NetScaler VPX 14.1

Machine translated content

Disclaimer

Contents

NetScaler VPX 支持列表

October 17, 2024

本文档列出了 NetScaler VPX 实例支持的不同虚拟机管理程序和功能。该文档还介绍了他们的使用指南和已知限制。

VMware ESX 虚拟机管理程序上的 VPX 实例

| ESXi 版本 | ESXi 发布日期（YYYY/MM/DD）| ESXi 内部版本号 | NetScaler VPX 版本 | 性能范围 |
|——
—————————	——-	————-	——————
	公共云 →|AWS 上的 VPX|Azure 上的 VPX|GCP 上的 VPX| |^^ 功能 ↓ |^^|^^|^^| |—|—|—|—| |* 多 PE 支持 *| 是	是	是	|** 群集化支持 **| 否	否	否	|**VLAN 标记 **| 否	否	否	|** 检测链接事件/HAMon**| 否[2]| 否[2]| 否[2]| |** 接口参数配置 **| 否	否	否	|** 静态 LA**| 否	否	否	|**LACP**| 否	否	否	|** 静态 CLAG**| 否	否	否	|**LACP CLAG**| 否	否	否	|** 热插拔 **| 是	否	否		2024/06/25	24022510	14.1-17.x 及更高版本	10 Mbps 至 100 Gbps
ESXi 8.0 更新 2b	2024/03/05	23825572	14.1-17.x 及更高版本	^^
ESXi 8.0 更新 2	2024/02/29	23305546	14.1-4.x 及更高版本	^^
ESXi 8.0 更新 2	2023/09/21	22380479	14.1-4.x 及更高版本	^^
ESXi 8.0 更新 1	2023/04/18	21495797	14.1-4.x 及更高版本	^^
ESXi 8.0c	2023/03/30	21493926	14.1-4.x 及更高版本	^^
ESXi 8.0	2022/10/11	20513097	14.1-4.x 及更高版本	^^
ESXi 7.0 更新 3o	2024/03/05	23794027	14.1-17.x 及更高版本	^^
ESXi 7.0 更新 3n	不适用	23307199	14.1-4.x 及更高版本	^^
ESXi 7.0 更新 3m	2023/09/28	22348816	14.1-4.x 及更高版本	^^
ESXi 7.0 更新 3n	2023/07/06	21930508	14.1-8.x 及更高版本	^^
ESXi 7.0 更新 3m	2023/05/03	21686933	14.1-4.x 及更高版本	^^

> 注意：
>
> 每个 ESXi 补丁支持均在上表中指定的 NetScaler VPX 版本上经过验证，适用于所有更高版本的 NetScaler VPX 14.1 版本。

有关使用指南的更多信息，请参阅 VMware ESXi 虚拟机管理程序的使用指南。

XenServer 或 Citrix Hypervisor 上的 VPX 实例

XenServer 或 Citrix Hypervisor 版本	SysID	性能范围
8.4，从 NetScaler VPX 版本 14.1 Build 17.x 起支持 8.2，从 NetScaler VPX 版本 13.0 Build 64.x 起支持 8.0, 7.6, 7.1	450000	10 Mbps 至 40 Gbps

Microsoft Hyper-V 上的 **VPX** 实例

Hyper-V 版本	SysID	性能范围
2016, 2019	450020	10 Mbps 至 3 Gbps

Nutanix AHV 上的 **VPX** 实例

Nutanix AHV 通过 Citrix Ready 合作伙伴关系支持 NetScaler VPX。Citrix Ready 是一项技术合作计划，旨在帮助软件和硬件供应商开发产品并将其与 NetScaler 技术相集成，用于数字工作区、网络连接和分析。

有关在 Nutanix AHV 上部署 NetScaler VPX 实例的分步方法的更多信息，请参阅在 Nutanix AHV 上部署 NetScaler VPX。

第三方支持：

如果您在 NetScaler 环境中集成特定的第三方 (Nutanix AHV) 时遇到任何问题，请直接向第三方合作伙伴 (Nutanix) 提交支持事件。

如果合作伙伴确定问题似乎出在 NetScaler 上，则可以向 NetScaler 支持部门寻求进一步的帮助。合作伙伴提供的专门技术资源将与 NetScaler 支持团队合作，直到问题得到解决。

通用 **KVM** 上的 **VPX** 实例

通用 KVM 版本	SysID	性能范围
RHEL 7.6、RHEL 8.0、RHEL 9.3 Ubuntu 16.04、Ubuntu 18.04、Ubuntu 22.04	450070	10 Mbps 至 100 Gbps

注意事项：

使用 KVM 虚拟机管理程序时请考虑以下几点。

- VPX 实例适用于表 1—4 中提到的虚拟机管理程序发行版本，而不适用于版本中的修补程序发行版本。但是，VPX 实例应与受支持的版本的修补程序版本无缝协作。如果没有，请记录支持案例以进行故障排除和调试。
- 在使用 RHEL 7.6 之前，请在 KVM 主机上完成以下步骤：
  1. 编辑 /etc/default/grub 并将 `"kvm_intel.preemption_timer=0"` 附加到 `GRUB_CMDLINE_LINUX` 变量。
  2. 使用命令 `"# grub2-mkconfig -o /boot/grub2/grub.cfg"` 重新生成 grub.cfg。
  3. 重新启动主机。
- 在使用 Ubuntu 18.04 之前，请在 KVM 主机上完成以下步骤：
  1. 编辑 /etc/default/grub 并将 `"kvm_intel.preemption_timer=0"` 附加到 `GRUB_CMDLINE_LINUX` 变量。
  2. 使用命令 `"# grub-mkconfig -o /boot/grub/grub.cfg` “重新生成 grub.cfg。
  3. 重新启动主机。

公共云上的 **VPX** 实例

公共云	SysID	性能范围
AWS	450040	10 Mbps 至 30 Gbps
Azure	450020	10 Mbps 至 10 Gbps
GCP	450070	10 Mbps 至 10 Gbps

虚拟机管理程序支持的 **VPX** 功能

虚拟机管理程序 →	XenServer 上的 VPX		VMware ESX 上的 VPX							
^^ 特点 ↓	^^		^^				^^	^^		
接口 →	光伏	**SRIOV**	光伏	**SRIOV**	模拟	**PCI** 直通	光伏	光伏	**SRIOV**	**PCI** 直通

^^ 特点 ↓	^^		^^				^^	^^		
多 **PE** 支持	是	是	是	是	是	是	是	是	是	是
集群支持	是	是[1]	是	是[1]	是	是	是	是	是[1]	是
VLAN 标记	是	是	是	是	是	是	是(仅限 2012R2)	是	是	是
检测链接事件**/HAMon**	否[2]	是[3]	否[2]	是[3]	否[2]	是[3]	否[2]	否[2]	是[3]	是[3]
接口参数配置	否	否	否	否	否	是	否	否	否	是
静态 **LA**	是[2]	是[3]	是[2]	否	是[2]	是[3]	是[2]	是[2]	是[3]	是[3]
LACP	否	是[3]	是[2]	否	是[2]	是[3]	否	是[2]	是[3]	是[3]
静态 **CLAG**	否	否	否	否	否	否	否	否	否	否
LACP CLAG	否	否	是[2]	否	是[2]	是[3]	否	是[2]	是[3]	是[3]
热插拔	否	否	否	否	否	否	否	否	否	否

公有云支持的 **VPX** 功能

公有云 →	AWS 上的 VPX	Azure 上的 VPX	GCP 上的 VPX

^^ 特点 ↓	^^	^^	^^
多 **PE** 支持	是	是	是
集群支持	否	否	否
VLAN 标记	否	否	否
检测链接事件**/HAMon**	否[2]	否[2]	否[2]

^^ 特点 ↓	^^	^^	^^
接口参数配置	否	否	否
静态 **LA**	否	否	否
LACP	否	否	否
静态 **CLAG**	否	否	否
LACP CLAG	否	否	否
热插拔	是	否	否

前面两个表中使用的上标数字（1、2、3）指的是以下各点，其编号分别为：

1. SRIOV 对面向客户端和面向服务器的接口提供群集支持，但不支持背板。
2. NetScaler VPX 实例中不记录接口关闭事件。
3. 对于静态 LA，仍可能会在其物理状态为 DOWN（关闭）的接口上发送流量。

以下几点适用于前面两个表中捕获的相应特征：

- 对于 LACP，对等设备根据 LACP 超时机制获知接口 DOWN（关闭）事件。
  - 短超时：3 秒
  - 长超时：90 秒
- 对于 LACP，请勿在 VM 之间共享接口。
- 对于动态路由，收敛时间取决于路由协议，因为无法检测到链接事件。
- 如果不将监视器绑定到静态路由，则受监视的静态路由功能将失败，因为路由状态取决于 VLAN 状态。VLAN 状态取决于链接状态。
- 如果链路出现故障，则在高可用性条件下不会进行部分故障检测。如果链路出现故障，可能会发生高可用性-大脑分裂情况。
  - 当从 VPX 实例生成任何链接事件（禁用/启用、重置）时，链接的物理状态不会改变。对于静态 LA，对等方启动的任何流量都会在实例上丢弃。
  - 为了使 VLAN 标记功能正常工作，在 VMware ESX 上，将 VMware ESX 服务器的 vSwitch 上的端口组的 VLAN ID 设置为 1–4095。
- 带有 ENA 接口的 VPX 实例不支持热插拔，如果尝试热插拔，则实例的行为可能无法预测。仅在 AWS 上使用 NetScaler 的 PV 和 SRIOV 接口支持热添加。
- NetScaler 的 PV、SRIOV 和 ENA 接口不支持通过 AWS Web 控制台或 AWS CLI 界面进行热删除。如果尝试热删除，实例的行为可能不可预测。

支持的浏览器

操作系统	浏览器和版本
Windows 7	Internet Explorer- 8、9、10 和 11；Mozilla Firefox 3.6.25 及更高版本；Google Chrome - 15 及更高版本
Windows 64 位	Internet Explorer - 8、9；Google Chrome - 15 及更高版本
MAC	Mozilla Firefox - 12 及更高版本；Safari - 5.1.3；Google Chrome - 15 及更高版本

针对 **VPX** 实例的 **AMD** 处理器支持

从 NetScaler 版本 13.1 开始，VPX 实例同时支持 Intel 和 AMD 处理器。VPX 虚拟设备可以部署在具有两个或更多虚拟化内核和超过 2 GB 内存的任何实例类型上。有关系统要求的更多信息，请参阅 NetScaler VPX 数据手册。

VPX 平台与 网卡矩阵表

下表列出了 VPX 平台或云上支持的 NIC。

NIC →	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/XL710 SRIOV VF	Intel X710/XL710/XXV710 PCI 直通模式
^^ 平台 ↓	^^	^^	^^	^^	^^	^^
VPX (ESXi)	否	是	否	是	否	是
VPX (Citrix Hypervisor)	不适用	不适用	不适用	是	是	否
VPX (KVM)	否	是	是	是	是	否
VPX (Hyper-V)	不适用	不适用	不适用	否	否	否
VPX (AWS)	不适用	不适用	不适用	是	不适用	不适用
VPX (Azure)	是	是	是	不适用	不适用	不适用

^^ 平台 ↓	^^	^^	^^	^^	^^	^^
VPX (GCP)	不适用	不适用	不适用	不适用	不适用	不适用

其他参考

- 有关 Citrix Ready 产品，请访问 Citrix Ready Marketplace。
- 有关 Citrix Ready 产品支持，请参阅常见问题页面。
- 有关 VMware ESX 硬件版本的信息，请参阅 升级 VMware Tools。

在 **VMware ESX**、**Linux KVM** 和 **Citrix Hypervisor** 上优化 **NetScaler VPX** 性能

October 17, 2024

NetScaler VPX 的性能因虚拟机管理程序、分配的系统资源和主机配置而异。要获得所需的性能，请首先遵循 VPX 数据手册中的建议，然后使用本文档中提供的最佳实践进一步优化它。

VMware ESX 虚拟机管理程序上的 **NetScaler VPX** 实例

本部分包含可配置选项和设置的详细信息，以及其他有助于您在 VMware ESX 虚拟机管理程序上实现 NetScaler VPX 实例的最佳性能的建议。

- Recommended configuration on ESX hosts
- 带有 E1000 网络接口的 NetScaler VPX
- 带有 VMXNET3 网络接口的 NetScaler VPX
- 具有 SR-IOV 和 PCI 直通网络接口的 NetScaler 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.

  –To find the NUMA affinity of a Vmnic, log in to the host locally or remotely, and type:


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

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

带有 **E1000** 网络接口的 **NetScaler VPX**

Perform the following settings on the VMware ESX host:

- On the VMware ESX host, create two vNICs from one pNIC vSwitch. Multiple vNICs create multiple Rx threads in the ESX host. This increases the Rx throughput of the pNIC interface. 多个 vNIC 在 ESX 主机中创建多个接收 (Rx) 线程。这会增加 pNIC 接口的 Rx 吞吐量。
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- 要提高 vNIC 传输 (Tx) 吞吐量，请在每个 vNIC 的 ESX 主机中使用单独的 Tx 线程。使用以下 ESX 命令：
  - For ESX version 5.5:

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

  - For ESX version 6.0 onwards:

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

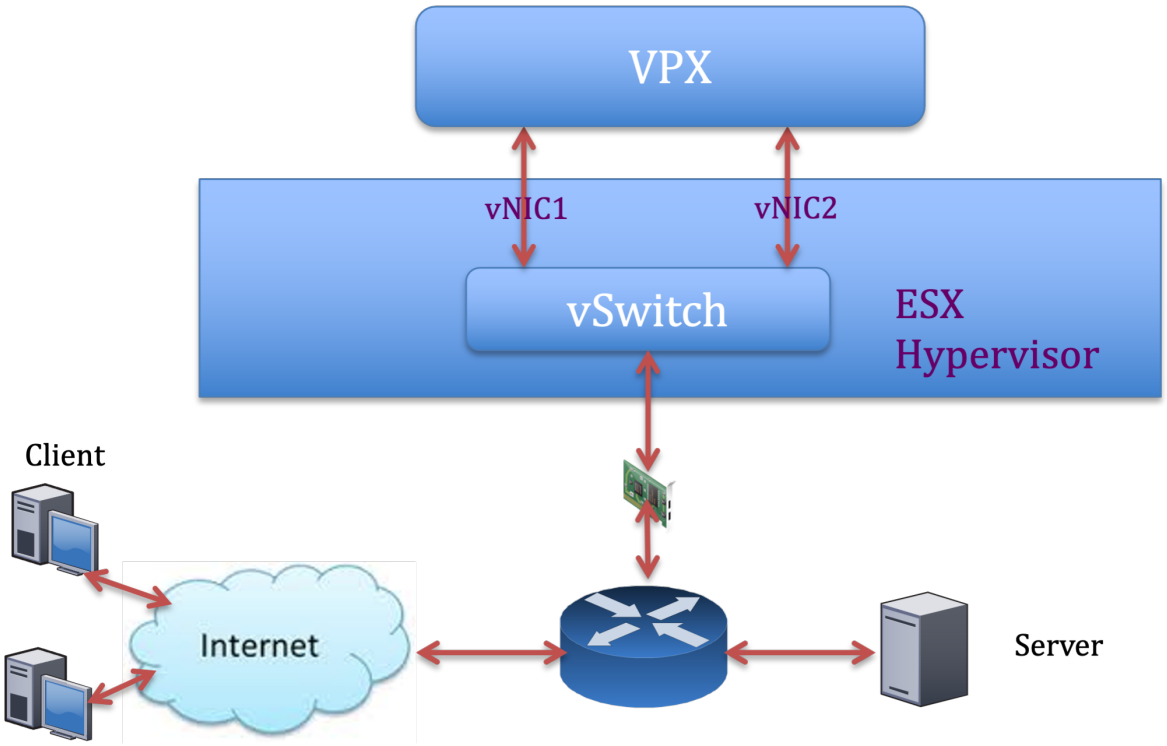
- To further increase the vNIC Tx throughput, use a separate Tx completion thread and Rx threads per device (NIC) queue. Use the following ESX command: 使用以下 ESX 命令：

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

> 注意：
>
> 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 示例配置：

要实现上述示例拓扑中显示的部署，请在 NetScaler VPX 实例上执行以下配置：

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

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

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

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

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

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


> 注意：
>
> 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

带有 **VMXNET3** 网络接口的 **NetScaler VPX**

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

- 从一台 pNIC vSwitch 创建两个虚拟网卡。多个虚拟网卡在 ESX 主机中创建多个 Rx 线程。这会增加 pNIC 接口的 Rx 吞吐量。
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- 要提高 vNIC 传输 (Tx) 吞吐量，请在每个 vNIC 的 ESX 主机中使用单独的 Tx 线程。使用以下 ESX 命令：
  - For ESX version 5.5:

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

  - For ESX version 6.0 onwards:

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

On the VMware ESX host, perform the following configuration:

- 在 VMware ESX 主机上，从一台 pNIC 虚拟交换机创建两个虚拟网卡。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. 这会增加 pNIC 接口的 Tx 和 Rx 吞吐量。
- 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. Use the following command: 使用以下命令：

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

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

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

- 通过在虚拟机的配置中添加以下设置，将虚拟机配置为每个 vNIC 最多使用 8 个传输线程：


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

> 注意：
>
> 增加每个 vNIC 的传输线程需要在 ESX 主机上使用更多 CPU 资源（最多 8 个）。在进行上述设置之前，请确保有足够的 CPU 资源可用。

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

You can configure VMXNET3 as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment. 有关详细信息，请参阅 每个 pNIC 部署两个 vNIC。

在 **VMware ESX** 上为 **VMXNET3** 设备配置多队列和 **RSS** 支持　默认情况下，VMXNET3 设备仅支持 8 个 Rx 和 Tx 队列。当 VPX 上的 vCPU 数量超过 8 时，默认情况下，为 VMXNET3 接口配置的 Rx 和 Tx 队列数量会切换为 1。通过更改 ESX 上的某些配置，您可以为 VMXNET3 设备配置多达 19 个 Rx 和 Tx 队列。此选项可提高数据包在 VPX 实例的 vCPU 间的性能和均匀分布。

> 注意：
>
> 从 NetScaler 版本 13.1 build 48.x 开始，NetScaler VPX 在 ESX 上支持多达 19 个 VMXNET3 设备的 Rx 和 Tx 队列。

必备条件：

要在 ESX 上为 VMXNET3 设备配置多达 19 个 Rx 和 Tx 队列，请确保满足以下先决条件：

- NetScaler VPX 版本是 13.1 版本 48.X 及更高版本。
- NetScaler VPX 配置了硬件版本 17 及更高版本的虚拟机，VMware ESX 7.0 及更高版本支持该虚拟机。

将 **VMXNET3** 接口配置为支持 **8** 个以上的 **Rx** 和 **Tx** 队列：

1. 打开虚拟机配置文件 (.vmx) 文件。
2. 通过配置和 `ethernetX.maxRxQueues` 值来指定 Rx 和 TX 队列的 `ethernetX.maxTxQueues` 数量（其中 X 是要配置的虚拟 NIC 的数量）。配置的最大队列数不得大于虚拟机中的 vCPU 数量。

   > 注意：
   >
   > 增加队列数量还会增加 ESX 主机的处理器开销。因此，在增加队列之前，请确保 ESX 主机中有足够的 CPU 资源可用。在队列数量被确定为性能瓶颈的情况下，您可以增加支持的最大队列数。在这些情况下，我们建议逐渐增加队列数量。例如，从 8 到 12，然后是 16，然后是 20，依此类推。评估每种设置下的性能，而不是直接提高到最大限制。

具有 **SR-IOV** 和 **PCI** 直通网络接口的 **NetScaler VPX**

要使用 SR-IOV 和 PCI 直通网络接口实现 NetScaler VPX 的高性能，请参阅 ESX 主机上的推荐配置。

VMware ESXi 虚拟机管理程序的使用指南

- 我们建议您在服务器的本地磁盘或基于 SAN 的存储卷上部署 NetScaler VPX 实例。

  请参阅 VMware vSphere 6.5 性能最佳实践文档中的 **VMware ESXi CPU** 注意事项部分。下面是一段摘录：

- 不建议在过度使用的主机或群集上部署 CPU 或内存需求高的虚拟机。
- 在大多数环境中，ESXi 允许大量 CPU 过载，而不会影响虚拟机性能。在主机上，您可以运行的 vCPU 数量超过该主机中的物理处理器核心总数。
- 如果 ESXi 主机变得 CPU 饱和，即主机上的虚拟机和其他负载需要主机拥有的所有 CPU 资源，则延迟敏感型工作负载可能无法良好运行。在这种情况下，例如，通过关闭某些虚拟机或将其迁移到其他主机（或允许 DRS 自动迁移它们）来降低 CPU 负载。
- NetScaler 建议使用最新的硬件兼容版本来为虚拟机使用 ESXi 虚拟机管理程序的最新功能集。有关硬件和 ESXi 版本兼容性的更多信息，请参阅 VMware 文档。
- NetScaler VPX 是一款延迟敏感的高性能虚拟设备。为了提供预期的性能，该设备需要在主机上预留 vCPU、内存预留和 vCPU 固定。此外，必须在主机上禁用超线程。如果主机不满足这些要求，则可能会出现以下问题：

  - 高可用性故障转移
  - VPX 实例内的 CPU 峰值
  - 访问 VPX CLI 时运行缓慢
  - Pit boss 守护程序崩溃
  - 数据包丢失
  - 低吞吐量

- 如果满足以下两个条件之一，虚拟机管理程序将被视为过度预配：

  - 在主机上配置的虚拟核心 (vCPU) 总数大于物理核心 (pCPU) 总数。
  - 预配的 VM 总数占用的 vCPU 数量超过 pCPU 总数。

    如果实例配置过度，虚拟机管理程序可能无法保证为实例预留的资源（例如 CPU、内存和其他资源），原因是管理程序计划开销、错误或管理程序的限制。这种行为可能导致 NetScaler 缺乏 CPU 资源，并可能导致使用指南下第一点中提到的问题。我们建议管理员减少主机的租期，使主机上配置的 vCPU 总数小于或等于 PCPU 的总数。

    Example:

    对于 ESX 虚拟机管理程序，如果 `esxtop` 命令输出中 VPX vCPU 的 %RDY% 参数大于 0，则说 ESX 主机存在调度开销，这可能会导致 VPX 实例出现延迟相关问题。

在这种情况下，请减少主机上的租赁，以便 %RDY% 始终返回 0。或者，联系虚拟机管理程序供应商，对不履行资源预留的原因进行分类。

控制数据包引擎 **CPU** 使用率的命令

您可以使用两个命令（`set ns vpxparam` 和 `show ns vpxparam`）来控制虚拟机管理程序和云环境中 VPX 实例的数据包引擎（非管理）CPU 使用行为：

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

  允许每个 VM 使用分配给另一个 VM 但未被使用的 CPU 资源。

  `Set ns vpxparam` 参数：

  -cpuyield：释放或不释放已分配但未使用的 CPU 资源。

  - **YES**：允许另一个 VM 使用已分配但未使用的 CPU 资源。
  - 否：为分配的虚拟机保留所有 CPU 资源。此选项显示，在虚拟机管理程序和云环境中，VPX CPU 使用率的百分比更高。
  - **DEFAULT**：No。

  > 注意：
  >
  > 在所有 NetScaler VPX 平台上，主机系统上的 vCPU 使用率为 100%。使用 `set ns vpxparam -cpuyield YES` 命令覆盖此用法。

  如果要将群集节点设置为“yield”，则必须在 CCO 上执行以下额外配置：

  - 如果形成群集，则所有节点都设置为“yield=DEFAULT”。
  - 如果使用已设置为“yield=YES”的节点组成群集，则使用“DEFAULT”收益率将节点添加到群集中。

  > 注意：
  >
  > 如果要将群集节点设置为“yield=YES”，则只能在形成群集之后进行配置，而不能在群集形成之前进行配置。

  -masterclockcpu1：可以将主时钟源从 CPU0（管理 CPU）移动到 CPU1。此参数具有以下选项：

  - 是：允许虚拟机将主时钟源从 CPU0 移动到 CPU1。
  - **NO**：VM 使用 CPU0 作为主时钟源。默认情况下，CPU0 是主时钟源。

- `show ns vpxparam`

  此命令显示当前 `vpxparam` 设置。

Linux-KVM 平台上的 NetScaler VPX 实例

本部分包含可配置选项和设置的详细信息，以及其他有助于您在 Linux-KVM 平台上实现 NetScaler VPX 实例的最佳性能的建议。

- KVM 的性能设置
- 具有光伏网络接口的 NetScaler VPX
- 配备 SR-IOV 和福特维尔 PCIe 直通网络接口的 NetScaler VPX

KVM 的性能设置

Perform the following settings on the KVM host:

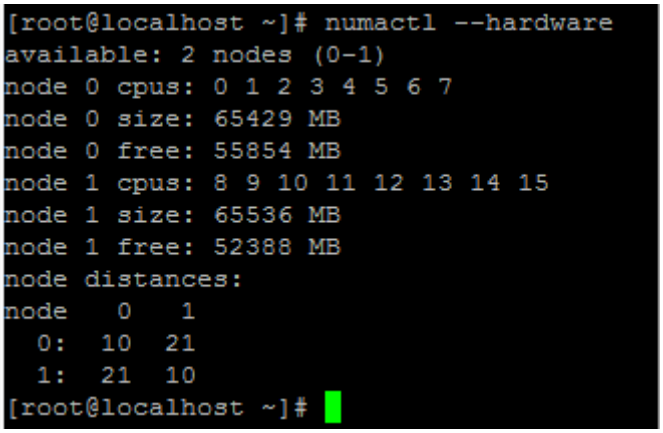
Find the NUMA domain of the NIC using the `lstopo` command:

Make sure that memory for the VPX and the CPU is pinned to the same location. In the following output, the 10G NIC “ens2” is tied to NUMA domain #1. 在以下输出中，10G 网卡“ens2”与 NUMA 域 #1 关联。

```
[root@localhost ~]# lstopo-no-graphics
Machine (128GB)
  NUMANode L#0 (P#0 64GB)
    Socket L#0 + L3 L#0 (20MB)
      L2 L#0 (256KB) + L1d L#0 (32KB) + L1i L#0 (32KB) + Core L#0 + PU L#0 (P#0)
      L2 L#1 (256KB) + L1d L#1 (32KB) + L1i L#1 (32KB) + Core L#1 + PU L#1 (P#1)
      L2 L#2 (256KB) + L1d L#2 (32KB) + L1i L#2 (32KB) + Core L#2 + PU L#2 (P#2)
      L2 L#3 (256KB) + L1d L#3 (32KB) + L1i L#3 (32KB) + Core L#3 + PU L#3 (P#3)
      L2 L#4 (256KB) + L1d L#4 (32KB) + L1i L#4 (32KB) + Core L#4 + PU L#4 (P#4)
      L2 L#5 (256KB) + L1d L#5 (32KB) + L1i L#5 (32KB) + Core L#5 + PU L#5 (P#5)
      L2 L#6 (256KB) + L1d L#6 (32KB) + L1i L#6 (32KB) + Core L#6 + PU L#6 (P#6)
      L2 L#7 (256KB) + L1d L#7 (32KB) + L1i L#7 (32KB) + Core L#7 + PU L#7 (P#7)
    HostBridge L#0
      PCIBridge
        PCI 8086:1521
          Net L#0 "eno1"
        PCI 8086:1521
          Net L#1 "eno2"
      PCIBridge
        PCI 8086:1584
          Net L#2 "ens3"
      PCIBridge
        PCI 8086:1584
          Net L#3 "ens4"
      PCI 8086:8d62
        Block L#4 "sda"
        Block L#5 "sdb"
      PCIBridge
        PCIBridge
          PCI 1a03:2000
            GPU L#6 "card0"
            GPU L#7 "controlD64"
      PCI 8086:8d02
  NUMANode L#1 (P#1 64GB)
    Socket L#1 + L3 L#1 (20MB)
      L2 L#8 (256KB) + L1d L#8 (32KB) + L1i L#8 (32KB) + Core L#8 + PU L#8 (P#8)
      L2 L#9 (256KB) + L1d L#9 (32KB) + L1i L#9 (32KB) + Core L#9 + PU L#9 (P#9)
      L2 L#10 (256KB) + L1d L#10 (32KB) + L1i L#10 (32KB) + Core L#10 + PU L#10 (P#10)
      L2 L#11 (256KB) + L1d L#11 (32KB) + L1i L#11 (32KB) + Core L#11 + PU L#11 (P#11)
      L2 L#12 (256KB) + L1d L#12 (32KB) + L1i L#12 (32KB) + Core L#12 + PU L#12 (P#12)
      L2 L#13 (256KB) + L1d L#13 (32KB) + L1i L#13 (32KB) + Core L#13 + PU L#13 (P#13)
      L2 L#14 (256KB) + L1d L#14 (32KB) + L1i L#14 (32KB) + Core L#14 + PU L#14 (P#14)
      L2 L#15 (256KB) + L1d L#15 (32KB) + L1i L#15 (32KB) + Core L#15 + PU L#15 (P#15)
    HostBridge L#6
      PCIBridge
        PCI 8086:1584
          Net L#8 "ens2"
      PCIBridge
        PCI 8086:10fb
          Net L#9 "ens1f0"
        PCI 8086:10fb
          Net L#10 "ens1f1"
        PCI ffff:ffff
          Net L#11 "enp131s16"
[root@localhost ~]#  modprobe kvm-intel acpienv=N
```

Allocate the VPX memory from the NUMA domain.

该 numactl 命令指示从中分配内存的 NUMA 域。The numactl command indicates the NUMA domain from which the memory is allocated. In the following output, around 10 GB RAM is allocated from NUMA node #0.



To change the NUMA node mapping, follow these steps.

1. 在主机上编辑 VPX 的.xml。

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

2. 添加以下标签：

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

3. 关闭 VPX。
4. 运行以下命令：

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

此命令使用 NUMA 节点映射更新 VM 的配置信息。

5. 打开 VPX 的电源。然后检查主机上的 numactl -hardware 命令输出以查看 VPX 的更新内存分配。


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

Pin vCPUs of VPX to physical cores.

- 要查看 VPX 的 vCPU 到 pCPU 的映射，请键入以下命令

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

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

vCPU 0—4 映射到物理内核 8—11。

- 要查看当前的 pCPU 使用情况，请键入以下命令：

```
mpstat -P ALL 5
```

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

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

在此输出中，8 是管理 CPU，9—11 是数据包引擎。

- 要将 vCPU 更改为 PCU 固定，有两个选项。
  - 使用以下命令在 VPX 启动后在运行时更改它：

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

  - 要对 VPX 进行静态更改，请使用以下标签像以前一样编辑 `.xml` 文件：

    1. 在主机上编辑 VPX 的.xml 文件

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

    2. 添加以下标签：

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

    3. 关闭 VPX。
    4. 使用以下命令使用 NUMA 节点映射更新 VM 的配置信息：

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

    5. 打开 VPX 的电源。然后检查主机上的 `virsh vcpupin <VPX name>` 命令输出以查看更新的 CPU 固定。

Eliminate host interrupt overhead.

- 使用 `kvm_stat` 命令检测 VM_EXITS。

  在虚拟机管理程序级别，主机中断映射到固定 VPX vCPU 的相同 PCU。这可能会导致 VPX 上的 vCPU 定期被踢出。

  要查找运行主机的虚拟机完成的 VM 退出，请使用 `kvm_stat` 命令。

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

  大小为 1+M 的较高值表示存在问题。

  如果存在单个虚拟机，则预期值为 30–100 K。除此之外的任何值都可能表明有一个或多个主机中断向量映射到同一个 pCPU。

- 检测主机中断并迁移主机中断。

  当您运行“/proc/interrupts”文件的 concatenate 命令时，它会显示所有主机中断映射。如果一个或多个活动 IRQ 映射到同一个 PCU，则其对应的计数器会增加。

  将与 NetScaler VPX 的 PCU 重叠的所有中断移动到未使用的 PCU 中：

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

- 禁用 IRQ 余额。

  禁用 IRQ 余额守护进程，这样即时不会进行重新安排。

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

  确保运行 kvm_stat 命令以确保计数器不多。

具有光伏网络接口的 **NetScaler VPX**

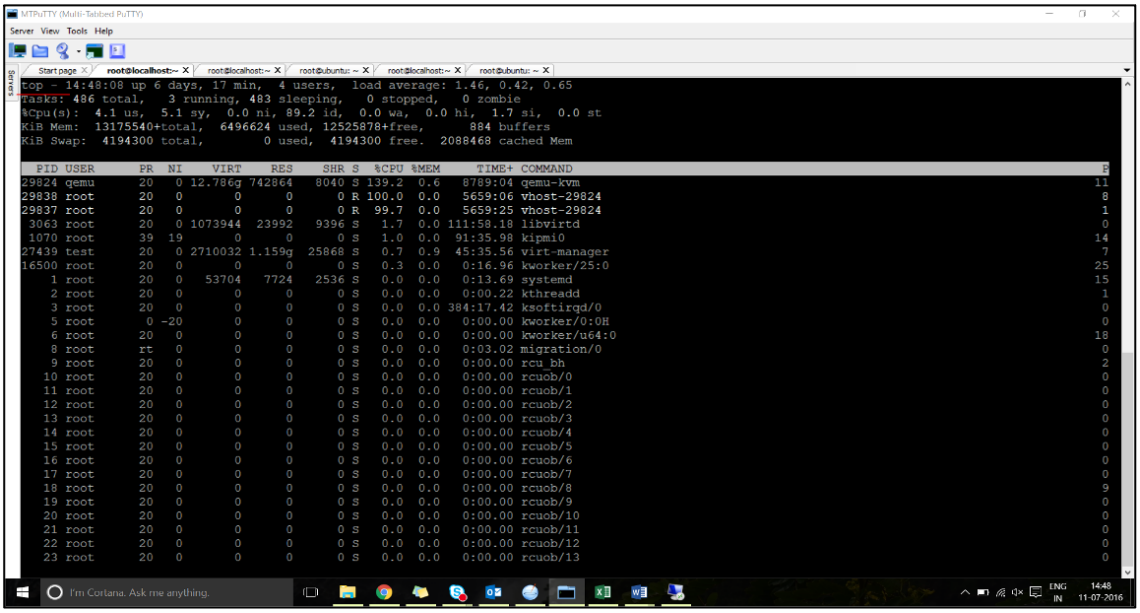
You can configure para-virtualization (PV), SR-IOV, and PCIe passthrough network interfaces as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment. 有关详细信息，请参阅 每个 pNIC 部署两个 vNIC。

For optimal performance of PV (virtio) interfaces, follow these steps:

- 确定 PCIe 插槽/网卡所属的 NUMA 域。
- VPX 的内存和 vCPU 必须固定到同一个 NUMA 域。
- 虚拟主机线程必须绑定到同一 NUMA 域中的 CPU。

Bind the virtual host threads to the corresponding CPUs:

1. 流量启动后，在主机上运行 top 命令。



2. 确定虚拟主机进程（命名为 vhost-<pid-of-qemu>）关联性。
3. 使用以下命令将 vHost 进程绑定到之前确定的 NUMA 域中的物理核心：

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

Example:

```
taskset -pc 12 29838
```

4. 可以使用以下命令识别与 NUMA 域对应的处理器内核：

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

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



```
            <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
            </cpus>

        <cpuselection/>
        <cpuselection/>
```

Bind the QEMU process to the corresponding physical core:

1. 确定运行 QEMU 进程的物理核心。有关更多信息，请参阅前面的输出。
2. 使用以下命令将 QEMU 进程绑定到与 vCPU 绑定到的相同物理核心：

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

配备 SR-IOV 和福特维尔 PCIe 直通网络接口的 NetScaler VPX

For optimal performance of the SR-IOV and Fortville PCIe passthrough network interfaces, follow these steps:

- 确定 PCIe 插槽/网卡所属的 NUMA 域。
- NetScaler VPX 的内存和 vCPU 必须固定到同一个 NUMA 域。

Sample VPX XML file for vCPU and memory pinning for Linux KVM:

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

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

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

        </domain>
```

Citrix Hypervisor 上的 NetScaler VPX 实例

本部分包含可配置选项和设置的详细信息，以及可帮助您在 Citrix Hypervisor 上实现 NetScaler VPX 实例的最佳性能的其他建议。

- Citrix Hypervisor 的性能设置
- 具有 SR-IOV 网络接口的 NetScaler VPX
- 具有半虚拟化接口的 NetScaler VPX

Citrix Hypervisor 的性能设置

Find the NUMA domain of the NIC using the "xl" command:

```
xl info -n
```

Pin vCPUs of VPX to physical cores.

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

Check binding of vCPUs.

```
xl vcpu-list
```

向 **NetScaler** 虚拟机分配 **8** 个以上的 **vCPU**。

For configuring more than 8 vCPUs, run the following commands from the Citrix Hypervisor console:

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

具有 SR-IOV 网络接口的 NetScaler VPX

For optimal performance of the SR-IOV network interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot or NIC is tied to.
- 将 VPX 的内存和 vCPU 固定到同一个 NUMA 域。
- 将域 0 vCPU 绑定到剩余的 CPU。

具有半虚拟化接口的 NetScaler VPX

For optimal performance, two vNICs per pNIC and one vNIC per pNIC configurations are advised, as in other PV environments.

To achieve optimal performance of para-virtualized (netfront) interfaces, follow these steps:

- 确定 PCIe 插槽或 NIC 所属的 NUMA 域。
- 将 VPX 的内存和 vCPU 固定到同一个 NUMA 域。
- 将域 0 vCPU 绑定到同一 NUMA 域的剩余 CPU。
- 将 vNIC 的主机 Rx/Tx 线程固定到域 0 vCPU。

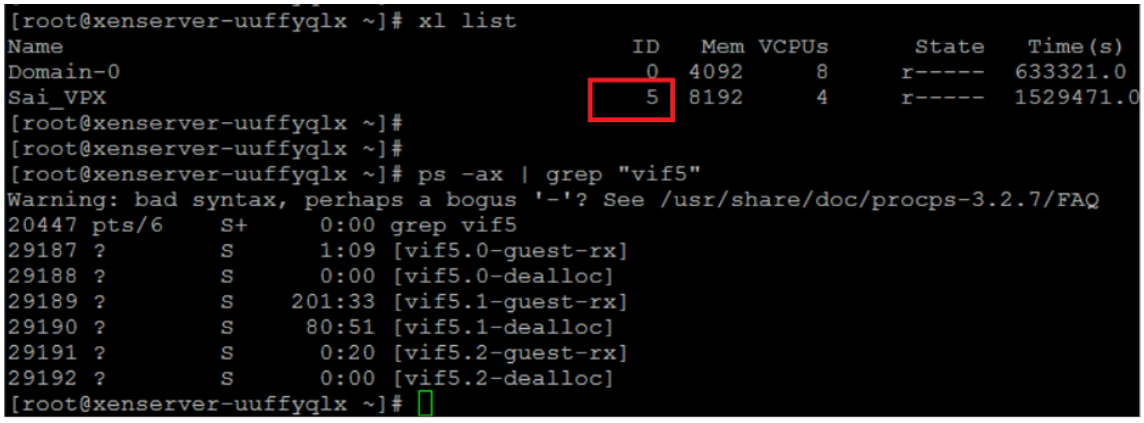
Pin host threads to Domain-0 vCPUs:

1. 使用 Citrix Hypervisor 主机 shell 上的 `xl list` 命令查找 NetScaler VPX 的 Xen-ID。
2. 使用以下命令识别主机线程：

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

在以下示例中，这些值表示：

- **vif5.0** -在 XenCenter 中分配给 VPX 的第一个接口的线程（管理接口）。
- **vif5.1** -分配给 VPX 的第二个接口的线程等等。



3. 使用以下命令将线程固定到 Domain-0 vCPU：

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

Example:

```
taskset -pc 1 29189
```

在云中首次启动 **NetScaler** 设备时应用 **NetScaler VPX** 配置

October 17, 2024

您可以在云环境中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。本文档将此阶段作为预引导阶段进行讨论。因此，在某些情况下，例如 ADC 池许可时，特定的 VPX 实例会在更短的时间内启动。此功能可在 Microsoft Azure、Google 云端平台和 AWS 云中使用。

用户数据是什么

在云环境中预配 VPX 实例时，可以选择将用户数据传递给实例。用户数据允许您执行常见的自动配置任务、自定义实例的启动行为以及在实例启动后运行脚本。首次启动时，NetScaler VPX 实例会执行以下任务：

- 读取用户数据。
- 解释用户数据中提供的配置。
- 在启动时应用新添加的配置。

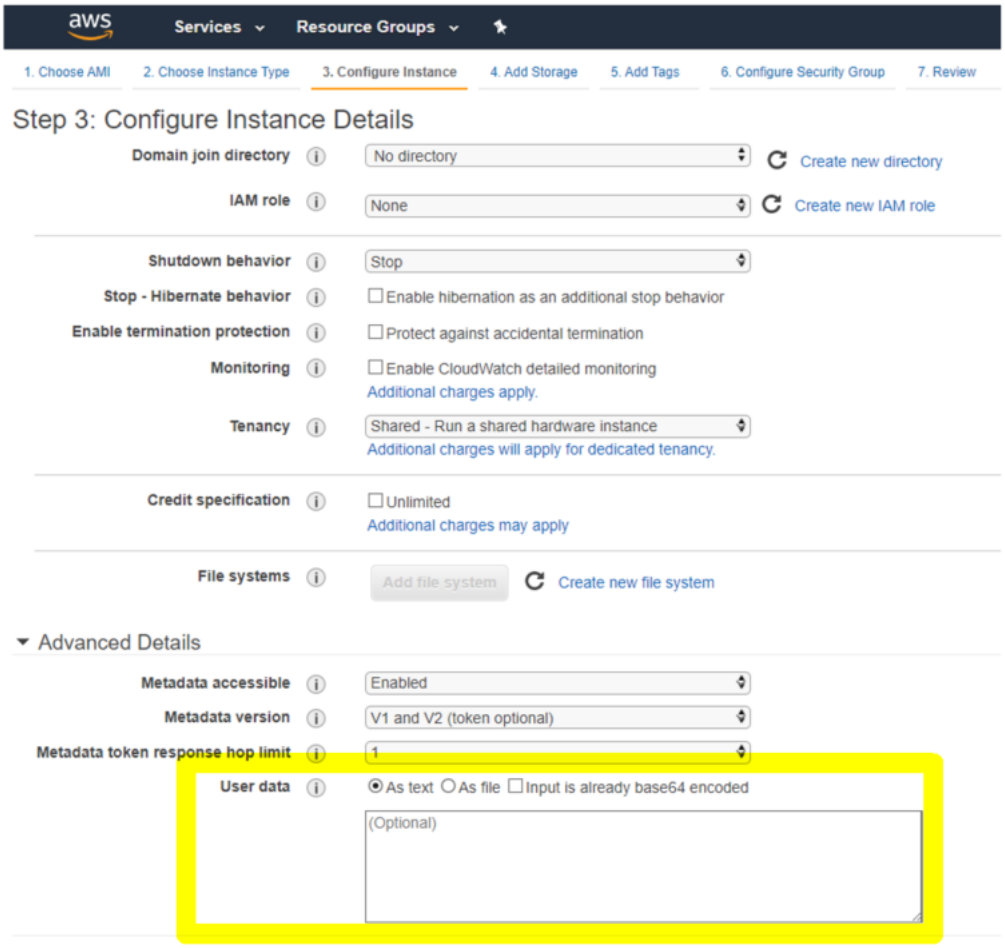
如何在云实例中提供预启动用户数据

可以使用 XML 格式向云实例提供预引导用户数据。不同的云有不同的接口来提供用户数据。

使用 **AWS** 控制台提供预引导用户数据

使用 AWS 控制台预配 NetScaler VPX 实例时，导航到 **Configure Instance Details**（配置实例详细信息）**> Advanced Details**（高级详细信息），然后在 **User data**（用户数据）字段中提供预引导用户数据配置。

有关每个步骤的详细说明，请参阅 使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例。有关更多信息，请参阅有关启动实例的 AWS 文档。



> 注意：
>
> NetScaler VPX 版本 13.1.48.x 及更高版本支持预启动用户数据功能的仅限 AWS IMDSv2 模式。

使用 **AWS CLI** 提供预启动用户数据

在 AWS CLI 中键入以下命令：

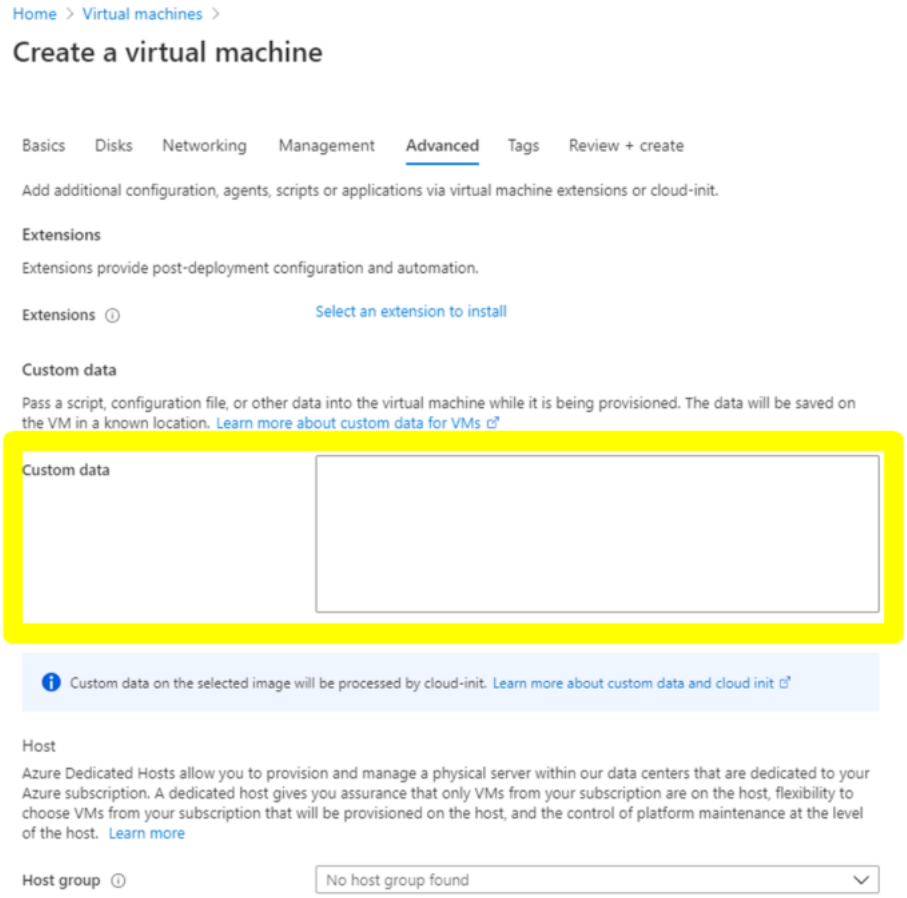
```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
```

有关更多信息，请参阅有关 运行实例的 AWS 文档。

有关更多信息，请参阅有关 使用实例用户数据的 AWS 文档

使用 **Azure** 控制台提供预引导用户数据

当您使用 Azure 控制台配置 NetScaler VPX 实例时，导航到 创建虚拟机 高级选项卡。在 **Custom data**（自定义数据）字段中，提供预引导用户数据配置。



使用 **Azure CLI** 提供预引导用户数据

在 Azure CLI 中键入以下命令：

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

Example:

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

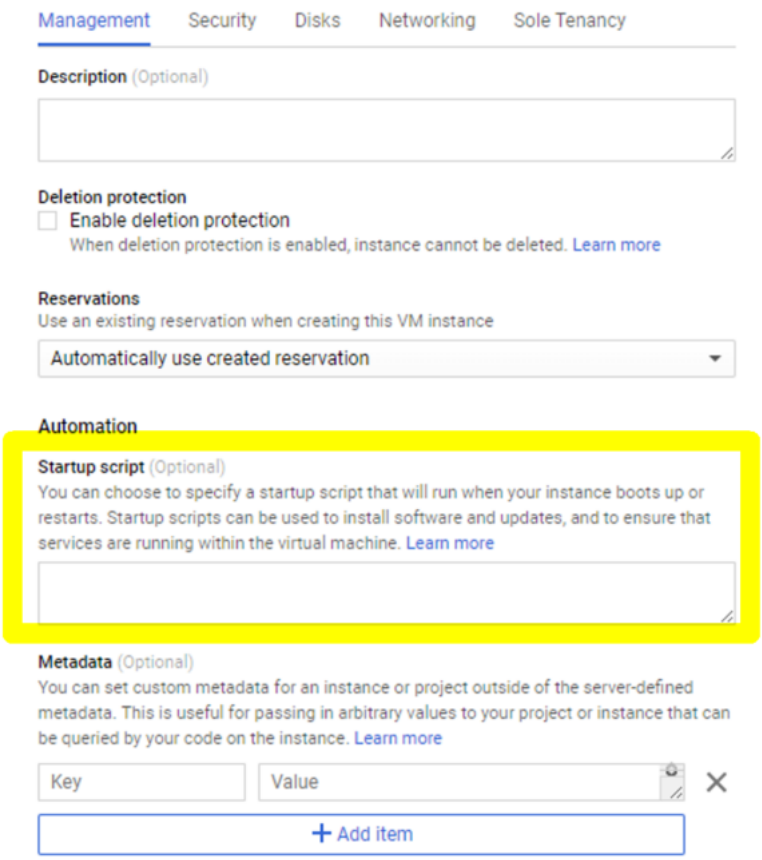
可以将自定义数据或预引导配置作为文件传递给“—custom-data”参数。在此示例中，文件名为 **MyCloudInitScript.txt**。

有关更多信息，请参阅 Azure CLI 文档。

使用 **GCP** 控制台提供预引导用户数据

当您使用 GCP 控制台配置 NetScaler VPX 实例时，请填写实例的属性。展开 **Management, security, disks, networking, sole tenancy**（管理、安全性、磁盘、网络连接和唯一租赁）。导航到 **Management**（管理）选项卡。在 **Automation**（自动化）部分中，在 **Startup Script**（启动脚本）字段中提供预引导用户数据配置。

有关使用 GCP 创建 VPX 实例的详细信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例。



使用 **gcloud CLI** 提供预启动用户数据

在 GCP CLI 中键入以下命令：

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

元数据源自文件- 从存储在 <LOCAL_FILE_PATH>。.

有关更多信息，请参阅 gcloud CLI 文档

预引导用户数据格式

必须以 XML 格式向云实例提供预引导用户数据。您在启动期间通过云基础架构提供的 NetScaler 预启动用户数据可以包括以下四个部分：

- NetScaler 配置用 <NS-CONFIG> 标签表示。
- 自定义引导用 <NS-BOOTSTRAP> 标签表示的 NetScaler。
- 将用户脚本存储在以 <NS-SCRIPTS> 标签表示的 NetScaler 中。
- 用 <NS-LICENSE-CONFIG> 标记表示的池许可配置。

可以在 ADC 预引导配置中按任意顺序提供前面的四个部分。在提供预引导用户数据时，请确保严格遵循以下部分中显示的格式。

> 注意：
>
> 整个预引导用户数据配置必须包含在 <NS-PRE-BOOT-CONFIG> 标记中，如以下示例所示。

示例 **1**：

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

示例 **2**：

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

使用 <NS-CONFIG> 标签提供需要在预启动阶段应用于 VPX 实例的特定 NetScaler VPX 配置。

> 注意：
>
> <NS-CONFIG> 部分必须具有有效的 ADC CLI 命令。没有验证 CLIS 是否存在语法错误或格式问题。

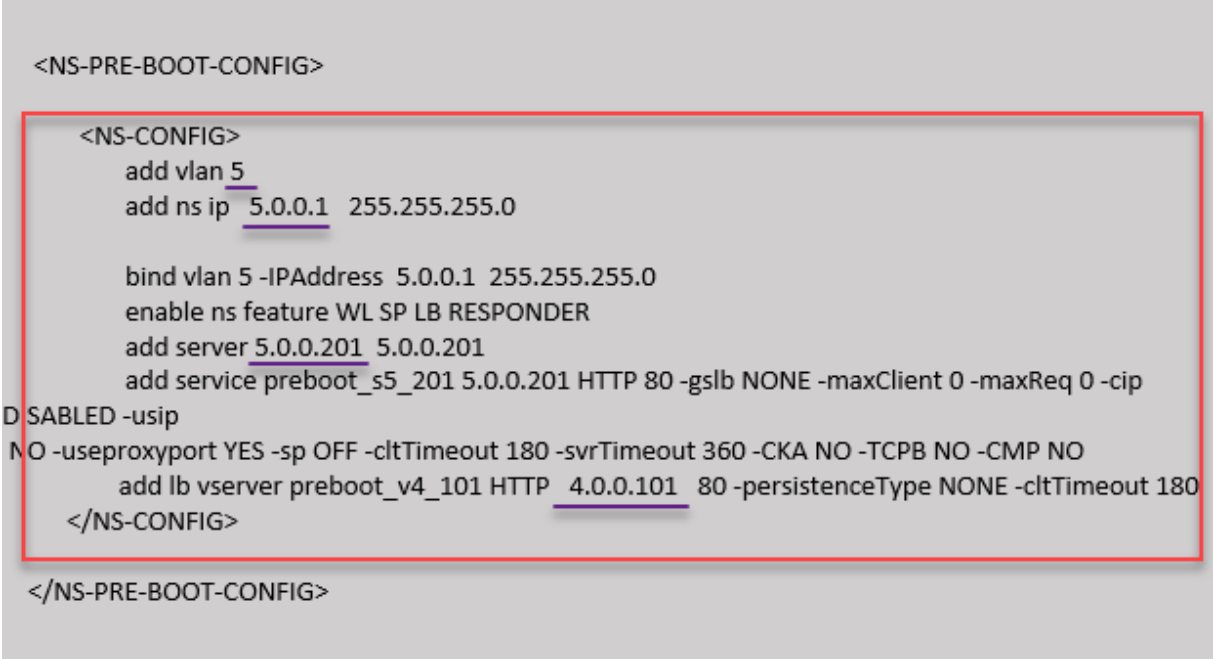
NetScaler 配置

使用 <NS-CONFIG> 标签提供需要在预启动阶段应用于 VPX 实例的特定 NetScaler VPX 配置。

> 注意：
>
> <NS-CONFIG> 部分必须具有有效的 ADC CLI 命令。没有验证 CLIS 是否存在语法错误或格式问题。

Example:

在以下示例中，<NS-CONFIG> 部分提供了配置的详细信息。ID 为“5”的 VLAN 已配置并绑定到 SNIP (5.0.0.1)。此外，还配置了负载平衡虚拟服务器 (4.0.0.101)。



你可以从这里复制上面的屏幕截图中显示的配置：

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

NetScaler VPX 实例提供了本 <NS-CONFIG> 节中应用的配置，如下图所示。


```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -------
1)      10.160.0.72      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      5.0.0.1          0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:48/64
        Interfaces : 1/1 1/2 LO/1

2)      VLAN ID: 5      VLAN Alias Name:
        IPs :
             5.0.0.1    Mask: 255.255.255.0

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 0/1
        IPs :
             10.160.0.72        Mask: 255.255.240.0
 Done
```

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

Service(s) Summary
                           IP  port         Type        State    Req/s
preb...5_201        5.0.0.201    80         HTTP         DOWN      0/s
gcpl...vice0 169.254.169.254    53          DNS           UP      0/s
 Done
> sh service preboot_s5_201
        preboot_s5_201 (5.0.0.201:80) - HTTP
        State: DOWN
        Last state change was at Tue Dec 29 07:18:28 2020
        Time since last state change: 0 days, 00:05:02.820
        Server Name: 5.0.0.201
        Server ID : None        Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Monitoring Owner: 0
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
        Monitor Connection Close : NONE
        Appflow logging: ENABLED
        Process Local: DISABLED
```


用户脚本

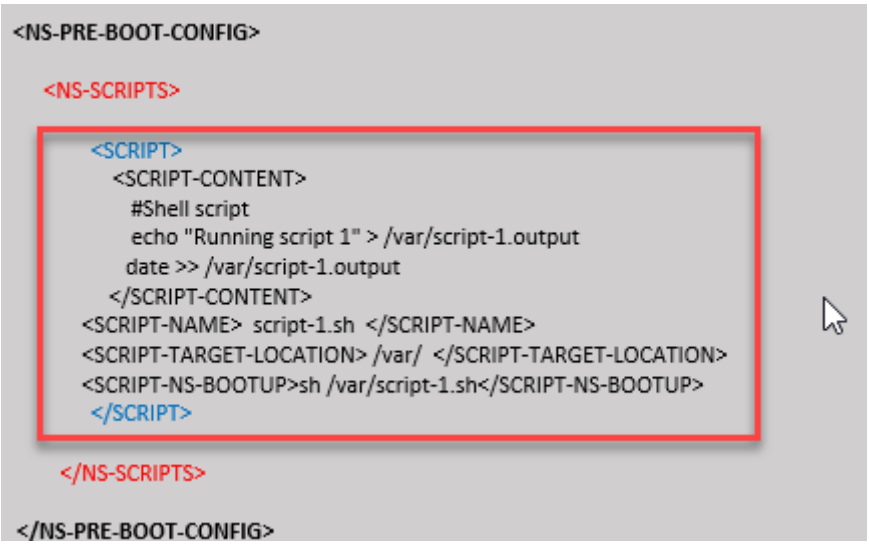
使用 <NS-SCRIPTS> 标签提供必须在 NetScaler VPX 实例中存储和运行的任何脚本。

可以在 <NS-SCRIPTS> 标记中包含许多脚本。每个脚本都必须包含在 <SCRIPT> 标记中。每个 <SCRIPT> 部分对应一个脚本，并使用以下子标记包含脚本的所有详细信息。

- **<SCRIPT-NAME>:** 指示必须存储的脚本文件的名称。
- **<SCRIPT-CONTENT>:** 指示必须存储的文件的内容。
- **<SCRIPT-TARGET-LOCATION>:** 指示必须存储此文件的指定目标位置。如果未提供目标位置，则默认情况下，文件或脚本将保存在“/nsconfig”目录中。
- **<SCRIPT-NS-BOOTUP>:** 指定用于运行脚本的命令。
  - 如果使用 <SCRIPT-NS-BOOTUP> 部分，该部分中提供的命令将存储在“/nsconfig/nsafter.sh”中，并且这些命令在数据包引擎启动后作为“nsafter.sh”执行的一部分运行。
  - 如果不使用 <SCRIPT-NS-BOOTUP> 部分，脚本文件将存储在指定的目标位置。

示例 **1**:

在此示例中，<NS-SCRIPTS> 标记仅包含一个脚本的详细信息：script-1.sh。“script-1.sh”脚本保存在“/var”目录中。脚本使用指定的内容填充，并在数据包引擎启动后使用“sh /var/script-1.sh”命令运行。



你可以从这里复制上面的屏幕截图中显示的配置：

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

```



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

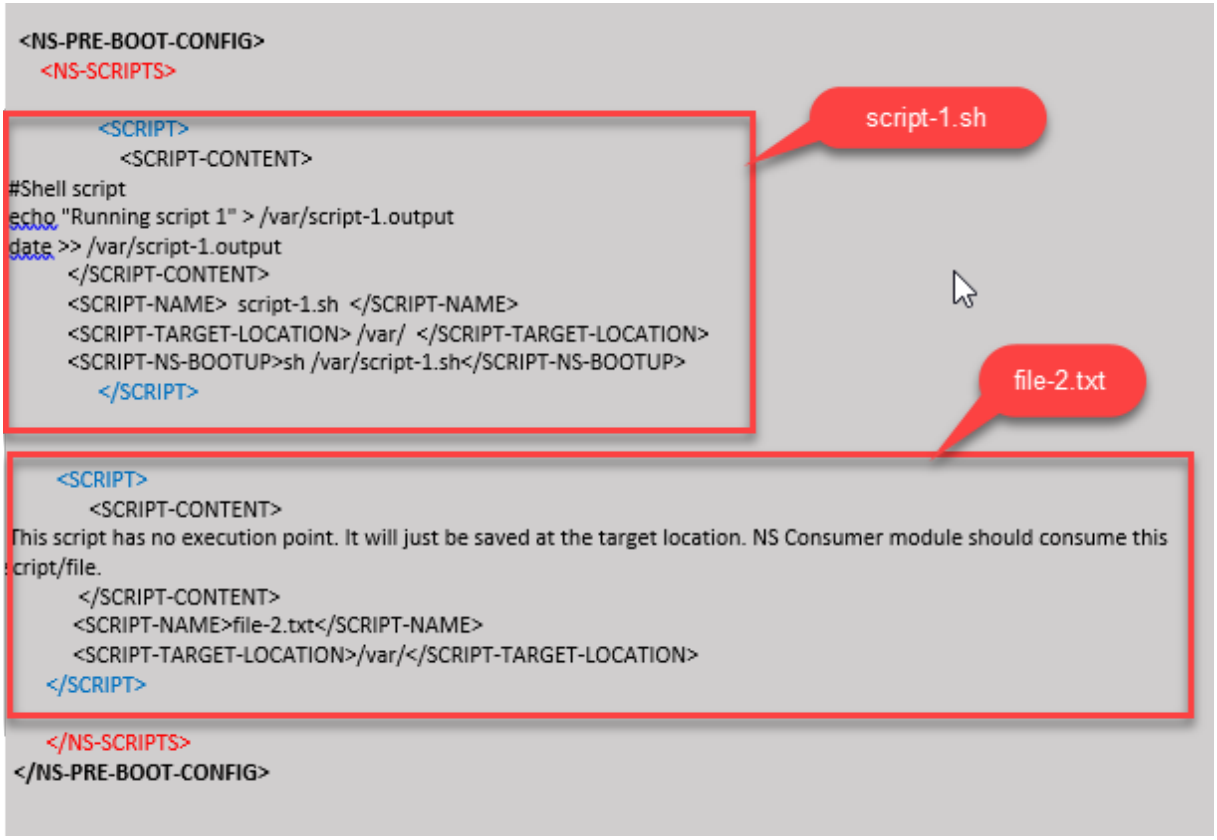
在下面的快照中，您可以验证“script-1.sh”脚本是否保存在“/var/”目录中。运行“Script-1.sh”脚本，并正确创建输出文件。

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

示例 **2**:

在以下示例中，<NS-SCRIPTS> 标记包含两个脚本的详细信息。

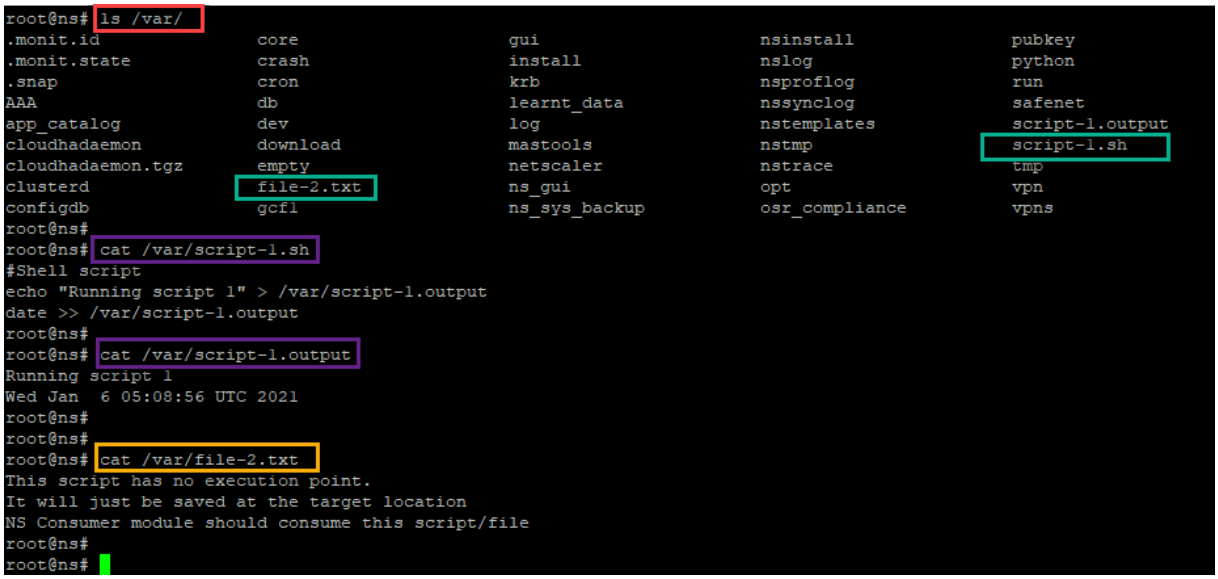
- 第一个脚本在“/var”目录中另存为“script-1.sh”。脚本使用指定的内容填充，并在数据包引擎启动后使用命令“sh /var/script-1.sh”运行。
- 第二个脚本在“/var”目录中另存为“file-2.txt”。此文件使用指定的内容填充。但此文件未运行，因为未提供启动执行命令 <SCRIPT-NS-BOOTUP>



你可以从这里复制上面的屏幕截图中显示的配置：

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

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

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


在下面的快照中，您可以验证 script-1.sh 和 file-2.txt 是否在“/var/”目录中创建。Script-1.sh 已运行，输出文件已恰当创建。



许可

在启动 VPX 实例时使用 <NS-LICENSE-CONFIG> 标签应用 NetScaler 池化许可。请使用 <NS-LICENSE-CONFIG> 部分中的 <LICENSE-COMMANDS> 标记提供池许可证命令。这些命令必须在语法上有效。

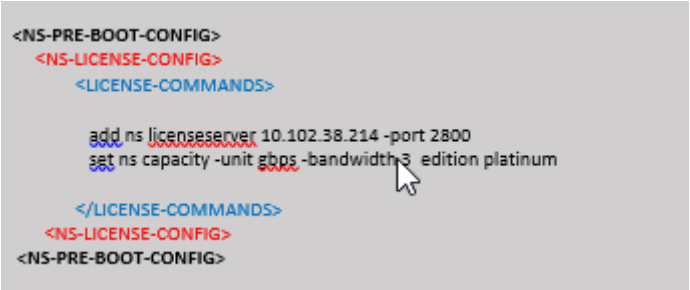
可以使用标准池许可命令在 <LICENSE-COMMANDS> 部分中指定池许可详细信息，例如许可证类型、容量和许可证服务器。有关更多信息，请参阅 配置 NetScaler 池容量许可。

应用 <NS-LICENSE-CONFIG> 后，VPX 会在启动时随附所请求的版本，VPX 会尝试从许可证服务器中签出配置的许可证。

- 如果许可证签出成功，配置的带宽将应用到 VPX。
- 如果许可证签出失败，大约在 10-12 分钟内不会从许可证服务器检索许可证。因此，系统将重新启动并进入未许可状态。

Example:

在以下示例中，应用 <NS-LICENSE-CONFIG> 后，VPX 在启动时会随附 Premium Edition，VPX 会尝试从许可证服务器 (10.102.38.214) 签出配置的许可证。



你可以从这里复制上面的屏幕截图中显示的配置：

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
```

如下图所示，您可以运行“show license server”命令，并验证许可证服务器 (10.102.38.214) 是否已添加到 VPX 中。

引导

使用 <NS-BOOTSTRAP> 标记可提供自定义引导信息。可以在 <NS-BOOTSTRAP> 部分中使用 <SKIP-DEFAULT-BOOTSTRAP> 和 <NEW-BOOTSTRAP-SEQUENCE> 标记。本节告知 NetScaler 设备是否要避免使用默认引导。如果避免使用默认引导程序，本部分内容为您提供了一个选项来提供新的引导序列。

默认引导配置

NetScaler 设备中的默认引导配置遵循以下接口分配：

- **Eth0** - 管理接口，具有特定 NSIP 地址。
- **Eth1** - 面向客户端的接口，具有特定 VIP 地址。
- **Eth2** - 面向服务器的接口，具有特定 SNIP 地址。

自定义引导配置

您可以跳过默认的引导序列，为 NetScaler VPX 实例提供新的引导顺序。使用 <NS-BOOTSTRAP> 标记可提供自定义引导信息。例如，可以更改默认引导，其中管理接口 (NSIP)、面向客户端的接口 (VIP) 和面向服务器的接口 (SNIP) 始终按特定顺序提供。

下表显示了具有允许使用的 <SKIP-DEFAULT-BOOTSTRAP> 和 <NEW-BOOTSTRAP-SEQUENCE> 标记的不同值的引导行为。

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	引导行为
是	是	将跳过默认引导行为，并运行 <NS-BOOTSTRAP> 部分中提供的新自定义引导序列。
是	否	将跳过默认的引导行为。将跳过默认引导行为，并运行 <NS-CONFIG> 部分中提供的引导命令。

可以通过以下三种方法自定义引导配置：

- 仅提供接口详细信息
- 提供接口详细信息以及 IP 地址和子网掩码
- 在 <NS-CONFIG> 部分中提供与引导程序相关的命令

方法 **1**：通过仅指定接口详细信息来自定义引导

可以指定管理接口、面向客户端的接口和面向服务器的接口，但不指定其 IP 地址和子网掩码。通过查询云基础结构来填充 IP 地址和子网掩码。

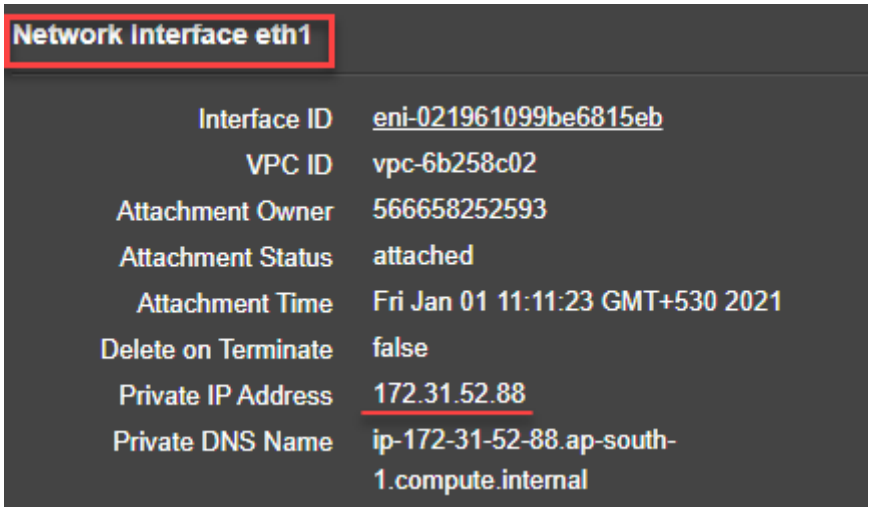
AWS 的自定义引导示例

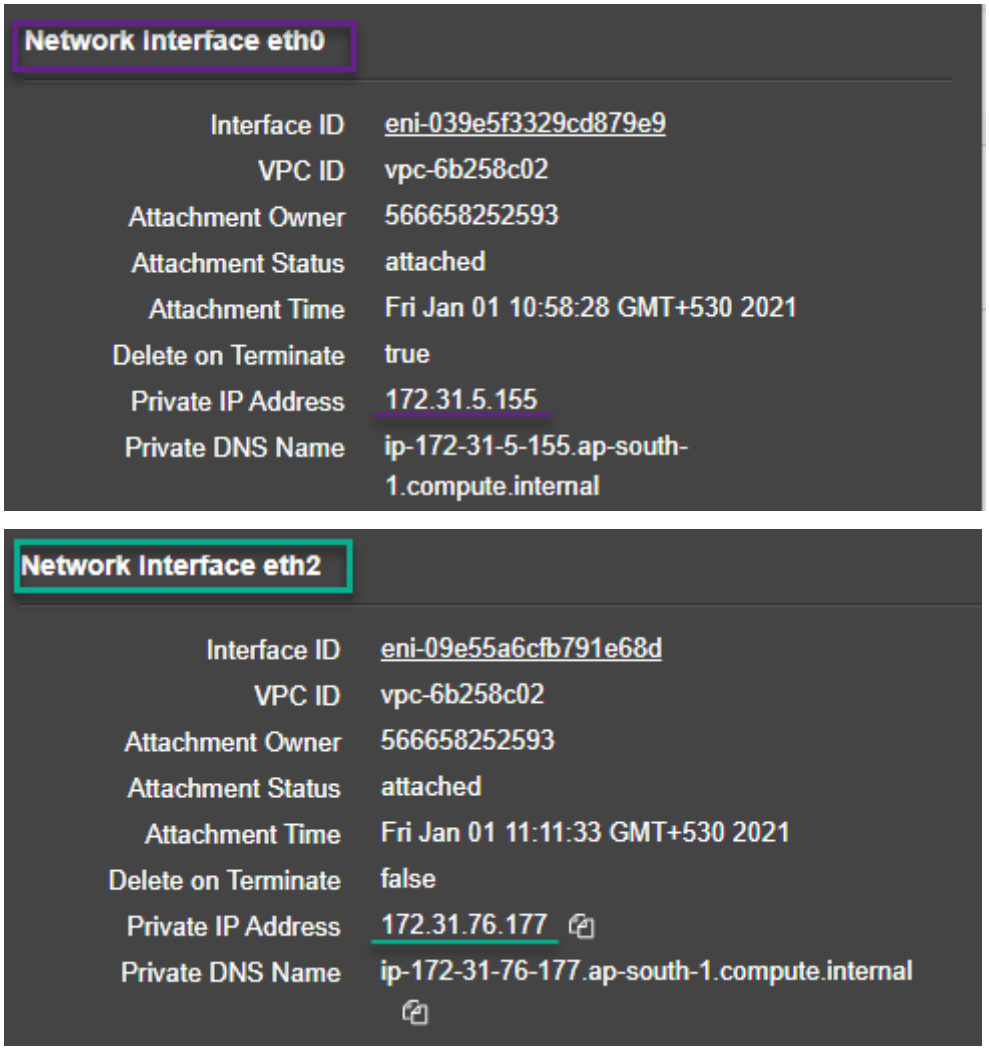
您提供自定义引导序列，如以下示例所示。有关更多信息，请参阅 如何在云实例中提供预引导用户数据。Eth1 接口被分配为管理接口 (NSIP)，Eth0 接口被分配为客户端接口 (VIP)，Eth2 接口被分配为服务器接口 (SNIP)。<NS-BOOTSTRAP> 部分仅包含接口详细信息，不包含 IP 地址和子网掩码的详细信息。


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

创建 VM 实例后，您可以在 AWS 门户中验证网络接口属性，如下所示：

1. 导航到 **AWS Portal**（**AWS** 门户）**> AWS Portal**（**EC2** 实例），然后通过提供自定义引导信息选择您创建的实例。
2. 在 **Description**（说明）选项卡中，您可以验证每个网络接口的属性，如下图所示。





您可以在 **ADC CLI** 中运行 `show nsip` 命令，并在 ADC 设备首次启动期间验证应用于 NetScaler VPX 实例的网络接口。

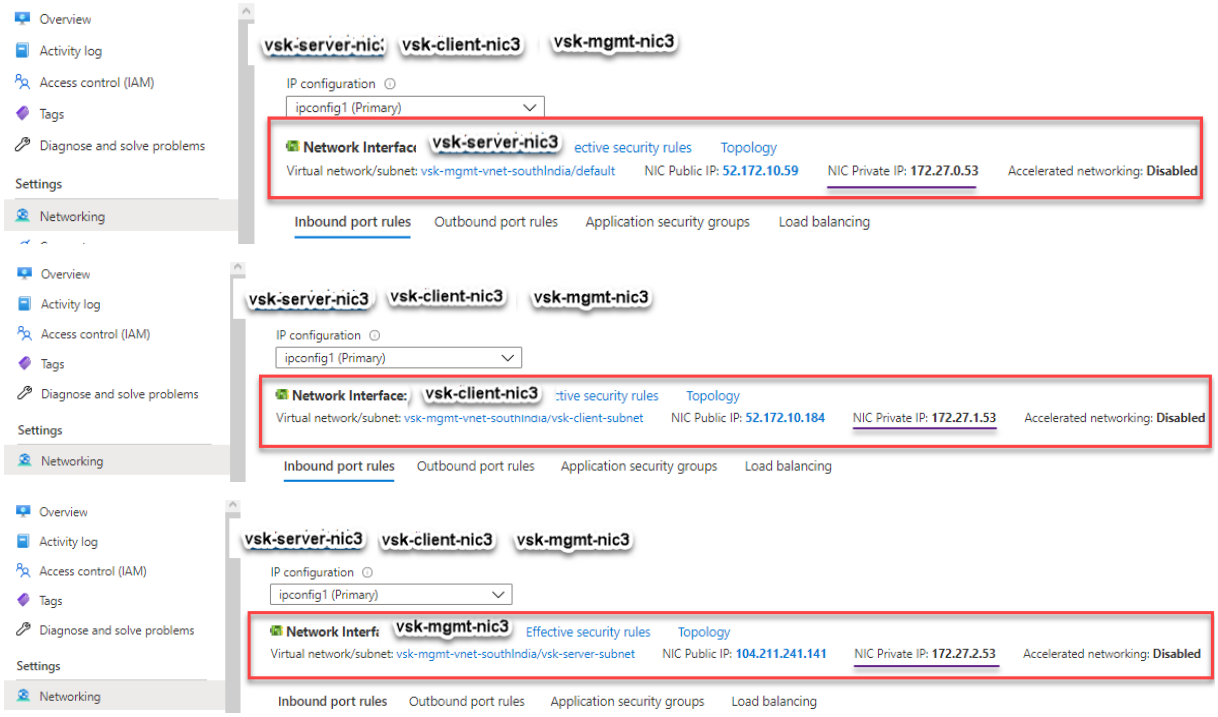

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
```

Azure 的自定义引导示例

您提供自定义引导序列，如以下示例所示。有关更多信息，请参阅 如何在云实例中提供预引导用户数据。Eth1 接口被分配为管理接口 (NSIP)，Eth0 接口被分配为客户端接口 (VIP)，Eth2 接口被分配为服务器接口 (SNIP)。<NS-BOOTSTRAP> 部分仅包含接口详细信息，不包含 IP 地址和子网掩码的详细信息。

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

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

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

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

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

    </NS-BOOTSTRAP>

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


您可以看到 NetScaler VPX 实例是用三个网络接口创建的。导航到 **Azure portal**（**Azure** 门户）**> VM instance**（**VM** 实例）**> Networking**（网络连接），然后验证三个 NIC 的网络属性，如下图所示。



可以在 ADC CLI 中运行 `show nsip` 命令，并验证是否应用了 <NS-BOOTSTRAP> 部分中指定的新引导序列。可以运行“show route”命令来验证子网掩码。

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

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

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


GCP 的自定义引导示例

您提供自定义引导序列，如以下示例所示。有关更多信息，请参阅 如何在云实例中提供预引导用户数据。Eth1 接口被分配为管理接口 (NSIP)，Eth0 接口被分配为客户端接口 (VIP)，Eth2 接口被分配为服务器接口 (SNIP)。<NS-BOOTSTRAP> 部分仅包含接口详细信息，不包含 IP 地址和子网掩码的详细信息。

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

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

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

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

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

在 GCP 门户中创建 VM 实例后，可以按如下方式验证网络接口属性：

1. 请通过提供自定义引导信息来选择您创建的实例。
2. 导航到网络接口属性并按如下方式验证 NIC 详细信息：

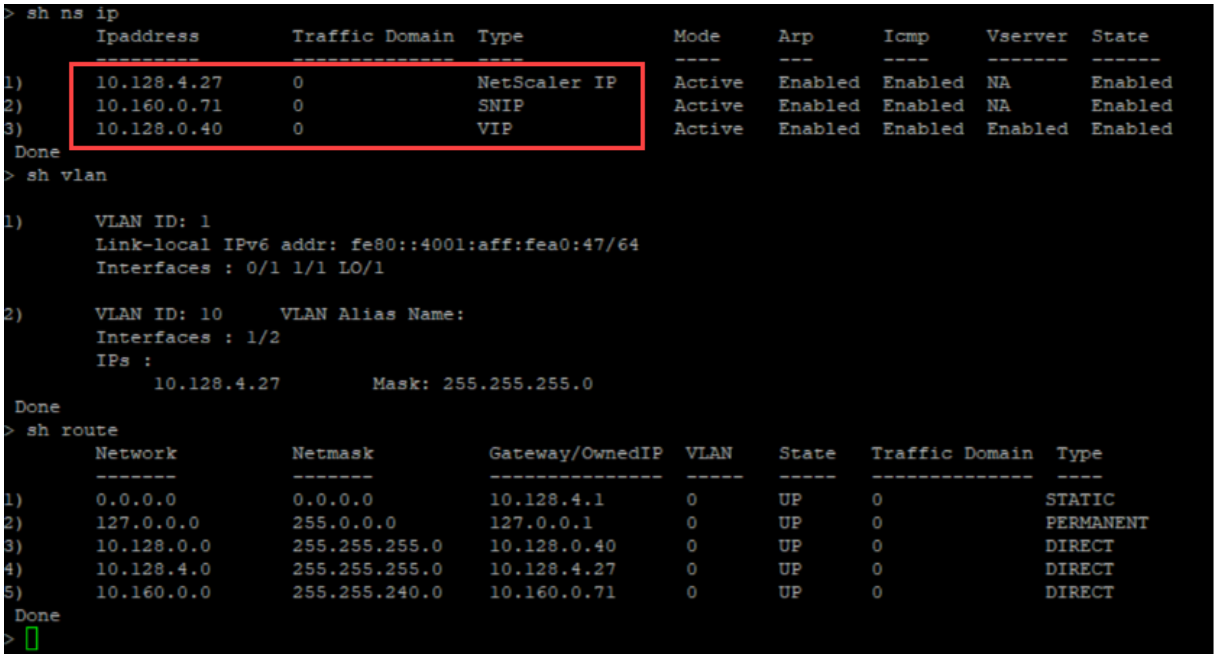
Network interfaces

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

Public DNS PTR Record

None

您可以在 **ADC CLI** 中运行 `show nsip` 命令，并在 ADC 设备首次启动期间验证应用于 NetScaler VPX 实例的网络接口。



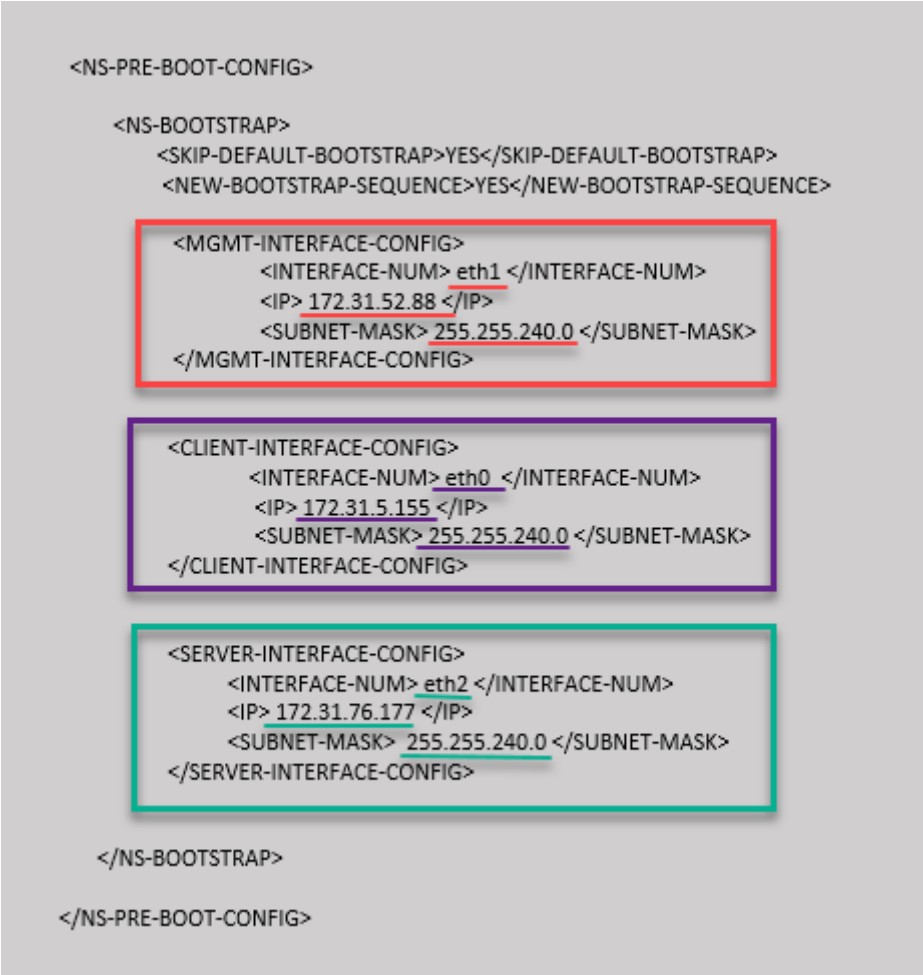
方法 **2**：通过指定接口、**IP** 地址和子网掩码来自定义引导

可以指定管理接口、面向客户端的接口和面向服务器的接口及其 IP 地址和子网掩码。

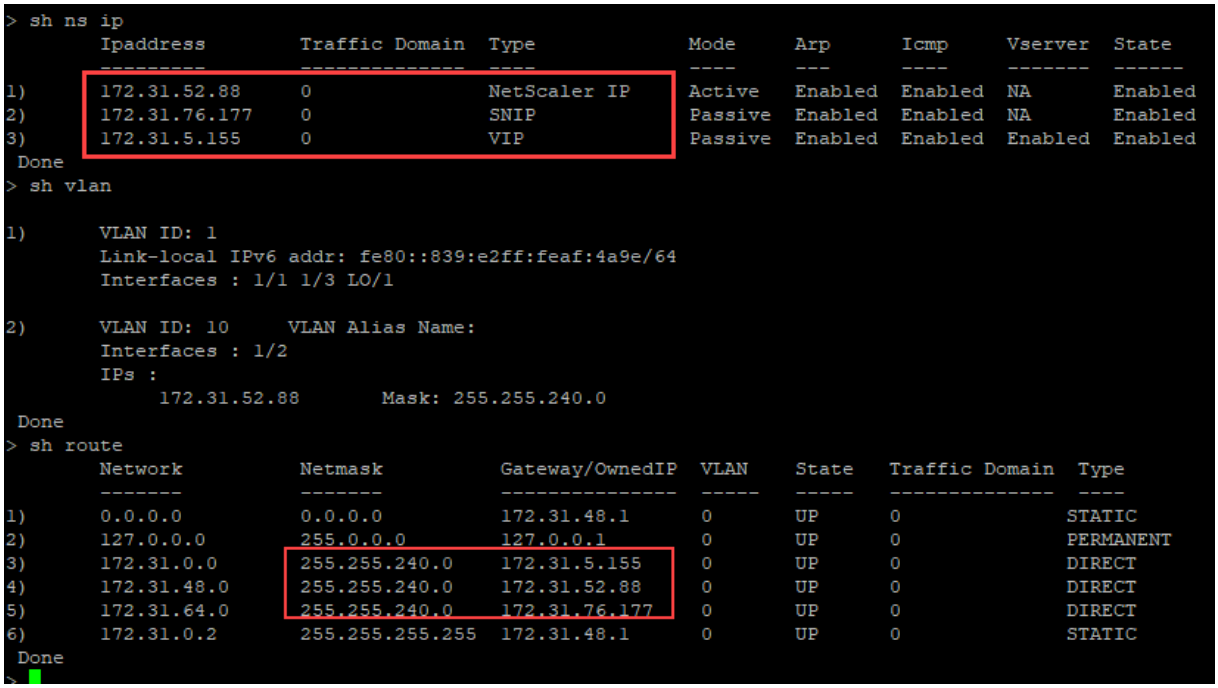
AWS 的自定义引导示例

在以下示例中，您跳过默认引导程序，为 NetScaler 设备运行新的引导序列。对于新的引导序列，您需要指定以下详细信息：

- 管理接口：接口 - Eth1，NSIP - 172.31.52.88，子网掩码 - 255.255.240.0
- 面向客户端的接口：接口 - Eth0，VIP - 172.31.5.155，子网掩码 - 255.255.240.0。
- 面向服务器的接口：接口 - Eth2，SNIP - 172.31.76.177，子网掩码 - 255.255.240.0。



可以在 ADC CLI 中运行“show nsip”命令，并验证是否应用了 <NS-BOOTSTRAP> 部分中指定的新引导序列。可以运行“show route”命令来验证子网掩码。



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

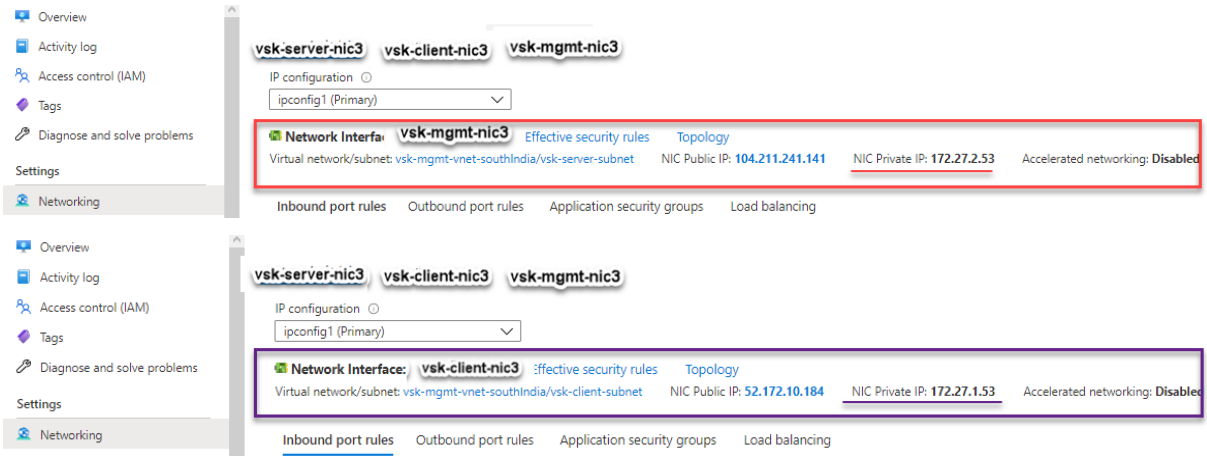
Azure 的自定义引导示例

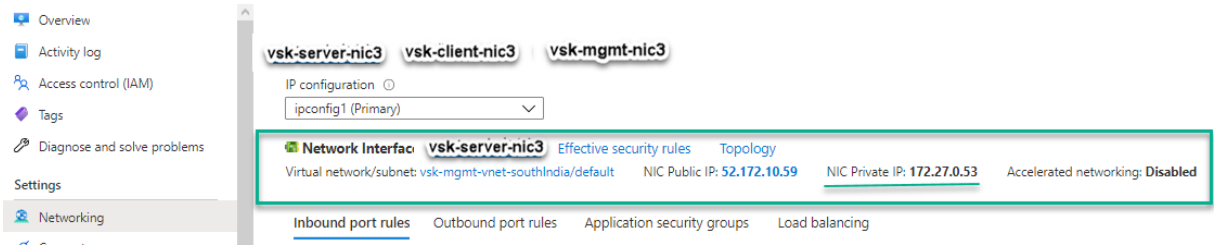
在以下示例中，提到了 ADC 的新引导序列，并跳过默认引导程序。您可以提供接口详细信息以及 IP 地址和子网掩码，如下所示：

- 管理接口 (eth2)、NSIP (172.27.2.53) 和子网掩码 (255.255.255.0)
- 面向客户端的接口 (eth1)、VIP (172.27.1.53) 和子网掩码 (255.255.255.0)
- 面向服务器的接口 (eth0)、SNIP (172.27.0.53) 和子网掩码 (255.255.255.0)


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

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

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

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

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

    </NS-BOOTSTRAP>

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

您可以看到 NetScaler VPX 实例是用三个网络接口创建的。导航到 **Azure portal**（**Azure** 门户）**> VM instance**（**VM** 实例）**> Networking**（网络连接），然后验证三个 NIC 的网络属性，如下图所示。





可以在 ADC CLI 中运行“show nsip”命令，并验证是否应用了 <NS-BOOTSTRAP> 部分中指定的新引导序列。可以运行“show route”命令来验证子网掩码。

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

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

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

GCP 的自定义引导示例

在以下示例中，提到了 ADC 的新引导序列，并跳过默认引导程序。您可以提供接口详细信息以及 IP 地址和子网掩码，如下所示：

- 管理接口 (eth2)、NSIP (10.128.4.31) 和子网掩码 (255.255.255.0)
- 面向客户端的接口 (eth1)、VIP (10.128.0.43) 和子网掩码 (255.255.255.0)
- 面向服务器的接口 (eth0)、SNIP (10.160.0.75) 和子网掩码 (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 10.128.4.31 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 10.128.0.43 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </CLIENT-INTERFACE-CONFIG>
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 10.160.0.75 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

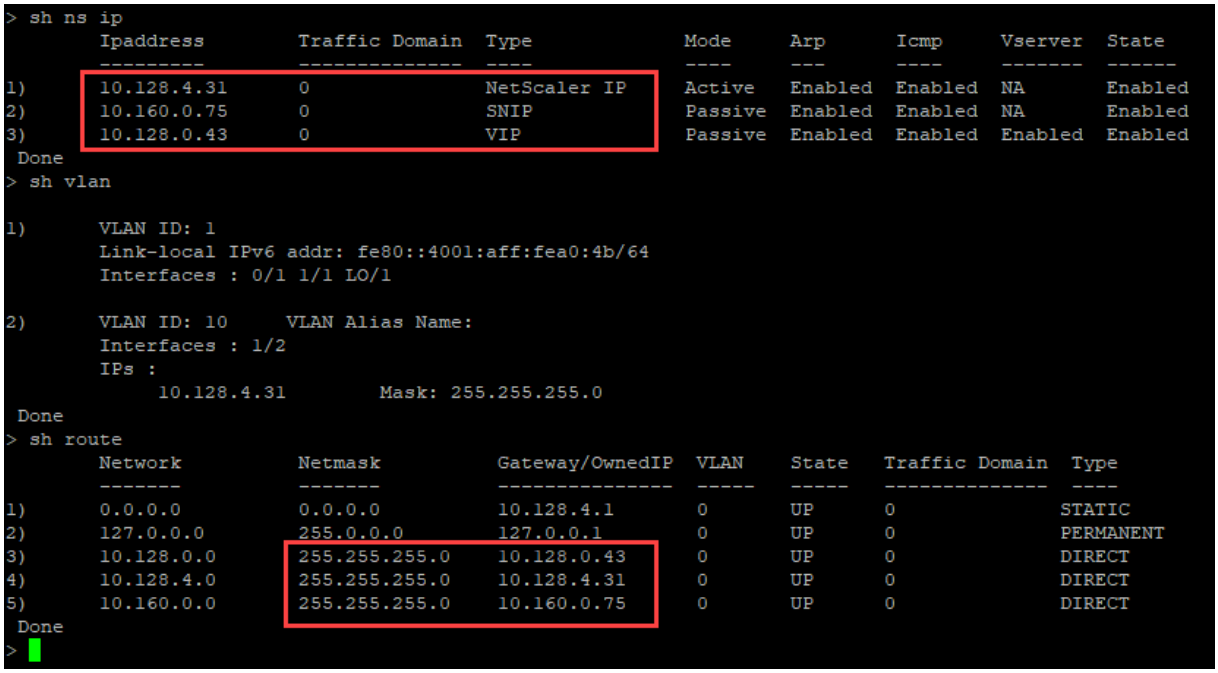
使用自定义引导程序在 GCP 门户中创建 VM 实例后，可以按如下方式验证网络接口属性：

1. 请通过提供自定义引导信息来选择您创建的实例。
2. 导航到网络接口属性并按如下方式验证 NIC 详细信息。

Network interfaces

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

可以在 ADC CLI 中运行“show nsip”命令，并验证是否应用了 <NS-BOOTSTRAP> 部分中指定的新引导序列。可以运行“show route”命令来验证子网掩码。



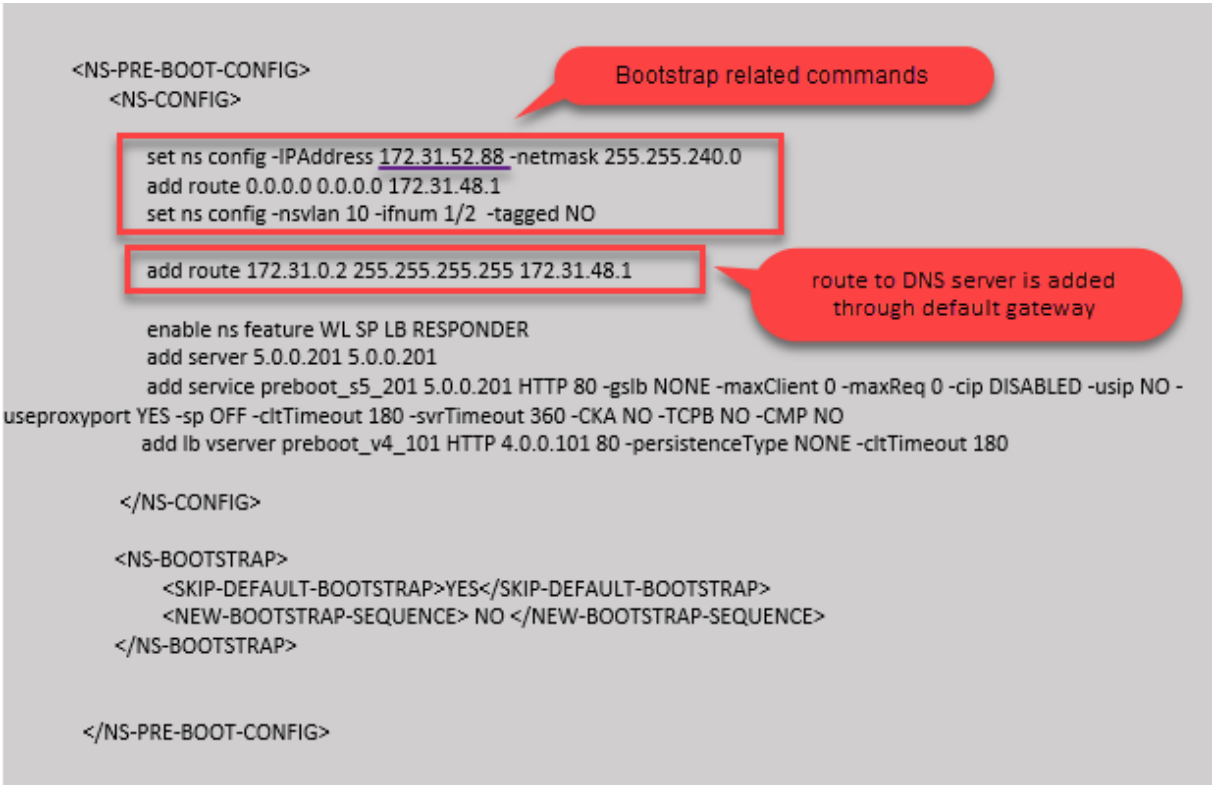
方法 **3**：通过在 **<NS-CONFIG>** 部分中提供引导程序相关的命令来自定义引导

可以在 <NS-CONFIG> 部分中提供引导程序相关的命令。在 <NS-BOOTSTRAP> 部分中，必须将 <NEW-BOOTSTRAP-SEQUENCE> 指定为“否”才能运行 <NS-CONFIG> 部分中的引导命令。还必须提供用于分配 NSIP、默认路由和 NSVLAN 的命令。此外，请提供与您使用的云相关的命令。

在提供自定义引导之前，请确保云基础结构支持特定的接口配置。

AWS 的自定义引导示例

在此示例中，<NS-CONFIG> 部分提供了引导程序相关的命令。<NS-BOOTSTRAP> 部分指示跳过默认引导，并运行 <NS-CONFIG> 部分中提供的自定义引导信息。还必须提供命令来创建 NSIP、添加默认路由和添加 NSVLAN。

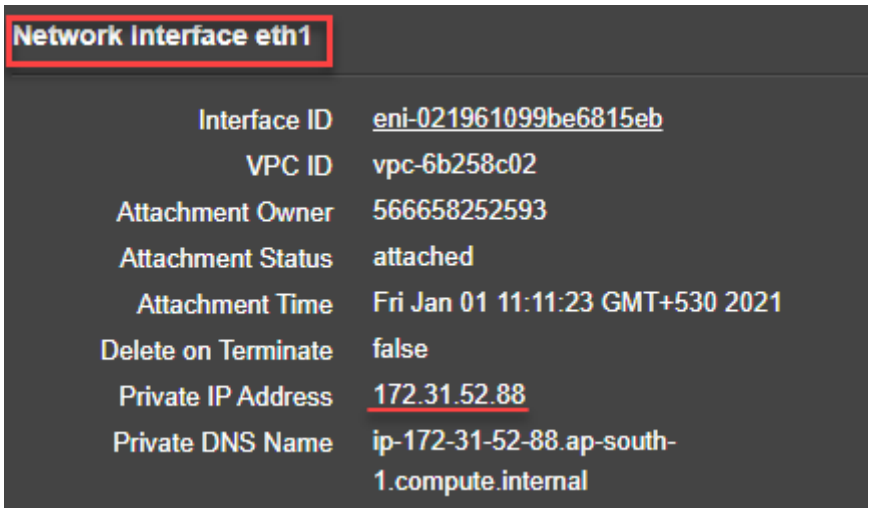


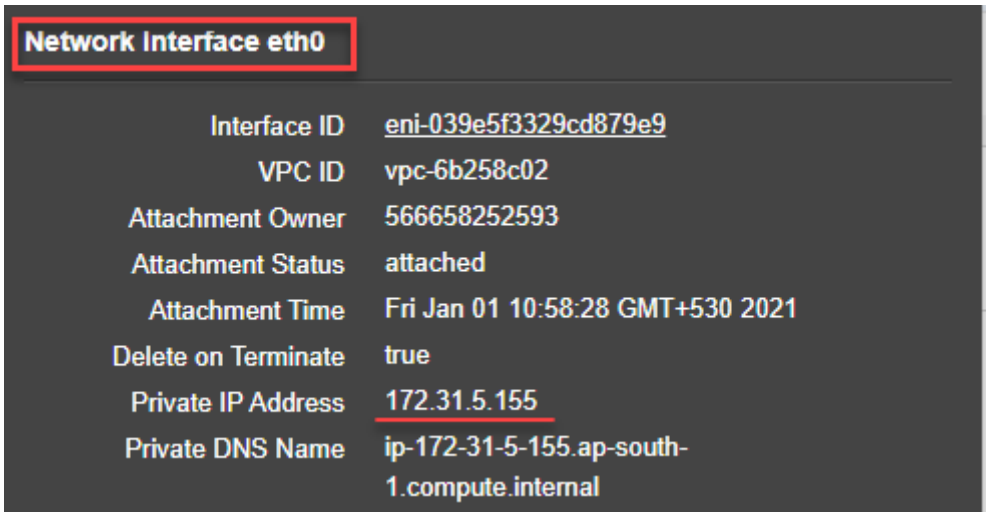
你可以从这里复制上面的屏幕截图中显示的配置：

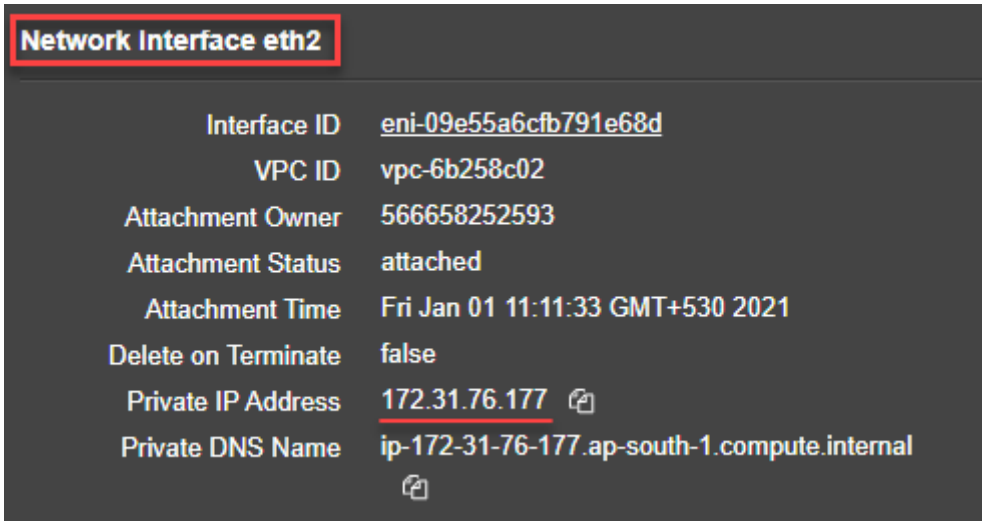
```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

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

    </NS-CONFIG>

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


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


创建 VM 实例后，您可以在 AWS 门户中验证网络接口属性，如下所示：

1. 导航到 **AWS Portal**（**AWS** 门户）**> AWS Portal**（**EC2** 实例），然后通过提供自定义引导信息选择您创建的实例。
2. 在 **Description**（说明）选项卡中，您可以验证每个网络接口的属性，如下图所示。







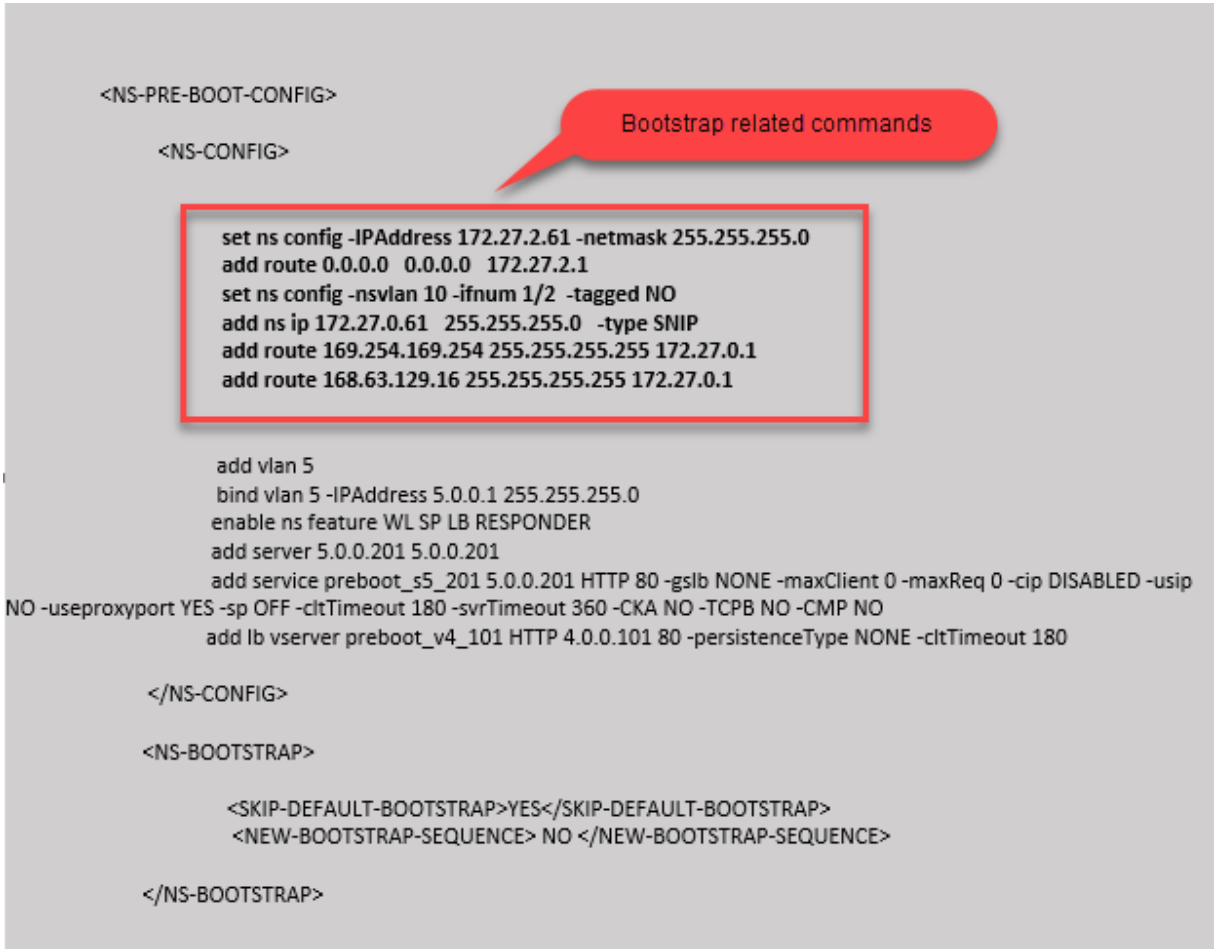
您可以在 **ADC CLI** 中运行 `show nsip` 命令，并在 ADC 设备首次启动期间验证应用于 NetScaler VPX 实例的网络接口。

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Azure 的自定义引导示例

在此示例中，<NS-CONFIG> 部分提供了引导程序相关的命令。<NS-BOOTSTRAP> 部分指示跳过默认引导，并运行 <NS-CONFIG> 部分中提供的自定义引导信息。

> 注意：
>
> 对于 Azure 云，实例元数据服务器 (IMDS) 和 DNS 服务器只能通过主接口 (Eth0) 访问。因此，如果 Eth0 接口未用作管理接口 (NSIP)，则 Eth0 接口必须至少配置为 SNIP，以便 IMDS 或 DNS 访问能够正常进行。还必须添加通过 Eth0 的网关到 IMDS 终端节点 (169.254.169.254) 和 DNS 终端节点 (168.63.129.16) 的路由。

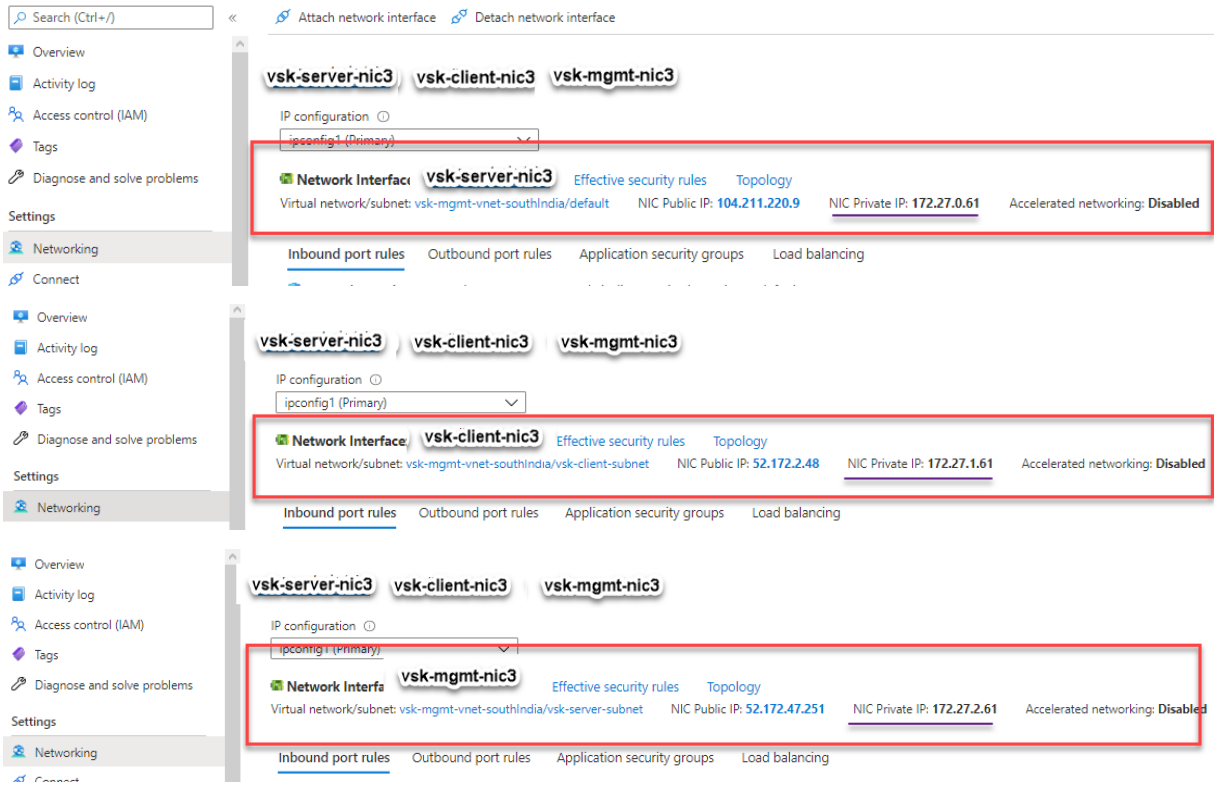



```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

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

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

    </NS-CONFIG>
```

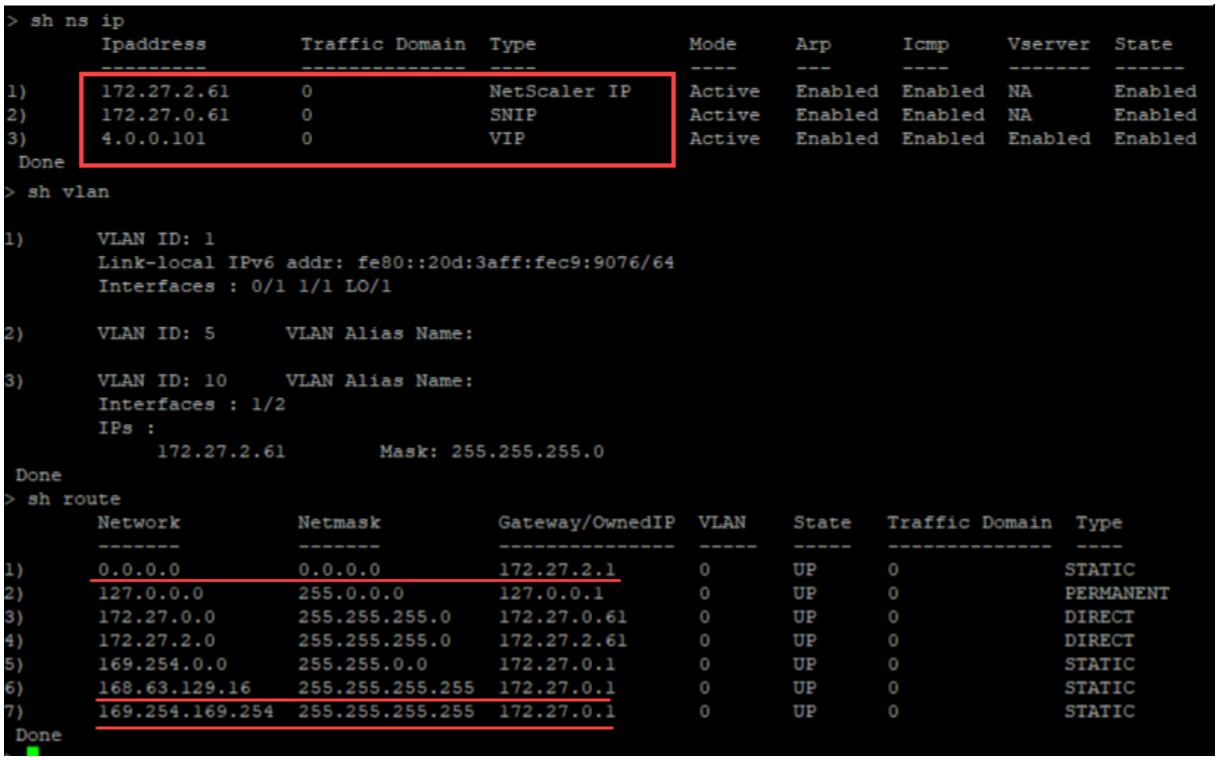


```
20
21          <NS-BOOTSTRAP>
22
23          <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24          <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26          </NS-BOOTSTRAP>
27
28      </NS-PRE-BOOT-CONFIG>
```

您可以看到 NetScaler VPX 实例是用三个网络接口创建的。导航到 **Azure portal**（**Azure** 门户）**> VM instance**（**VM** 实例）**> Networking**（网络连接），然后验证三个 NIC 的网络属性，如下图所示。



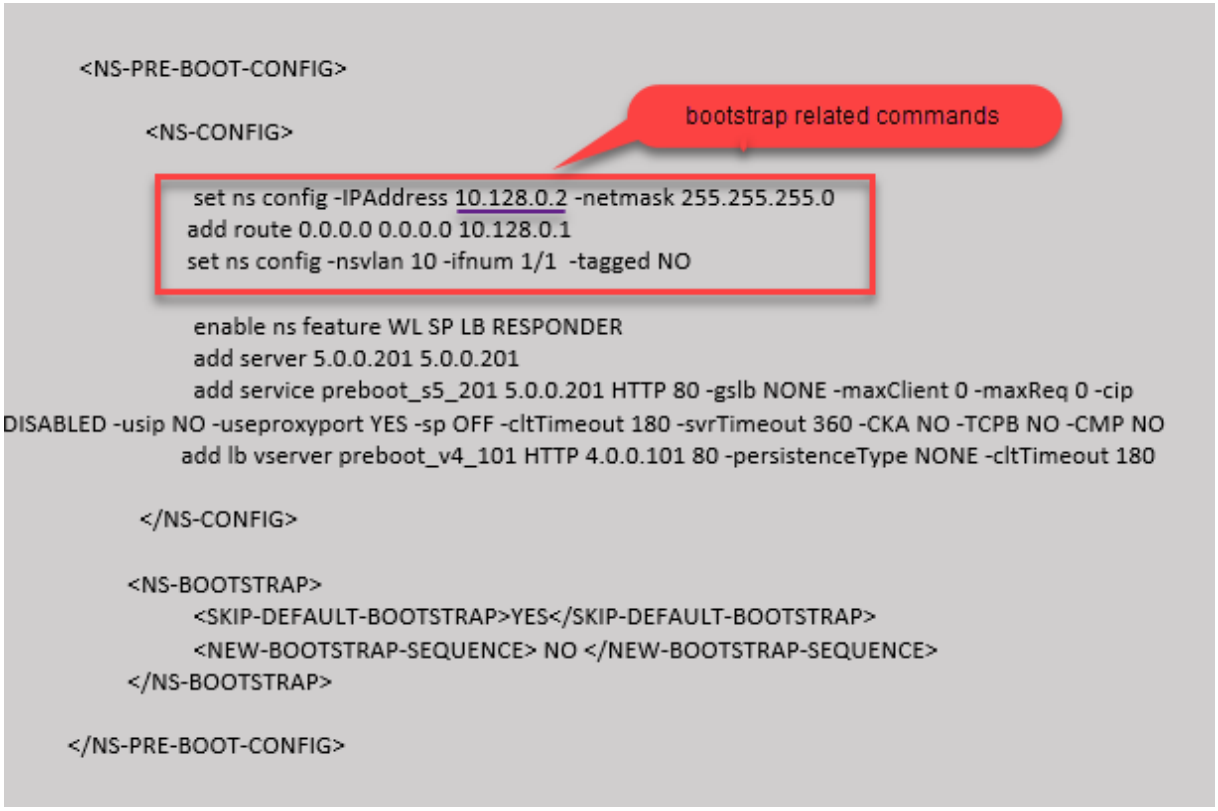
可以在 ADC CLI 中运行“show nsip”命令，并验证是否应用了 <NS-BOOTSTRAP> 部分中指定的新引导序列。可以运行“show route”命令来验证子网掩码。



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode       Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----       ---      ----     -------  -----
1)      172.27.2.61      0               NetScaler IP     Active     Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active     Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active     Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

GCP 的自定义引导示例

在此示例中，<NS-CONFIG> 部分提供了引导程序相关的命令。<NS-BOOTSTRAP> 部分表示跳过默认引导，并应用 <NS-CONFIG> 部分中提供的自定义引导信息。



你可以从这里复制上面的屏幕截图中显示的配置：

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

    <NS-CONFIG>

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

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

    </NS-CONFIG>

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

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


使用自定义引导程序在 GCP 门户中创建 VM 实例后，可以按如下方式验证网络接口属性：

1. 请通过提供自定义引导信息来选择您创建的实例。
2. 导航到网络接口属性并验证 NIC 详细信息，如图所示。

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)

可以在 **ADC CLI** 中运行 `show nsip` 命令，并验证在首次启动 ADC 设备时是否应用了前面 <NS-CONFIG> 部分中提供的配置。

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

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

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

在 **AWS** 和 **Azure** 中附加和分离 **NIC** 产生的影响

AWS 和 Azure 提供了将网络接口附加到实例以及将网络接口与实例分离的选项。连接或分离接口可能会改变接口位置。因此，Citrix 建议您不要将接口与 NetScaler VPX 实例分离。如果您在配置自定义引导时分离或连接接口，NetScaler VPX 实例会将管理接口的主 IP 重新分配为 NSIP 的管理接口。如果在您分离的接口之后没有其他可用的接口，则第一个接口将成为 NetScaler VPX 实例的管理接口。

例如，一个 NetScaler VPX 实例启动时有 3 个接口：Eth0（SNIP）、Eth1（NSIP）和 Eth2（VIP）。如果将 Eth1 接口与实例（管理接口）分离，ADC 会将下一个可用接口 (Eth2) 配置为管理接口。因此，NetScaler VPX 实例仍可通过 Eth2 接口的主要 IP 进行访问。如果 Eth2 也不可用，剩余的接口 (Eth0) 将成为管理接口。因此，对 NetScaler VPX 实例的访问权限仍然存在。

我们假设存在以下不同的接口分配：Eth0 (SNIP)、Eth1 (VIP) 和 Eth2 (NSIP)。如果分离 Eth2 (NSIP)（因为在 Eth2 之后没有新接口可用），第一个接口 (Eth0) 将成为管理接口。

提高公有云平台上的 **SSL-TPS** 性能

October 17, 2024

通过平均分配数据包引擎 (PE) 权重，您可以在 AWS 和 GCP 云上获得更好的 SSL-TPS 性能。启用此功能可能会导致 HTTP 吞吐量略有下降 10-12% 左右。

在 AWS 和 GCP 云上，具有 10-16 个 vCPU 的 NetScaler VPX 实例不会显示任何性能提升，因为默认情况下 PE 权重是平均分布的。

> 注意：
>
> 在 Azure 云中，默认情况下，PE 权重平均分配。此功能不会提高 Azure 实例的任何性能。

使用 **NetScaler CLI** 配置 **PE** 模式

设置 PE 模式后，必须重新启动系统才能使配置更改生效。

在命令提示符下，键入：

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

当 PE 模式设置为 CPUBOUND 时，PE 权重将平均分布。当 PE 模式设置为 DEFAULT 时，PE 权重将设置为默认值。

> 注意：
>
> 此命令特定于节点。在高可用性或群集设置中，必须在每个节点上运行命令。如果在 CLIP 上运行该命令，则会出现以下错误：`CLIP 上不允许操作`

要显示配置的 PE 模式的状态，请运行以下命令：

```
show cpuparam
```

Example:

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

在云中首次启动 **NetScaler** 设备时应用 **PE** 模式配置

要在云中首次启动 NetScaler 设备时应用 PE 模式配置，必须使用自定义脚本创建一个 `/nsconfig/.cpubound.conf` 文件。有关详细信息，请参阅 在云中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。

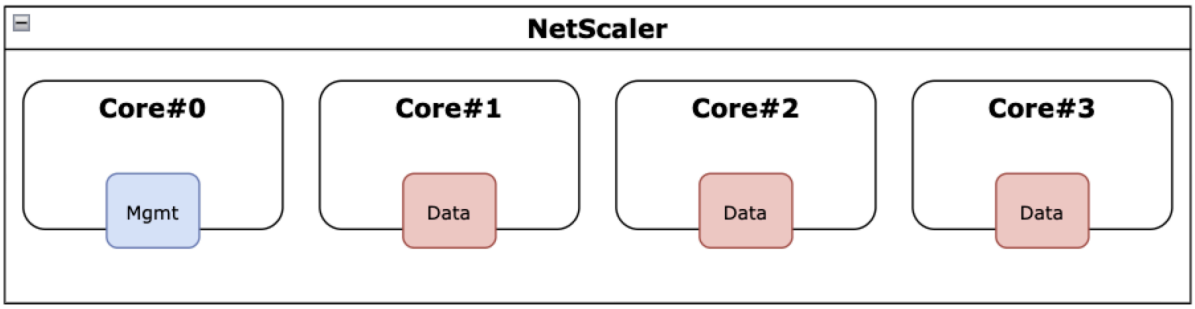
为公有云上的 **NetScaler VPX** 配置同步多线程

October 17, 2024

NetScaler 使用不同的专用内核进行管理和数据平面功能。一个核心通常分配给管理平面功能。其余可用内核分配给数据平面函数。

下图显示了 4 核 NetScaler VPX 的简化示意图。

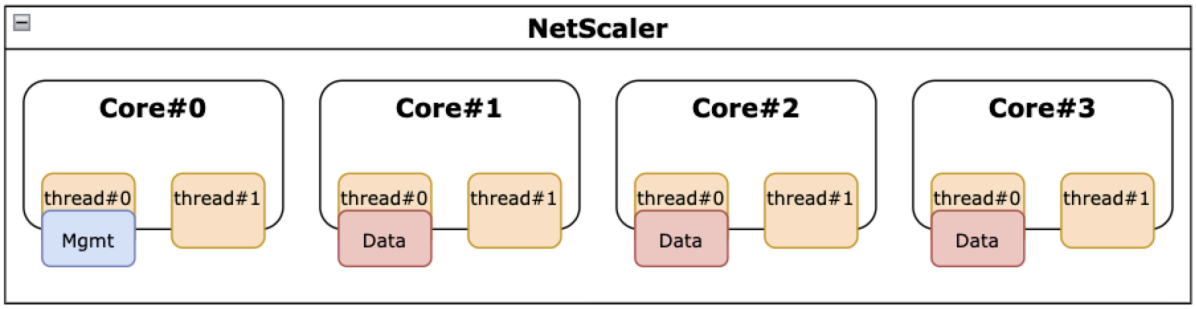
图 1. 内联部署 图 1. 4 核系统上的 NetScaler 管理和数据平面工作负载



虽然上图显示了 NetScaler 功能在可用内核上的分布，但它不一定是对底层硬件的精确描述。大多数现代 x86 CPU 通过商业上称为 Intel Hyperthreading (HT) 或 AMD 同步多线程 (SMT) 的功能为每个物理内核提供两个逻辑内核。

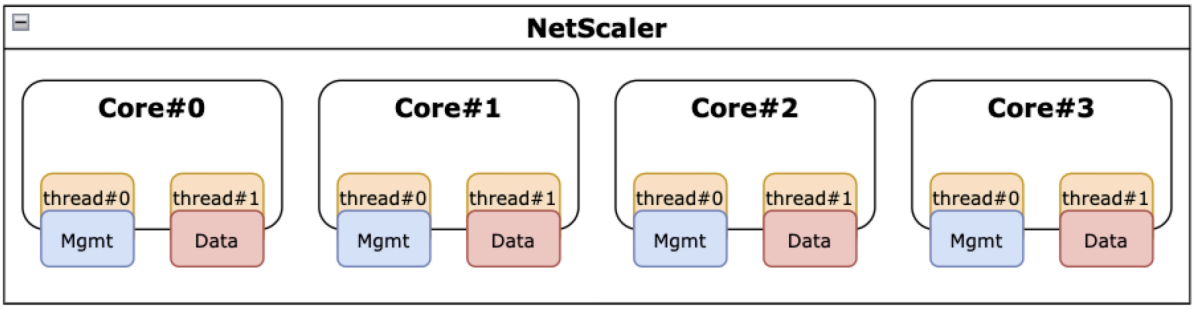
下图显示了 NetScaler VPX 在禁用 SMT 的现代 CPU 上运行。每个 CPU 内核分成两个或更多逻辑 CPU，通常称为线程。每个线程都有自己的一组复制资源、一部分分区资源，并与其兄弟线程争夺共享资源。

图 2. 图 2. 禁用 SMT 的 4 核/8 线程系统上的 NetScaler 管理和数据平面工作负载



下图显示了在启用 SMT 的现代 CPU 上运行的 NetScaler VPX。

图 3. 图 3. 启用 SMT 的 4 核系统上的 NetScaler 管理和数据平面工作负载



启用 SMT 可通过以下方式提高 NetScaler 性能：

- 在所有物理内核上运行数据平面函数。
- 将管理平面函数移至兄弟线程。
- 引入灵活的资源限制机制，以防止管理平面功能损害数据平面功能的性能。

SMT 支持列表

下表列出了支持 SMT 的 VPX 平台、云实例类型和 NetScaler 版本。

VPX 平台	实例类型	NetScaler VPX 版本
—	————	———-
AWS	M5、m5n、c5、c5n	14.1-12.x 及更高版本
Azure	任何具有超线程的实例系列，例如 Ds_v4	14.1-12.x 及更高版本
GCP	e2-instances	14.1-12.x 及更高版本

> 注意：
>
> 通过启用 SMT 功能，NetScaler VPX 在支持类型上的性能得到提高。

限制

SMT 功能实际上将 NetScaler 设备可用的 vCPU 增加了一倍。必须考虑许可限制，以允许 NetScaler 设备使用它们。

例如，以图 3 所示的 NetScaler VPX 为例。如果使用基于吞吐量的许可，则需要具有 SMT 功能的 10 Gbps 或以上的许可证才能启用 8 个 vCPU。以前，1 Gbps 许可证足以启用 4 个 vCPU。如果使用 vCPU 许可，则必须将 NetScaler VPX 配置为签出两倍的 vCPU 数量的许可才能正常运行。有关此主题的进一步指导，请联系 NetScaler 技术支持。

配置 SMT

在启用 SMT 功能之前，请确保您的平台支持此功能。请参阅上一节中的支持列表。

要启用 SMT 功能，请执行以下步骤：

1. 在“/nsconfig”目录下创建一个名为 .smt_handling 的空文件。
2. 保存当前配置。
3. 重启 NetScaler VPX 实例。

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

4. 重新启动后，NetScaler 会指示该功能既可用又已启用。

```
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
```

要禁用 SMT 功能，请执行以下步骤：

1. 删除 .smt_handling 文件。
2. 重启 NetScaler VPX 实例。

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

reboot

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

3. 重新启动后，NetScaler 会指示该功能可用但已禁用。

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

故障排除

运行 sysctl shell 命令以验证 SMT 功能的状态。

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


该命令可以返回以下任何输出。

- 缺少 SMT 功能。

  `sysctl` 命令不返回任何输出。

- 不支持 SMT 功能。

  由于以下任何原因，不支持 SMT 功能：

  - 您的 NetScaler VPX 版本早于 13.1-48.x 或 14.1-12.x。
  - 您的云不支持 SMT。
  - 您的虚拟机实例类型不支持 SMT，例如，vCPU 数量超过 8。

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

- 支持但未启用 SMT 功能。

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

在裸机服务器上安装 **NetScaler VPX** 实例

October 17, 2024

裸机是一个提供物理隔离的完全专用的物理服务器，完全集成到云环境中。它也称为单租户服务器。单一租赁可以避免吵闹的邻居效应 (noisy neighbor effect)。使用裸机时，您不会看到吵闹的邻居效应，因为您是唯一的用户。

随虚拟机管理程序一起安装的裸机服务器为您提供了一个管理套件，用于在服务器上创建虚拟机。虚拟机管理程序不会以本机方式运行应用程序。其目的是将工作负载虚拟化为单独的虚拟机，以获得虚拟化的灵活性和可靠性。

在裸机服务器上安装 **NetScaler VPX** 实例的先决条件

必须从满足相应虚拟机管理程序的所有系统要求的云供应商处获取裸机服务器。

在裸机服务器上安装 **NetScaler VPX** 实例

要在裸机服务器上安装 NetScaler VPX 实例，必须首先从云供应商那里获得具有足够系统资源的裸机服务器。在该裸机服务器上，在部署 NetScaler VPX 实例之前，必须安装和配置任何支持的虚拟机管理程序，例如 Linux KVM、VMware ESX、Citrix Hypervisor 或 Microsoft Hyper-V。

有关 NetScaler VPX 实例上支持的不同虚拟机管理程序和功能列表的更多信息，请参阅 支持矩阵和使用指南。

有关在不同虚拟机管理程序上安装 NetScaler VPX 实例的更多信息，请参阅相应的文档。

- **Citrix Hypervisor**：请参阅 在 Citrix Hypervisor上安装 NetScaler VPX 实例。
- **VMware ESX**：参见 在 VMware ESX上安装 NetScaler VPX 实例。
- **Microsoft Hyper-V**：参见 在 Microsoft Hyper-V 服务器上安装 NetScaler VPX 实例。
- **Linux KVM** 平台：参见 在 Linux-KVM 平台上安装 NetScaler VPX 实例。

在 **Citrix Hypervisor** 上安装 **NetScaler VPX** 实例

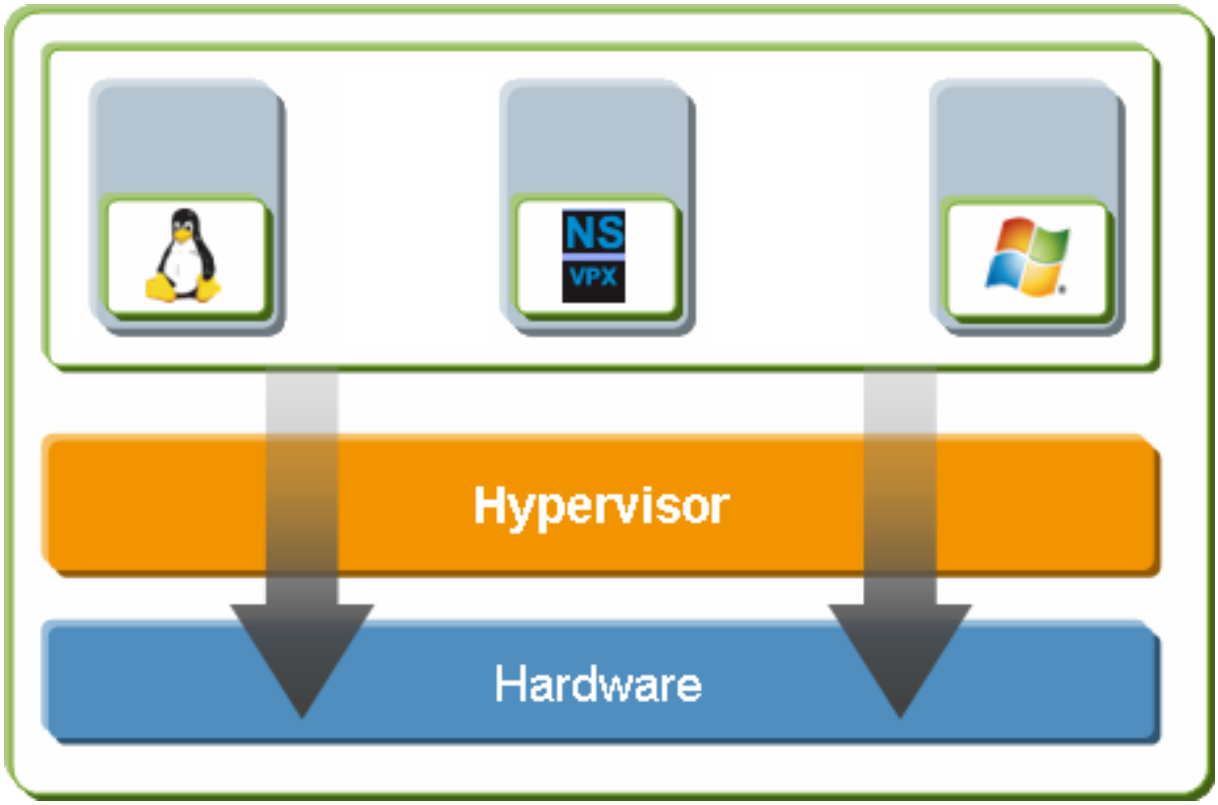
October 17, 2024

要在 Citrix Hypervisor 上安装 VPX 实例，必须首先在具有足够系统资源的计算机上安装虚拟机管理程序。要执行 NetScaler VPX 实例安装，可以使用 Citrix XenCenter，该软件必须安装在能够通过网络连接到虚拟机管理程序主机的远程计算机上。

有关 Hypervisor 的更多信息，请参阅 Citrix Hypervisor 文档。

下图显示了虚拟机管理程序上的 NetScaler VPX 实例的裸机解决方案体系结构。

图。 Citrix Hypervisor 上的 NetScaler VPX 实例



在虚拟机管理程序上安装 **NetScaler VPX** 实例的先决条件

在开始安装虚拟设备之前，请执行以下操作：

- 在满足最低要求的硬件上安装 Hypervisor 6.0 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 XenCenter。
- 获取虚拟设备许可证文件。有关虚拟设备许可证的更多信息，请参阅 NetScaler 许可指南。

虚拟机管理程序硬件要求

下表描述了运行 NetScaler VPX 实例的虚拟机管理程序平台的最低硬件要求。

表 **1**。运行 nCore VPX 实例的虚拟机管理程序的最低系统要求

组件	要求
CPU	两个或更多个启用了虚拟化助手 (Intel-VT) 的 64 位 x86 CPU 要运行 Citrix ADC VPX 实例，必须在 VMware ESX 主机上启用虚拟化硬件支持。两个或更多个启用了虚拟化助手 (Intel-VT) 的 64 位 x86 CPU 要运行 NetScaler VPX 实例，必须在虚拟机管理程序主机上启用虚拟化硬件支持。请确保未禁用用于虚拟化支持的 BIOS 选项。有关更多详细信息，请参阅 BIOS 文档。
RAM	3 GB
磁盘空间	本地连接的存储（PATA、SATA、SCSI）有 40 GB 磁盘空间。注意：虚拟机管理程序安装会为虚拟机管理程序主机控制域创建 4 GB 的分区。剩余的空间可用于 NetScaler VPX 实例和其他虚拟机。
NIC	一个 1-Gbps NIC；建议使用两个 1-Gbps NIC

有关安装 Hypervisor 的信息，请参阅 http://support.citrix.com/product/xens/上的 Hypervisor 文档。

下表列出了虚拟机管理程序必须为每个 nCore VPX 虚拟设备提供的虚拟计算资源。

表 **2**。运行 nCore VPX 实例所需的最低虚拟计算资源

组件	要求
———	—-
内存	2 GB
虚拟 CPU (vCPU)	2
虚拟网络接口	2

> 注意：
>
> 对于 NetScaler VPX 实例的生产用途，Citrix 建议必须将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

XenCenter 系统要求

XenCenter 是一款 Windows 客户端应用程序。它不能与虚拟机管理程序主机在同一台计算机上运行。有关最低系统要求和安装 XenCenter 的详细信息，请参阅以下虚拟机管理程序文档：

- 系统要求
- 安装

使用 **XenCenter** 在 **Hypervisor** 上安装 **NetScaler VPX** 实例

安装并配置虚拟机管理程序和 XenCenter 之后，可以使用 XenCenter 在虚拟机管理程序上安装虚拟设备。可以安装的虚拟设备数目取决于运行虚拟机管理程序的硬件上的可用内存量。

要使用 XenCenter 在 Hypervisor 上安装 NetScaler VPX 实例，请执行以下步骤：

1. 在您的工作站上启动 **XenCenter** 。
2. 在服务器菜单上，单击添加。
3. 在“添加新服务器”对话框的主机名文本框中，键入要连接的虚拟机管理程序的 IP 地址或 DNS 名称。
4. 在“用户名 和 密码”文本框中，键入管理员凭据，然后单击“连接”。该虚拟机管理程序名称将显示在导航窗格中，名称上的绿圈表示已连接虚拟机管理程序。
5. 在导航窗格中，单击要在其上安装 NetScaler VPX 实例的虚拟机管理程序的名称。
6. 在 **VM** 菜单上，单击“导入”。
7. 在“导入”对话框的“导入文件名”中，浏览到保存 NetScaler VPX 实例 `.xva` 映像文件的位置。确保选择“导出的虚拟机”选项，然后单击“下一步”。
8. 选择要在其上安装虚拟设备的虚拟机管理程序，然后单击“下一步”。
9. 选择要在其中存储虚拟设备的本地存储库，然后单击 导入 以开始导入过程。
10. 可以根据需要添加、修改或删除虚拟网络接口。完成后，单击“下一步”。
11. 单击“完成”完成导入过程。

    > 注意：
    >
    > 要查看导入过程的状态，请单击 **Log**（日志）选项卡。

12. 如果要安装其他虚拟设备，请重复步骤 5 到步骤 11。

> 注意：
>
> 初始配置 VPX 实例后，如果要将设备升级到最新的软件版本，请参阅 升级或降级系统软件。

将 **VPX** 实例配置为使用单根 **I/O** 虚拟化 **(SR-IOV)** 网络接口

October 17, 2024

在 Citrix Hypervisor 上安装和配置 NetScaler VPX 实例后，您可以将虚拟设备配置为使用 SR-IOV 网络接口。

支持以下 NIC：

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

限制

Citrix Hypervisor 不支持 SR-IOV 接口上的某些功能。以下各节列出了 Intel 82599、Intel X710 和 Intel XL710 网卡的限制。

Intel 82599 网卡的限制

Intel 82599 网卡不支持以下功能：

- L2 模式切换
- 群集
- 管理分区 [共享 VLAN 模式]
- 高可用性 [主主模式]
- 巨型帧
- 群集环境中的 IPv6 协议

Intel X710 10G 和 **Intel XL710 40G** 网卡的限制

Intel X710 10G 和 Intel XL710 40G 网卡有以下限制：

- 不支持 L2 模式切换。
- 不支持管理员分区（共享 VLAN 模式）。
- 在群集中，XL710 NIC 用作数据接口时，不支持巨型帧。
- 接口断开连接并重新连接时，接口列表会重新排序。
- 不支持速度、双工和自动协商等接口参数配置。
- 对于 Intel X710 10G 和 Intel XL710 40G 网卡，该接口都是 40/x 接口。
- VPX 实例最多只能支持 16 个 Intel X710/XL710 SR-IOV 接口。

> 注意：
>
> 要使 Intel X710 10G 和 Intel XL710 40G NIC 支持 IPv6，请在 Citrix Hypervisor 主机上键入以下命令在虚拟函数 (VF) 上启用信任模式：
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> **Example:**
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```


Intel 82599 网卡的必备条件

在 Citrix Hypervisor 主机上，确保您：

- 向主机中添加 Intel 82599 NIC (NIC)。
- 通过将以下注册表项添加到 **/etc/modprobe.d/blacklist.conf** 文件，将 `ixgbevf` 驱动程序列入阻止列表：

  blacklist ixgbevf
- 通过将以下条目添加到 **/etc/modprobe.d/ixgbe** 文件中，启用 SR-IOV 虚拟功能 (VF)：

  options ixgbe max_vfs=*<number_of_VFs>*

  其中 <*number_VFs*> 为要创建的 SR-IOV VF 的数量。
- 验证是否已在 BIOS 中启用 SR-IOV。

> 注意：
>
> 建议使用 IXGBE 驱动程序版本 3.22.3。

使用 Citrix Hypervisor 主机将 Intel 82599 SR-IOV VF 分配给 NetScaler VPX 实例

要将 Intel 82599 SR-IOV VF 分配给 NetScaler VPX 实例，请按照以下步骤操作：

1. 在 Citrix Hypervisor 主机上，使用以下命令将 SR-IOV VF 分配给 NetScaler VPX 实例：

   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>*

   其中：

   - <*Xen host UUID*> 是 Citrix Hypervisor 主机的 UUID。
   - <*NetScaler VM UUID*> 为 NetScaler VPX 实例的 UUID。
   - <*interface name*> 是 SR-IOV VF 的接口。
   - <*MAC address* > 为 SR-IOV VF 的 MAC 地址。

   > 注意：
   >
   > 指定要在 args:Mac= 参数中使用的 Mac 地址，如果未指定，`iovirt` 脚本将随机生成并分配一个 MAC 地址。此外，如果要在链路聚合模式下使用 SR-IOV VF，请务必将 MAC 地址指定为 00:00:00:00:00:00。

2. 启动 NetScaler VPX 实例。

使用 **Citrix Hypervisor** 主机将 **Intel 82599 SR-IOV VF** 取消分配给 **NetScaler VPX** 实例

如果您分配的 SR-IOV 虚拟文件不正确，或者要修改已分配的 SR-IOV VF，则需要取消分配 SR-IOV 虚拟文件并将其重新分配给 NetScaler VPX 实例。

要取消分配给 NetScaler VPX 实例的 SR-IOV 网络接口，请执行以下步骤：

1. 在 Citrix Hypervisor 主机上，使用以下命令将 SR-IOV VF 分配给 NetScaler VPX 实例并重启 NetScaler VPX 实例：

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

   其中：

   - <*Xen_host_UUID*> - Citrix Hypervisor 主机的 UUID。
   - ** <Netscaler_VM_UUID>-NetScaler VPX 实例的 UUID

2. 启动 NetScaler VPX 实例。

使用 **Citrix Hypervisor** 主机将 **Intel X710/XL710 SR-IOV VF** 分配给 **NetScaler VPX** 实例

要将 Intel X710/XL710 SR-IOV VF 分配给 NetScaler VPX 实例，请按照以下步骤操作：

1. 在 Citrix Hypervisor 主机上运行以下命令来创建网络。

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

   Example:

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

2. 确定要在其上配置 SR-IOV 网络的网卡的 PIF 通用唯一标识符 (UUID)。

   ```
   xe pif-list

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

3. 将网络配置为 SR-IOV 网络。以下命令还会返回新创建的 SR-IOV 网络的 UUID：

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

   Example:


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

要获取有关 SR-IOV 网络参数的详细信息，请运行以下命令：

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

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

4. 创建虚拟接口 (VIF) 并将其连接到目标 VM。

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

> 注意：
>
> 虚拟机的 NIC 索引号必须以 0 开头。

使用以下命令查找虚拟机 UUID：

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

使用 **Citrix Hypervisor** 主机从 **NetScaler** 实例中移除 **Intel X710/XL710 SR-IOV VF**

要从 NetScaler VPX 实例中删除 Intel X710/XL710 SR-IOV VF，请按照以下步骤操作：

1. 复制要销毁的 VIF 的 UUID。
2. 在 Citrix Hypervisor 主机上运行以下命令以销毁 VIF。

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

Example:

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


在 **SR-IOV** 接口上配置链路聚合

要在链路聚合模式下使用 SR-IOV 虚拟函数 (VF)，您需要禁用对已创建的虚拟函数的欺骗检查。

在 Citrix Hypervisor 主机上，使用以下命令禁用欺骗检查：

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

其中：

- <interface_name> 为接口名称。
- <VF_id> 为虚拟功能 ID。

对您创建的所有虚拟功能禁用欺骗检查后，重新启动 NetScaler VPX 实例，然后配置链接聚合。有关说明，请参阅 配置链路聚合。

> 重要：
>
> 在将 SR-IOV VF 分配给 NetScaler VPX 实例时，请务必为 VF 指定 MAC 地址 00:00:00:00:00:00。

在 **SR-IOV** 接口上配置 **VLAN**

您可以在 SR-IOV 虚拟功能上配置 VLAN。有关说明，请参阅配置 VLAN。

> 重要：
>
> 确保 Citrix Hypervisor 主机不包含 VF 接口的 VLAN 设置。

在 **VMware ESX** 上安装 **NetScaler VPX** 实例

October 17, 2024

在 VMware ESX 上安装 NetScaler VPX 实例之前，请确保 VMware ESX Server 安装在具有足够系统资源的计算机上。要在 VMware ESXi 上安装 NetScaler VPX 实例，请使用 VMware vSphere 客户端。该客户端或工具必须安装在可通过网络连接到 VMware ESX 的远程计算机上。

本节包括以下主题：

- 必备条件
- 在 VMware ESX 上安装 NetScaler VPX 实例

> 重要：
>
> 您无法安装标准 VMware Tools 或升级 NetScaler VPX 实例上可用的 VMware Tools 版本。适用于 NetScaler VPX 实例的 VMware Tools 作为 NetScaler 软件版本的一部分提供。

必备条件

在开始安装虚拟设备之前，请执行以下操作：

- 在满足最低要求的硬件上安装 VMware ESX。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 下载 NetScaler VPX 设备安装文件。
- 创建虚拟交换机并将物理 NIC 连接到虚拟交换机。
- 添加端口组并连接到虚拟交换机。
- 将端口组连接到 VM。
- 获取 VPX 许可证文件。有关 NetScaler VPX 实例许可证的更多信息，请参阅 许可概述。

VMware ESX 硬件要求

下表描述了运行 NetScaler VPX nCore 虚拟设备的 VMware ESX 服务器的最低系统要求。

表 1. VPX 功能列表 表 1. 运行 NetScaler VPX 实例的 VMware ESX 服务器的最低系统要求

组件	要求
CPU	两个或更多个启用了虚拟化助手 (Intel-VT) 的 64 位 x86 CPU 要运行 Citrix ADC VPX 实例，必须在 VMware ESX 主机上启用虚拟化硬件支持。两个或更多个启用了虚拟化助手 (Intel-VT) 的 64 位 x86 CPU 要运行 NetScaler VPX 实例，必须在 VMware ESX 主机上启用虚拟化硬件支持。确保未禁用用于虚拟化支持的 BIOS 选项。有关详细信息，请参阅 BIOS 文档。从 NetScaler 13.1 版本起，VMware ESXi 虚拟机管理程序上的 NetScaler VPX 实例支持 AMD 处理器。
RAM	2 GB VPX。对于关键部署，我们不建议对 VPX 使用 2 GB RAM，因为系统在内存受限的环境中运行。这可能会导致与规模、性能或稳定性相关的问题。建议使用 4 GB RAM 或 8 GB RAM。
磁盘空间	比 VMware 为设置 ESXi 提供的最低服务器要求多 20 GB。有关最低服务器要求，请参阅 VMware 文档。
网络	一个 1-Gbps NIC (NIC)；推荐使用两个 1-Gbps NIC

有关安装 VMware ESX 的信息，请参阅 http://www.vmware.com/。

要支持 SR-IOV 网络接口或 PCI 直通功能，请确保启用以下处理器和设置：

- 支持 Intel-VT 的 Intel 处理器

- 支持 AMD-V 的 AMD 处理器
- 在 BIOS 中启用 I/O 内存管理单元 (IOMMU) 或 SR-IOV

SR-IOV 模式支持以下 NIC：

- Mellanox ConnectX-4 NIC，从 NetScaler 版本 13.1-42.x 起开始
- Intel 82599 NIC

下表列出了 VMware ESX 服务器必须为每个 VPX nCore 虚拟设备提供的虚拟计算资源。

表 2. VPX 功能列表 表 2. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

组件	要求
———-	———————————–
内存	4 GB
虚拟 CPU (vCPU)	2
虚拟网络接口	在 ESX 中，如果 VPX 硬件升级到版本 7 或更高版本，您最多可以安装 10 个虚拟网络接口。
磁盘空间	20 GB

> 注意：
>
> 这是对虚拟机管理程序的磁盘要求的补充。

要在生产中使用 VPX 虚拟设备，必须保留完整的内存分配。必须保留至少等于 ESX 的一个 CPU 内核速度的 CPU 周期 (MHz)。

VMware vSphere Client 系统要求

VMware vSphere 是可在 Windows 和 Linux 操作系统上运行的客户端应用程序。它无法与 VMware ESX 服务器在同一台计算机上运行。下表说明了最低系统要求。

表 3. 参数值 表 3. 安装 VMware vSphere Client 的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 http://kb.vmware.com/ 上搜索“vSphere Compatibility Matrixes”（vSphere 兼容性表）PDF 文件。
CPU	750 MHz；建议使用 1 GHz 或速度更高的 CPU
RAM	1 GB. 建议 2 GB
NIC (NIC)	100 Mbps 或速度更高的 NIC

OVF Tool 1.0 系统要求

OVF 工具是可在 Windows 和 Linux 操作系统上运行的客户端应用程序。它无法与 VMware ESX 服务器在同一台计算机上运行。下表说明了最低系统要求。

表 4. VPX 功能列表 表 4. 安装 OVF 工具的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。
CPU	最低 750 MHz，建议使用 1 GHz 或速度更快的 CPU
RAM	最低 1 GB；建议使用 2 GB
NIC (NIC)	100 Mbps 或速度更高的 NIC

有关安装 OVF 的信息，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。

下载 **NetScaler VPX** 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例设置包遵循开放虚拟机 (OVF) 格式标准。可以从 Citrix Web 站点下载文件。需要使用 Citrix 帐户进行登录。如果您没有 Citrix 帐户，请访问主页 http://www.citrix.com，单击 新用户链接，然后按照说明创建 Citrix 帐户。

登录后，从 Citrix 主页浏览以下路径：

Citrix.com > 下载 **> NetScaler >** 虚拟设备。

将以下文件复制到 ESX 服务器所在网络中的一个工作站。将所有三个文件复制到同一个文件夹中。

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

在 **VMware ESX** 上安装 **NetScaler VPX** 实例

安装并配置 VMware ESX 后，可以使用 VMware vSphere Client 在 VMware ESX 服务器上安装虚拟设备。可以安装的虚拟设备数目取决于运行 VMware ESX 的硬件上的可用内存量。

要使用 VMware vSphere Client 在 VMware ESX 上安装 NetScaler VPX 实例，请执行以下步骤：

1. 在工作站上启动 VMware vSphere Client。
2. 在 **IP address / Name**（IP 地址/名称）文本框中，键入要连接到的 VMware ESX 服务器的 IP 地址。
3. 在 **User Name**（用户名）和 **Password**（密码）文本框中，键入管理员凭据，然后单击“Login”（登录）。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在部署 **OVF** 模板对话框的从文件部署中，浏览到保存 NetScaler VPX 实例安装文件的位置，选择.ovf 文件，然后单击下一步。
6. 将虚拟设备 OVF 模板中显示的网络映射到在 ESX 主机上配置的网络。单击 **Next**（下一步）开始在 VMware ESX 上安装虚拟设备。安装完成时，将显示一个弹出窗口，通知您安装成功。
7. 现在，您可以启动 NetScaler VPX 实例。在导航窗格中，选择已安装的 NetScaler VPX 实例，然后从右键单击菜单中选择开机。
8. 虚拟机启动后，从控制台配置 NetScaler IP、网络掩码和网关地址。完成配置后，在控制台中选择“保存并退出”选项。
9. 要安装其他虚拟设备，请从步骤 6 到步骤 8 重复操作。

> 注意：
>
> 默认情况下，NetScaler VPX 实例使用 E1000 网络接口。
>
> 安装完成后，您可以使用 vSphere 客户端或 vSphere Web Client 来管理 VMware ESX 上的虚拟设备。
>
> 要在 VMware ESX 上启用 VLAN 标记，请在 vSwitch 上将端口组的 VLAN ID 配置为全部 (4095)。有关在 vSwitch 上设置 VLAN ID 的详细说明，请参阅 VMware 文档。

使用 **VMware vMotion** 迁移 **NetScaler VPX** 实例

您可以使用 VMware vSphere vMotion 迁移 NetScaler VPX 实例。

请按照以下使用准则进行操作：

- VMware 不支持配置了 PCI 直通和 SR-IOV 接口的虚拟机上的 vMotion 功能。
- 支持的接口包括 E1000 和 VMXNET3。要在 VPX 实例上使用 vMotion，请确保实例配置了受支持的接口。
- 有关如何使用 VMware vMotion 迁移实例的详细信息，请参阅 VMware 文档。

将 **NetScaler VPX** 实例配置为使用 **VMXNET3** 网络接口

October 17, 2024

在 VMware ESX 上安装和配置 NetScaler VPX 实例后，您可以使用 VMware vSphere Web 客户端将虚拟设备配置为使用 VMXNET3 网络接口。

要使用 VMware vSphere Web Client 将 NetScaler VPX 实例配置为使用 VMXNET3 网络接口，请执行以下操作：

1. 在 vSphere Web Client 中，选择“Hosts and Clusters”（主机和群集）。

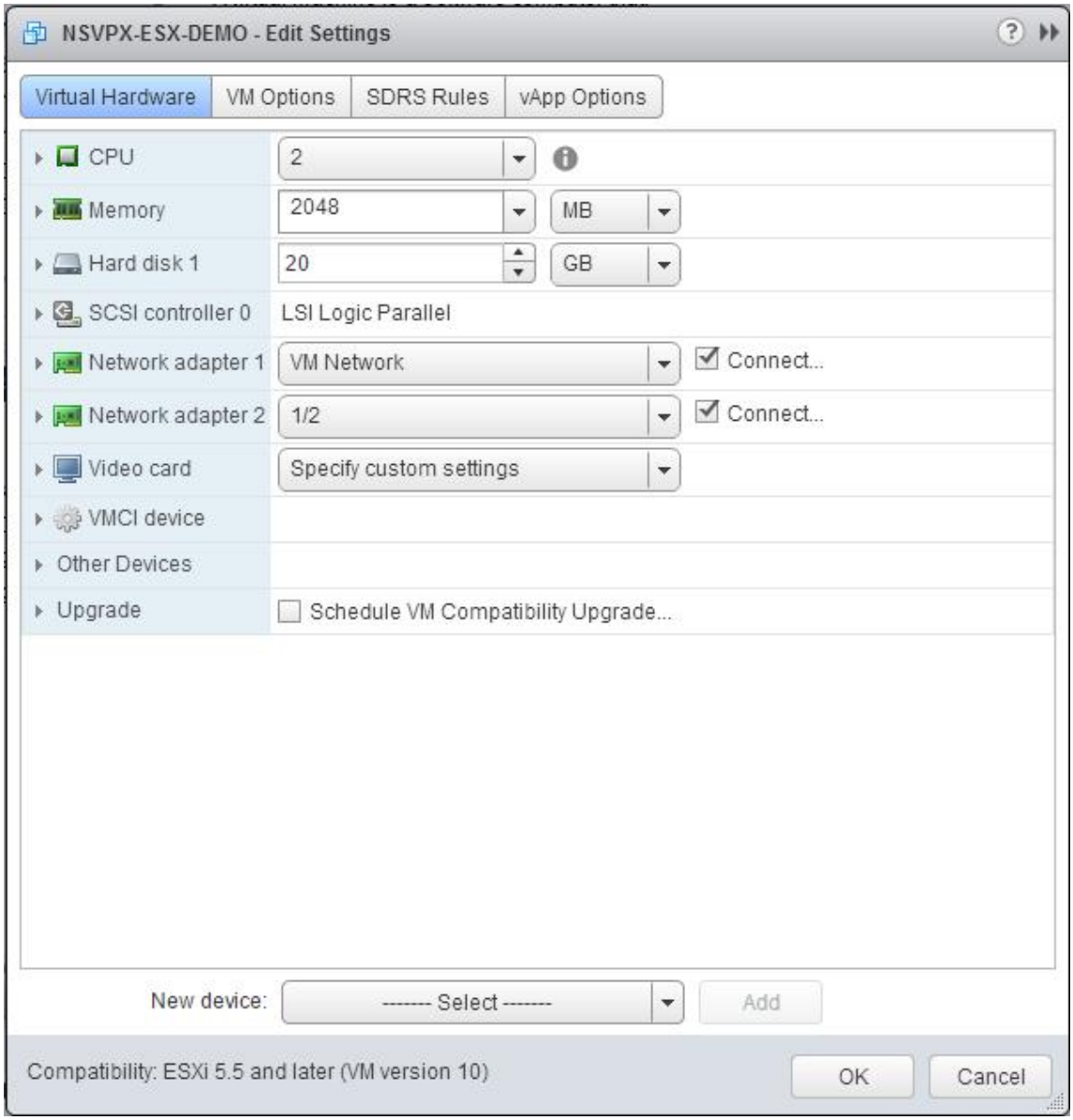
2. 将 NetScaler VPX 实例的兼容性设置升级到 ESX，如下所示：

   a。关闭 NetScaler VPX 实例的电源。

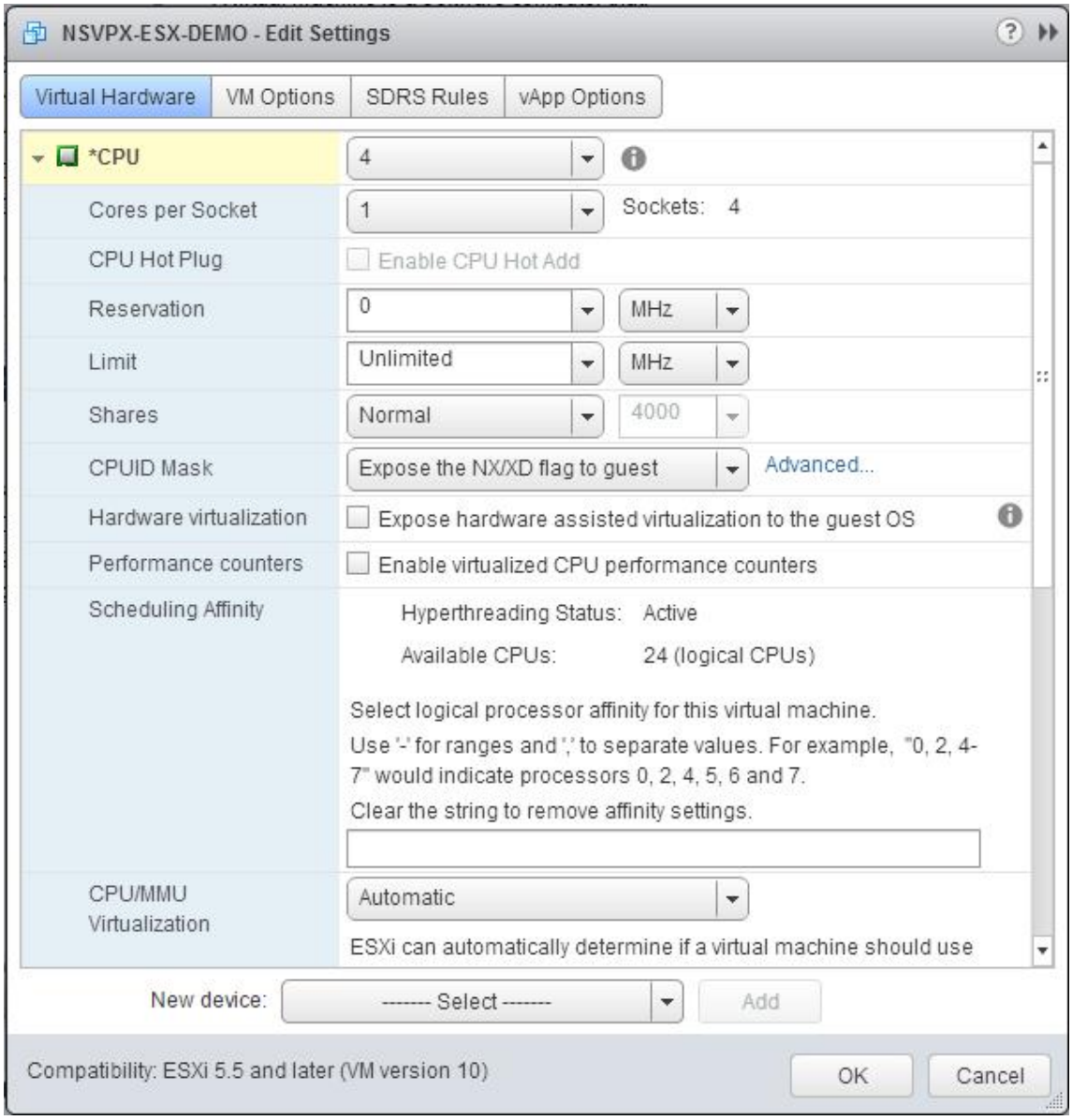
   a。在“Adapter Type”（适配器类型）下拉列表中，选择“VMXNET3”。

   a。在“CPU”下拉列表中，选择要分配给虚拟设备的 CPU 数量。

3. 右键单击 NetScaler VPX 实例，然后单击“编辑设置”。



4. 在“<virtual_appliance> - Edit Settings”（<virtual_appliance> - 编辑设置）对话框中，单击“CPU”部分。



5. 在“CPU”部分中，更新以下设置：

   - CPU 数量
   - 插槽数量
   - 预订
   - 限制
   - 共享数

   请按如下所示设置各个值：

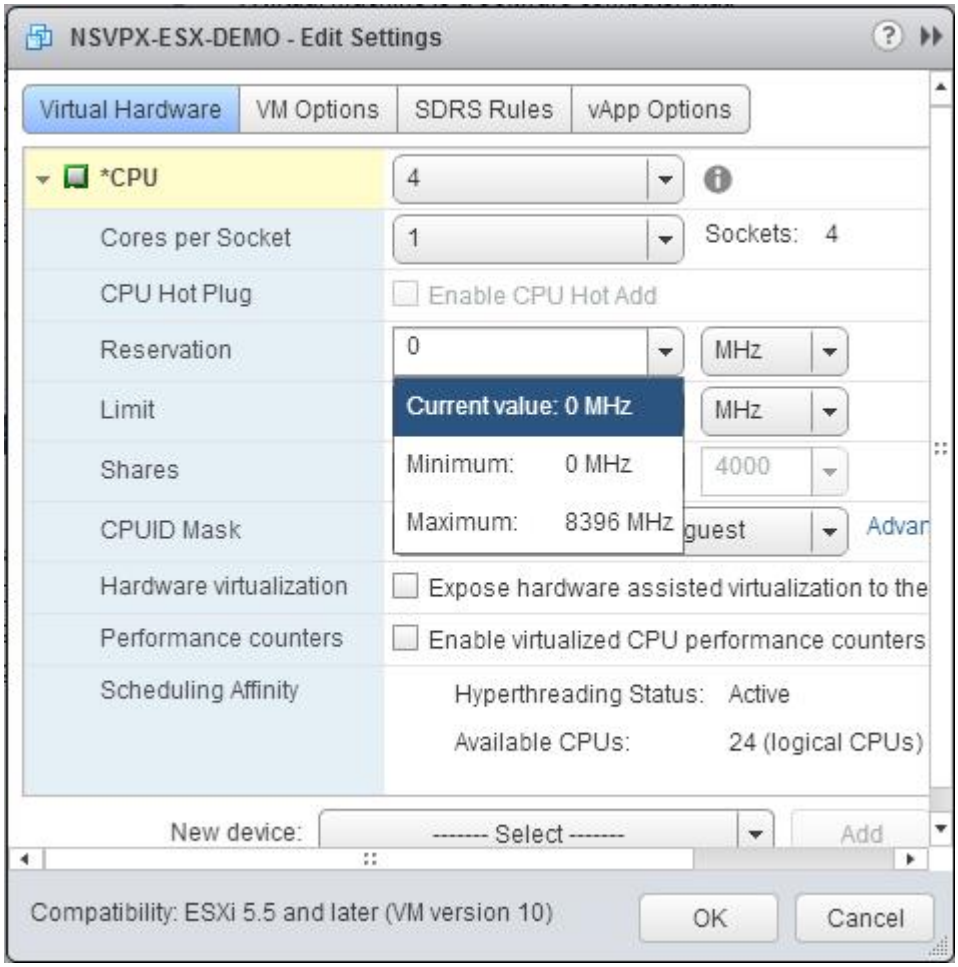
   a。a. 在“CPU”下拉列表中，选择要分配给虚拟设备的 CPU 数量。

   a。b. 在“Cores per Socket”（每个插槽的核心数）下拉列表中，选择插槽数量。

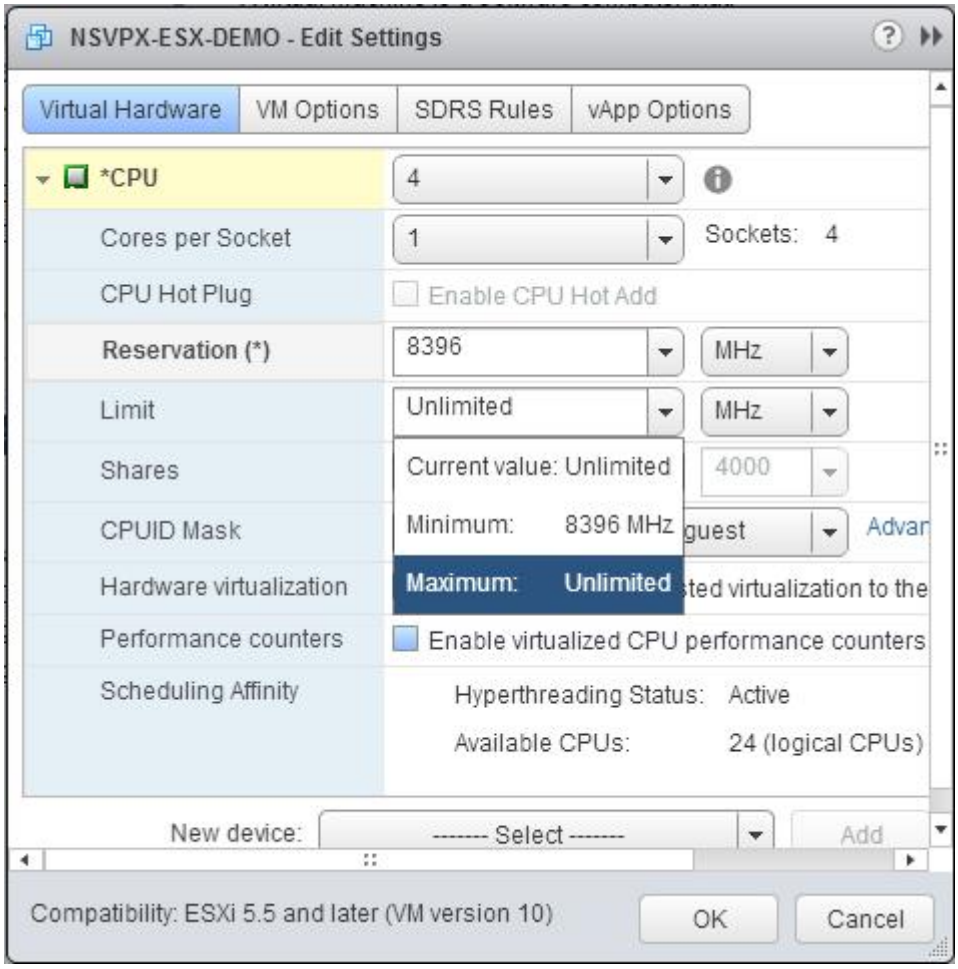
a。c. （可选）在“CPU Hot Plug”（CPU 热插拔）字段中，选中或取消选中“Enable CPU Hot Add”（启用 CPU 热添加）复选框。

> 注意：
>
> Citrix 建议接受默认设置（禁用）。

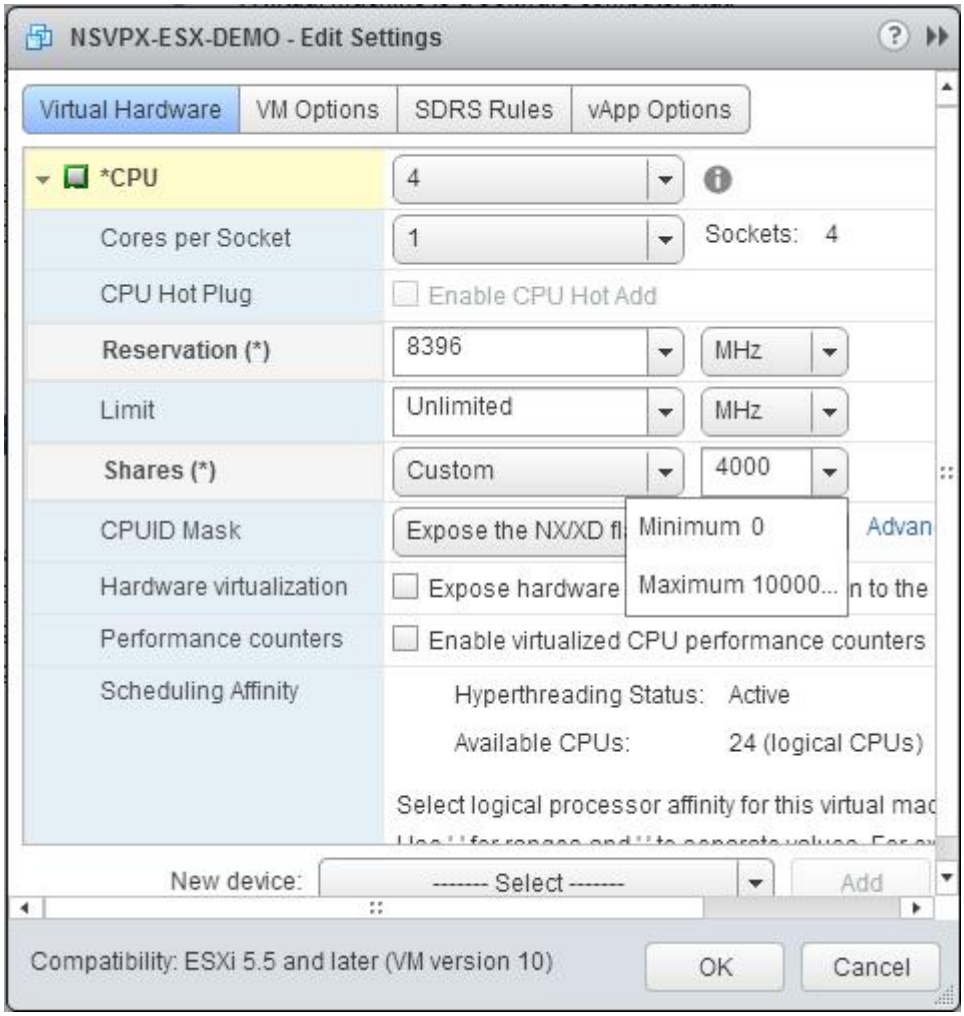
d. d. 在“Reservation”（预留）下拉列表中，选择将显示为最大值的数字。



e. e. 在“Limit”（限制）下拉列表中，选择将显示为最大值的数字。



f. f. 在“Shares”（共享）下拉列表中，选择“Custom”（自定义）以及将显示为最大值的数字。



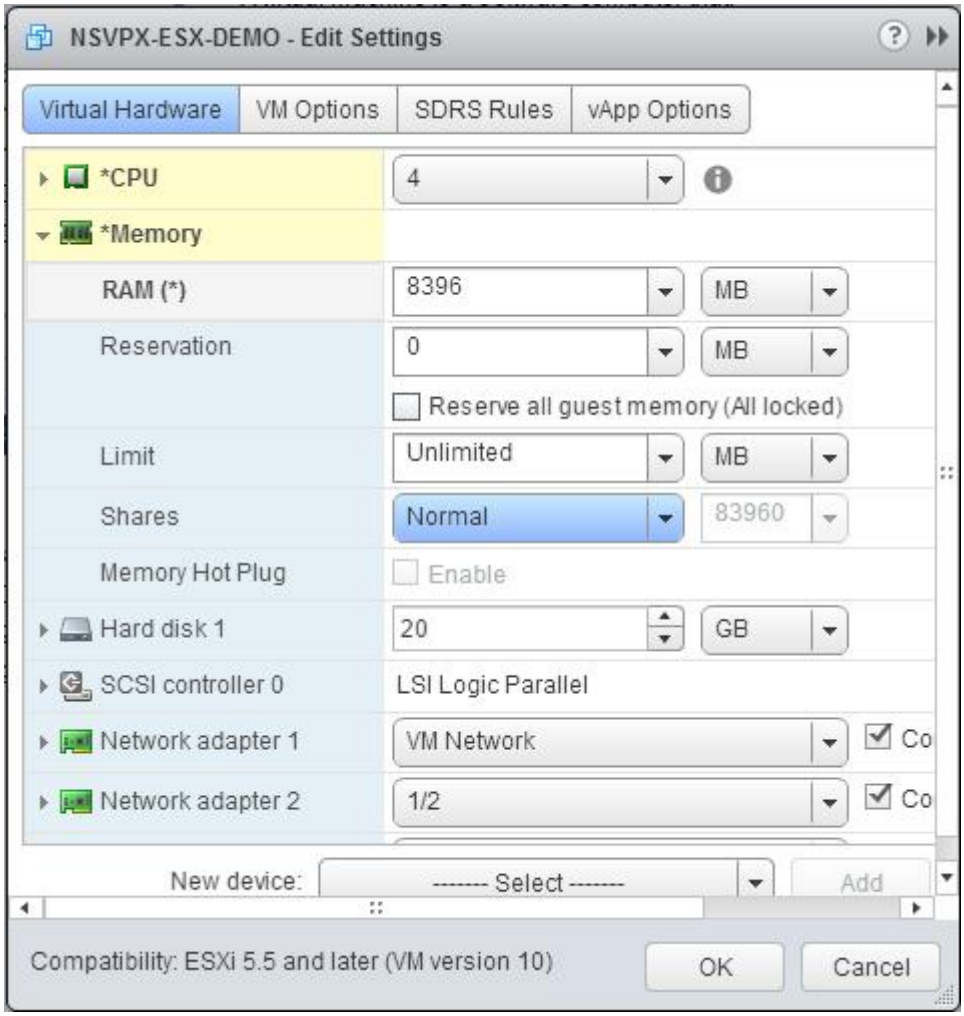
6. 在“Memory”（内存）部分中，更新以下设置：

   - RAM 大小
   - 预订
   - 限制
   - 共享数

   请按如下所示设置各个值：

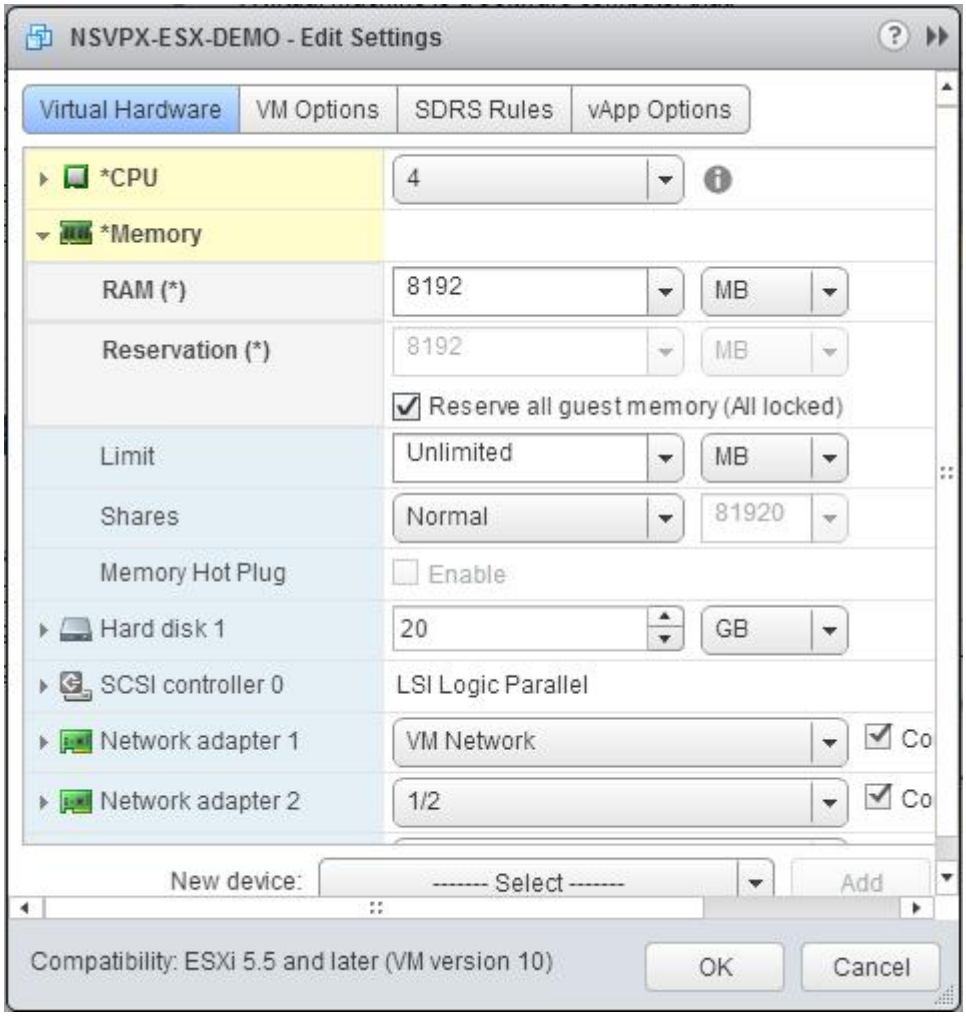
   a。在“RAM”下拉列表中，选择 RAM 的大小。必须为 vCPU 数 x 2 GB。例如，如果 vCPU 数为 4，则 RAM 必须为 4 x 2 GB = 8 GB。

   > 注意：
   >
   > 对于 NetScaler VPX 设备的高级版或优质版，请确保为每个 vCPU 分配 4 GB 的 RAM。例如，如果 vCPU 数为 4，则 RAM 为 4 x 4 GB =16 GB。

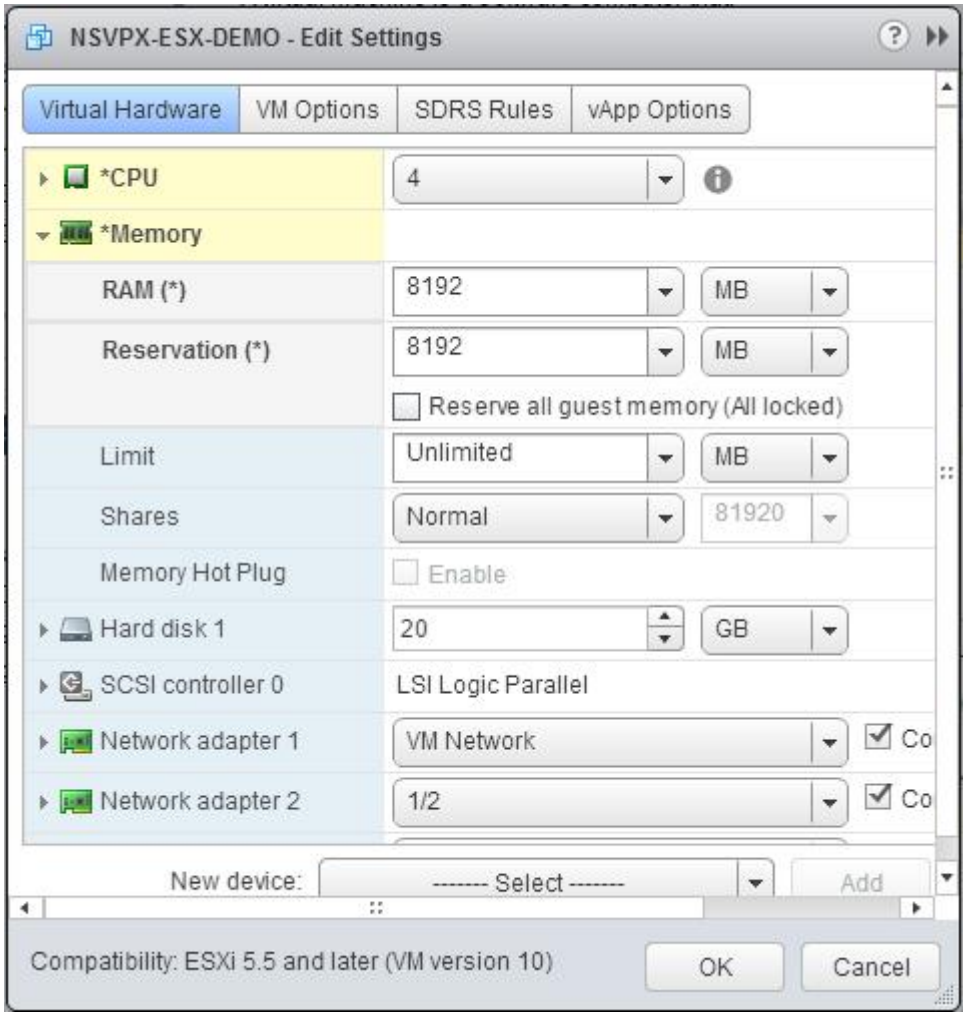


a。b. 在 Reservation（预留）下拉列表中，输入内存预留值，然后选中 Reserve all guest memory (All locked)（预留所有来宾内存 (全部锁定)）复选框。内存预留量必须为 vCPU 数 × 2 GB。例如，如果 vCPU 数为 4，则内存预留量必须为 4 x 2 GB = 8 GB。

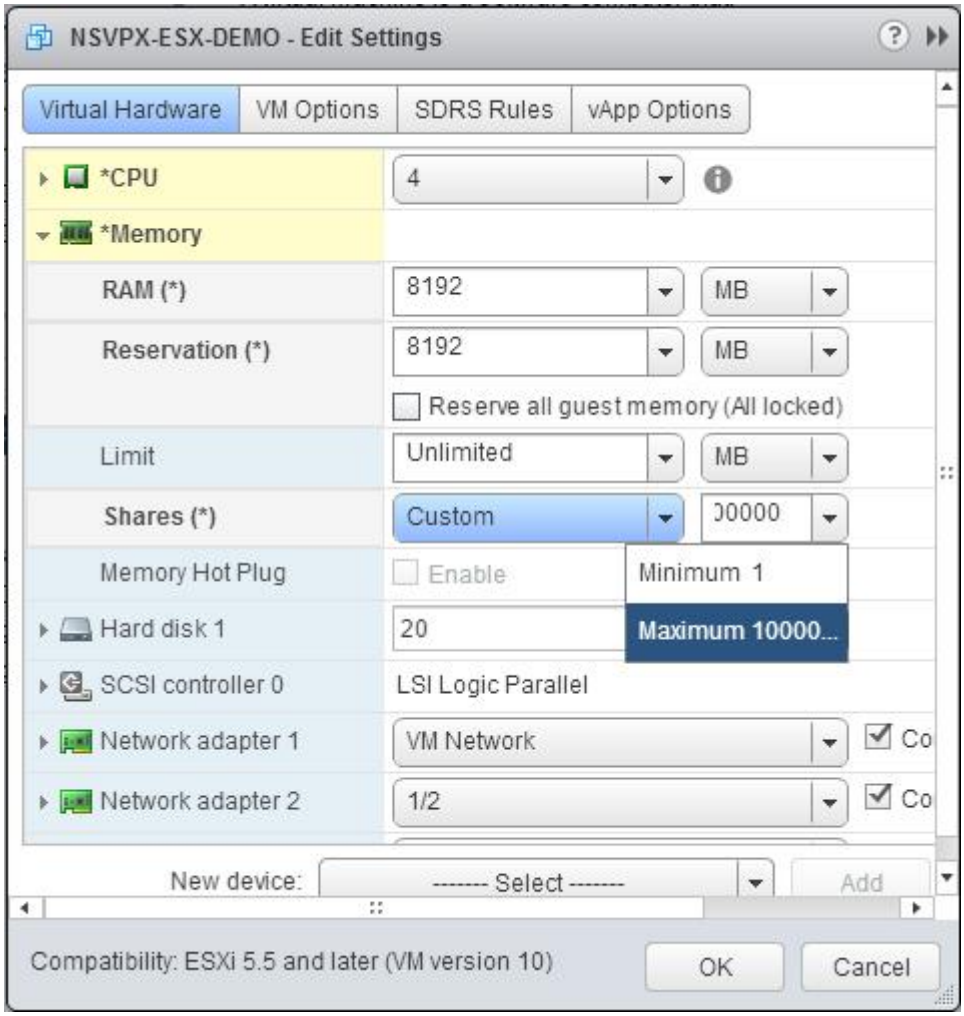
> 注意：
>
> 对于 NetScaler VPX 设备的高级版或优质版，请确保为每个 vCPU 分配 4 GB 的 RAM。例如，如果 vCPU 数为 4，则 RAM 为 4 x 4 GB =16 GB。



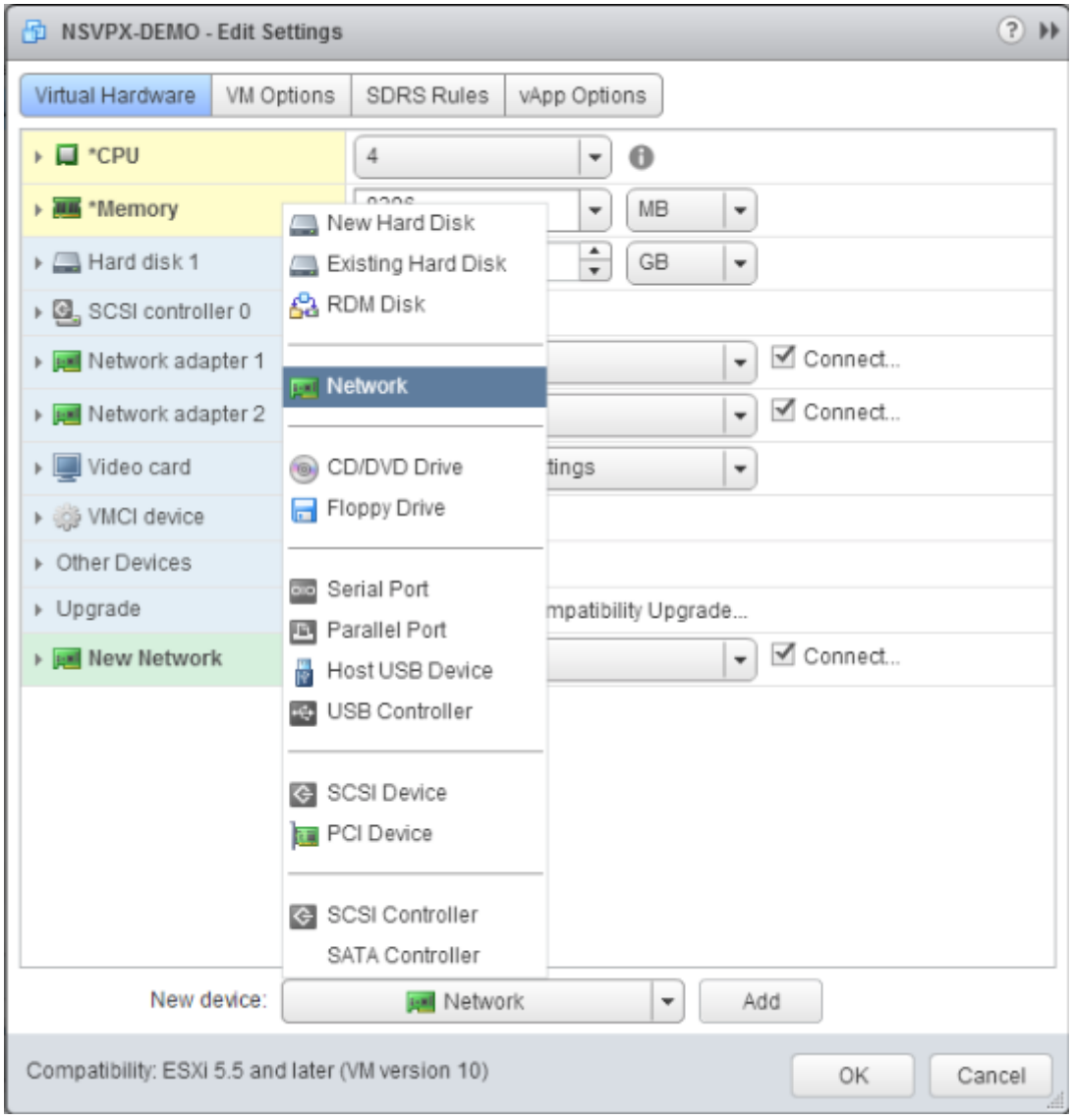
a。e. 在“Limit”（限制）下拉列表中，选择将显示为最大值的数字。



d. f. 在“Shares”（共享）下拉列表中，选择“Custom”（自定义）以及将显示为最大值的数字。



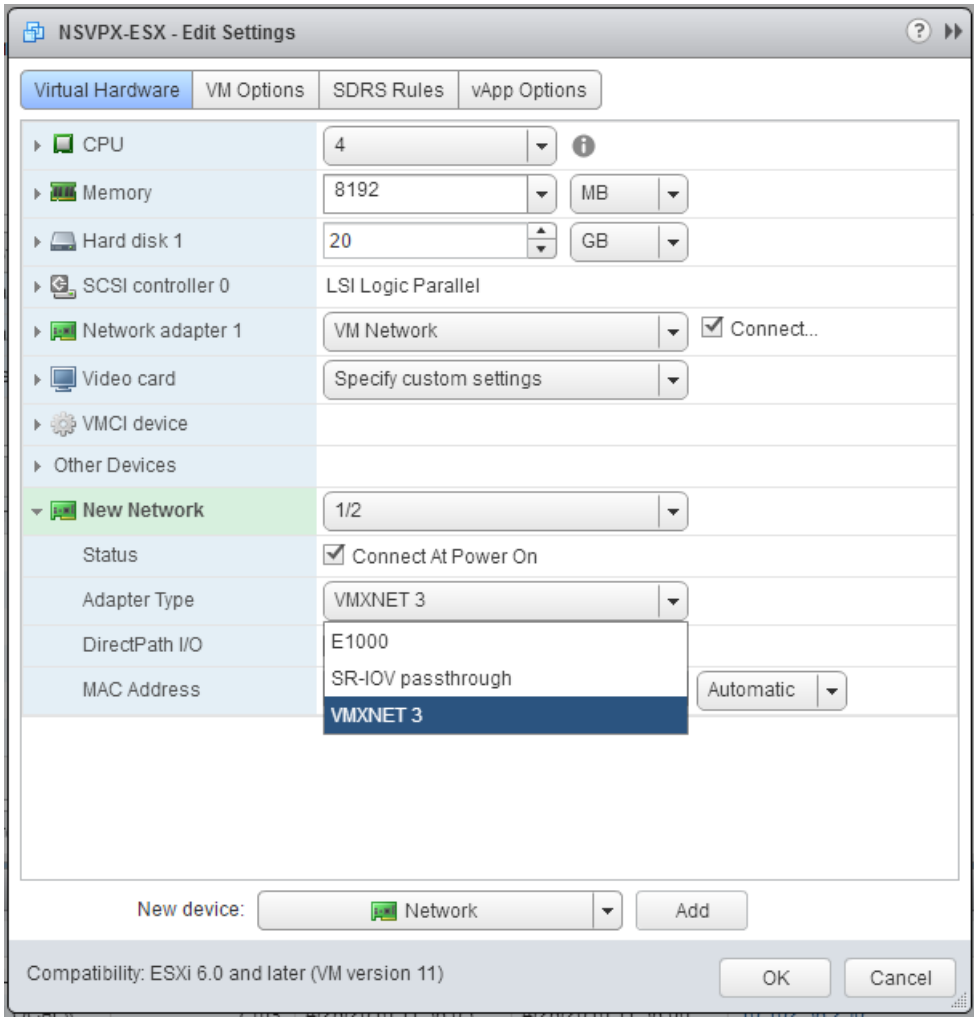
7. 添加 VMXNET3 网络接口。从“New device”（新建设备）下拉列表中，选择“Network”（网络），然后单击“Add”（添加）。



8. 在“New Network”（新建网络）部分中的下拉列表中选择网络接口，然后执行以下操作：

   a。a. 在“Adapter Type”（适配器类型）下拉列表中，选择“VMXNET3”。

   > 重要：
   >
   > 默认 E1000 网络接口无法与 VMXNET3 共存，请务必删除 E1000 网络接口，并使用 VMXNET3 (0/1) 作为管理接口。



9. 单击确定。
10. 打开 NetScaler VPX 实例的电源。
11. NetScaler VPX 实例启动后，您可以使用以下命令来验证配置：

    显示接口摘要

输出内容必须显示您已配置的所有接口：

```
> show interface summary
-------------------------------------------------------------------------------

      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------

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

> 注意：
>
> 添加 VMXNET3 接口并重新启动 NetScaler VPX 设备后，VMware ESX 虚拟机管理程序可能会更改 NIC 向 VPX 设备呈现的顺序。因此，网络适配器 1 可能并不始终保持 0/1，导致与 VPX 设备的管理连接断开。要避免出现此问题，请相应地更改网络适配器的虚拟网络。
>
> 这是 VMware ESX 虚拟机管理程序限制。

为 **VMXNET3** 网络接口设置接收环大小

您可以增加 VMware ESX 上 VMXNET3 网络接口的接收环大小。当流量突然爆发时，较高的环路大小可以减少数据包丢失的次数。

> 注意：
>
> 此功能在 14.1 版本 14.x 及更高版本中可用。

在 **VMXNET3** 网络接口上设置环路大小

在命令提示符下，键入：

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

您可以在 VMXNET3 接口上设置的最大振铃大小为 2048。仅支持固定环类型。要使设置生效，必须保存配置并重启 NetScaler VPX 实例。

将 **NetScaler VPX** 实例配置为使用 **SR-IOV** 网络接口

October 17, 2024

在 VMware ESX 上安装和配置 NetScaler VPX 实例后，您可以使用 VMware vSphere Web 客户端将虚拟设备配置为使用单根 I/O v 虚拟化 (SR-IOV) 网络接口。

限制

配置了 SR-IOV 网络接口的 NetScaler VPX 具有以下限制：

- 在 ESX VPX 上，以下功能在使用 Intel 82599 10G NIC 的 SR-IOV 接口上不受支持：
  - L2 模式切换

  - 静态链路聚合和 LACP
  - 群集
  - 管理分区 [共享 VLAN 模式]
  - 高可用性 [主主模式]
  - 巨型帧
  - IPv6

- 在 KVM VPX 上，以下功能在使用 Intel 82599 10G NIC 的 SR-IOV 接口上不受支持：

  - 静态链路聚合和 LACP
  - L2 模式切换
  - 群集
  - 管理分区 [共享 VLAN 模式]
  - 高可用性 [主动-主动模式]
  - 巨型帧
  - IPv6
  - 不支持通过 `ip link` 命令在适用于 SR-IOV VF 接口的虚拟机管理程序上对 VLAN 所做的配置。

必备条件

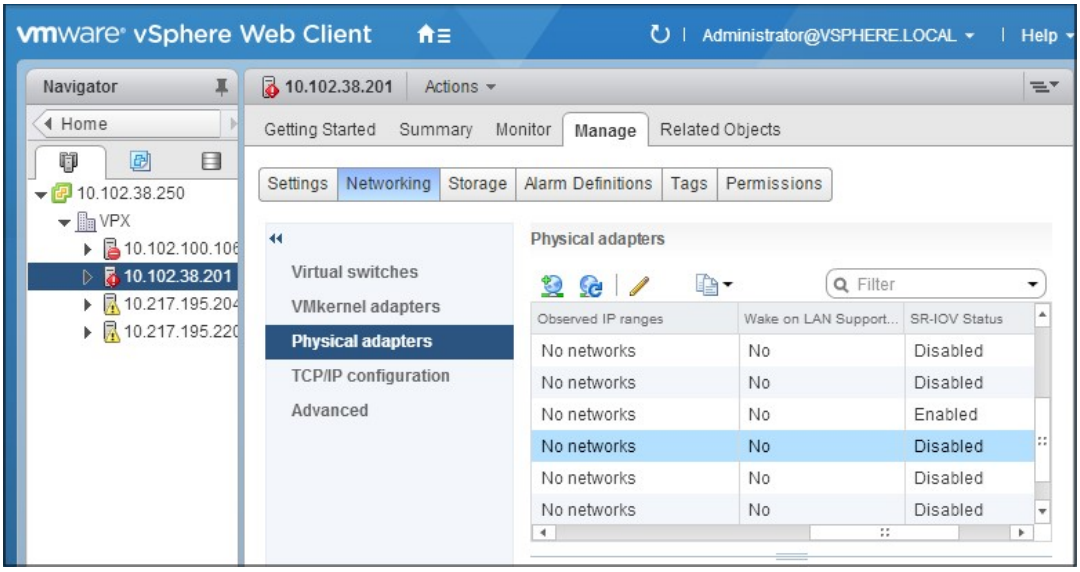
- 确保将以下任何 NIC 添加到 ESX 主机：

  - 推荐使用 Intel 82599 NIC、IXGBE 驱动程序版本 3.7.13.7.14iov 或更高版本。
  - Mellanox ConnectX-4 NIC

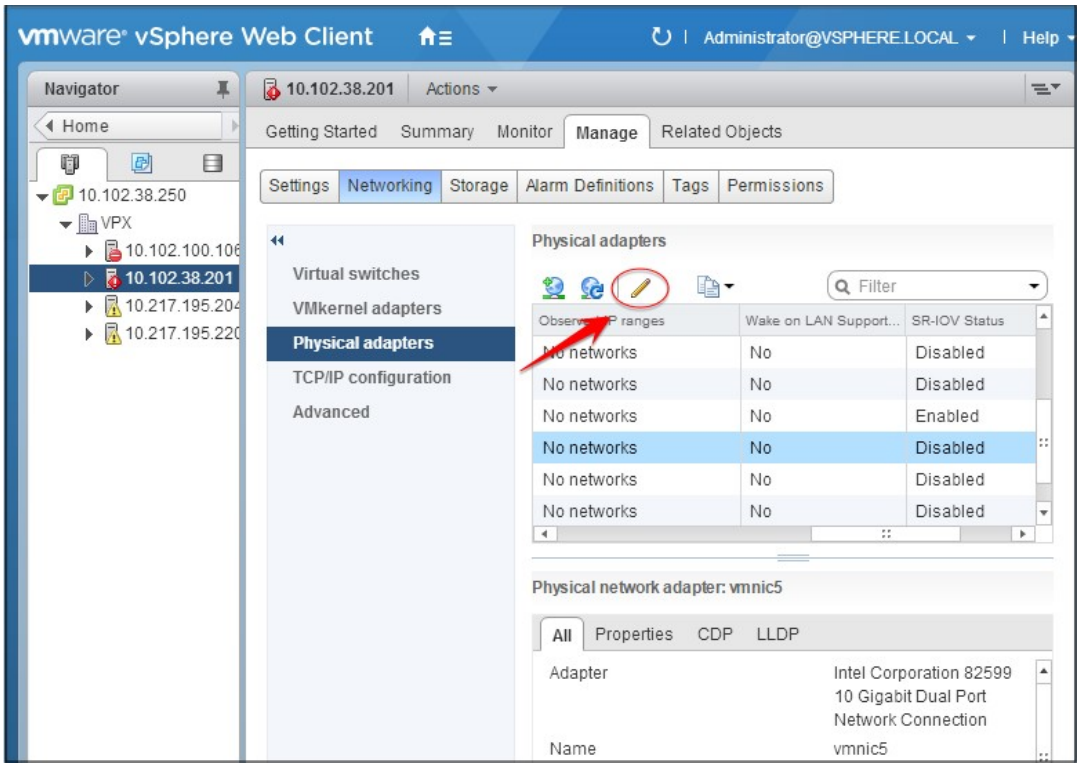
- 在主机物理适配器上启用 SR-IOV。

  按照以下步骤在主机物理适配器上启用 SR-IOV：

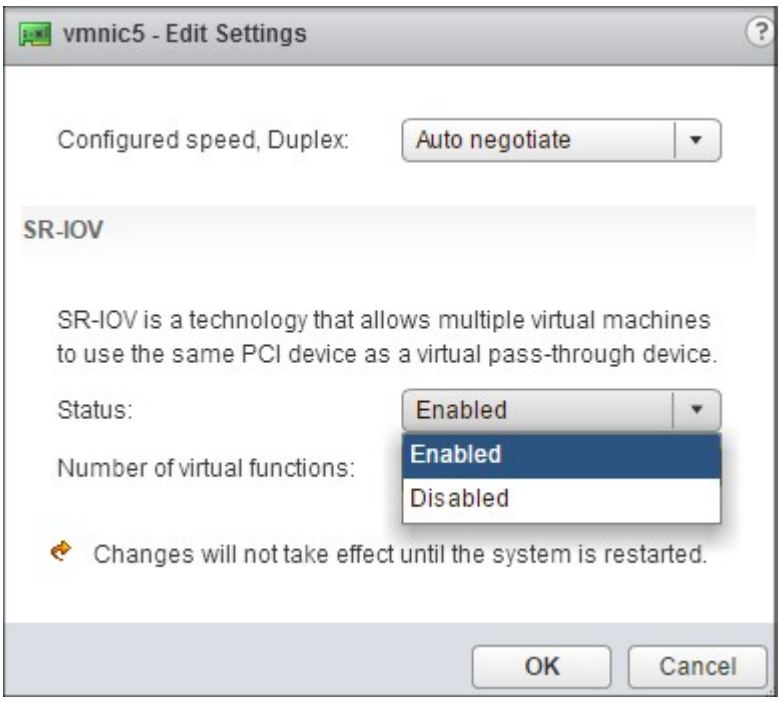
  1. 在 vSphere Web Client 中，导航到“主机”。
  2. 在 **Manage**（管理）**> Networking**（网络连接）选项卡中，选择 **Physical adapters**（物理适配器）。“SR-IOV Status”（SR-IOV 状态）字段将显示物理适配器是否支持 SR-IOV。



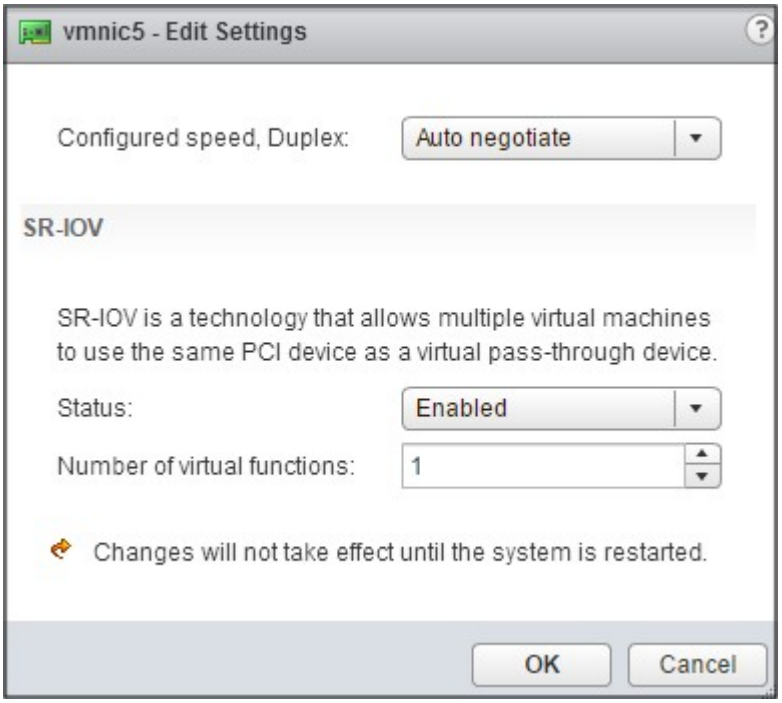
3. 选择物理适配器，然后单击铅笔图标以打开 **Edit Settings**（编辑设置）对话框。



4. 在“SR-IOV”下，从 **Status**（状态）下拉列表中选择 **Enabled**（已启用）。



5. 在 **Number of virtual functions**（虚拟功能数）字段中，输入要为适配器配置的虚拟功能的数量。



6. 单击确定。
7. 重新启动 主机。

- 创建分布式虚拟交换机 (DVS) 和Portgroups。有关说明，请参阅 VMware 文档。

> 注意：
>
> Citrix 仅有资格在 DVS 和Portgroups上配置 SR-IOV。

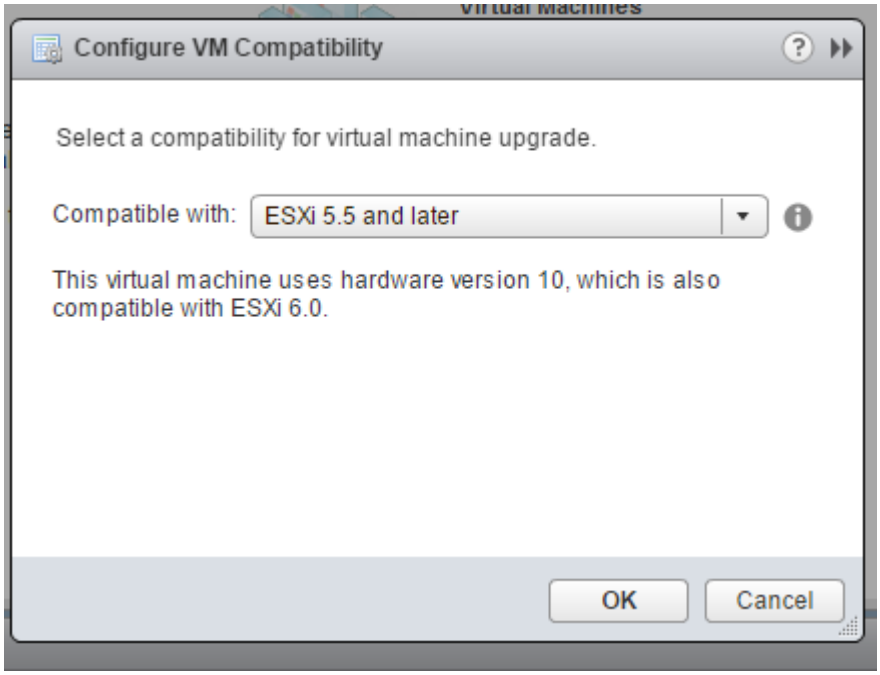
要使用 **VMware vSphere Web Client** 将 **NetScaler VPX** 实例配置为使用 **SR-IOV** 网络接口，请执行以下操作：

1. 在 vSphere Web Client 中，选择 主机和群集。
2. 将 NetScaler VPX 实例的兼容性设置升级到 ESX 5.5 或更高版本，如下所示：

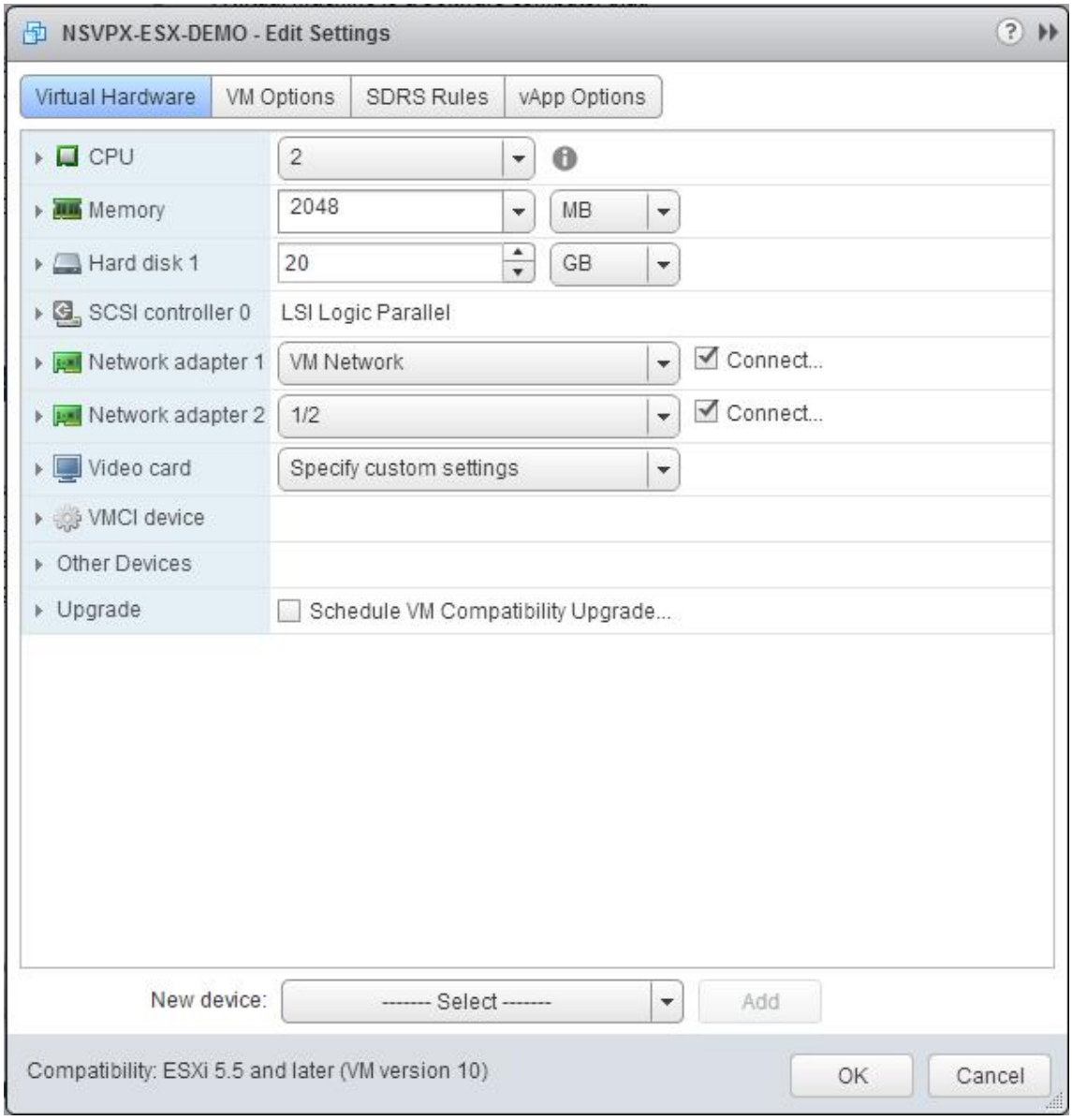
   a。关闭 NetScaler VPX 实例的电源。

   a。b. 右键单击 NetScaler VPX 实例，然后选择 兼容性 **>** 升级虚拟机兼容性。

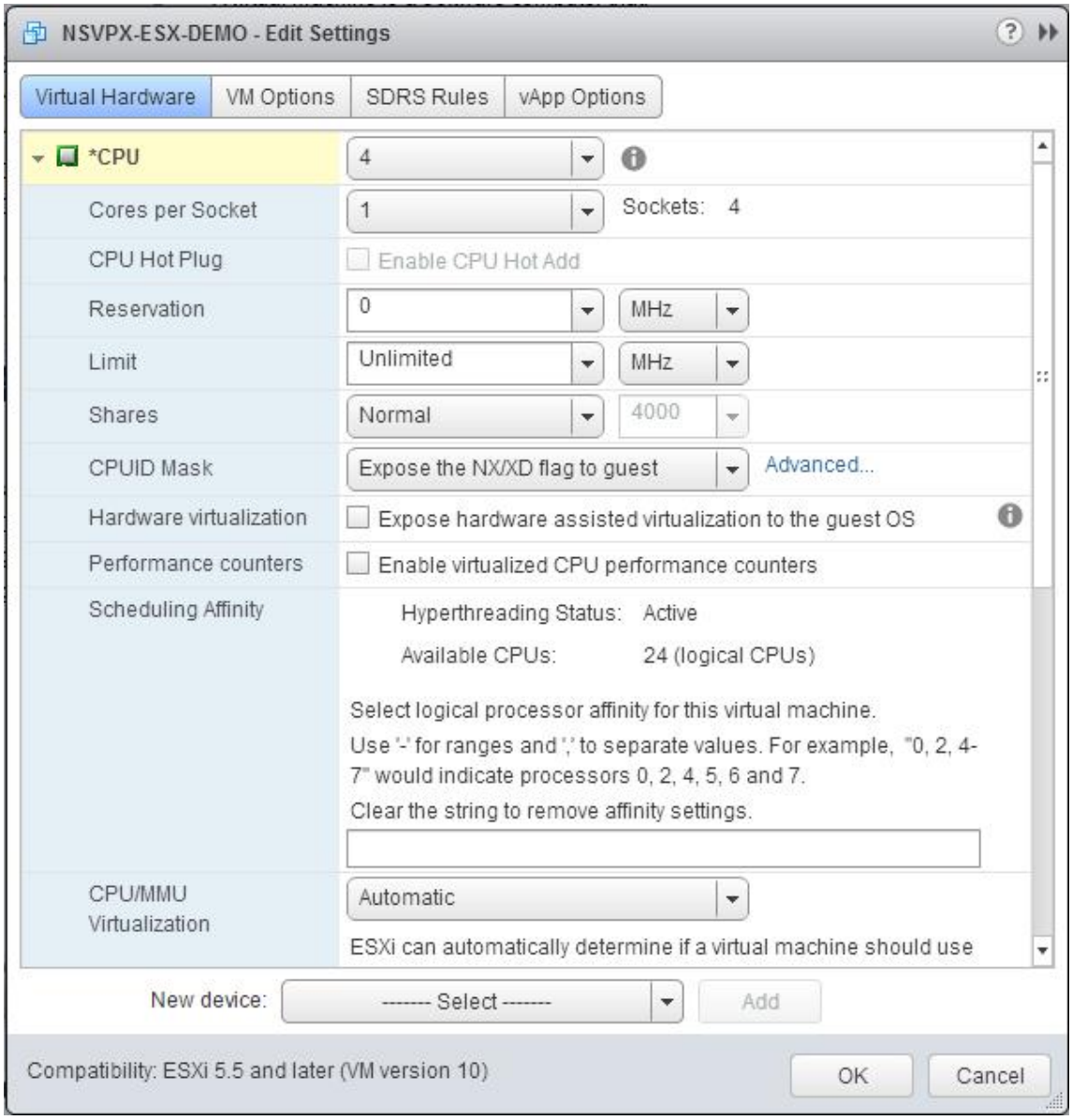
   a。c. 在“配置 **VM** 兼容性”对话框中，从“兼容 对于”下拉列表中选择 **ESXi 5.5** 及更高版本，然后 单 击确定。



3. 右键单击 NetScaler VPX 实例，然后单击“编辑设置”。



4. 在 **** <virtual_appliance>-**编辑设置对话框中，单击 ****CPU** 部分。



5. 在 **CPU** 部分中，更新以下设置：

   - CPU 数量
   - 插槽数量
   - 预订
   - 限制
   - 共享数

   请按如下所示设置各个值：

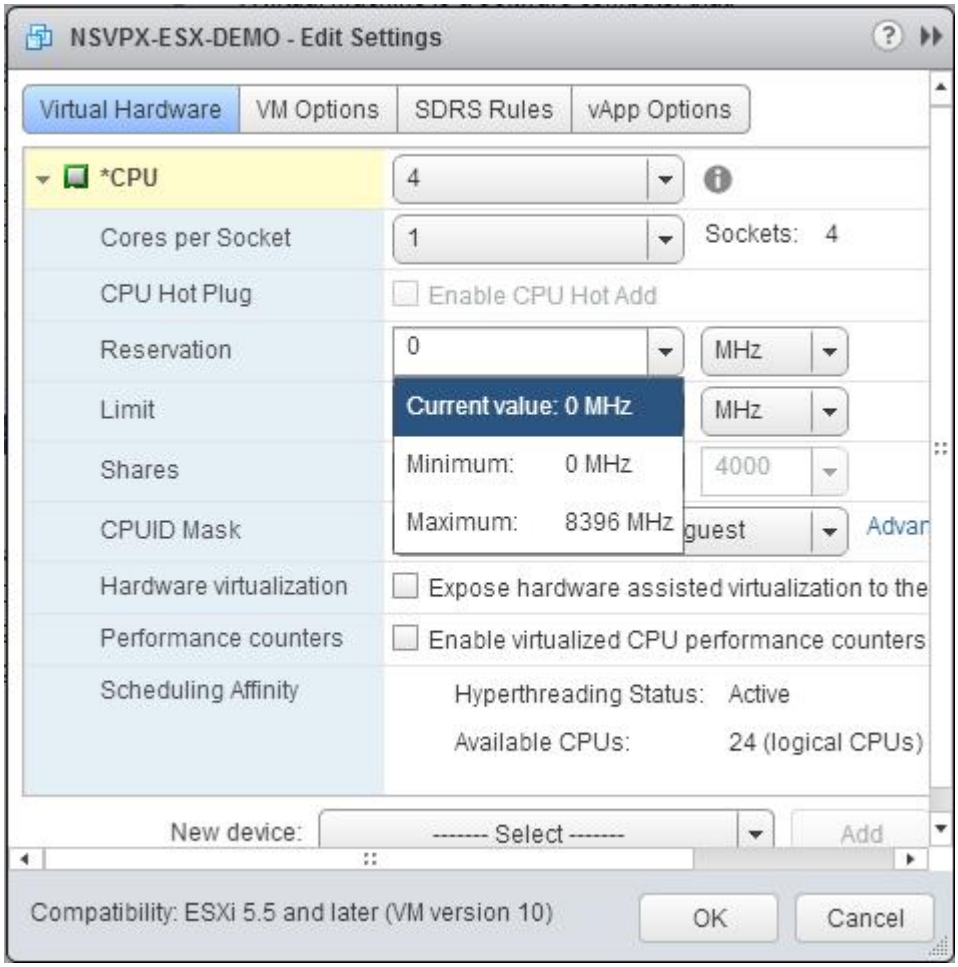
   a。a. 在 **CPU** 下拉列表中，选择要分配给虚拟设备的 CPU 数量。

   a。b. 在“每插槽内核”下拉列表中，选择插槽数量。

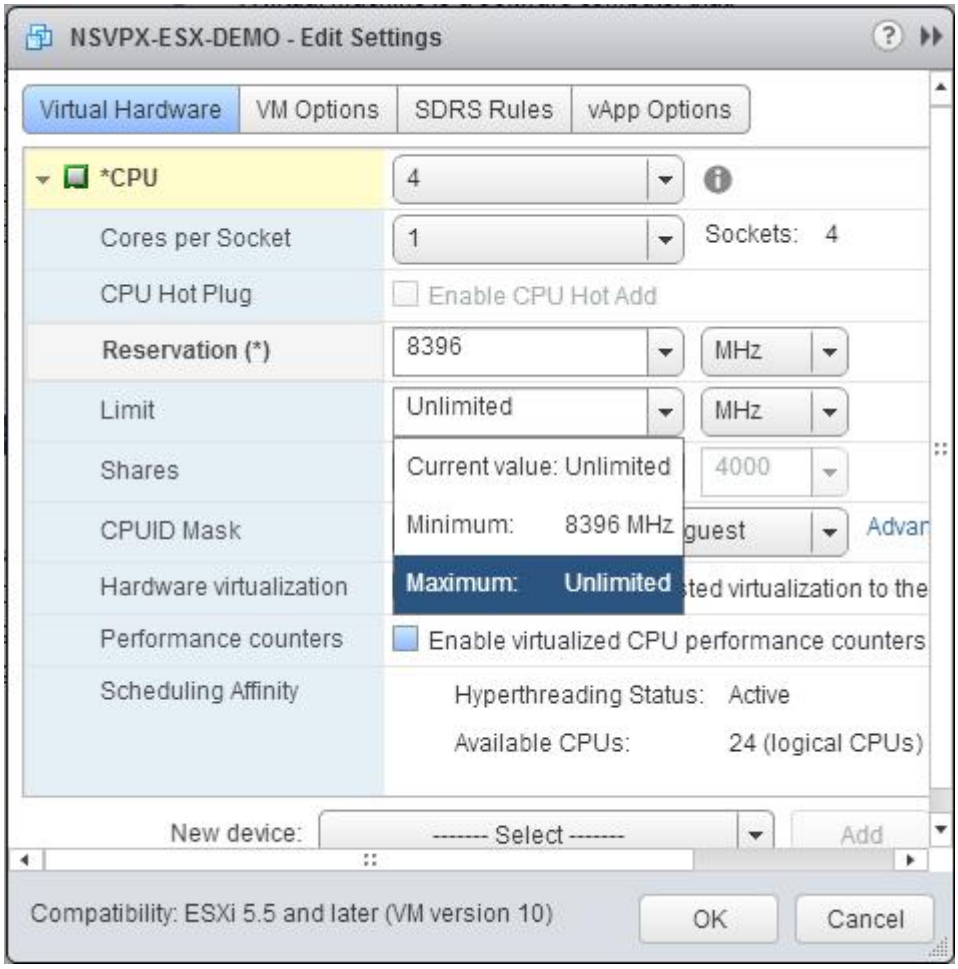
a。c. （可选）在 **CPU Hot Plug**（CPU 热插拔）字段中，选中或取消选中 **Enable CPU Hot Add**（启用 CPU 热添加）复选框。

> 注意：
>
> Citrix 建议接受默认设置（禁用）。

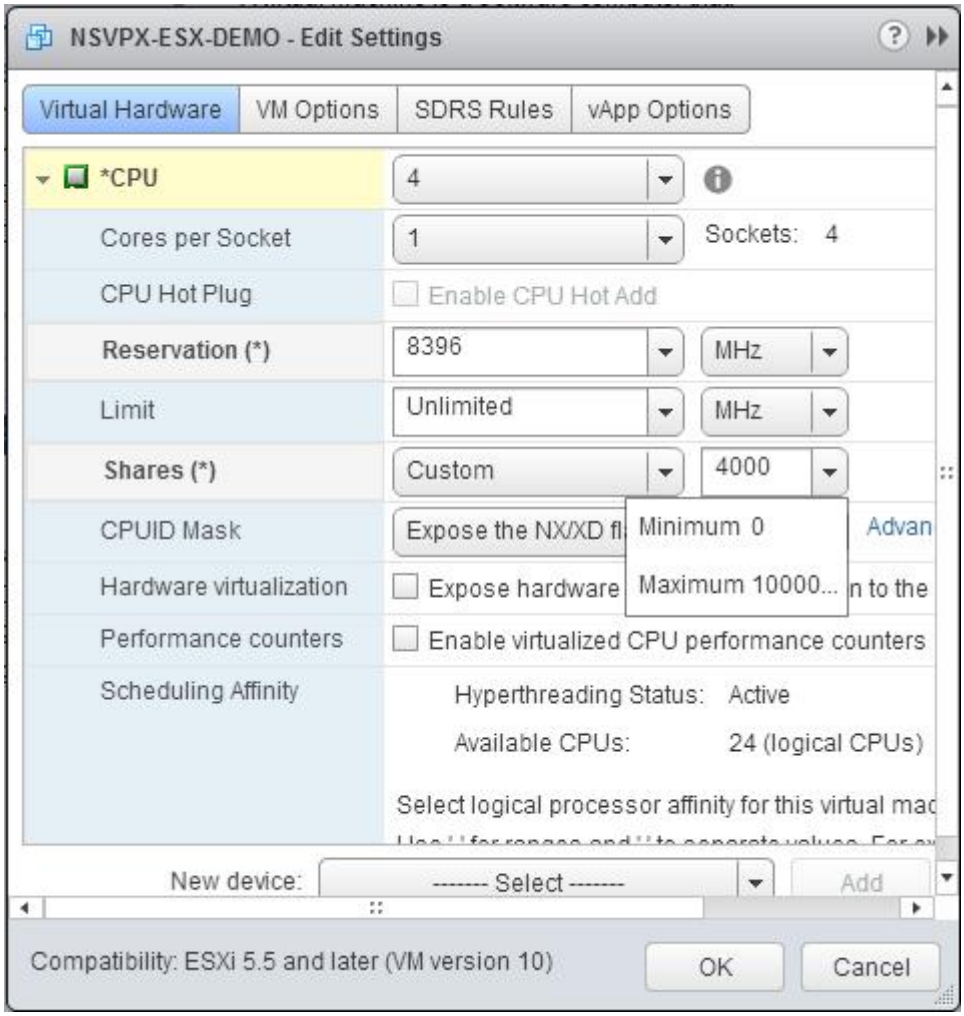
d. d. 在“预留”下拉列表中，选择显示为最大值的数字。



e. e. 在限制下拉列表中，选择显示为最大值的数字。



f. f. 在“共 享”下拉列表中，选择“自定义”和显示为最大值的数字。



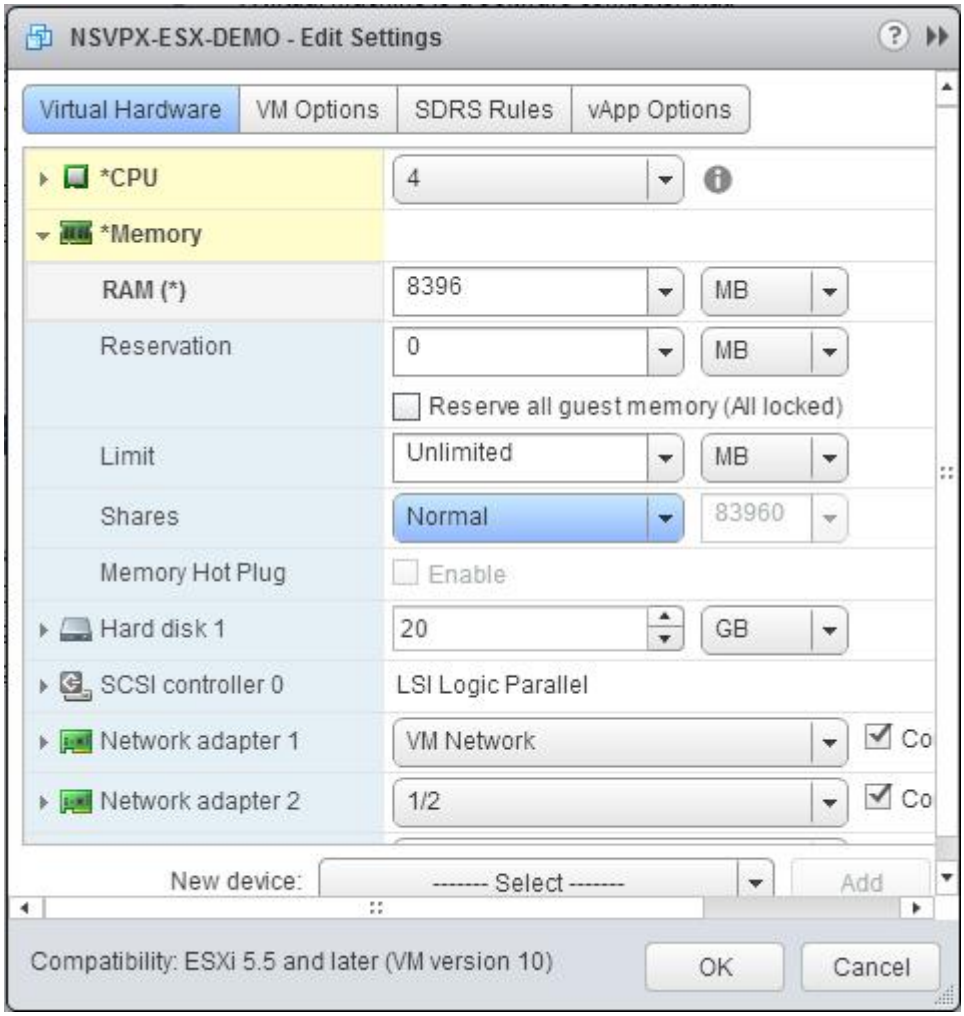
6. 在 **Memory**（内存）部分中，更新以下设置：

   - RAM 大小
   - 预订
   - 限制
   - 共享数

   请按如下所示设置各个值：

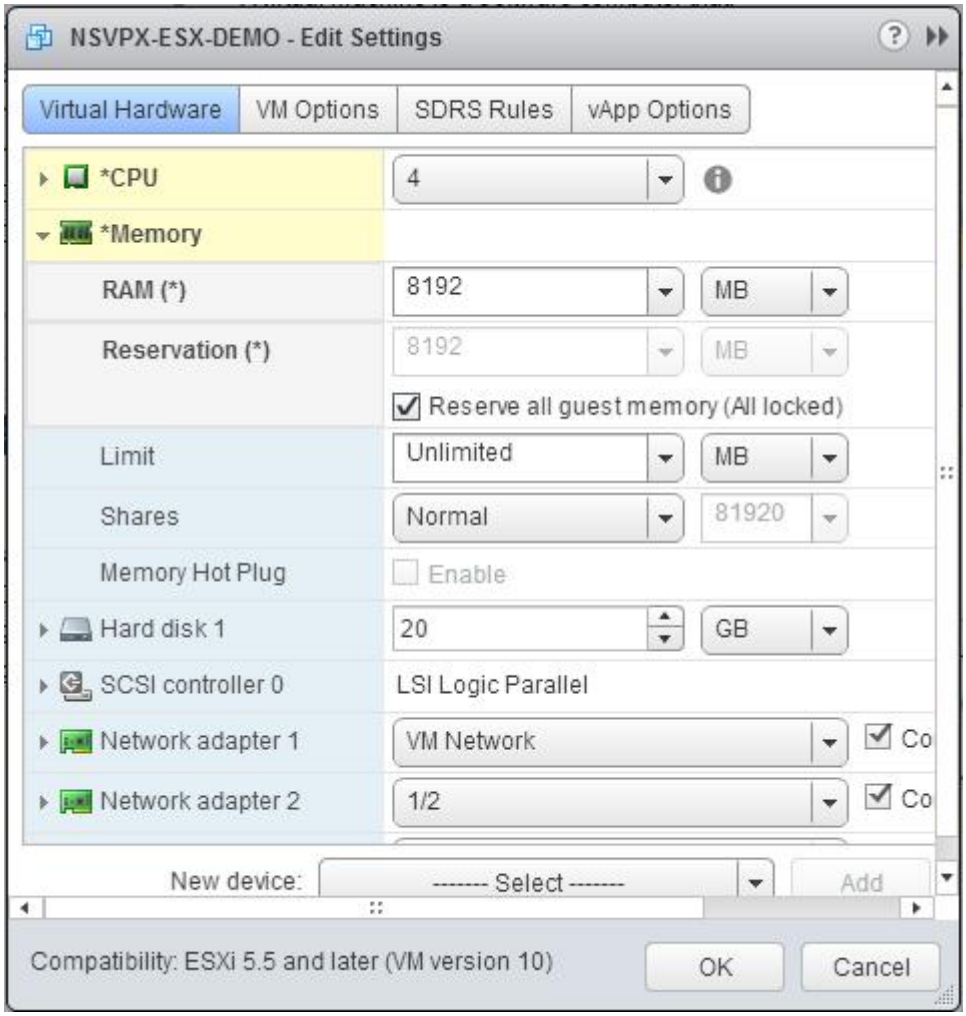
   a。a. 在 **RAM** 下拉列表中，选择 RAM 的大小。必须为 vCPU 数 x 2 GB。例如，如果 vCPU 数为 4，则 RAM 为 4 x 2 GB = 8 GB。

   > 注意：
   >
   > 对于 NetScaler VPX 设备的高级版或优质版，请确保为每个 vCPU 分配 4 GB 的 RAM。例如，如果 vCPU 数为 4，则 RAM 为 4 x 4 GB =16 GB。

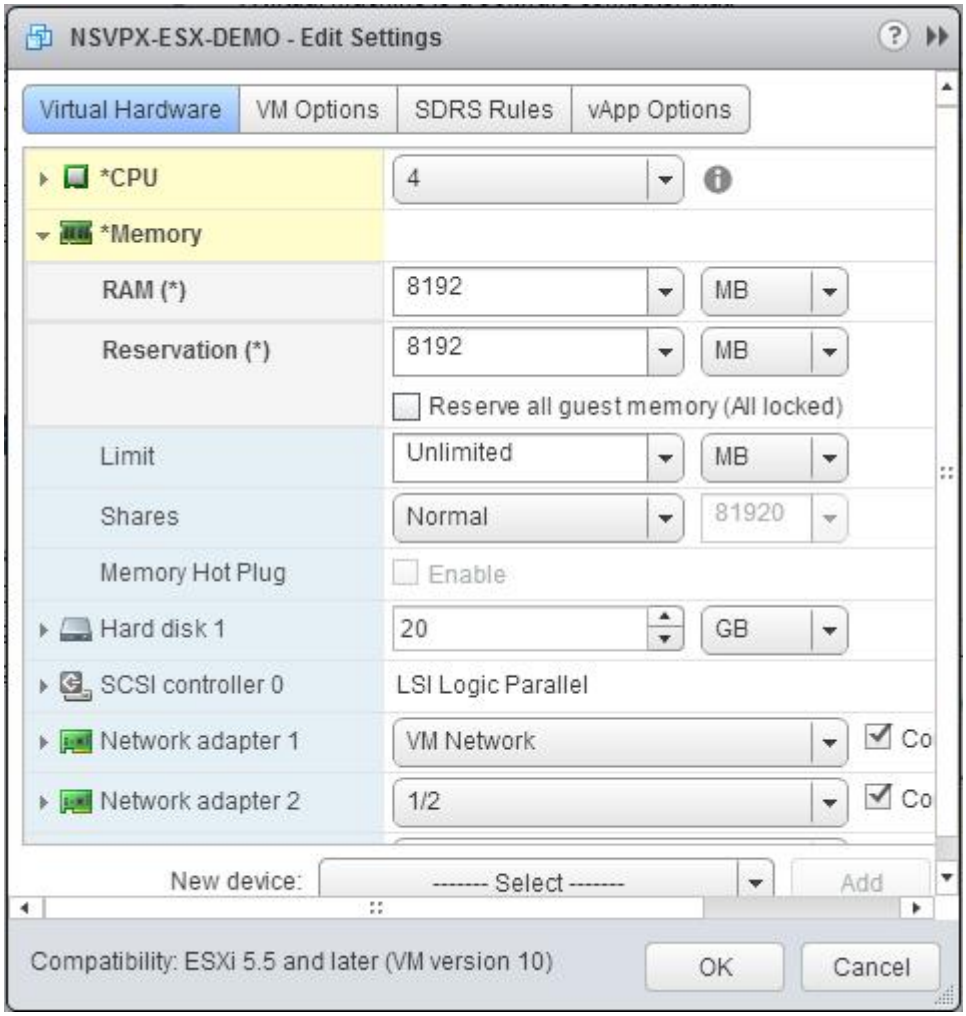


a。b. 在“预留”下拉列表中，输入内存预留的值，然后选中“预 留所有客户内存（全部锁定）”复选框。内存预留量必须为 vCPU 数 × 2 GB。例如，如果 vCPU 数为 4，则内存预留量必须为 4 x 2 GB = 8 GB。

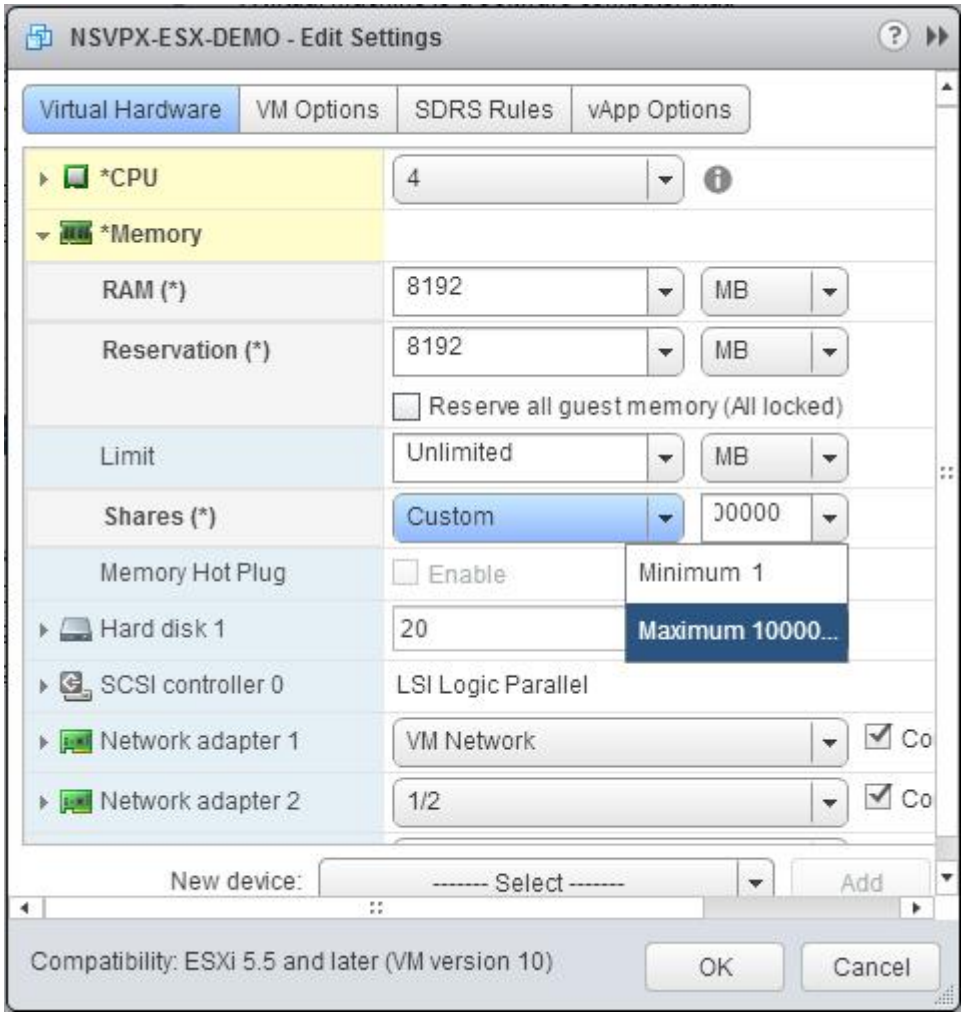
> 注意：
>
> 对于 NetScaler VPX 设备的高级版或优质版，请确保为每个 vCPU 分配 4 GB 的 RAM。例如，如果 vCPU 数为 4，则 RAM 为 4 x 4 GB =16 GB。



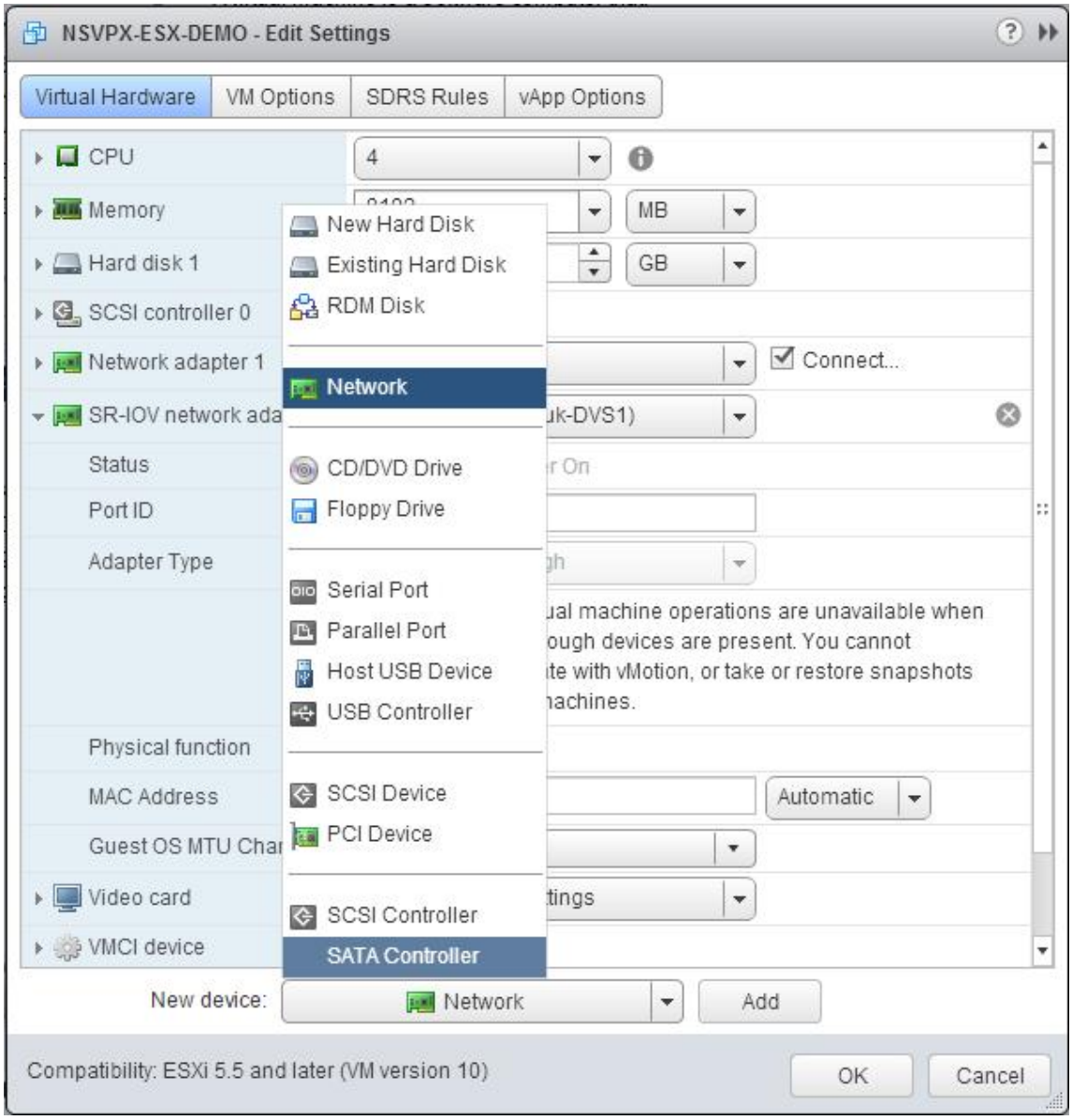
a。e. 在限制下拉列表中，选择显示为最大值的数字。



d. d. 在 **Shares**（共享）下拉列表中，选择 **Custom** 自定义），然后选择将显示为最大值的数字。

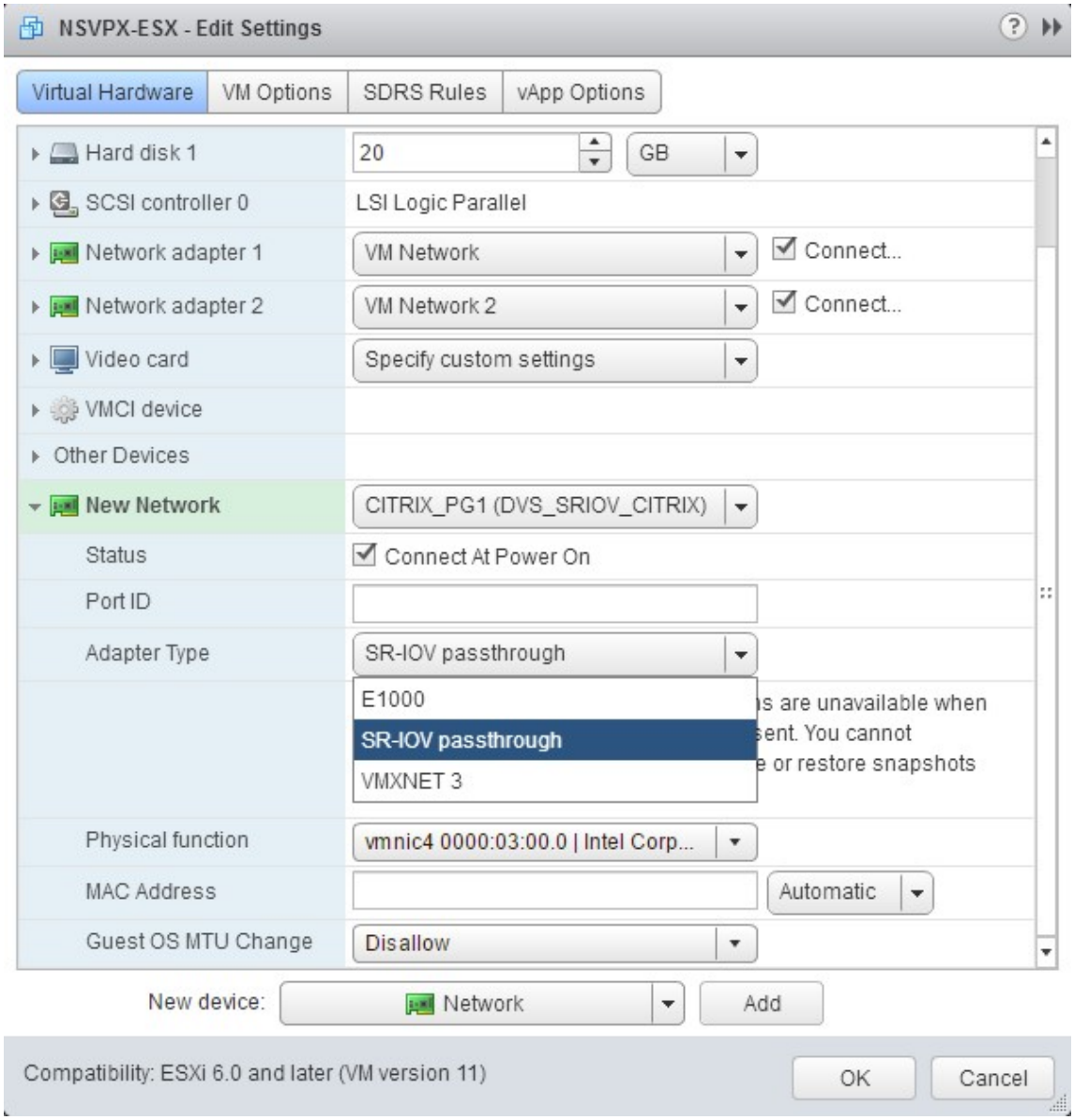


7. 添加 SR-IOV 网络接口。从 新设备 下拉列表中，选择 网络，然后单击 添加。

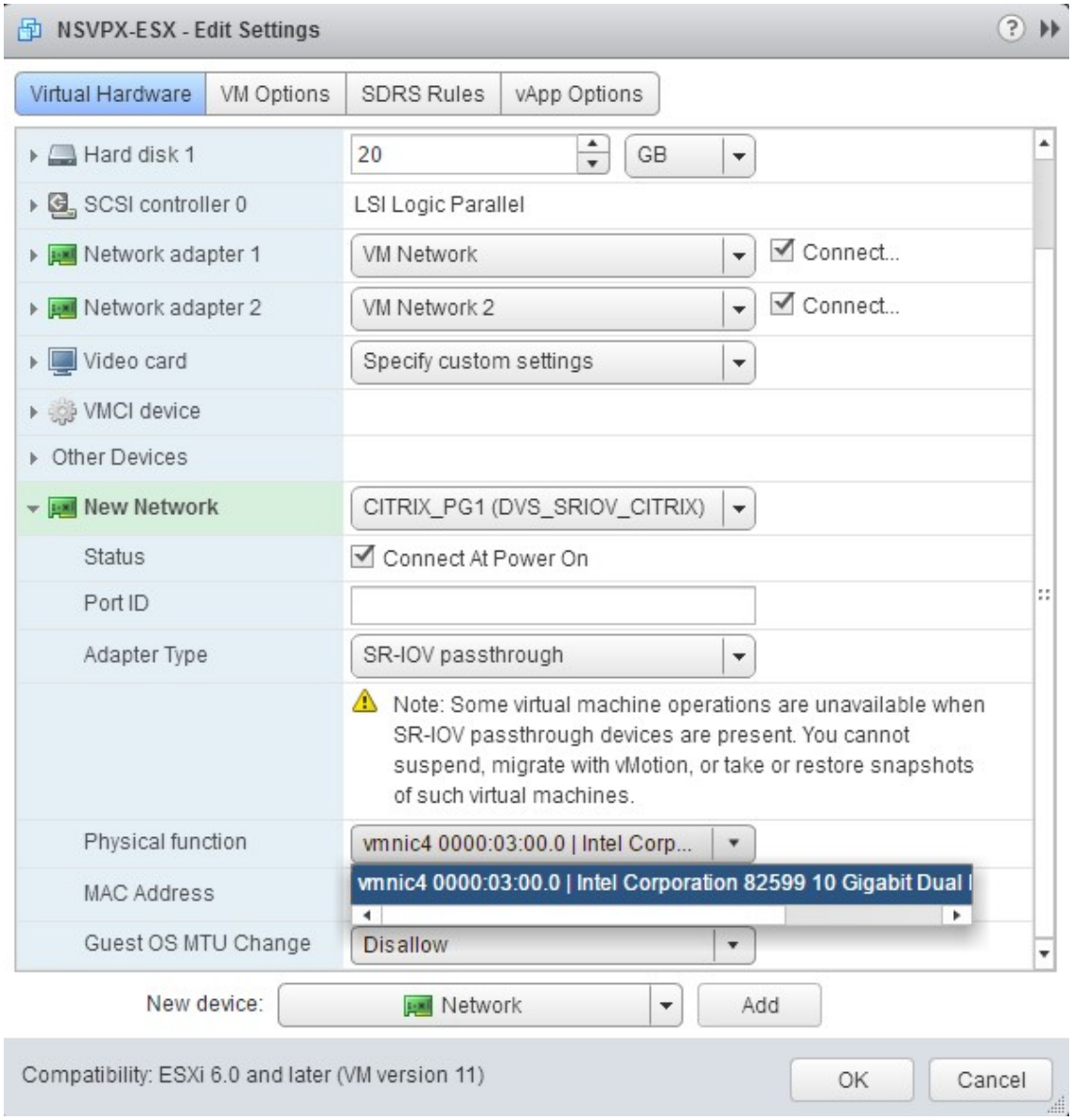


8. 在 **New Network**（新建网络）部分中。在下拉列表中选择已创建的Portgroup，然后执行以下操作：

   a。a. 在 **Adapter Type**（适配器类型）下拉列表中，选择 **SR-IOV passthrough**（SR-IOV 直通）。

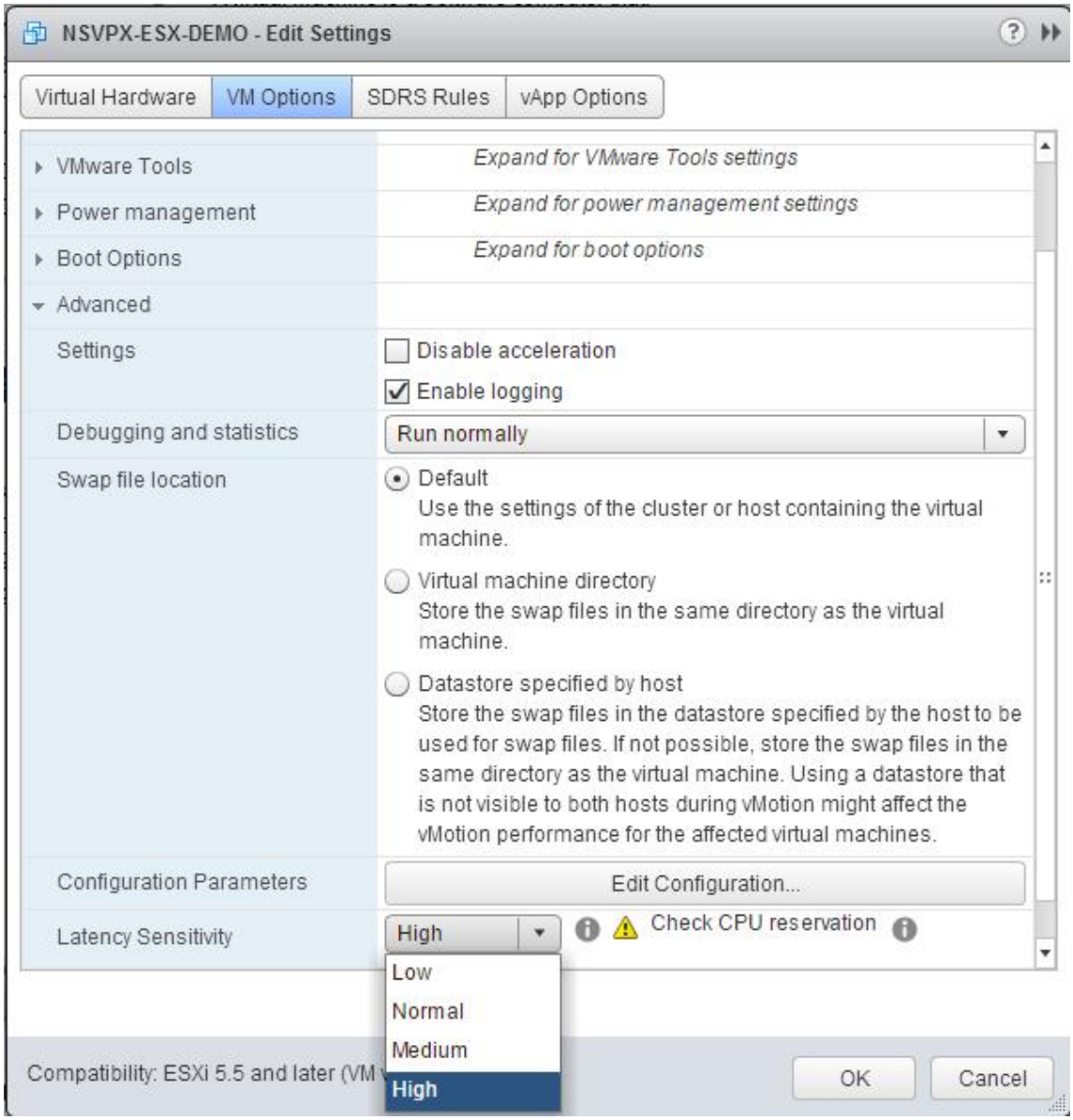


a。b. 在 **Physical function**（物理功能）下拉列表中，选择通过`Portgroup`映射的物理适配器。



a。c. 在 **Guest OS MTU Change**（来宾操作系统 MTU 更改）下拉列表中，选择 **Disallow**（不允许）。

9. 在 **<virtual_appliance> - Edit Settings**(<virtual_appliance> - 编辑设置)对话框中，单击 **VM Options**（VM 选项）选项卡。
10. 在 **VM Options**（VM 选项）选项卡中，选择 **Advanced**（高级）选项。从 **Latency Sensitivity**（延迟敏感度）下拉列表中，选择 **High**（高）。



11. 单击确定。
12. 打开 NetScaler VPX 实例的电源。
13. NetScaler VPX 实例启动后，您可以使用以下命令来验证配置：

    显示接口摘要

输出内容必须显示您已配置的所有接口：

```
> show interface summary
-------------------------------------------------------------------------------

      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
```



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

        RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
           Stalls(0)
        TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0)
           Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
           (0)
        Bandwidth thresholds are not set.
 Done
```

在 **ESX** 虚拟机管理程序上配置 **NetScaler VPX** 以在 **SR-IOV** 模式下使用 **Intel QAT** 进行 **SSL** 加速

October 17, 2024

VMware ESX 虚拟机管理程序上的 NetScaler VPX 实例可以使用 Intel QuickAssist 技术 (QAT) 来加速 NetScaler SSL 性能。使用 Intel QAT，所有高延迟的加密处理都可以卸载到芯片上，从而腾出一个或多个主机 CPU 来执行其他任务。

以前，所有 NetScaler 数据路径加密处理都是在软件中使用主机 vCPU 完成的。

> 注意：
>
> 目前，NetScaler VPX 仅支持 Intel QAT 系列下的 C62x 芯片型号。从 NetScaler 版本 14.1 版本 8.50 开始支

> 持此功能。

必备条件

- ESX 主机配备了一个或多个 Intel C62x (QAT) 芯片。
- NetScaler VPX 符合 VMware ESX 硬件要求。有关更多信息，请参阅 在 VMware ESX上安装 NetScaler VPX 实例。

限制

没有为单个虚拟机预留加密单位或带宽的规定。任何 Intel QAT 硬件的所有可用加密单元均在使用 QAT 硬件的所有虚拟机之间共享。

设置主机环境以使用 **Intel QAT**

1. 下载 Intel 提供的 C62x 系列 (QAT) 芯片型号的 VMware 驱动程序并将其安装到 VMware 主机中。有关 Intel 软件包下载和安装说明的更多信息，请参阅 Intel QuickAssist Technology Driver for VMware。
2. 在 ESX 主机上启用 SR-IOV。
3. 创建虚拟机。创建 VM 时，分配适当数量的 PCI 设备以满足性能要求。

> 注意：
>
> 每个 C62x (QAT) 芯片最多可以有三个独立的 PCI 端点。每个端点都是 VF 的逻辑集合，与芯片的其他 PCI 端点平均共享带宽。每个端点最多可以有 16 个 VF，显示为 16 个 PCI 设备。您可以将这些设备添加到 VM，使用 QAT 芯片进行加密加速。

注意事项

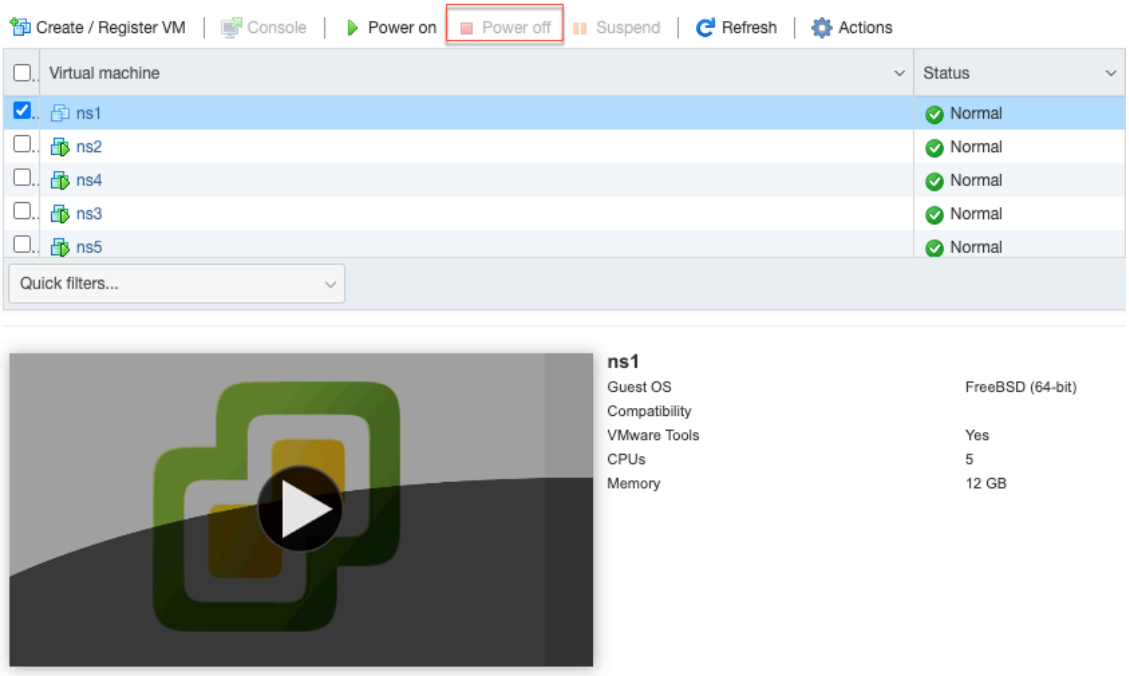
- 如果虚拟机加密要求使用多个 QAT PCI 端点/芯片，建议以循环方式选择相应的 PCI 设备/VF 以实现对称分布。
- 建议选择的 PCI 设备数量等于许可的 vCPU 数量（不包括管理 vCPU 数量）。添加比可用的 vCPU 数量更多的 PCI 设备不一定能提高性能。

  Example:

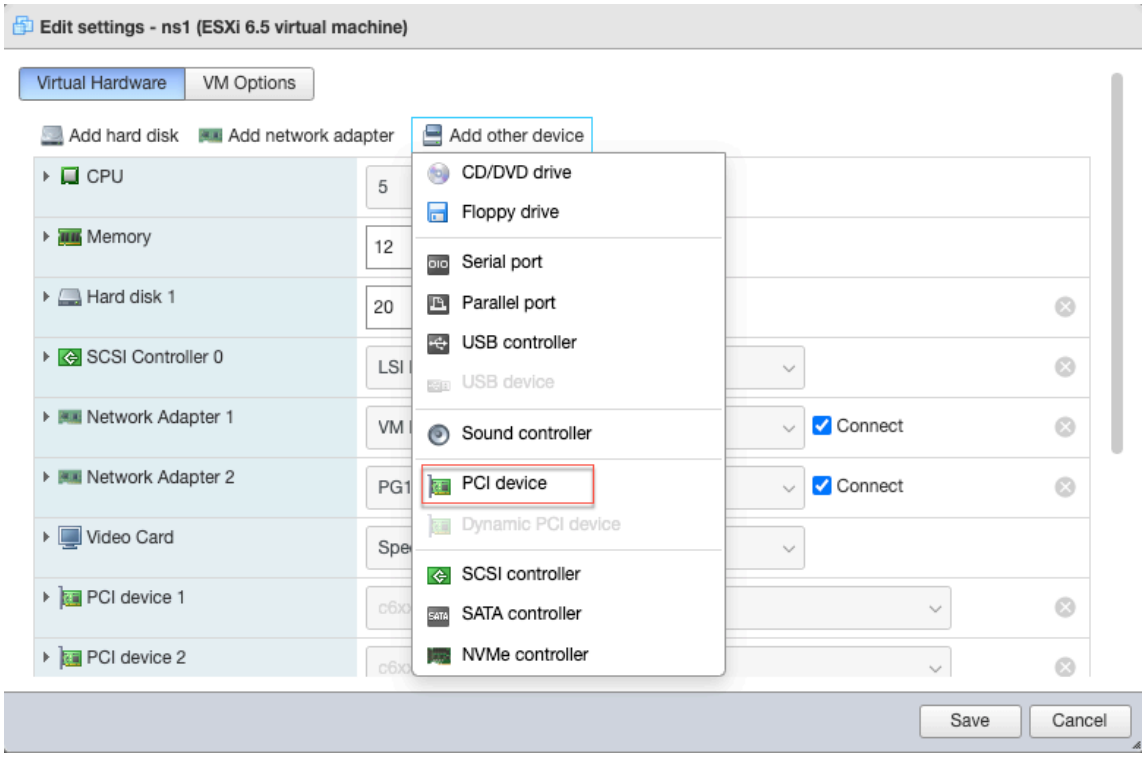
  考虑一台带有一个具有 3 个端点的 Intel C62x 芯片的 ESX 主机。在配置具有 6 个 vCPU 的虚拟机时，从每个端点中选择 2 个 VF，然后将其分配给虚拟机。这种分配可确保虚拟机有效且平等地分配加密单位。默认情况下，在可用的 vCPU 总数中，一个 vCPU 留给管理平面，其余 vCPU 可用于数据平面 PE。

使用 **vSphere** 网络客户端将 **QAT VF** 分配给 **VPX**

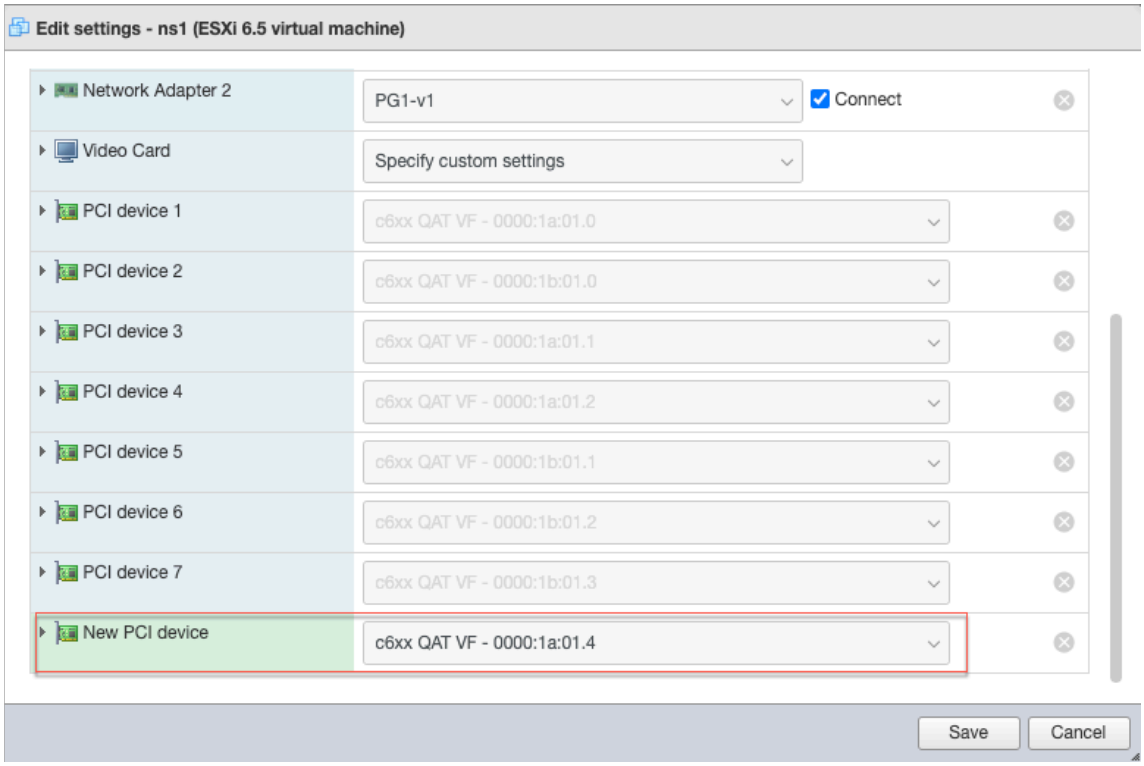
1. 在 vSphere Web 客户端中，导航到虚拟机所在的 ESX 主机，然后单击“关机”。



2. 导航到“操作” **>** “编辑设置” **>** “添加其他设备”，然后选择 PCI 设备。



3. 对于新添加的 PCI 设备，分配 c6xx QAT VF 并保存配置。



4. 再次打开 VM 的电源。
5. 在 NetScaler CLI 中运行 `stat ssl` 命令以显示 SSL 摘要，并在将 QAT VF 分配给 VPX 后验证 SSL 卡。

```
> stat ssl

SSL Summary

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

关于部署

此部署使用以下组件规格进行了测试：

- **NetScaler VPX** 版本和内部版本： 14.1—8.50
- **VMware ESXi** 版本： 7.0.3（内部版本 20036589）
- 适用于 **VMware** 的 **Intel C62x QAT** 驱动程序版本： 1.5.1.54

将 NetScaler VPX 从 E1000 迁移到 SR-IOV 或 VMXNET3 网络接口

October 17, 2024

May 24, 2018

可以将使用 E1000 网络接口的现有 NetScaler VPX 实例配置为使用 SR-IOV 或 VMXNET3 网络接口。

要配置现有的 NetScaler VPX 实例以使用 SR-IOV 网络接口，请参阅 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口。

要配置现有的 NetScaler VPX 实例以使用 VMXNET3 网络接口，请参阅 配置 NetScaler VPX 实例以使用 VMXNET3 网络接口。

将 NetScaler VPX 实例配置为使用 PCI 直通网络接口

October 17, 2024

概述

在 VMware ESX Server 上安装和配置 NetScaler VPX 实例后，您可以使用 vSphere Web Client 将虚拟设备配置为使用 PCI 直通网络接口。

PCI 直通功能允许来宾虚拟设备直接访问连接到主机的物理 PCI 和 PCIe 设备。

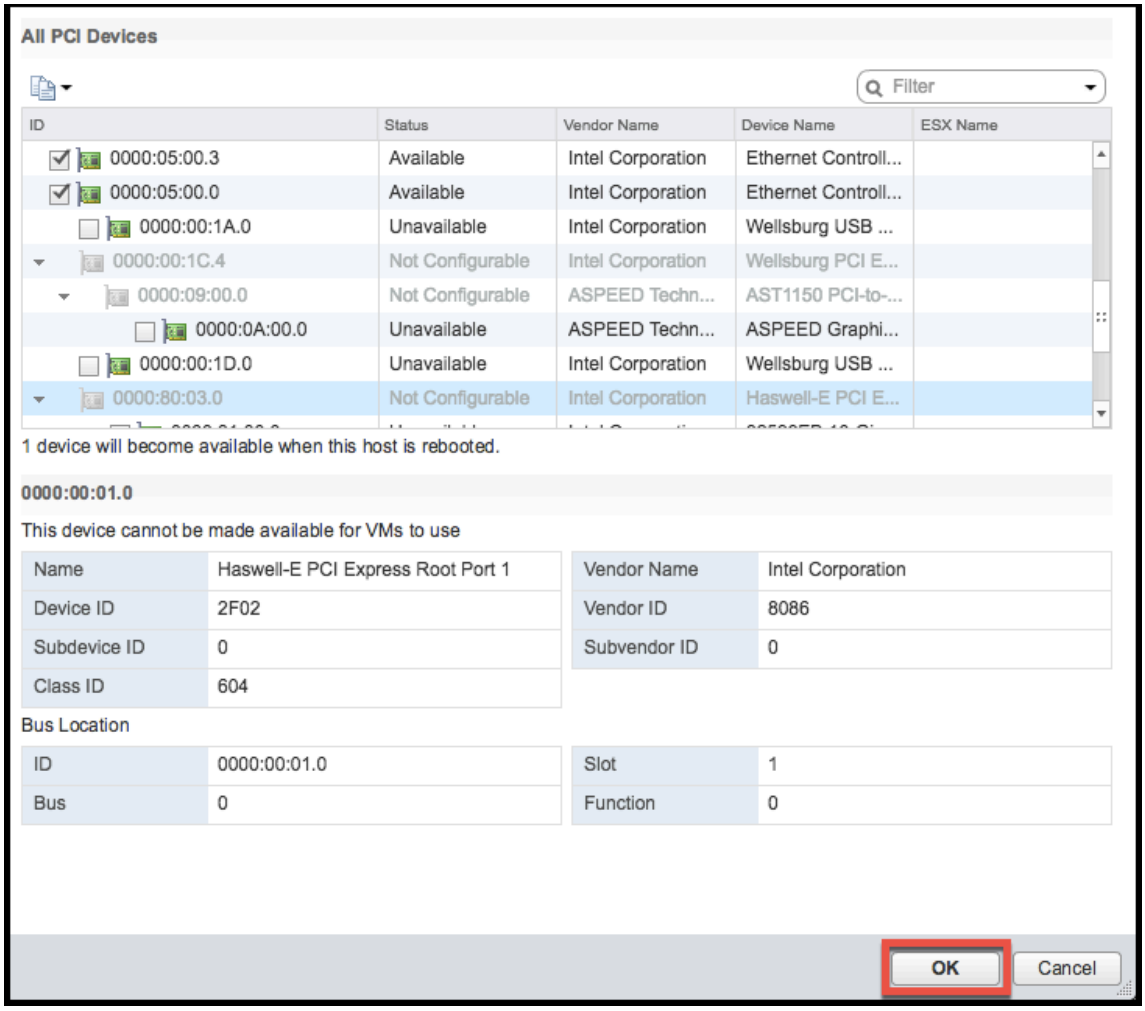
必备条件

- 主机上的 Intel XL710 NIC 的固件版本为 5.04。
- 连接到主机以及在主机上配置的 PCI 直通设备
- 支持的 NIC：
  - Intel X710 10G NIC
  - Intel XL710 双端口 40G 网卡
  - Intel XL710 单端口 40G 网卡
  - Intel XXV710 双端口 25G 网卡

在主机上配置直通设备

必须先在主机上配置 直通 PCI 设备，然后再在虚拟机上配置。请按照以下步骤在主机上配置直通设备。

1. 从 vSphere Web Client 的“导航器”面板中选择主机。
2. 单击 **Manage**（管理）> **Settings**（设置）> **PCI Devices**（PCI 设备）。此时将显示所有可用的直通设备。
3. 右键单击要配置的设备，然后单击 **Edit**（编辑）。
4. 此时将显示 **Edit PCI Device Availability** （编辑 PCI 设备可用性）窗口。
5. 选择用于直通的设备，然后单击 **OK**（确定）。



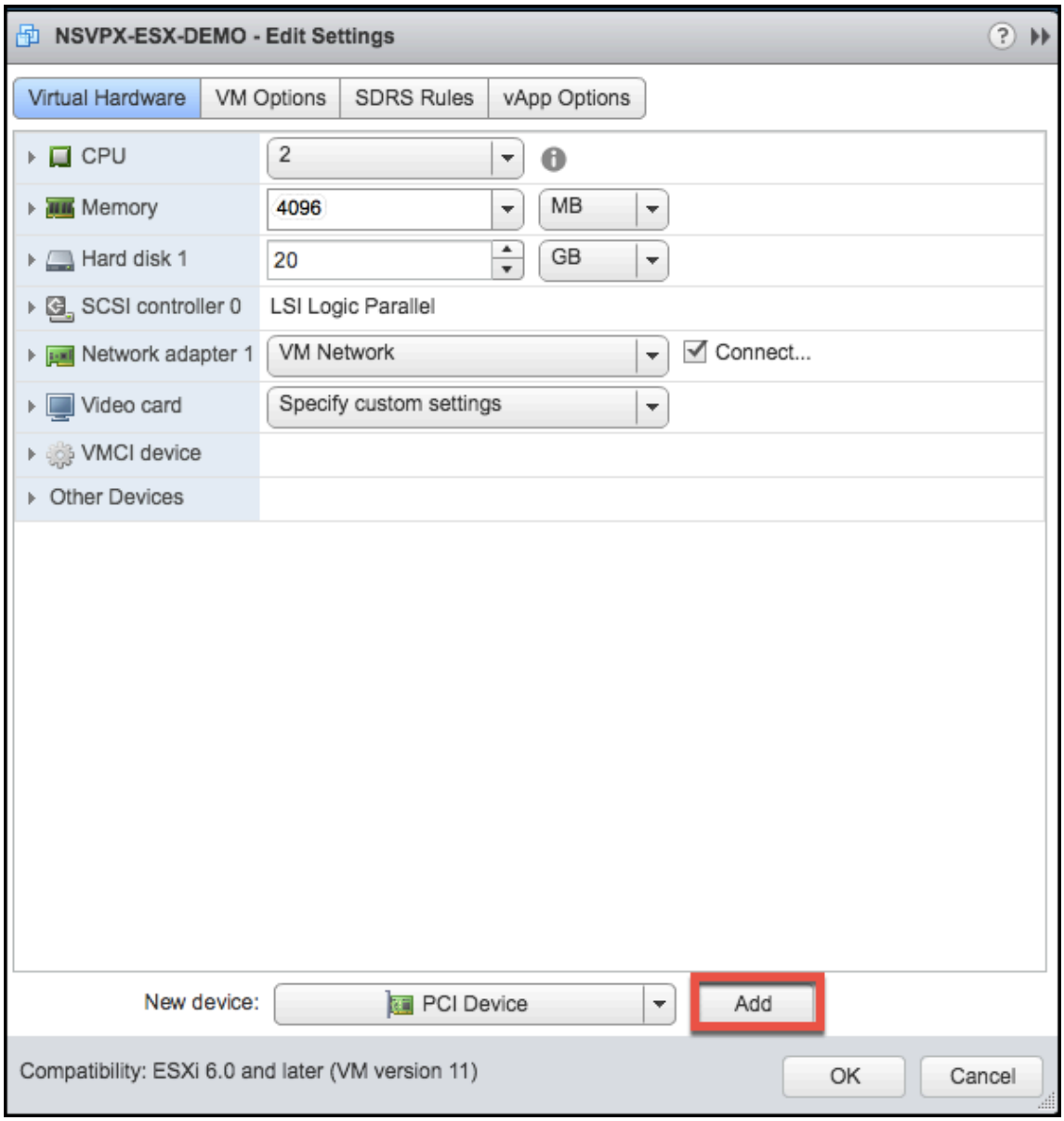
6. 重新启动主机。

在 **NetScaler VPX** 实例上配置直通设备

按照以下步骤在 NetScaler VPX 实例上配置直通 PCI 设备。

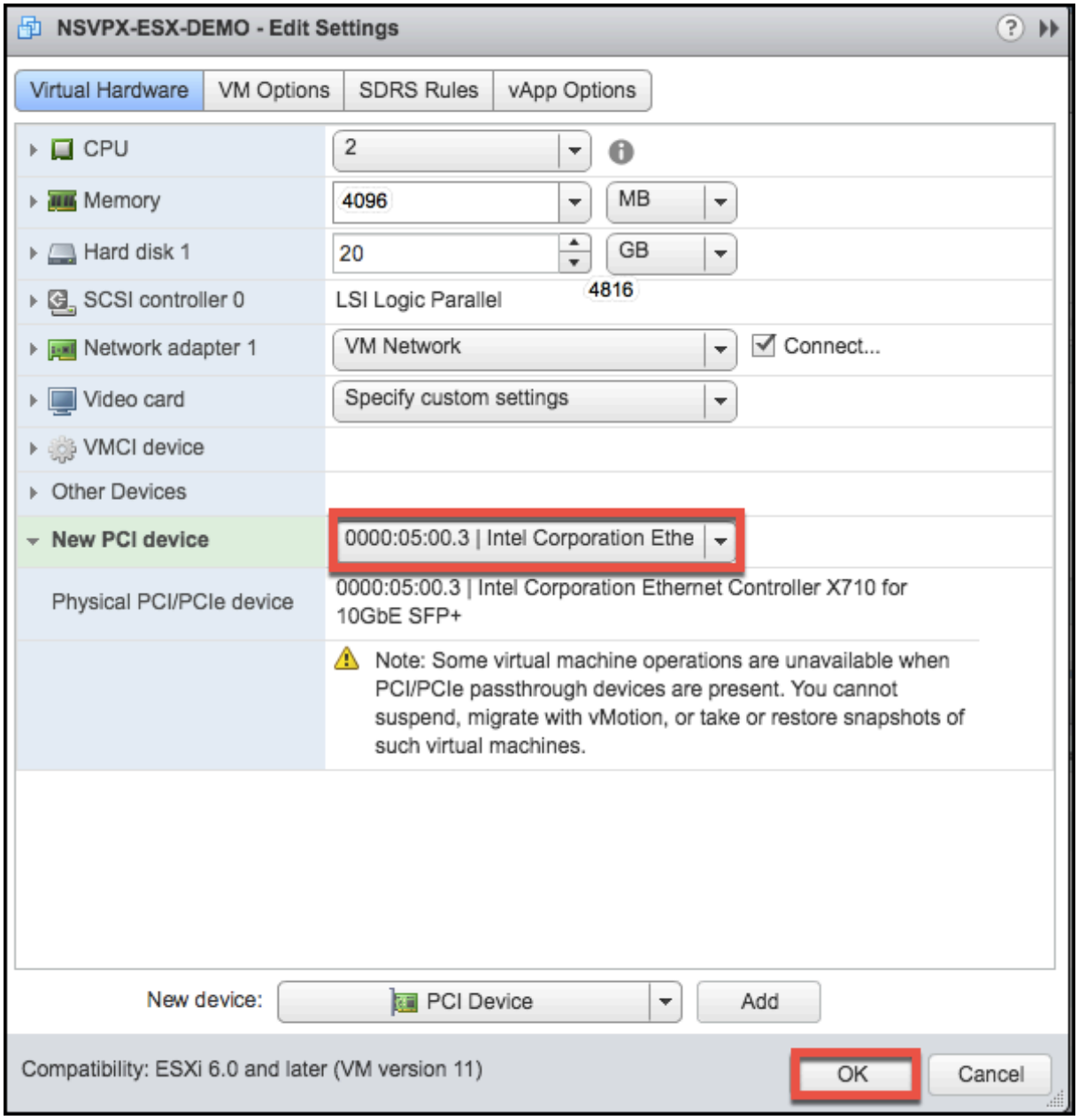
1. 关闭虚拟机的电源。
2. 右键单击该虚拟机，然后选择 **Edit Settings**（编辑设置）。

3. 在 **Virtual Hardware**（虚拟硬件）选项卡上，从 **New Device**（新建设备）下拉菜单中选择 **PCI Device**（PCI 设备），然后单击 **Add**（添加）。



4. 展开 **New PCI device**（新建 PCI 设备），然后从下拉列表中选择要连接到虚拟机的直通设备并单击 **OK**（确定）。

> 注意：
>
> VMXNET3 网络接口和 PCI 直通网络接口不能共存。



1. 关闭来宾虚拟机的电源。

您已完成将 NetScaler VPX 配置为使用 PCI 直通网络接口的步骤。

在 **VMware ESX** 虚拟机管理程序上首次启动 **NetScaler** 设备时应用 **NetScaler VPX** 配置

October 17, 2024

您可以在 VMware ESX 虚拟机管理程序上首次启动 NetScaler 设备期间应用 NetScaler VPX 配置。因此，在某些情况下，特定的设置或 VPX 实例会在更短的时间内启动。

有关预引导用户数据及其格式的更多信息，请参阅在云中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。

> 注意：
>
> 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. 有关 <NS-CONFIG> 标记内容的更多信息，请参见 [示例<NS-CONFIG>-部分]（apply-preboot-userdata-on-esx-vpx.html #sample-<ns-config>-部分）。

Sample <NS-CONFIG> section:

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

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

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

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

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

How to provide preboot user data on ESX hypervisor

您可以通过以下两种方式在 ESX Hypervisor 上从 Web 客户端或 vSphere 客户端提供预启动用户数据：

- Using CD/DVD ISO
- Using OVF Property

Provide user data using CD/DVD ISO

您可以使用 VMware vSphere 客户端使用 CD/DVD 驱动器将用户数据作为 ISO 映像注入虚拟机。

按照以下步骤使用 CD/DVD ISO 提供用户数据：

1. 使用文件名 userdata 创建一个包含预启动用户数据内容的文件。有关 <NS-CONFIG> 标签内容的更多信息，请参阅示例 <NS-CONFIG> 部分。

   > 注意：
   >
   > 文件名必须严格使用为 userdata。

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

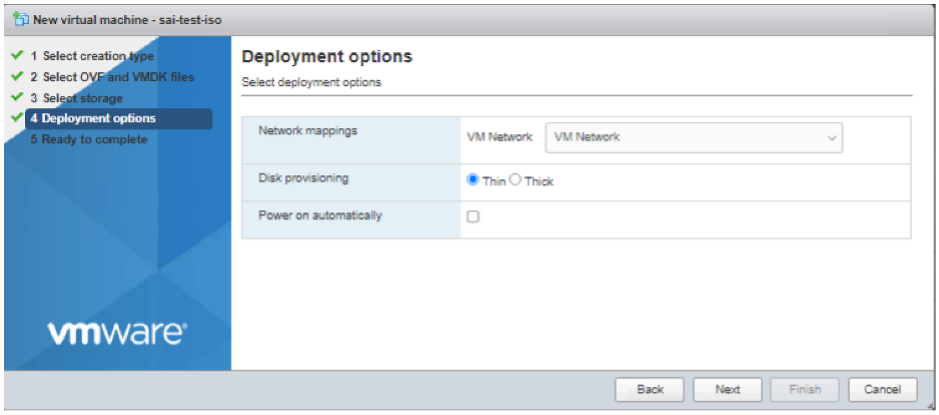
   You can build an ISO image with userdata file by the following two methods:

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

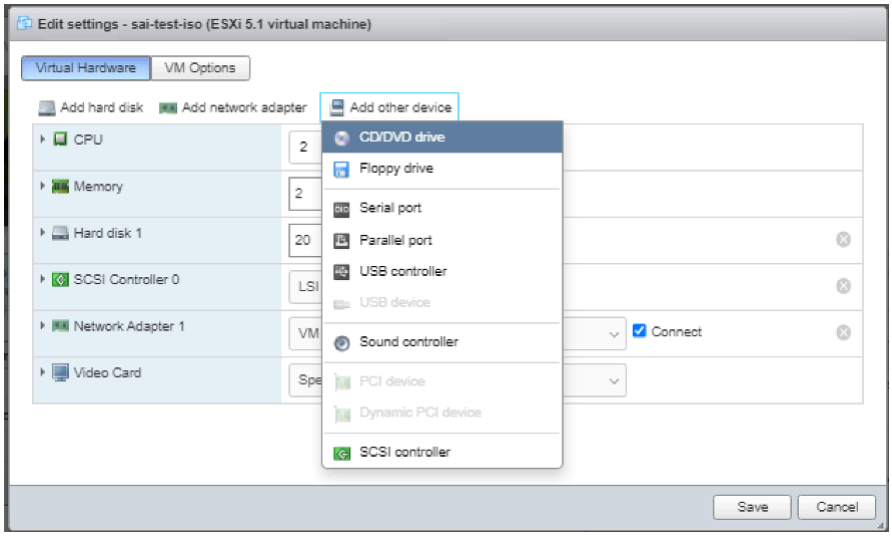
   The following sample configuration shows how to generate an ISO image using the mkisofs command in Linux.

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

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

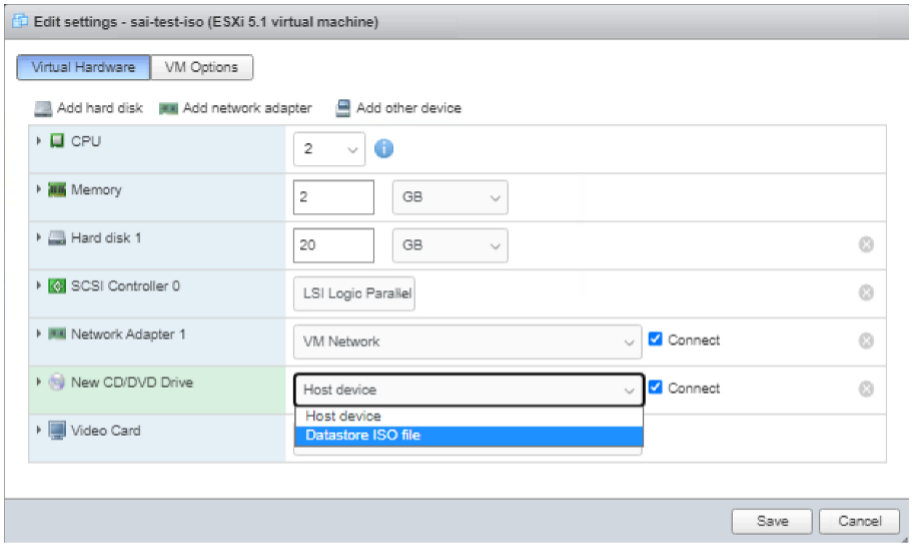
3. 使用标准部署流程预配 NetScaler VPX 实例以创建虚拟机。但是不要自动打开虚拟机的电源。



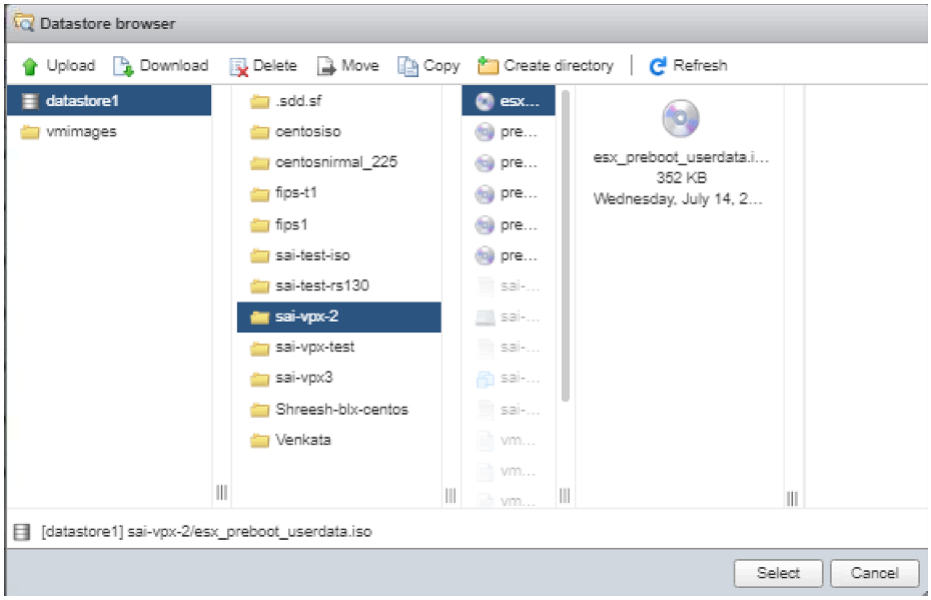
4. After the VM is successfully created, attach the ISO file as CD/DVD drive to the VM.



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



6. Select a Datastore in the vSphere Client.



7. Power on the VM.

使用 **ESX Web** 客户端中的 **OVF** 属性提供用户数据

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.

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

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

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

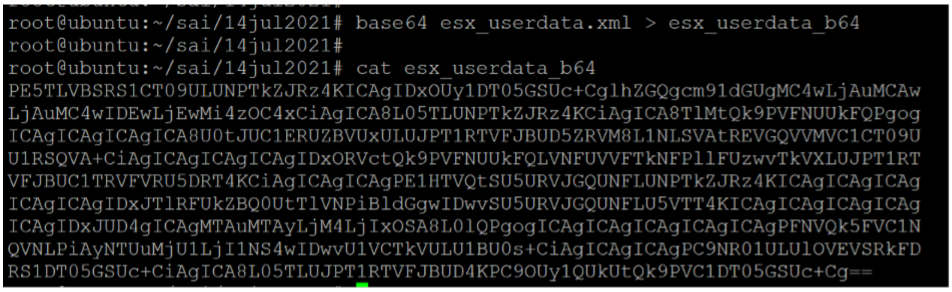
2. 使用 Base64 编码对用户数据内容进行编码。Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

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


Example:

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



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

3. 在 ESX 虚拟机管理程序上的 NetScaler VPX 实例的 OVF 模板中包含 产品 部分。

   Sample Product section:

```xml
<ProductSection>

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

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

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

</ProductSection>
```

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

```xml
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>
  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
      userConfigurable="true"
    ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
        CglhZGQgcm91dGUgMC4wLjAuMCAw
    LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUk
```

```
11        ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC
12        U1RSQVA+
              CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1R
13        VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgIC
14        ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgIC
15        ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgICAgPFNVQk
16        QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
              CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
17        RS1DT05GSUc+
              CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+
              Cg==">
18
19        <Label>Userdata</Label>
20        <Description> Userdata for ESX VPX </Description>
21      </Property>
22
23    </ProductSection>
```

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

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

使用 **ESX vSphere** 客户端中的 **OVF** 属性提供用户数据

按照以下步骤使用 ESX vSphere 客户端中的 OVF 属性提供用户数据。

1. Create a file with user data content.


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

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

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

2. 使用 Base64 编码对用户数据内容进行编码。Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

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

     Example:

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

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

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

3. 在 ESX 虚拟机管理程序上的 NetScaler VPX 实例的 OVF 模板中包含 产品 部分。

   Sample Product section:

   ```
   <ProductSection>

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

   ```



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

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

  </ProductSection>
```

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

```
  <ProductSection>

    <Info>Information about the installed software</Info>
    <Product>NSVPX-VSK Template</Product>
    <Vendor>Citrix</Vendor>
    <VendorUrl>www.Citrix.com</VendorUrl>
    <Category> Preboot Userdata </Category>
    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
       userConfigurable="true"
      ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
         CglhZGQgcm91dGUgMC4wLjAuMCAw
      LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkF

      ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1

      U1RSQVA+
         CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1R

      VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICA

      ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGggIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICA

      ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk

      QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
         CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
      RS1DT05GSUc+
         CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+
         Cg==">

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

  </ProductSection>
```

5. 将该属性添加 `ovf:transport="com.vmware.guestInfo"` 到“虚拟硬件”部分，如下所示：

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

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


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

在 **AWS** 上的 **VMware** 云上安装 **NetScaler VPX** 实例

October 17, 2024

借助 AWS 上的 VMware 云 (VMC)，您可以在 AWS 上创建具有所需数量的 ESX 主机的云软件定义的数据中心 (SDDC)。AWS 上的 VMC 支持 NetScaler VPX 部署。VMC 提供的用户界面与本地 vCenter 相同。其功能与基于 ESX 的 NetScaler VPX 部署相同。

必备条件

在开始安装虚拟设备之前，请执行以下操作：

- 一个 VMware SDDC 必须至少具有一个主机。
- 下载 NetScaler VPX 设备安装文件。
- 在虚拟机连接到的 VMware SDDC 上创建适当的网段。
- 获取 VPX 许可证文件。有关 NetScaler VPX 实例许可证的更多信息，请参阅 *NetScaler VPX* 许可指南 (</en-us/licensing/licensing-guide-for-netscaler.html>)。

VMware 云硬件要求

下表列出了 VMware SDDC 必须为每个 VPX nCore 虚拟设备提供的虚拟计算资源。

表 1. VPX 功能列表 表 2. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

组件	要求
内存	2 GB
虚拟 CPU (vCPU)	2
虚拟网络接口	在 VMware SDDC 中，如果 VPX 硬件升级到版本 7 或更高版本，则最多可以安装 10 个虚拟网络接口。
磁盘空间	20 GB

> 注意：
>
> 这是对虚拟机管理程序的磁盘要求的补充。

要在生产中使用 VPX 虚拟设备，必须保留完整的内存分配。

OVF Tool 1.0 系统要求

OVF 工具是可在 Windows 和 Linux 操作系统上运行的客户端应用程序。下表说明了最低系统要求。

表 2. VPX 功能列表 表 4. 安装 OVF 工具的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。
CPU	最低 750 MHz，建议使用 1 GHz 或速度更快的 CPU
RAM	最低 1 GB；建议使用 2 GB
NIC	100 Mbps 或速度更高的 NIC

有关安装 OVF 的信息，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。

下载 NetScaler VPX 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例设置包遵循开放虚拟机 (OVF) 格式标准。可以从 Citrix Web 站点下载文件。需要使用 Citrix 帐户进行登录。如果您没有 Citrix 帐户，请访问 http://www.citrix.com的主页。单击 **New Users link**（新建用户链接），然后按照说明创建新的 Citrix 帐户。

登录后，从 Citrix 主页浏览以下路径：

Citrix.com > 下载 **> NetScaler >** 虚拟设备。

将以下文件复制到 ESX 服务器所在网络中的一个工作站。将所有三个文件复制到同一个文件夹中。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk（例 如 NSVPX-ESX-13.0-79.64-disk1.vmdk）
- NSVPX-ESX-<release number>-<build number>.ovf （例如 NSVPX-ESX-13.0-79.64.ovf）
- NSVPX-ESX-<release number>-<build number>.mf（例如 NSVPX-ESX-13.0-79.64.mf）

在 **VMware** 云上安装 **NetScaler VPX** 实例

安装并配置 VMware SDDC 后，可以使用 SDDC 在 VMware 云上安装虚拟设备。可以安装的虚拟设备数量取决于 SDDC 上的可用内存量。

要在 VMware 云上安装 NetScaler VPX 实例，请按照以下步骤操作：

1. 在工作站上打开 VMware SDDC。
2. 在 **User Name**（用户名）和 **Password**（密码）文本框中，键入管理员凭据，然后单击“Login”（登录）。
3. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
4. 在部署 **OVF** 模板对话框的从文件部署中，浏览到保存 NetScaler VPX 实例安装文件的位置，选择.ovf 文件，然后单击下一步。

   > 注意：默认情况下，NetScaler VPX 实例使用 E1000 网络接口。要使用 VMXNET3 接口部署 ADC，请将 OVF 修改为使用 VMXNET3 接口而非 E1000 接口。

5. 将虚拟设备 OVF 模板中显示的网络映射到在 VMware SDDC 上配置的网络。单击 **Next**（下一步）开始在 VMware SDDC 上安装虚拟设备。
6. 现在，您可以启动 NetScaler VPX 实例。在导航窗格中，选择已安装的 NetScaler VPX 实例，然后从右键菜单中选择 **Power On**（开机）。单击 **Console**（控制台）选项卡模拟控制台端口。
7. 如果要安装其他虚拟设备，请重复步骤 6。
8. 指定来自选择作为管理网络的同一网段的管理 IP 地址。网关使用同一子网。
9. VMware SDDC 要求为属于网段的所有专用 IP 地址显式创建 NAT 和防火墙规则。

在 **Microsoft Hyper-V** 服务器上安装 **NetScaler VPX** 实例

October 17, 2024

要在 Microsoft Windows Server 上安装 NetScaler VPX 实例，必须先在系统资源充足的计算机上安装启用了 Hyper-V 角色的 Windows Server。安装 Hyper-V 角色时，请确保在服务器上指定 Hyper-V 用来创建虚拟网络的 NIC。可以保留某些 NIC 供主机使用。使用 Hyper-V 管理器执行 NetScaler VPX 实例安装。

适用于 Hyper-V 的 NetScaler VPX 实例以虚拟硬盘 (VHD) 格式交付。其中包括 CPU、网络接口以及硬盘大小和格式等元素的默认配置。安装 NetScaler VPX 实例后，可以在虚拟设备上配置网络适配器，添加虚拟 NIC，然后分配 NetScaler IP 地址、子网掩码和网关，然后完成虚拟设备的基本配置。

初始配置 VPX 实例后，如果要将设备升级到最新的软件版本，请参阅 升级 NetScaler VPX 独立设备

> 注意：
>
> HyperV-2012 平台上托管的 NetScaler VPX 虚拟设备上不支持中间系统对中间系统 (Intermediate System-to-Intermediate System, ISIS) 协议。

在 **Microsoft** 服务器上安装 **NetScaler VPX** 实例的必备条件

在开始安装虚拟设备之前，请执行以下操作：

- 在 Windows Server 上启用 Hyper-V 角色。有关详细信息，请参阅 http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx。
- 下载虚拟设备安装文件。
- 获取 NetScaler VPX 实例许可证文件。有关 NetScaler VPX 实例许可证的详细信息，请参阅中的 *NetScaler VPX Licensing Guide*（《NetScaler VPX 许可指南》），URL 为 https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US。

Microsoft Server 硬件要求

下表介绍了 Microsoft Server 的最低系统要求。

表 1. VPX 功能列表 表 1. Microsoft Server 的最低系统要求

组件	要求
CPU	1.4 GHz 64 位处理器
RAM	8 GB
磁盘空间	32 GB 或更大

下表列出了每个虚拟计算资源 NetScaler VPX 实例。

表 2. VPX 功能列表 表 2. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

组件	要求
RAM	4 GB
虚拟 CPU	2
磁盘空间	20 GB
虚拟网络接口	1

下载 **NetScaler VPX** 安装文件

适用于 Hyper-V 的 NetScaler VPX 实例以虚拟硬盘 (VHD) 格式交付。可以从 Citrix Web 站点下载文件。需要使用 Citrix 帐户进行登录。如果您没有 Citrix 帐户，请访问 http://www.citrix.com的主页，单击 登录 **>** 我的帐户 **>** 创建 **Citrix** 帐户，然后按照说明创建 Citrix 帐户。

要下载 NetScaler VPX 实例安装文件，请按照以下步骤进行操作：

1. 在 Web 浏览器中，转到 http://www.citrix.com/。
2. 使用您的用户名和密码登录。
3. 单击下载。
4. 在 选择产品下拉菜单中，选择 **NetScaler**（**NetScaler ADC**）。
5. 在 NetScaler 版本 X.X > 虚拟设备下，单击 **NetScaler VPX** 版本 **X.X**
6. 将压缩文件下载到服务器。

在 **Microsoft** 服务器上安装 **NetScaler VPX** 实例

在 Microsoft 服务器上启用 Hyper-V 角色并解压缩虚拟设备文件后，您可以使用 Hyper-V Manager 安装 NetScaler VPX 实例。导入虚拟机后，需要将其与 Hyper-V 创建的虚拟网络关联，以配置虚拟网卡。

最多可以配置八个虚拟 NIC。即使物理 NIC 为 DOWN（关闭），虚拟设备仍会假定虚拟 NIC 为 UP（打开），因为它仍然可与同一主机（服务器）上的其他虚拟设备通信。

> 注意：
>
> 在虚拟设备运行期间无法更改任何设置。要进行更改，请先关闭虚拟设备。

要使用 **Hyper-V** 管理器在 **Microsoft** 服务器上安装 **NetScaler VPX** 实例，请执行以下操作：

1. 要启动 Hyper-V 管理器，请单击开始，指向管理工具，然后单击 **Hyper-V** 管理器。
2. 在导航窗格中，在 **Hyper-V Manage** r 下，选择要在其上安装 NetScaler VPX 实例的服务器。
3. 在 **Action**（操作）菜单上，单击 **Import Virtual Machine**（导入虚拟机）。

4. 在“导入虚拟机”对话框的“位置”中，指定包含 NetScaler VPX 实例软件文件的文件夹的路径，然后选择 复制虚拟机（创建新的唯一 ID）。此文件夹是包含快照、虚拟硬盘和虚拟机文件夹的父文件夹。

> 注意：
>
> 如果收到压缩文件，请确保在指定文件夹的路径之前将文件解压到文件夹中。

1. 单击导入。
2. 验证您导入的虚拟设备是否在 **Virtual Machines**（虚拟机）下列出。
3. 要安装其他虚拟设备，请重复步骤 **2** 至步骤 **6**。

> 重要：
>
> 请确保将文件解压到步骤 **4** 中的其他文件夹。

在 **Hyper-V** 上自动配置 **NetScaler VPX** 实例

自动配置 NetScaler VPX 实例是可选的。如果不执行自动置备，则虚拟设备会提供一个用于配置 IP 地址等设置的选项。

要在 Hyper-V 上自动配置 NetScaler VPX 实例，请按照以下步骤操作。

1. 使用 xml 文件创建符合 ISO9660 标准的 ISO 映像，如以下示例所示。确保 xml 文件的名称为 **userdata**。

   可以使用以下方法从 XML 文件创建 ISO 文件：

   • 任何图像处理工具，例如 PowerISO。

   • Linux 中的 `mkisofs` 命令。

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

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

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

oe:id=""

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

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

```



```
21    </PlatformSection>
22
23    <PropertySection>
24
25    <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
          1.0"/>
26
27    <Property oe:key="com.citrix.netscaler.platform" oe:value="
          NS1000V"/>
28
29    <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="
          cisco-orch-env"/>
30
31    <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
          10.102.100.122"/>
32
33    <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
          255.255.255.128"/>
34
35    <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
          10.102.100.67"/></PropertySection>
36
37    </Environment>
```

2. 将 ISO 映像复制到 hyper-v 服务器。
3. 选择已导入的虚拟设备，然后在 **Action**（操作）菜单中选择 **Settings**（设置）。还可以选择虚拟设备，然后右键单击并选择 **Settings**（设置）。将显示选定虚拟设备的 **Settings**（设置）窗口。
4. 在 **Settings**（设置）窗口中的硬件部分下，单击 **IDE Controller**（IDE 控制器）。
5. 在右侧的窗口窗格中，选择 **DVD Drive**（DVD 驱动器），然后单击 **Add**（添加）。DVD 驱动器将添加到左侧窗格中的 **IDE Controller**（IDE 控制器）部分下。
6. 选择在步骤 5 中添加的 **DVD** 驱动器。在右侧窗口窗格中，选择 **Image file**（映像文件）单选按钮，然后单击 **Browse**（浏览），并选择您在步骤 2 中在 Hyper-V 服务器上复制的 ISO 映像。
7. 单击应用。

> 注意：
>
> 在以下情况下，虚拟设备实例以默认 IP 地址出现：

- 已连接 DVD 驱动器，并且未提供 ISO 文件。
- ISO 文件不包含用户数据文件。
- 用户数据文件的名称或格式不正确。

要在 NetScaler VPX 实例上配置虚拟网卡，请执行以下步骤：

1. 选择已导入的虚拟设备，然后在 **Action**（操作）菜单中选择 **Settings**（设置）。
2. 在 **Settings for <virtual appliance name>**（< 虚拟设备名称 > 的设置）对话框中，单击左侧窗格中的 **Add Hardware**（添加硬件）。虚拟设备名称 >

3. 在右侧窗格中，从设备列表中选择 **Network Adapter**（网络适配器）。
4. 单击添加。
5. 确认 **Network Adapter (not connected)**（网络适配器 (未连接)）是否显示在左侧窗格中。
6. 在左窗格中选择网络适配器。
7. 在右侧窗格中，从 **Network**（网络）菜单中选择要将适配器连接到的虚拟网络。
8. 要为您要使用的其他网络适配器选择虚拟网络，请重复步骤 **6** 和 **7**。
9. 单击 **Apply**（应用），然后单击 **OK**（确定）。

要配置 **NetScaler VPX** 实例，请执行以下操作：

1. 在您之前安装的虚拟设备上单击鼠标右键，然后选择 **Start**（启动）。
2. 通过双击虚拟设备访问控制台。
3. 键入虚拟设备的 NetScaler IP 地址、子网掩码和网关。

您已完成虚拟设备的基本配置。在 Web 浏览器中键入 IP 地址，以访问虚拟设备。

> 注意：
>
> 通过使用 SCVMM，您也可以使用虚拟机 (VM) 模板预配 NetScaler VPX 实例。
>
> 如果你将微软 Hyper-V NIC 组合解决方案与 NetScaler VPX 实例结合使用，请参阅文章 CTX224494 了解更多信息。

在 **Linux-KVM** 平台上安装 **NetScaler VPX** 实例

October 17, 2024

要为 Linux-KVM 平台设置 NetScaler VPX，可以使用图形化虚拟机管理器（虚拟管理器）应用程序。如果您更偏向于使用 Linux-KVM 命令行，可以使用 `virsh` 程序。

必须使用 KVM Module 和 QEMU 等虚拟化工具在适用的硬件上安装主机 Linux 操作系统。可以在虚拟机管理程序上部署的虚拟机 (VM) 数量取决于应用程序要求和所选硬件。

在配置 NetScaler VPX 实例后，您可以添加更多接口。

局限性与用法指南

一般建议

为避免发生不可预测的行为，请遵循以下建议：

- 请勿更改与 VPX VM 关联的 VNet 接口的 MTU。修改接口模式或 CPU 等任何配置参数前，请关闭 VPX VM。
- 请勿强制关闭 VPX VM。也就是说，请勿使用 **Force off** 命令。

- 在主机 Linux 上所做任何配置的持久性取决于 Linux 分布设置。可选择持久保持这些配置，以确保在主机 Linux 操作系统重新启动前后保持一致的行为。
- NetScaler 软件包对于每个置备的 NetScaler VPX 实例必须唯一。

限制

- 不支持实时迁移 KVM 上运行的 VPX 实例。

在 **Linux-KVM** 平台上安装 **NetScaler VPX** 实例的先决条件

October 17, 2024

查看在 NetScaler VPX 实例上运行的 Linux-KVM 服务器的最低系统要求。

CPU 要求：

- 64 位 x86 处理器，Intel VT-X 处理器中包含硬件虚拟化功能。

要测试您的 CPU 是否支持 Linux 主机，请在 Linux shell 提示下输入以下命令：

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

如果禁用了上一个扩展的 **BIOS** 设置，则必须在 BIOS 中启用它们。

- 至少为主机 Linux 提供 2 个 CPU 内核。
- 对于处理器的速度没有具体建议，但速度越高，VM 应用程序的性能越优异。

内存 **(RAM)** 要求：

最低 4 GB，用于主机 Linux 内核。根据 VM 的需要添加更多内存。

硬盘要求：

计算主机 Linux 内核和 VM 的空间要求。一个 NetScaler VPX VM 需要 20 GB 磁盘空间。

软件要求

使用的主机内核必须为 64 位 Linux 内核发行版 2.6.20 或更高版本，具有所有虚拟化工具。Citrix 建议使用较新的内核，例如 3.6.11-4 及更高版本。

许多 Linux 分发版（例如 Red Hat、CentOS 和 Fedora）具有已经过测试的内核版本及关联的虚拟化工具。

来宾 **VM** 硬件要求

NetScaler VPX 支持 IDE 和 virtIO 硬盘类型。硬盘类型已作为 NetScaler 软件包的一部分在 XML 文件中配置。

网络连接要求

NetScaler VPX 支持 virtIO 半虚拟化、SR-IOV 和 PCI 直通网络接口。

有关受支持的网络接口的详细信息，请参阅：

- 使用虚拟机管理器配置 NetScaler VPX 实例
- 将 NetScaler VPX 实例配置为使用 SR-IOV 网络接口
- 将 NetScaler VPX 实例配置为使用 PCI 直通网络接口

源接口和模式

源设备类型可以是“Bridge”（桥接）或“MacVTap”。在 macvTap 中，可以使用四种模式：VEPA、桥接、私人和直通模式。检查可以使用的接口类型和支持的流量类型，如下所示：

桥接：

- Linux 桥接。
- 如果未选择正确的设置或禁用了 `IPtable` 服务，则主机 Linux 上的 `Ebtables` 和 `iptables` 设置可能会过滤网桥上的通信。

MacVTap（**VEPA** 模式）：

- 性能优于桥接。
- 可以在 VM 之间共享同一低级设备的接口。
- 则可能仅支持使用同一低级设备在 VM 内部进行通信。
- 如果上游或下游交换机支持 VEPA 模式，

MacVTap（专用模式）：

- 性能优于桥接。
- 可以在 VM 之间共享同一低级设备的接口。
- 不支持使用同一低级设备在 VM 内部进行通信。

MacVTap（桥接模式）：

- 与桥接相比，性能更优异。
- 可以在 VM 之间共享不属于同一低级设备的接口。
- 如果低级设备链接为 UP，则可以使用同一低级设备在 VM 内部进行通信。

MacVTap（直通模式）：

- 与桥接相比，性能更优异。
- 无法在 VM 之间共享不属于同一低级设备的接口。
- 只有一个 VM 可以使用低级设备。

> 注意：
>
> 为了使 VPX 实例获得最佳性能，请确保在源接口上关闭 gro 和 lro 功能。

源接口的属性

确保关闭源接口的 generic-receive-offload (gro) 和 large-receive-offload (lro) 功能。要关闭 gro 和 lro 功能，请在主机 Linux shell 提示符下运行以下命令。

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

例如：

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

                    Offload parameters for eth6:

                                        rx-checksumming: on

                                        tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

[root@localhost ~]#
```

例如：

如果主机 Linux 桥接用作源设备（如下例所示），则必须在 VNet 接口上关闭 lro 功能，这是将主机连接到来宾 MV 时使用的虚拟接口。


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

bridge name     bridge  id               STP enabled interfaces

eth6_br         8000.00e0ed1861ae          no         eth6

                                                      vnet0

                                                      vnet2

[root@localhost ~]#
```

在上例中，这两个虚拟接口是从 eth6_br 派生的，用 vnet0 和 vnet2 表示。请运行以下命令以关闭这些接口上的 gro 和 lro 功能。

```
ethtool -K vnet0 gro off
        ethtool -K vnet2 gro off
        ethtool -K vnet0 lro off
                 ethtool -K vnet2 lro off
```

混杂模式

必须为以下功能启用混杂模式，这些功能才能运行：

- L2 模式
- 多播流量处理
- 广播
- IPV6 流量
- 虚拟 MAC
- 动态路由

请使用以下命令启用混杂模式。

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

[root@localhost ~]#
```


所需的模块

为了获得更好的网络性能，请确保 Linux 主机中存在 vhost_net 模块。要检查是否存在 vhost_net 模型，请在 Linux 主机上运行以下命令：

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

如果 vhost_net 尚未运行，请输入以下命令运行该模型：

```
modprobe vhost\_net
```

使用 **OpenStack** 配置 **NetScaler VPX** 实例

October 17, 2024

您可以使用 **Nova** 启动命令（OpenStack CLI）或 Horizon（OpenStack 控制面板）在 OpenStack 环境中配置 NetScaler VPX 实例。

预配 VPX 实例（可选）涉及使用配置驱动器中的数据。配置驱动器是一个在启动时作为 CD-ROM 设备附加到实例的特殊配置驱动器。可以使用此配置驱动器来传递网络连接配置（例如管理 IP 地址、网络掩码、默认网关），以及注入客户脚本。

在 NetScaler 设备中，默认的身份验证机制是基于密码的。现在，OpenStack 环境上的 NetScaler VPX 实例支持 SSH 密钥对身份验证机制。

请先生成密钥对（公钥和私钥），然后再使用公钥加密机制。可以使用不同的机制（例如 Horizon、适用于 Windows 的 Puttygen.exe 以及适用于 Linux 的 `ssh-keygen`）生成密钥对。有关生成密钥对的详细信息，请参阅各个机制的联机文档。

有了密钥对后，将私钥复制到已获得授权的人员有权访问的安全位置。在 OpenStack 中，可以使用 Horizon 或 Nova boot 命令将公钥部署在 VPX 实例上。使用 OpenStack 预配 VPX 实例时，它会首先通过读取特定 BIOS 字符串来检测实例是否在 OpenStack 环境中引导。此字符串为 “OpenStack Foundation”，对于 Red Hat Linux 发行版，此字符串存储在 /etc/nova/release 中。这是在基于 KVM 虚拟机管理程序平台的所有 OpenStack 实现中提供的标准机制。该驱动器必须具有特定的 OpenStack 标签。

如果检测到配置驱动器，该实例会尝试读取网络配置、自定义脚本和 SSH 密钥对（如果已提供）。

用户数据文件

NetScaler VPX 实例使用自定义 OVF 文件（也称为用户数据文件）来注入网络配置和自定义脚本。此文件作为配置驱动器的一部分提供。下面是自定义 OVF 文件示例。

```
```
```

 
```

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



```
49     my $name = "VPX";
50     print "Hello, World $name !\n" ;
51                         </Text>
52                 </Script>
53                 <Script>
54                      <Type>nscli</Type>
55                      <BootScript>after</BootScript>
56                      <Text>
57                       add vlan 33
58     bind vlan 33 -ifnum 1/2
59                      </Text>
60                 </Script>
61               </Scripts>
62           </ScriptSettingSection>
63     </cs:ScriptSection>
64    </Environment>
65 ``` 在 OVF 文件中，“PropertySection”用于 NetScaler 网络配置，而 <cs:ScriptSection\> 用于封装所有脚本。 \<Scripts\>\</Scripts\> 标签用于将所有脚本捆绑在一起。 每个脚本都在 \<Script\\> \</Script\> 标签之间定义。 每个脚本标记都有以下字段/标记：
```

a) <Type>：为脚本类型指定值。可能的值：Shell/Perl/Python/NSLCI（对于 NetScaler CLI 脚本）

b) <Parameter>：为脚本提供参数。每个脚本可以有多个 <Parameter> 标签。

c) <BootScript>：指定脚本执行点。此标记的可能值：before/after。“before”指定脚本将在 PE 启动之前运行。“after”指定脚本将在 PE 启动之后运行。

d)\ <Text\ >：粘贴脚本的内容。

> 注意：
>
> 目前，VPX 实例不负责清理脚本。作为管理员，您必须检查脚本的有效性。
>
> 并非所有部分都需要存在。可使用空的“PropertySection”仅定义要在首次引导时运行的脚本，或使用空的
>
> 填充了 OVF 文件（用户数据文件）的所需部分后，使用该文件预配 VPX 实例。

网络配置

作为网络配置的一部分，VPX 实例读取：

- Management IP address（管理 IP 地址）
- Network mask（网络掩码）
- Default gateway（默认网关）

参数成功读取后，将填入 NetScaler 配置中，从而允许远程管理实例。如果参数未成功读取，或者配置驱动器不可用，实例将转换为默认行为，即：

- 实例尝试从 DHCP 中检索 IP 地址信息。
- 如果 DHCP 失败或超时，实例将提供默认网络配置 (192.168.100.1/16)。

客户脚本

VPX 实例允许在初始预配期间运行自定义脚本。该设备支持 Shell、Perl、Python 和 NetScaler CLI 命令类型的脚本。

SSH 密钥对身份验证

VPX 实例将配置驱动器中作为实例元数据的一部分提供的公钥复制到其“authorized_keys”文件中。这样，用户可以使用私钥访问实例。

> 注意：
>
> 提供 SSH 密钥后，默认凭据 (nsroot/nsroot) 将不再起作用，如果需要基于密码的访问，请使用各自的 SSH 私钥登录并手动设置密码。

开始之前的准备工作

在 OpenStack 环境中预配 VPX 实例之前，请从.tgz 文件中提取 `.qcow2` 文件，并构建

从 qcow2 映像构建 OpenStack 映像。请按照以下步骤进行操作：

1. 键入以下命令从 `.tqz` 文件中提取 `.qcow2` 文件

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

2. 键入以下命令使用在步骤 1 中提取的 `.qcoz2` 文件构建 OpenStack 映像。

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

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

图 **1**：下图提供了 glance image-create 命令的示例输出。


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

预配 **VPX** 实例

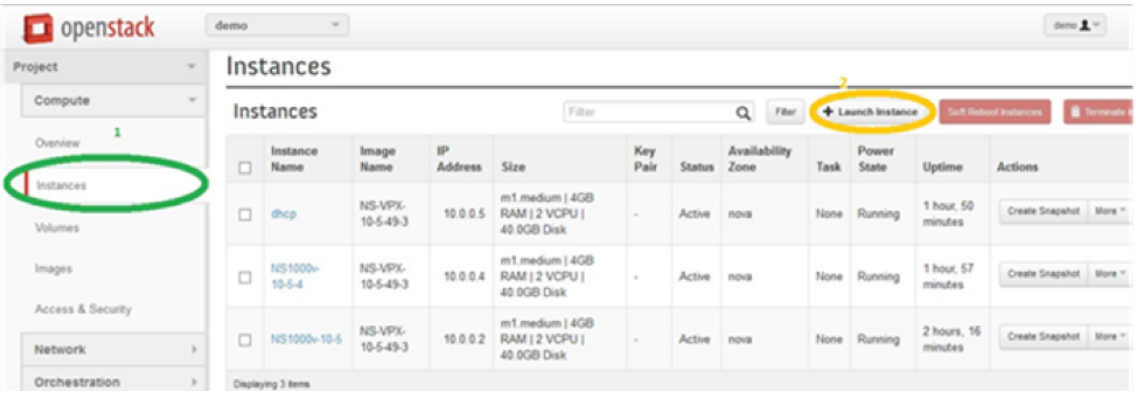
可以采用两种方式预配 VPX 实例，方法是使用以下选项之一：

- Horizon（OpenStack 控制板）
- Nova boot 命令 (OpenStack CLI)

使用 **OpenStack** 控制板预配 **VPX** 实例

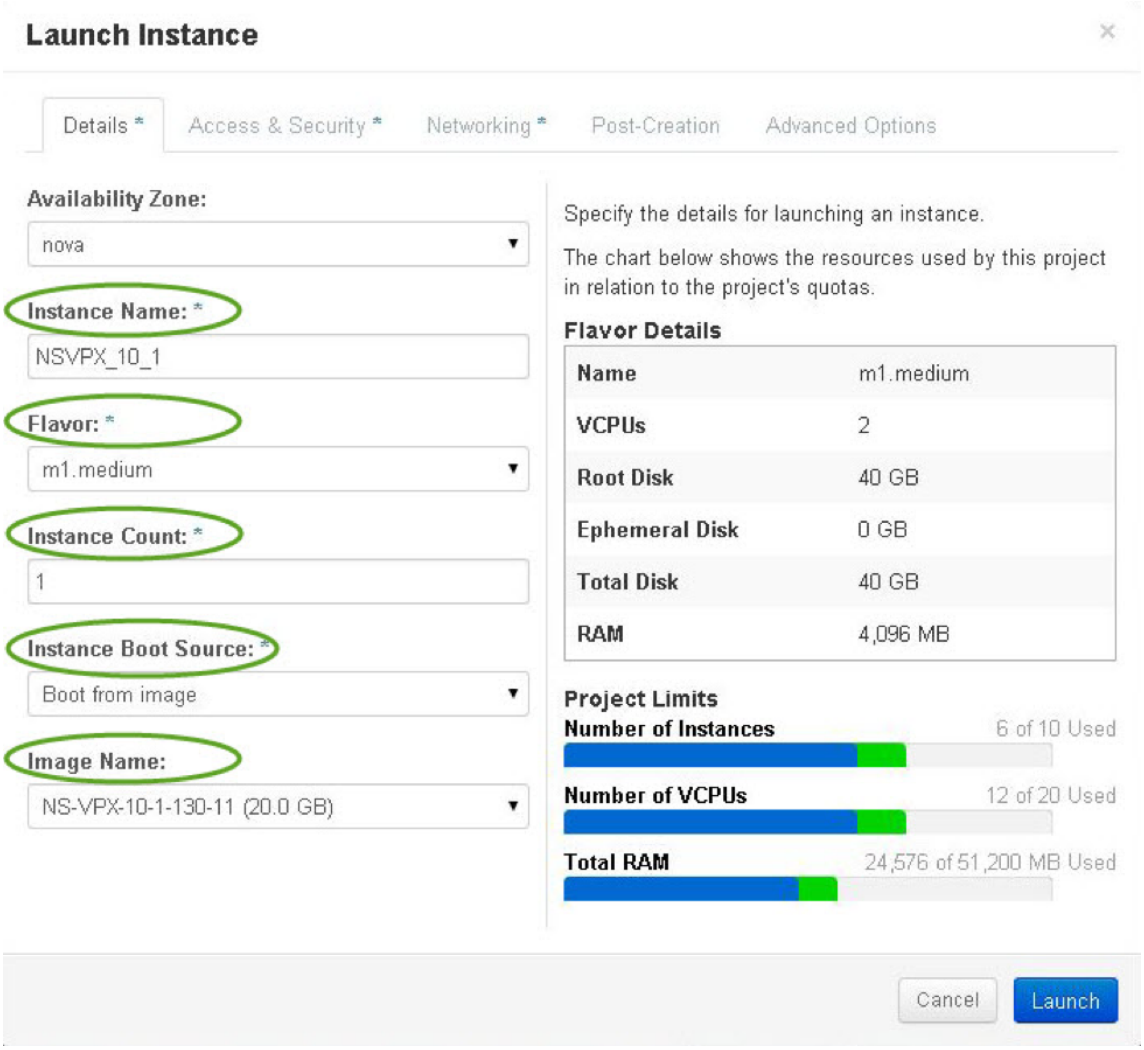
请按照以下步骤使用 Horizon 预配 VPX 实例：

1. 登录 OpenStack 控制板。
2. 在控制板左侧的“Project”（项目）面板中，选择 **Instances**（实例）。
3. 在“Instances”（实例）面板中，单击 **Launch Instance**（启动实例）打开“Instance Launching”（实例启动）向导。



4. 在“Launch Instance”（启动实例）向导中，填写详细信息，例如：

   a) Instance Name（实例名称）
   b) Instance Flavor（实例风格）
   c) Instance Count（实例计数）
   d) Instance Boot Source（实例启动源）
   e) Image Name（映像名称）



5. 完成以下步骤来通过 Horizon 部署新密钥对或现有密钥对：

   a) 如果您没有现有密钥对，请使用任何现有机制创建密钥。如果您有现有密钥，请跳过此步骤。

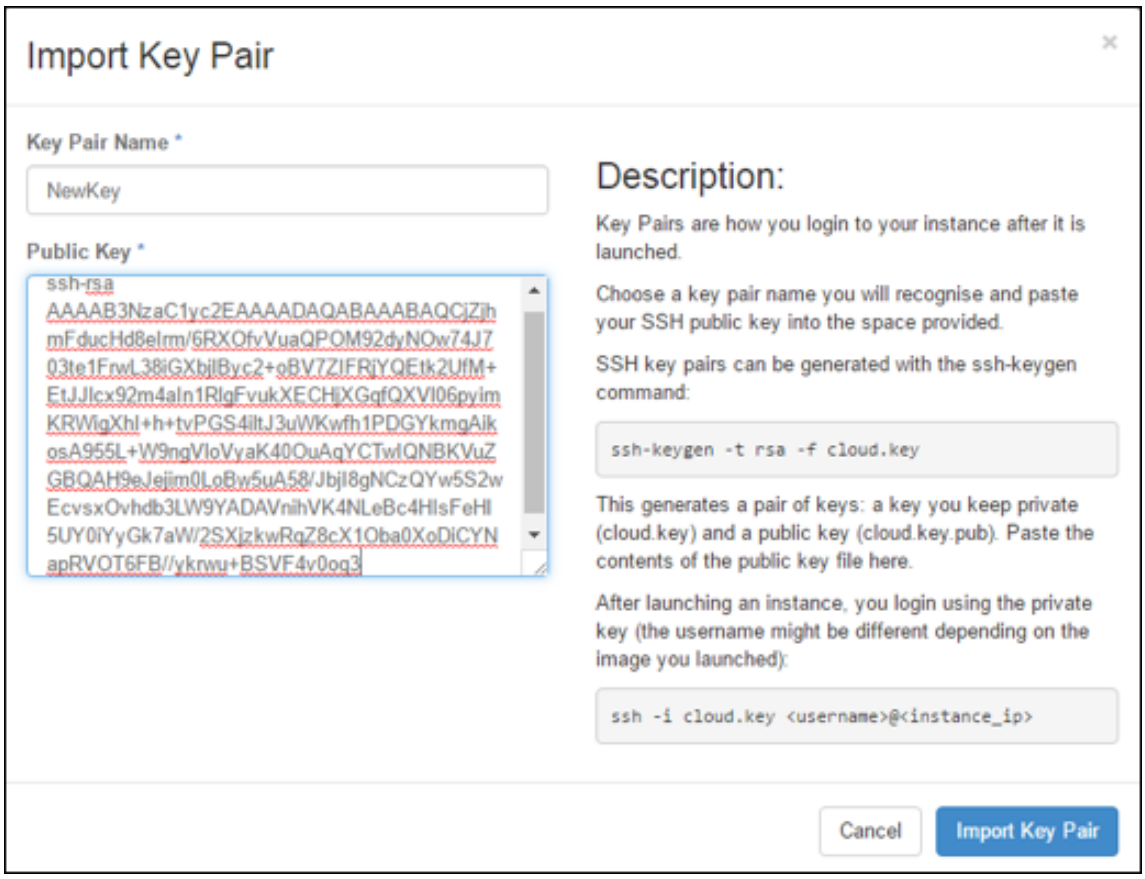
   b) 复制公钥的内容。

   c) 转到 **Horizon > Instances**（实例）**> Create New Instances**（创建新实例）。

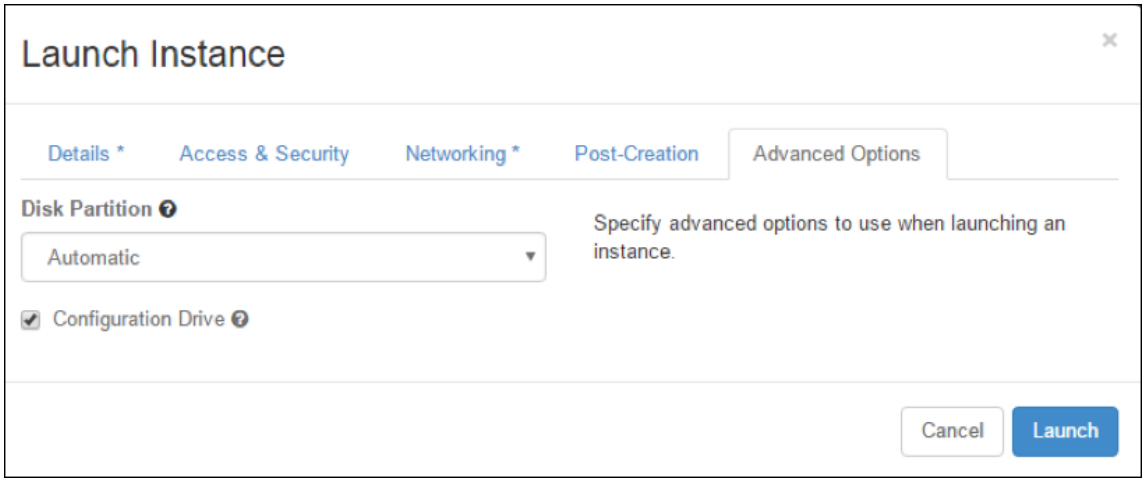
   d) 单击 **Access & Security**（访问和安全）。

   e) 单击 **Key Pair**（密钥对）下拉菜单旁边的 + 号，为所示参数提供值。

f) 在 *Public key*（公钥）框中粘贴公钥内容，为密钥提供名称，并单击 **Import Key Pair**（导入密钥对）。



6. 单击向导中的 **Post-Creation**（后期创建）选项卡。在“Customization Script”（自定义脚本）中，添加用户数据文件的内容。用户数据文件中包含 VPX 实例的 IP 地址、网络掩码和网关详细信息以及客户脚本。
7. 选择或导入密钥对后，选中“Configuration Drive”（配置驱动器），并单击 **Launch**（启动）。



使用 **OpenStack CLI** 预配 **VPX** 实例

按照以下步骤使用 OpenStack CLI 预配 VPX 实例。

1. 要从 qcow2 创建映像，请键入以下命令：

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

2. 要选择映像以创建实例，请键入以下命令：

   ```
   openstack image list | more
   ```

3. 要创建特定风格的实例，请键入以下命令从列表中选择风格 ID/名称：

   ```
   openstack flavor list
   ```

4. 要将 NIC 附加到特定网络，请键入以下命令从网络列表中选择网络 ID：

   ```
   openstack network list
   ```

5. 要创建实例，请键入以下命令：

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

图 **2**：下图提供了示例输出。

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

使用虚拟机管理器配置 **NetScaler VPX** 实例

October 17, 2024

Virtual Machine Manager 是一个用于管理 VM 来宾的桌面工具。通过此工具，您可以创建新 VM 来宾和各种类型的存储以及管理虚拟网络。可以通过内置的 VNC 查看器访问 VM 来宾的图形控制台以及本地或远程查看性能统计信息。

安装首选 Linux 发行版后，在启用了 KVM 虚拟化的情况下，可以继续置备虚拟机。

在使用虚拟机管理器配置 NetScaler VPX 实例时，有两种选择：

- 手动输入 IP 地址、网关和网络掩码
- 自动分配 IP 地址、网关和网络掩码（自动预配）

可以使用两种映像置备 NetScaler VPX 实例：

- RAW
- QCOW2

可以将 NetScaler VPX RAW 映像转换为 QCOW2 映像并置备 NetScaler VPX 实例。要将 RAW 映像转换为 QCOW2 映像，请键入以下命令：

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

例如：


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

KVM 上的典型 NetScaler VPX 部署包括以下步骤：

- 检查自动置备 NetScaler VPX 实例的必备条件
- 使用 RAW 映像置备 NetScaler VPX 实例
- 使用 QCOW2 映像 Provisioning NetScaler VPX 实例
- 使用 Virtual Machine Manager 向 VPX 实例添加其他接口

检查自动配置 **NetScaler VPX** 实例的先决条件

自动置备是一项可选功能，它涉及使用 CDROM 驱动器中的数据。如果启用了此功能，则不必在初始设置期间输入 NetScaler VPX 实例的管理 IP 地址、网络掩码和默认网关。

需要先完成以下任务，才能自动预配 VPX 实例：

1. 创建自定义开放虚拟化格式 (OVF) XML 文件或用户数据文件。
2. 使用联机应用程序（例如 PowerISO）将 OVF 文件转换为 ISO 映像。
3. 使用任何基于安全复制 (SCP) 的工具在 KVM 主机上装载 ISO 映像。

示例 **OVF XML** 文件：

下面是 OVF XML 文件内容示例，您可以将其用作示例来创建您的文件。

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

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

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

oe:id=""

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

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>
```



```
26
27    <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
28
29    <Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
30
31    <Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>
32
33    <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"
         />
34
35    <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
         255.255.255.0"/>
36
37    <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
         10.1.2.1"/>
38
39    </PropertySection>
40
41    </Environment>
```

在上面的 OVF XML 文件中，“PropertySection”用于 NetScaler 网络配置。创建该文件时，请为示例结尾处突出显示的参数指定值：

- Management IP address（管理 IP 地址）
- 网络掩码
- 网关

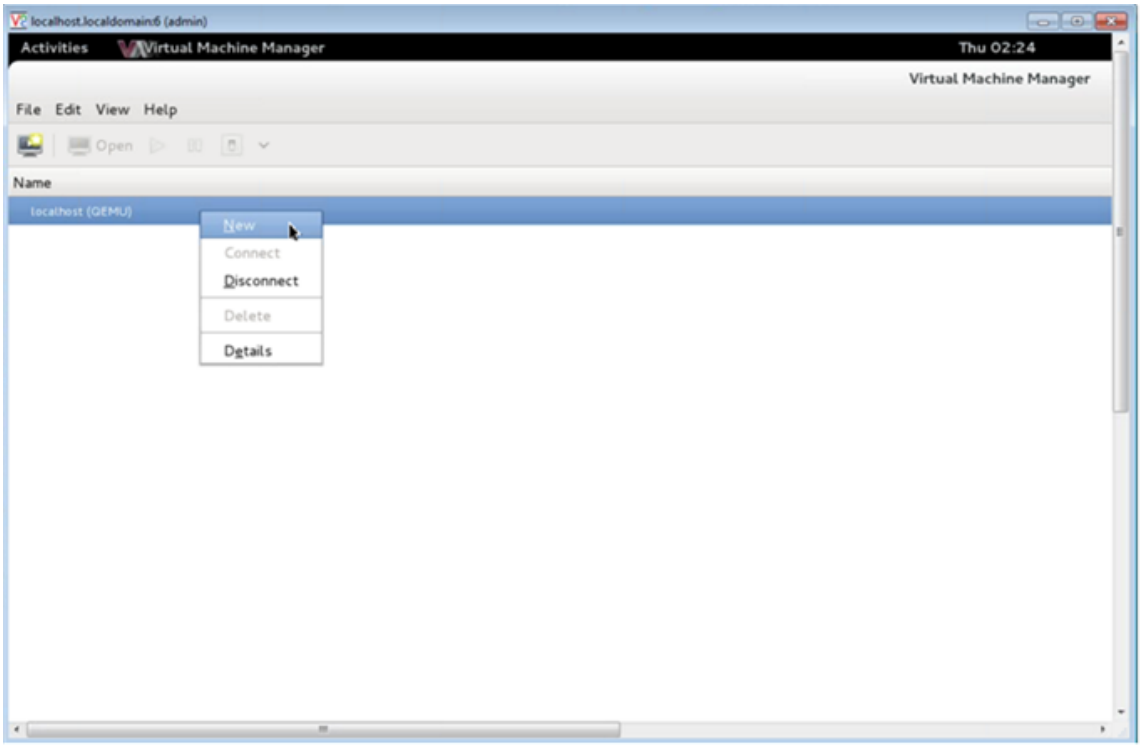
> 重要
>
> 如果 OVF 文件不是格式正确的 XML，则系统会为 VPX 实例分配默认网络配置，而不是该文件中指定的值。

使用 **RAW** 图像配置 **NetScaler VPX** 实例

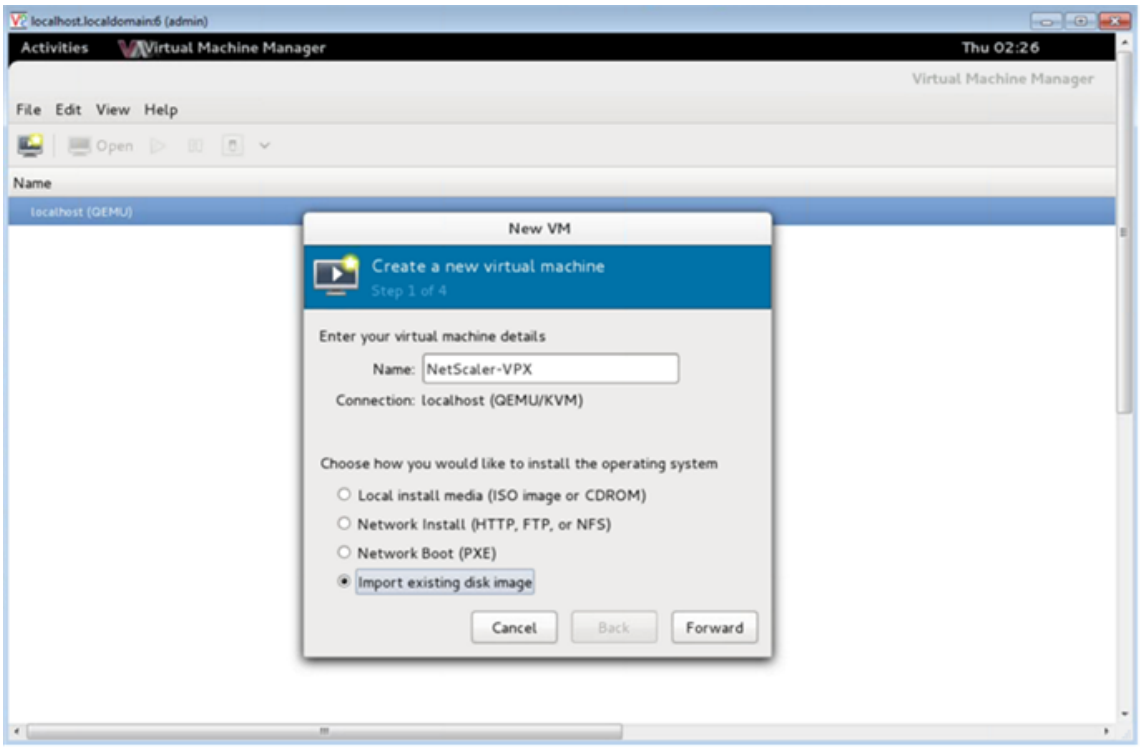
通过 Virtual Machine Manager 可以使用 RAW 映像置备 NetScaler VPX 实例.

要使用虚拟机管理器配置 NetScaler VPX 实例，请执行以下步骤：

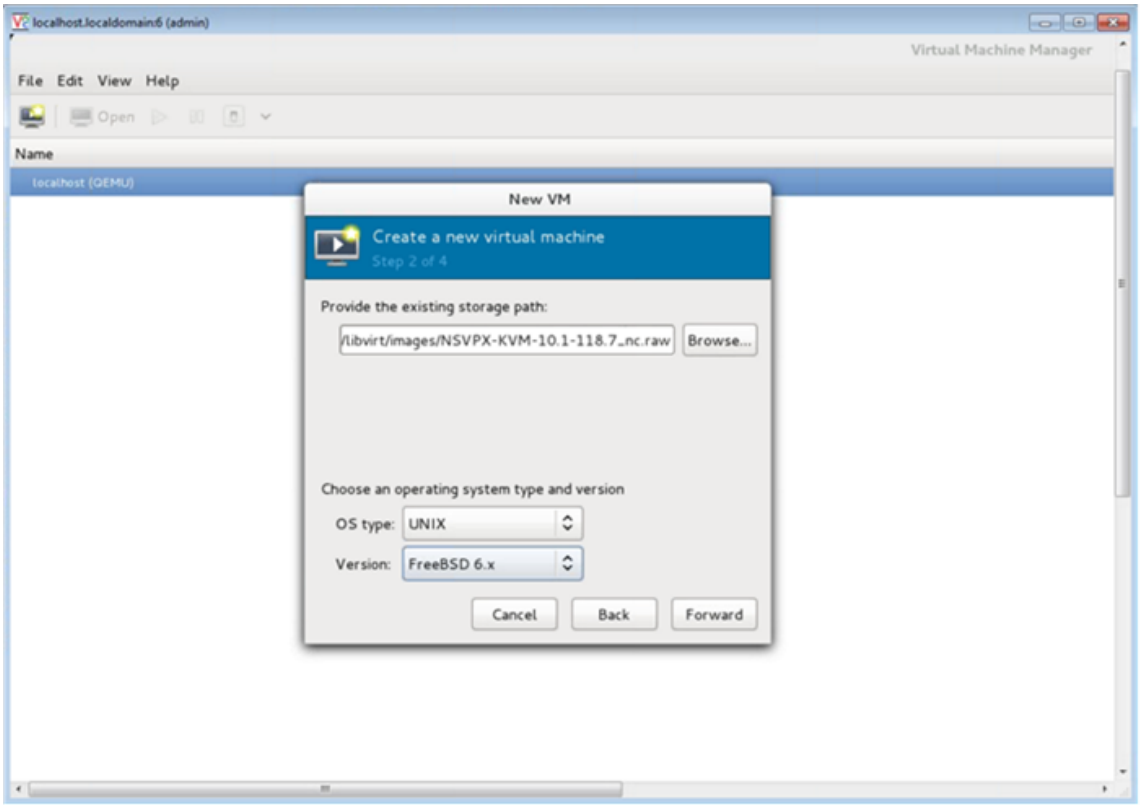
1. 打开 Virtual Machine Manager**[Application**（应用程序）> **System Tools**（系统工具）> **Virtual Machine Manager]**，然后在 **Authenticate**（身份验证）窗口中输入登录凭据。
2. 单击  图标或右键单击 **localhost (QEMU)** 创建新的 NetScaler VPX 实例。



3. 在 **Name**（名称）文本框中，输入新 VM 的名称（例如，NetScaler-VPX）。
4. 在 **New VM**（新建 VM）窗口中的“Choose how you would like to install the operating system”（选择您希望安装操作系统的方式）下，选择 **Import existing disk image**（导入现有磁盘映像），然后单击 **Forward**（转发）。

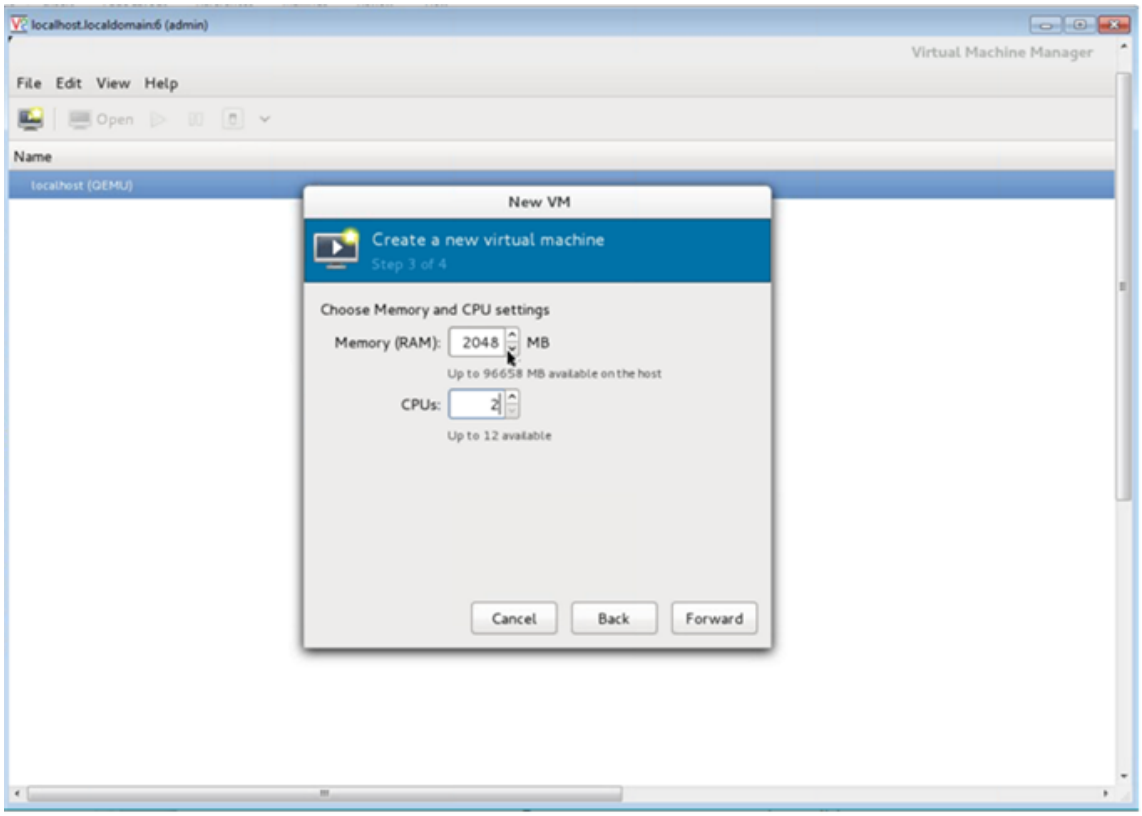


5. 在 **Provide the existing storage path**（提供现有存储路径）字段中，导航到映像的路径。选择操作系统类型“UNIX”，选择版本“FreeBSD 6.x”。然后，单击 **Forward**（转发）。

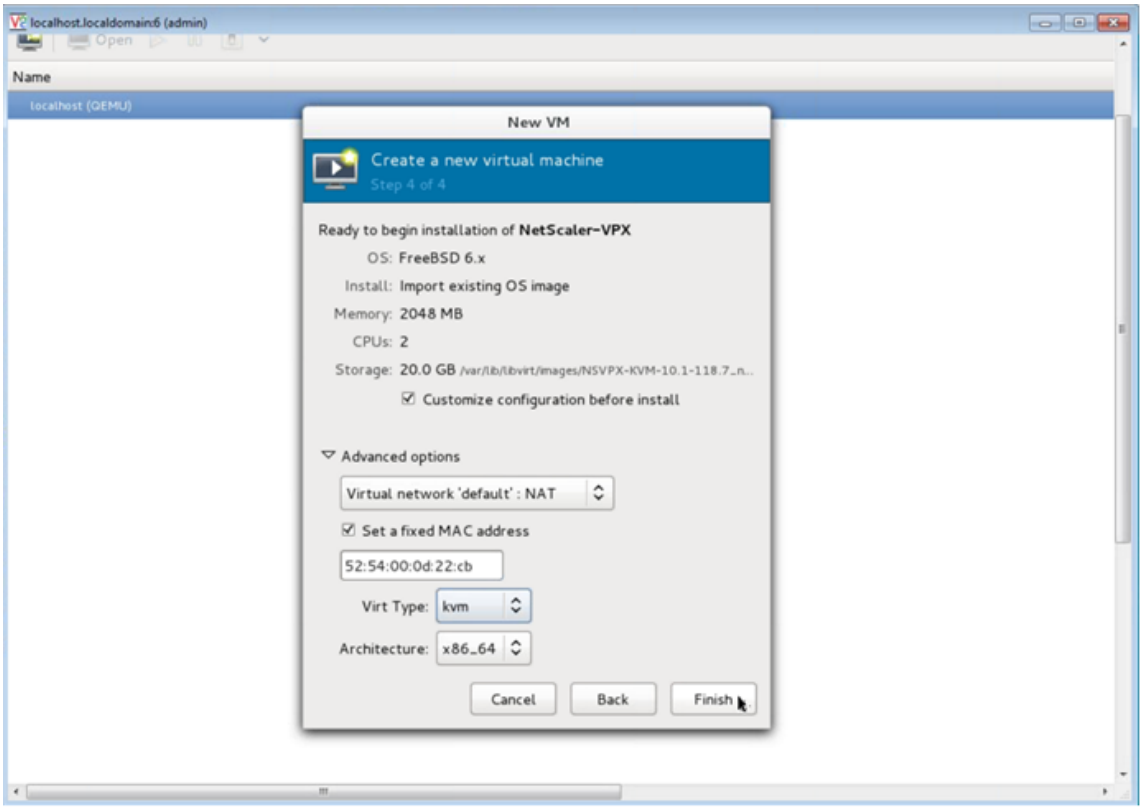


6. 在 **Choose Memory and CPU**（选择内存和 CPU）设置下，选择以下设置，然后单击 **Forward**（下一步）：

   - Memory (RAM)（内部 (RAM)）- 2048 MB
   - CPUs（CPU 数）- 2

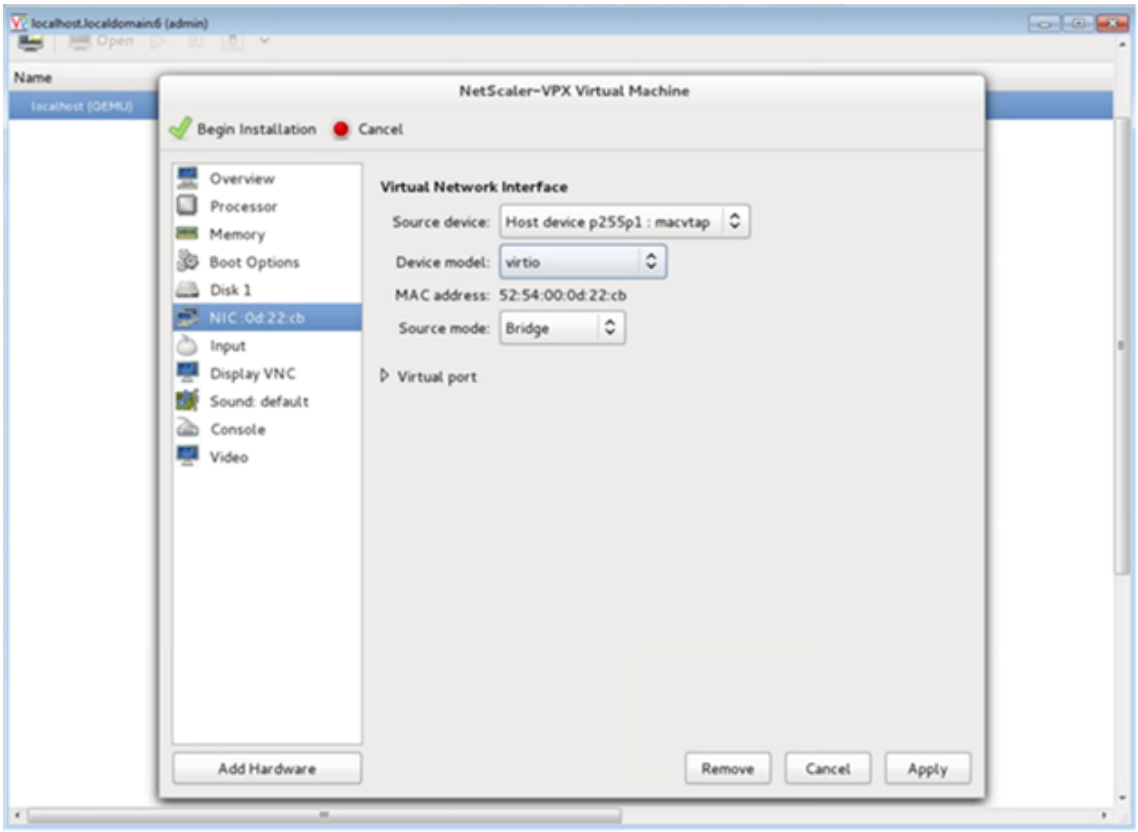


7. 选中 **Customize configuration before install**（安装前自定义配置）复选框。也可以在 **Advanced options**（高级选项）下自定义 MAC 地址。请确保所选 **Virt Type**（虚拟类型）为 KVM，所选 “Architecture”（体系结构）为 x86_64。单击完成。



8. 选择 NIC 并提供以下配置：

   - 源设备 - `ethX macvtap` 或桥接
   - 设备型号 - `virtio`
   - Source mode（源模式）- Bridge（桥接）



9. 单击应用。
10. 如果您要自动置备 VPX 实例，请参阅本文档中的通过附加 **CDROM** 驱动器启用自动预配部分。否则，请单击 **Begin Installation**（开始安装）。在 KVM 上配置 NetScaler VPX 后，您可以添加更多接口。

使用 **QCOW2** 映像配置 **NetScaler VPX** 实例

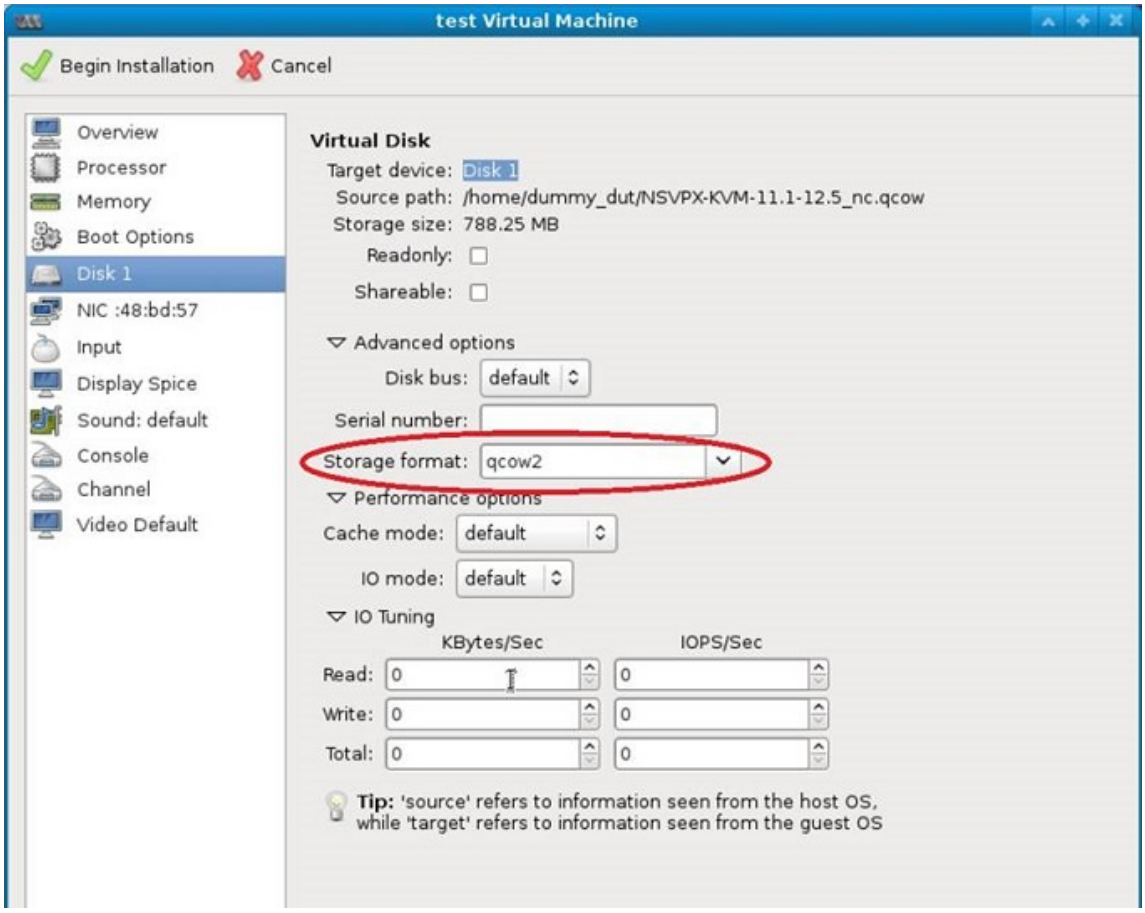
使用虚拟机管理器，您可以使用 QCOW2 映像配置 NetScaler VPX 实例。

要使用 QCOW2 映像预配 NetScaler VPX 实例，请按照以下步骤进行操作：

1. 按照 使用 RAW 映像预配 NetScaler VPX 实例中的步骤 1 到步骤 **8**。

   > 注意：
   >
   > 确保在 步骤 **5** 中选择了 **qcow2** 图像。

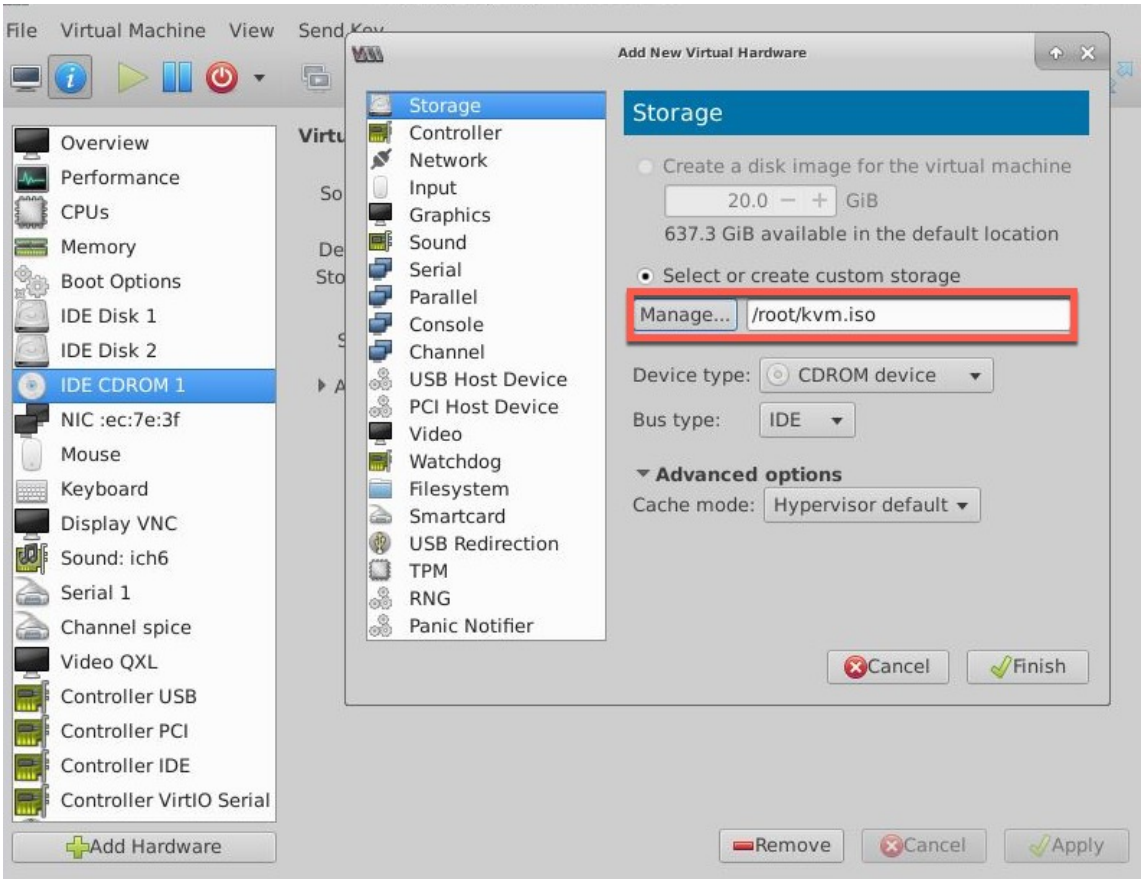
2. 选择 **Disk 1**（磁盘 1），并单击 **Advanced options**（高级选项）。
3. 从“Storage format”（存储格式）下拉列表中选择 **qcow2**。



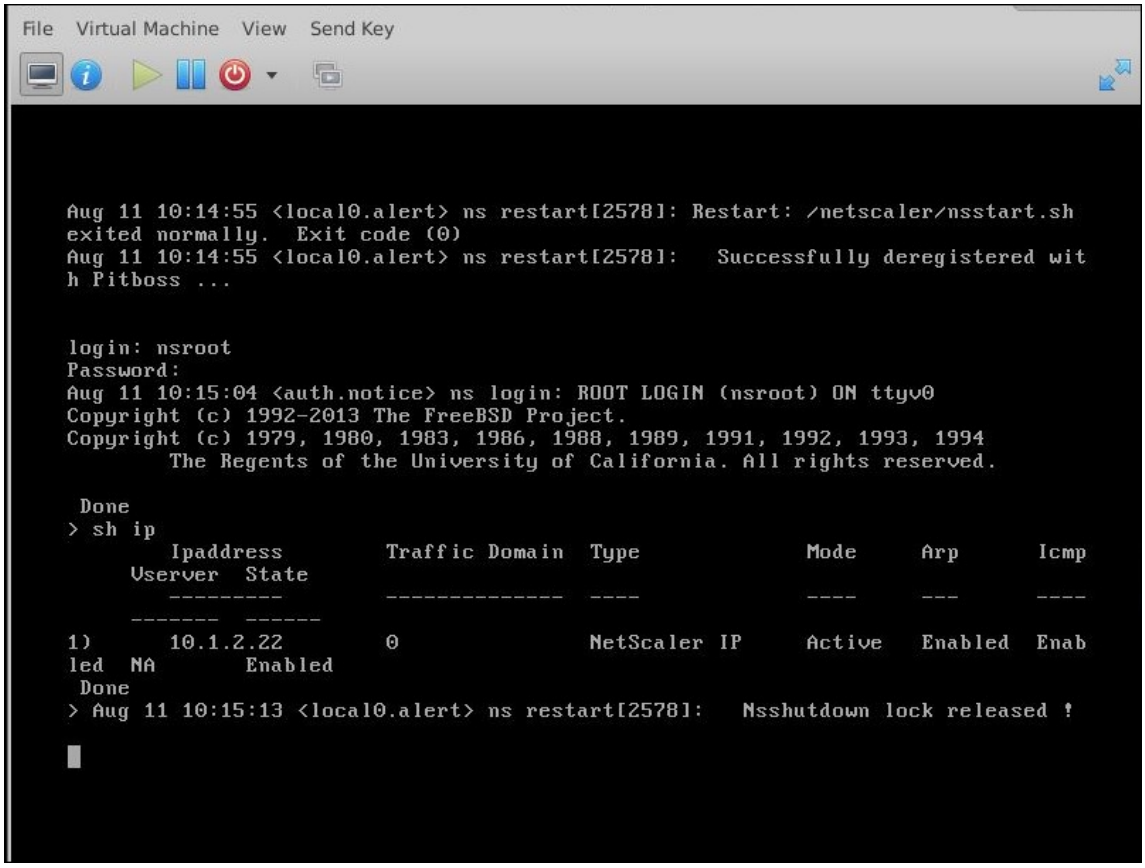
4. 单击 **Apply**（应用），然后单击 **Begin Installation**（开始安装）。在 KVM 上配置 NetScaler VPX 后，您可以添加更多接口。

通过附加 **CDROM** 驱动器启用自动预配

1. 依次单击 **Add Hardware**（添加硬件）**> Storage**（存储）**> Device type**（设备类型）**> CDROM device**（**CDROM** 设备）。
2. 单击“管理”，在“自动 **Provisioning NetScaler VPX** 实例的先决条件”部分中选择您安装的正确 **ISO** 文件，然后单击“完成”。即在 NetScaler VPX 实例上的“Resources”（资源）下创建一个新的 CDROM。



3. 打开 VPX 实例，它将使用 OVF 文件中提供的网络配置进行自动置备，如示例屏幕截图中所示。



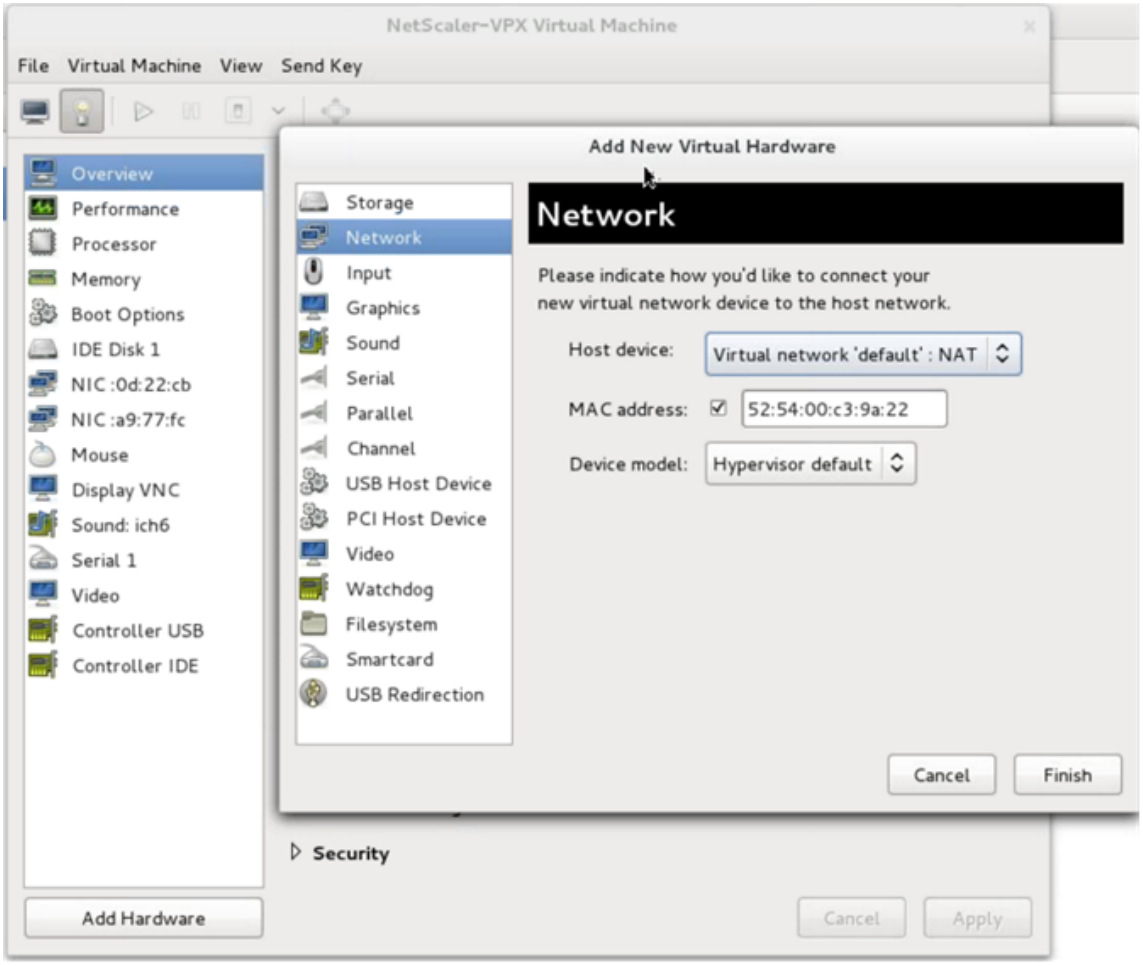
4. 如果自动预配失败，实例将提供默认 IP 地址 (192.168.100.1)。在该示例中，您必须手动完成初始配置。有关更多信息，请参阅 首次配置 ADC。

使用 **Virtual Machine Manager** 将更多接口添加到 **NetScaler VPX** 实例

在 KVM 上预配 NetScaler VPX 实例后，可以添加其他接口。

要添加更多接口，请按照以下步骤进行操作。

1. 关闭 KVM 上运行的 NetScaler VPX 实例。
2. 右键单击 VPX 实例，然后从弹出菜单中选择 **Open**（打开）。
3. 单击标题中的图  图标可查看虚拟硬件详细信息。
4. 单击 **Add Hardware**（添加硬件）。在 **Add New Virtual Hardware**（添加新虚拟硬件）窗口中，从导航菜单中选择 **Network**（网络）。



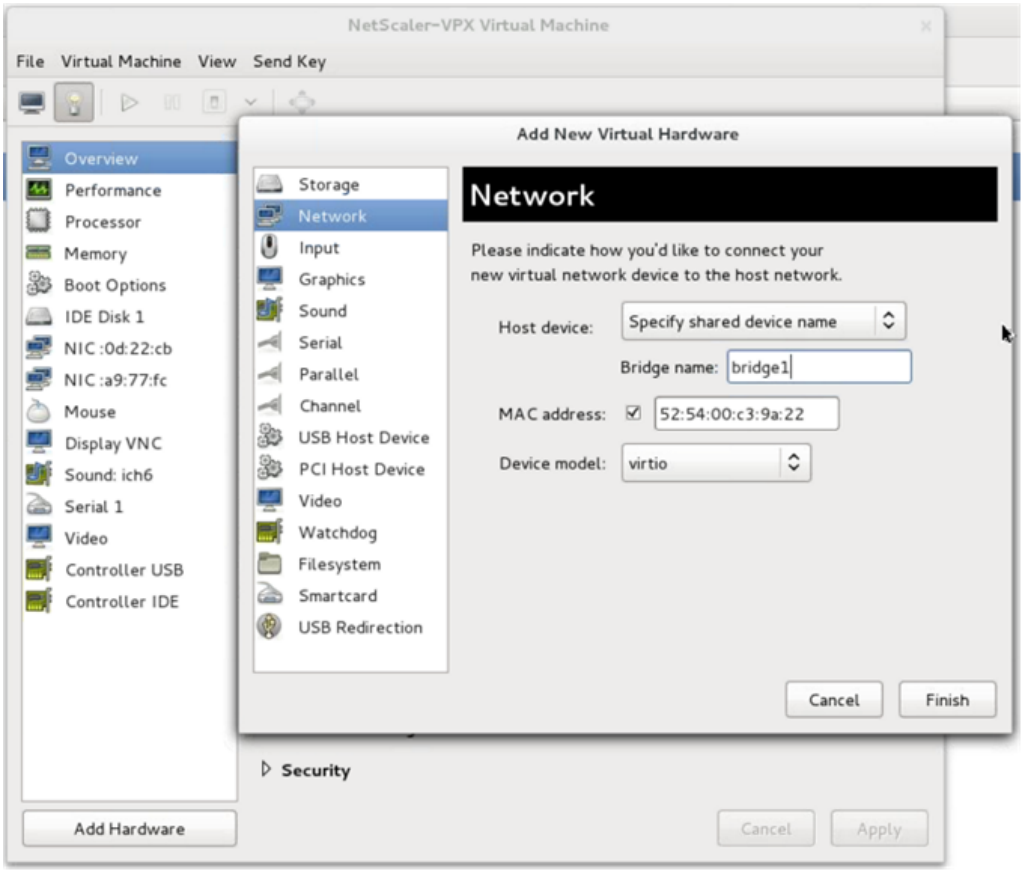
5. 在 **Host Device**（主机设备）字段中，选择物理接口类型。主机设备类型可以是 “Bridge”（桥接）或 “MacVTap”。如果是 “MacVTap”，则四种可能的模式为 “VEPA”、“Bridge”（桥接）、“Private”（专用）和 “Pass-through”（直通）。

   a) 对于 “Bridge”（桥接）

      i. Host device（主机设备）- 选择 “Specify shared device name”（指定共享设备名称）选项。

      ii. 提供在 KVM 主机中配置的桥接名称。

      > 注意：
      >
      > 确保您已在 KVM 主机中配置了 Linux 桥接器、将物理接口绑定到桥接器、并将桥接器置于 UP 状态。



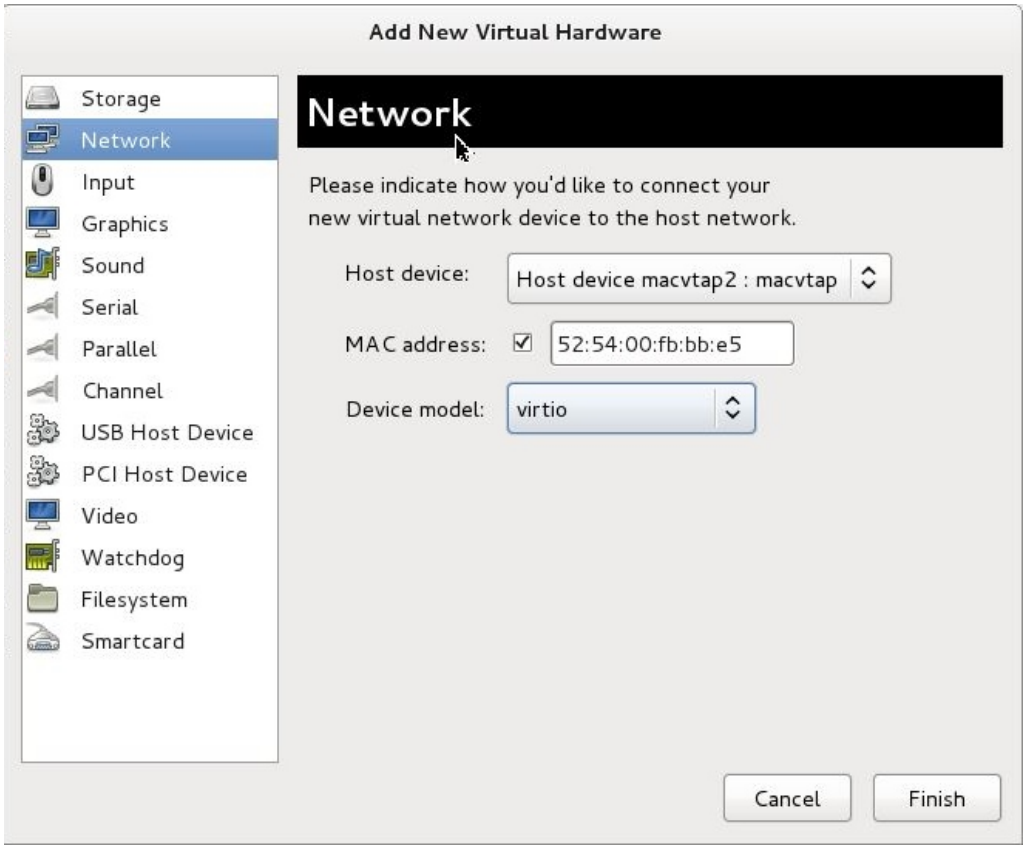
iii. 设备型号 - `virtio`。

iv. 单击完成。

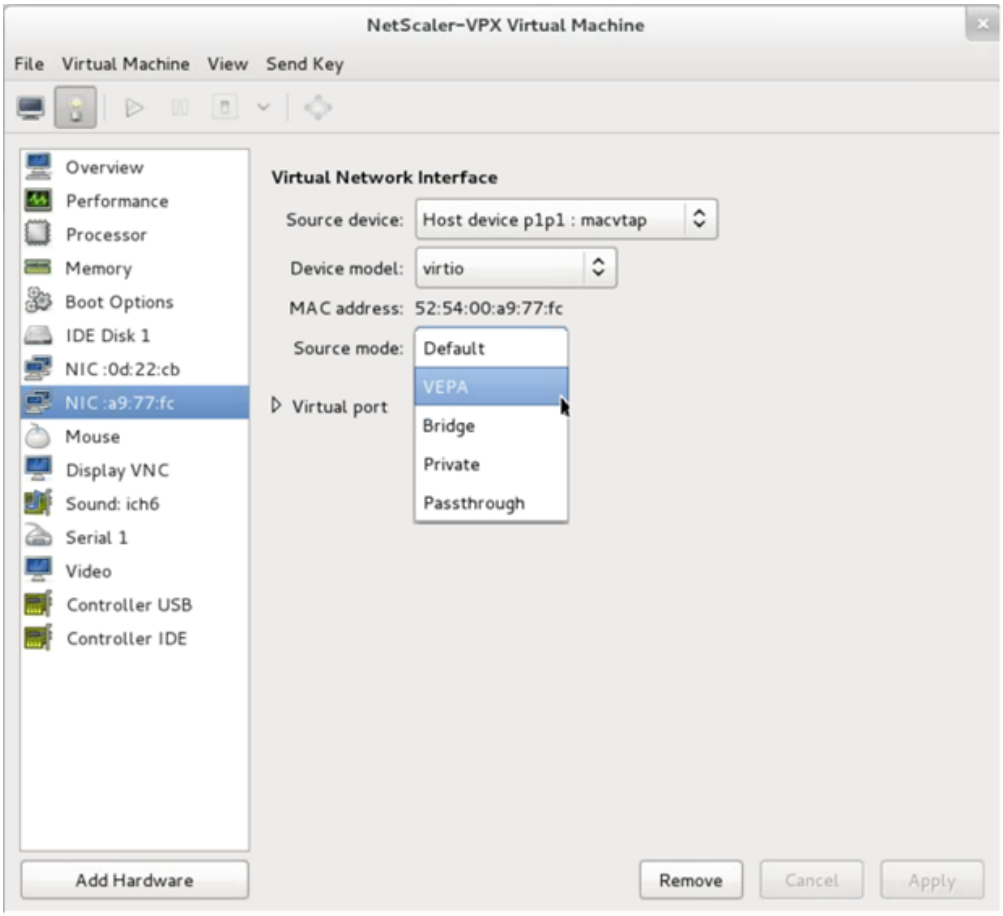
b) 适用于 MacVTap

i. Host device（主机设备）- 从菜单中选择物理接口。

ii. 设备型号 - `virtio`。



iii. 单击完成。可以在导航窗格中查看新添加的 NIC。



iv. 选择新添加的 NIC，然后为此 NIC 选择源模式。可用模式为 “VEPA”、“Bridge”（桥接）、“Private”（专用）和 “Passthrough”（直通）。有关接口和模式的更多详细信息，请参阅 “源接口和模式”。

v. 单击应用。

6. 如果您要自动置备 VPX 实例，请参阅本文档中的 “添加配置驱动器以启用自动置备” 一节。否则，请打开 VPX 实例以手动完成初始配置。

> 重要：
>
> 不支持速度、双工和自动协商等接口参数配置。

将 **NetScaler VPX** 实例配置为使用 **SR-IOV** 网络接口

October 17, 2024

您可以使用以下 NIC 使用单根 I/O 虚拟化 (SR-IOV) 配置在 Linux-KVM 平台上运行的 NetScaler VPX 实例：

- Intel 82599 10G

- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

本节将介绍如何：

- 将 NetScaler VPX 实例配置为使用 SR-IOV 网络接口
- 在 SR-IOV 接口上配置静态 LA/LACP
- 在 SR-IOV 接口上配置 VLAN

限制

使用 Intel 82599 NIC、X710 NIC、XL710 NIC 和 X722 NIC 时请注意一些限制。不支持以下功能。

Intel 82599 NIC 的限制：

- L2 模式切换。
- 管理分区（共享 VLAN 模式）。
- 高可用性（主动-主动模式）。
- 巨型帧.
- IPv6：如果您至少有一个 SR-IOV 接口，则在 VPX 实例中最多只能配置 30 个唯一的 IPv6 地址。
- 不支持通过 `ip link` 命令在适用于 SRIOV VF 接口的虚拟机管理程序上对 VLAN 所做的配置。
- 不支持速度、双工和自动协商等接口参数配置。

Intel X710 10G、**Intel XL710 40G** 和 **Intel X722 10G NIC** 的限制：

- L2 模式切换。
- 管理分区（共享 VLAN 模式）。
- 在群集中，XL710 NIC 用作数据接口时，不支持巨型帧。
- 接口断开连接并重新连接时，接口列表会重新排序。
- 不支持速度、双工和自动协商等接口参数配置。
- Intel X710 10G、Intel XL710 40G 和 Intel X722 10G NIC 的接口名称为 40/X
- 在 VPX 实例上，最多可以支持 16 个 Intel XL710/X710/X722 SRIOV 或 PCI 直通接口。

> 注意：
>
> 为了使 Intel X710 10G、Intel XL710 40G 和 Intel X722 10G NIC 支持 IPv6，您需要通过在 KVM 主机上键入以下命令在虚拟功能 (VF) 上启用信任模式：
>
> ```
> # ip link set <PNIC> <VF> trust on
> ```
>
> Example:
>
> ```
> # ip link set ens785f1 vf 0 trust on
> ```


必备条件

在将 NetScaler VPX 实例配置为使用 SR-IOV 网络接口之前，请完成以下先决条件任务。有关如何完成相应任务的详细信息，请参阅 NIC 列。

任务	Intel 82599 NIC	Intel X710、XL710 和 X722 NIC
1. 将 NIC 添加到 KVM 主机。	-	-
2. 下载并安装最新的英特尔驱动程序。	IXGBE 驱动程序	I40E 驱动程序
1. 将 KVM 主机上的驱动程序列入阻止名单。	在 /etc/modprobe.d/blacklist.conf 文件中添加以下条目：`blacklist ixgbevf`。使用 IXGBE 驱动程序版本 4.3.15（建议）。如果使用的是 3.8 版之前的内核，请向 /etc/modprobe.d/ixgbe 文件中添加以下条目并重新启动 KVM 主机：`options ixgbe max_vfs=<number_of_VFs>`。如果使用的是内核 3.8 版或更高版本，请使用以下命令创建 VF：`echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`。请参阅图 1 中的示例。	在 /etc/modprobe.d/blacklist.conf 文件中添加以下条目：`blacklist i40evf`。使用 i40e 驱动程序版本 2.0.26（建议）。如果使用的是 3.8 版之前的内核，请向 /etc/modprobe.d/i40e.conf 文件中添加以下条目并重新启动 KVM 主机：`options i40e max_vfs=<number_of_VFs>`。如果使用的是内核 3.8 版或更高版本，请使用以下命令创建 VF：`echo<number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`。请参阅图 2 中的示例。
1. 在 KVM 主机上启用 SR-IOV 虚拟功能 (VF)。在接下来两列中的两个命令中：`number_of_VFs` = 要创建的虚拟 VF 的数量。`device_name` = 接口名称。	请参阅图 3 中的示例。	请参阅图 3 中的示例。
1. 通过将用于创建 VF 的命令添加到 rc.local 文件，使 VF 持久化。		

> 重要：
>
> 创建 SR-IOV VF 时，请务必不要将 MAC 地址分配给 VF。

图 **1**：在 KVM 主机上为 Intel 82599 10G NIC 启用 SR-IOV VF。

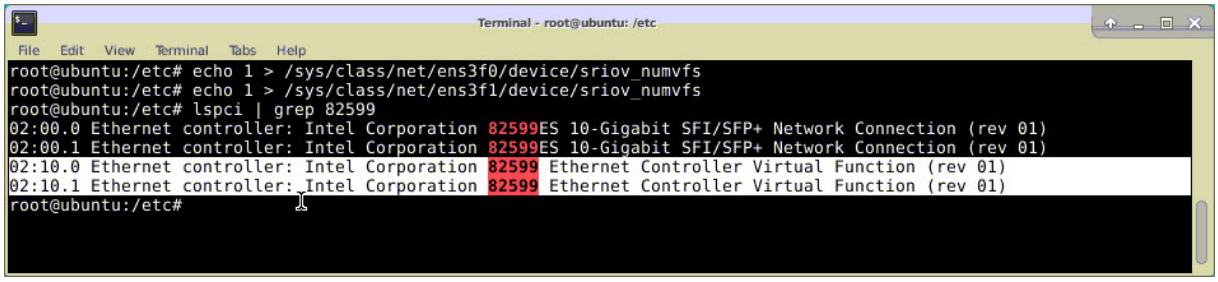


图 **2**：在 KVM 主机上为 X710 10G NIC 和 XL710 40G NIC 启用 SR-IOV VF。

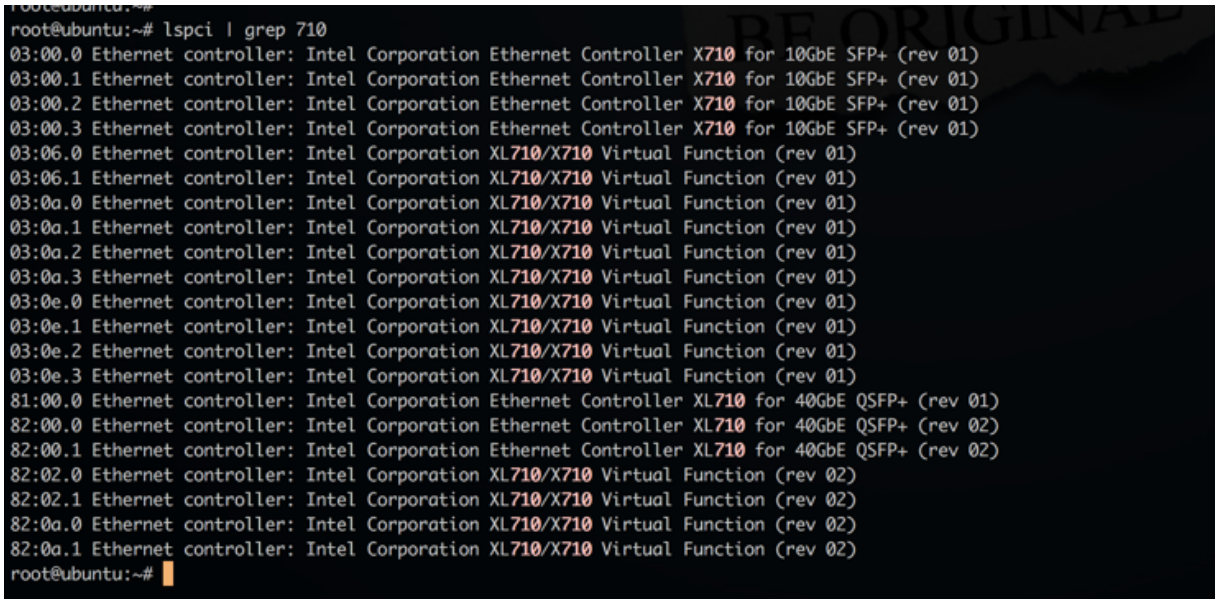


图 **3**：为 Intel X722 10G NIC 启用 KVM 主机上的 SR-IOV VF。

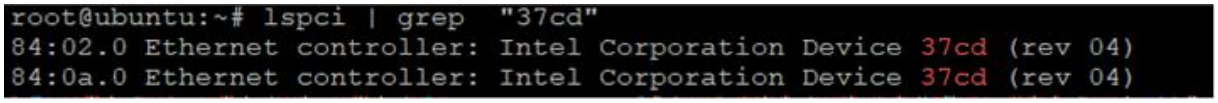
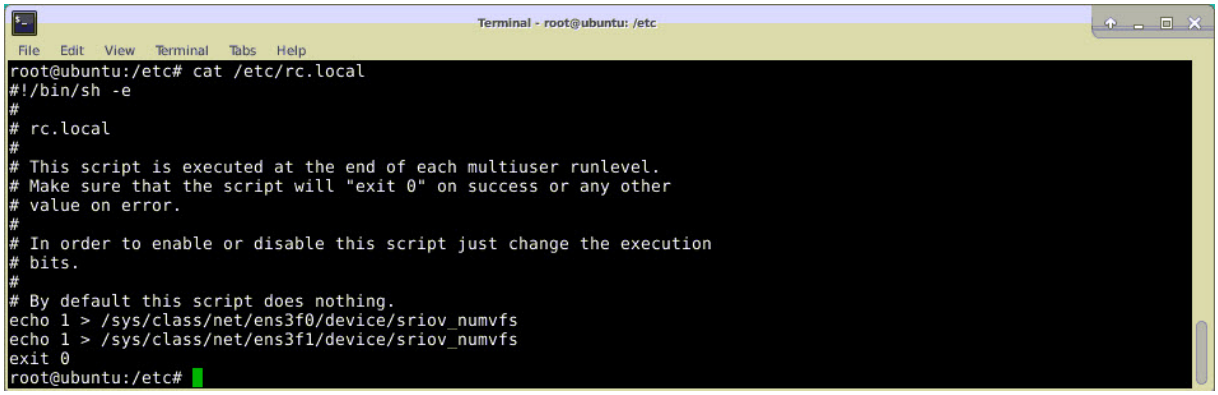


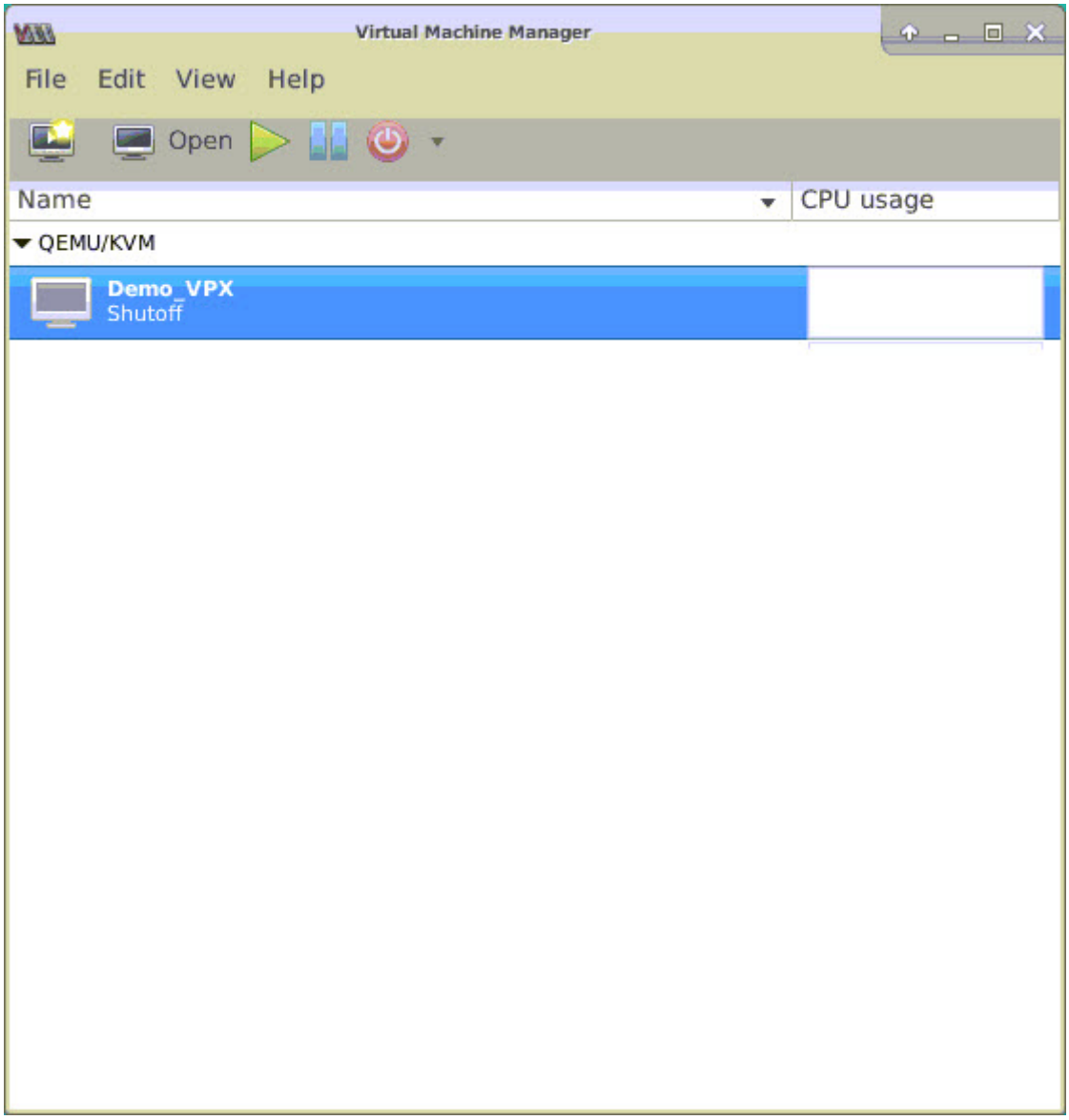
图 **4**：将 VF 设为永久存在。



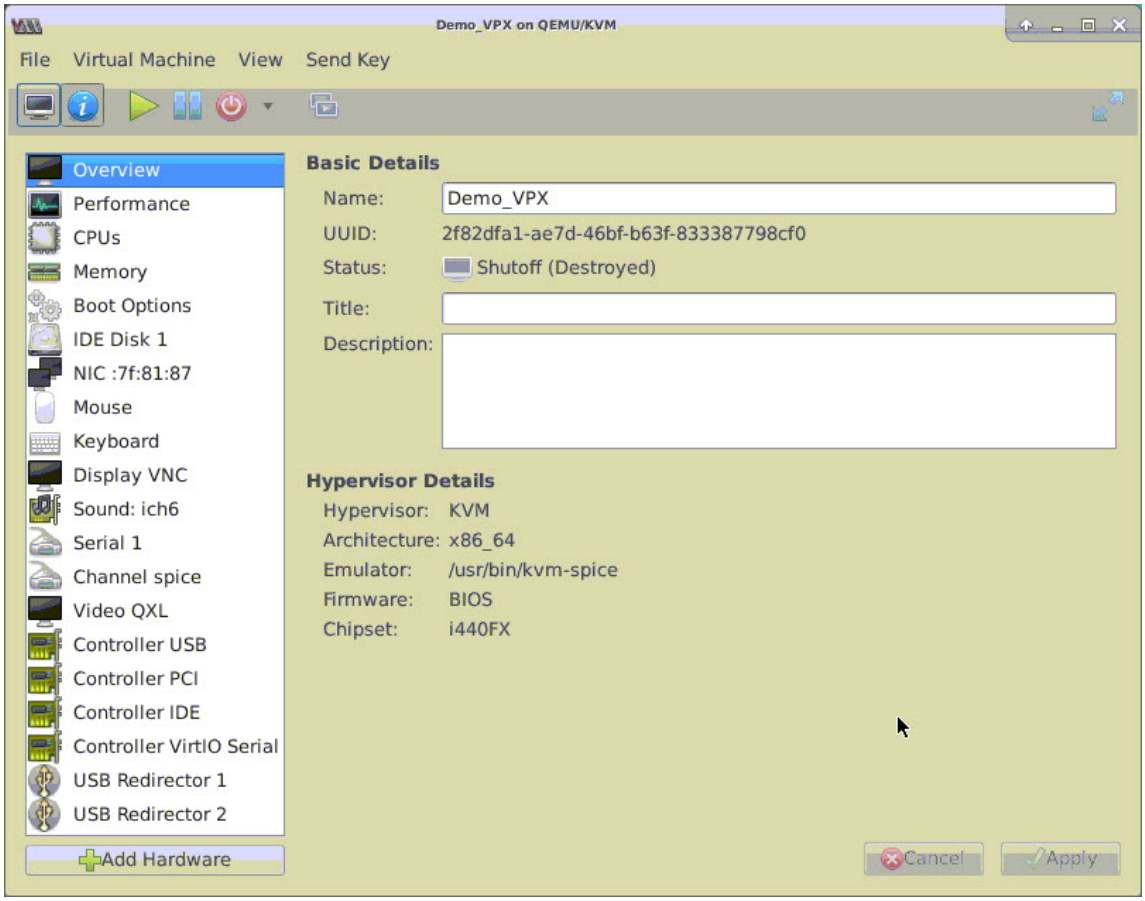
将 **NetScaler VPX** 实例配置为使用 **SR-IOV** 网络接口

要使用虚拟机管理器将 NetScaler VPX 实例配置为使用 SR-IOV 网络接口，请完成以下步骤：

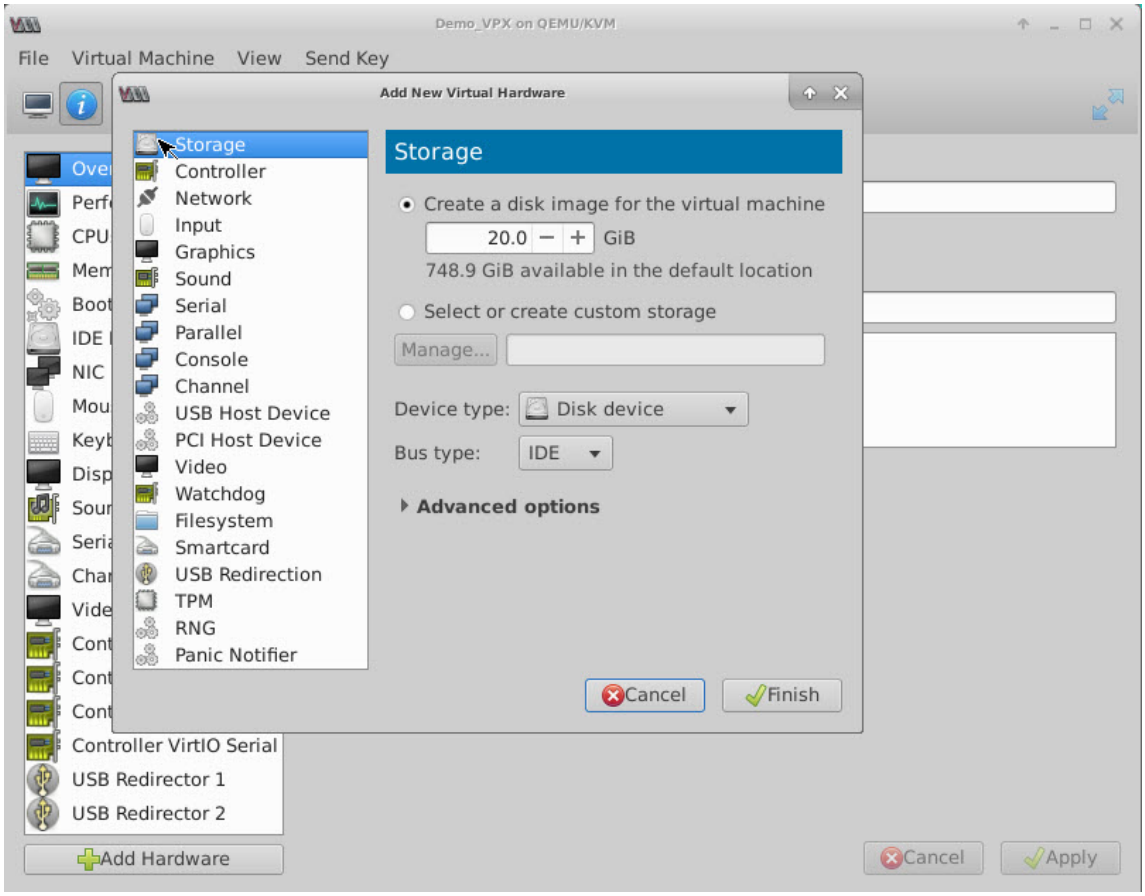
1. 关闭 NetScaler VPX 实例的电源。
2. 选择 NetScaler VPX 实例，然后选择“Open”（打开）。



3. 在 <virtual machine on KVM> 窗口中，选择 **i** 图标。



4. 选择 **Add Hardware**（添加硬件）。



5. 在 **Add New Virtual Hardware**（添加新虚拟硬件）对话框中，执行以下操作：

   a) 选择“PCI Host Device”（PCI 主机设备）。

   b) 在“Host Device”（主机设备）部分中，选择所创建的 VF，然后单击“Finish”（完成）。

图 **4**：82599 10G NIC 的 VF

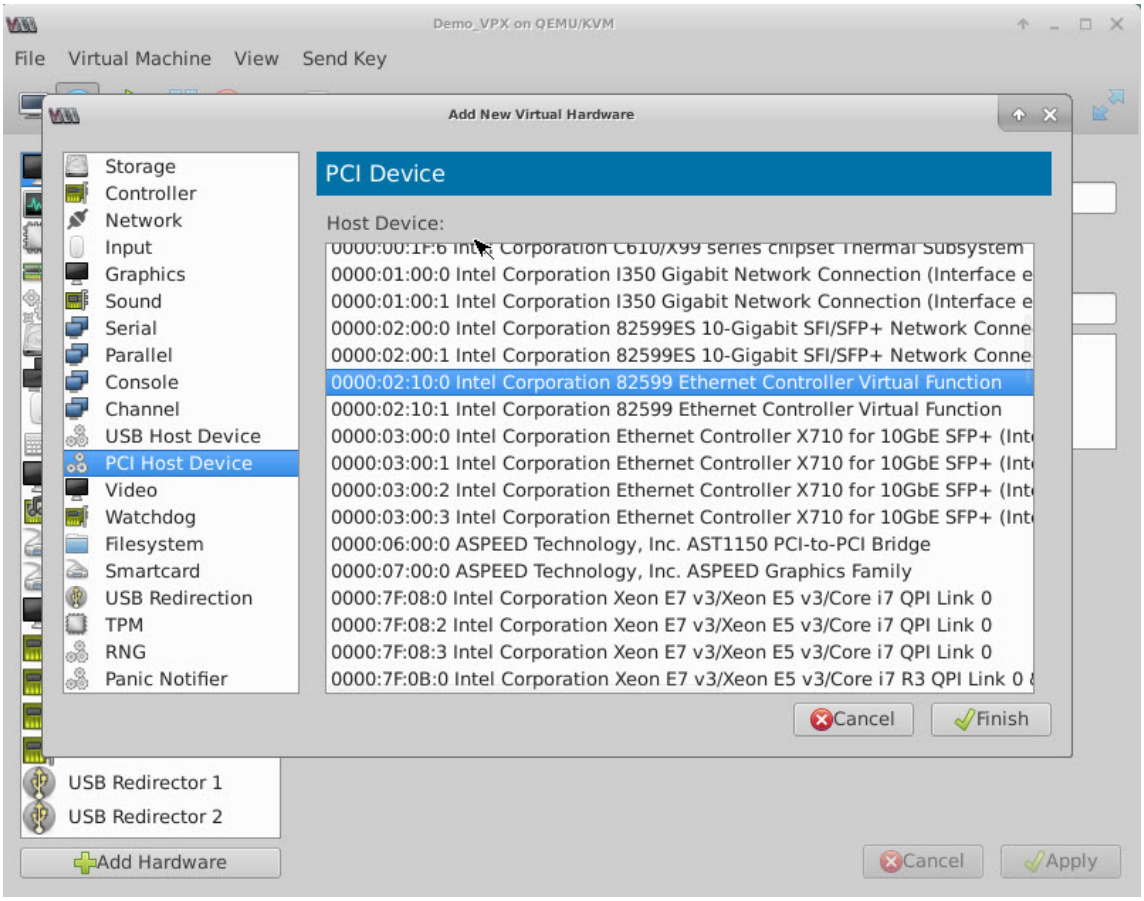


图 **5**：适用于 Intel XL710 40G NIC 的 VF

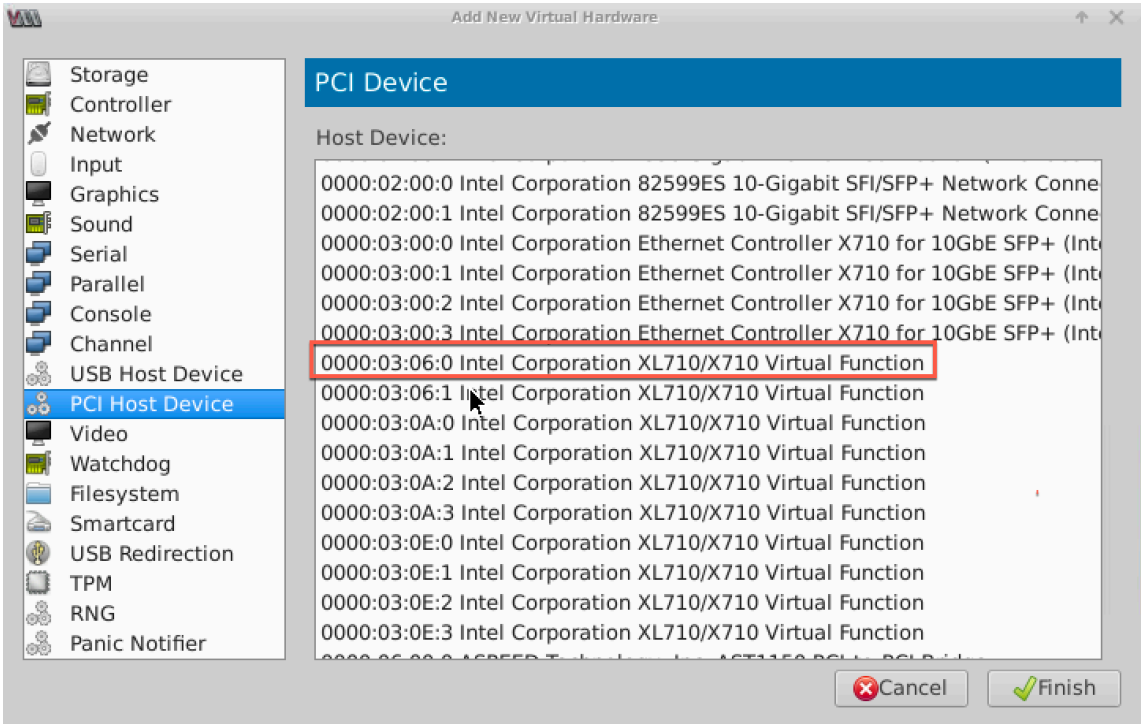
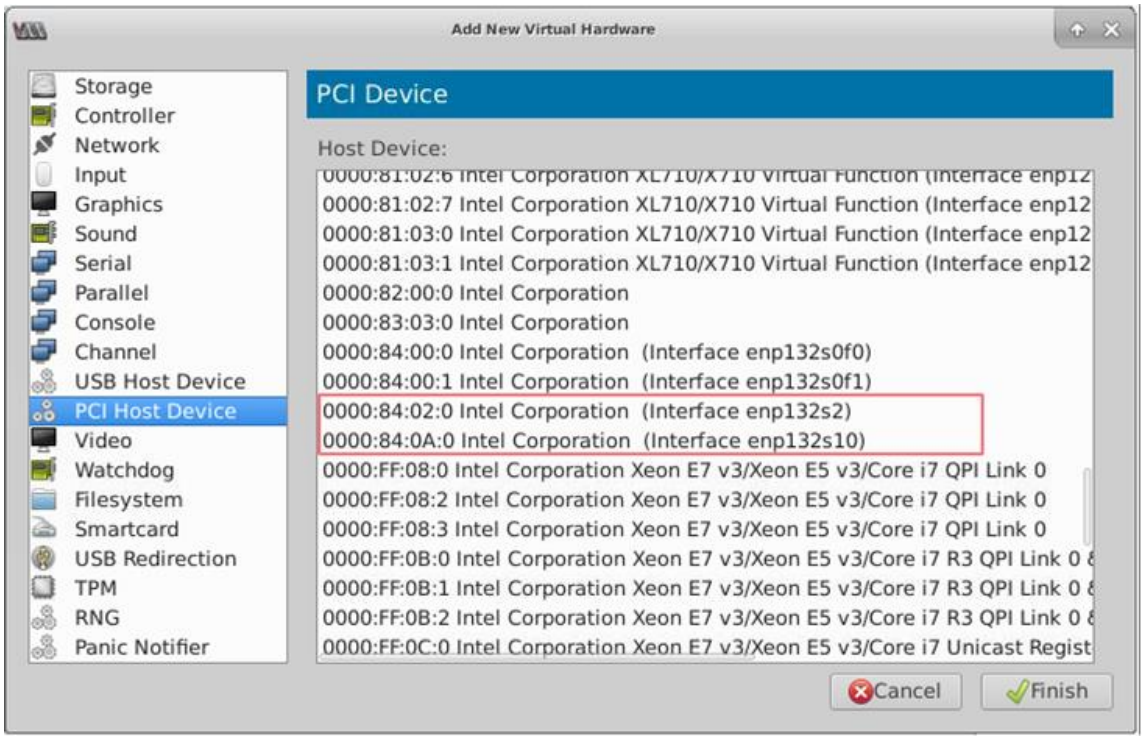


图 **6**：适用于 Intel X722 10G NIC 的 VF



6. 重复步骤 4 和 5 以添加所创建的 VF。
7. 打开 NetScaler VPX 实例的电源。
8. NetScaler VPX 实例开机后，使用以下命令验证配置：

```
1    show interface summary
```

输出内容显示您已配置的所有接口。

图 **6**：Intel 82599 NIC 的输出摘要。

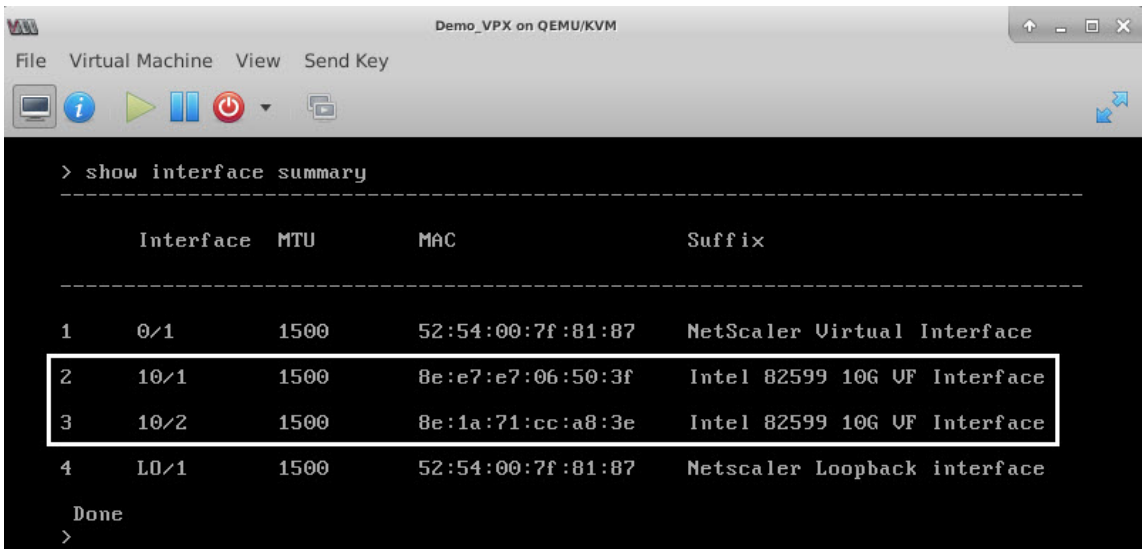
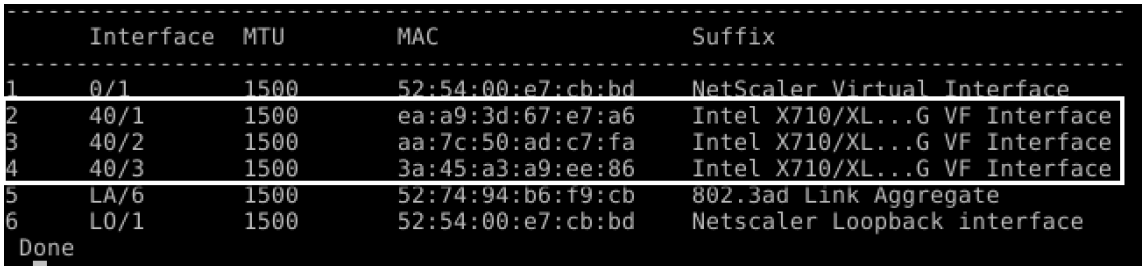


图 **7**。Intel X710 和 XL710 NIC 的输出摘要。



在 **SR-IOV** 接口上配置静态 **LA/LACP**

> 重要：
>
> 创建 SR-IOV VF 时，请务必不要将 MAC 地址分配给 VF。

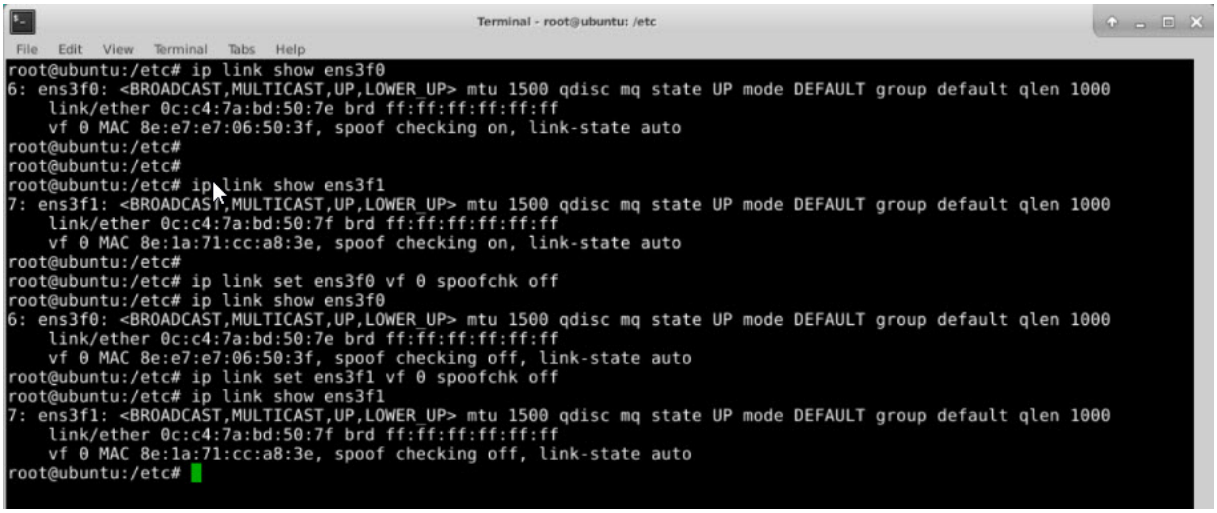
要在链路聚合模式下使用 SR-IOV VF，请禁用针对已创建的 VF 的欺骗检查。在 KVM 主机上，使用以下命令禁用欺骗检查：

*ip link set \\<**interface**_name\\> vf \\<VF_id \\> spoofchk off*

其中：

- Interface_name - 接口名称。
- VF_id - 虚拟功能 ID。

例如：



对已创建的所有 VF 禁用欺骗检查后，请执行以下操作。重启 NetScaler VPX 实例并配置链接聚合。有关详细说明，请参阅 配置链路聚合。

在 **SR-IOV** 接口上配置 **VLAN**

您可以在 SR-IOV VF 上配置 VLAN。有关详细说明，请参阅 配置 VLAN。

> 重要：
>
> 请确保 KVM 主机不包含 VF 接口的 VLAN 设置。

在 **KVM** 虚拟机管理程序上配置 **NetScaler VPX**，以便在 **SR-IOV** 模式下使用 **Intel QAT** 进行 **SSL** 加速

October 17, 2024

Linux KVM 虚拟机管理程序上的 NetScaler VPX 实例可以使用 Intel QuickAssist 技术 (QAT) 来加速 NetScaler SSL 性能。使用 Intel QAT，所有高延迟的加密处理都可以卸载到芯片上，从而腾出一个或多个主机 CPU 来执行其他任务。

以前，所有 NetScaler 数据路径加密处理都是在软件中使用主机 vCPU 完成的。

> 注意：
>
> 目前，NetScaler VPX 仅支持 Intel QAT 系列下的 C62x 芯片型号。从 NetScaler 版本 14.1 版本 8.50 开始支持此功能。

必备条件

- Linux 主机配备 Intel QAT C62x 芯片，可以直接集成到主板中，也可以添加在外部 PCI 卡上。

  Intel QAT C62x 系列型号： C625、C626、C627、C628。只有这些 C62x 型号包含公钥加密 (PKE) 功能。其他 C62x 变体不支持 PKE。
- NetScaler VPX 满足 VMware ESX 硬件要求。有关更多信息，请参阅 在 Linux KVM 平台上安装 NetScaler VPX 实例。

限制

没有为单个虚拟机预留加密单位或带宽的规定。任何 Intel QAT 硬件的所有可用加密单元均在使用 QAT 硬件的所有虚拟机之间共享。

设置主机环境以使用 **Intel QAT**

1. 在 Linux 主机中下载并安装 Intel 为 C62x 系列 (QAT) 芯片型号提供的驱动程序。有关 Intel 软件包下载和安装说明的更多信息，请参阅适用于 Linux 的 Intel QuickAssist 技术驱动程序。自述文件可作为下载包的一部分提供。此文件提供有关在主机中编译和安装软件包的说明。

   下载并安装驱动程序后，执行以下完整性检查：

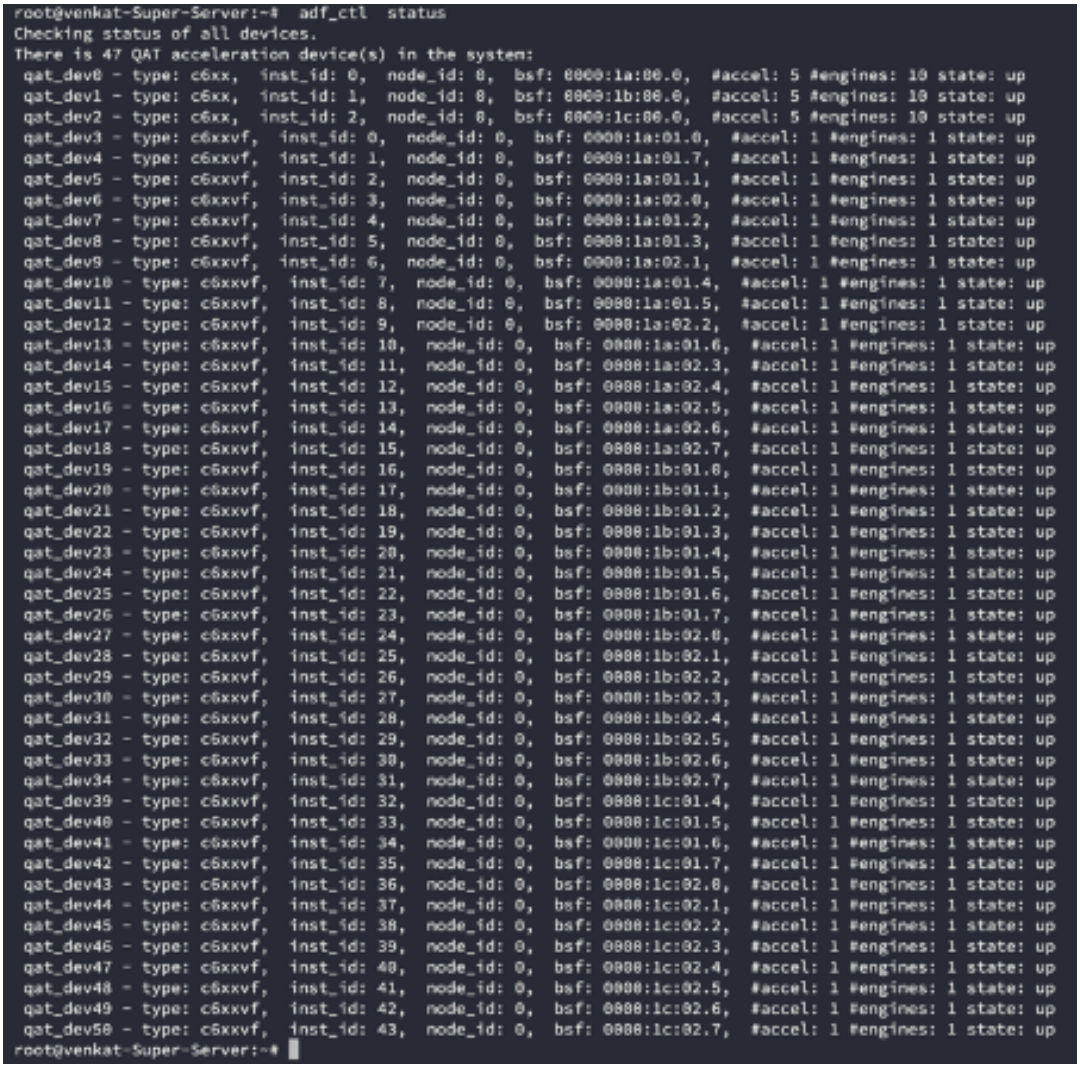
   - 记下 C62x 芯片的数量。每个 C62x 芯片最多有 3 个 PCIe 端点。
   - 确保所有端点都已启动。运行 `adf_ctl status` 命令以显示所有 PF 端点（最多 3 个）的状态。

     ```
     root@Super-Server:~# adf_ctl status

     Checking status of all devices.
     There is 51 QAT acceleration device(s) in the system
     qat_dev0 - type: c6xx,  inst_id: 0,  node_id: 0,  bsf:
         0000:1a:00.0,  #accel: 5 #engines: 10 state: up
     qat_dev1 - type: c6xx,  inst_id: 1,  node_id: 0,  bsf:
         0000:1b:00.0,  #accel: 5 #engines: 10 state: up
     qat_dev2 - type: c6xx,  inst_id: 2,  node_id: 0,  bsf:
         0000:1c:00.0,  #accel: 5 #engines: 10 state: up
     ```

   - 为所有 QAT 端点启用 SRIOV（VF 支持）。

     ```
     root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1a
         \:00.0/sriov_numvfs
     root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1b
         \:00.0/sriov_numvfs
     root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1c
         \:00.0/sriov_numvfs
     ```

   - 确保显示所有 VF（每个端点 16 个 VF，总计 48 个 VF）。
   - 运行 adf_ctl 状态命令以验证所有 PF 端点（最多 3 个）和每个 Intel QAT 芯片的 VF 是否已启动。在此示例中，系统只有一个 C62x 芯片。因此，它总共有 51 个端点（3 + 48 个 VF）。



2. 在 Linux 主机上启用 SR-IOV。
3. 创建虚拟机。创建 VM 时，分配适当数量的 PCI 设备以满足性能要求。

> 注意：
>
> 每个 C62x (QAT) 芯片最多可以有三个独立的 PCI 端点。每个端点都是 VF 的逻辑集合，与芯片的其他 PCI 端点平均共享带宽。每个端点最多可以有 16 个 VF，显示为 16 个 PCI 设备。将这些设备添加到 VM，使用 QAT 芯片进行加密加速。

注意事项

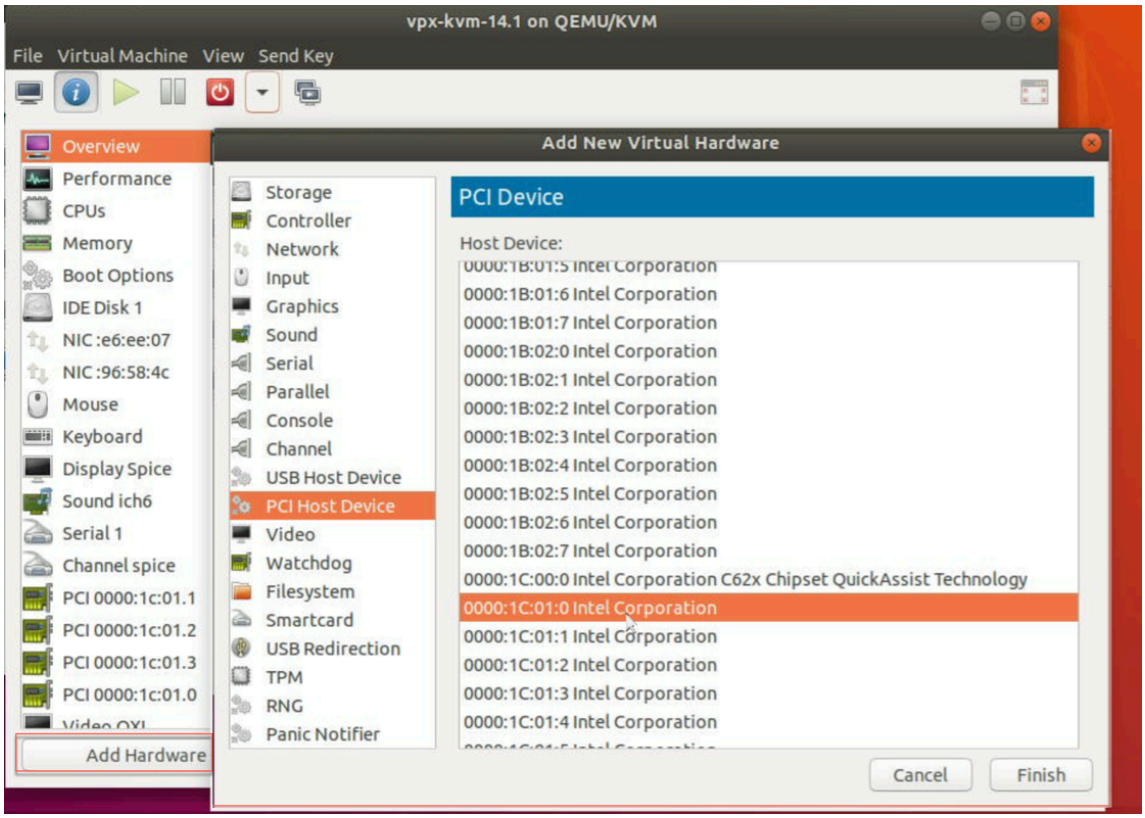
- 如果虚拟机加密要求使用多个 QAT PCI 端点/芯片，我们建议您以循环方式选择相应的 PCI 设备/VF 以实现对称分布。
- 我们建议所选的 PCI 设备数量等于许可的 vCPU 数量（不包括管理 vCPU 数量）。添加比可用的 vCPU 数量更多的 PCI 设备不一定能提高性能。

Example:

以一台具有 3 个端点的 Intel C62x 芯片的 Linux 主机为例。在配置具有 6 个 vCPU 的虚拟机时，从每个端点中选择 2 个 VF，然后将其分配给虚拟机。此分配可确保虚拟机加密单位的有效和平等分配。默认情况下，在可用的 vCPU 总数中，一个 vCPU 留给管理平面，其余 vCPU 可用于数据平面 PE。

将 **QAT VF** 分配给部署在 **Linux KVM** 虚拟机管理程序上的 **NetScaler VPX**

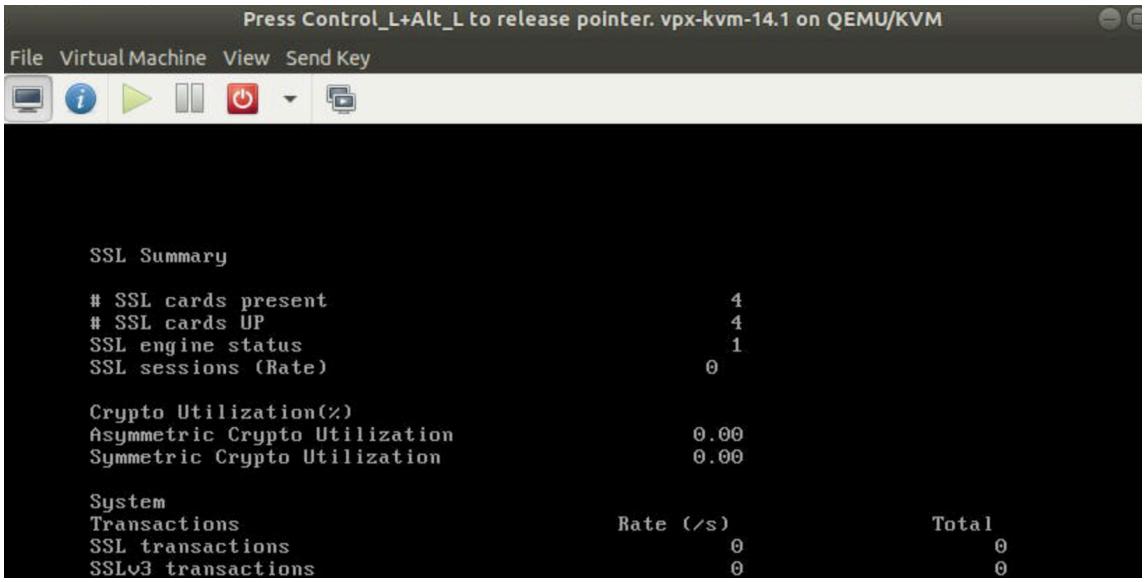
1. 在 Linux KVM 虚拟机管理器中，确保虚拟机（NetScaler VPX）已关闭。
2. 导航到添加硬件 **> PCI** 主机设备。
3. 为 PCI 设备分配 Intel QAT VF。



4. 单击完成。
5. 重复上述步骤，为 NetScaler VPX 实例分配一个或多个 Intel QAT VF，最多不超过 vCPU 总数少一个。因为一个 vCPU 是为管理过程保留的。

   每个 VM 的 QAT VF 数量 = vCPU 数量- 1
6. Power on the VM.
7. 在 NetScaler CLI 中运行 `stat ssl` 命令以显示 SSL 摘要，并在将 QAT VF 分配给 NetScaler VPX 后验证 SSL 卡。

在此示例中，我们使用了 5 个 vCPU，这意味着 4 个数据包引擎 (PE)。



关于部署

此部署使用以下组件规格进行了测试：

- **NetScaler VPX** 版本和内部版本： 14.1—8.50
- **Ubuntu** 版本： 18.04，内核 5.4.0-146
- 适用于 **Linux** 的 **Intel C62x QAT** 驱动程序版本： L.4.21.0-00001

将 **NetScaler VPX** 实例配置为使用 **PCI** 直通网络接口

October 17, 2024

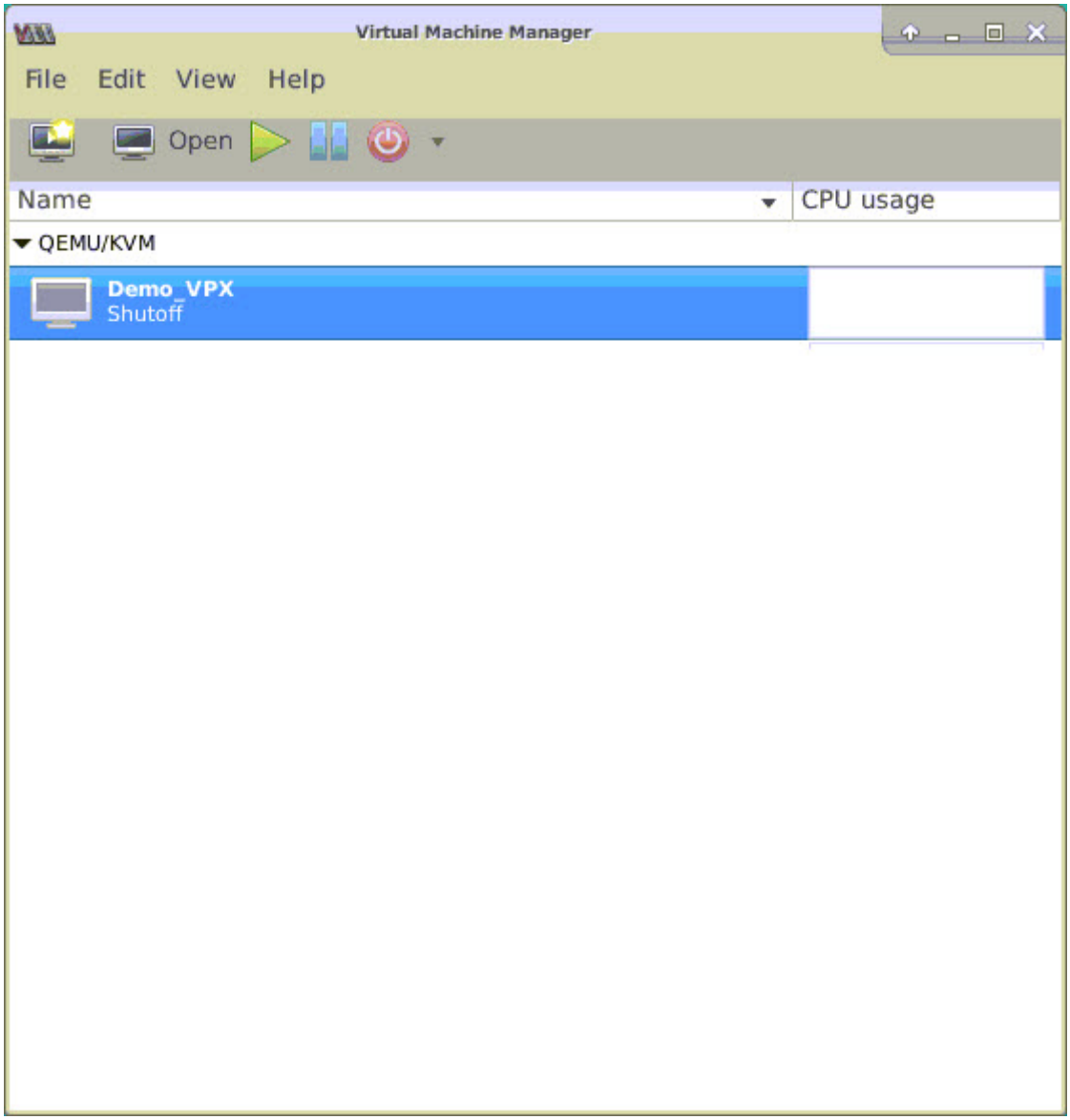
在 Linux-KVM 平台上安装和配置 NetScaler VPX 实例后，您可以使用虚拟机管理器将虚拟设备配置为使用 PCI 直通网络接口。

必备条件

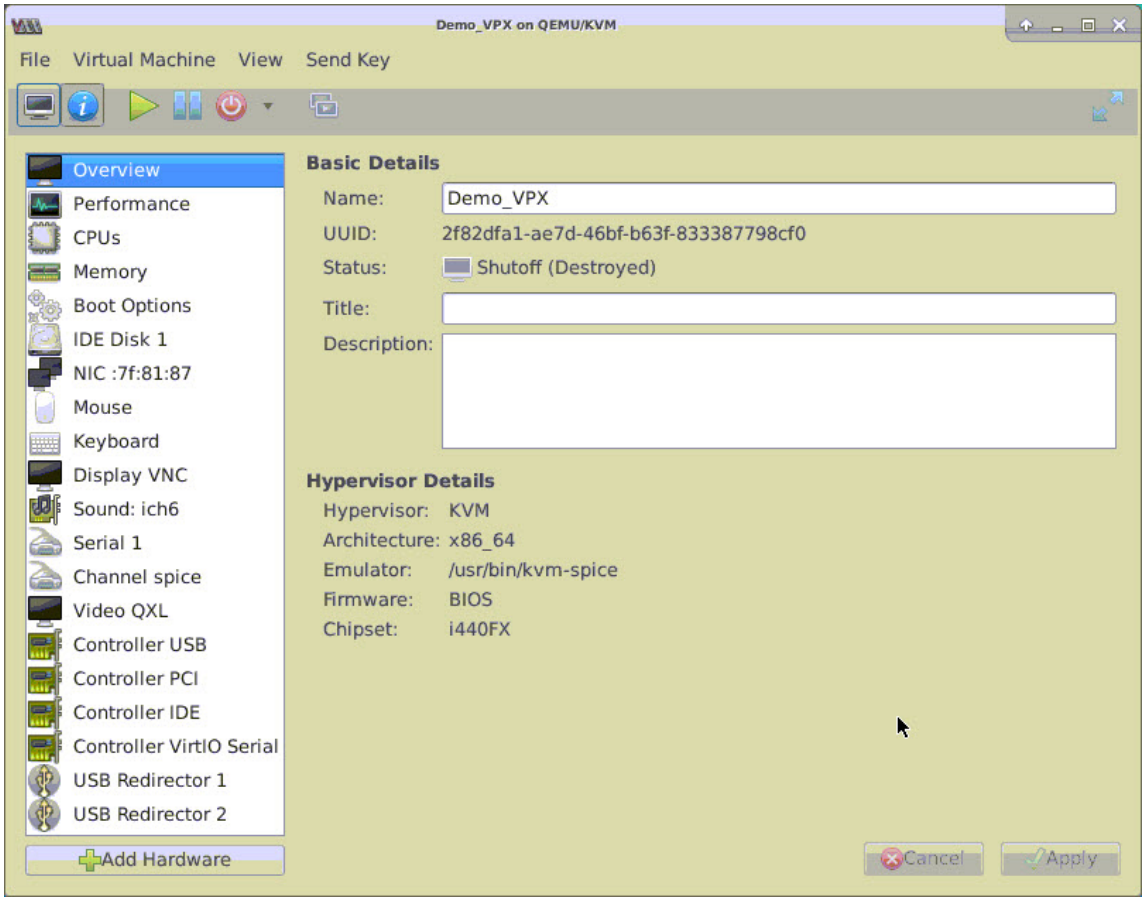
- KVM 主机上的 Intel XL710 NIC (NIC) 的固件版本为 5.04。
- KVM 主机支持输入输出内存管理单元 (IOMMU) 和 Intel VT-d，并且 IOMMU 和 Intel VT-d 在 KVM 主机的 BIOS 中处于启用状态。在 KVM 主机上，要启用 IOMMU，请将以下注册表项添加到 **/boot/grub2/grub.cfg** 文件：**intel_iommu=1**
- 运行以下命令并重新启动 KVM 主机：**Grub2-mkconfig –o /boot/grub2/grub.cfg**

要使用虚拟机管理器将 **NetScaler VPX** 实例配置为使用 **PCI** 直通网络接口，请执行以下操作：

1. 关闭 NetScaler VPX 实例的电源。
2. 选择 NetScaler VPX 实例，然后单击 **Open**（打开）。



3. 在 **<virtual_machine on KVM>** 窗口中，单击 **i** 图标。

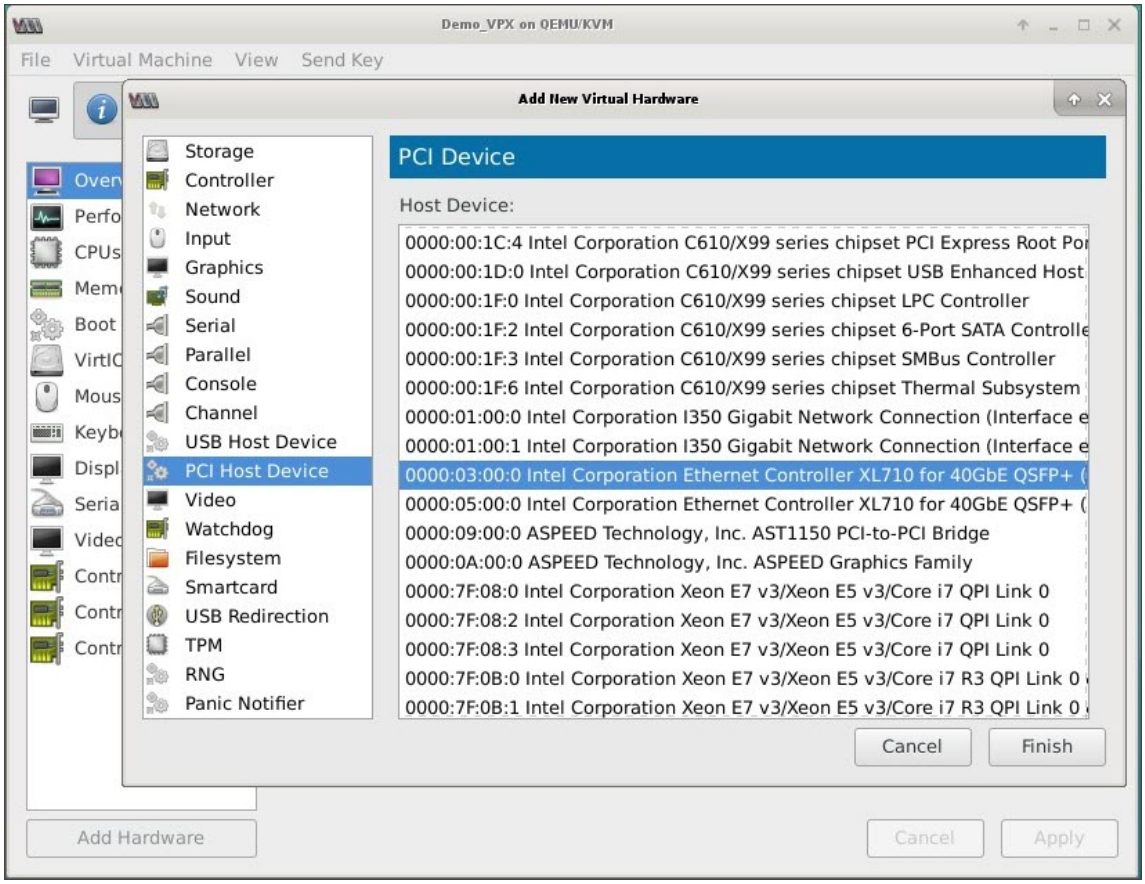


4. 单击 **Add Hardware**（添加硬件）。
5. 在 **Add New Virtual Hardware**（添加新虚拟硬件）对话框中，执行以下操作：

   a。a. 选择 **PCI Host Device**（PCI 主机设备）。

   a。b. 在 **Host Device**（主机设备）部分中，选择 Intel XL710 物理功能。

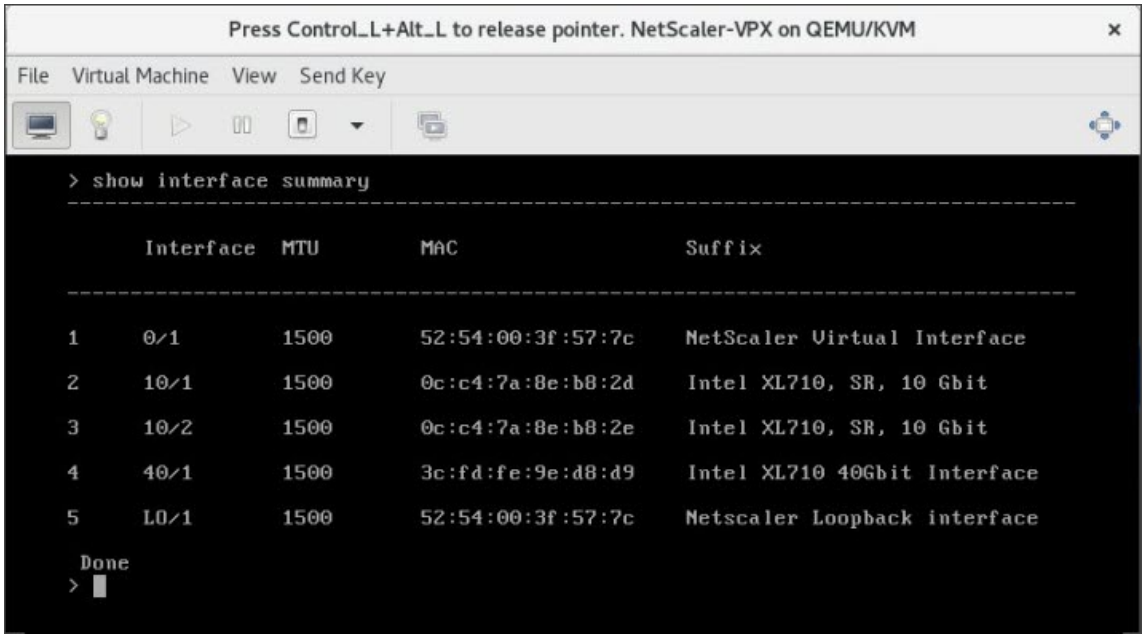
   a。单击完成。



6. 重复执行步骤 **4** 和 **5** 以添加任何其他 Intel XL710 物理功能。
7. 打开 NetScaler VPX 实例的电源。
8. NetScaler VPX 实例启动后，您可以使用以下命令来验证配置：

```
COMMAND
> show interface summary
```

输出内容必须显示您已配置的所有接口：



使用该程序配置 **NetScaler VPX** 实例 **virsh**

October 17, 2024

`virsh` 程序是用于管理 VM 来宾的命令行工具，其功能与 Virtual Machine Manager 的功能类似。其功能与虚拟机管理器类似。通过此程序，可以更改 VM 来宾的状态（启动、停止、暂停等）、设置新来宾和设备以及编辑现有配置。`virsh` 程序还对编写 VM 来宾管理操作的脚本非常有用。

要使用该 `virsh` 程序配置 NetScaler VPX，请按照以下步骤操作：

1. 使用 tar 命令解压缩 NetScaler VPX 软件包。NSVPX-KVM-*_nc.tgz 软件包包含以下组件：

   - 用于指定 VPX 属性 [NSVPX-KVM-*_nc.xml] 的域 XML 文件
   - NS-VM 磁盘映像的校验和 [Checksum.txt]
   - NS-VM 磁盘映像 [NSVPX-KVM-*_nc.raw]

   Example:

   ```
   tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
   NSVPX-KVM-10.1-117_nc.xml
   NSVPX-KVM-10.1-117_nc.raw
   checksum.txt
   ```

2. 将 `NSVPX-KVM-\*\_nc.xml` XML 文件复制到名为 `\<DomainName\>-NSVPX-KVM-\*\_nc.xml`的文件中。<DomainName> 也是虚拟机的名称。Example:


```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc
    .xml
```

3. 编辑 \\<DomainName\\>-NSVPX-KVM-*_nc.xml 文件以指定以下参数：

   - name —指定名称。
   - Mac —指定 MAC 地址。

     > 注意：
     >
     > 域名和 MAC 地址必须是唯一的。

   - source file —指定绝对磁盘映像源路径。文件路径必须为绝对路径。可以指定 RAW 映像文件或 QCOW2 映像文件的路径。

     如果要指定 RAW 映像文件，请指定磁盘映像源路径，如以下示例所示：

     Example:

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

     指定 QCOW2 磁盘映像绝对源路径，并将驱动程序类型定义为 **qcow2**，如以下示例所示：

     Example:

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

4. 编辑 \\<DomainName\\>-NSVPX-KVM-*_nc.xml 文件以配置网络详细信息：

   - source dev —指定接口。
   - mode —指定模式。默认接口为 **Macvtap Bridge**（Macvtap 桥接）。

   示例：模式：MacVTap 桥接将目标接口设置为 ethx，将模式设置为桥接模式，将类型设置为 virtio

   ```
   <interface type='direct'>
       <mac address='52:54:00:29:74:b3'/>
       <source dev='eth0' mode='bridge'/>
       <target dev='macvtap0'/>
       <model type='virtio'/>
       <alias name='net0'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
           function='0x0'/>
     </interface>
   ```

   在此处，eth0 是连接到 VM 的物理接口。

5. 使用以下命令在 \\<DomainName\\>-NSVPX-KVM-*_nc.xml 文件中定义 VM 属性：

```
virsh define \<DomainName\>-NSVPX-KVM-\*\_nc.xml
```

Example:

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

6. 输入以下命令启动虚拟机：

```
virsh start \[\<DomainName\> | \<DomainUUID\>\]
```

Example:

```
virsh start NetScaler-VPX
```

7. 通过控制台连接来宾 VM:

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

Example:

```
virsh console NetScaler-VPX
```

使用程序向 **NetScaler VPX** 实例添加更多接口 `virsh`

在 KVM 上置备 NetScaler VPX 后，可以添加其他接口。

要添加更多接口，请按照以下步骤进行操作：

1. 关闭 KVM 上运行的 NetScaler VPX 实例。
2. 使用以下命令编辑 \\<DomainName\\>-NSVPX-KVM-*_nc.xml 文件：

```
virsh edit \[\<DomainName\> | \<DomainUUID\>\]
```

3. 在 \\<DomainName\\>-NSVPX-KVM-*_nc.xml 文件中，附加以下参数：

   a) 适用于 **MacVTap**

   - 接口类型—将接口类型指定为 “direct”。
   - MAC 地址—指定 MAC 地址并确保 MAC 地址在各接口之间具有唯一性。
   - 源设备—指定接口名称。
   - mode —指定模式。支持的模式包括 - 桥接、VEPA、专用和直通
   - 模型类型—将模型类型指定为 `virtio`

   Example:

   模式：MacVTap 直通

将目标接口设置为 ethx，模式为 桥梁和模型类型 virtio

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
```

在此处，eth1 是连接到 VM 的物理接口。

b) 对于桥接模式

> 注意：
>
> 确保您已在 KVM 主机中配置了 Linux 桥接器、将物理接口绑定到桥接器、并将桥接器置于 UP 状态。

- 接口类型—将接口类型指定为 “bridge”。
- MAC 地址—指定 MAC 地址并确保 MAC 地址在各接口之间具有唯一性。
- 源网桥—指定网桥名称。
- 模型类型—将模型类型指定为 virtio

示例：桥接模式

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
 </interface>
```

管理 NetScaler VPX 客户机虚拟机

October 17, 2024

可以使用 Virtual Machine Manager 和 virsh 程序执行管理任务，例如启动或停止 VM 来宾、设置新来宾和设备、编辑现有配置以及通过虚拟网络计算 (Virtual Network Computing, VNC) 连接到图形控制台。

使用 Virtual Machine Manager 管理 VPX 来宾 VM

- 列出 VM 来宾

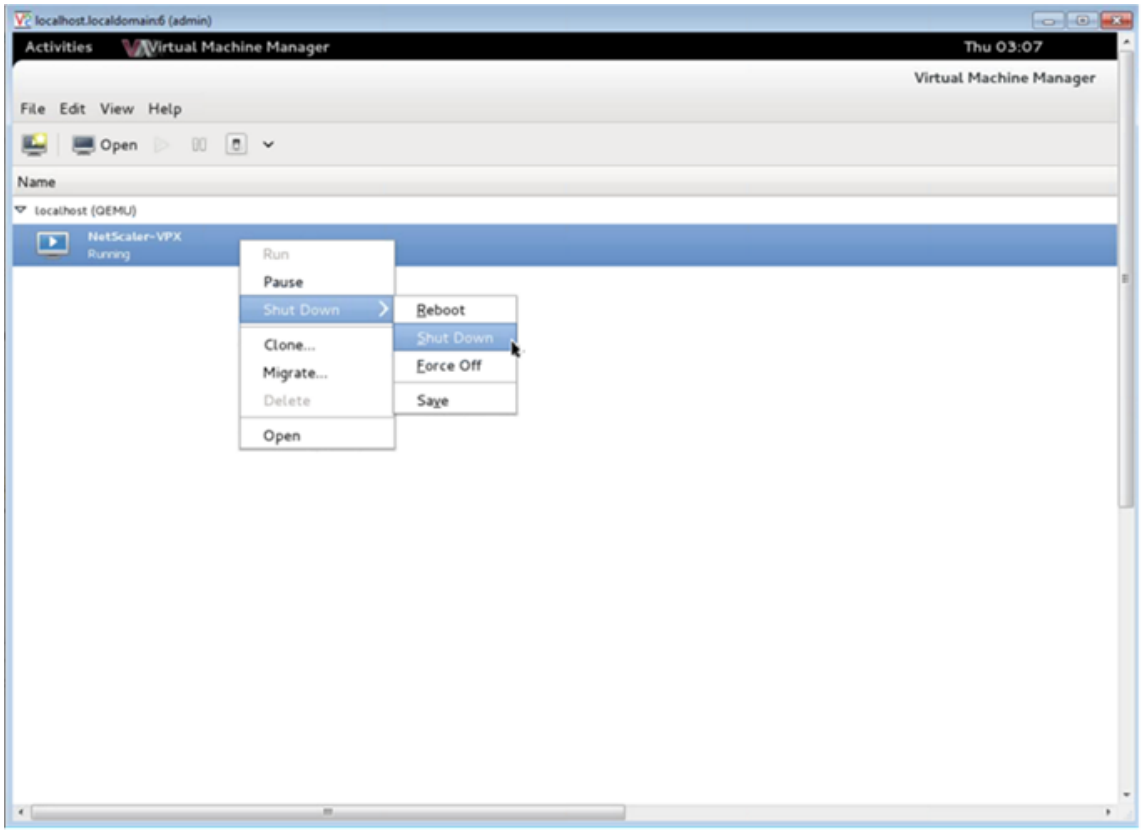
  Virtual Machine Manager 的主窗口中显示其连接到的每个 VM 主机服务器的所有 VM 来宾列表。每个 VM 来宾条目中包含虚拟机的名称，其状态（正在运行、已暂停或关闭）像在图标中一样显示。

- 打开图形控制台

打开 VM 来宾的图形控制台可以像通过 VNC 连接与物理主机交互一样与计算机进行交互。要在 Virtual Machine Manager 中打开图形控制台，请在 VM 来宾条目上单击鼠标右键，然后从弹出菜单中选择“Open”（打开）选项。

- 启动和关闭来宾

  可以从 Virtual Machine Manager 启动或停止 VM 来宾。要更改 VM 的状态，请在 VM 来宾条目上单击鼠标右键，然后从弹出菜单中选择“Run”（运行）或其中一个“Shut Down”（关机）选项。



- 重新启动来宾

  可以从 Virtual Machine Manager 重新启动 VM 来宾。要重新启动 VM，请在 VM 来宾条目上单击鼠标右键，然后从弹出菜单中选择“Shut Down”（关机）>“Reboot”（重新启动）。

- 删除来宾

  删除 VM 来宾默认会删除其 XML 配置。还可以删除来宾的存储文件。这样可以完全擦除来宾。

  1. 在 Virtual Machine Manager 中，在 VM 来宾条目上单击鼠标右键。
  2. 从弹出菜单中选择“Delete”（删除）。此时将显示一个确认窗口。

     > 注意：
     >
     > 仅当 VM Guest 关闭时才启用“删除”选项。

  3. 单击删除。

4. 要完成擦除来宾，请通过选中“Delete Associated Storage Files”（删除关联的存储文件）复选框删除关联的.raw 文件。

使用 **virsh** 程序管理 **NetScaler VPX** 客户机虚拟机

- 列出 VM 来宾及其当前的状态

  使用 virsh 显示与来宾有关的信息

  ```
  virsh list --all
  ```

  此命令输出显示所有域及其状态。示例输出：

  ```
  Id Name                 State
  ----------------------------------
    0 Domain-0            running
    1 Domain-1            paused
    2 Domain-2            inactive
    3 Domain-3            crashed
  ```

- 打开 virsh 控制台。

  通过控制台连接来宾 VM

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

  Example:

  ```
  virsh console NetScaler-VPX
  ```

- 启动和关闭来宾。

  可以使用 DomainName 或 Domain-UUID 启动来宾。

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Example:

  ```
  virsh start NetScaler-VPX
  ```

  要关闭来宾，请执行以下操作：

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Example:

  ```
  virsh shutdown NetScaler-VPX
  ```

- 重新启动来宾

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Example:

  ```
  virsh reboot NetScaler-VPX
  ```


删除来宾

要删除访客虚拟机，在运行删除命令之前，必须关闭客户机并取消定义 <DomainName>-NSVPX-KVM-*_nc.xml。

```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
```

Example:

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
```

> 注意：
>
> 删除命令不会删除磁盘映像文件，必须手动删除。

在 **OpenStack** 上使用 **SR-IOV** 配置 **NetScaler VPX** 实例

October 17, 2024

可以在 OpenStack 上部署使用单根 I/O 虚拟化 (SR-IOV) 技术的高性能 NetScaler VPX 实例。

可以采用三个步骤在 OpenStack 上部署使用 SR-IOV 技术的 NetScaler VPX 实例：

- 在主机上启用 SR-IOV 虚拟功能 (VF)。
- 配置 VF 并使其可用于 OpenStack。
- 在 OpenStack 上置备 NetScaler VPX。

必备条件

确保您：

- 向主机中添加 Intel 82599 NIC (NIC)。
- 从 Intel 下载并安装最新的 IXGBE 驱动程序。
- 在主机上将 IXGBEVF 驱动程序列入黑名单。在 /etc/modprobe.d/blacklist.conf 文件中添加以下条目：Block list `ixgbevf`

> 注意：
>
> `ixgbe` 驱动程序版本必须至少为 5.0.4。

在主机上启用 **SR-IOV VF**

执行以下步骤之一启用 SR-IOV VF：

- 如果使用的是 3.8 之前的内核版本，请向 /etc/modprobe.d/ixgbe 文件中添加以下条目并重新启动主机：options ixgbe max_vfs=<number_of_VFs>
- 如果使用的是内核 3.8 版或更高版本，请使用以下命令创建 VF：

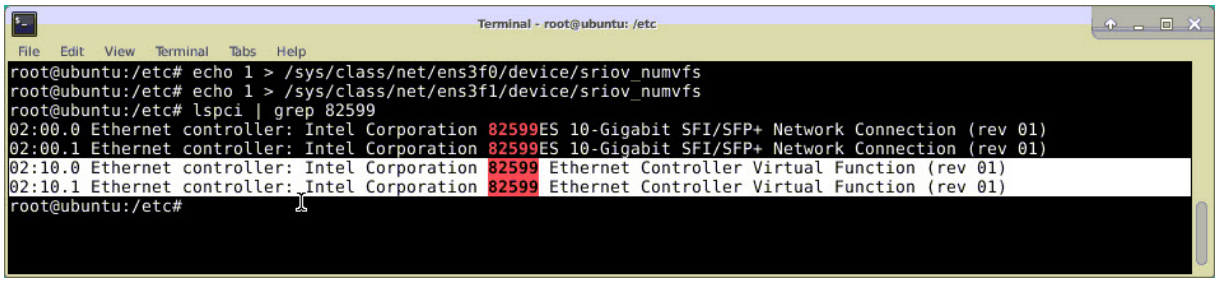
```
echo <number_of_VFs> > /sys/class/net/<device_name>/device/
   sriov_numvfs
```

其中：

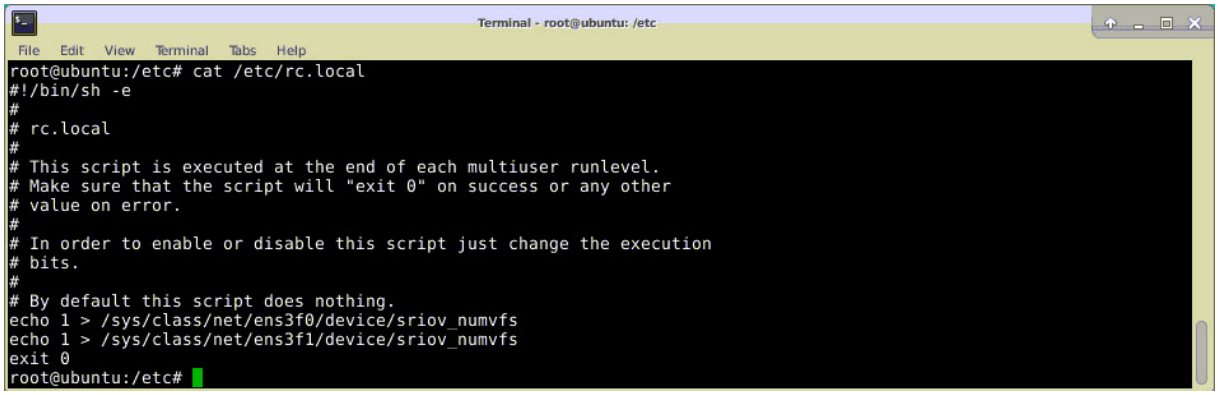
- number_of_VFs 是要创建的虚拟功能数。
- device_name 是接口名称。

> 重要：
>
> 创建 SR-IOV VF 过程中，请务必不要将 MAC 地址分配给 VF。

下面是创建四个 VF 的示例。



将 VF 设为永久存在，并向 **rc.local** 文件中添加用于创建 VF 的命令。下面是显示 rc.local 文件内容的示例。



有关更多信息，请参阅本 英特尔 SR-IOV 配置指南。

配置 **VF** 并使其可用于 **OpenStack**

请按照以下链接中给出的步骤在 OpenStack 上配置 SR-IOV：https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking。

在 **OpenStack** 上配置 **NetScaler VPX** 实例

您可以使用 OpenStack CLI 在 OpenStack 环境中配置 NetScaler VPX 实例。

预配 VPX 实例（可选）涉及使用配置驱动器中的数据。配置驱动器是一个在启动时附加到实例的特殊配置驱动器。在为实例配置网络设置之前，可以使用此配置驱动器将网络连接配置信息（例如管理 IP 地址、网络掩码和默认网关等）传递到实例。

当 OpenStack 置备 VPX 实例时，它会首先通过读取用于表示 OpenStack 的特定 BIOS 字符串 (OpenStack Foundation) 来检测实例是否在 OpenStack 环境中引导。对于 Redhat Linux 发行版，该字符串存储在 /etc/nova/release 中。这是在基于 KVM 虚拟机管理程序平台的所有 OpenStack 实现中提供的标准机制。该驱动器必须具有特定的 OpenStack 标签。如果检测到配置驱动器，实例将尝试从在 `nova` boot 命令中指定的文件名中读取以下信息。在下面的过程中，该文件称为“userdata.txt”。

- Management IP address（管理 IP 地址）
- Network mask（网络掩码）
- Default gateway（默认网关）

参数成功读取后，将填入 NetScaler 堆栈。这有助于远程管理实例。如果参数未成功读取，或者配置驱动器不可用，实例将转换为默认行为，即：

- 实例尝试从 DHCP 中检索 IP 地址信息。
- 如果 DHCP 失败或超时，实例将提供默认网络配置 (192.168.100.1/16)。

通过 **CLI** 在 **OpenStack** 上配置 **NetScaler VPX** 实例

可以在 OpenStack 环境中使用 OpenStack CLI 预配 VPX 实例。以下是在 OpenStack 上配置 NetScaler VPX 实例的步骤摘要：

1. 从.tgz 文件中提取 `.qcow2` 文件
2. 基于 qcow2 映像构建 OpenStack 映像
3. 预配 VPX 实例

要在 OpenStack 环境中预配 VPX 实例，请执行以下步骤。

1. 提取。键入以下命令从 `.tqz` 文件中提取 `qcow2` 文件：


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

2. 键入以下命令使用在步骤 1 中提取的 .qcoz2 文件构建 OpenStack 映像：

```
glance image-create --name="<name of the OpenStack image>" --
   property hw_disk_bus=ide --is-public=true --container-format=
   bare --disk-format=qcow2< <name of the qcow2 file>

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

下图提供了 glance image-create 命令的示例输出。

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

3. 创建 OpenStack 映像后，配置 NetScaler VPX 实例。

```
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
```


在上述命令中，userdata.txt 是包含 VPX 实例详细信息（例如 IP 地址、网络掩码和默认网关）的文件。用户数据文件是可由用户自定义的文件。NSVPX-KVM-12.0-26.2 是您要预配的虚拟设备的名称。–NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 为 OpenStack VF。

下图提供了 nova boot 命令的示例输出。

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

下图显示了 userdata.txt 文件的示例。标记内部的值是用户可配置的值，用于配置 IP 地址、网络掩码和默认网关等信息。

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1
    "
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="
    1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"
    />
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
```



```
17    oe:value="openstack-orch-env"/>
18    <Property oe:key="com.citrix.netscaler.mgmt.ip"
19    oe:value="10.1.0.100"/>
20    <Property oe:key="com.citrix.netscaler.mgmt.netmask"
21    oe:value="255.255.0.0"/>
22    <Property oe:key="com.citrix.netscaler.mgmt.gateway"
23    oe:value="10.1.0.1"/>
24    </PropertySection>
25    </Environment>
```

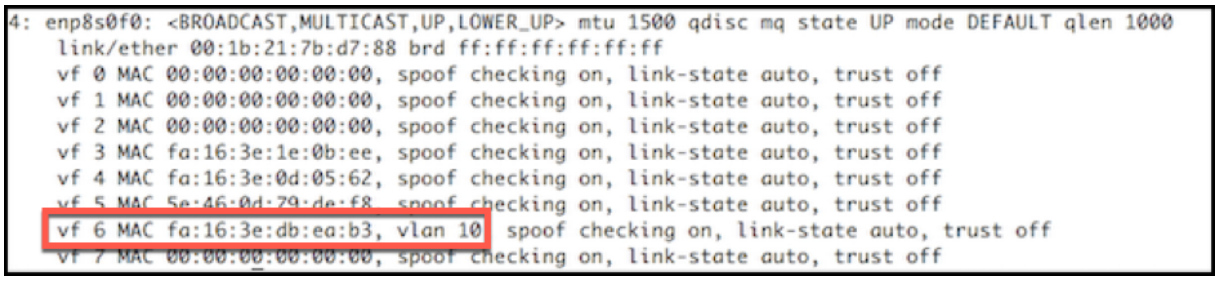
其他受支持的配置：从主机在 **SR-IOV VF** 上创建和删除 **VLAN**

键入以下命令在 SR-IOV VF 上创建 VLAN：

```
ip link show enp8s0f0 vf 6 vlan 10
```

在上面的命令中，“enp8s0f0”是物理功能的名称。

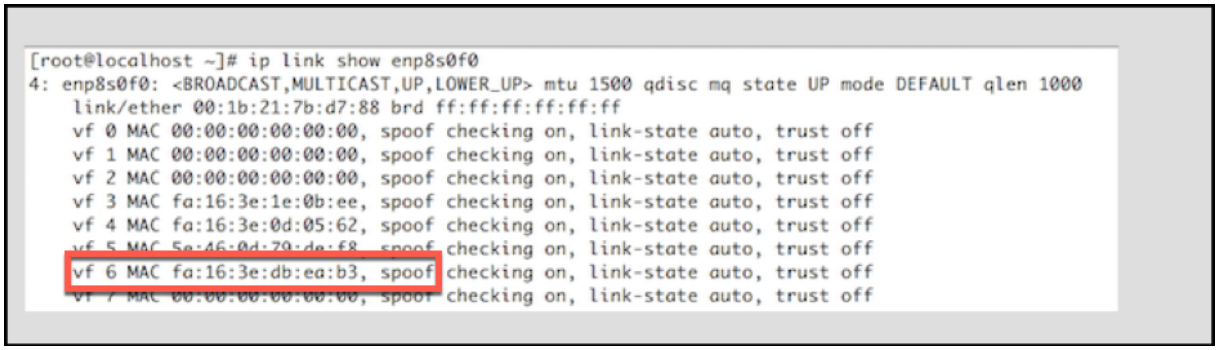
示例：VLAN 10，在 vf 6 上创建



键入以下命令在 SR-IOV VF 上删除 VLAN：

```
ip link show enp8s0f0 vf 6 vlan 0
```

示例：VLAN 10，从 vf 6 中删除



这些步骤即是在 OpenStack 上部署使用 SRIOV 技术的 NetScaler VPX 实例的过程。

在 KVM 上配置 NetScaler VPX 实例以使用基于 OVS DPDK 的主机接口

October 17, 2024

您可以将在 KVM（Fedora 和 RHOS）上运行的 NetScaler VPX 实例配置为使用带有数据平面开发套件 (DPDK) 的 Open vSwitch (OVS) 以提高网络性能。本文档介绍如何配置 NetScaler VPX 实例，使其在 OVS-DPDK 在 KVM 主机上公开的 `vhost-user` 端口上运行。

OVS 是根据开源 Apache 2.0 许可证许可的多层虚拟交换机。DPDK 是一组用于快速数据包处理的库和驱动程序。

以下 Fedora、RHOS、OVS 和 DPDK 版本符合配置 NetScaler VPX 实例的资格：

Fedora	RHOS
Fedora 25	RHOS 7.4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

必备条件

在安装 DPDK 之前，请确保主机具有 1 GB 大页。

有关更多信息，请参阅此 DPDK 系统要求文档。以下是在 KVM 上配置 NetScaler VPX 实例以使用基于 OVS DPDK 的主机接口所需的步骤摘要：

- 安装 DPDK。
- 构建和安装 OVS。
- 创建 OVS 桥接。
- 将物理接口附加到 OVS 桥接。
- 将 `vhost-user` 端口连接到 OVS 数据路径。
- 为 KVM-VPX 置备基于 OVS-DPDK 的 `vhost-user` 端口。

安装 DPDK

要安装 DPDK，请按照此 打开 vSwitch 与 DPDK 文档中的说明进行操作。

构建和安装 OVS

从 OVS 下载 页面下载OVS。然后，使用 DPDK 数据路径构建和安装 OVS。按照安 装打开 vSwitch 文档中的说明进行操作。

有关更多详细信息，请参阅《Linux 版 DPDK 入门指南》。

创建 **OVS** 桥接

根据您的需要，键入 Fedora 或 RHOS 命令以创建 OVS 桥接：

Fedora 命令：

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
   datapath_type=netdev
```

RHOS 命令：

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

将物理接口附加到 **OVS** 桥接

键入以下 Fedora 或 RHOS 命令将端口绑定到 DPDK，然后将其附加到 OVS 桥接：

Fedora 命令：

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set
   Interface dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set
   Interface dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
```

RHOS 命令：

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
   options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
   options:dpdk-devargs=0000:03:00.1
```

作为选项的一部分显示的 `dpdk-devargs` 指定各个物理 NIC 的 PCI BDF。

将 **`vhost-user`** 端口连接到 **OVS** 数据路径

键入以下 Fedora 或 RHOS 命令将 `vhost-user` 端口附加到 OVS 数据路径：

Fedora 命令：

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
   Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
   user1  mtu_request=9000

```



```
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 命令：

```
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*
```

为 **KVM-VPX** 预配基于 **OVS-DPDK** 的 **vhost-user** 端口

您可以使用以下 QEMU 命令从 CLI 在 Fedora KVM 上使用基于 OVS-DPDK 的 vhost-user 端口配置 VPX 实例：

Fedora 命令：

```
1    qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \
2
3    -object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages
        ,share=on -numa node,memdev=mem \
4
5    -mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-
        disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-
        format> \
6
7    -device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
        bootindex=1 \
8
9    -netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \
10
11   -device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
        bus=pci.0,addr=0x3 \
12
13   -chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
        user1> \
14
15   -netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
        virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \
16
17   -chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
        user2> \
18
19   -netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
        virtio-net
20
21   pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \
```



```
22
23    --nographic
```

对于 RHOS，使用以下 XML 示例文件通过使用 `virsh` 来配置 NetScaler VPX 实例。

```
1   <domain type='kvm'>
2
3     <name>dpdk-vpx1</name>
4
5     <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
6
7     <memory unit='KiB'>16777216</memory>
8
9     <currentMemory unit='KiB'>16777216</currentMemory>
10
11    <memoryBacking>
12
13      <hugepages>
14
15        <page size='1048576' unit='KiB'/>
16
17      </hugepages>
18
19    </memoryBacking>
20
21    <vcpu placement='static'>6</vcpu>
22
23    <cputune>
24
25      <shares>4096</shares>
26
27      <vcpupin vcpu='0' cpuset='0'/>
28
29      <vcpupin vcpu='1' cpuset='2'/>
30
31      <vcpupin vcpu='2' cpuset='4'/>
32
33      <vcpupin vcpu='3' cpuset='6'/>
34
35      <emulatorpin cpuset='0,2,4,6'/>
36
37    </cputune>
38
39    <numatune>
40
41      <memory mode='strict' nodeset='0'/>
42
43    </numatune>
44
45    <resource>
46
47      <partition>/machine</partition>
48
```



```
49      </resource>
50
51      <os>
52
53        <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55        <boot dev='hd'/>
56
57      </os>
58
59      <features>
60
61        <acpi/>
62
63        <apic/>
64
65      </features>
66
67      <cpu mode='custom' match='minimum' check='full'>
68
69        <model fallback='allow'>Haswell-noTSX</model>
70
71        <vendor>Intel</vendor>
72
73        <topology sockets='1' cores='6' threads='1'/>
74
75        <feature policy='require' name='ss'/>
76
77        <feature policy='require' name='pcid'/>
78
79        <feature policy='require' name='hypervisor'/>
80
81        <feature policy='require' name='arat'/>
82
83    <domain type='kvm'>
84
85      <name>dpdk-vpx1</name>
86
87      <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89      <memory unit='KiB'>16777216</memory>
90
91      <currentMemory unit='KiB'>16777216</currentMemory>
92
93      <memoryBacking>
94
95        <hugepages>
96
97          <page size='1048576' unit='KiB'/>
98
99        </hugepages>
100
101     </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>
<cpu mode='custom' match='minimum' check='full'>
  <model fallback='allow'>Haswell-noTSX</model>
  <vendor>Intel</vendor>
```



```
155         <topology sockets='1' cores='6' threads='1'/>
156
157         <feature policy='require' name='ss'/>
158
159         <feature policy='require' name='pcid'/>
160
161         <feature policy='require' name='hypervisor'/>
162
163         <feature policy='require' name='arat'/>
164
165         <feature policy='require' name='tsc\_adjust'/>
166
167         <feature policy='require' name='xsaveopt'/>
168
169         <feature policy='require' name='pdpe1gb'/>
170
171         <numa>
172
173           <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess=
                'shared'/>
174
175         </numa>
176
177       </cpu>
178
179       <clock offset='utc'/>
180
181       <on\_poweroff>destroy</on\_poweroff>
182
183       <on\_reboot>restart</on\_reboot>
184
185       <on\_crash>destroy</on\_crash>
186
187       <devices>
188
189         <emulator>/usr/libexec/qemu-kvm</emulator>
190
191         <disk type='file' device='disk'>
192
193           <driver name='qemu' type='qcow2' cache='none'/>
194
195           <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>
196
197           <target dev='vda' bus='virtio'/>
198
199           <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
                function='0x0'/>
200
201         </disk>
202
203         <controller type='ide' index='0'>
204
205           <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
```



```
            function='0x1'/>

      </controller>

      <controller type='usb' index='0' model='piix3-uhci'>

        <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
           function='0x2'/>

      </controller>

      <controller type='pci' index='0' model='pci-root'/>

      <interface type='direct'>

        <mac address='52:54:00:bb:ac:05'/>

        <source dev='enp129s0f0' mode='bridge'/>

        <model type='virtio'/>

        <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
           function='0x0'/>

      </interface>

      <interface type='vhostuser'>

        <mac address='52:54:00:55:55:56'/>

        <source type='unix' path='/var/run/openvswitch/vhost-user1'
           mode='client'/>

        <model type='virtio'/>

        <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
           function='0x0'/>

      </interface>

      <interface type='vhostuser'>

        <mac address='52:54:00:2a:32:64'/>

        <source type='unix' path='/var/run/openvswitch/vhost-user2'
           mode='client'/>

        <model type='virtio'/>

        <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
           function='0x0'/>

      </interface>
```



```
252
253         <interface type='vhostuser'>
254
255           <mac address='52:54:00:2a:32:74'/>
256
257           <source type='unix' path='/var/run/openvswitch/vhost-user3'
                 mode='client'/>
258
259           <model type='virtio'/>
260
261           <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
                 function='0x0'/>
262
263         </interface>
264
265         <interface type='vhostuser'>
266
267           <mac address='52:54:00:2a:32:84'/>
268
269           <source type='unix' path='/var/run/openvswitch/vhost-user4'
                 mode='client'/>
270
271          <model type='virtio'/>
272
273           <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
                 function='0x0'/>
274
275         </interface>
276
277         <serial type='pty'>
278
279           <target port='0'/>
280
281         </serial>
282
283         <console type='pty'>
284
285           <target type='serial' port='0'/>
286
287         </console>
288
289         <input type='mouse' bus='ps2'/>
290
291         <input type='keyboard' bus='ps2'/>
292
293         <graphics type='vnc' port='-1' autoport='yes'>
294
295           <listen type='address'/>
296
297         </graphics>
298
299         <video>
300
```



```
301         <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303         <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
               function='0x0'/>
304
305       </video>
306
307       <memballoon model='virtio'>
308
309         <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
               function='0x0'/>
310
311       </memballoon>
312
313     </devices>
314
315   </domain
```

注意事项

在 XML 文件中，hugepage 大小必须为 1 GB，如示例文件所示。

```
1   <memoryBacking>
2
3       <hugepages>
4
5         <page size='1048576' unit='KiB'/>
6
7       </hugepages>
```

此外，在示例文件中，vhost-user1 为绑定到 ovs-br0 的 vhost 用户端口。

```
1   <interface type='vhostuser'>
2
3         <mac address='52:54:00:55:55:56'/>
4
5         <source type='unix' path='/var/run/openvswitch/vhost-user1'
             mode='client'/>
6
7         <model type='virtio'/>
8
9         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
             function='0x0'/>
10
11      </interface>
```

要启动 NetScaler VPX 实例，请开始使用命令。virsh

在 KVM 虚拟机管理程序上首次启动 NetScaler 设备时应用 NetScaler VPX 配置

October 17, 2024

在 NetScaler 设备首次启动期间，您可以在 KVM 虚拟机管理程序上应用 NetScaler VPX 配置。因此，客户在 VPX 实例上的设置可以在更短的时间内完成配置。

有关预启动用户数据及其格式的更多信息，请参阅 在云中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。

> 注意：
>
> 要在 KVM 虚拟机管理程序中使用预引导用户数据进行引导，必须在 <NS-CONFIG> 部分中传递默认网关配置。有关 <NS-CONFIG> 标记内容的更多信息，请参阅下面的“示例” <NS-CONFIG>部分。

Sample <NS-CONFIG> section:

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

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

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

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

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

如何在 KVM 虚拟机管理程序上提供预引导用户数据

您可以通过使用 CDROM 设备附加的 ISO 文件在 KVM 虚拟机管理程序上提供预引导用户数据。

使用 CDROM ISO 文件提供用户数据

您可以使用虚拟机管理器 (VMM) 使用 CDROM 设备将用户数据作为 ISO 映像注入到虚拟机 (VM) 中。通过直接访问虚拟机主机服务器上的物理驱动器或访问 ISO 映像，KVM 支持 VM 来宾中的 CD-ROM。

通过以下步骤，您可以使用 CDROM ISO 文件提供用户数据：

1. 使用包含预引导用户数据内容的文件名 `userdata` 创建一个文件。

   > 注意：
   >
   > 文件名必须严格使用为 `userdata`。

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

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

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

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

```
root@ubuntu:~/sai/19oct# ls -lh
total 4.0K
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
```

3. 使用标准部署流程配置 NetScaler VPX 实例以创建虚拟机。但是不要自动打开虚拟机的电源。
4. 使用以下步骤使用虚拟机管理器添加 CD-ROM 设备：

   a) 双击虚拟机管理器中的虚拟机来宾条目以打开其控制台，然后通过查看 **>** 详细信息切换到详细信息视图。
   b) 单击“添加硬件”**>**“存储”**>**“设备类型”**>**“**CDROM** 设备”。
   c) 单击“管理”并选择正确的 ISO 文件，然后单击“完成”。在 NetScaler VPX 实例上的“资源”下创建了一张新光盘。

5. Power on the VM.

AWS 上的 NetScaler VPX

October 17, 2024

您可以在 Amazon Web Services (AWS) 上启动 NetScaler VPX 实例。NetScaler VPX 设备在 AWS 市场上作为 Amazon Machine Image (AMI) 上市。AWS 上的 NetScaler VPX 实例使您能够使用 AWS 云计算功能，并使用 NetScaler 负载平衡和流量管理功能来满足他们的业务需求。VPX 实例支持 NetScaler 物理设备的所有流量管理功能，它可以作为独立实例部署，也可以按高可用性对部署。有关 VPX 功能的更多信息，请参阅 VPX 数据手册。

入门

在开始 VPX 部署之前，您必须熟悉以下信息：

- AWS 术语
- AWS-VPX 支持列表
- 局限性与用法指南
- 必备条件
- AWS 上的 NetScaler VPX 实例的工作原理

在 **AWS** 上部署 **NetScaler VPX** 实例

在 AWS 中，VPX 实例支持以下部署类型：

- 独立
- 高可用性（主动-被动）
  - 同一区域内的高可用性
  - 使用弹性 IP 跨不同区域的高可用性
  - 使用专用 IP 跨不同区域的高可用性
- 主动-主动 GSLB
- 使用 ADM 的 Autoscaling（主动-主动）

混合部署

- 在 AWS 前哨基地部署 NetScaler
- 在 AWS 的 VMC 中部署 NetScaler

许可

AWS 上的 NetScaler VPX 实例需要许可证。以下许可选项适用于在 AWS 上运行的 NetScaler VPX 实例：

- 免费（无限制）
- 每小时
- 年度

- BYOL
- 免费试用（AWS Marketplace 中的所有 NetScaler VPX-AWS 订阅产品均为 21 天免费。）

自动化

- NetScaler ADM：智能部署
- GitHub CFT：用于 AWS 部署的 NetScaler 模板和脚本
- GitHub Ansible：用于 AWS 部署的 NetScaler 模板和脚
- GitHub Terraform：用于 AWS 部署的 NetScaler 模板和脚本
- AWS 模式库 (PL)：NetScaler VPX

博客

- AWS 上的 NetScaler 如何帮助客户安全地交付应用程序
- 使用 NetScaler 和 AWS 在混合云中交付应用程序
- Citrix 是 AWS 网络能力合作伙伴
- NetScaler：随时为公有云做好准备
- 通过 NetScaler 在公有云中轻松横向扩展或纵向扩展
- Citrix 通过 AWS Outposts 扩展 ADC 部署选项
- 将 NetScaler 与 Amazon VPC 入口路由一起使用
- Citrix 在 AWS 中提供选择、性能以及简化的部署
- NetScaler Web App Firewall 的安全性——现已在 AWS Marketplace 上线
- Aria Systems 是如何在 AWS 上使用 NetScaler Web App Firewall

视频

- 通过 ADM 简化公有云 NetScaler 的部署
- 使用现成的 terraform 脚本在 AWS 中 Provisioning 和配置 NetScaler VPX
- 使用 CloudFormation 模板在 AWS 中部署 NetScaler HA
- 使用 AWS QuickStart 跨可用区部署 NetScaler HA
- NetScaler 使用 ADM 自动缩放规模

客户案例研究

- 技术解决方案 - Xenit AB
- 使用 Citrix 和 AWS 云开展业务的更好方式—Aria
- 探索 NetScaler 和 AWS 的优势
- Rain for Rent - 客户案例

解决方案

- 使用 NetScaler 在 AWS 上部署数字广告平台
- 使用 NetScaler 增强 AWS 中单击流分析的功能

支持

- 开立支持案例
- 对于 NetScaler 订阅产品，请参阅 对 AWS 上的 VPX 实例进行故障排除。要提交支持案例，请找到您的 AWS 账号和支持 PIN 码，然后致电 NetScaler 支持人员。
- 对于 NetScaler 客户许可产品或 BYOL，请确保您拥有有效的支持和维护协议。如果您未达成协议，请联系您的 NetScaler 代表。

其他参考资料

- AWS 点播网络研讨会——NetScaler on AWS
- NetScaler VPX 数据手册
- AWS Marketplace 中的 NetScaler
- NetScaler 是 AWS 网络合作伙伴解决方案（负载平衡器）的一部分
- AWS 常见问题解答

AWS 术语

October 17, 2024

本部分内容介绍常用的 AWS 术语和短语列表。有关更多信息，请参阅 AWS 词汇表。

术语	定义
Amazon Machine Image (AMI)	计算机映像，提供启动实例（云中的虚拟服务器）所需的信息。
弹性块存储	提供永久块存储卷以用于 AWS 云中的 Amazon EC2 实例。
简单存储服务 (S3)	适用于 Internet 的存储。它旨在为开发人员简化 Web 规模的计算。
弹性计算云 (EC2)	在云中提供安全、可调整大小的计算能力的 Web 服务。它旨在为开发人员简化 Web 规模的云计算。
弹性负载平衡 (ELB)	在多个可用区中多个 EC2 实例之间分布传入应用程序流量。这可提高应用程序的容错。
弹性网络接口 (ENI)	可以连接到虚拟私有云 (VPC) 中的实例的虚拟网络接口。
弹性 IP (EIP) 地址	在 Amazon EC2 或 Amazon VPC 中分配且附加到实例的静态公用 IPv4 地址。弹性 IP 地址与您的帐户相关联，而不是与特定实例相关联。因为您可以在您的需求变化时轻松分配、附加、分离和释放这些地址，因此它们是弹性的。
实例类型	Amazon EC2 提供了多种实例类型，针对不同的用例进行了优化。实例类型包括 CPU、内存、存储和网络容量的各种组合，让您能够为您的应用程序灵活选择合适的资源组合。
身份识别和访问管理 (IAM)	具有权限策略的 AWS 身份，这些策略确定该身份在 AWS 中可以执行哪些操作以及不能执行哪些操作。您可以使用 IAM 角色启用 EC2 实例上运行的应用程序以安全地访问 AWS 资源。采用高可用性设置部署 VPX 实例时，需要 IAM 角色。
Internet 网关	将网络连接到 Internet。您可以将您的 VPC 外部的 IP 地址的流量路由到 Internet 网关。
密钥对	一组用于以电子方式证明您的身份的安全凭据。密钥对由私钥和公钥组成。
路由表	一组控制离开与路由表相关联的任何子网的流量的路由规则。您可以将多个子网与单个路由表相关联，但一个子网一次只能与一个路由表相关联。
安全组	实例的一组指定的允许入站网络连接。
Subnets	EC2 实例可以附加到的 VPC 的一段 IP 地址范围。您可以根据安全和操作需求创建子网来对实例进行分组。
虚拟私有云 (VPC)	用于置备 AWS 云的逻辑隔离部分的 Web 服务，在此部分您可以在您定义的虚拟网络中启动 AWS 资源。

术语	定义
Auto Scaling	用于根据用户定义的策略、计划和运行状况检查自动启动或终止 Amazon EC2 实例的 Web 服务。
CloudFormation	用于编写或更改模板的服务，这些模板用于将相关 AWS 资源作为一个单元进行创建和删除。

AWS-VPX 支持列表

October 17, 2024

下表列出了受支持的 VPX 模型和 AWS 区域、实例类型及服务。

表 1：AWS 上受支持的 VPX 模型

受支持的 VPX 模型
NetScaler VPX Advanced - 200 Mbps
NetScaler VPX Premium - 1 Gbps
NetScaler VPX Premium - 5 Gbps
NetScaler VPX Express-20 Mbps
NetScaler VPX - 客户许可
NetScaler VPX FIPS - 客户许可
NetScaler VPX FIPS ENA - 客户许可

表 2：支持的 AWS 区域

受支持的 AWS 区域
美国西部（俄勒冈州）
美国西部（加利福尼亚北部）加利福尼亚)
美国东部（俄亥俄州）
美国东部（弗吉尼亚北部）弗吉尼亚州）
亚太地区（孟买）
亚太地区（首尔）
亚太地区（新加坡）
亚太地区（悉尼）

| 亚太地区（东京）|
| 亚太地区（香港）|
| 亚太地区（大阪）|
| 亚太地区（雅加达）|
| 亚太地区（海得拉巴）|
| 加拿大（中部）|
| 欧洲（法兰克福）|
| 欧洲（爱尔兰）|
| 欧洲（伦敦）|
| 欧盟（巴黎）|
| 欧洲（米兰）|
| 南美洲（圣保罗）|
| AWS GovCloud（美国东部）|
| AWS GovCloud（美国西部）|
| AWS Top Secret (C2S) |
| 中东（巴林）|
| 非洲（开普敦）|
| C2S |

> 注意：
>
> 对于 AWS 香港区域，NetScaler VPX 支持仅在获得 BYOL 许可的情况下可用。

表 3：受支持的 AWS 实例类型

| 受支持的 AWS 实例类型 |
| ——————————————————————————————————|
| c4.large、c4.xlarge、c4.2xlarge、c4.4xlarge、c4.8xlarge |
| c5.large、c5.xlarge、c5.2xlarge、c5.4xlarge、c5.9xlarge、c5.18xlarge、c5.24xlarge |
| c5n.large、c5n.xlarge、c5n.2xlarge、c5n.4xlarge、c5n.9xlarge、c5n.18xlarge |
| d2.xlarge、d2.2xlarge、d2.4xlarge、d2.8xlarge |
| m3.large、m3.xlarge、m3.2xlarge |
| m4.large、m4.xlarge、m4.2xlarge、m4.4xlarge、m4.10xlarge、m4.16xlarge |
| m5.large、m5.xlarge、m5.2xlarge、m5.4xlarge、m5.8xlarge、m5.12xlarge、m5.16xlarge、m5.24xlarge |
| m5a.large、m5a.xlarge、m5a.2xlarge、m5a.4xlarge、m5a.8xlarge、m5a.12xlarge、m5a.16xlarge、m5a.24xlarge |
| m5n.large、m5n.xlarge、m5n.2xlarge、m5n.4xlarge、m5n.8xlarge、m5n.12xlarge、m5n.16xlarge、m5n.24xlarge |
| m6i.large、m6i.xlarge、m6i.2xlarge、m6i.4xlarge、m6i.8xlarge、m6i.12xlarge、m6i.16xlarge、m6i.24xlarge、m6i.32xlarge |
| r7iz.large、r7iz.xlarge、r7iz.2xlarge、r7iz.4xlarge、r7iz.8xlarge、r7iz.12xlarge、r7iz.16xlarge、r7iz.32xlarge |

|
| t2.medium、t2.large、t2.xlarge、t2.2xlarge |
| t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge |

> 注意：
>
> 在 AWS m6i 和 r7iz 实例类型上配置的 NetScaler VPX 不支持 ENA 低延迟队列 (LLQ) 功能。

表 4：受支持的 AWS 服务

受支持的 AWS 服务
EC2：启动 ADC 实例。
Lambda：在从 CFT 配置 NetScaler VPX 实例期间调用 NetScaler VPX NITRO API。
VPC 和 **VPC** 入口路由：VPC 将创建可在其中启动 ADC 的隔离网络。VPC 入口路由在防火墙负载平衡解决方案中使用。
Route53：在 NetScaler AutoScale 解决方案中的所有 NetScaler VPX 节点上分配流量。
ELB：在 NetScaler AutoScale 解决方案中的所有 NetScaler VPX 节点上分配流量。
Cloudwatch：监视 NetScaler VPX 实例的性能和系统参数。
AWS 自动缩放：用于后端服务器自动缩放。
云形成： CloudFormation 模板用于部署 NetScaler VPX 实例。
Simple Queue Service (SQS)：监视后端自动缩放中的纵向扩展和横向扩展事件。
Simple Notification Service (SNS)：监视后端自动缩放中的纵向扩展和横向扩展事件。
Identity and Access Management (IAM)：提供对 AWS 服务和资源的访问。
AWS Outposts：在 AWS Outposts 中配置 NetScaler VPX 实例。

NetScaler 推荐以下 AWS 实例类型：

- 适用于市场版本或基于带宽的池许可的 M5 和 C5n 系列。
- C5n 系列适用于基于 vCPU 的池许可。

AWS 市场中的 VPX 产品	AWS 实例推荐
VPX Express 20、VPX 200	M5.xLarge
VPX 1G、VPX 5G	M5.2xLarge

NetScaler 根据吞吐量推荐以下 AWS 实例类型。

具有池许可的 VPX（带宽许可证）	AWS 实例推荐
VPX 8G	C5n.4xLarge
VPX 10 克，VPX 15 克，VPX 25 克	C5n.9xLarge

> 注意：
>
> VPX 25G 产品无法在 AWS 中提供所需的 25G 吞吐量，但可以提供更高的 SSL 事务速率。

要实现超过 5G 的吞吐量，请执行以下操作：

- 在 AWS 市场上选择 **NetScaler VPX -** 客户许可 **(BYOL)** 产品。
- 在 NetScaler GUI 或 CLI 中选择 池许可（带宽许可证）。

要根据每秒数据包数、SSL 事务率等不同指标确定您的实例，请联系您的 NetScaler 联系人以获取指导。如需获取基于 vCPU 的池许可和规模调整指南，请联系 NetScaler 支持部门。

局限性与用法指南

October 17, 2024

在 AWS 上部署 NetScaler VPX 实例时，应遵循以下限制和使用准则：

- 在开始之前，请阅读 在 AWS上部署 NetScaler VPX 实例 中的 AWS 术语部分。
- VPX 不支持群集功能。
- 为使高可用性设置有效运行，请将专用 NAT 设备关联到管理界面或将 EIP 关联到 NSIP。有关 NAT 的详细信息，请参阅 AWS 文档中的 NAT Instances（NAT 实例）。
- 必须使用属于两个不同子网的 ENI 将数据流量与管理流量隔离。
- 管理 ENI 上必须仅存在 NSIP 地址。
- 如果使用 NAT 实例来实现安全性，而不是将 EIP 分配给 NSIP，需要更改恰当的 VPC 级别路由。有关更改 VPC 级别路由的说明，请参阅 AWS 文档中的 场景 2：带有公有子网和私有子网的 VPC。
- VPX 实例可以从一种 EC2 实例类型移动到另一种类型（例如，从 m3.large 到 m3.xlarge）。
- 对于 AWS 上的 VPX 的存储方案，Citrix 建议选择 EBS，因为它具有持久性，并且即使从实例断开连接，仍然可用。
- 不支持将 ENI 动态添加到 VPX。请重新启动 VPX 实例以应用更新。Citrix 建议您停止独立或高可用性实例，连接新的 ENI，然后重新启动实例。

- 您可以将多个 IP 地址分配给一个 ENI。每个 ENI 的最大 IP 地址数取决于 EC2 实例类型，请参阅 弹性网络接口中的“每个实例类型的每个网络接口的 IP 地址”一节。在将 IP 地址分配给 ENI 之前，您必须在 AWS 中分配 IP 地址。有关详细信息，请参阅 弹性网络接口。
- Citrix 建议您避免在 NetScaler VPX 接口上使用 enable interface 和 disable interface 命令。
- 默认情况下，NetScaler `set ha node \\<NODE\\_ID\\> -haStatus STAYPRIMARY` 和 `set ha node \\<NODE\\_ID\\> -haStatus STAYSECONDARY` 命令处于禁用状态。
- VPX 不支持 IPv6。
- 由于 AWS 的限制，不支持以下功能：
  - 免费 ARP (GARP)
  - L2 模式
  - 已标记的 VLAN
  - 动态路由
  - 虚拟 MAC
- 为了使 RNAT 正常工作，请确保 **Source/Destination Check**（源/目标检查）已禁用。有关更多信息，请参阅 弹性网络接口中的“更改源/目标检查”。
- 在 AWS 上的 NetScaler VPX 部署中，在某些 AWS 区域，AWS 基础结构可能无法解析 AWS API 调用。如果通过 NetScaler VPX 实例上的非管理接口发出 API 调用，就会发生这种情况。解决方法为，将 API 调用限制为仅对管理接口。为此，请在 VPX 实例上创建 NSVLAN，然后使用相应的命令将管理接口绑定到 NSVLAN。例如：`设置ns 配置 -nsvlan <vlan id> -ifnum 1/1 -tagged NO 保存配置` 在提示符下重新启动 VPX 实例。有关配置 `nsvlan` 的更多信息，请参阅 配置 NSVLAN。
- 在 AWS 控制台中，**Monitoring**（监视）选项卡下显示的 VPX 实例的 vCPU 使用率可能很高（高达 100%），即使实际使用率要低得多亦如此。要查看实际 vCPU 使用率，请导航到 **View all CloudWatch metrics**（查看所有 CloudWatch 指标）。有关更多信息，请参阅 使用 Amazon CloudWatch监控您的实例。
- 仅在 AWS 上使用 NetScaler 的 PV 和 SRIOV 接口支持热添加。具有 ENA 接口的 VPX 实例不支持热插拔，如果尝试热插拔，实例的行为可能会不可预测。
- NetScaler 的 PV、SRIOV 和 ENA 接口不支持通过 AWS Web 控制台或 AWS CLI 界面进行热删除。如果尝试热删除，实例的行为可能不可预测。

必备条件

October 17, 2024

尝试在 AWS 中创建 VPX 实例之前，请确保您具有以下条件：

- **AWS** 帐户：在 AWS 虚拟私有云 (VPC) 中启动 NetScaler VPX AMI。您可以在 www.aws.amazon.com 上免费创建 AWS 帐户。
- **AWS Identity and Access Management (IAM)** 用户帐户：用于安全地控制您的用户对 AWS 服务和资源的访问。有关如何创建 IAM 用户帐户的更多信息，请参阅 创建 IAM 用户 (控制台)。对于独立部署和高可用性部署，IAM 角色都是必需的。

  与您的 AWS 帐户关联的 IAM 角色在各种情况下必须具有以下 IAM 权限。

  高可用性与同一 **AWS** 区域中的 **IPv4** 地址配对：

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

  高可用性与同一 **AWS** 区域中的 **IPv6** 地址配对：

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

  在同一 **AWS** 区域中同时使用 **IPv4** 和 **IPv6** 地址的高可用性配对**:**

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

  HA 与跨不同 **AWS** 区域的弹性 **IP** 地址配对：

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

  HA 与不同 **AWS** 区域中的专用 **IP** 地址配对：

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
```



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

高可用性与不同 **AWS** 区域中的私有 **IP** 和弹性 **IP** 地址配对：

```
    "ec2:DescribeInstances",
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
    "ec2:CreateRoute",
    "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "ec2:CreateTags"
```

AWS 后端自动扩缩：

```
    "ec2:DescribeInstances",
    "autoscaling:*",
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sqs:CreateQueue",
    "sqs:ListQueues",
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole",
    "ec2:CreateTags"
```

> 注意：
>
> - 如果您使用上述功能的任意组合，请使用每个功能的 IAM 权限组合。
> - 如果使用 Citrix CloudFormation 模板，则会自动创建 IAM 角色。该模板不允许选择已创建的 IAM 角色。
> - 通过 GUI 登录 VPX 实例时，会出现为 IAM 角色配置所需权限的提示。如果已配置权限，请忽略该提示。

- **AWS CLI**：用于从您的终端程序使用 AWS 管理控制台提供的所有功能。有关更多信息，请参阅 AWS CLI 用户指南。还需要使用 AWS CLI 将网络接口类型更改为 SR-IOV。
- 弹性网络适配器 **(ENA)**：对于启用了 ENA 驱动程序的实例类型，例如 M5、C5 实例，固件版本必须为 13.0 及以上。
- 您必须在 EC2 实例上为 NetScaler VPX 配置实例元数据服务 (IMDS)。IMDSv1 和 IMDSv2 是两种可用于从正在运行的 AWS EC2 实例访问实例元数据的模式。IMDSv2 比 IMDSv1 更安全。您可以将实例配置为同时使

用两种方法（默认选项）或仅使用 IMDSv2 模式（通过禁用 IMDSv1）。从 NetScaler VPX 版本 13.1.48.x 起，Citrix ADC VPX 仅支持 IMDSv2 模式。

在 **NetScaler VPX** 实例上配置 **AWS IAM** 角色

October 17, 2024

在 Amazon EC2 实例上运行的应用程序必须在 AWS API 请求中包含 AWS 证书。您可以将 AWS 证书直接存储在 Amazon EC2 实例中，并允许该实例中的应用程序使用这些证书。但是您随后必须管理证书，确保它们安全地将证书传递给每个实例，并在需要轮换证书时更新每个 Amazon EC2 实例。这是大量额外的工作。

相反，您可以而且必须使用身份和访问管理 (IAM) 角色来管理在 Amazon EC2 实例上运行的应用程序的临时证书。使用角色时，不必向 Amazon EC2 实例分配长期证书（例如用户名和密码或访问密钥）。相反，该角色提供了应用程序在调用其他 AWS 资源时可以使用的临时权限。当您启动 Amazon EC2 实例时，您需要指定一个与该实例关联的 IAM 角色。然后，在实例上运行的应用程序可以使用角色提供的临时证书来签署 API 请求。

与您的 AWS 帐户关联的 IAM 角色在各种情况下必须具有以下 IAM 权限。

高可用性与同一 **AWS** 区域中的 **IPv4** 地址配对：

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

高可用性与同一 **AWS** 区域中的 **IPv6** 地址配对：

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

在同一 **AWS** 区域中同时使用 **IPv4** 和 **IPv6** 地址的高可用性配对**:**

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

HA 与跨不同 **AWS** 区域的弹性 **IP** 地址配对：

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
```



```
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

HA 与不同 **AWS** 区域中的专用 **IP** 地址配对：

```
    "ec2:DescribeInstances",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
    "ec2:CreateRoute",
    "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

高可用性与不同 **AWS** 区域中的私有 **IP** 和弹性 **IP** 地址配对：

```
    "ec2:DescribeInstances",
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DeleteRoute",
    "ec2:CreateRoute",
    "ec2:ModifyNetworkInterfaceAttribute",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

AWS 后端自动扩缩：

```
    "ec2:DescribeInstances",
    "autoscaling:*",
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sqs:CreateQueue",
    "sqs:ListQueues",
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes",
    "iam:SimulatePrincipalPolicy",
    "iam:GetRole"
```

注意事项：

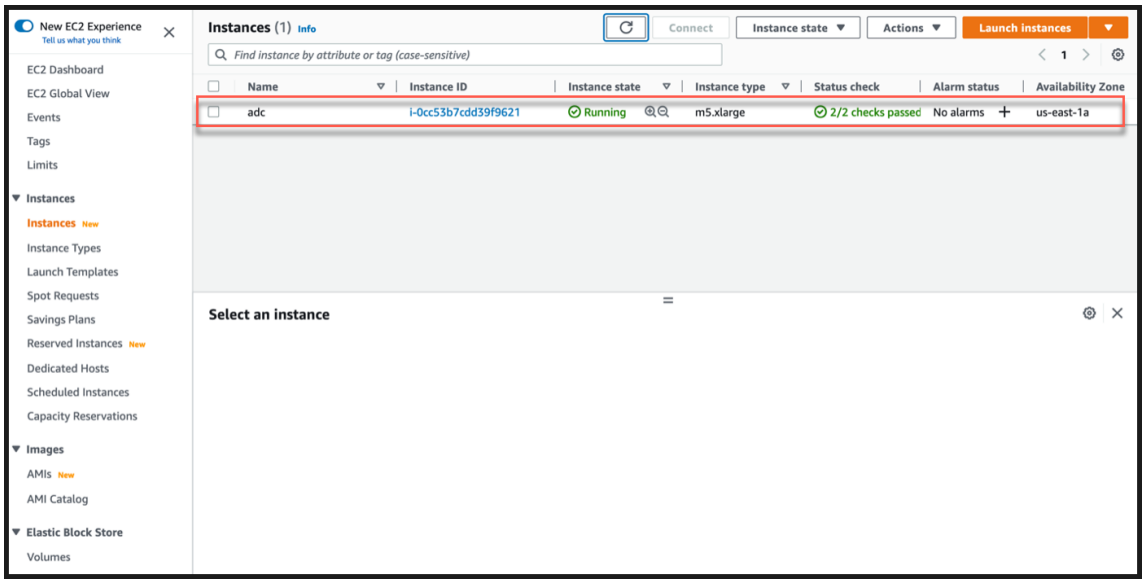
- 如果您使用上述功能的任意组合，请使用每个功能的 IAM 权限组合。
- 如果使用 Citrix CloudFormation 模板，则会自动创建 IAM 角色。该模板不允许选择已创建的 IAM 角色。
- 通过 GUI 登录 VPX 实例时，会出现为 IAM 角色配置所需权限的提示。如果已配置权限，请忽略该提示。
- 对于独立部署和高可用性部署，IAM 角色都是必需的。

创建 **IAM** 角色

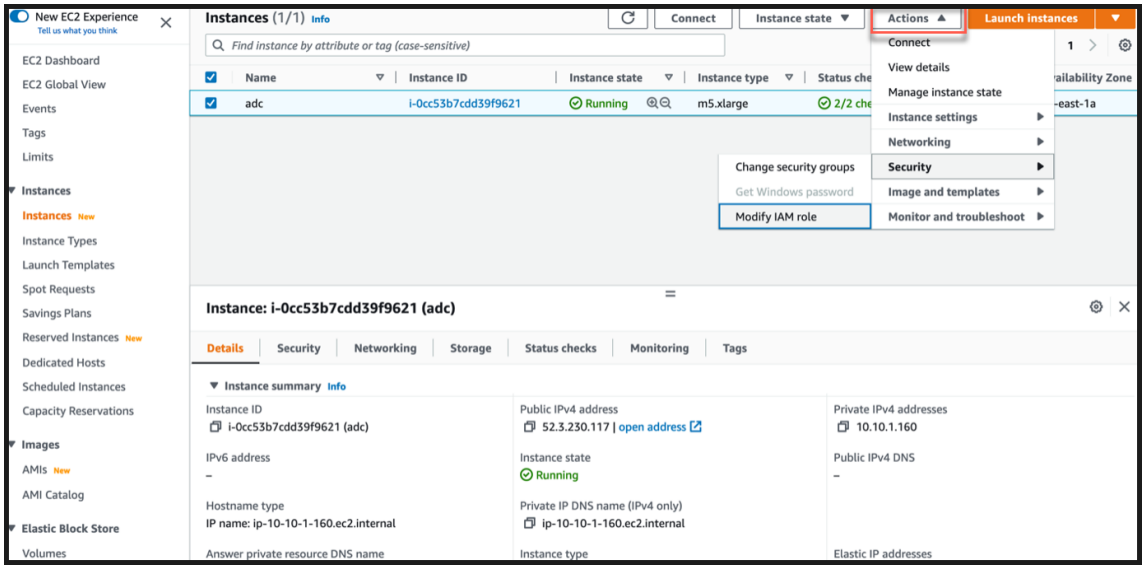
此过程介绍如何为 AWS 后端自动扩展功能创建 IAM 角色。

> 注意：
>
> 您可以按照相同的程序创建与其他功能对应的任何 IAM 角色。

1. 登录适用于 EC2 的 AWS 管理控制台。
2. 转到 EC2 实例页面，然后选择您的 ADC 实例。

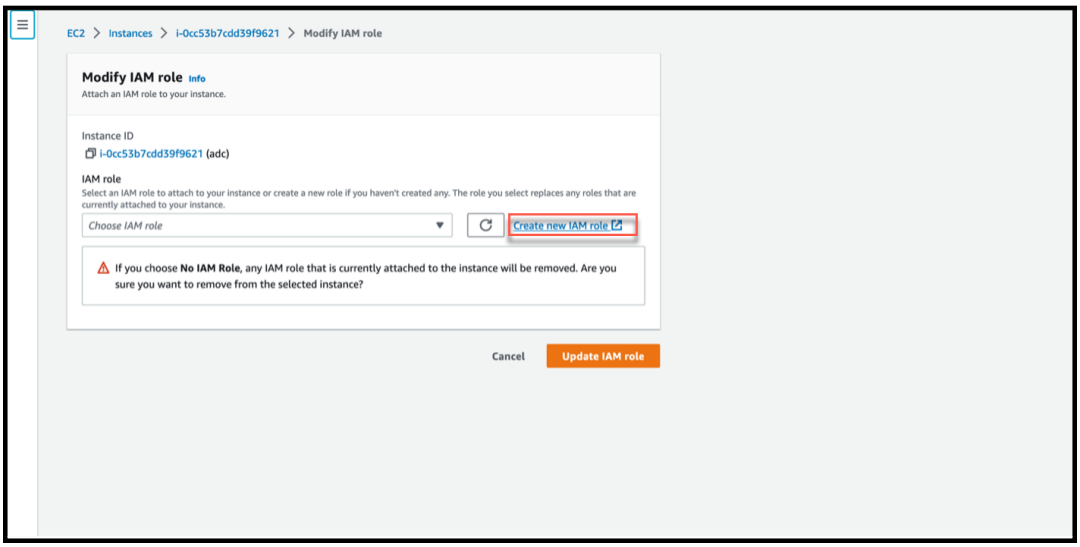


3. 导航到 操作 **>** 安全 **>** 修改 **IAM** 角色。

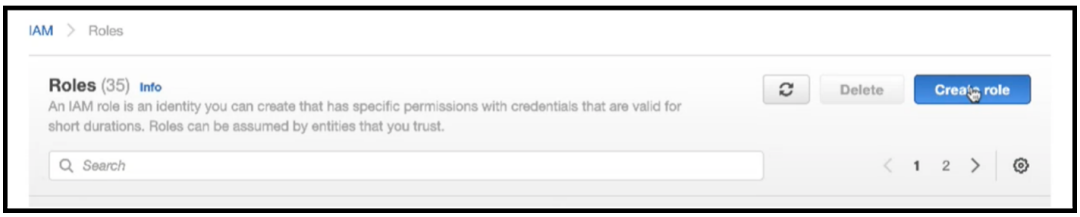


4. 在 修改 **IAM** 角色 页面中，您可以选择现有 IAM 角色或创建 IAM 角色。
5. 要创建 IAM 角色，请执行以下步骤：

a) 在 修改 **IAM** 角色 页面中，单击 创建新的 **IAM** 角色。



b) 在“角色”页面中，单击“创建角色”。



c) 在“可信实体类型”下选择 **AWS** 服务，在“常见用例”下选择 **EC2** ，然后单击“下一步”。

d) 在“添加权限”页面中，单击“创建策略”。

e) 单击 **JSON** 选项卡打开 JSON 编辑器。

f) 在 JSON 编辑器中，删除所有内容并粘贴要使用的功能的 IAM 权限。

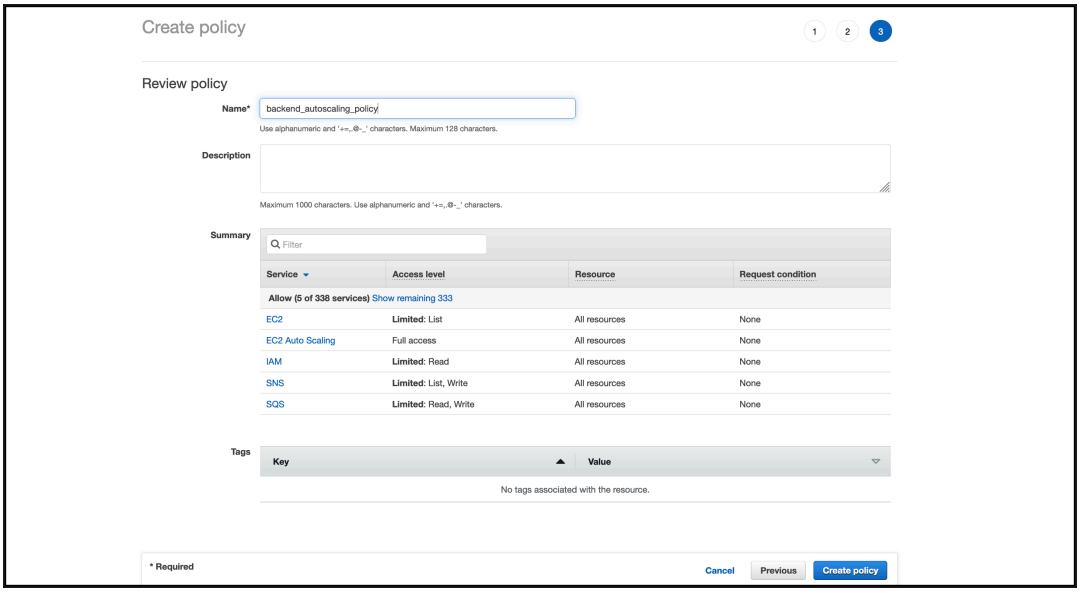
例如，粘贴以下 AWS 后端自动扩展功能的 IAM 权限：

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "autoscaling:*",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListTopics",
                "sns:Subscribe",
                "sqs:CreateQueue",
                "sqs:ListQueues",
                "sqs:DeleteMessage",
                "sqs:GetQueueAttributes",
                "sqs:SetQueueAttributes",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*"
        }

    ]
}
```

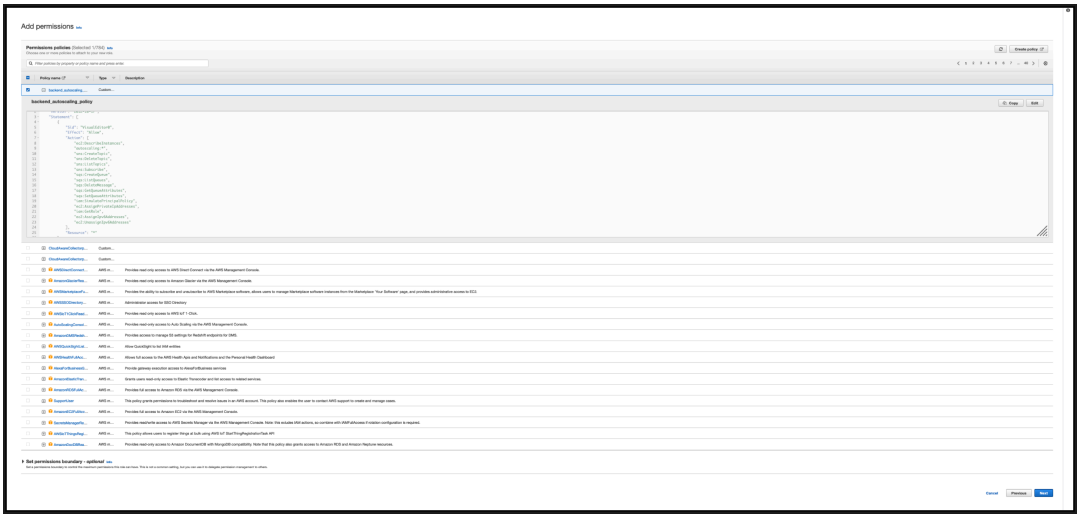
确保您提供的“版本”密钥值对与 AWS 自动生成的密钥值对相同。

g) 单击“下一步：审阅”。

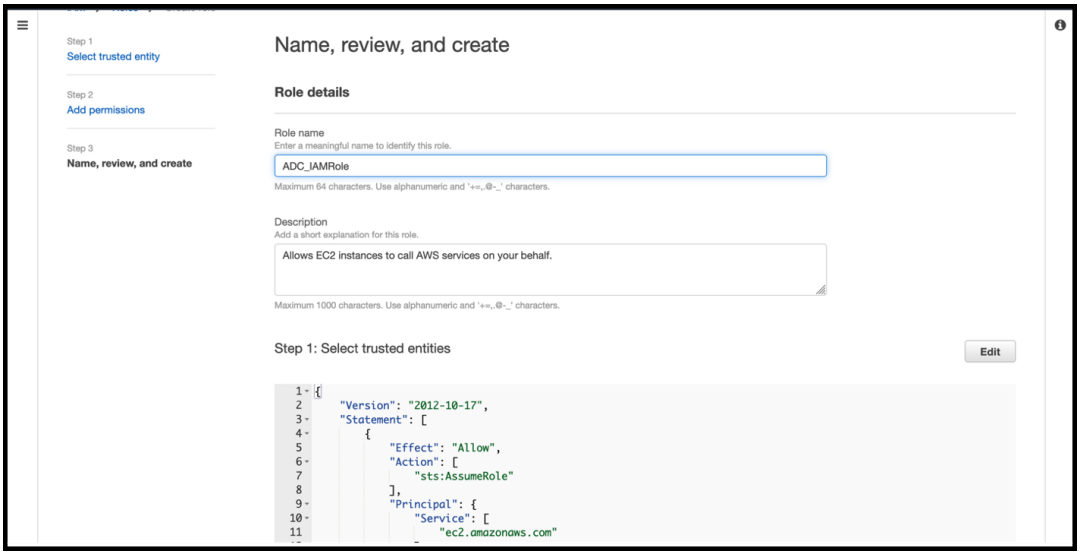
h) 在“查看策略”选项卡中，为策略指定有效名称，然后单击“创建策略”。



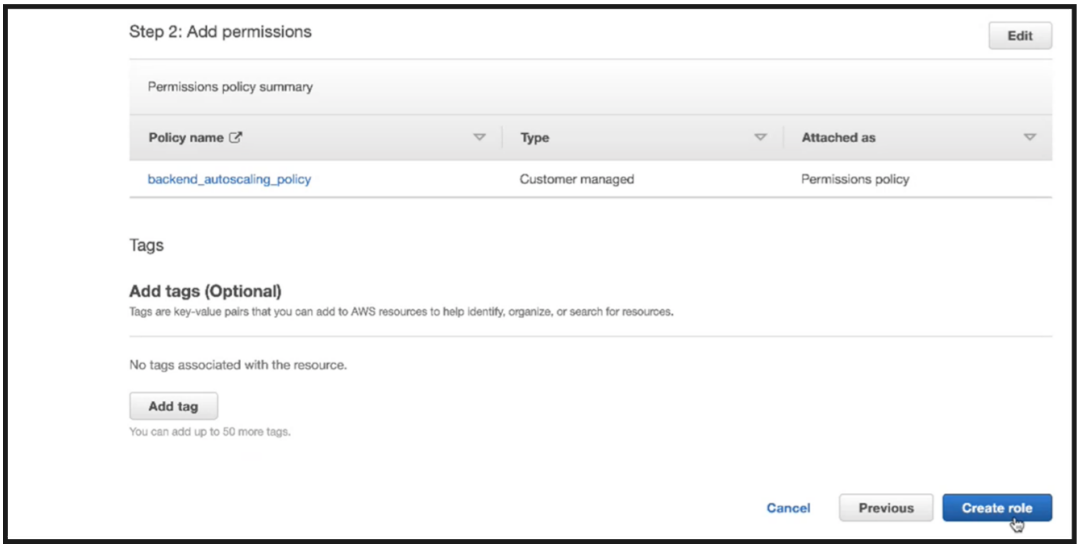
i) 在“身份访问管理”页面中，单击您创建的策略名称。展开策略以检查整个 JSON，然后单击“下一步”。



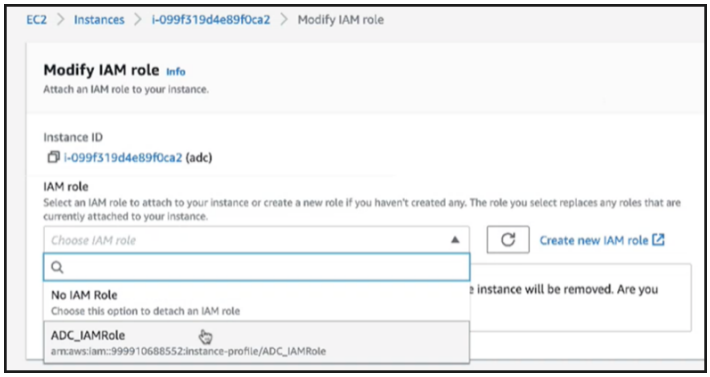
j) 在“名称、查看和创建”页面中，为角色指定有效名称。



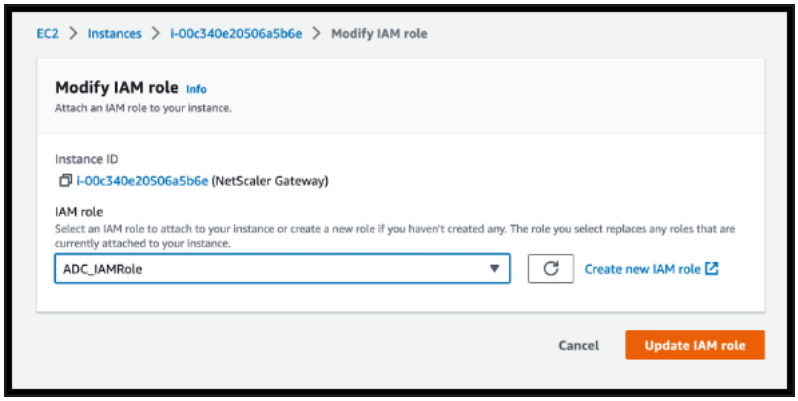
k) 单击“创建角色”。



6. 重复步骤：1、2 和 3。选择“刷新”按钮，然后选择下拉菜单以查看您创建的角色。



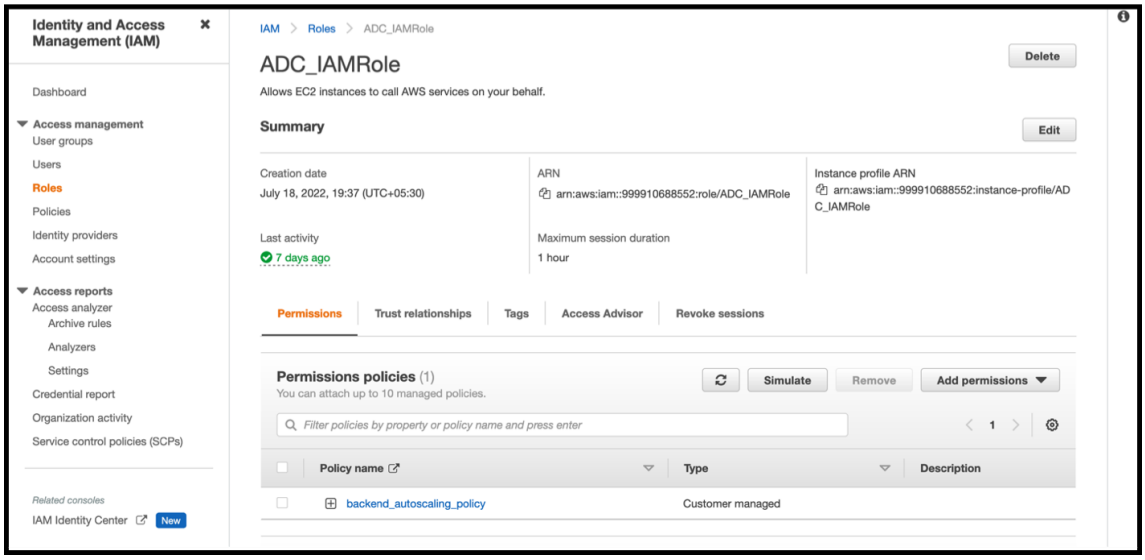
7. 单击“更新 **IAM** 角色”。



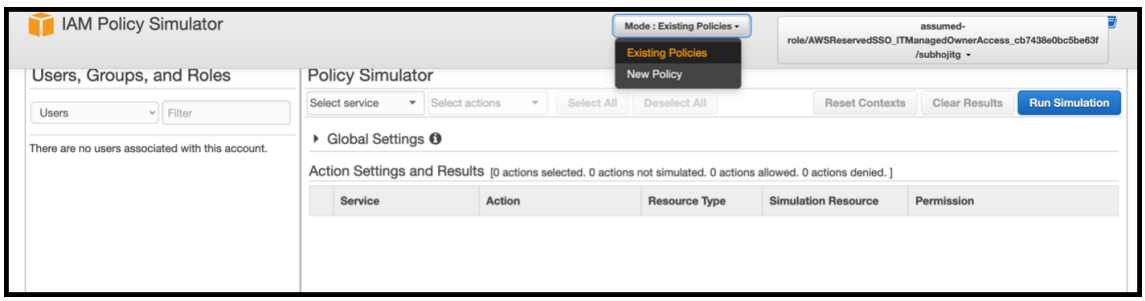
使用 **IAM** 策略模拟器测试 **IAM** 策略

IAM 策略模拟器是一种工具，可让您在将 IAM 访问控制策略提交到生产环境之前测试 IAM 访问控制策略的效果。验证权限和排除权限问题更容易。

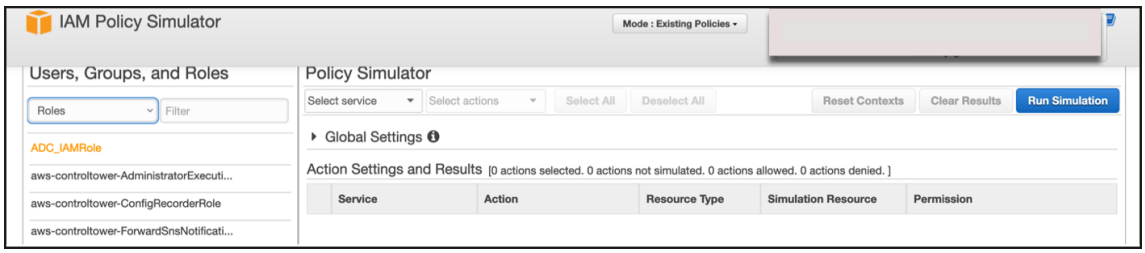
1. 在 **IAM** 页面中，选择要测试的 IAM 角色，然后单击“模拟”。在以下示例中，“ADC_IAMRole”是 IAM 角色。



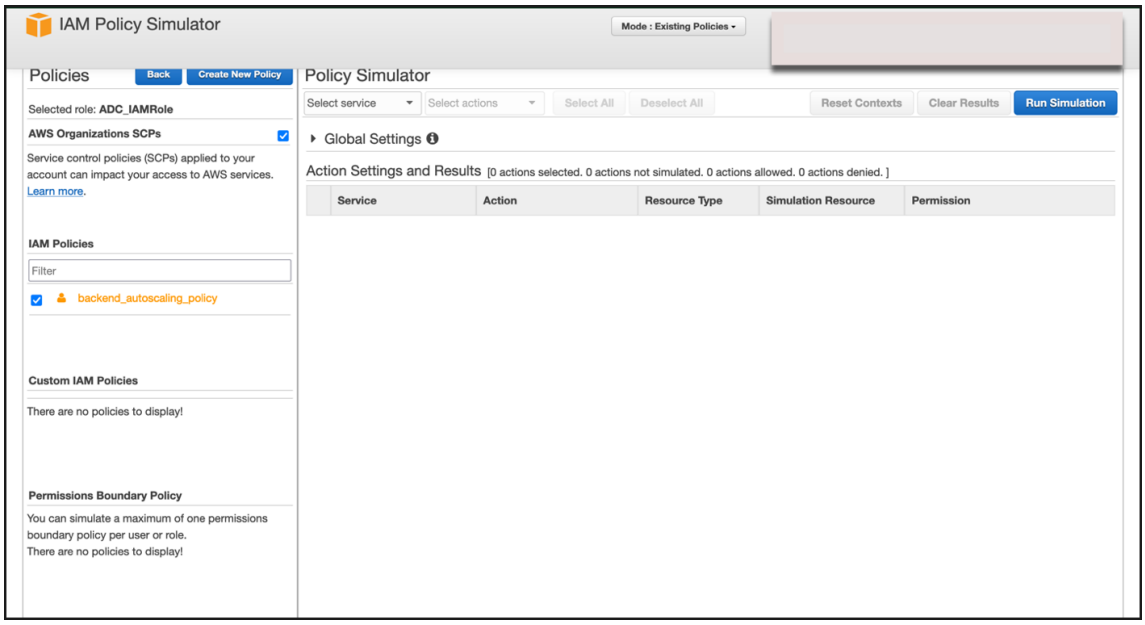
2. 在 **IAM** 策略模拟器 控制台中，选择 现有策略 作为 模式。



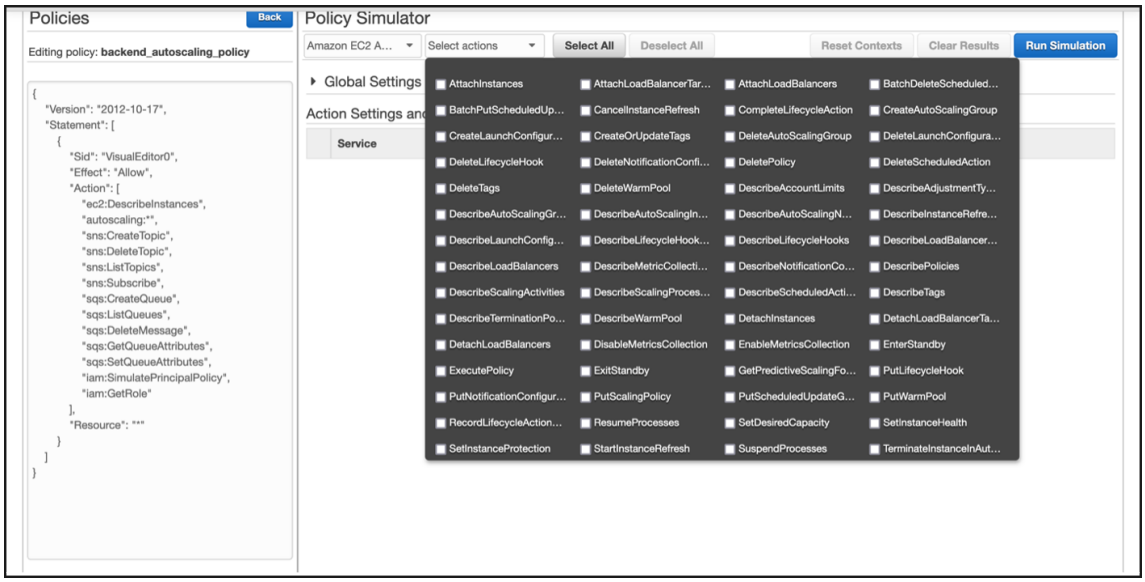
3. 在 用户、组和角色 选项卡中，从下拉菜单中选择 角色，然后选择现有角色。



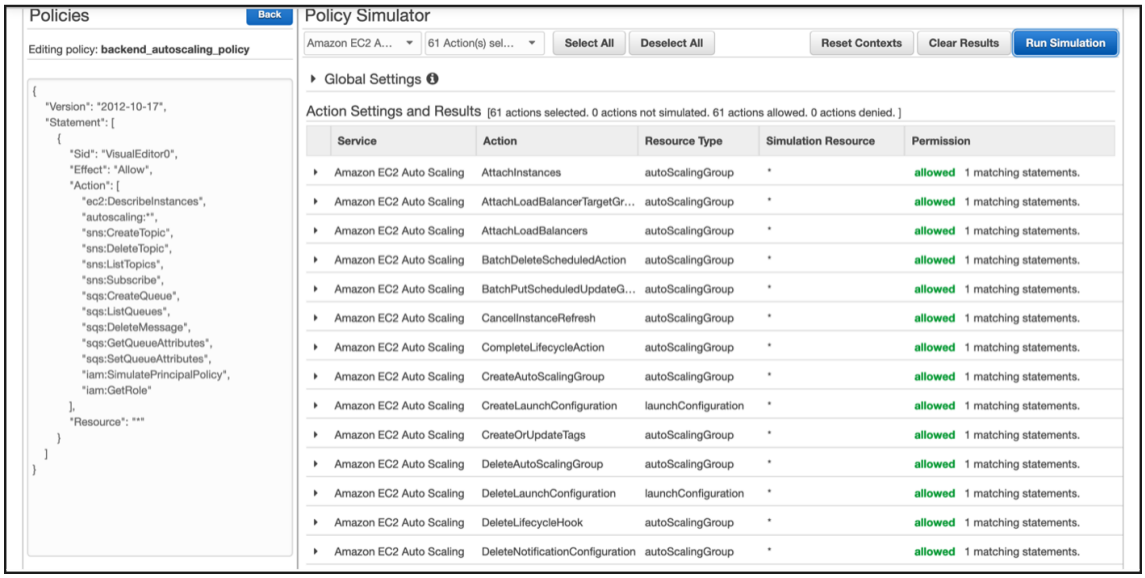
4. 选择现有角色后，选择其下的现有策略。



5. 选择策略后，您可以在屏幕左侧看到确切的 JSON。在“选择操作”下拉菜单中 选择所需的操作。



6. 单击“运行模拟”。



有关详细信息，请参阅 AWS IAM 文档。

其他参考文献

使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限

AWS 上的 NetScaler VPX 实例的工作原理

October 17, 2024

NetScaler VPX 实例在 AWS 市场中作为 AMI 提供，可以在 AWS VPC 中作为 EC2 实例启动。NetScaler VPX AMI 实例最低需要 2 个虚拟 CPU 和 2 GB 内存。从 AWS VPC 内启动的 EC2 实例还可以提供多个接口，每个接口有多个 IP 地址，以及 VPX 配置所需的公用和专用 IP 地址。每个 VPX 实例至少需要三个 IP 子网：

- 管理子网
- 面向客户端的子网 (VIP)
- 面向后端的子网（SNIP、MIP 等）

Citrix 建议对 AWS 安装上的标准 VPX 实例使用三个网络接口。

AWS 目前只对在 AWS VPC 中运行的实例提供多 IP 功能。VPC 中的 VPX 实例可用于对 EC2 实例中运行的服务器实现负载平衡。Amazon VPC 允许您创建和控制虚拟网络环境，包括您自己的 IP 地址范围、子网、路由表和网络网关。

> 注意：

> 默认情况下，每个 AWS 帐户的每个 AWS 区域最多可以创建 5 个 VPC 实例。可以通过提交 Amazon 的申请表 http://aws.amazon.com/contact-us/vpc-request 来申请更高的 VPC 限制。

图 **1.** AWS 架构上的 NetScaler VPX 实例部署示例

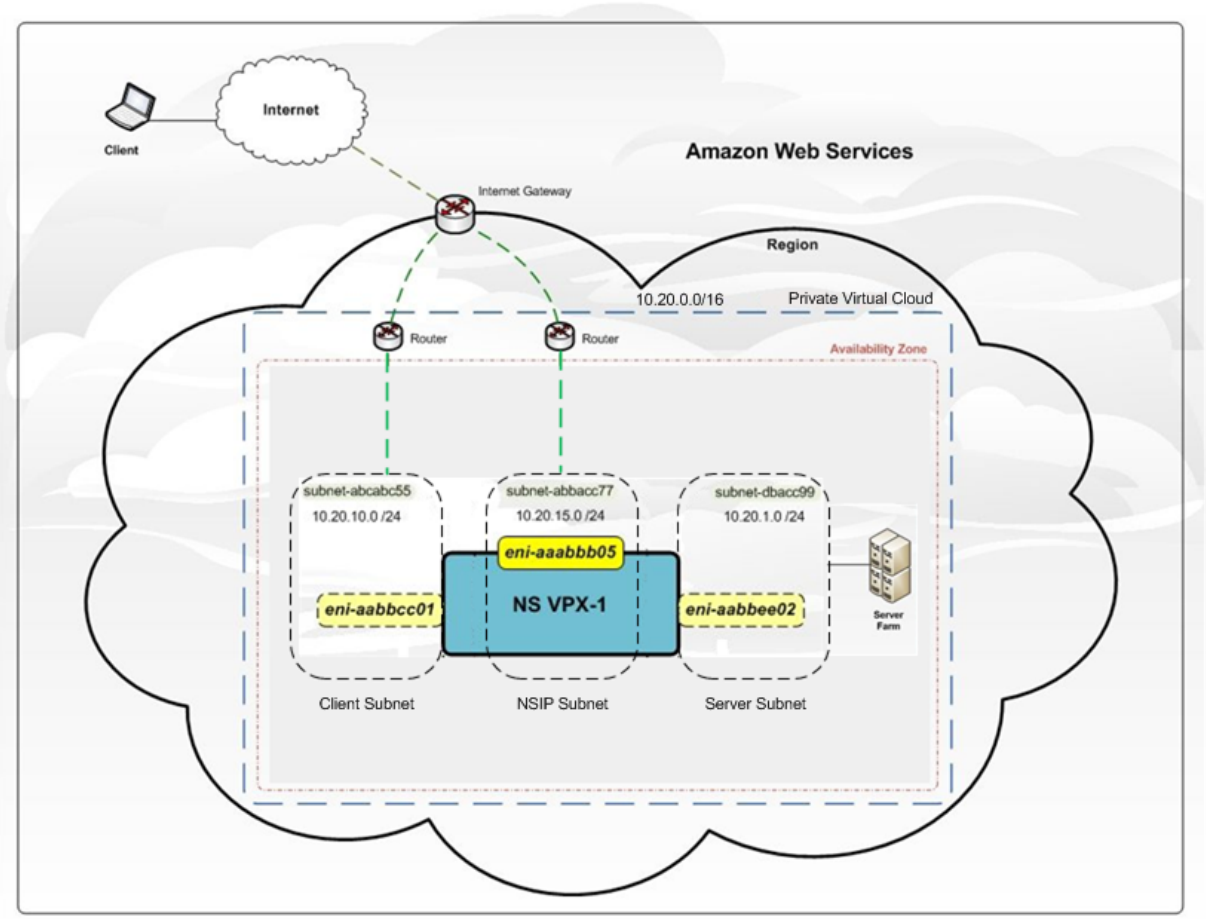


图 1 显示了 AWS VPC 的简单拓扑，其中 NetScaler VPX 部署。AWS VPC 包含：

1. 用于路由 VPC 内外部流量的单个 Internet 网关。
2. Internet 网关与 Internet 之间的网络连接。
3. 三个子网，分别用于管理、客户端和服务器。
4. Internet 网关与两个子网（管理和客户端）之间的网络连接。
5. 在 VPC 中部署的独立的 NetScaler VPX 实例。VPX 实例有三个 ENI，分别附加到每个子网。

在 **AWS** 上部署 **NetScaler VPX** 独立实例

October 17, 2024

您可以使用以下选项在 AWS 上部署 NetScaler VPX 独立实例：

- AWS Web 控制台
- Citrix 编写的 CloudFormation 模板
- AWS CLI

本主题介绍在 AWS 上部署 NetScaler VPX 实例的过程。

在开始部署之前，请阅读以下主题：

- 必备条件
- 局限性与用法指南

使用 **AWS Web** 控制台在 **AWS** 上部署 **NetScaler VPX** 实例

可以通过 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例。部署过程包括以下步骤：

1. 创建密钥对
2. 创建虚拟私有云 (VPC)
3. 添加更多子网
4. 创建安全组和安全规则
5. 添加路由表
6. 创建 Internet 网关
7. 创建 NetScaler VPX 实例
8. 创建和连接更多网络接口
9. 将弹性 IP 地址附加到管理 NIC
10. 连接到 VPX 实例

步骤 **1**：创建密钥对。

Amazon EC2 使用密钥对来加密和解密登录信息。要登录实例，必须创建密钥对，在启动实例时指定密钥对的名称，然后在连接到实例时提供私钥。

使用 AWS 启动实例向导查看和启动实例时，系统会提示您使用现有密钥对或创建新密钥对。有关如何创建密钥对的更多信息，请参阅 Amazon EC2 密钥对。

步骤 **2**：创建 **VPC**。

NetScaler VPC 实例部署在 AWS VPC 内部。VPC 允许您定义专用于您的 AWS 帐户的虚拟网络。有关 AWS VPC 的更多信息，请参阅 Amazon VPC 入门。

为您的 NetScaler VPX 实例创建 VPC 时，请注意以下几点。

- 使用“VPC with a Single Public Subnet Only”（仅限具有单个公用子网的 VPC）选项在 AWS 可用区中创建一个 AWS VPC。
- Citrix 建议您至少创建三个以下任一类型的子网：
  - 一个用于管理流量的子网。可将管理 IP (NSIP) 放置在此子网上。默认情况下，弹性网络接口 (ENI) eth0 用于管理 IP。

- 一个或多个用于客户端访问（用户到 NetScaler VPX）流量的子网，客户端可以通过这些子网连接到分配给 NetScaler 负载平衡虚拟服务器的一个或多个虚拟 IP (VIP) 地址。
- 一个或多个用于服务器访问（VPX 到服务器）流量的子网，服务器可以通过这些子网连接到 VPX 所拥有的子网 IP (SNIP) 地址。有关 NetScaler 负载平衡和虚拟服务器、虚拟 IP 地址 (VIP) 和子网 IP 地址 (SNIP) 的更多信息，请参见：
- 所有子网必须位于同一可用性区域中。

步骤 **3**：添加子网。

当您使用 VPC 向导时，只创建了一个子网。根据您的要求，您可能需要创建更多子网。有关如何创建更多子网的更多信息，请参阅 向 VPC 添加子网。

步骤 **4**：创建安全组和安全规则。

要控制入站和出站流量，请创建安全组并向组添加规则。有关如何创建组和添加规则的更多信息，请参阅 您的 VPC 的安全组。

对于 NetScaler VPX 实例，EC2 向导提供默认安全组，这是由 AWS Marketplace 生成并且基于 Citrix 建议的设置。但是，您可以根据您的要求创建更多安全组。

> 注意：
>
> 将分别在安全组中打开端口 22、80、443 以供 SSH、HTTP 和 HTTPS 访问。

步骤 **5**：添加路由表。

路由表包含一组用来确定网络流量的定向位置的规则（称为路由）。您的 VPC 中的每个子网都必须与一个路由表相关联。有关如何创建路由表的详细信息，请参阅 路由表。

步骤 **6**：创建 **Internet** 网关。

Internet 网关有两个用途：在您的 VPC 路由表中提供一个目标以用于 Internet 可路由的流量，以及为已分配公用 IPv4 地址的实例执行网络地址转换 (NAT)。

创建用于 Internet 流量的 Internet 网关。有关如何创建 Internet 网关的更多信息，请参阅 附加 Internet 网关一节。

步骤 **7**：使用 **AWS EC2** 服务创建 **NetScaler VPX** 实例。

要使用 AWS EC2 服务创建 NetScaler VPX 实例，请完成以下步骤。

1. 从 AWS 控制板中，转到 **Compute**（计算）**> EC2 > Launch Instance**（启动实例）**> AWS Marketplace**。

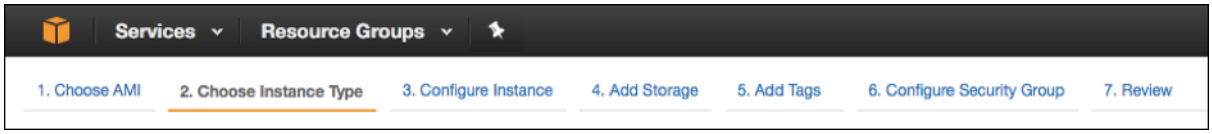
   在单击 **Launch Instance**（启动实例）之前，请通过检查 **Launch Instance**（启动实例）下显示的备注确保您的区域是正确的。

2. 在“Search AWS Marketplace”（搜索 AWS Marketplace）栏中，使用关键字 NetScaler VPX 进行搜索。
3. 选择要部署的版本，然后单击 **Select**（选择）。对于 NetScaler VPX 版本，您可以选择以下选项：

    - 许可使用的版本
    - NetScaler VPX Express 设备（这是一款免费的虚拟设备，可从 NetScaler 12.0 56.20 获得。）
    - 自带设备

“Launch Instance”（启动实例）向导将会启动。按照向导操作以创建实例。向导会提示您：

- 选择实例类型
- 配置实例
- 添加存储
- 添加标记
- 配置安全组
- 审查



步骤 **8**：创建和连接更多网络接口。

再为 VIP 和 SNIP 创建两个网络接口。有关如何创建更多网络接口的详细信息，请参阅 创建网络接口 部分。

创建了网络接口后，必须将其附加到 VPX 实例。在连接接口之前，请关闭 VPX 实例，连接接口，然后打开该实例的电源。有关如何连接网络接口的更多信息，请参阅 启动实例时连接网络接 口部分。

步骤 **9**：分配和关联弹性 **IP**。

如果您为 EC2 实例分配公用 IP 地址，则只有在实例停止之前才会使其保持分配状态。之后，该地址将释放回池中。重新启动实例时，会分配新的公用 IP 地址。

相反，弹性 IP (EIP) 地址会一直保留分配到从实例取消关联该地址时。

为管理 NIC 分配和关联弹性 IP。有关如何分配和关联弹性 IP 地址的详细信息，请参阅以下主题：

- 分配弹性 IP 地址
- 将弹性 IP 地址与正在运行的实例关联

这些步骤即是在 AWS 上创建 NetScaler VPX 实例的过程。实例准备就绪可能需要几分钟时间。检查您的实例是否已通过状态检查。可以在“Instances”（实例）页面的 **Status Checks**（状态检查）列中查看此信息。

步骤 **10**：连接到 **VPX** 实例。

创建 VPX 实例后，可以使用 GUI 和 SSH 客户端连接实例。

- GUI

用于访问 NetScaler VPX 实例的默认管理员凭据如下

用户名：`nsroot`

密码：ns 根帐户的默认密码设置为 NetScaler VPX 实例的 AWS 实例 ID。出于安全原因，首次登录时，系统会提示您更改密码。更改密码后，必须保存配置。如果未保存配置，但实例重新启动，则必须使用默认密码登录。请在出现提示时再次更改密码。

- SSH 客户端

在 **AWS** 管理控制台中，选择 **NetScaler VPX** 实例，然后单击“连接”。按照 Connect to Your Instance**（连接到您的实例）页面上提供的说明进行操作。</p>

有关如何使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 独立实例的更多信息，请参阅 场景：独立实例

使用 **Citrix CloudFormation** 模板配置 **NetScaler VPX** 实例

您可以使用 Citrix 提供的 CloudFormation 模板自动启动 VPX 实例。该模板提供了启动单个 NetScaler VPX 实例或使用一对 NetScaler VPX 实例创建高可用性环境的功能。

可以从 AWS Marketplace 或 GitHub 启动模板。

CloudFormation 模板需要现有的 VPC 环境，并启动一个带有三个弹性网络接口 (ENI) 的 VPX 实例。在启动 CloudFormation 模板之前，请确保满足以下要求：

- AWS 虚拟私有云 (VPC)
- VPC 内有三个子网：一个用于管理，一个用于客户端流量，另一个用于后端服务器
- 用于启用对实例的 SSH 访问的 EC2 密钥对
- 打开了 UDP 3003、TCP 3009—3010、HTTP、SSH 端口的安全组

有关如何完成必备条件的详细信息，请参阅“使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例”部分或 AWS 文档。

观看此 视频 ，了解如何使用 AWS Marketplace 中提供的 Citrix CloudFormation 模板配置和启动 NetScaler VPX 独立实例。

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

对于独立部署，IAM 角色不是强制性的。但是，Citrix 建议您创建一个具有所需权限的 IAM 角色并将其附加到实例，以满足将来的需要。IAM 角色可确保在需要时使用 SR-IOV 轻松将独立实例转换为高可用性节点。

有关所需权限的更多信息，请参阅 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口。

> 注意：
>
> 如果您使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例，则默认情况下，CloudWatch 服务处于启用状态。如果您使用 Citrix CloudFormation 模板部署 NetScaler VPX 实例，则默认选项为“是”。如果要禁用 CloudWatch 服务，请选择“否”。有关更多信息，请参阅 使用 Amazon CloudWatch 监控您的实例

使用 **AWS CLI** 配置 **NetScaler VPX** 实例

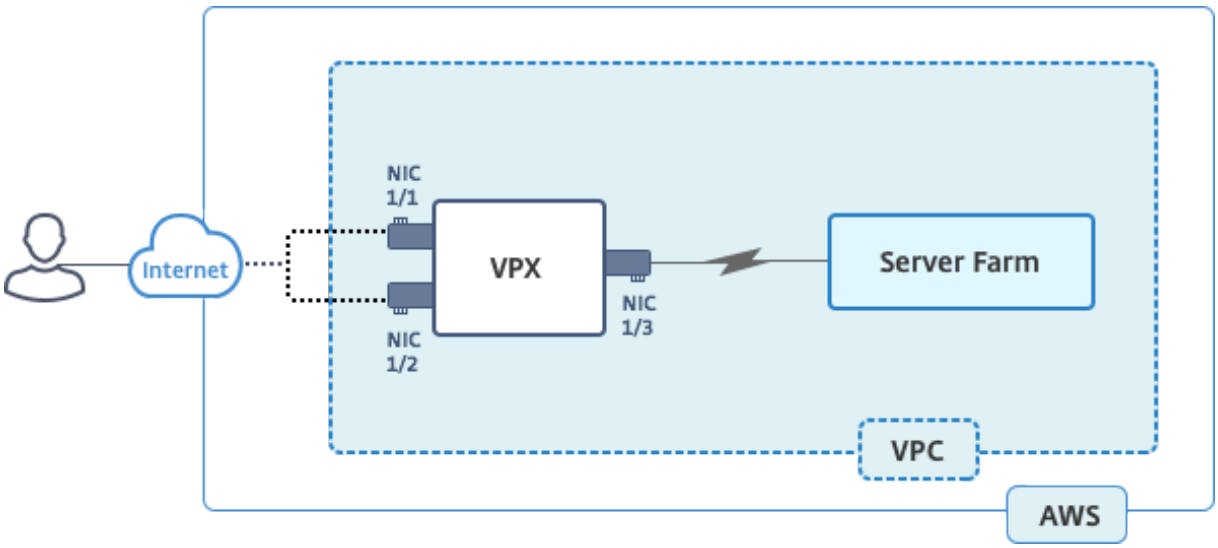
可以使用 AWS CLI 启动实例。有关更多信息，请参阅 AWS 命令行界面文档。

场景：独立实例

October 17, 2024

此场景说明了如何使用 AWS GUI 在 AWS 中部署 NetScaler VPX 独立 EC2 实例。创建一个带有三个 NIC 的独立 VPX 实例。配置为负载平衡虚拟服务器的实例与后端服务器（服务器场）通信。对于此配置，请设置实例与后端服务器之间以及实例与公共 Internet 上的外部主机之间的所需通信路由。

有关部署 VPX 实例的过程的更多详细信息，请参阅 在 AWS 上部署 NetScaler VPX 独立实例。



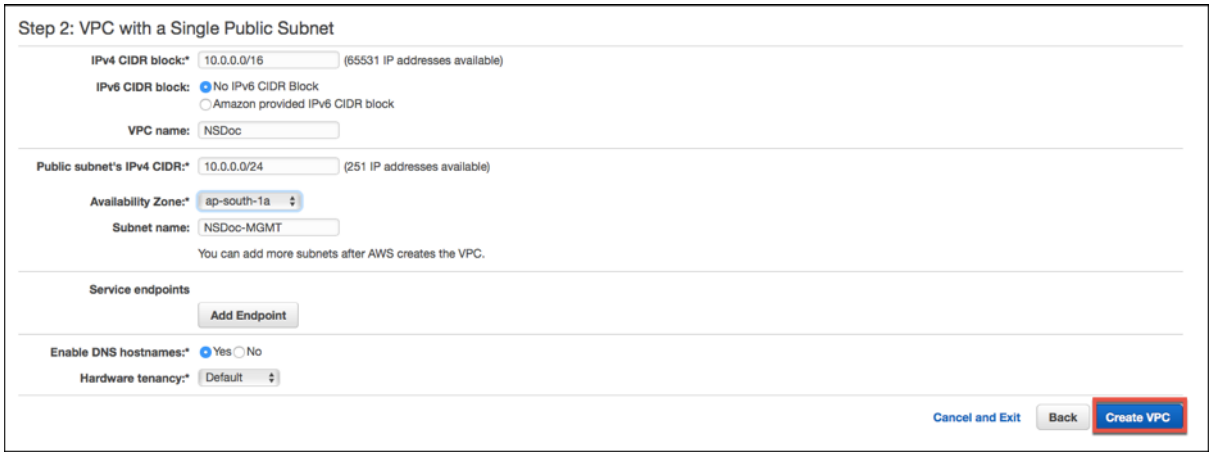
创建三个 NIC。可以为每个 NIC 配置一对 IP 地址（公用和专用）。NIC 用于以下用途。

NIC	用途	关联到
eth0	服务管理流量 (NSIP)	公用 IP 地址和专用 IP 地址
eth1	服务客户端流量 (VIP)	公用 IP 地址和专用 IP 地址

NIC	用途	关联到
eth2	与后端服务器通信 (SNIP)	公用 IP 地址（专用 IP 地址不是强制性的）

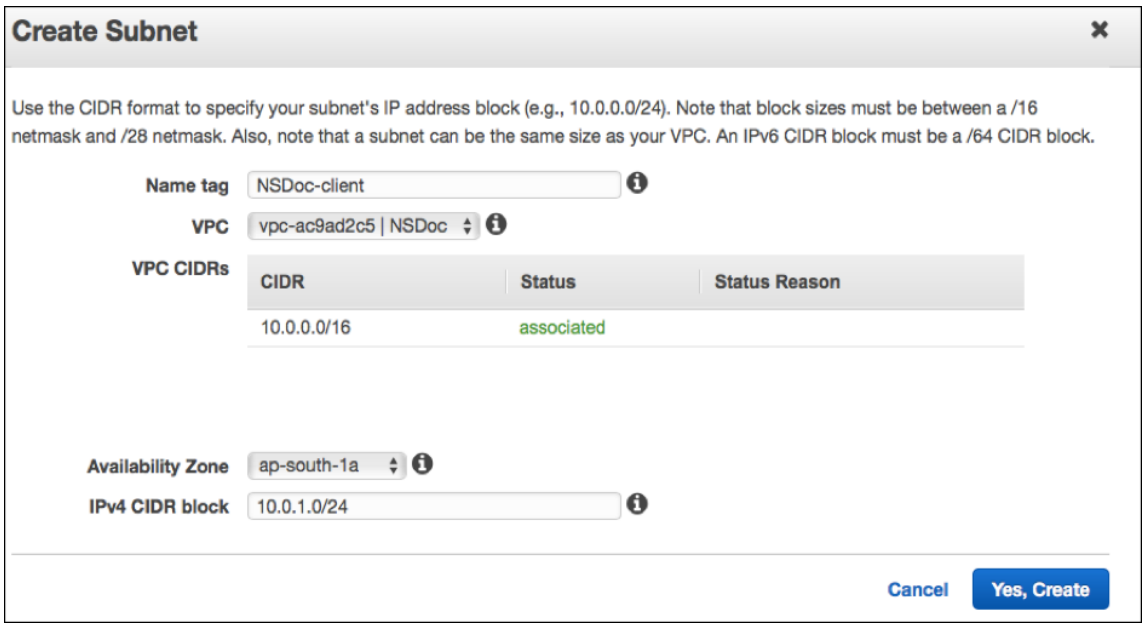
步骤 1：创建 VPC。

1. 登录 AWS Web 控制台，然后导航到 **Networking & Content Delivery**（网络连接和内容交付）> **VPC**。单击 **Start VPC Wizard**（启动 VPC 向导）。
2. 选择 **VPC with a Single Public Subnet**（具有单个公用子网的 VPC），然后单击 **Select**（选择）。
3. 在这种情况下，请将 IP CIDR 块设置为 10.0.0.0/16。
4. 为 VPC 提供一个名称。
5. 将公用子网设置为 10.0.0.0/24。（这是管理网络）。
6. 选择一个可用性区域。
7. 为该子网命名。
8. 点击创建 **VPC**。

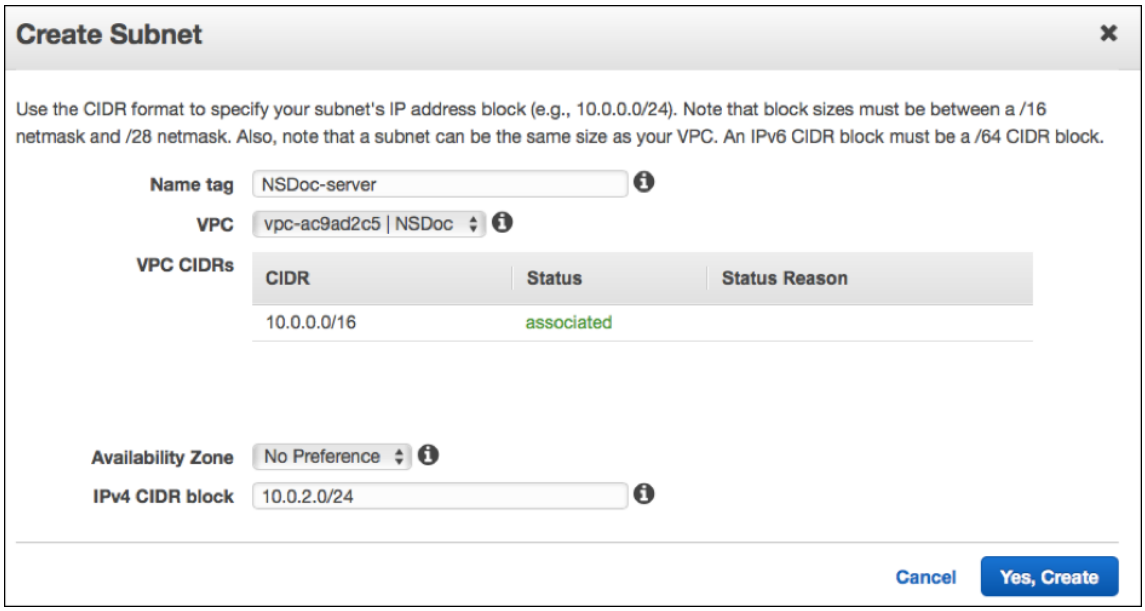


步骤 2：创建额外的子网。

1. 打开 Amazon VPC 控制台，网址为 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，在输入以下详细信息后，选择“Subnets”（子网）、“Create Subnet”（创建子网）。
   - Name tag（名称标记）：提供子网的名称。
   - VPC：选择要为其创建子网的 VPC。
   - Availability Zone（可用性区域）：选择在步骤 1 中创建 VPC 的可用性区域。
   - IPv4 CIDR block（IPv4 CIDR 块）：为您的子网指定 IPv4 CIDR 块。对于这种情况，请选择 10.0.1.0/24。

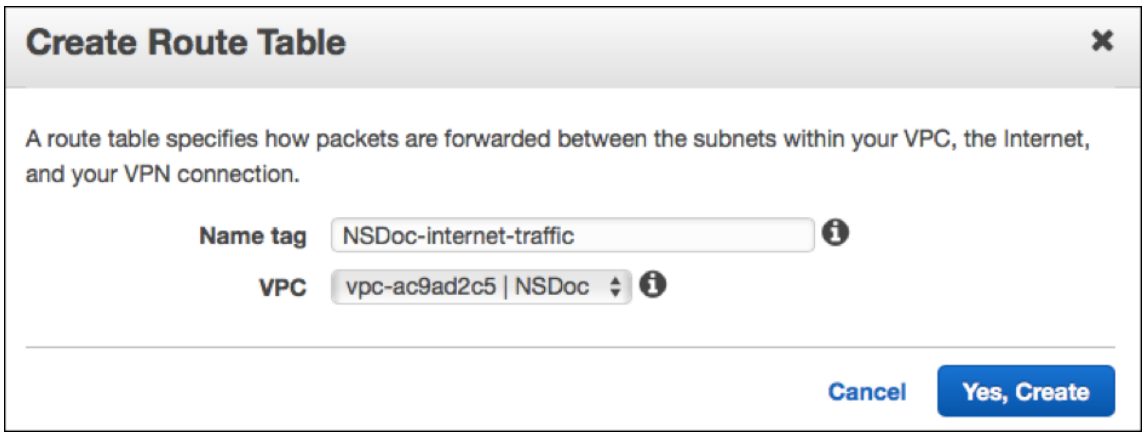


3. 重复这些步骤为后端服务器再创建一个子网。



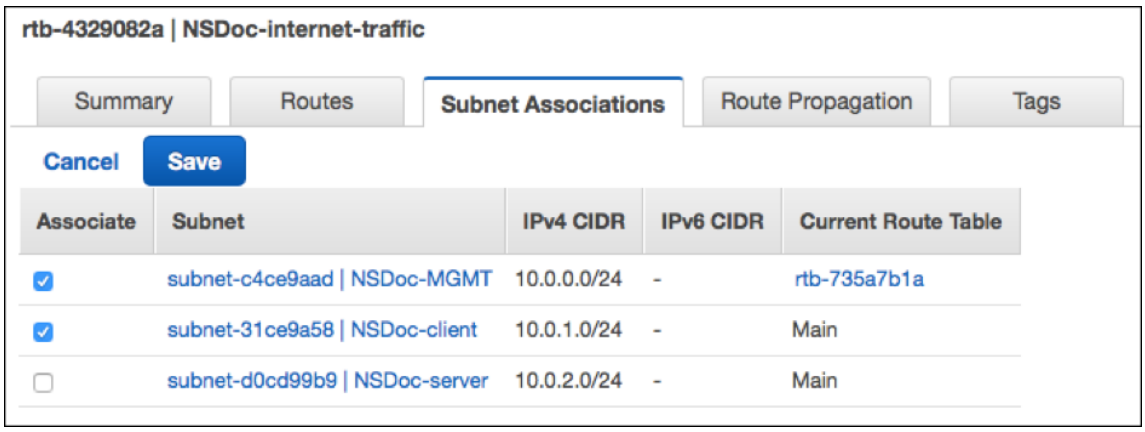
步骤 3：创建路由表。

1. 打开 Amazon VPC 控制台，网址为 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 **Route Tables**（路由表）> **Create Route Table**（创建路由表）。
3. 在“Create Route Table”（创建路由表）窗口中，添加名称并选择您在步骤 1 中创建的 VPC。
4. 单击 **Yes, Create**（是，创建）。

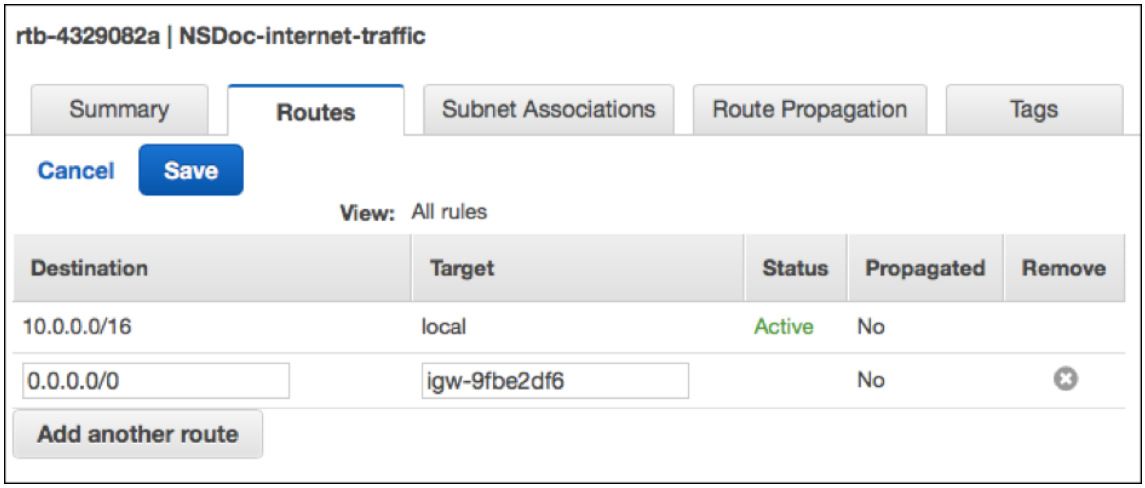


路由表将分配给您为此 VPC 创建的所有子网，以便从一个子网中的实例路由的流量可以到达另一个子网中的实例。

5. 单击 子网关联，然后单击 编辑。
6. 单击“management and client subnet ”（管理和客户端子网），然后单击“Save”（保存）。这将仅为 Internet 流量创建路由表。



7. 单击 **Routes**（路由）**> Edit**（编辑）**> Add another route**（添加另一个路由）。
8. 在“Destination”（目标）字段中添加 0.0.0.0/0，然后单击“Destination”（目标）字段以选择 VPC 向导自动创建的 igw-<xxxx> Internet 网关。
9. 单击保存。

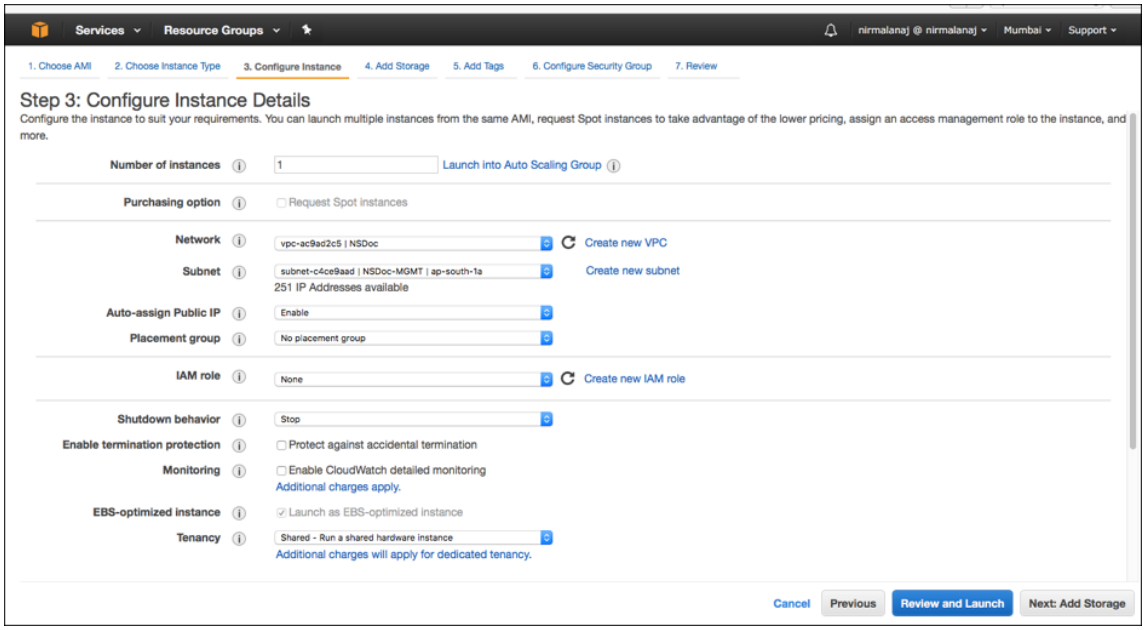


10. 请按照以下步骤为服务器端流量创建路由表。

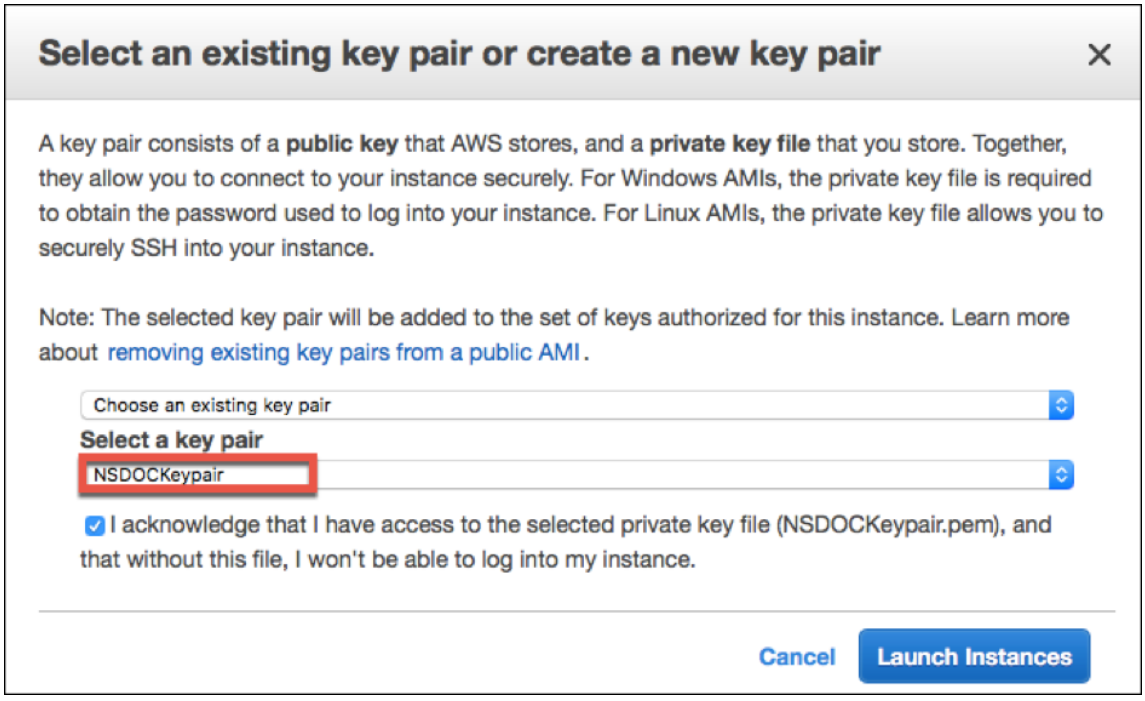
步骤 4：创建 NetScaler VPX 实例。

1. 登录 AWS 管理控制台，然后单击 **Compute**（计算）下的 **EC2**。
2. 单击“AWS Marketplace”。在搜索 AWS Marketplace 栏中，键入 NetScaler VPX 并按 Enter。将显示可用的 NetScaler VPX 版本。
3. 单击“选择”选择所需的 NetScaler VPX 版本。EC2 实例向导启动。
4. 在 **Choose Instance Type**（选择实例类型）页面中，选择 **m4. Xlarge**（推荐），然后单击 **Next: Configure Instance Details**（下一步：配置实例详细信息）。Xlarge（推荐）并点击 下一步：配置实例详细信息。
5. 在配置实例详细信息页面中，选择以下内容，然后单击 下一步：添加存储。

    - 实例数：1
    - Network（网络）：在步骤 1 中创建的 VPC
    - Subnet（子网）：管理子网
    - Auto-assign Public IP（自动分配公用 IP）：启用



6. 在添加存储页面中，选择默认选项，然后单击 下一步：添加标签。
7. 在添加标签页面，为实例添加名称，然后单击 下一步：配置安全组。
8. 在“Configure Security Group”（配置安全组）页面中，选择默认选项（由 AWS Marketplace 生成，基于 Citrix Systems 的推荐设置），然后单击 **Review and Launch**（检查并启动）**> Launch**（启动）。
9. 系统会提示您选择现有密钥对或创建新密钥对。从“Select a key pair”（选择密钥对）下拉列表中，选择您作为必备条件创建的密钥对（请参阅“必备条件”部分。）
10. 选中复选框以确认密钥对，然后单击 启动实例。



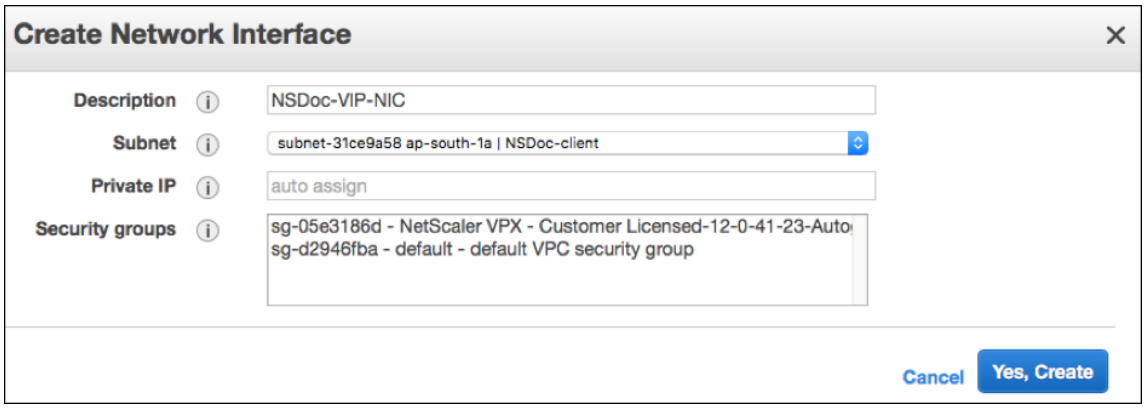
“Launch Instance”（启动实例）向导将显示“Launch Status”（启动状态），当实例完全启动时，该实例将显示在实例列表中。

检查实例，进入 AWS 控制台单击 **EC2 >** 正在运行的实例。选择实例并添加名称。确保“Instance State”（实例状态）为正在运行，“Status Checks”（状态检查）为已完成。

步骤 5：创建和连接更多网络接口。

创建 VPC 时，只有一个与其关联的网络接口。现在，向 VPC 添加另外两个网络接口，用于 VIP 和 SNIP。

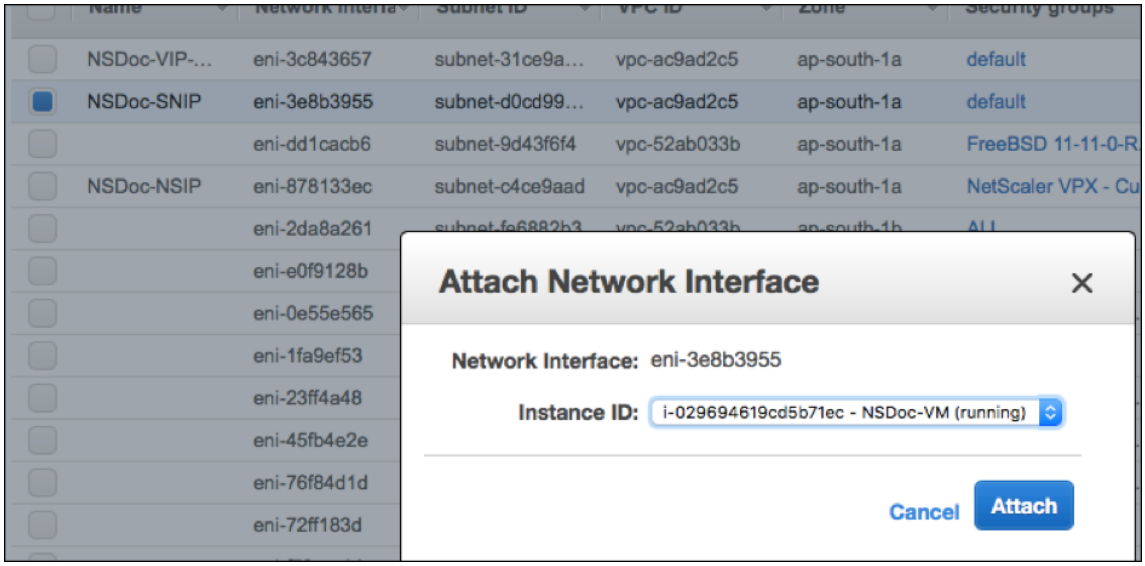
1. 打开 Amazon EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择“Create Network Interface”（创建网络接口）。
4. 对于 描述，输入一个描述性名称。
5. 对于 子网，选择您之前为 VIP 创建的子网。
6. 对于 私有 **IP**，保留默认选项。
7. 对于 安全组，选择该组。
8. 单击 **Yes, Create**（是，创建）。



9. 创建网络接口后，请为接口添加名称。
10. 重复这些步骤为服务器端流量创建网络接口。

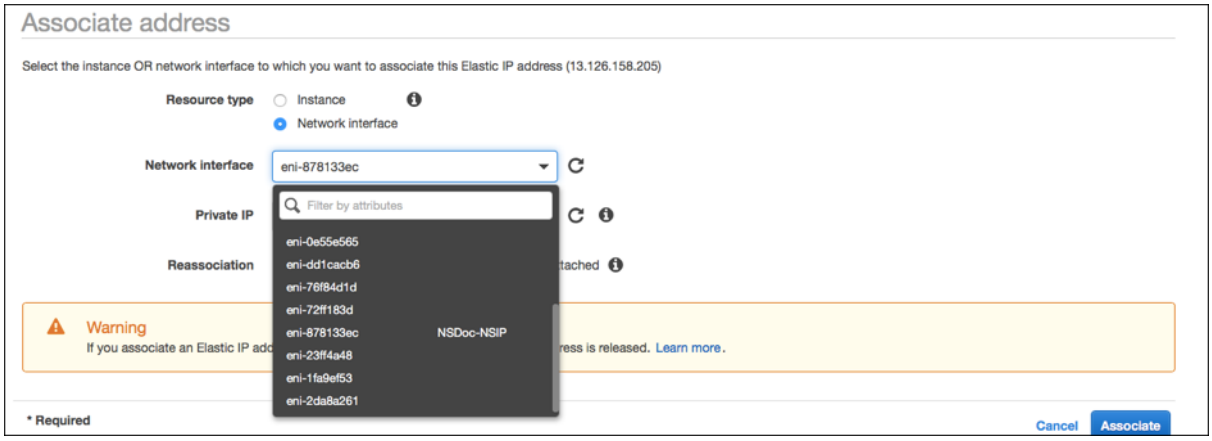
连接网络接口：

1. 在导航窗格中，选择 Network Interfaces（网络接口）。
2. 选择网络接口并单击 **Attach**。
3. 在附加网络接口对话框中，选择实例并单击 附加。



步骤 6：将弹性 IP 附加到 NSIP。

1. 在 AWS 管理控制台中，转到 **NETWORK & SECURITY**（网络与安全）**> Elastic IPs**（弹性 **IP**）。
2. 检查可附加的可用免费 EIP。如果没有，请单击 **Allocate new address**（分配新地址）。
3. 选择新分配的 IP 地址，然后选择 **Actions**（操作）**> Associate address**（关联地址）。
4. 单击 **Network interface**（网络接口）单选按钮。
5. 从“Network interface”（网络接口）下拉列表中，选择“management NIC”（管理 NIC）。
6. 从 **Private IP**（专用 IP）下拉菜单中，选择 AWS 生成的 IP 地址。
7. 选中 **Reassociation**（重新关联）复选框。
8. 单击 **Associate**（关联）。



访问 **VPX** 实例：

在配置了带有三个 NIC 的独立 NetScaler VPX 实例后，登录该 VPX 实例完成 NetScaler 端的配置。使用以下选项：

- GUI：在浏览器中键入管理 NIC 的公用 IP。使用 nsroot 作为用户名和实例 ID (i-0c1ffe1d987817522) 作为密码进行登录。

> 注意：
>
> 出于安全原因，首次登录时，系统会提示您更改密码。更改密码后，必须保存配置。如果未保存配置，但实例重新启动，则必须使用默认密码登录。请在出现提示时再次更改密码并保存配置。

- SSH：打开 SSH 客户端并键入：

```
ssh -i \\&#060;location of your private key\\&#062; ns root@\\&#060;
public DNS of the instance\\&#062;
```

要查找公用 DNS，请单击实例，然后单击 **Connect**（连接）。

相关信息：

- 要配置 Netscaler 拥有的 IP 地址（NSIP、VIP 和 SNIP），请参阅配置 NetScaler 拥有的 IP 地址。
- 您已经配置了 NetScaler VPX 设备的 BYOL 版本，有关更多信息，请参阅 VPX 许可指南，网址为 http://support.citrix.com/article/CTX122426

下载 **NetScaler VPX** 许可证

October 17, 2024

从 AWS 市场启动 NetScaler vpx 客户许可实例后，需要许可证。有关 VPX 许可的更多信息，请参阅 许可概述。

您必须：

1. 使用 Citrix Web 站点中的许可门户生成有效许可证。
2. 将许可证上载到实例。

如果这是付费商城实例，则无需安装许可证。正确的功能集和性能会自动激活。

如果您使用的 NetScaler VPX 实例的型号高于 VPX 5000，网络吞吐量可能与该实例的许可证指定的吞吐量不同。但是，其他功能（例如，每秒钟的 SSL 吞吐量和 SSL 事务量）可能会有所改进。

在 c4.8xlarge 实例类型中观察到 5 Gbps 的网络带宽。

如何将 **AWS** 订阅迁移到 **BYOL**

本节介绍从 AWS 订阅迁移到自带许可证 (BYOL) 的过程，相反。

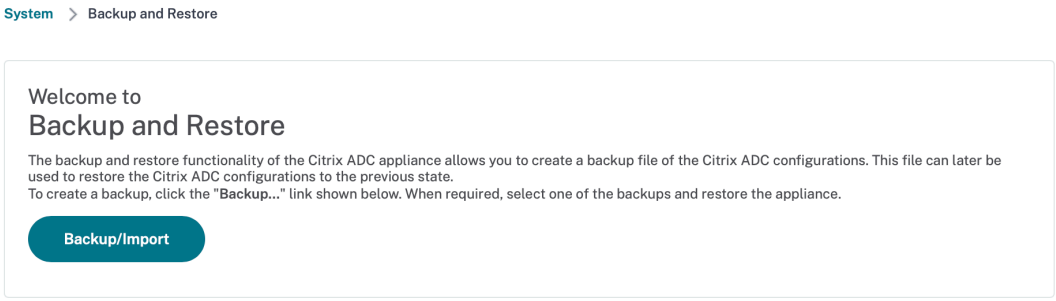
执行以下步骤将 AWS 订阅迁移到 BYOL：

> 注意：
>
> 步骤 **2** 和步骤 **3** 在 NetScaler VPX 实例上完成，所有其他步骤都在 AWS 门户网站上完成。

1. 使用 NetScaler VPX 创建 BYOL EC2 实例-与具有相同安全组、IAM 角色和子网的旧 EC2 实例在同一可用区中许可的客户许 可。新的 EC2 实例必须只有一个 ENI 接口。
2. 要使用 NetScaler GUI 备份旧 EC2 实例上的数据，请执行以下步骤。

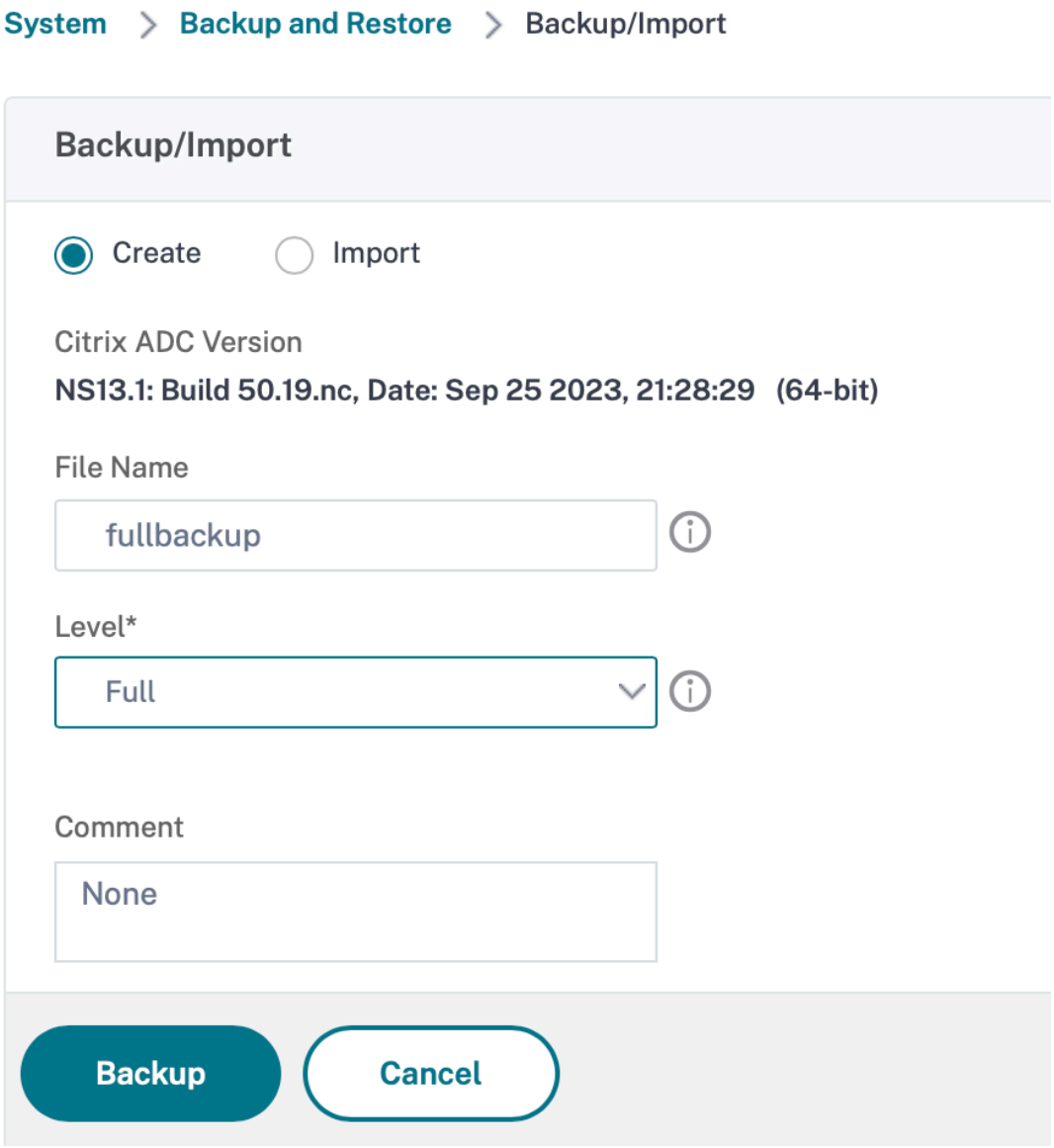
   a) 导航到“系统”**>**“备份和恢复”。

   b) 在 欢迎 页面中，单击 备份/导入 以启动该过程。

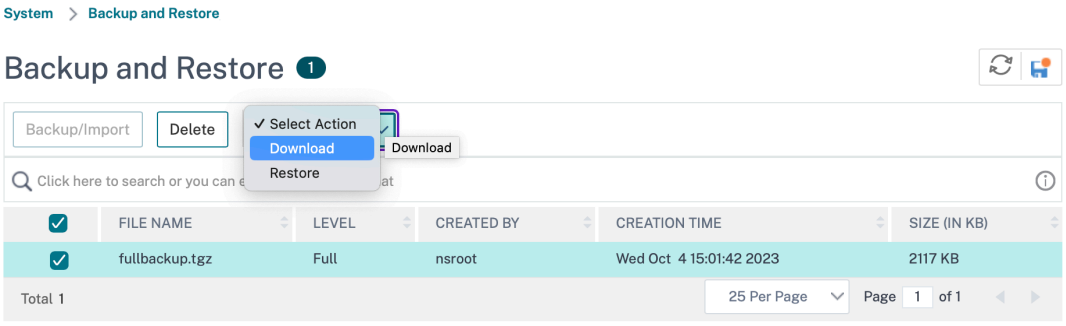


   c) 在“备份/导入”页面中，填写以下详细信息：

   - 名称—备份文件的名称。
   - 级别—选择备份级别为“完全”。
   - 评论—提供备份的简要说明。



d) 单击备份。备份完成后，您可以选择该文件并将其下载到本地计算机。

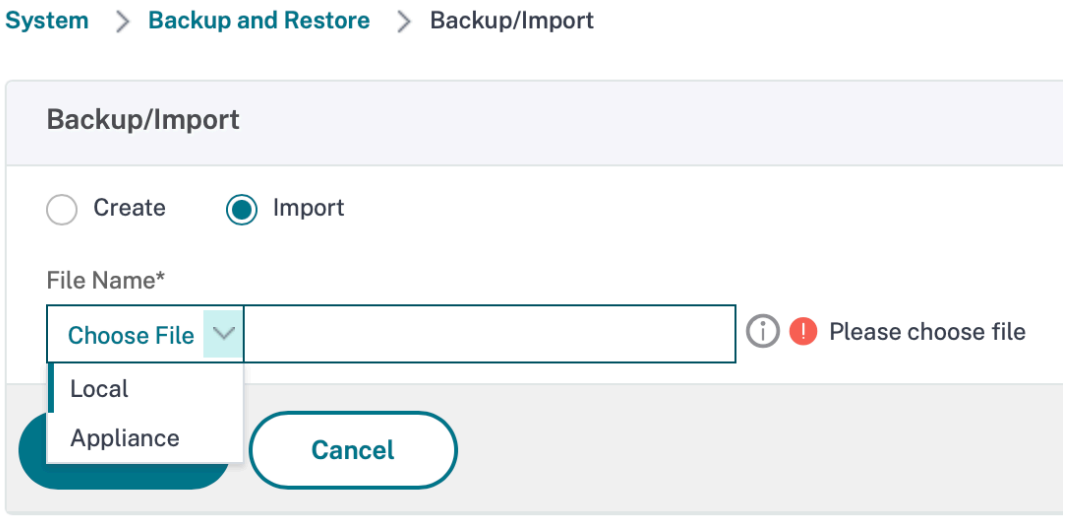


3. 要使用 NetScaler GUI 恢复新 EC2 实例上的数据，请执行以下步骤：

a) 导航到“系统”**>**“备份和恢复”。

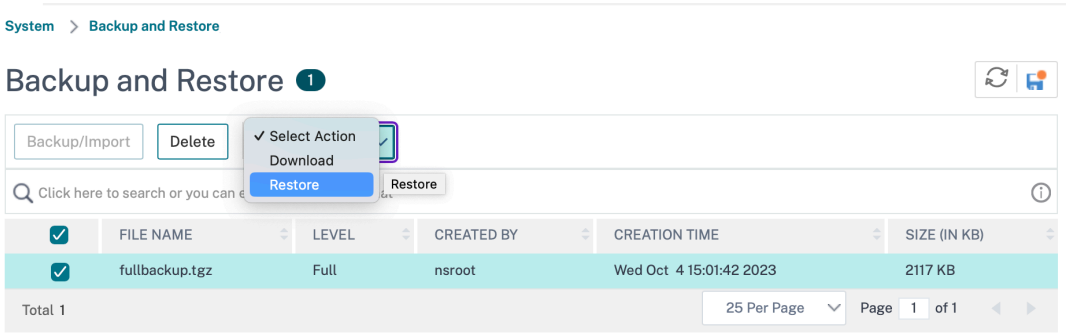
b) 单击备份/导入以启动该过程。

c) 选择 导入 选项并上载备份文件。

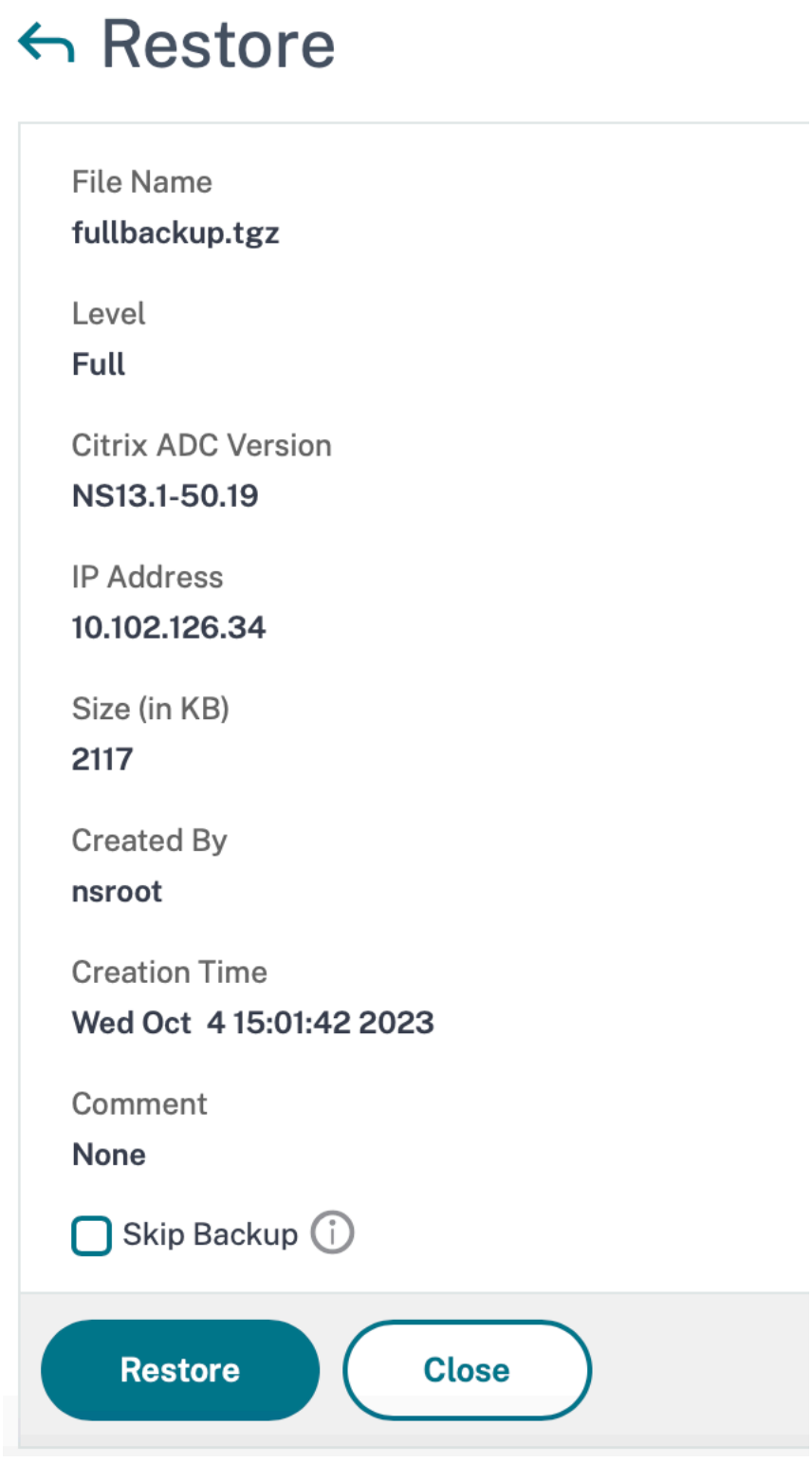


d) 选择该文件。

e) 从“选择操作”下拉菜单中，选择“还原”。



f) 在 还原 页面上，验证文件详细信息，然后单击 还原。



g) 恢复后，重新启动 EC2 实例。

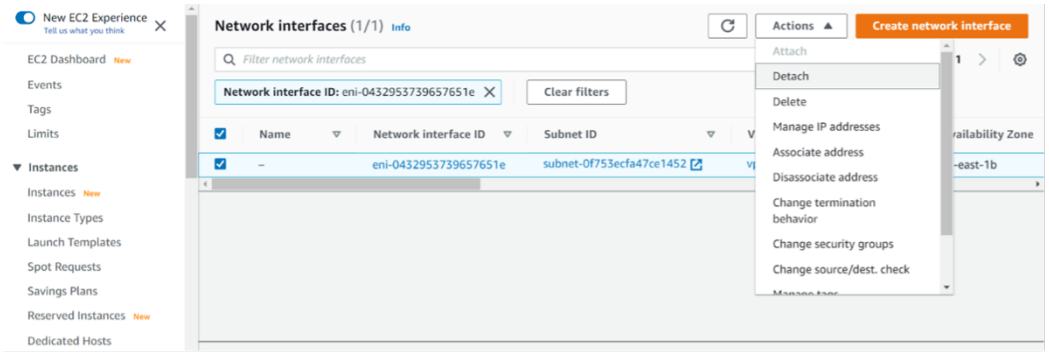
4. 将所有接口（NSIP 地址绑定到的管理接口除外）从旧 EC2 实例移动到新的 EC2 实例。要将网络接口从一个

EC2 实例移动到另一个 EC2 实例，请执行以下步骤：

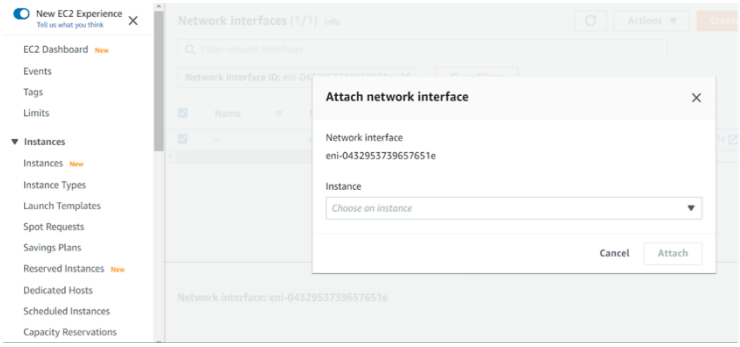
a) 在 **AWS** 门户中，停止旧的和新的 EC2 实例。

b) 导航到 网络接口，然后选择连接到旧 EC2 实例的网络接口。

c) 单击 操作 **>** 分离以分离 EC2 实例。



d) 单击 操作 **>** 附加，将网络接口附加到新的 EC2 实例。输入网络接口必须连接到的 EC2 实例名称。



e) 对连接的所有其他接口执行 步骤 1 至步骤 **4** 。确保遵循顺序并保持接口顺序。也就是说，首先分离接口 2 并连接它，然后分离接口 3 并连接它，依此类推。

5. 您无法从旧的 EC2 实例中分离管理接口。因此，将旧 EC2 实例的管理接口（主网络接口）上的所有辅助 IP 地址（如果有）移动到新的 EC2 实例。要将 IP 地址从一个接口移动到另一个接口，请执行以下步骤：

a) 在 **AWS** 门户中，确保旧的和新的 EC2 实例都处于 停止 状态。

b) 导航到 网络接口，然后选择连接到旧 EC2 实例的管理网络接口。

c) 单击 操作 **>** 管理 **IP** 地址，然后记下分配的所有辅助 IP 地址（如果有）。

d) 导航到新 EC2 实例的管理网络接口或主接口。

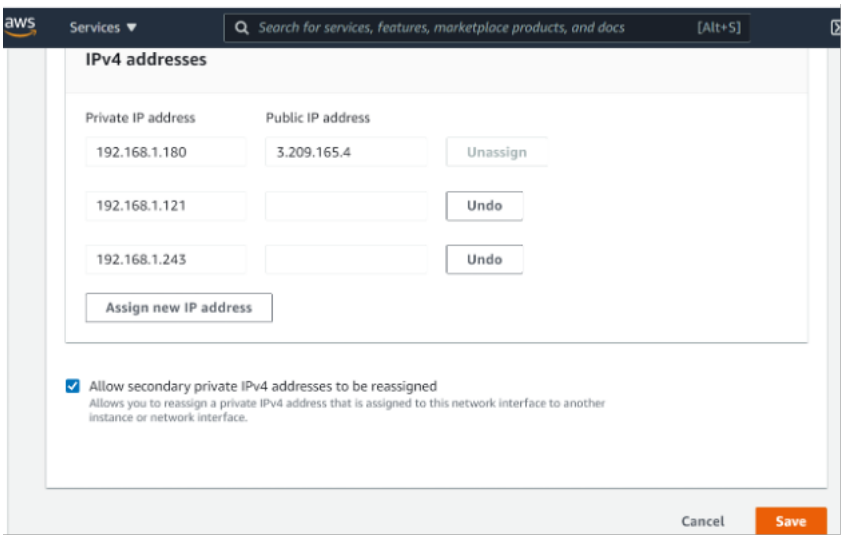
e) 单击 操作 **>** 管理 **IP** 地址。

f) 在 **IPv4** 地址下，单击 分配新的 **IP** 地址。

g) 输入 步骤 **3** 中注明的 IP 地址。

h) 选 中允许重新分配辅助专用 **IP** 地址 复选框。

i) 单击保存。



6. 启动新的 EC2 实例并验证配置。移动所有配置后，您可以根据要求删除或保留旧的 EC2 实例。
7. 如果任何 EIP 地址附加到旧 EC2 实例的 NSIP 地址，请将旧实例 NSIP 地址移动到新的实例 NSIP 地址。
8. 如果您想恢复到旧实例，请在旧实例和新实例之间以相反的方式执行相同的步骤。
9. 从订阅实例迁移到 BYOL 实例后，需要许可证。要安装许可证，请执行以下步骤：
    - 使用 Citrix 网站中的许可门户生成有效的许可证。
    - 将许可证上载到实例。

> 注意：
>
> 当您将 BYOL 实例移动到订阅实例（付费市场实例）时，您无需安装许可证。正确的功能集和性能将自动激活。

限制

无法将管理界面移动到新的 EC2 实例。因此，Citrix 建议您手动配置管理界面。有关详细信息，请参阅上述过程中的 步骤 **5** 。使用旧 EC2 实例的确切副本创建一个新的 EC2 实例，但只有 NSIP 地址有一个新的 IP 地址。

对不同可用性区域中的服务器实现负载平衡

October 17, 2024

使用 VPX 实例可以对在相同可用性区域中运行的服务器或在以下区域运行的服务器实现负载平衡：

- 同一 AWS VPC 中的不同可用性区域 (AZ)
- 不同 AWS 区域

- VPC 中的 AWS EC2

要启用 VPX 实例来平衡在 AWS VPC 之外运行的服务器的负载，VPX 实例处于启用状态，配置实例使用 EIP 通过 Internet 网关路由流量，如下所示：

1. 使用 NetScaler CLI 或 GUI 在 NetScaler VPX 实例上配置 SNIP。
2. 为服务器端流量创建面向公众的子网，在 AZ 外部路由流量。
3. 使用 AWS GUI 控制台将 Internet 网关路由添加到路由表中。
4. 将更新的路由表与服务器端子网相关联。
5. 将 EIP 与映射到 NetScaler SNIP 地址的服务器端专用 IP 地址相关联。

在同一 **AWS** 可用性区域中部署 **VPX** 高可用性对

October 17, 2024

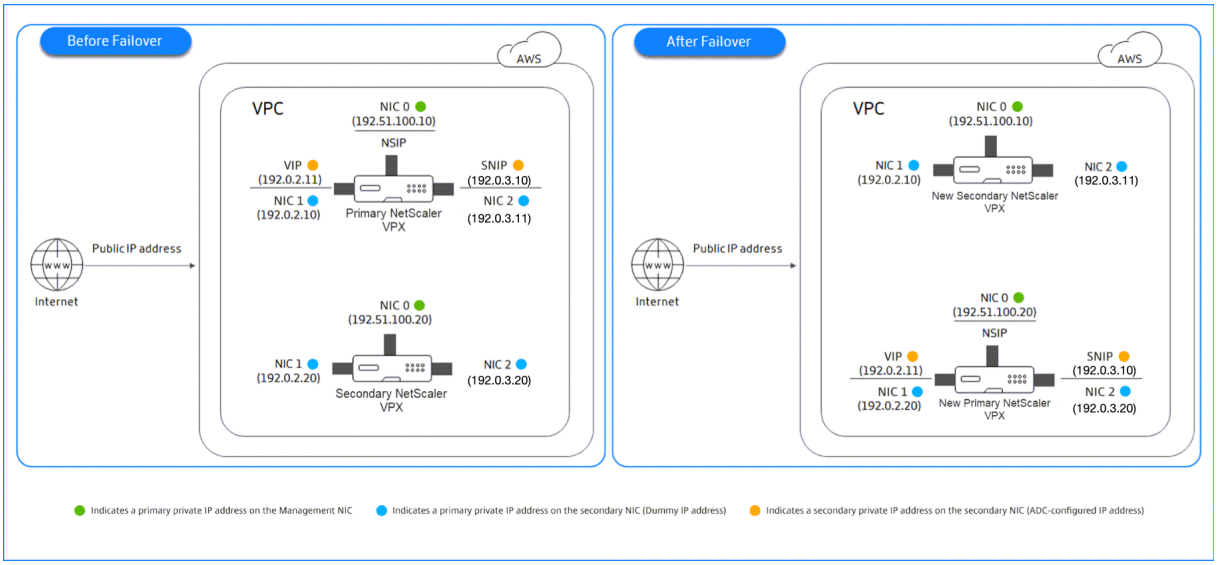
> 注意：
>
> 从 NetScaler 版本 13.1 build 27.x 起，同一 AWS 可用区中的 VPX HA 对支持 IPv6 地址。

您可以将 AWS 上的两个 NetScaler VPX 实例配置为高可用性对，位于同一 AWS 区域中，两个 VPX 实例位于同一子网中。高可用性通过在故障转移后将连接到主高可用性节点的 NIC（客户端和服务器端 NIC）的辅助专用 IP 地址迁移到辅助高可用性节点来实现。还会迁移与二级专用 IP 地址关联的所有弹性 IP 地址。

NetScaler VPX HA 对支持同一 AWS 可用区中的 IPv4 和 IPv6 地址。

下图描述了通过迁移辅助专用 IP 地址而出现的 HA 故障转移方案。

图 1. 内联部署 图 1. AWS 上的 NetScaler VPX HA 对，使用私有 IP 迁移



在开始阅读您的文档之前，请阅读以下文档：

- 必备条件
- 局限性与用法指南
- 在 AWS 上部署 NetScaler VPX 实例
- 高可用性

如何在同一区域中部署 **VPX** 高可用性对

下面是在同一区域中部署 VPX 高可用性对的步骤摘要：

1. 在 AWS 上创建两个 VPX 实例，每个实例都有三个 NIC。
2. 将 AWS 二级私有 IP 地址分配给主节点的 VIP 和 SNIP。
3. 使用 AWS 二级私有 IP 地址在主节点上配置 VIP 和 SNIP。
4. 在两个节点上配置 HA。

步骤 **1.** 步骤 **1.** 使用同一个 **VPC** 创建两个 **VPX** 实例（主节点和辅助节点），每个实例都有三个 **NIC**（以太网 **0**、以太网 **1**、以太网 **2**）

使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例中给出的步骤进行操作。

步骤 **2.** 步骤 **2.** 在主节点上，为以太网 **1**（客户端 **IP** 或 **VIP**）和以太网 **2**（后端服务器 **IP** 或 **SNIP**）分配专用 **IP** 地址

AWS 控制台会自动将主专用 IP 地址分配给配置的 NIC。为 VIP 和 SNIP 分配更多专用 IP 地址，称为二级专用 IP 地址。

要为网络接口分配专用 IP 地址，请执行以下步骤：

1. 打开 Amazon EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 网络接口，然后选择连接到实例的网络接口。
3. 选择 操作 **>** 管理 **IP** 地址。
4. 根据您的要求选择 **IPv4** 地址或 **IPv6** 地址。
5. 对于 IPv4 地址:

   a）选择分配新 **IP**。
   b）输入实例子网范围内的特定 IPv4 地址，或者将该字段留空以让 Amazon 为您选择 IP 地址。
   c）（可选）如果辅助专用 IP 地址已分配给另一个网络接口，则选择允许重新分配以允许重新分配该地址。

6. 对于 IPv6 地址:

   a）选择分配新 **IP**。
   b）输入实例子网范围内的特定 IPv6 地址，或将该字段留空以让 Amazon 为您选择 IP 地址。
   c）（可选）如果主专用 IP 地址或辅助专用 IP 地址已分配给另一个网络接口，则选择允许重新分配该地址。

7. 选择“是” **>** “更新”。

在 实例描述下，将显示分配的专用 IP 地址。

> 注意：
>
> 在 IPv4 HA 对部署中，只能在接口上分配辅助 IPv4 地址，并将其用作 VIP 和 SNIP 地址。但是在 IPv6 HA 对部署中，您可以在接口上分配主 IPv6 或辅助 IPv6 地址，并将其用作 VIP 和 SNIP 地址。

步骤 **3.** 步骤 **3.** 使用二级专用 **IP** 地址在主节点上配置 **VIP** 和 **SNIP**

使用 SSH 访问主节点。打开 ssh 客户端并键入：

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

接下来，配置 VIP 和 SNIP。

对于 VIP，请键入：

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

对于 SNIP，请键入：

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

键入 `save config` 以进行保存。

要查看配置的 IP 地址，请键入以下命令：

```
show ns ip
```

有关详细信息，请参阅以下主题：

- 配置和管理虚拟 IP (VIP) 地址
- 配置 NSIP 地址

步骤 **4**：在两个实例上配置高可用性

在主节点上，打开 Shell 客户端并键入以下命令：

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

在辅助节点上，键入以下命令：

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

键入 `save config` 以保存配置。

要查看已配置的高可用性节点，请键入 `show ha node`。

故障转移时，先前主节点上配置为 VIP 和 SNIP 的二级专用 IP 地址将迁移到新的主节点。

要在节点上强制故障转移，请键入 `force HA`failover。

根据二级私有 **IP** 迁移将传统 **HA** 对迁移到新的 **HA** 对

> 注意：
>
> 不推荐使用基于 ENI 迁移的 VPX HA 对的传统部署方法。因此，我们建议您使用基于二级私有 IP 迁移的 HA 对部署。

要基于二级私有 IP 迁移实现从传统 HA 对无缝迁移到新的 HA 对，请确保满足以下条件：

1. 主节点和辅助节点必须具有相同数量的接口，并且这些接口必须位于相同的子网中。
2. 在新方法中，必须将传统方法中配置为主要私有 IP 地址的 VIP 和 SNIP 迁移到辅助私有 IP 地址。
3. 新 HA 部署所需的 IAM 权限必须添加到主要和辅助 NetScaler 实例中。
4. 重启主 NetScaler 实例和辅助 NetScaler 实例。

有关更多信息，请参阅相同区域内的高可用性。

使用 **Citrix CloudFormation** 模板部署高可用性对

在启动 CloudFormation 模板之前，请确保您完成以下要求：

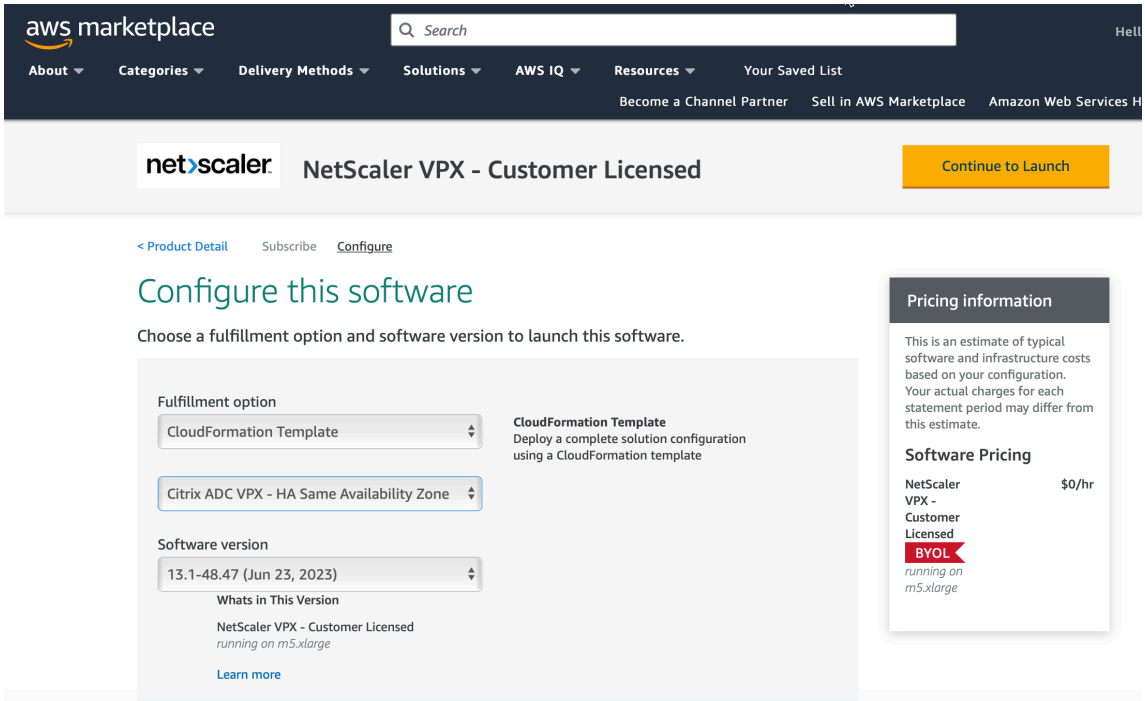
- 一个 VPC
- VPC 内的三个子网
- 打开了 UDP 3003、TCP 3009—3010、HTTP、SSH 端口的安全组
- 一对钥匙
- 创建 Internet 网关
- 编辑客户端和管理网络的路由表以指向 Internet 网关

> 注意：
>
> Citrix CloudFormation 模板会自动创建 IAM 角色。现有 IAM 角色不会显示在模板中。

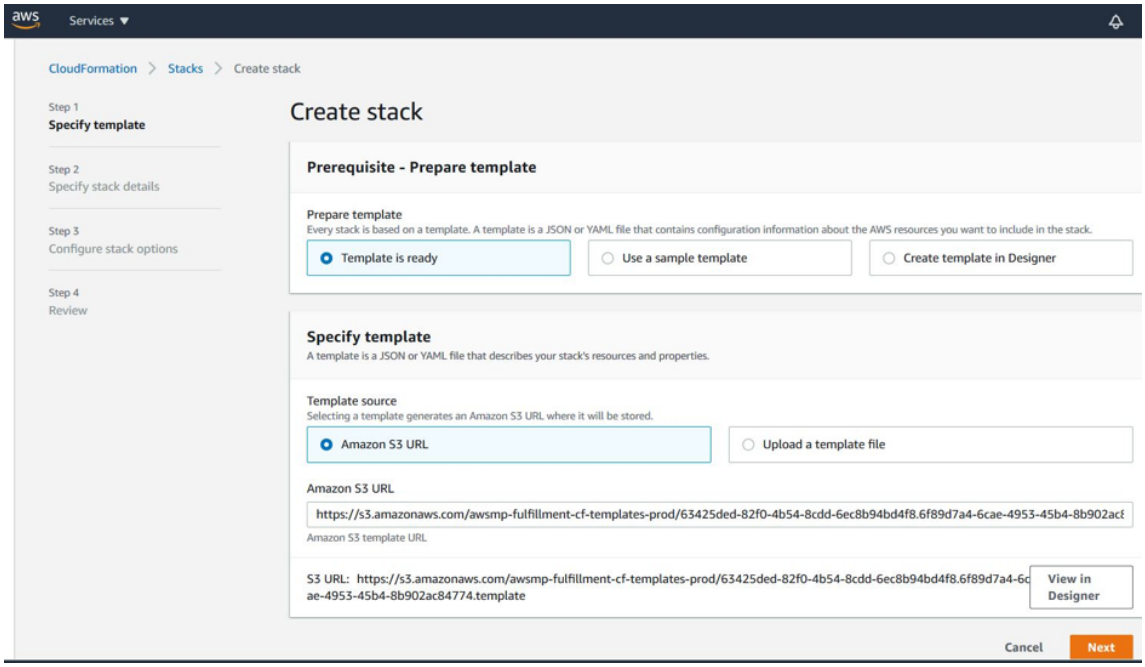
要启动 **Citrix CloudFormation** 模板，请执行以下操作：

1. 使用 AWS 凭据登录 AWS 市场 。
2. 在搜索字段中，键入 **NetScaler VPX** 搜索 NetScaler AMI，然后单击 **Go**（前往）。
3. 在搜索结果页面上，单击所需的 NetScaler VPX 产品。
4. 单击 **Pricing**（定价）选项卡，转至 **Pricing Information**（定价信息）。

5. 选择区域和 配送选项 为 **NetScaler VPX** —客户许可。
6. 单击 **Continue to Subscribe**（继续订阅）。
7. 检查 **Subscribe**（订阅）页面中的详细信息，然后单击 **Continue to Configuration**（继续配置）。
8. 选择 **CloudFormation Template**（CloudFormation 模板）作为 **Delivery Method**（交付方法）。
9. 选择所需的 CloudFormation 模板。
10. 选择 **Software Version**（软件版本）和 **Region**（区域），然后单击 **Continue to Launch**（继续启动）。



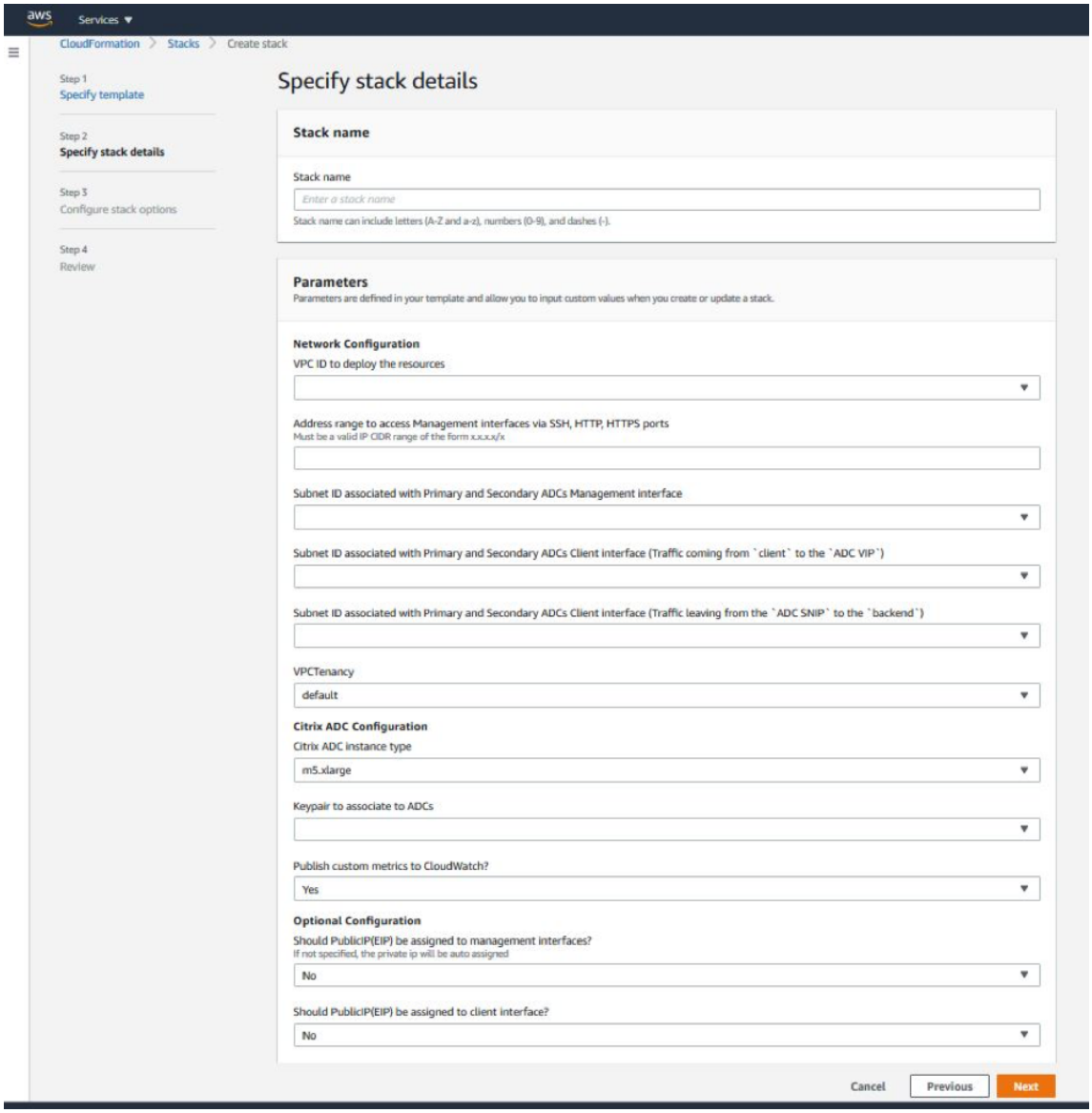
11. 在 **Choose Action**（选择操作）下，选择 **Launch CloudFormation**（启动 CloudFormation），然后单击 **Launch**（启动）。将出现“创建堆栈”页面。
12. 单击下一步。



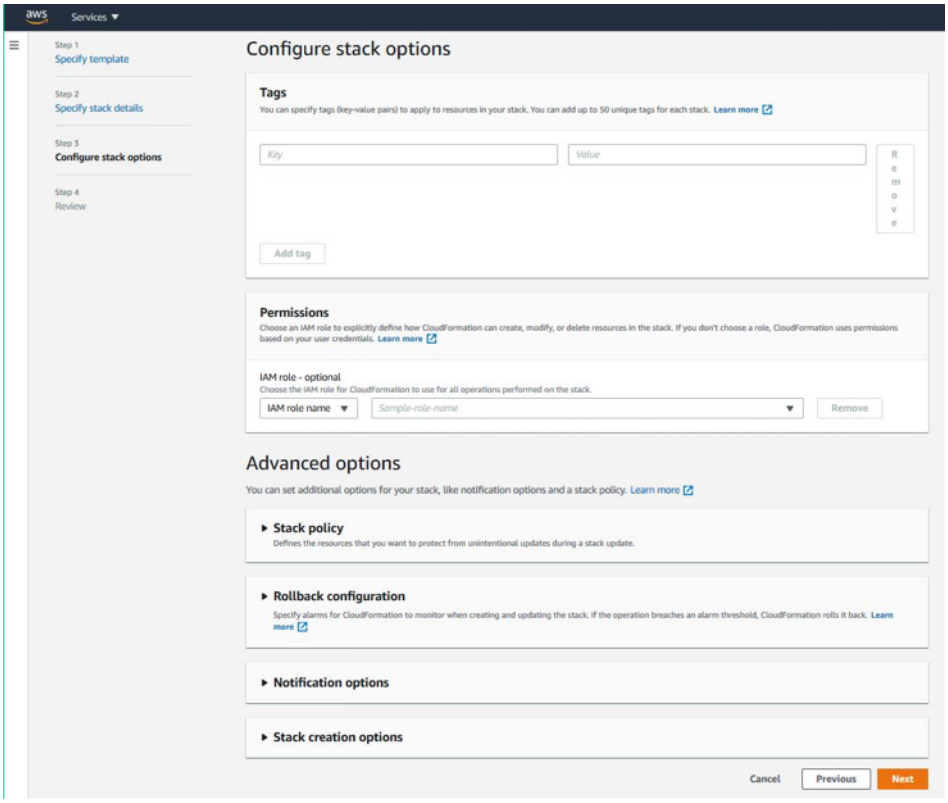
13. 此时将显示 **Specify stack details**（指定堆栈详细信息）。输入以下详细信息。

    - 键入堆 栈名称。名称必须在 25 个字符以内。
    - 在 **Network Configuration**（网络配置）下，执行以下操作：
        - 选择 **Management Subnetwork**（管理子网）、**Client Subnetwork**（客户端子网）和 **Server Subnetwork**（服务器子网）。确保选择在 VPC ID 下选择的 VPC 中创建的正确子网。
        - 添加 **Primary Management IP**（主管理 IP）、**Secondary Management IP**（辅助管理 IP）、**Client IP**（客户端 IP）和 **Server IP**（服务器 IP）。IP 地址必须属于相应子网的同一子网。或者，您可以让模板自动分配 IP 地址。
        - 对于 **VPCTenancy**，请选择 **default**（默认）。
    - 在 **NetScaler** 配置下，执行以下操作：
        - 对于 **Instance type**（实例类型），请选择 **m5.xlarge**。
        - 从 **Key Pair**（密钥对）的菜单中选择已创建的密钥对。
        - 默认情况下，将自定义指标发布到 **CloudWatch**? 选项设置为 是。如果要禁用此选项，请选择 **No**（否）。

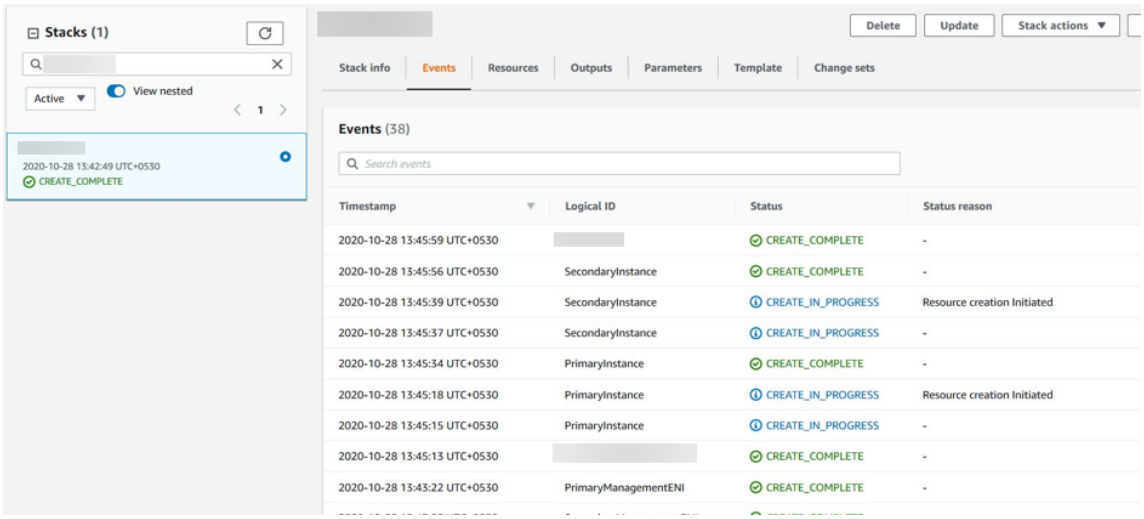
          有关 CloudWatch 指标的更多信息，请参阅 [使用 Amazon CloudWatch 监控您的实例](#monitor-your-instances-using-amazon-cloudWatch)。
    - 在“可选配置”下，执行以下操作：
        - 默认情况下，是否应将公共 **IP (EIP)** 分配给管理接口？选项设置为 否。
        - 默认情况下，是否应将公共 **IP (EIP)** 分配给客户端接口？选项设置为 否。



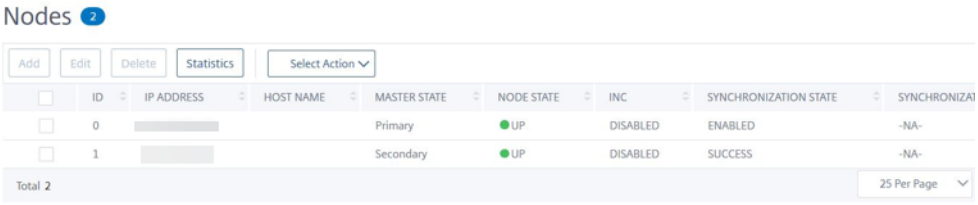
14. 单击下一步。
15. 此时将显示 **Configure stack options**（配置堆栈选项）页面。这是可选页面。



16. 单击下一步。
17. 此时将显示 **Options**（选项）页面。（这是可选页面。）。单击下一步。
18. 此时将显示 **Review**（检查）页面。请花点时间检查设置并根据需要做出任何更改。
19. 选择 我承认 **AWS CloudFormation** 可能会创建 **IAM** 资源。复选框，然后单击 创建堆栈。
20. 此时将显示 **CREATE-IN-PROGRESS**（正在创建中）状态。等到状态为 **CREATE-COMPLETE**（创建完成）。如果状态未更改为 **COMPLETE**（完成），请检查 **Events**（事件）选项卡以了解失败的原因，然后使用正确的配置重新创建实例。



21. 创建 IAM 资源后，导航到 **EC2 Management Console**（管理控制台）**> Instances**（实例）。您会找到两个使用 IAM 角色创建的 VPX 实例。创建主节点和辅助节点各有三个专用 IP 地址和三个网络接口。
22. 使用用户名 `nsroot` 和实例 ID 作为密码登录主节点。在 GUI 中，导航到 **System**（系统）**> High Availability**（高可用性）**> Nodes**（节点）。CloudFormation 模板已经在 HA 对中配置了 NetScaler VPX。
23. NetScaler VPX HA 对出现了。



使用 **Amazon CloudWatch** 监视您的实例

您可以使用亚马逊 CloudWatch 服务来监视一组 NetScaler VPX 指标，例如 CPU 和内存利用率以及吞吐量。CloudWatch 实时监视在 AWS 上运行的资源和应用程序。可以使用 AWS 管理控制台访问 Amazon CloudWatch 控制面板。有关更多信息，请参阅 Amazon CloudWatch。

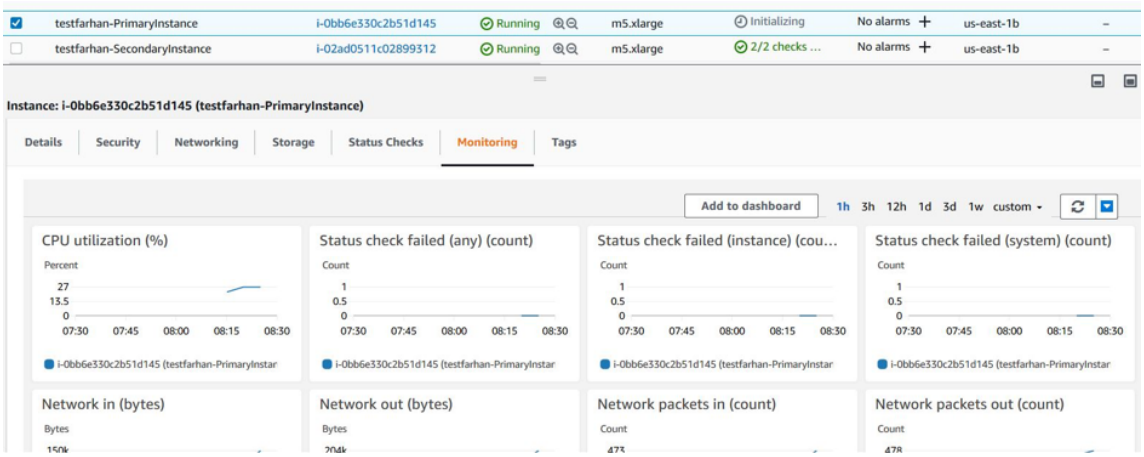
注意事项

- 如果您使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例，则默认情况下，CloudWatch 服务处于启用状态。
- 如果您使用 Citrix CloudFormation 模板部署 NetScaler VPX 实例，则默认选项为“是”。如果要禁用 CloudWatch 服务，请选择“否”。
- 可用于 CPU（管理和数据包 CPU 使用率）、内存和吞吐量（入站和出站）的指标。

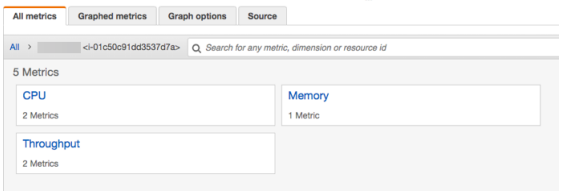
如何查看 **CloudWatch** 指标

要查看实例的 CloudWatch 指标，请执行以下步骤：

1. 登录 **AWS Management console**（**AWS** 管理控制台）**> EC2 > Instances**（实例）。
2. 选择实例。
3. 单击 **Monitoring**（监视）。
4. 单击 **View all CloudWatch metrics**（查看所有 CloudWatch 指标）。

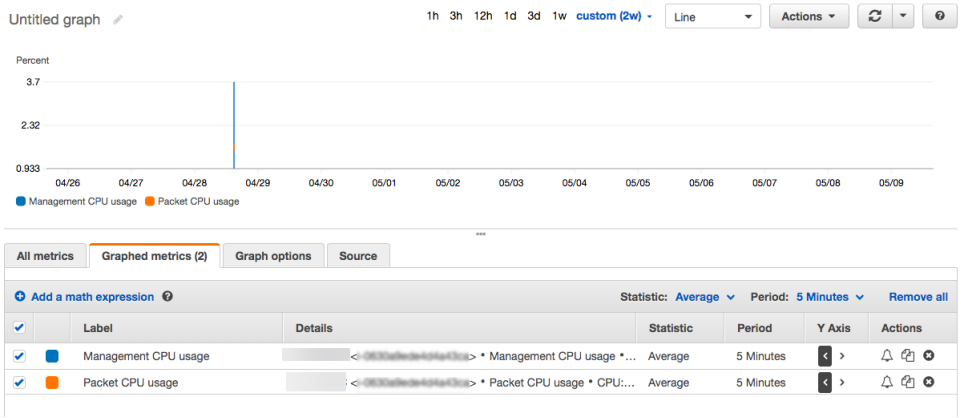


5. 在所有指标下，单击您的实例 ID。



6. 单击要查看的指标，设置持续时间（按分钟、小时、天、周、月）。
7. 单击 **Graphed metrics**（图表指标）以查看使用情况的统计信息。使用 **Graph options**（图表选项）自定义您的图表。

图. 图. CPU 使用率的图表指标



在高可用性设置中配置 **SR-IOV**

从 NetScaler 版本 12.0 57.19 起，即可在高可用性设置中支持 SR-IOV 接口。有关如何配置 SR-IOV 的更多信息，请参阅 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口。

相关资源

AWS 上的高可用性的工作原理

跨不同 **AWS** 可用区的高可用性

October 17, 2024

可以在两个不同的子网或两个不同的 AWS 可用性区域上将两个 NetScaler VPX 实例配置为独立网络配置 (INC) 模式下的高可用性主动-被动对。如果因任何原因主节点无法接受连接，将由辅助节点接替其职责。

有关高可用性的更多信息，请参阅 高可用性。有关 INC 的更多信息，请参阅 在不同子网中配置高可用性节点。

注意事项

- 在开始部署之前，请阅读以下文档：
  - AWS 术语
  - 必备条件
  - 局限性与用法指南
- VPX 高可用性对可以位于不同子网的同一可用性区域中，也可以位于两个不同的 AWS 可用性区域中。
- Citrix 建议您对管理 (NSIP)、客户端流量 (VIP) 和后端服务器 (SNIP) 使用不同的子网。
- 必须在独立网络配置 (INC) 模式下设置高可用性，故障转移才能正常运行。
- 这两个实例必须打开端口 3003 以传输 UDP 流量，因为该端口用于检测信号。
- 这两个节点的管理子网必须能够通过内部 NAT 访问 Internet 或 AWS API 服务器，以便其余的 API 能够正常运行。
- IAM 角色必须具有 E2 权限才能进行公用 IP 或弹性 IP (EIP) 迁移，必须具有 EC2 路由表权限才能进行专用 IP 迁移。

可以通过以下方式跨 AWS 可用性区域部署高可用性：

- 使用弹性 IP 地址
- 使用专用 IP 地址

其他参考资料

有关适用于 AWS 的 NetScaler 应用程序交付管理 (ADM) 的更多信息，请参阅 在 AWS 上安装 NetScaler ADM 代理。

跨不同 **AWS** 区域部署具有弹性 **IP** 地址的 **VPX** 高可用性对

October 17, 2024

您可以在 INC 模式下使用弹性 IP (EIP) 地址在两个不同的子网或两个不同的 AWS 可用区上配置两个 NetScaler VPX 实例。

有关高可用性的更多信息，请参阅 高可用性。有关 INC 的更多信息，请参阅 在不同子网中配置高可用性节点。

具有不同 **AWS** 区域的 **EIP** 地址的 **HA** 的工作原理

故障转移时，主实例的 VIP 的 EIP 将迁移到辅助实例，后者作为新的主实例接管。在故障转移过程中，AWS API：

1. 检查连接了 `IPSets` 的虚拟服务器。
2. 从虚拟服务器正在侦听的两个 IP 地址中查找具有关联公用 IP 的 IP 地址。一个直接连接到虚拟服务器，另一个是通过 IP 集连接的。
3. 将公用 IP (EIP) 重新关联到属于新的主 VIP 的专用 IP。

> 注意：
>
> 为了保护您的网络免受拒绝服务 (DoS) 等攻击，在使用 EIP 时，可以在 AWS 中创建安全组来限制 IP 访问。为了实现高可用性，可以根据您的部署要求从 EIP 切换到专用 IP 移动解决方案。

如何跨不同 **AWS** 区域部署具有弹性 **IP** 地址的 **VPX** 高可用性对

下面是在两个不同的子网或两个不同的 AWS 可用性区域中部署 VPX 对的步骤摘要。

1. 创建 Amazon 虚拟私有云。
2. 将两个 VPX 实例部署在两个不同的可用性区域中或同一个区域但不同的子网中。
3. 步骤 3. 配置高可用性
    a) 在两个实例中在 INC 模式下设置高可用性。
    b) 在两个实例中添加一个 IP 集 。
    c) 将两个实例中的 IP 集绑定到 VIP。
    d) 在主实例中添加虚拟服务器。

对于步骤 1 和 2，请使用 AWS 控制台。对于步骤 3，使用 NetScaler VPX GUI 或 CLI。

步骤 **1.** 创建 Amazon 虚拟私有云 (VPC)。

步骤 **2.** 在两个不同的可用区域或同一区域但不同的子网中部署两个 VPX 实例。将 EIP 附加到主 VPX 的 VIP。

有关如何在 AWS 上创建 VPC 和部署 VPX 实例的更多信息，请参阅 在 AWS 上部署 NetScaler VPX 独立实例 和 场景：独立实例

步骤 **3.** 配置高可用性. 您可以使用 NetScaler VPX CLI 或 GUI 来设置高可用性。

使用 **CLI** 配置高可用性

1. 在两个实例中在 INC 模式下设置高可用性。

   在主节点上：

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   在辅助节点上：

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> 是指辅助节点的管理 NIC 的专用 IP 地址。

   <prim_ip> 是指主节点的管理 NIC 的专用 IP 地址。

2. 在两个实例中添加 IP 集。

   在两个实例上键入以下命令。

   ```
   add ipset <ipsetname>
   ```

3. 将 IP 集绑定到两个实例上的 VIP 集。

   在两个实例上键入以下命令：

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   bind ipset <ipsetname> <secondary VIP>
   ```

   > 注意：
   >
   > 可以将 IP 集绑定到主 VIP 或二级 VIP。但是，如果将 IP 集绑定到主 VIP，请使用二级 VIP 添加到虚拟服务器，反之亦然。

4. 在主实例上添加一个虚拟服务器。

   键入以下命令：

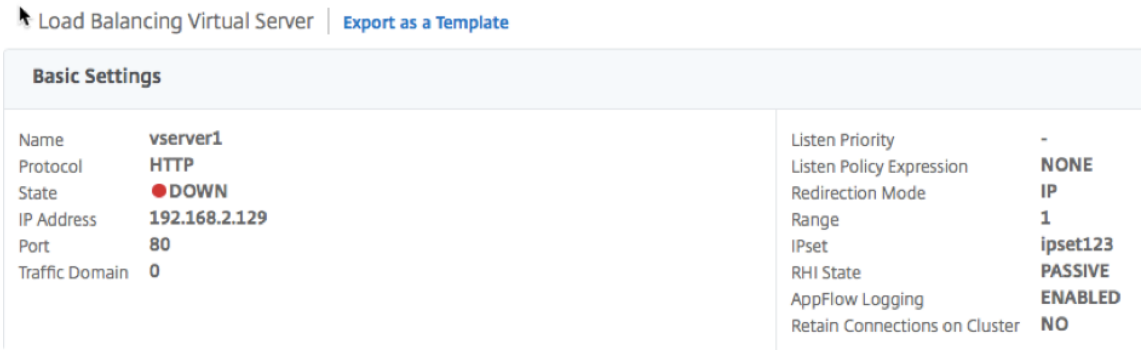
   ```
   add &#060;server_type&#062; vserver &#060;vserver_name&#062;
   &#060;protocol&#062; &#060;primary_vip&#062; &#060;port&#062; -
   ipset \\&#060;ipset_name&#062;
   ```

使用 **GUI** 配置高可用性

1. 在两个实例上在 INC 模式下设置高可用性。
2. 使用用户名 nsroot 和实例 ID 作为密码登录主节点。
3. 在 GUI 中，转到 配置 > 系统 > 高可用性。单击添加。
4. 在 远程节点 **IP** 地址 字段中，添加辅助节点的管理 NIC 的专用 IP 地址。

5. 选择在自助节点上打开 **NIC**（**Independent Network Configuration,** 独立网络配置）模式。
6. 在 **Remote System Login Credential**（远程系统登录凭据）下，添加辅助节点的用户名和密码，然后单击 **Create**（创建）。
7. 在辅助节点中重复这些步骤。
8. 添加 IP 集名称，然后单击 Insert（插入）。
9. 在 GUI 中，导航到“系统”>“网络”>“**IP**”>“添加”。
10. 添加 IP 地址、子网掩码、IP 类型（虚拟 IP）所需的值，然后单击 创建。
11. 导航到 系统 > 网络 > **IP** 集 > 添加。添加 IP 集名称，然后单击 **Insert**（插入）。
12. 在 IPv4s 页面中，选择虚拟 IP，然后单击 插入。单击 **Create**（创建）以创建 IP 集。
13. 在主实例中添加虚拟服务器

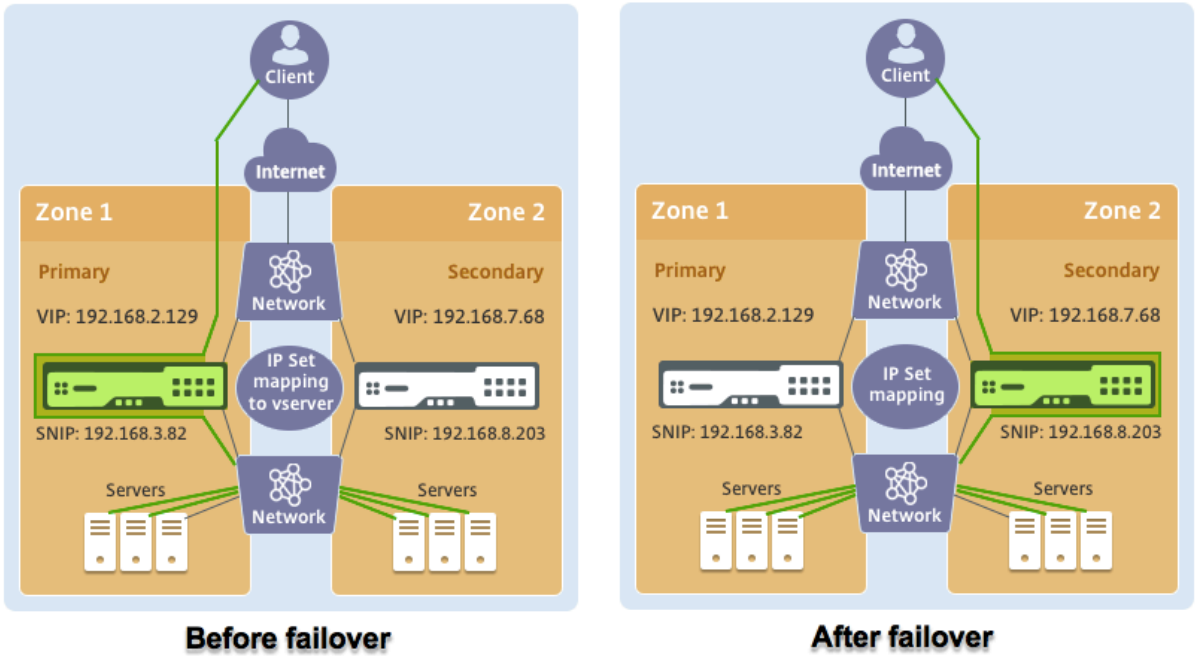
    在 GUI 中，转到 **Configuration**（配置）> **Traffic Management**（流量管理）> **Virtual Servers**（虚拟服务器）> **Add**（添加）。



场景

在这种情况下，将创建一个 VPC。在该 VPC 中，在两个可用性区域中创建了两个 VPX 实例。每个实例都有三个子网 - 一个用于管理，一个用于客户端，一个用于后端服务器。EIP 附加到主节点的 VIP。

图：此图说明了 AWS 上 INC 模式下的 NetScaler VPX 高可用性设置



对于这种情况，请使用 CLI 配置高可用性。

1. 在两个实例中在 INC 模式下设置高可用性。

   在主节点和辅助节点上键入以下命令。

   在主节点上：

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   此处，192.168.6.82 是指辅助节点的管理 NIC 的专用 IP 地址。

   在辅助节点上：

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   此处，192.168.1.108 是指主节点的管理 NIC 的专用 IP 地址。

2. 在两个实例上添加 IP 集并将 IP 集绑定到 VIP

   在主节点上：

   ```
   add ipset ipset123
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   bindipset ipset123 192.168.7.68
   ```

   在辅助节点上：

   ```
   add ipset ipset123
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   bind ipset ipset123 192.168.7.68
   ```

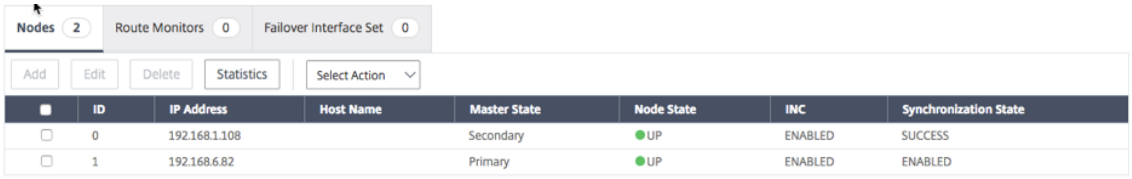

3. 在主实例上添加一个虚拟服务器。

   以下命令：

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. 步骤 7. 保存配置。

5. 执行强制故障转移后，辅助节点将成为新的主节点。



跨不同 **AWS** 区域部署具有专用 **IP** 地址的 **VPX** 高可用性对

October 17, 2024

可以在 INC 模式下使用专用 IP 地址在两个不同的子网或两个不同的 AWS 可用性区域中配置两个 NetScaler VPX 实例。该解决方案可以轻松地与具有弹性 IP 地址 的现有多区域
VPX 高可用性对集成。因此，您可以一起使用这两个解决方案。</p>

有关高可用性的更多信息，请参阅 高可用性。有关 INC 的更多信息，请参阅 在不同子网中配置高可用性节点。

> 注意：
>
> 此部署受 NetScaler 13.0 版本 67.39 以后的版本的支持。此部署与 AWS Transit Gateway 兼容。

使用 **AWS** 非共享 **VPC** 与专用 **IP** 地址进行高可用性配对

必备条件

确保与您的 AWS 帐户关联的 IAM 角色具有以下 IAM 权限：

```
1   {
2
3       "Version": "2012-10-17",
```



```
        "Statement": [
            {

                "Action": [
                    "ec2:DescribeInstances",
                    "ec2:DescribeAddresses",
                    "ec2:AssociateAddress",
                    "ec2:DisassociateAddress",
                    "ec2:DescribeRouteTables",
                    "ec2:DeleteRoute",
                    "ec2:CreateRoute",
                    "ec2:ModifyNetworkInterfaceAttribute",
                    "iam:SimulatePrincipalPolicy",
                    "iam:GetRole"
                ],
                "Resource": "*",
                "Effect": "Allow"
             }

        ]
    }
```

使用 **AWS** 非共享 **VPC** 部署具有专用 **IP** 地址的 **VPX HA** 对

下面是使用专用 IP 地址在两个不同子网或两个不同的 AWS 可用性区域中部署 VPX 对的步骤摘要。

1. 创建 Amazon 虚拟私有云。
2. 在两个不同的可用性区域中部署两个 VPX 实例。
3. 步骤 3. 配置高可用性

    a) 在两个实例中在 INC 模式下设置高可用性。
    b) 在 VPC 中添加指向客户端接口的相应路由表。
    c) 在主实例中添加虚拟服务器。

对于步骤 1、2 和 3b，请使用 AWS 控制台。对于步骤 3a 和 3c，请使用 NetScaler VPX GUI 或 CLI。

步骤 **1.** 创建 Amazon 虚拟私有云 (VPC)。

步骤 **2.** 在两个不同的可用区中部署具有相同数量 ENI（网络接口）的两个 VPX 实例。

有关如何在 AWS 上创建 VPC 和部署 VPX 实例的更多信息，请参阅 在 AWS 上部署 NetScaler VPX 独立实例 和 场景：独立实例

步骤 **3.** 通过选择与 Amazon VPC 子网不重叠的子网来配置 ADC VIP 地址。如果您的 VPC 为 192.168.0.0/16，要配置 ADC VIP 地址，可以从以下 IP 地址范围中选择任何子网：

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

在此示例中，选择了 10.10.10.0/24 子网并在此子网中创建了 VIP。可以选择 VPC 子网以外的任何子网 (192.168.0.0/16)。

步骤 **4.** 从 VPC 路由表中添加指向主节点的客户端接口 (VIP) 的路由。

在 AWS CLI 中，键入以下命令：

```
aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-block 10.10.10.0/24 --gateway-id <eni-client-primary>
```

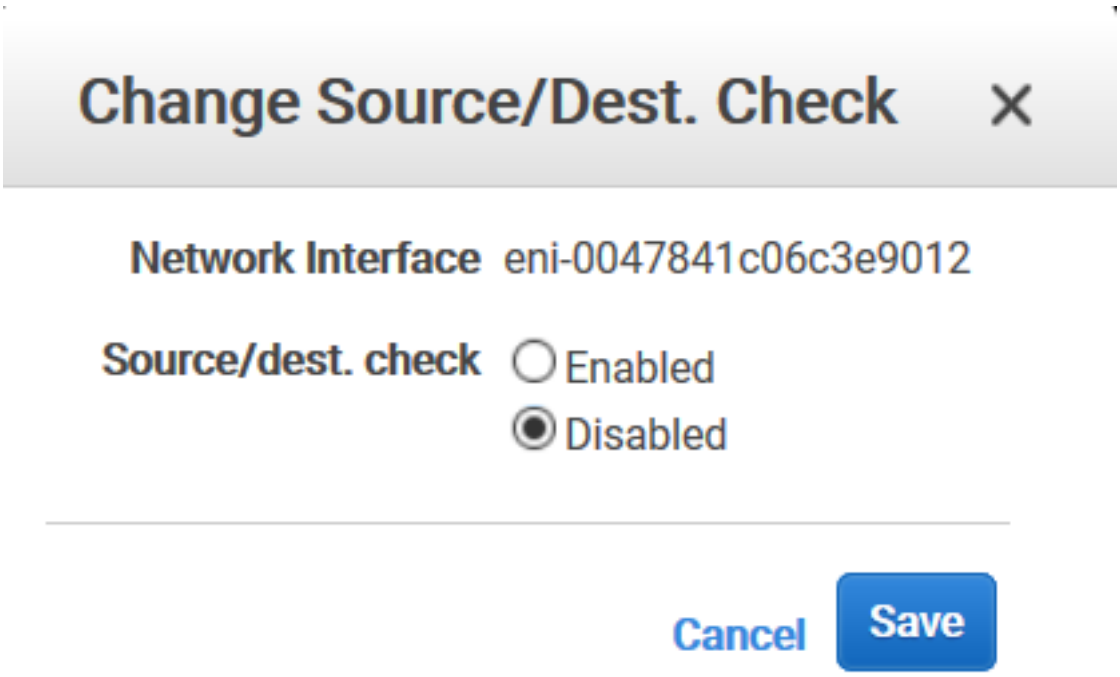
在 AWS GUI 中，执行以下步骤以添加路由：

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 **Route Tables**（路由表），然后选择路由表。
3. 选择 **Actions**（操作），然后单击 **Edit routes**（编辑路线）。
4. 要添加路线，请选择 **Add route**（添加路线）。对于 **Destination**（目标），输入目标 CIDR 块、单个 IP 地址或前缀列表的 ID。对于网关 ID，请选择主节点的客户端接口的 ENI。

> 注意：
>
> 必须在主实例的客户端 ENI 上禁用 **Source/Dest Check**（源/目标检查）。

要使用控制台禁用网络接口的源/目标检查，请执行以下步骤：

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 **Network Interfaces**（网络接口）。
3. 选择主客户端接口的网络接口，然后选择 **Actions**（操作），然后单击“**Change Source/Dest**”（更改源/目标）。检查。
4. 在对话框中，选择 **Disabled**（已禁用），然后单击 **Save**（保存）。



步骤 **5.** 配置高可用性. 您可以使用 NetScaler VPX CLI 或 GUI 来设置高可用性。

使用 **CLI** 配置高可用性

1. 在两个实例中在 INC 模式下设置高可用性。

在主节点上：

```
1 ```
2   add ha node 1 \<sec\_ip\> -inc ENABLED
3 ```
```

在辅助节点上：

```
1 ```
2   add ha node 1 \<prim\_ip\> -inc ENABLED
3 ```
```

<sec_ip> 是指辅助节点的管理 NIC 的专用 IP 地址。

<prim_ip> 是指主节点的管理 NIC 的专用 IP 地址。

1. 在主实例上添加一个虚拟服务器。必须从选定的子网进行添加，例如 10.10.10.0/24。

键入以下命令：

```
1 ```
```

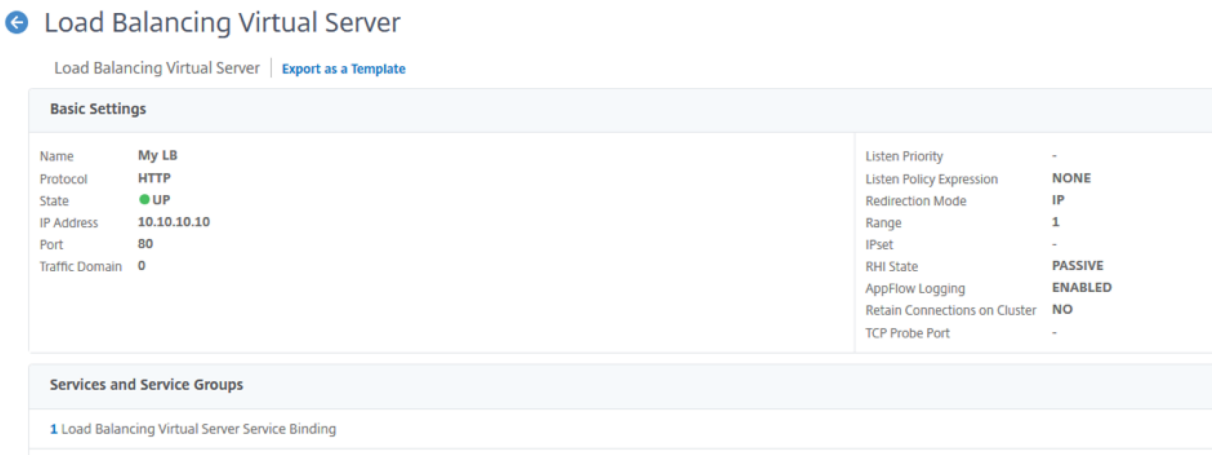


```
2    add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<primary
        \_vip\> \<port\>
3  ```
```

使用 **GUI** 配置高可用性

1. 在两个实例上在 INC 模式下设置高可用性。
2. 使用用户名 `nsroot` 和实例 ID 作为密码登录主节点。
3. 导航到 **Configuration**（配置）> **System**（系统）> **High Availability**（高可用性），然后单击 **Add**（添加）。
4. 在 远程节点 **IP** 地址 字段中，添加辅助节点的管理 NIC 的专用 IP 地址。
5. 选择在自助节点上打开 **NIC**（**Independent Network Configuration,** 独立网络配置）模式。
6. 在 **Remote System Login Credential**（远程系统登录凭据）下，添加辅助节点的用户名和密码，然后单击 **Create**（创建）。
7. 在辅助节点中重复这些步骤。
8. 在主实例中添加虚拟服务器

导航到 **Configuration**（配置）> **Traffic Management**（流量管理）> **Virtual Servers**（虚拟服务器）> **Add**（添加）。



使用 **AWS** 共享 **VPC** 部署具有专用 **IP** 地址的 **VPX HA** 对

在 AWS 共享 VPC 模型中，拥有 VPC 的帐户（所有者）与其他帐户（参与者）共享一个或多个子网。因此，您有一个 VPC 所有者帐户和一个参与者帐户。共享子网后，参与者可以在与其共享的子网中查看、创建、修改和删除其应用程序资源。参与者无法查看、修改或删除属于其他参与者或 VPC 所有者的资源。

有关 AWS 共享 VPC 的信息，请参阅 AWS 文档。

> 注意：
>
> 使用 AWS 共享 VPC 部署带有私有 IP 地址的 VPX HA 对的配置步骤 与使用 AWS 非共享 VPC 使用私有 IP 地址部署 VPX HA 对 的配置步骤相同，但以下情况除外：
>
> - VPC 中指向客户端接口的路由表必须从 *VPC* 所有者帐户中添加。

必备条件

- 确保 AWS 参与者帐户中与 NetScaler VPX 实例关联的 IAM 角色具有以下 IAM 权限：

```
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    }
```

> 注意：
>
> **AssumeRole** 允许 NetScaler VPX 实例担任由 VPC 所有者帐户创建的跨帐户 IAM 角色。

- 确保 VPC 所有者帐户使用跨帐户 IAM 角色向参与者帐户提供以下 IAM 权限：

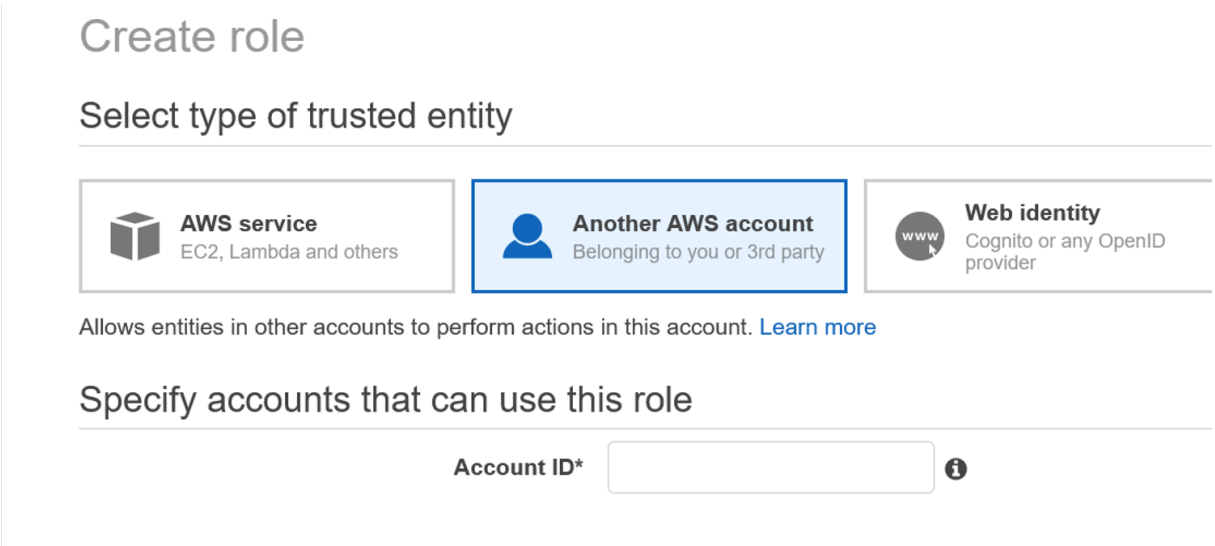
```
1    {
2
3        "Version": "2012-10-17",
4        "Statement": [
5            {
6
7                "Sid": "VisualEditor0",
8                "Effect": "Allow",
9                "Action": [
10                   "ec2:CreateRoute",
11                   "ec2:DeleteRoute",
12                   "ec2:DescribeRouteTables"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



```
                ],
                "Resource": "*"
            }

        ]
    }
```

创建跨帐户 **IAM** 角色

1. 登录 AWS Web 控制台。
2. 在 **IAM** 选项卡中，导航到 角色，然后选择 创建角色。
3. 选择 另一个 **AWS** 帐户。



1. 输入要授予管理员访问权限的参与者帐户的 12 位帐户 ID 号。

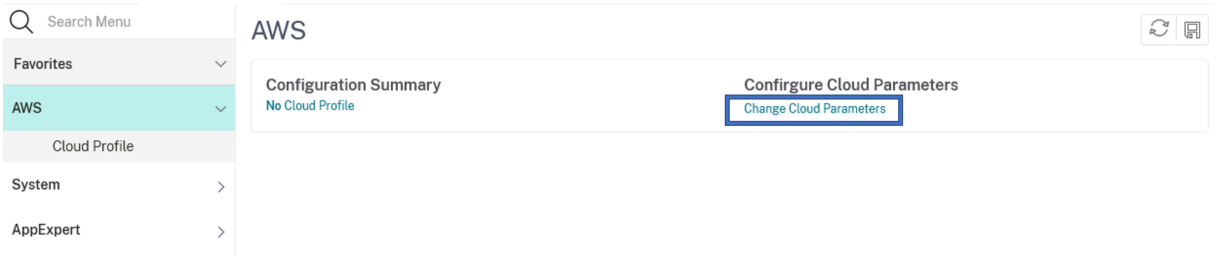
使用 **NetScaler CLI** 设置跨帐户 **IAM** 角色

以下命令使 NetScaler VPX 实例能够扮演 VPC 所有者帐户中存在的跨帐户 IAM 角色。

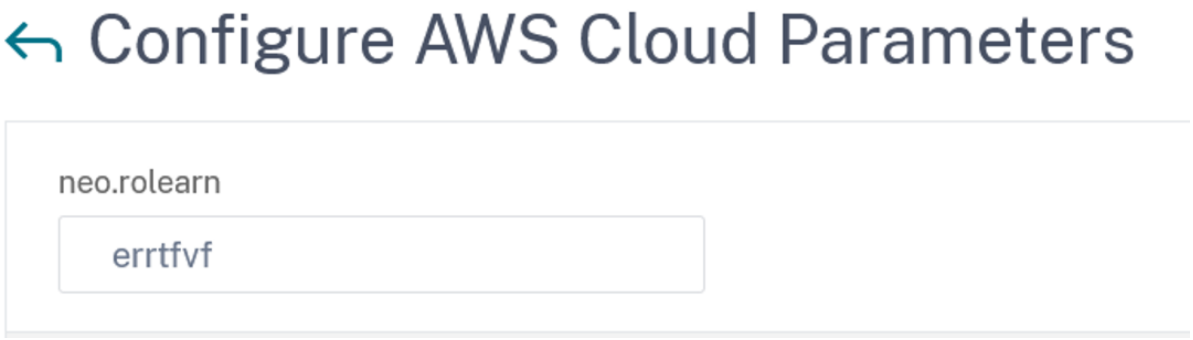
```
set cloud awsParam -roleARN <string>
```

使用 **NetScaler GUI** 设置跨帐户 **IAM** 角色

1. 登录 NetScaler 设备并导航到 配置 **> AWS >** 更改云参数。



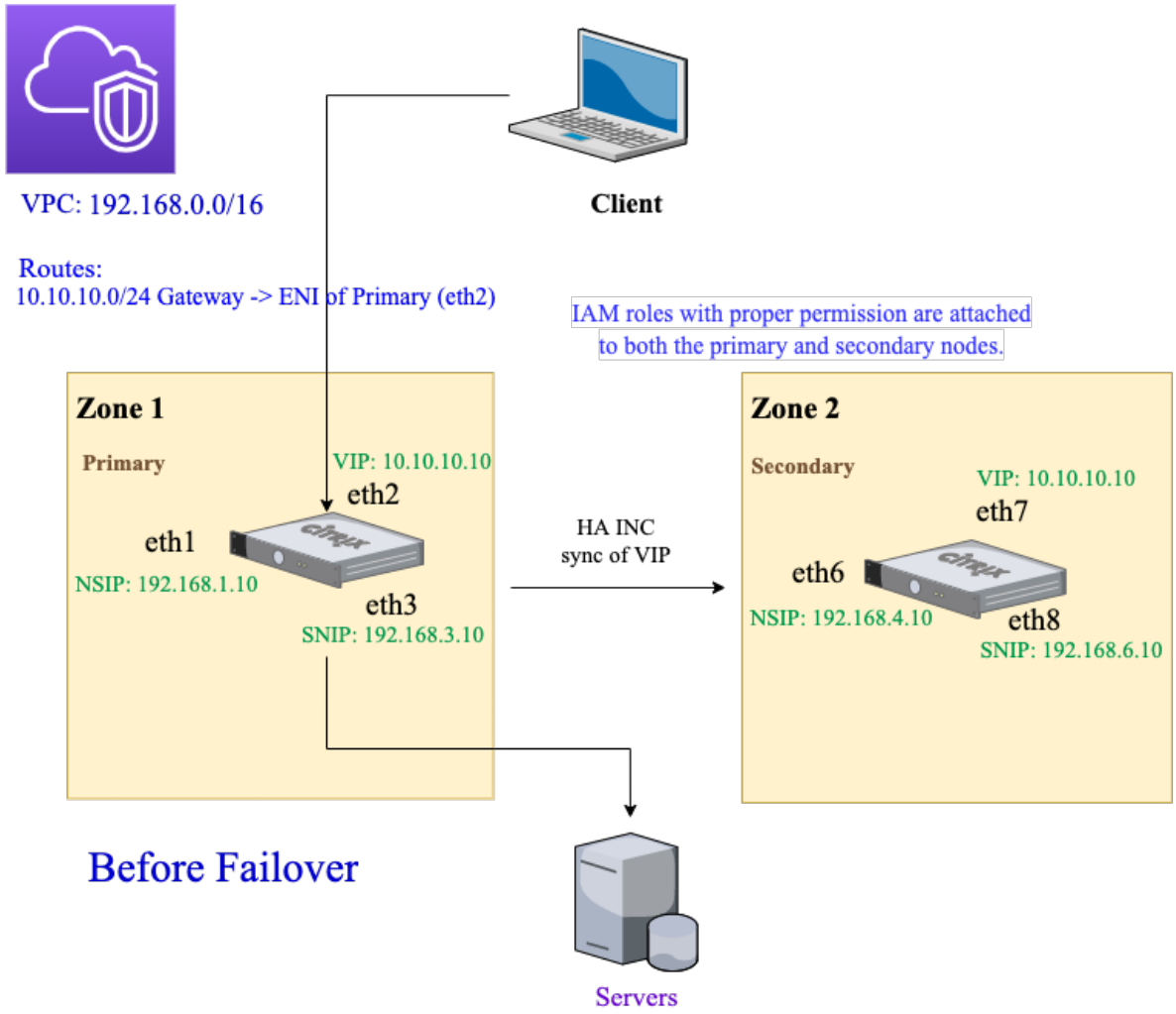
1. 在 配置 **AWS** 云参数 页面中，输入 **roLearn** 字段的值。

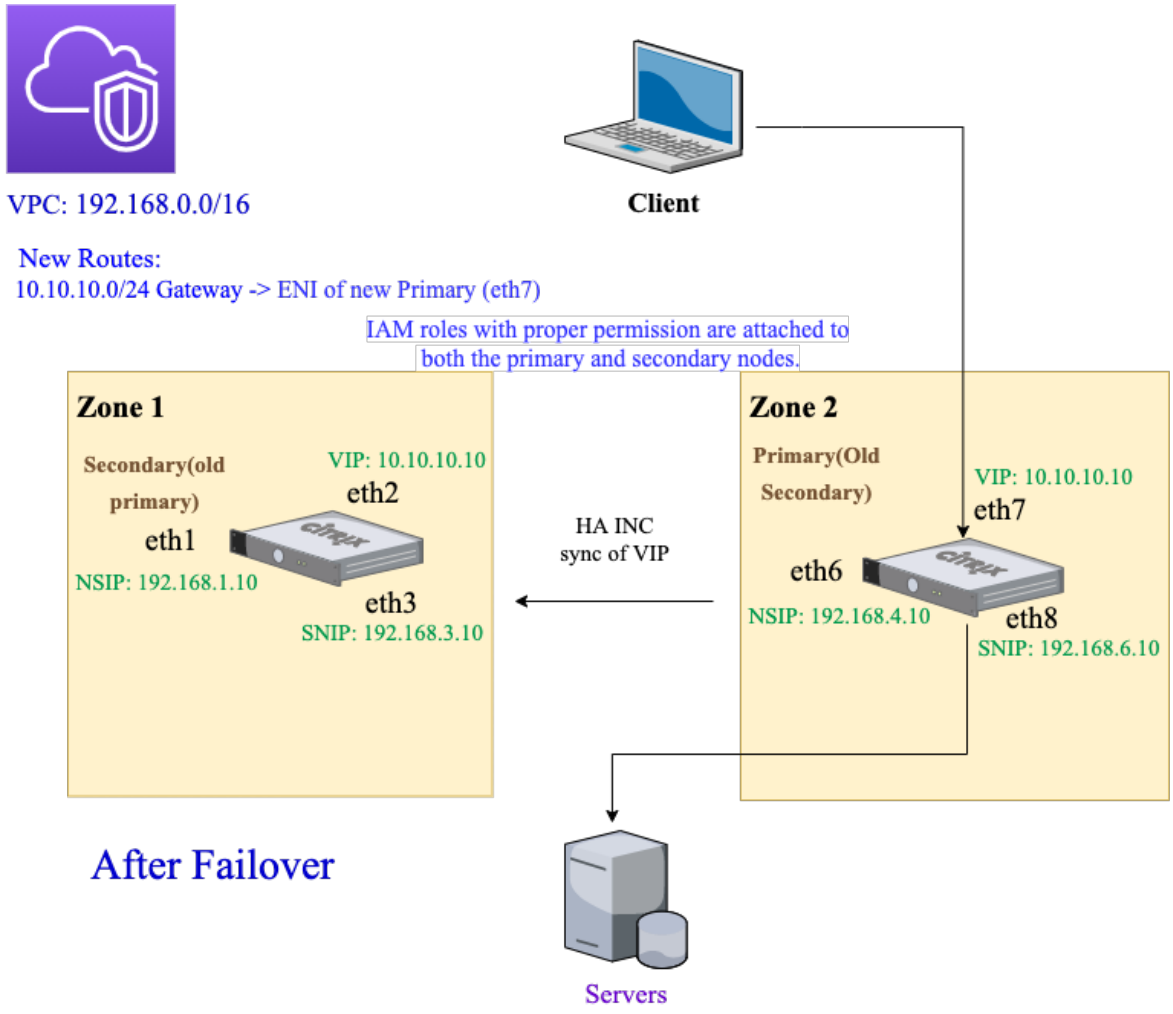


场景

在这种情况下，将创建一个 VPC。在该 VPC 中，在两个可用性区域中创建了两个 VPX 实例。每个实例都有三个子网 - 一个用于管理，一个用于客户端，一个用于后端服务器。

下图说明了 AWS 上 INC 模式下的 NetScaler VPX 高可用性设置。不属于 VPC 的自定义子网 10.10.10.10 用作 VIP。因此，10.10.10.10 子网可以跨可用性区域使用。





对于这种情况，请使用 CLI 配置高可用性。

1. 在两个实例中在 INC 模式下设置高可用性。

在主节点和辅助节点上键入以下命令。

在主节点上：

```
```
  add ha node 1 192.168.4.10 -inc enabled
```
```

此处，192.168.4.10 是指辅助节点的管理 NIC 的专用 IP 地址。

在辅助节点上：

```
```
  add ha node 1 192.168.1.10 -inc enabled
```
```

此处，192.168.1.10 是指主节点的管理 NIC 的专用 IP 地址。

1. 在主实例上添加一个虚拟服务器。

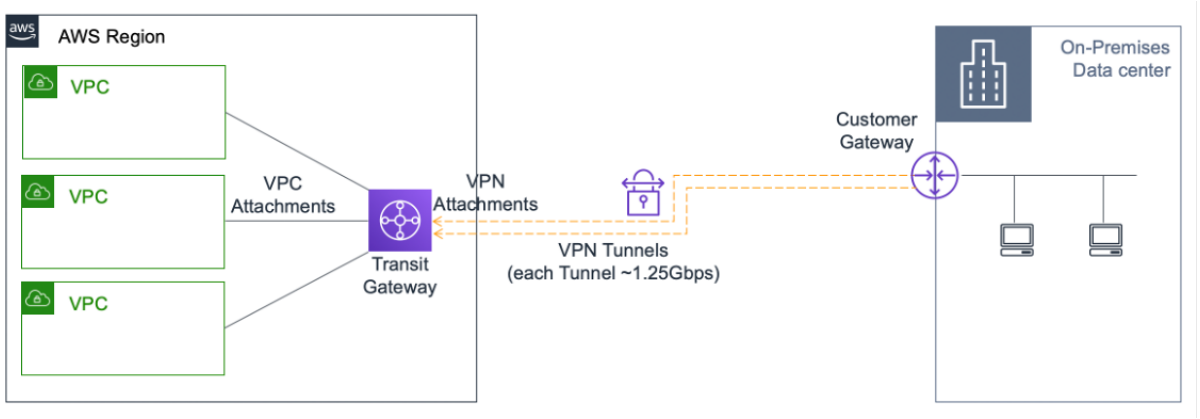
键入以下命令：

```
```
  add lbvserver vserver1 http 10.10.10.10 80
```
```

1. 步骤 7. 保存配置。
2. 强制故障转移后：
   - 辅助实例将成为新的主实例。
   - 指向主 ENI 的 VPC 路由迁移到辅助客户端 ENI。
   - 客户端流量将恢复到新的主实例。

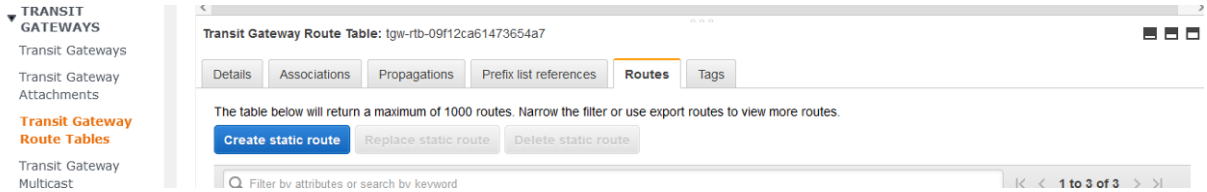
适用于 **HA** 专用 **IP** 解决方案的 **AWS Transit Gateway**

您需要使用 AWS Transit Gateway 才能使专用 VIP 子网在内部网络内、跨 AWS VPC、区域和本地网络进行路由。VPC 必须连接到 AWS Transit Gateway。AWS Transit Gateway 路由表中的 VIP 子网或 IP 池的静态路由将创建并指向 VPC。

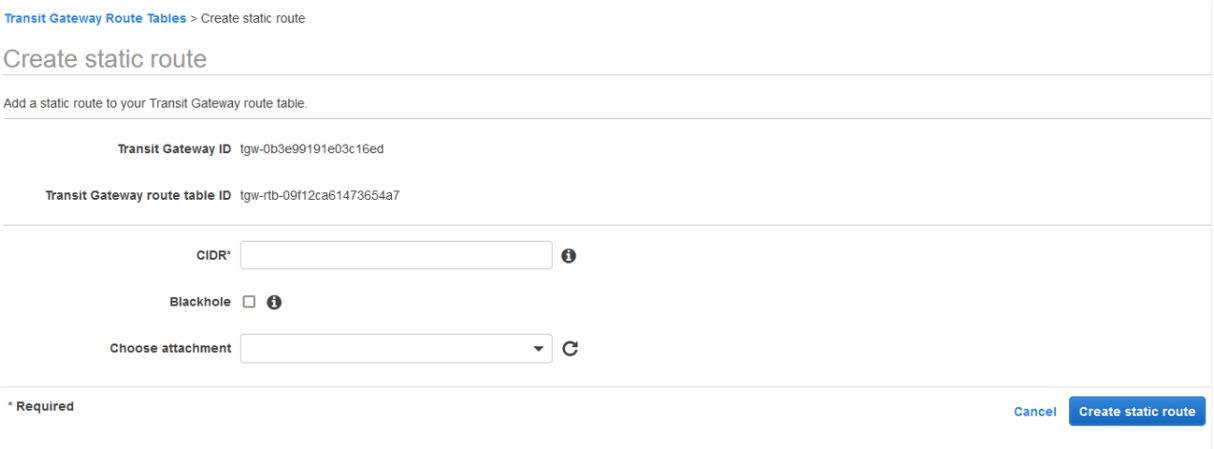


要配置 AWS Transit Gateway，请执行以下步骤：

1. 打开 Amazon VPC 控制台。
2. 在导航窗格上，选择 **Transit Gateway** 路由表。
3. 选择 路 由选项卡，然后单击 创建静态路由。



1. 创建静态路由，其中 CIDR 指向您的私有 VIPS 子网，连接指向具有 NetScaler VPX 的 VPC。



1. 单击 创建静态路由，然后选择 关闭。

故障排除

如果您在跨多区域高可用性配置高可用性专用 IP 解决方案时遇到任何问题，请检查以下要点进行故障排除：

- 主节点和辅助节点都具有相同的 IAM 权限集。
- 在主节点和辅助节点上均启用 INC 模式。
- 主节点和辅助节点的接口数量相同。
- 创建实例时，请根据设备索引号在主节点和辅助节点上按照相同的顺序连接接口。假设在主节点上，首先连接客户端接口，然后连接服务器接口。在辅助节点上也遵循相同的顺序。如果有任何不匹配，请分离接口，然后按正确的顺序重新连接接口。
- 您可以按照以下导航路径验证接口顺序：**AWS** 控制台 **>** 网络和安全 **> ENI >** 设备索引号。默认情况下，为这些接口分配了以下设备索引号：- 管理接口-0 - 客户端接口-1 - 服务器接口-2
  - 管理接口–0
  - 客户端接口–1
  - 服务器接口–2
- 如果主 ENI 上的设备索引号序列为：0、1、2。辅助 ENI 还必须遵循相同的设备索引号序列：0、1、2。

如果设备索引号序列不匹配，则所有不匹配的路由都将传输到索引 0（管理接口），以避免任何路由丢失。但是，您仍然必须分离接口，然后按照正确的顺序重新连接它们，以避免路由移动到管理接口，因为这可能会导致流量拥塞。

- 如果流量不流动，请确保“Source/dest. Check”首次在主节点的客户端界面上被禁用。首次在主节点的客户端界面上禁用“检查”。
- 确保 `cloudhadaemon` 命令 (`ps -aux | grep cloudha`) 正在命令行管理程序中运行。
- 确保 NetScaler 固件版本为 13.0 Build 70.x 或更高版本。
- 对于故障转移过程的问题，请检查以下日志文件：`/var/log/cloud-ha-daemon.log`

在 **AWS Outposts** 上部署 **NetScaler VPX** 实例

October 17, 2024

AWS Outposts 是部署在您的站点的 AWS 计算和存储容量。Outposts 在您的本地位置提供 AWS 基础结构和服务。AWS 作为 AWS 区域的一部分运营、监视和管理此容量。您可以在本地和 AWS 云中使用相同的 NetScaler VPX 实例、AWS API、工具和基础设施，以获得一致的混合体验。

可以在 Outposts 中创建子网，并在创建 EC2 实例、EBS 卷、ECS 群集和 RDS 实例等 AWS 资源时指定子网。Outposts 子网中的实例使用专用 IP 地址与 AWS 区域中的其他实例进行通信，所有这些都位于同一 Amazon 虚拟私有云 (VPC) 内。

有关更多信息，请参阅 AWS Outposts 用户指南。

AWS Outposts 的工作原理

AWS Outposts 旨在使用您的 Outposts 与 AWS 区域之间的持续一致连接运行。要实现与区域以及本地环境中的本地工作负载的连接，您必须将 Outposts 连接到本地网络。您的本地网络必须为区域和 Internet 提供 WAN 访问权限。Internet 还必须提供对本地工作负载或应用程序所在的本地网络的 LAN 或 WAN 访问。

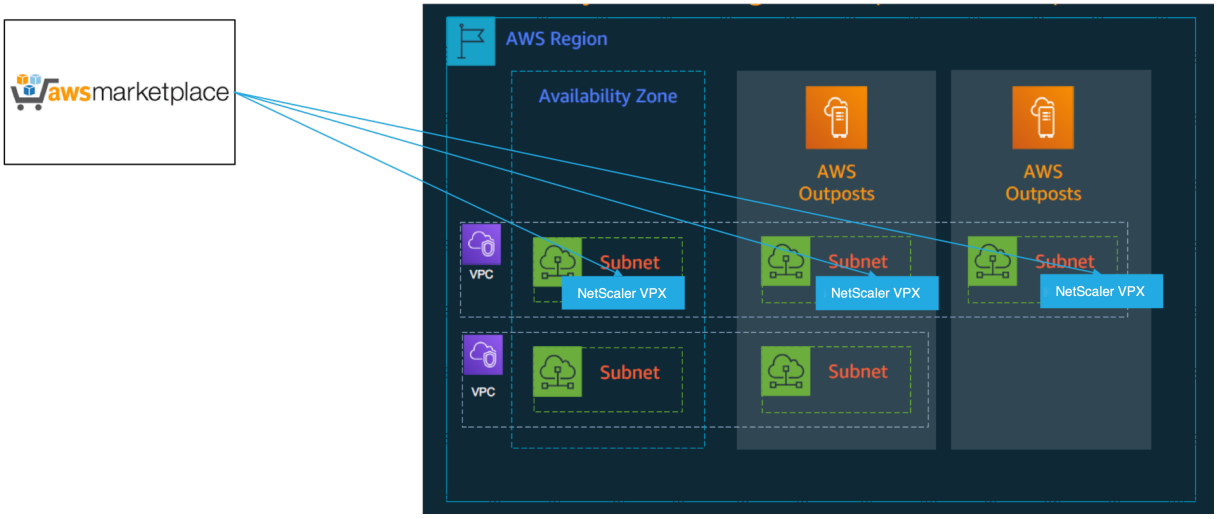
必备条件

- 必须在您的站点上安装 AWS Outposts。
- AWS Outposts 的计算和存储容量必须可供使用。

有关如何订购 AWS Outposts 的更多信息，请参阅以下 AWS 文档：https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

使用 **AWS Web** 控制台在 **AWS Outposts** 上部署 **NetScaler VPX** 实例

下图描述了 NetScaler VPX 实例在前哨基地的简单部署。AWS Marketplace 中存在的 NetScaler AMI 也部署在前哨基地中。



登录 AWS Web 控制台并完成以下步骤，在您的 AWS Outposts 上部署 NetScaler VPX EC2 实例。

1. 创建密钥对。
2. 创建虚拟私有云 (VPC)。
3. 添加更多子网。
4. 创建安全组和安全规则。
5. 添加路由表。
6. 创建 Internet 网关。
7. 使用 AWS EC2 服务创建 NetScaler VPX 实例。从 AWS 控制板中，导航到 **Compute**（计算）**> EC2 > Launch Instance**（启动实例）**> AWS Marketplace**。
8. 创建并连接更多网络接口。
9. 将弹性 IP 地址附加到管理 NIC。
10. 连接到 VPX 实例。

有关每个步骤的详细说明，请参阅 使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例。

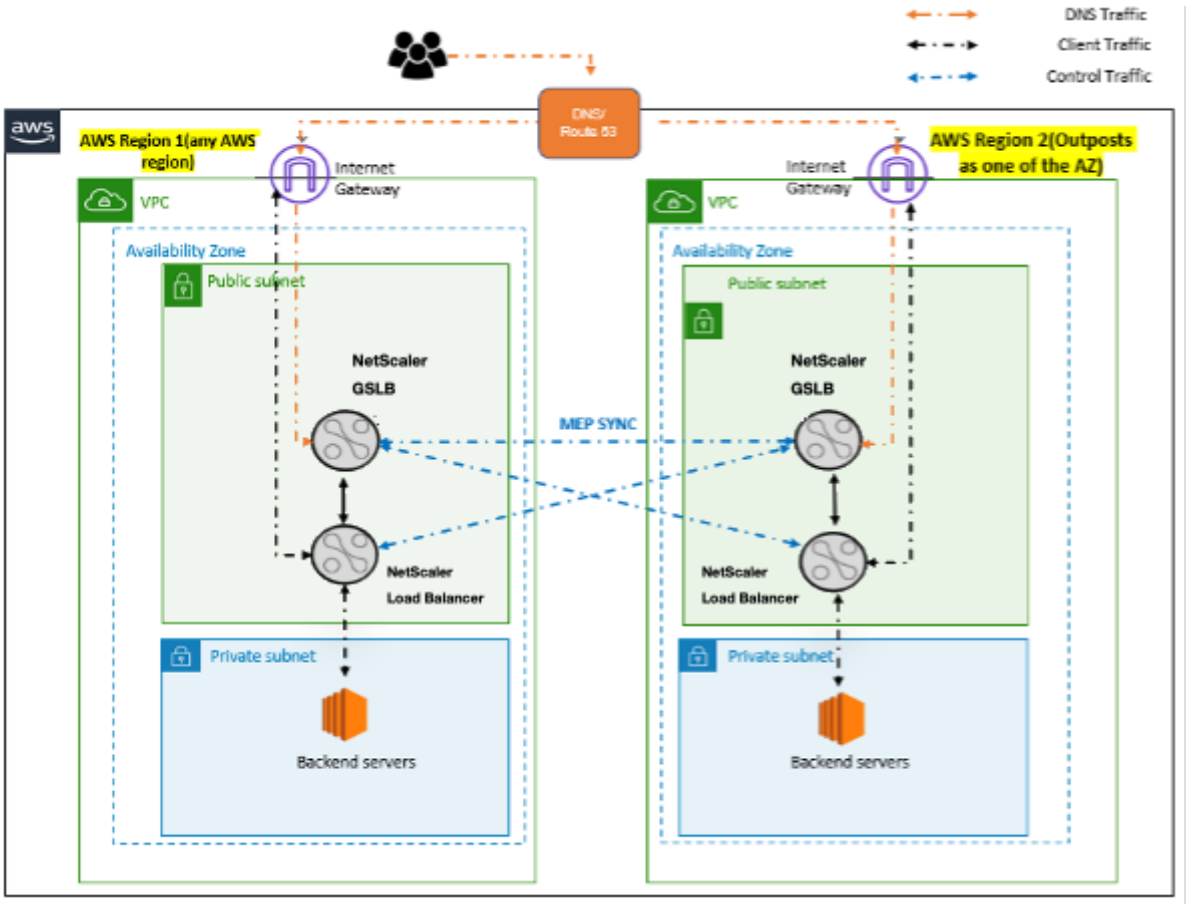
有关同一可用区域部署内的高可用性，请参阅 在 AWS上部署高可用性对。

使用 **AWS Outposts** 在混合云上部署 **NetScaler VPX** 实例

您可以在包含 AWS 前哨基地的 AWS 环境中的混合云上部署 NetScaler VPX 实例。您可以使用 NetScaler 全局服务器负载平衡 (GSLB) 解决方案简化应用程序交付机制。GSLB 解决方案在使用 AWS 区域和 AWS Outposts 基础设施构建的混合云中的多个数据中心之间分配应用程序流量。

NetScaler GSLB 支持主动-主动和主动-被动部署类型，以解决不同的用例。除了这些灵活的部署选项和应用程序交付机制外，NetScaler 还可以保护整个网络和应用程序组合，无论应用程序是在 AWS Cloud 还是 AWS Outposts 上本地部署。

下图说明了在 AWS 的混合云中使用 NetScaler 设备交付应用程序。



在主动-主动部署中，NetScaler 在分布式环境中全局引导流量。环境中的所有站点都通过指标交换协议 (MEP) 交换有关其可用性和资源运行状况的指标。NetScaler 设备使用此信息对站点间的流量进行负载平衡，并将客户端请求发送到由 GSLB 配置中指定的定义方法（循环调度、最小连接和静态邻近度）确定的最合适的 GSLB 站点。

您可以使用主动-主动 GSLB 部署来：

- 在所有节点处于活动状态的情况下优化资源利用率。
- 通过将请求引导到离每个用户最近的站点来增强用户体验。
- 按照用户定义的速度将应用程序迁移到云端。

您可以将主动-被动 GSLB 部署用于：

- 灾难恢复
- 云层爆裂

引用

- 在 AWS 上部署 NetScaler VPX 实例
- 使用 AWS Web 控制台在 AWS Outposts 上部署 NetScaler VPX 实例
- 在 NetScaler VPX 实例上配置 GSLB

使用 NetScaler Web App Firewall 保护 AWS API 网关

October 17, 2024

您可以在 AWS API 网关前部署 NetScaler 设备，并保护 API 网关免受外部威胁。NetScaler Web App Firewall (WAF) 可以保护您的 API 免受 OWASP 十大威胁和零日攻击。NetScaler Web App Firewall 在所有 ADC 外形规格中使用单一代码库。因此，您可以在任何环境中一致地应用和实施安全策略。NetScaler Web App Firewall 易于部署，可作为单一许可证使用。NetScaler Web App Firewall 为您提供以下功能：

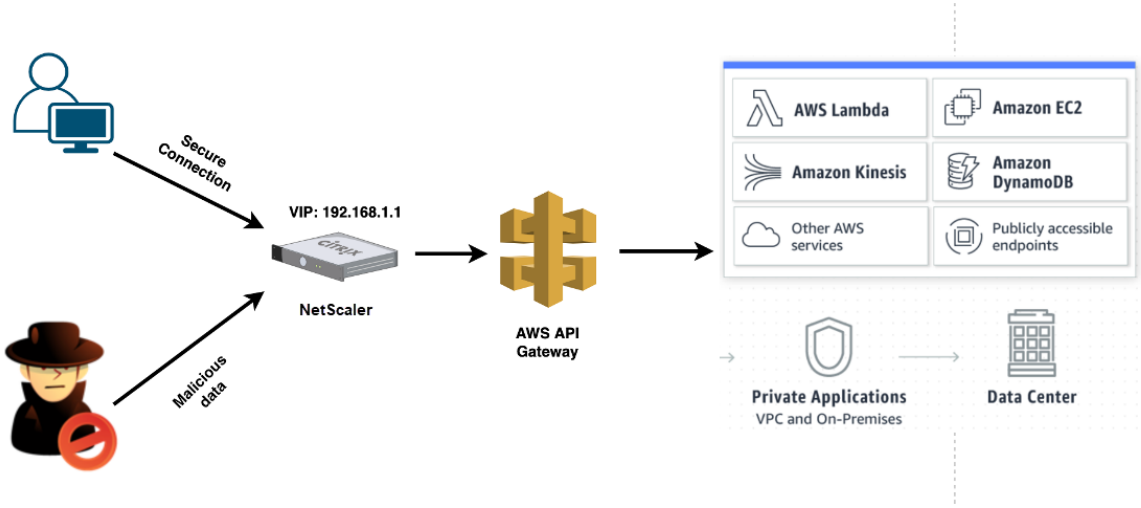
- 简化的配置
- 机器人管理
- 整体可见性
- 整理来自多个来源的数据，并在统一的屏幕中显示数据

除了 API 网关保护之外，您还可以使用其他 NetScaler 功能。有关更多信息，请参阅 NetScaler 文档。除了避免数据中心故障转移和最大限度地缩短关机时间外，您还可以在可用区内或跨可用区将 ADC 置于高可用性状态。您还可以使用或配置具有 AutoScale 功能的群集。

早些时候，AWS API Gateway 不支持保护其背后的应用程序所需的保护。如果没有 Web App Firewall (WAF) 保护，API 很容易受到安全威胁。

在 AWS API 网关前部署 NetScaler 设备

在以下示例中，NetScaler 设备部署在 AWS API 网关的前面。



让我们假设有一个对 AWS Lambda 服务的真正的 API 请求。此请求可以针对 亚马逊 API 网关文档中提到的任何API服务。如上图所示，流量流量如下：

1. 客户端向 AWS Lambda 函数 (XYZ) 发送请求。此客户端请求将发送到 NetScaler 虚拟服务器 (192.168.1.1)。

2. 虚拟服务器会检查数据包并检查是否存在任何恶意内容。
3. NetScaler 设备会触发重写策略以更改客户端请求中的主机名和 URL。例如，您要将 https://restapi.citrix.com/default/LamdaFunctionXYZ 更改为 https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ。
4. NetScaler 设备将此请求转发到 AWS API 网关。
5. AWS API 网关进一步将请求发送到 Lambda 服务并调用 Lambda 函数“XYZ”。
6. 同时，如果攻击者发送包含恶意内容的 API 请求，则该恶意请求将登陆到 NetScaler 设备上。
7. NetScaler 设备将检查数据包并根据配置的操作丢弃数据包。

配置启用 **WAF** 的 **NetScaler** 设备

要在 NetScaler 设备上启用 WAF，请执行以下步骤：

1. 添加内容交换或负载平衡虚拟服务器。假设虚拟服务器的 IP 地址是 192.168.1.1，它解析为域名 (restapi.citrix.com)。
2. 在 NetScaler 虚拟服务器上启用 WAF 策略。有关详细信息，请参阅 配置 Web App Firewall。
3. 启用重写策略以更改域名。比方说，您想将通过“restapi.citrix.com”域名向负载均衡器发送的传入请求更改为后端 AWS API 网关“citrix.execute-api”。<region>.amazonaws”域名。
4. 在 NetScaler 设备上启用 L3 模式以使其充当代理。使用以下命令：

```
enable ns mode L3
```

在上述示例的步骤 3 中，假设网站管理员希望 NetScaler 设备将“restapi.citrix.com”域名替换为“citrix.execute-api”。<region>.amazonaws.com”和带有“default/lambda/XYZ”的 URL。

以下过程介绍如何使用重写功能更改客户端请求中的主机名和 URL：

1. 使用 SSH 登录 NetScaler 设备。
2. 添加重写操作。

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

add rewrite action rewrite_url_act replace HTTP.REQ.URL.
    PATH_AND_QUERY "\"/default/lambda/XYZ\""
```

3. 为重写操作添加重写策略。

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

add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER(\"Host\").
    CONTAINS(\"restapi.citrix.com\") "rewrite_url_act
```


4. 将重写策略绑定到虚拟服务器。

```
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
```

有关详细信息，请参阅 在 NetScaler 设备上的客户端请求中配置重写以更改主机名和 URL。

NetScaler 特性和功能

除了保护部署安全之外，NetScaler 设备还可以根据用户要求增强请求。NetScaler 设备提供以下主要功能。

- 对 **API** 网关进行负载平衡：如果您有多个 API 网关，则可以使用 NetScaler 设备对多个 API 网关进行负载平衡，并定义 API 请求的行为。
  - 有不同的负载均衡方法可用。例如，最少连接方法可避免 API Gateway 限制过载，自定义加载方法在特定 API 网关上维护特定负载，依此类推。有关更多信息，请参阅 负载平衡算法。
  - SSL 卸载配置时不会中断流量。
  - 启用使用源 IP (USIP) 模式以保留客户端 IP 地址。
  - 用户定义的 SSL 设置：您可以使用自己签名的证书和算法拥有自己的 SSL 虚拟服务器。
  - 备份虚拟服务器：如果无法访问 API 网关，则可以将请求发送到备份虚拟服务器以执行进一步操作。
  - 还有许多其他负载平衡功能可用。有关更多信息，请参阅在 NetScaler 设备上对流量进行负载平衡。
- 身份验证、授权和审核：您可以定义自己的身份验证方法（如 LDAP、SAML、RADIUS），并授权和审核 API 请求。
- 响应者：您可以在关闭期间将 API 请求重定向到其他 API Gateway。
- 速率限制：您可以配置速率限制功能，以避免 API 网关过载。
- 更好的可用性：您可以在高可用性设置或群集设置中配置 NetScaler 设备，以便为 AWS API 流量提供更好的可用性。
- **REST API**：支持 REST API，可用于在云生产环境中自动执行工作。
- 监视数据：监视和记录数据以供参考。

NetScaler 设备提供了更多功能，这些功能可以与 AWS API 网关集成。有关更多信息，请参阅 NetScaler 文档。

添加后端 **AWS** 自动缩放服务

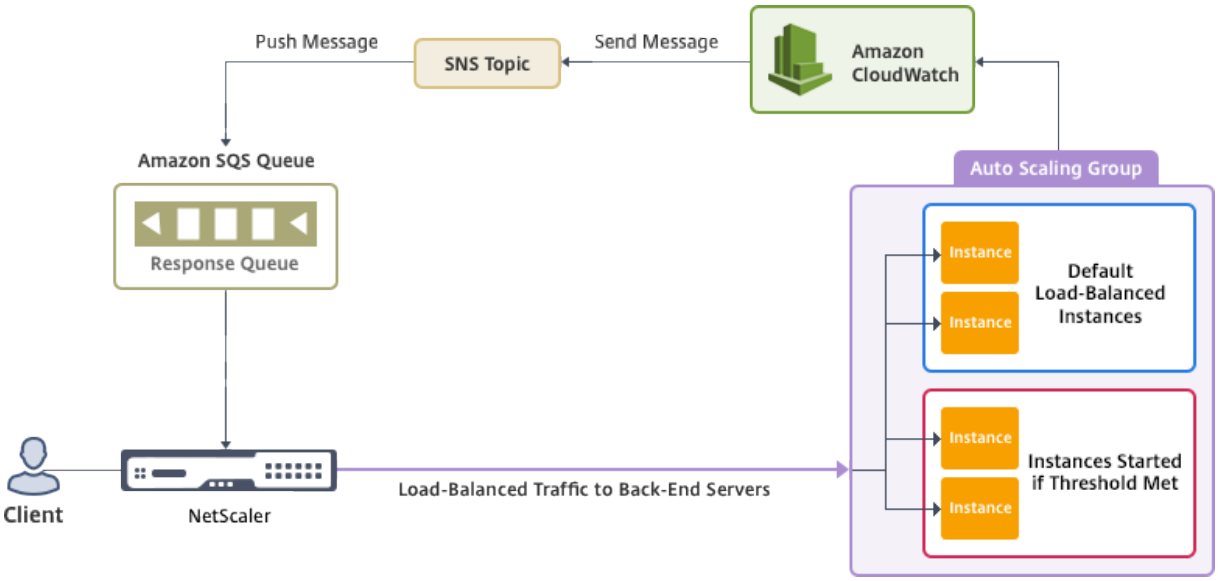
October 17, 2024

在云中高效托管应用程序涉及根据应用程序需求轻松且经济高效地管理资源。为了满足日益增长的需求，必须向上扩展网络资源。当需求减弱时，您需要缩小规模，以避免不必要的闲置资源成本。您可以通过在任何给定时间内仅部署所需数量的实例来最大限度地降低运行应用程序的成本。为此，您必须不断监视流量、内存和 CPU 使用情况等。但是，手动监视流量很麻烦。为了使应用程序环境动态地向上或向下扩展，您必须在必要时自动执行监视流量和向上和向下扩展资源的流程。

NetScaler VPX 实例与 AWS Auto Scaling 服务集成在一起，具有以下优势：

- 负载平衡和管理：根据需求，自动配置服务器以向上和向下扩展。VPX 实例会自动检测后端子网中的 AutoScale 组，并允许用户选择自动缩放组来平衡负载。所有这些操作都是通过在 VPX 实例上自动配置虚拟 IP 地址和子网 IP 地址来完成的。
- 高可用性：检测跨多个可用区和负载平衡服务器的 Autoscale 组。
- 提高了网络可用性：VPX 实例支持：
  - 通过使用 VPC 对等，后端服务器位于不同的 VPC 中
  - 位于相同置放组的后端服务器
  - 后端服务器位于不同的可用区中
- 正常连接终止：通过使用“Graceful Timeout”（正常超时）功能正常移除 Autoscale 服务器，从而避免在进行缩小活动时失去客户端连接。
- 备用服务器的连接耗尽：防止向处于待机状态的服务器发送任何新的客户端连接。但是，备用服务器仍然是 Autoscaling 组的一部分，它们将继续处理现有的客户端连接，直到它们关闭。当服务器变回 InService 状态时，服务器将恢复处理新连接。您可以使用待机状态来更新、修改服务器或对其进行故障排除，也可以根据要求缩小规模。有关更多信息，请参阅 A WS 文档。

图：带有 NetScaler VPX 实例的 AWS 自动扩缩服务



此图说明了 AWS 自动扩展服务如何与 NetScaler VPX 实例（负载平衡虚拟服务器）兼容。有关详细信息，请参阅以下 AWS 主题。

- 自动缩放组
- CloudWatch
- 简单通知服务 (SNS)
- Simple Queue Service (Amazon SQS)

开始之前的准备工作

在开始在 NetScaler VPX 实例上使用自动缩放之前，必须完成以下任务。

- 阅读以下主题：
  - 必备条件
  - 局限性与用法指南
- 根据您的要求在 AWS 上创建 NetScaler VPX 实例。
  - 有关如何创建 NetScaler VPX 独立实例的更多信息，请参阅 在 AWS 上部署 NetScaler VPX 独立实例 和 场景：独立实例
  - 有关如何在 HA 模式下部署 VPX 实例的更多信息，请参阅 在 AWS 上部署高可用性对。

  > 注意：
  >
  > 我们的建议如下：
  >
  > - 使用 CloudFormation 模板在 AWS 上创建 NetScaler VPX 实例。
  > - 创建三个独立的接口：一个用于管理 (NSIP)，一个用于面向客户端 LB 虚拟服务器 (VIP)，另一个用于子网 IP (NSIP)。

- 创建 AWS Autoscale 组。如果没有现有的自动缩放配置，您必须：
  1. 创建启动配置
  2. 创建自动扩缩组
  3. 验证自动扩缩组

  有关详细信息，请参阅 http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html。
- 从 NetScaler 版本 14.1-12.x 开始，在 AWS AutoScale 组中，只有启用了平滑选项后，才必须指定缩减策略。在 14.1-12.x 之前的 NetScaler 版本中，无论是否启用了 Graceful 选项，您都必须指定至少一个缩减策略。

  NetScaler VPX 实例仅支持步进扩展策略。AutoScale 组不支持简单扩展策略和目标跟踪扩展策略。
- 确保您的 AWS 帐户具有以下 IAM 权限：

```
1    {
2
3        "Version": "2012-10-17",
```



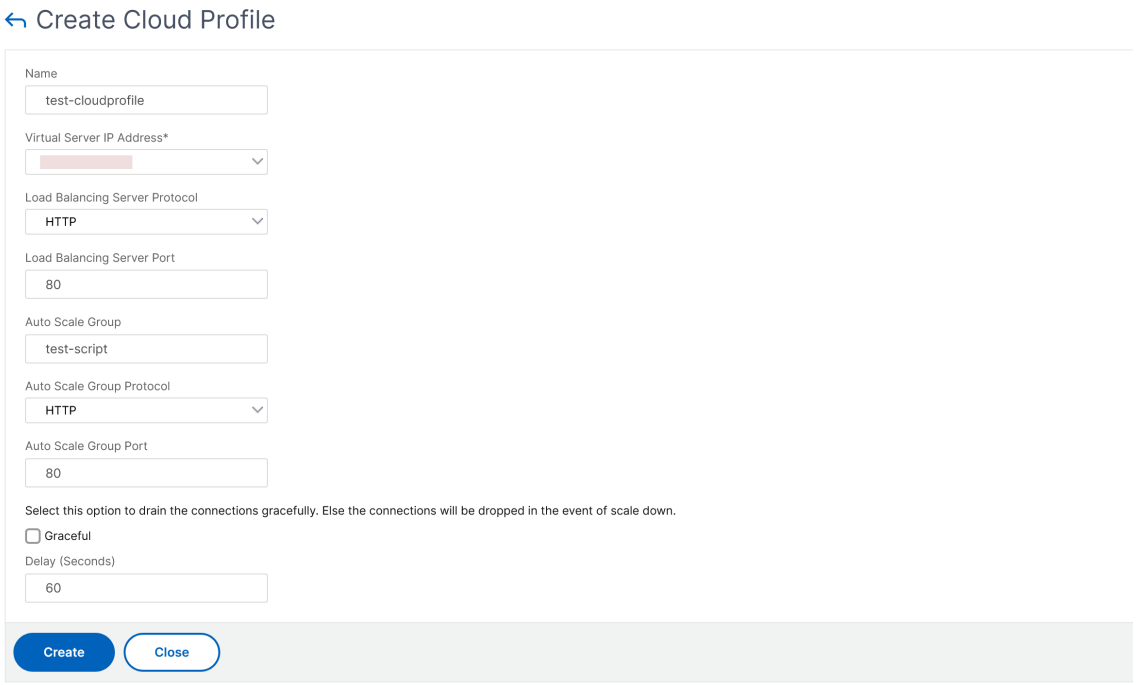
```
4          "Statement": \[
5           {
6
7                  "Action": \[
8                      "ec2:DescribeInstances",
9                      "ec2:DescribeNetworkInterfaces",
10                     "ec2:DetachNetworkInterface",
11                     "ec2:AttachNetworkInterface",
12                     "ec2:StartInstances",
13                     "ec2:StopInstances",
14                     "ec2:RebootInstances",
15                     "autoscaling:\*",
16                     "sns:\*",
17                     "sqs:\*"
18
19                     “iam: SimulatePrincipalPolicy”
20                     “iam: GetRole”
21                    \],
22                    "Resource": "\*",
23                    "Effect": "Allow"
24               }
25
26          \]
27      }
```

将 **AWS** 自动扩缩服务添加到 **NetScaler VPX** 实例

完成以下步骤，将自动扩展服务添加到 VPX 实例：

1. 使用您的 `nsroot` 凭证登录 VPX 实例。
2. 导航到“系统”**>**“**AWS**”**>**“云配置文件”，然后单击“添加”。

   将出现“创建云配置文件”配置页面。

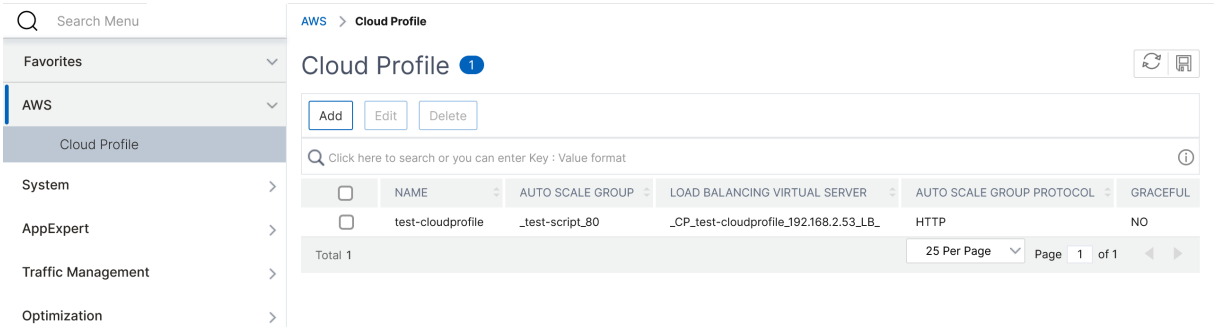


创建云端配置文件时的注意事项：

- 虚拟服务器 IP 地址是从 VPX 实例可用的免费 IP 地址中自动填充的。有关更多信息，请参阅 管理多个 IP 地址。
- 键入您在 AWS 帐户上配置的 AutoScale 组的确切名称。有关更多信息，请参阅 AWS 自动扩展组。
- 在选择自动缩放组协议和端口时，请确保您的服务器监听这些协议和端口，并在服务组中绑定正确的监视器。默认情况下，使用 TCP 监视器。
- 对于类型为自动缩放的 SSL 协议，创建云配置文件后，由于缺少证书，负载平衡虚拟服务器或服务组似乎已关闭。可以手动将证书绑定到虚拟服务器或服务组。
- 选择正常并在“延迟”字段中指定超时值以正常移除 AutoScale 服务器。此选项启动缩小事件。VPX 实例不会立即删除服务器，而是将其中一台服务器标记为要进行正常删除。在此期间，VPX 实例不允许与此服务器建立新连接。在超时发生之前，将为现有连接提供服务。超时后，VPX 实例将删除服务器。

  如果不选择“正常”选项，则负载下降后会立即移除 AutoScale 组中的服务器。这可能会导致现有已连接客户端的服务中断。

创建云配置文件后，将创建一个 NetScaler 负载平衡虚拟服务器和一个以成员作为自动扩展组服务器的服务组。您的后端服务器必须能够通过 VPX 实例上配置的 SNIP 进行访问。



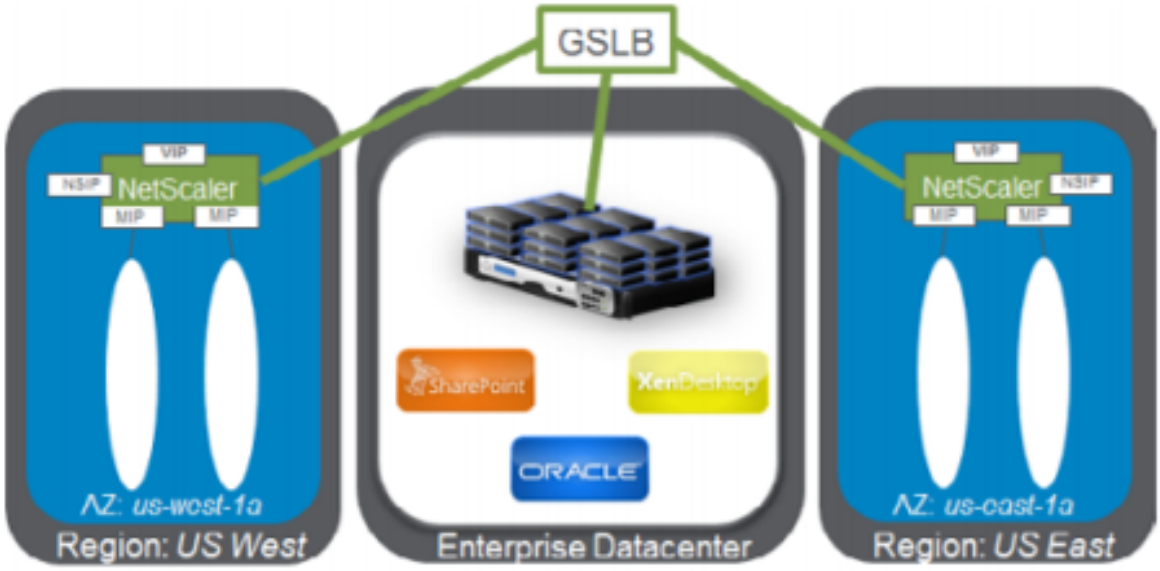
注意：

- 要在 AWS 控制台上查看与 Autoscale 相关的信息，请转到 **EC2** > **Dashboard**（控制板）> **Auto Scaling** > **Auto Scaling Group**（Auto Scaling 组）。
- 您可以在 AWS 中使用相同的自动扩展组 (ASG) 为不同的服务（使用不同的端口）创建不同的云配置文件。因此，NetScaler VPX 实例支持公有云中具有相同自动缩放组的多个服务。

在 **AWS** 上部署 **NetScaler GSLB**

October 17, 2024

在 AWS 上为 NetScaler 设置 GSLB 主要包括配置 NetScaler 以对位于 NetScaler 所属的 VPC 以外的服务器的流量进行负载平衡，例如在不同可用区域的另一个 VPC 内或本地数据中心内。



DBS 概述

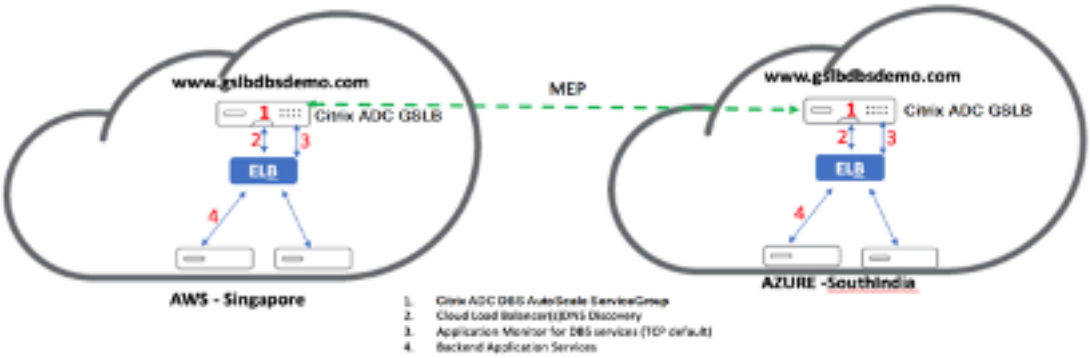
NetScaler GSLB 支持使用基于域名的服务 (DBS) 用于云负载均衡器，允许使用云负载均衡器解决方案自动发现动态云服务。此配置允许 NetScaler 在主动-主动环境中实现全局服务器负载平衡基于域名的服务 (GSLB DBS)。DBS 允许通过 DNS 发现扩展 AWS 环境中的后端资源。

本节介绍了 NetScaler 在 AWS AutoScaling 环境中的集成。本文档的最后一部分详细介绍了在特定于 AWS 区域的两个不同可用区 (AZ) 之间设置 NetScaler ADC 的 HA 对的能力。

使用 ELB 的 DBS

GSLB DBS 利用用户弹性负载平衡器 (ELB) 的 FQDN 动态更新 GSLB 服务组，以包括在 AWS 中创建和删除的后端服务器。AWS 中的后端服务器或实例可以配置为根据网络需求或 CPU 使用率进行扩展。要配置此功能，请将 NetScaler 指向 ELB，以动态路由到 AWS 中的不同服务器，而不必每次在 AWS 中创建和删除实例时都手动更新 NetScaler。GSLB 服务组的 NetScaler DBS 功能使用 DNS 感知服务发现来确定 Autoscale 组中标识的 DBS 命名空间的成员服务资源。

NetScaler GSLB DBS 与云负载均衡器的自动缩放组件：



配置 AWS 组件

安全组

> 注意：
>
> 我们建议您为 ELB、NetScaler GSLB 实例和 Linux 实例创建不同的安全组，因为每个实体所需的规则集不同。为简洁起见，此示例具有整合的安全组配置。

要确保虚拟防火墙的配置正确，请参阅 您的 VPC 的安全组。

1. 登录到用户 **AWS** 资源组，然后导航到 **EC2 >** 网络和安全 **>** 安全组。
2. 单击创建安全组并提供名称和描述。该安全组包括 NetScaler 和 Linux 后端网络服务器。

3. 添加以下屏幕截图中的入站端口规则。

> 注意：
>
> 建议限制源 IP 访问以实现粒度强化。有关更多信息，请参阅 Web 服务器规则。

1. Amazon Linux 后端网络服务

   a) 登录到用户 **AWS** 资源组，然后导航到 **EC2 >** 实例。

   b) 使用以下详细信息单击“启动实例”以配置 **Amazon Linux** 实例。

   输入有关在此实例上设置 Web 服务器或后端服务的详细信息。

2. NetScaler 配置

   a) 登录到用户 **AWS** 资源组，然后导航到 **EC2 >** 实例。

   b) 单击启动实例，然后使用以下详细信息配置 **Amazon AMI** 实例。

3. 弹性 IP 配置

> 注意：
>
> 如有必要，也可以使 NetScaler 使用单个弹性 IP 运行，以降低成本，方法是没有 NSIP 的公有 IP。相反，除了 GSLB 站点 IP 和 ADNS IP 之外，还可以在 SNIP 上附加一个弹性 IP，该弹性 IP 可以覆盖对盒子的管理访问权限。

```
1. 登录到用户**AWS 资源组**，然后导航到**EC2 > 网络与安全 > 弹性 IP**
   。

1. 单击**分配新地址**以创建弹性 IP 地址。

1. 将弹性 IP 配置为指向在 AWS 中运行 NetScaler 实例的用户。

1. 配置第二个弹性 IP，然后再次将其指向运行 NetScaler 实例的用户。
```

1. 弹性负载平衡器

   a) 登录到用户 **AWS** 资源组，然后导航到 **EC2 >** 负载平衡 **>** 负载平衡器。

   b) 单击创建负载平衡器以配置传统负载平衡器。

   用户弹性负载平衡器允许用户对其后端 Amazon Linux 实例进行负载平衡，同时还能够对根据需求启动的其他实例进行负载平衡。

配置基于域名的全局服务器负载平衡服务

有关流量管理配置，请参阅 配置基于 NetScaler GSLB 域的服务。

部署类型

三网卡部署

- 典型部署
  - GSLB 样书
  - 使用 ADM
  - 使用 GSLB（带域名注册的 Route53）
  - 许可-汇集/市场
- 使用案例
  - 采用三网卡部署，实现数据和管理流量的真正隔离。
  - 三 NIC 部署还可以提高 ADC 的规模和性能。
  - 三 NIC 部署用于吞吐量通常为 1 Gbps 或更高的网络应用，建议采用三 NIC 部署。

CFT 部署

如果客户正在自定义部署或者正在自动执行部署，他们将使用 CloudFormation 模板进行部署。

部署步骤

以下是部署步骤：

1. GSLB 的三个 NIC 部署
2. 许可
3. 部署选项

GSLB 的三个 **NIC** 部署　NetScaler VPX 实例在 AWS 市场中以 Amazon Machine Image (AMI) 的形式提供，也可以作为弹性计算云 (EC2) 实例在 AWS VPC 中启动。在 NetScaler VPX 上允许作为 AMI 支持的最低 EC2 实例类型为 m4.large。NetScaler VPX AMI 实例至少需要 2 个虚拟 CPU 和 2 GB 内存。从 AWS VPC 内启动的 EC2 实例还可以提供多个接口，每个接口有多个 IP 地址，以及 VPX 配置所需的公用和专用 IP 地址。每个 VPX 实例至少需要三个 IP 子网：

- 管理子网
- 面向客户端的子网 (VIP)
- 面向后端的子网 (SNIP)

NetScaler 建议在 AWS 上安装的标准 VPX 实例使用三个网络接口。

AWS 目前只对在 AWS VPC 中运行的实例提供多 IP 功能。VPC 中的 VPX 实例可用于对 EC2 实例中运行的服务器实现负载平衡。Amazon VPC 允许用户创建和控制虚拟联网环境，包括他们自己的 IP 地址范围、子网、路由表和网络网关。

> 注意：
>
> 默认情况下，用户可以为每个 AWS 帐户在每个 AWS 区域创建最多 5 个 VPC 实例。用户可以通过在此处提交 Amazon 的申请表来请求更高的 VPC 限制：Amazon VPC 请求。

许可　AWS 上的 NetScaler VPX 实例需要许可证。以下许可选项适用于在 AWS 上运行的 NetScaler VPX 实例：

- 免费（无限制）
- 每小时
- 年度
- 携带您自己的许可证
- 免费试用（所有 NetScaler VPX-AWS 订阅产品在 AWS 市场免费提供 21 天）。

部署选项　用户可以在 AWS 上部署 NetScaler VPX 独立实例。有关更多信息，请参阅在 AWS 上部署 NetScaler VPX 独立实例

适用于混合云和多云部署的 **NetScaler** 全局服务器负载平衡

NetScaler 混合和多云全球服务器负载平衡 (GSLB) 解决方案使用户能够在混合云、多云和本地部署中的多个数据中心之间分配应用流量。NetScaler 混合和多云 GSLB 解决方案可帮助用户在混合或多云环境中管理其负载平衡设置，而无需更改现有设置。此外，如果用户有本地设置，则在完全迁移到云之前，他们可以使用 NetScaler 混合和多云 GSLB 解决方案在云中测试部分服务。例如，用户只能将一小部分流量路由到云，并处理大部分本地流量。NetScaler 混合和多云 GSLB 解决方案还使用户能够通过单个统一的控制台跨地理位置管理和监视 NetScaler 实例。

混合云和多云架构还可以避免“供应商锁定”，并使用不同的基础架构来满足用户、合作伙伴和客户的需求，从而提高企业的整体绩效。借助多云架构，用户可以更好地管理其基础设施成本，因为他们现在只需为他们使用的部分付费。用户还可以更好地扩展其应用程序，因为他们现在可以按需使用基础架构。它还提供了从一个云快速切换到另一个云的能力，以充分利用每个提供商的最佳产品。

NetScaler GSLB 节点处理 DNS 名称解析。这些 GSLB 节点中的任何一个都可以从任何客户端位置接收 DNS 请求。接收 DNS 请求的 GSLB 节点返回配置的负载平衡方法选择的负载平衡器虚拟服务器 IP 地址。指标（站点、网络和持久性指标）使用指标交换协议 (MEP) 在 GSLB 节点之间进行交换，该协议是一种专有的 NetScaler 协议。有关 MEP 协议的更多信息，请参阅配置指标交换协议。

在 GSLB 节点中配置的监视器监视同一数据中心中负载平衡虚拟服务器的运行状况。在父子拓扑中，使用 MEP 交换 GSLB 和 NetScaler 节点之间的指标。但是，在父子拓扑中，在 GSLB 和 NetScaler LB 节点之间配置监视探测器是可选的。

NetScaler 代理支持 NetScaler ADM 与用户数据中心内的托管实例之间的通信。有关 NetScaler 代理及其安装方法的更多信息，请参阅入门。

> 注意：
>
> 本文档做出以下假设：
>
> - 如果用户有现有的负载平衡设置，则它已启动并正在运行。
> - 每个 NetScaler GSLB 节点上都配置了 SNIP 地址或 GSLB 站点 IP 地址。在与其他数据中心交换指标时，此 IP 地址用作数据中心源 IP 地址。
> - 每个 NetScaler GSLB 实例上都配置了 ADNS 或 ADNS-TCP 服务以接收 DNS 流量。
> - 云服务提供程序中配置了所需的防火墙和安全组。

安全组配置

用户必须在云服务提供商中设置所需的防火墙/安全组配置。有关 AWS 安全功能的更多信息，请参阅 AWS/Documentation/Amazon VPC/User Guide/Security。

此外，在 GSLB 节点上，用户必须为 ADNS 服务/DNS 服务器 IP 地址打开端口 53，为 GSLB 站点 IP 地址打开端口 3009 以进行 MEP 流量交换。在负载平衡节点上，用户必须打开相应的端口才能接收应用程序流量。例如，用户必须打开端口 80 以接收 HTTP 流量，打开端口 443 以接收 HTTPS 流量。打开端口 443 以进行 NetScaler 代理和 NetScaler ADM 之间的 NITRO 通信。

对于动态往返时间 GSLB 方法，用户必须打开端口 53 以允许 UDP 和 TCP 探测，具体取决于配置的 LDNS 探测类型。UDP 或 TCP 探测使用其中一个 SNIP 启动，因此必须为绑定到服务器端子网的安全组执行此设置。

NetScaler 混合和多云 GSLB 解决方案的功能

本节介绍了 NetScaler 混合和多云 GSLB 解决方案的某些功能。

与其他负载平衡解决方案的兼容性

NetScaler 混合和多云 GSLB 解决方案支持各种负载平衡方案，例如 NetScaler 负载平衡器、NGINX、HAProxy 和其他第三方负载平衡器。

> 注意：
>
> 仅当使用基于邻近度和非指标的 GSLB 方法且未配置父子拓扑时，才支持 NetScaler 以外的负载平衡方案。

GSLB 方法

NetScaler 混合和多云 GSLB 解决方案支持以下 GSLB 方法。

- 基于指标的 GSLB 方法。基于指标的 GSLB 方法通过指标交换协议从其他 NetScaler 节点收集指标。
  - 最少连接：客户端请求路由到活动连接最少的负载平衡器。
  - 最小带宽：客户端请求路由到当前服务的流量最少的负载平衡器。
  - 最少的数据包：客户端请求被路由到过去 14 秒内收到最少数据包的负载平衡器。
- 基于非指标的 GSLB 方法
  - 循环调度：客户端请求被路由到负载平衡器列表顶部的负载平衡器的 IP 地址。然后，该负载平衡器移至列表底部。
  - 源 IP 哈希：此方法使用客户端 IP 地址的哈希值来选择负载平衡器。
- 基于邻近度的 GSLB 方法
  - 静态邻近性：客户端请求路由到最接近客户端 IP 地址的负载平衡器。
  - 往返时间 (RTT)：此方法使用 RTT 值（客户端本地 DNS 服务器与数据中心之间连接的时间延迟）来选择性能最佳的负载平衡器的 IP 地址。

有关负载平衡方法的更多信息，请参阅 负载平衡算法。

GSLB 拓扑

NetScaler 混合和多云 GSLB 解决方案支持主动-被动拓扑和父子拓扑。

- 主动-被动拓扑-提供灾难恢复，并通过防范故障点确保应用程序的持续可用性。如果主数据中心出现故障，则被动数据中心将开始运行。有关 GSLB 主动-被动拓扑的更多信息，请参阅 配置 GSLB 以进行灾难恢复。
- 父子拓扑 - 如果客户使用基于度量的 GSLB 方法配置 GSLB 和负载平衡节点，并且负载平衡节点部署在不同的 NetScaler 实例上，则可以使用该拓扑。在父子拓扑中，LB 节点（子站点）必须是 NetScaler 设备，因为父站点和子站点之间的衡量指标交换是通过衡量指标交换协议 (MEP) 进行的。

有关父子拓扑的更多信息，请参阅 使用 MEP 协议进行父子拓扑部署。

IPv6 支持

NetScaler 混合和多云 GSLB 解决方案还支持 IPv6。

监视

NetScaler 混合云和多云 GSLB 解决方案支持内置监视器，并可选择启用安全连接。但是，如果 LB 和 GSLB 配置位于同一 NetScaler 实例上，或者如果使用父子拓扑，则配置监视器是可选的。

持久性

NetScaler 混合和多云 GSLB 解决方案支持以下内容：

- 基于源 IP 的持久性会话，因此，如果来自同一客户端的多个请求到达配置的超时窗口，则会将这些请求定向到同一服务。如果超时值在客户端发送另一个请求之前过期，则会放弃会话，并使用配置的负载平衡算法为客户端的下一个请求选择新服务器。
- 溢出持久性，以便备份虚拟服务器继续处理其收到的请求，即使在主服务器上的负载低于阈值之后也是如此。有关更多信息，请参阅 配置溢出。
- 站点持久化，这样 GSLB 节点可以选择一个数据中心来处理客户端请求，并将所选数据中心的 IP 地址转发给所有后续的 DNS 请求。如果配置的持久性适用于处于关闭状态的站点，则 GSLB 节点使用 GSLB 方法选择新站点，新站点将变为永久站点，以备来自客户端的后续请求。

使用 **NetScaler ADM** 样本进行配置

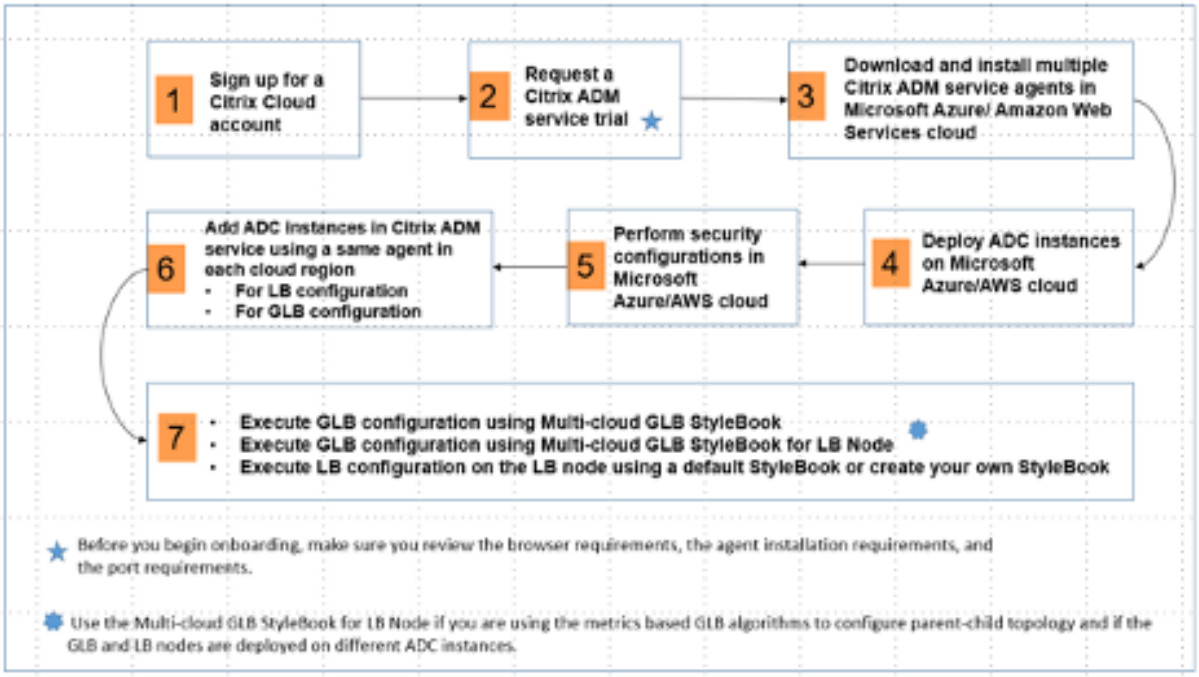
客户可以使用 NetScaler ADM 上的默认多云 GSLB StyleBook 来配置具有混合和多云 GSLB 配置的 NetScaler 实例。

客户可以使用默认的多云 GSLB 样本作为负载平衡节点样本来配置 NetScaler 负载平衡节点，这些节点是父子拓扑中处理应用程序流量的子站点。仅当用户想要在父子拓扑中配置负载平衡节点时才使用此样本。但是，必须使用此样书单独配置每个 LB 节点。

NetScaler 混合和多云 **GSLB** 解决方案配置的工作流程

客户可以使用 NetScaler ADM 上附带的多云 GSLB StyleBook 来配置具有混合和多云 GSLB 配置的 NetScaler 实例。

下图显示了配置 NetScaler 混合和多云 GSLB 解决方案的工作流程。工作流逻辑示意图中的步骤将在逻辑示意图之后进行更详细的解释。



以云管理员身份执行以下任务：

1. 注册 NetScaler Cloud 帐户。

   要开始使用 NetScaler ADM，请创建一个 NetScaler Cloud 公司帐户或加入公司某人创建的现有帐户。

2. 用户登录到 NetScaler 云后，单击 **NetScaler Application Delivery Management** 图块上的“管理”以首次设置 ADM 服务。

3. 下载并安装多个 NetScaler ADM 服务代理。

   用户必须在其网络环境中安装和配置 NetScaler ADM 服务代理，以实现 NetScaler ADM 与其数据中心或云中的托管实例之间的通信。在每个区域安装代理，以便他们可以在托管实例上配置 LB 和 GSLB 配置。LB 和 GSLB 配置可以共享一个代理。有关上述三个任务的更多信息，请参阅 入门。

4. 在 Microsoft AWS 云/本地数据中心上部署负载平衡器。

   根据用户在云端和本地部署的负载平衡器的类型，相应地配置它们。例如，用户可以在 Amazon Web Services (AWS) 虚拟专用云和本地数据中心中预配 NetScaler VPX 实例。通过创建虚拟机和配置其他资源，将 NetScaler 实例配置为在独立模式下充当 LB 或 GSLB 节点。有关如何部署 NetScaler VPX 实例的详细信息，请参阅以下文档：

   - AWS 上的 NetScaler VPX。
   - 配置 NetScaler VPX 独立实例。

5. 执行安全配置。

   在 ARM 和 AWS 中配置网络安全组和网络 ACL，以控制用户实例和子网的入站和出站流量。

6. 在 NetScaler ADM 中添加 NetScaler 实例。

   NetScaler 实例是用户想要从 NetScaler ADM 发现、管理和监控的网络设备或虚拟设备。要管理和监视这些实例，用户必须将实例添加到服务中并注册 LB（如果用户使用 NetScaler for LB）和 GSLB 实例。有关如何在 NetScaler ADM 中添加 NetScaler 实例的更多信息，请参阅入门

7. 使用默认的 NetScaler ADM StyleBooks 实现 GSLB 和 LB 配置。

   - 使用多云 GSLB StyleBook 在选定的 GSLB NetScaler 实例上运行 GSLB 配置。
   - 实现 负载平衡配置。（如果用户已经在托管实例上进行了 LB 配置，则可以跳过此步骤。）用户可以通过以下两种方式之一在 NetScaler 实例上配置负载均衡器：
   - 手动配置实例以实现应用程序的负载平衡。有关如何手动配置实例的更多信息，请参阅 设置基本负载平衡。
   - 使用样书。用户可以使用其中一个 NetScaler ADM 样本（HTTP/SSL 负载平衡样本或 HTTP/SSL 负载平衡（带监视器）样本）在选定的 NetScaler 实例上创建负载平衡器配置。用户还可以创建自己的样书。有关样书的更多信息，请参阅 样书。

8. 在以下任何情况下，使用多云 GSLB StyleBook for LB Node 配置 GSLB 父子拓扑：

   - 如果用户使用基于度量的 GSLB 算法（最少数据包、最少连接、最少带宽）来配置 GSLB 和负载平衡节点，并且负载平衡节点部署在不同的 NetScaler 实例上。
   - 如果需要站点持久性。

使用 **StyleBooks** 在 **NetScaler** 负载平衡节点上配置 **GSLB**

如果客户使用基于度量的 GSLB 算法（最少数据包、最少连接、最少带宽）来配置 GSLB 和负载平衡节点，并且负载平衡节点部署在不同的 NetScaler 实例上，则他们可以使用多云 **GSLB** 样本用于 **LB** 节点。

用户还可以使用此样书为现有父站点配置更多子站点。此样书一次配置一个子站点。因此，从此样书中创建的配置（配置包）与创建子站点的数量一样多。样书将 GSLB 配置应用于子站点。用户最多可以配置 1024 个子站点。

> 注意：
>
> 使用多云 GSLB StyleBook 配置父站点。

此样书作出以下假设：

- 配置了 SNIP 地址或 GSLB 站点 IP 地址。
- 云服务提供程序中配置了所需的防火墙和安全组。

使用多云 **GSLB** 样本为 **LB** 节点配置父子拓扑中的子站点

1. 导航到“应用程序”**>**“配置”**>**“新建”。

2. 导航到“应用程序”>“配置”，然后单击“新建”。

   样书显示为用户界面页面，用户可以在该页面上输入此样书中定义的所有参数的值。

> 注意：
>
> 在本文档中，“数据中心”和“站点”这两个术语可以互换使用。

1. 设置以下参数：

   - 应用程序名称。输入部署在要为其创建子站点的 GSLB 站点上的 GSLB 应用程序的名称。
   - 协议。从下拉列表框中选择已部署应用程序的应用程序协议。
   - **LB** 运行状况检查（可选）
   - 运行状况检查类型。从下拉列表框中，选择用于检查代表站点上应用程序的负载平衡器 VIP 地址运行状况的探测类型。
   - 安全模式。（可选）如果需要基于 SSL 的运行状况检查，请选择“是”以启用此参数。
   - **HTTP** 请求。（可选）如果用户选择 HTTP 作为运行状况检查类型，请输入用于探测 VIP 地址的完整 HTTP 请求。
   - **HTTP** 状态响应代码列表。（可选）如果用户选择 HTTP 作为运行状况检查类型，请输入在 VIP 运行正常时响应 HTTP 请求时应使用的 HTTP 状态代码列表。

2. 配置父站点。

   - 提供您要在其中创建子站点（LB 节点）的父站点（GSLB 节点）的详细信息。
     - 站点名称。输入站点的名称。
     - 网站 **IP** 地址。输入父站点与其他站点交换指标时用作其源 IP 地址的 IP 地址。假定已在每个站点的 GSLB 节点上配置了此 IP 地址。
     - 站点公有 **IP** 地址。（可选）输入用于交换指标的子站点的公有 IP 地址（如果该站点的 IP 地址是 NAT 的）。

3. 配置子站点。

   - 提供子站点的详细信息。
     - 站点名称。输入父站点的名称。
     - 网站 **IP** 地址。输入子站点的 IP 地址。在这里，使用配置为子站点的 NetScaler 节点的专用 IP 地址或 SNIP。
     - 站点公有 **IP** 地址。（可选）输入用于交换指标的父站点的公有 IP 地址（如果该站点的 IP 地址是 NAT 的）。

4. 配置活动的 GSLB 服务（可选）

- 仅在 LB 虚拟服务器 IP 地址不是公有 IP 地址时才配置活动的 GSLB 服务。本部分允许用户在部署应用程序的站点上配置本地 GSLB 服务列表。
  - 服务 **IP**。输入此站点上负载平衡虚拟服务器的 IP 地址。
  - 服务公有 **IP** 地址。如果虚拟 IP 地址是专用的，并且具有 NAT 的公有 IP 地址，请指定公有 IP 地址。
  - 服务端口。在此站点上输入 GSLB 服务的端口。
  - 站点名称。输入 GSLB 服务所在站点的名称。

5. 单击“目标实例”，然后在要部署 GSLB 配置的每个站点上选择配置为 GSLB 实例的 NetScaler 实例。
6. 单击“创建”在选定的 NetScaler 实例（负载平衡节点）上创建 LB 配置。用户还可以单击 **Dry Run** 来检查将在目标实例中创建的对象。用户创建的样书配置将显示在“配置”页面的配置列表中。用户可以使用 NetScaler ADM GUI 检查、更新或删除此配置。

CloudFormation 模板

NetScaler VPX 在 AWS Marketplace 中作为 Amazon Machine Images (AMI) 提供。在使用 CloudFormation 模板在 AWS 中预置 NetScaler VPX 之前，AWS 用户必须接受条款并订阅 AWS Marketplace 产品。市场中的每个版本的 NetScaler VPX 都需要此步骤。

CloudFormation 存储库中的每个模板都有描述模板用法和架构的并置文档。这些模板试图编纂 NetScaler VPX 的推荐部署架构，或向用户介绍 NetScaler，或演示特定的功能、版本或选项。用户可以重复使用、修改或增强模板，以满足其特定的生产和测试需求。除了创建 IAM 角色的权限外，大多数模板还需要完全的 EC2 权限。

CloudFormation 模板包含特定版本 NetScaler VPX（例如，版本 12.0-56.20）和版本（例如，NetScaler VPX 铂金版——10 Mbps）或 NetScaler BYOL 的 AMI ID。要将不同版本/版本的 NetScaler VPX 与 CloudFormation 模板一起使用，需要用户编辑模板并替换 AMI ID。

最新的 NetScaler AWS-AMI-ID 位于此处：NetScaler AWS CloudFormation 大师。

CFT 三 NIC 部署

此模板部署一个 VPC，其中包含 2 个可用区的 3 个子网（管理、客户端、服务器）。它部署了一个 Internet 网关，在公有子网上有一条默认路由。此模板还使用两个 NetScaler 实例跨可用区创建高可用性对：3 个 ENI 与主节点上的 3 个 VPC 子网（管理、客户端、服务器）关联，3 个 ENI 与 3 个 VPC 子网（管理、客户端、服务器）关联在辅助子网上。此 CFT 创建的所有资源名称都以堆栈名称的 tagName 作为前缀。

CloudFormation 模板的输出包括：

- PrimaryCitrixADCManagementURL - 主 VPX 的管理 GUI 的 HTTPS URL（使用自签名证书）
- PrimaryCitrixADCManagementURL2 - 主 VPX 的管理 GUI 的 HTTP URL
- PrimaryCitrixADCInstanceID - 新创建的主要 VPX 实例的实例 ID

- PrimaryCitrixADCPublicVIP - 与 VIP 关联的主要 VPX 实例的弹性 IP 地址
- PrimaryCitrixADCPrivateNSIP - 用于管理主 VPX 的专用 IP (NS IP)
- PrimaryCitrixADCPublicNSIP - 用于管理主 VPX 的公用 IP (NS IP)
- PrimaryCitrixADCPrivateVIP - 与 VIP 关联的主要 VPX 实例的专用 IP 地址
- PrimaryCitrixADCSNIP - 与 SNIP 关联的主要 VPX 实例的专用 IP 地址
- SecondaryCitrixADCManagementURL - 辅助 VPX 的管理 GUI 的 HTTPS URL（使用自签名证书）
- SecondaryCitrixADCManagementURL2 - 辅助 VPX 的管理 GUI 的 HTTP URL
- SecondaryCitrixADCInstanceID - 新创建的辅助 VPX 实例的实例 ID
- SecondaryCitrixADCPrivateNSIP - 用于管理辅助 VPX 的专用 IP (NS IP)
- SecondaryCitrixADCPublicNSIP - 用于管理辅助 VPX 的公用 IP (NS IP)
- SecondaryCitrixADCPrivateVIP - 与 VIP 关联的辅助 VPX 实例的专用 IP 地址
- SecondaryCitrixADCSNIP - 与 SNIP 关联的辅助 VPX 实例的专用 IP 地址
- 安全组-VPX 所属的安全组 ID

向 CFT 提供输入时，CFT 中针对任何参数的 * 都表示它是必填字段。例如，`VPC ID*` 是必填字段。

必须满足以下先决条件。CloudFormation 模板需要足够的权限来创建 IAM 角色，这超出了普通的 EC2 完全权限。使用此模板的用户还需要接受条款并订阅 AWS Marketplace 产品，然后才能使用此 CloudFormation 模板。

还应存在以下内容：

- Key Pair（密钥对）
- 3 个未分配的 EIP
- 主要管理层
- 客户端 VIP
- 二级管理

有关在 AWS 上配置 NetScaler VPX 实例的更多信息，用户可以访问：在 AWS 上配置 NetScaler VPX 实例。

有关如何使用 StyleBooks 配置 GSLB 的信息，请访问 使用 StyleBooks 配置 GSLB

灾难恢复 **(DR)**

灾害是由自然灾害或人为事件引起的业务功能突然中断。灾难会影响数据中心的运营，之后必须完全重建和恢复灾难现场丢失的资源和数据。数据中心中的数据丢失或停机至关重要，并使业务连续性崩溃。

如今，客户面临的挑战之一是决定将灾难恢复站点放置在何处。无论任何底层基础架构或网络故障如何，企业都在寻求一致性和性能。

要部署 GSLB 进行灾难恢复，请参阅 在 AWS 上部署 NetScaler VPX 独立实例

其他资源

NetScaler ADM GSLB 用于混合和多云部署。

将 **NetScaler VPX** 实例配置为使用 **SR-IOV** 网络接口

October 17, 2024

> 注意：
>
> 从 NetScaler 版本 12.0 57.19 起，即可在高可用性设置中支持 SR-IOV 接口。

在 AWS 上创建 NetScaler VPX 实例后，您可以使用 AWS CLI 将虚拟设备配置为使用 SR-IOV 网络接口。

在所有 NetScaler VPX 型号中，除 3G 和 5G 的 NetScaler VPX AWS Marketplace 版本外，在网络接口的默认配置中均未启用 SR-IOV。

在开始配置之前，请阅读以下主题：

- 必备条件
- 局限性与用法指南

本节包括以下主题：

- 将接口类型更改为 SR-IOV
- 在高可用性设置中配置 SR-IOV

将接口类型更改为 **SR-IOV**

您可以运行 show interface summary 命令以检查网络接口的默认配置。

示例 **1**：以下 CLI 屏幕截图显示了网络接口的配置，其中 SR-IOV 在 3G 和 5G 的 NetScaler VPX AWS Marketplace 版本上默认启用 SR-IOV。

```
> show interface summary
-------------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
1       1/1       1500       0a:1e:2e:17:a2:37    Intel 82599 10G VF Interface
2       LO/1      1500       0a:1e:2e:17:a2:37    Netscaler Loopback interface
 Done
```

示例 **2**：以下 CLI 屏幕截图显示了未启用 SR-IOV 的网络接口的默认配置。


```
 Done
> sh int s
-------------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
1     1/1        1500       12:fc:04:c5:d0:12  NetScaler Virtual Interface
2     LO/1       1500       12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

有关将接口类型更改为 SR-IOV 的详细信息，请参阅 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

将接口类型更改为 **SR-IOV**

1. 关闭 AWS 上运行的 NetScaler VPX 实例。
2. 要在网络接口上启用 SR-IOV，请在 AWS CLI 中键入以下命令。

   ```
   $ aws ec2 modify-instance-attribute --instance-id \\&#060;instance
   \\_id\\&#062; --sriov-net-support simple
   ```

3. 要检查是否已启用 SR-IOV，请在 AWS CLI 中键入以下命令。

   ```
   $ aws ec2 describe-instance-attribute --instance-id \\&#060;
   instance\\_id\\&#062; --attribute sriovNetSupport
   ```

   示例 **3**：使用 AWS CLI 将网络接口类型更改为 SR-IOV。

   ```
   aws ec2 modify-instance-attribute --instance-id i-008c1230aaf303bee --sriov-net-support simple
   aws ec2 describe-instance-attribute --instance-id   i-008c1230aaf303bee  --attribute sriovNetSupport
   {
       "InstanceId": "i-008c1230aaf303bee",
       "SriovNetSupport": {
           "Value": "simple"
       }
   }
   ```

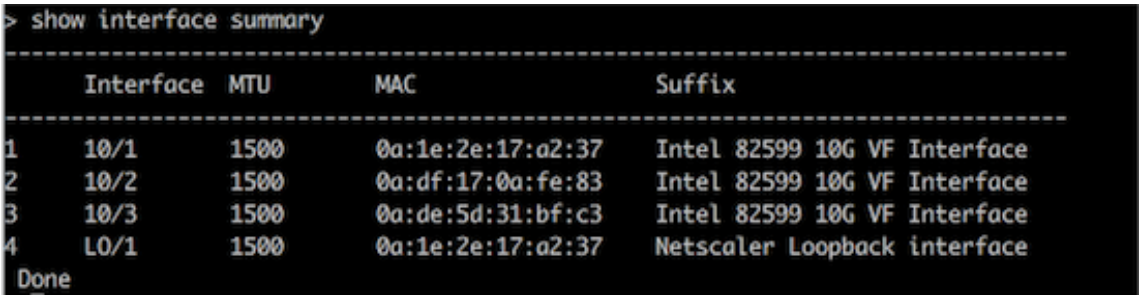
   如果未启用 SR-IOV，则会缺少 SriovNetSupport 值。

   示例 **4**：在以下示例中，未启用 SR-IOV 支持。

   ```
   {
       "InstanceId": "i-0c3e84cfa65b04cc8",
       "SriovNetSupport": {}
   }
   ```

4. 打开 VPX 实例。要查看网络接口的更改状态，请在 CLI 中键入“show interface summary”。

   示例 **5**：下面的屏幕截图显示了启用了 SR-IOV 的网络接口。接口 10/1、10/2 和 10/3 启用了 SR-IOV。



这些步骤即是配置 VPX 实例以使用 SR-IOV 网络接口的过程。

在高可用性设置中配置 **SR-IOV**

NetScaler 版本 12.0 版本版本 57.19 及更高版本的 SR-IOV 接口支持高可用性。

如果高可用性设置是手动部署的，或者使用适用于 NetScaler 版本 12.0 56.20 及更低版本的 Citrix CloudFormation 模板进行部署，则与高可用性设置关联的 IAM 角色必须具有以下权限：

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- sns:*
- sqs:*
- IAM:SimulatePrincipalPolicy
- IAM:GetRole

默认情况下，适用于 NetScaler 版本 12.0 57.19 的 Citrix CloudFormation 模板会自动为 IAM 角色添加所需的权限。

> 注意：
>
> 使用 SR-IOV 接口的高可用性设置需要约 100 秒的停机时间。

相关资源：

有关 IAM 角色的更多信息，请参阅 AWS 文档。

将 **NetScaler VPX** 实例配置为在 **AWS ENA** 中使用增强型联网

October 17, 2024

在 AWS 上创建 NetScaler VPX 实例后，您可以通过使用 AWS CLI 将虚拟设备配置为将 增强联网 与 AWS 弹性网络适配器 (ENA)结合使用。

与 AWS ENA 配合使用时，增强的网络连接可提供更高的带宽、更高的每秒数据包 (PPS) 性能，并持续降低实例间延迟。

在开始配置之前，请阅读以下主题：

- 必备条件
- 局限性与用法指南

启用了 ENA 的实例支持以下高可用性配置：

- 专用 IP 地址可以在同一可用性区域内移动。
- 弹性 IP 地址可以跨可用性区域移动。

在 **AWS** 上升级 **NetScaler VPX** 实例

October 17, 2024

可以升级 AWS 上运行的 NetScaler VPX 的 EC2 实例类型、吞吐量、软件版本和系统软件。对于某些类型的升级，Citrix 建议使用高可用性配置方法以将停机时间缩至最短。

> 注意：
>
> - 与 NetScaler VPX AMI（包括实用程序许可证和客户许可证）对应的 NetScaler 软件发行版 10.1.e-124.1308.e 或更高版本不支持 M1 和 M2 实例系列。
> - 由于 VPX 实例支持发生变化，因此，不支持从 10.1.e-124 或更高版本的发行版降级到 10.1.123.x 或更低版本。
> - 大部分升级不需要启动新 AMI，并且可以在当前的 NetScaler AMI 实例上完成升级。如果您需要升级到新 NetScaler AMI 实例，请使用高可用性配置方法。

在 **AWS** 上更改 **NetScaler VPX** 实例的 **EC2** 实例类型

如果您的 NetScaler VPX 实例运行发行版 10.1.e-124.1308.e 或更高版本，则可以从 AWS 控制台更改 EC2 实例类型，如下所示：

1. 停止 VPX 实例。

2. 从 AWS 控制台更改 EC2 实例类型。
3. 启动实例。

除非您需要将 EC2 实例类型更改为 M3，否则也可以使用上面的步骤来更改 10.1.e-124.1308.e 之前的发行版的实例类型。在这种情况下，您必须首先按照标准 NetScaler 升级程序（见）将 NetScaler 软件升级到 10.1.e-124 或更高版本，然后按照上述步骤操作。

在 **AWS** 上升级 **NetScaler VPX** 实例的吞吐量或软件版本

升级软件版本（例如从 Standard Edition 升级到 Premium Edition）或吞吐量（例如从 200 Mbps 升级到 1000 Mbps）的方法取决于实例的许可证。

使用客户许可证（自带许可证）

如果您使用的是客户许可证，则可以从 Citrix Web 站点购买并下载新许可证，然后在 VPX 实例上安装该许可证。有关从 Citrix Web 站点下载并安装许可证的详细信息，请参阅“VPX Licensing Guide”《VPX 许可指南》。

使用实用程序许可证（实用程序许可证，按小时收费）

AWS 不支持直接升级收费实例。要升级收费 NetScaler VPX 实例的软件版本或吞吐量，请启动配备所需许可证和容量的新 AMI，并将旧实例配置迁移到新实例。这可以通过使用 NetScaler 高可用性配置来实现，如本页中的 [使用 NetScaler 高可用性配置升级到新的 NetScaler AMI 实例] (#upgrade-to-a-new-citrix-adc-ami-instance-by-using-a-citrix-adc-high-availability-configuration) 小节中所述。

在 **AWS** 上升级 **NetScaler VPX** 实例的系统软件

如果您需要升级运行 10.1.e-124.1308.e 或更高版本的 VPX 实例，请按照升级和降级 NetScaler 设备中的标准 NetScaler 升级过程进行操作。

如果您需要将运行版本低于 10.1.e-124.1308.e 的发行版的 VPX 实例升级到 10.1.e-124.1308.e 或更高版本，请先升级系统软件，然后将实例类型更改为 M3，如下所示：

1. 停止 VPX 实例。
2. 从 AWS 控制台更改 EC2 实例类型。
3. 启动实例。

使用 **NetScaler** 高可用性配置升级到新的 **NetScaler AMI** 实例

要使用高可用性方法升级到新 NetScaler AMI 实例，请执行以下任务：

- 从 AWS marketplace 中创建一个具有所需的 EC2 实例类型、软件版本、吞吐量或软件发行版的新实例。
- 在旧实例（待升级）与新实例之间配置高可用性。在旧实例与新实例之间配置高可用性之后，旧实例中的配置将同步到新实例。
- 强制高可用性从旧实例故障转移到新实例。因此，新实例将成为主实例，并开始接收流量。
- 在 AWS 中停止、重新配置或删除旧实例。

必备条件和注意事项

- 确保您了解 AWS 上两个 NetScaler VPX 实例之间的高可用性是如何工作的。有关 AWS 上两个 NetScaler VPX 实例之间的高可用性配置的更多信息，请参阅 在 AWS 上部署高可用性对。
- 必须在与旧实例相同的可用性区域中创建新实例，以便具有完全相同的安全组和子网。
- 高可用性设置要求访问密钥和密钥与这两个实例的用户 AWS Identity and Access Management (IAM) 帐户相关联。如果创建 VPX 实例时未使用正确的密钥信息，高可用性设置将失败。有关为 VPX 实例创建 IAM 帐户的更多信息，请参阅 先决条件。
  - 必须使用 EC2 控制台创建新实例。不能使用 AWS 1-click 启动，因为该启动方法不接受访问密钥和密钥作为输入。
  - 新实例必须仅有一个 ENI 接口。

要使用高可用性配置升级 NetScaler VPX 实例，请执行以下步骤：

1. 在旧实例与新实例之间配置高可用性。要在两个 NetScaler VPX 实例之间配置高可用性，请在每个实例的命令提示符处键入：

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   例如：

   在旧实例的命令提示符下，键入：

   ```
   1    add ha node 30 192.0.2.30
   2    Done
   ```

   在新实例的命令提示符下，键入：

   ```
   1    add ha node 10 192.0.2.10
   2    Done
   ```

   请注意以下问题：

   - 在 HA 设置中，旧实例是主节点，新实例是辅助节点。
   - NSIP IP 地址不从旧实例复制到新实例。因此，升级后，您的新实例的管理 IP 地址与以前的 IP 地址不同。
   - 高可用性同步后，新实例的 `nsroot` 帐户密码将设置为旧实例的 nsroot 帐户密码。

   有关 AWS 上两个 NetScaler VPX 实例之间的高可用性配置的更多信息，请参阅 在 AWS 上部署高可用性对。

2. 强制执行高可用性故障转移。要强制在高可用性配置中执行故障转移，请在每个实例的命令提示符下键入以下命令：

```
1   force HA failover
```

由于强制执行了故障转移，因此，旧实例的 ENI 将迁移到新实例，并且流量将流经新实例（新的主节点）。旧实例（新的辅助节点）将重新启动。

如果显示以下警告消息，请键入 N 中止操作：

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

显示该警告消息的原因是两个 VPX 实例的系统软件不兼容高可用性。因此，强制故障转移期间旧实例的配置无法自动同步到新实例。

下面是此问题的解决方法：

a) 在旧实例的 NetScaler shell 提示符下，键入以下命令来创建配置文件的备份（ns.conf）：

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) 从备份配置文件 (ns.conf.bkp) 中删除以下行：

- set ns config -IPAddress <IP> -netmask <MASK>

例如，set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0

c) 将旧实例的备份配置文件（ns.conf.bkp）复制到新实例的 /nsconfig 目录。

d) 在新实例的 NetScaler shell 提示符下，键入以下命令，在新实例上加载旧实例的配置文件（ns.conf.bkp）：

- batch -f /nsconfig/ns.conf.bkp

e) 在新实例上保存配置。

- save conifg

f) 在其中任一节点的命令提示符下，键入以下命令以强制执行故障转移，然后对警告消息键入 Y 以确认强制执行故障转移操作：

- force ha failover

例如：

```
1           > force ha failover
2
3   WARNING]:Force Failover may cause configuration loss, peer
       health not optimum.
```



```
4            Reason(s):
5            HA version mismatch
6            HA heartbeats not seen on some interfaces
7            Please confirm whether you want force-failover (Y/N)?
                Y
```

3. 删除高可用性配置，以便这两个实例不再位于高可用性配置中。请先从辅助节点中删除高可用性配置，然后从主节点中删除高可用性配置。

   要删除两个 NetScaler VPX 实例之间的高可用性配置，请在每个实例的命令提示符下键入以下命令：

```
1        > remove ha node \<nodeID\>
2        >  save config
```

   有关 AWS 上两个 VPX 实例之间的高可用性配置的更多信息，请参阅 在 AWS 上部署高可用性对。

   例如：

在旧实例（新辅助节点）的命令提示符下，键入：

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

在新实例（新主节点）的命令提示符下，键入：

```
1            > remove ha node 10
2              Done
3            > save config
4              Done
```

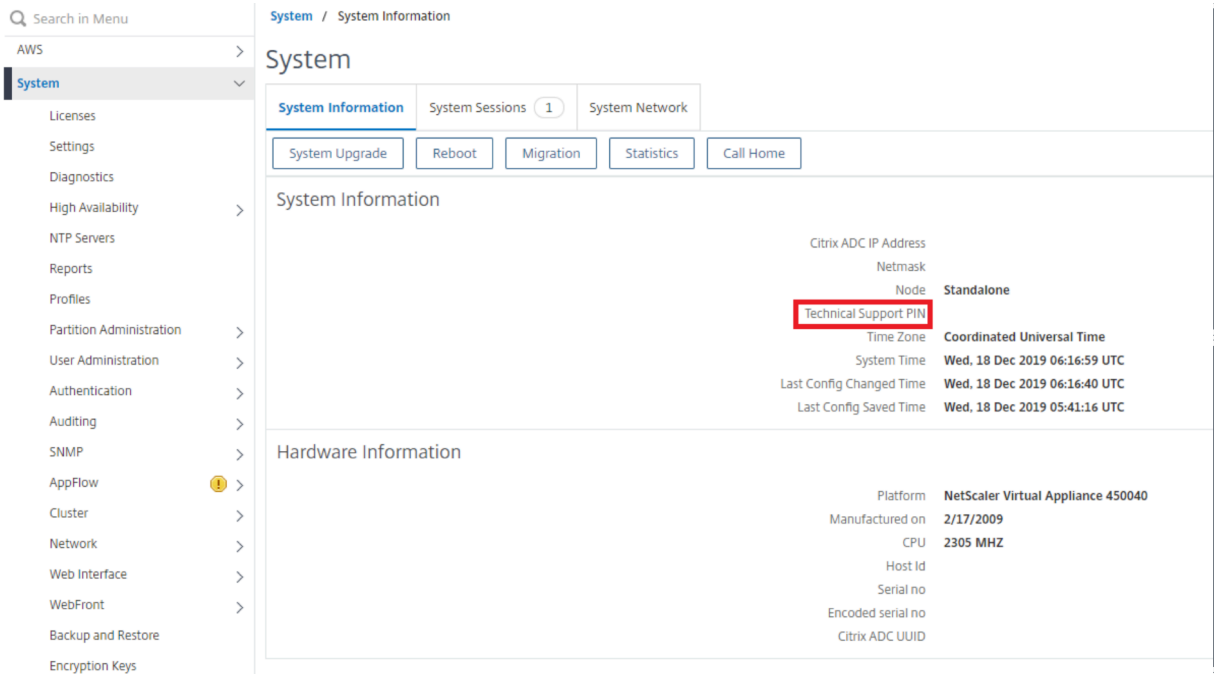
对 **AWS** 上的 **VPX** 实例进行故障排除

October 17, 2024

亚马逊不提供对 NetScaler VPX 实例的控制台访问权限。要进行故障排除，您必须使用 AWS GUI 查看活动日志。只能在建立网络连接的情况下进行调试。要查看实例的系统日志，请在实例上单击鼠标右键并选择“System Log”（系统日志）。

NetScaler 为 AWS 上经过 AWS Marketplace 许可的 NetScaler VPX 实例（按小时计费的公用事业许可证）提供支持。要提交支持案例，请找到您的 AWS 账号和支持 PIN 码，然后致电 NetScaler 支持人员。您还需要提供姓名和电子邮件地址。要查找支持 PIN，请登录 VPX GUI 并导航到 System（系统）页面。

下面是显示了支持 PIN 码的系统页面的示例。



AWS 常见问题解答

October 17, 2024

- **NetScaler VPX** 实例是否支持 **AWS** 中的加密卷?

  加密和解密发生在虚拟机管理程序级别，因此它可以与任何实例无缝协作。有关加密卷的详细信息，请参阅以下 AWS 文档:

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- 在 **AWS** 上预置 **NetScaler VPX** 实例的最佳方法是什么?

  您可以通过以下任何一种方式在 AWS 上预置 NetScaler VPX 实例:

  - AWS Marketplace 中的 AWS CloudFormation 模板 (CFT)
  - NetScaler ADM
  - AWS 快速入门
  - GitHub 中的 Citrix AWS CFT
  - GitHub 中的 Citrix Terraform 脚本
  - GitHub 中的 Citrix Ansible 操作手册
  - AWS EC2 启动工作流

  可以根据您使用的自动化工具选择列出的任何选项。

  有关选项的更多详细信息，请参阅 AWS 上的 NetScaler VPX。

- 如何在 **AWS** 中升级 **NetScaler VPX** 实例?

  要升级 AWS 中的 NetScaler VPX 实例，您可以按照 在 AWS 上升级 NetScaler VPX 实例中的步骤升级系统软件或升级到新的 NetScaler VPX Amazon 系统映像 (AMI)。

  升级 NetScaler VPX 实例的推荐方法是使用 ADM 服务，按照 使用任务升级 NetScaler 实例中的步骤操作。

- **AWS** 中 **NetScaler VPX** 的 **HA** 故障转移时间是多少?

  - 在 AWS 可用区内进行 NetScaler VPX 的 HA 故障转移大约需要 3 秒钟。
  - 在 AWS 可用区之间进行 NetScaler VPX 的 HA 故障转移大约需要 5 秒钟。

- 为提供技术支持 **PIN** 的 **NetScaler VPX** 市场订阅客户提供什么级别的支持?

  默认情况下，“选择软件”服务提供给提供技术支持 PIN 的客户。

- 在 使用弹性 **IP** 部署实现跨不同区域的高可用性中，我们是否需要为每个应用程序创建多个 **IPSets**?

  是。如果有多个应用程序具有多个 VIP 映射到多个 EIP，则需要多个 IPSet。因此，在 HA 故障切换期间，EIP 的所有主要 VIP 映射都更改为辅助（新的主）VIP 映射。

- 为什么在不同区域部署的高可用性中启用 **INC** 模式?

  跨可用区的 HA 对位于不同的网络中。对于 HA 同步，必须不同步网络配置。这是通过在 HA 对上启用 INC 模式来实现的。

- 一个可用区中的 **HA** 节点能否与另一个可用区中的后端服务器通信，前提是这些可用区域中的后端服务器位于同一 **VPC** 中?

  是的，通过 SNIP 添加指向后端服务器子网的额外路由，可以访问同一 VPC 的不同可用区中的子网。例如，如果 AZ1 中 ADC 的 SNIP 子网为 192.168.3.0/24，AZ2 中的后端服务器子网为 192.168.6.0/24，则必须在 AZ1 中的 NetScaler 设备中添加一条名为 192.168.6.0 255.255.255.0 192.168.3.1 的路由。

- 使用弹性 **IP** 跨不同区域的高可用性和 使用私有 **IP** 跨不同区域的高可用性部署可以一起工作吗?

  是的，两种配置都可以应用于同一 HA 对。

- 在 使用私有 **IP** 部署实现跨不同区域的高可用性中，如果 **VPC** 中有多个子网和多个路由表，**HA** 对中的辅助节点如何知道 **HA** 故障转移期间要检查的路由表?

  辅助节点了解主 NIC 并在 VPC 中的所有路由表中进行搜索。

- 在 **AWS** 上使用 **VPX** 的默认映像时，**/var** 分区的大小是多少？如何增加磁盘空间?

  为了保持磁盘映像的小，根磁盘的大小限制为 20 GB。

  如果要增加 /var/core/ 或 /var/crash/ 目录空间，请附加一个额外的磁盘。要增加 /var 的大小，目前必须在将关键内容复制到新磁盘之后，附加一个额外的磁盘并创建指向 /var 的符号链接。

- 激活并分配给 **vCPU** 的数据包引擎有多少?

  数据包引擎 (PE) 受许可 vCPU 数量的限制。NetScaler 守护程序未固定到任何特定的 vCPU，可能在任何非 PE vCPU 上运行。根据 AWS 的说法，C5.9xlarge 是一个具有 72 GB 内存的 36vCPU 实例。使用池化许可，

NetScaler VPX 实例将使用最大数量的 PE 进行部署。在这种情况下，19 个 PE 在核心 1—19 上运行。但是，ADC 管理流程从 CPU 20—31 运行。

- 如何决定适用于 **ADC** 的正确 **AWS** 实例？

  1. 了解您的使用案例和要求，例如吞吐量、PPS、SSL 要求和平均数据包大小。
  2. 选择符合您要求的正确 ADC 产品和许可，例如 VPX 带宽产品或基于 vCPU 的许可。
  3. 根据所选的产品，决定 AWS 实例。

  Example:

  5 Gbps 许可证启用 5 个数据包引擎。因此，vCPU 的要求是 6（管理 5+1）。但是 6 个 vCPU 实例不可用。因此，如果您选择支持 5 Gbps 带宽的网络，8 vCPU 就足以达到该吞吐量。例如，您必须选择 m5.2xlarge 作为 5 Gbps 带宽许可证，才能为 5 Gbps 许可证启用最大 PE 分配。但是，如果您使用的 vCPU 许可证不受吞吐量限制，则使用 m5.xlarge 实例本身可能会获得 5 Gbps 的吞吐量。

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** 中的 **ADC** 是否必须部署三个 **NICS-3** 子网？

  Three NICs-three subnets 是推荐的部署，其中每个部署用于管理、客户端和服务器网络。此部署提供了更好的流量隔离和 VPX 性能。其他可用选项是两个 NICS-2 子网和一个 NIC-One 子网。不建议在 AWS 中让多个 NIC 共享一个子网，例如两个 NIC 一个子网的部署。这种情况可能会导致不对称路由等网络问题。有关更多信息，请参阅 在 AWS 中配置网络接口的最佳实践。

- 为什么 **AWS** 上的 **ENA** 驱动程序始终指示 **1Gbps**（**1/1**）链接速度，而不管实例的网络功能如何？

  无论选择哪种实例类型，AWS 弹性网络适配器 (ENA) 的报告速度通常显示为 1Gbps (1/1)。这是因为指示的速度并不直接反映实际的网络性能。与传统网络接口不同，ENA 速度可以根据实例的要求和工作负载动态扩展。真正的网络性能主要由实例类型和大小决定。因此，实际网络吞吐量可能根据具体实例类型和当前网络负载而有很大差异。

在 **Microsoft Azure** 上部署 **NetScaler VPX** 实例

October 17, 2024

在 Microsoft Azure Resource Manager (ARM) 上部署 NetScaler VPX 实例时，可以使用以下两个功能集来满足业务需求：

- Azure 云计算功能
- NetScaler 负载平衡和流量管理功能

您可以在 ARM 上将 NetScaler VPX 实例作为独立实例或活动-备用模式下的高可用性对进行部署。

可以通过以下两种方式在 Microsoft Azure 上部署 NetScaler VPX 实例：

- 通过 Azure 应用商店。NetScaler VPX 虚拟设备在 Microsoft Azure 应用商店中作为映像提供。
- 使用 GitHub 上提供的 NetScaler Azure Resource Manager (ARM) json 模板。有关更多信息，请参阅 NetScaler 解决方案模板的 GitHub 存储库。

Microsoft Azure 堆栈是硬件和软件的集成平台，它在本地数据中心提供 Microsoft Azure 公有云服务，让组织构建混合云。现在，您可以在 Microsoft Azure 堆栈上部署 NetScaler VPX 实例。

> 注意：
>
> Azure 限制访问来自 Azure 外部的流量，并阻止这些流量。要提供访问权限，请在连接到公有 IP 地址的虚拟机的 NIC 的网络安全组中添加入站规则，从而启用服务或端口。有关更多信息，请参阅有关入站 NAT 规则的 Azure 文档。

必备条件

在 Azure 上部署 NetScaler VPX 实例之前，您需要一些必备条件知识。

- 熟悉 Azure 术语和网络详细信息。有关信息，请参阅 Azure 术语。
- 了解 NetScaler 设备。有关 NetScaler 设备的详细信息，请参阅 NetScaler
- NetScaler 网络知识。请参阅网络主题。

NetScaler VPX 实例在 Azure 上的工作原理

在本地部署中，NetScaler VPX 实例至少需要三个 IP 地址：

- 管理 IP 地址，称为 NSIP 地址
- 子网 IP (SNIP) 地址，用于与服务器场通信
- 虚拟服务器 IP (VIP) 地址，用于接收客户端请求

有关更多信息，请参阅 Microsoft Azure 上适用于 NetScaler VPX 实例的网络架构。

> 注意：
>
> NetScaler VPX 实例支持 Intel 和 AMD 处理器。VPX 虚拟设备可以部署在具有两个或更多虚拟化内核和超过 2 GB 内存的任何实例类型上。有关系统要求的更多信息，请参阅 NetScaler VPX 数据手册。

在 Azure 部署中，可以通过三种方式在 Azure 上预配 NetScaler VPX 实例：

- 多 NIC 多 IP 体系结构
- 单网卡多 IP 架构
- 单 NIC 单 IP

根据您的需求，您可以使用这些支持的架构类型中的任何一种。

多 **NIC** 多 **IP** 体系结构

在此部署类型中，可以将多个网络接口 (NIC) 连接到 VPX 实例。任何 NIC 都可以有一个或多个 IP 配置 - 为其分配的静态或动态公用 IP 地址和专用 IP 地址。

有关详细信息，请参阅以下用例：

- 使用多个 IP 地址和 NIC 配置高可用性设置
- 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置

> 注意：
>
> 为了避免 Azure 环境上的 MAC 移动和接口静音，Citrix 建议您为 NetScaler VPX 实例的每个数据接口（不带标签）创建 VLAN，并在 Azure 中绑定 NIC 的主要 IP。有关更多信息，请参阅 CTX224626 文章。

单网卡多 **IP** 架构

在此部署类型中，一个网络接口 (NIC) 与多个 IP 配置关联 - 向其分配的静态或动态公用 IP 地址和专用 IP 地址。有关详细信息，请参阅以下用例：

- 为 NetScaler VPX 独立实例配置多个 IP 地址
- 使用 PowerShell 命令为 NetScaler VPX 独立实例配置多个 IP 地址

单 **NIC** 单 **IP**

在此部署类型中，一个网络接口 (NIC) 与单个 IP 地址相关联，用于执行 NSIP、SNIP 和 VIP 的功能。

有关更多信息，请参阅 配置 NetScaler VPX 独立实例。

> 注意：
>
> 单 IP 模式仅适用于 Azure 部署。此模式不适用于您的本地、AWS 或其他类型的部署中的 NetScaler VPX 实例。

NetScaler VPX 许可

Azure 上的 NetScaler VPX 实例需要许可证。以下许可方式可用于 Azure 上运行的 NetScaler VPX 实例。

- 基于订阅的许可：NetScaler VPX 设备在 Azure 应用商店中作为付费实例提供。基于订阅的许可是即付即用方式。用户按小时收费。

> 注意：
>
> 对于基于订阅的许可证实例，您的订阅账单适用于特定许可模式的整个许可证期限。由于云限制，Azure 不支持更改或删除适用于您的订阅的许可模式。要更改或移除订阅许可证，请删除现有的 ADC VM，然后使用所需许可证重新创建新的 ADC VM。

NetScaler 为基于订阅的许可证实例提供技术支持。要提交支持案例，请参阅 Azure 上对 NetScaler 的支持—按小时价格计算的订阅许可证。

- 自带许可证 **(BYOL)**：如果您自带许可证 (BYOL)，请参阅 VPX 许可指南，URL 为 http://support.citrix.com/article/CTX122426。您必须：
  - 使用 NetScaler 网站内的许可门户生成有效许可。
  - 将许可证上载到实例。

> 注意：
>
> 在 Azure 堆栈环境中，**BYOL** 是唯一可用的许可选项。

- **NetScaler VPX** 检出/签出许可：有关详细信息，请参阅 NetScaler VPX 检出/签出许可。

  从 NetScaler 版本 12.0 56.20 开始，用于本地和云部署的 NetScaler VPX Express 不需要许可证文件。有关 NetScaler VPX Express 的更多信息，请参阅 NetScaler 许可概述中的“NetScaler VPX Express 许可证”部分。

VPX 性能和推荐的 Azure 实例类型

为了获得所需的 VPX 性能，建议使用以下 Azure 实例类型。

VPX 性能	Azure 实例类型 VPX 1 网卡/2 网卡	VPX 3 网卡	VPX 最多 8 个 NIC
高达 200 Mbps	Standard_D2s_v4 Standard_D2_v5 Standard_DS3_v2 标准_DS3_v2		标准_DS4_v2
高达 1 Gbps	Standard_D4s_v4 Standard_D4_v5 Standard_DS3_v2 标准_DS3_v2		标准_DS4_v2
高达 5 Gbps	Standard_D8s_v5 Standard_D8_v5 Standard_DS3_v2 Standard_D8s_v5 Standard_D8_v5 Standard_DS4_v2 标准_DS4_v2		
高达 10 Gbps	标准_D2_v5	标准_D8_v5	标准_D16_v5

注意事项

- 为了在具有 1 Gbps 和 5 Gbps 吞吐量的 NetScaler VPX 实例上实现最佳性能，必须启用 Azure 加速网络。

  有关配置加速网络的更多信息，请参阅 配置 NetScaler VPX 实例以使用 Azure 加速网络。

- 无论是从 Azure 应用商店购买的基于订阅的小时许可证，在极少数情况下，部署在 Azure 上的 NetScaler VPX 实例可能都会出现默认的 NetScaler 许可证。发生这种情况的原因是 Azure 实例元数据服务 (IMDS) 存在问题。
- 在 NetScaler VPX 实例上进行任何配置更改之前，请先进行热重启，以启用正确的 NetScaler VPX 许可证。

Azure 中对 NetScaler VPX 实例的 IPv6 支持

从 13.1-21.x 版起，NetScaler VPX 独立实例在 Azure 中支持 IPv6 地址。您可以在 Azure 云中的 NetScaler VPX 独立实例上将 IPv6 地址配置为 VIP 和 SNIP 地址。

有关如何在 Azure 上启用 IPv6 的信息，请参阅以下 Azure 文档：

- 什么是 Azure 虚拟网络的 IPv6?
- 将 IPv6 添加到 Azure 虚拟网络中的 IPv4 应用程序-Azure CLI
- 地址类型

有关 NetScaler 设备如何支持 IPv6 的信息，请参阅 Internet 协议版本 6。

IPv6 限制：

- NetScaler 中的 IPv6 部署目前不支持 Azure 后端自动缩放。
- NetScaler VPX HA 部署不支持 IPv6。

限制

在 ARM 上运行 NetScaler VPX 负载平衡解决方案会带来以下限制：

- Azure 体系结构不支持以下 NetScaler 功能：
  - 免费 ARP (GARP)
  - 二级模式
  - 已标记的 VLAN
  - 动态路由
  - 虚拟 MAC
  - USIP
  - 群集

> 注意：
>
> 借助 NetScaler Application Delivery Management (ADM) AutoScale 功能（云部署），ADC 实例支持在所有许可证上进行群集。有关信息，请参阅 使用 NetScaler ADM在 Microsoft Azure 中自动扩展 NetScaler VPX。

- 如果您预计可能需要随时关闭并暂时取消分配 NetScaler VPX 虚拟机，则可以在创建虚拟机期间分配静态内部 IP 地址。如果不分配静态内部 IP 地址，Azure 可能会在每次重新启动时为虚拟机分配一个不同的 IP 地址，并且虚拟机可能会变得无法访问。
- Azure 支持高达 10 Gbps 的 VPX 吞吐量。有关更多信息，请参阅 NetScaler VPX 数据表。
- 当使用吞吐量超过 3 Gbps 的 NetScaler VPX 实例时，实际网络吞吐量可能与实例许可证中指定的吞吐量不一致。但是，其他功能，例如 SSL 吞吐量和每秒 SSL 交易量可能会有所改善。
- 用户在 ARM 中看不到虚拟机置备期间由 Azure 生成的部署 ID。您不能使用部署 ID 在 ARM 上部署 NetScaler VPX 设备。
- NetScaler VPX 实例在初始化时支持 20 Mbps 吞吐量和标准版功能。
- Azure 上启用了加速联网功能的 NetScaler VPX 实例可提供更好的性能。从版本 13.0 Build 76.x 起，NetScaler VPX 实例支持 Azure 加速的网络连接。要在 NetScaler VPX 上启用加速联网，Citrix 建议您使用支持加速联网的 Azure 实例类型。
- 对于 Citrix Virtual Apps and Desktops 部署，可以将 VPX 实例上的 VPN 虚拟服务器配置为以下模式：
  - “基本”模式，其中 `ICAOnly` VPN 虚拟服务器参数设置为 ON。“基本”模式完全适用于未获许可的 NetScaler VPX 实例。
  - SmartAccess 模式，在此模式下，`ICAOnly` VPN 虚拟服务器参数设置为 OFF。SmartAccess 模式仅适用于未获许可的 NetScaler VPX 实例上的五个 NetScaler AAA 会话用户。

> 注意：
>
> 要配置 SmartControl 功能，必须将 Premium 许可证应用到 NetScaler VPX 实例。

Azure 术语

October 17, 2024

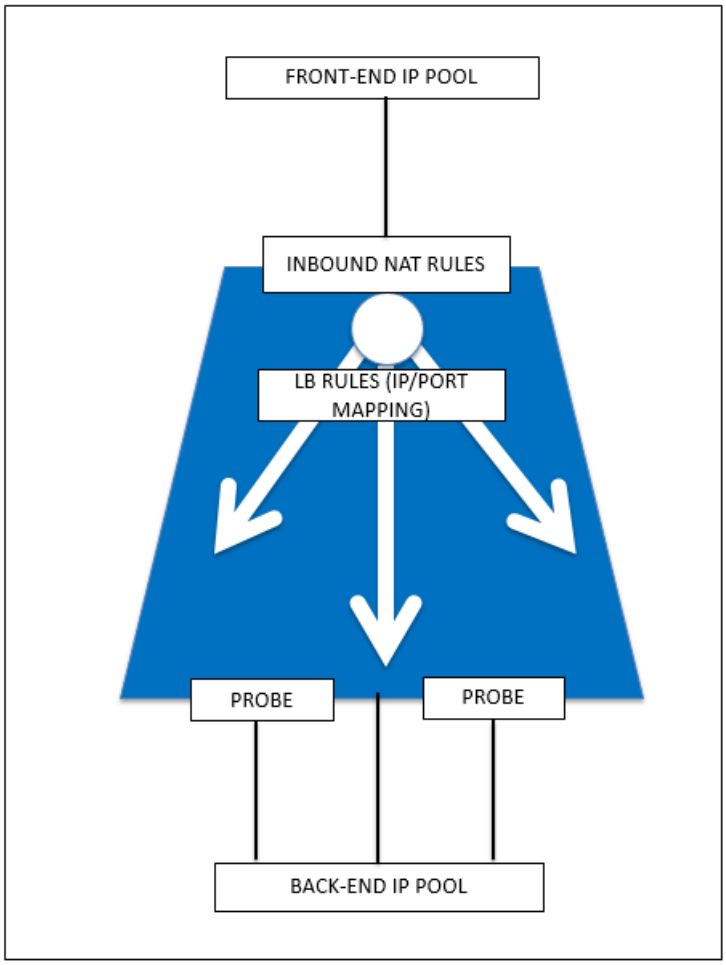
下面列出了在 NetScaler VPX Azure 文档中使用的一些 Azure 术语。

1. Azure 负载均衡器–Azure 负载均衡器是指在网络中的计算机之间分配传入流量的资源。流量在负载均衡器集中定义的虚拟机之间分配。负载均衡器可以是外部负载均衡器或面向 Internet 的负载均衡器，也可以是内部负载均衡器。

2. Azure Resource Manager (ARM) –ARM 是指 Azure 中的服务的新管理框架。Azure 负载均衡器使用基于 ARM 的 API 和工具进行管理。
3. 后端地址池–这是指要将负载分配到的与虚拟机 NIC (NIC) 相关联的 IP 地址。
4. BLOB - 二进制大对象–可以存储在 Azure 存储中的文件或图像等任何二进制对象。
5. 前端 IP 配置–Azure 负载均衡器可以包括一个或多个前端 IP 地址，又称为虚拟 IP (VIP)。这些 IP 地址用作流量的入口。
6. 实例级公用 IP (ILPIP) –ILPIP 是指能够直接分配给您的虚拟机或角色实例（而非您的虚拟机或角色实例所在的云服务）的公用 IP 地址。这不会取代分配给您的云服务的 VIP（虚拟 IP）。更确切地说，这是一个能够用于直接连接到您的虚拟机或角色实例的额外 IP 地址。

   > 注意：
   >
   > 过去，ILPIP 被称为 PIP，代表公共 IP。

7. 入站 NAT 规则–其中包括用于将负载均衡器上的公用端口映射到后端地址池中的特定虚拟机的端口的规则。
8. IP-Config - 可以将其定义为与单个 NIC 相关联的 IP 地址对（公用 IP 和 专用 IP）。在 IP-Config 中，公用 IP 地址可以为空。每个 NIC 可以具有与之关联的多个 IP-Config，最多可以具有 255 个。
9. 负载平衡规则–用于将指定的前端 IP 和端口组合映射到一组后端 IP 地址和端口组合的规则属性。通过负载均衡器资源的单个定义，您可以定义多条负载平衡规则，其中每条规则都反映一个前端 IP 和端口与虚拟机关联的后端 IP 和端口的组合。



10. 网络安全组–包含允许或拒绝网络流量传输到虚拟网络中的虚拟机实例的访问控制列表 (ACL) 规则的列表。可以将 NSG 与子网或该子网中的各个虚拟机实例相关联。将网络安全组与子网相关联时，ACL 规则将应用到该子网中的所有虚拟机实例。此外，可以通过将网络安全组直接与该虚拟机相关联，进一步限制传输到各个虚拟机的流量。

11. 专用 IP 地址–用于 Azure 虚拟网络以及您的本地网络（使用 VPN 网关将您的网络扩展到 Azure 时）中的通信。专用 IP 地址允许 Azure 资源通过 VPN 网关或 ExpressRoute 环路与虚拟网络或本地网络中的其他资源通信，不需要使用可通过 Internet 访问的 IP 地址。在 Azure Resource Manager 部署模型中，专用 IP 地址与以下类型的 Azure 资源相关联：虚拟机、内部负载均衡器 (ILB) 和应用程序网关。

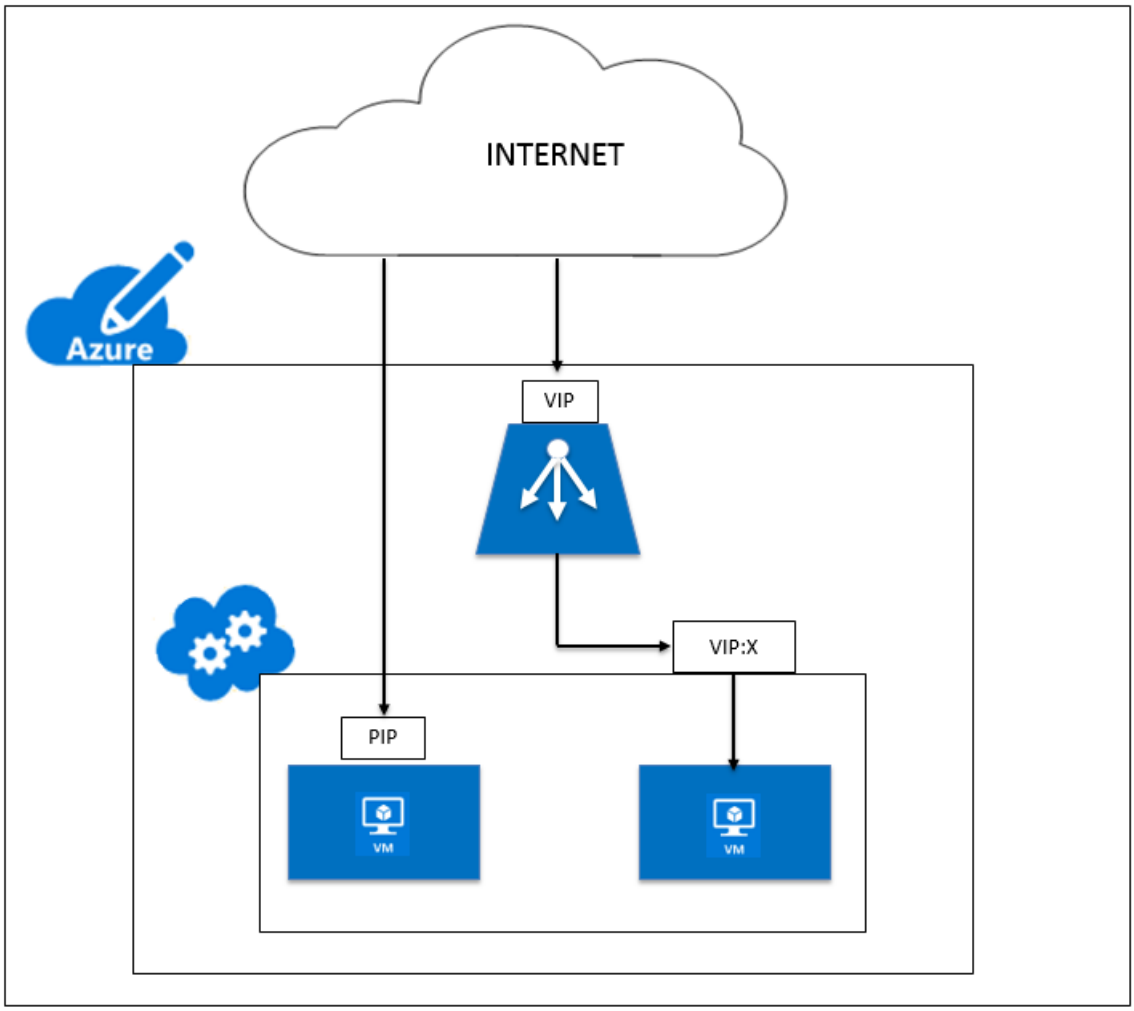
12. 探测–包括用于检查后端地址池中的虚拟机实例的可用性的运行状况探测。如果特定的虚拟机在一段时间内不响应运行状况探测，则不会再向其发送流量。可以通过探测跟踪虚拟实例的运行状况。如果运行状况探测失败，则不会再自动轮转虚拟实例。

13. 公用 IP 地址 (PIP) –PIP 用于与 Internet 的通信，包括 Azure 面向公众且与虚拟机相关联的服务、面向 Internet 的负载均衡器、VPN 网关和应用程序网关。

14. 区域 - 地理上不跨越国境并且包含一个或多个数据中心的区域。定价、地区服务以及产品/服务类型在地区级别展现。一个地区通常与另一个地区配对（其距离最多可以相隔几百英里）以组成一个地区对。地区对可以用作灾难

恢复和高可用性方案的机制。通常又称为位置。

15. 资源组 - 资源管理器中的某个容器保留某个应用程序的相关资源。资源组可以包括某个应用程序的所有资源，或者仅包括逻辑上编组在一起的资源。
16. 存储帐户–Azure 存储帐户向您提供了对 Azure 存储中的 Azure blob、队列、表格和文件服务的访问权限。存储帐户为您的 Azure 存储数据对象提供唯一的命令空间。
17. 虚拟机–运行某个操作系统的物理机的软件实现。多个虚拟机可以同时在同一硬件上运行。在 Azure 中，提供的虚拟机有各种大小。
18. 虚拟网络 - Azure 虚拟网络是您自己的网络在云中的表示。虚拟网络是您的订阅专用的 Azure 云的逻辑隔离。您可以完全控制此网络中的 IP 地址块、DNS 设置、安全策略和路由表。也可以进一步将您的 VNet 分段为几个子网并启动 Azure IaaS 虚拟机和云服务（PaaS 角色实例）。此外，可以使用 Azure 中提供的其中一个连接选项将虚拟网络连接到您的本地网络。实际上，您可以将自己的网络扩展到 Azure，实现对 IP 地址块的完全控制，同时享有企业级 Azure 提供的优势。



适用于 **Microsoft Azure** 上 **NetScaler VPX** 实例的网络体系结构

October 17, 2024

在 Azure Resource Manager (ARM) 中，NetScaler VPX 虚拟机 (VM) 位于虚拟网络中。可以在虚拟网络的给定子网中创建单个网络接口，并且可以连接到 VPX 实例。可以使用网络安全组过滤传输到 Azure 虚拟网络中的 VPX 实例的网络流量以及从该实例传输的网络流量。网络安全组包含允许或拒绝传入 VPX 实例的入站网络流量或从 VPX 实例传出的出站网络流量的安全规则。有关详细信息，请参阅 安全组。

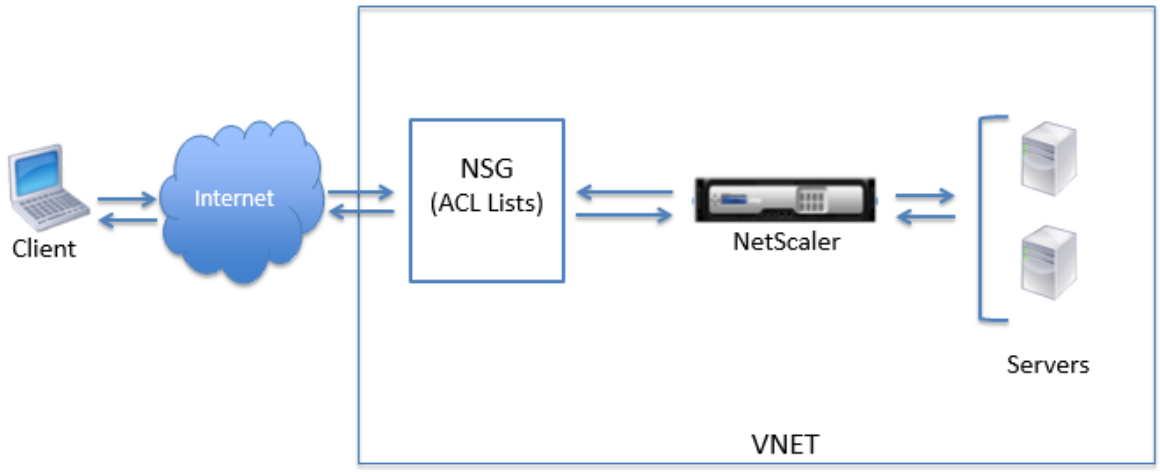
网络安全组筛选发给 NetScaler VPX 实例的请求，然后 VPX 实例将其发送到服务器。来自服务器的响应以相反方向通过相同的路径。可以将网络安全组配置为筛选单个 VPX VM，或者，在子网和虚拟网络中，可以筛选多个 VPX 实例的部署中的流量。

NIC 包含虚拟网络、子网、内部 IP 地址和公用 IP 地址等网络配置详细信息。

在 ARM 上，最好知道用于访问使用单个 NIC 和单个 IP 地址部署的 VM 的以下 IP 地址：

- 公有 IP (PIP) 地址是直接在 NetScaler 虚拟机的虚拟 NIC 上配置的面向 Internet 的 IP 地址。这允许您直接从外部网络访问 VM。
- NetScaler IP（也称为 NSIP）地址是在虚拟机上配置的内部 IP 地址。该地址不可路由。
- 虚拟 IP 地址 (VIP) 是使用 NSIP 和端口号配置的。客户端通过 PIP 地址访问 NetScaler 服务，并且当请求到达 NetScaler VPX VM 的 NIC 或 Azure 负载均衡器时，VIP 将被转换为内部 IP (NSIP) 和内部端口号。
- 内部 IP 地址是指 VM 的来自虚拟网络的地址空间池的专用内部 IP 地址。此 IP 地址无法从外部网络进行访问。此 IP 地址默认是动态的，除非您将其设置为静态。根据在网络安全组上创建的规则，来自 Internet 的流量将被路由到此地址。网络安全组与 NIC 相集成，以将正确类型的流量选择性发送到 NIC 上的正确端口，这取决于在 VM 上配置的服务。

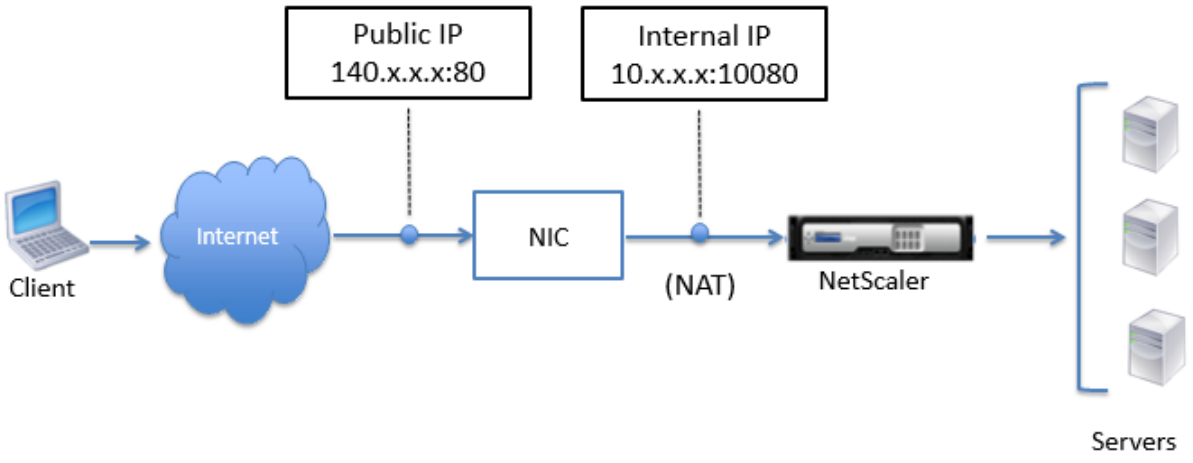
下图显示了流量如何通过在 ARM 中预配的 NetScaler VPX 实例从客户端流向服务器。



通过网络地址转换传输流量

您也可以为您的 NetScaler VPX 实例（实例级别）申请公有 IP (PIP) 地址。如果您在 VM 级别使用此直接 PIP，则不需要定义入站和出站规则即可拦截网络流量。来自 Internet 的传入请求直接在 VM 上接收。Azure 执行网络地址转换 (NAT)，并将流量转发到 VPX 实例的内部 IP 地址。

下图显示了 Azure 如何执行网络地址转换以映射 NetScaler 内部 IP 地址。



在此示例中，分配给网络安全组的公用 IP 地址为 140.x.x.x，内部 IP 地址为 10.x.x.x。定义入站和出站规则时，公有 HTTP 端口 80 被定义为接收客户端请求的端口，相应的私有端口 10080 被定义为 NetScaler VPX 实例监听的端口。客户端请求在公用 IP 地址 (140.x.x.x) 上接收。Azure 执行网络地址转换，以将 PIP 映射到端口 10080 上的内部 IP 地址 10.x.x.x，并转发客户端请求。

> 注意：
>
> 处于高可用性模式的 NetScaler VPX VM 由在其上配置了入站规则以控制负载平衡流量的外部或内部负载平衡器进行控制。外部流量首先被这些负载均衡器拦截，并且流量将根据所配置的负载平衡规则（在负载均衡器上定义了后端池、NAT 规则和运行状况探测）改变方向。

端口用法指南

在创建 NetScaler VPX 实例时或配置虚拟机后，您可以在网络安全组中配置更多入站和出站规则。每个入站和出站规则都与一个公用端口和一个专用端口相关联。

在配置网络安全组规则之前，请注意以下关于可使用的端口号的指南：

1. NetScaler VPX 实例保留以下端口。在对来自 Internet 的请求使用公用 IP 地址时，不能将这些端口定义为专用端口。

   端口 21、22、80、443、8080、67、161、179、500、520、3003、3008、3009、3010、3011、4001、5061、9000、7000。

但是，如果您希望面向 Internet 的服务（例如 VIP）使用标准端口（例如端口 443），则必须使用网络安全组创建端口映射。然后，标准端口会映射到 NetScaler 上为此 VIP 服务配置的其他某个端口。

例如，VIP 服务可能会在 VPX 实例上的端口 8443 上运行，但映射到公用端口 443。因此，当用户通过公用 IP 访问端口 443 时，请求将定向到专用端口 8443。

2. 公用 IP 地址不支持动态打开端口映射的协议，例如被动 FTP 或 ALG。
3. 高可用性不适用于使用与 VPX 实例关联的公用 IP 地址 (PIP)，而非在 Azure 负载均衡器上配置的 PIP。

> 注意：
>
> 在 Azure Resource Manager 中，NetScaler VPX 实例与两个 IP 地址（公用 IP 地址 (PIP) 和内部 IP 地址）相关联。外部流量连接到 PIP，而内部 IP 地址或 NSIP 是不可路由的。要在 VPX 中配置 VIP，请使用内部 IP 地址和任何可用的空闲端口。请勿使用 PIP 来配置 VIP。

配置 **NetScaler VPX** 独立实例

October 17, 2024

通过创建虚拟机和配置其他资源，您可以在 Azure Resource Manager (ARM) 门户中以独立模式预置单个 NetScaler VPX 实例。

开始之前的准备工作

请确保您具有以下对象：

- Microsoft Azure 用户帐户
- Microsoft Azure Resource Manager 的访问权限
- Microsoft Azure SDK
- Microsoft Azure PowerShell

在 Microsoft Azure 门 户页面上，通过提供用户名和密码登录 Azure Resource Manager 门户。

> 注意：
>
> 在 ARM 门户中，单击某个窗格中的某个选项会在右侧打开一个新窗格。可以从一个窗格导航到另一个窗格以配置您的设备。

配置步骤汇总

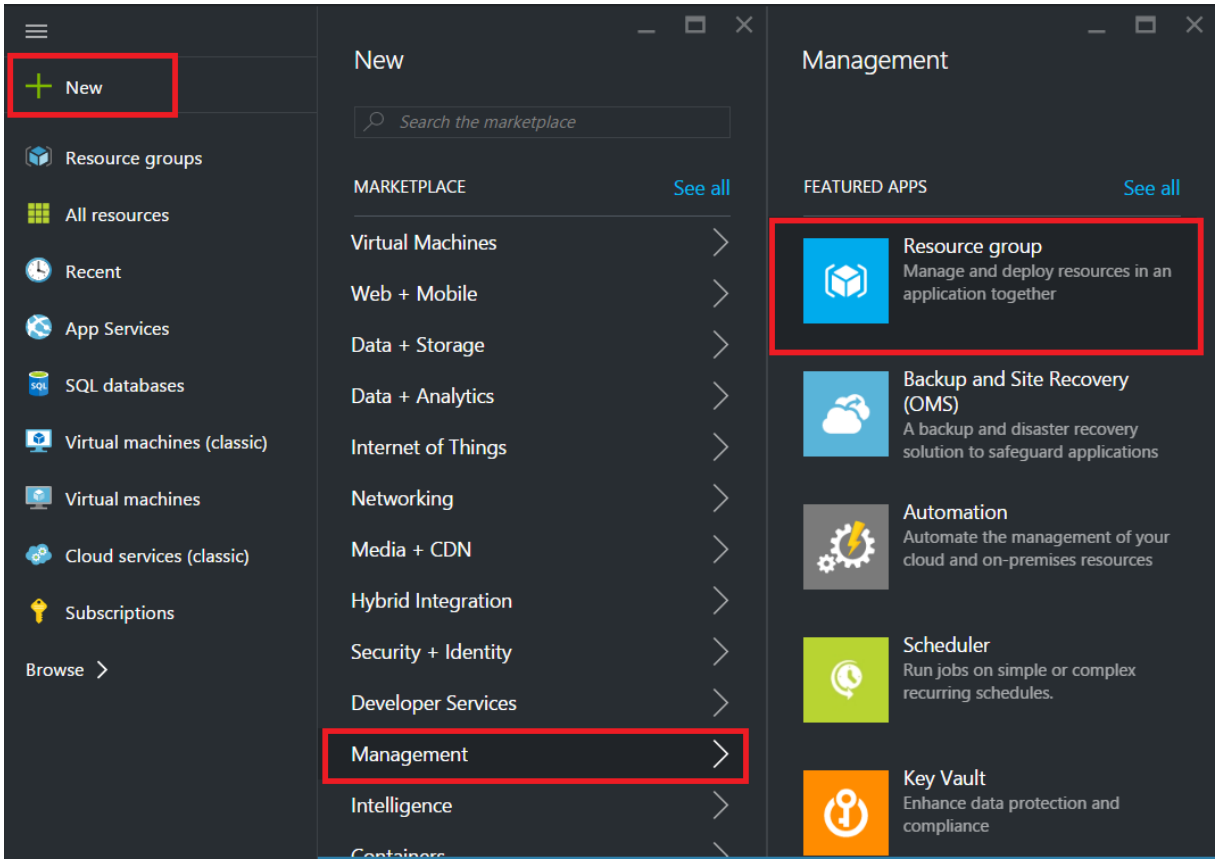
1. 配置资源组

2. 配置网络安全组
3. 配置虚拟网络及其子网
4. 配置存储帐户
5. 配置可用性集
6. 配置 NetScaler VPX 实例。

配置资源组

创建一个新资源组作为您的所有资源的容器。使用该资源组成组部署、管理和监视您的资源。

1. 单击 **New**（新建）>**Management**（管理）>**Resource group**（资源组）。
2. 在 **Resource group**（资源组）窗格中，输入以下详细信息：
   - 资源组名称
   - 资源组位置
3. 单击创建。

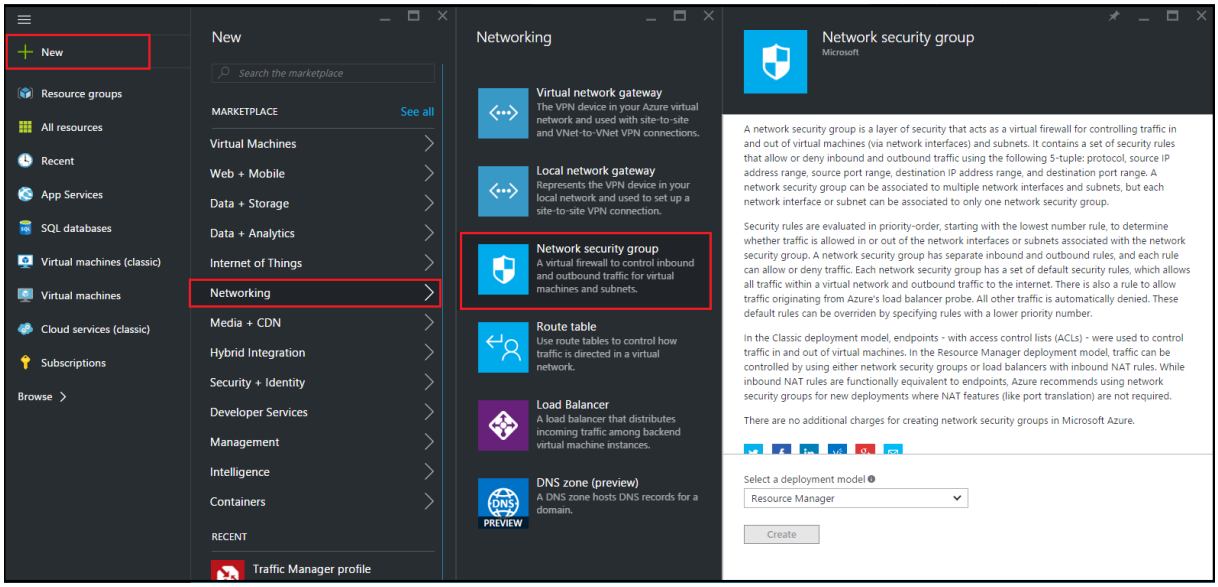


配置网络安全组

创建一个网络安全组，以分配用于控制虚拟网络内部的传入和传出流量的入站和出站规则。网络安全组允许您为单个虚拟机定义安全规则，此外，还允许您为虚拟网络子网定义安全规则。

1. 单击 **New**（新建）> **Networking**（网络连接）> **Network security group**（网络安全组）。
2. 在 **Create network security group**（创建网络安全组）窗格中，输入以下详细信息，然后单击 **Create**（创建）。
   - Name（名称）- 键入安全组的名称
   - Resource group（资源组）- 从下拉列表中选择资源组

> 注意：
>
> 请务必选择正确的位置。在下拉列表中显示的资源列表因位置而异。

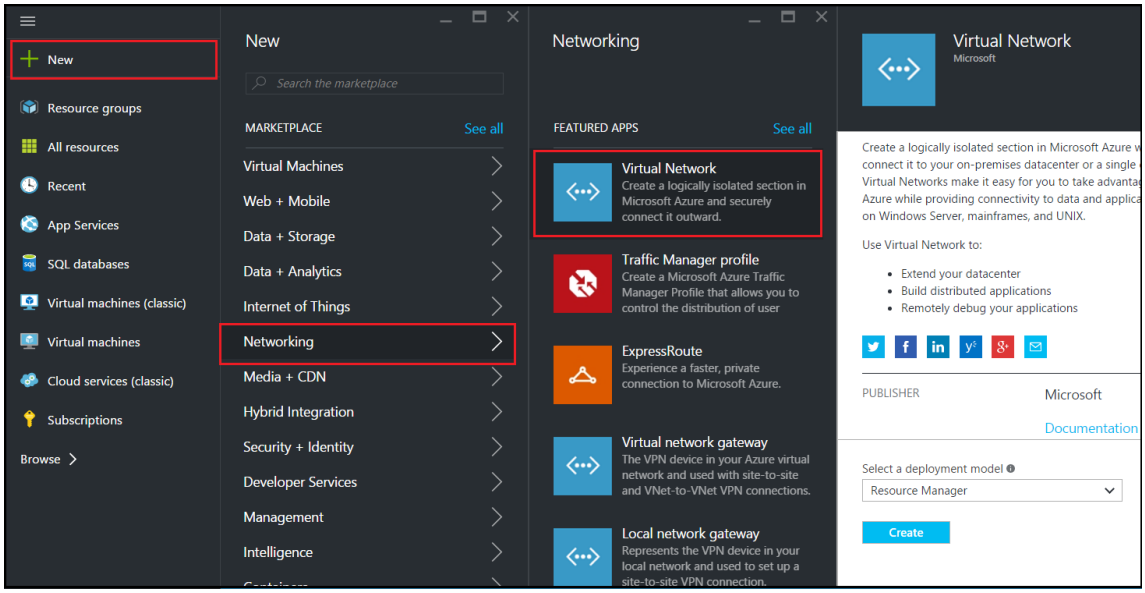


配置虚拟网络和子网

ARM 中的虚拟网络为您的服务提供了一个安全和隔离层。作为同一虚拟网络的一部分的 VM 和服务可以相互访问。

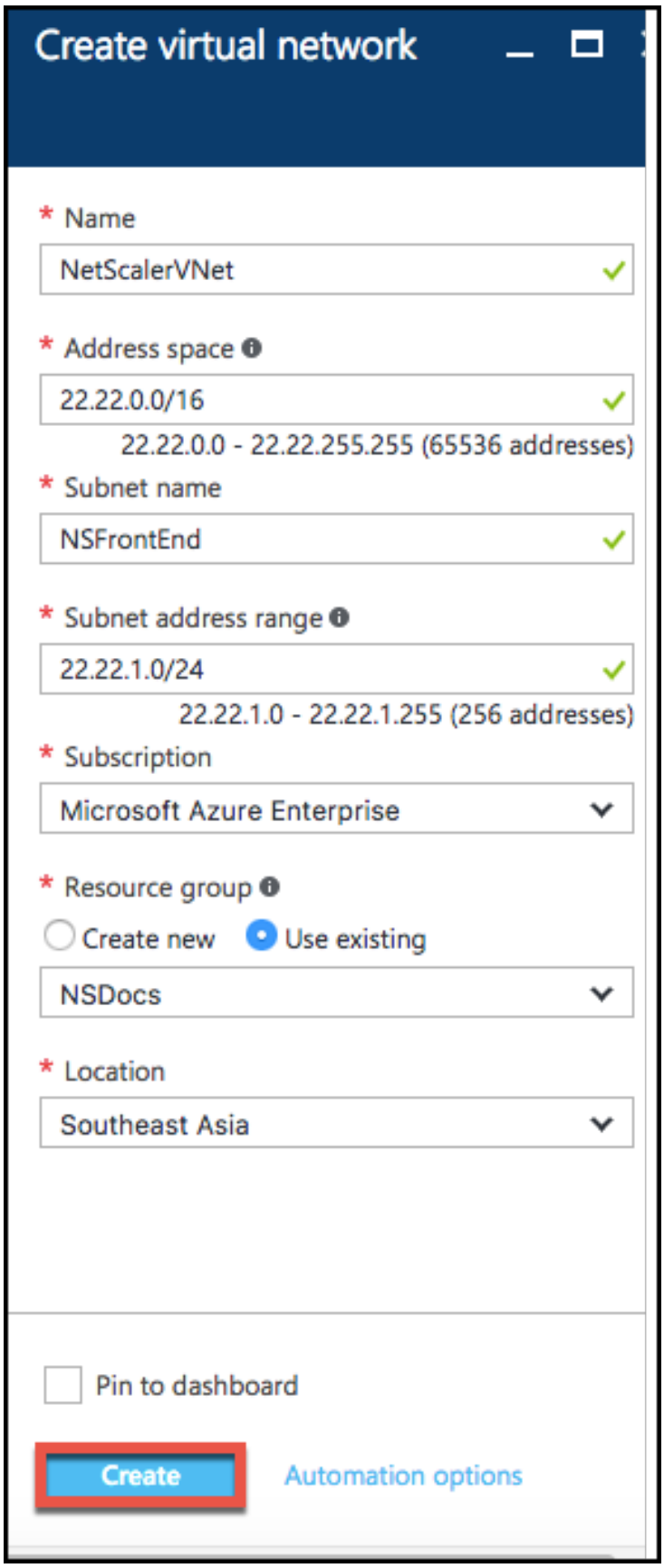
请执行以下步骤以创建虚拟网络和子网。

1. 单击 **New**（新建）> **Networking**（网络连接）> **Virtual Network**（虚拟网络）。
2. 在 **Virtual Network**（虚拟网络）窗格中，确保部署模式为 **Resource Manager**（资源管理器）并单击 **Create**（创建）。



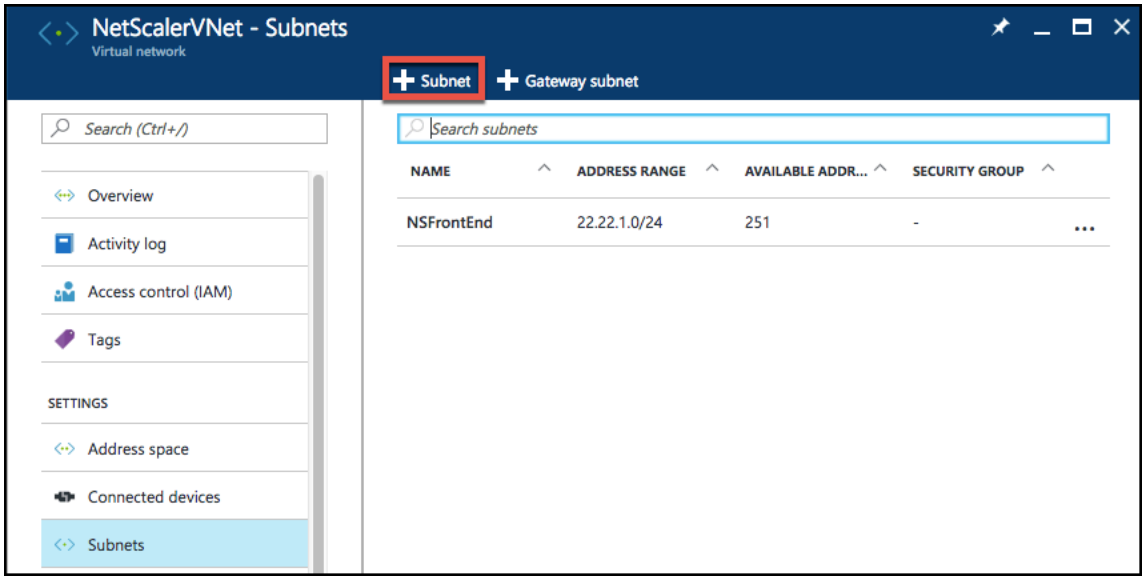
3. 在 **Create virtual network**（创建虚拟网络）窗格中，输入以下值，然后单击 **Create**（创建）。

   - 虚拟网络的名称
   - Address space（地址空间）- 键入虚拟网络的预留 IP 地址块
   - Subnet（子网）- 键入第一个子网的名称（稍后您将在此步骤中创建第二个子网）
   - Subnet address range（子网地址范围）- 键入子网的预留 IP 地址块
   - Resource group（资源组）–从下拉列表中选择之前创建的资源组



配置第二个子网

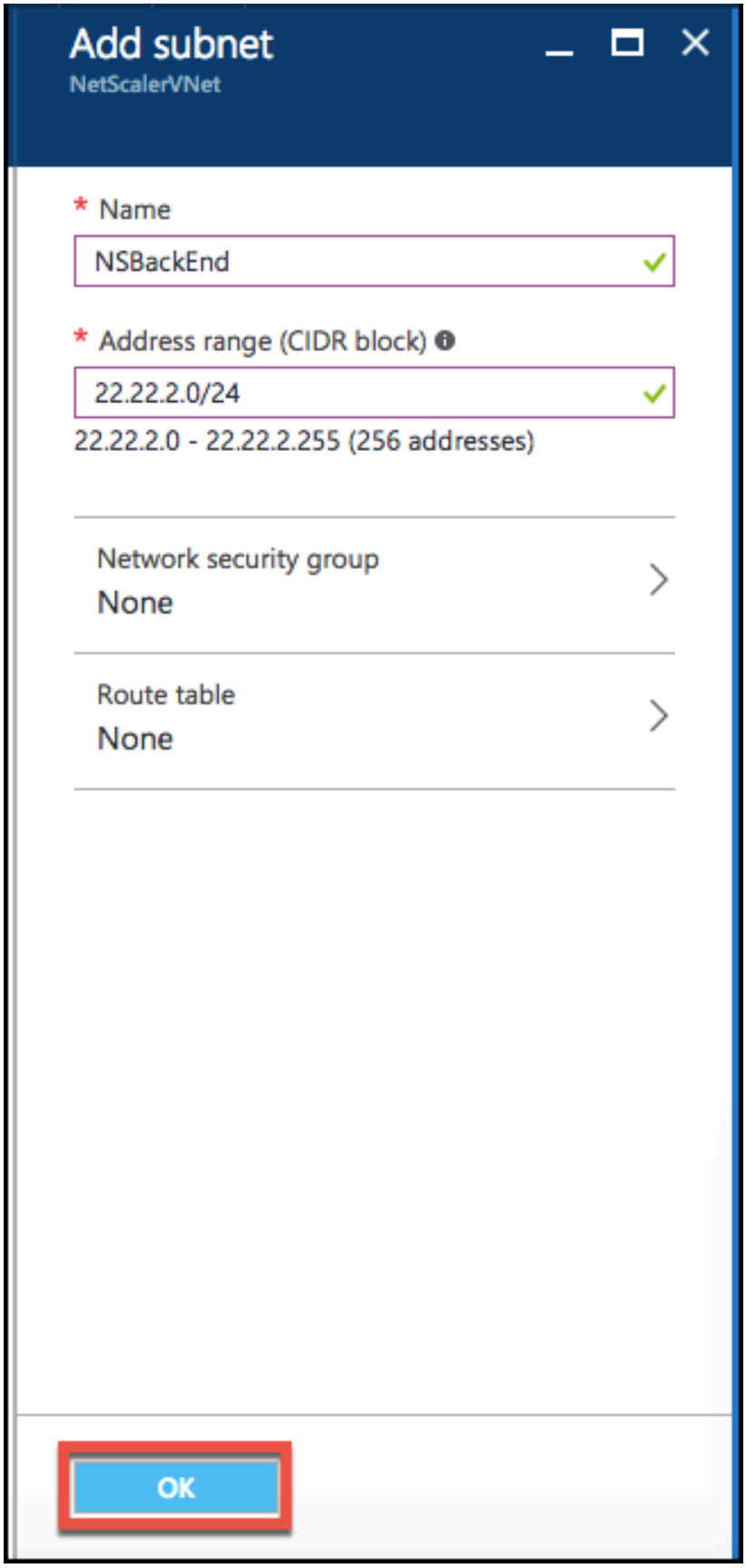
1. 从 **All resources**（所有资源）窗格中选择新创建的虚拟网络，然后在 **Settings**（设置）窗格中单击 **Subnets**（子网）。



2. 单击 **+Subnet**（+ 子网）并通过输入以下详细信息创建第二个子网。

   - 第二个子网的名称
   - Address range（地址范围）- 键入子网的预留 IP 地址块
   - 网络安全组 - 从下拉列表中选择网络安全组

3. 单击创建。

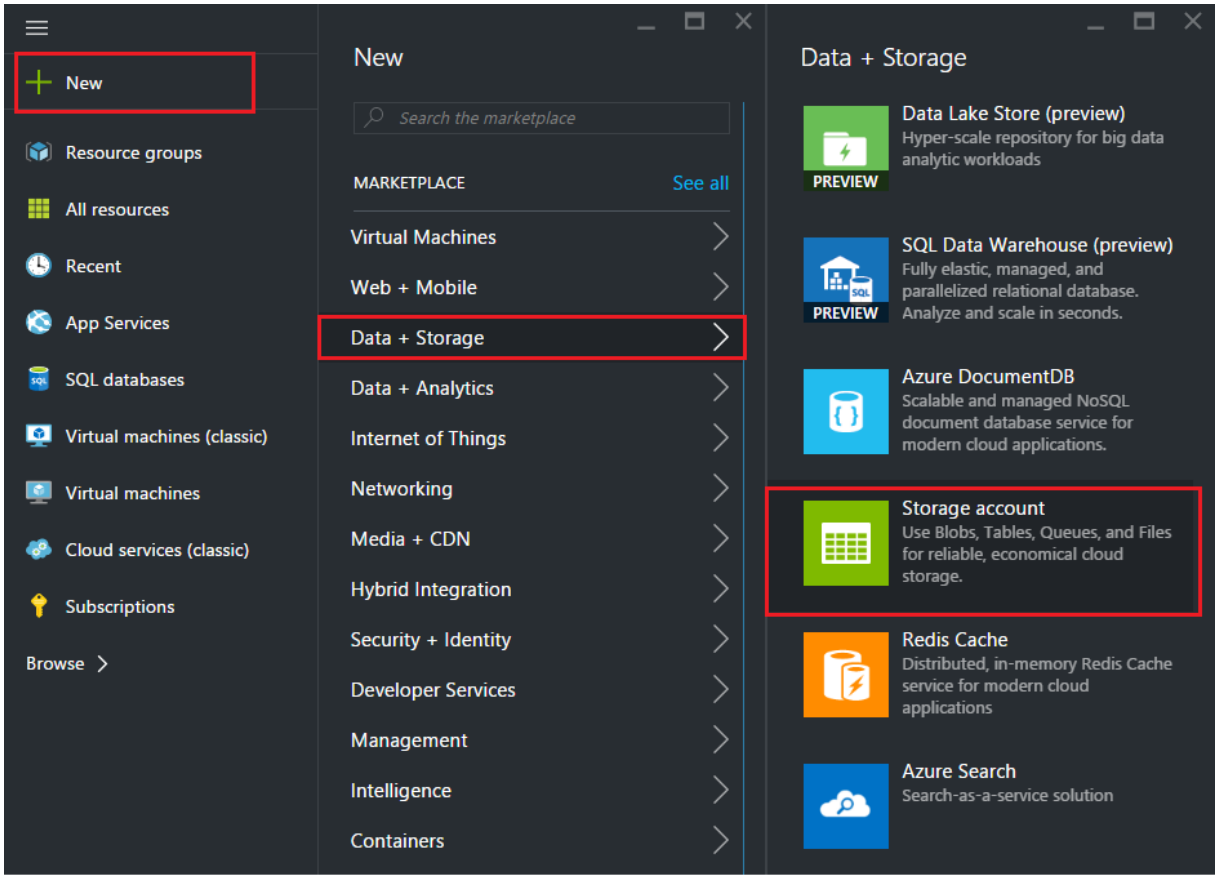


配置存储帐户

ARM IaaS 基础结构存储包括我们能够在其中以 blob、表格、队列和文件格式存储数据的所有服务。还可以使用 ARM 中这些格式的存储数据创建应用程序。

创建一个存储帐户以存储您的所有数据。

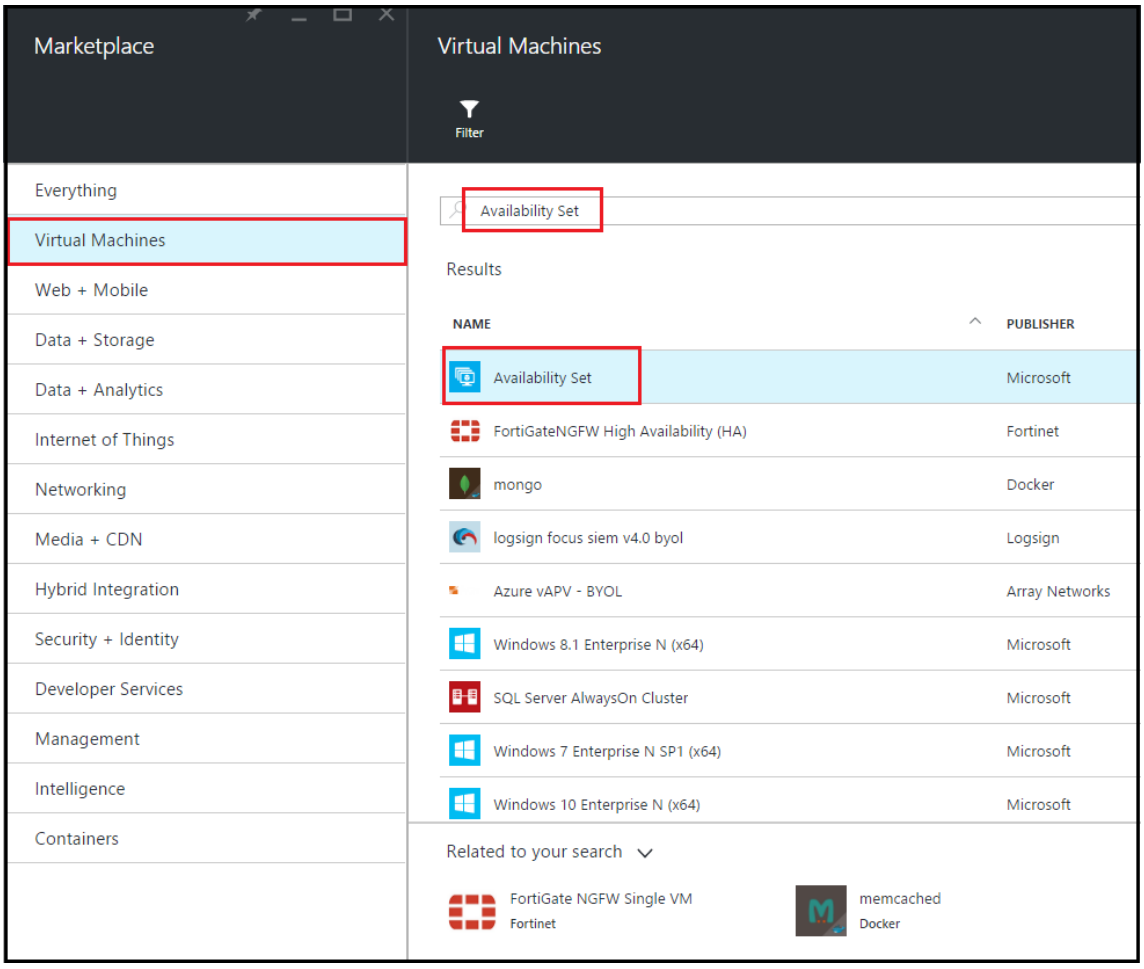
1. 单击 **+New** （+ 新建）> **Data + Storage**（数据 + 存储）> **Storage account**（存储帐户）。
2. 在 **Create storage account**（创建存储帐户）窗格中，输入以下详细信息：
    - 帐户的名称
    - Deployment mode（部署模式）–请务必选择 **Resource Manager**（资源管理器）
    - Account kind（帐户类型）–从下拉列表中选择 **General purpose**（常规用途）
    - Replication（复制）–从下拉列表中选择 **Locally redundant storage**（本地冗余存储）
    - Resource group（资源组）- 从下拉列表中选择新创建的资源组
3. 单击创建。



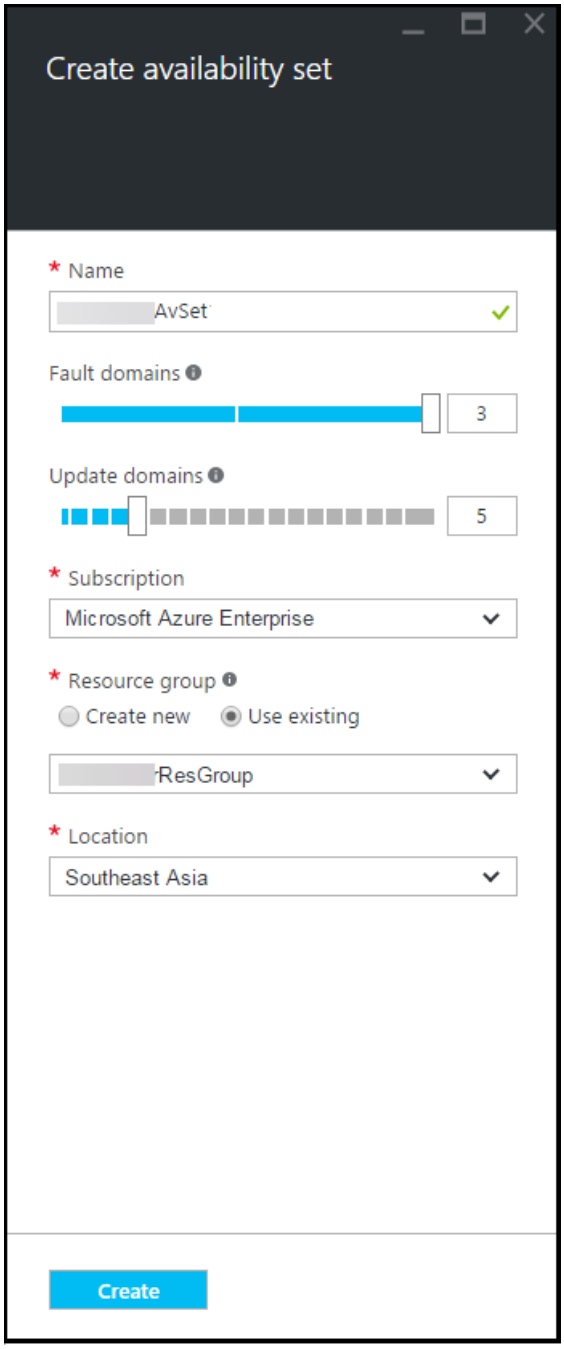
配置可用性集

可用性集可保证在进行计划内维护或非计划内维护时至少一个 VM 保持启动并运行。同一“可用性集”下的两个或多个 VM 放置在不同的容错域中以实现冗余服务。

1. 单击 **+New**（+ 新建）。
2. 单击“MARKETPLACE”（商城）窗格中的 **See all**（查看全部），然后单击 **Virtual Machines**（虚拟机）。
3. 搜索可用性集，然后从显示的列表中选择 **Availability set**（可用性集）条目。



4. 单击 **Create**（创建），然后在 **Create availability set**（创建可用性集）窗格中输入以下详细信息：
   - 可用性集的名称
   - Resource group（资源组）- 从下拉列表中选择新创建的资源组
5. 单击创建。



配置 **NetScaler VPX** 实例

在虚拟网络中创建 NetScaler VPX 的实例。从 Azure 市场获取 NetScaler VPX 映像，然后使用 Azure Resource Manager 门户创建 NetScaler VPX 实例。

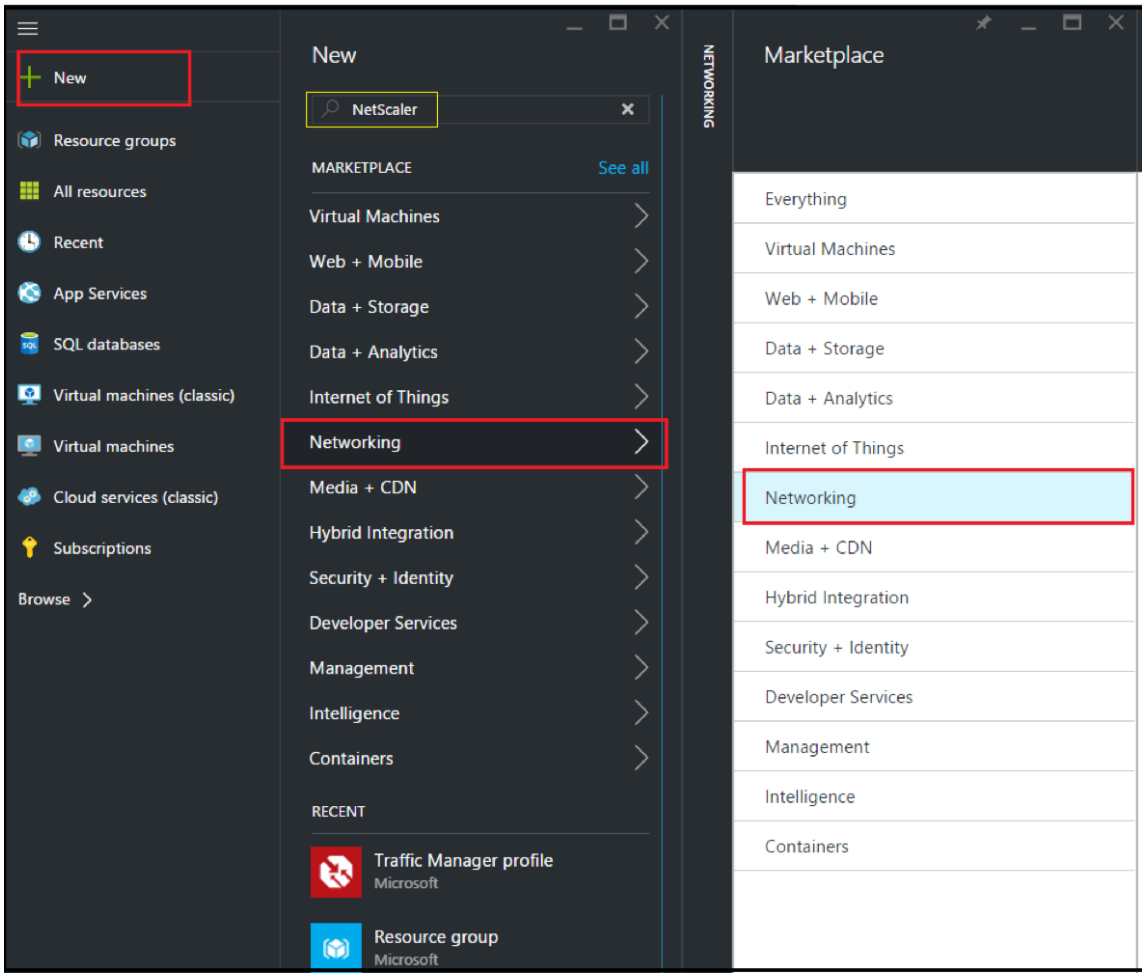
在开始创建 NetScaler VPX 实例之前，请确保您已经创建了一个包含该实例所在子网的虚拟网络。可以在 VM 置备期间创建虚拟网络，但无法灵活地创建不同的子网。有关创建虚拟网络的信息，请参阅 http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/。

配置 DNS 服务器和 VPN 连接以允许虚拟机访问 Internet 资源（可选操作）。

> 注意：
>
> Citrix 建议您在置备 NetScaler VPX VM 之前创建资源组、网络安全组、虚拟网络和其他实体，以便置备期间网络信息可用。

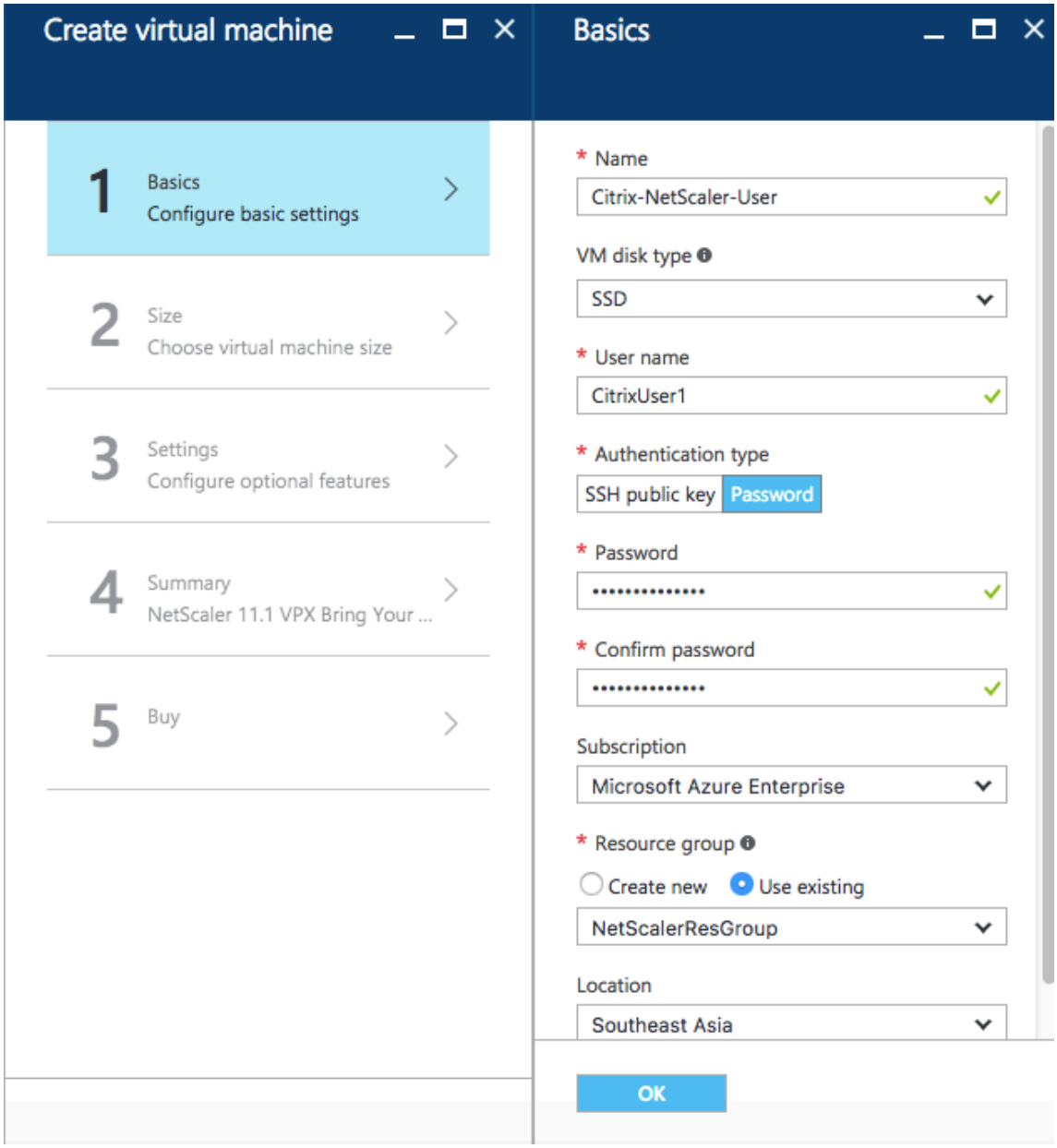
1. 单击 **+New**（+ 新建）> **Networking**（网络连接）。
2. 单击“查看全部”，然后在“网络”窗格中单击 **NetScaler**13.0。
3. 从软件套餐列表中选择 **NetScaler 13.0 VPX** 自带许可证。

   作为在 ARM 门户上查找任何实体的快速方法，您还可以在 Azure Marketplace 搜索框中键入该实体的名称，然后按\ <Enter\ >。在搜索框中键入 NetScaler 以查找 NetScaler 映像。



> 注意：
>
> 请务必选择最新映像。您的 NetScaler 映像名称中可能包含版本号。

4. 在 NetScaler VPX 自带许可证页面上，从下拉列表中选择资源管理器，然后单击创建。



5. 在 **Create virtual machine**（创建虚拟机）窗格中，在各个部分中指定所需的值以创建虚拟机。在每个部分中单击 **OK**（确定）保存您的配置。

Basic（基本）：

- Name（名称）- 指定 NetScaler VPX 实例的名称
- VM disk type（VM 磁盘类型）- 从下拉菜单中选择 SSD（默认值）或 HDD
- User name and Password（用户名和密码）- 指定访问已创建的资源组中的资源时使用的用户名和密码
- Authentication Type（身份验证类型）- 选择“SSH Public Key”（SSH 公钥）或“Password”（密码）
- Resource group（资源组）- 从下拉列表中选择已创建的资源组

可以在此处创建一个资源组，但 Citrix 建议您从 Azure Resource Manager 中的资源组创建资源组，然后从下拉列表

中选择该组

> 注意：
>
> 在 Azure 堆栈环境中，除了基本参数外，还指定了以下参数：
>
> - Azure 堆栈域
> - Azure 堆栈租户（可选）
> - Azure 客户端（可选）
> - Azure 客户端密钥（可选）

Size（大小）：

此时将显示磁盘大小，具体取决于您在基本设置中选择的 VM 磁盘类型（SDD 或 HDD）。

- 根据您的要求选择一个磁盘大小，然后单击 **Select**（选择）。

设置：

- 选择默认（标准）磁盘类型
- Storage account（存储帐户）- 选择存储帐户
- Virtual network（虚拟网络）- 选择虚拟网络
- Subnet（子网）- 设置子网地址
- Public IP address（公用 IP 地址）- 选择 IP 地址分配的类型
- Network security group（网络安全组）- 选择已创建的安全组。请务必在安全组中配置入站和出站规则。
- Availability Set（可用性集）- 从下拉菜单框中选择可用性集

Summary（摘要）：

配置设置已验证，“Summary”（摘要）页面将显示验证结果。如果验证失败，“Summary”（摘要）页面将显示失败原因。返回到特定部分，并根据需要进行更改。如果验证通过，请单击 **OK**（确定）。

Buy（购买）：

查看“Purchase”（购买）页面上的商品详细信息和法律条款，然后单击 **Purchase**（购买）。

对于高可用性部署，请在相同的可用性集中以及相同的资源组中创建两个独立的 NetScaler VPX 实例，以在主动-备份配置中部署这些实例。

为 **NetScaler VPX** 独立实例配置多个 **IP** 地址

October 17, 2024

本节介绍如何在 Azure Resource Manager (ARM) 中为独立 NetScaler VPX 实例配置多个 IP 地址。VPX 实例可以附加一个或多个 NIC，每个 NIC 可以分配一个或多个静态或动态公用和专用 IP 地址。可以将多个 IP 地址分配为 NSIP、VIP、SNIP 等。

有关更多信息，请参阅 Azure 文档 使用 Azure 门户为虚拟机分配多个 IP 地址。

如果您想使用 PowerShell 命令，请参阅 使用 PowerShell 命令为独立模式下的 NetScaler VPX 实例配置多个 IP 地址。

用例

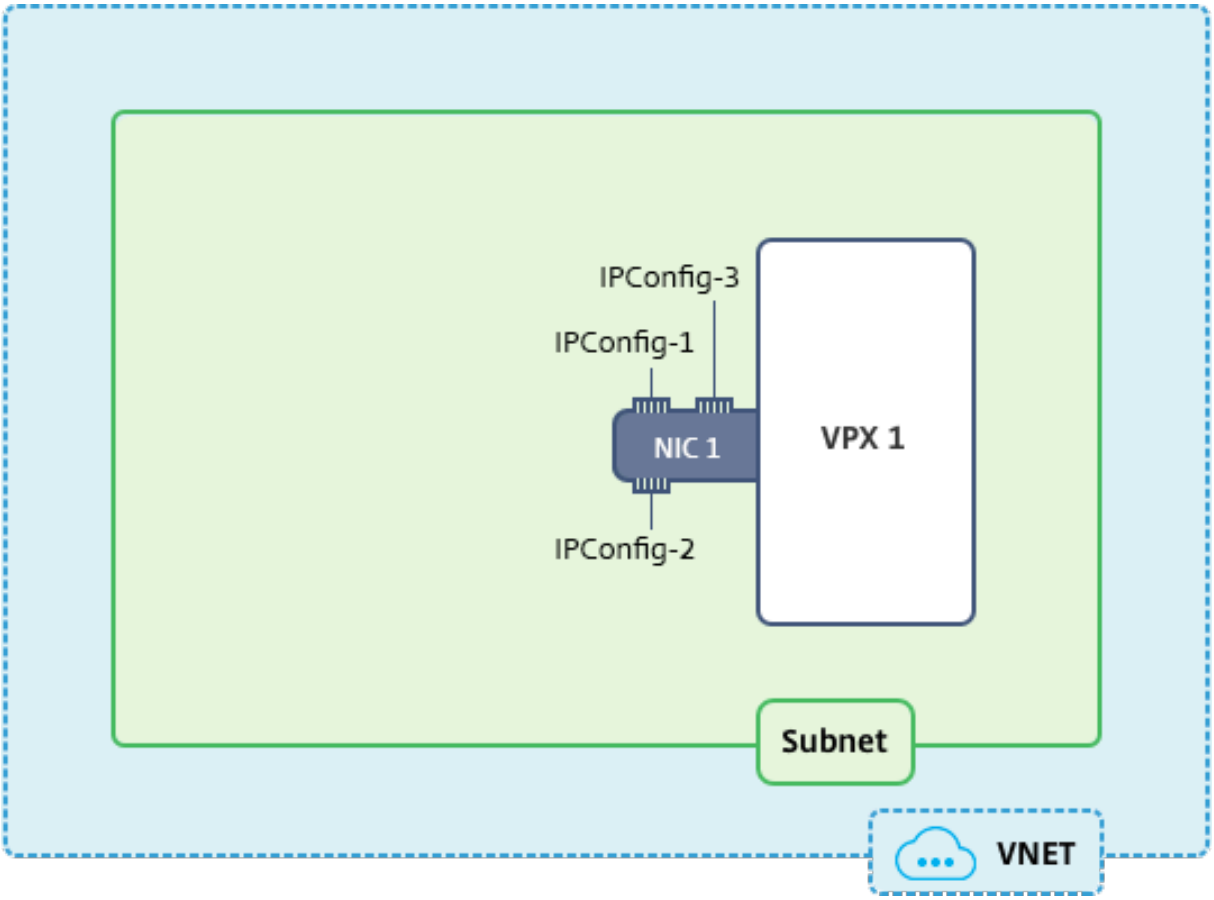
在此用例中，为一个独立 NetScaler VPX 设备配置了一个连接到虚拟网络 (VNET) 的 NIC。该 NIC 与三个 IP 配置 (ipconfig) 相关联，每个配置用于不同的用途 - 如表中所示。

IP 配置	关联到	用途
ipconfig1	静态公用 IP 地址；静态专用 IP 地址	服务管理流量
ipconfig2	静态公用 IP 地址；静态专用地址	服务客户端流量
ipconfig3	静态专用 IP 地址	与后端服务器通信

> 注意：
>
> `IPConfig-3` 不与任何公用 IP 地址相关联。

示意图：拓扑

以下是用例的直观表示。



> 注意：
>
> 在多 NIC、多 IP Azure NetScaler VPX 部署中，与主（第一个）网卡的主要（第一个）`IPConfig` 关联的私有 IP 会自动添加为设备的管理 NSIP。而与 `IPConfigs` 关联的其余专用 IP 地址，需要使用 `add ns ip` 命令作为 VIP 或 SNIP 添加到 VPX 实例中，具体取决于您的要求。

开始之前的准备工作

开始之前，请按照此链接上给定的步骤操作来创建 VPX 实例：

配置 NetScaler VPX 独立实例

对于此用例，创建了 NSDoc0330VM VPX 实例。

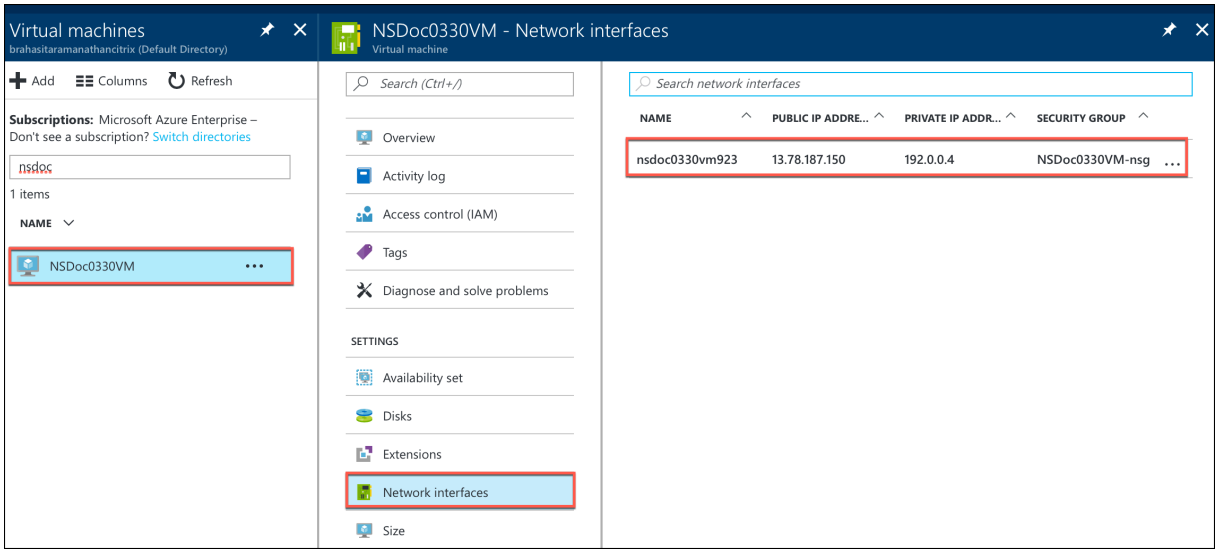
为处于独立模式的 **NetScaler VPX** 实例配置多个 **IP** 地址的过程。

要在独立模式下为 NetScaler VPX 设备配置多个 IP 地址：

1. 向 VM 添加 IP 地址
2. 配置 NetScaler 拥有的 IP 地址

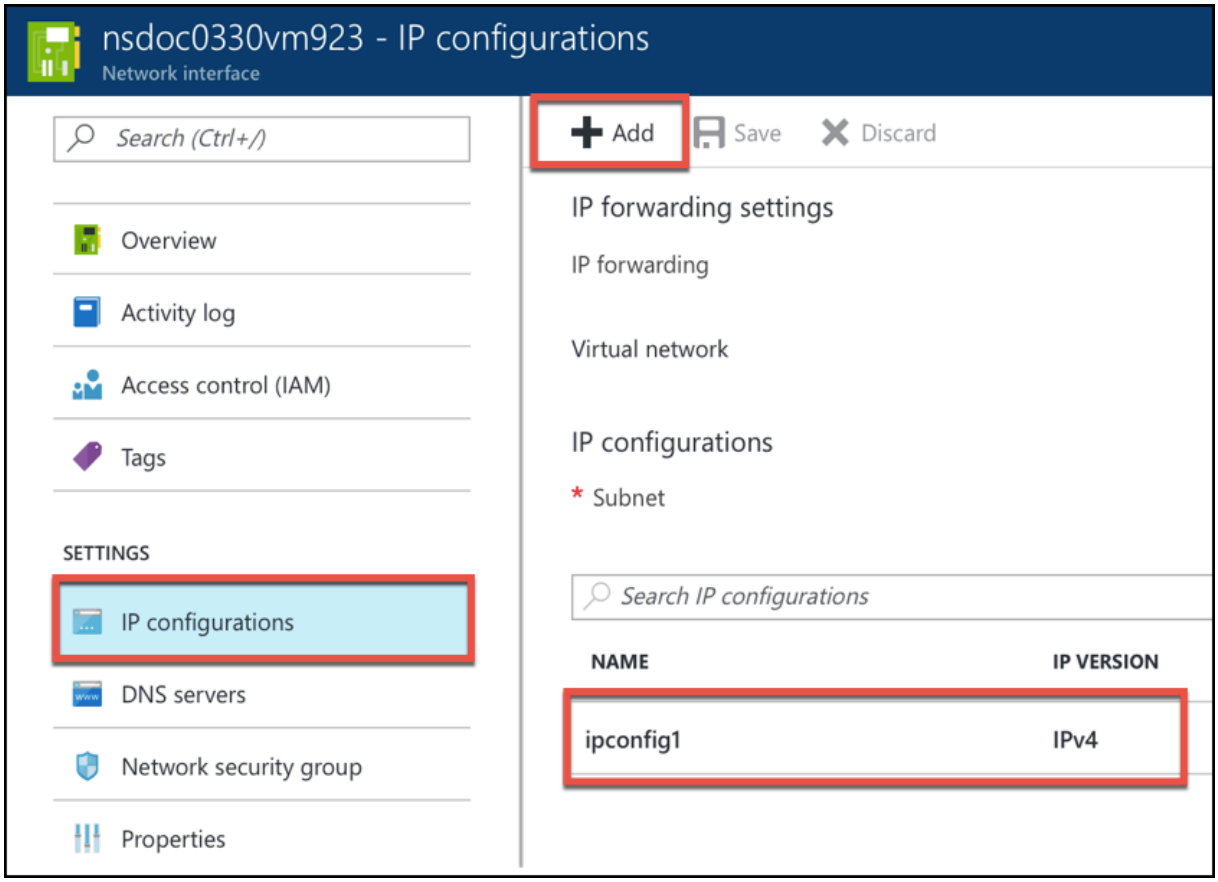
步骤 **1**：向 VM 添加 IP 地址

1. 在门户中，单击 **More services**（更多服务）**>** 在过滤器框中键入 **virtual machines**（虚拟机），然后单击 **Virtual machines**（虚拟机）。
2. 在 **Virtual machines**（虚拟机）边栏中，单击要向其添加 IP 地址的 VM。单击显示的虚拟机边栏中的 **Network interfaces**（网络接口），然后选择网络接口。



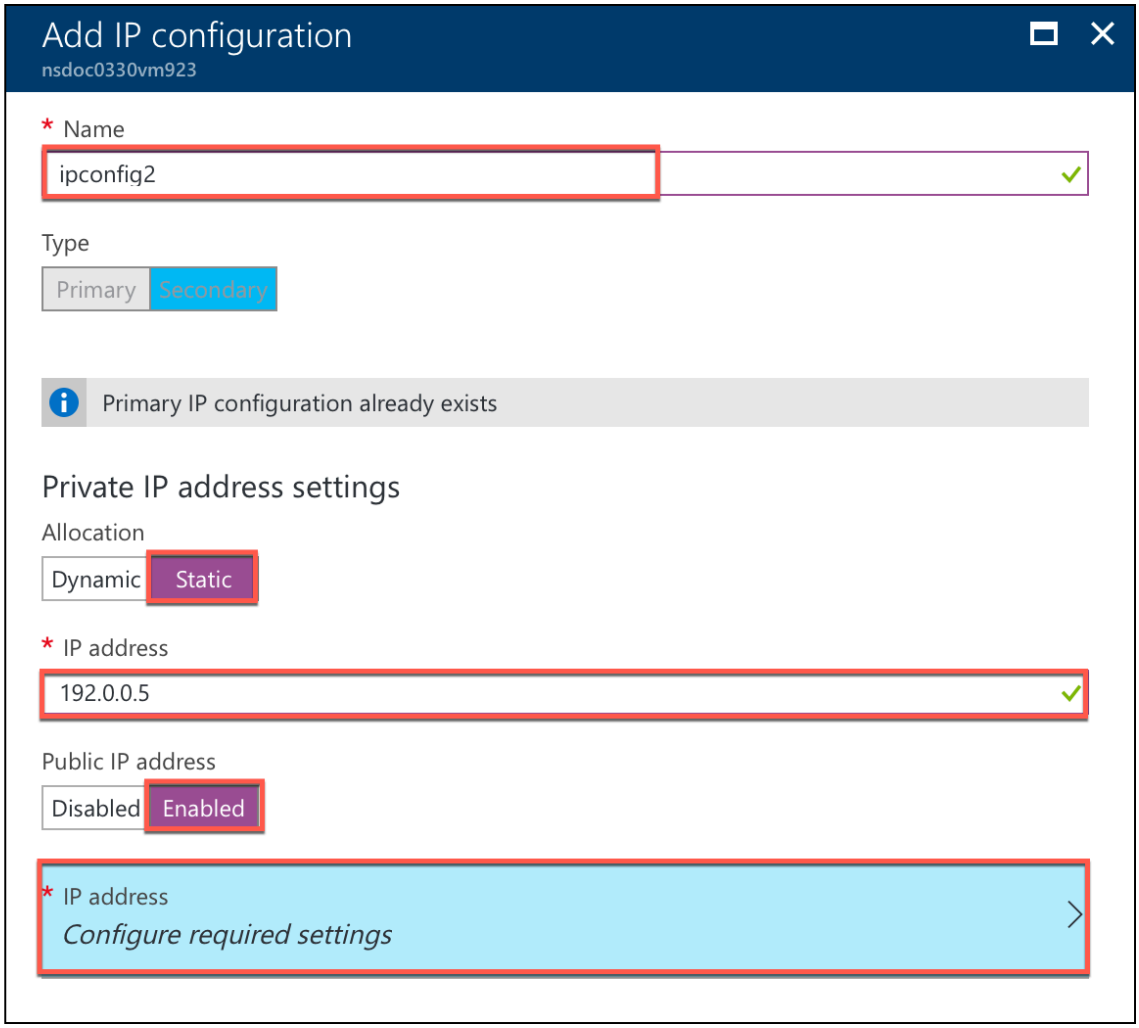
在为所选 NIC 显示的刀片式服务器中，单击 **IP configurations**（IP 配置）。此时将显示创建 VM **ipconfig1** 时分配的现有 IP 配置。对于此用例，请确保与 ipconfig1 相关联的 IP 地址是静态的。然后，创建另外两个 IP 配置：ipconfig2 (VIP) 和 ipconfig3 (SNIP)。

要创建更多 `ipconfigs`，请创建 **Add**（添加）。



在 **Add IP configuration**（添加 IP 配置）窗口中，输入 **Name**（名称），指定分配方法 **Static**（静态），输入 IP 地址（对于此用例为 192.0.0.5），然后启用 **Public IP address**（公用 IP 地址）。

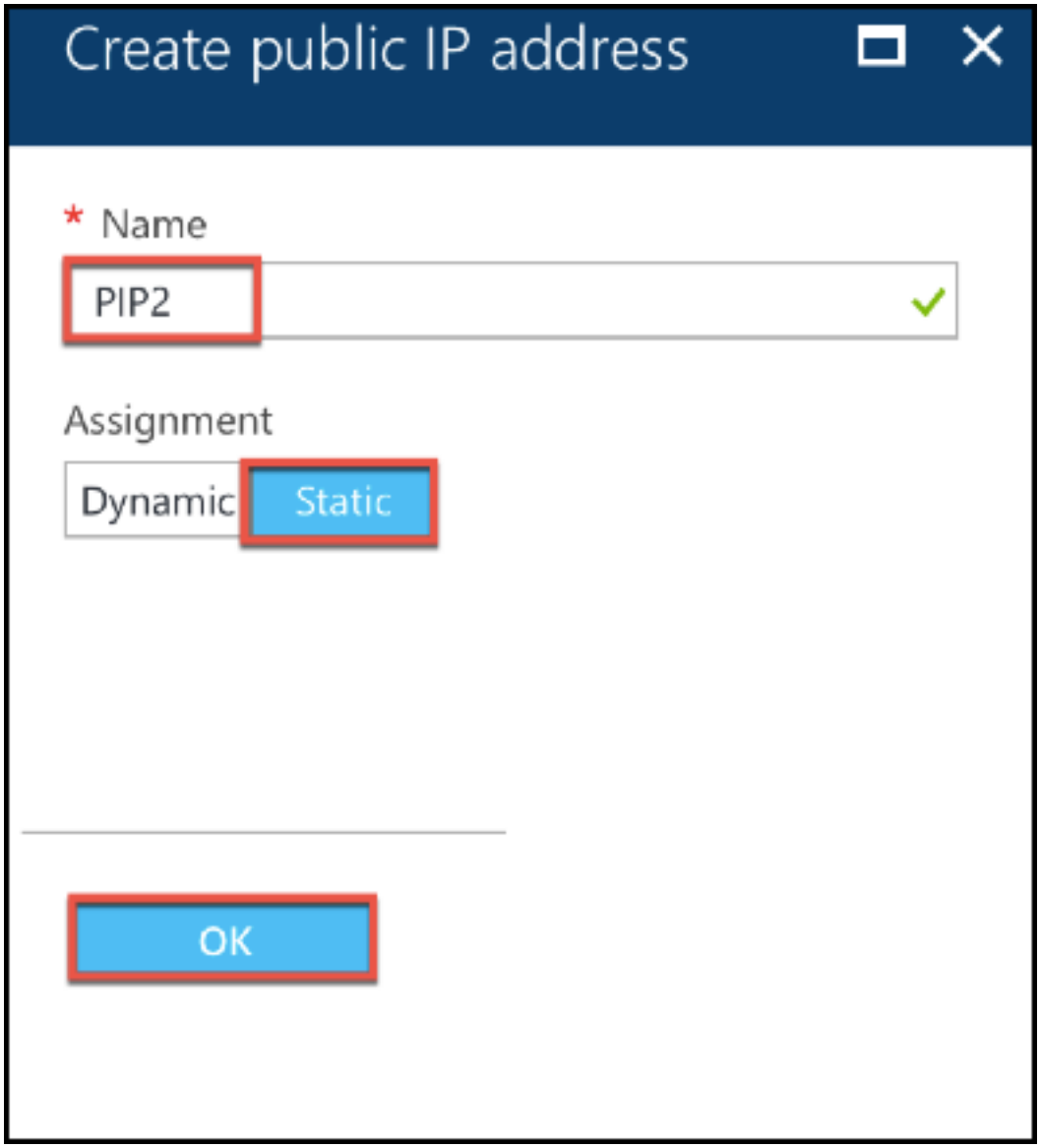
> 注意：
>
> 在添加静态专用 IP 地址之前，请检查 IP 地址可用性，并确保该 IP 地址属于 NIC 附加到的同一子网。



然后，单击 **Configure required settings**（配置所需设置）为 ipconfig2 创建静态公用 IP 地址。

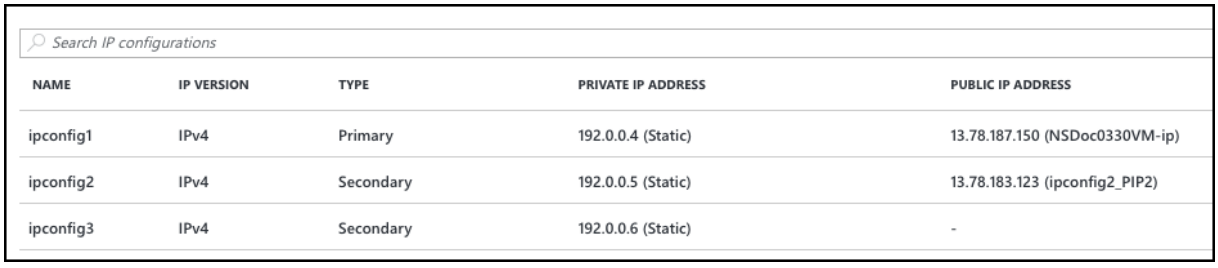
默认情况下，公用 IP 是动态的。为了确保 VM 始终使用同一公用 IP 地址，请创建一个静态公用 IP。

在 “Create public IP address”（创建公用 IP 地址）边栏中，添加名称，在 “Assignment”（分配）下方单击 **Static**（静态）。然后单击 **OK**（确定）。



> 注意：
>
> 即使您将分配方法设置为静态，您也不能指定分配给公用 IP 资源的实际 IP 地址。而是从创建资源的 Azure 位置中的可用 IP 地址池中分配地址。

按照这些步骤为 ipconfig3 再添加一个 IP 配置。公用 IP 不是必需的。



步骤 **2**：配置 **NetScaler** 自有 **IP** 地址

使用 GUI 或命令 `add ns ip` 配置 NetScaler 拥有的 IP 地址。有关更多信息，请参阅 配置 NetScaler 拥有的 IP 地址。

使用多个 **IP** 地址和 **NIC** 配置高可用性设置

October 17, 2024

在 Microsoft Azure 部署中，通过使用 Azure 负载均衡器 (ALB) 实现两个 NetScaler VPX 实例的高可用性配置。这是通过在 ALB 上配置一个运行状况探测来实现的，该探测通过每 5 秒向主实例和辅助实例发送一次运行状况探测来监视每个 VPX 实例。

在此设置中，只有主节点响应运行状况探测，而辅助节点不响应运行状况探测。一旦主实例将响应发送到运行状况探测，ALB 将开始向实例发送数据流量。如果主实例错过两个连续的运行状况探测，则 ALB 不会将流量重定向至该实例。发生故障转移时，新的主实例开始响应运行状况探测，且 ALB 将流量重定向至该实例。标准 VPX 高可用性故障转移时间为三秒。切换流量可能需要的故障转移总时间最长为 13 秒。

可以在 Azure 上的主动-被动高可用性 (HA) 设置中部署一对具有多个 NIC 的 NetScaler VPX 实例。每个 NIC 都可以包含多个 IP 地址。

以下选项可用于多 NIC 高可用性部署：

- 使用 Azure 可用性集实现高可用性
- 使用 Azure 可用性区域实现高可用性

有关 Azure 可用性集和可用区的更多信息，请参阅 Azure 文档 管理 Linux 虚拟机的可用性。

使用可用性集实现高可用性

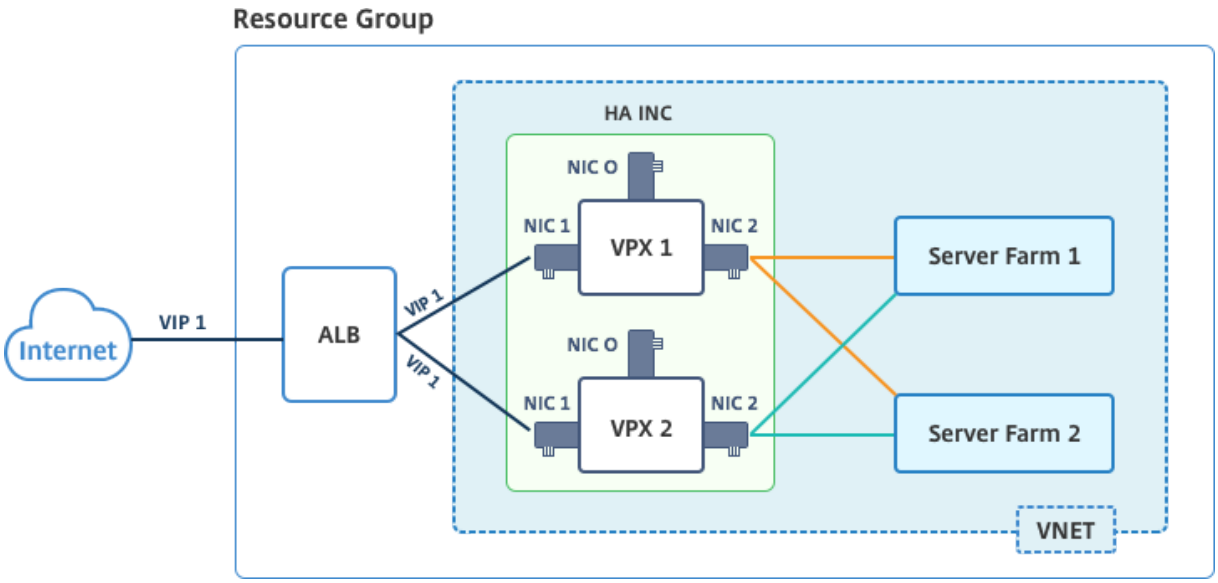
使用可用性集的高可用性设置必须满足以下要求：

- HA 独立网络配置 (INC) 配置
- 处于直接服务器返回 (DSR) 模式的 Azure 负载均衡器 (ALB)

所有流量均通过主节点。在主节点发生故障前，辅助节点一直处于备用模式。

> 注意：
>
> 要在 Azure 云上部署 NetScaler VPX 高可用性部署，您需要一个可以在两个 VPX 节点之间移动的浮动公共 IP (PIP)。Azure 负载均衡器 (ALB) 提供浮动 PIP，在发生故障转移时自动移动到第二个节点。

示意图：使用 Azure 可用性集的高可用性部署体系结构示例



在主动-被动部署中，ALB 前端公用 IP (PIP) 地址作为 VIP 地址添加在每个 VPX 节点中。在 HA-INC 配置中，VIP 地址是浮动的，而 SNIP 地址是实例特定的。

可以通过以下两种方式在主动-被动高可用性模式下部署 VPX 对：

- **NetScaler VPX** 标准高可用性模板：使用此选项配置 HA 对，默认选项为三个子网和六个 NIC。
- **Windows PowerShell** 命令：此选项用于根据您的子网和 NIC 要求来配置高可用性对。

本主题介绍了如何使用 Citrix 模板在主动-被动高可用性设置中部署 VPX 对。如果您想使用 PowerShell 命令，请参阅使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的 HA 设置。

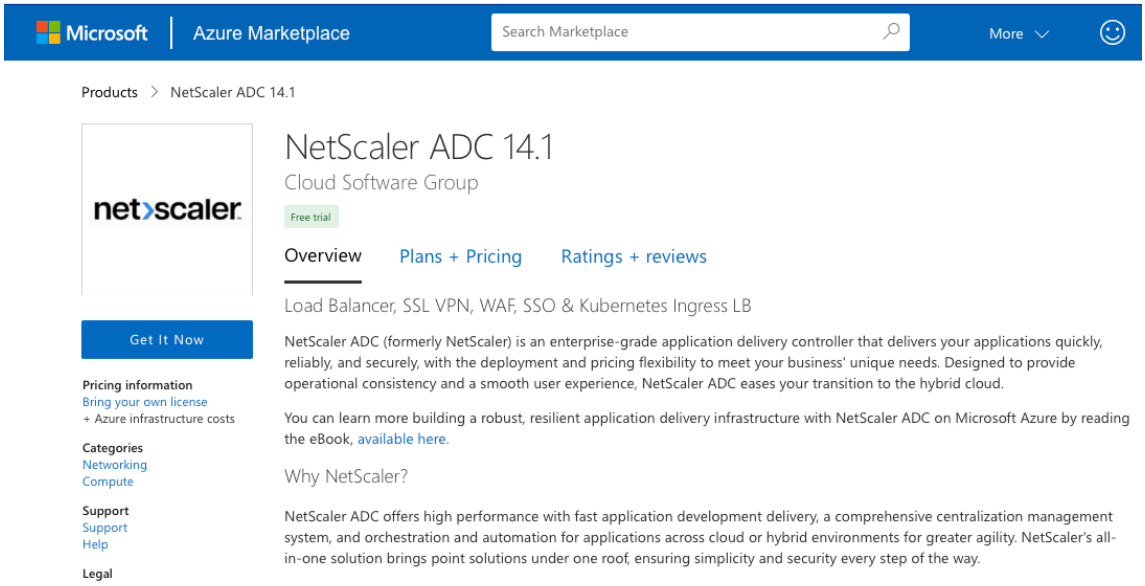
使用 **NetScaler** 高可用性模板配置 **HA-INC** 节点

可以通过使用标准模板快速高效地部署处于 HA-INC 模式的一对 VPX 实例。模板会创建两个节点，使用三个子网和六个 NIC。子网用于管理、客户端和服务器端流量，每个子网均有两个 NIC 用于两个 VPX 实例。

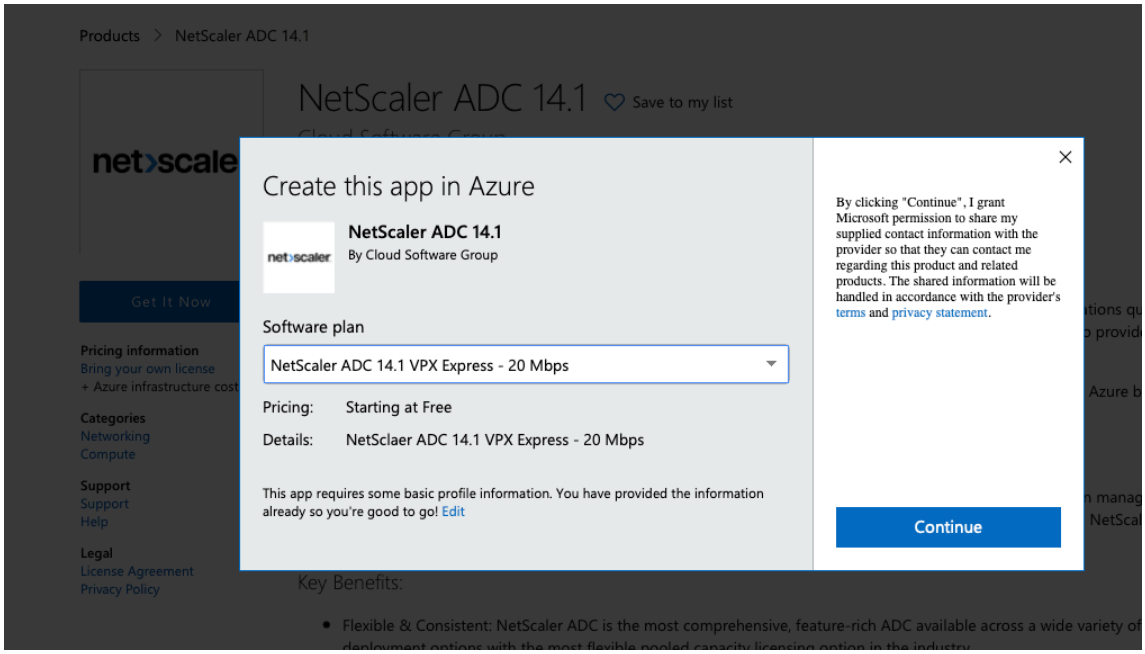
您可以在 Azure 市场获取 NetScaler HA 对模板。

完成以下步骤，通过使用 Azure 可用性集启动模板并部署高可用性 VPX 对。

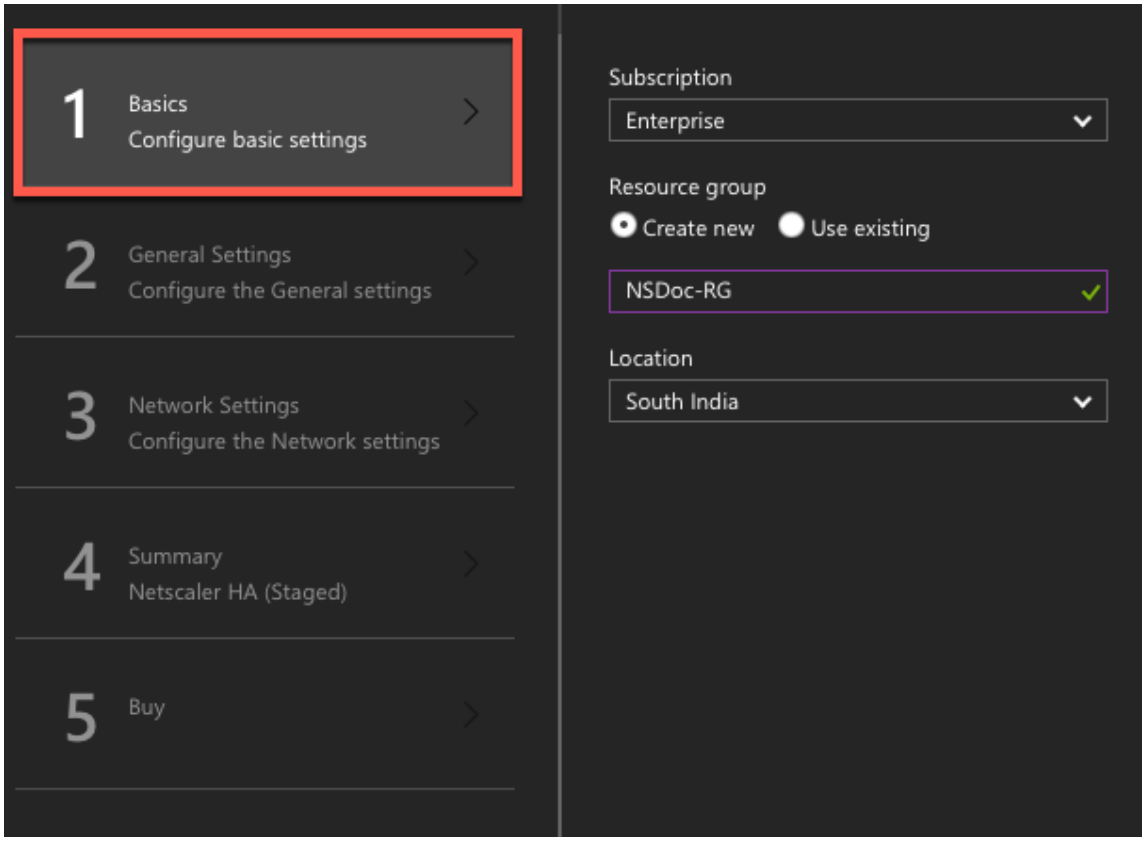
1. 在 Azure 市场中搜索 **NetScaler**。



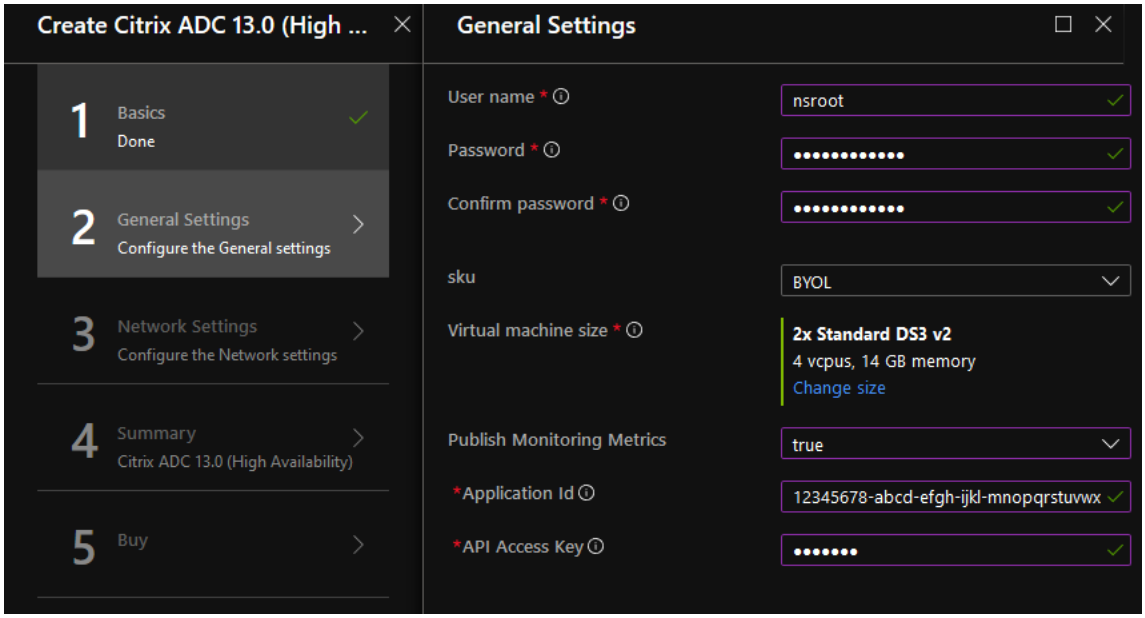
2. 单击 **GET IT NOW**（立即获取）。
3. 选择所需的高可用性部署以及许可证，然后单击 **Continue**（继续）。



4. 此时将显示 **Basics**（基本）页面。创建一个资源组并选择 **OK**（确定）。



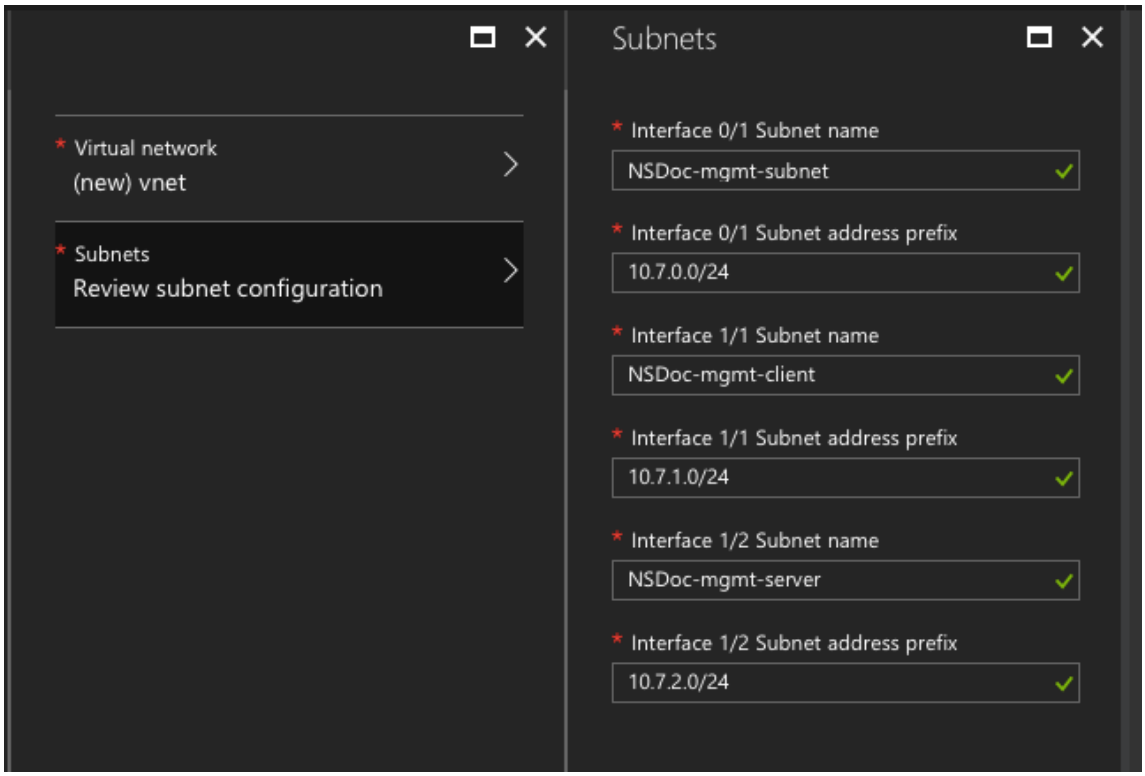
5. 此时将显示 **General Settings**（常规设置）页面。键入详细信息并选择 **OK**（确定）。



> 注意：
>
> 默认情况下，**Publishing Monitoring Metrics**（发布监视指标）选项设置为 **false**。如果要启用此选项，请选择 **true**。创建可访问资源的 Azure Active Directory (ADD) 应用程序和服务主体。将贡献者

> 角色分配给新创建的 AAD 应用程序。有关更多信息，请参阅 使用门户创建可以访问资源的 Azure Active Directory 应用程序和服务委托人。

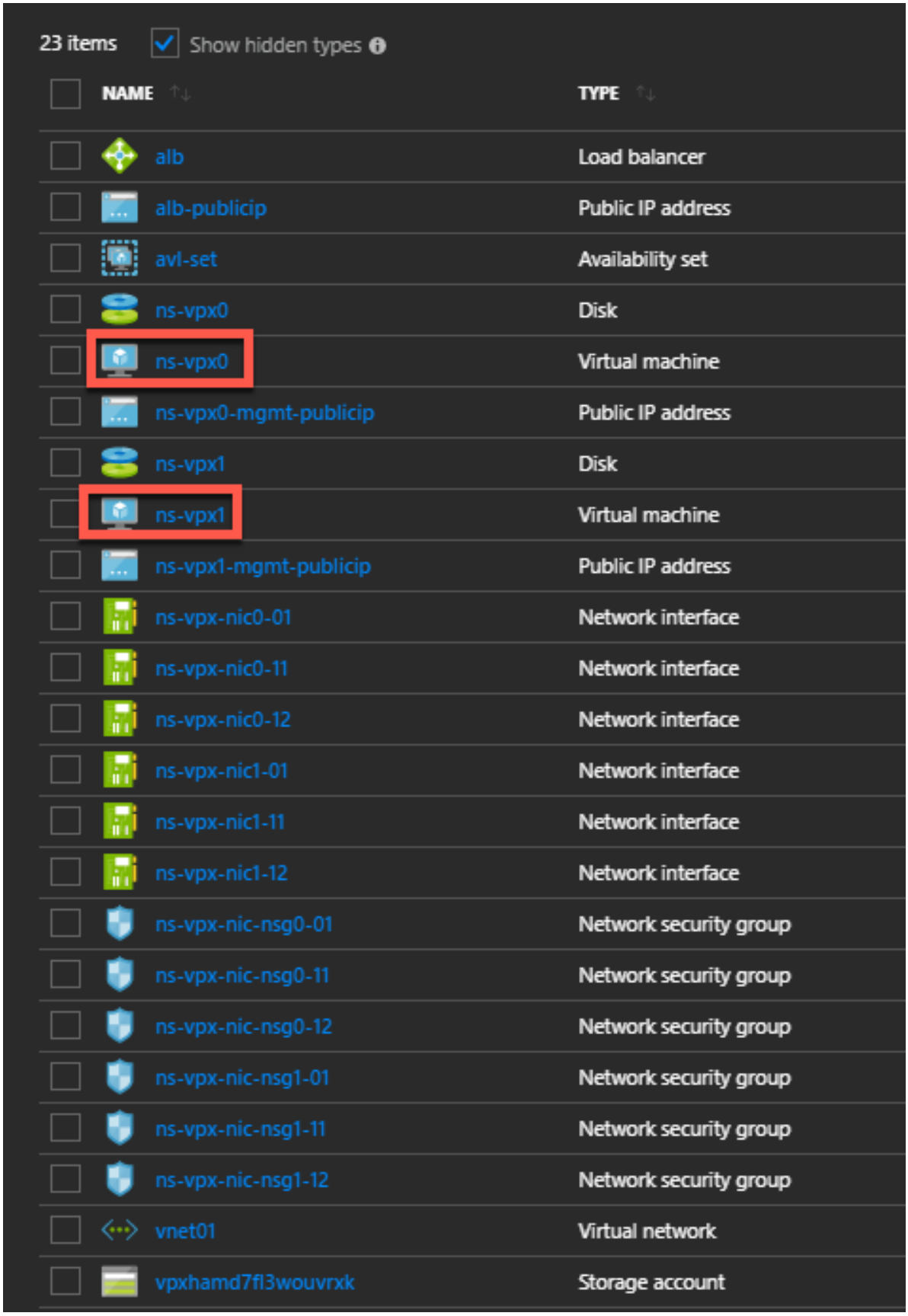
6. 此时将显示 **Network Setting**（网络设置）页面。检查 VNet 和子网配置，编辑所需的设置，然后选择 **OK**（确定）。



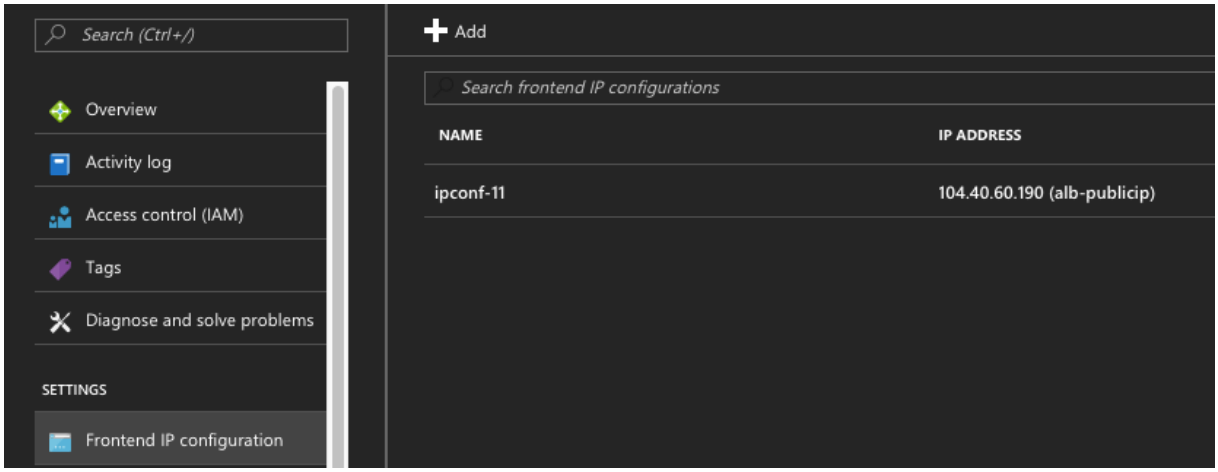
7. 此时将显示摘要页面。检查配置并相应地进行编辑。选择确定进行确认。
8. 此时将显示 **Buy**（购买）页面。选择 **Purchase**（购买）以完成部署。

可能需要一段时间采用所需配置来创建 Azure 资源组。完成后，选择 Azure 门户中的 资源组 以查看配置详细信息，例如 LB 规则、后端池、运行状况探测。高可用性对显示为 ns-vpx0 和 ns-vpx1。

如果需要对您的高可用性设置进行进一步修改（例如，创建更多安全规则和端口），可以在 Azure 门户中完成。



然后，需要在主节点上为负载平衡虚拟服务器配置 **ALB** 前端公用 **IP (PIP)** 地址。要查找 ALB PIP，请选择“ALB”> **Frontend IP configuration**（前端 IP 配置）。



有关如何配置负载平衡虚拟服务器的详细信息，请参阅资源部分。

资源：

以下链接提供了与 HA 部署和虚拟服务器配置相关的其他信息：

- 在不同的子网中配置高可用性节点
- 设置基本负载平衡

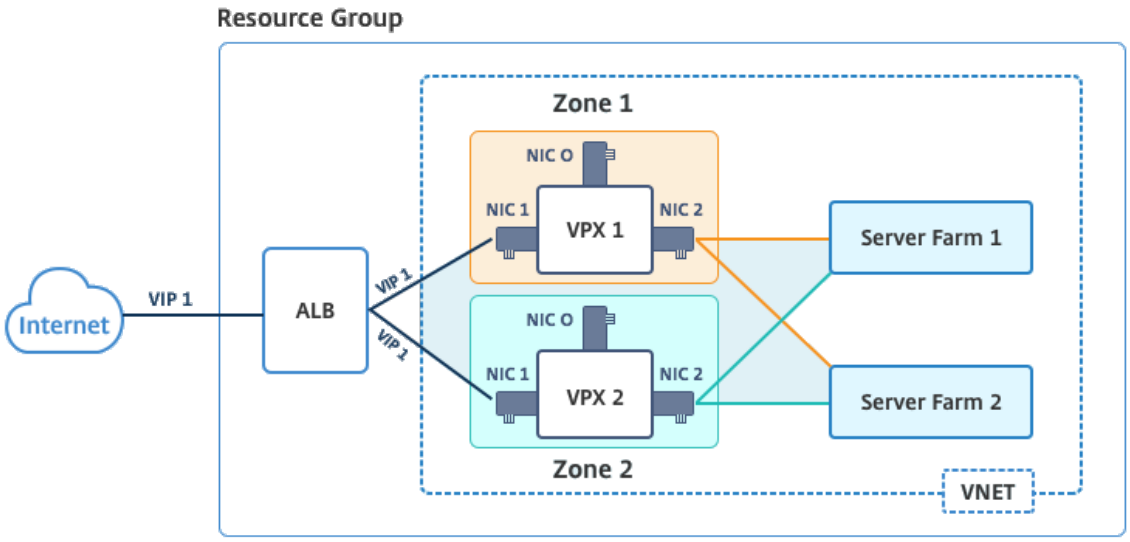
相关资源：

- 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置
- 在 Azure 上的主动-备用高可用性部署中配置 GSLB

使用可用性区域实现高可用性

Azure 可用性区域是 Azure 区域内的故障隔离位置，可提供冗余电源、冷却和网络连接，并提高恢复能力。只有特定的 Azure 区域支持可用性区域。有关支持可用区域的区域的更多信息，请参阅 Azure 文档 Azure 中什么是可用区？.

示意图：使用 Azure 可用性区域的高可用性部署体系结构示例



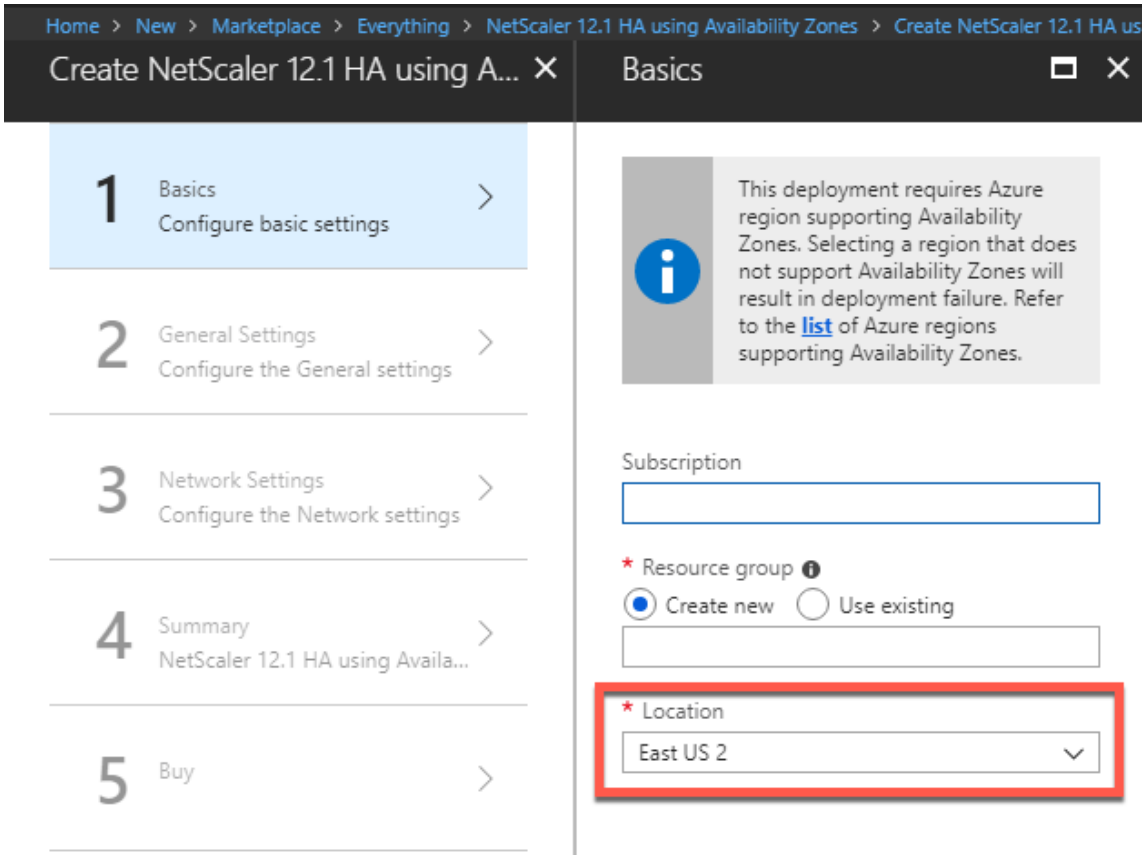
通过使用 Azure 应用商店中提供的名为“NetScaler 13.0 HA using Availability Zones”的模板，可以在高可用性模式下部署 VPX 对。

完成以下步骤，通过使用 Azure 可用性区域启动模板并部署高可用性 VPX 对。

1. 在 Azure 应用商店中，选择并启动 Citrix 解决方案模板。

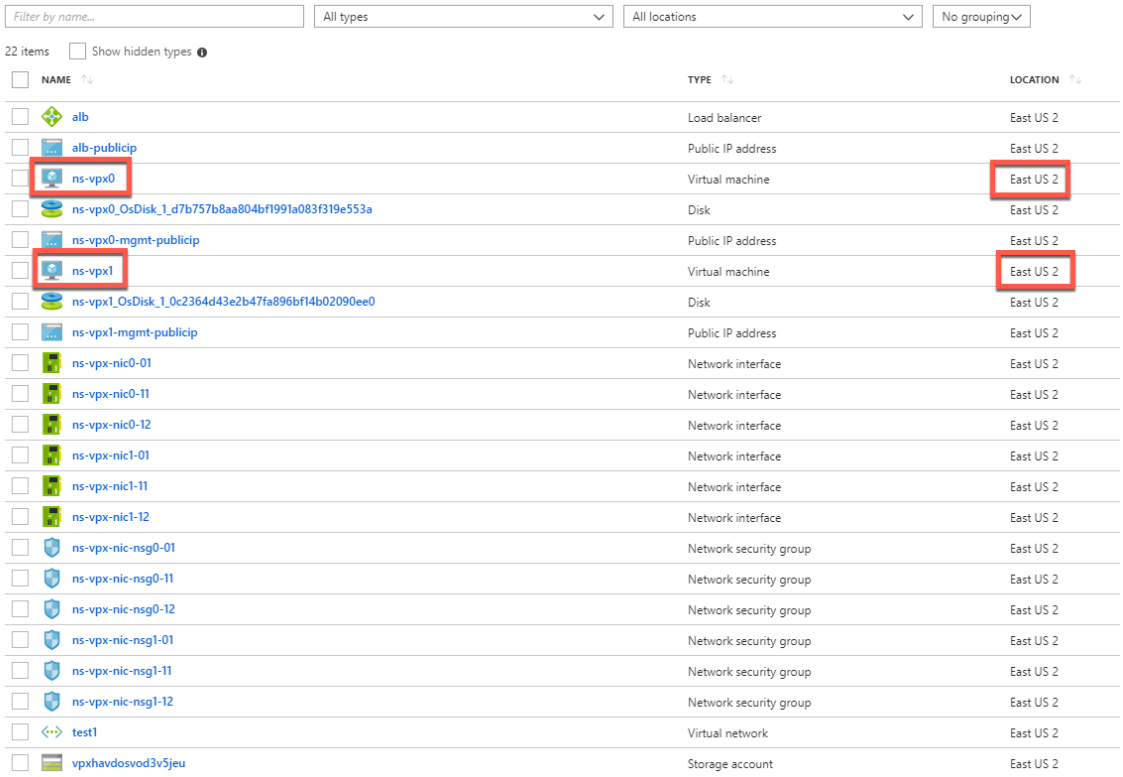
2. 确保部署类型为“Resource Manager”（资源管理器），并选择 **Create**（创建）。
3. 此时将显示 **Basics**（基本）页面。输入详细信息，然后单击 **OK**（确定）。

> 注意：
>
> 确保选择支持可用性区域的 Azure 区域。有关支持可用区域的区域的更多信息，请参阅 Azure 文档 Azure 中什么是可用区?



4. 此时将显示 **General Settings**（常规设置）页面。键入详细信息并选择 **OK**（确定）。
5. 此时将显示 **Network Settings**（网络设置）页面。检查 VNet 和子网配置，编辑所需的设置，然后选择 **OK**（确定）。
6. 此时将显示摘要页面。检查配置并相应地进行编辑。选择确定进行确认。
7. 此时将显示 **Buy**（购买）页面。选择 **Purchase**（购买）以完成部署。

   可能需要一段时间采用所需配置来创建 Azure 资源组。完成后，选择 **Resource Group**（资源组）以查看 Azure 门户中的配置详细信息，例如 LB 规则、后端池、运行状况探测等。高可用性对显示为 ns-vpx0 和 ns-vpx1。此外，还可以在 **Location**（位置）列下查看位置。



如果需要对您的高可用性设置进行进一步修改（例如，创建更多安全规则和端口），可以在 Azure 门户中完成。

使用 **Azure** 监视器中的指标监视实例

您可以使用 Azure 监视器数据平台中的指标来监视一组 NetScaler VPX 资源，例如 CPU、内存利用率和吞吐量。指标服务实时监视在 Azure 上运行的 NetScaler VPX 资源。可以使用 **Metrics Explorer**（指标资源管理器）访问收集的数据。有关更多信息，请参阅 Azure 监视器指标概述。

注意事项

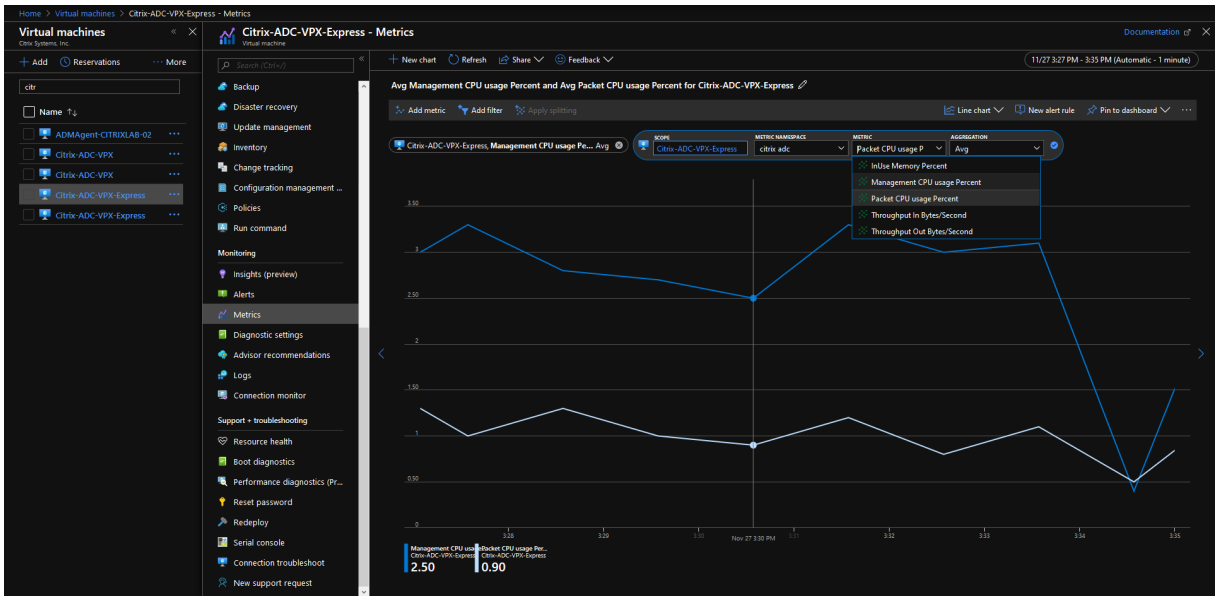
- 如果您使用 Azure 市场优惠在 Azure 上部署 NetScaler VPX 实例，则默认情况下，指标服务处于禁用状态。
- Azure CLI 不支持指标服务。
- 可用于 CPU（管理和数据包 CPU 使用率）、内存和吞吐量（入站和出站）的指标。

如何在 **Azure** 监视器中查看指标

要在 Azure 监视器中查看实例的指标，请执行以下步骤：

1. 登录 **Azure Portal**（**Azure** 门户）**> Virtual Machines**（虚拟机）。
2. 选择作为主节点的虚拟机。

3. 在 **Monitoring**（就爱您是）部分中，单击 **Metrics**（指标）。
4. 从 指标命名空间 下拉菜单中，单击 **NetScaler**。
5. 在 **Metrics**（指标）下拉菜单中的 **All metrics**（所有指标）下，单击要查看的指标。
6. 单击 **Add metric**（添加指标）可在同一图表上查看另一个指标。使用“Chart options”（图表选项）自定义您的图表。



使用 **PowerShell** 命令配置具有多个 **IP** 地址和 **NIC** 的高可用性设置

October 17, 2024

可以在 Azure 上的主动-被动高可用性 (HA) 设置中部署一对具有多个 NIC 的 NetScaler VPX 实例。每个 NIC 都可以包含多个 IP 地址。

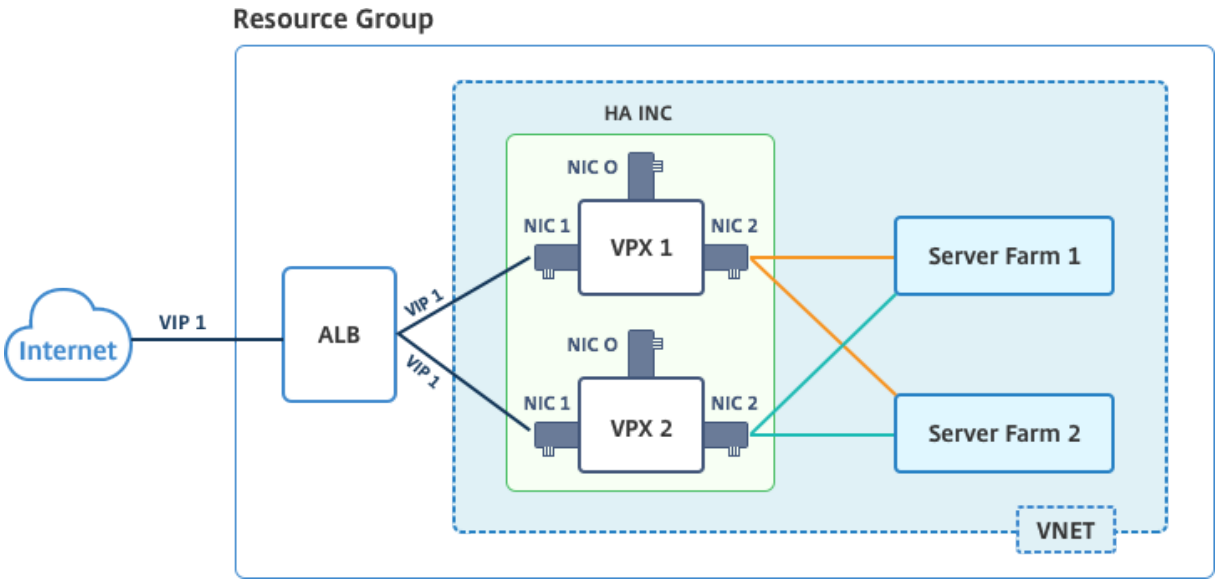
主动-被动部署需要：

- HA 独立网络配置 (INC) 配置
- 处于直接服务器返回 (DSR) 模式的 Azure 负载均衡器 (ALB)

所有流量均通过主节点。在主节点发生故障前，辅助节点一直处于备用模式。

> 注意：
>
> 要在 Azure 云上部署 NetScaler VPX 高可用性部署，您需要一个可以在两个高可用性节点之间移动的浮动公共 IP (PIP)。Azure 负载均衡器 (ALB) 提供浮动 PIP，在发生故障转移时自动移动到第二个节点。

示意图：主动-被动部署体系结构示例



在主动-被动部署中，ALB 浮动公用 IP (PIP) 地址作为 VIP 地址添加在每个 VPX 节点中。在 HA-INC 配置中，VIP 地址是浮动的，而 SNIP 地址是实例特定的。

ALB 通过每 5 秒发送一次运行状况探测来监视每个 VPX 实例，并将流量仅重定向至按固定时间间隔发送运行状况探测响应的实例。因此，在 HA 设置中，主节点响应运行状况探测，而辅助节点不响应。如果主实例错过两个连续的运行状况探测，则 ALB 不会将流量重定向至该实例。发生故障转移时，新的主实例开始响应运行状况探测，且 ALB 将流量重定向至该实例。标准 VPX 高可用性故障转移时间为三秒。切换流量可能需要的故障转移总时间最长为 13 秒。

可以通过以下两种方式在主动-被动高可用性设置中部署 VPX 对：

- **NetScaler VPX** 标准高可用性模板：使用此选项配置 HA 对，默认选项为三个子网和六个 NIC。
- **Windows PowerShell** 命令：此选项用于根据您的子网和 NIC 要求来配置高可用性对。

本主题介绍了如何使用 PowerShell 命令在主动-被动高可用性设置中部署 VPX 对。如果您想使用 NetScaler VPX 标准 HA 模板，请参阅 配置具有多个 IP 地址和 NIC 的 HA 设置。

使用 **PowerShell** 命令配置 **HA-INC** 节点

场景：**HA-INC PowerShell** 部署

在这种情况下，您可以使用表中给出的拓扑来部署 NetScaler VPX 对。每个 VPX 实例均包含三个 NIC，每个 NIC 均部署在不同的子网中。每个 NIC 均分配了一个 IP 配置。

ALB	VPX1	VPX2
ALB 与公用 IP 3 (pip3) 关联	管理 IP 配置了 IPConfig1，其中包括一个公用 IP (pip1) 和一个专用 IP (12.5.2.24); nic1; Mgmtsubnet=12.5.2.0/24	管理 IP 配置了 IPConfig5，其中包括一个公用 IP (pip3) 和一个专用 IP (12.5.2.26);nic4;Mgmtsubnet=12.5.2.0/24
配置的 LB 规则和端口包括 HTTP (80)、SSL (443)、运行状况探测 (9000)	客户端 IP 配置了 IPConfig3，其中包括一个专用 IP(12.5.1.27);nic2; FrontEndsubet=12.5.1.0/24	客户端 IP 配置了 IPConfig7，其中包括一个专用 IP (12.5.1.28);nic5;FrontEndsubet=12.5.1.0/24
-	服务器端 IP 配置了 IPConfig4，其中包括一个专用 IP (12.5.3.24); nic3;BackendSubnet=12.5.3.0/24	服务器端 IP 配置了 IPConfig8，其中包括一个专用 IP (12.5.3.28);nic6;BackendSubnet=12.5.3.0/24
-	NSG 的规则和端口包括：SSH (22)、HTTP (80)、HTTPS (443)	-

参数设置

在此场景中将使用以下参数设置。

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$publisher = “Citrix”

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=” latest”

$pubIPName1=” VPX1MGMT”

$pubIPName2=” VPX2MGMT”

$pubIPName3=” ALBPIP”

$domName1=” vpx1dns”

$domName2=” vpx2dns”

$domName3=” vpxalbdns”

$vmNamePrefix=” VPXMultiIPALB”

$osDiskSuffix1=” osmultiipalbdiskdb1”

$osDiskSuffix2=” osmultiipalbdiskdb2”

$lbName= “MultiIPALB”

$frontEndConfigName1= “FrontEndIP”

$backendPoolName1= “BackendPoolHttp”

$lbRuleName1= “LBRuleHttp”

$healthProbeName= “HealthProbe”

$nsgName=” NSG-MultiIP-ALB”

$rule1Name=” Inbound-HTTP”

$rule2Name=” Inbound-HTTPS”

$rule3Name=” Inbound-SSH”

要完成部署，请使用 PowerShell 命令完成以下步骤：

1. 创建资源组、存储帐户和可用性集
2. 创建网络安全组并添加规则
3. 创建虚拟网络和三个子网

4. 创建公用 IP 地址
5. 为 VPX1 创建 IP 配置
6. 为 VPX2 创建 IP 配置
7. 为 VPX1 创建 NIC
8. 为 VPX2 创建 NIC
9. 创建 VPX1
10. 创建 VPX2
11. 创建 ALB

创建资源组、存储帐户和可用性集。

```
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
```

创建网络安全组并添加规则。

```
$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 "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 110


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 443


$rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
    Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 120


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 22


```



```
$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
    Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
    $rule3
```

创建虚拟网络和三个子网。

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
    parameter value should be as per your requirement)


$mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $mgmtSubnetName -AddressPrefix $mgmtSubnetRange


$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backEndSubnetName -AddressPrefix $backEndSubnetRange


$vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vNetAddressRange -
    Subnet $frontendSubnet,$backendSubnet, $mgmtSubnet


$subnetName ="frontEndSubnet"


 \$subnet1=\$vnet.Subnets|?{
\$\_.Name -eq \$subnetName }


$subnetName="backEndSubnet"


 \$subnet2=\$vnet.Subnets|?{
\$\_.Name -eq \$subnetName }


$subnetName="mgmtSubnet"


 \$subnet3=\$vnet.Subnets|?{
\$\_.Name -eq \$subnetName }
```

创建公用 **IP** 地址。

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
     $rgName -DomainNameLabel $domName1 -Location $locName -
    AllocationMethod Dynamic

$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
```

为 **VPX1** 创建 **IP** 配置。

```
1   $IpConfigName1 = "IPConfig1"
2
3
4   $IPAddress = "12.5.2.24"
5
6
7   $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
    $pip1 -Primary
8
9
10  $IPConfigName3="IPConfig-3"
11
12
13  $IPAddress="12.5.1.27"
14
15
16  $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19  $IPConfigName4 = "IPConfig-4"
20
21
22  $IPAddress = "12.5.3.24"
23
24
25  $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
        -Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

为 **VPX2** 创建 **IP** 配置。

```
1   $IpConfigName5 = "IPConfig5"
2
3
4   $IPAddress="12.5.2.26"
5
6
7   $IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress
    $pip2 -Primary
8
9
10  $IPConfigName7="IPConfig-7"
```



```
11
12
13    $IPAddress="12.5.1.28"
14
15
16    $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
          Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19    $IPConfigName8="IPConfig-8"
20
21
22    $IPAddress="12.5.3.28"
23
24
25    $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
          Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

为 **VPX1** 创建 **NIC**。

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

为 **VPX2** 创建 **NIC**。

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

创建 **VPX1**。

此步骤包括以下子步骤：

- 创建 VM 配置对象
- 设置凭据、操作系统和映像
- 添加 NIC
- 指定操作系统磁盘并创建 VM

```
$suffixNumber = 1

$vmName=$vmNamePrefix + $suffixNumber

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id

$cred=Get-Credential -Message "Type the name and password for
    VPX login."

$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
     $publisher -Offer $offer -Skus $sku -Version $version

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1
    .Id -Primary

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2
    .Id

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3
    .Id

$osDiskName=$vmName + "-" + $osDiskSuffix1

$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +
     "vhds/" + $osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -
    VhdUri $osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product
    $offer -Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -
    Location $locName
```

创建 **VPX2**。

```
```
  $suffixNumber=2

  $vmName=$vmNamePrefix + $suffixNumber
```

 
```

```
6
7
8    $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avSet.Id
9
10
11   $cred=Get-Credential -Message "Type the name and password for VPX
        login."
12
13
14   $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
        ComputerName $vmName -Credential $cred
15
16
17   $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
        $publisher -Offer $offer -Skus $sku -Version $version
18
19
20   $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
        Primary
21
22
23   $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
26   $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
29   $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32   $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
        /" + $osDiskName + ".vhd"
33
34
35   $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
         $osVhdUri -CreateOption fromImage
36
37
38   Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
         -Name $sku
39
40
41   New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
        $locName
42 ```
```

要查看分配给 NIC 的专用和公用 IP 地址，请键入以下命令：

```
1  ```
2    $nic1.IPConfig
3
4
```



```
  $nic2.IPConfig


  $nic3.IPConfig


  $nic4.IPConfig


  $nic5.IPConfig


  $nic6.IPConfig
```

创建 **Azure** 负载平衡 **(ALB)**。

此步骤包括以下子步骤：

- 创建前端 IP 配置
- 创建运行状况探测
- 创建后端地址池
- 创建负载平衡规则（HTTP 和 SSL）
- 使用前端 IP 配置、后端地址池和 LB 规则创建 ALB
- 将 IP 配置与后端池相关联

```
$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
```

成功部署了 NetScaler VPX 对后，登录每个 VPX 实例以配置 HA-INC、SNIP 和 VIP 地址。

1. 键入以下命令以添加 HA 节点。

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. 针对 VPX1 (NIC2) 和 VPX2 (NIC5)，将客户端 NIC 的专用 IP 地址添加为 SNIP

   ```
   添加nsip privateIPofNIC2 255.255.255.0 -type SNIP 添加nsip privateIPofNIC5
    255.255.255.0 -type SNIP
   ```

3. 在具有 ALB 的前端 IP 地址（公用 IP）的主节点上添加负载平衡虚拟服务器。

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

相关资源：

在 Azure 上的主动-备用高可用性部署中配置 GSLB

在 **Azure** 上部署 **NetScaler** 高可用性对，**ALB** 处于浮动 **IP** 禁用模式

October 17, 2024

可以在 Azure 上的主动-被动高可用性 (HA) 设置中部署一对具有多个 NIC 的 NetScaler VPX 实例。每个 NIC 可以包含多个 IP 地址。

主动-被动部署需要：

- HA 独立网络配置 (INC) 配置
- Azure 负载平衡器 (ALB) 具有：
  - 启用 IP 的浮动模式或直接服务器返回 (DSR) 模式
  - 浮动 IP 禁用模式

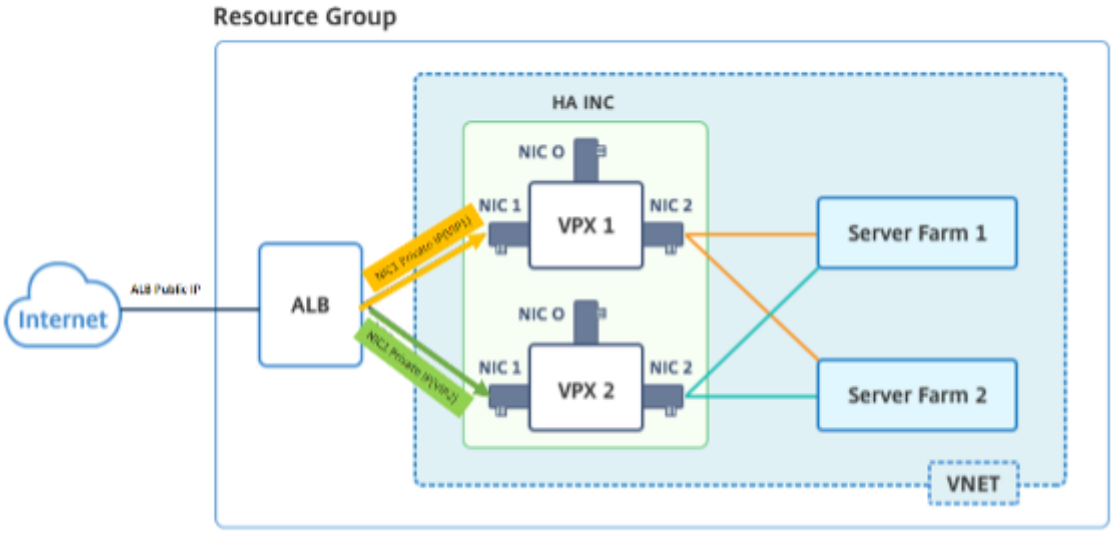
有关 ALB 浮动 IP 选项的更多信息，请参阅 Azure 文档。

如果要在启用 ALB 浮动 IP 的 Azure 上在主动-被动 HA 设置中部署 VPX 对，请参阅 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置。

ALB 处于浮动 IP 禁用模式的 HA 部署架构

在主动-被动部署中，每个实例的客户端接口的专用 IP 地址将作为 VIP 地址添加到每个 VPX 实例中。在 HA-INC 模式下进行配置，使用 IPset 共享 VIP 地址，而 SNIP 地址特定于实例。所有流量都通过主实例。辅助实例处于备用模式，直到主实例出现故障。

示意图：主动-被动部署体系结构示例



必备条件

在 Azure 上部署 NetScaler VPX 实例之前，您必须熟悉以下信息。

- Azure 术语和网络详细信息。有关更多信息，请参阅 Azure 术语。
- NetScaler 设备的工作原理。有关更多信息，请参阅 NetScaler 文档。
- NetScaler 联网。有关更多信息，请参阅 ADC 网络。
- Azure 负载平衡器和负载平衡规则配置。有关更多信息，请参阅 Azure ALB 文档。

如何在禁用 ALB 浮动 IP 的情况下在 Azure 上部署 VPX HA 对

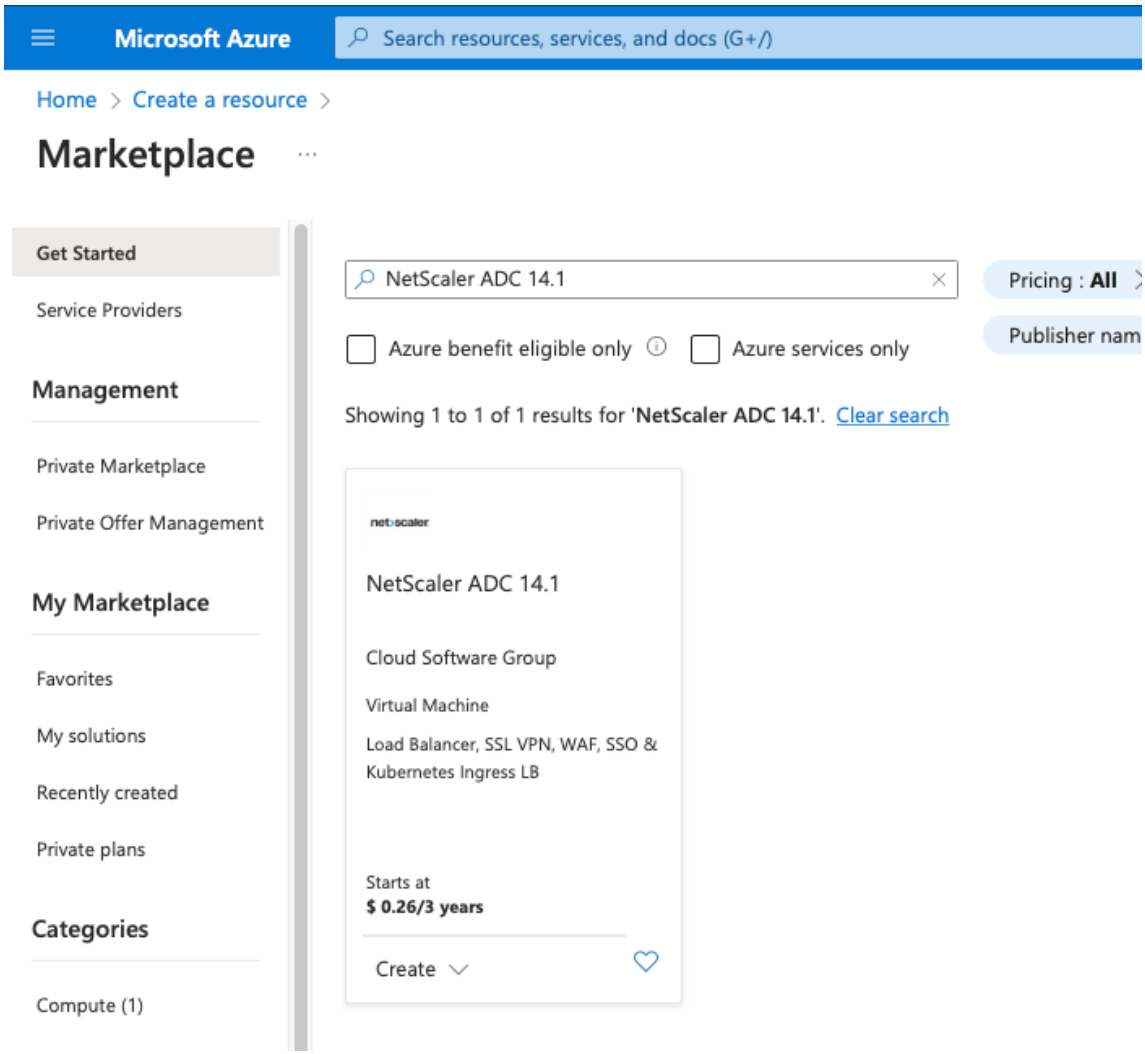
以下是 HA 和 ALB 部署步骤的摘要：

1. 在 Azure 上部署两个 VPX 实例（主实例和辅助实例）。
2. 在两个实例上添加客户端和服务器 NIC。
3. 部署禁用浮动 IP 模式的带负载均衡规则的 ALB。
4. 使用 NetScaler GUI 在两个实例上配置 HA 设置。

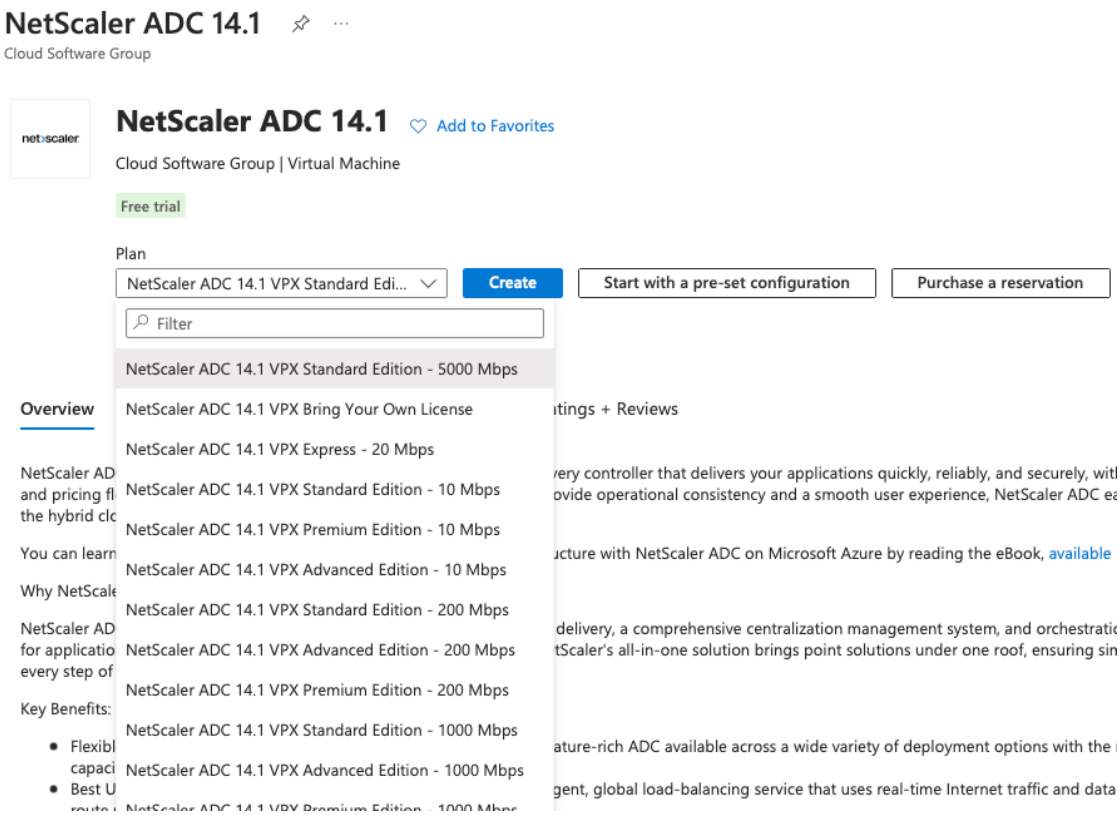
步骤 **1.** 步骤 **1.** 在 **Azure** 上部署两个 **VPX** 实例。

按照以下步骤创建两个 VPX 实例：

1. 从 Azure 市场中选择 NetScaler 版本（在本示例中，使用的是 NetScaler 版本 13.1）。

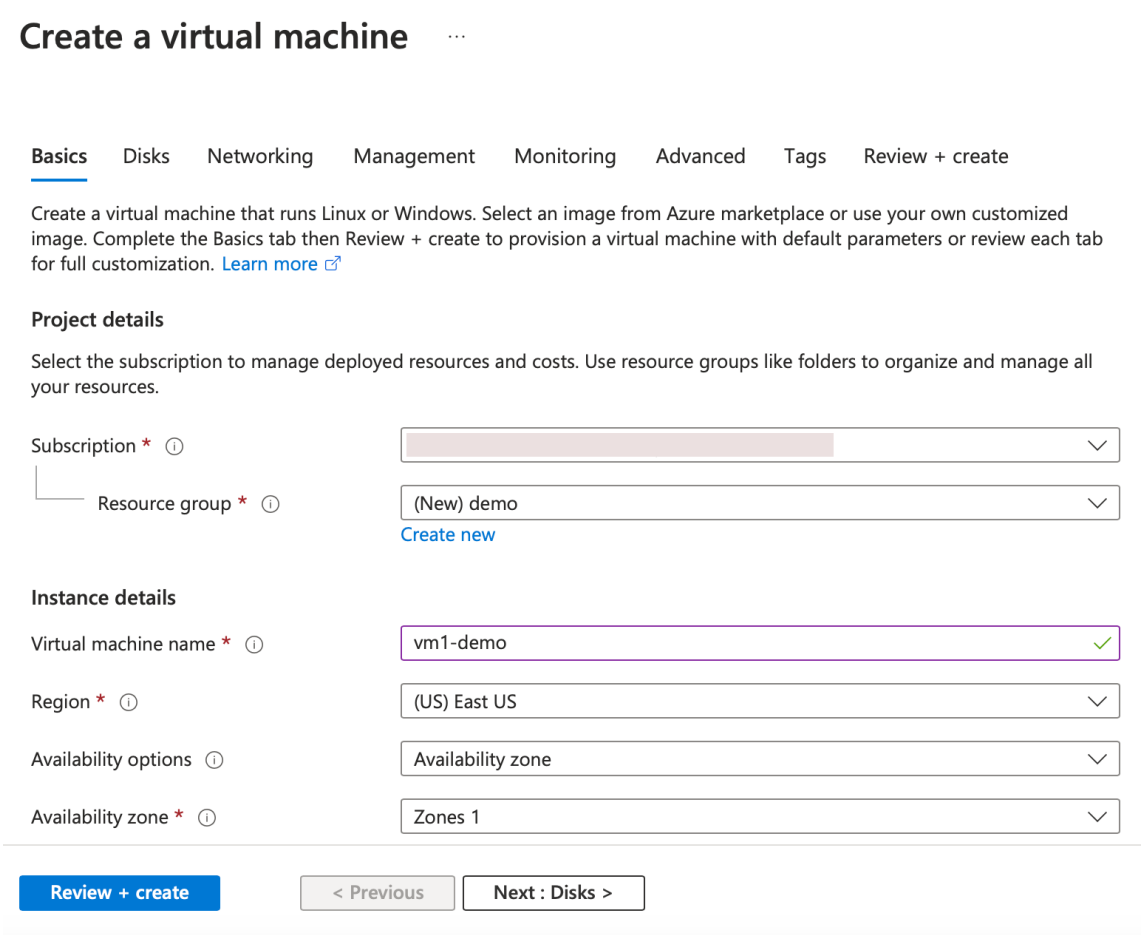


2. 选择所需的 ADC 许可模式，然后单击 创建。



创建虚拟机 页面随即打开。

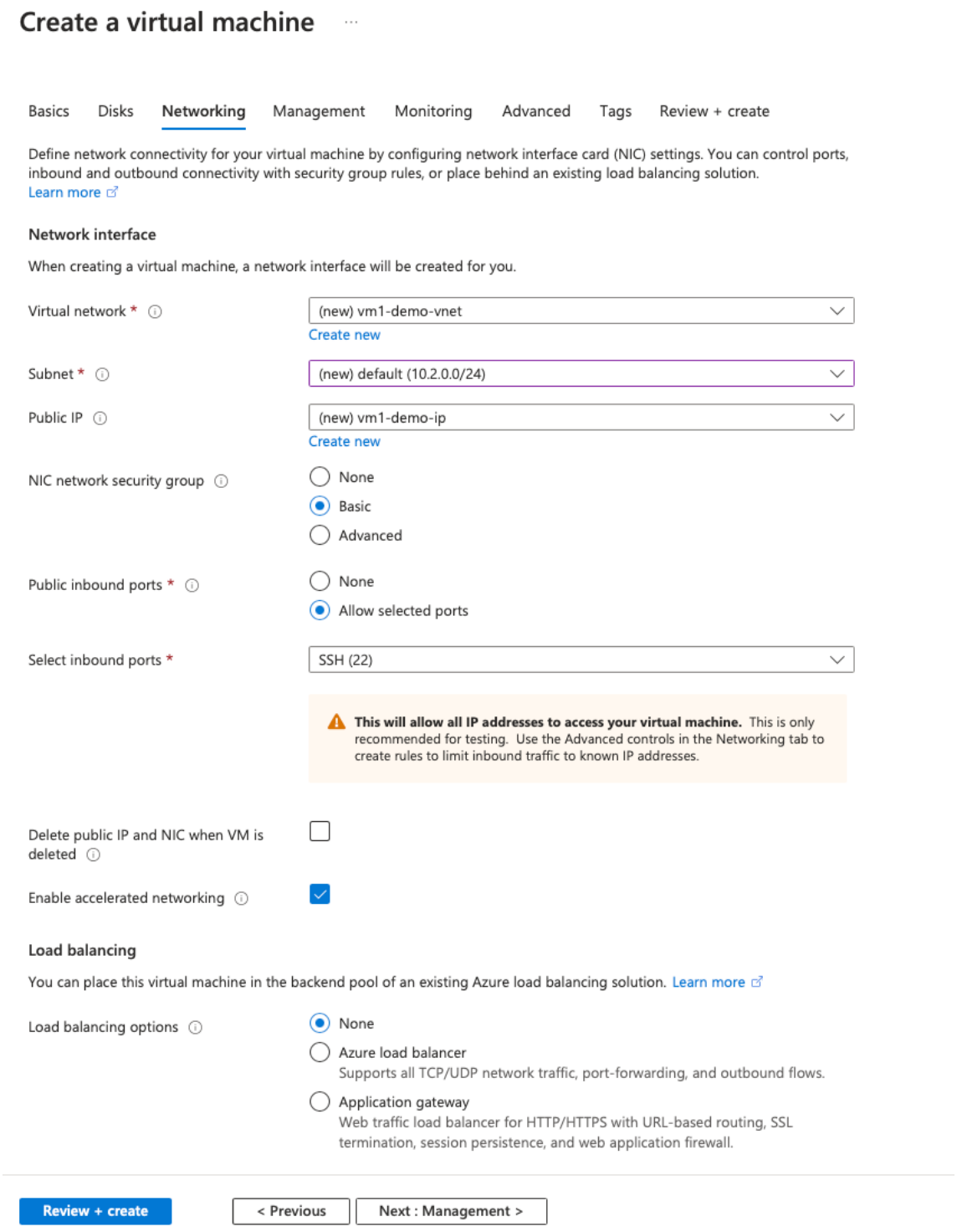
3. 在每个选项卡中填写所需的详细信息：“基础知识”、“磁盘”、“网络”、“管理”、“监视”、“高级”和“标签”，即可成功部署。



在“网络”选项卡中，创建一个包含 3 个子网的新虚拟网络，每个子网分别用于：管理、客户端和服务器 NIC。否则，您也可以使用现有的虚拟网络。管理 NIC 是在虚拟机部署期间创建的。客户端和服务器 NIC 在创建 VM 后创建并连接。对于 NIC 网络安全组，您可以执行以下操作之一：

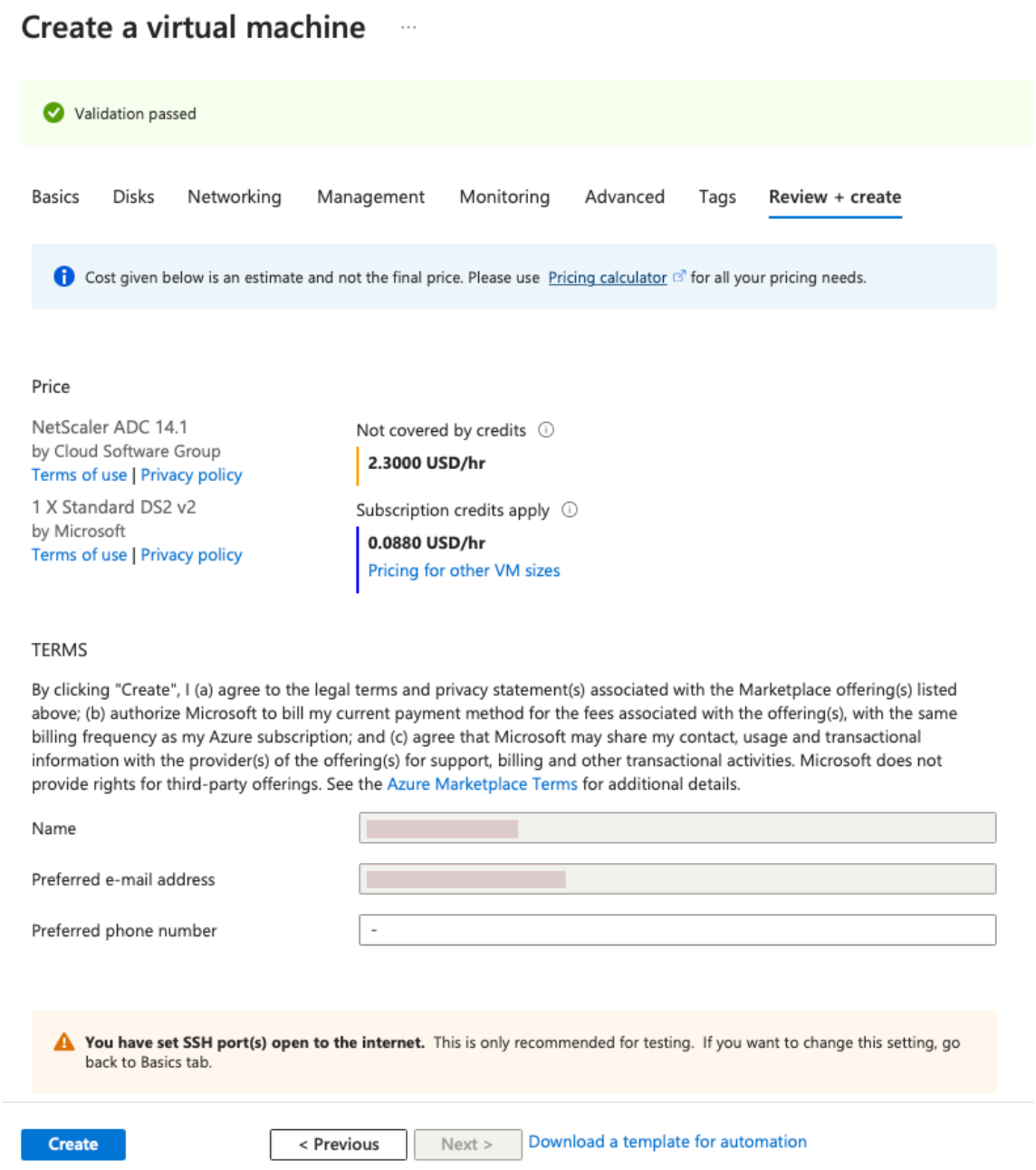
- 选择“高级”，然后使用符合您要求的现有网络安全组。
- 选择 基本 并选择所需的端口。

> 注意：
>
> 您还可以在虚拟机部署完成后更改网络安全组设置。

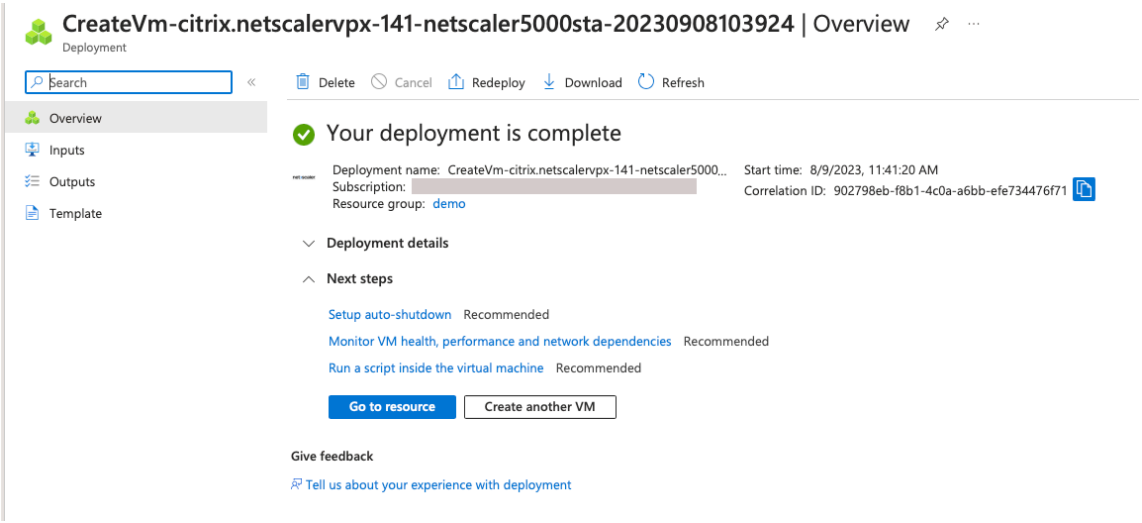


4. 单击“下一步：查看 + 创建”。

   验证成功后，查看基本设置、VM 配置、网络和其他设置，然后单击 **Create**（创建）。



5. 部署完成后，单击“转到资源”以查看配置详细信息。



同样，部署第二个 NetScaler VPX 实例。

步骤 **2.** 步骤 **2.** 在两个实例上添加客户端和服务器 **NIC**。

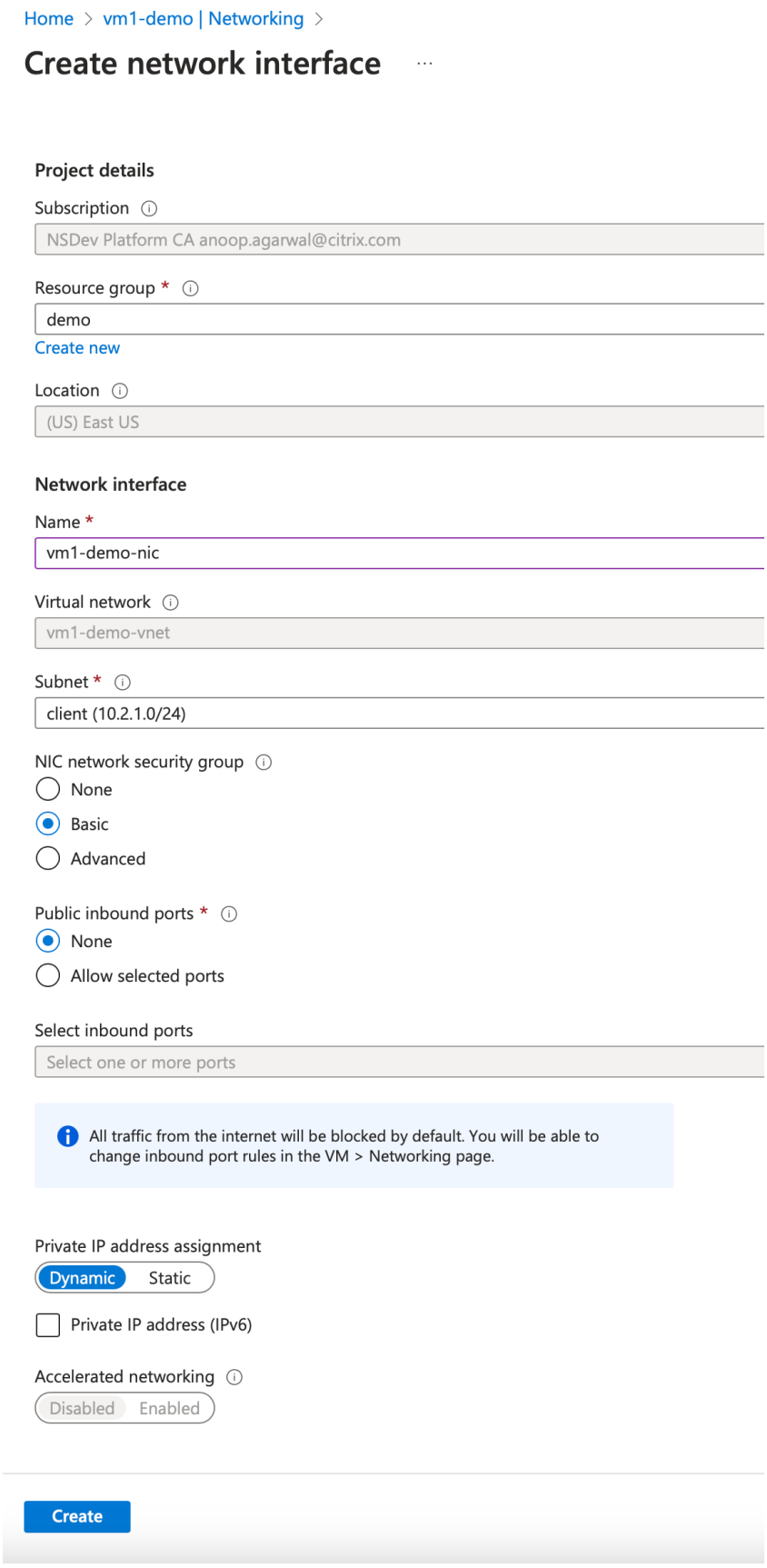
> 注意：
>
> 要连接更多 NIC，必须先停止 VM。在 Azure 门户中，选择要停止的 VM。在“概述”选项卡中，单击“停止”。等待状态显示为“已停止”。

要在主实例上添加客户端 NIC，请执行以下步骤：

1. 导航到 网络 **>** 连接网络接口。

   您可以选择现有 NIC，也可以创建并连接新接口。

2. 对于 NIC 网络安全组，您可以通过选择“高级”来使用现有的网络安全组，也可以通过选择“基本”来创建一个安全组。



要添加服务器 NIC，请执行与添加客户端 NIC 相同的步骤。

NetScaler VPX 实例连接了所有三个网卡（管理网卡、客户端网卡和服务器网卡）。

重复上述步骤，在辅助实例上添加 NIC。

在两个实例上创建并连接 NIC 后，通过转至 概述 **>** 启动来重启这两个实例。

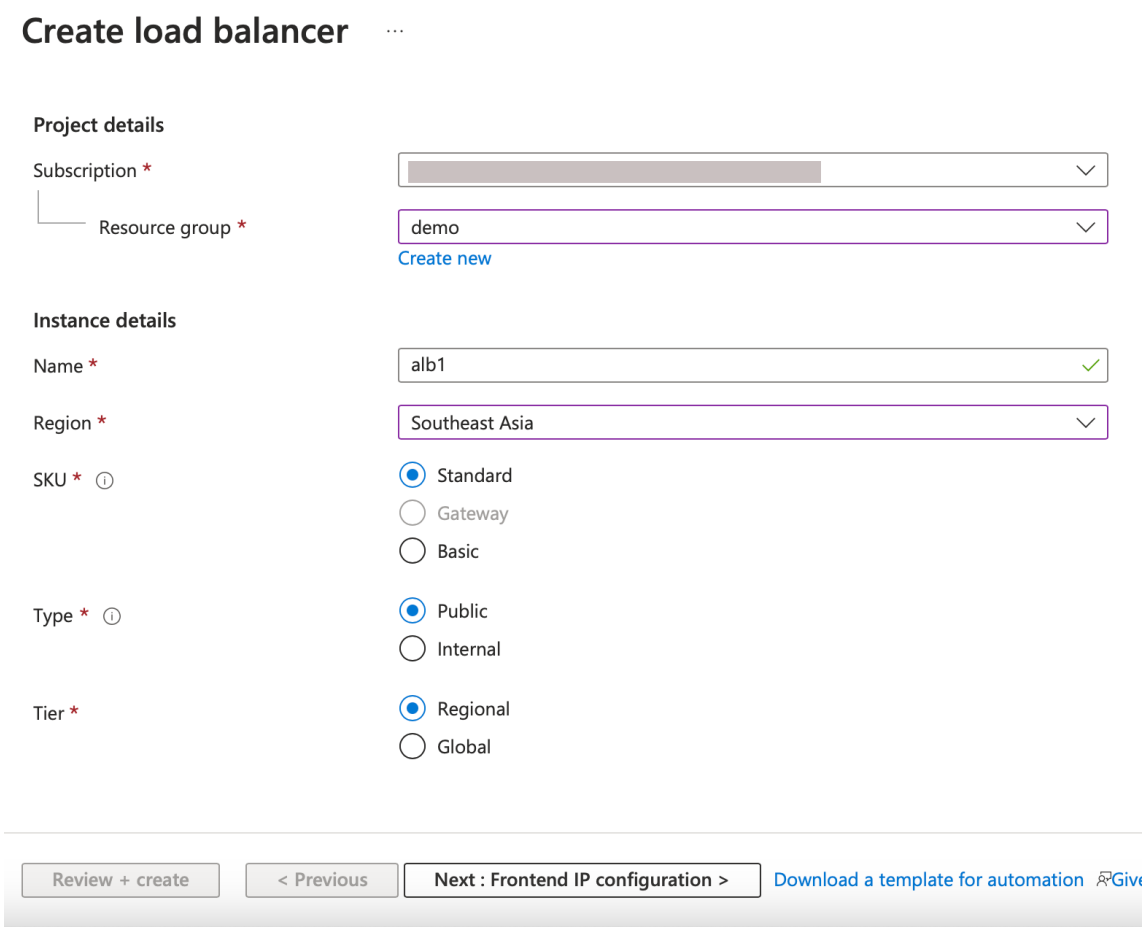
> 注意：
>
> 您必须允许流量通过客户端网卡入站规则中的端口，稍后在配置 NetScaler VPX 实例时使用该规则创建负载平衡虚拟服务器。

步骤 **3.** 部署禁用浮动 **IP** 模式的带负载均衡规则的 **ALB**。

要开始配置 ALB，请执行以下步骤：

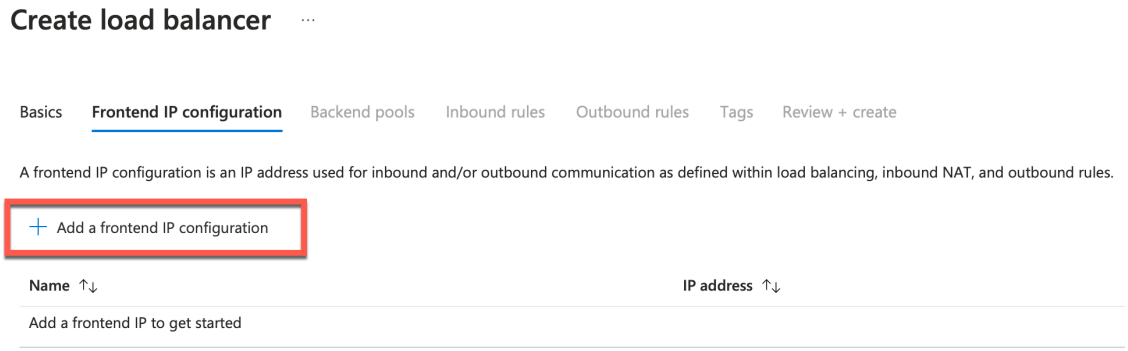
1. 转到 负载平衡器 页面，然后单击 创建。
2. 在“创建负载平衡器”页面中，根据需要提供详细信息。

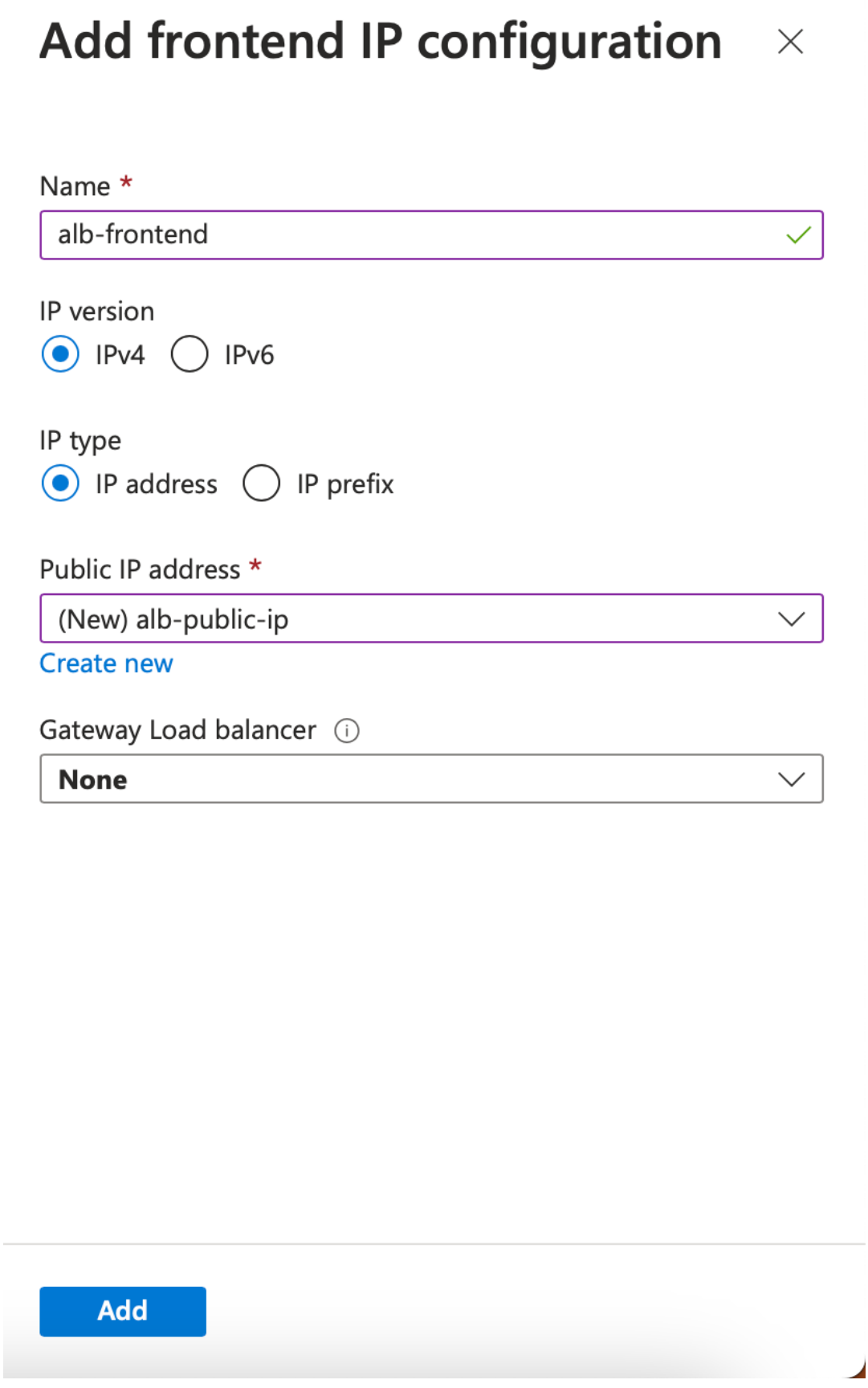
   在以下示例中，我们部署了标准 SKU 的区域公共负载平衡器。



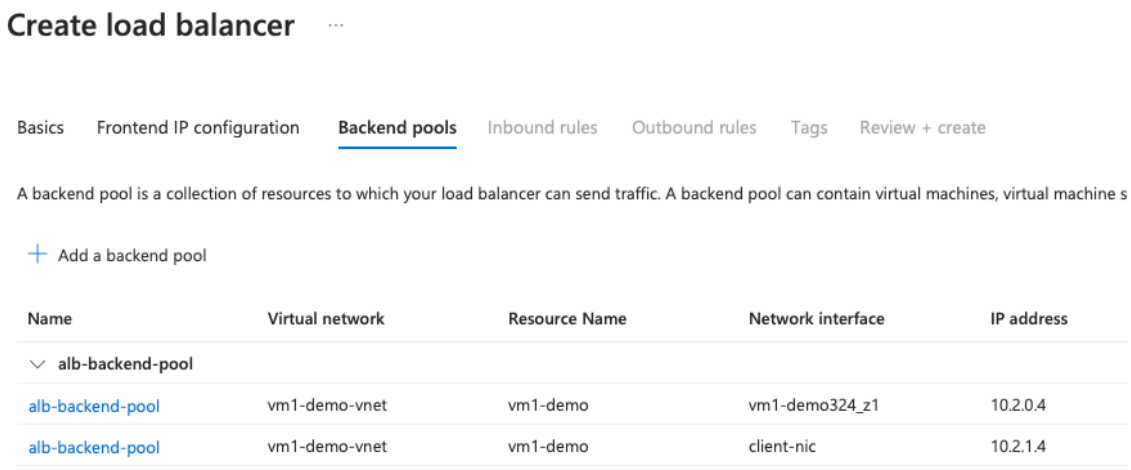
> 注意：
>
> 连接到 NetScaler 虚拟机的所有公有 IP 必须与 ALB 的 SKU 相同。有关 ALB SKU 的更多信息，请参阅 Azure 负载平衡器 SKU 文档。

3. 在“前端 **IP** 配置”选项卡中，创建 IP 地址或使用现有 IP 地址。

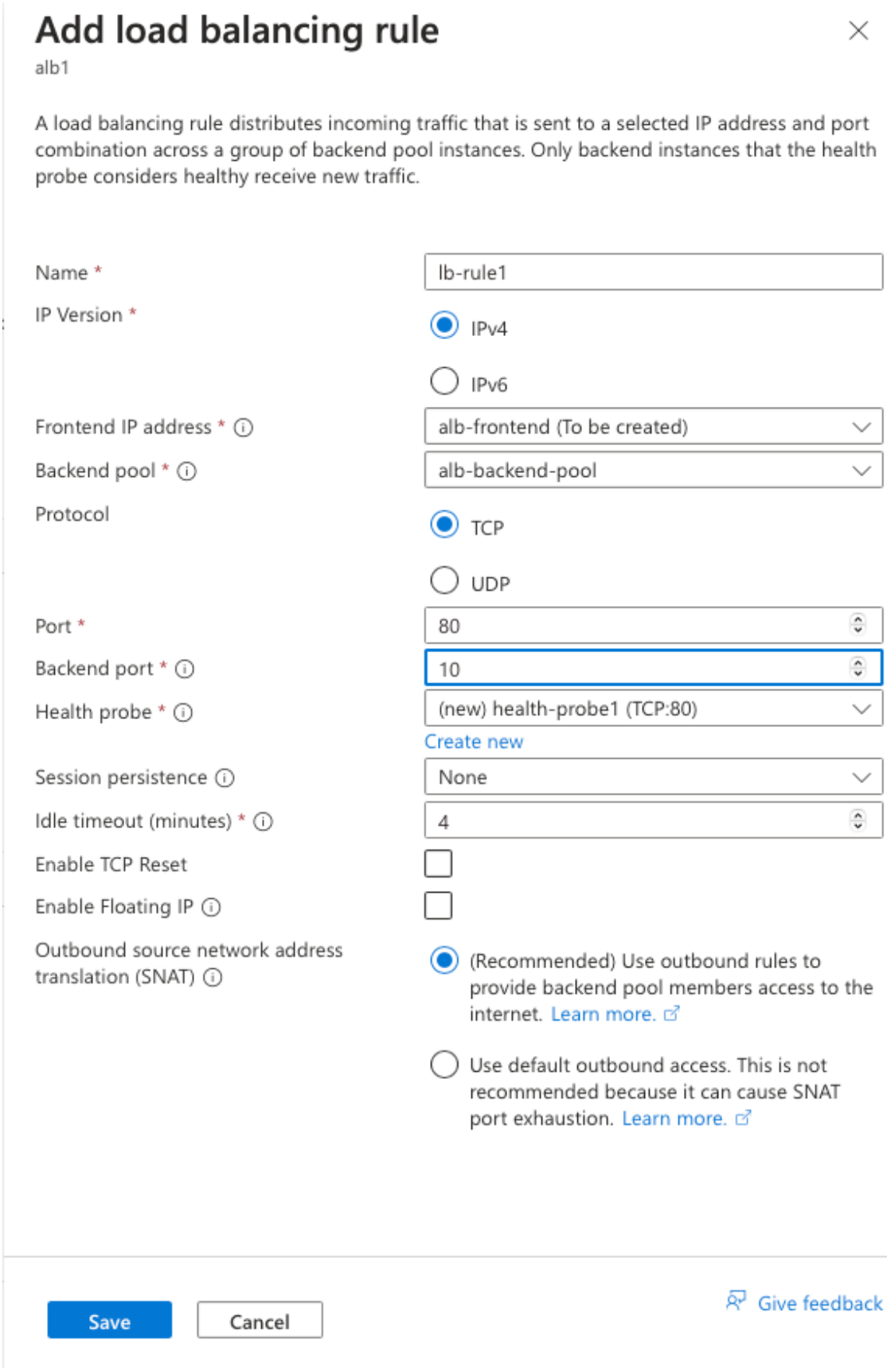




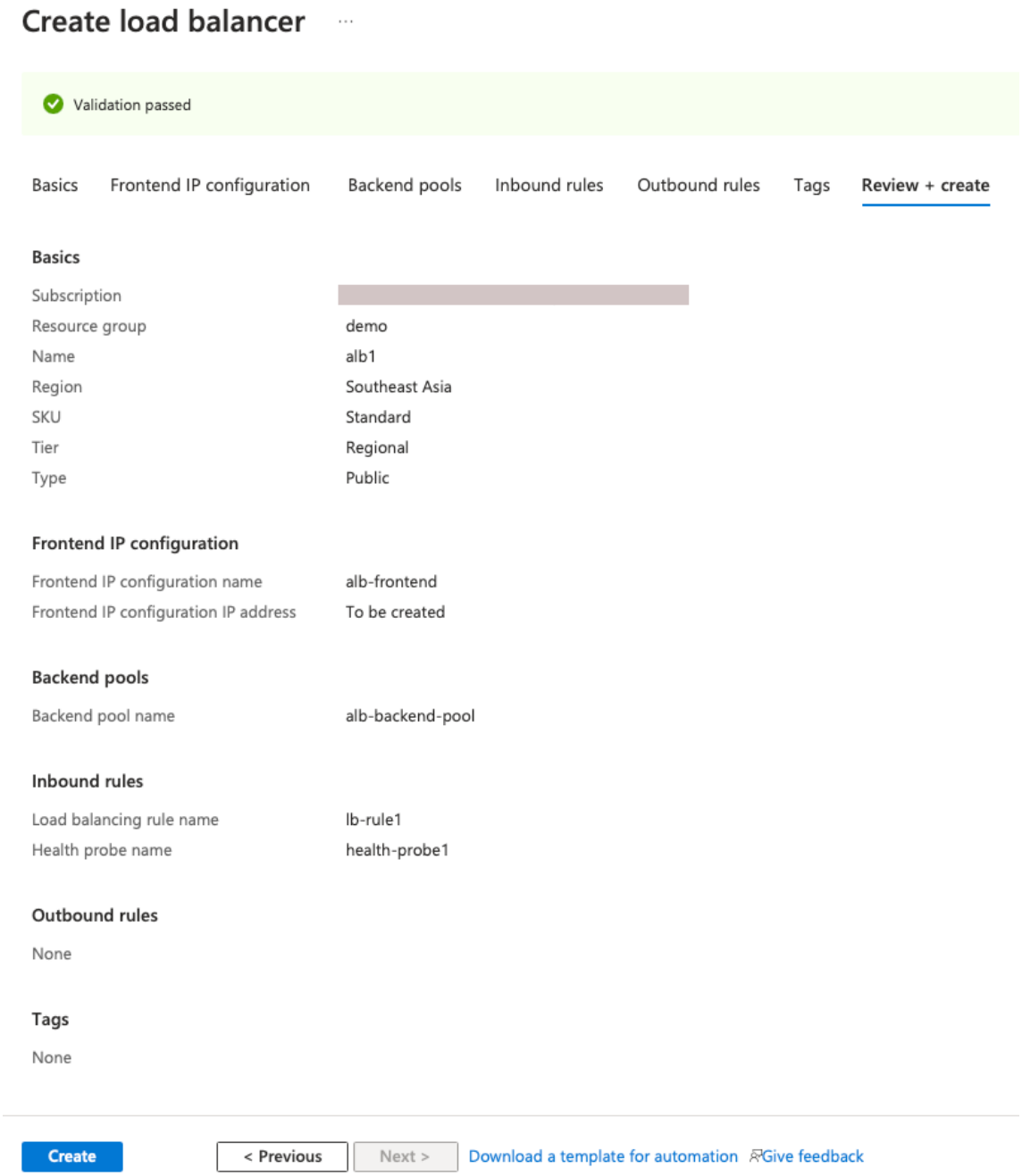
4. 在 后端池 选项卡中，选择基于 NIC 的后端池配置，然后添加两个 NetScaler 虚拟机的客户端网卡。



5. 在 入站规则 选项卡中，单击 添加负载均衡规则，并提供前面步骤中创建的前端 IP 地址和后端池。根据您的要求选择协议和端口。创建或使用现有的运行状况探测。清除“启用浮动 **IP**”复选框。



6. 单击“查看 + 创建”。验证通过后，单击“创建”。



步骤 **4.** 步骤 **4.** 使用 **NetScaler GUI** 在两个 **NetScaler VPX** 实例上配置高可用性设置。

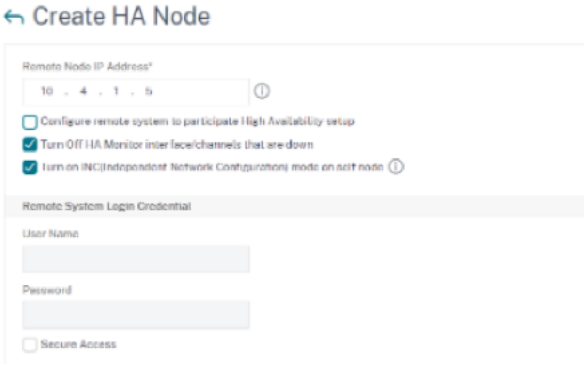
在 Azure 上创建 NetScaler VPX 实例后，您可以使用 NetScaler GUI 配置高可用性。

步骤 **1.** 在两个实例中在 **INC** 模式下设置高可用性。

在主实例上，执行以下步骤：

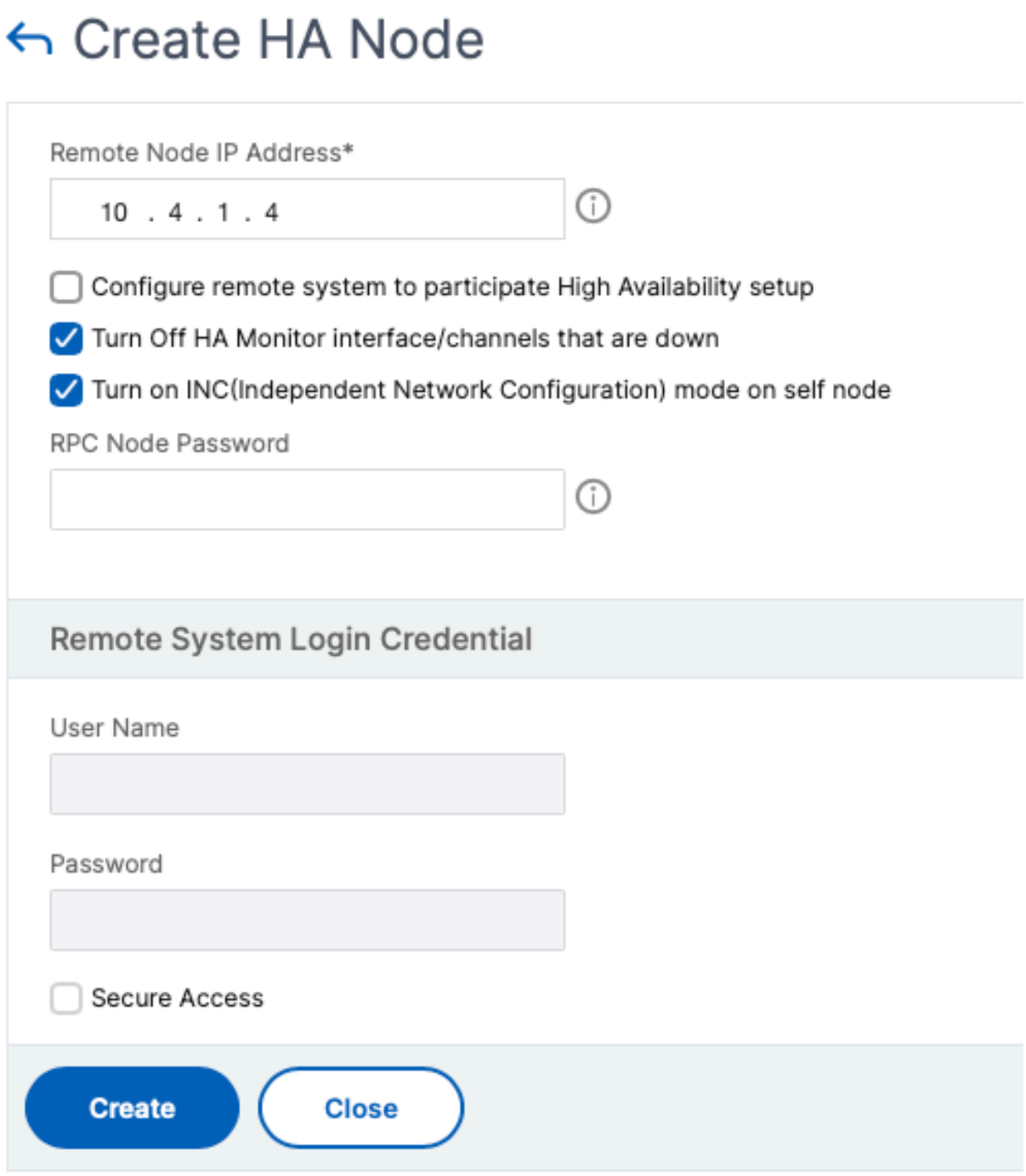
1. 使用部署实例时提供的用户名 `nsroot` 和密码登录实例。

2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 远程节点 **IP** 地址 字段中，输入辅助实例的管理 NIC 的专用 IP 地址，例如：10.4.1.5。
4. 选中“在 自身节点上打开 **INC**（独立网络配置）模式”复选框。
5. 单击创建。



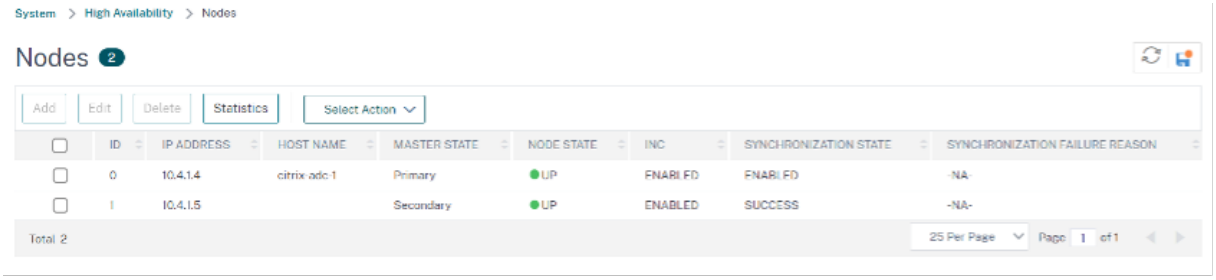
在辅助实例上，执行以下步骤：

1. 使用部署实例时提供的用户名 `nsroot` 和密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 远程节点 **IP** 地址 字段中，输入主实例的管理 NIC 的专用 IP 地址，例如：10.4.1.4。
4. 选中“在 自身节点上打开 **INC**（独立网络配置）模式”复选框。
5. 单击创建。



在继续操作之前，请确保辅助实例的 同步状态 在“节点”页面中显示为 SU **CC** ESS。

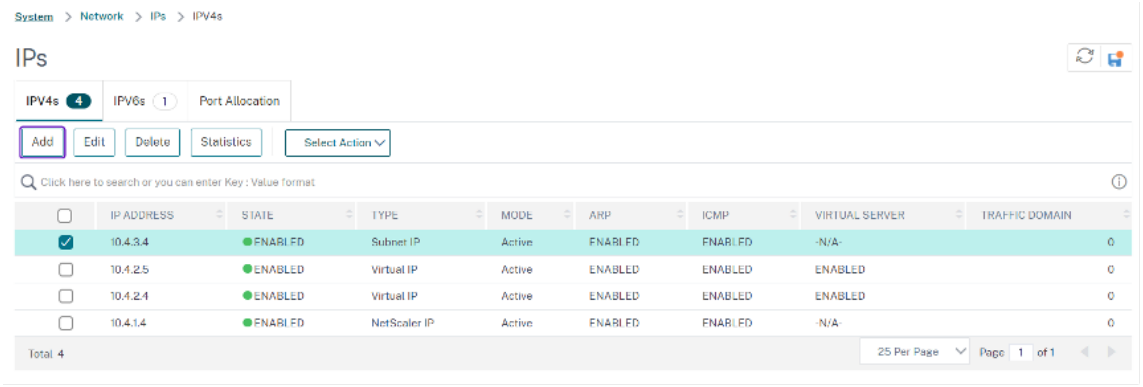
> 注意：
>
> 现在，辅助实例与主实例具有相同的登录凭证。



步骤 **2.** 步骤 **2.** 在两个实例上添加虚拟 **IP** 地址和子网 **IP** 地址。

在主实例上，执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 请按照以下步骤添加主 VIP 地址：
   a) 输入主实例的客户端 NIC 的私有 IP 地址以及为虚拟机实例中的客户端子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
   c) 单击创建。
3. 请按照以下步骤添加主 SNIP 地址：
   a) 输入主实例的服务器 NIC 的内部 IP 地址，以及为主实例中的服务器子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。
4. 按照以下步骤添加辅助 VIP 地址：
   a) 输入辅助实例的客户端 NIC 的内部 IP 地址，以及为虚拟机实例中的客户端子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
   c) 单击创建。



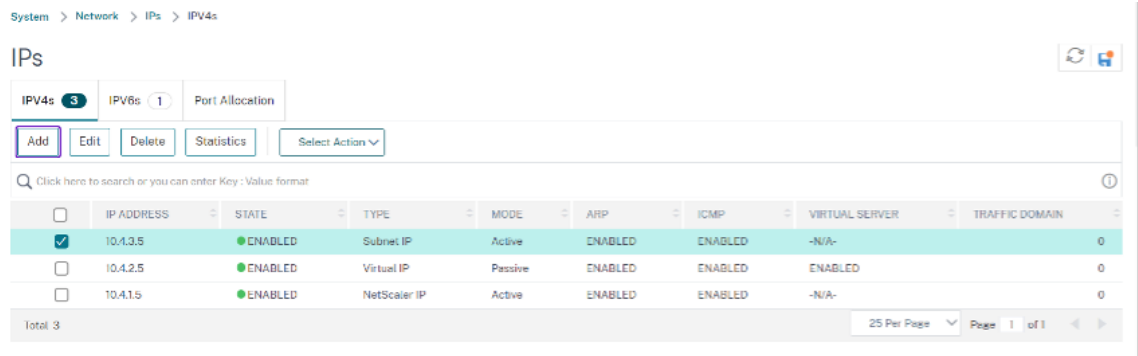
在辅助实例上，执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 按照以下步骤添加辅助 VIP 地址：

a) 输入辅助实例的客户端 NIC 的内部 IP 地址，以及为虚拟机实例中的客户端子网配置的网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。

3. 请按照以下步骤添加辅助 SNIP 地址：

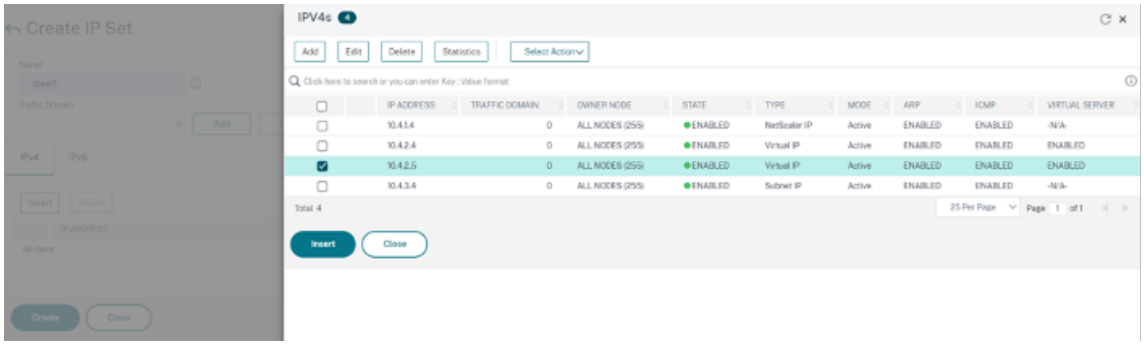
a) 输入辅助实例的服务器 NIC 的内部 IP 地址，以及为辅助实例中的服务器子网配置的网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
c) 单击创建。



步骤 **3.** 在两个实例上添加 **IP** 集并将 **IP** 集绑定到二级 **VIP**。

在主实例上，执行以下步骤：

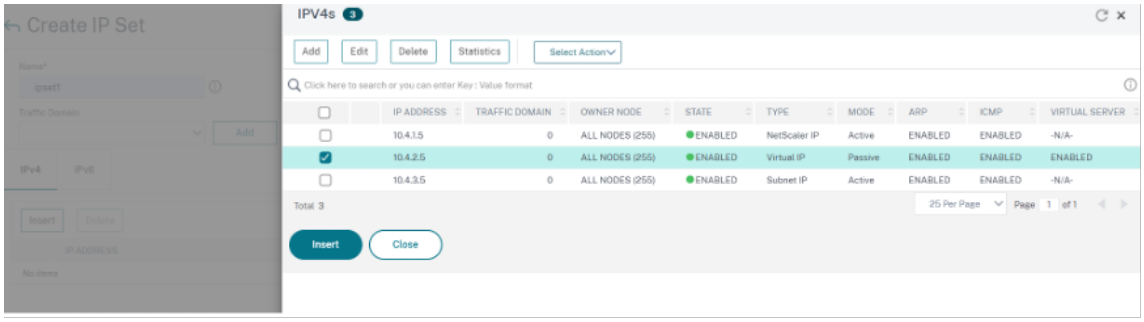
1. 导航到 **System**（系统）**> Network**（网络）**> IP Sets**（**IP** 集）**> Add**（添加）。
2. 添加 IP 集名称，然后单击 **Insert**（插入）。
3. 在 **IPV4s**（IPv4）页面中，选择虚拟 IP（二级 VIP），然后单击 **Insert**（插入）。
4. 单击 **Create**（创建）以创建 IP 集。



在辅助实例上，执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IP Sets**（**IP** 集）**> Add**（添加）。
2. 添加 IP 集名称，然后单击 **Insert**（插入）。
3. 在 **IPv4s** 页面中，选择虚拟 IP（辅助 VIP），然后单击 插入。

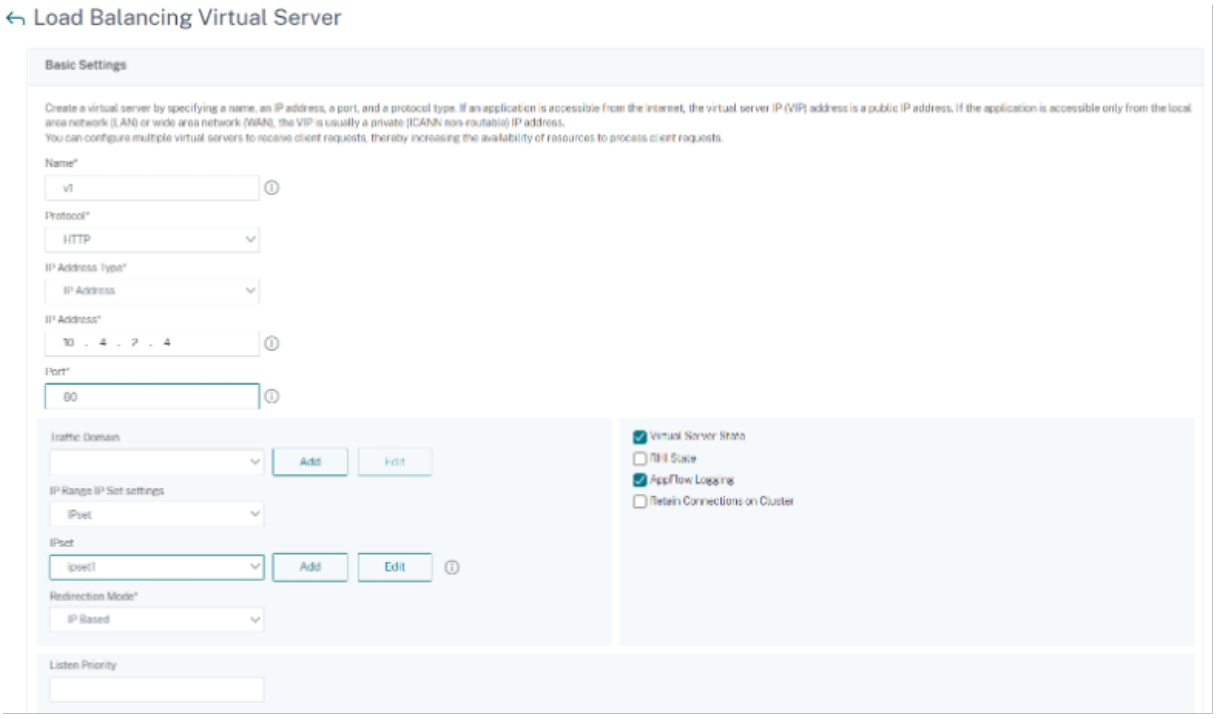
4. 单击 **Create**（创建）以创建 IP 集。



> 注意：
>
> 主实例和辅助实例上的 IP 集名称必须相同。

步骤 **4.** 在主实例上添加负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加）。
2. 添加“Name”（名称）、“Protocol”（协议）、“IP Address Type (IP Address)”（IP 地址类型 (IP 地址)）、“IP address (primary VIP)”（IP 地址 (主 VIP 地址)）和“Port”（端口）所需的值。
3. 单击 **More**（更多）。导航到 **IP Range IP Set Settings**（IP 范围 IP 集设置），从下拉菜单中选择 **IPSet** =（IP 集），并提供在步骤 **3** 中创建的 IP 集。
4. 单击 **OK**（确定）以创建负载平衡虚拟服务器。

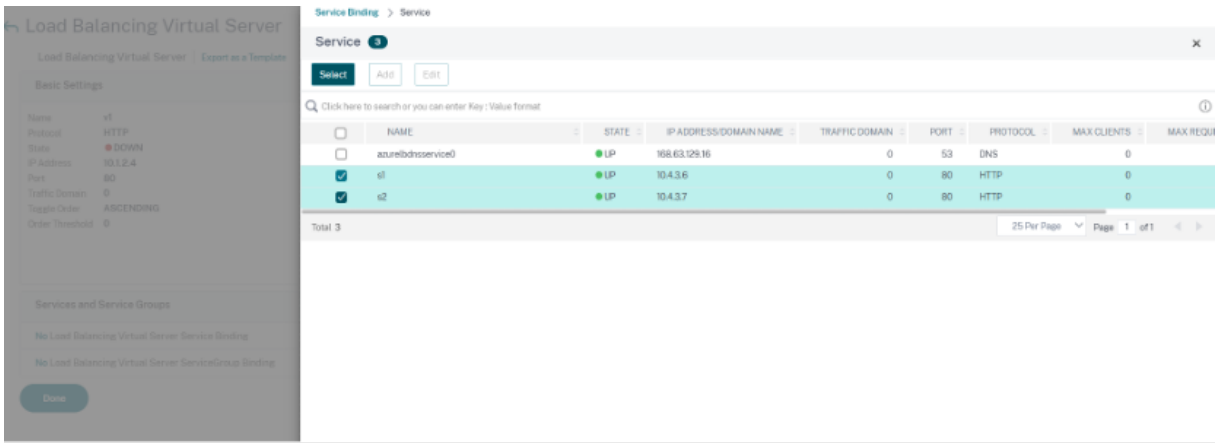


步骤 **5.** 在主实例上添加服务或服务组。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）**> Add**（添加）。
2. 添加“Service Name”（服务名称）、“IP Address”（IP 地址）、“Protocol”（协议）和“Port”（端口）所需的值，然后单击 **OK**（确定）。

步骤 **6.** 步骤 **6.** 将服务或服务组绑定到主实例上的负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。
2. 选择在 **Step 4**（步骤 4）中配置的负载平衡虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **Service and Service Groups**（服务和服务组）选项卡中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。
4. 选择在 **Step 5**（步骤 5）中配置的服务，然后单击 **Bind**（绑定）。



步骤 **7.** 步骤 **7.** 保存配置。

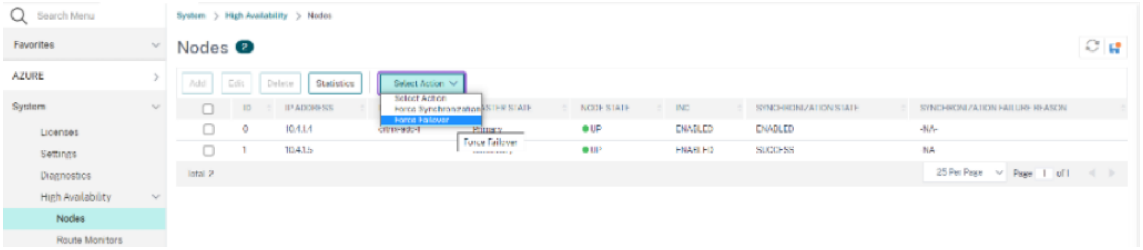
否则，在重新启动后或立即重新启动后，所有配置都将丢失。

步骤 **8.** 验证配置。

确保在故障转移后可以访问 ALB 前端 IP 地址。

1. 复制 ALB 前端 IP 地址。
2. 将 IP 地址粘贴到浏览器上，并确保后端服务器可以访问。
3. 在主实例上，执行故障转移：

   在 NetScaler GUI 中，导航到 配置 **>** 系统 **>** 高可用性 **>** 操作 **>** 强制故障转移。



4. 确保通过之前使用的 ALB 前端 IP 进行故障切换后可以访问后端服务器。

部署适用于 **Azure DNS** 私有区域的 **NetScaler**

October 17, 2024

Azure DNS 是 Microsoft 基础结构上的服务，用于托管 DNS 域和提供名称解析。

Azure DNS 私有区域是一项专注于解析私有网络中域名的服务。对于私有区域，客户可以使用自己的自定义域名，而不是 Azure 目前提供的名称。

领先的应用程序交付解决方案 NetScaler 最适合为 Azure DNS 私有区域提供负载平衡和 GSLB 功能。通过订阅 Azure DNS 私有区域，企业可以依靠 NetScaler 全球服务器负载平衡 (GSLB) 的强大功能和智能，通过安全 VPN 隧道连接的多个地理位置和数据中心跨工作负载分配内部网流量。这种合作可确保企业无缝访问他们想要迁移到 Azure 公有云的部分工作负载。

Azure DNS 概述

域名系统 (DNS) 负责将服务名称转换或解析为其 IP 地址。Azure DNS 是一款面向 DNS 域的托管服务，它使用 Microsoft Azure 基础结构提供名称解析。除了支持面向 Internet 的 DNS 域外，Azure DNS 现在还支持私有 DNS 域。

Azure DNS 提供可靠、安全的 DNS 服务来管理和解析虚拟网络中的域名，而无需自定义 DNS 解决方案。通过使用私有 DNS 区域，您可以使用自己的自定义域名，而不是 Azure 提供的名称。使用自定义域名可帮助您定制虚拟网络体系结构，以最适合您组织的需求。它为虚拟网络内和虚拟网络之间的虚拟机 (VM) 提供名称解析。此外，客户还可以使用水平分割视图配置区域名称，从而允许私有 DNS 区域和公有 DNS 区域共享名称。

为什么 **NetScaler GSLB** 适用于 **Azure DNS** 私有区域

在当今世界，企业希望将其工作负载从本地迁移到 Azure 云。向云的过渡使他们能够将时间推向市场、资本支出/价格、易于部署和安全性。Azure DNS 私有区域服务为正在将部分工作负载过渡到 Azure 云的企业提供了独特的提议。这些企业在使用私有区域服务时，可以创建自己的私有 DNS 名称，这是他们在本地部署中多年来一直使用的。由于这种混合模式的内部网应用程序服务器位于本地，Azure 云通过安全 VPN 隧道连接，因此唯一的挑战是无缝访问这些内部网应用程序。NetScaler 通过其全局负载平衡功能解决了这个独特的用例，该功能可将应用程序流量路由到本地或 Azure 云上最优的分布式工作负载/服务器，并提供应用程序服务器的健康状态。

用例

本地网络和不同 Azure VNet 中的用户可以连接到内部网络中最优的服务器来访问所需内容。这样可以确保应用程序始终可用，成本得到优化，用户体验良好。Azure 私有流量管理 (PTM) 是这里的主要要求。Azure PTM 可确保用户的

DNS 查询解析为应用程序服务器的相应私有 IP 地址。

用例解决方案

NetScaler 包括全局服务器负载平衡 (GSLB) 功能，以满足 Azure PTM 的要求。GSLB 的作用类似于 DNS 服务器，它获取 DNS 请求并将该 DNS 请求解析为相应的 IP 地址以提供：

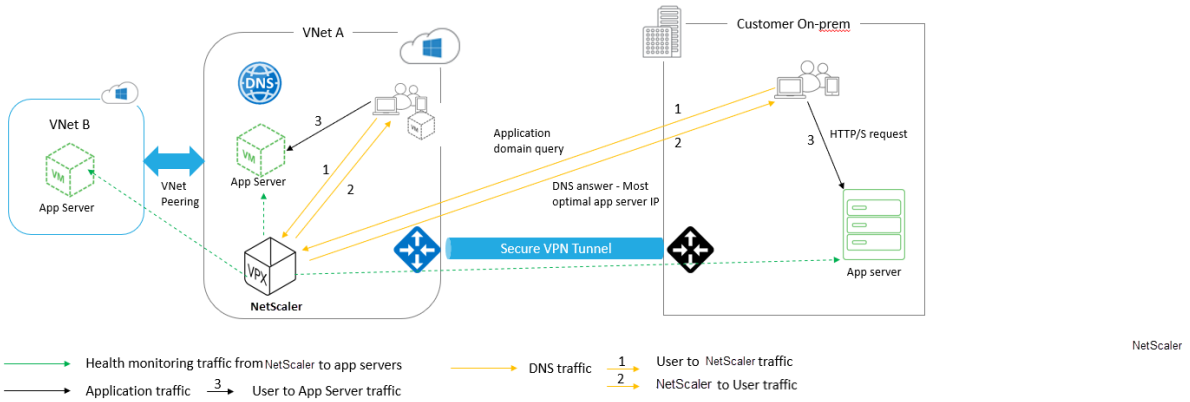
- 基于 DNS 的无缝故障转移。
- 分阶段从本地迁移到云端。
- A/B 测试一项新功能。

在支持的众多负载平衡方法中，以下方法可能适用于此解决方案：

1. 循环赛
2. 静态邻近度（基于位置的服务器选择）。它可以通过两种方式部署：
    a) NetScaler 上基于 EDNS 客户端子网 (ECS) 的 GSLB。
    b) 为每个虚拟网络部署 DNS 转发器。

拓扑

下图描述了 Azure 私有 DNS 区域的 NetScaler GSLB 部署。



根据 Azure 私有 DNS 区域中的 NetScaler GSLB 方法，用户可以访问 Azure 上或本地的任何应用程序服务器。本地和 Azure 虚拟网络之间的所有流量仅通过安全的 VPN 隧道进行。应用程序流量、DNS 流量和监视流量显示在前面的拓扑中。根据所需的冗余，NetScaler 和 DNS 转发器可以部署在虚拟网络和数据中心中。为简单起见，此处仅显示一个 NetScaler，但我们建议在 Azure 区域至少使用一组 NetScaler 和 DNS 转发器。所有用户 DNS 查询首先转到 DNS 转发器，该转发器定义了将查询转发到相应的 DNS 服务器的规则。

为 **Azure DNS** 私有区域配置 **NetScaler**

经过测试的产品和版本：

产品	版本
Azure	云端订阅
NetScaler VPX	BYOL（自带许可证）

> 注意：
>
> 部署已经过测试，并且在 NetScaler 12.0 及更高版本中保持不变。

必备条件

以下是一般先决条件。

- 具有有效订阅的微软 Azure 门户帐户。
- 确保本地和 Azure 云之间的连接（安全 VPN 隧道）。要在 Azure 中设置安全 VPN 隧道，请参阅 分步操作：在 Azure 和本地之间配置站点到站点 VPN 网关。

解决方案描述

如果你想托管一个应用程序 Azure DNS 私有区域 (rr.ptm.mysite.net)，该区域在 HTTP 上运行，部署在 Azure 和本地，可根据循环 GSLB 负载平衡方法进行内部网访问。要实现此部署，请使用包含以下配置的 NetScaler 为 Azure 私有 DNS 区域启用 GSLB：

1. 配置 Azure 和本地安装程序。
2. Azure 虚拟网络上的 NetScaler 设备。

配置 **Azure** 和本地安装程序

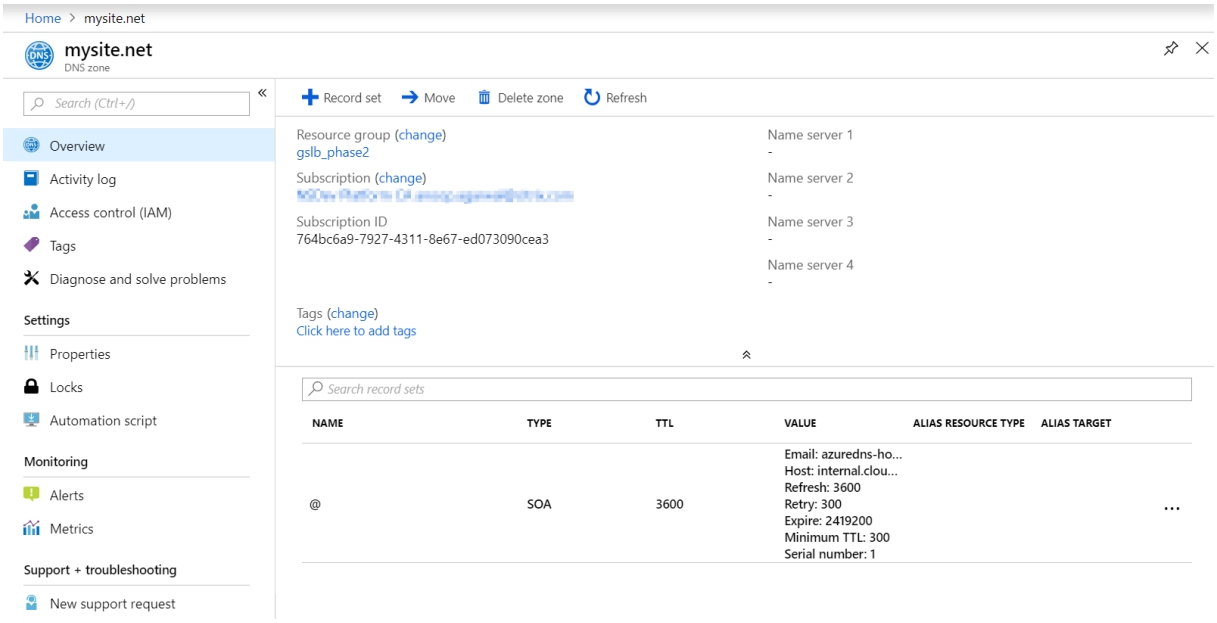
如拓扑所示，设置 Azure 虚拟网络（在本例中为 vNet A、vNet B）和本地设置。

1. 使用域名 (mysite.net) 创建 Azure 私有 DNS 区域。
2. 在 Azure 区域的中心和分支模型中创建两个虚拟网络（vNet A、vNet B）。
3. 在 vNet A 中部署 App Server、DNS 转发器、Windows 10 Pro 客户端、NetScaler
4. 如果有任何客户端位于 vNet B 中，则部署应用服务器并部署 DNS 转发器
5. 在本地部署应用程序服务器、DNS 转发器和 Windows 10 专业版客户端。

Azure 私有 **DNS** 区域

使用域名创建 Azure 私有 DNS 区域。

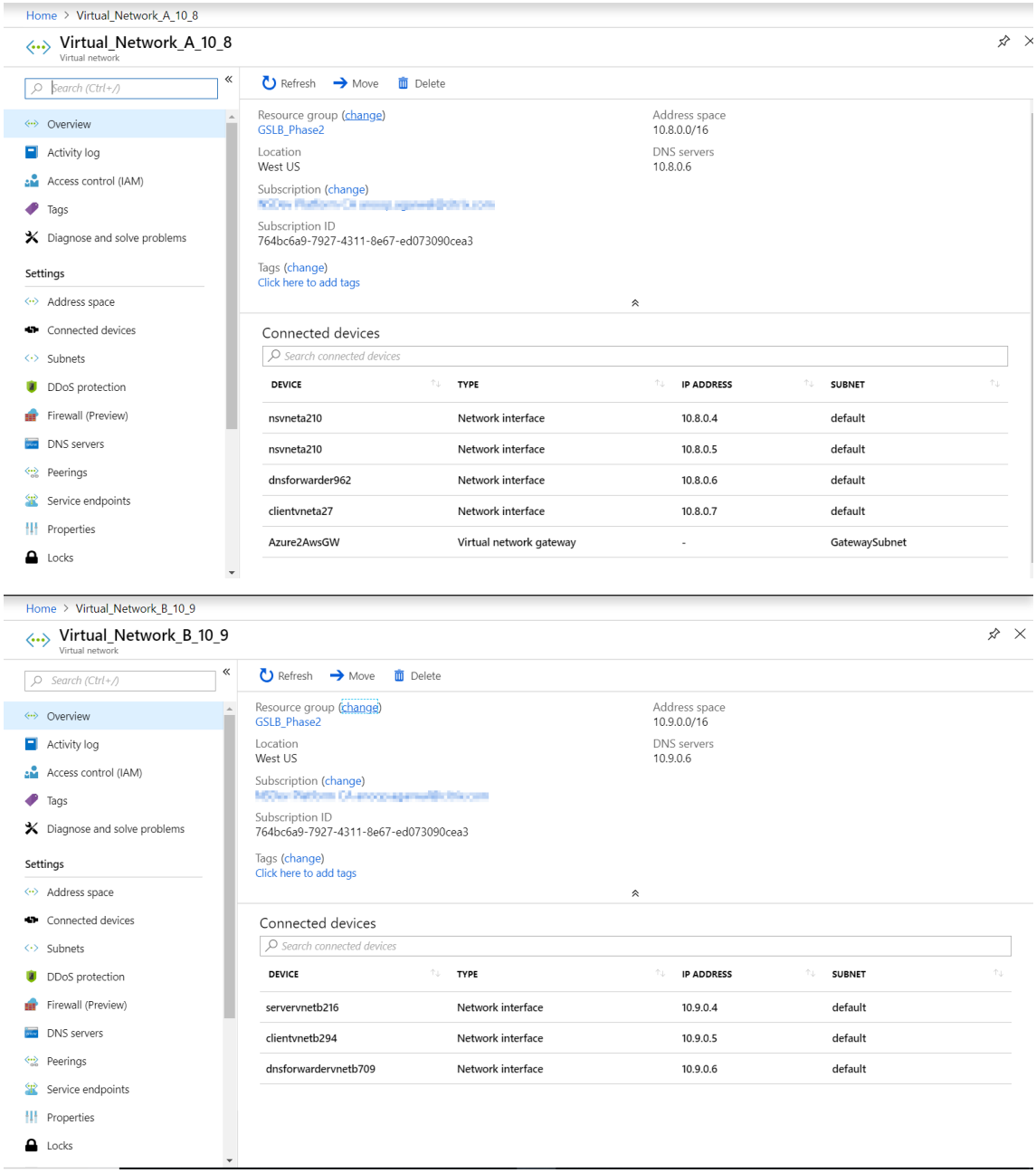
1. 登录 Azure 门户并选择或创建仪表板。
2. 单击“创建资源”，然后搜索要创建的 DNS 区域（在本例中为 mysite.net）带有域名（mysite.net）的 Azure 私有 DNS 区域（mysite.net）。



中心和分支模式中的 **Azure** 虚拟网络（**vNet A**、**vNet B**）

在 Azure 区域的中心和分支模型中创建两个虚拟网络（vNet A、vNet B）。

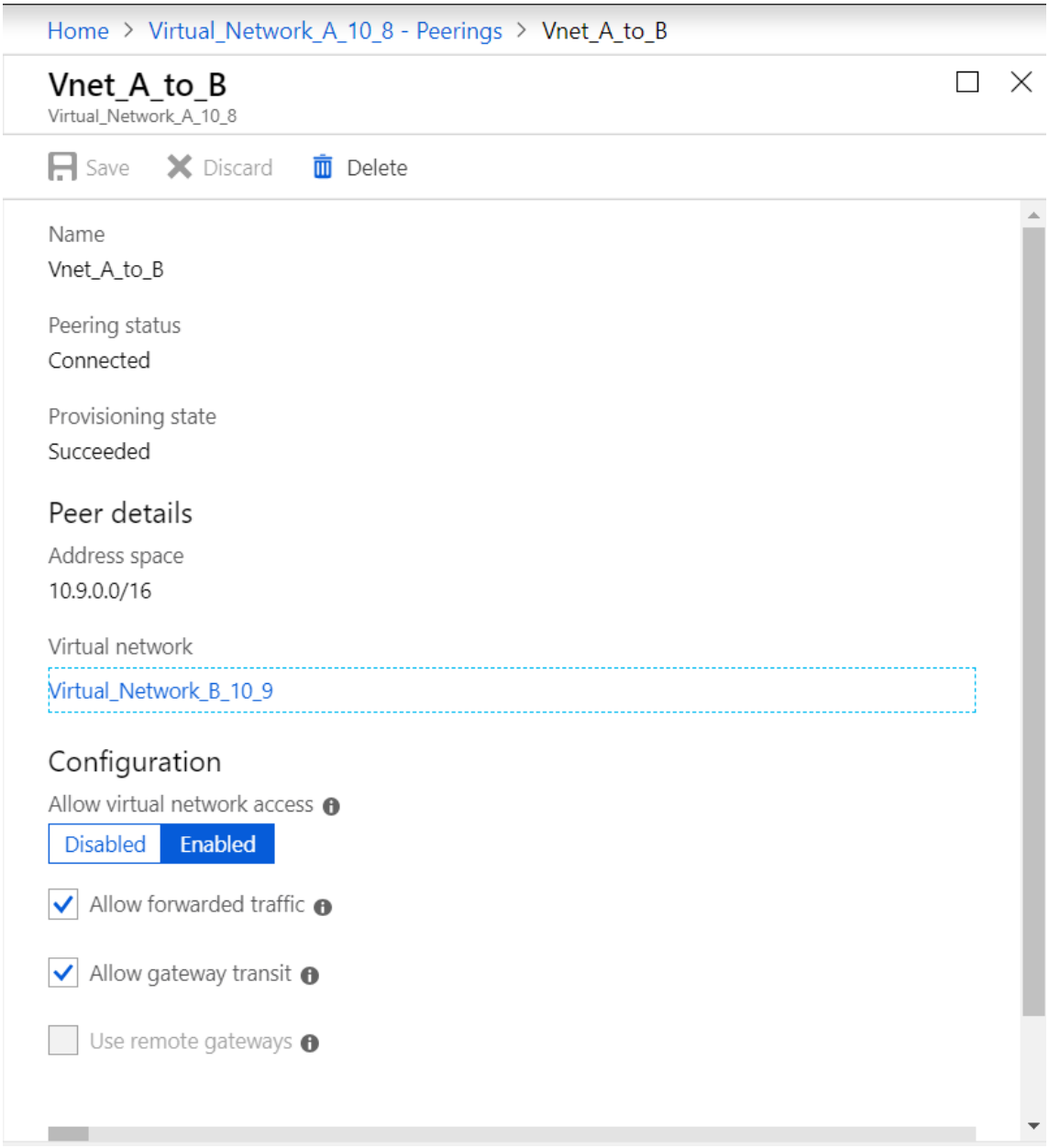
1. 创建两个虚拟网络。
2. 选择同 一个仪表板并单击“创建资源”，搜索虚拟网络，在同一区域中创建两个虚拟网络，即 vNet A、vNet B，并将它们对等以形成集线器和分支模型，如下图所示。有关如何设置中心和分支拓扑的更多信息，请参见在 Azure 中实现中心辐射型网络拓扑。



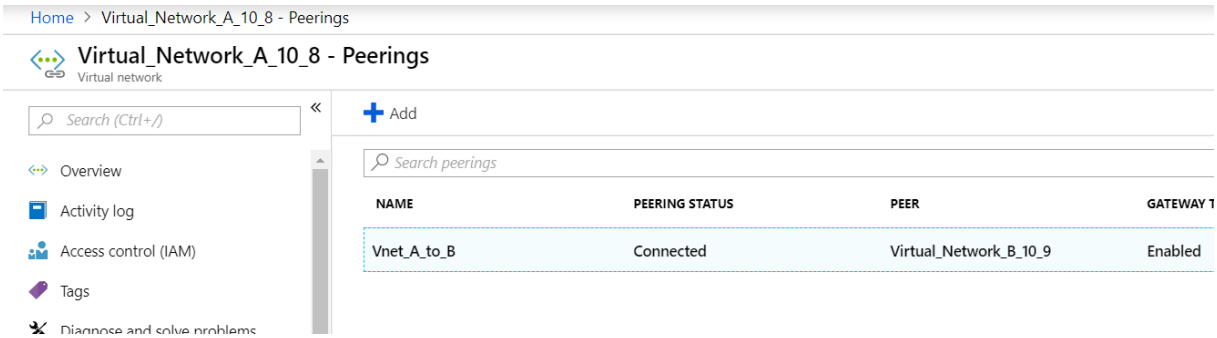
VNet A 到 **vNet B** 对等

要对等 vNet A 和 vNet B，请执行以下操作：

1. 从 vN **et A** 和 对等 vNet B 的“设置”菜单中单击“对等”。
2. 启用“允许转发流量”和“允许网关传输”，如下图所示。



下图描绘了 vNet A 与 vNet B 的成功对等关系。

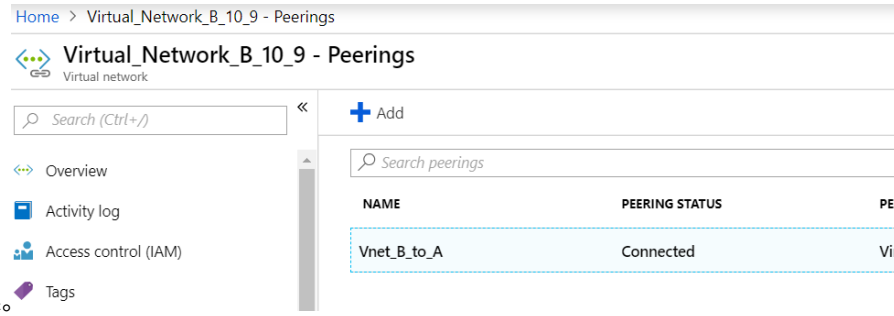


vNet B 到 **vNet A** 对等

要对等 vNet B 和 vNet A，请执行以下操作：

1. 从 vN **et B** 和 对等 vNet A 的“设置”菜单中单击“对等”
2. 启用“允许转发流量”并使用远程网关，如下图所示。

```
1 ![VNet B to A](/en-us/vpx/media/image-07.png)
```



下图描绘了 vNet B 与 vNet A 的成功对等关系。

在 **vNet A** 中部署应用程序服务器、**DNS** 转发器、**Windows 10 Pro** 客户端、**NetScaler**

我们将简要讨论应用服务器、DNS 转发器、Windows 10 专业版客户端和 vNet A 上的 NetScaler。

1. 选择同一个控制面板，单击“创建资源”。
2. 搜索相应的实例并从 vNet A 子网分配一个 IP。

应用程序服务器　应用服务器不过是 Web 服务器（HTTP 服务器），其中 Ubuntu 服务器 16.04 作为实例部署在 Azure 或本地虚拟机上。要将其设为 Web 服务器，请在命令提示符下键入：

```
sudo apt install apache2
```

Windows 10 Pro 客户端　在 vNet A 和本地以客户端计算机的身份启动 Windows 10 专业版实例。

NetScaler　NetScaler 通过 NetScaler MAS 的运行状况检查和分析来补充 Azure DNA 私有区域。根据你的要求从 Azure 市场启动 NetScaler，此处我们使用了 NetScaler (BYOL) 进行此部署。

有关如何在微软 Azure 上部署 NetScaler 的详细步骤。请参阅 在 Microsoft Azure上部署 NetScaler VPX 实例。

部署后，使用 NetScaler IP 配置 NetScaler GSLB。

DNS 转发器　它用于转发绑定到 NetScaler GSLB（ADNS IP）的托管域的客户端请求。以 Linux 实例启动 Ubuntu 服务器 16.04（Ubuntu 服务器 16.04），并参考以下 URL 了解如何将其设置为 DNS 转发器。

> 注意：
>
> 对于 Round Robin GSLB 负载平衡方法，一个 Azure 区域的 DNS 转发器就足够了，但是对于静态邻近性，我们需要每个虚拟网络一个 DNS 转发器。

1. 部署转发器后，使用 vNet A DNS 转发器 IP 将虚拟网络 A 的 DNS 服务器设置从默认设置更改为自定义，如下图所示。
2. 修改 vNet A DNS 转发器中的 `named.conf.options` 文件，将域 (mysite.net) 和子域 (ptm.mysite.net) 的转发规则添加到 NetScaler GSLB 的 ADNS IP 中。
3. 重新启动 DNS 转发器以反映文件 `named.conf.options`中所做的更改。

VNet A DNS 转发器设置

```
      zone "mysite.net" {

                  type forward;
      forwarders {
  168.63.129.16;  }
 ;
       }
 ;
      zone "ptm.mysite.net" {

          type forward;
          forwarders {
  10.8.0.5;  }
 ;
       }
 ;
```

> 注意：
>
> 对于域（“mysite.net”）区域 IP 地址，请使用你的 Azure 区域的 DNS IP 地址。对于子域（“ptm.mysite.net”）区域 IP 地址，请使用您的 GSLB 实例的所有 ADNS IP 地址。

如果 **vNet B** 中有客户端，则部署应用程序服务器和 **DNS** 转发器

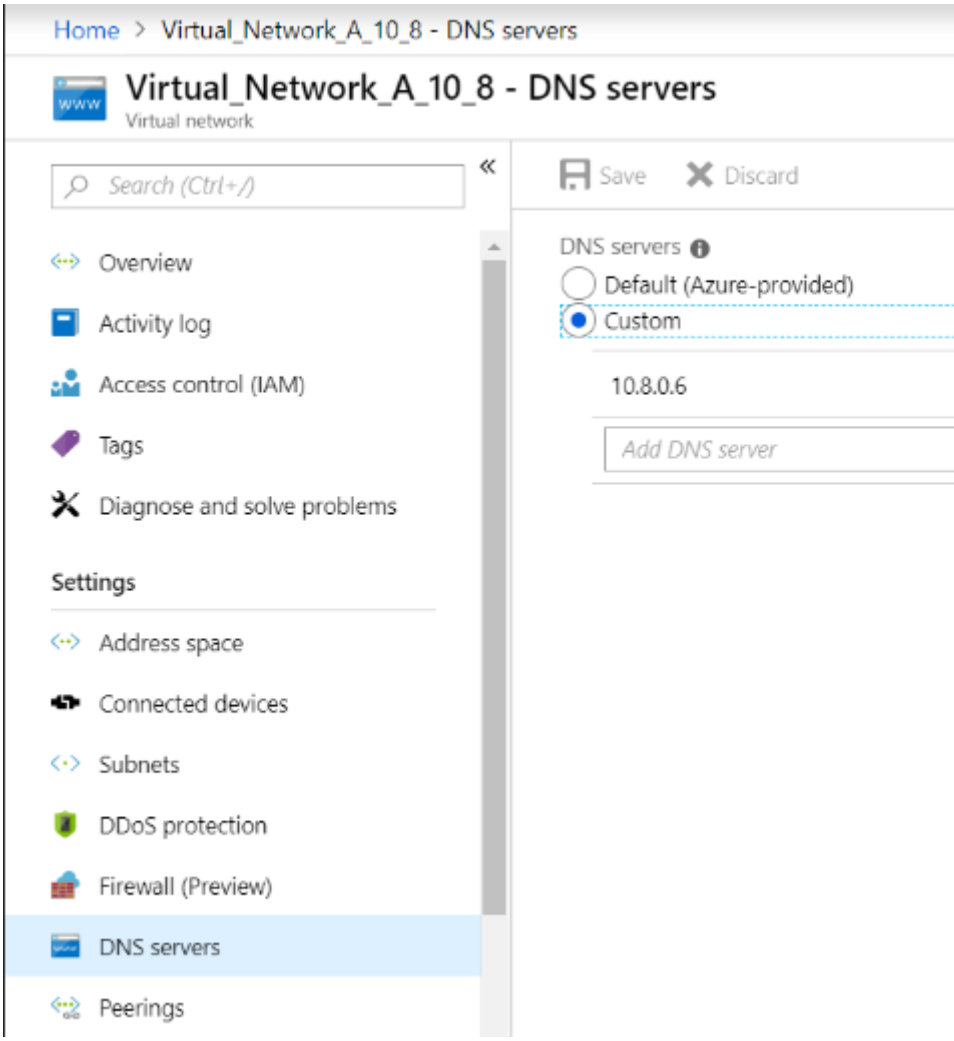
1. 对于虚拟网络 B，选择相同的控制面板，单击“创建资源”。
2. 搜索相应的实例，然后从 vNet B 子网分配一个 IP。
3. 如果存在类似于 vNet A 的静态临近 GSLB 负载平衡，则启动应用程序服务器和 DNS 转发器。
4. 在中编辑 vNet B DNS 转发器设置 `named.conf.options` ，如以下设置所示：

   VNet B DNS 转发器设置：

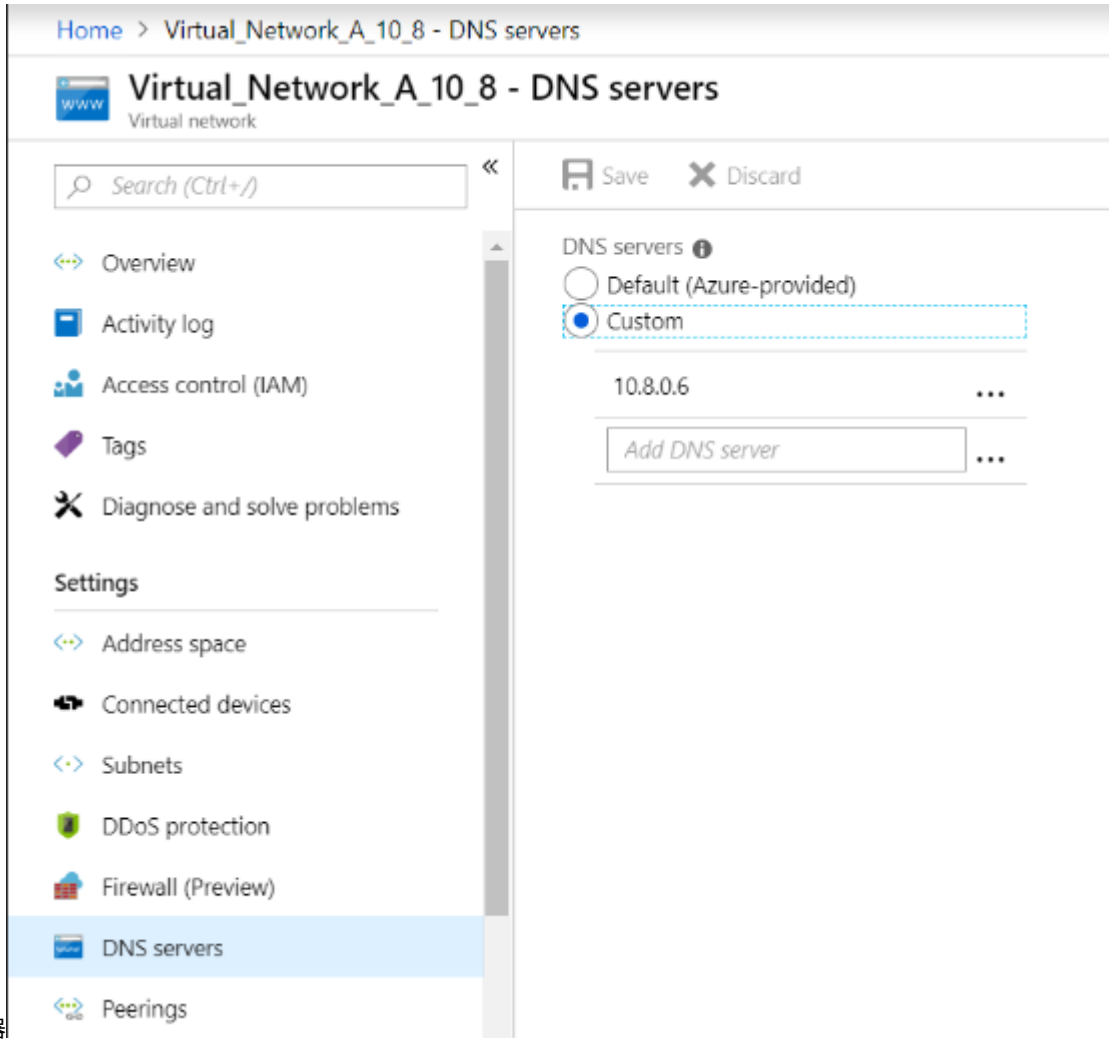
```
      zone "ptm.mysite.net" {

          type forward;
```



```
4            forwarders {
5    10.8.0.5;  }
6   ;
7          }
8   ;
```



下图描绘了 vNet B 的 DNS 转发器设置：



DNS 服务器

在本地部署应用程序服务器、**DNS** 转发器和 **Windows 10** 专业版客户端

1. 对于本地，请在裸机上启动虚拟机，然后使用类似于 vNet A 的应用程序服务器、DNS 转发器和 Windows 10 pro 客户端。
2. 在中编辑本地 DNS 转发器设置 `named.conf.options`，如以下示例所示。

本地 **DNS** 转发器设置

```
1        zone "mysite.net" {
2
3                    type forward;
4                    forwarders {
5     10.8.0.6;   }
6    ;
7           }
8    ;
9        zone "ptm.mysite.net" {
10
```



```
11            type forward;
12            forwarders {
13     10.8.0.5;  }
14    ;
15          }
16    ;
```

因为 mysite.net，我们提供了 vNet A 的 DNS 转发器 IP，而不是 Azure 私有 DNS 区域服务器 IP，因为这是一个特殊的 IP 地址，无法从本地访问。因此，需要在本地的 DNS 转发器设置中进行此更改。

在 **Azure** 虚拟网络上配置 **NetScaler**

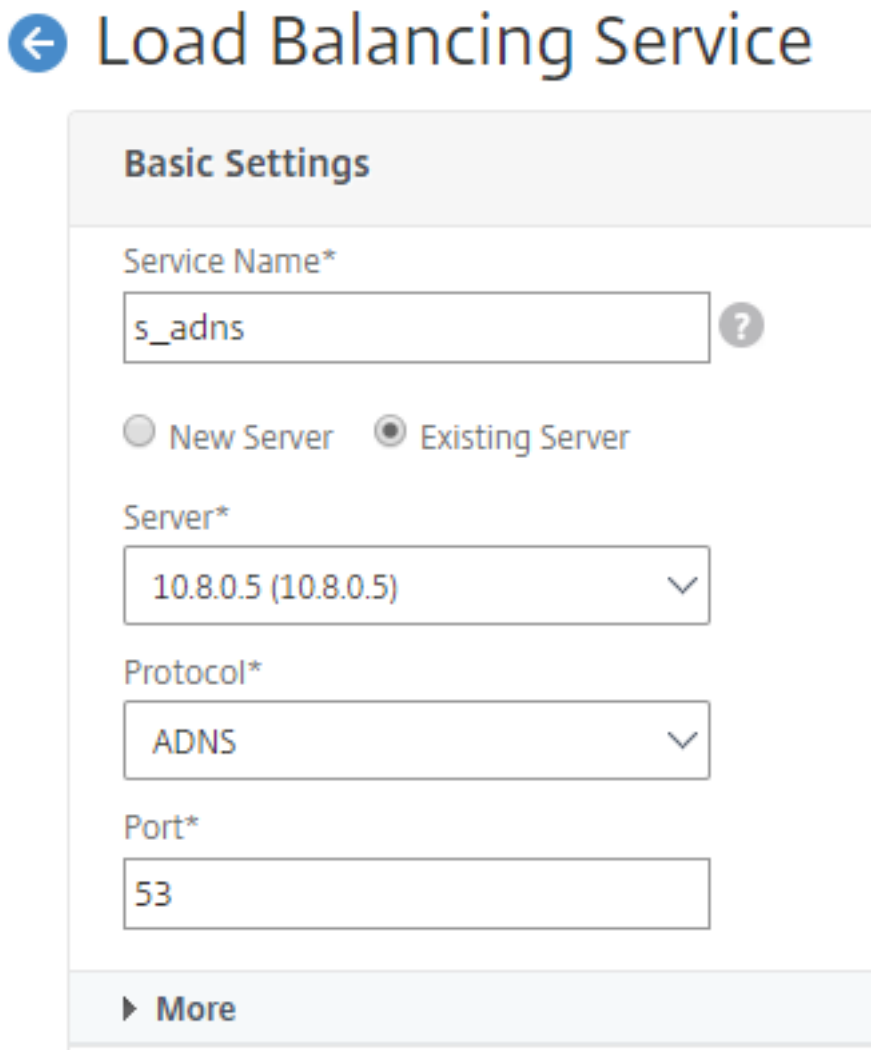
如拓扑所示，在 Azure 虚拟网络（在本例中为 vNet A）上部署 NetScaler，然后通过 NetScaler GUI 对其进行访问。

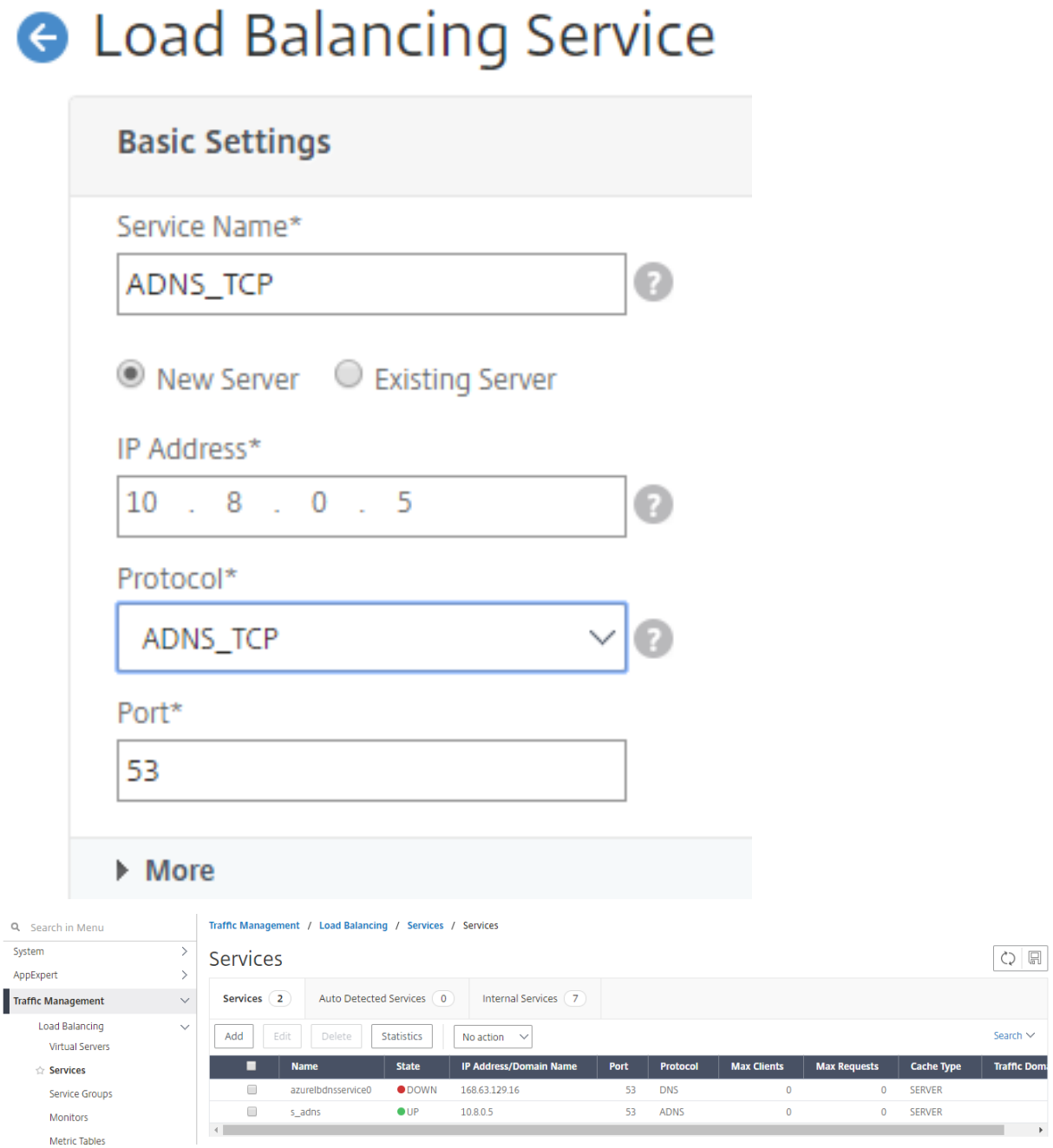
配置 **NetScaler GSLB**

1. 创建 ADNS 服务。
2. 创建本地和远程站点。
3. 为本地虚拟服务器创建服务。
4. 为 GSLB 服务创建虚拟服务器。

添加 **ADNS** 服务

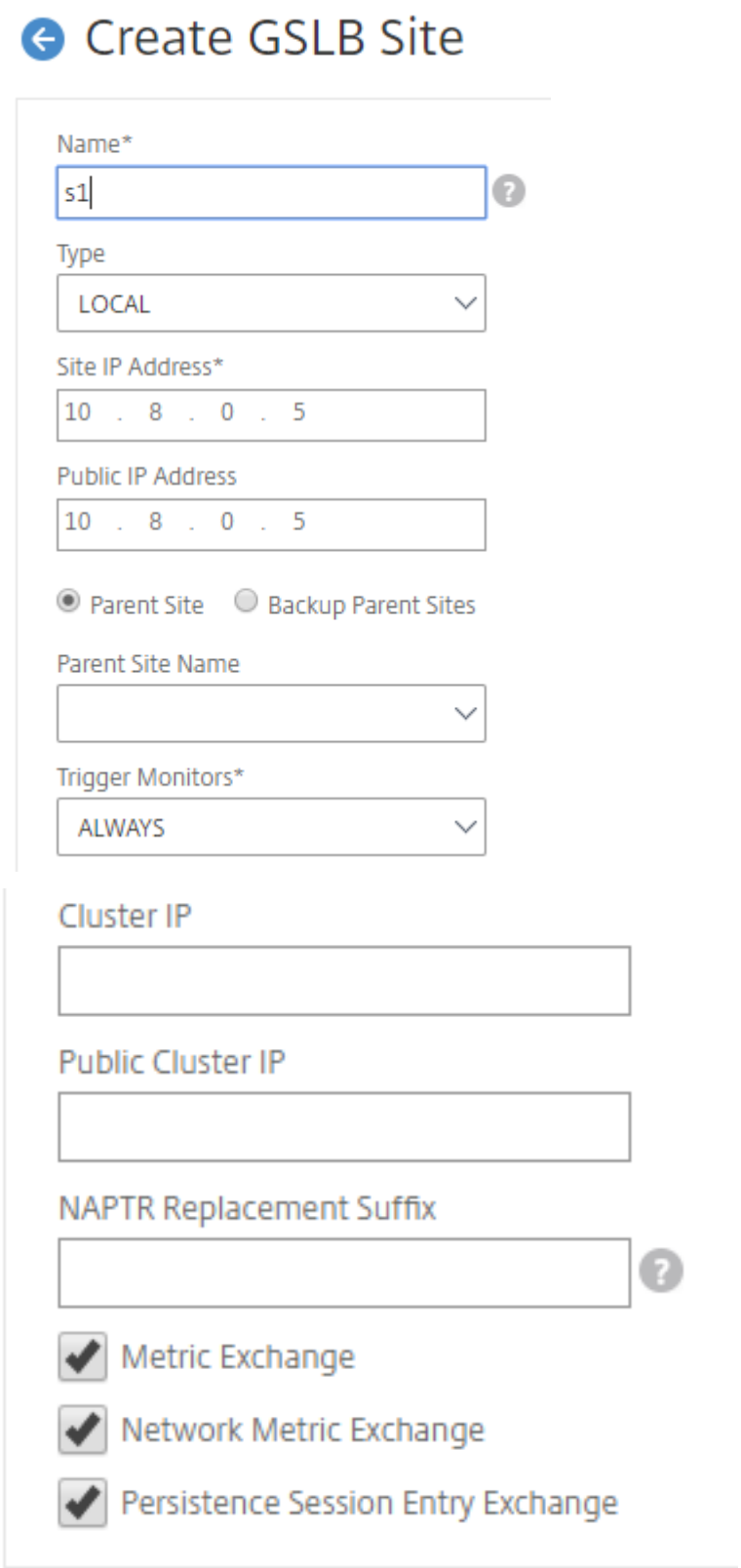
1. 登录 NetScaler GUI。
2. 在“配置”选项卡中，导航到“流量管理” **>** “负载平衡” **>** “服务”。
3. 添加服务。我们建议您在 TCP 和 UDP 中同时配置 ADNS 服务，如下图所示：

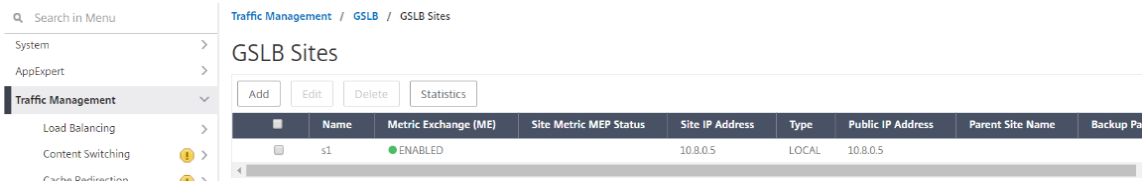




添加 **GSLB** 网站

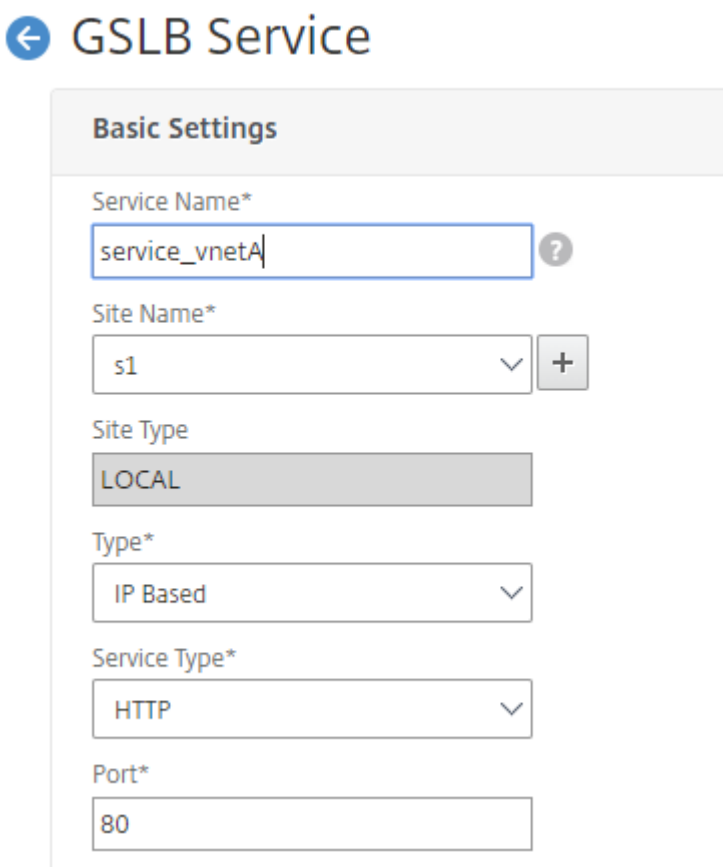
1. 添加要在其中配置 GSLB 的本地和远程站点。
2. 在 配置 选项卡上，导航到 流量管理 **> GSLB > GSLB** 站点。添加一个站点，如以下示例所示，然后对其他站点重复相同的步骤。





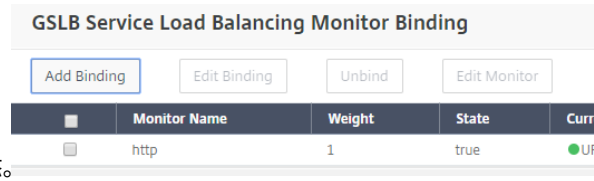
添加 **GSLB** 服务

1. 为本地和远程虚拟服务器添加 GSLB 服务，以平衡应用程序服务器的负载。
2. 在 配置 选项卡上，导航到 流量管理 **> GSLB > GSLB** 服务。
3. 添加服务，如以下示例所示。
4. 绑定 HTTP 监视器以检查服务器状态。

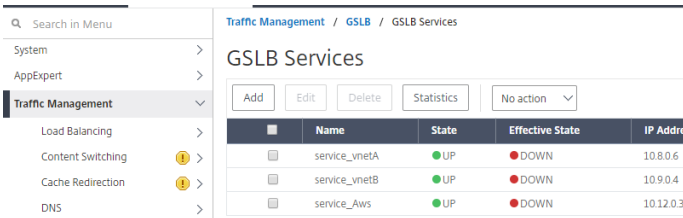


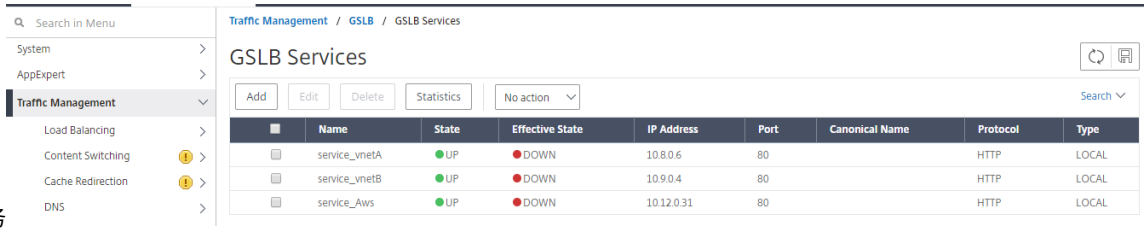
5. 创建服务后，转到 GSLB 服务内的 高级设置 选项卡。

6. 单击“添加监视器”将 GSLB 服务与 HTTP 监视器绑定以显示服务状态。



7. 与 HTTP 监视器绑定后，服务状态将标记为 UP，如下图所示：



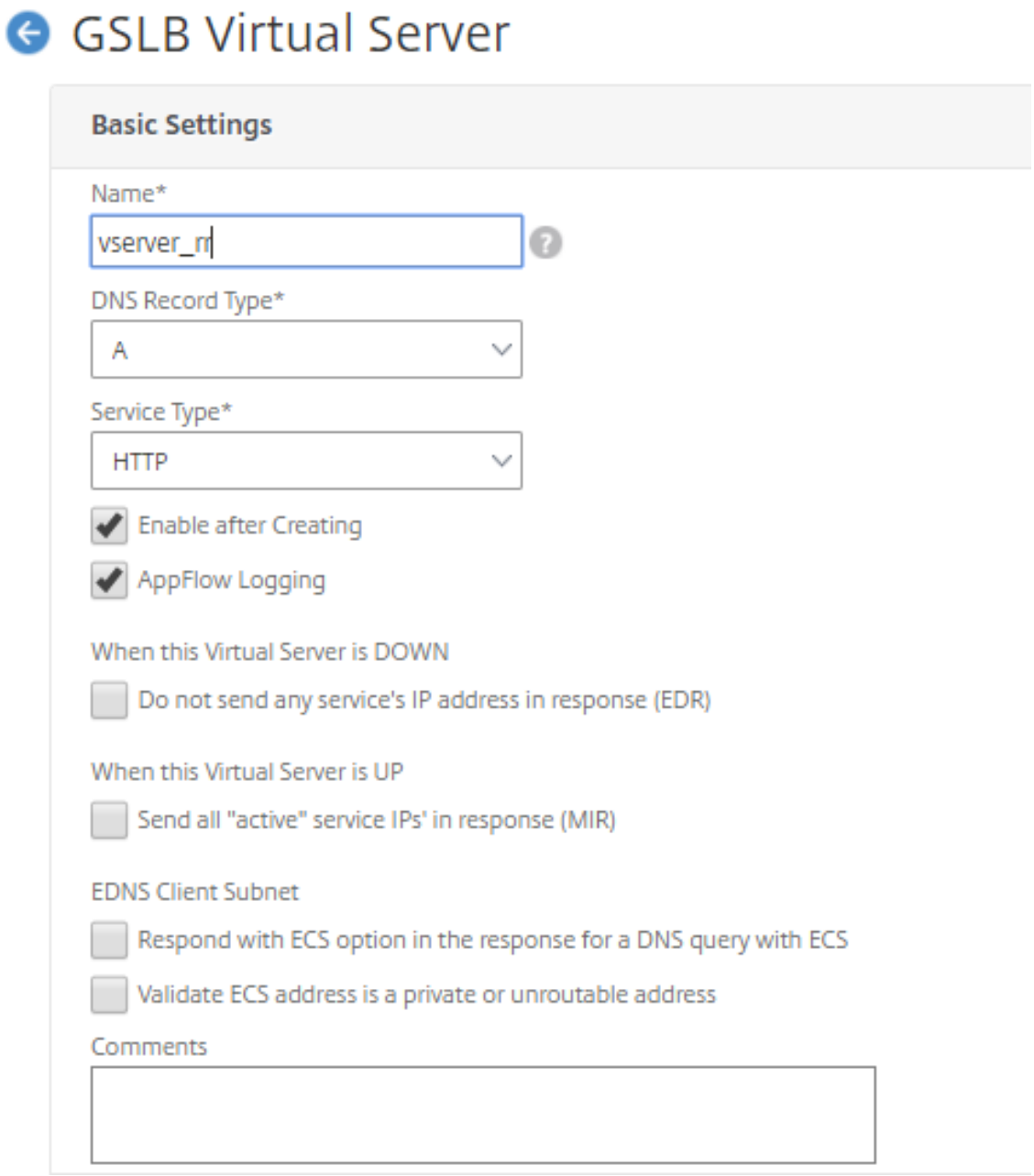


务

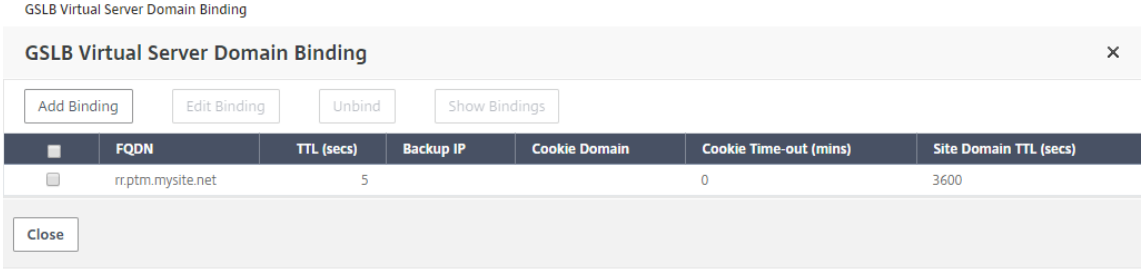
添加 **GSLB** 虚拟服务器

添加 GSLB 虚拟服务器，通过该服务器可以访问应用程序服务器的别名 GSLB 服务。

1. 在 配置 选项卡上，导航到 流量管理 **> GSLB > GSLB** 虚拟服务器。
2. 添加虚拟服务器，如以下示例所示。
3. 将 GSLB 服务和域名绑定到它。

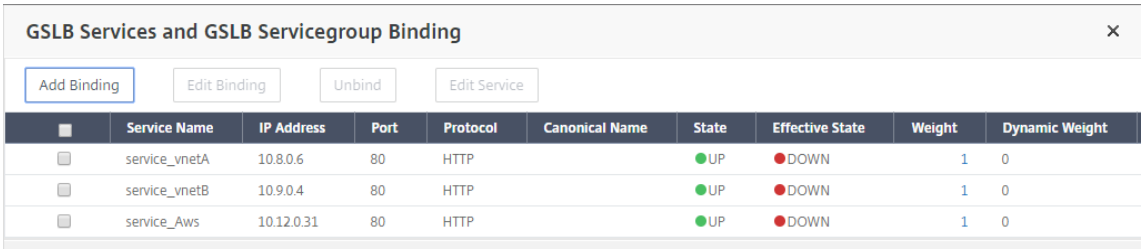


4. 创建 GSLB 虚拟服务器并选择适当的负载平衡方法（在本例中为轮询）后，绑定 GSLB 服务和域以完成该步骤。

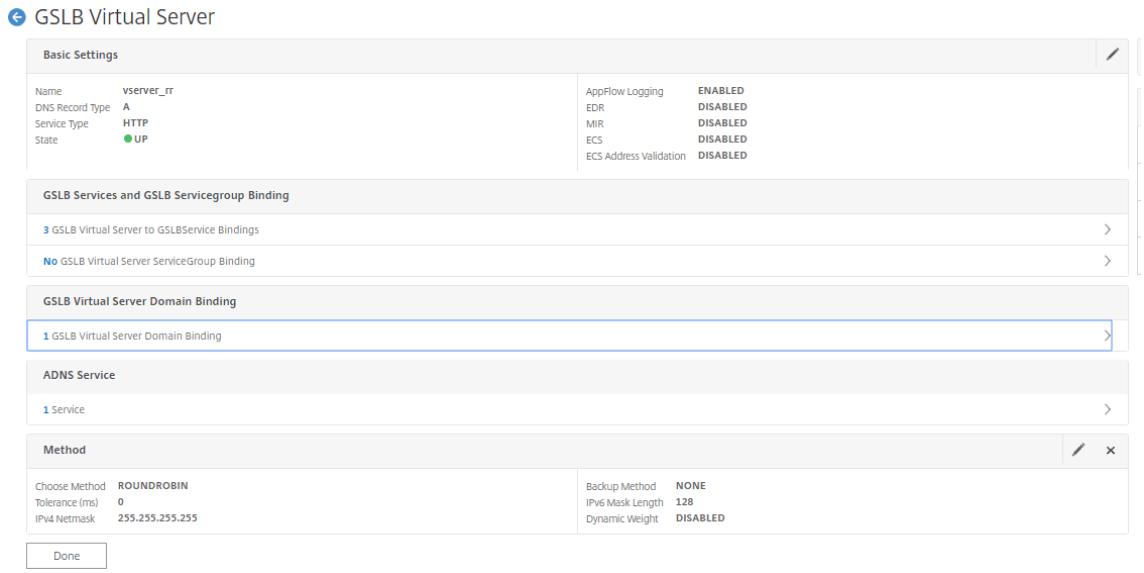


5. 转到虚拟服务器内的 高级设置 选项卡，然后单击 添加域 选项卡绑定域。

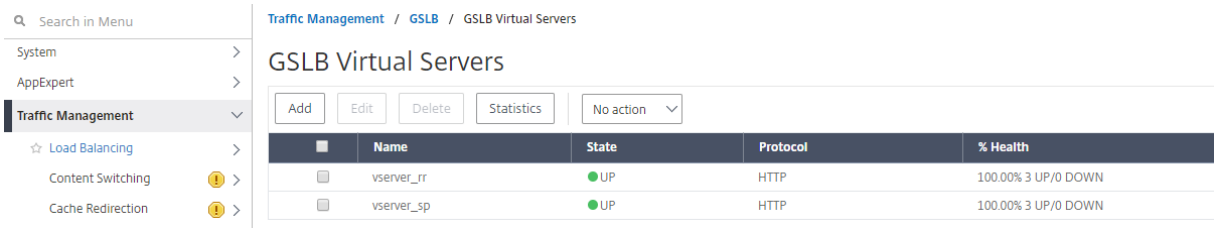
6. 转至 高级 > 服务，然后单击箭头绑定 GSLB 服务，并将所有三个服务（vNet A、vNet B、本地）绑定到虚拟服务器。



将 GSLB 服务和域绑定到虚拟服务器后，它将如下图所示：



检查 GSLB 虚拟服务器是否已启动且 100% 正常。当监视器显示服务器已启动且运行正常时，表示站点处于同步状态，并且后端服务可用。



要测试部署，请 `rr.ptm.mysite.net` 从云客户端计算机或本地客户端计算机访问域 URL。如果您从云端 Windows 客户端计算机访问它，请确保在私有 DNS 区域中访问本地应用程序服务器，无需第三方或自定义 DNS 解决方案。

配置 NetScaler VPX 实例以使用 Azure 加速网络

October 17, 2024

加速网络使虚拟机的单根 I/O 虚拟化 (SR-IOV) 虚拟功能 (VF) NIC 能够连接到虚拟机，从而提高了网络性能。可以将此功能用于需要以更高吞吐量发送或接收数据的繁重工作负载，具有可靠的流技术推送和较低的 CPU 利用率。当使用加速联网启用 NIC 时，Azure 将网卡的现有分段虚拟化 (PV) 接口与 SR-IOV VF 接口捆绑在一起。SR-IOV VF 接口的支持可实现并增强 NetScaler VPX 实例的吞吐量。

加速的网络连接提供了以下优势：

- 更低的延迟
- 更高的每秒数据包 (pps) 性能
- 增强的吞吐量
- 降低了抖动
- CPU 利用率降低

> 注意：
>
> 从版本 13.0 版本 76.29 起，NetScaler VPX 实例支持 Azure 加速联网。

必备条件

- 确保您的 VM 大小符合 Azure 加速的网络连接的要求。
- 在任何 NIC 上启用加速的网络连接之前，请停止 VM（单个 VM 或可用性集中的 VM）

限制

只能在某些实例类型上启用加速的网络连接。有关更多信息，请参阅 支持的实例类型。

支持加速的网络连接的 NIC

Azure 在 SR-IOV 模式下提供 Mellanox ConnectX3、ConnectX4 和 ConnectX5 网卡，用于加速联网。

在 NetScaler VPX 接口上启用加速联网后，Azure 会将 ConnectX3、ConnectX4 或 ConnectX5 接口与 NetScaler VPX 设备的现有 PV 接口捆绑在一起。

有关在将接口连接到虚拟机之前启用加速网络的更多信息，请参阅 创建具有加速网络连接的网络接口。

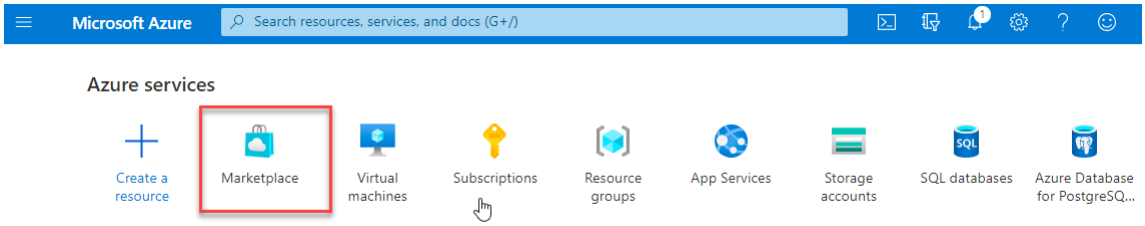
有关在虚拟机上的现有接口上启用加速联网的更多信息，请参阅在虚拟 机上启用现有接口。

如何使用 **Azure** 控制台在 **NetScaler VPX** 实例上启用加速联网

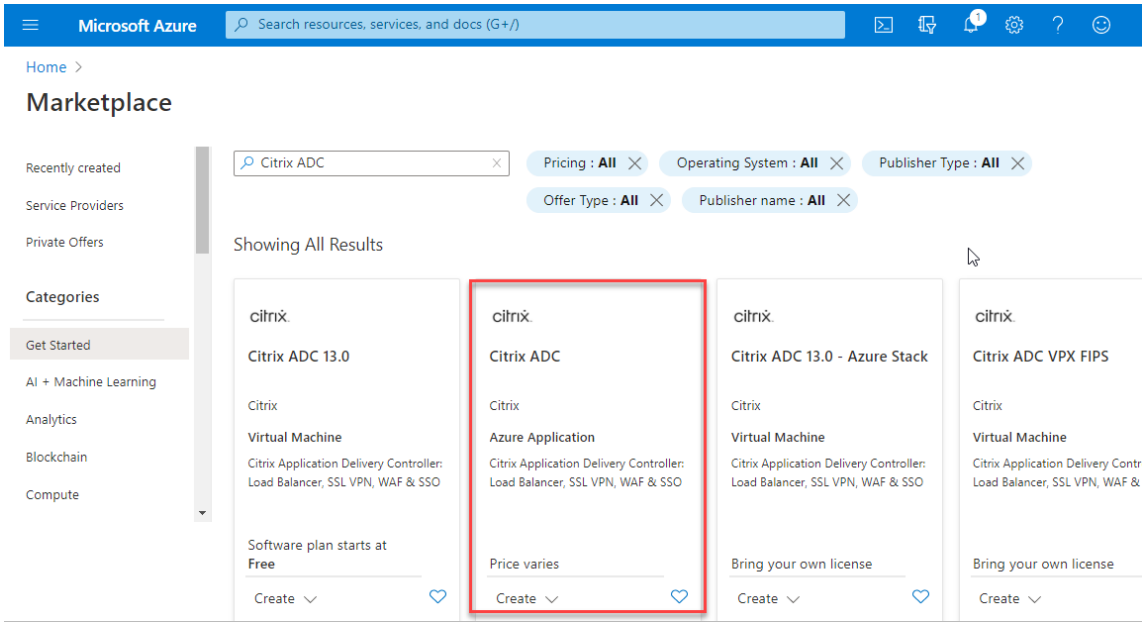
可以使用 Azure 控制台或 Azure PowerShell 在特定界面上启用加速的网络连接。

请执行以下步骤，通过使用 Azure 可用性集或可用区启用加速联网。

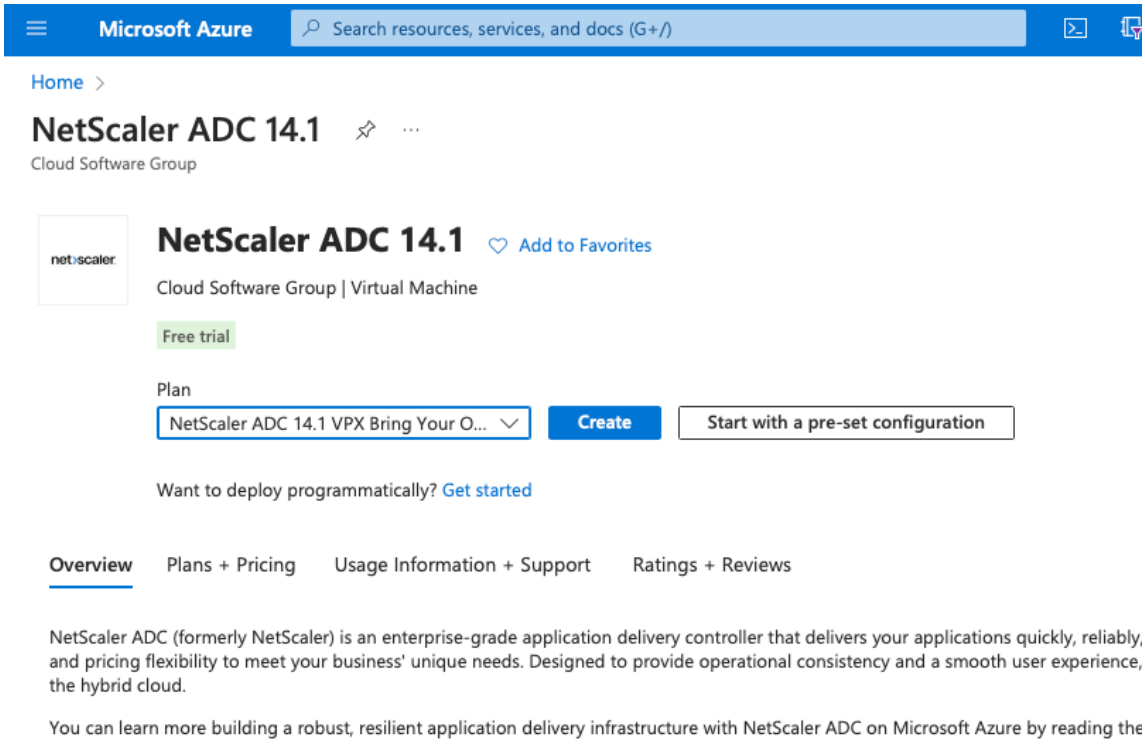
1. 登录 Azure 门户，然后导航到 **Azure** 市场。



2. 在 **Azure** 市场中，搜索 **NetScaler**。

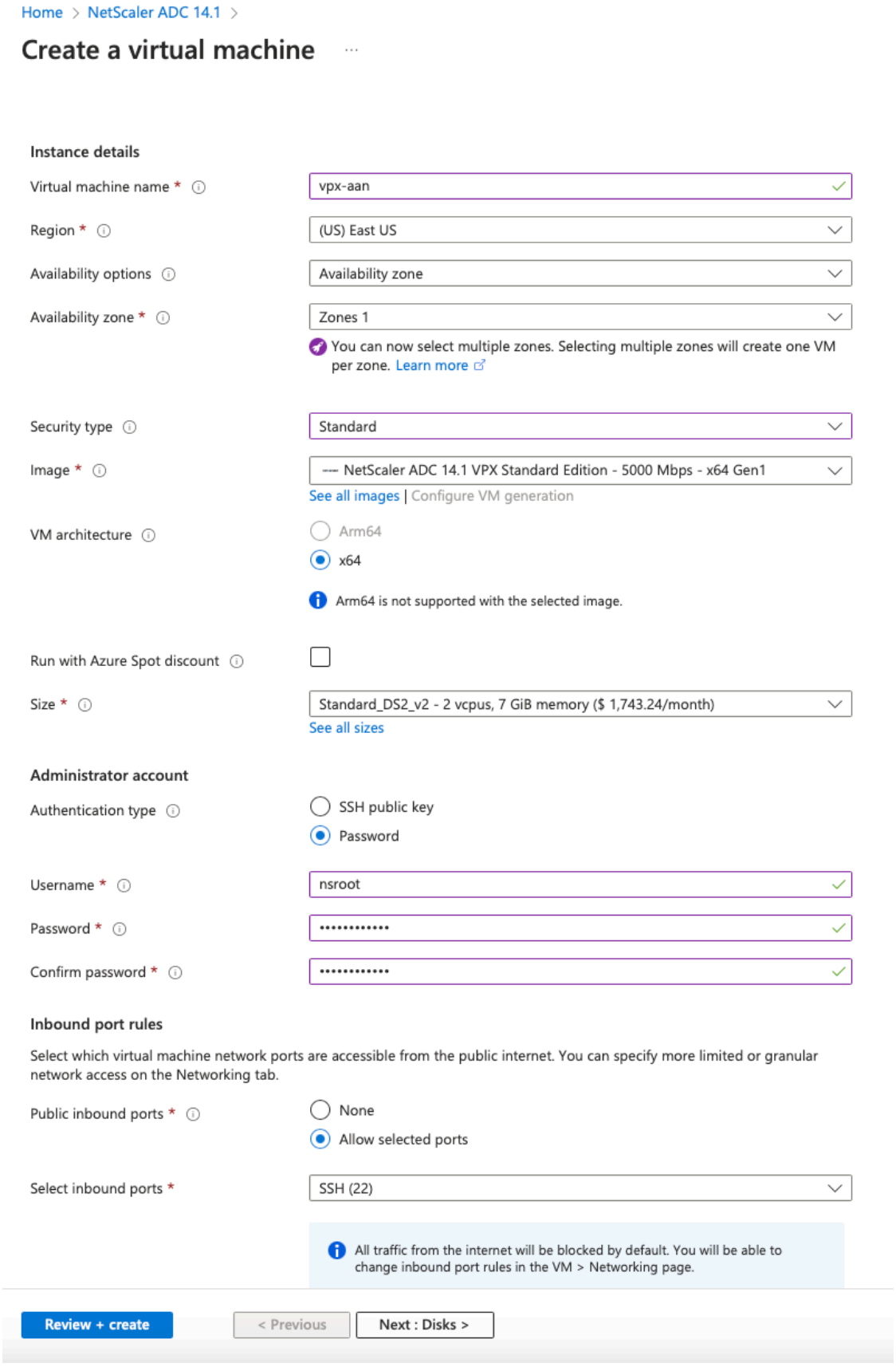


3. 选择非 FIPS NetScaler 计划以及许可证，然后单击 创建。



将出现“创建 **NetScaler**”页面。

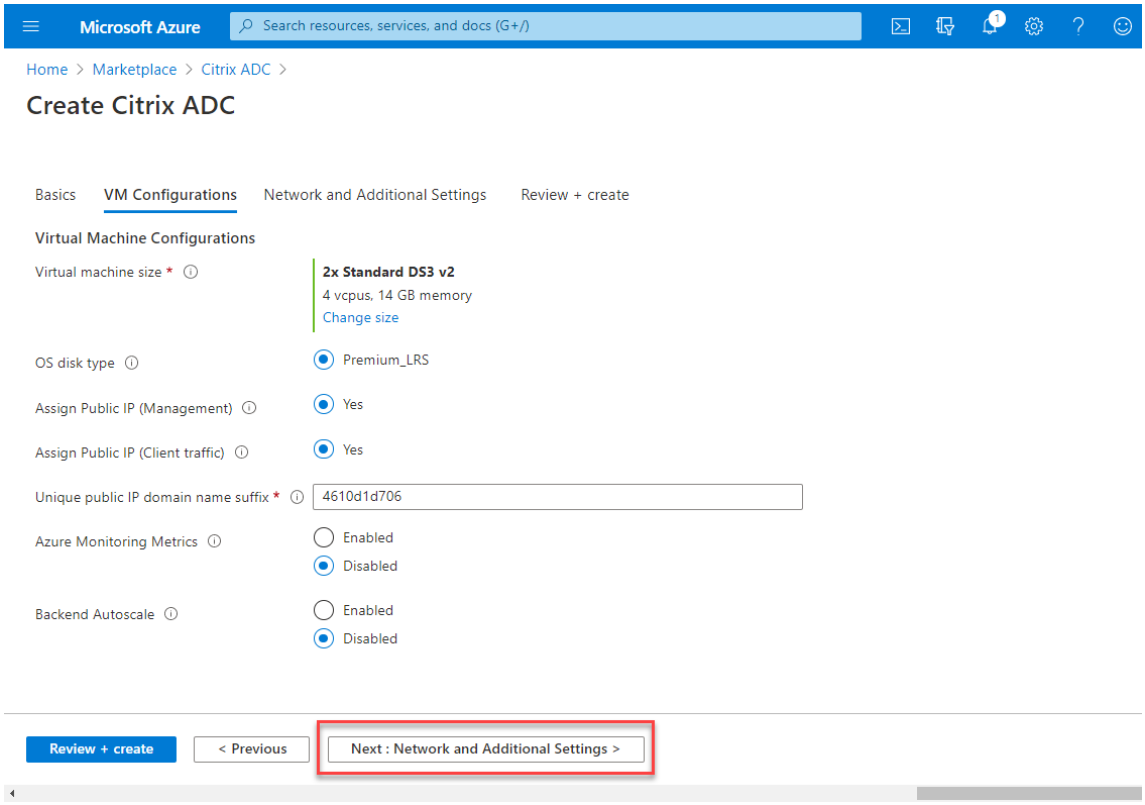
4. 在 **Basics**（基础知识）选项卡中，创建资源组。在 **Parameters**（参数）选项卡下，输入“Region”（区域）、“Admin user name”（管理员用户名）、“Admin Password”（管理员密码）、“license type (VM SKU)”（许可证类型 (VM SKU)）以及其他字段的详细信息。



5. 单击 **Next : VM Configurations >**（下一步: VM 配置 >）。

   在 **VM Configurations**（VM 配置）页面上，执行以下操作:

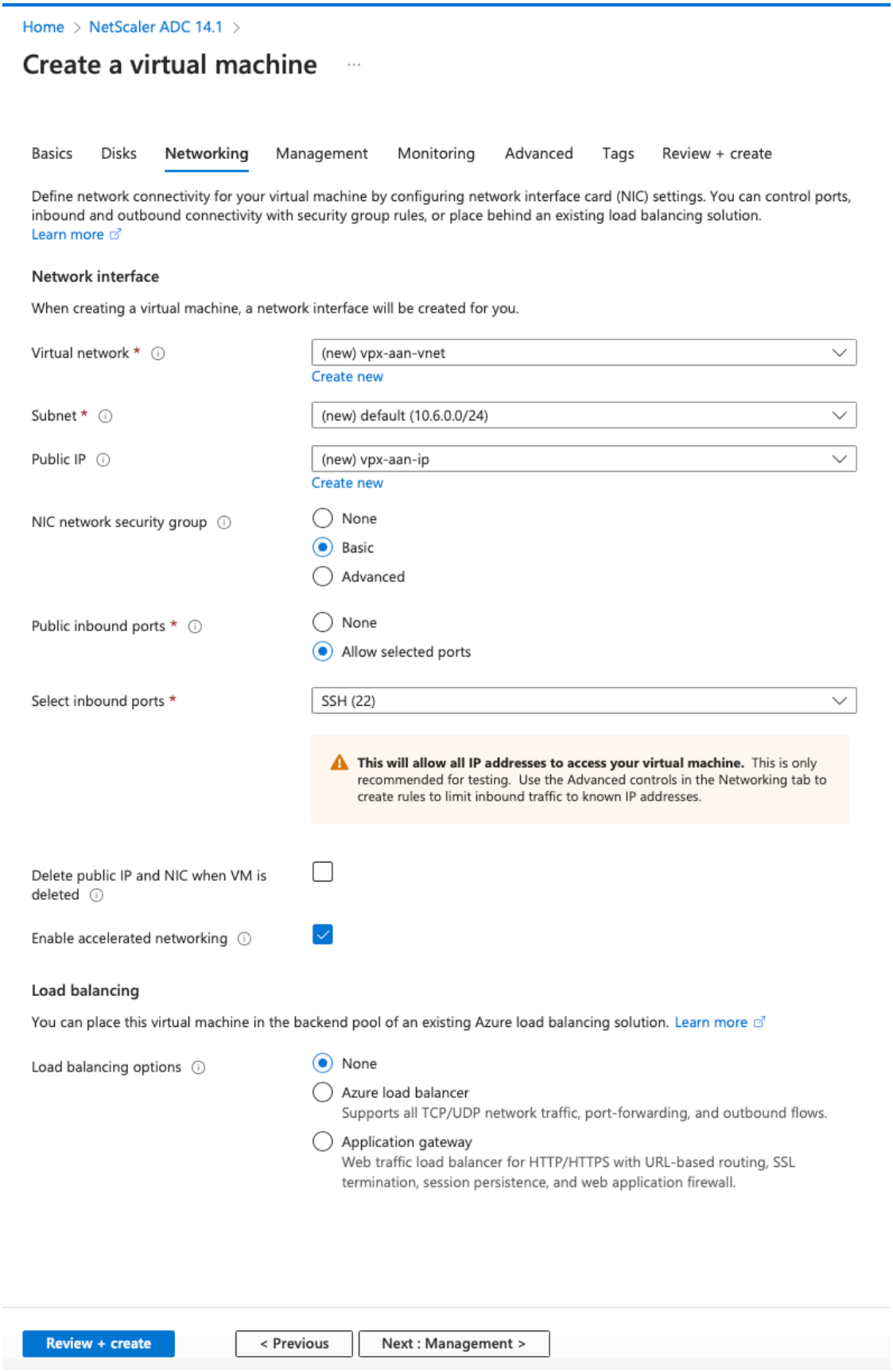
   a) 配置公有 IP 域名后缀。
   b) 启用或禁用 **Azure Monitoring Metrics**（Azure 监视指标）。
   c) 启用或禁用 **Backend Autoscale**（后端 Autoscale）。



6. 单击 **Next: Network and Additional settings >**（下一步: 网络和其他设置 >）。

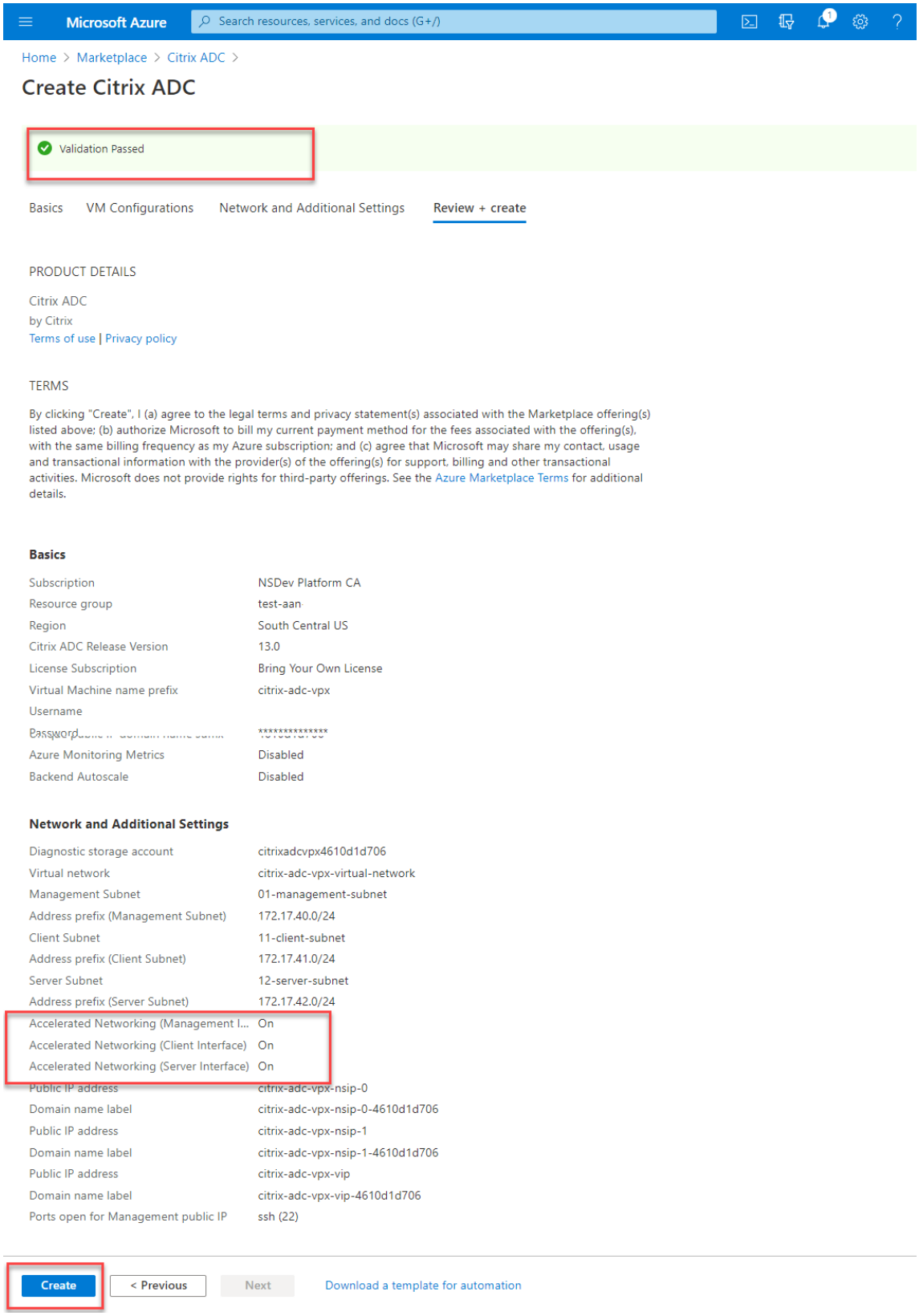
   在 **Network and Additional Settings**（网络和其他设置）页面上，创建启动诊断帐户并配置网络设置。

   在 **Accelerated Networking**（加快的网络连接）部分下，可以选择为管理接口、客户端接口和服务器接口分别启用或禁用加速的网络连接。

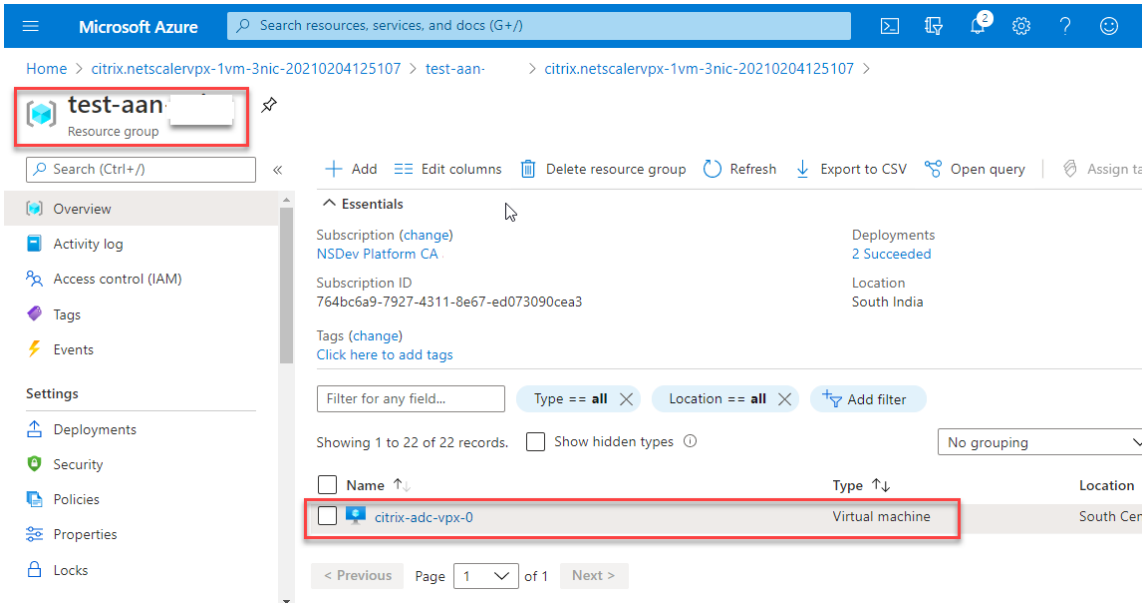


7. 单击 **Next: Review + create >**（下一步: 检查 + 创建 >）。

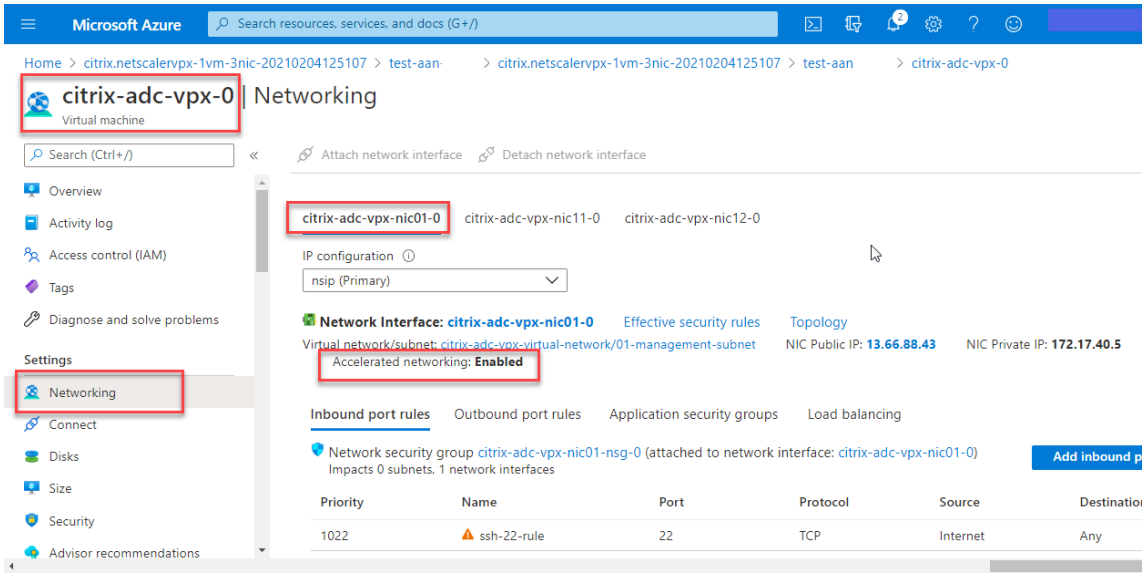
   验证成功后，查看基本设置、VM 配置、网络和其他设置，然后单击 **Create**（创建）。可能需要一段时间采用所需配置来创建 Azure 资源组。



8. 部署完成后，选择资源组以查看配置详细信息。



9. 要验证加速的网络连接配置，请选择 **Virtual machine**（虚拟机）**> Networking**（网络连接）。每个 NIC 的加速的网络连接状态显示为 **Enabled**（已启用）或 **Disabled**（已禁用）。



使用 **Azure PowerShell** 启用加速的网络连接

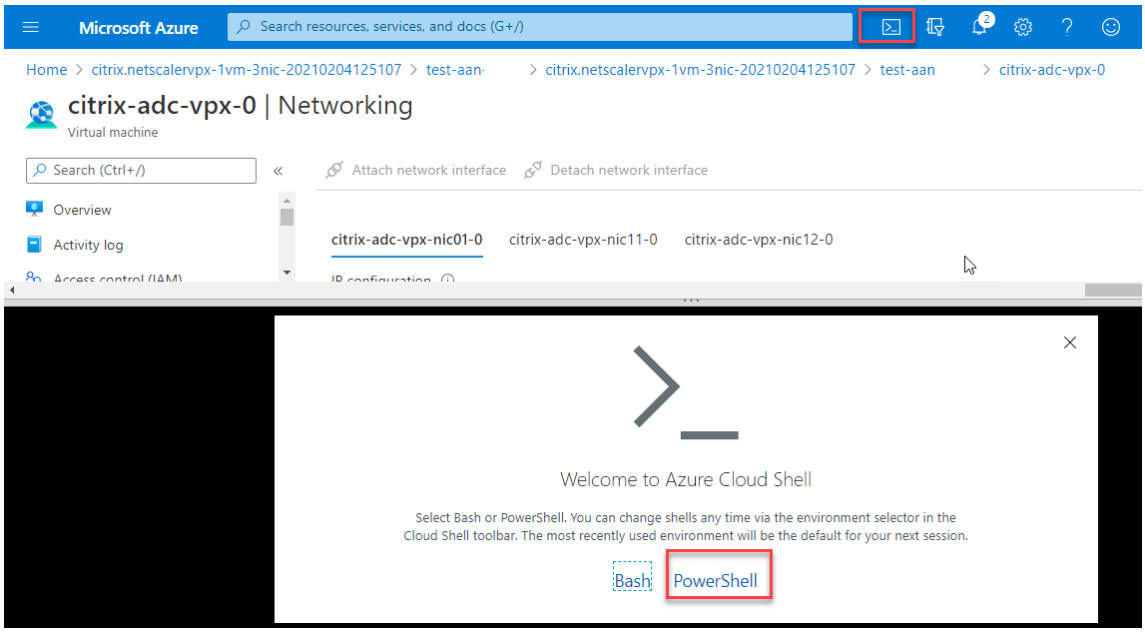
如果需要在创建 VM 后启用加速的网络连接，则可以使用 Azure PowerShell 来执行此操作。

> 注意：
>
> 确保在使用 Azure PowerShell 启用加速的网络连接之前停止 VM。

执行以下步骤以使用 Azure PowerShell 启用加速的网络连接。

1. 导航到 **Azure portal**（Azure 门户），单击右上角的 **PowerShell** 图标。

> 注意：
>
> 如果您处于 Bash 模式，请切换到 PowerShell 模式。



2. 在命令提示符下，运行以下命令：

```
az network nic update --name <nic-name> --accelerated-networking
    [true | false] --resource-group <resourcegroup-name>
```

加速的网络连接参数接受以下任一值：

- **True**：在指定的 NIC 上启用加速的网络连接。
- **False**：在指定的 NIC 上禁用加速的网络连接。

要在特定 **NIC** 上启用加速的网络连接，请执行以下操作：

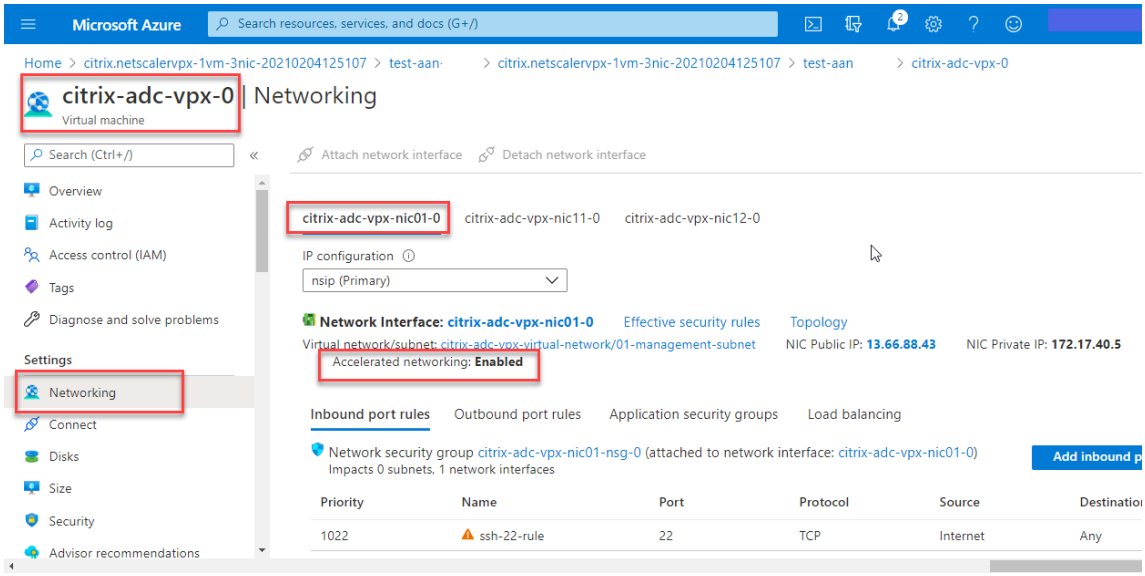
```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking true --resource-group rsgp1-aan
```

要在特定 **NIC** 上禁用加速的网络连接，请执行以下操作：

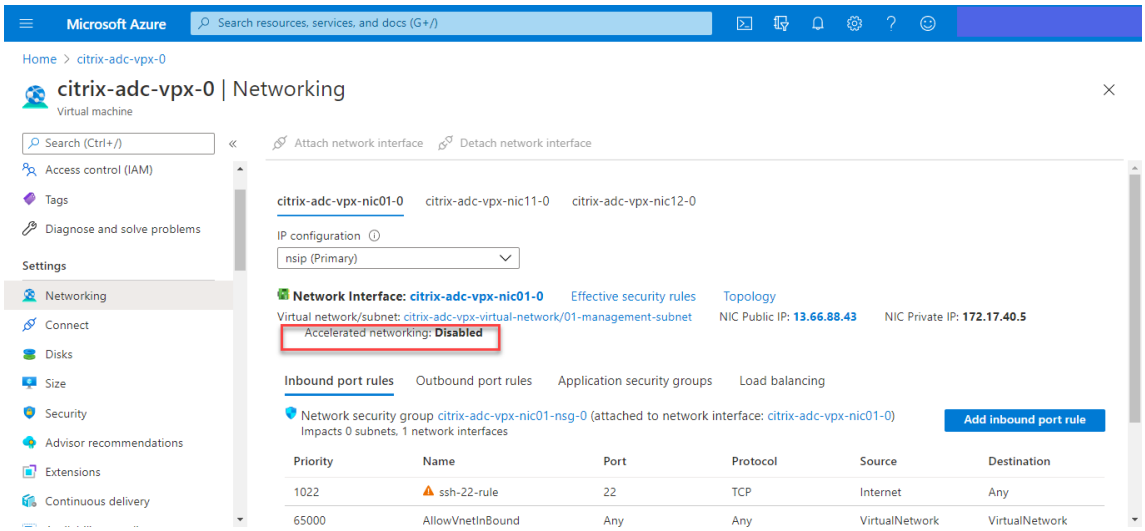
```
az network nic update --name citrix-adc-vpx-nic01-0 --
    accelerated-networking false --resource-group rsgp1-aan
```

3. 要验证部署完成后的加速联网状态，请导航到 虚拟机 **>** 联网。

在以下示例中，您可以看到加速的网络连接处于 **Enabled**（已启用）状态。



在以下示例中，您可以看到加速的网络连接处于 **Disabled**（已禁用）状态。



使用 **NetScaler** 的 **FreeBSD Shell** 在接口上验证网络连接的加速

您可以登录 NetScaler 的 FreeBSD 外壳，然后运行以下命令来验证加速的联网状态。

ConnectX3 NIC 的示例：

以下示例显示了 Mellanox ConnectX3 NIC 的“ifconfig”命令输出。“50/n”表示 Mellanox ConnectX3 NIC 的 VF 接口。0/1 和 1/1 表示 NetScaler VPX 实例的 PV 接口。您可以观察到 PV 接口 (1/1) 和 CX3 VF 接口 (50/1) 具有相同的 MAC 地址 (00:22:48:1c:99:3e)。这表示两个接口已捆绑在一起。


```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

ConnectX4 NIC 的示例：

以下示例显示了 Mellanox ConnectX4 NIC 的“ifconfig”命令输出。“100/n”表示 Mellanox ConnectX4 NIC 的 VF 接口。0/1、1/1 和 1/2 表示 NetScaler VPX 实例的 PV 接口。您可以观察到 PV 接口 (1/1) 和 CX4 VF 接口 (100/1) 具有相同的 MAC 地址 (00:0d:3a:9b:f2:1d)。这表示两个接口已捆绑在一起。同样，PV 接口 (1/2) 和 CX4 VF 接口 (100/2) 具有相同的 MAC 地址 (00:0d:3a:1e:d2:23)。


```
root@SmartNIC-CX4-NS-DUT-NEW1# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:9b:f2:1d
        inet 10.0.1.29 netmask 0xffffff00 broadcast 10.0.1.255
        inet6 fe80::20d:3aff:fe9b:f21d%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active

1/2: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:1e:d2:23
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active

100/1: flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:0d:3a:9b:f2:1d
        media: Ethernet autoselect <full-duplex,rxpause,txpause> (autoselect
<full-duplex,rxpause>)
        status: active

100/2: flags=8a03<UP,BROADCAST,ALLMULTI,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:0d:3a:1e:d2:23
        media: Ethernet autoselect <full-duplex,rxpause,txpause> (autoselect
<full-duplex,rxpause>)
        status: active
```

使用 **ADC CLI** 验证接口上的加速的网络连接

ConnectX3 NIC 的示例：

以下 show interface 命令输出表示 PV 接口 1/1 与虚拟函数 50/1 捆绑在一起，即 SR-IOV VF NIC。1/1 和 50/1 NIC 的 MAC 地址相同。启用加速的网络连接后，1/1 接口的数据将通过 50/1 接口的数据路径发送，该接口是 ConnectX3 接口。您可以看到 PV 接口 (1/1) 的“显示接口”输出指向 VF (50/1)。同样，VF 接口 (50/1) 的“show interface”输出指向 PV 接口 (1/1)。


```
> show interface 1/1

        Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1, Datapath 50/1) #1
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done

> show interface 50/1

      Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s
        Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
```

ConnectX4 NIC 的示例：

以下 show interface 命令输出表示 PV 接口 1/1 与虚拟函数 100/1 捆绑在一起，即 SR-IOV VF NIC。1/1 和 100/1 NIC 的 MAC 地址相同。启用加速的网络连接后，1/1 接口的数据将通过 100/1 接口的数据路径发送，即 ConnectX4 接口。您可以看到 PV 接口的“show interface”输出 (1/1) 指向 VF (100/1)。同样，VF 接口 (100/1) 的“show interface”输出指向 PV 接口 (1/1)。

```
> show interface 1/1

1)      Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 100/1, Datapath 100/1) #0
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d, uptime 10h49m10s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(310366) Bytes(98476082) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(44) Bytes(6368) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.


 Done
> show interface 100/1

1)      Interface 100/1 (CX4 VF Interface, SmartNIC, PV 1/1) #3
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=10, MAC=00:0d:3a:9b:f2:1d, uptime 10h49m11s
        Actual: media FIBER, speed NONE, duplex FULL, fctl NONE, throughput
0
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(1135870) Bytes(1487381079) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(1143020) Bytes(143165922) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.


 Done
>
```


NetScaler 中的注意事项

- PV 接口被视为所有必要操作的主接口。只能在 PV 接口上执行配置。
- VF 接口上的所有“设置”操作都被阻止，但以下情况除外：
  - 启用接口
  - 禁用接口
  - reset interface
  - 清除统计信息

> 注意：
>
> Citrix 建议您不要在 VF 接口上执行任何操作。

- 您可以使用 `show interface` 命令验证 PV 接口与 VF 接口的绑定。
- 从 NetScaler 版本 13.1-33.x 开始，NetScaler VPX 实例可以无缝处理 Azure 加速网络中移除和重新连接已删除网卡的动态 NIC。Azure 可以在其主机维护活动中移除加速联网的 SR-IOV VF NIC。每当从 Azure 虚拟机中删除 NIC 时，NetScaler VPX 实例都会将接口状态显示为“链接关闭”，并且流量仅通过虚拟接口。重新连接已移除的 NIC 后，VPX 实例将使用重新连接的 SR-IOV VF NIC。此过程无缝进行，不需要任何配置。

将 VLAN 配置为 PV 接口

当 PV 接口绑定到 VLAN 时，关联的加速 VF 接口也绑定到与 PV 接口相同的 VLAN。在此示例中，PV 接口 (1/1) 绑定到 VLAN (20)。与 PV 接口 (1/1) 捆绑在一起的 VF 接口 (100/1) 也绑定到 VLAN 20。

Example:

1. 创建 VLAN。

```
add vlan 20
```

2. 将 VLAN 绑定到 PV 接口。

```
bind vlan 20  - ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2
```


> 注意：
>
> 不允许在加速的 VF 接口上执行 VLAN 绑定操作。

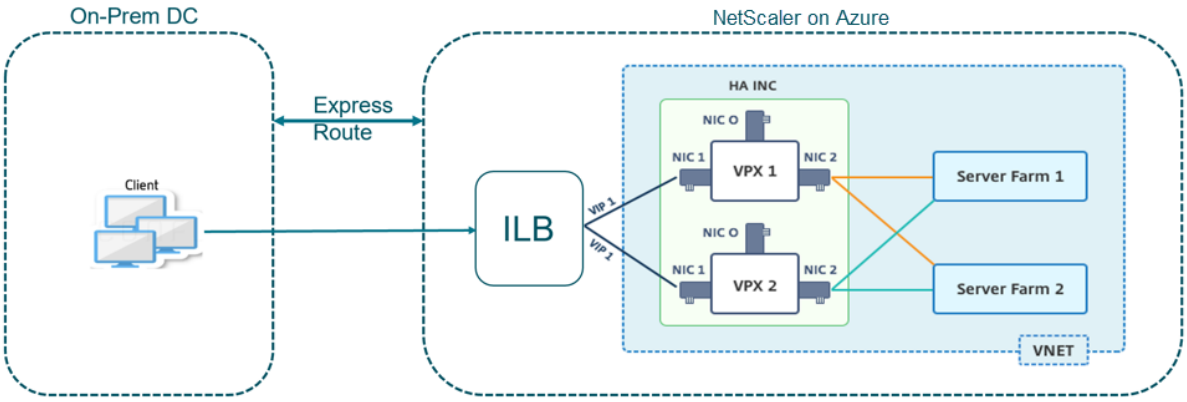
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
```

使用带有 **Azure ILB** 的 **NetScaler** 高可用性模板配置 **HA-INC** 节点

October 17, 2024

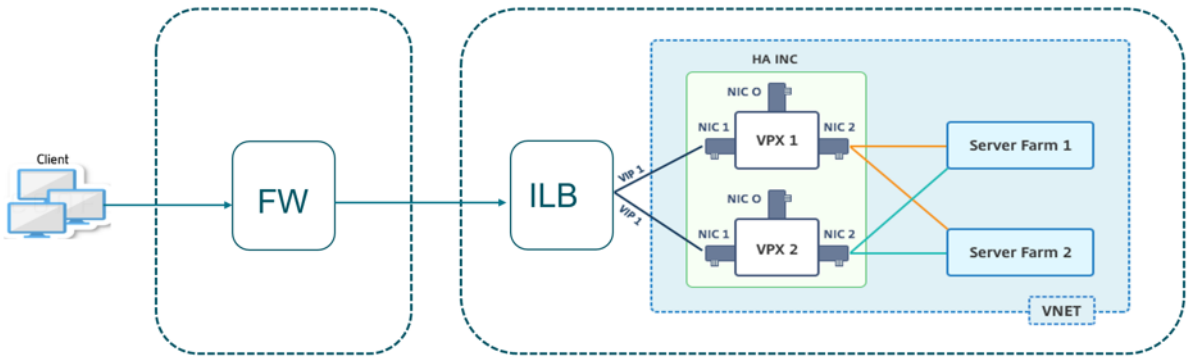
可以通过对 Intranet 应用程序使用标准模板快速高效地部署处于 HA-INC 模式的一对 VPX 实例。Azure 内部负载均衡器 (ILB) 使用内部 IP 地址或专用 IP 地址作为前端，如图 1 所示。模板会创建两个节点，使用三个子网和六个 NIC。这些子网用于管理流量、客户端流量和服务器端流量，每个子网都属于每台设备上的不同 NIC。

图 1：内部网络中客户端的 NetScaler HA 对



如图 2 所示，当 NetScaler HA 对位于防火墙后面时，您也可以使用此部署。公有 IP 地址属于防火墙，是 ILB 前端 IP 地址的 NAT 地址。

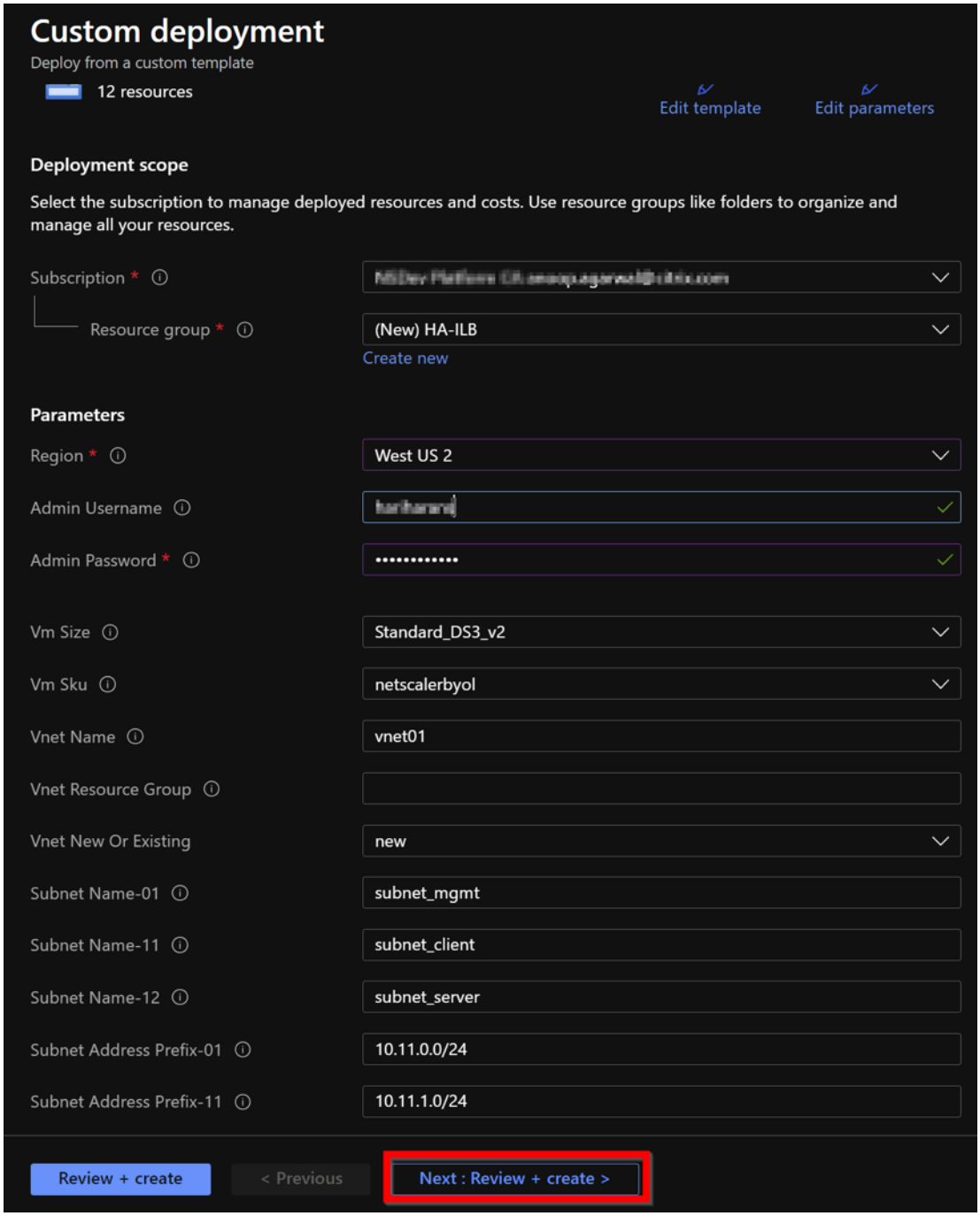
图 2：NetScaler 高可用性与具有公用 IP 地址的防火墙配对



您可以在 Azure 门户网站上获取内联网应用程序的 NetScaler HA 配对模板

完成以下步骤，通过使用 Azure 可用性集启动模板并部署高可用性 VPX 对。

1. 在 Azure 门户中，导航到 **Custom deployment**（自定义部署）页面。
2. 此时将显示 **Basics**（基本）页面。创建资源组。在 **Parameters**（参数）选项卡下，输入“Region”（区域）、“Admin user name”（管理员用户名）、“Admin Password”（管理员密码）、“license type (VM sku)”（许可证类型 (VM sku)）以及其他字段的详细信息。

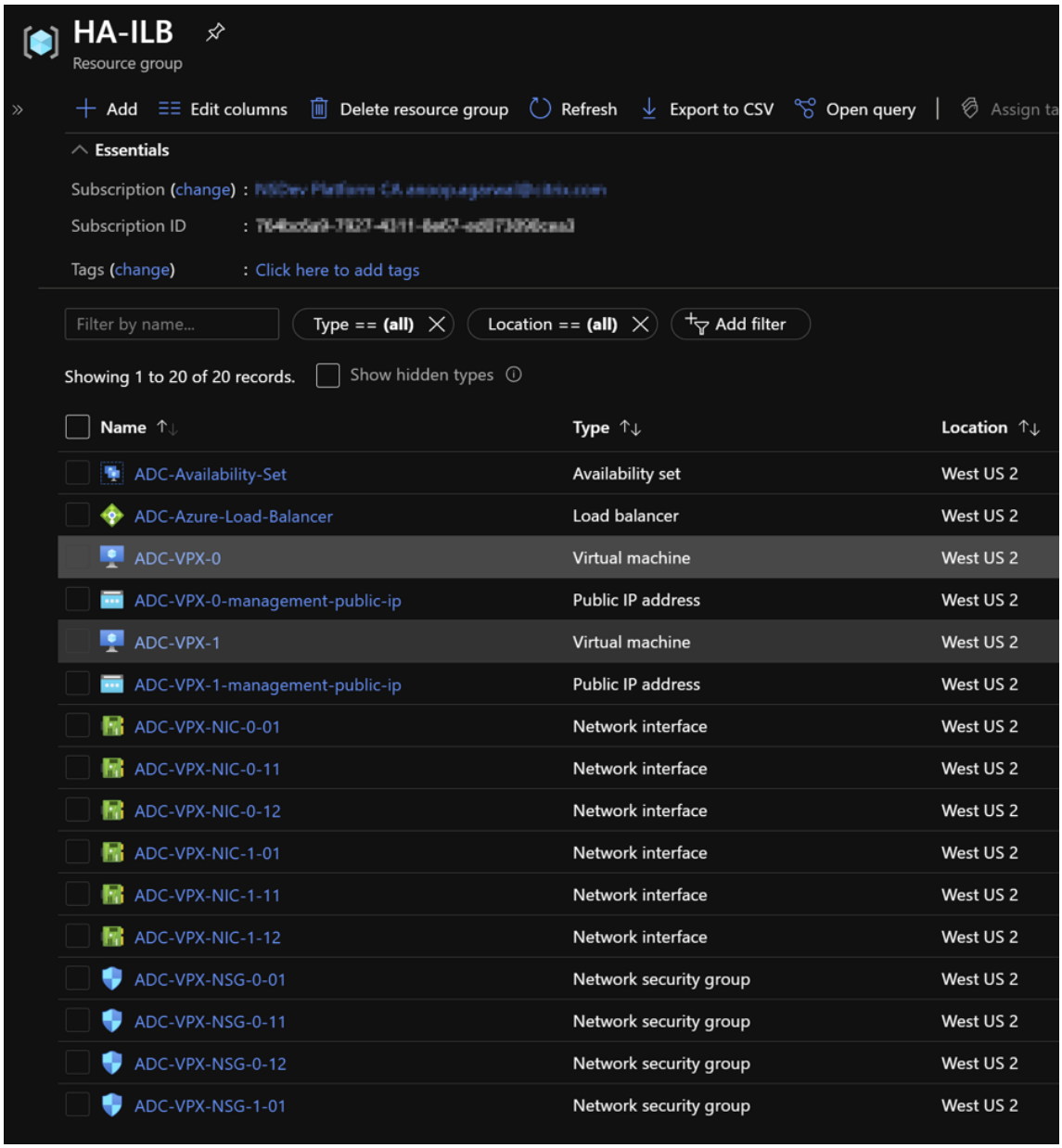


3. 单击 **Next: Review + create >**（下一步: 检查 + 创建 >）。

   可能需要一段时间采用所需配置来创建 Azure 资源组。完成后，在 Azure 门户中选择资源组以查看配置详细信息，例如 LB 规则、后端池、运行状况探测。高可用性对显示为 ADC-VPX-0 和 ADC-VPX-1。

   如果需要对您的高可用性设置进行进一步修改（例如，创建更多安全规则和端口），可以在 Azure 门户中完成。

   完成所需配置后，将创建以下资源。



4. 登录 **ADC-VPX-0** 和 **ADC-VPX-1** 节点以验证以下配置：

   - 两个节点的 NSIP 地址必须位于管理子网中。
   - 在主节点 (ADC-VPX-0) 和辅助节点 (ADC-VPX-1) 上，您必须看到两个 SNIP 地址。一个 SNIP（客户端子网）用于响应 ILB 探测，另一个 SNIP（服务器子网）用于后端服务器通信。

> 注意：
>
> 在 HA-INC 模式下，在同一子网中时 ADC-VPX-0 和 ADC-VPX-1 VM 的 SNIP 地址不同，这一点与传统的本地 ADC 高可用性部署不同，后者两者都相同。要在 VPX 对 SNIP 位于不同子网中时或 VIP 与 SNIP 不在同一子网中时支持部署，必须启用基于 Mac 的转发 (MBF)，或者为每个 VPX 节点的每个 VIP 添加静态主机路由。

在主节点 (ADC-VPX-0) 上

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.11.0.5        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.4        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

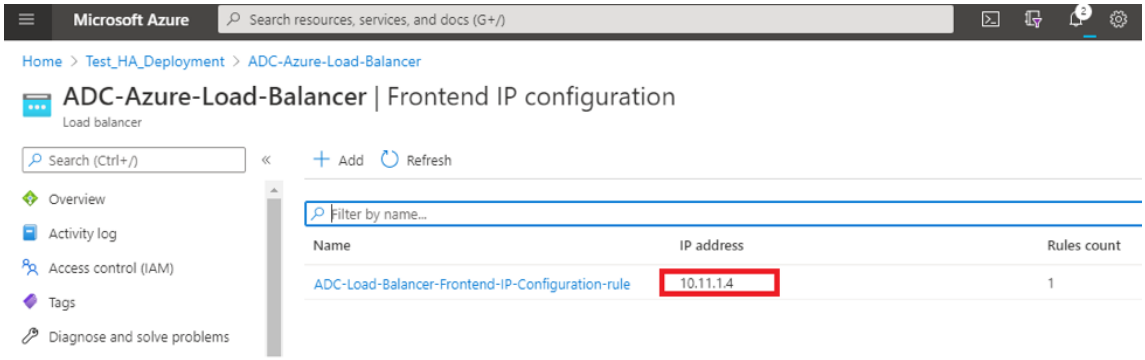
```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled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

在辅助节点上 (ADC-VPX-1)

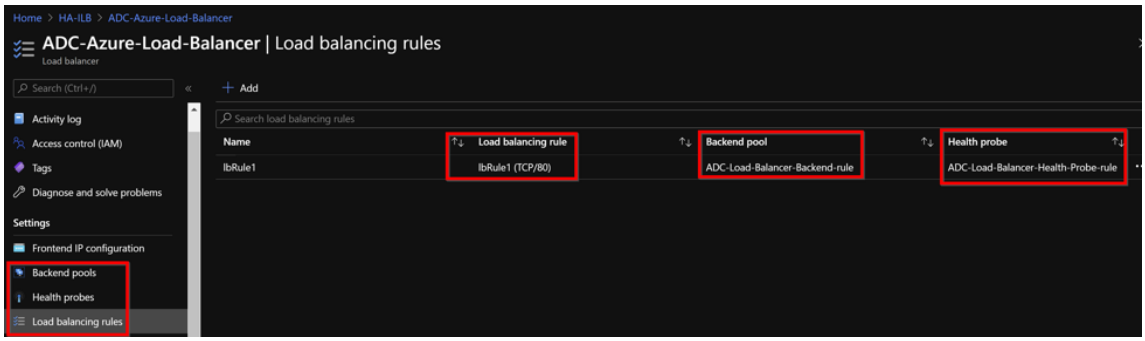

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.11.0.4        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.6        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

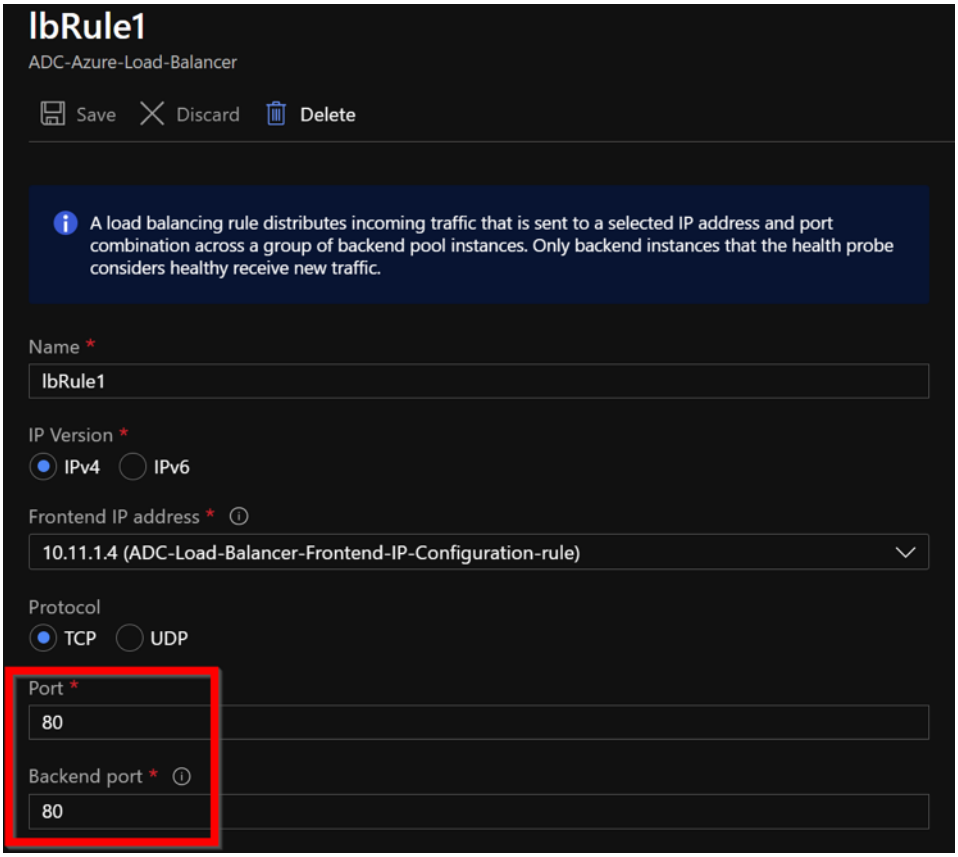
5. 在主节点和辅助节点启动且同步状态为 成功后，必须使用 ADC Azure 负载平衡器的专用浮动 IP (FIP) 地址在主节点 (ADC-VPX-0) 上配置负载平衡虚拟服务器或网关虚拟服务器。有关更多信息，请参阅示 例配置 部分。
6. 要查找 ADC Azure 负载均衡器的专用 IP 地址，请导航到 **Azure portal**（**Azure** 门户）**> ADC Azure Load Balancer**（**ADC Azure** 负载均衡器）**> Frontend IP configuration**（前端 **IP** 配置）。



7. 在 **Azure Load Balancer**（Azure 负载均衡器）配置页面中，ARM 模板部署可帮助创建 LB 规则、后端池和运行状况探测。

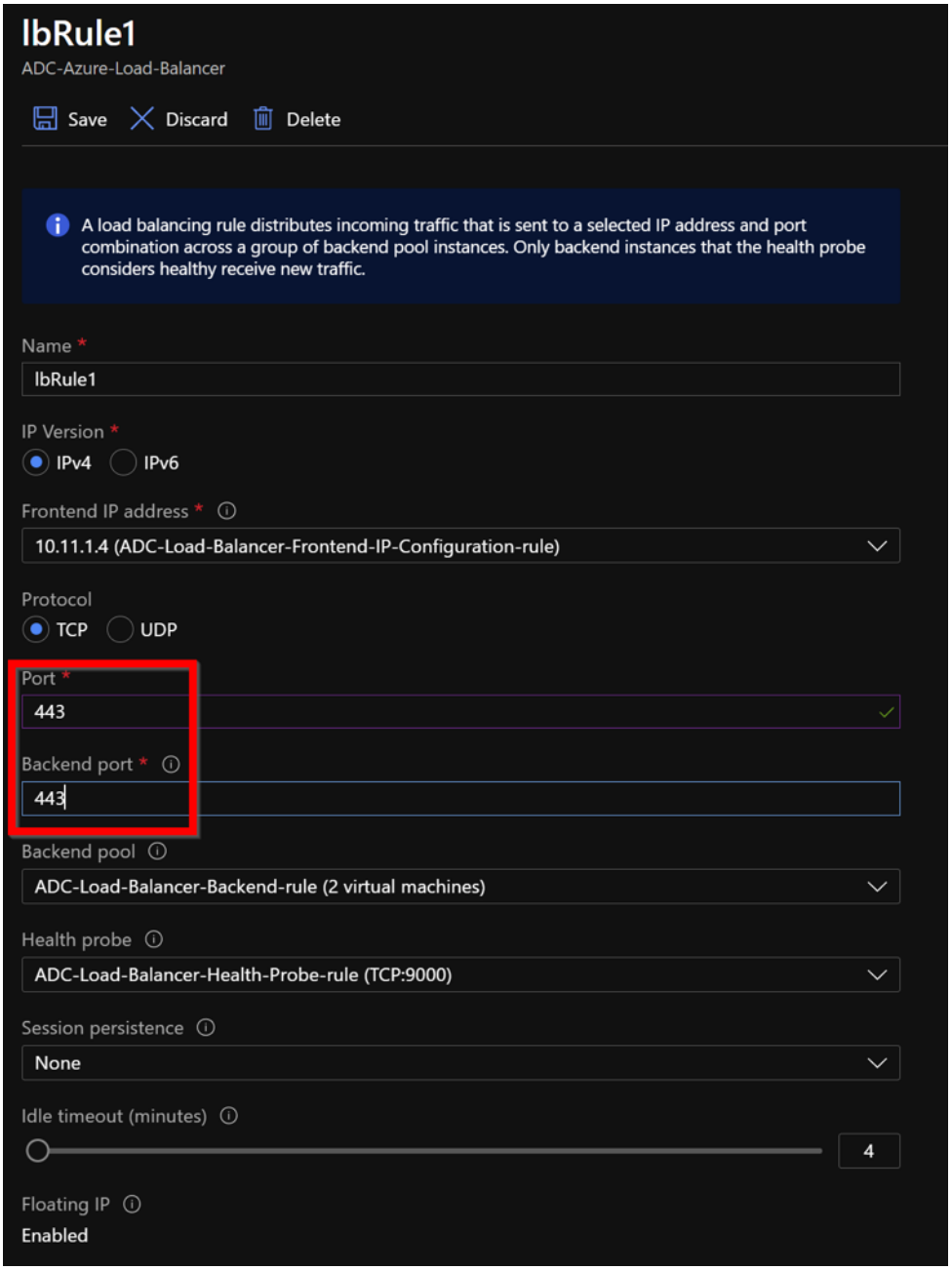


   - 默认情况下，LB 规则 (LbRule1) 使用端口 80。



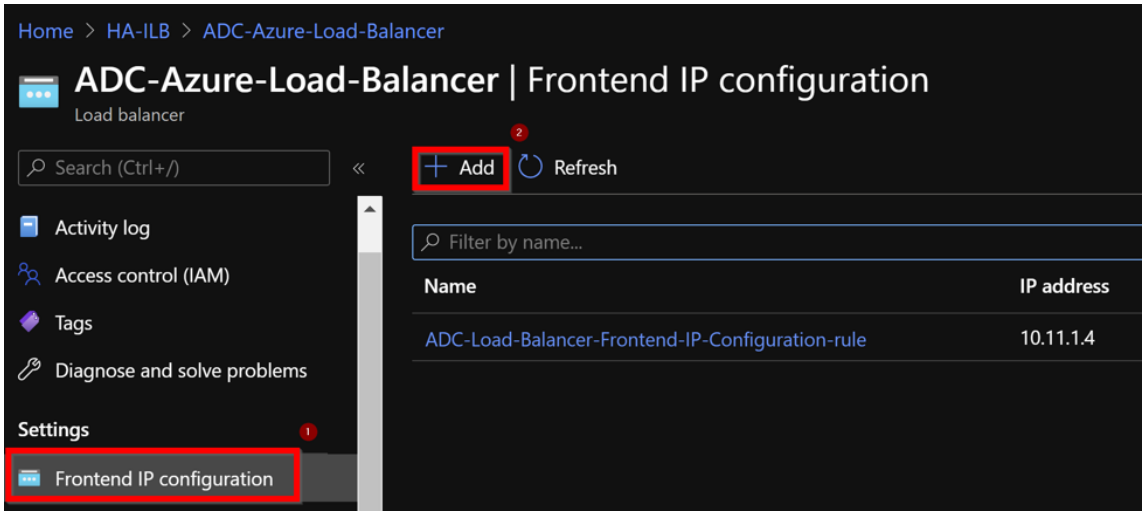
- 编辑规则以使用端口 443，然后保存更改。

  > 注意：
  >
  > 为了增强安全性，Citrix 建议您对 LB 虚拟服务器或网关虚拟服务器使用 SSL 端口 443。

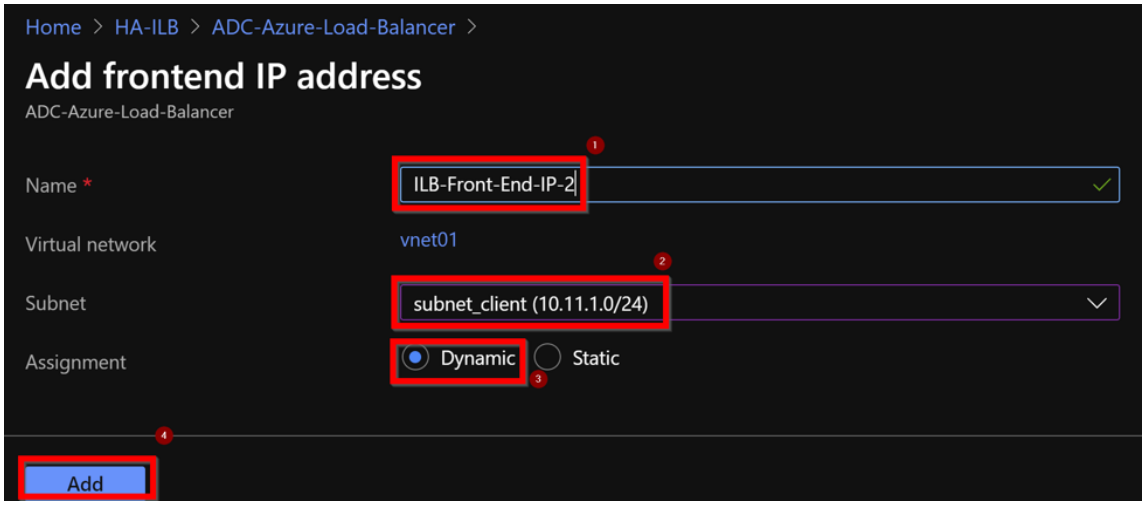


要在 ADC 上添加更多 VIP 地址，请执行以下步骤：

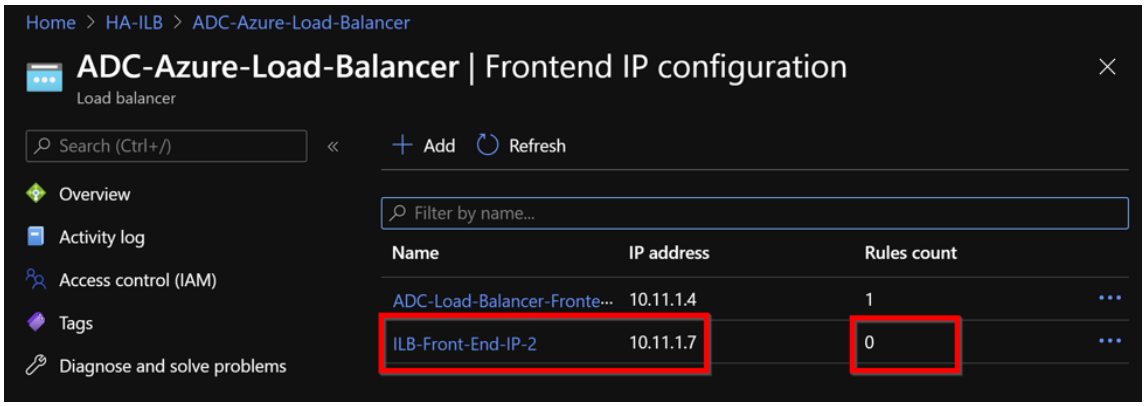
1. 导航到 **Azure Load Balancer**（**Azure** 负载均衡器）**> Frontend IP configuration**（前端 **IP** 配置），然后单击 **Add**（添加）以创建新的内部负载均衡器 IP 地址。



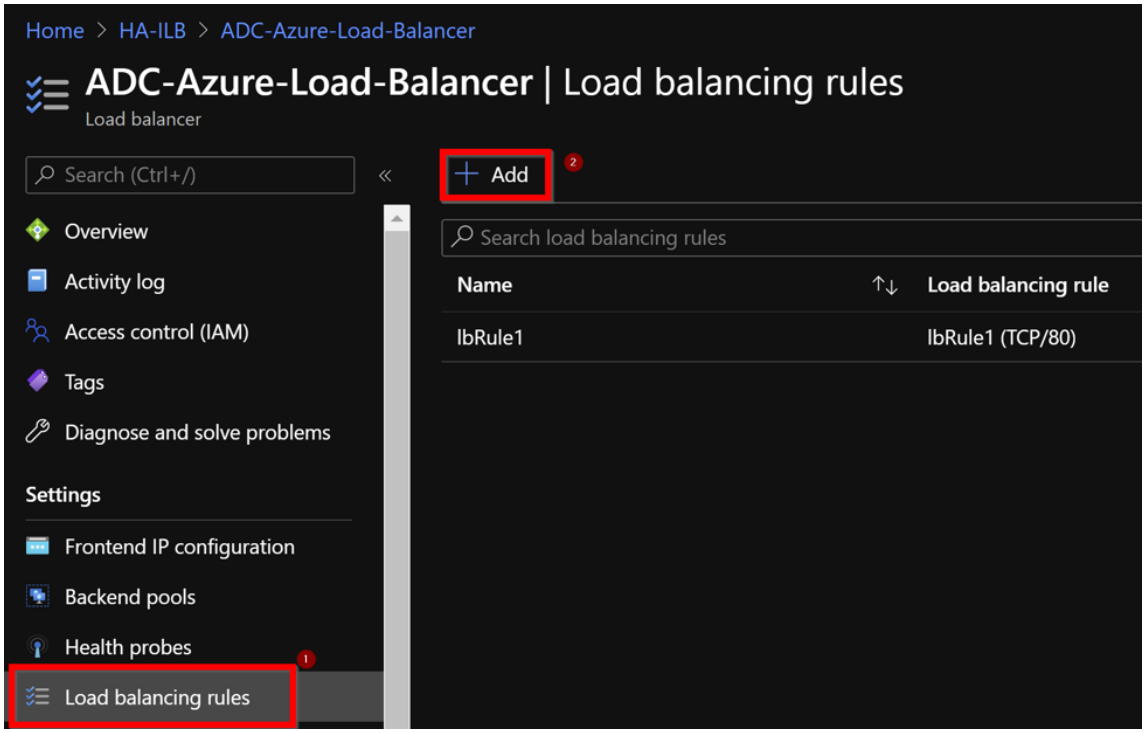
2. 在 **Add frontend IP address**（添加前端 IP 地址）页面中，输入名称，选择客户端子网，分配动态或静态 IP 地址，然后单击 **Add**（添加）。



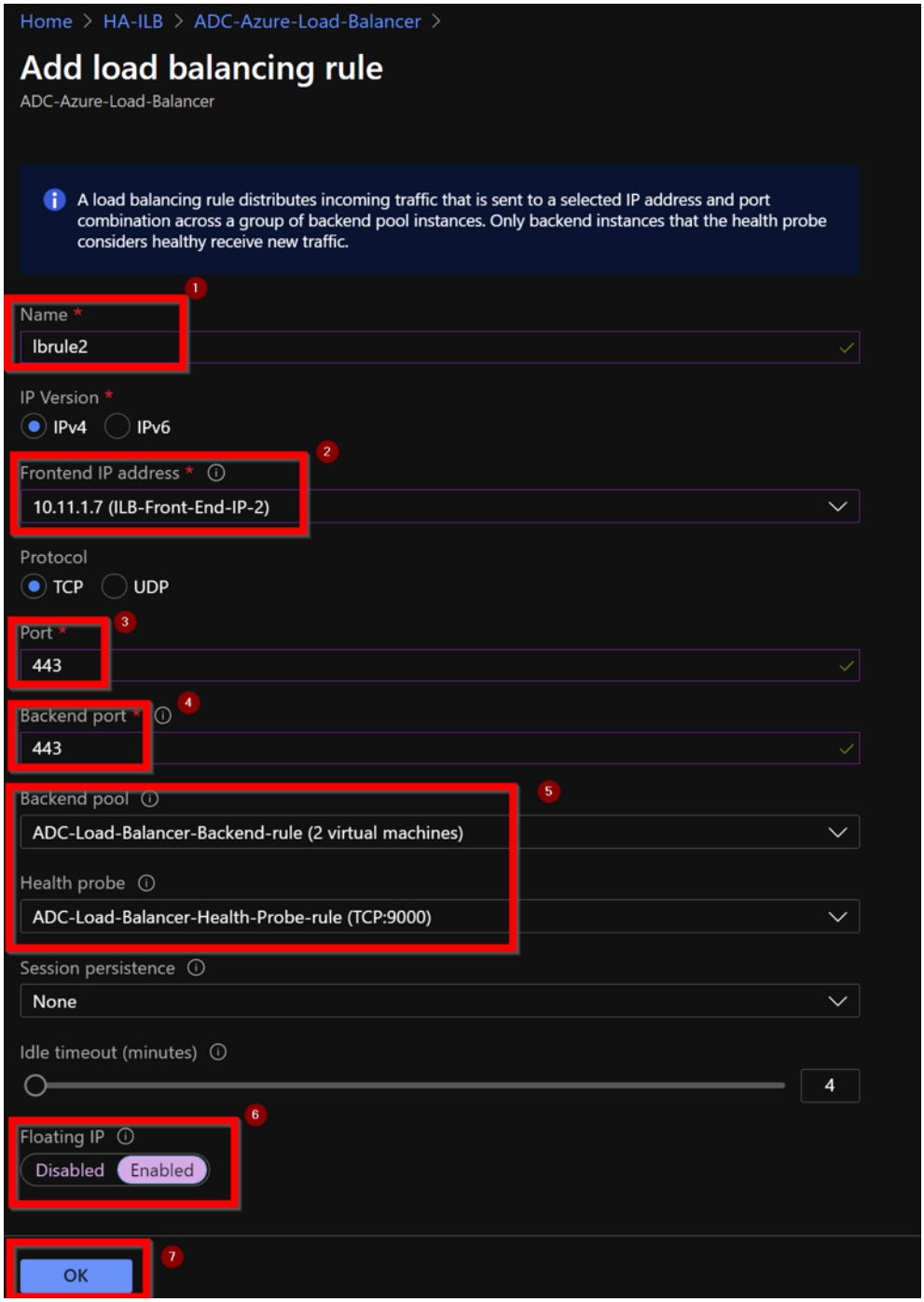
3. 创建了前端 IP 地址，但没有关联 LB 规则。创建新的负载平衡规则，并将其与前端 IP 地址关联。



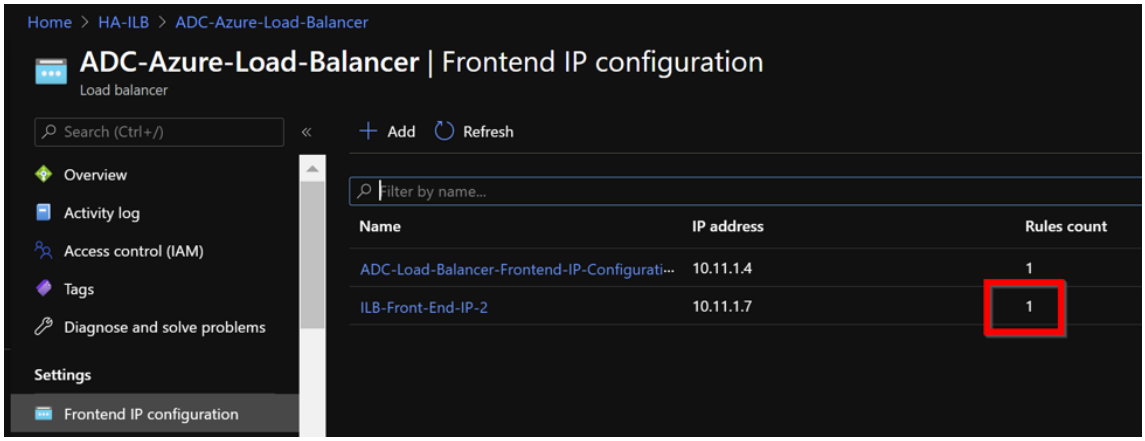
4. 在 **Azure Load Balancer**（Azure 负载均衡器）页面中，选择 **Load balancing rules**（负载平衡规则），然后单击 **Add**（添加）。



5. 通过选择新的前端 IP 地址和端口来创建新的 LB 规则。**Floating IP**（浮动 IP）字段必须设置为 **Enabled**（已启用）。



6. 现在，**Frontend IP configuration**（前端 IP 配置）显示了应用的 LB 规则。



示例配置

要配置网关 VPN 虚拟服务器和负载平衡虚拟服务器，请在主节点 (ADC-VPX-0) 上运行以下命令。配置自动同步到辅助节点 (ADC-VPX-1)。

网关示例配置

```
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
```

负载平衡示例配置

```
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
```

现在，您可以使用与 ILB 的内部 IP 地址关联的完全限定域名 (FQDN) 访问负载平衡或 VPN 虚拟服务器。

有关如何配置负载平衡虚拟服务器的详细信息，请参阅资源部分。

资源：

以下链接提供了与 HA 部署和虚拟服务器配置相关的其他信息：

- 在不同的子网中配置高可用性节点
- 设置基本负载平衡

相关资源：

- 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置
- 在 Azure 上的主动-备用高可用性部署中配置 GSLB

使用 **NetScaler** 高可用性模板为面向 **Internet** 的应用程序配置 **HA-INC** 节点

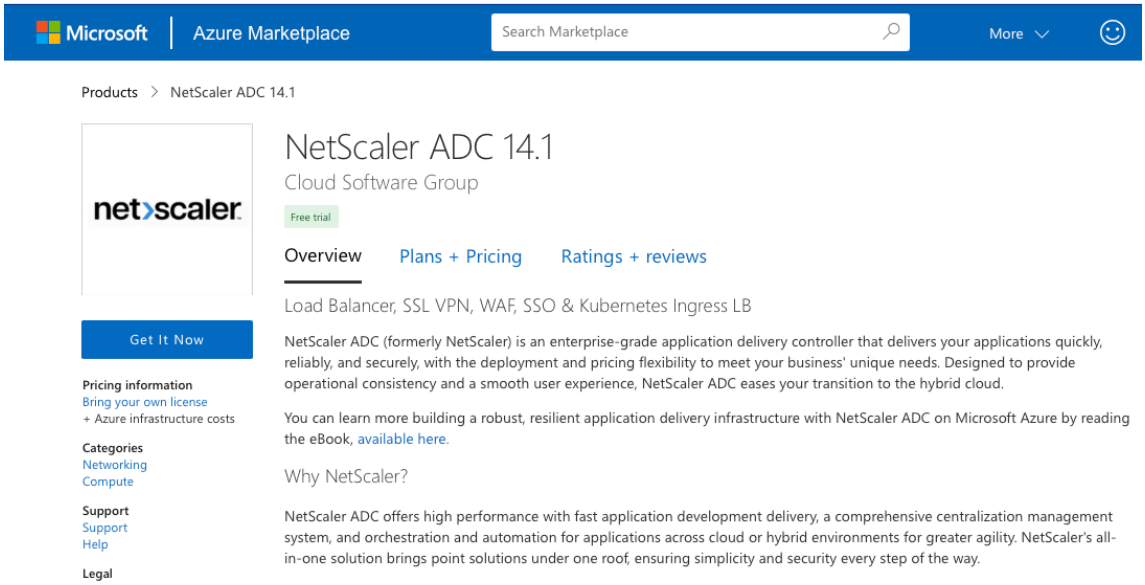
October 17, 2024

可以通过对面向 Internet 的应用程序使用标准模板快速高效地部署处于 HA-INC 模式的一对 VPX 实例。Azure 负载均衡器 (ALB) 使用公用 IP 地址作为前端。模板会创建两个节点，使用三个子网和六个 NIC。这些子网用于管理、客户端和服务器端流量。每个子网中的两个 VPX 实例都有两个 NIC。

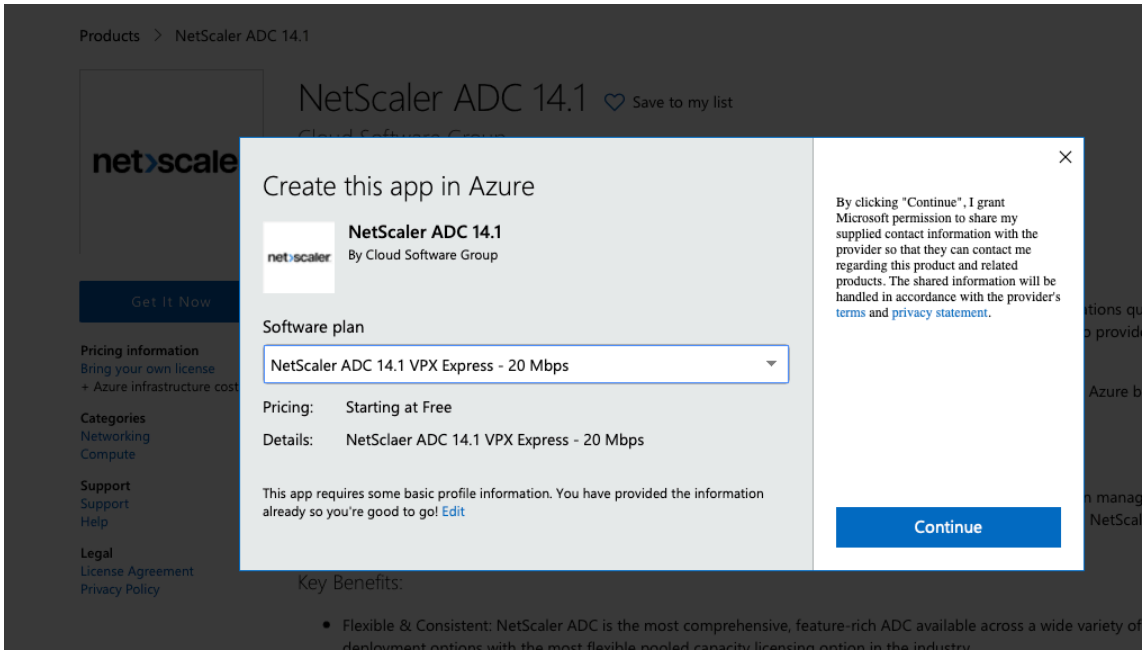
您可以在 Azure Marketplace 上获取面向互联网的应用程序的 NetScaler HA 配对模板。

完成以下步骤，以通过使用 Azure 可用性集或可用性区域启动模板并部署高可用性 VPX 对。

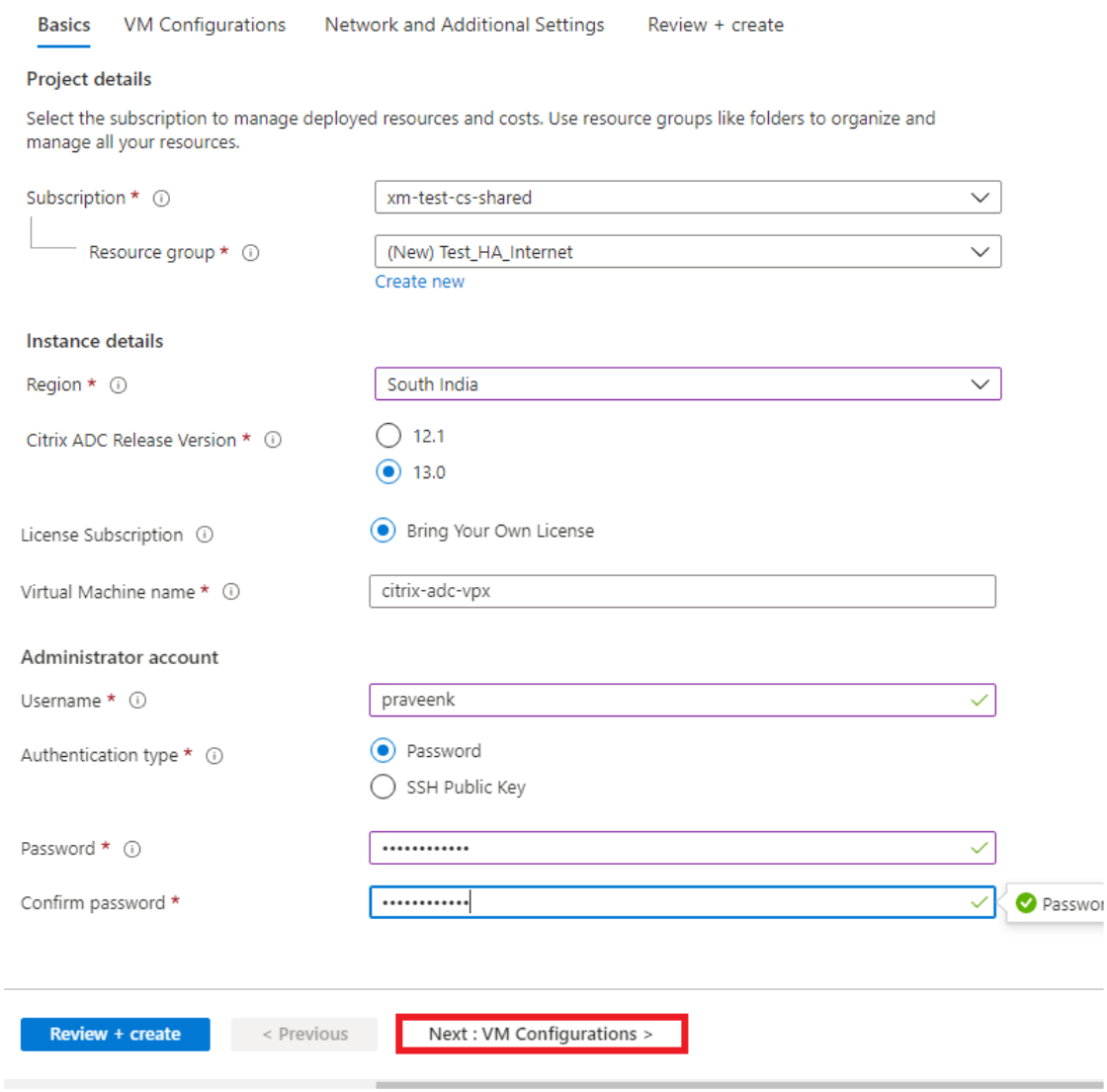
1. 在 Azure 市场中搜索 **NetScaler**。
2. 单击 **GET IT NOW**（立即获取）。



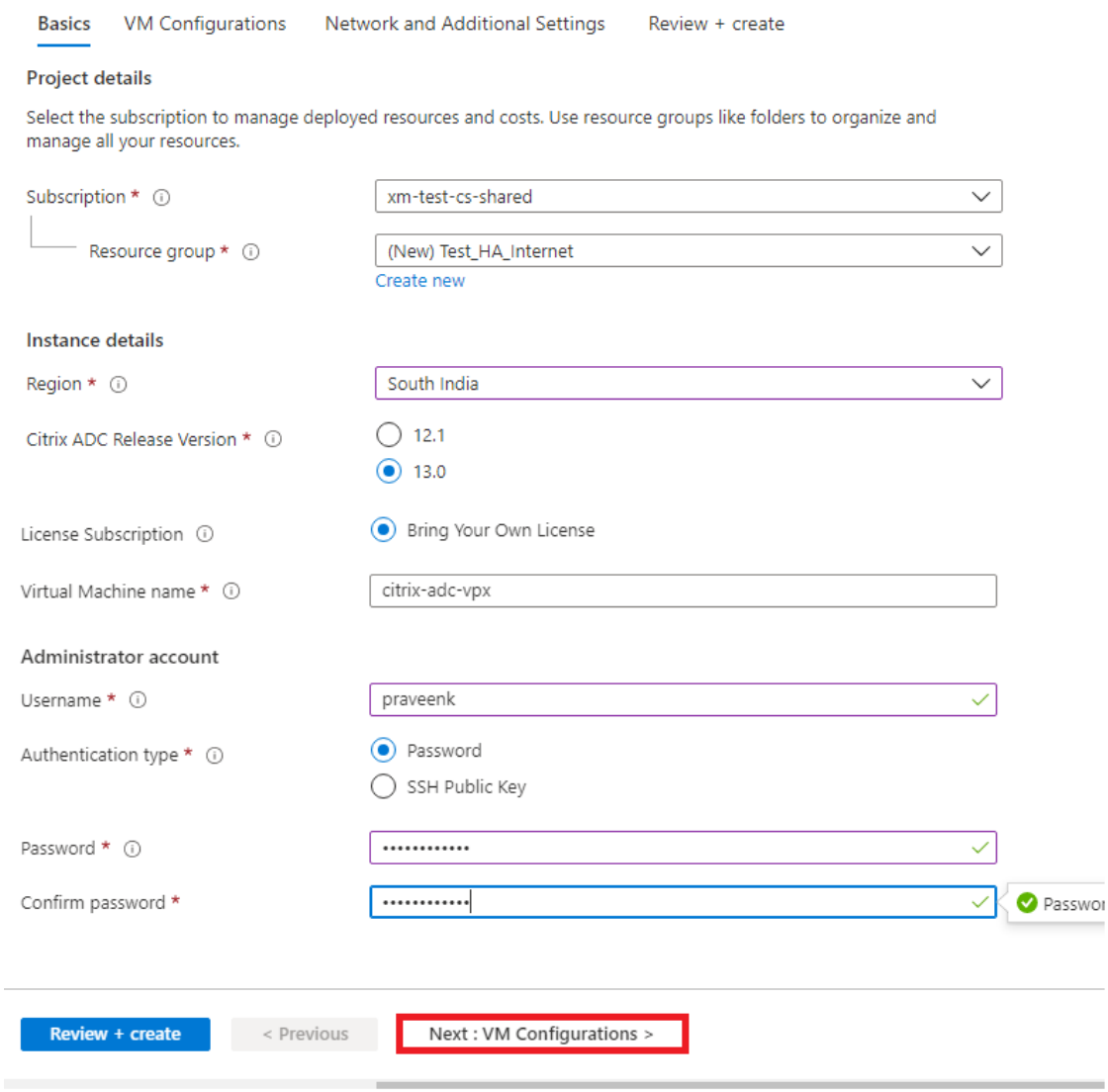
3. 选择所需的高可用性部署以及许可证，然后单击 **Continue**（继续）。



4. 此时将显示 **Basics**（基本）页面。创建资源组。在 **Parameters**（参数）选项卡下，输入“Region”（区域）、“Admin user name”（管理员用户名）、“Admin Password”（管理员密码）、“license type (VM SKU)”（许可证类型 (VM SKU)）以及其他字段的详细信息。



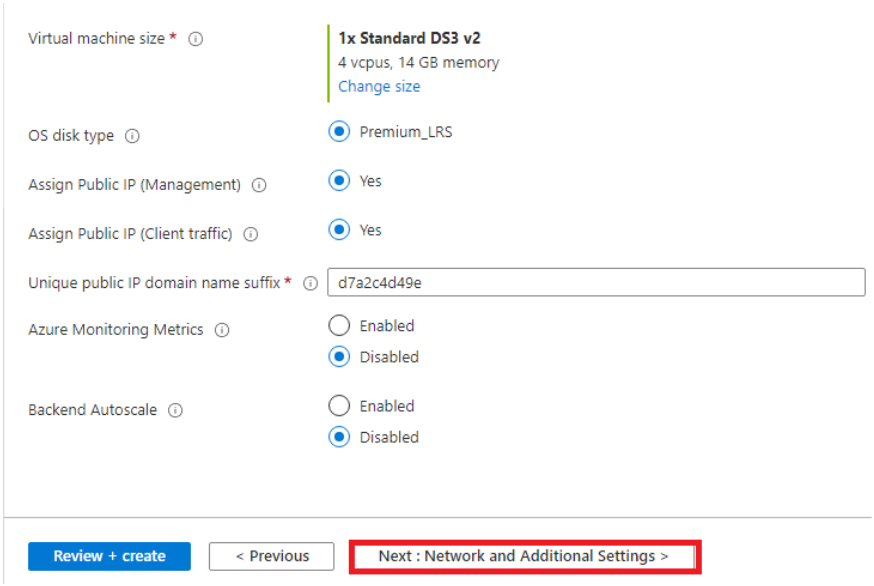
5. 单击 **Next : VM Configurations >**（下一步: VM 配置 >）。



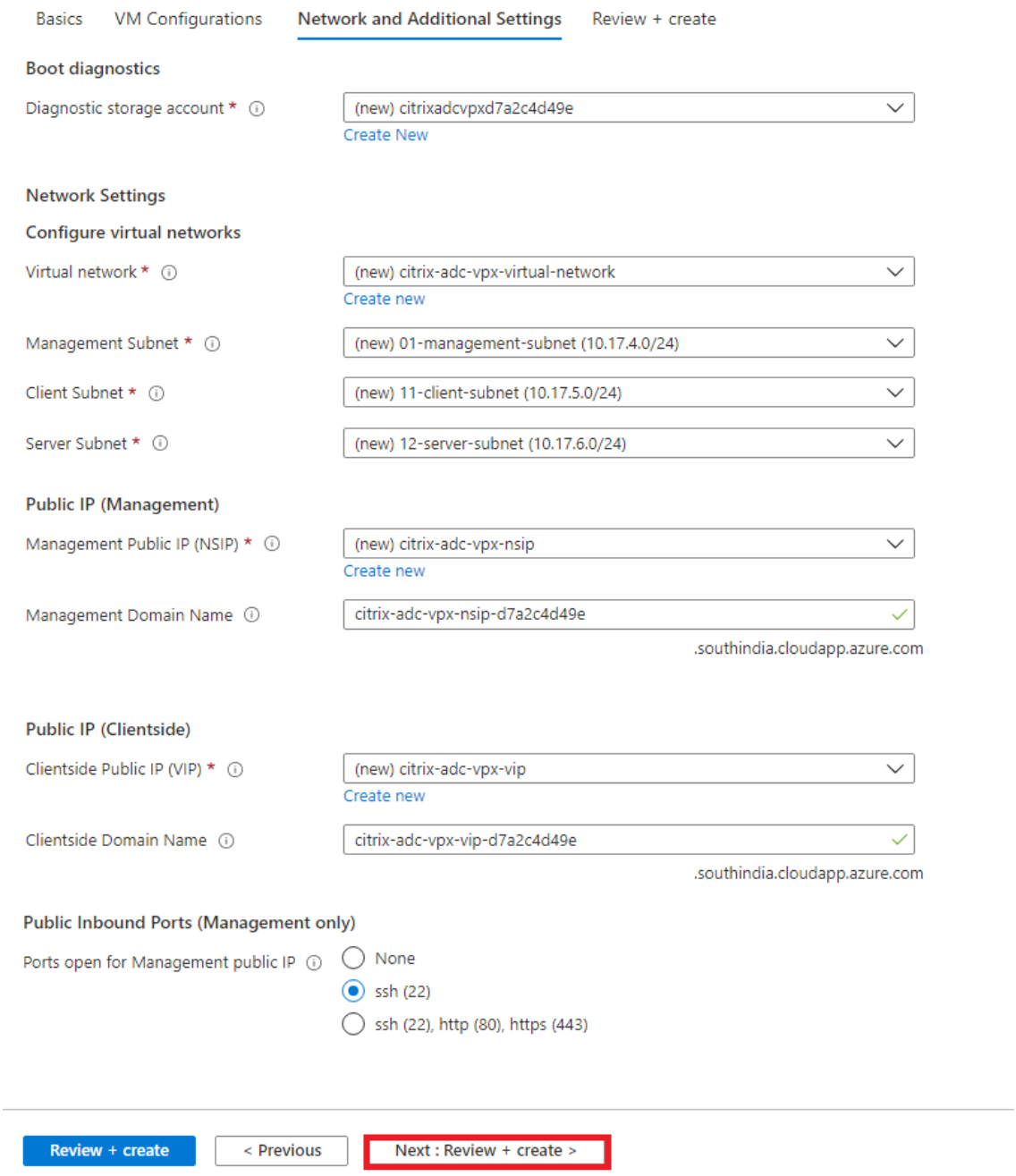
6. 在 **VM Configurations**（VM 配置）页面上，执行以下操作：

   - 配置公用 IP 域名后缀
   - 启用或禁用 **Azure Monitoring Metrics**（Azure 监视指标）
   - 启用或禁用 **Backend AutoScale**（后端 AutoScale）

7. 单击 **Next: Network and Additional settings >**（下一步: 网络和其他设置 >）



8. 在 **Network and Additional Settings**（网络和其他设置）页面上，创建启动诊断帐户并配置网络设置。

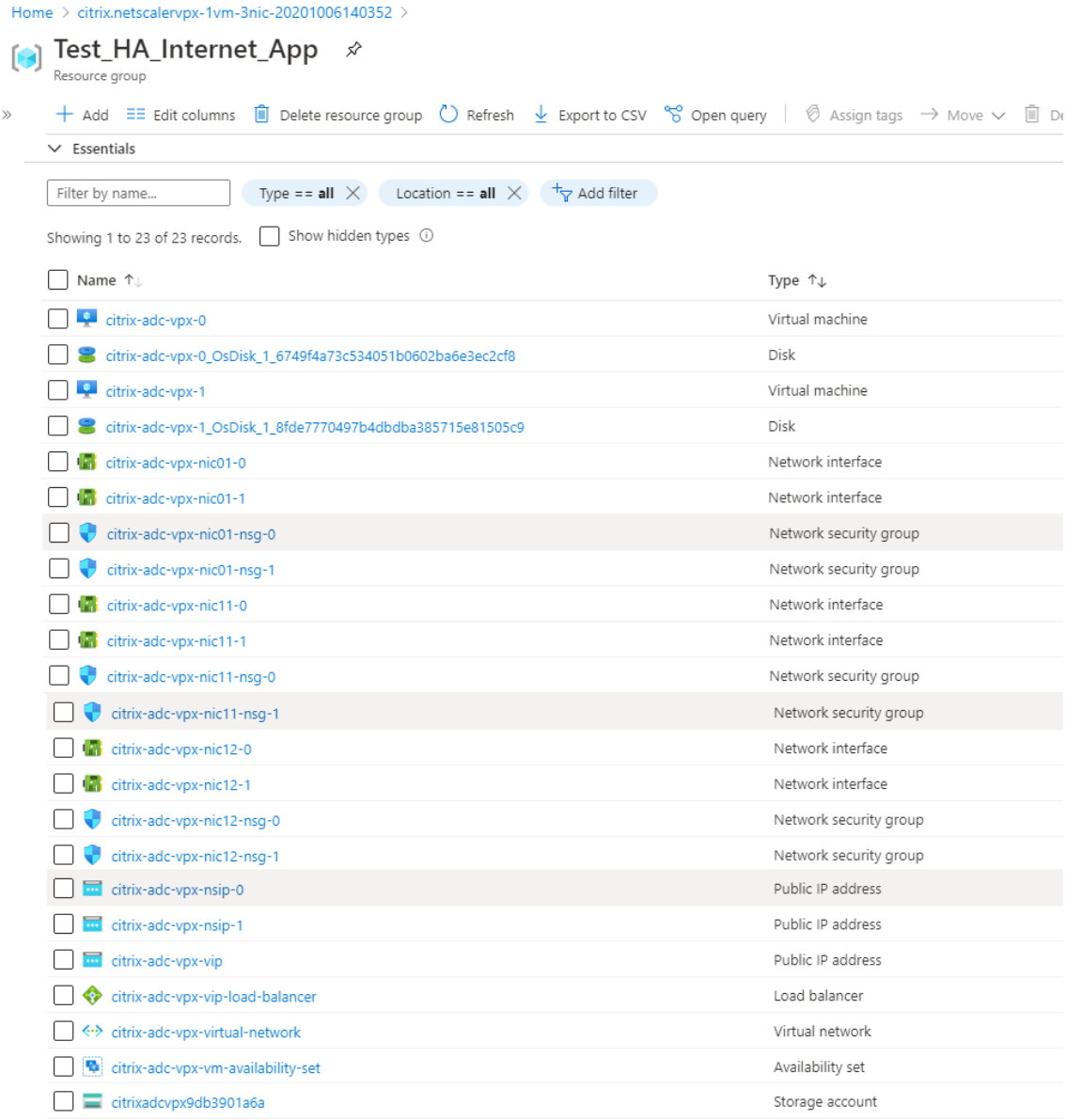


9. 单击 **Next: Review + create >**（下一步: 检查 + 创建 >）。
10. 查看基本设置、VM 配置、网络和其他设置，然后单击 **Create**（创建）。

    可能需要一段时间采用所需配置来创建 Azure 资源组。完成后，在 Azure 门户中选择资源组以查看配置详细信息，例如 LB 规则、后端池、运行状况探测。高可用性对显示为 **citrix-adc-vpx-0** 和 **citrix-adc-vpx-1**。

    如果需要对您的高可用性设置进行进一步修改（例如，创建更多安全规则和端口），可以在 Azure 门户中完成。

完成所需配置后，将创建以下资源。



11. 必须登录 **citrix-adc-vpx-0** 和 **citrix-adc-vpx-1** 节点才能验证以下配置：

    - 两个节点的 NSIP 地址必须位于管理子网中。
    - 在主节点 (citrix-adc-vpx-0) 和辅助节点 (citrix-adc-vpx-1) 上，您必须看到两个 SNIP 地址。一个 SNIP（客户端子网）用于响应 ALB 探测，另一个 SNIP（服务器子网）用于后端服务器通信。

    > 注意：
    >
    > 在 HA-INC 模式下，citrix-adc-vpx-0 和 citrix-adc-vpx-1 VM 的 SNIP 地址不同，这一点与传统的本地 ADC 高可用性部署不同，后者两者都相同。

    在主节点上 (citrix-adc-vpx-0)


```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  -----
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

在辅助节点上 (citrix-adc-vpx-1)

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  -----
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

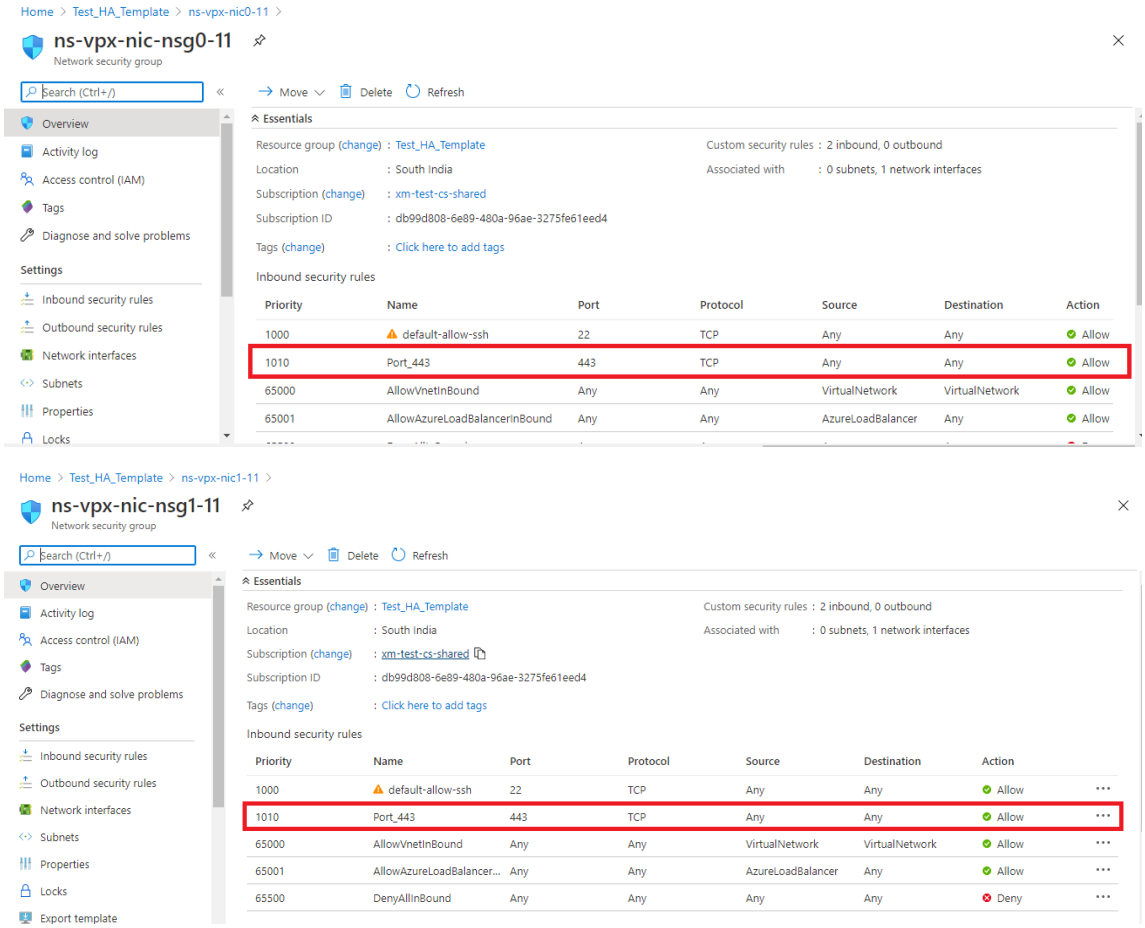


```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

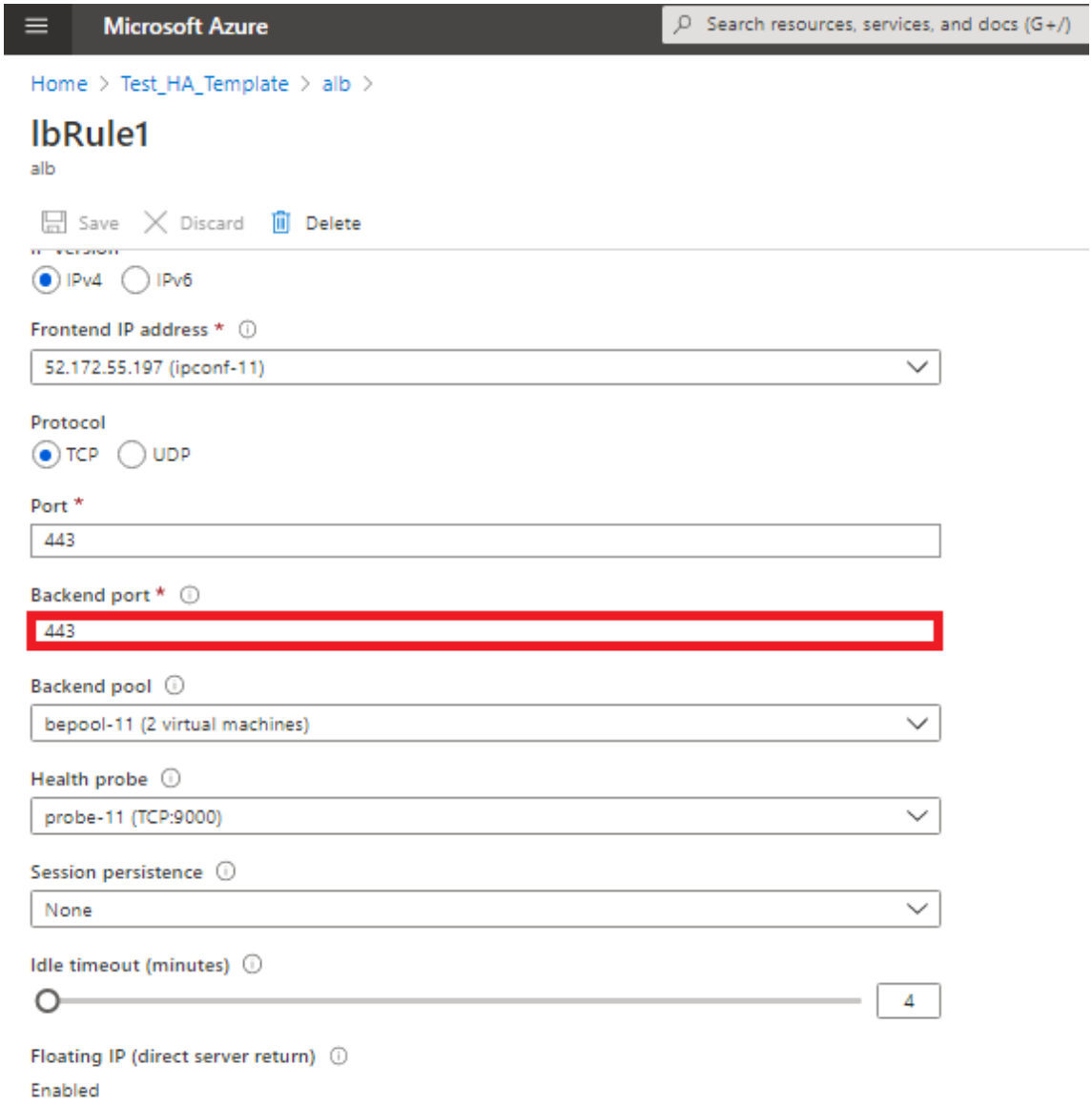
12. 在主节点和辅助节点处于启动状态且同步状态为 **SUCCESS**（成功）后，您必须使用 ALB 虚拟服务器的公用 IP 地址配置主节点 (citrix-adc-vpx-0) 上的负载平衡虚拟服务器或网关虚拟服务器。有关更多信息，请参阅示 例配置 部分。

13. 要查找 ALB 虚拟服务器的公用 IP 地址，请导航到 **Azure portal**（**Azure** 门户）**> Azure Load Balancer**（**Azure** 负载均衡器）**> Frontend IP configuration**（前端 **IP** 配置）。

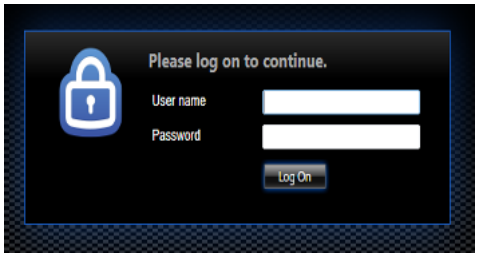
14. 在两个客户端接口的网络安全组中添加虚拟服务器端口 443 的入站安全规则。



15. 配置要访问的 ALB 端口，并为指定端口创建入站安全规则。后端端口是负载平衡虚拟服务器端口或 VPN 虚拟服务器端口。



16. 现在，您可以使用与 ALB 公有 IP 地址关联的完全限定域名 (FQDN) 访问负载平衡虚拟服务器或 VPN 虚拟服务器。



示例配置

要配置网关 VPN 虚拟服务器和负载平衡虚拟服务器，请在主节点 (ADC-VPX-0) 上运行以下命令。配置自动同步到辅助节点 (ADC-VPX-1)。

网关示例配置

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
```

负载平衡示例配置

```
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
```

现在，您可以使用与 ALB 的公有 IP 地址关联的 FQDN 访问负载平衡或 VPN 虚拟服务器。

有关如何配置负载平衡虚拟服务器的详细信息，请参阅资源部分。

资源：

以下链接提供了与 HA 部署和虚拟服务器配置相关的其他信息：

- 创建虚拟服务器
- 设置基本负载平衡

同时使用 **Azure** 外部和内部负载平衡器配置高可用性设置

October 17, 2024

Azure 上的高可用性对同时支持外部和内部负载均衡器。

有以下两个选项可以使用 Azure 外部和内部负载均衡器配置高可用性对：

- 在 NetScaler 设备上使用两台 LB 虚拟服务器。
- 使用一台 LB 虚拟服务器和一个 IP 集。单个 LB 虚拟服务器为多个 IP 提供流量，这些 IP 由 IPSet 定义。

执行以下步骤，同时使用外部和内部负载均衡器在 Azure 上配置高可用性对：

对于步骤 1 和 2，请使用 Azure 门户。对于步骤 3 和 4，使用 NetScaler VPX GUI 或 CLI。

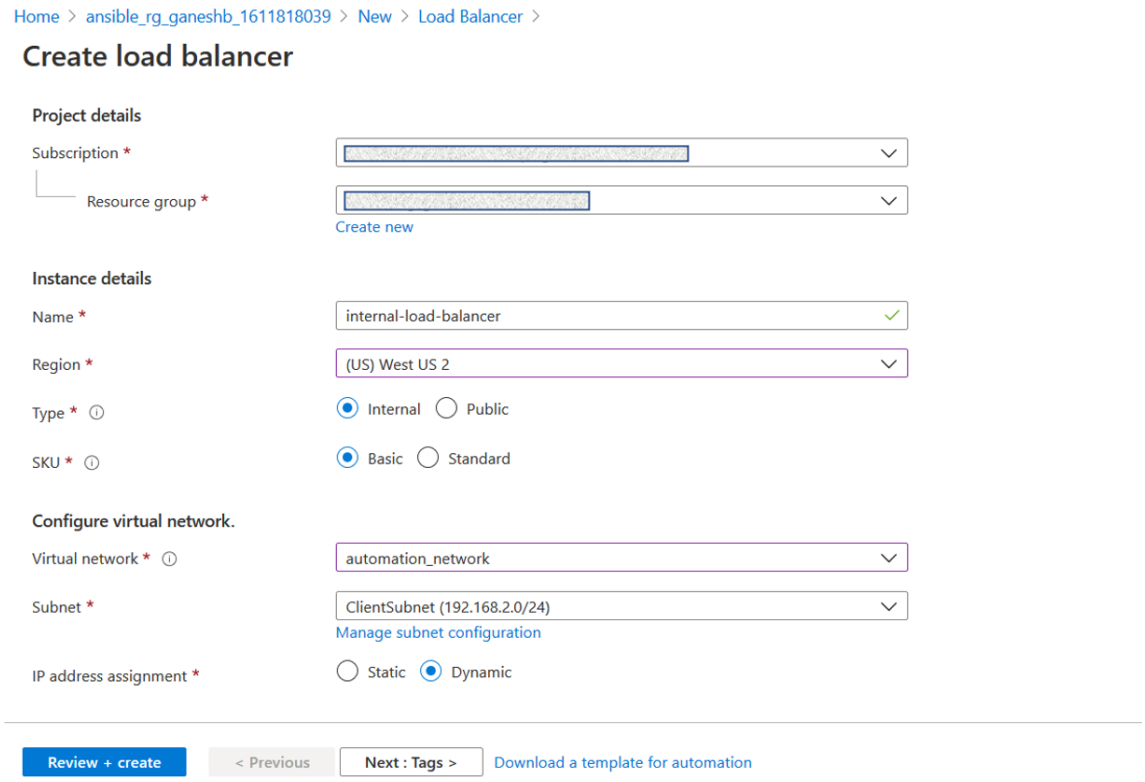
步骤 **1.** 配置 Azure 负载均衡器，可以是外部负载均衡器或内部负载均衡器。

有关使用 Azure 外部负载均衡器配置高可用性设置的详细信息，请参阅 使用多个 IP 地址和 NIC配置高可用性设置。

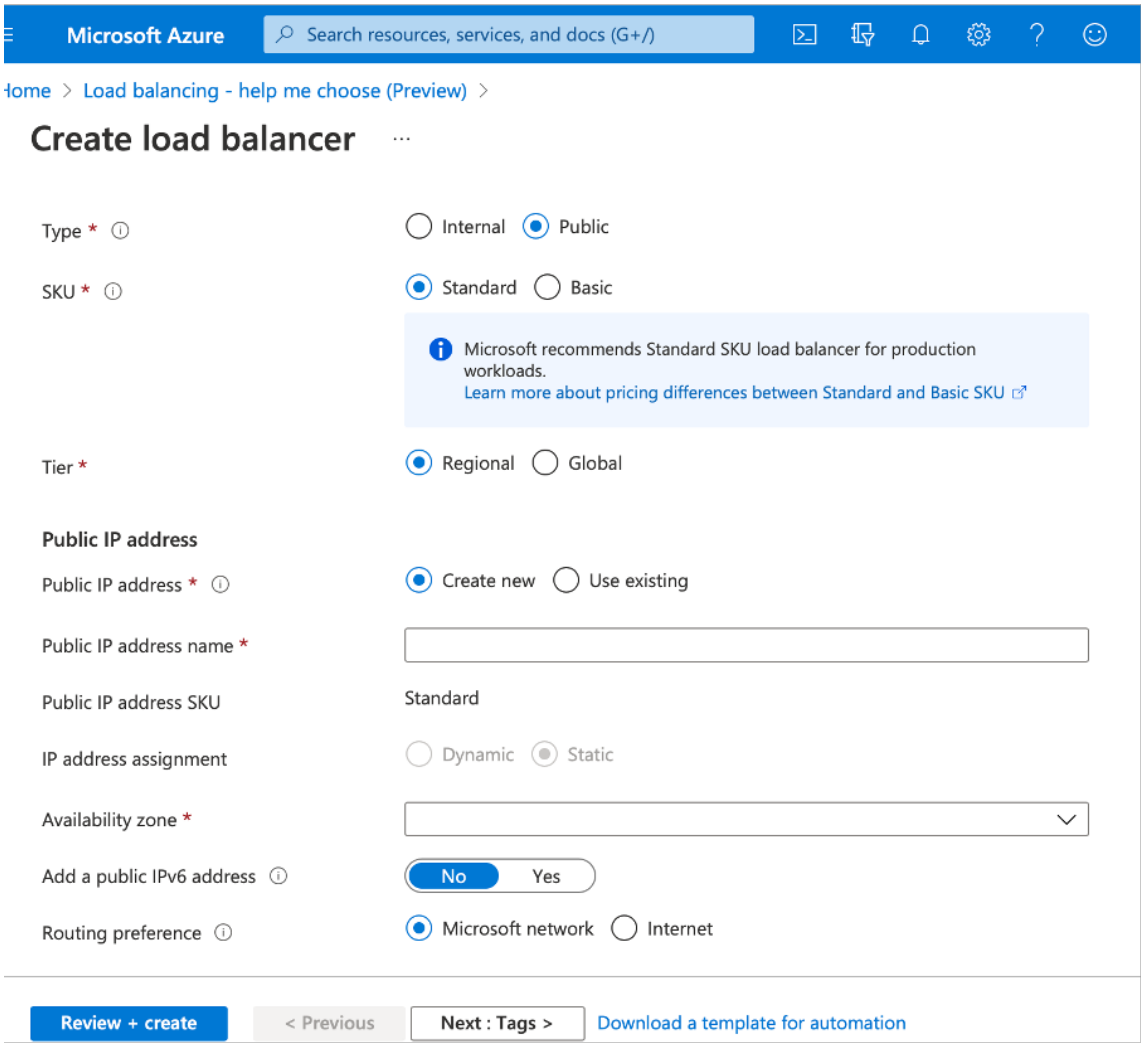
有关使用 Azure 内部负载均衡器配置高可用性设置的详细信息，请参阅 使用 NetScaler 高可用性模板和 Azure ILB配置 HA-INC 节点。

步骤 **2.** 在资源组中创建额外的负载均衡器 (ILB)。在步骤 1 中，如果您创建了外部负载均衡器，则现在创建内部负载均衡器，相反。

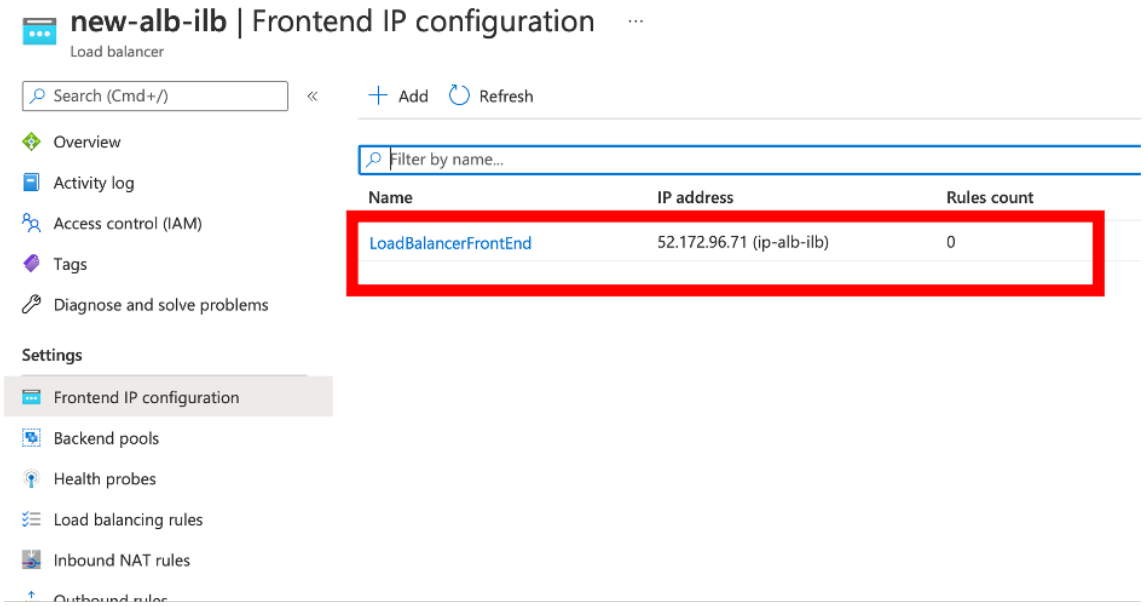
- 要创建内部负载均衡器，请选择负载均衡器类型作为 内部。对于 子网 字段，必须选择 NetScaler 客户端子网。如果没有冲突，您可以选择在该子网中提供静态 IP 地址。否则，请选择动态 IP 地址。



- 要创建外部负载均衡器，请选择负载均衡器类型作为 P **ublic** ，然后在此处创建公有 IP 地址。



1. 创建 Azure 负载均衡器后，导航到 前端 **IP** 配置 并记下此处显示的 IP 地址。如步骤 3 所示，在创建 ADC 负载平衡虚拟服务器时必须使用此 IP 地址。



2. 在 **Azure** 负载均衡器配置 页面中，ARM 模板部署有助于创建 LB 规则、后端池和运行状况探测器。
3. 将高可用性对客户端 NIC 添加到 ILB 的后端池中。
4. 创建运行状况探测器（TCP，9000 端口）
5. 创建两个负载平衡规则：
   - 端口 80 上的 HTTP 流量（web 应用程序使用案例）的一个 LB 规则。该规则还必须使用后端端口 80。选择创建的后端池和运行状况探测器。必须启用浮动 IP。
   - 另一个用于端口 443 上 HTTPS 或 CVAD 流量的 LB 规则。该过程与 HTTP 流量相同。

步骤 **3.** 在 NetScaler 设备的主节点上，为 ILB 创建负载平衡虚拟服务器。

1. 添加负载平衡虚拟服务器。

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

Example:

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```

> 注意：
>
> 使用负载均衡器前端 IP 地址，该地址与您在步骤 2 中创建的额外负载均衡器关联。

2. 将服务绑定到负载平衡虚拟服务器。

```
bind lb vserver <name> <serviceName>
```

Example:


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

有关详细信息，请参阅 设置基本负载均衡

步骤 **4**：作为步骤 3 的替代方法，您可以使用 IPSet 为 ILB 创建负载平衡虚拟服务器。

1. 添加虚拟服务器 IP (VIP) 类型的 IP 地址。

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

   Example:

   ```
   add nsip 52.172.96.71 -type vip
   ```

2. 在主节点和辅助节点上添加 IPSet。

   ```
   add ipset <name>
   ```

   Example:

   ```
   add ipset ipset1
   ```

3. 将 IP 地址绑定到 IP 集。

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

   Example:

   ```
   bind ipset ipset1 52.172.96.71
   ```

4. 将现有的 LB 虚拟服务器设置为使用 IPSet。

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

   Example:

   ```
   set lb vserver vserver_name -ipset ipset1
   ```

有关详细信息，请参阅 配置多 IP 虚拟服务器。

在 **Azure VMware** 解决方案上安装 **NetScaler VPX** 实例

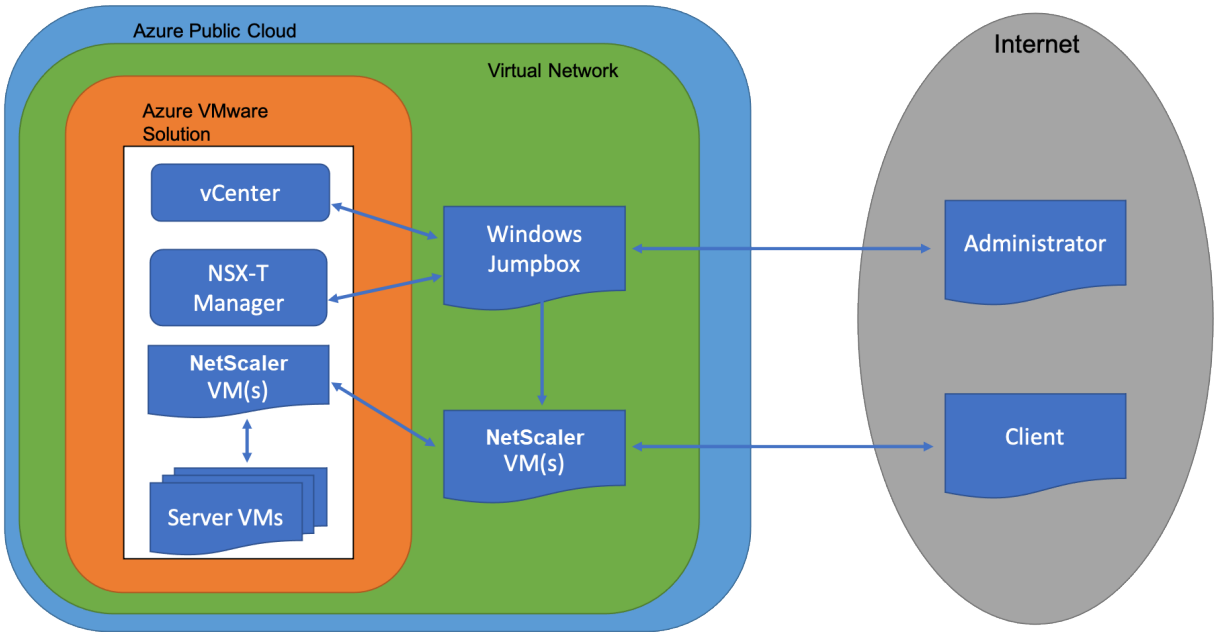
October 17, 2024

Azure VMware 解决方案 (AVS) 为您提供包含 vSphere 群集的私有云，这些群集是由专用裸机 Azure 基础架构构建的。最少初始部署为三台主机，但是每个群集最多可以添加一台主机，最多可以添加 16 台主机。所有预配的私有云都有 vCenter Server、vSAN、vSphere 和 NSX-T。

Azure 上的 VMware 云 (VMC) 使您能够在 Azure 上使用所需的 ESX 主机数量创建云软件定义的数据中心 (SDDC)。Azure 上的 VMC 支持 NetScaler VPX 部署。VMC 提供的用户界面与本地 vCenter 相同。它的功能类似于基于 ESX 的 NetScaler VPX 部署。

下图显示了 Azure 公有云上的 Azure VMware 解决方案，管理员或客户端可以通过 Internet 访问该解决方案。管理员可以使用 Azure VMware 解决方案创建、管理和配置工作负载或服务器虚拟机。管理员可以从 Windows Jumpbox 访问 AVS 的基于 Web 的 vCenter 和 NSX-T 管理器。您可以使用 vCenter 在 Azure VMware 解决方案中创建 NetScaler VPX 实例（独立或高可用性对）和服务器虚拟机，并使用 NSX-T 管理器管理相应的网络。AVS 上的 NetScaler VPX 实例的工作方式与本地 VMware 主机群集类似。AVS 由在同一虚拟网络中创建的 Windows Jumpbox 进行管理。

客户只能通过连接到 ADC 的 VIP 来访问 AVS 服务。Azure VMware 解决方案之外的另一个 NetScaler VPX 实例位于同一 Azure 虚拟网络中，这有助于将 NetScaler VPX 实例的 VIP 作为服务添加到 Azure VMware 解决方案中。根据要求，您可以配置 NetScaler VPX 实例以通过 Internet 提供服务。



必备条件

在开始安装虚拟设备之前，请执行以下操作：

- 有关 Azure VMware 解决方案及其先决条件的更多信息，请参阅 Azure VMware 解决方案文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware 解决方案私有云。
- 有关创建 Windows Jump Box 虚拟机以访问和管理 Azure VMware 解决方案的详细信息，请参阅 访问 Azure VMware 解决方案私有云
- 在 Windows 跳转框虚拟机中，下载 NetScaler VPX 设备安装文件。
- 在虚拟机连接到的 VMware SDDC 上创建适当的 NSX-T 网段。有关详细信息，请参阅在 Azure VMware 解决方案中添加网段

- 获取 VPX 许可证文件。
- 创建或迁移到 Azure VMware 解决方案私有云的虚拟机 (VM) 必须连接到网络分段。

VMware 云硬件要求

下表列出了 VMware SDDC 必须为每个 VPX nCore 虚拟设备提供的虚拟计算资源。

表 1. VPX 功能列表 表 2. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

组件	要求
内存	2 GB
虚拟 CPU (vCPU)	2
虚拟网络接口	在 VMware SDDC 中，如果 VPX 硬件升级到版本 7 或更高版本，则最多可以安装 10 个虚拟网络接口。
磁盘空间	20 GB

> 注意：
>
> 这是对虚拟机管理程序的磁盘要求的补充。

要在生产中使用 VPX 虚拟设备，必须保留完整的内存分配。

OVF Tool 1.0 系统要求

OVF 工具是可在 Windows 和 Linux 操作系统上运行的客户端应用程序。下表描述了安装 OVF 工具的系统要求。

表 2. VPX 功能列表 表 2. OVF 工具安装的系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。
CPU	最低 750 MHz，建议使用 1 GHz 或速度更快的 CPU
RAM	最低 1 GB；建议使用 2 GB
NIC	100 Mbps 或速度更高的 NIC

有关安装 OVF 的信息，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。

下载 **NetScaler VPX** 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例设置包遵循开放虚拟机 (OVF) 格式标准。可以从 Citrix Web 站点下载文件。需要使用 Citrix 帐户进行登录。如果您没有 Citrix 帐户，请访问 http://www.citrix.com的主页。单击 **New Users link**（新建用户链接），然后按照说明创建新的 Citrix 帐户。

登录后，从 Citrix 主页浏览以下路径：

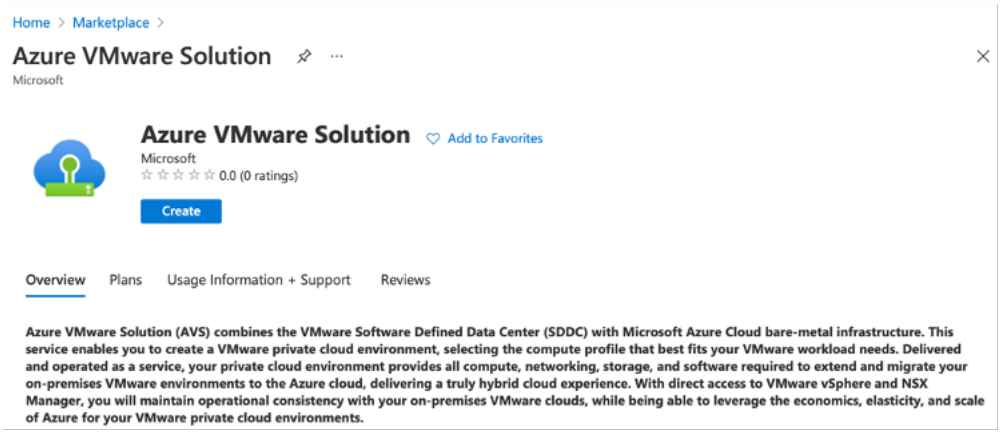
Citrix.com > 下载 **> NetScaler >** 虚拟设备。

将以下文件复制到 ESX 服务器所在网络中的一个工作站。将所有三个文件复制到同一个文件夹中。

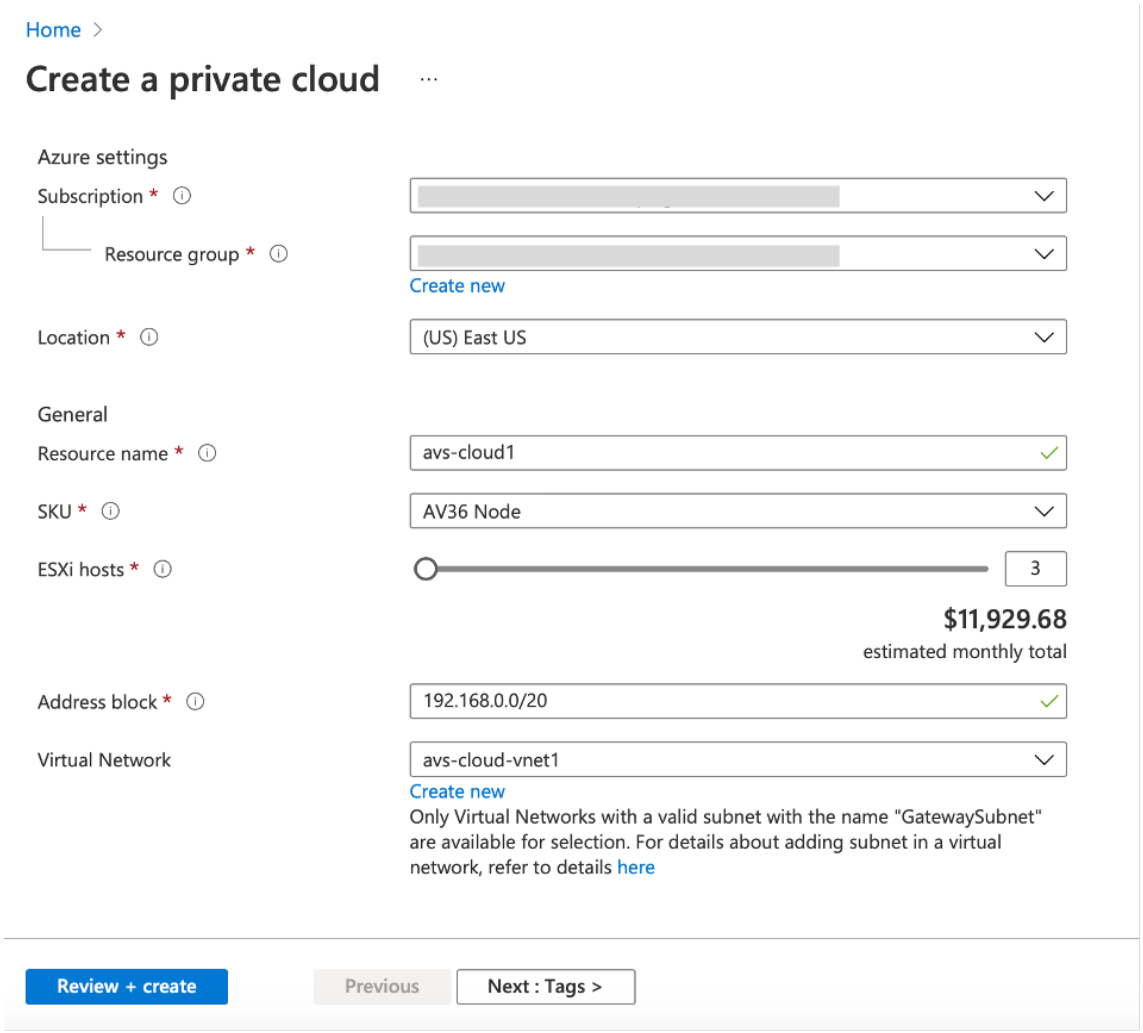
- NSVPX-ESX-<release number>-<build number>-disk1.vmdk（例 如 NSVPX-ESX-13.0-79.64-disk1.vmdk）
- NSVPX-ESX-<release number>-<build number>.ovf （例如 NSVPX-ESX-13.0-79.64.ovf）
- NSVPX-ESX-<release number>-<build number>.mf（例如 NSVPX-ESX-13.0-79.64.mf）

部署 **Azure VMware** 解决方案

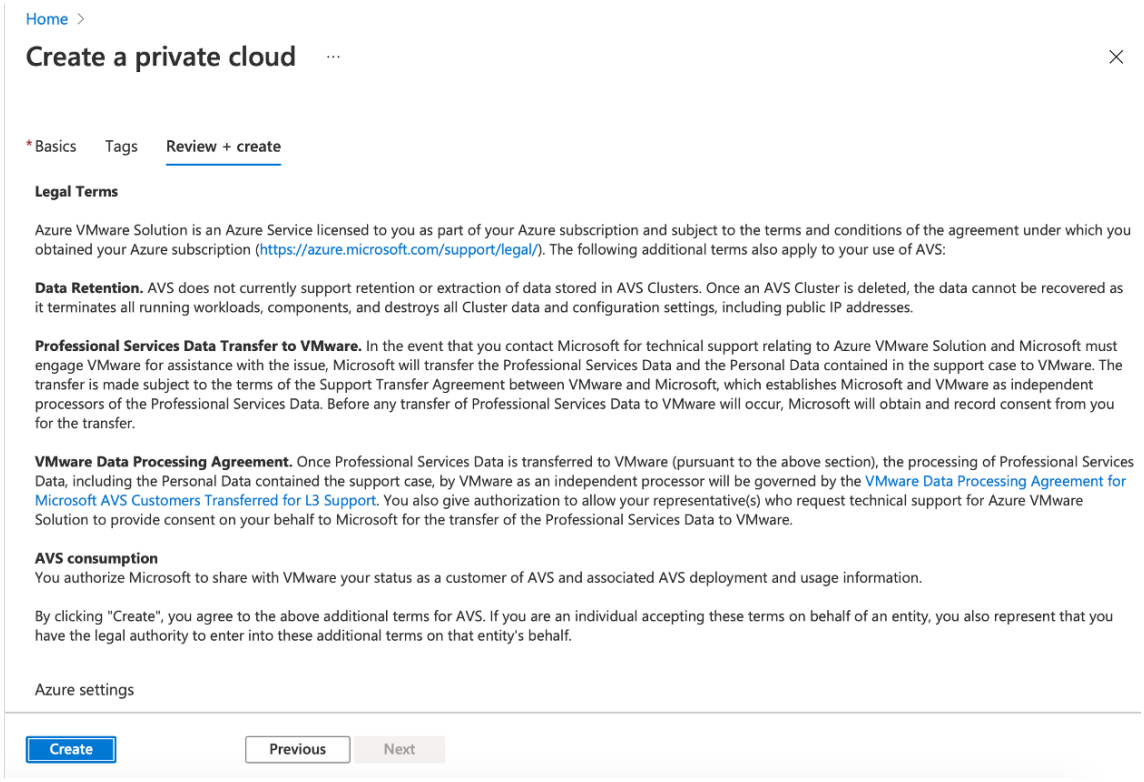
1. 登录到您的 Microsoft Azure 门户，然后导航到 **Azure** 市场。
2. 在 **Azure** 市场中，搜索 **Azure VMware** 解决方案，然后单击 创建。



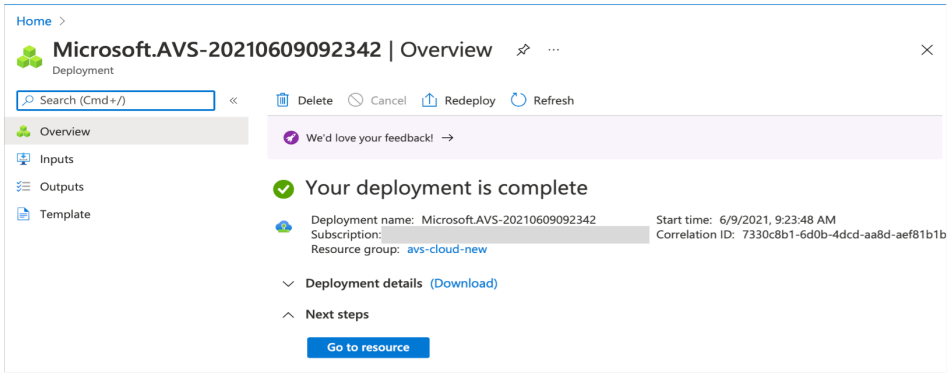
3. 在 创建私有云 页面中，输入以下详细信息：
    - 至少选择 3 个 ESXi 主机以创建私有云的默认群集。
    - 对于地 址块 字段，请使用 **/22** 地址空间。
    - 对于 虚拟网络，请确保 CIDR 范围不与任何本地或其他 Azure 子网（虚拟网络）或网关子网重叠。
    - 网关子网用于表达与私有云的连接路由。



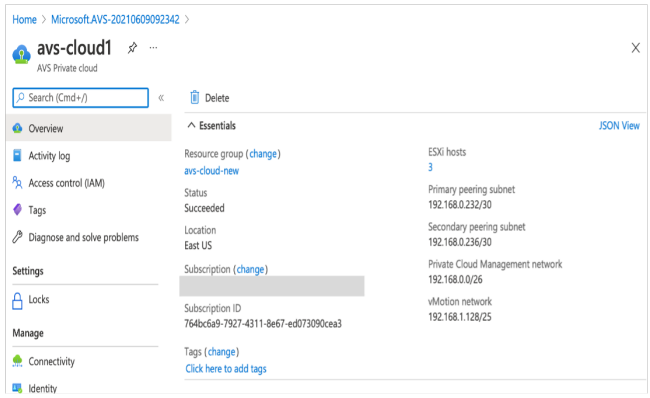
4. 单击“查看 + 创建”。
5. 检查设置。如果必须更改任何设置，请单击“上一步”。



6. 单击创建。私有云配置过程开始。配置私有云最多可能需要两个小时。



7. 单击 转到资源，验证创建的私有云。



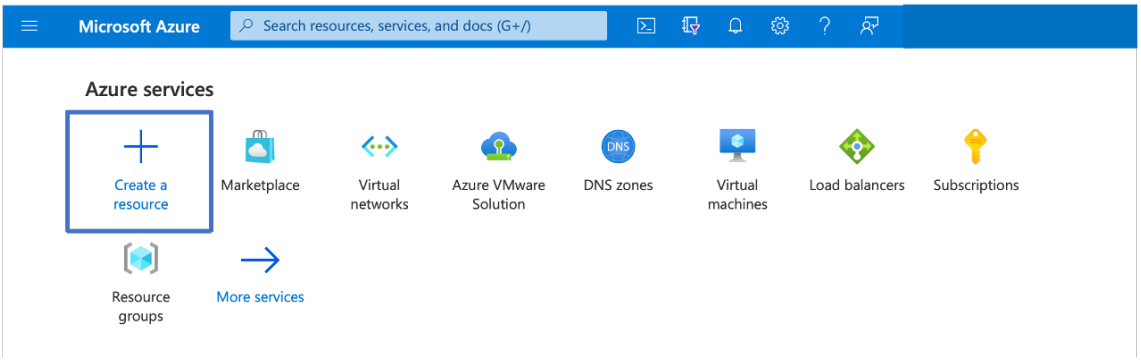
> 注意：
>
> 要访问此资源，您需要 Windows 中的虚拟机充当跳转框。

连接到运行 **Windows** 的 **Azure** 虚拟机

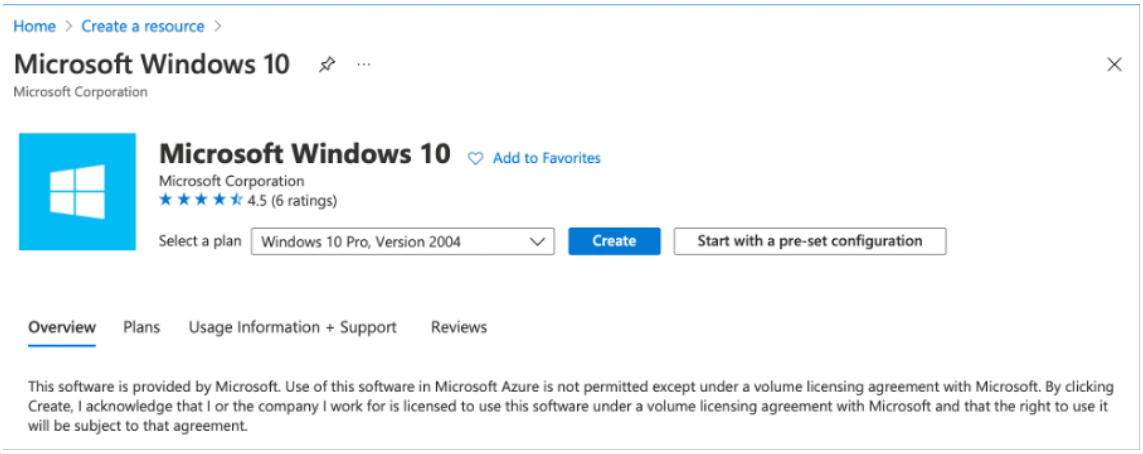
此过程向您展示如何使用 Azure 门户在 Azure 中部署运行 Windows Server 2019 的虚拟机 (VM)。要查看虚拟机的运行，然后 RDP 到虚拟机并安装 IIS Web 服务器。

要访问已创建的私有云，您需要在同一虚拟网络中创建 Windows 跳转框。

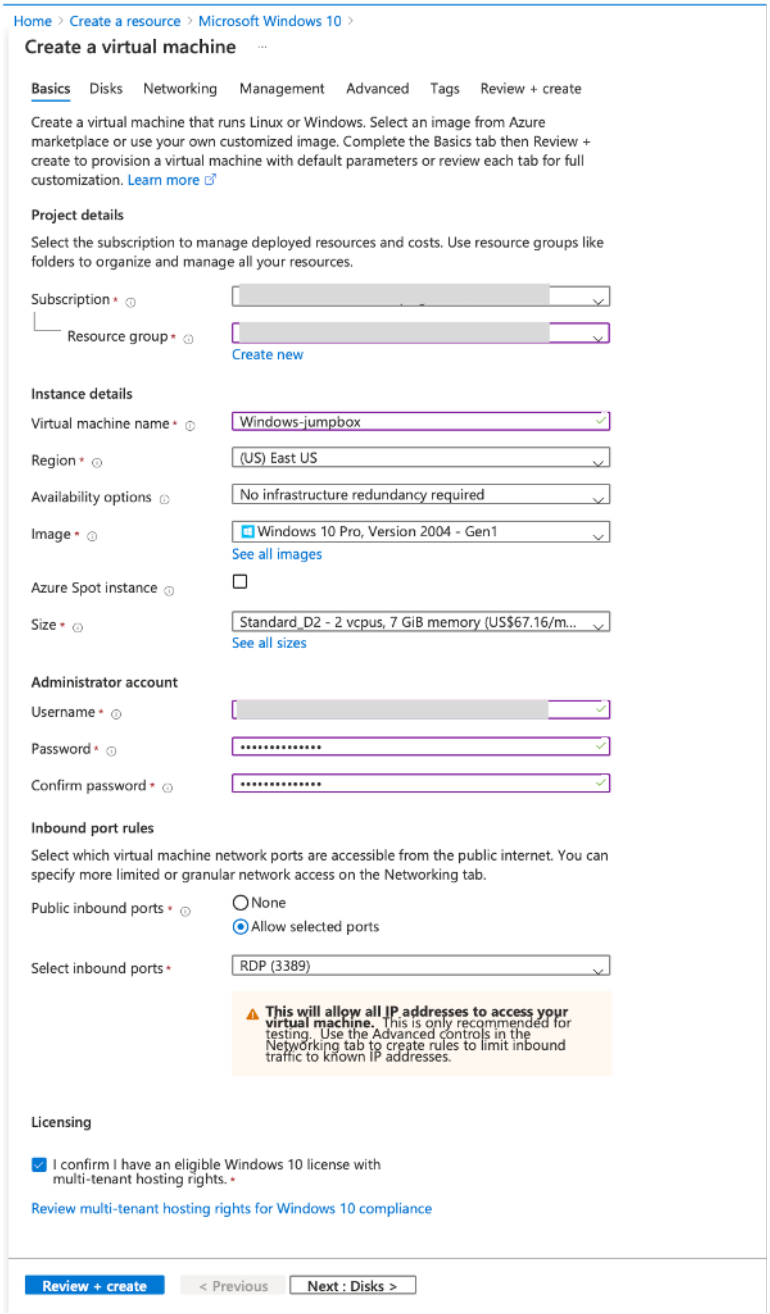
1. 转到 **Azure** 门户，然后单击 创建资源。



2. 搜索 **Microsoft Windows 10**，然后单击 创建。



3. 创建运行 Windows Server 2019 的虚拟机 (VM)。此时将显示“创建虚拟机”页面。在 基础知识 选项卡中输入所有详细信息，然后选中 许可 复选框。保留其余的默认值，然后选择页面底部的“审阅 + 创建”按钮。



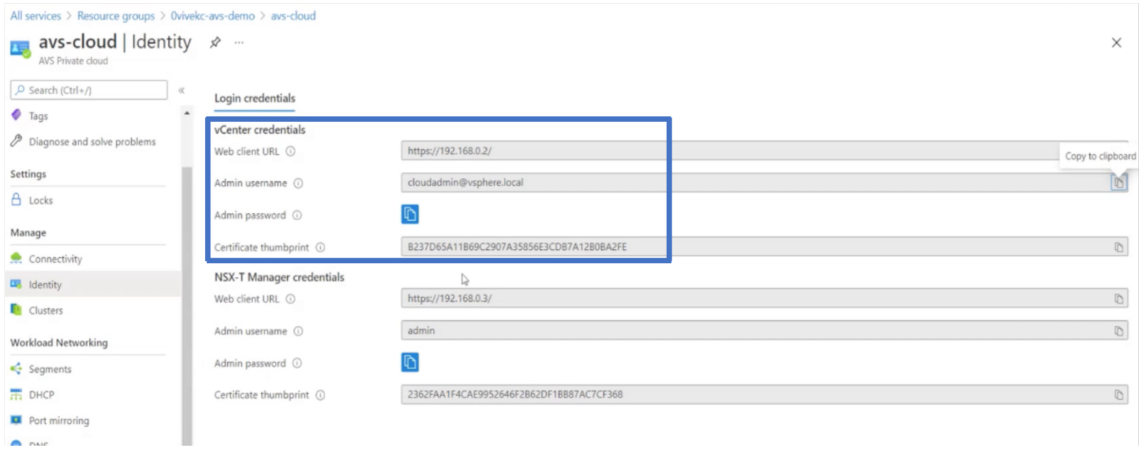
4. 验证运行后，选择页面底部的 创建 按钮。
5. 部署完成后，选择 转到资源。
6. 转到您创建的 Windows 虚拟机。使用 Windows 虚拟机的公有 IP 地址并使用 RDP 进行连接。

   使用 Azure 门户中的 连接 按钮从 Windows 桌面启动远程桌面 (RDP) 会话。首先您连接到虚拟机，然后您登录。

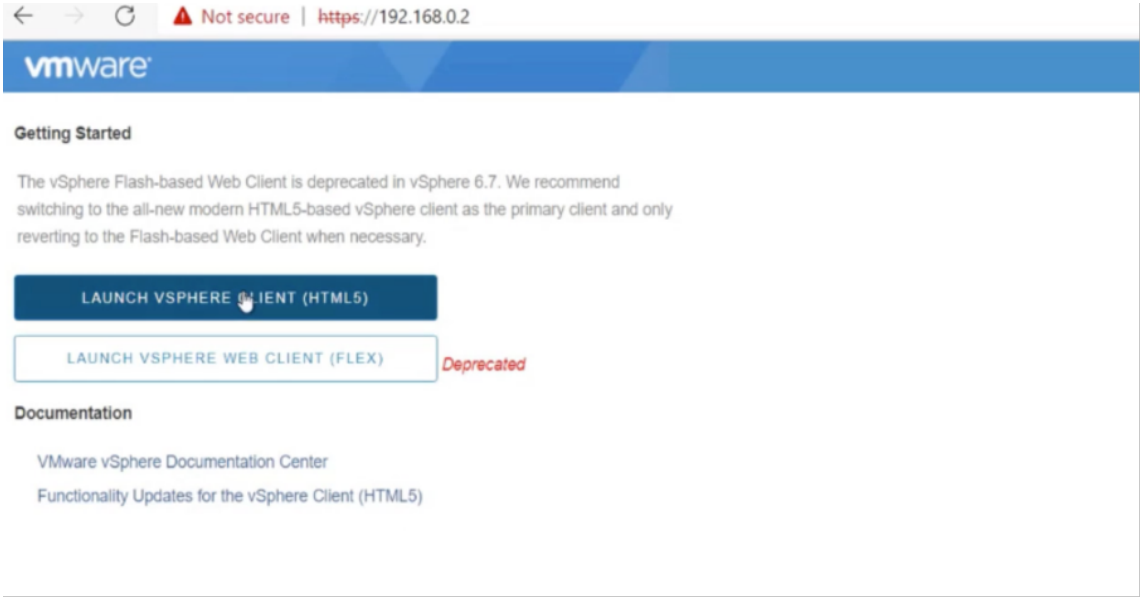
   要从 Mac 连接到 Windows 虚拟机，必须为 Mac 安装 RDP 客户端，例如 Microsoft 远程桌面。有关更多信息，请参阅 如何连接和登录运行 Windows 的 Azure 虚拟机。

访问私有云 **vCenter** 门户

1. 在 Azure VMware 解决方案私有云中的 管理下，选择 身份。记下 vCenter 凭据。

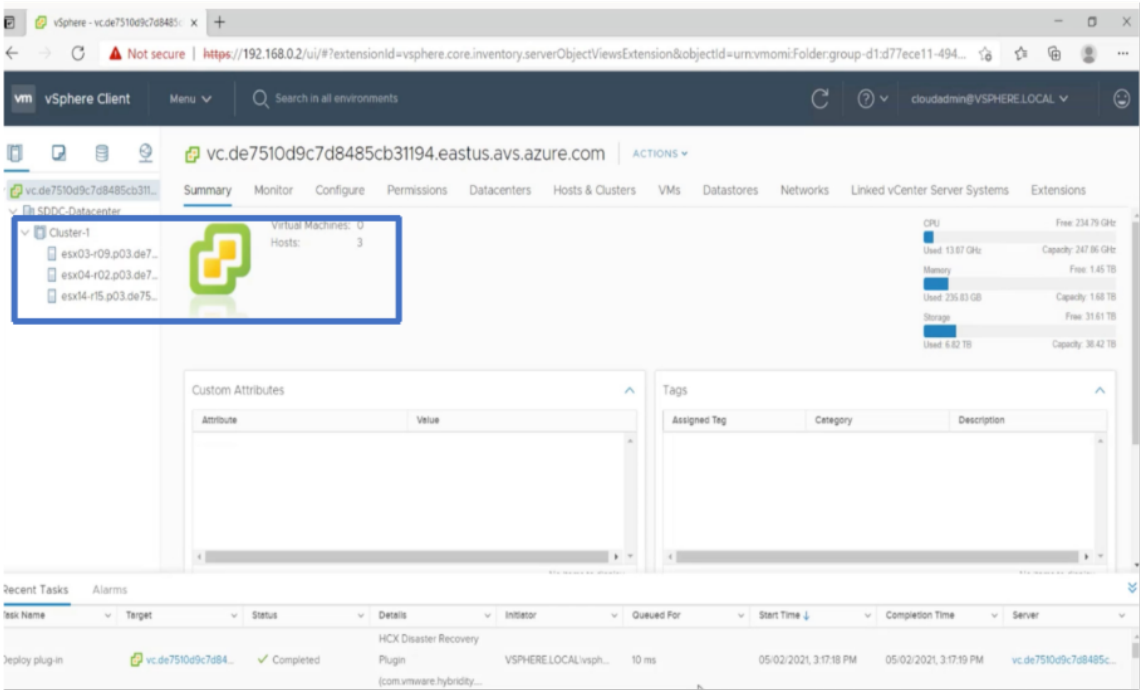


2. 通过键入 vCenter Web 客户端 URL 来启动 vSphere 客户端。



3. 使用 Azure VMware 解决方案私有云的 vCenter 凭据登录 VMware vSphere。

4. 在 vSphere 客户端中，可以验证在 Azure 门户中创建的 ESXi 主机。

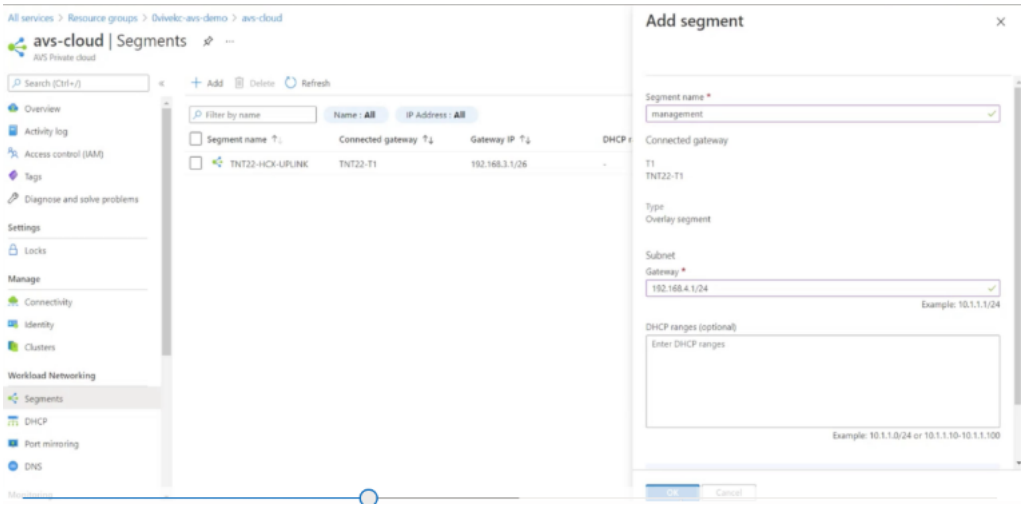


有关更多信息，请参阅 访问私有云 vCenter 门户。

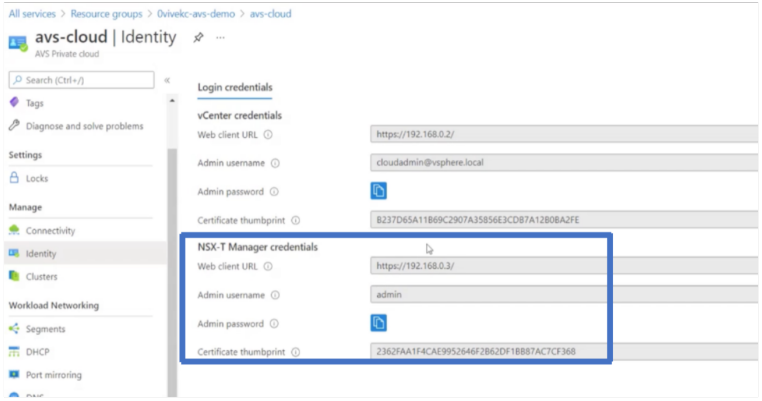
在 **Azure** 门户中创建 **NSX-T** 区段

您可以从 Azure 门户中的 Azure VMware 解决方案控制台创建和配置 NSX-T 区段。这些网段连接到默认的 Tier-1 网关，这些网段上的工作负载可以实现东西和南北连接。创建区段后，它将显示在 NSX-T 管理器和 vCenter 中。

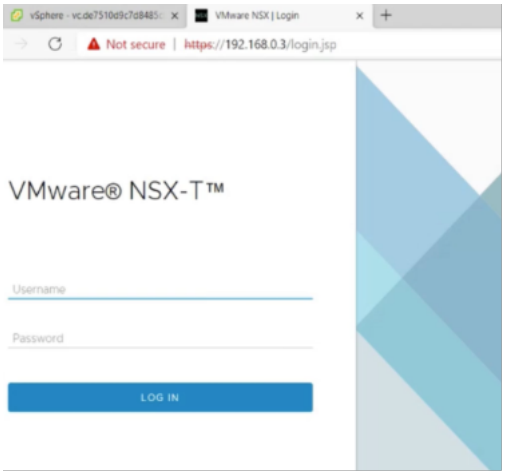
1. 在 Azure VMware 解决方案私有云中的 工作负载网络下，选择 区段 > 添加。提供新逻辑段的详细信息，然后选择确定。您可以为客户端、管理界面和服务器界面创建三个单独的区段。



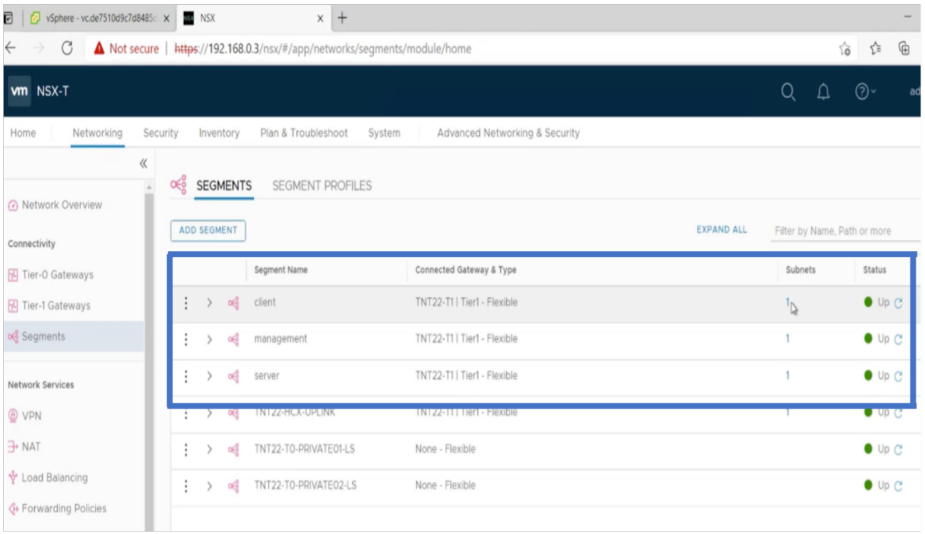
2. 在 Azure VMware 解决方案私有云中的 管理下，选择 身份。记下 NSX-T 管理器凭据。



3. 通过键入 NSX-T Web 客户端 URL 来启动 VMware NSX-T 管理器。



4. 在 NSX-T 管理器中的 网络 > 区段下，您可以看到已创建的所有区段。您还可以验证子网。



有关更多信息，请参阅在 Azure 门户中创建 NSX-T 区段。

在 **VMware** 云上安装 **NetScaler VPX** 实例

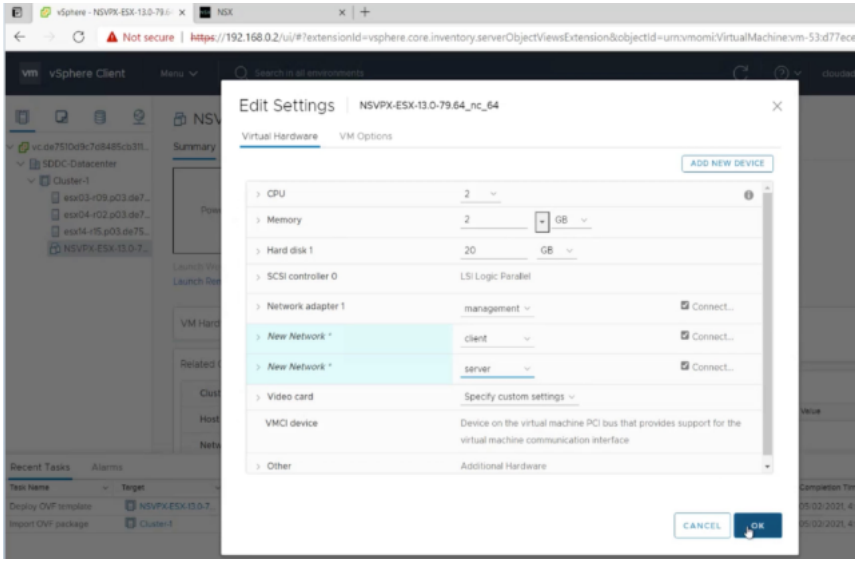
安装和配置 VMware 软件定义数据中心 (SDDC) 后，可以使用 SDDC 在 VMware 云上安装虚拟设备。可以安装的虚拟设备数量取决于 SDDC 上的可用内存量。

要在 VMware 云上安装 NetScaler VPX 实例，请在 Windows Jumpbox 虚拟机中执行以下步骤：

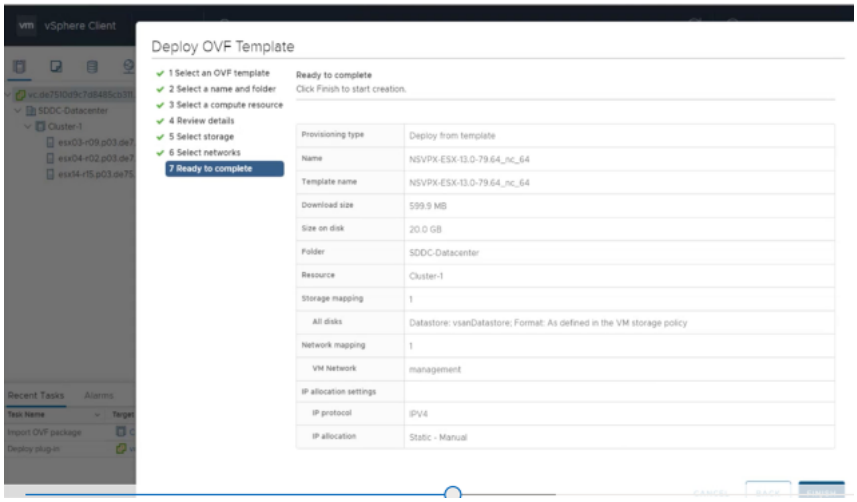
1. 从 NetScaler 下载网站下载适用于 ESXi 主机的 NetScaler VPX 实例设置文件。
2. 在 Windows 跳转框中打开 VMware SDDC。
3. 在“用户名”和“密码”字段中，键入管理员凭据，然后单击“登录”。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在“部 署 **OVF** 模板”对话框的“从文件部署”字段中，浏览到保存 NetScaler VPX 实例安装文件的位置，选择.ovf 文件，然后单击 下一步。

   > 注意：
   >
   > 默认情况下，NetScaler VPX 实例使用 E1000 网络接口。要使用 VMXNET3 接口部署 ADC，请将 OVF 修改为使用 VMXNET3 接口而非 E1000 接口。VMXNET3 接口的可用性受 Azure 基础架构的限制，可能不在 Azure VMware 解决方案中提供。

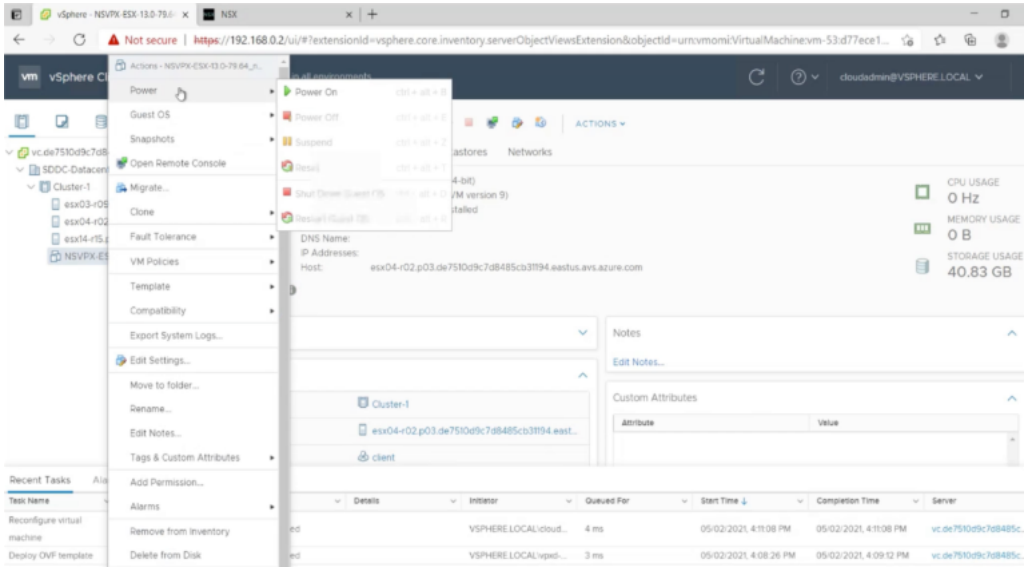
6. 将虚拟设备 OVF 模板中显示的网络映射到在 VMware SDDC 上配置的网络。单击确定。



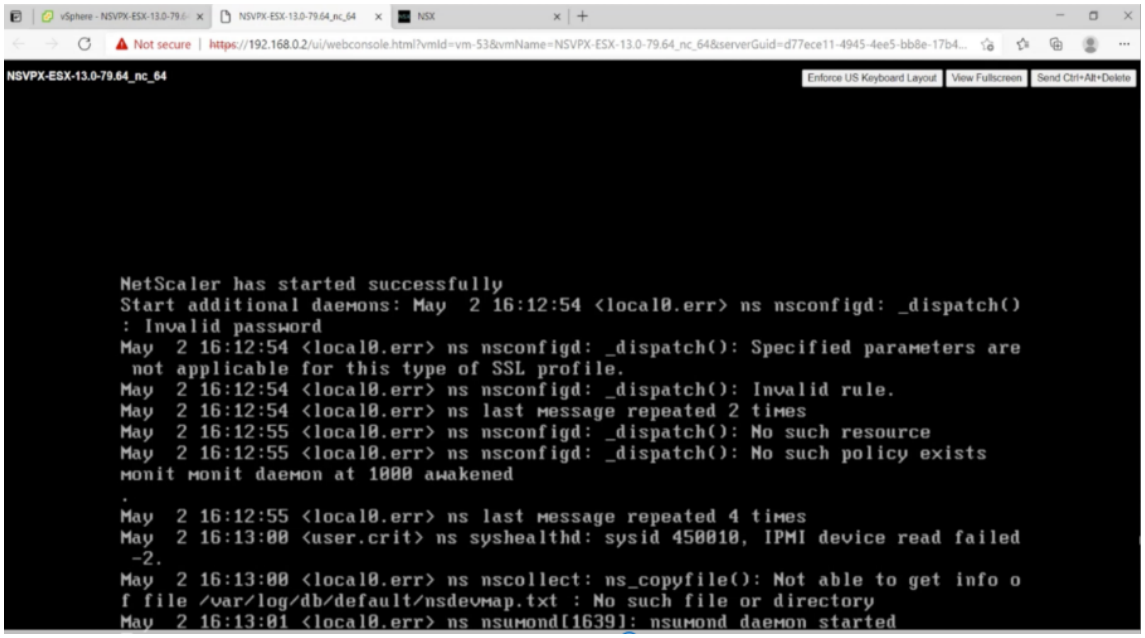
7. 单击“完成”开始在 VMware SDDC 上安装虚拟设备。



8. 现在，您可以启动 NetScaler VPX 实例。在导航窗格中，选择已安装的 NetScaler VPX 实例，然后从右键菜单中选择 **Power On**（开机）。单击 **Console**（控制台）选项卡模拟控制台端口。



9. 现在，您已从 vSphere 客户端连接到 NetScaler 虚拟机。



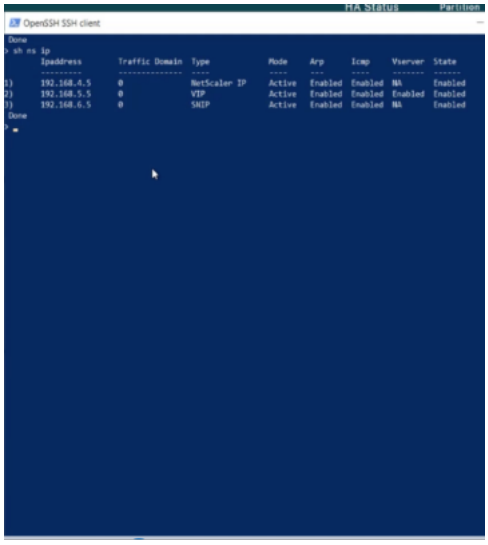
10. 要使用 SSH 密钥访问 NetScaler 设备，请在 CLI 中键入以下命令：

```
ssh nsroot@<management IP address>
```

Example:

```
ssh nsroot@192.168.4.5
```

11. 您可以使用 `show ns ip` 命令验证 ADC 配置。

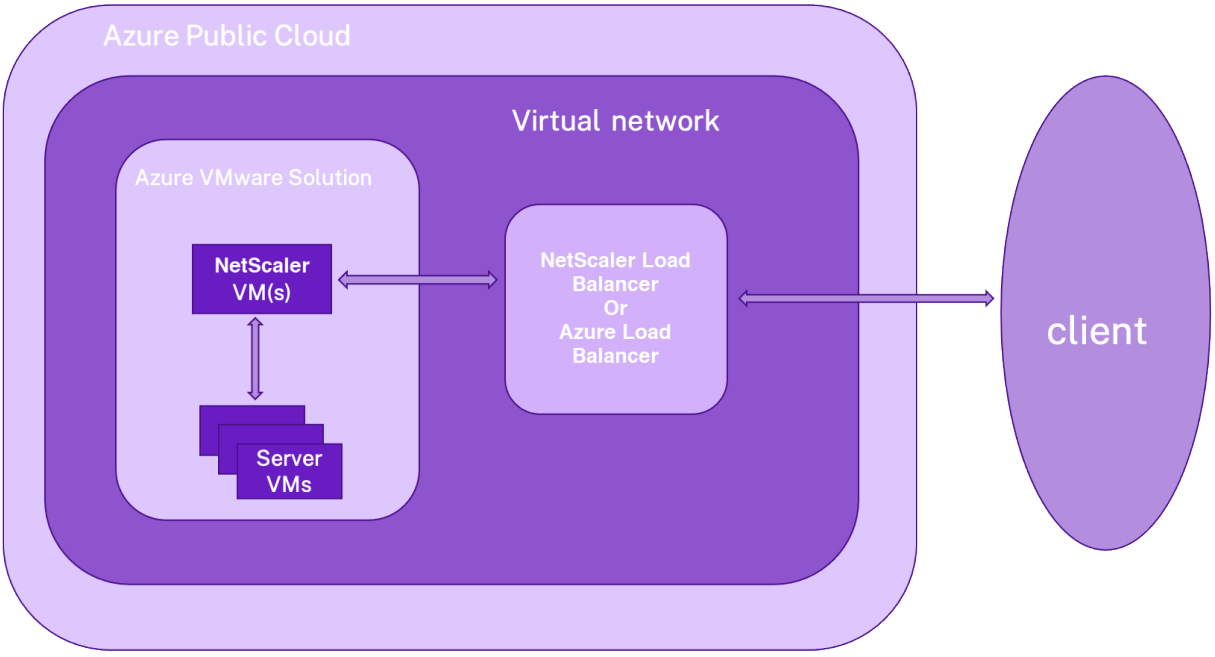


在 **Azure VMware** 解决方案上配置 **NetScaler VPX** 独立实例

October 17, 2024

您可以在 Azure VMware 解决方案 (AVS) 上为面向互联网的应用程序配置 NetScaler VPX 独立实例。

下图显示了 Azure VMware 解决方案上的 NetScaler VPX 独立实例。客户端可以通过连接到 AVS 内 NetScaler 的虚拟 IP (VIP) 地址来访问 AVS 服务。您可以通过在 AVS 外部但在同一 Azure 虚拟网络中预配 NetScaler 负载平衡器或 Azure 负载平衡器实例来实现此目的。配置负载平衡器以访问 AVS 服务中 NetScaler VPX 实例的 VIP。



必备条件

在开始安装虚拟设备之前，请阅读以下 Azure 先决条件：

- 有关 Azure VMware 解决方案及其先决条件的更多信息，请参阅 Azure VMware 解决方案文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware 解决方案私有云。
- 有关创建 Windows Jump box VM 以访问和管理 Azure VMware 解决方案的详细信息，请参阅 访问 Azure VMware 解决方案私有云。
- 在 Windows 跳转框虚拟机中，下载 NetScaler VPX 设备安装文件。
- 在虚拟机连接到的 VMware SDDC 上创建适当的 NSX-T 网段。有关详细信息，请参阅在 Azure VMware 解决方案中添加网段
- 有关如何在 VMware 云上安装 NetScaler VPX 实例的更多信息，请参阅 在 VMware 云上安装 NetScaler VPX 实例。

使用 **NetScaler** 负载平衡器在 **AVS** 上配置 **NetScaler VPX** 独立实例

请按照以下步骤使用 NetScaler 负载平衡器在 AVS 上为面向互联网的应用程序配置 NetScaler VPX 独立实例。

1. 在 Azure 云上部署 NetScaler VPX 实例。有关更多信息，请参阅 配置 NetScaler VPX 独立实例。

   > 注意：
   >
   > 确保其部署在与 Azure VMware 云相同的虚拟网络上。

2. 配置 NetScaler VPX 实例以访问部署在 AVS 上的 NetScaler VPX 的 VIP 地址。

   a) 添加负载平衡虚拟服务器。

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

   Example:

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   ```

   b) 添加一项服务，该服务可连接到部署在 AVS 上的 NetScaler VPX 的 VIP。

   ```
   add service <name> <ip> <serviceType> <port>
   ```

   Example:

   ```
   add service webserver1 192.168.4.10 HTTP 80
   ```

   c) 将服务绑定到负载平衡虚拟服务器。

   ```
   bind lb vserver <name> <serviceName>
   ```

   Example:


```
bind lb vserver lb1 webserver1
```

使用 **Azure** 负载平衡器在 **AVS** 上配置 **NetScaler VPX** 独立实例

请按照以下步骤在 AVS 上为使用 Azure 负载平衡器的面向互联网的应用程序配置 NetScaler VPX 独立实例。

1. 在 Azure 云上配置 Azure 负载均衡器实例。有关详细信息，请参阅有关 创建负载均衡器的 Azure 文档。
2. 将部署在 AVS 上的 NetScaler VPX 实例的 VIP 地址添加到后端池中。

   以下 Azure 命令将一个后端 IP 地址添加到负载平衡后端地址池中。

```
az network lb address-pool address add
                                      --resource-group <Azure VMC
                                         Resource Group>
                                      --lb-name <LB Name>
                                      --pool-name <Backend pool
                                         name>
                                      --vnet <Azure VMC Vnet>
                                      --name <IP Address name>
                                      --ip-address <VIP of ADC in
                                         VMC>
```

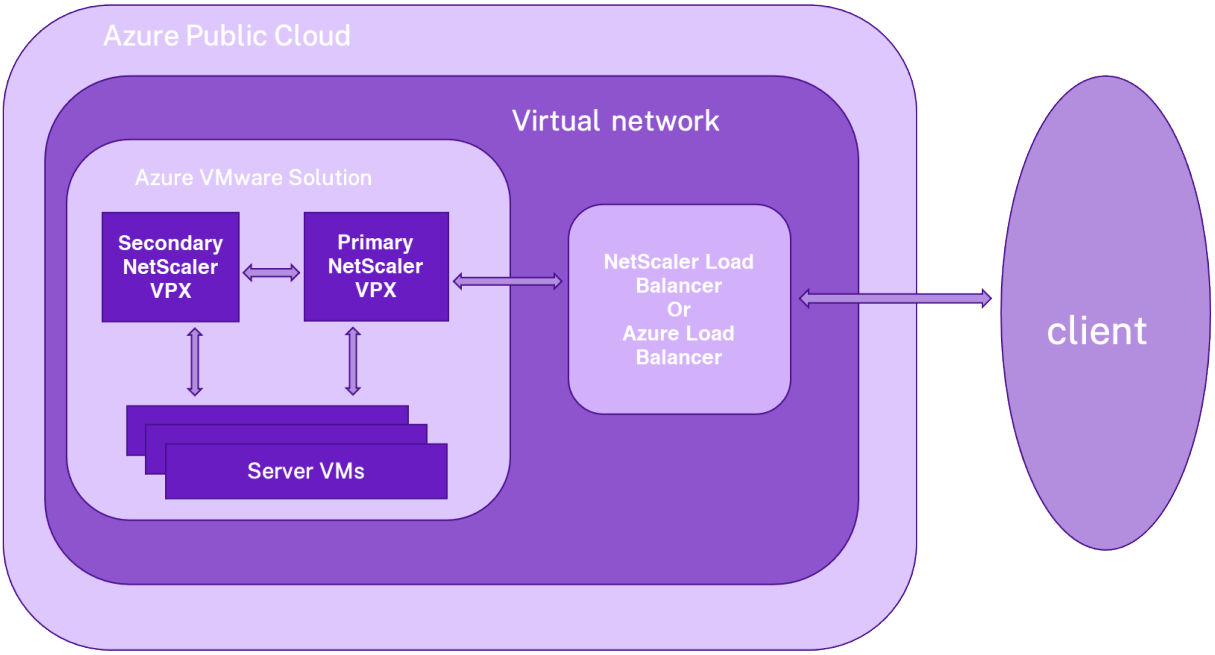
> 注意：
>
> 确保 Azure 负载平衡器部署在与 Azure VMware 云相同的虚拟网络中。

在 **Azure VMware** 解决方案上配置 **NetScaler VPX** 高可用性设置

October 17, 2024

您可以在 Azure VMware 解决方案 (AVS) 上为面向互联网的应用程序配置 NetScaler VPX HA 设置。

下图显示了 AVS 上的 NetScaler VPX HA 对。客户端可以通过连接到 AVS 内的主 ADC 节点的 VIP 来访问 AVS 服务。您可以通过在 AVS 外部但在同一 Azure 虚拟网络中预配 NetScaler 负载平衡器或 Azure 负载平衡器实例来实现此目的。配置负载均衡器以访问 AVS 服务中主 ADC 节点的 VIP。



必备条件

在开始安装虚拟设备之前，请阅读以下 Azure 先决条件：

- 有关 Azure VMware 解决方案及其先决条件的更多信息，请参阅 Azure VMware 解决方案文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware 解决方案私有云。
- 有关创建 Windows Jump box VM 以访问和管理 Azure VMware 解决方案的详细信息，请参阅 访问 Azure VMware 解决方案私有云。
- 在 Windows 跳转框虚拟机中，下载 NetScaler VPX 设备安装文件。
- 在虚拟机连接到的 VMware SDDC 上创建适当的 NSX-T 网段。有关详细信息，请参阅 在 Azure VMware 解决方案中添加网段。

配置步骤

请按照以下步骤在 AVS 中为面向互联网的应用程序配置 NetScaler VPX 高可用性设置。

1. 在 VMware 云上创建两个 NetScaler VPX 实例。有关更多信息，请参阅 在 VMware 云上安装 NetScaler VPX 实例。
2. 配置 NetScaler HA 设置。有关更多信息，请参阅 配置高可用性。
3. 将 NetScaler HA 设置配置为面向互联网的应用程序可以访问。
    - 要使用 NetScaler 负载均衡器配置 NetScaler VPX 实例，请参阅 使用 NetScaler 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例。

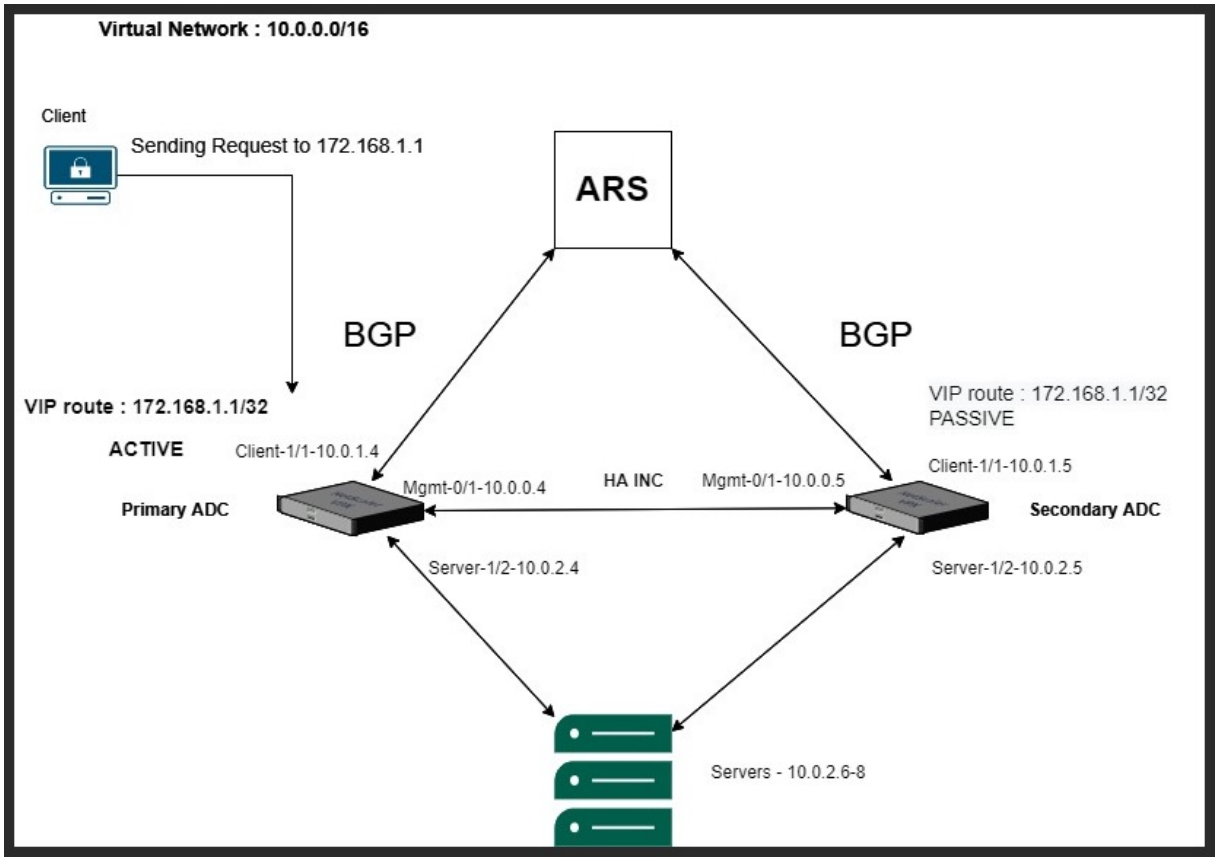
- 要使用 Azure 负载均衡器配置 NetScaler VPX 实例，请参阅 使用 Azure 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例。

使用 **NetScaler VPX HA** 对配置 **Azure** 路由服务器

October 17, 2024

您可以使用 NetScaler VPX 实例配置 Azure 路由服务器，以交换使用 BGP 协议配置为虚拟网络的 VIP 路由。NetScaler 可以独立部署或在 HA-INC 模式下部署，然后使用 BGP 进行配置。此部署不需要在 ADC HA 对前面安装 Azure 负载平衡器 (ALB)。

下图描述了 VPX HA 拓扑如何与 Azure 路由服务器集成。每个 ADC 实例都有 3 个接口：一个用于管理，一个用于客户端流量，另一个用于服务器流量。



拓扑图使用以下 IP 地址。

主 **ADC** 实例的 **IP** 配置示例：

```
NSIP: 10.0.0.4/24
SNIP on 1/1: 10.0.1.4/24
SNIP on 1/2: 10.0.2.4/24
```



```
4    VIP: 172.168.1.1/32
```

辅助 **ADC** 实例的 **IP** 配置示例：

```
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
```

必备条件

在 Azure 上部署 NetScaler VPX 实例之前，您必须熟悉以下信息。

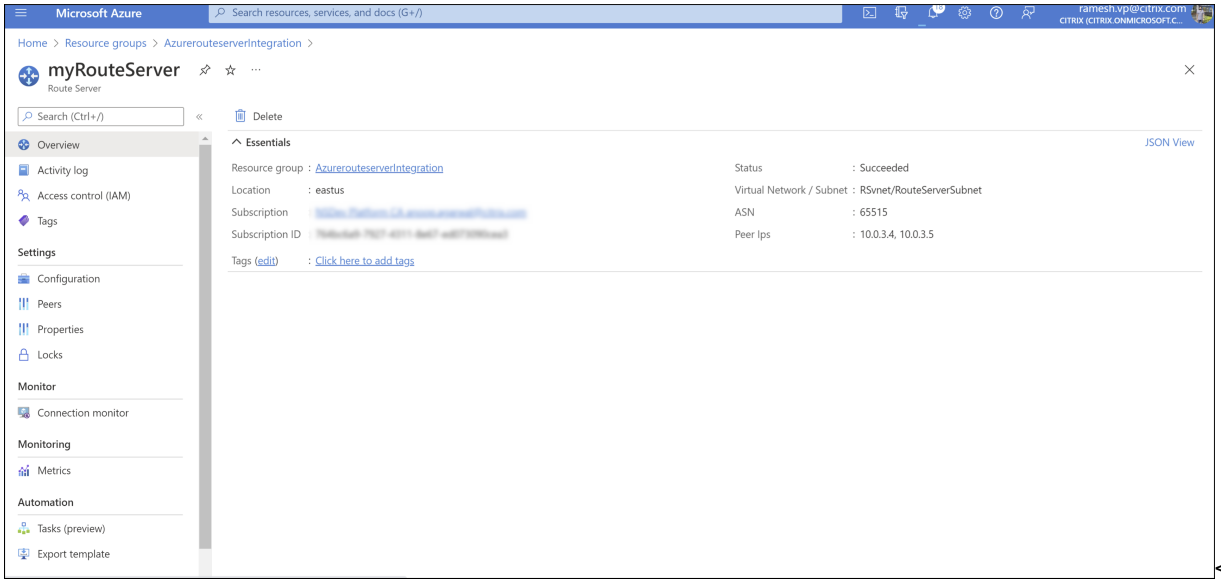
- Azure 术语和网络详细信息。有关更多信息，请参阅 Azure 术语。
- 在 Azure 门户中创建路由服务器。有关详细信息，请参阅 使用 Azure 门户创建和配置路由服务器。
- NetScaler 设备的工作原理。有关更多信息，请参阅 NetScaler 文档。
- NetScaler 联网。有关更多信息，请参阅 ADC 网络。

如何使用 **NetScaler VPX HA** 对配置 **Azure** 路由服务器

1. Azure 路由服务器概述。有关详细信息，请参阅

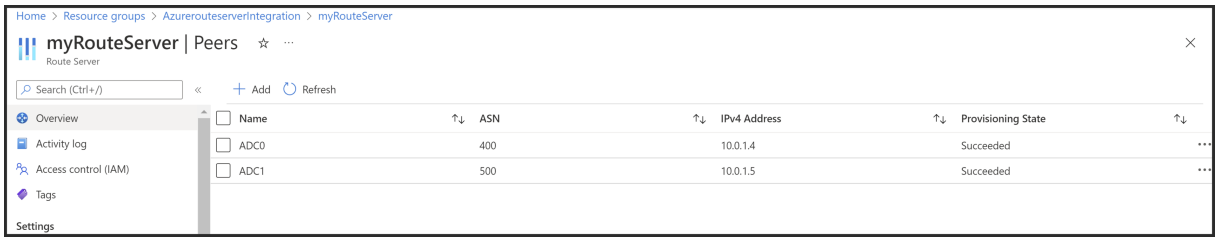
   什么是 Azure 路由服务器？ </p>

在以下示例中，子网 10.0.3.0/24 用于部署 Azure 服务器。创建路由服务器后，获取路由服务器 IP 地址，例如：10.0.3.4、10.0.3.5。



1 在 Azure 门户中设置与网络虚拟设备 (NVA) 的对等互连。将您的 NetScaler VPX 实例添加为 NVA。有关更多信息，请参阅 设置与 NVA 的对等互连。

在以下示例中, 添加对等项时使用了 1/1 接口上的 ADC SNIP: 10.0.1.4 和 10.0.1.5 以及 ASN: 400 和 500。



1 为高可用性配置添加两个 NetScaler VPX 实例。

完成以下步骤:

```
1.  在 Azure 上部署两个 VPX 实例（主实例和辅助实例）。
1.  在两个实例上添加客户端和服务器 NIC。
1.  使用 NetScaler GUI 在两个实例上配置 HA 设置。 1  在主 ADC 实例中配置动态路由。
```

示例配置:

```
```
  enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
  enable ns feature LB BGP
  add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -dynamicRouting ENABLED
  VTYSH
  configure terminal
  router BGP 400
  timers bgp 1 3
  neighbor 10.0.3.4 remote-as 65515
  neighbor 10.0.3.4 advertisement-interval 3
  neighbor 10.0.3.4 fall-over bfd
  neighbor 10.0.3.5 remote-as 65515
  neighbor 10.0.3.5 advertisement-interval 3
  neighbor 10.0.3.5 fall-over bfd
  address-family ipv4
  redistribute kernel
  redistribute static
```
```

1 在辅助 ADC 实例中配置动态路由。

示例配置:

```
```
  enable ns mode L3 MBF USNIP SRADV DRADV PMTUD
  enable ns feature LB BGP
  add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting ENABLED
  VTYSH
  configure terminal
  router BGP 500
  timers bgp 1 3
```

 
```

```
  neighbor 10.0.3.4 remote-as 65515
  neighbor 10.0.3.4 advertisement-interval 3
  neighbor 10.0.3.4 fall-over  bfd
  neighbor 10.0.3.5 remote-as 65515
  neighbor 10.0.3.5 advertisement-interval 3
  neighbor 10.0.3.5 fall-over  bfd
  address-family ipv4
  redistribute kernel
  redistribute static
```

1 验证在 VTY 外壳接口中使用 BGP 命令建立的 BGP 对等体。有关更多信息，请参阅 验证 BGP 配置。

```
  show ip bgp neighbors
```

1 在主 ADC 实例中配置 LB 虚拟服务器。

示例配置：

```
  add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED
  add lbvserver v1 HTTP 172.16.1.1 80
  add service s1 10.0.2.6 HTTP 80
  bind lbvserver v1 s1
  enable ns feature lb
```

与 NetScaler VPX 实例处于同一虚拟网络中的客户端现在可以访问 LB 虚拟服务器。在这种情况下，NetScaler VPX 实例会向 Azure 路由服务器通告 VIP 路由。

添加后端 **Azure** 自动缩放服务

October 17, 2024

在云中高效托管应用程序涉及根据应用程序需求轻松且经济高效地管理资源。为了满足不断增长的需求，您必须扩大网络资源。而当需求减少时，必须缩小以避免不必要的闲置资源成本。为了最大限度地降低运行应用程序的成本，您必须不断监视流量、内存和 CPU 使用情况等。但是，手动监视流量很麻烦。为了使应用程序环境动态地向上或向下扩展，您必须在必要时自动执行监视流量和向上和向下扩展资源的流程。

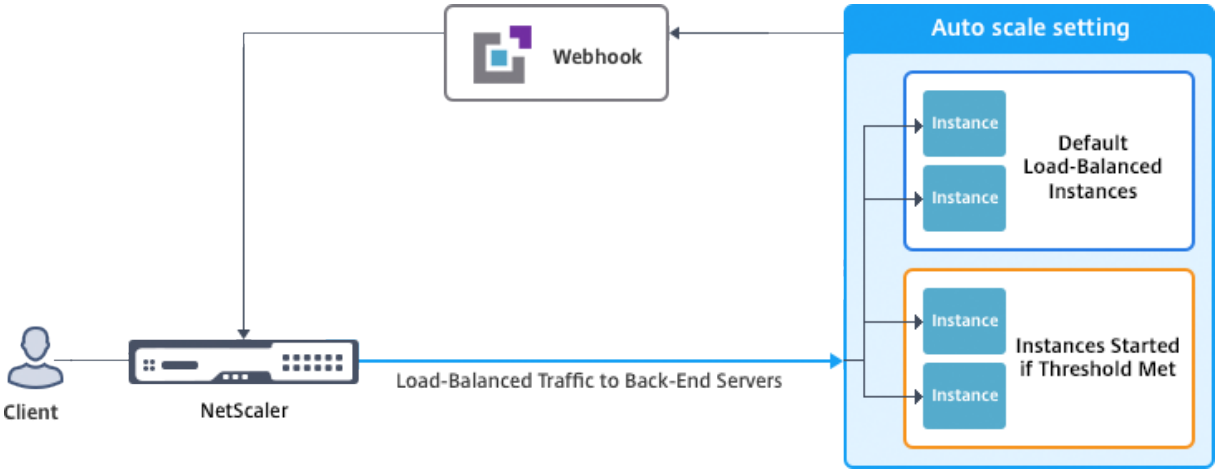
可以将 AutoScale 与 Azure 虚拟机规模集 (VMSS) 结合使用，以便在 Azure 上实现 VPX 多 IP 独立部署和高可用性部署。

NetScaler VPX 实例与 Azure VMSS 和 AutoScale 功能集成，具有以下优势：

- 负载平衡和管理：根据需要自动配置服务器以纵向扩展和横向扩展。NetScaler VPX 实例会在部署 VPX 实例的同一虚拟网络中自动检测 VMSS AutoScale 设置，或者在同一 Azure 订阅中的对等虚拟网络中自动检测

VMSS AutoScale 设置。您可以选择 VMSS AutoScale 设置来平衡负载。这是通过在 VPX 实例上自动配置 NetScaler 虚拟 IP 地址和子网 IP 地址来完成的。

- 高可用性：检测 AutoScale 组并对服务器进行负载平衡。
- 更好的网络可用性：VPX 实例支持不同虚拟网络 (VNet) 上的后端服务器。



有关详细信息，请参阅以下 Azure 主题：

- 虚拟机规模集文档
- Microsoft Azure 虚拟机、云服务和 Web 应用程序中的 AutoScale 概述

开始之前的准备工作

- 阅读 Azure 相关的使用指南。有关更多信息，请参阅 在 Microsoft Azure 上部署 NetScaler VPX 实例。
- 根据您的要求（独立部署或高可用性部署）在 Azure 上创建一个或多个 NetScaler VPX 实例，其中包含三个网络接口。
- 在 VPX 实例的 0/1 接口的网络安全组中打开 TCP 9001 端口。VPX 实例使用此端口接收横向扩展和纵向扩展通知。
- 在部署 NetScaler VPX 实例的同一虚拟网络中创建 Azure VMSS。如果 VMSS 和 NetScaler VPX 实例部署在不同的 Azure 虚拟网络中，则必须满足以下条件：
  - 两个虚拟网络必须位于同一 Azure 订阅中。
  - 必须使用 Azure 的虚拟网络对等互连功能连接这两个虚拟网络。

  如果您没有现有 VMSS 配置，请完成以下任务：

  a) 创建 VMSS

  b) 在 VMSS 上启用 AutoScale

  c) 在 VMSS 自动缩放设置中创建向内和向外扩展策略

  有关更多信息，请参阅 使用 Azure 虚拟机规模集进行自动缩放概述。

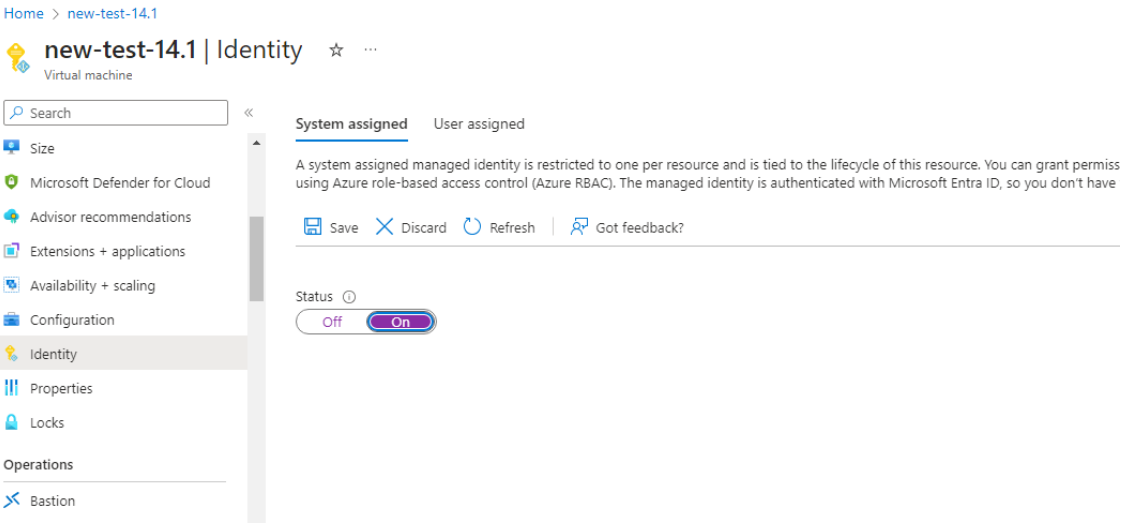
- NetScaler VPX 仅支持具有统一编排功能的 VMSS。不支持具有灵活编排功能的 VMSS。有关更多信息，请参阅 Azure 中虚拟机规模集的编排模式。
- 从 NetScaler 版本 14.1-12.x 开始，NetScaler VPX 支持 Azure 云中的托管身份。托管身份将服务主体链接到 Azure 资源，例如虚拟机。使用托管身份，您无需管理云证书（应用程序 ID、应用程序密钥和租户 ID），从而避免安全风险。目前，NetScaler VPX 仅支持系统分配的身份和单用户分配的托管身份。不支持多用户分配的托管身份。

  对于 14.1-12.x 之前的 NetScaler 版本，您必须通过 Azure Active Directory (AAD) 手动管理 NetScaler VPX 中的云证书。为新创建的 AAD 应用程序分配贡献者角色。云证书过期后必须定期重新创建。有关更多信息，请参见 创建 Azure Active Directory 应用程序和服务主体。

  在 Azure 控制台上配置托管身份和在 NetScaler 中配置云凭据时，托管身份优先于云证书。

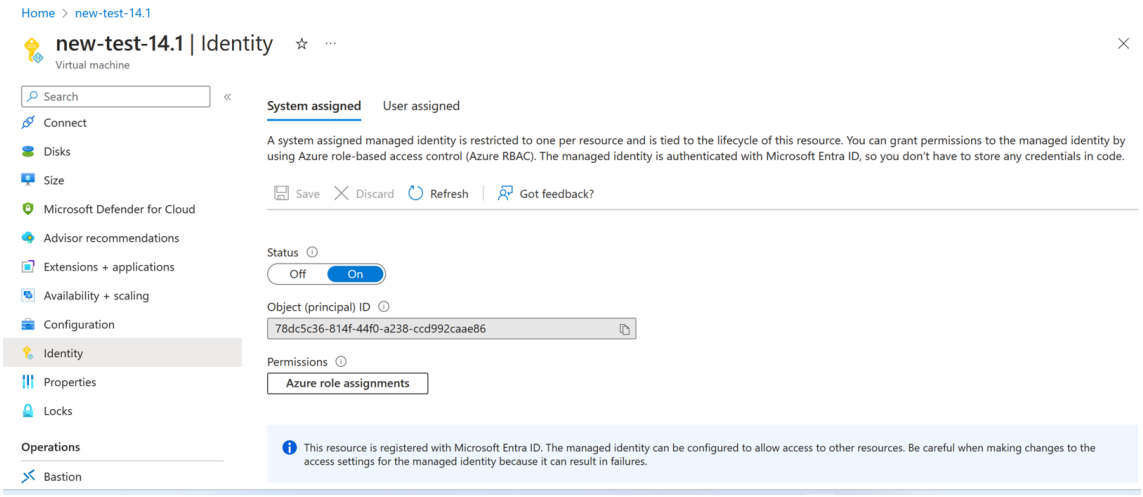
在虚拟机上配置托管身份

1. 登录 Azure 门户。
2. 导航到您的虚拟机并选择 身份。
3. 根据您的要求选择“系统分配”或“用户分配”。
4. 在“状态”下，选择“开”，然后单击“保存”。



   保存状态后，您会看到服务主体对象已创建并分配给虚拟机。

5. 单击 **Azure** 角色分配。



6. 在“添加角色分配”窗口中，选择作用域。您可以从以下选项中进行选择：

   - 订阅

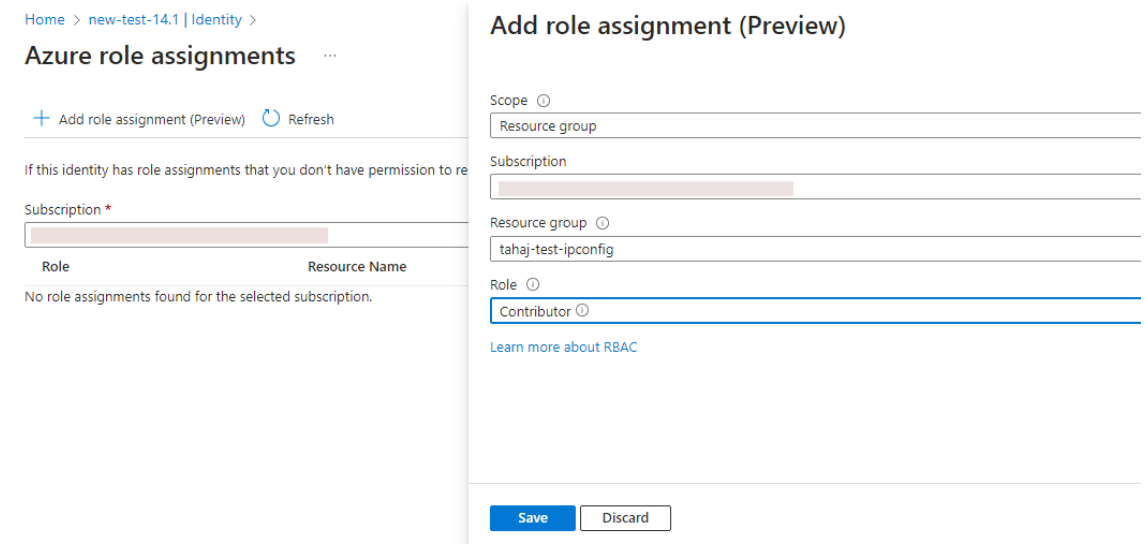
     如果 VMSS 和 VM 位于不同的资源组中，请使用 订阅 作为范围。

   - 资源组

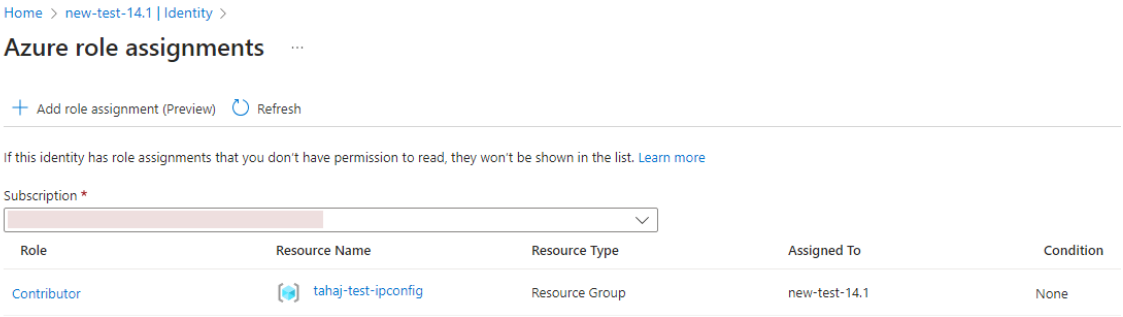
     如果 VMSS 与您的虚拟机位于同一个资源组中，请使用 资源组 作为范围。

   - 密钥保管库
   - 存储
   - SQL

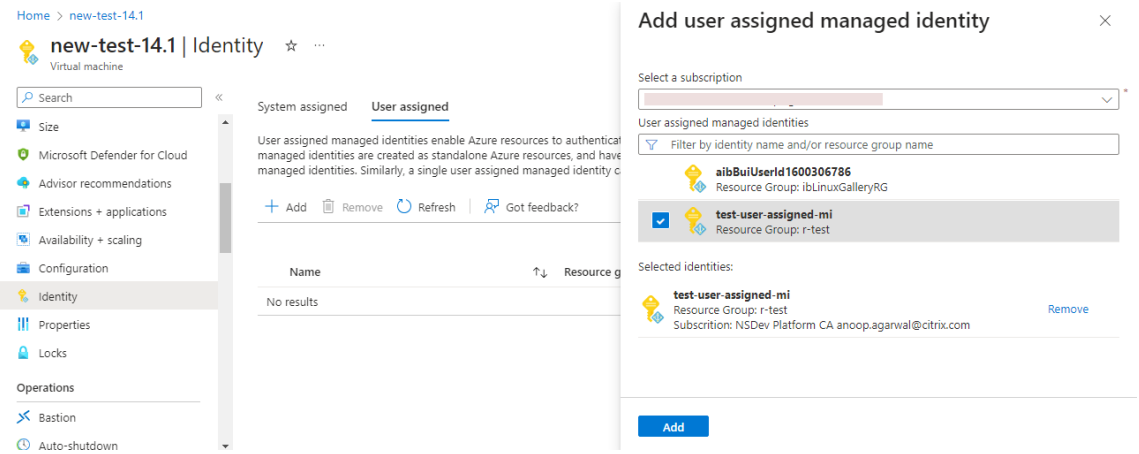
   根据您的范围选择，填写其他字段的详细信息。分配 贡献 者角色并 保存 配置。



   Azure 角色分配页面显示您创建的托管身份。



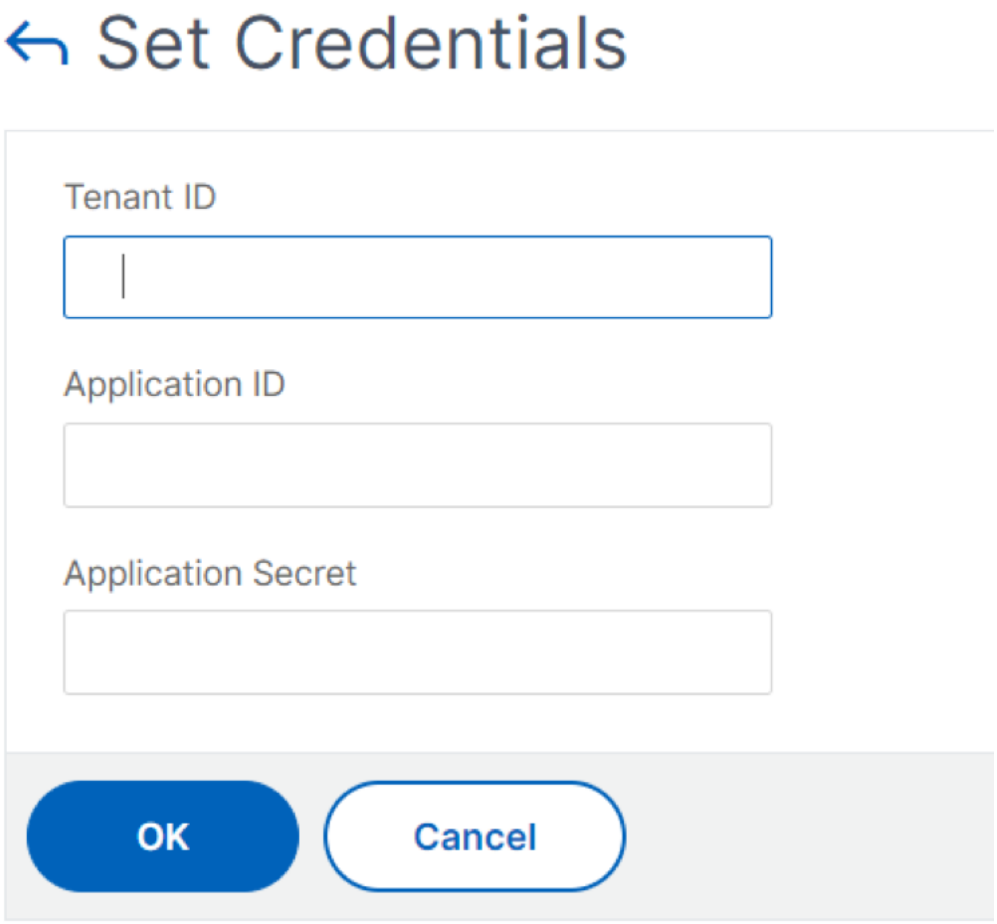
7. 要创建分配给用户的托管身份，请选择订阅，选择为用户分配的托管身份，然后单击“添加”。



将 **VMSS** 添加到 **NetScaler VPX** 实例

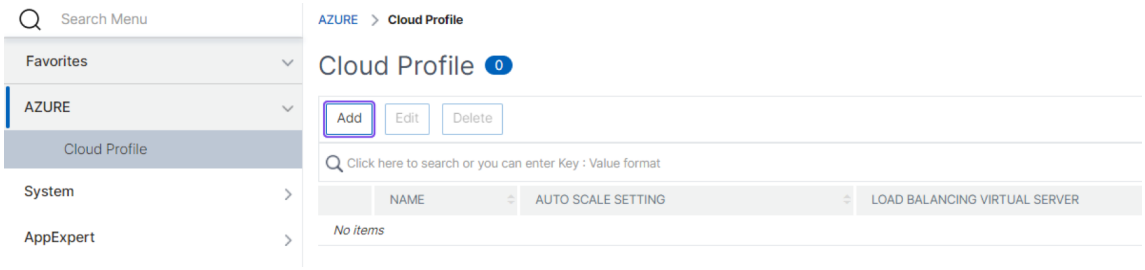
完成以下步骤，将 AutoScale 设置添加到 VPX 实例：

1. 登录到 VPX 实例。
2. 导航到 配置 **> Azure >** 设置凭据。添加所需的 Azure 凭据以使 AutoScale 功能能够运行。

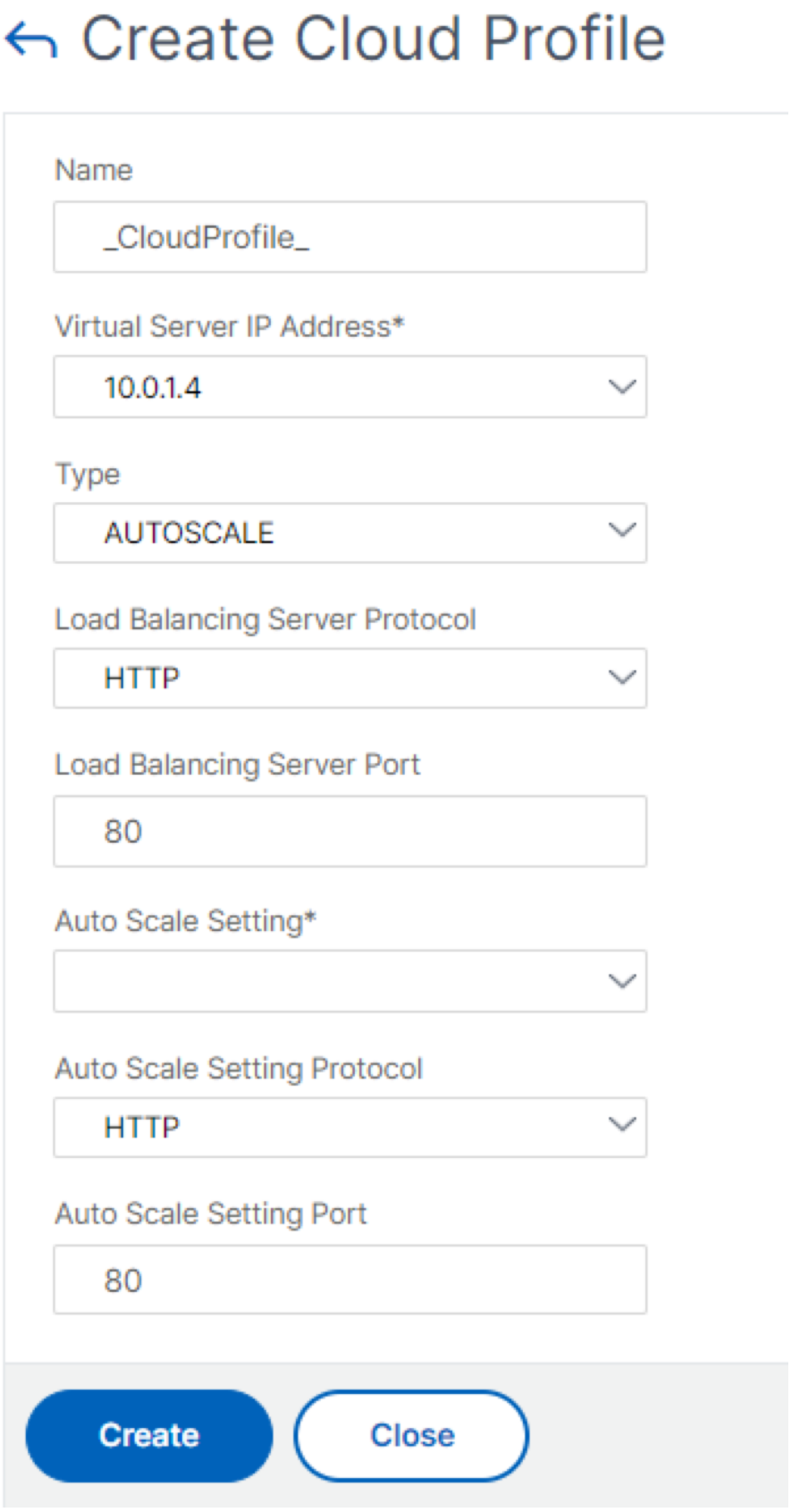


> 注意：
>
> 如果您使用的是 Azure 托管身份，则无需设置凭据。

3. 转到“系统”**>**“**Azure**”**>**“云配置文件”，然后单击“添加”以创建云配置文件。



将出现“创建云配置文件”配置页面。



云配置文件创建一个 NetScaler 负载平衡虚拟服务器和一个以成员（服务器）作为 Auto Scaling 组服务器的服务组。您的后端服务器必须能够通过 VPX 实例上配置的 SNIP 进行访问。

创建云配置文件时需要注意的几点

- 虚拟服务器 IP 地址是从 VPX 实例可用的可用 IP 地址自动填充的。有关更 多信息，请参阅使用 Azure 门户为虚拟机分配多个 IP 地址。
- AutoScale 设置是从连接到 NetScaler VPX 实例的 VMSS 实例中预先填充的，该实例位于同一个虚拟网络或对等虚拟网络中。有关更多信息，请参阅 使用 Azure 虚拟机规模集进行自动缩放概述。
- 在选择 **Auto Scale** 设置协议和自动扩展设置端口时，请确保您的服务器监听协议和端口，并在服务组中绑定正确的显示器。默认情况下，使用 TCP 监视器。
- 对于 SSL 协议类型的自动扩展，创建云配置文件后，由于缺少证书，负载平衡虚拟服务器或服务组将关闭。可以手动将证书绑定到虚拟服务器或服务组。

> 注意：
>
> 自 NetScaler 版本 13.1-42.x 起，您可以在 Azure 中使用相同的 VMSS 为不同的服务（使用不同的端口）创建不同的云配置文件。因此，NetScaler VPX 实例支持公有云中具有相同自动缩放组的多个服务。

要在 Azure 门户中查看与 AutoScale 相关的信息，请转到虚拟机规模集，然后选择虚拟机规模集 > 缩放。

引用

有关使用 NetScaler 应用程序交付和管理在 Microsoft Azure 中自动缩放 NetScaler VPX 的信息，请参阅 使用 NetScaler ADM 的 Azure 自动缩放。

部署 **NetScaler VPX** 的 **Azure** 标签

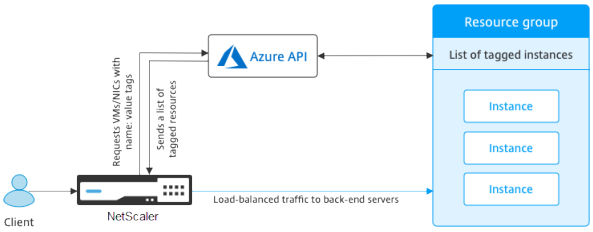
October 17, 2024

在 Azure 云门户中，可以使用名称: 值对（例如 Dept: Finance）对资源进行标记，以跨资源组以及在门户中跨订阅对资源进行分类和查看。当您需要组织资源以进行计费、管理或自动化时，标记非常有用。

Azure 标记在 **VPX** 部署中的工作原理

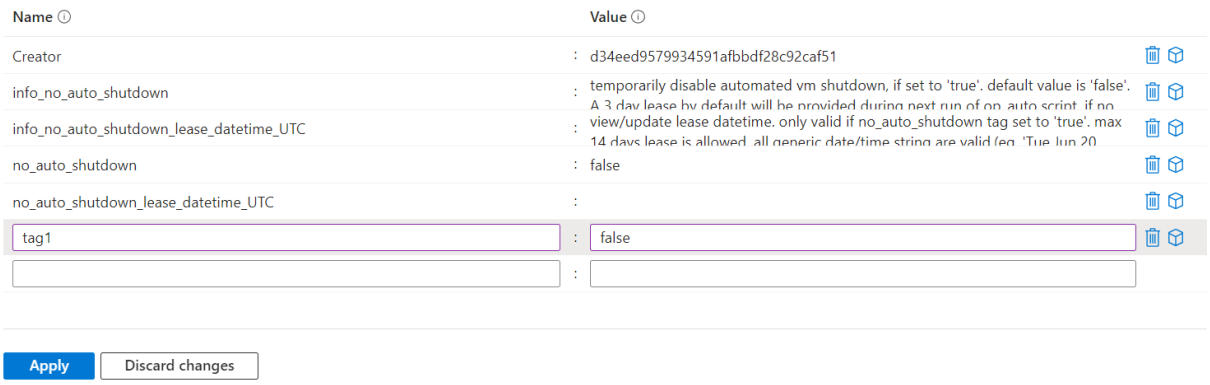
对于部署在 Azure 云上的 NetScaler VPX 独立实例和高可用性实例，现在您可以创建与 Azure 标签关联的负载平衡服务组。VPX 实例使用相应的标记持续监视 Azure 虚拟机（后端服务器）和网络接口 (NIC)（或两者），并相应地更新服务组。

VPX 实例创建使用标记平衡后端服务器负载的服务组。实例在 Azure API 中查询使用特定标记名称和标记值进行标记的所有资源。根据分配的轮询周期（默认值为 60 秒），VPX 实例定期轮询 Azure API 并使用在 VPX GUI 中分配的标记名称和标记值检索可用的资源。每当添加或删除带有相应标记的 VM 或 NIC 时，ADC 都会检测相应的更改，并自动从服务组中添加或删除 VM 或 NIC IP 地址。



开始之前的准备工作

在创建 NetScaler 负载平衡服务组之前，请向 Azure 中的服务器添加标签。可以将标记分配给虚拟机或 NIC。



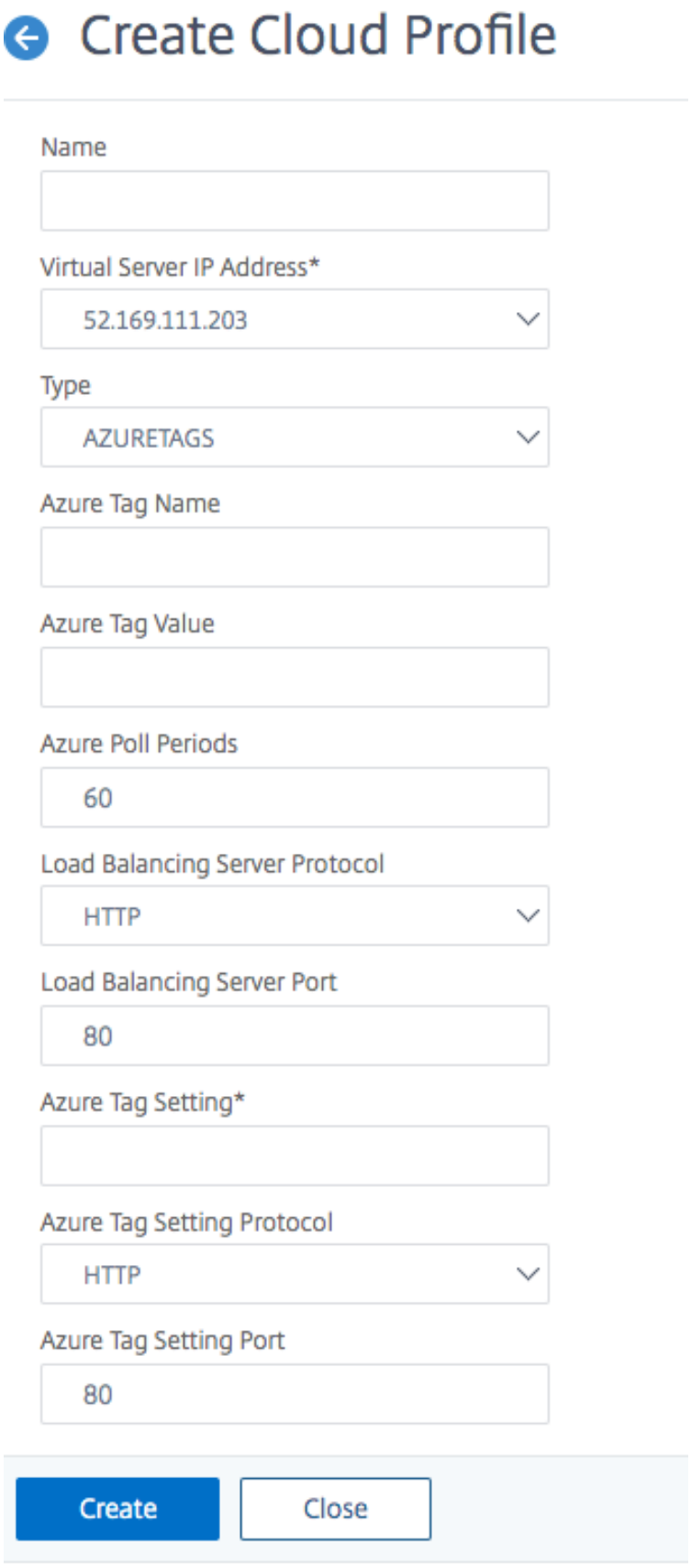
有关添加 Azure 标签的更多信息，请参阅 Microsoft 文档 使用标签来组织 Azure 资源。

> 注意：
>
> 用于添加 Azure 标签设置的 ADC CLI 命令支持仅以数字或字母开头而非其他键盘字符开头的标签名称和标签值。

如何使用 **VPX GUI** 添加 **Azure** 标记设置

可以使用 VPX GUI 将 Azure 标记云配置文件添加到 VPX 实例，以便该实例可以使用指定的标记平衡后端服务器。请按照以下步骤进行操作：

1. 从 VPX GUI 中，转到 **Configuration**（配置）**> Azure > Cloud Profile**（云配置文件）。
2. 单击“Add”（添加）创建云配置文件。此时将打开云配置文件窗口。



1. 为以下字段输入值：

   - Name（名称）：为您的配置文件添加名称
   - Virtual Server IP Address（虚拟服务器 IP 地址）：虚拟服务器 IP 地址是从 VPX 实例可用的可用 IP 地址自动填充的。有关更 多信息，请参阅使用 Azure 门户为虚拟机分配多个 IP 地址。
   - Type（类型）：从菜单中选择“AZURETAGS”。
   - Azure Tag Name（Azure 标记名称）：输入已分配给 Azure 门户中的 VM 或 NIC 的名称。
   - Azure Tag Value（Azure 标记值）：输入已分配给 Azure 门户中的 VM 或 NIC 的值。
   - Azure Poll Periods（Azure 轮询周期）：默认情况下，轮询周期为 60 秒，即最小值。可以根据您的要求进行更改。
   - Load Balancing Server Protocol（负载平衡服务器协议）：选择负载均衡器侦听的协议。
   - Load Balancing Server Port（负载平衡服务器端口）：选择负载均衡器侦听的端口。
   - Azure tag setting（Azure 标记设置）：将为此云配置文件创建的服务组的名称。
   - Azure Tag Setting Protocol（Azure 标记设置协议）：选择后端服务器侦听的协议。
   - Azure Tag Setting Port（Azure 标记设置端口）：选择后端服务器侦听的端口。

2. 单击创建。

将为带标记的 VM 或 NIC 创建负载均衡器虚拟服务器和服务组。要查看负载均衡器虚拟服务器，请从 VPX GUI 中导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。

如何使用 **VPX CLI** 添加 **Azure** 标记设置

在 NetScaler CLI 上键入以下命令为 Azure 标签创建云配置文件。

```
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：
>
> 您必须保存所有配置；否则重启实例后配置将会丢失。键入 `save config`。

示例 **1**：下面是带“myTagName/myTagValue”对标记的所有 Azure VM/NIC 的 HTTP 流量的云配置文件的命令示例：

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
   MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
   serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
    -vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue
   myTagValue -azurePollPeriod 60
Done
```


要显示云配置文件，请键入 show cloudprofile。

示例 **2**：以下 CLI 命令在示例 1 中打印有关新添加的云配置文件的信息。

```
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
```

要删除云配置文件，请键入 rm cloud profile <cloud profile name>

示例 **3**：以下命令删除在示例 1 中创建的云配置文件。

```
1   > rm cloudprofile MyTagCloudProfile
2     Done
```

故障排除

问题：在极少数情况下，“rm cloud profile” CLI 命令可能无法删除与已删除的云配置文件关联的服务组和服务器。如果在被删除的云配置文件的轮询周期过去之前发出命令，则会发生这种情况。

解决方案：通过为其余每个服务组输入以下 CLI 命令，手动删除剩余的服务组：

```
1   #> rm servicegroup <serviceGroupName>
```

还可以通过为其余每个服务器输入以下 CLI 命令来删除每个剩余的服务器：

```
1   #> rm server <name>
```

问题：如果使用 CLI 将 Azure 标记设置添加到 VPX 实例，则热重启后，rain_tag 进程将继续在高可用性对节点上运行。

解决方案：在热重启后手动终止辅助节点上的进程。从辅助高可用性节点的 CLI 退出到 shell 提示符：

```
1   #> shell
```

使用以下命令终止 rain_tag 进程：

```
1   # PID=`ps -aux | grep rain_tags | awk '{
2  print $2 }
3  '`; kill -9 $PID
```

问题：后端服务器可能无法访问，并由 VPX 实例报告为“DOWN”（关闭），尽管运行状况良好亦如此。解决方案：确保 VPX 实例可以到达与后端服务器对应的带标记的 IP 地址。对于带标记的 NIC，这是 NIC IP 地址；而对于带标记的 VM，这是 VM 的主 IP 地址。如果 VM/NIC 驻留在其他 Azure VNet 中，请确保已启用 VNet 对等。

在 **NetScaler VPX** 实例上配置 **GSLB**

October 17, 2024

针对全局服务器负载平衡 (GSLB) 配置的 NetScaler 设备通过保护 WAN 中的故障点，提供应用程序的灾难恢复和持续可用性。GSLB 可以通过将客户端请求导向到最近或性能最佳的数据中心，或者在出现中断时导向到无故障的数据中心，在数据中心之间平衡负载。

本节介绍如何使用 Windows PowerShell 命令在 Microsoft Azure 环境中两个站点上的 VPX 实例上启用 GSLB。

> 注意：
>
> 有关 GSLB 的更多信息，请参阅 全局服务器负载平衡。

您可以执行两个步骤在 Azure 上的 NetScaler VPX 实例上配置 GSLB：

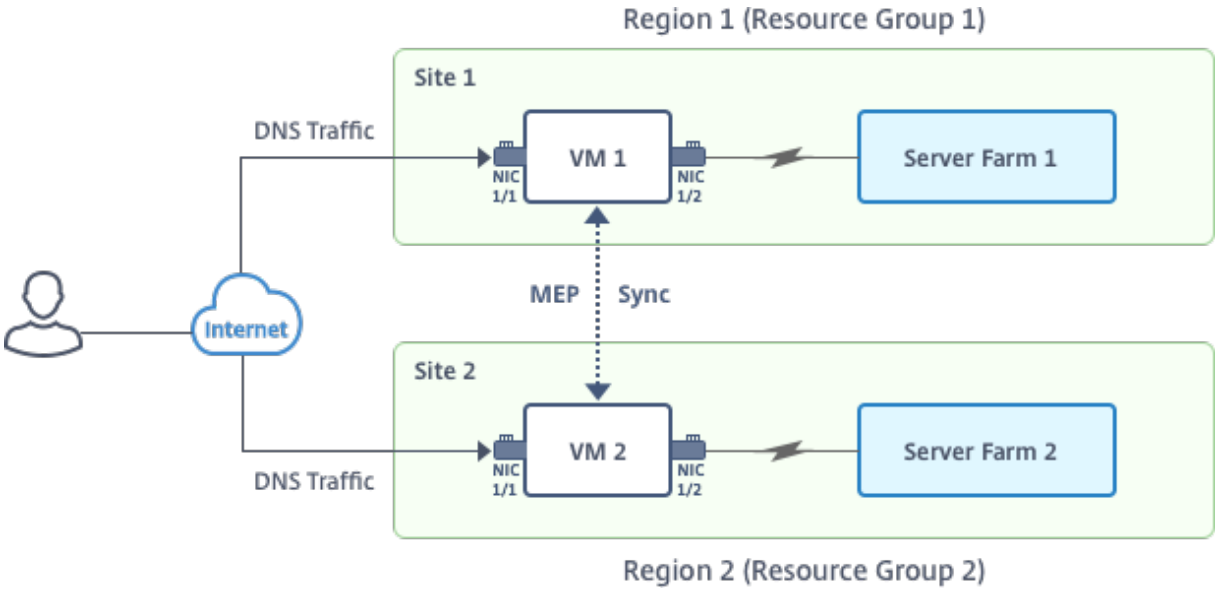
1. 在每个站点上创建一个包含多个 NIC 和多个 IP 地址的 VPX 实例。
2. 在 VPX 实例上启用 GSLB。

> 注意：
>
> 有关配置多个 NIC 和 IP 地址的更多信息，请参阅：使用 PowerShell 命令 在独立模式下为 NetScaler VPX 实例配置多个 IP 地址

场景

此场景包括两个站点 - 站点 1 和站点 2。每个站点都有一个配置了多个 NIC、多个 IP 地址和 GSLB 的 VM（VM1 和 VM2）。

图。 GSLB 设置在两个站点（站点 1 和站点 2）上实施。



在此场景中，每个 VM 都有三个 NIC - NIC 0/1、1/1 和 1/2。每个 NIC 都可以有多个专用 IP 地址和公用 IP 地址。这些 NIC 配置为用于以下用途。

- NIC 0/1：服务管理流量
- NIC 1/1：服务客户端流量
- NIC 1/2：与后端服务器通信

有关在此场景中每个网卡上配置的 IP 地址的信息，请参阅 IP 配置详细 信息部分。

参数

下面是本文档中此场景的示例参数设置。如果需要，可以使用不同的设置。

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard\_DS3\_V2"
```

> 注意：
>
> VPX 实例的最低要求是 2 个 vCPU 和 2 GB RAM。

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."
```



```
22
23    $pubIPName1="MultiIP-pip1"
24
25    $pubIPName2="MultiIP-pip2"
26
27    $IpConfigName1="IPConfig1"
28
29    $IPConfigName2="IPConfig-2"
30
31    $IPConfigName3="IPConfig-3"
32
33    $IPConfigName4="IPConfig-4"
34
35    $frontendSubnetName="default"
36
37    $backendSubnetName1="subnet\_1"
38
39    $backendSubnetName2="subnet\_2"
40
41    $suffixNumber=10
```

创建 **VM**

按照步骤 1-10 使用 PowerShell 命令创建具有多个 NIC 和多个 IP 地址的 VM1：

1. 创建资源组
2. 创建存储帐户
3. 创建可用性集
4. 创建虚拟网络
5. 创建公用 IP 地址
6. 创建 NIC
7. 创建 VM 配置对象
8. 获取凭据并为 VM 设置操作系统属性
9. 添加 NIC
10. 指定操作系统磁盘并创建 VM

完成创建 VM1 的所有步骤和命令后，重复执行这些步骤来创建 VM2 并为其设置特定参数。

创建资源组

```
1    New-AzureRMResourceGroup -Name $RGName -Location $location
```


创建存储帐户

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

创建可用性集

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

创建虚拟网络

1. 添加子网。

```
$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. 添加虚拟网络对象。

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

3. 检索子网。

```
 $frontendSubnet=$vnet.Subnets|?{
$_.Name -eq $frontendSubnetName }

 $backendSubnet1=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName1 }

 $backendSubnet2=$vnet.Subnets|?{
$_.Name -eq $backendSubnetName2 }
```

创建公用 **IP** 地址

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
```


创建 **NIC**

创建 NIC 0/1

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -
    PrivateIpAddress $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
```

创建 NIC 1/1

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2,
    $IpConfig3
```

创建 NIC 1/2

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
```

创建 **VM** 配置对象

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
```

获取凭据并设置操作系统属性

```
$cred=Get-Credential -Message "Type the name and password for VPX
    login."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
```


添加 **NIC**

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
```

指定操作系统磁盘并创建 **VM**

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds
    /" +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
     $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
     -Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
```

> 注意：
>
> 重复执行“使用 PowerShell 命令创建多 NIC VM”中列出的步骤 1-10 来创建 VM2 并为其设置特定参数。

IP 配置详细信息

使用以下 IP 地址。

表 **1**。VM1 中使用的 IP 地址

NIC	专用 IP	公用 IP (PIP)	说明
0/1	10.0.0.10	PIP1	配置为 NSIP（管理 IP）
1/1	10.0.1.10	PIP2	配置为 SNIP/GSLB 站点 IP
-	10.0.1.11	-	配置为 LB 服务器 IP。公用 IP 不是必需的
1/2	10.0.2.10	-	配置为 SNIP 以用于向服务发送监视探测；公用 IP 不是必需的

表 **2.** VM2 中使用的 IP 地址

NIC	内部 IP	公用 IP (PIP)	说明
0/1	20.0.0.10	PIP4	配置为 NSIP（管理 IP）
1/1	20.0.1.10	PIP5	配置为 SNIP/GSLB 站点 IP
-	20.0.1.11	-	配置为 LB 服务器 IP。公用 IP 不是必需的
1/2	20.0.2.10	-	配置为 SNIP 以用于向服务发送监视探测；公用 IP 不是必需的

以下是此场景的示例配置，显示了通过 NetScaler VPX CLI 为 VM1 和 VM2 创建的 IP 地址和初始 LB 配置。

下面是 VM1 上的一个确认示例。

```
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]
```

下面是 VM2 上的一个确认示例。

```
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]
```

配置 **GSLB** 站点和其他设置

执行以下主题中所述任务来配置两个 GSLB 站点和其他必要设置：

全局服务器负载平衡

下面是 VM1 和 VM2 上的 GSLB 确认示例。

```
1   enable ns feature LB GSLB
2   add gslb site site1 10.0.1.10 -publicIP PIP2
3   add gslb site site2 20.0.1.10 -publicIP PIP5
4   add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP
       PIP3 -publicPort 80 -siteName site1
```



```
5   add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP
       PIP6 -publicPort 80 -siteName site2
6   add gslb vserver gslb_http_vip1 HTTP
7   bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
8   bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
9   bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

您已在 Azure 上运行的 NetScaler VPX 实例上配置 GSLB。

灾难恢复

灾害是由自然灾害或人为事件引起的业务功能突然中断。灾难会影响数据中心的运营，之后必须完全重建和恢复灾难现场丢失的资源和数据。数据中心中的数据丢失或停机至关重要，并使业务连续性崩溃。

如今，客户面临的挑战之一是决定将灾难恢复站点放置在何处。无论任何底层基础架构或网络故障如何，企业都在寻求一致性和性能。

许多组织决定迁移到云的可能原因是：

- 拥有本地数据中心非常昂贵。通过使用云端，企业可以腾出时间和资源来扩展自己的系统。
- 许多自动编排可以实现更快的恢复
- 通过提供持续的数据保护或连续快照来复制数据，以防范任何中断或攻击。
- 支持客户需要许多不同类型的合规性和安全控制的用例，这些合规性和安全控制已经存在于公共云上。这些使他们更容易实现所需的合规性，而不是建立自己的合规性。

为 GSLB 配置的 NetScaler 将流量转发到负载最少或性能最佳的数据中心。此配置称为主动-主动安装程序，不仅可以提高性能，而且可以通过将流量路由到其他数据中心（如果属于安装程序的一部分的数据中心）提供即时灾难恢复。因此，NetScaler 为客户节省了宝贵的时间和金钱。

用于灾难恢复的多 **NIC** 多 **IP**（三 **NIC**）部署

如果客户要部署到安全性、冗余、可用性、容量和可扩展性至关重要的生产环境中，他们可能会使用三个 NIC 部署进行部署。使用这种部署方法，复杂性和易管理性并不是用户最关心的问题。

用于灾难恢复的单网卡多 **IP**（一个 **NIC**）部署

如果客户出于以下原因部署到非生产环境中，他们可能会使用单网卡部署进行部署：

- 设置环境进行测试，或者他们在生产部署之前暂存新环境。
- 快速高效地直接部署到云端。
- 在寻求单一子网配置的简单性的同时。

在主动-备用高可用性设置中配置 **GSLB**

October 17, 2024

可以通过三个步骤在 Azure 上的主动-备用高可用性部署中配置全局服务器负载平衡 (GSLB)：

1. 在每个 GSLB 站点上创建一个 VPX 高可用性对。有关如何创建 HA 对的信息，请参阅 使用多个 IP 地址和 NIC 配置高可用性设置 。
2. 使用前端 IP 地址和规则配置 Azure 负载均衡器 (ALB)，以允许传输 GSLB 和 DNS 流量。

   此步骤涉及以下子步骤。请参阅本部分中的场景，了解用于完成这些子步骤的 PowerShell 命令。

   a。a. 为 GSLB 站点创建一个前端 `IPconfig`。

   a。b. 创建一个后端地址池，其 IP 地址为高可用性中的节点的 NIC 1/1。

   a。c. 为以下对象创建负载平衡规则：

   ```
   TCP/3009  -  gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

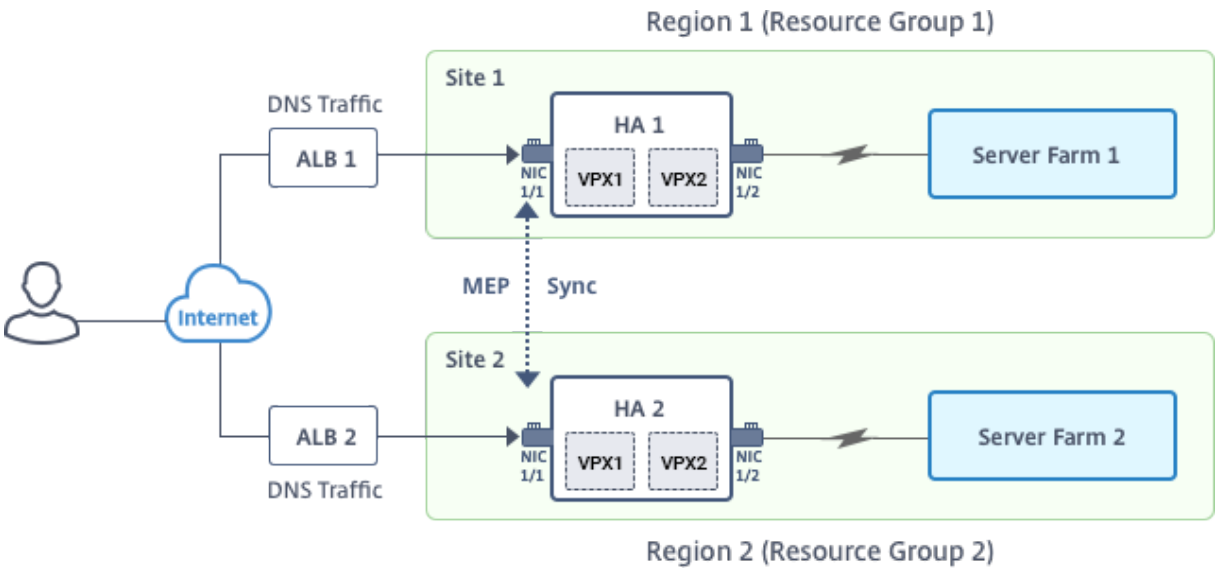
   d. d. 将后端地址池与在步骤 c 中创建的 LB 规则相关联。

   e. e. 更新两个 HA 对中节点的 NIC 1/1 的网络安全组，以允许 TCP 3008、TCP 3009 和 UDP 53 端口的流量。
3. 在每个高可用性对上启用 GSLB。

场景

此场景包括两个站点 - 站点 1 和站点 2。每个站点都有一个配置了多个 NIC、多个 IP 地址和 GSLB 的高可用性对（HA1 和 HA2）。

图： Azure 上主动-备用高可用性部署中的 GLSB



在此场景中，每个 VM 都有三个 NIC - NIC 0/1、1/1 和 1/2。这些 NIC 配置为用于以下用途。

NIC 0/1：服务管理流量

NIC 1/1：服务客户端流量

NIC 1/2：与后端服务器通信

参数设置

下面是 ALB 的示例参数设置。如果需要，可以使用不同的设置。

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"

$lbRuleName3="LBRuleGSLB2"

$lbRuleName4="LBRuleDNS"

$healthProbeName="HealthProbe"
```


使用前端 **IP** 地址和规则配置 **ALB** 以允许传输 **GSLB** 和 **DNS** 流量

步骤 1. 步骤 1. 为 **GSLB** 站点 **IP** 创建公用 **IP**

```
$pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
    $rgName -DomainNameLabel $domName4 -Location $locName -
    AllocationMethod Dynamic


Get-AzureRmLoadBalancer -Name \$lbName -ResourceGroupName \$rgName |
    Add-AzureRmLoadBalancerFrontendIpConfig -Name \
    $frontEndConfigName2 -PublicIpAddress \$pip4 | Set-
    AzureRmLoadBalancer
```

步骤 2. 步骤 2. 创建 **LB** 规则并更新现有 **ALB**。

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName


$frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2


$backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1


$healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName


\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName2 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3009 -
    BackendPort 3009 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName3 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Tcp\" -FrontendPort 3008 -
    BackendPort 3008 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


\$alb | Add-AzureRmLoadBalancerRuleConfig -Name \$lbRuleName4 -
    BackendAddressPool \$backendPool -FrontendIPConfiguration  \
    $frontendipconfig2 -Protocol \"Udp\" -FrontendPort 53 -BackendPort
     53 -Probe \$healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
```


在每个高可用性对上启用 **GSLB**

现在，每个 ALB 都有两个前端 IP 地址：ALB 1 和 ALB 2。一个 IP 地址用于 LB 虚拟服务器，另一个用于 GSLB 站点 IP。

HA 1 具有以下前端 IP 地址：

- FrontEndIPofALB1 （适用于 LB 虚拟服务器）
- PIPFORGSLB1 (GSLB IP)

HA 2 具有以下前端 IP 地址：

- FrontEndIPofALB2 （适用于 LB 虚拟服务器）
- PIPFORGSLB2 (GSLB IP)

以下命令用于此场景。

```
enable ns feature LB GSLB

add service dnssvc PIPFORGSLB1 ADNS 53

add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1

add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2

add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
   publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
   publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

相关资源：

在 NetScaler VPX 实例上配置 GSLB

全局服务器负载平衡

在 **Azure** 上部署 **NetScaler GSLB**

October 17, 2024

随着需求的增长，运营本地数据中心为区域客户服务的企业希望使用 Azure 云在全球范围内进行扩展和部署。有了 NetScaler 站在网络管理员一边，您可以使用 GSLB 样书在本地和云端配置应用程序。您可以使用 NetScaler ADM 将相同的配置传输到云端。根据与 GSLB 的距离，您可以访问本地资源或云资源。无论您身在世界何处，都可以获得无缝体验。

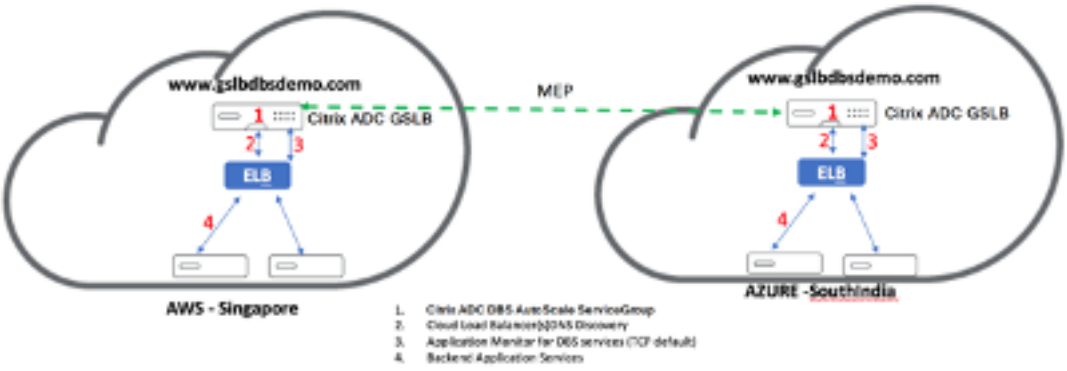
DBS 概述

NetScaler GSLB 支持将基于域的服务 (DBS) 用于云负载平衡器。这允许使用云负载平衡器解决方案自动发现动态云服务。此配置允许 NetScaler 在 Active-Active 环境中实现 GSLB DBS。DBS 允许从 DNS 发现中缩放 Microsoft Azure 环境中的后端资源。本节介绍了 Azure AutoScale 环境中 NetScaler 之间的集成。

使用 Azure 负载平衡器 (ALB) 的基于域名的服务

GLSB DBS 利用用户 ALB 的 FQDN 动态更新 GSLB 服务组，以包括在 Azure 中创建和删除的后端服务器。要配置此功能，用户将 Citrix ADC 指向其 ALB 以动态路由到 Azure 中的不同服务器。他们可以执行此操作，而不必在每次在 Azure 中创建和删除实例时手动更新 Citrix ADC。适用于 GSLB 服务组的 Citrix ADC DBS 功能使用 DNS 感知服务发现来确定 AutoScale 组中识别的 DBS 命名空间的成员服务资源。

下图描绘了带有云负载平衡器的 NetScaler GSLB DBS AutoScale 组件：



Azure GSLB 必备条件

NetScaler GSLB 服务组的先决条件包括具有配置安全组知识和能力的正常运行的 Microsoft Azure 环境、Linux Web 服务器、AWS 中的 NetScaler 设备、弹性 IP 和弹性负载平衡器 (ELB)。

- GSLB DBS 服务集成需要 NetScaler 版本 12.0.57 用于 Microsoft Azure 负载平衡器实例。
- GSLB 服务组实体：NetScaler 版本 12.0.57。
- 引入了 GSLB 服务组，该组支持使用 DBS 动态发现进行自动扩展。
- DBS 功能组件（基于域的服务）必须绑定到 GSLB 服务组。

Example:

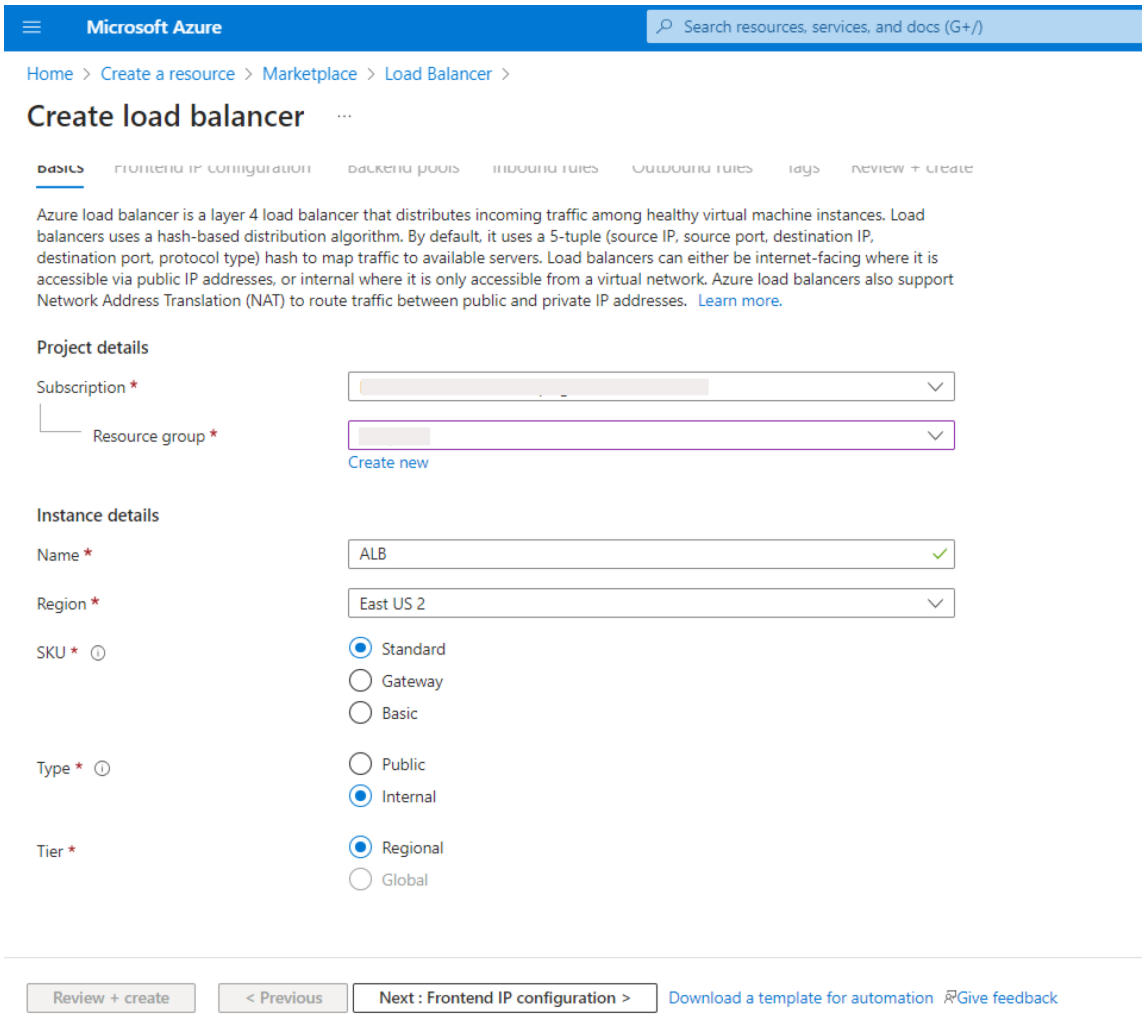
```
```

    > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.amazonaws.com
    > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney
    > bind gslb serviceGroup sydney_sg sydney_server 80

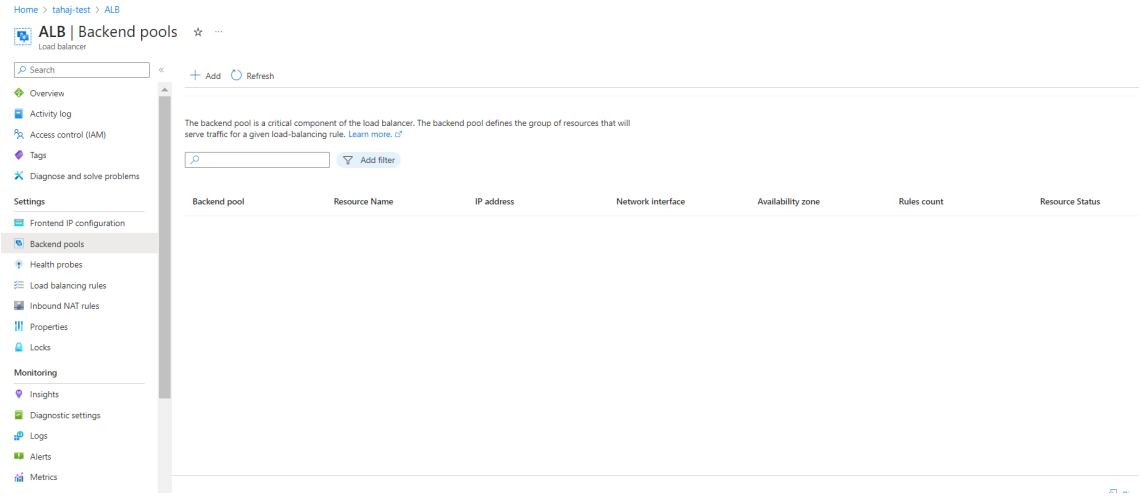
```
```

配置 **Azure** 组件

1. 登录到用户 Azure 门户并通过 NetScaler 模板创建新的虚拟机。
2. 创建 Azure 负载平衡器。



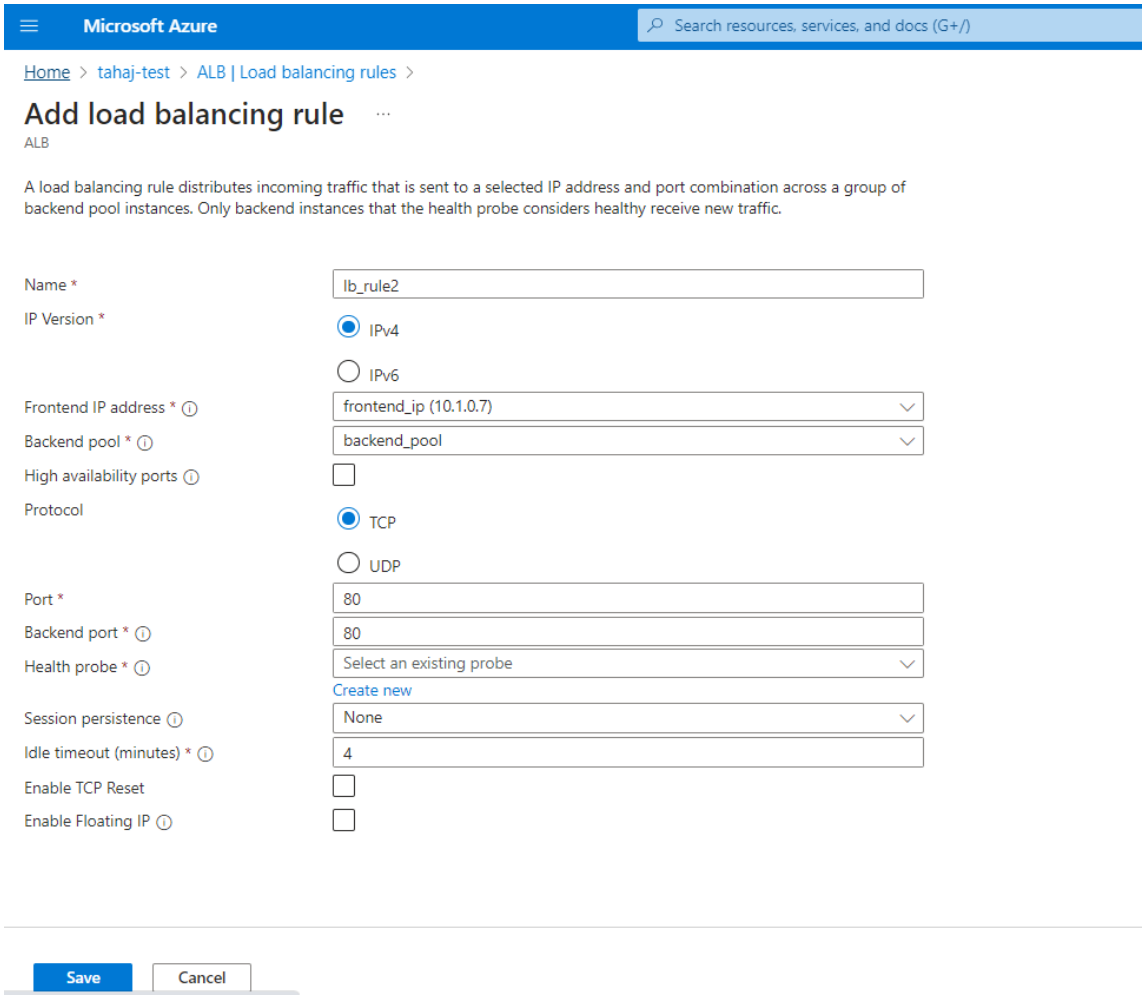
3. 添加创建的 NetScaler 后端池。



4. 为端口 80 创建运行状况探测器。

   使用从负载平衡器创建的前端 IP 创建负载平衡规则。

   - 协议：TCP
   - 后端端口：80
   - 后端池：在步骤 1 中创建的 NetScaler
   - 运行状况探测：在步骤 4 中创建
   - 会话持续性：无



配置 **NetScaler GSLB** 基于域的服务

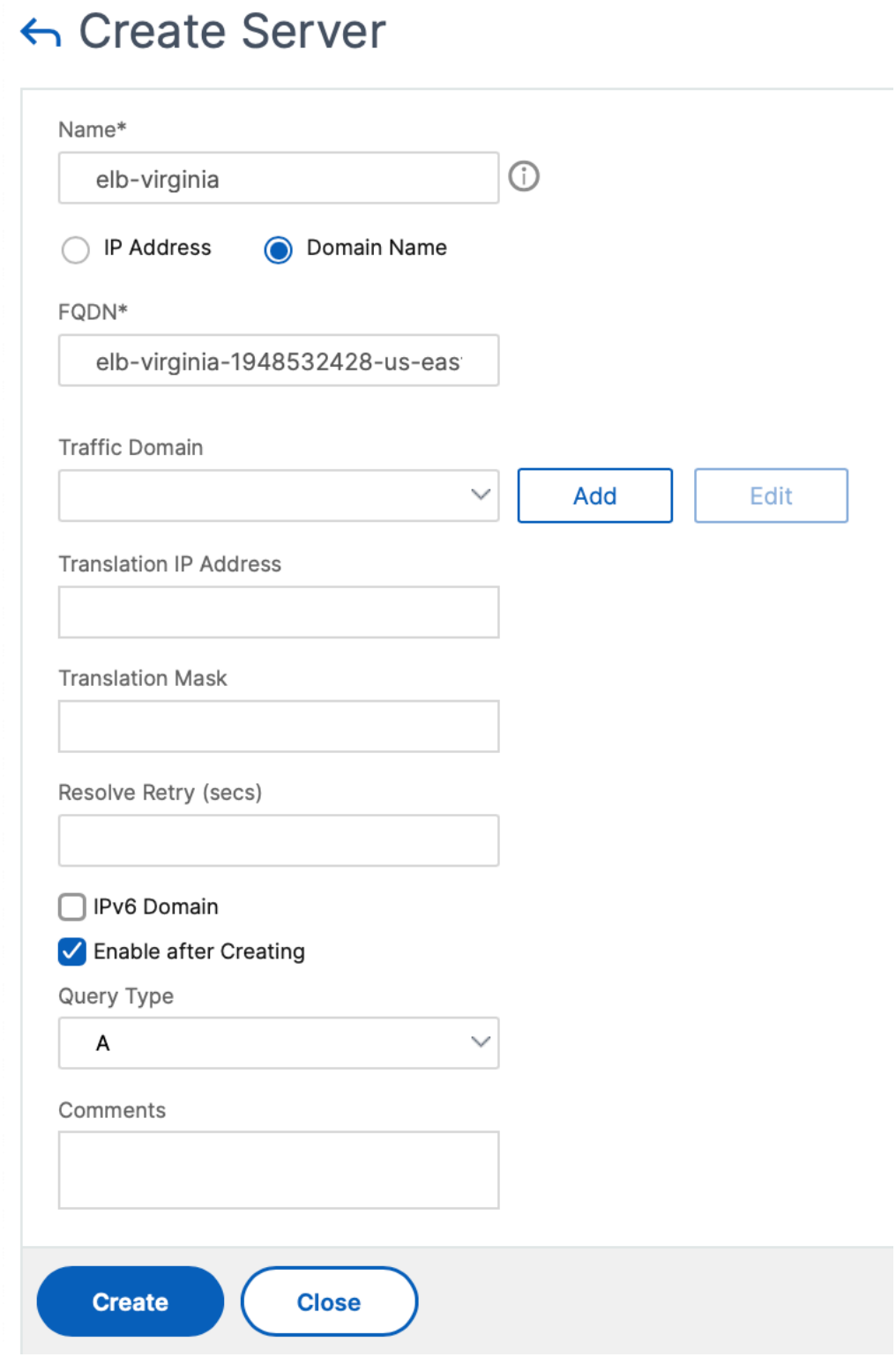
以下配置总结了在启用 GSLB 的环境中为自动扩展 ADC 启用基于域的服务所需的条件。

- 流量管理配置
- GSLB 配置

流量管理配置

> 注意：
>
> 必须使用域名服务器或 DNS 虚拟服务器配置 NetScaler，通过这些服务器为星展银行服务组解析 ELB /ALB 域。有关域名服务器或 DNS 虚拟服务器的更多信息，请参阅：DNS nameServer

1. 导航到“流量管理”**>**“负载平衡”**>**“服务器”。
2. 单击“添加”创建服务器，提供与 Azure 中 ALB 的 A 记录（域名）对应的名称和 FQDN。



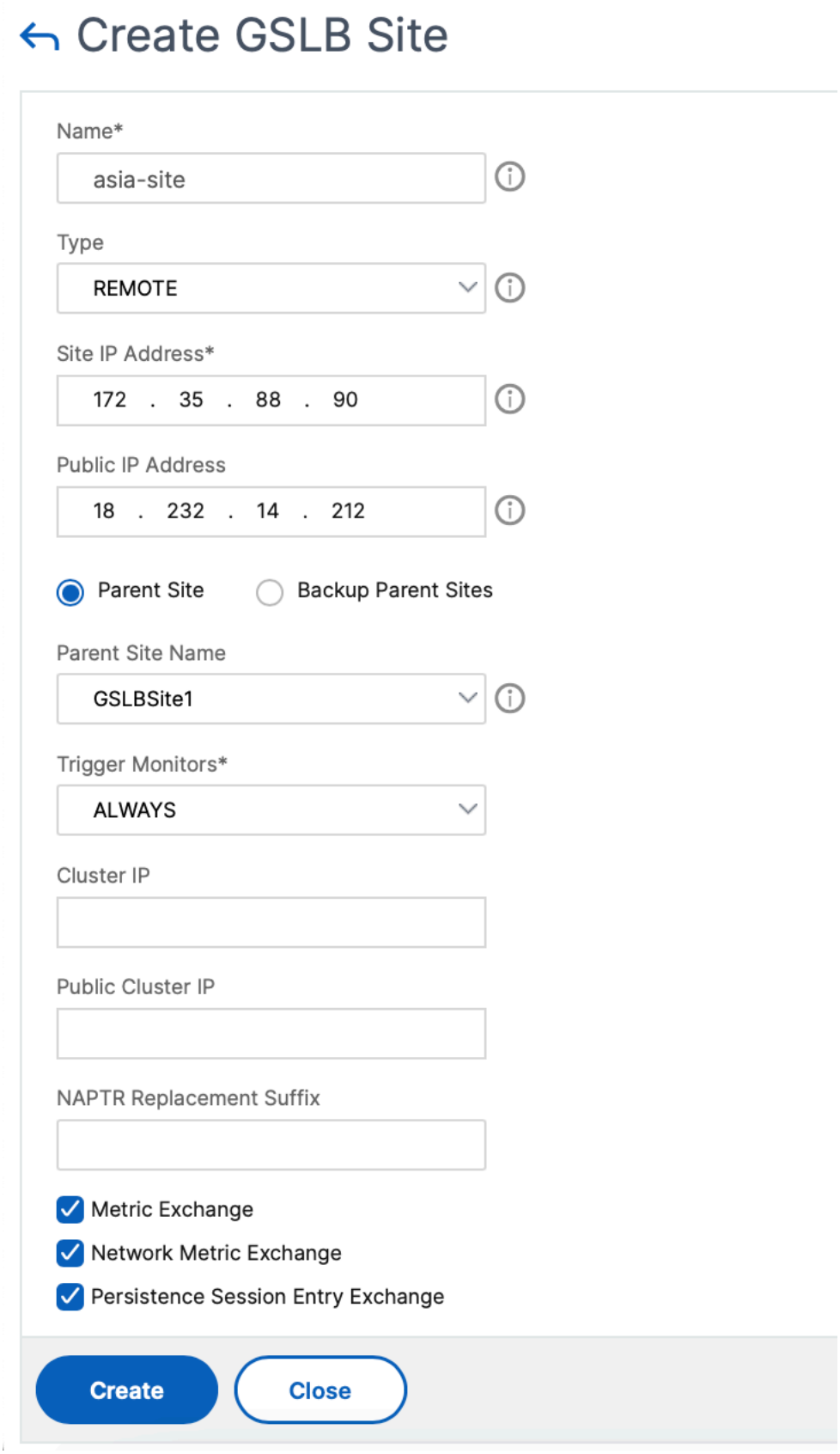
3. 重复步骤 2 以从 Azure 中的第二个资源添加第二个 ALB。

GSLB 配置

1. 单击 添加以配置 GSLB 站点。
2. 指定配置 GSLB 站点的详细信息

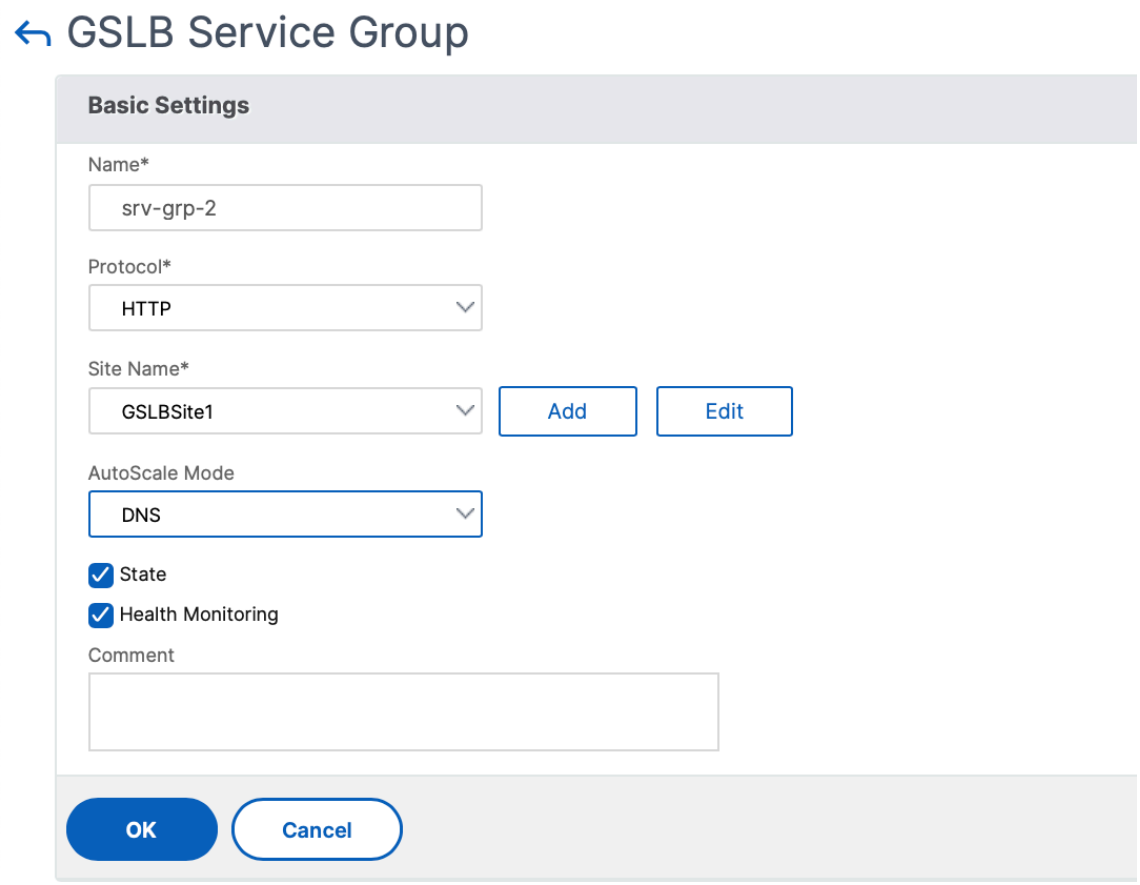
   命名该网站。根据您在哪个 NetScaler 上配置站点，将类型配置为远程或本地。站点 IP 地址是 GSLB 站点的 IP 地址。GSLB 站点使用此 IP 地址与其他 GSLB 站点通信。使用云服务时，如果特定 IP 地址托管在外部防火墙或 NAT 设备上，则需要公有 IP 地址。应将该站点配置为父站点。确保将“触发监视器”设置为“始终”。另外，请务必选中底部的三个复选框，分别是“指标交换”、“网络指标交换”和“持久性会话条目交换”。

   我们建议您将 触发监视 器设置为 **MEPDOWN**。有关更多信息，请参阅配置 GSLB 服务组。

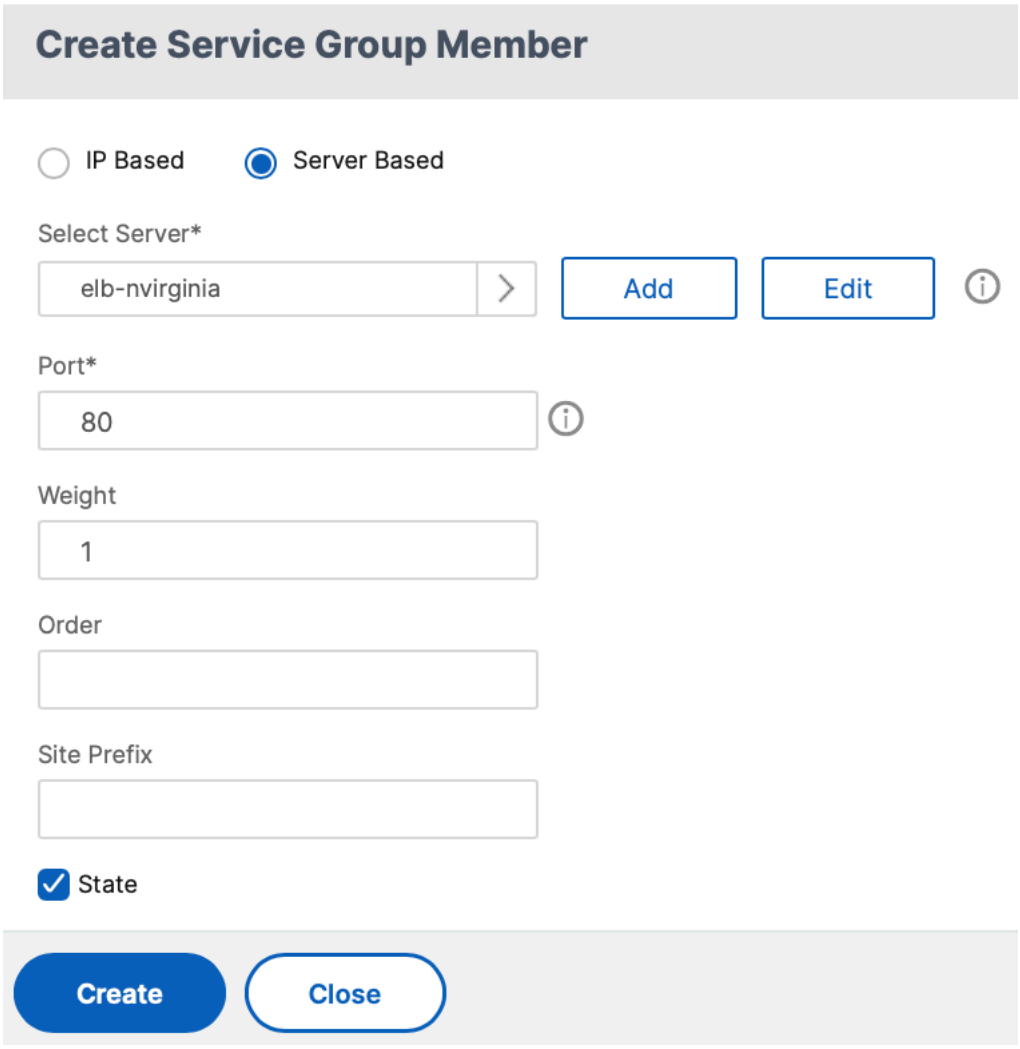


3. 单击创建。
4. 导航到流量管理 **> GSLB >** 服务组。
5. 单击“添加”以添加服务组。
6. 指定配置服务组的详细信息

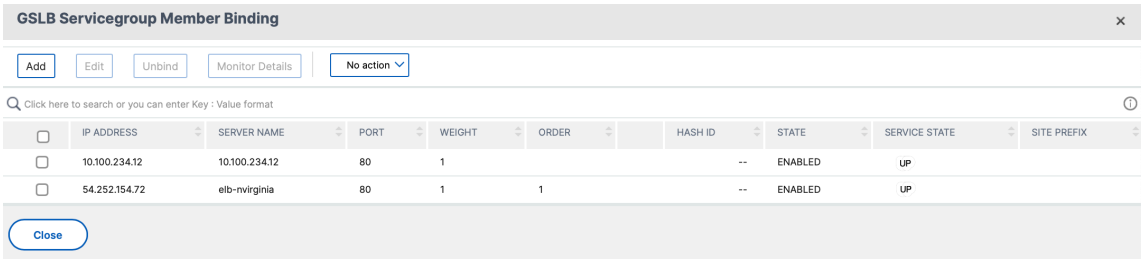
   命名服务组，使用 HTTP 协议。在“站点名称”下，选择您创建的相应站点。请务必将 AutoScale 模式配置为 DNS，并勾选“状态”和“运行状况监视”对应的复选框。单击“确定”创建服务组。



7. 单击服务组成员，然后选择基于服务器。选择在运行指南开头部分配置的相应的 ELB。将流量配置为通过端口 80。单击创建。

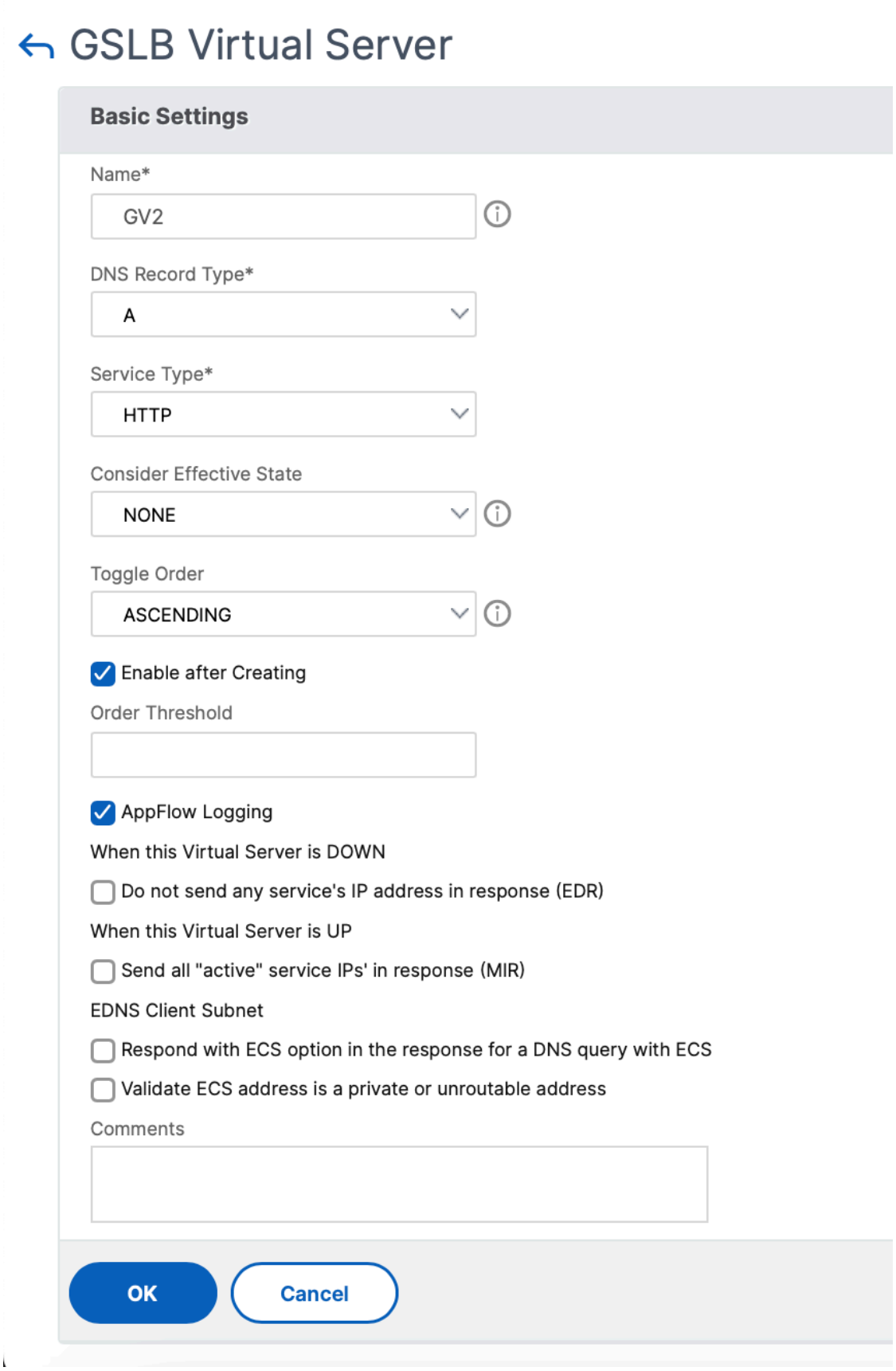


服务组成员绑定应填充从 ELB 接收的 2 个实例。

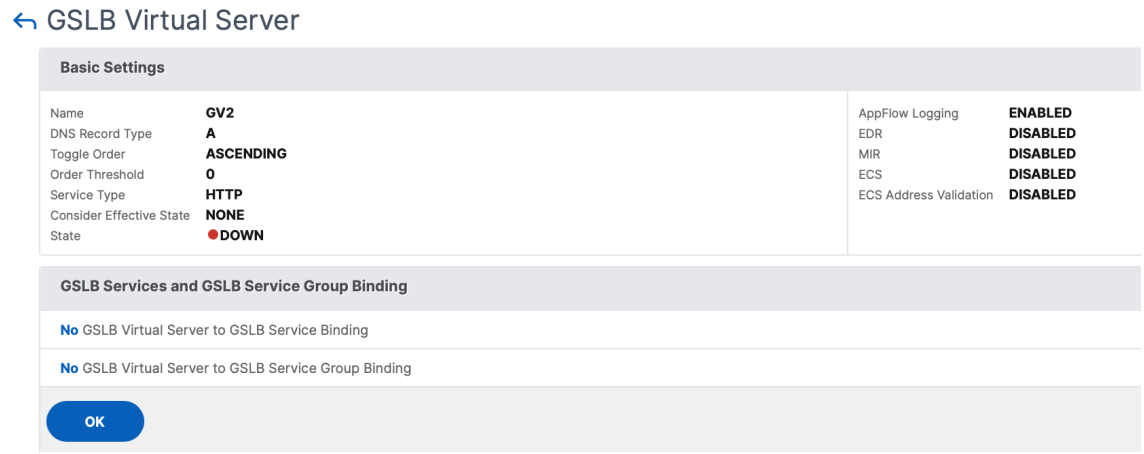


8. 重复步骤 5 和 6，为 Azure 中的第二个资源位置配置服务组。（这可以通过相同的 NetScaler GUI 来完成）。
9. 设置 GSLB 虚拟服务器。导航到流量管理 **> GSLB >** 虚拟服务器。
10. 单击“添加”以创建虚拟服务器。
11. 指定配置 GSLB 虚拟服务器的详细信息。

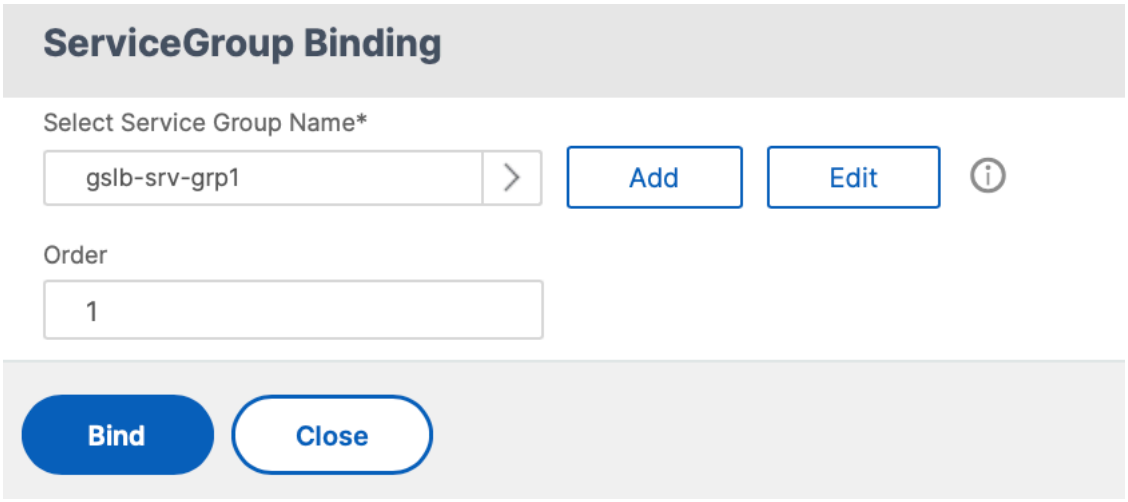
    命名服务器，将 DNS 记录类型设置为 A，服务类型设置为 HTTP，并选中“创建后启用”和“AppFlow 日志记录”复选框。单击“确定”创建 GSLB 虚拟服务器。



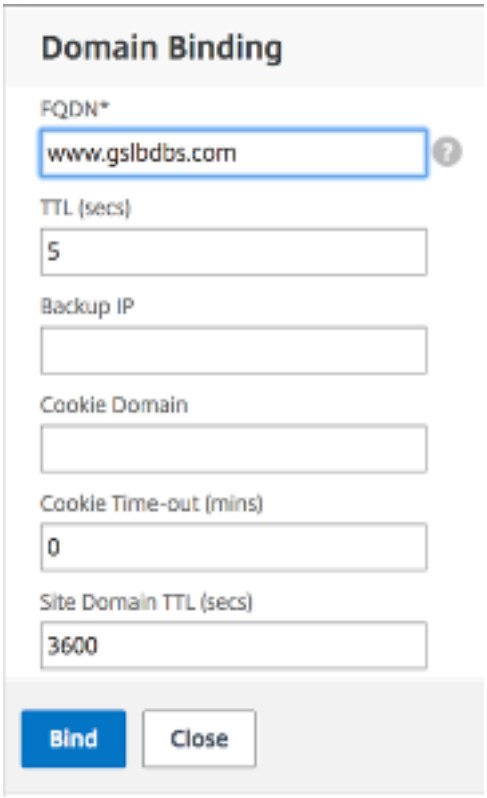
12. 创建 GSLB 虚拟服务器后，单击“无 **GSLB** 虚拟服务器服务组绑定”。



13. 在 **ServiceGroup** 绑定 下，使用选择服务组名 称来选择和添加在前面的步骤中创建的服务组。

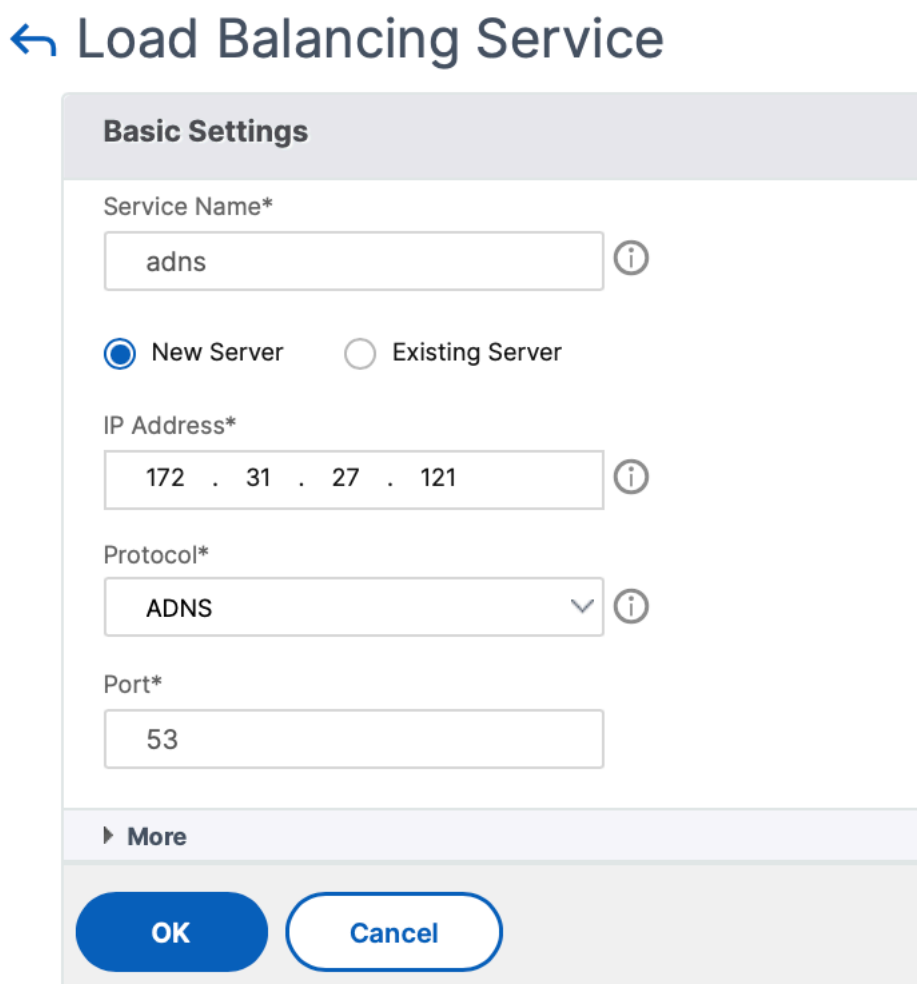


14. 单击“无 **GSLB** 虚拟服务器域绑定”配置 GSLB 虚拟服务器域绑定。配置 FQDN 并绑定。保留其他参数的默认设置。



15. 单击“无服务”配置 **ADNS** 服务。
16. 指定配置负载平衡服务的详细信息。

    添加 服务名，单击“新建服务器”，然后输入 ADNS 服务器 的 **IP** 地址。如果已经配置了用户 ADNS，则用户可以选择“现有服务器”，然后从下拉菜单中选择用户 ADNS。确保协议为 ADNS 且流量配置为流经端口 53。



17. 将 方法 配置为 最少连接，将备份方法配置为 循环。
18. 单击“完成”，验证用户 GSLB 虚拟服务器是否显示为 Up。

其他资源

面向混合和多云部署的 NetScaler 全局负载平衡

为 **NetScaler Gateway** 设备配置地址池内联网 **IP**

October 17, 2024

在某些情况下，连接 NetScaler Gateway 插件的用户需要 NetScaler Gateway 设备的唯一 IP 地址。当您为组启用地址池（也称为 IP 池）时，NetScaler Gateway 设备可以为每个用户分配一个唯一的 IP 地址别名。应使用 Intranet IP (IIP) 地址配置地址池。

您可以按照以下两步过程在部署在 Azure 上的 NetScaler Gateway 设备上配置地址池：

- 在 Azure 中，注册用于地址池的专用 IP 地址
- 在 NetScaler Gateway 设备中配置地址池

在 **Azure** 门户中注册专用 **IP** 地址

在 Azure 中，您可以部署具有多个 IP 地址的 NetScaler VPX 实例。可以采用两种方式将 IP 地址添加到 VPX 实例：

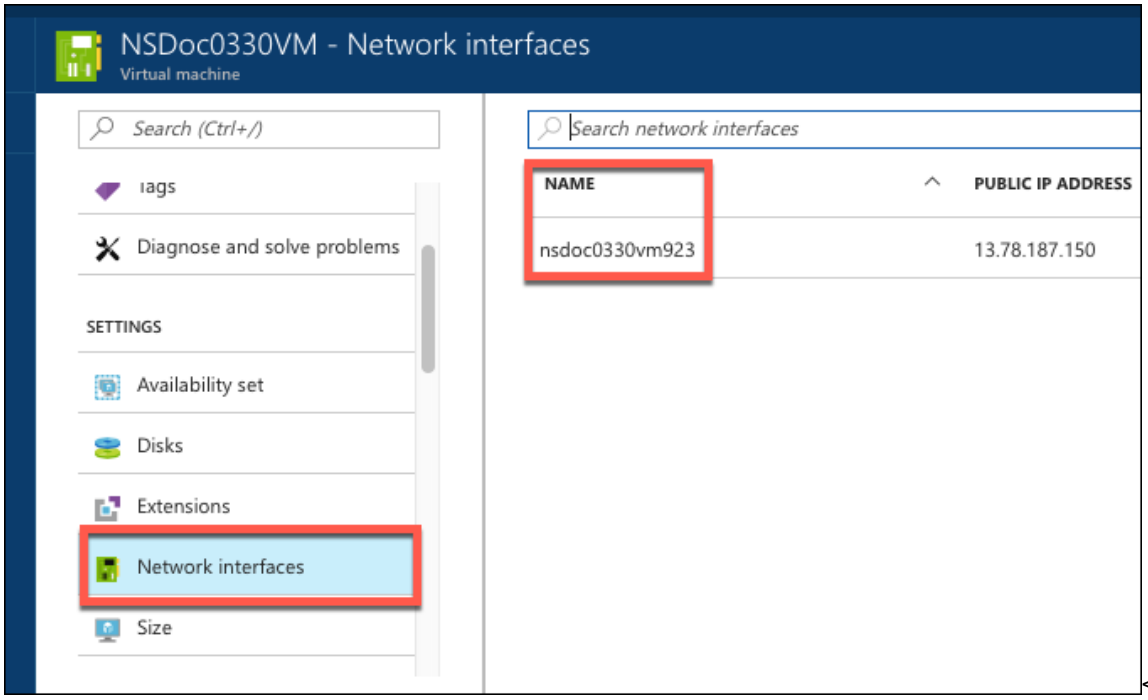
a。a. 置备 VPX 实例时

有关如何在配置 VPX 实例时添加多个 IP 地址的更多信息，请参阅 为 NetScaler 独立实例配置多个 IP 地址。要在配置 VPX 实例时使用 PowerShell 命令添加 IP 地址，请参阅 使用 PowerShell 命令为独立模式下的 NetScaler VPX 实例配置多个 IP 地址。

a。b. 置备 VPX 实例后

配置 VPX 实例后，按照以下步骤在 Azure 门户中注册专用 IP 地址，在 NetScaler Gateway 设备中将其配置为地址池。

1. ** 在 Azure Resource Manager (ARM) 中，转到已经创建的 NetScaler VPX 实例 > 网络接口。选择绑定到您要注册的 IIP 所属的子网的网络接口。</p>



1

单击 **IP Configurations**（IP 配置），然后单击 **Add**（添加）。

```
1 ![IP 配置 IIP](/en-us/vpx/media/ip-configuration-iip.png)
```

1

按照下面的示例中所示提供所需详细信息，然后单击 **OK**（确定）。

```
1 ![详细信息 IIP](/en-us/vpx/media/details-iip.png)</ol>
```

在 **NetScaler Gateway** 设备中配置地址池

有关如何在 NetScaler Gateway 上配置地址池的详细信息，请参阅 配置地址池。

> 限制：
>
> 您不能将 IIP 地址范围绑定到用户。必须注册地址池中使用的每个 IIP 地址。

使用 **PowerShell** 命令为 **NetScaler VPX** 独立实例配置多个 **IP** 地址

October 17, 2024

在 Azure 环境中，可以为 NetScaler VPX 虚拟设备部署多个 NIC。每个 NIC 都可以有多个 IP 地址。本节介绍如何使用 PowerShell 命令部署具有单个 NIC 和多个 IP 地址的 NetScaler VPX 实例。您可以将同一脚本用于多 NIC 和多 IP 部署。

> 注意：
>
> 在本文档中，IP-Config 是指与单个 NIC 关联的一对 IP 地址（公用 IP 和专用 IP）。有关更多信息，请参阅 Azure 术语 部分。

用例

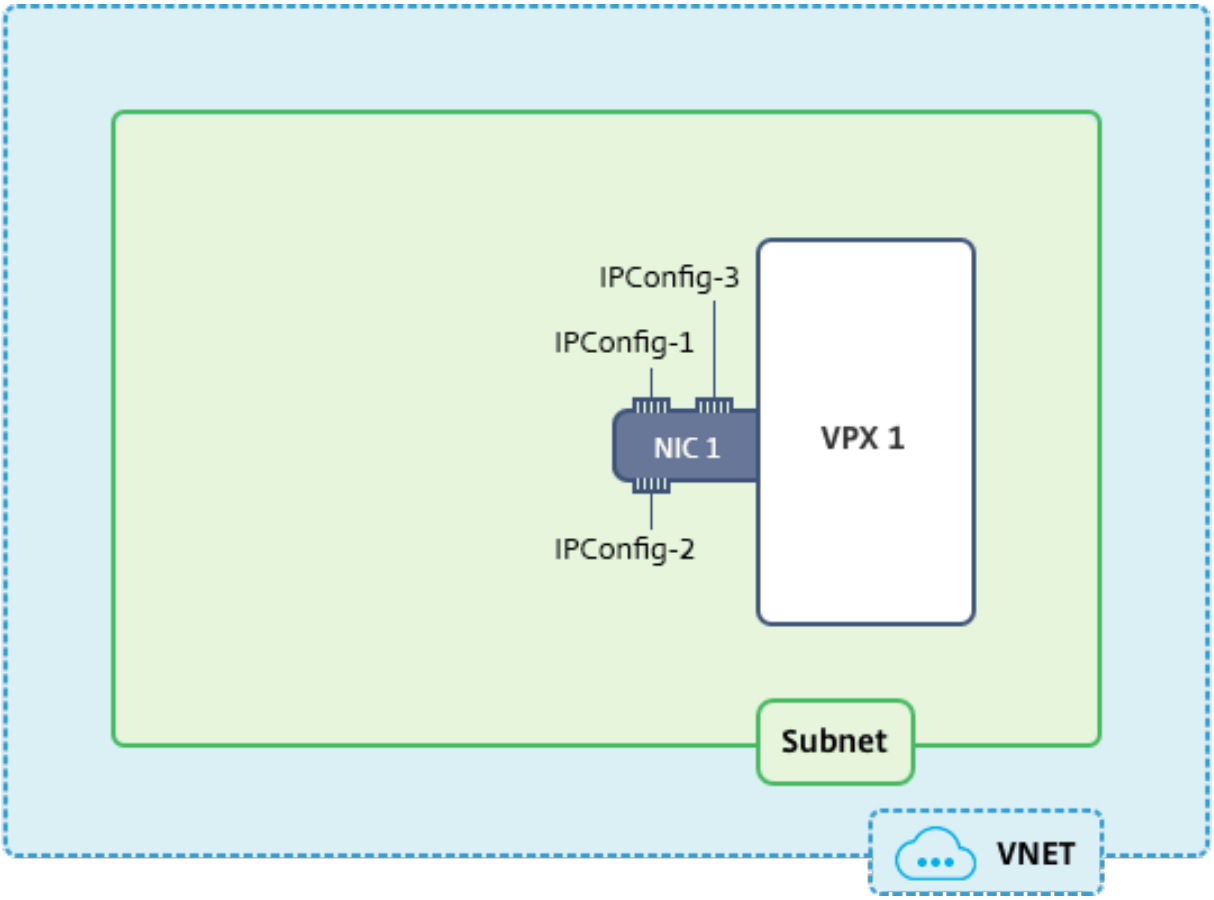
在此用例中，一个 NIC 连接到虚拟网络 (VNET)。该 NIC 与三个 IP 配置相关联，如下表中所示。

IP 配置	关联到
IPConfig-1	静态公用 IP 地址；静态专用 IP 地址
IPConfig-2	静态公用 IP 地址；静态专用地址
IPConfig-3	静态专用 IP 地址

> 注意：
>
> IPConfig-3 不与任何公用 IP 地址相关联。

示意图：拓扑

以下是用例的直观表示。



> 注意：
>
> 在多 NIC、多 IP Azure NetScaler VPX 部署中，与主（第一个）网卡的主要（第一个）`IPConfig` 关联的专用 IP 地址会自动添加为设备的管理 NSIP 地址。而与 `IPConfigs` 关联的其余专用 IP 地址，必须使用 `add ns ip` 命令作为 VIP 或 SNIP 添加到 VPX 实例中，具体取决于您的要求。

下面总结了为处于独立模式的 NetScaler VPX 虚拟设备配置多个 IP 地址所需的步骤：

1. 创建资源组
2. 创建存储帐户
3. 创建可用性集
4. 创建网络服务组
5. 创建虚拟网络
6. 创建公用 IP 地址
7. 分配 IP 配置
8. 创建 NIC
9. 创建 NetScaler VPX 实例
10. 检查 NIC 配置
11. 检查 VPX 端配置

脚本

参数

下面是本文档中用例的示例参数设置。如果需要，可以使用不同的设置。

$locName=”westcentralus”

$rgName=”Azure-MultiIP”

$nicName1=”VM1-NIC1”

$vNetName=”Azure-MultiIP-vnet”

$vNetAddressRange=”11.6.0.0/16”

$frontEndSubnetName=”frontEndSubnet”

$frontEndSubnetRange=”11.6.1.0/24”

$prmStorageAccountName=”multiipstorage”

$avSetName=”multiip-avSet”

$vmSize=”Standard_DS4_V2”（此参数会创建最多具有 4 个 NIC 的 VM。）

注意：一个 VPX 实例的最低要求是 2 个 vCPU 和 2 GB RAM。

$publisher=”Citrix”

$offer=”netscalervpx110-6531”（您可以使用不同的 offer。）

$sku=”netscalerbyol”（根据您的 offer，SKU 可以不同。）

$version=”latest”

$pubIPName1=”PIP1”

$pubIPName2=”PIP2”

$domName1=”multiipvpx1”

$domName2=”multiipvpx2”

$vmNamePrefix=”VPXMultiIP”

$osDiskSuffix=”osmultiipalbdiskdb1”

网络安全组 **(NSG)** 相关的信息：

$nsgName=”NSG-MultiIP”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=” IPConfig1”

$IPConfigName2=” IPConfig-2”

$IPConfigName3=” IPConfig-3”

1. 创建资源组

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. 创建存储帐户

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. 创建可用性集

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
 $rgName -Location $locName
```

4. 创建网络安全组

1. 添加规则。对于任何提供流量的端口，您必须向网络安全组中添加规则。

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -名称 $rule1Name -描述
    “允许 HTTP” -访问允许 -协议 Tcp -方向入站 -优先级 101 -SourceAddressPrefix
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortR
    80 $rule2=New-AzureRmNetworkSecurityRuleConfig -名称 $rule2Name -
   描述“允许 HTTPS” -访问允许 -协议 Tcp -方向入站 -优先级 110 -SourceAddressPrefix
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortR
    443 $rule3=New-AzureRmNetworkSecurityRuleConfig -名称 $rule3Name -
   描述“允许 SSH” -访问允许 -协议 Tcp -方向入站 -优先级 120 -SourceAddressPrefix
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortR
    22
   ```

2. 创建网络安全组对象。

   ```
   $nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName
   -Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,
   $rule3
   ```


5. 创建虚拟网络

1. 添加子网。

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$frontEndSubnetName -AddressPrefix $frontEndSubnetRange
```

2. 添加虚拟网络对象。

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
 $rgName -Location $locName -AddressPrefix $vNetAddressRange -
Subnet $frontendSubnet
```

3. 检索子网。

```
$subnetName="frontEndSubnet"    $subnet1=$vnet.子网|?{ $_.Name -eq
$subnetName }
```

6. 创建公网 **IP** 地址

```
$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
```

> 注意：
>
> 在使用前先检查域名的可用性。
>
> IP 地址分配方法可以是动态的，也可以是静态的。

7. 分配 **IP** 配置

在此用例中，请在分配 IP 地址之前考虑以下几点：

- IPConfig-1 属于 VPX1 的 subnet1。
- IPConfig-2 属于 VPX1 的 subnet 1。
- IPConfig-3 属于 VPX1 的 subnet 1。

> 注意：
>
> 为 NIC 分配多个 IP 配置时，必须将一个配置分配为主配置。


```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress
    $pip1  - Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress
    $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

使用满足您的子网要求的有效 IP 地址，并检查其可用性。

8. 创建网卡

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
 $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,
$IPConfig3 -NetworkSecurityGroupId $nsg.Id
```

9. 创建 **NetScaler VPX** 实例

1. 初始化变量。

   ```
   $suffixNumber = 1 $vmName = $vmNamePrefix + $suffixNumber
   ```

2. 创建 VM 配置对象。

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
   AvailabilitySetId $avSet.Id
   ```

3. 设置凭据、操作系统和映像.

   ```
   $cred=Get-Credential -Message “输入 VPX 登录的名称和密码。”  $vmConfig=
   Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
   $vmName -Credential $cred  $vmConfig=Set-AzureRMVMSourceImage -VM
    $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -
   Version $version
   ```

4. 添加 NIC。

   ```
   $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
   Id -Primary
   ```

   > 注意：
   >
   > 在多 NIC NetScaler VPX 部署中，一个 NIC 必须是主 NIC。因此，将该 NIC 添加到 NetScaler VPX 实

> 例时必须附加“-Primary”。

5. 指定操作系统磁盘并创建 VM。

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1$osVhdUri=$prmStorageAccount
.PrimaryEndpoints.Blob.ToString()+ "vhds/"+ $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName
 -VhdUri $osVhdUri -CreateOption fromImage    Set-AzureRmVMPlan -
VM $vmConfig -Publisher $publisher -Product $offer -Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. 检查网卡配置

NetScaler VPX 实例启动后，您可以使用以下命令检查分配给 NetScaler VPX NIC 的 `IPConfigs` 的 IP 地址。

```
$nic.IPConfig
```

11. 检查 **VPX** 端配置

当 NetScaler VPX 实例启动时，将与主网卡的主 `IPconfig` 关联的专用 IP 地址添加为 NSIP 地址。其余专用 IP 地址必须添加为 VIP 或 SNIP 地址，具体取决于您的要求。使用的命令如下。

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

您现在已为处于独立模式的 NetScaler VPX 实例配置多个 IP 地址。

用于 **Azure** 部署的其他 **PowerShell** 脚本

October 17, 2024

本部分内容提供了一些 PowerShell cmdlet，可以使用这些 cmdlet 在 Azure PowerShell 中执行以下配置：

- 配置 NetScaler VPX 独立实例
- 在高可用性设置中使用 Azure 外部负载均衡器配置 NetScaler VPX 对
- 使用 Azure 内部负载均衡器在高可用性设置中配置 NetScaler VPX 对

另请参阅以下主题，了解您可以使用 PowerShell 命令执行的配置：

- 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置
- 在 NetScaler VPX 实例上配置 GSLB
- 在 NetScaler 主动-备用高可用性设置中配置 GSLB
- 使用 PowerShell 命令在独立模式下为 NetScaler VPX 实例配置多个 IP 地址

配置 **NetScaler VPX** 独立实例

1. 创建资源组

   资源组可以包括解决方案的所有资源，也可以仅包括要作为一个组管理的资源。此处指定的位置是该资源组中的资源的默认位置。请确保用于创建负载均衡器的所有命令均使用同一资源组。

   ```
   $rgName="&lt;resource group name&gt;" $locName="&lt;location name , such as West US&gt;"  New-AzureRmResourceGroup -名称 $rgName -位置 $locName
   ```

   例如：

   ```
   1    $rgName = "ARM-VPX"
   2    $locName = "West US"
   3    New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. 创建存储帐户

   为您的存储帐户选择仅包含小写字母和数字的唯一名称。

   ```
   $saName="&lt;storage account name&gt;"      $saType="&lt;storage account type&gt;",指定一个：Standard_LRS、Standard_GRS、Standard_RAGRS 或 Premium_LRS New-AzureRmStorageAccount -名称 $saName -ResourceGroupName $rgName -类型 $saType -位置 $locName
   ```

   例如：

   ```
   1    $saName="vpxstorage"
   2    $saType="Standard\_LRS"
   3    New-AzureRmStorageAccount -Name $saName -ResourceGroupName
           $rgName -Type $saType -Location $locName
   ```

3. 创建可用性集

   可用性集可帮助使您的虚拟机在停机期间（例如，在维护期间）保持可用。配置了可用性集的负载均衡器可确保您的应用程序始终可用。

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName
   ```

4. 创建虚拟网络

   如果以前未创建子网，请添加一个至少包含一个子网的新虚拟网络。

   ```
   $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
```

例如：

```
1   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix
2
3   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       backendSubnet -AddressPrefix $BackendAddressPrefix
4
5   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName
       $rgName -Location $locName -AddressPrefix $vnetAddressPrefix
       -Subnet $frontendSubnet,$backendSubnet
```

5. 创建 **NIC**

创建一个 NIC 并将该 NIC 与 NetScaler VPX 实例相关联。上述过程中创建的前端子网索引编号为 0，后端子网索引编号为 1。现在采用以下三种方式之一创建 NIC：

a) 使用公用 *IP* 地址创建 *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) 使用公用 *IP* 和 *DNS* 标签创建 *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
```

分配 $domName 之前，请使用以下命令检查其是否可用：

```
Test-AzureRmDnsAvailability -DomainQualifiedName $domName -
Location $locName

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
 $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex
].Id -PublicIpAddressId $pip.Id
```


例如：

```
$nicName="frontendNIC"

$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
     $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets\[0\].Id -PublicIpAddressId $pip.Id
```

c) 使用动态公用地址和静态专用 *IP* 地址创建 *NIC*

请确保您添加到 VM 的专用（静态）IP 地址的范围必须与指定的子网的范围相同。

```
$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. 创建虚拟对象

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
 $rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. 获取 **NetScaler VPX** 图片

```
$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."
```

提供用于登录 VPX 的凭据


```
$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
```

例如：

```
$pubName="citrix"
```

以下命令用于显示 Citrix 提供的所有产品/服务：

```
1   Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
        Select Offer
2
3   $offerName="netscalervpx110-6531"
```

以下命令用于获知发布者提供的 SKU 的特定产品/服务名称：

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -
Offer $offerName | Select Skus
```

8. 创建虚拟机

```
$diskName="<name identifier for the disk in Azure storage, such
as OSDisk>"
```

例如：

```
1   $diskName="dynamic"
2
3   $pubName="citrix"
4
5   $offerName="netscalervpx110-6531"
6
7   $skuName="netscalerbyol"
8
9   $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
10
11  $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/
       " + $diskName  + ".vhd"
12
13  $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri
       $osDiskUri -CreateOption fromImage
```

基于应用商店中提供的映像创建 VM 时，请使用以下命令指定 VM 计划：

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName
 -Name $skuName
```



```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
$vm
```

在高可用性设置中使用 **Azure** 外部负载均衡器配置 **NetScaler VPX** 对

使用您的 Azure 用户凭据登录 AzureRmAccount。

1. 创建资源组

   此处指定的位置是该资源组中的资源的默认位置。请确保用于创建负载均衡器的所有命令均使用同一资源组。

   ```
   $rgName="<resource group name>"
   ```

   ```
   $locName="<location name, such as West US>"
   ```

   ```
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   例如：

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. 创建存储帐户

   为您的存储帐户选择仅包含小写字母和数字的唯一名称。

   ```
   $saName="<storage account name>"
   ```

   ```
   $saType="&lt;storage account type&gt;", 指 定 一 个: Standard_LRS、
   Standard_GRS、Standard_RAGRS 或 Premium_LRS
   ```

   ```
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
   $rgName -Type $saType -Location $locName
   ```

   例如：

   ```
   $saName="vpxstorage"

   $saType="Standard_LRS"

   New-AzureRmStorageAccount -Name $saName -ResourceGroupName
       $rgName -Type $saType -Location $locName
   ```

3. 创建可用性集

   配置了可用性集的负载均衡器可确保您的应用程序始终可用。

   ```
   $avName="<availability set name>"
   ```



```
New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName -Location $locName
```

4. 创建虚拟网络

   如果以前未创建子网，请添加一个至少包含一个子网的新虚拟网络。

```
$vnetName = "LBVnet"

$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-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

$vnet=New-AzureRmVirtualNetwork -Name $vnetName -
    ResourceGroupName $rgName -Location $locName -AddressPrefix
    $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet
```

   > 注意：
   >
   > 根据您的要求选择 AddressPrefix 参数值。

   为您在此步骤前面创建的虚拟网络分配前端和后端子网。

   如果前端子网是阵列 VNet 的第一个元素，则 subnetId 必须为 $vnet.Subnets[0].Id。

   如果前端子网是阵列中的第二个元素，则 subnetId 必须为 $vnet.Subnets[1].Id，依此类推。

5. 配置前端 **IP** 地址并创建后端地址池

   配置前端 IP 地址用于传入负载均衡器网络流量，并创建后端地址池用于接收负载平衡的流量。

```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -
    AllocationMethod Static -DomainNameLabel nsvpx
```

   > 注意：
   >
   > 检查 DomainNameLabel 的值是否可用。

```
        $FIPName = "ELBFIP"

        $frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -
            Name $FIPName -PublicIpAddress $publicIP1
```



```
4
5       $BEPool = "LB-backend-Pool"
6
7       $beaddresspool1= New-
            AzureRmLoadBalancerBackendAddressPoolConfig -Name
            $BEPool
```

6. 创建运行状况探测 **Create a health detector**

   创建使用端口 9000 且时间间隔为 5 秒的 TCP 运行状况探测。

```
1   $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
        HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
        ProbeCount 2
```

7. 创建负载平衡规则

   为您要进行负载平衡的每个服务创建 LB 规则。

   例如：

   可以使用以下示例对 HTTP 服务进行负载平衡。

```
1   $lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
        FrontendIpConfiguration $frontendIP1 -BackendAddressPool
        $beAddressPool1 -Probe $healthProbe -Protocol Tcp -
        FrontendPort 80 -BackendPort 80
```

8. 创建入站 **NAT** 规则

   为您不进行负载平衡的服务创建 NAT 规则。

   例如，在创建 NetScaler VPX 实例的 SSH 访问权限时。

   注意：

   对于两个 NAT 规则，协议-前端端口-后端端口三元组不能相同。

```
1       $inboundNATRule1= New-
            AzureRmLoadBalancerInboundNatRuleConfig -Name SSH1
                -FrontendIpConfiguration $frontendIP1 -Protocol
            TCP -FrontendPort 22 -BackendPort 22
2
3       $inboundNATRule2= New-
            AzureRmLoadBalancerInboundNatRuleConfig -Name SSH2 -
            FrontendIpConfiguration $frontendIP1 -Protocol TCP -
            FrontendPort 10022 -BackendPort 22
```

9. 创建负载均衡器实体

   通过将所有对象（NAT 规则、负载均衡器规则、探测配置）添加在一起来创建负载均衡器。

```
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. 创建 **NIC**

    创建两个 NIC 并将每个 NIC 与各个 VPX 实例相关联

    (a) 使用 VPX1 的 NIC1

    例如：

```
1    $nicName="NIC1"
2
3    $lbName="ELB"
4
5    $bePoolIndex=0
6
7    \* Rule indexes starts from 0.
8
9    $natRuleIndex=0
10
11   $subnetIndex=0
12
13   \* Frontend subnet index
14
15   $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
        $rgName
16
17   $nic1=New-AzureRmNetworkInterface -Name $nicName -
        ResourceGroupName $rgName -Location $locName -Subnet $vnet.
        Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
        BackendAddressPools\[$bePoolIndex\] -
        LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex
        \]
```

    b) 使用 VPX2 的 NIC2

    例如：

```
1    $nicName="NIC2"
2
3    $lbName="ELB"
4
5    $bePoolIndex=0
6
7    $natRuleIndex=1
8
9    \* Second Inbound NAT (SSH) rule we need to use
10
11   `$subnetIndex=0
```



```
12
13   \* Frontend subnet index
14
15   $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
        $rgName
16
17   $nic2=New-AzureRmNetworkInterface -Name $nicName -
        ResourceGroupName $rgName -Location $locName -Subnet $vnet.
        Subnets\[$subnetIndex\] -LoadBalancerBackendAddressPool $lb.
        BackendAddressPools\[$bePoolIndex\] -
        LoadBalancerInboundNatRule  $lb.InboundNatRules\[
        $natRuleIndex\]
```

11. 创建 **NetScaler VPX** 实例

    创建两个 NetScaler VPX 实例作为相同资源组和可用性集的一部分，并将其附加到外部负载平衡器。

    a) NetScaler VPX 实例 1

    例如：

```
1    $vmName="VPX1"
2
3    $vmSize="Standard\_A3"
4
5    $pubName="citrix"
6
7    $offerName="netscalervpx110-6531"
8
9    $skuName="netscalerbyol"
10
11   $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
12
13   $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
14
15   $cred=Get-Credential -Message "Type Credentials which will be
        used to login to VPX instance"
16
17   $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
        $vmName -Credential $cred -Verbose
18
19   $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
20
21   $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id
22
23   $diskName="dynamic"
24
25   $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
         -Name $saName
26
27   $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
```



```
        vhds1/" + $diskName  + ".vhd"
28
29  $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
30
31  Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
        $offerName -Name $skuName
32
33  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm1
```

b) NetScaler VPX 实例 2

例如：

```
1   $vmName="VPX2"
2
3   $vmSize="Standard\_A3"
4
5   $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
7   $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
8
9   $cred=Get-Credential -Message " Type Credentials which will be
        used to login to VPX instance "
10
11  $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
        $vmName -Credential $cred -Verbose
12
13  $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15  $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17  $diskName="dynamic"
18
19  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
20
21  $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds2/" + $diskName  + ".vhd"
22
23  $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25  Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
        $offerName -Name $skuName
26
27  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm2
```


12. 配置虚拟机

    两个 NetScaler VPX 实例启动后，使用 SSH 协议连接到这两个 NetScaler VPX 实例以配置虚拟机。

    a) Active-Active：在两个 NetScaler VPX 实例的命令行上运行相同的配置命令集。

    b) 主动-被动：在两个 NetScaler VPX 实例的命令行上运行此命令。

    ```
    add ha node #nodeID <nsip of other NetScaler VPX>
    ```

    在主动-被动模式下，仅在主节点上运行配置命令。

使用 **Azure** 内部负载均衡器在高可用性设置中配置 **NetScaler VPX** 对

使用您的 Azure 用户凭据登录 AzureRmAccount。

1. 创建资源组

   此处指定的位置是该资源组中的资源的默认位置。请确保用于创建负载均衡器的所有命令均使用同一资源组。

   ```
   $rgName="\\&#060;resource group name\\&#062;"
   $locName="\\&#060;location name, such as West US\\&#062;"
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   例如：

   ```
   1  $rgName = "ARM-LB-NS"
   2
   3  $locName = "West US"
   4
   5  New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. 创建存储帐户

   为您的存储帐户选择仅包含小写字母和数字的唯一名称。

   ```
   $saName="<storage account name>"
   $saType="&lt;storage account type&gt;", 指定一个：Standard_LRS、Standard_GRS、Standard_RAGRS 或 Premium_LRS
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName
   ```

   例如：

   ```
   1  $saName="vpxstorage"
   2
   3  $saType="Standard_LRS"
   4
   5  New-AzureRmStorageAccount -Name $saName -ResourceGroupName
          $rgName -Type $saType -Location $locName
   ```


3. 创建可用性集

   配置了可用性集的负载均衡器可确保您的应用程序始终可用。

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
   $rgName -Location $locName
   ```

4. 创建虚拟网络

   如果以前未创建子网，请添加一个至少包含一个子网的新虚拟网络。

   ```
   1   $vnetName = "LBVnet"
   2
   3   $vnetAddressPrefix="10.0.0.0/16"
   4
   5   $FrontendAddressPrefix="10.0.1.0/24"
   6
   7   $BackendAddressPrefix="10.0.2.0/24"
   8
   9   $vnet=New-AzureRmVirtualNetwork -Name $vnetName -
           ResourceGroupName $rgName -Location $locName -AddressPrefix
           $vnetAddressPrefix -Subnet $frontendSubnet,$backendSubnet\`
   10
   11  $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
           frontendSubnet -AddressPrefix $FrontendAddressPrefix
   12
   13  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
           backendSubnet -AddressPrefix $BackendAddressPrefix
   ```

   > 注意：
   >
   > 根据您的要求选择 AddressPrefix 参数值。

   为您在此步骤前面创建的虚拟网络分配前端和后端子网。

   如果前端子网是阵列 VNet 的第一个元素，则 subnetId 必须为 $vnet.Subnets[0].Id。

   如果前端子网是阵列中的第二个元素，则 subnetId 必须为 $vnet.Subnets[1].Id，依此类推。

5. 创建后端地址池

   ```
   $beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -
   Name "LB-backend"
   ```

6. 创建 **NAT** 规则

   为您不进行负载平衡的服务创建 NAT 规则。

   ```
   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
```

根据您的要求使用前端端口和后端端口。

7. 创建运行状况探测 **Create a health detector**

   创建使用端口 9000 且时间间隔为 5 秒的 TCP 运行状况探测。

```
1    $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
        HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5
         -ProbeCount 2
```

8. 创建负载平衡规则

   为您要进行负载平衡的每个服务创建 LB 规则。

   例如：

   可以使用以下示例对 HTTP 服务进行负载平衡。

```
1    $lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
        FrontendIpConfiguration $frontendIP -BackendAddressPool
        $beAddressPool -Probe $healthProbe -Protocol Tcp -
        FrontendPort 80 -BackendPort 80
```

   根据您的要求使用前端端口和后端端口。

9. 创建负载均衡器实体

   通过将所有对象（NAT 规则、负载均衡器规则、探测配置）添加在一起来创建负载均衡器。

```
1    $NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -
        Name "InternalLB" -Location $locName -FrontendIpConfiguration
         $frontendIP -InboundNatRule $inboundNATRule1,
        $inboundNatRule2 -LoadBalancingRule $lbrule -
        BackendAddressPool $beAddressPool -Probe $healthProbe
```

10. 创建 **NIC**

    创建两个 NIC 并将每个 NIC 与各个 NetScaler VPX 实例相关联

```
1    $backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
        $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
         10.0.2.6 -Subnet $backendSubnet -
        LoadBalancerBackendAddressPool $nrplb.BackendAddressPools
        \[0\] -LoadBalancerInboundNatRule $nrplb.InboundNatRules\[0\]
```

    此 NIC 用于 NetScaler VPX 1。专用 IP 必须与添加的子网的专用 IP 位于同一子网。

```
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
        \[1\].
```

这个 NIC 适用于 NetScaler VPX 2。根据您的要求，参数 `Private IPAddress` 可以有任何私有 IP。

11. 创建 **NetScaler VPX** 实例

    创建两个 VPX 实例作为相同资源组和可用性集的一部分，并将其附加到内部负载均衡器。

    a) NetScaler VPX 实例 1

    例如：

```
1   $vmName="VPX1"
2
3   $vmSize="Standard\_A3"
4
5   $avSet=Get-AzureRmAvailabilitySet -Name $avName -
        ResourceGroupName $rgName
6
7   $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
        AvailabilitySetId $avset.Id
8
9   $cred=Get-Credential -Message "Type Credentials which will be
        used to login to VPX instance"
10
11  $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
        $vmName -Credential $cred -Verbose
12
13  $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
        Offer $offerName -Skus $skuName -Version "latest"
14
15  $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id
16
17  $diskName="dynamic"
18
19  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
        -Name $saName
20
21  $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
        vhds1/" + $diskName  + ".vhd"
22
23  $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
        $osDiskUri1 -CreateOption fromImage
24
25  Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product
        $offerName -Name $skuName
26
27  New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
        $vm1
```

    b) NetScaler VPX 实例 2

例如：

```
$vmName="VPX2"

$vmSize="Standard\_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -
    ResourceGroupName $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName
     -Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "
    vhds2/" + $diskName  + ".vhd"

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product
    $offerName -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
```

12. 配置虚拟机

两个 NetScaler VPX 实例启动后，使用 SSH 协议连接到这两个 NetScaler VPX 实例以配置虚拟机。

a) Active-Active：在两个 NetScaler VPX 实例的命令行上运行相同的配置命令集。

b) 主动-被动：在两个 NetScaler VPX 实例的命令行上运行此命令。

```
add ha node #nodeID <nsip of other NetScaler VPX>
```

在主动-被动模式下，仅在主节点上运行配置命令。

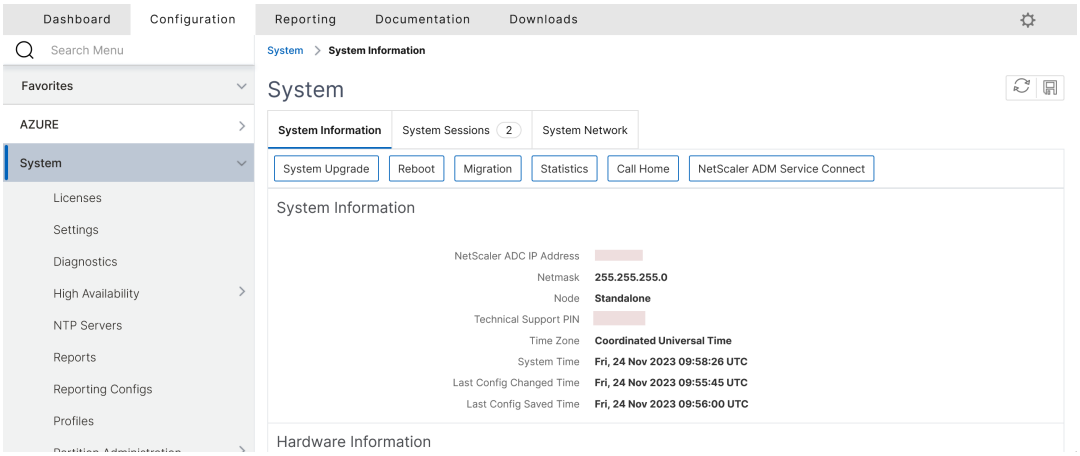
Create a support ticket for the VPX instance on Azure

April 23, 2024

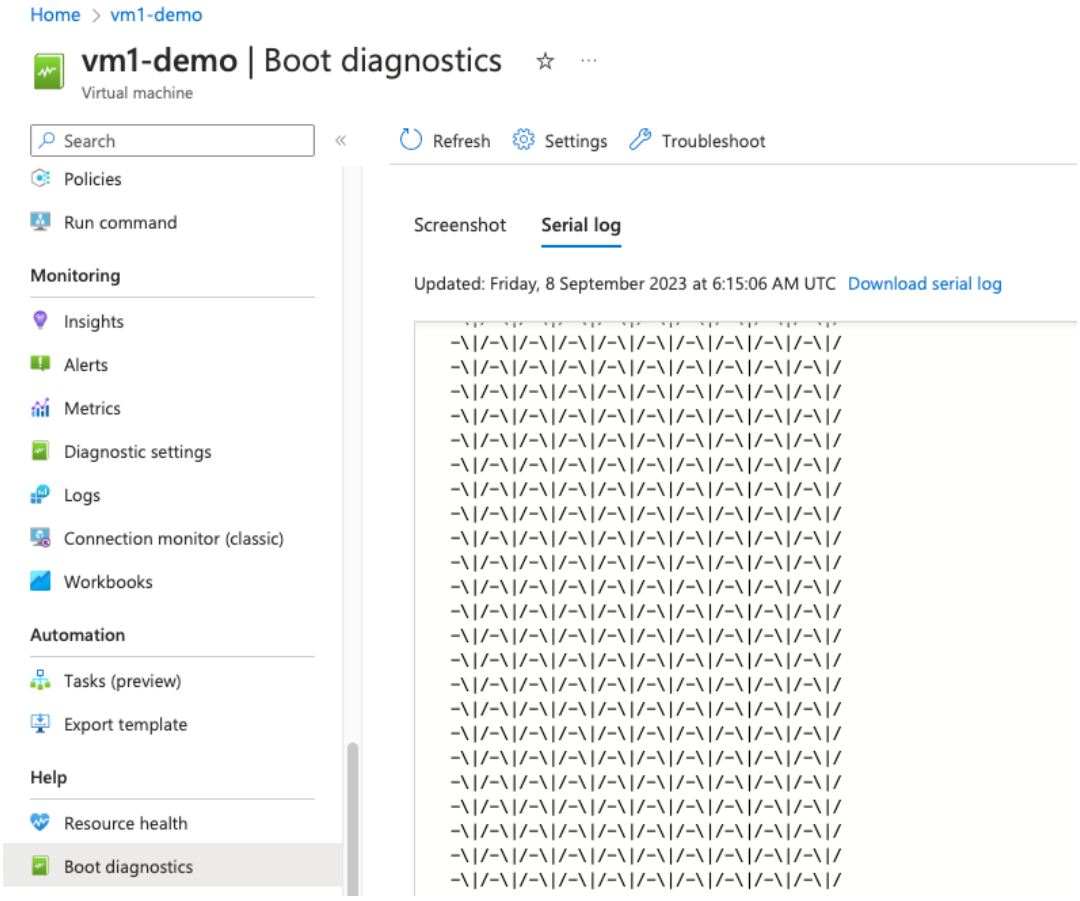
If you' re experiencing issues with your NetScaler VPX instance on Azure, for troubleshooting, you can create a support ticket in the NetScaler support portal.

To file a support ticket, make sure the following:

- Your network is connected.
- You have your Azure account number, the support PIN code of the NetScaler subscription-based offering that you have deployed on Azure, and the Azure serial log handy.
  - You can find the support PIN code on the **Systems page** in the VPX GUI.



  - You can find the serial log in the Azure portal (**Boot diagnostics** section of your VM).



> **Note:**
>
> NetScaler supports subscription-based offerings on Azure (subscription license with hourly price).

Once you have all the information ready, call NetScaler support. You’ re asked to provide your name and email address.

Azure 常见问题解答

October 17, 2024

- 从 **Azure Marketplace** 安装的 **NetScaler VPX** 实例的升级过程与本地升级过程有什么不同吗?

  没有。您可以使用标准的 NetScaler VPX 升级程序将 Microsoft Azure 云中的 NetScaler VPX 实例升级到 NetScaler VPX 版本 11.1 或更高版本。可以使用 GUI 或 CLI 过程进行升级。对于任何新安装，请使用适用于 Microsoft Azure 云的 NetScaler VPX 映像。

  要下载 **NetScaler VPX** 升级版本，请前往 **NetScaler** 下载 **>**NetScaler** 固件。

- 如何更正在 **Azure** 上托管的 **NetScaler VPX** 实例上观察到的 **MAC** 移动和接口静音？

  默认情况下，在 Azure 多网卡环境中，所有数据接口可能会显示 MAC 移动和界面静音。为了避免 Azure 环境上的 MAC 移动和接口静音，Citrix 建议您为 NetScaler VPX 实例创建每个数据接口（不带标签）的 VLAN，并在 Azure 中绑定 NIC 的主 IP。

  有关更多信息，请参阅 CTX224626 文章。

在 **Google Cloud Platform** 上部署 **NetScaler VPX** 实例

October 17, 2024

您可以在 Google Cloud Platform (GCP) 上部署 NetScaler VPX 实例。GCP 中的 VPX 实例使您能够利用 GCP 云计算功能，并使用 Citrix 负载平衡和流量管理功能来满足业务需求。可以将 VPX 实例作为独立实例在 GCP 中部署。同时支持单 NIC 和多 NIC 配置。

支持的功能

GCP 支持所有高级、高级和标准功能，具体取决于所使用的许可证/版本类型。

限制

- 不支持 IPv6。

硬件要求

GCP 中的 VPX 实例必须至少有 2 个 vCPU 和 4 GB RAM。

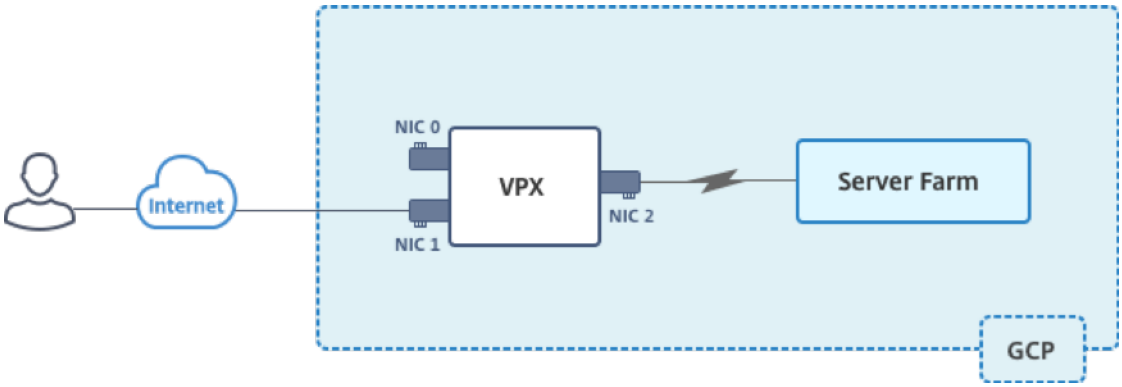
注意事项

在开始部署之前，请注意以下 GCP 特定的注意事项。

- 创建实例后，您无法添加或移除任何网络接口。
- 对于多 NIC 部署，请为每个 NIC 创建单独的 VPC 网络。一个 NIC 只能与一个网络相关联。
- 对于单网卡实例，默认情况下，GCP 控制台创建网络。
- 对于具有两个以上网络接口的实例，至少需要 4 个 vCPU。
- 如果需要 IP 转发，则必须在创建实例和配置 NIC 时启用 IP 转发。

场景：部署多 **NIC**、多 **IP** 独立 **NetScaler VPX** 实例

此场景说明了如何在 GCP 中部署 NetScaler VPX 独立实例。在这种情况下，您将创建一个包含多个 NIC 的独立 VPX 实例。实例与后端服务器（服务器场）进行通信。



创建三个 NIC 以实现以下目的。

NIC	用途	与 VPC 网络相关联
NIC 0	为管理流量提供服务（NetScaler IP）	管理网络
NIC 1	服务客户端流量 (VIP)	客户端网络
NIC 2	与后端服务器通信 (SNIP)	后端服务器网络

在以下各项之间设置所需的通信路由：

- NetScaler VPX 实例和后端服务器。
- NetScaler VPX 实例和公共互联网上的外部主机。

部署步骤摘要

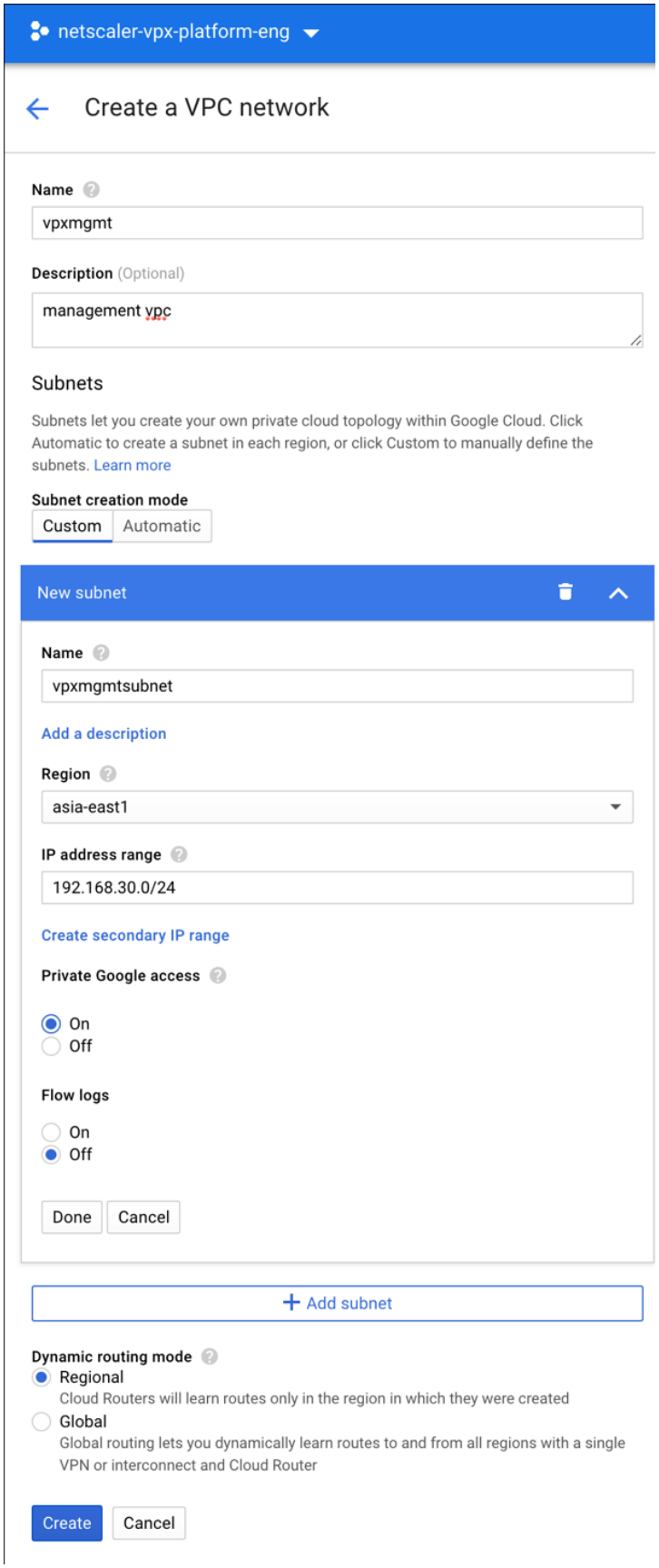
1. 为三个不同的 NIC 创建三个 VPC 网络。
2. 步骤 2. 为端口 22、80 和 443 创建防火墙规则。
3. 使用三个 NIC 创建实例。

从 GCP 市场中选择 NetScaler VPX 实例。

> 注意：
>
> 在创建 VPC 网络的同一区域中创建实例。

步骤 **1.** 步骤 **1.** 创建 **VPC** 网络。

创建三个与管理 NIC、客户端 NIC 和服务器 NIC 相关联的 VPC 网络。要创建 VPC 网络，请登录 **Google** 控制台 **>** 网络 **> VPC** 网络 **>** 创建 **VPC** 网络。填写必填字段，如屏幕截图中所示，然后单击 **Create**（创建）。

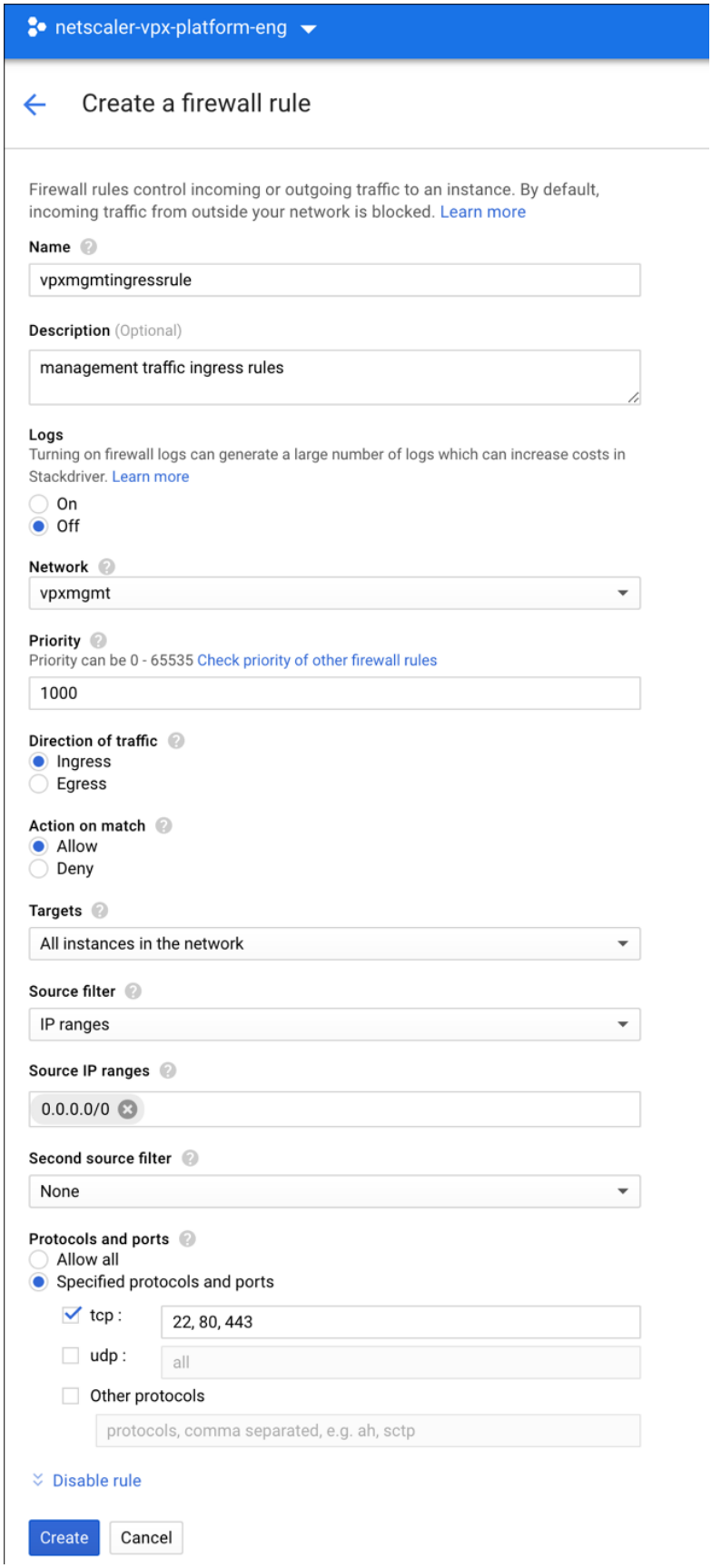


同样，请为客户端和服务器端 NIC 创建 VPC 网络。

> 注意：
>
> 所有三个 VPC 网络必须位于同一区域，在此场景中为 asia-east1。

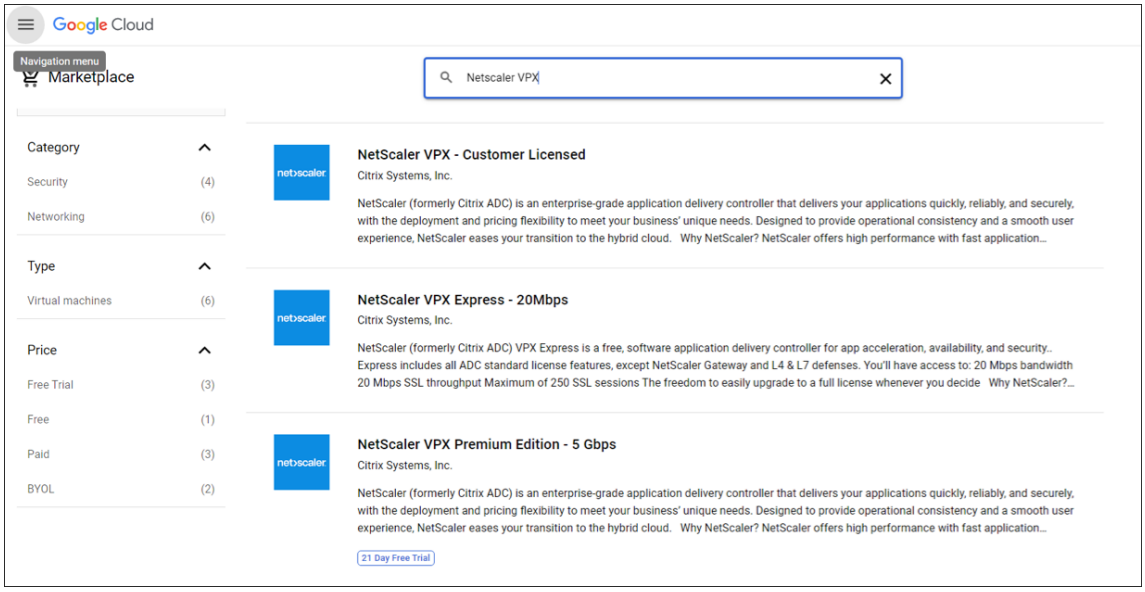
步骤 **2.** 步骤 **2.** 为端口 **22**、**80** 和 **443** 创建防火墙规则。

为每个 VPC 网络创建 SSH（端口 22）、HTTP（端口 80）和 HTTPS（端口 443）的规则。有关防火墙规则的详细信息，请参阅 防火墙规则概述。

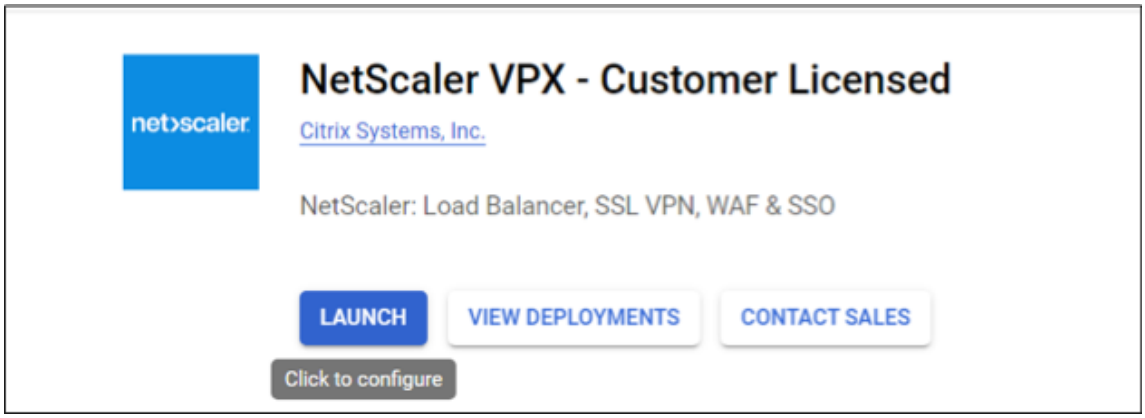


步骤 **3.** 步骤 **3.** 创建 **VPX** 实例。

1. 登录 GCP 控制台。
2. 导航到 GCP 市场。
3. 根据您的要求选择订阅。



4. 在所选订阅上单击“启动”。



5. 填写部署表单，然后单击“部署”。

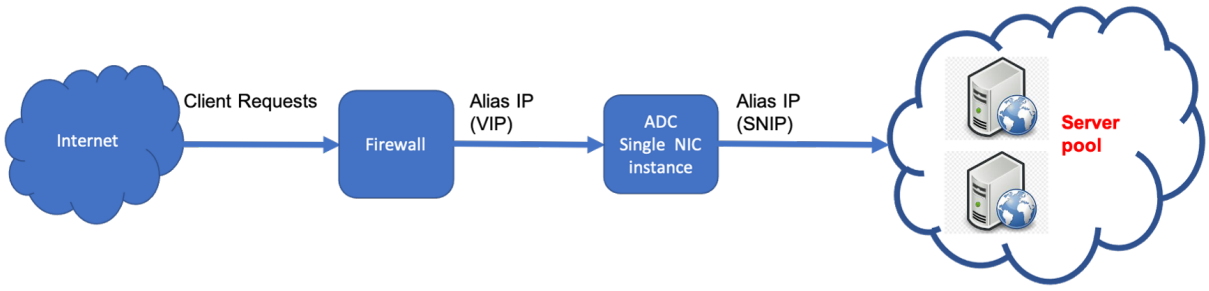
> 注意：
>
> 使用在 步骤 **1** 中创建的 VPC 网络。

6. 已部署的实例显示在“计算引擎” **>** “虚拟机实例”下。

   使用 GCP SSH 或串行控制台配置和管理 VPX 实例。

场景：部署单网卡、独立 **VPX** 实例

此场景说明了如何在 GCP 中使用单个 NIC 部署 NetScaler VPX 独立实例。别名 IP 地址用于实现此部署。



创建单个 NIC (NIC0) 以实现以下目的：

- 处理管理网络中的管理流量（NetScaler IP）。
- 处理客户端网络中的客户端流量 (VIP)。
- 与后端服务器网络中的后端服务器 (SNIP) 进行通信。

在以下各项之间设置所需的通信路由：

- 实例和后端服务器。
- 公共 Internet 上的实例和外部主机。

部署步骤摘要

1. 为 NIC0 创建 VPC 网络。
2. 步骤 2. 为端口 22、80 和 443 创建防火墙规则。
3. 使用单个 NIC 创建实例。
4. 将别名 IP 地址添加到 VPX。
5. 在 VPX 上添加 VIP 和 SNIP。
6. 添加负载平衡虚拟服务器。
7. 在实例上添加服务或服务组。
8. 将服务或服务组绑定到实例上的负载平衡虚拟服务器。

> 注意：
>
> 在创建 VPC 网络的同一区域中创建实例。

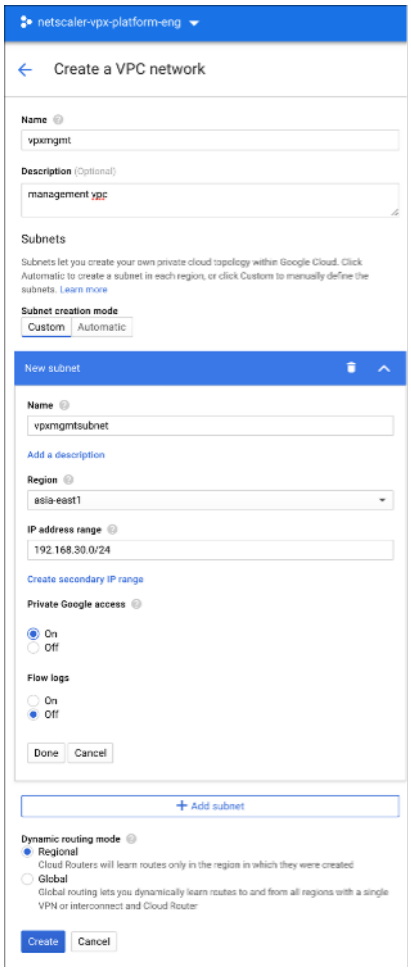
步骤 **1.** 步骤 **1.** 创建一个 **VPC** 网络。

创建一个 VPC 网络以与 NIC0 关联。

要创建 VPC 网络，请执行以下步骤：

1. 登录 **GCP** 控制台 **>** 网络 **> VPC** 网络 **>** 创建 **VPC** 网络

2. 填写必填字段，然后单击 **Create**（创建）。



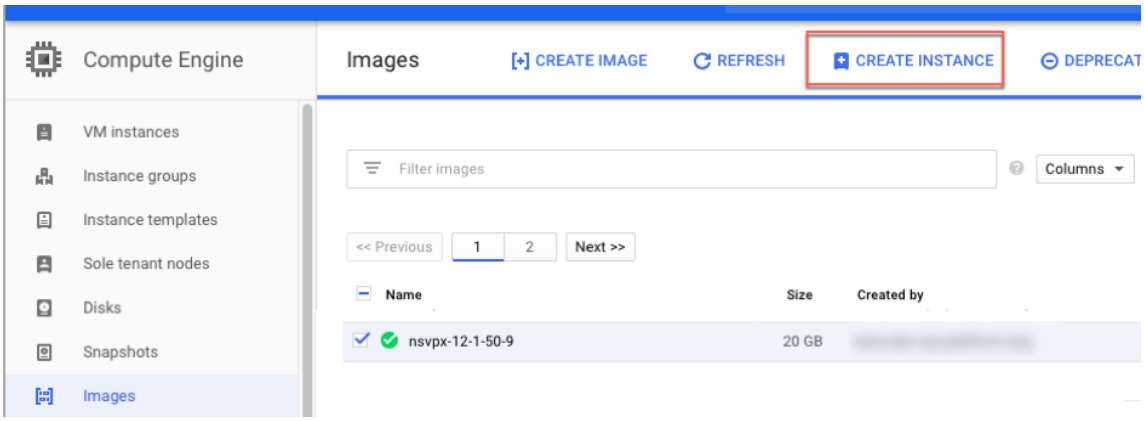
步骤 **2.** 步骤 **2.** 为端口 **22**、**80** 和 **443** 创建防火墙规则。

为 VPC 网络创建 SSH（端口 22）、HTTP（端口 80）和 HTTPS（端口 443）的规则。有关防火墙规则的详细信息，请参阅 防火墙规则概述。

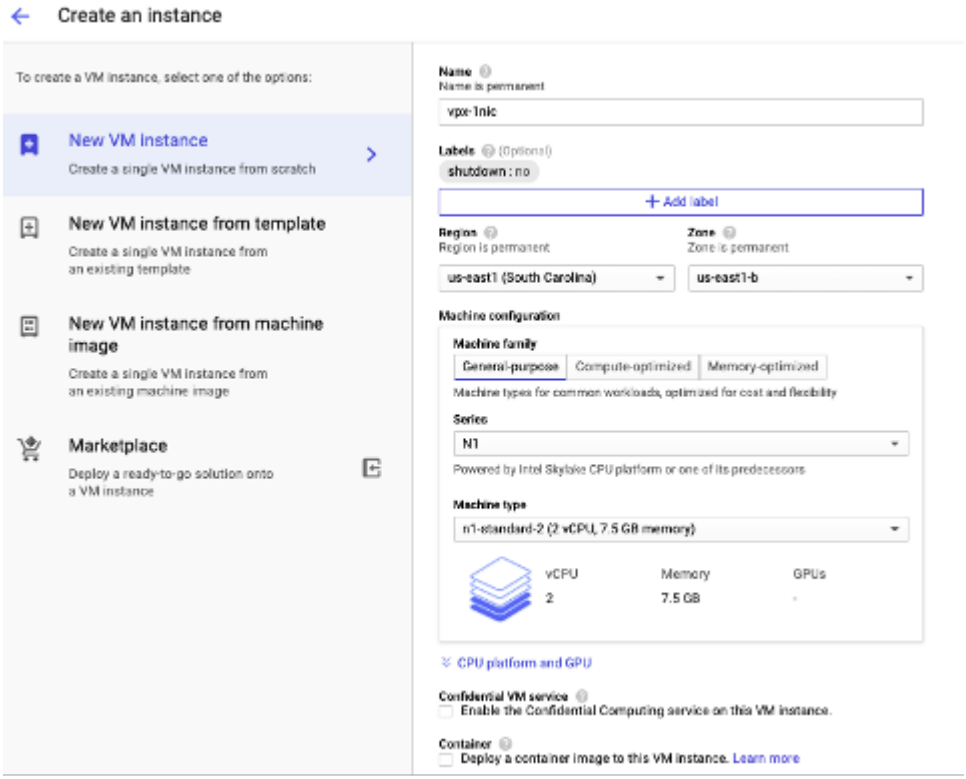
步骤 **3.** 步骤 **3.** 使用单个 **NIC** 创建实例。

要使用单个 NIC 创建实例，请执行以下步骤：

1. 登录 **GCP** 控制台。
2. 在 计算下，将鼠标悬停在 计算引擎上，然后选择 图像。
3. 选择映像，然后单击 **Create Instance**（创建实例）。



4. 选择具有两个 vCPU 的实例类型（ADC 的最低要求）。



5. 在 管理、安全、磁盘、网络窗口中单击网络 选项卡。
6. 在 网络接口下，单击 编辑 图标以编辑默认 NIC。
7. 在 网络接口窗口 的 网络下，选择您创建的 VPC 网络。
8. 您可以创建静态外部 IP 地址。在 外部 **IP** 地址下，单击 创建 **IP** 地址。
9. 在“保留静态地址”窗口中，添加名称和描述，然 后单击“保留”。
10. 单击 创建 以创建 VPX 实例。新实例将显示在虚拟机实例下。

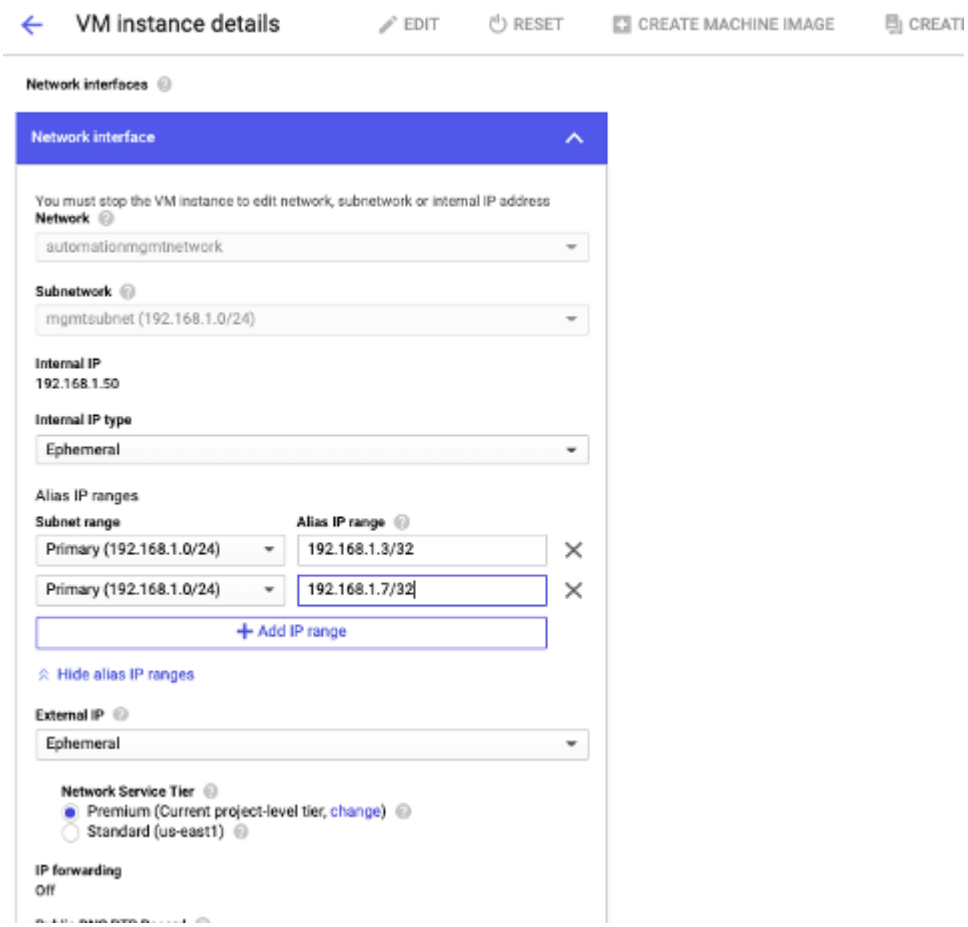
步骤 **4.** 步骤 **4.** 向 **VPX** 实例添加别名 **IP** 地址。

为 VPX 实例分配两个别名 IP 地址以用作 VIP 和 SNIP 地址。

> 注意：
>
> 不要使用 VPX 实例的主要内部 IP 地址来配置 VIP 或 SNIP。

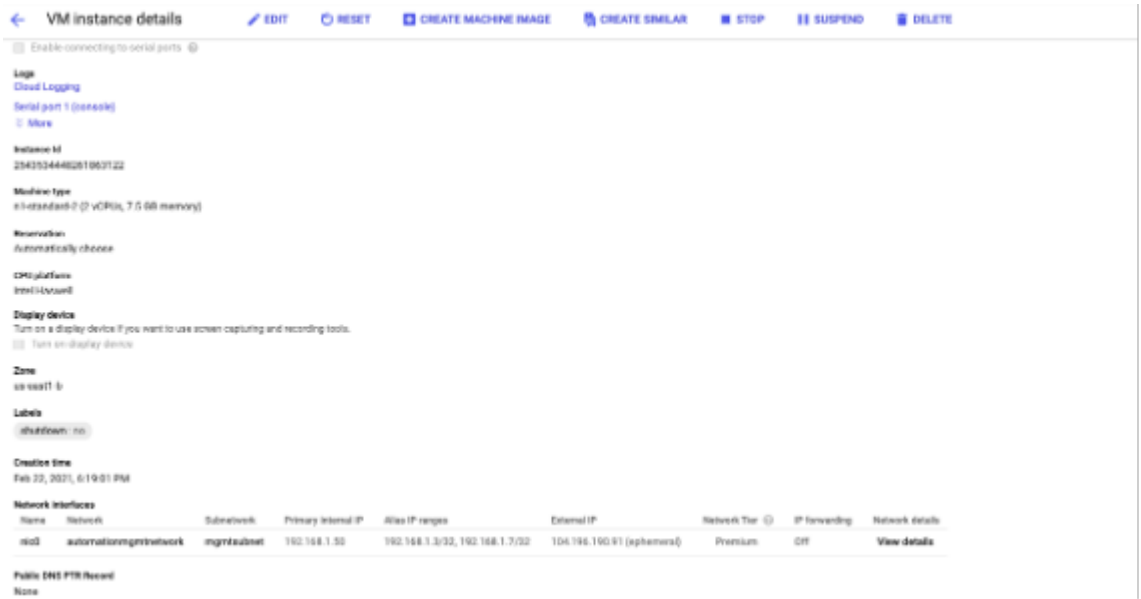
要创建别名 IP 地址，请执行以下步骤：

1. 导航到 VM 实例，然后单击编辑。
2. 在 网络接口 窗口中，编辑 NIC0 接口。
3. 在 别名 **IP** 范围 字段中，输入别名 IP 地址。



4. 单击 完成，然后单击 保存。

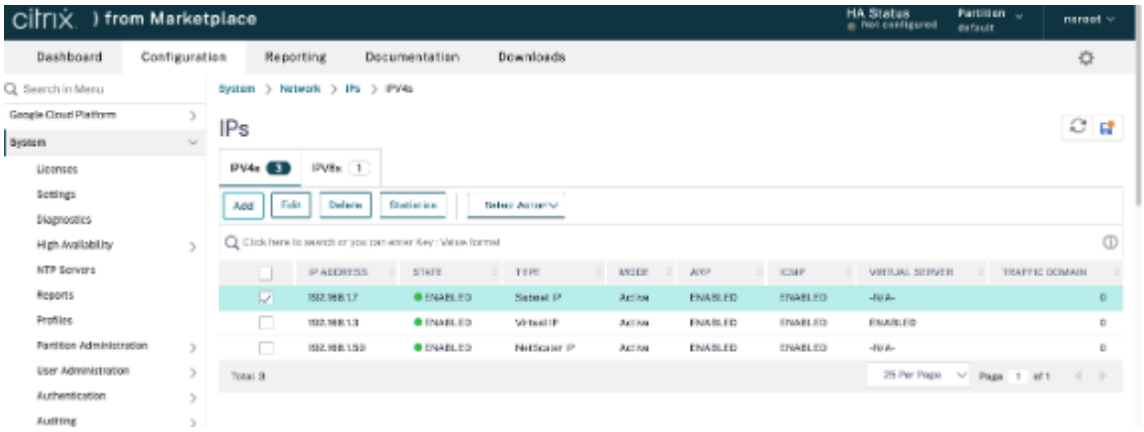
5. 在 虚拟机实例详细信息 页面中验证别名 IP 地址。



步骤 **5.** 步骤 **5.** 在 **VPX** 实例上添加 **VIP** 和 **SNIP**。

在 VPX 实例上，添加客户端别名 IP 地址和服务器别名 IP 地址。

1. 在 NetScaler GUI 上，导航到“系统”**>**“网络”**>**“**IP**”**>**“**IPv4s**”，然后单击“添加”。



2. 要创建客户端别名 IP (VIP) 地址，请执行以下操作：

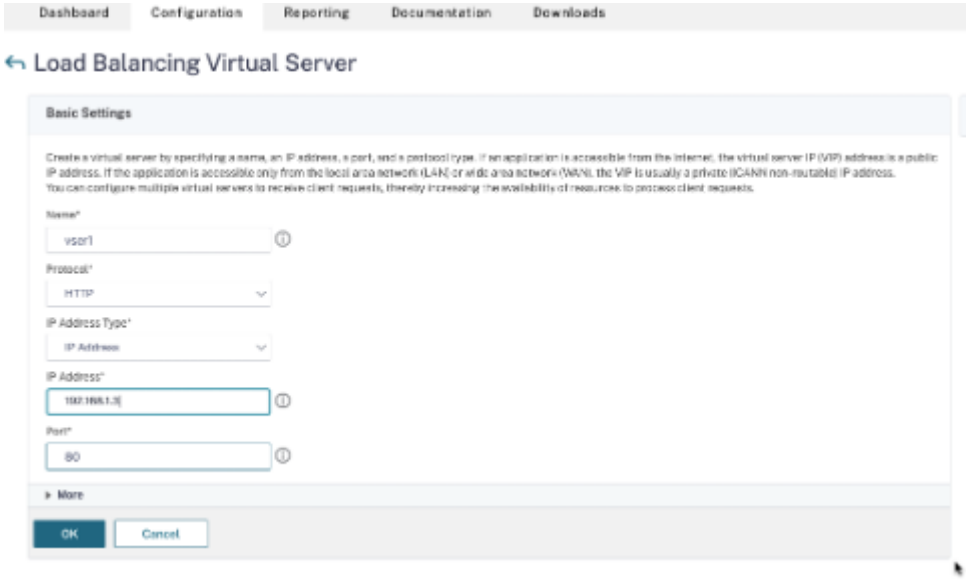
   - 输入为虚拟机实例中的 VPC 子网配置的客户端别名 IP 地址和网络掩码。
   - 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
   - 单击创建。

3. 要创建服务器别名 IP (SNIP) 地址，请执行以下操作：

   - 输入为虚拟机实例中的 VPC 子网配置的服务器别名 IP 地址和网络掩码。
   - 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   - 单击创建。

步骤 **6.** 步骤 **6.** 添加负载平衡虚拟服务器。

1. 在 NetScaler GUI 上，导航到 配置 **>** 流量管理 **>** 负载平衡 **>** 虚拟服务器，然后单击 添加。
2. 添加名称、协议、IP 地址类型（IP 地址）、IP 地址（客户端别名 IP）和端口所需的值。
3. 单击 **OK**（确定）以创建负载平衡虚拟服务器。



步骤 **7.** 步骤 **7.** 在 **VPX** 实例上添加服务或服务组。

1. 在 NetScaler GUI 中，导航到 配置 **>** 流量管理 **>** 负载平衡 **>** 服务，然后单击 添加。
2. 添加服务名称、IP 地址、协议和端口所需的值，然 后单击确定。

步骤 **8.** 步骤 **8.** 将服务/服务组绑定到实例上的负载平衡虚拟服务器。

1. 从 GUI 中，导航到 配置 **>** 流量管理 **>** 负载平衡 **>** 虚拟服务器。
2. 选择在 步骤 **6** 中配置的负载平衡虚拟服务器，然后单击 编辑。
3. 在“服务和服务组”窗口中，单击“无负载平衡虚拟服务器服务绑定”。
4. 选择在 步骤 **7** 中配置的服务，然后单击 绑定。

在 **GCP** 上部署 **VPX** 实例后需要注意的要点

- 使用用户名 `nsroot` 和实例 ID 作为密码登录 VPX。出现提示时，请更改密码并保存配置。
- 要收集技术支持包，请运行命令 `shell /netscaler/showtech_cloud.pl` 而非惯常使用的命令 `show techsupport`。
- 从 GCP 控制台删除 NetScaler 虚拟机后，还要删除关联的 NetScaler 内部目标实例。为此，请转到 gcloud CLI 并键入以下命令：

```
1    gcloud compute -q  target-instances delete <instance-name>-
        adcinternal --zone <zone>
```

> 注意：
>
> <instance-name>-adcinternal 是必须删除的目标实例的名称。

NetScaler VPX 许可

GCP 上的 NetScaler VPX 实例需要许可证。以下许可选项适用于在 GCP 上运行的 NetScaler VPX 实例。

- 基于订阅的许可：NetScaler VPX 设备在 GCP 市场上以付费实例的形式提供。基于订阅的许可是即付即用方式。用户按小时收费。GCP 应用商店中提供以下 VPX 型号和许可证版本。

支持的 VPX 性能
NetScaler VPX Advanced - 200 Mbps
NetScaler VPX Premium - 1 Gbps
NetScaler VPX Premium - 5 Gbps
NetScaler VPX Express-20 Mbps
NetScaler VPX - 客户许可
NetScaler VPX FIPS - 客户许可

- 自带许可证 **(BYOL)**：如果您自带许可证 (BYOL)，请参阅 VPX 许可指南，URL 为 http://support.citrix.com/article/CTX122426。您必须：
  - 使用 Citrix Web 站点中的许可门户生成有效许可证。
  - 将许可证上载到实例。
- **NetScaler VPX** 检出/签出许可：有关详细信息，请参阅 NetScaler VPX 检出/签出许可。

适用于本地部署和云部署的 VPX Express 不需要许可证文件。有关 NetScaler VPX Express 的更多信息，请参阅 NetScaler 许可概述中的“NetScaler VPX Express 许可证”部分。

用于部署 NetScaler VPX 实例的 GDM 模板

您可以使用 NetScaler VPX Google 部署管理器 (GDM) 模板在 GCP 上部署 VPX 实例。有关详细信息，请参阅 NetScaler GDM 模板。

NetScaler 应用商店示意图

您可以使用 GDM 模板中的图像来启动 NetScaler 设备。

下表列出了 GCP 应用商店中提供的映像。

释放	映像名称	图片位置
14.1	citrix-adc-vpx-express-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-express-14-1-21-57
14.1	citrix-adc-vpx-200-enterprise-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-14-1-21-57
14.1	citrix-adc-vpx-1000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-platinum-14-1-21-57
14.1	citrix-adc-vpx-5000-platinum-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-14-1-21-57
14.1	citrix-adc-vpx-byol-14-1-21-57	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-14-1-21-57

资源

- 使用多个网络接口创建实例
- 创建和启动 VM 实例

相关信息

- 在 Google 云端平台上部署 VPX 高可用性对

在 **Google** 云端平台上部署 **VPX** 高可用性对

October 17, 2024

您可以在 Google Cloud Platform (GCP) 上将两个 NetScaler VPX 实例配置为高可用性 (HA) 主动-被动对。当您将一个实例配置为主节点，将另一个实例配置为辅助节点时，主节点将接受连接并管理服务器。辅助节点负责监视主节点。如果因任何原因主节点无法接受连接，将由辅助节点接替其职责。

有关 HA 的更多信息，请参阅 高可用性。

这些节点必须位于同一个地理区域；但是，它们可以位于同一个区域，也可以位于不同的区域。有关更多信息，请参阅地区和区域。

每个 VPX 实例至少需要三个 IP 子网（Google VPC 网络）：

- 管理子网
- 面向客户端的子网 (VIP)
- 面向后端的子网（SNIP、MIP 等）

Citrix 建议对标准 VPX 实例使用三个网络接口。

可以使用以下方法部署 VPX 高可用性对：

- 使用外部静态 IP 地址
- 使用专用 IP 地址
- 使用具有专用 IP 地址的单个 nic 虚拟机

用于在 **GCP** 上部署 **VPX** 高可用性对的 **GDM** 模板

可以使用 NetScaler Google Deployment Manager (GDM) 模板在 GCP 上部署 VPX 高可用性对。有关详细信息，请参阅 NetScaler GDM 模板。

GCP 上支持 **VPX** 高可用性对的转发规则

可以使用转发规则在 GCP 上部署 VPX 高可用性对。

有关转发规则的详细信息，请参阅 转发规则概述。

必备条件

- 转发规则必须与 VPX 实例位于同一区域中。
- 目标实例必须与 VPX 实例位于同一区域中。
- 主节点和辅助节点的目标实例数必须匹配。

Example:

在 `us-east1` 区域中有一个高可用性对，主 VPX 位于 `us-east1-b` 区域中，辅助 VPX 位于 `us-east1-c` 区域中。为目标实例位于 `us-east1-b` 区域中的主 VPX 配置了转发规则。为 `us-east1-c` 区域中的辅助 VPX 配置目标实例，以更新故障转移时的转发规则。

限制

VPX 高可用性部署中仅支持在后端使用目标实例配置的转发规则。

在 **Google** 云端平台上部署具有外部静态 **IP** 地址的 **VPX** 高可用性对

October 17, 2024

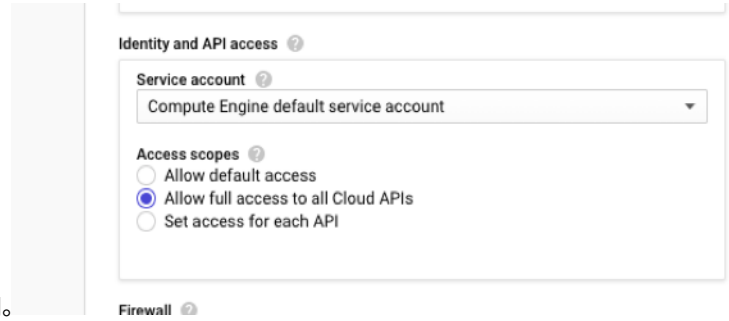
可以使用外部静态 IP 地址在 GCP 上部署 VPX 高可用性对。主节点的客户端 IP 地址必须绑定到外部静态 IP 地址。故障转移时，外部静态 IP 地址将移动到辅助节点以便恢复流量。

静态外部 IP 地址是在您决定释放之前为项目保留的外部 IP 地址。如果使用 IP 地址访问服务，则可以保留该 IP 地址，以便只有您的项目可以使用。有关更多信息，请参阅 保留静态外部 IP 地址。

有关 HA 的更多信息，请参阅 高可用性。

开始之前的准备工作

- 阅读 在 Google Cloud Platform上部署 NetScaler VPX 实例中提到的限制、硬件要求和注意事项。此信息也适用于高可用性部署。
- 为您的 GCP 项目启用 **Cloud Resource Manager API**。
- 在创建实例时允许对所有云 API 进行完全访问。



- 确保与您的 GCP 服务帐户关联的 IAM 角色具有以下 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.instances.get",
"Compute.instances.list",
"compute.networks.useExternalIp",
```



```
    "compute.subnetworks.useExternalIp",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.targetInstances.create",
    "compute.zones.list",
    "compute.zoneOperations.get",
    ]
```

- 如果您在管理界面以外的其他接口上配置了别名 IP 地址，请确保您的 GCP 服务帐户具有以下其他 IAM 权限：

```
    "compute.instances.updateNetworkInterface"
```

- 如果您已在主节点上配置了 GCP 转发规则，请阅读 GCP 上 VPX 高可用性对的转发规则支持 中提到的限制和要求，以便在故障转移时将它们更新为新的主节点。

如何在 **Google** 云端平台上部署 **VPX** 高可用性对

以下是 HA 部署步骤的摘要：

1. 在同一地理地区创建多个 VPC 网络。例如，Asia-east。
2. 在同一地理区域创建两个 VPX 实例（主节点和辅助节点）。它们可以位于同一个区域，也可以位于不同的区域。例如，Asia east-1a 和 Asia east-Ib。
3. 使用 NetScaler GUI 或 ADC CLI 命令在两个实例上配置 HA 设置。

步骤 **1.** 步骤 **1.** 创建 **VPC** 网络

根据您的要求创建 VPC 网络。Citrix 建议您创建三个 VPC 网络，分别用于与管理 NIC、客户端 NIC 和服务器 NIC 关联。

要创建 VPC 网络，请执行以下步骤：

1. 登录 **Google** 控制台 **> Networking**（网络连接）**> VPC network**（**VPC** 网络）**> Create VPC Network**（创建 **VPC** 网络）。
2. 填写必填字段，然后单击 **Create**（创建）。

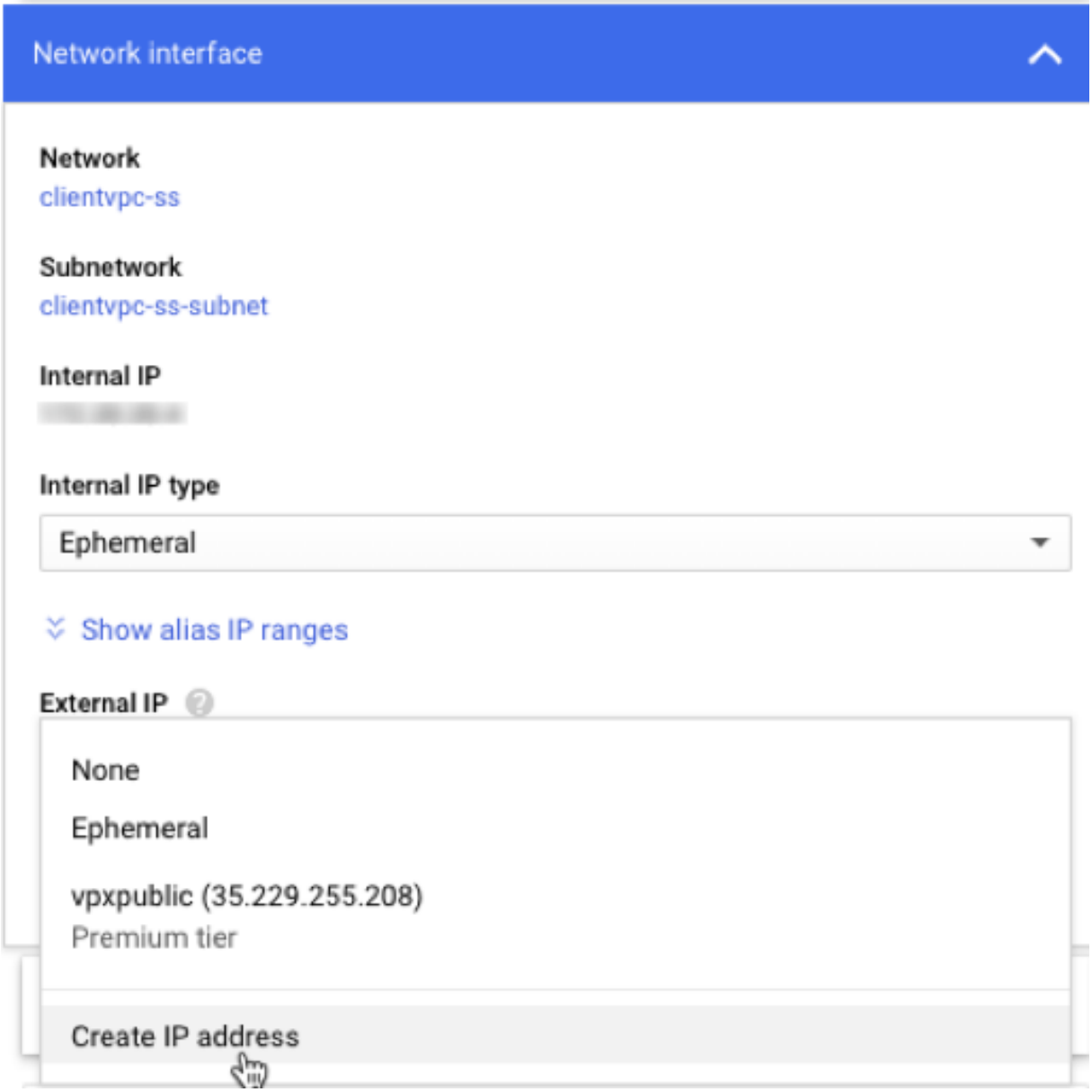
有关更多信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例中的 创建 **VPC** 网络 部分。

步骤 **2.** 步骤 **2.** 创建两个 **VPX** 实例

按照 场景中给出的步骤创建两个 VPX 实例：部署多 NIC、多 IP 独立 VPX 实例。

> 重要：
>
> 为主节点的客户端 IP 地址 (VIP) 分配静态外部 IP 地址。可以使用现有的预留 IP 地址或创建新的 IP 地址。要创建静态外部 IP 地址，请导航到 **Network interface**（网络接口）**> External IP**（外部 **IP**），单击 **Create IP**

address（创建 IP 地址）。



执行故障转移后，当旧主节点成为新辅助主节点时，静态外部 IP 地址将从旧主节点移动并连接到新的主节点。有关更多信息，请参阅 Google 云文档预留静态外部 IP 地址。

配置 VPX 实例后，您可以配置 VIP 和 SNIP 地址。有关更多信息，请参阅 配置 NetScaler 拥有的 IP 地址。

步骤 **3.** 步骤 **3.** 配置高可用性

在 Google Cloud Platform 上创建实例后，您可以使用适用于 CLI 的 NetScaler GUI 来配置 HA。

使用 **GUI** 配置高可用性　第 **1** 步。在两个实例中在 INC 模式下设置高可用性。

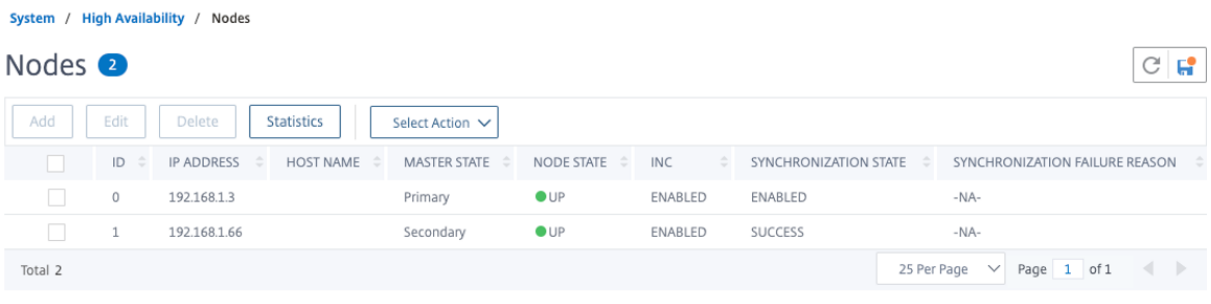
在主节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入辅助节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

在辅助节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入主节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

继续操作之前，请确保辅助节点的同步状态在 **Nodes**（节点）页面上显示为 **SUCCESS**（成功）。



> 注意：
>
> 现在，辅助节点具有与主节点相同的登录凭据。

第 **2** 步。在两个节点上添加虚拟 IP 和子网 IP。

在主节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 请按照以下步骤添加主 VIP 地址：

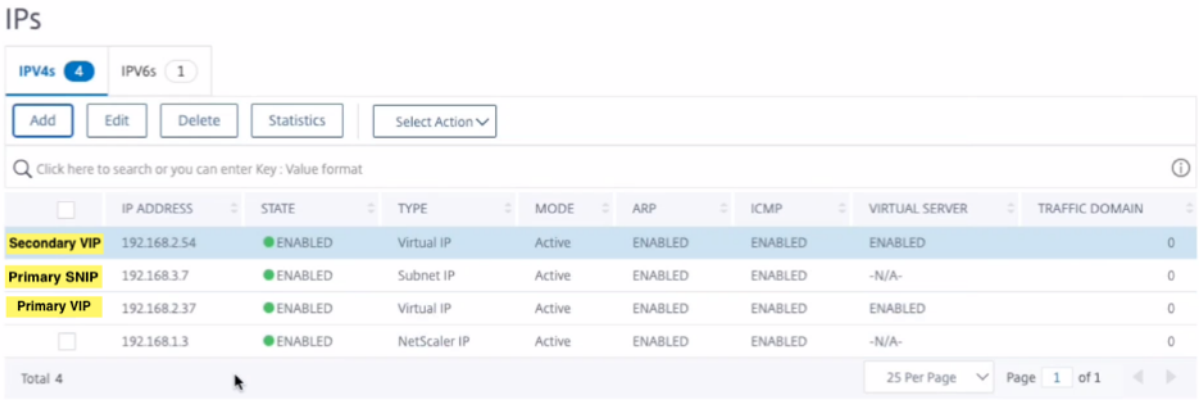
    a) 输入主实例的面向客户端的接口的内部 IP 地址以及为 VM 实例中的客户端子网配置的网络掩码。
    b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
    c) 单击创建。

3. 请按照以下步骤添加主 SNIP 地址：

   a) 输入主实例面向服务器的接口的内部 IP 地址和为主实例中的服务器子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。

4. 按照以下步骤添加辅助 VIP 地址：

   a) 输入辅助实例的面向客户端的接口的内部 IP 地址以及为 VM 实例中的客户端子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
   c) 单击创建。



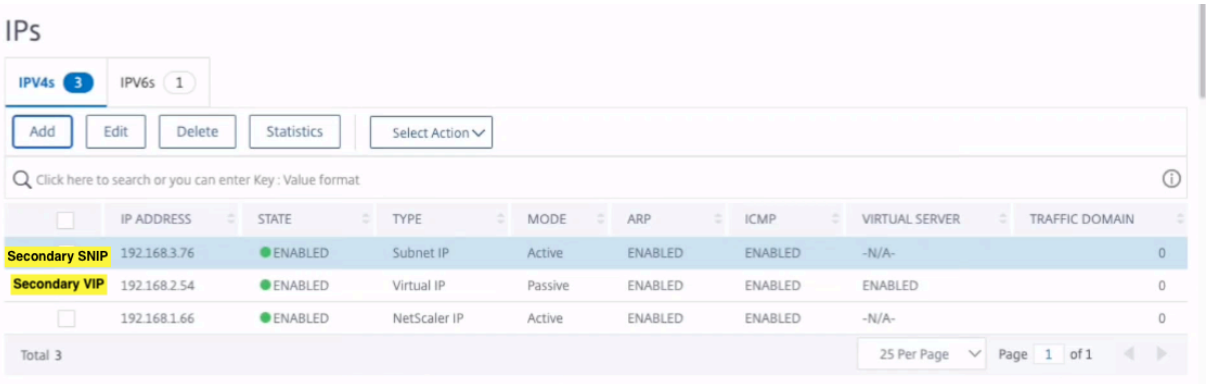
在辅助节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 按照以下步骤添加辅助 VIP 地址：

   a) 输入辅助实例的面向客户端的接口的内部 IP 地址以及为 VM 实例中的客户端子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。

3. 请按照以下步骤添加辅助 SNIP 地址：

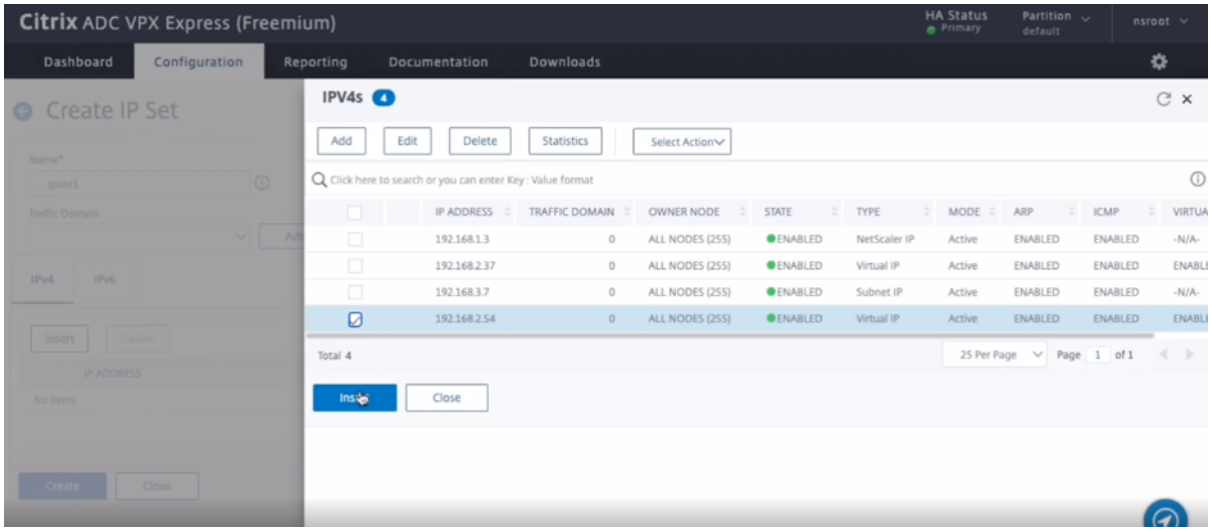
   a) 输入辅助实例的面向服务器的接口的内部 IP 地址以及为辅助实例中的服务器子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。



第 **3** 步。在两个实例上添加 IP 集并将 IP 集绑定到二级 VIP。

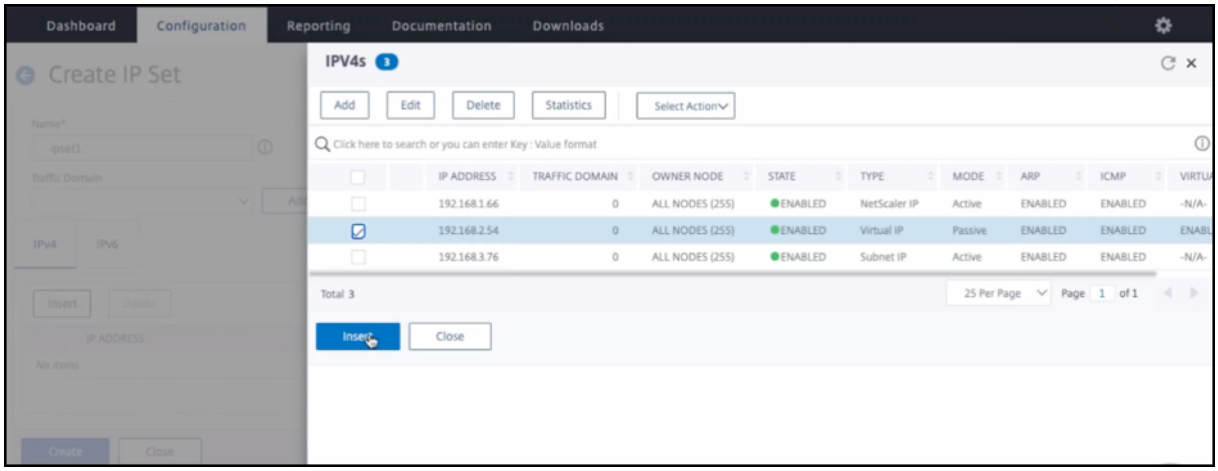
在主节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IP Sets**（**IP** 集）**> Add**（添加）。
2. 添加 IP 集名称，然后单击 **Insert**（插入）。
3. 在 **IPV4s**（IPv4）页面中，选择虚拟 IP（二级 VIP），然后单击 **Insert**（插入）。
4. 单击 **Create**（创建）以创建 IP 集。



在辅助节点上执行以下步骤：

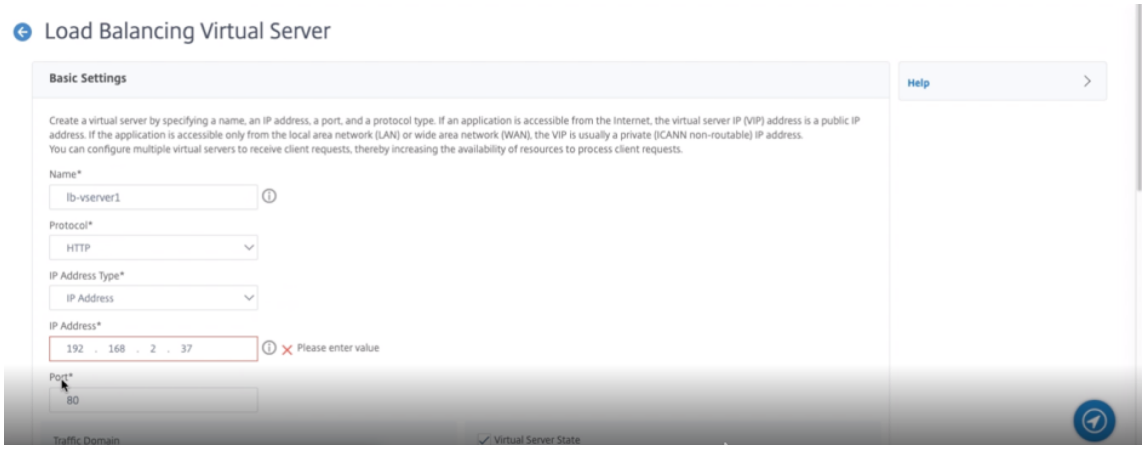
1. 导航到 **System**（系统）**> Network**（网络）**> IP Sets**（**IP** 集）**> Add**（添加）。
2. 添加 IP 集名称，然后单击 **Insert**（插入）。
3. 在 **IPV4s**（IPv4）页面中，选择虚拟 IP（二级 VIP），然后单击 **Insert**（插入）。
4. 单击 **Create**（创建）以创建 IP 集。



> 注意：
>
> 两个实例上的 IP 集名称必须相同。

第 **4** 步。在主实例上添加负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加）。
2. 添加“Name”（名称）、“Protocol”（协议）、“IP Address Type (IP Address)”（IP 地址类型 (IP 地址)）、“IP address (primary VIP)”（IP 地址 (主 VIP 地址)）和“Port”（端口）所需的值。



3. 单击 **More**（更多）。导航到 **IP Range IP Set Settings**（IP 范围 IP 集设置），从下拉菜单中选择 **IPSet** =（IP 集），并提供在步骤 **3** 中创建的 IP 集。
4. 单击 **OK**（确定）以创建负载平衡虚拟服务器。

第 **5** 步。在主节点上添加服务或服务组。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）**> Add**（添加）。
2. 添加“Service Name”（服务名称）、“IP Address”（IP 地址）、“Protocol”（协议）和“Port”（端口）所需的值，然后单击 **OK**（确定）。

第 **6** 步。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。
2. 选择在 **Step 4**（步骤 4）中配置的负载平衡虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **Service and Service Groups**（服务和服务组）选项卡中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。
4. 选择在 **Step 5**（步骤 5）中配置的服务，然后单击 **Bind**（绑定）。

步骤 7. 保存配置。执行强制故障转移后，辅助节点将成为新的主节点。旧的主 VIP 的外部静态 IP 将移至新的辅助 VIP。

使用 **CLI** 配置高可用性　第 **1** 步。在两个实例中在 INC 模式下设置高可用性。

在主节点上，键入以下命令。

```
add ha node 1 <sec_ip> -inc ENABLED
```

在辅助节点上，键入以下命令。

```
add ha node 1 <prim_ip> -inc ENABLED
```

sec_ip 是指辅助节点的管理 NIC 的内部 IP 地址。

prim_ip 是指主节点的管理 NIC 的专内部 IP 地址。

第 **2** 步。在两个节点上添加虚拟 IP 地址和子网 IP 地址。

在主节点上，键入以下命令。

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
```

primary_vip 是指主实例面向客户端的接口的内部 IP 地址。

secondary_vip 是指辅助实例面向客户端的接口的内部 IP 地址。

primary_snip 是指主实例面向服务器的接口的内部 IP 地址。

在辅助节点上，键入以下命令。

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
```

secondary_vip 是指辅助实例面向客户端的接口的内部 IP 地址。

secondary_snip 指辅助实例面向服务器的接口的内部 IP 地址。

第 **3** 步。在两个实例上添加 IP 集并将 IP 集绑定到二级 VIP。

在主节点上，键入以下命令：

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
```

在辅助节点上，键入以下命令：

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
```

> 注意：
>
> 两个实例上的 IP 集名称必须相同。

第 **4** 步。在主实例上添加一个虚拟服务器。

键入以下命令：

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <
   port> -ipset <ipset_name>
```

第 **5** 步。在主实例上添加服务或服务组。

键入以下命令：

```
add service <service_name> <service_ip_address> <protocol> <port>
```

第 **6** 步。将服务/服务组绑定到主实例上的负载平衡虚拟服务器。

键入以下命令：

```
bind <server_type> vserver <vserver_name> <service_name>
```

> 注意：
>
> 要保存配置，请键入命令 `save config`。否则，在您重新启动实例后，配置将丢失。

第 **7** 步。验证配置。

确保连接到主客户端 NIC 的外部 IP 地址在故障切换时移至辅助实例。

1. 向外部 IP 地址发出 cURL 请求，并确保其可以访问。
2. 在主实例上，执行故障转移：

   从 GUI 中，导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Action**（操作）**> Force Failover**（强制故障转移）。

   在 CLI 中，键入以下命令：

   ```
   force ha failover -f
   ```

   在 GCP 控制台上，转到“Secondary instance”（辅助实例）。故障转移后，外部 IP 地址必须移至辅助实例的客户端 NIC。
3. 向外部 IP 发出 cURL 请求并确保可以再次访问该 IP。

在 **Google** 云端平台上部署具有专用 **IP** 地址的单个 **NIC VPX** 高可用性对

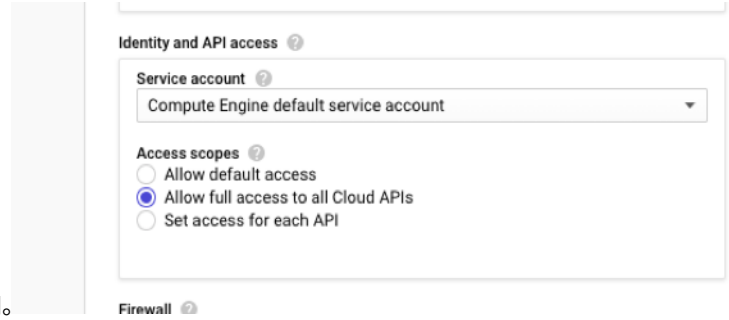
October 17, 2024

可以使用专用 IP 地址在 GCP 上部署单个 NIC VPX 高可用性对。必须在主节点上将客户端 IP (VIP) 地址配置为别名 IP 地址。故障转移后，客户端 IP 地址将移动到辅助节点，以便恢复流量。还必须将每个节点的子网 IP (SNIP) 地址配置为别名 IP 范围。

有关高可用性的更多信息，请参阅 高可用性。

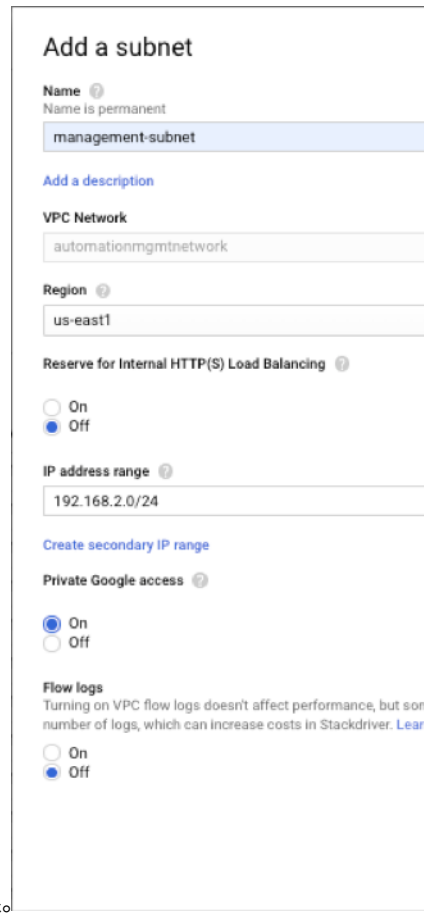
开始之前的准备工作

- 阅读 在 Google Cloud Platform上部署 NetScaler VPX 实例中提到的限制、硬件要求和注意事项。此信息也适用于高可用性部署。
- 为您的 GCP 项目启用 **Cloud Resource Manager API**。
- 在创建实例时允许对所有云 API 进行完全访问。



- 确保您的 GCP 服务账户具有以下 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
```

- 如果您的虚拟机无法访问 Internet，则必须在 VPC 子网上启用专用 **Google** 访问权限。
- 如果您已在主节点上配置了 GCP 转发规则，请阅读 GCP 上 VPX 高可用性对的转发规则支持 中提到的限制和要求，以便在故障转移时将它们更新为新的主节点。

如何在 **Google Cloud Platform** 上部署 **VPX** 高可用性对

以下是使用单个 NIC 部署 HA 对的步骤摘要：

1. 步骤 1. 创建一个 VPC 网络。
2. 在同一区域创建两个 VPX 实例（主节点和辅助节点）。它们可以位于同一个区域，也可以位于不同的区域。例如，Asia east-1a 和 Asia east-Ib。
3. 使用 NetScaler GUI 或 ADC CLI 命令在两个实例上配置 HA 设置。

步骤 **1.** 步骤 **1.** 创建一个 **VPC** 网络

要创建 VPC 网络，请执行以下步骤：

1. 登录 **Google** 控制台 **>** 网络连接 **> VPC** 网络 **>** 创建 **VPC** 网络。
2. 填写必填字段，然后单击 **Create**（创建）。

有关更多信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例中的 创建 **VPC** 网络 部分。

步骤 **2.** 步骤 **2.** 创建两个 **VPX** 实例

按照 场景中给出的步骤 1 到步骤 3 创建两个 VPX 实例：部署单 NIC、独立 VPX 实例。

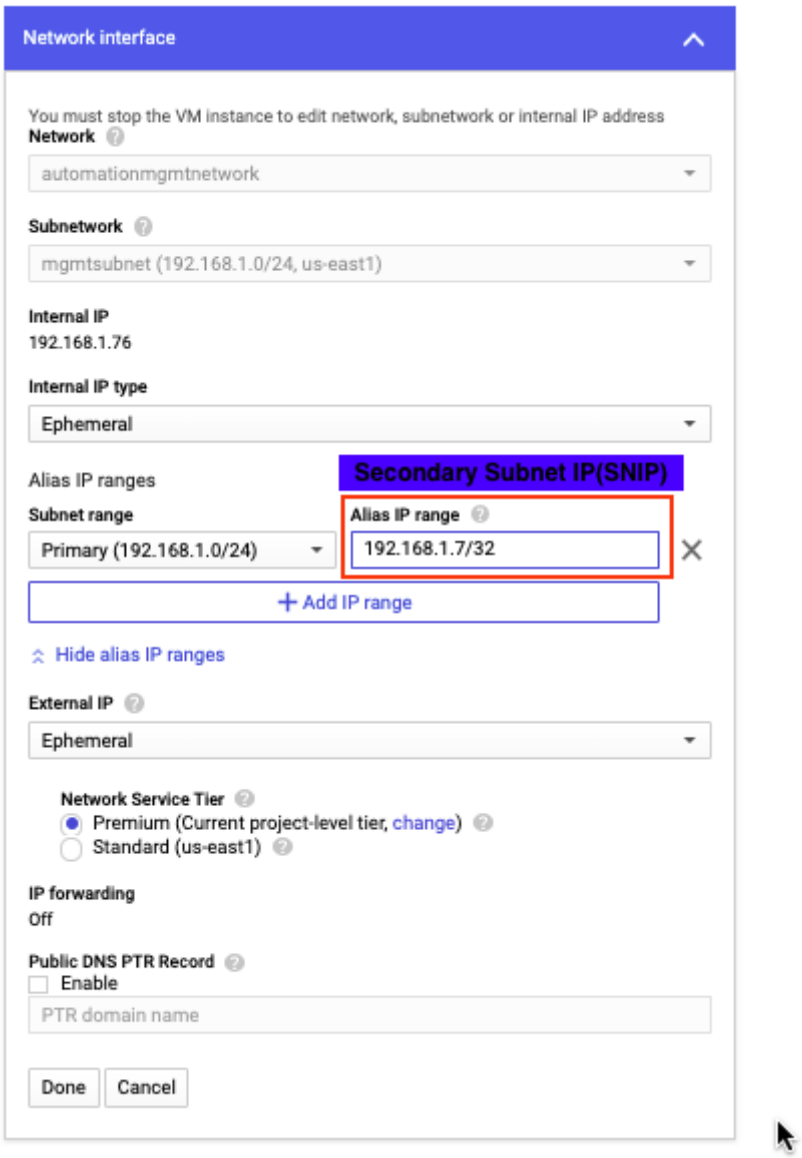
> 重要：
>
> 仅为主节点分配客户端别名 IP 地址，为主节点和辅助节点分配服务器别名 IP 地址。请勿使用 VPX 实例的内部 IP 地址来配置 VIP 或 SNIP。

要创建客户端和服务器别名 IP 地址，请在主节点上执行以下步骤：

1. 导航到 VM 实例，然后单击编辑。
2. 在“网络接口”窗口中，编辑客户端 (NIC0) 接口。
3. 在 **Alias IP range**（别名 IP 范围）字段中，输入客户端别名 IP 地址。
4. 单击“添加 **IP** 范围”并输入服务器别名 IP 地址。

要创建服务器别名 IP 地址，请在辅助节点上执行以下步骤：

1. 导航到 VM 实例，然后单击编辑。
2. 在“网络接口”窗口中，编辑客户端 (NIC0) 接口。
3. 在 **Alias IP range**（别名 IP 范围）字段中，输入服务器别名 IP 地址。



故障切换后，当旧的主服务器变为新的辅助服务器时，客户端别名 IP 地址将从旧的主服务器移出并连接到新的主服务器。

配置 VPX 实例后，可以配置虚拟 IP 地址 (VIP) 和子网 IP (SNIP) 地址。有关更多信息，请参阅 配置 NetScaler 拥有的 IP 地址。

步骤 **3.** 步骤 **3.** 配置高可用性

在 Google Cloud Platform 上创建实例后，您可以使用 NetScaler GUI 或 CLI 配置高可用性。

使用 **GUI** 配置高可用性

第 **1** 步。在两个节点上以 INC 启用模式设置高可用性。

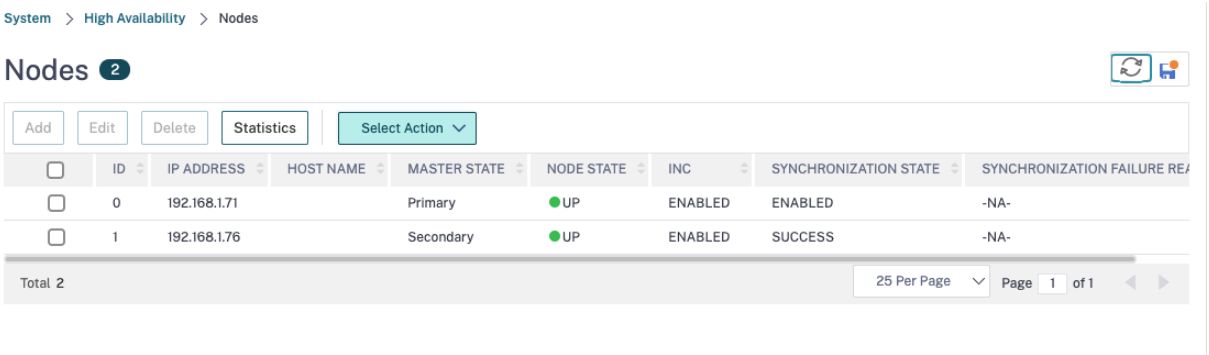
在主节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入辅助节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

在辅助节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入主节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

继续操作之前，请确保辅助节点的同步状态在 **Nodes**（节点）页面上显示为 **SUCCESS**（成功）。



> 注意：
>
> 当辅助节点与主节点同步后，辅助节点具有与主节点相同的登录凭据。

第 **2** 步。在两个节点上添加虚拟 IP 和子网 IP。

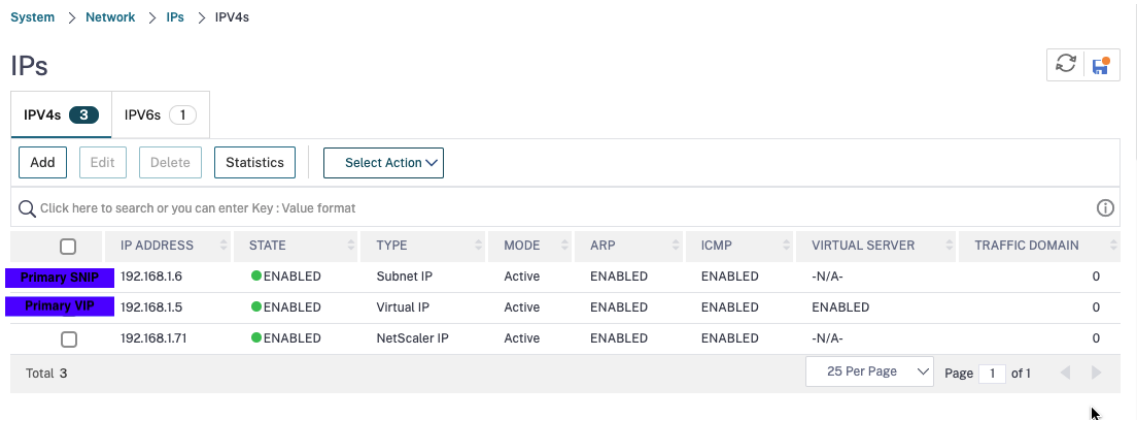
在主节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 要创建客户端别名 IP (VIP) 地址，请执行以下操作：

a) 输入为主虚拟机实例中的 VPC 子网配置的客户端别名 IP 地址和网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
c) 单击创建。

3. 要创建服务器别名 IP (SNIP) 地址，请执行以下操作：

a) 输入为主虚拟机实例中的 VPC 子网配置的服务器别名 IP 地址和网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
c) 单击创建。



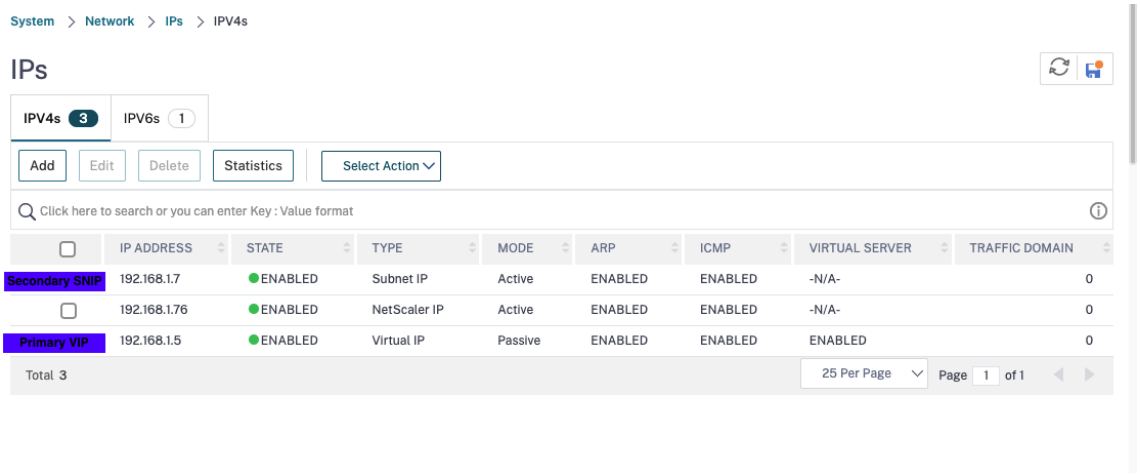
在辅助节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 要创建客户端别名 IP (VIP) 地址，请执行以下操作：

a) 输入为主虚拟机实例的 VPC 子网配置的客户端别名 IP 地址和网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
c) 单击创建。

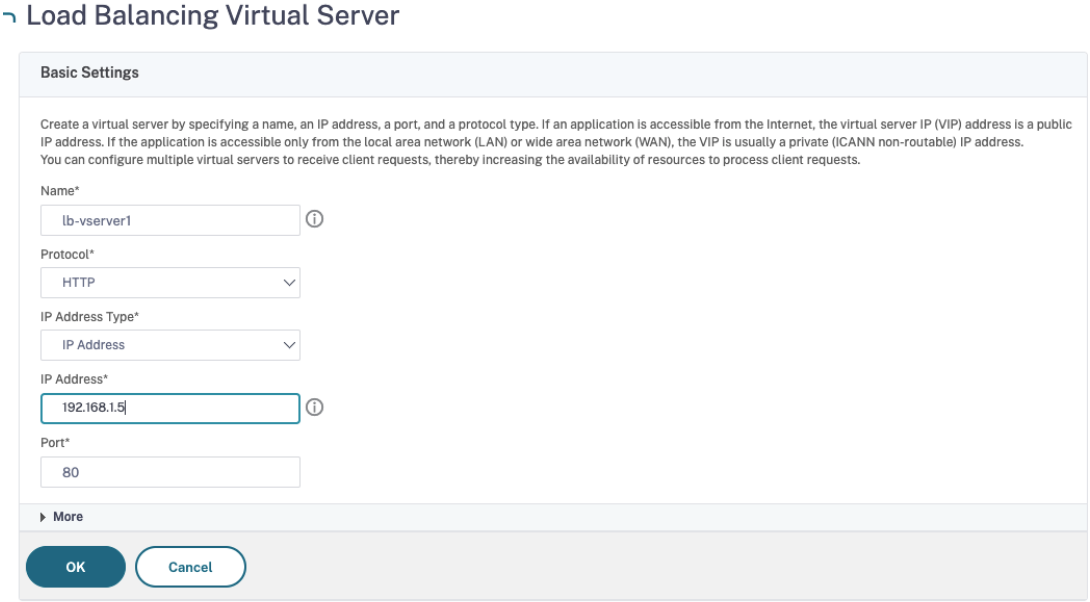
3. 要创建服务器别名 IP (SNIP) 地址，请执行以下操作：

a) 输入为辅助虚拟机实例的 VPC 子网配置的服务器别名 IP 地址和网络掩码。
b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
c) 单击创建。



第 **3** 步。在主节点上添加负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加）。
2. 添加“Name”（名称）、“Protocol”（协议）、“IP Address Type (IP Address)”（IP 地址类型 (IP 地址)）、“IP Address (primary client alias IP address)”（IP 地址 (主客户端别名 IP 地址)）和“Port”（端口）所需的值，然后单击 **OK**（确定）。



第 **4** 步。在主节点上添加服务或服务组。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）**> Add**（添加）。
2. 添加“Service Name”（服务名称）、“IP Address”（IP 地址）、“Protocol”（协议）和“Port”（端口）所需的值，然后单击 **OK**（确定）。

第 **5** 步。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。
2. 选择在 **Step 3**（步骤 3）中配置的负载平衡虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **Service and Service Groups**（服务和服务组）选项卡中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。
4. 选择在 **Step 4**（步骤 4）中配置的服务，然后单击 **Bind**（绑定）。

第 **6** 步。步骤 7. 保存配置。

执行强制故障转移后，辅助节点将成为新的主节点。旧主服务器的客户端别名 IP (VIP) 移至新的主服务器。

使用 **CLI** 配置高可用性

第 **1** 步。使用 NetScaler CLI 在两个实例中以已启用 **INC** 模式设置高可用性。

在主节点上，键入以下命令。

```
add ha node 1 <sec_ip> -inc ENABLED
```

在辅助节点上，键入以下命令。

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` 是指辅助节点的管理 NIC 的内部 IP 地址。

`prim_ip` 是指主节点的管理 NIC 的专内部 IP 地址。

第 **2** 步。在主节点和辅助节点上添加 VIP 和 SNIP。

在主节点上键入以下命令：

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> 注意：
>
> 输入为虚拟机实例中的客户端子网配置的别名 IP 地址和网络掩码。

```
add ns ip <primary_server_alias_ip> <subnet> -type SNIP
```

在辅助节点上键入以下命令：

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> 注意：
>
> 输入为虚拟机实例中的客户端子网配置的别名 IP 地址和网络掩码。

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```


> 注意：
>
> 输入为虚拟机实例中的服务器子网配置的别名 IP 地址和网络掩码。

第 **3** 步。在主节点上添加虚拟服务器。

键入以下命令：

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```

第 **4** 步。在主节点上添加服务或服务组。

键入以下命令：

```
add service <service_name> <service_ip_address> <protocol> <port>
```

第 **5** 步。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

键入以下命令：

```
bind <server_type> vserver <vserver_name> <service_name>
```

> 注意：
>
> 要保存配置，请键入命令 `save config`。否则，在您重新启动实例后，配置将丢失。

在 **Google** 云端平台上部署具有专用 **IP** 地址的 **VPX** 高可用性对

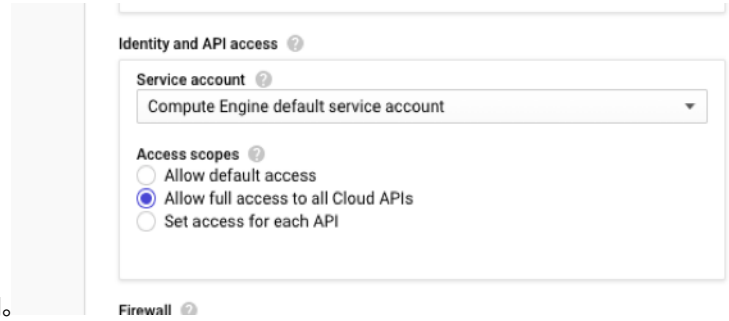
October 17, 2024

可以使用专用 IP 地址在 GCP 上部署 VPX 高可用性对。必须将客户端 IP (VIP) 配置为主节点上的别名 IP 地址。故障转移后，客户端 IP 地址将移动到辅助节点，以便恢复流量。

有关高可用性的更多信息，请参阅 高可用性。

开始之前的准备工作

- 阅读 在 Google Cloud Platform上部署 NetScaler VPX 实例中提到的限制、硬件要求和注意事项。此信息也适用于高可用性部署。
- 为您的 GCP 项目启用 **Cloud Resource Manager API**。



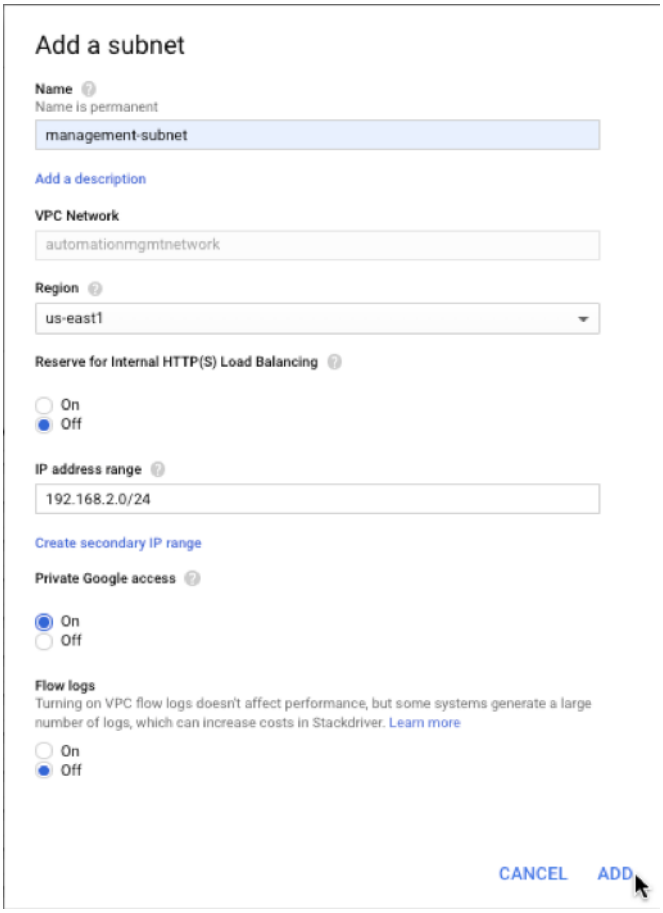
- 在创建实例时允许对所有云 API 进行完全访问。
- 确保您的 GCP 服务账户具有以下 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
```

- 如果您在管理接口以外的接口上配置了外部 IP 地址，请确保您的 GCP 服务帐户具有以下额外的 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.addresses.use"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
]
```

- 如果您的 VM 没有 Internet 访问权限，则必须在管理子网上启用 **Private Google Access**（专用 Google 访



问权限)。

- 如果您已在主节点上配置了 GCP 转发规则，请阅读 GCP 上 VPX 高可用性对的转发规则支持 中提到的限制和要求，以便在故障转移时将它们更新为新的主节点。

如何在 **Google Cloud Platform** 上部署 **VPX** 高可用性对

以下是高可用性部署步骤的摘要：

1. 在同一地理地区创建多个 VPC 网络。例如，Asia-east。
2. 在同一地理区域创建两个 VPX 实例（主节点和辅助节点）。它们可以位于同一个区域，也可以位于不同的区域。例如，Asia east-1a 和 Asia east-Ib。
3. 使用 NetScaler GUI 或 ADC CLI 命令在两个实例上配置高可用性设置。

步骤 **1.** 步骤 **1.** 创建 **VPC** 网络

根据您的要求创建 VPC 网络。Citrix 建议您创建三个 VPC 网络，分别用于与管理 NIC、客户端 NIC 和服务器 NIC 关联。

要创建 VPC 网络，请执行以下步骤：

1. 登录 **Google** 控制台 **> Networking**（网络连接）**> VPC network**（**VPC** 网络）**> Create VPC Network**（创建 **VPC** 网络）。
2. 填写必填字段，然后单击 **Create**（创建）。

有关更多信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例中的 创建 **VPC** 网络 部分。

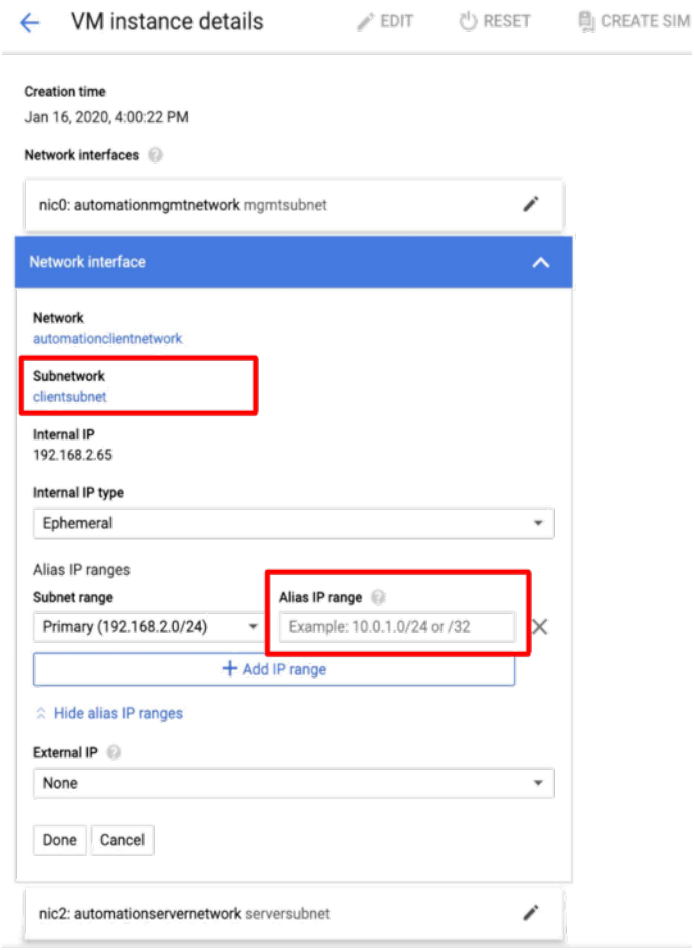
步骤 **2.** 步骤 **2.** 创建两个 **VPX** 实例

按照 场景中给出的步骤创建两个 VPX 实例：部署多 NIC、多 IP 独立 VPX 实例。

> 重要：
>
> 为主节点分配客户端别名 IP 地址。不要使用 VPX 实例的内部 IP 地址配置 VIP。

要创建客户端别名 IP 地址，请执行以下步骤：

1. 导航到 VM 实例，然后单击编辑。
2. 在 **Network Interface**（网络接口）窗口中，编辑客户端接口。
3. 在 **Alias IP range**（别名 IP 范围）字段中，输入客户端别名 IP 地址。



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	–	adc-ha–instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	–	None			View details

故障转移之后，当旧主服务器成为新的辅助服务器时，别名 IP 地址将从旧主 IP 地址移动并附加到新的主服务器。

配置 VPX 实例后，可以配置虚拟 IP 地址 (VIP) 和子网 IP (SNIP) 地址。有关更多信息，请参阅 配置 NetScaler 拥有的 IP 地址。

步骤 **3.** 步骤 **3.** 配置高可用性

在 Google Cloud Platform 上创建实例后，您可以使用 NetScaler GUI 或 CLI 配置高可用性。

使用 **GUI** 配置高可用性

第 **1** 步。在两个节点上以 INC 启用模式设置高可用性。

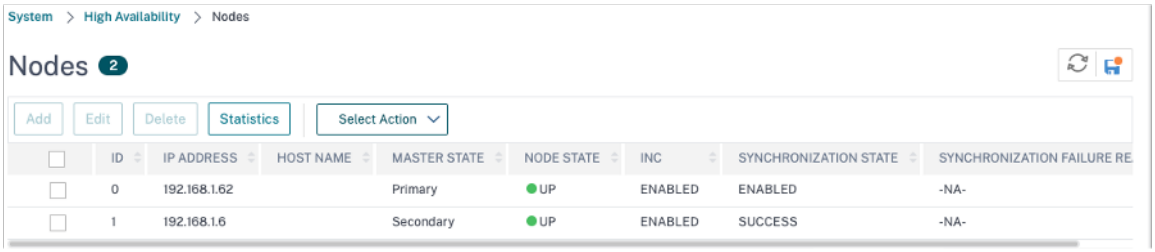
在主节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入辅助节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

在辅助节点上执行以下步骤：

1. 使用用户名 `nsroot` 以及 GCP 控制台中的节点的实例 ID 作为密码登录实例。
2. 导航到 **Configuration**（配置）**> System**（系统）**> High Availability**（高可用性）**> Nodes**（节点），然后单击 **Add**（添加）。
3. 在 **Remote Node IP address**（远程节点 IP 地址）字段中，输入主节点的管理 NIC 的专用 IP 地址。
4. 选择 **Turn on INC (Independent Network Configuration) mode on self node**（在自助节点上打开 INC (Independent Network Configuration) 模式）复选框。
5. 单击创建。

继续操作之前，请确保辅助节点的同步状态在 **Nodes**（节点）页面上显示为 **SUCCESS**（成功）。

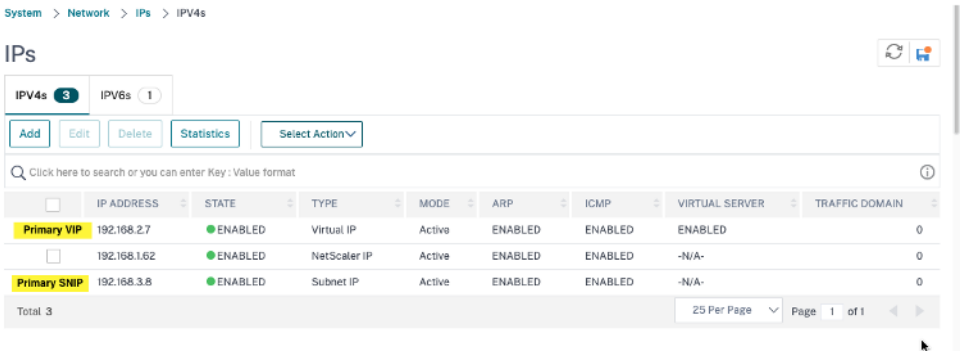


> 注意：
>
> 当辅助节点与主节点同步后，辅助节点具有与主节点相同的登录凭据。

第 **2** 步。在两个节点上添加虚拟 IP 和子网 IP。

在主节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 要创建客户端别名 IP (VIP) 地址，请执行以下操作：
   a) 输入 VM 实例中为客户端子网配置的别名 IP 地址和子网掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Virtual IP**（虚拟 IP）。
   c) 单击创建。
3. 要创建服务器 IP (SNIP) 地址：
   a) 输入主实例面向服务器的接口的内部 IP 地址和为服务器子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。

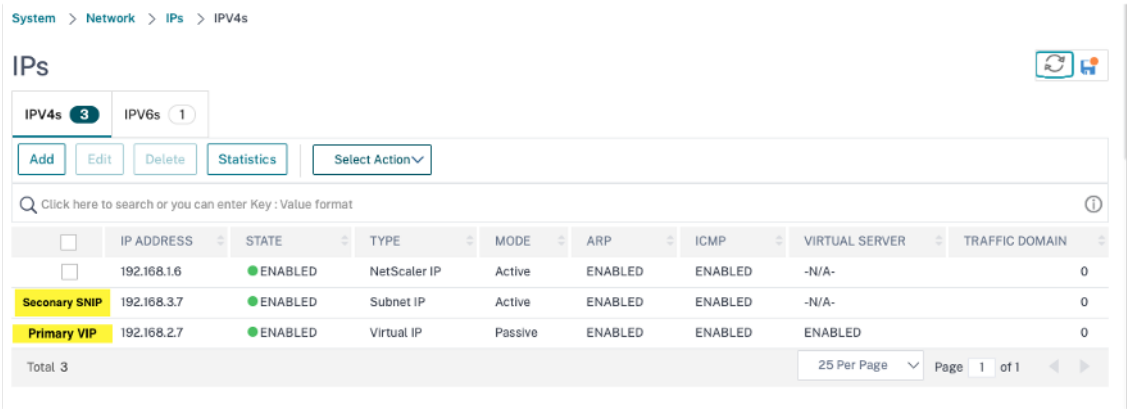


在辅助节点上执行以下步骤：

1. 导航到 **System**（系统）**> Network**（网络）**> IPs**（**IP**）**> IPv4s**（**IPv4**），然后单击 **Add**（添加）。
2. 要创建客户端别名 IP (VIP) 地址，请执行以下操作：
   a) 输入为主虚拟机实例上的客户端子网配置的别名 IP 地址和网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。

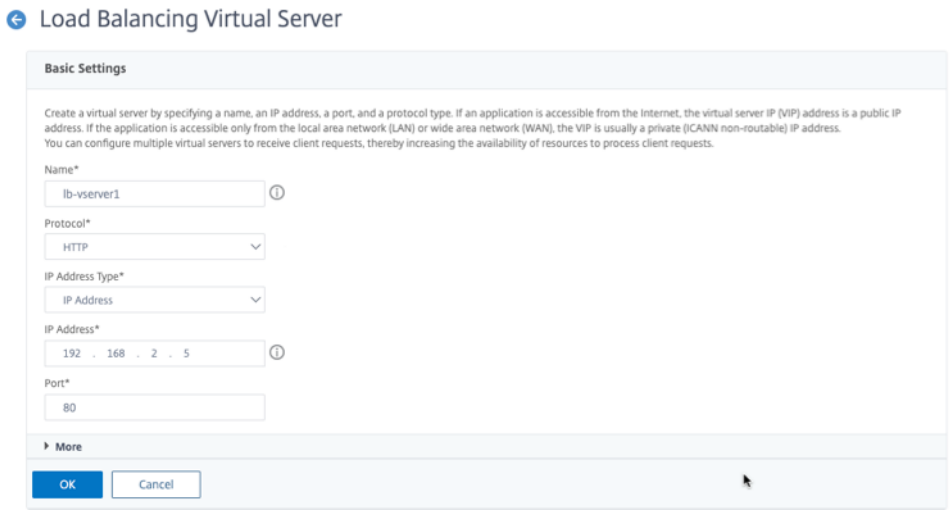
3. 要创建服务器 IP (SNIP) 地址：

   a) 输入辅助实例面向服务器的接口的内部 IP 地址和为服务器子网配置的网络掩码。
   b) 在 **IP Type**（IP 类型）字段中，从下拉菜单中选择 **Subnet IP**（子网 IP）。
   c) 单击创建。



第 **3** 步。在主节点上添加负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加）。
2. 添加“Name”（名称）、“Protocol”（协议）、“IP Address Type (IP Address)”（IP 地址类型 (IP 地址)）、“IP Address (primary client alias IP address)”（IP 地址 (主客户端别名 IP 地址)）和“Port”（端口）所需的值，然后单击 **OK**（确定）。



第 **4** 步。在主节点上添加服务或服务组。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）**> Add**（添加）。
2. 添加“Service Name”（服务名称）、“IP Address”（IP 地址）、“Protocol”（协议）和“Port”（端口）所需的值，然后单击 **OK**（确定）。

第 **5** 步。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。
2. 选择在 **Step 3**（步骤 3）中配置的负载平衡虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **Service and Service Groups**（服务和服务组）选项卡中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。
4. 选择在 **Step 4**（步骤 4）中配置的服务，然后单击 **Bind**（绑定）。

第 **5** 步。步骤 7. 保存配置。

执行强制故障转移后，辅助节点将成为新的主节点。来自旧的主服务器的客户端别名 IP (VIP) 和服务器别名 IP (SNIP) 移动到新的主服务器。

使用 **CLI** 配置高可用性

第 **1** 步。使用 NetScaler CLI 在两个实例中以已启用 **INC** 模式设置高可用性。

在主节点上，键入以下命令。

```
add ha node 1 <sec_ip> -inc ENABLED
```

在辅助节点上，键入以下命令。

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` 是指辅助节点的管理 NIC 的内部 IP 地址。

`prim_ip` 是指主节点的管理 NIC 的专内部 IP 地址。

第 **2** 步。在两个节点上添加 VIP 和 SNIP。

在主节点上键入以下命令：

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

> 注意：
>
> 输入 VM 实例中为客户端子网配置的别名 IP 地址和子网掩码。

```
add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_snip` 是指主实例面向服务器的接口的内部 IP 地址。

在辅助节点上键入以下命令：

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```


> 注意：
>
> 输入为主虚拟机实例上的客户端子网配置的别名 IP 地址和网络掩码。

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_snip` 是指辅助实例的面向服务器的接口的内部 IP 地址。

> 注意：
>
> 输入为虚拟机实例中服务器子网配置的 IP 地址和网络掩码。

第 3 步。在主节点上添加虚拟服务器。

键入以下命令：

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
```

第 4 步。在主节点上添加服务或服务组。

键入以下命令：

```
add service <service_name> <service_ip_address> <protocol> <port>
```

第 5 步。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

键入以下命令：

```
bind <server_type> vserver <vserver_name> <service_name>
```

> 注意：
>
> 要保存配置，请键入命令 `save config`。否则，在您重新启动实例后，配置将丢失。

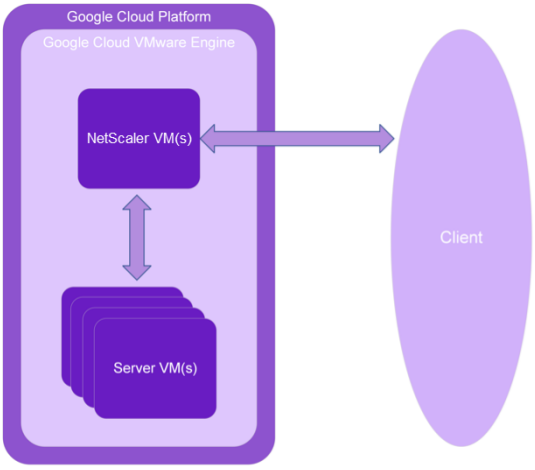
在 Google Cloud VMware Engine 上安装 NetScaler VPX 实例

October 17, 2024

Google Cloud VMware Engine (GCVE) 为您提供包含 vSphere 群集的私有云，这些群集由专用的裸机 Google Cloud Platform 初始部署的最低限度为三台主机，但可以一次添加一台额外的主机。初始部署的最低要求是三台主机，但可以一次添加一台主机。所有预配的私有云都有 vCenter Server、vSAN、vSphere 和 NSX-T。

GCVE 使您能够在 Google Cloud Platform 上使用所需数量的 ESX 主机创建云软件定义的数据中心 (SDDC)。GCVE 支持 NetScaler VPX 部署。GCVE 提供的用户界面与本地 vCenter 相同。其功能与基于 ESX 的 NetScaler VPX 部署相同。

下图显示了 Google 云端平台上的 GCVE，管理员或客户可以通过 Internet 访问该平台。管理员可以使用 GCVE 创建、管理和配置工作负载或服务器虚拟机。管理员可以使用 OpenVPN 连接访问 GCVE 基于 Web 的 vCenter 和 NSX-T Manager。您可以使用 vCenter 在 GCVE 中创建 NetScaler VPX 实例（独立或 HA 对）和服务器虚拟机，并使用 NSX-T 管理器管理相应的网络。GCVE 上的 NetScaler VPX 实例的工作原理类似于本地 VMware 主机群集。GCVE 可以通过连接到管理基础设施的 OpenVPN 进行管理。



必备条件

在开始安装虚拟设备之前，请执行以下操作：

- 有关 Google Cloud VMware Engine 及其必备条件的更多信息，请参阅 Google Cloud VMware Engine 文档。
- 有关部署 Google Cloud VMware Engine 的更多信息，请参阅部署 Google Cloud VMware Engine 私有云。
- 有关使用点对点 VPN 网关连接到私有云以访问和管理 Google Cloud VMware Engine 的更多信息，请参阅访问 Google Cloud VMware Engine 私有云。
- 在 VPN 客户端计算机上，下载 NetScaler VPX 设备安装文件。
- 在虚拟机连接到的 VMware SDDC 上创建适当的 NSX-T 网段。有关更多信息，请参阅 在 Google Cloud VMware 引擎中添加网络分段。
- 获取 VPX 许可证文件。有关 NetScaler VPX 实例许可证的更多信息，请参阅 许可概述。
- 创建或迁移到 GCVE 私有云的虚拟机 (VM) 必须连接到网络分段。

VMware 云硬件要求

下表列出了 VMware SDDC 必须为每个 VPX nCore 虚拟设备提供的虚拟计算资源。

表 1. VPX 功能列表 表 2. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

组件	要求
内存	2 GB
虚拟 CPU (vCPU)	2
虚拟网络接口	在 VMware SDDC 中，如果 VPX 硬件升级到版本 7 或更高版本，则最多可以安装 10 个虚拟网络接口。
磁盘空间	20 GB

> 注意：
>
> 这是对虚拟机管理程序的磁盘要求的补充。

要在生产中使用 VPX 虚拟设备，必须保留完整的内存分配。

OVF Tool 1.0 系统要求

OVF 工具是可在 Windows 和 Linux 操作系统上运行的客户端应用程序。下表描述了安装 OVF 工具的最低系统要求。

表 2. VPX 功能列表 表 4. 安装 OVF 工具的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。
CPU	最低 750 MHz，建议使用 1 GHz 或速度更快的 CPU
RAM	最低 1 GB；建议使用 2 GB
NIC	100 Mbps 或速度更高的 NIC

有关安装 OVF 的信息，请在 http://kb.vmware.com/ 上搜索“OVF Tool User Guide”（《OVF 工具用户指南》）PDF 文件。

下载 NetScaler VPX 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例设置包遵循开放虚拟机 (OVF) 格式标准。可以从 Citrix Web 站点下载文件。需要使用 Citrix 帐户进行登录。如果您没有 Citrix 帐户，请访问 http://www.citrix.com的主页。单击 **New Users link**（新建用户链接），然后按照说明创建新的 Citrix 帐户。

登录后，从 Citrix 主页浏览以下路径：

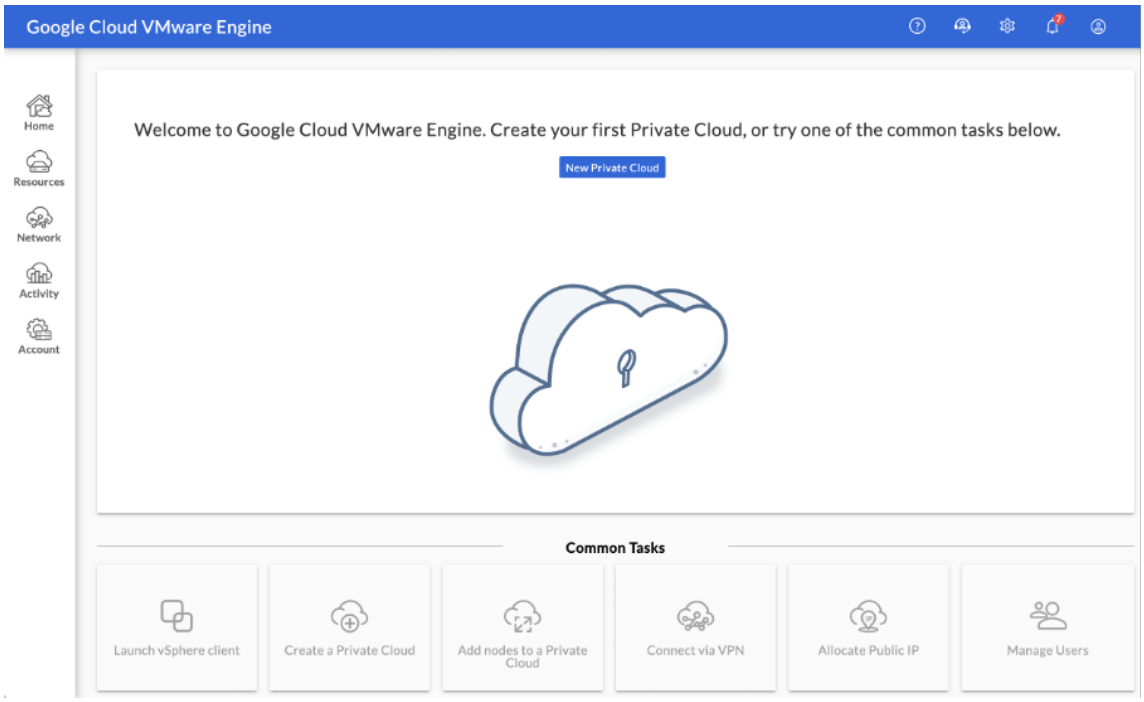
Citrix.com > 下载 **> NetScaler >** 虚拟设备。

将以下文件复制到 ESX 服务器所在网络中的一个工作站。将所有三个文件复制到同一个文件夹中。

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk（例 如 NSVPX-ESX-13.0-79.64-disk1.vmdk）
- NSVPX-ESX-<release number>-<build number>.ovf （例如 NSVPX-ESX-13.0-79.64.ovf）
- NSVPX-ESX-<release number>-<build number>.mf（例如 NSVPX-ESX-13.0-79.64.mf）

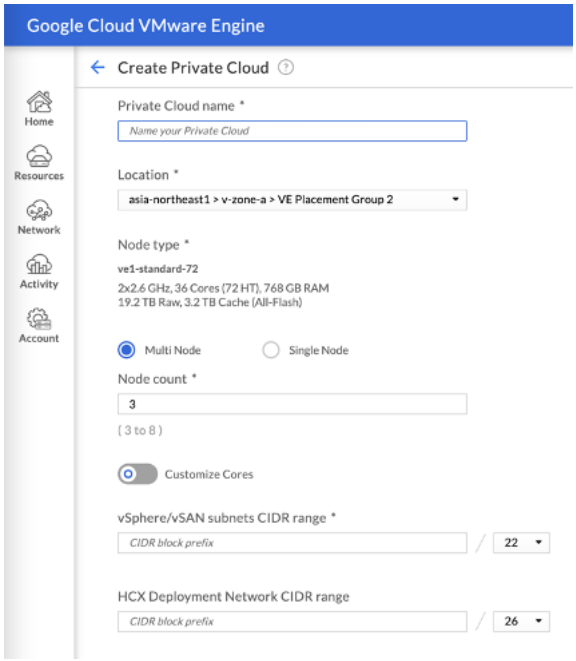
部署 **Google Cloud VMware Engine**

1. 登录您的 GCVE 门户，然后导航到 主页。

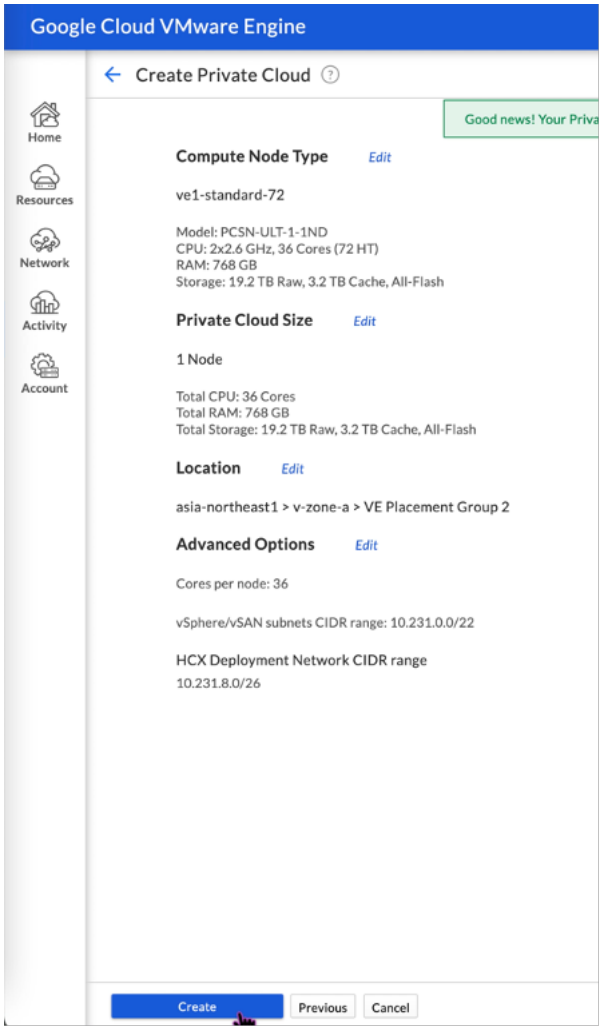


2. 在“新建私有云”页面中，输入以下详细信息：

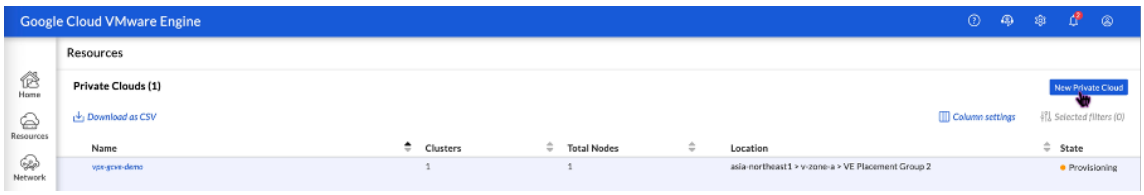
   - 至少选择 3 个 ESXi 主机以创建私有云的默认群集。
   - 对于 **vSphere/vSAN** 子网 **CIDR** 范围 字段，使用 /22 地址空间。
   - 对于 **HCX** 部署网络 **CIDR** 范围 字段，使用 /26 地址空间。
   - 对于虚拟网络，请确保 CIDR 范围不与您的任何本地或其他 GCP 子网（虚拟网络）重叠。



3. 单击“查看并创建”。
4. 检查设置。如果您需要更改任何设置，请单击“上一步”。



5. 单击创建。私有云配置过程启动。配置私有云最多可能需要两个小时。
6. 转到 资源 以验证创建的私有云。

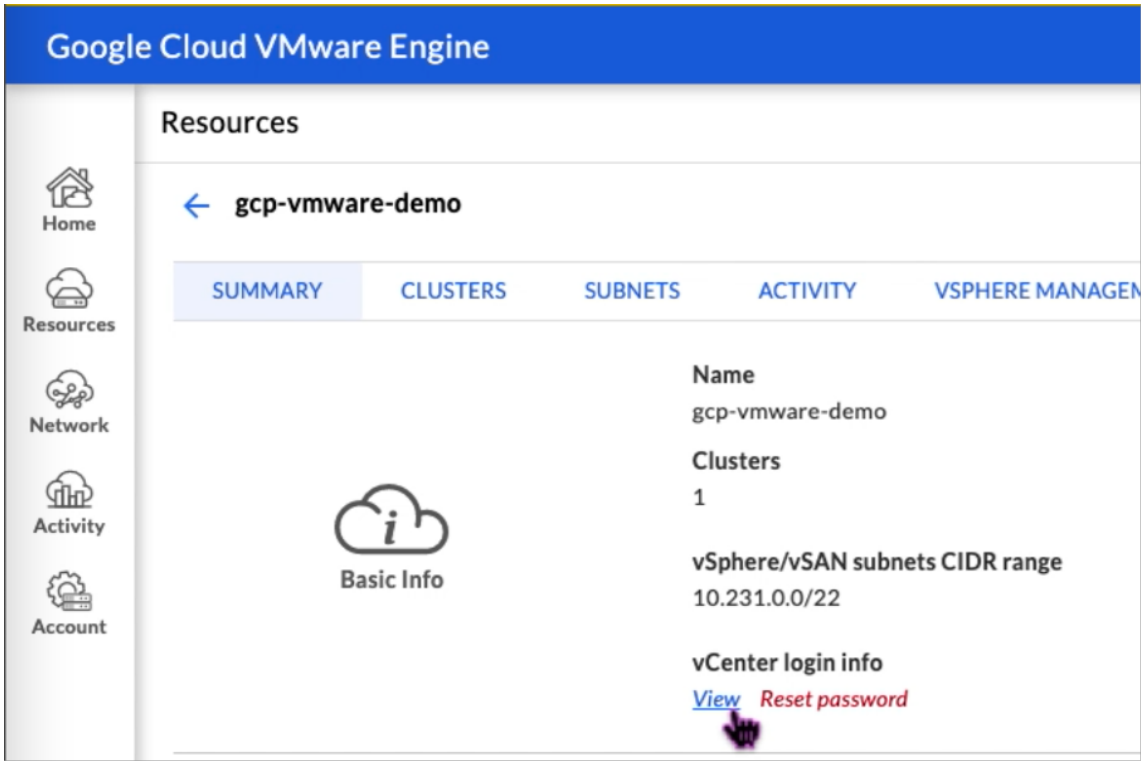


7. 要访问此资源，必须使用点对点 VPN 连接到 GCVE。有关更多信息，请参阅以下文档：

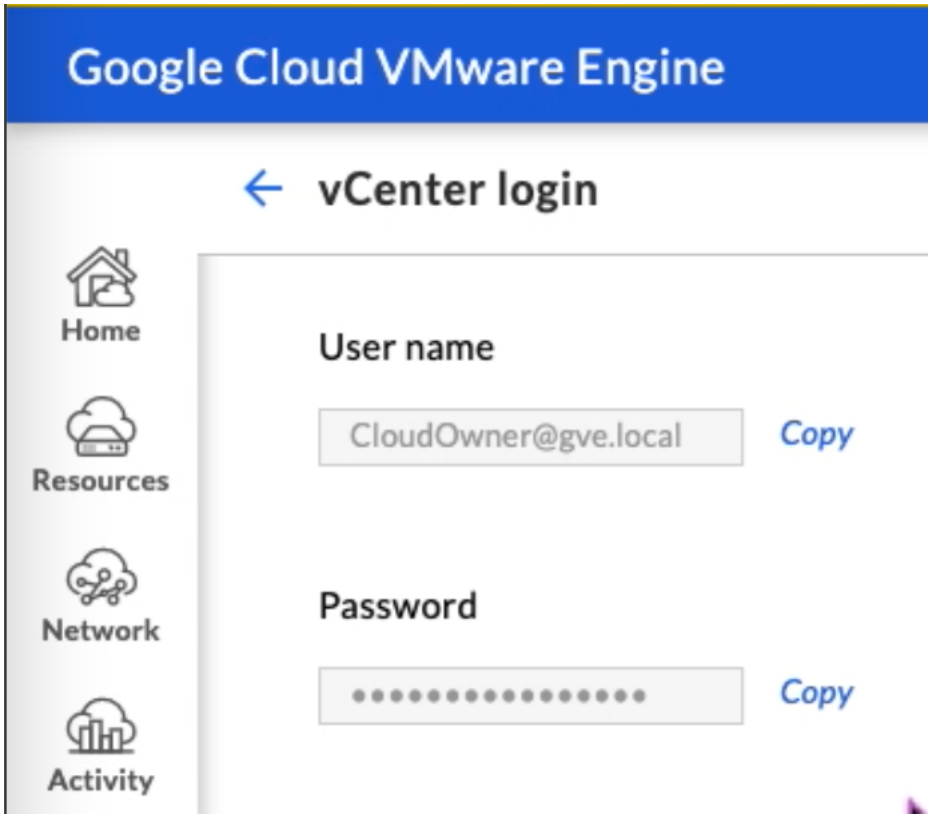
   - VPN 网关
   - 使用 VPN 进行连接

访问私有云 **vCenter** 门户

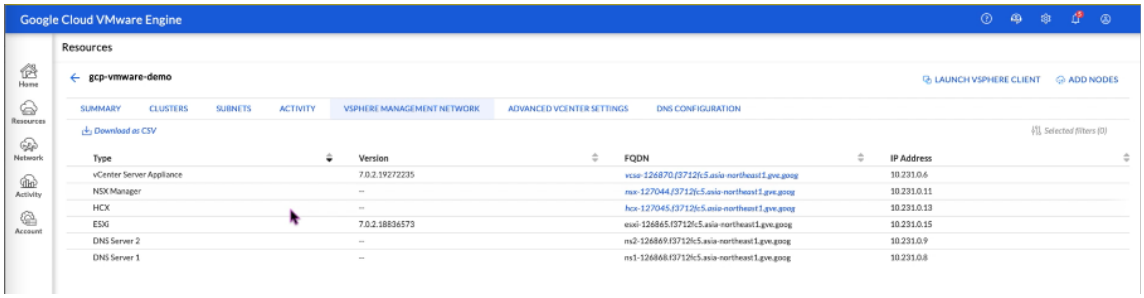
1. 导航到您的 Google Cloud VMware Engine 私有云。在“摘要”选项卡的“**vCenter** 登录信息”下，单击“查看”。



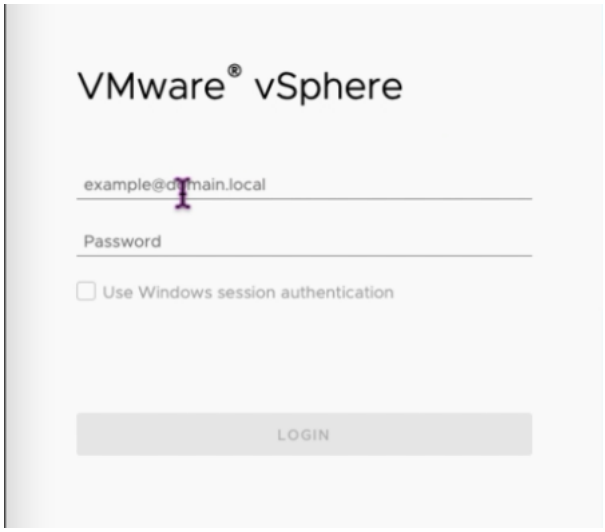
2. 记下 vCenter 凭据。



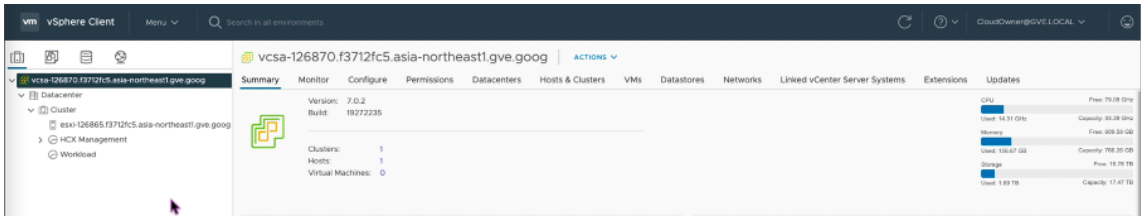
3. 单击 **LAUNCH VSPHERE CLIENT** 启动 vSphere 客户端，或者导航到 **VSPHERE** 管理网络，然后单击 **vCenter Server** 设备 FQDN。



4. 使用本过程步骤 2 中记录的 vCenter 凭据登录 VMware vSphere。



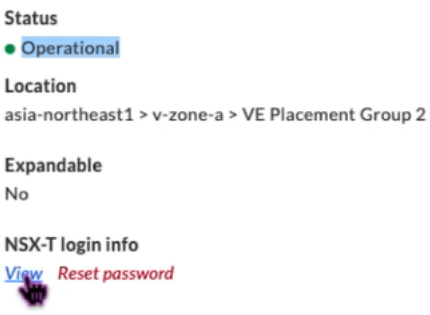
5. 在 vSphere 客户端中，您可以验证在 GCVE 门户中创建的 ESXi 主机。



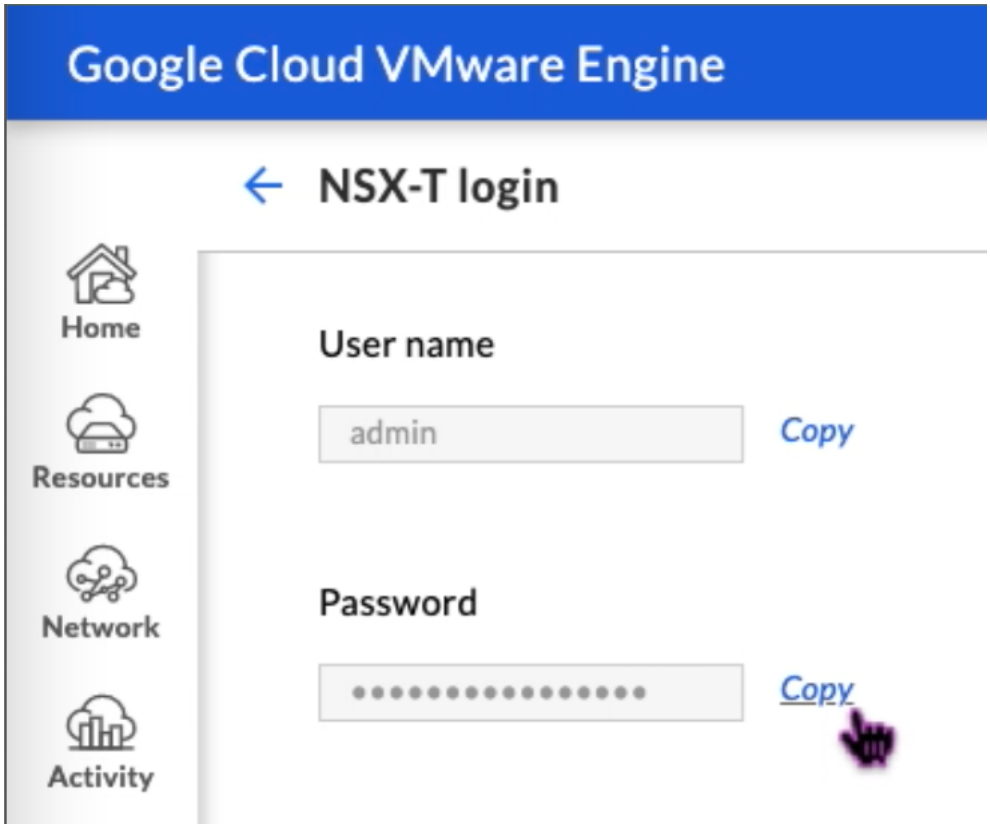
在 **GCVE NSX-T** 门户中创建 **NSX-T** 分段

您可以在 Google Cloud VMware Engine 控制台中通过 NSX 管理器创建和配置 NSX-T 分段。这些网段连接到默认的 Tier-1 网关，这些网段上的工作负载可以实现东西和南北连接。创建分段后，它将显示在 vCenter 中。

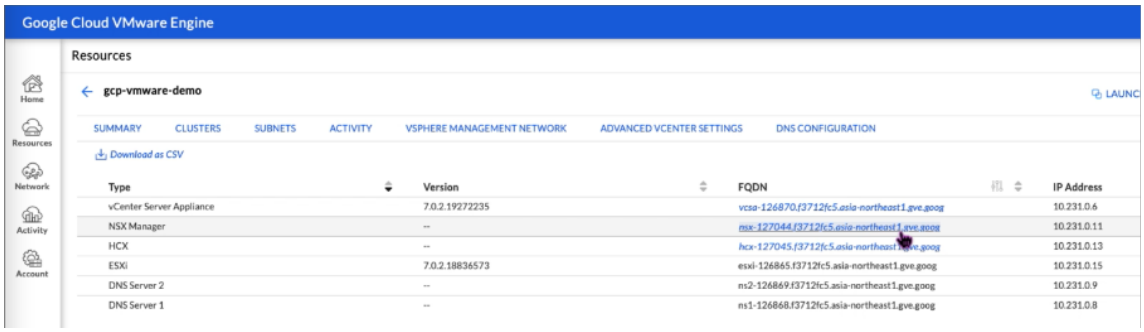
1. 在您的 GCVE 私有云中，在“摘要”**->**“**NSX-T** 登录信息”下，选择“查看”。



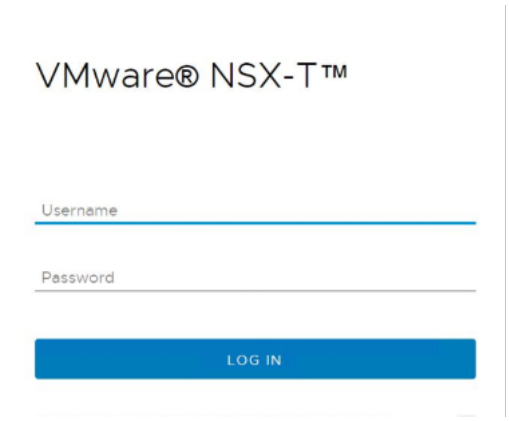
2. 记下 NSX-T 证书。



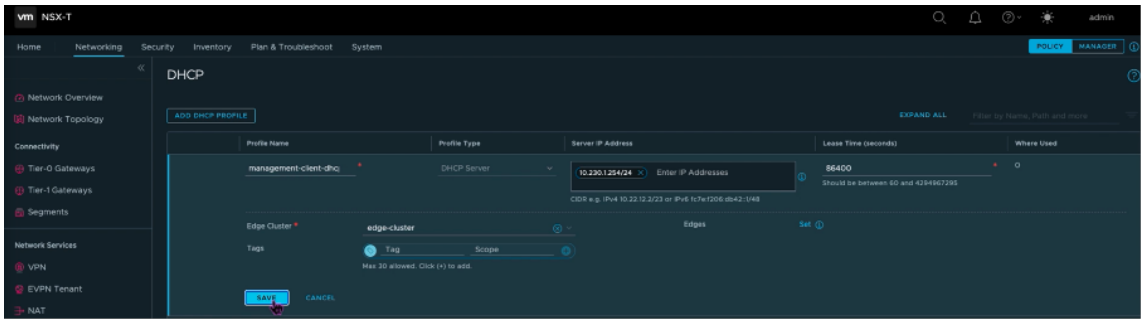
3. 导航到 **VSPHERE** 管理网络启动 NSX 管理器，然后单击 **NSX** 管理器。



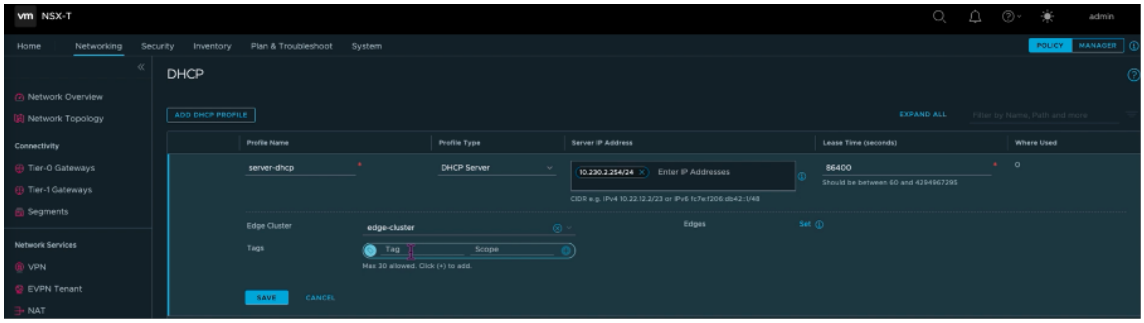
4. 使用此过程步骤 2 中记录的凭据登录 NSX Manager。



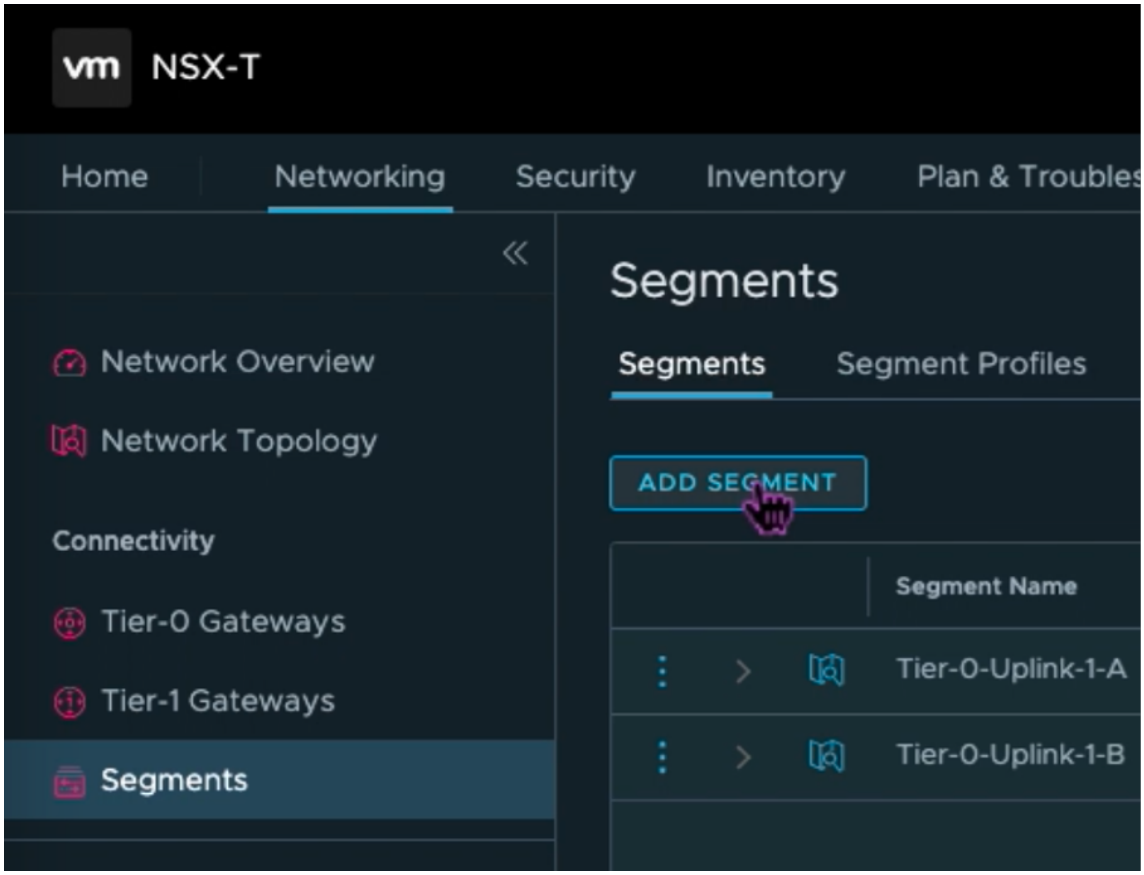
5. 为新的分段或子网设置 DHCP 服务。
6. 在创建子网之前，请先设置 DHCP 服务。
7. 在 NSX-T 中，转到 网络 **> DHCP**。网络控制面板显示该服务创建了一个 Tier-0 和一个 Tier-1 网关。
8. 要开始配置 DHCP 服务器，请单击“添加 **DHCP** 配置文件”。
9. 在 DHCP 名称字段中，输入 客户机管理 配置文件的名称。
10. 选择 **DHCP** 服务器 作为配置文件类型。
11. 在“服务器 **IP** 地址”列中，提供 DHCP 服务 IP 地址范围。
12. 选择您的 **Edge** 群集。
13. 单击 **Save**（保存）以创建 DHCP 服务。



14. 对服务器 DHCP 范围重复步骤 6 到 13。



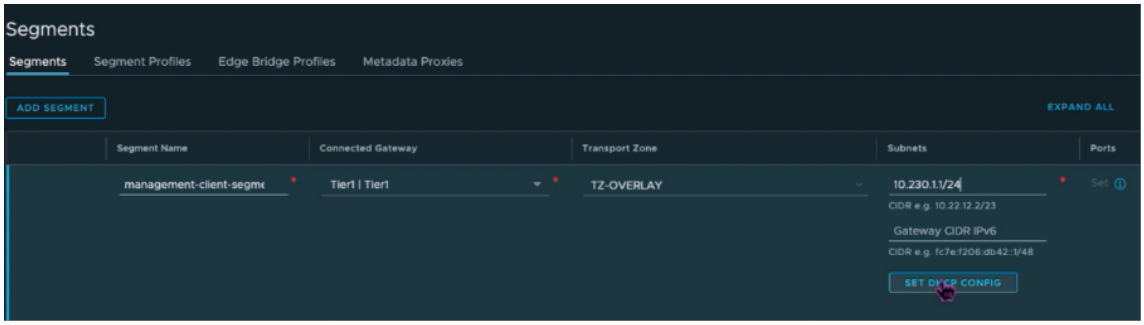
15. 创建两个单独的分段：一个用于客户端和管理接口，另一个用于服务器接口。
16. 在 NSX-T 中，转到 网络 **>** 分段。
17. 单击 **Add Segment**（添加区段）。



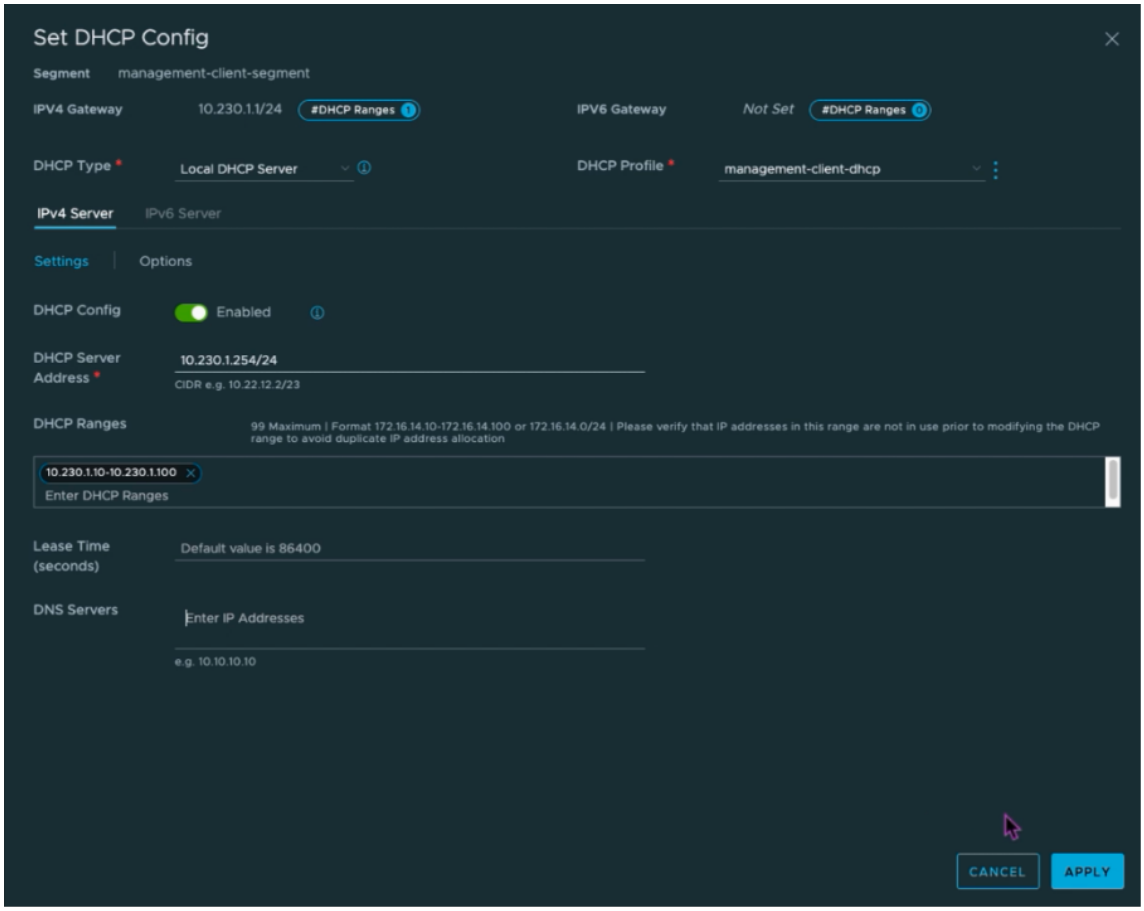
18. 在“分段名称”字段中，输入您的 客户管理 分段的名称。
19. 在“连接的网关”列表中，选择 **Tier1** 以连接到 Tier-1 网关。

在“传输区域”列表中，选择 **TZ-OVERLAY 叠加 **。

20.
21. 在子 网 列中，输入子网范围。将子网范围指定 **.** 1 为最后一个八位字节。例如，10.12.2.1/24。

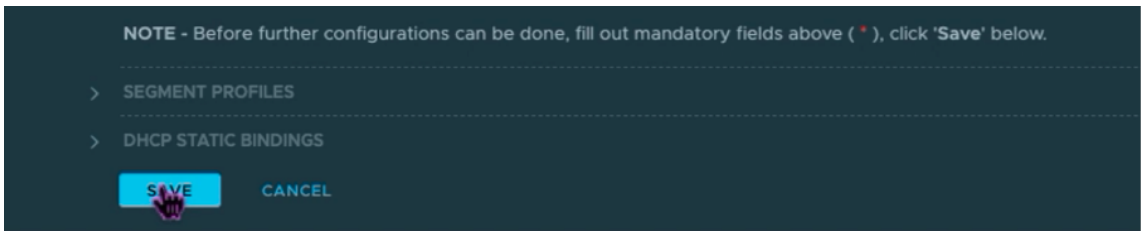


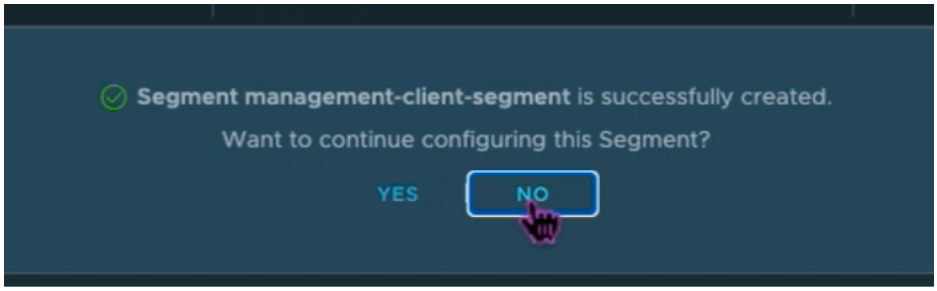
22. 单击“设置 **DHCP** 配置”，并为“**DHCP** 范围”字段提供值。



23. 单击“应用”保存您的 DHCP 配置。

24. 单击保存。





25. 还要对服务器分段重复步骤 17 到 24。

26. 现在，您可以在创建虚拟机时在 vCenter 中选择这些网络分段。

有关更多信息，请参阅 创建您的第一个子网。

在 **VMware** 云上安装 **NetScaler VPX** 实例

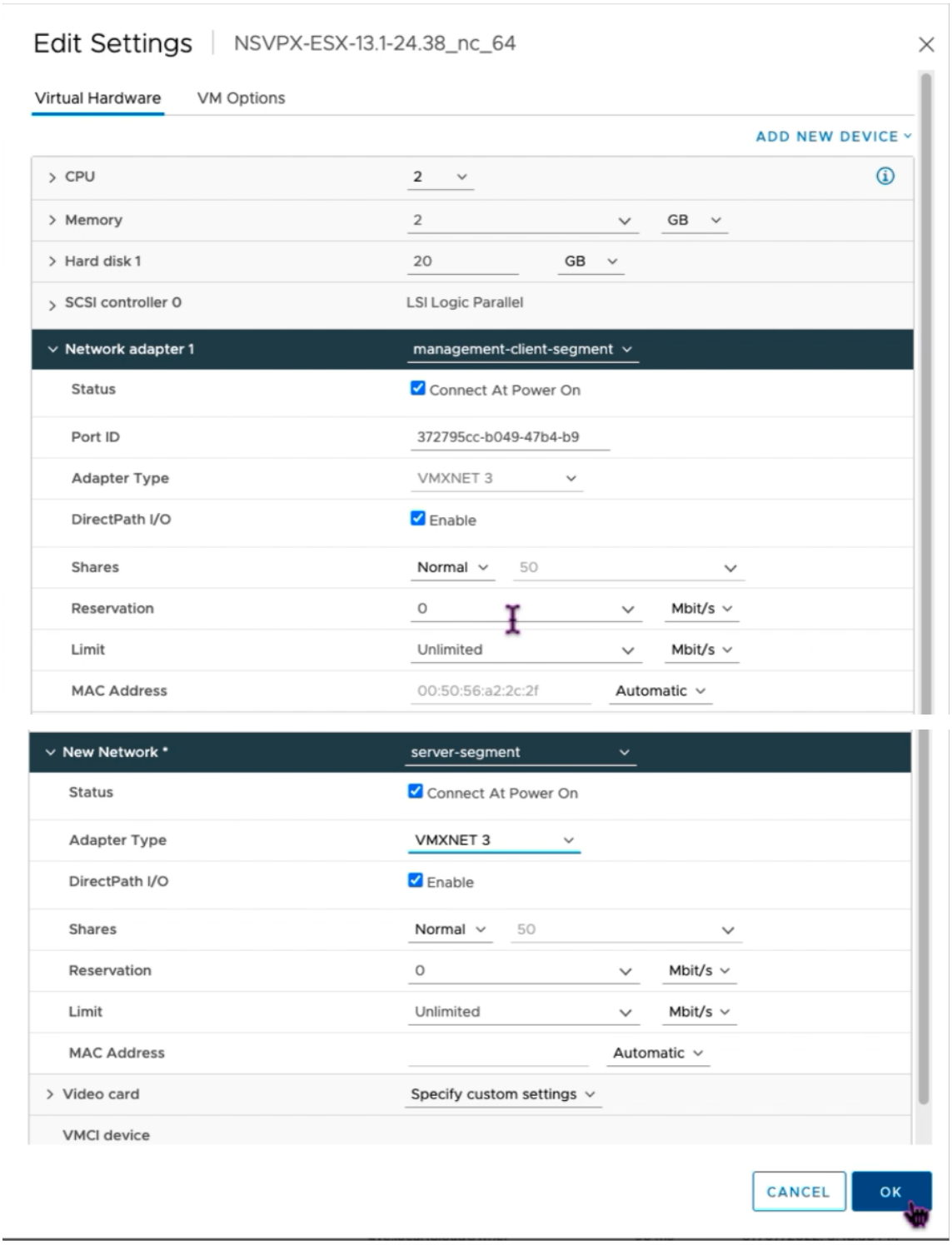
在 GCVE 上安装和配置私有云后，您可以使用 vCenter 在 VMware 引擎上安装虚拟设备。您可以安装的虚拟设备的数量取决于私有云上可用的资源量。

要在私有云上安装 NetScaler VPX 实例，请在连接到私有云点对点 VPN 的桌面上执行以下步骤：

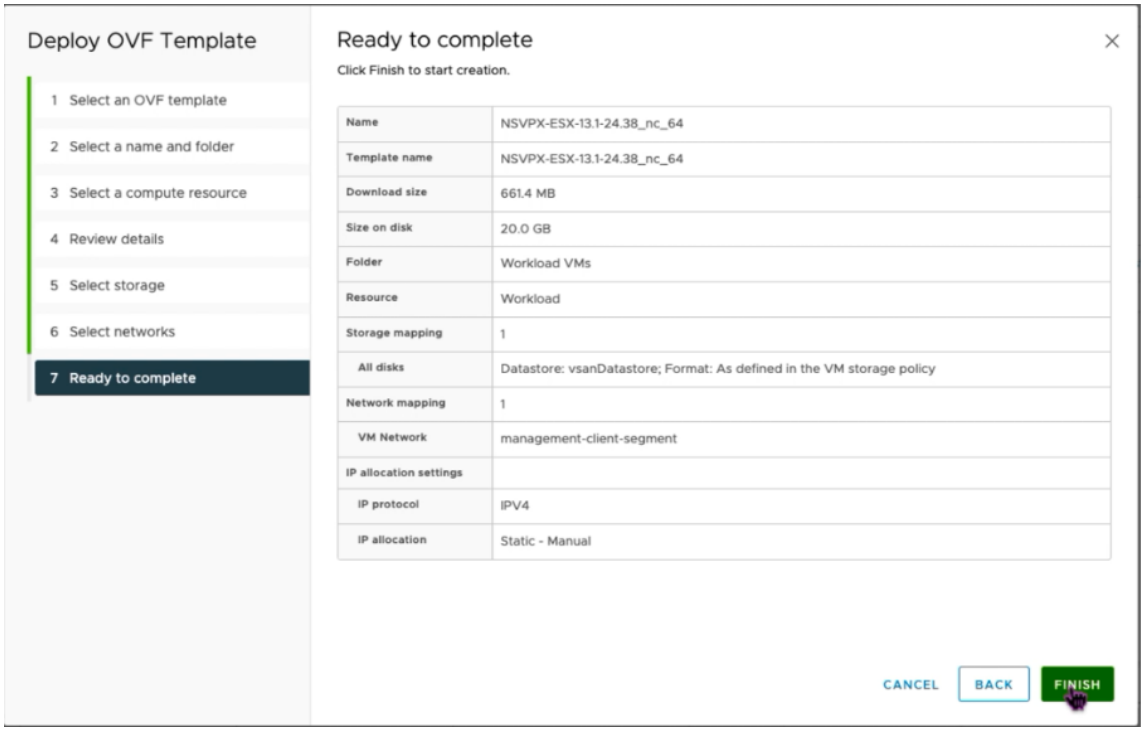
1. 从 NetScaler 下载网站下载适用于 ESXi 主机的 NetScaler VPX 实例设置文件。
2. 在连接到私有云点对点 VPN 的浏览器中打开 VMware vCenter。
3. 在“用户名”和“密码”字段中，键入管理员凭据，然后单击“登录”。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在“部 署 **OVF** 模板”对话框的“从文件部署”字段中，浏览到保存 NetScaler VPX 实例安装文件的位置，选择.ovf 文件，然后单击 下一步。

   > 注意：
   >
   > 默认情况下，NetScaler VPX 实例使用 E1000 网络接口。要使用 VMXNET3 接口部署 ADC，请将 OVF 修改为使用 VMXNET3 接口而非 E1000 接口。VMXNET3 接口的可用性受到 GCP 基础架构的限制，可能无法在 Google Cloud VMware Engine 中使用。

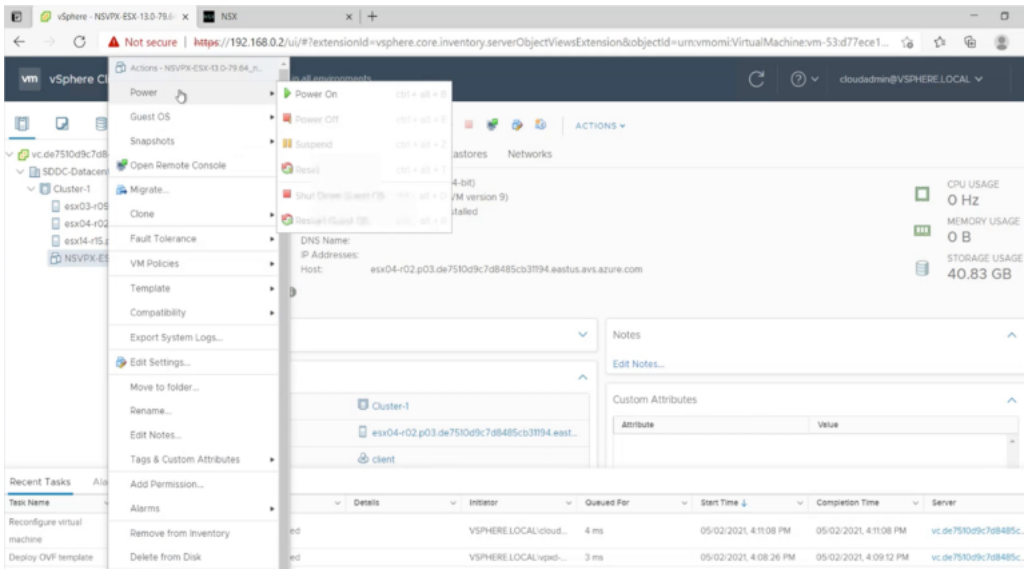
6. 将虚拟设备 OVF 模板中显示的网络映射到您在 NSX-T Manager 上配置的网络。单击确定。



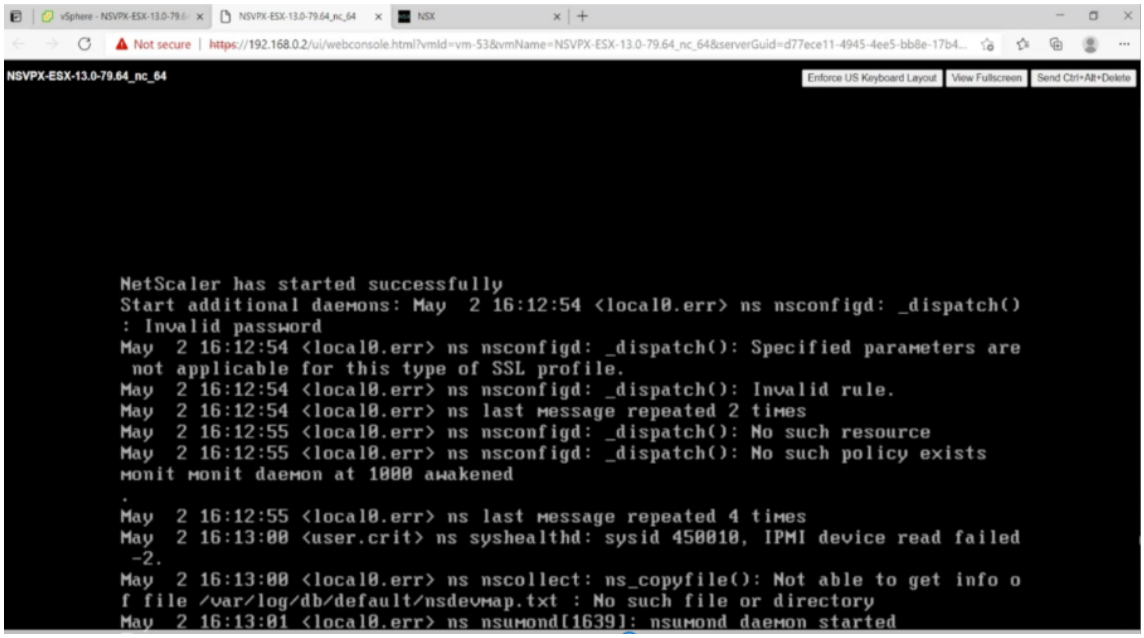
7. 单击“完成”开始在 VMware 云上安装虚拟设备。



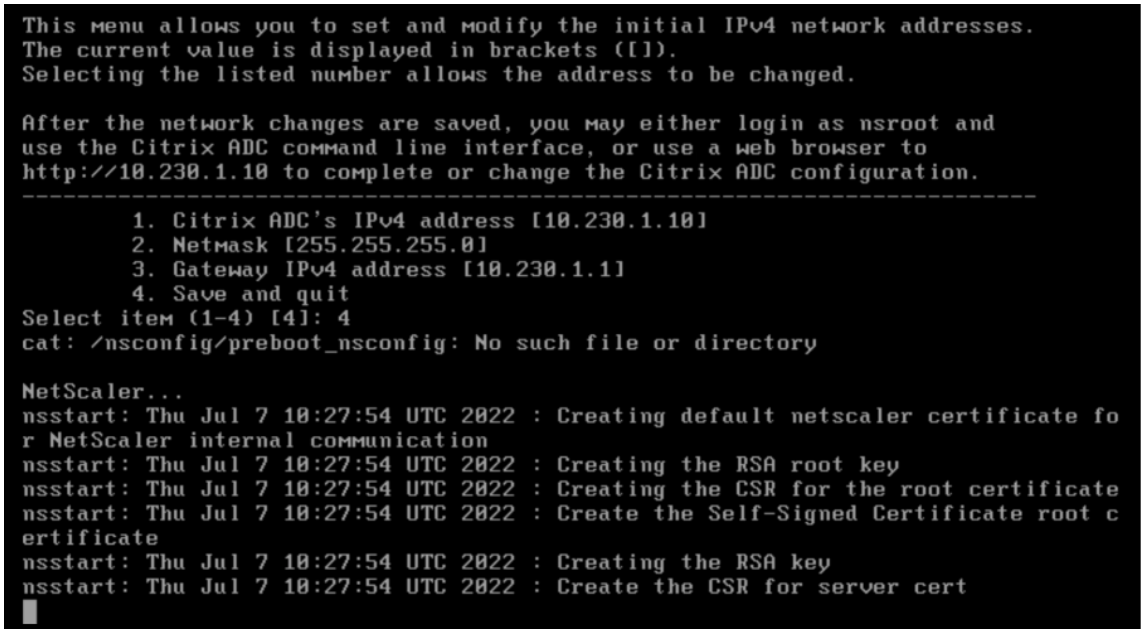
8. 现在，您可以启动 NetScaler VPX 实例。在导航窗格中，选择已安装的 NetScaler VPX 实例，然后从右键菜单中选择 **Power On**（开机）。单击“启动 **Web** 控制台”选项卡以模拟控制台端口。



9. 现在，您已从 vSphere 客户端连接到 NetScaler 虚拟机。



10. 首次启动时，为 ADC 实例设置管理 IP 和网关。



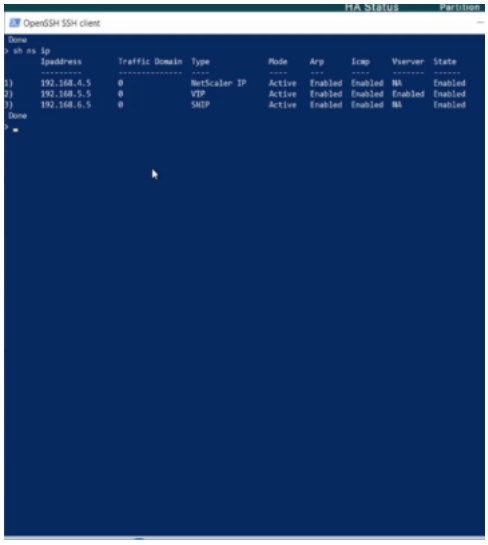
11. 要使用 SSH 密钥访问 NetScaler 设备，请在 CLI 中键入以下命令：

```
ssh nsroot@<management IP address>
```

Example:

```
ssh nsroot@10.230.1.10
```

12. 您可以使用 `show ns ip` 命令验证 ADC 配置。

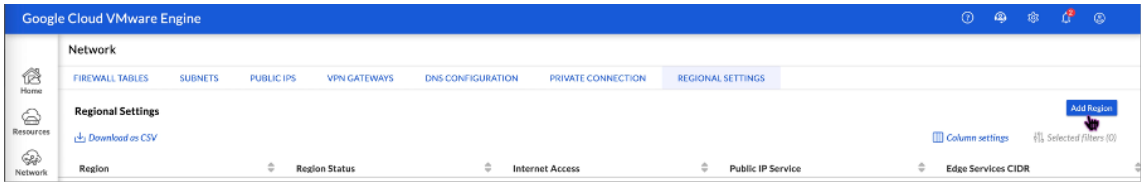


为 **VMware** 云上的 **NetScaler VPX** 实例分配公有 **IP** 地址

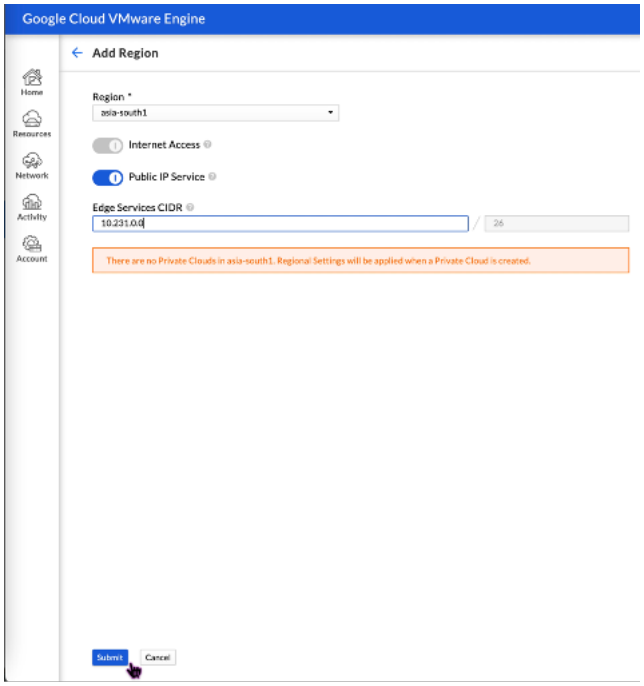
在 GCVE 上安装并配置 NetScaler VPX 实例后，必须为客户端接口分配公有 IP 地址。在为虚拟机分配公有 IP 地址之前，请确保为您的 Google Cloud 区域启用了公有 IP 服务。

要为新区域启用公有 IP 服务，请执行以下步骤：

1. 在 GCVE 控制台上，导航到 网络 **>** 区域设置 **>** 添加区域。



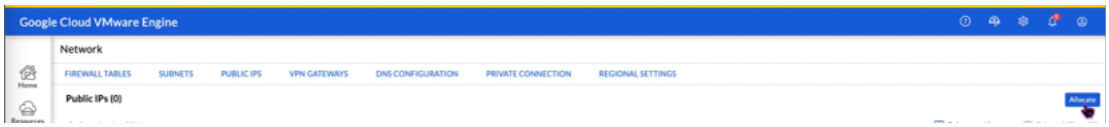
2. 选择您的区域并启用 **Internet** 接入 和公有 **IP** 服务。
3. 分配边缘服务 CIDR，确保 CIDR 范围不会与您的任何本地或其他 GCP/GCVE 子网（虚拟网络）重叠。



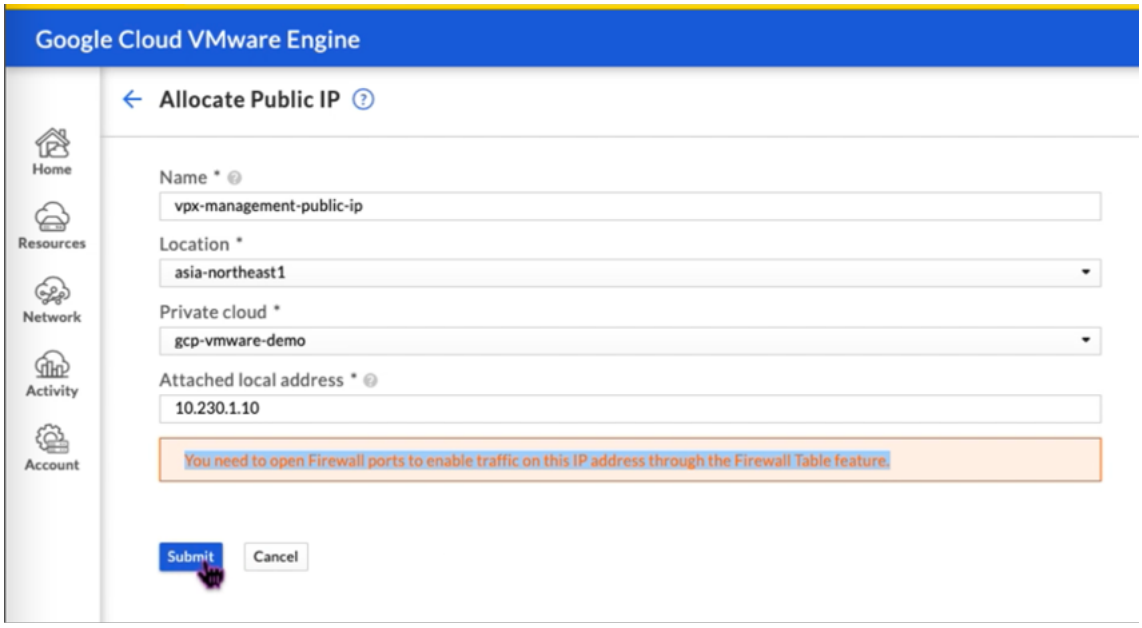
4. 将在几分钟后为所选区域启用公有 IP 服务。

要将公有 IP 分配给 GCVE 上的 NetScaler VPX 实例上的客户端接口，请在 GCVE 门户上执行以下步骤：

1. 在 GCVE 控制台上，导航到 网络 **>** 公共 **IPS >** 分配。



2. 输入公有 IP 的名称。选择您的区域，然后选择要使用 IP 的私有云。
3. 为要将公有 IP 映射到的接口提供私有 IP。这将是您的 客户端 接口的 私有 **IP** 。
4. 单击 **Submit**（提交）。



5. 公有 IP 在几分钟后就可以使用了。
6. 您必须添加防火墙规则以允许访问公共 IP，然后才能使用它。有关更多信息，请参阅 防火墙规则。

添加后端 **GCP** 自动缩放服务

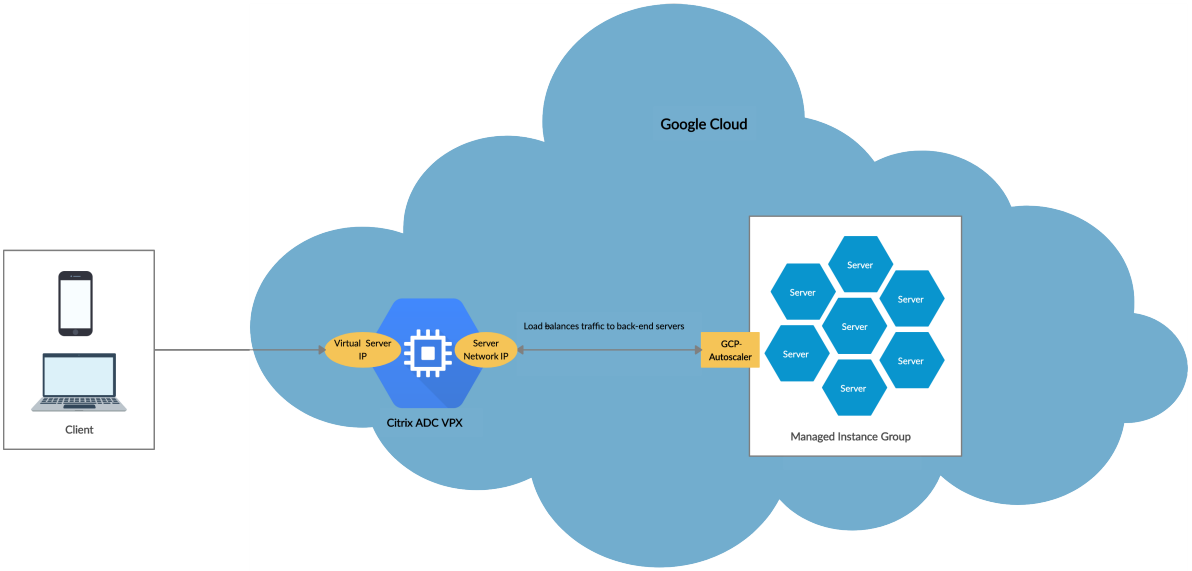
October 17, 2024

在云中高效托管应用程序需要根据应用程序需求轻松且经济高效地管理资源。为了满足日益增长的需求，必须向上扩展网络资源。当需求减少时，需要缩小以避免不必要的使用率不足的资源成本。为了最大限度地降低运行应用程序的成本，您必须不断监视流量、内存和 CPU 使用情况等。但是，手动监视流量很麻烦。为了应用程序环境可动态扩大或缩小，必须自动执行监视流量的过程以及必要时扩大和缩小资源的过程。

NetScaler VPX 实例与 GCP 自动扩缩服务集成，具有以下优点：

- 负载平衡和管理：根据需求，自动配置服务器以向上和向下扩展。VPX 实例会自动检测后端子网中的托管实例组，并允许您选择托管实例组来平衡负载。虚拟 IP 地址和子网 IP 地址是在 VPX 实例上自动配置的。
- 高可用性：检测跨多个区域和负载平衡服务器的托管实例组。
- 提高了网络可用性：VPX 实例支持：
  - 后端服务器位于相同的放置组中
  - 不同区域中的后端服务器

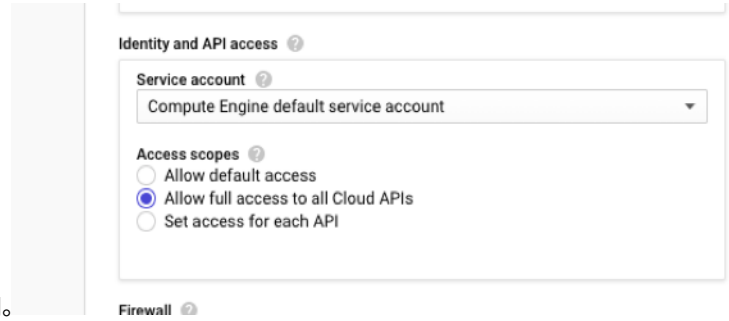
此图说明了 GCP 自动扩缩服务在充当负载平衡虚拟服务器的 NetScaler VPX 实例中的工作原理。



开始之前的准备工作

在开始在 NetScaler VPX 实例上使用自动缩放之前，必须完成以下任务。

- 根据您的要求在 GCP 上创建 NetScaler VPX 实例。
  - 有关如何创建 NetScaler VPX 实例的更多信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例。
  - 有关如何在 HA 模式下部署 VPX 实例的更多信息，请参阅 在 Google Cloud Platform 上部署 VPX 高可用性对。
- 为您的 GCP 项目启用 **Cloud Resource Manager API**。
- 在创建实例时允许对所有云 API 进行完全访问。



- 请确保您的 GCP 服务帐户具有以下 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.instances.get",
"compute.instanceGroupManagers.get",
"compute.instanceGroupManagers.list",
"compute.zones.list",
```



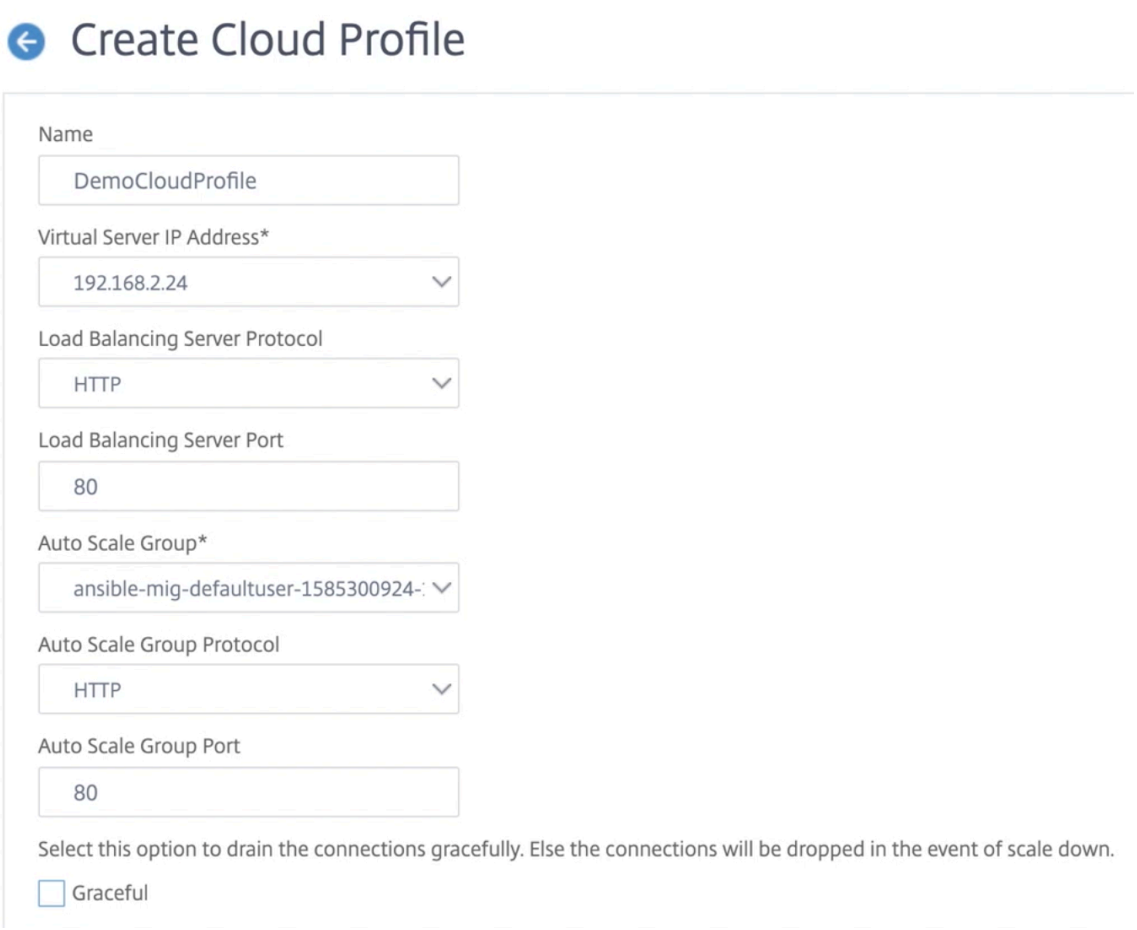
```
    "logging.sinks.create",
    "logging.sinks.delete",
    "logging.sinks.get",
    "logging.sinks.list",
    "logging.sinks.update",
    "pubsub.subscriptions.consume",
    "pubsub.subscriptions.create",
    "pubsub.subscriptions.delete",
    "pubsub.subscriptions.get",
    "pubsub.topics.attachSubscription",
    "pubsub.topics.create",
    "pubsub.topics.delete",
    "pubsub.topics.get",
    "pubsub.topics.getIamPolicy",
    "pubsub.topics.setIamPolicy",
    ]
```

- 要设置自动缩放，请确保配置了以下内容：
  - 实例模板
  - 托管实例组
  - 自动缩放策略

将 **GCP** 自动缩放服务添加到 **NetScaler VPX** 实例

在 GUI 中单击一次即可将自动缩放服务添加到 VPX 实例。完成以下步骤可将自动缩放服务添加到 VPX 实例：

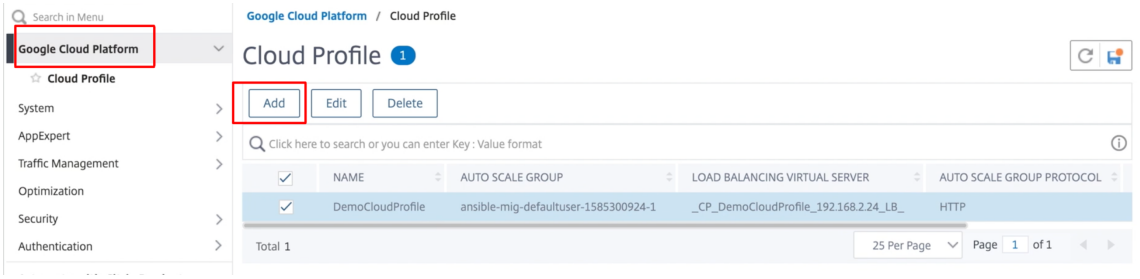
1. 使用您的 `nsroot` 凭证登录 VPX 实例。
2. 首次登录 NetScaler VPX 实例时，您会看到默认的“Cloud Profile”（云配置文件）页面。从下拉菜单中选择 GCP 托管实例组，然后单击 **Create**（创建）以创建云配置文件。



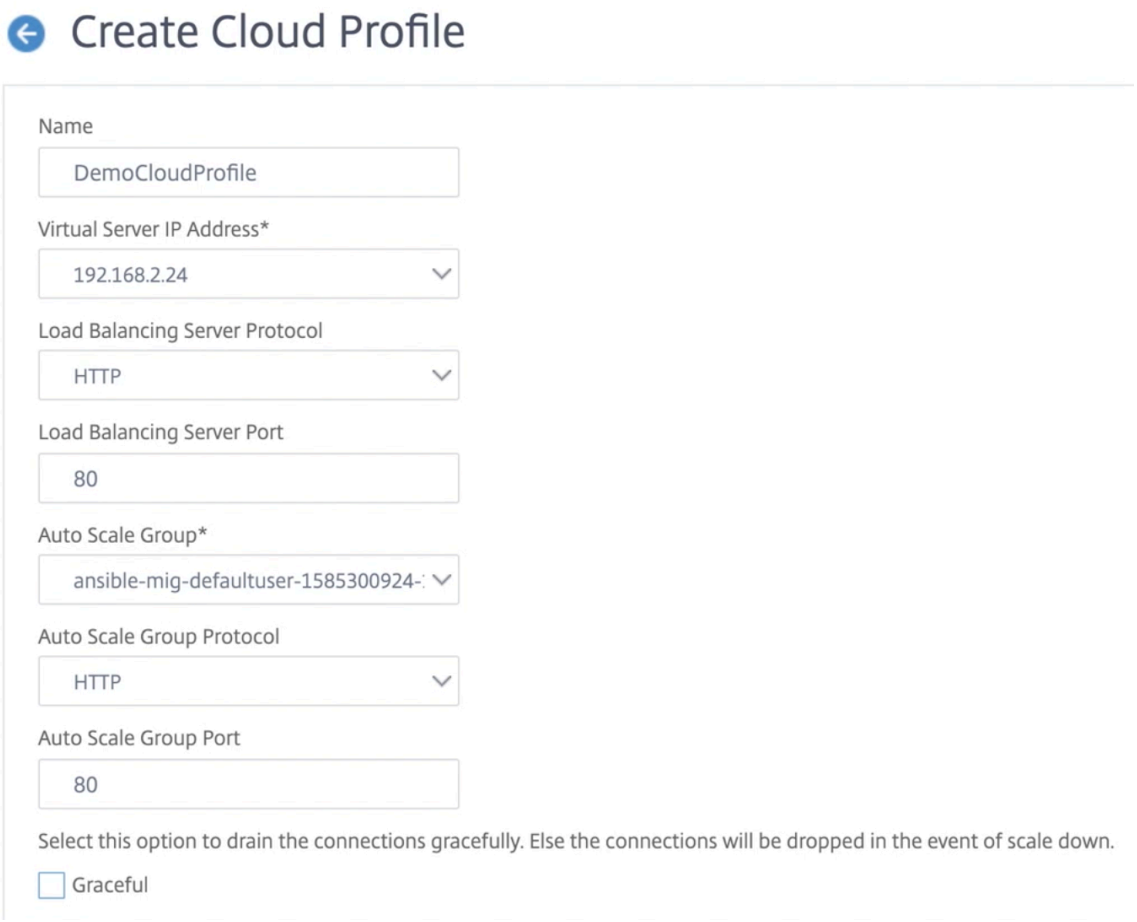
- **Virtual Server IP Address**（虚拟服务器 IP 地址）字段是从与实例关联的所有 IP 地址自动填充的。
- **AutoScale** 组 是从您的 GCP 帐户上配置的托管实例组预填充的。
- 选择 **Autoscale Group Protocol**（Autoscale 组协议）和 **Autoscale Group Port**（Autoscale 组端口）时，请确保服务器监听配置的协议和端口。在服务组中绑定正确的监视器。默认情况下，使用 TCP 监视器。
- 清除“正常”复选框，因为不支持该复选框。

> 注意：
>
> 对于 SSL 协议类型 Autosscaling，您创建云配置文件后，负载平衡虚拟服务器或服务组将由于缺少证书而关闭。可以手动将证书绑定到虚拟服务器或服务组。

3. 首次登录后，如果要创建云配置文件，请在 GUI 上转到 **System**（系统）**> Google Cloud Platform**（**Google** 云端平台）**> Cloud Profile**（云配置文件），然后单击 **Add**（添加）。

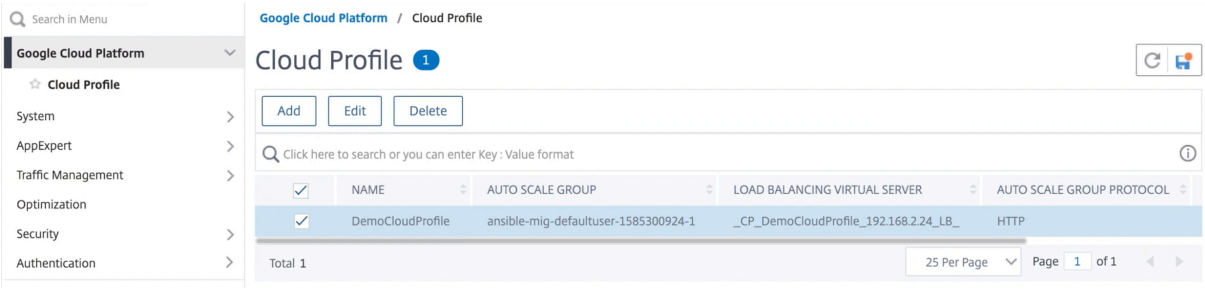


将出现“创建云配置文件”配置页面。



云配置文件创建了一个 NetScaler 负载平衡虚拟服务器和一个服务组，其成员是托管实例组的服务器。您的后端服务器必须能够通过 VPX 实例上配置的 SNIP 进行访问。

> 注意：
>
> 从 NetScaler 版本 13.1-42.x 起，您可以在 GCP 中使用相同的托管实例组为不同的服务（使用不同的端口）创建不同的云配置文件。因此，NetScaler VPX 实例支持公共云中具有同一自动缩放组的多个服务。



GCP 上的 NetScaler VPX 实例支持 VIP 扩展

October 17, 2024

NetScaler 设备的位置介于客户端与服务器之间，以便客户端请求和服务器响应都能经过该设备。在典型安装中，在设备上配置的虚拟服务器提供连接点，客户端使用这些连接点来访问位于设备后面的应用程序。部署所需的公用虚拟 IP (VIP) 地址数量因具体情况而异。

GCP 体系结构限制实例上的每个接口连接到不同的 VPC。GCP 上的 VPC 是子网的集合，每个子网可以跨地理区域的区域。此外，GCP 还规定了以下限制：

- 存在公用 IP 地址数量与 NIC 数量的 1:1 映射。一个 NIC 只能分配一个公用 IP 地址。
- 在容量较高的实例类型上最多只能附加 8 个 NIC。

例如，n1-standard-2 实例只能有 2 个 NIC，可以添加的公用 VIP 限制为 2 个。有关更多信息，请参阅 VPC 资源配额。

要在 NetScaler VPX 实例上实现更高的公共虚拟 IP 地址规模，您可以将 VIP 地址配置为实例元数据的一部分。NetScaler VPX 实例在内部使用 GCP 提供的转发规则来实现 VIP 扩展。NetScaler VPX 实例还为配置的 VIP 提供高可用性。将 VIP 地址配置为元数据的一部分后，可以使用创建转发规则所用的相同 IP 配置 LB 虚拟服务器。因此，我们可以使用转发规则来缓解在 GCP 上的 NetScaler VPX 实例上使用公有 VIP 地址时 w.r.t scale 的限制。

有关转发规则的详细信息，请参阅 转发规则概述。

有关 HA 的更多信息，请参阅 高可用性。

注意事项

- Google 会对每个虚拟 IP 转发规则收取一些额外的费用。实际成本取决于创建的条目数量。相关费用可以从 Google 定价文档中找到。
- 转发规则仅适用于公用 VIP。当部署需要专用 IP 地址作为 VIP 时，可以使用别名 IP 地址。
- 只能为需要 LB 虚拟服务器的协议创建转发规则。VIP 可以即时创建、更新或删除。还可以添加具有相同 VIP 地址但使用不同协议的新负载平衡虚拟服务器。

开始之前的准备工作

- NetScaler VPX 实例必须部署在 GCP 上。
- 必须保留外部 IP 地址。有关详细信息，请参阅 保留静态外部 IP 地址。
- 确保您的 GCP 服务账户具有以下 IAM 权限：

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]
```

- 为您的 GCP 项目启用 **Cloud Resource Manager API**。
- 如果您在独立 VPX 实例上使用 VIP 扩展，请确保您的 GCP 服务帐户具有以下 IAM 权限：

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
]
```

- 如果您在高可用性模式下使用 VIP 扩展，请确保您的 GCP 服务帐户具有以下 IAM 权限：

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.use",
```



```
    "compute.instances.get",
    "compute.instances.list",
    "compute.instances.setMetadata",
    "compute.subnetworks.use",
    "compute.targetInstances.create",
    "compute.targetInstances.list",
    "compute.targetInstances.use",
    "compute.zones.list",
    ]
```

> 注意：
>
> 在高可用性模式下，如果您的服务帐号没有所有者或编辑者角色，则必须将 服务帐户用户角 色添加到服务帐号中。

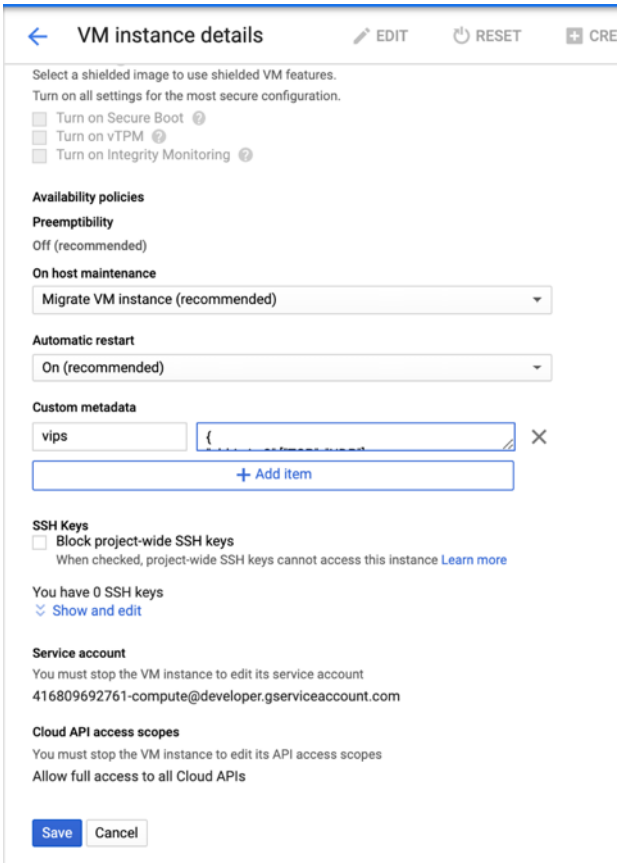
在 **NetScaler VPX** 实例上配置外部 **IP** 地址以进行 **VIP** 扩展

1. 在 Google 云控制台中，导航至 **VM Instances**（VM 实例）页面。
2. 创建新的虚拟机实例或使用现有实例。
3. 单击实例名称。在 虚拟机实例详细信息 页面上，单击 编辑。
4. 通过输入以下内容来更新 **Custom metadata**（自定义元数据）：
   - 键 = VIPs
   - 值 = 提供以下 JSON 格式的值：

     { “Name of external reserved IP”：[list of protocols], }

   GCP 支持以下协议：

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



有关详细信息，请参阅 自定义元数据

自定义元数据示例：

{ “外部 IP1 名称”：[“TCP” ，“UDP”]，“外部 IP2 名称”：[“ICMP” ，“AH”] }

在此示例中，NetScaler VPX 实例在内部为每个 IP 协议对创建了一个转发规则。元数据条目将映射到转发规则。此示例可帮助您了解为元数据条目创建了多少条转发规则。

请按如下方式创建四条转发规则：

a) 外部 ip1 名称和 TCP
b) 外部 ip1 名称和 UDP
c) 外部 ip2 名称和 ICMP
d) 外部 ip2-name 和 AH

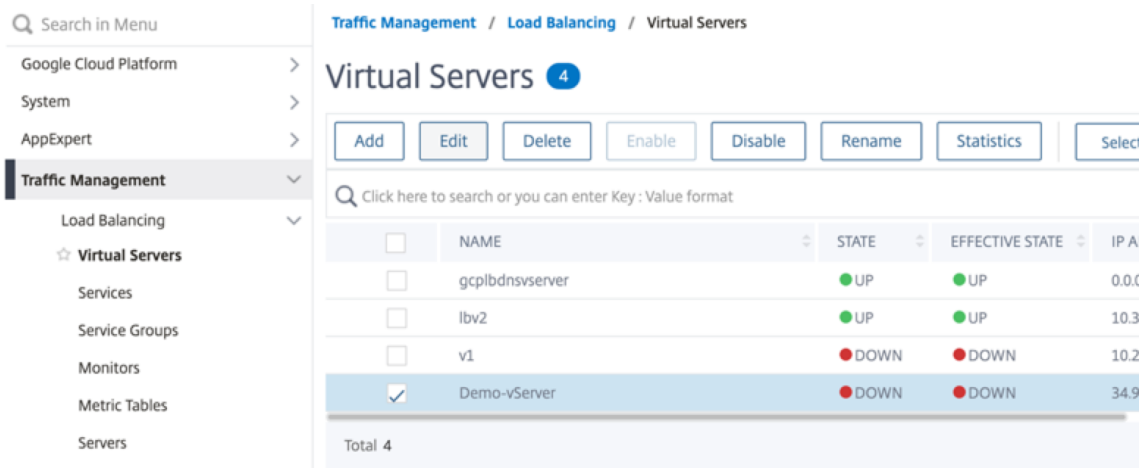
> 注意：
>
> 在高可用模式下，您只能在主实例上添加自定义元数据。在故障转移时，自定义元数据将同步到新的主节点。

5. 单击保存。

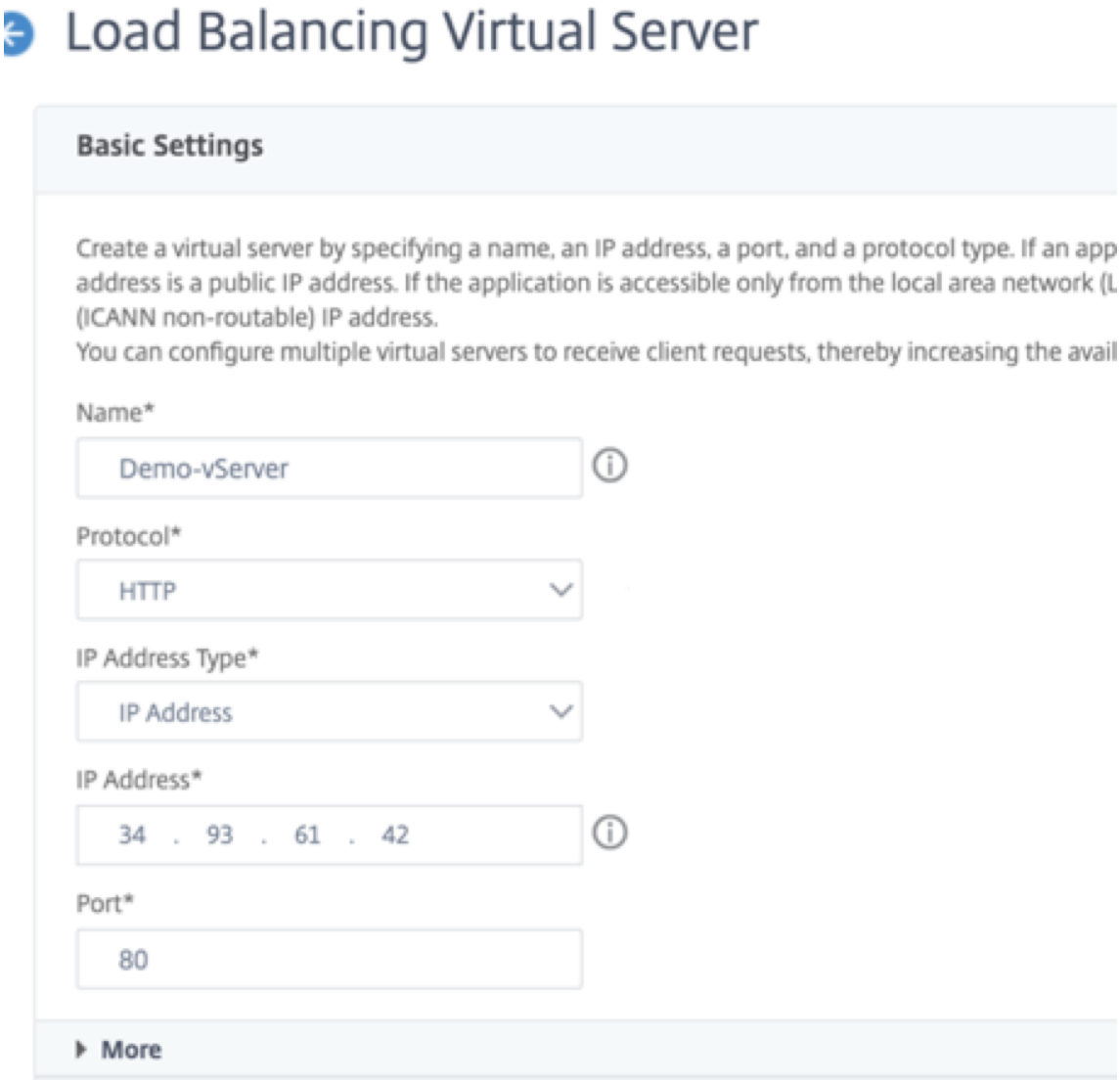
在 **NetScaler VPX** 实例上使用外部 **IP** 地址设置负载平衡虚拟服务器

第 **1** 步。添加负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）**> Add**（添加）。

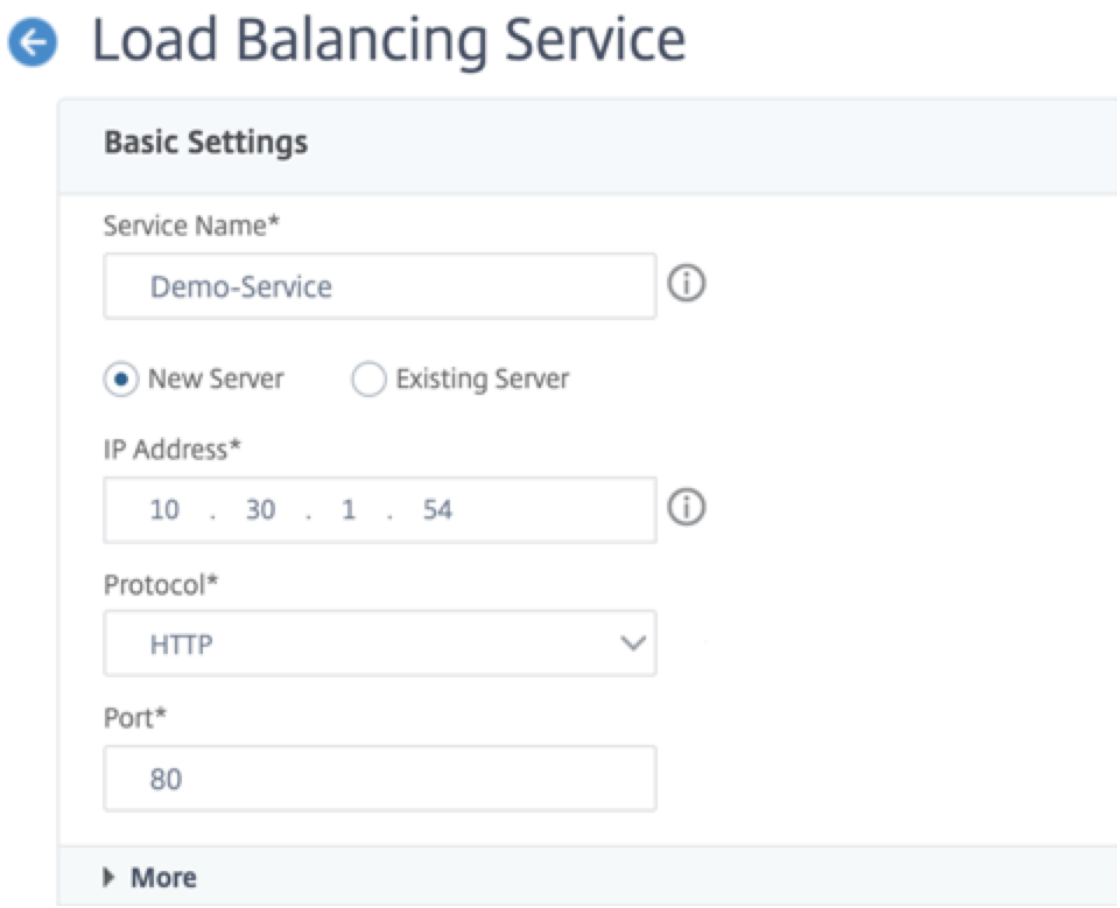


2. 添加“Name”（名称）、“Protocol”（协议）、IP Address Type (IP Address)（IP 地址类型 (IP 地址)）、“IP Address”（IP 地址）（在 ADC 上作为 VIP 添加的转发规则的外部 IP 地址）和“Port”（端口）所需的值，然后单击 **OK**（确定）。



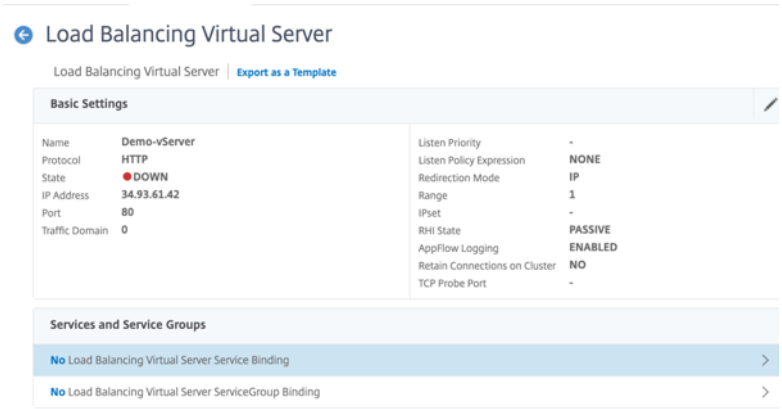
第 **2** 步。添加服务或服务组。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）**> Add**（添加）。
2. 添加“Service Name”（服务名称）、“IP Address”（IP 地址）、“Protocol”（协议）和“Port”（端口）所需的值，然后单击 **OK**（确定）。

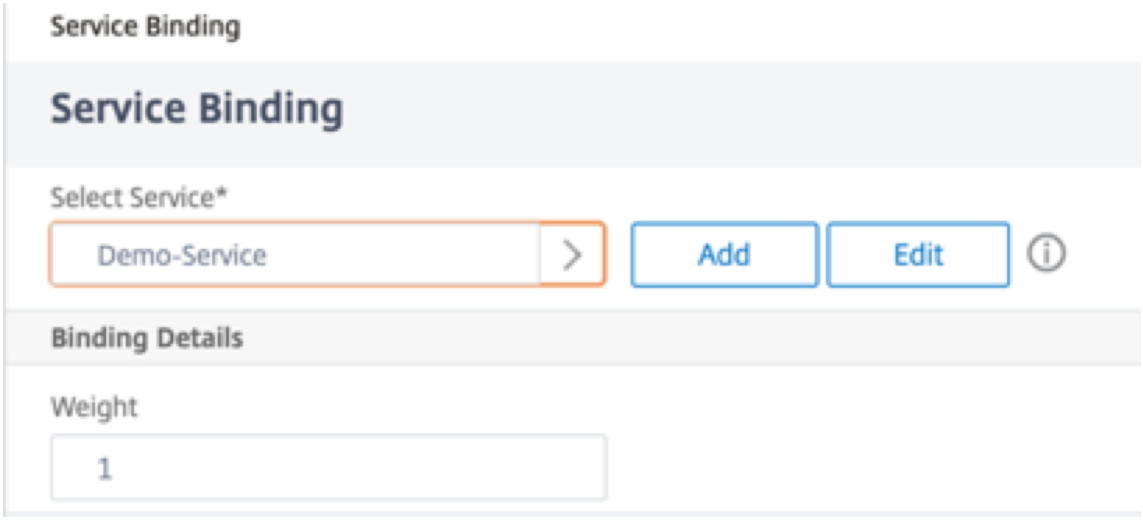


第 **3** 步。将服务或服务组绑定到负载平衡虚拟服务器。

1. 导航到 **Configuration**（配置）**> Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。
2. 选择在 **Step 1**（步骤 1）中配置的负载平衡虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **Service and Service Groups**（服务和服务组）页面中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。



4. 选择在 **Step 3**（步骤 3）中配置的服务，然后单击 **Bind**（绑定）。



5. 步骤 7. 保存配置。

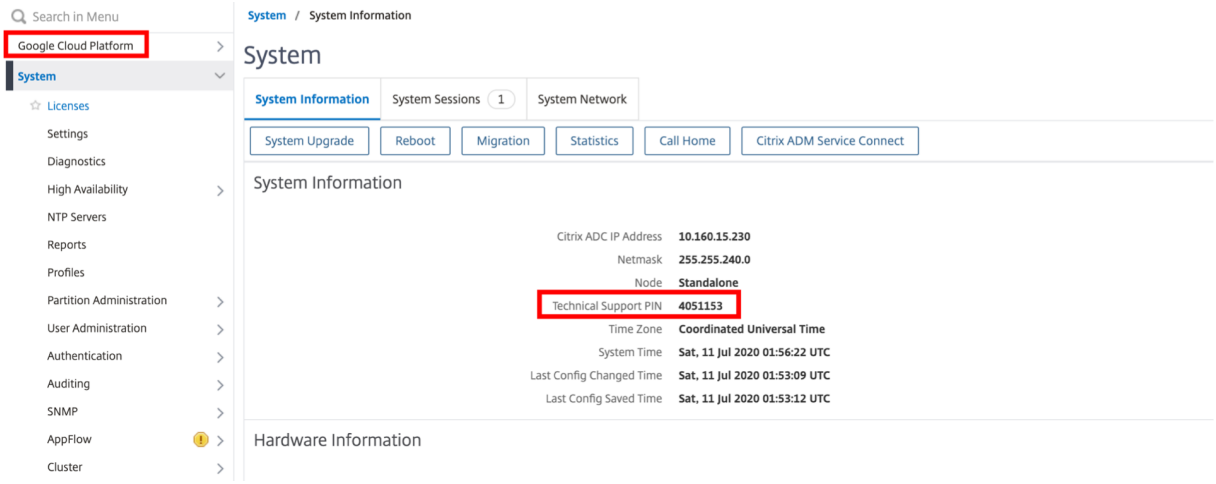
对 **GCP** 上的 **VPX** 实例进行故障排除

October 17, 2024

Google Cloud Platform (GCP) 提供对 NetScaler VPX 实例的控制台访问权限。只能在建立网络连接的情况下进行调试。要查看实例的系统日志，请访问控制台并检查 **System Log files**（系统日志文件）。

NetScaler 在 GCP 上支持基于费用的 NetScaler VPX 实例（按小时计费的公用事业许可证）。要提交支持案例，请找到您的 GCP 账号和支持 PIN 码，然后致电 NetScaler 支持人员。系统要求您提供姓名和电子邮件地址。要查找支持 PIN，请登录 VPX GUI 并导航到 **System**（系统）页面。

下面是显示了支持 PIN 码的系统页面的示例。



NetScaler VPX 实例上的巨型帧

October 17, 2024

NetScaler VPX 设备支持接收和发送最多包含 9216 字节 IP 数据的巨型帧。相比于 1500 字节的标准 IP MTU 大小，巨型帧可以更有效地传输大文件。

NetScaler 设备可在下列部署方案中使用巨型帧：

- 巨型帧到巨型帧。设备接收巨型帧形式的数据，并将其作为巨型帧进行发送。
- 非巨型帧到巨型帧。设备接收普通帧形式的数据，并将其作为巨型帧进行发送。
- 巨型帧到非巨型帧。设备接收巨型帧形式的数据，并将其作为通帧帧进行发送。

有关更多信息，请参阅在 NetScaler 设备上配置巨型帧支持。

在运行于以下虚拟化平台的 NetScaler VPX 设备上可支持巨型帧：

- VMware ESX
- Linux-KVM 平台
- Citrix XenServer
- Amazon Web Services (AWS)

VPX 设备上巨型帧的工作原理类似于 MPX 设备上巨型帧的工作原理。有关巨型帧及其用例的详细信息，请参阅“在 MPX 设备上配置巨型帧”。MPX 设备上的巨型帧用例也适用于 VPX 设备。

为在 VMware ESX 上运行的 VPX 实例配置巨型帧

执行以下任务，在 VMware ESX 服务器上运行的 NetScaler VPX 设备上配置巨型帧：

1. 将 VPX 设备的接口或通道的 MTU 设置为一个介于 1501–9000 的值。使用 CLI 或 GUI 设置 MTU 大小。在 VMware ESX 上运行的 NetScaler VPX 设备支持接收和传输最多仅包含 9000 字节 IP 数据的巨型帧。
2. 通过使用其管理应用程序，在 VMware ESX 服务器的对应物理接口上设置相同的 MTU 大小。有关在 VMware ESX 的物理接口上设置 MTU 大小的详细信息，请参阅 http://vmware.com/。

为在 Linux-KVM 服务器上运行的 VPX 实例配置巨型帧

执行以下任务，在 Linux-KVM 服务器上运行的 NetScaler VPX 设备上配置巨型帧：

1. 将 VPX 设备的接口或通道的 MTU 设置为一个介于 1501–9216 的值。使用 NetScaler VPX CLI 或 GUI 设置 MTU 大小。
2. 通过使用 Linux-KVM 服务器的管理应用程序，在此服务器的对应物理接口上设置相同的 MTU 大小。有关如何在 Linux-KVM 的物理接口上设置 MTU 大小的详细信息，请参阅 http://www.linux-kvm.org/。

为在 **Citrix XenServer** 上运行的 **VPX** 实例配置巨型帧

执行以下任务，在 Citrix XenServer 上运行的 NetScaler VPX 设备上配置巨型帧：

1. 使用 XenCenter 连接到 XenServer。
2. 关闭所有使用必须更改 MTU 的网络的 VPX 实例。
3. 在 **Networking**（网络连接）选项卡上，选择网络 - 网络 0/1/2。
4. 选择 **Properties**（属性）并编辑 MTU。

在 XenServer 上配置 Jumbo 帧后，可以在 ADC 设备上配置巨型帧。有关更多信息，请参阅在 NetScaler 设备上配置巨型帧支持。

为在 **AWS** 上运行的 **VPX** 实例配置巨型帧

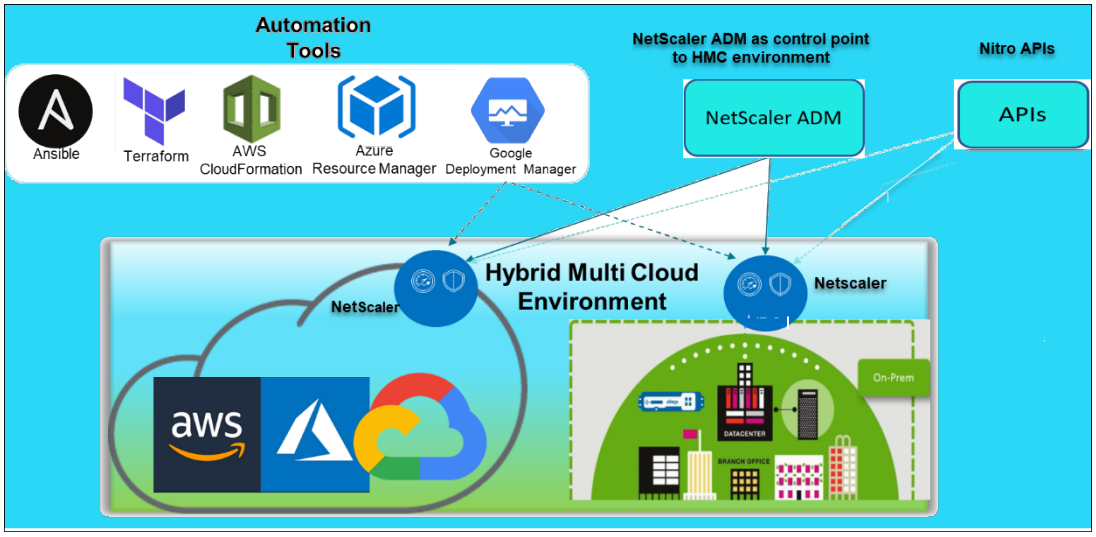
Azure 上的 VPX 不需要主机级别的配置。要在 VPX 上配置巨型帧，请按照在 NetScaler 设备上配置巨型帧支持中的步骤进行操作。

自动部署和配置 **NetScaler**

October 17, 2024

NetScaler 提供多种工具来自动执行您的 ADC 部署和配置。本文档简要介绍了各种自动化工具以及可用于管理 ADC 配置的各种自动化资源的参考资料。

下图概述了混合多云 (HMC) 环境中的 NetScaler 自动化。



使用 **NetScaler ADM** 实现 **NetScaler** 自动化

NetScaler ADM 充当分布式 ADC 基础设施的自动化控制点。NetScaler ADM 提供了一套全面的自动化功能，从配置 ADC 设备到升级它。以下是 ADM 的主要自动化功能：

- 在 AWS 上 Provisioning NetScaler VPX 实例
- 在 Azure 上 Provisioning NetScaler VPX 实例
- StyleBooks
- 配置作业
- 配置审核
- ADC 升级
- SSL 证书管理
- 集成- GitHub、ServiceNow、事件通知集成

有关自动化的 **NetScaler ADM** 博客和视频

- 使用样书进行应用程序迁移
- 使用 ADM 样书将 ADC 配置与 CI/CD 集成
- 通过 ADM 简化公有云 NetScaler 的部署
- NetScaler ADM 服务支持更轻松的 NetScaler 升级的 10 种方式

NetScaler ADM 还为其各种功能提供 API，将 NetScaler ADM 和 NetScaler 集成为整体 IT 自动化的一部分。有关更多信息，请参阅 NetScaler ADM 服务 API。

使用 **Terraform** 自动执行 **NetScaler**

Terraform 是一种将基础结构作为代码方法来预配和管理云、基础结构或服务的工具。NetScaler 地形资源可在 GitHub 中使用。有关详细的文档和用法，请参阅 GitHub。

- NetScaler Terraform 模块用于为负载平衡和 GSLB 等各种用例配置 ADC
- 用于在 AWS 中部署 ADC 的 Terraform 云脚本
- 用于在 Azure 中部署 ADC 的 Terraform 云脚本
- 在 GCP 中部署 ADC 的 Terraform 云脚本
- 使用 NetScaler VPX 和 Azure 管道进行蓝绿色部署

关于用于 **ADC** 自动化的 **Terraform** 的博客和视频

- 使用 Terraform 自动执行 NetScaler 部署
- 使用 Terraform 在 AWS 的 HA 设置中预配和配置 ADC

使用 **Consul-Terraform-Sync** 自动化 **NetScaler**

NetScaler Consul-Terraform-Sync (CTS) 模块使应用程序团队能够自动向 NetScaler 添加或删除新的服务实例。无需向 IT 管理员或网络团队提交手动工单即可进行必要的 ADC 配置更改。

- 用于网络基础设施自动化的 NetScaler Consul-Terraform-Sync 模块
- Citrix-HashiCorp 联合网络研讨会：Terraform En terprise 和 NetScaler 使用 Consul-Terraform-Sync 进操作态

使用 **Ansible** 自动执行 **NetScaler**

Ansible 是一款支持基础结构即代码的开源软件预配、配置管理和应用程序部署工具。NetScaler Ansible 模块和示例剧本可以在 GitHub 上找到，以供使用。有关详细的文档和用法，请参阅 GitHub。

- 用于配置 ADC 的 Ansible 模块
- ADC Ansible 模块文档/参考指南
- 适用于 ADM 的 Ansible 模块

Citrix 是经过认证的 Ansible 自动化合作伙伴。订阅了红帽 Ansible 自动化平台的用户可以从 红帽自动化中心访问 NetScaler 集合。

Terraform 和 **Ansible** 自动化博客

- Citrix 被评为 HashiCorp 年度最佳集成合作伙伴
- Citrix 现已成为红帽 Ansible 自动化平台身份验证合作伙伴
- 用于交付和保护应用程序的 Terraform 和 Ansible 自动化

用于部署 **ADC** 的公有云模板

公有云模板简化了公有云中部署的预配。不同的 NetScaler 模板可用于各种环境。有关如何使用的详细信息，请参阅相应的 GitHub 存储库。

AWS CFT:

- CFT 将在 AWS 上配置 NetScaler VPX

Azure Resource Manager (ARM) 模板：

- 用于在 Azure 上配置 NetScaler VPX 的 ARM 模板

Google 云部署管理器 **(GDM)** 模板：

- 用于在 Google 上配置 NetScaler VPX 的 GDM 模板

有关模板的视频

- 使用 CloudFormation 模板在 AWS 中部署 NetScaler HA
- 使用 AWS QuickStart 跨可用区部署 NetScaler HA
- 使用 GDM 模板在 GCP 中部署 NetScaler HA

NITRO API

NetScaler NITRO 协议允许您使用代表性状态传输 (REST) 接口以编程方式配置和监视 NetScaler 设备。因此，可以用任何编程语言来开发 NITRO 应用程序。对于必须以 Java 或.NET 或 Python 开发的应用程序，NITRO API 将通过打包为独立软件开发工具包 (SDK) 的相关库公开。

- NITRO API 文档
- 使用 NITRO API 的示例 ADC 用例配置

常见问题解答

October 17, 2024

以下部分将帮助您根据 Citrix Application Delivery Controller (ADC) VPX 对常见问题进行分类。

- 特性和功能
- 加密
- 定价和包装
- NetScaler VPX Express 和 90 天免费试用
- 虚拟机管理程序
- 容量规划或大小调整
- 系统要求
- 其他技术常见问题解答

特性和功能

什么是 **NetScaler VPX**

NetScaler VPX 是一种虚拟 ADC 设备，可以托管在安装在行业标准服务器上的虚拟机管理程序上。

NetScaler VPX 是否将所有 **Web** 应用程序优化功能作为 **ADC** 设备包括在内

是。NetScaler VPX 包括所有负载平衡、流量管理、应用程序加速、应用程序安全性（包括 NetScaler Gateway 和 Citrix Application Firewall）以及卸载功能。有关 NetScaler 特性和功能的完整概述，请参阅按 自己的方式交付应用程序。

在 **NetScaler VPX** 上使用 **Citrix Application Firewall** 时是否存在任何限制**?**

NetScaler VPX 上的 Citrix 应用程序防火墙提供与 NetScaler 设备相同的安全保护。Citrix Application Firewall 的性能或吞吐量因平台而异。

NetScaler VPX 上的 **NetScaler Gateway** 和 **NetScaler** 设备上的 **NetScaler Gateway** 之间有什么区别吗

从功能上讲，它们是相同的。NetScaler VPX 上的 NetScaler Gateway 支持 NetScaler 软件版本 14.1 中提供的所有可用的 NetScaler Gateway 功能。但是，由于 NetScaler 设备提供专用的 SSL 加速硬件，因此与 NetScaler VPX 实例相比，它提供更大的 SSL VPN 可扩展性。

除了 **NetScaler VPX** 可以在虚拟机管理程序上运行的明显区别之外，它与 **NetScaler** 物理设备有何不同

客户可以看到两个主要领域的行为差异。首先是 NetScaler VPX 无法提供与许多 NetScaler 设备相同的性能。其次，虽然 NetScaler 设备集成了自己的 L2 网络功能，但 NetScaler VPX 依赖虚拟机管理程序提供其 L2 网络服务。通常，它不会限制 NetScaler VPX 的部署方式。在物理 NetScaler 设备上配置的某些 L2 功能可能必须在底层虚拟机管理程序上配置。

NetScaler VPX 如何在应用程序交付市场中发挥作用

NetScaler VPX 通过以下方式改变了应用程序交付市场的游戏规则：

- 通过让 NetScaler 设备更实惠，NetScaler VPX 使任何 IT 组织都能部署 NetScaler 设备。它不仅适用于这些组织的最关键的 Web 应用程序，而且适用于其所有 Web 应用程序。
- NetScaler VPX 允许客户在其数据中心内进一步融合网络和虚拟化。NetScaler VPX 不能仅用于优化虚拟化服务器上托管的 Web 应用程序。它还使 Web 应用程序交付本身成为可轻松快速地部署在任何位置的虚拟化服务。IT 部门使用标准数据中心流程执行 Web 应用程序交付基础结构的预配、自动化和收费等任务。
- NetScaler VPX 开辟了新的部署架构，如果只使用物理设备，这些架构是不切实际的。NetScaler VPX 和 NetScaler MPX 设备可以根据每个应用程序的具体需求进行定制，以处理压缩和应用程序防火墙检查等处理器密集型操作。在数据中心边缘，NetScaler MPX 设备可处理大容量的网络范围任务，例如初始流量分配、SSL 加密或解密、拒绝服务 (DoS) 攻击防护和全局负载均衡。将高性能 NetScaler MPX 设备与易于部署的 NetScaler VPX 虚拟设备配对，为新式大型数据中心环境带来了无与伦比的灵活性和自定义功能，同时还降低了整体数据中心成本。

NetScaler VPX 如何适应我们的 **Citrix** 交付中心战略

随着 NetScaler VPX 的可用性，整个 Citrix 交付中心产品将作为虚拟化产品提供。整个 Citrix 交付中心受益于 Citrix XenCenter 中提供的强大的管理、资源调配、监视和报告功能。这可以快速部署到几乎任何环境中，并可以从任何地方集中管理。借助一个集成的虚拟化应用程序交付基础结构，组织可以交付桌面、客户端-服务器应用程序和 Web 应用程序。

加密

NetScaler VPX 支持 **SSL** 卸载吗

是。但是，NetScaler VPX 在软件中进行所有 SSL 处理，因此 NetScaler VPX 提供的 SSL 性能与 NetScaler 设备不同。NetScaler VPX 每秒最多可以支持 750 个新 SSL 交易。

安装在托管 **NetScaler VPX** 的服务器上的第三方 **SSL** 卡是否会加速 **SSL** 加密或解密

没有。支持第三方 SSL 卡无法将 NetScaler VPX 与特定的硬件实现相关联。它极大地削弱了组织在数据中心任何地方灵活托管 NetScaler VPX 的能力。当需要的 SSL 吞吐量超过 NetScaler VPX 提供的吞吐量时，必须使用 NetScaler MPX 设备。

NetScaler VPX 支持与物理 **NetScaler** 设备相同的加密密码吗

VPX 支持所有加密密码作为物理 NetScaler 设备，ECDSA 除外。

NetScaler VPX 的 **SSL** 事务吞吐量是什么**?**

有关 SSL 交易吞吐量的信息，请参阅 NetScaler VPX 数据表 。

定价和包装

NetScaler VPX 是如何打包的

NetScaler VPX 的选择与 NetScaler 设备的选择类似。首先，客户根据其功能要求选择 NetScaler 版本。然后，客户根据其吞吐量要求选择特定的 NetScaler VPX 带宽层。NetScaler VPX 有标准版、高级版和高级版可供选择。NetScaler VPX 提供从 10 Mbps (VPX 10) 到 100 Gbps (VPX 100G) 不等。更多详细信息可以在 NetScaler VPX 数据表中找到。

所有虚拟机管理程序的 **NetScaler VPX** 定价是否相同

是。

所有虚拟机管理程序上用于 **VPX** 的 **NetScaler SKU** 是否相同

是。

NetScaler VPX 许可证能否从一个虚拟机管理程序移动到另一个虚拟机管理程序（例如从 **VMware** 转移到 **Hyper-V**）

是。NetScaler VPX 许可证独立于底层虚拟机管理程序。如果您决定将 NetScaler VPX 虚拟机从一个虚拟机管理程序移至另一个虚拟机管理程序，则无需获得新的许可证。但是，您可能需要重新托管现有的 NetScaler VPX 许可证。

NetScaler VPX 实例能否升级

是。吞吐量限制和 NetScaler 系列版都可以升级。升级 SKU 可使用两种类型的升级。

如果我想在高可用性配对中部署 **NetScaler VPX**，我需要多少许可证

与 NetScaler 物理设备一样，NetScaler 高可用性配置需要两个活动实例。因此，客户必须购买两个许可证。

NetScaler VPX Express 和 90 天免费试用

NetScaler VPX 提供良好的性能。有关使用 **NetScaler VPX** 可达到的特定性能级别，请参阅 **NetScaler VPX** 数据手册

是。NetScaler VPX Express 包含完整的 NetScaler Premium 功能。从 NetScaler 版本 14.1–29.65 开始，NetScaler 修改了 VPX Express 行为。

NetScaler VPX Express 需要许可证吗

使用最新的 NetScaler VPX Express 版本（14.1–29.65 及更高版本），VPX Express 可以免费使用，并且不需要许可证文件即可安装或使用。无需任何承诺。如果您已经拥有 VPX Express 许可证，则之前的许可行为仍然有效。但是，如果您删除现有的 VPX Express 许可证文件并使用 14.1–29.65 或更高版本，则将应用更新的 VPX Express 行为。

NetScaler VPX Express 许可证会过期吗

使用新的 VPX express，无需许可证，也没有到期日期。如果您已经拥有 VPX 快速许可证，则该许可证在下载后一年到期。

NetScaler VPX Express 是否支持与 **NetScaler MPX** 设备相同的加密密码**?**

为了全面普及，NetScaler VPX 和 NetScaler VPX Express 上提供了 NetScaler 设备支持的所有相同的高度加密密码。它必须遵守相同的进出口条例。

我可以为 **NetScaler VPX Express** 提交技术支持案例吗

没有。NetScaler VPX Express 用户可以自由使用 NetScaler VPX 知识中心，也可以通过讨论论坛向社区寻求帮助。

NetScaler VPX Express 能否升级到零售版

是。只需购买所需的零售 NetScaler VPX 许可，然后将相应的许可应用到 NetScaler VPX Express 实例即可。

虚拟机管理程序

NetScaler VPX 支持哪些 **VMware** 版本

NetScaler VPX 支持 3.5 或更高版本的 VMware ESX 和 ESXi 版本。有关更多信息，请参阅 支持矩阵和使用指南

对于 **VMware**，您可以为 **VPX** 分配多少个虚拟网络接口**?**

您最多可以为 NetScaler VPX 分配 10 个虚拟网络接口。

在 **vSphere** 中，我们怎样才能访问 **NetScaler VPX** 命令行

VMware vSphere 客户端通过控制台选项卡提供对 NetScaler VPX 命令行的内置访问权限。此外，还可以使用任何 SSH 或 Telnet 客户端访问命令行。您可以在 SSH 或 Telnet 客户端中使用 NetScaler VPX 的 NSIP 地址。

您怎么能访问 **NetScaler VPX GUI**

要访问 NetScaler VPX GUI，请在任何浏览器的地址字段 `http://NSIP address` 中键入 NetScaler VPX 的 NSIP。

能否在高可用性设置中配置安装在同一 **VMware ESX** 上的两个 **NetScaler VPX** 实例

是，但不建议。硬件故障将影响两个 NetScaler VPX 实例。

能否在高可用性设置中配置两个运行在两个不同的 **VMware ESX** 系统上的 **NetScaler VPX** 实例

是。建议在高可用性设置中使用。

对于 **VMware** 来说，**NetScaler VPX** 是否支持与接口相关的事件

没有。不支持与接口相关的事件。

对于 **VMware** 来说，**NetScaler VPX** 支持带标签的 **VLAN** 吗

是。11.0 版及更高版本的 NetScaler VPX 支持带标记的 NetScaler VLAN。有关更多信息，请参阅 NetScaler 文档。

对于 **VMware**，**NetScaler VPX** 是否支持链路聚合和 **LACP?**

没有。NetScaler VPX 不支持链路聚合和 LACP。链路聚合必须在 VMware 级别进行配置。

我们如何访问 **NetScaler VPX** 文档

该文档可从 NetScaler VPX GUI 获得。登录后，选择 **Documentation**（文档）选项卡。

容量规划或大小调整

使用 **NetScaler VPX** 可以期待什么性能

NetScaler VPX 提供良好的性能。有关使用 NetScaler VPX 可达到的特定性能级别，请参阅 NetScaler VPX 数据手册 。

鉴于服务器 **CPU** 功率各不相同，我们如何估计 **NetScaler** 实例的最大性能**?**

使用更快的 CPU 可以带来更高的性能（达到许可证允许的最大值），而使用较慢的 CPU 肯定会限制性能。

NetScaler VPX 带宽或吞吐量限制是仅限入站流量，还是同时适用于入站和出站流量

NetScaler VPX 带宽限制仅适用于入站 NetScaler 的流量，无论请求流量还是响应流量。这表明 NetScaler VPX-1000（例如）可以同时处理 1 Gbps 的入站流量和 1 Gbps 的出站流量。入站和出站流量与请求流量和响应流量不同。对于 NetScaler，来自终端的流量（请求流量）和来自源服务器的流量（响应流量）都是“入站”（即进入 NetScaler）。

是否可以在同一台服务器上运行多个 **NetScaler VPX** 实例**?**

是。但是，请确保物理服务器有足够的 CPU 和 I/O 容量来支持主机上运行的总工作负载，否则 NetScaler VPX 性能可能会受到影响。

如果多个 **NetScaler VPX** 实例在物理服务器上运行，则每个 **NetScaler VPX** 实例的最低硬件要求是多少

必须为每个 NetScaler VPX 实例分配 2 GB 的物理 RAM、20 GB 的硬盘空间和 2 个 vCPU。对于关键部署，我们不建议对 VPX 使用 2 GB RAM，因为系统在内存受限的环境中运行。这可能会导致与规模、性能或稳定性相关的问题。建议使用 4 GB 内存或 8 GB 内存。

> 注意：
>
> NetScaler VPX 是一款延迟敏感的高性能虚拟设备。为了提供预期性能，设备需要在主机上预留 vCPU、预留内存以及固定 vCPU。此外，必须在主机上禁用超线程。如果主机不满足这些要求，则会出现诸如高可用性故障转移、VPX 实例内的 CPU 峰值、访问 VPX CLI 迟缓、pit boss 守护程序崩溃、数据包丢弃和吞吐量低等问题。
>
> 确保每个 VPX 实例都满足预定义的条件。

我是否可以在同一台服务器上托管 **NetScaler VPX** 和其他应用程序**?**

是。例如，NetScaler VPX、Citrix Virtual Apps Web Interface 和 Citrix Virtual Apps XML Broker 都可以虚拟化并且可以在同一台服务器上运行。为了获得最佳性能，请确保物理主机具有足够的 CPU 和 I/O 容量来支持所有正在运行的工作负载。

向单个 **NetScaler VPX** 实例添加 **CPU** 内核会提高该实例的性能吗

根据许可证，NetScaler VPX 实例目前最多可以使用 4 个 vCPU。向可以使用更多 CPU 的 NetScaler VPX 实例添加额外的 CPU 可以提高性能。

NetScaler VPX 为什么看起来像占用 **90%** 以上的 **CPU**，即使处于空闲状态亦如此**?**

这是正常行为，NetScaler 设备表现出相同的行为。要查看 NetScaler VPX CPU 利用率的真实程度，请使用 NetScaler CLI 中的 stat CPU 命令，或者从 NetScaler GUI 中查看 NetScaler VPX CPU 利用率。即使没有工作要

完成，NetScaler 数据包处理引擎始终“寻找工作”。因此，它会尽一切努力控制 CPU，而非释放 CPUI。在安装了 NetScaler VPX 的服务器上（而非其他服务器上），结果看起来像（从虚拟机管理程序的角度来看）NetScaler VPX 正在占用整个 CPU。从 “NetScaler 内部”（通过使用 CLI 或 GUI）中查看 CPU 利用率，可以显示正在使用的 NetScaler VPX CPU 容量。

系统要求

NetScaler VPX 的最低硬件要求是多少

下表说明了 NetScaler VPX 的最低硬件要求。

类型	要求
——-	——————————————————————
处理器	配备 Intel Xeon 或 AMD EPYC 的双核服务器。
内存	至少 2 GB。但是，建议使用 4 GB。
磁盘	至少 20 GB 的硬盘驱动器。
虚拟机管理程序	Citrix Hypervisor 5.6 或更高版本、VMware ESX/ESXi 3.5 或更高版本，或者带有 Hyper-V 的 Windows Server 200
网络连接	最低 100 Mbps，但建议使用 1 Gbps。
NIC	与您正在使用的虚拟机管理程序兼容的 NIC。

> 注意：
>
> 对于关键部署，NetScaler VPX 首选 4 GB 内存。NetScaler VPX 拥有 2 GB 的内存，可在内存受限的环境中运行。这可能会导致与规模、性能或稳定性相关的问题。

有关系统要求的更多信息，请参阅 NetScaler VPX 数据手册。

> 注意：
>
> 从 NetScaler 13.1 版本开始，VMware ESXi 虚拟机管理程序上的 NetScaler VPX 实例支持 AMD EPYC 处理器。

什么是 **Intel VT-x**

这些功能有时被称为“硬件辅助”或“虚拟化辅助”，会将客户机操作系统运行的敏感或特权 CPU 指令捕获到虚拟机管理程序。这简化了虚拟机管理程序上的托管来宾操作系统（适用于 NetScaler VPX 的 BSD）。

VT-x 有多常见**?**

实际上，过去两年内发货的所有服务器都可能支持 VT-x。许多服务器在 BIOS 中都禁用了虚拟化协助功能。在假设无法运行 NetScaler VPX 之前，请检查是否需要在服务器上更改此设置。

NetScaler VPX 有硬件兼容性列表 **(HCL)** 吗

只要服务器支持 Intel VT-x，NetScaler VPX 就必须在任何与底层虚拟机管理程序兼容的服务器上运行。有关受支持的平台的完整列表，请参阅虚拟机管理程序 HCL。

NetScaler VPX 基于哪个版本的 **NetScaler** 操作系统

NetScaler VPX 基于 NetScaler 9.1 或更高版本。

由于 **NetScaler VPX** 在 **BSD** 上运行，它能否在安装了 **BSD Unix** 的服务器上本地运行

没有。NetScaler VPX 需要运行虚拟机管理程序。详细的虚拟机管理程序支持可在 NetScaler VPX 数据表中找到。

其他技术常见问题解答

配备多个 **NIC** 的物理服务器上的链路聚合是否有效**?**

不支持 LACP。对于 Citrix Hypervisor，支持静态链路聚合，并且限制为四个通道和七个虚拟接口。对于 VMware，NetScaler VPX 不支持静态链接聚合，但可以在 VMware 级别进行配置。

VPX 是否支持基于 **MAC** 的转发 **(MBF)?** 与 **NetScaler** 设备的实现相比有什么变化吗 与 **NetScaler** 设备的实现相比有什么变化吗

支持 MBF，其行为方式与 NetScaler 设备相同。虚拟机管理程序基本上是将从 NetScaler VPX 收到的所有数据包切换到外部，反之亦然。

NetScaler VPX 升级过程是如何进行的

升级的执行方式与 NetScaler 设备相同：下载内核文件并在 GUI 中使用 install ns 或升级实用程序。

如何分配闪存和磁盘空间**?** 我们可以改变该方式吗**?** 我们可以改变该方式吗

/闪存 = 965M /var = 14G 必须为每个 NetScaler VPX 实例分配至少 2 GB 内存。NetScaler VPX 磁盘映像的大小为 20 GB 以便于维护，例如，可以获取和存储多达 4 GB 核心转储以及日志和跟踪文件的空间。虽然可以生成较小的磁盘映像，但目前还没有计划这样做。/flash 和 /var 都在同一个磁盘映像中。出于兼容性的考虑，它们作为单独的文件系统保存。有关详细的内存分配建议，请参阅 NetScaler VPX 数据表。

我们能否添加新的硬盘驱动器来增加 **NetScaler VPX** 实例上的空间

是。从 NetScaler 版本 13.1 build 21.x 起，您可以选择通过添加第二个磁盘来增加 NetScaler VPX 实例上的磁盘空间。连接第二个磁盘时，“/var/crash”目录将自动安装到该磁盘上。第二个磁盘用于存储核心文件和日志记录。用于存储核心文件和日志文件的现有目录继续像以前一样工作。

> 注意：
>
> 在 NetScaler 设备降级时进行外部备份，以避免数据丢失。

有关如何将新硬盘驱动器 (HDD) 附加到云上的 NetScaler VPX 实例的信息，请参阅以下内容：

- Azure 文档

  > 注意：
  >
  > 要在 Azure 上部署的 NetScaler VPX 实例上附加辅助磁盘，请确保 Azure VM 大小具有本地临时磁盘。有关更多信息，请参阅 没有本地临时磁盘的 Azure 虚拟机大小。

- AWS 文档
- GCP 文档

> 警告：
>
> 向 NetScaler VPX 添加新 HDD 后，在以下情况下，一些处理移动到新 HDD 的文件的脚本可能会失败：
>
> 如果您使用“链接”shell 命令创建指向文件的硬链接，这些文件已移动到新的 HDD。
>
> 将所有此类命令替换为“ln-s”以使用符号链接。另外，相应地修改失败的脚本。

我可以增加 **NetScaler VPX** 上的主磁盘大小吗

自 NetScaler 版本 14.1 Build 21.x 起，管理员可以动态地将 NetScaler VPX 的主磁盘大小从 20 GB 增大到 1 TB。随后，您可以再次增加到 1 TB。要增加磁盘空间，请在相应的云或虚拟机管理程序用户界面中将主磁盘大小扩展到至少 1 GB。

> 注意：
>
> 您只能增加磁盘的大小。一旦分配了新大小，以后就无法减小了。因此，仅在必要时才增加磁盘大小。

如何手动增加 **NetScaler VPX** 的主磁盘大小

按照以下步骤手动增加虚拟机管理程序或云中的 VPX 主磁盘大小：

1. 关闭 VM。
2. 将默认磁盘大小 20 GB 扩展到更高的值。例如，20 GB 到 30 GB 或 40 GB。对于 Azure，将 32 GB 的默认磁盘大小扩展到 64 GB。

3. 打开 VM 并输入启动提示符。
4. 使用“boot -s”命令登录到单用户模式。
5. 验证磁盘空间。您可以使用“gpart show”命令检查新分配的磁盘空间。
6. 记下分区名称。例如，虚拟机分区为 da0。
7. 使用“gpart resize”命令调整磁盘分区的大小。

   示例：让我们通过运行以下命令调整 da0 MBR 分区的大小以包含 10 GB 的可用空间。

   ```
   gpart resize -i 1 da0
   ```
8. 将空闲空间合并到最后一个分区。

   Example:

   ```
   gpart resize -i 5 da0s1
   ```
9. 使用“growfs”命令扩展文件系统以包括新分配的可用空间。

   Example:

   ```
   growfs /dev/ada0s1e
   ```
10. 重启虚拟机并在 shell 提示符下使用“df -h”命令验证增加的磁盘空间。

关于 **NetScaler VPX** 版本编号以及与其他版本的互操作性，我们可以期待什么

NetScaler VPX 的内部版本编号与 9.1 类似。Cl（经典）和 9.1。Nc (nCore) 发行版，例如 9.1_97.3.vpx、9.1_97.3.nc 和 9.1_97.3.cl。

NetScaler VPX 能否成为 **NetScaler** 设备高可用性设置的一部分

不是支持的配置。

NetScaler VPX 中所有可见的接口是否与虚拟机管理程序上的接口数量直接相关

没有。您最多可以通过 NetScaler VPX 配置实用程序添加七个接口（10 个适用于 VMware），在虚拟机管理程序上只有一个物理 NIC。

能否使用 **Citrix Hypervisor XenMotion**、**VMware vMotion** 或 **Hyper-V** 实时迁移来移动 **NetScaler VPX** 的活动实例

NetScaler VPX 不支持 Hyper-V 实时迁移。从 NetScaler 版本 13.0 开始支持 vMotion。从 NetScaler 版本 14.1 版本 17.38 开始，支持实时迁移（前身为 XenMotion）。