>
150	
151 152	<model fallback="allow">Haswell-noTSX</model>
153 154	<vendor>Intel</vendor>
155	<topology cores="6" sockets="1" threads="1"></topology>
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	(feature policy loguinal nemotives)
167	<pre>creature potrcy=require name='xsaveopt'/></pre>
169 170	<feature name="pdpe1gb" policy="require"></feature>
171	<numa></numa>
172	<cell cpus="0-5" id="0" memaccess="<br" memory="16777216" unit="KiB">'shared'/></cell>
174 175	
176	
178	<clock offset="utc"></clock>
180 181 182	<on_poweroff>destroy</on_poweroff>
183	<on_reboot>restart</on_reboot>
185	<on_crash>destroy</on_crash>
187	<devices></devices>
189	<emulator>/usr/libexec/qemu-kvm</emulator>
191	<disk device="disk" type="file"></disk>
192	<pre><driver cache="none" name="qemu" type="qcow2"></driver></pre>
194	<source file="/home/NSVPX-KVM-12.0-52.18_nc.qcow2"/>
196	<target bus="virtio" dev="vda"></target>
198 199	<address <br="" bus="0x00" domain="0x0000" slot="0x07" type="pci">function='0x0'/></address>

200	
201	
202	
203	<controller index="0" type="ide"></controller>
204	
205	<address <br="" bus="0x00" domain="0x0000" slot="0x01" type="pci">function='0x1'/></address>
206	
207	
208	
209	<controller index="0" model="piix3-uhci" type="usb"></controller>
210	
211	<address <br="" bus="0x00" domain="0x0000" slot="0x01" type="pci">function='0x2'/></address>
212	
213	
214	
215	<controller index="0" model="pci-root" type="pci"></controller>
216	
217	<pre><interface type="direct"></interface></pre>
218	
219	<mac address="52:54:00:bb:ac:05"></mac>
220	(accurate days lows 120-060), mades that deal ()
221	<source dev=".eubi238010." mode=".pridge./"/>
222	(model type=lyistic1/)
223	<pre><modet type="*vfrtfo//v</pre"></modet></pre>
225	<address <br="" bus="0x00" domain="0x0000" slot="0x03" type="pci">function='0x0'/></address>
226	
227	
228	
229	<interface type="vhostuser"></interface>
230	
231	<mac address="52:54:00:55:55:56"></mac>
232	
233	<source <br="" path="/var/run/openvswitch/vhost-user1" type="unix"/> mode='client'/>
234	
235	<model type="virtio"></model>
236	
237	<address <br="" bus="0x00" domain="0x0000" slot="0x04" type="pci">function='0x0'/></address>
238	
239	
240	
241	<interface type="vhostuser"></interface>
242	
243	<mac address="52:54:00:2a:32:64"></mac>
244	
245	<source <br="" path="/var/run/openvswitch/vhost-user2" type="unix"/> mode='client'/>
246	

247	<model type="virtio"></model>
248	
249	<address <br="" bus="0x00" domain="0x0000" slot="0x05" type="pci">function='0x0'/></address>
250	
251	
252	
253	<interface type="vhostuser"></interface>
254	
255	<mac address="52:54:00:2a:32:74"></mac>
250	Converse type=lupix1 path=1/var/rup/openvewitch/vheat_veer21
257	mode='client'/>
258	(model turner luistic 1/)
259	<model type="virtio"></model>
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	<pre>worke type='unix' path='/var/run/openvswitch/vhost-user4' mode='client'/></pre>
271	<pre>(model_type='virtio'/>)</pre>
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="ply"></console>
285	<pre><target nort="!0!/" type="!serial!"></target></pre>
286	Carget type- servat port- 0 //
287	
288	
289	<input bus="ps2" type="mouse"/>
290	
291	<input bus="ps2" type="keyboard"/>
292	
293	<pre><graphics autoport="yes" port="-1" type="vnc"></graphics></pre>
294	

295	<listen type="address"></listen>
296	
297	
298	
299	<video></video>
300	
301	<model heads="1" primary="yes" type="cirrus" vram="16384"></model>
302	
303	<address <br="" bus="0x00" domain="0x0000" slot="0x02" type="pci">function='0x0'/></address>
304	
305	
306	
307	<memballoon model="virtio"></memballoon>
308	
309	<address <br="" bus="0x00" domain="0x0000" slot="0x08" type="pci">function='0x0'/></address>
310	
311	
312	
313	
314	
315	

注意事項

XML ファイルでは、サンプルファイルに示されているように、hugepage サイズは 1GB である必要があります。

1	<memorybacking></memorybacking>
2	
3	<hugepages></hugepages>
4	
5	<page size="1048576" unit="KiB"></page>
6	
7	

また、サンプルファイルでは、vhost-user1 は ovs-br0 にバインドされたvhostユーザーポートです。

1	<interface type="vhostuser"></interface>
2	
3	<mac address="52:54:00:55:55:56"></mac>
4	
5	<source <br="" path="/var/run/openvswitch/vhost-user1" type="unix"/> mode='client'/>
6	
7	<model type="virtio"></model>
8	
9	<address <br="" bus="0x00" domain="0x0000" slot="0x04" type="pci">function='0x0'/></address>
10	
11	

NetScaler VPX インスタンスを起動するには、virsh コマンドの使用を開始します。

KVM ハイパーバイザーでの NetScaler ADC アプライアンスの初回起動時に

NetScaler ADC VPX の構成を適用する

October 17, 2024

NetScaler ADC アプライアンスの初回起動時に、KVM ハイパーバイザーに NetScaler ADC VPX 構成を適用でき ます。したがって、VPX インスタンスでのお客様のセットアップは、はるかに短時間で構成できます。

プリブート ユーザー データとその形式の詳細については、「クラウド内の NetScaler アプライアンスの最初の起動 時に NetScaler VPX 構成を適用する」を参照してください。

注

KVM Hypervisor でプレブートユーザーデータを使用してブートストラップするには、デフォルトのゲートウ ェイ設定を<NS-CONFIG>セクションに渡す必要があります。<NS-CONFIG>タグ の内容について詳しくは、次の「サンプル」<NS-CONFIG>セクションを参照してください。

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

KVM ハイパーバイザーでプリブートユーザーデータを提供する方法

KVM ハイパーバイザー上のプリブートユーザーデータは、CD-ROM デバイスを使用して接続された ISO ファイルを 介して提供できます。 CD-ROM ISO ファイルを使用したユーザーデータの提供

バーチャルマシンマネージャー (VMM) を使用すると、CDROM デバイスを使用して ISO イメージとしてバーチャル マシン (VM) にユーザーデータを挿入できます。KVM は、VM ホストサーバー上の物理ドライブに直接アクセスする か、ISO イメージにアクセスして VM ゲストの CD-ROM をサポートします。

CD-ROM ISO ファイルを使用してユーザーデータを指定するには、次の手順に従います。

- 1. プレブートユーザーデータコンテンツを含むファイル名userdataでファイルを作成します。
 - 注 ファイル名は厳密に userdataとして使用する必要があります。
- 2. Store the userdata file in a folder, and build an ISO image using the folder.

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

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

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

```
1
     root@ubuntu:~/sai/19oct# ls -lh
2
     total 4.0K
     -rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
3
4
    root@ubuntu:~/sai/19oct#
5
     root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
     I: -input-charset not specified, using utf-8 (detected in locale
6
         settings)
7
     Total translation table size: 0
     Total rockridge attributes bytes: 0
8
9
     Total directory bytes: 0
10
     Path table size(bytes): 10
11
     Max brk space used 0
     175 extents written (0 MB)
12
13
     root@ubuntu:~/sai/19oct#
14
     root@ubuntu:~/sai/19oct# ls -lh
15
     total 356K
     -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. 標準の展開プロセスを使用して NetScaler ADC VPX インスタンスをプロビジョニングし、仮想マシンを作成 します。But do not power on the VM automatically.
- 4. 仮想マシンマネージャーで CD-ROM デバイスを追加するには、次の手順に従います。
 - a) 仮想マシンマネージャで VM ゲストエントリをダブルクリックしてコンソールを開き、[表示] > [詳細] の順に選択して [詳細] ビューに切り替えます。
 - b) [ハードウェアの追加]>[ストレージ]>[デバイスの種類]>[CDROM デバイス]をクリックします。

- c) [管理] をクリックして正しい ISO ファイルを選択し、[完了] をクリックします。NetScaler VPX イン スタンスの「リソース」の下に新しい CDROM が作成されます。
- 5. Power on the VM.

AWS での NetScaler VPX

April 1, 2025

NetScaler VPX インスタンスは、Amazon Web Services (AWS) で起動できます。NetScaler VPX アプライアン スは、AWS マーケットプレイスで Amazon Machine Image (AMI) として利用できます。AWS 上の NetScaler VPX インスタンスを使用すると、AWS のクラウドコンピューティング機能を使用したり、NetScaler の負荷分散機 能とトラフィック管理機能をビジネスニーズに合わせて使用したりできます。VPX インスタンスは、物理 NetScaler アプライアンスのすべてのトラフィック管理機能をサポートし、スタンドアロンインスタンスまたは HA ペアとして 展開できます。VPX の機能の詳細については、VPX のデータシートを参照してください。

はじめに

VPX のデプロイを開始する前に、次の情報を理解しておく必要があります。

- AWS 用語
- AWS-VPX サポートマトリックス
- 制限事項と使用ガイドライン
- 前提条件
- AWS 上の NetScaler VPX インスタンスの仕組み

AWS で NetScaler ADC VPX インスタンスを展開する

AWS では、VPX インスタンスで次のデプロイタイプがサポートされています。

- Standalone
- 高可用性 (アクティブ-パッシブ)
 - 同一ゾーン内での高可用性
 - Elastic IP を使用した異なるゾーンでの高可用性
 - プライベート IP を使用して、異なるゾーン間で高可用性
- アクティブ-アクティブ GSLB
- ADM を使用した自動スケーリング (アクティブ-アクティブ)

ハイブリッド展開

- NetScaler を AWS アウトポストにデプロイ
- AWS の VMC に NetScaler をデプロイする

ライセンス

AWS 上の NetScaler VPX インスタンスにはライセンスが必要です。AWS 上で動作する NetScaler VPX インスタ ンスで使用できるライセンスオプションは、Bring Your Own License(BYOL) です。

自動化

- NetScaler ADM: スマートな導入
- GitHub CFT: AWS デプロイ用の NetScaler テンプレートとスクリプト
- GitHub Ansible: AWS デプロイ用の NetScaler テンプレートとスクリプト
- GitHub Terraform: AWS デプロイ用の NetScaler テンプレートとスクリプト
- AWS パターンライブラリ (PL): NetScaler VPX

ブログ

- NetScaler on AWS が顧客によるアプリケーションの安全な配信をどのように支援するか
- NetScaler と AWS によるハイブリッドクラウドでのアプリケーション配信
- Citrix は AWS ネットワーキングコンピテンシーパートナーです
- NetScaler: いつでもパブリッククラウドに対応
- NetScaler を使用してパブリッククラウドで簡単にスケールアウトまたはスケールインできます
- Citrix、AWS Outposts で ADC のデプロイメントの選択肢を拡大
- NetScaler と Amazon VPC イングレスルーティングの使用
- Citrix は、AWS での選択肢、パフォーマンス、シンプルなデプロイメントを提供します
- NetScaler Web App Firewall のセキュリティー現在 AWS Marketplace で公開中
- Aria Systems が AWS で NetScaler Web App Firewall を使用する方法

ビデオ

- ADM によるパブリッククラウドの NetScaler 導入の簡素化
- すぐに使用できるテラフォームスクリプトを使用して AWS で NetScaler VPX を Provisioning および構成 する
- クラウドフォーメーションテンプレートを使用して NetScaler HA を AWS にデプロイ
- AWS クイックスタートを使用してアベイラビリティーゾーン全体に NetScaler HA
- ADM を使用した NetScaler オートスケール

お客様のケーススタディ

- テクノロジーソリューション-Xenit AB
- NetScaler と AWS の優位性をご覧ください

解決方法

- NetScaler を使用して AWS にデジタル広告プラットフォームをデプロイする
- NetScaler による AWS でのクリックストリーム分析の強化

サポート

- サポートケースを開く
- NetScaler サブスクリプションオファリングについては、「AWS 上の VPX インスタンスのトラブルシューティング」を参照してください。サポートケースを提出するには、AWS アカウント番号とサポート PIN コードを見つけて、NetScaler サポートに連絡してください。
- NetScaler カスタマーライセンスサービスまたは BYOL の場合は、有効なサポートおよびメンテナンス契約 を結んでいることを確認してください。契約を結んでいない場合は、NetScaler の担当者にお問い合わせくだ さい。

その他の参考資料

- AWS オンデマンドウェビナー-AWS 上の NetScaler
- NetScaler VPX データシート
- AWS Marketplace O NetScaler
- NetScaler は、AWS ネットワーキングパートナーソリューション(ロードバランサー)の一部です。
- AWS に関するよくある質問

AWS 用語

October 17, 2024

このセクションでは、よく使用される AWS の用語と語句のリストについて説明します。詳細については、「AWS 用語集」を参照してください。

用語	定義
Amazon マシンイメージ(AMI)	マシンイメージ。クラウド内の仮想サーバーであるイン
Elastic Block Store	AWS クラウドで Amazon EC2 インスタンスと一緒に 使用される、永続ブロックストレージボリュームを提供
Simple Storage Service (S3)	します。 Internet 用のストレージ。Web 規模のコンピューティ
	ングを開発者が簡単に実施できるように設計されていま す。
Elastic Compute Cloud (EC2)	クラウドで、安全でサイズ変更できる処理能力を提供す る Web サービスです。Web 規模のクラウドコンピュー ティングを開発者が簡単に実施できるように設計されて います。
Elastic Load Balancing (ELB)	複数のアベイラビリティゾーンで、複数の EC2 インスタ ンスにまたがる受信アプリケーショントラフィックを分 散します。これによってアプリケーションのフォールト トレランスが増加します。
エラスティックネットワークインターフェイス (ENI)	仮想プライベートクラウド(VPC)内のインスタンスに アタッチできる仮想ネットワークインターフェイス。
Elastic IP(EIP)アドレス	Amazon EC2 または Amazon VPC で割り当てられ、 インスタンスにアタッチされた、静的パブリック IPv4 アドレスです。Elastic IP アドレスは特定のインスタン スではなく、お使いのアカウントに関連しています。ニ ーズの変化に応じて、割り当て、アタッチ、デタッチ、 および解放が簡単にできるため、Elastic(融通が利く) と呼ばれています。
インスタンスの種類	Amazon EC2 では、さまざまなユースケースに対応で きるよう最適化された幅広い種類のインスタンスを提供 してます。インスタンスタイプを構成する CPU、メモ リ、ストレージ、およびネットワーク機能の組み合わせ はさまざまで、アプリケーションに合わせて最適なリソ ースの組み合わせを柔軟に選択できます。

用語	定義
Identity and Access Management (IAM)	AWS で ID が実行できること、または実行できないこと
	を決定する許可ポリシーを持つ AWS の ID。IAM ロール
	を使うことで EC2 インスタンス上で実行されるアプリケ
	ーションが、AWS リソースに安全にアクセスできるよう
	になります。高可用性セットアップで VPX インスタンス
	を展開する場合、IAM ロールは必須です。
インターネットゲートウェイ	ネットワークをインターネットに接続します。VPC 外部
	の IP アドレスのトラフィックをインターネットゲート
	ウェイにルーティングできます。
キーペア	身元を電子的に証明するために使用する一連の資格情報。
	キーペアはプライベートキーとパブリックキーで構成さ
	れます。
ルートテーブル	関連付けられているサブネットからのトラフィックを制
	御するための一連のルーティング規則。1 つのルートテ
	ーブルに対して複数のサブネットを関連付けることがで
	きますが、各サブネットは一度に1つのルートテーブル
	にしか関連付けることができません。
セキュリティグループ	あるインスタンスに対して許可されている、名前が付け
	られた一連の受信方向のネットワーク接続。
サブネット	EC2 インスタンスをアタッチできる VPC の IP アドレス
	範囲の一部分。セキュリティと運用上の必要に応じて、
	サブネットを作成し、インスタンスをグループ分けでき
	ます。
Virtual Private Cloud (VPC)	定義した仮想ネットワーク内で AWS リソースを起動で
	きる、AWS クラウドの論理的に隔離されたセクションを
	プロビジョニングする Web サービス。
Auto Scaling	ユーザー定義のポリシー、スケジュール、ヘルスチェッ
	クに基づいて Amazon EC2 インスタンスを自動的に起
	動または終了するウェブサービス。
クラウドの形成	関連する AWS リソースを 1 つの単位として一緒に作成
	および削除するテンプレートを書き込んだり変更したり
	するサービス。

AWS-VPX サポートマトリックス

January 15, 2025

次の表に、サポートされている VPX オファリング、AWS リージョン、インスタンスタイプ、およびサービスを示し ます。

表 1:AWS でサポートされている VPX オファリング

サポートされている VPX オファリング

NetScaler VPX - 顧客ライセンス

NetScaler VPX FIPS - 顧客ライセンス

NetScaler VPX FIPS ENA - 顧客ライセンス

表 2: サポートされている AWS リージョン

サポートされている AWS リージョン

米国西部 (オレゴン)

米国東部 (バージニア北部)米国西部 (北カリフォルニア)

米国東部 (オハイオ)

米国東部 (北アメリカ) バージニア州

アジアパシフィック(ムンバイ)

アジアパシフィック (メルボルン)

アジアパシフィック (ソウル)

アジアパシフィック (シンガポール)

アジアパシフィック (シドニー)

アジアパシフィック (東京)

アジアパシフィック (香港)

アジアパシフィック (大阪)

アジアパシフィック (ジャカルタ)

アジアパシフィック (ハイデラバード)

カナダ (中部)

```
サポートされている AWS リージョン
```

```
EU (フランクフルト)
欧州 (アイルランド)
欧州 (ロンドン)
欧州 (パリ)
欧州 (ミラノ)
南米 (サンパウロ)
AWS GovCloud (米国東部)
AWS GovCloud (米国西部)
AWS トップシークレット (C2S)
中東 (バーレーン)
中東 (UAE)
アフリカ (ケープタウン)
C2S
```

表 3: サポートされている AWS インスタンスタイプ

サポートされる AWS インスタンスタイプ

c4.large、c4.xlarge、c4.2xlarge、c4.4xlarge、c4.8xlarge

c5.large、c5.xlarge、c5.2xlarge、c5.4xlarge、c5.9xlarge、c5.18xlarge、c5.24xlarge

c5n.large、c5n.xlarge、c5n.2xlarge、c5n.4xlarge、c5n.9xlarge、c5n.18xlarge

c6in. ラージ、c6in. 特大、c6in.2 特大、c6in.4 特大、c6in.8 特大、c6in.12 特大、c6in.16 特大、c6in.24 特大、 c6in.32 特大

奥行 2.XL サイズ、D2.2xL サイズ、D2.4xL サイズ、D2.8xL サイズ

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

サポートされる AWS インスタンスタイプ

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

表 4: サポートされる AWS サービス

サポートされている AWS サービス

EC2: ADC インスタンスを起動します。

ラムダ: CFT からの NetScaler VPX インスタンスのプロビジョニング中に、NetScaler VPX NITRO API を呼び出します。

VPC と VPC イングレスルーティング: VPC は、ADC を起動できる分離されたネットワークを作成します。VPC 入力ルーティング

Route53: NetScaler Autoscale e ソリューション内のすべての NetScaler VPX ノードにトラフィックを分散します。

ELB: NetScaler Autoscale e ソリューション内のすべての NetScaler VPX ノードにトラフィックを分散します。

Cloudwatch: NetScaler VPX インスタンスのパフォーマンスとシステムパラメーターを監視します。

AWS Autoscaling: バックエンドサーバーの自動スケーリングに使用されます。

クラウドの形成: CloudFormation テンプレートは、NetScaler VPX インスタンスをデプロイするために使用されます。

Simple Queue Service (SQS): バックエンド自動スケーリングでスケールアップおよびスケールダウンイベントを監視します。

簡易通知サービス (SNS): バックエンド自動スケーリングでスケールアップおよびスケールダウンイベントを監視します。

ID とアクセス管理 (IAM): AWS のサービスとリソースへのアクセスを提供します。

AWS Outposts: AWS Outposts で NetScaler VPX インスタンスをプロビジョニングします。

NetScaler では、以下の AWS インスタンスタイプを推奨しています:

• マーケットプレイスエディションまたは帯域幅ベースのプールライセンス用の M5 および C5n シリーズ。

• vCPU ベースのプールライセンス用の C5n シリーズ

プールまたはフレックスライセンスの VPX(帯域幅ライ センス) 推奨される AWS インスタンス

最大 200 Mbps

m5.x ラージ

プールまたはフレックスライセンスの VPX(帯域幅ライ	
センス)	推奨される AWS インスタンス
1-5 Gbps	m5.2x ラージ
5-8 Gbps	c5n.4x ラージ
8-25 Gbps	c5n.9x ラージ

1 秒あたりのパケット数、SSL トランザクションレートなどのさまざまなメトリックに基づいてインスタンスを決定 するには、NetScaler の担当者に連絡してガイダンスを受けてください。vCPU ベースのプールライセンスとサイジ ングのガイダンスについては、NetScaler サポートにお問い合わせください。

制限事項と使用ガイドライン

October 17, 2024

NetScaler VPX インスタンスを AWS にデプロイする際には、以下の制限事項と使用上のガイドラインが適用されます。

- 始める前に、「AWS に NetScaler VPX インスタンスをデプロイする」の AWS 用語のセクションをお読みく ださい。
- クラスタリング機能は、VPX ではサポートされていません。
- 高可用性セットアップを効果的に機能させるには、専用のNATデバイスを管理インターフェイスに関連付けるか、EIPをNSIPに関連付けます。NATについて詳しくは、AWSドキュメントの「NAT Instances」を参照してください。
- データトラフィックおよび管理トラフィックは、異なるサブネットに属する ENI で分離する必要があります。
- 管理 ENI には NSIP アドレスのみが必要です。
- セキュリティ上の理由により、EIPを NSIP に関連付ける代わりに NAT インスタンスを使用する場合は、VPC レベルでルーティングを適切に変更する必要があります。VPC レベルのルーティングの変更手順については、 AWS ドキュメントの「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC」を参照して ください。
- VPX インスタンスは、ある EC2 インスタンスタイプから別のインスタンスタイプへ(たとえば、m3.large から m3.xlarge へ)移動できます。
- AWS 上の VPX のストレージオプションについては、EBS は耐久性があり、インスタンスからデタッチした後 でもデータが利用可能になるため、EBS をお勧めします。

- VPX への ENI の動的追加はサポートされていません。VPX インスタンスを再起動して更新を適用します。ス タンドアロンインスタンスまたは HA インスタンスを停止し、新しい ENI を接続してからインスタンスを再起 動することをお勧めします。
- 1つの ENI に複数の IP アドレスを割り当てることができます。ENI あたりの IP アドレスの最大数は EC2 イ ンスタンスタイプによって決まります。Elastic Network Interfacesの「インスタンスタイプごとのネット ワークインターフェイスごとの IP アドレス」のセクションを参照してください。IP アドレスを ENI に割り当 てる前に、AWS で割り当てる必要があります。詳細については、「Elastic ネットワークインターフェイス」を 参照してください。
- NetScaler VPX インターフェイスでは、インターフェイスの有効化および無効化コマンドは使用しないこと をお勧めします。
- NetScalerset ha node \\<NODE_ID\\> -haStatus STAYPRIMARY とset ha node \\<NODE_ID\\> -haStatus STAYSECONDARY コ マンドはデフォルトで無効になっています。
- IPv6 は VPX ではサポートされていません。
- AWS の制限により、次の機能はサポートされていません。
 - GARP (Gratuitous ARP)
 - L2 モード
 - タグ付き VLAN
 - 動的ルーティング
 - 仮想 MAC
- RNAT が機能するには、送信元/送信先チェックが無効になっていることを確認してください。詳細について は、Elastic Network Interfacesの「ソース/デスティネーションチェックの変更」を参照してください。
- AWS での NetScaler VPX デプロイメントでは、一部の AWS リージョンで AWS インフラストラクチャが AWS API 呼び出しを解決できない場合があります。これは、API 呼び出しが NetScaler VPX インスタンス の非管理インターフェイスを介して発行された場合に発生します。回避策として、API 呼び出しを管理インタ ーフェイスにのみ制限してください。回避策として、API 呼び出しを管理インターフェースのみに制限しま す。これを行うには、VPX インスタンス上に NSVLAN を作成し、適切なコマンドを使用して管理インター フェイスを NSVLAN にバインドします。例えば: ns config -nsvlan を設定します <vlan id> -ifnum 1/1 -tagged NO 設定を保存 プロンプトで VPX インスタンスを再起動しま す。nsvlanの設定の詳細については、NSVLAN の設定を参照してください。
- AWS コンソールでは、実際の使用量がはるかに低い場合でも、監視タブに表示される VPX インスタンスの vCPU 使用率が高い場合があります(最大 100%)。実際の vCPU 使用率を確認するには、「すべての CloudWatch メトリックスを表示」に移動します。詳細については、「Amazon CloudWatch を使用してインスタンスを監視する」を参照してください。
- ホットアドは、AWS 上の NetScaler を使用する PV および SRIOV インターフェイスでのみサポートされます。ENA インターフェイスを持つ VPX インスタンスはホットプラグをサポートしていないため、ホットプラ

グを試みるとインスタンスの動作が予測できない場合があります。

 AWS ウェブコンソールまたは AWS CLI インターフェイスを介したホット削除は、NetScaler の PV、SRIOV、 および ENA インターフェイスではサポートされていません。ホット削除を試みると、インスタンスの動作が 予測できなくなる可能性があります。

前提条件

October 17, 2024

AWS で VPX インスタンスを作成する前に、次のものがあることを確認してください。

- **AWS** アカウント:AWS 仮想プライベートクラウド (VPC) で NetScaler VPX AMI を起動します。AWS アカ ウントは www.aws.amazon.comで無料で作成できます。
- AWS ID およびアクセス管理(IAM) ユーザーアカウント: ユーザーの AWS サービスおよびリソースへのア クセスを安全にコントロールします。IAM ユーザーアカウントの作成方法の詳細については、「IAM ユーザー の作成 (コンソール)」を参照してください。IAM ロールは、スタンドアロンデプロイと高可用性デプロイの両 方で必須です。

AWS アカウントに関連付けられた IAM ロールには、さまざまなシナリオで次の IAM アクセス権限が必要です。

同じ AWS ゾーン内の IPv4 アドレスと HA ペア:

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

同じ AWS ゾーン内の IPv6 アドレスと HA ペア:

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

同じ AWS ゾーン内の IPv4 と IPv6 の両方のアドレスとの HA ペア:

"ec2:DescribeInstances",
 "ec2:AssignPrivateIpAddresses",
 "ec2:AssignIpv6Addresses",
 "ec2:UnassignIpv6Addresses",

5 "iam:SimulatePrincipalPolicy",

```
6 "iam:GetRole",
7 "ec2:CreateTags"
```

異なる AWS ゾーンにまたがる Elastic IP アドレスを持つ HA

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

異なる AWS ゾーンのプライベート IP アドレスを持つ HA ペア:

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

異なる AWS ゾーンのプライベート IP アドレスと Elastic IP アドレスの両方を持つ HA ペア:

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

AWS バックエンドの自動スケーリング:

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

14 "ec2:CreateTags"

注

- 前述の機能を組み合わせて使用する場合は、各機能に IAM アクセス権限を組み合わせて使用します。
- Citrix CloudFormation テンプレートを使用すると、IAM ロールが自動的に作成されます。この テンプレートでは、作成済みの IAM ロールを選択することはできません。
- GUI から VPX インスタンスにログオンすると、IAM ロールに必要な権限を設定するよう求めるプロンプトが表示されます。権限をすでに構成している場合は、このプロンプトを無視してください。
- AWS CLI: ターミナルプログラムから AWS マネジメントコンソールが提供するすべての機能を使用する。詳細については、AWS CLI ユーザーガイドを参照してください。また、ネットワークインターフェイスの種類を SR-IOV に変更するには、AWS CLI も必要です。
- Elastic Network Adapter (ENA): M5、C5 インスタンスなどの ENA ドライバー対応インスタンスタイプ の場合、ファームウェアバージョンは 13.0 以降である必要があります。
- NetScaler VPX の EC2 インスタンスでインスタンスメタデータサービス (IMDS) を構成する必要があります。IMDSv1 と IMDSv2 は、実行中の AWS EC2 インスタンスからインスタンスメタデータにアクセスするための 2 つのモードです。IMDSv2 は IMDSv1 よりも安全です。インスタンスを両方の方法(デフォルトオプション)を使用するように構成することも、IMDSv2 モードのみを使用するように構成することもできます(IMDSv1 を無効にする)。Citrix ADC VPX は、NetScaler VPX リリース 13.1.48.x 以降の IMDSv2 専用モードをサポートしています。

NetScaler VPX インスタンスで AWS IAM ロールを設定します

April 9, 2025

Amazon EC2 インスタンスで実行されるアプリケーションには、AWS API リクエストに AWS 認証情報を含める必要があります。AWS 認証情報を Amazon EC2 インスタンス内に直接保存し、そのインスタンス内のアプリケーションがそれらの認証情報を使用できるようにすることができます。ただし、認証情報を管理し、認証情報が各インスタンスに安全に渡されるようにし、認証情報をローテーションするときに各 Amazon EC2 インスタンスを更新する必要があります。それは多くの追加作業です。

代わりに、Amazon EC2 インスタンスで実行されるアプリケーションの一時的な認証情報を管理するには、ID とア クセス管理 (IAM) ロールを使用することができ、また使用する必要があります。ロールを使用すると、長期にわたる 認証情報 (ユーザー名、パスワード、アクセスキーなど) を Amazon EC2 インスタンスに配布する必要はありません。 代わりに、ロールはアプリケーションが他の AWS リソースを呼び出すときに使用できる一時的なアクセス権限を提 供します。Amazon EC2 インスタンスを起動するときに、インスタンスに関連付ける IAM ロールを指定します。イ ンスタンスで実行されるアプリケーションは、ロールが提供した一時的な認証情報を使用して API リクエストに署名 できます。 AWS アカウントに関連付けられた IAM ロールには、さまざまなシナリオで次の IAM アクセス権限が必要です。

同じ AWS ゾーン内の IPv4 アドレスと HA ペア:

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

同じ AWS ゾーン内の IPv6 アドレスと HA ペア:

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

同じ AWS ゾーン内の IPv4 と IPv6 の両方のアドレスとの HA ペア:

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

異なる AWS ゾーンにまたがる Elastic IP アドレスを持つ HA:

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

異なる AWS ゾーンのプライベート IP アドレスを持つ HA ペア:

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

異なる AWS ゾーンのプライベート IP アドレスと Elastic IP アドレスの両方を持つ HA ペア:

```
    "ec2:DescribeInstances",
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
```

```
7 "ec2:CreateRoute",
```

- 8 "ec2:ModifyNetworkInterfaceAttribute",
- 9 "iam:SimulatePrincipalPolicy",
- 10 "iam:GetRole"

AWS バックエンドの自動スケーリング:

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

注意事項:

- 前述の機能を組み合わせて使用する場合は、各機能に IAM アクセス権限を組み合わせて使用します。
- Citrix CloudFormation テンプレートを使用すると、IAM ロールが自動的に作成されます。このテンプレートでは、作成済みの IAM ロールを選択することはできません。
- GUI から VPX インスタンスにログオンすると、IAM ロールに必要な権限を設定するよう求めるプロンプトが 表示されます。権限をすでに構成している場合は、このプロンプトを無視してください。
- IAM ロールは、スタンドアロンデプロイと高可用性デプロイの両方で必須です。

IAM 役割を作成する

この手順では、AWS バックエンド自動スケーリング機能の IAM ロールを作成する方法について説明します。

注

同じ手順に従って、他の機能に対応する任意の IAM ロールを作成できます。

- 1. EC2 用 AWS マネジメントコンソールにログインします。
- 2. EC2 インスタンスページに移動し、ADC インスタンスを選択します。

New EC2 Experience Tell us what you think	Instances (1) Info
EC2 Dashboard	Q. Find instance by attribute or tog (case-sensitive) < 1 > ③
EC2 Global View	manne - i manne - i manne sance - janas enece - janas enece - janas enece - naminatura - remanny con
Events	auc POCC3DU/CUS3D3021 C Rumming QQ IIISJairge C 2/2 Circus passer into atamins T Usease-1a
Tags	
Limits	
▼ Instances	
Instances New	
Instance Types	
Launch Templates	
Spot Requests	=
Savings Plans	Select an instance 💿 🗙
Reserved Instances New	
Dedicated Hosts	
Scheduled Instances	
Capacity Reservations	
▼ Images	
AMIS New	
AMI Catalog	
Elastic Block Store	
Volumes	

3. [アクション]>[セキュリティ]>[IAM ロールの変更]に移動します。

New EC2 Experience ×	Instances (1/1) Info	C Connect	Instance state	Actions 🔺 Launch ins	tances 🔹 🔻
rea us what you think	Q. Find instance by attribute or tag (case-sensitive)			Connect	1 > ©
EC2 Dashboard	Name V Instance ID	Linctance state		View details	ailability Zone
EC2 Global View	Name V Instance ID	Instance state V Insta	ince type V Statu	Manage instance state	allability Zone
Events	adc i-0cc53b7cdd39f962	21 ⊘ Running @Q m5.x	large 🕑 2/	2 che Instance settings	-east-1a
Tags				Networking	
Limits			C	Networking P	
			Change security group	security	·
Instances			Get Windows passwor	rd Image and templates	•
Instances New			Modify IAM role	Monitor and troubleshoot	•
Instance Types					
Launch Templates					
Spot Requests		=			
Savings Plans	Instance: i-0cc53b7cdd39f9621 (adc)				⊚ ×
Reserved Instances New	Details Security Networking Storage	Status shocks Monitoring	Tage		
Dedicated Hosts	Details Security Networking Storage	Status checks Monitoring	rags		
Scheduled Instances	▼ Instance summary Info				
Capacity Reservations	Instance ID	Public IPv4 address	Pri	ivate IPv4 addresses	
	i-0cc53b7cdd39f9621 (adc)	D 52.3.230.117 open address 🗹	6	10.10.1.160	
 Images 	IPv6 address	Instance state	Pu	blic IPv4 DNS	
AMIS New	-	⊘ Running	-		
AMI Catalog	Hostname type	Private IP DNS name (IPv4 only)			
Elastic Block Store	IP name: ip-10-10-1-160.ec2.internal	ip-10-10-1-160.ec2.internal			
Volumes	Answer private resource DNS name	Instance type	Ela	astic IP addresses	

- 4. IAM ロールの変更ページでは、既存の IAM ロールを選択するか、IAM ロールを作成できます。
- 5. IAM ロールを作成するには、次の手順に従います。
 - a)「IAM ロールの変更」ページで、「新しい IAM ロールを作成」をクリックします。

Attach an IAM role to your instance.		
Instance ID		
D i-0cc53b7cdd39f9621 (adc)		
IAM role Select an IAM role to attach to your instance or create a new role if currently attached to your instance	you haven't created any. The role you select replaces any roles that are	
Choose IAM role	C Create new IAM role	
sure you want to remove from the selected instance	er	
	Cancel Update IAM role	

b)「ロール」ページで、「ロールを作成」をクリックします。

Roles (35) Info		0	Delete	Create role
An IAM role is an identity you can creat	e that has specific permissions with credentials that an	valid for	Delete	Creating role
hort durations. Roles can be assumed	by entities that you trust.			

c) [信頼できるエンティティタイプ]で[AWS service]を選択し、[一般的な使用例]で[EC2]を選択し、[次へ]をクリックします。

Trusted entity type			
AWS service Alter AWS services like EC2, Landes, or others to perform actions in this account.	AINS account Above entities in other AINS account belonging to you or a Brd party to perform actions in this account.	 Web identity Allows users todesteed by the specified external web identify provider to assume them sins to perform actions in this account. 	
SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	Custom trust policy Create a custom trust policy to enable others to perform actions in this account.		
Use case Allow an AIN'S service like EC2, Lambda, or o	thers to perform actions in this account.		
Common use cases			
EC2 Allows EC2 instances to call AIMS service	is on your behalf.		
 Lambda Alows Lambda functions to call AWS sat 	vices on your behalf.		
Use cases for other AWS services:			
Channes a secolar in view one seco		*	

d)「権限の追加」ページで、「ポリシーの作成」をクリックします。

dd permissions											
Permissions policies (755) Choose one or more policies to attach to your new role.							C	С	reate	olicy	C.
Q Filter policies by property or policy name and press enter	<	1	2	3	4	5	6	7	38	>	0

e) **JSON** タブをクリックして JSON エディターを開きます。

policy defines the AWS permissions the	hat you can assign to a user, group, or role	e. You can create and edit a policy in the	visual editor and using JSON. Learn more	
Visual editor JSON				Import managed policy
1* {				
2 "Version": "2012- 3 "Statement": □	-10-17",			
4 }				

f) JSON エディターで、すべてを削除し、使用したい機能の IAM 権限を貼り付けます。

たとえば、AWS バックエンド自動スケーリング機能用の次の IAM アクセス権限を貼り付けます。



指定する「バージョン」キーと値のペアが、AWS によって自動的に生成されるものと同じであることを 確認してください。

g) [次へ:確認]をクリックします。

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

h) [ポリシーの確認] タブで、ポリシーに有効な名前を付けて、[ポリシーの作成] をクリックします。

Create policy				1 2 3	
Review policy					
Name*	backend_autoscaling_poli	cy			
Description	Use alphanumeric and '+=,.@'	characters. Maximum 128 characters.			
Description					
	Maximum 1000 characters. Use	alphanumeric and '+=,,@' characters.		///	
Summary	Q Filter				
	Service 👻	Access level	Resource	Request condition	
	Allow (5 of 338 services	Show remaining 333			
	EC2	Limited: List	All resources	None	
	EC2 Auto Scaling	Full access	All resources	None	
	IAM	Limited: Read	All resources	None	
	SNS	Limited: List, Write	All resources	None	
	SQS	Limited: Read, Write	All resources	None	
Tags					
	Key		Value	~	
		No	tags associated with the resource.		

i) **ID** アクセス管理ページで、作成したポリシー名をクリックします。ポリシーを展開して JSON 全体を 確認し、[次へ] をクリックします。

spatial powerst V000 vs	Ø truste potry (7
stan junces in stants i più atta rata.	(11111-0)
	(11111111)
name (7) = V Type = V Type = V Type = Type (7)	
steel sheety Calan.	
autocama juoto	© logy Ket
The second polations and polations and the second sec	11.
Carland Server Carland	
Profiles/Connel, Art m. Profiles read-only access to WD Deal Connel with the Att Management Connels.	
Presolution/has. Art II Provide reacony access to instant Stack et al IV ATS Manapoint Chalder.	
Profestangeounful. And m. Protest the address and analysis address and analysis address address address address interests from the Managelice Your Software' pape, and profests administrative access to ESS.	
B MOSSIONETHY. AND M. Administrative stress to 500 Clivitary	
Verder/1000Feed. ARL m. Provide need only areas to IRVE 4T + Gale.	
Andoningformat. ABLn. Provide mark of parents to Add Daning on Pro Add Danapored Coronals.	
Immuno(Miljinshi, ARI n., Posta alona to nanga El astiopi fe Relatifi education 2003.	
Introducting can Anti m. Mine Calcilly cush at Alf metion	
Distribution Adva Addit m	
Interfultureneel. ARI m. Protein patrony second a some to American second as a second a some to American second as a second a some to American second as a se	
Annucleanities. All n distributions to bails foundation to bails foundation to bails	
Responded Adv., Add m., Proceeding and the Advance RDM and the Add Management Classice.	
Speporklaw AMD m. This polysy parts permissions to tooplantum and mocks have AMD account. This poly also another the same to contact AMD support to practice and memory account.	
InstructiCityAllier, ANII m., Provides Nationane to Aneson TC2-Init Me 2005 Witeogenetic Constant.	
Secondanogunia ARI m. Provides and/or for another Social Dennis Managament Consults National Market Mill adverses II relations and paratime Another ARI Adverses II relations ARI Adverses II relations and paratime Another ARI Adverses II relations ARI Adverses II relations and paratime Another ARI Adverses II relations A	
a volget Throughing. ARI n	
Inservice/Colline. All II Protein-Inducing Science II. And And DocumEDE with MangeDitionagability Net That The policy and games science to Andore TCB and Andreso Topology amounted.	
kan kanadary ng kaland sa Janang and thu sama yamaan ku sa utaka Ne Le La samarang Mya au an et a lagan yaman nangarar Lakan.	

j)「名前、レビュー、作成」ページで、ロールに有効な名前を付けます。

=	Step 1 Select trusted entity	Name, review, and create	0
	Step 2 Add permissions	Role details	
	Step 3	Role name Enter a meaningful name to identify this role.	
	Name, review, and create	ADC_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 '+=, 0-," characters.	
		Step 1: Select trusted entities	Edit
		<pre>1 - { "Version": "2012-10-17", "Statement": [{</pre>	

k)「ロールを作成」をクリックします。

Permissions policy summary					
Policy name C	\bigtriangledown	Туре	\bigtriangledown	Attached as	
backend_autoscaling_policy		Customer managed		Permissions policy	
Tags are key-value pairs that you can add to AWS re	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re No tags associated with the resource.	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re No tags associated with the resource.	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re No tags associated with the resource. Add tag You can add up to 50 more tags.	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re No tags associated with the resource.	sources to help identify	, organize, or search for resources.			
Tags are key-value pairs that you can add to AWS re No tags associated with the resource. Add tag You can add up to 50 more tags.	sources to help identify	; organize, or search for resources.	Car	Provinue	Graat

6. 手順 1、2、3 を繰り返します。[更新] ボタンを選択し、ドロップダウンメニューを選択すると、作成したロー ルが表示されます。

Modify IAM role Info	
Attach an IAM role to your instance.	
Instance ID	
D I-099f319d4e89f0ca2 (adc)	
IAM role Select an IAM role to attach to your instance or create a new role if yo currently attached to your instance.	w haven't created any. The role you select replaces any roles the
Choose IAM role	C Create new IAM role
Q	

7.「**IAM** ロールを更新」をクリックします。

Modify IAM rol Attach an IAM role to y	2 Info uur instance.
Instance ID i-00c340e20500 iAM role Select an IAM role to al currently attached to y	a5b6e (NetScaler Gateway) tach to your instance or create a new role if you haven't created any. The role you select replaces any roles that a ur instance.
ADC_IAMRole	C Create new IAM role

IAM ポリシーシミュレーターで IAM ポリシーをテストする

IAM ポリシーシミュレーターは、IAM アクセスコントロールポリシーを実稼働環境に導入する前にその効果をテスト できるツールです。権限の確認とトラブルシューティングが簡単になります。

1. IAM ページで、テストする IAM ロールを選択し、「Simulate」をクリックします。次の例では、「ADC_IAMRole」 が IAM ロールです。

Identity and Access × Management (IAM)			Delete
Dashboard	Allows EC2 instances to call AWS services on your be	ehalf.	
 Access management User groups 	Summary		Edit
Users	Creation date	ABN	Instance profile ARN
Roles	July 18, 2022, 19:37 (UTC+05:30)	arn:aws:iam::999910688552:role/ADC_IAMRole	Carn: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)	C Simulat	Add normissions
Credential report	You can attach up to 10 managed policies.		
Organization activity	Q Filter policies by property or policy name and	press enter	< 1 > @
Service control policies (SCPs)		•	
	Policy name	⊽ Туре	▽ Description
Related consoles	backend_autoscaling_policy	Customer managed	
IAM Identity Center 12" New			

2. IAM ポリシーシミュレーターコンソールで、「モード」として「既存のポリシー」を選択します。

IAM Policy Simulator				lode : Existing Policies -		1110D	assumed-	
				Existing Policies	role/	AWSReservedSSO_IIM	/subhojitg -	CD743860DC5D603T
Users, Groups, and Roles	Policy Simulato	r		New Policy				
Users ~ Filter	Select service *	Select actions 👻	Select All	Deselect All		Reset Contexts	Clear Results	Run Simulation
There are no users associated with this account.	 Global Settings Action Settings and 	Results [0 actions set	lected. 0 action:	s not simulated. 0 actions	allowed. 0	actions denied.]		
	Service	Action		Resource Type	Simulat	ion Resource	Permission	

3. [ユーザー、グループ、ロール]タブで、ドロップダウンメニューから [ロール]を選択し、既存のロールを選 択します。

IAM Policy Simulator			Mode : Existing Policies -			7
Users, Groups, and Roles	Policy Simulato	or				
Roles - Filter	Select service -	Select actions Select	ct All Deselect All	Reset Contexts	Clear Results	Run Simulation
ADC_IAMRole	 Global Settings 	0				
aws-controltower-AdministratorExecuti	Action Settings an	d Results [0 actions selected. 0	actions not simulated. 0 actions all	owed. 0 actions denied.]		
aws-controltower-ConfigRecorderRole	Service	Action	Resource Type	Simulation Resource	Permission	
aws-controltower-ForwardSnsNotificati						

4. 既存のロールを選択したら、その下にある既存のポリシーを選択します。

IAM Policy Simulator			Mode : Existing Policies -				
Policies Back Create New Policy	Policy Simulator						
Selected role: ADC_IAMRole	Select service	ct actions	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. ポリシーを選択すると、画面の左側に正確な JSON が表示されます。[アクションの選択] ドロップダウンメニ ューで目的のアクションを選択します。



Policies Back	Policy Simulato	r				
Editing policy: backend_autoscaling_policy	Amazon EC2 A 🔻	Select actions 🔹	Select All Deselect All	Reset 0	Clear Results	Run Simulation
ſ	 Global Settings 	AttachInstances	AttachLoadBalancerTar	AttachLoadBalancers	BatchDeleteScheduled	
"Version": "2012-10-17",	Action Settings and	BatchPutScheduledUp	CancelInstanceRefresh	CompleteLifecycleAction	CreateAutoScalingGroup	
"Statement": [{	Service	CreateLaunchConfigur	CreateOrUpdateTags	DeleteAutoScalingGroup	DeleteLaunchConfigura	
"Sid": "VisualEditor0", "Effect": "Allow"		DeleteLifecycleHook	DeleteNotificationConfi	DeletePolicy	DeleteScheduledAction	
"Action": [DeleteTags	DeleteWarmPool	DescribeAccountLimits	DescribeAdjustmentTy	
"ec2:DescribeInstances", "autoscaling:*",		DescribeAutoScalingGr	DescribeAutoScalingIn	DescribeAutoScalingN	DescribeInstanceRefre	
"sns:CreateTopic",		DescribeLaunchConfig	DescribeLifecycleHook	DescribeLifecycleHooks	DescribeLoadBalancer	
"sns:ListTopics",		DescribeLoadBalancers	DescribeMetricCollecti	DescribeNotificationCo	DescribePolicies	
"sns:Subscribe", "sqs:CreateQueue",		DescribeScalingActivities	DescribeScalingProces	DescribeScheduledActi	DescribeTags	
"sqs:ListQueues",		DescribeTerminationPo	DescribeWarmPool	DetachInstances	DetachLoadBalancerTa	
"sqs:Deletemessage, "sqs:GetQueueAttributes",		DetachLoadBalancers	DisableMetricsCollection	EnableMetricsCollection	EnterStandby	
"sqs:SetQueueAttributes", "iam:SimulatePrincipalPolicy",		ExecutePolicy	ExitStandby	GetPredictiveScalingFo	PutLifecycleHook	
"iam:GetRole"		PutNotificationConfigur	PutScalingPolicy	PutScheduledUpdateG	PutWarmPool	
J, "Resource": "*"		RecordLifecycleAction	ResumeProcesses	SetDesiredCapacity	SetInstanceHealth	
}		SetInstanceProtection	StartInstanceRefresh	SuspendProcesses	TerminateInstanceInAut	
}						

6. [シミュレーションを実行]をクリックします。

Policies	Policy Simulator				
Editing policy: backend_autoscaling_policy	Amazon EC2 A 👻 61 Action	(s) sel • Select All	Deselect All	Reset Contexts	Clear Results Run Simulation
{	 Global Settings ¹ 				
"Version": "2012-10-17", "Statement": [Action Settings and Result	S [61 actions selected. 0 actions	not simulated. 61 action	s allowed. 0 actions denied.]	
{	Service	Action	Resource Type	Simulation Resource	Permission
"Effect": "Allow",	Amazon EC2 Auto Scaling	AttachInstances	autoScalingGroup	•	allowed 1 matching statements.
"ectons ["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", "sqs:SetQueueAttributes",	Amazon EC2 Auto Scaling	CompleteLifecycleAction	autoScalingGroup	•	allowed 1 matching statements.
"iam:SimulatePrincipalPolicy", "iam:GetRole"	Amazon EC2 Auto Scaling	CreateAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.
], "Recourse": "*"	Amazon EC2 Auto Scaling	CreateLaunchConfiguration	launchConfiguration	•	allowed 1 matching statements.
}	Amazon EC2 Auto Scaling	CreateOrUpdateTags	autoScalingGroup	•	allowed 1 matching statements.
}	Amazon EC2 Auto Scaling	DeleteAutoScalingGroup	autoScalingGroup	•	allowed 1 matching statements.
	Amazon EC2 Auto Scaling	DeleteLaunchConfiguration	launchConfiguration	•	allowed 1 matching statements.
	Amazon EC2 Auto Scaling	DeleteLifecycleHook	autoScalingGroup	•	allowed 1 matching statements.
	Amazon EC2 Auto Scaling	DeleteNotificationConfiguration	autoScalingGroup	•	allowed 1 matching statements.

詳細については、AWS IAM ドキュメントを参照してください。

その他の参考資料

IAM ロールを使用して Amazon EC2 インスタンスで実行されているアプリケーションにアクセス権限を付与する

AWS 上の NetScaler VPX インスタンスの仕組み

October 17, 2024

NetScaler VPX インスタンスは AWS マーケットプレイスで AMI として入手でき、AWS VPC 内で EC2 インスタン スとして起動することもできます。NetScaler VPX AMI インスタンスには、少なくとも 2 つの仮想 CPU と 2 GB の メモリが必要です。また、AWS VPC 内で起動される EC2 インスタンスは、複数のインターフェイス、インターフェ イスごとに複数の IP アドレス、VPX 構成に必要なパブリックおよびプライベート IP アドレスも提供できます。各 VPX インスタンスには、少なくとも 3 つの IP サブネットが必要です。

- 管理サブネット
- クライアント側サブネット (VIP)
- バックエンド向けサブネット (SNIP、MIP など)

AWS での標準の VPX インスタンスのインストールには、3 つのネットワークインターフェイスをお勧めします。

現在、AWS では、AWS VPC 内で実行しているインスタンスでのみ、マルチ IP 機能を使用できます。VPC 内の VPX インスタンスを使用して、EC2 インスタンスで実行しているサーバーの負荷を分散できます。Amazon VPC を使用 すれば、独自の IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどを含めて、仮想ネッ トワーク環境を作成および管理できます。

注

デフォルトでは、各 AWS アカウントの AWS リージョンごとに最大 5 つの VPC インスタンスを作成 できます。Amazon のリクエストフォームを送信することで、より高い VPC 制限をリクエストhttp: //aws.amazon.com/contact-us/vpc-requestできます。



図 1. AWS アーキテクチャ上の NetScaler VPX インスタンスのサンプル展開

図1は、AWS VPC のシンプルなトポロジを示しています。NetScaler VPX の展開。AWS VPC は、以下の要素で構成されています。

- 1. VPC からの送受信トラフィックをルーティングするための単一のインターネットゲートウェイ。
- 2. インターネットゲートウェイとインターネット間のネットワーク接続。
- 3.3つのサブネット(管理、クライアント、サーバー用に1つずつ)。
- 4. インターネットゲートウェイと2つのサブネット(管理用とクライアント用)間のネットワーク接続。
- 5. VPC 内にデプロイされたスタンドアロンの NetScaler VPX インスタンス。VPX インスタンスには、各サブネットに 1 つずつ接続された ENI が 3 つあります。

NetScaler VPX スタンドアロンインスタンスを AWS にデプロイする

April 1, 2025

NetScaler VPX スタンドアロンインスタンスは、次のオプションを使用して AWS にデプロイできます。

- AWS ウェブコンソール
- Citrix が作成した CloudFormation テンプレート
- AWS CLI

このトピックでは、NetScaler VPX インスタンスを AWS にデプロイする手順について説明します。

展開を開始する前に、以下のトピックをお読みください。

- 前提条件
- 制限事項と使用上のガイドライン

AWS ウェブコンソールを使用して NetScaler VPX インスタンスを AWS にデプロイします

AWS Web コンソールを使用して、AWS で NetScaler VPX インスタンスを展開できます。展開のプロセスには、次の手順が含まれます。

1. キーペアの作成

- 2. 仮想プライベートクラウド (VPC) の作成
- 3. サブネットをさらに追加する
- 4. セキュリティグループとセキュリティルールの作成
- 5. ルートテーブルの追加
- 6. インターネットゲートウェイを作成する
- 7. NetScaler VPX インスタンスを作成する
- 8. ネットワークインターフェースをさらに作成してアタッチする
- 9. エラスティック IP の管理 NIC へのアタッチ
- 10. VPX インスタンスに接続する

ステップ **1:** キーペアを作成します。

Amazon EC2 は、キーペアを使用してログオン情報を暗号化および復号します。インスタンスにログオンするには、 キーペアを作成し、インスタンスを起動するときにキーペアの名前を指定し、インスタンスに接続するときにプライ ベートキーを指定する必要があります。

AWS Launch Instance ウィザードを使用してインスタンスを確認し、起動すると、既存のキーペアを使用するか、 新しいキーペアを作成するように求められます。キーペアの作成方法の詳細については、「Amazon EC2 キーペア」 を参照してください。

ステップ **2: VPC** を作成します。

NetScaler VPC インスタンスは AWS VPC 内で展開されます。VPC では、AWS アカウント専用の仮想ネットワー クを定義できます。AWS VPC の詳細については、「Amazon VPC の使用開始」を参照してください。

NetScaler VPX インスタンスに対する VPC の作成中は、次の点に留意してください。

- AWS アベイラビリティーゾーンに AWS VPC を作成するには、単一のパブリックサブネットのみのオプションで VPC を使用します。
- Citrix では、以下のタイプのサブネットを少なくとも3つ作成することをお勧めします。
 - 管理トラフィック用の1つのサブネット。このサブネットに管理 IP (NSIP) を配置します。デフォルトでは、エラスティックネットワークインターフェース (ENI) eth0 が管理 IP に使用されます。
 - クライアントアクセス(ユーザーから NetScaler ADC VPX)トラフィック用の1つ以上のサブネット。
 クライアントが NetScaler ADC 負荷分散仮想サーバーに割り当てられた1つ以上の仮想 IP(VIP)アドレスに接続します。
 - サーバーアクセス(VPX からサーバーへ)トラフィック用の1つ以上のサブネット。サーバーはこのサ ブネットを介して VPX 所有のサブネット IP(SNIP)アドレスに接続します。NetScaler 負荷分散と仮 想サーバー、仮想 IP アドレス(VIP)、サブネット IP アドレス(SNIP)の詳細については、以下を参照 してください。
 - すべてのサブネットは、同じアベイラビリティーゾーンに存在する必要があります。

ステップ **3:** サブネットを追加します。

VPC ウィザードを使った場合、作成されたサブネットは1つのみです。要件に応じて、さらにサブネットを作成する こともできます。サブネットをさらに作成する方法について詳しくは、「VPC へのサブネットの追加」を参照してく ださい。

ステップ 4: セキュリティグループとセキュリティルールを作成します。

受信トラフィックと送信トラフィックを制御するには、セキュリティグループを作成し、そのグループに規則を追加 します。グループを作成してルールを追加する方法の詳細については、「VPC のセキュリティグループ」を参照して ください。

NetScaler VPX インスタンスの場合、EC2 ウィザードはデフォルトのセキュリティグループを提供します。このセ キュリティグループは、AWS マーケットプレイスによって生成され、Citrix が推奨する設定に基づいています。ただ し、要件に応じてさらにセキュリティグループを作成できます。

注

ポート 22、80、443 をセキュリティグループでそれぞれ SSH、HTTP、HTTPS アクセス用に開きます。

ステップ **5:** ルートテーブルを追加します。

ルートテーブルには、ネットワークトラフィックの経路を判断する際に使用される、ルートと呼ばれる一連のルール が含まれます。VPC の各サブネットはルートテーブルに関連付ける必要があります。ルートテーブルの作成方法につ いて詳しくは、「ルートテーブル」を参照してください。

ステップ 6:インターネット Gateway を作成します。

インターネットゲートウェイには 2 つの目的があります。1 つは、インターネットでルーティング可能なトラフィッ クのターゲットを VPC ルートテーブルに提供すること、もう 1 つはパブリック IPv4 アドレスが割り当てられたイン スタンスに対してネットワークアドレス変換 (NAT) を実行することです。

インターネットトラフィックに対して、インターネットゲートウェイを作成します。インターネットゲートウェイの 作成方法の詳細については、「インターネットゲートウェイをアタッチする」を参照してください。

ステップ 7: AWS EC2 サービスを使用して NetScaler ADC VPX インスタンスを作成します。

AWS EC2 サービスを使って NetScaler VPX インスタンスを作成するには、次の手順に従います。

1. AWS ダッシュボードから、[コンピューティング] > [EC2] > [インスタンスの起動] > [AWS マーケットプレ イス] に移動します。

Launch Instance をクリックする前に、Launch Instance の下に表示される注記を確認して、リージョ ンが正しいことを確認してください。

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

- 2. [Search AWS Marketplace] バーで、「NetScaler VPX」と入力して検索します。
- 3. 展開するバージョンを選択し、[**Select**] をクリックします。NetScaler VPX バージョンでは、次のオプションがあります。
 - ライセンスバージョン
 - NetScaler VPX Express アプライアンス(これは無料の仮想アプライアンスで、NetScaler 12.0 56.20 から入手できます。)
 - 自分のデバイスを持参

Launch Instance ウィザードが起動します。ウィザードに従って、インスタンスを作成します。このウィザードでは、次のことを求められます。

- インスタンスの種類の選択
- インスタンスの構成
- ストレージの追加
- タグの追加
- セキュリティグループの構成
- ・レビュー

1. Choose AMI 2. Cl	hoose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review

ステップ8:ネットワークインターフェースをさらに作成してアタッチします。

VIP と SNIP 用に 2 つのネットワークインターフェイスを作成します。ネットワークインターフェイスの作成方法の 詳細については、「ネットワークインターフェイスの作成」を参照してください。

ネットワークインターフェイスを作成したら、VPX インスタンスにアタッチする必要があります。インターフェイス を接続する前に、VPX インスタンスをシャットダウンし、インターフェイスを接続し、インスタンスの電源をオンに します。ネットワークインターフェイスの接続方法の詳細については、「インスタンスの起動時にネットワークインタ ーフェイスをアタッチする」セクションを参照してください。

ステップ 9: Elastic IP を割り当てて関連付けます。

EC2 インスタンスにパブリック IP アドレスを割り当てた場合、そのアドレスはインスタンスが停止されるまで割り 当てられたままになります。その後、アドレスはプールに解放されます。インスタンスを再起動すると、新しいパブ リック IP アドレスが割り当てられます。

対照的に、Elastic IP (EIP) アドレスは、インスタンスとの関連付けが解除されるまで割り当てられたままになります。

管理 NIC のエラスティック IP を割り当てて、関連付けます。Elastic IP アドレスを割り当てて関連付ける方法の詳 細については、以下のトピックを参照してください。

- Elastic IP アドレスの割り当て
- Elastic IP アドレスを実行中のインスタンスに関連付ける

これらのステップで、AWS に NetScaler VPX インスタンスを作成する手順が完了します。インスタンスの準備が完 了するまで数分かかる場合があります。インスタンスがステータスチェックに合格したことを確認します。この情報 は、「インスタンス」ページの「ステータスチェック」列で確認できます。

ステップ 10: VPX インスタンスに接続します。

VPX インスタンスを作成したら、GUI と SSH クライアントを使用してインスタンスを接続します。

• GUI

NetScaler VPX インスタンスにアクセスするためのデフォルト管理者の資格情報は以下のとおりです。

ユーザー名: nsroot

パスワード:ns root アカウントのデフォルトパスワードは、NetScaler VPX インスタンスの AWS インスタンス ID に設定されます。最初のログオン時に、セキュリティ上の理由からパスワードを変更するように求められます。パス ワードを変更した後、構成を保存する必要があります。構成が保存されずにインスタンスが再起動する場合は、デフ ォルトのパスワードでログオンする必要があります。プロンプトでパスワードを再度変更します。

• SSH クライアント
AWS マネジメントコンソールから、NetScaler VPX インスタンスを選択して [接続] をクリックします。「インス タンスへの接続」ページの指示に従ってください。

AWS Web コンソールを使用して AWS に NetScaler VPX スタンドアロンインスタンスを展開する方法の詳細につ いては、「シナリオ: スタンドアロンインスタンス」を参照してください。

Citrix の CloudFormation テンプレートを使用して NetScaler VPX インスタンスを構成する

Citrix が提供する CloudFormation テンプレートを使用して、VPX インスタンスの起動を自動化できます。このテ ンプレートには、単一の NetScaler VPX インスタンスを起動したり、NetScaler VPX インスタンスのペアを使用し て高可用性環境を作成したりする機能があります。

テンプレートは AWS Marketplace または GitHub から起動できます。

CloudFormation テンプレートには既存の VPC 環境が必要で、3 つのエラスティックネットワークインターフェース (ENI)を備えた VPX インスタンスを起動します。CloudFormation テンプレートを開始する前に、以下の要件を満たしていることを確認してください。

- AWS 仮想プライベートクラウド(VPC)
- VPC内の3つのサブネット(1つは管理用、1つはクライアントトラフィック用、もう1つはバックエンドサ ーバー用)
- インスタンスへの SSH アクセスを有効にする EC2 キーペア
- UDP 3003、TCP 3009—3010、HTTP、SSH ポートが開いているセキュリティグループ

前提条件を満たす方法の詳細については、「AWS ウェブコンソールを使用して AWS に NetScaler ADC VPX インス タンスをデプロイする」セクションまたは AWS のドキュメントを参照してください。

このビデオでは、AWS Marketplace で利用可能な Citrix CloudFormation テンプレートを使用して、NetScaler VPX スタンドアロンインスタンスを構成して起動する方法について説明します。

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

IAM ロールはスタンドアロンデプロイでは必須ではありません。ただし、Citrix では、将来の必要に備えて、必要な 権限を持つ IAM ロールを作成してインスタンスにアタッチすることを推奨しています。IAM ロールにより、スタンド アロンインスタンスは、必要に応じて SR-IOV を使用して高可用性ノードに簡単に変換されます。

必要な権限の詳細については、「SR-IOV ネットワーク インターフェイスを使用するための NetScaler VPX インスタ ンスの構成」を参照してください。

注

AWS ウェブコンソールを使用して AWS に NetScaler VPX インスタンスをデプロイすると、CloudWatch サ ービスはデフォルトで有効になります。Citrix CloudFormation テンプレートを使用して NetScaler VPX イ ンスタンスを展開する場合、デフォルトのオプションは「はい」です。CloudWatch サービスを無効にする場 合は、「いいえ」を選択します。詳細については、「Amazon CloudWatch を使用してインスタンスを監視する」を参照してください。

AWS CLI を使用して NetScaler ADC VPX インスタンスを構成する

AWS CLI を使用してインスタンスを起動できます。詳細については、AWS コマンドラインインターフェイスのドキュメントを参照してください。

シナリオ:スタンドアロンインスタンス

April 1, 2025

このシナリオでは、AWS GUI を使用して NetScaler VPX スタンドアロン EC2 インスタンスを AWS にデプロイす る方法を示しています。3 つの NIC を持つスタンドアロン VPX インスタンスを作成します。インスタンスは、負荷分 散仮想サーバーとして構成されており、バックエンドサーバー(サーバーファーム)と通信します。この設定では、 インスタンスとバックエンドサーバー間、およびパブリックインターネット上のインスタンスと外部ホスト間の必要 な通信ルートを設定します。

VPX インスタンスを展開する手順の詳細については、「AWS に NetScaler VPX スタンドアロンインスタンスを展開 する」を参照してください。



3 つの NIC を作成します。各 NIC は、IP アドレスのペア(パブリックとプライベート)を使用して構成できます。 NIC は、次の目的に役立ちます。

NIC	目的	関連付けられている
eth0	NSIP(管理トラフィックを処理す	パブリック IP アドレスとプライベー
	る)	トIPアドレス
eth1	クライアント側のトラフィック	パブリック IP アドレスとプライベー
	(VIP)をサービスする	トIPアドレス
eth2	バックエンド・サーバ(SNIP)との	パブリック IP アドレス (プライベー
	通信	ト IP アドレスは必須ではありませ
		ん)

ステップ 1: VPC を作成します。

- 1. AWS ウェブコンソールにログオンし、[ネットワークとコンテンツ配信] > [**VPC**] に移動します。[**VPC** ウィザ ードの開始] をクリックします。
- 2. 単一のパブリックサブネットを持つ **VPC** を選択し、[Select] をクリックします。
- 3. このシナリオでは、IP CIDR ブロックを 10.0.0.0/16 に設定します。
- 4. VPC の名前を指定します。
- 5. パブリックサブネットを 10.0.0/24 に設定します。(これは管理ネットワークです)。
- 6. アベイラビリティ ゾーンを選択してください。
- 7. サブネットの名前を付けます。
- 8. [VPC の作成] をクリックします。

Step 2: VPC with a Sin	Step 2: VPC with a Single 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:*	10.0.0.0/24 (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							

ステップ 2: 追加のサブネットを作成します。

- 1. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。
- 2. ナビゲーションペインで、次の詳細を入力した後、[Subnets]、[Create Subnet] の順に選択します。
 - 名前タグ: サブネットの名前を指定します。

- VPC: サブネットを作成する VPC を選択します。
- アベイラビリティーゾーン: ステップ1で VPC を作成したアベイラビリティーゾーンを選択します。
- IPv4 CIDR ブロック: サブネットの IPv4 CIDR ブロックを指定します。 このシナリオでは、 10.0.1.0/24 を選択します。

Create Subnet						×
Use the CIDR format to spec netmask and /28 netmask. A	cify your subnet's IP address bloo Iso, note that a subnet can be th	ck (e.g., 10.0.0 e same size as	.0/24). Not your VPC	te that block sizes mus C. An IPv6 CIDR block	t be between a / must be a /64 Cli	16 DR block.
Name tag	NSDoc-client		0			
VPC	vpc-ac9ad2c5 NSDoc 💠 🕄)				
VPC CIDRs	CIDR	Status		Status Reason		
	10.0.0/16	associated				
Availability Zone IPv4 CIDR block	ap-south-1a 🛟 🛈		0			
					Cancel Yes	s, Create

3. この手順を繰り返して、バックエンドサーバー用のサブネットをもう1つ作成します。

Create Subnet					×				
Use the CIDR format to spec netmask and /28 netmask. A	ify your subnet's IP address blo Iso, note that a subnet can be th	ck (e.g., 10.0.0.0/24 ne same size as you	4). Note that block sizes must ir VPC. An IPv6 CIDR block m	be between a /16 ust be a /64 CIDR b	lock.				
Name tag	Name tag NSDoc-server								
VPC	vpc-ac9ad2c5 NSDoc 🛟 🖸								
VPC CIDRs	CIDR	Status	Status Reason						
	10.0.0/16	associated							
Availability Zone	No Preference	A							
IPV4 CIDR DIOCK	10.0.2.0/24	0							
			c	Cancel Yes, Cr	eate				

ステップ 3: ルートテーブルを作成します。

- 1. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。
- 2. ナビゲーションペインで、「ルートテーブル」>「ルートテーブル**を作成」を選択します。**
- 3. [Create Route Table] ウィンドウで、名前を追加し、ステップ1で作成した VPC を選択します。

4. [Yes, Create] をクリックします。

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

ルートテーブルは、この VPC 用に作成したすべてのサブネットに割り当てられます。これにより、あるサブ ネット内のインスタンスからのトラフィックのルーティングが別のサブネットのインスタンスに到達できるよ うになります。

- 5. サブネットの関連付けをクリックし、次に 編集をクリックします。
- 6. 管理サブネットとクライアントサブネットをクリックし、[Save] をクリックします。これにより、インターネ ットトラフィック専用のルートテーブルが作成されます。

rtb-4329082a NSDoc-internet-traffic									
Summa	ry	Routes	Subne	et Associatio	ns	Route	Propagation	٢	ags
Cancel	Save								
Associate	Subne	ət		IPv4 CIDR	IPve	CIDR	Current Route	Table	
	subnet	t-c4ce9aad NSDoc	-MGMT	10.0.0/24	-		rtb-735a7b1a		
	subnet	t-31ce9a58 NSDoc	-client	10.0.1.0/24	-		Main		
	subnet	t-d0cd99b9 NSDoo	c-server	10.0.2.0/24	-		Main		

- 7. [ルート]>[編集]>[別のルートを追加]をクリックします。
- 8. [Destination] フィールドに 0.0.0.0/0 を追加し、[Target] フィールドをクリックして [igw] (<xxxx> VPC ウィザードによって自動的に作成されたインターネットゲートウェイ) を選択します。
- 9. [保存] をクリックします。

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

10. サーバー側のトラフィックのルートテーブルを作成する手順に従います。

ステップ 4: NetScaler VPX インスタンスを作成します。

- 1. AWS マネジメントコンソールにログオンし、[Compute] の下の [EC2] をクリックします。
- [AWS マーケットプレイス] をクリックします。AWS Marketplace 検索バーに「NetScaler VPX」と入力し、 Enter キーを押します。使用可能な NetScaler VPX エディションが表示されます。
- 3.「選択」をクリックして、目的の NetScaler VPX エディションを選択します。EC2 インスタンスウィザードが 起動します。
- 4. [インスタンスタイプの選択] ページで、[**m4**] を選択します。Xlarge (推奨) をクリックし、[次へ: インスタンスの詳細を設定] をクリックします。
- 5.「インスタンスの詳細の構成」ページで、以下を選択し、「次へ:ストレージの追加」をクリックします。
 - インスタンス数:1
 - ネットワーク: ステップ1で作成した VPC
 - サブネット:管理サブネット
 - パブリック IP の自動割り当て: 有効

Choose AMI 2. Choose Instance Type	3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review	
ep 3: Configure Instan figure the instance to suit your require	CP Details nents. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower	r pricing, assign an access management role to the instance
Number of instances	Launch Into Auto Scaling Group ()	
Purchasing option	G Request Spot Instances	
Network	1 vpc-ac9ad2c5 NSDoc Create new VPC	
Subnet	subnet-c4ce9aad NSDcc-MGMT ap-south-ta Source new subnet 251 IP Addresses available	
Auto-assign Public IP	1 Enable	
Placement group	No placement group	
IAM role	I None C Create new IAM role	
Shutdown behavior	() Stop	
Enable termination protection	Protect against accidental termination	
Monitoring	Enable CloudWatch detailed monitoring Additional charges apply.	
EBS-optimized instance	Z Launch as EBS-optimized instance	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	

- 6. [ストレージの追加]ページで、デフォルトのオプションを選択し、[次へ:タグの追加]をクリックします。
- 7.「タグの追加」ページでインスタンスの名前を追加し、「次へ: セキュリティ グループの構成」をクリックしま す。
- 8. [セキュリティグループの設定] ページで、デフォルトのオプション(AWS Marketplace によって生成され、 Citrix Systems の推奨設定に基づいています)を選択し、[レビューして起動] をクリックします > 起動しま す。
- 9. 既存のキーペアを選択するか、新しいキーペアを作成して新しいキーペアを選択するように求められます。 [Select a key pair] ドロップダウンリストから、前提条件として作成したキーペアを選択します(「前提条件」 セクションを参照)。
- 10. キーペアを確認するにはチェックボックスをオンにして、[インスタンスの起動]をクリックします。

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. they allow you to connect to your instance securely. For Windows AMIs, the private key file to obtain the password used to log into your instance. For Linux AMIs, the private key file securely SSH into your instance.	. Together, le is required allows you to
Note: The selected key pair will be added to the set of keys authorized for this instance. L	earn more
about removing existing key pairs from a public AMI.	
Choose an existing key pair	٥
Select a key pair	
NSDOCKeypair	۵
I acknowledge that I have access to the selected private key file (NSDOCKeypair.p.)	em), and
that without this file. I won't be able to log into my instance.	
Cancel	Instances

[Launch Instance Wizard] に [Launch Status] が表示され、インスタンスが完全に起動されるとインスタンスの リストに表示されます。

インスタンスを確認するには、AWS コンソールに移動し、**EC2 >** 実行中のインスタンスをクリックします。インス タンスを選択し、名前を追加します。インスタンスの状態が実行中で、ステータスチェックが完了していることを確 認します。

ステップ5:より多くのネットワークインターフェイスを作成し、アタッチします。

VPC を作成したとき、それに関連付けられたネットワークインターフェイスは1つだけです。ここで、VIP と SNIP 用に、VPC にさらに2つのネットワーク インターフェイスを追加します。

- 1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
- 2. ナビゲーションペインで、[ネットワークインターフェイス]を選択します。
- 3.「ネットワークインタフェースの作成」を選択します。
- 4. 説明には、わかりやすい名前を入力します。
- 5. サブネットには、以前に VIP 用に作成したサブネットを選択します。
- 6. プライベート **IP** については、デフォルトオプションのままにします。
- 7. セキュリティ グループの場合は、グループを選択します。
- 8. [**Yes, Create**] をクリックします。

Create Netwo	ork l	nterface		×
Description	()	NSDoc-VIP-NIC		
Subnet		subnet-31ce9a58 ap-south-1a NSDoc-client		
Private IP	i	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. ネットワークインターフェースが作成されたら、インターフェースに名前を追加します。
- 10. この手順を繰り返して、サーバー側のトラフィック用のネットワークインターフェイスを作成します。

ネットワークインターフェイスをアタッチします。

- 1. ナビゲーションペインで、[ネットワークインターフェイス]を選択します。
- 2. ネットワークインターフェースを選択し、アタッチをクリックします。
- 3. [ネットワーク インターフェイスの接続] ダイアログ ボックスでインスタンスを選択し、[接続] をクリックします。

Name	Network Interna	Subliet ID	VPCID	Zone	Security groups
NSDoc-VIP	eni-3c843657	subnet-31ce9a	vpc-ac9ad2c5	ap-south-1a	default
NSDoc-SNIP	eni-3e8b3955	subnet-d0cd99	vpc-ac9ad2c5	ap-south-1a	default
	eni-dd1cacb6	subnet-9d43f6f4	vpc-52ab033b	ap-south-1a	FreeBSD 11-11-0-R
NSDoc-NSIP	eni-878133ec	subnet-c4ce9aad	vpc-ac9ad2c5	ap-south-1a	NetScaler VPX - Cu
	eni-2da8a261	subnot-fa6882b3	vnc-52ab033b	an-south-1h	AL1
	eni-e0f9128b	Attach Net	work Interf	ace	×
	eni-0e55e565				
	eni-1fa9ef53	Network Interf	ace: eni-3e8b395	5	
	eni-23ff4a48	Instance	D: 1029694619	cd5b71ec - NSDoc-V	M (running)
	eni-45fb4e2e				
	eni-76f84d1d				Attests
	eni-72ff183d			Cano	Attach
					I

ステップ 6: エラスティック IP を NSIP に接続します。

- 1. AWS マネジメントコンソールから、[ネットワークとセキュリティ] > [Elastic IP] に移動します。
- 2. アタッチする無料の EIP がないか確認してください。存在しない場合は、[新しいアドレスの割り当て] をクリ ックします。
- 3. 新しく割り当てられた IP アドレスを選択し、[アクション]>[アドレスの関連付け]を選択します。

- 4. [ネットワークインターフェイス] オプションボタンをクリックします。
- 5. [Network Interface] ドロップダウンリストから、管理 NIC を選択します。
- 6. [プライベート IP] ドロップダウンメニューから、AWS によって生成された IP アドレスを選択します。
- 7. [再関連付け] チェックボックスをオンにします。
- 8. [関連付け]をクリックします。

Associate address	Associate address							
Select the instance OR network interface to	which you want to associate th	his Elastic IP addres	ss (13.126.158.205)					
Resource type	Instance							
	 Network interface 							
Network interface	eni-878133ec	-	C					
Private IP	Q Filter by attributes		CO					
Reassociation	eni-0e55e565 eni-dd1cacb6 eni-76f84d1d		tached 🚯					
Warning If you associate an Elastic IP ad	eni-72ff183d eni-878133ec N eni-23ff4a48 eni-1fa9ef53	ISDoc-NSIP	ress is released. Learn more.					
* Required	eni-2da8a261			Cancel	Associate			

VPX インスタンスにアクセスします。

スタンドアロンの NetScaler VPX インスタンスを 3 つの NIC で構成したら、VPX インスタンスにログオンして NetScaler 側の構成を完了します。次のオプションを使用します。

• GUI: ブラウザに管理 NIC のパブリック IP を入力します。ユーザー名として nsroot を使用し、パスワード としてインスタンス ID(i-0c1ffe1d987817522)を使用してログオンします。

注

最初のログオン時に、セキュリティ上の理由からパスワードを変更するように求められます。パスワードを変 更した後、構成を保存する必要があります。構成が保存されずにインスタンスが再起動する場合は、デフォルト のパスワードでログオンする必要があります。プロンプトでパスワードを再度変更し、構成を保存します。

• SSH: SSH クライアントを開き、次のように入力します。

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

パブリック DNS を見つけるには、インスタンスをクリックし、[接続] をクリックします。

関連情報:

- Citrix ADC が所有する IP アドレス (NSIP、VIP、および SNIP) を構成するには、Citrix ADC 所有の IP ア ドレスの構成を参照してください。
- NetScaler VPX アプライアンスの BYOL バージョンを構成しました。詳細については、VPX ライセンス ガイド (https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrixnetscaler-vpx-licenses?language=en_US)

NetScaler VPX ライセンスをダウンロードする

October 17, 2024

AWS マーケットプレイスから NetScaler ADC VPX-カスタマーライセンスインスタンスを起動した後、ライセンス が必要です。VPX ライセンスの詳細については、ライセンスの概要を参照してください。

次の操作を実行する必要があります:

- 1. Citrix Web サイト内のライセンスポータルを使用して、有効なライセンスを生成します。
- 2. ライセンスをインスタンスにアップロードします。

有料 マーケットプレイスインスタンスの場合は、ライセンスをインストールする必要はありません。正しい機能セッ トとパフォーマンスが自動的にアクティブ化されます。

モデル番号が VPX5000 より大きい NetScaler VPX インスタンスを使う場合は、ネットワークのスループットはイ ンスタンスのライセンスに規定されているのと同じではないことがあります。ただし、SSL スループットや 1 秒あた りの SSL トランザクションといった他の機能は改善されている場合があります。

c4.8xlargeインスタンスタイプでは5Gbpsのネットワーク帯域幅が観測されます。

AWS サブスクリプションを BYOL に移行する方法

このセクションでは、AWS サブスクリプションから独自のライセンス (BYOL) に移行する手順、およびその逆につい て説明します。

AWS サブスクリプションを BYOL に移行するには、次の手順を実行します。

注

ステップ 2 と ステップ 3 は NetScaler VPX インスタンスで実行され、その他のすべての手順は AWS ポータ ルで実行されます。

- NetScaler VPX-同じセキュリティグループ、IAM ロール、サブネットを持つ古い EC2 インスタンスと同じア ベイラビリティーゾーンで、カスタマーライセンスを使用して BYOL EC2 インスタンスを作成します。新し い EC2 インスタンスには ENI インターフェイスが1つだけ必要です。
- 2. NetScaler GUI を使用して古い EC2 インスタンスのデータをバックアップするには、次の手順に従います。
 - a) [システム]>[バックアップと復元]に移動します。
 - b) [ようこそ] ページで、[バックアップ**/**インポート] をクリックしてプロセスを開始します。

System > Backup and Restore
Welcome to Backup and Restore
The backup and restore functionality of the Citrix ADC appliance allows you to create a backup file of the Citrix ADC configurations. This file can later be used to restore the Citrix ADC configurations to the previous state. To create a backup, click the "Backup" link shown below. When required, select one of the backups and restore the appliance.
Backup/Import

- c) [バックアップ/インポート]ページで、次の詳細を入力します。
 - Name: バックアップファイルの名前。
 - Level: バックアップレベルを「フル」として選択します。
 - [コメント]: バックアップの簡単な説明を入力します。

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

Backup/Import
Create Import
Citrix ADC Version NS13.1: Build 50.19.nc, Date: Sep 25 2023, 21:28:29 (64-bit)
File Name
fullbackup
Level*
Full V
Comment
None
Backup Cancel

d) [バックアップ] をクリックします。バックアップが完了したら、ファイルを選択してローカルマシンに ダウンロードできます。

System > B	ackup and Restore						
Backup	o and Resto	ore 🕕				/ R	2 📑
Backup/Im	port Delete	✓ Select Action Download Restore	Download				()
	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. NetScaler GUI を使用して新しい EC2 インスタンスにデータを復元するには、次の手順に従います。
 - a) [システム]>[バックアップと復元]に移動します。
 - b) [バックアップ/インポート] をクリックして、プロセスを開始します。
 - c) [インポート]オプションを選択し、バックアップファイルをアップロードします。

System > Backup and Restore > Backup/Import

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

- d) ファイルを選択します。
- e) [アクションの選択] ドロップダウンメニューから、[復元] を選択します。

System > B	ackup and Restore				
Backup	o and Rest	ore 🕕			
Backup/Im	port Delete	 ✓ Select Action Download Restore 	Restore		0
	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 Pa	ge V Page 1 of 1 < 🕨

```
f) [復元] ページで、ファイルの詳細を確認し、[復元] をクリックします。
```

File Name	
fullbackup.tgz	
Level	
Full	
Citrix ADC Version	
NS13.1-50.19	
P Address	
10.102.126.34	
Size (in KB)	
2117	
Created By	
nsroot	
Creation Time	
Wed Oct 4 15:01:42 20	23
Comment	
None	
🔵 Skip Backup 🚺	
Destars	Class

- 古い EC2 インスタンスから新しい EC2 インスタンスに、すべてのインターフェイス(NSIP アドレスがバインドされている管理インターフェイスを除く)を移動します。ネットワークインターフェイスを別の EC2 インスタンスに移動するには、次の手順を実行します。
 - a) AWS ポータルで、古い EC2 インスタンスと新しい EC2 インスタンスの両方を停止します。
 - b) [ネットワークインターフェイス] に移動し、古い EC2 インスタンスにアタッチされたネットワークイ ンターフェイスを選択します。
 - c) [アクション]>[デタッチ]をクリックして EC2 インスタンスをデタッチします。



d) [アクション]>[Attach] の順にクリックして、ネットワークインターフェイスを新しい EC2 インスタ ンスにアタッチします。ネットワークインターフェイスをアタッチする必要がある EC2 インスタンス名 を入力します。

New EC2 Experience X	Network interfaces (1/1			
EC2 Dashboard New				
Events				
Tags		Attach network interface	×	
Limits				
▼ Instances		Network interface		
Instances New	<u>a</u>	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) 接続されている他のすべてのインターフェイスについて、ステップ1からステップ4を実行します。シ ーケンスに従い、インターフェイスの順序を維持するようにしてください。つまり、まずインターフェ イス2をデタッチして接続し、次にインターフェイス3をデタッチして接続します。
- 古い EC2 インスタンスから管理インターフェイスをデタッチすることはできません。したがって、古い EC2 インスタンスの管理インターフェイス(プライマリネットワークインターフェイス)上のすべてのセカンダリ IP アドレス(存在する場合)を新しい EC2 インスタンスに移動します。IP アドレスをあるインターフェイス から別のインターフェイスに移動するには、次の手順を実行します。
 - a) AWS ポータルで、古い EC2 インスタンスと新しい EC2 インスタンスの両方が Stop 状態であること を確認します。

- b) [ネットワークインターフェイス] に移動し、古い EC2 インスタンスにアタッチされた管理ネットワー クインターフェイスを選択します。
- c) [アクション]>[IP アドレスの管理] の順にクリックし、割り当てられているすべてのセカンダリ IP ア ドレス(存在する場合)を書き留めます。
- d) 新しい EC2 インスタンスの管理ネットワークインターフェイスまたはプライマリインターフェイスに 移動します。
- e) [アクション] > [IP アドレスの管理] の順にクリックします。
- f) [IPv4 アドレス] で、[新しい IP アドレスを割り当て] をクリックします。
- g) ステップ 3 で説明する IP アドレスを入力します。
- h) [セカンダリプライベート IP アドレスの再割り当てを許可する] チェックボックスをオンにします。
- i) [保存] をクリックします。

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

- 6. 新しい EC2 インスタンスを起動し、設定を確認します。すべての設定が移動されたら、要件に従って古い EC2 インスタンスを削除または保持できます。
- 7. 古い EC2 インスタンスの NSIP アドレスに EIP アドレスがアタッチされている場合は、古いインスタンスの NSIP アドレスを新しいインスタンスの NSIP アドレスに移動します。
- 8. 古いインスタンスに戻す場合は、古いインスタンスと新しいインスタンスの逆の方法で同じ手順を実行します。
- 9. サブスクリプションインスタンスから BYOL インスタンスに移行した後、ライセンスが必要です。ライセンス をインストールするには、次の手順に従います。
 - Citrix Web サイトのライセンスポータルを使用して、有効なライセンスを生成します。
 - ライセンスをインスタンスにアップロードします。

注

BYOL インスタンスをサブスクリプションインスタンス (有料マーケットプレイスインスタンス) に移動する場合、ライセンスをインストールする必要はありません。正しい機能セットとパフォーマンスが自動的にアクティブ化されます。

制限事項

管理インターフェイスを新しい EC2 インスタンスに移動することはできません。したがって、管理インターフェイス を手動で構成することをお勧めします。詳細については、前の手順の手順 5 を参照してください。新しい EC2 インス タンスは、古い EC2 インスタンスの正確なレプリカで作成されますが、新しい IP アドレスは NSIP アドレスだけで す。

異なる可用性ゾーンでの負荷分散サーバー

October 17, 2024

VPX インスタンスを使用して、同じアベイラビリティーゾーンまたは以下の場所で稼働しているサーバーの負荷分散 を行うことができます。

- 同じ AWS VPC 内の異なるアベイラビリティーゾーン (AZ)
- 別の AWS リージョン
- ・ VPC 内の AWS EC2

VPX インスタンスが AWS VPC 外で稼働するサーバーの負荷を分散できるようにするには、VPX インスタンスが存 在する場合は、次のように、EIP を使用してインターネット ゲートウェイ経由でトラフィックをルーティングするよ うにインスタンスを構成します。

- 1. NetScaler CLI または GUI を使用して、NetScaler VPX インスタンスで SNIP を構成します。
- 2. サーバー側のトラフィック用にパブリックサブネットを作成することで、トラフィックが AZ からルーティン グされるようにします。
- 3. AWS GUI コンソールを使用して、インターネット Gateway ルートをルーティングテーブルに追加します。
- 4. 更新したルーティングテーブルをサーバー側のサブネットに関連付けます。
- 5. NetScaler SNIP アドレスにマップされているサーバー側のプライベート IP アドレスに EIP を関連付けます。

AWSでの高可用性の機能

October 17, 2024

AWS 上の2 つの NetScaler ADC VPX インスタンスを高可用性(HA)アクティブ/パッシブペアとして構成できま す。1 つのインスタンスをプライマリノードとして構成し、もう1 つをセカンダリノードとして設定すると、プライ マリノードは接続を受け入れ、サーバーを管理します。セカンダリノードはプライマリを監視します。何らかの理由 で1次ノードが接続を受け入れることができない場合は、2 次ノードが引き継ぎます。

AWS では、VPX インスタンスで次のデプロイタイプがサポートされています。

- 同一ゾーン内での高可用性
- 異なるゾーン間の高可用性
- 注

高可用性を機能させるには、両方の NetScaler ADC VPX インスタンスに IAM ロールがアタッチされ、Elastic IP(EIP)アドレスが NSIP に割り当てられていることを確認してください。NSIP が NAT インスタンスを介 してインターネットにアクセスできる場合は、NSIP に EIP を割り当てる必要はありません。

同じゾーン内の高可用性

同じゾーン内の高可用性展開では、両方の VPX インスタンスのネットワーク構成が類似している必要があります。

次の2つのルールに従います。

ルール 1. 1 つの VPX インスタンスの NIC は、他の VPX の対応する NIC と同じサブネットにある必要があります。 どちらのインスタンスにも次のものが必要です。

- 同じサブネット (管理サブネットと呼ばれる) 上の管理インターフェイス
- 同じサブネット (クライアントサブネットと呼ばれる) 上のクライアントインターフェイス
- 同じサブネット (サーバーサブネットと呼ばれる) 上のサーバーインターフェイス

ルール 2。両方のインスタンスの管理 NIC、クライアント NIC、およびサーバ NIC のシーケンスが同じである必要 があります。たとえば、次のシナリオはサポートされていません。たとえば、次のシナリオはサポートされていませ ん。

VPX インスタンス1

NIC 0: 管理 NIC 1: クライアント NIC 2: サーバー

VPX インスタンス2

NIC 0: 管理

NIC 1: サーバ

NIC 2: クライアント

このシナリオでは、インスタンス1の NIC1はクライアントサブネットにあり、インスタンス2の NIC1はサーバ ーサブネットにあります。HA が機能するには、両方のインスタンスの NIC1がクライアントサブネットまたはサー バーサブネット内にある必要があります。 13.0 41.xx から、フェールオーバー後にプライマリ HA ノードの NIC(クライアント側およびサーバ側の NIC)に接続されたセカンダリプライベート IP アドレスをセカンダリの HA ノードに移行することで、高可用性を実現できます。この展開は、以下のように管理されます。

- 両方の VPX インスタンスは、NIC 列挙に従って NIC の数とサブネットマッピングが同じです。
- 各 VPX NIC には、管理 IP アドレスに対応する最初の NIC を除き、追加のプライベート IP アドレスが 1 つあ ります。追加のプライベート IP アドレスは、AWS ウェブコンソールでプライマリプライベート IP アドレス として表示されます。このドキュメントでは、この余分な IP アドレスをダミー IP アドレスと呼んでいます)。
- ダミー IP アドレスは、NetScaler インスタンスで VIP および SNIP として構成しないでください。
- 必要に応じて、その他のセカンダリプライベート IP アドレスを作成し、VIP および SNIP として設定する必要があります。
- フェールオーバー時に、新しいプライマリノードは設定された SNIP および VIP を検索し、前のプライマリに 接続されている NIC から新しいプライマリ上の対応する NIC に移動します。
- NetScaler インスタンスでは、HA が機能するためには IAM アクセス許可が必要です。各インスタンスに追加された IAM ポリシーに次の IAM 権限を追加します。

"iam:GetRole"「ec2:インスタンスの説明」「ec2:ネットワークインターフェースの説明」「ec2 :プライベートIPアドレスの割り当て」

注

unassignPrivateIpAddress は必要ありません。

この方法は従来の方法よりも高速です。古い方法では、HA はプライマリノードの AWS Elastic ネットワークインタ ーフェイスからセカンダリノードへの移行に依存します。

従来の方法では、次のポリシーが必要です。

"iam:GetRole"「ec2:インスタンスの説明」「ec2:アドレスの説明」 "ec2:アソシエイトアドレス "「ec2:アドレスの関連付けを解除」

詳細については、「AWS に高可用性ペアをデプロイする」を参照してください。

異なるゾーン間の高可用性

独立ネットワーク構成(INC) モードでは、2 つの異なるサブネットまたは 2 つの異なる AWS アベイラビリティーゾ ーンに 2 つの NetScaler ADC VPX インスタンスを高可用性アクティブ/パッシブのペアとして構成できます。フェ イルオーバー時に、プライマリインスタンスの VIP の EIP (Elastic IP) がセカンダリに移行し、セカンダリが新しい プライマリとして引き継がれます。フェイルオーバープロセスでは、AWS API は以下を実行します。

• IPSetsが接続されている仮想サーバーをチェックします。

- 仮想サーバーがリッスンしている 2 つの IP アドレスから、パブリック IP が関連付けられている IP アドレス を検索します。1 つは仮想サーバに直接接続され、もう 1 つは IP セットを介して接続されます。
- パブリック IP (EIP) を、新しいプライマリ VIP に属するプライベート IP に再関連付けします。

異なるゾーン間の HA には、次のポリシーが必要です。

"iam:GetRole"「ec2:インスタンスの説明」「ec2:アドレスの説明」 "ec2:アソシエイトアドレス"「ec2:アドレスの関連付けを解除」

詳細については、「AWS アベイラビリティーゾーン全体の高可用性」を参照してください。

展開を開始する前に

AWS で HA のデプロイを開始する前に、次のドキュメントをお読みください。

- 前提条件
- 制限事項と使用ガイドライン
- AWS で NetScaler ADC VPX インスタンスを展開する
- 高可用性

トラブルシューティング

AWS クラウド上の NetScaler ADC VPX インスタンスの HA フェイルオーバー中の障害をトラブルシューティング するには、/var/log/の場所に保存されているcloud-ha-daemon.logファイルを確認してください。

同じ AWS 可用性ゾーンに VPX HA ペアを展開する

October 17, 2024

注

NetScaler リリース 13.1 ビルド 27.x 以降、同じ AWS アベイラビリティーゾーン内の VPX HA ペアは IPv6 アドレスをサポートします。

両方の VPX インスタンスが同じサブネット上にある同じ AWS ゾーンで、AWS 上の 2 つの NetScaler VPX インス タンスを HA ペアとして構成できます。HA は、フェイルオーバー後に、プライマリ HA ノードの NIC(クライアン ト側およびサーバ側 NIC)に接続されているセカンダリプライベート IP アドレスをセカンダリ HA ノードに移行す ることで実現されます。セカンダリプライベート IP アドレスに関連付けられているすべての Elastic IP アドレスも 移行されます。

NetScaler VPX HA ペアは、同じ AWS アベイラビリティーゾーンで IPv4 アドレスと IPv6 アドレスの両方をサポートします。

次の図は、セカンダリプライベート IP アドレスを移行する HA フェールオーバーのシナリオを示しています。



図1: インライン展開図1: プライベート IP マイグレーションを使用した、AWS 上の NetScaler VPX HA ペア

ドキュメントを開始する前に、次のドキュメントをお読みください。

- 前提条件
- 制限事項と使用ガイドライン
- AWS で NetScaler ADC VPX インスタンスを展開する
- 高可用性

VPX HA ペアを同じゾーンにデプロイする方法

VPX HA ペアを同じゾーンにデプロイする手順の概要を次に示します。

- 手順1:同じVPCを使用して、それぞれ3つのNIC(イーサネット0、イーサネット1、イーサネット2)を 持つ2つのVPX インスタンス(プライマリノードとセカンダリノード)を作成します
- 2. AWS セカンダリプライベート IP アドレスをプライマリノードの VIP と SNIP に割り当てます。
- 3. AWS セカンダリプライベート IP アドレスを使用して、プライマリノードで VIP と SNIP を設定します。
- 4. 両方のノードで HA を設定します。

手順 1. AWS 上に 2 つの VPX インスタンスを作成します。各インスタンスには 3 つの NIC があります

AWS ウェブコンソールを使用して、NetScaler VPX インスタンスを AWS にデプロイするに記載されている手順に 従います。 手順 3. 手順 2: プライマリノードで、イーサネット 1 (クライアント IP または VIP) とイーサネット 2 (バックエン ドサーバー IP または SNIP) にプライベート IP アドレスを割り当てます

AWS コンソールは、設定された NIC にプライマリプライベート IP アドレスを自動的に割り当てます。VIP と SNIP には、セカンダリプライベート IP アドレスと呼ばれる、より多くのプライベート IP アドレスを割り当てます。

プライベート IP アドレスをネットワークインターフェイスに割り当てるには、次の手順に従います。

- 1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
- 2. ナビゲーションペインで、[Network Interfaces]を選択し、インスタンスにアタッチされているネットワ ークインターフェイスを選択します。
- 3. アクション > IP アドレスの管理を選択します。
- 4. 要件に基づいて [IPv4 アドレス] または [IPv6 アドレス] を選択します。
- 5. IPv4 アドレスの場合:
 - a) [新しい IP を割り当てる]を選択します。
 - b) インスタンスのサブネット範囲内にある特定の IPv4 アドレスを入力するか、フィールドを空白のまま にして Amazon が IP アドレスを選択するようにします。
 - c) (オプション) セカンダリプライベート IP アドレスが既に別のネットワークインターフェイスに割り当 てられている場合に、そのアドレスを再割り当てできるようにするには、[Allow reassign] を選択しま す。
- 6. IPv6 アドレスの場合:
 - a) [新しい IP を割り当てる]を選択します。
 - b) インスタンスのサブネット範囲内にある特定の IPv6 アドレスを入力するか、フィールドを空白のまま にして Amazon が IP アドレスを選択できるようにします。
 - c) (オプション) プライマリまたはセカンダリプライベート IP アドレスが既に別のネットワークインタ ーフェイスに割り当てられている場合に、そのアドレスを再割り当てできるようにするには、[Allow reassign] を選択します。
- 7. はい>更新を選択します。

インスタンスの説明の下に、割り当てられたプライベート IP アドレスが表示されます。

注

IPv4 HA ペア展開では、インターフェイスにセカンダリ IPv4 アドレスのみを割り当て、それらを VIP アドレ スおよび SNIP アドレスとして使用できます。ただし、IPv6 HA ペア展開では、インターフェイスでプライマ リ IPv6 アドレスまたはセカンダリ IPv6 アドレスを割り当て、それらを VIP アドレスおよび SNIP アドレスと して使用できます。

手順 3. 手順 3: セカンダリプライベート IP アドレスを使用して、プライマリノードで VIP と SNIP を構成します

SSH を使用してプライマリノードにアクセスします。ssh クライアントを開き、次のように入力します。

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

次に、VIP と SNIP を設定します。

VIP の場合は、次のように入力します。

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

SNIP の場合は次のように入力します。

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

save configを入力して保存します。

設定された IP アドレスを表示するには、次のコマンドを入力します。

1 show ns ip

詳しくは、次のトピックを参照してください:

- 仮想 IP (VIP) アドレスの構成と管理
- NSIP アドレスの構成

ステップ 4: 両方のインスタンスで HA を設定する

プライマリノードでシェルクライアントを開き、次のコマンドを入力します。

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

セカンダリノードで、次のコマンドを入力します。

save configと入力して、設定を保存します。

構成された HA ノードを表示するには、show ha nodeと入力します。

フェイルオーバー時に、前のプライマリノードで VIP および SNIP として構成されたセカンダリプライベート IP ア ドレスは、新しいプライマリノードに移行されます。

ノードでフェイルオーバーを強制するには、force HAfailoverと入力します。

セカンダリプライベート IP 移行に基づいて、レガシー HA ペアを新しい HA ペアに移行

注

ENI 移行に基づいて機能する VPX HA ペアをデプロイする従来の方法は廃止されました。そのため、セカンダ リプライベート IP 移行に基づく HA ペア展開を使用することをお勧めします。

セカンダリプライベート IP の移行に基づいてレガシー HA ペアから新しい HA ペアへのシームレスな移行を可能に するには、次の点を確認してください:

- 1. プライマリノードとセカンダリノードの両方に同じ数のインターフェイスが必要で、これらのインターフェイ スは同じサブネット内にある必要があります。
- 2. 従来の方法でプライマリプライベート IP アドレスとして設定された VIP と SNIP は、新しい方法ではセカン ダリプライベート IP アドレスに移行する必要があります。
- 3. 新しい HA 展開に必要な IAM 権限を、プライマリおよびセカンダリの NetScaler インスタンスに追加する必要があります。
- 4. プライマリとセカンダリの NetScaler インスタンスの両方を再起動します。

詳細については、「同じゾーン内の高可用性」を参照してください。

Citrix CloudFormation テンプレートを使用して高可用性ペアをデプロイする

CloudFormation テンプレートを開始する前に、次の要件を満たしていることを確認してください。

- VPC
- VPC 内の3つのサブネット
- UDP 3003、TCP 3009—3010、HTTP、SSH ポートが開いているセキュリティグループ
- キーペア
- インターネットゲートウェイを作成する
- クライアントネットワークと管理ネットワークのルートテーブルを編集して、インターネットゲートウェイを 指すようにする

注

Citrix CloudFormation テンプレートは、IAM ロールを自動的に作成します。既存の IAM ロールはテンプレートには表示されません。

Citrix CloudFormation テンプレートを起動するには、次の手順に従います。

- 1. AWS 認証情報を使用して AWS マーケットプレイスにログオンします。
- 2. 検索フィールドに「NetScaler VPX」と入力して NetScaler AMI を検索し、[Go] をクリックします。
- 3. 検索結果ページで、目的の NetScaler VPX 製品をクリックします。
- 4.「価格設定」タブをクリックして、「価格情報」に移動します。
- 5. リージョンとフルフィルメントオプションを「NetScaler VPX-カスタマーライセンス」として選択します。

- 6. [続行]をクリックして購読します。
- 7. [購読]ページで詳細を確認し、[構成に進む]をクリックします。
- 8. CloudFormation テンプレートとして [配信方法]を選択します。
- 9. 必要な CloudFormation テンプレートを選択します。
- 10. [** ソフトウェアのバージョンとリージョン]を選択し、[** 続行]をクリックして起動します。

aws ma	rketplace		Q Search					Hell
About 👻	Categories 🔻	Delivery Methods 🔻	Solutions 🔻	AWS IQ 👻	Resources 👻	Your Sav	red List	
					Become a Chann	el Partner	Sell in AWS Marketplace	Amazon Web Services H
	net>sc	aler. NetScal	.er VPX - C	Sustomer	Licensed		Con	tinue to Launch
	< Product Detai	l Subscribe <u>Configure</u>	e					
	Config	jure this sof	tware	- to 1 1	1		Pricing i	information
	Choose a fu Fulfillmen CloudFor	ιπιιment option and s t option mation Template	ortware versioi	n το launch th CloudFormatio Deploy a compl	IS SOftWare.	ion	This is an e software a based on y Your actual statement this estima	estimate of typical nd infrastructure costs our configuration. l charges for each period may differ from te.
	Citrix AD	C VPX - HA Same Availab	ility Zone 💲	using a CloudFo	ormation template		Softwar NetScaler VPX - Customer Licensed	e Pricing \$0/hr
	Software v 13.1-48. W N n	Version 47 (Jun 23, 2023) /hats in This Version etScaler VPX - Customer Lice Inning on m5.xlarge 2017	nsed				BYOL ⊂ running on m5.xlarge	

- 11. [AWS CloudFormation が IAM リソースを作成する可能性があることを承認します] を選択します。** チ ェックボックスをオンにし、[** スタックを作成] をクリックします。
- 12. [次へ] をクリックします。

Step 1 Specify template	Create stack	
Step 2 Specify stack details	Prerequisite - Prepare template	
Step 3	Prepare template Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the state	ck.
CONTIQUEE STALK ODUOTIS	Template is ready Use a sample template Create template in Designer	
and and and approved		
Step 4 Review	Specify template	
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon 53 URL where it will be stored.	
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL, where it will be stored. Image: Complex Selecting a template generates an Amazon S3 URL where it will be stored.	
Step 4 Review	Specify template A template is a JSON or YAML file that describes your stack's resources and properties. Template source Selecting a template generates an Amazon S3 URL where it will be stored. Imazon S3 URL Imazon S3 URL Amazon S3 URL	o include in the stack. in Designer ae-4953-45b4-8b902a
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. Imazon S3 URL Amazon S3 URL Amazon S3 URL Intps://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/63425ded-82f0-4b54-8cdd-6ec8b94bd4f8.6f89d7a4-6cae-4953-45b4-8l	b9

- 13. [スタックの詳細を指定]ページが表示されます。次の詳細を入力します。
 - スタック名を入力します。名前は25文字以内である必要があります。
 - [ネットワーク構成]で、次の操作を実行します。
 - [管理サブネットワーク]、[クライアントサブネットワーク]、および [サーバーサブネットワーク] を選択します。[VPC ID] で選択した VPC 内で作成した正しいサブネットワークを選択しているこ とを確認します。
 - プライマリ管理 IP、セカンダリ管理 IP、クライアント IP、およびサーバ IP を追加します。IP アドレスは、それぞれのサブネットワークの同じサブネットに属している必要があります。または、テンプレートに IP アドレスが自動的に割り当てられるようにすることもできます。
 - **vpcTenancy** で [デフォルト] を選択します。
 - NetScaler 構成で、以下を実行します。
 - [インスタンスタイプ]で[m5.xlarge]を選択します。
 - [Key Pair] のメニューから、作成済みのキーペアを選択します。
 - デフォルトでは、CloudWatch にカスタム メトリックを公開しますか? オプションは はいに設定されています。グラフをカスタマイズするには、[グラフ] オプションを使用します。
 CloudWatch メトリクスの詳細については、[Amazon CloudWatch を使用してインスタンスを 監視する] (#monitor-your-instances-using-amazon-cloudWatch) を参照してください。
 - [オプション構成]で、次の操作を行います。
 - デフォルトでは、管理インターフェースにパブリック IP(EIP) を割り当てる必要がありますか?オ プションは いいえに設定されています。
 - デフォルトでは、パブリック IP(EIP) をクライアントインターフェースに割り当てる必要があり ますか? オプションは いいえに設定されています。



14. [次へ] をクリックします。

15. 【スタックオプションの設定】 ページが表示されます。これはオプションのページです。

Step 1 Specify template	Configure stack options					
Step 2 Specify stack details	Tags You can specify tags Bey-value pains) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more 🛃					
Step 3 Configure stack options	Koy Volue					
Step 4 Review						
	Add tag					
	Permissions Choose an MM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permission based on your user ordentials. Learn more 🕑					
	IAM role - optional Crosse the UAH old for CloadFormation 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 [2]					
	Stack policy Defines the resources that you want to protect from unintentional updates during a stack update.					
	Rollback configuration Specify adams for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. Learn more C					
	Notification options					
	Stack creation options					

- 16. [次へ] をクリックします。
- 17. [オプション]ページが表示されます。(これはオプションのページです)。[次へ] をクリックします。
- 18. [Review] ページが表示されます。しばらくして、設定を確認し、必要に応じて変更を加えます。
- 19. AWS CloudFormation が IAM リソースを作成する可能性があることを承認します。を選択します。チェ ックボックスをオンにして、[スタックの作成]をクリックします。
- 20. CREATE-IN-PROGRESS が表示されます。ステータスが CREATE-COMPLETE になるまで待ちます。ス テータスが COMPLETE に変更されない場合は、[Events]タブで失敗の原因を確認し、適切な構成でイン スタンスを再作成します。

C View nested	C X < 1 >	Stack info Events F Events (38)	Resources	Outputs Parameters	Delete Template Change sets	Update Stack actions V
2020-10-28 13:42:49 UTC+0530 CREATE_COMPLETE	•	Q Search events		Legisl ID	Status	Fashing services
		Timescamp	· ·	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	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	

- IAM リソースが作成されたら、[EC2 マネジメントコンソール]>[インスタンス]に移動します。IAM ロール で作成された 2 つの VPX インスタンスがあります。プライマリノードとセカンダリノードは、それぞれ 3 つ のプライベート IP アドレスと 3 つのネットワークインターフェイスを使用して作成されます。
- ユーザー名nsrootとインスタンス ID をパスワードとしてプライマリノードにログオンします。GUI から、 [システム]>[高可用性]>[ノード]に移動します。NetScaler VPX は、CloudFormation テンプレートに よって HA ペアで既に構成されています。
- 23. NetScaler VPX HA ペアが表示されます。

Nodes	5 💿									
Add	Edit	statist	cs	Select Action	~					
	ID ¢	IP ADDRESS		HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE		SYNCHRONIZA
	0				Primary	• UP	DISABLED	ENABLED		-NA-
	1				Secondary	• UP	DISABLED	SUCCESS		-NA-
Total 2									2	5 Per Page 🗸 🗸

Amazon CloudWatch を使用してインスタンスをモニタリングする

Amazon CloudWatch サービスを使用して、CPU とメモリの使用率、スループットなど、一連の NetScaler VPX メトリクスを監視できます。CloudWatch は AWS で実行されるリソースとアプリケーションをリアルタイムでモニ タリングします。AWS マネジメントコンソールを使用して、Amazon CloudWatch ダッシュボードにアクセスで きます。詳細については、「Amazon CloudWatch」を参照してください。

注意事項

• AWS ウェブコンソールを使用して AWS に NetScaler VPX インスタンスをデプロイすると、CloudWatch サービスはデフォルトで有効になります。

- Citrix CloudFormation テンプレートを使用して NetScaler VPX インスタンスをデプロイする場合、デフ ォルトのオプションは「はい」です。CloudWatch サービスを無効にする場合は、「いいえ」を選択します。
- メトリクスは、CPU (管理およびパケット CPU 使用率)、メモリ、およびスループット (インバウンドとアウトバウンド) で使用できます。

CloudWatch メトリクスの表示方法

インスタンスの CloudWatch メトリックスを表示するには、次の手順に従います。

- 1. AWS マネジメントコンソール > EC2 > インスタンスにログオンします。
- 2. インスタンスを選択します。
- 3. [監視]をクリックします。
- 4. [CloudWatch メトリックスをすべて表示]をクリックします。

testfarhan-PrimaryInstance	i-0bb6e330c2b51d145 ORunning	⊕ Q m5.xlarge	 Initializing 	No alarms +	us-east-1b	-
testfarhan-SecondaryInstance	i-02ad0511c02899312	⊕⊖ m5.xlarge	⊘ 2/2 checks …	No alarms +	us-east-1b	-
istance: i-0bb6e330c2b51d145 (testfarhan-Primar	vinstance)					
Details Security Networking Storag	ge Status Checks Monitoring	Tags				
	· · · · · ·					
		[Add to dashboard 1h	3h 12h 1d 3	3d 1w custom -	2
CPU utilization (%)	Status check failed (any) (count)	Status check f	ailed (instance) (cou	Status che	ck failed (syste	m) (count)
Percent	Count	Count		Count		
27	1	1		1		
13.5	0.5	0.5	_	0.5		_
07:30 07:45 08:00 08:15 08:30	07:30 07:45 08:00 08:15 08:	30 07:30 07:4	5 08:00 08:15 08:30	07:30	07:45 08:00	08:15 08:30
i-0bb6e330c2b51d145 (testfarhan-PrimaryInstar	i-0bb6e330c2b51d145 (testfarhan-PrimaryInstar	i-0bb6e330c2b51	ld145 (testfarhan-PrimaryInstar	i-Obb6e330c	2b51d145 (testfarhan	n-PrimaryInstar
Network in (bytes)	Network out (bytes)	Network pack	ets in (count)	Network p	ackets out (cou	int)
Bytes	Bytes	Count		Count		
150k	204k	473	,	478		_

5. [すべてのメトリックス] で、インスタンス ID をクリックします。

All metrics	Graphed metrics	Graph options	Source	
All >	<i-01c50c91dd353< td=""><td>7d7a> Q Search</td><td>or any metric, dimension or resource ic</td><td>d</td></i-01c50c91dd353<>	7d7a> Q Search	or any metric, dimension or resource ic	d
5 Metrics				
CPU			Memory	
2 Metrics			1 Metric	
Throughp	out			
2 Metrics				

- 6. 表示するメトリクスをクリックし、期間(分、時間、日、週、月)を設定します。
- 7. グラフ化されたメトリクスをクリックして、使用量の統計を表示します。 オプションが [はい] に 設定されています。
- 図。CPU 使用率に関するグラフ化されたメトリック

NetScaler VPX 14.1

Intitled graph 🖉	1h 3h 12h 1d	3d 1w custom (2w) - Line	- Action	S • 2 •	0
Percent						
3.7						
2.32						
0.933 04/26 04/27 04/28 04/29 04/30 05/01	05/02 05/0	3 05/04 05	/05 05/06	05/07 0	05/08 05/09	
Management CPU usage 🧧 Packet CPU usage						
All metrics Graphed metrics (2) Graph options Source						
Add a math expression 🔞		Sta	tistic: Average	 Period: 5 Mi 	nutes 🗸 🛛 Remo	ove all
Label Details			Statistic	Period	Y Axis Actions	s
Management CPU usage <	> • Mana	gement CPU usage •	Average	5 Minutes	< > 4 名	0
Packet CPU usage	> • Packe	t CPU usage • CPU:	Average	5 Minutes	< > 4	0

高可用性セットアップでの SR-IOV の設定

高可用性セットアップでの SR-IOV インターフェイスのサポートは、NetScaler リリース 12.0 57.19 以降から利用 できます。SR-IOV を構成する方法の詳細については、「SR-IOV ネットワーク インターフェイスを使用するための NetScaler VPX インスタンスの構成」を参照してください。

関連情報

AWS での高可用性の機能

異なる AWS アベイラビリティーゾーンでの高可用

October 17, 2024

独立ネットワーク構成(INC)モードでは、2つの異なるサブネットまたは2つの異なるAWSアベイラビリティーゾ ーンに2つのNetScaler ADC VPX インスタンスを高可用性アクティブ/パッシブのペアとして構成できます。何ら かの理由で1次ノードが接続を受け入れることができない場合は、2次ノードが引き継ぎます。

高可用性の詳細については、「高可用性」を参照してください。INC の詳細については、「異なるサブネットでの高可 用性ノードの設定」を参照してください。

注意事項

- 配置を開始する前に、次のドキュメントをお読みください。
 - AWS 用語
 - 前提条件
 - 制限事項と使用ガイドライン

- VPX 高可用性ペアは、異なるサブネットの同じアベイラビリティーゾーンに存在することも、2 つの異なる AWS アベイラビリティーゾーンに存在することもできます。
- 管理(NSIP)、クライアントトラフィック(VIP)、バックエンドサーバー(SNIP)には異なるサブネットを使用することをお勧めします。
- フェイルオーバーを機能させるには、独立ネットワーク構成 (INC) モードで高可用性を設定する必要があります。
- 2 つのインスタンスでは、ハートビートに使用される UDP トラフィック用にポート 3003 が開いている必要 があります。
- 残りの API が機能するように、両方のノードの管理サブネットは、内部 NAT を介してインターネットまたは AWS API サーバーにアクセスできる必要があります。
- IAM ロールには、パブリック IP または Elastic IP (EIP) 移行用の E2 アクセス権限と、プライベート IP 移行 用の EC2 ルートテーブルのアクセス許可が必要です。

次の方法で AWS アベイラビリティーゾーン間で高可用性をデプロイできます。

- エラスティック IP アドレスの使用
- プライベート IP アドレスの使用

その他の参考資料

AWS 向け NetScaler Application Delivery Management (ADM) の詳細については、「AWS に NetScaler ADM エージェントをインストールする」を参照してください。

異なる AWS ゾーンに Elastic IP アドレスを使用した VPX 高可用性ペアをデプロイす る

October 17, 2024

INC モードで Elastic IP (EIP) アドレスを使用して、2 つの異なるサブネットまたは 2 つの異なる AWS アベイラビ リティーゾーンに 2 つの NetScaler VPX インスタンスを設定できます。

高可用性の詳細については、「高可用性」を参照してください。INC の詳細については、「異なるサブネットでの高可 用性ノードの設定」を参照してください。

異なる AWS ゾーンにわたる EIP アドレスを持つ HA のしくみ

フェールオーバー時には、プライマリインスタンスの VIP の EIP がセカンダリに移行し、セカンダリが新しいプライ マリとして引き継がれます。フェイルオーバープロセスでは、AWS API は以下を行います。

1. IPSetsが接続されている仮想サーバーをチェックします。

- 2. 仮想サーバーがリッスンしている 2 つの IP アドレスから、パブリック IP が関連付けられている IP アドレス を検索します。1 つは仮想サーバに直接接続され、もう 1 つは IP セットを介して接続されます。
- 3. パブリック IP (EIP) を、新しいプライマリ VIP に属するプライベート IP に再関連付けします。
- 注

EIP を使用する際に、サービス拒否 (DoS) などの攻撃からネットワークを保護するために、AWS でセキュリティグループを作成して IP アクセスを制限できます。高可用性を実現するために、展開に従って EIP からプライベート IP 移動ソリューションに切り替えることができます。

異なる AWS ゾーン間でエラスティック IP アドレスを使用して VPX 高可用性ペアをデプロイする方法

VPX ペアを 2 つの異なるサブネットまたは 2 つの異なる AWS アベイラビリティーゾーンにデプロイする手順の概要 を以下に示します。

- 1. Amazon 仮想プライベートクラウドを作成します。
- 2. 2 つの VPX インスタンスを、2 つの異なるアベイラビリティーゾーン、または同じゾーンで異なるサブネット にデプロイします。
- 3. 高可用性の構成
 - a) 両方のインスタンスで INC モードで高可用性をセットアップします。
 - b) 両方のインスタンスに IP セット を追加します。
 - c) 両方のインスタンスの IP セットを VIP にバインドします。
 - d) プライマリ・インスタンスに仮想サーバを追加します。

ステップ1と2では、AWS コンソールを使用します。手順3では、NetScaler VPX GUI または CLI を使用しま す。

ステップ**1**。Amazon 仮想プライベートクラウド (VPC) を作成します。

ステップ **2**。2 つの異なるアベイラビリティーゾーン、または同じゾーンだが異なるサブネットに 2 つの VPX インス タンスをデプロイします。プライマリ VPX の VIP に EIP を接続します。

VPC を作成し、AWS に VPX インスタンスを展開する方法の詳細については、「AWS に NetScaler VPX スタンドア ロン インスタンスを展開する 」および「シナリオ: スタンドアロン インスタンス」を参照してください。

ステップ 3。高可用性の構成. NetScaler VPX CLI または GUI を使用して、高可用性をセットアップできます。

CLIを使用した高可用性の設定

1. 両方のインスタンスで INC モードで高可用性をセットアップします。

プライマリノードで、次の操作を行います。

add ha node 1 <sec_ip> -inc ENABLED

```
セカンダリノード:
```

add ha node 1 <prim_ip> -inc ENABLED

<sec_ip>はセカンダリノードの管理 NIC のプライベート IP アドレスを指します。

<prim_ip>はプライマリノードの管理 NIC のプライベート IP アドレスを指します

2. 両方のインスタンスに IP セットを追加します。

両方のインスタンスで以下のコマンドを入力します。

add ipset <ipsetname>

3. IP セットを両方のインスタンスの VIP セットにバインドします。

両方のインスタンスで次のコマンドを入力します。

add ns ip <secondary vip> <subnet> -type VIP

bind ipset <ipsetname> <secondary VIP>

注

IP セットは、プライマリ VIP またはセカンダリ VIP にバインドできます。ただし、IP セットをプライ マリ VIP にバインドする場合は、セカンダリ VIP を使用して仮想サーバに追加し、逆にセカンダリ VIP を使用します。

4. プライマリ・インスタンスに仮想サーバを追加します。

次のコマンドを入力します:

```
add <server_type&#062; vserver &#060;vserver_name&#062;
<protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -
ipset \\<ipset_name&#062;
```

GUIを使用した高可用性の構成

- 1. 両方のインスタンスで INC モードで高可用性をセットアップする
- 2. ユーザー名nsrootとインスタンス ID をパスワードとしてプライマリノードにログオンします。
- 3. GUIから、[設定]>[システム]>[ハイアベイラビリティ]に移動します。[追加]をクリックします。
- 4. リモートノード IP アドレスフィールドに、2次ノードの管理 NIC のプライベート IP アドレスを追加します。
- 5. [セルフノードで NIC (独立ネットワーク構成) モードをオンにする]を選択します。
- 6. [リモートシステムログイン認証情報]で、セカンダリノードのユーザー名とパスワードを追加し、[作成]を クリックします。
- 7. セカンダリノードで手順を繰り返します。

- 8. IP セット名を追加し、[Insert] をクリックします。
- 9. GUIから、[システム]>[ネットワーク]>[IP]>[追加]に移動します。
- 10. [IP アドレス]、[ネットマスク]、[IP タイプ (仮想 IP)] に必要な値を追加し、[作成] をクリックします。
- 11. システム > ネットワーク > **IP** セット > **Add** にナビゲートして下さい。**IP** セット名を追加し、[**Insert**] をク リックします。
- 12. [IPv4] ページで、仮想 IP を選択し、[挿入] をクリックします。[**Create**] をクリックして IP セットを作成し ます。
- 13. プライマリ・インスタンスに仮想サーバを追加する

GUIから、[構成]>[トラフィック管理]>[仮想サーバ]>[追加]に移動します。

```
Load Balancing Virtual Server Export as a Template
```

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

シナリオ

このシナリオでは、1 つの VPC が作成されます。その VPC では、2 つのアベイラビリティーゾーンに 2 つの VPX イ ンスタンスが作成されます。各インスタンスには、管理用、クライアント用、バックエンドサーバー用の 3 つのサブ ネットがあります。EIP はプライマリノードの VIP に接続されます。

図: この図は、AWS での INC モードでの Citrix ADC VPX の高可用性セットアップを示しています



Before failover

After failover

このシナリオでは、CLI を使用して高可用性を設定します。

```
1. 両方のインスタンスで INC モードで高可用性をセットアップします。
  プライマリノードとセカンダリノードで次のコマンドを入力します。
  プライマリ:
  add ha node 1 192.168.6.82 -inc enabled
  ここで、192.168.6.82 は、セカンダリノードの管理 NIC のプライベート IP アドレスを指します。
 セカンダリ:
  add ha node 1 192.168.1.108 -inc enabled
  ここで、192.168.1.108 は、プライマリノードの管理 NIC のプライベート IP アドレスを指します。
2. IP セットを追加し、IP セットを両方のインスタンスの VIP にバインドします。
  プライマリ:
  add ipset ipset123
  add ns ip 192.168.7.68 255.255.255.0 -type VIP
 bindipset ipset123 192.168.7.68
 セカンダリ:
  add ipset ipset123
  add ns ip 192.168.7.68 255.255.255.0 -type VIP
```

bind ipset ipset123 192.168.7.68
3. プライマリ・インスタンスに仮想サーバを追加します。

以下のコマンドを実行します。

add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123

4. 構成を保存します。

Add	Edit	Delete Statistics	Select Action \checkmark				
	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. 強制フェールオーバーの後、セカンダリは新しいプライマリになります。

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

異なる AWS ゾーンにプライベート IP アドレスを使用して VPX 高可用性ペアを展開す る

October 17, 2024

INC モードのプライベート IP アドレスを使用して、2 つの異なるサブネットまたは 2 つの異なる AWS アベイラビリ ティーゾーンで 2 つの NetScaler ADC VPX インスタンスを設定できます。このソリューションは、弾性 IP アドレ ス を備えた既存のマルチゾーン

VPX 高可用性ペアと簡単に統合できます。したがって、両方のソリューションを一緒に使用できます。

高可用性の詳細については、「高可用性」を参照してください。INC の詳細については、「異なるサブネットでの高可 用性ノードの設定」を参照してください。

注

このデプロイは、NetScaler リリース 13.0 ビルド 67.39 以降でサポートされています。このデプロイは AWS Transit Gateway と互換性があります。

AWS 非共有 VPC を使用したプライベート IP アドレスを使用した高可用性ペア

前提条件

AWS アカウントに関連付けられた IAM ロールに次の IAM アクセス権限があることを確認します。

```
1
     {
2
          "Version": "2012-10-17",
3
4
          "Statement": [
5
              {
6
7
                  "Action": [
                       "ec2:DescribeInstances",
8
                       "ec2:DescribeAddresses",
9
                       "ec2:AssociateAddress",
10
                       "ec2:DisassociateAddress",
11
                       "ec2:DescribeRouteTables",
12
                       "ec2:DeleteRoute",
13
                       "ec2:CreateRoute",
14
15
                       "ec2:ModifyNetworkInterfaceAttribute",
                       "iam:SimulatePrincipalPolicy",
16
                       "iam:GetRole"
17
18
                  ],
                  "Resource": "*",
19
                  "Effect": "Allow"
20
21
               }
23
          ]
       }
24
```

AWS 非共有 VPC を使用して、プライベート IP アドレスを持つ VPX HA ペアをデプロイする

次に、プライベート IP アドレスを使用して 2 つの異なるサブネットまたは 2 つの異なる AWS アベイラビリティー ゾーンに VPX ペアをデプロイする手順の概要を示します。

- 1. Amazon 仮想プライベートクラウドを作成します。
- 2. 2 つの異なるアベイラビリティーゾーンに 2 つの VPX インスタンスをデプロイします。
- 3. 高可用性の構成
 - a) 両方のインスタンスで INC モードで高可用性をセットアップします。
 - b) クライアントインターフェイスを指すそれぞれのルートテーブルを VPC に追加します。
 - c) プライマリ・インスタンスに仮想サーバを追加します。

ステップ 1、2、および 3b では、AWS コンソールを使用します。ステップ 3a と 3c では、NetScaler VPX GUI または CLI を使用します。

ステップ 1。Amazon 仮想プライベートクラウド (VPC) を作成します。

ステップ **2**。同じ数の ENI (ネットワーク インターフェイス) を持つ 2 つの異なるアベイラビリティ ゾーンに 2 つの VPX インスタンスをデプロイします。

VPC を作成し、AWS に VPX インスタンスを展開する方法の詳細については、「AWS に NetScaler VPX スタンドア ロン インスタンスを展開する 」および「シナリオ: スタンドアロン インスタンス」を参照してください。

ステップ **3**。 Amazon VPC サブネットと重複しないサブネットを選択して、ADC VIP アドレスを設定します。VPC が 192.168.0.0/16 の場合、ADC VIP アドレスを設定するには、次の IP アドレス範囲から任意のサブネットを選択 できます。

- 0.0.0.0-192.167.0.0
- 192.169.0.0-254.255.255.0

この例では、10.10.10.0/24 サブネットを選択し、このサブネットに VIP を作成しました。VPC サブネット以外の 任意のサブネットを選択できます (192.168.0.0/16).

ステップ **4**。 VPC ルート テーブルからプライマリ ノードのクライアント インターフェイス (VIP) を指すルートを追加します。

AWS CLI から、次のコマンドを入力します。

1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidrblock 10.10.10.0/24 --gateway-id <eni-client-primary>

AWS GUI から、次の手順を実行してルートを追加します。

- 1. Amazon EC2 コンソールを開きます。
- 2. ナビゲーションペインで、ルートテーブルを選択し、ルートテーブルを選択します。
- 3. [アクション]を選択し、[ルートの編集]をクリックします。
- ルートを追加するには、[Add route]を選択します。[宛先]に、宛先 CIDR ブロック、単一の IP アドレス、 またはプレフィックスリストの ID を入力します。ゲートウェイ ID には、プライマリノードのクライアントイ ンターフェイスの ENI を選択します。

aws Services V

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	oni 00od18f01f85/b8ob	

注

プライマリ・インスタンスのクライアント ENI で Source/Dest Check を無効にする必要があります。

コンソールを使用してネットワークインターフェイスの source/destination チェックを無効にするには、次の手順 を実行します。

- 1. Amazon EC2 コンソールを開きます。
- 2. ナビゲーションペインで、[ネットワークインターフェイス]を選択します。
- 3. プライマリクライアントインターフェイスのネットワークインターフェイスを選択し、[アクション]を選択し、[** ソース/デストを変更]をクリックします。** を確認してください。
- 4. ダイアログボックスで、[無効]を選択し、[保存]をクリックします。



ステップ 5。高可用性の構成. NetScaler VPX CLI または GUI を使用して、高可用性をセットアップできます。

CLI を使用した高可用性の設定

1. 両方のインスタンスで INC モードで高可用性をセットアップします。

プライマリノードで、次の操作を行います。

```
1 ```
2 add ha node 1 \<sec\_ip\> -inc ENABLED
3 ```
```

セカンダリノード:

```
1 ```
2 add ha node 1 \<prim\_ip\> -inc ENABLED
3 ```
```

<sec_ip> セカンダリノードの管理 NIC のプライベート IP アドレスを参照します。

<prim_ip> プライマリノードの管理 NIC のプライベート IP アドレスを参照します。

1. プライマリ・インスタンスに仮想サーバを追加します。選択したサブネット(10.10.10.0/24 など)から追加 する必要があります。

次のコマンドを入力します:

```
add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<primary
        \_vip\> \<port\>
```

GUIを使用した高可用性の構成

- 1. 両方のインスタンスで INC モードで高可用性をセットアップする
- 2. ユーザー名nsrootとインスタンス ID をパスワードとしてプライマリノードにログオンします。
- 3. [構成] > [システム] > [高可用性]に移動し、[追加]をクリックします。
- 4. リモートノード IP アドレスフィールドに、2 次ノードの管理 NIC のプライベート IP アドレスを追加します。
- 5. [セルフノードで NIC (独立ネットワーク構成) モードをオンにする]を選択します。
- 6. [リモートシステムログイン認証情報]で、セカンダリノードのユーザー名とパスワードを追加し、[作成]を クリックします。
- 7. セカンダリノードで手順を繰り返します。
- 8. プライマリ・インスタンスに仮想サーバを追加する

[設定]>[トラフィック管理]>[仮想サーバー]>[追加]に移動します。

G Load Balancing Virtual Server

My Ba Listen Priority - My Ba Listen Priority NONE My Ba Listen Policy Expression NONE Mater OP Redirection Mode IP Address 10.10.00 Range 1 My Ba OP Participation Participation Mater 0 Participation Participation My Ba None Participation Participation Mater None Participation Participation Mater None Participation Participation My Ba None Participation Participation Mater None Participation Participation	Basic Settin	gs		
	lame rotocol tate ⁹ Address ort raffic Domain	My LB HTTP • UP 10.10.10.10 80 0	Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- NONE IP 1 - PASSIVE ENABLED NO

AWS 共有 VPC を使用して、プライベート IP アドレスを持つ VPX HA ペアをデプロイする

AWS 共有 VPC モデルでは、VPC を所有するアカウント (所有者) が 1 つ以上のサブネットを他のアカウント (参加 者) と共有します。そのため、VPC 所有者アカウントと参加者アカウントがあります。サブネットが共有されると、 参加者は共有されたサブネット内のアプリケーションリソースを表示、作成、変更、および削除できます。参加者は、 他の参加者または VPC 所有者に属するリソースを表示、変更、削除することはできません。

AWS 共有 VPC の詳細については、AWS ドキュメントを参照してください。

注

AWS 共有 VPC を使用してプライベート IP アドレスで VPX HA ペアをデプロイする設定手順は、AWS 非共有 VPC を使用してプライベート IP アドレスで VPX HA ペアをデプロイする手順と同じです。

 クライアントインターフェイスを指す VPC 内のルートテーブルは、VPC 所有者アカウントから追加する 必要があります。

前提条件

• AWS 参加者アカウントの NetScaler VPX インスタンスに関連付けられている IAM ロールに次の IAM 権限が あることを確認してください。

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	}			



AssumeRole を使用すると、NetScaler VPX インスタンスは、VPC 所有者アカウントによって作成 されたクロスアカウント IAM ロールを引き継ぐことができます。

• VPC 所有者アカウントが、クロスアカウント IAM ロールを使用して、参加者アカウントに次の IAM アクセス 権限を付与していることを確認します。

1	{
2	
3	"Version": "2012-10-17",
4	"Statement": [
5	{
6	
7	"Sid": "VisualEditor0",
8	"Effect": "Allow",
9	"Action": [
10	"ec2:CreateRoute",
11	"ec2:DeleteRoute",
12	"ec2:DescribeRouteTables"
13],
14	"Resource": "*"
15	}
16	
17]
18	}

クロスアカウント IAM ロールの作成

- 1. AWS ウェブコンソールにログインします。
- 2. [IAM]タブで[ロール]に移動し、[** ロールの作成 **]を選択します。
- 3. [別の AWS アカウント]を選択します。

	AWS convice		Another AWS account		Web identity
	EC2, Lambda and others		Belonging to you or 3rd party	www	Cognito or any OpenII provider
Allows e	entities in other accounts to p	erform actio	ns in this account. Learn mo	re	

1. 管理者アクセス権を付与する参加者アカウントの12桁のアカウントID番号を入力します。

NetScaler CLI を使用してクロスアカウント IAM ロールを設定する

次のコマンドを実行すると、NetScaler VPX インスタンスが VPC 所有者アカウントに存在するクロスアカウント IAM ロールを引き継ぐことができます。

set cloud awsParam -roleARN <string>

NetScaler GUI を使用してクロスアカウント IAM ロールを設定

1. NetScaler アプライアンスにサインインし、[構成] > [AWS] > [クラウドパラメータの変更] に移動します。

Q Search Menu		AWS	2 G
Favorites	\sim	Configuration Summary	Confirmure Claud Deremeters
AWS	~	No Cloud Profile	Change Cloud Parameters
Cloud Profile			
System	>		
AppExpert	>		

1. AWS クラウドパラメータの設定ページで、RolLearn フィールドの値を入力します。

← Configure AWS Cloud Parameters

neo.rolearn

errtfvf

シナリオ

このシナリオでは、1 つの VPC が作成されます。その VPC では、2 つのアベイラビリティーゾーンに 2 つの VPX イ ンスタンスが作成されます。各インスタンスには、管理用、クライアント用、バックエンドサーバー用の 3 つのサブ ネットがあります。

次の図は、AWS 上の INC モードでの NetScaler VPX 高可用性セットアップを示しています。VPC の一部ではない カスタムサブネット 10.10.10.10 が VIP として使用されます。したがって、10.10.10.10 サブネットはアベイラビ リティーゾーン全体で使用できます。





このシナリオでは、CLI を使用して高可用性を設定します。

1. 両方のインスタンスで INC モードで高可用性をセットアップします。

プライマリノードとセカンダリノードで次のコマンドを入力します。

プライマリノードで、次の操作を行います。

1 ... 2 add ha node 1 192.168.4.10 -inc enabled

ここで、192.168.4.10 は、セカンダリノードの管理 NIC のプライベート IP アドレスを指します。

セカンダリノード:

...

1 ... 2 add ha node 1 192.168.1.10 -inc enabled 3 ...

ここで、192.168.1.10 は、プライマリノードの管理 NIC のプライベート IP アドレスを指します。

1. プライマリ・インスタンスに仮想サーバを追加します。

次のコマンドを入力します:

```
1 ```
2 add lbvserver vserver1 http 10.10.10.10 80
3 ```
```

- 1. 構成を保存します。
- 2. 強制フェールオーバーの後:
 - セカンダリインスタンスが新しいプライマリインスタンスになります。
 - プライマリ ENI を指す VPC ルートは、セカンダリクライアント ENI に移行します。
 - クライアントトラフィックは、新しいプライマリインスタンスに再開されます。

HA プライベート IP ソリューションの AWS Transit Gateway の設定

AWS Transit Gateway は、AWS VPC、リージョン、およびオンプレミスネットワーク全体で、内部ネットワーク 内でプライベート VIP サブネットをルーティング可能にする必要があります。VPC は AWS Transit Gateway に接 続する必要があります。AWS Transit Gateway ルートテーブル内の VIP サブネットまたは IP プールの静的ルート が作成され、VPC をポイントします。



AWS Transit Gateway を設定するには、次の手順に従います。

- 1. Amazon VPC コンソールを開きます。
- 2. ナビゲーションペインで、[Transit Gateway ートテーブル]を選択します。
- 3. [ルート]タブを選択し、[静的ルートの作成]をクリックします。

TRANSIT	<						
GATEWAYS	Transit Gat	eway Route Tab	le: tgw-rtb-09f12c	a61473654a7			
Transit Gateways							
Transit Gateway	Details	Associations	Propagations	Prefix list references	Routes	Tags	
Attachments	The table	below will return	a maximum of 100) routes. Narrow the filter	or use export	t routes to	to view more routes
Transit Gateway			a maximum or root	routes. Harrow the litter	or abe experi		
Route Tables	Create	static route					
Transit Gateway							
Multicast	Q Filte	er bv attributes or s	earch by keyword				$ \langle \langle 1 \text{ to } 3 \text{ of } 3 \rangle \rangle $

1. CIDR がプライベート VIPS サブネットを指し、アタッチメントが NetScaler VPX のある VPC を指す静的ル ートを作成します。

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*		θ	
Blackhole	• •		
Choose attachment	•	C	
* Required		Cancel Create static	route

1. [スタティックルートの作成]をクリックし、[閉じる]を選択します。

トラブルシューティング

マルチゾーン HA で HA プライベート IP ソリューションを設定する際に問題が発生した場合は、トラブルシューティングのために次の重要なポイントを確認してください。

- プライマリノードとセカンダリノードの両方に同じ IAM 権限セットがあります。
- INC モードは、プライマリノードとセカンダリノードの両方で有効になっています。
- プライマリノードとセカンダリノードの両方に同じ数のインターフェイスがあります。
- インスタンスを作成するときは、デバイスインデックス番号に基づいてプライマリノードとセカンダリノードの両方にインターフェイスをアタッチする同じ手順に従います。プライマリノードで、クライアントインターフェイスが最初に接続され、サーバーインターフェイスが2番目に接続されているとします。セカンダリノードでも同じ手順に従います。不一致がある場合は、正しい順序でインターフェイスを取り外して再接続します。
- インターフェイスの順序を確認するには、[AWS コンソール]>[ネットワークとセキュリティ]>[ENI]> [デバイスインデックス番号]のナビゲーションパスをたどります。デフォルトでは、これらのインターフェイ スには次のデバイスインデックス番号が割り当てられます。- 管理インターフェイス-0 - クライアントインタ ーフェイス-1-サーバーインターフェイス-2 デフォルトでは、これらのインターフェイスには次のデバイス インデックス番号が割り当てられます。
 - 管理インターフェース-0
 - クライアントインターフェース-1
 - サーバーインターフェース-2
- プライマリ ENI のデバイスインデックス番号の順序が0、1、2の場合。セカンダリ ENI も、デバイスインデックス番号と同じシーケンス(0、1、2)に従う必要があります。

デバイスインデックス番号の順序に不一致がある場合、ルートが失われないように、一致しないすべてのルートが管 理インターフェイスであるインデックス0に転送されます。ただし、管理インターフェイスへのルートの移動は、ト ラフィックの輻輳を引き起こす可能性があるため、インターフェイスを切り離してから正しい順序で接続し直す必要 があります。

- トラフィックが流れない場合は、「送信元/宛先」を確認してください。プライマリノードのクライアントイン ターフェイスで「Check」が初めて無効になります。
- cloudhadaemon コマンド (ps -aux | grep cloudha) がシェルで実行されていることを確認 します。
- NetScaler ファームウェアのバージョンが 13.0 ビルド 70.x 以降であることを確認してください。
- フェイルオーバープロセスに関する問題については、次の場所にあるログファイルを確認してください: /var/log/cloud-ha-daemon.log

AWS Outpost で NetScaler VPX インスタンスを展開する

October 17, 2024

AWS Outposts は、お客様のサイトにデプロイされている AWS のコンピューティングおよびストレージ容量のプ ールです。Outposts は、オンプレミスの場所に AWS のインフラストラクチャとサービスを提供します。AWS は AWS リージョンの一部としてこの容量を運用、監視、管理します。オンプレミスと AWS クラウドで同じ NetScaler VPX インスタンス、AWS API、ツール、およびインフラストラクチャを使用して、一貫したハイブリッドエクスペリ エンスを実現できます。

Outposts にサブネットを作成し、EC2 インスタンス、EBS ボリューム、ECS クラスター、RDS インスタンスなど の AWS リソースを作成するときに指定できます。Outposts サブネット内のインスタンスは、プライベート IP アド レスを使用して AWS リージョンの他のインスタンスと通信します。これらはすべて、同じ Amazon 仮想プライベー トクラウド(VPC)内にあります。

詳細については、AWS Outposts ユーザーガイドを参照してください。

AWS アウトポストの仕組み

AWS Outposts は、お客様のアウトポストと AWS リージョンの間で常時接続された状態で稼働するように設計さ れています。リージョンとオンプレミス環境のローカルワークロードにこの接続を実現するには、Outpost をオン プレミスネットワークに接続する必要があります。オンプレミスネットワークは、リージョンとインターネットへの WAN アクセスを提供する必要があります。また、インターネットは、オンプレミスのワークロードやアプリケーショ ンが存在するローカルネットワークへの LAN または WAN アクセスを提供する必要があります。

前提要件

- サイトに AWS Outposts をインストールする必要があります。
- AWS Outposts のコンピューティングおよびストレージ容量が使用可能である必要があります。

AWS Outposts の注文方法の詳細については、次の AWS ドキュメントを参照してください。https://aws.amaz on.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

AWS ウェブコンソールを使用して NetScaler VPX インスタンスを AWS アウトポストにデプロイする

次の図は、アウトポストへの NetScaler VPX インスタンスの簡単な展開を示しています。AWS Marketplace にあ る NetScaler AMI は、アウトポストにもデプロイされています。



AWS ウェブコンソールにログインし、次の手順を実行して、NetScaler VPX EC2 インスタンスを AWS アウトポス トにデプロイします。

- 1. キーペアを作成します。
- 2. 仮想プライベートクラウド (VPC) を作成します。
- 3. サブネットをさらに追加します。
- 4. セキュリティグループとセキュリティルールを作成します。
- 5. ルートテーブルを追加します。
- 6. インターネットゲートウェイを作成します。
- AWS EC2 サービスを使用して NetScaler VPX インスタンスを作成します。AWS EC2 サービスを使用して NetScaler VPX インスタンスを作成します。AWS ダッシュボードから、[コンピュート]>[EC2]>[インス タンスの起動]>[AWS Marketplace] に移動します。
- 8. ネットワークインターフェースをさらに作成して接続します。
- 9. エラスティック IP を管理用 NIC に接続します。
- 10. VPX インスタンスに接続します。

各手順の詳細な手順については、「AWS Web コンソールを使用して AWS に NetScaler VPX インスタンスをデプロ イする」を参照してください。

同じアベイラビリティーゾーン内での高可用性の展開については、「AWS に高可用性ペアを展開する」を参照してください。

AWS アウトポストを使用してハイブリッドクラウドに NetScaler VPX インスタンスをデプロイする

NetScaler VPX インスタンスは、AWS のアウトポストを含む AWS 環境のハイブリッドクラウドにデプロイできま す。NetScaler グローバルサーバー負荷分散(GSLB)ソリューションを使用すると、アプリ配信メカニズムを簡素 化できます。GSLB ソリューションは、AWS リージョンと AWS Outposts インフラストラクチャを使用して構築さ れたハイブリッドクラウド内の複数のデータセンターにアプリケーショントラフィックを分散します。

NetScaler GSLB は、さまざまなユースケースに対応するために、アクティブ-アクティブとアクティブ-パッシブの 両方の展開タイプをサポートしています。これらの柔軟な導入オプションとアプリケーション配信メカニズムに加え て、NetScaler は、アプリケーションが AWS Cloud にネイティブにデプロイされているか、AWS Outposts にネ イティブにデプロイされているかに関係なく、ネットワークとアプリケーションのポートフォリオ全体を保護しま す。

次の図は、AWS とのハイブリッドクラウドにおける NetScaler アプライアンスによるアプリケーション配信を示しています。



アクティブ-アクティブ展開では、NetScaler は分散環境全体でトラフィックをグローバルに誘導します。環境内の すべてのサイトは、メトリクス交換プロトコル (MEP) を通じて、リソースの可用性と状態に関するメトリックを交換 します。NetScaler アプライアンスは、この情報を使用してサイト間のトラフィックを負荷分散し、GSLB 構成で指 定された定義された方法(ラウンドロビン、最小接続、および静的近接性)によって決定された最も適切な GSLB サ イトにクライアント要求を送信します。

アクティブ-アクティブ GSLB デプロイメントは次の目的で使用できます。

- すべてのノードがアクティブな状態で、リソース使用率を最適化します。
- リクエストを個々のユーザーに最も近いサイトに誘導することで、ユーザーエクスペリエンスを向上させます。
- ユーザーが定義したペースでアプリケーションをクラウドに移行します。

アクティブ/パッシブ GSLB デプロイメントは次の用途に使用できます。

- 障害回復
- クラウドバースト

参照ドキュメント

• AWS で NetScaler ADC VPX インスタンスを展開する

- AWS ウェブコンソールを使用して NetScaler VPX インスタンスを AWS アウトポストにデプロイする
- NetScaler VPX インスタンスで GSLB を構成する

NetScaler Web App Firewall を使用して AWS API ゲートウェイを保護

October 17, 2024

NetScaler アプライアンスを AWS API Gateway の前にデプロイし、API ゲートウェイを外部の脅威から保護でき ます。NetScaler Web App Firewall (WAF) は、OWASP の上位 10 件の脅威とゼロデイ攻撃から API を保護でき ます。NetScaler Web App Firewall は、すべての ADC フォームファクターで単一のコードベースを使用します。 そのため、あらゆる環境にわたってセキュリティポリシーを一貫して適用し、適用することができます。NetScaler Web App Firewall は導入が簡単で、単一のライセンスとして利用できます。NetScaler Web App Firewall には 次の機能があります。

- 構成の簡素化
- ボットの管理
- 総合的な可視性
- 複数のソースからのデータを照合し、統一された画面にデータを表示する

API ゲートウェイ保護に加えて、他の Citrix ADC 機能も使用できます。詳しくは、NetScaler のドキュメントを参照してください。データセンターのフェイルオーバーを回避し、シャットダウン時間を最小限に抑えるだけでなく、 アベイラビリティーゾーン内またはアベイラビリティーゾーン間で ADC を高可用性に設定できます。Autoscale 機能でクラスタリングを使用または構成することもできます。

以前、AWS API Gateway は、その背後にあるアプリケーションを保護するために必要な保護をサポートしていませんでした。Web アプリケーションファイアウォール (WAF) 保護がなければ、API はセキュリティ上の脅威にさらされがちでした。

AWS API ゲートウェイの前に Citrix ADC アプライアンスをデプロイする

次の例では、NetScaler アプライアンスが AWS API ゲートウェイの前にデプロイされています。



AWS Lambda サービスに対する本物の API リクエストがあるとします。このリクエストは、Amazon API Gateway のドキュメントに記載されているどの APIサービスにも適用できます。上の図に示すように、トラフィックフローは 次のようになります。

- クライアントが AWS Lambda 関数 (XYZ) にリクエストを送信します。このクライアント要求は、Citrix ADC 仮想サーバー(192.168.1.1)に送信されます。
- 2. 仮想サーバはパケットを検査し、悪意のあるコンテンツがないかチェックします。
- Citrix ADC アプライアンスは、書き換えポリシーをトリガーして、クライアント要求のホスト名と URL を変 更します。たとえば、https://restapi.citrix.com/default/LamdaFunctionXYZ をhttps://citrix.execute-api.<region>.amazonaws.com/default /LambdaFunctionXYZに変更するとします。
- 4. NetScaler アプライアンスは、このリクエストを AWS API ゲートウェイに転送します。
- 5. AWS API Gateway はさらに Lambda サービスにリクエストを送信し、Lambda 関数「XYZ」を呼び出し ます。
- 6. 同時に、攻撃者が悪意のあるコンテンツを含む API リクエストを送信すると、その悪意のあるリクエストは Citrix ADC アプライアンスに到達します。
- 7. NetScaler ADC アプライアンスはパケットを検査し、構成されたアクションに基づいてパケットをドロップ します。

WAF を有効にして NetScaler ADC アプライアンスを構成する

NetScaler ADC アプライアンスで WAF を有効にするには、次の手順を実行します。

- 1. コンテンツスイッチまたは負荷分散仮想サーバーを追加します。仮想サーバーの IP アドレスが 192.168.1.1 で、ドメイン名(restapi.citrix.com)に解決されるとします。
- 2. NetScaler 仮想サーバーで WAF ポリシーを有効にします。詳細については、「Web App Firewall の構成」 を参照してください。

- 書き換えポリシーを有効にして、ドメイン名を変更します。たとえば、「restapi.citrix.com」ドメイン名のロ ードバランサーへの受信リクエストを、「citrix.execute-api」のバックエンド AWS API ゲートウェイに書き 換えるように変更するとします。<region>.amazonaws"ドメイン名。
- 4. Citrix ADC アプライアンスで L3 モードを有効にして、プロキシとして機能させます。次のコマンドを使用します:

1 enable ns mode L3

前の例のステップ3で、Webサイト管理者がCitrix ADC アプライアンスで「restapi.citrix.com」ドメイン名を 「citrix.execute-api」に置き換えることを望んでいるとします。<region>.amazonaws.com"と入 力し、URL に「デフォルト/ラムダ/XYZ」を付けます。

次の手順では、書き換え機能を使用してクライアント要求のホスト名と URL を変更する方法について説明します。

- 1. SSH を使用して NetScaler ADC アプライアンスにログオンします。
- 2. 書き換えアクションを追加する。

1 add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER
 (\"Host\")" "\"citrix.execute-api.<region>.amazonaws.com\""
2
3 add rewrite action rewrite_url_act replace HTTP.REQ.URL.
 PATH_AND_QUERY "\"/default/lambda/XYZ\""

3. 書き換えアクションの書き換えポリシーを追加します。

4. 書き換えポリシーを仮想サーバにバインドします。

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

詳しくは、「Citrix ADC アプライアンスのクライアント要求でホスト名と URL を変更するように書き換えを構成する」を参照してください。

NetScaler の機能と機能

NetScaler ADC アプライアンスは、展開を保護するだけでなく、ユーザーの要件に基づいて要求を強化することもできます。NetScaler ADC アプライアンスには、次の主要な機能があります。

- API ゲートウェイの負荷分散: 複数の API ゲートウェイがある場合は、Citrix ADC アプライアンスを使用して複数の API ゲートウェイを負荷分散し、API リクエストの動作を定義できます。
 - さまざまな負荷分散方式を使用できます。たとえば、Least 接続メソッドは API Gateway 制限のオー バーロードを回避し、Custom load メソッドは特定の API ゲートウェイの特定の負荷を維持するなど です。詳細については、負荷分散アルゴリズムを参照してください。
 - SSL オフロードは、トラフィックを中断することなく設定されます。
 - [送信元 IP (USIP)を使用] モードを有効にすると、クライアント IP アドレスが保持されます。
 - ユーザー定義の SSL 設定: 独自の署名証明書とアルゴリズムを使用して、独自の SSL 仮想サーバーを作 成できます。
 - バックアップ仮想サーバー:API ゲートウェイにアクセスできない場合は、追加のアクションのためにリクエストをバックアップ仮想サーバーに送信できます。
 - 他にも多くの負荷分散機能を使用できます。詳しくは、「Citrix ADC アプライアンスのトラフィックの 負荷分散」を参照してください。
- 認証、承認、監査: LDAP、SAML、RADIUS などの独自の認証方法を定義し、API リクエストの承認と監査を 行うことができます。
- レスポンダー:シャットダウン時に API リクエストを他の API Gateway にリダイレクトできます。
- レート制限:レート制限機能を設定して、API ゲートウェイの過負荷を回避できます。
- 可用性の向上: NetScaler アプライアンスを高可用性セットアップまたはクラスターセットアップで構成して、AWS API トラフィックの可用性を高めることができます。
- REST API: REST API をサポートします。REST API は、クラウド本番環境での作業の自動化に使用できます。
- データの監視:参照用にデータを監視し、ログに記録します。

NetScaler アプライアンスにはさらに多くの機能があり、AWS API ゲートウェイと統合できます。詳しくは、 NetScaler のドキュメントを参照してください。

バックエンドの AWS Autoscaling サービスを追加する

October 17, 2024

クラウドでアプリケーションを効率的にホストすると、アプリケーションの必要に応じて、リソースを簡単にコスト 効率よく管理できます。需要の増大に対応するには、ネットワークリソースをスケールアップする必要があります。 需要が収まったら、アイドル状態のリソースによる不要なコストを避けるためにスケールダウンする必要があります。 常に必要な数のインスタンスのみをデプロイすることで、アプリケーションの実行コストを最小限に抑えることがで きます。これを実現するには、トラフィック、メモリ、CPU 使用率などを常に監視する必要があります。しかし、ト ラフィックを手動で監視するのは煩雑です。アプリケーション環境を動的にスケールアップまたはスケールダウンす るには、トラフィックを監視し、必要に応じてリソースをスケールアップまたはスケールダウンするプロセスを自動 化する必要があります。

AWS Auto Scaling サービスと統合され、NetScaler VPX インスタンスには次の利点があります。

- 負荷分散と管理:需要に応じてサーバーをスケールアップおよびスケールダウンするように自動構成します。VPX インスタンスは、バックエンドサブネット内の Autoscale グループを自動検出し、ユーザーが Autoscale グループを選択して負荷を分散できるようにします。これはすべて、VPX インスタンスの仮想 IP アドレスとサブネット IP アドレスを自動構成することによって行われます。
- 高可用性: 複数のアベイラビリティーゾーンにまたがる Autoscale e グループを検出し、サーバーの負荷を分 散します。
- ネットワークの可用性の向上:VPX インスタンスは以下をサポートします。
 - VPC ピアを使用した異なる VPC のバックエンドサーバー
 - 同じプレイスメントグループのバックエンドサーバー
 - 異なるアベイラビリティゾーンのバックエンドサーバー
- 正常な接続終了: グレースフルタイムアウト機能を使用して、スケールダウンアクティビティが発生してもク ライアント接続が失われないように、Autoscale サーバーを正常に削除します。
- スタンバイサーバーの接続ドレイニング:スタンバイ状態のサーバーに新しいクライアント接続を送信しない ようにします。ただし、スタンバイサーバーはまだオートスケーリンググループの一部であり、閉じられるま で既存のクライアント接続を処理し続けます。サーバーが InService 状態に戻ると、サーバーは新しい接続の 処理を再開します。スタンバイ状態を使用して、サーバーを更新、変更、またはトラブルシューティングした り、要件に基づいてスケールダウンしたりできます。スタンバイ状態を使用して、サーバーの更新、変更、ト ラブルシューティングを行ったり、要件に基づいてスケールダウンしたりできます。詳細については、AWS のドキュメントを参照してください。

図:NetScaler VPX インスタンスによる AWS オートスケーリングサービス



この図は、AWS オートスケーリングサービスが NetScaler VPX インスタンス(負荷分散仮想サーバー)とどのよう に互換性があるかを示しています。詳しくは、次の AWS のトピックを参照してください。

- オートスケーリンググループ
- CloudWatch
- Simple Notification Service (SNS)
- シンプルキューサービス (Amazon SQS)

はじめに

NetScaler VPX インスタンスで自動スケーリングの使用を開始する前に、次のタスクを完了する必要があります。

- 次のトピックをお読みください。
 - 前提条件
 - 制限事項と使用上のガイドライン
- 要件に応じて、AWS で NetScaler VPX インスタンスを作成します。
 - NetScaler VPX スタンドアロン インスタンスの作成方法の詳細については、「AWS に NetScaler VPX スタンドアロン インスタンスをデプロイする」および「シナリオ: スタンドアロン インスタンス」を参 照してください。
 - VPX インスタンスを HA モードでデプロイする方法の詳細については、「AWS に高可用性ペアをデプロ イする」を参照してください。

注

以下をお勧めします:

- AWS 上で NetScaler VPX インスタンスを作成するには、クラウドフォーメーションテンプレートを使用してください。
- 3 つの個別のインターフェイスを作成します。1 つは管理 (NSIP) 用、もう1 つはクライアント側のLB 仮想サーバー (VIP) 用、もう1 つはサブネット IP (NSIP) 用です。
- AWS Autoscale グループを作成します。既存の自動スケーリング設定がない場合は、次のことを行う必要が あります。
 - 1. 起動設定を作成する
 - 2. Autoscaling グループの作成
 - 3. Autoscaling グループの検証

詳しくは、http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial. htmlを参照してください。 NetScaler リリース 14.1-12.x 以降、AWS Autoscale グループでは、グレースフルオプションを有効にしている場合にのみスケールダウンポリシーを指定する必要があります。NetScaler 14.1-12.x より前のリリースでは、Graceful オプションが有効かどうかに関係なく、少なくとも1つのスケールダウン ポリシーを指定する必要がありました。

NetScaler VPX インスタンスは、ステップスケーリングポリシーのみをサポートしています。簡易スケーリ ングポリシーとターゲット追跡スケーリングポリシーは、Autoscale グループではサポートされていません。

• AWS アカウントに次の IAM 権限があることを確認してください:

```
1
      {
2
3
           "Version": "2012-10-17",
4
           "Statement": \[
5
            {
6
7
                   "Action": \[
8
                        "ec2:DescribeInstances",
                        "ec2:DescribeNetworkInterfaces",
9
                        "ec2:DetachNetworkInterface",
10
                        "ec2:AttachNetworkInterface",
11
                        "ec2:StartInstances",
12
13
                        "ec2:StopInstances",
                        "ec2:RebootInstances",
14
15
                        "autoscaling:\*",
                        "sns:\*",
                        "sqs:\*"
17
18
19
                    "iam: SimulatePrincipalPolicy"
20
                    "iam: GetRole"
21
                   \],
                   "Resource": "\*",
22
23
                   "Effect": "Allow"
24
                }
25
26
           1
27
        }
```

AWS 自動スケーリングサービスを NetScaler VPX インスタンスに追加する

次の手順を実行して、自動スケーリングサービスを VPX インスタンスに追加します:

- 1. nsrootの認証情報を使用して VPX インスタンスにログオンします。
- [システム]>[AWS]>[クラウドプロファイル]に移動し、[追加]をクリックします。
 クラウドプロファイルの作成設定ページが表示されます。

← Create Cloud Profile

Name	
test-cloudprofile	
Virtual Server IP Address*	
	\checkmark
Load Balancing Server Protocol	
HTTP	\checkmark
Load Balancing Server Port	
80	
Auto Scale Group	
test-script	
Auto Scale Group Protocol	
НТТР	\sim
Auto Scale Group Port	
80	
Select this option to drain the conne	tions gracefully. Else the connections will be dronped in the event of scale dow
Graceful	
Delay (Seconds)	

クラウドプロファイルを作成する際の注意点:

- 仮想サーバーの IP アドレスは、VPX インスタンスで使用可能な空き IP アドレスから自動入力されます。
 詳細については、「複数の IP アドレスの管理」を参照してください。
- AWS アカウントで設定した Autoscale グループの正確な名前を入力します。詳細については、「AWS Auto Scaling グループ」を参照してください。
- オートスケーリンググループのプロトコルとポートを選択する際には、サーバーがそれらのプロトコル とポートでリッスンしていることを確認し、サービスグループに正しいモニターをバインドしてくださ い。デフォルトでは、TCP モニターが使用されます。
- SSL プロトコルタイプの自動スケーリングでは、クラウドプロファイルを作成した後、証明書がないために負荷分散仮想サーバーまたはサービスグループがダウンしているように見えます。証明書は、仮想サーバまたはサービスグループに手動でバインドできます。
- Autoscale e サーバーを正常に削除するには、「Graceful」を選択し、「Delay」フィールドにタイム アウト値を指定します。このオプションはスケールダウンイベントを開始します。VPX インスタンスは サーバーをすぐには削除しませんが、サーバーの1つを正常に削除するようにマークします。この間、 VPX インスタンスはこのサーバーへの新規接続を許可しません。既存の接続は、タイムアウトが発生す るまで処理されます。タイムアウト後、VPX インスタンスはサーバーを削除します。

Graceful オプションを選択しない場合、負荷が下がった直後に Autoscale グループのサーバーが削除 されます。これにより、接続されている既存のクライアントのサービスが中断される可能性があります。

クラウドプロファイルを作成すると、NetScaler 負荷分散仮想サーバーと、自動スケーリンググループのサーバーと してメンバーを含むサービスグループが作成されます。バックエンドサーバーは、VPX インスタンスで構成された

SNIP を介して到達可能である必要があります。

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

- AWS コンソールでオートスケール関連の情報を表示するには、[**EC2]>[ダッシュボード]>[自動ス ケーリング]>[Auto Scaling Group]に移動します。
- AWSの同じAutoScaling Group (ASG)を使用して、サービスごとに (異なるポートを使用して) 異なるクラウドプロファイルを作成できます。したがって、NetScaler VPX インスタンスは、パブリッククラウド内の同じ自動スケーリンググループを持つ複数のサービスをサポートします。

NetScaler GSLB を AWS に展開

April 1, 2025

GSLB for NetScaler on AWS を設定するには、基本的に、NetScaler が属する VPC の外部にあるサーバー(別の アベイラビリティリージョンの別の VPC 内やオンプレミスのデータセンターなど)にトラフィックを負荷分散する ように NetScaler を構成する必要があります。



DBSの概要

クラウド ロード バランサー用のドメイン名ベース サービス (DBS) を使用した NetScaler GSLB サポートにより、 クラウド ロード バランサー ソリューションを使用して動的なクラウド サービスを自動検出できるようになります。 この構成により、NetScaler はアクティブ/アクティブ環境でグローバル サーバー負荷分散ドメイン名ベース サービ ス (GSLB DBS) を実装できます。DBS では、DNS 検出から AWS 環境のバックエンドリソースを拡張できます。

このセクションでは、AWS AutoScaling 環境における NetScaler 間の統合について説明します。このドキュメントの最後のセクションでは、AWS リージョンに固有の 2 つの異なる可用性ゾーン(AZ)にまたがる NetScaler ADCの HA ペアを設定する機能について詳しく説明します。

DBS と ELB

GSLB DBS は、ユーザー Elastic Load Balancer (ELB) の FQDN を利用して、AWS 内で作成および削除されるバ ックエンドサーバーを含むように GSLB サービスグループを動的に更新します。AWS のバックエンドサーバーまた はインスタンスは、ネットワーク需要または CPU 使用率に基づいてスケーリングするように設定できます。この 機能を構成するには、NetScaler を ELB にポイントして、AWS 内でインスタンスが作成および削除されるたびに NetScaler を手動で更新しなくても、AWS 内のさまざまなサーバーに動的にルーティングできます。GSLB サービ ス グループの NetScaler DBS 機能は、DNS 対応のサービス検出を使用して、Autoscale グループで識別された DBS 名前空間のメンバー サービス リソースを決定します。





AWS コンポーネントの設定

セキュリティグループ

注

ELB、NetScaler GSLB インスタンス、Linux インスタンスには、それぞれ必要なルールセットが異なるため、

異なるセキュリティグループを作成することをお勧めします。この例では、簡潔にするために、統合セキュリティグループ設定があります。

仮想ファイアウォールが適切に構成されていることを確認するには、「VPC のセキュリティ グループ」を参照してく ださい。

- 1. ユーザー AWS リソースグループにログインし、[EC2]>[ネットワークとセキュリティ]>[セキュリティグ ループ] に移動します。
- 2. [セキュリティグループの作成] をクリックし、名前と説明を入力します。このセキュリティグループには、 NetScaler と Linux のバックエンド Web サーバーが含まれます。
- 3. 次のスクリーンショットから受信ポートルールを追加します。

注

きめ細かなセキュリティ強化には、ソース IP アクセスを制限することが推奨されます。詳細については、「Web サーバー ルール」を参照してください。

- 1. Amazon Linux バックエンドウェブサービス
 - a) ユーザー AWS リソースグループにログインし、[EC2] > [インスタンス] に移動します。
 - b) 以下の詳細を使用して [インスタンスを起動] をクリック し、Amazon Linux インスタンスを設定します。

このインスタンスでの Web サーバーまたはバックエンド サービスの設定に関する詳細を入力します。

- 2. NetScaler の構成
 - a) ユーザー AWS リソースグループにログインし、[EC2] > [インスタンス] に移動します。
 - b) [Launch Instance] をクリックし、次の詳細を使用して Amazon AMI インスタンスを設定します。

3. エラスティック IP 設定

注

NetScaler は、NSIP 用のパブリック IP を持たないことで、コストを削減するために必要に応じて単一の Elastic IP で実行することもできます。代わりに、GSLB サイト IP と ADNS IP に加えて、ボックスへの管理 アクセスをカバーできる Elastic IP を SNIP に添付します。

 ユーザー**AWS リソースグループにログインし**、[**EC2] > [ネットワー クとセキュリティ] > [Elastic IP**] に移動します。
 Elastic IP アドレスを作成するには、[**新しいアドレスの割り当て**] をクリックします。
 AWS内でNetScalerインスタンスを実行しているユーザーを指すように Elastic IPを設定します。 6

- 2つ目のElastic IPを構成し、NetScalerインスタンスを実行しているユー ザーに再度割り当てます。
- 1. エラスティックロードバランサー
 - a) ユーザー AWS リソースグループにログインし、[EC2] > [負荷分散] > [ロードバランサー] に移動しま す。
 - b) [Create Load Balancer] をクリックして、クラシックロードバランサーを設定します。

ユーザー Elastic Load Balancers を使用すると、ユーザーはバックエンド Amazon Linux インスタンスの 負荷を分散できると同時に、需要に基づいてスピンアップされる他のインスタンスの負荷を分散することもで きます。

グローバルサーバー負荷分散ドメイン名ベースのサービスの設定

トラフィック管理の構成については、「NetScaler GSLB ドメインベース サービスの構成」を参照してください。

デプロイメントの種類

- 3 つの NIC の展開
 - ・ 典型的な展開
 - GSLB StyleBook
 - ADM と
 - GSLB (ドメイン登録ありの Route53)
 - ライセンス-プール/マーケットプレイス
 - 使用例
 - 3 つの NIC の展開は、データと管理トラフィックの実際の分離を実現するために使用されます。
 - 3 つの NIC を導入すると、ADC のスケールとパフォーマンスも向上します。
 - 3 つの NIC の展開は、スループットが通常 1 Gbps 以上であるネットワーク アプリケーションで使用され、3 つの NIC の展開が推奨されます。

CFT デプロイメント

お客様は、デプロイをカスタマイズする場合や、デプロイを自動化する場合、CloudFormation テンプレートを使 用してデプロイします。

展開手順

展開手順は次のとおりです。

- 1. GSLB 用の 3 つの NIC デプロイメント
- 2. ライセンス
- 3. 展開オプション

GSLB 用の 3 つの NIC デプロイメント NetScaler VPX インスタンスは、AWS Marketplace では Amazon マシ ンイメージ (AMI) として入手でき、AWS VPC 内のエラスティックコンピューティングクラウド (EC2) インスタン スとして起動できます。NetScaler VPX でサポートされる AMI として許可されている最小 EC2 インスタンスタイプ は m4.large です。NetScaler VPX AMI インスタンスには、最低 2 つの仮想 CPU と 2 GB のメモリが必要です。ま た、AWS VPC 内で起動される EC2 インスタンスは、複数のインターフェイス、インターフェイスごとに複数の IP アドレス、VPX 構成に必要なパブリックおよびプライベート IP アドレスも提供できます。各 VPX インスタンスには、 少なくとも 3 つの IP サブネットが必要です。

- 管理サブネット
- クライアント側サブネット (VIP)
- バックエンド向けサブネット (SNIP)

NetScaler では、AWS に標準 VPX インスタンスをインストールする場合、3 つのネットワークインターフェイスを 推奨しています。

現在、AWS では、AWS VPC 内で実行しているインスタンスでのみ、マルチ IP 機能を使用できます。VPC 内の VPX インスタンスを使用して、EC2 インスタンスで実行しているサーバーの負荷を分散できます。Amazon VPC を使用 すると、ユーザーは、独自の IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどの仮想 ネットワーク環境を作成および制御できます。

注

デフォルトでは、ユーザーは AWS アカウントごとに AWS リージョンごとに最大 5 つの VPC インスタンスを 作成できます。ユーザーは、Amazon のリクエストフォーム「Amazon VPC リクエスト」を送信することで、 VPC 制限の引き上げをリクエストできます。

ライセンス AWS 上の NetScaler VPX インスタンスにはライセンスが必要です。AWS で実行されている NetScaler VPX インスタンスでは、次のライセンスオプションを使用できます。

- 無料 (無制限)
- 毎時
- 年次
- 自分のライセンスを持参する
- ・ 無料トライアル(すべての NetScaler VPX-AWS サブスクリプションは、AWS Marketplace で 21 日間無料)。

展開オプション ユーザーは、AWS 上に NetScaler VPX スタンドアロンインスタンスを展開できます。ユーザー は NetScaler VPX スタンドアロンインスタンスを AWS にデプロイできます。詳しくは、「NetScaler VPX スタン ドアロンインスタンスを AWS にデプロイする」を参照してください

ハイブリッドおよびマルチクラウド展開向けの NetScaler グローバル サーバー負荷分散

NetScaler ハイブリッドおよびマルチクラウドのグローバルサーバー負荷分散(GSLB)ソリューションにより、ユ ーザーはハイブリッドクラウド、複数のクラウド、およびオンプレミス展開の複数のデータセンターにアプリケーシ ョントラフィックを分散できます。NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションにより、 ユーザーは既存の設定を変更することなく、ハイブリッドまたはマルチクラウド環境で負荷分散設定を管理できます。 また、ユーザーがオンプレミス環境を使用している場合は、クラウドに完全に移行する前に、NetScaler ハイブリッ ドおよびマルチクラウドの GSLB ソリューションを使用して一部のサービスをクラウドでテストできます。たとえ ば、ユーザーはトラフィックのごく一部しかクラウドにルーティングできず、トラフィックのほとんどをオンプレミ スで処理できます。また、NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションにより、ユーザー は地理的に離れた場所にある NetScaler インスタンスを単一の統合コンソールから管理および監視できます。

ハイブリッドおよびマルチクラウドアーキテクチャは、「ベンダーロックイン」を回避し、さまざまなインフラストラ クチャを使用してユーザーパートナーや顧客のニーズを満たすことで、企業全体のパフォーマンスを向上させること もできます。マルチクラウド アーキテクチャにより、ユーザーは使用した分だけ支払うことになるため、インフラス トラクチャ コストをより適切に管理できます。また、オンデマンドでインフラストラクチャを使用するようになった ため、ユーザーはアプリケーションをより適切に拡張できます。また、クラウド間ですばやく切り替えて、各プロバ イダーの最高のサービスを活用することもできます。

NetScaler GSLB ノードは DNS 名の解決を処理します。これらの GSLB ノードはいずれも、任意のクライアントロ ケーションから DNS リクエストを受信できます。DNS リクエストを受信する GSLB ノードは、設定された負荷分散 方法で選択されたロードバランサー仮想サーバーの IP アドレスを返します。メトリクス(サイト、ネットワーク、お よびパーシスタンスメトリック)は、独自の NetScaler プロトコルであるメトリック交換プロトコル(MEP)を使 用して GSLB ノード間で交換されます。MEP プロトコルの詳細については、「メトリック交換プロトコルの構成」を 参照してください。

GSLB ノードに設定されたモニターは、同じデータセンター内の負荷分散仮想サーバーのヘルスステータスを監視し ます。親子トポロジでは、GSLB ノードと NetScaler ノード間のメトリックは MEP を使用して交換されます。ただ し、親子トポロジーでは、GSLB と NetScaler LB ノード間のモニタープローブの構成はオプションです。

NetScaler エージェントは、NetScaler ADM とユーザー データセンター内の管理対象インスタンス間の通信を可能 にします。NetScaler エージェントとそのインストール方法の詳細については、「はじめに」を参照してください。

注

このドキュメントでは、次の前提条件を定めています。

- ユーザーが既存の負荷分散設定を持っている場合は、起動して実行中です。
- SNIP アドレスまたは GSLB サイトの IP アドレスは、NetScaler GSLB ノードごとに構成されていま

す。この IP アドレスは、他のデータセンターとメトリックスを交換するときに、データセンターのソー ス IP アドレスとして使用されます。

- 各 NetScaler GSLB インスタンスには、DNS トラフィックを受信するように ADNS または ADNS-TCP サービスが構成されています。
- 必要なファイアウォールとセキュリティグループは、クラウドサービスプロバイダーで設定されます。

セキュリティグループの設定

ユーザーは、クラウドサービスプロバイダーで必要なファイアウォール/セキュリティグループ構成を設定 する必要があります。AWS セキュリティ機能の詳細については、AWS/Documentation/Amazon VPC/User Guide/Securityを参照してください。

また、GSLB ノードでは、ユーザーは MEP トラフィック交換用の ADNS サービス/DNS サーバーの IP アドレス用 にポート 53 を開き、GSLB サイトの IP アドレス用にポート 3009 を開く必要があります。負荷分散ノードでは、ユ ーザーはアプリケーショントラフィックを受信するために適切なポートを開く必要があります。たとえば、ユーザー は HTTP トラフィックを受信するためにポート 80 を開き、HTTPS トラフィックを受信するためにポート 443 を開 く必要があります。NetScaler エージェントと NetScaler ADM 間の NITRO 通信用にポート 443 を開きます。

動的ラウンドトリップタイム GSLB 方式では、ユーザーはポート 53 を開いて、設定されている LDNS プローブタイ プに応じて UDP および TCP プローブを許可する必要があります。UDP または TCP プローブは SNIP の 1 つを使 用して開始されるため、この設定はサーバー側のサブネットにバインドされたセキュリティグループに対して行う必 要があります。

NetScaler ハイブリッドおよびマルチクラウド GSLB ソリューションの機能

このセクションでは、NetScaler ハイブリッドおよびマルチクラウド GSLB ソリューションの機能の一部について 説明します。

他の負荷分散ソリューションとの互換性

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは、NetScaler ロードバランサー、NGINX、 HAProxy、その他のサードパーティ製ロードバランサーなど、さまざまな負荷分散ソリューションをサポートしてい ます。

注

NetScaler 以外の負荷分散ソリューションは、近接ベースおよび非メトリックベースの GSLB メソッドが使用 され、親子トポロジが構成されていない場合にのみサポートされます。

GSLB の方式

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは、以下の GSLB メソッドをサポートして います。

- メトリックベースの GSLB メソッド。メトリックベースの GSLB メソッドは、メトリック交換プロトコルを 介して他の NetScaler ノードからメトリックを収集します。
 - 最小接続: クライアント要求は、アクティブな接続数が最も少ないロードバランサーにルーティングされます。
 - 最小帯域幅: クライアント要求は、現在最も少ない量のトラフィックを処理しているロードバランサーに ルーティングされます。
 - -
- 非メトリックベースの GSLB メソッド
 - ラウンドロビン: クライアントリクエストは、ロードバランサーのリストの上部にあるロードバランサーのIP アドレスにルーティングされます。その後、そのロードバランサーはリストの一番下に移動します。
 - ソース IP ハッシュ: このメソッドは、クライアント IP アドレスのハッシュ値を使用してロードバランサーを選択します。
- 近接ベースの GSLB メソッド
 - 静的近接: クライアントリクエストは、クライアント IP アドレスに最も近いロードバランサーにルーティングされます。
 - ラウンドトリップ時間 (RTT): この方法では、RTT 値 (クライアントのローカル DNS サーバーとデータ センター間の接続における遅延時間)を使用して、最もパフォーマンスの高いロードバランサーの IP ア ドレスを選択します。

負荷分散方法の詳細については、「負荷分散アルゴリズム」を参照してください。

GSLB トポロジ

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは、アクティブ/パッシブトポロジーと親子 トポロジーをサポートします。

アクティブ/パッシブトポロジ:障害点からの保護により、災害復旧を実現し、アプリケーションの継続的な可用性を確保します。プライマリデータセンターがダウンすると、パッシブデータセンターは運用可能になります。GSLB アクティブ/パッシブトポロジの詳細については、「災害復旧用の GSLB の構成」を参照してください。

親子トポロジー顧客がメトリックベースの GSLB 方式を使用して GSLB および負荷分散ノードを構成しており、負荷分散ノードが別の NetScaler インスタンスに展開されている場合に使用できます。親子トポロジでは、LB ノード(子サイト)は NetScaler アプライアンスである必要があります。親サイトと子サイト間のメトリックの交換はメトリック交換プロトコル(MEP)を介して行われます。

親子トポロジの詳細については、「MEP プロトコルを使用した親子トポロジの展開」を参照してください。

IPv6 サポート

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは IPv6 もサポートしています。

監視

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは、安全な接続を有効にするオプションを 備えた組み込みモニターをサポートしています。ただし、LB 構成と GSLB 構成が同じ NetScaler インスタンス上に ある場合、または親子トポロジーが使用されている場合、モニターの構成は任意です。

永続性

NetScaler のハイブリッドおよびマルチクラウド GSLB ソリューションは以下をサポートします:

- ソース IP ベースの永続性セッション。これにより、設定されたタイムアウトウィンドウ内に到達した場合に、 同じクライアントからの複数の要求が同じサービスに送信されます。クライアントが別の要求を送信する前に タイムアウト値が期限切れになると、セッションは破棄され、構成された負荷分散アルゴリズムを使用して、 クライアントの次の要求に対して新しいサーバーが選択されます。
- プライマリへの負荷がしきい値を下回った後も、バックアップ仮想サーバは受信した要求を処理し続けます。
 詳細については、「スピルオーバーの構成」を参照してください。
- サイトパーシステンスにより、GSLB ノードがクライアントリクエストを処理するデータセンターを選択し、 選択したデータセンターの IP アドレスを以降のすべての DNS リクエストに転送します。構成された永続性が ダウンしているサイトに適用される場合、GSLB ノードは GSLB メソッドを使用して新しいサイトを選択し、 新しいサイトはクライアントからのその後の要求に対して永続的になります。

NetScaler ADM スタイルブックを使用した構成

お客様は、NetScaler ADM 上のデフォルトのマルチクラウド GSLB スタイルブックを使用して、ハイブリッドおよ びマルチクラウド GSLB 構成で NetScaler インスタンスを構成できます。

お客様は、ロード バランシング ノード スタイルブックのデフォルトのマルチクラウド GSLB スタイルブックを使用 して、アプリケーション トラフィックを処理する親子トポロジ内の子サイトである NetScaler ロード バランシング ノードを構成できます。このスタイルブックは、ユーザーが親子トポロジで負荷分散ノードを構成する場合にのみ使 用してください。ただし、各 LB ノードは、この StyleBook を使用して個別に設定する必要があります。

NetScaler ハイブリッドおよびマルチクラウド GSLB ソリューション構成のワークフロー

お客様は、NetScaler ADM に同梱されているマルチクラウド GSLB スタイルブックを使用して、ハイブリッドおよ びマルチクラウド GSLB 構成で NetScaler インスタンスを構成できます。

次の図は、NetScaler ハイブリッドおよびマルチクラウド GSLB ソリューションを構成するためのワークフローを 示しています。ワークフロー図の手順については、図の後で詳しく説明します。



クラウド管理者として次のタスクを実行します:

1. NetScaler ラウドアカウントにサインアップしてください。

NetScaler ADM の使用を開始するには、NetScaler Cloud 企業アカウントを作成するか、社内の誰かが作成した既存のアカウントに参加します。

- 2. ユーザーが NetScaler Cloud にログオンした後、**NetScaler** アプリケーション配信管理 タイルの 「管理 **」をクリック して、ADM サービスを初めて設定します。
- 3. 複数の NetScaler ADM サービス エージェントをダウンロードしてインストールします。

NetScaler ADM とデータセンターまたはクラウド内の管理対象インスタンス間の通信を可能にするには、ユ ーザーはネットワーク環境に NetScaler ADM サービス エージェントをインストールして構成する必要があ ります。各リージョンにエージェントをインストールして、管理対象インスタンスで LB と GSLB の設定を構 成できるようにします。LB 構成と GSLB 構成では、1 つのエージェントを共有できます。上記の 3 つのタス クの詳細については、「はじめに」を参照してください。 4. Microsoft AWS クラウド/オンプレミスのデータセンターにロードバランサーをデプロイします。

ユーザーがクラウドとオンプレミスにデプロイするロードバランサーのタイプに応じて、それに応じてプロビ ジョニングします。たとえば、ユーザーは Amazon Web Services (AWS) の仮想プライベートクラウドと オンプレミスのデータセンターに NetScaler VPX インスタンスをプロビジョニングできます。仮想マシンを 作成して他のリソースを構成することにより、NetScaler インスタンスがスタンドアロンモードで LB または GSLB ノードとして機能するように構成します。NetScaler VPX インスタンスを展開する方法の詳細につい ては、次のドキュメントを参照してください:

- AWS 上の NetScaler VPX。
- NetScaler VPX スタンドアロンインスタンスを構成します。
- 5. セキュリティ設定を実行します。

ARM と AWS でネットワークセキュリティグループとネットワーク ACL を設定し、ユーザーインスタンスと サブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御します。

6. NetScaler ADM に NetScaler インスタンスを追加します。

NetScaler インスタンスは、ユーザーが NetScaler ADM から検出、管理、監視するネットワーク アプライ アンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するには、ユーザーはインス タンスをサービスに追加し、LB(ユーザーが NetScaler for LB を使用している場合)と GSLB インスタンス の両方を登録する必要があります。NetScaler ADM に NetScaler インスタンスを追加する方法の詳細につ いては、「はじめに」を参照してください。

- 7. デフォルトの NetScaler ADM スタイルブックを使用して、GSLB および LB 構成を実装します。
 - マルチクラウド GSLB StyleBook を使用して、選択した GSLB NetScaler インスタンスで GSLB 構成を実行します。
 - 負荷分散設定を実装します。(管理対象インスタンスにすでに LB 構成がある場合は、この手順をスキップできます。) ユーザーは、次の2つの方法のいずれかで NetScaler インスタンスにロード バランサーを構成できます。
 - アプリケーションの負荷分散のためにインスタンスを手動で設定します。インスタンスを手動で構成する方法の詳細については、「基本的な負荷分散の設定」を参照してください。
 - StyleBook を使用してください。ユーザーは、NetScaler ADM スタイルブック (HTTP/SSL ロード バ ランシング スタイルブックまたは HTTP/SSL ロード バランシング (モニター付き) スタイルブック) の いずれかを使用して、選択した NetScaler インスタンスにロード バランサー構成を作成できます。ユ ーザーは独自の StyleBook を作成することもできます。StyleBook について詳しくは、「StyleBook」 を参照してください。
- 8. 次のいずれかの場合に GSLB 親子トポロジを構成するには、LB ノード用のマルチクラウド GSLB スタイルブ ックを使用します。
- ユーザーがメトリックベースの GSLB アルゴリズム (最小パケット、最小接続、最小帯域幅)を使用して GSLB および負荷分散ノードを構成しており、負荷分散ノードが別の NetScaler インスタンスに展開 されている場合。
- サイトの永続性が必要な場合。

StyleBooks を使用して NetScaler 負荷分散ノードで GSLB を構成する

メトリックベースの GSLB アルゴリズム (最小パケット、最小接続、最小帯域幅) を使用して GSLB および負荷分散 ノードを構成しており、負荷分散ノードが別の NetScaler インスタンスに展開されている場合、お客様は LB ノード 用のマルチクラウド GSLB スタイルブックを使用できます。

ユーザーはこの StyleBook を使用して、既存の親サイトに対してさらに多くの子サイトを構成することもできます。 この StyleBook は、一度に1つの子サイトを構成します。したがって、この StyleBook から子サイトと同じ数の 構成(構成パック)を作成します。StyleBook は子サイトに GSLB 設定を適用します。ユーザーは最大 1024 の子 サイトを構成できます。

マルチクラウド GSLB StyleBook を使用して親サイトを構成します。

この StyleBook では、次の前提条件があります:

- SNIP アドレスまたは GSLB サイトの IP アドレスが設定されています。
- 必要なファイアウォールとセキュリティグループは、クラウドサービスプロバイダーで設定されます。
- LB ノード用のマルチクラウド GSLB スタイルブックを使用して親子トポロジで子サイトを構成する
 - 1. アプリケーション>構成>新規作成に移動します。
 - 2. [アプリケーション] > [構成] に移動し、[新規作成] をクリック します。

StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザー・インタフ ェース・ページとして表示されます。

このドキュメントでは、データセンターとサイトという用語は同じ意味で使用されています。

- 1. 次のパラメーターを設定します:
 - アプリケーション名。子サイトを作成する GSLB サイトにデプロイされている GSLB アプリケーションの名前を入力します。
 - プロトコル。ドロップダウンリストボックスから、デプロイされたアプリケーションのアプリケーションプロトコルを選択します。

注

注

- **LB** ヘルスチェック (オプション)
- ヘルスチェックの種類。ドロップダウンリストボックスから、サイト上のアプリケーションを表すロードバランサー VIP アドレスの正常性のチェックに使用するプローブのタイプを選択します。
- セキュアモード。(オプション) SSL ベースのヘルスチェックが必要な場合は、[はい]を選択してこのパ ラメーターを有効にします。
- HTTP リクエスト。(オプション) ユーザがヘルスチェックタイプとして HTTP を選択した場合は、VIP アドレスのプローブに使用される完全な HTTP 要求を入力します。
- HTTP ステータス応答コードのリスト。(オプション) ユーザがヘルスチェックタイプとして HTTP を 選択した場合は、VIP が正常であるときに HTTP 要求への応答で予想される HTTP ステータスコード のリストを入力します。
- 2. 親サイトを構成します。
 - 子サイト(LB ノード)を作成する親サイト(GSLB ノード)の詳細を指定します。
 - サイト名。サイトの名前を入力します。
 - サイト IP アドレス。親サイトが他のサイトとメトリックを交換するときにソース IP アドレスとして使用する IP アドレスを入力します。この IP アドレスは、各サイトの GSLB ノードですでに設定されていることを前提としています。
 - サイトのパブリック IP アドレス。(オプション) メトリックの交換に使用される子サイトのパブリック IP アドレスを入力します (そのサイトの IP アドレスが NAT の場合)。
- 3. 子サイトを構成します。
 - 子サイトの詳細を入力します。
 - サイト名。親サイトの名前を入力します。
 - サイト IP アドレス。子サイトの IP アドレスを入力します。ここでは、子サイトとして構成されて いる NetScaler ノードのプライベート IP アドレスまたは SNIP を使用します。
 - サイトのパブリック IP アドレス。(オプション) メトリックの交換に使用される親サイトのパブリック IP アドレスを入力します (そのサイトの IP アドレスが NAT の場合)。
- 4. アクティブな GSLB サービスの設定 (オプション)
 - LB 仮想サーバーの IP アドレスがパブリック IP アドレスでない場合にのみ、アクティブな GSLB サービスを構成します。このセクションでは、ユーザーがアプリケーションがデプロイされているサイトのローカル GSLB サービスのリストを設定できます。
 - サービス IP。このサイトの負荷分散仮想サーバーの IP アドレスを入力します。
 - サービスのパブリック IP アドレス。仮想 IP アドレスがプライベートで、パブリック IP アドレス
 が NAT に設定されている場合は、パブリック IP アドレスを指定します。

- サービスポート。このサイトの GSLB サービスのポートを入力します。
- サイト名。GSLB サービスがあるサイトの名前を入力します。
- 5.「ターゲットインスタンス」をクリック し、GSLB 構成を展開する各サイトの GSLB インスタンスとして構成 された NetScaler インスタンスを選択します。
- 6.「作成」をクリックして、選択した NetScaler インスタンス(LB ノード)にLB構成を作成します。ユーザーは、[ドライラン]をクリックして、ターゲットインスタンスに作成されるオブジェクトを確認することもできます。ユーザーが作成した StyleBook 構成は、構成ページの構成リストに表示されます。ユーザーは、NetScaler ADM GUI を使用してこの構成を確認、更新、または削除できます。

CloudFormation テンプレートの展開

NetScaler VPX は、AWS Marketplace で Amazon マシンイメージ (AMI) として入手できます。CloudFormation テンプレートを使用して AWS で NetScaler VPX をプロビジョニングする前に、AWS ユーザーは条件に同意し、 AWS Marketplace 製品に登録する必要があります。マーケットプレイスで販売されている NetScaler VPX の各エ ディションでは、この手順が必要です。

CloudFormation リポジトリ内の各テンプレートには、テンプレートの使用法とアーキテクチャを説明するドキュ メントが併置されています。テンプレートは、NetScaler VPX の推奨される展開アーキテクチャを体系化したり、ユ ーザーに NetScaler を紹介したり、特定の機能、エディション、またはオプションをデモンストレーションしたりす ることを目的としています。ユーザーは、特定の制作およびテストのニーズに合わせてテンプレートを再利用、変更、 または拡張できます。ほとんどのテンプレートには、IAM ロールを作成する権限に加えて、完全な EC2 権限が必要で す。

CloudFormation テンプレートには、NetScaler VPX の特定のリリース(リリース 12.0-56.20 など)とエディション(たとえば、NetScaler VPX プラチナエディション-10 Mbps)または NetScaler BYOL に固有の AMI ID が含まれています。CloudFormation テンプレートで別のバージョン/エディションの NetScaler VPX を使用するには、ユーザーがテンプレートを編集して AMI ID を置き換える必要があります。

最新の NetScaler AWS-AMI-ID はここにあります: NetScaler AWS CloudFormation マスター。

CFT スリー NIC デプロイメント

このテンプレートは、2 つの可用性ゾーンに3 つのサブネット(管理、クライアント、サーバー)を持つ VPC をデプ ロイします。パブリックサブネットにデフォルトルートを持つインターネットゲートウェイをデプロイします。また、 このテンプレートは、NetScaler の2 つのインスタンスを持つ可用性ゾーン間で HA ペアを作成します。プライマリ の3 つの VPC サブネット(管理、クライアント、サーバー)に関連付けられた3 つの ENI と、セカンダリの3 つの VPC サブネット(管理、クライアント、サーバー)に関連付けられた3 つの ENI です。この CFT によって作成され るすべてのリソース名には、スタック名の tagName が接頭辞として付けられます。

CloudFormation テンプレートの出力には以下が含まれます。

- primaryCitrixADCManagementURL-プライマリ VPX の管理 GUI への HTTPS URL(自己署名証明書を 使用)
- PrimaryCitrixADCManagementUrl2-プライマリ VPX の管理 GUI への HTTP URL
- primaryCitrixADCInstanceId-新しく作成されたプライマリ VPX インスタンスのインスタンス ID
- primaryCitrixADCPublicVIP-VIP に関連付けられているプライマリ VPX インスタンスの Elastic IP アドレス
- PrimaryCitrixADCPrivateNSIP-プライマリ VPX の管理に使用されるプライベート IP (NS IP)
- PrimaryCitrixADCPublicNSIP-プライマリ VPX の管理に使用されるパブリック IP (NS IP)
- PrimaryCitrixADCPrivateVIP-VIP に関連付けられているプライマリ VPX インスタンスのプライベート IP アドレス
- PrimaryCitrixADCSnip-SNIP に関連付けられているプライマリ VPX インスタンスのプライベート IP アドレス
- SecondaryCitrixADCManagementURL-セカンダリ VPX の管理 GUI への HTTPS URL(自己署名証明書 を使用)
- セカンダリ CitrixADCManagementUrl2-セカンダリ VPX の管理 GUI への HTTP URL
- secondaryCitrixADCInstanceId-新しく作成されたセカンダリ VPX インスタンスのインスタンス ID
- SecondaryCitrixADCPrivateNSIP-セカンダリ VPX の管理に使用されるプライベート IP (NS IP)
- SecondaryCitrixADCPublicNSIP-セカンダリ VPX の管理に使用されるパブリック IP (NS IP)
- secondaryCitrixADCPrivateVIP-VIP に関連付けられているセカンダリ VPX インスタンスのプライベート IP アドレス
- SecondaryCitrixADCSnip-SNIP に関連付けられているセカンダリ VPX インスタンスのプライベート IP ア ドレス
- SecurityGroup-VPX が属するセキュリティグループ ID

CFT に入力を提供する場合、CFT のあらゆる パラメーターに対して*は、それが必須フィールドであることを意味します。たとえば、VPC ID* は必須フィールドです。

次の前提条件が満たされている必要があります。CloudFormation テンプレートには、通常の EC2 の完全な権限を超えて、IAM ロールを作成するための十分な権限が必要です。また、このテンプレートのユーザーは、この CloudFormation テンプレートを使用する前に、条件に同意して AWS Marketplace 製品に登録する必要があります。

以下のものも存在している必要があります。

- ・キーペア
- 3つの未割り当て EIP

- 一次管理
- ・ クライアント VIP
- 二次管理

AWS での NetScaler VPX インスタンスのプロビジョニングの詳細については、「AWS での NetScaler VPX インス タンスのプロビジョニング」を参照してください。

StyleBooks を使用して GSLB を構成する方法については、StyleBooks を使用して GSLB を構成するをご覧くだ さい。

災害復旧 (DR)

災害(さいがん)とは、自然の災害、または人為的な出来事によって引き起こされる事業機能の突然の混乱である。 災害はデータセンターの運用に影響を及ぼします。その後、災害現場で失われたリソースとデータを完全に再構築し て復元する必要があります。データ消失やデータセンターのダウンタイムは重要であり、ビジネス継続性が低下しま す。

お客様が今日直面している課題の1つは、DR サイトをどこに置くかを決めることです。企業は、基盤となるインフ ラストラクチャやネットワーク障害に関係なく、一貫性とパフォーマンスを求めています。

災害復旧のために GSLB を展開するには、AWS に NetScaler VPX スタンドアロンインスタンスを展開するを参照 してください。

そのほかの参照先

ハイブリッドおよびマルチクラウド展開向けの NetScaler ADM GSLB。

AWS への NetScaler Web App Firewall デプロイ

October 17, 2024

NetScaler Web App Firewall は、レイヤー3ネットワークデバイスとして、または顧客サーバーと顧客ユーザー 間のレイヤー2ネットワークブリッジとして、通常は顧客企業のルーターまたはファイアウォールの背後に設置でき ます。NetScaler Web App Firewall は、Web サーバーとハブ間のトラフィックを傍受できる場所にインストール するか、ユーザーがそれらの Web サーバーにアクセスする際に経由するスイッチを使用する必要があります。次に、 ユーザーは、要求を Web サーバーに直接送信するのではなく Web アプリケーションファイアウォールに送信し、ユ ーザーに直接応答するのではなく Web アプリケーションファイアウォールに応答するようにネットワークを構成し ます。Web アプリケーションファイアウォールは、内部ルールセットとユーザーの追加と変更の両方を使用して、ト ラフィックを最終的な宛先に転送する前にフィルタリングします。有害であると検出したアクティビティをブロック またはレンダリングし、残りのトラフィックを Web サーバに転送します。上の図は、フィルタリングプロセスの概 要を示しています。

詳細については、「NetScaler Web App Firewall の仕組み」を参照してください。

本番環境への導入のための AWS 上の NetScaler Web App Firewall アーキテクチャ

この画像は、AWS クラウドに NetScaler Web App **Firewall** 環境を構築するデフォルトパラメータ付きの仮想プ ライベートクラウド(VPC)を示しています。



実稼働環境では、NetScaler Web App Firewall 環境用に次のパラメーターが設定されます:

- このアーキテクチャでは、AWS CloudFormation テンプレートの使用を前提としています。
- 2つの可用性ゾーンにまたがる VPC。AWS のベストプラクティスに従って、2つのパブリックサブネットと4 つのプライベートサブネットで構成され、/16 クラスレスドメイン間ルーティング (CIDR) ブロック (65,536 個のプライベート IP アドレスを持つネットワーク)を持つ AWS 上の独自の仮想ネットワークを提供します。。
- NetScaler Web App Firewall の 2 つのインスタンス (プライマリとセカンダリ)。各可用性ゾーンに 1 つずつ。
- ネットワークインターフェイス (管理、クライアント、サーバー) ごとに1つずつ、関連付けられたインスタン スのトラフィックを制御する仮想ファイアウォールとして機能する3つのセキュリティグループ。
- インスタンスごとに3つのサブネット。1つは管理用、1つはクライアント用、もう1つはバックエンドサーバー用です。

- VPC にアタッチされたインターネットゲートウェイ、およびインターネットへのアクセスを許可するために パブリックサブネットに関連付けられた Public Subnets ルートテーブル。このゲートウェイは、Web App Firewall ホストがトラフィックを送受信するために使用されます。インターネット・ゲートウェイの詳細 は、「インターネット・ゲートウェイ」を参照してください。
- 5 つのルートテーブル-プライマリとセカンダリ Web App Firewall の両方のクライアントサブネットに関連 付けられた1つのパブリックルートテーブル。残りの4つのルートテーブルは、4つのプライベートサブネッ ト (プライマリおよびセカンダリ Web App Firewall の管理サブネットとサーバー側サブネット)のそれぞれ にリンクしています。
- Web App Firewall の AWS Lambda は次のことを処理します:
 - HA モードの各可用性ゾーンに 2 つの Web App Firewall を設定する
 - サンプルの Web アプリケーションファイアウォールプロファイルを作成し、この構成を Web App Firewall に関してプッシュします
- AWS Identity and Access Management (IAM) は、ユーザーの AWS サービスとリソースへのアクセスを 安全に制御します。デフォルトでは、CloudFormation テンプレート (CFT) によって必要な IAM ロールが 作成されます。ただし、ユーザーは NetScaler ADC インスタンスに独自の IAM ロールを提供できます。
- パブリックサブネットでは、パブリックサブネット内のリソースへのアウトバウンドインターネットアクセス
 を許可する2つのマネージドネットワークアドレス変換(NAT)ゲートウェイ。

注

NetScaler Web App Firewall を既存の VPC に展開する CFT Web App Firewall テンプレートは、アスタ リスクでマークされたコンポーネントをスキップし、ユーザーに既存の VPC 構成の入力を求めます。

バックエンドサーバーは CFT によって展開されません。

コストとライセンス

ユーザーは、AWS デプロイの実行中に使用される AWS サービスの費用を負担します。このデプロイに使用できる AWS CloudFormation テンプレートには、ユーザーが必要に応じてカスタマイズできる設定パラメータが含まれて います。インスタンスタイプなど、これらの設定の一部は、デプロイのコストに影響します。コストの見積もりにつ いては、ユーザーが使用している各 AWS サービスの料金表ページを参照してください。価格は変更される場合があ ります。

AWS 上の NetScaler Web App Firewall にはライセンスが必要です。NetScaler Web App Firewall のライセン スを取得するには、ユーザーはライセンスキーを S3 バケットに配置し、展開を起動するときにその場所を指定する 必要があります。

注

ユーザーが自分のライセンス使用 (BYOL) ライセンスモデルを選択するときは、AppFlow 機能が有効になって

いることを確認する必要があります。BYOL ライセンスの詳細については、「AWS Marketplace/CitrixVPX-カ スタマーライセンス」を参照してください。

AWS で実行されている Citrix ADC Web App Firewall では、次のライセンスオプションを使用できます。ユーザーは、スループットなどの1つの要素に基づいて AMI (Amazon マシンイメージ) を選択できます。

- ライセンスモデル:従量制(本番ライセンスの場合は PAYG)または自分のライセンスの使用(BYOL、カス タマーライセンス AMI-NetScaler ADC プール容量)。NetScaler ADC プールキャパシティの詳細について は、「NetScaler ADC プールキャパシティ」を参照してください。
 - BYOL には、次の3つのライセンスモードがあります:
 - * NetScaler プールキャパシティの構成: Citrix ADC プールキャパシティの構成
 - * NetScaler VPX チェックインおよびチェックアウトライセンス (CICO): Citrix ADCVPX チェック インおよびチェックアウトライセンス

ヒント:

ユーザーが VPX-200、VPX-1000、VPX-3000、VPX-5000、または VPX-8000 のアプリケーショ ンプラットフォームタイプで CICO ライセンスを選択した場合は、NetScaler Console ライセン スサーバーに同じスループットライセンスがあることを確認する必要があります。

* NetScaler 仮想 CPU ライセンス: NetScaler 仮想 CPU ライセンス

注

ユーザーが VPX インスタンスの帯域幅を動的に変更したい場合は、BYOL オプションを選択する必要がありま す。たとえば、**NetScaler Console** からライセンスを割り当てることができる **NetScaler** プールキャパシ ティを選択するか、再起動せずにオンデマンドでインスタンスの最小容量と最大容量に従って **NetScaler** か らライセンスをチェックアウトできます。再起動は、ユーザーがライセンスエディションを変更する場合のみ 必要です。

- スループット:200 Mbps または 1 Gbps
- バンドル: プレミアム

展開オプション

この導入ガイドには、次の2つの展開オプションがあります:

- 最初のオプションは、クイックスタートガイド形式と次のオプションを使用して展開することです:
 - NetScaler Web App Firewall を新しい VPC に展開します (エンドツーエンド展開)。このオプションは、VPC、サブネット、セキュリティグループ、およびその他のインフラストラクチャコンポーネントで構成される新しい AWS 環境を構築し、その新しい VPC に NetScaler Web App Firewall をデプロイします。

- 既存の VPC に NetScaler Web App Firewall を展開します。このオプションは、ユーザーの既存の AWS インフラストラクチャに NetScaler Web App Firewall をプロビジョニングします。
- 2 つ目のオプションは、NetScaler Console を使用して Web App Firewall StyleBook を使用して展開す ることです

AWS クイックスタート

ステップ 1: ユーザー AWS アカウントにサインインする

- AWS のユーザーアカウントにサインインする:Amazon アカウントの作成 (必要な場合) または Amazon ア カウントにサインインするために必要なアクセス権限を持つ IAM (アイデンティティおよびアクセス管理) ユ ーザーロールを持つ AWS。
- ナビゲーションバーのリージョンセレクターを使用して、ユーザーが AWS 可用性ゾーン全体に高可用性をデ プロイする AWS リージョンを選択します。
- ユーザー AWS アカウントが正しく設定されていることを確認してください。詳細については、このドキュメントの「技術要件」セクションを参照してください。
- ステップ 2: NetScaler Web App Firewall AMI にサブスクライブする
 - このデプロイには、AWS Marketplace にある NetScaler Web App Firewall 用の AMI へのサブスクリプ ションが必要です。
 - ユーザー AWS アカウントにサインインします。
 - 次の表のいずれかのリンクを選択して、NetScaler Web App Firewall オファリングのページを開きます。
 - ユーザーは、以下のステップ3でクイックスタートガイドを起動して NetScaler Web App Firewall を展開するときに、NetScaler Web App Firewall イメージパラメーターを使用して、AMI サブスク リプションに一致するバンドルとスループットオプションを選択します。次のリストは、AMI オプショ ンと対応するパラメーター設定を示しています。この VPX AMI インスタンスには2つ以上の仮想 CPU と 2GB 以上のメモリが必要です。

注

AMI ID を取得するには、GitHub の「AWS Marketplace 上の NetScaler 製品: AWS Marketplace 上の Citrix 製品」ページを参照してください。

- AWS Marketplace AMI
 - NetScaler Web App Firewall (Web App Firewall)-200 Mbps: Citrix Web App Firewall (Web ア プリケーションファイアウォール)-200 Mbps

- NetScaler Web App Firewall (Web App Firewall)-1000 Mbps: Citrix Web App Firewall (Web アプリケーションファイアウォール)-1000 Mbps
- AMI ページで、[購読を続ける] を選択します。

∰r aws Griegories -	marketplace	ielutions = Myratio	n Mapping Autolant	Yaur Saved List		Partners 5	Q el In AMS Marketpicor	Amuor Wb Se	Hallo, M Mas Form
	CİTRİX	Citrix Web A In: Onix Systems, in Linux/Unix end	pp Firewall	(WAF) - 20 ion: 13:0-47:34 inves	0 Mbps		Continue to 1 Save to Typical Tek \$2.15 Tetal pricing per teta hedred on mit along o Vegenal. Were Detail	List List al Price /hr rese for services to 5 Bed (%	
	overview Product Ove	erview	ing	Usage		Support		Reviews	
	Gitik Web App Firewall () the art protections for m public-facing assets, indu IP reputation based filter protections, Layer 7 0000 enforce autometication; y policies, Using beth basic prohodos campenhemiale (ef use, Getting up and nu automuted learning med protections time, By automo Citris WAF adapts to the applications, Citris WWF and bedies, including PCI templates, It has never be	IBAF) is an enterprise gra otem applications. Caris ding websites, web appring, Bot mitigation, OWA is protection and mare. A tong 552,/TLS ciphen, T as well as advanced WA protection for your appli metter of mitig to attem of the application of the called dynamic profile teally learning how a pr application over as devel espe with overplaneo to OSS, HEMAA, and mare.	de salution offering (WAF mitigates the s, and APts. Clock W SP Top 10 applicate tap included are op 15 1.3, nate limiting F protections, Clock cations with unparts uns. Fur ther, using ng, Citris WAF save treected application ispens deploy and a sall major regulato With our CloudFern summing quickly. Wit	p stare of cats against AF includes ion threats tions to gand rewrite WAF distol case an typou an typou works, door the patient the typou typou typou typou the typou typou the typou typou the typo	Highlights • Comprehensive App powerful ADC platfor cloud, physical, virtu- enables consistency applications and we security from Lays 2 protection-ensures y vulnerable. • Secure your Website applications is more Cetrix WWF includes 1 reputation based fills	Security Clinix m - a single to al, bare-metal, across your hy Aflaws, Huloto I to Layer 7 an ou don't have 1 s, Apps, and Af than just baric basic through a uring, bot mitb	WAV is based on the de base across and containers that brid multi-doud c application doubt-in APH ts werry about being % Securing WAV functionality. dvanced WAV, IP gation,		

• ソフトウェアの使用に関する契約条件を確認し、[AcceptTerms]を選択します。



注

ユーザーは確認ページを受け取り、アカウント所有者に確認メールが送信されます。サブスクリプションの詳細な手順については、AWS Marketplace ドキュメントの「はじめに」の「はじめに」を参照してください。

サブスクリプションプロセスが完了したら、それ以上アクションを行わずに AWS Marketplace を終了します。AWS Marketplace からソフトウェアをプロビジョニングしないでください。ユーザーは、クイックスタートガイドを使用して AMI をデプロイします。

ステップ 3: AWS クイックスタートを起動する

- ユーザー AWS アカウントにサインインし、次のいずれかのオプションを選択して AWS CloudFormation テンプレートを起動します。オプションの選択に関するヘルプについては、このガイドの前半の「展開オプシ ョン」を参照してください。
 - 以下のいずれかの AWS CloudFormation テンプレートを使用して、AWS 上の新しい VPC に NetScaler VPX をデプロイします:
 - * Citrix/Citrix-ADC-AWS-CloudFormation / テンプレート/高可用性/クロス可用性ゾーン
 - * Citrix/Citrix-ADC-AWS-CloudFormation / テンプレート/高可用性/同一可用性ゾーン

重要:

ユーザーが NetScaler Web App Firewall を既存の VPC に展開する場合、VPC が 2 つの可用性ゾーンにまた がり、ワークロードインスタンスの各可用性ゾーンに 1 つのパブリックサブネットと 2 つのプライベートサブ ネットがあり、サブネットが共有されていないことを確認する必要があります。このデプロイガイドは共有サ ブネットをサポートしていません。共有 VPC の操作: 共有 VPCの操作を参照してください。これらのサブネッ トでは、インスタンスがインターネットに公開されずにパッケージやソフトウェアをダウンロードできるよう に、ルートテーブルに NAT Gateway が必要です。NAT ゲートウェイの詳細については、「NAT ゲートウェイ」 を参照してください。サブネットが重複しないようにサブネットを構成します。

また、ユーザーは、DHCP オプションのドメイン名オプションが、次の Amazon VPC ドキュメントで説明されて いるとおりに設定されていることを確認する必要があります: DHCP オプション セット DHCP オプション セット。 ユーザーは、クイックスタートガイドを起動したときに VPC 設定の入力を求められます。

- 各デプロイが完了するまでに約15分かかります。
- ナビゲーションバーの右上隅に表示される AWS リージョンを確認し、必要に応じて変更します。ここで、 Citrix Web App Firewall のネットワークインフラストラクチャが構築されます。テンプレートは、デフォル トで米国東部 (オハイオ) リージョンで起動されます。

注

このデプロイには NetScaler Web App Firewall が含まれていますが、これは現在すべての AWS リージョン でサポートされているわけではありません。サポートされているリージョンの最新リストについては、「AWS サービスエンドポイント: AWS サービスエンドポイント」を参照してください。

- [テンプレートの選択] ページで、テンプレート URL のデフォルト設定を保持し、[次へ] を選択します。
- 【詳細の指定】ページで、ユーザーの都合に合わせてスタック名を指定します。テンプレートのパラメータを確認します。入力が必要なパラメータの値を指定します。その他すべてのパラメータについては、デフォルト設定を確認し、必要に応じてカスタマイズします。
- 次の表では、パラメータがカテゴリ別にリストされ、デプロイオプションについて個別に説明されています:
- NetScaler Web App Firewall を新規または既存の VPC に展開するためのパラメータ(展開オプション1)

• パラメータのレビューとカスタマイズが完了したら、[次へ]を選択する必要があります。

NetScaler Web App Firewall を新しい VPC に展開するためのパラメーター

١	/P	С	ネッ	トワー	-ク	設定
---	----	---	----	-----	----	----

パラメータラベル (名前)	デフォルト	説明
プライマリアベイラビリティゾーン (primaryAvailabilityZone)	入力が必要	プライマリ NetScaler Web App Firewall 展開の可用性ゾーン
セカンダリ可用性ゾーン (セカンダ リ可用性ゾーン)	入力が必要	NetScaler Web App Firewall セ カンダリ展開の可用性ゾーン
VPC CIDR (VPCCIDR)	10.0.0/16	VPC の CIDR ブロック。x.x.x.x/x 形式の有効な IP CIDR 範囲である必 要があります。
リモート SSH CIDR IP (管理) (restrictedsSHCIDR)	入力が必要	EC2 インスタンスに SSH できる IP アドレス範囲 (ポート:22)。
リモート HTTP CIDR IP (クライア ント) (制限付き WebAppCIDR)	0.0.0.0/0	たとえば、0.0.0.0/0 を使用すると、 すべての IP アドレスが SSH または RDP を使用してユーザーインスタン スにアクセスできるようになります。 注: ユーザーインスタンスを本番環 境で使用するのは安全ではないため、 特定の IP アドレスまたはアドレス範 囲のみにユーザーインスタンスへの アクセスを許可してください。 EC2 インスタンスに HTTP できる IP アドレス範囲 (ポート:80)
リモート HTTP CIDR IP (クライア ント) (制限付き WebAppCIDR)	0.0.0/0	EC2 インスタンスに HTTP できる IP アドレス範囲 (ポート:80)
プライマリ管理プライベートサブネ ット CIDR (プライマリ管理プライ ベートサブネット CIDR)	10.0.1.0/24	可用性ゾーン1にあるプライマリ管 理サブネットの CIDR ブロック。
プライマリ管理プライベート IP (プ ライマリ管理プライベート IP)	_	プライマリ管理サブネット CIDR か らプライマリ管理 ENI(最後のオク テットは 5 から 254 の間でなければ ならない)に割り当てられたプライ ベート IP。

	デフォルト	説明
プライマリクライアントパブリック サブネット CIDR (primary ClientPublicSubnetCIDR)	10.0.2.0/24	可用性ゾーン 1 にあるプライマリク ライアントサブネットの CIDR ブロ ック。
プライマリクライアントプライベー ト IP (プライマリクライアントプラ イベート IP)	_	プライマリクライアントサブネット CIDR のプライマリクライアント IP からプライマリクライアント ENI (最後のオクテットは 5〜254 でなけ ればなりません) に割り当てられた プライベート IP。
プライマリサーバプライベートサブ ネット CIDR (プライマリサーバプ ライベートサブネット CIDR)	10.0.3.0/24	可用性ゾーン1にあるプライマリサ ーバーの CIDR ブロック。
プライマリサーバプライベート IP (プライマリサーバプライベート IP)	_	プライマリサーバサブネット CIDR からプライマリサーバ ENI(最後の オクテットは 5 ~254)に割り当て られたプライベート IP。
セカンダリ管理プライベートサブネ ット CIDR (セカンダリ管理プライ ベートサブネット CIDR)	10.0.4.0/24	可用性ゾーン 2 にあるセカンダリ管 理サブネットの CIDR ブロック。
セカンダリ管理プライベート IP (セ カンダリ管理プライベート IP)	_	セカンダリ管理 ENI に割り当てられ たプライベート IP(最後のオクテッ トは 5 ~254 である必要がありま す)。セカンダリ管理サブネット CIDR からセカンダリ管理 IP を割り 当てます。
セカンダリクライアントパブリック サブネット CIDR (セカンダリ ClientPublicSubnetCIDR)	10.0.5.0/24	可用性ゾーン 2 にあるセカンダリク ライアントサブネットの CIDR ブロ ック。
セカンダリクライアントプライベー ト IP (セカンダリクライアントプラ イベート IP)	_	セカンダリクライアント ENI に割り 当てられたプライベート IP(最後の オクテットは 5 ~254 である必要が あります)。セカンダリ・クライアン ト・サブネット CIDR からセカンダ リ・クライアント IP を割り当てま す。

パラメータラベル (名前)	デフォルト	
セカンダリサーバプライベートサブ ネット CIDR (セカンダリサーバプ ライベートサブネット CIDR)	10.0.6.0/24	可用性ゾーン 2 にあるセカンダリサ ーバーサブネットの CIDR ブロック。
セカンダリサーバプライベート IP (セカンダリサーバプライベート IP)	_	セカンダリサーバ ENI に割り当てら れたプライベート IP(最後のオクテ ットは 5 ~254 である必要がありま す)。セカンダリサーバサブネット CIDR からセカンダリサーバ IP を割
VPC テナンシー属性 (VPCTenancy)	デフォルト	り当てます。 VPC に起動されたインスタンスの許 可されたテナンシー。単一の顧客専 用の EC2 インスタンスを起動するに は、[Dedicated tenancy] を選択 します。

踏み台ホスト設定

パラメータラベル (名前)	デフォルト	説明
踏み台ホストが必要	いいえ	デフォルトでは、踏み台ホストは設
(LinuxBastionHostEIP)		定されません。ただし、ユーザーが
		サンドボックス展開を選択したい場
		合は、メニューから「はい」を選択
		します。これにより、ユーザーはプ
		ライベートサブネットとパブリック
		サブネットのコンポーネントにアク
		セスできる EIP を使用して、パブリ
		ックサブネットに Linux Bastion
		Host がデプロイされます。

NetScaler Web App Firewall 構成

パラメータラベル (名前)	デフォルト	説明
キーペア名 (keyPairName)	入力が必要	公開鍵と秘密鍵のペア。これにより、
		ユーザーは起動後にユーザーインス
		タンスに安全に接続できます。これ
		は、ユーザーが希望する AWS リー
		ジョンで作成したキーペアです。「技
		術要件」セクションを参照してくだ
		さい。
NetScaler インスタンスタイプ	m4.xlarge	ADC インスタンスに使用する EC2
(CitrixADCInstanceType)		インスタンスタイプ。選択したイン
		スタンスタイプが AWS
		Marketplace で利用可能なインス
		タンスタイプと一致していることを
		確認してください。一致しない場合、
		CFT が失敗する可能性があります。
NetScaler ADC AMI ID (Citrix	_	NetScaler Web App Firewall 導
ADC ImageID)		入に使用される AWS Marketplace
		AMI。これは、ステップ2でサブス
		クライブした AMI ユーザーと一致す
		る必要があります。
NetScaler ADC VPX IAM $\Box - \mu$	_	このテンプレート:
(iam:GetRole)		AWS-QuickStart/Quickstart-
		Citrix-ADC-VPX/テンプレートは、
		NetScaler VPX に必要な IAM ロー
		ルとインスタンスプロファイルを作
		成します。空のままにすると、CFT
		は必要な IAM ロールを作成します。
クライアント・パブリック IP (EIP)	いいえ	ユーザーがユーザーのクライアント
(クライアント・パブリック IP)		ネットワークインターフェイスにパ
		ブリック EIP を割り当てる場合は、
		[はい] を選択します。それ以外の場
		合、展開後でも、ユーザーは必要に
		応じて後で割り当てることができま
		す。

プールライセンス設定

パラメータラベル (名前)	デフォルト	説明
NetScaler コンソールプールライ センス	いいえ	ライセンスに BYOL オプションを選 択する場合は、リストから [はい] を 選択します。これにより、ユーザー はすでに購入したライセンスをアッ プロードできます。ユーザーは作業 を開始する前に、NetScaler ADC プールキャパシティを構成して、 NetScaler Console のプールライ センスが利用可能であることを確認 する必要があります。「NetScaler プール容量の構成」を参照してくだ さい。
アクセス可能な NetScaler コンソ ール /NetScaler コンソールエージ ェント IP	入力が必要	カスタマーライセンスオプションで は、ユーザーが NetScaler Console をオンプレミスで展開する か、エージェントをクラウドに展開 するかにかかわらず、入力パラメー ターとして使用できる NetScaler Console IP にアクセスできること を確認してください。
ライセンスモード	オプション	オーック はう フのフィビンス ビート から選択できます: NetScaler プールキャパシティを設 定します。詳しくは、「Citrix ADC プール容量の構成」を参照してくだ
ライセンス帯域幅 (Mbps)	0 メガビット/秒 Premium	さい ライセンスモードが NetScaler VPX チェックインおよび Pooled-Licensing の場合のお、こ チョックールド表示されます。これ 詳しくは、「Citrix ADC VPX チェッ は、BYOL ADC が作成された後に割 り当くちれるラチゼンスの初期帯域 いてます。10 NetScaler 仮想 CPU ライセンス。 Mbps の倍数でなければなりません。 詳しくは、「Citrix ADC 仮想 CPUラ
, , , , , , , , , , , , , , , , , , ,		イセンス」を参照してください ドのライセンスエディションはプレ ミアムです。

パラメータラベル (名前)	デフォルト	説明
アプライアンスプラットフォームタ	オプション	ユーザが CICO ライセンスモードを
イプ		選択する場合のみ、必要なアプライ
		アンスプラットフォームタイプを選
		択してください。ユーザーには、
		VPX-200、VPX-1000、VPX-3000、
		VPX-5000、VPX-8000 などのオプ
		ションが表示されます。
ライセンスエディション	Premium	vCPU ベースのライセンスのライセ
		ンスエディションはプレミアムです。

AWS クイックスタート設定

注

独自の配置プロジェクト用にクイックスタートガイドテンプレートをカスタマイズする場合を除き、次の2つ のパラメータの既定の設定を維持することをお勧めします。これらのパラメーターの設定を変更すると、コー ド参照が自動的に更新され、新しいクイックスタートガイドの場所が示されます。詳細については、AWS クイ ックスタートガイド寄稿者ガイドを参照してください。AWS Quick Starts/Option 1-クイックスタートを採 用する。

パラメータラベル (名前)	デフォルト	説明
クイックスタートガイド S3 バケッ ト名 (qss3BucketName)	aws-quickstart	ユーザーがクイックスタートガイド アセットのコピー用に作成した S3 バケット(ユーザーがクイックスタ ートガイドを自分で使用するために カスタマイズまたは拡張することを 決定した場合)。バケット名には、数 字、小文字、大文字、ハイフンを含め ることができますが、ハイフンで開
		始または終了することはできません。

パラメータラベル (名前)	デフォルト	説明
クイックスタートガイド S3 キープ	クイックスタート-citrix-adc-vpx/	[オブジェクトキー] と [メタデータ:
レフィックス (qss3KeyPrefix)		[オブジェクトキーとメタデータ] の
		S3 キー名プレフィックスは](https:
		//docs.aws.amazon.com/Amaz
		onS3/latest/dev/UsingMetadat
		a.html)%E3%80%81%E3%82
		%AF%E3%82%A4%E3%83%8
		3%E3%82%AF%E3%82%B9%
		E3%82%BF%E3%83%BC%E3
		%83%88%E3%82%AC%E3%8
		2%A4%E3%83%89%E3%82%
		A2%E3%82%BB%E3%83%83
		%E3%83%88%E3%81%AE%E
		3%83%A6%E3%83%BC%E3%
		82%B6%E3%83%BC%E3%82
		%B3%E3%83%94%E3%83%B
		C%E7%94%A8%E3%81%AE%
		E3%83%95%E3%82%A9%E3
		%83%AB%E3%83%80%E3%8
		3%BC%E3%82%92%E3%82%
		B7%E3%83%9F%E3%83%A5
		%E3%83%AC%E3%83%BC%E
		3%83%88%E3%81%99%E3%
		82%8B%E3%81%9F%E3%82
		%81%E3%81%AB%E4%BD%B
		F%E7%94%A8%E3%81%95%
		E3%82%8C%E3%81%BE%E3
		%81%99%E3%80%82 この接頭
		辞には、数字、小文字、大文字、ハ
		イフン、およびスラッシュを含める
		ことができます。

- 【オプション】ページで、ユーザーはスタック内のリソースにリソースタグまたはキーと値のペアを指定し、詳細オプションを設定できます。リソースタグの詳細については、「リソースタグ」を参照してください。AWS CloudFormation スタックオプションの設定の詳細については、「AWS CloudFormation スタックオプションの設定」を参照してください。完了したら、[次へ]を選択する必要があります。
- [Review]ページで、テンプレートの設定を確認して確認します。[Capabilities]で、2つのチェックボッ

クスをオンにして、テンプレートが IAM リソースを作成し、マクロを自動展開する機能が必要になる可能性が あることを確認します。

- [Create]を選択してスタックをデプロイします。
- スタックのステータスを監視します。ステータスが CREATE_COMPLETE の場合、NetScaler Web App Firewall インスタンスは準備完了です。
- スタックの [出力] タブに表示される URL を使用して、作成されたリソースを表示します。

OoudFormation > Stacks > quickstant wolf ik				
🗉 Stacks (1) 🛛 🔿	Stack info Events Resources	Outputs Parameters	Template Change sets	
Q, Filter by stack name				
Active: # Of Vex-netted	Outputs (16)			σ
quidatan waf-ik 2020-os on tantat VPC-0020 © CMARE_COMPLETE	Q, Search extputs			0
	Key A	Value v	Description v	Export name ==
	ClentSecurityGroupID	sg-0056etc025c9c5a264	Security group 10 for client ADC DNs	
	ManagementSecurityGroupID	sg-08c5c20x6a282206d	Security group 10-for management ADC DNs	
	PrimaryA0Onstance®	106804119286x9084	Primary ADC Instance ID	
	PrimaryClientPrivateVP	10.0.2.118	Primary Client private VIP	
	PrimaryClientPublicSubnet(0	subret-025745e2566d13d59	Primary Client public subret ID	
	PrimaryHanagementPrivatehSiP	10.0.1.149	Primary Management, private NSIP	
	PrimaryManagementPrivatxSubnetID	subret-0810b54%x8925813	Primary Management private subnet ID	
	PrimaryServerHivatzSubnettD	subret-071053012154ec15c	Primary Server private subnet ID	
	SecondaryADCrestance0	10056495795845564	Secondary ADC instance ID	
	Secondary/ClientPrivata/dP	10.8.5.231	Secondary Client private VIP	
	SecondaryClientPublicSubnetD	subnet-01941cd7905840aec	Secondary Client public subnet ID	
	SecondaryManagementPrivateNS/P	10.0.4.213	Secondary Management: private NSIP	
	SecondaryHanagementPrivateSubnettD	subret-00x82966625546x22	Secondary Management private subnet ID	
	SecondaryServerPrivateSubnettD	subret: 030018e63558/4453	Secondary Server private subnet ID	
	ServerSecurityGroup/D	sg-0s?##htSeafkSecd?	Security group 10 for server ADC ENIS	
	VPOD	vpc-06a7v8/9x80425/9x	VPC/D	

ステップ 4: デプロイメントをテストする

このデプロイでは、** インスタンスをプライマリとセカンダリと呼びます **。各インスタンスには、それぞれ異な る IP アドレスが関連付けられています。クイックスタートが正常に展開されると、トラフィックは可用性ゾーン 1 で構成されたプライマリ NetScaler Web App Firewall インスタンスを経由します。フェイルオーバー状態で、プ ライマリインスタンスがクライアントの要求に応答しない場合、セカンダリの Web App Firewall インスタンスが 引き継ぎます。

プライマリインスタンスの仮想 IP アドレスの Elastic IP アドレスがセカンダリインスタンスに移行され、セカンダ リインスタンスが新しいプライマリインスタンスとして引き継がれます。

フェイルオーバープロセスでは、NetScaler Web App Firewall は次の処理を行います:

• NetScaler Web App Firewall は、IP セットが接続されている仮想サーバーをチェックします。

- NetScaler Web App Firewall は、仮想サーバーがリッスンしている2つのIP アドレスから、関連するパブ リックIP アドレスを持つIP アドレスを見つけます。1つは仮想サーバに直接接続され、もう1つはIP セッ トを介して接続されます。
- NetScaler Web App Firewall は、パブリック Elastic IP アドレスを、新しいプライマリ仮想 IP アドレスに 属するプライベート IP アドレスに再関連付けます。

デプロイを検証するには、以下を実行します:

• プライマリインスタンスに接続する

たとえば、プロキシサーバー、ジャンプホスト(AWS で実行されている Linux/Windows/FW インスタンス、また は踏み台ホスト)、またはその VPC に到達可能な別のデバイス、またはオンプレミス接続を扱う場合は直接接続など です。

トリガーアクションを実行してフェイルオーバーを強制し、セカンダリインスタンスが引き継ぐかどうかを確認します。

ヒント:

NetScaler Web App Firewall に関する構成をさらに検証するには、プライマリ **NetScaler**Web App Firewall インスタンスに接続した後に次のコマンドを実行します。

Sh appfw profile QS-Profile

踏み台ホストを使用して NetScaler Web App Firewall HA ペアに接続

ユーザーがサンドボックス展開を選択している場合(たとえば、CFT の一部としてユーザーが踏み台ホストの設定を 選択する場合)、パブリックサブネットにデプロイされた Linux 踏み台ホストは、Web App Firewall インターフェ イスにアクセスするように構成されます。

ここでサインインしてアクセスする AWS CloudFormation コンソールで、サインインしてマスタースタックを選択し、[出力] タブで **LinuxBastionHostelP1** の値を見つけます。

Outputs (17)		
Q. Search autputs		
Key 🔺	Value	♥ Description
InstanceProfileName	tCaT-tag-citrix-adc-master-10599539- WorkLoadStack-GZX61DAOP4J- IAMRoleStack-36JSFNFGO22N- CitrixNodesProfile-7R84KI62FPA3	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

- PrivateManagementPrivatenSIP と primaryADCInstanceId キーの値は、ADC に SSH 接続するための後のステップで使用します。
- [サービス]を選択します。
- [コンピュート] タブで [**EC2**] を選択します。
 - リソースで、実行中のインスタンスを選択します。
 - プライマリ Web App Firewall インスタンスの [説明] タブで、IPv4 パブリック IP アドレスを書き留めます。ユーザーは SSH コマンドを構築するためにその IP アドレスが必要です。

tost-tag-cit	trix-ado-master-eu-ce	entral-1-97a6acc9-V	VorkLoad	Stack-XYC4-PrimaryADC	Instance-1XID05VH2MRAWG P	himary	i-07197878fc2cafaed	m4.xlarge
toat-tag-ci	trix-ado-master-eu-or	entral-1-97a6acc9-V	WorkLoad	Stack-XY-SecondaryADC	Instance-NV30OQYJ9DBJ Sec	ondary	i-0d671adb473d1d7	m4.xlarge
Instance: I-07 1X:006VH2MRA	197878fc2cataed WG Primary) E	(tcat-tag-citrix-a Ilastic IP: 3.122.1	dc-mast 41.245	er-eu-central-1-97a6a	cc9-WorkLoadStack-XYC4	-PrimaryA	DCInstance-	
Description	Status Checks	Monitoring	Tags	Usage Instructions				
	Instance ID	i-07197878fc2ce	feed		Public DNS (Pv4)			
	Instance state	running			IPv4 Public IP	3.122.14	1.245	
	Instance type	m4.xlarge			IPv6 IPs			
	Eastic IPs	3.122.141.245*			Private DNS	ip-10-0-1 1.compu	-61.eu-central- te.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-ad 1-97a6acc9-Wor SecurityGroupSt	ic-master kLoadSta ack-	eu-central- ck-XYC4-	Secondary private IPs			

キーをユーザーキーチェーンに保存するには、次のコマンドを実行します。ssh-add -K [your-key -pair].pem

Linux では、ユーザーは-K フラグを省略する必要があるかもしれません。

 ユーザーがステップ1でメモした LinuxBastionHostelP1 の値を使用して、次のコマンドを使用して踏み 台ホストにログインします。

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

• 踏み台ホストから、ユーザーは SSH を使用してプライマリ Web App Firewall インスタンスに接続できます。

ssh nsroot@[Primary Management Private NSIP]

パスワード:[プライマリ ADC インスタンス ID]

```
lubuntu@ip-10-0-5-243:~$ ssh nsroot@10.0.1.71
ponnnnpoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonnppoonn
```

これで、ユーザーは NetScaler Web App Firewall プライマリインスタンスに接続されました。使用可能なコマン ドを確認するには、help コマンドを実行します。現在の HA 設定を表示するには、show HA node コマンドを実行 します。

NetScaler コンソール

NetScaler アプリケーション配信管理サービスは、オンプレミスまたはクラウドに展開されている NetScaler MPX、 NetScaler VPX、NetScaler Gateway、NetScaler Secure Web Gateway、NetScaler SDX、NetScaler ADC CPX、NetScaler SD-WAN アプライアンスなどの NetScaler 展開を管理するための簡単でスケーラブルなソリュ ーションを提供します。

NetScaler Console Service ドキュメントには、サービスの開始方法、サービスでサポートされている機能のリスト、およびこのサービスソリューションに固有の構成に関する情報が含まれています。

詳しくは、「NetScaler コンソールの概要」を参照してください。

NetScaler コンソールを使用して AWS に NetScaler VPX インスタンスをデプロイする

顧客がアプリケーションをクラウドに移行すると、アプリケーションの一部であるコンポーネントが増え、分散性が 高まり、動的に管理する必要があります。

詳細については、「AWS での NetScaler VPX インスタンスの Provisioning」を参照してください。

NetScaler Web App Firewall と OWASP トップ 10 –2017

オープン Web アプリケーションセキュリティプロジェクト: OWASP は、Web アプリケーションセキュリティの ための 2017 年の OWASP トップ 10 をリリースしました。このリストは、最も一般的な Web アプリケーションの 脆弱性を説明しており、Web セキュリティを評価するための優れた出発点です。ここでは、これらの欠陥を軽減す るために NetScaler Web App Firewall (Web App Firewall)を構成する方法について詳しく説明します。Web App Firewall は、NetScaler (プレミアムエディション)の統合モジュールとしてだけでなく、さまざまなアプラ イアンスでも利用できます。

OWASP Top 10 の完全なドキュメントは OWASP Top Tenで入手できます。

署名は、ユーザーがユーザーアプリケーションの保護を最適化するのに役立つ次の展開オプションを提供します:

- ネガティブセキュリティモデル:ネガティブセキュリティモデルでは、ユーザーは事前に構成された豊富なシ グネチャルールを使用して、パターンマッチングの機能を適用して攻撃を検出し、アプリケーションの脆弱性 から保護します。ユーザーは望まないものだけをブロックし、残りを許可します。ユーザーは、ユーザーアプ リケーションの特定のセキュリティニーズに基づいて独自の署名ルールを追加して、独自のカスタマイズされ たセキュリティソリューションを設計できます。
- ハイブリッドセキュリティモデル:署名の使用に加えて、ユーザーはポジティブセキュリティチェックを使用して、ユーザーアプリケーションに最適な構成を作成できます。署名を使用してユーザーが望まないものをブロックし、肯定的なセキュリティチェックを使用して許可されているものを強制します。

署名を使用してユーザーアプリケーションを保護するには、ユーザーは署名オブジェクトを使用するように1つ以上 のプロファイルを構成する必要があります。ハイブリッドセキュリティ構成では、ユーザー署名オブジェクトの SQL インジェクションおよびクロスサイトスクリプティングパターン、および SQL 変換ルールは、シグニチャルールだ けでなく、Web アプリケーションファイアウォールプロファイルで設定されたポジティブセキュリティチェックに よっても使用されます。署名オブジェクト。

Web アプリケーションファイアウォールは、ユーザ保護された Web サイトおよび Web サービスへのトラフィック を調べ、シグネチャと一致するトラフィックを検出します。一致は、ルール内のすべてのパターンがトラフィックに 一致する場合にのみトリガーされます。一致が発生すると、ルールに対して指定されたアクションが呼び出されます。 要求がブロックされると、ユーザーはエラーページまたはエラーオブジェクトを表示できます。ログメッセージは、 ユーザーがユーザーアプリケーションに対して開始されている攻撃を特定するのに役立ちます。ユーザーが統計を有 効にすると、Web アプリケーションファイアウォールは、Web アプリケーションファイアウォールの署名またはセ キュリティチェックに一致する要求に関するデータを保持します。

トラフィックがシグニチャとポジティブセキュリティチェックの両方に一致する場合、2 つのアクションのうち、よ り厳しい制限が適用されます。たとえば、ブロックアクションが無効になっているシグネチャルールにリクエストが 一致し、アクションがブロックされている SQL Injection ポジティブセキュリティチェックにも一致する場合、リク エストはブロックされます。この場合、署名違反は [ブロックされていない] として記録される可能性がありますが、 要求は SQL インジェクションチェックによってブロックされます。

カスタマイズ: 必要に応じて、ユーザーは独自のルールを署名オブジェクトに追加できます。ユーザーは SQL/XSS パ ターンをカスタマイズすることもできます。ユーザーアプリケーションの特定のセキュリティニーズに基づいて独自 の署名ルールを追加するオプションにより、ユーザーは独自のカスタマイズされたセキュリティソリューションを柔 軟に設計できます。ユーザーは望まないものだけをブロックし、残りを許可します。特定の場所で特定の高速一致パ ターンを使用すると、処理オーバーヘッドを大幅に削減してパフォーマンスを最適化できます。ユーザーは、SQL イ ンジェクションおよびクロスサイトスクリプティングパターンを追加、変更、または削除できます。組み込みの正規 表現と式エディタは、ユーザーがユーザーパターンを構成し、その正確性を検証するのに役立ちます。

NetScaler Web App Firewall

Web App Firewall は、最新のアプリケーションに最先端の保護を提供するエンタープライズグレードのソリューシ ョンです。NetScaler Web App Firewall は、Web サイト、Web アプリケーション、API などの一般公開資産に 対する脅威を軽減します。NetScaler Web App Firewall には、IP レピュテーションベースのフィルタリング、ボ ット対策、OWASP トップ 10 アプリケーション脅威対策、レイヤー 7 DDoS 保護などが含まれています。また、認 証を強制するオプション、強力な SSL/TLS 暗号、TLS 1.3、レート制限、および書き換えポリシーも含まれていま す。NetScaler Web App Firewall は、基本的な保護機能と高度な Web App Firewall 保護の両方を使用して、比 類のない使いやすさでアプリケーションを包括的に保護します。起動して実行するのはほんの数分です。さらに、 NetScaler Web App Firewall は動的プロファイリングと呼ばれる自動学習モデルを使用することで、ユーザーの 貴重な時間を節約できます。Web App Firewall は、保護されたアプリケーションの仕組みを自動的に学習すること で、開発者がアプリケーションをデプロイしたり変更したりしても、アプリケーションに適応します。NetScaler Web App Firewall は、PCI-DSS、HIPAA などを含むすべての主要な規制基準や機関へのコンプライアンスに役立 ちます。CloudFormation テンプレートを使えば、これまでになく簡単に立ち上げてすぐに実行できます。Auto Scaling を使用すると、トラフィックが拡大しても、ユーザーはアプリケーションを保護したまま安心できます。

Web App Firewall 導入戦略

Web アプリケーションファイアウォールを展開するための最初のステップは、最大限のセキュリティ保護が必要な アプリケーションまたは特定のデータ、脆弱性の低いアプリケーション、およびセキュリティ検査を安全に回避でき るものを評価することです。これにより、ユーザーは最適な構成を考案し、トラフィックを分離するための適切なポ リシーとバインドポイントを設計できます。たとえば、ユーザーは、画像、MP3 ファイル、ムービーなどの静的な Web コンテンツに対する要求のセキュリティ検査をバイパスするポリシーを構成し、動的コンテンツのリクエスト に高度なセキュリティチェックを適用する別のポリシーを構成することができます。ユーザーは複数のポリシーとプ ロファイルを使用して、同じアプリケーションの異なるコンテンツを保護できます。

次のステップは、展開のベースラインを設定することです。まず、仮想サーバーを作成し、そのサーバーを介してテ ストトラフィックを実行して、ユーザーシステムを通過するトラフィックの速度と量を把握します。

次に、Web App Firewall をデプロイします。NetScaler コンソールと Web App Firewall StyleBook を使用し て、Web App Firewall を構成します。詳細については、このガイドの下の「StyleBook」セクションを参照してく ださい。

Web アプリファイアウォールを Web App Firewall StyleBook で展開および構成したら、次のステップとして役 立つ次のステップは、NetScaler ADC Web App Firewall と OWASP トップ 10 を実装することです。 最後に、Web App Firewall 保護のうち 3 つは、一般的な種類の Web 攻撃に対して特に効果的であるため、他のど の保護よりも一般的に使用されています。したがって、これらは初期展開時に実装する必要があります。

NetScaler コンソール

NetScaler コンソールは、オンプレミスまたはクラウドに展開されている NetScaler ADC MPX、NetScaler ADC VPX、NetScaler Gateway、NetScaler Secure Web Gateway、NetScaler ADC SDX、NetScaler ADC CPX、NetScaler SD-WAN アプライアンスなどの NetScaler ADC 展開を管理するためのスケーラブルなソリューション を提供します。

NetScaler コンソールのアプリケーション分析 および管理機能

NetScaler コンソールでサポートされている機能は、アプリセキュリティにおける NetScaler Console の役割にとって重要です。

機能の詳細については、「機能と解決策」を参照してください。

前提条件

AWS で VPX インスタンスを作成する前に、ユーザーは前提条件が満たされていることを確認する必要があります。 詳細については、前提条件を参照してください。

制限事項と使用ガイドライン

制限事項と使用ガイドライン に記載されている制限事項と使用ガイドラインは、Citrix ADC VPX インスタンスを AWS にデプロイする場合に適用されます。

技術的要件

ユーザーがクイックスタートガイドを起動してデプロイを開始する前に、次のリソーステーブルで指定されているようにユーザーアカウントを設定する必要があります。そうしないと、デプロイが失敗する可能性があります。

リソース

必要に応じて、ユーザー Amazon アカウントにサインインし、次のリソースのサービス制限の引き上げをリクエス トします。AWS/Sign in。これらのリソースを使用する既存の展開がすでにあり、この展開で既定の制限を超える可 能性があると思われる場合は、これを実行する必要があります。デフォルトの制限については、AWS ドキュメント 「AWS サービスクォータ」の「AWS サービスクォータ」を参照してください。 AWS Trusted Advisor (こちらを参照): AWS/Sign inは、一部のサービスのいくつかの側面の使用状況と制限を表示するサービス制限チェックを提供します。

リソース	この展開では
VPC	1
エラスティック IP アドレス	0/1 (踏み台ホスト用)
IAM セキュリティグループ	3
IAMロール	1
サブネット	6 (3/アベイラビリティゾーン)
インターネットゲートウェイ	1
ルートテーブル	5
Web App Firewall VPX インスタンス	2
要塞ホスト	0/1
NAT ゲートウェイ	2

領域

AWS 上の NetScaler Web App Firewall は、現在すべての AWS リージョンでサポートされているわけではありま せん。サポートされているリージョンの最新リストについては、AWS ドキュメント「AWS サービスエンドポイント」 の「AWS サービスエンドポイント」を参照してください。

AWS リージョンの詳細と、クラウドインフラストラクチャが重要な理由については、「グローバルインフラストラク チャ」を参照してください。

キーペア

クイックスタートガイドを使用して、ユーザーがデプロイする予定のリージョンのユーザー AWS アカウントに、少 なくとも 1 つの Amazon EC2 キーペアが存在することを確認します。キーペア名を書き留めます。ユーザーは、展 開中にこの情報の入力を求められます。キーペアを作成するには、AWS ドキュメント「Amazon EC2 キーペアと Linux インスタンス」の Amazon EC2 キーペアと Linux インスタンスの指示に従います。

ユーザーがテストまたは概念実証の目的でクイックスタートガイドをデプロイする場合は、本番インスタンスですで に使用されているキーペアを指定する代わりに、新しいキーペアを作成することをお勧めします。

参照ドキュメント

• HTML SQL インジェクションチェック

- XML SQL インジェクションチェック
- コマンドラインを使用して HTML クロスサイトスクリプティングチェックを設定する
- XML クロスサイトスクリプティングチェック
- コマンドラインによるバッファオーバーフローセキュリティチェックの設定
- 署名オブジェクトの追加または削除
- 署名オブジェクトの設定または変更
- 署名オブジェクトの更新
- Snort 規則の統合
- ボットの検出
- Microsoft Azure で NetScaler VPX インスタンスを展開する

SR-IOV ネットワークインターフェイスの使用を NetScaler ADC VPX インスタンス で構成する

October 17, 2024

注

```
高可用性セットアップでの SR-IOV インターフェイスのサポートは、NetScaler リリース 12.0 57.19 以降か
ら利用できます。
```

AWS で NetScaler ADC VPX インスタンスを作成した後、AWS CLI を使用して、SR-IOV ネットワークインターフ ェイスを使用するように仮想アプライアンスを構成できます。

NetScaler VPX 3G および 5G の NetScaler ADC VPX AWS マーケットプレイスエディションを除き、すべての NetScaler ADC VPX モデルでは、ネットワークインターフェイスのデフォルト構成で SR-IOV が有効になっていま せん。

設定を開始する前に、次のトピックをお読みください。

- 前提条件
- 制限事項および使用上のガイドライン

このセクションでは、以下のトピックについて説明します。

- インターフェイスタイプを SR-IOV に変更
- 高可用性セットアップでの SR-IOV の設定

インターフェイスタイプをSR-IOV に変更

show interface summary コマンドを実行すると、ネットワークインターフェイスのデフォルト設定を確認できます。

例 **1**:次の CLI スクリーンキャプチャは、NetScaler VPX AWS Marketplace エディションの 3G および 5G で SR-IOV がデフォルトで有効になっているネットワークインターフェイスの構成を示しています。

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

例 **2:** 次の CLI 画面キャプチャは、SR-IOV が有効になっていないネットワークインターフェイスのデフォルト設定 を示しています。

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

インターフェイスの種類を SR-IOV に変更する方法の詳細については、http://docs.aws.amazon.com/AWSEC2 /latest/UserGuide/sriov-networking.htmlを参照してください

インターフェイスタイプを SR-IOV に変更するには

- 1. AWS の上で動作している NetScaler VPX インスタンスをシャットダウンします。
- 2. ネットワークインターフェイスで SR-IOV を有効にするには、次のコマンドを AWS CLI に入力します。

\$ aws ec2 modify-instance-attribute --instance-id \\<instance _id\\> --sriov-net-support simple

3. SR-IOV が有効にされたかどうか確認するには、次のコマンドを AWS CLI に入力します。

\$ aws ec2 describe-instance-attribute --instance-id \\< instance_id\\> --attribute sriovNetSupport

例 3: AWS CLI を使用して、ネットワークインターフェイスの種類が SR-IOV に変更されました。



SR-IOV が有効になっていない場合、SriovNetSupport の値は存在しません。

例 4: 次の例では、SR-IOV サポートが有効になっていません。



4. VPX インスタンスの電源を入れます。ネットワークインターフェイスの変更されたステータスを確認するに は、CLI で「show interface summary」と入力します。

例 **5:** 次の画面キャプチャは、SR-IOV が有効になっているネットワークインターフェイスを示しています。イ ンターフェイス 10/1、10/2、10/3 で SR-IOV が有効にされています。

> :	show interface	summary		
	Interface	MTU	мас	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
3	10/3	1500	0a:de:5d:31:bf:c3	Intel 82599 10G VF Interface
4	L0/1	1500	@a:1e:2e:17:a2:37	Netscaler Loopback interface
Do	one			

これらの手順では、SR-IOV ネットワークインターフェイスを使用するように VPX インスタンスを構成する手順を完 了します。

高可用性セットアップでのSR-IOVの設定

NetScaler リリース 12.0 ビルド 57.19 以降の SR-IOV インターフェイスでは、高可用性がサポートされています。

高可用性セットアップを手動で展開した場合、または NetScaler バージョン 12.0 56.20 以前の Citrix CloudFormation テンプレートを使用して展開した場合、高可用性セットアップにアタッチされた IAM ロールには次の権限が 必要です。

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface

- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns: *
- sqs:*
- IAM: プリンシパルポリシーのシミュレーション
- IAM:GetRole

デフォルトでは、NetScaler ADC バージョン 12.0 57.19 用の Citrix CloudFormation テンプレートによって、必要な権限が IAM ロールに自動的に追加されます。

注

SR-IOV インターフェイスを使用したハイアベイラビリティのセットアップには、約 100 秒のダウンタイムが 発生します。

関連リソース:

IAM ロールの詳細については、AWS ドキュメントを参照してください。

AWS ENA での拡張ネットワークの使用を Citrix ADC VPX インスタンスで構成する

October 17, 2024

AWS で Citrix ADC VPX インスタンスを作成した後、AWS CLI を使用して、AWS Elastic Network Adapter (ENA) を使用した拡張ネットワーキングを使用するように仮想アプライアンスを構成できます。

AWS ENA と組み合わせると、拡張ネットワーキングは、より高い帯域幅、高いパケット/秒(PPS)パフォーマンス、 一貫して低いインスタンス間レイテンシーを提供します。

設定を開始する前に、次のトピックをお読みください。

- 前提条件
- 制限事項および使用上のガイドライン

ENA 対応インスタンスでは、次の HA 構成がサポートされています。

- プライベート IP アドレスは同じアベイラビリティーゾーン内で移動できます。
- Elastic IP アドレスは、アベイラビリティーゾーン間で移動できます。

AWS 上の NetScaler VPX インスタンスのアップグレード

October 17, 2024

AWS 上で動作する NetScaler VPX の EC2 インスタンスの種類、スループット、ソフトウェアエディション、およ びシステムソフトウェアをアップグレードすることができます。一部のアップグレード方法では、高可用性構成を使 用してダウンタイムを最小限に抑えることができます。

- 注
- NetScaler VPX AMI 用の NetScaler ソフトウェアの Release 10.1.e-124.1308.e 以降(ユーティリ ティライセンスおよびカスターマーライセンスを含む)では、M1 および M2 のインスタンスファミリを サポートしません。
- VPX インスタンスのサポートが変更されたため、10.1.e-124 以降のリリースから 10.1.123.x 以前のリ リースへのダウングレードはサポートされていません。
- ほとんどのアップグレードでは新規の AMI を起動する必要はなく、現在の NetScaler AMI インスタン ス上でアップグレードできます。新規の NetScaler AMI インスタンスへのアップグレードを行う場合は、 高可用性構成を使用してください。

AWS 上の NetScaler VPX インスタンスの EC2 インスタンスタイプを変更する

Release 10.1.e-124.1308.e 以降が動作する NetScaler VPX インスタンスでは、AWS コンソールで EC2 インスタンスの種類を変更できます。次の手順に従います。

- 1. VPX インスタンスを停止します。
- 2. AWS コンソールで EC2 インスタンスの種類を変更します。
- 3. インスタンスを起動します。

ただし、EC2 インスタンスの種類を M3 に変更することはできません。その場合は、NetScaler ADC ソフトウェア を 10.1.e-124 以降のリリースにアップグレードするには、まず標準の NetScaler ADC アップグレード手順()に 従って、上記の手順を実行する必要があります。

AWS での NetScaler VPX インスタンスのスループットまたはソフトウェアエディションのアップグレ ード

ソフトウェアエディション(Standard エディションから Premium エディションへのアップグレードなど)または スループット(たとえば、200 Mbps から 1000 Mbps へのアップグレードなど)をアップグレードするには、イン スタンスのライセンスによって異なります。 カスタマーライセンスの使用(自分のライセンスの持ち込み)

カスタマーライセンスを使用している場合は、Citrix Web サイトから新しいライセンスを購入してダウンロードし、 VPX インスタンスにライセンスをインストールできます。Citrix Web サイトからライセンスをダウンロードおよび インストールする方法については、『VPX ライセンスガイド』を参照してください。

ユーティリティライセンスの使用(時間単位のユーティリティライセンス)

AWS では課金ベースのインスタンスの直接アップグレードがサポートされていません。課金ベースの NetScaler VPX インスタンスのソフトウェアエディションやスループットをアップグレードする場合は、適切なライセンス およびキャパシティの新規の AMI を起動して、古いインスタンスから構成を移行します。これは、このページの [NetScaler 高可用性構成を使用して新しい NetScaler AMI インスタンスにアップグレードする] (#upgrade-to-anew-citrix-adc-ami-instance-by-using-a-citrix-adc-high-availability-configuration) サブセクションで説 明されているように、NetScaler 高可用性構成を使用することで実現できます。

AWS での NetScaler VPX インスタンスのシステムソフトウェアのアップグレード

10.1.e-124.1308.e 以降のリリースを実行している VPX インスタンスをアップグレードする必要がある場合 は、「Citrix ADC アプライアンスのアップグレードとダウングレード」の標準の Citrix ADC アップグレード手順に従 ってください。

10.1.e-124.1308.e より古いリリースを実行している VPX インスタンスを 10.1.e-124.1308.e 以降のリリースに アップグレードする必要がある場合は、まずシステムソフトウェアをアップグレードしてから、インスタンスタイプ を次のように M3 に変更します。

- 1. VPX インスタンスを停止します。
- 2. AWS コンソールで EC2 インスタンスの種類を変更します。
- 3. インスタンスを起動します。

NetScaler の高可用性構成を使用して新しい NetScaler AMI インスタンスにアップグレードする

高可用性構成を使用して新しい NetScaler AMI インスタンスにアップグレードするには、以下のタスクを実行しま す。

- AWS Marketplace で、EC2 インスタンスの種類、ソフトウェアエディション、スループット、またはソフト ウェアリリースを指定して新しいインスタンスを作成します。
- 古いインスタンス(アップグレード前)と新しいインスタンスとの間に高可用性を構成します。これにより、 古いインスタンスの構成内容が新しいインスタンスに同期されます。
- 古いインスタンスから新しいインスタンスへの強制高可用性フェールオーバーを実行します。これにより、新しいインスタンスがプライマリノードとして設定され、新しいトラフィックを受信し始めます。
- 古いインスタンスを停止して、再構成するか AWS から削除します。

前提条件と考慮すべきポイント

- AWS 上の 2 つの Citrix ADC VPX インスタンス間で高可用性がどのように機能するかを理解してください。
 AWS 上の 2 つの NetScaler VPX インスタンス間の高可用性構成の詳細については、「AWS に高可用性ペア をデプロイする」を参照してください。
- 新しいインスタンスは、古いインスタンスと同じアベイラビリティゾーン内に作成し、同じセキュリティグル ープおよびサブネットが設定されている必要があります。
- 高可用性のセットアップでは、両インスタンスのユーザーのAWS IAM (Identity and Access Management) アカウントに関連付けられたアクセスキーと秘密キーが必要です。正しいキー情報を使用して VPX インスタンスを作成しないと、高可用性のセットアップに失敗します。VPX インスタンスの IAM アカウント作成の詳細については、「前提条件」を参照してください。
 - 新しいインスタンスを作成するには EC2 コンソールを使用する必要があります。AWS の 1-Click 起動 は使用できません。これは、アクセスが許可されず、秘密キーを入力できないためです。
 - 新しいインスタンスには ENI インターフェイスが1つだけ必要です。

高可用性構成を使用して Citrix ADC VPX インスタンスをアップグレードするには、次の手順に従います。

- 1. 古いインスタンスと新しいインスタンスの間で高可用性を構成します。2 つの Citrix ADC VPX インスタンス 間で高可用性を構成するには、各インスタンスのコマンドプロンプトで次のように入力します。
 - add ha node <nodeID> <IPaddress of the node to be added>
 - save config

例:

古いインスタンスのコマンドプロンプトで、次のように入力します。

```
1 add ha node 30 192.0.2.30
2 Done
```

新しいインスタンスのコマンドプロンプトで、次のように入力します。

1 add ha node 10 192.0.2.10 2 Done

以下の点に注意してください:

- この高可用性セットアップで、古いインスタンスがプライマリノードで新しいインスタンスがセカンダ リノードになります。
- NSIP アドレスは古いインスタンスから新しいインスタンスにコピーされません。このため、アップグレード完了時に新しいインスタンスには異なる管理 IP アドレスが設定されます。
- 新しいインスタンスのnsrootアカウントパスワードは、HA 同期後に古いインスタンスのアカウント パスワードに設定されます。

AWS 上の 2 つの NetScaler VPX インスタンス間の高可用性構成の詳細については、「AWS に高可用性ペア をデプロイする」を参照してください。

2. HA フェールオーバーを強制します。高可用性構成でフェイルオーバーを強制するには、いずれかのインスタンスのコマンドプロンプトで次のように入力します。

1 force HA failover

強制フェールオーバーにより、古いインスタンスの ENI が新しいインスタンスに移行され、トラフィックが新 しいインスタンス(新しいプライマリノード)に流れます。また、古いインスタンス(新しいセカンダリノー ド)が再起動します。

次の警告メッセージが表示された場合は、N を入力して操作を中止します。

```
    [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)?
```

この警告メッセージは、2 つの VPX インスタンスのシステムソフトウェアで高可用性がサポートされていない 場合に表示されます。このため、強制フェールオーバー時に古いインスタンスの構成情報が新しいインスタン スに同期されません。

この問題に対する回避策を次に示します。

a) 古いインスタンスの NetScaler シェルプロンプトで、次のコマンドを入力して、構成ファイル (ns.conf)のバックアップを作成します。

copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp

- b) バックアップ構成ファイル (ns.conf.bkp) から次の行を削除します。
 - set ns config -IPAddress <IP> -netmask <MASK>

tcticset ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0

- c) 古いインスタンスのバックアップ構成ファイル (ns.conf.bkp) を新しいインスタンスの / nsconfig ディレクトリにコピーします。
- d) 新しいインスタンスの NetScaler シェルプロンプトで、次のコマンドを入力して、古いインスタンスの 構成ファイル (ns.conf.bkp)を新しいインスタンスにロードします。
 - batch -f /nsconfig/ns.conf.bkp
- e) 新しいインスタンスに設定を保存します。

save conifg

- f) いずれかのノードのコマンドプロンプトで、次のコマンドを入力してフェールオーバーを強制し、強制 フェールオーバー操作を確認する警告メッセージにYを入力します。
 - force ha failover

例:

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. HA 設定を削除して、2 つのインスタンスが HA 設定に含まれないようにします。これを行うには、まずセカ ンダリノードの高可用性構成を削除して、次にプライマリノードの高可用性を削除します。

2 つの NetScaler VPX インスタンス間の高可用性構成を削除するには、各インスタンスのコマンドプロンプ トで以下のコマンドを実行します。

> remove ha node \<nodeID\> 1 2 > save config

AWS 上の 2 つの VPX インスタンス間の高可用性構成の詳細については、「AWS に高可用性ペアをデプロイす る」を参照してください。

例:

古いインスタンス (新しいセカンダリノード) のコマンドプロンプトで、次のように入力します。

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

新しいインスタンス(新しいプライマリノード)のコマンドプロンプトで、次のように入力します。

1	> remove ha node 10
2	Done
3	> save config
4	Done

AWS での VPX インスタンスのトラブルシューティング

October 17, 2024

Amazon では、NetScaler VPX インスタンスへのコンソールアクセスを提供していません。トラブルシューティン グを行うには、AWS GUI を使用してアクティビティログを表示する必要があります。デバッグできるのは、ネット ワークが接続されている場合だけです。インスタンスのシステムログを表示するには、インスタンスを右クリックし て [System Log] を選択します。

NetScaler は、AWS マーケットプレイスでライセンスされた NetScaler VPX インスタンス(時間単位の料金がか かるユーティリティライセンス)を AWS 上でサポートします。サポートケースを提出するには、AWS アカウント番 号とサポート PIN コードを見つけて、NetScaler サポートに連絡してください。また、名前とメールアドレスの入力 を求められます。サポート PIN を見つけるには、VPX GUI にログオンし、システムページに移動します。

Q Search in Menu		System / System Information	
AWS	>	System	
System	\sim	5 ystern	
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	>	Time Zone 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	Ś	Last Config Saved Time Wed, 18 Dec 2019 05:41:16 UTC	
SNMP	>	Hardware Information	
AppFlow	! >		
Cluster	>	Platform NetScaler Virtual Appliance 450040	
Network	ĺ.	CPU 2305 MHZ	
Webleterface	(Host Id	
weblittenace	>	Serial no	
webFront	>	Encoded serial no	
Backup and Restore		Citrix ADC UUID	
Encryption Keys			

サポート PIN を示すシステムページの例を次に示します。

AWS に関するよくある質問

October 17, 2024

• NetScaler VPX インスタンスは AWS の暗号化されたボリュームをサポートしていますか?

暗号化と復号化はハイパーバイザーレベルで行われるため、どのインスタンスでもシームレスに機能します。 暗号化されたボリュームの詳細については、次の AWS ドキュメントを参照してください。

https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

• AWS で NetScaler VPX インスタンスをプロビジョニングする最も良い方法は何ですか?

NetScaler VPX インスタンスは、次のいずれかの方法で AWS にプロビジョニングできます。

- AWS マーケットプレイスの AWS CloudFormation テンプレート (CFT)
- NetScaler アドミニストレーター
- AWS クイックスタート
- GitHub の Citrix AWS CFT
- GitHubのCitrix Terraform スクリプト
- GitHubの Citrix Ansible プレイブック
- AWS EC2 起動ワークフロー

使用するオートメーションツールに基づいて、一覧表示されたオプションのいずれかを選択できます。

オプションの詳細については、「NetScaler VPX on AWS」を参照してください。

• AWS で NetScaler VPX インスタンスをアップグレードするには?

AWS で NetScaler VPX インスタンスをアップグレードするには、「AWS で NetScaler VPX インスタンスを アップグレードする」の手順に従って、システムソフトウェアをアップグレードするか、新しい NetScaler VPX Amazon Machine Image (AMI) にアップグレードします。

NetScaler VPX インスタンスをアップグレードする推奨される方法は、ジョブを使用した NetScaler インス タンスのアップグレードの手順に従って、ADM サービスを使用することです。

- AWS での NetScaler VPX の HA フェイルオーバー時間はどれくらいですか?
 - AWS アベイラビリティーゾーン内での NetScaler VPX の高可用性フェイルオーバーには約3秒かかり ます。
 - AWS アベイラビリティーゾーン全体の NetScaler VPX の HA フェイルオーバーには、約5秒かかります。
- テクニカルサポート PIN を提供する NetScaler VPX マーケットプレイスのサブスクリプションをご利用の お客様には、どのレベルのサポートが提供されますか?

デフォルトでは、テクニカルサポート PIN を提供するお客様には「ソフトウェアの選択」サービスが提供され ます。

• Elastic IP デプロイメントを使用した異なるゾーンにわたる高可用性では、アプリケーションごとに複数の IPSet を作成する必要がありますか?

はい。複数の VIP が複数の EIP にマッピングされた複数のアプリケーションがある場合は、複数の IPSet が 必要です。したがって、HA フェールオーバー中に、EIP のすべてのプライマリ VIP マッピングがセカンダリ (新しいプライマリ) VIP に変更されます。

• 異なるゾーン展開で高可用性で INC モードが有効になるのはなぜですか。

アベイラビリティーゾーン全体の HA ペアは、異なるネットワークにあります。HA 同期の場合、ネットワーク構成を同期してはいけません。これは、HA ペアで INC モードを有効にすることによって実現されます。

 アベイラビリティーゾーンが同じ VPC 内にある場合、あるアベイラビリティーゾーンの HA ノードは、別の アベイラビリティーゾーンのバックエンドサーバーと通信できますか。

はい。同じ VPC の異なるアベイラビリティーゾーンにあるサブネットには、SNIP 経由でバックエンドサーバ ーのサブネットを指す追加のルートを追加することで到達できます。たとえば、AZ1 の ADC の SNIP サブネ ットが 192.168.3.0/24、AZ2 のバックエンドサーバーのサブネットが 192.168.6.0/24 の場合、AZ1 に存在 する NetScaler アプライアンスに 192.168.6.0 255.255.0 192.168.3.1 としてルートを追加する必要があ ります。

• Elastic IP を使用した異なるゾーン間の高可用性 と プライベート IP を使用した異なるゾーン間の高可用性 のデプロイメントは連携して機能しますか?

はい、両方の設定を同じ HA ペアに適用できます。

プライベート IP デプロイメントを使用した異なるゾーン間の高可用性において、VPC 内に複数のルート テーブルを持つ複数のサブネットがある場合、HA ペアのセカンダリ ノードは、HA フェイルオーバー中にチェックされるルート テーブルをどのように認識するのでしょうか。

セカンダリノードはプライマリ NIC を認識し、VPC 内のすべてのルートテーブルを検索します。

• AWS で VPX のデフォルトイメージを使用する場合の/varパーティションのサイズはどれくらいですか? ディスク容量を増やすには?

ディスクイメージを小さく保つために、ルートディスクのサイズは 20 GB に制限されています。

/var/core/または/var/crash/ディレクトリ領域を増やす場合は、追加のディスクを接続します。 /varサイズを大きくするには、現在のところ、重要なコンテンツを新しいディスクにコピーした後、追加の ディスクを接続して/varにシンボリックリンクを作成する必要があります。

• **vCPU** にアクティブ化され、割り当てられるパケットエンジンは何台ありますか。

パケットエンジン(PE)は、ライセンスされた vCPU の数によって制限されます。NetScaler デーモンは特定の vCPU に固定されず、非 PE vCPU で実行される可能性があります。AWS によると、C5.9xLarge は 72GB のメモリを持つ 36vCPU インスタンスです。プールライセンスでは、NetScaler VPX インスタンスが最大数の PE でデプロイされます。この場合、19 PE がコア 1 ~19 で実行されます。ただし、ADC 管理プロセスは CPU 20~31 から実行されます。

- ADC の適切な AWS インスタンスを決定するには?
 - 1. スループット、PPS、SSL 要件、平均パケットサイズなどのユースケースと要件を理解します。
 - 2. VPX 帯域幅オファリングや vCPU ベースのライセンスなど、要件を満たす適切な ADC 製品とライセン スを選択します。
 - 3. 選択したオファリングに基づいて、AWS インスタンスを決定します。

例

5 Gbps ライセンスでは、5 つのデータパケットエンジンが有効になります。したがって、vCPU 要件は6(管理の場合は5+1)です。ただし、6 つの vCPU インスタンスは利用できません。したがって、5 Gbps の帯域幅をサポートするネットワークを選択すれば、8 vCPU はそのスループットに到達するのに十分です。たとえば、5 Gbps のライセンスの最大 PE 割り当てを有効にするには、5 Gbps 帯域幅ライセンスに m5.2xlargeを選択する必要があります。ただし、スループットによって制限されない vCPU ライセンスを使用すると、m5.xlarge インスタンス自体を使用して 5 Gbps のスループットが得られる可能性があります。

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

• AWS の ADC には 3 つの NIC 3 サブネットのデプロイメントが必須ですか?

Three NICs-three subnets は、管理、クライアント、およびサーバーネットワーク用の推奨展開です。この 展開により、トラフィックの分離と VPX パフォーマンスが向上します。2 つの NIC-2 サブネット、および 1 つの nic-One サブネットは、他の使用可能なオプションです。AWS で複数の NIC でサブネットを共有する (2 つの NIC と 1 つのサブネットの展開など) ことは推奨されません。このシナリオでは、非対称ルーティング などのネットワークの問題が発生する可能性があります。詳細については、「AWS でネットワークインターフ ェイスを設定するためのベストプラクティス」を参照してください。

 インスタンスのネットワーク機能に関係なく、AWS の ENA ドライバーが常に 1Gbps (1/1) のリンク速度を 示すのはなぜですか?

AWS Elastic Network Adapter (ENA) の報告された速度は、選択したインスタンスタイプに関係なく、 1Gbps (1/1) と表示されることが多いです。これは、表示される速度が実際のネットワーク パフォーマンス を直接反映するものではないためです。従来のネットワーク インターフェイスとは異なり、ENA の速度はイ ンスタンスの要件とワークロードに基づいて動的にスケーリングできます。実際のネットワーク パフォーマン スは、主にインスタンスのタイプとサイズによって決まります。したがって、実際のネットワーク スループッ トは、特定のインスタンスの種類と現在のネットワーク負荷によって大きく異なる可能性があります。

Microsoft Azure で NetScaler VPX インスタンスを展開する

March 20, 2025

NetScaler VPX インスタンスを Microsoft Azure Resource Manager (ARM) にデプロイすると、次の機能セットの両方を使用してビジネスニーズを満たすことができます。

- Azure クラウドコンピューティング機能
- NetScaler の負荷分散とトラフィック管理機能

NetScaler VPX インスタンスは、スタンドアロンインスタンスとして、またはアクティブ/スタンバイモードの高可 用性ペアとして ARM にデプロイできます。

NetScaler VPX インスタンスを Microsoft Azure にデプロイするには、次の 2 つの方法があります。

- Azure マーケットプレイスを通じて。NetScaler VPX 仮想アプライアンスは、Microsoft Azure Marketplace でイメージとして使用することができます。
- GitHub で入手可能な NetScaler Azure Resource Manager (ARM) json テンプレートを使用する。詳細に ついては、NetScaler ソリューションテンプレートの GitHub リポジトリを参照してください。

注

Azure は、Azure の外部から発信されるトラフィックへのアクセスを制限し、ブロックします。アクセスを提供するには、パブリック IP アドレスがアタッチされている VM の NIC に接続されているネットワークセキュ リティグループにインバウンドルールを追加して、サービスまたはポートを有効にします。詳細については、イ ンバウンド NATルールに関する Azure ドキュメントを参照してください。

前提要件

NetScaler VPX インスタンスを Azure にデプロイする前に、ある程度の前提知識が必要です。

- Azure の用語とネットワークの詳細に精通しています。詳細については、Azure の用語を参照してください。
- NetScaler ネットワークに関する知識。ネットワーキング トピックを参照してください。
- NetScaler アプライアンスに関する知識。ネットワーク トピックを参照してください。

NetScaler VPX インスタンスが Azure 上で動作する仕組み

オンプレミス展開では、NetScaler VPX インスタンスは、少なくとも次の3つのIP アドレスを必要とします。

- 管理 IP アドレス。NSIP アドレスと呼ばれます。
- ・ サーバーファームとやり取りするためのサブネット IP(SNIP)アドレス
- クライアント要求を受け付ける仮想サーバー IP (VIP) アドレス

詳しくは、「Microsoft Azure 上の NetScaler VPX インスタンスのネットワークアーキテクチャ」を参照してくださ い。

注

NetScaler VPX インスタンスは Intel プロセッサと AMD プロセッサの両方をサポートします。VPX 仮想アプ ライアンスは、2 つ以上の仮想コアと 2 GB を超えるメモリを備えた任意のインスタンスタイプにデプロイでき ます。システム要件の詳細については、NetScaler VPX のデータシートを参照してください。

Azure 環境では、次の3つの方法で Azure 上に NetScaler VPX インスタンスをプロビジョニングできます。

- マルチ NIC マルチ IP アーキテクチャ
- ・ シングル NIC マルチ IP アーキテクチャ
- 単一の NIC シングル IP

ニーズに応じて、これらのサポートされているアーキテクチャタイプのいずれかを使用できます。

マルチ NIC マルチ IP アーキテクチャ

このデプロイタイプでは、VPX インスタンスに複数のネットワークインターフェイス (NIC) をアタッチできます。 NIC には、静的または動的パブリック IP アドレスとプライベート IP アドレスを 1 つ以上割り当てることができま す。

詳細については、次のユースケースを参照してください:

- 複数の IP アドレスと NIC を使用して高可用性設定を構成する
- PowerShell コマンドを使用して複数の IP アドレスと NIC を使用して高可用性セットアップを構成する

注

Azure 環境で MAC が移動したり、インターフェイスがミュートされたりしないように、NetScaler VPX イン スタンスのデータインターフェイス(タグなし)ごとに VLAN を作成し、NIC のプライマリ IP を Azure にバ インドすることを Citrix では推奨しています。詳細については、CTX224626 の記事を参照してください。

シングル NIC マルチ IP アーキテクチャ

この展開タイプでは、複数の IP 構成(静的または動的パブリック IP アドレスおよびプライベート IP アドレスに割り 当てられている)に関連付けられた 1 つのネットワークインターフェイス(NIC)。詳細については、次のユースケー スを参照してください:詳細については、次のユースケースを参照してください:

- NetScaler VPX スタンドアロンインスタンスに複数の IP アドレスを構成する
- PowerShell コマンドを使用して、NetScaler VPX スタンドアロンインスタンスに複数の IP アドレスを構成 する

単一の NIC シングル IP

この展開タイプでは、単一の IP アドレスに関連付けられた 1 つのネットワークインターフェイス(NIC)で、NSIP、 SNIP、および VIP の機能を実行するために使用されます。

詳細については、「NetScaler VPX スタンドアロン インスタンスの構成」を参照してください。

注

単一 IP モードは Azure 展開環境でのみ使用することができます。このモードは、オンプレミス、AWS、また はその他の種類の展開にある NetScaler VPX インスタンスでは使用できません。

NetScaler VPX ライセンス

Azure 上の NetScaler VPX インスタンスには、有効なライセンスが必要です。Azure 上で実行される NetScaler VPX インスタンスで使用できるライセンスオプションは次のとおりです。

- ライセンス持ち込み (BYOL): BYOL オプションを使用するには、次の手順を実行します。
 - NetScaler Web サイトのライセンスポータルを使用して、有効なライセンスを生成します。
 - 生成されたライセンスをインスタンスにアップロードします。
- NetScaler VPX チェックインおよびチェックアウトライセンス: このライセンス モデルでは、使用可能なラ イセンスのプールからライセンスをチェックアウトし、不要になったときに再度チェックインできます。詳細 および詳細な手順については、以下を参照してください。NetScaler VPX チェックインおよびチェックアウ トライセンス.

注

- サブスクリプションベースのライセンスは、Azure上のNetScaler VPX インスタンスではサポートされ なくなりました。
- NetScaler VPX インスタンスで構成を変更する前にウォームリスタートを行い、正しい NetScaler VPX ライセンスを有効にします。

VPX のパフォーマンスと推奨される Azure インスタンスの種類

必要な VPX パフォーマンスを得るには、次の Azure インスタンス タイプが推奨されます。

VPX パフォ	Azure インスタンス タイプ
ーマンス	VPX1 VPX最大8
	NIC/2 NIC VPX3 NIC NIC
最大 200	Standard_D2 Stav5 dard_D8標準5
Mbps	_D16_v5
最大	Standard_D4 S tan5dard_D8標準5
1Gbps	_D16_v5
最大	Standard_D8 sitsa_nd5 ard_D8 sitsa_nd5 ard_DS sit<u>a</u>n2dard_D8sitsa_nd5ard_D8sitsa_nd5ard_DS標準2
5Gbps	_D16_v5
最大	Standard_D8 <u>St</u> av5dard_D8標準5
10Gbps	_D16_v5

注意事項

- Azure は最大 10 Gbps の VPX スループットをサポートします。詳しくは、NetScaler VPX のデータシート を参照してください。
- 1 Gbps を超えるスループットの NetScaler VPX インスタンスで最適なパフォーマンスを実現するには、 Azure の高速ネットワークを有効にする必要があります。この目的のために、高速ネットワークをサポート

する Azure インスタンスの種類を使用することをお勧めします。高速ネットワークの構成の詳細について は、「Azure 高速ネットワークを使用するように NetScaler VPX インスタンスを構成する」を参照してくだ さい。

- NetScaler VPX 仮想マシンを任意のタイミングでシャットダウンし、一時的に割り当てを解除しなければな らないことが予想される場合は、仮想マシンの作成時に静的内部 IP アドレスを割り当てます。静的内部 IP ア ドレスを割り当てないと、Azure が再起動のたびに異なる IP アドレスを仮想マシンに割り当てる可能性があ り、仮想マシンにアクセスできなくなる場合があります。
- Citrix Virtual Apps and Desktops の導入では、VPX インスタンス上の VPN 仮想サーバーを次のモードで 構成できます:
 - 基本モード。ICAOnly VPN 仮想サーバーパラメーターが ON に設定されます。基本モードは、ライ センスされていない NetScaler VPX インスタンスでも完全に動作します。
 - SmartAccess モード。ICAOnly VPN 仮想サーバーパラメーターが OFF に設定されています。
 SmartAccess モードは、ライセンスのない NetScaler VPX インスタンス上の5人の NetScaler AAA セッションユーザーに対してのみ機能します。
 - 注

SmartControl 機能を設定するには、NetScaler VPX インスタンスにプレミアムライセンスを適用す る必要があります。

Azure における NetScaler VPX インスタンスの IPv6 サポート

NetScaler VPX スタンドアロンインスタンスは、Azure の IPv6 アドレスをサポートします。IPv6 アドレスは、 Azure クラウドの NetScaler VPX スタンドアロンインスタンスで VIP アドレスと SNIP アドレスとして構成できま す。

Azure で IPv6 を有効にする方法については、次の Azure ドキュメントを参照してください。

- Azure 仮想ネットワークの IPv6 とは何ですか?
- Azure 仮想ネットワークの IPv4 アプリケーションに IPv6 を追加する-Azure CLI
- 住所の種類

NetScaler アプライアンスが IPv6 をサポートする方法については、「インターネット プロトコル バージョン 6」を 参照してください。

IPv6の制限事項:

- NetScaler の IPv6 環境では現在、Azure バックエンドの自動スケーリングはサポートされていません。
- IPv6 は NetScaler VPX HA 展開ではサポートされていません。

制限事項

NetScaler VPX 負荷分散ソリューションを ARM で実行すると、次の制限があります。

- Azure アーキテクチャでは、以下の NetScaler 機能をサポートしていません。
 - Gratuitous ARP (GARP)
 - L2 モード
 - タグ付き VLAN
 - 動的ルーティング
 - 仮想 MAC
 - USIP
 - クラスタリング
- スループットが3 Gbps を超える NetScaler VPX インスタンスを使用する場合、実際のネットワーク スルー プットはインスタンスのライセンスで指定されたスループットと一致しない可能性があります。ただし、SSL スループットや SSL トランザクション/秒など、その他の機能が向上する可能性があります。
- 仮想マシンのプロビジョニング中に Azure によって生成されたデプロイ ID は、ARM のユーザーには表示されません。デプロイ ID を使用して NetScaler VPX アプライアンスを ARM にデプロイすることはできません。

Azure 用語集

October 17, 2024

NetScaler VPX Azure のドキュメントで使用されている Azure 用語の一部を以下に示します。

- Azure ロードバランサー—Azure ロードバランサーは、ネットワーク内のコンピューター間で着信トラフィッ クを分散するリソースです。トラフィックは、ロードバランサーセット内に定義された仮想マシンに分配され ます。ロードバランサーには、外部ロードバランサー、インターネットに接続するロードバランサー、または 内部ロードバランサーがあります。
- 2. Azure Resource Manager (ARM) —ARM は、Azure のサービスの新しい管理フレームワークです。Azure Load Balancer は、ARM ベースの API およびツールを使用して管理されます。
- 3. バックエンドアドレスプール—負荷が分散される仮想マシンの NIC (NIC) に関連付けられた IP アドレスです。
- 4. BLOB-バイナリラージオブジェクト—Azure ストレージに格納できるファイルまたはイメージのようなバイ ナリオブジェクト。
- 5. フロントエンド IP 構成—Azure ロードバランサーには、仮想 IP (VIP) とも呼ばれる 1 つ以上のフロントエン ド IP アドレスを含めることができます。これらの IP アドレスがトラフィックの入口として使用されます。

 インスタンスレベルのパブリック IP (ILPIP) –ILPIP は、仮想マシンまたはロールインスタンスが存在するク ラウドサービスではなく、仮想マシンまたはロールインスタンスに直接割り当てることができるパブリック IP アドレスです。これは、クラウドサービスに割り当てられた VIP (仮想 IP) に代わるものではありません。こ れは、仮想マシンまたはロールインスタンスに直接接続するために使用できる追加の IP アドレスです。

注

以前は、ILPIP は PIP (パブリック IP) と呼ばれていました。

- インバウンド NAT ルールーロードバランサーのパブリックポートを、バックエンドアドレスプール内の特定の仮想マシンのポートにマッピングするルールが含まれます。
- IP-Config: 個々の NIC に関連付けられた IP アドレスのペア (パブリック IP とプライベート IP) として定義 できます。IP-Config では、パブリック IP アドレスが NULL の場合があります。各 NIC には、最大 255 まで の IP 構成を関連付けることができます。
- 9. 負荷分散ルール:特定のフロントエンド IP とポートの組み合わせを、バックエンド IP アドレスとポートの組み合わせのセットにマップする規則プロパティ。ロードバランサーリソースの単一の定義を使用して複数のロードバランサー規則を定義でき、その各規則は、フロントエンド IP およびポートと、仮想マシンに関連付けられたバックエンド IP およびポートの組み合わせを示します。



- 10. ネットワークセキュリティグループー仮想ネットワーク内の仮想マシンインスタンスへのネットワークトラフィックを許可または拒否するアクセス制御リスト (ACL) ルールのリストが含まれます。NSG は、サブネット、またはそのサブネット内の個々の仮想マシンインスタンスに関連付けることができます。ネットワークセキュリティグループがサブネットに関連付けられている場合、ACL ルールはそのサブネット内のすべての仮想マシンインスタンスに適用されます。さらに、ネットワークセキュリティグループをその仮想マシンに直接関連付けることで、個々の仮想マシンへのトラフィックをさらに制限できます。
- プライベート IP アドレス–Azure 仮想ネットワーク内の通信に使用され、VPN Gateway を使用してネット ワークを Azure に拡張するときのオンプレミスネットワークで使用されます。プライベート IP アドレスを 使用すると、Azure リソースは、VPN ゲートウェイまたは ExpressRoute 回路を経由して、インターネッ トで到達できる IP アドレスを使用せずに、仮想ネットワークまたはオンプレミスネットワーク内の他のリソ ースと通信できます。Azure Resource Manager 展開モデルでは、プライベート IP アドレスは次の種類の Azure リソースに関連付けられます - 仮想マシン、内部ロードバランサー(ILB)、およびアプリケーションゲ ートウェイ。
- 12. Probes –これには、バックエンドアドレスプール内の仮想マシンインスタンスの可用性をチェックするため に使用されるヘルスプローブが含まれます。個別の仮想マシンが一定時間ヘルスプローブに応答しない場合、 それはトラフィック供用から除外されます。プローブを使用すると、仮想インスタンスのヘルスを追跡できま す。ヘルスプローブが失敗した場合、仮想インスタンスはローテーションから自動的に除外されます。
- パブリック IP アドレス (PIP) PIP は、Azure のパブリック向けサービスを含むインターネットとの通信に 使用され、仮想マシン、インターネット向けロードバランサー、VPN ゲートウェイ、およびアプリケーション ゲートウェイに関連付けられます。
- 14. リージョン-国境を越えず、1つ以上のデータセンターを含む地理内のエリア。価格設定、地域サービスおよび タイプは、リージョンレベルで公開されます。リージョンは通常、(最大で数百マイル離れた)別のリージョン と対にされ、リージョンペアを形成します。障害回復シナリオおよび高可用性シナリオでは、リージョンペア をメカニズムとして使用できます。また、一般に場所とも呼ばれます。
- リソースグループ-リソースマネージャのコンテナは、アプリケーションに関連するリソースを保持します。リ ソースグループには、アプリケーションのリソースをすべて含めることも、論理的にグループにまとめられた リソースだけを含めることもできます。
- ストレージアカウント–Azure ストレージアカウントを使用すると、Azure Storage の Azure BLOB、キュ ー、テーブル、およびファイルサービスにアクセスできます。ストレージアカウントは、Azure ストレージデ ータオブジェクトに一意の名前空間を提供します。
- 17. 仮想マシン-オペレーティングシステムを実行する物理コンピュータのソフトウェア実装。同じハードウェア 上で複数の仮想マシンを同時に実行できます。Azure には、いろいろなサイズの仮想マシンが用意されていま す。
- 18. 仮想ネットワーク-Azure 仮想ネットワークは、クラウド内の独自のネットワークを表現したものです。それ はサブスクリプション専用の Azure クラウドの論理的隔離です。IP アドレスブロック、DNS 設定、セキュリ ティポリシー、およびこのネットワーク内のルートテーブルを全面的に制御できます。さらに VNet のサブネ ットに分割したり、Azure IaaS 仮想マシンおよびクラウドサービス(PaaS ロールインスタンス)を起動した

りすることもできます。また、Azure で利用できる接続性オプションの1つを使用して、仮想ネットワークを オンプレミスネットワークに接続できます。本質的には、Azure が提供するエンタープライズスケールの利点 を持つ IP アドレスブロック上の全面的なコントロールを使用して、ネットワークを Azure に拡張できます。



Microsoft Azure 上の **NetScaler ADC VPX** インスタンスのネットワークアーキテク チャ

October 17, 2024

Azure Resource Manager (ARM) では、NetScaler VPX 仮想マシン (VM) は仮想ネットワークに存在します。仮 想ネットワークの特定のサブネットに単一のネットワークインターフェイスを作成でき、VPX インスタンスに接続で きます。ネットワークセキュリティグループを使用して、Azure 仮想ネットワーク内の VPX インスタンスとの間の ネットワークトラフィックをフィルタリングできます。ネットワークセキュリティグループには、VPX インスタンス へのインバウンドネットワークトラフィックまたは VPX インスタンスからのアウトバウンドネットワークトラフィ ックを許可または拒否するセキュリティルールが含まれています。詳細については、「セキュリティグループ」を参照 してください。

ネットワークセキュリティグループは、NetScaler VPX インスタンスへの要求をフィルタリングし、VPX インスタ ンスはそれらをサーバーに送信します。サーバーからの応答は、逆の順序で同じパスをたどります。ネットワークセ キュリティグループは、単一の VPX VM をフィルタリングするように構成することも、サブネットと仮想ネットワー クを使用して、複数の VPX インスタンスを展開するトラフィックをフィルタリングすることもできます。

NIC には、ネットワーク構成の詳細(仮想ネットワーク、サブネット、内部 IP アドレス、パブリック IP アドレスな ど)が含まれます。

ARM では、単一の NIC と 1 つの IP アドレスでデプロイされた仮想マシンにアクセスするために使用される、次の IP アドレスを知っておくとよいでしょう。

- パブリック IP(PIP)アドレスは、NetScaler VMの仮想 NIC上で直接構成されるインターネット側 IP アドレスです。これにより、外部ネットワークから VMに直接アクセスできます。
- NetScaler IP(NSIP とも呼ばれる)アドレスは、仮想マシン上で構成された内部 IP アドレスです。これは ルーティング不可能です。
- 仮想 IP アドレス(VIP)は、NSIPとポート番号を使用して構成されます。クライアントは PIP アドレスから NetScaler サービスにアクセスし、要求が NetScaler VPX VM または Azure ロードバランサーの NIC に到 達すると、VIP が内部 IP(NSIP)および内部ポート番号に変換されます。
- ・内部 IP アドレスは、仮想ネットワークのアドレス空間プールにある、VM のプライベート内部 IP アドレスです。この IP アドレスは、外部ネットワークから到達できません。この IP アドレスは、静的に設定しない限り、デフォルトで動的です。インターネットからのトラフィックは、ネットワークセキュリティグループで作成されたルールに従って、このアドレスにルーティングされます。ネットワークセキュリティグループは NIC と統合して、仮想マシンで設定されたサービスに応じて、適切なタイプのトラフィックを NIC の適切なポートに選択的に送信します。

以下の図は、ARM でプロビジョニングされた NetScaler VPX インスタンスを介したクライアントからサーバーへの トラフィックフローを示しています。



ネットワークアドレス変換によるトラフィックフロー

NetScaler VPX インスタンス(インスタンスレベル)のパブリック IP(PIP)アドレスをリクエストすることもできます。この直接 PIP を VM レベルで使用する場合、ネットワークトラフィックを傍受する受信および送信規則を定義する必要はありません。インターネットからの着信要求が VM で直接受信されます。Azure はネットワークアドレス変換(NAT)を実行し、VPX インスタンスの内部 IP アドレスにトラフィックを転送します。

以下の図は、Azure がネットワークアドレス変換を実行し、NetScaler 内部 IP アドレスをマップする方法を示して います。



この例では、ネットワークセキュリティグループに割り当てられたパブリック IP は 140.x.x.x で、内部 IP アドレス は 10.x.x.x です。インバウンドルールとアウトバウンドルールが定義されている場合、パブリック HTTP ポート 80 はクライアントリクエストを受信するポートとして定義され、対応するプライベートポート 10080 は NetScaler ADC VPX インスタンスがリッスンするポートとして定義されます。クライアント要求はパブリック IP アドレス 140.x.x.x で受信されます。Azure がネットワークアドレス変換を実行して、PIP を内部 IP アドレス 10.x.x.x (ポー ト 10080) にマップし、クライアント要求を転送します。

注

高可用性における NetScaler VPX VM は、自身に定義された受信規則により負荷分散トラフィックを制御す る、外部または内部のロードバランサーによって制御されます。外部トラフィックは最初にこれらのロードバ ランサによって代行受信され、トラフィックは設定されたロードバランシング規則に従って迂回されます。ロ ードバランサには、バックエンドプール、NAT ルール、および健全性プローブが定義されています。

ポートの使用に関する注意事項

NetScaler VPX インスタンスの作成中または仮想マシンのプロビジョニング後に、ネットワークセキュリティグル ープでより多くのインバウンドルールとアウトバウンドルールを構成できます。各受信および送信規則は、パブリッ クポートおよびプライベートポートに関連付けられています。 ネットワークセキュリティグループルールを設定する前に、使用できるポート番号に関する次のガイドラインに注意 してください。

1. NetScaler VPX インスタンスは次のポートを予約します。インターネットからの要求にパブリック IP アドレ スを使用する場合、これらをプライベートポートとして定義することはできません。

 $\pi - F 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.$

ただし、VIP などのインターネットに直接接続するサービスで標準ポート(ポート 443 など)を使用する場合 は、ネットワークセキュリティグループを使用してポートマッピングを作成する必要があります。これにより、 標準ポートがこの VIP サービス用に NetScaler で構成された別のポートにマップされます。

たとえば、VIP サービスが VPX インスタンスのポート 8443 で実行されているが、パブリックポート 443 に マッピングされているとします。したがって、ユーザーがパブリック IP を介してポート 443 にアクセスする と、要求はプライベートポート 8443 に送信されます。

- 2. パブリック IP アドレスでは、ポートマッピングが動的に解放される、パッシブ FTP や ALG のようなプロト コルをサポートしていません。
- 3. 高可用性は、Azure ロードバランサーで構成された PIP ではなく、VPX インスタンスに関連付けられたパブ リック IP アドレス (PIP) を使用するトラフィックでは機能しません。
- 注

Azure Resource Manager では、NetScaler VPX インスタンスにはパブリック IP アドレス (PIP) と内部 IP アドレスの 2 つの IP アドレスが関連付けられています。外部トラフィックは PIP に接続しますが、内部 IP ア ドレスまたは NSIP はルーティング不可能です。VPX で VIP を設定するには、内部 IP アドレスと使用可能な空 きポートのいずれかを使用します。VIP の構成に PIP を使用してはいけません。

NetScaler VPX スタンドアロンインスタンスを構成する

January 15, 2025

仮想マシンを作成して他のリソースを構成することにより、スタンドアロンモードで Azure Resource Manager (ARM) ポータルで単一の NetScaler VPX インスタンスをプロビジョニングできます。

はじめに

お使いの環境が次の要件を満たしていることを確認してください:

- Microsoft Azure ユーザーアカウント
- Microsoft Azure Resource Manager へのアクセス

- Microsoft Azure SDK
- Microsoft Azure PowerShell

Microsoft Azure ポータルのページで、ユーザー名とパスワードを指定して Azure Resource Manager ポータル にログオンします。

注

ARM ポータルで、1 つのペインでオプションをクリックすると、右側に新しいペインが開きます。ペイン間を 移動してデバイスを構成します。

設定手順の概要

- 1. リソースグループの構成
- 2. ネットワークセキュリティグループの構成
- 3. 仮想ネットワークインターフェイスとそのサブネットの構成
- 4. ストレージアカウントの構成
- 5. 可用性セットの構成
- 6. NetScaler VPX インスタンスを構成します。

リソースグループの構成

すべてのリソースのコンテナとなる新しいリソースグループを作成します。リソースグループを使用して、リソース をグループとして展開、管理、および監視します。

- 1. 新規>管理>リソースグループをクリックします。
- 2. リソースグループペインで、次の詳細を入力します。
 - リソースグループ名
 - リソースグループの場所

3. [Create] をクリックします。



ネットワークセキュリティグループの構成

仮想ネットワーク内の着信トラフィックと発信トラフィックを制御するインバウンドルールとアウトバウンドルール を割り当てるネットワークセキュリティグループを作成します。ネットワークセキュリティグループを使用すると、 単一の仮想マシンのセキュリティルールを定義したり、仮想ネットワークサブネットのセキュリティルールを定義し たりできます。

- 1. [新規] > [ネットワーク] > [ネットワークセキュリティグループ] をクリックします。
- 2. [ネットワークセキュリティグループの作成]ペインで、次の詳細を入力し、[作成]をクリックします。
 - Name セキュリティグループの名前を入力します
 - Resource group ボックスの一覧からリソースグループを選択します

注

正しい場所を選択していることを確認します。場所が異なれば、ボックスの一覧に表示されるリソースの一覧 も異なります。

≡	_ 🗆 ×	_ = ×	×=×			
+ New	New	Networking	Network security group			
Resource groups	MARKETPLACE See all	The VPN device in your Azure virtual				
All resources	Virtual Machines	and VNet-to-VNet VPN connections.	A network security group is a layer of security that acts as a virtual firewall for controlling traffic in and out of virtual machines (via network interfaces) and subnets. It contains a set of security rules			
🕒 Recent	Web + Mobile	Local network gateway	that allow or deny inbound and outbound traffic using the following 5-tuple: protocol, source IP address range, source port range, destination IP address range, and destination port range. A			
🔕 App Services	Data + Storage	Represents the VPN device in your local network and used to set up a	network security group can be associated to multiple network interfaces and subnets, but each network interface or subnet can be associated to only one network security group.			
👼 SQL databases	Data + Analytics	site to site ven connection.	Security rules are evaluated in priority-order, starting with the lowest number rule, to determine			
Virtual machines (classic)	Internet of Things	A virtual firewall to control inbound and outbound traffic for virtual	memory dames another in 60 dot of the network interfaces of subtrest associated with the network security group. A network security group has separate inhound and outbound rules, and each rule can allow or deny traffic. Each network security group has a set of default security rules, which allows in the original security rules.			
Virtual machines	Networking	machines and subnets.	all traffic within a virtual network and outbound traffic to the internet. There is also a rule to allow traffic originating from Azure's load balancer probe. All other traffic is automatically denied. The			
Cloud services (classic)	Media + CDN	Route table	default rules can be overriden by specifying rules with a lower priority number.			
? Subscriptions	Hybrid Integration	Use route tables to control now traffic is directed in a virtual	traffic in and out of virtual machines. In the Resource Manager deployment model, traffic can be controlled by using either network security groups or load balancers with inbound NAT rules. While			
Browse >	Security + Identity		inbound NAT rules are functionally equivalent to endpoints, Azure recommends using network security groups for new deployments where NAT features (like port translation) are not required.			
blonat y	Developer Services	A load balancer that distributes	There are no additional charges for creating network security groups in Microsoft Azure.			
	Management >	incoming traffic among backend virtual machine instances.				
	Intelligence	DNS zone (preview)	Select a deployment model 🖲			
	Containers >	A DNS zone hosts DNS records for a domain.	Resource Manager			
	RECENT	PREVIEW	Create			
	Traffic Manager profile					

仮想ネットワークとサブネットを構成する

ARM の仮想ネットワークは、サービスのセキュリティを強化し、隔離するものです。同じ仮想ネットワークに属する VM およびサービスは、互いにアクセスできます。

仮想ネットワークとサブネットを作成する手順は次のとおりです。

- 1. 新規>ネットワーク>仮想ネットワークをクリックします。
- 2. [仮想ネットワーク] ペインで、展開モードが [リソースマネージャ] であることを確認し、[作成] をクリックします。



3. 仮想ネットワークの作成 ウィンドウで、次の値を入力し、作成 をクリックします。

- 仮想ネットワークの名前
- Address space 仮想ネットワークの予約済 IP アドレスブロックを入力します
- サブネット-最初のサブネットの名前を入力します (2 つ目のサブネットはこのステップの後半で作成します)
- Subnet address range サブネットの予約済 IP アドレスブロックを入力します
- Resource group ボックスの一覧から以前に作成したリソースグループを選択します。

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

2番目のサブネットを設定する

1. [すべてのリソース] ペインから新しく作成した仮想ネットワークを選択し、[設定] ペインで [サブネット] をク リックします。

	NetScalerVNet - Subnet	S						*	-	×
			Subnet	Gatev	vay subnet					
Q	Search (Ctrl+/)		Search s	ubnets						
(m)	Quentiew		NAME	^	ADDRESS RANGE	^	AVAILABLE ADDR \land	SECURITY GROUP	^	
	Activity log		NSFrontEnd		22.22.1.0/24		251	-		
	Access control (IAM)									
	Tags									
•	1995									
SETT	NGS									
<••>	Address space									
-02-	Connected devices									
$\langle \cdot \rangle$	Subnets									

- 2. +Subnet をクリックし、次の詳細を入力して 2 番目のサブネットを作成します。
 - 2 番目のサブネットの名前
 - Address range サブネットの予約済 IP アドレスブロックを入力します
 - ネットワークセキュリティグループ-ドロップダウンリストからネットワークセキュリティグループを選択します。
- 3. [**Create**] をクリックします。

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	

ストレージアカウントの構成

ARM IaaS インフラストラクチャストレージには、BLOB、表、キューおよびファイルの形式でデータを保存できる すべてのサービスが含まれます。ARM では、これらの形式のストレージデータを使用してアプリケーションを作成す ることもできます。

ストレージアカウントを作成してすべてのデータを保存します。

- 1. [+新規]>[データ]+[ストレージ]>[ストレージアカウント]をクリックします。
- 2. ストレージアカウントの作成ペインで、次の詳細を入力します。
 - アカウントの名前
 - デプロイモード-必ずリソースマネージャーを選択してください
 - アカウントの種類-ドロップダウンリストから「汎用」を選択します
 - レプリケーション-ドロップダウンリストから「ローカル冗長ストレージ」を選択します
 - Resource group ボックスの一覧から新しく作成したリソースグループを選択します

3. [Create] をクリックします。

		_ 🗖 ×		_ = ×
	New		Data + St	orage
				Data Lake Store (preview)
📦 Resource groups			4	Hyper-scale repository for big data analytic workloads
	MARKETPLACE	See all	PREVIEW	
	Virtual Machines	>		SQL Data Warehouse (preview)
🕒 Recent	Web + Mobile	>		Fully elastic, managed, and parallelized relational database.
🔇 App Services	Data + Storage	, 	PREVIEW	Analyze and scale in seconds.
👼 SOI databases				Azure DocumentDB
	Data + Analytics	/		Scalable and managed NoSQL
Virtual machines (classic)	Internet of Things			modern cloud applications.
Virtual machines	Networking	>	_	Storage account
Cloud services (classic)	Media + CDN	>		Use Blobs, Tables, Queues, and Files
	Hybrid Integration	>		storage.
💡 Subscriptions	C			
Browse >	Security + Identity			Distributed, in-memory Redis Cache
	Developer Services			service for modern cloud applications
	Management	>		
	Intelligence	>		Azure Search Search-as-a-service solution
	Containers	>		

可用性セットの構成

可用性セットにより、計画的または計画外のメンテナンスが発生した場合でも、少なくとも1つの VM が稼働し続け ることが保証されます。同じ可用性セットに属する2台以上の VM は、異なるフォールトドメインに配置されて、サ ービスの冗長性を確保します。

- 1. [+新規]をクリックします。
- 2. MARKETPLACE ペインで「すべて表示」をクリックし、「仮想マシン」をクリックします。
- 3. 可用性セットを検索し、表示されたリストから [可用性セット エンティティ]を選択します。

Aarketplace 🖉 🗕 🗶	Virtual Machines	
	Fiter	
Everything	Availability Set	
Virtual Machines		
Web + Mobile	Kesuits	
Data + Storage	NAME	PUBLISHER
Data + Analytics	availability Set	Microsoft
Internet of Things	FortiGateNGFW High Availability (HA)	Fortinet
Networking	Nongo 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. [作成]をクリックし、 [可用性セットの作成] ウィンドウで、次の詳細を入力します。
 - セットの名前
 - Resource group ボックスの一覧から新しく作成したリソースグループを選択します
- 5. [Create] をクリックします。

_ I Create availability set		×
* Name		
AvSet:	~	
Fault domains 🛛	3	
Update domains 🛛		
	5	
* Subscription		
Microsoft Azure Enterprise	~	
* Resource group ● Create new ● Use existing		
ResGroup	~	
* Location		
Southeast Asia	~	
Create		

NetScaler VPX インスタンスの構成

仮想ネットワークに NetScaler VPX のインスタンスを作成します。Azure Marketplace から NetScaler VPX イメ ージを取得し、Azure Resource Manager ポータルを使用して NetScaler VPX インスタンスを作成します。

NetScaler VPX インスタンスの作成を開始する前に、インスタンスが存在する必要なサブネットを持つ仮想ネット ワークが作成されていることを確認してください。仮想マシンのプロビジョニング時に仮想ネットワークを作成する こともできますが、柔軟性に欠けるため別のサブネットを作成することはできません。 オプションで、仮想マシンがインターネットリソースにアクセスできるようにする DNS サーバと VPN 接続を設定します。

注

プロビジョニング時にネットワーク情報を利用できるよう、NetScaler VPX VM をプロビジョニングする前に、 リソースグループ、ネットワークセキュリティグループ、仮想ネットワークおよび他のエンティティを作成す ることをお勧めします。

- 1. [+新規]>[ネットワーク]をクリックします。
- 2. [すべて表示]をクリックし、[ネットワーク]ペインで [NetScaler 13.0] をクリックします。
- 3. ソフトウェアプランのリストから「NetScaler 13.0 VPX Bring Your Own License」を選択します。

ARM ポータルでエンティティをすばやく見つける方法として、Azure Marketplace 検索ボックスにエン ティティの名前を入力して を押すこともできます <Enter>。検索ボックスに「NetScaler 」と入力して、 NetScaler イメージを検索します。

		_ D ×		* _ D ×
+ New	New		NETWO	Marketplace
	🔎 NetScaler	×	RKING	
Resource groups	ΜΔΡΚΕΤΡΙ Δ. ΓΕ	See all		
All resources				Everything
🕒 Recent	Virtual Machines			Virtual Machines
A Ci	Web + Mobile	>		
S 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	>		
	Intelligence	>		Developer Services
	Containers	>		Management
	RECENT			Intelligence
	Traffic Manager profile			Containers
	Microsoft			
	Resource group			

注

最新のイメージを選択するようにしてください。Citrix ADC イメージの名前にリリース番号が含まれて いる場合があります。

4. [NetScaler VPX 自分のライセンスを持参] ページのドロップダウンリストから [リソースマネージャー] を 選択し、[作成] をクリックします。

Create	virtual machine _		×	Basics	_ C	×
1	Basics Configure basic settings	>		* Name Citrix-NetScaler-User		2
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		2
5	Buy	>	_	Subscription Microsoft Azure Enterprise	~	2
				 Resource group • Create new • Use existing NetScalerResGroup Location Southeast Asia 	~	•
				OK		

5. [仮想マシンの作成] ウィンドウで、各セクションで必要な値を指定して、仮想マシンを作成します。各セクションで「**OK**」をクリックして設定を保存します。

ベーシック:

- Name NetScaler VPX インスタンスの名前を指定します
- VM disk type ボックスの一覧から SSD (デフォルト値)または HDD を選択します。
- User name and Password 作成したリソースグループのリソースにアクセスするためのユーザー名および パスワードを指定します
- Authentication Type [SSH Public Key] または [Password] を選択します
- Resource group ボックスの一覧から作成したリソースグループを選択します。

ここではリソースグループを作成できますが、Azure Resource Manager で[Resource groups]からリソース グループを作成して、そのグループをボックスの一覧から選択することをお勧めします

注

Azure スタック環境では、基本パラメータに加えて、次のパラメータを指定します。

- Azure スタックドメイン
- Azure スタックテナント (オプション)
- Azure クライアント (オプション)
- Azure クライアントシークレット (オプション)

サイズ:

基本設定で選択した仮想マシンのディスクタイプ、SDD、または HDD に応じて、ディスクサイズが表示されます。

• 必要に応じてディスクサイズを選択し、[選択]をクリックします。

概要:

- ・ デフォルトのディスクタイプ([Standard])を選択します
- Storage account ストレージアカウントを選択します
- Virtual network 仮想ネットワークを選択します
- Subnet サブネットアドレスを設定します
- Public IP address IP アドレス割り当ての種類を選択します
- Network security group 作成したセキュリティグループを選択します。セキュリティグループで、受信規 則および送信規則が構成されていることを確認します。
- アベイラビリティセット-ドロップダウンメニューボックスからアベイラビリティセットを選択します

設定:

構成設定が検証され、[Summary] ページに検証の結果が表示されます。検証が失敗すると、[Summary] ページ に障害の理由が表示されます。個別のセクションに戻り、必要に応じて変更します。検証に合格したら、「**OK**」をク リックします。

購入ページでオファーの詳細と法的条件を確認し、「購入」をクリックします。

購入ページでオファーの詳細と法的条件を確認し、「購入」をクリックします。

高可用性導入では、同じ可用性セットおよび同じリソースグループに NetScaler VPX 独立したインスタンスを 2 つ 作成して、アクティブ/スタンバイ構成で展開します。

NetScaler VPX スタンドアロンインスタンスに複数の IP アドレスを構成する

October 17, 2024

このセクションでは、Azure Resource Manager (ARM) で複数の IP アドレスを使用してスタンドアロン NetScaler ADC VPX インスタンスを構成する方法について説明します。VPX インスタンスには 1 つ以上の NIC を接続でき、各 NIC には 1 つ以上の静的または動的なパブリックおよびプライベート IP アドレスを割り当てることができます。複 数の IP アドレスを NSIP、VIP、SNIP などとして割り当てることができます。

詳細については、Azure のドキュメント「Azure ポータルを使用して仮想マシンに複数の IP アドレスを割り当てる」 を参照してください。

PowerShell コマンドを使用する場合は、「PowerShell コマンドを使用してスタンドアロン モードで NetScaler VPX インスタンスに複数の IP アドレスを構成する」を参照してください。

使用例

この使用例では、スタンドアロンの NetScaler ADC VPX アプライアンスは、仮想ネットワーク(VNET)に接続された単一の NIC で構成されます。NIC は、表に示すように、3 つの IP 構成(ipconfig)に関連付けられ、各サーバは異なる目的で使用されます。

IP コンフィグ	関連付けられている	目的
ipconfig1	静的パブリック IP アドレス; 静的プ	管理トラフィックを提供する
	ライベート IP アドレス	
ipconfig2	静的パブリック IP アドレス; 静的プ	クライアント側のトラフィックを提
	ライベートアドレス	供する
ipconfig3	静的プライベート IP アドレス	バックエンドサーバーと通信する

注

IPConfig-3はパブリック IP アドレスに関連付けられていません。

図: トポロジ

次の図はこの使用例を視覚的に示しています。



注

マルチ NIC、マルチ IP Azure NetScaler VPX 展開では、プライマリ(最初の)NIC のプライマリ(最初) IPConfig に関連付けられたプライベート IP が、アプライアンスの管理 NSIP として自動的に追加されま す。IPConfigsに関連付けられた残りのプライベート IP アドレスは、必要に応じて、add ns ip コマ ンドを使用して VIP または SNIP として VPX インスタンスに追加する必要があります。

はじめに

始める前に、次のリンクに示す手順に従って VPX インスタンスを作成します。

NetScaler VPX スタンドアロンインスタンスを構成する

このユースケースでは、NSDoc0330VM VPX インスタンスが作成されます。

スタンドアロンモードで、NetScaler VPX インスタンスに対して複数 IP アドレスを構成する手順。

スタンドアロンモードの NetScaler VPX アプライアンスに複数の IP アドレスを構成するには:

- 1. VM への IP アドレス追加
- 2. NetScaler が所有する IP アドレスを構成する

ステップ **1**: VM に IP アドレスを追加する

- 1. ポータルで [その他のサービス]をクリックし、フィルターボックスに「仮想マシン」と入力し、[仮想マシン] をクリックします。
- 2. 仮想マシンのブレードで、IP アドレスを追加する仮想マシンをクリックします。表示される仮想マシンブレードの [ネットワーク インターフェイス] をクリックし、ネットワークインターフェイスを選択します。

Virtual machines 💉 🗙 brahasitaramanathancitrix (Default Directory)	NSDoc0330VM - Network in	terfaces	*	×
+ Add ≣≣ Columns ひ Refresh		> Search network interfaces		
Subscriptions: Microsoft Azure Enterprise – Don't see a subscription? Switch directories	Overview	NAME ^ PUBLIC IP ADDRE ^ PRIVATE IP ADDR ^ SECURITY GROUP ^		1
nsdoc 1 itoms	Activity log	nsdoc0330vm923 13.78.187.150 192.0.0.4 NSDoc0330VM-nsg	1	
NAME V	Access control (IAM)			
NSDoc0330VM •••	🛷 Tags			
	X Diagnose and solve problems			
	SETTINGS			
	Availability set			
	😑 Disks			
	Extensions			
	Retwork interfaces			
	🚺 Size			

選択した NIC のブレードで、[IP 構成] をクリックします。仮想マシンの作成時に割り当てられた既存の IP 構成、 ipconfig1 が表示されます。この使用例では、ipconfig1 に割り当てられている IP アドレスが静的アドレスである ことを確認します。次に、さらに 2 つの IP 構成、ipconfig2(VIP)と ipconfig3(SNIP)を作成します。

さらにipconfigsを作成するには、Add を作成します。

nsdoc0330vm923 - IP config Network interface	jurations	
Search (Ctrl+/)	➡ Add 🕞 Save 🗙 Discard	
 Overview Activity log Access control (IAM) 	IP forwarding settings IP forwarding Virtual network	
P Tags	IP configurations * Subnet	
SETTINGS		
IP configurations	Search IP configurations	IP VERSION
DNS servers		
Network security group	ipconfig1	IPv4
Properties		

[**IP** 構成の追加] ウィンドウで、[名前] を入力し、割り当て方法として [静的] を指定し、IP アドレス (このユースケー スでは 192.0.0.5) を入力し、[パブリック **IP** アドレス] を有効にします。

注

静的なプライベート IP アドレスを追加する前に、IP アドレスの可用性をチェックし、その IP アドレスが、NIC の接続先と同じサブネットに属していることを確認します。

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

次に、[必要な設定の構成]をクリックして ipconfig2 の静的パブリック IP アドレスを作成します。

デフォルトでは、パブリック IP アドレスは動的なアドレスです。VM に常に同じパブリック IP アドレスを使用させるために、静的なパブリック IP アドレスを作成します。

「パブリック IP アドレスの作成」ブレードで「名前」を追加し、「割り当て」で「静的」をクリックします。[**OK**] をクリックします。

Create public IP address	
* Name PIP2	~
Assignment Dynamic Static	
OK	

注

割り当て方式を静的に設定している場合でも、パブリック IP リソースに割り当てられる実際の IP アドレスを 指定することはできません。代わりに、リソースが作成された Azure の場所で利用可能な IP アドレスプールか ら割り当てられます。

手順に従って、もう1つの IP 構成 ipconfig3 を追加します。パブリック IP アドレスは必須ではありません。

Search IP con	earch 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)	

手順 2: NetScaler 固有の IP アドレスの構成

GUI またはadd ns ipコマンドを使用して、NetScaler が所有する IP アドレスを設定します。詳細について は、「Citrix ADC 所有の IP アドレスの構成」を参照してください。

複数の IP アドレスと NIC を使用して高可用性設定を構成する

April 1, 2025

Microsoft Azure デプロイメントでは、Azure ロードバランサー(ALB)を使用して、2 つの NetScaler VPX イン スタンスの高可用性構成を実現します。これは、ALB でヘルスプローブを構成することによって実現されます。ALB は、プライマリインスタンスとセカンダリインスタンスの両方に 5 秒ごとにヘルスプローブを送信することで、各 VPX インスタンスを監視します。

この設定では、プライマリノードだけがヘルスプローブに応答し、セカンダリノードは応答しません。プライマリが ヘルスプローブに応答を送信すると、ALB はインスタンスへのデータトラフィックの送信を開始します。プライマリ インスタンスが2回連続してヘルスプローブに失敗した場合、ALB はトラフィックをそのインスタンスにリダイレク トしません。フェイルオーバー時は、新しいプライマリがヘルスプローブへの応答を開始し、ALB はそのプライマリ にトラフィックをリダイレクトします。標準の VPX 高可用性フェイルオーバー時間は3秒です。トラフィックスイッ チングにかかる合計フェールオーバー時間は、最大13秒です。

Azure のアクティブ/パッシブ高可用性(HA)セットアップで、複数の NIC を持つ一対の NetScaler VPX インスタンスを展開できます。各 NIC に複数の IP アドレスを設定できます。

マルチ NIC の高可用性導入では、次のオプションを使用できます。

- Azure 可用性セットを使用した高可用性
- Azure アベイラビリティーゾーンを使用した高可用性

Azure アベイラビリティセットとアベイラビリティーゾーンの詳細については、Azure のドキュメント「Linux 仮想 マシンの可用性の管理」を参照してください。

可用性セットを使用した高可用性

可用性セットを使用した高可用性セットアップは、次の要件を満たす必要があります。

- HA Independent Network Configuration (INC) 構成
- Direct Server Return (DSR) モードの Azure Load Balancer (ALB)

すべてのトラフィックはプライマリノードを通過します。セカンダリノードは、プライマリノードが失敗するまでス タンバイモードを維持します。

注

Azure クラウド上の NetScaler VPX 高可用性デプロイが機能するには、2 つの VPX ノード間で移動できるフ ローティングパブリック IP (PIP) が必要です。Azure ロードバランサー (ALB) は、フローティング PIP を提 供します。このフローティング PIP は、フェールオーバーが発生した場合に自動的に第 2 ノードに移動されま す。



図:Azure 可用性セットを使用した高可用性デプロイアーキテクチャの例 **Resource Group**

アクティブ/パッシブ展開では、ALB フロントエンドパブリック IP (PIP) アドレスが各 VPX ノードに VIP アドレス として追加されます。HA-INC 構成では、これらの VIP アドレスはフローティングされ、SNIP アドレスはインスタ ンス固有のアドレスとなります。

VPX ペアをアクティブ/パッシブ高可用性モードでデプロイするには、次の2つの方法があります:

- NetScaler VPX 標準高可用性テンプレート: このオプションを使用して、3 つのサブネットと6 つの NIC の デフォルトオプションで HA ペアを構成します。
- Windows PowerShell コマンド: このオプションを使用して、サブネットと NIC の要件に応じて HA ペア を構成します。

このトピックでは、Citrix テンプレートを使用してアクティブ/パッシブ HA セットアップで VPX ペアを展開する方 法について説明します。PowerShell コマンドを使用する場合は、「PowerShell コマンドを使用して複数の IP アド レスと NIC で HA セットアップを構成する」を参照してください。

NetScaler の高可用性テンプレートを使用して HA-INC ノードを構成する

標準テンプレートを使用すると、一対の VPX インスタンスを HA-INC モードで迅速かつ効率的にデプロイできます。 このテンプレートでは、3 つのサブネットと 6 つの NIC を持つ 2 つのノードが作成されます。各サブネットには、両 方の VPX インスタンスに対して 2 つの NIC があります。 NetScaler HA ペアテンプレートは、Azure マーケットプレイスで入手できます。

次の手順を実行して、Azure 可用性セットを使用して、テンプレートを起動し、高可用性 VPX ペアをデプロイしま す。

1. Azure Marketplace から NetScaler を検索します。



- 2. [今すぐ入手]をクリックします。
- 3. 必要な HA 導入とライセンスを選択し、[続行] をクリックします。

Products > NetScaler	ADC 14.1	
	NetScaler ADC 14.1 \heartsuit Save to my list	
net>scale	Create this app in Azure NetScaler ADC 14.1 By Cloud Software Group	By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be
Get It Now Pricing information Bring your own license + Azure infrastructure cost	Software plan NetScaler ADC 14.1 VPX Express - 20 Mbps	handled in accordance with the provider's terms and privacy statement.
Categories Networking Compute	Pricing: Starting at Free Details: NetSclaer ADC 14.1 VPX Express - 20 Mbps	
Support Support Help Legal	This app requires some basic profile information. You have provided the information already so you're good to go! Edit	Continue
License Agreement Privacy Policy	Key Benefits:	
	Flexible & Consistent: NetScaler ADC is the most comprehensive, fe	ature-rich ADC available across a wide

4. [基本] ページが表示されます。リソースグループを作成し、**OK** を選択します。


5. [一般設定]ページが表示されます。詳細を入力して「**OK**」を選択します。

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

注

デフォルトでは、監視メトリックの公開 オプションは **false** に設定されています。このオプションを有 効にする場合は、**true** を選択します。リソースにアクセスできる AzureActive Directory(ADD)ア プリケーションとサービスプリンシパルを作成します。新しく作成された AAD アプリケーションにコン トリビュータロールを割り当てます。詳細については、「ポータルを使用してリソースにアクセスできる Azure Active Directory アプリケーションおよびサービスプリンシパルを作成する」を参照してください。

6. [ネットワーク設定]ページが表示されます。VNet とサブネットの構成を確認し、必要な設定を編集して、[OK]を選択します。

	□ ×	Subnets	□ ×
* Virtual network (new) vnet	>	* Interface 0/1 Subnet name NSDoc-mgmt-subnet	~
* Subnets Review subnet configuration	>	* Interface 0/1 Subnet address prefix 10.7.0.0/24	~
		* Interface 1/1 Subnet name NSDoc-mgmt-client	~
		* Interface 1/1 Subnet address prefix 10.7.1.0/24	~
		* Interface 1/2 Subnet name	
		 NSDoc-mgmt-server * Interface 1/2 Subnet address prefix 	<u> </u>
		10.7.2.0/24	~

7. [概要] ページが開きます。構成を確認し、適宜編集します。[**OK**] を選択して確定します。

8.「購入」ページが表示されます。[購入]を選択してデプロイを完了します。

必要な構成で Azure リソースグループが作成されるまで時間がかかることがあります。完了後、Azure ポータルで リソースグループを選択し、LB ルール、バックエンドプール、ヘルスプローブなどの構成の詳細を表示します。高可 用性ペアは、ns-vpx0 および ns-vpx1 と表示されます。

追加のセキュリティルールやポートを作成するなど、HA セットアップでさらに変更が必要な場合は、Azure Portal から実行できます。

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

次に、プライマリノードで ALB のフロントエンドパブリック IP(PIP)アドレスを使用して負荷分散仮想サーバー を構成する必要があります。ALB PIP を検索するには、ALB > フロントエンド IP 設定を選択します。

🥬 Search (Ctrl+/)	🕂 Add		
	Search frontend IP configu	ırations	
💠 Overview	NAME		IP ADDRESS
Activity log	inconf-11		104 40 60 190 (alb-publicip)
Access control (IAM)			
🧳 Tags			
🗙 Diagnose and solve problems			
SETTINGS			
Frontend IP configuration			

負荷分散仮想サーバーの構成方法の詳細については、「リソース」セクションを参照してください。

リソース:

次のリンクには、HA の導入と仮想サーバの設定に関する追加情報が表示されます。

- 異なるサブネットでの高可用性ノードの構成
- 基本的な負荷分散を設定する

関連リソース:

- PowerShell コマンドを使用して複数の IP アドレスと NIC を使用して高可用性セットアップを構成する
- Azure でのアクティブスタンバイ HA デプロイメントでの GSLB の構成

アベイラビリティーゾーンを使用した高可用性

Azure アベイラビリティーゾーンは、Azure リージョン内の障害分離された場所であり、冗長な電源、冷却、ネット ワーキングを提供し、回復力を高めます。特定の Azure リージョンだけがアベイラビリティーゾーンをサポートしま す。アベイラビリティーゾーンをサポートするリージョンの詳細については、Azure のドキュメントを参照してくだ さい。Azure のアベイラビリティーゾーンは何ですか。.

図:Azure アベイラビリティーゾーンを使用した高可用性デプロイアーキテクチャの例



Azure Marketplace e で入手可能な「アベイラビリティーゾーンを使用した NetScaler 13.0 HA」というテンプレートを使用して、VPX ペアを高可用性モードでデプロイできます。

Azure アベイラビリティーゾーンを使用してテンプレートを起動し、高可用性 VPX ペアをデプロイするには、次の 手順を実行します。

1. Azure Marketplace から、Citrix ソリューションテンプレートを選択して開始します。

Create a resource	NetScaler 12.1 HA using Availability Zones
•	Citrix

2. デプロイメント・タイプがリソース・マネージャーであることを確認し、「作成」を選択します。

3. [基本]ページが表示されます。詳細を入力し、[**OK**]をクリックします。

注

可用性ゾーンをサポートする Azure リージョンを選択してください。アベイラビリティーゾーンをサポ ートするリージョンの詳細については、Azure のドキュメントを参照してください。Azure のアベイラ ビリティーゾーンは何ですか。

Home > N Create	lew > Marketplace > Everything : NetScaler 12.1 HA using	A	Scaler X	12.1 HA using Av Basics	ailability Zones >	Create NetScaler	12.1	HA us X
1	Basics Configure basic settings	>		•	This deploymer region supporti Zones. Selecting	nt requires Azure ng Availability g a region that d	e loes	
2	General Settings Configure the General settings	>		U	result in deploy to the <u>list</u> of Az supporting Ava	ment failure. Rei ure regions ilability Zones.	fer	
3	Network Settings Configure the Network settings	>	-	Subscriptio	n -			
4	Summary NetScaler 12.1 HA using Availa	>		Resource Create	e group 🚯 e new 🕜 Use e	existing		
5	Buy	>		* Location East US 2			~	

- 4. [一般設定]ページが表示されます。詳細を入力して「**OK**」を選択します。
- 5. [ネットワーク設定]ページが表示されます。VNet とサブネットの構成を確認し、必要な設定を編集して、[OK]を選択します。
- 6. [概要] ページが開きます。構成を確認し、適宜編集します。[**OK**] を選択して確定します。
- 7.「購入」ページが表示されます。[購入]を選択してデプロイを完了します。

必要な構成で Azure リソースグループが作成されるまで時間がかかることがあります。完了後、リソースグル ープを選択すると、LB ルール、バックエンドプール、ヘルスプローブなどの構成の詳細が Azure ポータルに 表示されます。高可用性ペアは、ns-vpx0 および ns-vpx1 と表示されます。また、「場所」列にも場所が表示 されます。

Filter by n	ame	All types	✓ All loca	tions ~	No grouping∨
22 items	Show hidden types ()				
NAM	ie ↑↓			TYPE 👈	LOCATION 🛝
	alb			Load balancer	East US 2
	alb-publicip			Public IP address	East US 2
	ns-vpx0			Virtual machine	East US 2
2	ns-vpx0_OsDisk_1_d7b757b8aa804bf1991a08	33f319e553a		Disk	East US 2
	ns-vpx0-mgmt-publicip			Public IP address	East US 2
	ns-vpx1			Virtual machine	East US 2
	ns-vpx1_OsDisk_1_0c2364d43e2b47fa896bf1	4b02090ee0		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	East US 2

追加のセキュリティルールやポートを作成するなど、HA セットアップでさらに変更が必要な場合は、Azure Portal から実行できます。

Azure モニターのメトリックを使用してインスタンスを監視する

Azure モニターデータプラットフォームのメトリックを使用して、CPU、メモリ使用率、スループットなどの一連の NetScaler VPX リソースを監視できます。メトリックサービスは、Azure 上で稼働する NetScaler VPX リソースを リアルタイムで監視します。メトリックスエクスプローラーを使用して、収集されたデータにアクセスできます。詳 細については、「Azure Monitor メトリックスの概要」を参照してください。

注意事項

- Azure Marketplace オファーを使用して NetScaler VPX インスタンスを Azure にデプロイすると、メトリ ックスサービスはデフォルトで無効になります。
- メトリックスサービスは Azure CLI ではサポートされていません。
- メトリクスは、CPU (管理およびパケット CPU 使用率)、メモリ、およびスループット (インバウンドとアウトバウンド) で使用できます。

Azure モニターでメトリックを表示する方法

インスタンスの Azure モニターでメトリックスを表示するには、次の手順を実行します。

- 1. Azure Portal > Virtual Machines にログオンします。
- 2. プライマリノードとなる仮想マシンを選択します。
- 3. モニタリングセクションで、メトリクスをクリックします。
- 4. メトリック名前空間のドロップダウンメニューから、NetScaler をクリックします。
- 5.「指標」ドロップダウンメニューの「すべての指標 **」で、表示したい指標をクリックします。
- 6. [指標を追加]をクリックすると、同じグラフに別の指標が表示されます。チャートオプションを使用してチャ ートをカスタマイズします。



PowerShell コマンドを使用して複数の **IP** アドレスと **NIC** を使用して高可用性セット アップを構成する

January 15, 2025

Azure のアクティブ/パッシブ高可用性(HA)セットアップで、複数の NIC を持つ一対の NetScaler VPX インスタンスを展開できます。各 NIC に複数の IP アドレスを設定できます。

アクティブ/パッシブ展開には以下が必要です。

- HA Independent Network Configuration (INC) 構成
- Direct Server Return (DSR) $\neq \aleph o$ Azure Load Balancer (ALB)

すべてのトラフィックはプライマリノードを通過します。セカンダリノードは、プライマリノードが失敗するまでス タンバイモードを維持します。

注

Azure クラウド上の Citrix ADC VPX 高可用性展開を機能させるには、2 つの高可用性ノード間で移動できる フローティングパブリック IP (PIP) が必要です。Azure ロードバランサー (ALB) は、フローティング PIP を 提供します。このフローティング PIP は、フェールオーバーが発生した場合に自動的に第 2 ノードに移動され ます。

図:アクティブ-パッシブ展開アーキテクチャの例



アクティブ/パッシブ展開では、ALB フローティングパブリック IP(PIP)アドレスが各 VPX ノードに VIP アドレス として追加されます。HA-INC 構成では、これらの VIP アドレスはフローティングされ、SNIP アドレスはインスタ ンス固有のアドレスとなります。

ALB は 5 秒ごとにヘルスプローブを送信して各 VPX インスタンスを監視し、定期的にヘルスプローブ応答を送信す るトラフィックのみをそのインスタンスにリダイレクトします。そのため、HA セットアップでは、プライマリノー ドがヘルスプローブに応答し、セカンダリノードは応答しません。プライマリインスタンスが 2 つの連続したヘルス プローブを見逃した場合、ALB はそのインスタンスにトラフィックをリダイレクトしません。フェイルオーバー時 は、新しいプライマリがヘルスプローブへの応答を開始し、ALB はそのプライマリにトラフィックをリダイレクトし ます。標準の VPX 高可用性フェイルオーバー時間は 3 秒です。トラフィック切り替えにかかる合計フェイルオーバー 時間は、最大で 13 秒になる可能性があります。

VPX ペアをアクティブ-パッシブ HA セットアップで展開するには、次の 2 つの方法があります。

- NetScaler VPX 標準高可用性テンプレート: このオプションを使用して、3 つのサブネットと6 つの NIC の デフォルトオプションで HA ペアを構成します。
- Windows PowerShell コマンド: このオプションを使用して、サブネットと NIC の要件に応じて HA ペア を構成します。

このトピックでは、PowerShell コマンドを使用してアクティブ/パッシブ HA セットアップで VPX ペアを展開する 方法について説明します。NetScaler VPX Standard HA テンプレートを使用する場合は、「複数の IP アドレスと NIC を使用した HA セットアップの構成」を参照してください。

PowerShell コマンドを使用して HA-INC ノードを構成する

シナリオ:HA-INC PowerShell の展開

このシナリオでは、表に示されているトポロジを使用して NetScaler VPX ペアをデプロイします。各 VPX インスタンスには 3 つの NIC があり、各 NIC は異なるサブネットに展開されます。各 NIC には IP 構成 が割り当てられます。

ALB	VPX1	VPX2
 ALB はパブリック IP 3 (pip3) に関	管理 IP は IPConfig1 を使用して構	管理 IP は IPConfig5 を使用して構
連付けられています。	成され、これには 1 つのパブリック	成され、これには 1 つのパブリック
	IP (パイプ 1) と 1 つのプライベート	IP (パイプ 3) と1つのプライベート
	IP (12.5.2.24) が含まれます。	IP (12.5.2.26) が含まれます。
設定された LB ルールおよびポート	クライアント側の IP は IPConfig3	クライアント側の IP は IPConfig7
は、HTTP (80)、SSL (443)、ヘル	を使用して構成され、これには1つ	で構成され、これには1つのプライ
スプローブ(9000)です。	のプライベート IP (12.5.1.27) が含	ベート IP (12.5.1.28) が含まれます。
	まれます。	
-	サーバー側の IP は IPConfig4 を使	サーバー側の IP は IPConfig8 を使
	用して構成され、これには1つのプ	用して構成され、これには1つのプ
	ライベート IP (12.5.3.24)、nic3、	ライベート IP (12.5.3.28)、nic6、
	バックエンドサブネット゠	バックエンドサブネット゠
	12.5.3.0/24 が含まれます。	12.5.3.0/24 が含まれます。
-	NSG のルールとポートは、SSH	-
	(22)、HTTP (80)、HTTPS (443)	

パラメータ設定

このシナリオでは、次のパラメータ設定が使用されます。

```
1 $locName= "South east Asia"
2
3 $rgName = "MulitIP-MultiNIC-RG"
4
5 $nicName1= "VM1-NIC1"
6
7 $nicName2 = "VM1-NIC2"
8
```

9	\$nicName3= "VM1-NIC3"
10 11 12	<pre>\$nicName4 = "VM2-NIC1"</pre>
12 13 14	<pre>\$nicName5= "VM2-NIC2"</pre>
15 16	<pre>\$nicName6 = "VM2-NIC3"</pre>
17 18	<pre>\$vNetName = "Azure-MultiIP-ALB-vnet"</pre>
19 20	<pre>\$vNetAddressRange= "12.5.0.0/16"</pre>
21 22	<pre>\$frontEndSubnetName= "frontEndSubnet"</pre>
23 24	<pre>\$frontEndSubnetRange= "12.5.1.0/24"</pre>
25 26	<pre>\$mgmtSubnetName= "mgmtSubnet"</pre>
27 28	<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 36	<pre>\$avSetName = "multiple-avSet"</pre>
37 38	<pre>\$vmSize= "Standard_DS4_V2"</pre>
39 40	<pre>\$publisher = "Citrix"</pre>
41 42	\$offer = "netscalervpx-120"
43 44	\$sku = "netscalerbyol"
45 46	\$version="latest"
47 48	<pre>\$pubIPName1="VPX1MGMT"</pre>
49 50	<pre>\$pubIPName2="VPX2MGMT"</pre>
51 52	\$pubIPName3="ALBPIP"
53 54	\$domName1="vpx1dns"
55 56	\$domName2="vpx2dns"
57 58	<pre>\$domName3="vpxalbdns"</pre>
59 60	<pre>\$vmNamePrefix="VPXMultiIPALB"</pre>
61	<pre>\$osDiskSuffix1="osmultiipalbdiskdb1"</pre>

02	
63	<pre>\$osDiskSuffix2="osmultiipalbdiskdb2"</pre>
64	
65	<pre>\$lbName= "MultiIPALB"</pre>
66	
67	<pre>\$trontEndConfigName1= "FrontEndIP"</pre>
68	chackandDoolNamo1- UPackandDoolUttpU
69 70	spackendPoolNamei= "BackendPoolHttp"
71	<pre>\$lbRuleName1= "LBRuleHttp"</pre>
72	end condiner Ebha centep
73	<pre>\$healthProbeName= "HealthProbe"</pre>
74	
75	\$nsgName="NSG-MultiIP-ALB"
76	
77	<pre>\$rule1Name="Inbound-HTTP"</pre>
78	
79	<pre>\$rule2Name="Inbound-HTTPS"</pre>
80	¢rule2Neme=UTrebound_CCUU
ÖL	stutesnalle="fnuounu=SSH"

展開を完了するには、PowerShell コマンドを使用して次の手順を完了します。

1. リソースグループ、ストレージアカウント、高可用性セットの作成

- 2. ネットワークセキュリティグループの作成と規則の追加
- 3. 仮想ネットワークと3つのサブネットの作成
- 4. パブリック IP アドレスの作成
- 5. VPX1の IP 構成の作成
- 6. VPX2 の IP 構成の作成
- 7. VPX1のNICの作成
- 8. VPX2 の NIC の作成
- 9. VPX1 の作成
- 10. VPX2 の作成
- 11. ALB の作成

リソースグループ、ストレージアカウント、および可用性セットを作成します。

```
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
```

ネットワークセキュリティグループを作成し、ルールを追加します。

```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
1
        Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
        Inbound -Priority 101
2
3
4
     -SourceAddressPrefix Internet -SourcePortRange * -
        DestinationAddressPrefix * -DestinationPortRange 80
5
6
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
     -SourceAddressPrefix Internet -SourcePortRange * -
16
        DestinationAddressPrefix * -DestinationPortRange 22
17
     $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
        Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
        $rule3
```

仮想ネットワークと**3**つのサブネットを作成します。

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
1
         $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
         parameter value should be as per your requirement)
2
3
4
     $mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
         $mgmtSubnetName -AddressPrefix $mgmtSubnetRange
5
6
7
     $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
         $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
     $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
10
         $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
21
     $subnetName="backEndSubnet"
22
23
24
     \$subnet2=\$vnet.Subnets|?{
25
    \$\_.Name -eq \$subnetName }
26
27
28
29
     $subnetName="mgmtSubnet"
31
32
     \$subnet3=\$vnet.Subnets|?{
    \$\_.Name -eq \$subnetName }
```

パブリック IP アドレスを作成します。

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

VPX1の **IP** 構成を作成します。

```
$IpConfigName1 = "IPConfig1"
1
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
     $IPConfigName3="IPConfig-3"
10
11
12
13
     $IPAddress="12.5.1.27"
14
15
```

```
16 $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
	Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19 $IPConfigName4 = "IPConfig-4"
20
21
21
22 $IPAddress = "12.5.3.24"
23
24
25 $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
-Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

VPX2の **IP** 構成を作成します。

```
$IpConfigName5 = "IPConfig5"
1
2
3
4
     $IPAddress="12.5.2.26"
5
6
7
     $IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
         Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
         $pip2 -Primary
8
9
     $IPConfigName7="IPConfig-7"
10
11
12
13
     $IPAddress="12.5.1.28"
14
     $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
16
         Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19
     $IPConfigName8="IPConfig-8"
20
21
22
     $IPAddress="12.5.3.28"
23
24
     $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
25
         Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

VPX1 用の **NIC** を作成します。

1	<pre>\$nic1=New-AzureRmNetworkInterface -Name \$nicName1 -ResourceGroupName</pre>
	<pre>\$rgName -Location \$locName -IpConfiguration \$IpConfig1 -</pre>
	NetworkSecurityGroupId \$nsg.Id
2	
3	
4	<pre>\$nic2=New-AzureRmNetworkInterface -Name \$nicName2 -ResourceGroupName</pre>

```
$rgName -Location $locName -IpConfiguration $IpConfig3 -
NetworkSecurityGroupId $nsg.Id
5
6
7 $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig4 -
NetworkSecurityGroupId $nsg.Id
```

VPX2 用の **NIC** を作成します。

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

VPX1を作成します。

この手順には、次の下位手順が含まれています。

- VM 設定オブジェクトの作成
- 資格情報、OS、イメージの設定
- NIC の追加
- OS ディスクの指定と VM の作成

```
1
      $suffixNumber = 1
2
      $vmName=$vmNamePrefix + $suffixNumber
3
4
      $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
5
         AvailabilitySetId $avSet.Id
6
      $cred=Get-Credential -Message "Type the name and password for
7
         VPX login."
8
9
      $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
         ComputerName $vmName -Credential $cred
10
      $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
11
          $publisher -Offer $offer -Skus $sku -Version $version
12
      $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1
13
          .Id -Primary
```

```
14
15
      $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2
          .Id
16
      $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3
17
          .Id
18
19
      $osDiskName=$vmName + "-" + $osDiskSuffix1
21
      $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +
           "vhds/" + $osDiskName + ".vhd"
22
23
      $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -
         VhdUri $osVhdUri -CreateOption fromImage
24
25
      Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product
         $offer -Name $sku
26
      New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -
27
          Location $locName
```

VPX2 を作成します。

```
. . .
1
2
     $suffixNumber=2
3
4
     $vmName=$vmNamePrefix + $suffixNumber
5
6
7
8
     $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
         AvailabilitySetId $avSet.Id
9
     $cred=Get-Credential -Message "Type the name and password for VPX
11
        login."
12
13
     $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
14
         ComputerName $vmName -Credential $cred
15
16
     $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
17
         $publisher -Offer $offer -Skus $sku -Version $version
18
19
     $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
20
         Primary
21
23
     $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
```

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
26
27
28
29
     $osDiskName=$vmName + "-" + $osDiskSuffix2
31
     $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
32
         /" + $osDiskName + ".vhd"
33
34
     $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
          $osVhdUri -CreateOption fromImage
37
     Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
38
          -Name $sku
39
40
     New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
41
         $locName
   • • •
42
```

NIC に割り当てられたプライベート IP アドレスとパブリック IP アドレスを表示するには、次のコマンドを入力します。

```
...
1
2
     $nic1.IPConfig
3
4
     $nic2.IPConfig
5
6
7
     $nic3.IPConfig
8
9
10
     $nic4.IPConfig
11
12
13
14
    $nic5.IPConfig
15
16
17
     $nic6.IPConfig
   . . .
18
```

Azure の負荷分散 (ALB) を作成します。

この手順には、次の下位手順が含まれています。

- フロントエンド IP 構成を作成する
- ヘルスプローブの作成
- バックエンドアドレスプールを作成する

- 負荷分散規則(HTTP および SSL)の作成
- フロントエンド IP 設定、バックエンドアドレスプール、および LB ルールを使用して ALB を作成します。
- IP 構成をバックエンドプールに関連付ける

```
$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

NetScaler VPX ペアを正常に展開したら、各 VPX インスタンスにログオンして HA-INC、SNIP アドレス、および VIP アドレスを構成します。

1. 次のコマンドを入力して HA ノードを追加します。

add ha node 1 PeerNodeNSIP -inc Enabled

2. クライアント側 NIC のプライベート IP アドレスを VPX1 (NIC2) および VPX2 (NIC5) の SNIP として追加 する

nsip privateIPofNIC2 255.255.255.0 -type SNIP を追加します nsip privateIPofNIC5 255.255.255.0 -type SNIP を追加します 3. ALB のフロントエンド IP アドレス (パブリック IP) を持つプライマリノードに負荷分散仮想サーバーを追加 します。

add lb virtual server v1 HTTP FrontEndIPofALB 80

関連リソース:

Azure でのアクティブスタンバイ HA デプロイメントでの GSLB の構成

フローティング **IP** 無効モードの **ALB** を使用して **Azure** に **NetScaler** 高可用性ペアを デプロイする

October 17, 2024

Azure のアクティブ/パッシブ高可用性(HA)セットアップで、複数の NIC を持つ一対の NetScaler VPX インスタンスを展開できます。各 NIC には多数の IP アドレスを含めることができます。

アクティブ/パッシブ展開には以下が必要です。

- HA Independent Network Configuration (INC) 構成
- Azure Load Balancer (ALB) には次の機能があります。
 - フローティング IP 対応モードまたはダイレクトサーバーリターン (DSR) モード
 - フローティング IP 無効モード

ALB Floating IP オプションの詳細については、Azure のドキュメントを参照してください。

ALB フローティング IP を有効にして、Azure でアクティブ/パッシブ HA セットアップで VPX ペアをデプロイする 場合は、「PowerShell コマンドを使用して複数の IP アドレスと NIC で高可用性セットアップを構成する」を参照し てください。

フローティング IP 無効モードの ALB を使用した HA 導入アーキテクチャ

アクティブ/パッシブ展開では、各インスタンスのクライアントインターフェイスのプライベート IP アドレスが各 VPX インスタンスの VIP アドレスとして追加されます。HA-INC モードで、IP セットを使用して VIP アドレスを共 有し、SNIP アドレスをインスタンス固有に設定します。すべてのトラフィックはプライマリインスタンスを通過し ます。セカンダリインスタンスは、プライマリインスタンスに障害が発生するまでスタンバイモードです。

図:アクティブ-パッシブ展開アーキテクチャの例



前提条件

NetScaler VPX インスタンスを Azure に展開する前に、次の情報を理解している必要があります。

- Azure の用語とネットワークの詳細。詳細については、「Azure 用語」を参照してください。
- NetScaler アプライアンスの動作。詳しくは、NetScaler のドキュメントを参照してください。
- NetScaler ネットワーキング。詳細については、ADC ネットワークを参照してください。
- Azure ロードバランサーと負荷分散ルール設定。詳細については、Azure ALBのドキュメントを参照してください。

ALB フローティング IP を無効にして VPX HA ペアを Azure にデプロイする方法

HA と ALB の導入手順の概要は次のとおりです。

- 1. Azure に 2 つの VPX インスタンス (プライマリインスタンスとセカンダリインスタンス) をデプロイします。
- 2. 両方のインスタンスにクライアントとサーバーの NIC を追加します。
- 3. フローティング IP モードが無効になっている負荷分散ルールを持つ ALB をデプロイします。
- 4. NetScaler GUI を使用して、両方のインスタンスで高可用性設定を構成します。

手順 1. Azure に 2 つの VPX インスタンスをデプロイします。

次の手順に従って、2 つの VPX インスタンスを作成します。

1. Azure Marketplace から NetScaler バージョンを選択します(この例では、NetScaler リリース 13.1 が使用されています)。



2. 必要な ADC ライセンスモードを選択し、[作成] をクリックします。

NetScaler ADC 14.1 🛷 \cdots Cloud Software Group NetScaler ADC 14.1 \bigcirc Add to Favorites netoscale Cloud Software Group | Virtual Machine Free trial Plan NetScaler ADC 14.1 VPX Standard Edi... Start with a pre-set configuration Purchase a reservation \sim Create ₽ Filter NetScaler ADC 14.1 VPX Standard Edition - 5000 Mbps Overview NetScaler ADC 14.1 VPX Bring Your Own License tings + Reviews NetScaler ADC 14.1 VPX Express - 20 Mbps NetScaler AD very controller that delivers your applications guickly, reliably, and securely, with NetScaler ADC 14.1 VPX Standard Edition - 10 Mbps and pricing fl ovide operational consistency and a smooth user experience, NetScaler ADC ea the hybrid clc NetScaler ADC 14.1 VPX Premium Edition - 10 Mbps You can learn cture with NetScaler ADC on Microsoft Azure by reading the eBook, available NetScaler ADC 14.1 VPX Advanced Edition - 10 Mbps Why NetScale NetScaler ADC 14.1 VPX Standard Edition - 200 Mbps NetScaler AD delivery, a comprehensive centralization management system, and orchestratic for applicatio NetScaler ADC 14.1 VPX Advanced Edition - 200 Mbps tScaler's all-in-one solution brings point solutions under one roof, ensuring sin every step of NetScaler ADC 14.1 VPX Premium Edition - 200 Mbps Key Benefits: NetScaler ADC 14.1 VPX Standard Edition - 1000 Mbps Flexibl ature-rich ADC available across a wide variety of deployment options with the capaci NetScaler ADC 14.1 VPX Advanced Edition - 1000 Mbps Best U gent, global load-balancing service that uses real-time Internet traffic and data NotScolor ADC 14.1 VPV Promium Edition - 1000 Mbn route i

[仮想マシンの作成]ページが開きます。

 展開を成功させるには、各タブ(基本、ディスク、ネットワーク、管理、監視、詳細、タグ)で必要な詳細を入 力します。

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)	✓
Resource group * ①	(New) demo
Instance details	
Virtual machine name * 🕕	vm1-demo 🗸
Region * ()	(US) East US 🗸 🗸
Availability options (i)	Availability zone
Availability zone * ①	Zones 1 V
Review + create < Preview	Next : Disks >

[ネットワーク] タブで、管理、クライアント、サーバーの NIC の 3 つのサブネットを持つ新しい仮想ネット ワークを作成します。それ以外の場合は、既存の仮想ネットワークを使用することもできます。管理 NIC は、 VM の展開中に作成されます。クライアントとサーバーの NIC は、仮想マシンの作成後に作成および接続され ます。NIC ネットワークセキュリティグループでは、次のいずれかを実行できます。

- [詳細]を選択し、要件に合った既存のネットワークセキュリティグループを使用します。
- [基本]を選択し、必要なポートを選択します。

注

仮想マシンのデプロイが完了した後に、ネットワークセキュリティグループの設定を変更することもで きます。

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
	Create new
Subnet * 🕕	(new) default (10.2.0.0/24)
Public IP (i)	(new) vm1-demo-ip
NIC network security group ①	O None
	• Basic
	Advanced
Public inhound ports *	O None
	Allow selected ports
	O management from
Select inbound ports *	SSH (22) 🗸
	This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Delete public IP and NIC when VM is deleted ①	
Enable accelerated networking 🔅	
Load balancing	
You can place this virtual machine in th	ne backend pool of an existing Azure load balancing solution. Learn more $\ensuremath{\mathbb{C}}^2$
Load balancing options	None
	Azure load balancer
	Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
	Application gateway
	Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
Destion 1 consta	Neurisure Neuris Managements
Review + create <	revious ivext : Management >

4. 次へをクリックします:確認+作成>。

検証が成功したら、基本設定、仮想マシンの構成、ネットワーク、および追加設定を確認し、[作成]をクリッ クします。

Create a virtual machine

Validation pa	assed					
Basics Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create
1 Cost given	below is an estimate	and not the final pri	ce. Please use Pri	<u>cing calculator</u> वं	for all you	r pricing needs.
Price						
NetScaler ADC 1 by Cloud Softwar Terms of use Pri 1 X Standard DS by Microsoft Terms of use Pri	4.1 e Group vacy policy 2 v2 vacy policy	Not covered 2.3000 US Subscription 0.0880 US Pricing for	d by credits ① 5D/hr a credits apply ① 5D/hr other VM sizes	D		
TERMS						
By clicking "Creat above; (b) author billing frequency information with provide rights for	e", I (a) agree to th ize Microsoft to bil as my Azure subsci the provider(s) of t third-party offerin	e legal terms and p I my current payme ription; and (c) agre he offering(s) for su gs. See the Azure N	rivacy statement nt method for th te that Microsoft upport, billing an Marketplace Term	(s) associated w ne fees associate may share my o d other transact ns for additional	vith the Ma ed with the contact, us tional activ details.	arketplace offering(s) listed e offering(s), with the same age and transactional rities. Microsoft does not
Name						
Preferred e-mail a	address					
Preferred phone	number	-				
A You have a back to Bas	et SSH port(s) ope	n to the internet. Th	his is only recomm	nended for testin	g. If you w	ant to change this setting, go

Create

< Previous

Next > Download a template for automation

5. デプロイが完了したら、「リソースに移動」をクリックして設定の詳細を確認します。

Search	📋 Delete 🚫 Cancel 🏦 Redeploy 🞍 Download 💍 Refresh
Overview Inputs Outputs	Your deployment is complete Deployment name: CreateVm-citrix.netscalervpx-141-netscaler5000 Subscription: Resource group: demp
Template	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

同様に、2 つ目の NetScaler VPX インスタンスを展開します。

手順 3. クライアントとサーバーの NIC を両方のインスタンスに追加します。

注

さらに NIC を接続するには、まず仮想マシンを停止する必要があります。Azure ポータルで、停止する VM を 選択します。[概要] タブで、[停止] をクリックします。ステータスが [停止] と表示されるまで待ちます。

プライマリインスタンスにクライアント NIC を追加するには、次の手順に従います。

1. [ネットワーク]>[ネットワークインターフェイスの接続]に移動します。

既存の NIC を選択するか、新しいインターフェイスを作成して接続できます。

2. NIC ネットワークセキュリティグループについては、[詳細]を選択して既存のネットワークセキュリティグ ループを使用するか、[基本]を選択して作成できます。

Home > vm1-demo | Networking >

Create network interface

Project details
Subscription (i)
NSDev Platform CA anoop.agarwal@citrix.com
Create new
Location ①
(US) East US
Natural interface
Network Interface
Name *
vm1-demo-nic
Virtual network 🕕
vm1-demo-vnet
Subnet * ()
client (10.2.1.0/24)
NIC network security group 🕧
○ None
• Basic
O Advanced
Public inbound ports * (i)
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

サーバ NIC を追加するには、クライアント NIC を追加する場合と同じ手順に従います。

NetScaler VPX インスタンスには、3 つの NIC(管理 NIC、クライアント NIC、およびサーバー NIC)がすべて接続 されています。

前の手順を繰り返して、セカンダリインスタンスに NIC を追加します。

両方のインスタンスで NIC を作成してアタッチしたら、[**Overview] > [Start**] に移動して両方のインスタンスを 再起動します。

注

クライアント NIC インバウンドルールでは、ポートを通過するトラフィックを許可する必要があります。この ルールは、後で NetScaler VPX インスタンスの構成時に負荷分散仮想サーバーを作成するために使用されま す。

手順 3. フローティング IP モードが無効になっている負荷分散ルールを持つ ALB をデプロイします。

ALB の設定を開始するには、次の手順に従います。

- 1. [ロードバランサー]ページに移動し、[作成]をクリックします。
- 2. [ロードバランサーの作成]ページで、必要に応じて詳細を入力します。

次の例では、Standard SKU のリージョンパブリックロードバランサーをデプロイします。

Create load balancer

Project details	
Subscription *	
Resource group *	demo ✓ Create new
Instance details	
Name *	alb1 🗸
Region *	Southeast Asia
SKU * 🕠	 Standard Gateway Basic
Туре * 🛈	Public Internal
Tier *	 Regional Global
Review + create < Previous	Next : Frontend IP configuration > Download a template for automation RGive
注 NetScaler 仮想マシンに接続され 要があります。ALB SKU の詳細し ください。	cているすべてのパブリック IP は、ALB の SKU と同じ SKU を持つ必 については、 <mark>Azure Load Balancer SKU のドキュメントを参照して</mark>

3. [フロントエンド IP 設定]タブで、IP アドレスを作成するか、既存の IP アドレスを使用します。

Create load balancer

Basics	Frontend IP configuration	Backend pools	Inbound rules	Outbound rules	Tags	Review + create
A fronten	d IP configuration is an IP addre	ss used for inbound	and/or outbound co	ommunication as defir	ned withir	n load balancing, inbound NAT, and outbound rules.
+ Add	a frontend IP configuration]				
Name 2	¢↑			IP a	ddress 1	,†
Add a fr	ontend IP to get started					

Add frontend IP configuration	\times
Name *	
alb-frontend	\checkmark
$\bullet PV4 \cup PV6$	
ID to me	
• IP address () IP prefix	
Public IP address *	
(New) alb-public-ip	\sim
Create new	
Gateway Load balancer (i)	
None	\sim
·	



4. [バックエンドプール] タブで、[NIC ベースのバックエンドプール構成] を選択し、両方の NetScaler 仮想マ シンのクライアント NIC を追加します。

Create load balancer

Basics	Frontend IP configuration	Backend pools In	bound rules Outbound	ules Tags	Review + create
A backen	d pool is a collection of resource	s to which your load bal	ancer can send traffic. A backe	nd pool can cont	ain virtual machines, virtual machine s
+ Add	d a backend pool				
Name	Virtual	network	Resource Name	Network inter	face IP address
Name \checkmark alb	-backend-pool	network	Resource Name	Network inter	face IP address
Name	-backend-pool vm1-de	network mo-vnet	Resource Name vm1-demo	Network intervention vm1-demo324	face IP address 4_z1 10.2.0.4

5. [受信ルール] タブで、[負荷分散ルールの追加] をクリックし、前の手順で作成したフロントエンド IP アドレ スとバックエンドプールを指定します。要件に基づいてプロトコルとポートを選択します。ヘルスプローブを 作成するか、既存のヘルスプローブを使用します。「フローティング IP を有効にする」チェックボックスをオ フにします。

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

 \times

6. [レビュー]+[作成]をクリックします。検証に合格したら、[作成]をクリックします。 Create load balancer

🕑 Vali	idation passed					
Basics	Frontend IP configuration	Backend pools	Inbound rules	Outbound rules	Tags	Review + create
Basics						
Subscript	tion					
Resource	group	demo				
Name		alb1				
Region		Southeast Asia				
SKU		Standard				
Tier		Regional				
Туре		Public				
Fronten	d IP configuration					
Frontend	IP configuration name	alb-frontend				
Frontend	IP configuration IP address	To be created				
Backend	l pools					
Backend	pool name	alb-backend-pool				
Ductoria	poortiume	and backenia poor				
Inbound	l rules					
Load bala	ancing rule name	lb-rule1				
Health p	robe name	health-probe1				
Outbou	nd rules					
None						
Tags						
None						
Create	< Previous	Next > D	ownload a template	e for automation RGi	ve feedba	ck

手順 4: IP セットを追加し、両方のインスタンスで IP セットをセカンダリ VIP にバインドします。

Azure で NetScaler VPX インスタンスを作成したら、NetScaler GUI を使用して HA を構成できます。

手順 1. 両方のインスタンスで INC モードで高可用性をセットアップします。

プライマリ・インスタンスで、次の手順を実行します。

1. インスタンスのデプロイ時に指定したユーザー名nsrootとパスワードを使用して、インスタンスにログオンします。

- 2. 構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノードの IP アドレス] フィールドに、セカンダリインスタンスの管理 NIC のプライベート IP アドレス(例: 10.4.1.5)を入力します。
- 4.「セルフノードで INC (独立ネットワーク構成) モードを有効にする」チェックボックスを選択します。
- 5. [**Create**] をクリックします。

← Create HA Node

Remote Node IP Address*	
10 . 4 . 1 . 5	0
Configure remote system to participate I	ligh Availability setup
🗹 Turn Off HA Monitor inter face/channels	that are down
 Lum on INC(Independent Network Cont) 	puration) mode en scit node 🕕
Remote System Login Credential	
User Name	
Password	
Secure Access	

セカンダリインスタンスで、次の手順を実行します。

- 1. インスタンスのデプロイ時に指定したユーザー名nsrootとパスワードを使用して、インスタンスにログオンします。
- 2. 構成 > システム > 高可用性 > ノードに移動し、追加をクリックします。
- 3. [リモートノードの IP アドレス] フィールドに、プライマリインスタンスの管理 NIC のプライベート IP アドレス (例: 10.4.1.4) を入力します。
- 4.「セルフノードで INC (独立ネットワーク構成) モードを有効にする」チェックボックスを選択します。
- 5. [Create] をクリックします。

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 Configuration) mode on self node	
RPC Node Password	
	$(\mathbf{\hat{I}})$
Remote System Login Credential	
User Name	
Password	
Secure Access	
Create Close	

先に進む前に、セカンダリインスタンスの同期状態が [ノード] ページで [**SUCCESS**] と表示されていることを確認 します。

注

これで、セカンダリインスタンスはプライマリインスタンスと同じログオン認証情報を持つようになりました。
System > High	h Availability	> Nodes							
Nodes (2								ି 😭
Add Edi	t Delet	e Statistics	Select Acti	on V					
	ID 0 IP	ADDRESS 0	HOST NAME	MASTER STATE	NODE STATE	INC 0	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE R	EASON 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 of 1	►

手順 3. 両方のインスタンスに仮想 IP アドレスとサブネット IP アドレスを追加します。

プライマリ・インスタンスで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. 次の手順に従って、プライマリ VIP アドレスを追加します。
 - a) プライマリインスタンスのクライアント NIC のプライベート IP アドレスと、VM インスタンスのクラ イアントサブネットに設定されているネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [Create] をクリックします。
- 3. 次の手順に従って、プライマリ SNIP アドレスを追加します。
 - a) プライマリ・インスタンスのサーバ NIC の内部 IP アドレスと、プライマリ・インスタンスのサーバ・ サブネットに設定されているネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [**Create**] をクリックします。
- 4. 次の手順に従って、セカンダリ VIP アドレスを追加します。
 - a) セカンダリインスタンスのクライアント NIC の内部 IP アドレスと、VM インスタンスのクライアント サブネットに設定されているネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [**Create**] をクリックします。

System > N	letwork > IPs >	IPV4s								
IPs									Ŕ	C 😭
IPV4s 🗲	IPV6s 1	Port Allocation								
Add	Edit Delete	Statistics Select	Action 🗸							
Q Click her	e to search or you ca	n enter Key : Value format								0
	IP ADDRESS	© STATE	C TYPE	MODE	C ARP	CMP	 VIRTUAL S 	SERVER 0	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	•

セカンダリインスタンスで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. 次の手順に従って、セカンダリ VIP アドレスを追加します。
 - a) セカンダリインスタンスのクライアント NIC の内部 IP アドレスと、VM インスタンスのクライアント サブネットに設定されているネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
- 3. 次の手順に従って、セカンダリ SNIP アドレスを追加します。
 - a) セカンダリインスタンスのサーバ NIC の内部 IP アドレスと、セカンダリインスタンスのサーバサブネ ットに設定されているネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [**Create**] をクリックします。

System > Net	work > IPs > I	PV4s												
IPs													C	•
IPV4s 3	IPV6s 1	Port A	Allocation											
Add Edi	it Delete	Statis	stics	et Acti	on 🗸									
Q Click here to	o search or you can	enter K	ley : Value format											0
	IP ADDRESS		STATE		TYPE	MODE	ARP	ICMP	VIRTUA	L SERVER		TRAFFIC DOMAIN		
Z	10.4.3.5		ENABLED		Subnet IP	Active	ENABLED	ENABLED	-N/A-				0	5
	10.4.2.5		ENABLED		Virtual IP	Passive	ENABLED	ENABLED	ENABLI	ED			0)
	10.4.1.5		ENABLED		NetScaler IP	Active	ENABLED	ENABLED	-N/A-				0)
Total 3										25 Per Page	~	Page 1 of 1	<)	

手順 3. IP セットを追加し、両方のインスタンスで IP セットをセカンダリ VIP にバインドします。

プライマリ・インスタンスで、次の手順を実行します。

- 1. ステップ 2: 両方のインスタンスに IP セットを追加します。
- 2. IP セット名を追加し、[Insert] をクリックします。
- 3. [IPv4]ページで、仮想 IP(セカンダリ VIP)を選択し、[挿入]をクリックします。
- 4. [Create] をクリックして IP セットを作成します。

⇔ Create IP Set	IPV4s 🖪										С×
New'	Add Edit	Delete Stati	stics Select Actio	nv.							
spoart ()	Q. Click here to search	ar you can enter Key :	Value Fermat								0
Traffic Donain	0	IP ADDRESS :	TRAFFIC DOMAIN :	OWNER NODE	: STATE :	TYPE	: MODE	ARP	: ICMP	: VIRTUAL SE	RVER :
And V		10.4.1.4	0	ALL NODES (255)	ENABLED	NetScalar IP	Active	ENABLED	ENABLED	-N/A-	
PM	0	10.4.2.4	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	
1994 1990	2	10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED	
	0	10.4.3.4	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-	
Insert Delete	Total 4								25 Per Page 🛛 🛩	Page 1 of 1	$\neg (-) \in [$
IP ADDRESS No turns	Prest (Close									
Create Class											

セカンダリインスタンスで、次の手順を実行します。

- 1. ステップ 2: 両方のインスタンスに IP セットを追加します。
- 2. IP セット名を追加し、[Insert] をクリックします。
- 3. [IPv4s]ページで、仮想 IP (セカンダリ VIP) を選択し、[挿入] をクリックします。
- 4. [Create] をクリックして IP セットを作成します。

	IPV4s 🖪									С×
	Add E	dit Delete St	stistics Sele	ct Action~						
	Q Click here to	search or you can enter Ke	y : Value format							G
		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-
		10.4.2.5	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED
		10.4.3.5	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
	Total 3							25 Per Pa	se 🗸 Page	1 of1 🚽 🕨
	Insert	Close								

注

IP セット名は、プライマリインスタンスとセカンダリインスタンスの両方で同じである必要があります。

手順 4: プライマリインスタンスにサービスまたはサービスグループを追加します。

- 1. [設定]>[トラフィック管理]>[負荷分散]>[仮想サーバー]>[追加]に移動します。
- 2. [名前]、[プロトコル]、[IP アドレスタイプ (IP アドレス)]、[IP アドレス] (プライマリ VIP)、および [ポート] に必要な値を追加します。
- 3. [詳細] クリックします。[IP 範囲 IP セット設定] に移動し、ドロップダウンメニューから [IPSet] を選択し、 ステップ 3 で作成した IPSet を指定します。
- 4. OK をクリックして、負荷分散仮想サーバーを作成します。

← Load Balancing Virtual Server

Basic Settings		
Create a virtual server by specifying a nan area network (LAN) or wide area network i You can configure multiple virtual servers	re, an IP address, a port, and a protocol type. If an application is accessible fm WANE, the VIP is usually a private (ICANN non-routable) IP address, to receive client requests, thereby increasing the availability of resources to ;	om the internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local process client requests.
Name*		
vī	0	
Protocol"		
HTTP	~	
IP Address Type*		
IP Address	~	
IP Address*		
10 . 4 . 2 . 4	0	
Port"		
80	[©]	
Traffic Domain		Vintual Server State
	V Add Edit	D RHI State
IP Range IP Set settings		S AppRov Logging
Post	×	Instan connections on cluster
IPset		
ipset1	V Add Edit ()	
Redirection Mode*		
IP Based	v	
Listen Priority		

手順5: プライマリインスタンスにサービスまたはサービスグループを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [サービス] > [追加] に移動します。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、[OK] をクリックします。

手順 6: 手順 6: サービスまたはサービスグループを、プライマリインスタンスの負荷分散仮想サーバにバインドします。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動します。
- 2. 手順4で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
- 3. [サービスとサービスグループ]タブで、[負荷分散仮想サーバーサービスバインドなし]をクリックします。
- 4. 手順5で構成したサービスを選択し、[バインド]をクリックします。

6 Load Ba	Jancing Virtual Server	Service Bind	Ring > Service							
Load Balan		Service	0							×
Basic Setting		Select	Add Edit							
Marra		Q Clickhere	to search or you can enter Key : Value format							0
Protocol			NAME	STATE :	IP ADDRESS/DOMAIN NAME ()	TRAFFIC DOMAIN	PORT :	PROTOCOL :	MAX CLIENTS ::	MAX REQU
State IP Address	DOWN 10.1.2.4		azurelbdnsservice0	• UP	168.63.129.16	0	53	DNS	0	
Port			sl	●UP	10.4.3.6	0	80	HTTP	0	
Traffic Domain Toggle Order			62	●UP	10.4.3.7	0	80	HTTP	0	
Order Threshold		Total 3						25 Per Pag	Page 1 of1	\rightarrow
Services and										
No Lord Bala										
No Load Balar										
Date										

手順**7**:構成を保存します。

そうしないと、再起動後、または即時再起動が行われた場合、すべての設定が失われます。

手順8:設定を確認します。

フェイルオーバー後に ALB フロントエンド IP アドレスに到達できることを確認します。

- 1. ALB フロントエンド IP アドレスをコピーします。
- 2. ブラウザに IP アドレスを貼り付け、バックエンドサーバーにアクセスできることを確認します。
- 3. プライマリインスタンスで、フェイルオーバーを実行します:

NetScaler GUI から、[構成] > [システム] > [高可用性] > [アクション] > [強制フェールオーバー] に移 動します。

Q Search Menu		System > High A	vailability > Nodos						
Favorites	\sim	Nodes 😰							0
AZURE	>	Add Edit	Delete Statistics	Select Action 🗸					
System	\sim	0 10	: IPADORESS :	Scient Action Force Synchronization STER STATE	* NODE STATE	: INC	SYNCHRONIZATION STATE	: SYNCHRONIZATION FAILURE REASON	
Licenses		•	10.4.1.4	citro-ado-1 Primery	• UP	ENABLED	ENABLED	-8.0-	
Settings		0 1	10.4.1.5	Force Failover	• 1112	ENAMEND	SLCO-SS	NA	
Diagnostics		lotal 2						25 Per Page ✓ Page I of I	
High Availability	\sim								
Nodes									
Route Monitors									

4. フェイルオーバー後、以前に使用した ALB フロントエンド IP を介してバックエンドサーバーにアクセスでき ることを確認してください。

Azure DNS プライベートゾーン用 NetScaler デプロイ

October 17, 2024

Azure DNS は、DNS ドメインをホストし、名前解決を行うための Microsoft Azure インフラストラクチャ上のサ ービスです。

Azure DNS プライベートゾーンは、プライベートネットワーク内のドメイン名の解決に重点を置いたサービスです。 プライベートゾーンでは、顧客は Azure が提供している現在提供されている名前ではなく、独自のカスタムドメイン 名を使用できます。

業界をリードするアプリケーション配信ソリューションである NetScaler は、Azure DNS プライベートゾーン の負荷分散と GSLB 機能を提供するのに最適です。Azure DNS プライベートゾーンに登録することで、企業は NetScaler Global Server Load Balancing (GSLB)の機能とインテリジェンスを利用して、安全な VPN トンネ ルを介して接続された複数の地域のワークロードやデータセンターにイントラネットトラフィックを分散できます。 このコラボレーションにより、企業は Azure パブリッククラウドに移行したいワークロードの一部にシームレスにア クセスできるようになります。

Azure DNS の概要

ドメインネームシステム (DNS) は、サービス名をその IP アドレスに変換または解決します。DNS ドメイン用のホス ティングサービスである Azure DNS は、Microsoft Azure インフラストラクチャを使用して名前解決を行います。 Azure DNS は、インターネットに直接接続する DNS ドメインをサポートするだけでなく、プライベート DNS ドメ インもサポートするようになりました。

Azure DNS は、カスタム DNS ソリューションを必要とせずに仮想ネットワーク内のドメイン名を管理および解決す るための、信頼性が高く安全な DNS サービスを提供します。プライベート DNS ゾーンを使用すると、Azure が提供 する名前ではなく、独自のカスタムドメイン名を使用できます。カスタムドメイン名を使用すると、組織のニーズに 合わせて仮想ネットワークアーキテクチャを調整できます。仮想ネットワーク内および仮想ネットワーク間の仮想マ シン (VM) の名前解決を行います。また、お客様はスプリットホライズンビューでゾーン名を設定できます。これに より、プライベート DNS ゾーンとパブリック DNS ゾーンで名前を共有できます。

Azure DNS プライベートゾーン用の NetScaler GSLB を選ぶ理由

今日の世界では、企業はワークロードをオンプレミスから Azure クラウドに移行したいと考えています。クラウドへ の移行により、市場投入までの時間、設備投資/価格、導入のしやすさ、セキュリティを確保できます。Azure DNS プライベートゾーンサービスは、ワークロードの一部を Azure クラウドに移行する企業に独自の提案を提供します。 これらの企業は、プライベートゾーンサービスを使用するときに、オンプレミス展開で長年使用していたプライベー ト DNS 名を作成できます。このハイブリッドモデルのイントラネットアプリケーションサーバーはオンプレミスに あり、Azure クラウドは安全な VPN トンネルを介して接続されているため、課題の1つは、これらのイントラネッ トアプリケーションにシームレスにアクセスできるようにすることです。NetScaler は、アプリケーショントラフィ ックをオンプレミスまたは Azure クラウド上の最適な分散ワークロード/サーバーにルーティングし、アプリケーシ ョンサーバーのヘルスステータスを提供するグローバル負荷分散機能によって、このユニークなユースケースを解決 します。

使用例

オンプレミスネットワークと異なる Azure VNet のユーザーは、内部ネットワーク内の最適なサーバーに接続して、 必要なコンテンツにアクセスできます。これにより、アプリケーションが常に利用可能になり、コストが最適化され、 ユーザーエクスペリエンスが向上します。ここでは、Azure プライベートトラフィック管理 (PTM) が主な要件です。 Azure PTM は、ユーザーの DNS クエリがアプリケーションサーバーの適切なプライベート IP アドレスに解決され るようにします。

ユースケースソリューション

NetScaler には、Azure PTM の要件を満たすグローバルサーバー負荷分散(GSLB)機能が含まれています。GSLB は DNS サーバーのように機能し、DNS リクエストを受け取り、DNS リクエストを適切な IP アドレスに解決して以下を提供します。

- DNS ベースのシームレスなフェイルオーバー。
- オンプレミスからクラウドへの段階的移行。
- 新機能の A/B テスト。

サポートされている多くの負荷分散方法の中で、このソリューションでは次の方法が役立ちます。

- 1. ラウンドロビン
- 2. 静的近接性 (ロケーションベースのサーバー選択)。次の2つの方法で導入できます。
 - a) NetScaler 上の EDNS クライアントサブネット (ECS) ベースの GSLB。
 - b) すべての仮想ネットワークに DNS フォワーダーをデプロイします。

トポロジ



次の図は、Azure プライベート DNS ゾーンの NetScaler GSLB デプロイメントを示しています。

ユーザーは、Azure プライベート DNS ゾーンの NetScaler GSLB メソッドに基づいて、Azure またはオンプレミ スの任意のアプリケーションサーバーにアクセスできます。オンプレミスと Azure 仮想ネットワーク間のすべてのト ラフィックは、安全な VPN トンネルのみを経由します。アプリケーショントラフィック、DNS トラフィック、およ びモニタリングトラフィックは、前述のトポロジに示されています。必要な冗長性に応じて、NetScaler と DNS フ ォワーダーを仮想ネットワークとデータセンターに導入できます。わかりやすくするために、ここでは NetScaler を 1 つだけ表示していますが、Azure リージョンには少なくとも 1 セットの NetScaler と DNS フォワーダーを使用す ることをお勧めします。すべてのユーザー DNS クエリは、まずクエリを適切な DNS サーバーに転送するためのルー ルが定義されている DNS フォワーダーに送られます。

Azure DNS プライベートゾーン用 NetScaler 構成

テストした製品とバージョン:

ProductバージョンAzureクラウドサブスクリプションNetScaler VPXBYOL (独自のライセンスを持参)

注

導入はテスト済みで、NetScaler バージョン 12.0 以降と変わりません。

前提条件

一般的な前提条件は次のとおりです。

- サブスクリプションが有効な Microsoft Azure ポータルアカウント。
- オンプレミスと Azure クラウド間の接続 (セキュア VPN トンネル) を確認します。Azure で安全な VPN トン ネルを設定するには、「ステップバイステップ:Azure とオンプレミス間のサイト間 VPN ゲートウェイの設定」 を参照してください。

ソリューションの説明

HTTP 上で動作し、ラウンドロビン GSLB 負荷分散方式に基づくイントラネットアクセスで Azure とオンプレミス 全体にデプロイされる Azure DNS プライベートゾーン (rr.ptm.mysite.net) を 1 つのアプリケーションをホスト する場合。この展開を実現するには、NetScaler を使用して Azure プライベート DNS ゾーンの GSLB を有効にし ます。このゾーンには次の構成が含まれます。

- 1. Azure とオンプレミスのセットアップを設定します。
- 2. Azure 仮想ネットワーク上の NetScaler アプライアンス。

Azure とオンプレミスセットアップの設定

トポロジに示されているように、Azure 仮想ネットワーク (この場合は VNet A、VNet B) とオンプレミスセットアップを設定します。

- 1. ドメイン名 (mysite.net) を使用して Azure プライベート DNS ゾーンを作成します。
- 2. Azure リージョンのハブアンドスポークモデルに2つの仮想ネットワーク (VNet A、VNet B) を作成します。
- 3. VNet A にアプリケーションサーバー、DNS フォワーダー、Windows 10 Pro クライアント、NetScaler を デプロイします。
- 4. アプリケーションサーバーをデプロイし、VNet B にクライアントがある場合は DNS フォワーダーをデプロ イします。
- 5. アプリケーションサーバー、DNS フォワーダー、および Windows 10 pro クライアントをオンプレミスにデ プロイします。

Azure プライベート DNS ゾーン

ドメイン名を使用して Azure プライベート DNS ゾーンを作成します。

- 1. Azure Portal にログインし、ダッシュボードを選択または作成します。
- 2. [リソースの作成] をクリックし、DNS ゾーンを検索して、ドメイン名 (mysite.net) の Azure プライベート DNS ゾーン (この場合は mysite.net) を作成します。

Home > mysite.net							
mysite.net							\$ ×
	$\overset{K}{+} \operatorname{Record} \operatorname{set} \rightarrow \operatorname{Move}$	e 🛅 Delete zone 👌 R	efresh				
Overview	Resource group (change) gslb_phase2			Name server 1			
Activity log	Subscription (change)	agained Stationary		Name server 2			
Access control (IAM)	Subscription ID	7 ad072000caa2		Name server 3			
🛹 Tags	10400085-1521-4511-000	1-eu0/3030Cea3		-			
lpha Diagnose and solve problems				Name server 4 -			
Settings	Tags (change) Click here to add tags						
Properties				*			
Locks	\wp Search record sets						
Automation script	NAME	TYPE	TTL	VALUE	ALIAS RESOURCE TYPE	ALIAS TARGET	
Monitoring				Email: azuredns-ho Host: internal.clou			
😲 Alerts	@	SOA	3600	Refresh: 3600 Retry: 300			
iii Metrics				Expire: 2419200 Minimum TTL: 300 Social number: 1			
Support + troubleshooting				Serial humber: 1			
New support request							

ハブアンドスポークモデルの Azure 仮想ネットワーク (VNet A、VNet B)

Azure リージョンのハブアンドスポークモデルに2つの仮想ネットワーク (VNet A、VNet B) を作成します。

- 1.2つの仮想ネットワークを作成します。
- 同じダッシュボードを選択し、リソースの作成 をクリックして仮想ネットワークを検索し、同じリージョン に VNet A と VNet B という 2 つの仮想ネットワークを作成し、それらをピアリングして、次の図に示すよう にハブ アンド スポーク モデルを形成します。ハブ アンド スポーク トポロジを設定する方法の詳細について は、「Azure でハブ スポーク ネットワーク トポロジを実装する」を参照してください。

Virtual_INELWORK_A_I					
,♀ Search (Ctrl+/)	≪ 🏷 Refresh → M	ove 🔟 Delete			
> Overview	Resource group (cha GSLB_Phase2	<u>nge)</u>	Address space 10.8.0.0/16		
Activity log	Location		DNS servers		
Access control (IAM)	Subscription (change	e)	10.8.0.6		
👂 Tags	NSDev Platform Cit	ment assessible to a com			
K Diagnose and solve problems	Subscription ID 764bc6a9-7927-431	1-8e67-ed073090cea3			
iettings	Tags (change)				
-> Address space	Click here to add tags		*		
 Connected devices 	Connected devi	ces			
 Subnets 		1 devices			
DDoS protection	DEVICE	°↓ TYPE	1 IP ADDRESS	↑↓ SUBNET	
Firewall (Preview)	nsvneta210	Network interface	10.8.0.4	default	
DNS servers	nsvneta210	Network interface	10.8.0.5	default	
>> Peerings	dnsforwarder962	Network interface	10.8.0.6	default	
Service endpoints	clientvneta27	Network interface	10.8.0.7	default	
Properties Locks tome > Virtual_Network_B_10_9 Virtual_Network_B_11_9	Azure2AwsGW	Virtual network gateway		GatewaySubnet	
Properties Locks Home > Virtual_Network_B_10.9 Virtual_Network_B_11 Virtual_network	Azure2AwsGW	Virtual network gateway		GatewaySubnet	
Properties Locks Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual network Search (Ctrl+/)	Azure2AwsGW 0_9 ≪ Č Refresh → Ma	Virtual network gateway	•	GatewaySubnet	
Properties Locks Home > Virtual_Network_B_10_9 Virtual_Network_B_10_9 Virtual_Network Search (Ctrl+/) Overview	Azure2AwsGW Azure2AwsGW	Virtual network gateway	- Address space 10.9.00/16	GatewaySubnet	
Properties Locks torks Virtual_Network_B_10_9 Virtual_Network_B_10 Search (Ctr(+/) Overview Activity log	Azure2AwsGW Azure2AwsGW 0_9	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	,
Properties Locks Home > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Overview Activity log Activity log Access control (IAM)	Azure2AwsGW Azure2AwsGW 0_9 ≪ Č Refresh → Ma GSLB_Phase2 Location West US Subscription (change	Virtual network gateway	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	
Properties Locks Home > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags	Azure2AwsGW Azure2AwsGW 0_9 ≪ C Refresh → Mc GSLB_Phase2 Location West US Subscription (change	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	;
Properties Locks tome > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Verview Activity log Access control (IAM) Tags Diagnose and solve problems	Azure2AwsGW Azure2AwsGW 0_9 ≪ ℃ Refresh → Mc GSLB_Phase2 Location West US Subscription (Change Subscription ID 764bc6a9-7927-4311	Virtual network gateway	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	;
Properties Locks Nome > Virtual_Network_B_10_9 Virtual_Network_B_10 Virtual_network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings	Azure2AwsGW Azur	Virtual network gateway	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	,
Properties Locks Cocks Cock	Azure2AwsGW Azure2AwsGW Azure2AwsGW 0_9 ≪ C Refresh → Ma GSLB_Phase2 Location West US Subscription (change Subscription ID 764bc6a9-7927-4311 Tags (change) Click here to add tags	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	
Properties Locks Conce > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems settings Address space Connected devices	Azure2AwsGW A	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	,
Properties Locks Home > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Access control (IAM) Connected devices Subnets	Azure2AwsGW A	Virtual network gateway	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	,
 Properties Locks Home > Virtual_Network_B_10_9 Virtual network Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems iettings Address space Connected devices Subnets DDoS protection 	Azure2AwsGW A	Virtual network gateway Virtua	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	;
 Properties Locks torks Virtual_Network_B_10_9 Virtual_Network_B_11_ Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems iettings Address space Connected devices Subnets DDoS protection Firewall (Preview) 	Azure2AwsGW A	Virtual network gateway Virtua	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	
 Properties Locks Locks Virtual_Network_B_10_9 Virtual_network Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems Address space Connected devices Subnets DDoS protection Firewall (Preview) DNS servers 	Azure2AwsGW A	Virtual network gateway Virtual network interface Virtual network interf	- Address space 10.9.00/16 DNS servers 10.9.0.6	GatewaySubnet	;
Properties Locks Conserverse Conserverse Connected devices Conne	Azure2AwsGW Azur	Virtual network gateway Virtual network interface Virtual network inte	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	
Properties Locks Conce > Virtual_Network_B_10_9 Virtual_Network_B_11 Virtual_Network_B_11 Virtual network Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Diagnose and solve problems Activity log Access control (IAM) Tags Connected devices Subnets DDoS protection Firewall (Preview) DDOS protection Firewall (Preview) DDNS servers Peerings Service endpoints	Azure2AwsGW Azur	Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network gateway Virtual network interface	- Address space 10.9.0.0/16 DNS servers 10.9.0.6	GatewaySubnet	,

VNet A から VNet B へのピアリング

VNet A \geq VNet B $\leq \ell \sim \ell$ VNet A $\leq \ell \sim \ell$

- 1. VNet A とピア VNet B の [** 設定] メニューから [ピアリング **] をクリックします。
- 2. 次の図に示すように、[転送トラフィックを許可する]と[ゲートウェイトランジットを許可する]を有効にします。

Vnet_A_to_B Virtual_Network_A_10_8		
R Save X Discard	🛅 Delete	
Name		
Vnet_A_to_B		
Peering status		
Connected		
Provisioning state		
Succeeded		
Peer details		
Address space		
10.9.0.0/16		
Virtual network		
Virtual_Network_B_10_9		
Configuration		
Allow virtual network a	cess 🚯	
Disabled Enabled		
✓ Allow forwarded tr	ffic 🚯	
✓ Allow gateway trans	it O	

次の図は、VNet A と VNet B の正常なピアリングを示しています。

Home > Virtual_Network_A_10_8 - Peerin	gs			
Virtual_Network_A_10_8 -	Peerings			
	🕂 Add			
Overview	✓ Search peerings			
Activity log	NAME	PEERING STATUS	PEER	GATEWAY 1
Access control (IAM)	Vnet_A_to_B	Connected	Virtual_Network_B_10_9	Enabled
🛹 Tags				
X Diagnose and solve problems				

VNet B から VNet A へのピアリング

- 1. VNet B とピア VNet A の [** 設定] メニューから [ピアリング **] をクリックします。
- 2. 次の図に示すように、[転送トラフィックを許可し、リモートゲートウェイを使用する]を有効にします。

<pre>1 ![VNet B to A](/en-us/vpx/media/image-07.png)</pre>				
	Но	me > Virtual_Network_B_10_9 - Peer	ings	
	.	Virtual_Network_B_10_9	- Pe	erings
	,0	Search (Ctrl+/)	<	🕂 Add
	$\langle \cdots \rangle$	Overview	A	
		Activity log		NAME
		Access control (IAM)		Vnet_B_to_A
次の図は、VNet B から VNet A へのピアリングが成功したことを示しています		Tags		L

VNet A にアプリケーションサーバー、DNS フォワーダー、Windows 10 Pro クライアント、NetScaler をデプ ロイします

アプリケーションサーバー、DNS フォワーダー、Windows 10 プロクライアント、および VNet A 上の NetScaler について簡単に説明します。

- 1. 同じダッシュボードを選択し、[リソースを作成]をクリックします。
- 2. それぞれのインスタンスを検索し、VNet A サブネットから IP を割り当てます。

アプリケーションサーバー アプリケーションサーバーは、Ubuntu サーバー 16.04 が Azure またはオンプレミス VM にインスタンスとしてデプロイされている Web サーバー(HTTP サーバー)に他なりません。Web サーバーと して設定するには、コマンドプロンプトで次のように入力します。

sudo apt install apache2

Windows 10 Pro Client Windows 10 Pro インスタンスを VNet A およびオンプレミスのクライアントマシン として起動します。

NetScaler NetScaler は、NetScaler MAS のヘルスチェックと分析によって Azure DNA プライベートゾーン を補完しています。要件に基づいて Azure Marketplace から NetScaler を起動します。ここでは、NetScaler (BYOL) を使用してデプロイしました。

Microsoft Azure に NetScaler をデプロイする方法の詳細な手順については、こちらをご覧ください。Microsoft Azure に NetScaler VPX インスタンスをデプロイするを参照してください。

展開後、NetScaler IP を使用して NetScaler ADC GSLB を構成します。

DNS フォワーダー NetScaler GSLB (ADNS IP) にバインドされたホストドメインのクライアント要求を転送す るために使用されます。Ubuntu サーバー 16.04 を Linux インスタンス(Ubuntu サーバー 16.04)として起動し、 DNS フォワーダーとして設定する方法については、以下の URL を参照してください。

注

ラウンドロビン GSLB 負荷分散方法では、Azure リージョン用の DNS フォワーダーは 1 つで十分ですが、静 的近接の場合は、仮想ネットワークごとに 1 つの DNS フォワーダーが必要です。

- 1. フォワーダーをデプロイしたら、次の図に示すように、仮想ネットワーク A の DNS サーバー設定をデフォル トから VNet A の DNS フォワーダー IP を使用してカスタムに変更します。
- 2. VNet A DNS named.conf.options フォワーダー内のファイルを変更して、ドメイン (mysite.net) とサブドメイン (ptm.mysite.net) の転送ルールを NetScaler GSLB の ADNS IP に追加します。
- 3. DNS フォワーダーを再起動して、named.conf.optionsファイルに加えられた変更を反映します。

```
VNetAのDNSフォワーダー設定
zone "mysite.net" {
1
2
3
                       type forward;
          forwarders {
4
5
     168.63.129.16;
                        }
6
    ;
7
            }
8
     ;
          zone "ptm.mysite.net" {
9
10
               type forward;
11
               forwarders {
13
     10.8.0.5; }
14
     ;
            }
15
16
```

注

ドメイン (「mysite.net」) ゾーンの IP アドレスには、Azure リージョンの DNS IP アドレスを使用してくだ さい。サブドメイン (「ptm.mysite.net」) ゾーン IP アドレスには、GSLB インスタンスのすべての ADNS IP アドレスを使用してください。

VNet B にクライアントがある場合は、アプリケーションサーバーと DNS フォワーダーをデプロイします

1. 仮想ネットワーク B の場合は、同じダッシュボードを選択し、「リソースを作成」をクリックします。

2. それぞれのインスタンスを検索し、VNet B サブネットから IP を割り当てます。

- 3. VNet A と同様の静的近接 GSLB 負荷分散がある場合は、アプリケーションサーバーと DNS フォワーダーを 起動します。
- 4. 次の設定に示すように、named.conf.optionsの VNet B の DNS フォワーダ設定を編集します。

VNet B の DNS フォワーダー設定:







アプリケーションサーバー、DNS フォワーダー、および Windows 10 pro クライアントをオンプレミスにデプロイ

- 1. オンプレミスの場合は、ベアメタルで仮想マシンを起動し、アプリケーションサーバー、DNS フォワーダー、 および VNet A と同様の Windows 10 プロクライアントを用意します。
- 2. 次の例に示すように、named.conf.optionsのオンプレミス DNS フォワーダー設定を編集します。

```
オンプレミス DNS フォワーダー設定
1
        zone "mysite.net" {
2
3
                    type forward;
4
                    forwarders {
5
   10.8.0.6; \}
6
  ;
7
          }
8
    ;
9
        zone "ptm.mysite.net" {
```

```
11 type forward;
12 forwarders {
13 10.8.0.5; }
14 ;
15 }
16 ;
```

mysite.netについては、Azure プライベート DNS ゾーンサーバー IP の代わりに VNet A の DNS フォワーダ ー IP を指定しました。そのため、オンプレミスの DNS フォワーダー設定ではこの変更が必要です。

Azure 仮想ネットワーク上で NetScaler を構成します

トポロジーに示されているように、NetScaler を Azure 仮想ネットワーク(この場合は VNet A)にデプロイし、 NetScaler GUI を介してアクセスします。

NetScaler GSLB の設定

- 1. ADNS サービスを作成します。
- 2. ローカルサイトとリモートサイトを作成します。
- 3. ローカル仮想サーバー用のサービスを作成します。
- 4. GSLB サービス用の仮想サーバーを作成します。

ADNS サービスを追加

- 1. NetScaler ユーザーインターフェイスにログインします。
- 2. [設定]タブで、[トラフィック管理]>[負荷分散]>[サービス]に移動します。
- 3. サービスを追加します。サービスを追加します。次の図に示すように、ADNS サービスを TCP と UDP の両方 で設定することをお勧めします。

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

Service Name*	
s_adns	2
O New Server	
Server*	
10.8.0.5 (10.8.0.5)	\sim
Protocol*	
ADNS	\sim
Port*	
53	

Service	¢	Load	Ba	lano	cing	Serv	ice
---------	---	------	----	------	------	------	-----

	Basic Settings	
	Service Name*	
	ADNS_TCP	
	New Server Existing Server	
	IP Address*	
	10 . 8 . 0 . 5	
	Protocol*	
	ADNS_TCP V	
	Port*	
	53	
	More	
Q Search in Menu	Traffic Management / Load Balancing / Services / Services	
System	> Services	Q
Traffic Management	Services 2 Auto Detected Services 0 Internal Services 7	
Load Balancing	✓ Add Edit Delete Statistics No action ✓	Search \sim
Virtual Servers Services	Name State IP Address/Domain Name Port Protocol Max Clients Max Requests Cache Type	Traffic D
Service Group	s azurelbdnsservice0 • DOWN 168.63.129.16 53 DNS 0 0 SERVER	
Monitors	□ s_adins ●UP 10.8.0.5 53 ADNS 0 0 SERVER	

GSLB サイトを追加する

- 1. GSLB を設定するローカルサイトとリモートサイトを追加します。
- 2. [設定]タブで、[トラフィック管理]>[GSLB]>[GSLB サイト]に移動します。次の例のようにサイトを追加し、他のサイトについても同じ手順を繰り返します。次の例に示すようにサイトを追加し、他のサイトに対しても同じ手順を繰り返します。

Ġ Create GSLB Site

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

Q. Search in Menu		Traffic Manag	gement / GS	LB / GSLB Sites						
System	>	GSLB S	Sites							
AppExpert	>									
Traffic Management	~	Add	Edit De							
Load Balancing	>		Name	Metric Exchange (ME)	Site Metric MEP Status	Site IP Address	Туре	Public IP Address	Parent Site Name	Backup Pa
Content Switching	(1) >		s1	ENABLED		10.8.0.5	LOCAL	10.8.0.5		
Carbo Dadiraction	<u>~</u> \	4								

GSLB サービスの追加

- アプリケーションサーバーの負荷分散を行うローカルおよびリモートの仮想サーバー用の GSLB サービスを 追加します。
- 2. [設定] タブで、[トラフィック管理] > [GSLB] > [GSLB サービス] に移動します。
- 3. 次の例に示すようにサービスを追加します。
- 4. HTTP モニターをバインドしてサーバーのステータスを確認します。

GSLB Service

Basic Settings	
Service Name*	
service_vnetA	
Site Name*	_
s1 ~ +	
Site Type	
LOCAL	
Type*	
IP Based 🗸 🗸	
Service Type*	
HTTP 🗸	
Port*	
80	

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. サービスを作成したら、GSLB サービス内の [詳細設定] タブに移動します。
- 6.「モニターを追加」をクリックして、GSLB サービスを HTTP モニターにバインドし、サービスの状態を表示しま GSLB Service Load Balancing Monitor Binding ×

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

7. HTTP モニターにバインドすると、次の図に示すように、サービスの状態は UP とマークされます。

Q Search in Menu		Traffic Manage	ement / GSLB / GS	SLB Services							
System	>	GSLB S	ervices								
AppExpert	>										
Traffic Management	\sim	Add	Edit Delete	Statistics	No action 🗸					Search 🗠	
Load Balancing	>	•	Name	State	Effective State	IP Address	Port	Canonical Name	Protocol	Туре	
Content Switching	•		service_vnetA	●UP	DOWN	10.8.0.6	80		HTTP	LOCAL	
Cache Redirection	•		service_vnetB	• UP	DOWN	10.9.0.4	80		HTTP	LOCAL	
DNS	>		service_Aws	• UP	DOWN	10.12.0.31	80		HTTP	LOCAL	

Q Search in Menu		Traffic Manag	ement / GSLB / GS	LB Services							
System	>	GSLB S	_B Services								
Traffic Management	~	Add	Edit Delete	Statistics	No action 🗸 🗸					Search \vee	
Load Balancing	>	•	Name	State	Effective State	IP Address	Port	Canonical Name	Protocol	Туре	
Content Switching	<u> </u>		service_vnetA	• UP	• DOWN	10.8.0.6	80		HTTP	LOCAL	
Cache Redirection	<u> </u>		service_vnetB	• UP	DOWN	10.9.0.4	80		HTTP	LOCAL	
DNS	>		service_Aws	O UP	DOWN	10.12.0.31	80		HTTP	LOCAL	

GSLB 仮想サーバーの追加

アプリケーションサーバーのエイリアス GSLB サービスにアクセスできる GSLB 仮想サーバーを追加します。

- 1. [設定] タブで、[トラフィック管理] > [GSLB] > [GSLB 仮想サーバー] に移動します。
- 2. 次の例のように仮想サーバーを追加します。
- 3. GSLB サービスとドメイン名をそれにバインドします。

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 (EDR)	
When this Virtual Server is LIP	
Send all "active" service IPs' in response (MIP)	
Send all active service is intesponse (with)	
EDNS Client Subnet	
Respond with ECS option in the response for a DNS query with EC	S
Validate ECS address is a private or unroutable address	
Comments	

4. GSLB 仮想サーバーを作成し、適切な負荷分散方法 (この場合はラウンドロビン) を選択したら、GSLB サービ スとドメインをバインドして手順を完了します。

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

- 5. 仮想サーバー内の [詳細設定] タブに移動し、[ドメインの追加] タブをクリックしてドメインをバインドしま す。
- 6. [詳細設定]>[サービス] に移動し、矢印をクリックして GSLB サービスをバインドし、3 つのサービス (VNet A、VNet B、オンプレミス) すべてを仮想サーバーにバインドします。

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

GSLB サービスとドメインを仮想サーバーにバインドすると、次の図のように表示されます。

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

GSLB 仮想サーバーが稼働していて、100% 正常かどうかを確認します。モニターにサーバーが稼働していて正常で あることが示されたら、サイトが同期されており、バックエンドサービスが利用可能であることを意味します。

Q Search in Menu		Traffic Manage	ement / GSLB / GSLB Virtual Ser	vers						
System	>	GSLB V	SLB Virtual Servers							
AppExpert	>									
Traffic Management	\sim	Add Edit 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				

デプロイをテストするには、クラウドクライアントマシンまたはオンプレミスクライアントマシンからドメイン URL rr.ptm.mysite.netにアクセスします。クラウド Windows クライアントマシンからアクセスする場合は、 サードパーティの DNS ソリューションやカスタム DNS ソリューションを必要とせずに、プライベート DNS ゾーン でオンプレミスのアプリケーションサーバーにアクセスするようにしてください。 Azure アクセラレーションネットワークを使用するように NetScaler VPX インスタン スを構成する

October 17, 2024

高速ネットワーキングにより、仮想マシンへのシングルルート I/O 仮想化 (SR-IOV) 仮想機能 (VF) NIC が有効にな り、ネットワークのパフォーマンスが向上します。この機能は、信頼性の高いストリーミングと低い CPU 使用率で、 より高いスループットでデータを送受信する必要がある負荷の高いワークロードで使用できます。NIC で高速ネット ワークが有効になっている場合、Azure は NIC の既存の準仮想化 (PV) インターフェイスを SR-IOV VF インターフ ェイスとバンドルします。SR-IOV VF インターフェイスのサポートにより、NetScaler VPX インスタンスのスルー プットが有効になり、向上します。

高速ネットワーキングには、次の利点があります。

- 低レイテンシ
- •1秒あたりのパケット数 (pps) のパフォーマンスが向上
- スループットの強化
- ジッタの低減
- CPU 使用率の低下

注

Azure アクセラレーションネットワーキングは、リリース 13.0 ビルド 76.29 以降の NetScaler VPX インス タンスでサポートされています。

前提条件

- VM のサイズが Azure アクセラレーションネットワーキングの要件と一致していることを確認します。
- 任意の NIC で高速ネットワーキングを有効にする前に、VM(個別または可用性セット内)を停止します。

制限事項

高速ネットワーキングは、一部のインスタンスタイプでのみ有効にできます。詳細については、「サポートされるイン スタンスタイプ」を参照してください。

高速ネットワーキングでサポートされる NIC

Azure では、ネットワークを高速化するために SR-IOV モードの Mellanox ConnectX3、ConnectX4、および ConnectX5 NIC が提供されています。

NetScaler VPX インターフェイスでアクセラレーテッドネットワーキングが有効になっている場合、Azure は ConnectX3、ConnectX4、または ConnectX5 インターフェイスのいずれかを NetScaler VPX アプライアンスの 既存の PV インターフェイスにバンドルします。

仮想マシンにインターフェイスをアタッチする前に高速ネットワークを有効にする方法の詳細については、「高速ネッ トワークを使用したネットワークインターフェイスの作成」を参照してください。

仮想マシンの既存のインターフェイスで高速ネットワーキングを有効にする方法の詳細については、「仮想マシンで既存のインターフェイスを有効にする」を参照してください。

Azure コンソールを使用して NetScaler VPX インスタンスで高速ネットワークを有効にする方法

Azure コンソールまたは Azure PowerShell を使用して、特定のインターフェイスで高速ネットワークを有効にできます。

Azure のアベイラビリティセットまたはアベイラビリティーゾーンを使用して高速ネットワークを有効にするには、 次の手順を実行します。

1. Azure ポータルにログインし、Azureマーケットプレイスにナビゲートします。

Microsoft Azure	resources, services	s, and docs (G+/)			2	IF 🗘 🤅	≩ ? ☺
Azure services	e Virtual machines	Subscriptions	Resource	Co App Services	Storage	SQL databases	Azure Database

2. Azure Marketplace から NetScaler を検索してください。

\equiv Microsoft Azure	$ \mathcal{P}$ Search resources, services, and do	cs (G+/)	D 4	↓ @ ? ©
Home >				
Marketplace				
Recently created		X Pricing : All X Oper	rating System : All 🗙 Publisher	Type : All $ imes$
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
Blockchain	Citrix Application Delivery Controller:	Azure Application 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 Free	Price varies	Bring your own license	Bring your own license
	Create 🗸 💙	Create 🗸 🛇	Create 🗸 💙	Create \checkmark

3. ライセンスとともに FIPS 以外の NetScaler プランを選択し、[作成] をクリックします。



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

[NetScaler の作成] ページが表示されます。

4. [基本] タブで、リソースグループを作成します。[パラメータ] タブで、地域、管理者ユーザー名、管理者パス ワード、ライセンスタイプ (VM SKU)、およびその他のフィールドの詳細を入力します。

Home > NetScaler ADC 14.1 >

Create a virtual machine

Instance details		
Virtual machine name * 🔅	vpx-aan	~
Region * 🥡	(US) East US	\sim
Availability options ①	Availability zone	~
Availability zone * 🕠	Zones 1	~
	You can now select multiple zones. Selecting multiple zones will create o per zone. Learn more 2	ne VM
Security type 🔅	Standard	\sim
Image * 🕕	NetScaler ADC 14.1 VPX Standard Edition - 5000 Mbps - x64 Gen1	\sim
	See all images Configure VM generation	
VM architecture (i)	O Arm64	
	● x64	
	Arm64 is not supported with the selected image.	
Run with Azure Spot discount 🕕		
Size * i	Standard_DS2_v2 - 2 vcpus, 7 GiB memory (\$ 1,743.24/month)	~
	See all sizes	
Administrator account		
Authentication type (i)	○ SSH public key	
	Password	
Username * 🔅	nsroot	
Password * (i)	••••••	
Confirm password * 🕠		
Inhound port rules		
Select which virtual machine network	y parts are accessible from the public internet. You can specify more limited or grap	ular
network access on the Networking ta	ab.	ulai
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.	
Devidence & encoder	Density of Nexts Disland	

5. [次へ]をクリックします: VM 構成 >。

[VM構成]ページで、次の手順を実行します。

- a) パブリック IP ドメイン名サフィックスを設定します。
- b) Azure モニタリングメトリクスを有効または無効にします。
- c) バックエンドオートスケールを有効または無効にします。

■ Microsoft Azure	resources, services, and docs (G+/)	2	Ŗ	L	?	\odot
Home > Marketplace > Citrix ADC >						
Create Citrix ADC						
Basics VM Configurations Netwo	rk and Additional Settings Review + create					
Virtual Machine Configurations						
Virtual machine size * 🕠	2x Standard DS3 v2					
	Change size					
OS disk type ①	Premium_LRS					
Assign Public IP (Management) ①	• Yes					
Assign Public IP (Client traffic) ①	• Yes					
Unique public IP domain name suffix * 🔅	4610d1d706					
Azure Monitoring Metrics ①	Enabled					
	Disabled					
Backend Autoscale 🛈	C Enabled					
	Disabled					
Review + create < Previous	Next : Network and Additional Settings >					

6. 次へ:ネットワークと追加設定をクリックします。

[ネットワークとその他の設定]ページで、ブート診断アカウントを作成し、ネットワーク設定を構成します。

[高速ネットワーキング] セクションには、管理インターフェイス、クライアントインターフェイス、およびサ ーバインターフェイスについて、アクセラレーションネットワーキングを個別に有効または無効にするオプシ ョンがあります。

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. [次へ]をクリックします: レビュー+作成する>。

検証が成功したら、基本設定、仮想マシンの構成、ネットワーク、および追加設定を確認し、[作成]をクリックします。Azure リソースグループが必要な構成で作成されるまでに時間がかかる場合があります。



8. デプロイが完了したら、リソースグループを選択して設定の詳細を確認します。

Download a template for automation

< Previous Next

Create

	resources, services, and docs (G+/)		} 🗘 🕸	? 😊
Home > citrix.netscalervpx-1vm-3nic-20	210204125107 > test-aan· > citrix.netscalervpx-1vm-3nic-20210204	125107 >		
✓ Search (Ctrl+/) «	$+$ Add $\equiv\equiv$ Edit columns 📋 Delete resource group 💍 Refresh 🚽	Export to CSV	Open query	🖉 Assign ta
Overview Activity log Access control (IAM) Tags Events Events Image: Control (IAM)	✓ Essentials Subscription (change) NSDev Platform CA. Subscription ID 764bc6a9-7927-4311-8e67-ed073090cea3 Tags (change) Click here to add tags	Deployments 2 Succeeded Location South India		
Settings	Filter for any field Type == all × Location == all ×	⁺┳ Add filter		
DeploymentsSecurity	Showing 1 to 22 of 22 records. Show hidden types ①		No grouping	~
Policies	Name ↑↓	Туре ↑↓	_	Location
Properties Locks	<pre></pre>	Virtual machine		South Cer
	in the second se			

9. 高速ネットワーク構成を確認するには、[仮想マシン]>[ネットワーク]を選択します。アクセラレートネット ワーキングのステータスは、NIC ごとに [有効]または [無効]と表示されます。

■ Microsoft Azure	esources, services, and docs	(G+/)		D D	🖉 🐵 ? 🤅)
Home > citrix.netscalervpx-1vm-3nic-2021 citrix-adc-vpx-0 Virtual machine P Search (Ctrl+/)	10204125107 > test-aan- tworking	> citrix.netscalerv	px-1vm-3nic-20210204125107 interface	> test-aan	> citrix-adc-vpx-0	
Overview Activity log Access control (IAM) Tags	citrix-adc-vpx-nic01-0 IP configuration ① nsip (Primary)	citrix-adc-vpx-nic11-	0 citrix-adc-vpx-nic12-0	ß		
Diagnose and solve problems Settings Networking Ornect	Network Interface: Virtual network/subnet: c Accelerated network Inbound port rules	citrix-adc-vpx-nic01-0 itrix-adc-vox-virtual-netw sing: Enabled	Effective security rules ork/01-management-subnet Application security groups	Topology NIC Public IP: 13. Load balance	66.88.43 NIC Priv	ate IP: 172.17.40.5
DisksSize	Network security gi Impacts 0 subnets, 1 Priority	roup citrix-adc-vpx-nic0 network interfaces Name	1-nsg-0 (attached to network i Port	nterface: citrix-ad	dc-vpx-nic01-0) Source	Add inbound p
 Security Advisor recommendations 	1022	▲ ssh-22-rule	22	тср	Internet	Any

Azure PowerShell を使用して高速ネットワーキングを有効にする

仮想マシンの作成後に高速ネットワークを有効にする必要がある場合は、Azure PowerShell を使用して有効化でき ます。

注

Azure PowerShell を使用した高速ネットワーキングを有効にする前に、仮想マシンを停止してください。

Azure PowerShell を使用して高速ネットワークを有効にするには、次の手順を実行します。

1. Azure ポータルに移動し、右上隅にある PowerShell アイコンをクリックします。

注

Bash モードの場合は、PowerShell モードに切り替えます。

≡	Microsoft Azure		🕑 🎡 (? 😳			
Но	Home > citrix.netscalervpx-1vm-3nic-20210204125107 > test-aan > citrix.netscalervpx-1vm-3nic-20210204125107 > test-aan > citrix-adc-vpx-0						
Ś	citrix-adc-vp	x-0 Networking					
P	Search (Ctrl+/)	« $\beta^{\mathcal{G}}$ Attach network interface $\beta^{\mathcal{G}}$ Detach network interface					
•	Overview	A					
	Activity log	citrix-adc-vpx-nic01-0 citrix-adc-vpx-nic11-0 citrix-adc-vpx-nic12-0					
<mark>م</mark> ا	Access control (IAM)	▼ ID configuration ∩	<u>}</u>				
			:	×			
		Welcome to Azure Cloud Shell					
		Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session. Bash PowerShell					

2. コマンドプロンプトで、次のコマンドを実行します:

1 az network nic update --name <nic-name> --accelerated-networking
[true | false] --resource-group <resourcegroup-name>

アクセラレートネットワーキングパラメータは、次のいずれかの値を受け入れます。

- True: 指定した NIC で高速ネットワーキングを有効にします。
- False: 指定された NIC のアクセラレーションネットワーキングを無効にします。

特定の NIC で高速ネットワーキングを有効にするには、次の手順を実行します。

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

特定の NIC で高速ネットワーキングを無効にするには、次の手順を実行します。

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

3. デプロイが完了した後にアクセラレーテッドネットワーキングのステータスを確認するには、[VM]>[ネット ワーク] に移動します。

次の例では、アクセラレートネットワーキングが有効になっていることを確認します。

		10 - 0		— —	2 m o	
	sources, services, and doc	s (G+/)		∑_ ¶\$	L, 1235 (
Home > citrix.netscalervpx-1vm-3nic-2021	0204125107 > test-aan	 > citrix.netscalery 	px-1vm-3nic-20210204125107	> test-aan	> citrix-adc-v	рх-0
citrix-adc-vpx-0 Net	working					
✓ Search (Ctrl+/) «	🖉 Attach network inter	face 🖉 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)			۲ ۲	}	
🗳 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-vox-virtual-netw rking: Enabled	ork/01-management-subnet	NIC Public IP: 1	3.66.88.43 NI	C Private IP: 172.17.40.5
S Connect	Inbound port rules	Outbound port rules	Application security groups	Load balan	cing	
😸 Disks	Network security of Impacts 0 subnets,	group citrix-adc-vpx-nic0 1 network interfaces	11-nsg-0 (attached to network ir	nterface: citrix-a	dc-vpx-nic01-0)	Add inbound p
📮 Size	Priority	Name	Port	Protocol	Source	Destinatio
🔋 Security	1022	▲ ssh-22-rule	22	TCP	Interne	t Any
Advisor recommendations						

次の例では、アクセラレートネットワーキングが無効になっていることがわかります。

	Microsoft Azure	𝒫 Search re	sources, services, and docs	(G+/)		∑ ¶7 Q	🎯 ? 😳	
Hon	ne > citrix-adc-vpx-0							
	citrix-adc-vp>	<-0 Net	working					×
P	Search (Ctrl+/)	«	🖉 Attach network interfa	ce 🔊 Detach network	interface			
<u>የ</u> ዶ	Access control (IAM)	-						A
1	Tags	- 1	citrix-adc-vpx-nic01-0	citrix-adc-vpx-nic11-	0 citrix-adc-vpx-nic12-0			
Þ	Diagnose and solve probler	ns	IP configuration ①					
Sett	ings	- 1	nsip (Primary)	\checkmark				
2	Networking		Network Interface:	citrix-adc-vpx-nic01-0	Effective security rules	Topology		
ø	Connect Virtual network/subnet: citrix-adc-vpx-virtual-network/01-management-subnet NIC Public IP: 13.66.88.43 NIC Public IP: 14				.88.43 NIC Private IP	vate IP: 172.17.40.5		
8	Disks		L	-				
<u>,</u>	Size		Inbound port rules	Outbound port rules	Application security groups	Load balancing		
۲	Security Network security group citrix-adc-vpx-nic01-nsg-0 (attached to network interface: citrix-adc-vpx-nic01-0) Impacts 0 subnets. 1 network interfaces Add inbound port rule					Add inbound port rule		
	Extensions		Priority	Name	Port	Protocol	Source	Destination
6	Continuous delivery		1022	▲ ssh-22-rule	22	TCP	Internet	Any
		-	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork -

NetScaler FreeBSD Shell を使用してインターフェイス上で高速ネットワークを検証するには

NetScaler の FreeBSD シェルにログインし、次のコマンドを実行してアクセラレーションネットワークのステータ スを確認できます。

ConnectX3 NIC の例:

次の例は、Mellanox ConnectX3 NIC の「ifconfig」コマンド出力を示しています。「50/n」は、Mellanox ConnectX3 NIC の VF インターフェイスを示します。 0/1 と 1/1 は、NetScaler VPX インスタンスの PV インターフェイスを示 します。PV インターフェイス (1/1) と CX3 VF インターフェイス (50/1) の両方が同じ MAC アドレス (00:22:48:1 c: 99:3 e)を持つことがわかります。これは、2 つのインターフェイスが一緒にバンドルされていることを示しま す。

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, multicast="" simplex,=""> metric 0 mtu 1500</broadcast,>
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>)

status: active

ConnectX4 NIC の例:

次の例は、Mellanox ConnectX4 NIC の「ifconfig」コマンド出力を示しています。「100/n」は、Mellanox ConnectX4 NIC の VF インターフェイスを示します。0/1、1/1、および 1/2 は、NetScaler VPX インスタンスの PV インターフェイスを示します。PV インターフェイス(1/1)と CX4 VF インターフェイス(100/1)の両方が同じ MAC アドレス(00:0 d: 3a: 9b: f 2:1 d)を持つことがわかります。PV インターフェイス (1/1) と CX4 VF インターフェイス (100/1) の両方に同じ MAC アドレス (00:0d:3a:9b:f2:1d) があることがわかります。これは、2 つのイ ンターフェイスが一緒にバンドルされていることを示します。同様に、PV インターフェイス(1/2)と CX4 VF イン
ターフェイス(100/2)は同じ MAC アドレス(00:0 d: 3a: 1:D 2:23)を持ちます。

```
root@SmartNIC-CX4-NS-DUT-NEW1# ifconfig
 100: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
ether 00:0d:3a:9b:f2:1d
        inet 10.0.1.29 netmask 0xffffff00 broadcast 10.0.1.255
inet6 fe80::20d:3aff;fe9b;f21d%0/1 prefixlen 64 autocout scopeid 0x2
        nd6 options=3<PERFORMNUD, ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/2: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM, VLAN_MTU, VLAN_HWTAGGING, LINKSTATE>
       ether 00:0d:3a:1e:d2:23
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
100/1: flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX.MULTICAST> metric 0 mtu 1500
       ether 00:0d:3a:9b:f2:1d
        media: Ethernet autoselect <full-duplex.rxpause.txpause> (autoselect
<full-duplex.rxpause>)
        status: active
100/2:
        flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX.MULTICAST> metric 0 mtu 1500
        ether 00:0d:3a:1e:d2:23
        media: Ethernet autoselect <full-duplex.rxpause.txpause> (autoselect
<full-duplex.rxpause>)
        status: active
```

ADC CLI を使用してインターフェイスで高速ネットワーキングを検証するには

ConnectX3 NIC の例:

次の show interface コマンドの出力は、PV インターフェイス 1/1 が SR-IOV VF NIC である仮想機能 50/1 にバンドルされていることを示しています。1/1 と 50/1 の NIC の両方の MAC アドレスは同じです。高速ネットワーキングが有効になると、1/1 インターフェイスのデータは、ConnectX3 インターフェイスである 50/1 インターフェイスのデータパスを介して送信されます。PV インターフェイス (1/1) の「show interface」出力が VF (50/1) を指していることがわかります。同様に、VF インターフェイス (50/1) の「show interface」出力は PV インターフェイス (1/1) を指します。

> show interface 1/1

Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1 tlags=0xe060 <enabled, 802.1q="" heartbeat,="" up,=""> MTU=1500, native ylan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s LLDP Mode: NONE, LR Priority: 1024</enabled,>) #1
RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0) NIC: InDisc(0) OutDisc(0) Ectls(0) Stalls(0) Hangs(0) Muted(0) Bandwidth thresholds are not set.	I
Done	
> show interface 50/1	
Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2 Tlaus=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, Tctl 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.	

ConnectX4 NIC の例:

次の show interface コマンドの出力は、PV インターフェイス 1/1 が SR-IOV VF NIC である仮想機能 100/1 にバ ンドルされていることを示しています。1/1 と 100/1 の NIC の両方の MAC アドレスは同じです。高速ネットワーキ ングが有効になると、1/1 インターフェイスのデータは、ConnectX4 インターフェイスである 100/1 インターフェ イスのデータパスを介して送信されます。PV インターフェイス (1/1) の「show interface」出力が VF (100/1) を 指すことがわかります。同様に、VF インターフェイス (100/1) の「show interface」出力は PV インターフェイス (1/1) を指します。 interform 1/1

> Show	Incertace 1/1
1)	Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 100/1, Datapath 100/1) #0 flags=0xe060 <enabled, 802.1q="" heartbeat,="" up,=""> MTU=1500, native vlan=10. MAC=00:0d:3a:9b:f2:1d, uptime 10h49m10s LLDP Mode: NONE, LR Priority: 1024</enabled,>
	RX: Pkts(310366) Bytes(98476082) Errs(0) Drops(0) Stalls(0) TX: Pkts(44) Bytes(6368) Errs(0) Drops(0) Stalls(0) NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0) Bandwidth thresholds are not set.
Done > show	interface 100/1
1)	<pre>Interface 100/1 (CX4 VF Interface, SmartNIC, PV 1/1) #3 flags=0xe460 <enabled, 802.1g="" up.=""> MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d uptime 10h49m11s Actual: media FIBER, speed NONE, duplex FULL, fctl NONE, throughput</enabled,></pre>
5	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	

NetScaler での注意点

- PV インターフェイスは、必要なすべての操作のプライマリインターフェイスまたはメインインターフェイス
 と見なされます。設定は PV インターフェイスでのみ実行する必要があります。
- VF インターフェイスでのすべての「set」操作は、以下を除いてブロックされます。
 - インターフェイスを有効にする
 - インターフェイスを無効にする
 - インターフェイスをリセット
 - 統計をクリアする

注		

VF インターフェイスでは操作を実行しないことをお勧めします。

- show interfaceコマンドを使用して、PV インターフェイスと VF インターフェイスとのバインディン グを確認できます。
- NetScaler リリース 13.1~33.x 以降、NetScaler VPX インスタンスは、Azure アクセラレーテッドネット ワークでの動的な NIC の取り外しと、取り外された NIC の再接続をシームレスに処理できます。Azure は、ホ ストのメンテナンス作業のために、高速ネットワークの SR-IOV VF NIC を削除できます。NIC が Azure VM から削除されると、NetScaler VPX インスタンスのインターフェイスステータスが「リンクダウン」と表示さ

れ、トラフィックは仮想インターフェイスのみを経由します。取り外した NIC が再接続されると、VPX インス タンスは再接続された SR-IOV VF NIC を使用します。このプロセスはシームレスに行われ、設定は不要です。

PV インターフェースへの VLAN の構成

PV インターフェイスが VLAN にバインドされている場合、関連するアクセラレーション VF インターフェイスも PV インターフェイスと同じ VLAN にバインドされます。この例では、PV インターフェイス(1/1)は VLAN(20)にバ インドされています。PV インターフェイス(1/1)にバンドルされている VF インターフェイス(100/1)も VLAN 20 にバインドされます。

例

1. VLAN を作成します。

1 add vlan 20

2. VLAN を PV インターフェイスにバインドします。

```
bind vlan 20 - ifnum 1/1
1
2
3
     show vlan
4
     1) VLAN ID: 1
5
         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
10
11
         IPs : 10.0.1.29 Mask: 255.255.255.0
12
     3) VLAN ID: 20
                       VLAN Alias Name:
13
         Interfaces : 1/1 100/2
14
```

注

VLAN バインディング操作は、アクセラレーション VF インターフェイスでは許可されません。

bind vlan 1 -ifnum 100/1
 ERROR: Operation not permitted

Azure ILB で NetScaler 高可用性テンプレートを使用して HA-INC ノードを構成する

October 17, 2024

イントラネットアプリケーション用の標準テンプレートを使用すると、HA-INC モードで一対の VPX インスタンスを 迅速かつ効率的にデプロイできます。Azure 内部ロードバランサー (ILB) は、図1に示すように、フロントエンドに 内部 IP アドレスまたはプライベート IP アドレスを使用します。このテンプレートでは、3 つのサブネットと 6 つの NIC を持つ 2 つのノードが作成されます。サブネットは、管理、クライアント、およびサーバー側のトラフィック用 で、各サブネットはデバイスごとに異なる NIC に属します。

図 1: 内部ネットワーク内のクライアント用の NetScaler ADC HA ペア



この展開は、図 2 に示すように、NetScaler HA ペアがファイアウォールの内側にある場合にも使用できます。パブ リック IP アドレスはファイアウォールに属し、ILB のフロントエンド IP アドレスに NAT されます。

図 2: パブリック IP アドレスを持つファイアウォールと NetScaler ADC HA のペア



イントラネットアプリケーション用の NetScaler ADC HA ペアテンプレートは、Azure ポータルで入手できます。 次の手順を実行してテンプレートを起動し、Azure 可用性セットを使用して高可用性 VPX ペアをデプロイします。

- 1. Azure Portal から、[カスタム展開]ページに移動します。
- 2. [基本] ページが表示されます。リソースグループを作成します。[パラメータ] タブで、[リージョン]、[管理者 ユーザー名]、[管理者パスワード]、[ライセンスタイプ] (VM sku)、およびその他のフィールドの詳細を入力 します。

Custom deployment Deploy from a custom template 12 resources	<i>v v</i>
	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 * ①	NSDev Platform CA anaop.agarwei@citric.com
Resource group * ①	(New) HA-ILB
	Create new
Parameters	
Region * 🛈	West US 2
Admin Username ①	hariharan)
Admin Password * ①	···········
Vm Size 🕕	Standard_DS3_v2 V
Vm Sku 🛈	netscalerbyol V
Vnet Name ①	vnet01
Vnet Resource Group ①	
Vnet New Or Existing	new
Subnet Name-01 (i)	subnet_mgmt
Subnet Name-11 🛈	subnet_client
Subnet Name-12 ①	subnet_server
Subnet Address Prefix-01 ①	10.11.0.0/24
Subnet Address Prefix-11 ①	10.11.1.0/24
Review + create < Previous	Next : Review + create >

3. 次へ:確認+作成>をクリックします。

必要な構成で Azure リソースグループが作成されるまで時間がかかることがあります。完了後、Azure ポー タルでリソースグループを選択して、LB ルール、バックエンドプール、ヘルスプローブなどの構成の詳細を 確認します。高可用性ペアは ADC-VPX-0 と ADC-VPX-1 として表示されます。

追加のセキュリティルールやポートを作成するなど、HA セットアップでさらに変更が必要な場合は、Azure Portal から実行できます。

必要な構成が元」9 ると、人のワノースがIF成され	A 9 0	
(i) HA-ILB Resource group		
» + Add ≡≡ Edit columns 💼 Delete resource grou	ıp 💍 Refresh 🞍 Export to CSV 😚 Open	query Assign ta
∧ Essentials		
Subscription (change):		
Subscription ID : 764bc6a9-7027-4011-6e67-ee0	73098cm3	
Tags (change) : Click here to add tags		
Filter by name Type == (all) X	ocation == (all) \times + Add filter	
Showing 1 to 20 of 20 records. Show hidden types	0	
Name ↑↓	Type \uparrow_\downarrow	Location $\uparrow \downarrow$
ADC-Availability-Set	Availability set	West US 2
📄 💠 ADC-Azure-Load-Balancer	Load balancer	West US 2
ADC-VPX-0	Virtual machine	West US 2
ADC-VPX-0-management-public-ip	Public IP address	West US 2
ADC-VPX-1	Virtual machine	West US 2
ADC-VPX-1-management-public-ip	Public IP address	West US 2
ADC-VPX-NIC-0-01	Network interface	West US 2
ADC-VPX-NIC-0-11	Network interface	West US 2
ADC-VPX-NIC-0-12	Network interface	West US 2
ADC-VPX-NIC-1-01	Network interface	West US 2
ADC-VPX-NIC-1-11	Network interface	West US 2
ADC-VPX-NIC-1-12	Network interface	West US 2
ADC-VPX-NSG-0-01	Network security group	West US 2
ADC-VPX-NSG-0-11	Network security group	West US 2
ADC-VPX-NSG-0-12	Network security group	West US 2
ADC-VPX-NSG-1-01	Network security group	West US 2

必要な構成が完了すると、次のリソースが作成されます。

- 4. ADC-VPX-0 および ADC-VPX-1 ノードにログオンして、次の設定を検証します。
 - 両方のノードの NSIP アドレスは管理サブネットに存在する必要があります。
 - プライマリ(ADC-VPX-0)ノードとセカンダリ(ADC-VPX-1)ノードには、2つのSNIPアドレスが表示される必要があります。一方のSNIP(クライアントサブネット)はILBプローブへの応答に使用され、もう1つのSNIP(サーバーサブネット)はバックエンドサーバー通信に使用されます。

注

HA-INC モードでは、ADC-VPX-0VM と ADC-VPX-1VM の SNIP アドレスは、両方が同じである従来の オンプレミス ADC HA 展開とは異なり、同じサブネット内では異なります。VPX ペア SNIP が異なるサ ブネットにある場合、または VIP が SNIP と同じサブネット内にない場合に展開をサポートするには、 Mac ベース転送 (MBF) を有効にするか、各 VIP の静的ホストルートを各 VPX ノードに追加する必要 があります。VPX ペアの SNIP が異なるサブネットにある場合、または VIP が SNIP と同じサブネット にない場合に展開をサポートするには、Mac ベース転送 (MBF) を有効にするか、各 VIP の静的ホスト ルートを各 VPX ノードに追加する必要があります。

プライマリノード (ADC-VPX-0)

> sh ip								
	Ipaddress	Traffic Domain	Type	Mode	Arp	Icmp	Vserver	State
			TD					
1) 2)	10.11.1.5		SNTP	Active	Enabled	Enabled	NA. NA	Enabled
3)	10.11.3.4		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								
> _								
>								
> sn n	a node							
T)	Node ID:	0						
	IP: I	.0.11.0.5 (ADC	-VPX-0)					
	Node State:	UP De émocra						
	Master Stat	e: Primary						
	Fail-Safe M	lode: OFF						
	INC State:	ENABLED						
	Sync State:	ENABLED						
	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 no	ot seen :	1/1 1/	2		
	Interfaces	causing Parti	al Failure:	None				
	SSL Card St	atus: NOT PRE	SENT					
	Sync Status	Strict Mode:	DISABLED					
	Hello Interval: 200 msecs							
	Dead Interval: 3 secs							
	Node in thi	s Master Stat	e for: 0:0:20	0:26 (day	/s:hrs:m	in:sec)		
2)	Node ID:	L						
	IF: I	.0.11.0.4						
	Node State:							
	Master Stat	e: Secondary						
	TNC State M	Dode: Off						
	INC State:	ENABLED						
	Sync State:	SUCCESS						
	Propagation Eachlad Lat	ENABLED	1/1 1/0					
	Enabled Int	eriaces : 0/1	1/1 1/2					
	Disabled in	terraces : No	ne					
	HA MON ON I	nterraces : N	one					
	HA HEARIBEA	i off interfa	ces : None		/ /			
	Interfaces	on which hear	theats are no	ot seen :	1/1 1/	2		
	Interfaces	causing Parti	ai railure: 1	None				
Dee	SSL Card St	acus: NOI PRE	JEN1					
> Jone								

セカンダリノード(ADC-VPX-1)

> sh ip								
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
1)	10.11.0.4	0	NetScaler IP	Active	 Enabled	Enabled	NA	Enabled
2)	10.11.1.6		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.11.3.5	0	SNIP	Active	Enabled	Enabled	NA	Enabled
> Done								
>								
> sh	ha node							
1)	Node TD:	0						
-,	TP:	10.11.0.4	(ADC-VPX-1)					
	Node Sta	te: UP	(1100 (111 1)					
	Master S	tate: Second	arv					
	Fail-Saf	e Mode: OFF						
	INC Stat	e: ENABLED						
	Sync Sta	te: SUCCESS						
	Propagat	ion: ENABLED						
	Enabled	Interfaces :	0/1 1/1 1/2					
	Disabled	Interfaces	: None					
	HA MON O	N Interfaces	: None					
	HA HEART	BEAT OFF Int	erfaces : No	ne				
	Interfac	es on which	heartbeats a	re not	seen :	1/1 1/	2	
	Interfac	es causing P	artial Failu	re: Nor	ne			
	SSL Card	Status: NOT	PRESENT					
	Sync Sta	tus Strict M	ode: DISABLE	D				
	Hello In	terval: 200	msecs					
	Dead Int	erval: 3 sec	s					
	Node in	this Master	State for: 0	:0:24:1	18 (day	s:hrs:m	ain:sec)
2)	Node ID:	1						
	IP:	10.11.0.5						
	Node Sta	te: UP						
	Master S	tate: Primar	У					
	Fail-Saf	e Mode: OFF						
	INC Stat	e: ENABLED						
	Sync Sta	te: ENABLED						
	Propagat	ion: ENABLED						
	Enabled	Interfaces :	0/1 1/1 1/2					
	Disabled	Interfaces	: None					
	HA MON O	N Interfaces	: None					
	HA HEART	BEAT OFF Int	erfaces : No	ne				
	Interfac	es on which	heartbeats a	re not	seen :	1/1 1/	2	
	Interfac	es causing P	artial Failu	re: Nor	ie			
D	SSL Card	Status: NOT	PRESENT					
Done								
>								

- 5. プライマリノードとセカンダリノードが UP で、同期ステータスが **SUCCESS** になったら、プライマリノー ド (ADC-VPX-0) の負荷分散仮想サーバーまたはゲートウェイ仮想サーバーを、ADC Azure ロードバランサ ーのプライベートフローティング IP (FIP) アドレスで構成する必要があります。詳細については、「サンプル 設定」セクションを参照してください。
- 6. ADC Azure 負荷分散サーバーのプライベート IP アドレスを見つけるには、Azure portal > ADC Azure Load Balancer > Frontend IP configuration に移動します。

≡ Microsoft Azure 🔑 Sea	rch resources, services, and docs (G+/)	∑ 17 ¢ ©
Home > Test_HA_Deployment > ADC ADC-Azure-Load-R Load balancer	C-Azure-Load-Balancer Balancer Frontend IP configuration	
Search (Ctrl+/) « Overview	+ Add D Refresh	
 Activity log Access control (IAM) 	Name IP address	Rules count
 Tags Diagnose and solve problems 	Abe coor balance from the computation fore to the	

7. Azure Load Balancer の 構成ページで、ARM テンプレートの展開は、LB ルール、バックエンドプール、 およびヘルスプローブの作成に役立ちます。

Home > HA-IL8 > ADC-Azure-Load-Balancer								
S and C-Azure-Load-Balancer Load balancing rules								
	+ Add							
Activity log								
Access control (IAM)	Name	↑↓	Load balancing rule		Backend pool	¢↓	Health probe	î↓
🔶 Tags	IbRule1		lbRule1 (TCP/80)		ADC-Load-Balancer-Backend-rule		ADC-Load-Balancer-Health-Probe-r	ule •
Diagnose and solve problems								
Settings								
Frontend IP configuration								
Backend pools								
1 Health probes								
E Load balancing rules								

• LB ルール (lbrule1) はデフォルトでポート 80 を使用します。

IbRule1 ADC-Azure-Load-Balancer
🔚 Save 🗙 Discard 💼 Delete
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.
Name *
IbRule1
IP Version * IPv4 IPv6
Frontend IP address * ①
10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule)
Protocol
• TCP UDP
Port *
80
Backend port * ①
80
Name * IbRule1 IP Version * IPv6 Frontend IP address * 10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule) Protocol TCP UDP Port * 80 Backend port * 80

• ポート 443 を使用するようにルールを編集し、変更を保存します。

注

セキュリティを強化するため、LB 仮想サーバーまたはゲートウェイ仮想サーバーには SSL ポート 443 を使用することをお勧めします。

IbRule1 ADC-Azure-Load-Balancer	
🔚 Save 🗙 Discard 💼 Delete	
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health prol considers healthy receive new traffic.	be
Name *	
IbRule1	
IP Version * IPv4 IPv6 Frontend IP address * ①	
10.11.1.4 (ADC-Load-Balancer-Frontend-IP-Configuration-rule)	\sim
Port *	
Backend port * ①	
443	
Backend pool ①	
ADC-Load-Balancer-Backend-rule (2 virtual machines)	\sim
Health probe 🕕	
ADC-Load-Balancer-Health-Probe-rule (TCP:9000)	\sim
Session persistence ①	
None	\sim
O	4
Lindoled	

ADC に VIP アドレスを追加するには、次の手順に従います。

1. Azure Load Balancer > Frontend IP 構成に移動し、[追加]をクリックして新しい内部ロードバランサ - IP アドレスを作成します。

Home > HA-ILB > ADC-Azure-Load-Balancer							
ADC-Azure-Load-Balancer Frontend IP configuration							
		🕂 Add 💍 Refresh					
Activity log	•	₽ Filter by name					
Access control (IAM)		Name	IP address				
🔶 Tags		ADC-Load-Balancer-Frontend-IP-Configuration-rule	10.11.1.4				
Diagnose and solve probler	ns						
Settings	0						
Frontend IP configuration							

2. **[Add frontend IP address**] ページで、名前を入力し、クライアントサブネットを選択し、動的 IP アドレ スまたは静的 IP アドレスを割り当てて、**[Add]** をクリックします。

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

3. フロントエンド IP アドレスは作成されますが、LB ルールは関連付けられていません。新しい負荷分散ルール を作成し、フロントエンド IP アドレスに関連付けます。

Ho	me > HA-ILB > ADC-Azure-Lo	oad-Balar	ncer					
••	ADC-Azure-Loa	d-Bal	ancer Frontend	IP con	figuration		×	<
2	Search (Ctrl+/)		+ Add 💍 Refresh					
	Overview		Q Filter by name					
	Activity log			ID address		Dulas sourt		
80	Access control (IAM)		Name	IP address		Rules count		
			ADC-Load-Balancer-Fronte	10.11.1.4		1		••
-	Tags		ILB-Front-End-IP-2	10.11.1.7		0		
Þ	Diagnose and solve problems					<u> </u>		

4. [Azure ロードバランサー] ページで、[負荷分散ルール] を選択し、[追加] をクリックします。

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

5. 新しいフロントエンド IP アドレスとポートを選択して、新しい LB ルールを作成します。[フローティング IP] フィールドは [有効] に設定する必要があります。

Home > HA-ILB > ADC-Azure-Load-Balancer > Add load balancing rule ADC-Azure-Load-Balancer
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.
Name *
IP Version *
Frontend IP address * (i) 10.11.1.7 (ILB-Front-End-IP-2)
Protocol TCP UDP
Port * 3 443 ~ .
Backend port 1 0 4 443 V
Backend pool ① ADC-Load-Balancer-Backend-rule (2 virtual machines)
Health probe ①
ADC-Load-Balancer-Health-Probe-rule (TCP:9000)
Session persistence () None V
Idle timeout (minutes) ①
Floating IP 0 Disabled Enabled
ОК

6. これで、フロントエンド IP 設定に、適用されている LB ルールが表示されます。

Home > HA-ILB > ADC-Azure-Load-Balancer ADC-Azure-Load-Balancer Frontend IP configuration Load balancer					
		+ Add 💍 Refresh			
💠 Overview	^	O tilter by name			
Activity log		Name	IP address	Rules	count
Access control (IAM)		ADC-Load-Balancer-Frontend-IP-Configuration	10.11.1.4	1	
🔶 Tags		II B Front End ID 2	10 11 1 7	1	
Diagnose and solve problems					
Settings					
Frontend IP configuration					

設定例

ゲートウェイ VPN 仮想サーバーと負荷分散仮想サーバーを設定するには、プライマリノード (ADC-VPX-0) で次のコ マンドを実行します。設定はセカンダリノード(ADC-VPX-1)に自動的に同期されます。

ゲートウェイのサンプル構成

```
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
```

負荷分散のサンプル構成

```
    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
```

ILB の内部 IP アドレスに関連付けられている完全修飾ドメイン名 (FQDN) を使用して、負荷分散または VPN 仮想サ ーバーにアクセスできるようになりました。

負荷分散仮想サーバーの構成方法の詳細については、「リソース」セクションを参照してください。

リソース:

次のリンクには、HA の導入と仮想サーバの設定に関する追加情報が表示されます。

- 異なるサブネットでの高可用性ノードの構成
- 基本的な負荷分散を設定する

関連リソース:

- PowerShell コマンドを使用して複数の IP アドレスと NIC を使用して高可用性セットアップを構成する
- Azure でのアクティブスタンバイ HA デプロイメントでの GSLB の構成

インターネット向けアプリケーション用の NetScaler 高可用性テンプレートを使用し て HA-INC ノードを構成する

October 17, 2024

インターネット向けアプリケーションの標準テンプレートを使用すると、一対の VPX インスタンスを HA-INC モードで迅速かつ効率的にデプロイできます。Azure ロードバランサー (ALB) は、フロントエンドにパブリック IP アドレスを使用します。このテンプレートでは、3 つのサブネットと 6 つの NIC を持つ 2 つのノードが作成されます。サブネットは、管理、クライアント、およびサーバー側のトラフィック用です。各サブネットには、両方の VPX インスタンス用に 2 つの NIC があります。

インターネット向けアプリケーションの Citrix ADC HA ペアテンプレートは、Azure Marketplace で入手できま す。

次の手順を実行してテンプレートを起動し、Azure 可用性セットまたは可用性ゾーンを使用して高可用性 VPX ペア をデプロイします。

- 1. Azure Marketplace から NetScaler を検索してください。
- 2. [今すぐ入手]をクリックします。



3. 必要な HA 導入とライセンスを選択し、[続行] をクリックします。



4. [基本] ページが表示されます。リソースグループを作成します。[パラメータ] タブで、地域、管理者ユーザー 名、管理者パスワード、ライセンスタイプ (VM SKU)、およびその他のフィールドの詳細を入力します。

Basics VM Configurations I	Network and Additional Settings Review + create	
Project details		
Select the subscription to manage dep manage all your resources.	oloyed resources and costs. Use resource groups like folders to organize and	
Subscription * 🛈	xm-test-cs-shared	/
Resource group * ()	(New) Test_HA_Internet Create new	/
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 * ①	 Password SSH Public Key 	
Password * 🔋		•
Confirm password *	······································	🖌 🕑 Passwor
Review + create < Previo	Next : VM Configurations >	

5. [次へ]をクリックします: VM 構成 >。

Basics \	VM Configurations	Network and Additional Settings Review + create	
Project deta	ails		
Select the sul manage all ye	bscription to manage d our resources.	eployed resources and costs. Use resource groups like folders to organize and	
Subscription	* ()	xm-test-cs-shared	\sim
Reso	urce group * 🕞	(New) Test_HA_Internet Create new	\checkmark
Instance de	tails		
Region * 🕡		South India	\sim
Citrix ADC Re	elease Version * 🛈	12.113.0	
License Subsc	ription 🛈	Bring Your Own License	
Virtual Machin	ne name * 🛈	citrix-adc-vpx	
Administrate	or account		
Username *	(i)	praveenk	\checkmark
Authenticatio	n type * 🔅	 Password SSH Public Key 	
Password * (D		~
Confirm pass	word *	••••••	V Passwor
Review +	create < Prev	vious Next : VM Configurations >	

- 6. [**VM** 構成]ページで、次の手順を実行します。
 - パブリック IP ドメイン名サフィックスの設定
 - Azure 監視メトリクスを有効または無効にする
 - バックエンド Autoscale を有効または無効にする
- 7. [次へ:ネットワークとその他の設定]をクリックします。

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

8. [ネットワークとその他の設定]ページで、ブート診断アカウントを作成し、ネットワーク設定を行います。

Basics VM Configurations	Network and Additional Settings Review + create	
Boot diagnostics		
Diagnostic storage account * 🛈	(new) citrixadcvpxd7a2c4d49e	\sim
	Create New	
Network Settings		
Configure virtual networks		
Virtual network * 🕡	(new) citrix-adc-vpx-virtual-network	\sim
	Create new	
Management Subnet * 🛈	(new) 01-management-subnet (10.17.4.0/24)	\sim
Client Subnet * 🕡	(new) 11-client-subnet (10.17.5.0/24)	\sim
Server Subnet * 🛈	(new) 12-server-subnet (10.17.6.0/24)	~
Public IP (Management)		
Management Public IP (NSIP) * 🛈	(new) citrix-adc-vpx-nsip	~
	Create new	
Management Domain Name 🛈	citrix-adc-vpx-nsip-d7a2c4d49e	~
	.southindia.	cloudapp.azure.cor
Public IP (Clientside)		
	Create new	~
Clientside Domain Name 🛈	citrix-adc-vpx-vip-d7a2c4d49e	~
	.southindia.	cloudapp.azure.con
Public Inbound Ports (Manageme	ent only)	
Ports open for Management public II	p 🕠 🔿 None	
	ssh (22)	
	Ssh (22), http (80), https (443)	
Review + create < Prev	ious Next : Review + create >	

- 9. [次へ]をクリックします: レビュー+作成する>。
- 10. 基本設定、VM 構成、ネットワーク、その他の設定を確認して、[作成]をクリックします。

必要な構成で Azure リソースグループが作成されるまで時間がかかることがあります。完了したら、Azure ポータルでリソースグループを選択すると、LB ルール、バックエンドプール、ヘルスプローブなどの構成の 詳細が表示されます。高可用性ペアは、**citrix-adc-vpx-0** と **citrix-adc-vpx-1** として表示されます。 追加のセキュリティルールやポートを作成するなど、HA セットアップでさらに変更が必要な場合は、Azure Portal から実行できます。

必要な構成が完了すると、次のリソースが作成されます。

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

[e] Test_HA_Internet_App ☆ Resource group

- + Add 📰 Edit columns 📋 Delete resource group 🕐 Refresh 🞍 Export to CSV 😽 Open query 🛛 🖄 Assign tags ightarrow Move ightarrow 🗍 De ✓ Essentials Type == all \times Location == all \times $+_{\nabla}$ Add filter Filter by name... Showing 1 to 23 of 23 records. Show hidden types ① Name ↑↓ Tvpe ↑. citrix-adc-vpx-0 Virtual machine citrix-adc-vpx-0_OsDisk_1_6749f4a73c534051b0602ba6e3ec2cf8 Disk citrix-adc-vpx-1 Virtual machine Citrix-adc-vpx-1_OsDisk_1_8fde7770497b4dbdba385715e81505c9 Disk Citrix-adc-vpx-nic01-0 Network interface citrix-adc-vpx-nic01-1 Network interface citrix-adc-vpx-nic01-nsg-0 Network security group citrix-adc-vpx-nic01-nsg-1 Network security group 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 citrix-adc-vpx-nic12-0 Network interface Citrix-adc-vpx-nic12-1 Network interface citrix-adc-vpx-nic12-nsq-0 Network security group citrix-adc-vpx-nic12-nsg-1 Network security group citrix-adc-vpx-nsip-0 Public IP address citrix-adc-vpx-nsip-1 Public IP address citrix-adc-vpx-vip Public IP address citrix-adc-vpx-vip-load-balancer Load balancer ☐ ↔ citrix-adc-vpx-virtual-network Virtual network citrix-adc-vpx-vm-availability-set Availability set citrixadcvpx9db3901a6a Storage account
- 11. 次の構成を検証するには、citrix-adc-vpx-0 ノードと citrix-adc-vpx-1 ノードにログオンする必要がありま す **。
 - 両方のノードの NSIP アドレスは管理サブネットに存在する必要があります。
 - ・ プライマリ (citrix-adc-vpx-0) ノードとセカンダリ (citrix-adc-vpx-1) ノードには、2 つの SNIP アド レスが必要です。1 つの SNIP (クライアントサブネット) は ALB プローブへの応答に使用され、もう1 つの SNIP (サーバーサブネット) はバックエンドサーバー通信に使用されます。

注

HA-INC モードでは、citrix-adc-vpx-0 と citrix-adc-vpx-1 VM の SNIP アドレスは異なります。これ は、両方が同じである従来のオンプレミス ADC 高可用性導入環境とは異なります。

プライマリノード (citrix-adc-vpx-0) で

> sh ip									
	Ipaddress	Traffic Domain	Type		Mode	Arp	Icmp	Vserver	State
1.5	10 18 0 4		Not Sepler	TD	Activo	 Enabled			Enabled
1) 2)	10.18.1.5		SNTP	TF	Active	Enabled	Enabled	NA NA	Enabled
3)	10.18.2.4		SNIP		Active	Enabled	Enabled	NA	Enabled
Done									
. .									
> sn n	a node								
T)	Node ID:	0							
	IP:	10.18.0.4 (ns-	vpx0)						
	Node State	e: UP - De internet							
	Master Sta	ate: Primary							
	Fall-Safe	Mode: OFF							
	INC State:	: ENABLED							
	Sync State	e: ENABLED							
	Propagatio	on: ENABLED	- / /-						
	Enabled In	nterfaces : 0/1	1/1 1/2						
	Disabled 1	Interfaces : No	ne						
	HA MON ON	Interfaces : N	one						
	HA HEARTBI	EAT OFF Interia	ces : Non	ie .		- / /	_		
	Interfaces	s on which hear	tbeats ar	e not	; seen :	1/1 1/	2		
	Interfaces	s causing Parti	al Failur	e: No	one				
	SSL Card S	Status: NOT PRE	SENT						
	Sync Stati	us Strict Mode:	DISABLEL)					
	Hello Inte	erval: 200 msec	S						
	Dead Inter	rval: 3 secs		0.04	01 (1				
~	Node in th	nis Master Stat	e for: U:	3:34:	21 (day	s:nrs:m	in:sec)		
2)	Node ID:	10 10 0 5							
	IP:	10.18.0.5							
	Node State	e: UP							
	Master Sta	Ate: Secondary							
	Tall-Sale	Mode: OFF							
	INC States	: ENABLED							
	Sync State	e: SUCCESS							
	Propagatio	ON: ENABLED	1/1 1/0						
	Enabled In	nterraces : 0/1	1/1 1/2						
	Disabled I	Interfaces : No	ne						
	HA MON ON	Interfaces : N	one						
	HA HEARTBI	LAI OFF Interia	ces : Non	18		2 / 2 2 /	•		
	Interfaces	s on which hear	tpeats ar	e not	; seen :	1/1 1/	2		
	Interfaces	s causing Parti	al Failur	e: No	one				
-	SSL Card S	Status: NOT PRE	SENT						
Done									

セカンダリノード (citrix-adc-vpx-1) 上

> show	ip							
	Ipaddress	Traffic Domain	Туре	Mode	Arp	Icmp	Vserver	State
1)	10.18.0.5		NetScaler IP	Active	Enabled	Enabled	NA	Enabled
2)	10.18.1.4		SNIP	Active	Enabled	Enabled	NA	Enabled
3)	10.18.2.5		SNIP	Active	Enabled	Enabled	NA	Enabled
Done								



- プライマリノードとセカンダリノードが UP になり、同期ステータスが SUCCESS になったら、ALB 仮想の パブリック IP アドレスを使用して、プライマリノード(citrix-adc-vpx-0)の負荷分散仮想サーバーまたは ゲートウェイ仮想サーバーを構成する必要があります。詳細については、「サンプル設定」セクションを参照 してください。
- 13. ALB 仮想サーバーのパブリック IP アドレスを見つけるには、Azure portal > Azure Load Balancer > Frontend IP configuration に移動します。

Home > Test_HA_Template > alb Frontend IP co	onfiguration			×
P Search (Ctrl+/) ≪	earch (Ctrl+/) « + Add 🕐 Refresh			
Overview	A P 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				
Diagnose and solve problems Settings				
Diagnose and solve problems Settings Frontend IP configuration				

14. 仮想サーバーポート 443 のインバウンドセキュリティルールを、両方のクライアントインターフェイスのネ ットワークセキュリティグループに追加します。

Home > Test_HA_Template > ns-vp>	x-nic0-11 >							
ns-vpx-nic-nsg0-1 Network security group	1 ☆							×
	 → Move ∨ Î D 	elete 🕐 Refresh						
💎 Overview	^							
Activity log	Resource group (chan	ge) : Test_HA_Template			Custom security ru	les:2 inbound, 0 outb	ound	
Access control (IAM)	Location	: South India			Associated with	: 0 subnets, 1 netw	ork interfaces	
Tans	Subscription (change)	: xm-test-cs-shared						
9 Diagnass and solve problems	Subscription ID	: db99d808-6e89-480a	a-96ae-3275fe	e61eed4				
 Diagnose and solve problems 	Tags (change)	: Click here to add tag	5					
ettings	Inbound security rule	25						
Inbound security rules	Priority	Name		Port	Protocol	Source	Destination	Action
Outbound security rules	1000	A default-allow-ssh		22	тср	Any	Any	Allow
Network interfaces	1010	Port_443		443	TCP	Any	Any	Allow
Subnets	65000	AllowVnetInBound		Any	Any	VirtualNetwork	VirtualNetwork	Allow
Properties	65001	AllowAzurel oadBalanc	erinBound	Δην	Δηγ	Azurel oadBalance	r Anv	Allow
Locks	+							
P ns-vpx-nic-nsg1-11								
Activity log	Resource group (change)	Resource group (change) : Test HA Template Custom security rules : 2 inbound. 0 outbound						
Activity log	Location	: South India			Associated with	: 0 subnets, 1 networ	k interfaces	
Access control (IAIVI)	Subscription (change)	: xm-test-cs-shared 🗅						
ags	Subscription ID	: db99d808-6e89-480a-96	ae-3275fe61e	ed4				
Diagnose and solve problems	Tags (change)	: Click here to add tags						
ettings	Inbound security rules							
inbound security rules	Priority	Name	Port	Protocol	Source	Destinatio	n Action	
Outbound security rules	1000	A default-allow-ssh	22	TCP	Any	Any	Allow	
Network interfaces	1010	Port_443	443	TCP	Any	Any	Allow	
> Subnets	65000	AllowVnetInBound	Any	Any	VirtualNetw	ork VirtualNet	work 🔮 Allow	
Properties	65001	AllowAzureLoadBalancer	Any	Any	AzureLoadE	alancer Any	S Allow	
Locks	65500	DenvAllinBound	Anv	Any	Anv	Any	Denv	
Export template				Ally	~~ <u>~</u>	City	• Deny	

15. アクセスする ALB ポートを設定し、指定したポートのインバウンドセキュリティルールを作成します。バッ クエンドポートは、負荷分散仮想サーバーポートまたは VPN 仮想サーバーポートです。

	\mathcal{P} Search resources, services, and docs (G+/)
Home > Test_HA_Template > alb >	
IbRule1	
🖫 Save 🗙 Discard 📋 Delete	
● IPv4 O 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)	~
Health probe 🕕	
probe-11 (TCP:9000)	~
Session persistence (i)	
None	~
Idle timeout (minutes) 🕕	
0	4
Floating IP (direct server return)	
Enabled	

16. これで、ALB パブリック IP アドレスに関連付けられた完全修飾ドメイン名 (FQDN) を使用して、負荷分散仮 想サーバーまたは VPN 仮想サーバーにアクセスできます。

	Please log on to	continue.	
	User name Password		
		Log On	

設定例

ゲートウェイ VPN 仮想サーバーと負荷分散仮想サーバーを設定するには、プライマリノード (ADC-VPX-0) で次のコ マンドを実行します。設定はセカンダリノード(ADC-VPX-1)に自動的に同期されます。

ゲートウェイのサンプル構成

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

負荷分散のサンプル構成

```
    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
```

ALB のパブリック IP アドレスに関連付けられた FQDN を使用して、負荷分散または VPN 仮想サーバーにアクセス できるようになりました。

負荷分散仮想サーバーを構成する方法の詳細については、「リソース」セクションを参照してください。

リソース:

次のリンクには、HAの導入と仮想サーバの設定に関する追加情報が表示されます。

- 仮想サーバーを作成する
- 基本的な負荷分散を設定する

Azure 外部および内部ロードバランサーで同時に高可用性セットアップを構成する

October 17, 2024

Azure の高可用性ペアは、外部ロードバランサーと内部ロードバランサーの両方を同時にサポートします。

Azure 外部ロードバランサーと内部ロードバランサーの両方を使用して高可用性ペアを構成するには、次の2つのオ プションがあります。

- NetScaler ADC アプライアンス上で2つのLB 仮想サーバーを使用する。
- 1つのLB仮想サーバーとIPセットを使用する。単一のLB仮想サーバは、IPSetによって定義された複数の IPにトラフィックを処理します。

外部ロードバランサーと内部ロードバランサーを同時に使用して Azure で高可用性ペアを構成するには、次の手順を 実行します。 手順 1 と 2 については、Azure ポータルを使用します。手順 3 および 4 では、NetScaler VPX GUI または CLI を使 用します。

ステップ **1**。外部ロード バランサーまたは内部ロード バランサーのいずれかの Azure ロード バランサーを構成しま す。

Azure 外部ロード バランサーを使用した高可用性設定の構成の詳細については、「複数の IP アドレスと NIC を使用 して高可用性設定を構成する」を参照してください。

Azure 内部ロードバランサーを使用した高可用性セットアップの構成の詳細については、以下を参照してください。 NetScaler 高可用性テンプレートと Azure ILB を使用した HA-INC ノードの構成.

ステップ **2**。リソース グループに追加のロード バランサー (ILB) を作成します。ステップ 1 では、外部ロードバラン サーを作成した場合は、内部ロードバランサーを作成し、逆に作成します。

 内部ロードバランサーを作成するには、ロードバランサのタイプを [内部] として選択します。[サブネット] フィールドで、NetScaler ADC クライアントサブネットを選択する必要があります。競合がない限り、その サブネットに静的 IP アドレスを指定することもできます。それ以外の場合は、ダイナミック IP アドレスを選 択します。

Home > ansible_rg_ganeshb_1611818039 > New > Load Balancer >

Create load balancer

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

外部ロードバランサーを作成するには、ロードバランサの種類を[パブリック]として選択し、ここにパブリック IP アドレスを作成します。

Microsoft Azure	✓ Search resources, services, and docs (G+/) ∑ 47 ②			
ome > Load balancing - help me choose (Preview) >				
Create load balancer				
Туре * 🕕	O Internal 💿 Public			
SKU * i	• 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 * 🕕	● Create new ○ Use existing			
Public IP address name *				
Public IP address SKU Standard				
IP address assignment	O Dynamic () Static			
Availability zone *	ailability zone *			
Add a public IPv6 address	O No Yes			
Routing preference (i)	Microsoft network Internet			
Review + create	< Previous Next : Tags > Download a template for automation			

1. Azure Load Balancer を作成したら、フロントエンド **IP** 設定に移動し、ここに示す IP アドレスを書き留め ます。ステップ 3 のように ADC 負荷分散仮想サーバーを作成するときは、この IP アドレスを使用する必要が あります。

new-alb-ilb Fronte	nd IP configuration				
✓ Search (Cmd+/) «	🕂 Add 💍 Refresh				
🚸 Overview	P Filter by name				
Activity log	Name	IP address	Rules count		
Access control (IAM)	LoadBalancerFrontEnd	52,172,96,71 (ip-alb-ilb)	0		
🗳 Tags	Eodupularicentontena				
Diagnose and solve problems					
Settings					
Frontend IP configuration					
Backend pools					
Health probes					
३ Load balancing rules					
lnbound NAT rules					
1 O II - I - I					

- 2. Azure Load Balancer の設定ページで、ARM テンプレートのデプロイは、LB ルール、バックエンドプー ル、およびヘルスプローブの作成に役立ちます。
- 3. 高可用性ペアのクライアント NIC を ILB のバックエンドプールに追加します。
- 4. ヘルスプローブの作成(TCP、9000 ポート)
- 5. 次の2つの負荷分散ルールを作成します。
 - ポート 80の HTTP トラフィック(Webapp ユースケース)の1つのLB ルール。ルールでは、バック エンドポート 80も使用する必要があります。作成したバックエンドプールとヘルスプローブを選択し ます。フローティング IP を有効にする必要があります。
 - ポート 443の HTTPS または CVAD トラフィックに対する別の LB ルール。プロセスは HTTP トラフィックと同じです。
- ステップ 3。 NetScaler アプライアンスのプライマリ ノードで、ILB 用の負荷分散仮想サーバーを作成します。
 - 1. 負荷分散仮想サーバーを追加します。

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

例

add lb vserver vserver_name HTTP 52.172.96.71 80

注

ステップ2で作成した追加のロードバランサーに関連付けられた、ロードバランサーのフロントエンド IP アドレスを使用します。

2. サービスを負荷分散仮想サーバーにバインドします。

1 bind lb vserver <name> <serviceName>

例

1 bind lb vserver Vserver-LB-1 Service-HTTP-1

詳細については、「基本的な負荷分散の設定」を参照してください。

ステップ 4: ステップ3の代わりに、IPSetを使用して ILB の負荷分散仮想サーバーを作成できます。

1. 仮想サーバー IP (VIP) タイプの IP アドレスを追加します。

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

例

```
1 add nsip 52.172.96.71 -type vip
```

2. プライマリノードとセカンダリノードの両方に IPSet を追加します。

1 add ipset <name>

例

```
1 add ipset ipset1
```

3. IP アドレスを IP セットにバインドします。

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

例

```
1 bind ipset ipset1 52.172.96.71
```

4. 既存の LB 仮想サーバーを IPSet を使用するように設定します。

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

例

```
1 set lb vserver vserver_name -ipset ipset1
```

詳細については、「マルチ IP 仮想サーバーの構成」を参照してください。

Azure VMware ソリューションに NetScaler VPX インスタンスをインストールする

October 17, 2024

Azure VMware ソリューション (AVS) は、専用のベアメタル Azure インフラストラクチャから構築された vSphere クラスタを含むプライベートクラウドを提供します。最初のデプロイメントは最小で 3 台のホストですが、追加ホス トは一度に 1 つずつ追加でき、クラスタごとに最大 16 台のホストを追加できます。プロビジョニングされたすべて のプライベートクラウドには、vCenter Server、vSAN、vSphere、NSX-T があります。

Azure 上の VMware クラウド (VMC) を使用すると、必要な数の ESX ホストを使用して Azure 上にクラウドソフト ウェア定義データセンター (SDDC) を作成できます。Azure 上の VMC は、NetScaler VPX デプロイメントをサポ ートしています。VMC は、オンプレミスの vCenter と同じユーザー・インタフェースを提供します。これは、ESX ベースの NetScaler VPX 展開と同様に機能します。

次の図は、管理者またはクライアントがインターネット経由でアクセスできる Azure パブリッククラウド上の Azure VMware ソリューションを示しています。管理者は、Azure VMware ソリューションを使用して、ワークロードまた はサーバー仮想マシンを作成、管理、および構成できます。管理者は、Windows ジャンプボックスから AVS の Web ベースの vCenter および NSX-T マネージャにアクセスできます。vCenter を使用して Azure VMware Solution 内に NetScaler VPX インスタンス(スタンドアロンまたは高可用性ペア)とサーバー仮想マシンを作成し、NSX-T Manager を使用して対応するネットワークを管理できます。AVS 上の NetScaler VPX インスタンスは、オンプレ ミスの VMware ホストのクラスタと同様に機能します。AVS は、同じ仮想ネットワーク内に作成された Windows ジャンプボックスから管理されます。

クライアントは、ADC の VIP に接続することによってのみ AVS サービスにアクセスできます。Azure VMware ソリ ューション外の別の NetScaler VPX インスタンスは、同じ Azure 仮想ネットワーク内にある別の NetScaler VPX インスタンスは、Azure VMware ソリューション内の NetScaler VPX インスタンスの VIP をサービスとして追加 するのに役立ちます。要件に応じて、インターネット上でサービスを提供するように NetScaler VPX インスタンス を構成できます。



前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- Azure VMware ソリューションとその前提条件の詳細については、Azure VMware ソリューションのドキュ メントを参照してください。
- Azure VMware ソリューションのデプロイの詳細については、「Azure VMware ソリューションのプライベ ートクラウドをデプロイする」を参照してください。
- Azure VMware ソリューションにアクセスして管理するための Windows ジャンプボックス仮想マシンの作成の詳細については、「Azure VMware ソリューションのプライベートクラウドにアクセスする」を参照してください。
- Windows ジャンプボックス仮想マシンで、NetScaler VPX アプライアンスセットアップファイルをダウン ロードします。
- 仮想マシンが接続する VMware SDDC 上に、適切な NSX-T ネットワークセグメントを作成します。詳細については、「Azure VMware ソリューションでのネットワークセグメントの追加」を参照してください。
- VPX ライセンスファイルを入手します。
- Azure VMware Solution プライベートクラウドに作成または移行された仮想マシン (VM) は、ネットワーク セグメントに接続する必要があります。

VMware クラウドのハードウェア要件

次の表に、VMware SDDC が各 VPX nCore 仮想アプライアンスに対して提供する必要がある仮想コンピューティン グリソースを示します。

表 1. NetScaler VPX インスタンスの実行に必要な最小限の仮想コンピューティングリソース

コンポーネント	条件
メモリ	2 GB
仮想 CPU(VCPU)	2
仮想ネットワークインターフェイス	VMware SDDC では、VPX ハードウェアをバージョン7 以上にアップグレードすると、最大 10 個の仮想ネット ワーク インターフェイスをインストールできます。
ディスク領域	20GB

注

これは、ハイパーバイザーのディスク要件に加えて必要になります。

VPX 仮想アプライアンスを実稼働で使用するには、フルメモリ割り当てを予約する必要があります。

OVF ツール 1.0 のシステム要件

Open Virtualization Format Tool (OVF Tool) は、Windows および Linux システムで実行できるクライアント アプリケーションです。次の表に、OVF ツールをインストールするためのシステム要件を示します。

```
表 2. OVF ツールのインストールに関するシステム要件
```

コンポーネント	条件
オペレーティングシステム	VMware からの詳細な要件については、
	http://kb.vmware.com/で『OVF ツールユーザーガ
	イド』の PDF ファイルを検索してください。
CPU	最低 750MHz、1GHz 以上推奨
RAM	最小1GB、推奨2GB
NIC	100Mbps 以上の NIC。

OVF のインストールについては、http://kb.vmware.com/で『OVF ツールユーザーガイド』の PDF ファイルを検 索してください。

NetScaler VPX セットアップファイルのダウンロード

VMware ESX 用の NetScaler VPX インスタンスセットアップパッケージは、オープン仮想マシン(OVF)フォーマット標準に準拠しています。これらのファイルは、Citrix Web サイトからダウンロードできます。ログオンするには、Citrix アカウントが必要です。Citrix アカウントをお持ちでない場合は、http://www.citrix.comのホームページにアクセスしてください。[新しいユーザー] リンクをクリックし、指示に従って新しい Citrix アカウントを作成します。

ログオンしたら、Citrix のホームページから次のパスをナビゲートします。

Citrix.com > ダウンロード > NetScaler > 仮想アプライアンス。

次のファイルを、ESX サーバーと同じネットワーク上のワークステーションにコピーします。3 つのファイルをすべ て同じフォルダーにコピーします。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (例えば、NSVPX-ESX-13.0-79.64disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf(例えば、NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf(例えば、NSVPX-ESX-13.0-79.64.mf)

Azure VMware ソリューションをデプロイする

1. Microsoft Azure ポータルにログインし、Azureマーケットプレイスに移動します。

2. Azure マーケットプレイスから AzureVMware ソリューションを検索し、[作成] をクリックします。



- 3. [プライベートクラウドの作成]ページで、次の詳細を入力します。
 - プライベートクラウドのデフォルトクラスタを作成するには、最低3つの ESXi ホストを選択します。
 - [Address ブロック] フィールドには、/22 アドレス空間を使用します。
 - 仮想ネットワークの場合、CIDR 範囲が、オンプレミスまたはその他の Azure サブネット (仮想ネット ワーク) またはゲートウェイサブネットと重複していないことを確認します。
 - ゲートウェイサブネットは、プライベートクラウドとの接続のルーティングを表現するために使用されます。
Home >

g_		
Subscription * (i)		~
Resource group * 🛈		~
	Create new	
Location * (i)	(US) East US	\sim
General		
Resource name * 🛈	avs-cloud1	~
SKU * 🛈	AV36 Node	\checkmark
ESXi hosts * 🕕	0	3
		\$11,929.68
		estimated monthly total
Address block * 🛈	192.168.0.0/20	~
Virtual Network	avs-cloud-vnet1	\sim
	Create new Only Virtual Networks with a valid subnet with the r	name "GatewaySubnet"

4. [レビュー]+[作成]をクリックします。

5. 設定を確認します。設定を変更する必要がある場合は、[前へ]をクリックします。

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. [**Create**] をクリックします。プライベートクラウドのプロビジョニングプロセスが開始されます。プライベ ートクラウドのプロビジョニングには最大2時間かかることがあります。

Home > Microsoft.AVS-20210 Deployment	0609092342 Overview 🖈 … ×
✓ Search (Cmd+/) «	💼 Delete 🚫 Cancel <u> </u> Redeploy C Refresh
👶 Overview	Ø We'd love your feedback! →
🔄 Inputs	
š≣ Outputs	Your deployment is complete
Template	Deployment name: MicrosoftAVS-20210609092342 Subscription: Resource group: avs-cloud-new Subscription: Correlation ID: 7330c8b1-6d0b-4dcd-aa8d-aef81b1b
	✓ Deployment details (Download)
	∧ Next steps
	Go to resource

7. [リソースに移動]をクリックして、作成されたプライベートクラウドを確認します。

JSON Vie
ork

このリソースにアクセスするには、Windows でジャンプボックスとして機能する仮想マシンが必要です。

Windows を実行している Azure 仮想マシンに接続する

この手順では、Azure ポータルを使用して、Windows Server 2019 を実行する仮想マシン (VM) を Azure にデプ ロイする方法について説明します。VM の動作を確認するには、仮想マシンに RDP し、IIS Web サーバーをインスト ールします。

作成したプライベートクラウドにアクセスするには、同じ仮想ネットワーク内に Windows ジャンプボックスを作成 する必要があります。

1. Azure ポータルに移動し、[リソースの作成] をクリックします。

≡	Microsoft Azure		sources, services,	and docs (G+/)	Σ	🕞 Q 🥸	≥ ? <i>?</i> ?		
	Azure service	s							
	+		<u> </u>		DNS			•	
	Create a resource	Marketplace	Virtual networks	Azure VMware Solution	DNS zones	Virtual machines	Load balancers	Subscriptions	
	()	\rightarrow							
	Resource groups	More services							

2. Microsoft Windows 10 を検索し、[作成] をクリックします。

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

3. Windows Server 2019 を実行する仮想マシン (VM) を作成します。[仮想マシンの作成] ページが表示され ます。[基本] タブにすべての詳細を入力し、[ライセンス] チェックボックスをオンにします。残りのデフォル トのままにして、ページの下部にある [**Review + create**] ボタンを選択します。

Home > Create a resource > Microsoft Windows 10 >					
Create a virtual machin	e				
Basics Disks Networking	Management Advanced Tags Review + create				
Create a virtual machine that r marketplace or use your own o create to provision a virtual m customization. Learn more o Project details	uns Linux or Windows. Select an image from Azure customized image. Complete the Basics tab then Review + achine with default parameters or review each tab for full				
Select the subscription to man folders to organize and manage	age deployed resources and costs. Use resource groups like e 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 * 🕢	See all images				
Azure Spot instance $_{\odot}$					
Size * 💿	Standard_D2 - 2 vcpus, 7 GiB memory (US\$67.16/m See all sizes				
Administrator account					
Username * 💿					
Password * 🕕	······································				
Confirm password *	······ ·				
Inbound port rules					
Select which virtual machine n specify more limited or granul	etwork ports are accessible from the public internet. You can ar network access on the Networking tab.				
Public inbound ports * 💿	O None Allow selected ports				
Select inbound ports *	RDP (3389)				
	▲ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced Controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.				
Licensing					
 I confirm I have an eligible multi-tenant hosting rights 	Windows 10 license with .*				
Review multi-tenant hosting ri	ghts for Windows 10 compliance				
Review + create < Pt	revious Next : Disks >				

- 4. 検証の実行後、ページの下部にある [作成] ボタンを選択します。
- 5. デプロイが完了したら、[リソースに移動]を選択します。
- 6. 作成した Windows 仮想マシンに移動します。Windows 仮想マシンのパブリック IP アドレスを使用し、 RDP を使用して接続します。

Azure ポータルの [接続] ボタンを使用して、Windows デスクトップからリモートデスクトップ (RDP) セッションを開始します。まず仮想マシンに接続し、次にサインオンします。

Mac から Windows 仮想マシンに接続するには、Microsoft リモートデスクトップなどの Mac 用 RDP クラ

イアントをインストールする必要があります。詳細については、「Windows を実行する Azure 仮想マシンに 接続してサインオンする方法」を参照してください。

プライベートクラウド vCenter ポータルにアクセスする

1. Azure VMware ソリューションのプライベートクラウドで、[管理]で[アイデンティティ]を選択します。 vCenter の認証情報を書き留めます。

All services > Resource groups > Ovive	kc-avs-demo > avs-cloud		
avs-cloud Identity	\$		×
	Login credentials		
🔷 Tags 🏠			
Diagnose and solve problems	Web client URL ①	https://192.168.0.2/	Copy to clipboard
Settings	Admin username (0)	cloudadmin@vsphere.local	M
🔒 Locks	Admin password ①		U
Manage			
🔶 Connectivity	Certificate thumbprint ①	B237D65A11869C2907A35856E3CD87A1280BA2FE	U
🖳 Identity	NSX-T Manager credentials		
Clusters	Web client URL ①	https://192.168.0.3/	۵) ا
Workload Networking	Admin username ③	admin	Ø
4 Segments	Admin password ①	0	
T DHCP	Certificate thumbprint ()	2362FAA1F4CAE9952646F2B62DF1BB87AC7CF368	۵
Port mirroring			
C DNC			

2. vCenter Web クライアントの URL を入力して、vSphere クライアントを起動します。

	https://192.168.0.2
vm ware [.]	
Setting Started	
The vSphere Flash-based Web Client is switching to the all-new modern HTML5 reverting to the Flash-based Web Clien LAUNCH VSPHERE G	s deprecated in vSphere 6.7. We recommend 5-based vSphere client as the primary client and only it when necessary.
LAUNCH VSPHERE WEB CLIE	ENT (FLEX) Deprecated
VMware vSphere Documentation Ce	enter

3. Azure VMware ソリューションプライベートクラウドの vCenter 認証情報を使用して VMware vSphere にログインします。



4. vSphere クライアントでは、Azure ポータルで作成した ESXi ホストを確認できます。

VSphere - vc.de7510d9c7d848:	50 x +					- o ×
← → C ▲ Not security	re https://192.168.0.2/ui/#?exte	nsionId=vsphere.core.inventory.s	erverObjectViewsExtension	n&objectId=urn:vmomi:Fol	der:group-d1:d77ece11-494 🏠	¢ @ …
vm vSphere Client	tenu 🗸 🛛 📿 Search in all envi	ronments			C ? v cloudadmin@VSPH	
	🗗 vc.de7510d9c7d84	85cb31194.eastus.avs.a	ZURE.COM	NS ¥		
🖉 vc.de7510d9c7d8485cb311	Summary Monitor Configu	re Permissions Datacenters	Hosts & Clusters VI	Ms Datastores Netwo	orks Linked vCenter Server System	s Extensions
 Is SDC-Datacenter Cluster-1 esx03-r09.p03.de7 esx04-r02.p03.de7 esx14-r15.p03.de75 	Vetual Machines: Hosts:	0			CPU Unet 11.87 CHz Manazy Unet 25.63 GB Samage Unet 6.82 78	Free 234.79 GHz Capachy 247.86 GHz Free 1.45 TB Capachy 168 TB Free 3161 TB Capachy 364 TB
	Custom Attributes		^ T	ags		^
	Attribute	Value		Assigned Tag	Cetegory Description	
			×	4		Ĵ
Recent Tasks Alarms						*
Task Name v Target	✓ Status 510d9c7d84 ✓ Completed	Details V Initiation HCX Disaster Recovery Plugin VSPH from umware hubble/blue VSPH	er v Queued f	For v Start Time 4	Completion Time V 3:17:18 PM 05/02/2021, 3:17:19 PM	Server v vc.de7510d9c7d8485c

詳細については、「プライベートクラウド vCenter ポータルへのアクセス」を参照してください。

Azure ポータルで NSX-T セグメントを作成します

NSX-T セグメントは、Azure ポータルの Azure VMware ソリューションコンソールから作成および構成できま す。これらのセグメントはデフォルトの Tier-1 ゲートウェイに接続され、これらのセグメントのワークロードは East-West および North-South 接続を取得します。セグメントを作成すると、NSX-T Manager および vCenter に表示されます。

Azure VMware ソリューションのプライベートクラウドで、[ワークロードネットワーキング]で、[セグメント]>[追加]の順に選択します。新しい論理セグメントの詳細を入力し、「OK」を選択します。クライアント、管理、およびサーバーインターフェイスに対して3つの別々のセグメントを作成できます。

All services > Resource groups > 0 avs-cloud Segment AVS Private cloud	vivekc-avs-dem ents ☆	o > avs-cloud				Add segment	×
P Search (Ctrl+/)	« + Add	🗐 Delete 💍 Refre	sh				
Overview	* "O Filte	r by name	Name : All IP Address :	All		Segment name * management	~
Activity log	Seg	ment name 1	Connected gateway 14	Gateway IP ↑↓	DHCP r	Connected gateway	
Access control (IAM) Tags		TNT22-HCK-UPUNK	TNT22-T1	192.168.3.1/26		T1 TNT22-T1	
Diagnose and solve problems Settings						Type Overlay segment	
🛆 Locks						Subnet Gateway *	
Manage						192.168.4.1/24	Example: 10.1.1.1/24
🖳 Identity						DHCP ranges (optional)	
Clusters						Enter DHCP ranges	
Workload Networking							
Segments							
T DHCP							
Port mirroring							Example: 10.1.1.0/24 or 10.1.1.10-10.1.1.100
DNS							
Monitoring			0			OK Cancel	

2. Azure VMware ソリューションのプライベートクラウドで、[管理]で[アイデンティティ]を選択します。 NSX-T マネージャのクレデンシャルを書き留めます。

avs-cloud Identity Image Login credentials 0 big-note and solve problems Vecnter credentials Web client UBL ○ https://192.168.0.2/ Admin username ○ doudadmin@vsphere.local 1 tocks Admin passeord ○ Image 2 contentity Certificate thumbprint ○ Big3270/65A11869C2807A35856EDCB7A12808A2FE Contentity NSX-T Manager credentials Image 2 contentity NSX-T Manager credentials Image 2 contentity NSX-T Manager credentials Image 2 contentity NSX-T Manager credentials Image 2 contentity Admin username ○ Image 3 contentity Certificate thumbprint ○ Image 4 dmin username ○ Image Image 6 contentity Admin passeord ○ Image 6 contentity Certificate thumbprint ○ Image 6 contentity Certificate thumbprint ○ Image 6 contentity Certificate thumbprint ○ Image	All services > Resource groups > Oviv	vekc-avs-demo > avs-cloud			
D Sarch (Criti-/) Kogin credentials b Jagnois and solve problems Vicente credentials Web Client URL Intrp://192.168.0.2/ strings Admin usemame O Connectivity Certificate thumbprint O B27Db5A11866C2907A32856B2C0D7A1280BA3FE Connectivity Stdently Veb client URL O MSX-T Manager credentials Web client URL O Admin usemame O Connectivity Stdently Outrers Charters Stopments OLCP Certificate thumbprint O Stopments OLCP	AVS Private cloud Identity	1 \$			
Objignose and solve problems Web client URL	Search (Ctrl+/) « Tags	Login credentials			
sttligs Admin usemame () douldatini@vsphere.local anage Admin password () Image Connectivity Certificate thumbprint () IB327D65A11869C2097A35856E3CD87A12808A2FE Connectivity Certificate thumbprint () IB327D65A11869C2097A35856E3CD87A12808A2FE Connectivity NSX-T Manager credentials	Diagnose and solve problems	Web client URL ①	https://192.168.0.2/		
Admin password ① Image Connectivity Certificate thumbprint ① E237065A11869C2907A35856E3CD87A1280RA3FE MSX.T Manager credentials Imager Connectivity	ettings	Admin username 🕕	cloudadmin@vsphere.local		
Jange Certificate thumbprint © B237D65A11869C2907A35856E3CD87A1280BA2FE © Connectivity NSX-T Manager credentials	LOCKS	Admin password ①	ß		
kidentity NSX-T Manager credentials D Cutters Web client URL O https://192.168.0.3/ Image: Comparison of Compa	Connectivity	Certificate thumbprint ①	B237D65A11B69C2907A35856E3CD87A12B0BA2FE		
Cutters Web client UFL O https://192.168.0.3/ Konfold Networking Admin usemane O admin Segments Admin password O Image: Client UFL Cl	Identity	NSX-T Manager credentials			
vkload Networking Admin username O admin Segments Admin password O C DHCP Certificate thumbprint O 2362FAA1F4CAE9952646F2862DF18887AC7CF368	Clusters	Web client URL ①	https://192.168.0.3/		
Segments Admin password O Segments DHCP Certificate thumbprint O 236276A1F46C459952646F2862D1F18887ACTCF368	orkload Networking	Admin username 🛈	admin		
DHCP Certificate thumbprint ① 2362FAA1F4CAE9952646F2862DF18B87AC7CF368	Segments	Admin password 🛈			
	DHCP	Certificate thumbprint 🕕	2362FAA1F4CAE9952646F2B62DF1BB87AC7CF368		
Port mirroring	Port mirroring				

3. NSX-T Web クライアント URL を入力して VMware NSX-T マネージャを起動します。



4. NSX-T マネージャの [ネットワーク]> [セグメント] の下に、作成したすべてのセグメントが表示されます。 サブネットを確認することもできます。

🕑 VSphere - vc.de7510d9c7d8485	× MSX		× +						-
$\leftarrow ightarrow extsf{C} \ igstarrow extsf{Not secure}$	https://19	2.168.0	0.3/nsx/#/app/networks/segments/	module/home			ίô	£≣	œ
vm NSX-T						Q	¢		ad
Home Networking Secur	rity Inver	ntory	Plan & Troubleshoot System	Advanced Networking & Security					
Network Overview Connectivity	ADD SEGN		SEGMENT PROFILES		EXPAND ALL	Filter by I	Name, Pai	th or more	
🔁 Tier-O Gateways			Segment Name	Connected Gateway & Type		Subnet	5	Status	Т
🔁 Tier-1 Gateways	\Rightarrow	~	client	TNT22-T1 Tier1 - Flexible		1⊳		• Up	с
🝕 Segments	\vdots >	~	management	TNT22-T1 Tier1 - Flexible		1		• Up	с
Network Services	\Rightarrow	\$	server	TNT22-T1 Tier1 - Flexible		1		• Up	C
VPN	: >	œą	TNT22-HCX-UPLINK	TN 122-11 Tiert - Mexible		1		🔮 Ορ	C
∃• NAT	$: \rightarrow$	oe{	TNT22-T0-PRIVATE01-LS	None - Flexible				• Up	С
Load Balancing	\Rightarrow	¢	TNT22-T0-PRIVATE02-LS	None - Flexible				• Up	С
Porwarding Policies									

詳細については、「Azure ポータルで NSX-T セグメントを作成する」を参照してください。

VMware クラウドへの Citrix ADC VPX インスタンスのインストール

VMware ソフトウェア定義データセンター(SDDC)をインストールして構成したら、SDDC を使用して VMware クラウドに仮想アプライアンスをインストールできます。インストールできる仮想アプライアンスの数は、SDDC で 使用可能なメモリの量によって異なります。

VMware クラウドに NetScaler VPX インスタンスをインストールするには、Windows ジャンプボックス仮想マシンで次の手順を実行します。

- 1. ESXi ホスト用の NetScaler VPX インスタンスセットアップファイルを、NetScaler ダウンロードサイトか らダウンロードします。
- 2. Windows のジャンプボックスで VMware SDDC を開きます。

- 3. [ユーザー名] フィールドと [パスワード] フィールドに管理者の資格情報を入力し、[ログイン] をクリックします。
- 4. [File] メニューの [Deploy OVF Template] を選択します。
- 5. [OVF テンプレートのデプロイ] ダイアログボックスの [ファイルからの展開] フィールドで、NetScaler VPX インスタンスセットアップファイルを保存した場所を参照し、.ovf ファイルを選択し、[次へ] をクリッ クします。

) しょり。 注

> デフォルトでは、NetScaler VPX インスタンスは E1000 ネットワークインターフェイスを使用します。 VMXNET3 インターフェイスで ADC を展開するには、E1000 ではなく VMXNET3 インターフェイスを 使用するように OVF を変更します。VMXNET3 インターフェイスの可用性は Azure インフラストラク チャによって制限され、Azure VMware ソリューションでは利用できない場合があります。

6. 仮想アプライアンス OVF テンプレートに表示されるネットワークを、VMware SDDC で設定したネットワー クにマッピングします。[作成] または [**OK**] をクリックします。

 vSphere - NSV9%-ESX-13.0-7 C A Not see: 	9.6- x NSX	x +	uantou ranue Obiart Viewe Externion Robiart Idu	mumomi/litualMachineum.53:d77eea
vm vSphere Client	Menu 🗸 🔤	 Search in all environments 	анның зеглегылдал темәлдегін тылық елім - ч	C
0 0 9 0	Summary	Edit Settings NSVPX-ESX-13.0- Virtual Hardware VM Options	79.64_nc_64	×
SDDC-Datacenter Guster-1				ADD NEW DEVICE
esx03-r09.p03.de7		> CPU	2 ~	0
esx14-r15.p03.de7	Pown	> Memory	2 GB ~	
		> Hard disk 1	20 GB ~	
	Launch Ren	> SCSI controller 0	LSI Logic Parallel	
	(marine)	> Network adapter 1	management ~	Connect
	VMHaro	> New Network *	client ~	Connect
	Related (> New Network *	server v	Connect
	Clust	> Video card	Specify custom settings ~	
	Host	VMCI device	Device on the virtual machine PCI bus that provid	es support for the
	Netw		virtual machine communication interface	
Recent Tasks Alarms		> Other	Additional Hardware	
Task Name v Target				Completion Tim
Deploy OVF template	X-ESX-13:0-7			05/02/2021, 4
Import OVF package				CANCEL OK DSID2/2021.4

7. [完了]をクリックして VMware SDDC への仮想アプライアンスのインストールを開始します。

C.de7510d9c7d8485cb311, ✓ 2 Select a na ✓ 2 Select a na ✓ 2 Select a na	VF template Ready to complete me and folder Click Finish to start crea	Ready to complete Click Printh to start creation.					
SDDC-Datacenter Cluster-1 exx03-r09.p03.de7. Select son	ails age Provisioning type	Deploy from template					
esx04-r02.p03.de7 Ready to o	omplete	NSVPX-ESX-13.0-79.64_nc_64					
	Template name	NSVPX-ESX-13.0-79.64_nc_64					
	Download size	599.9 MB					
	Size on disk	20.0 GB					
	Folder	SDDC-Datacenter					
	Resource	Cluster-1					
	Storage mapping	1					
	All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy					
	Network mapping	1					
	VM Network	management					
ent Tasks Alarms	IP allocation settings						
iame v Target	IP protocol	IPv4					
t OVF peckage	IP allocation	Challe - Marcual					

8. これで、NetScaler VPX インスタンスを起動する準備ができました。ナビゲーションペインで、インストー ルした Citrix ADC VPX インスタンスを選択し、右クリックメニューから [パワーオン] を選択します。コン ソールポートをエミュレートするには、[**Console**] タブをクリックします。

	Actions - NSVPX-ESX-13.0-79.64_n_	≜									~				
vm vSphere Cl	Power &	Power On	ctrl + all + B							G	?) ~	cloudadming	IVSPHER	ELOCA	· *
	Guest OS	Power Off			B 🖏	ACTIO	DNS ¥								
Due de 7510 d0 - 7 d0	Snapshots	 Suspend 		astores	Naturala										
SDDC-Datacent	💕 Open Remote Console	🙆 Resal		astores	NETWORKS										
Cluster-1	🚰 Migrate	Shut Drive Scient (15		4-bit) Mis alt + D VM version 9)							O H	USAGE IZ			
esx04-r02	Clone	Restart Gaint III.		stalled										MEN	ORY USAGE
esx14-r15.c	Fault Tolerance	DNS Name:												08	3
D NSVPX-ES	VM Policies	Host: esx0	4-r02.p03.de	1.de7510d9c7d8485cb31194.eastus.avs.azure.com							STO 40	RAGE USAG			
	Template												40	.00 00	
	Compatibility														
	Export System Logs					~	Notes								^
	🚱 Edit Settings						Edit Not	es							
	Move to folder					<u></u>									
	Rename	Cluster-1				Custom Attributes							^		
	Edit Notes	🛛 esc	04-r02.p03.de	7510d9c7d84	85cb31194.east.		Attribut	10			Velu	*			
	Tags & Custom Attributes	e cier	vt												
ecent Tasks Ala	Add Permission														
sk Name	Alarms	- Details		 Initiator 	~	Que	ued For	~	Start Time 🕹		~ Con	pietion Time	×	Server	
configure virtual achine	Remove from Inventory	ed		VSPHERE	LOCAL\cloud	4 m	5		05/02/2021,	4:11:08 PM	05/0	2/2021, 4:11:08	PM	vc.de751	0d9c7d8485
aniou OME template	Delate from Disk	ed.		VSPHERE	LOCAL write	2 m			05/02/2021	4:08:26 PM	05.0	2/2021 4:09:12	DM .	ur de 751	0-10-7-18485-

9. これで、vSphere クライアントから NetScaler 仮想マシンに接続されています。

🔽 🛛 🕢 vSphere - NS	VPX-ESX-13.0-79.6 ×	NSVPX-ESX-1	1.0-79.64 nc. 64 X	NSX		x +	+	- (x c
< → C	A Not secure	https://192.168.0	2/ui/webconsole.h	tml?vmld=v	m-53&vmName=	NSVP	YX-ESX-13.0-79.64_nc_64&serverGuid=d77ece11-4945-4ee5-bb8e-17b4 🏠 兌 🤇	b (5	
NSVPX-ESX-13 0-79	64 pc 64						Enform IIC Keyboard Jawait Visus Euligeneon Co.	d ChinA	ta Doloto
HOTT A-EGA-10.0-19	iii						Entirol US Reyouard Layout View Fullscheim Sen	d Gill*A	(*Delete
	NotScal	or has st	arted out	cossfu	. 1 1				
	Start a	dditional	daemons	: Mau	2 16:12	:54	<local0.err> ns nsconfigd: dispatch()</local0.err>		
	: Inval	id passwo	ord	, indy	E 20-26	- 0 -	(isoaisteri) ne neesniigaaispatent,		
	May 2 1	16:12:54	<local0.e< td=""><td>err> ns</td><td>s nsconf</td><td>igd</td><td>: _dispatch(): Specified parameters are</td><td></td><td></td></local0.e<>	err> ns	s nsconf	igd	: _dispatch(): Specified parameters are		
	not app	plicable	for this	type o	of SSL p	rof	ile.		
	May 2	16:12:54	<local0.0< td=""><td>err> ns</td><td>s nsconf</td><td>igd</td><td>: _dispatch(): Invalid rule.</td><td></td><td></td></local0.0<>	err> ns	s nsconf	igd	: _dispatch(): Invalid rule.		
	Mau 2	16:12:55		err> ns	s last me	iad	aye repeated 2 times : disnatch(): No such resource		
	May 2	16:12:55	<local0.e< td=""><td>err> ns</td><td>s nsconf</td><td>iaq</td><td>: _dispatch(): No such policy exists</td><td></td><td></td></local0.e<>	err> ns	s nsconf	iaq	: _dispatch(): No such policy exists		
	Monit M	onit daer	ion at 100	10 awa)	kened	- 9			
	May 2	16:12:55	<loca10.0< td=""><td>err> ns</td><td>s last me</td><td>ess</td><td>age repeated 4 times</td><td></td><td></td></loca10.0<>	err> ns	s last me	ess	age repeated 4 times		
	May 2:	10:13:00	<user.cr< td=""><td>it> ns</td><td>sysheal</td><td>τηα</td><td>: SYSIA 450010, IPMI device read failed</td><td></td><td></td></user.cr<>	it> ns	sysheal	τηα	: SYSIA 450010, IPMI device read failed		
	Mau 2 1	16:13:00	<local0.e< td=""><td>err> ns</td><td>s nscolle</td><td>ect</td><td>: ns conufile(): Not able to get info o</td><td></td><td></td></local0.e<>	err> ns	s nscolle	ect	: ns conufile(): Not able to get info o		
	f file /	/var/log/	'db∕defau	lt/nsde	evmap.tx	t :	No such file or directory		
	May 2	16:13:01	<local0.0< td=""><td>err> ns</td><td>s nsumon</td><td>d [1</td><td>639]: nsumond daemon started</td><td></td><td></td></local0.0<>	err> ns	s nsumon	d [1	639]: nsumond daemon started		

10. SSH キーを使用して NetScaler アプライアンスにアクセスするには、CLI で次のコマンドを入力します。

1 ssh nsroot@<management IP address> 例

- 1 ssh nsroot@192.168.4.5
- 11. ADC の設定は、show ns ipコマンドを使用して確認できます。



Azure VMware ソリューションでスタンドアロンの NetScaler ADC VPX インスタ

ンスを構成する

October 17, 2024

インターネット向けアプリケーション用の Azure VMware ソリューション(AVS)上の NetScaler VPX スタンドア ロンインスタンスを構成できます。

次の図は、Azure VMware ソリューション上の NetScaler VPX スタンドアロンインスタンスを示しています。クラ イアントは、AVS 内の NetScaler の仮想 IP(VIP)アドレスに接続することで AVS サービスにアクセスできます。 これを実現するには、NetScaler ロードバランサーまたは Azure ロードバランサーインスタンスを AVS の外部で同 じ Azure 仮想ネットワーク内にプロビジョニングします。AVS サービス内の NetScaler VPX インスタンスの VIP にアクセスするようにロードバランサーを構成します。



前提条件

仮想アプライアンスのインストールを開始する前に、次の Azure の前提条件をお読みください。

- Azure VMware ソリューションとその前提条件の詳細については、Azure VMware ソリューションのドキュ メントを参照してください。
- Azure VMware ソリューションのデプロイの詳細については、「Azure VMware ソリューションのプライベ ートクラウドをデプロイする」を参照してください。
- Azure VMware ソリューションにアクセスして管理するための Windows ジャンプボックス仮想マシンの作成の詳細については、「Azure VMware ソリューションのプライベートクラウドへのアクセス」を参照してください。

- Windows ジャンプボックス仮想マシンで、NetScaler VPX アプライアンスセットアップファイルをダウン ロードします。
- 仮想マシンが接続する VMware SDDC 上に、適切な NSX-T ネットワークセグメントを作成します。詳細に ついては、「Azure VMware ソリューションでのネットワークセグメントの追加」を参照してください。
- VMware クラウドに NetScaler VPX インスタンスをインストールする方法の詳細については、「VMware ク ラウドに NetScaler VPX インスタンスをインストールする」を参照してください。

NetScaler ロードバランサーを使用して AVS 上の NetScaler VPX スタンドアロンインスタンスを構成 します

次の手順に従って、NetScaler ロードバランサーを使用するインターネット向けアプリケーション用に AVS 上の NetScaler VPX スタンドアロンインスタンスを構成します。

1. NetScaler VPX インスタンスを Azure クラウドにデプロイします。詳細については、「NetScaler VPX スタンドアロン インスタンスの構成」を参照してください。

```
注
```

Azure VMware Cloud と同じ仮想ネットワークにデプロイされていることを確認します。

- 2. AVS にデプロイされた NetScaler VPX の VIP アドレスにアクセスするように NetScaler VPX インスタンス を構成します。
 - a) 負荷分散仮想サーバーを追加します。

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

例

1 add lb vserver lb1 HTTPS 172.31.0.6 443

b) AVS にデプロイされた NetScaler VPX IP に接続するサービスを追加します。

```
1 add service <name> <ip> <serviceType> <port>
```

add service webserver1 192.168.4.10 HTTP 80

c) サービスを負荷分散仮想サーバーにバインドします。

1 bind lb vserver <name> <serviceName>

- 例
 - 1 bind lb vserver lb1 webserver1

Azure ロードバランサーを使用して AVS 上の NetScaler VPX スタンドアロンインスタンスを構成する

以下の手順に従って、Azure ロードバランサーを使用するインターネット向けアプリケーション用に AVS 上の NetScaler VPX スタンドアロンインスタンスを構成します。

- 1. Azure クラウドで Azure ロードバランサーインスタンスを構成します。詳しくは、ロードバランサーの作成 に関する Azure ドキュメントを参照してください。
- 2. AVS にデプロイされている NetScaler VPX インスタンスの VIP アドレスをバックエンドプールに追加しま す。

次の Azure コマンドは、1 つのバックエンド IP アドレスを負荷分散バックエンドアドレスプールに追加します。

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="" td=""></vip>
	VMC>

注

Azure ロードバランサーが Azure VMware クラウドと同じ仮想ネットワークにデプロイされているこ とを確認します。

Azure VMware ソリューションで **Citrix ADC VPX** の高可用性セットアップを構成する

October 17, 2024

インターネットに接続するアプリケーション用の Azure VMware ソリューション(AVS)で NetScaler VPX HA セ ットアップを構成できます。

次の図は、AVS 上の NetScaler VPX HA ペアを示しています。クライアントは、AVS 内のプライマリ ADC ノードの VIP に接続することで、AVS サービスにアクセスできます。これを実現するには、NetScaler ロードバランサーまた は Azure ロードバランサーインスタンスを AVS の外部で同じ Azure 仮想ネットワーク内にプロビジョニングしま す。AVS サービス内のプライマリ ADC ノードの VIP にアクセスするようにロードバランサを設定します。



前提条件

仮想アプライアンスのインストールを開始する前に、次の Azure の前提条件をお読みください。

- Azure VMware ソリューションとその前提条件の詳細については、Azure VMware ソリューションのドキュ メントを参照してください。
- Azure VMware ソリューションのデプロイの詳細については、「Azure VMware ソリューションのプライベ ートクラウドをデプロイする」を参照してください。
- Azure VMware ソリューションにアクセスして管理するための Windows ジャンプボックス仮想マシンの作成の詳細については、「Azure VMware ソリューションのプライベートクラウドへのアクセス」を参照してください。
- Windows ジャンプボックス仮想マシンで、NetScaler VPX アプライアンスセットアップファイルをダウン ロードします。
- 仮想マシンが接続する VMware SDDC 上に、適切な NSX-T ネットワークセグメントを作成します。詳細に ついては、「Azure VMware Solution でのネットワークセグメントの追加」を参照してください。

構成の手順

以下の手順に従って、インターネット向けアプリケーションの AVS で NetScaler VPX 高可用性セットアップを構成 します。

1. VMware クラウド上に 2 つの NetScaler VPX インスタンスを作成します。詳細については、「VMware クラ ウドに NetScaler VPX インスタンスをインストールする」を参照してください。

- 2. NetScaler HA のセットアップを構成します。詳細については、「高可用性の構成」を参照してください。
- 3. インターネットに接続されたアプリケーションにアクセスできるように NetScaler HA セットアップを構成 します。
 - NetScaler ロードバランサーを使用して NetScaler VPX インスタンスを構成するには、「NetScaler ロードバランサーを使用して AVS 上に NetScaler VPX スタンドアロンインスタンスを構成する」を参照してください。
 - Azure ロード バランサーを使用して NetScaler VPX インスタンスを構成するには、「Azure ロード バランサーを使用して AVS で NetScaler VPX スタンドアロン インスタンスを構成する」を参照してください。

NetScaler VPX HA ペアで Azure ルートサーバーを構成する

October 17, 2024

NetScaler VPX インスタンスを使用して Azure ルートサーバーを構成し、BGP プロトコルを使用して仮想ネット ワークで構成された VIP ルートを交換できます。Citrix ADC は、スタンドアロンまたは HA-INC モードで展開し、 BGP で構成できます。この展開では、ADC HA ペアの前に Azure ロードバランサー (ALB) は必要ありません。

次の図は、VPX HA トポロジが Azure ルートサーバーとどのように統合されるかを示しています。各 ADC インスタ ンスには、管理用、クライアントトラフィック用、サーバートラフィック用の 3 つのインターフェイスがあります。



トポロジ図では、次の IP アドレスを使用します。

プライマリ ADC インスタンスの IP 設定の例:

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

セカンダリ ADC インスタンスの IP 設定の例:

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

前提条件

NetScaler VPX インスタンスを Azure に展開する前に、次の情報を理解している必要があります。

- Azure の用語とネットワークの詳細。詳細については、「Azure 用語」を参照してください。
- Azure Portal にルートサーバーを作成します。詳細については、「Azure portal を使用したルートサーバーの作成と構成」を参照してください。

- NetScaler アプライアンスの動作。詳しくは、NetScaler のドキュメントを参照してください。
- NetScaler ネットワーキング。詳細については、ADC ネットワークを参照してください。

NetScaler VPX HA ペアで Azure ルートサーバーを構成する方法

1. Azure ポータルでルート サーバーを作成します。詳細については、「

Azure Route Server とは」を参照してください。

次の例では、サブネット 10.0.3.0/24 が Azure サーバーのデプロイに使用されます。ルートサーバーが作成された ら、ルートサーバーの IP アドレスを取得します (例:10.0.3.4、10.0.3.5)。

Microsoft Azure	Search resources, services, and docs (G+/)	
Home > Resource groups > Azurer	uteserverIntegration >	
myRouteServer Route Server	? ☆ ···	×
	Delete	
😵 Overview	↑ Essentials	JSON View
Activity log	Resource group : <u>AzurerouteserverIntegration</u> Sta	us : Succeeded
Access control (IAM)	Location : eastus Virt	ual Network / Subnet : RSvnet/RouteServerSubnet
🔷 Tags	Subscription ASI	1 : 65515
Settings	Subscription ID Pee	/ lps : 10.0.3.4, 10.0.3.5
Configuration	Tags (edit) : <u>Click here to add tags</u>	
Peers		
Properties		
Locks		
Monitor		
Connection monitor		
Monitoring		
M Metrics		
Automation		
🔓 Tasks (preview)		
😫 Export template		

1 Azure Portal でネットワーク仮想アプライアンス (NVA) とのピアリングを設定します。NetScaler VPX インスタ ンスを NVA として追加します。詳細については、「NVA とのピアリングの設定」を参照してください。

次の例では、1/1 インターフェイスの ADC SNIP(10.0.1.4 と 10.0.1.5)と ASN: 400 と 500 がピアの追加時に使 用されます。

Home > Resource groups > AzurerouteserverIntegration > myRouteServer					
myRouteServer Peers * ··· Route Server ··· ···					×
✓ Search (Ctrl+/)	🗧 🕂 Add 💍 Refresi	h			
😵 Overview	Name	↑↓ ASN	↑↓ IPv4 Address	\uparrow Provisioning State	\uparrow_{\downarrow}
Activity log	ADC0	400	10.0.1.4	Succeeded	
Access control (IAM)	ADC1	500	10.0.1.5	Succeeded	
🧳 Tags					
Settings					

1高可用性構成用に2つの NetScaler ADC VPX インスタンスを追加します。

次の手順を実行します:

Azureに2つのVPXインスタンス (プライマリインスタンスとセカンダリインスタンス) をデプロイします。
 両方のインスタンスにクライアントとサーバーの NIC を追加します。

```
3 1. NetScaler GUIを使用して、両方のインスタンスで高可用性設定を構成しま
す。 1 プライマリ ADC インスタンスで動的ルーティングを設定します。
```

設定例:

```
1 ...
 2
   enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
3 enable ns feature LB BGP
4 add ns ip 10.0.1.4 255.255.25.0 -vServer DISABLED -dynamicRouting
         ENABLED
 5
   VTYSH
     configure terminal
 6
 7
     router BGP 400
8
   timers bgp 1 3
9 neighbor 10.0.3.4 remote-as 65515
10 neighbor 10.0.3.4 advertisement-interval 3
11 neighbor 10.0.3.4 fall-over bfd
12 neighbor 10.0.3.5 remote-as 65515
13 neighbor 10.0.3.5 advertisement-interval 3
14 neighbor 10.0.3.5 fall-over bfd
   address-family ipv4
15
   redistribute kernel
17 redistribute static
18 ```
16
```

1 セカンダリ ADC インスタンスで動的ルーティングを設定します。

設定例:

1	· · · ·
2	enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
3	enable ns feature LB BGP
4	add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting
	ENABLED
5	VTYSH
6	configure terminal
7	router BGP 500
8	timers bgp 1 3
9	neighbor 10.0.3.4 remote-as 65515
10	neighbor 10.0.3.4 advertisement-interval 3
11	neighbor 10.0.3.4 fall-over bfd
12	neighbor 10.0.3.5 remote-as 65515
13	neighbor 10.0.3.5 advertisement-interval 3
14	neighbor 10.0.3.5 fall-over bfd
15	address-family ipv4
16	redistribute kernel
17	redistribute static
18	

1 VTY シェルインターフェイスで BGP コマンドを使用して確立された BGP ピアを確認します。詳細については、「BGP 設定の確認」を参照してください。

1 ```

2 show ip bgp neighbors
3 ```

1 プライマリ ADC インスタンスで LB 仮想サーバーを設定します。

設定例:

. . .

1	
2	add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED
3	add lbvserver v1 HTTP 172.16.1.1 80
4	add service s1 10.0.2.6 HTTP 80
5	bind lbvserver v1 s1
6	enable ns feature lb
7	

NetScaler VPX インスタンスと同じ仮想ネットワーク内のクライアントが、LB 仮想サーバーにアクセスできるよう になりました。この場合、NetScaler VPX インスタンスは VIP ルートを Azure ルートサーバーにアドバタイズしま す。

バックエンドの Azure 自動スケーリングサービスを追加

October 17, 2024

クラウドでアプリケーションを効率的にホストすると、アプリケーションの必要に応じて、リソースを簡単にコスト 効率よく管理できます。増加する需要に対応するには、ネットワークリソースをスケールアップする必要があります。 需要が収まるかどうかにかかわらず、アイドル状態のリソースの不必要なコストを避けるためにスケールダウンする 必要があります。アプリケーションの実行コストを最小限に抑えるには、トラフィック、メモリ、CPU の使用などを 常に監視する必要があります。しかし、トラフィックを手動で監視するのは煩雑です。アプリケーション環境を動的 にスケールアップまたはスケールダウンするには、トラフィックを監視し、必要に応じてリソースをスケールアップ またはスケールダウンするプロセスを自動化する必要があります。

Azure での VPX マルチ IP スタンドアロンおよび高可用性のデプロイには、Azure 仮想マシンスケールセット (VMSS) で Autoscale を使用できます。

Azure VMSS および AAutoscale 機能と統合された NetScaler VPX インスタンスには、次の利点があります。

- 負荷分散と管理:需要に応じてサーバーをスケールアップおよびスケールダウンするように自動構成します。 NetScaler VPX インスタンスは、VPX インスタンスが展開されているのと同じ仮想ネットワーク、または同 じ Azure サブスクリプション内のピアリングされた仮想ネットワーク内の VMS AAutoscale e 設定を自動検 出します。VMSS Autoscale 設定を選択して、負荷を分散できます。これは、VPX インスタンスで NetScaler 仮想 IP アドレスとサブネット IP アドレスを自動構成することによって行われます。
- 高可用性:Autoscale グループを検出し、サーバーの負荷を分散します。
- ネットワークの可用性の向上: VPX インスタンスは、異なる仮想ネットワーク(VNet)上のバックエンドサ ーバーをサポートします。



詳細については、次の Azure トピックを参照してください。

- 仮想マシンのスケールセットのドキュメント
- Microsoft Azure 仮想マシン、クラウドサービス、および Web アプリケーションの Autoscale の概要

はじめに

- Azure 関連の使用に関するガイドラインを参照してください。詳細については、「Microsoft Azure に NetScaler VPX インスタンスをデプロイする」を参照してください。
- 要件(スタンドアロンまたは高可用性デプロイ)に応じて、Azure上に3つのネットワークインターフェイス を使用して1つまたは複数のNetScaler VPX インスタンスを作成します。
- VPX インスタンスの 0/1 インターフェイスのネットワークセキュリティグループで TCP 9001 ポートを開き ます。VPX インスタンスは、このポートを使用してスケールアウトおよびスケールイン通知を受け取ります。
- NetScaler VPX インスタンスが展開されている同じ仮想ネットワークに Azure VMSS を作成します。VMSS と NetScaler VPX インスタンスが異なる Azure 仮想ネットワークに展開されている場合、次の条件を満たす 必要があります。
 - 両方の仮想ネットワークが同じ Azure サブスクリプションに含まれている必要があります。
 - 2 つの仮想ネットワークは、Azure の仮想ネットワークピアリング機能を使用して接続する必要があります。

既存の VMSS 設定がない場合は、次のタスクを完了します:

- a) VMSS の作成
- b) VMSS でオートスケールを有効にする
- c) VMSS Autoscale 設定でスケールインポリシーとスケールアウトポリシーを作成する

詳細については、「Azure 仮想マシンのスケールセットを使用した Autoscale の概要」を参照してください。

- NetScaler VPX は、ユニフォームオーケストレーションを使用する VMSS のみをサポートしています。フレ キシブルオーケストレーション機能を備えた VMSS はサポートされていません。詳細については、「Azure の 仮想マシンスケールセットのオーケストレーションモード」を参照してください。
- NetScaler リリース 14.1-12.x 以降、NetScaler VPX は Azure クラウドのマネージド ID をサポートしています。マネージド ID は、サービスプリンシパルを仮想マシンなどの Azure リソースにリンクします。マネージド ID では、クラウド認証情報 (アプリケーション ID、アプリケーションシークレット、テナント ID) を管理する必要がないため、セキュリティリスクを回避できます。現在、NetScaler VPX は、システムによって割り当てられた管理対象 ID と単ーユーザーが割り当てた管理対象 ID のみをサポートしています。複数ユーザーに割り当てられたマネージド ID はサポートされていません。

14.1-12.x より前の NetScaler リリースでは、Azure Active Directory(AAD)を介して NetScaler VPX クラウド認証情報を手動で管理する必要があります。新しく作成した AAD アプリケーションに貢献者の役割 を割り当てます。クラウド認証情報は、有効期限が切れた後、定期的に再作成する必要があります。詳細につ いては、「Azure Active Directory アプリケーションとサービスプリンシパルの作成」を参照してください。

Azure コンソールでマネージド ID を構成し、NetScaler でクラウド認証情報を構成すると、マネージド ID がクラウド認証情報よりも優先されます。

仮想マシンでのマネージド ID の設定

- 1. Azure Portal にサインインします。
- 2. 仮想マシンに移動し、[ID]を選択します。
- 3. 要件に応じて、[システム割り当て]または[ユーザー割り当て]のいずれかを選択します。
- 4. [ステータス]で[オン]を選択し、[保存]をクリックします。

new-test-14.1 Iden Virtual machine	tity ☆ …
₽ Search «	System assigned User assigned
📮 Size 🔺	
Ø Microsoft Defender for Cloud	A system assigned managed identity is restricted to one per resource and is tied to the inecycle of this resource. You can grant permiss using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have
Advisor recommendations	🗟 Save 🗙 Discard 🕐 Refresh 🛛 🖗 Got feedback?
Extensions + applications	
Availability + scaling	Status ①
Configuration	Off On
😢 Identity	
Properties	
Locks	
Operations	
✗ Bastion	

ステータスが保存されると、サービスプリンシパルオブジェクトが作成され、VM に割り当てられていることがわかります。

5.「Azure ロール割り当て」をクリックします。

Home > new-test-14.1	
new-test-14.1 Identi Virtual machine	ty ☆ ×
	System assigned User assigned
🖉 Connect	
🗧 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	
O Microsoft Defender for Cloud	Save X Discard V Retresh X Got feedback?
Advisor recommendations	
Extensions + applications	Status () Off On
Availability + scaling	Object (orincipal) ID
Configuration	78dc5c36-814f-44f0-a238-ccd992caae86
🐍 Identity	Permissions
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
✗ Bastion	access settings for the managed mentity because it can result in families.

- 6.「ロール割り当ての追加」ウィンドウで、スコープを選択します。次のオプションから選択できます:
 - サブスクリプション

VMSS と VM が異なるリソースグループにある場合は、スコープとして **Subscription** を使用してください。

• リソースグループ

VMSS が VM と同じリソースグループにある場合は、リソースグループをスコープとして使用します。

- Key Vault
- ストレージ
- SQL

選択した範囲に基づいて、他のフィールドの詳細を入力します。寄稿者の役割を割り当て、構成を保存します。

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

Azure ロール割り当てページには、作成したマネージド ID が表示されます。

Home > new-test-14.1 Identity >				
Azure role assignme	nts …			
+ Add role assignment (Preview)	🕐 Refresh			
If this identity has role assignments that	t you don't have permission to read, they	won't be shown in the list. Learn more	2	
Subscription *				
		\sim		
Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	() tahaj-test-ipconfig	Resource Group	new-test-14.1	None

7. ユーザー割り当てマネージド ID を作成するには、サブスクリプションを選択し、ユーザー割り当てマネージ ド ID を選択して、「追加」をクリックします。

Home > new-test-14.1		Add user assigned managed identity	×
new-test-14.1 Ic Virtual machine	dentity 🛪 …	Select a subscription	
₽ Search	System assigned User assigned		× *
📮 Size	▲	User assigned managed identities	
Ø Microsoft Defender for Cloud	User assigned managed identities enable Azure resources to authentic managed identities are created as standalone Azure resources, and ha	Filter by identity name and/or resource group name	
Advisor recommendations	managed identities. Similarly, a single user assigned managed identity	c aibBuiUserId1600306786 Resource Group: ibLinuxGalleryRG	
Extensions + applications	+ Add 📋 Remove 💍 Refresh 🛛 🞘 Got feedback?	test-user-assigned-mi	
Availability + scaling		Kesource Group. Prest	
Configuration	Name ↑↓ Resource	g Selected identities:	
🗞 Identity	No results	etest-user-assigned-mi	Pamawa
Properties		Subscrition: NSDev Platform CA anoop.agarwal@citrix.com	Remove
Locks			
Operations			
× Bastion		Add	
Auto-shutdown	Ŧ		

VMSS を NetScaler VPX インスタンスに追加する

次のステップを実行して、VPX インスタンスに Autoscale e 設定を追加します:

- 1. VPX インスタンスにログオンします。
- 2. [構成] > **[Azure**] > **[**認証情報の設定] に移動します。Autoscale 機能を機能させるために必要な Azure 認証 情報を追加します。

← Set Credentials

Application ID		
Application Secret		
ок	Cancel	

- 3. [システム]>[Azure]>[クラウドプロファイル]に移動し、[追加]をクリックしてクラウドプロファイルを 作成します。

Q Search Menu	ile
Favorites	ile 💿
AZURE	Delete
Cloud Profile	ch or you can enter Key : Value format
System	AUTO SCALE SETTING LOAD BALANCING VIRTUAL SERVER
AppExpert	

クラウドプロファイルの作成設定ページが表示されます。

← Create Cloud Profile

CloudProfile	
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*	
	\sim
uto Scale Setting Protocol	
нттр	\sim
uto Scale Setting Port	
80	

クラウドプロファイルは、NetScaler 負荷分散仮想サーバーと、Auto Scaling グループのサーバーとしてメ ンバー(サーバー)を持つサービスグループを作成します。バックエンドサーバーは、VPX インスタンスで構 成された SNIP を介して到達可能である必要があります。

クラウドプロファイルの作成時に留意すべきポイント

- 仮想サーバーの IP アドレスは、VPX インスタンスで使用可能な空き IP アドレスから自動的に設定されます。 詳細については、「Azure ポータルを使用して仮想マシンに複数の IP アドレスを割り当てる」を参照してくだ さい。
- オートスケール設定は、同じ仮想ネットワークまたはピアリングされた仮想ネットワーク内の NetScaler VPX インスタンスに接続されている VMSS インスタンスから事前入力されます。詳細については、「Azure 仮 想マシンのスケールセットを使用した Autoscale の概要」を参照してください。
- Auto Scale Setting Protocol と Auto Scale Setting Port を選択する際は、サーバーがプロトコルと ポートをリッスンしていることを確認し、サービスグループに正しいモニターをバインドしてください。デフ ォルトでは、TCP モニターが使用されます。
- SSL プロトコルタイプの自動スケーリングでは、クラウドプロファイルを作成した後、証明書がないために負荷分散仮想サーバーまたはサービスグループがダウンします。証明書は、仮想サーバまたはサービスグループ に手動でバインドできます。

注

NetScaler リリース 13.1-42.x 以降では、Azure の同じ VMSS を使用して、(異なるポートを使用して)サー ビスごとに異なるクラウドプロファイルを作成できます。したがって、NetScaler VPX インスタンスは、パブ リッククラウド内の同じ自動スケーリンググループを持つ複数のサービスをサポートします。

Azure portal でオートスケール関連の情報を表示するには、[仮想マシンスケールセット] に移動し、[** 仮想マシンスケールセット]>[スケーリング]**を選択します。

参照ドキュメント

NetScaler Application Delivery and Management を使用した Microsoft Azure での NetScaler VPX の自動 スケーリングの詳細については、「Azure Autoscale using NetScaler ADM」を参照してください。

NetScaler VPX 展開用の Azure タグ

October 17, 2024

Azure クラウドポータルでは、名前: 値のペア (Dept: Finance など) でリソースにタグを付けて、リソースグループ 間、およびポータル内でサブスクリプション間でリソースを分類して表示できます。タグ付けは、課金、管理、また は自動化のためにリソースを整理する必要がある場合に役立ちます。

VPX デプロイにおける Azure タグの仕組み

Azure Cloud にデプロイされた NetScaler VPX スタンドアロンおよび高可用性インスタンスの場合、Azure タグに 関連付けられた負荷分散サービスグループを作成できるようになりました。VPX インスタンスは、Azure 仮想マシン (バックエンドサーバー)とネットワークインターフェイス (NIC)、またはその両方をそれぞれのタグで常に監視し、 それに応じてサービスグループを更新します。

VPX インスタンスは、タグを使用してバックエンドサーバーの負荷分散を行うサービスグループを作成します。イン スタンスは、特定のタグ名とタグ値でタグ付けされたすべてのリソースについて Azure API にクエリします。割り当 てられたポーリング期間(デフォルトでは 60 秒)に応じて、VPX インスタンスは定期的に Azure API をポーリング し、VPX GUI で割り当てられたタグ名とタグ値を使用して利用可能なリソースを取得します。適切なタグが付いた VM または NIC が追加または削除されると、ADC はそれぞれの変更を検出し、VM または NIC の IP アドレスをサー ビスグループに自動的に追加または削除します。



はじめに

Citrix ADC 負荷分散サービスグループを作成する前に、Azure のサーバーにタグを追加します。タグは、仮想マシン または NIC に割り当てることができます。

Creator d34eed9579934591afbbdf28c92caf51 Im Gr info_no_auto_shutdown temporarily disable automated vm shutdown, if set to 'true', default value is 'false', A 3 dav lease by default will be provided during next run of on auto script if no view/update lease datetime. only valid if no_auto_shutdown tag set to 'true', max 14 davs lease is allowed all generic date/time string are valid (eg. 'Tue lun 20) no auto shutdown if alse	Name 🕕		Value ①	
info_no_auto_shutdown temporarily disable automated vm shutdown, if set to 'true'. default value is 'false'. info_no_auto_shutdown_lease_datetime_UTC A 3 dav lease by default will be provided during next run of on auto scrint if no view/update lease datetime. only valid if no_auto_shutdown tag set to 'true'. max 14 davs lease is allowed all generic date/time string are valid (en 'Tue lun 20') no auto shutdown : false	Creator	:	d34eed9579934591afbbdf28c92caf51	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 lun 20 if false if alse	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 rup of on auto script if no	1
no auto shutdown 🕴 false 🕅 🕅	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 lun 20	1
	no_auto_shutdown	:	false	1
no_auto_shutdown_lease_datetime_UTC : 🔟 🔂	no_auto_shutdown_lease_datetime_UTC	:		1
tag1 : false 🗎 🕅 🕅	tag1	:	false	10
		:		

```
Apply Discard changes
```

Azure タグの追加の詳細については、Microsoft ドキュメント「タグを使用して Azure リソースを整理する」を参照 してください。

注

Azure タグ設定を追加する ADC CLI コマンドは、数字またはアルファベットのみで始まり、他のキーボード文 字で始まらないタグ名とタグ値をサポートします。

VPX GUI を使用して Azure タグ設定を追加する方法

VPX GUI を使用して Azure タグクラウドプロファイルを VPX インスタンスに追加すると、インスタンスは指定され たタグを使用してバックエンドサーバーの負荷を分散できます。以下の手順を実行します:

- 1. VPX GUI から、[構成] > [Azure] > [クラウドプロファイル] に移動します。
- 2. [追加] をクリックしてクラウドプロファイルを作成します。クラウドプロファイルウィンドウが開きます。

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. 次のフィールドに値を入力します。
 - 名前: プロフィールの名前を追加します
 - 仮想サーバーの IP アドレス: 仮想サーバーの IP アドレスは、VPX インスタンスで使用可能な空き IP アドレスから自動的に設定されます。詳細については、「Azure ポータルを使用して仮想マシンに複数の IP アドレスを割り当てる」を参照してください。
 - タイプ: メニューから「AZURETAGS」を選択します。
 - Azure タグ名:Azure ポータルで仮想マシンまたは NIC に割り当てた名前を入力します。
 - Azure タグ値:Azure ポータルの VM または NIC に割り当てた値を入力します。
 - Azure ポーリング期間: デフォルトでは、ポーリング間隔は最小値の 60 秒です。必要に応じて変更でき ます。
 - 負荷分散サーバープロトコル: ロードバランサーがリッスンするプロトコルを選択します。
 - 負荷分散サーバーポート: ロードバランサーが受信するポートを選択します。
 - Azure タグ設定: このクラウドプロファイル用に作成されるサービスグループの名前。
 - Azure タグ設定プロトコル: バックエンドサーバーがリッスンするプロトコルを選択します。
 - Azure タグ設定ポート: バックエンドサーバーがリッスンするポートを選択します。

2. [Create] をクリックします。

タグ付けされた仮想マシンまたは NIC に対して、ロードバランサー仮想サーバーとサービスグループが作成されま す。ロードバランサー仮想サーバーを確認するには、VPX GUI から [** トラフィック管理] > [負荷分散] **[仮想サー バー] に移動します。

VPX CLI を使用して Azure タグ設定を追加する方法

NetScaler CLI で次のコマンドを入力して、Azure タグのクラウドプロファイルを作成します。

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

重要:

すべての構成を保存する必要があります。そうしないと、インスタンスを再起動した後に構成が失われま す。「save config」と入力します。

例 **1**:「mytagName/MyTagValue」ペアでタグ付けされたすべての Azure VM/NIC の HTTP トラフィックのクラ ウドプロファイルのサンプルコマンドを次に示します。

1 add cloud profile MyTagCloudProfile -type azuretags -vServerName MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP 2

```
    -vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue
    myTagValue -azurePollPeriod 60
    Done
```

クラウドプロファイルを表示するには、次のように入力します show cloudprofile。

例 2: 次の CLI コマンドは、例1 で新しく追加されたクラウドプロファイルに関する情報を出力します。

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

クラウドプロファイルを削除するには、「rm cloud profile <cloud profile name>」と入力し ます。

例3:次のコマンドは、例1で作成したクラウドプロファイルを削除します。

```
1 > rm cloudprofile MyTagCloudProfile
2 Done
```

トラブルシューティング

問題: ごくまれに、「rm cloud profile」CLI コマンドで、削除されたクラウドプロファイルに関連付けられているサ ービスグループおよびサーバーの削除に失敗することがあります。これは、削除されるクラウドプロファイルのポー リング期間が経過する秒前にコマンドが発行された場合に発生します。

解決方法:残りのサービスグループごとに次の CLI コマンドを入力して、残りのサービスグループを手動で削除しま す。

1 #> rm servicegroup <serviceGroupName>

残りの各サーバに対して次の CLI コマンドを入力して、残りのサーバもそれぞれ削除します。

1 #> rm server <name>

問題:CLI を使用して VPX インスタンスに Azure タグ設定を追加すると、ウォームリブート後も HA ペアノードで rain_tags プロセスが実行され続けます。

解決方法: ウォームリブート後に、セカンダリノードでプロセスを手動で終了します。セカンダリ HA ノードの CLI からシェルプロンプトに出ます。

1 #> shell

rain_tags プロセスを強制終了するには、次のコマンドを使用します。

```
1 # PID=`ps -aux | grep rain_tags | awk '{
2 print $2 }
3 '`; kill -9 $PID
```

問題: バックエンドサーバーは正常であるにもかかわらず、VPX インスタンスから到達できず、DOWN として報告さ れることがあります。解決方法: VPX インスタンスが、バックエンドサーバーに対応するタグ付き IP アドレスに到達 できることを確認します。タグ付きの NIC の場合、これは NIC の IP アドレスです。タグ付きの VM の場合、これは 仮想マシンのプライマリ IP アドレスです。VM/NIC が別の Azure VNet 上に存在する場合は、VNet ピアリングが有 効になっていることを確認します。

NetScaler VPX インスタンスで GSLB を構成する

January 15, 2025

グローバルサーバー負荷分散(GSLB)用に構成された NetScaler ADC アプライアンスは、WAN の障害点から保護 することにより、ディザスタリカバリとアプリケーションの継続的な可用性を提供します。GSLB は、クライアント 要求を最も近い、または最もパフォーマンスの高いデータセンター、または停止が発生した場合に存続しているデー タセンターに送信することにより、データセンター間で負荷を分散できます。

このセクションでは、Windows PowerShell コマンドを使用して、Microsoft Azure 環境の 2 つのサイトの VPX インスタンスで GSLB を有効にする方法について説明します。

注

GSLB の詳細については、「グローバルサーバーの負荷分散」を参照してください。

Azure 上の NetScaler VPX インスタンスで GSLB を構成するには、次の 2 つのステップがあります。

- 1. 各サイトに、複数の NIC と複数の IP アドレスを持つ VPX インスタンスを作成します。
- 2. VPX インスタンスで GSLB を有効にします。

注

複数の NIC および IP アドレスの構成の詳細については、「PowerShell コマンドを使用してスタンドアロンモ ードで Citrix ADC VPX インスタンスの複数の IP アドレスを構成する」を参照してください。

シナリオ

このシナリオには、2 つのサイト(Site 1 と Site 2)が含まれています。各サイトの VM(VM1 と VM2)には、複数の NIC、複数の IP アドレス、および GSLB が構成されています。

図. GSLB セットアップは、サイト1とサイト2の2つのサイトに実装されています。



Region 2 (Resource Group 2)

このシナリオでは、各 VM には 3 つの NIC(NIC 0/1、1/1、1/2)が設定されています。各 NIC に複数のプライベートおよびパブリック IP アドレスを設定できます。これらの NIC は次の目的で構成されています。

- NIC 0/1: 管理トラフィックを提供する
- NIC 1/1: クライアント側のトラフィックを提供する
- NIC 1/2: バックエンドサーバーと通信する

このシナリオで各 NIC に設定された IP アドレスの詳細については、「IP 構成の詳細 」セクションを参照してください。

パラメーター

このドキュメントのこのシナリオのサンプルパラメーター設定は、次のとおりです。

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

注

VPX インスタンスの最小要件は、2 つの vCPU と 2 GB の RAM です。

1	\$publisher="citrix"
2	Soffer="netscalerynx111"
4	
5	\$sku="netscalerbyol"
6 7	\$vorsion="]atost"
8	
9	\$vmNamePrefix="MultiIPVPX"
10	
11 12	shickamePretix="MultiipvPX"
13	<pre>\$osDiskSuffix="osdiskdb"</pre>
14	
15 16	<pre>\$number0†VMs=1</pre>
17	<pre>\$ipAddressPrefix="10.0.0."</pre>
18	
19	\$ipAddressPrefix1="10.0.1."
20	<pre>\$ipAddressPrefix2="10.0.2."</pre>
22	
23	\$pubIPName1="MultiIP-pip1"
24	<pre>\$pubIPName2="MultiIP-pip2"</pre>
26	
27	\$IpConfigName1="IPConfig1"
20	\$IPConfigName2="IPConfig-2"
30	
31	\$IPConfigName3="IPConfig-3"
32	STPConfigName4="TPConfig-4"
34	
35	<pre>\$frontendSubnetName="default"</pre>
36 27	$\frac{1}{1}$
38	spackendsublicitamet- sublici/_t
39	<pre>\$backendSubnetName2="subnet_2"</pre>
40	Course for Number of 10
41	ŞSUTTTXNUMDer=10

仮想マシンの作成

PowerShell コマンドを使用して、ステップ1~10 に従って、複数の NIC と複数の IP アドレスを使用して VM1 を 作成します。

- 1. リソースグループの作成
- 2. ストレージアカウントの作成
- 3. アベイラビリティセットの作成
- 4. 仮想ネットワークの作成
- 5. パブリック IP アドレスの作成
- 6. NIC の作成
- 7. VM 設定オブジェクトの作成
- 8. 認証情報を取得し、VMのOSプロパティを設定します
- 9. NIC の追加
- **10.** OS ディスクの指定と VM の作成

すべての手順とコマンドを完了して VM1 を作成した後で、これらの手順を繰り返して VM2 固有のパラメーターで VM2 を作成します。

リソースグループの作成

1 New-AzureRMResourceGroup -Name \$RGName -Location \$location

ストレージアカウントの作成

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

アベイラビリティセットの作成

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

仮想ネットワークの作成

1

1. サブネットを追加します。

 \$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name \$frontendSubnetName -AddressPrefix "10.0.0.0/24"
 \$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name \$backendSubnetName1 -AddressPrefix "10.0.1.0/24"
 \$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name \$backendSubnetName2 -AddressPrefix "10.0.2.0/24"

2. 仮想ネットワークオブジェクトを追加します。

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

3. サブネットを取得します。

1	<pre>\$frontendSubnet=\$vnet.Subnets</pre>
2	<pre>\$Name -eq \$frontendSubnetName }</pre>
3	
4	<pre>\$backendSubnet1=\$vnet.Subnets</pre>
5	<pre>\$_ Name -eq \$backendSubnetName1 }</pre>
6	
7	<pre>\$backendSubnet2=\$vnet.Subnets</pre>
8	<pre>\$Name -eq \$backendSubnetName2 }</pre>

パブリック IP アドレスの作成

1	<pre>\$pip1=New-AzureRmPublicIpAddress -Name \$pubIPName1 -ResourceGroupName</pre>
	<pre>\$RGName -Location \$location -AllocationMethod Dynamic</pre>
2	<pre>\$pip2=New-AzureRmPublicIpAddress -Name \$pubIPName2 -ResourceGroupName</pre>
	<pre>\$RGName -Location \$location -AllocationMethod Dynamic</pre>

NIC の作成

NIC 0/1 の作成

1	\$nic1Name=\$nicNamePrefix + \$suffixNumber + "-Mgmnt"
2	<pre>\$ipAddress1=\$ipAddressPrefix + \$suffixNumber</pre>
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 の作成

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 の作成

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

VM 設定オブジェクトの作成

1	\$vmName=\$vmNamePrefix
2	<pre>\$vmConfig=New-AzureRMVMConfig -VMName \$vmName -VMSize \$vmSize -</pre>
	AvailabilitySetId \$avSet.Id

認証情報の取得と OS プロパティの設定

1	<pre>\$cred=Get-Credential -Message "Type the name and password for VPX</pre>
	login."
2	\$vmConfig=Set-AzureRMVMOperatingSystem -VM \$vmConfig -Linux -
	ComputerName \$vmName -Credential \$cred
3	\$vmConfig=Set-AzureRMVMSourceImage -VM
	\$publisher -Offer \$offer -Skus \$sku -Version \$version

NIC の追加

1	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic1.Id -</pre>
	Primary
2	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic2.Id</pre>
3	<pre>\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic3.Id</pre>

OS ディスクの指定と VM の作成

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

注

「PowerShell コマンドを使用したマルチ NIC 仮想マシンの作成」に記載されている手順 1~10 を繰り返して、 VM2 に固有のパラメータを使用して VM2 を作成します。

IP 構成の詳細

次の IP アドレスを使用します。

テーブル **1**. VM1 で使用する IP アドレス

NIC	プライベート IP	パブリック IP(PIP)	説明
0/1	10.0.0.10	PIP1	NSIP(管理 IP)として構
			成
1/1	10.0.1.10	PIP2	SNIP/GSLB サイト IP と
			して設定されています
-	10.0.1.11	-	LB サーバ IP として設定
			されています。パブリック
			IP アドレスは必須ではあ
			りません
1/2	10.0.2.10	-	モニタプローブをサービス
			に送信するための SNIP と
			して設定。パブリック IP
			は必須ではありません。

表 2. VM2 で使用される IP アドレス

NIC	内部 IP	パブリック IP(PIP)	説明
0/1	20.0.0.10	PIP4	NSIP(管理 IP)として構 成
1/1	20.0.1.10	PIP5	SNIP/GSLB サイト IP と
-	20.0.1.11	-	して設定されています LB サーバ IP として設定
			されています。パブリック
			IP アドレスは必須ではあ
			りません

NIC	内部 IP	パブリック IP(PIP)	説明
1/2	20.0.2.10	-	モニタプローブをサービス に送信するための SNIP と して設定。パブリック IP
			は必須ではありません。

このシナリオの構成例を次に示します。VM1 と VM2 の NetScaler VPX CLI で作成された IP アドレスと初期 LB 構成を示しています。

VM1の設定例を次に示します。

1 add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
2 Add nsip 10.0.2.10 255.255.255.0
3 add service svc1 10.0.1.10 ADNS 53
4 add lb vserver v1 HTTP 10.0.1.11 80
5 add service s1 10.0.2.120 http 80
6 Add service s2 10.0.2.121 http 80
7 Bind lb vs v1 s[1-2]

VM2 の設定例を次に示します。

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]

GSLB サイトおよびその他の設定を構成する

次のトピックで説明するタスクを実行して、2つの GSLB サイトとその他の必要な設定を構成します。

Global Server Load Balancing

VM1 および VM2 での GSLB 設定の例を次に示します。

```
enable ns feature LB GSLB
1
    add gslb site site1 10.0.1.10 -publicIP PIP2
2
    add gslb site site2 20.0.1.10 -publicIP PIP5
3
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
    add gslb vserver gslb_http_vip1 HTTP
6
    bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
7
8
    bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
    bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
9
```

Azure で実行されている NetScaler VPX インスタンスに GSLB を構成しました。

障害回復

災害(さいがん)とは、自然の災害、または人為的な出来事によって引き起こされる事業機能の突然の混乱である。 災害はデータセンターの運用に影響を及ぼします。その後、災害現場で失われたリソースとデータを完全に再構築し て復元する必要があります。データ消失やデータセンターのダウンタイムは重要であり、ビジネス継続性が低下しま す。

お客様が今日直面している課題の1つは、DR サイトをどこに置くかを決めることです。企業は、基盤となるインフ ラストラクチャやネットワーク障害に関係なく、一貫性とパフォーマンスを求めています。

多くの組織がクラウドへの移行を決定している理由として考えられるのは、次のとおりです。

- オンプレミスのデータセンターを持つことは非常に高価です。クラウドを使用することで、企業は自社のシス テムを拡張する時間とリソースを解放できます。
- 自動オーケストレーションの多くは、より迅速なリカバリを可能にします
- 継続的なデータ保護や継続的なスナップショットを提供してデータを複製し、システム停止や攻撃から保護します。
- パブリッククラウドにすでに存在しているさまざまな種類のコンプライアンスやセキュリティ制御を顧客が必要とするユースケースをサポートします。これらにより、独自に構築するよりも、必要なコンプライアンスを 簡単に達成できます。

GSLB 用に構成された NetScaler ADC は、トラフィックを最も負荷の少ないデータセンターまたは最もパフォーマ ンスの高いデータセンターに転送します。この構成は、アクティブ-アクティブ設定と呼ばれ、パフォーマンスが向上 するだけでなく、セットアップの一部であるデータセンターがダウンした場合に、トラフィックを他のデータセンタ ーにルーティングすることで、ディザスタリカバリを即座に実行できます。これにより、NetScaler はお客様の貴重 な時間と費用を節約できます。

災害復旧のためのマルチ NIC マルチ IP (3 つの NIC)の導入

お客様は、セキュリティ、冗長性、可用性、容量、およびスケーラビリティが重要な本番環境に導入する場合、3つの NIC 導入を使用して導入する可能性があります。この展開方法では、複雑さと管理の容易さはユーザーにとって重大 な問題ではありません。

ディザスタリカバリ用の単一 NIC マルチ IP (1NIC) 導入

お客様は、以下の理由で非実稼働環境に導入する場合、NIC を1つにまとめて導入する可能性があります。

• テスト用の環境をセットアップするか、本番環境への導入前に新しい環境をステージングします。

- クラウドに迅速かつ効率的に直接デプロイします。
- 単一のサブネット構成のシンプルさを求めながら。

アクティブ/スタンバイの高可用性セットアップで GSLB を構成する

October 17, 2024

Azure のアクティブ/スタンバイ HA 展開には、次の 3 つの手順でグローバルサーバー負荷分散(GSLB)を構成できます。

- 1. 各 GSLB サイトで VPX HA ペアを作成します。HA ペアの作成方法については、「複数の IP アドレスと NIC を使用して高可用性セットアップを構成する 」を参照してください。
- 2. Azure Load Balancer(ALB)をフロントエンド IP アドレスと、GSLB よび DNS トラフィックを許可する 規則で構成します。

この手順には、次の下位手順が含まれています。これらの下位手順の完了に使用する PowerShell コマンドについては、このセクションのシナリオを参照してください。

a. GSLB サイトのフロントエンドIPconfigを作成します。

b. HA 内のノードの NIC 1/1 の IP アドレスを持つバックエンドアドレスプールを作成します。

c. 次のような負荷分散規則を作成します。

TCP/3009 - gslb communication
 TCP/3008 - gslb communication
 UDP/53 - DNS communication

d. バックエンドアドレスプールと手順 c で作成した LB 規則を関連付けます。

e. 両方の HA ペアのノードの NIC 1/1 のネットワークセキュリティグループを更新して、TCP 3008、TCP 3009、および UDP 53 ポートのトラフィックを許可します。

3. 各 HA ペアで GSLB を有効にします。

シナリオ

このシナリオには、2 つのサイト(Site 1 と Site 2)が含まれています。各サイトの HA ペア(HA1 と HA2)には、 複数の NIC、複数の IP アドレス、および GSLB が構成されています。

図: Azure でのアクティブ-スタンバイ HA デプロイメントでの GLSB



Region 2 (Resource Group 2)

このシナリオでは、各 VM には 3 つの NIC(NIC 0/1、1/1、1/2)が設定されています。これらの NIC は次の目的で 構成されています。

- NIC 0/1: 管理トラフィックを提供する
- NIC 1/1: クライアント側のトラフィックを提供する
- NIC 1/2: バックエンドサーバーと通信する

パラメーター設定

ALB のサンプルパラメーター設定は、次のとおりです。必要な場合は、異なる設定を使用できます。

1	<pre>\$locName="South east Asia"</pre>
3	<pre>\$rgName="MulitIP-MultiNIC-RG"</pre>
4 5	<pre>\$pubIPName4="PIPFORGSLB1"</pre>
6 7	<pre>\$domName4="vpxgslbdns"</pre>
8 9	<pre>\$lbName="MultiIPALB"</pre>
10 11	<pre>\$frontEndConfigName2="FrontEndTP2"</pre>
12	<pre>chackendDeelNeme1=UDeelcondDeelUttpU</pre>
13	
15 16	<pre>\$lbRuleName2="LBRuleGSLB1"</pre>
17 18	<pre>\$lbRuleName3="LBRuleGSLB2"</pre>
19	<pre>\$lbRuleName4="LBRuleDNS"</pre>
21	<pre>\$healthProbeName="HealthProbe"</pre>

フロントエンド IP アドレスとルールを使用して ALB を構成し、GSLB と DNS トラフィックを許可する

手順 1. 手順 1: GSLB サイト IP 用のパブリック IP を作成する

手順 3. 手順 2: LB ルールを作成し、既存の ALB を更新します。

```
1
     $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
        $rgName
2
3
     $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
4
        LoadBalancer $alb -Name $frontEndConfigName2
5
6
     $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
7
        LoadBalancer $alb -Name $backendPoolName1
8
9
     $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
10
        Name $healthProbeName
11
12
13
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
        BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
14
15
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
        BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
17
18
     \$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName4 -
19
        BackendAddressPool \$backendPool -FrontendIPConfiguration \
        $frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort
         53 -Probe \$healthprobe -EnableFloatingIP | Set-
        AzureRmLoadBalancer
```

各高可用性ペアで GSLB を有効にします

各 ALB(ALB 1 と ALB 2)で 2 つのフロントエンド IP アドレスを設定しました。1 つめの IP アドレスは LB 仮想サ ーバー、もう 1 つは GSLB サイトの IP です。

HA1には次のフロントエンド IP アドレスがあります。

- frontendiPOFalb1 (LB 仮想サーバー用)
- PIPFORGSLB1 (GSLB IP)

HA 2 には次のフロントエンド IP アドレスがあります。

- frontendiPOFALB2 (LB 仮想サーバー用)
- PIPFORGSLB2 (GSLB IP)

このシナリオでは、次のコマンドを使用します。

1	enable ns feature LB GSLB
2	
3	add service dnssvc PIPFORGSLB1 ADNS 53
4	
5	add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1
6	
7	add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8	
9	add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 - publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10	
11	add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 - publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2
12	
13	add gslb vserver gslb_http_vip1 HTTP
14	
15	bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
16	
17	bind gslb vserver gslb http vip1 -serviceName site1 gslb http svc1
18	
19	<pre>bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5</pre>

関連リソース:

NetScaler VPX インスタンスで GSLB を構成する

Global Server Load Balancing

Azure に NetScaler GSLB を展開

April 10, 2025

需要が高まる中、地域の顧客にサービスを提供するオンプレミスデータセンターを運営している企業は、Azure ク ラウドを使用して世界中に規模を拡大してデプロイしたいと考えています。NetScaler をネットワーク管理者側 で使用すると、GSLB StyleBook を使用してオンプレミスとクラウドの両方でアプリケーションを構成できます。 NetScaler ADM を使用して同じ構成をクラウドに転送できます。GSLB との距離に応じて、オンプレミスリソース とクラウドリソースのいずれかにアクセスできます。これにより、世界中のどこにいてもシームレスな体験が可能に なります。

DBSの概要

NetScaler GSLB は、クラウドロードバランサーでのドメインベースサービス(DBS)の使用をサポートしていま す。これにより、クラウドロードバランサーソリューションを使用して動的クラウドサービスを自動検出できます。 この構成により、NetScaler はアクティブ-アクティブ環境に GSLB DBS を実装できます。DBS では、DNS 検出か ら Microsoft Azure 環境のバックエンドリソースを拡張できます。このセクションでは、AzureAutoscale 環境に おける NetScaler 間の統合について説明します。

Azure ロードバランサー (ALB) を使用するドメイン名ベースのサービス

GSLB DBS は、ユーザー ALB の FQDN を使用して、Azure 内で作成および削除されるバックエンド サーバーが含 まれるように GSLB サービス グループを動的に更新します。この機能を設定するには、ユーザーは NetScaler を ALB にポイントして、Azure 内のさまざまなサーバーに動的にルーティングします。これは、Azure 内でインスタ ンスが作成および削除されるたびに NetScaler を手動で更新しなくても実行できます。GSLB サービス グループの Citrix ADC DBS 機能は、DNS 対応のサービス検出を使用して、Autoscale グループで識別された DBS 名前空間の メンバー サービス リソースを決定します。

次の図は、クラウド ロード バランサーを備えた NetScaler GSLB DBS Autoscale コンポーネントを示していま す。



Azure GSLB の前提条件

NetScaler GSLB サービス グループの前提条件には、機能している Microsoft Azure 環境に加えて、Linux Web サーバー、Azure 内の NetScaler アプライアンス、パブリック IP アドレス、Azure ロード バランサー (ALB) を構 成するための知識と能力が含まれます。

- GSLB DBS サービスの統合には、Microsoft Azure ロードバランサーインスタンス用の NetScaler バージョン 12.0.57 が必要です。
- GSLB サービスグループエンティティ:NetScaler バージョン 12.0.57
- DBS 動的検出を使用した自動スケーリングをサポートする GSLB サービスグループが導入されました。
- DBS 機能コンポーネント (ドメインベースのサービス) は GSLB サービスグループにバインドする必要があり ます。

例:

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 コンポーネントの設定

- 1. ユーザー Azure Portal にログインし、NetScaler テンプレートから新しい仮想マシンを作成します。
- 2. Azure Load Balancer を作成します。

\equiv Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)
Home > Create a resource > Marketplac	ce > Load Balancer >	
Create load balancer		
	oackena hoois impound raies o	ninnnin i niez i i i i i i i i i i i i i i i i i i
Azure load balancer is a layer 4 load balanc balancers uses a hash-based distribution al destination port, protocol type) hash to ma accessible via public IP addresses, or intern Network Address Translation (NAT) to route	er that distributes incoming traffic among gorithm. By default, it uses a 5-tuple (sour p traffic to available servers. Load balance al 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 *		×
Resource group *	Create new	\vee
Instance details		
Name *	ALB	~
Region *	East US 2	~
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. 作成した NetScaler バックエンドプールを追加します。

Home > tahaj-test > ALB	÷ …						
Load balancer	2						
₽ Search «	+ Add 💍 Refresh						
Overview							
Activity log	The local section without sectors	and address in a balances. The basis of		han			
Access control (IAM)	serve traffic for a given load-balancing	rule. Learn more. d'	r poor dennes the group of resources t	nat will			
Tags	P						
X Diagnose and solve problems							
Settings	Backend pool	Resource Name	IP address	Network interface	Availability zone	Rules count	Resource Status
Frontend IP configuration							
Backend pools							
Health probes							
Ecoad balancing rules							
Inbound NAT rules							
II Properties							
Locks							
Monitoring							
Insights							
Diagnostic settings							
🧬 Logs							
💵 Alerts							
m Metrics							

4. ポート 80 のヘルスプローブを作成します。

ロード バランサーから作成されたフロントエンド IP を使用して、負荷分散ルールを作成します。

- プロトコル:TCP
- バックエンドポート:80
- バックエンドプール: 手順1 で作成した NetScaler
- ヘルスプローブ:ステップ4で作成
- セッションの永続性:なし

\equiv Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)	
Home > tahaj-test > ALB Load bala	ncing rules >		
Add load balancing ru	le ···		
A load balancing rule distributes incoming backend pool instances. Only backend ins	g traffic that is sent to a selected IP address a tances that the health probe considers health	nd port combination across a group of ny receive new traffic.	
Name *	lb_rule2		
IP Version *	IPv4		
	O IPv6		
Frontend IP address * 🛈	frontend_ip (10.1.0.7)	~	
Backend pool * (i)	backend_pool		
High availability ports 🛈			
Protocol	● тср		
	O UDP		
Port *	80		
Backend port * 🕡	80		
Health probe * 🕡	Select an existing probe	\sim	
	Create new		
Session persistence 🕕	None	~	
Idle timeout (minutes) * 🛈	4		
Enable TCP Reset			
Enable Floating IP 🕕			

Save Cancel

NetScaler GSLB ドメインベースのサービスの設定

次の構成は、GSLB 対応環境で ADC を自動スケーリングするためのドメインベースのサービスを有効にするために 必要なものをまとめたものです。

- トラフィック管理の設定
- GSLB 構成

トラフィック管理の設定

注

DBS サービス グループの ALB ドメインを解決するネーム サーバーまたは DNS 仮想サーバーのいずれかを 使用して NetScaler を構成する必要があります。ネーム サーバーまたは DNS 仮想サーバーの詳細について は、「DNS nameServer」を参照してください。

- 1. [トラフィック管理]>[負荷分散]>[サーバー]に移動します。
- 2. [追加] をクリックしてサーバーを作成し、ALB の Azure の A レコード (ドメイン名) に対応する名前と FQDN を指定します。

← 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		
C Enable after Creating		
Query Type		
~	*	
Comments		

3. 手順2を繰り返して、Azureの2番目のリソースから2番目のALBを追加します。

GSLB 構成

- 1. GSLB サイトを構成するには、[追加] をクリックします。
- 2. GSLB サイトを構成するための詳細を指定します。

サイトに名前を付けます。タイプは、サイトを構成する NetScaler に基づいてリモートまたはローカルとし て構成されます。サイト IP アドレスは GSLB サイトの IP アドレスです。GSLB サイトは、この IP アドレス を使用して他の GSLB サイトと通信します。パブリック IP アドレスは、特定の IP アドレスが外部のファイア ウォールまたは NAT デバイスでホストされているクラウドサービスを使用する場合に必要です。サイトを親 サイトとして構成し、トリガー モニター が 常にに設定されていることを確認します。 また、下部 にある [メトリック交換]、[ネットワークメトリック交換]、および [** パーシスタンスセッションエントリ交 換 **] の 3 つのボックスを必ずオンにしてください。

トリガーモニターを **MEPDOWN** に設定することをお勧めします。詳細については、「GSLB サービス グループの構成」を参照してください。

← 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. 作成をクリックします。
- 4. [トラフィック管理] > [GSLB] > [サービスグループ] に移動します。
- 5. [追加]をクリックしてサービスグループを追加します。
- 6. 詳細を指定してサービスグループを設定します

サービスグループに名前を付け、HTTP プロトコルを使用します。[サイト名]で、作成した各サイトを選択します。必ず自動スケールモードを DNS として設定し、状態およびヘルスモニタリングのチェックボックスをオフにします。**OK** をクリックしてサービスグループを作成します。

← GSLB Service Group

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

 [サービスグループメンバー]をクリックし、[サーバーベース]を選択します。実行ガイドの開始時に構成され たそれぞれの ALBを選択します。トラフィックがポート 80 を通過するように設定します。作成をクリックし ます。

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

サービス グループ メンバー バインディングには、ALB から受信した 2 つのインスタンスが入力されます。

GSLB S	ervicegroup Memb	per Binding								×
Add	Edit Unbind	Monitor Details	No action 🗸							
${\sf Q}$ Click here	to search or you can enter Ke	ay : Value format								0
	IP ADDRESS	SERVER NAME	PORT	WEIGHT \$	ORDER	HASH ID	STATE	SERVICE STATE	SITE PREFIX	
	10.100.234.12	10.100.234.12	80	1			 ENABLED	UP		
	54.252.154.72	elb-nvirginia	80	1	1		 ENABLED	UP		
Close										

- 8. 手順5と6を繰り返して、Azureの2番目のリソースの場所のサービス グループを構成します。(これは同じ NetScaler GUI から実行できます)。
- 9. GSLB 仮想サーバーをセットアップします。[トラフィック管理]>[GSLB]>[仮想サーバー]に移動します。
- 10. [追加] をクリックして仮想サーバーを作成します。
- 11. 詳細を指定して GSLB 仮想サーバーを構成します。

サーバーの名前を指定し、DNS レコードタイプが A に設定され、サービスタイプが HTTP に設定され、

AppFlow ロギングの作成後に有効にするチェックボックスをオンにします。**OK** をクリックして GSLB 仮想 サーバーを作成します。

← 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. GSLB 仮想サーバーを作成したら、「**GSLB** 仮想サーバーサービスグループバインディングなし」をクリックします。
 - ← 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 ODOWN	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.「サービスグループバインディング」で、「サービスグループ名の選択」を使用して、前のステップで作成した サービスグループを選択して追加します。

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

14. GSLB 仮想サーバードメインバインディングを設定するには、「**GSLB** 仮想サーバードメインバインディング なし」をクリックします。FQDN とバインドを設定します。他のパラメータについてはデフォルト設定を保持 します。

Domain	Binding
Domain	Diffulling

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

- 15. [サービスなし] をクリックして ADNS サービスを設定します。
- 16. 詳細を指定して負荷分散サービスを設定します。

サービス名を追加し、[新規サーバー] をクリックして、ADNS サーバーの **IP** アドレスを入力します。ユーザ ADNS がすでに設定されている場合、ユーザは [既存のサーバ] を選択し、ドロップダウンメニューからユーザ ADNS を選択できます。プロトコルが ADNS で、トラフィックがポート 53 を経由するように設定されている ことを確認します。

← Load Balancing Service

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

- 17. 方法を [最小接続] に、[バックアップ方法] を [ラウンドロビン] に設定します。
- 18.「完了」をクリックし、ユーザーの GSLB 仮想サーバーが「Up」と表示されていることを確認します。

 Search in Mercu 		Tuffic Management / 43	A / Kital Virtual Senses			
ANS	>	GSLB Virtual S	ervers.			0 😭
Syttem		Greb Threads				
Appliquet	>	Add 5.00	Oriete Statistics No action	~		Search 🛩
Tuffic Management	\vee	B Name	Refe	Peteral	S. Haaddh	
Load Balancing	>	14 COD	• UP	1079	100.00% # UP/0 DOWN	
Content Switching	• •					
Cache Redirection						
0%5						
651.8	~					
Gauhtstand						
 Virtual Servers 						
Services						

そのほかの参照先

ハイブリッドおよびマルチクラウド環境向けの NetScaler グローバル負荷分散

NetScaler Web App Firewall & Azure にデプロイする

October 17, 2024

NetScaler Web App Firewall は、最新のアプリケーションに最先端の保護を提供するエンタープライズグレード のソリューションです。NetScaler Web App Firewall は、Web サイト、Web アプリケーション、API などの一 般公開資産に対する脅威を軽減します。NetScaler Web App Firewall には、IP レピュテーションベースのフィル タリング、ボット対策、OWASP トップ 10 アプリケーション脅威対策、レイヤー 7 DDoS 保護などが含まれてい ます。また、認証を強制するオプション、強力な SSL/TLS 暗号、TLS 1.3、レート制限、および書き換えポリシー も含まれています。NetScaler Web App Firewall は、基本的な WAF 保護と高度な WAF 保護の両方を使用して、 比類のない使いやすさでアプリケーションを包括的に保護します。起動して実行するのはほんの数分です。さらに、 NetScaler Web App Firewall は動的プロファイリングと呼ばれる自動学習モデルを使用することで、ユーザーの 貴重な時間を節約できます。NetScaler Web App Firewall は、保護対象アプリケーションの動作を自動的に学習す ることで、開発者がアプリケーションを展開したり変更したりしても、アプリケーションに適応します。NetScaler Web App Firewall は、PCI-DSS、HIPAA などを含むすべての主要な規制基準や機関へのコンプライアンスに役立 ちます。CloudFormation テンプレートを使えば、これまでになく簡単に立ち上げてすぐに実行できます。Auto Scaling を使用すると、トラフィックが拡大しても、ユーザーはアプリケーションを保護したまま安心できます。

NetScaler Web App Firewall は、顧客サーバーと顧客ユーザー間のレイヤー3ネットワークデバイスまたはレイ ヤー2ネットワークブリッジとして、通常は顧客企業のルーターまたはファイアウォールの背後に設置できます。詳 細については、「NetScaler Web App Firewall の概要」を参照してください。

NetScaler Web App Firewall 導入戦略

- Web アプリケーションファイアウォールの導入は、どのアプリケーションや特定のデータを最大限のセキュ リティ保護が必要か、どのアプリケーションが脆弱性が低く、どのアプリケーションまたは特定のデータがセ キュリティ検査を安全に回避できるかを評価することです。これにより、ユーザーは最適な構成を考案し、ト ラフィックを分離するための適切なポリシーとバインドポイントを設計できます。たとえば、ユーザーは、画 像、MP3 ファイル、ムービーなどの静的な Web コンテンツに対する要求のセキュリティ検査をバイパスする ポリシーを構成し、動的コンテンツのリクエストに高度なセキュリティチェックを適用する別のポリシーを構 成することができます。ユーザーは複数のポリシーとプロファイルを使用して、同じアプリケーションの異な るコンテンツを保護できます。
- 2. 導入のベースラインとなるには、仮想サーバーを作成し、そのサーバーを通過するトラフィックをテストして、 ユーザーシステムを流れるトラフィックの速度と量を把握します。
- 3. Web アプリケーションファイアウォールを展開します。NetScaler ADM と Web アプリケーション ファイ アウォール スタイルブックを使用して、Web アプリケーション ファイアウォールを構成します。詳細につい ては、このガイドの下の「StyleBook」セクションを参照してください。
- 4. NetScaler Web App Firewall と OWASP トップテンを実装します。

Web Application Firewall の 3 つの保護は、一般的な種類の Web 攻撃に対して特に効果的であるため、他のどの 保護よりも一般的に使用されています。したがって、これらは初期展開時に実装する必要があります。これには、次 の種類のアカウントがあります。

- HTML クロスサイトスクリプティング:スクリプトが配置されている Web サイトとは異なる Web サイトの コンテンツにアクセスまたは変更しようとするスクリプトのリクエストとレスポンスを調べます。このチェッ クは、このようなスクリプトを検出すると、要求または応答を宛先に転送する前にスクリプトを無害にするか、 接続をブロックします。
- HTML SQL インジェクション: フォームフィールドデータを含むリクエストに SQL コマンドを SQL データ ベースに挿入しようとしていないかを調べます。このチェックは、挿入された SQL コードを検出すると、要 求をブロックするか、または Web サーバーに要求を転送する前に、挿入された SQL コードを無害にします。

注

構成に次の条件が適用されるように Web App Firewall が正しく構成されていることを確認してください。

- ユーザーが HTML クロスサイト スクリプティング チェックまたは HTML SQL インジェクション チェ ック (あるいはその両方) を有効にした場合。
- ユーザー保護された Web サイトでは、ファイルのアップロードが受け入れられたり、大きな POST 本文 データを含む Web フォームが含まれたりします。

このケースを処理するための Web アプリケーション ファイアウォールの構成の詳細については、「アプリケーショ ン ファイアウォールの構成: Web アプリケーション ファイアウォールの構成」を参照してください。

バッファオーバーフロー: リクエストを調べて、Web サーバーでバッファオーバーフローを引き起こそうとする試みを検出します。

Web アプリケーションファイアウォールの設定

NetScaler Web App Firewall がすでに有効になっていて、正しく機能していることを確認します。Web アプリケ ーションファイアウォールスタイルブックを使用して NetScaler Web App Firewall を構成することをお勧めしま す。ほとんどのユーザーは、これが Web アプリケーションファイアウォールを構成する最も簡単な方法であり、間 違いを防ぐように設計されています。GUI とコマンドラインインターフェースはどちらも、主に既存の構成を変更し たり、詳細オプションを使用したりする経験のあるユーザーを対象としています。

SQL インジェクション

NetScaler Web App Firewall HTML SQL インジェクションチェックは、ユーザーアプリケーションのセキュリ ティを侵害する可能性のある不正な SQL コードの注入に対する特別な防御策を提供します。NetScaler Web App Firewall は、1) POST 本文、2) ヘッダー、3) クッキーの 3 つの場所で、注入された SQL コードのリクエストペイ ロードを調べます。詳細については、HTML SQL インジェクション チェックを参照してください。 クロスサイトスクリプティング

HTML クロスサイトスクリプティング(クロスサイトスクリプティング)チェックでは、クロスサイトスクリプティ ング攻撃の可能性がないか、ユーザー要求のヘッダーと POST ボディの両方を調べます。クロスサイトスクリプトが 見つかった場合は、攻撃を無害化するようにリクエストを変更(変換)するか、リクエストをブロックします。詳細 については、HTML クロスサイト スクリプティング チェックを参照してください。

バッファオーバーフローチェック

バッファオーバーフローチェックは、Web サーバ上でバッファオーバーフローを引き起こす試みを検出します。 Web アプリケーションファイアウォールが URL、Cookie、またはヘッダーが設定された長さよりも長いことを検出 すると、バッファオーバーフローを引き起こす可能性があるため、要求をブロックします。詳細については、バッフ ァオーバーフロー チェックを参照してください。

仮想パッチ/署名

シグネチャは、既知の攻撃からユーザーの Web サイトを保護するタスクを簡略化するために、特定の設定可能なル ールを提供します。シグニチャは、オペレーティングシステム、Web サーバー、Web サイト、XML ベースの Web サービス、またはその他のリソースに対する既知の攻撃のコンポーネントであるパターンを表します。事前設定され た豊富な組み込みルールやネイティブルールは、パターンマッチングの力を利用して攻撃を検出し、アプリケーショ ンの脆弱性から保護する、使いやすいセキュリティソリューションを提供します。詳細については、「署名」を参照し てください。

NetScaler Web App Firewall は、署名の自動更新と手動更新の両方をサポートしています。また、署名の自動更新 を有効にして最新の状態に保つことをお勧めします。署名を最新の状態に保つために、自動更新 を有効にすることを お勧めします。



Automatic signatures updates

これらの署名ファイルは AWS 環境でホストされているため、最新の署名ファイルを取得するには、ネットワークフ ァイアウォールから NetScaler IP アドレスへのアウトバウンドアクセスを許可することが重要です。リアルタイム トラフィックの処理中に NetScaler の署名を更新しても影響はありません。

アプリケーション・セキュリティ分析

アプリケーションセキュリティダッシュボードは、ユーザーアプリケーションのセキュリティ状態の全体像を提供し ます。たとえば、セキュリティ違反、署名違反、脅威インデックスなどの主要なセキュリティメトリックが表示され ます。アプリケーションセキュリティダッシュボードには、検出された NetScaler の syn 攻撃、スモールウィンド ウ攻撃、DNS フラッド攻撃などの攻撃関連情報も表示されます。

注

アプリケーションセキュリティダッシュボードのメトリックを表示するには、ユーザーが監視したい NetScaler インスタンスで AppFlow for Security Insight を有効にする必要があります。

アプリケーションセキュリティダッシュボードで NetScaler インスタンスのセキュリティメトリックを表示するに は:

- 1. 管理者の資格情報を使用して NetScaler ADM にログインします。
- 2. [アプリケーション] > [App Security Dashboard] に移動し、[デバイス] リストからインスタンスの IP ア ドレスを選択します。

ユーザーは、グラフにプロットされたバブルをクリックすることで、Application Security Investigator で報告さ れた不一致をさらに掘り下げることができます。

ADM での集中型学習

NetScaler Web App Firewall は、SQL インジェクションやクロスサイトスクリプティング(XSS)などの悪意の ある攻撃からユーザーの Web アプリケーションを保護します。データ侵害を防ぎ、適切なセキュリティ保護を提供 するために、ユーザーはトラフィックの脅威を監視し、攻撃に関する実用的なデータをリアルタイムで監視する必要 があります。報告された攻撃は誤検知であり、例外として提供する必要がある場合があります。

NetScaler ADM の集中学習は、WAF がユーザーの Web アプリケーションの動作 (通常のアクティビティ) を学習 できるようにする繰り返しパターン フィルターです。エンジンは、モニタリングに基づいて、HTTP トラフィックに 適用されるセキュリティチェックごとに推奨されるルールまたは例外のリストを生成します。

必要な緩和として手動で展開するよりも、学習エンジンを使用して緩和ルールを展開する方がはるかに簡単です。

学習機能を展開するには、ユーザーは最初にユーザー NetScaler で Web アプリケーションファイアウォールプロフ ァイル(セキュリティ設定セット)を構成する必要があります。詳細については、「Web アプリケーション ファイア ウォール プロファイルの作成」を参照してください。

NetScaler ADM は、セキュリティ チェックごとに例外 (緩和) のリストを生成します。管理者は、NetScaler ADM で例外のリストを確認し、展開するかスキップするかを決定できます。

NetScaler ADM の WAF 学習機能を使用すると、次のことが可能になります。

- 次のセキュリティチェックを使用して学習プロファイルを設定します。
 - バッファオーバーフロー
 - HTML クロスサイトスクリプティング

注

```
クロスサイトスクリプトの場所の制限は FormField のみです。
- HTML SQL インジェクション
```

```
    **注**
    >
    HTML SQLインジェクションチェックを行うには、 ユーザーがNetScaler
で`set -sqlinjectionTransformSpecialChars ON`と`set -
sqlinjectiontype sqlspclcharorkeywords`を構成する必要がありま
す。
```

- NetScaler ADM の緩和ルールを確認し、必要なアクション (展開またはスキップ) を実行するかどうかを決定 します。
- メール、Slack、ServiceNow を通じて通知を受け取ることができます。
- ダッシュボードを使用してリラクゼーションの詳細を表示します。

NetScaler ADM で WAF 学習を使用するには:

- 1. 学習プロファイルを設定します: 学習プロファイルを設定します
- 2. リラクゼーションルールを参照してください: リラクゼーションルールとアイドルルールを表示
- 3. WAF ラーニングダッシュボードを使用する: WAF ラーニングダッシュボードを表示する

StyleBooks

StyleBooks は、ユーザーアプリケーションの複雑な NetScaler 構成を管理するタスクを簡素化します。StyleBook は、ユーザーが NetScaler 構成を作成および管理するために使用できるテンプレートです。ここでは、ユーザーは主 に Web アプリケーションファイアウォールの展開に使用される StyleBook に関心があります。StyleBook につい て詳しくは、「StyleBook」を参照してください。

セキュリティインサイト分析

インターネットに接続している Web アプリケーションや Web サービスアプリケーションの攻撃に対する脆弱性が 高まってきています。アプリケーションを攻撃から保護するために、ユーザーは過去、現在、差し迫った脅威の性質 と範囲、攻撃に関するリアルタイムの実用的なデータ、および対策に関する推奨事項を可視化する必要があります。 Security Insight は、ユーザーがユーザーアプリケーションのセキュリティ状態を評価し、ユーザーアプリケーショ ンを保護するための是正措置を講じるのに役立つ、単一ペインのソリューションを提供します。詳細については、「 セキュリティインサイト」を参照してください。詳細については、セキュリティ インサイトを参照してください。 セキュリティ侵害に関する詳細情報の取得

ユーザーは、アプリケーションに対する攻撃のリストを表示し、攻撃の種類と重大度、ADC インスタンスによって実 行されたアクション、要求されたリソース、および攻撃元に関する洞察を得ることができます。

たとえば、ユーザーは、ブロックされた Microsoft Lync に対する攻撃の数、要求されたリソース、および送信元の IP アドレスを特定したい場合があります。

Security Insight ダッシュボードで、[Lync]>[合計違反数]をクリックします。テーブルで、[実行されたアクション]列見出しのフィルタアイコンをクリックし、[ブロック]を選択します。

b	application	Summary									
					Action Taken	Q.				Sear	
	Security Check Violation	Severity 🖓	Wederlass Category 🖓	Artist Taken	Backed Not Backed Touched		Location	Signature Violation	Violation Name	Violation Video	
	Set UR.	Critical	Breken Authentication and Section Management	Buched		wi/Real/Linked					
	Set URL	Citical	Distan Authentication and Sesion Management	Doded		uri/Real/Linded					
	Set URL	Critical	Brites Authentication and Sector Management	Docked	Mp.(10.10.41.6	Curr/RestCitional					
	Sec URL	Critical	Brites Authentication and Sector Management	Doctored	Mp.(10.10.414)	(w//Testil.Nev)					
8	Sec URL	Critical	Brites Authentication and Section Management	Docted	Mp/70.12.616	Ver/TextUnited					
8	Set URL	Critical	Brites Authentication and Section Management	Docted	Mp.(10.12.618)	/wi/featl.html					
	3md 10%	Critical	Bottes Authentication and Sectors Menagement	Doctord	Mp.(10.10.41.6	Var/Teal? Med					
8	Sec URL	Critical	Brites Authentication and Section Management	Disting	Mp/70.10.41.6	Ver/TextD Mont					
8	Sec URL	Citical	Broten Authentication and Section Management	Disched	Mp.(10.12.618	/wither to have					
	2mm (197)	Critical	Broken Authentication and Section Management	Ducked	Mp.(10.10.43.6	/wi/teatlined					
	Sec URL	Citical	Broten Authentication and Sector Management	Buched	Mp.(10.10.41.6	/wr/teal/1.html					
	1000	Called	Busines & attentionation and Service Microsomers	Sec. And	And the second second second	the state of the second					

要求されたリソースについては、[URL] 列を確認してください。攻撃元については、「Client IP 」列を参照 してく ださい。

ログ式の詳細を表示する

NetScaler は、アプリケーションファイアウォールプロファイルで構成されたログ式を使用して、ユーザーエンター プライズ内のアプリケーションに対する攻撃に対処します。Security Insight では、ユーザーは ADC インスタン スが使用するログ式に対して返された値を表示できます。これらの値には、要求ヘッダー、要求本文などがあります。 ログ式の値に加えて、ユーザーは、ADC インスタンスが攻撃のアクションを実行するために使用したアプリケーショ ンファイアウォールプロファイルで定義されたログ式の名前とコメントを表示することもできます。

前提条件:

ユーザーが以下を行うことを確認します。

- アプリケーションファイアウォールプロファイルでログ式を設定します。詳しくは、「アプリケーションファ イアウォール」を参照してください。
- NetScaler ADM でログ式ベースのセキュリティインサイト設定を有効にします。以下を実行します:
 - [分析] > [設定] に移動し、[分析の機能を有効にする] をクリックします。
 - 「分析の機能を有効にする」ページで、「** ログ式ベースの Security Insight 設定」セクションで 「Security Insight を有効にする」を選択し、「OK」** をクリックします。



たとえば、ユーザーエンタープライズ内の Microsoft Lync への攻撃に対して実行したアクションについて、ADC イ ンスタンスから返されたログ式の値を表示したい場合があります。

Security Insight ダッシュボードで、[**Lync**]>[合計違反数]に移動します。[アプリケーションサマリ] テーブル で、URL をクリックして、[違反情報] ページに、ログ式の名前、コメント、アクションの ADC インスタンスによっ て返された値など、違反の完全な詳細を表示します。

Cateway Insight	Violation Inform	ation				×
			Violation	Informatio	n	
	Attack Time	NA				
	Signature Violation					
	Violation Name					
	Violation value					
	Security Check Violation	Start U	/RL			
	Violation Catogory	Broker	Authentication and Session Ma	nagement		
	Threat Indias	5				
	Severity	Mediu	m			
	Action Taken	Blacke	4			
	UNL	Mapov	10.142.40.245/csrf_ft/ft///wwf	field1-asifasal		
	Pound in	Other	Location			
	Clentip	10.502	63.79			
	Location	Bangar	ane			
	104170300	*				
	Log Expression Name		Log Expression Comment	Log Depressi	ios Value	
	L6D/P97		http request contains keyword	false		
	LGEXPRB		to request contains header	faise		
	LSEXPRE		http:method.expression	GET /GMT_MG User-Agent: 0 OpenSiL/03 Hext: 33.102 Accept: 1/1	/ffc/ten//feldi-setaol HTTP/1.1 ourl/7.19-7 (x86, 64-pc-lmux-gmu) lbcurl/7.19.7 Uk z86/1.2.1.3 lbider/1.15 60.245	
	LGD/PR0		http method expression	true		
	LSEXPRE		http request contains header			
	LSEXPRE		http:request:header.contains-u seragent	0/17/15/7 0/ 2/0/12/33 R	86_54-ac-linux-gnul Ibcurl/7.19.7 Open55L/19.8k bidh/1.15	
	LGD/PR2		http method expression	faite		
	LGDXPRS		htp method expression			
	NA 10.102	63.79	Start URL	Medium	Broken Authentication and Section Manageme	ere .

構成を展開する前に安全指数を決定してください。セキュリティ違反は、ユーザーがセキュリティ構成を ADC イン スタンスに展開した後に発生しますが、ユーザーはセキュリティ構成を展開する前にその有効性を評価したい場合が あります。

たとえば、ユーザーは、IP アドレスが 10.102.60.27 の ADC インスタンス上の SAP アプリケーションの構成の安全 性指標を評価したい場合があります。

Security Insight ダッシュボードの [デバイス] で、ユーザーが設定した ADC インスタンスの IP アドレスをクリ ックします。ユーザーは、脅威インデックスと攻撃の総数の両方が 0 であることがわかります。脅威インデックスは、 アプリケーションに対する攻撃の数と種類を直接反映しています。攻撃回数がゼロということは、アプリケーション がまったく脅威にさらされていないことを示しています。

8	10w		1 February 2016 10:20:05-21	Workey 2016 1320-25				
0v	erview piotiens have higher ant Application has in	e Three Inde	n & Lewest Safety Index Attacks		NPL of Lysten Security of 10, 10	10.71 Dever in New Compliant		
A	pplications						48 for	87
				Thread Index	Tabley Index	Total Atlantic	Devices	
	Lyne			Level 4	Level 2	49/22	10.000.00.07	
	Sap			Level 0	Level 3		Threat Index	
	Outlook			Level a	Level &	•	AB High Madata	
	SharePoint .			boot a	Level 4		Low Safety Index	-

Sap > 安全性指数 >SAP_Profile** をクリックし、表示される安全性指標情報を評価します。

Application Summary							
Total Victoriess	Total Violations Violations Ry Severity Violations Ry Action Violations Ry Catego 5534 Critical 5846 Blocked 5846 Cross also Scripting						
These loads (cont 6 🙆 Saliday balan	- Level 2 🙆						
aloty Index Summary							
Application Firms Signatures: 1295/1300 No Security Check: 1/14 No	il Configuration A Configured A Configured	System Se 6/10 Not	configured				
Application Finnese Configuration	Name	Sufuty Balance					
Level 2	tag. Postar	,					
NotScalor System Security Level 2							

アプリケーションファイアウォールの概要では、ユーザーはさまざまな保護設定の構成ステータスを表示できます。 ログを記録する設定になっている場合や、構成されていない設定がある場合は、アプリケーションに割り当てられる 安全性指数は低くなります。

Security Check	Latvet B	Signatures Hubblen	Love 1
	Backed (3) Ref Backed (1) Challed (1)		Binded(0) RecEnd(0) Solution(1) Solution(1)
Production		Configuration Status	
XNR, Variabelian		Not Configurati	
		And the second sec	
INE SOAP Fault		Next Contrappened	
INA, SOAF Fault		Rect Configuration	
104, SSAF Fealt 204, Milalineari 204, 105		Rest Configured Rest Configured	

セキュリティ違反

インターネットに公開されている Web アプリケーションは、攻撃に対して非常に脆弱になっています。NetScaler ADM を使用すると、アクション可能な違反の詳細を視覚化し、アプリケーションを攻撃から保護できます。

アプリケーションのセキュリティ違反の詳細を表示する

インターネットに公開されている Web アプリケーションは、攻撃に対して非常に脆弱になっています。NetScaler ADM を使用すると、ユーザーは実行可能な違反の詳細を視覚化して、アプリケーションを攻撃から保護できます。「セ キュリティ」> 「** セキュリティ違反 **」に 移動すると、単一ペインのソリューションで次のことが可能になりま す:

- ネットワーク、ボット、WAF などのカテゴリに基づいてアプリケーションセキュリティ違反にアクセスする
- アプリケーションを保護するための是正措置を講じる

NetScaler ADM でセキュリティ違反を表示するには、次の点を確認します。

- ユーザーは NetScaler のプレミアムライセンス(WAF および BOT 違反用)を持っています。
- ユーザーは、負荷分散またはコンテンツスイッチ仮想サーバー(WAF および BOT 用)のライセンスを申請しました。詳細については、「仮想サーバーのライセンスの管理」を参照してください。
- ユーザーはより多くの設定を有効にできます。詳しくは、NetScaler 製品ドキュメントの「セットアップ」セクション「セットアップ」に記載されている手順を参照してください。

違反カテゴリ

NetScaler ADM を使用すると、ユーザーは すべての違反で利用可能な違反を表示できます。

設定する

違反については、メトリクスコレクターが有効になっているか どうか を確認してください。デフォルトでは、 NetScaler の メトリックコレクターは有効になっています。詳細については、「インテリジェント アプリ分析を構 成する」を参照してください。

高度なセキュリティ分析を有効にする

- [ネットワーク]>[インスタンス]>[NetScaler]に移動し、インスタンスタイプを選択します。たとえば、 MPX。
- NetScaler インスタンスを選択し、[アクションの選択] リストから [分析の設定] を選択 します。
- 仮想サーバーを選択し、「アナリティクスを有効にする」をクリックします。
- [アナリティクスを有効にする] ウィンドウで:
 - 「**Web** インサイト」を選択 します。ユーザーが Web Insight を選択すると、読み取り専用の [高度なセ キュリティ分析] オプションが自動的に有効になります。

注 高度なセキュリティ分析 オプションは、プレミアムライセンスの ADC インスタンスにのみ表示されま す。

- トランスポートモードとして Logstream を選択します。
- 式はデフォルトで true です
- OK をクリック

Enable Analytics	×
Selected Virtual Server - Load Balancing: 1	
V Web Insight	
Client Side Measurement	
Security Insight	
Bot Insight	
Advanced Security Analytics	
Advanced Options	
For ADC version less than 12.0 IPFIX is default Transport mode.	
Transport Mode	
Logstream IPFIX	
Instance level options	
Enable HTTP X-Forwarded-For	
Citrix Gateway	
Expression Configuration	
OK Close	

ウェブトランザクション設定を有効にする

• [アナリティクス] >[設定] に 移動します。

「設定」ページが表示されます。

- •「アナリティクスの機能を有効にする」をクリックします。
- [Web トランザクション設定] で、[すべて] を選択します。

 Enable Features for Analytics
Multing Tatlaga
Enable the Webback backward I he release deployment has more than one Obin ASC appliance to Obin Sateway appliance between a single direct and unner connection. Obin ASM analyses the number of hops for Obin-Sateway appliances through which the Obin connections and on the object of the obin Sateway appliances through which the Obin connections and on the object of the obin Sateway appliances through which the Obin connections and on the object of
C Sodk Willow
13 indukt betilings
Enable the VP insigh feature of Disk ADM's provide an easy and solidate solidar for monitoring the metrics of the optimization techniques and congestion control strategies for algorithmal and in Disk ADI appliances to avoid meteoric in data featurestics.
C fould KP holps
Bith traight Settings
Enable the Web major function to allow Cells HOM is instance the performance reports of web applications (sublimation) and anter anti-holing and anterest adulting and anterest (but at function the Cells KKK. Web traight enables citability into entroping and action of anterestation is mention and web applications being towards performance reports and allows if CEL statistic web include.
Rob Transactions furthings
Enable Web Transaction Nature to allow Cells RMM to ordine Web transaction From Cells RML
Eadline Web Spreachants
Avenuitue Trans
Incurity insights Lettings
Endbit Log Domains based locarity insides to report to export to provide data configured with Application Freewall profile. This will help use to use desilied tog advect electrics.
ÓM Dinne

• [**OK**] をクリック します。
セキュリティ違反ダッシュボード

セキュリティ違反ダッシュボードでは、ユーザーは以下を表示できます。

 すべての NetScaler とアプリケーションで発生した違反の合計数。違反の合計は、選択した期間に基づいて 表示されます。

Security Wolations	61/91/3012 60:00:00	- 2000 V

• 各カテゴリの下での違反の合計数。

Network	Bot	WAF
No violations detected	52K violations	55 violations

• 影響を受けた ADC の合計、影響を受けたアプリケーションの合計、および影響を受けたアプリケーションの 合計数に基づいて、上位レベルの違反数が表示されます。

5 7	
Top Violations Text on the earliest of increases and the affinish applications COUNT 	Collection (2017) 507 Violations Sectors Chemistry Chemi

違反の詳細については、「すべての違反」を参照してください。

ボットの洞察

NetScaler でボットインサイトを設定します。詳細については、「Bot」を参照してください。

ボットを表示

仮想サーバーをクリックして、アプリケーションの概要を表示します



- 1. 次のようなアプリケーション概要の詳細を提供します。
 - ・ 平均 RPS –仮想サーバーで受信した1秒あたりの平均ボットトランザクションリクエスト (RPS) を示します。
 - 重要度別のボット—重大度に基づいて発生したボットトランザクションの数が最も多かったことを示します。重要度は、「緊急」、「高」、「中」、「低」に基づいて分類されます。

たとえば、仮想サーバーに重大度の高いボットが 11770 個、重大度が重大なボットが 1550 個ある場合、 NetScaler ADM は、重大度別のボットの下に 重大 **1.55 K** を表示します。

• 最大のボットカテゴリ —ボットカテゴリに基づいて発生したボット攻撃の数が最も多いことを示します。

たとえば、仮想サーバーにブロックリストに登録されたボットが 8000 個、許可リストに登録されたボットが 5000 個、レート制限を超えたボットが 10000 個ある場合、NetScaler ADM は「最大ボット カテゴリ」の下 に「レート制限を超えました **10 K**」と表示します。

• 最大のジオソース —地域に基づいて発生したボット攻撃の数が最も多いことを示します。

たとえば、仮想サーバーでサンタクララに 5000 件のボット攻撃、ロンドンに 7000 件のボット攻撃、バンガ ロールに 9000 件のボット攻撃が発生した場合、NetScaler ADM は「最大のジオソース」の下に「バンガロ ール **9 K**」と表示します。

• 平均ボットトラフィック%一人間のボット比率を示します。

- 2. マップビュー内の場所に基づいてボット攻撃の重大度を表示します
- 3. ボット攻撃の種類(「良好」、「悪い」、「すべて」)を表示します
- 4. ボット攻撃の合計数と、対応する構成されたアクションを表示します。たとえば、次の設定があるとします。
 - IP アドレスの範囲 (192.140.14.9 ~192.140.14.254) をブロックリストボットとして選択し、これらの IP アドレス範囲のアクションとして [ドロップ]を選択します。
 - IP 範囲(192.140.15.4 から 192.140.15.254)をブロックリストボットとして指定し、これらの IP 範囲のアクションとしてログメッセージを作成するように選択されました

このシナリオでは、NetScaler ADM には次のように表示されます。

ブロックリストされたボットの総数
 ボットの総数は**未満、ドロップされたボットは**です
 ログに記録されているボットの総数

CAPTCHA ボットを表示する

ウェブページでは、CaptCha は、着信トラフィックが人間か自動化されたボットからのものかを識別するように設計されています。NetScaler ADM で CAPTCHA アクティビティを表示するには、NetScaler ADM インスタンスで IP レピュテーションおよびデバイス フィンガープリント検出技術のボット アクションとして CAPTCHA を構成する 必要があります。詳細については、「ボット管理の構成」を参照してください。

NetScaler ADM が Bot Insights に表示する CAPTCHA アクティビティは次のとおりです。

- キャプチャ試行回数超過 ログイン失敗後に行われた CAPTCHA の最大試行回数を示します
- Captcha client muted—CAPTCHA チャレンジで以前に不正なボットとして検出されたためにドロップまたはリダイレクトされたクライアント要求の数を示します。
- 人間-人間のユーザーが実行したキャプチャ入力を示します
- ・ 無効なキャプチャ応答-NetScaler が CAPTCHA チャレンジを送信したときに、ボットまたは人間から受信した不正な CAPTCHA 応答の数を示します

DOT CATEGORY	TOTAL ATTACKS	# DROPPED 🔅	# CAPTO IA 🔅	# ALLOWED 🔅	# RATE LIMIT 🔅	# REDIRECT - 0	#LOG 0
Captche Attempts Exceeded	11	11	0	0	0	0	0
Captche Client Muted	2	0	0	0	0	2	0
Crawler	36	86	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Involid Captcha Response	40	23	0	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scoper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

ボットトラップを見る

NetScaler ADM でボット トラップを表示するには、NetScaler でボット トラップを設定する必要があります。詳 細については、「ボット管理の構成」を参照してください。

Applications	6								10	1.0	- 10 miles	÷		Instances
Tural Bots on In	stance 18.3	06154240	ene 9.77 K.											BUR_2HE (30.30%.25%.240)
	Tetal Barts	Total Illuman Browsets	Bot Human Ratio	Signatured Both	Fingerprint ed Suits	Rate Record Bots	ar Reputation Bots	Whitefait Bots	Backlet Bots	Bot Tape	75.845			
test_R1	440	0	300:0	0	0	0	0	0	0	0	440			
test_vserve r	9.30 K	0	300:0	•	•	0	0	•	0	5	9.32 K			

ボットトラップを識別するために、スクリプトはウェブページで有効になっており、このスクリプトは人間には見え ませんが、ボットには見えません。NetScaler ADM は、ボットがこのスクリプトにアクセスしたときに、ボット ト ラップを識別して報告します。

仮想サーバーをクリックし、「ゼロピクセルリクエスト」を選択 します

BOT CATEGORY	TOTAL 0	# DROPPED 0	JI CAPICHA	# ALLOWED	# RATE LIMIT	3 REDIRECT	1106 0
Invalid Device?P	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

ボットの詳細の表示

詳細については、[ボットカテゴリ]の[ボット攻撃タイプ]をクリックします。

選択したキャプチャカテゴリの攻撃時間やボット攻撃の総数などの詳細が表示されます。

ris y Berneger y	pm.,8	3 Bet	Rink	Carlingo														
But Category -	Capitch	a Attair	nyeta B	Access								2	Last 1.4	Aurith			36	nh
Timeline Details													ir maar 2	1.210, 1.1	- 140 - 144 - 1	i apri	2100.1	.50
1.					i.													5

ユーザーは棒グラフをドラッグして、ボット攻撃で表示する特定の時間範囲を選択することもできます。

1000	3 But Hages 3 Math, Service 3 But Atlantic Company			
	Rot Category - "BackLit"	×	LATIMAN V	Search
Ter	aine Detain		27 Aug 2013, 13.51 to 26 log 201	8.1551
	· · · · · · · · · · · · · · · · · · ·			-

ボット攻撃の追加情報を取得するには、をクリックして展開します。

	171276	1.000	82.108	MARKET I	10103-0408	ALC: UNLOW	AP STUDIE	LOCAL DE LA COMPANY	No. of Lot, No.	
	NUMBER.	10.000 L M	**	1994	-	Market	BARLIN	Respire	AND, N. M.	
\sim	100 00 0248 P.,	101021.88	Bad	Onball	Drap	BlackUSI	Black167	Bangalore	/0448_168_3681	
	Instance IP: 30.10 HTTP Request UR Region: Kamataka	6154240 Er/bleck_bk_texth	trel	Total Cour Profil	Dots: 1 itry Code: IN ie Name: bot_profit	÷				
	Ing Other States	101003-000	-	COMM N	-	Marrie	Ballon.	Respire	Ann. 10, 100.	

- インスタンス IP NetScaler インスタンスの IP アドレスを示します。
- Total Bots その特定の期間に発生したボット攻撃の合計数を示します。
- HTTP リクエスト URL: キャプチャレポート用に設定されている URL を示します。
- 国コード —ボット攻撃が発生した国を示します。
- 地域 ボット攻撃が発生した地域を示します。
- プロファイル名 -構成中にユーザーが提供したプロファイル名を示します。

高度な検索

ユーザーは、検索テキストボックスと期間リストを使用して、ユーザーの要件に従ってボットの詳細を表示すること もできます。ユーザーが検索ボックスをクリックすると、検索ボックスに次の検索候補のリストが表示されます。

- インスタンス IP NetScaler インスタンスの IP アドレス。
- クライアント IP クライアント IP アドレス。
- ボットタイプー「良い」または「悪い」などのボットタイプ。
- 重要度 ボット攻撃の重大度。

- アクション実行 ドロップ、アクションなし、リダイレクトなど、ボット攻撃後に実行されたアクション。
- ボットカテゴリーブロック リスト、許可リスト、フィンガープリントなどのボット攻撃のカテゴリ。カテゴリ
 に基づいて、ユーザーはボットアクションをそのカテゴリに関連付けることができます。
- ボット検出 ―ユーザーが NetScaler で構成したボット検出タイプ(ブロックリスト、許可リストなど)。
- 場所 ボット攻撃が発生した地域/国
- リクエスト URL ボット攻撃の可能性がある URL

ユーザーは、ユーザー検索クエリで演算子を使用して、ユーザー検索の焦点を絞り込むこともできます。たとえば、 ユーザーがすべての不良ボットを閲覧したい場合は次のようにします。

- 検索ボックスをクリックし、「ボットタイプ」を選択します
- 検索ボックスをもう一度クリックし、演算子 = を選択します =
- 検索ボックスをもう一度クリックし、[Bad]を選択します
- [検索]をクリックして結果を表示します



異常に高いリクエスト率

ユーザーは、アプリケーションとの間で送受信されるトラフィックを制御できます。ボット攻撃は、異常に高い要求 率を実行する可能性があります。たとえば、ユーザーがアプリケーションを 100 リクエスト/分を許可するように設 定し、ユーザーが 350 リクエストを監視した場合、ボット攻撃である可能性があります。

異常に高い要求率インジケーターを使用して、ユーザーはアプリケーションに受け取った異常な要求率を分析できま す。

NetScaler VPX 14.1

VIOLATION DETAILS	
Descolve Client Connections 4 11 Mar 10:11 (2) Behavior Secol Dhomally High Request Rate 2	Unusually High Request Rate senserment Abnormal deviation from usual Request rate on a nearer indicates possibility of an bot Attack.
20pm William Belantes band Unsexually Large Described V. 80 Non-On-1020 m Belantes band	What Happened Last Occurred Time Tetal Occurrences Applications Affected 82 April 103 ares 7 1
Unusually Large Uplead Value 19 Toler 10:00 em Rehadour based	Event Details
	Affected Application rec.res.tel.04.040.217360.00
	Regard Rate Read Form
	anina anina trina trina trina trina trina

[イベントの詳細] で、ユーザーは以下を表示できます。

- 影響を受けるアプリケーション。複数のアプリケーションが違反の影響を受ける場合、ユーザーはリストから アプリケーションを選択することもできます。
- すべての違反を示すグラフ
- 違反の発生時刻
- 違反の検出メッセージ。受信した要求の合計と、予想された要求よりも受信した過剰な要求の割合を示します。
- 想定されるリクエストレートの許容範囲は、アプリケーションにより異なる

ボットの検出

NetScaler ボット管理システムは、さまざまな手法を使用して受信ボットトラフィックを検出します。この手法は、 ボットタイプを検出するための検出ルールとして使用されます。

GUI によるボット管理の設定 ユーザーは、最初にアプライアンスで機能を有効にすることで、NetScaler ボット 管理を構成できます。詳細については、「ボット検出」を参照してください。

IP レピュテーション

IP レピュテーションは、不要な要求を送信する IP アドレスを識別するツールです。IP レピュテーションリストを使 用すると、レピュテーションの悪い IP アドレスからのリクエストを拒否できます。

GUIを使用して IP レピュテーションを設定する この設定は、ボット IP レピュテーション機能の前提条件です。詳細については、「IP レピュテーション」を参照してください。

Bot シグネチャの自動更新 ボット静的シグニチャ手法では、シグニチャルックアップテーブルと良いボットと不良 ボットのリストを使用します。詳細については、署名の自動更新を参照してください。

NetScaler Web App Firewall と OWASP トップ 10–2021

オープンウェブアプリケーションセキュリティプロジェクト(OWAP)は、ウェブアプリケーションセキュリティに 関する 2021 年の OWASP トップ 10 を発表しました。このリストは、最も一般的な Web アプリケーションの脆弱 性を説明しており、Web セキュリティを評価するための優れた出発点です。このセクションでは、これらの欠陥を軽 減するように NetScaler Web App Firewall を構成する方法について説明します。WAF は、NetScaler(プレミア ムエディション)およびさまざまなアプライアンスの統合モジュールとして利用できます。

OWASP Top 10 の完全なドキュメントは OWASP Top Tenで入手できます。

OWASP トップ 10 2021	NetScaler Web App Firewall 機能
A 1:2021 壊れたアクセスコントロール	AAA、NetScaler の AAA モジュール内の認証セキュリ
	ティ機能、フォーム保護、Cookie 改ざん保護、
	StartURL、ClosureURL
A 2:2021-暗号化の失敗	クレジットカード保護、セーフコマース、クッキープロ
	キシ、クッキー暗号化
A 3:2021-インジェクション	インジェクション攻撃防止 (SQL または OS コマンドイ
	ンジェクション、XPath インジェクション、LDAP イン
	ジェクションなどのカスタムインジェクション)、シグネ
	チャの自動更新機能
A 5:2021 セキュリティの設定ミス	WSI チェック、XML メッセージ検証、XML SOAP 障害
	フィルタリングチェックを含むこの保護
A 6:2021-脆弱性と古いコンポーネント	脆弱性スキャンレポート、アプリケーションファイアウ
	ォールテンプレート、およびカスタム署名
A 7:2021-識別と認証の失敗	AAA、クッキー改ざん防止、クッキープロキシ、クッキ
	一暗号化、CSRF タギング、SSL の使用
A 8:2021 – ソフトウェアとデータの整合性に関する障害	XML セキュリティチェック、GWT コンテンツタイプ、
	カスタム署名、JSON および XML 用の Xpath
A 9:2021 —セキュリティロギングと監視の失敗	ユーザー設定可能なカスタムロギング、管理および分析
	システム

A 1:2021 壊れたアクセスコントロール

認証されたユーザーに許可される内容の制限は、多くの場合、適切に適用されません。攻撃者はこれらの欠陥を悪用 して、他のユーザーのアカウントへのアクセス、機密ファイルの閲覧、他のユーザーのデータの変更、アクセス権の 変更など、不正な機能やデータにアクセスできます。

NetScaler Web App Firewall 保護

- すべてのアプリケーショントラフィックの認証、認可、および監査をサポートする AAA 機能により、サイト管 理者は ADC アプライアンスでアクセス制御を管理できます。
- ADC アプライアンスの AAA モジュール内の認証セキュリティ機能により、アプライアンスは、保護されてい るサーバ上のどのコンテンツに各ユーザにアクセスを許可するかを検証できます。
- フォームフィールドの一貫性:オブジェクト参照がフォームに非表示フィールドとして保存されている場合、 フォームフィールドの一貫性を使用して、これらのフィールドが以降のリクエストで改ざんされていないこと を検証できます。
- Cookie プロキシと Cookie の一貫性: クッキー値に保存されているオブジェクト参照は、これらの保護機能 で検証できます。
- URL クロージャで URL チェックを開始: 事前定義された URL の許可リストへのユーザーアクセスを許可します。URL クロージャは、ユーザーセッション中に有効な応答に表示されるすべての URL のリストを作成し、そのセッション中に自動的にアクセスを許可します。

A 2:2021-暗号化の失敗

多くの Web アプリケーションと API は、財務、医療、PII などの機密データを適切に保護していません。攻撃者は、 クレジットカード詐欺、個人情報の盗難、またはその他の犯罪を行うために、そのような保護が不十分なデータを盗 んだり変更したりする可能性があります。機密データは、保存中または転送中の暗号化など、追加の保護なしで侵害 される可能性があり、ブラウザと交換する場合は特別な予防措置が必要です。

NetScaler Web App Firewall 保護

- Web Application Firewall は、クレジットカード情報などの機密データの漏洩からアプリケーションを保護 します。
- 機密データをセーフコマース保護のセーフオブジェクトとして設定して、露出を防ぐことができます。
- クッキー内の機密データは、クッキープロキシとクッキー暗号化によって保護できます。

A 3:2021-インジェクション

SQL、NoSQL、OS、LDAP インジェクションなどのインジェクションの欠陥は、信頼できないデータがコマンドま たはクエリの一部としてインタープリターに送信されるときに発生します。攻撃者の敵対的なデータは、通訳者を騙 して意図しないコマンドを実行させたり、適切な許可なしにデータにアクセスさせたりする可能性があります。

XSS の欠陥は、アプリケーションが適切な検証やエスケープを行わずに信頼できないデータを新しい Web ページに 含めたり、HTML または JavaScript を作成できるブラウザ API を使用してユーザー提供のデータで既存の Web ペ ージを更新したりする場合に発生します。XSS を使用すると、攻撃者は被害者のブラウザでスクリプトを実行して、 ユーザーセッションをハイジャックしたり、Web サイトを改ざんしたり、ユーザーを悪意のあるサイトにリダイレク トしたりできます。

NetScaler Web App Firewall 保護

- SQL インジェクション防止機能は、一般的なインジェクション攻撃から保護します。カスタム・インジェクション・パターンをアップロードして、XPath や LDAP を含むあらゆる種類のインジェクション攻撃から保護できます。これは HTML ペイロードと XML ペイロードの両方に適用されます。
- シグネチャの自動更新機能は、インジェクションシグネチャを最新の状態に保ちます。
- フィールドフォーマット保護機能を使用すると、管理者は任意のユーザーパラメータを正規表現に制限できます。たとえば、郵便番号フィールドには整数のみを含めることも、5桁の整数を含めることもできます。
- フォームフィールドの一貫性では、送信された各ユーザーフォームをユーザーセッションフォームの署名と照合して検証し、すべてのフォーム要素の有効性を確認します。
- バッファオーバーフローチェックは、URL、ヘッダー、および Cookie が適切な制限内にあることを確認し、 大きなスクリプトやコードを挿入する試みをブロックします。
- XSS 保護は、一般的な XSS 攻撃から保護します。カスタム XSS パターンをアップロードして、許可されているタグと属性のデフォルトリストを変更できます。ADC WAF は、許可された HTML 属性とタグのホワイトリストを使用して、XSS 攻撃を検出します。これは HTML ペイロードと XML ペイロードの両方に適用されます。
- ADC WAF は、OWASP XSS フィルター評価チートシートに記載されているすべての攻撃をブロックします。
- フィールドフォーマットチェックは、攻撃者が XSS 攻撃の可能性がある不適切な Web フォームデータを送信 するのを防ぎます。
- フォームフィールドの一貫性。

A 5:2021-セキュリティの設定ミス

セキュリティの設定ミスは、最もよく見られる問題です。これは通常、安全でないデフォルト設定、不完全または即 興の構成、オープンクラウドストレージ、誤って構成された HTTP ヘッダー、機密情報を含む詳細なエラーメッセー ジの結果です。すべてのオペレーティングシステム、フレームワーク、ライブラリ、アプリケーションを安全に構成 する必要があるだけでなく、パッチを適用してタイムリーにアップグレードする必要があります。

古いまたは構成が不十分な XML プロセッサの多くは、XML ドキュメント内の外部エンティティ参照を評価します。 外部エンティティは、ファイル URI ハンドラー、内部ファイル共有、内部ポートスキャン、リモートコード実行、お よびサービス拒否攻撃を使用して内部ファイルを開示するために使用できます。

NetScaler Web App Firewall 保護

- アプリケーションファイアウォールによって生成される PCI-DSS レポートには、ファイアウォールデバイスのセキュリティ設定が記録されます。
- スキャンツールからのレポートは、セキュリティ設定ミスを処理するために ADC WAF シグネチャに変換されます。
- NetScaler Web アプリケーションファイアウォールは、Cenzic、IBM AppScan(エンタープライズおよび スタンダード)、Qualys、TrendMicro、WhiteHat、およびカスタム脆弱性スキャンレポートをサポートし ています。
- XML ベースのアプリケーション (クロスサイトスクリプティング、コマンドインジェクションなど) への攻撃
 に適応できる一般的なアプリケーションの脅威を検出してブロックすることに加えて。
- NetScaler Web App Firewall Web アプリケーションファイアウォールには、XML 固有のセキュリティ保 護機能が豊富に含まれています。これには、SOAP メッセージと XML ペイロードを徹底的に検証するスキー マ検証や、悪意のある実行可能ファイルまたはウイルスを含む添付ファイルをブロックする強力な XML 添付 ファイルチェックが含まれます。
- 自動トラフィック検査方法は、アクセスを獲得することを目的とした URL やフォームに対する XPath インジェクション攻撃をブロックします。
- NetScaler Web App Firewall Web アプリケーションファイアウォールは、外部エンティティ参照、再帰的 拡張、過剰なネスト、長いまたは多くの属性や要素を含む悪意のあるメッセージなど、さまざまな DoS 攻撃 も阻止します。

A 6:2021-脆弱で時代遅れのコンポーネント

ライブラリ、フレームワーク、その他のソフトウェアモジュールなどのコンポーネントは、アプリケーションと同じ 権限で実行されます。脆弱なコンポーネントが悪用された場合、そのような攻撃は重大なデータ損失またはサーバー の乗っ取りを助長する可能性があります。既知の脆弱性を持つコンポーネントを使用するアプリケーションと API は、アプリケーションの防御を弱体化させ、さまざまな攻撃や影響を引き起こす可能性があります。

NetScaler Web App Firewall 保護

- サードパーティのコンポーネントを最新の状態にしておくことをお勧めします。
- ADC シグネチャに変換された脆弱性スキャンレポートを使用して、これらのコンポーネントに仮想的にパッ チを適用できます。
- これらの脆弱なコンポーネントに使用できるアプリケーションファイアウォールテンプレートを使用できます。
- カスタムシグネチャをファイアウォールにバインドして、これらのコンポーネントを保護できます。

A7:2021 -- 認証が壊れています

認証とセッション管理に関連するアプリケーション機能は正しく実装されていないことが多く、攻撃者はパスワード、 キー、またはセッショントークンを侵害したり、他の実装の欠陥を悪用して他のユーザーの ID を一時的または永続的 に引き継ぐことができます。

NetScaler Web App Firewall 保護

- NetScaler AAA モジュールは、ユーザー認証を実行し、バックエンドアプリケーションにシングルサインオン機能を提供します。これは NetScaler AppExpert ポリシーエンジンに統合され、ユーザーおよびグループの情報に基づくカスタムポリシーを許可します。
- ファイアウォールは、SSLオフロードと URL 変換機能を使用して、サイトが安全なトランスポート層プロト コルを使用して、ネットワークスニッフィングによるセッショントークンの盗用を防ぐこともできます。
- Cookie プロキシと Cookie 暗号化を使用すると、クッキーの盗難を完全に軽減できます。

A 8:2021-ソフトウェアとデータの整合性の失敗

安全でないデシリアライゼーションは、多くの場合、リモートでコードが実行される原因になります。デシリアライ ゼーションの欠陥によってリモートコードが実行されない場合でも、リプレイ攻撃、インジェクション攻撃、権限昇 格攻撃などの攻撃を実行するために使用できます。

NetScaler Web App Firewall 保護

- カスタム署名付きの JSON ペイロード検査。
- XML セキュリティ:XML サービス拒否 (XDoS)、XML SQL および Xpath インジェクション、クロスサイトス クリプティング、フォーマットチェック、WS-I 基本プロファイルコンプライアンス、XML 添付ファイルチェ ックから保護します。
- フィールドフォーマットチェックとクッキーコンシステンシーとフィールドコンシステンシーを使用できます。

A 9:2021-セキュリティロギングと監視の失敗

不十分なロギングと監視、およびインシデント対応との統合の欠落または非効率的な統合により、攻撃者はシステム をさらに攻撃し、永続性を維持し、より多くのシステムにピボットし、データを改ざん、抽出、または破壊すること ができます。ほとんどの侵害調査では、侵害を検出する時間は 200 日を超え、通常は内部のプロセスや監視ではなく 外部の関係者によって検出されることが示されています。

NetScaler Web App Firewall 保護

- セキュリティチェックまたは署名に対してログアクションが有効になっている場合、生成されるログメッセージには、アプリケーションファイアウォールがWebサイトとアプリケーションを保護している間に監視した要求と応答に関する情報が提供されます。
- アプリケーションファイアウォールは、組み込みの ADC データベースを使用して、悪意のある要求の発信元 である IP アドレスに対応する場所を識別する便利さを提供します。
- デフォルトフォーマット (PI) 式を使用すると、ログに含まれる情報を柔軟にカスタマイズできます。また、ア プリケーションファイアウォールが生成するログメッセージにキャプチャする特定のデータを追加することも できます。
- アプリケーションファイアウォールは CEF ログをサポートしています。

参照ドキュメント

- HTML SQL インジェクションチェック
- XML SQL インジェクションチェック
- コマンドラインを使用して HTML クロスサイトスクリプティングチェックを設定する
- XML クロスサイトスクリプティングチェック
- コマンドラインによるバッファオーバーフローセキュリティチェックの設定
- 署名オブジェクトの追加または削除
- 署名オブジェクトの設定または変更
- 署名オブジェクトの更新
- Snort 規則の統合
- ボットの検出
- Microsoft Azure で NetScaler VPX インスタンスを展開する

NetScaler Gateway アプライアンスのアドレスプールのイントラネット IP を構成する

October 17, 2024

場合によっては、NetScaler Gateway プラグインを使用して接続するユーザーは、NetScaler Gateway アプライ アンス用に一意の IP アドレスが必要です。グループのアドレスプール(IP プーリングとも呼ばれる)を有効にする と、NetScaler Gateway アプライアンスは一意の IP アドレスエイリアスを各ユーザーに割り当てることができま す。アドレスプールは、イントラネット IP (IIP) アドレスを使用して構成します。

Azure にデプロイされた NetScaler Gateway アプライアンスでアドレスプールを構成するには、次の2ステップの手順に従います。

- アドレスプールで使用されるプライベート IP アドレスを Azure に登録する
- NetScaler Gateway アプライアンスでのアドレスプールの構成

Azure ポータルにプライベート IP アドレスを登録する

Azure では、複数の IP アドレスを持つ NetScaler ADC VPX インスタンスを展開できます。次の 2 つの方法で IP アドレスを VPX インスタンスに追加できます。

a. VPX インスタンスの Provisioning 中

VPX インスタンスのプロビジョニング中に複数の IP アドレスを追加する方法の詳細については、「NetScaler スタ ンドアロン インスタンスに複数の IP アドレスを構成する」を参照してください。VPX インスタンスのプロビジョニ ング中に PowerShell コマンドを使用して IP アドレスを追加するには、「PowerShell コマンドを使用してスタン ドアロン モードで NetScaler VPX インスタンスに複数の IP アドレスを構成する」を参照してください。

b. VPX インスタンスをプロビジョニング後

VPX インスタンスをプロビジョニングしたら、次の手順に従って Azure ポータルにプライベート IP アドレスを登録 します。この IP アドレスは、NetScaler Gateway アプライアンスでアドレスプールとして構成します。

 Azure Resource Manager (ARM) から、すでに作成されている NetScaler VPX インスタンス > ネットワ ークインターフェイスに移動します。登録する IIP が属しているサブネットにバインドされているネットワー クインターフェイスを選択します。

NSDoc0330VM - Network in	terfaces	
	Search network interfaces	
ags 🗸	NAME	PUBLIC IP ADDRESS
X Diagnose and solve problems	nsdoc0330vm923	13.78.187.150
SETTINGS		
Availability set		
😑 Disks		
Extensions		
Network interfaces		
i Size		

2. [IP 構成] をクリックし、[追加] をクリックします。

Microsoft Azure NSDoc0330VM - Network interfaces > nsdoc0330vm923 - IP configurations					
	nsdoc0330vm923 - IP confinentiate	gurations			
+		📥 Add 🔛 Sa	ave 🗙 Discard		
	Overview	IP forwarding s	ettings		Disabled Enabled
••• (*)	 Activity log Access control (IAM) 	Virtual network			NSDoc0330VNET
٩	🧳 Tags	IP configuration	ns		
۲	SETTINGS	" Subnet			Frontend (192.0.0.0/24)
<u>.</u>	IP configurations		nfigurations		
	DNS servers	NAME	IP VERSION	ТҮРЕ	PRIVATE IP ADDRE
<i>.</i>	Network security group	ipconfig1	IPv4	Primary	192.0.0.4 (Static)
e		ipconfig2	IPv4	Secondary	192.0.0.5 (Static)
I		ipconfig3	IPv4	Secondary	192.0.0.6 (Static)

3. 以下の例のように必要な詳細を入力し、[OK]をクリックします。

Add IP configuration	
* Name	
PrivateIP5	~
Type Primary Secondary	
Primary IP configuration already exists	
Private IP address settings Allocation Dynamic Static	
* IP address	
192.0.0.8	~
Public IP address Disabled Enabled	
ок	

NetScaler Gateway アプライアンスでアドレスプールを構成する

NetScaler Gateway でアドレス プールを構成する方法の詳細については、「アドレス プールの構成」を参照してください。

制限事項:

```
IIP アドレスの範囲をユーザーにバインドすることはできません。アドレスプールで使用されるすべての IIP ア
ドレスを登録する必要があります。
```

PowerShell コマンドを使用して、**NetScaler VPX** スタンドアロンインスタンスに複数の **IP** アドレスを構成する

January 15, 2025

Azure 環境では、複数の NIC を設定して NetScaler VPX 仮想アプライアンスを展開できます。各 NIC に複数の IP アドレスを設定できます。このセクションでは、PowerShell コマンドを使用して、単一の NIC と複数の IP アドレ スを使用して Citrix ADC VPX インスタンスを展開する方法について説明します。複数 NIC と複数 IP の展開にも同 じスクリプトを使用できます。

注

このドキュメントでは、IP-config は、個々の NIC に関連付けられている IP アドレス、パブリック IP、プライ ベート IP のペアを指します。詳細については、「Azure 用語 」セクションを参照してください。

使用例

この使用例では、1 つの NIC が仮想ネットワーク(VNET)に接続されています。この NIC には、次の表に示す 3 つの IP 構成が関連付けられています。

IP コンフィグ	関連付けられている
IPConfig-1	静的パブリック IP アドレス; 静的プライベート IP アド
	レス
IPConfig-2	静的パブリック IP アドレス; 静的プライベートアドレス
IPConfig-3	静的プライベート IP アドレス

注

IPConfig-3 は、パブリック IP アドレスに関連付けられていません。

図: トポロジ

次の図はこの使用例を視覚的に示しています。



注

マルチ NIC、マルチ IP Azure NetScaler VPX 展開では、プライマリ(最初の)NIC のプライマリ(最初) IPConfigに関連付けられたプライベート IP アドレスが、アプライアンスの管理 NSIP アドレスとして 自動的に追加されます。IPConfigsに関連付けられた残りのプライベート IP アドレスは、要件に応じ てadd ns ipコマンドを使用して、VPX インスタンスに VIP または SNIP として追加する必要があります。

スタンドアロンモードで NetScaler VPX 仮想アプライアンスに対して複数 IP アドレスを構成する場合に必要な手順の概要は次のとおりです。

- 1. リソースグループの作成
- 2. ストレージアカウントの作成
- 3. 可用性セットの作成
- 4. ネットワークサービスグループの作成
- 5. 仮想ネットワークの作成
- 6. パブリック IP アドレスの作成
- 7. IP 構成の割り当て
- 8. NIC の作成
- 9. NetScaler VPX インスタンスの作成
- 10. NIC 構成のチェック

11. VPX 側の構成のチェック

スクリプト

パラメーター

このドキュメントのこの使用例のサンプルパラメーター設定は、次のとおりです。

1	<pre>\$locName="westcentralus"</pre>
2	
3	<pre>\$rgName="Azure-MultiIP"</pre>
4	
5	<pre>\$nicName1="VM1-NIC1"</pre>
6	
7	\$vNetName="Azure-MultiIP-vnet"
8	
9	<pre>\$vNetAddressRange="11.6.0.0/16"</pre>
10	
11	<pre>\$frontEndSubnetName="frontEndSubnet"</pre>
12	
13	<pre>\$frontEndSubnetRange="11.6.1.0/24"</pre>
14	
15	<pre>\$prmStorageAccountName="multiipstorage"</pre>
16	
17	<pre>\$avSetName="multiip-avSet"</pre>
18	
19	<pre>\$vmSize="Standard_DS4_V2" (This parameter creates a VM with up to four NICs.)</pre>

注

VPX インスタンスの最小要件は、2 つの vCPU と 2 GB の RAM です。

```
$publisher="Citrix"
1
2
3
     $offer="netscalervpx110-6531" (You can use different offers.)
4
     $sku="netscalerbyol" (According to your offer, the SKU can be
5
        different.)
6
7
     $version="latest"
8
9
     $pubIPName1="PIP1"
     $pubIPName2="PIP2"
11
12
     $domName1="multiipvpx1"
13
14
15
     $domName2="multiipvpx2"
16
     $vmNamePrefix="VPXMultiIP"
17
```

18 19 \$osDiskSuffix="osmultiipalbdiskdb1" 20 21 **Network Security Group (NSG)-related information**: 22 23 \$nsgName="NSG-MultiIP" 24 25 \$rule1Name="Inbound-HTTP" 26 \$rule2Name="Inbound-HTTPS" 27 28 29 \$rule3Name="Inbound-SSH" \$IpConfigName1="IPConfig1" 31 32 33 \$IPConfigName2="IPConfig-2" 34 \$IPConfigName3="IPConfig-3"

1. リソースグループを作成する

New-AzureRmResourceGroup -Name \$rgName -Location \$locName

2. ストレージアカウントを作成する

\$prmStorageAccount = New-AzureRMStorageAccount -Name \$prmStorageAccountName
-ResourceGroupName \$rgName -Type Standard_LRS -Location \$locName

3. 可用性セットを作成する

\$avSet = New-AzureRMAvailabilitySet -Name \$avSetName -ResourceGroupName \$rgName -Location \$locName

4. ネットワークセキュリティグループを作成する

1. 規則を追加します。トラフィックを処理するポートのネットワークセキュリティグループにルールを追加する 必要があります。

\$rule1=New-AzureRmNetworkSecurityRuleConfig -Name \$rule1Name Description "Allow HTTP"-Access Allow -Protocol Tcp -Direction
Inbound -Priority 101 -SourceAddressPrefix Internet -SourcePortRange
 * -DestinationAddressPrefix * -DestinationPortRange 80 \$rule2=
New-AzureRmNetworkSecurityRuleConfig -Name \$rule2Name -Description

"HTTPS を許可する"-Access Allow -Protocol Tcp -Direction Inbound -Priority 110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 443 \$rule3=New -AzureRmNetworkSecurityRuleConfig -Name \$rule3Name -Description "SSH を許可する"-Access Allow -Protocol Tcp -Direction Inbound -Priority 120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 22

2. ネットワークセキュリティグループオブジェクトを作成します。

\$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName \$rgName
-Location \$locName -Name \$nsgName -SecurityRules \$rule1,\$rule2,
\$rule3

5. 仮想ネットワークを作成する

1. サブネットを追加します。

\$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
\$frontEndSubnetName -AddressPrefix \$frontEndSubnetRange

2. 仮想ネットワークオブジェクトを追加します。

\$vnet=New-AzureRmVirtualNetwork -Name \$vNetName -ResourceGroupName
\$rgName -Location \$locName -AddressPrefix \$vNetAddressRange Subnet \$frontendSubnet

3. サブネットを取得します。

```
$subnetName="フロントエンドサブネット" $subnet1=$vnet.サブネット|?{ $_.Name -
eq $subnetName }
```

6. パブリック IP アドレスを作成する

\$pip1=New-AzureRmPublicIpAddress -Name \$pubIPName1 -ResourceGroupName \$rgName -DomainNameLabel \$domName1 -Location \$locName -AllocationMethod Static\$pip2=New-AzureRmPublicIpAddress -Name \$pubIPName2 -ResourceGroupName \$rgName -DomainNameLabel \$domName2 -Location \$locName -AllocationMethod Static

```
注
使用する前にドメイン名の可用性をチェックします。
IP アドレスの割り当て方法は動的または静的にできます。
```

7. IP 設定を割り当てる

この使用例では、IP アドレスを割り当てる前に次の点を検討します。

- IPConfig-1 が VPX1 の subnet1 に属していること
- IPConfig-2 が VPX1 の subnet 1 に属していること
- IPConfig-3 が VPX1 の subnet 1 に属していること

```
注
複数の IP 構成を 1 つの NIC に割り当てるときには、1 つの構成をプライマリとして割り当てる必要がありま
す。
```

```
$IPAddress1="11.6.1.27"
1
    $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
        Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress
        $pip1 - Primary
    $IPAddress2="11.6.1.28"
3
    $IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
4
        Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress
        $pip2
5
    $IPAddress3="11.6.1.29"
6
    $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
        Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

サブネットの要件に合う有効な IP アドレスを使用して、その可用性をチェックします。

8. NIC を作成する

\$nic1=New-AzureRmNetworkInterface -Name \$nicName1 -ResourceGroupName \$rgName -Location \$locName -IpConfiguration \$IpConfig1,\$IpConfig2, \$IPConfig3 -NetworkSecurityGroupId \$nsg.Id

9. NetScaler VPX インスタンスを作成する

1. 変数を初期化します。

```
$suffixNumber = 1$vmName = $vmNamePrefix + $suffixNumber
```

2. VM Config オブジェクトを作成します。

```
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
AvailabilitySetId $avSet.Id
```

3. 資格情報、OS、イメージを設定します。

```
$cred=Get-Credential -Message "VPXログインの名前とパスワードを入力してくだ
さい。" $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -
Linux -ComputerName $vmName -Credential $cred $vmConfig=Set-
AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -
Offer $offer -SKU $sku -バージョン $version
```

4. NIC を追加します。

\$vmConfig=Add-AzureRMVMNetworkInterface -VM \$vmConfig -Id \$nic1. Id -Primary

注

マルチ NIC NetScaler VPX 展開では、1 つの NIC がプライマリである必要があります。したがって、 その NIC を NetScaler VPX インスタンスに追加するときに、「-Primary」を追加する必要があります。

5. OS ディスクを指定して、VM を作成します。

\$osDiskName=\$vmName + "-"+ \$osDiskSuffix1\$osVhdUri=\$prmStorageAccount .PrimaryEndpoints.Blob.ToString()+ "vhds/"+ \$osDiskName + ".vhd" \$vmConfig=Set-AzureRMVMOSDisk -VM \$vmConfig -名前 \$osDiskName -VhdUri \$osVhdUri -CreateOption fromImage Set-AzureRmVMPlan -VM \$vmConfig -発行元 \$publisher -製品 \$offer -名前 \$sku New-AzureRMVM -VM \$vmConfig -リソースグループ名 \$rgName -場所 \$locName

10. NIC 設定を確認する

NetScaler VPX インスタンスが起動したら、以下のコマンドを使用して、NetScaler VPX NIC の IPConfigs に 割り当てられている IP アドレスを確認できます。

\$nic.IPConfig

11. VPX 側の設定を確認する

NetScaler VPX インスタンスが起動すると、IPconfig プライマリ NIC のプライマリに関連付けられたプライベ ート IP アドレスが NSIP アドレスとして追加されます。残りのプライベート IP アドレスは、要件に従って、VIP ま たは SNIP アドレスとして追加する必要があります。次のコマンドを使用します。

add nsip <Private IPAddress><netmask> -type VIP/SNIP

スタンドアロンモードの NetScaler VPX インスタンスに対して複数 IP アドレスを構成しました。

Azure 展開の追加の PowerShell スクリプト

October 17, 2024

このセクションでは、Azure PowerShell で次の構成を実行できる PowerShell コマンドレットについて説明しま す。

- NetScaler VPX スタンドアロンインスタンスのプロビジョニング
- Azure 外部ロードバランサーを使用した高可用性セットアップで NetScaler VPX ペアをプロビジョニングします
- Azure 内部ロードバランサーを使用した高可用性セットアップで NetScaler VPX ペアをプロビジョニングします

PowerShell コマンドを使用して実行できる構成については、次のトピックも参照してください。

- PowerShell コマンドを使用して複数の IP アドレスと NIC を使用して高可用性セットアップを構成する
- NetScaler VPX インスタンスで GSLB を構成する
- NetScaler のアクティブ/スタンバイ高可用性セットアップで GSLB を構成する
- PowerShell コマンドを使用して、スタンドアロンモードの NetScaler ADC VPX インスタンスで複数の IP アドレスを構成する

NetScaler VPX スタンドアロンインスタンスのプロビジョニング

1. リソースグループの作成

リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソー スのみを含めることもできます。ここで指定した場所は、そのリソースグループ内のリソースのデフォルトの 場所です。ロードバランサーを作成する場合、すべてのコマンドで同じリソースグループを使用してください。

```
$rgName="<resource group name&gt;" $locName="&lt;location name
, such as West US> New-AzureRmResourceGroup -名前 $rgName -場所
$locName
```

例えば:

```
    $rgName = "ARM-VPX"
    $locName = "West US"
    New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. ストレージアカウントの作成

ストレージアカウントには、小文字と数字のみを含む一意の名前を選択する必要があります。

```
$saName="<storage account name&gt;" $saType="&lt;storage account type&gt;"、1 つ 指 定 し て く だ さ い: Standard_LRS、Standard_GRS、
```

```
Standard_RAGRS 、 ま た はPremium_LRS New-AzureRmStorageAccount -名前
$saName -リソースグループ名 $rgName -タイプ $saType -場所 $locName
```

例えば:

```
1 $saName="vpxstorage"
2 $saType="Standard\_LRS"
3 New-AzureRmStorageAccount -Name $saName -ResourceGroupName
    $rgName -Type $saType -Location $locName
```

3. アベイラビリティセットの作成

可用性セットにより、メンテナンス時などのダウンタイム中でも仮想マシンを使用し続けることができます。 可用性セットが構成されたロードバランサーでは、アプリケーションをいつでも使用できます。

\$avName="<availability set name>"

```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. 仮想ネットワークの作成

```
以前に作成されたサブネットがない場合、少なくとも1つのサブネットを持つ新しい仮想ネットワークを追加
します。
```

```
$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 New-
AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
-Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
$frontendSubnet, $backendSubnet
```

例えば:

1	\$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix \$FrontendAddressPrefix
2	
3	<pre>\$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix \$BackendAddressPrefix</pre>
5	New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet

5. NIC を作成する

NIC を作成し、それを NetScaler VPX インスタンスに関連付けます。上記の手順で作成されたフロントエン ドサブネットは 0 でインデックス付けされ、バックエンドサブネットは 1 でインデックス付けされます。次の 3 つのいずれかの方法で NIC を作成します。

```
a)パブリックIPアドレスを持つNIC

$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)パブリックIPアドレスとDNS ラベルが付けられたNIC

$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
```

\$domName を割り当てる前に、次のコマンドを使用して、それが利用できるかどうかを確認します。

```
Test-AzureRmDnsAvailability -DomainQualifiedName $domName -
Location $locName
```

\$nic = New-AzureRmNetworkInterface -Name \$nicName -ResourceGroupName
\$rgName -Location \$locName -SubnetId \$vnet.Subnets[\$subnetIndex
].Id -PublicIpAddressId \$pip.Id

例えば:

```
1 $nicName="frontendNIC"
2 $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) 動的パブリックアドレスと静的プライベート IP アドレスを持つ NIC

仮想マシンに追加するプライベート(静的)IP アドレスが、指定したサブネットのアドレスと同じ範囲である 必要があります。

\$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. 仮想オブジェクトの作成

\$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. NetScaler VPX イメージを取得

\$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."

VPX へのログインに使用する資格情報を入力してください

```
$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

例えば:

\$pubName="citrix"

次のコマンドを使用すると、Citrix からのすべてのオファーが表示されます。

```
1 Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
2
3 $offerName="netscalervpx110-6531"
```

次のコマンドは、特定のオファー名について発行元から提供される SKU を知るために使用します。

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -
Offer $offerName | Select Skus
```

8. 仮想マシンの作成

\$diskName="<name identifier for the disk in Azure storage, such
as OSDisk>"

例えば:

```
$diskName="dynamic"
1
2
3
     $pubName="citrix"
4
5
     $offerName="netscalervpx110-6531"
6
     $skuName="netscalerbyol"
7
8
9
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
10
11
     $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/
        " + $diskName + ".vhd"
12
13
     $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri
        $osDiskUri -CreateOption fromImage
```

MarketPlace に存在するイメージから VM を作成する場合、次のコマンドを使用して VM プランを指定します。

Set-AzureRmVMPlan -VM \$vm -Publisher \$pubName -Product \$offerName -Name \$skuName

```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
$vm
```

Azure 外部ロードバランサーを使用した高可用性セットアップで NetScaler VPX ペアをプロビジョニン グします

Azure のユーザー資格情報を使用して AzureRmAccount にログオンします。

1. リソースグループの作成

ここで指定した場所は、そのリソースグループ内のリソースのデフォルトの場所です。ロードバランサーを作 成する場合、すべてのコマンドで同じリソースグループを使用してください。

\$rgName="<resource group name>"

\$locName="<location name, such as West US>"

New-AzureRmResourceGroup -Name \$rgName -Location \$locName

例えば:

```
1 $rgName = "ARM-LB-NS"
2
3 $locName = "West US"
4
5 New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. ストレージアカウントの作成

ストレージアカウントには、小文字と数字のみを含む一意の名前を選択する必要があります。

\$saName="<storage account name>"

\$saType="<storage account type>"、1つ指定してください:Standard_LRS、 Standard_GRS、Standard_RAGRS、またはPremium_LRS

New-AzureRmStorageAccount -Name \$saName -ResourceGroupName \$rgName -Type \$saType -Location \$locName

例えば:

```
$ $saName="vpxstorage"
$ $saType="Standard_LRS"
$ New-AzureRmStorageAccount -Name $saName -ResourceGroupName
$ $rgName -Type $saType -Location $locName
```

3. アベイラビリティセットの作成

可用性セットが構成されたロードバランサーでは、アプリケーションをいつでも使用できます。

```
$avName="<availability set name>"
```

New-AzureRmAvailabilitySet -Name \$avName -ResourceGroupName
\$rgName -Location \$locName

4. 仮想ネットワークの作成

```
以前に作成されたサブネットがない場合、少なくとも1つのサブネットを持つ新しい仮想ネットワークを追加
します。
```

```
$vnetName = "LBVnet"
1
2
3
     $FrontendAddressPrefix="10.0.1.0/24"
4
     $BackendAddressPrefix="10.0.2.0/24"
5
6
     $vnetAddressPrefix="10.0.0.0/16"
7
8
     $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
9
        frontendSubnet -AddressPrefix $FrontendAddressPrefix
10
```

11	<pre>\$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix \$BackendAddressPrefix</pre>
12	
13	<pre>\$vnet=New-AzureRmVirtualNetwork -Name \$vnetName - ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet</pre>

注

要件に応じて AddressPrefix パラメータ値を選択します。

フロントエンドおよびバックエンドサブネットを、前の手順で作成した仮想ネットワークに割り当てます。

フロントエンドサブネットが配列 VNet の最初の要素である場合、subnetId は \$vnet.subnets [0] .Id でな ければなりません。

フロントエンドサブネットが配列の 2 番目の要素である場合、subnetId は \$vnet.subnets [1] .Id というよ うにする必要があります。

5. フロントエンド IP アドレスを構成し、バックエンドアドレスプールを作成する

受信ロードバランサーネットワークトラフィック用のフロントエンド IP アドレスを構成し、負荷分散トラフィックを受信するバックエンドアドレスプールを作成します。

```
注
```

DomainNameLabel の値が使用可能かどうかを確認します。

1	<pre>\$FIPName = "ELBFIP"</pre>
2	
3	<pre>\$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig - Name \$FIPName -PublicIpAddress \$publicIP1</pre>
4	
5	\$BEPool = "LB-backend-Pool"
6	
7	\$beaddresspool1= New- AzureRmLoadBalancerBackendAddressPoolConfig -Name \$BEPool

6. ヘルスプローブの作成

ポート 9000、間隔 5 秒で TCP ヘルププローブを作成します。

1 \$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2 7. 負荷分散ルールを作成する

負荷分散するサービスごとに LB ルールを作成します。

例えば:

次の例を使用して、HTTP サービスの負荷分散を行うことができます。

```
1 $lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
FrontendIpConfiguration $frontendIP1 -BackendAddressPool
$beAddressPool1 -Probe $healthProbe -Protocol Tcp -
FrontendPort 80 -BackendPort 80
```

8. インバウンド NAT ルールの作成

負荷分散していないサービスに対する NAT 規則を作成します。

たとえば、NetScaler VPX インスタンスへの SSH アクセスを作成する場合などです。

注

2 つの NAT ルールでは、Protocol-FrontEndPort-BackendPort トリプレットが同じであってはなりません。

1	<pre>\$inboundNATRule1= New-</pre>
	AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1
	-FrontendIpConfiguration \$frontendIP1 -Protocol
	TCP -FrontendPort 22 -BackendPort 22
2	
3	\$inboundNATRule2= New-
	AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 -
	FrontendIpConfiguration \$frontendIP1 - Protocol TCP -
	FrontendPort 10022 -BackendPort 22

9. ロードバランサーエンティティの作成

すべてのオブジェクト(NAT 規則、ロードバランサー規則、プローブ構成)を一度に追加してロードバランサ ーを作成します。

```
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. NIC を作成する

2つの NIC を作成し、各 NIC を各 VPX インスタンスに関連付けます

a) NIC1をVPX1に

例えば:

```
$nicName="NIC1"
1
2
3
     $lbName="ELB"
4
5
     $bePoolIndex=0
6
     \* Rule indexes starts from 0.
7
8
9
     $natRuleIndex=0
     $subnetIndex=0
11
12
13
     \* Frontend subnet index
14
15
     $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
        $rgName
     $nic1=New-AzureRmNetworkInterface -Name $nicName -
17
        ResourceGroupName $rgName -Location $locName -Subnet $vnet.
        Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
        BackendAddressPools\[$bePoolIndex\] -
        LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
        1
```

b) NIC2をVPX2に

例えば:

1	\$nicName="NIC2"
2	
3	<pre>\$lbName="ELB"</pre>
4	
5	<pre>\$bePoolIndex=0</pre>
6	
7	<pre>\$natRuleIndex=1</pre>
8	
9	<pre>* Second Inbound NAT (SSH) rule we need to use</pre>
10	
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. NetScaler VPX インスタンスの作成

2 つの NetScaler VPX インスタンスを、同じリソースグループおよび可用性セットの一部として作成し、外 部ロードバランサーに割り当てます。

a) NetScaler VPX インスタンス1

例えば:

1	\$vmName="VPX1"
3	<pre>\$vmSize="Standard_A3"</pre>
5	<pre>\$pubName="citrix"</pre>
7	<pre>\$offerName="netscalervpx110-6531"</pre>
9	\$skuName="netscalerbyol"
11	\$avSet=Get-AzureRmAvailabilitySet -Name \$avName - ResourceGroupName \$rgName
13	\$vm1=New-AzureRmVMConfig -VMName \$vmName -VMSize \$vmSize - AvailabilitySetId \$avset.Id
14 15	<pre>\$cred=Get-Credential -Message "Type Credentials which will be used to login to VPX instance"</pre>
16 17	\$vm1=Set-AzureRmVMOperatingSystem -VM \$vm1 -Linux -ComputerName \$vmName -Credential \$cred -Verbose
18 19	<pre>\$vm1=Set-AzureRmVMSourceImage -VM \$vm1 -PublisherName \$pubName - Offer \$offerName -Skus \$skuName -Version "latest"</pre>
20 21 22	\$vm1=Add-AzureRmVMNetworkInterface -VM \$vm1 -Id \$nic1.Id
23 24	\$diskName="dynamic"
25	<pre>\$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName \$rgName -Name \$saName</pre>
26	
27	<pre>\$osDiskUri1=\$storageAcc.PrimaryEndpoints.Blob.ToString() + " vhds1/" + \$diskName + ".vhd"</pre>
28	
29	\$vm1=Set-AzureRmVMOSDisk -VM \$vm1 -Name \$diskName -VhdUri \$osDiskUri1 -CreateOption fromImage
30	
31	Set-AzureRmVMPlan -VM \$vm1 -Publisher \$pubName -Product \$offerName -Name \$skuName
32	
33	New-AzureRmVM -ResourceGroupName \$rgName -Location \$locName -VM \$vm1

b) NetScaler VPX インスタンス 2

例えば:

```
$vmName="VPX2"
1
2
3
     $vmSize="Standard\_A3"
4
5
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
     $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
     $cred=Get-Credential -Message " Type Credentials which will be
9
        used to login to VPX instance "
     $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
         $vmName -Credential $cred -Verbose
12
13
     $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15
     $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
     $diskName="dynamic"
17
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
20
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName + ".vhd"
23
     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
         $osDiskUri1 -CreateOption fromImage
24
25
     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
         $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $vm2
```

12. 仮想マシンを構成する

両方の NetScaler VPX インスタンスが開始された場合、SSH プロトコル経由で両方の VPX インスタンスに 接続して仮想マシンを構成します。

a) アクティブ-アクティブ: 両方の NetScaler VPX インスタンスのコマンドラインで同じ構成コマンドセット を実行します。

b) アクティブ/パッシブ: このコマンドを両方の NetScaler VPX インスタンスのコマンドラインで実行します。

add ha node #nodeID <nsip of other NetScaler VPX>

アクティブ-パッシブモードでは、プライマリノードでのみ構成コマンドを実行します。

Azure 内部ロードバランサーを使用した高可用性セットアップで **NetScaler VPX** ペアをプロビジョニン グします

Azure のユーザー資格情報を使用して AzureRmAccount にログオンします。

1. リソースグループの作成

ここで指定した場所は、そのリソースグループ内のリソースのデフォルトの場所です。ロードバランサーを作 成する場合、すべてのコマンドで同じリソースグループを使用してください。

```
$rgName="\\<resource group name\\&#062;"
```

```
$locName="\\<location name, such as West US\\&#062;"
```

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

例えば:

```
1 $rgName = "ARM-LB-NS"
2
3 $locName = "West US"
4
5 New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. ストレージアカウントの作成

```
ストレージアカウントには、小文字と数字のみを含む一意の名前を選択する必要があります。
```

\$saName="<storage account name>"

\$saType="<storage account type>"、1つ指定してください:Standard_LRS、 Standard_GRS、Standard_RAGRS、またはPremium_LRS

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName
$rgName -Type $saType -Location $locName
```

例えば:

```
1 $saName="vpxstorage"
2
3 $saType="Standard_LRS"
4
5 New-AzureRmStorageAccount -Name $saName -ResourceGroupName
$rgName -Type $saType -Location $locName
```

3. アベイラビリティセットの作成

```
可用性セットが構成されたロードバランサーでは、アプリケーションをいつでも使用できます。
```

\$avName="<availability set name>"

```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. 仮想ネットワークの作成

以前に作成されたサブネットがない場合、少なくとも1つのサブネットを持つ新しい仮想ネットワークを追加 します。

\$vnetName = "LBVnet"
<pre>\$vnetAddressPrefix="10.0.0/16"</pre>
<pre>\$FrontendAddressPrefix="10.0.1.0/24"</pre>
\$BackendAddressPrefix="10.0.2.0/24"
\$vnet=New-AzureRmVirtualNetwork -Name \$vnetName - ResourceGroupName \$rgName -Location \$locName -AddressPrefix \$vnetAddressPrefix -Subnet \$frontendSubnet,\$backendSubnet\`
\$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix \$FrontendAddressPrefix
\$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix \$BackendAddressPrefix

注

要件に応じて AddressPrefix パラメータ値を選択します。

フロントエンドおよびバックエンドサブネットを、前の手順で作成した仮想ネットワークに割り当てます。

フロントエンドサブネットが配列 VNet の最初の要素である場合、subnetId は \$vnet.subnets [0] .Id でな ければなりません。

フロントエンドサブネットが配列の2番目の要素である場合、subnetId は \$vnet.subnets [1] .Id というようにする必要があります。

5. バックエンドアドレスプールを作成する

\$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig Name "LB-backend"

6. NAT ルールを作成する

負荷分散していないサービスに対する NAT 規則を作成します。

```
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
```

要件に応じて、フロントエンドポートおよびバックエンドポートを使用します。
7. ヘルスプローブの作成

ポート 9000、間隔 5 秒で TCP ヘルププローブを作成します。

```
1 $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
HealthProbe" " -Protocol tcp -Port 9000 -IntervalInSeconds 5
-ProbeCount 2
```

8. 負荷分散ルールを作成する

負荷分散するサービスごとに LB ルールを作成します。

例えば:

次の例を使用して、HTTP サービスの負荷分散を行うことができます。

```
1 $lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
FrontendIpConfiguration $frontendIP -BackendAddressPool
$beAddressPool -Probe $healthProbe -Protocol Tcp -
FrontendPort 80 -BackendPort 80
```

要件に応じて、フロントエンドポートおよびバックエンドポートを使用します。

9. ロードバランサーエンティティの作成

すべてのオブジェクト(NAT 規則、ロードバランサー規則、プローブ構成)を一度に追加してロードバランサ ーを作成します。



10. NIC を作成する

2つの NIC を作成し、各 NIC を各 NetScaler VPX インスタンスに関連付けます



この NIC は NetScaler VPX 1 用です。プライベート IP は、追加されたサブネットと同じサブネット内に存 在する必要があります。

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 \[1\]. この NIC は NetScaler ADC VPX 用です 2. Private IPAddressパラメーターには、要件に応じて任 意のプライベート IP を設定できます。

11. NetScaler VPX インスタンスの作成

同じリソースグループと可用性セットの一部である 2 つの VPX インスタンスを作成し、それを内部ロードバ ランサーにアタッチします。

a) NetScaler VPX インスタンス1

例えば:

```
1
     $vmName="VPX1"
2
3
     $vmSize="Standard\_A3"
4
5
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
7
     $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
8
9
     $cred=Get-Credential -Message "Type Credentials which will be
        used to login to VPX instance"
11
     $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
         $vmName -Credential $cred -Verbose
12
     $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
13
        Offer $offerName -Skus $skuName -Version "latest"
14
15
     $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id
16
     $diskName="dynamic"
17
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
          -Name $saName
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds1/" + $diskName + ".vhd"
22
     $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
23
        $osDiskUri1 -CreateOption fromImage
24
25
     Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
         $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm1
```

b) NetScaler VPX インスタンス 2

例えば:

```
$vmName="VPX2"
1
2
3
     $vmSize="Standard\_A3"
4
5
     $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
     $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
7
        AvailabilitySetId $avset.Id
8
     $cred=Get-Credential -Message " Type Credentials which will be
9
        used to login to VPX instance "
     $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
         $vmName -Credential $cred -Verbose
12
13
     $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15
     $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
     $diskName="dynamic"
17
18
19
     $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
20
21
     $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName + ".vhd"
23
     $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
         $osDiskUri1 -CreateOption fromImage
24
25
     Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
         $offerName -Name $skuName
26
     New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
27
        $vm2
```

12. 仮想マシンを構成する

両方の NetScaler VPX インスタンスが開始された場合、SSH プロトコル経由で両方の VPX インスタンスに 接続して仮想マシンを構成します。

a) アクティブ-アクティブ: 両方の NetScaler VPX インスタンスのコマンドラインで同じ構成コマンドセット を実行します。

b) アクティブ/パッシブ: このコマンドを両方の NetScaler VPX インスタンスのコマンドラインで実行します。

add ha node #nodeID <nsip of other NetScaler VPX>

アクティブ-パッシブモードでは、プライマリノードでのみ構成コマンドを実行します。

Azure で VPX インスタンスのサポートチケットを作成する

January 15, 2025

Azure 上の NetScaler VPX インスタンスで問題が発生している場合は、トラブルシューティングのために、 NetScaler サポートポータル.

サポート チケットを提出するには、次のことを確認してください。

- ネットワークが接続されています。
- Azure アカウント番号、Azure にデプロイした NetScaler サブスクリプションベースの製品のサポート PIN コード、および Azure シリアルログが手元にあります。
 - サポート PIN コードは、システムページ VPX GUI で。

Dashboard Conf	figuration	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 255.255.255.0	
High Availability		Node Standalone	
NTP Servers		Technical Support PIN	
Reports		Time Zone Coordinated Universal Time	
		Last Config Changed Time Eri 24 Nov 2023 09:55:45 UTC	
Reporting Configs		Last Config Gaved Time Fri 24 Nov 2023 09:56:00 ITC	
Profiles			
Destition Administration		Hardware Information	

- シリアル ログは、Azure ポータル (ブート診断 セクションに貼り付けます)。

O Search «	💍 Refresh 🛛 🔯 Settings 🧷 Troubleshoot
Policies	
Run command	Screenshot Serial log
onitoring	Updated: Friday, 8 September 2023 at 6:15:06 AM UTC Download serial log
Insights	مات باب باب باب باب باب باب باب
Alasta	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Alerts	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Metrics	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
Diagnostic settings	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Logs	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
5-	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-
Connection monitor (classic)	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Workbooks	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
WORDOOKS	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
tomation	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
Tasks (preview)	-\/-\/-\//-\//-\//-\//-\//-\//-\//-\//-
	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Export template	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
lp	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Pesource health	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-
Resource fieditif	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /
Boot diagnostics	-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /-\ /

すべての情報の準備ができたら、NetScaler サポートに電話してください。名前とメールアドレスを入力するよう求められます。

Azure に関するよくある質問

October 17, 2024

• Azure Marketplace からインストールされた NetScaler VPX インスタンスのアップグレード手順は、オ ンプレミスアップグレード手順とは異なりますか?

いいえ。標準の NetScaler VPX アップグレード手順を使用して、Microsoft Azure クラウド内の NetScaler VPX インスタンスを NetScaler VPX リリース 11.1 以降にアップグレードできます。GUI または CLI の手順を使用してアップグレードできます。新規インストールの場合は、Microsoft Azure クラウド用の Citrix ADC VPX イメージを使用します。

NetScaler VPX アップグレードビルドをダウンロードするには、「**NetScaler** ダウンロード」>「NetScaler ファームウェア ** 」に移動します。

• Azure でホストされている Citrix ADC VPX インスタンスで観察される MAC 移動とインターフェイスミュ ートを修正するにはどうすればよいですか?

Azure マルチ NIC 環境では、デフォルトでは、すべてのデータインターフェイスに MAC 移動とインターフェ イスのミュートが表示されることがあります。Azure 環境で MAC が移動したりインターフェイスがミュート されたりしないように、NetScaler VPX インスタンスのデータインターフェイス(タグなし)ごとに VLAN を作成し、NIC のプライマリ IP を Azure にバインドすることを Citrix では推奨しています。

詳細については、CTX224626の記事を参照してください。

Google Cloud Platform AD NetScaler ADC VPX ADD

January 30, 2025

NetScaler VPX インスタンスを Google Cloud Platform (GCP) にデプロイできます。GCP の VPX インスタン スを使用すると、GCP クラウドコンピューティング機能を活用し、ビジネスニーズに合わせて Citrix の負荷分散機 能とトラフィック管理機能を使用できます。VPX インスタンスを GCP にスタンドアロンインスタンスとしてデプロ イできます。シングル NIC 構成とマルチ NIC 構成の両方がサポートされています。

サポートされる機能

Premium、Advanced、Standard のすべての機能は、使用されているライセンス/バージョンタイプに基づいて GCP でサポートされます。

制限事項

• IPv6 はサポートされていません。

ハードウェア要件

GCP の VPX インスタンスには、最低 2 つの vCPU と 4 GB の RAM が必要です。

注意事項

デプロイを開始する前に、次の GCP 固有の点を考慮してください。

- インスタンスの作成後は、ネットワークインターフェイスの追加や削除はできません。
- マルチ NIC デプロイの場合は、NIC ごとに個別の VPC ネットワークを作成します。1つの NIC を関連付ける ことができるネットワークは1つだけです。

- シングル NIC インスタンスの場合、GCP コンソールはデフォルトでネットワークを作成します。
- 2 つ以上のネットワークインターフェースを持つインスタンスには、最低 4 つの vCPU が必要です。
- IP 転送が必要な場合は、インスタンスの作成と NIC の設定中に IP 転送を有効にする必要があります。

シナリオ:マルチ NIC、マルチ IP のスタンドアロン NetScaler VPX インスタンスを展開する

このシナリオでは、NetScaler VPX スタンドアロンインスタンスを GCP にデプロイする方法を示しています。この シナリオでは、多数の NIC を持つスタンドアロン VPX インスタンスを作成します。インスタンスはバックエンドサ ーバー (サーバーファーム) と通信します。



次の目的に応える NIC を 3 つ作成します。

		VPC ネットワークに関連付けられて
NIC	目的	いる
NIC 0	管理トラフィック(NetScaler IP) にサービスを提供する	管理ネットワーク
NIC 1	クライアント側のトラフィック	クライアントネットワーク
NIC 2	(VIP)をサービスする バックエンド・サーバ(SNIP)との	バックエンドサーバーネットワーク
	通信	

次の間の必要な通信ルートを設定します。

- NetScaler VPX インスタンスとバックエンド サーバー。
- NetScaler VPX インスタンスとパブリック インターネット上の外部ホスト。

導入手順の概要

- 1. 3 つの異なる NIC に対して 3 つの VPC ネットワークを作成します。
- 2. ポート 22、80、および 443 のファイアウォールルールを作成します。
- 3.3 つの NIC を持つインスタンスを作成します。

GCP マーケットプレイスから NetScaler VPX インスタンスを選択します。

注

VPC ネットワークを作成したのと同じリージョンにインスタンスを作成します。

手順 1. 手順 1: VPC ネットワークを作成する.

管理 NIC、クライアント NIC、およびサーバー NIC に関連付けられた 3 つの VPC ネットワークを作成します。VPC ネットワークを作成するには、**Google** コンソール > ネットワーク > **VPC** ネットワーク > **VPC** ネットワークの作成 にログオンします。スクリーン・キャプチャに示されている必須フィールドに入力し、「作成」をクリックします。

- Cr	eate a VPC network	
Name 🕜		
vpxmgmt		
Description	(Optional)	
managen	ient ypc	
Subnets		
Subnets let Automatic t subnets. Le	you create your own private cloud topology within Google Cloud. Click o create a subnet in each region, or click Custom to manually define the arn more	
Subnet crea	ltion mode	
Custom	Automatic	
New subn	et 🥫	^
Nama 🗿		
voxman	itsubnet	
*Pxiligi		
Add a des	cription	
Region 🔞		
asia-eas	t1	-
IP addres		
192 168	30 0/24	
Create se	ondary IP range	
Private Go	ogle access 📀	
🔘 On		
On Off		
OnOffFlow logs		
 On Off Flow logs On 		
 On Off Flow logs On Off 		
 On Off Flow logs On Off Done 	Cancel	
 On Off Flow logs On Off Off 	Cancel	
 On Off Flow logs On Off Done 	Cancel + Add subnet	
On Off Flow logs On Off On Off Done Dynamic ro Region	Cancel Add subnet	
 On Off Flow logs On Off Done 	Cancel Add subnet Add subnet Sting mode	
On Off Flow logs On Off Done Done Cloud R Global Global r VPN or	Cancel Add subnet Add subnet Iting mode al Duters will learn routes only in the region in which they were created puting lets you dynamically learn routes to and from all regions with a sin interconnect and Cloud Router	ngle
 On Off Flow logs On Off Done Done 	Cancel Add subnet Uting mode al Duters will learn routes only in the region in which they were created Duting lets you dynamically learn routes to and from all regions with a sin nterconnect and Cloud Router	ngle

同様に、クライアント側およびサーバー側 NIC 用の VPC ネットワークを作成します。

注

3 つの VPC ネットワークはすべて同じリージョン (このシナリオでは asia-east1) にある必要があります。

手順 3. ポート 22、80、および 443 のファイアウォールルールを作成します。

VPC ネットワークごとに SSH (ポート 22)、HTTP (ポート 80)、HTTPS (ポート 443) のルールを作成します。フ ァイアウォールルールの詳細については、「ファイアウォールルールの概要」を参照してください。

😔 netscaler-vp	x-platform-eng 👻
← Create	a firewall rule
Firewall rules con incoming traffic f	trol incoming or outgoing traffic to an instance. By default, rom outside your network is blocked. Learn more
Name 🕜	
vpxmgmtingress	srule
Description (Option	nal)
management tra	ffic ingress rules
Logs Turning on firewall Stackdriver. Learn r On	ogs can generate a large number of logs which can increase costs in nore
Off	
Network	
vpxmgmt	•
Priority 🕜 Priority can be 0 - 6	5535 Check priority of other firewall rules
1000	
Ingress Egress Action on match Allow Deny Targets	
All instances in t	he network 👻
Source filter 🕜	
IP ranges	•
Source IP ranges	0
0.0.0/0 😢	
Out and a survey film	
None	er 🕑
None	
Protocols and port Allow all Specified prot	s 😨
🗹 tcp :	22, 80, 443
udp :	all
Other pro	tocols
protoco	ols, comma separated, e.g. ah, sctp
Y Dischla mile	
 Disable rule 	
Create	el

手順 3. VPX インスタンスにサービスまたはサービスグループを追加します。

- 1. GCP コンソールにログインします。
- 2. GCP マーケットプレイスに移動します。
- 3. 要件に基づいてサブスクリプションを選択してください。

≡ Google Cloud			
🖄 Marketplace			Q NetScaler VPX X
Marketplace > "NetScaler VF	PX"		
Marketplace home		2 results	
★ Your products		netscaler	NetScaler VPX FIPS - Customer Licensed
★ Your orders		The Discardi	curx 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	^		NetScaler VPX - Customer Licensed
Security	(1)	net>scaler	Citrix Systems, Inc.
Networking	(2)		NetScaler (formerly Citrix ADC) is an enterprise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to meet your business' unique needs. Designed to provide operational consistency and a smooth user experience, NetScaler eases your transition to the hybrid cloud. Why NetScaler Offers high performance with fast application
Туре	^		
Virtual machines	(2)		
Price	^		
BYOL	(2)		

4. 選択したサブスクリプションで [起動]をクリックします。

net>scaler	NetScaler VPX - Customer Licensed				
	NetScaler: Lo	ad Balancer, SSL VPN, V	WAF & SSO		
	LAUNCH	VIEW DEPLOYMENTS	CONTACT SALES		
I	Click to configure				

5. デプロイフォームに必要事項を記入し、「デプロイ」をクリックします。

注 ステップ **1** で作成した VPC ネットワークを使用します。

6. デプロイされたインスタンスは Compute Engine > VM インスタンスの下に表示されます。

GCP SSH またはシリアルコンソールを使用して VPX インスタンスを構成および管理します。

シナリオ:シングル NIC のスタンドアロン VPX インスタンスをデプロイする

このシナリオでは、NetScaler VPX スタンドアロンインスタンスを単一の NIC で GCP にデプロイする方法を示しています。エイリアス IP アドレスは、この展開を実現するために使用されます。



1つの NIC (NIC0) を作成して、次の目的を果たします。

- 管理ネットワーク内の管理トラフィック(NetScaler IP)を処理します。
- クライアントネットワーク内のクライアント側トラフィック (VIP) を処理します。
- バックエンドサーバーネットワーク内のバックエンドサーバー (SNIP) と通信します。

次の間の必要な通信ルートを設定します。

- インスタンスとバックエンドサーバー。
- パブリックインターネット上のインスタンスと外部ホスト。

導入手順の概要

- 1. NIC0 用の VPC ネットワークを作成します。
- 2. ポート 22、80、および 443 のファイアウォールルールを作成します。
- 3.1 つの NIC でインスタンスを作成します。
- 4. VPX にエイリアス IP アドレスを追加します。
- 5. VPX に VIP と SNIP を追加します。
- 6. 負荷分散仮想サーバーを追加します。
- 7. インスタンスにサービスまたはサービスグループを追加します。
- 8. サービスまたはサービスグループをインスタンス上の負荷分散仮想サーバーにバインドします。

注

VPC ネットワークを作成したのと同じリージョンにインスタンスを作成します。

手順 1. 手順 1: 1 つの VPC ネットワークを作成します。

NIC0 に関連付ける VPC ネットワークを1つ作成します。

VPC ネットワークを作成するには、次の手順を実行します。

- 1. GCP コンソール > ネットワーク > VPC ネットワーク > VPC ネットワークの作成にログオンします。
- 2. 必須フィールドに入力し、[Create] をクリックします。

netsc	aler-vpx-platform-eng 👻	
← Ci	eate a VPC network	
Name 🛞		
vpxmgm	t	
Descriptio	(Optional)	
manager	ment ypp	
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. Le	arn more	
Subnet cre	ation mode	
Custom	Automatic	
New sub	net	^
Name 💿		
vpxmgr	ntsubnet	
Add a de	scription	
Region	9	
asia-ea	st1	×
IP addres	s ranne 💿	
192.16	3.30.0/24	
Create se	condary IP range	
Private G	oogle access 🛞	
On		
Ö off		
F 1		
Flow logs		
On Off		
Deep	Ormat	
Done	Cancel	
		_
	+ Add subnet	
Dynamic n	auting mode 💿	
Region	al	
Cloud I Global	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 sin	çle
VPN or	interconnect and Cloud Router	
Consta	Cascal	
create	Cancer	

手順 3. ポート 22、80、および 443 のファイアウォールルールを作成します。

VPC ネットワークの SSH (ポート 22)、HTTP (ポート 80)、HTTPS (ポート 443) のルールを作成します。ファイ アウォールルールの詳細については、「ファイアウォールルールの概要」を参照してください。

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
vescription (optional)
management trainc ingress rules
Logs Turning on frewall logs can generate a large number of logs which can increase costs in Stackdriver, Learn more
• 011
Network
Priority @ Priority of the priority of the finewall rules
1000
 Egress Action on match ⊕ Allow Dony Targets ⊕
All instances in the network *
Source filter 💿
IP ranges *
Source IP ranges 💿
0.0.0.0/0 🕲
Second source filter
None
Protocols and ports Allow all Specified protocols and ports Ver: 22, 80, 443 up: an
Other protocols
protocols, comma separated, e.g. ah, sctp
X. Disable rule
 Disable rule
Create Cancel

手順 3. 手順 3: 1 つの NIC でインスタンスを作成します。

単一の NIC でインスタンスを作成するには、次の手順を実行します。

- 1. **GCP** コンソールにログインします。
- 2. [コンピュート]で[** コンピュートエンジン]にカーソルを合わせ、[** イメージ]を選択します。
- 3. イメージを選択し、[インスタンスの作成]をクリックします。

۲	Compute Engine	Images	[+] CREATE IMAGE	C REFRESH	CREATE INSTANCE]	⊖ DEPRECAT
	VM instances						
я <mark>я</mark> а	Instance groups	= Filter image	s			0	Columns 🔻
	Instance templates						
8	Sole tenant nodes	<< Previous	2 Next >>				
۵	Disks	Name		Size	Created by		
٥	Snapshots	✓ ✓ nsvpx-12-1	-50-9	20 GB			
[II]	Images						

4. 2 つの vCPU を持つインスタンスタイプを選択します (ADC の最小要件)。

÷	Create an instance		
To cr	eate a VIM instance, select one of the options:		Name () Name is permanent
R	New VM Instance Create a single VM instance from scratch	>	Labels © (Optional) shutdown : 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 v
E Ž	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	ŧ	Machine configuration 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 platform or one of its predecessors Machine type
			n1-standard-2 (2 vCPU, 7.5 GB memory) vCPU Memory GPUs 2 7.5 GB CPU platform and GPU Confidential VM service Enable the Confidential Computing service on this VM instance. Container Deploy a container image to this VM instance. Learn more

- 5. [管理、セキュリティ、ディスク、** ネットワーク]ウィンドウから[ネットワーク**]タブをクリックします。
- 6. [ネットワークインターフェイス]で、[編集]アイコンをクリックして、デフォルトの NIC を編集します。
- 7. [ネットワークインターフェイス] ウィンドウの [ネットワーク] で、作成した VPC ネットワークを選択しま す。
- 8. 静的外部 IP アドレスを作成できます。[外部 IP アドレス]で、[**IP アドレスの作成 **]をクリックします。
- 9. [静的アドレスを予約]ウィンドウで、名前と説明を追加し、[予約]をクリックします。
- 10. [作成] をクリックして VPX インスタンスを作成します。新しいインスタンスが [VM インスタンス] の下に表示されます。新しいインスタンスが VM インスタンスの下に表示されます。

手順 4: VPX インスタンスに VIP と SNIP を追加します。

VIP アドレスと SNIP アドレスとして使用する VPX インスタンスに 2 つのエイリアス IP アドレスを割り当てます。

注

VPX インスタンスのプライマリ内部 IP アドレスを使用して VIP または SNIP を構成しないでください。

エイリアス IP アドレスを作成するには、次の手順を実行します。

1. VM インスタンスに移動し、[編集] をクリックします。

- 2. [ネットワークインターフェイス] ウィンドウで、NICO インターフェイスを編集します。
- 3. [エイリアス IP 範囲] フィールドに、エイリアス IP アドレスを入力します。

✓ M instance details
 ✓ EDI
 ✓ RESET
 CREATE MACHINE IMAGE
 © CREATE

Network interface

 Network interface

 Vou must stop the VM instance to edit network, subnetwork or internal IP address

 Network @

 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)	٠	192.168.1.3/32	×
Primary (192.168.1.0/24)	٠	192.168.1.7/32	×
	+ Add	IP range	
☆ Hide alias IP ranges			
External IP			
Ephemeral			
Network Service Tier			
	ect-lev	vel tier, change) 💿	
 Premium (Current proj Standard (us-east1) (9		
Premium (Current proj Standard (us-east1) IP forwarding	9		

- 4. [完了]、[保存]の順にクリックします。
- 5. VM インスタンスの詳細ページでエイリアス IP アドレスを確認します。

< \	/M instance details	10	DIT ORESET	CREATE MACHINE IMAG	DE 🛛 🐴 CREATE SIMILAR	STOP	II SUSPEND	DELET
III Erab	le connecting to serial ports)						
Logs Doud Lo	acina							
Serial po	rt 1 (console)							
© More								
Instance	M							
2543534	HHHEL01003122							
mi-stand	type last-2 (2 vCPUs, 7.5 68 memory	6						
Reservab	an .							
Automat	ically choose							
CPUpiat	farm.							
miller	tard							
Display d Turn on a	ievice I display device illyce want to use :	ecnien capturing in	nd recording tools.					
11 Tarr	en-display device.							
Zane								
10 10011								
Labels								
Dreation 1	5me							
140 22, 3	ALCO, BETWEET PAR							
Name	Network	Submativerk	Primary internal IP	Alias IP ranges	External IP	Network Tiler (i)	IP forwarding	Network details
nicū	automationingentretwork	ingritaubeet	192.168.1.50	192.148.1.3/32, 192.168.1.7/32	106.196.190.91 (sphemoral)	Premium	Off	View details
Partie 14	I PTR Decard							
None								

手順 5: VPX インスタンスに VIP と SNIP を追加します。

VPX インスタンスで、クライアントエイリアス IP アドレスとサーバーエイリアス IP アドレスを追加します。

1. NetScaler GUI で、[システム] > [ネットワーク] > [IP] > [IPv4] に移動し、[追加] をクリックします。

CİİTIX.) from	Market	place							HA Status Not configured	Partition 😞 defeuit	naraet 🗸
Dashboard Configuration Reporting Documentation Downloads											¢
Q, Search in Menu		System > Net	work > IPs >	PV4s							
Google Cloud Platform	>	IDe									0.0
Bystem	~	IPS									~ •
Licenses		IPV4s 🛐	IPV8x 1								
Sottings		444	-	Constantion Mat	an Astronya						
Diagnostics											
High Availability	>	Q Clickhere I	o sevencia or scale cau	enter Key : Value Iorrial							O
NTP Servers			IP AEDRESS	STATE 1	TIPE	I MODE D	A82 1	ICMP 3	VIELAL SERVER	TRAFFIC	DOMAIN I
Reports			192.168.17	ENABLED	Sabrel P	Active	ENABLED	ENABLED	-10.4-		D
Profiles			192.168.1.3	ENABLED	Vetual IP	Action	ENABLED	ENABLED	ENABLED		D
Partition Administration	>		192.168.150	ENABLED	NetScelar P	Active	ENABLED	ENABLED	-10.6-		D
User Administration	>	Total 3							25 Per Page	V Page 1 e	n
Authentication	>										
Auditing	2										

- 2. クライアントエイリアス IP(VIP)アドレスを作成するには、次の手順を実行します。
 - VM インスタンスで VPC サブネットに設定されたクライアントエイリアス IP アドレスとネットマスク を入力します。
 - [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - [**Create**] をクリックします。
- 3. サーバーエイリアス IP (SNIP) アドレスを作成するには、次の手順を実行します。
 - VM インスタンスの VPC サブネットに設定されたサーバーエイリアス IP アドレスとネットマスクを入 力します。
 - [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。

• [Create] をクリックします。

手順 6: サービス/サービスグループをインスタンス上の負荷分散仮想サーバーにバインドします。

- 1. NetScaler GUI で、[構成] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動し、[追加] をク リックします。
- 2. [名前]、[プロトコル]、[IP アドレスタイプ (IP アドレス)]、[IP アドレス] (クライアントエイリアス IP)、および [ポート] に必要な値を追加します。
- 3. OK をクリックして、負荷分散仮想サーバーを作成します。

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Virtual Server

Create a virtual server by specifi IP address. If the application is a You can configure multiple virtu	(ng a sama, an IP address, a part, and a portood (yes. The application is accessible from the internet, the virtual server IP (VP) addressible eccessible only from the local area network (LAN) or wide area network (VAN). the VP is usually a private (IAN) non-mutable) IP address. Is servers to review of both results. Therefore increasing the private limits in the survey is preven to receive their security.	s public
Name*	a no en el concercio sobre estretesta con esta e concerció de conservado en conservado en processo en esta esta	
vser1	0	
Protocol*		
нттр	v	
IP Address Type*		
IP Addresses	~	
P Address*		
192.168.1.3	0	
Part*		
80	0	
Mare		

手順 7: VPX インスタンスにサービスまたはサービス グループを追加します。

- 1. NetScaler GUI から、[構成]> [トラフィック管理] > [負荷分散] > [サービス] に移動し、[追加] をクリ ックします。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、「**OK**」をクリックします。
- 手順8:サービス/サービス グループをインスタンス上の負荷分散仮想サーバーにバインドします。
 - 1. GUI から、[設定]>[トラフィック管理]>[負荷分散]>[仮想サーバ]に移動します。
 - 2. 手順6で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
 - 3. [サービスとサービスグループ]ウィンドウで、[負荷分散仮想サーバーサービスのバインドなし]をクリック します。
 - 4. ステップ**7**で設定したサービスを選択し、[バインド(Bind)]をクリックします。

VPX インスタンスを GCP にデプロイした後の注意点

 ユーザー名nsrootとインスタンス ID をパスワードとして VPX にログオンします。プロンプトで、パスワ ードを変更し、設定を保存します。

- テクニカルサポートバンドルを収集するには、慣例show techsupportではなくコマンドshell / netscaler/showtech_cloud.plを実行します。
- GCP コンソールから NetScaler ADC VM を削除した後、関連する NetScaler ADC 内部ターゲットインスタンスも削除します。これを行うには、gcloud CLI に移動し、次のコマンドを入力します。

注

<instance-name>-adcinternalは、削除する必要があるターゲットインスタン スの名前です。

NetScaler VPX ライセンス

GCP 上の NetScaler VPX インスタンスには、有効なライセンスが必要です。GCP 上で実行される NetScaler VPX インスタンスで使用できるライセンスオプションは次のとおりです。

ライセンス持ち込み (BYOL): BYOL オプションを使用するには、次の手順を実行します。

- NetScaler Web サイトのライセンスポータルを使用して、有効なライセンスを生成します。
- 生成されたライセンスをインスタンスにアップロードします。
- NetScaler VPX チェックインおよびチェックアウトライセンス: このライセンス モデルでは、使用可能なラ イセンスのプールからライセンスをチェックアウトし、不要になったときに再度チェックインできます。詳細 および詳細な手順については、以下を参照してください。NetScaler VPX チェックインおよびチェックアウ トライセンス.

サブスクリプションベースのライセンスは、GCP 上の NetScaler VPX インスタンスではサポートされなくなりました。

GCP でサポートされる NetScaler VPX 製品

次の表に、GCP でサポートされている NetScaler VPX 製品を示します。

サポートされている VPX オファリング

NetScaler VPX - 顧客ライセンス

NetScaler VPX FIPS - 顧客ライセンス

注

サポートされている GCP マシンタイプ ファミリー

マシンタイプファミリー	最小マシンタイプ
汎用機械	e2-中、e2-標準-2、e2-高メモリ-2、n1-標準-2、n1-高
	メモリ-2、n2-標準-2、n2-高メモリ-2、n2d-標準-2、 n2d-高メモリ-2
コンピューティング最適化マシン	c2-標準-4、c2d-標準-2、c2d-ハイメモリ-2

NetScaler VPX インスタンスを展開するための GDM テンプレート

NetScaler VPX Google デプロイメントマネージャー(GDM)テンプレートを使用して、GCP に VPX インスタン スを展開できます。詳細については、NetScaler GDM テンプレートを参照してください。

リソース

- 複数のネットワークインターフェースを持つインスタンスの作成
- VM インスタンスの作成と起動

関連情報

• VPX の高可用性ペアを Google Cloud Platform に展開する

VPX の高可用性ペアを Google Cloud Platform に展開する

October 17, 2024

Google Cloud Platform (GCP) 上の2つの NetScaler ADC VPX インスタンスを、高可用性 (HA) アクティブ/パ ッシブペアとして構成できます。1つのインスタンスをプライマリノードとして構成し、もう1つをセカンダリノー ドとして設定すると、プライマリノードは接続を受け入れ、サーバーを管理します。セカンダリノードはプライマリ を監視します。何らかの理由で1次ノードが接続を受け入れることができない場合、2次ノードが引き継ぎます。

HA の詳細については、「高可用性」を参照してください。

ノードは同じリージョンにある必要がありますが、同じゾーンまたは異なるゾーンにある可能性があります。詳細に ついては、「リージョンとゾーン」を参照してください。

各 VPX インスタンスには、少なくとも 3 つの IP サブネット(Google VPC ネットワーク)が必要です。

- 管理サブネット
- クライアント側サブネット (VIP)
- バックエンド向けサブネット (SNIP、MIP など)

Citrix では、標準の VPX インスタンスには3つのネットワークインターフェイスを推奨しています。

VPX 高可用性ペアは、次の方法でデプロイできます。

- 外部静的 IP アドレスの使用
- プライベート IP アドレスの使用
- プライベート IP アドレスを持つシングル NIC 仮想マシンの使用

VPX 高可用性ペアを GCP にデプロイするための GDM テンプレート

NetScaler Google デプロイメントマネージャー(GDM)テンプレートを使用して、GCP に VPX 高可用性ペアを展 開できます。詳細については、NetScaler GDM テンプレートを参照してください。

GCP での VPX 高可用性ペアの転送ルールのサポート

転送ルールを使用して、GCP に VPX 高可用性ペアをデプロイできます。

転送ルールの詳細については、「転送ルールの概要」を参照してください。

前提条件

- 転送ルールは、VPX インスタンスと同じリージョンにある必要があります。
- ターゲットインスタンスは、VPX インスタンスと同じゾーンにある必要があります。
- プライマリノードとセカンダリノードの両方のターゲットインスタンスの数が一致する必要があります。

例

us-east1 リージョンに高可用性ペアがあり、プライマリ VPX が us-east1-b ゾーンにあり、セカンダリ VPX が us-east1-c ゾーンにあります。us-east1-b ゾーンにターゲットインスタンスがあるプライマリ VPX に対して転送ルールが設定されます。us-east1-c ゾーンでセカンダリ VPX のターゲットインスタンスを構成して、フェイルオーバー時に転送ルールを更新します。

制限事項

VPX 高可用性デプロイメントでは、バックエンドでターゲットインスタンスを使用して構成された転送ルールのみが サポートされます。 **Google Cloud Platform** に外部の静的 **IP** アドレスを指定した **VPX** 高可用性ペアを デプロイする

October 17, 2024

VPX ハイアベイラビリティペアは、外部の静的 IP アドレスを使用して GCP にデプロイできます。プライマリノード のクライアント IP アドレスは、外部の静的 IP アドレスにバインドする必要があります。フェールオーバー時に、外 部静的 IP アドレスがセカンダリノードに移動され、トラフィックが再開されます。

静的外部 IP アドレスは、プロジェクトを解放するまでプロジェクト用に予約されている外部 IP アドレスです。IP ア ドレスを使用してサービスにアクセスする場合、その IP アドレスを予約して、プロジェクトのみが使用できるように することができます。詳細については、「静的外部 IP アドレスの予約」を参照してください。

HA の詳細については、「高可用性」を参照してください。

はじめに

- Google Cloud Platform に NetScaler VPX インスタンスをデプロイするに記載されている制限事項、ハー ドウェア要件、注意事項をお読みください。この情報は、HA 配置にも適用されます。
- GCP プロジェクトで クラウドリソースマネージャー API を有効にします。

Service account 🕜	
Compute Engine	default service account
 Allow full acces Set access for 	each API

- インスタンスの作成中に、すべての Cloud API へのフルアクセスを許可します。
- GCP サービスアカウントに関連付けられた IAM ロールに次の IAM 権限があることを確認します。

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]
- 管理インターフェイス以外のインターフェイスでエイリアス IP アドレスを設定している場合は、GCP サービ スアカウントに次の追加の IAM 権限があることを確認してください。

```
1 "compute.instances.updateNetworkInterface"
```

• プライマリノードで GCP 転送ルールを構成している場合は、GCP 上の VPX 高可用性ペアの転送ルールのサポート に記載されている制限と要件を読んで、フェイルオーバー時に新しいプライマリに更新してください。

Google Cloud Platform に VPX HA ペアを展開する方法

HA 展開手順の概要を次に示します。

- 1. 同じリージョンに VPC ネットワークを作成します。たとえば、アジア東です。
- 同じリージョンに2つのVPXインスタンス(プライマリノードとセカンダリノード)を作成します。それらは、同じゾーンまたは異なるゾーンに存在することができます。たとえば、アジア東-1a、アジア東-lb。
- 3. NetScaler GUI または ADC CLI コマンドを使用して、両方のインスタンスで高可用性設定を構成します。

手順 1. 手順 1: VPC ネットワークを作成する

要件に基づいて VPC ネットワークを作成します。管理 NIC、クライアント NIC、サーバー NIC に関連付けるために 3 つの VPC ネットワークを作成することをお勧めします。

VPC ネットワークを作成するには、次の手順を実行します。

- 1. Google コンソールにログインし、[ネットワーク]>[VPC ネットワーク]>[VPC ネットワークの作成] をク リックします。
- 2. 必須フィールドに入力し、[Create] をクリックします。

詳細については、「Google Cloud Platform に NetScaler VPX インスタンスをデプロイする」の「**VPC** ネットワ ークの作成」セクションを参照してください。

手順 3. 手順 2:2 つの VPX インスタンスを作成する

シナリオ: マルチ NIC、マルチ IP のスタンドアロン VPX インスタンスをデプロイするに記載されている手順に従っ て、2 つの VPX インスタンスを作成します。

重要:

プライマリノードのクライアント IP アドレス (VIP) に静的外部 IP アドレスを割り当てます。既存の予約済み IP アドレスを使用するか、新しい予約済み IP アドレスを作成できます。静的外部 IP アドレスを作成するには、 [ネットワークインターフェイス] > [外部 IP] に移動し、[IP アドレスの作成] をクリックします。

Network interface	^
Network	
clientvpc-ss	
Subnetwork	
clientvpc-ss-subnet	
Internal IP	
Industry of UD down	
Internal IP type	
Ephemeral	•
X. Chevy elice ID reason	
Show allas iP ranges	
External IP	
None	
Feb and a lateral late	
Ephemeral	
vpxpublic (35.229.255.208)	
Premium tier	-
Create IP address	
<"D	

フェールオーバー後、古いプライマリが新しいセカンダリになると、スタティック外部 IP アドレスは古いプライマリ から移動し、新しいプライマリに接続されます。詳細については、Google Cloud ドキュメント「静的外部 IP アド レスを予約する」を参照してください。

VPX インスタンスを構成したら、VIP アドレスと SNIP アドレスを構成できます。詳細については、「Citrix ADC 所 有の IP アドレスの構成」を参照してください。 手順3.高可用性の構成

Google Cloud Platform でインスタンスを作成した後、CLI 用 Citrix ADC GUI を使用して HA を構成できます。

GUI を使用した HA の設定 ステップ 1. 両方のインスタンスで INC モードで高可用性をセットアップします。

プライマリノードで、次の手順を実行します。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2.構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノードの IP アドレス] フィールドに、セカンダリノードの管理 NIC のプライベート IP アドレスを 入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [Create] をクリックします。

先に進む前に、[Nodes]ページにセカンダリノードの同期状態が SUCCESS と表示されていることを確認してくだ さい。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2.構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノード IP アドレス] フィールドに、プライマリノードの管理 NIC のプライベート IP アドレスを入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [**Create**] をクリックします。

セカンダリノードで、次の手順を実行します。

System / Hi	System / High Availability / Nodes											
Nodes	2										C F	
Add	Edit	Delete	Statistics	Select Action $ \checkmark $								
	ID ¢	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC \Diamond	SYNCHRONIZATION S	STATE 0	SYNCHRON	NIZATION 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 Pa	ge 🗸	Page 1 of 1	•	
~												

注

これで、セカンダリノードは、プライマリノードと同じログオン資格情報を持ちます。

ステップ 2. 両方のノードに仮想 IP アドレスとサブネット IP アドレスを追加します。

プライマリノードで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. 次の手順に従って、プライマリ VIP アドレスを追加します。
 - a) セカンダリインスタンスのクライアント側インターフェイスの内部 IP アドレスと、VM インスタンスの クライアントサブネットに設定されたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [**Create**] をクリックします。
- 3. 次の手順に従って、プライマリ SNIP アドレスを追加します。
 - a) セカンダリインスタンスのサーバ側インターフェイスの内部 IP アドレスと、セカンダリインスタンスの サーバサブネットに設定されたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [Create] をクリックします。
- 4. 次の手順に従って、セカンダリ VIP アドレスを追加します。
 - a) プライマリ・インスタンスのクライアント側インターフェイスの内部 IP アドレスと、VM インスタンス のクライアント・サブネットに対して構成されたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [**Create**] をクリックします。

	_	
		-
		C
	-	_
		~

IPV4s (4) IPV6s (1)											
Add Edit Delete Statistics Select Action ~											
Q Click here to search or you can enter Key : Value format											
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP	ICMP 0	VIRTUAL SERVER	TRAFFIC DOMAIN			
Secondary VIP	192.168.2.54	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLED		0		
Primary SNIP	192.168.3.7 ENABLED Subnet IP Active		Active	ENABLED	ENABLED	-N/A-					
Primary VIP	192.168.2.37	37 ENABLED Virtual IP Active ENABLED ENABLED		ENABLED	ENABLED		0				
	192.168.1.3	ENABLED NetScaler IP Active ENABLED ENABLED		ENABLED	-N/A-		0				
Total 4							25 Per Page ∨ Pag	e 1 of 1 🔍	$\left \cdot \right $		

先に進む前に、[Nodes]ページにセカンダリノードの同期状態が SUCCESS と表示されていることを確認してくだ さい。

- 1. System > Network > IP Sets > Add に移動します。
- 2. 次の手順に従って、セカンダリ VIP アドレスを追加します。
 - a) プライマリ・インスタンスのクライアント側インターフェイスの内部 IP アドレスと、VM インスタンス のクライアント・サブネットに対して構成されたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
- 3. 次の手順に従って、セカンダリ SNIP アドレスを追加します。
 - a) プライマリ・インスタンスのサーバ側インターフェイスの内部 IP アドレスと、プライマリ・インスタン スのサーバ・サブネットに対して構成されたネットマスクを入力します。

b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
c) [Create] をクリックします。

IPs									
IPV4s 3	IPV6s 1								
Add E	dit Delete	Statistics	Select Action 🗸						
\mathbf{Q} Click here to	search or you can enter	Key : Value format							(j)
	IP ADDRESS	STATE 0	TYPE 🗘	MODE 0	ARP	CMP	UIRTUAL SERVER	TRAFFIC DOMAIN	
Secondary SNIP	192.168.3.76	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-		0
Secondary VIP	192.168.2.54	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED		0
	192.168.1.66	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-		0
Total 3							25 Per Page →	Page 1 of 1 4	•

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。IP セットを追加し、両方のインスタンスで IP セットをセカンダリ VIP にバインドします。

プライマリノードで、次の手順を実行します。

- 1. ステップ 2: 両方のインスタンスに IP セットを追加します。
- 2. IP セット名を追加し、[Insert] をクリックします。
- 3. [IPv4] ページで、仮想 IP(セカンダリ VIP)を選択し、[挿入] をクリックします。
- 4. [Create] をクリックして IP セットを作成します。

Citrix ADC VP	Citrix ADC VPX Express (Freemium)										oot ~
Dashboard	Configuration	Reporting	Documentation	Downloads							¢
G Create IP	Set	IPV4s	0								С×
Name*		Add	Edit Delete	Statistics	Select Action ~						
ipset1		Q Click her	e to search or you can enter Ke	y : Value format							()
Traffic Domain			IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE :	MODE 0	ARP :	ICMP	VIRTUA
		Ade	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-
Course Lower			192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Active	ENABLED	ENABLED	ENABLE
Insert Dele		Total 4						25 Per Pa	ge 🗸 Page	1 of 1	
No items		Inste	Close								
Create											
										(0

先に進む前に、[Nodes]ページにセカンダリノードの同期状態が SUCCESS と表示されていることを確認してくだ さい。

- 1. ステップ 2: 両方のインスタンスに IP セットを追加します。
- 2. IP セット名を追加し、[**Insert**] をクリックします。
- 3. [IPv4]ページで、仮想 IP(セカンダリ VIP)を選択し、[挿入]をクリックします。
- 4. [Create] をクリックして IP セットを作成します。

NetScaler VPX 14.1

Dashboard Configuration Re	porting Docum	entation	Downloads		*********					¢
G Create IP Set	IPV4s 3									С×
Name*	Add Edit	Delete	Statistics	Select Action >>						
ipset1	Q Click here to search or	r you can enter Key	: Value format							()
Traffic Domain		IP ADDRESS	TRAFFIC DOMAIN	OWNER NODE	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP	VIRTU
✓ Ad		192.168.1.66	0	ALL NODES (255)	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
Ind Inc.		192.168.2.54	0	ALL NODES (255)	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENAB
1710		192.168.3.76	0	ALL NODES (255)	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-
Insert Delete	Total 3						25 Per Pag	e 🗸 Page	1 of 1	<>
IP ADDRESS	Insert	Close								
No items										
Create										

注

IP セット名は、両方のインスタンスで同じである必要があります。

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリインスタンスにサービスまたはサービスグループを追加します。

- 1. [設定]>[トラフィック管理]>[負荷分散]>[仮想サーバー]>[追加]に移動します。
- 2. [名前]、[プロトコル]、[IP アドレスタイプ (IP アドレス)]、[IP アドレス] (プライマリ VIP)、および [ポート] に必要な値を追加します。
 - G Load Balancing Virtual Server

Basic Settings		Help	>
Create a virtual server by specifying iddress. If the application is accessil You can configure multiple virtual se	name, an IP address, a port, and a protocol type. If an application is accessible from the internet, the virtual server IP (VIP) address i e only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. vers to receive client requests, thereby increasing the availability of resources to process client requests.	is a public IP	
Name*			
lb-vserver1	0		
Protocol*			
HTTP	\checkmark		
P Address Type*			
IP Address	\checkmark		
P Address*			
192 . 168 . 2 . 37	⑦ ★ Please enter value		
Port*			
80			-

- 3. [詳細] クリックします。[IP 範囲 IP セット設定] に移動し、ドロップダウンメニューから [IPSet]を選択し、 ステップ 3 で作成した IPSet を指定します。
- 4. **OK**をクリックして、負荷分散仮想サーバーを作成します。

ステップ 5. プライマリノードにサービスまたはサービスグループを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [サービス] > [追加] に移動します。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、[OK]をクリックします。

ステップ **6**. サービスまたはサービスグループをプライマリノードの負荷分散仮想サーバーにバインドします。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動します。
- 2. 手順4で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
- 3. [サービスとサービスグループ]タブで、[負荷分散仮想サーバーサービスバインドなし]をクリックします。
- 4. 手順5で構成したサービスを選択し、[バインド]をクリックします。

構成を保存します。強制フェールオーバーの後、セカンダリは新しいプライマリになります。古いプライマリ VIP の 外部スタティック IP は、新しいセカンダリ VIP に移動します。

CLI を使用した高可用性の設定 ステップ **1**. 両方のインスタンスで INC モードで高可用性をセットアップしま す。

セカンダリノードで、次のコマンドを入力します。

1 add ha node 1 <sec_ip> -inc ENABLED

プライマリノードで、次のコマンドを入力します。

```
1 add ha node 1 <prim_ip> -inc ENABLED
```

prim_ipは、プライマリノードの管理 NIC の内部 IP アドレスを指します。

sec_ipは、セカンダリノードの管理 NIC の内部 IP アドレスを指します。

ステップ 2. 両方のノードに仮想 IP とサブネット IP を追加します。

セカンダリノードで、次のコマンドを入力します。

2

4

5

```
1 add ns ip <primary_vip> <subnet> -type VIP
```

```
3 add ns ip <secondary_vip> <subnet> -type VIP
```

```
add ns ip <primary_snip> <subnet> -type SNIP
```

secondary_vipは、セカンダリインスタンスのクライアント側インターフェイスの内部 IP アドレスを指しま す。

primary_snipは、プライマリ・インスタンスのサーバ側インターフェイスの内部 IP アドレスを指します。

```
primary_vipは、プライマリ・インスタンスのクライアント側インターフェイスの内部 IP アドレスを指します。
```

プライマリノードで、次のコマンドを入力します。

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_snip> <subnet> -type SNIP
```

primary_snipは、プライマリ・インスタンスのサーバ側インターフェイスの内部 IP アドレスを指します。

secondary_vipは、セカンダリインスタンスのクライアント側インターフェイスの内部 IP アドレスを指しま す。 ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。IP セットを追加し、両方のインスタンスで IP セ ットをセカンダリ VIP にバインドします。

セカンダリノードで、次のコマンドを入力します。

1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>

セカンダリノードで、次のコマンドを入力します。

1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>

注

IP セット名は、両方のインスタンスで同じである必要があります。

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリ・インスタンスに仮想サーバを追加 します。

次のコマンドを入力します:

ステップ 5. プライマリインスタンスにサービスまたはサービスグループを追加します。

次のコマンドを入力します:

1 add service <service_name> <service_ip_address> <protocol> <port>

ステップ **6.** サービス/サービスグループをプライマリインスタンス上の負荷分散仮想サーバーにバインドします。 次のコマンドを入力します:

1 bind <server_type> vserver <vserver_name> <service_name>

注

設定を保存するには、コマンドsave configを入力します。そうしないと、インスタンスの再起動後に設 定が失われます。

ステップ **7**. 設定を確認します。

プライマリクライアント NIC に接続されている外部 IP アドレスが、フェールオーバー時にセカンダリに移動するこ とを確認します。

1. 外部 IP アドレスに cURL 要求を行い、それが到達可能であることを確認します。

2. プライマリインスタンスで、フェイルオーバーを実行します:

GUIから、[設定]>[システム]>[高可用性]>[アクション]>[強制フェールオーバー]に移動します。

CLI から、次のコマンドを入力します。

1 force ha failover -f

GCP コンソールで、セカンダリインスタンスに移動します。外部 IP アドレスは、フェールオーバー後にセカンダリのクライアント NIC に移動されている必要があります。

3. 外部 IP に cURL 要求を発行し、再び到達可能であることを確認します。

Google Cloud Platform にプライベート **IP** アドレスを指定した **1** つの **NIC VPX** 高 可用性ペアをデプロイします

October 17, 2024

プライベート IP アドレスを使用して、単一の NIC VPX 高可用性ペアを GCP にデプロイできます。クライアント IP (VIP) アドレスは、プライマリノードのエイリアス IP アドレスとして設定する必要があります。フェールオーバー時 に、クライアント IP アドレスがセカンダリノードに移動され、トラフィックが再開されます。各ノードのサブネット IP (SNIP) アドレスもエイリアス IP 範囲として設定する必要があります。

高可用性の詳細については、「高可用性」を参照してください。

はじめに

- Google Cloud Platform に NetScaler VPX インスタンスをデプロイするに記載されている制限事項、ハー ドウェア要件、注意事項をお読みください。この情報は、高可用性展開にも適用されます。
- GCP プロジェクトで クラウドリソースマネージャー API を有効にします。

Service a	ccount 🕜
Compu	te Engine default service accoun
Access s	copes 🖉
Allow	default access
Allov	full access to all Cloud APIs
O Set a	ccess for each API

- インスタンスの作成中に、すべての Cloud API へのフルアクセスを許可します。
- GCP サービスアカウントに次の IAM 権限があることを確認します。

1	REQUIRED_INSTANCE_IAM_PERMS = L
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 "compute.targetInstances.use", 9 "compute.targetInstances.create", 10 11 "compute.zones.list", "compute.zoneOperations.get", 12 13]
- VM がインターネットにアクセスできない場合は、VPC サブネットでプライベート Google アクセスを有効

Name 🛞	
management-subnet	
Add a description	
VPC Network	
automationmgmtnetwork	
Region 🛞	
us-east1 -	
Reserve for Internal HTTP(S) Load Balancing 🕡	
On Off	
IP address range 🔞	
192.168.2.0/24	
Create secondary IP range	
Private Google access 💿	
On Off	
Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more	
On Off	
CANCEL	ADD

• プライマリノードで GCP 転送ルールを構成している場合は、GCP 上の VPX 高可用性ペアの転送ルールのサポート に記載されている制限と要件を読んで、フェイルオーバー時に新しいプライマリに更新してください。

VPX 高可用性ペアを Google Cloud Platform にデプロイする方法

NIC が1つの HA ペアを導入する手順の概要は次のとおりです。

- 1. 手順1:1つの VPC ネットワークを作成します。
- 同じリージョンに2つのVPXインスタンス(プライマリノードとセカンダリノード)を作成します。それらは、同じゾーンまたは異なるゾーンに存在することができます。たとえば、アジア東-1a、アジア東-lb。
- 3. NetScaler GUI または ADC CLI コマンドを使用して、両方のインスタンスで高可用性設定を構成します。

手順 1. VPC ネットワークを 1 つ作成

VPC ネットワークを作成するには、次の手順を実行します。

- 1. Google コンソール > [ネットワーク] > [VPC ネットワーク] > [VPC ネットワークの作成] にログインしま す。
- 2. 必須フィールドに入力し、[Create] をクリックします。

詳細については、「Google Cloud Platform に NetScaler VPX インスタンスをデプロイする」の「**VPC** ネットワ ークの作成」セクションを参照してください。

手順 3. 手順 2:2 つの VPX インスタンスを作成する

シナリオ:単一 NIC のスタンドアロン VPX インスタンスをデプロイするの手順1から手順3に従って、2つの VPX インスタンスを作成します。

重要:

クライアントエイリアス IP アドレスをプライマリノードにのみ割り当て、サーバエイリアス IP アドレスをプ ライマリノードとセカンダリノードに割り当てます。VPX インスタンスの内部 IP アドレスを使用して VIP ま たは SNIP を構成しないでください。

クライアントとサーバーのエイリアス IP アドレスを作成するには、プライマリノードで次の手順を実行します。

1. VM インスタンスに移動し、[編集]をクリックします。

- 2. ネットワークインターフェースウィンドウで、クライアント (NIC0) インターフェースを編集します。
- 3. [エイリアス IP 範囲(Alias IP range)] フィールドに、クライアントエイリアス IP アドレスを入力します。
- 4.「IP 範囲を追加」をクリックし、サーバーのエイリアス IP アドレスを入力します。

Network interface You must stop the VM instance to edit network, subnetwork or internal IP address Network automationmgmtnetwork Subnetwork mgmtsubnet (192.168.1.0/24, us-east1) Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP ranges Subnet range Primary (192.168.1.0/24) Alias IP range Primary (192.168.1.0/24) Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range Alias IP range	Primary Client Alia (VIP) Primary Server Al
You must stop the VM Instance to edit network, subnetwork or internal IP address Network automationmgmtnetwork Subnetwork mgmtsubnet (192.168.1.0/24, us-east1) Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP ranges Subnet range Primary (192.168.1.0/24) Ig2.168.1.5/32 Primary (192.168.1.0/24) Ig2.168.1.6/32	Primary Client Alia (VIP) Primary Server Al
automationmgmtnetwork Subnetwork mgmtsubnet (192.168.1.0/24, us-east1) Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP ranges Subnet range Primary (192.168.1.0/24) I 192.168.1.5/32 Primary (192.168.1.0/24) Alias IP range	Primary Client Alia: (VIP) Primary Server Ali
Subnetwork Image: Subnet (192.168.1.0/24, us-east1) Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP ranges Alias IP range Subnet range Alias IP range Primary (192.168.1.0/24) 192.168.1.6/32 + Add IP range 192.168.1.6/32	Primary Client Alla (VIP) Primary Server All
mgmtsubnet (192.168.1.0/24, us-east1) Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP range Primary (192.168.1.0/24) IP2.168.1.5/32 Primary (192.168.1.0/24) Alias IP range	Primary Client Alia (VIP) Primary Server Ali
Internal IP 192.168.1.71 Internal IP type Ephemeral Alias IP ranges Subnet range Alias IP range P Primary (192.168.1.0/24) Ig2.168.1.6/32 + Add IP range	Primary Client Alia: (VIP) Primary Server Ali
Ephemeral Alias IP ranges Subnet range Primary (192.168.1.0/24) + Add IP range	Primary Client Aliar (VIP) Primary Server Ali
Alias IP ranges Subnet range Primary (192.168.1.0/24) Primary (192.168.1.0/24) Alias IP range + Add IP range	Primary Client Alia (VIP) Primary Server Ali
Subnet range Alias IP range Primary (192.168.1.0/24) • Primary (192.168.1.0/24) • Had IP range •	Primary Client Alia (VIP) Primary Server Ali
Primary (192.168.1.0/24) Primary (192.168.1.0/24) Primary (192.168.1.0/24) Add IP range	(VIP) Primary Server Ali
Primary (192.168.1.0/24) - 192.168.1.6/32 + Add IP range	Primary Server Ali
+ Add IP range	IP(SNIP)
Ride allas IP ranges External IP @ Ephemeral	•
Network Service Tier Premium (Current project-level tier, change) Standard (us-east1) IP forwarding Off Public DNS PTP Record	
Enable	
PTR domain name	

サーバエイリアス IP アドレスを作成するには、セカンダリノードで次の手順を実行します。

- 1. VM インスタンスに移動し、[編集]をクリックします。
- 2. ネットワークインターフェースウィンドウで、クライアント (NICO) インターフェースを編集します。
- 3.「エイリアス IP 範囲」フィールドに、サーバーのエイリアス IP アドレスを入力します。

Network interface		^
You must stop the VM instance to edit n	etwork, subnetwork or internal IP address	
automationmgmtnetwork		-
Subnetwork		
mgmtsubnet (192.168.1.0/24, us-e	ast1)	Ŧ
Internal IP 192.168.1.76		
Internal IP type		
Ephemeral		•
Alias IP ranges	Secondary Subnet IP(SNIP)	
Subnet range	Alias IP range 🐵	
Primary (192.168.1.0/24) *	192.168.1.7/32	×
+ Add	IP range	
Hide alias IP ranges External IP @		
Ephemeral		-
Network Service Tier @ Premium (Current project-lev Standard (us-east1) @ IP forwarding Off	el tier, change) <i>©</i>	
Public DNS PTR Record Enable		
PTR domain name		
Done Cancel		

フェイルオーバー後、古いプライマリが新しいセカンダリになると、クライアントのエイリアス IP アドレスが古いプ ライマリから移動され、新しいプライマリに接続されます。

k

VPX インスタンスを構成したら、仮想 (VIP) アドレスとサブネット IP (SNIP) アドレスを構成できます。詳細については、「Citrix ADC 所有の IP アドレスの構成」を参照してください。

手順3.高可用性の構成

Google Cloud Platform でインスタンスを作成した後、NetScaler GUI または CLI を使用して高可用性を構成できます。
GUIを使用した高可用性の構成

ステップ **1**. 両方のノードで INC Enabled モードで高可用性を設定します。

プライマリノードで、次の手順を実行します。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2.構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノードの IP アドレス] フィールドに、セカンダリノードの管理 NIC のプライベート IP アドレスを 入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [Create] をクリックします。

先に進む前に、[Nodes]ページにセカンダリノードの同期状態が SUCCESS と表示されていることを確認してくだ さい。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2. 構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノード **IP** アドレス] フィールドに、プライマリノードの管理 NIC のプライベート IP アドレスを入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [**Create**] をクリックします。

セカンダリノードで、次の手順を実行します。

System > High Availability > Nodes

Nodes	2							2
Add	Edit	Delete Statis	tics	t Action 🗸				
	ID ¢	IP ADDRESS 🔅	HOST NAME 🔅	MASTER STATE	NODE STATE	INC \$	SYNCHRONIZATION STATE	SYNCHRONIZATION FAILURE REA
	0	192.168.1.71		Primary	• UP	ENABLED	ENABLED	-NA-
	1	192.168.1.76		Secondary	• UP	ENABLED	SUCCESS	-NA-
Total 2							25 Per Page	✓ Page 1 of 1 < ▶

注

セカンダリノードがプライマリノードと同期されると、セカンダリノードにはプライマリノードと同じログオン認証情報が割り当てられます。

ステップ 2. 両方のノードに仮想 IP アドレスとサブネット IP アドレスを追加します。

プライマリノードで、次の手順を実行します。

1. System > Network > IP Sets > Add に移動します。

- 2. クライアントエイリアス IP(VIP)アドレスを作成するには、次の手順を実行します。
 - a) プライマリ VM インスタンスの VPC サブネットに設定されているクライアントエイリアス IP アドレス とネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [**Create**] をクリックします。
- 3. サーバーエイリアス IP (SNIP) アドレスを作成するには、次の手順を実行します。
 - a) プライマリ VM インスタンスの VPC サブネットに設定されているサーバーエイリアス IP アドレスとネ ットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [**Create**] をクリックします。

System > Network > IPs > IF	PV4s						
IPs							(²)
IPV4s 3 IPV6s 1							
Add Edit Delete	Statistics Sel	ect Action 🗸					
Q Click here to search or you can e	enter Key : Value format						Û
IP ADDRESS	STATE 0	TYPE 0	MODE 0	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 ∨ Pag	re 1 of 1 🔹 🕨

セカンダリノードで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. クライアントエイリアス IP(VIP)アドレスを作成するには、次の手順を実行します。
 - a) プライマリ VM インスタンスの VPC サブネットに設定されているクライアントエイリアス IP アドレス とネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
 - c) [**Create**] をクリックします。
- 3. サーバーエイリアス IP (SNIP) アドレスを作成するには、次の手順を実行します。
 - a) セカンダリ VM インスタンスの VPC サブネットに設定されているサーバエイリアス IP アドレスとネッ トマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [**Create**] をクリックします。

System > Netw	work > IPs > IPV	4s						\sim	F
IPV4s 3	IPV6s 1								
Add Edi	t Delete Si	tatistics Se	lect Action \checkmark						
Q Click here to	search or you can ent	er Key : Value format							(j)
	IP ADDRESS	STATE \$	TYPE	\$ MODE \$	ARP	ICMP	VIRTUAL SERVER	TRAFFIC DOMAIN	
Secondary SNIP	192.168.1.7	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-N/A-		0
	192.168.1.76	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-N/A-		0
Primary VIP	192.168.1.5	ENABLED	Virtual IP	Passive	ENABLED	ENABLED	ENABLED		0
Total 3							25 Per Page \vee Pag	ge 1 of 1 🔍	

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。ステップ **3:** プライマリノードに負荷分散仮想サ ーバーを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] > [追加] に移動します。
- 2. 名前、プロトコル、IP アドレスタイプ(IP アドレス)、IP アドレス(プライマリクライアントエイリアス IP アドレス)、およびポートに必要な値を追加し、「**OK**」をクリックします。
 - Load Balancing Virtual Server

Basic Settings	
Create a virtual server by specifying a nam IP address. If the application is accessible You can configure multiple virtual servers i	e, 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 only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. o receive client requests, thereby increasing the availability of resources to process client requests.
Name*	
lb-vserver1	\odot
Protocol*	
HTTP	\checkmark
IP Address Type*	
IP Address	\checkmark
IP Address*	
192.168.1.5	0
Port*	_
80	
► More	
OK Cancel	

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリノードにサービスまたはサービスグ ループを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [サービス] > [追加] に移動します。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、[**OK**]をクリックします。

ステップ 5. サービスまたはサービスグループをプライマリノードの負荷分散仮想サーバーにバインドします。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動します。
- 2. 手順3で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
- 3. [サービスとサービスグループ]タブで、[負荷分散仮想サーバーサービスバインドなし]をクリックします。
- 4. 手順4で構成したサービスを選択し、「バインド」をクリックします。

ステップ 6. 構成を保存します。

強制フェールオーバーの後、セカンダリは新しいプライマリになります。古いプライマリのクライアントエイリアス IP (VIP) が新しいプライマリに移動します。

CLI を使用した高可用性の設定

ステップ **1**. ステップ **1**: NetScaler CLI を使用して、両方のインスタンスで **INC** 対応モードで高可用性を設定しま す。

セカンダリノードで、次のコマンドを入力します。

1 add ha node 1 <sec_ip> -inc ENABLED

プライマリノードで、次のコマンドを入力します。

1 add ha node 1 <prim_ip> -inc ENABLED

sec_ipは、セカンダリノードの管理 NIC の内部 IP アドレスを指します。

prim_ipは、プライマリノードの管理 NIC の内部 IP アドレスを指します。

ステップ 2. ステップ 2: プライマリノードとセカンダリノードの両方に VIP と SNIP を追加します。

プライマリノードで次のコマンドを入力します。

1 add ns ip <primary_client_alias_ip> <subnet> -type VIP

注

VM インスタンスのクライアントサブネットに設定されているエイリアス IP アドレスとネットマスクを入力します。

1 add ns ip <primary_server_alias_ip> <subnet> -type SNIP

セカンダリノードで次のコマンドを入力します。

1 add ns ip <primary_client_alias_ip> <subnet> -type VIP

注

VM インスタンスのクライアントサブネットに設定されているエイリアス IP アドレスとネットマスクを入力します。

add ns ip <secondary_server_alias_ip> <subnet> -type SNIP

注

1

VM インスタンスのサーバサブネットに設定されているエイリアス IP アドレスとネットマスクを入力します。

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。ステップ **3:** プライマリノードに仮想サーバを追加します。

次のコマンドを入力します:

1 add <server_type> vserver <vserver_name> <protocol> <
 primary_client_alias_ip> <port>

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリノードにサービスまたはサービスグ ループを追加します。

次のコマンドを入力します:

1 add service <service_name> <service_ip_address> <protocol> <port>

ステップ **5**. サービスまたはサービスグループをプライマリノードの負荷分散仮想サーバーにバインドします。 次のコマンドを入力します:

1 bind <server_type> vserver <vserver_name> <service_name>

注

設定を保存するには、コマンドsave configを入力します。そうしないと、インスタンスの再起動後に設 定が失われます。

プライベート IP アドレスを持つ VPX 高可用性ペアを Google Cloud Platform にデ プロイする

October 17, 2024

プライベート IP アドレスを使用して、VPX 高可用性ペアを GCP にデプロイできます。クライアント IP(VIP)は、 プライマリノードのエイリアス IP アドレスとして設定する必要があります。フェールオーバー時に、クライアント IP アドレスがセカンダリノードに移動され、トラフィックが再開されます。

高可用性の詳細については、「高可用性」を参照してください。

はじめに

- Google Cloud Platform に NetScaler VPX インスタンスをデプロイするに記載されている制限事項、ハー ドウェア要件、注意事項をお読みください。この情報は、高可用性展開にも適用されます。
- GCP プロジェクトで クラウドリソースマネージャー API を有効にします。

Se	rvice account 🛞
C	compute Engine default service account
Ac	0 2800 2000 P
Õ	Allow default access
ŏ	Allow full access to all Cloud APIs
	Set access for each API

- インスタンスの作成中に、すべての Cloud API へのフルアクセスを許可します。
- GCP サービスアカウントに次の IAM 権限があることを確認します。

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]

• 管理インターフェイス以外のインターフェイスに外部 IP アドレスを設定している場合は、GCP サービスアカ ウントに次の追加の IAM 権限があることを確認します。

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]

• 仮想マシンにインターネットアクセスがない場合は、管理サブネットでプライベート Google Access を有効

Name Parae is permanent management-subnet Add a description VPC Network automationingmtnetwork megion us-east1 us-east1 on off Padress range 192.168.2.0/24 Prote Google access off	Add a subnet	
management-subnet Add a description vert Network automationmgmtnetwork Region (*) us-east1 us-east1 (*) On On Off IP address range (*) 192.168.2.0/24 Private Google access (*) On On Off IP address range (*) IP address range (*) Ip address range (*)	Name 🔞 Name is permanent	
Add a description sutomationmgmtnetwork Region ws-east1 ws-east1 Reserve for Internal HTTP(\$) Load Balancing On On Off Intracts accordary IP range Private Google access On	management-subnet	
VPC Network automationmgmtnetwork Region w:east1 w:east1 On Off IP address range IP 2.168.2.0/24 Create secondary IP range Private Google access Off Off IP 2.168.2.0/24 Create secondary IP range IP 1000 Private Google access IP 000 Off IP 0000 Off IP 0000 IP 0000 IP 0000 IP 0000 IP	Add a description	
automationmgmtnetwork Region ② us-east1 reserve for Internal HTTP(S) Load Balancing ③ ③ On ③ Off P address range ③ 192.168.2.0/24 Private Google access ③ ④ On ④ Off ● On ④ Off ● On ● Off ■ Dirivate Google access ⑥ ● On ● Off ■ Dirivate Google access ⑥ ● On ● Off ■ Off ■ Off ■ Off ■ Off ■ Off ■ Off ■ Off ■ Off ● On ● Off ■ Off On International Content Access In Stackdriver. Learn more International Content Access In Stackdriver. Learn more International Content Access In Stackdriver. Learn more International Content Access In Stackdriver. Learn more International Content Access International Content Access International Content Internation Content International Content Internation Content Internation	VPC Network	
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 Off Diff Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On On On On On On On On On On On On	automationmgmtnetwork	
wseat1 Reserve for Internal HTTP(S) Load Balancing (*) On Off IP address range (*) 192.168.2.0/24 Create secondary IP range Private Google access (*) On Off Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Of Of Of On Of Of On Of Of Of On Of Of On Of Of On Of On Of Of Of	Region 💿	
Reserve for Internal HTTP(S) Load Balancing (*) On Off P address range (*) 192.168.2.0/24 Create secondary IP range Private Google access (*) On Off 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 Image: Off	us-east1 -	
 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 Off 	Reserve for Internal HTTP(S) Load Balancing	
IP address range Image: Contract a secondary IP range Private Google access Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP range Image: Contract a secondary IP	On Off	
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 • Off • Off	IP address range 💿	
Create secondary IP range Private Google access On Off Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Off Off	192.168.2.0/24	
Private Google access On Off Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Off CANCEL ADD	Create secondary IP range	
On Off Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Off CANCEL ADD	Private Google access 💿	
Flow logs Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more On On Off	● On ○ Off	
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	
CANCEL ADD	On Off	
CANCEL ADD		
	 CANCEL	ADD

プライマリノードでGCP転送ルールを構成している場合は、GCP上のVPX高可用性ペアの転送ルールのサポートに記載されている制限と要件を読んで、フェイルオーバー時に新しいプライマリに更新してください。

VPX 高可用性ペアを Google Cloud Platform にデプロイする方法

ここでは、高可用性展開手順の概要を示します。

- 1. 同じリージョンに VPC ネットワークを作成します。たとえば、アジア東です。
- 2. 同じリージョンに 2 つの VPX インスタンス(プライマリノードとセカンダリノード)を作成します。それら は、同じゾーンまたは異なるゾーンに存在することができます。たとえば、アジア東-1a、アジア東-lb。
- 3. NetScaler GUI または ADC CLI コマンドを使用して、両方のインスタンスで高可用性設定を構成します。

手順 1. 手順 1: VPC ネットワークを作成する

要件に基づいて VPC ネットワークを作成します。管理 NIC、クライアント NIC、サーバー NIC に関連付けるために 3 つの VPC ネットワークを作成することをお勧めします。

VPC ネットワークを作成するには、次の手順を実行します。

- 1. Google コンソールにログインし、[ネットワーク] > [VPC ネットワーク] > [VPC ネットワークの作成] をク リックします。
- 2. 必須フィールドに入力し、[Create] をクリックします。

詳細については、「Google Cloud Platform に NetScaler VPX インスタンスをデプロイする」の「**VPC** ネットワ ークの作成」セクションを参照してください。

手順 3. 手順 2:2 つの VPX インスタンスを作成する

シナリオ: マルチ NIC、マルチ IP のスタンドアロン VPX インスタンスをデプロイするに記載されている手順に従っ て、2 つの VPX インスタンスを作成します。

重要:

クライアントエイリアス IP アドレスをプライマリノードに割り当てます。VPX インスタンスの内部 IP アドレ スを使用して VIP を構成しないでください。

- クライアントエイリアス IP アドレスを作成するには、次の手順を実行します。
 - 1. VM インスタンスに移動し、[編集] をクリックします。
 - 2. [ネットワークインターフェイス(Network Interface)] ウィンドウで、クライアントインターフェイスを 編集します。
 - 3. [エイリアス IP 範囲(Alias IP range)] フィールドに、クライアントエイリアス IP アドレスを入力します。

NetScaler VPX 14.1

 vivi instance deta 	ils	/ EDIT	心 RESET	CREATE SIM			
Creation time							
Jan 16, 2020, 4:00:22 PM							
Network interfaces							
nic0: automationmgmtnetwork	mgmtsubnet		1				
Network interface			^				
Network							
automationclientnetwork							
Subnetwork	٦ .						
clientsubnet							
Internal IP							
192.168.2.65							
Internal IP type							
Ephemeral			•				
Alias IP ranges							
Subnet range	Alias IP ra	inge 🔞					
· · · · · · · · · · · · · · · · ·							
Primary (192.168.2.0/24)	▼ Example	e: 10.0.1.0/24 or /	32 🗙				
Primary (192.168.2.0/24)	Example Add IP range	e: 10.0.1.0/24 or /3	32				
Primary (192.168.2.0/24)	Example Add IP range	e: 10.0.1.0/24 or /3	32				
Primary (192.168.2.0/24) + A Hide alias IP ranges	Example Add IP range	e: 10.0.1.0/24 or /:	32				
Primary (192.168.2.0/24)	Example Add IP range	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) + Hide alias IP ranges External IP	Exampl Add IP range	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) Hide alias IP ranges External IP	Exampl Add IP range	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) Hide alias IP ranges External IP None Done Cancel	Exampl Add IP range	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) + A Hide alias IP ranges External IP None Done Cancel	Exampl Add IP range	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) + Hide alias IP ranges External IP	Exampl Add IP range ; serversubnet	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) Hide alias IP ranges External IP None Done Cancel nic2: automationservernetwork	Exampl Add IP range serversubnet	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) Primary (192.168.2.0/24) Hide alias IP ranges External IP @ None Done Cancel nic2: automationservernetwork stwork interfaces	Exampl Add IP range serversubnet	e: 10.0.1.0/24 or /:	32 ×				
Primary (192.168.2.0/24) Hide alias IP ranges External IP Toone Done Cancel nic2: automationservernetwork Ptwork Interfaces Name Network	Exampl Add IP range serversubnet Subnetwork	e: 10.0.1.0/24 or /: Primary internal IP	32 X	External IP	Network Tier @	IP forwarding	Network details
Primary (192.168.2.0/24) Hide alias IP ranges External IP Toone Cancel nic2: automationservernetwork nic0 automationmgmtnetwork	Exampl Add IP range serversubnet Subnetwork mgmtsubnet	e: 10.0.1.0/24 or /: Primary internal IP 192.168.1.62	32 X Alias IP ranges	External IP adc-ha-instance1-ip1 (35.185.108.124)	Network Tier @ Premium	IP forwarding Off	Network details View details
Primary (192.168.2.0/24) Primary (192.168.2.0/24) + A Hide alias IP ranges External IP None Done Cancel nic2: automationservernetwork Name Network Network nic0 automationnight network nic1 automationclientnetwork	Exampl Exampl Add IP range serversubnet subnetwork mgmtsubnet clientsubnet	e: 10.0.1.0/24 or /: Primary internal IP 192.168.1.62 192.168.2.8	32 X Alias IP ranges - 192.168.2.7/32	External IP adc-ha-instance1-ip1 (35.185.108.124) None	Network Tier 📀 Premium	IP forwarding Off	Network details View details View details

フェールオーバー後、古いプライマリが新しいセカンダリになると、エイリアス IP アドレスは古いプライマリから移動し、新しいプライマリに接続されます。

VPX インスタンスを構成したら、仮想 (VIP) アドレスとサブネット IP (SNIP) アドレスを構成できます。詳細については、「Citrix ADC 所有の IP アドレスの構成」を参照してください。

手順3.高可用性の構成

Google Cloud Platform でインスタンスを作成した後、NetScaler GUI または CLI を使用して高可用性を構成で きます。 GUIを使用した高可用性の構成

ステップ 1. 両方のノードで INC Enabled モードで高可用性を設定します。

プライマリノードで、次の手順を実行します。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2. 構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノードの IP アドレス] フィールドに、セカンダリノードの管理 NIC のプライベート IP アドレスを 入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [Create] をクリックします。

先に進む前に、[Nodes]ページにセカンダリノードの同期状態が SUCCESS と表示されていることを確認してくだ さい。

- 1. GCP Console nsroot からノードのユーザー名とインスタンス ID をパスワードとしてインスタンスにロ グオンします。
- 2. 構成>システム>高可用性>ノードに移動し、追加をクリックします。
- 3. [リモートノード **IP** アドレス] フィールドに、プライマリノードの管理 NIC のプライベート IP アドレスを入力します。
- 4. [セルフノードで INC (独立ネットワーク構成) モードをオンにする] チェックボックスをオンにします。
- 5. [Create] をクリックします。

セカンダリノードで、次の手順を実行します。

Nodes 2
Add Edit Delete Statistics Select Action ~
ID © IP ADDRESS © HOST NAME © MASTER STATE © NODE STATE © INC © SYNCHRONIZATION STATE © SYNCHRONIZATION FAILURE
0 192.168.1.62 Primary OUP ENABLED ENABLED -NA-
1 192.168.1.6 Secondary ● UP ENABLED SUCCESS -NA-

注

セカンダリノードがプライマリノードと同期されると、セカンダリノードにはプライマリノードと同じログオン認証情報が割り当てられます。

ステップ 2. 両方のノードに仮想 IP アドレスとサブネット IP アドレスを追加します。

プライマリノードで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. クライアントエイリアス IP (VIP) アドレスを作成するには、次の手順を実行します。

- a) 仮想マシンインスタンスのクライアントサブネットに設定されたエイリアス IP アドレスとネットマス クを入力します。
- b) [IP Type] フィールドで、ドロップダウンメニューから [Virtual IP] を選択します。
- c) [Create] をクリックします。
- 3. サーバ IP (SNIP) アドレスを作成するには、次の手順を実行します。
 - a) プライマリ・インスタンスのサーバ側インターフェイスの内部 IP アドレスと、サーバ・サブネットに設 定されたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [Create] をクリックします。

System > Netv	vork > IPs >	IPV4s								
IPs									C	F.
IPV4s 3	IPV6s 1									
Add Edit	Delete	Statistics	Selec	t Action V						
Q Click here to	search or you can	n enter Key : Value fo	rmat							i
	IP ADDRESS	© STATE		TYPE	MODE	ARP	ICMP	VIRTUAL SERVER	AIN	
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	۹.	

セカンダリノードで、次の手順を実行します。

- 1. System > Network > IP Sets > Add に移動します。
- 2. クライアントエイリアス IP (VIP) アドレスを作成するには、次の手順を実行します。
 - a) プライマリ VM インスタンスのクライアントサブネットに対して構成された Alias IP アドレスとネット マスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [**Create**] をクリックします。
- 3. サーバ IP (SNIP) アドレスを作成するには、次の手順を実行します。
 - a) セカンダリインスタンスのサーバ側インターフェイスの内部 IP アドレスと、サーバサブネットに設定さ れたネットマスクを入力します。
 - b) [IP Type] フィールドで、ドロップダウンメニューから [Subnet IP] を選択します。
 - c) [Create] をクリックします。

System > Netv	vork > IPs > IPV	4s						
IPs] 😭
IPV4s 3	IPV6s 1							
Add Edit	Delete	sele	ct Action 🗸					
Q Click here to	search or you can ent	er Key : Value format						(i)
	IP ADDRESS	STATE 0	TYPE 0	MODE 0	ARP 0	ICMP 0	VIRTUAL SERVER	¢ 1
	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 V Page 1 of 1	•

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。ステップ **3:** プライマリノードに負荷分散仮想サ ーバーを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] > [追加] に移動します。
- 2. 名前、プロトコル、IP アドレスタイプ(IP アドレス)、IP アドレス(プライマリクライアントエイリアス IP アドレス)、およびポートに必要な値を追加し、「**OK**」をクリックします。

G Load Balancing Virtual Server

Basic Settings		
Create a virtual server by specifying a address. If the application is accessib You can configure multiple virtual ser	i name, ar ile only fro rvers to re	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. zeeve client requests, thereby increasing the availability of resources to process client requests.
Name*		
lb-vserver1		O
Protocol*		
HTTP	~	
IP Address Type*		
IP Address	~	
IP Address*		
192 . 168 . 2 . 5		Ō
Port*		
80		
▶ More		
OK Cancel		*

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリノードにサービスまたはサービスグ ループを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [サービス] > [追加] に移動します。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、[OK]をクリックします。

ステップ 5. サービスまたはサービスグループをプライマリノードの負荷分散仮想サーバーにバインドします。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動します。
- 2. 手順3で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
- 3. [サービスとサービスグループ]タブで、[負荷分散仮想サーバーサービスバインドなし]をクリックします。
- 4. 手順4 で構成したサービスを選択し、[バインド]をクリックします。

ステップ **5**. 構成を保存します。

強制フェールオーバーの後、セカンダリは新しいプライマリになります。古いプライマリからのクライアントエイリ アス IP (VIP) とサーバエイリアス IP (SNIP) が新しいプライマリに移動します。

CLIを使用した高可用性の設定

ステップ **1**. ステップ **1**: NetScaler CLI を使用して、両方のインスタンスで **INC** 対応モードで高可用性を設定しま す。

セカンダリノードで、次のコマンドを入力します。

1 add ha node 1 <sec_ip> -inc ENABLED

プライマリノードで、次のコマンドを入力します。

1 add ha node 1 <prim_ip> -inc ENABLED

sec_ipは、セカンダリノードの管理 NIC の内部 IP アドレスを指します。

prim_ipは、プライマリノードの管理 NIC の内部 IP アドレスを指します。

ステップ **2**. 両方のノードに VIP と SNIP を追加します。

プライマリノードで次のコマンドを入力します。

1 add ns ip <primary_client_alias_ip> <subnet> -type VIP

注

仮想マシンインスタンスのクライアントサブネットに設定されたエイリアス IP アドレスとネットマスクを入力 します。

1 add ns ip <primary_snip> <subnet> -type SNIP

primary_snipは、プライマリインスタンスのサーバ側インターフェイスの内部 IP アドレスを指します。

セカンダリノードで次のコマンドを入力します。

1 add ns ip <primary_client_alias_ip> <subnet> -type VIP

注

プライマリ VM インスタンスのクライアントサブネットに対して構成された Alias IP アドレスとネットマスク を入力します。

1 add ns ip <secondary_snip> <subnet> -type SNIP

secondary_snipは、セカンダリインスタンスのサーバ側インターフェイスの内部 IP アドレスを指します。

注

VM インスタンスのサーバサブネットに設定された IP アドレスとネットマスクを入力します。

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。ステップ **3:** プライマリノードに仮想サーバを追加します。

次のコマンドを入力します:

1 add <server_type> vserver <vserver_name> <protocol> <
 primary_client_alias_ip> <port>

ステップ **4:** プライマリ・インスタンスに仮想サーバを追加します。プライマリノードにサービスまたはサービスグ ループを追加します。

次のコマンドを入力します:

1 add service <service_name> <service_ip_address> <protocol> <port>

ステップ **5.** サービスまたはサービスグループをプライマリノードの負荷分散仮想サーバーにバインドします。

次のコマンドを入力します:

1 bind <server_type> vserver <vserver_name> <service_name>

注

設定を保存するには、コマンドsave configを入力します。そうしないと、インスタンスの再起動後に設 定が失われます。

Google Cloud VMware Engine に **NetScaler VPX** インスタンスをインストールする

October 17, 2024

Google Cloud VMware Engine (GCVE) は、専用のベアメタルの Google Cloud Platform インフラストラクチ ャから構築された vSphere クラスタを含むプライベートクラウドを提供します。最小初期デプロイメントは 3 ホス トですが、追加ホストは一度に 1 つずつ追加できます。プロビジョニングされたすべてのプライベートクラウドには、 vCenter Server、vSAN、vSphere、NSX-T があります。

GCVE を使用すると、必要な数の ESX ホストを使用して Google Cloud Platform 上にクラウドソフトウェア定義 データセンター (SDDC) を作成できます。GCVE は NetScaler VPX の導入をサポートします。GCVE はオンプレ ミス vCenter と同じユーザーインターフェイスを提供します。ESX ベースの Citrix ADC VPX デプロイメントと同 じように機能します。 次の図は、管理者またはクライアントがインターネット経由でアクセスできる Google Cloud Platform 上の GCVE を示しています。管理者は GCVE を使用してワークロードまたはサーバー VM を作成、管理、構成できます。管理者は OpenVPN 接続を使用して GCVE のウェブベースの vCenter と NSX-T Manager にアクセスできます。vCenter を使用して GCVE 内に NetScaler VPX インスタンス(スタンドアロンまたは HA ペア)とサーバ仮想マシンを作 成し、NSX-T Manager を使用して対応するネットワークを管理できます。GCVE 上の NetScaler VPX インスタン スは、オンプレミスの VMware ホストクラスタと同様に機能します。GCVE は、管理インフラストラクチャへの OpenVPN 接続を使用して管理できます。



前提条件

仮想アプライアンスのインストールを開始する前に、次の操作を行います。

- Google Cloud VMware エンジンとその前提条件の詳細については、Google Cloud VMware エンジンのド キュメントを参照してください。
- Google Cloud VMware Engine のデプロイに関する詳細については、「Google Cloud VMware Engine プライベートクラウドのデプロイ」を参照してください。
- ポイントツーサイト VPN ゲートウェイを使用してプライベートクラウドに接続し、Google Cloud VMware Engine にアクセスして管理する方法の詳細については、「Google Cloud VMware Engine プライベートク ラウドへのアクセス」を参照してください。
- VPN クライアントマシンで、NetScaler VPX アプライアンスのセットアップファイルをダウンロードします。
- 仮想マシンが接続する VMware SDDC 上に、適切な NSX-T ネットワークセグメントを作成します。詳細に ついては、「Google Cloud VMware Engine でのネットワークセグメントの追加」を参照してください。
- VPX ライセンスファイルを入手します。NetScaler VPX インスタンスライセンスの詳細については、「ライセンスの概要」を参照してください。
- GCVE プライベートクラウドに作成または移行された仮想マシン (VM) は、ネットワークセグメントに接続す る必要があります。

VMware クラウドのハードウェア要件

次の表に、VMware SDDC が各 VPX nCore 仮想アプライアンスに対して提供する必要がある仮想コンピューティン グリソースを示します。

表 1. NetScaler VPX インスタンスの実行に必要な最小限の仮想コンピューティングリソース

コンポーネント	条件
メモリ	2 GB
仮想 CPU(VCPU)	2
仮想ネットワークインターフェイス	VMware SDDC では、VPX ハードウェアをバージョン7 以上にアップグレードすると、最大 10 個の仮想ネット ワーク インターフェイスをインストールできます。
ディスク領域	20GB

注

これは、ハイパーバイザーのディスク要件に加えて必要になります。

VPX 仮想アプライアンスを実稼働で使用するには、フルメモリ割り当てを予約する必要があります。

OVF ツール 1.0 のシステム要件

Open Virtualization Format Tool (OVF Tool) は、Windows および Linux システムで実行できるクライアント アプリケーションです。次の表は、OVF ツールをインストールするための最小システム要件を示しています。

表 2. OVF ツールのインストールに必要な最小システム要件

コンポーネント	条件
オペレーティングシステム	VMware からの詳細な要件については、 http://kb.vmware.com/で『OVF ツールユーザーガ イド』の PDF ファイルを検索してください。
CPU	最低 750MHz、1GHz 以上推奨
RAM	最小1GB、推奨2GB
NIC	100Mbps 以上の NIC。

OVF のインストールについては、http://kb.vmware.com/で『OVF ツールユーザーガイド』の PDF ファイルを検 索してください。

NetScaler VPX セットアップファイルのダウンロード

VMware ESX 用の NetScaler VPX インスタンスセットアップパッケージは、オープン仮想マシン(OVF)フォーマット標準に準拠しています。これらのファイルは、Citrix Web サイトからダウンロードできます。ログオンするには、Citrix アカウントが必要です。Citrix アカウントをお持ちでない場合は、http://www.citrix.comのホームページにアクセスしてください。[新しいユーザー] リンクをクリックし、指示に従って新しい Citrix アカウントを作成します。

ログオンしたら、Citrix のホームページから次のパスをナビゲートします。

Citrix.com > ダウンロード > NetScaler > 仮想アプライアンス。

次のファイルを、ESX サーバーと同じネットワーク上のワークステーションにコピーします。3 つのファイルをすべ て同じフォルダーにコピーします。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (例えば、NSVPX-ESX-13.0-79.64disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf(例えば、NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf(例えば、NSVPX-ESX-13.0-79.64.mf)

Google Cloud VMware エンジンをデプロイする

- Google Cloud VMware Engine (?) 🙈 歳 ĉ Welcome to Google Cloud VMware Engine. Create your first Private Cloud, or try one of the common tasks below. S New Private Cloud P ∰ Activit ŝ Common Tasks G P 6 20 Ð 63 ch vSphere client Create a Private Cloud Connect via VPN Allocate Public IP Add nodes to a
- 1. GCVE ポータルにログインし、ホームに移動します。

- 2.「新規プライベートクラウド」ページで、次の詳細を入力します。
 - プライベートクラウドのデフォルトクラスタを作成するには、最低3つの ESXi ホストを選択します。

- vSphere/vSAN サブネットの CIDR 範囲フィールドには、/22 アドレススペースを使用します。
- HCX デプロイメントネットワーク CIDR 範囲フィールドには、/26 アドレススペースを使用します。
- 仮想ネットワークの場合、CIDR 範囲がオンプレミスまたは他の GCP サブネット (仮想ネットワーク)
 と重複していないことを確認します。

Google	e Cloud VMware Engine
	← Create Private Cloud ③
6 Home	Private Cloud name *
Resources	Nume your Private Liono
- Ga	asia-northeast1 > v-zone-a > VE Placement Group 2 •
Network	Node type *
Activity	ve_stanoar6-72 2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM 19-2 TB Raw, 3.2 TB Cache (All-Flash)
Account	Multi Node Single Node Node count*
	Customize Cores
	vSphere/vSAN subnets CIDR range *
	CIDR block prefix / 22 •
	HCX Deployment Network CIDR range
	CIDR block prefix / 26 -

- 3. [確認して作成]をクリックします。
- 4. 設定を確認します。設定を変更する必要がある場合は、[前へ]をクリックします。

Googl	e Cloud VMware Engine
	← Create Private Cloud ③
Home	Good news! Your Priva
6	Compute Node Type Edit
Resources	ve1-standard-72
Network	Model: PCSN-ULT-1-1ND CPU: 2x2.6 GHz, 36 Cores (72 HT) RAM: 768 GB Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
血 Activity	Private Cloud Size Edit
(j)	1 Node
Account	Total CPU: 36 Cores Total RAM: 768 GB Total Storage: 19.2 TB Raw, 3.2 TB Cache, All-Flash
	Location Edit
	asia-northeast1 > v-zone-a > VE Placement Group 2
	Advanced Options Edit
	Cores per node: 36
	vSphere/vSAN subnets CIDR range: 10.231.0.0/22
	HCX Deployment Network CIDR range 10.231.8.0/26
	Create Previous Cancel

- 5. [**Create**] をクリックします。プライベートクラウドのプロビジョニングプロセスが開始されます。プライベ ートクラウドのプロビジョニングには最大2時間かかることがあります。
- 6.「リソース」に移動して、作成されたプライベートクラウドを確認します。

Google	e Cloud VMware Engine						e		4	\$	¢	8
	Resources											
Home	Private Clouds (1)									•	lew Priva	te Cloud
	🕁 Download as CSV						Colur	in seti	tings	482 5	selected (ilters (0)
-	Name	÷	Clusters	÷	Total Nodes	\$ Location				\$	State	
ියුට Network	vjas-gave-demo		1		1	asia-northeast1 > v-zone-a > VE Placement Group :	2				 Provis 	ioning

- このリソースにアクセスするには、ポイントツーサイト VPN を使用して GCVE に接続する必要があります。
 詳細については、次のドキュメントを参照してください。
 - VPN ゲートウェイ
 - VPN を使用して接続する

プライベートクラウド vCenter ポータルにアクセスする

Google Cloud VMware Engine プライベートクラウドに移動します。[概要]タブの [vCenter ログイン情報]で、[表示]をクリックします。

Googl	e Cloud VMwar	e Engine			
	Resources				
Home	← gcp-vmwa	re-demo			
Resources	SUMMARY	CLUSTERS	SUBNETS	ACTIVITY	VSPHERE MANAGEN
Network			N	lame cp-vmware-demo	
Ē		<u></u>	C 1	lusters	
Activity	Ba	i asic Info	v 1	Sphere/vSAN sub 0.231.0.0/22	nets CIDR range
			v <u>v</u>	Center login info <u>(iew</u> Reset passwor	rd

2. vCenter の認証情報を書き留めます。

Googl	e Cloud VMware Engine
	← vCenter login
Home	User name CloudOwner@gve.local Copy
Network Activity	Password Copy

3. vSPHERE CLIENT の起動をクリックして vSphere クライアントを起動するか、VSPHERE 管理ネットワ ークに移動して vCenter Server アプライアンスの FQDN をクリックします。

Googl	e Cloud VMware Engine						0 4)	4 8	
	Resources									
Home	← gcp-vmware-demo						C LAUNCH VSPHERE CI	.ient 😡	ADD NOD	ES
6	SUMMARY CLUSTERS	SUBNETS ACTIVITY	vsi	PHERE MANAGEMENT NETWORK	ADVANCED VCENTER SETTING	S DNS CONFIGURATION				
Resources	🛃 Download as CSV							해3 Select	ed filters (D)	
Network	Type		÷	Version	\$	FQDN	\$ IP Address			\$
(A)	vCenter Server Appliance			7.0.2.19272235		vcsa-126870./3712/c5.asia-northeast1.gve.goog	10.231.0.6			
Activity	NSX Manager			-		mx-127044./3712fc5.asia-northeast1.gve.goog	10.231.0.11			
0	HCX			-		hcx-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. この手順のステップ2でメモした vCenter 認証情報を使用して VMware vSphere にログインします。

VMware	e [®] vSphere
example@dfma	in.local
Password	
Use Windows	s session authentication
	LOGIN

5. vSphere クライアントでは、GCVE ポータルで作成した ESXi ホストを確認できます。

vm vSphere Client Menu ∨ Q, Se		2) V GoudOwner@GVELOCAL V
	Vcsa-126870.f3712fc5.asia-northeast1.gve.goog Actiens > Summary Monitor Confexue Permissions Datasetters Host & Clusters VMs. Datastores Networks Livied vCenter Server Systems Eth	ensions Updates
	Version: 7.0.2 Bule 19272235	CPU Prec 70.08 Drie Used: 14.31 Drie Capacity: 82.38 Drie
> C HCX Management Workload		Merrory France 600, 50, 50, 50 Usawit, 150, 57, 50 Grompie Prive: 18, 76, 18
•		Used 1.69 TB Capacity: 17.47 TD

GCVE NSX-T ポータルで NSX-T セグメントを作成します

NSX-T セグメントは、Google Cloud VMware エンジンコンソールの NSX マネージャから作成および設定できま す。これらのセグメントはデフォルトの Tier-1 ゲートウェイに接続され、これらのセグメントのワークロードは East-West および North-South 接続を取得します。セグメントを作成すると、vCenter に表示されます。

1. GCVE プライベートクラウドの [概要]-> [NSX-T ログイン情報] で、[表示] を選択します。

Status Operational
Location asia-northeast1 > v-zone-a > VE Placement Group 2
Expandable No
NSX-T login info View Reset password

2. NSX-T の認証情報を書き留めておきます。

Google Cloud VMware Engine				
	 NSX-T login 			
Home	User name			
Resources	admin Copy			
کی Network	Password			
Activity	Copy			

3. [**VSPHERE** 管理ネットワーク] に移動して NSX Manager を起動し、**NSX Manager** の FQDN をクリック します。

	Resources									
	← gcp-vmware-demo									ତ (
\$	SUMMARY CLUSTERS	SUBNETS	ACTIVITY	VSPHERE	MANAGEMENT NETWORK	ADVANCED VCENTE	R SETTI	NGS DNS CONFIGURATION		
irces B	Jownload as CSV									
rork	Туре		4	Versi	on		÷	FQDN	相 🗢	IP Address
	vCenter Server Appliance			7.0.2	19272235			vcsa-126870.f3712fc5.asia-northeast1.gve.goog		10.231.0.6
2 ity	NSX Manager							nsx-127044.(3712/c5.asia-northeast1.ave.aooa		10.231.0.11
	HCX							hcx-127045.f3712fc5.asia-northeast1.gve.goog		10.231.0.13
	ESXi			7.0.2	18836573			esxi-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.f3712fr5.asia-northeast1.gve.goog		10,231,0,8

4. この手順のステップ2でメモした認証情報を使用して NSX Manager にログインします。

√Mware® NSX-T™
Username
Password
LOG IN

- 5. 新しいセグメントまたはサブネットの DHCP サービスを設定します。
- 6. サブネットを作成する前に、DHCP サービスを設定します。
- 7. NSX-T で、[ネットワーク] > [DHCP] に移動します。ネットワークダッシュボードには、サービスが Tier-0 ゲートウェイを 1 つと Tier-1 ゲートウェイを 1 つ作成していることがわかります。
- 8. DHCP サーバーのプロビジョニングを開始するには、「DHCP プロファイルの追加」をクリックします。
- 9. DHCP 名フィールドに、クライアント管理プロファイルの名前を入力します。
- 10. プロファイルタイプとして **DHCP** サーバーを選択します。
- 11.「サーバー IP アドレス」列に、DHCP サービスの IP アドレス範囲を指定します。
- 12. Edge クラスタを選択します。
- 13. [Save] をクリックして、DHCP サービスを作成します。

vm NSX-T							Q	Â	0.	×	admin	
Home Networking Secu										POLICY		
*	DHCP											
Network Overview												
🚺 Network Topology												
Connectivity		Profile Name		Profile Type	Server IP Address		Lease Time (seconds)		wh	ere Used		
😝 Tier-O Gateways		management-client-dhq			(10.230.1.254/24 ×	Enter IP Addresses	86400					
Iter-1 Gateways												
Segments						Educe						
Natural Services		Eage Cluster -	edge-cluster									
NON			Max 30 allowed. Clic									
S EV/PN Tenant												
■ NAT		SAVE CANCEL										

14. サーバの DHCP 範囲について、手順 6~13 を繰り返します。

vm NSX-T				Q	🗘 🗇 🔆 admin
Home Networking Security Inventory					POLICY MANAGER
K DHCP					
Network Overview					
Network Topology ADD CHCP PROF					
Connectivity	Profile Name	Profile Type	Server IP Address	Lease Time (seconds)	Where Used
Tier-O Gateways	server-dhcp *	DHCP Server V	10.230.2.254/24 × Enter IP Addresses	86400	
III Tier-1 Gateways					
Segments					
Natural Constant	Edge Cluster edge-cluster		- CDBes 20		
PRETABLE ATTACES	Tags (O Tag				
() VPN	Max 30 allowed. 0				
EVPN Tenant	SAVE CANCEL				
⇒ NAT					

- 15. 2 つのセグメントを作成します。1 つはクライアントと管理インターフェイス用、もう1 つはサーバーインタ ーフェイス用です。
- 16. NSX-T で、[ネットワーク]>[セグメント]に移動します。
- 17. [Add Segment] をクリックします。

vm NSX-T					
Home Networking	Security	<i>'</i>	Inver	ntory	Plan & Troubles
	« s	Seg	mei	nts	
🙆 Network Overview	2	Segm	ents	Se	gment Profiles
🔞 Network Topology		ADD	SEGM		
Connectivity			~	<u>a</u>	Segment Name
🍈 Tier-0 Gateways					Segment Name
🕕 Tier-1 Gateways				(đ)	Tier-0-Uplink-1-A
Segments				LA)	Tier-0-Uplink-1-B

- 18. セグメント名フィールドに、クライアント管理セグメントの名前を入力します。
- 19. 接続されたゲートウェイリストで、**Tier1** を選択して Tier-1 ゲートウェイに接続します。

「トランスポートゾーン」リストで「**TZ-OVERLAY」を	オーバーレイ **。
選択します	

20.

21. [サブネット]列に、サブネット範囲を入力します。サブネット範囲で・1を最後のオクテットとして指定しま す。例: 10.12.2.1/24。

Segments Segments Si	egment Profiles Edge Bridge Pro	ofiles Metadata Proxies			
ADD SEGMENT					
	Segment Name	Connected Gateway	Transport Zone	Subnets	Ports
	management-client-segme *	Tierl Tierl 🔹 *	TZ-OVERLAY ~	10.230.1.1/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7er1206.db42:1/48 SET DYCEP CONFIG	Set 🕦

22.「DHCP 構成を設定」をクリックし、「DHCP 範囲」フィールドに値を入力します。

Segment man	agement-client-segment			
IPV4 Gateway	10.230.1.1/24 #DHCP Ranges	IPV6 Gateway	Not Set #DHCP Ranges 0	
DHCP Type [#]	Local DHCP Server 🛛 🗸 🛈	DHCP Profile *	management-client-dhcp	
IPv4 Server				
Settings C	Options			
DHCP Config	C Enabled			
DHCP Server Address *	10.230.1.254/24 			
DHCP Ranges	99 Maximum Format 172.16.14.10-172.16.1 range to avoid duplicate IP address alloca	4.100 or 172.16.14.0/24 Please verify t		
	range to avoid dupicate in address anota	ition		
10.230.1.10-10.230 Enter DHCP Ran	1100 ×) Iges	ition		
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds)	Ange to avoid depicate in eduless and a nges 			
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Default value is 86400			
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Default value is 86400 Enter IP Addresses e.g. 10.10.10.10			
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Default value is 86400 Enter IP Addresses e.g. 10.10.10.10			
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Default value is 86400 Enter IP Addresses e.g. 10.10.10.10	EBON		
(10 230 1.10-10 230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Default value is 86400 Enter IP Addresses e.g. 10.10.10.10	EBON		
(10.230.1.10-10.230 Enter DHCP Ran Lease Time (seconds) DNS Servers	Ilion x Iges Default value is 86400 Enter IP Addresses e.g. 10.10.10.10	EGON		

- 23. [**Apply**]をクリックして DHCP 設定を保存します。
- 24. [保存]をクリックします。

	NOTE - Before further configurations can be done, fill out mandatory fields above (*), click 'Save' below.
>	SEGMENT PROFILES
>	DHCP STATIC BINDINGS
	CANCEL



25. サーバーセグメントについても手順 17 ~24 を繰り返します。

26. 仮想マシンの作成時に vCenter でこれらのネットワークセグメントを選択できるようになりました。

詳細については、「最初のサブネットの作成」を参照してください。

VMware クラウドへの Citrix ADC VPX インスタンスのインストール

GCVE にプライベートクラウドをインストールして設定したら、vCenter を使用して VMware Engine に仮想アプ ライアンスをインストールできます。インストールできる仮想アプライアンスの数は、プライベートクラウドで使用 可能なリソースの量によって異なります。

NetScaler VPX インスタンスをプライベートクラウドにインストールするには、プライベートクラウドのポイント ツーサイト VPN に接続されたデスクトップで以下の手順を実行します。

- 1. ESXi ホスト用の NetScaler VPX インスタンスセットアップファイルを、NetScaler ダウンロードサイトか らダウンロードします。
- 2. プライベートクラウドのポイントツーサイト VPN に接続されたブラウザで VMware vCenter を開きます。
- 3. [ユーザー名] フィールドと [パスワード] フィールドに管理者の資格情報を入力し、[ログイン] をクリックします。
- 4. [File] メニューの [Deploy OVF Template] を選択します。
- 5. [**OVF** テンプレートのデプロイ] ダイアログボックスの [ファイルからの展開] フィールドで、NetScaler VPX インスタンスセットアップファイルを保存した場所を参照し、.ovf ファイルを選択し、[次へ] をクリッ クします。
 - 注

デフォルトでは、NetScaler VPX インスタンスは E1000 ネットワークインターフェイスを使用します。 VMXNET3 インターフェイスで ADC を展開するには、E1000 ではなく VMXNET3 インターフェイスを 使用するように OVF を変更します。VMXNET3 インターフェイスの可用性は GCP インフラストラクチ ャによって制限され、Google Cloud VMware Engine では利用できない場合があります。

6. 仮想アプライアンスの OVF テンプレートに表示されるネットワークを、NSX-T Manager で設定したネット ワークにマッピングします。[作成]または[OK]をクリックします。

tual Hardware VM Options				
			A	DD NEW DEVICE
CPU	2 ~			i
Memory	2	~	GB 🗸	
Hard disk 1	20	GB 🗸		
SCSI controller 0	LSI Logic Parallel			
V Network adapter 1	management-client-se	egment 🗸		
Status	Connect At Power C	Dn		
Port ID	372795cc-b049-47b4-t	09		
Adapter Type	VMXNET 3	~		
DirectPath I/O	Enable			
Shares	Normal ~ 50		~	
Reservation	• T	~	Mbit/s ∨	
Limit	Unlimited	~	Mbit/s ∨	
MAC Address	00:50:56:a2:2c:2f	Autor	natic ~	
New Network *	server-segment	~		
Status	Connect At Power C	n		
Adapter Type	VMXNET 3	~		
DirectPath I/O	Enable			
Shares	Normal V 50		~	
Reservation	0	~	Mbit/s ∨	
Limit	Unlimited	~	Mbit/s ∨	
MAC Address		Auton	natic 🗸	
Video card	Specify custom setting	js v		
VMCI device				

7. [完了] をクリックして VMware クラウドへの仮想アプライアンスのインストールを開始します。

Deploy OVF Template	Ready to complete Click Finish to start creation.			
1 Select an OVF template	Name	NEVEX 554 121 24 29 pc 64		
2 Select a name and folder	Template name	NSVPX-E3X-13.1-24.30_11C_04		
3 Select a compute resource	Download size	661.4 MB		
4. Daview details	Size on disk	20.0 GB		
4 Review details	Folder	Workload VMs		
5 Select storage	Resource	Workload		
6 Select networks	Storage mapping	1		
7 Ready to complete	All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy		
	Network mapping	1		
	VM Network	management-client-segment		
	IP allocation settings			
	IP protocol	IPV4		
	IP allocation	Static - Manual		
		CANCEL BACK FINISH		

8. これで、NetScaler VPX インスタンスを起動する準備ができました。ナビゲーションペインで、インストー ルした Citrix ADC VPX インスタンスを選択し、右クリックメニューから [パワーオン] を選択します。コン ソールポートをエミュレートするには、「**Web** コンソールの起動」タブをクリックします。

VSphere - NSV	PX-ESX-13.0-79.6 × NSX	× +	- 0
< → C	Not secure https://192.168	0.2/ui/#?extensionId=vsphere.core.inventory.serverObjectViewsExtension&objectId=urn:vmomi:VirtualMachine:vm-53:d77eo	el. is is 🖷 🛢
w vSobere Cl	Actions - NSVPX-ESX-13.0-79.64_n.		
Ville Vopinere Cr	Power &	Power On christen B	Interaction -
vc.de7510d9c7d8-	Guest OS Snapshots Popen Remote Console	Power Off dbf+all+E # @ @ @ ACTIONS - astores Networks dbf+all+E	
 Cluster-1 esx03-r09 esx04-r02 	Gione Migrate	Bout Dever Select (15 - 15 - 16 - 0) (Al version 9) Select Called (25 - 16 - 0) (Al version 9)	CPU USAGE O HZ MEMORY USAGE
esx14-r15.c	Fault Tolerance VM Policies	DNS Name: P Addresse: Most: acr04.c01.c03.dc750/dic7d8/85ch1034 acrbs and across one	O B STORAGE USAGE
	Template Compatibility		40.83 GB
	Export System Logs	✓ Notes	^
	Edit Settings	Edit Notes	
	Move to folder Rename	Ouster-1 Custom Attributes	^
	Edit Notes	esx04-r02.p03.de7510d9c7d8485cb31194.east.	
	Tags & Custom Attributes	& client	
Recent Tasks Ala Task Name	Add Permission Alarms	v Details v Initiator v Queued For v Start Time ↓ v Completion Time	ne v Server
Reconfigure virtual machine	Remove from Inventory	ed VSPHERE LOCALIdoud 4 ms 05/02/2021, 41:08 PM 05/02/2021, 4	(11:08 PM vc.de7510d9c7d8485c
Deploy OVF template	Delete from Disk	ed VSPHERELOCAL/vpxd 3 ms 05/02/2021, 4:08:26 PM 05/02/2021, 4	09.12 PM vc.de7510d9c7d8485c

9. これで、vSphere クライアントから NetScaler 仮想マシンに接続されています。

0	🕗 vSph	here - NSV	PX-ESX-13.0-7	9.6- ×		WPX-ESX-	13.0-79	64_nc_64	×	NSX				×	+													-	٥	×
	\rightarrow	C .	Not sec	ure	https://	192.168	1.0.2/u	i/webc	onsole.h	tmi?vm	ld=vm	n-538tv	mNam	e=NSV	PX-ES	X-13.(0-79.64	_nc_648	kserver	Guid=d	177ece1	-4945-4	ee5-b	b8e-17	b4	6	£°≡			
NSVP)	K-ESX-1	13.0-79.6	64_nc_64																		Enfo	ce US Key	board	Layout	View	Fullscree	in 1	Send Ctr	1+Alt+D	elete
			NetSc	ale	r h	as s	tar	ted	suc	ces	sfu	110																		
			Start	ad	dit	iona	1 d	аем	ons	Ma	y	2 Î	6:12	2:54	4 <	loc	a 10	.err	> n	s n	scon	figd		dis	pat	ch()			
			: Inv	ali	d pa	ISSH	ord																							
			May	2 1	6:12	2:54	<1	oca	10.0	err>	ns	ns	cont	figd	l:	_d i	spa	tch():	Spe	cifi	ed p	ara	met	ers	ar	8			
			not	app	1100	ible	IO	r t	his	typ	eo	1 5	SL]	prot		e.		t a b (· · ·	T	. 1. 2. 4		_							
			нау Ман	21	6.1	2:54		oca	10.0	rr/	ns	ns la	con: et i	190	l: an	_u1 0 r	spa	tCn(atod	2	1 n 0 0	a 1 1 a a c	rui	е.							
			Mau	2 1	6:1	2:55	<1	oca	10.0	err>	ns	ns	cont	iad	say 1:	di	spa	tch():	No	such	res	our	ce						
			May	2 1	6:1	2:55	<]	oca	10.6	err>	ns	ns	con	figd	1:	_d i	spa	tch():	No :	such	pol	icy	ex	ist	s				
			Monit	MO	nit	dae	MOT	at	100	90 a	ыak	ene	d																	
			May	21	6:12	2:55		oca	10.0	err>	ns	la	sti	1855	sag	e r	epe	ated	4	tim					£ -					
			May -2	2 1	6:1.	3:00	×u	ser	.cr	17>	ns	sys	nea.		1:	sys	10	4500	10,	11	MI a	evic	e r	ead	Ia	110	1			
			Mau	2 1	6:11	3:00	<1	oca	10.6	err>	ns	ns	col	lect	::	ns	con	ufil	e()	: N	ot a	ble	to	αet	in	fo	n			
			f fil	e /	var	log	/dł	i∕de	fau	lt/n	sde	VMa	p.t:	ct	N	0 S	uch	fil	e o	r d	irec	tory		3.0 0						
			May	2 1	6:1	3:01	<]	oca	10.0	err>	ns	ns		nd [1	163	91:	ns	имоп	id d	аем	on s	tart	ed							

10. 初回起動時に、ADC インスタンスの管理 IP とゲートウェイを設定します。

11. SSH キーを使用して NetScaler アプライアンスにアクセスするには、CLI で次のコマンドを入力します。

1 ssh nsroot@<management IP address>

例

1 ssh nsroot@10.230.1.10

12. ADC の設定は、show ns ipコマンドを使用して確認できます。



VMware クラウド上の NetScaler VPX インスタンスにパブリック IP アドレスを割り当てる

GCVE に NetScaler VPX インスタンスをインストールして構成したら、クライアントインターフェイスにパブリック IP アドレスを割り当てる必要があります。VM にパブリック IP アドレスを割り当てる前に、Google Cloud リージョンでパブリック IP サービスが有効になっていることを確認してください。

新しいリージョンのパブリック IP サービスを有効にするには、次の手順に従います。

1. GCVE コンソールで、[ネットワーク]>[地域設定]>[地域の追加]に移動します。

Google	e Cloud VMware E	ngine							0	ą.	愈	Ø	\$
	Network												
ß	FIREWALL TABLES	SUBNETS	PUBLIC IPS	VPN GATEWAYS	DNS CONFIGURATION	PRIVATE CONNECTION	REGIONAL SETTINGS						
	Regional Settings											Add	Region
Resources	🕁 Download as CSV							[]] Co	umn setti	ings	∳ll, Se	lected fil	iters (0)
Retwork	Region		≑ Reg	ion Status	≑ Inter	net Access	Public IP Service	≑ Ed	ge Servic	es CID	R		4

- 2. 地域を選択し、インターネット アクセス と パブリック IP サービスを有効にします。
- 3. エッジサービス CIDR を割り当てて、CIDR 範囲がオンプレミスまたは他の GCP/GCVE サブネット (仮想ネットワーク) と重複しないようにします。

÷	Add Re	gion							
	Region '								
	asia-so	ch1			•				
		nternet Acce	ess ©						
		Public IP Serv	vice 🛛						
	Edge Ser	vices CIDR (Ð						
	10,231	ord					/	26	
	There	are no Private	Clouds in asia	-south1. Regi	onal Settings will	be applied when	a Private Clo	ad is created.	

4. 数分後に、選択したリージョンのパブリック IP サービスが有効になります。

GCVE 上の NetScaler VPX インスタンスのクライアントインターフェイスにパブリック IP を割り当てるには、 GCVE ポータルで以下の手順を実行します。

1. GCVE コンソールで、[ネットワーク]>[パブリック IP]>[割り当て]に移動します。

Googl	e Cloud VMware F	Engine							0	4	\$ đ	۲
	Network											
ß	FIREWALL TABLES	SUBNETS	PUBLIC IPS	VPN GATEWAYS	DNS-CONFIGURATION	PRIVATE CONNECTION	REGIONAL SETTINGS					
6	Public IPs (0)											Allocate
Reserves												•

- 2. パブリック IP の名前を入力します。地域を選択し、IP を使用するプライベートクラウドを選択します。
- 3. パブリック IP をマッピングするインターフェイスのプライベート IP を指定します。** これはクライアント インターフェースのプライベート IP になります ** 。
- 4. [**Submit**] をクリックします。

Googl	e Cloud VMware Engine
	← Allocate Public IP ③
Home	Name * 🐵
â	vpx-management-public-ip
Resources	Location *
	asia-northeast1 -
(ඉදුං) Network	Private cloud *
0	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. パブリック IP は数分で使用可能になります。
- 6. パブリック IP を使用する前に、パブリック IP へのアクセスを許可するファイアウォール ルールを追加する必要があります。詳細については、「ファイアウォールルール」を参照してください。

バックエンドの GCP Auto Scaling サービスを追加する

October 17, 2024

クラウドでアプリケーションを効率的にホストするには、アプリケーションの需要に応じて、簡単で費用対効果の高 いリソース管理が必要です。増加する需要を満たすには、ネットワークリソースを拡大する必要があります。需要が 収まったら、十分に活用されていないリソースによる不必要なコストを避けるために規模を縮小する必要があります。 アプリケーションの実行コストを最小限に抑えるには、トラフィック、メモリ、CPUの使用などを常に監視する必要 があります。しかし、トラフィックを手動で監視するのは煩雑です。アプリケーション環境を動的にスケールアップ またはスケールダウンするには、トラフィックの監視プロセスを自動化し、必要に応じてリソースを増減する必要が あります。

GCP 自動スケーリングサービスと統合された NetScaler VPX インスタンスには、次の利点があります。

- 負荷分散と管理:需要に応じてサーバーをスケールアップおよびスケールダウンするように自動構成します。
 VPX インスタンスはバックエンドサブネット内のマネージドインスタンスグループを自動検出し、負荷を分散 するマネージドインスタンスグループを選択できます。仮想 IP アドレスとサブネット IP アドレスは、VPX インスタンスで自動構成されます。
- 高可用性: 複数のゾーンにまたがるマネージドインスタンスグループを検出し、サーバーの負荷を分散します。
- ネットワークの可用性の向上:VPX インスタンスは以下をサポートします。

- 同じ配置グループのバックエンドサーバー
- 異なるゾーンのバックエンドサーバー

この図は、負荷分散仮想サーバーとして機能する NetScaler ADC VPX インスタンスで GCP 自動スケーリングサービスがどのように機能するかを示しています。



はじめに

NetScaler VPX インスタンスで自動スケーリングの使用を開始する前に、次のタスクを完了する必要があります。

- 要件に応じて、GCP 上に NetScaler ADC VPX インスタンスを作成します。
 - NetScaler VPX インスタンスを作成する方法の詳細については、「Google Cloud Platform に NetScaler VPX インスタンスをデプロイする」を参照してください。
 - VPX インスタンスを HA モードでデプロイする方法の詳細については、「Google Cloud Platform に VPX 高可用性ペアをデプロイする」をご覧ください。
- GCP プロジェクトで クラウドリソースマネージャー API を有効にします。

	Identity and API access ② Service account ③ Compute Engine default service account
	Access scopes Allow default access Allow full access to all Cloud APIs Set access for each API
• インスタンスの作成中に、すべての Cloud API へのフルアクセスを許可します。	Firewall 🙆

• GCP サービスアカウントに次の IAM 権限があることを確認してください。

```
REQUIRED_INSTANCE_IAM_PERMS = [
1
2
      "compute.instances.get",
3
      "compute.instanceGroupManagers.get",
4
      "compute.instanceGroupManagers.list",
5
      "compute.zones.list",
6
      "logging.sinks.create",
      "logging.sinks.delete",
7
      "logging.sinks.get",
8
      "logging.sinks.list"
9
      "logging.sinks.update",
      "pubsub.subscriptions.consume",
11
      "pubsub.subscriptions.create",
12
      "pubsub.subscriptions.delete",
13
      "pubsub.subscriptions.get",
14
15
      "pubsub.topics.attachSubscription",
      "pubsub.topics.create",
16
      "pubsub.topics.delete",
17
      "pubsub.topics.get",
18
      "pubsub.topics.getIamPolicy",
19
20
      "pubsub.topics.setIamPolicy",
21
      1
```

- 自動スケーリングを設定するには、以下が設定されていることを確認してください。
 - インスタンステンプレート
 - マネージドインスタンスグループ
 - 自動スケーリングポリシー

GCP 自動スケーリングサービスを NetScaler VPX インスタンスに追加する

GUI を使用して、ワンクリックで VPX インスタンスに自動スケーリングサービスを追加できます。次の手順を実行 して、VPX インスタンスに自動スケーリングサービスを追加します。

- 1. nsrootの認証情報を使用して VPX インスタンスにログオンします。
- 2. NetScaler VPX インスタンスに初めてログオンすると、デフォルトの Cloud Profile ページが表示されます。 ドロップダウンメニューから GCP マネージドインスタンスグループを選択し、[作成]をクリックしてクラウ ドプロファイルを作成します。

G Create Cloud Profile

Name	
DemoCloudProfile	
Virtual Server IP Address*	
192.168.2.24	V
Load Balancing Server Protocol	
HTTP	~
Load Balancing Server Port	
80	
Auto Scale Group*	
ansible-mig-defaultuser-1585300924-	~
Auto Scale Group Protocol	
HTTP	~
Auto Scale Group Port	
80	

Select this option to drain the connections gracefully. Else the connections will be dropped in the event of scale down.

- [Virtual Server IP Address] フィールドは、インスタンスに関連付けられたすべての IP アドレスか ら自動的に入力されます。
- Autoscale グループは、GCP アカウントで設定されたマネージドインスタンスグループから事前設定 されています。
- [自動スケールグループプロトコル] と [自動スケールグループポート] を選択するときは、サーバが構成 済みのプロトコルとポートでリッスンしていることを確認します。サービスグループに適切なモニター をバインドします。デフォルトでは、TCP モニターが使用されます。
- サポートされていないため、「Graceful 」チェックボックスはオフにします。
- 注

SSL プロトコルタイプ Auto Scaling の場合、クラウドプロファイルを作成すると、証明書がないため に負荷分散仮想サーバーまたはサービスグループがダウンします。証明書は、仮想サーバまたはサービ スグループに手動でバインドできます。

3. 初めてログオンした後、クラウドプロファイルを作成する場合は、GUI で [システム] > [Google Cloud Platform] > [クラウドプロファイル] に移動し、[追加] をクリックします。
| Q Search in Menu | | Google Cloud | Platform / Cloud Pro | file | | | | |
|-----------------------|--------|--------------|--------------------------|--------------------------------------|---|---------------------------------------|---------------------------|---|
| Google Cloud Platform | \sim | Cloud F | Profile 💶 | | | | C | • |
| 🕸 Cloud Profile | | | | | | | | _ |
| System | > | Add | Edit Delete | | | | | |
| AppExpert | > | Q Click here | to search or vou can ent | er Kev : Value format | | | (| G |
| Traffic Management | > | - | | | | | | _ |
| Ontimization | | \checkmark | NAME 0 | AUTO SCALE GROUP | | LOAD BALANCING VIRTUAL SERVER | AUTO SCALE GROUP PROTOCOL | |
| Optimization | | \checkmark | DemoCloudProfile | ansible-mig-defaultuser-1585300924-1 | | _CP_DemoCloudProfile_192.168.2.24_LB_ | HTTP | |
| Security | > | | | | _ | | | |
| Authentication | > | Total 1 | | | | 25 Per Pagi | e V Page 1 of 1 🔺 🕨 | |
| | | | | | | | | |

クラウドプロファイルの作成設定ページが表示されます。

G Create Cloud Profile

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	
HTTP	\sim
Auto Scale Group Port	
80	

Select this option to drain the connections gracefully. Else the connections will be dropped in the event of scale down.

Cloud Profile は、NetScaler 負荷分散仮想サーバーと、マネージドインスタンスグループのサーバーとして メンバーを含むサービスグループを作成します。バックエンドサーバーは、VPX インスタンスで構成された SNIP を介して到達可能である必要があります。

注

NetScaler リリース 13.1-42.x 以降では、GCP の同じマネージドインスタンスグループを使用して、(異なるポートを使用して)サービスごとに異なるクラウドプロファイルを作成できます。したがって、NetScaler VPX インスタンスは、パブリッククラウド内の同じ自動スケーリンググループを持つ複数のサービスをサポートします。

Q Search in Menu		Google Cloud	Platform / Cloud Profi	le			
Google Cloud Platform	\sim	Cloud F	Profile 💶				C 🗜
Cloud Profile							
System	>	Add	Edit Delete				
AppExpert	>	Q Click here	to search or you can ente	r Key : Value format			(i
Traffic Management	>						
Optimization			NAME	AUTO SCALE GROUP	COAD BALANCING VIRTUAL SE	RVER	AUTO SCALE GROUP PROTOCOL
Security	>	~	DemoCloudProfile	ansible-mig-defaultuser-1585300924-1	_CP_DemoCloudProfile_192.1	68.2.24_LB_	HTTP
Authentication	>	Total 1				25 Per Page	e V Page 1 of 1 🔹 🕨

GCP上の NetScaler VPX インスタンスの VIP スケーリングサポート

October 17, 2024

NetScaler アプライアンスはクライアントとサーバーの間に設置され、クライアント要求とサーバー応答は NetScaler アプライアンスを経由します。一般的な設置では、アプライアンス上で構成された仮想サーバーによって 接続ポイントが提供され、クライアントはこれを使用してアプライアンスの背後にあるアプリケーションにアクセス します。展開に必要なパブリック仮想 IP(VIP)アドレスの数は、ケースバイケースで異なります。

GCP アーキテクチャでは、インスタンスの各インターフェイスが異なる VPC に接続されるように制限します。GCP 上の VPC はサブネットの集合であり、各サブネットはリージョンのゾーンにまたがることができます。さらに、GCP には次の制限があります。

- パブリック IP アドレス数と NIC の数が 1:1 でマッピングされています。NIC に割り当てることができるパブ リック IP アドレスは1つだけです。
- 大容量のインスタンスタイプには最大 8 つの NIC しか接続できません。

たとえば、n1-standard-2 インスタンスは 2 つの NIC しか持つことができず、追加できるパブリック VIP は 2 つに 制限されています。詳細については、「VPC リソースクォータ」を参照してください。

NetScaler VPX インスタンスでより大規模なパブリック仮想 IP アドレスを実現するために、インスタンスのメタデ ータの一部として VIP アドレスを構成できます。NetScaler VPX インスタンスは、GCP が提供する転送ルールを内 部で使用して VIP スケーリングを実現します。NetScaler VPX インスタンスは、構成された VIP に高可用性も提供 します。ADC VPX インスタンスは、構成された VIP に高可用性も提供します。メタデータの一部として VIP アドレ スを設定した後、転送ルールの作成に使用するのと同じ IP を使用して LB 仮想サーバを設定できます。そのため、転 送ルールを使用することで、GCP 上の NetScaler VPX インスタンスでパブリック VIP アドレスを使用する際のスケ ーリング上の制限を緩和できます。

転送ルールの詳細については、「転送ルールの概要」を参照してください。

HA の詳細については、「高可用性」を参照してください。

注意事項

- Google は、各仮想 IP 転送ルールに対して追加費用を請求します。実際のコストは、作成されるエントリの数 によって異なります。関連するコストは、Google の価格設定ドキュメントから確認できます。
- 転送ルールは、パブリック VIP にのみ適用されます。展開でプライベート IP アドレスが VIP として必要な場合は、エイリアス IP アドレスを使用できます。
- 転送ルールは、LB 仮想サーバーを必要とするプロトコルに対してのみ作成できます。VIP は、その場で作成、 更新、または削除できます。同じ VIP アドレスを持つが、プロトコルが異なる新しい負荷分散仮想サーバーを 追加することもできます。

はじめに

- NetScaler VPX インスタンスは、GCP にデプロイする必要があります。
- 外部 IP アドレスは予約する必要があります。詳細については、「静的外部 IP アドレスの予約」を参照してくだ さい。
- GCP サービスアカウントに次の IAM 権限があることを確認します。

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]

- GCP プロジェクトで クラウドリソースマネージャー API を有効にします。
- スタンドアロン VPX インスタンスで VIP スケーリングを使用する場合は、GCP サービスアカウントに次の IAM 権限があることを確認してください。

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 ]
```

 高可用性モードで VIP スケーリングを使用する場合は、GCP サービスアカウントに次の IAM 権限があること を確認してください。

1	REQUIRED_IAM_PERMS = [
2	"compute.addresses.get",
3	"compute.addresses.list",
4	"compute.addresses.use",
5	"compute.forwardingRules.create",
6	"compute.forwardingRules.delete",
7	"compute.forwardingRules.get",
8	"compute.forwardingRules.list",
9	"compute.forwardingRules.setTarget",
10	"compute.instances.use",
11	"compute.instances.get",
12	"compute.instances.list",
13	"compute.instances.setMetadata",
14	"compute.subnetworks.use",
15	"compute.targetInstances.create",
16	"compute.targetInstances.list",
17	"compute.targetInstances.use",
18	"compute.zones.list",
19	1

注

高可用性モードでは、サービスアカウントに所有者または編集者の役割がない場合は、サービスアカウ ントにサービスアカウントユーザーの役割を追加する必要があります。

NetScaler VPX インスタンスでの VIP スケーリング用の外部 IP アドレスを構成する

- 1. Google Cloud コンソールで、[VM インスタンス]ページに移動します。
- 2. 新しい VM インスタンスを作成するか、既存のインスタンスを使用します。
- 3. インスタンス名をクリックします。VM インスタンスの詳細ページで、[編集]をクリックします。
- 4. 次のように入力して、カスタムメタデータを更新します。
 - キー=VIP
 - 値 = 次の JSON 形式で値を指定します。
 - {「外部予約 IP の名前」: [プロトコルのリスト], }

GCP は次のプロトコルをサポートしています。

• AH

- ESP
- ICMP
- SCT
- TCP
- UDP

 VM instance 	details	/ EDIT	也 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 configuratio 2 toring 2	s. n.		
Availability policies				
Preemptibility				
Off (recommended)				
On host maintenance				
Migrate VM instance (re	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 ad	ccess this instanc	e Learn more	
Service account				
You must stop the VM insta	nce to edit its service ac	count		
416809692761-compute@	developer.gservicead	count.com		
Cloud API access scopes				
You must stop the VM instar	nce to edit its API acces	s scopes		
Allow full access to all Clo	ud APIs			
Save Cancel				

詳細については、「カスタムメタデータ」を参照してください。

カスタムメタデータの例:

{ "外部 IP1 名":["TCP", "UDP"], "外部 IP2 名":["ICMP", "AH"]}

この例では、NetScaler VPX インスタンスは、IP、プロトコルのペアごとに1つの転送ルールを内部で作成 します。メタデータエントリは、転送ルールにマッピングされます。この例では、メタデータエントリに対し て作成される転送ルールの数を把握するのに役立ちます。

次の4つの転送ルールが作成されます。

- a) external-ip1-name \succeq TCP
- b) external-ip1-name \succeq UDP
- c) external-ip2-name と ICMP
- d) external-ip2-name と AH

注

HA モードでは、プライマリインスタンスにのみカスタムメタデータを追加する必要があります。フェー ルオーバー時に、カスタムメタデータが新しいプライマリに同期されます。

5. [保存] をクリックします。

NetScaler VPX インスタンスで外部 IP アドレスを使用した負荷分散仮想サーバーのセットアップ

ステップ 1. 負荷分散仮想サーバーを追加します。

1. [設定]>[トラフィック管理]>[負荷分散]>[仮想サーバー]>[追加]に移動します。

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 V	Q Click here to search or you can enter Key : Value format			
Load Balancing 🗸 🗸				
🟫 Virtual Servers	NAME 0	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. 名前、プロトコル、IP アドレスタイプ(IP アドレス)、IP アドレス(ADC で VIP として追加される転送ルー ルの外部 IP アドレス)、およびポートに必要な値を追加し、「**OK**」をクリックします。

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	~
IP Address Type*	
IP Address	~
IP Address*	
34 . 93 . 61 . 42	
Port*	
80	

ステップ 2. サービスまたはサービス グループを追加します。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [サービス] > [追加] に移動します。
- 2. サービス名、IP アドレス、プロトコル、およびポートに必要な値を追加し、[OK]をクリックします。

G Load Balancing Service

Basic Settings	
Service Name*	
Demo-Service	(i)
New Server Existing Server IP Address*	
10 . 30 . 1 . 54	(i)
Protocol*	
НТТР	\sim
Port*	
80	

ステップ **3:** プライマリ・インスタンスに仮想サーバを追加します。サービスまたはサービス グループを負荷分散仮 想サーバーにバインドします。

- 1. [設定] > [トラフィック管理] > [負荷分散] > [仮想サーバー] に移動します。
- 2. 手順1で構成した負荷分散仮想サーバーを選択し、[編集]をクリックします。
- 3. [サービスとサービスグループ]ページで、[負荷分散仮想サーバーサービスのバインドなし]をクリックしま す。

Basic Setti	ngs			
Name Protocol State IP Address Port Traffic Domain	Demo-vServer HTTP • DOWN 34.93.61.42 80	Listen Priority Listen Policy Expression Redirection Mode Range IFset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- NONE IP 1 - PASSIVE ENABLED NO -	
Services ar	nd Service Groups			

4. 手順3で構成したサービスを選択し、[バインド]をクリックします。

Service Binding	
Service Binding	
Select Service*	
Demo-Service	> Add Edit (i
Binding Details	
Weight	
1	

5. 構成を保存します。

GCP での VPX インスタンスのトラブルシューティング

January 15, 2025

Google Cloud Platform (GCP) は、NetScaler VPX インスタンスへのコンソールアクセスを提供します。デバ ッグできるのは、ネットワークが接続されている場合だけです。インスタンスのシステムログを表示するには、コン ソールにアクセスし、システムログファイルを確認します。

サポートケースを提出するには、GCP アカウント番号とサポート PIN コードを見つけて、NetScaler サポートに連 絡してください。名前と E メールアドレスの入力を求められます。サポート PIN を検索するには、VPX GUI にログ オンし、[システム]ページに移動します。

サポート PIN を示すシステムページの例を次に示します。

Q Search in Menu		System / System Information
Google Cloud Platform	>	System
System	\sim	
☆ 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	Ś	Last Config Saved Time Sat, 11 Jul 2020 01:53:12 UTC
AppFlow	• >	Hardware Information
Cluster	>	

NetScaler VPX インスタンスのジャンボフレーム

October 17, 2024

NetScaler VPX アプライアンスは、最大 9216 バイトの IP データを含むジャンボフレームの送受信をサポートして います。ジャンボフレームでは、標準の IP MTU サイズ(1500 バイト)を使用するよりも効率的に大きなファイル を送信することができます。

NetScaler アプライアンスは、以下の展開シナリオでジャンボフレームを使用することができます。

- ジャンボからジャンボへ。アプライアンスがデータをジャンボフレームで受信し、それを通常のフレームで送信します。
- ・ 非ジャンボからジャンボへ。アプライアンスはデータを通常のフレームとして受信し、ジャンボ フレームとして送信します。
- ジャンボから非ジャンボへ。アプライアンスがデータを通常のフレームで受信し、それをジャンボフレームで 送信します。

詳細については、「Citrix ADC アプライアンスでのジャンボフレームサポートの構成」を参照してください。

ジャンボフレームのサポートは、次の仮想化プラットフォームで実行されている NetScaler ADC VPX アプライアン スで利用できます。

- VMware ESX
- Linux-KVM プラットフォーム
- Citrix XenServer
- Amazon Web Services (AWS)

VPX アプライアンスのジャンボフレームは、MPX アプライアンスのジャンボフレームと同様に機能します。ジャン ボフレームおよびそのユースケースについて詳しくは、「MPX アプライアンスでのジャンボフレームの構成」を参照 してください。MPX アプライアンスのジャンボフレームの使用例は、VPX アプライアンスにも当てはまります。

VMware ESX で実行中の VPX インスタンスのジャンボフレームを構成する

VMware ESX サーバーで実行されている NetScaler ADC VPX アプライアンスでジャンボフレームを構成するには、 次のタスクを実行します。

- VPX アプライアンスのインターフェイスまたはチャネルの MTU を 1501~9000 の範囲の値に設定します。 CLI または GUI を使用して MTU サイズを設定します。VMware ESX 上で動作する NetScaler VPX アプラ イアンスは、最大 9000 バイトの IP データのみを含むジャンボフレームの送受信をサポートします。
- 管理アプリケーションを使用して、VMware ESX サーバーの対応する物理インターフェイスで同じ MTU サイズを設定します。VMware ESX の物理インターフェイスでの MTU サイズの設定の詳細については、 http://vmware.com/を参照してください。

Linux-KVM サーバーで実行されている VPX インスタンスのジャンボフレームを構成する

Linux-KVM サーバーで実行されている NetScaler VPX アプライアンスでジャンボフレームを構成するには、次の タスクを実行します。

- VPX アプライアンスのインターフェイスまたはチャネルの MTU を 1501~9216 の範囲の値に設定します。 NetScaler VPX CLI または GUI を使用して MTU サイズを設定します。
- 2. 管理アプリケーションを使用して、Linux-KVM サーバーの対応する物理インターフェイスで同じ MTU サイズを設定します。Linux-KVM の物理インターフェイスの MTU サイズの設定の詳細については、 http://www.linux-kvm.org/を参照してください。

Citrix XenServer 上で実行されている VPX インスタンスのジャンボフレームを構成する

Citrix XenServer で実行されている NetScaler VPX アプライアンスでジャンボフレームを構成するには、次のタス クを実行します。

- 1. XenCenter を使用して XenServer に接続します。
- 2. MTU を変更する必要があるネットワークを使用するすべての VPX インスタンスをシャットダウンします。
- 3. [ネットワーク]タブで、ネットワーク-[ネットワーク 0/1/2]を選択します。
- 4. [プロパティ]を選択し、MTU を編集します。

XenServer でジャンボフレームを構成した後、ADC アプライアンスでジャンボフレームを構成できます。詳細については、「Citrix ADC アプライアンスでのジャンボフレームサポートの構成」を参照してください。

AWS で実行中の VPX インスタンスのジャンボフレームを設定する

Azure 上の VPX では、ホストレベルの構成は不要です。VPX でジャンボフレームを構成するには、Citrix ADC アプ ライアンスでのジャンボフレームサポートの構成に記載されている手順に従います。

NetScaler の導入と構成を自動化する

October 17, 2024

NetScaler には、ADC の展開と構成を自動化するための複数のツールが用意されています。このドキュメントでは、 さまざまな自動化ツールの概要と、ADC 構成の管理に使用できるさまざまな自動化リソースの参照について説明しま す。

次の図は、ハイブリッドマルチクラウド(HMC)環境における NetScaler 自動化の概要を示しています。



NetScaler ADM を使用して NetScaler を自動化する

NetScaler ADM は、分散 ADC インフラストラクチャへの自動化制御ポイントとして機能します。NetScaler ADM は、ADC アプライアンスのプロビジョニングからアップグレードまで、包括的な自動化機能セットを提供します。 ADM の主な自動化機能は次のとおりです:

- AWS での NetScaler VPX インスタンスのプロビジョニング
- Azure での NetScaler VPX インスタンスのプロビジョニング
- StyleBooks
- 構成ジョブ
- 構成監査
- ADC アップグレード
- SSL 証明書の管理
- 統合- GitHub、ServiceNow、イベント通知の統合

NetScaler ADM の自動化に関するブログとビデオ

- StyleBooks を使用したアプリケーションの移行
- ADM スタイルブックを使用して ADC 構成を CI/CD と統合する
- ADM によるパブリッククラウドの NetScaler 導入の簡素化
- NetScaler ADM サービスが NetScaler のアップグレードを容易にする 10 の方法

NetScaler ADM は、全体的な IT 自動化の一環として NetScaler ADM と NetScaler を統合するさまざまな機能用 の API も提供します。詳細については、「NetScaler ADM サービス API」を参照してください。

Terraform を使用して NetScaler を自動化する

Terraform は、クラウド、インフラストラクチャ、またはサービスのプロビジョニングと管理に、インフラストラ クチャをコードアプローチとして採用するツールです。NetScaler テラフォームリソースは、GitHub で使用できま す。詳細なドキュメントと使用法については、GitHub を参照してください。

- NetScaler Terraform モジュールにより、負荷分散や GSLB などのさまざまなユースケースに合わせて ADC を構成できます
- AWS に ADC をデプロイするための Terraform クラウドスクリプト
- Azure に ADC をデプロイするための Terraform クラウドスクリプト
- Terraform クラウドスクリプトで ADC を GCP にデプロイ
- NetScaler VPX および Azure パイプラインを使用したブルーグリーン展開

Terraform の ADC 自動化に関するブログとビデオ

- Terraform で NetScaler の展開を自動化
- Terraform を使用した AWS の HA セットアップで ADC をプロビジョニングおよび設定する

領事-Terraform-Sync を使用して NetScaler を自動化する

NetScaler Consul-Terraform-Sync(CTS)モジュールにより、アプリケーションチームはサービスの新しいイン スタンスを NetScaler に自動的に追加または削除できます。必要な ADC 構成の変更を行うために、IT 管理者やネッ トワーキングチームに手動でチケットを提出する必要はありません。

- ネットワークインフラストラクチャ自動化のための NetScaler 領事 Terraform-Sync モジュール
- Citrix-HashiCorp 共同ウェビナー: Terraform Enterprise および NetScaler 向けの領事 Terraform-Sync を使用した動的ネットワーキング

Ansible を使用して NetScaler を自動化する

Ansible は、インフラストラクチャをコードとして実現する、オープンソースのソフトウェアプロビジョニング、構成管理、およびアプリケーションデプロイメントツールです。NetScaler Ansible モジュールとサンプルプレイブックは、GitHub にあります。詳細なドキュメントと使用法については、GitHub を参照してください。

- ADC を構成するための Ansible モジュール
- ADC Ansible モジュールドキュメント/リファレンスガイド
- ADM 用の Ansible モジュール

Citrix は認定された AnsibleAutomation パートナーです。Red Hat Ansible オートメーションプラットフォーム のサブスクリプションをお持ちのユーザーは、Red Hat オートメーションハブから NetScalerコレクションにアク セスできます。

Terraform と Ansible の自動化ブログ

- Citrix、HashiCorp 統合パートナー・オブ・ザ・イヤーに選出
- Citrix は Red Hat Ansible オートメーションプラットフォーム認定パートナーになりました
- アプリケーションの配信とセキュリティのための Terraform と Ansible Automation

ADC 展開用のパブリッククラウドテンプレート

パブリッククラウドテンプレートは、パブリッククラウドでのデプロイメントのプロビジョニングを簡素化します。 さまざまな環境で、さまざまな NetScaler テンプレートを使用できます。使用方法の詳細については、それぞれの GitHub リポジトリを参照してください。

AWS CFT:

• AWS で NetScaler VPX をプロビジョニングするための CFT

Azure Resource Manager (ARM) テンプレート:

• Azure で NetScaler VPX をプロビジョニングするための ARM テンプレート

Google Cloud デプロイメントマネージャー (GDM) テンプレート:

• Google で NetScaler VPX をプロビジョニングするための GDM テンプレート

テンプレートに関する動画

- クラウドフォーメーションテンプレートを使用して NetScaler HA を AWS にデプロイ
- AWS クイックスタートを使用してアベイラビリティーゾーン全体に NetScaler HA
- GDM テンプレートを使用した GCP での NetScaler HA の展開

NITRO API

NetScaler NITRO プロトコルを使用すると、表現状態転送(REST)インターフェイスを使用して、NetScaler ア プライアンスをプログラムで構成および監視できます。そのため、NITRO アプリケーションはあらゆるプログラミ ング言語で開発することができます。Java、.NET、または Python で開発する必要があるアプリケーションの場合、 NITRO API は、個別のソフトウェア開発キット (SDK) としてパッケージ化された関連ライブラリを通じて公開され ます。

- NITRO API ドキュメント
- NITRO API を使用した ADC ユースケースの設定例

よくある質問

January 15, 2025

次のセクションでは、Citrix アプリケーション Delivery Controller(ADC)VPX に基づいて FAQ を分類するのに 役立ちます。

- 機能と機能
- 暗号化
- 価格設定と梱包
- NetScaler VPX Express と 90 日間の無料トライアル
- ハイパーバイザー
- キャパシティプランニングまたはサイジング
- システム要件
- その他の技術的なよくある質問

機能と機能

NetScaler VPX とは何ですか?

NetScaler VPX は、業界標準のサーバーにインストールされた Hypervisor でホストできる仮想 ADC アプライアン スです。

NetScaler VPX には、すべての Web アプリケーション最適化機能が ADC アプライアンスとして含まれています か

はい。NetScaler VPX には、すべての負荷分散、トラフィック管理、アプリケーションアクセラレーション、アプリ ケーションセキュリティ(NetScaler Gateway および Citrix アプリケーションファイアウォールを含む)、および オフロード機能が含まれています。NetScaler の機能と機能の完全な概要については、「アプリケーションの配信方 法」を参照してください。

Citrix アプリケーションファイアウォールを NetScaler VPX で使用する場合、制限はありますか?

NetScaler VPX 上の Citrix アプリケーションファイアウォールは、NetScaler アプライアンスと同じセキュリティ 保護を提供します。Citrix アプリケーションファイアウォールのパフォーマンスまたはスループットは、プラットフ ォームによって異なります。 NetScaler VPX 上の NetScaler Gateway と NetScaler アプライアンスの NetScaler Gateway の間に違い はありますか?

機能的には同じです。NetScaler VPX 上の NetScaler Gateway は、NetScaler ソフトウェアリリース 14.1 で利 用可能なすべての NetScaler Gateway 機能をサポートします。ただし、NetScaler アプライアンスは専用の SSL アクセラレーションハードウェアを提供するため、NetScaler VPX インスタンスよりも優れた SSL VPN スケーラビ リティを提供します。

NetScaler VPX はハイパーバイザー上で実行できるという明らかな違い以外に、NetScaler の物理アプライアン スとどう違うのですか

顧客に行動の違いが見られる主な領域は 2 つあります。1 つ目は、NetScaler VPX は多くの NetScaler アプライア ンスと同じパフォーマンスを提供できないことです。2 つ目は、NetScaler アプライアンスは独自の L2 ネットワー ク機能を組み込んでいるが、NetScaler VPX は L2 ネットワークサービスのために Hypervisor に依存していると いうことです。一般的に、NetScaler VPX の展開方法は制限されません。物理 NetScaler アプライアンスに構成さ れている特定の L2 機能は、基盤となる Hypervisor で構成する必要があります。

NetScaler VPX は、アプリケーションデリバリー市場でどのように役割を果たしていますか?

NetScaler VPX は、アプリケーション配信市場のゲームを次のように変えます。

- NetScaler アプライアンスをさらに手頃な価格にすることで、NetScaler VPX は、あらゆる IT 組織が NetScaler アプライアンスを展開できるようにします。これは、最もミッションクリティカルな Web アプリ ケーションだけでなく、すべての Web アプリケーション用です。
- NetScaler VPX を使用すると、データセンター内でネットワーキングと仮想化をさらに統合できます。 NetScaler VPX は、仮想サーバーでホストされている Web アプリケーションを最適化するためだけに使用 することはできません。また、Web アプリケーションの配信自体を、どこでも簡単かつ迅速に展開できる仮 想化サービスにすることができます。IT 組織は、Web アプリケーション配信インフラストラクチャのプロビ ジョニング、自動化、チャージバックなどのタスクに標準的なデータセンタープロセスを使用します。
- NetScaler VPX は、物理アプライアンスだけを使用する場合は実用的ではない新しい展開アーキテクチャを 開きます。NetScaler VPX および NetScaler MPX アプライアンスは、圧縮やアプリケーションファイアウォ ール検査などのプロセッサ負荷の高いアクションを処理するために、各アプリケーションの個々のニーズに合 わせてベースで使用できます。データセンターエッジでは、NetScaler MPX アプライアンスは、初期トラフ ィック分散、SSL 暗号化または復号化、サービス拒否(DoS)攻撃防止、グローバル負荷分散など、大量のネ ットワーク全体のタスクを処理します。高性能の NetScaler MPX アプライアンスと展開しやすい NetScaler VPX 仮想アプライアンスを組み合わせることで、データセンター全体のコストを削減しながら、最新の大規模 データセンター環境に比類のない柔軟性とカスタマイズ機能を提供します。

NetScaler VPX はシトリック Citrix デリバリーセンター戦略にどのように適合していますか

NetScaler VPX を利用することで、Citrix デリバリーセンターの全サービスを仮想化されたサービスとして利用でき ます。Citrix XenCenter で利用可能な強力な管理、プロビジョニング、監視、およびレポート機能によって、Citrix デリバリーセンター全体がメリットを得られます。これは、ほぼすべての環境に迅速に導入でき、どこからでも一元 的に管理できます。1 つの統合された仮想化アプリケーション配信インフラストラクチャにより、組織はデスクトッ プ、クライアント/サーバーアプリケーション、Web アプリケーションを配信できます。

暗号化

NetScaler VPX は **SSL** オフロードをサポートしていますか?

はい。ただし、NetScaler VPX はすべての SSL 処理をソフトウェアで行うため、NetScaler VPX は NetScaler ア プライアンスと同じ SSL パフォーマンスを提供しません。NetScaler VPX は、毎秒最大 750 の新しい SSL トラン ザクションをサポートできます。

NetScaler VPX をホストするサーバーにインストールされているサードパーティの SSL カードは、SSL 暗号化または復号化を高速化しますか?

いいえ。NetScaler VPX ライセンスは、基盤となる Hypervisor から独立しています。NetScaler VPX 仮想マシン をある Hypervisor から別の Hypervisor に移動する場合は、新しいライセンスを取得する必要はありません。ただ し、既存の NetScaler VPX ライセンスを再ホストする必要がある場合があります。

NetScaler VPX は、物理的な NetScaler アプライアンスと同じ暗号化暗号をサポートしていますか?

VPX は、ECDSA を除くすべての暗号化暗号を物理 NetScaler アプライアンスとしてサポートします。

NetScaler VPX SSL トランザクションスループットとは何ですか?

SSL トランザクションのスループットについては、NetScaler VPX のデータシートを参照してください。

価格設定と梱包

NetScaler VPX はどのようにパッケージ化されていますか

NetScaler VPX の選択は、NetScaler アプライアンスの選択に似ています。まず、お客様は、機能要件に基づいて NetScaler エディションを選択します。次に、スループット要件に基づいて、特定の NetScaler VPX 帯域幅層を選 択します。NetScaler VPX は、スタンダード、アドバンスエディション、およびプレミアムエディションで利用でき ます。NetScaler VPX は、10Mbps(VPX 10)から 100Gbps(VPX 100G)まで対応している。詳細については、 NetScaler VPX のデータシートを参照してください。

NetScaler VPX の価格はすべての Hypervisor で同じですか?

はい。

すべての Hypervisor で VPX に同じ NetScaler SKU が使用されていますか?

はい。

NetScaler VPX ライセンスをある **Hypervisor** から別の **Hypervisor** に移動できますか(たとえば、**VMware** から **Hyper-V** へ)**?**

はい。NetScaler VPX ライセンスは、基盤となるハイパーバイザーとは独立しています。NetScaler VPX 仮想マシ ンをあるハイパーバイザーから別のハイパーバイザーに移動する場合、新しいライセンスを取得する必要はありませ ん。ただし、既存の NetScaler VPX ライセンスを再ホストする必要がある場合があります。

NetScaler VPX インスタンスはアップグレードできますか?

はい。スループット制限と NetScaler ファミリエディションの両方をアップグレードできます。両方のタイプのアッ プグレードのアップグレード SKU が利用可能です。

NetScaler VPX を高可用性ペアに展開する場合、必要なライセンスはいくつですか

NetScaler 物理アプライアンスと同様に、NetScaler 高可用性構成には 2 つのアクティブなインスタンスが必要で す。したがって、お客様は 2 つのライセンスを購入する必要があります。

NetScaler VPX Express と 90 日間の無料トライアル

NetScaler VPX Express には、NetScaler 標準機能がすべて含まれていますか? NetScaler Gateway と、 Citrix Virtual Apps Web インターフェイスと XML ブローカーの負荷分散が含まれていますか

はい。NetScaler VPX Express には、NetScaler Premium の完全な機能が含まれています。NetScaler リリース 14.1~29.65 以降、NetScaler は VPX Express の動作を変更しました。

NetScaler VPX Express にはライセンスが必要ですか

最新の NetScaler VPX Express リリース (14.1~29.65 以降) では、VPX Express は無料で使用でき、インストー ルや使用にライセンス ファイルは必要ありません。いかなる約束も必要ありません。すでに VPX Express ライセン スをお持ちの場合は、以前のライセンス動作が引き続き有効になります。ただし、既存の VPX Express ライセンス フ ァイルを削除し、バージョン 14.1~29.65 以降を使用すると、更新された VPX Express の動作が適用されます。

NetScaler VPX Express ライセンスは期限切れになりますか

新しい VPX Express にはライセンスも有効期限もありません。すでに VPX エクスプレス ライセンスをお持ちの場 合、ライセンスはダウンロード後1年で期限切れになります。

NetScaler VPX Express は、NetScaler MPX アプライアンスと同じ暗号化暗号をサポートしていますか

一般的な可用性のために、NetScaler アプライアンスでサポートされている同じ強力な暗号化暗号はすべて、 NetScaler VPX および NetScaler VPX Express で利用できます。これは、同じ輸出入規制の対象となります。

NetScaler VPX Express のテクニカルサポートケースを報告できますか

いいえ。NetScaler VPX Express ユーザーは、NetScaler VPX ナレッジ センターを自由に使用でき、ディスカッシ ョン フォーラムを使用してコミュニティにサポートをリクエストすることもできます。

NetScaler VPX Express を製品版にアップグレードできますか?

はい。必要な小売用 NetScaler VPX ライセンスを購入し、対応するライセンスを NetScaler VPX Express インス タンスに適用するだけです。

ハイパーバイザー

NetScaler VPX はどのバージョンの VMware をサポートしていますか

NetScaler VPX は、バージョン 3.5 以降では、VMware ESX と ESXi の両方をサポートしています。詳細について は、サポート マトリックスと使用ガイドラインを参照してください。

VMware の場合、VPX に割り当てることができる仮想ネットワーク・インタフェースはいくつですか?

最大 10 個の仮想ネットワークインターフェイスを NetScaler VPX に割り当てることができます。

vSphere から、NetScaler VPX コマンドラインにどのようにアクセスできますか

VMware vSphere クライアントは、コンソールタブから NetScaler VPX コマンドラインへの組み込みアクセスを 提供します。また、任意の SSH または Telnet クライアントを使用してコマンドラインにアクセスすることもできま す。NetScaler VPX の NSIP アドレスは、SSH または Telnet クライアントで使用できます。

NetScaler VPX GUI にはどのようにアクセスできますか

NetScaler VPX GUI にアクセスするには、任意のブラウザーのアドレスフィールドに、NetScaler VPX の NSIP (たとえば、http://NSIP address) を入力します。

同じ VMware ESX にインストールされている 2 つの NetScaler VPX インスタンスを高可用性セットアップで構成できますか?

はい、でもお勧めできません。ハードウェア障害は、両方の NetScaler VPX インスタンスに影響します。

2 つの異なる VMware ESX システム上で実行されている 2 つの NetScaler VPX インスタンスを、高可用性セットアップで構成できますか?

はい。これは、高可用性セットアップで推奨されます。

VMware の場合、インターフェイス関連のイベントは NetScaler VPX でサポートされていますか

いいえ。インターフェイス関連のイベントはサポートされていません。

VMware の場合、タグ付き VLAN は NetScaler VPX でサポートされていますか?

はい。NetScaler タグ付き VLAN は、リリース 11.0 以降の NetScaler VPX でサポートされています。詳しくは、 NetScaler のドキュメントを参照してください。

VMware の場合、リンクアグリゲーションと LACP は NetScaler VPX でサポートされていますか?

いいえ。なしリンクアグリゲーションと LACP は、NetScaler VPX ではサポートされていません。リンクアグリゲ ーションは VMware レベルで設定する必要があります。

NetScaler VPX ドキュメントにはどのようにアクセスするのですか

このドキュメントは、NetScaler VPX GUI から入手できます。ログイン後、[ドキュメント] タブを選択します。

キャパシティプランニングまたはサイジング

NetScaler VPX で期待できるパフォーマンスは何ですか

NetScaler VPX は、優れたパフォーマンスを提供します。NetScaler VPX を使用して達成可能な特定のパフォーマンスレベルについては、NetScaler VPX のデータシートを参照してください。

サーバーの CPU パワーが変化することを考えると、NetScaler インスタンスの最大パフォーマンスをどのように 見積もることができますか?

より高速な CPU を使用すると(ライセンスで許可されている最大値まで)パフォーマンスが向上しますが、低速の CPU を使用すると、パフォーマンスが確実に制限されます。

NetScaler VPX の帯域幅またはスループットの制限は、インバウンドのみのトラフィック、またはインバウンドと アウトバウンドの両方のトラフィックですか

NetScaler VPX 帯域幅制限は、要求トラフィックか応答トラフィックかにかかわらず、NetScaler への着信トラフ ィックにのみ適用されます。これは、NetScaler VPX-1000(たとえば)が1Gbpsのインバウンドトラフィックと 1Gbpsのアウトバウンドトラフィックの両方を同時に処理できることを示します。インバウンドおよびアウトバウ ンドトラフィックは、要求および応答トラフィックと同じではありません。NetScaler では、エンドポイントからの トラフィック(リクエストトラフィック)とオリジンサーバーからのトラフィック(レスポンストラフィック)の両 方が「インバウンド」(つまり、NetScaler に着信)です。

同じサーバー上で NetScaler VPX 複数のインスタンスを実行できますか?

はい。Hypervisor 上に物理 NIC が 1 つしかない NetScaler VPX 構成ユーティリティを使用して、最大 7 つのイン ターフェイス(VMware では 10)を追加できます。

NetScaler VPX の複数のインスタンスが物理サーバーで実行されている場合、**NetScaler VPX** インスタンスごと の最小ハードウェア要件は何ですか**?**

各 NetScaler VPX インスタンスには、2 GB の物理 RAM、20 GB のハードディスク容量、および 2 つの vCPU を割 り当てる必要があります。2 ギガバイトの VPX 重要な展開では、システムがメモリに制約のある環境で動作するた め、VPX に 2 GB の RAM を使用することはお勧めしません。これにより、スケール、パフォーマンス、または安定性 に関連する問題が発生する可能性があります。4 GB または 8 GB のメモリが推奨されます。

注

NetScaler VPX は、レイテンシーに敏感で高性能な仮想アプライアンスです。期待されるパフォーマンスを実現するには、アプライアンスに vCPU 予約、メモリ予約、ホストでの vCPU ピン接続が必要です。また、ホス

ト上でハイパースレッディングを無効にする必要があります。ホストがこれらの要件を満たさない場合、高可 用性フェイルオーバー、VPX インスタンス内の CPU スパイク、VPX CLI へのアクセスにおける低速化、ピッ トボスデーモンのクラッシュ、パケットドロップ、低スループットなどの問題が発生します。

すべての VPX インスタンスが事前定義された条件を満たしていることを確認してください。

NetScaler VPX と他のアプリケーションを同じサーバーでホストできますか?

はい。たとえば、NetScaler VPX、Citrix Virtual Apps Web インターフェイス、および Citrix Virtual Apps XML ブローカーはすべて仮想化でき、同じサーバー上で実行できます。最高のパフォーマンスを得るには、実行中のすべ てのワークロードをサポートするのに十分な CPU および I/O 容量が物理ホストにあることを確認します。

単一の NetScaler VPX インスタンスに CPU コアを追加すると、そのインスタンスのパフォーマンスが向上します か**?**

はい、NetScaler VPX インスタンスに追加の vCPU のライセンスが付与されている場合、CPU コアを追加すると NetScaler VPX のパフォーマンスが向上します。NetScaler VPX は、構成とパフォーマンス層に応じて、最大 20 個の vCPU (41 Gbps ~100 Gbps のパフォーマンス)をサポートできます。特に高パフォーマンスのシナリオでは、 vCPU を増やすとスループットが向上します。ただし、パフォーマンスへの影響は、ネットワーク ドライバー (PCI パススルーや SR-IOV など) や特定のワークロードなどの要因によっても異なります。さまざまな VPX パフォーマン ス層でサポートされる vCPU の数については、NetScaler VPX データ シートを参照してください。

NetScaler VPX がアイドル状態のにもかかわらず、CPU の 90%以上を消費しているように見えるのはなぜですか?

これは正常な動作であり、NetScaler アプライアンスは同じ動作を示します。NetScaler VPX CPU 使用率の実程度 を確認するには、NetScaler CLI で stat CPU コマンドを使用するか、NetScaler GUI から NetScaler VPX CPU 使用率を表示します。NetScaler パケット処理エンジンは、やるべき作業がない場合でも、常に「仕事を探している」 ことです。したがって、CPU を制御し、それを解放しないためにすべてを行います。NetScaler VPX がインストー ルされたサーバーでは、NetScaler VPX が CPU 全体を消費しているような外観になります(Hypervisor の観点か ら)。CLI または GUI を使用した「NetScaler 内部」からの CPU 使用率を見ると、NetScaler VPX CPU 容量が使 用されている様子が表示されます。

システム要件

NetScaler VPX 最小ハードウェア要件を教えてください

次の表では、NetScaler VPX 最小ハードウェア要件について説明しています。

|種類|要件| |_____|____

- |

| プロセッサ | VPX プラットフォームのプロセッサ要件については、を参照してください。[NetScaler VPX でサポートされているプロセッサ](/ja-jp/vpx/current-release/supported-hypervisors-featureslimitations.html#supported-processors-for-netscaler-vpx) テーブル。|

|メモリ|最低 2 GB。ただし、4 GB が推奨されます。|

|ディスク|最低 20 GB のハードドライブ。|

| ハイパーバイザー | Citrix Hypervisor 5.6 以降、VMware ESX/ESXi 3.5 以降、または Hyper-V を搭載した Windows Server 2008 R2 |

|ネットワーク接続性 | 最小値は 100 Mbps ですが、1 Gbps が推奨されます。|

|NIC|ハイパーバイザーと互換性のある NIC を使用します。詳細については、以下を参照してください。 [NetScaler VPX でサポートされている NIC](/ja-jp/vpx/current-release/supported-hypervisors-featureslimitations.html#supported-nics-for-netscaler-vpx).|

注

- 重要な導入環境では、NetScaler VPX には 4 GB のメモリが推奨されます。2 GB のメモリを搭載した NetScaler VPX は、メモリに制約のある環境で動作します。これにより、スケール、パフォーマンス、または安定性に関連する問題が発生する可能性があります。
- NetScaler 13.1 リリース以降、VMware ESXi ハイパーバイザー上の NetScaler VPX インスタンスは AMD EPYC プロセッサをサポートしています。

システム要件の詳細については、NetScaler VPX のデータシートを参照してください。

インテル **VT-x** とは何ですか**?**

これらの機能は「ハードウェアアシスト」または「仮想化アシスト」と呼ばれることもあり、ゲスト OS が実行 する機密性の高い CPU 命令や特権が必要な CPU 命令をハイパーバイザーにトラップアウトします。これにより、 Hypervisor でのゲスト OS(NetScaler VPX 用の BSD)のホスティングが簡単になります。

VT-X はどれくらい一般的ですか

多くのサーバーでは、仮想化支援機能 (VT-x や AMD-V など) が BIOS 設定でデフォルトで無効になっています。 NetScaler VPX を実行できないと判断する前に、BIOS 構成を確認してください。仮想化サポートが無効になってい る場合は、サーバーが NetScaler VPX などの仮想化アプリケーションを適切に実行できるように、BIOS で仮想化 サポートを有効にする必要があります。

NetScaler VPX ハードウェア互換性リスト(HCL)はありますか?

サーバーが Intel VT-X をサポートしている限り、NetScaler VPX は、基盤となる Hypervisor と互換性のあるサー バーで実行する必要があります。サポートされるプラットフォームの包括的なリストについては、Hypervisor HCL を参照してください。

NetScaler VPX はどのバージョンの NetScaler OS をベースにしていますか

NetScaler VPX は、NetScaler 9.1 以降のリリースをベースにしています。

NetScaler VPX は BSD 上で動作するので、BSD Unix がインストールされているサーバーでネイティブに実行で きますか

いいえ。NetScaler MPX アプライアンスは、NetScaler VPX が提供するよりも高い SSL スループットが必要な場 合に使用する必要があります。ハイパーバイザーのサポートの詳細については、NetScaler VPX データ シートを参 照してください。

その他の技術的なよくある質問

複数の NIC を持つ物理サーバでのリンクアグリゲーションは機能しますか?

LACP はサポートされていません。Citrix Hypervisor では、静的リンクアグリゲーションがサポートされ、4 つ のチャネルと 7 つの仮想インターフェイスの制限があります。VMware の場合、静的リンクアグリゲーションは NetScaler VPX 内ではサポートされていませんが、VMware レベルで構成できます。

MAC ベースの転送 (MBF) は VPX でサポートされていますか? NetScaler アプライアンスの実装から変更はありますか?

MBF はサポートされており、NetScaler アプライアンスと同じように動作します。Hypervisor は基本的に、 NetScaler VPX から受信したすべてのパケットを外部に切り替え、逆に切り替えます。

NetScaler VPX のアップグレードプロセスはどのように実行されますか?

アップグレードは、NetScaler アプライアンスの場合と同じ方法で実行されます。カーネルファイルをダウンロード し、GUI で install ns またはアップグレードユーティリティを使用します。 フラッシュとディスク容量はどのように割り当てられますか。それを変えることはできますか

各 NetScaler VPX インスタンスには、最低 2 GB のメモリを割り当てる必要があります。NetScaler VPX ディスク イメージのサイズは、最大 4GB のコアダンプ、ログファイル、トレースファイルを保存するためのスペースなど、保 守性のニーズに対応するために 20GB に設定されています。これより小さいディスクイメージを生成することは可能 ですが、現時点ではこれを実行する予定はありません。/flashおよび/varは両方とも同じディスクイメージ内に あります。互換性を保つために、これらは別々のファイル システムとして保持されます。

次の値は、NetScaler VPX インスタンス上の特定のディレクトリに割り当てられたディスク容量を表します。

- /フラッシュ=965M
- /var = 14G

互換性のために別々のファイルシステムとして保管されています。メモリ割り当ての推奨事項の詳細については、 NetScaler VPX データシートを参照してください。

新しいハードドライブを追加して、NetScaler VPX インスタンスのスペースを増やすことはできますか

はい。NetScaler リリース 13.1 ビルド 21.x 以降では、2 台目のディスクを追加して NetScaler VPX インスタンス のディスク容量を増やすことができます。2 番目のディスクを接続すると、「/var/crash」ディレクトリが自動的にこ のディスクにマウントされます。2 つ目のディスクは、コアファイルの保存とロギングに使用されます。コアファイ ルとログファイルの保存に使用される既存のディレクトリは、以前と同様に機能します。

注

データの損失を防ぐために、NetScaler アプライアンスのダウングレード時に外部バックアップを作成します。

クラウド上の NetScaler VPX インスタンスに新しいハードディスクドライブ(HDD)を接続する方法については、 以下を参照してください。

• Azure ドキュメンテーション

注

Azure にデプロイされた NetScaler VPX インスタンスにセカンダリ ディスクを接続するには、Azure VM サイズにローカル一時ディスクがあることを確認します。詳細については、「ローカル一時ディスク なしの Azure VM サイズ」を参照してください。

- AWS ドキュメント
- GCP ドキュメント

警告:

NetScaler VPX に新しい HDD を追加した後、新しい HDD に移動されたファイルに対して機能するスクリプトの一部が、次の条件下で失敗する可能性があります。

「link」シェルコマンドを使用して、新しい HDD に移動されたファイルへのハードリンクを作成した場合。 シンボリックリンクを使用するには、このようなコマンドはすべて「ln-s」に置き換えてください。また、失敗 したスクリプトを適宜修正してください。

NetScaler VPX のプライマリ ディスクのサイズを増やすことはできますか?

NetScaler リリース 14.1 ビルド 21.x 以降、管理者は NetScaler VPX プライマリディスクサイズを一度に 20 GB から 1TB に動的に増やすことができます。その後、再び最大 1 TB まで増やすことができます。ディスク容量を増や すには、それぞれのクラウドまたはハイパーバイザー UI でプライマリディスクサイズを少なくとも 1 GB に拡張しま す。

注

ディスクのサイズを増やすことしかできません。新しいサイズを割り当てると、後でサイズを減らすことはで きません。そのため、必要な場合にのみディスクサイズを増やしてください。

NetScaler VPX プライマリディスクサイズを手動で増やすにはどうすればよいですか?

次の手順に従って、ハイパーバイザーまたはクラウドから VPX プライマリディスクサイズを手動で増やします:

- 1. 仮想マシンをシャットダウンします。
- 2. デフォルトのディスクサイズである 20 GB をより高い値に拡張します。たとえば、20 ギガバイトから 30 ギ ガバイトまたは 40 ギガバイトです。Azure の場合は、デフォルトのディスクサイズである 32 GB を 64 GB に拡張します。
- 3. VM の電源を入れ、ブートプロンプトを入力します。
- 4.「boot-s」コマンドを使用してシングルユーザーモードにログインします。
- 5. ディスク容量を確認してください。新しく割り当てられたディスク容量は、「gpart show」コマンドを使用して確認できます。
- 6. パーティション名を書き留めておきます。たとえば、VM パーティションは da0 です。
- 7.「gpart resize」コマンドを使用してディスクパーティションのサイズを変更します。
 例:次のコマンドを実行して、da0 MBR パーティションのサイズを変更し、10 GB の空き領域を含めます。
 gpart resize -i 1 da0
- 8. 空き領域を最後のパーティションにマージします。

例 gpart resize -i 5 da0s1 9.「growfs」コマンドを使用して、新しく割り当てられた空き領域を含むようにファイルシステムを拡張します。 例

growfs /dev/ada0s1e

10. VM を再起動し、シェルプロンプトで「df-h」コマンドを使用して増加したディスク容量を確認します。

NetScaler VPX ビルドの番号付けと、他のビルドとの相互運用性に関して、どのようなことが期待できますか?

NetScaler VPX には、9.1 と同様のビルド番号が付けられています。Cl (クラシック) と 9.1. Nc (nCore) リリース。 たとえば、9.1_97.3.vpx、9.1_97.3.nc、9.1_97.3.cl。

NetScaler VPX を NetScaler アプライアンスを使用した高可用性セットアップの一部にすることはできますか?

サポートされていない構成です。

NetScaler VPX に表示されるすべてのインターフェイスは、**Hypervisor** 上のインターフェイスの数に直接関係 していますか

いいえ。ハイパーバイザー上の物理 NIC が 1 つだけの場合、NetScaler VPX 構成ユーティリティを使用して最大 7 つのインターフェイス (VMware の場合は 10) を追加できます。

Citrix Hypervisor XenMotion、VMware VMotion、または **Hyper-V** ライブマイグレーションを使用して **NetScaler VPX** のアクティブなインスタンスを移動できますか**?**

NetScaler VPX は Hyper-V ライブマイグレーションをサポートしていません。vMotion は NetScaler リリース 13.0 以降でサポートされています。ライブマイグレーション(以前の XenMotion)は、NetScaler リリース 14.1 ビルド 17.38 以降でサポートされています。

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.